Dell EMC™ Isilon with OneFS 8.2.0

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2102-000-D102
Version: 1.3
22 October 2019

Dell EMC
176 South Street
Hopkinton, MA, USA
01748

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8 Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	Dell EMC™ Isilon with OneFS 8.2.0 Security Target
ST Version:	1.3
ST Date:	22 October 2019

1.3 TOE REFERENCE

TOE Identification: Dell EMC™ Isilon with OneFS 8.2.0.0.011 with Patches 254792, 257595, and 257593

TOE Developer: Dell EMC

TOE Type: Data Storage (Other Devices and Systems)

1.4 TOE OVERVIEW

Dell EMC Isilon OneFS is a data storage solution that combines the three layers of traditional storage architectures – file system, volume manager, and data protection – into a unified software layer, creating a single distributed file system that runs on an Isilon storage cluster, and eliminates the need for volume management.

OneFS provides controlled access to data accessed over Server Message Block (SMB), Network File System (NFS) and Hadoop Distributed File System (HDFS) protocols. Physical and logical access may be restricted to identified groups or departments within the organization. Access to management functionality is based on roles.

Isilon protects the confidentiality of data by offering self-encrypting drives (SEDs) for data storage. Cryptographic functionality is also provided to protect communications between OneFS and remote administrators. These security features are provided by validated cryptographic modules and algorithms.

Isilon OneFS Smartlock protects files on an Isilon cluster from being modified, overwritten, or deleted. Organizations can identify a directory in OneFS as a Write Once, Read Many (WORM) domain. All files within the WORM domain can be committed to a WORM state, meaning that those files cannot be overwritten, modified, or deleted.

Stored data is monitored for integrity, and where integrity errors are detected, the data is rebuilt using Reed-Soloman encoding.

Synchronization between clusters ensures the provision of data in multiple physical locations. A secure state is maintained in the case of a failure of one of these locations, and the secure state is maintained as automated recovery procedures recover lost data.

Administrators must be identified and authenticated prior to accessing the security management features of Isilon OneFS. Active Directory (AD) and local authentication are supported in the evaluated configuration. Administrators of various roles are able to manage Isilon features through a Command Line Interface (CLI), Web User Interface (WebUI) and Platform Application Programming Interface (PAPI). An access banner is implemented on the CLI and WebUI to display an administrator customizable message prior to login. Unused network services may be disabled for improved security.

Comprehensive auditing creates records of administrator actions, configuration changes and protocol activity. Logs may be viewed through the CLI and WebUI.

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The following operating system, hardware and networking components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Data Path User (SMB)	Windows 10	General Purpose Computing Hardware
Data Path User (NFS and HDFS)	RHEL 7.5 (with NFS-Utils, cURL)	General Purpose Computing Hardware
Administrator Workstation	Windows 10	General Purpose Computer Hardware
Active Directory	Windows 10	General Purpose Computer Hardware

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

Figure 1 shows the TOE boundary in a single cluster deployment configuration. In the evaluated configuration, two clusters are implemented to demonstrate synchronization between clusters. A cluster is made up of a minimum of three nodes and a switch.

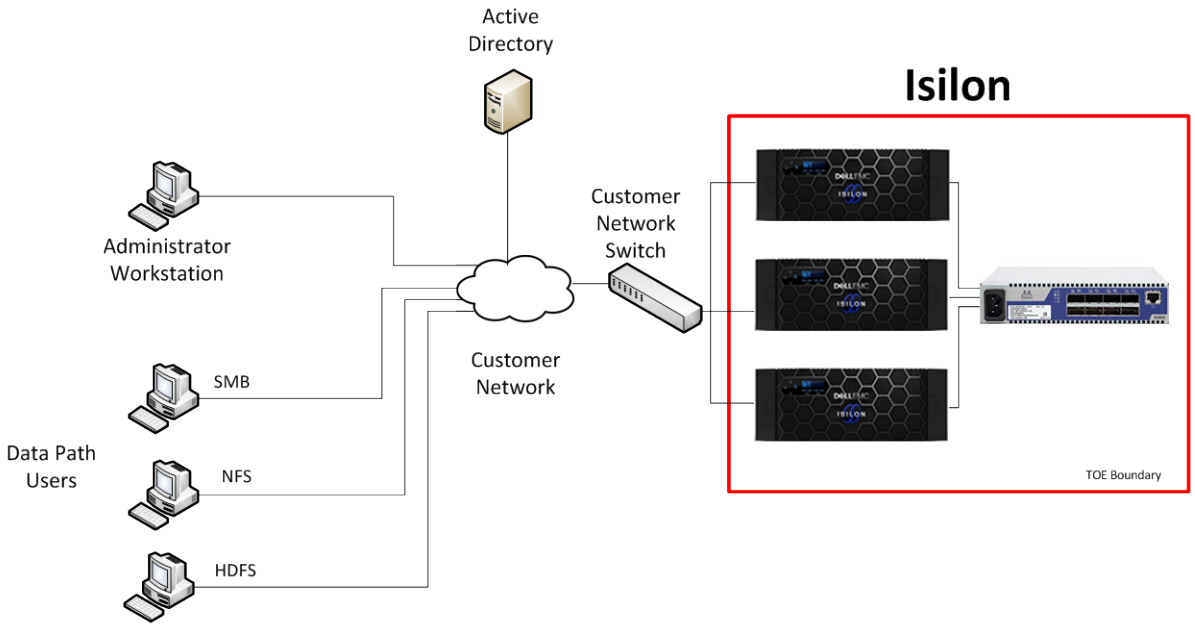

Figure 1 – TOE Diagram

1.5.1.1 TOE Delivery

The TOE includes the OneFS 8.2.0 software on the hardware models in Table 2.

