EMC Corporation
EMC Celerra Network Server Version 5.5 running on EMC® Celerra® NSX series and EMC® Celerra® NS series

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 1.0

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
0.1	2006-06-29	Matthew Appler	Initial draft.
0.2	2006-06-30	Nathan Lee	Updated threat text based on lab feedback.
0.3	2006-07-05	Nathan Lee	Updated EAL and associated text.
0.4	2006-07-06	Nathan Lee	Added *Life Cycle Support* subsection to TSS Rationale section.
0.5	2006-11-03	Christie Kummers	Minor updates and changes in response to lab verdicts.
0.6	2006-11-22	Christie Kummers	Minor updates and changes to Section 1.
0.7	2006-12-13	Christie Kummers	Minor updates and changes throughout.
0.8	2007-02-21	Christie Kummers	Minor updates and changes throughout.
0.9	2007-07-24	Christie Kummers	Updates in response to Lab ORs v1.1 and v1.2.
1.0	2007-09-20	Nathan Lee Elizabeth Pugrud	Additional Environmental SFR defined with additional appropriate updates throughout to incorporate it.

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 Celerra Network Server Version 5.5 running on EMC® Celerra® NSX series and EMC® Celerra® NS series, and will hereafter be referred to as the TOE or the Celerra Network Server throughout this document. The Celerra Network Server is a Network Attached Storage (NAS) device that provides access to Storage Area Network (SAN) based storage through standard file sharing protocols.

1.1 Overview

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 (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target, TOE and CC Identification and Conformance

Table 1 - ST, TOE, and CC Identification and Conformance

ST Title	EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series Security Target
Version	Version 1.0
Author	Corsec Security, Inc. Nathan Lee and Matthew Appler
TOE Identification	EMC Celerra Network Server Version 5.5.30.4 running on EMC Celerra NSX series and EMC Celerra NS series
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; 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	Network Attached Storage (NAS), Storage Area Network (SAN)

1.3 Conventions and Terminology

1.3.1 Conventions

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

The Common Criteria (CC) allows for several operations to be performed on security 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.

1.3.2 Terminology

The term “User” is used in this document to refer to any operator of the TOE who is utilizing it to store data.

The term “User Data” is used in this document to refer to the data that an operator has used to store data on the storage system.

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 Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series is a Network Attached Storage (NAS) server that provides Internet Protocol (IP) or Fibre Channel[1] access to storage, either locally or on a Storage Area Network (SAN). The purpose of a SAN is to allow many different application servers to share storage provided by centrally managed storage devices. The Celerra Network Server supports several protocols to provide file sharing access to centrally managed storage.

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

[1] Fibre Channel is a serial data transfer interface that operates over copper wire and/or optical fiber at data rates currently supported at 400 MB/s.

