Dell EMC™ Unity® OE v4.2

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2009-000-D102
Version: 1.4
20 July 2017

EMC Corporation
176 South Street
Hopkinton, MA, USA
01748

Prepared by:
EWA-Canada
1223 Michael Street, 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 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 Target of Evaluation (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 (ST) reference, the Target of Evaluation (TOE) 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 any extended components.

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

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

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

1.2 SECURITY TARGET REFERENCE

ST Title:	Dell EMC™ Unity® OE v4.2 Security Target
ST Version:	1.4
ST Date:	20 July 2017

1.3 TOE REFERENCE

TOE Identification: Dell EMC™ Unity™ OE 4.2.0.9392909 with Unity 300/350F, 400/450F, 500/550F or 600/650F hardware

TOE Developer: Dell EMC

TOE Type: Data Storage (Other Devices and Systems)

1.4 TOE OVERVIEW

The TOE is a midrange capacity storage system comprised of the Unity hardware platform and the Unity Operating Environment (OE) software.

The Unity hardware houses the disks in the storage array which are managed by the storage processors. It provides Network Access Server (NAS) and Storage Area Network (SAN) services by interfacing with the front-end clients (application hosts) and the back-end storage disks.

Application hosts (such as database servers, file servers, etc.) can access the Unity storage through traditional block and file protocols. The TOE presents storage to application hosts as a standard network-based virtual file server, or in the form of Logical Units (LUNs) to block-based client machines.

Unity supports the following storage protocols:

- File Storage Protocols
  - Common Internet File System (CIFS) / Server Message Block (SMB)
  - Network File System (NFS)

- Block Storage Protocols
  - Internet Small Computer System Interface (iSCSI)
  - Fibre Channel (FC)

Each LUN is a useable storage system volume that the TOE can expose to individual hosts. Application hosts can only access LUNs for which permission has been granted by an authorized administrator.

Each File-based NAS server on the TOE can be configured to interface with a Lightweight Directory Access Protocol (LDAP) or Network Information Service (NIS) server. When a request for data access is made from a File-based client machine, the TOE checks the Access Control List (ACL) of the requested file or directory, and either grants or denies access to the user.

The TOE is managed by authorized administrators through the Unified Element Management Command Line Interface (UEMCLI) (also known as the Unisphere CLI) and the Unisphere Graphical User Interface (GUI). Administrators are assigned a user role that provides them with access to specific TOE features and functions.

The UEMCLI is a command line interface that provides access to common functions for monitoring and managing the TOE. The UEMCLI provides access to functions for storage provisioning, status and configuration information retrieval, and other TOE administrative functions. The Unisphere GUI is an HTML5

application that runs within a web browser. To access the functions available via Unisphere, an authorized administrator must open a web browser and enter the Internet Protocol (IP) address or hostname of the Unity management port.

The TOE is a combined software and hardware TOE. The Unity hardware consists of a disk processor enclosure (DPE) that contains two storage processors (SPs) and houses either 12 or 25 disk drives. It may also include one or more optional disk-array enclosures (DAEs) containing additional disk drives. The DAEs are available in a 15 drive, 3.5-inch disk 3-unit (3U) enclosure or a 25 drive, 2.5-inch disk 2-unit (2U) enclosure.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE is a stand-alone appliance consisting of the Unity hardware and the Unity OE software. The 25 Disk Processor Enclosure (DPE) hardware model will be used for the purpose of this evaluation. Figure 1 represents the TOE in its evaluated configuration:

