EMC Corporation
VPLEX with GeoSynchrony 5.0

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.6

Prepared for:

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

Phone: +1 508 435 1000
Email: info@emc.com
http://www.emc.com

Prepared by:

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

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the EMC VPLEX with GeoSynchrony 5.0, and will hereafter be referred to as the TOE throughout this document. The TOE is a software-only, storage network-based federation[1] solution that provides non-disruptive, heterogeneous data movement and volume management functionality.

1.1 Purpose

This ST is divided into nine sections, as follows:

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

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 - ST and TOE References

ST Title	EMC Corporation VPLEX with GeoSynchrony 5.0 Security Target
ST Version	Version 0.6
ST Author	Corsec Security, Inc.
ST Publication Date	12/6/2011
TOE Reference	EMC VPLEX with GeoSynchrony 5.0 build 5.0.0.00.00.38 Management Server Software v5.0 build 5.0.0.00.00.38 VPLEX Witness Software v5.0 build 5.0.0.00.00.38

[1] See Section 9.2 for the definition of federation.

1.3 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.

EMC VPLEX is a storage network-based federation solution that provides non-disruptive, heterogeneous data movement and volume management functionality. VPLEX is an appliance-based solution that connects to Fibre Channel (FC) SAN[2] or Ethernet switches. The VPLEX architecture is designed as a highly-available solution and, as with all data management products, high availability (HA) is a major component in most deployment strategies.

VPLEX is offered in three hardware configurations based on how many engines are installed in the cabinet: Single-engine, dual-engine, and quad-engine. A single engine consists of two independent directors running the director software with GeoSynchrony 5.0. The directors within the engine handle all I/O traffic, including read/write requests, from hosts to back-end storage

The TOE consists of only the software portion of EMC VPLEX, which comprises the following:

- The management server software, including the VPLEX CLI[3] and the management console web-based graphical user interface (GUI)
- The director software
- VPLEX Witness software

The Metro deployment configuration (synchronous communications between two or more clusters) and the Geo deployment configuration (asynchronous communications between two or more clusters) are the two CC evaluated configurations.

A Metro deployment configuration consists of two clusters located within synchronous distance[4] connected via FC for inter-cluster communication, a VPLEX Witness connected to the clusters over a WAN[5], front-end hosts and back-end storage arrays connected to each cluster over SAN fabrics, and one or more management workstations connected to the management servers over a LAN[6]. Figure 1 below illustrates a Metro deployment configuration.

[2] SAN – Storage Area Network
[3] CLI – Command Line Interface
[4] See Section 9.2 for a definition of synchronous.
[5] WAN – Wide Area Network
[6] LAN – Local Area Network

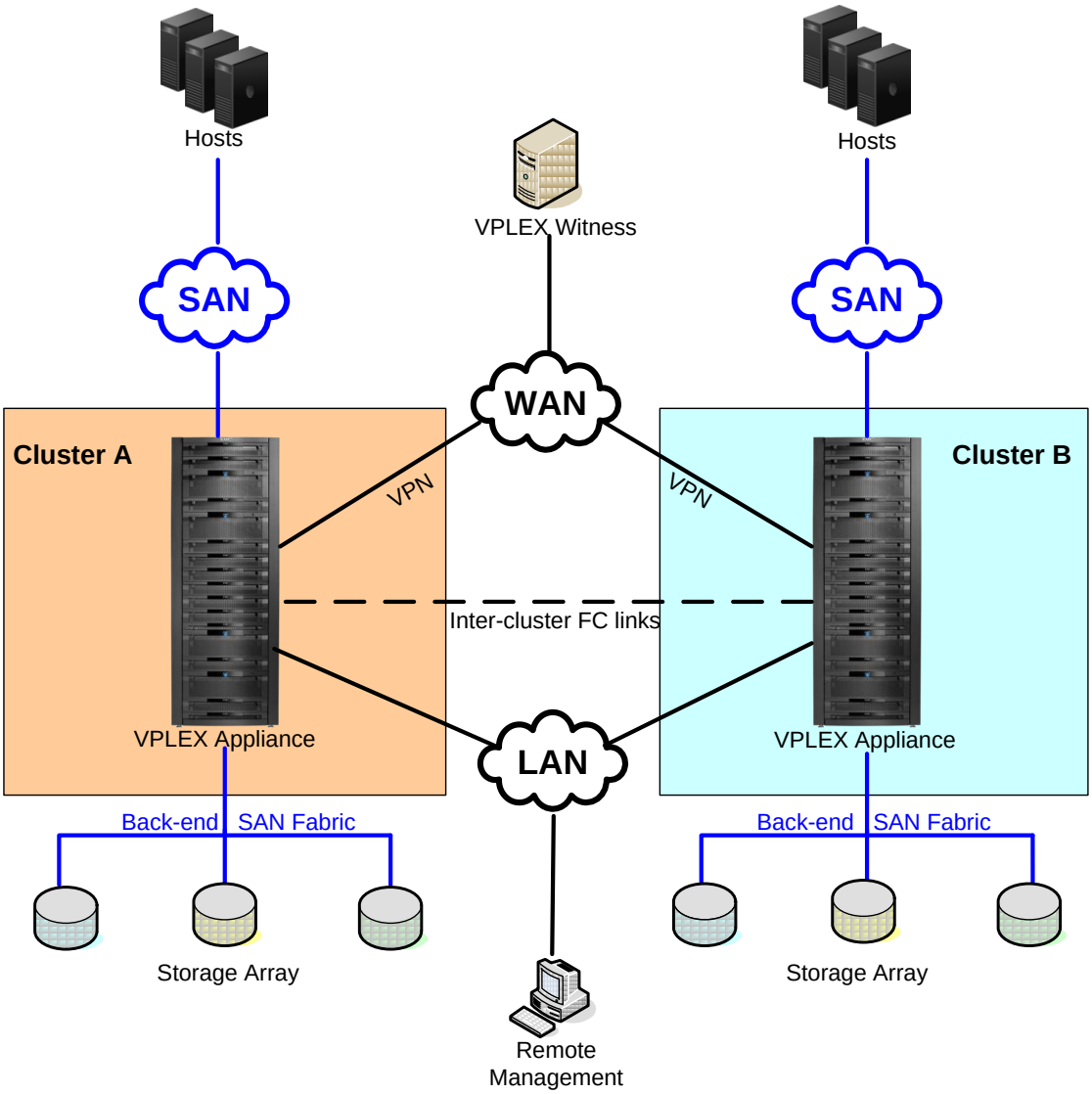

Figure 1 - Metro Deployment Configuration of the TOE

A Geo deployment configuration is identical to a Metro configuration with two exceptions:

- The clusters are separated over longer, asynchronous distances[7].
- Inter-cluster communication is performed over a WAN instead of FC.

Figure 2 below illustrates a Geo deployment configuration.

[7] See Section 9.2 for a definition of asynchronous.

