EMC Corporation
EMC® CLARiiON® FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 0.5

Prepared for:

EMC Corporation
176 South Street
Hopkinton, MA 01748
Phone: (508) 435-1000

http://www.emc.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050

http://www.corsec.com

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the EMC CLARiiON FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems, and will hereafter be referred to as the TOE throughout this document. The TOE is a storage operating environment and management software suite combination designed for CLARiiON storage arrays. CLARiiON storage arrays provide midrange Storage Area Network (SAN) storage.

1.1 Purpose

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats:

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

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	EMC Corporation EMC® CLARiiON® FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems Security Target
ST Version	Version 0.5
ST Author	Corsec Security, Inc.
ST Publication Date	2010-01-12
TOE Reference	EMC CLARiiON FLARE v4.29.000.5.003 with Navisphere v6.29.000.6.034 running on CX4 Series Storage Systems.
Keywords	Storage Area Network (SAN), storage array, data storage, CLARiiON, EMC, FLARE, Navisphere

1.3 Product and TOE Overview

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

1.3.1 Product Description

The EMC CLARiiON is a storage device designed to provide managed storage on a SAN. The CLARiiON hardware runs the TOE, which is comprised of the FLARE v4.29 and Navisphere v6.29 software suite. The product includes a Storage Operating Environment (SOE) (FLARE), which provides Redundant Array of Independent Disks (RAID) and virtual storage capability, as well as an interface (Navisphere) by which EMC CLARiiON storage appliances in a SAN environment can be administered and managed. The product provides the ability to combine several individual drives into useful logical groups, provides fault tolerance for stored data, and manages access to the data that it stores. The CLARiiON accomplishes this through purpose-built hardware and software. They are designed to allow customers to scale both system performance and storage capacity.

The purpose of a SAN is to allow many different application servers or file servers to share storage provided by centrally managed storage devices. The EMC CLARiiON FLARE/Navisphere allows an organization to manage its storage needs separately from its application and file servers. This allows greater control over storage allocation, fault tolerance, and backups versus storage that is directly attached to individual application or file servers. In a typical deployment scenario, individual application servers are attached to a SAN through a Fibre Channel or iSCSI[1] switch. These application servers are then configured to use storage on the CLARiiON, in the form of Logical Units (LUNs) (described in Section 1.3.3.1 below), as storage for their applications. CLARiiON storage can also be used

[1] iSCSI – Internet Small Computer System Interface

through an EMC Celerra file server to provide Network Attached Storage (NAS) for traditional Internet Protocol (IP) based clients. The CLARiiON can also be monitored by an EMC ControlCenter Agent Server to collect information on the health or status of the TOE. Figure 1 shows the details of the deployment configuration of the TOE:

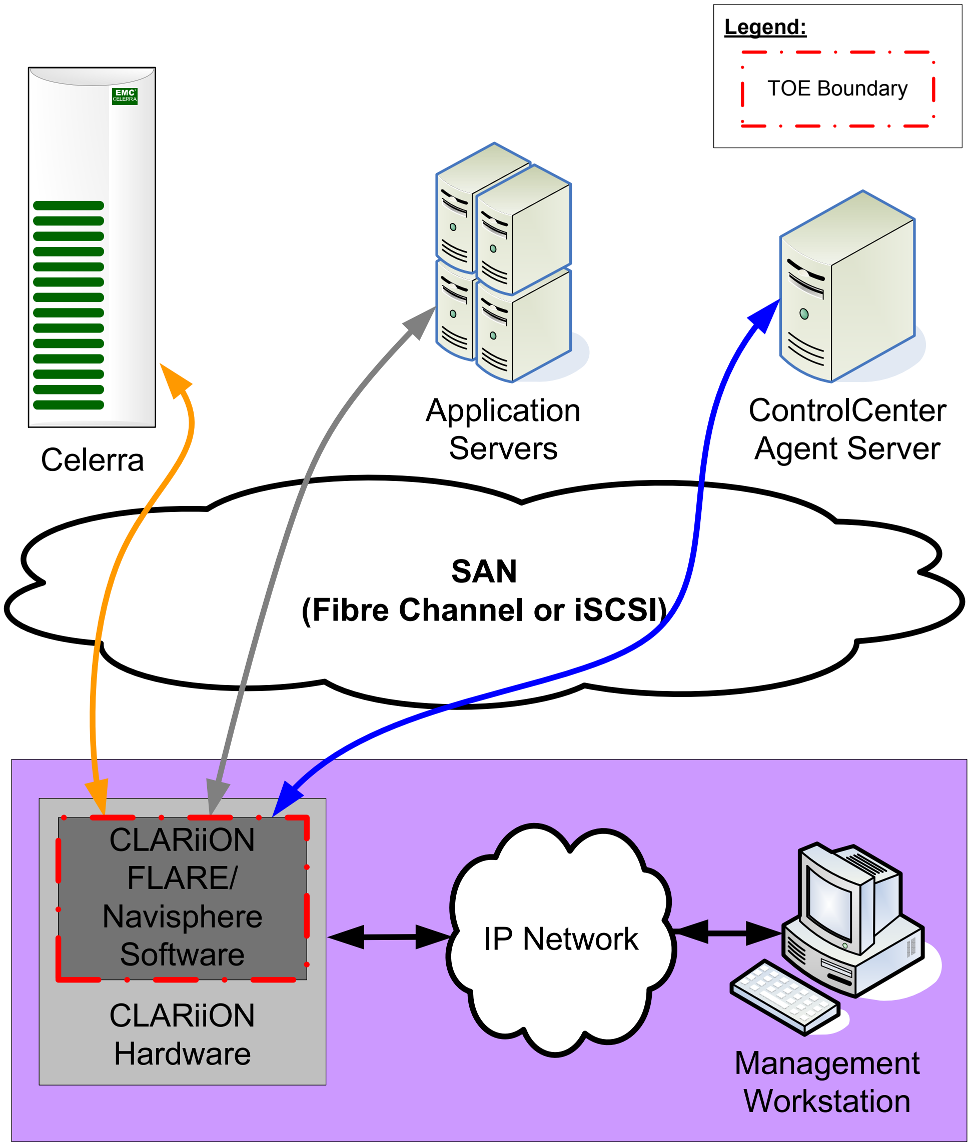

Figure 1 – Deployment Configuration of the TOE

1.3.2 TOE Description

The software-only TOE is the EMC CLARiiON FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems. It includes an SOE (FLARE), which provides RAID and virtual storage capability, as well as an interface (Navisphere) by which EMC CLARiiON storage appliances in a SAN environment can be administered and managed.

The EMC Navisphere software is a management application suite designed to be the central console in a CLARiiON-based SAN. The SAN allows many different application servers to share storage provided by centrally managed storage devices. This architecture allows an organization to manage its storage needs separately from its application servers, allowing greater control over storage allocation, fault tolerance, and backups than storage that is directly attached to individual application servers.

The TOE is managed by authorized users through the Navisphere Manager and the Navisphere Secure CLI[2] interfaces. Navisphere Manager is a Java-based applet that runs within a web browser. To access the functions available via Navisphere Manager, an authorized user must open a web browser and enter the IP address or hostname of the desired storage system Storage Processor (SP) (described in Section 1.3.3.2 below). Navisphere Secure CLI is a command line interface that provides access to common functions for monitoring and managing the TOE. The Secure CLI provides access to functions for storage provisioning, status and configuration information retrieval, and other TOE administrative functions. Secure CLI commands can also be used to automate management functions via shell scripts and batch files.

The EMC FLARE software is an SOE optimized for implementation of RAID storage architectures, providing fault detection, isolation, and diagnosis capabilities. It enables the use of virtual storage elements (LUNs) to improve performance and capacity utilization. The FLARE software also provides a Navisphere-managed storage appliance with the flexibility to support multiple generations of CLARiiON hardware and different types of interconnects with consistent functionality. FLARE also implements a technology called Access Logix. Access Logix lets multiple hosts share a storage system by using Storage Groups (described in Section 1.3.3.4 below). A Storage Group is one or more LUNs within a storage system that is reserved for one or more hosts and is inaccessible to other hosts. Access Logix enforces the host-to-Storage Group permissions.

