EMC RecoverPoint® v4.4 Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 1926-000-D102
Version: 0.9
16 May 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 RecoverPoint® v4.4 Security Target
ST Version:	0.9
ST Date:	16 May 2016

1.3 TOE REFERENCE

TOE Identification:	EMC RecoverPoint® 4.4 SP1 (h.138) with Gen5 Hardware (100-564-200-03) or VMware vSphere 5.x
TOE Developer:	EMC Corporation
TOE Type:	Other Devices and Systems – Software and Hardware

1.4 TOE OVERVIEW

EMC RecoverPoint is an appliance-based product that provides real-time, block-level data replication for systems and devices in an enterprise storage area network (SAN) environment. RecoverPoint runs on an out-of-band RecoverPoint Appliance (RPA), and provides near-zero-data-loss protection both locally and remotely over a wide area network (WAN) as well as zero data loss synchronous replication over IP or extended Fibre Channel links. It is also possible to run RPA software as a virtual appliance on VMware infrastructure; this is referred to as a virtual RPA (vRPA). The functionality of RPAs and vRPAs is the same.

Data is forwarded to RPAs from storage devices or hosts by splitters, which is software that sends a copy of data being written to the RPAs. This enables RecoverPoint to transparently perform real-time and continuous backups of the protected storage.

Up to 8 RPAs may be interconnected at a site to form a cluster. Each RPA is a physical appliance (Gen5 hardware) or a VMware virtual machine instance. RPAs within a cluster are controlled and monitored by a single management access point. The management access point executes on one of the RPAs in the cluster that is dynamically chosen.

Up to 5 RPA clusters at different sites may be interconnected to form a system. The clusters within a system dynamically communicate amongst themselves to exchange data as directed by administrators.

Replication can be performed locally, remotely, or both. With local replication, a SAN connects systems and devices to a local RPA for replication designed to allow operational recovery from logical corruptions such as human errors or viruses. With remote replication, geographically dispersed SANs are connected by two or more RPA clusters, allowing recovery primarily from geographical or site disasters.

The following diagram shows a representative RecoverPoint system with 4 clusters. The RPAs work in the following way:

1. In New York, the splitters intercept all host writes to the storage, sending them to the RPAs in New York, and then to their normally designated storage volumes.
2. The RPAs in New York make intelligent decisions regarding when and what data to transfer to each target destination. They base these decisions on each RPAs continuous analysis of application load and resource availability, balanced against the need to prevent degradation of host

application performance and to deliver maximum adherence to the specified replication policies.