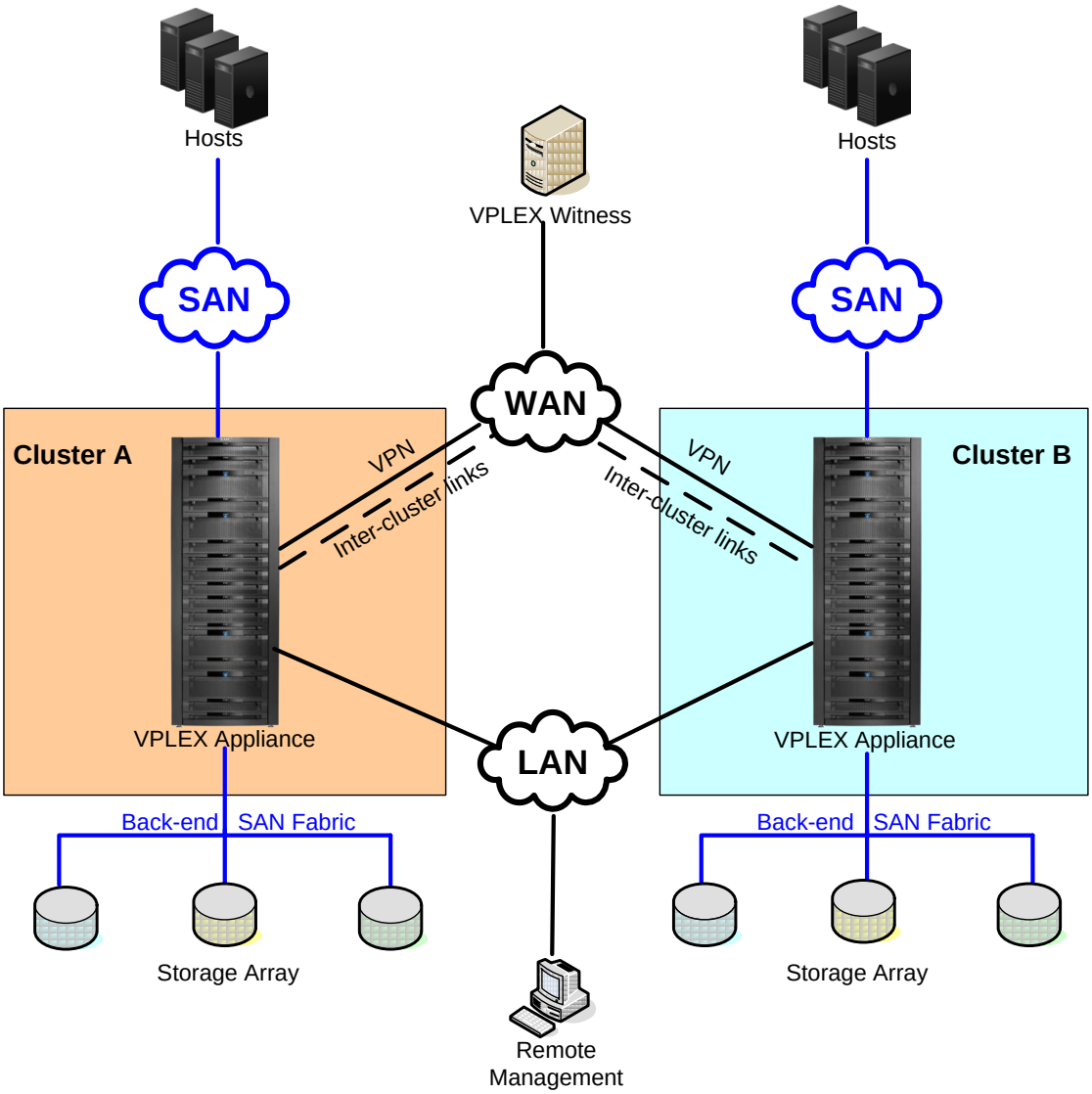

Figure 2 - Geo Deployment Configuration of the TOE

The director software includes EMC's GeoSynchrony operating environment running on top of a Linux kernel. The primary function of GeoSynchrony is to facilitate I/O[8] communication between the front-end hosts and the back-end storage arrays in a SAN using EMC's distributed cache coherency technology. The director software also collates and sends log messages to the management server for auditing and reporting purposes.

The management server software is based on the Novell SLES[9] 10 distribution and provides remote management capabilities for administrators to make configuration changes through the VPLEX CLI, API[10], and VPLEX management console. The VPLEX management console is a web GUI that is accessed by administrators over an IP[11] network. The API is accessed using user-created custom applications, referred to as RESTful web services or RESTful web APIs, that can interact with the management server to issue

[8] I/O – Input/Ouput
[9] SLES – SUSE Linux Enterprise Server
[10] API – Application Programming Interface
[11] IP – Internet Protocol

administrative commands. Each interface requires that administrators identify and authenticate themselves before the TOE performs any actions on their behalf.

In a Metro and Geo configuration, administrators can manage data centers in different locations through a single interface from any management server within the configuration. In the deployment scenario presented in Figure 2, for example, an administrator can perform configuration changes to Cluster B through the management server in Cluster A and vice versa.

The VPLEX Witness connects to and monitors the VPLEX clusters in the Geo and Metro configuration via SSH[12]. The VPLEX Witness monitors the VPLEX clusters in the Geo and Metro configurations. By reconciling its own observations with the information reported periodically by the clusters, the VPLEX Witness enables the cluster(s) to distinguish between inter-cluster failures and cluster failures and automatically resume I/O in these situations.

The TOE facilitates the management user data by applying a three-tiered, logical abstraction to encapsulate traditional storage array devices. The TOE aggregates *Extents*, or storage volumes, into *Devices* using RAID[13] schemes. *Virtual Volumes*, the uppermost tier in the VPLEX storage abstraction, are made up of one or more Devices. The Virtual Volumes are exposed to the hosts connected to the SAN as "pools" of logical volumes[14]. Administrators configure which hosts have access to which Virtual Volumes based on the parameters discussed in Section 7.1.2.

Figure 3 below illustrates the three-tier abstraction the TOE uses to give end-users access to the user data within its scope of control.

[12] SSH – Secure Shell
[13] RAID – Redundant Array of Independent Disks
[14] See Section 9.2 for definitions of Extent, Device, and Virtual Volume and "pool".

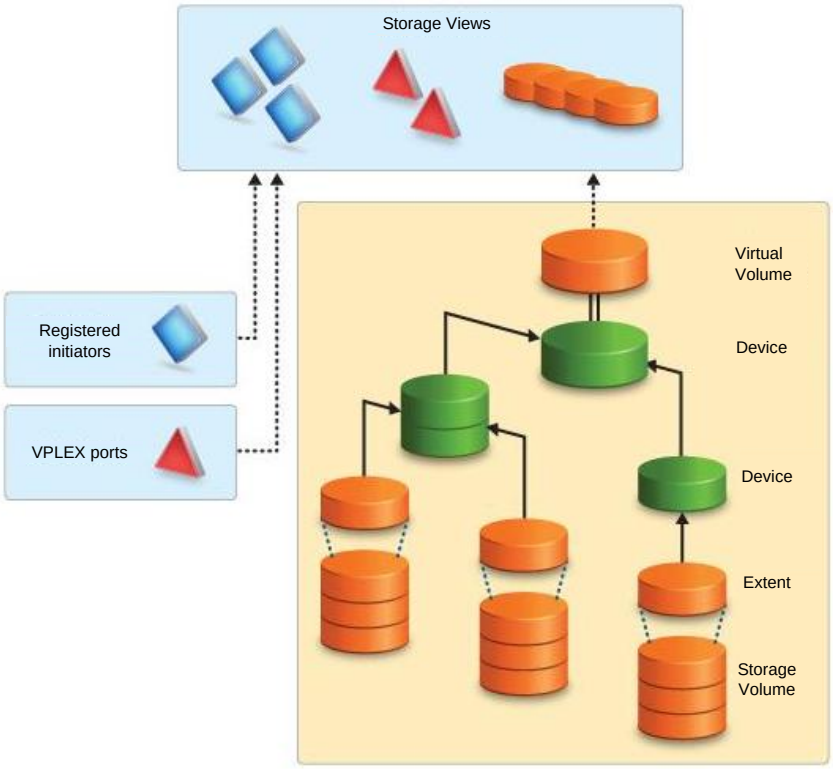

Figure 3 - Three-Tier Storage Abstraction

1.3.1 User Data Access

Access to user data controlled by the TOE is managed using VPLEX's "Storage View," a logical construct that unifies the following components to determine access permissions:

- **Registered initiators** – hosts with HBA[15]s installed that are connected to VPLEX through the front-end SAN.
- **VPLEX Ports** – the front-end ports physically located on the VPLEX directors that are exposed to the hosts.
- **Virtual Volumes** – logical storage volumes constructed from the back-end storage arrays connected to VPLEX. Hosts are presented with Virtual Volumes when accessing the data controlled by the TOE.

A Storage View defines which hosts can access which Virtual Volumes on which VPLEX ports. A Storage View consists of at least one each of a registered initiator, a VPLEX port, and a Virtual Volume.

1.3.2 TOE Environment

The evaluated deployment configuration of the TOE requires the following environmental components in order to function properly:

- Front-end and back-end SAN fabrics to allow hosts to connect to the TOE and access storage,
- A WAN with SSH to facilitate communication between the clusters and the VPLEX Witness

[15] HBA – Host Bus Adapter

- Hosts requesting access to the storage arrays within the TOE's scope of control
- Storage arrays controlled by the TOE and accessed by the hosts
- Cables and connectors that allow the devices to connect to the SANs and WANs, and
- VMware ESX v4.0 or higher host deployed in a failure domain to host the VPLEX Witness
- An administrator workstation with access to the management server that satisfies the following software requirements:
    - Windows OS
    - PuTTY (version 0.60 or later or similar SSH client) to connect to the CLI
    - Web browser (Firefox v3.5.5 or v3.5.7, or Internet Explorer 7) and Adobe Flash Player 10.0.0 or higher to connect to the GUI

The TOE is intended to be deployed in a physically secure cabinet room or data center with the appropriate level of physical access control and physical protection (e.g., fire control, locks, alarms, etc.) The TOE is intended to be managed by administrators operating under a consistent security policy.

1.4 TOE Description

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

1.4.1 Physical Scope

Figure 4 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE's physical boundary consists of the director software, management server software, and the VPLEX Witness software. The TOE is implemented as depicted in the figure below.

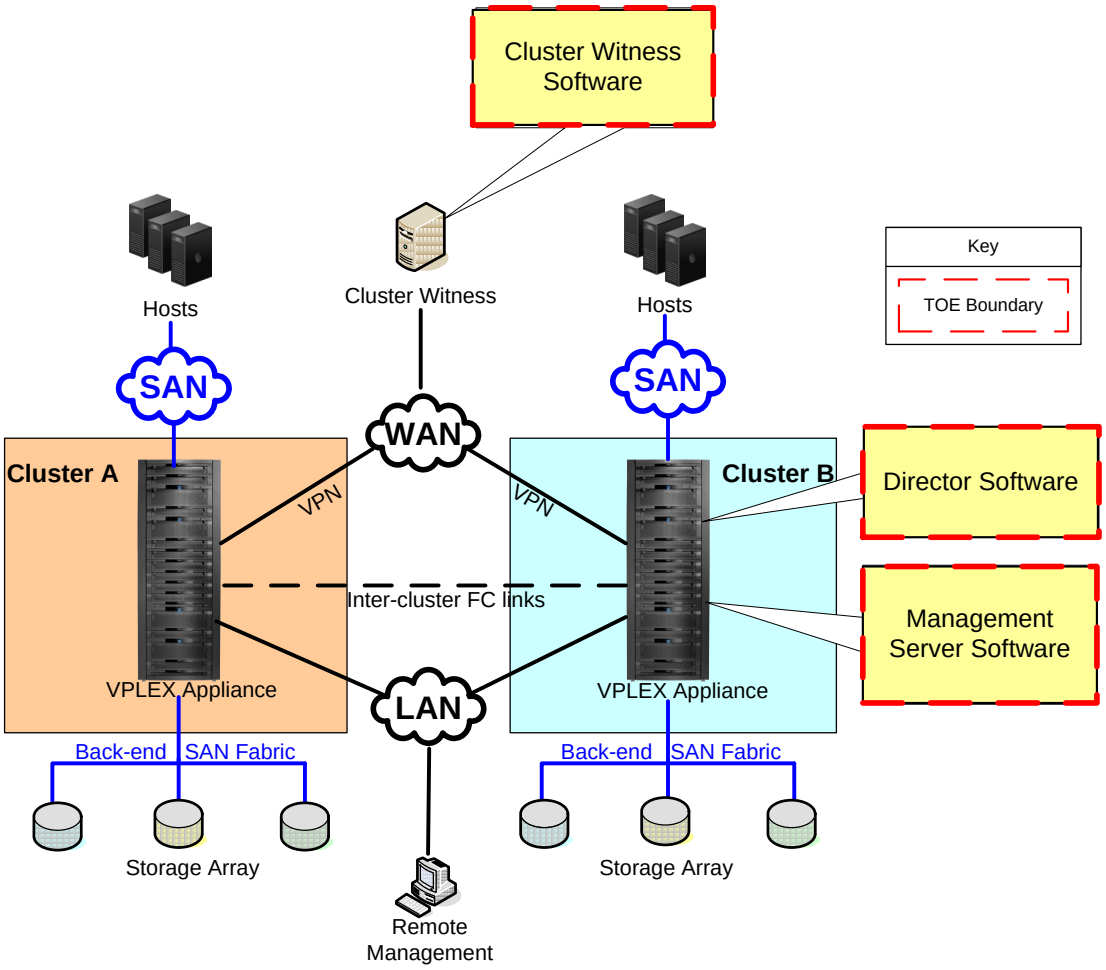

Figure 4 - Physical TOE Boundary

1.4.1.1 Guidance Documentation

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

- EMC® VPLEX™ Getting Started Guide
- EMC® VPLEX™ with GeoSynchrony™ 5.0 Product Guide
- Implementation and Planning Best Practices for EMC® VPLEX™ Technical Notes
- EMC® VPLEX™ with GeoSynchrony™ 5.0.1 Release Notes
- EMC® VPLEX™ with GeoSynchrony™ 5.0 Configuration Guide
- EMC® VPLEX™ Hardware Installation Guide
- EMC® VPLEX™ with GeoSynchrony™5.0 CLI Guide
- EMC® VPLEX™ Security Configuration Guide
- EMC® VPLEX™ with GeoSynchrony™ 5.0 Management Console Help (online help)
- EMC® VPLEX™ with GeoSynchrony™ 5.0 Best Practices Guide

1.4.2 Logical Scope

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

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access

1.4.2.1 Security Audit

The TOE is capable of generating audit messages that administrators can review. Audit messages are collected in log files stored on the management server. Log files are maintained for administrative commands, VPN events, and director events.