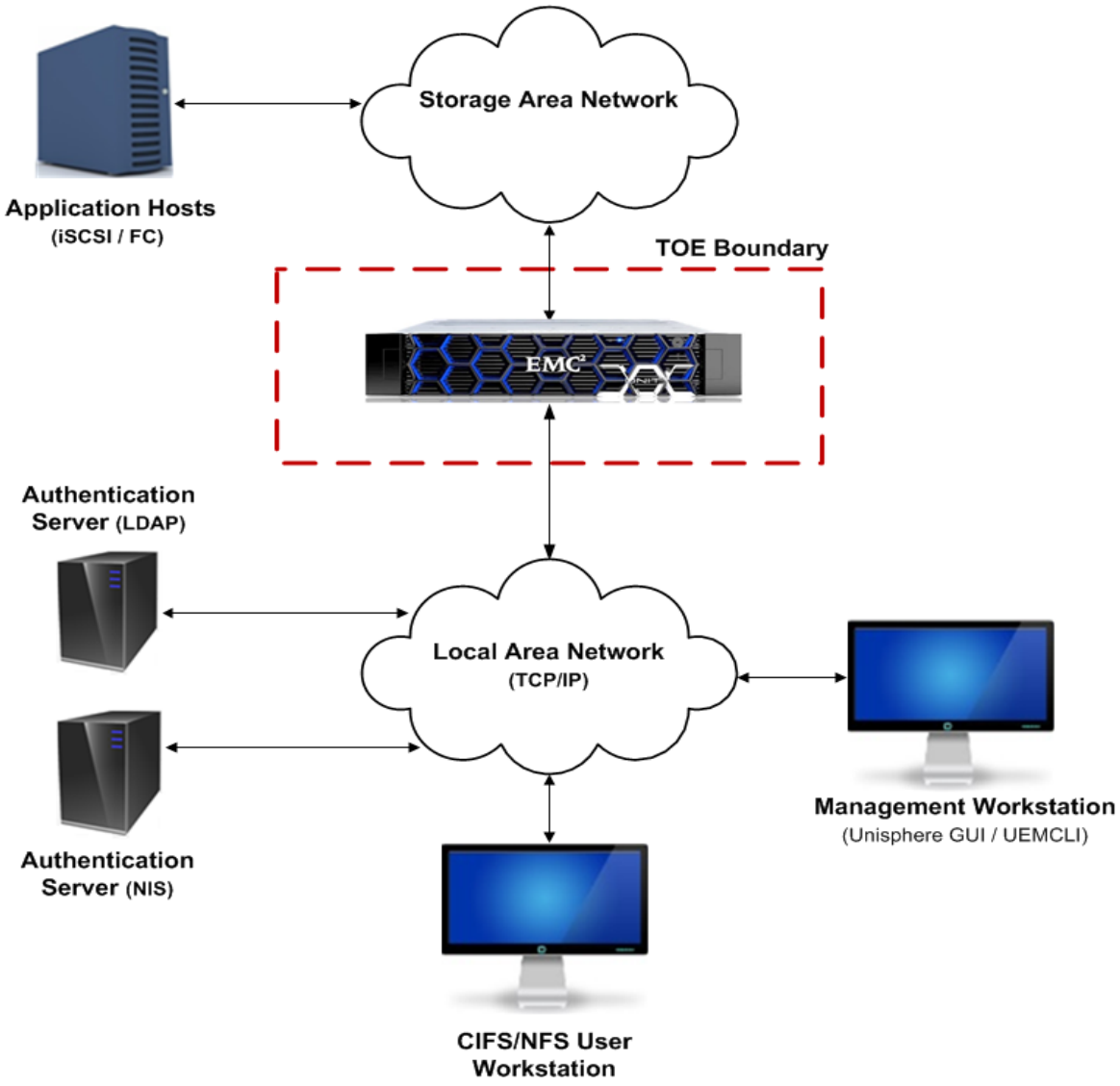

Figure 1 - TOE Boundary

1.5.2 TOE Components

The following hardware and software make up the TOE.

TOE Component	Description
Hardware	• Unity 300 and Unity 350F • Unity 400 and Unity 450F • Unity 500 and Unity 550F • Unity 600 and Unity 650F

TOE Component	Description
Software	Unity Operating Environment (OE) 4.2.0.9392909
	Unisphere 4.2.0.9392909
	Unisphere CLI version 4.2.0.1.1786

Table 1 – TOE Hardware and Software

1.5.3 TOE Environment

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

Non-TOE Component	Requirements	Description
Management	General purpose computing platform with: • Microsoft Windows Server 2008 R2 SP1 operating system • Adobe Flash Player v18 • Mozilla Firefox (minimum v44) • PuTTY 0.6	Provides TOE management functions to administrators via the Unisphere Command Line Interface (CLI) and/or the Unisphere Graphical User Interface (GUI).
Active Directory Server	General purpose computing platform that supports Windows Server 2012 R2, including Microsoft Active Directory.	Provides the TOE with authentication services for administrators and CIFS/SMB file shares.
NIS Server	General purpose computing platform that supports NFSv3, NFSv4.0, or NFSv4.1	Provides the TOE with authentication services for NFS file shares.
Application Hosts	General purpose computing platform that supports Internet Small Computer Systems Interface (iSCSI) and Fibre Channel (FC) connectivity	Application servers are able to access data from the storage area network (SAN)

Table 2 – Non-TOE Hardware and Software

1.5.4 TOE Guidance

The TOE includes the following guidance documentation:

- Dell EMC Unity: Introduction to the Unity Platform, A Detailed Review

- Dell EMC Unity: Best Practices Guide, Best Practices for Performance and Availability UnityOE v4.2
- Dell EMC Unity™ Family, Dell EMC Unity All Flash, Unity Hybrid, UnityVSA Security Configuration Guide
- Dell EMC Unity™ Family, Version 4.2 Unisphere® Command Line Interface User Guide
- Dell EMC Unity™ Family, Dell EMC Unity All Flash, and Unity Hybrid Hardware Information Guide
- Dell EMC Unity™ Family, EMC Unity All Flash, and Unity Hybrid Installation Guide
- EMC Unity™ Quick Start Guide
- Unisphere® Online Help

1.5.5 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. The following breakdown also provides the description of the security features of the TOE and follows the security functional classes described in Section 6.

Functional Classes	Description
Security Audit	The TOE generates audit records for administrator login attempts and changes to the TOE configuration.
User Data Protection	The TOE only allows authorized application servers access to stored user data. The integrity of stored data is protected using RAID technology.
Identification and Authentication	TOE administrators must identify and authenticate prior to gaining access to the TOE management functionality.
Security Management	The TOE provides management capabilities via a web-based GUI and a CLI. Management functions allow authorized administrators to configure system access and storage settings.
Protection of the TSF	The TOE provides reliable time stamps for auditable events.

