EMC Corporation
Isilon OneFS v7.2.0.4

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.0

Prepared for:	Prepared by:
EMC Corporation 505 1st Avenue South Seattle, WA 98104 United States of America	**Corsec Security, Inc.** 13921 Park Center Road, Suite 460 Herndon, VA 20171 United States of America
Phone: +1 800 782 4362 Email: info@emc.com http://www.emc.com	Phone: +1 703 267 6050 Email: info@corsec.com http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

The subject of this evaluation is EMC Isilon OneFS v7.2.0.4, hereafter referred to as the TOE[1] throughout this document. The software/hardware TOE includes the OneFS Operating System (OS) that provides a distributed file system for storage and management of unstructured and file-based data on the Isilon clustered storage system and the hardware platforms that are running the OS.

1.1 Document Organization

This ST is divided into nine sections, as follows:

- (Section 0) – 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 functionality 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 Security 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

The ST and TOE references are in Table 1 below.

Table 1 ST and TOE References

ST Title	EMC Corporation Isilon OneFS v7.2.0.4 Security Target
ST Version	Version 1.0
ST Author	Corsec Security, Inc.
ST Publication Date	12/3/2015
TOE Reference	EMC Isilon OneFS v7.2.0.4 B7_2_0_196(RELEASE) Patch-164118

1.3 Product Overview

EMC Isilon takes a scale-out approach to storage by creating a cluster of nodes that runs a distributed file system. OneFS combines the three layers of storage architecture—file system, volume manager, and data protection – into a scale-out NAS[2] cluster. Each node adds resources to the cluster. Because each node

[1] TOE – Target of Evaluation

[2] NAS – Network-Attached Storage

contains globally coherent RAM[3], as a cluster becomes larger, it becomes faster. Meanwhile, the file system expands dynamically and redistributes content, which eliminates the work of partitioning disks and creating volumes. Segmenting and distributing data —a process known as striping—not only protects data, but also enables a user connecting to any node to take advantage of the entire cluster's performance.

OneFS uses distributed software to scale data across commodity hardware. Nodes work as peers to spread data across the cluster. No master device controls the cluster; no slaves invoke dependencies. Instead, each node helps control data requests, boosts performance, and expands the cluster's capacity.

An Isilon cluster consists of three or more hardware nodes, up to 144. Each node runs the Isilon OneFS operating system, the distributed file-system software that unites the nodes into a cluster. A cluster's storage capacity ranges from a minimum of 18 TB[4] to a maximum of 15.5 PB[5]. Isilon offers the following four classes of node hardware:

- S-Series – IOPS[6]-intensive applications
- X-Series – High-concurrency and throughput-driven workflows
- NL-Series – Near-primary accessibility, with near-tape value
- HD-Series – High-density storage.

1.3.1 Data Layout

OneFS evenly distributes data among a cluster's nodes with layout algorithms that maximize storage efficiency and performance. The system continuously reallocates data to conserve space. OneFS breaks data down into smaller sections called blocks, and then the system places the blocks in a stripe unit. By referencing either file data or erasure codes, a stripe unit helps safeguard a file from a hardware failure. The size of a stripe unit depends on the file size, the number of nodes, and the protection setting. After OneFS divides the data into stripe units, OneFS allocates, or stripes, the stripe units across nodes in the cluster.

1.3.2 Striping

OneFS segments files into units of data and then distributes the units across nodes in a cluster. Striping protects the user's data and improves cluster performance. OneFS distributes erasure codes that protect the file as the system allocates stripe units to nodes over the internal network. The erasure codes encode the file's data in a distributed set of symbols, adding space-efficient redundancy. With only a part of the symbol set, OneFS can recover the original file data. Taken together, the data and its redundancy form a protection group for a region of file data.

1.3.3 Data Protection

An Isilon cluster is designed to serve data even when components fail. By default, OneFS protects data with erasure codes, enabling you to retrieve files when a node or disk fails. As an alternative to erasure codes, the user can protect data with two to eight mirrors. When you create a cluster with five or more nodes, erasure codes deliver as much as 80 percent efficiency. On larger clusters, erasure codes provide as much as four levels of redundancy.

OneFS supports N+M erasure code levels of N+1, N+2, N+3, and N+4. In the N+M data model, N represents the number of nodes, and M represents the number of simultaneous failures of nodes or drives that the cluster can handle without losing data. To protect drives and nodes separately, OneFS also supports N+M:B. In the N+M:B notation, M is the number of disk failures, and B is the number of node failures. The default protection level for clusters larger than 18 TB is N+2:1. The default for clusters smaller than 18 TB is N+1. The quorum rule dictates the number of nodes required to support a protection level. For example, N+3 requires at least seven nodes so the user can maintain a quorum if three nodes fail. The user can, however,

[3] RAM – Read-Access Memory

[4] TB – Terabyte

[5] PB – Petabyte

[6] IOPS – Input/Output Operations Per Second

set a protection level that is higher than the cluster can support. In a four-node cluster, for example, you can set the protection level at 5x. OneFS protects the data at 4x until a fifth node is added, after which OneFS automatically reprotects the data at 5x.

1.3.4 Data Mirroring

The user can protect on-disk data with mirroring, which copies data to multiple locations. OneFS supports two to eight mirrors. You can use mirroring instead of erasure codes, or you can combine erasure codes with mirroring. During a write operation, OneFS divides data into redundant protection groups. For files protected by erasure codes, a protection group consists of data blocks and their erasure codes. For mirrored files, a protection group contains all the mirrors of a set of blocks. OneFS can switch the type of protection group as it writes a file to disk. By changing the protection group dynamically, OneFS can continue writing data despite a node failure that prevents the cluster from applying erasure codes. After the node is restored, OneFS automatically converts the mirrored protection groups to erasure codes.

1.3.5 The File System Journal

A journal, which records file-system changes in a battery-backed NVRAM[7] card, recovers the file system after failures, such as a power loss. When a node restarts, the journal replays file transactions to restore the file system.

1.3.6 Virtual Hot Spare

When a drive fails, OneFS uses space reserved in a subpool instead of a hot spare drive. The reserved space is known as a virtual hot spare. In contrast to a spare drive, a virtual hot spare automatically resolves drive failures and continues writing data. If a drive fails, OneFS migrates data to the virtual hot spare to reprotect it.

1.3.7 FlexProtect

OneFS uses the FlexProtect proprietary system to detect and repair files and directories that are in a degraded state due to node or drive failures. OneFS protects data in the cluster based on the configured protection policy. OneFS rebuilds failed disks, uses free storage space across the entire cluster to further prevent data loss, monitors data, and migrates data off of at-risk components. OneFS distributes all data and error-correction information across the cluster and ensures that all data remains intact and accessible even in the event of simultaneous component failures. Under normal operating conditions, all data on the cluster is protected against one or more failures of a node or drive. However, if a node or drive fails, the cluster protection status is considered to be in a degraded state until the data is protected by OneFS again. OneFS reprotects data by rebuilding data in the free space of the cluster. While the protection status is in a degraded state, data is more vulnerable to data loss. Because data is rebuilt in the free space of the cluster, the cluster does not require a dedicated hot-spare node or drive in order to recover from a component failure. Because a certain amount of free space is required to rebuild data, it is recommended that you reserve adequate free space through the virtual hot spare feature. As you add more nodes, the cluster gains more CPU[8], memory, and disks to use during recovery operations. As a cluster grows larger, data restriping operations become faster.

1.3.8 Smartfail

OneFS protects data stored on failing nodes or drives through a process called smartfailing. During the smartfail process, OneFS places a device into quarantine. Data stored on quarantined devices is read only. While a device is quarantined, OneFS reprotects the data on the device by distributing the data to other devices. After all data migration is complete, OneFS logically removes the device from the cluster, the cluster logically changes its width to the new configuration, and the node or drive can be physically replaced. OneFS smartfails devices only as a last resort.

[7] NVRAM – Non-Volatile Random-Access Memory

[8] CPU – Central Processing Unit

1.3.9 Identity Management and Access Control

OneFS works with multiple identity management systems to authenticate users and control access to files. In addition, OneFS features access zones that allow users from different directory services to access different resources based on their IP[9] address. Role-based access control, meanwhile, segments administrative access by role.

OneFS authenticates users with the following identity management systems:

- Microsoft Active Directory (AD)
- Lightweight Directory Access Protocol (LDAP)
- Kerberos services
- Network Information Service (NIS) l for local users and local groups
- A file provider for accounts in */etc/spwd.db* and */etc/group* files. With the file provider, you can add an authoritative third-party source of user and group information.

You can manage users with different identity management systems; OneFS maps the accounts so that Windows and UNIX identities can coexist. A Windows user account managed in Active Directory, for example, is mapped to a corresponding UNIX account in NIS or LDAP. To control access, an Isilon cluster works with both the Access Control Lists (ACLs) of Windows systems and the POSIX[10] mode bits of UNIX systems. When OneFS must transform a file's permissions from ACLs to mode bits or from mode bits to ACLs, OneFS merges the permissions to maintain consistent security settings. OneFS presents protocol-specific views of permissions so that NFS[11] exports display mode bits and SMB[12] shares show ACLs. You can, however, manage not only mode bits but also ACLs with standard UNIX tools, such as the chmod and chown commands. In addition, ACL policies enable you to configure how OneFS manages permissions for networks that mix Windows and UNIX systems.

1.3.10 Access Zones

OneFS includes an access zones feature. Access zones allow users from different authentication providers, such as two untrusted Active Directory domains, to access different OneFS resources based on an incoming IP address. An access zone can contain multiple authentication providers and SMB namespaces.

1.3.11 RBAC[13] for administration

OneFS includes RBAC for administration. In place of a root or administrator account, RBAC lets you manage administrative access by role. A role limits privileges to an area of administration. For example, you can create separate administrator roles for security, auditing, storage, and backup.

1.3.12 Data-Access Protocols

With the OneFS operating system, the user can access data with multiple file-sharing and transfer protocols. As a result, Microsoft Windows, UNIX, Linux, and Mac OS X clients can share the same directories and files. OneFS supports the following protocols:

- SMB – The SMB protocol enables Windows users to access the cluster. OneFS works with SMB 1, SMB 2, and SMB 2.1, as well as SMB 3.0 for Multichannel only. With SMB 2.1, OneFS supports client opportunity locks (also referred to as oplocks) and large (1 MB[14]) MTU[15] sizes. The default file share is */ifs*.

[9] IP – Internet Protocol
[10] POSIX – Portable Operating System Interface
[11] NFS – Network File System
[12] SMB – Server Message Block
[13] RBAC – Role-Based Access Control
[14] MB – Megabyte
[15] MTU – Maximum Transmission Unit

- NFS – The NFS protocol enables UNIX, Linux, and Mac OS X systems to remotely mount any subdirectory, including subdirectories created by Windows users. OneFS works with NFS versions 3 and 4. The default export is */ifs*.
- FTP[16] – FTP allows systems with an FTP client to connect to the cluster and exchange files.
- HTTP[17] – HTTP gives systems browser-based access to resources. OneFS includes limited support for WebDAV[18].

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 TOE includes the OneFS v7.2.0.4 operating system that provides distributed file system management software (including the licensable components listed in 1.4.1) running on a homogenous cluster made up of at least three S210, X410, NL400, or HD400 nodes. Authenticated administrators can manage the TOE through a set of CLI[19] commands, PAPI[20], or the Web Administration GUI[21]. The Web Administration GUI is accessed using HTTP and standard web browsers such as Chrome, Firefox, Internet Explorer, or Safari. The CLI interface is used for initial configuration and is accessed via a serial connection. PAPI is used to manage the TOE over HTTP connections to the REST[22]ful Platform API[23]. All of these 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 front bezel of the node hardware. Through this interface users may view status on the hardware and cluster.

Figure 1 shows the details of the deployment configuration of the TOE. Acronyms that appear in the figure but have not been previously defined are:

- HTTPS – Hypertext Transfer Protocol Secure
- SSH – Secure Shell
- TLS – Transport Layer Security

[16] FTP – File Transfer Protocol
[17] HTTP – Hypertext Transfer Protocol
[18] WebDAV – Web Distributed Authoring and Versioning
[19] CLI – Command Line Interface
[20] PAPI – Platform API
[21] GUI – Graphical User Interface
[22] REST – Representational State Transfer
[23] API – Application Programming Interface

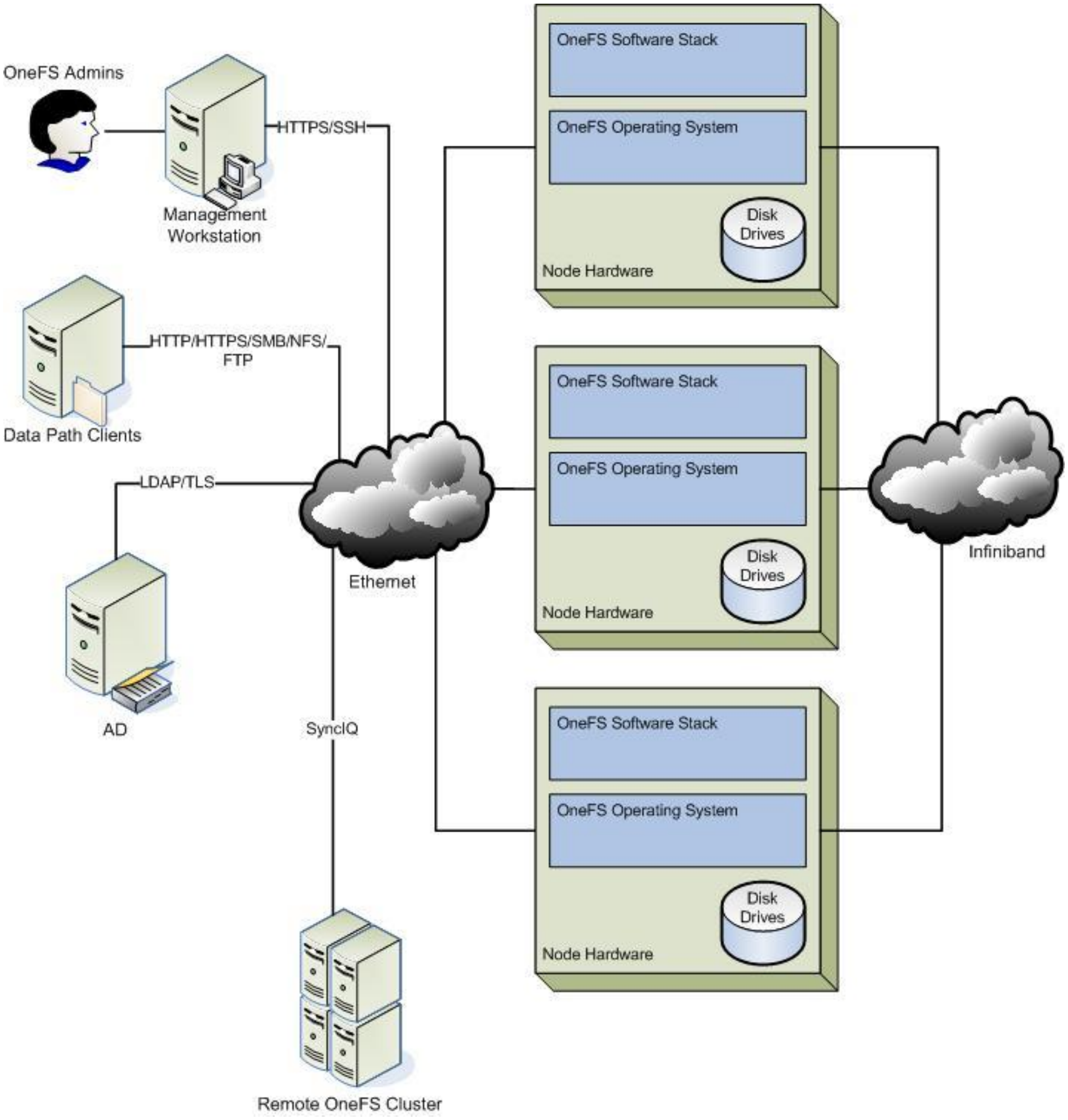

Figure 1 Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The TOE includes the following:

- Isilon OneFS v7.2.0.4 – the OS that provides distributed file system management including a Web Administration GUI, PAPI, and CLI for TOE management
- The following licensable features:
  - 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
- A homogenous three-node cluster made up of S210, X410, NL400, or HD400 nodes.

1.4.2 TOE Environment

The typical deployment is in a large enterprise or government data center. The TOE software is designed to run on Isilon's clustered storage system hardware. The Isilon Platform nodes are S Series, X Series, NL Series, and HD Series. The TOE boundary envelops the software and hardware components described in the TOE description (section 1.5) and does not include the network infrastructures.

The TOE requires 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[24] buffer per switch port, and jumbo frame support for front-end network, and Infiniband switches for the back-end network. The following were used in the evaluated configuration:
    - S210
        - Arista 7150S (front-end)
        - Flextronics F-X430044 (back-end)
    - X410
        - Arista 7150S (front-end)
        - Intel Qlogic 12000 (back-end)
    - NL400
        - Intel Qlogic 12200
    - HD400
        - Cisco Catalyst 3750, Brocade VDX6740 (front end)
        - Mellanox IS5023 (back-end)
- Client systems (the following were used in the evaluated configuration):
    - Microsoft Windows 8
    - Red Hat Enterprise Linux 5
- Client software:
    - An FTP client program
    - An SSH client program
    - An SMB 1, SMB 2, SMB 2.1 (SMB Multichannel only), or SMB 3 client program
    - An NFS 3 or NFS 4 client program
- A management workstation with the most recent Google Chrome browser
- AD domain controller (Windows Server 2008 R2)

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 InfiniBand 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 as 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 that are included in the evaluation.

[24] MB – Megabyte

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 includes 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
- A homogenous three-node cluster made up of S210, X410, NL400, or HD400 nodes

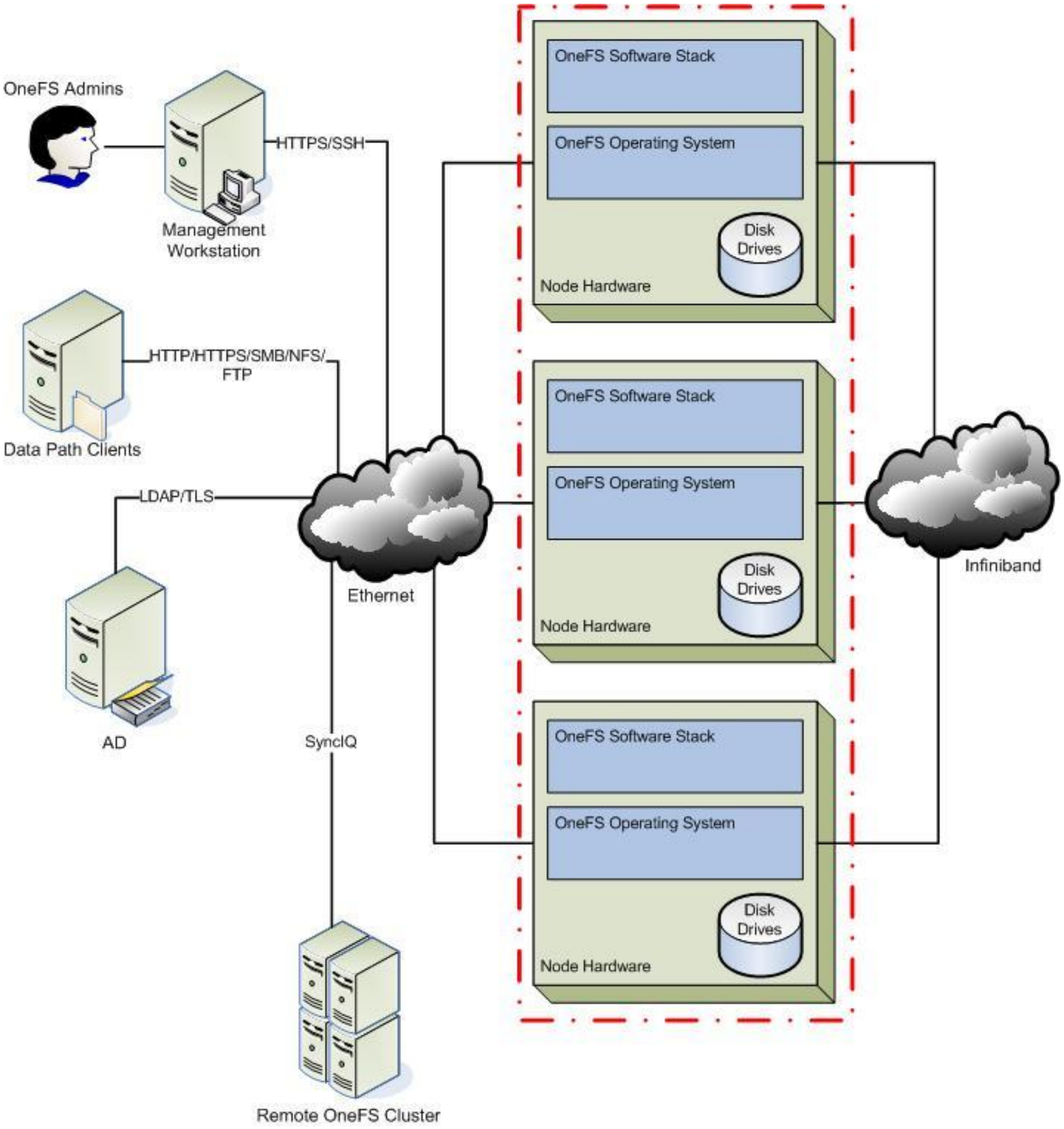

Figure 2 Physical TOE Boundary

1.5.1.1 Guidance Documentation

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

- Isilon OneFS 7.2.0 Web Administration Guide, 2015
- Isilon OneFS 7.2.0 CLI Administration Guide, 2015
- Isilon OneFS 7.2.0.0-7.2.0.4 Release Notes, 2015
- Isilon OneFS 7.2.0 Event Reference, 2015
- Isilon OneFS 7.2.0 OneFS API Reference, 2015
- Isilon OneFS 7.2.0 Security Configuration Guide, 2015
- Isilon OneFS 7.2.0 OneFS Migration Tools Guide, 2015
- Isilon OneFS 7.2.0 Supportability & Compatibility Guide, 2015
- Isilon Site Preparation and Planning Guide, 2015
- Isilon S210 Installation Guide, 2015
- Isilon X410 Installation Guide, 2015
- Isilon HD400 Installation Guide, 2015
- Isilon NL400 Installation Guide, 2015

1.5.1.2 Logical Scope

The logical boundary of the TOE will be broken down into the following functional 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 function classes described below.

1.5.1.3 Security Audit

The TOE generates many different types of logs. PAPI generated audit logs include configuration changes made through Web Administration GUI and CLI, SMB protocol events, and administrator logins. All other audit logs are produced by the syslog. The audit data is stored on the nodes in the cluster. Access to the audit data is restricted to the root role and authorised 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.

1.5.1.4 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 authorised administrator or owner can change the file permissions. The TOE can translate UNIX permissions into ACLs and vice versa. Additionally the TOE maintains and monitors 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 TOE monitors files and directories for integrity errors based on computed file checksums and disk or node failures. 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 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 to a separate cluster.