The TOE also performs event monitoring of system status and host registration of application servers. This is done through the TOE's SP Agent. The SP Agent collects event information about the state of the system, including FLARE, the TOE's hardware components, and the TOE's LUNs and reports this information to authorized TOE users. The SP Agents also communicate host registration information between the SP Agents and the application servers. These agents periodically retrieve volume-mapping information from the application servers and forward it to Navisphere Manager for display.

1.3.3 Brief Description of the Components of the TOE

1.3.3.1 LUNs

A central concept of the CLARiiON product is a virtual unit called a LUN. The CLARiiON storage appliance presents storage to the SAN in the form of a LUN, and the CLARiiON FLARE/Navisphere software provides for the management of LUNs. Each LUN represents a unit of storage to an application server, analogous to a local disk drive. However, the LUN provided by the CLARiiON FLARE/Navisphere is not constrained to be a single individual disk. In fact, a typical deployment would have LUNs that span multiple individual disks that are grouped into a RAID Group (described in Section 1.3.3.3 below).

1.3.3.2 Storage Processors

The central component of the CLARiiON is the SP. The SP is responsible for interfacing with the SAN and with each of the individual disks within the CLARiiON. There are two SPs in each CLARiiON which logically operate as a single entity to provide increased performance and fault tolerance. The SP provides administrators with the ability to manage the CLARiiON and establish LUNs and RAID Groups.

1.3.3.3 RAID Groups

A RAID Group is a collection of individual disks. The CLARiiON supports a variety of disk types and capacities (chosen by the customer when the product is purchased). In a RAID Group, disks of a similar type are typically grouped together. This RAID Group can then be configured by an administrator with various attributes, such as

[2] CLI – Command Line Interface

which RAID level to provide. In this manner, an administrator can manage the CLARiiON through successive levels of abstraction.

1.3.3.4 Storage Groups

The CLARiiON manages access to LUNs through a component of the SP called Access Logix. Access Logix allows an administrator to group LUNs together in a Storage Group. Each Storage Group can then be mapped to one or more application servers, identified by their Fibre Channel World Wide Name[3] (WWN) or iSCSI Qualified Name[4] (IQN). When this mechanism is used, only the LUNs that are present in a Storage Group that a particular application server has been given access to are made accessible to that application server.

It is also possible that multiple application servers are given access to the same Storage Group. This is used in cases where the application server has been deployed in such a way as to manage multiple servers accessing the same LUN, for example, in a clustered environment.

1.3.4 TOE Environment

The TOE is intended to be deployed in a secure data center that protects physical access to the TOE. The TOE is intended to be connected to a SAN with the constituent servers managed by administrators operating under a consistent security policy with the administrators that manage the TOE.

The TOE provides access control to individual LUNs through its Access Logix component. For this to operate correctly, the WWN that is provided to the TOE must be accurate and must not be spoofed. The TOE Environment is required to provide this.

1.4 Physical and Logical Scope

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

1.4.1 Physical Scope

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is the EMC CLARiiON FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systemssoftware suite. The TOE runs on the EMC CLARiiON CX4 Series hardware, models CX4-120, CX4-240, CX4-480, and CX4-960.

1.4.1.1 Guidance Documentation

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

- EMC Navisphere Manager Online Help 6.29
- EMC Navisphere Analyzer Command Line Interface (CLI) Reference
- EMC Navisphere Command Line Interface (CLI) Reference
- EMC CX4 Series FLARE Operating Environment Version 04.29 Release Notes
- EMC CLARiiON CX4-120 Setup Guide
- EMC CLARiiON CX4-240 Setup Guide
- EMC CLARiiON CX4-480 Setup Guide

[3] A World Wide Name is a unique identifier in a Fibre Channel.

[4] An iSCSI Qualified Name is a unique identifier in a Serial Attached SCSI storage network.