1.4.2.2 User Data Protection

The TOE controls access to the storage that it provides to end-users. End-users access the storage only if an administrator has configured the TOE's Storage Access Control SFP[16] to allow them access to an area of storage. If administrators have not assigned permissions to an end- user for a storage area, then the end-user cannot access that storage.

1.4.2.3 Identification and Authentication

The TOE ensures that VPLEX administrators must identify themselves and authenticate their identities before accessing any of the functionality available on the management server. Administrators must authenticate before accessing both the web GUI, the API, and the CLI.

1.4.2.4 Security Management

The TOE provides administrators with the ability to manage the behavior of security functions and security attributes. Administrators are assigned one of two roles: Administrator or Service. The TOE allows administrators to manage the attributes associated with the Storage Access Control SFP.

1.4.2.5 Protection of the TSF

The TOE provides both external and internal failover capabilities. Redundant front-end and back-end connections and the VPLEX Witness ensure that a failure of a director, engine, or an entire cluster does not hinder VPLEX functionality or access to the data stores.

The TOE provides consistency for replicated TSF data on metadata volumes located on back-end storage arrays connected to VPLEX. This redundancy provides the ability to resynchronize the metadata on the functioning volume with the replicated volume when it is recovered.

1.4.2.6 TOE Access

The TOE terminates an administrative user session after a set period of administrator inactivity.

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

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

- The VPLEX hardware components
- The hardware and VMware ESX host that the VPLEX Witness runs on
- ConnectEMC call home feature

[16] SFP – Security Functional Policy

- LDAP/LDAPS authentication of administrators
- SNMP[17] Functionality

[17] SNMP – Simple Network Management Protocol

2 Conformance Claims

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

Table 2 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2011/05/01 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

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

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

3.1 Threats to Security

This section identifies the threats to the IT[18] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

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

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[19] and 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. Table 3 below lists the applicable threats.

Table 3 - Threats

Name	Description
T.IA	Threat agents may attempt to compromise the TOE or network resources controlled by the TOE by attempting actions that they are not authorized to perform on the TOE or network resources.
T.IMPROPER_CONFIG	The TOE could be misconfigured by an administrator to provide improper storage or enforce improper access to user data.
T.UNAUTH	An unauthorized user could access data stored by the TOE by bypassing the protection mechanisms of the TOE.
T.DATA_AVAILABILITY	User data could become unavailable due to hardware failure or threat agents performing malicious, incorrect system operations.
T.NO_AUDIT	Threat agents may perform security-relevant operations on the TOE without being held accountable for it.

3.2 Organizational Security Policies

There are no Organizational Security Policies defined for this ST.

[18] IT – Information Technology
[19] TSF – TOE Security Functionality

3.3 Assumptions

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

Table 4 - Assumptions

Name	Description
A.PHYSICAL	It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrators only.
A.CONNECTIVITY	It is assumed that the IT Environment will be configured in such a way as to allow TOE users to access the information stored on the TOE.
A.TIMESTAMP	It is assumed that the IT environment provides the TOE with the necessary reliable timestamps.
A.SECURE_CONFIG	It is assumed that the TOE will be implemented in a SAN environment that is securely configured.
A.MANAGE	It is assumed that there are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	It is assumed that the users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.SECURE_CONNECT	It is assumed that remote session connections are secured by the IT environment.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

Table 5 - Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record events of security relevance at the "not specified" level of audit. The TOE must provide authorized administrators with the ability to review the audit trail.
O.FAIL_PRO	The TOE shall preserve a secure and functional operating state when a director, engine, or an entire cluster fails.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUTHENTICATE	The TOE must be able to identify and authenticate administrative users prior to allowing access to TOE administrative functions and data.
O.STOR_ACC	TOE users will be granted access only to user data for which they have been authorized based on the security attributes associated with the Storage Access Control Policy.
O.STRONG_PWD	The TOE must ensure that all passwords will be at least 8 characters in length and will consist of numbers and alphabetic characters. Password construction must be complex enough to avoid use of passwords that are easily guessed or otherwise left vulnerable, e.g. names, dictionary words, phone numbers, birthdays, etc. should not be used. Passwords must be compared against previous passwords to check for palindromes, case-only changes, and password similarity to prevent use of old passwords with slight changes. The TOE must obscure passwords so that they are unreadable when being entered at the management interfaces.
O.INACTIVE	The TOE will terminate an inactive management session after a set interval of time.
O.TIMESTAMP	The TOE will provide a reliable timestamp for audit purposes.
O.CONSISTENCY	The TOE must ensure that, when a replicated volume fails or is disconnected from the system, the consistency of the data on the volume remains intact when it is brought back online.
O.ADMIN_ROLES	The TOE must provide administrative roles to isolate administrative actions. The TOE must maintain the username, password, and role attributes for all administrative users and ensure that only secure

Name	Description
	values are accepted for each of these attributes.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

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

Table 6 - IT Security Objectives

Name	Description
OE.SECURE_SERVERS	The TOE Environment must provide properly configured authentication servers and host machines to communicate with the TOE.
OE.AUTH_HOSTS	The IT Environment will ensure that only authorized hosts systems are attached to the SAN in which the TOE is located.
OE.NTP	The IT Environment will aid the TOE in providing reliable time stamps by implementing the Network Time Protocol (NTP).
OE.TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.
OE.SECURE_COMMUNICATIONS	The TOE Environment must ensure that external systems and devices communicate securely with the TOE when they are connected to the TOE through front-end and back-end Storage Area Networks.
OE.SECURE_REMOTE	The TOE environment provides secure remote sessions for the Cluster Witness and Remote management sessions.

4.2.2 Non-IT Security Objectives

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

Table 7 - Non-IT Security Objectives

Name	Description
OE.MANAGE	Those responsible for the TOE must be competent TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE and the IT Environment critical to security policy are protected

Name	Description
	from any physical attack that might compromise the IT security objectives.
OE.NOEVIL	Sites using the TOE shall ensure that TOE administrators are not careless, negligent, or willfully hostile, and follow all guidance.

5 Extended Components

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

5.1 Extended TOE Security Functional Components

This section specifies the extended SFR for the TOE. The extended SFR is organized by class. Table 8 identifies the extended SFR implemented by the TOE. The rationale for this extended component is described in Section 8.3.

Table 8 - Extended TOE Security Functional Requirements

Name	Description
EXT_FPT_RTC.1	Replicated TSF data consistency

5.1.1 Class EXT_FPT: Protection of the TSF

Families in this class address the requirements related to the protection of the TSF data. The extended family "EXT_FPT_RTC: Replicated TSF data consistency" was modeled after FPT_TRC.

5.1.1.1 Replicated TSF Data Consistency (EXT_FPT_RTC)

Family Behavior

This extended component defines the set of rules in which the VPLEX with GeoSynchrony 5.0 uses to ensure replicated TSF data consistency.

