EMC Avamar® v7.2.1 Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 1908-000-D102
Version: 0.5
15 June 2016

Prepared For:

EMC Corporation
176 South Street
Hopkinton, MA, USA
01748

Prepared by:

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

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

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

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

1.1 DOCUMENT ORGANIZATION

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

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

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

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

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

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

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

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

1.2 SECURITY TARGET REFERENCE

ST Title:	EMC Avamar® v7.2.1 Security Target
ST Version:	0.5
ST Date:	15 June 2016

1.3 TOE REFERENCE

TOE Identification: EMC Avamar® v7.2.1 (Build 32)

TOE Developer: EMC Corporation

TOE Type: Other Devices and Systems

1.4 TOE OVERVIEW

EMC Avamar performs backups and restores for remote offices, data center local area networks (LAN), and VMware environments. Using patented data deduplication technology, redundancies are identified at the source, saving network and data storage resources. Backups are based on changes to data and occur at administrator-scheduled intervals, making each backup a full backup, while significantly reducing backup time.

Avamar consists of multiple components. The server component provides centralized storage for the backups, while agent components execute on platforms being backed up. There are also special categories of agents for VMware environments and NDMP-based storage solutions.

The Avamar Server may be deployed on a single-node server that includes management and storage in one node, or in a multi-node server that uses one node as the utility management node and up to 16 nodes for storage. Client communications are dynamically load-balanced across all of the storage nodes within the server, but all management is done through only the utility node. Avamar Servers are delivered as physical appliances.

Management of the Server is performed via a Java-based GUI application executing on Windows or Linux workstations, or via a CLI remotely accessed on the Server. The management interfaces support multiple roles so that different access rights can be assigned to different user accounts. Users can also be assigned to domains to further limit their access. The GUI application is delivered as software.

The Avamar Agents on end user systems (Clients) run on many operating systems. Each Client is associated with a domain within Avamar to link related systems and help in defining user access to their backup data. The Agents execute backups at pre-configured intervals, or on demand. The Agents determine the data that needs to be backed up and send it to the Server. The Avamar Agents are delivered as software.

Authorized users on Clients can interact with the Agents to initiate backups and restores of the Client they are on. Backups may be performed via the Client application or the Client Web UI, while restores may be performed via the Client Web UI or the Web Restore interface. When restoring data, only data from Clients within the same domain can be accessed.

In addition to the OS-based Agents, two special-purpose Agents are supported. These Agents act as the Client for the system they work with.

The Avamar NDMP Accelerator acts as a front-end to NDMP-based storage systems (such as EMC VNX) to enable backups and restores of the data sets on a storage system with an Avamar Server. Avamar NDMP Accelerators are delivered as physical appliances.

The Avamar VMware Universal Proxy acts as a proxy backup server and is installed as a virtual machine on VMware vSphere ESXi platforms. One Universal Proxy instance can provide backup and restore functionality to multiple other virtual machines on the same or different ESXi platforms. The Universal Proxy uses the VMware vStorage API for Data Protection (VADP). The Avamar VMware Universal Proxy is delivered as software.

Avamar may be integrated with EMC Data Domain appliances. In this mode, metadata for backup files is stored on the Avamar Server, but the actual data is stored on a Data Domain appliance. The usage of Data Domain is recommended for data that changes frequently, and is transparent to users and administrators in backup and restore operations.

User credential validation is performed internally by Avamar.

Audit records are generated for actions taken by users on Servers and Agents. The audit information may be viewed by authorized users.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE includes:

- One or more Server appliances (either single node or multi-node) with Gen4S hardware
- One or more Agent software instances executing on end user systems
- One or more VMware Universal Proxy software instances executing on vSphere ESXi platforms
- One or more NDMP Accelerator appliances front-ending NDMP-based storage systems
- One or more instances of the GUI (MCGUI) management application executing on Windows or Linux platforms

For the appliances, both the hardware and software are included in the TOE. For the software instances, only the Avamar-specific software is included in the TOE. For the Universal Proxy, the entire virtual machine is included in the TOE. The following diagram illustrates the TOE boundary.

