EMC Corporation®

Ionix™ for IT Operations Intelligence (SMARTS®) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.8

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, 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 Ionix™ for IT Operations Intelligence (SMARTS®) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3, collectively referred to as EMC Ionix™ for IT Operations Intelligence Suite, and will hereafter be referred to as the TOE throughout this document. The TOE is a suite of software-based products intended to monitor enterprise IT[1] network, server, and storage performance and availability, as well as perform root cause analysis and business impact analysis for service degradation or failure conditions.

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 - ST and TOE References

ST Title	EMC Corporation® Ionix™ for IT Operations Intelligence (SMARTS®) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3 Security Target
ST Version	Version 0.8
ST Author	Corsec Security, Inc.
ST Publication Date	2/17/2012

[1] Information Technology

ST Title	EMC Corporation® Ionix™ for IT Operations Intelligence (SMARTS®) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3 Security Target
TOE Reference	EMC® Ionix for IT Operations Intelligence (SMARTS) SAM 8.1.1.0 build 19 IP 8.1.1.0 build 59 NPM 3.1.2.0 build 4 SIA 2.3.1.1 build 2 EISM 3.0.0.0 build 91 SAM Adapters 1.3.0.0 build 28

1.3 Product Overview

The EMC Corporation Ionix™ for IT Operations Intelligence (SMARTS®) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3 suite is a suite of products consisting of four major monitoring components, including IP Management Suite, Server Manager (EISM[2]), Network Protocol Manager, and the Storage Insight for Availability Suite. These components are responsible for performing discovery and mapping out networked assets, including IP network nodes, servers, and networked storage, collecting the resource information from monitored assets, and passing the resource data back to the central management server, known as Service Assurance Manager (SAM). The SAM is responsible for parsing the monitored resource event data, normalizing it into a common format, aggregating it and presenting it to the end user.

The SAM Suite can be broken down into four components: the Global Console, the Business Dashboard, the Business Impact Manager, and the SAM Adapter platform. The Global Console is the primary management tool for administrators and operators, providing a central graphical user interface (GUI) for managing the monitored resources, and responding to notifications. The functionality of the Global Console can also be provided through a web based interface known as the Web Console. The Business Dashboard is a web-based portal for displaying summary information on monitored assets, including maps, notifications, status tables, and other customized views. The Business Impact Manager is capable of analyzing the event data provided by the SAM and performing calculations to measure the collateral impacts of failures or service degradations. The SAM Adapter platform allows for integration with third-party management and monitoring tools.

One of the main capabilities provided by the EMC Ionix suite is the root cause analysis that it performs on resource data to identify the root cause of a service failure based on a set of signatures. The consequential failure events are suppressed, allowing for immediate identification and response to service failures and related incidents. Escalation policies can be created, allowing for automated actions to be performed on known failure conditions, minimizing response time to almost zero.

Table 2 details the minimum software and hardware requirements for the various Ionix components:

Table 2 - Minimum Requirements

Component	Software/OS Requirements	Hardware Requirements
Service Assurance Management Suite	- Red Hat Linux Enterprise Linux ○ AS[3] 4	2 Xeon 2.8 GHz[4] CPUs[5] OR UltraSPARC-T2 4 GB[6] RAM[7]

[2] EMC Ionix Server Manager
[3] Advanced Server
[4] Gigahertz
[5] Central Processing Unit

Component	Software/OS Requirements	Hardware Requirements
	○ AS 5 64-bit - Solaris ○ 9 ○ 10 - Windows Server ○ 2003 SP2 32-bit ○ 2008 SP2 32-bit ○ 2003 Enterprise Edition R2 64-bit ○ 2003 Enterprise Edition SP2 64-bit ○ 2008 Enterprise Edition 64-bit - Windows ○ XP Professional SP3 32- or 64-bit (console only) ○ Vista 32- or 64-bit (console only) ○ 7 32- or 64-bit (console only) - Virtual machines ○ Solaris 10 Sun Zones 64-bit ○ VMware ESX Server 3.5x	500-750 MB[8] disk space (SAM Server) 300-500 MB disk space (SAM Console) 512 MB RAM and 100 MB disk space for Service Assurance Manager 256 MB RAM and 150 MB disk space for Global Console, Web Console, and Business Dashboard 512 MB RAM and 100 MB disk space for each SAM Adapter 256 MB RAM and 50 MB disk space for each Syslog Adapter 256 MB RAM and 50 MB disk space for each SNMP Trap Adapter 256 MB RAM and 200 MB disk space for each XML Adapter
IP Management Suite	Supported OS: - Red Hat Enterprise Linux ○ AS 4 64-bit ○ AS 5 64-bit - Solaris ○ 9 ○ 10 64-bit - Windows Server ○ 2003 SP2 64-bit ○ 2008 SP2 64-bit ○ 2003 Enterprise Edition SP2 64-bit ○ 2008 Enterprise Edition 64-bit - Virtual machines ○ Solaris 10 Sun Zones 64-bit	1.25 GB disk space Memory and CPU requirements depend on deployment scope
Network Protocol Manager	Supported OS: - Red Hat Enterprise Linux ○ AS 4 ○ AS/AP 5 (64-bit operating system	1GB disk space Memory and CPU requirements depend on deployment scope