Component Leveling

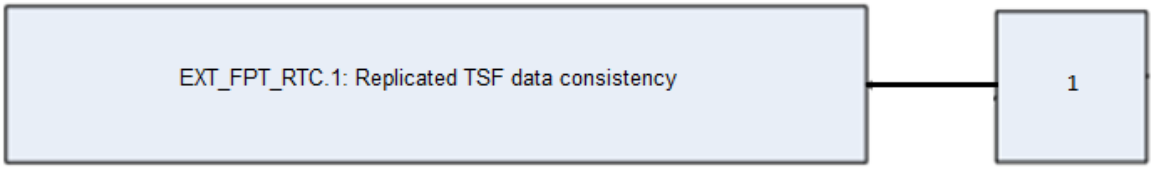

Figure 5 - Replicated TSF Data Consistency class decomposition

EXT_FPT_RTC.1 Replicated TSF Data Consistency defines that TSF data shall maintain consistency when replicated between trusted IT products controlled by the TOE. It was modeled after FPT_TRC.1.

Management: EXT_FPT_RTC.1

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

a) The management of the VPLEX metadata volumes that store the replicated TSF data

Audit: EXT_FPT_RTC.1

a) There are no auditable events

EXT_FPT_RTC.1 Replicated TSF data consistency

Hierarchical to: No other components.

FPT_RTC.1.1

The TSF shall ensure that TSF data is consistent when replicated between trusted IT products controlled by the TOE.

FPT_RTC.1.2

When the trusted IT products controlled by the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection.

Dependencies: FPT_ITC.1 Inter-TSF confidentiality during transmission

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

6 Security Requirements

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

6.1 Conventions

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

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

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

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User Identity Association				
FAU_SAR.1	Audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FIA_ATD.1	User attribute definition		✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.2	User authentication before any action				
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓	✓	
FMT_MSA.1	Management of security attributes	✓	✓		

Name	Description	S	A	R	I
FMT_MSA.2	Secure security attributes		✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of secure state		✓		
FPT_STM.1	Reliable time stamps				
FTA_SSL.1	TSF-initiated session locking		✓		
EXT_FPT_RTC.1	Replicated TSF data consistency				

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation
Hierarchical to: No other components.
FAU_GEN.1.1
The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*management server events, management console events, VPN events, and director events*].
FAU_GEN.1.2
The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association
Hierarchical to: No other components.
FAU_GEN.2.1
For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

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

6.2.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1
The TSF shall enforce the [*Storage Access Control SFP*] on
[
Subjects: hosts accessing storage controlled by the TOE,
Objects: storage space, and
Operations: read/write from storage
].

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 [*Storage Access Control SFP*] to objects based on the following:
[
Subject (hosts accessing storage controlled by the TOE) attributes:
- *Initiator Group*

Object (storage space) attributes:
- *Virtual Volume Group*
- *Port Group*

].
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 host can access a Virtual Volume if:
- *The host's registered initiator belongs to the Virtual Volume's Storage View,*

].
FDP_ACF.1.3
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].
FDP_ACF.1.4
The TSF shall explicitly deny access of subjects to objects based on the [*no additional rules*].
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

Application Note: Although it is a dependency for FDP_ACF.1, FMT_MSA.3 is not included in the evaluation because the Storage Access Control SFP security attributes do not have default values.

6.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
FIA_ATD.1.1
The TSF shall maintain the following list of security attributes belonging to individual users: [*username, password, and role*].
Dependencies: No dependencies

FIA_SOS.1 Verification of secrets
Hierarchical to: No other components.
FIA_SOS.1.1
The TSF shall provide a mechanism to verify that secrets meet [*the following password strength rules:*
a. The minimum password length shall be eight characters, including numbers
b. There shall be no dictionary words
c. New passwords will be compared to the previous password to check for palindromes, case-only changes, and password similarity and rotation to prevent use of old passwords with only a slight change].
Dependencies: No dependencies

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_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
FIA_UAU.7.1
The TSF shall provide only [*obscured feedback*] to the user while the authentication is in progress.
Dependencies: FIA_UAU.1 Timing of authentication

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

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1

The TSF shall restrict the ability to [~~determine the behaviour of, disable, enable, modify the behaviour of~~ **perform**] the functions [*listed in the 'Security Functions Behavior Permissions' column of Table 10*] to [*the roles listed in the 'Role' column of Table 10*].

Table 10 - Management of Security Functions Behaviour by Role on Management Server

Role	Security Functions Behavior Permissions
Administrator	• create, modify, delete, reset TOE user accounts • start and stop management server services • access to the management server desktop, VPLEX CLI, and Management Console GUI • change own password • reset other users' passwords
Service	• inspect log files • upgrade firmware and software • start and stop management server services • access to the management server desktop, VPLEX CLI, and Management Console GUI • change own password

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

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1

The TSF shall enforce the [*restrictive role permissions*] to restrict the ability to [*perform the operations specified in the 'Security Attribute Permissions' column of Table 11 on]* the security attributes [*listed in the 'Security Attribute Permissions' column of Table 11*] to [*the roles listed in the 'Role' column of Table 11*].

Table 11 - Management of Security Attributes by Role

Role	Security Attribute Permissions
Administrator	Can perform all operations on all security attributes
Service	Change own password

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.2 Secure security attributes
Hierarchical to: No other components.
FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for [*username, password, and role*].

Dependencies: **[FDP_ACC.1 Subset access control or**
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [query, modify, delete, *[other operations as defined in column 'Operation' of Table 12]*] the [*TSF data as defined in column 'TSF Data' of Table 12*] to [*the authorized identified roles as defined in column 'Authorized Role' of Table 12*].

Table 12 - Management of TSF Data

Operation	TSF Data	Authorized Role
Create, Modify, Query, Delete	User accounts	Administrator
Reset	User passwords	Administrators, Service users can modify their own passwords only
Create, Modify, Delete	Configuration information for administrator defined: • Extents • Devices • Virtual Volumes • Storage Views	Administrator, Service
Register, Unregister	HBA information for hosts	Administrator, Service
View, Delete	Log files	Administrator, Service

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

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

Dependencies: **No Dependencies**

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Administrator and Service*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: **FIA_UID.1 Timing of identification**

6.2.5 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [*a director fails; an engine fails; a cluster fails; port fails*].
Dependencies: No dependencies.

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

EXT_FPT_RTC.1 Replicated TSF data consistency
Hierarchical to: No other components.
FPT_RTC.1.1
The TSF shall ensure that TSF data is consistent when replicated between trusted IT products controlled by the TOE.
FPT_RTC.1.2
When the trusted IT products controlled by the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection.
Dependencies: FPT_ITC.1 Inter-TSF confidentiality during transmission

6.2.6 Class FTA: TOE Access

FTA_SSL.1 TSF-initiated session locking

Hierarchical to: No other components.

FTA_SSL.1.1

The TSF shall lock an interactive session after [*10 minutes of administrator inactivity on the web GUI, 30 minutes of inactivity on the API, and 15 minutes of administrator inactivity on the CLI*] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the administrator's data access/display devices other than unlocking the session.

FTA_SSL.1.2

The TSF shall require the following events to occur prior to unlocking the session: [*administrator must re-enter password*].

Dependencies: FIA_UAU.1 Timing of authentication

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 13 - Assurance Requirements summarizes the requirements.

Table 13 - Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw Reporting Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

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

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 14 lists the security functions and their associated SFRs.