3. The RPAs at Shanghai, London and Moscow receive the data and distribute the data to the storage at each destination.

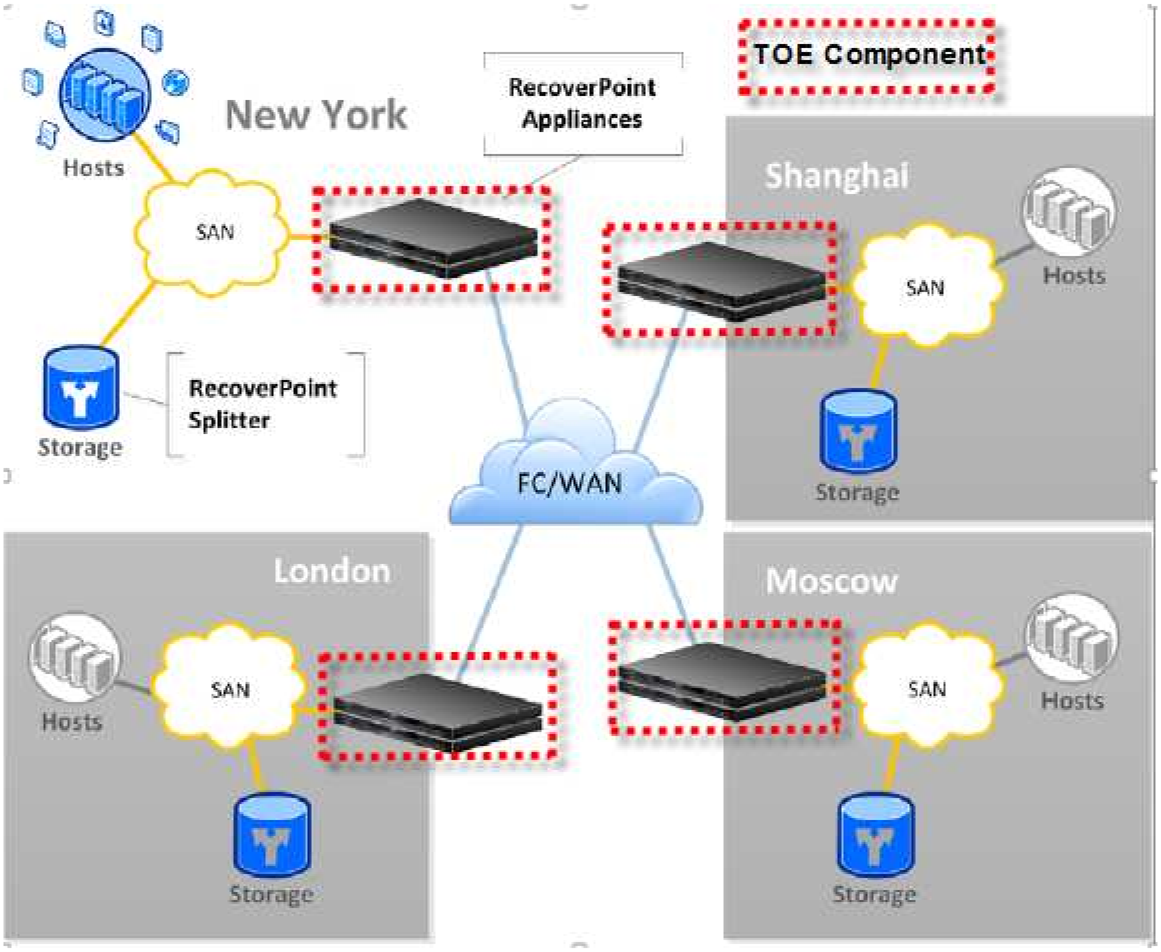

Figure 1 - EMC RecoverPoint Representative Deployment

Protected volumes are organized into Consistency Groups, which define the type of protection performed. In addition to data being stored locally and/or remotely, the Consistency Group may specify policies for restoration of data.

RecoverPoint digitally signs replicated data for integrity and records data change journals, allowing roll-back, recovery, and forensic analysis of data writes. RecoverPoint uses back-end storage for the replicated data as well as journals and meta-data associated with the data. The back-end storage is provided by the TOE Environment.

Data can be restored to protected storage (rollback), or copies of data can be made available for other purposes (e.g. testing, disaster recovery).

Users interact with the RecoverPoint system via a CLI or browser GUI (known as Unisphere for RecoverPoint). Multiple user accounts are supported and each one is assigned a role; multiple roles are supported to limit the capabilities available to different users. Users must provide a valid username and password at the beginning of each session. The credentials are validated internally.

Within each cluster, a single RPA provides the management interfaces for the cluster. An entire system can be managed from any of the clusters.

Event logs are generated for user actions as well as replication events. Events can be viewed via the CLI. Events can also be transmitted to external systems via Syslog, SNMP Traps, and SMTP. Filters can be configured to determine what events are sent to the external systems.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

A RecoverPoint system includes two to five clusters, each including two to 8 RPAs. RPAs provide interfaces for host connections, storage connections, and connections to other RPAs/clusters. The RPAs in a cluster dynamically select one RPA to provide the management interface for the cluster.

RPAs within a cluster are required to be all hardware or all vRPA instances. Hardware RPAs are Gen5 hardware appliances. vRPAs are VMware virtual machine instances running on ESXi systems that satisfy the minimum requirements specified in Table 1.

For hardware RPAs, the Gen5 appliance hardware and RecoverPoint software are included in the TOE boundary. When a vRPA is used, only the RecoverPoint software is included in the TOE boundary; the ESXi hardware and hypervisor are not part of the TOE.

1.5.2 TOE Environment

When a vRPA is used, the server hardware and hypervisor are part of the TOE Environment. vRPA is supported on VMware ESXi 5.x with vCenter 5.x. The following requirements must be satisfied for the system hosting the vRPA VM.

Item	Minimum Requirement
Virtual CPUs	2
RAM	4GB for 2 or 4 CPUs; 8GB for 8CPUs
Network Connections	4 (LAN, WAN, iSCSI1, iSCSI2)
Protected Storage	1 or more EMC VNX OE v05.32.000.5.2 or later, with at least one iSCSI port

Table 1 – Virtual Hardware Requirements for vRPA

The hosts and storage devices in the SANs that are connected to RecoverPoint are part of the TOE Environment. It is the responsibility of the TOE Environment to protect SAN traffic, administrator traffic with RPAs, and inter-RPA traffic (within a cluster and between clusters) from unauthorized disclosure or modification.