- EMCCLARiiON CX4-960 Setup Guide
- EMC Navisphere Analyzer Version 6.29.00 Release Notes
- EMC Navisphere Manager Version 6.29.00 Release Notes
- EMC Navisphere Host Agent/CLI and Utilities Version 6.29 for FLARE OE 04.29 Release Notes

1.4.2 Logical Scope

The TOE is a software-only TOE consisting of EMC CLARiiON FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems. The TOE runs the Navisphere software suite (version 6.29.000.6.034), which includes Navisphere Storage System Initialization Utility, Navisphere Host and SP Agents, Navisphere Server Utility, Navisphere Manager, Navisphere Integrator, Navisphere Storage Management Server, and Navisphere Secure CLI. The TOE also includes FLARE version v4.29.000.5.003.

The TOE is managed by authorized users through the Navisphere Manager and the Navisphere Secure CLI. Navisphere Manager is a Java applet that runs within a web browser. Navisphere Secure CLI is a command line interface that provides access to common functions for monitoring and managing the TOE.

The TOE logical boundary is defined by the security functions that it implements. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- User Data Protection
- Identification and Authentication
- Security Management

1.4.2.1 User Data Protection

The User Data Protection function implements functionality necessary to protect User Data which is entrusted to the TOE. The TOE protects user data primarily in two ways. First, it ensures that only the application servers that have been granted access to a LUN have access to that LUN. Second, it ensures the integrity of the data entrusted to it through its use of RAID levels.

1.4.2.2 Identification and Authentication

The TOE provides the ability for administrators to manage the security functions of the TOE. The Identification and Authentication security function allows the TOE to identify and authenticate administrators of the TOE. Administrators are assigned a role to determine what aspects of the TOE they are allowed to manage.

1.4.2.3 Security Management

The Security Management function provides administrators with the ability to properly manage and configure the TOE to store user data. Administrators are assigned a role that governs what aspects of the TOE they are authorized to manage. Configuration of RAID settings, Storage Group membership, and administrator access is all supported through this security function.

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

Features and functionality that are not part of the evaluated configuration of the TOE are:

- CLARiiON storage appliance hardware
- iSCSI with Challenge-Handshake Authentication Protocol (CHAP) authentication
- Remotely Anywhere
- Navisphere Analyzer
- Navisphere SnapView

- Navisphere MirrorView/Asynchronous
- Navisphere MirrorView/Synchronous
- Navisphere SAN Copy
- Navisphere Quality of Service Manager (NQM)

2 Conformance Claims

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

Table 2 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007; CC Part 2 conformant; CC Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted CEM as of 2009/05/15 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2 Augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem Definition

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

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

3.1 Threats to Security

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

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE).

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 - Security Objectives.

The following threats are applicable:

Table 3 – Threats

Name	Description
T.DATA_CORRUPTION	Data could become corrupted due to hardware failure or incorrect system access by users of the TOE or attackers.
T.IMPROPER_SERVER	A system connected to the TOE could access data to which it was not intended to gain access by bypassing the protection mechanisms of the TOE.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no Organizational Security Policies.

3.3 Assumptions

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

Table 4 – Assumptions

Name	Description
A.PHYSICAL	Physical security will be provided for the TOE and its environment.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.I&A	The TOE environment will provide identification and authentication of Application Server users before allowing any other TSF[5]-mediated actions on behalf of that user.

[5] TSF – TOE Security Functionality

4 Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 5 – Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must provide a method for administrative control of the TOE.
O.PROTECT	The TOE must protect data that it has been entrusted to protect.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 6 – IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.PROPER_NAME_ASSIGNMENT	The TOE environment must provide accurate World Wide Names for each system that communicates with the TOE.
OE.SECURE_COMMUNICATIONS	The TOE environment must provide secure communications between systems connected to the Storage Area Network.
OE.SECURE_SERVERS	The TOE environment must provide properly configured application servers to communicate with the TOE.
OE.I&A	The TOE environment must provide identification and authentication of Application Server users before allowing any other TSF-mediated actions on behalf of that user.