Table 14 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.2	Secure security attributes
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functions	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps
	EXT_FPT_RTC.1	Replicated TSF data consistency
TOE Access	FTA_SSL.1	TSF-initiated session locking

7.1.1 Security Audit

The TOE generates audit messages to keep a record of security related events. Audit messages are collected in log files stored in */var/log* on the management server. Log files are generated for:

- Actions taken by administrators at the management interfaces
- Management server events
- VPN events
- Director events

Administrative users are associated with the actions they take by the file name of the session log that is generated. For example, commands entered at the management console by the **admin** user will generate a *session.log_admin* file. Table 15 below presents the locations on the management server where the various security-related audit logs are stored.

Table 15 - Security Log File Location

Component	Location
Management Console	/var/log/VPlex/cli/session.log_<*username*>
Management server OS	/var/log/messages
VPN	/var/log/events.log
Director	/var/log/VPlex/cli/firmware.log

The TOE audit records contain the information described in Table 16 below.

Table 16 - Audit Record Contents

Field	Content
Date	Date that the audit record was created in YYY-MM-DD format.
Time	Time that the audit record was created in HH:MM:SS format.
Command	Action taken and outcome.

Audit records can be viewed by all VPLEX user roles listed in Table 10. The audit records are protected from unauthorized modification or deletion since only those users listed in Table 10 have access to them on the VPLEX management server.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1.

7.1.2 User Data Protection

The TOE enforces a Storage Access Control Policy on devices attempting to read from or write to the storage that the TOE controls. Access via the Storage Access Control Policy is based on VPLEX's Storage View. The Initiator Group, Port Group, and Virtual Volume Group attributes are used to determine access permissions.

- The Initiator Group consists of registered initiators that contain the WWPN[20] of the HBAs in the hosts connected to the VPLEX.
- The Port Group consists of the front-end ports physically located on the VPLEX directors.
- The Virtual Volume Group consists of one or more VPLEX Virtual Volumes.

Hosts, through their registered initiators, access the Virtual Volumes through the ports within the same Storage View. A host will not have access to the data controlled by the TOE if it is not part of the same Storage View as the Virtual Volume that contains the requested data. Please see Section 1.3.1 for more information about Storage Views.

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

7.1.3 Identification and Authentication

VPLEX administrative users must first be identified and authenticated before they can perform any administrative action against the TOE. Identification and authentication is performed locally by the TOE. Usernames, roles, and hashed passwords are stored on the management server.

The VPLEX management server enforces minimum password requirements using a pluggable authentication module (PAM). Password feedback is obscured by asterisks when entered at the web GUI and blank characters when entered at the CLI.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2.

7.1.4 Security Management

The TOE provides three management interfaces for administrators: a CLI, an API, and a GUI. The GUI is accessed through a web browser on an administrator workstation. The CLI is accessed through an SSH client, such as OpenSSH and PuTTY, from an administrator workstation. The API is accessed over HTTPS[21] using custom applications running on an administrator workstation.

The CLI provides administrators with the ability to perform all management functions. The API provides most of the administrative commands allowed by the CLI. However, session aware commands, such as the commands to upload or download files to and from the management server, are blocked. The web GUI provides only the following functions:

- System status summary
- Storage provisioning capabilities, including the ability to create/delete/modify Extents, Devices, Virtual Volumes, and Storage Views
- Data mobility
- Performance monitoring

The TOE presents two roles to administrators: Administrator and Service. These roles have varying permissions that are described in Table 10 and Table 12. The TOE ensures that only secure values are accepted for the username, password, and role security attributes. The Administrator role can modify all security attributes of all administrative users and the Service role can only modify its own password.

All administrator roles can manage and modify the subject and object security attributes associated with the Storage Access Control SFP. All administrator roles can create, modify, and delete the parameters used to determine front-end host access to back-end storage volumes connected to VPLEX. See Section 7.1.2 for more information about how administrators can manage the Storage Access Control SFP.

[20] WWPN – World Wide Port Name
[21] HTTPS – Hypertext Transfer Protocol Secure

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

The TOE preserves a secure state when a single component fails. Failure protection is achieved through multiple data paths on redundant ports, directors, engines, and clusters. VPLEX also physically connects redundantly to back-end and front-end SAN fabrics. This data path redundancy, along with the failure protection provided by the VPLEX Witness, ensures that a single failure in any of these components will not affect the availability or the integrity of the data controlled by the TOE.

The TOE provides consistency when TSF data is replicated between parts of the TOE. TSF data is stored as metadata on storage volumes located in the storage arrays connected to the TOE. Metadata includes information specific to each VPLEX Cluster, such as virtual-to-physical mapping information, data about Devices and Virtual Volumes, and system configuration settings. The metadata is mirrored across two different Devices provisioned from two different arrays. Each director in the cluster has access to both metadata Devices. Each cluster in the Metro and Geo configurations has its own independent pair of metadata Devices.

The TOE provides timestamps used to generate audit events. It obtains the timestamps from the system clock. The system clock retrieves its time from an external NTP server.

TOE Security Functional Requirements Satisfied: FPT_FLS.1, FPT_STM.1, EXT_FPT_RTC.1.

7.1.6 TOE Access

The TOE automatically locks administrative user sessions after a predefined period of inactivity. Administrators are signed out of CLI sessions after 15 minutes of inactivity, GUI sessions after 10 minutes of inactivity, and API sessions after 30 minutes of inactivity. Administrators must re-authenticate by re-entering their usernames and passwords before they can continue to perform the management functions of the TOE.

TOE Security Functional Requirements Satisfied: FTA_SSL.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Parts 2 and 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 Revision 3 with the addition of the EXT_FPT_RTC extended requirement. The extended requirement "EXT_FPT_RTC: Replicated TSF data consistency" was modeled after the Protection of the TSF (FPT) class.

There are no protection profile claims for this ST.

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

Table 17 below provides a mapping of the objects to the threats they counter.

Table 17 - Threats:Objectives Mapping

Threats	Objectives	Rationale
T.IA Threat agents may attempt to compromise the TOE or network resources controlled by the TOE by attempting actions that they are not authorized to perform on the TOE or network resources.	O.AUTHENTICATE The TOE must be able to identify and authenticate administrative users prior to allowing access to TOE administrative functions and data.	O.AUTHENTICATE counters this threat by requiring that administrators identify and authenticate themselves before any actions can be taken.
	O.ADMIN_ROLES The TOE must provide administrative roles to isolate administrative actions. The TOE must maintain the username, password, and role attributes for all administrative users and ensure that only secure values are accepted for each of these attributes.	O.ADMIN_ROLES counters this threat by maintaining administrative roles and restricting what functions administrators can perform based on their role.
T.IMPROPER_CONFIG The TOE could be misconfigured by an administrator to provide improper storage or enforce improper access to user data.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN counters this threat by ensuring that only authorized users, following proper procedures, may configure the TOE security mechanisms.
T.UNAUTH An unauthorized user could access	O.AUTHENTICATE The TOE must be able to identify	O.AUTHENTICATE counters this threat by requiring that