The RecoverPoint splitter is proprietary software that is installed on hosts and/or storage subsystems. The RecoverPoint splitter is used to "split" the application writes from hosts so that they are sent first to the RecoverPoint appliance and then to their normally designated storage volumes. The Splitters enable RecoverPoint to transparently back up the protected storage and perform recovery operations.

Users access RecoverPoint from workstations in the TOE Environment. For the CLI, the "PuTTY" utility is recommended.

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- *EMC RecoverPoint Installation and Deployment Guide*
- *EMC RecoverPoint Version 4.4 Administrator's Guide*
- *EMC RecoverPoint Release 4.4 CLI Reference Guide*
- *EMC RecoverPoint Release number 4.4 Release Notes*
- *EMC RecoverPoint Release number 4.4 Security Configuration Guide*
- *EMC RecoverPoint 4.4 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 authorized users.
Volume Replication	Replication is performed for configured volumes. Up to 4 simultaneous copies may be maintained. The primary volume may be restored to a point in time or snapshot. Each of the copies may be used for testing or to act as a failover instance.
Identification and Authentication	Administrators must identify and authenticate prior to TOE access. GUI users must supply a valid username and password. CLI users can supply a valid username and password or an SSH Fingerprint.

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 inactivity limit. A configured banner is displayed to users during login.

Table 2 - Logical Scope of the TOE

1.5.5 Required Configuration Settings

The following options must be configured:

1. The Security Level must be set to High.
2. Event Filters must allow generation of events for the following event types:
    a. Login activity (Successful and failed logins, logging out)
    b. Configuration changes
    c. Restoration actions
    d. Failure to send event messages to external systems
3. Custom roles are not configured; the pre-configured roles are used.

1.5.6 Functionality Excluded from the Evaluated Configuration

In addition to internal user accounts, RecoverPoint user accounts may be integrated with external LDAP servers for credential validation.

In addition to Gen5 hardware, RecoverPoint is also supported on Gen6 hardware.

The following product features are excluded from this evaluation:

- REST API
- High Availability
- EMC Secure Remote Support (ESRS)
- Call-Home

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 3 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.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
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 3 - 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 4 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.
P.REPLICATE	The TOE shall replicate volumes and enable rollback and testing of volumes.

Table 4 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 5.

Assumptions	Description
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NETWORK	The SAN devices will be interconnected by a segregated SAN that protects the traffic from disclosure to or modification by untrusted systems or users.
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.

Table 5 – 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.REPLICATE	The TOE shall replicate volumes and enable rollback and testing of volumes.
O.TIME	The TOE will maintain reliable timestamps.

Table 6 – 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 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.NETWORK	The operational environment will provide a segregated SAN that protects the traffic between the SAN devices 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.PROTCOMMS	The OE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

Table 7 – 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.EAVES	T.IMPCON	T.PRIVIL	T.UNAUTH_ACCESS	P.ACCACT	P.MANAGE	P.PROTECT	P.REPLICATE	A.MANAGE	A.NETWORK	A.NOEVIL	A.PROTECT
O.ACCESS		X	X	X		X						
O.AUDITS				X	X							

	T.EAVES	T.IMPCON	T.PRIVIL	T.UNAUTH_ACCESS	P.ACCACT	P.MANAGE	P.PROTECT	P.REPLICATE	A.MANAGE	A.NETWORK	A.NOEVIL	A.PROTECT
O.EADMIN		X				X						
O.IDAUTH		X	X		X	X						
O.PROTCT			X			X						
O.REPLICATE								X				
O.TIME					X							
OE.CREDEN						X					X	
OE.INSTAL		X				X					X	
OE.NETWORK										X		
OE.PERSON						X			X			
OE.PHYCAL							X				X	X
OE.PROTCOMMS	X											

Table 8 - 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 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.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.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	
Objectives:	OE.PROTCOMMS	The OE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
Rationale:	The OE.PROTCOMMS objective requires the OE to provide protected channels and paths.	

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.	

Policy: P.REPLICATE	The TOE shall replicate volumes and enable rollback and testing of volumes.	
Objectives:	O.REPLICATE	The TOE shall replicate volumes and enable rollback and testing of volumes.
Rationale:	The O.REPLICATE objective requires the TOE to replicate volumes and enable testing and/or rollback of volumes.	

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.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.NETWORK	The SAN devices will be interconnected by a segregated SAN that protects the traffic from disclosure to or modification by untrusted systems or users.	
Objectives:	OE.NETWORK	The operational environment will provide a segregated SAN that protects the traffic between the SAN devices from disclosure to or modification by untrusted systems or users.
Rationale:	The OE.NETWORK objective ensures that a segregated SAN will protect the data sent by the devices connected to it.	