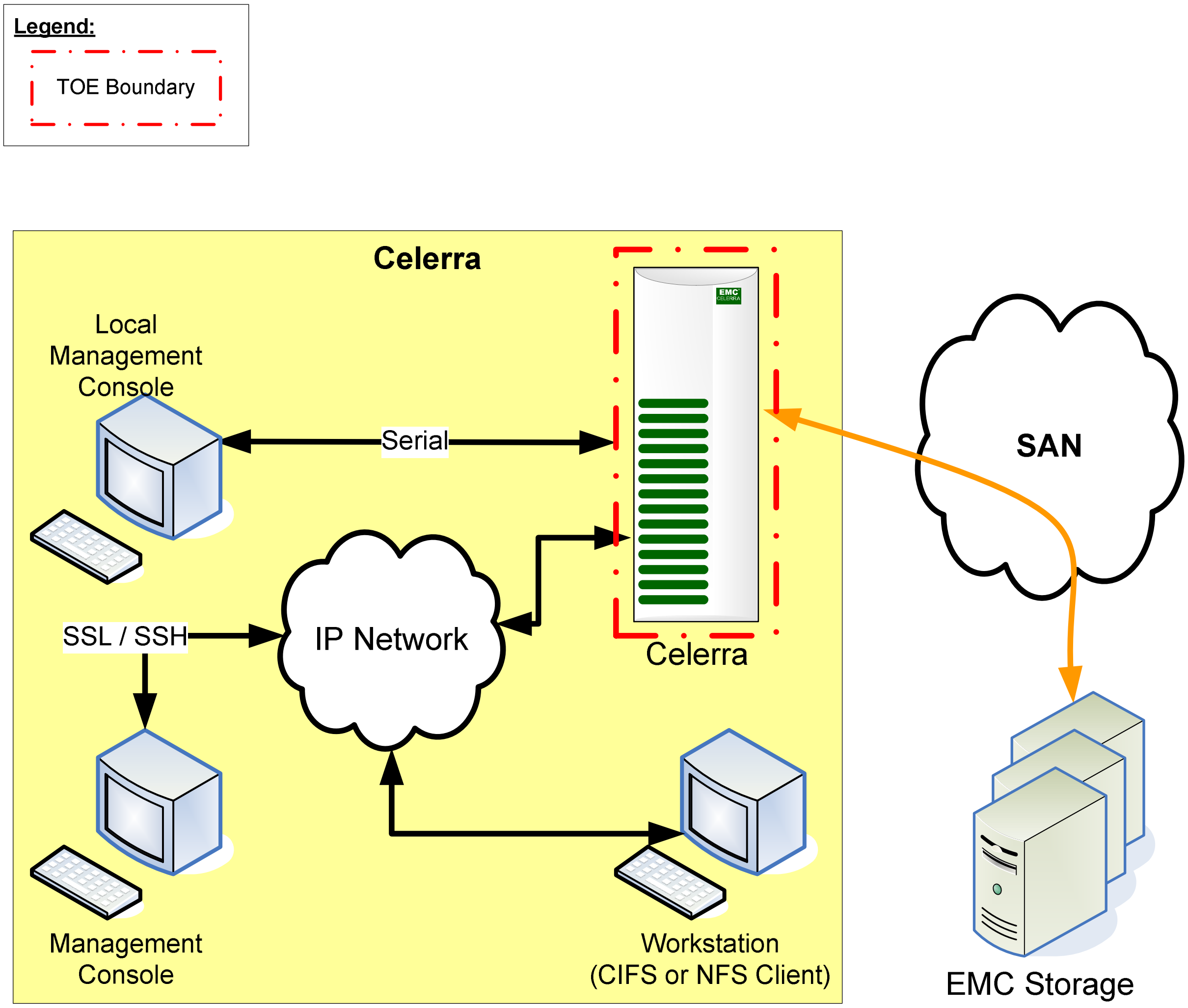

Figure 1 - Deployment Configuration of the TOE

2.2 Product Description

As described above, the EMC Celerra Network Server is a Network Attached Storage (NAS) gateway solution. The Celerra Network Server provides storage access to clients and servers in a corporate network through a variety of access protocols. These protocols include:

- Common Internet File System (CIFS)[2]
- Network File System (NFS)[3] versions 2, 3, and 4
- FTP[4] and TFTP[5]
- iSCSI[6]

2.2.1 Physical Description of the Product

To implement this functionality, the Celerra Network Server is architected using two types of hardware components: the Control Station and Data Movers. Each of these is described below.

The Control Station is a dedicated management computer that monitors and controls all components of the Celerra Network Server. The Control Station provides access to the administrative functionality of the Celerra Network Server software. It contains utilities for installing and configuring the Celerra Network Server, maintaining the system, and monitoring system performance. The Control Station runs a set of programs that are collectively referred to as the Control Station software. The Control Station itself uses an EMC-customized version of Linux as its operating system. The Control Station connects internally to each of the Data Movers within the Celerra Network Server. Only Control Station Administrators are granted access to the Celerra Control Station.

The Data Movers are the Celerra Network Server components that perform the actual transfer of data between the storage system and the network client. The Data Mover operating system is referred to as DART (Data Access in Real Time). Administrators do not typically manage a Data Mover directly. Rather, the Control Station is used to send commands to an individual Data Mover. The Celerra Network Server can have from 1 to 8 Data Movers. Additionally, there are several different models of Data Movers. However, use and management of all Data Movers is performed the same way.

2.2.2 Logical Description of the Product

The Celerra Network Server presents itself as one or more standard network-based file servers to client machines. In fact, each Data Mover on the Celerra Network Server can host one or more "virtual servers" that present shared file systems to client machines. The type of server and protocols that are supported by that server (CIFS, NFS, etc.) are configurable by an Administrator. Client machines, with the appropriate access privileges, can then use the Celerra Network Server to store and access data as they would any other network-based file server. Additionally, shared file systems can be configured for FTP or TFTP access.