[6] Gigabyte (1,000,000,000 bytes)
[7] Random Access Memory
[8] Megabyte (1,000,000 bytes)

Component	Software/OS Requirements	Hardware Requirements
	version only for AMD64/EM64T chipsets) - Solaris o 9 (64-bit operating system version only for ultrasparc/Niagra chipsets) o 10 (64-bit operating system version only for ultrasparc/Niagra chipsets) - Windows Server o 2003 Enterprise Edition R2 SP2, 32-bit o 2003 Enterprise Edition R2 SP2, 64-bit o 2008 SP2, 64-bit - Virtual machines o Solaris 10 Sun Zones o VMware ESX Server 3.5 o VMware ESX Server 4.0	
Server Manager	Supported OS: - Red Hat Enterprise Linux o AS 5 64-bit - Solaris o 9 o 10 64-bit - Windows Server o 2003 Enterprise Edition 32, 64-bit o 2008 SP2 64-bit o 2008 Enterprise Edition (Parent Partition) - Virtual machines o VMware ESX 3.5, 4.0 (vSphere) on Linux and Windows o Windows Server 2008 Hyper-V as a child partition on Windows 2008 and Red Hat Linux AS 5 - F5 BIG-IP o 9.1.2 o 9.4.x	2 Xeon 2.8 GHz CPUs OR SunFire V240 4 GB RAM ~500 MB disk space Additional 512 MB RAM and 100 MB disk space per instance
Storage Insight for Availability	Supported OS: - Windows Server	N/A

Component	Software/OS Requirements	Hardware Requirements
	○ 2003 SP2 34-bit ○ 2008 SP2 64-bit Required software: EMC Ionix SAM EMC Ionix Global Console EMC ControlCenter EMC Ionix IP Availability Manager for NAS (optional) EMC Ionix Server Manager for VMWare ESX and Virtual Hosts (optional)	
SAM Adapters	Supported OS: - Windows Server ○ 2003 Enterprise Edition R2 SP2 32-bit - Solaris ○ 9 ○ 10 - Red Hat Enterprise Linux ○ AS 4, 5 64-bit	X86, AMD64, EM64T, or UltraSPARC CPU 512 MB RAM 500 MB disk space

1.4 TOE Overview

The TOE is a software-only suite of monitoring, discovery, asset management, service availability and performance assurance, and root cause and impact analysis tools. The next section provides an overview of the TOE identifying the TOE's usage and security features, as well as outlines a deployment scenario for the evaluated configuration.

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

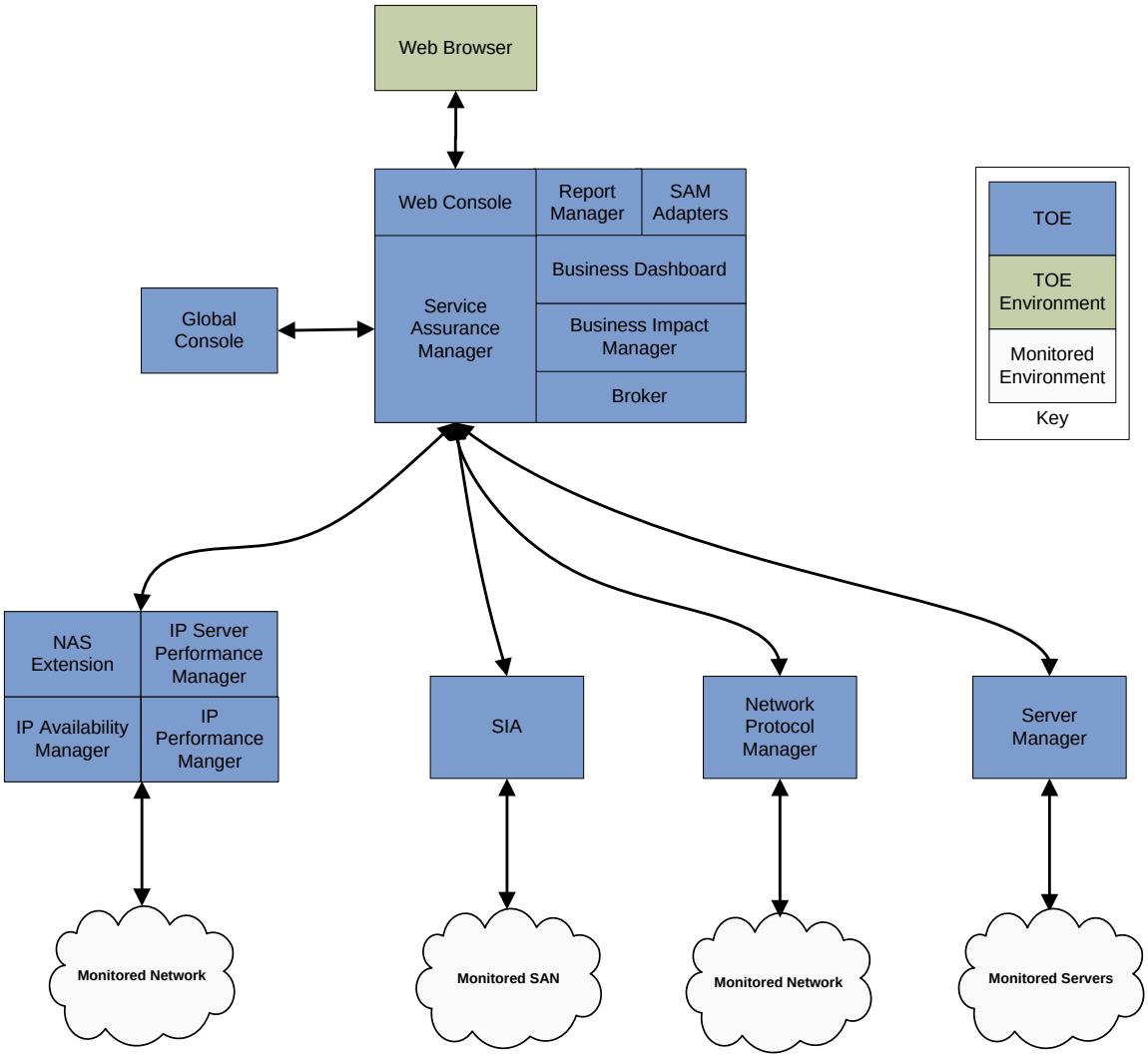

Figure 1 - Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The TOE includes the following products:

- Global Manager (Service Assurance Manager) – the core management server for the TOE
- Global Console – a user interface that provides different views into EMC Ionix-managed domains
- Web Console – a Web based version of the Global Console
- Business Impact Manager – a component that extends the capabilities of Service Assurance Manager by calculating the business impact of events.
- Business Dashboard – flexible, business-oriented web-based user interface that displays a collection of EMC Ionix analysis data alongside important data from other sources in a web page.
- SAM Adapters and Report Manager – extends the capabilities of Service Assurance Manager by storing events in a database ready to compile into reports.
- Broker - manages a registry of EMC Ionix server applications.
- IP Management Suite – performs automatic topology discovery and monitors the availability and performance of IP networks. This is further subdivided into four components: the IP Availability

Manager, IP Performance Manager, IP Server Performance Manager, and the IP Availability Manager Extension for NAS.

- Server Manager (EISM) – monitors the vital statistics and performance of critical servers, virtual machines, and clusters.
- Storage Insight for Availability – diagnoses availability issues across block and file protocol-based storage networks, including Fibre Channel and iSCSI[9] Storage Area Network (SAN) and Networked Attached Storage (NAS), as well as providing impact to servers and business services.
- Network Protocol Manager – discovers and monitors performance of layer 3 network protocols including Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), Extended Inter-Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF).

1.4.2 TOE Environment

The TOE environment consists of the operating systems, runtime environments, and physical or virtual hardware platforms on which the TOE is intended to operate. The typical deployment is in a large enterprise or government data center. The TOE supports multiple platforms, including Microsoft Windows Server, Red Had Enterprise Linux, and Solaris. Windows and Red Hat are also supported as guest Operating Systems (OS) on the VMware ESX Server virtualization platform. Table 3 below lists the various platform requirements for each subsystem of the TOE. Each component is generally deployed on its own dedicated physical or virtual server running a supported OS. The TOE boundary envelops only those software components described in the TOE reference, and none of the underlying software, hardware, storage, or network infrastructures.

1.5 TOE Description

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

1.5.1 TOE Description

The TOE consists of four monitoring components (IP Management Suite, Storage Insight for Availability, Network Protocol Manager, and Server Manager). These components map and monitor IP networks, critical servers, and network storage devices. They pass the information gathered to the core management server – the Service Assurance Manager (also known as Global Manager). This management server aggregates this information and presents it to the user through the Global Console or the web browser. The Service Assurance Modules (Business Impact Manager, Business Dashboard, and Reports Manager) provide additional capabilities to calculate and display the business impact of infrastructure problems and to produce a wide variety of reports. The Broker manages a registry of EMC Ionix server applications, which allows each component to discover other components of the system.

The product helps system administrators cope with the flood of raw events which will be generated by a problem in the IT infrastructure. The system uses a normalized event reporting structure, the EMC Ionix Common Information Model (ICIM), which identifies and consolidates duplicated events.

The TOE can also distinguish between the root cause of problems and the collateral impacts. For example, one router failing might increase the throughput of other routers and cause them to fail. The system administrator will receive events from many routers, but only needs to address the problem on one router. The system uses patented Codebook Correlation Technology. This set of algorithms computes a correlation between the set of possible symptoms and the root cause that can best explain the symptoms, based on the nature of the symptoms and the network topology. The processing of these algorithms is distributed throughout the system for optimal performance, but the final correlation analysis, policy

[9] Internet Small Computer System Interface

implementation and presentation to the user occurs in the Service Assurance Manager. The information is made available to the administrator through a web browser or the Global Console.

1.5.2 TOE Components

The TOE consists of the elements described in the following sections.

1.5.2.1 IP Management Suite

The IP Management Suite consists of the following:

- IP Availability Manager
- IP Performance Manager
- IP Server Performance Manager
- IP Availability Manager Extension for NAS

The IP Management Suite products are a set of tools that can discover network topology of IP networks. It operates at layers 2 and 3 of the Open System Interconnection (OSI) model. Devices are identified by their IP and Media Access Control (MAC) addresses. It can determine the physical and logical relationships between entities and the network protocols in use. The information is updated in real-time and presented in a traversable topology map. It also provides root cause analysis and can distinguish between the root issue and the collateral effects.

The IP Management Suite components are all deployed using a single server topology. Discovery and device monitoring features make use of Simple Network Management Protocol version 3 (SNMPv3) and Internet Control Message Protocol (ICMP) polling and traps, which are used to develop topology information, and generate availability and performance related events. The IP Management Suite components then perform post-processing on these events and topology to provide root cause analysis, problem identification, and notifications to the SAM.

In addition, the IP Availability Extension for NAS discovers and monitors NAS devices, including EMC Celerra and NetApp Filers. Discovery and monitoring is performed by reading HTTPS[10] and XML[11] data from the Celerra Network Server. The information gathered by the NAS extension is used to aid in root cause analysis of monitored storage devices, extending the IP Availability Manager's functionality to cover critical enterprise storage.

1.5.2.2 Storage Insight for Availability

SIA is a SAN and NAS monitoring tool. SIA monitors storage topologies for availability problems and analyzes alerts to identify the root-cause of outages and other problems, as well as to provide analysis of the impact on hosts and business services. When SIA and IP Availability Manager are used together, the root of problems across the entire network can be pin-pointed to the exact location to minimize downtime.

The SIA is split into two components, the Storage Insight Topology Server, and the Storage Insight Analysis Server, which both run on the same host. The Topology Server performs discovery of storage topology while the Analysis Server processes events and correlates alerts indicative of a network or storage failure. SIA also integrates with Server Manager to give root cause analysis for VMWare ESX host and VM hosts down root cause. Server Manager is discussed in the following section.

The SIA depends on EMC ControlCenter to obtain storage topology and events. It retrieves data from the ControlCenter Repository through SQL[12] queries using Java Database Connectivity (JDBC), from Celerra

[10] Hypertext Transfer Protocol Secure
[11] eXtensible Markup Language
[12] Structured Query Language

Control Stations using the Celerra CLI[13] and Application Programming Interface (API), from NetApp arrays using the Data ONTAP API, from Hitachi and Sun arrays using HTTP[14]and HTTPS, and from Hewlett-Packard arrays using the StorageWorks CVCLI[15].

1.5.2.3 Server Manager (EISM)

The Server Manager is capable of performing discovery, monitoring, availability and performance analysis, in conjunction with the IP Management Suite and Service Assurance Management Suite. It can determine when servers are not performing optimally and help to identify possible future failures. It supports several server technologies, including VMware ESX and vSphere, virtual machines, VirtualCenter, VMware Cluster, Windows Hyper-V, Microsoft Clustering Services, and Veritas Cluster Server. It performs process monitoring to identify issues with application processes or services, hardware monitoring, including temperature, power supply, fan, and voltage sensor monitoring, and operating system monitoring, including chassis, disk, file system, host, network interface, memory, and processor monitoring. It also supports F5 BIG-IP load balancers.

The Server Manager utilizes Microsoft Windows Management Instrumentation (WMI) and SNMP, Veritas CLI and Veritas SNMP traps, and the VMware Infrastructure API to retrieve data from its monitored servers. It interfaces with the IP Availability Manager to perform root-case and impact analysis. The Server Manager also includes the Remote Java Adapter component for interfacing with VMware products.

1.5.2.4 Network Protocol Manager

The Network Protocol Manager provides discovery and monitoring services for layer 3 networking devices, specifically for routing protocols such as BGP, EIGRP, IS-IS, and OSPF. It is intended to diagnose routing protocol availability problems in IP networks and explains protocol-specific failures. It collects information from monitored devices using SNMP and CLI polling and, in conjunction with the EMC Ionix IP Availability Manager, it performs root cause and impact analysis; the results of which are provided to the SAM.

1.5.2.5 Service Assurance Manager

The Service Assurance Manager, or Global Manager, serves as the cornerstone of network operations management. The Service Assurance Manager provides integrated, unified, and individualized views of the systems, network infrastructure, applications, and business entities that comprise the managed domain. The Service Assurance Manager communicates with the EMC Ionix monitoring components and consolidates the following information:

- Network, system, application, and business resources
- Results of domain-specific root-cause analysis
- Results of domain-specific impact analysis

The Service Assurance Manager automatically correlates topology and event data from multiple EMC Ionix managed domains to diagnose root-cause problems.

1.5.2.6 Business Impact Manager

The Business Impact Manager extends the capabilities of Service Assurance Manager to analyze events by calculating the business impact of events and propagating the impacts to affected business entities as discrete notifications that are linked to topology within the managed domain. The impacts are displayed in the Business Services Maps. Impact analysis is done by associating business-level objects, including departments, services, and customers, to applications and network infrastructure.

[13] Command Line Interface
[14] Hypertext Transfer Protocol
[15] Command View Command Line Interface

To complement the root cause analysis features of the TOE, the Business Impact Manager assigns a numeric impact value, or weight, to business, application and infrastructure elements, and propagates root cause notifications to elements, enabling TOE administrators to quickly identify and respond to high-impact issues on mission-critical systems. The larger the impact value, the higher degree of impairment to monitored resources. Business Impact Manager helps meet service level agreements by providing a methodology for mapping business entities and their related resources, and a topology map enabling operators to quickly identify affected entities.

1.5.2.7 Business Dashboard

The Business Dashboard is a web console that displays a collection of EMC Ionix analysis data alongside important data from other sources. Each part of the dashboard is presented as a viewlet, which is a modular graphical representation of data from a particular EMC Ionix component. Viewlets connect directly to the Global Manager to retrieve data. The Business Dashboard is flexible and more business-oriented than the Global Console or Web Console, however, it has much less capability than its counterparts. It is intended to provide information at-a-glance to management entities or as part of a network operations center (NOC) display monitor.

Using the Business Dashboard viewlets enables operators to quickly identify critical security events and respond to notifications as they occur on monitored resources. Viewlets are restricted to authorized operators.

1.5.2.8 SAM Adapters and Report Manager

The SAM Adapters and Report Manager enable EMC Ionix to import event and topology data and to export analysis results to third-party tools. They also allow imported events to be associated with network topology in order to provide context for root cause analysis and impact analysis.

Through the use of SAM Adapters, TOE administrators can extend the root cause and resource monitoring capabilities of the TOE by integrating with third-party systems using both proprietary and industry standard protocols such as SNMP and Syslog. Information retrieved by the SAM Adapters is normalized into the ICIM data model for root cause analysis. The products supported by SAM Adapters include:

- BMC Remedy ARS[16]
- Concord eHealth
- InfoVista
- Microsoft Operations Manager 2005
- Microsoft System Center Operations Manager 2007
- NetIQ AppManager
- SiteScope

The Report Manager enables network administrators to produce and display or print network operations and management reports through Business Objects software. Report Manager is supplied with the following products:

- Business Objects XI for Windows or UNIX – provides reporting functionality and a collection of predefined reports.
- Crystal Reports XI Professional Edition – allows users to create custom reports
.

Report Manager is deployed with the EMC Ionix SQL Data Interface Adapter, a third-party database installation (Oracle or Microsoft SQL), and an Open Database Connectivity (ODBC) driver. Through this interface, administrators can extract notification and event data using a schema customized for third-party

[16] Action Request System

reporting applications. Reporting information, including resource availability notifications and other event data is restricted to authorized users.

1.5.2.9 Broker

The Broker manages a registry of EMC Ionix server applications. When an EMC Ionix server application starts it registers with the broker, providing its IP address and listening port number. When an EMC Ionix application needs to connect with another application, it gets the necessary information from the Broker. Periodically, the Broker pings the applications in its registry to determine whether they are still active. The Broker also ensures that distributed domain managers are authenticated with each other, as well as client applications such as the Global Console.

1.5.2.10 Global Console

The Global Console is the primary user interface for the administration of the Service Assurance Manager. The console displays the network topology and the status of network components. Through the Global Console administrators can monitor EMC Ionix domains, acquire detailed information about topology and events, respond to problems, and take corrective action. EMC Ionix administrators with appropriate privileges can administer EMC Ionix users, user profiles and policies. The Global Console runs as a standalone Java program, or as an applet through the Web Console.

The Global Console contains several sub-consoles, including the following:

- Notification Log Console – presents notifications in tabular format.
- Map Console – graphically presents topology information on a map. Each item on the map changes color to reflect its condition.
- Topology Browser Console – represents the topology in a hierarchical format.
- Summary View Console – shows overview or summaries of notifications organized by criteria.
- Status Table Console – represents status of infrastructure elements.
- Web Console – provides Global Console functionality from a web browser.
- Domain Manager Administration Console – enables administrators to discover topology and manage EMC Ionix suite components.
- Topology Builder Console – allows administrators to modify and refine topology maps.

1.5.3 Physical Scope

The TOE is a suite of software tools which run on multiple operating platforms, compliant to the minimum software and hardware requirements as listed in Section 1.5.3.1. The OS and hardware components are not part of the TOE. The TOE is installed on the OS and hardware as depicted in Figure 2.

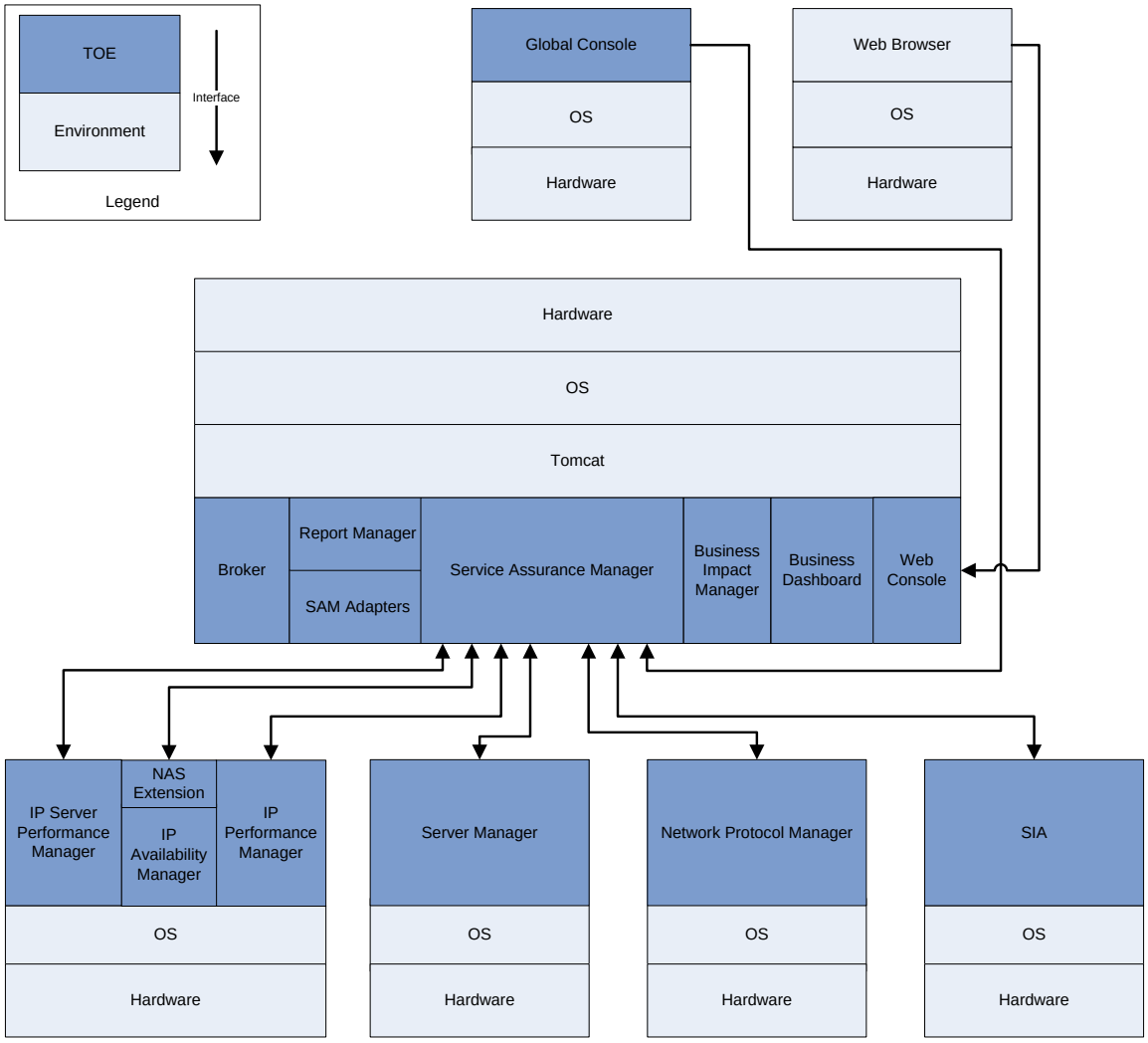

Figure 2 - Physical TOE Boundary

The essential physical components for the proper operation of the TOE in the evaluated configuration are five physical or virtual guest servers and one server or workstation class machine running the Global Console. The SAM suite components, including the Global Manager, Business Impact Manager, Business Dashboard, Broker, and SAM Adapters, together run on a single server, the SIA Analysis and Topology components on another, the IP Availability, Performance, and Discover Managers run on another, and the Server Manager and Network Protocol Manager each on their own respective machine.

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment. This represents the CC-evaluated deployment configuration; however, actual deployments will vary greatly in scope. The TOE is scalable from small to large enterprise networks.

1.5.3.1 TOE Software

The TOE is an array of software applications that are distributed across several physical or virtual servers. Table 3 specifies tested platforms and architectures for the TOE in the CC-evaluated configuration.

Table 3 - Evaluated Configuration

Component	Platform Tested	Architecture
Service Assurance Management Suite	Windows Server 2003 Enterprise Edition SP2	32-bit
	Red Hat Enterprise Linux AS 5	64-bit
Global Console	Windows Server 2003 SP2 Windows Server 2008 SP2	32-bit
SAM Adapters: - NetIQ SAM Adapter - System Center Operations Manager SAM Adapter - ARS Remedy SAM Adapter - SQL Data Interface SAM Adapter	Windows Server 2003 Enterprise Edition R2 SP2	32-bit
	Red Hat Enterprise Linux AS 5	64-bit
IP Management Suite	Windows Server 2003 SP2 Windows Server 2008 SP2 Red Hat Enterprise Linux AS 4 Red Hat Enterprise Linux AS 5 Solaris 10	64-bit
SIA	Windows Server 2003 SP2	32-bit
	Windows Server 2008 SP2	64-bit
EISM	Windows Server 2003 Enterprise Edition R2 SP2	32-bit
	Windows Server 2003 Enterprise Edition R2 SP2 Windows Server 2008 SP2 Red Hat Enterprise Linux AS 5 Solaris 10	64-bit
NPM	Windows Server 2003 Enterprise Edition R2 SP2	32-bit
	Windows Server 2003 Enterprise Edition R2 SP2 Windows Server 2008 SP2 Red Hat Enterprise Linux AS 5 Solaris 10	64-bit

On the client The EMC Ionix Web Console and Business Dashboard require Internet Explorer 6.0 SP1 or 7.0, Firefox 2 or greater, and the Java Runtime Environment 1.5.x or 1.6.x.

1.5.3.2 Guidance Documentation

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

- EMC Ionix Service Assurance Management Suite Deployment Guide
- EMC Ionix Service Assurance Management Suite Installation and Migration Guide
- EMC Ionix Service Assurance Manager Operator Guide
- EMC Ionix Service Assurance Manager Configuration Guide
- EMC Ionix Service Assurance Manager Dashboard Configuration Guide
- EMC Ionix Business Impact Manager User Guide
- EMC Ionix Service Assurance Manager Failover System User Guide
- EMC Ionix Service Assurance Manager Adapter Platform User Guide
- EMC Ionix Service Assurance Manager Notification Adapters User Guide
- EMC Ionix XML Adapter User Guide
- EMC Ionix Storage Insight for Availability Discovery Guide
- EMC Ionix Storage Insight for Availability Installation and Configuration Guide
- EMC Ionix Storage Insight for Availability User Guide
- EMC Ionix IP Management Suite Installation Guide
- EMC Ionix IP Management Suite Deployment Guide
- EMC Ionix IP Management Suite Configuration Guide
- EMC Ionix IP Management Suite Discovery Guide
- EMC Ionix IP Availability Manager User Guide
- EMC Ionix IP Performance Manager and Server Performance Manager User Guide
- EMC Ionix IP Availability Manager Extension for NAS User Guide
- EMC Ionix Server Manager Installation Guide
- EMC Ionix Server Manager Configuration Guide
- EMC Ionix Server Manager User Guide
- EMC Ionix Network Protocol Management Suite Installation Guide
- EMC Ionix Network Protocol Manager for BGP User's Guide
- EMC Ionix Network Protocol Manager for EIGRP User's Guide
- EMC Ionix Network Protocol Manager for IS-IS User's Guide
- EMC Ionix Network Protocol Manager for OSPF User's Guide
- EMC Ionix Network Protocol Manager Configuration Guide
- EMC Ionix Network Protocol Manager Discovery Guide
- EMC Ionix Adapter for Concord eHealth User Guide
- EMC Ionix Adapter for InfoVista User Guide
- EMC Ionix Adapter for Microsoft Operations Manager 2005 User Guide
- EMC Ionix Adapter for Microsoft System Center Operations Manager 2007 User Guide
- EMC Ionix Adapter for NetIQ AppManager User Guide
- EMC Ionix Adapter for Remedy ARS User Guide
- EMC Ionix Adapter for SiteScope User Guide
- EMC Ionix SQL Data Interface Adapter User Guide
- EMC Ionix Report Manager User Guide
- EMC Ionix Service Assurance Manager Adapters Suite and Report Manager Installation Guide
- EMC Ionix Foundation 9.0 ITOps[17] System Administration Guide