Table 3 – Logical Scope of the TOE

1.5.6 Functionality Excluded from the Evaluated Configuration

1.5.6.1 Excluded TOE Features

The following TOE features are supported but not included in this evaluation:

- Data at Rest Encryption (D@RE) – encrypts data as it is written to disk
- Common Event Enabler (CEE)
- File-level retention
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Transfer Protocol (SNMP)
- Replication
- Network Data Management Protocol (NDMP)
- Common Anti-Virus Agent (CAVA)
- EMC Secure Remote Services support (ESRS)

1.5.6.2 Excluded TOE Interfaces

The following TOE interfaces are supported but not included in this evaluation:

- Representational State Transfer (REST) Interface
- Storage Management Initiative Specification (SMI-S) Interface
- vStorage APIs for Storage Awareness (VASA) Interface
- Storage Processor (SP) Ethernet Service Port connection
- Unity Service Secure Shell (SSH) Interface

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-2012-09-001, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

As follows:

- CC Part 2 conformant
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 [CEM] has to be taken into account.

2.2 ASSURANCE PACKAGE CLAIM

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

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

The TOE for this ST does not claim conformance with any Protection Profile (PP).

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 4 lists the threats addressed by the TOE. Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Potential threat agents are authorized TOE users, and unauthorized persons. 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 level of skill commensurate with their responsibilities. 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.

Threat	Description
T.ACCESS	Access to user data could be improperly granted to application hosts which should not have access to it, and users with access to those hosts.
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.UNAUTH	A hostile/unauthorized user could gain access to stored data by bypassing the protection mechanisms of the TOE.
T.UNDETECT	Authorized or unauthorized 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.

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 OSP that is presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

Organizational Security Policy	Description
P.RAID	User data must be protected from loss due to disk failure.

Table 5 – Organizational Security Policy

3.3 ASSUMPTIONS

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

Assumptions	Description
A.ATTRIBUTE	The attributes used by the TOE to make File Storage Access Control decisions are provided by the operational environment.
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NOEVIL	The authorized 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.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.AUDIT	The TOE must provide a means of logging security related events.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and TSF data.
O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to disk failure.
O.PROTECT	The TOE must protect the data that it has been entrusted to store from unauthorized access.

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 domain or by non-technical or procedural means.

Security Objective	Description
OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to the enforcement of security are protected from any physical attack.
OE.SERVER	The operational environment shall provide an Active Directory server and a NIS server for maintaining access control security attributes for file-based storage on the TOE. Files support Unix-style Access Control Lists (ACLs) or NT-style Discretionary Access Control Lists (DACLs) as appropriate.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following Table maps the security objectives to the assumptions and threats identified for the TOE.

	T.ACCESS	T.ACCOUNT	T.UNAUTH	T.UNDETECT	P.RAID	A.ATTRIBUTE	A.LOCATE	A.NOEVIL
O.ADMIN	X	X	X	X				
O.AUDIT				X				
O.IDAUTH		X	X	X				
O.INTEGRITY					X			
O.PROTECT	X							
OE.ADMIN							X	
OE.PHYSICAL								X
OE.SERVER						X		

Table 9 – Mapping Between Objectives, Threats, 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 and the Operational Environment back to the threats addressed by the TOE.

Threat: **T.ACCESS**	Access to user data could be improperly granted to application hosts which should not have access to it.	
Objectives:	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.PROTECT	The TOE must protect the data that it has been entrusted to store from unauthorized access.
Rationale:	O.ADMIN mitigates this threat by only allowing authorized administrators the ability to manage TOE access functions. O.PROTECT mitigates this threat by identifying application hosts by name before allowing access to protected data.	

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 must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and TSF data.
Rationale:	O.ADMIN mitigates this threat by ensuring that access to the security management functions of the TOE are restricted to authorized administrators. O.IDAUTH mitigates this threat by ensuring that all authorized administrators are identified and authenticated prior to gaining access to the TOE security management functions.	

Threat: **T.UNAUTH**	A hostile/unauthorized user could gain access to stored data by bypassing the protection mechanisms of the TOE.	
Objectives:	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and TSF data.
Rationale:	O.ADMIN mitigates this threat by providing authorized administrators the ability to manage TOE security functions. O.IDAUTH mitigates this threat by ensuring that all users are identified and authenticated prior to gaining access to the TOE security management functions.	

Threat: **T.UNDETECT**	Authorized or unauthorized 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.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.AUDIT	The TOE must provide a means of logging security related events.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and TSF data.
Rationale:	O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized administrators. O.AUDIT counters this threat by ensuring that the TOE tracks all management actions taken against the TOE. O.IDAUTH mitigates this threat by ensuring that all authorized administrators are identified and authenticated prior to gaining access to the TOE security management functions.	