[2] CIFS is a platform-independent file sharing system commonly used by Microsoft Windows network file sharing

[3] NFS is a platform-independent file sharing system commonly used by UNIX and UNIX variants for file sharing

[4] File Transfer Protocol

[5] Trivial File Transfer Protocol

[6] internet Small Computer System Interface

The Celerra Network Server is responsible for enforcing all access permissions for User Data. Each "virtual server" on the Celerra Network Server 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, the Celerra Network Server 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 Data Mover User. User Data can be stored directly on the Celerra Network Server or storage of User Data can be provided by the SAN.

The internal storage or the SAN that the Celerra Network Server is connected to is configured to provide a storage system for use by the Celerra Network Server. This storage system stores and retrieves block units of data for the Celerra Network Server. 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 the Celerra Network Server as Logical Units (LUNs). Each LUN is a useable storage system volume that can be used to store User Data by the Celerra Network Server.

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 2 illustrates the physical scope and the physical boundary of the Celerra Network Server and ties together all of the components of the TOE and the constituents of the TOE Environment. The Celerra Network Server will hereafter be referred to as the TOE throughout this document.

The TOE is a NAS product which runs on the platform as specified above. The evaluated configuration of the TOE includes the following Celerra Network Server models: NS20, NS40, NS40G, NS80, NS80G, NS350, NS500, NS500G, NS700, NS700G, NS704, NS704G, and NSX.[7] The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- Control Station – 1 to 2 Control Stations v5.5 are present in the Celerra Network Server. The Control Station is a dedicated management computer used to manage the Celerra Network Server
- Data Movers – 1 to 8 Data Movers are present in a Celerra Network Server running DART v5.5. Each Data Mover is used to mediate access to storage provided by a SAN to client machines that are connected via an IP network. The evaluated configuration of the TOE includes the following Data Movers models: X-Blade 40 (installed on the NS20, NS40, and NS40G models), X-Blade 60 and X-Blade 65 (installed on the NS80, NS80G, and NSX models[8]), NS500 (installed on the NS350, NS500, and NS500G models), and NS700 (installed on the NS700, NS700G,NS704, and NS704G models).

[7] The TOE models that end with a "G" as well as the NSX model are the Celerra Gateway products. These models consist of only the Celerra Control Station(s) and Data Mover(s). The SAN storage array is configured and purchased separately. The TOE models without the "G" (with the exception of the NSX model) are the integrated TOE models that include a CLARiiON™ storage array.

[8] The Celerra Network Server NSX model can have both the X-Blade 60 and X-Blade 65 model Data Movers installed in the TOE at the same time.

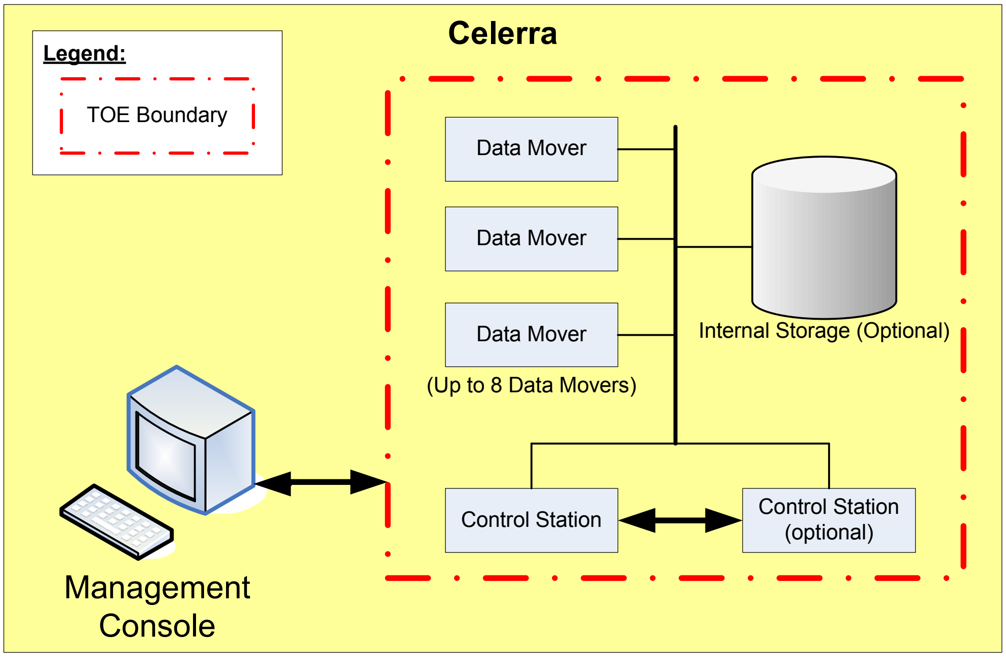

Figure 2 - Physical TOE Boundary

2.3.1.1 Security Considerations of the TOE Environment

The TOE relies on secure access provided by the SAN 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. This functionality requires that the communications path to the SAN and the storage that is provided by the SAN be managed properly.