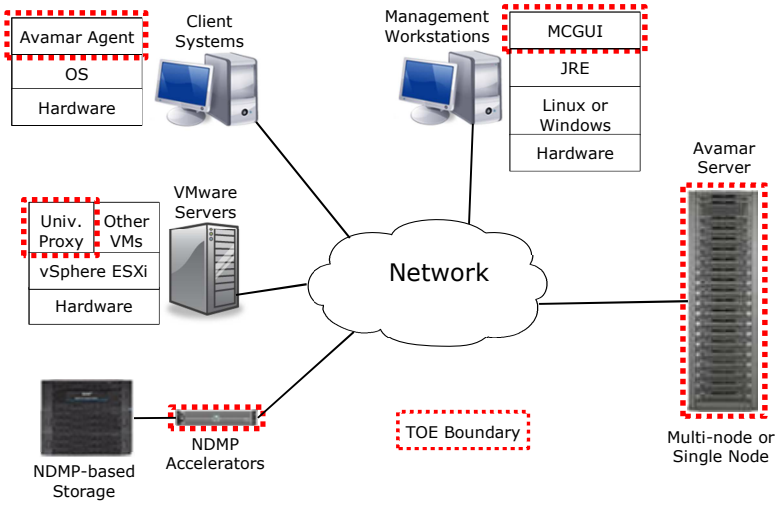

Figure 1 – EMC Avamar® v7.2.1 Diagram

1.5.2 TOE Environment

The MCGUI application is installed on management workstations. The required components from the TOE Environment are specified in the following table. Other options are supported but not evaluated; these options are described in section 1.5.5.

Item	Minimum Requirement
Operating System	Red Hat Enterprise Linux Release 5 (64-bit) or Microsoft Windows 7
RAM	256 MB
Hard Drive Space	60 MB
Network Interface	10BaseT or higher
Java Runtime Environment	JRE 1.6 Update 12 or later

Table 1 – MCGUI Management Workstation Minimum Requirements

Agents are installed on client systems that need backup and restore services. The required components from the TOE Environment are specified in the following table. Other options are supported but not evaluated; these options are described in section 1.5.5.

Item	Minimum Requirement
CPU	1 GHz

Item	Minimum Requirement
RAM	1 GB
Hard Drive Space	250 MB
Network Interface	1 10BaseT or higher, OR 1 IEEE 802.11a/b/g
Operating System	Windows Server 2012 (64-bit), OR Windows Server 2008 (32-bit), OR SLES 11 (32-bit or 64-bit)

Table 2 – Avamar Client Minimum Requirements

The Avamar Universal Proxy virtual machine is installed on VMware vSphere ESXi 6.0 servers (in the TOE Environment). Other options are supported but not evaluated; these options are described in section 1.5.5. The required components from the TOE Environment are specified in the following table.

Item	Minimum Requirement
CPUs	4 virtual CPUs
RAM	4 GB
Hard Drive Space	21 GB (can be thin provisioned)
Network Interface	1
IP Address	Static, with reverse lookup of hostname/IP

Table 3 – Universal Proxy Minimum Requirements

User data is passed over the network. It is the responsibility of the TOE Environment to protect this traffic from unauthorized disclosure or modification.

Administrator traffic is passed between the management workstations and Server. It is the responsibility of the TOE Environment to protect this traffic from unauthorized disclosure or modification.

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- *EMC Avamar Administration Guide (August, 2014)*
- *EMC Avamar Management Console Command Line Interface MCCLI Programmer Guide (June, 2014)*
- *EMC Avamar Product Security Guide (August, 2014)*

- *EMC Avamar Compatibility and Interoperability Matrix (February 2015)*
- *EMC Avamar Operational Best Practices (August, 2014)*
- *EMC Avamar Backup Clients User Guide (June, 2014)*
- *EMC Avamar for Windows Server User Guide (December, 2014)*
- *EMC Avamar NDMP Accelerator for EMC NAS Systems User Guide (August, 2014)*
- *EMC Avamar Data Store Gen4S Single Node Customer Installation Guide (July, 2013)*
- *EMC Avamar Data Store Gen4S Comprehensive Reference Guide (April, 2015)*
- *EMC Avamar Common Criteria Supplement (16 January 2016)*

1.5.4 Logical Scope

Functional Classes	Description
Security Audit	Audit entries are generated for security related events, and can be reviewed by authorized users. System time is maintained and included in all audit records.
User Data Protection	The TOE uses the Server Access Control SFP to control access through the management interfaces on the server. Users may only access data within their assigned domain. The user's role defines the type of operations the user can perform on the data within their domain. The Client Access Control SFP controls how users access the TOE through a client system. Only the data from the client system and its related audit data can be viewed from the client system. The user must be assigned to the client within the TOE and can then perform the actions that the user's role allows.
Identification and Authentication	Users of the management interfaces must identify and authenticate prior to TOE access.
Security Management	The TOE provides management capabilities via GUI and CLI interfaces. Multiple roles are supported to provide varying levels of access to data and functions. Users are assigned to domains, and their data access is limited to their assigned domain.

Table 4 - Logical Scope of the TOE

1.5.5 Functionality Excluded from the Evaluated Configuration

The following product features are excluded from this evaluation:

- REST API
- EMC Secure Remote Support (ESRS)
- Enterprise authentication
- Local user access from clients (pass-through authentication)

Avamar Servers with Gen4 and Gen3 hardware are supported in addition to those with Gen4S hardware.

The MCGUI application is supported on Microsoft Windows 8.x, as well as Microsoft Windows Server 2003, 2008 and 2012, in addition to Windows 7.

Agents are supported on the following operating systems (in addition to those specified in section 1.5.2): AIX, CentOS, Debian, Free BSD, HP-UX, Mac OS X, Novell Netware, Novell Open Enterprise Server, Oracle Linux, RHEL, Red Hat Linux, SCO UNIX, Solaris, SLES, Symantec Enterprise Vault, Ubuntu, Windows, and Windows Storage Server.

In addition to vSphere ESXi 6.0, the Universal Proxy is supported on ESXi 5.x.

In addition to internal validation of user credentials by Avamar, external validation via integration with LDAP servers is also supported.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

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

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

As follows:

- CC Part 2 conformant
- CC Part 3 conformant

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

2.2 ASSURANCE PACKAGE CLAIM

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

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

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

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 5 lists the threats addressed by the TOE. Mitigation to the threats is through the objectives identified in Section 4.1 Security Objectives.

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

Table 5 - Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed upon an organization in the operational environment. Table 6 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.BACKUP	The TOE shall backup specified client data and make it available for restore operations.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Table 6 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 7.

Assumptions	Description
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NETWORK	The TOE components, front-end hosts, back-end storage and management workstations will be interconnected by a segregated network that protects the traffic from disclosure to or modification by untrusted systems or users.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTCT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.

Table 7 – Assumptions

4 SECURITY OBJECTIVES

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

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

4.1 SECURITY OBJECTIVES FOR THE TOE

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

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

Table 8 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

Security Objective	Description
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
OE.NETWORK	The operational environment will provide a segregated network that protects the traffic between the TOE components and front-end hosts, back-end storage and management workstations from disclosure to or modification by untrusted systems or users.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.TIME	The operational environment will maintain reliable timestamps for use by TOE components.

Table 9 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

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

	T.IMPCON	T.PRIVIL	T.UNAUTH_ACCESS	P.ACCACT	P.BACKUP	P.MANAGE	P.PROTECT	A.MANAGE	A.NETWORK	A.NOEVIL	A.PROTECT
O.ACCESS	X	X	X			X					
O.AUDITS			X	X							

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

Table 10 - Mapping Between Objectives, Threats, Organizational Security Policies, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

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

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

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

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

Threat: T.UNAUTH_ACCESS	A user may attempt to access user data (backup files) that is not authorized.

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

4.3.2 Security Objectives Rationale Related to OSPs

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

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

Policy: P.BACKUP	The TOE shall backup specified client data and make it available for restore operations.

Objectives:	O.BACKUP	The TOE shall backup specified client data and make it available for restore operations.
Rationale:	The O.BACKUP objective requires the TOE to backup specified client data and make it available for restore operations.	

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

	O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.

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

4.3.3 Security Objectives Rationale Related to Assumptions

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

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

Assumption: A.NETWORK	The TOE components, front-end hosts, back-end storage and management workstations will be interconnected by a segregated network that protects the traffic from disclosure to or modification by untrusted systems or users.	
Objectives:	OE.NETWORK	The operational environment will provide a segregated network that protects the traffic between the TOE components and front-end hosts,

		back-end storage and management workstations from disclosure to or modification by untrusted systems or users.
Rationale:	The OE.NETWORK objective ensures that the management traffic will be protected by a segregated LAN.	

Assumption: A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	
Objectives:	OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.	