4.3.2 Security Objectives Rationale Related to OSPs

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

Policy: **P.RAID**	User data must be protected from loss due to disk failure.	
Objectives:	O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to disk failure.
Rationale:	O.INTEGRITY supports this policy by ensuring that the TOE provides the ability to protect data in the case of disk failure.	

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.ATTRIBUTE**	The attributes used by the TOE to make File Storage Access Control decisions are provided by the operational environment.	
Objectives:	OE.SERVER	The operational environment shall provide an Active Directory server and a NIS server for maintaining access control security attributes for file-based storage on the TOE. Files support Unix-style Access Control Lists (ACLs) or NT-style Discretionary Access Control Lists (DACLs) as appropriate.
Rationale:	OE.SERVER supports this assumption by providing the attributes required by the TOE to make access control decisions for File-based storage.	

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 the enforcement of security are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	

Assumption: **A.NOEVIL**	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

Objectives:	OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
Rationale:	OE.ADMIN supports this assumption by ensuring that the administrators managing the TOE have been specifically chosen to be careful, attentive and non-hostile.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This ST does not include extended Security Functional Requirements.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

This section 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 (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC:

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (Block Storage)
	FDP_ACC.1(2)	Subset access control (File Storage)
	FDP_ACF.1(1)	Security attribute based access control (Block Storage)
	FDP_ACF.1(2)	Security attribute based access control (File Storage)
	FDP_SDI.2	Stored data integrity monitoring and action

Class	Identifier	Name
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1(1)	Management of security attributes (Block Storage)
	FMT_MSA.1(2)	Management of security attributes (File Storage)
	FMT_MSA.3(1)	Static attribute initialisation (Block Storage)
	FMT_MSA.3(2)	Static attribute initialisation (File Storage)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps

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) [*Administrator login attempts, the following administrator actions that result in a configuration change to the storage array:*

- *adding, modifying, or deleting LUNs*
- *adding, modifying, or deleting CIFS shares*
- *adding, modifying, or deleting SMB shares*
- *adding, modifying, or deleting NFS mounts*
- *changes to host access permissions*].

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 [*authorised administrators*] 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 User Data Protection (FDP)

6.2.2.1 FDP_ACC.1(1) Subset access control (Block Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1(1) Security attribute based access control (Block Storage)

FDP_ACC.1.1(1) The TSF shall enforce the [*Block Storage Access Control SFP*] on

[S*ubjects: Hosts (application servers);*

Objects: LUNs;

Operations: Read and write].

6.2.2.2 FDP_ACC.1(2) Subset access control (File Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1(2) Security attribute based access control (File Storage)

FDP_ACC.1.1(2) The TSF shall enforce the [*File Storage Access Control SFP*] on

[S*ubjects: Users (accessing storage from client machines);*

Objects: CIFS and SMB shares, and NFS mounts;

Operations: Read, Write, Execute].

6.2.2.3 FDP_ACF.1(1) Security attribute based access control (Block Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1(1) Subset access control (Block Storage)

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(1) The TSF shall enforce the [*Block Storage Access Control SFP*] to objects based on the following:

[S*ubjects: Hosts (application servers)*

Security Attributes:

1) *iSCSI Qualified Name (IQN)*
2) *World Wide Name (WWN)*

Objects: LUNs

Security Attributes:

1) *IQN access list*
2) *WWN access list*].

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[*A valid subject of the TOE is allowed to read and write to TOE storage if the IQN or WWN of the subject is included in the list of hosts that have access to the LUN*].

FDP_ACF.1.3(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

6.2.2.4 FDP_ACF.1(2) Security attribute based access control (File Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1(2) Subset access control (File Storage)
FMT_MSA.3(2) Static attribute initialisation

FDP_ACF.1.1(2) The TSF shall enforce the [*File Storage Access Control SFP*] to objects based on the following:

[S*ubjects: Users (accessing storage from client machines)*

Security Attributes:

1) *Username*
2) *Authentication status (success or failure)*
3) *IP address (for NFS access)*

Objects: File Shares

Security Attributes:

1) *NFS Mount permissions: Unix-style ACLs for each file and directory*
2) *CIFS and SMB Share Permissions: NT-style Discretionary Access Control Lists (DACLs) for each file and directory*].

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[*A successfully authenticated subject of the TOE is allowed to perform an operation if the content of the Access Control List (containing permissions) for the object authorizes the Subject to perform the desired operation*].

FDP_ACF.1.3(2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [

1. *For CIFS and SMB access, subjects that are members of the group Domain Administrators shall be authorized to backup, restore, and take ownership of all objects and control over the overall share permissions for the entire domain;*

2. *For NFS access, the user must access the NFS mount from a computer running an IP address listed in the allowed hosts configuration for the TOE;*
3. *For NFS access, subjects that are authorized as superusers (root) can perform all operations on all objects;*
4. *For root users accessing an NFS mount, access will be permitted if the host that the root user is using to connect to the NFS mount is listed under the 'trusted hosts' list in the TOE configuration*].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no other rules*].

