EMC Corporation
EMC® Disk Library v3.1

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 1.02

Prepared for:

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

http://www.emc.com

Prepared by:

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

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
1.02	2008-01-08	Nathan Lee	Initial release.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The TOE is the EMC Disk Library, and will hereafter be referred to as the TOE throughout this document. The TOE is composed of a disk based backup solution that provides emulation of virtual tape libraries, virtual tapes, and virtual tape drives, and a management console software program.

1.1 Purpose

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

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- Security Environment (Section 3) – Describes the threats 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.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile (PP) claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- Acronyms and Terminology (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target, TOE and CC Identification and Conformance

Table 1 - Identification and Conformance

ST Title	EMC Corporation EMC® Disk Library v3.1 Security Target
ST Version	Version 1.02
Author	Corsec Security, Inc. Nathan Lee and Matthew Appler
TOE Identification	EMC Disk Library v3.1 (build 1549)
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 (aligned with ISO/IEC 15408:2005); CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted CEM as of 2006-06-29 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+: EAL2 Augmented with ALC_FLR.1 Basic flaw remediation
Keywords	Disk based backup, virtual tape, virtual tape library

1.3 Conventions and Terminology

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 several operations to be performed on security functional requirements: assignment, refinement, selection and iteration. All of these operations are used within this ST. These operations are presented in the same manner in which they appear in Parts 2 and 3 of the CC with the following exceptions:

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

1.3.1 Terminology

The term “User” is used in this document to refer to any operator of the TOE.

The term “User Data” is used in this document to refer to the data that is stored on the TOE.

2 TOE Description

This section provides a general overview of the TOE as an aid to understanding the general capabilities and security functions provided by the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

The EMC® Disk Library (EDL) is a disk-based backup solution. The EDL provides emulated physical tapes that can be used by backup servers connected to a Storage Area Network (SAN). These backup servers are used by an organization to perform backup of corporate user machines or corporate data servers. Since the EDL is a disk based backup solution, it offers significant speed improvements over traditional tape backup. However, since it emulates a traditional tape storage solution, it can be used in conjunction with an organization's existing backup solution. In a typical deployment scenario, the EDL is connected to a SAN through one or more Fibre Channel connections. Backup servers are also connected to this SAN to allow them to make use of the EDL.

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

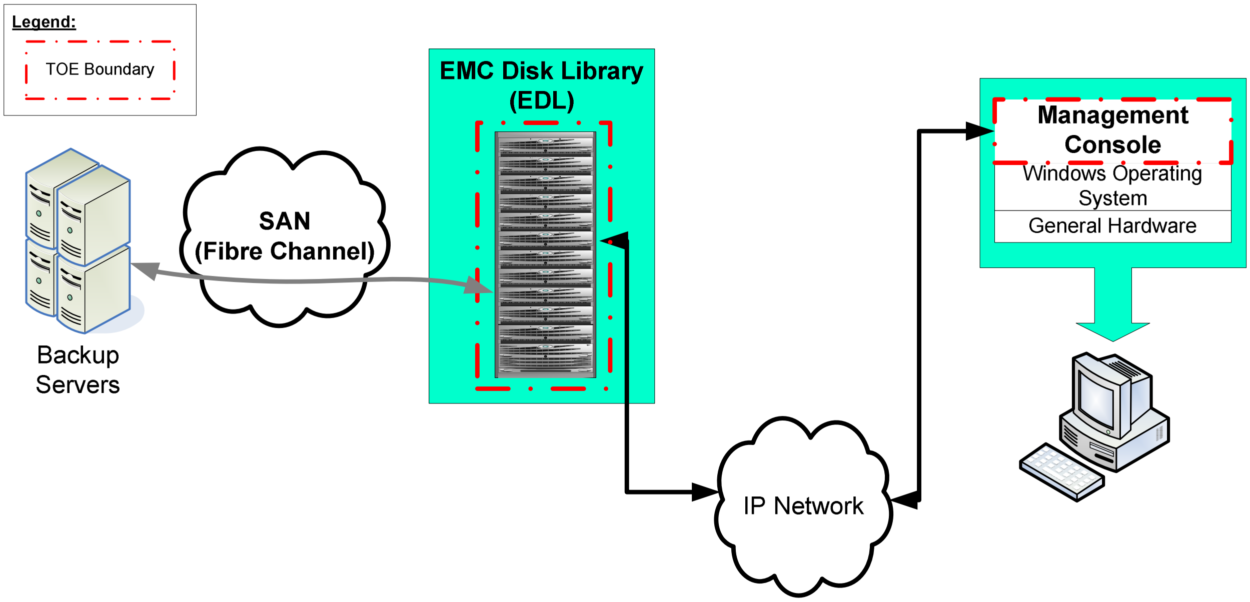

Figure 1 – TOE Boundary and Deployment Configuration

2.2 Product Description

The EMC Disk Library provides a disk based backup solution in a SAN environment. The product ensures that user data is stored securely and is also designed to ensure the integrity of the data that is entrusted to it.

The EDL provides the ability for administrators to configure virtual tapes. A virtual tape is the basic unit of storage provided to backup servers. Each virtual tape is created with either a fixed capacity or a variable capacity. The storage provided by the virtual tape exists on the drive storage system provided by the EDL and is stored using disks configured in a RAID[1] 5 configuration. RAID 5 provides for data integrity when an individual disk drive fails.

Each virtual tape that is created by an administrator can be assigned to a virtual tape library. A virtual tape library is a collection of virtual tapes. This virtual tape library is also configured to support a certain number of virtual tape drives. Since the EDL is designed to emulate traditional tape based backup hardware, the library, drives, and tapes must all be emulated. The virtual tape drive in the EDL emulates the interface of a traditional tape drive and allows a backup server to read and write data to a virtual tape.

In addition to grouping together virtual tapes and virtual tape drives, a virtual tape library also is assigned to one or more backup servers. Each backup server is connected to the SAN through a Fibre Channel card. Each Fibre Channel port on a Fibre Channel card has a World Wide Port Name (WWPN) associated with it that is transmitted through the SAN with every data request. Administrators of the EDL can configure the access permissions for each virtual tape library based on the backup server WWPN. This allows an administrator to restrict access to the virtual tapes contained within each virtual library to authorized backup servers.

Administration of the EDL is performed through the EMC Disk Library Management Console (EDL Console GUI[2] or the EDL CLI[3] via a Secure Shell (SSH) connection). The EDL Console is a Microsoft Windows-based application that allows administrators to manage the EDL. Administrators can create and manage virtual tapes, virtual tape drives, and virtual tape libraries through the EDL Console. The EDL Console is installed on a general purpose computer running the Windows Server 2003 SP2 operating system (Figure 1 above) which is connected to the TOE via a protected IP-based management network (shown as “IP network” in the figure above).

2.3 TOE Boundaries and Scope

This section will primarily address what physical and logical components of the TOE are included in evaluation.

2.3.1 Physical Boundary

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment. The TOE is a purpose-built hardware/software appliance (models DL4100, DL4200, and DL4400), and a software application which runs on a general purpose computer with a Windows-based operating system.

The TOE provides access control to virtual tape libraries, and through that to individual virtual tapes. For this to operate correctly, the WWPN that is provided to the TOE must be accurate and must not be spoofed. The TOE Environment is required to provide this assurance.

2.3.2 Logical Boundary

The Security Functional Requirements met by the TOE are usefully grouped under the following Security Function Classes:

- Identification and Authentication
- Protection of the TSF
- Security Management

[1] RAID – Redundant Array of Independent Disks

[2] GUI – Graphical User Interface

[3] CLI – Command Line Interface

- User Data Protection

2.3.2.1 Identification and Authentication

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

2.3.2.2 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TOE Security Function (TSF). The security functions in this evaluation are impractical to bypass because the TOE is designed in such a way that no access is possible without passing through key security features, such as identification and authentication and access control mediation. The TOE maintains its own domain for execution and does not share any hardware with other applications.

2.3.2.3 Security Management

The Security Management function provides administrators with the ability to properly manage and configure the TOE to store user data. Configuration of virtual tapes, virtual tape drives, virtual tape libraries, and administrator access is all supported through this security function.

2.3.2.4 User Data Protection

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

2.3.3 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

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

- Encryption of data to an external tape drive

3 Security Environment

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:

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

3.1 Assumptions

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

Table 2 – 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.

3.2 Threats to Security

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

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

The following threats are applicable:

Table 3 – Threats

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

3.3 Organizational Security Policies

There are no Organizational Security Policies.

4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the TOE's security needs.

4.1 Security Objectives for the TOE

The specific security objectives to be satisfied by the TOE are as follows:

Table 4 – TOE Security Objectives

Name	Description
O.ADMIN	The TOE must provide a method for administrative control of the TOE.
O.BYPASS	The TOE must ensure that the TSFs cannot be bypassed.
O.PROTECT	The TOE must protect data that it has been entrusted to protect.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

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

Table 5 – Security Objectives for the TOE Environment

Name	Description
OE.PROPER_NAME_ASSIGNMENT	The TOE environment must provide accurate World Wide Port Names for each system that communicates with the TOE
OE.SECURE_COMMUNICATIONS	The TOE environment must provide secure communications between systems connected to the Storage Area Network
OE.SECURE_SERVERS	The TOE environment must provide properly configured backup servers to communicate with the TOE.

4.2.2 Non-IT Security Objectives

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

Table 6 – Non-IT Security Objectives

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

5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE as well as SFRs met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3 above.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 7 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 7 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓	✓	
FDP_SDI.2	Stored data integrity		✓	✓	
FIA_UAU.2(a)	User authentication before any action				✓
FIA_UID.2(a)	User identification before any action				✓
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1(a)	Management of TSF data	✓	✓		✓
FMT_MTD.1(b)	Management of TSF data	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_RVM.1	Non-bypassability of the TSP				
FPT_SEP.1(a)	TSF domain separation				✓

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

Section 5.1 contains the security functional requirement components from the Common Criteria (CC) Part 2 with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.

5.1.1 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

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

[

a) Subjects: *Backup Servers*

b) Objects: *Virtual Tapes*

c) Operations: *Read and Write*

].

Dependencies: FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

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

[

Subject Attributes:

1. *Word Wide Port Name*
2. *Virtual Tape Library permissions*

Object Attributes:

1. *Word Wide Port Name*
2. *Virtual Tape Library permissions*

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*A valid Subject of the TOE is allowed to Read and Write to a Virtual Tape if* *the Subject has been given permissions to access the Virtual Tape Library that the Virtual Tape is assigned to*].

FDP_ACF.1.3

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

FDP_ACF.1.4

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

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

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: **FDP_SDI.1 Stored data integrity monitoring**

FDP_SDI.2.1

The TSF shall monitor user data stored within the TSC for [*integrity errors*] on all **user data** ~~objects~~, based on the following attributes: [*parity data for RAID 5*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*reconstruct the user data and notify an administrator*].

Dependencies: **No dependencies**

5.1.2 Class FIA: Identification and Authentication

FIA_UAU.2(a) 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(a) User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.3 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*] to restrict the ability to [*query, modify, delete*] the security attributes [*Virtual Tapes assigned to Virtual Tape Libraries and Subject permissions on Virtual Tape Libraries*] to [*the dladmin and dlroot roles*].

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.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

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

FMT_MSA.3.2

The TSF shall allow the [*the dladmin role*] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MTD.1(a) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*query*] the [*virtual tape library information*] to [*the dlmon, dladmin, dlroot, and root roles*].

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

FMT_MTD.1(b) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*query, modify, delete, [create]*] the [*virtual tapes and virtual tape libraries*] to [*the dladmin and dlroot roles*].

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

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 security management functions:

[

a) Management of security functions behaviour;

b) Management of TSF data;

c) Management of security attributes

].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*as the authorized identified roles in* Table 8].