4.2.2 Non-IT Security Objectives

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

Table 7 – Non-IT Security Objectives

Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.
OE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.
OE.NOEVIL	Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.

5 Extended Components Definition

This section defines the extended SFRs and extended SARs met by the TOE. There are no extended components defined for this TOE.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

6.1.1 Conventions

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

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Parts 2 and 3 of the CC, and are shown as follows:

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

6.2 Security Functional Requirements

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

Table 8 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓	✓	
FDP_SDI.2	Stored data integrity		✓	✓	
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1(a)	Management of TSF data	✓	✓		✓

Name	Description	S	A	R	I
FMT_MTD.1(b)	Management of TSF data	✓	✓		✓
FMT_MTD.1(c)	Management of TSF data	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		

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

6.2.1 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*] on

[*a) Subjects: Application Servers;*

b) Objects: LUNs

c) Operations: Read and Write

].

Application note: The Subjects are Application Servers connected to the SAN acting on behalf of an authorized user.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*] to objects based on the following:

[

Subject attributes:

1. *World Wide Name*
2. *Storage Group Membership*

Object attributes:

1. *LUN ID*
2. *Storage Group Membership*

].

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 valid Subject of the TOE is allowed to Read and Write to a LUN if the Subject and the LUN are members of the same Storage Group

].

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on ~~the following~~ **no** additional rules: ~~[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].~~

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on **no additional rules** ~~the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]~~.

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

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

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 3, RAID 5, and RAID 6; mirrored data for RAID 1 and RAID 1+0*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*reconstruct the user data for RAID 3, RAID 5, and RAID 6; replace erroneous data with the mirrored data for RAID 1, and RAID 1+0; and notify an administrator*].

Dependencies: No dependencies

6.2.2 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

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.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

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.

Dependencies: No dependencies

6.2.3 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*] to restrict the ability to [*query, modify, delete*] the security attributes [*Storage Group Membership*] to [*the Administrator and Manager roles*].

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

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*Discretionary Access control 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 [*Administrator and Manager roles*] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MTD.1(a) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*query*] the [*storage system information*] to [*the Administrator, Manager, and Monitor roles*].

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

FMT_MTD.1(b) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*query, modify, delete, [create]*] the [*LUNs, RAID Groups, and Storage Groups*] to [*the Administrator and Manager roles*].

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

FMT_MTD.1(c) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*query, modify, delete, [create]*] the [*user accounts*] to [*the Security Administrator role*].

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:

[

a) *Management of security functions behavior;*

b) *Management of TSF data;*

c) *Management of security attributes*

].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*as the authorized identified roles in* Table 9].

Table 9 – Authorized Roles

Roles	Description
Administrator	This role can access all administrative and management interfaces and data, can delete users, and depending on the scope of the account can add or delete information from a domain.
Manager	This role can view all storage system information and perform storage-system operations (such as binding LUNs), but cannot add, modify, or delete user or domain information.
Monitor	This role can view all storage-system information, but cannot add, modify, or delete information from a domain or perform configuration operations such as binding LUNs.
Security Administrator	This role can grant users access rights to the array and configure IP filtering, but cannot configure LUNs. This is the only role that can create accounts and assign roles to them.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 10 – Assurance Requirements summarizes the requirements.

Table 10 – Assurance Requirements

Assurance Requirements	
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw Reporting Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

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

7.1 TOE Security Functions

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

Table 11 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1(a)	Management of TSF data
	FMT_MTD.1(b)	Management of TSF data
	FMT_MTD.1(c)	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_SDI.2	Stored data integrity

7.1.1 User Data Protection

The TOE provides the User Data Protection security function to manage access from application servers to configured LUNs. The purpose of SAN attached storage is to allow high speed, scalable, fault-tolerant storage separate from individual application servers. The TOE provides this functionality for servers connected to the SAN.

Using the Security Management security function, Administrators of the TOE can configure LUNs to provide storage to application servers. These LUNs are then placed into Storage Groups, which allows an Administrator to limit access to each LUN to one or more application servers. When an application server requests a list of available LUNs from the TOE, the TOE Environment provides a WWN. This WWN is used to identify the application server to the TOE. The TOE then provides a list of LUNs that the application server has been granted access to. With each successive request to read or write information to a LUN, the TOE ensures that only authorized application servers have access to the LUNs to which they have been given access.

The TOE also provides for the integrity of user data. When creating RAID Groups from individual disk drives, an Administrator can configure RAID levels 0, 1, 1+0, 3, 5, or 6. Each of these, except RAID level 0, provides fault tolerance for integrity errors or individual disk drive failure. The TOE provides mechanisms to check data integrity continuously while reading and writing data to individual disks. Integrity errors or drive errors are fixed on-the-fly. Additionally, Administrators can 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 is provided while real-time access to user data continues.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_SDI.2.

7.1.2 Identification and Authentication

The Identification and Authentication security function provides the TOE with the ability to govern access by administrators. Administrators of the TOE can access the TOE in one of two methods. An administrator can manage the TOE through the Navisphere Manager, a web-based graphical user interface. An administrator can also manage the TOE through the Navisphere Secure CLI, a command line interface application. Prior to allowing access through these interfaces, the TOE requires an administrator to be identified using a username and password. Before successful completion of the security function, an administrator is unable to perform any management function.

Identification and Authentication of application servers connecting to the TOE to access LUNs is provided by the TOE Environment through the proper assignment and use of WWNs.

TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UID.2.

7.1.3 Security Management

The purpose of the TOE is to provide a storage system to application servers attached to a SAN. The TOE provides mechanisms to govern which application servers can access which LUNs. The Security Management function allows Administrators to properly configure this functionality.

Management of the TOE occurs through either the Navisphere Manager or the Navisphere Secure CLI. Administrators of the TOE are assigned one of four roles. The following description of the Security Management function is described through the capabilities of each of the roles.

The Monitor role allows an Administrator to query information about the TOE. The Monitor role may view information about individual disk drives, RAID Groups, LUNs, and Storage Groups. This functionality is provided through the Navisphere interfaces.

The Manager role can perform all of the functionality of the Monitor role and can configure and modify storage system objects. The Manager role can:

- add and remove individual disk drives to a RAID Group
- create and modify LUNs
- administer membership of LUNs and application servers in a Storage Group

The Security Administrator role can manage user accounts. This includes creating, deleting, and changing the role of any user account on the TOE.

The Administrator role can perform all of the functionality of the Monitor and Manager roles, can delete user accounts, and can add or delete information from a domain.

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3 FMT_MTD.1(a), FMT_MTD.1(b), FMT_MTD.1(c), FMT_SMF.1, FMT_SMR.1.

8 Rationale

8.1 Conformance Claims Rationale

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

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 12 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.DATA_CORRUPTION Data could become corrupted due to hardware failure or incorrect system access by users of the TOE or attackers.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN supports the mitigation of this threat by allowing an administrator to properly configure the mechanisms of the TOE designed to mitigate this threat.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT mitigates this threat by providing mechanisms to protect the data that has been entrusted to the TOE.
T.IMPROPER_SERVER A system connected to the TOE could access data to which it was not intended to gain access by bypassing the protection mechanisms of the TOE.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN supports the mitigation of this threat by allowing an administrator to properly configure the mechanisms of the TOE designed to mitigate this threat.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT ensures that the TOE provides adequate mechanisms to give only authorized servers access to the appropriately authorized data.
	OE.PROPER_NAME_ASSIGNMENT The TOE environment must provide accurate World Wide Names for each system that communicates with the TOE.	OE.PROPER_NAME_ASSIGNMENT ensures that the World Wide Names provided to the TOE are accurate. This allows the mechanisms provided by O.PROTECT to properly protect data.

Threats	Objectives	Rationale
	OE.SECURE_COMMUNICATIONS The TOE environment must provide secure communications between systems connected to the Storage Area Network.	OE.SECURE_COMMUNICATIONS ensures that all communications with the TOE are secure for administration of the TOE, internal TOE communications, and data sent to or from the TOE.
	OE.SECURE_SERVERS The TOE environment must provide properly configured application servers to communicate with the TOE.	OE.SECURE_SERVERS mitigates this threat by ensuring that each server connected to the Storage Area Network operates properly and does not intentionally compromise data.

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no policies defined for this Security Target.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 13 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.PHYSICAL Physical security will be provided for the TOE and its environment.	OE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	Physical security is provided within the domain for the value of the IT resources protected by the operating system and the value of the stored, processed, and transmitted information. OE.PHYSICAL satisfies this assumption.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the	OE.MANAGE Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used	Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these

Assumptions	Objectives	Rationale
information it contains.	securely.	functions and facilities from unauthorized use. OE.MANAGE satisfies this assumption.
A.NOEVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	OE.NOEVIL Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.	Sites using the TOE ensure that administrators are non-hostile, appropriately trained, and follow all administrator guidance. OE.NOEVIL satisfies this assumption.
A.I&A The TOE environment will provide identification and authentication of Application Server users before allowing any other TSF-mediated actions on behalf of that user.	OE.I&A The TOE environment must provide identification and authentication of Application Server users before allowing any other TSF-mediated actions on behalf of that user.	OE.I&A satifies the assumption that the environment provides identification and authentication of Appplication Server users.

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

8.3 Rationale for Extended Security Functional Requirements

There are no extended functional requirements defined for this TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended assurance requirements defined for this TOE.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 14 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN	FIA_UAU.2	The TOE shall successfully authenticate each administrator before

Objective	Requirements Addressing the Objective	Rationale
The TOE must provide a method for administrative control of the TOE.	User authentication before any action	allowing her to manage the TOE.
	FIA_UID.2 User identification before any action	The TOE will properly identify and authenticate all administrators.
	FMT_MSA.1 Management of security attributes	Security attributes of the TOE can only be changed by authorized administrators.
	FMT_MSA.3 Static attribute initialisation	Permissive values for data access are provided, and the TOE administrator can changed them when a data object is created.
	FMT_MTD.1(a) Management of TSF data	The ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_MTD.1(b) Management of TSF data	The ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_MTD.1(c) Management of TSF data	The ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 specifies each of the management functions that are utilized to securely manage the TOE.
	FMT_SMR.1 Security roles	Specific roles are defined to govern management of the TOE.
O.PROTECT The TOE must protect data that it has been entrusted to protect.	FDP_ACC.1 Subset access control	The TOE has an access control policy that ensures that only authorized servers can gain access to data within the TOE.
	FDP_ACF.1 Security attribute based access control	The TOE provides access control functionality to manage access to data within the TOE.

Objective	Requirements Addressing the Objective	Rationale
	FDP_SDI.2 Stored data integrity	The TOE protects the stored user data from integrity errors.

8.5.2 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2+, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

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

8.6 Rationale for Refinements of Security Functional Requirements

The following refinements of Security Functional Requirements from CC version 3.1 have been made to clarify the content of the SFRs, and make them easier to read:

The words "no additional rules" was added, and others stricken, to FDP_ACF.1.

The word "objects" was changed to "user data" to specify more precisely what is protected with FDP_SDI.2.

8.6.1 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 15 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 15 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_SDI.2	No Dependencies	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies		
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(a)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MTD.1(b)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(c)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_SMF.1	No dependencies		
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.

9 Acronyms

Table 16 – Acronyms

Acronym	Definition
CC	Common Criteria
CHAP	Challenge-Handshake Authentication Protocol
CLI	Command Line Interface
DoD	Department of Defense
EAL	Evaluation Assurance Level
IP	Internet Protocol
IQN	iSCSI Qualified Name
iSCSI	Internet Small Computer System Interface
ISO	International Organization for Standardization
IT	Information Technology
LUN	Logical Unit
NAS	Network Attached Storage
NQM	Navisphere Quality of Service Manager
OSP	Organizational Security Policy
PP	Protection Profile
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Functional Policy

Acronym	Definition
SFR	Security Functional Requirement
SOE	Storage Operating Environment
SOF	Strength of Function
SP	Storage Processor
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	Toe Summary Specification
WWN	World Wide Name