EMC XtremIO® v4.0.2
Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 1906-000-D102
Version: 0.8
21 March 2016

Prepared For:

EMC Corporation
176 South Street
Hopkinton, MA, USA
01748

Prepared by:

EWA-Canada
1223 Michael Street
Ottawa, Ontario, Canada
K1J7T2

Common Criteria Consulting LLC
15804 Laughlin Ln
Silver Spring, MD, USA
20906

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

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

1.1 DOCUMENT ORGANIZATION

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

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

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

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

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

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

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

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

1.2 SECURITY TARGET REFERENCE

ST Title:	EMC XtremIO® v4.0.2 Security Target
ST Version:	0.8
ST Date:	21 March 2016

1.3 TOE REFERENCE

TOE Identification:	EMC XtremIO® v4.0.2 (Build 80)
TOE Developer:	EMC Corporation
TOE Type:	Other Devices and Systems

1.4 TOE OVERVIEW

EMC XtremIO® is an all-flash system providing storage for enterprise applications, based on a scale-out architecture. The system uses building blocks, called X-Bricks, which can be clustered together. The XtremIO Storage Array provides a very high level of performance that is consistent over time, system conditions and access patterns. It is designed for high granularity true random I/O. An XtremIO cluster scales from 40 TB to 320 TB of raw capacity.

XtremIO's array architecture is specifically designed to deliver the full performance potential of flash, while linearly scaling all resources such as CPU, RAM, SSDs, and host ports in a balanced manner. This allows the array to achieve any desired performance level, while maintaining consistency of performance that is critical to predictable application behavior.

Due to its content-aware storage architecture, XtremIO provides:

- Even distribution of data blocks, inherently leading to maximum performance and minimal flash wear
- Even distribution of metadata
- No data or metadata hotspots
- Easy setup and no tuning
- Advanced storage functionality, including Inline Data Deduplication and Compression, thin provisioning, advanced data protection (XDP), and snapshots

XtremIO is fully VAAI compliant, allowing vSphere server to offload I/O intensive work to the XtremIO array and provide accelerated storage vMotion, virtual machine provisioning, and thin provisioning functionality.

The system operation is controlled via a stand-alone dedicated server (using a proprietary hardened Linux OS), called the XtremIO Management Server (XMS). Each XtremIO cluster requires its own XMS host, which can be either a physical or a virtual server. The array continues operating if it is disconnected from the XMS, but cannot be configured or monitored.

The XMS enables you to control and manage the XtremIO cluster, including:

- Creating, formatting, and initializing new clusters
- Monitoring cluster health and events
- Monitoring cluster performance

- Collecting cluster performance statistics
- Providing GUI and CLI services to clients
- Implementing volume management and data protection groups operation logic
- Providing operational support functions such as stopping and starting the cluster or any of the Storage Controllers

Since the XMS is not in the data path, it can be disconnected from the XtremIO cluster without affecting the I/O. An XMS failure only affects monitoring and configuration activities, such as creating and deleting volumes.

The system GUI is implemented using a Java client. The GUI provides easy-to-use tools for performing most of the cluster operations (certain management operations must be performed using the CLI). Additionally, operations on multiple components, such as creating multiple volumes, can only be performed using the GUI.

The system's Command Line Interface (CLI) allows administrators and other XtremIO cluster users to perform supported management operations. It is preinstalled on the XMS and can be accessed using the standard SSH protocol or via CLI window in the GUI.

Users of the CLI and GUI must authenticate with the XMS before they may access controlled functions or data. Authentication is performed entirely within XMS. Individual user accounts are configured in XMS, and one of four roles is assigned to each user. The management capabilities provided to each user are determined by their role.

Enterprise systems access data on the XtremIO system via Fibre Channel (FC) or iSCSI interfaces. Volumes within XtremIO are only exposed to initiators that they have been mapped to, and may further be restricted by VLANs. CHAP may optionally be configured for authentication of initiators.

A representative deployment of XtremIO is shown in the following diagram.