6.2.2.5 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 **user data** ~~objects~~, based on the following attributes: [*parity data for RAID 5 and RAID 6; mirrored data for RAID 1/0*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*reconstruct the user data for RAID 5 and RAID 6; replace erroneous data with mirrored data for RAID 1/0; and log an alert*].

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual **Administrators** ~~users~~: [*UserID, password, role*].

Application Note: UserID, password and role information is maintained for Administrators using local authentication. When LDAP authentication is used, the Administrator's username and password are maintained by the Directory server and the Administrator's role is maintained by the TOE. The term 'Administrator' is used to refer to a user in the Operator, Storage Administrator or Administrator role.

6.2.3.2 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: User authentication applies to users accessing File-based storage on the TOE as well as administrators accessing management functions via the management interfaces.

6.2.3.3 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: User identification applies to users accessing File-based storage on the TOE as well as administrators accessing management functions via the management interfaces.

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MSA.1(1) Management of security attributes (Block Storage)

Hierarchical to: No other components.

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

FMT_MSA.1.1(1) The TSF shall enforce the [*Block Storage Access control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*WWN and IQN access lists*] to [*the Administrator and Storage Administrator roles*].

Application Note: The Block Storage Access Control SFP does not actually control access to the security attributes; rather, these attributes are used in the enforcement of the Block Storage Access Control SFP and are restricted by role-based access control.

6.2.4.2 FMT_MSA.1(2) Management of security attributes (File Storage)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1(2) Subset access control (File Storage) or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(2) The TSF shall enforce the [*File Storage Access control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*trusted hosts*] to [*the Administrator and Storage Administrator roles*].

Application Note: The File Storage Access Control SFP does not actually control access to the security attributes; rather, these attributes are used in the enforcement of the File Storage Access Control SFP and are restricted by role-based access control.

6.2.4.3 FMT_MSA.3(1) Static attribute initialisation (Block Storage)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes (Block Storage)

FMT_SMR.1 Security roles

FMT_MSA.3.1(1) The TSF shall enforce the [*Block Storage Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [*Administrator and Storage Administrator*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.4 FMT_MSA.3(2) Static attribute initialisation (File Storage)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1(2) Management of security attributes (File Storage)

FMT_SMR.1 Security roles

FMT_MSA.3.1(2) The TSF shall enforce the [*File Storage Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [*Administrator and Storage Administrator*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.5 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:

[

a) viewing administrative information;
b) administering the Block Storage Access Control SFP;
c) administering the File Storage Access Control SFP;
d) managing storage; and
e) managing user account information

].

6.2.4.6 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

[

- *Operator*
- *Storage Administrator*
- *Administrator*

].

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

6.2.5 Protection of the TSF (FPT)

6.2.5.1 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.

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The following table provides a mapping between the Security Functional Requirements (SFRs) and Security Objectives.

	O.ADMIN	O.AUDIT	O.IDAUTH	O.INTEGRITY	O.PROTECT
FAU_GEN.1		X			
FAU_SAR.1		X			
FDP_ACC.1(1)					X
FDP_ACC.1(2)					X
FDP_ACF.1(1)					X
FDP_ACF.1(2)					X
FDP_SDI.2				X	
FIA_ATD.1	X		X		
FIA_UAU.2	X		X		X
FIA_UID.2	X		X		X
FMT_MSA.1(1)	X				X
FMT_MSA.1(2)	X				X
FMT_MSA.3(1)	X				X
FMT_MSA.3(2)	X				X
FMT_SMF.1	X				X
FMT_SMR.1	X				
FPT_STM.1		X			

Table 11 – Mapping of SFRs to Security Objectives

6.3.1 SFR Rationale Related to Security Objectives

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

Objective: **O.ADMIN**	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	
Security Functional Requirements:	FDP_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_MSA.1(1)	Management of security attributes (Block Storage)
	FMT_MSA.1(2)	Management of security attributes (File Storage)
	FMT_MSA.3(1)	Static attribute initialisation (Block Storage)
	FMT_MSA.3(2)	Static attribute initialisation (File Storage)
	FMT_SMF.1	Management of TSF data
	FMT_SMR.1	Security roles
Rationale:	FDP_ATD.1 supports this objective by ensuring that the TOE maintains security attributes for administrative users. FDP_UAU.2 and FDP_UID.2 support this objective by ensuring that only authorized administrators have access to TOE functions and data. FMT_MSA.1(1) and FMT_MSA.3(1) support this objective by identifying the management restrictions of the Block Storage Access Control SFP. FMT_MSA.1(2) and FMT_MSA.3(1) support this objective by identifying the management restrictions of the File Storage Access Control SFP. FMT_SMF.1 meets this objective by ensuring that the management functions are utilized to securely manage the TOE. FMT_SMR.1 supports this objective by ensuring that specific roles are defined to govern management of the TOE.	

Objective: **O.AUDIT**	The TOE must provide a means of logging security related events.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FPT_STM.1	Reliable time stamps
Rationale:	FAU_GEN.1 supports this objective by generating records for	

	auditable events. FAU_SAR.1 supports this objective by ensuring that the TOE provides the ability to review the audit trail. FPT_STM.1 ensures that a time stamp is provided for each auditable event.