Threats	Objectives	Rationale
data stored by the TOE by bypassing the protection mechanisms of the TOE.	and authenticate administrative users prior to allowing access to TOE administrative functions and data.	administrators identify and authenticate themselves before any actions can be taken.
	O.STOR_ACC TOE users will be granted access only to user data for which they have been authorized based on the security attributes associated with the Storage Access Control Policy.	O.STOR_ACC counters this threat by ensuring that end-users only have access to the user data controlled by the TOE for which they have been permitted to access under the Storage Access Control SFP.
	O.STRONG_PWD The TOE must ensure that all passwords will be at least 8 characters in length and will consist of numbers and alphabetic characters. Password construction must be complex enough to avoid use of passwords that are easily guessed or otherwise left vulnerable, e.g. names, dictionary words, phone numbers, birthdays, etc. should not be used. Passwords must be compared against previous passwords to check for palindromes, case-only changes, and password similarity to prevent use of old passwords with slight changes. The TOE must obscure passwords so that they are unreadable when being entered at the management interfaces.	O.STRONG_PWD counters this threat by requiring that passwords be eight characters long and contain numbers, upper and lower-case letters, and special characters. Passwords are obscured when entered at the management interfaces.
	O.INACTIVE The TOE will terminate an inactive management session after a set interval of time.	O.INACTIVE counters this threat by terminating an administrative session after ten minutes of inactivity at the GUI, 15 minutes of inactivity at the CLI, and 30 minutes of inactivity at the API.
	O.ADMIN_ROLES The TOE must provide administrative roles to isolate administrative actions. The TOE must maintain the username, password, and role attributes for all administrative users and ensure that only secure values are accepted for each of these attributes.	O.ADMIN_ROLES counters this threat by ensuring that administrators can only perform the actions that their assigned role permits.
T.DATA_AVAILABILITY	O.FAIL_PRO	O.FAIL_PRO counters this threat

Threats	Objectives	Rationale
User data could become unavailable due to hardware failure or threat agents performing malicious, incorrect system operations.	The TOE shall preserve a secure and functional operating state when a director, engine, or an entire cluster fails.	by providing redundant paths between components of the TOE and the IT Environment to ensure that the failure of a director, engine, or cluster does not impede user access to data.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN counters this threat by allowing administrators to properly configure the mechanisms of the TOE that prevent loss of data availability.
	O.CONSISTENCY The TOE must ensure that, when a replicated volume fails or is disconnected from the system, the consistency of the data on the volume remains intact when it is brought back online.	O.CONSISTENCY counters this threat by ensuring that failed storage volumes that are brought back online are resynchronized to ensure they contain consistent data when part of a RAID 1 Device.
T.NO_AUDIT Threat agents may perform security-relevant operations on the TOE without being held accountable for it.	O.AUDIT The TOE must record events of security relevance at the "not specified" level of audit. The TOE must provide authorized administrators with the ability to review the audit trail.	O.AUDIT counters this threat by ensuring that an audit trail of management events is generated and maintained by the TOE. Administrators are associated with the actions they take. Audit logs are reviewable by authorized administrators.
	O.TIMESTAMP The TOE will provide a reliable timestamp for audit purposes.	O.TIMESTAMP counters this threat by ensuring that accurate timestamps are provided for all audit records, allowing the order of events to be preserved.

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no Organizational Security Policies defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 18 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 18 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.PHYSICAL	OE.PHYSICAL	OE.PHYSICAL satisfies this

Assumptions	Objectives	Rationale
It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrators only.	Those responsible for the TOE must ensure that those parts of the TOE and the IT Environment critical to security policy are protected from any physical attack that might compromise the IT security objectives.	assumption by ensuring that physical security is provided for the TOE.
A.CONNECTIVITY It is assumed that the IT Environment will be configured in such a way as to allow TOE users to access the information stored on the TOE.	OE.TRAFFIC The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.TRAFFIC satisfies the assumption by ensuring that the IT Environment is configured appropriately to allow users to access data controlled by the TOE.
A.TIMESTAMP It is assumed that the IT environment provides the TOE with the necessary reliable timestamps.	OE.NTP The IT Environment will aid the TOE in providing reliable time stamps by implementing the Network Time Protocol (NTP).	OE.NTP satisfies the assumption that the IT Environment will provide reliable timestamps by using NTP.
A.SECURE_CONFIG It is assumed that the TOE will be implemented in a SAN environment that is securely configured.	OE.SECURE_SERVERS The TOE Environment must provide properly configured authentication servers and host machines to communicate with the TOE.	OE.SECURE_SERVERS satisfies the assumption that authentication servers used by the TOE and hosts connected to the TOE are configured properly.
	OE.AUTH_HOSTS The IT Environment will ensure that only authorized hosts systems are attached to the SAN in which the TOE is located.	OE.AUTH_HOSTS satisfies the assumption by connecting only authorized hosts to the SAN in which the TOE is located.
	OE.SECURE_COMMUNICATIONS The TOE Environment must ensure that external systems and devices communicate securely with the TOE when they are connected to the TOE through front-end and back-end Storage Area Networks.	OE.SECURE_COMMUNICATIONS satisfies the assumption that TOE components will communicate with each other in a secure SAN environment.
A.MANAGE It is assumed that there are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Those responsible for the TOE must be competent TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption by ensuring that those responsible for the TOE provide competent individuals to perform management of the security of the environment.
A.NOEVIL It is assumed that the users who manage the TOE are non-hostile,	OE.NOEVIL Sites using the TOE shall ensure that TOE administrators are not	OE.NOEVIL satisfies the assumption by ensuring that administrators are not careless,

Assumptions	Objectives	Rationale
appropriately trained, and follow all guidance.	careless, negligent, or willfully hostile, and follow all guidance.	negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.SECURE_CONNECT It is assumed that remote session connections are secured by the IT environment.	OE.SECURE_REMOTE The TOE environment provides secure remote sessions for the Cluster Witness and Remote management sessions.	OE.SECURE_REMOTE satisfies the assumptions that the IT Environment provides a secure connection for remote sessions with the TOE.

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

EXT_FPT_RTC.1: Replicated TSF data consistency was created to address the TOE's capability to ensure that replicated TSF data stored on external, trusted IT products controlled by the TOE is maintained in a consistent manner and that, should one of the replicated volumes fail, the TSF data on the surviving volume will be resynchronized with the failed volume once it is recovered.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this ST.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 19 below shows a mapping of the objectives and the SFRs that support them.

