EMC® Corporation

EMC VNXe™ Operating Environment v2.0 with Unisphere™ running on VNXe Series hardware models VNXe3300™ and VNXe3100™

Security Target

Evaluation Assurance Level (EAL): EAL3+
Document Version: 0.7

Prepared for:

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

Phone: +1 (508) 435 1000
http://www.emc.com

Prepared by:

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

Phone: +1 (703) 267 6050
http://www.corsec.com

Table of Contents

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table of Figures

List of Tables

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is EMC VNXe™ Operating Environment v2.0 with Unisphere™ running on VNXe Series hardware models VNXe3300™ and VNXe3100™, and may hereafter be referred to as "the TOE" or "VNXe". The TOE is a combination File (IP[1]) and Block (iSCSI[2] over IP) operating environment with Unified Management (Unisphere). The TOE provides storage and access controls for block services over IP and standard IP-based file sharing protocols. The only Block service offered is iSCSI over an IP network.

1.1 Purpose

This ST is divided into nine sections, as follows:

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

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	EMC® Corporation EMC VNXe™ Operating Environment v2.0 with Unisphere™ running on VNXe Series hardware models VNXe3300™ and VNXe3100™ Security Target
ST Version	Version 0.7
ST Author	Corsec Security, Inc.
ST Publication Date	2011/07/12
TOE Reference	EMC VNXe Operating Environment v2.0.1 with SP1 image 12861

[1] IP – Internet Protocol
[2] iSCSI – Internet Small Computer Systems Interface

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

ST Title	EMC® Corporation EMC VNXe™ Operating Environment v2.0 with Unisphere™ running on VNXe Series hardware models VNXe3300™ and VNXe3100™ Security Target
Keywords	VNXe, Storage Area Network, SAN, storage array, data storage, Unisphere, Network Attached Storage, NAS, iSCSI

1.3 Product Overview

The Product Overview provides a high-level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

VNXe/Unisphere allows an organization to manage its storage needs separately from its application and file servers. This allows greater control over storage allocation, fault tolerance, and backups versus storage that is directly attached to individual application or file servers. In a typical deployment scenario, client machines connect to VNXe/Unisphere over an IP-based network through standard IP-based networking equipment (routers and switches as needed). These client machines are then configured to use storage on VNXe in the form of Logical Units or file systems for their applications.

VNXe includes the VNXe Operating Environment v2.0, which provides RAID[3] and virtual storage capabilities. The product provides the ability to combine several individual drives into useful logical groups, provides fault tolerance for stored data, and manages access to stored data. The product is designed to allow customers to scale both system performance and storage capacity.

VNXe Operating Environment v2.0 software is the management software that allows administrators to manage and configure VNXe. VNXe Hardware is the hardware platform, which includes back-end disks. Together these components provide three main features:

1. Block services (iSCSI over IP)
2. File services (Network File System (NFS) and Common Internet File System (CIFS))
3. A unified management suite that allows administrators to configure all parts of the VNXe from a single management console.

VNXe users access storage through traditional IP-based block and file protocols. VNXe can present itself as one or more standard network-based file servers to IP-based client machines (as a NAS[4]), or as a block storage device to client machines with iSCSI over IP. Administrators manage VNXe and control the policies that govern access to storage with VNXe Operating Environment v2.0 software.

The product runs Unified Block and File protocols, allowing the product to provide and control access to storage from IP-connected clients.

Data Access in Real Time (DART) implements the NAS functionality. DART is an operating system processes that performs the actual transfer of data between the back-end disk drives and IP-based clients. Each DART process provided by VNXe can host one or more "virtual servers" that present shared services to IP-based client machines. IP-based protocols that VNXe supports include:

[3] RAID – Redundant Array of Independent Disks
[4] NAS – Network Attached Storage

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- CIFS[5]
- NFS[6] versions 2 and 3
- iSCSI

Administrators can configure the type of protocols that are supported for that server per DART process. IP-connected client machines, with the appropriate access privileges, can then use VNXe to store and access data.

VNXe is responsible for enforcing all access permissions for user data. Each "virtual server" on VNXe can be configured to interface with a Microsoft Active Directory server or utilize local user authentication files. When a request for data access is made from an IP-based client machine, VNXe utilizes the appropriate authentication mechanism, checks the Access Control List (ACL) of the requested file or directory, and either grants or denies access to the user. User data is stored directly on storage provided by VNXe.

The VNXe Hardware includes disk drives. This disk storage is configured to provide a storage system for use by VNXe users. The block storage portion of VNXe allows this storage system to store and retrieve block units of data for VNXe users. Each of these block units is associated with a Logical Unit, which is in turn associated with a Logical Unit Number (LUN). Individual elements of the storage system are presented to VNXe as Logical Units. Each Logical Unit is a useable storage system volume that VNXe can expose to the user.

The VNXe Operating Environment v2.0 software contains utilities and a user interface for installing and configuring VNXe, maintaining the system, and monitoring system performance.