Table 8 – Authorized Roles

Roles	Description
dladmin	This role can access all administrative functions available through the EDL Console application. This role can manage all virtual tape libraries, virtual drives, and virtual tapes. This role can perform all functionality of dlmon.
dlmon	This role can view all TOE information through the EDL Console application.
dlroot	This role is a special role reserved for use by EMC service technicians, and is not available for use by the end-user. This role can access the TOE through an SSH interface on the EDL and

Roles	Description
	can start and stop services. dlroot can perform all functionality available to dladmin.
root	This role is a special role reserved for use by EMC service technicians, and is not available for use by the end-user. This role can access the TOE through a directly attached serial connection or a directly attached keyboard and monitor. root can not access the TOE via SSH, or through the EDL Console application. root is the “superuser” and can perform any action.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.4 Class FPT: Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

FPT_SEP.1(a) TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1(a)

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2(a)

The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.2 Security Functional Requirements on the IT Environment

The TOE has the following security requirements for its IT environment. The stated Security Functional Requirements on the IT Environment of the TOE presented in this section has been drawn from Part 2 of CC Version 2.3 and hence conformant to CC Version 2.3 Part 2.

Table 9 – Security Functional Requirements for the Environment

Name	Description	S	A	R	I
FIA_UAU.2(b)	User authentication before any action			✓	✓
FIA_UID.2(b)	User identification before any action			✓	✓
FPT_SEP.1(b)	TSF domain separation			✓	✓

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

5.2.1 Class FIA: Identification and Authentication

FIA_UAU.2(b) User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1

The TSF shall require each user **of an Backup Server** to be successfully authenticated **to the TOE Environment** before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2(b) User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

The TSF shall require each user **of an Backup Server** to identify itself **to the TOE Environment** before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

FPT_SEP.1(b) TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1(b)

The ~~TSF~~ **TOE Environment** shall maintain a security domain for ~~its own~~ **the TOE's** execution that protects ~~it~~ **the TOE** from interference and tampering by untrusted subjects.

FPT_SEP.1.2(b)

The ~~TSF~~ **TOE Environment** shall enforce separation between the security domains of subjects in the ~~TSC~~ **TOE Environment's Scope of Control**.

Dependencies: No dependencies

5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from Part 3 of the CC at EAL2+ augmented with ALC_FLR.1. Table 10 – Assurance Requirements summarizes the requirements.

Table 10 – Assurance Requirements

Assurance Requirements	
Class ACM: Configuration management	ACM_CAP.2 Configuration items
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Flaw Remediation	ALC_FLR.1 Basic flaw remediation
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

6 TOE Summary Specification

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

6.1 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 are suitable to satisfy the necessary requirements.

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

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

6.1.1 Identification and Authentication

The Identification and Authentication security function provides the TOE with the ability to govern access by administrators. Administrators of the TOE can access the TOE in one of two methods. An administrator can manage the TOE through the EDL Console, a Microsoft Windows graphical user interface. An administrator can also manage the TOE through the EDL CLI via an SSH connection to the TOE. Prior to allowing access through these interfaces, the TOE requires an Administrator to be identified using a username and password. Before successful completion of the security function, an administrator is unable to perform any management function.

Identification and Authentication of backup servers connecting to the TOE to access a virtual tape library LUNs is provided by the TOE Environment through the proper assignment and use of Word Wide Port Names (WWPNs).

6.1.2 Protection of the TSF

Protection of the TSF provides for the integrity of the mechanisms that protect the TOE. The TOE is a purpose built hardware appliance. It does not share memory or processors with any other application or system. The TOE maintains its own domain for its execution. Interfacing with the TOE is only done through well defined interfaces, each utilizing security functions to maintain the security of that interface. The TOE relies on its environment to provide protection from physical tampering.

Non-bypassability of the TSP is provided through basic configuration and enforcement of the security mechanisms. All Administrators and Users of the TOE must be authenticated prior to performing any security functionality. Once authenticated, Administrators and Users can only perform operations which they have been explicitly granted permission to perform. The TOE uses unique sessions for each user of the TOE and maintains separation between concurrent operators.

6.1.3 Security Management

The purpose of the TOE is to provide a virtual tape backup system to backup servers attached to a SAN. The TOE provides mechanisms to govern which backup servers can access which virtual tape libraries, and therefore which virtual tapes. The Security Management function allows administrators to properly configure this functionality.