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

5 EXTENDED COMPONENTS DEFINITION

5.1 EXTENDED FUNCTIONAL COMPONENTS

5.1.1 FDP_BCK_EXT User Data Backup/Restore

Family Behaviour:

This family defines the requirements for the TOE to provide backup and restore services for IT systems in the operational environment.

Component Levelling:

FDP_BCK_EXT User Data Backup/Restore	1

FDP_BCK_EXT.1 User Data Backup/Restore provides for the functionality to perform backup and restore operations as directed by administrators and users.

Management:

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

a) Configuration of the backup and restore operations to be performed.

Audit:

There are no auditable events foreseen.

FDP_BCK_EXT.1 User Data Backup/Restore

Hierarchical to: No other components.

Dependencies: None

FDP_BCK_EXT.1.1 **The TSF shall provide a capability to backup systems as configured by authorized administrators.**

FDP_BCK_EXT.1.2 **The TSF shall provide a capability for authorized administrators to restore files to systems from previously-created backups.**

FDP_BCK_EXT.1.3 **The TSF shall provide a capability for authorized users on a system to restore files from previously-created backups of that same system, subject to file access control permissions configured on that system for the user.**

5.2 EXTENDED ASSURANCE COMPONENTS

This ST does not include extended security assurance requirements.

6 SECURITY REQUIREMENTS

6.1 CONVENTIONS

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

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

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC, summarized in Table 11 - Summary of Security Functional Requirements.

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

Class	SFR	Name
	FIA_UID.1	Timing of identification
	FIA_USB.1	User-subject binding
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps

Table 11 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) *all logins and logouts on the system;*

d) all user actions performed].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

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

6.2.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*Root Administrators and Domain Administrators*] with the capability to read [*all audit data*] from the audit records.

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

6.2.1.4 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

6.2.2 User Data Protection

6.2.2.1 FDP_ACC.1(1) Subset access control (Server)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(1) The TSF shall enforce the [*Server Access Control SFP*] on [

Subjects: Users of MCGUI and MCCLI,

Objects: Clients, Backup Files, and

Operations: Backup, Restore].

6.2.2.2 FDP_ACC.1(2) Subset access control (Client)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(2) The TSF shall enforce the [*Client Access Control SFP*] on [

Subjects: Users on clients,

Objects: Clients, Backup Files, and

Operations: Backup, Restore].

6.2.2.3 FDP_ACF.1(1) Security attribute based access control (Server)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(1) The TSF shall enforce the [*Server Access Control SFP*] to objects based on the following: [

Users: Role, associated Domain;

Clients: associated Domain;

Backup Files: associated Domain].

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

1. *Users with the Root Administrator, Domain Administrator, Backup Only Operator, and Backup/Restore Operator roles may perform a backup operation from a Client in the same Domain (or one that is subordinate) to the user's associated Domain.*
2. *Users with the Root Administrator, Domain Administrator, Restore Only Operator, and Backup/Restore Operator roles may perform a restore operation:*
   a. *from a Backup File in the same Domain (or one that is subordinate) to the user's associated Domain*
   b. *to a Client in the same Domain (or one that is subordinate) to the user's associated Domain.]*

FDP_ACF.1.3(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*all Domains are considered subordinate to the root level and are therefore accessible to user accounts defined at the root level*].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*access is denied if the conditions in FDP_ACF.1.2(1) are not satisfied*].

6.2.2.4 FDP_ACF.1(2) Security attribute based access control (Client)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(2) The TSF shall enforce the [*Client Access Control SFP*] to objects based on the following: [

Users: Role, associated Domain;

Clients: associated Domain;

Backup Files: associated Domain].

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

1. *Users with the Back Up Only User and Back Up/Restore User roles may perform a backup operation from the Client on which the user is executing if the Client's Domain is in the user's Domain.*
2. *Users with the Restore Only User, Back Up/Restore User and Restore Ignore User roles may perform a restore operation (from a Backup File in the same (or subordinate) Domain as the Client on which the user is executing) to the Client on which the user is executing.]*

FDP_ACF.1.3(2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*access is denied if the conditions in FDP_ACF.1.2(2) are not satisfied*].

6.2.2.5 FDP_BCK_EXT.1 User Data Backup/Restore

Hierarchical to: No other components.

Dependencies: None

FDP_BCK_EXT.1.1 The TSF shall provide a capability to backup systems as configured by authorized administrators.

FDP_BCK_EXT.1.2 The TSF shall provide a capability for authorized administrators to restore files to systems from previously-created backups.

FDP_BCK_EXT.1.3 The TSF shall provide a capability for authorized users on a system to restore files from previously-created backups of that same system, subject to file access control permissions configured on that system for the user.

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.3.2 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*no actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before

6.2.3.3 FIA_UAU. 7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*dots for the GUI, no output for the CLI*] to the user while the authentication is in progress.

6.2.3.4 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [*no actions*] on behalf of the user to be performed before the user is identified.

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

6.2.3.5 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

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

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

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

6.2.4 Security Management

6.2.4.1 FMT_MSA.1(1) Management of security attributes (Server)

Hierarchical to: No other components.

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

FMT_MSA.1.1(1) The TSF shall enforce the [*Server Access Control SFP*] to restrict the ability to [query, modify] the security attributes [*Users: Role and Domain; Clients: Domain*] to [*users with the Root Administrator or Domain Administrator roles*].

6.2.4.2 FMT_MSA.1(2) Management of security attributes (Client)

Hierarchical to: No other components.

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

FMT_MSA.1.1(2) The TSF shall enforce the [*Client Access Control SFP*] to restrict the ability to [query, modify] the security attributes [*Users: Role and Domain; Clients: Domain*] to [*users with the Root Administrator or Domain Administrator roles*].

6.2.4.3 FMT_MSA.3(1) Static attribute initialisation (Server)

Hierarchical to: No other components.

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

FMT_MSA.3.1(1) The TSF shall enforce the [*Server Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [*users with the Root Administrator or Domain Administrator roles*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.4 FMT_MSA.3(2) Static attribute initialisation (Client)

Hierarchical to: No other components.

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

FMT_MSA.3.1(2) The TSF shall enforce the [*Client Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [*users with the Root Administrator or Domain Administrator roles*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.5 FMT_MTD.1 Management of TSF data

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

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

Role / TSF Data	Administrators		Operators			
	Root	**Domain**	**Restore Only**	**Back Up Only**	**Back Up Restore**	**Activity**
Activities	Query	Query	Query	Query	Query	Query
Client Groups	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query	Query	Query	Query
Clients	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query	Query	Query	Query
Domains	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query	Query	Query	Query
Operations Processing	Query, Modify	None	None	None	None	None
Scheduled Operations	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query, Modify, Delete, Create for restores	Query, Modify, Delete, Create for backups	Query, Modify, Delete, Create	None

Role / TSF Data	Administrators		Operators			
	Root	Domain	Restore Only	Back Up Only	Back Up Restore	Activity
User Accounts	Query, Modify, Delete, Create	Query, Modify, Delete, Create	None	None	None	None

Table 12 – TSF Data Access Permissions

Application Note: For user accounts associated with a Domain, access is limited to objects within that Domain (or subordinate Domains). All Domains are considered to be subordinate to the root level and are therefore accessible to user accounts associated with the root level.

Application Note: Domain Administrators may not add or modify user accounts with the Domain Administrator role.

6.2.4.6 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- *User management*
- *Client and Client Group management*
- *Domain management*
- *Operations Processing management*
- *Scheduled Operations management*].

6.2.4.7 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Root Administrator, Domain Administrator, Restore Only Operator, Back Up Only Operator, Back Up/Restore Operator, Activity Operator, Back Up Only User, Restore Only User, Back Up/Restore User, Restore Only/Ignore File Permissions User*].

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

6.2.5 Protection of the TSF

6.2.5.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application Note: This SFR applies to the Avamar Server and NDMP Accelerator.

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

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

	O.ACCESS	O.AUDITS	O.BACKUP	O.EADMIN	O.IDAUTH	O.PROTCT	O.TIME
FAU_GEN.1		X					
FAU_GEN.2		X					
FAU_SAR.1		X					
FAU_SAR.2		X					
FDP_ACC.1(1)			X			X	
FDP_ACC.1(2)			X			X	
FDP_ACF.1(1)			X			X	
FDP_ACF.1(2)			X			X	
FDP_BCK_EXT.1			X				
FIA_ATD.1					X		
FIA_UAU.1	X				X		
FIA_UAU.7	X				X		
FIA_UID.1	X				X		
FIA_USB.1	X						
FMT_MSA.1(1)	X		X	X			
FMT_MSA.1(2)	X		X	X			
FMT_MSA.3(1)			X			X	
FMT_MSA.3(2)			X			X	
FMT_MTD.1	X			X			
FMT_SMF.1				X			

	O.ACCESS	O.AUDITS	O.BACKUP	O.EADMIN	O.IDAUTH	O.PROTCT	O.TIME
FMT_SMR.1	X			X			
FPT_STM.1		X					X

Table 13 – Mapping of SFRs to Security Objectives

6.3.1 SFR Rationale Related to Security Objectives

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

Security Objective	Rationale
O.ACCESS	FIA_UID.1 and FIA_UAU.1 require users to complete the I&A process, which ensures only authorized users gain access and enables each user session to be bound to a role to limit. FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE. FIA_USB.1 defines the user attributes that are bound to each user session upon session upon completion of the I&A process, enabling access restrictions to be properly enforced for each user session. FMT_MSA.1(*) and FMT_MTD.1 define the access permissions to TSF data for each role. FMT_SMR.1 ensures the TOE supports multiple roles so that appropriate data access can be provided to different users.
O.AUDITS	FAU_GEN.1 and FAU_GEN.2 require audit records to be generated for specific events and define the contents of the records. FAU_SAR.1 and FAU_SAR.2 require the audit records to be available to all authorized users of the TOE, and for access to be restricted for unauthorized users. FPT_STM.1 requires accurate time stamps to be available for the audit records.
O.BACKUP	FDP_ACC.1(*) and FDP_ACF.1(*) assure that backup data is created as directed and is available for restores subject to access rights. FDP_BCK_EXT.1 ensures that the TOE supports backup and restore operations by administrators and users. FMT_MSA.1(*) ensure that appropriate security attributes are maintained for the subjects and objects.

Security Objective	Rationale
	FMT_MSA.3(*) require that restrictive attributes based on Domain membership are applied.
O.EADMIN	FMT_MSA.1(*) and FMT_MTD.1 define the access permissions required for each role for TSF data. FMT_SMF.1 specifies the management functionality required for effective management of the TOE. FMT_SMR.1 defines the roles required to provide effective management capabilities for different categories of users.
O.IDAUTH	FIA_UID.1 and FIA_UAU.1 require users to complete the I&A process, which ensures only authorized users gain access and defines their access permissions prior to completing the I&A process. FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE. FIA_ATD.1 specifies the security attributes that are supported for each defined user account.
O.PROTCT	FDP_ACC.1(*) and FDP_ACF.1(*) define the access control policy for users of the Server and Agent management interfaces. FMT_MSA.3(*) requires restrictive access to backup data by default so that no access is granted until explicitly configured by authorized users.
O.TIME	FPT_STM.1 requires accurate time stamps to be available.

Table 14 – Security Objectives for the TOE

6.4 DEPENDENCY RATIONALE

Table 15 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependencies	Dependency Satisfied / Rationale
FAU_GEN.1	FPT_STM.1	Satisfied
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Satisfied Satisfied
FAU_SAR.1	FAU_GEN.1	Satisfied
FAU_SAR.2	FAU_SAR.1	Satisfied
FDP_ACC.1(1)	FDP_ACF.1	Satisfied by FDP_ACF.1(1)

SFR	Dependencies	Dependency Satisfied / Rationale
FDP_ACC.1(2)	FDP_ACF.1	Satisfied by FDP_ACF.1(2)
FDP_ACF.1(1)	FDP_ACC.1 FMT_MSA.3	Satisfied by FDP_ACC.1(1) Satisfied by FMT_MSA.3(1)
FDP_ACF.1(2)	FDP_ACC.1 FMT_MSA.3	Satisfied by FDP_ACC.1(2) Satisfied by FMT_MSA.3(2)
FDP_BCK_EXT.1	None	n/a
FIA_ATD.1	None	n/a
FIA_UAU.1	FIA_UID.1	Satisfied
FIA_UAU.7	FIA_UAU.1	Satisfied
FIA_UID.1	None	n/a
FIA_USB.1	FIA_ATD.1	Satisfied
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1 FMT_SMF.1	Satisfied by FDP_ACC.1(1) Satisfied Satisfied
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1 FMT_SMF.1	Satisfied by FDP_ACC.1(2) Satisfied Satisfied
FMT_MSA.3(1)	FMT_MSA.1 FMT_SMR.1	Satisfied by FMT_MSA.1(1) Satisfied
FMT_MSA.3(2)	FMT_MSA.1 FMT_SMR.1	Satisfied by FMT_MSA.1(2) Satisfied
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Satisfied Satisfied
FMT_SMF.1	None	n/a
FMT_SMR.1	FIA_UID.1	Satisfied
FPT_STM.1	None	n/a

Table 15 - Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2+ level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). EAL 2+ was chosen for competitive reasons. The developer is claiming the ALC_FLR.2

augmentation since there are a number of areas where current practices and procedures exceed the minimum requirements for EAL 2+.