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:	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical

A.PROTCT	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.	

5 EXTENDED COMPONENTS DEFINITION

5.1 EXTENDED FUNCTIONAL COMPONENTS

5.1.1 FDP_REP_EXT User Data Replication

Family Behaviour:

This family defines the requirements for the TOE to provide data replication for specified volumes in the operational environment.

Component Levelling:

FDP_REP_EXT User Data Replication

1

FDP_REP_EXT.1 User Data Backup/Restore provides for functionality to perform data replication for volumes as directed by administrators.

Management:

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

a) Configuration of the replication operations to be performed.

Audit:

There are no auditable events foreseen.

FDP_REP_EXT.1 User Data Replication

Hierarchical to: No other components.

Dependencies: None

FDP_REP_EXT.1.1 **The TSF shall provide the capability of replicating user data as configured by an authorized administrator.**

5.2 EXTENDED ASSURANCE COMPONENTS

This ST does not include extended security assurance 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 9 - 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
	FDP_REP_EXT.1	User data replication
	FDP_ROL.1	Basic rollback
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication

Class	SFR	Name
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	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 9 - 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) [*Login attempts, configuration changes, restoration actions*].

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 additional information*].

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.

6.2.1.3 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 data*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.4 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.

6.2.2 User Data Protection (FDP)

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 Replication SFP*] on [

Subjects: SAN Interfaces (on which Volume updates are received);

Objects: Volumes (associated with replication);

Operations: Transfer, Distribute].

Application Note: Transfer refers to the transmission of Volume updates to the RPAs included in the Consistency Group that the Volume is a member of, and adding this information to the journal maintained for the Volume. Distribution refers to writing the Volume updates to the replicated Volume.

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 Replication SFP*] to objects based on the following: [

SAN Interfaces: Interface ID;

Replica Volumes: Volume ID, associated Replication Sets, Volume Role, Storage Mode].

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. *When the Volume Role of the Volume ID and Interface ID for a Volume update is Production (normal operation) and the Storage Mode is Direct Access:*
   a. *The update is transferred to all Volumes in the Replication Set with a Volume Role of Local Copy or Remote Copy and a Storage Mode of Logged Access.*
   b. *The update is transferred and distributed to all Volumes in the Consistency Group with a Volume Role of Local Copy or Remote Copy and a Storage Mode of No Access.*
2. *When the Volume Role of the Volume ID and Interface ID for a Volume update is Local Source or Remote Source (failover operation) and the Storage Mode is Direct Access:*
   a. *The update is transferred to the Production Volume for the Replication Set if it has a Volume Role of Target and a Storage Mode of Logged Access.*
   b. *The update is transferred and distributed to the Production Volume for the Replication Set if it has a Volume Role of Target and a Storage Mode of No Access*].

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: [

1. *The Volume ID is not associated with a Replication Set for the Interface ID on which a Volume update is received.*
2. *The Volume Role of the Volume ID and Interface ID for a Volume update is Local Copy, Remote Copy, or Disabled*].

6.2.2.3 FDP_REP_EXT.1 User Data Replication

Hierarchical to: No other components.

Dependencies: None

FDP_REP_EXT.1.1 The TSF shall provide the capability of replicating user data as configured by an authorized administrator.

6.2.2.4 FDP_ROL.1 Basic rollback

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ROL.1.1 The TSF shall enforce [*Volume Replication SFP*] to permit the rollback of the [*replicated data*] on the [*volumes*].

FDP_ROL.1.2 The TSF shall permit operations to be rolled back within the [*points in time or snapshots maintained for volumes*].

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 or public key, Role*].

6.2.3.2 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.

6.2.3.3 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].*

6.2.3.4 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 for the GUI, no output for the CLI*] to the user while the authentication is in progress.

6.2.3.5 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.

6.2.3.6 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: [*the attributes do not change during a 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 Replication SFP*] to restrict the ability to [query, modify, delete] the security attributes [*Volume ID, Consistency Group membership, Volume Role, Storage Mode*] to [the *Admin role, the Security role (query only) and the Monitor role (query only)*].