2.3.2 Logical Boundary

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:

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

2.3.2.1 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 each of the Data Movers in the TOE. Users of the TOE are identified and authenticated, either by the TOE or the TOE Environment. These Data Mover 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 Data Mover Users of TOE to that object.

2.3.2.2 Identification and Authentication

This function of the TOE is used to identify and authenticate each operator of the TOE. In the case of Control Station Administrators, the TOE provides username and password verification functionality. Data Mover Users of the TOE can be authenticated directly by the TOE or can be authenticated by a separate Active Directory, Kerberos, or NFS client machine. This functionality is configured by an Administrator.

2.3.2.3 Security Management

The Security Management functionality of the TOE specifies several aspects of management of the TOE Security Function (TSF). Proper management of the TSF is required to properly mediate access to User Data.

2.3.2.4 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the 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.

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

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

- iSCSI functionality
- Access Control Levels for Control Station Administrators
- Multi-Path File System
- Replication Technologies
- Celerra FileMover

The TOE supports several File System Access Policies. For the purposes of this evaluation, only the “MIXED” Access Policy is to be evaluated. The “NATIVE”, “NT”, “UNIX”, “SECURE”, and “MIXED_COMPAT” Policies are excluded from the evaluation.

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.

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

3.2 Threats to Security

This section identifies the threats to the 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:

Name	Description
T.BYPASS	The TOE could be bypassed by a server with direct access to the SAN.
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.

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 are as follows:

Name	Description
O.ADMIN	The TOE must provide a method for administrative control of the TOE.
O.BYPASS	The TOE must ensure that the TSF cannot be bypassed.
O.I&A	The TOE will uniquely identify users and will authenticate the claimed identity before granting a User access to the TSF's when local authentication is required.
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:

Name	Description
OE.BYPASS	The TOE environment must ensure that the TSF cannot be bypassed
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

Name	Description
OE.SECURE_SERVERS	The TOE environment must provide properly configured authentication 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.

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.
OE.PROTECT	The TOE environment must protect the data it has been entrusted to protect

5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE as well as Security Functional Requirements met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.1.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 2 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 2 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FIA_ATD.1(a)	User attribute definition		✓		✓
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	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_RVM.1(a)	Non-bypassability of the TSP				✓
FPT_SEP.1	TSF domain separation				

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

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: *CIFS and NFS Users*

b) Objects: *Files and Directories*

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.1 Security attribute based access control

Application Note: The CIFS naming convention has been used for operations. Equivalent operations are provided via NFSv4, but may be named slightly differently by NFS clients. FTP, NFSv2, and NFSv3 access supports a subset of these operations.

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. *UserID*
2. *GroupIDs*

Object attributes:

1. *UTF-8 Filename*
2. *UTF-16 Filename*
3. *8.3 MS-DOS Filename*
4. *Access Control List*

].

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 perform an operation if the contents of the Access Control List for the object authorize the UserID or a GroupID of the Subject to perform the desired operation*].

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

[

- *For CIFS access, subjects that are members of the group Domain Administrators shall be authorized to backup, restore, and take ownership of all objects*
- *For NFS access, subjects that are authorized as superusers can perform all operations on all objects*

].

FDP_ACF.1.4

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 UserID or a GroupID of the Subject to perform the desired operation*].

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

5.1.1 Class FIA: Identification and Authentication

FIA_ATD.1(a) User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [*UserID, one or more GroupIDs, and a password*].

Dependencies: No dependencies

Application Note: "Users" refers to Data Mover Users, defined in FMT_SMR.1. The TOE allows either local or remote management of Data Mover Users. This SFR applies when local administration of Data Mover Users is selected for the TOE.

FIA_UAU.2(a) User authentication before any action

Hierarchical to: FIA_UAU.1

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

Application Note: The TOE allows either local or remote management of users. This SFR applies when local administration of users is selected for the TOE

FIA_UID.2(a) User identification before any action

Hierarchical to: FIA_UID.1

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

Application Note: The TOE allows either local or remote management of users. This SFR applies when local administration of users is selected for the TOE

5.1.2 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 [*modify, delete, [add]*] the security attributes [UserID and GroupID assignment] to [*Authorized Users*].