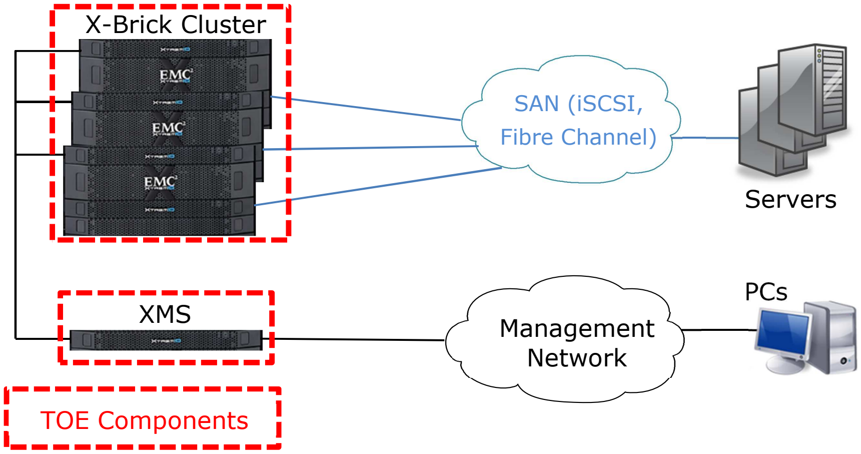

Figure 1 - EMC XtremIO Representative Deployment

The X-Bricks and XMS are delivered as physical appliances; the TOE includes both the hardware and software.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

An XtremIO system includes the following components:

- One instance of XMS executing on a physical appliance supplied by EMC
- One or more instances of 40 TB X-Bricks

All components of the X-Bricks and XMS, hardware and software, are included in the TOE boundary.

1.5.2 TOE Environment

Information is passed over the LAN between TOE components or with management workstations. User data is passed over the SAN. It is the responsibility of the Operational Environment to protect this traffic from unauthorized disclosure or modification.

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- *EMC XtremIO Storage Array Version 4.0 and 4.0.1 User Guide*
- *EMC XtremIO Storage Array Version 4.0 and 4.0.1 Security Configuration Guide*
- *EMC XtremIO Storage Array Version 4.0 and 4.0.1 Site Preparation Guide*
- *EMC XtremIO Common Criteria Supplement*

1.5.4 Logical Scope

Functional Classes	Description
Security Audit	Audit entries are generated for security related events, and can be reviewed by any authorized user of the TOE.
User Data Protection	The TOE mediates all data requests from Initiators to prevent unauthorized access to volumes. By default access to volumes is restricted. Authorized administrators may configure allowed mappings between Initiators and LUNs (volumes) via specified Targets.
Identification and Authentication	Users must identify and authenticate prior to TOE access.

Functional Classes	Description
Security Management	The TOE provides management capabilities via GUI and CLI interfaces. Multiple roles are supported to provide varying levels of access to data and functions.
TOE Access	User sessions may be terminated by users, or by the TOE if they are inactive longer than the configured inactivity limit. A configured banner is displayed to users during login.

Table 1 - Logical Scope of the TOE

1.5.5 Functionality Excluded from the Evaluated Configuration

In addition to the 40TB X-Bricks included in the evaluation, X-Bricks are also available on 5 TB, 10 TB and 20 TB systems.

In addition to the XMS executing on a physical appliance, XMS executing as a Virtual Machine is also supported on VMware ESXi 4.x, 5.x and 6.x.

As an option to performing credential validation in the TOE, user accounts may be integrated with external LDAP servers for credential validation.

The following product features are excluded from this evaluation:

- REST API
- High Availability
- Data at Rest Encryption (DARE)
- EMC Secure Remote Support (ESRS)
- Connect-Home
- OpenStack

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

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

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

As follows:

- CC Part 2 conformant
- CC Part 3 conformant

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

2.2 ASSURANCE PACKAGE CLAIM

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

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

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

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 2 lists the threats addressed by the TOE. Mitigation to the threats is through the objectives identified in Section 4.1 Security Objectives.

Threat	Description
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential unauthorized data accesses to go undetected.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.UNAUTH_ACCESS	A server may attempt to access user data (volumes) that it is not authorized to access.