1.4 TOE Overview

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

The software-only TOE is the EMC VNXe™ Operating Environment v2.0 with Unisphere™ running on VNXe Series hardware models VNXe3300™ and VNXe3100™. The VNXe Operating Environment v2.0 provides RAID and virtual storage capabilities, one or more NAS servers that allow IP-based clients to connect and use storage, and an interface by which the TOE provides access controls for storage under management by VNXe.

The TOE is managed by authorized users through the UEMCLI[7] and the Unisphere GUI[8] interfaces. Unisphere GUI is an Adobe Flex application that runs within a web browser. To access the functions available via Unisphere GUI, an authorized user must open a web browser and enter the IP address or hostname of the VNXe management port. UEMCLI is a command line interface that provides access to common functions for monitoring and managing the TOE. The UEMCLI provides access to functions for storage provisioning, status and configuration information retrieval, and other TOE administrative functions. UEMCLI commands can also be used to automate management functions via shell scripts and batch files.

[5] CIFS is a platform-independent file sharing system commonly used by Microsoft Windows network file sharing
[6] NFS is a platform-independent file sharing system commonly used by UNIX and UNIX variants for file sharing
[7] UEMCLI – Unified Element Manager Command Line Interface
[8] GUI – Graphical User Interface

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The TOE software provides RAID storage architectures, fault detection, isolation, and diagnosis capabilities. It enables the use of virtual storage elements (LUNs) to improve performance and capacity utilization.

The TOE provides NAS services that allow hosts on an IP network to access file systems via one of the supported file-based protocols (CIFS and NFS). The TOE presents this storage as one or more file servers on the customer's network. Client systems that attempt to access the file systems must pass TOE access controls before the TOE allows the access to occur. The TOE provides SAN services that allow hosts to access storage as Logical Units via iSCSI protocol over an IP network.

The TOE also performs identification and authorization of TOE Administrators, and Users; discovery and monitoring of File-side and Block-side components; storage configuration and allocation; status and configuration information display; and event management.

Figure 1 shows the details of the deployment configuration of the TOE:

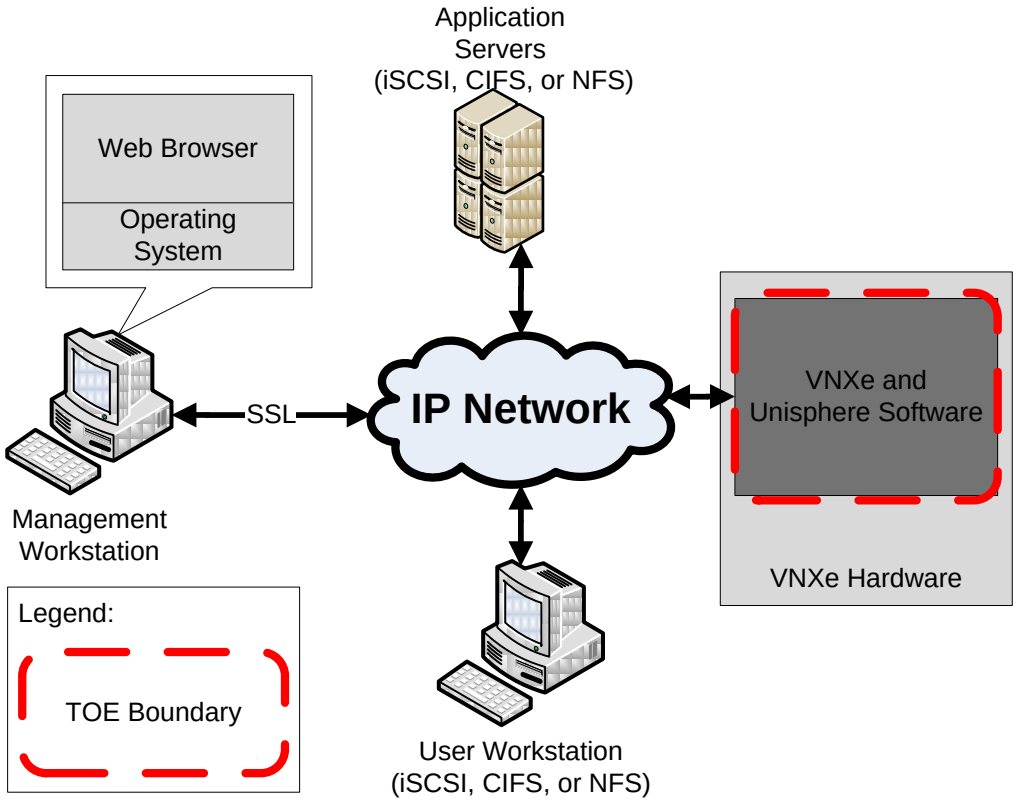

Figure 1 – Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The following sections describe the technologies and concepts related to the TOE.

1.4.1.1 Logical Units and File Systems

A central concept of the TOE is a virtual unit called a Logical Unit. The TOE presents storage to client machines on the IP network in the form of Logical Units and File Systems. The TOE software provides for the management of Logical Units and File Systems. Each Logical Unit represents a unit of storage to a client machine, analogous to a local disk drive. However, the Logical Unit provided by the TOE is not

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

constrained to be a single individual disk. In fact, a typical deployment would have Logical Units that span multiple individual disks that are grouped into a RAID Group.

1.4.1.2 Storage Processors (SPs)

The SP hardware (with VNXe Operating Environment v2.0 software) is responsible for interfacing with the front-end IP-based clients and the back-end disks within the VNXe. The SP provides administrators with the ability to manage the TOE and establish Logical Units and RAID Groups.

1.4.1.3 RAID Groups

A RAID Group is a collection of individual disks. The TOE supports a variety of disk types and capacities (chosen by the customer when the product is purchased). In a RAID Group, disks of a similar type are typically grouped together. This RAID Group can then be configured by an administrator with various attributes, such as which RAID level to provide. In this manner, an administrator can manage the TOE through successive levels of abstraction.

1.4.1.4 Storage Groups

Logical Units grouped together are called a Storage Group. Each Storage Group can then be mapped to one or more client machines. When this mechanism is used, a client machine can only access Logical Units that are present in a Storage Group that the client machine has been permitted to access.

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

1.4.1.5 Unisphere

Unisphere is the Adobe Flex GUI used to manage the TOE. Administrators must log into Unisphere in order to manage the TOE or the policies that control user access. Management functionality is presented in the form of multiple screens that contain graphical elements, such as fields, buttons, and boxes. Unisphere also provides utilities to maintain and install the TOE.

1.4.1.6 Data Access in Real Time (DART)

DART Processes are described above in section 1.3.

1.4.2 TOE Environment

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

The TOE relies on secure access provided by the network to which it is attached. The purpose of the TOE is to mediate access to user data for client machines connected to an IP network.

1.5 TOE Description

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

1.5.1 Physical Scope

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

The essential physical components for the proper operation of the TOE in the evaluated configuration are:

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- TOE software
- VNXe hardware (not included in the TOE boundary)
- Management workstation to access the VNXe Operating Environment v2.0 software via a web browser or the UEMCLI (not included in the TOE boundary)

1.5.1.1 TOE Software

The TOE is a software-only TOE meant to be used with the VNXe Hardware. The essential components for the proper operation of the TOE in the evaluated configuration are:

- VNXe Operating Environment v2.0 software

1.5.1.2 Guidance Documentation

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

- Using an EMC VNXe System with CIFS Shared Folders, 300-010-548, A01
- Using an EMC VNXe System with NFS Shared Folders, 300-010-549, A01
- Using an EMC VNXe System with Generic iSCSI Storage, 300-010-550, A01
- EMC VNXe3300 System Installation Guide, 300-011-182, A02
- EMC VNXe3100 System Installation Guide, 300-011-183, A02
- VNXe Series Quick Start, 300-012-107, A01
- EMC VNXe Security Configuration Guide, 300-012-190, 1.0
- EMC Unisphere CLI Version 1.5 User Guide, 300-011-236, A01
- Unisphere for VNXe Online Help 1.05 A01 (Available at https://sso.emc.com/sso/login.htm?CTAuthMode=BASIC)
- EMC Unisphere for VNXe: Next-Generation Storage Management A Detailed Review, h8179,

1.5.2 Logical Scope

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

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management

1.5.2.1 Security Audit

The TOE generates audit records for all administrator actions that result in a configuration change and all login attempts. Authorized administrators can view, sort, and filter the audit records.

1.5.2.2 User Data Protection

The User Data Protection function implements functionality necessary to protect user data which is entrusted to the TOE. This functionality is primarily enforced by DART processes in the TOE. DART hosts of the TOE are identified and authenticated, either by the TOE or the TOE Environment. These DART users are then granted access to files and directories managed by the TOE. Each file and directory has an Access Control List (ACL) that contains the access privileges for DART hosts of the TOE to that object.

The TOE protects user data primarily in two additional ways. First, it ensures that only the client machines that have been granted access to a LUN have access to that LUN. Second, by ensuring the integrity of the data entrusted to it through its use of RAID levels.

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.5.2.3 Identification and Authentication

This function of the TOE is used to identify and authenticate each operator of the TOE. In the case of Unisphere Administrators, the TOE provides username and password verification functionality. DART hosts of the TOE can be authenticated directly by the TOE or can be authenticated by a separate Active Directory. Administrators are assigned a role to determine what aspects of the TOE they are allowed to manage. This functionality is configured by an Administrator.

1.5.2.4 Security Management

The Security Management functionality of the TOE specifies several aspects of management of the TOE Security Functionality (TSF). Proper management of the TSF is required to properly mediate access to user data.

The TOE is managed by authorized users through the Unisphere GUI and the UEMCLI. Unisphere GUI is an Adobe Flex application that runs within a web browser. UEMCLI is a command line interface that provides access to common functions for monitoring and managing the TOE.

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

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

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

- VNXe Hardware
- Windows Active Directory

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2 Conformance Claims

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

Table 2 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2010/10/13 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL3+ augmented with Flaw Remediation (ALC_FLR.2)

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3 Security Problem

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

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

3.1 Threats to Security

This section identifies the threats to the IT[9] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

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

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[10] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The threats in Table 3 are applicable.

Table 3 – Threats

Name	Description
T.DATA_CORRUPTION	Data could become corrupted due to hardware failure or incorrect system access by users of the TOE or attackers.
T.IMPROPER_SERVER	A system connected to the TOE could access data that it was not intended to gain access by bypassing the protection mechanisms of the TOE.
T.IMPROPER_CONFIG	The TOE could be misconfigured to provide improper storage or enforce improper access to user data.
T.MEDIATE_ACCESS	Access to user data could be improperly granted to users who should not have access to it.
T.UNAUTH	An unauthorized user could access data stored by the TOE by bypassing the protection mechanisms of the TOE.

[9] IT – Information Technology
[10] TSF – TOE Security Functionality

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3.2 Organizational Security Policies

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

3.3 Assumptions

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

Table 4 – Assumptions

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

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4 Security Objectives

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

4.1 Security Objectives for the TOE

Table 5 lists the specific security objectives for the TOE.

Table 5 – Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record audit records for data accesses and use of the TOE functions on the management system.
O.AUDIT_REVIEW	The TOE must provide authorized administrators with the ability to review the audit trail.
O.ADMIN	The TOE must provide a method for administrative control of the TOE.
O.PROTECT	The TOE must protect data that it has been entrusted to protect.
O.I&A	The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

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

Table 6 – IT Security Objectives

Name	Description
OE.I&A	The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.
OE.SECURE_COMMUNICATIONS	The TOE Environment must provide secure communications between systems connected to the Storage Area Network.
OE.SECURE_SERVERS	The TOE Environment must provide properly configured authentication servers and client machines to communicate with the TOE.
OE.TIME	The TOE environment must provide reliable time stamps to the TOE.
OE.PROPER_NAME_ASSIGNMEN	The TOE Environment must provide accurate World Wide Names

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description
T	for each system that communicates with the TOE.

4.2.2 Non-IT Security Objectives

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

Table 7 – Non-IT Security Objectives

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

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

5 Extended Components

There are no extended SFRs and extended SARs for this evaluation of the TOE.

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6 Security Requirements

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

6.1.1 Conventions

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

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

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

6.2 Security Functional Requirements

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

Table 8 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FDP_ACC.1a	Subset access control		✓		✓
FDP_ACF.1a	Security attribute based access control		✓		✓
FDP_ACC.1b	Subset access control		✓		✓
FDP_ACF.1b	Security attribute based access control		✓		✓
FDP_SDI.2	Stored data integrity		✓	✓	
FIA_ATD.1	User attribute definition		✓	✓	
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MSA.1a	Management of security attributes	✓	✓		✓
FMT_MSA.1b	Management of security attributes	✓	✓		✓
FMT_MSA.3a	Static attribute initialisation	✓	✓		✓

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	S	A	R	I
FMT_MSA.3b	Static attribute initialisation	✓	✓		✓
FMT_MTD.1a	Management of TSF data	✓	✓		✓
FMT_MTD.1b	Management of TSF data	✓	✓		✓
FMT_MTD.1c	Management of TSF data	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		

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

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

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

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

c) [*all administrator actions that result in a configuration change to the storage array, all administrator login attempts*].

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*the Administrator, Storage Administartor and Operator*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.2 Class FDP: User Data Protection

FDP_ACC.1a Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1a

The TSF shall enforce the [*Discretionary Access Control SFP*[11]] on
[
a) Subjects: Hosts
b) Objects: LUNs
c) Operations: Read and write
].

Application note: the Subjects are client machines connected to the TOE acting on behalf of an authorized user.

Dependencies: FDP_ACF.1a Security attribute based access control

FDP_ACF.1a Security attribute based access control
Hierarchical to: No other components.
FDP_ACF.1.1a

The TSF shall enforce the [*Discretionary Access Control SFP*] to objects based on the following:
[
Subject attributes:
1. IQN[12]
Object Attributes:
1. LUN ID[13]
].

FDP_ACF.1.2a

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[
A valid subject of the TOE is allowed to read and write to a LUN if the subject and the LUN are members of the same storage group
].

FDP_ACF.1.3a

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

FDP_ACF.1.4a

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

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

FDP_ACC.1b Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1b

The TSF shall enforce the [*NFS and CIFS Access SFP*] on
[
a) Subjects: Hosts

[11] SFP – Security Functional Policy
[12] IQN – iSCSI Qualified Name
[13] ID – Identifier

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

b) *Objects: NFS Mounts, CIFS Shares*
c) *Operations: Create, Read, Write, Append, Execute, Delete, Change Ownership, Read Permissions, Change Permissions, Read Attributes, Write Attributes, Read Extended Attributes, and Write Extended Attributes*].

Dependencies: FDP_ACF.1b Security attribute based access control

Application Note: The CIFS naming convention has been used for operations. NFS v2, and NFS v3 access supports a subset of these operations.

FDP_ACF.1b Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1b

The TSF shall enforce the [*NFS and CIFS Access SFP*] to objects based on the following:
[
Subject attributes:
1. *Hosts*

Object attributes:
1. *NFS Mounts*
2. *CIFS Shares*

].

FDP_ACF.1.2b

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*A valid subject of the TOE is allowed to perform an operation if the contents of the Access Control List for the object authorizes the Subject to perform the desired operation*].

FDP_ACF.1.3b

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:
[
1. *For CIFS access, subjects that are members of the group Domain Administrators shall be authorized to backup, restore, and take ownership of all objects*
2. *For NFS access, subjects that are authorized as superusers can perform all operations on all objects*

].

FDP_ACF.1.4b

The TSF shall explicitly deny access of subjects to objects based on the [*A valid subject of the TOE is explicitly denied the ability to perform an operation if the contents of the Access Control List for the object explicitly deny the Subject to perform the desired operation*].

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

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.2.1

The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all **user data** ~~objects~~, based on the following attributes: [*parity data for RAID 5 and RAID 6; mirrored data for RAID 1+0*].

FDP_SDI.2.2

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

Dependencies: No dependencies

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.3 Class FIA: Identification and Authentication

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

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
FIA_UAU.2.1
The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
FIA_UID.2.1
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: No dependencies

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.4 Class FMT: Security Management

FMT_MSA.1a Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1a
The TSF shall enforce the [*Discretionary Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*Storage Group Membership*] to [*the Administrator and Storage Administrator roles*].
Dependencies: FDP_ACC.1a Subset access control or
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1b Management; of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1b
The TSF shall enforce the [*NFS and CIFS Access SFP*] to restrict the ability to [modify, delete, [*add*]] the security attributes [*Host assignment*] to [*the Administrator and Storage Administrator*].
Dependencies: FDP_ACC.1b Subset access control or
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3a Static attribute initialisation
Hierarchical to: No other components.
FMT_MSA.3.1a
The TSF shall enforce the [*Discretionary Access control SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2a
The TSF shall allow the [*Administrator and Storage Administrator*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies: FMT_MSA.1a Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3b Static attribute initialisation
Hierarchical to: No other components.
FMT_MSA.3.1b
The TSF shall enforce the [*NFS and CIFS Access SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2b
The TSF shall allow the [*Object Owner*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies: FMT_MSA.1b Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1a Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1a
The TSF shall restrict the ability to [query] the [*storage system information*] to [*the Administrator, Storage Administrator, and Operator roles*].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

FMT_MTD.1b Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1b
The TSF shall restrict the ability to [modify, delete, [*create*]] the [*LUNs, RAID Groups, and Storage Groups*] to [*the Administrator and Storage Administrator roles*].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1c Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1c
The TSF shall restrict the ability to [modify, delete, [*create*]] the [*user accounts*] to [*the Administrator role*].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
FMT_SMF.1.1
The TSF shall be capable of performing the following management functions:
[
a) Management of security functions behavior;
b) Management of TSF data;
c) Management of security attributes
].
Dependencies: No Dependencies

FMT_SMR.1 Security roles
Hierarchical to: No other components.
FMT_SMR.1.1
The TSF shall maintain the roles [*the authorised roles identified in* Table 9].
FMT_SMR.1.2
The TSF shall be able to associate users with roles.
Dependencies: FIA_UID.1 Timing of identification

Table 9 – Authorized Roles

Role	Description
Operator	Can only perform monitoring activities in Unisphere. Read only access.
Storage Administrator	Can configure Unisphere, and provision and reclaim storage.
Administrator	All administration capabilities.

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL3 augmented with ALC_FLR.2. Table 10 – Assurance Requirements summarizes the requirements.

Table 10 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
	ATE_DPT.1 Testing basic design
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7 TOE Specification

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

7.1 TOE Security Functions

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

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

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

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7.1.1 Security Audit

The TOE generates audit records for startup and shutdown of the audit function, all administrator actions that result in a configuration change, and all login attempts. Audit records contain the date and time of the event, the type of event, subject identity (if applicable), and the outcome of the event. Authorized administrators can view the audit records from the CLI or GUI. Audit records are presented to administrators in a clearly understandable format.

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

7.1.2 User Data Protection

This section describes the various User Data Protection SFRs claimed.

7.1.2.1 NFS and CIFS Access SFP

The TOE enforces the NFS and CIFS Access SFP[14] on each DART User of the TOE based on the security attributes of that user.

NFS and CIFS Access SFP*:* The TOE enforces the NFS and CIFS Access SFP on DART hosts by assigning access privileges to hosts. The ability to perform operations on objects, which are governed by the NFS and CIFS Access SFP, are granted to DART hosts by Administrators or Storage Administrators.

A Linux/Unix host can mount to the VNXe hosted NFS Shared Folder Server if the host has been explicitly authorized to the NFS Shared Folder Server. Similarly a Windows host can map to the VNXe hosted CIFS Shared Folder Server if the host has been explicitly authorized to the CIFS Shared Folder.

The export of a CIFS Shared Folder Server is based off of the Server Configuration Active Directory setting. The VNXe hosted CIFS Shared Folder Server must be in a Windows domain with Active Directory set up. A windows host can map to the share only if a member of the domain defined. For CIFS access, subjects that are members of the group Domain Administrators shall be authorized to backup, restore, and take ownership of all objects.

Hosts Access to the VNXe hosted NFS Shared Folder Server can be configured based on IP address or network host name, IP subnet range, or a Netgroup. For the NFS access protocol, DART Users who are *superusers* can perform all operations on all objects.

Each file and directory has an ACL associated with it. Each ACL has a set of permissions that are granted or explicitly denied to that host. Whenever a DART User requests an access to a file or directory, the TOE utilizes its NFS and CIFS Access SFP to decide whether or not that access is permitted.

7.1.2.2 Discretionary Access Control SFP

The TOE also provides the User Data Protection security function to manage access from client machines to configured Logical Units. The purpose of the TOE's storage is to allow high speed, scalable, fault-tolerant storage separate from individual client machines. The TOE provides this functionality to IP-connected hosts.

Using the Security Management security function, Administrators of the TOE can configure Logical Units to provide storage to client machines. These Logical Units are then placed into Storage Groups, which allows an Administrator to limit access to each Logical Unit to one or more client machines. When a client machine requests a list of available Logical Units from the TOE, the TOE Environment provides an IQN. This IQN is used to identify the client machine to the TOE. The TOE then provides a list of Logical Units

[14] SFP – Security Functional Policy

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

that the client machine has been granted access to. With each successive request to read or write information to or from a Logical Unit, the TOE ensures that only authorized client machines have access to the Logical Units to which they have been given access.

The TOE also provides for the integrity of user data. When creating RAID Groups from individual disk drives, an Administrator can configure RAID levels 1/0, 5, or 6. Each of these provides fault tolerance for integrity errors or individual disk drive failure. The TOE provides mechanisms to check data integrity continuously while reading and writing data to individual disks. Integrity errors or drive errors are fixed on-the-fly. Additionally, Administrators can configure "hot spare" disk drives. These "hot spares" are used when a disk failure has been detected by the system. Once a failure has been detected, the drive that has been lost will be recreated on the "hot spare". The Administrator can then replace the failed drive and configure it as a new "hot spare". This process is provided while real-time access to user data continues.

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

7.1.3 Identification and Authentication

The TOE performs identification and authentication of both Administrators and DART Users. The purpose of the identification and authentication function is to allow the TOE to restrict access to both administrative functions and to user data based upon the authenticated identity and associated attributes of a user.

7.1.3.1 Administrative I&A

Unisphere Administrators can access the TOE through a web browser or through a command line interface. The TOE supports internally enforced username and password-based authentication as well as authentication against Active Directory. TOE maintains UserIDs, and passwords of all the local TOE Administrators. The first action that operators must take when attempting to interact with the TOE is to provide a username and password. Before identification and authentication, the TOE operator is not able to perform any TOE security functionality.

7.1.3.2 User I&A

DART hosts of the TOE are defined as those subjects that wish to use the TOE to store and mediate access to data.

Windows environments use Microsoft Active Directory for authentication. A Windows host can only map to CIFS Shared Folder Server if the Windows host is on the same domain as the VNXe, and the Windows domain with Active Directory set up.

For NFSv2 and NFSv3, the server from which the request is coming has already identified and authenticated each DART host based on host IP address or network host name, or IP Subnet range, or Netgroup . For this configuration, the TOE relies on its environment to perform proper identification and authentication.

Identification and Authentication of client machines connecting to the TOE to access LUNs is provided by the TOE through the proper assignment and use of IQNs.

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

7.1.4 Security Management

Unisphere Administrators are primarily responsible for managing and configuring system objects. This includes managing the use of LUNs provided by the storage system, grouping those LUNs into useful storage groups called Volumes, and creating and managing individual file systems on those Volumes. The Administrator creates and manages "Storage Resources", and maps shares on those file servers to

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

configured file systems. The Administrator is responsible for configuring the access control mechanisms to be supported by each "Storage Resource".

The TOE provides mechanisms to govern which client machines can access which LUNs. The Security Management function allows Administrators to properly configure this functionality.

Administrators of the TOE are assigned one of the roles described in Table 9 above.

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

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8 Rationale

8.1 Conformance Claims Rationale

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

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

Table 12 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.DATA_CORRUPTION Data could become corrupted due to hardware failure or incorrect system access by users of the TOE or attackers.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT counters this threat by providing mechanisms to protect the data that has been entrusted to the TOE.
T.IMPROPER_SERVER A system connected to the TOE could access data that it was not intended to gain access by bypassing the protection mechanisms of the TOE.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	OE.SECURE_COMMUNICATIONS The TOE Environment must provide secure communications between systems connected to the Storage Area Network.	OE.SECURE_COMMUNICATIONS counters this threat by ensuring that all communications with the TOE are secure for administration of the TOE, internal TOE communications, and data sent to or from the TOE.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT counters this threat by providing adequate mechanisms to give only authorized servers access to the appropriately authorized data.
	OE.SECURE_SERVERS The TOE Environment must provide properly configured authentication servers and client machines to communicate with the TOE.	OE.SECURE_SERVERS counters this threat by ensuring that each server connected to the storage area network operates properly and does not intentionally compromise data.

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
	OE.PROPER_NAME_ASSIGNMENT The TOE Environment must provide accurate World Wide Names for each system that communicates with the TOE.	OE.PROPER_NAME_ASSIGNMENT counters this threat by ensuring that the World Wide Names provided to the TOE are accurate. This allows the mechanisms provided by O.PROTECT to properly protect data.
T.IMPROPER_CONFIG The TOE could be misconfigured to provide improper storage or enforce improper access to user data.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.	O.I&A counters this threat by ensuring that all authorized administrators are properly identified and authenticated.
T.MEDIATE_ACCESS Access to user data could be improperly granted to users who should not have access to it.	OE.I&A The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.	O.I&A and OE.I&A (depending on TOE configuration) work together to counter this threat by ensuring that the TOE or the TOE environment has properly identified and authenticated a user prior to providing access to user data.
	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	OE.SECURE_COMMUNICATIONS The TOE Environment must provide secure communications between systems connected to the Storage Area Network.	OE.SECURE_COMMUNICATIONS counters this threat by ensuring that identification and authentication performed by the TOE Environment is done over a secure communications channel.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT counters this threat by providing mechanisms to protect the data that has been entrusted to the TOE.
	OE.SECURE_SERVERS The TOE Environment must provide properly configured authentication servers and client machines to communicate with the TOE.	OE.SECURE_SERVERS counters this threat by ensuring that the servers that communicate with the TOE on behalf of a user are managed securely.
	O.I&A The TOE will uniquely identify	O.I&A and OE.I&A (depending on TOE configuration) work together

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
	users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.	to counter this threat by ensuring that the TOE or the TOE environment have properly identified and authenticated a user prior to providing access to user data.
T.UNAUTH An unauthorized user could access data stored by the TOE by bypassing the protection mechanisms of the TOE.	O.AUDIT The TOE must record audit records for data accesses and use of the TOE functions on the management system.	O.AUDIT counters this threat by ensuring that the TOE tracks all management actions taken against the TOE.
	O.AUDIT_REVIEW The TOE must provide authorized administrators with the ability to review the audit trail.	O.AUDIT_REVIEW counters this threat by ensuring that administrators can review the audited changes to the TOE configuration.
	OE.I&A The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.	O.I&A and OE.I&A (depending on TOE configuration) work together to counter this threat by ensuring that the TOE or the TOE Environment has properly identified and authenticated a user prior to providing access to user data.
	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	OE.SECURE_COMMUNICATIONS The TOE Environment must provide secure communications between systems connected to the Storage Area Network.	OE.SECURE_COMMUNICATIONS counters this threat by ensuring that identification and authentication performed by the TOE Environment is done over a secure communications channel.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT counters this threat by providing mechanisms to protect the data that has been entrusted to the TOE.
	OE.SECURE_SERVERS The TOE Environment must provide properly configured authentication servers and client machines to communicate with the TOE.	OE.SECURE_SERVERS counters this threat by ensuring that the servers that communicate with the TOE on behalf of a user are managed securely. Depending upon the access mechanism chosen, the TOE may depend upon these servers for identification and authentication of users.

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
	O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.	O.I&A and OE.I&A (depending on TOE configuration) work together to counter this threat by ensuring that the TOE or the TOE Environment has properly identified and authenticated a user prior to providing access to user data.

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no OSPs defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 13 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	NOE.MANAGE Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.	NOE.MANAGE upholds this assumption by ensuring that those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use.
A.NOEVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	NOE.NOEVIL Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.	NOE.NOEVIL upholds this assumption by ensuring that administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSICAL Physical security will be provided for the TOE and its environment.	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	NOE.PHYSICAL upholds this assumption by ensuring that physical security is provided within the domain for the value of the IT resources protected by the operating system and the value of the stored, processed, and transmitted information.
A.PROTECT The IT Environment shall provide a secure place to store user data of which access to that data will be mediated by the TOE.	NOE.PROTECT The TOE Environment must protect the data it has been entrusted to protect.	NOE.PROTECT upholds this assumption by ensuring that sites using the TOE will connect the TOE to a storage area network that provides data storage. This data storage should be configured and managed securely to allow the TOE to properly mediate access

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Assumptions	Objectives	Rationale
		to user data.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable time stamps to the TOE.	OE.TIME upholds this assumption by ensuring that the environment provides reliable time stamps to the TOE.
A.I&A The TOE environment will provide identification and authentication of Application Server users before allowing any other TSF-mediated actions on behalf of those users.	OE.I&A The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.	OE.I&A upholds this assumption by ensuring that the environment provides identification and authentication of client machine users.

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

8.3 Rationale for Extended Security Functional Requirements

There are no extended functional requirements defined for this TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended assurance requirements defined for this TOE.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 14 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must record audit records for data accesses and use of the TOE functions on the management system.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security-related events, including relevant details about the event.
O.AUDIT_REVIEW The TOE must provide authorized administrators with the ability to review the audit trail.	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review the audit trail.

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method for administrative control of the TOE.	FIA_UAU.2 User authentication before any action	This SFR supports O.ADMIN by ensuring that the TOE shall successfully authenticate each administrator before allowing management of the TOE.
	FIA_UID.2 User identification before any action	This SFR supports O.ADMIN by ensuring that the TOE will properly identify and authenticate all administrators.
	FMT_MSA.1a Management of security attributes	This SFR supports O.ADMIN by ensuring that security attributes of the TOE can only be changed by authorized administrators.
	FMT_MSA.1b Management of security attributes	This SFR supports O.ADMIN by ensuring that security attributes of the TOE can only be changed by authorized administrators.
	FMT_MSA.3a Static attribute initialisation	This SFR supports O.ADMIN by ensuring that permissive values for data access are provided and the TOE administrator can change them when a data object is created.
	FMT_MSA.3b Static attribute initialisation	This SFR supports O.ADMIN by ensuring that restrictive values for data access are provided, and the Object Owner can change them when a data object is created.
	FMT_MTD.1a Management of TSF data	This SFR supports O.ADMIN by ensuring that the ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_MTD.1b Management of TSF data	This SFR supports O.ADMIN by ensuring that the ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_MTD.1c Management of TSF data	This SFR supports O.ADMIN by ensuring that the ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_SMF.1 Specification of management functions	This SFR supports O.ADMIN by ensuring that each of the management functions are utilized to securely manage the TOE.
	FMT_SMR.1 Security roles	This SFR supports O.ADMIN by ensuring that specific roles are

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
		defined to govern management of the TOE.
O.PROTECT The TOE must protect data that it has been entrusted to protect.	FDP_ACC.1a Subset access control	This SFR supports O.PROTECT by ensuring that the TOE has an access control policy that ensures that only authorized servers can gain access to data within the TOE.
	FDP_ACF.1a Security attribute based access control	This SFR supports O.PROTECT by ensuring that the TOE provides access control functionality to manage access to data within the TOE.
	FDP_ACC.1b Subset access control	This SFR supports O.PROTECT by ensuring that the TOE provides access control functionality to manage access to data protected by the TOE.
	FDP_ACF.1b Security attribute based access control	This SFR supports O.PROTECT by ensuring that the TOE has an access control policy which ensures that only authorized hosts gain access to data protected by the TOE.
	FDP_SDI.2 Stored data integrity	This SFR supports O.PROTECT by ensuring that the TOE protects the stored user data from integrity errors.
O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.	FIA_ATD.1 User attribute definition	This SFR supports O.I&A by ensuring that the TOE, when configured for local user administration, maintains security attributes for each user.
	FIA_UAU.2 User authentication before any action	This SFR supports O.I&A by ensuring that the TOE authenticates each Administrator, and when configured for local user administration each user, prior to granting access to the TSF.
	FIA_UID.2 User identification before any action	This SFR supports O.I&A by ensuring that the TOE identifies each Administrator and when configured for local user administration, each user prior to granting access to the TSF.

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8.5.2 Security Assurance Requirements Rationale

EAL3+ was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. The TOE is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL3+, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

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

8.5.3 Rationale for Refinements of Security Functional Requirements

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

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

8.5.4 Dependency Rationale

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

Table 15 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Although FPT_STM.1 is not included, the TOE Environment provides reliable timestamps to the TOE. An environmental objective states that the TOE will receive reliable timestamps, thereby satisfying this dependency.
FAU_SAR.1	FAU_GEN.1	✓	
FDP_ACC.1a	FDP_ACF.1a	✓	
FDP_ACF.1a	FMT_MSA.3a	✓	
	FDP_ACC.1a	✓	
FDP_ACC.1b	FDP_ACF.1b	✓	
FDP_ACF.1b	FMT_MSA.3b	✓	
	FDP_ACC.1b	✓	

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

SFR ID	Dependencies	Dependency Met	Rationale
FDP_SDI.2	None	Not applicable	
FIA_ATD.1	None	Not applicable	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not claimed, FIA_UID.2 is claimed and is hierarchical to FIA_UID.1.
FIA_UID.2	None	Not applicable	
FMT_MSA.1a	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_ACC.1a	✓	
FMT_MSA.1b	FDP_ACC.1b	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3a	FMT_SMR.1	✓	
	FMT_MSA.1a	✓	
FMT_MSA.3b	FMT_SMR.1	✓	
	FMT_MSA.1b	✓	
FMT_MTD.1a	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MTD.1b	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MTD.1c	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	Not applicable	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not claimed, FIA_UID.2 is claimed and is hierarchical to FIA_UID.1.

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

9 Acronyms

This section describes the acronyms used in this document.

Table 16 – Acronyms

Acronym	Definition
ACL	Access Control List
CC	Common Criteria
CIFS	Common Internet File System
CLI	Command Line Interface
DART	Data Access in Real Time
DOS	Disk Operating System
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
ID	Identifier
IP	Internet Protocol
IQN	iSCSI Qualified Name
iSCSI	Internet Small Computer System Interface
IT	Information Technology
LUN	Logical Unit
MS	Microsoft
NAS	Network Attached Storage
NFS	Network File System
OSP	Organizational Security Policy
PP	Protection Profile
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SOE	Storage Operating Environment v2.0
SP	Storage Processor

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
ST	Security Target
TSF	TOE Security Functionality
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
UEMCLI	Unified Element Manager Command Line Interface
UQM	Unisphere Quality of Service Manager
UTF	Unicode Transformation Format

© 2011 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Prepared by:
Corsec Security, Inc.

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

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