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 Replication 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**	**Security**	**Admin**	**Monitor**
Security Configuration	Q, M, D, C	Q	Q
User's Own Password	M	M	M
System Configuration	Q	Q, M, D, C	Q
Storage Configuration	Q	Q, M, D, C	Q

Role TSF Data	Security	Admin	Monitor
Group Configuration	Q	Q, M, D, C	Q
Data Transfer Configuration	Q	Q, M, D, C	Q
Target Image Configuration	Q	Q, M, D, C	Q
Splitter Configuration	Q	Q, M, D, C	Q

Table 10 – 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: [

- *Security configuration*
- *User password changes*
- *System configuration*
- *Group configuration*
- *Data transfer configuration*
- *Target image configuration*
- *Splitter configuration*].

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 [*Security, Admin, Monitor*].

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

Application Note: The TOE also provides the Boxmgmt and Webdownload roles. However, since these roles concern appliance installation, maintenance and upgrades only, they are not relevant to the TOE when it is in an operational state.

6.2.5 Protection of the TSF (FPT)

6.2.5.2 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_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 [*period of inactivity of 12 hours*].

6.2.6.2 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.

6.2.6.3 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.

Application Note: The login banner applies to CLI sessions only.

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.REPLICATE	O.TIME
FAU_GEN.1		X					
FAU_GEN.2		X					
FAU_SAR.1		X					
FAU_SAR.2		X					
FDP_ACC.1						X	
FDP_ACF.1						X	
FDP_REP_EXT.1						X	
FDP_ROL.1						X	

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.PROTCT	O.REPLICATE	O.TIME
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 11 – 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 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.

Security Objective	Rationale
	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 specifies the I&A mechanisms that must be supported by the TOE. 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	FMT_MSA.3 requires restrictive access to replica Volumes by default so that no replication access is granted until explicitly configured by authorized users.
O.REPLICATION	FDP_ACC.1 and FDP_ACF.1 define the policy for the journaling and updating of replica Volumes.

Security Objective	Rationale
	FDP_REP_EXT.1 requires the TOE to provide replication capabilities. FDP_ROL.1 specifies that rollback capabilities are provided for Volumes being replicated.
O.TIME	FPT_STM.1 requires accurate time stamps to be available.

Table 12 – Security Objectives for the TOE

6.4 DEPENDENCY RATIONALE

Table 13 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
FDP_REP_EXT.1	None	n/a
FDP_ROL.1	FDP_ACC.1 or FDP_IFC.1	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

SFR	Dependencies	Dependency Satisfied / Rationale
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
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 13 - 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 14.

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

Assurance Class	Assurance Components	
	Identifier	Name
	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
	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 14 - 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. The audit trail is maintained on each cluster.

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).

Any authorized user of the TOE may view the audit records via the CLI and GUI.

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

7.1.2 Volume Replication

Any volume can be simultaneously replicated on up to 4 separate replica copies by configuring Replication Sets within Consistency Groups. As updates are received for each volume, they are forwarded to each of the active copies. A separate journal is maintained for each copy, and the updates are applied to the copies.

Each copy may be used as a target for testing. During this time, the journals are maintained but the volume is not updated, since hosts may be writing to it independently. Once testing is discontinued, the copy is synchronized with the primary volume.

Failovers may also be performed to make one of the copies the primary volume.

Volumes may be rolled back to a specific point in time or to a snapshot.

TOE Security Functional Requirements addressed: FDP_ACC.1, FDP_ACF.1, FDP_REP_EXT.1, FDP_ROL.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. GUI users always must present a valid username and password; CLI users may present a valid username and password or an SSH Fingerprint.

During collection of the password, only dots are echoed for each character supplied to the GUI and no characters are echoed by the CLI.

Upon successful login, the user's username and role are bound to 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 a production Volume is added, it is not included in any Consistency Group or Replication Set. Therefore, no replication data is created for the Volume. Users with the Admin role have the ability to configure Consistency Groups that include the Volume to cause replication data to be saved.

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

User sessions may be terminated by the user or the TOE. The TOE automatically terminates a session that remains idle for more than the allowed inactivity timer value.

The configured banner is displayed to CLI 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
CLI	Command Line Interface
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
ESRS	EMC Secure Remote Support
FC	Fibre Channel
GB	GigaByte
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTP	HyperText Transfer Protocol
ID	IDentifier
iSCSI	Internet Small Computer System Interface
IT	Information Technology
I&A	Identification & Authentication
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
OE	Operational Environment
OSP	Organizational Security Policy
PP	Protection Profile
RAM	Random Access Memory
RPA	RecoverPoint Appliance
REST	REpresentational State Transfer
SAN	Storage Area Network
SFP	Security Function Policy

Acronym	Definition
SFR	Security Functional Requirement
SP	Special Publication
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
vRPA	Virtual RecoverPoint Appliance
WAN	Wide Area Network

Table 15 - Acronyms