Table 2 - Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed upon an organization in the operational environment. Table 3 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Table 3 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 4.

Assumptions	Description
A.LANNETWORK	The TOE components and management workstations will be interconnected by a segregated LAN that protects the intra-TOE management traffic from disclosure to or modification by untrusted systems or users.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTCT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.
A.SANNETWORK	The TOE and the servers accessing them will be interconnected by a segregated SAN that protects the user data traffic from disclosure to or modification by untrusted systems or users.

Table 4 – Assumptions

4 SECURITY OBJECTIVES

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

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

4.1 SECURITY OBJECTIVES FOR THE TOE

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

Security Objective	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for security relevant events.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.TIME	The TOE will maintain reliable timestamps.

Table 5 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

Security Objective	Description
OE.CREDEN	Those responsible for the TOE must ensure that all access

Security Objective	Description
	credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
OE.LANNETWORK	The operational environment will provide a segregated LAN that protects the intra-TOE and management traffic from disclosure to or modification by untrusted systems or users.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.SANNETWORK	The operational environment will provide a segregated SAN that protects the user data exchanged between servers and the TOE from disclosure to or modification by untrusted systems or users.

Table 6 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

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

	T.IMPCON	T.PRIVIL	T.UNAUTH_ACCESS	P.ACCACT	P.MANAGE	P.PROTECT	A.LANNETWORK	A.MANAGE	A.NOEVIL	A.PROTECT	A.SANNETWORK
O.ACCESS	X	X	X		X						
O.AUDITS				X							

	T.IMPCON	T.PRIVIL	T.UNAUTH_ACCESS	P.ACCACT	P.MANAGE	P.PROTECT	A.LANNETWORK	A.MANAGE	A.NOEVIL	A.PROTECT	A.SANNETWORK
O.EADMIN	X		X		X						
O.IDAUTH	X	X		X	X						
O.PROTCT		X			X						
O.TIME				X							
OE.CREDEN					X				X		
OE.INSTAL	X				X				X		
OE.LANNETWORK							X				
OE.PERSON					X			X			
OE.PHYCAL						X			X	X	
OE.SANNETWORK											X

Table 7 - Mapping Between Objectives, Threats, Organizational Security Policies, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

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

Threat: T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential unauthorized data accesses to go undetected.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing

		access to TOE functions and data.
	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
Rationale:	The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.	

Threat: T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
Rationale:	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.	

Threat: T.UNAUTH_ACCESS	A server may attempt to access user data (volumes) that it is not authorized to access.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.

	O.AUDITS	The TOE must record audit records for security relevant events.
Rationale:	The O.ACCESS objective only permits authorized access TOE data. The O.AUDITS objective supports O.ACCESS by requiring the TOE to record audit data for unauthorized access attempts.	

4.3.2 Security Objectives Rationale Related to Organizational Security Policies

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

Policy: **P.ACCACT**	Users of the TOE shall be accountable for their actions within the TOE.	
Objectives:	O.AUDITS	The TOE must record audit records for security relevant events.
	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.TIME	The TOE will maintain reliable timestamps.
Rationale:	The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.TIME objective supports this policy by providing a time stamp for insertion into the audit records. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.	

Policy: **P.MANAGE**	The TOE shall only be managed by authorized users.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.

	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
	OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
Rationale:	The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.	

Policy: **P.PROTCT**	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.	
Objectives:	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.	

4.3.3 Security Objectives Rationale Related to Assumptions

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

Assumption: A.LANNETWORK	The TOE components and management workstations will be interconnected by a segregated LAN that protects the intra-TOE management traffic from disclosure to or modification by untrusted systems or users.	
Objectives:	OE.LANNETWORK	The operational environment will provide a segregated LAN that protects the intra-TOE and management traffic from disclosure to or modification by untrusted systems or users.
Rationale:	The OE.LANNETWORK objective ensures that the management traffic will be protected by a segregated LAN.	

Assumption: A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	
Objectives:	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
Rationale:	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.	

Assumption: A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	
Objectives:	OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.

	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.	

Assumption: **A.PROTCT**	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.	
Objectives:	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.PHYCAL provides for the physical protection of the TOE software and the hardware on which it is installed.	

Assumption: **A.SANNETWORK**	The TOE and the servers accessing them will be interconnected by a segregated SAN that protects the user data traffic from disclosure to or modification by untrusted systems or users.	
Objectives:	OE.SANNETWORK	The operational environment will provide a segregated SAN that protects the user data exchanged between servers and the TOE from disclosure to or modification by untrusted systems or users.
Rationale:	The OE.SANNETWORK objective ensures that the user data exchanged with the TOE will be protected by a segregated SAN.	

5 EXTENDED COMPONENTS DEFINITION

This ST does not include extended security requirements.

6 SECURITY REQUIREMENTS

6.1 CONVENTIONS

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

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

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC, summarized in Table 8 - Summary of Security Functional Requirements.

Class	SFR	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback

Class	SFR	Name
	FIA_UID.1	Timing of identification
	FIA_USB.1	User-subject binding
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners

Table 8 - Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) [*Logins, Changes to TSF data*].

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, [*user specified parameters for configuration changes*].

6.2.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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.

7.2.1.1 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*all authorized users*] with the capability to read [*all audit records from the events log*] 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.

7.2.1.2 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

User Data Protection

6.2.2.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

Subjects: Initiators,

Objects: Targets, LUNs, and

Operations: Access].

6.2.2.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

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

Initiators: Initiator ID, VLAN, Supplied Target ID, Supplied CHAP Parameters (optional), Initiator CHAP Parameters;

Targets: Target ID, Target VLAN;

LUNs: Mapped Initiator Groups, Mapped Target Groups].

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

1. *An Initiator may access a Target if all of the following conditions are satisfied:*
    a. *The Supplied Target ID matches a configured Target ID;*

b. *The Initiator ID matches a configured Initiator ID;*
c. *No Target VLAN is configured for the Supplied Target ID, or the VLAN used by the Initiator matches the Target VLAN;*
d. *No Initiator CHAP Parameters are configured for the Initiator ID, or the Supplied CHAP Parameters match the Initiator CHAP Parameters.*

2. *An Initiator may access a LUN if all of the following conditions are satisfied:*
   a. *The Initiator may access the Target being used;*
   b. *The Initiator is included in the Initiator Group that the LUN is mapped to;*
   c. *The Target is included in the Target Group that the LUN is mapped to].*

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*access is denied if any condition in FDP_ACF.1.2 is not satisfied*].

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*Username, Password/Public Key, and Role*].

6.2.3.3 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*viewing the configured login banner*] on behalf of the user to be performed before the user is authenticated.

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

6.2.3.4 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [*userid/password and SSH Fingerprint*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*following:*

- *Userid/password is used for all GUI users;*
- *SSH Fingerprint is used for CLI users when fingerprint parameters are supplied when the SSH connection is established;*
- *Userid/password is used for CLI users when fingerprint parameters are not supplied when the SSH connection is established].*

6.2.3.5 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*dots or no echoed charters*] to the user while the authentication is in progress.

6.2.3.6 FIA_UID.1 Timing of identification

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [*viewing the configured login banner*] on behalf of the user to be performed before the user is identified.

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

6.2.3.7 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*Username and Role*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*attributes are bound to the user session upon successful login*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*attributes do not change during a user session*].

6.2.4 Security Management

6.2.4.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*Volume Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*Initiator CHAP Parameters, Target ID, Target VLAN, Mapped Initiator Groups, Mapped Target Groups*] to [*Read_only (query only), Configuration, and Admin*].

6.2.4.2 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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

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

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

6.2.4.3 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [query, modify, delete, [*create*]] the [*list of TSF data in the following table*] to [*the authorised identified roles in the following table*].

Role TSF Data	Admin	Configuration	Read_only
User Accounts	Query, Modify, Delete, Create	Query	None
User Session Parameters	Query, Modify	Query, Modify	Query
Clusters	Query, Modify, Delete, Create	Query	Query
Volumes	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query
Initiators	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query
Targets	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query
LUN Mappings	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query

Table 9 – TSF Data Access Permissions

6.2.4.4 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- *User management*
- *User session management*
- *Cluster management*
- *Volume management*
- *Initiator management*
- *Target management*
- *LUN mapping management*].

6.2.4.5 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Read_only, Configuration, and Admin*].

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

6.2.5 Protection of the TSF (FTP)

6.2.5.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.6 TOE Access (FTA)

6.2.6.1 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.6.2 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*time interval of user inactivity configured by a user with the Configure or Administrator role*].

6.2.6.3 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

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

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.PROTCT	O.TIME
FAU_GEN.1		X				
FAU_GEN.2		X				
FAU_SAR.1		X				
FAU_SAR.2		X				

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.PROTCT	O.TIME
FDP_ACC.1					X	
FDP_ACF.1					X	
FIA_ATD.1				X		
FIA_UAU.1	X			X		
FIA_UAU.5				X		
FIA_UAU.7	X			X		
FIA_UID.1	X			X		
FIA_USB.1	X					
FMT_MSA.1	X		X			
FMT_MSA.3					X	
FMT_MTD.1	X		X			
FMT_SMF.1			X			
FMT_SMR.1	X		X			
FPT_STM.1		X				X
FTA_SSL.3	X					
FTA_SSL.4	X					
FTA_TAB.1	X					

Table 10 – Mapping of SFRs to Security Objectives

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

Security Objective	**Rationale**
O.ACCESS	FIA_UID.1 and FIA_UAU.1 require users to complete the I&A process, which ensures only authorized users gain access and enables each user

Security Objective	Rationale
	session to be bound to a role to limit. FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE. FIA_USB.1 defines the user attributes that are bound to each user session upon session upon completion of the I&A process, enabling access restrictions to be properly enforced for each user session. FMT_MSA.1 and FMT_MTD.1 define the access permissions to TSF data for each role. FMT_SMR.1 ensures the TOE supports multiple roles so that appropriate data access can be provided to different users. FTA_SSL.3 and FTA_SSL.4 require session termination mechanisms to protect against idle sessions being used by unauthorized users. FTA_TAB.1 provides a mechanism to warn unauthorized users against unauthorized access.
O.AUDITS	FAU_GEN.1 and FAU_GEN.2 require audit records to be generated for specific events and define the contents of the records. FAU_SAR.1 and FAU_SAR.2 require the audit records to be available to all authorized users of the TOE, and for access to be restricted for unauthorized users. FPT_STM.1 requires accurate time stamps to be available for the audit records.
O.EADMIN	FMT_MSA.1 and FMT_MTD.1 define the access permissions required for each role for TSF data. FMT_SMF.1 specifies the management functionality required for effective management of the TOE. FMT_SMR.1 defines the roles required to provide effective management capabilities for different categories of users.
O.IDAUTH	FIA_UID.1 and FIA_UAU.1 require users to complete the I&A process, which ensures only authorized users gain access and defines their access permissions prior to completing the I&A process. FIA_UAU.5 defines the mechanisms provided by the TOE to authenticate users. FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE. FIA_ATD.1 specifies the security attributes that are supported for each defined user account.
O.PROTCT	FDP_ACC.1 and FDP_ACF.1 define the access control policy for LUN access by Initiators.

Security Objective	Rationale
	FMT_MSA.3 requires restrictive access to LUNs by default so that no access is granted until explicitly configured by authorized users.
O.TIME	FPT_STM.1 requires accurate time stamps to be available.

Table 11 – Security Objectives for the TOE

6.4 DEPENDENCY RATIONALE

Table 12 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependencies	Dependency Satisfied / Rationale
FAU_GEN.1	FPT_STM.1	Satisfied
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Satisfied Satisfied
FAU_SAR.1	FAU_GEN.1	Satisfied
FAU_SAR.2	FAU_SAR.1	Satisfied
FDP_ACC.1	FDP_ACF.1	Satisfied
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Satisfied Satisfied
FIA_ATD.1	None	n/a
FIA_UAU.1	FIA_UID.1	Satisfied
FIA_UAU.5	None	n/a
FIA_UAU.7	FIA_UAU.1	Satisfied
FIA_UID.1	None	n/a
FIA_USB.1	FIA_ATD.1	Satisfied
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1 FMT_SMF.1	Satisfied Satisfied Satisfied
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Satisfied Satisfied

SFR	Dependencies	Dependency Satisfied / Rationale
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Satisfied Satisfied
FMT_SMF.1	None	n/a
FMT_SMR.1	FIA_UID.1	Satisfied
FPT_STM.1	None	n/a
FTA_SSL.3	None	n/a
FTA_SSL.4	None	n/a
FTA_TAB.1	None	n/a

Table 12 - Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

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

The assurance requirements are summarized in Table 13.

Assurance Class	Assurance Components	
	Identifier	Name
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage

Assurance Class	**Assurance Components**	
	Identifier	**Name**
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw Reporting Procedures
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
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 13 - EAL 2+ Assurance Requirements

7 TOE SUMMARY SPECIFICATION

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

7.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

7.1.1 Security Audit

Audit records are generated for the events specified with FAU_GEN.1. Startup of the audit function is equivalent to a power on event. It is not possible to shut down the audit function. The following information is included in all audit records:

- Data and time of the event,
- Type of event,
- Subject identity (if applicable),
- (for configuration actions) the configuration parameters specified by the user.

Any authorized user may view any audit record via the CLI and GUI by displaying events with a category of "Audit".

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FPT_STM.1.

7.1.2 User Data Protection

Initiators are only permitted to access LUNs via authorized Targets and for which a LUN mapping has been explicitly configured. Target access may also be restricted to configured VLANs. Individual Initiators may optionally be required to provide CHAP authentication parameters.

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

7.1.3 Identification and Authentication

When GUI or CLI users initiate sessions, they must complete the login process. Prior to successful completion, the only controlled data or function they can access is viewing the configured banner. CLI users may supply fingerprint parameters when an SSH connection is established, or they must present a valid userid and password. GUI users always must present valid userid and password.

During collection of the password, only dots are echoed for each character supplied in the GUI. In the CLI, no characters are echoed.

Upon successful login, the user's username and role are bound to the session. These attributes do not change during the session.

TOE Security Functional Requirements addressed: FIA_ATD.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.7, FIA_UID.1, and FIA_USB.1.

7.1.4 Security Management

The GUI and CLI interfaces provide functionality for authorized users to manage the TOE. Each user session is bound to a role upon login, and that role determines access permissions as specified in FMT_MTD.1.

When volumes are created, initially no mappings to Initiators or Targets exist. Users with the Admin and Configuration roles have the ability to configure mappings to expose the volumes to Initiators.

TOE Security Functional Requirements addressed: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

7.1.5 TOE Access

Once a user has logged in, the session may be terminated by the user, or by the TOE if the session remains idle for more than the configured inactivity timer value.

Users with the Admin role has the ability to configure the banner to be displayed to users during login.

TOE Security Functional Requirements addressed: FTA_SSL.3, FTA_SSL.4, FTA_TAB.1.

8 TERMINOLOGY AND ACRONYMS

8.1 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
API	Application Program Interface
CC	Common Criteria
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CPU	Central Processing Unit
DARE	Data At Rest Encryption
EAL	Evaluation Assurance Level
ESRS	EMC Secure Remote Support
FC	Fibre Channel
GB	GigaByte
GUI	Graphical User Interface
iSCSI	Internet Small Computer System Interface
IT	Information Technology
I&A	Identification & Authentication
I/O	Input/Output
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number
OE	Operational Environment
OSP	Organizational Security Policy
PP	Protection Profile
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
REST	REpresentational State Transfer
SAN	Storage Area Network

Acronym	Definition
SFP	Security Function Policy
SFR	Security Functional Requirement
SSD	Solid State Drive
SSH	Secure SHell
ST	Security Target
TB	TeraByte
TOE	Target of Evaluation
TSF	TOE Security Functionality
VAAI	VStorage APIs for Array Integration
VLAN	Virtual LAN
XDP	Advanced Data Protection
XMS	XtremIO Management Server

Table 14 - Acronyms