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

Application Note: Authorized Users are either superusers in the case of NFS, or members of the Local Administrator or Domain Administrator groups for CIFS.

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 [*Object Owner*] 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 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*modify, delete,[add]*] the [*Control Station Administrator and Data Mover User accounts*] to [*Control Station Administrators*].

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 security management functions:

[

1. *Management of security functions behavior;*
2. *Management of TSF data;*
3. *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

[

1. *Control Station Administrator*
2. *Data Mover User*

].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.3 Class FPT: Protection of the TSF

FPT_RVM.1(a) 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 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1

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

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 SFR 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.

Name	Description	S	A	R	I
FIA_ATD.1(b)	User attribute definition		✓	✓	✓
FIA_UAU.2(b)	User authentication before any action			✓	✓
FIA_UID.2(b)	User identification before any action			✓	✓
FPT_RVM.1(b)	Non-bypassability of the TSP				✓
FTP_ITC.1	Inter-TSF trusted channel			✓	

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

FIA_ATD.1(b) User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1

The ~~TSF~~ **TOE Environment** shall maintain the following list of security attributes belonging to individual users: [*UserID and one or more GroupIDs*].

Dependencies: No dependencies

Application Note: The TOE allows either local or remote management of users. This SFR applies when remote Active Directory or NFS v2 and v3 administration of Data Mover Users is selected for the TOE

FIA_UAU.2(b) User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1

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

Dependencies: FIA_UID.1 Timing of identification

Application Note: The TOE allows either local or remote management of users. This SFR applies when remote Active Directory, Kerberos, or NFS v2 and v3 administration of Data Mover Users is selected for the TOE.

FIA_UID.2(b) User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1

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

Dependencies: No dependencies

Application Note: The TOE allows either local or remote management of users. This SFR applies when remote Active Directory, Kerberos, or NFS v2 and v3 administration of Data Mover Users is selected for the TOE.

FPT_RVM.1(b) Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

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

Dependencies: No dependencies

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1

The ~~TSF~~ **TOE Environment** shall provide a communication channel between ~~itself and a remote trusted IT product~~ **systems connected to the Storage Area Network** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

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+. Table 3 – Assurance Requirements summarizes the requirements.

Table 3 – 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

Assurance Requirements	
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 4 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Identification and Authentication	FIA_ATD.1(a)	User attribute definition
	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(a)	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control

6.1.1 Identification and Authentication

The TOE performs identification and authentication of both Administrators and Data Mover 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.

6.1.1.1 Administrative I&A

Control Station 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. 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.

6.1.1.2 User I&A

Data Mover Users of the TOE are defined as those subjects that wish to use the TOE to store and mediate access to data. Data Mover Users of the TOE would typically not be Administrators (although they could be). The way identification and authentication works on the TOE for Data Mover Users is configurable by an Administrator. This security function provides the ability for the TOE to internally identify and authenticate users, and manage their attributes. The TOE can also utilize this functionality through its environment.

For CIFS and NFSv4 access, the TOE will identify and authenticate the username and password with each request for access. If configured for local administration of Data Mover Users, the TOE will refer to its list of authorized users and groups. If the user can be authenticated, the function will allow the user access. Access to individual files and directories is then governed by the User Data Protection security function. If configured to use Active Directory or Kerberos, the TOE will communicate with the respective server to authenticate the user and provide a list of groups that the user is a member of. Authentication will then be performed by the TOE.

For NFSv2 and NFSv3, the server from which the request is coming has already identified and authenticated each Data Mover User. For this configuration, the TOE relies on its environment to perform proper identification and authentication. The TOE also relies on the environment to provide a list of GroupIDs that the user has been assigned.

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

6.1.3 Security Management

The purpose of the TOE is to allow Data Mover Users, connected to an IP network, to securely store data on internal storage or on storage devices connected to a SAN. The Security Management function allows authorized Administrators to properly configure this functionality.

Management of the TOE is typically performed by Control Station Administrators through a web-based application called the Celerra Manager. Control Station Administrators can also manage the TOE through a command line interface (CLI) through the Control Station.

Control Station 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 Celerra Administrator also manages individual Data Movers, creates and manages "virtual servers", and maps shares on those file servers to configured file systems. The Celerra Administrator is responsible for configuring the access control mechanisms to be supported by each "virtual server".

6.1.4 User Data Protection

The TOE enforces the Discretionary Access Control SFP[9] on each Data Mover User of the TOE based on the security attributes of that user.