The assurance requirements are summarized in Table 16.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw Reporting Procedures
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample

Assurance Class	Assurance Components	
	Identifier	**Name**
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 16 - EAL 2+ Assurance Requirements

7 TOE SUMMARY SPECIFICATION

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

7.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

7.1.1 Security Audit

Audit records are generated for the events specified with FAU_GEN.1. System time is maintained and included in all audit records. The audit trail is maintained on the Avamar Server.

Startup of the audit function is equivalent to a power on event. It is not possible to shut down the audit function. The following information is included in all audit records:

- Data and time of the event,
- Type of event,
- Subject identity (if applicable).

Users with the Root Administrator or Domain Administrator role may view the audit records via the MCGUI application.

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

7.1.2 User Data Protection

Administrators configure backup policies for applicable IT systems. And the TOE is responsible for performing those configured backups. Administrators may configure restore operations to be performed from backup files' users may perform restore operations to the system on which they are logged in.

Access control for the TOE differs depending on how a user accesses the TOE. The users of the TOE fall into one of three categories: Administrators, Operators, and Users. Operators and Administrators access the TOE via MCGUI or MCCLI and their access permissions are defined by the Server Access Control SFP. Users access the TOE only via a client system (using GUI and/or CLI interfaces on the clients) and their access permissions are defined by the Client Access Control SFP.

The Server Access Control SFP defines access to backup files through MCGUI and MCCLI. The server-side user attributes Assigned Domain and Role determine the accesses allowed.

Root Administrators have full access to all backup files. Users with any other role are organized and segregated within the server through the use of domains. The domains are hierarchical so users added to a higher level domain has access to the lower levels. Users can only perform functions on the backup

files within their assigned domains, involving clients in the domain, and according to the functions allowed for their role.

The Client Access Control SFP defines access to backup files through local interfaces on a client. Users can only perform functions on the backup files within their assigned domains, involving the client they are executing on and which also belongs to their Domain, and according to the functions allowed for their role.

TOE Security Functional Requirements addressed: FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACF.1(1), FDP_ACF.1(2), FDP_BCK_EXT.1.

7.1.3 Identification and Authentication

When GUI or CLI users initiate sessions with the TOE, they must complete the login process. Prior to successful completion, the only controlled data or function they can access is viewing the configured banner. CLI and GUI users always must present a valid username and password.

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

Upon successful login, the user's username, domain and role are bound to the session.

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

7.1.4 Security Management

Management of the TOE is performed by users with the Operators and/or Administrators roles via MCGUI or MCCLI. Each user session is bound to a role and domain upon login, and those attributes determine access permissions as specified in FMT_MTD.1.

Backup and restore operations may be scheduled by users with the Administrators and/or Operators roles. These operations may be performed once or according to a defined schedule. Scheduled operations are performed autonomously by the TOE.

Security attributes for users and clients can only be changed by Root Administrators and Domain Administrators. Domain Administrators are limited to user account management for users with Operator or User roles.

Default attribute settings are restrictive. When backup files are created, they have the same Domain as the client providing the data. Root Administrators and Domain Administrators may change the initial attributes for users and clients.

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

8 TERMINOLOGY AND ACRONYMS

8.1 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
API	Application Program Interface
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
ESRS	EMC Secure Remote Support
GUI	Graphical User Interface
IT	Information Technology
I&A	Identification & Authentication
JRE	Java Runtime Environment
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MB	MegaBytes
MCCLI	Management Console CLI
MCGUI	Management Console GUI
NDMP	Network Data Management Protocol
OE	Operational Environment
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
REST	REpresentational State Transfer
RHEL	Red Hat Enterprise Linux
SFP	Security Function Policy
SFR	Security Functional Requirement

Acronym	Definition
ST	Security Target
SLES	Suse Linux Enterprise Server
TOE	Target of Evaluation
TSF	TOE Security Functionality
VADP	vStorage API for Data Protection
VM	Virtual Machine

Table 17 - Acronyms