EMC Corporation
Isilon® OneFS® v6.5.4

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.4

Prepared for:

EMC Corporation
176 South Street
Hopkinton, MA 01748
United States of America

Phone: +1 508 435 1000

http://www.emc.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The subject of the evaluation is the EMC Isilon® OneFS® v6.5.4, and will hereafter be referred to as the TOE throughout this document. The TOE is an operating system that provides a distributed file system for storage and management of unstructured and file-based data on the Isilon clustered storage system.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	EMC Corporation Isilon® OneFS® v6.5.4 Security Target
ST Version	Version 1.4
ST Author	Corsec Security, Inc.
ST Publication Date	4/12/2012
TOE Reference	EMC Isilon® OneFS® v6.5.4.10

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

The Isilon® OneFS® v6.5.4 distributed file operating system provides a single point of management for Isilon's clustered storage system. It combines three layers of traditional storage architectures: file systems, volume manager, and RAID[1] into one unified software layer. OneFS provides a capacity of over 85 gigabytes per second of throughput and more than 10.4 petabytes of capacity in a single file system. The nodes are fully symmetric and can be deployed with a minimum of three nodes and a maximum of 144 nodes per cluster. The nodes are connected through a private, back-end Infiniband network.

Each node on an Isilon clustered storage system is a peer, so any node can handle a request. For each job one node takes the point to participate in a protocol, but any of the nodes can perform this function. OneFS provides each node in the system with knowledge of the entire file system layout. Each cluster creates a single namespace and file system. There is no partitioning, and no need for volume creation. All data is striped across multiple nodes in the cluster and metadata is also distributed across the cluster. Every node has access to the data in the event of a failure. When a new node is added content is load balanced across all nodes.

The Isilon cluster is designed to continuously serve data, even when one or more components simultaneously fail. Data protection is applied at the system or file level and metadata is protected at the same (or higher) level of protection as the data they reference. Isilon provides a cluster-wide data protection tool called FlexProtect. FlexProtect detects and repairs files and directories that are in a degraded state. The system can be configured with different data protection levels. The protection levels can be modified without taking the cluster or file system offline. The following protection levels are possible and can be set globally, or at the file or directory level:

- N+1 – The cluster can absorb the failure of any single drive or the unscheduled shutdown of any single node without causing any loss of stored data.
- N+2 - The cluster can recover from two simultaneous drive or node failures without sustaining any data loss.
- N+2:1 - The cluster can recover from two simultaneous drive failures or one node failure without sustaining any data loss.
- N+3 - The cluster can recover from three simultaneous drive or node failures without sustaining any data loss.
- N+3:1 - The cluster can recover from three simultaneous drive failures or one node failure without sustaining any data loss.
- N+4 – The cluster can recover from four simultaneous drive or node failures without sustaining any data loss.

Data mirroring of one to eight mirrors of specified content is also supported, but requires significant overhead. Each node contains a battery-backed non-volatile read access memory (NVRAM) card that holds the cluster journal and can last up to three days without system power. The files journal system is a write-ahead journal that stores information about changes to the file system before it is written to disk. This journal can be used for consistency when recovering from a system failure. The system can continuously reallocate data and make storage space more usable and efficient. Isilon AutoBalance adjusts the cluster's data layout so that capacity is balanced equally, within 5%, across all nodes. AutoBalance automatically runs when new nodes or drives are added to the cluster.

If a drive or node fails, the protection status of the data on that failed drive or node is considered degraded until the data has been re-protected to the configured level. No data is lost in the degraded status; the node is in the process of restriping the data to fully protect it. OneFS supports a smartfail that puts a device in quarantine and restripes the data before it is removed from the cluster. This data can be available for read-only access when in quarantine. Rebuilding data is performed in the free space of the cluster, eliminating the need for a hot spare node or drive. Isilon monitors the health of all disk drives to determine if a smartfail is necessary.

Isilon supports the following authentication methods:

[1] Redundant Array of Independent Disks (RAID)

- Local-user mode
- External authentication:
    - Microsoft Active Directory Services
    - Lightweight Directory Access Protocol (LDAP)
    - Network Information Service (NIS)

Clients connect to the cluster using multiple external GigE connections. OneFS supports standard network communications protocols including; Network Files System (NFS)v3, NFSv4, NFS Kerberized Sessions (UDP[2] or TCP[3]), UNIX file sharing protocols; Internet Small Computer System Interface (iSCSI), Server Message Block (SMB)1, SMB2, Windows file sharing protocols; Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), network data management protocol (NDMP), simple network management protocol(SNMP), lightweight directory access protocol (LDAP), active directory service (ADS), network information service (NIS) reads and writes, and File Transfer Protocol (FTP). OneFS supports both UNIX, Windows, and mixed UNIX and Windows permissions. OneFS can be managed through a web-based user interface (UI), Web Administration, through a command-line interface (CLI), or through the front panel controls on the storage node.

SmartConnect is a software module that balances and manages client connections to the cluster. SmartConnect allows the administrator to manage user connections based on central processing unit (CPU) utilization, aggregate throughput, connection count or round robin. Internet Protocol (IP) addresses can be allocated statically or dynamically. If they are allocated dynamically than automatic rebalancing and failover can also be configured. If a node fails or goes offline the effected IP addresses migrate to another node in the cluster maintaining client connections. IP address pools can be defined within a subnet to logically partition the network interfaces.

Isilon SyncIQ is an optional software tool that allows flexible management and data synchronization between clusters. The tool automatically generates a snapshot of the data set on the source cluster when a data synchronization or copy job starts. The most recent snapshot is retained until the next job runs. This snapshot can be used to rollback to the previous system state if necessary. SyncIQ policies can be set for each job profile to determine how and when synchronization jobs will run. In addition SnapshotIQ can be used to capture point-in-time images of data stored on a cluster. These snapshots can be scheduled to be performed at hourly, daily, weekly, monthly or yearly recurring intervals at the directory, sub-directory, or file-system levels. SnapshotIQ can be used independently or in conjunction with SyncIQ. SyncIQ can also be configured to validate file integrity by performing a checksum on each file data packet in a synchronization job.

OneFS supports Network Data Management Protocol (NDMP) versions 3 and 4 for backing up data to a data management application (DMA). Backup logs are created that log all NDMP sessions and activity. The following types of backups are supported:

- Full backups
- Full restores
- Direct access restore (DAR) single-file restores and three-way backup
- Incremental backups
- Restore-to-arbitrary system
- Integration with access control list (ACL)s
- Integration with alternative data streams

Isilon technical support personnel can request logs on all systems that have SupportIQ enabled. They use data gathering scripts to gather log data and collect information about a cluster's configuration setting and operations. This is sent by SFTP for support personnel to review.

[2] UDP – User Datagram Protocol
[3] TCP – Transmission Control Protocol

Another option for the system is the Isilon SmartQuotas module that monitors and enforces administrator defined storage limits. SmartQuotas can manage storage utilization, monitor disk storage, and issue alerts when disk storage limits are exceeded. There are two types of quotas supported, accounting quotas that monitor disk storage, and enforcement quotas that monitor and limit disk storage.

Lastly, SmartPools can be enabled to define subgroups of nodes within a cluster to create disk pools. The disk pools are a dynamic group of disks that can be configured through provisioning rules to filter files into specific disk pools according to file attributes such as: files size, file type, location, file creation, and change, modification or access time. File pool policies can also be set to determine the performance access profile, set the protection level and define movement of specific data among the tiers. SmartPools also allows an administrator to configure disk pool spillover that defines how write operations are handled to a full disk pool.

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The software-only TOE is the Isilon® OneFS® v6.5.4 operating system that provides distributed file system management software and multiple add-on software components that are listed in 1.4.1. Six nodes are required for the evaluated configuration of the TOE, so six instances of Isilon® OneFS® v6.5.4 with all add-on components comprise the TOE. Authenticated administrators can manage the TOE through a CLI commands and Web Administration interface. The Web Administration interface is accessed using HTTP or HTTPS and standard web browsers such as Internet Explorer 7.x or Firefox 3.x. The CLI commands interface is used for initial configuration and is accessed over a secure shell (SSH) connection. Both interfaces require authentication. Users access the file system through a front end Local Area Network (LAN) connected to external ethernet connections and must also authenticate prior to access. There is also a front panel external interface on the hardware. While the panel itself is outside of the TOE boundary the logical mapping of the panel is an interface on the TOE. Through this interface users may view status on the hardware and cluster, perform an install of a new version of the software, and change the cluster to read-only or read/write. The installation of the new software can only be done after an authorized administrator downloads the file onto the cluster and would take the TOE out of the evaluated configuration.

Inter-cluster communication takes place on a dedicated InfiniBand backplane. Figure 1 shows the details of the deployment configuration of the TOE:

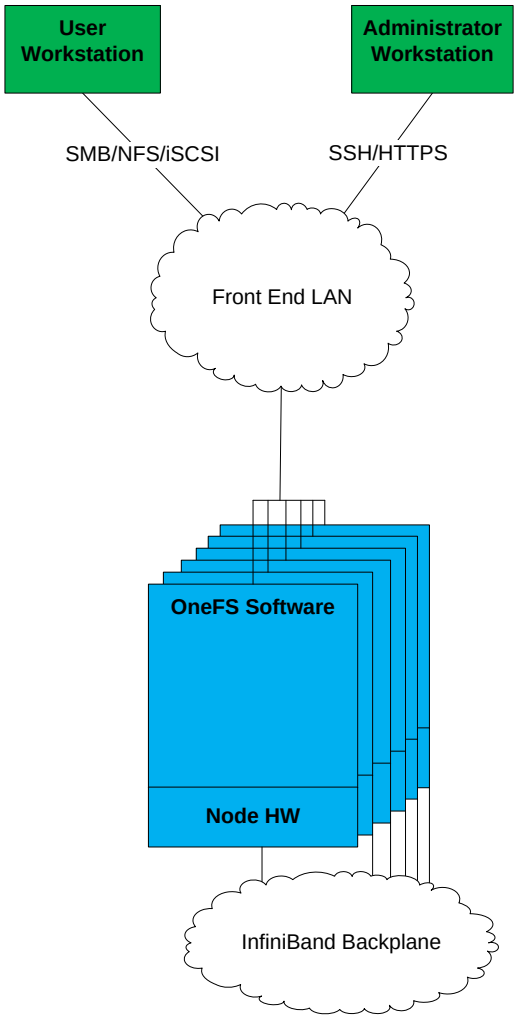

Figure 1 Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The TOE includes the following components and add-on products:

- OneFS® 6.5.4 – the operating system (OS) that provides distributed file system management including a Web GUI and CLI for TOE management
- FlexProtect™ – monitors disk and node health, rebuilds failed disks, and preemptively migrates data off of at-risk components
- SmartConnect™ Advanced – Software module add-on that balances connections to the cluster
- SyncIQ® – Software module add-on that provides policy-based file replication, standard disk-to-disk file backup and restores.
- SmartQuotas – Add-on software module that provides quota management and enforces administrator defined storage limits
- SnapshotIQ™ – Add-on software module that creates a point-in-time copy of any of the shared file directories
- SmartPools™ – Defines subgroups of nodes, called disk pools, that allow data to be stored and moved according to file attributes
- iSCSI – Add-on software module that provides iSCSI targets on the cluster and enables initiators on client computers to send SCSI commands to those targets

1.4.2 TOE Environment

The TOE environment consists of the runtime environments and physical or virtual hardware platforms on which the TOE is intended to operate. The typical deployment is in a large enterprise or government data center. The TOE is designed to run on Isilon's clustered storage system hardware. The Isilon Platform nodes are: S Series, X Series, and NL Series. The TOE boundary envelops only those software components described in the TOE description, section 1.5 and none of the underlying, hardware, or network infrastructures.

In addition to hardware, the TOE needs the following environmental components in order to function properly:

- cables and connectors, that allow all of the TOE and environmental components to communicate with each other
- Ethernet switches that are non-blocking switch fabric with a minimum 1MB buffer per switch port, and jumbo frame support for front-end network
- One of the following InfiniBand Switches:
  - Cisco SFS 7000 or 7008
  - Flextronics F-X430061, F-X430062, or F-X 430066
  - Mellanox MTS2400
- At least two client systems. One running Microsoft Windows operating system and the other running a Linux operating system.
- An administrator workstation with a web browser such as Internet Explorer, Firefox, Opera, or Safari

The TOE is intended to be deployed in a secure data center that protects physical access to the TOE. The TOE is intended to be interconnected by an InifiBand back-end private network that does not connect directly to external hosts.

The TOE provides access control to a clustered storage system with analytic capabilities. Some of the available access control mechanisms (such LDAP) require the use of a remote authentication server. The TOE environment is required to provide this.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE. The TOE is a distributed file system that manages Isilon clustered storage systems, which are compliant to the minimum software and hardware requirements as listed in 1.4.2. The TOE is installed in a large enterprise network as depicted in the figure below. The essential components for the proper operation of the TOE in the evaluated configuration are three of each of the below items:

- OneFS software, which includes FlexProtect
- SmartConnect Advanced software module
- SyncIQ software module
- SmartQuotas software module
- SnapshotIQ software module
- iSCSI module

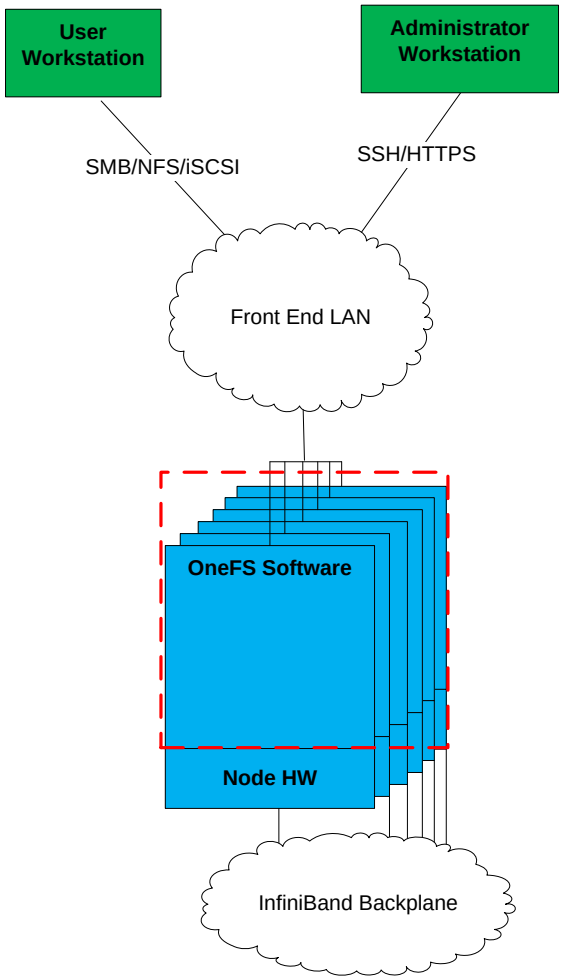

Figure 2 Physical TOE Boundary

1.5.1.1 TOE Software

The TOE is a software only TOE meant to be run on Isilon platform nodes.

1.5.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- Isilon OneFS 6.5.4 User Guide, 2011
- Isilon OneFS 6.5 Command Reference, 2011
- Isilon Systems S200 Installation and Setup Guide, February 2011
- Isilon IQ Quick Start Guide, Rev A
- Isilon Systems Rail Kit Installation Guide: 1U or 1U Node, Rev A
- Isilon Systems Site Planning and Preparation Guide, September 2011

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions (TSF)
- Resource Utilization
- Trusted Path/Channels

1.5.2.1 Security Audit

The TOE generates many different types of logs. Logs are maintained for cluster and node health, configuration, and performance; data protection processes; user access to file shares, directories and file system; jobs performed on the system; and anti-virus scans. The audit data is stored on the nodes in the cluster. Access to the audit data is restricted to authorized administrators. Logs can be accessed individually, but it is more common to use a gathering script to retrieve information from multiple logs. Logs are automatically rotated when they reach an administrator set capacity. Audit data is protected at the same level as the user data.

1.5.2.2 User Data Protection

The TOE controls access to user data via a Data Access Security Functional Policy (SFP). The Data Access SFP relies on Windows ACL and UNIX permissions, collectively called authorization data, to protect data at the file level. The Root role is, by default, the owner of all files and directories. The file owner can assign permissions to the file. An authorized administrator can change the file permissions. The TOE can translate UNIX permissions into ACLs and vice versa. Additionally the TOE maintains data integrity via a Data Transfer SFP that covers the assigned access controls and integrity checking when data is transferred within or outside of the TOE. The FlexProtect system and configurable mirroring of data support the Data Transfer SFP by detecting and correcting errors and mirroring data across the cluster to prevent single points of failure. The SnapshotIQ module also enforces the Data Transfer SFP by assisting in rollback of the directories or file system. The SyncIQ module also enforces administrator defined policies when transferring data for synchronization and backup to a separate cluster.

1.5.2.3 Identification and Authentication

Identification and Authentication can be performed locally or using external methods such as: Active Directory, LDAP, or NIS. Users access the TOE through one of the following file-share protocols:

- NFS – UNIX file exports that is enabled by default and configurable by admin through the Web Administration or CLI commands interface.
- SMB – Windows file share that is enabled by default and configurable by an administrator through the Web Administration interface.
- HTTP – The Web Administration interface for cluster administration. HTTP services in the TOE are managed collectively through the **File Sharing > HTTP** page on the Web Administration interface. Services must be in the **Disable HTTP and redirect to web interface**. This means that HTTP access is disabled and only HTTPS access to the Web Administration interface is allowed.

There is an external interface on the node hardware that enables users to view status, attach a hard disk, update the software, and change the cluster from read-only to read and write access. This interface is protected by the TOE environment from unauthorized users. All other tasks performed by a user or administrator require successful authentication with the TOE. Once authenticated the ACLs and permissions on files will be used to determine what access the user has to each file.

1.5.2.4 Security Management

There are two interfaces for security management, the Web Administration interface and the CLI commands interface. There is a root and admin role that can create and manage additional user accounts, manage protection levels and disk quotas, access and modify log records, and enable or disable authentication modes. The root and admin roles access the TOE through both interfaces. In addition the

root role has access to the TOE through the CLI to perform OS upgrades. The admin and root roles can enable and disable authentication protocols, set protection levels, assign disk quotas to users and groups, and monitor system health and performance.

1.5.2.5 Protection of the TSF

The TOE also enforces the Data Transfer SFP through protection of the TSF. FlexProtect detects potential disk or node failures and restripes data to separate disks or nodes. The failed disk is then taken offline and rebuilt. This process is automated and data is protected before the disk or node can go offline. The TOE also includes a sysclock, which provides the TOE with a reliable timestamp. The system also performs backup of ACLs, logs, and user data using NDMP to ensure inter-TSF data consistency.

1.5.2.6 Resource Utilization

The TOE includes a SmartQuotas software module that enforces administrator defined disk storage quotas for users, groups, and directories.

1.5.2.7 Trusted Path/Channels

A dedicate line is used for communication between clusters when performing synchronization or backup of data to another cluster.

1.5.3 Product Physical and Logical Features and Functionality not included in the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- All hardware systems upon which the TOE runs
- InsightIQ
- Isilon for vCenter
- SmartLock
- Administrator workstations
- SupportIQ
- Anti-Virus Scans

2 Conformance Claims

This section and Table 2 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 2 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2011/05/30 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[4] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They 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.
- TOE users: They 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 users are, however, assumed not to be willfully hostile to the TOE.)

Both 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. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 3 below lists the applicable threats.

Table 3 Threats

Name	Description
T.ACCOUNTABILITY	An unidentified threat could result in authorized users of the TOE not being held accountable for their actions within the TOE.
T.AUDIT_COMPROMISE	A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
T.CRITICAL_FAILURE	An unidentified threat agent could cause the TOE to experience a failure of a critical component that prevents users and administrators from being able to access TOE functionality.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.TAMPERING	A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment and gain unauthorized access to TOE functionality.
T.UNAUTH	A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.
T.UNAVAILABILITY	The TOE may be overwhelmed by legitimate user tasks, preventing or

[4] IT – Information Technology

Name	Description
	delaying any TOE functionality from being accessed.

3.2 Organizational Security Policies

There are no organizational security policies defined for this Security Target.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 4 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 4 Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware.
A.LOCATE	The TOE is 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.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 5 below.

Table 5 Security Objectives for the TOE

Name	Description
O.AUDIT_STORAGE	The TOE will contain mechanisms to provide secure storage and management of the audit log.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users.
O.AUDIT_REVIEW	The TOE will contain mechanisms to allow the authorized security administrator to view and sort the audit logs.
O.AUDIT_MONITOR	The TOE will provide the ability to monitor logs, alert administrators, and perform automated functions if logs exceed capacity.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.FAIL_SECURE	The TOE will provide mechanisms to allow for secure failure and recovery.
O.PROTECT	The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized security administrator in management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE must protect user data in accordance with its security policy.
O.TIMESTAMP	The TOE will provide reliable time stamps.
O.QUOTAS	The TOE will provide the ability to define quotas for usage of TOE resources, and prevent further allocation of resources once the quotas are reached.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 6 below lists the IT security objectives that are to be satisfied by the environment.

Table 6 IT Security Objectives

Name	Description
OE.NO_BYPASS	The operational environment shall ensure the TOE security mechanisms cannot by bypassed in order to gain access to the TOE resources.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.PLATFORM	The hardware on which the TOE operates must support all required TOE functions.
OE.SECURE_COMMS	The operational environment will provide a secure line of communications between external entities and the TOE.
OE.TRUST_IT	Each operational entity the TOE relies on for security functions will be installed, configured, managed and maintained in a manner appropriate to the IT entity, and consistent with the security policy of the TOE and the relationship between them.

4.2.2 Non-IT Security Objectives

Table 7 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 7 Non-IT Security Objectives

Name	Description
NOE.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.
NOE.PHYSICAL	Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This Security Target does not define any extended functional components.

5.2 Extended TOE Security Assurance Components

This Security Target does not define any extended assurance components.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 8 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 8 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓	✓	
FAU_SAR.1	Audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FAU_STG.4	Prevention of audit data loss	✓	✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security based attribute control		✓		
FDP_ETC.2	Export of user data with security attributes		✓		
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FDP_ITC.2	Import of user data with security attributes		✓		
FDP_ROL.1	Basic rollback		✓	✓	
FIA_UAU.1	Timing of authentication		✓		
FIA_UAU.5	Multiple authentication mechanisms		✓		

Name	Description	S	A	R	I
FIA_UID.1	Timing of identification		✓		
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1(a)	Management of security attributes	✓	✓		
FMT_MSA.1(b)	Management of security attributes	✓	✓		✓
FMT_MSA.3(a)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(b)	Static attributes 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_ITT.1	Basic internal TSF data transfer protection	✓			
FPT_RCV.3	Automated recovery without undue loss		✓		
FPT_STM.1	Reliable time stamps				
FPT_TDC.1	Inter-TSF basic TSF data consistency		✓		
FRU_RSA.1	Maximum quotas	✓	✓		
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation
Hierarchical to: No other components.
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) [*disk quotas, synchronizations, file and directory repairs, disk and nodes failures, connection and disconnection attempts*].
FAU_GEN.1.2
The TSF shall record within each **connection and disconnection** 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, [*node name and IP address (if applicable)*].
Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review
Hierarchical to: No other components.
FAU_SAR.1.1
The TSF shall provide [*root and admin roles*] with the capability to read [*all audit information*] from the audit records.
FAU_SAR.1.2
The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1 Protected audit trail storage
Hierarchical to: No other components.
FAU_STG.1.1
The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2
The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss
Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
FAU_STG.4.1
The TSF shall [overwrite the oldest stored audit records] and [*send email alert*] if the audit trail is full.
Dependencies: FAU_STG.1 Protected audit trail storage

6.2.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1
The TSF shall enforce the [*Data Access SFP*] on [*Subjects: users and client systems accessing data; Objects: files, directories, exports, targets, shares, and clusters; and Operations: access, read, write, delete, execute*].
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
FDP_ACF.1.1
The TSF shall enforce the [*Data Access SFP*] to objects based on the following: [
Subject attributes: as defined in column two, Subject Attributes, of Table 9
Objects: as defined in column three, Data Attributes, of Table 9.]

Table 9 Security Attributes for TOE

File Share Type	Subject Attributes	Data Attributes
SMB	SID[5]	DACL[6], ACE[7]
NFS	UID[8], GID[9]	rwx[10] permissions, DACL
iSCSI	Username	target's CHAP secrets list

FDP_ACF.1.2
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*a user can perform the operations granted to their SID, ACE, UID, or GID according to the file or directory's DACL or rwx permissions*].
FDP_ACF.1.3
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [
1) *With SMB protocol an authorized administrator has assigned the user to a DACL that permits access to the share and the file*
2) *With NFS protocol an authorized administrator has granted access for the client system on the export and assigned the user to a DACL*
3) *Access to an iSCSI target is authorized only to users with a username and CHAP secret in the target's CHAP secrets list*].
FDP_ACF.1.4
The TSF shall explicitly deny access of subjects to objects based on the [
1) *With SMB protocol an authorized user denies permission to the object through a DACL*
2) *With NFS protocol an authorized administrator denies the client name access to the export or an authorized user denies permission to the object through a DACL*
3) *Access to iSCSI targets is denied if username and CHAP secret is not in the target's CHAP secrets list*].
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

[5] SID – Security Identifier
[6] DACL – Discretionary Access Control List
[7] ACE – Access Control Entry
[8] UID – Unique Identifier
[9] GID – Group Identifier
[10] rwx – read, write, execute

FDP_ETC.2 Export of user data with security attributes

Hierarchical to: No other components.

FDP_ETC.2.1

The TSF shall enforce the [*Data Transfer SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2

The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3

The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4

The TSF shall enforce the following rules when user data is exported from the TOE: [*access control data is sent for files or directories, error correction information is sent with data so data integrity can be maintained, and authorized administrator set SyncIQ policies are followed*].

Dependencies: FDP_IFC.1 Subset information flow control

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1

The TSF shall enforce the [*Data Transfer SFP*] on [
Subjects: *Users, Administrators, FlexProtect process, SyncIQ process, SnapshotIQ process*
Information: files, directories
Operations: mirror data to separate node, rebuild data, synchronize data
].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1

The TSF shall enforce the [*Data Transfer SFP*] based on the following types of subject and information security attributes: [
Subjects: Users, Administrators, privileged kernel code, such as FlexProtect, SyncIQ, and SnapshotIQ processes
Information: files, directories
Information security attribute: DACLs, rwx permissions, integrity of subject
].

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*rebuild data to separate node when integrity error is detected and maintain access control for files*].

FDP_IFF.1.3

The TSF shall enforce the [*access controls and data integrity*].

FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules: [*detected data integrity error authorizes file or directory rebuilding or user access controls define rules for users to access data*].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [*no rules*].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3(b) Static attribute initialisation

FDP_ITC.2 Import of user data with security attributes

Hierarchical to: No other components.

FDP_ITC.2.1

The TSF shall enforce the [*Data Transfer SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2

The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3

The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4

The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*protection level is maintained at file system level or higher, error correction information is received with data to confirm data integrity, access controls are followed, and authorized administrator set SyncIQ policies are followed*].

Dependencies: FDP_IFC.1 Subset information flow control
FTP_ITC.1 Inter-TSF trusted channel
FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ROL.1 Basic rollback

Hierarchical to: No other components.

FDP_ROL.1.1

The TSF shall enforce [*Data Transfer SFP*] to permit the rollback of the [*all operations*] on the [*directory, sub-directory, or file-system*].

FDP_ROL.1.2

The TSF shall permit operations to be rolled back ~~within~~ **to** the [*last TOE created snapshot*].

Dependencies: FDP_IFC.1 Subset information flow control

6.2.3 Class FIA: Identification and Authentication

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components

FIA_UAU.1.1

The TSF shall allow [*attaching a hard disk, viewing of cluster status, updating to new software version, changing node service parameters, and joining an unconfigured node to a cluster*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1

The TSF shall provide [*local database, Active Directory service, LDAP, NIS, file provider database, and CHAP*[11]] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*authorized user-defined configuration and the external protocol's rules*].

Dependencies: No dependencies

FIA_UID.1 Timing of identification

Hierarchical to: No other components

FIA_UID.1.1

The TSF shall allow [*attaching a hard disk, viewing of cluster status, updating to new software version, changing node service parameters, and joining an unconfigured node to a cluster*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

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

Dependencies: No dependencies

[11] CHAP – Challenge-Handshake Authentication Protocol

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1
The TSF shall restrict the ability to [determine the behavior of, disable, enable, modify the behavior of] the functions [*authentication protocols, disk storage quotas, access modes, run or schedule jobs, and protection levels*] to [*root, admin, or users with sufficient permissions*].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(a) Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1
The TSF shall enforce the [*Data Access SFP*] to restrict the ability to [change, query, modify, delete, *[create]*] the security attributes [*DACL and rwx permissions*] to [*root and admin roles*].
Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(b) Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1
The TSF shall enforce the [*Data Transfer SFP*] to restrict the ability to [change, query, modify, delete, [*none*]] the security attributes [*file integrity data*] to [*root and admin roles*].
Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3(a) Static attribute initialisation
Hierarchical to: No other components.
FMT_MSA.3.1
The TSF shall enforce the [*Data Access 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 [*root or admin roles*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3(b) Static attribute initialisation
Hierarchical to: No other components.
FMT_MSA.3.1
The TSF shall enforce the [*Data Transfer 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 [*root and admin roles*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies: FMT_MSA.1(b) Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1

The TSF shall restrict the ability to [query, modify, delete, [*other operations as defined in column 'Operation' of Table 10*]] the [*TSF data as defined in column 'TSF Data' of Table 10*] to [*Roles as defined in 'Role' of Table 10*].

Table 10 Management of TSF Data

Operation	TSF Data	Role
Create, Modify, Query, Delete	User accounts	Root , Admin
Reset	User passwords	Root, Admin
Set, Modify	Protection levels	Root, Admin, User w/ permission
Enable, Disable	Authentication mode	Root, Admin
View, Modify, Query	Audit records	Root, Admin

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*management of security function behavior, management of security attributes, and management of TSF data*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*root, admin, and user*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [*disk or node failure*].
Dependencies: No dependencies.

FPT_ITT.1 Basic internal TSF data transfer protection
Hierarchical to: No other components.
FPT_ITT.1.1
The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.
Dependencies: No dependencies

FPT_RCV.3 Automated recovery without undue loss
Hierarchical to: FPT_RCV.2 Automated recovery
FPT_RCV.3.1
When automated recovery from [*disk, interface, or node failures*] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.
FPT_RCV.3.2
For [*disk or interface failure*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.
FPT_RCV.3.3
The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [*none*] for loss of TSF data or objects under the control of the TSF.
FPT_RCV.3.4
The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.
Dependencies: AGD_OPE.1 Operational user guidance

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
FPT_STM.1.1
The TSF shall be able to provide reliable time stamps.
Dependencies: No dependencies

FPT_TDC.1 Inter-TSF basic TSF data consistency
Hierarchical to: No other components.
FPT_TDC.1.1
The TSF shall provide the capability to consistently interpret [*file information security attributes*] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2
The TSF shall use [*access controls and integrity checks*] when interpreting the TSF data from another trusted IT product.
Dependencies: No dependencies

6.2.6 Class FRU: Resource Utilization

FRU_RSA.1 Maximum quotas
Hierarchical to: No other components.
FRU_RSA.1.1
The TSF shall enforce maximum quotas of the following resources: [*disk storage usage*] that [individual user, defined group of users] can use [simultaneously].
Dependencies: No dependencies

6.2.7 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

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 [the TSF, 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 [*synchronization between clusters*].

Dependencies: No dependencies

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2+ augmented with ALC_FLR.2. Table 11 summarizes the requirements.

Table 11 Assurance Requirements

Assurance Requirements	
Class 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
Class 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.2 Flaw Reporting Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 12 lists the security functions and their associated SFRs.

Table 12 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security based attribute control
	FDP_ETC.2	Export of user data with security attributes
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITC.2	Import of user data with security attributes
	FDP_ROL.1	Basic rollback
Identification and Authentication	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(a)	Management of security attributes
	FMT_MSA.1(b)	Management of security attributes
	FMT_MSA.3(a)	Static attribute initialisation
	FMT_MSA.3(b)	Static attributes initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions

TOE Security Function	SFR ID	Description
	FMT_SMR.1	Security roles
Protection of TOE Security Functions	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RCV.3	Automated recovery without undue loss
	FPT_STM.1	Reliable time stamps
	FPT_TDC.1	Inter-TSF basic TSF data consistency
Resource Utilization	FRU_RSA.1	Maximum quotas
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel

7.1.1 Security Audit

The TOE maintains many logging daemons which are used by administrators and Isilon support to monitor and troubleshoot the system. Each log contains a record of the start-up and shutdown of the log. The syslog is a configurable system log platform that allows multiple log files capturing logging data based on selectors and actions specified in the syslogd.conf file. Table 13 contains a list of security relevant logs configured by default for the syslog.

Table 13 Audit Records

Audit Name	Description
SMB access log	Network and object events for SMB file share
NFS access log	User connections and disconnections to NFS file share
Active Directory (AD) log	Logs successful and unsuccessful AD authentication attempts
Apache log	Administrator connections and disconnections to HTTPS
SmartConnect log	IP address assignments and reassignments
Snapshot log	Log of all snapshot events
Error and Warning messages	File and directory repairs, disk and node failure, and integrity scans and any associated errors.
Jobs log	Log of administrator run jobs, including integrity jobs
SyncIQ log	Logs synchronizations
NDMP log	Logs backups and restores over NDMP
SMB log	File share events with SMB protocol
NFS log	File exports events with NFS protocol
iSCSI log	File events with iSCSI protocol
Anti-virus log	Logs anti-virus scans, quarantines, and file rebuilds

The logging level for all logs can be set to error, warning, info, verbose, debug, or trace. Each level is successively more detailed, with error being the default setting. The TOE audit records contain the following information:

- Timestamp of event
- Event description, which includes success or failure if applicable
- Node name or IP address

The username of the user connecting or disconnecting from the TOE is recorded in the connection and disconnection records.

Only authorized administrators can view or access the logs. Individual logs can be viewed through the CLI or an administrator can perform an *isi_gather* command to view information from the logs. The TOE maintains additional records of events related to health and performance of a cluster. These additional events may be viewed through the Web Administration GUI Events tab. When a log reaches its administrator defined capacity an email or Simple Network Management Protocol (SNMP) trap can be sent, the log is branched and compressed and a new log is started.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_STG.1, FAU_STG.4.

7.1.2 User Data Protection

There are two main security function policies for the TOE. The first is the Data Access SFP, which uses Windows DACLs and UNIX permissions to create authorization data for files stored on the TOE. The TOE supports a mixed-access environment using SMB or NFS protocols by default. The TOE uses a Samba-based suite to enable Windows and UNIX interoperability. All files can use DACLs and UNIX permissions to determine the access rights of a user. Access tokens are generated for users when they authenticate to the TOE. These access tokens are compared to a file's authorization data to determine if the user has authorization to access the file. Windows users are assigned a security identifier (SID). The SID is a unique identifier for each user. UNIX users are assigned user identifier (UID) and at least one group identifier (GID) each of which can have permissions assigned to them. The tokens are comprised of all UIDs, GIDs, and SIDs associated with a user.

Files and directories are assigned permissions by the file owner, who is the creator of the file. The default setting for all files is read-only permissions for anyone who is not the owner. The TOE stores authorization data in the form of DACLs for shares, exports, and files. The rwx permissions are derived from these DACLs. The TOE uses default policies to translate the UNIX permissions to a Windows ACL to ensure proper access to file. An authorized administrator can configure the permission translation policies using the Web Administration interface. The possible options are UNIX only, Balanced, or Windows only. Balanced is the default setting and performs the operations as described above. UNIX or Windows only will allow only that type of permissions for the TOE.

The second policy is the data transfer policy, which states that files and directories are monitored by FlexProtect for integrity errors using the Reed Solomon algorithm and protected from unauthorized access through the access controls discussed in the Data Access SFP. When integrity errors are detected files or directories are rebuilt. Files, access controls, and error correction information are distributed across the cluster according to the set protection level, ensuring that all data remains intact and accessible even in the event of multiple disk or a node failures. The protection levels are defined in Table 14. FlexProtect will restripe data to different disks or nodes in the event of disk degradation. Data travels through a dedicated backend line to protect it from modification while it is being transferred between nodes in the restriping process. The SmartConnect feature of the TOE allows an authorized administrator to define zones that correspond to IP address pools and policies for these zones. The TOE can allocate user connections based on a simple round robin policy, CPU utilization, connection counting, or network throughput. If a TOE interface fails SmartConnect will automatically move the user connections from that interface to a different interface according to the configured policy.

The TOE can be configured to synchronize data between clusters. SyncIQ is responsible for this process and maintains all file security attributes in a copy or synchronization process. As part of the synchronization process a snapshot of the data in the source and possibly target directory is taken. These snapshots can also be used for file restoration. SnapshotIQ creates snapshots of data and state information in a directory for safekeeping. The snapshot is stored in the TOE and can be used to rollback the data to that snapshot. If a file is accidentally deleted the file can be found in the stored snapshot and restored. SnapshotIQ is used to perform the snapshot function and it can be used stand-alone or in conjunction with SyncIQ. When synchronizing or copying data between clusters a dedicated line will be used between the TOE and the additional cluster.
TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_ETC.2, FDP_IFC.1, FDP_IFF.1, FDP_ITC.2, FDP_ROL.1.

7.1.3 Identification and Authentication

The TOE requires users and administrators to authenticate with the TOE before all actions except those that are done through the front panel. There is no authentication that takes place through the front panel. The TOE environment ensures that the front panel cannot be accessed by unauthorized personnel. The following functions are available from the front panel:

- Attach – Allows a user to add or format a new hard disk
- Status – Allows for viewing of the following information
    - Alerts
    - Clusters details, capacity, and throughput
    - Node details, capacity, throughput, disk read/write access, and CPU throttling
    - Drive status
    - Hardware statistics – Battery voltage, CPU operations, and CPU speed limit
- Update – Allows user to update software from version residing on the file system
- Service – Allows user to change the following:
    - Throttle/Unthrottle CPU speed
    - Set node to Read-Only access
    - Set node to Read-Write access
    - Turn UnitLED on or off
- Shutdown the node
- Join – Only available on an unconfigured node. Allows node to join cluster.

Multiple authentication methods are supported by the TOE that differ based on the user's operating system. Windows users can use local authentication or Active Directory service. File provider credentials are stored in the /etc/passwd file of the OneFS operating system. Local users can be created using the web GUI and are stored in a local database. Permissions are enforced by the application software for all users. Only the local-user and domain modes are enabled in the evaluated configuration. Windows users are typically assigned a security identifier (SID) which uniquely identifies each user. An access token is created with this SID and any other UIDs, GIDs, or SIDs associated with this user are added to the token. UNIX users can use local authentication, LDAP, or NIS and are typically assigned user identifiers (UID). An access token is created using the same process described above. File provider authentication is used for identities associated with running and administering the cluster. The root and admin role can access the TOE through the CLI commands or Web Administration interfaces. The HTTP service redirects traffic to the Web Administration interface where HTTPS is used to protect the interface and a user name and password is required. Users access the TOE through an external Gigabit Ethernet connection supporting standard network communication protocols including: NFS and SMB.

The TOE also provides CHAP to conduct one-way authentication for iSCSI connections. An authorized administrator must configure CHAP authentication for each iSCSI target.
TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UAU.5, FIA_UID.2.

7.1.4 Security Management

The TOE maintains three roles: root, admin, and user. Both the root and the admin roles may perform management tasks through the Web Administration GUI. Although the admin role may log in to the CLI, most of this interface's functionality is available only to the root user. The root role is the default owner of all files and directories stored in the TOE and is the only role that can install the TOE and perform initial configuration. Users access the TOE through client systems and are not allowed access to the Web Administration GUI or any management functions other than setting permissions for files that they own. Table 10 explains the management functions for the TOE and which roles are permitted to perform those functions.

The root and admin roles are both capable of creating user accounts and assigning them to an ACL or UNIX group, through the CLI commands or Web Administration interface. Once a user has been created the accounts and permissions are managed from the Web Administration or CLI commands interface. Creation of user accounts can be delegated to Windows Active Directory (AD), LDAP servers, or a NIS domain server. When creation of user accounts is delegated to an external server the user is still assigned a UID or SID. This UID or SID can be accessed by the TOE and assigned permissions in the same way as a local user is assigned permissions.

Default permission levels are set for all directories at their creation and all users are assigned the default permissions unless modified by an authorized administrator. File integrity data is protected at the same level as the file itself. This data can only be changed or removed by an authorized administrator. Protection levels are normally set at the cluster level by an authorized administrator. A separate protection level can be set at the file or directory level by the file or directory owner, if the data requires additional protection. At the directory and file level an owner can be any user with permission to create files. The root and admin roles maintain the ability to change protection levels and permissions for files with a user as the owner. Authentication modes for the cluster can also be configured. The acceptable levels are: local-user mode and external authentication mode. The external authentication mode will additionally specify AD, LDAP, or NIS.

Cluster access is also configurable. SMB and NFS are enabled by default. HTTP must be enabled by an authorized administrator. Lastly, administrators can use SmartQuotas to set disk storage quotas for users and groups. Disk usage quotas can also be set for directories within the file system. The quotas can be accounting quotas, which monitor but do not limit disk storage, or enforcement quotas, which monitor and limit disk storage. Each type of quota will send an alert when the quota is met. Enforcement quotas may then have a grace period where they will continue to allow writes for an administrator specified period, or they may immediately disallow writes when a quota is met.
TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3(a), FMT_MSA.3(b), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

The TOE has extensive protocols to ensure that failure of multiple disks or nodes do not cause data loss. Table 14 details the levels of protection that can be configured for a file, directory, or cluster. A protection level is set at the cluster level. This then becomes the default protection level that all files are assigned upon creation. If a file or directory requires additional protection it can manually be assigned a higher protection level. The file or directory would then be striped across additional drives or nodes depending on the level. The TOE does allow a protection level to be set that that the cluster is not currently capable of matching. If the level is set above what the cluster can match the TOE will continue to try to match the requested level until a match is possible. The protection level and the data integrity compose the file information security attributes that the data transfer SFP cover. FlexProtect automatically stripes data across the cluster to ensure the configured level of protection. The individual nodes within the cluster are connected through an InfiniBand dedicated back-end line. The back-end line is connected directly from node to node and there are no non-TOE connections to this line.

Table 14 TSF Protection Levels

Level	Failure without loss	Minimum Number of Nodes
N+1	1 drive or 1 node	3 nodes
N+2:1	2 drives or 1 node	3 nodes
N+2	2 drives or 2 nodes	5 nodes
N+3:1	3 drives or 1 node	3 nodes
N+3	3 drives or 3 nodes	7 nodes
N+4	4 drives or 4 nodes	9 nodes

In the event of a failure, FlexProtect is responsible for restriping and re-protecting the data. Smart failing a device puts the device in quarantine. This allows read-only access to the data on the device. While in quarantine the restriping and re-protection will take place. When the restriping is complete the drive or node can be removed from the cluster and replaced. Data is restriped to available space within the cluster, so a hot-space is not necessary. Once the data has been re-protected the cluster and all its data is again fully available.

The TOE is capable of automatically recovering from a disk or interface failure. If a node or node interface fails the TSF will follow the authorized administrator defined IP failover policy to move user connections from that node to another node. This SmartConnect feature maintains user connections even when an interface or node fails. A disk failure automatically triggers FlexProtect to restripe or rebuild data from the failed disk to available free space in the TOE. Once all data is moved to available free space within the TOE the drive is logically removed from the cluster and the cluster is no longer in a degraded state. An administrator can then confirm the FlexProtect operations success and hot-swap the drive. A node failure does not automatically trigger FlexProtect to perform a reprotection operation. A node can reboot and all data will have remained intact during the temporary failure. User data on the other nodes within the cluster will still remain available. If an administrator determines a node must be removed from the cluster a smartfail process similar to that of a failed disk is performed. All data is migrated to other nodes within the cluster and the failed node is not removed until this process is complete.

Backups and synchronization of data between clusters is supported for the TOE. SyncIQ is used to perform the backups and synchronization. Authorized administrator defined policies maintain data integrity during these transfers. The set user access controls are maintained during transfer and error correction information is transferred with the data to enable integrity checking. During synchronization, each packet is sent with a checksum and the checksum is verified at the destination directory. If the checksum is not correct the packet is resent. The SyncIQ policies allow an administrator to define how often backup and synchronization occurs, what the source and target directories are, and specific file criteria for what will be synchronized. The NDMP protocol is used for data backup. A dedicated line between the clusters is also used for all of these operations.

The TOE maintains a secure state when a disk or node failure occurs. Data is stored on separate disks and nodes ensure that the data remains available even when a disk or node fails. When a disk or node failure is suspected the TOE smartfails the device, placing it in quarantine. In quarantine a device is accessed only as a last resort and only for read-only operations. Access is still verified by the TOE before attempting to access any data.

The sysclock provides a reliable timestamp for the TOE. The nodes perform network time protocol (NTP) peer operations to synchronize the node clocks with the sysclock.
TOE Security Functional Requirements Satisfied: FPT_FLS.1, FPT_ITT.1, FPT_RCV.3, FPT_STM.1, FPT_TDC.1.

7.1.6 Resource Utilization

The SmartQuotas module of the TOE allows authorized administrators to define disk storage utilization quotas for users and groups on the system. The module monitors storage limits and enforces the limits set by administrators. Automated email notifications can also be enabled to alert administrators to users exceeding quota. Table 15 defines the types of thresholds that can be defined for an enforcement quota.

Table 15 Enforcement Quota Types

Threshold Type	Description
Hard	A limit that cannot be exceeded. Operations will fail if over limit. Alert is logged and notification is sent.
Soft	A limit can be exceeded until a grace period has expired. Hard limit takes place after grace period. Alert is logged and notification sent.
Advisory	An informational limit that can be exceeded. Alert if logged and notification is sent.

TOE Security Functional Requirements Satisfied: FRU_RSA.1.

7.1.7 Trusted Path/Channels

The TOE environment provides a dedicated line between the TOE and other clusters for synchronization and backup operations. This dedicated line is connected to the TOE and another cluster directly with no other connections to the line, creating a trusted channel.

TOE Security Functional Requirements Satisfied: FTP_ITC.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.2 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 16 below provides a mapping of the objects to the threats they counter.

Table 16 Threats:Objectives Mapping

Threats	Objectives	Rationale
T.ACCOUNTABILITY An unidentified threat could result in authorized users of the TOE not being held accountable for their actions within the TOE.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS counters this threat by requiring the TOE to identify and authenticate all authorized users prior to allowing any TOE access or any TOE mediated access on behalf of those users.
	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	O.AUDIT_GENERATION counters this threat by providing the authorized security administrator with the capability of configuring the audit mechanism to record the actions of a specific user. Additionally, the security administrator's ID is recorded when any security relevant change is made to the TOE.
	O.AUDIT_REVIEW The TOE will contain mechanisms to allow the authorized security administrator to view and sort the audit logs.	O.AUDIT_REVIEW counters this threat by allowing the authorized security administrator to review the audit trail based on the identity of the user.
T.AUDIT_COMPROMISE A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	O.AUDIT_STORAGE The TOE will contain mechanisms to provide secure storage and management of the audit log.	O.AUDIT_STORAGE counters this threat by requiring the TOE to securely store all audit data.
	O.AUDIT_REVIEW The TOE will contain mechanisms to allow the authorized security	O.AUDIT_REVIEW counters this threat by ensuring that the TOE will provide mechanisms to

Threats	Objectives	Rationale
	administrator to view and sort the audit logs.	review the audit logs. These requirements will ensure the data is in a suitable manner for the security administrator to interpret.
	O.AUDIT_MONITOR The TOE will provide the ability to monitor logs, alert administrators, and perform automated functions if logs exceed capacity.	O.AUDIT_MONITOR counters this threat by alerting authorized administrators if log capacity is exceed.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT counters this threat ensuring the integrity of audit data by protecting itself from unauthorized modifications and access.
	O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized security administrator in management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	O.MANAGE counters this threat by ensuring that the TOE will provide all the functions and facilities necessary to support the authorized security administrator in the management of the security of the audit logs, and restrict these functions and facilities from unauthorized use.
	O.TIMESTAMP The TOE will provide reliable time stamps.	O.TIMESTAMP counters this threat by ensuring that accurate timestamps are provided for all audit records, allowing the order of events to be preserved.
T.CRITICAL_FAILURE An unidentified threat agent could cause the TOE to experience a failure of a critical component that prevents users and administrators from being able to access TOE functionality.	O.FAIL_SECURE The TOE will provide mechanisms to allow for secure failure and recovery.	O.FAIL_SECURE counters this threat by ensuring that the TOE provides a mechanism to allow for secure failure and recovery.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS counters this threat by controlling access to the TOE and its resources. The Data Access policy constrains how and when authorized users can access the TOE, and mandates the type of authentication mechanisms, thereby mitigating the possibility of a user attempting to login and masquerade as an authorized user.
	O.AUTHENTICATE	O.AUTHENTICATE counters this

Threats	Objectives	Rationale
	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	threat by ensuring that the TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
T.TAMPERING A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment and gain unauthorized access to TOE functionality.	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	O.AUDIT_GENERATION counters this threat by ensuring that security relevant events that may indicate attempts to tamper with the TOE are recorded.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification.
	O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized security administrator in management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	O.MANAGE supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.
T.UNAUTH A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.AUTHENTICATE mitigates this threat by ensuring that users are identified and authenticated prior to gaining access to TOE security data.
	O.MEDIATE The TOE must protect user data in accordance with its security policy.	O.MEDIATE counters this threat by ensuring that all access to user data is subject to mediation. The TSF will ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The TOE restricts the ability to modify the security attributes associated with access control rules to the security administrator. This feature ensures that no other user can modify the data access policy to bypass the intended TOE security policy.
T.UNAVAILABILITY The TOE may be overwhelmed by	O.QUOTAS The TOE will provide the ability	O.QUOTAS counters this threat by ensuring that the TOE limits

Threats	Objectives	Rationale
legitimate user tasks, preventing or delaying any TOE functionality from being accessed.	to define quotas for usage of TOE resources, and prevent further allocation of resources once the quotas are reached.	the amount of disk storage space that can be used by a user or a group.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no organizational security policies defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 17 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 17 Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware.	OE.PLATFORM The hardware on which the TOE operates must support all required TOE functions.	OE.PLATFORM ensures that the hardware platform supports the OS and TOE functions.
	OE.TRUST_IT Each operational entity the TOE relies on for security functions will be installed, configured, managed and maintained in a manner appropriate to the IT entity, and consistent with the security policy of the TOE and the relationship between them.	OE.TRUST_IT ensures that all security entities that the TOE relies on are installed, configured and managed appropriately.
	NOE.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.	NOE.MANAGE fulfills this assumption by ensuring that competent non-hostile administrators who are trained and follow guidance will be provided for the TOE.
A.LOCATE The TOE is located within a controlled access facility.	NOE.PHYSICAL Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.	NOE.PHYSICAL satisfies this assumption by ensuring physical security is provided within the TOE environment to provide appropriate protection to the network resources.
A.PROTECT The TOE software will be protected from unauthorized	OE.NO_BYPASS The operational environment shall ensure the TOE security	OE.NO_BYPASS satisfies this assumption. The TOE environment ensures that security

Assumptions	Objectives	Rationale
modification.	mechanisms cannot by bypassed in order to gain access to the TOE resources.	mechanisms cannot be bypassed.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT satisfies this assumption. The TOE environment provides protection from external interference or tampering.
	OE.SECURE_COMMS The operational environment will provide a secure line of communications between external entities and the TOE.	OE.SECURE_COMMS satisfies this assumption. The TOE environment protects communications between itself and external entities from external interference or tampering.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	NOE.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.	NOE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

No extended SFRs have been defined for this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE security assurance requirements defined for this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 18 below shows a mapping of the objectives and the SFRs that support them.

Table 18 Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT_STORAGE The TOE will contain mechanisms to provide secure storage and management of the audit log.	FAU_STG.1 Protected audit trail storage	FAU_STG.1 supports this objective by requiring that only the authorized security administrator may delete the audit records ensuring that no malicious users may compromise the data stored within the audit records.
O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	FDP_ACC.1 Subset access control	FDP_ACC.1 supports this objective by requiring the TSF to enforce the data access policy with ACLs and permissions.
	FDP_ACF.1 Security based attribute control	FDP_ACF.1 supports this objective by requiring the TSF to follow the Data Access SFP for access to TOE data.
	FIA_UID.1 Timing of identification	FIA_UID.1 supports this objective by requiring the TSF to identify each user before allowing TSF action except those listed.
O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	FAU_GEN.1 Audit Data Generation	FAU_GEN.1 supports this objective by defining the set of events that the TOE must be capable of recording. This requirement ensures that the security administrator has the ability to audit any security relevant events that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event.
O.AUDIT_REVIEW The TOE will contain mechanisms to allow the authorized security administrator to view and sort the audit logs.	FAU_SAR.1 Audit review	FAU_SAR.1 supports this objective by requiring that only the authorized security administrator has the capability to read the audit records which must be presented in a manner suitable for the security administrator to interpret them.
O.AUDIT_MONITOR The TOE will provide the ability to monitor logs, alert administrators, and perform automated functions if logs exceed capacity.	FAU_STG.4 Prevention of audit data loss	FAU_STG.4 supports this objective by requiring that audit records be rotated and email alerts sent when audit trail exceeds administrator defined capacity.
O.AUTHENTICATE	FIA_UAU.1	FIA_UAU.1 supports this

Objective	Requirements Addressing the Objective	Rationale
The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	Timing of authentication	objective by requiring the TOE to successfully authenticate a user before access to TOE functions except those listed.
	FIA_UAU.5 Multiple authentication mechanisms	FIA_UAU.5 supports this objective by providing external authentication methods.
	FIA_UID.1 Timing of identification	FIA_UID.1 supports this objective by requiring the TSF to identify each user before allowing TSF action except those listed.
	FMT_SMR.1 Security roles	FMT_SMR.1 supports this objective by describing the roles users are associated with when they authenticate.
O.FAIL_SECURE The TOE will provide mechanisms to allow for secure failure and recovery.	FDP_IFC.1 Subset information flow control	FDP_IFC.1 supports this objective by defining operations to protect data as it flows within the TOE.
	FDP_IFF.1 Simple security attributes	FDP_IFF.1 supports this objective by requiring the TSF to use the Data Transfer SFP to meet defined data protection levels.
	FPT_FLS.1 Failure with preservation of secure state	FPT_FLS.1 supports this objective by ensuring that the TOE preserves a secure state when a drive or node fails.
	FPT_RCV.3 Automated recovery without undue loss	FPT_RCV.3 supports this objective by ensuring the TOE provides an automated procedure for recovery from drive or node failure.
O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1 supports this objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only users with appropriate permissions may manage the security behaviour of the TOE.
	FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 supports this objective by describing the TSF management functions for managing security behavior, security attributes and TSF data.
	FTP_ITC.1 Inter-TSF trusted channel	FTP_ITC.1 supports this objective by requiring the TSF to provide a

Objective	Requirements Addressing the Objective	Rationale
		distinct line between clusters when performing synchronization.
O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized security administrator in management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FAU_GEN.1 Audit Data Generation	FAU_GEN.1 supports this objective by providing authorized administrators access to the audit data necessary to manage the TOE.
	FAU_SAR.1 Audit review	FAU_SAR.1 supports this objective by providing an authorized administrator with a readable audit record.
	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1 supports this objective by ensuring that the TOE authenticates users prior to allowing access to administrative functions to ensure that only those trusted users may manage the security behaviour of the TOE.
	FMT_MSA.1(a) Management of security attributes	FMT_MSA.1(a) supports this objective by defining the management functions involved with data access.
	FMT_MSA.1(b) Management of security attributes	FMT_MSA.1(b) supports this objective by defining the management functions involved with data transfer from node to node.
	FMT_MSA.3(a) Static attribute initialisation	FMT_MSA.3(a) supports this objective by requiring a restrictive default for the data access SFP.
	FMT_MSA.3(b) Static attributes initialisation	FMT_MSA.3(b) supports this objective by requiring a permissive default for the data transfer SFP.
	FMT_MTD.1 Management of TSF data	FMT_MTD.1 supports this objective by defining the management operations possible on the TSF data.
	FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 supports this objective by describing the management functions the TSF provides.
O.MEDIATE The TOE must protect user data in accordance with its security policy.	FDP_ACC.1 Subset access control	FDP_ACC.1 supports this objective by defining the Access Control policy that will be enforced on a list of subjects

Objective	Requirements Addressing the Objective	Rationale
		acting on the behalf of users attempting to gain access to a list of named objects. All the operations between subject and object covered are defined by the TOE's policy.
	FDP_ACF.1 Security based attribute control	FDP_ACF.1 supports this objective by requiring the TSF to use the Data Access SFP for access to TOE data.
	FDP_ETC.2 Export of user data with security attributes	FDP_ETC.2 supports this objective by requiring that the TOE's access control policy be enforced when exporting data.
	FDP_IFC.1 Subset information flow control	FDP_IFC.1 supports this objective by defining an information flow policy for the TSF.
	FDP_IFF.1 Simple security attributes	FDP_IFF.1 supports this objective by requiring the TSF to use the Data Transfer SFP.
	FDP_ITC.2 Import of user data with security attributes	FDP_ITC.2 supports this objective by requiring that the TOE's access control policy be enforced when importing data.
	FDP_ROL.1 Basic rollback	FDP_ROL.1 supports this objective by requiring the TOE to be capable of performing rollback to the last performed snapshot.
	FPT_ITT.1 Basic internal TSF data transfer protection	FDP_ITT.1 supports this objective by ensuring that the TOE protects TSF data from modification when transmitted within the TOE.
	FPT_RCV.3 Automated recovery without undue loss	FPT_RCV.3 supports this objective by requiring that the TOE will recover from disk or node failure without loss of user data.
	FPT_TDC.1 Inter-TSF basic TSF data consistency	FPT_TDC.1 supports this objective by ensuring the TOE protects TSF data during backup to a trusted IT product.
O.TIMESTAMP The TOE will provide reliable time stamps.	FPT_STM.1 Reliable time stamps	FPT_SMT.1 supports this objective by requiring the TOE to provide a reliable timestamp.
O.QUOTAS	FRU_RSA.1	FRU_RSA.1 supports this

Objective	Requirements Addressing the Objective	Rationale
The TOE will provide the ability to define quotas for usage of TOE resources, and prevent further allocation of resources once the quotas are reached.	Maximum quotas	objective by requiring the TOE to support disk storage quotas on users and groups.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 19 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 19 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_ETC.2	FDP_IFC.1	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FMT_MSA.3(b)	✓	
	FDP_IFC.1	✓	
FDP_ITC.2	FDP_IFC.1	✓	
	FTP_ITC.1	✓	
	FPT_TDC.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ROL.1	FDP_IFC.1	✓	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.5	No dependencies	n/a	
FIA_UID.1	No dependencies	n/a	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(a)	FDP_ACC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(b)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_IFC.1	✓	
FMT_MSA.3(a)	FMT_MSA.1(a)	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(b)	FMT_MSA.1(b)	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	n/a	
FMT_SMR.1	FIA_UID.1	✓	
FPT_FLS.1	No dependencies	n/a	
FPT_ITT.1	No dependencies	n/a	
FPT_RCV.3	AGD_OPE.1	✓	
FPT_STM.1	No dependencies	n/a	
FPT_TDC.1	No dependencies	n/a	
FRU_RSA.1	No dependencies	n/a	
FTP_ITC.1	No dependencies	n/a	

9 Acronyms and Terms

This section and Table 20 define the acronyms and terms used throughout this document.

9.1 Acronyms

Table 20 Acronyms

Acronym	Definition
ACE	Access Control Entity
ACL	Access Control List
CC	Common Criteria
CHAP	Challenge-Handshake Authentication Protocol
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
DACL	Discretionary Access Control List
DAR	Direct Access Restore
DMA	Data Management Application
EAL	Evaluation Assurance Level
GID	Group Identifier
GigE	Gigabit Ethernet
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NDMP	Network Data Management Protocol
NFS	Network File System
NIS	Network Information Service
NTP	Network Time Protocol
NVRAM	Non-volatile Read Access Memory
OS	Operating System
PP	Protection Profile
RAID	Redundant Array of Independent Disks

Acronym	Definition
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SFTP	SSH File Transfer Protocol
SID	Security Identifier
SNMP	Simple Network Management Protocol
SMB	Server Message Block
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
UID	User Identifier

9.2 Terms

Table 21 Terms

Term	Definition
rwx permissions	Unix permission flags of read, write, and execute

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com