> **Discretionary Access Control SFP*:*** The TOE enforces the Discretionary Access Control SFP on Data Mover Users by assigning access privileges to Users based on their UserID and GroupIDs. The ability to perform operations on objects, which are governed by the Discretionary Access Control SFP, are granted to Data Mover Users by an object's owner. Thus, a Data Mover User is allowed to perform an operation on an object so long as permission is granted to the User within the object's ACL. A Data Mover User can also be denied the ability to perform an operation on an object if the contents of the object's ACL deny the desired operation based on the UserID or GroupID of the User.
>
> Under the CIFS access protocol, Data Mover Users are allowed to backup, restore, and take ownership of all objects if they are member of the local Administrators group. For the NFS access protocol, Data Mover Users who are *superusers* can perform all operations on all objects.

The primary purpose of the TOE is to provide the User Data Protection security function. The TOE is designed to mediate access to files and directories for authorized Data Mover Users. These files and directories are either stored within the TOE or stored remotely on a storage system. The TOE accesses the storage system through a SAN to provide Data Mover Users access to their data through several standard IP network file sharing mechanisms.

Identification and authentication of Data Mover Users is performed by the Identification and Authentication security function. Once a user has been successfully authenticated, the TOE is then in possession of the UserID and one or more GroupIDs for that User. These credentials are used to mediate access to files and directories.

Each file and directory managed by the TOE has an ACL associated with it. This ACL contains one or more Access Control Entries (ACEs). Each ACE contains a UserID or GroupID and a set of permissions that are granted or explicitly denied to that UserID or GroupID. Whenever a Data Mover User requests access to a file or directory, the TOE utilizes its Discretionary Access Control SFP to decide whether or not that access is permitted. The TOE uses the UserID and GroupIDs of the user and the contents of the ACL to determine if the operation should be allowed to proceed.

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.

[9] SFP – Security Function Policy

Table 5 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure	Description
ACM_CAP.2	EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series - Configuration Management: Capabilities	The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at EMC
ADO_DEL.1	EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series - Delivery and Operation: Secure Delivery	The Delivery and Operation document provides a description of the secure delivery procedures implemented by EMC to protect against TOE modification during product delivery.
ADO_IGS.1	Celerra Network Server Celerra NS350/NS500/NS600/NS700/NS704 Integrated Configuration Version 5.5 PHASE 1 AND 2 SETUP GUIDE P/N 300-002-070 REV A04	These are the Guidance documents for Installation and configuration of the EMC Celerra Network Server.
ADV_FSP.1	EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence	This document describes the system security functions and externally visible interfaces.
ADV_HLD.1	EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence	This document describes the system interfaces and subsystems.
ADV_RCR.1	EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series- TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence	This document establishes the correspondence between the ST, the FSP, and the HLD design data.
AGD_ADM.1	Celerra Network Server Celerra NS350/NS500/NS600/NS700/NS704 Integrated Configuration Version 5.5 PHASE 1 AND 2 SETUP GUIDE P/N 300-002-070 REV A04	These are Guidance documents designed to assist the management user with the EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series.
AGD_USR.1	Celerra Network Server Version 5.5 COMMAND REFERENCE MANUAL P/N 300-002-697 REV A02 Celerra CDMS Version 2.0 for NFS and CIFS Version 5.5 USER'S GUIDE P/N 300-002-712 REV A01	The Users Guides instruct the user on how to properly use the EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series.
ALC_FLR.1	EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series – Life Cycle Support: Flaw Remediation	This document describes the flaw remediation process for the EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series.
ATE_COV.1	EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series – Testing: Coverage	This document describes the completeness of test coverage preformed against the TOE.
ATE_FUN.1	EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series – Tests: Functional Tests	This document describes the functional testing for the TOE to establish that the TSF exhibits the properties necessary to satisfy the functional requirements

Assurance Component	Assurance Measure	Description
ATE_IND.2	Provided by laboratory evaluation	None
AVA_SOF.1	EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series - Vulnerability Assessment	This document provides The Strength of TOE Security Function Analysis.
AVA_VLA.1	EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series - Vulnerability Assessment	This document provides evidence of how the TOE is resistant to attacks.

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 ST. The following tables demonstrate the mapping between the assumptions, threats, and polices to the security objectives is complete. The Rationale column provides detailed evidence of coverage for each assumption, threat, and policy.

