EMC Corporation
EMC® Avamar® v6.1

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.0

Prepared for:

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

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

Prepared by:

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

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the EMC® Avamar® v6.1, and will hereafter be referred to as the TOE throughout this document. The TOE is backup and recovery software that uses data deduplication technology to reduce daily backups before transferring across the network for storage on disk.

1.1 Purpose

This ST is divided into nine sections, as follows:

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

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	EMC Corporation EMC® Avamar® v6.1 Security Target
ST Version	Version 1.0
ST Author	Corsec Security, Inc.
ST Publication Date	8/20/2012
TOE Reference	EMC® Avamar® v6.1.0-402

1.3 Product Overview

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

EMC Avamar® v6.1 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. Variable block deduplication divides data into sub-file segments further reducing duplications. Backups are on changes to data occur at administrator-scheduled intervals, making each backup a full backup, while significantly reducing backup time.

Data is secured through RAIN[1] technology at the Data Store server. RAIN secures the data by striping and mirroring data across multiple storage nodes, protecting the data from a node failure. RAID[2] 1 level protection is provided at the disk level. Data can be encrypted in flight or at rest[3]. Checkpoints are created twice daily and server data is hashed to ensure integrity. The server can be quickly rolled back to one of these checkpoints at any time.

The software 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.

The Avamar agent, which runs on client systems, is designed to run on many operating systems including:

- Microsoft Windows
- Microsoft Windows Server
- Red Hat Enterprise Linux (RHEL)
- Red Hat Linux
- Solaris
- SUSE Linux Enterprise Server (SLES)
- Apple Macintosh
- CentOS
- Debian
- FreeBSD[4]
- HP-UX[5]
- IBM[6] AIX[7]
- NetWare
- Novell Open Enterprise Server
- Oracle Enterprise Linux
- Santa Cruz Operation (SCO) Open Server
- SCO UnixWare

Replication can also be performed from a source Avamar server to a target Avamar server to perform backup to another location for disaster recovery. The replication feature uses the same functions as the backup, reducing duplications prior to sending data to the destination server, reducing network traffic and storage needs.

[1] RAIN – Redundant Array of Independent Nodes
[2] RAID – Redundant Array of Independent Disks
[3] Data encryption is not part of the CC evaluation.
[4] BSD – Berkeley Software Distribution
[5] HP-UX – Hewlett Packard UniX
[6] IBM – International Business Machines
[7] AIX – Advanced Interactive eXecutive

1.4 TOE Overview

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

The TOE is deduplication backup and restore software that runs on EMC hardware. Deduplication breaks data into variable length segments and eliminates redundant sub-file data segments. Each data segment is assigned a unique ID which the TOE uses to compare it to other data segments that are already backed up. Only new data is transferred for back up. The software is deployed in a client-server configuration supporting over 14 different platforms on the client side. The TOE provides faster backups, easier recoveries, flexible deployment, and network efficiency. The deduplication is performed on the client and server side decreasing storage and network load. The TOE can also be used to create offsite copies of data for disaster recovery purposes via global deduplicated replication over a wide area network (WAN) connection. The TOE can be used for enterprise applications, remote offices, desktops, laptops, network attached storage (NAS), or VMware.

Incremental backups are performed daily. Only the changed data is backed up and these changes combined with previous backups ensure a full backup is stored, eliminating the need for full weekly backups. The utility node backs up all user-defined data and parameters each hour to the storage nodes, allowing recovering of system data in the event of a utility node failure.

The TOE simplifies recovery by always having a full backup image. Recovery can be for the entire file system or individual files and can be directed to any client running the TOE client software. The use of RAIN architecture at the file-system level stripes data across three or more nodes and uses parity to recreate data lost during a single node failure. RAID architecture at the physical disk level mirrors the data and protects it from disk failure.

The TOE has two possible evaluated configurations. Figure 1 shows the details of the multi-node deployment configuration of the TOE:

The figure includes the following previously undefined acronyms:

- JVM – Java Virtual Machine
- NDMP – Network Data Management Protocol
- OS – Operating System
- MCS – Management Console Service
- ASCD – Avamar Server Connection Daemon
- LM – Login Manager

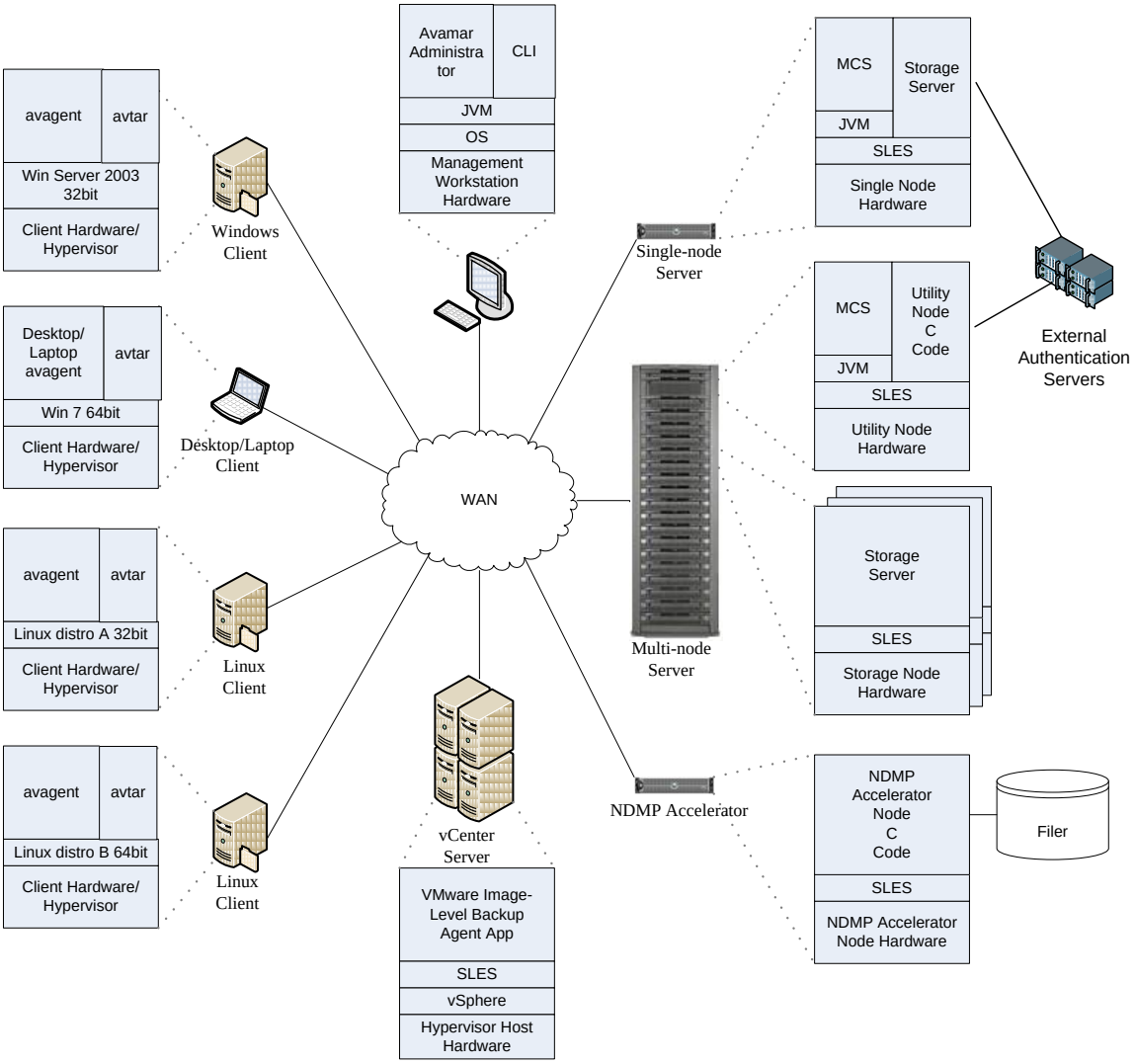

Figure 1 Multi-Node Deployment Configuration of the TOE

The TOE can also be deployed in a single-node, stand alone configuration where only the single-node server is used on the server side. The single-node server is often used for remote branch offices to locally backup and restore data. Figure 2 shows this configuration.

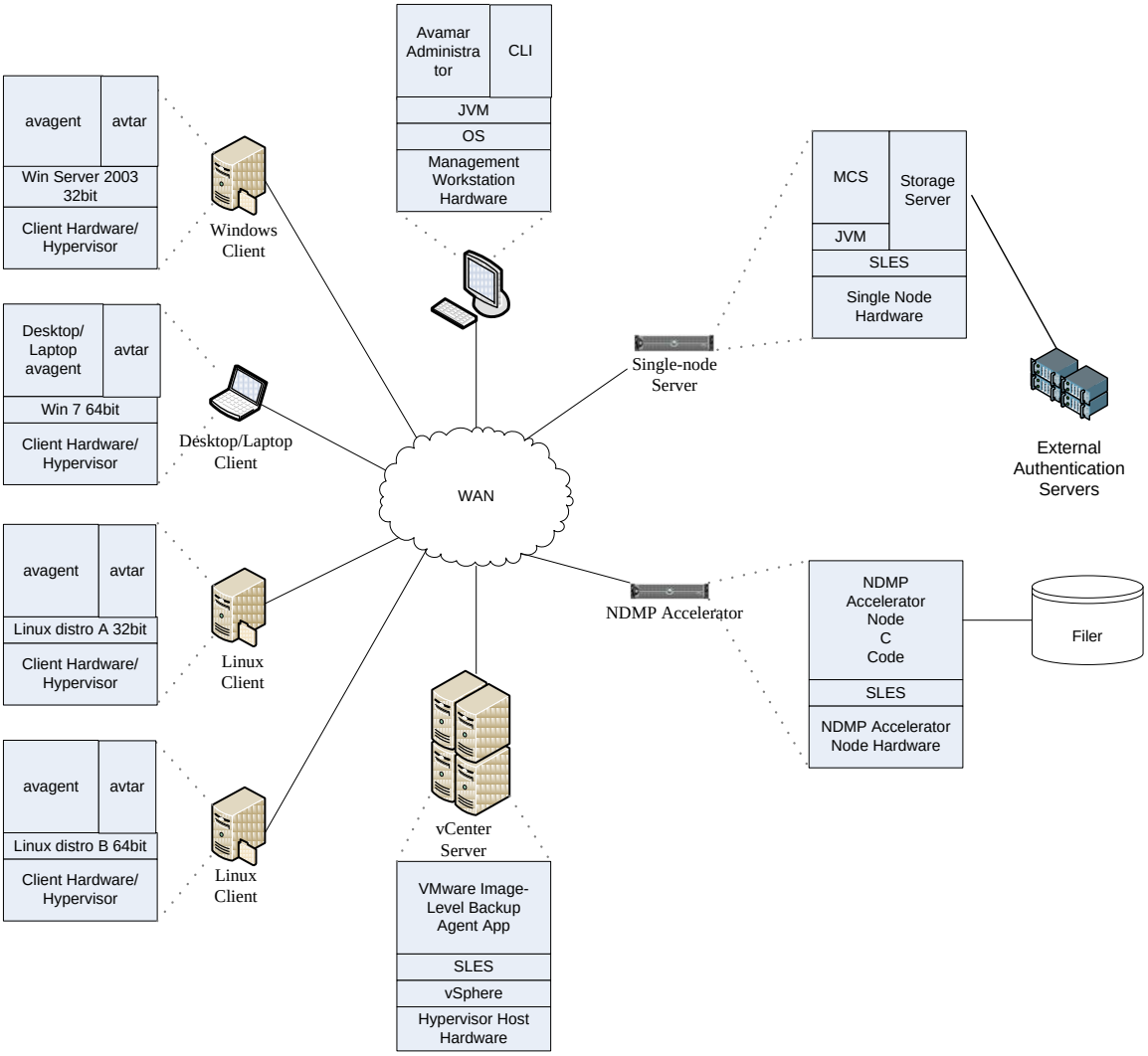

Figure 2 Single-node Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The Avamar Server is a logical grouping of one or more nodes. Each node is a self-contained, network addressable computer that runs the Avamar software and SLES OS. In the multi-node server the node is configured to be either a utility node or a storage node at installation. The utility node includes the MCS that monitors the data server, maintains a database of all server activity, and provides the management interface for the server. MCS maintains a PostgreSQL database to store management data such as backup schedules, datasets, configurations, and high level information about backup and restore activity, including timestamps, success or failure of an event, and the identification of the user performing the action. Administrators remotely access the utility node using the Avamar Administrator interface, a Java graphical user interface (GUI) or the management command line interface (CLI). These interfaces communicate with the MCS using a Transport Layer Security (TLS)-encrypted Java Remote Method Invocation (RMI) using a JVM that is provided by the TOE environment. Figure 3 shows the components of the utility node and how they interact with each other.

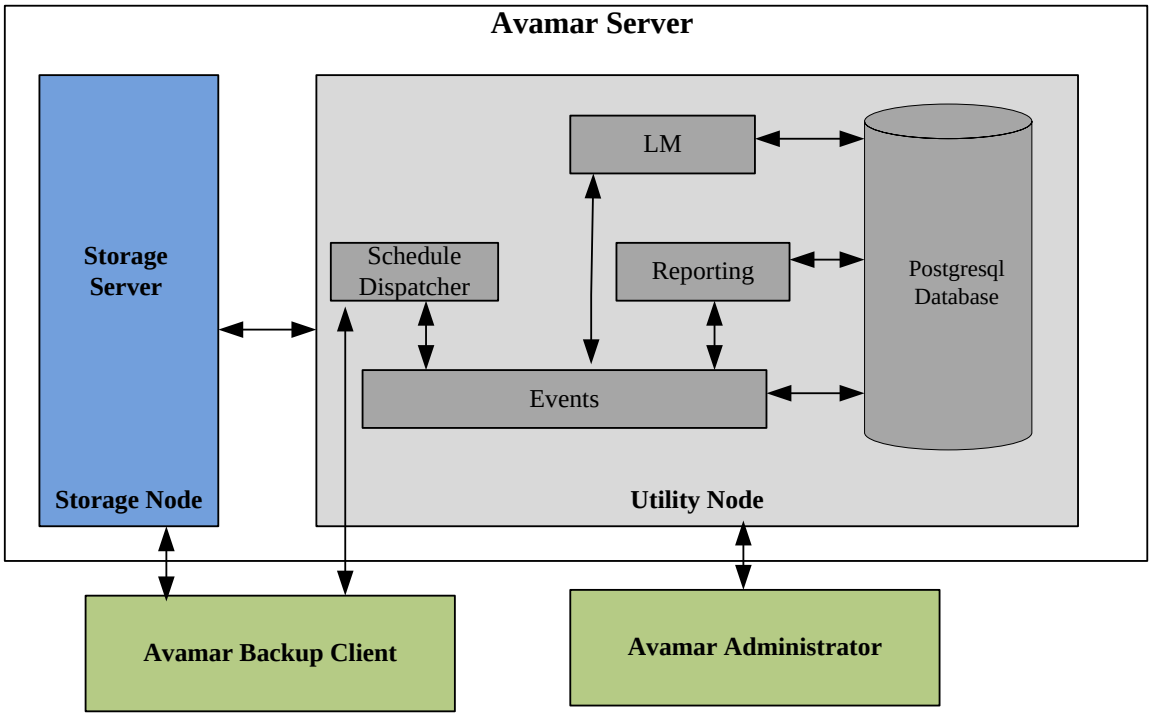

Figure 3 Avamar Functional Block Diagram

The storage node consists of a storage server that controls access to the physical storage. Each storage node manages its own two to twelve disks of RAID 1 storage. The storage nodes are connected to each other within the server via two redundant 1Gb[8] Ethernet connections. The client systems connect directly to any of the storage nodes and data is striped across the storage nodes. Nodes can be added to expand the system up to 16 nodes.

Client systems are network computers or workstations that access the Avamar server over a LAN or WAN. Clients must be registered and activated with the Avamar system before their data can be backed up or restored. The *avagent* binary runs on the client systems and connects to the MCS and waits for workorders. The *avtar* binary is used to conduct client data backup and connects directly to the storage server on the storage node. Window client systems use *avsss* to provide a user interface to the TOE. Clients also have one or more plug-ins. Filesystem plug-ins are used to browse, backup, and restore files on the client system and are specific for the OS on the client system. The following filesystem plug-ins are included:

- Linux
- Microsoft Windows
- VMware

Application plug-ins are used for operations on databases or other special applications. The NDMP application plug-in for NAS devices, including EMC storage systems and Network Appliance filers is a component of the TOE. The NDMP Accelerator accepts NDMP backups and acts as an Avamar client, allowing the Avamar deduplication process to back up a NAS device to the Avamar server.

When implementing VMware Image Backup and Restore the MCS communicates with the vCenter server to detect virtual machine clients and enable efficient management of backup jobs. The vCenter server is a

[8] Gb- Gigabit

scalable platform for management of virtual machines. The avagent resides on the vCenter server and does not need to be installed on each virtual client machine.

1.4.2 TOE Environment

The TOE runs on EMC Avamar Data Store Gen4 servers or general purpose hardware. The client software supports a number of operating systems Linux and Windows Operating Systems requirements are described in this section. Clients and servers are connected through a LAN or WAN of at least 1Gb Ethernet. Table 2 specifies the minimum system requirements for the proper operation of the TOE.

Table 2 TOE Minimum Requirements

Category	Requirement
Application Modules	Microsoft SQL[9] Server 7.0, 2000, 2005, or 2008 EMC NDMP (Celerra® DART 5.5, 5.6, 6; VNX™ OE for File 7.0) or NetApp NDMP (ONTAP 6.5, 7.0.4, 7.0.5, 7.0.6, 7.1.x, 7.2, 7.3.x, 8);
VMware	ESX Server 4.0, 4.1 ESX(i) hosts running proxy virtual machines, at least one of which runs Red Hat Linux VMware vSphere (ESXi) 4, 4.1 VMware vCenter v4.0, 4.1
Hardware	EMC Avamar® Data Store Gen4
Network	10baseT interface 1 Gb Ethernet Support for TCP/IP protocol

Linux systems can be used for the client side portion of the TOE with the *avagent* and *avtar* binaries. The minimum Linux system requirements are listed in Table 3. The TOE configurations in Figure 1 and Figure 2 include a 32-bit and 64-bit representation of these client systems.

Table 3 Linux Client Minimum Requirements

Name	Description
Operating System	• Red Hat Enterprise Linux Release 3, 4, 5, 6 (32- and 64-bit) • Red Hat Enterprise Linux Release 5.4 for System Z (64-bit)• • Red Hat Linux Release 9 • SUSE Linux Enterprise Server 8.2, 9, 10, 11 (32- and 64-bit) • SUSE Linux Enterprise Server 10.3 for System Z (64-bit) **IMPORTANT:** 32-bit Red Hat Enterprise Linux Release 5 requires Red Hat LIBC-5 compatibility libraries in order to install and run Avamar for Linux Client software. **IMPORTANT:** SUSE Linux Enterprise Server 11 (32- and 64-bit), requires libxml2 and libxml2-python compatibility libraries in order to install and run Avamar for Linux Client software. Use the latest version available (2.7.6-0.1 minimum) and correct RPM (that is, *.i586.rpm for 32-bit platforms, and *.x86_64.rpm for 64-bit platforms) for your specific application.
CPU[10]	x86
Filesystem	• ext2

[9] SQL – Structured Query Language
[10] CPU – Central Processing Unit

Name	Description
	• ext3 • Journaled File System (JFS) • ReiserFS
RAM[11]	128 MB[12]
Hard drive space	100 MB permanent hard drive space (1GB[13] recommended) for software installation. The Avamar client software also requires an additional 12 MB of permanent hard drive space for each 64 MB of physical RAM. This space is used for local cache files.
Network interface	10BaseT or higher, configured with the latest drivers for the platform.

Windows systems can also be used for the client side portion of the TOE with the *avagent* and *avtar* binaries. The TOE configurations in Figure 1 and Figure 2 include a 32-bit and 64-bit representation of the Windows client systems. The Windows operating systems must be one of those listed below:

Table 4 Windows Client Minimum Requirements

Name	Description
Operating System	• Windows 7 (32- and 64-bit) • Windows Vista (32- and 64-bit) • Microsoft Windows XP (32- and 64-bit) • Microsoft Windows Server 2008 and 2008 R2 • Microsoft Windows Server 2003, 2003 x64, and 2003 R2
CPU	1 GHz[14]
Filesystem	• FAT16 • FAT32 • NTFS
RAM	512 MB
Hard drive space	250 MB permanent hard drive space (1GB recommended) for software installation. The Avamar client software also requires an additional 12 MB of permanent hard drive space for each 64 MB of physical RAM. This space is used for local cache files. Backing up the Windows System State requires an additional 1GB of free disk space.
Network interface	10BaseT or higher, configured with latest drivers for the platform. Or IEEE 802.11a/b/g, configured with latest drivers for the platform

[11] RAM – Random Access Memory
[12] MB – Megabyte
[13] GB – Gigabyte
[14] GHz – Gigahertz

Name	Description
Web browser	Windows Internet Explorer v6.x, 7.x, and 8.x or Mozilla Firefox v3.x
Java	J2SE 5.0 Update 18

1.5 TOE Description

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

1.5.1 Physical Scope

Figure 4 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE is a backup and restore software system that runs on EMC hardware compliant to the minimum software and hardware requirements as listed in Table 2 (above). The TOE is installed within a company's network in a client-server configuration as depicted in Figure 4 or Figure 5 (below). The TOE can be deployed in a single-node configuration, with the utility and storage combined on one server as depicted in Figure 5, or in a multi-node configuration with one utility node, three storage nodes, and a remote single-node server as depicted in Figure 4. There are two management interfaces for the TOE, the Avamar Administrator GUI and the management CLI. Both management interfaces access the TOE through the utility node on the Avamar server using an RMI connection. The user interface on the client is a web user interface (UI), a client CLI, or a desktop interface. These interfaces access the storage nodes through the client system using an Avamar proprietary binary messaging protocol. The essential components for the proper operation of the TOE in the multi-node evaluated configuration are:

- For Utility node:
  - Utility Node software,
  - MCS,
  - JVM,
  - SLES 11 (64 bit);
- For Storage Node:
  - Storage server,
  - SLES 11 (64 bit);
- For single-node configuration:
  - Utility Node software,
  - MCS,
  - Storage server,
  - JVM,
  - SLES 11 (64 bit);
- For Client:
  - avagent,
  - avtar;
- For NDMP Accelerator Node:
  - NDMP Accelerator Node software,
  - SLES 11 (64 bit);
- For VMware Backup:
  - Vmware Image-level Backup Agent Application

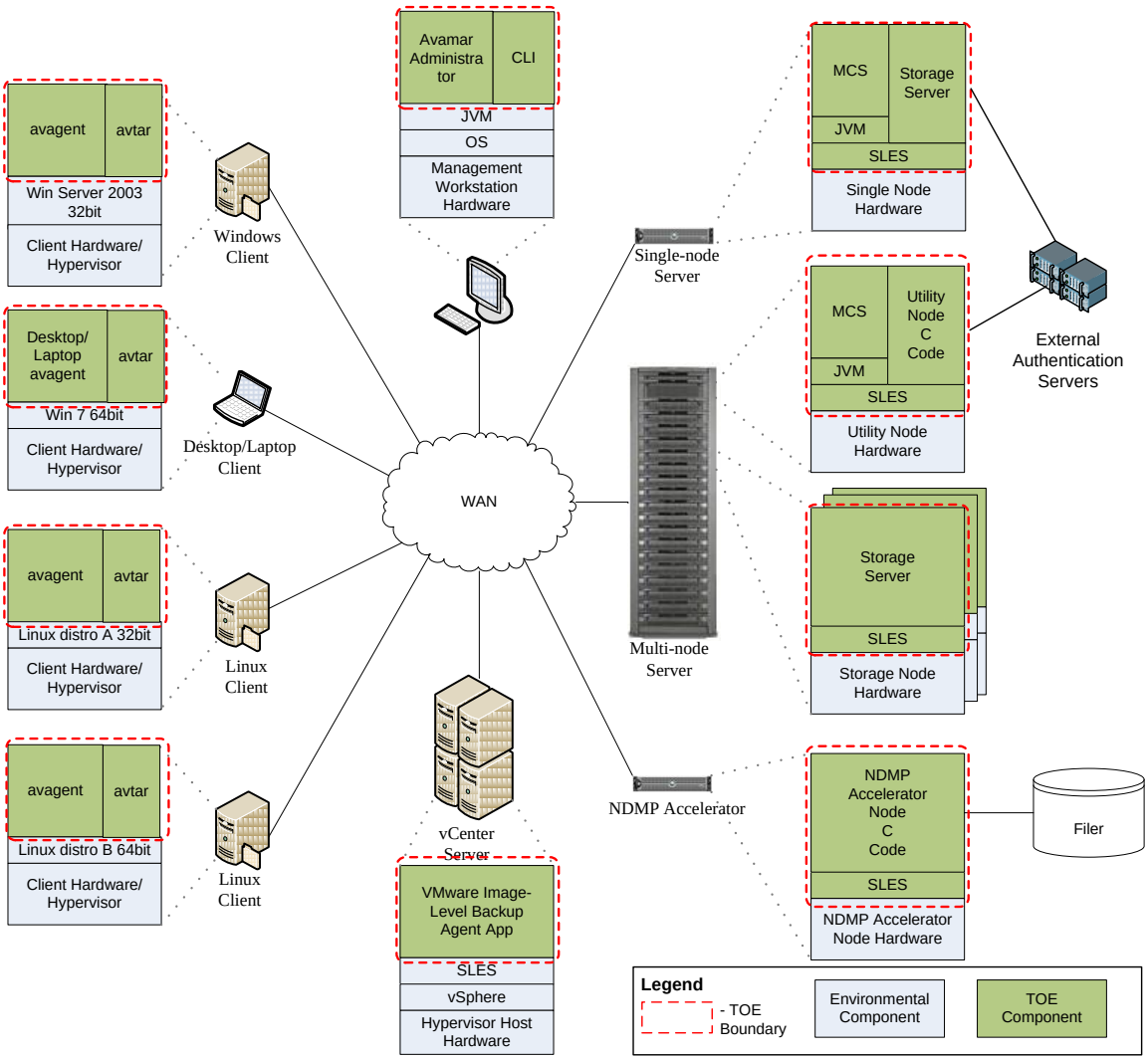

Figure 4 Physical Multi-node TOE Boundary

The essential components for the TOE in the single-node evaluated configuration are:

- For single-node configuration:
  - Utility Node software,
  - MCS,
  - Storage server,
  - JVM,
  - SLES 11 (64 bit);
- For Client:
  - avagent,
  - avtar;
- For NDMP Accelerator Node:
  - NDMP Accelerator Node software,
  - SLES 11 (64 bit);
- For Vmware Backup:
  - Vmware Image-level Backup Agent Application

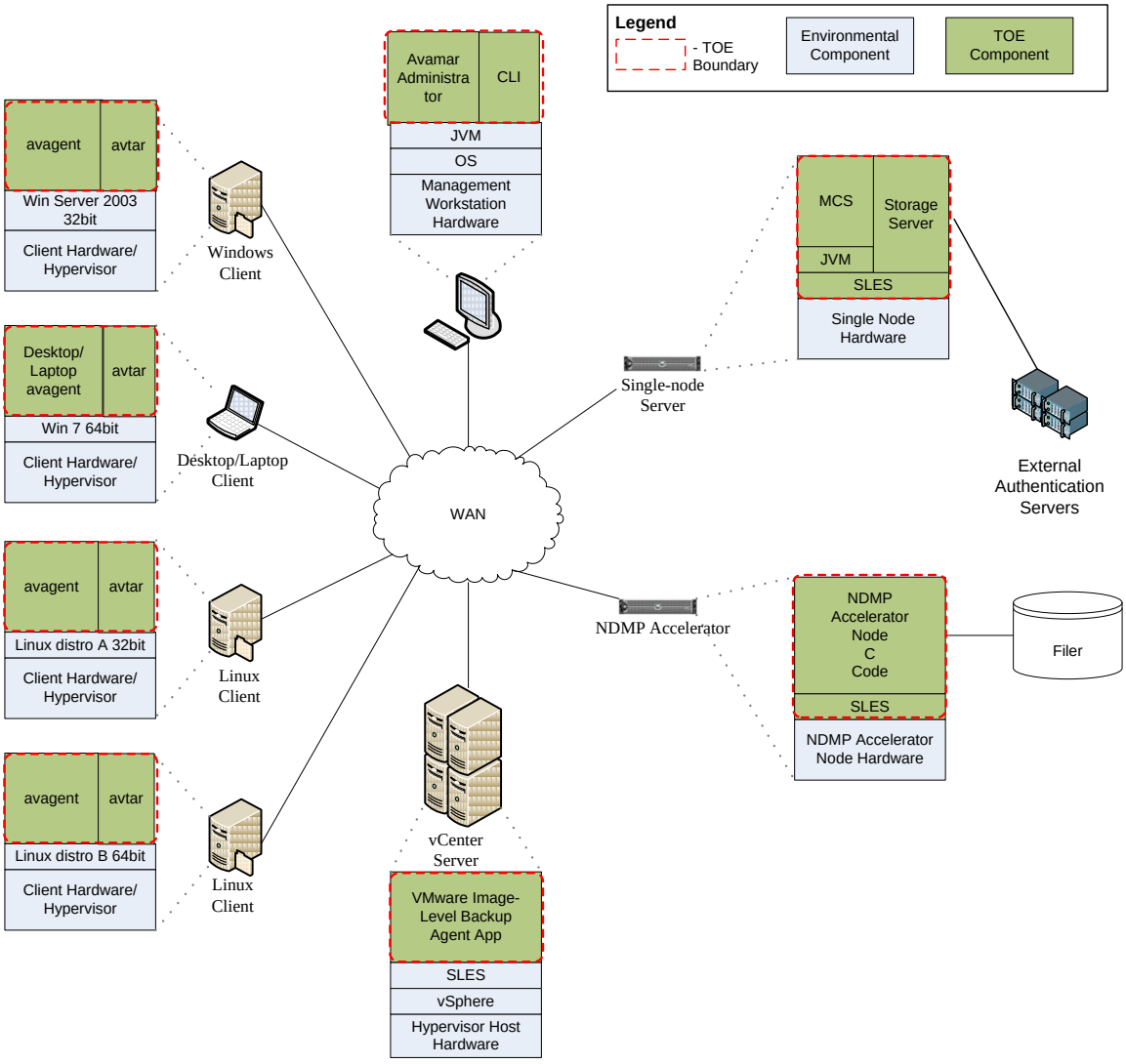

Figure 5 Physical Single-node TOE Boundary

1.5.1.1 TOE Software

The TOE consists of client/server backup and restore software and the underlying server OS. The Avamar server software includes utility node and storage node software. There is also an optional single-node which combines these functions into one component. All management functions are completed through the utility node. The client systems communicate directly with the storage nodes to perform backups and restores and with the utility node for scheduling and policies.

1.5.1.2 Guidance Documentation

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

- EMC® Avamar® v6.1 Data Store Gen4 Multi-Node System Installation Guide
- EMC® Avamar® v6.1 Data Store Gen4 Single-Node Customer Installation Guide
- EMC® Avamar® v6.1 Administration Guide
- EMC® Avamar® v6.1Management Console Command Line Interface (MCCLI) Programmer Guide
- EMC® Avamar® v6.1 Product Security Guide
- EMC® Avamar® v6.1 Operational Best Practices

- EMC® Avamar® v6.1 Release Notes
- EMC® Avamar® 6.1 Backup Clients Guide
- EMC® Avamar® 6.1 for VMware Guide
- EMC® Avamar® 6.1 for Windows Servers Guide
- EMC® Avamar® v6.1 NDMP Accelerator Guide
- EMC® Avamar® v6.1 for Lotus Domino Guide
- EMC® Avamar® v6.1 for Oracle Guide
- EMC® Avamar® v6.1 for SAP with Oracle Guide
- EMC® Avamar® v6.1 for Data Domain Integration Guide
- EMC® Avamar® v6.1 for SharePoint VSS[15] Guide
- EMC® Avamar® v6.1 for Exchange VSS Guide
- EMC® Avamar® v6.1 for IBM DB2 Guide
- EMC® Avamar® v6.1 for SQL Server Guide
- EMC® Avamar® v6.1 for Sybase ASE Guide
- EMC® Avamar® v6.1 Data Store Site Prep Technical Specifications
- EMC® Avamar® v6.1 SVR-D2U-R510 Installation and Replacement Guide
- EMC® Avamar® v6.1 Guidance Supplement

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Duplication
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of TOE Security Functions

1.5.2.1 Security Audit

The TOE audits startup and shutdown events of the system, as well as logout and login events on both the server and client-side. All administrative operations taken through the management interface are also logged. The audit records contain the events, the user identification (ID) of the user responsible for the event, the date and time of the event, and the outcome of the event. Users can only view the audit records for their assigned domains. System level audit records can only be viewed by an authorized administrator. The audit records are available through the Avamar Administrator GUI. Backup and restore events are logged in the storage server. The storage server log files are saved to a new file and stored on the server when the file exceeds 25MB. The log then overwrites the old file with new audit data. The auditd and syslog-ng are rotated daily if they are over 4MB. The old log file is compressed and archived and a new log file is started.

1.5.2.2 User Data Duplication

User data from client systems is broken into variable length, sub-file segments and compared for duplicate data at the client. Each unique piece of data is then given an object ID and compared to data already stored on the server. Duplications are replaced with the pointer for the previously stored information. Only non-duplicate data is transferred to the server and stored.

[15] VSS - Volume Snapshot Service

1.5.2.3 User Data Protection

The TOE uses the Server Access Control SFP[16] 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. Only the Root Administrator role has access to global configurations and to add or modify other administrator accounts. The Domain Administrator role can perform actions within their domain, including adding or modifying users 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.

The backup features of the Avamar system import data from a client to the Avamar server. This data can later be used to restore data to the client by exporting the data from the Avamar server back to the client. Replication of stored data to another Avamar Server is performed using the Server Access Control SFP. All replicated data is stored within a read-only REPLICATE domain on the destination server. The data can be used for disaster recovery, but cannot be changed while in the REPLICATE domain to maintain data consistency. Data also uses the Server Access Control SFP when transferring between nodes. The TOE employs a private back-end network to connect the nodes to prevent disclosure, modification or loss of user data during transport.

User data imported into the TOE is then stored on the Avamar server. The TOE maintains data integrity through the use of RAIN and RAID architecture at the node and disk level. RAIN architecture is only implemented in the multi-node configuration as it requires multiple nodes to stripe data. Data is striped across the nodes ensuring that a single node or disk failure does not result in loss of stored data. RAID architecture mirrors data at the disk level, ensuring an increased data reliability. A single-node configuration can also replicate its data to a multi-node instance of the TOE to ensure data integrity.

1.5.2.4 Identification and Authentication

An authorized administrator or an external authentication server assigns TOE users a username and password. These are mapped to an Avamar role and domain or client. The TOE stores username, password, user role, and access data in the storage nodes along with a field specifying if the authentication was performed locally or on an external server. When external authentication servers are used the TOE utilizes the Linux Pluggable Authentication Module (PAM) framework to verify that identification and authentication credentials provided to the external authentication server match the credentials stored within the TOE. Only an authorized administrator can change the security attributes of users.

User accessing the TOE through the server must be identified and authenticate with the TOE prior to any actions. Their username and role is bound to all actions taken on the TOE. Users accessing the TOE through a client system are not allowed access to management functions. Client-side users authenticate through the client CLI or through the client web UI. Once a user is authenticated with the TOE, his username and role is bound to all actions taken on the TOE. The TOE presents to each user only those actions for which his role has permissions.

Users on Windows and Mac clients also have the option to use a one click tray icon for backup of the client system. No authentication is required for this backup operation. The client system passes the UID of the user with the backup and the operation is logged and associated with the UID of the user.

1.5.2.5 Security Management

All management of the TOE is done through either the Avamar Administrator GUI or the CLI interface on the server. Only an authorized administrator can change system configuration or audit functions. The creation and deletion of user accounts and the modification of their security attributes is also limited to

[16] SFP- Security Functional Policy

authorized administrators. The TOE uses the Server and Client Access Control SFPs to manage access to the TOE. Pre-defined roles exist on the system and these roles cannot be added or modified. Operations on TOE data are restricted to those authorized to the user's assigned role.

1.5.2.6 Protection of TOE Security Functions

The server OS provides a reliable timestamp that is synchronized throughout the system. Data transmitted to separate nodes on the server is protected from disclosure or modification through the private, back-end network that connects the nodes. The Server Access Control SFP is used to interpret replicated data in the TOE. All replicated data is placed in the read-only REPLICATE domain.

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

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

- Avamar Gen4 Data Store hardware
- WAN client/server connection
- Ethernet back-end server connection
- Client-side OS and hardware
- Management workstation OS and hardware
- External authentication server
- Avamar product features:
    - Avamar Web Restore – legacy client-side user interface
    - FreeBSD, HP-UX, IBM AIX, Mac OS X, SCO OpenServer, SCO UnixWare, Sun Solaris, and Novell NetWare clients system plug-ins
    - EMC Connect Email Home
    - Avamar Filesystem and Vmware File-level Restore
    - Avamar Downloader Service
    - Data encryption

2 Conformance Claims

This section and Table 5 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 5 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim none; Parts 2 and 3 Interpretations of the CEM as of 2011/06/17 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

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

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

3.1 Threats to Security

This section identifies the threats to the IT[17] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into three categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- Failed storage disks: Overloaded storage could lead to corruption of data within the TOE. Storage is assumed to be of a sufficient size for TOE users' needs.

The first two categories are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[18] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 6 below lists the applicable threats.

Table 6 Threats

Name	Description
T.MASQUERADE	A user may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.TAMPERING	A user may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.
T.UNAUTH	A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.
T.FAILED DISK	A disk failure could occur because of improper configuration of the TOE by an authorized administrator.

3.2 Organizational Security Policies

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

[17] IT – Information Technology
[18] TSF – TOE Security Functionality

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 7 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 7 Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and client operating system.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.LOCATE	The TOE is located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.I&A	The operational environment will provide identification and authentication mechanisms when necessary for use of TOE.
A.SCONNECT	The operational environment will protect client and remote management sessions with the TOE.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 8 below.

Table 8 Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, associate users with events, and provide the authorized administrators with the ability to review the audit trail.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.PROTECT	The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data. The TOE must ensure the integrity of user data by monitoring the integrity of stored data and enforcing access policies on transferred data.
O.DATA OPTIMIZATION	The TOE must identify and remove duplicate user data prior to storage and/or movement across the network and ensure that adequate storage space is available.
O.TIMESTAMP	The TOE will provide reliable time stamps.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 9 below lists the IT security objectives that are to be satisfied by the environment.

Table 9 IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.PLATFORM	The TOE hardware and client OS must support all required TOE functions.
OE.I&A	The TOE environment must provide identification and authentication mechanisms if required for user access to TOE.
OE.SCONNECT	The TOE environment must provide a secure connection for client systems and remote administrators to access the TOE.

4.2.2 Non-IT Security Objectives

Table 10 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 10 Non-IT Security Objectives

Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 11 identifies all extended SFRs implemented by the TOE.

Table 11 Extended TOE Security Functional Requirements

Name	Description
EXT_FDD_DDR.1	Duplicate data removal

5.1.1 Class FDD: Data Deduplication

Data deduplication involves optimizing network usage and storage capacity by identifying previously stored data and deleting redundancies prior to moving data across the network and storing it in the TOE. The EXT_FDD: Data Deduplication class was modeled after the CC FDP: User Data Protection class. The extended family EXT_FDD_DDR: Duplicate Data Removal was modeled after the CC family FDP_RIP: Subset residual information protection.

5.1.1.1 Duplicate Data Removal (EXT_FDD_DDR)

Family Behaviour

This family defines the requirements for removal of duplicate data.

Component Leveling

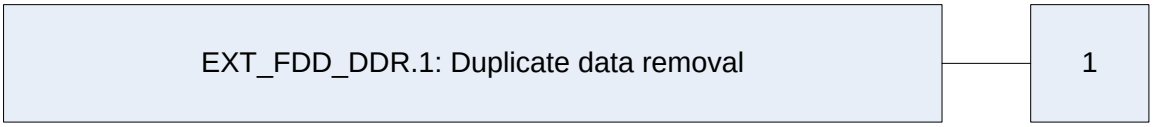

Figure 6 EXT_FDD_DDR Duplicate data removal family decomposition

EXT_FDD_DDR.1 Duplicate data removal provides the capability to remove redundant data prior to transferring user data for storage.

Management: EXT_FDD_DDR.1

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

- Maintenance (deletion, modification, addition) of the group of users with access rights to the stored user data.

EXT_FDD_DDR.1 Duplicate data removal
Hierarchical to: No other components
EXT_FDD_DDR.1.1
The TSF shall ensure that any previously stored data segments in user data marked for storage are identified and removed from the user data before the user data is transferred and stored.
Dependencies: No dependencies

5.2 Extended TOE Security Assurance Components

This ST does not define any extended TOE security assurance requirements.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

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

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

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(1) Audit Data Generation would be the first iteration and FAU_GEN.1(2) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 12 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 12 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FAU_STG.1	Protected audit trail storage	✓			
FAU_STG.3	Action in case of possible audit data loss		✓		
FDP_ACC.2(1)	Complete access control (server)		✓		✓
FDP_ACC.2(2)	Complete access control (client)		✓		✓
FDP_ACF.1(1)	Security attribute based access control (server)		✓		✓
FDP_ACF.1(2)	Security attribute based access control (client)		✓		✓
FDP_ETC.1	Export of user data without security attributes		✓		
FDP_ITC.1	Import of user data without security attributes		✓		
FDP_ITT.1	Basic internal transfer protection	✓	✓		

Name	Description	S	A	R	I
FDP_SDI.2(1)	Stored data integrity monitoring and action(multi-node)		✓	✓	✓
FDP_SDI.2(2)	Stored data integrity monitoring and action (single-node)		✓	✓	✓
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.1	Timing of authentication (client)		✓		
FIA_UAU.2	User authentication before any action (server)				
FIA_UID.2	User identification before any action				
FIA_USB.1	User-subject binding		✓		
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_ITT.1	Basic internal TSF data transfer protection	✓		✓	
FPT_STM.1	Reliable time stamps				
EXT_FDD_DDR.1	Duplicate data removal				

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

- Start-up and shutdown of the audit functions;
- All auditable events, for the [not specified] level of audit; and
- [*all login and logout on the system;*
- *all administrative actions performed on the CLI and GUI*].

FAU_GEN.1.2

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

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.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*authorised administrators*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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.

Dependencies: FAU_SAR.1 Audit review

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2

The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

FAU_STG.3.1

The TSF shall [*rename and store the log file*] if the audit trail exceeds [*25MB*].

Dependencies: FAU_STG.1 Protected audit trail storage

6.2.3 Class EXT_FDD: User Data Deduplication

EXT_FDD_DDR.1 Duplicate data removal
Hierarchical to: No other components.
EXT_FDD_DDR.1.1

The TSF shall ensure that any previously stored data segments in user data marked for storage are identified and removed from the user data before the user data is transferred and stored.

Dependencies: **No dependencies**

6.2.4 Class FDP: User Data Protection

FDP_ACC.2(1) Complete access control (server)
Hierarchical to: FDP_ACC.1 Subset access control
FDP_ACC.2.1
The TSF shall enforce the [*Server Access Control SFP*] on [
Subjects: users accessing server,
Objects: user data, server audit data, activity monitor, and TOE configuration data
]
and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2
The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.
Dependencies: FDP_ACF.1(1) Security attribute based access control (server)

FDP_ACC.2(2) Complete access control (client)
Hierarchical to: FDP_ACC.1 Subset access control
FDP_ACC.2.1
The TSF shall enforce the [*Client Access Control SFP*] on [
Subjects: users on clients systems,
Objects: user data and client audit data
]
and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2
The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.
Dependencies: FDP_ACF.1(2) Security attribute based access control (client)

FDP_ACF.1(1) Security attribute based access control (server)
Hierarchical to: No other components.
FDP_ACF.1.1
The TSF shall enforce the [*Server Access Control SFP*] to objects based on the following: [

- *Subjects: users accessing server*
  - *Security Attributes:*
    - *Username*
    - *Role*
    - *Login Domain*
- *Objects: user data, audit data, and TOE configuration data*
  - *Security Attributes:*
    - *Domain*
    - *User access lists*

].
FDP_ACF.1.2
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*a user may only view, modify, delete, backup or restore TOE data, audit data and/or the TOE configuration if the user is assigned to that domain and the user's role has the appropriate permissions*].

FDP_ACF.1.3
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].
FDP_ACF.1.4
The TSF shall explicitly deny access of subjects to objects based on the [*the rule that data stored in the replicate domain shall be read-only*].

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

FDP_ACF.1(2) Security attribute based access control (client)
Hierarchical to: No other components.
FDP_ACF.1.1
The TSF shall enforce the [*Client Access Control SFP*] to objects based on the following: [
- *Subjects: client systems*
  - *Security Attributes: username, role, domain*
- *Objects: user data and client audit data*
  - *Security Attributes: user access list, client properties*

].
FDP_ACF.1.2
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*a user may only view, backup, or restore user data and audit data if username, role, and domain are on the client's user access list; the client properties must authorize the operation*].
FDP_ACF.1.3
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].
FDP_ACF.1.4
The TSF shall explicitly deny access of subjects to objects based on the [*no additional rules*].
Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialization

FDP_ETC.1 Export of user data without security attributes
Hierarchical to: No other components.
FDP_ETC.1.1
The TSF shall enforce the [*Server Access Control SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2
The TSF shall export the user data without the user data's associated security attributes.
Dependencies: **FDP_ACC.1 Subset access control**

FDP_ITC.1 Import of user data without security attributes
Hierarchical to: No other components.
FDP_ITC.1.1
The TSF shall enforce the [*Server Access Control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2
The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*data is placed in the read-only REPLICATE domain*].
Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialisation

FDP_ITT.1 Basic internal transfer protection
Hierarchical to: No other components.
FDP_ITT.1.1
The TSF shall enforce the [*Client Access Control SFP*] to prevent the [disclosure, modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE.
Dependencies: **FDP_ACC.1 Subset access control**

FDP_SDI.2(1) Stored data integrity monitoring and action (multi-node)

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.2.1

The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all **user data** ~~objects~~, based on the following attributes: [*none, all data is monitored*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*reconstruct user data based on striping at nodes with RAIN in a multi-node configuration*].

Dependencies: No dependencies

FDP_SDI.2(2) Stored data integrity monitoring and action (single-node)

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.2.1

The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all **user data** ~~objects~~, based on the following attributes: [*none, all data is monitored*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*reconstruct user data based on mirroring at disk or replication to another instance of the TOE in single-node configuration*].

Dependencies: No dependencies

6.2.5 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
FIA_ATD.1.1
The TSF shall maintain the following list of security attributes belonging to individual users: [
- *Username*
- *Password*
- *Role*
- *Domain*

].
Dependencies: No dependencies

FIA_UAU.1 Timing of authentication (client)
Hierarchical to: No other components.
FIA_UAU.1.1
The TSF shall allow [*backup and restore of client data*] 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 allowing any other TSF-mediated actions on behalf of that user.
Dependencies: FIA_UID.1 Timing of identification

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

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

FIA_USB.1: User-subject binding
Hierarchical to: No other components
FIA_USB.1.1:
The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [
- *Username*
- *Password*
- *Role*

].
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: [
- *For users connecting to the server, the TSF will only present operations for which the user's role has permissions*
- *For users connecting to the client, the TSF will only present operations for that client for which the user's role has permissions*

].

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: [*only an authorized administrator may change user security attributes*].

Dependencies: FIA_ATD.1 User Attribute Definition

6.2.6 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1
The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [*system configuration*] to [*authorized administrators*].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1
The TSF shall enforce the [*Server Access Control SFP*] to restrict the ability to [change, default, query, modify, delete] the security attributes [*user access lists, domain, client properties, role*] to [*an authorised administrator*].
Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1
The TSF shall restrict the ability to [modify, delete, clear, [*other operations as defined in column 2 of Table 13*]] the [*TSF data as defined in Table 13 column 'TSF Data'*] to [*the roles listed in column 1 of Table 13*].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Table 13 Management of TSF Data

Role	Operation	TSF Data
Root Administrator	Read, create, backup, restore, view activity monitor, view Audit log and Syslog	top level server domain, access to all data, domains, backup schedules, groups, retention policies, and user accounts, Audit log and Syslog
Domain Administrator	Read, create, backup, restore, and view activity monitor, view Audit log and Syslog	domains, backup schedules, groups, retention policies, and data in assigned domain only, Audit log and Syslog

Role	Operation	TSF Data
Restore only operator	Perform restores, view activity monitor	Data from administrator assigned domain only
Backup only operator	Perform and schedule backups, view activity monitor	Data from administrator assigned domain only
Backup/restore operator	Perform restores, perform and schedule backups, view activity monitor	Data from administrator assigned domain only
Activity operator	View activity monitor, create reports	Data from administrator assigned domain only
Backup only user	Perform backups	Data from administrator assigned client only
Restore (Read) only user	Perform restores	Data from administrator assigned client only for which the user has permission
Backup/Restore user	Perform backup and restores	Data from administrator assigned client only
Restore only/Ignore File Permissions	Performs restores, view activity monitor	All data from administrator assigned client

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*management of security attributes as listed in Table 13 column 'TSF Data', management of TSF, management of security functions behavior as listed in Table 13 column 'Operation'*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*root administrator, domain administrator, restore only operator, back up only operator, backup/restore operator, activity operator, back up only user, restore (read) only user, backup/restore user, restore (read) only/ignore file permissions,*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.7 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection
Hierarchical to: No other components.
FPT_ITT.1.1
The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between ~~separate parts of the TOE~~ **distributed server nodes**.
Dependencies: No dependencies

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
FPT_STM.1.1
The TSF shall be able to provide reliable time stamps.
Dependencies: No dependencies

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2+ augmented with ALC_FLR.2. Table 14 summarizes the requirements.

Table 14 Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Basic Flaw Remediation
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

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

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 15 lists the security functions and their associated SFRs.

Table 15 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
User Data Duplication	EXT_FDD_DDR.1	Duplicate data removal
User Data Protection	FDP_ACC.2(1)	Complete access control (server)
	FDP_ACC.2(2)	Complete access control (client)
	FDP_ACF.1(1)	Security attribute based access control (server)
	FDP_ACF.1(2)	Security attribute based access control (client)
	FDP_ETC.1	Export of user data without security attributes
	FDP_ITC.1	Import of user data without security attributes
	FDP_ITT.1	Basic internal transfer protection
	FDP_SDI.2(1)	Stored data integrity monitoring and action(multi-node)
	FDP_SDI.2(2)	Stored data integrity monitoring and action (single-node)
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication (client)
	FIA_UAU.2	User authentication before any action (server)

TOE Security Function	SFR ID	Description
	FIA_UID.2	User identification before any action
	FIA_USB.1	User-subject binding
Security Management	FMT_MOF.1	Management of security functions behaviour
	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 TOE Security Functions	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_STM.1	Reliable time stamps

7.1.1 Security Audit

The TOE contains multiple audit logs, all of which can only be accessed by authorized administrators through the Avamar Administrator interface. Client-side users are only permitted to view the logs stored on that client system. A complete list of logs can be found in *EMC Avamar 6.0 Product Security Guide*. Following is a list of security relevant logs:

- syslogd – A daemon that can be configured to output Avamar server events in SLES OS syslog format.
- auditd – Captures system activity on a server that has been kickstarted. This log is disabled once the Avamar software is installed.
- Audit Log – Logs operations initiated by users in the Avamar system. Available as a sub-tab of Event Management in Avamar Administrator GUI.
- mccli.log – Contains debug and process data related to the operation of the MCCLI.
- mcclient.log – Contains debug, process, and login information for the MCGUI.
- Application level audits – These are logs are maintained in the PostgreSQL database on the utility node in the MCS. These logs can be accessed by authorized administrators using SQL commands from the CLI or through the Avamar Administrator interface.
- avagent.log – Status of all backup and restore activity for the client.
- workorder log – The log title is the workorder ID. Includes details about the specific workorder.
- avscc.log – Contains process and status information for Windows clients.

The storage server on the storage nodes contains a log file, *gsan.log*, with backup and restore information. It is limited to 25 MB. When the file is full it is renamed *gsan.log.1*, at which point new backup and restore audit data is written to a new file named *gsan.log* and the original file is overwritten. The TOE's auditing daemons, including auditd and syslog-ng, are rotated daily once they exceed 4MB. The old log file is compressed and archived and a new log file is started. Utility Subsystem logs are stored in a PostgreSQL database. The *getlogs* command can be used by an authorized administrator to gather important log files from a specified node.

The TOE audit records contain the information listed in Table 16.

Table 16 Audit Record Contents

Field	Content
Timestamp	Date and time event occurred
Event code	Code number associated with event
User ID	User ID of person performing action
Role	Role associated with person performing action
Product	Product that initiated the action. Must be one of the following: EM — Feature that is outside of TOE EMS — Feature that is outside of TOE END_USER MCCLI — Avamar Administrator CLI MCGUI — Avamar Administrator NONE — No product associated with event SNMP_SUB_AGENT — Initiated by SNMP agent TEST — Event part of test WEB_RESTORE — Feature that is outside of TOE
Component	Specific area with the product from which the action was initiated
Severity	Severity of the action. Must be one of the following: • OK • USER • PROCESS • NODE • USER_FATAL • PROCESS_FATAL • NODE_FATAL • SYSTEM_FATAL
Domain	The domain in which the action occurred

The Events or Activity Monitor tab in the Avamar Administrator GUI can be used to view audit information. Users can only view audit information from their assigned domains and system level audit data can only be viewed by an authorized administrator.
TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.3.

7.1.2 User Data Duplication

The TOE divides data on the client system into variable length, sub-file chunks called objects. A data deduplication algorithm is run on these objects to identify redundancies. Each unique object is assigned an object ID. The client software then checks if that object ID is already stored on the server by querying its local cache to determine if the file has been previously backed up. If an object ID is a duplicate the data will not be backed up and a pointer to the stored location within the server will be added to the backup. This reduces storage needs and backup time while also reducing network traffic. The objects are striped across the storage nodes with only non-duplicate segments requiring backup. The deduplication occurs both on the client side prior to being backed up to the server.
TOE Security Functional Requirements Satisfied: EXT_FDD_DDR.1

7.1.3 User Data Protection

Access control for the TOE differs depending on how a user accesses the TOE. Operators and Administrators can access the TOE through the server and are authorized by the Server Access Control SFP. Users can access the TOE only from a client system and are authorized by the Client Access Control SFP.

The Server Access Control SFP is used to manage access through the management interfaces. Users added to the Avamar server access user data, audit data, the activity monitor, and system configuration through the Avamar Administrator GUI or the Avamar Administrator CLI. Server-side users have a username, assigned domain, and one of the following roles:

- Root Administrator
- Domain Administrator
- Restore Only Operator
- Back Up Only Operator
- Backup/Restore Operator
- Activity Operator

Only the Root Administrator role has access to global configurations and to add or modify user accounts. Clients and users are organized and segregated within the server through the use of domains. Domain access is controlled through access control lists (ACLs). The domains are hierarchical so users added to a higher level domain can manage clients and policies in the lower levels. Users can only perform functions on the clients within their assigned domains.

The client systems follow the Client Access Control policy that allows users on the client system to access and view only data from the client and the client's associated audit data. No other data can be accessed through the client and no management functions can be done through the client. Client-side users have a username, assigned domain, and one of the following roles:

- Back Up Only User
- Restore (read) Only User
- Backup/Restore User
- Restore (read) Only/Ignore File Permissions

Users must be assigned to the client through the TOE before access is allowed. Clients can also be assigned retention policies and backup schedules by an authorized administrator through one of the management interfaces. Administrators can modify the client properties, including disabling backups initiated from that client. Vmware clients can only be managed from the management interfaces. Authorized users can perform on-demand backup and restores from all other clients.

The TOE can replicate data to another Avamar server in a different location. Exporting and importing of data is controlled by the Server Access Control SFP. Data does not retain its access control lists, but is placed in the read-only REPLICATE domain. Internally data is transferred over a private, back-end network between nodes, preventing disclosure, modification and loss of data. Data transferred between nodes retains the security attributes assigned to it for access control.

The integrity of user data stored on the server is ensured through a combination of RAIN architecture for the nodes in the multi-node configuration and RAID architecture for the disks in both multi-node and single-node configurations. Data is striped and mirrored across the nodes and disks ensuring that the loss of a node or of a disk will not result in the loss of data. Data can be reconstructed from the mirror copies in the event of a failure. Checkpoints are also created twice a day and the server can be rolled back to one of the checkpoints for disaster recovery.

TOE Security Functional Requirements Satisfied: FDP_ACC.2(1), FDP_ACC.2(2), FDP_ACF.1(1), FDP_ACF.1(2), FDP_ETC.1, FDP_ITC.1, FDP_ITT.1, FDP_SDI.2(1), FDP_SDI2.(2).

7.1.4 Identification and Authentication

The username, password, authentication type, domain, and role for each user are stored in the storage server on one of the storage nodes. Server-side users are required to identify and authenticate on the server prior to any action. Client-side users are allowed to backup data prior to authentication (they are identified with their Windows user ID through the backup request), but must identify and authenticate prior to any other action on the TOE. The TOE assigns a role to each user and only presents the user with functions allowed by their role.

Administrator and Operator roles access the TOE through the management interfaces on the server. The utility node's account management component authenticates users and binds the user's role to all operations the user performs. The User role is always assigned to a specific client and is constrained to that client. The User role cannot log into Avamar Administrator or directly access the utility node. Client-side authentication varies with the client platform. Users accessing the client side of the TOE through a CLI or the client web UI are required to login before all actions. Users on Windows or Mac platforms can access the client side of the TOE through the client web UI or through a tray in Windows or in the Menu on a Mac client. The desktop icon can only perform backups of that particular client system and the user does not have to authenticate prior to performing the backup. The client system does pass the user's UID to the server with the backup request so that the log entry can still be associated with the UID and the Client Access Control SFP is followed. Users must authenticate prior to performing restorations on the client-side.

The username is associated with a role and the role's permissions are used to determine access to data and permission to perform operations in the TOE. An authorized administrator can add users to the TOE and can change user attributes through the management interface.
TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1.

7.1.5 Security Management

Administrators have access to Avamar Administrator or the management CLI as the TOE management interfaces. The management interfaces access the MCS on the utility node to conduct all TOE management functions. All Avamar system configurations, including capacity management are done through these interfaces. Scheduled backups and restores are also normally done through these interfaces.

System configuration including:

- creating, modifying, and deleting domains
- adding, registering, and managing clients
- managing users and roles
- assigning users to clients and domains
- managing datasets, schedules, and retention policies
- managing events, notifications, and profile settings
- performing integrity checks

can only be accessed through the management interfaces by authorized administrators. System-level audit data can only be viewed by authorized administrators. Users are authorized read-only access to audit data within their assigned domain. Creation, deletion, and modification of users accounts is also limited to authorized administrators. The system roles are pre-defined and cannot be changed. Every user must be assigned a role and a domain. The possible server-side roles are:

- Root administrator – Top level domain access with full control of user data, schedules and policies, and system configuration within the Avamar system.
- Domain administrator – Full control of user data and schedules and policies within the assigned domain and lower. No access to global features, cannot add or edit other administrators, cannot change their role.
- Operator role – limited access to perform backups and restores

- Restore only operator – only allowed to perform and monitor restores for assigned domain
- Backup only operator – only allowed to perform and monitor backups for assigned domain
- Backup/restore operator – allowed to perform and monitor backups and restores for assigned domains
- Activity operator – only allowed to monitor backup and restore activities and create certain reports

These following are the client-side Users roles:

- Back up only user – can initiate backups directly from client using *avtar* command
- Restore (read) only user – can initiate restores directly from client using *avtar*
- Backup/restore user – can initiate backups and restores using *avtar*
- Restore (read) only/ ignore file permissions – Only available with external authentication. Similar to restore only, but OS file permissions are ignored during the restore, allowing the user to restore any file stored for their assigned client. The backup retains the OS file permissions.

User roles are created by an authorized administrator such as the Root and Domain administrators, using Avamar Administrator. The user role is selected from a drop down menu with the permissive default value for the menu being Administrator, creating a domain administrator for the current domain. An administrator can change the role through the menu. Administrators are assigned a domain and can only control backups and restores for their assigned domain. Users are assigned to a client system and can only access data originating from that client or audit data related to that client system. The default value for a new client-side user is Backup/restore user. Some management functions require access to the server OS. The TOE has default user accounts for this access.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.6 Protection of the TSF

The nodes within the server are connected via a dedicated Ethernet connection. This private back-end network is only used for internal TOE communications and ensures the internal protection of TSF data. The TOE can protect user data by replicating all user data to another instance of the TOE.

The TOE synchronizes with an external network time protocol (NTP) server to maintain the OS system clock. Port 123 is used for this communication.

TOE Security Functional Requirements Satisfied: FPT_ITT.1, FPT_STM.1.

8 Rationale

8.1 Conformance Claims Rationale

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

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

Table 17 below provides a mapping of the objects to the threats they counter.

Table 17 Threats:Objectives Mapping

Threats	Objectives	Rationale
T.MASQUERADE A user may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN mitigates this threat by ensuring that only authorized TOE users can manage TOE functions and data.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	By ensuring that the TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data, O.AUTHENTICATE satisfies this threat.
T.TAMPERING A user may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, associate users with events, and provide the authorized administrators with the ability to review the audit trail.	The objective O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded.
	O.ADMIN The TOE must include a set of functions that allow efficient	O.ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure

Threats	Objectives	Rationale
	management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	the TOE security mechanisms.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data. The TOE must ensure the integrity of user data by monitoring the integrity of stored data and enforcing access policies on transferred data.	O.PROTECT mitigates this threat by providing mechanisms to protect TOE data from unauthorized modification.
	O.TIMESTAMP The TOE will provide reliable time stamps.	The objective O.TIMESTAMP ensures that the TOE time cannot be altered in order to bypass TOE security.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE is protected from external interference or tampering.
T.UNAUTH A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, associate users with events, and provide the authorized administrators with the ability to review the audit trail.	The objective O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	The objective O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to	The objective O.AUTHENTICATE ensures that users are identified and

Threats	Objectives	Rationale
	allowing access to TOE administrative functions and data.	authenticated prior to gaining access to TOE security data.
T.FAILED DISK A disk failure could occur because of improper configuration of the TOE by an authorized administrator.	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data. The TOE must ensure the integrity of user data by monitoring the integrity of stored data and enforcing access policies on transferred data.	O.PROTECT mitigates this threat by requiring the TOE to ensure the integrity of user data.
	O.DATA OPTIMIZATION The TOE must identify and remove duplicate user data prior to storage and/or movement across the network and ensure that adequate storage space is available.	O.DATA OPTIMIZATION ensures that duplicated data is not transferred or stored, decreasing the likelihood of TOE overload. Also ensures adequate disk space is available.

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no organizational security policies defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 18 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 18 Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and client operating system.	OE.PLATFORM The TOE hardware and client OS must support all required TOE functions.	OE.PLATFORM ensures that the TOE hardware and OS supports the TOE functions.
	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. OE.MANAGE satisfies this assumption.
	OE.PHYSICAL The physical environment must be suitable for supporting a	OE.PHYSICAL satisfies this assumption by providing a physical environment that is suitable for

Assumptions	Objectives	Rationale
	computing device in a secure setting.	the TOE.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the hardware environment provides reliable timestamps to the TOE OS.
A.LOCATE The TOE is located within a controlled access facility.	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	Physical security is provided within the TOE environment to provide appropriate protection to network resources. OE.PHYSICAL satisfies this assumption.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.
A.I&A The operational environment will provide identification and authentication mechanisms when necessary for use of TOE.	OE.I&A The TOE environment must provide identification and authentication mechanisms if required for user access to TOE.	OE.I&A upholds this assumption by ensuring that the operational enviroment will provide mechanisms for users to be authenticated to the server before performing operations on data stored within the TOE.
A.SCONNECT The operational environment will protect client and remote management sessions with the TOE.	OE.SCONNECT The TOE environment must provide a secure connection for client systems and remote administrators to access the TOE.	OE.SCONNCET satisfies the assumption that client and remote administrator connection are secure by the operational environment providing a secure connection.

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

8.3 Rationale for Extended Security Functional Requirements

A family of User Data Deduplication requirements was created to specifically address the TOE's ability to identify duplicate segments of data and ensure that only original data is transferred and stored within the TOE. The purpose of this family of requirements is to define the deduplication process. These requirements have no dependencies since the stated requirements embody all the necessary security functions. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Security Requirements Rationale

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

8.4.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 19 below shows a mapping of the objectives and the SFRs that support them.

Table 19 Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, associate users with events, and provide the authorized administrators with the ability to review the audit trail.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User identity association	The requirement meets the objective by associating each auditable event with the identity of the user who caused the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensure that the TOE provides the ability to review logs.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by preventing unauthorized modification of the audit trail.
	FAU_STG.3 Action in case of possible audit data loss	The requirement meets the objective by storing old log files for later review by an authorized administrator.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by providing a record of security related events for administrators.
	FAU_GEN.2 User identity association	The requirement meets the objective by ensuring

Objective	Requirements Addressing the Objective	Rationale
those TOE users, may exercise such control.		administrators can determine the user responsible for each event.
	FAU_SAR.2 Restricted audit review	The requirement meets the objective by ensuring that TOE users may not access the audit records unless they are granted appropriate privileges.
	FAU_STG.3 Action in case of possible audit data loss	The requirement meets the objective by storing log files for authorized administrator to view to maintain the TOE.
	FDP_ACC.2(1) Complete access control (server)	The requirement meets the objective by defining server access control rules that administrators can use to protect data.
	FDP_ACC.2(2) Complete access control (client)	The requirement meets the objective by defining client access control rules that administrators can use to protect data.
	FIA_ATD.1 User attribute definition	The requirement meets the objective by defining the security attributes that an administrator can manage for each user.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control. O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE restricts system configuration and audit data changes to only those users with the appropriate privileges.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE restricts changes to the access policies only those users with the appropriate privileges.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by allowing only authorized administrators to change attributes from the default values.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by defining the management functions for the TOE.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles

Objective	Requirements Addressing the Objective	Rationale
		to provide access to TSF management functions and data.
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_ATD.1 User attribute definition	The requirement meets the objective by defining the security attributes that the TOE must maintain for each user.
	FIA_UAU.1 Timing of authentication (client)	The requirement meets the objective by requiring users to authenticate with the TOE prior to performing any action except a backup from the client side of the TOE.
	FIA_UAU.2 User authentication before any action (server)	The requirement meets the objective by ensuring that users are authenticated before access to TOE administrative functions is allowed.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that users are identified before access to TOE administrative functions is allowed.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing access to administrative functions to ensure that only those trusted users may manage the security behaviour of the TOE.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.
O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data. The TOE must ensure the integrity of user data by monitoring the integrity of stored data and enforcing access policies on transferred data.	FAU_SAR.2 Restricted audit review	Prohibits access to audit records unless explicitly authorized. This meets the objective by protecting the audit data from unauthorized modification.
	FDP_ACC.2(1) Complete access control (server)	The requirement meets the objective by defining server access control for all objects on the server.
	FDP_ACC.2(2) Complete access control (client)	The requirement meets the objective by defining the access control policy for the client-side of the TOE.

Objective	Requirements Addressing the Objective	Rationale
	FDP_ACF.1(1) Security attribute based access control (server)	The requirement meets the objective by requiring the TOE to enforce the server access policy and defining the security attributes and rules associated with the policy.
	FDP_ACF.1(2) Security attribute based access control (client)	The requirement meets the objective by requiring the TOE to enforce the client access policy and defining the security attributes and rules associated with the policy.
	FDP_ETC.1 Export of user data without security attributes	The requirement meets the objective by requiring the TOE to enforce the Server Access Control policy when exporting user data.
	FDP_ITC.1 Import of user data without security attributes	The requirement meets the objective by requiring the TOE to enforce the Server Access Control policy when importing user data.
	FDP_ITT.1 Basic internal transfer protection	The requirement meets the objective by requiring the TOE to enforce the Server Access Control policy for transmissions between nodes.
	FDP_SDI.2(1) Stored data integrity monitoring and action(multi-node)	The requirement meets the objective by monitoring stored user data for integrity errors and reconstructing data found to be in error in the multi-node configuration.
	FDP_SDI.2(2) Stored data integrity monitoring and action (single-node)	The requirement meets the objective by monitoring stored user data for integrity errors and reconstructing data found to be in error in the single-node configuration.
	FIA_UAU.1 Timing of authentication (client)	The requirement meets the objective by ensuring that only authorized users can access the backed up data on the TOE.
	FIA_UAU.2 User authentication before any action (server)	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The

Objective	Requirements Addressing the Objective	Rationale
		TOE does this by ensuring that only authenticated users are allowed access to TOE server functions.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only identified users are allowed access to TOE functions.
	FIA_USB.1 User-subject binding	The requirement meets the objective by associating each user with a role and only presenting the user with operations for which the role has permissions.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only privileged users may manage the security behaviour of the TOE.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE protects the access policies from unauthorized modification. The TOE does this by ensuring that only privileged users may manage the access policies of the TOE.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by requiring the TSF to enforce the Server Access Control and Client Access Control SFPs and allow only an authorized administrator to override default security attribute values.
O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data. The TOE must ensure the integrity of user data by monitoring the integrity of stored	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authorized users have access to TSF data.
	FPT_ITT.1	The requirement meets the

Objective	Requirements Addressing the Objective	Rationale
data and enforcing access policies on transferred data.	Basic internal TSF data transfer protection	objective by ensuring the integrity of data transmitted between separate parts of the TOE.
O.DATA OPTIMIZATION The TOE must identify and remove duplicate user data prior to storage and/or movement across the network and ensure that adequate storage space is available.	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1 meets the objective by allowing authorized administrators to configure the TOE to ensure data overload does not occur.
	EXT_FDD_DDR.1 Duplicate data removal	The requirement meets this objective by checking user data against previously stored data segments and removing duplicates prior to moving or storing the data.
O.TIMESTAMP The TOE will provide reliable time stamps.	FAU_GEN.1 Audit Data Generation	The requirement meets the objective by providing a reliable timestamp for all audit records.
	FPT_STM.1 Reliable time stamps	The requirement meets the objective by providing a reliable timestamp for TOE components.

8.4.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.4.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 20 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 20 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	No	Although FIA_UID.1 is not included for the server-side, FIA_UID.2, which is hierarchical to FIA_UID.1 is included.

SFR ID	Dependencies	Dependency Met	Rationale
			This satisfies this dependency.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.3	FAU_STG.1	✓	
FDP_ACC.2(1)	FDP_ACF.1(1)	✓	
FDP_ACC.2(2)	FDP_ACF.1(2)	✓	
FDP_ACF.1(1)	FMT_MSA.3	✓	
	FDP_ACC.1(1)	No	Although FDP_ACC.1 is not included, FDP_ACC.2, which is hierarchical to FDP_ACC.1 is included. This satisfies this dependency.
FDP_ACF.1(2)	FMT_MSA.3	✓	
	FDP_ACC.1(2)	No	Although FDP_ACC.1 is not included, FDP_ACC.2, which is hierarchical to FDP_ACC.1 is included. This satisfies this dependency.
FDP_ETC.1	FDP_ACC.1	No	Although FDP_ACC.1 is not included, FDP_ACC.2, which is hierarchical to FDP_ACC.1 is included. This satisfies this dependency.
FDP_ITC.1	FDP_ACC.1	No	Although FDP_ACC.1 is not included for the server-side, FDP_ACC.2, which is hierarchical to FDP_ACC.1 is included. This satisfies this dependency.
	FMT_MSA.3	✓	
FDP_ITT.1	FDP_ACC.1	No	Although FDP_ACC.1 is not included, FDP_ACC.2, which is hierarchical to FDP_ACC.1 is included.

SFR ID	Dependencies	Dependency Met	Rationale
			This satisfies this dependency.
FDP_SDI.2(1)	No dependencies	✓	
FDP_SDI.2(2)	No dependencies	✓	
FIA_ATD.1	No dependencies	✓	
FIA_UAU.1	FIA_UID.1	No	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UAU.2	FIA_UID.1	No	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies	✓	
FIA_USB.1	FIA_ATD.1	✓	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_ACC.1	No	Although FDP_ACC.1 is not included, FDP_ACC.2, which is hierarchical to FDP_ACC.1 is included. This satisfies this dependency.
FMT_MSA.3	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	No	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.

SFR ID	Dependencies	Dependency Met	Rationale
FPT_ITT.1	No dependencies	✓	
FPT_STM.1	No dependencies	✓	
EXT_FDD_DDR.1	No dependencies	✓	

9 Acronyms and Terms

This section and Table 21 define the acronyms and terms used throughout this document.

9.1 Acronyms and Terms

Table 21 Acronyms and Terms

Acronym	Definition
ACL	Access Control List
AIX	Advanced Interactive eXecutive
CC	Common Criteria
CID	Client Identification
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
Gb	Gigabit
GB	Gigabyte
GHz	Gigahertz
GUI	Graphic User Interface
HP-UX	Hewlett Packard UniX
IBM	International Business Machines
ID	Identification
IT	Information Technology
JFS	Journaled File System
JVM	Java Virtual Machine
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
MCS	Java Management Console Service
MOSS	Microsoft Office Sharepoint Server
NAS	Network Attached Storage
NDMP	Network Data Management Protocol
NIS	Network Information Service
NTP	Network Time Protocol

Acronym	Definition
OS	Operating System
OSP	Organizational Security Policy
PAM	Pluggable Authentication Module
PP	Protection Profile
RAID	Redundant Array of Independent Disks
RAIN	Redundant Array of Independent Nodes
RAM	Random Access Memory
RHEL	Red Hat Enterprise Linux
RMI	Remote Method Invocation
SAR	Security Assurance Requirement
SCO	Santa Cruz Operation
SFP	Security Functional Policy
SFR	Security Functional Requirement
SLES	Suse Linux Enterprise Server
SQL	Structured Query Language
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
UI	User Interface
VSS	Volume Snapshot Service
WAN	Wide Area Network

Prepared by:
Corsec Security, Inc.

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

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