Management of the TOE typically occurs through EDL Console. Administrators using this interface are assigned one of two roles: dladmin or dlmon. The dladmin role is responsible for all configuration of the TOE. The dladmin can manage virtual tapes, virtual tape drives, and virtual tape libraries. The dladmin role is responsible for ensuring that only those backup servers that should have access to a given virtual tape are granted access. The dladmin role is also responsible for managing data integrity through the RAID features of the TOE. The dlmon role is provided to allow monitoring of the TOE. This allows an administrator who is tasked with monitoring the status of the TOE access to the TOE through the EDL Console, but does not grant the dlmon role permission to change any configuration settings. The dladmin role possesses all the privileges that the dlmon role has.

The TOE also provides access via SSH to the EDL. The dlroot role can access the TOE via SSH to perform certain specific management functions not available through the EDL Console, as well as all functionality of the dladmin role. The dlroot user can view information on system processes and start and stop system processes. There is also a root role which provides access to the embedded operating system. The dlroot and root roles are special roles used by EMC service technicians, and are not used by the end-user.

6.1.4 User Data Protection

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

Using the Security Management security function, administrators of the TOE can configure virtual tape libraries for access by backup servers to provide a well defined interface to the TOE. Virtual tapes can be created and placed into the virtual tape libraries, which provide the backup servers with allocated storage on the TOE. Administrators can limit access to the allocated storage (the virtual tapes) by granting a backup server access to one or more Virtual Tape Libraries by specifying the WWPN and type of access granted to the Backup Server within the EDL Console.

The TOE also provides for the integrity of user data. Every virtual tape that is created is stored within a storage device configured with RAID 5. RAID 5 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 using 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 the user data continues, however the performance will be in a degraded state until the rebuild completes.

6.2 TOE Security Assurance Measures

EAL2+ was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL2+ level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 12 – Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ACM_CAP.2	EMC Disk Library – Configuration Management: Capabilities
ADO_DEL.1	EMC Disk Library – Delivery and Operations: Secure Delivery
ADO_IGS.1	[Installation and Setup Procedure]
ADV_FSP.1	EMC Disk Library – Development: High Level Design, Functional Specification, and Representation Correspondence
ADV_HLD.1	EMC Disk Library – Development: High Level Design, Functional Specification, and Representation Correspondence
ADV_RCR.1	EMC Disk Library – Development: High Level Design, Functional Specification, and Representation Correspondence v0.1
AGD_ADM.1	[Administrator Guides]
AGD_USR.1	[User Guides]
ALC_FLR.1	EMC Disk Library – Life Cycle Support: Flaw Remediation
ATE_COV.1	EMC Disk Library – Functional Tests and Coverage
ATE_FUN.1	EMC Disk Library – Functional Tests and Coverage
ATE_IND.2	Provided by laboratory evaluation
AVA_SOF.1	EMC Disk Library – Vulnerability Assessment
AVA_VLA.1	EMC Disk Library – Vulnerability Assessment

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

There are no Protection Profile claims for this Security Target.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Security Objectives Rationale

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

8.1.1 Security Objectives Rationale Relating to Threats

Table 13 – Security Objectives Rationale Relating to Threats

Threats	Objectives	Rationale
T.DATA_CORRUPTION Data could become corrupted due to hardware failure or incorrect system access.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN supports the mitigation of this threat by allowing an administrator to properly configure the mechanisms of the TOE designed to mitigate this threat.
	O.BYPASS The TOE must ensure that the TSFs cannot be bypassed.	The objective O.BYPASS ensures that the protection mechanisms of the TOE designed to mitigate this threat cannot be bypassed.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT mitigates this threat by providing mechanisms to protect the data that has been entrusted to the TOE.
T.IMPROPER_SERVER A system connected to the TOE could be used by Users of the TOE or attackers to gain access to data that it was not intended to access.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN supports the mitigation of this threat by allowing an administrator to properly configure the mechanisms of the TOE designed to mitigate this threat.
	O.BYPASS The TOE must ensure that the TSFs cannot be bypassed.	The objective O.BYPASS ensures that the protection mechanisms of the TOE designed to mitigate this threat cannot be bypassed.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT ensures that the TOE provides adequate mechanisms to give only authorized servers access to the appropriately authorized data.

Threats	Objectives	Rationale
	OE.PROPER_NAME_ASSIGNMENT The TOE environment must provide accurate World Wide Port Names for each system that communicates with the TOE	OE.PROPER_NAME_ASSIGNMENT ensures that the World Wide Port Names provided to the TOE are accurate. This allows the mechanisms provided by O.PROTECT to properly protect data.
	OE.SECURE_COMMUNICATIONS The TOE environment must provide secure communications between systems connected to the Storage Area Network	OE.SECURE_COMMUNICATIONS ensures that all communications with the TOE are secure for administration of the TOE, internal TOE communications, and data sent to or from the TOE.
	OE.SECURE_SERVERS The TOE environment must provide properly configured backup servers to communicate with the TOE.	OE.SECURE_SERVERS mitigates this threat by ensuring that each server connected to the Storage Area Network operates properly and does not intentionally compromise data.

8.1.2 Security Objectives Rationale Relating to Assumptions

Table 14 – Security Objectives Rationale Relating to Assumptions

Assumptions	Objectives	Rationale
A.PHYSICAL Physical security will be provided for the TOE and its environment.	OE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	Physical security is provided within the domain for the value of the IT resources protected by the operating system and the value of the stored, processed, and transmitted information. OE.PHYSICAL satisfies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.	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. OE.MANAGE satisfies this assumption.
A.NOEVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	OE.NOEVIL Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained and follow all administrator guidance.	Sites using the TOE ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance. OE.NOEVIL satisfies this assumption.

8.2 Security Functional Requirements Rationale

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

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 15 – SFR Rationale Related to TOE Objectives

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method for administrative control of the TOE.	FIA_UAU.2(a) User authentication before any action	The TOE will properly identify and authenticate all administrators.
	FIA_UID.2(a) User identification before any action	The TOE will properly identify and authenticate all administrators.
	FMT_MSA.1 Management of security attributes	Security attributes of the TOE can only be changed by authorized administrators.
	FMT_MSA.3 Static attribute initialisation	Permissive values for data access are provided, and the TOE administrator can change them when a data object is created.
	FMT_MTD.1(a) Management of TSF data	The ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_MTD.1(b) Management of TSF data	The ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_SMF.1 Specification of management functions	FMT_SMF specifies each of the management functions that are utilized to securely manage the TOE.
	FMT_SMR.1 Security roles	Specific roles are defined to govern management of the TOE.
O.BYPASS The TOE must ensure that the TSFs cannot be bypassed.	FPT_RVM.1 Non-bypassability of the TSP	The TOE ensures that policy enforcement functions are invoked and succeed before each function is allowed to proceed.

Objective	Requirements Addressing the Objective	Rationale
	FPT_SEP.1(a) TSF domain separation	The TOE maintains a security domain for its execution that protects it from interference and tampering.
O.PROTECT The TOE must protect data that it has been entrusted to protect.	FDP_ACC.1 Subset access control	The TOE has an access control policy which ensures that only authorized servers gain access to data within the TOE.
	FDP_ACF.1 Security attribute based access control	The TOE provides access control functionality to manage access to data within the TOE.
	FDP_SDI.2 Stored data integrity	The TOE protects stored data integrity by checking for integrity errors on the data.

8.2.2 Rationale for Security Functional Requirements of the IT Environment

Table 16 – SFR Rationale Related to Objectives of the TOE Environment

Objective	Requirements Addressing the Objective	Rationale
OE.SECURE_SERVERS The TOE environment must provide properly configured backup servers to communicate with the TOE.	FIA_UAU.2(b) User authentication before any action	The TOE will not give access to a user until the environment has properly authenticated the TOE user.
OE.PROPER_NAME_ASSIGNMENT The TOE environment must provide accurate World Wide Port Names for each system that communicates with the TOE	FIA_UID.2(b) User identification before any action	The TOE will not give access to a user until the environment has properly identified the TOE user.
OE.SECURE_COMMUNICATIONS The TOE environment must provide secure communications between systems connected to the Storage Area Network	FPT_SEP.1(b) TSF domain separation	The TOE Environment ensures that communications to and from the TOE are routed to the proper network host.

8.3 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2+, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The inclusion of the ALC_FLR.1 ensures that there are flaw remediation procedures that describe how to track all reported security-relevant flaws in each release of the TOE and that identified flaws in the TOE are tracked from discovery through mitigation.

8.4 Rationale for Refinements of Security Functional Requirements

The following refinements of Security Functional Requirements from CC version 2.3 have been made to clarify the content of the SFRs, and make them easier to read:

The words “no additional rules” were added, and others stricken, to FDP_ACF.1.

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

The words “to the TOE Environment” were added to FIA_UAU.2(b) and FIA_UID.2(b).

8.5 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 17 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 17 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_SDI.2	No Dependencies	✓	
FIA_UAU.2(a)	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency.
FIA_UAU.2(b)	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency.
FIA_UID.2(a)	No Dependencies	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UID.2(b)	No Dependencies	✓	
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(a)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(b)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No Dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency.
FPT_RVM.1	No Dependencies	✓	
FPT_SEP.1(a)	No Dependencies	✓	

8.6 TOE Summary Specification Rationale

8.6.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (Section 6.1) describes a security function of the TOE. Each description is organized by set of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. These sets of security functions work together to satisfy all of the security functional requirements. Furthermore, all of the security functions are necessary in order for the TSF to meet the security functional requirements. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 11 identifies the relationship between SFR and security functions, showing that all SFR are addressed and all security functions are necessary (i.e., they correspond to at least one SFR).

8.6.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL2+ was chosen to provide a basic level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

8.6.2.1 Configuration Management

The *EMC Disk Library – Configuration Management: Capabilities* documentation provides a description of tools used to control the configuration items and how they are used at the EMC. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Configuration Items

8.6.2.2 Delivery and Operation

The *EMC Disk Library – Delivery and Operations: Secure Delivery* documentation provides a description of the secure delivery procedures implemented by EMC to protect against TOE modification during product delivery. The Installation Documentation provided by EMC details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation, and Start-Up Procedures

8.6.2.3 Development

The *EMC Disk Library – Development: High Level Design, Functional Specification, and Representation Correspondence* design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

- Informal Functional Specification
- Descriptive High-Level Design
- Informal Representation Correspondence

8.6.2.4 Guidance Documentation

The EMC Guidance documentation provides administrator and user guidance on how to securely operate the TOE. The Administrator Guidance provides describes the security functions provided by the TOE. Additionally, it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they are to be used and explains the user's role in maintaining the TOE's security. EMC provides combined versions of documents which include Administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator users of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance

8.6.2.5 Life Cycle Support

The *EMC Disk Library – Life Cycle Support: Flaw Remediation* documentation describes the processes that EMC follows to capture, track, and correct flaws (or "bugs") that are found within the TOE. The documentation demonstrates that all discovered flaws are recorded and that the process ensures that flaws are tracked through their entire life cycle.

Corresponding CC Assurance Components:

- Basic Flaw Remediation

8.6.2.6 Tests

There are a number of components that make up the *EMC Disk Library – Functional Tests and Coverage* documentation. The Coverage Analysis demonstrates the testing performed against the Functional Specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. EMC Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing

8.6.2.7 Vulnerability and TOE Strength of Function Analyses

The *EMC Disk Library – Vulnerability Assessment documentation* is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

Corresponding CC Assurance Components:

- Strength of TOE Security Function analysis
- Vulnerability Analysis

8.7 Strength of Function

SOF rating of SOF-basic was claimed for this TOE to meet the EAL2+ assurance requirements. This SOF is sufficient to resist the threats identified in Section 3 of the Security Target. Section 8.1 of the Security Target provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8.2 of the Security Target demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and Department of Defense (DoD) low robustness environments processing unclassified information.

The relevant security functions and security functional requirements which have probabilistic or permutational functions are:

- FIA_UAU.2 - User Authentication before any action

9 Acronyms and Terminology

Table 18 – Acronyms and Terminology

Acronym	Definition
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
EAL	Evaluation Assurance Level
EDL	EMC Disk Library
EDL Console	EDL Management Console
GUI	Graphical User Interface
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
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
SOF	Strength of Function
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
Virtual Tape	A logical representation of a physical tape
Virtual Tape Drive	A logical representation of a physical tape drive
Virtual Tape Library	A logical representation of an automated collection of tapes
WWPN	Word Wide Port Name