8.1.1 Security Objectives Rationale Relating to Threats

Threats	Objectives	Rationale
T.BYPASS The TOE could be bypassed by a server with direct access to the SAN.	OE.BYPASS The TOE environment must ensure that the TSF cannot be bypassed	OE.BYPASS ensures that other IT systems will not access User Data being protected by the TOE using direct access to the SAN. All access to User Data will be through the TOE and its protection mechanisms.
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 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 TSF cannot be bypassed.	The objective O.BYPASS ensures that the protection mechanisms of the TOE designed to mitigate this threat cannot be bypassed.
	O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a User access to the TSF's when local authentication is required.	O.I&A supports the mitigation of 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.	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.

Threats	Objectives	Rationale
	O.BYPASS The TOE must ensure that the TSF cannot be bypassed.	The objective O.BYPASS ensures that the protection mechanisms of the TOE designed to mitigate this threat cannot be bypassed.
	O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a User access to the TSF's when local authentication is required.	O.I&A and OE.I&A (depending on TOE configuration) work together to ensure that the TOE or the TOE environment has properly identified and authenticated a user prior to providing access to user data.
	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.
	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 ensure that the TOE or the TOE environment has properly identified and authenticated a user prior to providing access to user data.
	OE.SECURE_COMMUNICATIONS The TOE environment must provide secure communications between systems connected to the Storage Area Network	OE.SECURE_COMMUNICATIONS ensures that identification and authentication performed by the TOE Environment is done over a secure communications channel.
	OE.SECURE_SERVERS The TOE environment must provide properly configured authentication servers to communicate with the TOE.	OE.SECURE_SERVERS supports the mitigation of 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.
T.UNAUTH An unauthorized user could access data stored by the TOE.	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.

Threats	Objectives	Rationale
	O.BYPASS The TOE must ensure that the TSF cannot be bypassed.	The objective O.BYPASS ensures that the protection mechanisms of the TOE designed to mitigate this threat cannot be bypassed.
	O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a User access to the TSF's when local authentication is required.	O.I&A and OE.I&A (depending on TOE configuration) work together to ensure that the TOE or the TOE environment has properly identified and authenticated a user prior to providing access to user data.
	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.
	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 ensure that the TOE or the TOE environment has properly identified and authenticated a user prior to providing access to user data.
	OE.SECURE_COMMUNICATIONS The TOE environment must provide secure communications between systems connected to the Storage Area Network	OE.SECURE_COMMUNICATIONS ensures that identification and authentication performed by the TOE Environment is done over a secure communications channel.
	OE.SECURE_SERVERS The TOE environment must provide properly configured authentication servers to communicate with the TOE.	OE.SECURE_SERVERS supports the mitigation of 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.

8.1.2 Security Objectives Rationale Relating to Assumptions

Assumptions	Objectives	Rationale

Assumptions	Objectives	Rationale
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	OE.PROTECT The TOE environment must protect the data it has been entrusted to protect	Sites using the TOE will connect the TOE to a SAN that provides data storage. This data storage should be configured and managed securely to allow the TOE to properly mediate access to User Data.
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

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method for administrative control of the TOE.	FIA_UID.2(a) User identification before any action	The TOE will properly identify and authenticate all administrators.
	FIA_UAU.2(a) User authentication before any action	The TOE shall successfully authenticate each administrator before allowing them to manage the TOE

Objective	Requirements Addressing the Objective	Rationale
	FMT_SMR.1 Security roles	Specific roles are defined to govern management of 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_MTD.1 Management of TSF data	The ability to modify TSF data is granted only to certain roles managed by the TOE
	FMT_MSA.3 Static attribute initialisation	Restrictive values for data access are provided, and the Object Owner can change them when a data object is created.
	FMT_MSA.1 Management of security attributes	Security attributes of the TOE can only be changed by authorized administrators.
O.BYPASS The TOE must ensure that the TSF cannot be bypassed.	FPT_SEP.1 TSF domain separation	The TOE maintains a security domain for its execution that protects it from interference and tampering.
	FPT_RVM.1(a) Non-bypassability of the TSP	The TOE ensures that policy enforcement functions are invoked and succeed before each function is allowed to proceed
O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a User access to the TSF's when local authentication is required.	FIA_UID.2(a) User identification before any action	The TOE identifies each Administrator and, when configured for local user administration, each User prior to granting access to the TSF.
	FIA_ATD.1(a) User attribute definition	The TOE, when configured for local user administration, maintains security attributes for each user.
	FIA_UAU.2(a) User authentication before any action	The TOE authenticates each Administrator and, when configured for local user administration, each User prior to granting access to the TSF.