1.5.1.5 Identification and Authentication

Identification and Authentication can be performed locally, through the file provider (*/etc/passwd*) database, or using external methods such as: AD, LDAP, or NIS. Users access the TOE through one of the following file-share protocols:

- NFS – UNIX file export protocol that is enabled by default and configurable by an administrator through the Web Administration GUI, PAPI, or CLI interface.
- SMB – Windows file share protocol that is enabled by default and configurable by an administrator through PAPI or the Web Administration GUI.

- FTP – A network protocol that is enabled by default and configurable by an administrator through the Web Administration GUI or CLI interface.
- HTTP – The Web Administration GUI for cluster administration. HTTP services in the TOE are managed collectively through the File Sharing > HTTP page on the Web Administration GUI.

The TOE provides the external front panel interface on the node hardware that enables users to view status information about the TOE. This interface is protected by the TOE environment from unauthorised 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.

1.5.1.6 Security Management

There are three interfaces for security management, the Web Administration GUI, PAPI, and the CLI interface. The TOE maintains a root role, file owners, customized roles, and three built-in administrator roles provided by the TOE. The administrative roles include the AuditAdmin, SecurityAdmin, and SystemAdmin roles. The AuditAdmin provides read-only access to view configurations and settings. The SecurityAdmin provides the ability to administer security configuration on the cluster including manage authentication providers, local users and groups, and role membership. The SystemAdmin provides all administrative and configuration functionality not exclusively defined under the SecurityAdmin role, including modifying and querying audit configuration settings and events. In addition to administrator roles, file owners can also modify the rwx permissions[25] and DACL[26] access to their own resources. The root, SystemAdmin, SecurityAdmin, and AuditAdmin roles access the TOE through security management interfaces. In addition, the root role has access to the TOE through the CLI to perform OS upgrades. The SystemAdmin, SecurityAdmin, 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 depending on their permissions.

1.5.1.7 Protection of the TOE Security Functionality (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 performs the synchronization of ACLs, logs, and user data to ensure inter-TSF data consistency.

1.5.1.8 Resource Utilization

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

1.5.1.9 TOE Access

Before a session is initiated, the TOE displays an advisory warning message via the Web Administration GUI and CLI regarding any unauthorised use of the TOE. Users are locked out of their sessions after a 4-hour period of inactivity. Once a user is locked out, they must re-authenticate to the TOE to regain access.

1.5.2 Product Physical/Logical Features and Functionality not included in the TOE

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

- InsightIQ
- Isilon for vCenter
- iSCSI[27]

[25] rwx – Unix permission flags of read, write, and execute
[26] DACL – Discretionary Access Control List
[27] iSCSI – Internet Small Computer System Interface

- CHAP[28]
- NDMP[29]
- SmartLock
- HDFS[30]
- Swift
- Management workstations
- SupportIQ
- Unauthenticated SMB/FTP
- RESTful Access to Namespace (RAN)
- Anti-Virus Scans
- Configuration changes performed via SMB data path

[28] CHAP – Challenge-Handshake Authentication Protocol
[29] NDMP – Network Data Management Protocol
[30] HDFS – Hadoop Distributed File System

2 Conformance Claims

Table 2 identifies all 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, Release 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; Parts 2 and 3 Interpretations of the CEM as of 2014/03/10 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[31] 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.

[31] IT – Internet Technology

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 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 enforcing self-tests and 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 [<u>underlined text within brackets</u>].
- 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(a)	Audit Data Generation (Syslog)	✓	✓		✓
FAU_GEN.1(b)	Audit Data Generation (PAPI)	✓	✓		✓
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.1	Export of user data without security attributes		✓		
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FDP_ITC.1	Import of user data without security attributes		✓		
FDP_ROL.1	Basic rollback		✓		
FDP_SDI.1	Stored data integrity monitoring		✓		
FIA_UAU.1	Timing of authentication		✓		

Name	Description	S	A	R	I
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UID.1	Timing of identification		✓		
FMT_MSA.1(a)	Management of security attributes	✓	✓		✓
FMT_MSA.1(b)	Management of security attributes	✓	✓		✓
FMT_MSA.3(a)	Static attribute initialization	✓	✓		✓
FMT_MSA.3(b)	Static attributes initialization	✓	✓		✓
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_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	✓	✓		
FTA_SSL.3	TSF-initiated termination		✓		

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1(a) Audit Data Generation (Syslog)
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps
FAU_GEN.1.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*file system errors and repairs, hardware events, snapshot events, software status, disk quotas, synchronizations, disk and nodes failures, connection and disconnection attempts*].

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*node name and IP address (if applicable)*].

FAU_GEN.1(b) Audit Data Generation (PAPI)
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps
FAU_GEN.1.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*administrator logins, configuration changes made through Web Administration GUI and CLI, and SMB share creation, modification, SMB file actions (create, read, delete)*].

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other information*].

FAU_SAR.1 Audit review
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FAU_SAR.1.1

The TSF shall provide [*root, SystemAdmin, SecurityAdmin, AuditAdmin, and custom roles with sufficient privileges*] 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.

FAU_STG.1 Protected audit trail storage
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2

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

FAU_STG.4 Prevention of audit data loss
Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1

The TSF shall [overwrite the oldest stored **Syslog** audit records] and [*send email alert, SNMP*[32] *traps, or klog events*] if the audit trail is full.

[32] SNMP - Simple Network Management Protocol

6.2.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1

The TSF shall enforce the [*Data Access SFP*] on [*Subjects: users and client systems accessing data; Objects: files, directories, exports, shares, and clusters; and Operations: access, read, write, delete, execute*].

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1

The TSF shall enforce the [*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[33]	DACL, ACE[34]
NFS	UID[35] , GID[36]	rwx permissions, DACL

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) *SMB protocol – an authorised administrator has assigned the user to a DACL that permits access to the share and the file*
2) *NFS protocol – an authorised administrator has granted access for the client system on the export and assigned the user to a DACL*

].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [
Rules:

1) *SMB protocol – an authorised administrator denies permission to the object through a DACL*
2) *NFS protocol – an authorised administrator denies the client name access to the export or an authorised user denies permission to the object through a DACL*

FDP_ETC.1 Export of user data without security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

[33] SID – Security Identifier
[34] ACE – Access Control Entry
[35] UID – User Identifier
[36] GID – Group Identifier

FDP_ETC.1.1

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

FDP_ETC.1.2

The TSF shall export the user data without the user data's associated security attributes.

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1

The TSF shall enforce the [*Data Transfer SFP*] on [
Subjects: Source TOE Root Directory, Target TOE Host
Information: files, directories
Operations: mirror data to separate node via the SnapshotIQ process and synchronize data via the SyncIQ process
].

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1

The TSF shall enforce the [*Data Transfer SFP*] based on the following types of subject and information security attributes: [
Subjects: Source TOE Root Directory, Target TOE Host
Information: files, directories
Information security attribute: SyncIQ replication policy criteria
].

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: [*The Target TOE matches the criteria specified in the SyncIQ replication policy of the source TOE*].

FDP_IFF.1.3

The TSF shall enforce the [*SyncIQ policy*].

FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules: [*SyncIQ policy rules*].

FDP_IFF.1.5

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

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1

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

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*no other rules*].

FDP_ROL.1 Basic rollback

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ROL.1.1

The TSF shall enforce [*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 the [*last TOE created snapshot*].

FDP_SDI.1 Stored data integrity monitoring

Hierarchical to: No other components.
Dependencies: No dependencies

FDP_SDI.1.1

The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all objects, based on the following attributes: [*disk and node failures, file checksums*].

6.2.3 Class FIA: Identification and Authentication

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1

The TSF shall allow [*viewing of cluster status*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

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

FIA_UAU.5 Multiple authentication mechanisms
Hierarchical to: No other components.
Dependencies: No dependencies

FIA_UAU.5.1

The TSF shall provide [*local (SAM*[37]*) database, Active Directory service]* to support user authentication.

FIA_UAU.5.2

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

FIA_UID.1 Timing of identification
Hierarchical to: No other components.
Dependencies: No dependencies

FIA_UID.1.1

The TSF shall allow [*viewing of cluster status*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

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

[37] SAM – Security Account Manager

6.2.4 Class FMT: Security Management

FMT_MSA.1(a) Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall enforce the [*Data Access SFP*] to restrict the ability to [change, query, modify, delete, *[create]*] the security attributes [*DACL, ACEs, and rwx permissions*] to [*root, SecurityAdmin role, SystemAdmin role, custom roles with sufficient privileges, or file owners*].

FMT_MSA.1(b) Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall enforce the [*Data Transfer SFP*] to restrict the ability to [change, query, modify, delete, *[none]*] the security attributes [*SyncIQ policy attributes*] to [*root, SecurityAdmin role, or custom roles with sufficient privileges*].

FMT_MSA.3(a) Static attribute initialisation
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1

The TSF shall enforce the [*Data Access SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*root, SecurityAdmin role, or custom role with sufficient privileges*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(b) Static attribute initialisation
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1

The TSF shall enforce the [*Data Transfer SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*root, SecurityAdmin role, or custom role with sufficient privileges*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1

The TSF shall restrict the ability to [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, SecurityAdmin, Custom role with sufficient permission
Reset	User passwords	Root, SecurityAdmin, Custom role with sufficient permission
Set, Modify	Protection levels	Root, SystemAdmin, Custom role with sufficient permission
Enable, Disable	Authentication mode	Root, SecurityAdmin, Custom role with sufficient permission
Modify, Query	Audit configuration settings, Events	Root, SystemAdmin, Custom role with sufficient permission
View	Audit configuration settings, Events	Root, SystemAdmin, AuditAdmin, Custom role with sufficient permission

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No Dependencies

FMT_SMF.1.1

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

FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [*Root, SecurityAdmin, SystemAdmin, AuditAdmin, file owner, and custom*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.5 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*disk or node failure*].

FPT_RCV.3 Automated recovery without undue loss
Hierarchical to: FPT_RCV.2 Automated recovery
Dependencies: AGD_OPE.1 Operational user guidance
FPT_RCV.3.1

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

FPT_RCV.3.2

For [*disk or 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.

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
Dependencies: No dependencies
FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

FPT_TDC.1 Inter-TSF basic TSF data consistency
Hierarchical to: No other components.
Dependencies: No dependencies
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.

6.2.6 Class FRU: Resource Utilization

FRU_RSA.1 Maximum quotas
Hierarchical to: No other components.
Dependencies: No dependencies

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].

6.2.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination
Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*4 hour time period of user inactivity*].

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[38] system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Basic Flaw Remediation
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

[38] CM – Configuration Management

7 TOE Security 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 Functionality

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

Table 12 Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1(a)	Audit Data Generation (Syslog)
	FAU_GEN.1(b)	Audit Data Generation (PAPI)
	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.1	Export of user data without security attributes
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITC.1	Import of user data without security attributes
	FDP_ROL.1	Basic rollback
	FDP_SDI.1	Stored data integrity monitoring
Identification and Authentication	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification
Security Management	FMT_MSA.1(a)	Management of security attributes
	FMT_MSA.1(b)	Management of security attributes
	FMT_MSA.3(a)	Static attribute initialization
	FMT_MSA.3(b)	Static attributes initialization
	FMT_MTD.1	Management of TSF data

TOE Security Functionality	SFR ID	Description
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functions	FPT_FLS.1	Failure with preservation of secure state
	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
TOE Access	FTA_SSL.3	TSF-initiated termination

7.1.1 Security Audit

The TOE maintains many logging daemons that are used by administrators to monitor and troubleshoot the system. Each log contains a record of the start-up of the audit function. Although the TOE does not audit the shutdown of the audit function, it does audit the shutdown of the TOE, thereby indicating when the audit function is stopped as well.

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. Syslog audit records are generated from file system errors and repairs, hardware events and failures, snapshot events, software status, synchronizations, and connection and disconnection attempts. Table 13 contains a list of security relevant logs configured by default for the syslog. The TOE audit records contain the following information:

Table 13 Syslog Audit Record Contents

Field	Content
SMB access log	Network and object events for SMB file share
NFS access log	User connections and disconnections to NFS file share
Active Directory log	Logs successful and unsuccessful AD authentication attempts
Apache log	Administrator connections and disconnections to HTTP
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
SMB log	File share events with SMB protocol

Field	Content
NFS log	File exports events with NFS protocol

PAPI generated audit logs are generated from PAPI-driven events including administrator logins, configuration changes made through the Web Administration GUI and CLI, and SMB protocol events. PAPI-driven events are logged into a JSON[39] format that is stored in a per-node file/namespace. Table 14 contains a list of security relevant logs produced by PAPI generated events.

Table 14 PAPI Audit Record Contents

Field	Content
Connection log	Administration log for CLI, Web Administration GUI, and PAPI connections
SMB protocol log	Log of SMB events including the creation and management of SMB shares
Configuration log	Log of configuration changes to the cluster or file system via Web Administration GUI and CLI

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 (if applicable)

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

Only the root role and authorised 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. Logs can also be viewed through PAPI using the "GET /platform/1/audit/topics/<name>" API call. 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 syslog audit trail reaches its administrator defined capacity, an email, SNMP trap, or klog event is sent, the log is overwritten and a new log is started.

TOE Security Functional Requirements Satisfied: FAU_GEN.1(a), FAU_GEN.1(b), 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 an SID. The SID is a unique identifier for each user. UNIX users are assigned a UID and at least one 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

[39] JSON – JavaScript Object Notation

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 authorised administrator can configure the permission translation policies using the Web Administration GUI, and file owners can configure the permission translation policies via a data path. 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 SFP. This policy enforces information flow control using the SyncIQ, SnapshotIQ, and SmartConnect criteria according to defined SyncIQ replication policies. SyncIQ is used to synchronize data between clusters. SyncIQ associates a replication policy with a target cluster by marking the target cluster when the job runs for the first time. Even if the name or IP address of the target cluster is modified, the mark persists on the target cluster. When a replication policy is run, SyncIQ checks the mark to ensure that data is being replicated to the correct location. On the target cluster, an association between a replication policy and target directory can be manually broken by an authorized user. Breaking the association between a source and target cluster causes the mark on the target cluster to be deleted.

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. The SnapshotIQ and SyncIQ processes are controlled according to the TOE's SyncIQ replication policy which includes many settings such as Action, Source Root Directory, Target Host, and SnapshotIQ settings.

The SyncIQ replication policy can determine whether replication jobs connect only to nodes in a given SmartConnect zone. This setting applies only if the Target Host is specified as a SmartConnect zone. The SmartConnect feature of the TOE allows an authorised 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.

Files and directories are monitored by FlexProtect for integrity errors using the Reed Solomon algorithm (for disk and node failures) and file checksums. Files and directories are also protected from unauthorised 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 node failures. The protection levels are defined in Table 15. 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.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1, FDP_ROL.1, FDP_SDI.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 unauthorised personnel. The following functions are available from the front panel:

- 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

Multiple authentication methods are supported by the TOE that differ based on the user's operating system. Users can use local authentication or the Active Directory service. 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 an 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 are typically assigned UIDs. An access token is created using the same process described above. The root, SecurityAdmin, AuditAdmin, and SystemAdmin can access the TOE through the CLI interface, PAPI, or the Web Administration GUI. Users access the TOE through an external Gigabit Ethernet connection supporting standard network communication protocols including: NFS and SMB.

TOE Security Functional Requirements Satisfied: FIA_UAU.1, FIA_UAU.5, FIA_UID.1.

7.1.4 Security Management

The TOE maintains the root role and three built-in administrative roles: SecurityAdmin, SystemAdmin, and AuditAdmin. Custom roles may also be created with specified privileges. The root, SecurityAdmin, and SystemAdmin roles may perform management tasks through the Web Administration GUI. Although the SecurityAdmin, SystemAdmin, and AuditAdmin roles 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 the files and directories stored in the TOE, and is the only role that can install the TOE and perform initial configuration. File owners 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 SecurityAdmin roles are both capable of creating user accounts and assigning them to an ACL or UNIX group, through the CLI interface, PAPI, or Web Administration GUI. The root and SecurityAdmin can also create customized roles. Once a user has been created, their accounts and permissions are managed from the Web Administration GUI, PAPI, and CLI interface. Creation of user accounts can be delegated to Windows 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.

The TOE enforces the management of disk storage quotas accounting and enforcement, access modes, scheduling jobs, and setting protection levels. Default permission levels are set for all directories at their creation and all users are assigned the default permissions unless modified by an authorised administrator. File integrity data is protected at the same level as the file itself. This data can only be changed or removed by an authorised administrator. Protection levels are normally set at the cluster level by an authorised 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, SecurityAdmin role, SystemAdmin role, and file owners 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 and FTP must be enabled or a license must be activated by an authorised administrator with the SystemAdmin or customized role with sufficient privileges. Lastly, SystemAdmins 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_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 15 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 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.

Table 15 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 authorised 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 operation’s 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.

Synchronization of data between clusters is supported for the TOE. SyncIQ is used to perform the synchronization. Authorised administrator defined policies maintain data integrity during these transfers. 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 synchronization occurs, what the source and target directories are, and specific file criteria for what will be synchronized.

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

The sysclock provides a reliable timestamp for the TOE. One or more Network Time Protocol (NTP) servers can be setup to synchronize the system time on the EMC cluster. The cluster periodically contacts the NTP servers and sets the date and time based on the information it receives.

TOE Security Functional Requirements Satisfied: FPT_FLS.1, FPT_RCV.3, FPT_STM.1, FPT_TDC.1

7.1.6 Resource Utilization

The SmartQuotas module of the TOE allows authorised 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 16 defines the types of thresholds that can be defined for an enforcement quota.

Table 16 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 TOE Access

After users log in to the TOE via the Web Administration GUI or CLI, there is a 4-hour login timeout where a user needs to login again to regain access to their interactive session.

TOE Security Functional Requirements Satisfied: FTA_SSL.3.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Release 4.

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 8.2.3 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 17 below provides a mapping of the objectives to the threats they counter.

Table 17 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	O.AUDIT_REVIEW counters this threat by ensuring that the TOE will provide mechanisms to

Threats	Objectives	Rationale
	authorized security 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 enforcing self-tests and 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

Threats	Objectives	Rationale
		masquerade as an authorized user.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.AUTHENTICATE counters this 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 enforcing self-tests and 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

Threats	Objectives	Rationale
		modify the data access policy to bypass the intended TOE security policy.
T.UNAVAILABILITY The TOE may be overwhelmed by legitimate user tasks, preventing or delaying any TOE functionality from being accessed.	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.	O.QUOTAS counters this threat by ensuring that the TOE limits 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 18 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 18 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,	NOE.PHYSICAL satisfies this assumption by ensuring physical security is provided within the TOE environment to provide

Assumptions	Objectives	Rationale
	processed, and transmitted information.	appropriate protection to the network resources.
A.PROTECT The TOE software will be protected from unauthorized modification.	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.NO_BYPASS satisfies this assumption. The TOE environment ensures that security 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 19 below shows a mapping of the objectives and the SFRs that support them.

Table 19 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(a) Audit Data Generation (Syslog)	FAU_GEN.1(a) 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.
	FAU_GEN.1(b) Audit Data Generation (PAPI)	FAU_GEN.1(b) 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

Objective	Requirements Addressing the Objective	Rationale
		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 overwritten and email alerts sent when syslog audit trail exceeds administrator defined capacity.
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_UAU.1 Timing of authentication	FIA_UAU.1 supports this 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	FPT_RCV.3 supports this objective by ensuring the TOE

Objective	Requirements Addressing the Objective	Rationale
	Automated recovery without undue loss	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 enforcing self-tests and protecting itself from unauthorized modifications and access to its functions and data.	FDP_SDI.1 Stored data integrity monitoring	FDP_SDI.1 supports this objective by enforcing the monitoring of the TOE for integrity errors.
	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.
	FTA_SSL.3 TSF-initiated termination	FTA_SSL.3 supports this objective by terminating interactive sessions after a configurable period of inactivity.
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(a) Audit Data Generation (Syslog)	FAU_GEN.1(a) supports this objective by providing authorized administrators access to the audit data necessary to manage the TOE.
	FAU_GEN.1(b) Audit Data Generation (PAPI)	FAU_GEN.1(b) 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_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 initialization	FMT_MSA.3(a) supports this objective by requiring a restrictive default for the data access SFP.
	FMT_MSA.3(b) Static attributes initialization	FMT_MSA.3(b) supports this objective by requiring a

Objective	Requirements Addressing the Objective	Rationale
		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 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.1 Export of user data without security attributes	FDP_ETC.1 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.1 Import of user data without security attributes	FDP_ITC.1 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_RCV.3 Automated recovery without undue loss	FPT_RCV.3 supports this objective by requiring that the TOE will recover from disk or

Objective	Requirements Addressing the Objective	Rationale
		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 synchronization 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 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.	FRU_RSA.1 Maximum quotas	FRU_RSA.1 supports this 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

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 20 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 20 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1(a)	FPT_STM.1	✓	
FAU_GEN.1(b)	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3(a)	✓	
FDP_ETC.1	FDP_IFC.1	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FMT_MSA.3(b)	✓	
	FDP_IFC.1	✓	
FDP_ITC.1	FMT_MSA.3(b)	✓	
	FDP_IFC.1	✓	
FDP_ROL.1	FDP_IFC.1	✓	
FDP_SDI.1	No dependencies	n/a	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.5	No dependencies	n/a	
FIA_UID.1	No dependencies	n/a	
FMT_MSA.1(a)	FDP_ACC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(b)	FDP_IFC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(a)	FMT_MSA.1(a)	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(b)	FMT_SMR.1	✓	
	FMT_MSA.1(b)	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_SMF.1	No dependencies	n/a	
FMT_SMR.1	FIA_UID.1	✓	
FPT_FLS.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	
FTA_SSL.3	No dependencies	n/a	

9 Acronyms and Terms

This section, Table 21, and Table 22 define the acronyms and terms used throughout this document.

9.1 Acronyms

Table 21 Acronyms

Acronym	Definition
ACE	Access Control Entry
ACL	Access Control List
AD	Active Directory
API	Application Programming Interface
CC	Common Criteria
CHAP	Challenge-Handshake Authentication Protocol
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
DACL	Discretionary Access Control List
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
GID	Group Identifier
GigE	Gigabit Ethernet
GUI	Graphical User Interface
HDFS	Hadoop Distributed File System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IOPS	Input/Output Operations Per Second
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface
IT	Information Technology
JSON	JavaScript Object Notation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
MTU	Maximum Transmission Unit

Acronym	Definition
NAS	Network-Attached Storage
NDMP	Network Data Management Protocol
NFS	Network File System
NIS	Network Information Service
NTP	Network Time Protocol
NVRAM	Non-Volatile Random-Access Memory
OS	Operating System
PAPI	Platform API
PB	Petabyte
POSIX	Portable Operating System Interface
PP	Protection Profile
RAM	Random-Access Memory
RAN	Restful Access to Namespace
REST	Representational State Transfer
SAM	Security Account Manager
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SID	Security Identifier
SNMP	Simple Network Management Protocol
SMB	Server Message Block
SSH	Secure Shell
ST	Security Target
TB	Terabyte
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
UI	User Interface
UID	User Identifier
VTL	Virtual Tape Libraries
WebDAV	Web Distributed Authoring and Versioning

9.2 Terminology

Table 22 Terms

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

Prepared by:
Corsec Security, Inc.

13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

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