Generation	Model
Gen5	X210
	X410
	NL410
	HD400
	S210
Gen6	A200
	A2000
	H400
	H500
	H600
	F800

Table 2 –TOE Hardware

The TOE is delivered as a hardware device, with software, by trusted courier. The customer typically prepares for the installation following the instructions in the planning guide and engages professional services to complete the installation and initial configuration at the customer site.

If the software that is delivered with the hardware is not the evaluated version, the customer may download the following file from the Dell EMC support site:

OneFS_v8.2.0.0_Install.tar.gz

1.5.1.2 TOE Guidance

The TOE guidance is available for download from the Dell EMC support site. The TOE includes the following guidance documentation:

- Generation 6 Site Preparation and Planning Guide, June 2019
  - docu52911_Generation-6-Site-Preparation-and-Planning-Guide.pdf
- Isilon OneFS Version 8.2.0 CLI Administration Guide, June 2019
  - docu93697_OneFS-8.2.0-CLI-Administration-Guide.pdf
- Isilon OneFS Version 8.2.0 Web Administration Guide, May 2019
  - docu93698_OneFS-8.2.0-Web-Administration-Guide.pdf
- Isilon OneFS 8.2.0 Security Configuration Guide, Version 8.2.0, Security Configuration Guide, May 2019
  - docu93703_OneFS_8.2.0_Security_Configuration_Guide.pdf
- Isilon OneFS Version 8.2 Event Reference, May 2019
  - docu93701_OneFS-8.2.0-Event-Reference.pdf

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. The audit logs can be reviewed by authorized administrators.
Cryptographic Support	Cryptographic functionality is provided to allow the communications links between the TOE and its remote administrators to be protected. Stored user data is encrypted.

Functional Classes	Description
User Data Protection	Access to data is restricted to authorized users. Access to user data may be further restricted by creating access zones for internal groups or departments. The TOE provides a role-based access control capability to ensure that only authorized administrators are able to administer the TOE. Data is monitored for integrity errors and the data is rebuilt when errors are detected.
Identification and Authentication	Administrative users are identified and authenticated prior to being granted access to TOE functions. Local authentication and Active Directory authentication are supported.
Security Management	The TOE provides management capabilities via a Web-Based Graphical User Interface (GUI), a CLI and a Platform Application Programming Interface (API). Management functions allow the administrators to manage access control, configure system settings, and view audit records.
Protection of the TSF	Data is replicated to other clusters to ensure availability. Data is automatically recovered in the case of loss in multiple scenarios. Timestamp information is provided to support auditing.
TOE Access	A banner is presented on user login to the WebUI or CLI.
Trusted Path/Channel	The communications links between the TOE and its remote administrators are protected using Transport Layer Security (TLS).

Table 3 – Logical Scope of the TOE

1.5.3 Functionality Supported but not Included in the Evaluated Configuration

The following features are supported, but were not examined as part of this evaluation:

- Support for NFS v4
- A description of how the access control decisions are executed in a mixed permission environment is available in the Isilon OneFS Version 8.2.0 Web Administration Guide; however, this is outside the scope of this evaluation

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

2.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2 Flaw Reporting Procedures.

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP, therefore a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 4 lists the threats addressed by the TOE. Potential threat agents are authorized TOE users, unauthorized persons, and accidental corruption or hardware failure. The level of expertise of both types of attacker is assumed to be unsophisticated. TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters, but are assumed not to be wilfully hostile. Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.
T.AVAIL	User data may become unavailable due to corruption of the data, or loss of the supporting hardware.
T.UNDETECT	Authorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.
T.UNAUTH	An unauthorized user may be able to gain access to user data in order to view or modify private information.

Table 4 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 5 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.PRIVATE	The TOE shall protect the privacy of stored data.
P.PROTECT	The TOE shall incorporate cryptographic mechanisms to protect against potential disclosure or modification of sensitive information,

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

Table 5 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 6.

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

Table 6 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ACCESS	The TOE must restrict access to the user data held by the TOE to only authorized data path users. The TOE must be able to restrict user access based on defined access zones.
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security functions provided by the TOE, and restrict these functions and facilities from unauthorized use.
O.AUDIT	The TOE must record audit events for changes to the TOE configuration, and use of the TOE data channels. Audit records must be readable by authorized administrators. Multiple authentication mechanisms must be supported by the TOE.
O.BANNER	The TOE must display an access warning to administrative users prior to login on the Web and CLI applications.
O.CRYPTO	The TOE shall use validated cryptographic algorithms in support of cryptographic operations.
O.IDENTAUTH	The TOE must ensure that users are identified and authenticated prior to allowing access to the administrative functions and data of the TOE. Multiple authentication mechanisms must be supported by the TOE.
O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to data corruption, or disk or node failure.
O.PROTECT	The TOE must provide a means of disabling access to unused TOE services.

Security Objective	Description
O.RETAIN	The TOE must prevent the deletion of data prior to expiry of the assigned retention period.
O.SECURE	The TOE must ensure the confidentiality and integrity of interactive administrative sessions.
O.TIME	The TOE must provide reliable timestamps.

Table 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

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

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

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

Table 9 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE back to the threats addressed by the TOE.

Threat: T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security functions provided by the TOE, and restrict these functions and facilities from unauthorized use.
	O.BANNER	The TOE must display an access warning to administrative users prior to login on the Web

		and CLI applications.
	O.CRYPTO	The TOE shall use validated cryptographic algorithms in support of cryptographic operations.
	O.IDENTAUTH	The TOE must ensure that users are identified and authenticated prior to allowing access to the administrative functions and data of the TOE. Multiple authentication mechanisms must be supported by the TOE.
	O.PROTECT	The TOE must provide a means of disabling access to unused TOE services.
	O.SECURE	The TOE must ensure the confidentiality and integrity of interactive administrative sessions.
Rationale:	O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized users. O.BANNER mitigates the threat of access by user error by allowing a clear message related to authorized access to be displayed prior to login. O.CRYPTO mitigates the threat of system error by providing trusted cryptographic functions to protect data from unauthorized access. O.IDENTAUTH mitigates the threat by providing the means for users to authenticate prior to gaining access to the functions assigned to that user. O.PROTECT mitigates this threat by disabling access to the TOE services that should not be in use. O.SECURE mitigates the threat by ensuring that the confidentiality of administrative sessions is protected.	