Objective	Requirements Addressing the Objective	Rationale
O.PROTECT The TOE must protect data that it has been entrusted to protect.	FDP_ACF.1 Security attribute based access control	The TOE provides access control functionality to manage access to data protected by the TOE.
	FDP_ACC.1 Subset access control	The TOE has an access control policy which ensures that only authorized users gain access to data protected by the TOE.

8.2.2 Rationale for Security Functional Requirements of the IT Environment

Objective	Requirements Addressing the Objective	Rationale
OE.I&A The TOE environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE	FIA_ATD.1(b) User attribute definition	The TOE Environment, when configured for remote user administration, maintains security attributes for each user.
	FIA_UAU.2(b) User authentication before any action	The TOE Environment, when configured for remote user administration, authenticates each user.
	FIA_UID.2(b) User identification before any action	The TOE Environment, when configured for remote user administration, uniquely identifies each user.
OE.SECURE_COMMUNICATIONS The TOE environment must provide secure communications between systems connected to the Storage Area Network	FIA_ATD.1(b) User attribute definition	The TOE Environment, when configured for remote user administration, maintains security attributes for each user.
	FIA_UAU.2(b) User authentication before any action	The TOE Environment, when configured for remote user administration, authenticates each user.
	FIA_UID.2(b) User identification before any action	The TOE Environment, when configured for remote user administration, uniquely identifies each user.

Objective	Requirements Addressing the Objective	Rationale
	FTP_ITC.1 Inter-TSF trusted channel	The TOE Environment provides a communication channel between systems connected to the Storage Area Network that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
OE.SECURE_SERVERS The TOE environment must provide properly configured authentication servers to communicate with the TOE.	FIA_ATD.1(b) User attribute definition	The TOE Environment, when configured for remote user administration, maintains security attributes for each user.
	FIA_UAU.2(b) User authentication before any action	The TOE Environment, when configured for remote user administration, authenticates each user.
	FIA_UID.2(b) User identification before any action	The TOE Environment, when configured for remote user administration, uniquely identifies each user.
OE.BYPASS The TOE environment must ensure that the TSF cannot be bypassed	FPT_RVM.1(b) Non-bypassability of the TSP	The TOE Environment ensures that policy enforcement functions are invoked and succeed before access to data is granted to a user.

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.

8.4 Rationale for Refinements of Security Functional Requirements

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

The term “TSF” has been refined to “TOE Environment” for FIA_ATD.1(b), FPT_RVM.1(b), and FTP_TRP.1.

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

The words “between itself and a remote trusted IT product” has been refined to “systems connected to the Storage Area Network” for FTP_TRP.1.

8.5 Dependency Rationale

This ST does satisfy all the requirement dependencies of the CC. Table 6 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 6 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FIA_ATD.1(a)	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	✓	
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	FMT_SMF.1	✓	
	FMT_SMR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
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(a)	No Dependencies	✓	
FPT_RVM.1(b)	No Dependencies	✓	
FPT_SEP.1	No Dependencies	✓	
FTP_TRP.1	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. 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 4 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 Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series - 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 Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series - Delivery and Operation: 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 Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series - TOE Architecture: 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 descriptions of 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 single versions of documents which address the Administrator Guidance and User Guidance; there are no separate guidance documents for a non-administrative user of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance

8.6.2.5 Life Cycle Support

The *EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series – 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 Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series* Functional Tests and Coverage documentation, *EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series Testing: Coverage* and *EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series Testing: Functional Tests*. The Coverage Analysis document 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. Also provided are EMC Test Plans and Functional Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing

8.6.2.7 Vulnerability and TOE Strength of Function Analyses

The *EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC Celerra NSX series and EMC Celerra NS series - 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

A 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 ST. 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 ST 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:

- Identification and Authentication: FIA_UAU.2(a) - User Authentication before any action

The only mechanisms within the TOE that are probabilistic and permutational in nature are the passwords used to authenticate users to the TOE.

9 Acronyms

Table 7 - Acronyms

Acronym	Definition
ACE	Access Control Entry
AGD	Assurance Guidance Document
ACL	Access Control List
CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
CIFS	Common Internet File System
CLI	Command Line Interface
DART	Data Access in Real Time
DoD	Department of Defense
EAL	Evaluation Assurance Level
IP	Internet Protocol
iSCSI	internet Small Computer System Interface
ISO	International Organization for Standardization
IT	Information Technology
LUN	Logical Unit Number
NAS	Network Attached Storage
NFS	Network File System
PP	Protection Profile
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy