Dell EMC™ Avamar® v18.1

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2095-000-D102
Version: 1.8
19 September 2019

Dell EMC
176 South Street
Hopkinton, MA, USA
01748

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J7T2

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 Target of Evaluation (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 reference, the Target of Evaluation 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 IT environment.

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

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

1.2 SECURITY TARGET REFERENCE

ST Title:	Dell EMC™ Avamar® v18.1 Security Target
ST Version:	1.8
ST Date:	19 September 2019

1.3 TOE REFERENCE

TOE Identification: Dell EMC™ Avamar® v18.1.0.33 with Hotfixes 301590, 300449, 300443, 305019, 309443, and AvPlatformOsRollup Security Patch

TOE Developer: Dell EMC

TOE Type: Data Backup (Other Devices and Systems)

1.4 TOE OVERVIEW

Dell EMC Avamar performs backups and restores for remote offices, data center local area networks (LAN), and VMware environments. Using 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 Network Data Management Protocol (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 Java-based GUI application executing on a Windows or Linux workstation, or via a Command Line Interface (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 sends it to the Server. The Avamar Agents are delivered as software.

Authorized users on Client machines 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.

The Avamar NDMP Accelerator acts as a front-end to NDMP-based storage systems (such as Dell 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 running the NDMP Accelerator software.

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.

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The required components from the TOE Environment are specified in the following table.

Component	Operating System	Hardware
Management Workstation	Red Hat Enterprise Linux Release (RHEL) 7 (64-bit) Microsoft Windows 10	General Purpose Computing Hardware
Client Systems	Windows Server 2016 (64-bit) SLES 12 (64-bit)	General Purpose Computing Hardware
VMWare Servers	VMWare vSphere ESXi 6.0	General Purpose Computer Hardware
NDMP-Based Storage	Unity 4.4.0	General purpose storage device front-ended by the NDMP Accelerator

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE includes the following components:

Component	Version
Avamar Server Appliance	Multi-node system with Gen4T Hardware and supporting the MCCLI
NDMP Accelerator Appliance	Gen4T NDMP Accelerator Node

Component	Version
Avamar Server Software	V18.1.0.33 with Hotfixes 301590, 300449, 300443, 305019, 309443, and AvPlatformOsRollup Security Patch
Avamar NDMP Accelerator Software	V18.1.0.33
Avamar Agent for Windows	V18.1.100.33
Avamar Agent for Linux	V18.1.100.33
Avamar VMware Universal Proxy	V18.1.100.33
Avamar MCGUI for Windows	V18.1.0.33
Avamar MCGUI for Linux	V18.1.0.33

Table 2 – TOE Components

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. Figure 1 illustrates the TOE in its evaluated configuration.

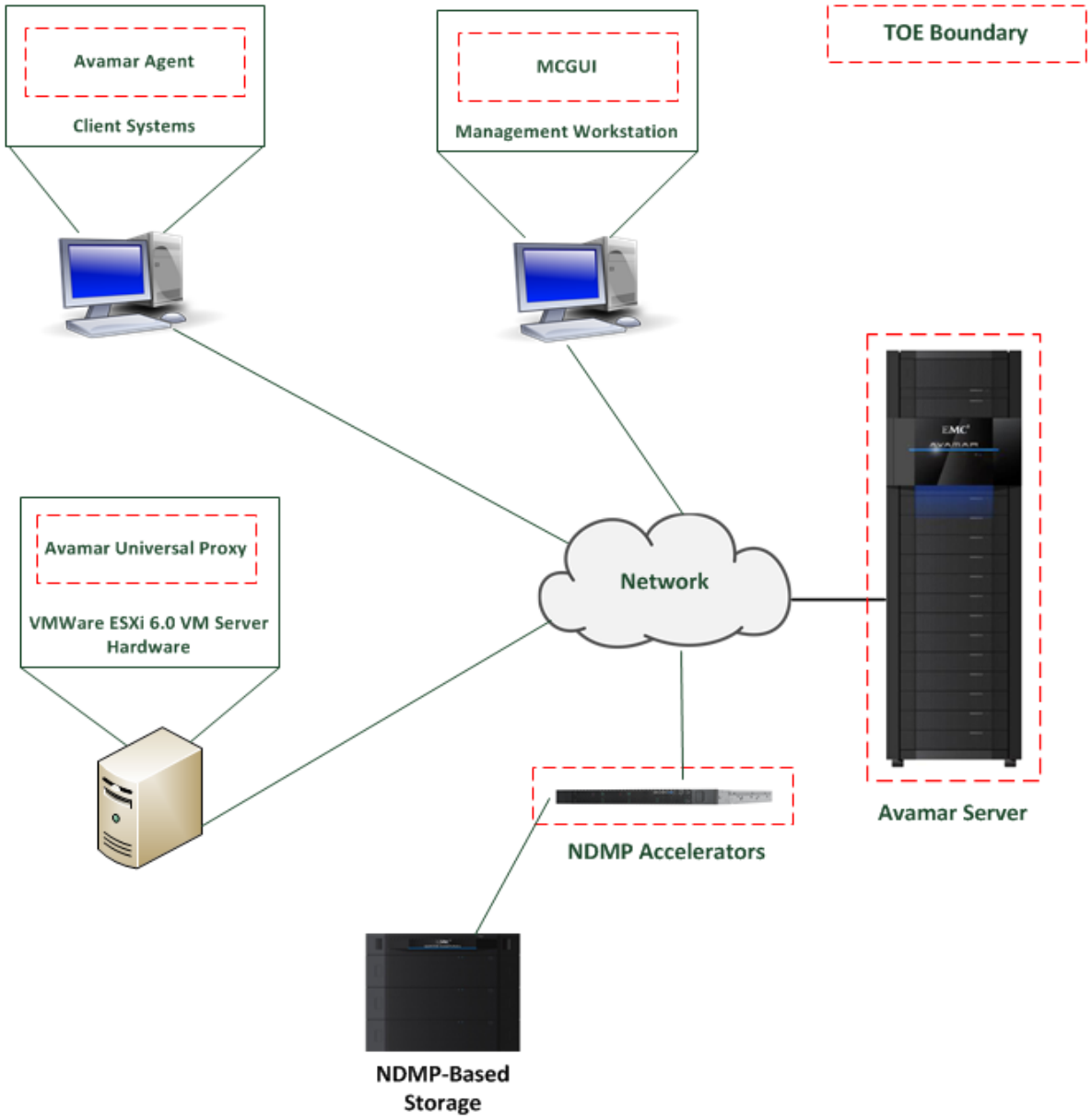

Figure 1 – Avamar TOE Diagram

1.5.1.1 TOE Delivery

The Avamar Server appliances come pre-loaded with the TOE software and are shipped directly to the customer. All other software components are available for download to registered customers at: https://support.emc.com/downloads/.

The following table identifies each TOE software component in its delivered format:

Software	Version	File Name/Format
Avamar Server Software	V18.1.0.33	AvamarBundle_SLES11_64-18.1.0-33.zip
Avamar Server Hotfix 301590	V18.1.0.33	V18.1.0.33_HF_301590.avp
Avamar Server Hotfix 300449	V18.1.0.33	HF300449.tgz
Avamar Server Hotfix 300443	V18.1.0.33	V18_1_0_33_HF_300443.avp
Avamar Server Hotfix 305019	V18.1.0.33	Gen4TcpuSecurityHotfix-HF305019.avp
Avamar Server Hotfix 309443	V18.1.0.33	WorkflowUpdate-v1.avp
AvPlatformOsRollup Security Patch	V18.1.0.33	AvPlatformOsRollup_2019-R1-v4.avp
Avamar NDMP Accelerator Software	V18.1.0.33	AcceleratorInstallSles-18.1.0-33.avp
Avamar MCGUI for Windows	V18.1.0.33	AvamarConsoleMultiple-windows-x86_64-18.1.0-33.exe
Avamar MCGUI for Linux	V18.1.0.33	AvamarConsole-linux-rhel-x86_64-18.1.0-33.rpm
Avamar VMware Universal Proxy	V18.1.100.33	AvamarCombinedProxy-linux-sles12sp1_64-18.1.100-33.ova
Avamar Agent for Windows	V18.1.100.33	AvamarClient-windows-x86_64-18.1.100-33.msi
Avamar Agent for SLES	V18.1.100.33	AvamarClient-linux-sles11sp1-x86_64-18.1.100-33.rpm

Table 3 - TOE Software Files & Format

1.5.1.2 TOE Guidance

The TOE includes the following guidance documentation:

- Dell EMC Avamar, Administration Guide, Version 18.1, July 2018
- Dell EMC Avamar Backup Clients, User Guide, Version 18.1, July 2018
- Dell EMC Avamar for VMware, User Guide, Version 18.1, July 2018
- Dell EMC Avamar for Windows Servers, User Guide, Version 18.1, July 2018
- Dell EMC Avamar, Management Console Command Line Interface (MCCLI) Guide, Version 18.1, July 2018
- Dell EMC Avamar, NDMP Accelerator for Dell EMC NAS Systems, User Guide, Version 18.1, July 2018

- Dell EMC Avamar, Product Security Guide, Version 18.1, July 2018
- Dell EMC Avamar, Virtual Edition for VMware, Version 18.1, July 2018

All guidance documentation is provided in PDF format and is available for download to registered users at: https://support.emc.com/products/ .

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 4 summarizes the logical scope of the TOE.

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 gaining TOE access.
Security Management	The TOE provides management capabilities via the 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.
Protection of the TSF	The TOE provides reliable time stamps for auditable events.

Table 4 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The following product features are excluded from this evaluation:

- REST API - Disabled (requires installation)
- EMC Secure Remote Services (ESRS) – Not used (requires configuration)

- Enterprise authentication – Disabled (requires configuration)
- Local user access from clients (pass-through authentication) – Not used (requires configuration)

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

Agents are supported on the following operating systems (in addition to those specified in Table 1): 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. This feature requires configuration and is not used as part of the evaluation.

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-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

2.3 PACKAGE CLAIM

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

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP, therefore a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 5 lists the threats addressed by the TOE.

Potential threat agents are unauthorized persons. Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential unauthorized data accesses to go undetected.
T.PRIVILEGE	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	An unauthorized user may attempt to access user data (backup files) which could result in data leakage.

Table 5 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on 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.ACCOUNT	The authorized users of the TOE shall be held 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 be managed only by authorized users.

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 are one or more competent individuals assigned to manage the TOE.
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, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.
A.PROTECT	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.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.AUDIT	The TOE must record audit records for security related events.
O.BACKUP	The TOE shall backup specified client data and make it available for restore operations.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.PROTECT	The TOE must ensure the integrity of all system and audit data by protecting itself from unauthorized access.
O.TIME	The TOE must provide reliable timestamps.[1]

Table 8 – Security Objectives for the TOE

[1] The O.TIME objective only applies to the Avamar Server and NDMP Accelerator.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

Security Objective	Description
OE.INSTALL	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.PHYSICAL	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.[2]

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 organizational policies identified for the TOE.

	T.IMPCON	T.PRIVILEGE	T.UNAUTH_ACCESS	P.ACCOUNT	P.BACKUP	P.MANAGE	A.MANAGE	A.NETWORK	A.NOEVIL	A.PROTECT

[2] The OE.TIME objective only applies to the Avamar Agent and Universal Proxy components.

	T.IMPCON	T.PRIVILEGE	T.UNAUTH_ACCESS	P.ACCOUNT	P.BACKUP	P.MANAGE	A.MANAGE	A.NETWORK	A.NOEVIL	A.PROTECT
O.ACCESS	X	X	X			X				
O.ADMIN	X					X				
O.AUDIT			X	X						
O.BACKUP					X					
O.IDENTAUTH	X	X		X		X				
O.PROTECT		X				X				
O.TIME				X						
OE.INSTALL	X					X			X	
OE.NETWORK								X		
OE.PERSON						X	X		X	
OE.PHYSICAL									X	X
OE.TIME				X						

Table 10 – Mapping Between Objectives, Threats, OSPs, 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.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.

	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	OE.INSTALL	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.INSTALL objective states the authorized administrators will configure the TOE properly. The O.ADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDENTAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTAUTH objective by only permitting authorized users to access TOE functions.	

Threat: **T.PRIVILEGE**	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.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.PROTECT	The TOE must ensure the integrity of all system and audit data by protecting itself from unauthorized access.
Rationale:	The O.IDENTAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTAUTH objective by only permitting authorized users to access TOE functions. The O.PROTECT objective addresses this threat by providing TOE self-protection.	

Threat: **T.UNAUTH_ ACCESS**	An unauthorized user may attempt to access user data (backup files) which could result in data leakage.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.AUDIT	The TOE must record audit records for security related events.

Rationale:	The O.ACCESS objective only permits authorized access TO 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.ACCOUNT**	The authorized users of the TOE shall be held accountable for their actions within the TOE.	
Objectives:	O.AUDIT	The TOE must record audit records for security related events.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.TIME	The TOE must provide reliable timestamps.
	OE.TIME	The operational environment will maintain reliable timestamps for use by TOE components.
Rationale:	The O.AUDIT 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 for the remaining TOE components. The O.IDENTAUTH 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 makes it available for restore operations.	

Policy: **P.MANAGE**	The TOE shall be managed only by authorized users.	
Objectives:	O.ACCESS	The TOE must allow authorized users to

		access only appropriate TOE functions and data.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.PROTECT	The TOE must ensure the integrity of all system and audit data by protecting itself from unauthorized access.
	OE.INSTALL	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.ADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTALL objective supports the OE.PERSON objective by ensuring administrators follow all provided documentation and maintain the security policy. The O.IDENTAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTAUTH objective by only permitting authorized users to access TOE functions. The O.PROTECT objective addresses this policy by providing TOE self-protection.	

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 are one or more competent individuals assigned to manage the TOE.	
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, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE.INSTALL	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.
	OE.PHYSICAL	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.INSTALL objective ensures that the TOE is properly installed and operated and the OE.PHYSICAL objective provides for physical protection of the TOE by authorized administrators. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.	

Assumption: A.PROTECT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.	
Objectives:	OE.PHYSICAL	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.PHYSICAL objective provides for the physical protection of the TOE software and the hardware on which it is installed.

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the extended Security Functional Requirements (SFRs) used in this ST. The following extended SFR has been created to address additional security features of the TOE:

a. User Data Backup/Restore (FDP_BCK_EXT.1)

5.1.1 Family FDP_BCK_EXT: User Data Backup/Restore

User Data Backup/Restore provides for the functionality to perform backup and restore operations as directed by administrators and users. The User Data Backup/Restore family was modeled after FDP_ACC: Access Control Policy. The User Data Backup/Restore SFR was loosely modeled after FDP_ACC.1: Subset access control.

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

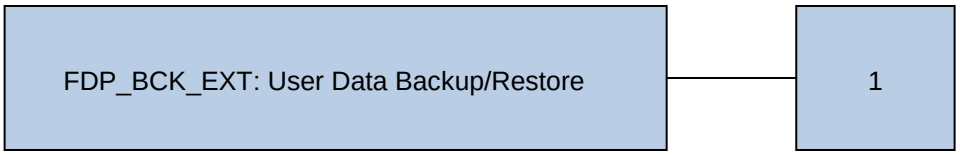

Figure 2 – FDP_BCK_EXT: User Data Backup/Restore Component Levelling

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.

5.1.1.1 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 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

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 **bold** for 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 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5:

Class	Identifier	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

Class	Identifier	Name
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (server)
	FDP_ACC.1(2)	Subset access control (client)
	FDP_ACF.1(1)	Security attribute based access control (server)
	FDP_ACF.1(2)	Security attribute based access control (client)
	FDP_BCK_EXT.1	User data backup/restore
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1(1)	Management of security attributes (server)
	FMT_MSA.1(2)	Management of security attributes (client)
	FMT_MSA.3(1)	Static attribute initialisation (server)
	FMT_MSA.3(2)	Static attribute initialisation (client)
	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; and*

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 (FDP)

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

Hierarchical to: No other components.

Dependencies: FDP_ACF.1(1) Security attribute based access control (Server)

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

Subjects: Users on client machines;

Objects: Clients, Backup Files;

Operations: Backup, Restore].

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

Hierarchical to: No other components.

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

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

Subjects: Users on client machines;

Objects: Clients, Backup Files;

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(1) Subset access control (Server)

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

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

- *Subjects: Authorized Users*
  Security Attributes: UserID, Role, associated Domain
- *Objects: User data*[3]
  Security Attributes: 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 on 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*].

[3] User data is categorized as any data on a client machine that can be backed up or restored by the TOE.

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1(2) Subset access control (Client)
FMT_MSA.3(2) Static attribute initialisation (Client)

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

- *Subjects: Authorized Users*
  Security Attributes: UserID, Role, associated Domain

- *Objects: User data*
  Security Attributes: 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 Backup Only User and Backup/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, Backup/Restore User, and Restore/Ignore File Permissions 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: [*none*].

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.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication.

Dependencies: FIA_UID.1 Timing of identification

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.

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.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of authentication.

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.4 Security Management (FMT)

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

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1(1) Subset access control (server), 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(2) Subset access control (Server), 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(1) Management of security attributes (server)

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(2) Management of security attributes (client)

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_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*].

6.2.4.6 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, Backup Only Operator, Backup/Restore Operator, Activity Operator, Backup Only User, Restore Only User, Backup/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 (FPT)

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 ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 12.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	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)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction

Assurance Class	Assurance Components	
	Identifier	**Name**
	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)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 12 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

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

	O.ACCESS	O.ADMIN	O.AUDIT	O.BACKUP	O.IDENTAUTH	O.PROTECT	O.TIME
FAU_GEN.1			X				
FAU_GEN.2			X				
FAU_SAR.1			X				
FAU_SAR.2			X				
FDP_ACC.1(1)				X		X	

	O.ACCESS	O.ADMIN	O.AUDIT	O.BACKUP	O.IDENTAUTH	O.PROTECT	O.TIME
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.2	X				X		
FIA_UAU.7	X				X		
FIA_UID.2	X				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_SMF.1		X					
FMT_SMR.1	X	X					
FPT_STM.1			X				X

Table 13 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

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

Objective: O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action

	FMT_MSA.1(1)	Management of security attributes (server)
	FMT_MSA.1(2)	Management of security attributes (client)
	FMT_SMR.1	Security roles
Rationale:	FIA_UID.2 and FIA_UAU.2 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. FMT_MSA.1(1) and FMT_MSA.1(2) 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.	

Objective: **O.ADMIN**	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	FMT_MSA.1(1)	Management of security attributes (server)
	FMT_MSA.1(2)	Management of security attributes (client)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Rationale:	FMT_MSA.1(1) and FMT_MSA.1(2) 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.	

Objective: **O.AUDIT**	The TOE must record audit records for security related events.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FPT_STM.1	Reliable time stamps

Rationale:	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.

Objective: **O.BACKUP**	The TOE shall backup specified client data and make it available for restore operations.	
Security Functional Requirements:	FDP_ACC.1(1)	Subset access control (server)
	FDP_ACC.1(2)	Subset access control (client)
	FDP_ACF.1(1)	Security attribute based access control (server)
	FDP_ACF.1(2)	Security attribute based access control (client)
	FDP_BCK_EXT.1	User data backup/restore
	FMT_MSA.1(1)	Management of security attributes (server)
	FMT_MSA.1(2)	Management of security attributes (client)
	FMT_MSA.3(1)	Static attribute initialisation (server)
	FMT_MSA.3(2)	Static attribute initialisation (client)
Rationale:	FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACF.1(1), and FDP_ACF.1(2) 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(1) and FMT_MSA.1(2) ensure that appropriate security attributes are maintained for the subjects and objects. FMT_MSA.3(1) and FMT_MSA.3(2) require that restrictive attributes based on Domain membership are applied.	

Objective: **O.IDENTAUTH**	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	
Security Functional	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action

Requirements:	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Rationale:	FIA_UID.2 and FIA_UAU.2 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.	

Objective: **O.PROTECT**	The TOE must ensure the integrity of all system and audit data by protecting itself from unauthorized access.	
Security Functional Requirements:	FDP_ACC.1(1)	Subset access control (server)
	FDP_ACC.1(2)	Subset access control (client)
	FDP_ACF.1(1)	Security attribute based access control (server)
	FDP_ACF.1(2)	Security attribute based access control (client)
	FMT_MSA.3(1)	Static attribute initialisation (server)
	FMT_MSA.3(2)	Static attribute initialisation (client)
Rationale:	FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACF.1(1), and FDP_ACF.1(2) define the access control policy for users of the Server and Agent management interfaces. FMT_MSA.3(1) and FMT_MSA.3(2) requires restrictive access to backup data by default so that no access is granted until explicitly configured by authorized users.	

Objective: **O.TIME**	The TOE must provide reliable timestamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 requires accurate time stamps to be available.	

6.4.3 Dependency Rationale

Table 14 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	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FDP_ACC.1(1)	FDP_ACF.1(1)	✓	
FDP_ACC.1(2)	FDP_ACF.1(2)	✓	
FDP_ACF.1(1)	FDP_ACC.1(1)	✓	
	FMT_MSA.3(1)	✓	
FDP_ACF.1(2)	FDP_ACC.1(2)	✓	
	FMT_MSA.3(2)	✓	
FDP_BCK_EXT.1	None	N/A	
FIA_ATD.1	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UAU.7	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MSA.1(1)	FDP_ACC.1(1) or FDP_IFC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1(2) or FDP_IFC.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(1)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	
	FMT_MSA.3	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_STM.1	None	N/A	

Table 14 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

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.

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 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:

- Date 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. Users with any other user roles are denied access.

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

7.2 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 the MCGUI or MCCLI. 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). Their access permissions are defined by the Client Access Control SFP.

The Server Access Control SFP defines access to backup files through the MCGUI and MCCLI. The server-side user assigned attributes 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 client domains. Avamar client domains are distinct zones to organize and segregate clients in the Avamar server. The server provides enhanced security by enabling you to define administrative user accounts on a domain-by-domain basis. The domains are hierarchical so users added to a higher level domain have 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.

The Avamar VMware Universal Proxy acts as a proxy backup server and is installed as a virtual machine on VMware vSphere ESXi platforms. It provides the interface to virtual machines images via VADP to receive backup and restore instructions, send images related to backup and restore operations, and respond to polls from the Avamar server.

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.

7.3 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 must present a valid username and password before gaining access to the TOE.

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.

Avamar Agent users on client systems must also authenticate before being granted access to any of the TOE functions. Users can access the Avamar Agent through either a Web or client GUI application.

TOE Security Functional Requirements addressed: FIA_ATD.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2.

7.4 SECURITY MANAGEMENT

Management of the TOE is performed by users with an Operator and/or Administrator role via the MCGUI or MCCLI. Each user session is bound to a role and domain upon login, and those attributes determine their access permissions.

Backup and restore operations may be scheduled by users with an Administrator and/or Operator role. 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(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_SMF.1, FMT_SMR.1.

7.5 PROTECTION OF THE TSF

The TOE provides reliable time stamps for auditable events.

TOE Security Functional Requirements addressed: FPT_STM.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terms are used in this ST:

Term	Description
User Data	User data is categorized as any data on a client machine that can be backed up or restored by the TOE.

Table 15 - Terminology

8.2 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

Acronym	Definition
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
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
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 16 – Acronyms