Objective: **O.IDAUTH**	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and TSF data.	
Security Functional Requirements:	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Rationale:	FIA_ATD.1 supports this objective by ensuring that the TOE maintains security attributes for administrative users. FIA_UAU.2 meets this objective by ensuring that TOE Administrators are successfully authenticated before gaining access to TOE functions and data. FIA_UID.2 supports this objective by ensuring that the identity of each TOE Administrator is known before allowing access to TOE functions and data.	

Objective: **O.INTEGRITY**	The TOE must protect the data that it has been entrusted to store from integrity errors due to disk failure.	
Security Functional Requirements:	FDP_SDI.2	Stored data integrity monitoring and action
Rationale:	FDP_SDI.2 meets this objective by providing the RAID functionality that protects against integrity errors due to a hardware fault.	

Objective: **O.PROTECT**	The TOE must protect the data that it has been entrusted to store from unauthorized access.	
Security Functional Requirements:	FDP_ACC.1(1)	Subset access control (Block Storage)
	FDP_ACC.1(2)	Subset access control (File Storage)
	FDP_ACF.1(1)	Security attribute based access control (Block Storage)
	FDP_ACF.1(2)	Security attribute based access control (File

		Storage)
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_MSA.1(1)	Management of security attributes (Block Storage)
	FMT_MSA.1(2)	Management of security attributes (File Storage)
	FMT_MSA.3(1)	Static attribute initialisation (Block Storage)
	FMT_MSA.3(2)	Static attribute initialisation (File Storage)
	FMT_SMF.1	Specification of management functions
Rationale:	FDP_ACC.1(1) and FDP_ACF.1(1) support this objective by identifying the rules and attributes of the Block Storage Access Control SFP, which are used to control application host access to data stored on the TOE. FDP_ACC.1(2) and FDP_ACF.1(2) support this objective by identifying the rules and attributes of the File Storage Access Control SFP, which control user access to data stored on the TOE. FDP_UAU.2 and FIA_UID.2 support this objective by ensuring that only authorized administrators have access to TOE functions and data, and are identified and authenticated before being provided with TOE access. FMT_MSA.1(1) and FMT_MSA.3(1) support this objective by restricting the management of the Block Storage Access Control SFP to authorized administrators. FMT_MSA.1(2) and FMT_MSA.3(2) support this objective by restricting the management of the File Storage Access Control SFP to authorized administrators. FMT_SMF.1 meets this objective by ensuring that the management functions are utilized to securely manage the TOE, thus protecting the integrity of stored user data.	

6.4 DEPENDENCY RATIONALE

The Following Table 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	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FDP_ACC.1(1)	FDP_ACF.1(1)	✓	
FDP_ACC.1(2)	FDP_ACF.1(2)	✓	
FDP_ACF.1(1)	FDP_ACC.1(1)	✓	
	FMT_MSA.3	✓	
FDP_ACF.1(2)	FDP_ACC.1(2)	✓	
	FMT_MSA.3	✓	
FDP_SDI.2	None	N/A	
FIA_ATD.1	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MSA.1(1)	FDP_ACC.1(1)	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1(2)	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3(1)	FMT_MSA.1(1)	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1(2)	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_STM.1	None	N/A	

Table 12 – Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

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 there are a number of areas where current practices and procedures exceed the minimum requirements for EAL 2.

The assurance requirements are summarized in the following table:

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

Assurance Class	Assurance Components	
	Identifier	**Name**
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 13 – Security Assurance Requirements

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. A description of each of the TOE security functions follows.

7.1 TOE SECURITY FUNCTIONS

7.1.1 Security Audit

The TOE generates audit records for startup and shutdown of the audit function, all administrator login attempts, and all administrator actions that result in a configuration change. Audit records contain the date and time of the event, the type of event, subject identity (if applicable), and the outcome of the event (success or failure).

Authorized administrators can view the audit records from the UEMCLI or Unisphere GUI. The audit records are presented in a manner suitable for a user to interpret the information.

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

7.1.2 User Data Protection

The TOE supports user data protected by the File Storage Access Control SFP and the Block Storage Access Control SFP. File Users are any users accessing data or storage on the TOE via one of the file protocols (CIFS, SMB or NFS). Block Users are any application servers (hosts) accessing data or storage on the TOE via one of the block protocols (iSCSI, or FC).

7.1.2.1 File Storage Access Control SFP

All access to storage is performed via a CIFS/SMB or NFS client on behalf of the user. These clients are basic pieces of software (such as the CIFS client within Windows Explorer) used to map and access file-based storage. The TOE enforces the File Storage Access Control SFP on users connecting to the storage on the TOE for NFS and CIFS/SMB. After successful authentication for NFS users, the TOE checks user permissions for each file or directory's ACL on each user's access request to determine if the user has appropriate permissions to access the files or directories. After successful authentication for CIFS/SMB users, the TOE checks user permissions for each file or directory's DACL on each user's access request to determine if the user has appropriate permissions to access the files or directories. The ability to connect to an NFS mount, and CIFS/SMB share, is granted to users by Administrators or Storage Administrators. Users are associated with CIFS/SMB shares via an access list, while a list of IP addresses is associated with NFS mounts as an access list.

Individual file and directory access control management is granted to CIFS/SMB users with File Owner or Change Permissions set in the DACL for the user. NFS users with the root role can modify permissions for all files and directories, or users with the File Owner or Change Permissions for any given file or directory can manage access controls for those particular files and directories.

A Linux/Unix host can mount to the Unity-hosted NFS Shared Folder Server if the host has been explicitly authorized. Similarly, a Windows user can map to the Unity-hosted CIFS/SMB NAS Servers if the user has been explicitly authorized.

The export of a CIFS/SMB Shared Folder Server is determined in part by the Server Configuration LDAP setting. The Unity-hosted CIFS/SMB Shared Folder Server must be in a Windows domain with an LDAPv3-compatible server set up. A Windows client machine can map to the share only if it is a member of the defined domain. For CIFS/SMB access, subjects that are members of the group Domain Administrators shall be authorized to backup, restore, and take ownership of all objects.

Client machine access to the Unity-hosted NFS Shared Folder Server can be configured based on IP address or network host name, IP subnet range, or a Netgroup. For the NFS access protocol, users connecting to TOE storage who are *superusers* can perform all operations on all objects. Clients must be recognized as “trusted” by the system in order to submit a root request, otherwise it will be mapped to the “nobody” role.

Each file and directory has an ACL associated with it. Each ACL has a set of permissions that are granted or explicitly denied to that user. Whenever a user requests an access to a file or directory, the TOE utilizes its File Storage Access Control SFP (stored with each file and directory) to decide whether or not that access is permitted.

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

7.1.2.2 Block Storage Access Control SFP

The TOE enforces the Block Storage Access Control Security Function Policy (SFP) which is used to manage access from block-based application servers to configured Logical Units on the TOE. Access must specifically be granted for a host to access storage.

When a host is configured, the administrator provides:

- the name of the host
- the IP address of the host
- For iSCSI access, the iSCSI address (iSCSI Qualified Name (IQN)) of the host. Within the Storage Area Network (SAN), this is the address of the iSCSI initiator
- For FC access, the WWN of the host. This is the unique address of the Host Bus Adapter (HBA) that initiates the connection to the storage resources
- Access settings. The options are:
    - No access
    - LUN access

- Snapshot access
- LUN and Snapshot access

When a LUN is configured, the administrator identifies:

- Name and description of the storage resource
- The storage size associated with the LUN
- The hosts that have access to this resource. Hosts are identified by address:
  - For iSCSI, this is the IQN
  - For FC access, this is the WWN of the host

When a user attempts to access storage resources, Unity verifies the IQN or WWN of the host initiator and verifies that the host has access to the requested LUN target before allowing access.

Storage may be accessed as a LUN or a snapshot. A snapshot is a point-in-time copy of data stored on the LUN. It provides a record of the content in the targeted storage resource at a particular date and time, and may be used to support data protection and recovery. The presentation of stored data as a snapshot is beyond the scope of the evaluation; however, the Block Storage Access Control SFP applies equally to both access types.

Both Windows and Linux hosts may access storage via iSCSI and FC as follows.

- iSCSI Access
  - For a Windows host, the host must be able to access the iSCSI interface. The Microsoft iSCSI initiator service must be started.
  - For a Linux host, hosts connect to LUN storage resources by using Linux iSCSI software available on the host. Those responsible for the host will have to mount the directory for the file system associated with the storage.
- FC Access
  - On the Windows host, the server connection must be added using Microsoft Storage Manager for SANs. Storage Manager for SANs is a Microsoft Management Console (MMC) snap-in used to create and manage logical unit numbers (LUNs) on Fibre Channel.
  - Hosts connect to LUN storage resources by using Linux FC software available on the host. Those responsible for the host will have to mount the directory for the file system associated with the storage.

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

The TOE also ensures the integrity of user data. Unity may be configured with Redundant Array of Independent Disks (RAID) levels 1/0, 5 or 6. Each of these provides fault tolerance for integrity errors or disk failure. The RAID implementation provides mechanisms to continuously check data integrity while

reading and writing data to individual disks. Integrity errors or drive errors are fixed on-the-fly. Additionally, Administrators may configure 'hot spare' disk drives. These hot spares are used when a disk failure has been detected by the system. Once a failure has been detected, the drive that has been lost will be recreated on the hot spare. The Administrator can then replace the failed drive and configure it as a new hot spare. This process does not interfere with user data access.

With RAID 1/0, two or more groups of two mirrored (RAID 1) disks are put in a RAID 0 array, or a stripe of mirrors. In the case of a disk failure, the mirrored data is recovered. For a RAID 5 implementation, data is striped across several disks, and parity data is divided across all the disks in the array. RAID 6 also stripes data across several disks, but uses double parity data distributed across multiple disks for added protection.

When an integrity error is detected, an alert is placed in a log file. Administrators may view alerts via the Alerts page of Unisphere or from the UEMCLI.

TOE Security Functional Requirements addressed: FDP_SDI.2

7.1.3 Identification and Authentication

The TOE uses an LDAPv3-compatible server in the TOE environment to provide authentication services for both Administrators and CIFS/SMB file-based users. A NIS server is used to provide authentication services for NFS file-based users. For all authentication processes, once the username and password have been verified, the TOE uses the message returned from the authentication server to assign an administrative role, or a role to file-based users.

7.1.3.1 Administrative Identification and Authentication

The TOE also supports the use of local authentication. In this case, the UserID, password and role are maintained by the TOE. The TOE verifies the UserID and password on login and assigns a role.

Administrators can access the TOE through a web browser or through a command line interface. Identification and authentication must be completed before Administrators are provided with access to the TOE.

The TOE maintains the UserID, password and role for Administrators subject to local authentication, and only the role information for users authenticating via an LDAP directory.

7.1.3.2 File-Based User Identification and Authentication

Windows environments use an LDAPv3-compatible server for authentication. A Windows host can only map to a CIFS Shared Folder Server if the Windows host is on the same domain as Unity, and the Windows domain with an LDAPv3-compatble server is set up.

For NFS, users are authenticated against a NIS server. The server from which the request is coming is identified and authenticated based on the username and

password. If the user ID is “root” then the host must also be assigned as a “trusted host” within the TOE configuration.

TOE Security Functional Requirements addressed: FIA_ATD.1, FIA_UAU.2, FIA_UID.2

7.1.4 Security Management

The TOE is shipped with a factory default Management account (*admin*) and password (*Password123#*) for initial access and configuration. With this default account, administrators can reset default passwords, configure the system settings, create user accounts, and allocate storage. Changing the default password for the admin account is a requirement during the initial configuration process.

Once the TOE has been configured, authorized administrators can access the TOE management functions via the UEMCLI or the Unisphere GUI. Each administrator is assigned a role which determines TOE access capabilities. Table 14 identifies the administrative roles and describes the available TOE functions:

Management Task	Operator	Storage Administrator	Administrator
Change own local login password	X	X	X
Add, delete, or modify hosts			X
Create storage		X	X
Delete storage		X	X
Add storage objects, such as LUNs, shares, and storage groups to a storage resource		X	X
View storage configuration and status	X	X	X
View Unisphere user accounts		X	X
Add, delete or modify Unisphere user accounts			X
View current software or license status	X	X	X
Perform software or license upgrade			X
Perform initial configuration			X
Modify NAS server configuration			X
Modify system settings			X
Modify network settings			X

Management Task	Operator	Storage Administrator	Administrator
Change management interface language	X	X	X
View log and alert information	X	X	X

Table 14 – TOE Administrative Roles and Privileges

Default attributes for the Block Access Control SFP are considered to be restrictive because an application host will not have access to storage resources until its WWN or IQN is specifically listed in the LUN's host access list. The TOE provides mechanisms to govern which hosts can access which LUNs. Default attributes for the File Access Control SFP are considered to be restrictive because trusted host does not exist until entered by an Administrator. The Security Management functions allow Administrators assigned the appropriate role to configure this functionality.

Client machines accessing the TOE via CIFS, SMB, or NFS protocols do not have access until the user is authenticated. Once authenticated, the user is granted access according to the Access Control List associated with each file and directory. CIFS/SMB, and NFS file and directory attributes that can be modified include read, write, and execute permissions. There are no set default permissions.

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

7.1.5 Protection of the TSF

The TOE provides reliable time stamps for auditable events.

TOE Security Functional Requirements addressed: FPT_STM.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Administrator	The generic term 'Administrator' is used to refer to a user in the Operator, Storage Administrator or Administrator role.
Application Host	An Application Host is a term used to generically define systems and/or applications accessing storage on the TOE.

Table 15 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ACL	Access Control List
API	Application Programming Interface
CAVA	Common Anti-Virus Agent
CC	Common Criteria
CCE	Common Event Enabler
CLI	Command Line Interface
DACL	Discretionary Access Control List
DAE	Disk Array Enclosure
DPE	Disk Processor Enclosure
D@RE	Data at Rest Encryption
EAL	Evaluation Assurance Level
FC	Fibre Channel
GUI	Graphical User Interface
HBA	Host Bus Adapter
HTML5	Hypertext Markup Language 5
IP	Internet Protocol
IQN	iSCSI Qualified Name

Acronym	Definition
iSCSI	Internet Small Computer System Interface
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number
NDMP	Network Data Management Protocol
OE	Operating Environment
OSP	Organizational Security Policy
PP	Protection Profile
RAID	Redundant Array of Independent Disks
REST	Representational State Transfer
SAN	Storage Area Network
SFP	Security Function Policy
SFR	Security Functional Requirement
SMB	Server Message Block
SMI-S	Storage Management Initiative Specification
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Transfer Protocol
SP	Storage Processor
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UEMCLI	Unified Element Manager Command Line Interface
VASA	vStorage APIs for Storage Awareness
WWN	World Wide Name

Table 16 – Acronyms