Table 19 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must record events of security relevance at the "not specified" level of audit. The TOE must provide authorized administrators with the ability to review the audit trail.	FAU_GEN.1 Audit Data Generation	The requirement supports O.AUDIT by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User Identity Association	This requirement supports O.AUDIT by associating auditable events with the users who performed them.
	FAU_SAR.1	This requirement supports

Objective	Requirements Addressing the Objective	Rationale
	Audit review	O.AUDIT by requiring the TOE to make the recorded audit records available for review.
	FAU_STG.1 Protected audit trail storage	The requirement supports O.AUDIT by ensuring that the TOE protects the audit data from unauthorized deletion.
O.FAIL_PRO The TOE shall preserve a secure and functional operating state when a director, engine, or an entire cluster fails.	FPT_FLS.1 Failure with preservation of secure state	The requirement supports O.FAIL_PRO by ensuring that the TOE preserves a secure state when a director, engine, or cluster fails.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_MOF.1 Management of security functions behaviour	The requirement supports O.ADMIN by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MSA.1 Management of security attributes	The requirement supports O.ADMIN by ensuring that the TOE restricts modification of administrator security attributes to only those administrators with the appropriate roles.
	FMT_MTD.1 Management of TSF data	The requirement supports O.ADMIN by ensuring that the TOE restricts modification of TSF data to only those administrators with the appropriate roles.
	FMT_SMF.1 Specification of management functions	The requirement supports O.ADMIN by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
O.AUTHENTICATE The TOE must be able to identify and authenticate administrative users prior to allowing access to TOE administrative functions and data.	FIA_UAU.2 User authentication before any action	The requirement supports O.AUTHENTICATE by ensuring that administrators are authenticated before access to TOE administrative functions is allowed.
	FIA_UID.2 User identification before any action	The requirement supports O.AUTHENTICATE by ensuring that administrators are authenticated before access to TOE administrative functions is allowed.
O.STOR_ACC TOE users will be granted access	FDP_ACC.1 Subset access control	This requirement supports O.STOR_ACC by enforcing an

Objective	Requirements Addressing the Objective	Rationale
only to user data for which they have been authorized based on the security attributes associated with the Storage Access Control Policy.		access control policy that ensures that only authorized hosts gain access to the user data controlled by the TOE.
O.STOR_ACC TOE users will be granted access only to user data for which they have been authorized based on the security attributes associated with the Storage Access Control Policy.	FDP_ACF.1 Security attribute based access control	This requirement supports O.STOR_ACC by enforcing an access control policy that ensures that only authorized hosts gain access to the user data controlled by the TOE.
O.STRONG_PWD The TOE must ensure that all passwords will be at least 8 characters in length and will consist of numbers and alphabetic characters. Password construction must be complex enough to avoid use of passwords that are easily guessed or otherwise left vulnerable, e.g. names, dictionary words, phone numbers, birthdays, etc. should not be used. Passwords must be compared against previous passwords to check for palindromes, case-only changes, and password similarity to prevent use of old passwords with slight changes. The TOE must obscure passwords so that they are unreadable when being entered at the management interfaces.	FIA_SOS.1 Verification of secrets	The requirement supports O.STRONG_PWD by ensuring that the TOE protects itself from unauthorized access by enforcing password strength rules.
	FIA_UAU.7 Protected authentication feedback	This requirement supports O.STRONG_PWD by obscuring passwords characters when an administrator enters them during authentication.
O.INACTIVE The TOE will terminate an inactive management session after a set interval of time.	FTA_SSL.1 TSF-initiated session locking	The requirement supports O.INACTIVE by terminating an administrative session after ten minutes of inactivity at the GUI, 15 minutes of inactivity at the CLI, and 30 minutes of inactivity at the API.
O.TIMESTAMP The TOE will provide a reliable timestamp for audit purposes.	FPT_STM.1 Reliable time stamps	The requirement supports O.TIMESTAMP by ensuring that the TOE provides a reliable timestamp for audit purposes using the NTP protocol.
O.CONSISTENCY The TOE must ensure that, when a replicated volume fails or is disconnected from the system, the consistency of the data on the volume remains intact when it is	EXT_FPT_RTC.1 Replicated TSF data consistency	The requirement supports O.CONSISTENCY by ensuring that the TOE maintains data consistency when a failed replicated volume is recovered.

Objective	Requirements Addressing the Objective	Rationale
brought back online.		
O.ADMIN_ROLES The TOE must provide administrative roles to isolate administrative actions. The TOE must maintain the username, password, and role attributes for all administrative users and ensure that only secure values are accepted for each of these attributes.	FIA_ATD.1 User attribute definition	This requirement supports O.ADMIN_ROLES by maintaining security attributes of administrative users.
	FMT_MSA.2 Secure security attributes	The requirement supports O.ADMIN_ROLES by ensuring that the TOE requires secure values for administrator security attributes.
	FMT_SMR.1 Security roles	The requirement supports O.ADMIN_ROLES by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.

8.5.2 Security Assurance Requirements Rationale

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

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

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 20 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 20 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.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.

SFR ID	Dependencies	Dependency Met	Rationale
	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FMT_MSA.3	Not applicable	FMT_MSA.3 is not included because the Storage Access Control SFP security attributes do not have default values.
	FDP_ACC.1	✓	
FIA_ATD.1	No Dependencies	Not applicable	
FIA_SOS.1	No dependencies	Not applicable	
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_UAU.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1, is included. This satisfies this dependency.
FIA_UID.2	No dependencies	Not applicable	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_ACC.1	✓	
FMT_MSA.2	FDP_ACC.1	✓	
	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	Not applicable	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2,

SFR ID	Dependencies	Dependency Met	Rationale
			which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FPT_FLS.1	No dependencies	Not applicable	
FPT_STM.1	No dependencies	Not applicable	
FTA_SSL.1	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1, is included. This satisfies this dependency.
EXT_FPT_RTC.1	FPT_ITC.1	✓	FPT_ITC.1 is not included because the environment protects transmitted TSF data from disclosure, as stated by the OE.SECURE_COMMUNICATIONS environmental objective.

9 Acronyms and Terms

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

9.1 Acronyms

Table 21 - Acronyms

Acronym	Definition
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
FC	Fibre Channel
GUI	Graphical User Interface
HA	High Availability
HBA	Host Bus Adapters
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
I/O	Input/Output
IT	Information Technology
LAN	Local Area Network
NTP	Network Time Protocol
OS	Operating System
PAM	Pluggable Authentication Module
PP	Protection Profile
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SLES	SUSE Linux Enterprise Server
SNMP	Simple Network Management Protocol
SPS	Standby Power Supply
SSD	Solid State Drive

Acronym	Definition
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
UPS	Uninterrupted Power Supply
VPN	Virtual Private Network
WAN	Wide Area Network
WWPN	World Wide Port Name

9.2 Terminology

AccessAnywhere – Technology that enables VPLEX clusters to provide access to information between clusters that are separated by distance.

Administrative user (Administrator) – TOE users that have the capability to manage the TSF and user data controlled by the TOE.

Asynchronous – Describes objects or events that are not coordinated in time. A process operates independently of other processes, being initiated and left for another task before being acknowledged.

Device – A combination of one or more extents to which you add specific RAID properties. Devices use storage from one cluster only; Distributed Devices use storage from both clusters in a multi-cluster configuration.

End-user – TOE users that access the user data controlled by the TOE through the front-end hosts.

Extent – A range of blocks of a storage volume.

Fabric – The hardware that connects devices to storage arrays in a SAN.

Federation – A federated network consists of multiple computing and/or network providers agreeing upon standards of operation. In the context of the TOE, federation allows the TOE and the heterogeneous components (specifically the data storage components) of the IT environment to communicate seamlessly.

Pool – A group of one or more logical disks.

RAID – A technology that copies redundant data across an array of disks. This technique preserves data stored in a RAID in case one or more (depending on RAID type) of the drives in a RAID fails.

SAN – A SAN is a network architecture that allows remote storage to appear local to devices accessing that storage.

Synchronous – Describes objects or events that are coordinated in time. A process is initiated and must be completed before another task is allowed to begin.

Virtual Volumes – A Virtual Volume looks like a contiguous volume, but can be distributed over two or more storage volumes. Virtual Volumes are presented to hosts.

Prepared by:
Corsec Security, Inc.

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

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