EMC Corporation
EMC® ProSphere™ v2.0

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.7

Prepared for:

EMC²
where information lives®

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

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

Prepared by:

Corsec®

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
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 TOE is the EMC® ProSphere™ v2.0, and will hereafter be referred to as the TOE throughout this document. The TOE is an integrated family of software components that provide storage environment monitoring and management.

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 ProSphere™ v2.0 Security Target
ST Version	Version 0.7
ST Author	Corsec Security, Inc.
ST Publication Date	5/1/2013
TOE Reference	EMC® ProSphere™ v2.0 build 106

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.

ProSphere gives an enterprise-level view of an organization's data center. It enables administrators to discover, monitor, and report on all storage related resources across the entire information environment from a single workstation. ProSphere also allows administrators to monitor capacity utilization of the environment, measure application performance, be notified of conditions that require attention, and ensure storage environment compliance to the company's or EMC's best practices. ProSphere is deployed as a collection of interdependent virtual machines (VM) configured at the VM and virtual application (vApp) level. The three VMs that constitute the core of ProSphere are:

- Discovery Engine – Discovers managed resources in a data center and periodically refreshes data collected for these resources according to user-defined policies. Multiple instances can be used to increase scalability.
- Historical Database – Manages the storage of collected resource data, historical performance, capacity data, compliance and configuration change information, alert history, configuration parameters, and other data that requires persistence. The Historical Database hosts a Relational Database Management System (RDBMS). This data is used to populate dashboards and performance charts in the web graphical user interface (GUI).
- ProSphere Application – Hosts the web server that provides access to the web GUI and associated applications on the management workstation. The ProSphere Application includes application security, configuration, resource searching, and a distributed information cache for data access. Topology and configuration data collected from the discovered resources is stored in the ProSphere Appication's Resource Description Framework (RDF) database.

ProSphere shows a consolidated view of the storage environment. This view allows administrators to monitor the health of, track the status of, report on, and control each managed resource. From a single workstation, ProSphere can manage or monitor:

- Storage components – such as EMC Symmetrix®, CLARiiON®, and VNX™ arrays.
- Connectivity components – such as Fibre Channel switches and hubs.
- Host components – such as host operating systems, and file systems.

ProSphere pulls data from managed resources using multiple different protocols and presents them through simple Representational State Transfer (REST) API[1]s to Storage Area Network (SAN) administrators. The data comes from multiple sources, such as element managers, device management interfaces, and customers. ProSphere collects, aggregates, and normalizes this data so that it becomes easily accessible to users through the REST API which can be accessed by third-party applications or by the ProSphere GUI. The aggregated data is an up-to-date representation of a SAN and the Information Technology (IT) resources utilizing the SAN resources.

In a typical deployment scenario, a variety of application servers and SAN devices are connected to the ProSphere infrastructure via IP[2] networking or Fibre Channel. SAN or Storage administrators utilize the ProSphere product to manage and monitor these various SAN devices. ProSphere collects key configuration information on data center assets and monitors the SAN elements and fabrics for configuration changes and performance.

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.

[1] API- Application Programming Interface
[2] IP – Internet Protocol

The TOE performs storage resource management in a virtualized environment. The TOE connects through the established SAN and discovers resources attached to the network using standard protocols such as Storage Management Initiative – Specification (SMI-S), Simple Network Management Protocol (SNMP), Secure Shell (SSH), Windows Management Instrumentation (WMI), Web Service Management (WS-MAN) and VMware API. The Discovery Engine then pulls configuration and performance data from each discovered resource. SAN resource configurations are saved in the ProSphere Application's RDF database. Users can establish performance thresholds that trigger alerts when a performance threshold is exceeded. Users can also be notified when their environment is no longer in compliance with best practices due to configuration changes. The ProSphere Application serves discovered data to authorized users through the web GUI.

Administrators can name resources and place them into resource groups. Information imported into the TOE from the managed resources are assigned the resource name. Users are assigned to one of three pre-defined roles within the TOE. The user's role determines their level of access.

Figure 1 shows the details of the deployment configuration of the TOE and contain the following previously undefined acronyms:

- NTP – Network Time Protocol
- SLES – SUSE Linux Enterprise Server
- LDAP – Lightweight Directory Access Protocol

–

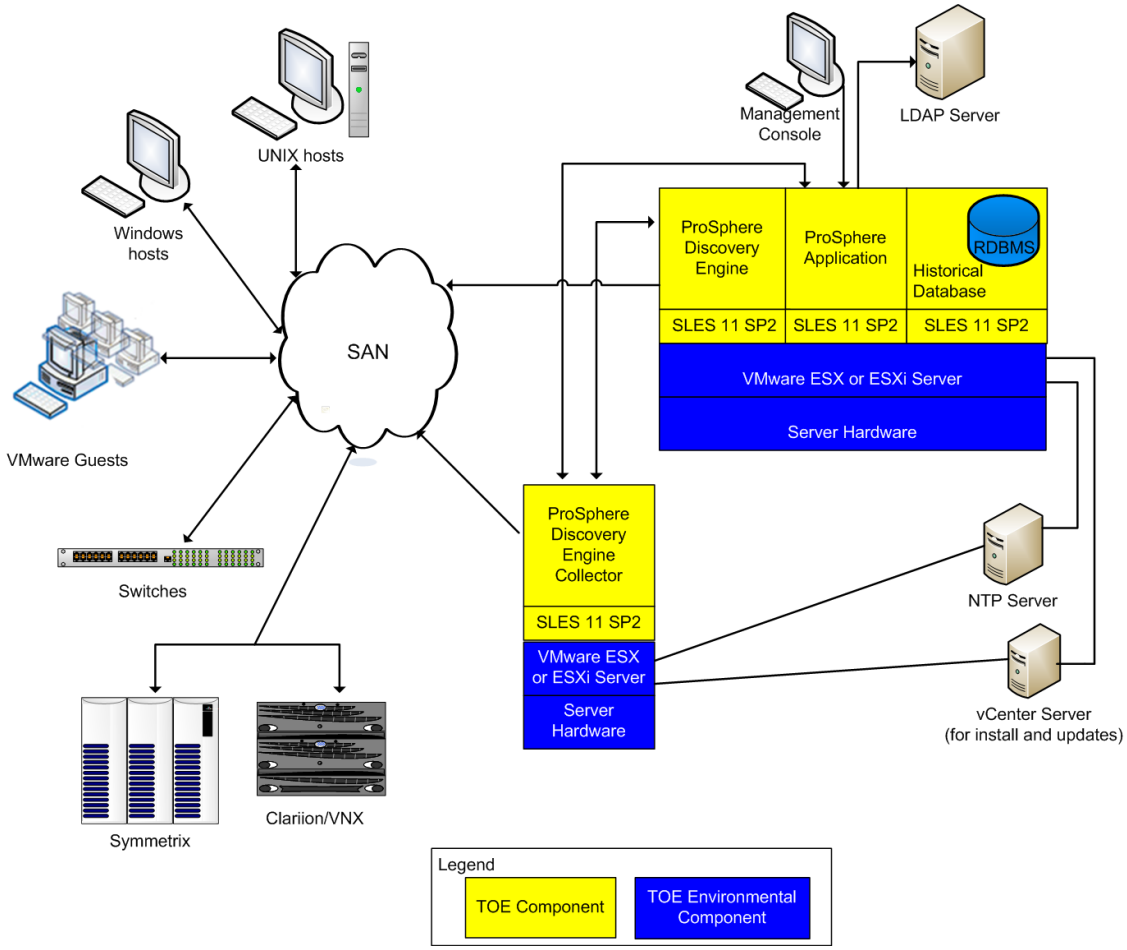

Figure 1 Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

ProSphere comprises four virtual machines:

- ProSphere Discovery Engine – Discovers managed resources in a data center and maintains data collected for these resources according to user-defined policies using a variety of network protocols and standards-based interfaces to collect data from SAN devices such as hosts, storage arrays, and switches. The Discovery Engine provides load balancing and management capabilities for any additional Discovery Engine Collectors. The is the ProSphere Discovery System Disk virtual machine file name that contains the ProSphere Discovery Engine and its SLES 11 SP2 OS.
- ProSphere Discovery Engine Collector – An optional component for increased scalability. Multiple instances of the ProSphere Discovery Engine Collector can be used together to collect data from managed resources. Since the ProSphere Discovery Engine Collector can be deployed separately two software components are required:
    - ProSphere Discovery Engine Collector Appliance – This file contains the VM setup and configuration for this VM.
    - ProSphere Discovery Engine Collector System Disk – This file contains the ProSphere Discovery Engine Collector and its SLES 11 SP2 OS.
- Historical Database – Manages the storage of collected resource data, historical performance data, historical capacity data, historical alert data, compliance information, configuration parameters, and any other data that requires persistence. The Historical Database VM requires two software components for additional storage:
    - ProSphere Historical Database System Disk – This file contains the Historical Database Appliance and its SLES 11 SP2 OS.
    - ProSphere Historical Database Data Disk – This file contains an interface for an expandable disk for data storage.
- ProSphere Application – Hosts the web server and other services that provide access to the management workstation and its applications. Provides connectivity for any applications that interact with ProSphere.. The ProSphere Appliacation VM requires two software components for additional storage:
    - ProSphere Application System Disk – This file contains the ProSphere Application and its SLES 11 SP2 OS.
    - ProSphere Application Data Disk – This file contains an interface for an expandable disk for data storage.

The ProSphere vApp is required to install the four VMs and includes the VM setup and configuration for the ProSphere Application, Discovery Engine, and Historical Database VMs.

1.4.2 TOE Environment

ProSphere is deployed as a vApp and therefore requires VMware and host system hardware. Table 2 specifies the minimum system requirements for the proper operation of the TOE.

Table 2 TOE Minimum Requirements

Category	Requirement
VMware	vSphere 4.0 or later virtualized computing environment for installation and updates ESX or ESXi server version 4.0 or later running the vSphere environment

Category	Requirement
Network Time Protocol (NTP) server	All ESX or ESXi servers must be synchronized with an NTP server
Management Workstation	General purpose CPU[3] with a web browser that supports Adobe flash
Virtual Hardware	ProSphere Application: 4 x 64-bit CPUs, 8GB[4] RAM[5], 230 GB Storage ProSphere Discovery Engine: 4 x 64-bit CPUs, 8 GB RAM, 40 GB Storage ProSphere Discovery Colletor: 4 x 64-bit CPUs, 8 GB RAM, 40 GB Storage Historical Database: 2 x 64-bit CPUs, 6 GB RAM, 230 GB Storage

The managed resources must meet the requirements in Table 3 to ensure successful discovery by the TOE.

Table 3 Managed Resources Minimum Requirements

Category	Requirement
Windows Hosts	Windows 2000 or later, Windows Server 2003 or later with WMI or WS-MAN installed All Host Bus Adapters (HBA) must include Storage Networking Industry Association (SNIA)-compliant libraries
Unix Hosts	Solaris 9 or higher, Red Hat Enterprise Linux AS/ES 4.0 or higher, and SUSE ES 9 or higher with iostat 5.0.5 IBM AIX6 5.1 or higher, HP-UX 11iv1, 11iv2: with sar All HBAs must including SNIA-complaint libraries
Arrays	Symmetrix DMX series or VMAX with Symmetrix Management Solution v7.3 or higher, CLARiiON AX or CX series, VNX storage devices Block Mode, and VMAXe series All arrays must have a host with SMI-S Provider 4.3.0.3 or higher installed connected to the array.
Switches	EMC Connectrix/Cisco MDS (SAN OS[7] 3.0 or higher, NX OS 4.1 or higher) EMC Connectrix/Brocade Fabric OS series with Brocade SMI Agent v120.10.0 or higher or Connectrix Manager Data Center Edition/Data

[3] CPU – Central Processing Unit
[4] GB – Gigabyte
[5] RAM – Random Access Memory
[6] AIX – Advanced Interactive eXecutive
[7] OS – Operating System

Category	Requirement
	Center Fabric Manager 10.4.0 or higher EMC Connectrix/Brocade M-Class with SMI Agent v2.7.0 or higher
VMware	ESX/ESXi 3.5 or later through vCenter or directly from the ESX/ESXi server

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

The TOE performs storage management and runs in a virtual environment compliant to the minimum software and hardware requirements as listed in Table 2 and Table 3. The TOE is installed in a data center SAN as depicted in the figure below. The essential software components for the proper operation of the TOE in the evaluated configuration are:

- ProSphere 2.0 vApp – VM setup and configurations for ProSphere Application, Discovery Engine, and Historical Database.
- ProSphere 2.0 Discovery System Disk – Discovery Engine VM.
- ProSphere 2.0 Historical Database System Disk – Historical Databse VM.
- ProSphere 2.0 Historical Database Data Disk – Additional data storage for Historical Database VM.
- ProSphere 2.0 ProSphere Application System Disk – ProSphere Application VM.
- ProSphere 2.0 ProSphere Application Data Disk – Additional data storage for ProSphere Application VM.
- ProSphere 2.0 Discovery Engine Collector System Disk – Discovery Engine Collector VM.
- ProSphere 2.0 Discovery Engine Collector Appliance – VM setup and configurations for ProSphere Discovery Engine Collector.

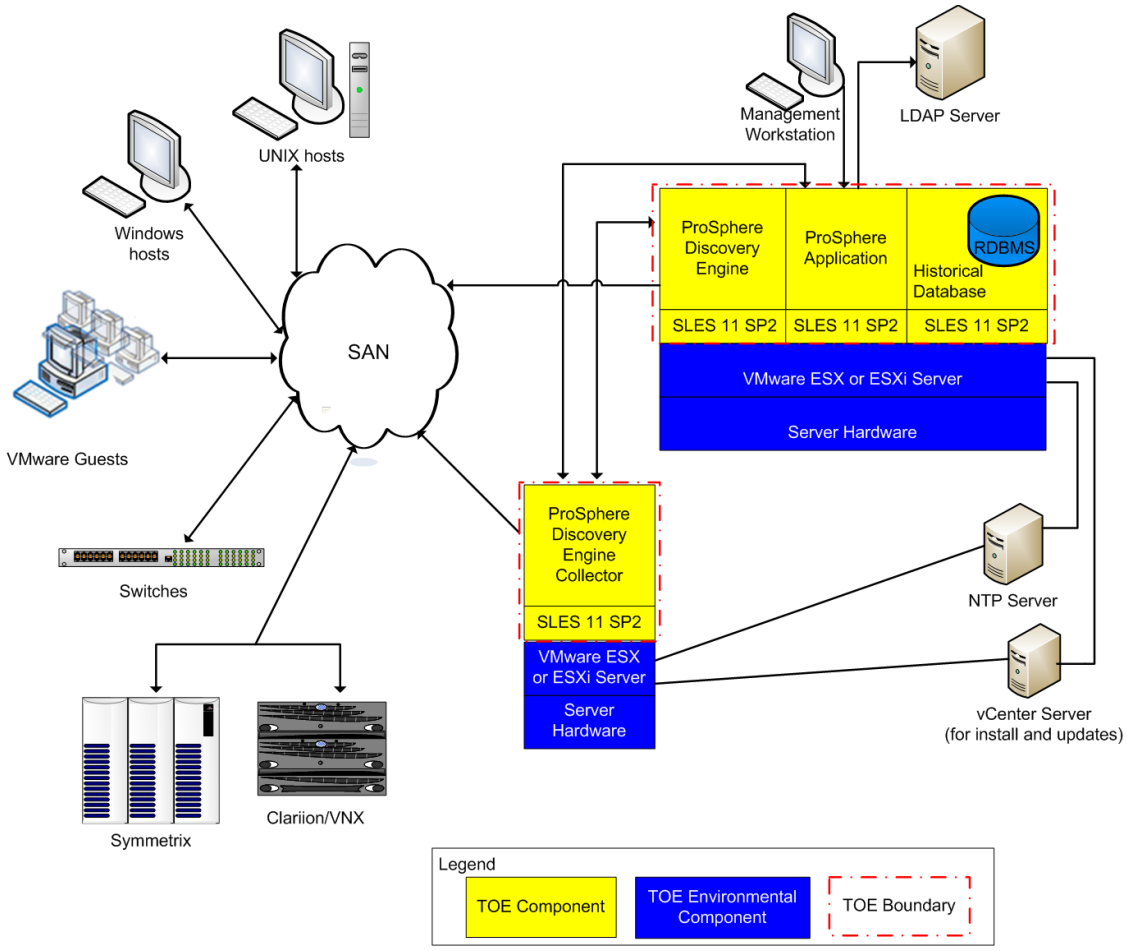

Figure 2 Physical TOE Boundary

1.5.1.1 TOE Software

The TOE is software only TOE that consists of a virtual application for SAN monitoring and management. The vApp consists of three or more separate VMs: ProSphere Discovery Engine, ProSphere Application, and ProSphere Historical Database with the option of an additional Discovery Engine Collector. Each VM includes SLES as the host operating system. The vApp can be deployed on a single VMware ESX or ESXi server, in an ESX cluster, or across multiple ESX or ESXi servers. The VMware and hardware on which the vApp is deployed are part of the TOE environment and require an NTP server for proper operation.

1.5.1.2 Guidance Documentation

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

- EMC ProSphere v2.0 Administrators Guide
- EMC ProSphere v2.0 Deployment Guide
- EMC ProSphere v2.0 Release Notes
- EMC ProSphere v2.0 Security Configuration Guide
- EMC ProSphere v2.0 RestAPI
- EMC Prosphere v2.0 Guidance Documentation Supplement, v0.1, 1 May 2013

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 Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Function (TSF)
- TOE Access

1.5.2.1 Security Audit

The TOE generates log files by service to record audit events. The audit logs are stored in internal files specific to each VM and can be viewed by retrieving all auditable events from within the ProSphere Application's web GUI through an embedded search window, or by using a secure REST API call. The files are protected by Access Control Lists (ACLs) maintained by the SLES OS so that they cannot be modified or deleted. The audit records contain a timestamp and user identity if the action was initiated by a user. Start-up and shutdown of audit functions, user management, configuration of discovery jobs, and changes to the TOE configuration are audited.

1.5.2.2 User Data Protection

The Access Control Security Funtional Policy (SFP) determines who can access a managed resource's configuration and performance data after it is imported into the TOE. Authorized administrators create discovery jobs and link them to access profiles. These discovery jobs initiate discovery of managed resources and allow resource configuration, capacity, and performance data to be imported into the TOE. The data is not imported with its security attributes, but follows the Access Control SFP that allows all authorized administrators to view, modify, and delete the data.

1.5.2.3 Identification and Authentication

Users can identify and authenticate to a local database that stores usernames and the roles associated with each user. Identification and authentication can also be performed through an external Lightweight Directory Access Protocol (LDAP) server. Users must identify and authenticate with a valid username and password on the management workstation before accessing any TOE functionality. The management workstation passes this identification and authentication data to the ProSphere Application for verification with the attributes stored in the local database or on the LDAP server. Upon successful authentication the user is assigned a role with its associated permissions. Passwords are obscured during entry.

1.5.2.4 Security Management

The TOE is managed through the management workstation which connects to the ProSphere Application through REST APIs or a web GUI; both interfaces require an HTTPS connection. ProSphere maintains three roles: Security Administrator, System Administrator, and User. All roles are SAN administrators and will be referred to as authorized administrators. The TSF restricts all user management functions to the Security Administrator, including creating, managing, assigning a role, disabling user accounts, and configuring LDAP authentication. By default, all users are created with the role User. Only the Security Administrator can change a user to a different role. All authorized administrators can create discovery jobs that determine what resources are discovered. Discovered resource configuration, capacity, and performance data is stored in the TOE and can be viewed, modified, and deleted by authorized administrators. System configuration and audit is restricted to Security Administrators and System Administrators. Both administrator roles and authorized users can discover resources and assign resource object names and resource groups.

1.5.2.5 Protection of the TSF

The TOE operating system (SLES) is responsible for providing the time stamps used by each of the four (4) virtual machines. The time stamps must be synchronized between all the TOE's virtual machines for proper functionality of the TOE. The underlying ESX(i) server must be synchronized with an external NTP server to ensure the timestamps are synchronized across each virtual machine installed upon the ESX(i) server.

1.5.2.6 TOE Access

TOE sessions timeout after 30 minutes of inactivity and users are required to reauthenticate to regain access. The TSF also provides a configurable advisory message prior to session establishment warning users of unauthorized use of the TOE.

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

There are no features/functionality that are excluded from the evaluated configuration of the TOE.

2 Conformance Claims

This section and Table 4 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 4 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 conformant; CC Part 3 conformant; no PP claim; Parts 2 and 3 Interpretations of the CEM as of 2012/02/13 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2 augmented (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 encountered 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 assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE. Attackers are referred to as an unauthorized individual in the below threats.
- 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.

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF 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 5 below lists the applicable threats.

Table 5 Threats

Name	Description
T.COMINT	An unauthorized individual may attempt to compromise the integrity of the audit data collected and produced by the TOE or TOE configuration data by bypassing a security mechanism.
T.PRIVIL	A user may gain access to TOE security functions and data without authorization by exploiting system privileges.

3.2 Organizational Security Policies

There are no Organizational Security Policies for this evaluation.

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 6 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 6 Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate hypervisor and hardware.
A.LOCATE	The TOE is located within a controlled access facility.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

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 7 below.

Table 7 Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate functions and data.
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.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, and provide the authorized administrators with the ability to review the audit trail.
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 protect itself from unauthorized modifications and access to its functions, audit data, and configuration data.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 8 below lists the IT security objectives that are to be satisfied by the environment.

Table 8 IT Security Objectives

Name	Description
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.PLATFORM	The TOE hypervisor and hardware must support all required TOE functions.

4.2.2 Non-IT Security Objectives

Table 9 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 9 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

There are no extended TOE Security Functional Components for this evaluation.

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components for this evaluation.

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(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) 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 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based control		✓		
FDP_ITC.1	Import of user data without security attributes		✓		
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	User authentication before any action				
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3(1)	Static attribute initialisation (user)	✓	✓	✓	✓

Name	Description	S	A	R	I
FMT_MSA.3(2)	Static attribute initialisation (object)	✓	✓	✓	✓
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_STM.1	Reliable time stamps				
FTA_SSL.3	TSF-initiated termination		✓		
FTA_TAB.1	Default TOE access banner				

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:

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

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

c) [*user account management, and configuration of discovery jobs and TOE configuration changes*].

FAU_GEN.1.2

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*thread id, log level, application name, component name, and subcomponent name (if applicable*)].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*authorised users*] 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_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

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1
The TSF shall enforce the [*Access Control SFP*] on
[*Subjects: Users, System Administrators, and Security Administrators,*
Objects: stored data from managed resources
Operations: viewing, modifying, and deleting].
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
FDP_ACF.1.1
The TSF shall enforce the [*Access Control SFP*] to objects based on the following:
[*Subjects: TOE users, System Administrators, and Security Administrators*
Attributes: username and role
Objects: stored resource data
Attributes: resource object name, resource type, and IP address].
FDP_ACF.1.2
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*authorized administrators can view, modify, and delete stored data from discovered resources*].
FDP_ACF.1.3
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].
FDP_ACF.1.4
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ITC.1 Import of user data without security attributes
Hierarchical to: No other components.
FDP_ITC.1.1
The TSF shall enforce the [*Access Control SFP*] when importing user data, controlled under the SFP, from outside 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: [*no additional rules*].
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

6.2.4 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 and role*].
Dependencies: No dependencies

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

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
FIA_UAU.7.1
The TSF shall provide only [*asterisks*] to the user while authentication is in progress.
Dependencies: FIA_UAU.1 Timing of authentication

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

6.2.5 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 [*user accounts, system services, discovery jobs*] to [*authorised 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 [*Access Control SFP*] to restrict the ability to [modify, delete] the security attributes [*username and role*] to [*a Security Administrator*].
Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3(1) Static attribute initialisation(user)
Hierarchical to: No other components.
FMT_MSA.3.1
The TSF shall enforce the [*Access Control SFP*] to provide [restrictive] default values for **user** security attributes that are used to enforce the SFP.
FMT_MSA.3.2
The TSF shall allow the [*Security 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_MSA.3(2) Static attribute initialisation(object)
Hierarchical to: No other components.
FMT_MSA.3.1
The TSF shall enforce the [*Access Control SFP*] to provide [restrictive] default values for **object** security attributes that are used to enforce the SFP.
FMT_MSA.3.2
The TSF shall allow the [*authorized administrators*] 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 [query [*other operations as defined in column 'Operation' of Table 11*]] the [*TSF data as defined in column 'TSF Data' of Table 11*] to [*Roles as defined in "Roles of Table 11*].

Table 11 Management of TSF Data

Privilege	Security Administrator	System Administrator	User
Create and manage operators	Yes	No	No
Assign operator roles	Yes	No	No
Configure LDAP authentication	Yes	No	No
Modify system password	Yes	No	No
Monitor system services	Yes	Yes	Yes
Configure and manage data sources	Yes	Yes	No
View appliance settings	Yes	Yes	No
Update licenses	Yes	Yes	No
Create and manage discovery jobs	Yes	Yes	Yes
Search for objects	Yes	Yes	Yes
View objects in map	Yes	Yes	Yes
View object properties	Yes	Yes	Yes
Manage and view alerts	Yes	Yes	Yes
View audit logs, view audit log categories/components, Download audit logs, Edit audit log level	Yes	Yes	No
Export data for reproducing customer environment, Cancel export job, Delete exported data, Check export job status	Yes	Yes	No
Download exported data for reproducing customer environment use case	Yes	Yes	Yes
View Groups and group members, View members for given smart group criteria	Yes	Yes	Yes
Create/Edit/Delete Groups, add or remove members, Turning on/off performance collection on Group	Yes	Yes	No
Create, Edit, Delete, Reorder ServiceLevels/Definitions	No	Yes	No
View ServiceLevels and Definitions	Yes	Yes	Yes

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

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: [*security attribute management, TSF data management, and security function management*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles
Hierarchical to: No other components.
FMT_SMR.1.1
The TSF shall maintain the roles [*Security Administrator, System Administrator, and User*].
FMT_SMR.1.2
The TSF shall be able to associate users with roles.
Dependencies: FIA_UID.1 Timing of identification

6.2.6 Class FPT: Protection of TSF

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

6.2.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*30 minute interval of inactivity*].

Dependencies: No Dependencies

FTA_TAB.1 Default TOE access banner

Hierarchical to: No other components.

FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

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 12 Assurance Requirements summarizes the requirements.

Table 12 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 Flaw reporting procedures
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 13 lists the security functions and their associated SFRs.

Table 13 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based control
	FDP_ITC.1	Import of user data without security attributes
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3(1)	Static attribute initialisation (user)
	FMT_MSA.3(2)	Static attribute initialisation (object)
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TSF data	FPT_STM.1	Reliable time stamps
TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banner

7.1.1 Security Audit

The Security Audit function records manipulation of TOE user accounts, including their addition, deletion, or modification. The creation, updating, or deletion of discovery jobs, and changes to TOE configuration are also audited. Start-up and shutdown of the audit function is also audited.

The TOE audit records contain the following information:

Table 14 Audit Record Contents

Field	Content
Time	Time specified in the year-month-day hour-minute-second format.
Thread id	unique number that identifies the thread
log level	the level at which the log is currently set: • Trace • Debug • Info • Warn • Error
application name	Name of the ProSphere application that output the message
component name	Name of the managed component that output the message
subcomponent name	Name of the managed subcomponent that output the message (if applicable)
Message	Description of event including success or failure

The audit logs are stored in internal files specific to each application and can be viewed by retrieving all auditable events from within ProSphere web GUI through an embedded search window, or by using a secure REST API call. The files are protected by ACLs maintained by the SLES OS so that they cannot be modified or deleted.
TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_STG.1.

7.1.2 User Data Protection

The TOE enforces an Access Control SFP to manage access to data imported into and stored in the TOE from managed resources. All TOE users are SAN administrators, so authorized administrators to the TOE include the roles, User, System Administrator, and Security Administrator. Authorized administrators can view, modify, and delete all stored data from a discovered resource. Discovery jobs that include resource type and an IP address range are used to determine what resources are discovered. Resources must be discovered before the TOE can access, import, store, and present the resource's configuration, capacity, and performance data. Data imported into the TOE does not retain the security attributes from the managed resource. The resource is assigned a resource name that is associated with all data received from that resource and the resources IP address is also associated with the data.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_ITC.1.

7.1.3 Identification and Authentication

Users identify and authenticate to the web GUI and their identification and authentication data is passed to the ProSphere Application. The ProSphere Application maintains a local database that stores usernames, passwords, and the roles associated with each user or username and password can be passed to an external LDAP server for verification. Users must authenticate with a valid username and password to the web GUI before accessing any TOE functionality. The ProSphere Application stores and associates username and roles in the local database. Upon successful authentication the user is assigned a role with its associated permissions. Passwords are obscured when entered by astericks.
TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2.

7.1.4 Security Management

The TOE maintains three roles: Security Administrator, System Administrator, and User. All roles are SAN administrators and are collectively referred to as authorized administrators. The User role is restricted to creating discovery jobs and access profiles, viewing stored resource data, and viewing and managing alerts. Discovery jobs define the resource type that the TOE should search for and the IP address range to search. Resource types can be arrays, switches, fabrics, or hosts. Access profiles define the access protocol, which can be SMI-S, SNMP, SSH, WMI, WS-MAN, or VMware infrastructure and the required resource username and password. The access profiles are linked to the discovery jobs. Resource configuration and performance data will not be collected and stored in the TOE unless the resource attributes match a discovery job. Users cannot perform any system or security administrative functions.

The System Administrator can perform all User operations and can monitor and configure the TOE. Security Administrators can perform all operations allowed for the System Administrator and can manage users. The Security Administrator can create users, assign roles, modify, and delete users and configure LDAP authentication. Users are given the User role by default and only the Security Administrator can modify the role. Resource data is only imported into the TOE if the resource matches the attributes in a discovery job. An authorize administrator must create a discovery job with a resource type and IP address range that matches a resource in order for the resource to be discovered and it's data to be imported into and stored in the TOE.

The TSF restricts all user management and LDAP configuration functions to the Security Administrator, including creating, managing, assigning a role, and disabling user accounts. System configuration, other than LDAP configuration, is restricted to Security Administrators and System Administrators. Both administrator roles can create discovery jobs and assign resource object names and resource groups. Modification and deletion of objects names and resource groups is restricted to System or Security Administrators.
TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3(1), FMT_MSA.3(2), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of TSF

The TOE operating system (SLES) is responsible for providing the time stamps used by each of the four (4) virtual machines. The time stamps must be synchronized between all the TOE's virtual machines for proper functionality of the TOE. The underlying ESX(i) server must be synchronized with an external NTP server to ensure the timestamps are synchronized across each virtual machine installed upon the ESX(i) server..
TOE Security Functional Requirements Satisfied: FPT_STM.1

7.1.6 TOE Access

TOE session are terminated after 30 minutes of inactivity. Users are required to reauthenticate after a session timeout. The TSF provides an administrator configurable advisory message regarding unauthorized use of the TOE prior to user session establishment.

TOE Security Functional Requirements Satisfied: FTA_SSL.3, FTA_TAB.1

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, 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 15 below provides a mapping of the objects to the threats they counter.

Table 15 Threats:Objectives Mapping

Threats	Objectives	Rationale
T.COMINT An unauthorized individual may attempt to compromise the integrity of the audit data collected and produced by the TOE or TOE configuration data by bypassing a security mechanism.	O.ACCESS The TOE must allow authorized users to access only appropriate functions and data.	The O.ACCESS objective ensures that unauthorized modification and access to functions and data is prevented. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data.
	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, and provide the authorized administrators with the ability to review the audit trail.	O.AUDIT provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE.
	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.
	O.PROTECT The TOE must protect itself from unauthorized modifications and access to its functions, audit data, and configuration data.	O.PROTECT requires that the TOE protect itself from unauthorized modifications and access to its functions and data.

Threats	Objectives	Rationale
T.PRIVIL A user may gain access to TOE security functions and data without authorization by exploiting system privileges.	O.ACCESS The TOE must allow authorized users to access only appropriate functions and data.	O.ACCESS provides that the TOE must allow authorized operators to access only appropriate TOE functions and data.
	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 supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.
	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, 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.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	This threat is mitigated by O.AUTHENTICATE, which requires that the TOE must be identify and authenticate operators prior to allowing access to TOE functions and data.
	O.PROTECT The TOE must protect itself from unauthorized modifications and access to its functions, audit data, and configuration data.	O.PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification.
	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.

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 evaluation.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 16 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 16 Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate hypervisor and hardware.	OE.PLATFORM The TOE hypervisor and hardware must support all required TOE functions.	OE.PLATFORM ensures that the TOE hypervisor and hardware support 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.
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 the network resources. OE.PHYSICAL satisfies this assumption.
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.

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

No extended security functional requirements have been defined for this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

No extended security assurance requirements have been defined for this ST.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 17 below shows a mapping of the objectives and the SFRs that support them.

Table 17 Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must allow authorized users to access only appropriate functions and data.	FDP_ACC.1 Subset access control	FDP_ACC.1 meets this objective by defining the subjects, objects, and operations controlled by the Access Control SFP.
	FDP_ACF.1 Security attribute based control	FDP_ACF.1 meets this objective by defining the access rules that the TSF enforces for the Access Control SFP.
	FDP_ITC.1 Import of user data without security attributes	The requirement meets the objective by requiring data imported into the TOE to use follow the access control SFP.
	FIA_UAU.2 User authentication before any action	The TOE will not give any security sensitive access to a user until the user has authenticated.
	FIA_UID.2 User identification before any action	The TOE will not give any security sensitive access to a user until the user has identified.
	FMT_MOF.1 Management of security functions behaviour	The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE.
	FMT_MSA.3(1) Static attribute initialisation (user)	Restrictive values for user attributes are provided and only an authorized administrator can change these values.
	FMT_MSA.3(2) Static attribute initialisation (object)	Permissive default values are provided for object attributes and only authorized administrators are allowed to change these values.
	FTA_SSL.3 TSF-initiated termination	The requirement meets the objective by terminating inactive

Objective	Requirements Addressing the Objective	Rationale
		sessions after 30 minutes.
	FTA_TAB.1 Default TOE access banner	The requirement meets the objective by warning user's against unauthorized use of the TOE prior to authentication.
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 administrative functions to only those users with the appropriate privileges.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the user's role.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
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, 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_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 ensuring that the TOE protects the audit data from unauthorized deletion.
	FMT_MSA.1 Management of security attributes	Only authorized users of the system may query and modify TOE data.
	FMT_MTD.1 Management of TSF data	Only authorized users of the system may query and view audit data.
	FPT_STM.1 Reliable time stamps	The requirement supports the objective by providing a reliable

Objective	Requirements Addressing the Objective	Rationale
		time stamp for audit records.
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	Security attributes of subjects used to enforce the authentication policy of the TOE must be defined.
	FIA_UAU.2 User authentication before any action	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 the users are identified before access to TOE administrative functions is allowed.
	FMT_SMR.1 Security roles	The TOE must be able to recognize the different user roles that exist for the TOE.
O.PROTECT The TOE must protect itself from unauthorized modifications and access to its functions, audit data, and configuration data.	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that no one may delete or alter information in the audit logs.
	FIA_UAU.2 User authentication 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 authenticated users are allowed access to TOE functions.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by obscuring passwords during authentication, keeping unauthorized users from viewing passwords and obtaining unauthorized access.
	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.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE protects itself from

Objective	Requirements Addressing the Objective	Rationale
		unauthorized modification. The TOE does this by ensuring that only privileged users may manage the security behaviour of the TOE.
	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.
	FTA_SSL.3 TSF-initiated termination	The requirement meets the objective by terminating inactive sessions after 30 minutes. This protects the TOE from an unauthorized user taking over an authorized user's session.

8.5.2 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. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended 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, including flaw reporting procedures.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria. Table 18 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 18 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_ITC.1	FDP_ACF.1	✓	
	FMT_MSA.3(1)	✓	
	FMT_MSA.3(2)	✓	
FIA_ATD.1	No dependencies	n/a	
FIA_UAU.2	FIA_UID.1	✓	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.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies	n/a	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1	✓	
FMT_MSA.3(1)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	n/a	
FMT_SMR.1	FIA_UID.1	✓	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_STM.1	No dependencies	n/a	
FTA_SSL.3	No dependencies	n/a	
FTA_TAB.1	No dependencies	n/a	

9 Acronyms and Terms

This section and Table 19 define the acronyms and terms used throughout this document.

9.1 Acronyms

Table 19 Acronyms

Acronym	Definition
ANSI	American National Standards Institute
API	Application Programming Interface
CC	Common Criteria
CM	Configuration Management
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
GB	Gigabyte
GUI	Graphical User Interface
HBA	Host Bus Adapter
HTTPS	Hypertext Transfer Protocol – Secure
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
RAM	Random Access Memory
RDBMS	Relational Database Mangement System
RDF	Resource Description Framework
REST	Representational State Transfer
SAN	Storage Attached Network
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SLES	SUSE Linux Enterprise Server
SMI-S	Storage Management Initiative – Specification
SNIA	Storage Networking Industry Association
SNMP	Storage Network Management Protocol

Acronym	Definition
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
vApp	Virtual Application
VM	Virtual Machine
WMI	Windows Management Instrumentation
WS-MAN	Web Service Managment

9.2 Terminology

Table 20 Terms

Term	Definition
resource object	A discovered resource. EMC documentation refers to these as "objects". They are refered to as "resource objects" in this document to avoid confusion with the objects identified in the Access Control SFP.
Resource	A physical thing, such as a storage array, a logical thing, such as a user group or a collection of things. The basis of the Resource Oriented Architecture.
Resource data	Configuration, performance, and capacity information taken from a discovered resource.
virtual machine	A software computer that, like a physical computer, runs an operating system and applications. Multiple virtual machines can operate on the same host system concurrently.
virtual appliance	A software solution composed of one or more virtual machines. A virtual appliance is packaged as a unit by an appliance vendor and is deployed, managed, and maintained as a unit.

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
United States of America

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