Threat: **T.AVAIL**	User data may become unavailable due to corruption of the data, or loss of the supporting hardware.	
Objectives:	O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to data corruption, or disk or node failure.
Rationale:	O.INTEGRITY mitigates this threat by protecting the integrity of user data from corruption, or hardware loss.	

Threat: **T.UNAUTH**	An unauthorized user may be able to gain access to user data in order to view or modify private information.	
Objectives:	O.ACCESS	The TOE must restrict access to the user data

		held by the TOE to only authorized data path users. The TOE must be able to restrict user access based on defined access zones.
	O.PROTECT	The TOE must provide a means of disabling access to unused TOE services.
Rationale:	O.ACCESS mitigates this threat by ensuring that only authorized users are permitted access to user data, and users may be further restricted based on access zones. O.PROTECT mitigates this threat by allowing unused services to be disabled, providing fewer paths for unauthorized users to reach the data.	

Threat: **T.UNDETECT**	Authorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.	
Objectives:	O.AUDIT	The TOE must record audit events for changes to the TOE configuration, and use of the TOE data channels. Audit records must be readable by authorized administrators. Multiple authentication mechanisms must be supported by the TOE.
	O.TIME	The TOE must provide reliable timestamps.
Rationale:	O.AUDIT mitigates the threat by ensuring that audit records are generated for security relevant events. O.TIME supports the O.AUDIT objective by providing accurate time to those audit records.	

4.3.2 Security Objectives Rationale Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE back to the OSPs applicable to the TOE.

Policy: **P.PRIVATE**	The TOE shall protect the privacy of stored data.	
Objectives:	O.CRYPTO	The TOE shall use validated cryptographic algorithms in support of cryptographic operations.
Rationale:	O.CRYPTO supports this policy by providing cryptographic algorithms to protect user data.	

Policy: **P.PROTECT**	The TOE shall incorporate cryptographic mechanisms to protect against potential disclosure or modification of sensitive information, which is transferred between the TOE and administrators.	
Objectives:	O.CRYPTO	The TOE shall use validated cryptographic algorithms in support of cryptographic operations.
Rationale:	O.CRYPTO supports this policy by providing cryptographic algorithms to protect administrator data.	

Policy: **P.RETAIN**	The TOE shall provide a means to identify a retention period before which data is not to be deleted, and prevent data from being deleted prior to the expiry of the retention period.	
Objectives:	O.RETAIN	The TOE must prevent the deletion of data prior to expiry of the assigned retention period.
	O.TIME	The TOE must provide reliable timestamps.
Rationale:	O.RETAIN supports this policy by preventing the accidental deletion of data, thereby ensuring that the data is retained in accordance with policy. O.TIME supports O.RETAIN by providing reliable time in support of this function.	

4.3.3 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption: **A.AUTH**	Data path users are identified and authentication prior to gaining access to the TOE.	
Objectives:	OE.USERAUTH	Data path users must be identified and authenticated in the operational environment.
Rationale:	OE.USERAUTH supports this assumption by ensuring that identification and authentication of users is provided by the operational environment.	

Assumption: **A.LOCATE**	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by ensuring that the operational environment provides physical protection of the TOE.	

Assumption: **A.MANAGE**	There are one or more competent individuals assigned to manage the TOE. These administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE.ADMIN	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
Rationale:	OE.ADMIN supports this assumption by ensuring the availability of trained, competent administrators who are trustworthy and not malicious.	

5 EXTENDED COMPONENTS DEFINITION

This section specifies the extended Security Functional Requirements (SFRs) used in this ST. Two extended SFRs have been created to address additional security features of the TOE. Retention of data (FDP_RET_EXT.1) addresses the requirement to retain data and Service Access (FTA_SAC_EXT.1) defines requirements for controlling access to TOE services.

5.1 CLASS FDP: USER DATA PROTECTION

A new family has been added with one SFR. FDP_RET_EXT Retention of data addresses the requirement to retain data. FDP_RET_EXT.1 Retention of data addresses retention requirements for stored data, and is modelled after FDP_SDI.1 Stored data integrity monitoring and FPT_RCV.1 Manual recovery.

5.1.1 FDP_RET_EXT

Family Behaviour

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

Component Levelling

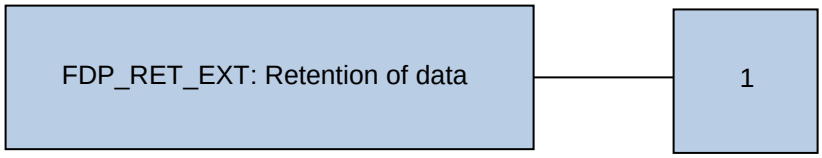

Figure 2 – FDP_RET_EXT: Data Retention Component Levelling

Management: FDP_RET_EXT.1

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

a) Setting the retention period.

Audit: FDP_RET_EXT.1

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

a) Minimal: changes to the retention period.

5.1.1.1 FDP_RET_EXT.1 Retention of data

Hierarchical to: No other components.

Dependencies: FPT_STM.1

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

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

5.2 CLASS FTA: TOE ACCESS

A new family has been added with one SFR. FTA_SAC_EXT.1 Service Access has been created to define requirements for controlling access to TOE services. FTA_SAC_EXT.1 Service access is modelled after FTA_TSE.1 TOE Session Establishment.

5.2.1 FTA_SAC_EXT Service Access Controls

Family Behaviour

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

Component Levelling

Figure 3 – FTA_SAC_EXT: Service Access Controls Component Levelling

FTA_SAC_EXT.1 Service access requires the TOE to provide functionality to restrict access to TOE services.

Management

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

a. configuration of allowed services.

Audit

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

a. changes to the configuration of allowed services.

5.2.1.1 FTA_SAC_EXT.1 Service and Port Access Controls

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.3 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (Data path)' and 'FDP_ACC.1(2) Subset access control (RBAC)'.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 10.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (TOE Management)
	FCS_COP.1(2)	Cryptographic operation (Data at rest encryption)

Class	Identifier	Name
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (Data path)
	FDP_ACC.1(2)	Subset access control (RBAC)
	FDP_ACC.1(3)	Subset access control (Access Zones)
	FDP_ACF.1(1)	Security attribute based access control (Data path)
	FDP_ACF.1(2)	Security attribute based access control (RBAC)
	FDP_ACF.1(3)	Security attribute based access control (Access Zones)
	FDP_RET_EXT.1	Retention of data
	FDP_SDI.2	Stored data integrity monitoring and action
Identification and Authentication (FIA)	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MSA.1(1)	Management of security attributes (Data path)
	FMT_MSA.1(2)	Management of security attributes (RBAC)
	FMT_MSA.1(3)	Management of security attributes (Access Zones)
	FMT_MSA.3(1)	Static attribute initialisation (Data path)
	FMT_MSA.3(2)	Static attribute initialisation (RBAC)
	FMT_MSA.3(3)	Static attribute initialisation (Access Zones)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles

Class	Identifier	Name
Protection of the TSF (FPT)	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RCV.3	Automated recovery without undue loss
	FPT_STM.1	Reliable time stamps
	FPT_TRC.1	Internal TSF consistency
TOE Access (FTA)	FTA_TAB.1	Default TOE access banners
	FTA_SAC_EXT.1	Service access
Trusted path/channels (FTP)	FTP_TRP.1	Trusted path

Table 10 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

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

c) [*no other specifically defined auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

6.2.1.2 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 [*users assigned the SystemAdmin or AuditAdmin role*] 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.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*cryptographic key generation algorithm in* Table 11] and specified cryptographic key sizes [*cryptographic key sizes in* Table 11] that meet the following: [*list of standards in* Table 11].

Usage	Key Generation Algorithm	Key Size (bits)	Standard
RSA[1]	RSA Key Generation	2048 bit	FIPS[2] 186-4
AES[3]	Deterministic Random Bit Generator	128, 256	SP[4] 800-90A

Table 11 – Cryptographic Key Generation

6.2.2.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*key zeroization*] that meets the following: [*FIPS 140-2*].

6.2.2.3 FCS_COP.1(1) Cryptographic operation (TOE Management)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

[1] Rivest, Shamir and Adleman

[2] Federal Information Processing Standards

[3] Advanced Encryption Standard

[4] Special Publication

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(1) The TSF shall perform [*cryptographic operations in Table 12*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm in Table 12*] and cryptographic key sizes [*cryptographic key sizes in Table 12*] that meet the following: [*list of standards in Table 12*].

Operation	Algorithm	Key or Digest Size (bits)	Standards
Signature Generation and Verification	RSA	2048	FIPS 186-4
Symmetric Encryption/ Decryption	AES	128, 256	FIPS 197
Keyed-Hash Message Authentication Code	HMAC[5]-SHA[6]-1 HMAC-SHA2-256 HMAC-SHA2-512	160 256 512	FIPS 198
Secure Hash	SHA SHA-256 SHA-512	160 256 512	FIPS 180-4

Table 12 – Cryptographic Operations

6.2.2.4 FCS_COP.1(2) Cryptographic operation (Data at rest encryption)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

[5] Hash Message Authentication Code

[6] Secure Hash Algorithm

FCS_COP.1.1(2) The TSF shall perform [*symmetric encryption*] in accordance with a specified cryptographic algorithm [*AES*] and cryptographic key sizes [*256 bits*] that meet the following: [*Federal Information Processing Standard Publication 197*].

6.2.3 User Data Protection (FDP)

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

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

Subjects: *SMB, NFS and HDFS Users*
Objects: Files, Directories
Operations: read, write, delete, execute].

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

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

Subjects: *Administrators*
Objects: Security Management data and functions
Operations: view, create, delete, execute].

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

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

Subjects: *SMB, NFS and HDFS Users*
Objects: Files, Directories
Operations: read, write, delete, execute].

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

Hierarchical to: No other components.

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

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

Subjects: SMB, NFS and HDFS Users
Subject Attributes: Subject attributes defined in Table 13
Objects: Files, Directories
Object Attributes: Object attributes defined in Table 13].

File Share Type	Subject Attributes	Object Attributes
SMB	SID[7]	ACL[8]
NFS	UID[9], GID[10]	POSIX[11] mode bits
HDFS	UID, GID	POSIX mode bits

Table 13 – Data Path Security Attributes

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*a user may access an object if the object's ACL or POSIX mode bits indicate that the SID, UID or GID associated with the user is permitted access*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*an authorized administrator has granted explicit access through a DACL[12] or ACE[13], the user is the owner of the root account*].

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

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

Hierarchical to: No other components.

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

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

Subjects: Administrators
Subject Attributes: Role
Objects: Security Management data and functions
Object Attributes: none].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*an administrator may access security management data and functions if the user is assigned to a role that permits access*].

[7] Security Identifier

[8] Access Control List

[9] User Identifier

[10] Group Identifier

[11] Portable Operating System Interface

[12] Discretionary Access Control List

[13] Access Control Entry

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

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

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

Hierarchical to: No other components.

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

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

Subjects: SMB, NFS and HDFS Users
Subject Attributes: Groupnet, IP[14] Address
Objects: Files, Directories
Object Attributes: Access Zone].

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

A user can access files and directories in an Access Zone if the user:
1. belongs to a Groupnet assigned to the Access Zone;
2. is coming from an IP Address in the IP Address pool assigned to the Access Zone; and
3. has permission to access the object in accordance with the Data Path SFP].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

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

6.2.3.7 FDP_RET_EXT.1 Retention of data

Hierarchical to: No other components.

Dependencies: FPT_STM.1

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

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

6.2.3.8 FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all objects, based on the following attributes: [*Forward Error Correction (FEC) codes*].

[14] Internet Protocol

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

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*viewing of node status, events, cluster details, capacity, IP and MAC[15] addresses, throughput, and drive status*] on behalf of the user to be performed before the user is authenticated.

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

6.2.4.2 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*authentication provider configuration*].

6.2.4.3 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6.2.5 Security Management (FMT)

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

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*Data Access SFP*] to restrict the ability to [change_default, query, modify, delete] the security attributes [*ACL,*

[15] Media Access Control

POSIX mode bits] to [*users in the SystemAdmin or SecurityAdmin role*, *or in a custom role with appropriate permissions*].

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

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*Role Based Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*role*] to [*users in the SecurityAdmin role*, *or in a custom role with appropriate permissions*].

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

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*Access Zone SFP*] to restrict the ability to [query, modify, delete,] the security attributes [*Groupnet, Access Zone*] to [*users in the SecurityAdmin role*, *or in a custom role with appropriate permissions*].

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

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Data Access SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*the file owner*] to specify alternative initial values to override the default values when an object or information is created.

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

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Role Based Access Control SFP*] to provide [selection, choose one of: restrictive] default values for security attributes that are used to enforce the SFP.

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

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

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Access Zone SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

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

6.2.5.7 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*view audit information, configure SmartLock retention periods, configure users and roles, configure authentication providers, configure service access, configure SyncIQ data replication, configure access banners*].

6.2.5.8 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 **administrative** roles [*SecurityAdmin, SystemAdmin, AuditAdmin and custom roles*].

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

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.6.2 FPT_RCV.3 Automated recovery without undue loss

Hierarchical to: FPT_RCV.2 Automated recovery

Dependencies: AGD_OPE.1 Operational user guidance

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

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

FPT_RCV.3.3 The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [*no losses*] for loss of TSF data or objects under the control of the TSF.

FPT_RCV.3.4 The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.

6.2.6.3 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.

6.2.6.4 FPT_TRC.1 Internal TSF consistency

Hierarchical to: No other components.

Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [*changes to the cluster data*].

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.2.7.2 FTA_SAC_EXT.1 Service Access

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.8 Trusted Path/Channels (FTP)

6.2.8.1 FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

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

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

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 14.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests (ATE)	ATE_COV.1	Evidence of coverage

Assurance Class	Assurance Components	
	Identifier	**Name**
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 14 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

The following Table provides a mapping between the SFRs and Security Objectives.

	O.ACCESS	O.ADMIN	O.AUDIT	O.BANNER	O.CRYPTO	O.IDENAUTH	O.INTEGRITY	O.PROTECT	O.RETAIN	O.SECURE	O.TIME
FAU_GEN.1			X								
FAU_SAR.1			X								
FCS_CKM.1					X						
FCS_CKM.4					X						
FCS_COP.1(1)					X						
FCS_COP.1(2)					X						
FDP_ACC.1(1)	X										
FDP_ACC.1(2)	X	X									
FDP_ACC.1(3)	X										
FDP_ACF.1(1)	X										
FDP_ACF.1(2)	X	X									
FDP_ACF.1(3)	X										
FDP_RET_EXT.1									X		
FDP_SDI.2							X				

	O.ACCESS	O.ADMIN	O.AUDIT	O.BANNER	O.CRYPTO	O.IDENAUTH	O.INTEGRITY	O.PROTECT	O.RETAIN	O.SECURE	O.TIME
FIA_UAU.1						X					
FIA_UAU.5						X					
FIA_UID.1						X					
FMT_MSA.1(1)		X									
FMT_MSA.1(2)		X									
FMT_MSA.1(3)		X									
FMT_MSA.3(1)		X									
FMT_MSA.3(2)		X									
FMT_MSA.3(3)		X									
FMT_SMF.1		X									
FMT_SMR.1		X									
FPT_ITT.1							X				
FPT_RCV.3							X				
FPT_STM.1											X
FPT_TRC.1							X				
FTA_TAB.1				X							
FTA_SAC_EXT.1								X			
FTP_TRP.1										X	

Table 15 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: O.ACCESS	The TOE must restrict access to the user data held by the TOE to only authorized data path users. The TOE must be able to restrict user access based on defined access zones.	
Security	FDP_ACC.1(1)	Subset access control (Data path)

Functional Requirements:	FDP_ACC.1(3)	Subset access control (Access Zones)
	FDP_ACF.1(1)	Security attribute based access control (Data path)
	FDP_ACF.1(3)	Security attribute based access control (Access Zones)
Rationale:	FDP_ACC.1(1) and FDP_ACF.1(1) ensure that user data is accessible only to authorized users. FDP_ACC.1(3) and FDP_ACF.1(3) ensure that access to user data is restricted based on access zones.	

Objective: **O.ADMIN**	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security functions provided by the TOE, and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	FDP_ACC.1(2)	Subset access control (RBAC)
	FDP_ACF.1(2)	Security attribute based access control (RBAC)
	FMT_MSA.1(1)	Management of security attributes (Data path)
	FMT_MSA.1(2)	Management of security attributes (RBAC)
	FMT_MSA.1(3)	Management of security attributes (Access Zones)
	FMT_MSA.3(1)	Static attribute initialisation (Data path)
	FMT_MSA.3(2)	Static attribute initialisation (RBAC)
	FMT_MSA.3(3)	Static attribute initialisation (Access Zones)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Rationale:	FMT_MSA.1(1), FMT_MSA.1(2) and FMT_MSA.1(3) control administrative access to the security attributes used to make access control decisions and provide the security management functionality to manage these attributes. FMT_MSA.3(1), FMT_MSA.3(2) and FMT_MSA.3(3) describe the default values for those attributes. FMT_SMF.1 provides the ability to administer other security management functions. FMT_SMR.1 provides the roles that are used to distinguish permissions for different users. FDP_ACC.1(2) and FDP_ACF.1(2) provide the Role Based Access Control policy used to control access to administrative functions.	

Objective: **O.AUDIT**	The TOE must record audit events for changes to the TOE configuration, and use of the TOE data channels. Audit records must be readable by authorized administrators.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
Rationale:	FAU_GEN.1 outlines what data must be included in audit records and what events must be audited. FAU_SAR.1 describes the function that allows these audit records to be viewed using the TOE.	

Objective: **O.BANNER**	The TOE must display an access warning to administrative users prior to login on the Web and CLI applications.	
Security Functional Requirements:	FTA_TAB.1	Default TOE access banners
Rationale:	FTA_TAB.1 describes the ability to display a message prior to user login on the web and CLI applications.	

Objective: **O.CRYPTO**	The TOE shall use validated cryptographic algorithms in support of cryptographic operations.	
Security Functional Requirements:	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key Destruction
	FCS_COP.1(1)	Cryptographic operation (TOE Management)
	FCS_COP.1(2)	Cryptographic operation (Data at rest encryption)
Rationale:	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1(1) describe the use of validated algorithms for the protection of data in transit. FCS_COP.1(2) describes the use of a validated algorithm for the protection of data at rest.	

Objective: **O.IDENTAUTH**	The TOE must ensure that users are identified and authenticated prior to allowing access to the administrative functions and data of the TOE. Multiple authentication mechanisms must be supported by the TOE.	
Security	FIA_UAU.1	Timing of authentication

Functional Requirements:	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification
Rationale:	FIA_UID.1 and FIA_UAU.1 require the identification and authentication of administrative users prior to being granted access to TOE management functionality (other than cluster identification and status). FIA_UAU.5 requires multiple authentication mechanisms.	

Objective: O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to data corruption, or disk or node failure.	
Security Functional Requirements:	FDP_SDI.2	Stored data integrity monitoring and action
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RCV.3	Automated recovery without undue loss
	FPT_TRC.1	Internal TSF Consistency
Rationale:	FDP_SDI.2 describes the ability to correct integrity errors. FPT_RCV.3 describes the ability to recover from disk or node failures. FPT_ITT.1 ensures that data integrity is maintained during replication, and FPT_TRC.1 ensures that the consistency is maintained when the nodes become disconnected.	

Objective: O.PROTECT	The TOE must provide a means of disabling access to unused TOE services.	
Security Functional Requirements:	FTA_SAC_EXT.1	Service Access
Rationale:	FTA_SAC_EXT.1 requires the ability to disable unused services.	

Objective: O.RETAIN	The TOE must prevent the deletion of data prior to expiry of the assigned retention period.	
Security Functional Requirements:	FDP_RET_EXT.1	Retention of data
Rationale:	FDP_RET_EXT.1 describes the TOE's ability to enforce a retention period during which data may not be deleted.	

Objective: **O.SECURE**	The TOE must ensure the confidentiality and integrity of interactive administrative sessions.	
Security Functional Requirements:	FTP_TRP.1	Trusted path
Rationale:	FTP_TRP.1 describes the protection provided to the communications link used for remote administration of the TOE.	

Objective: **O.TIME**	The TOE must provide reliable timestamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 requires the availability of reliable timestamps.	

6.4.3 Dependency Rationale

Table 16 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1(1)
	FCS_CKM.4	✓	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1
FCS_COP.1(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1
	FCS_CKM.4	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FCS_COP.1(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by OE.CRYPTO in the operational environment
	FCS_CKM.4	✓	Satisfied by OE.CRYPTO in the operational environment
FDP_ACC.1(1)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(1)
FDP_ACC.1(2)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(2)
FDP_ACC.1(3)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(3)
FDP_ACF.1(1)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(1)
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(1)
FDP_ACF.1(2)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(2)
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(2)
FDP_ACF.1(3)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(3)
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(3)
FDP_RET_EXT.1	FPT_STM.1	✓	
FDP_SDI.2	None	N/A	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.5	None	N/A	
FIA_UID.1	None	N/A	
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(1)
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(2)
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(3)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(3)
	FMT_SMR.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
	FMT_SMF.1	✓	
FMT_MSA.3(1)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(1)
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(2)
	FMT_SMR.1	✓	
FMT_MSA.3(3)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(3)
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	
FPT_ITT.1	None	N/A	
FPT_RCV.3	AGD_OPE.1	✓	
FPT_STM.1	None	N/A	
FPT_TRC.1	FPT_ITT.1	✓	
FTA_TAB.1	None	N/A	
FTA_SAC_EXT.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 16 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.2 augmentation since current practices and procedures exceed the minimum requirements for EAL 2.

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 SECURITY AUDIT

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

Platform Application Programming Interface (PAPI) logs, which must be explicitly enabled, record user activities and start up and shutdown functions. PAPI auditing tracks and records all configuration events that are handled by the OneFS Platform API. The process involves auditing the CLI, web administration interface, and OneFS APIs. System configuration auditing events are stored in the config audit topic directories.

Protocol auditing tracks and stores activity performed through SMB, NFS, and HDFS protocol connections. When protocol auditing is enabled for an access zone, file access events through the SMB, NFS, and HDFS protocols are recorded in the protocol audit topic directories. The audit events are logged on the individual nodes where the SMB, NFS, or HDFS client initiated the activity. The events are then stored in a binary file under /ifs/.ifsvar/audit/logs.

The audit logs include security relevant information including date and time of the event, type of event and the identity of the user causing the event, where applicable.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_SAR.1.

7.2 CRYPTOGRAPHIC SUPPORT

7.2.1 Data in Transit

Cryptographic protection of data in transit in support of the management interfaces is provided by OpenSSL FIPS Object Module software version 2.0.8 (Cryptographic Module Validation Program (CMVP) certificate number 1747) libraries. These libraries provide support for TLS 1.1 and TLS 1.2 for the WebUI and PAPI applications, and for Secure Shell (SSH) for the CLI. The algorithms supported are noted in Table 12.

The vendor affirms that no source code changes were made to the cryptographic module prior to recompilation into the TOE software.

TOE Security Functional Requirements addressed: FCS_CKM.1, FCS_CKM.4, FCS_COP.1(1).

7.2.2 Data at Rest

Data at rest encryption is provided by self-encrypting drives within the Isilon hardware. These are the Seagate Secure® TCG Self-Encrypting Enterprise drives. The cryptographic functions provided by these drives are FIPS 140-2

Level 2 validated under CMVP certificate number 2317. The drives provide 256 bit AES symmetric encryption, as well as key generation and destruction functions to support this activity.

TOE Security Functional Requirements addressed: FCS_CKM.1, FCS_CKM.4, FCS_COP.1(2).

7.3 USER DATA PROTECTION

This is a description of how the TOE meets the security objectives.

7.3.1 Data Path

OneFS supports two types of permissions data on files and directories that control who has access: Windows-style access control lists (ACLs) and POSIX mode bits (UNIX permissions). Global policy settings can be configured to customize default ACL and UNIX permissions to best support the environment.

The OneFS file system installs with UNIX permissions as the default. An administrator can give a file or directory an ACL by using Windows Explorer or OneFS administrative tools. Typically, files created over SMB or in a directory that has an ACL, receive an ACL. If a file receives an ACL, OneFS stops enforcing the file's mode bits; the mode bits are provided for only protocol compatibility, not for access control.

7.3.1.1 UNIX permissions

In a UNIX environment, file and directory access is controlled by POSIX mode bits, which grant read, write, or execute permissions to the owning user, the owning group, and everyone else.

OneFS supports the standard UNIX tools for viewing and changing permissions: `ls`, `chmod`, and `chown`.

All files contain 16 permission bits, which provide information about the file or directory type and the permissions. The lower 9 bits are grouped as three 3-bit sets, called triples, which contain the read, write, and execute (rwx) permissions for each class of users—owner, group, and other. Permissions flags can be set to grant permissions to each of these classes.

Unless the user is root, OneFS checks the class to determine whether to grant or deny access to the file. The classes are not cumulative: The first class matched is applied.

7.3.1.2 Windows ACLs

In Windows environments, file and directory permissions, referred to as access rights, are defined in access control lists (ACLs). ACLs are more complex than mode bits, and therefore can be used to express much more granular sets of access rules. OneFS checks the ACL processing rules commonly associated with Windows ACLs.

A Windows ACL contains zero or more access control entries (ACEs), each of which represents the SID of a user or a group as a trustee. In OneFS, an ACL

can contain ACEs with a UID, GID, or SID as the trustee. Each ACE contains a set of rights that allow or deny access to a file or folder. An ACE can optionally contain an inheritance flag to specify whether the ACE should be inherited by child folders and files.

Instead of the standard three permissions available for mode bits, ACLs have 32 bits of fine-grained access rights. Of these, the upper 16 bits are general and apply to all object types. The lower 16 bits vary between files and directories but are defined in a way that allows most applications to apply the same bits for files and directories.

Rights grant or deny access for a given trustee. User access can be blocked explicitly through a deny ACE or implicitly by ensuring that a user does not directly, or indirectly through a group, appear in an ACE that grants the right.

TOE Security Functional Requirements addressed: FDP_ACC.1(1), FDP_ACF.1(1).

7.3.2 Role Based Access Control

Role based access control (RBAC) is used to grant the right to perform particular administrative actions to authenticated users. Roles are created by a Security Administrator, assigned privileges, and then assigned members. There are three built-in roles relevant to the security claims[16]: SecurityAdmin, SystemAdmin, and AuditAdmin. Administrators with sufficient privileges are also able to create new roles, with a customized set of privileges. During installation, a root user account is created with the privileges of all roles.

Only the root user and users in administrative roles can log in to the WebUI, PAPI applications or the CLI. Using roles, the root and admin users can assign others to built-in or custom roles that have login and administrative privileges to perform specific administrative tasks. Table 17 provides a general description of the privileges associated with the built-in roles.

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

[16] Additional built-in roles exist, but cannot be used to demonstrate claimed security functionality, and are therefore not included here.

Role	Privileges
AuditAdmin	The AuditAdmin role has the required privileges to view all system configuration settings.

Table 17 – Roles and Privileges

TOE Security Functional Requirements addressed: FDP_ACC.1(2), FDP_ACF.1(2).

7.3.3 Access Zones

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

When an Access Zone is created, it is associated with a base directory (e.g. /ifs/Department A), assigned a Groupnet and is assigned an authentication provider. A Groupnet is a logical container that includes subnets, IP address pools and provisioning rules. In the evaluated configuration, an authentication provider is a specific instance of AD. The Access Zone is then associated with an IP address pool. Clients can connect to this zone only when coming from IP addresses in this pool.

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

TOE Security Functional Requirements addressed: FDP_ACC.1(3), FDP_ACF.1(3).

7.3.4 Data Retention

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

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

TOE Security Functional Requirements addressed: FDP_RET_EXT.1.

7.3.5 Data Integrity Monitoring and Correction

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

TOE Security Functional Requirements addressed: FDP_SDI.2.

7.4 IDENTIFICATION AND AUTHENTICATION

Prior to identification and authentication, administrators have no access to TOE data or functionality through the WebUI, CLI or PAPI interfaces. The only access to TOE data prior to login is through the front panel, which requires physical access to the TOE hardware. From the Liquid Crystal Display (LCD) screen front panel, administrators may view node status, events, cluster details, capacity, IP and MAC addresses, throughput, and drive status.

In the evaluated configuration, both local authentication and AD authentication are supported for administrative users. Isilon ensures that administrative users are authenticated by the configured authentication provided for that user account prior to allowing access to TOE data and functions.

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

7.5 SECURITY MANAGEMENT

The Isilon cluster can be managed through the WebUI, the CLI or a PAPI application.

Table 18 shows the security management privileges associated with the built-in roles. Security management privileges can be associated with custom roles in combinations determined by a user with the SecurityAdmin role.

Role	Privileges
SecurityAdmin	view audit information configure users and roles configure authentication providers configure SyncIQ data replication configure access banners
SystemAdmin	view audit information configure SmartLock retention periods configure SyncIQ data replication configure access banners

Role	Privileges
AuditAdmin	view audit information configure SmartLock retention periods (read-only) configure SyncIQ data replication (read-only)

Table 18 – Security Management Privileges

TOE Security Functional Requirements addressed: FMT_SMF.1, FMT_SMR.1.

7.5.1 Data Path

For the Data Access SFP, the subject attributes are provided by the operating system, and cannot be modified using Isilon administrative functions. The default values for the object attributes are the ACL or POSIX mode bits on the file or directory. Isilon administrators in the SystemAdmin or SecurityAdmin role may change the default value, query, modify and delete these attributes. The default value of these attributes may be considered to be permissive, in that the file owner is able to determine their values. The file owner may also change the default values. Default values may be determined by the directory in which the object is created.

Modification of Data Access attributes by Isilon administrators is performed using the CLI.

TOE Security Functional Requirements addressed: FMT_MSA.1(1), FMT_MSA.3(1).

7.5.2 Role Based Access Control

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

TOE Security Functional Requirements addressed: FMT_MSA.1(2), FMT_MSA.3(2).

7.5.3 Access Zones

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

TOE Security Functional Requirements addressed: FMT_MSA.1(3), FMT_MSA.3(3).

7.6 PROTECTION OF THE TSF

7.6.1 Automated Recovery

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

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

In the case of a component failure, a constant, secure state is maintained where the Isilon cluster continues to respond to requests to read and write data. Under normal operating conditions, all data on the cluster is protected against one or more failures of a node or drive. However, if a node or drive fails, the cluster protection status is considered to be in a degraded state until the data is protected by 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.

TOE Security Functional Requirements addressed: FPT_RCV.3.

7.6.2 Timestamps

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

TOE Security Functional Requirements addressed: FPT_STM.1.

7.6.3 Replication

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

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

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

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

TOE Security Functional Requirements addressed: FPT_ITT.1, FPT_TRC.1.

7.7 TOE ACCESS

7.7.1 Access Banner

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

TOE Security Functional Requirements addressed: FTA_TAB.1.

7.7.2 Service Access

Unused services can be disabled. Disabling is performed on a protocol by protocol basis. The protocols that can be enabled or disabled, and their defaults are shown in Table 19.

Protocol	Default
FTP	Disabled by default
HDFS	Enabled by default
HTTP	Enabled by default, but disabled in the evaluated configuration
NFS	Enabled by default

Protocol	Default
SMB	Enabled by default
SNMP	Enabled by default, but disabled in the evaluated configuration
Swift	Enabled by default, but disabled in the evaluated configuration

Table 19 – Service Access

TOE Security Functional Requirements addressed: FTA_SAC_EXT.1.

7.8 TRUSTED PATH / CHANNELS

When the WebUI, PAPI or SSH interface is used, the connection between the Isilon node and the remote administrator's browser is protected from modification and disclosure using TLS. This connection is logically distinct from other communication channels. The Isilon end point is identified by the user when attempting to access the node, and the user is authenticated prior to being granted access to security management functions.

TOE Security Functional Requirements addressed: FTP_TRP.1.

8 ACRONYMS

8.1 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ACE	Access Control Entry
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
DACL	Discretionary Access Control List
EAL	Evaluation Assurance Level
FEC	Forward Error Correction
FIPS	Federal Information Processing Standards
GID	Group Identifier
GUI	Graphical User Interface
HDFS	Hadoop Distributed File System
HMAC	Hash Message Authentication Code
IP	Internet Protocol
IT	Information Technology
LCD	Liquid Crystal Display
MAC	Media Access Control
NFS	Network File System
OSP	Organizational Security Policy
PAPI	Platform Application Programming Interface
POSIX	Portable Operating System Interface
PP	Protection Profile

Acronym	Definition
RBAC	Role Based Access Control
RSA	Rivest, Shamir and Adleman
SED	Self-encrypting drive
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SID	Security Identifier
SMB	Server Message Block
SP	Special Publication
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UID	User Identifier
WebUI	Web User Interface
WORM	Write Once, Read Many

Table 20 – Acronyms