1.5.4 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 f 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

[17] IT Operations

- Identification and Authentication
- Security Management
- TOE Access
- IT Operations Intelligence

1.5.4.1 Security Audit

The TOE is capable of generating audit records for logon failures and notification responses, using timestamps provided by the OS, and can be viewed by the TOE user via the Global Console and Web Console. The events are recorded in the standardized ICIM format and stored in the file system of the OS running the SAM. Security events are analyzed to determine a potential security violation based on thresholds. Events can only be modified or deleted by authorized administrators.

1.5.4.2 Identification and Authentication

The Identification and Authentication function ensures that the TOE user that requests a service has provided a valid username and password. When TOE users enter their username and password at the Global Console or Web Console interface, the information is passed to the Service Assurance Manager, where it is verified against the credentials stored in the TOE. If the provided username and password match, the TOE user is assigned the role associated with that username. Before identification and authentication, the TOE user is only able to view active TOE components.

1.5.4.3 Security Management

The TOE maintains three roles: All, Monitor, and Ping. The All role has access to all elements of the TOE. The Monitor role can only view information. The Ping role can only discover which TOE components are active. Users perform all management of the TOE through the Global Console or Web Console.

1.5.4.4 TOE Access

TOE users are presented with a security message or disclaimer prior to authenticating when the Global Console, Web Console, or Business Dashboard is launched.

1.5.4.5 IT Operations Intelligence

The TOE is capable of providing IT Operations Intelligence which enforces availability of monitored devices and resources. It collects information from its various monitoring services, and records events in the ICIM format, using timestamps provided by the OS. Resource event data is analyzed to perform root cause and impact analysis of failure conditions; notifications are provided to the end user upon detection of an availability violation. Event data is viewable by authorized users through the Global Console or Web Console.

1.5.5 Product Physical/Logical Features and Functionality not included in the TSF

The following protocols implemented by the TOE are not considered secure and therefore are excluded from the evaluated configuration and not considered to be part of the TSF:

- SNMPv1
- SNMPv2
- SSH[18]v1
- Telnet

The following software is excluded from the evaluated configuration:

[18] Secure Shell

- EMC Ionix ITOps Notification Module
- EMC Ionix ITOps Health Monitor

2 Conformance Claims

This section provides 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 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the Common Evaluation Methodology (CEM) as of 12/23/2010 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 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.
- 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[19] 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. The following threats are applicable:

Table 5 - Threats

Name	Description
T.PRIVIL	An unauthorized individual may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.TAMPERING	A user or process 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.AVAIL	An unauthorized individual might disrupt the availability or performance of IP networks, servers or storage in the TOE environment.
T.AVAIL2	The root cause of an extended disruption of service provided by the TOE environment may not be immediately apparent, exhausting time and personnel resources to identify, troubleshoot, and correct the root condition, potentially incurring a financial loss or other collateral damage to the organization.
T.AVAIL3	Resources in the TOE environment might become over-allocated, causing a denial of service condition when resources are exhausted.

[19] TOE Security Functionality

Name	Description
T.COMINT	An unauthorized individual may attempt to compromise the security of the data collected and produced by the TOE by bypassing a security mechanism.
T.EAVESDROP	An external attacker might listen in on data communications traversing public networks, potentially exposing sensitive infrastructure information.

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. The following OSPs are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration:

Table 6 - Organizational Security Policies

Name	Description
P.MANAGE	The TOE may only be managed by authorized users.
P.INTEGRITY	Data collected and produced by the TOE must be protected from modification.
P.ESCALATE	The organization must have a defined incident escalation policy with procedures for responding to performance or availability conditions occurring within critical IT assets.

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. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 7 - Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to monitor its resources.
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.

Name	Description
A.MANAGE	There are one or more competent individuals assigned to manage the TOE
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.SECURE	The communication between the TOE and its monitored resources will be protected from alteration or impersonation.

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 as follows:

Table 8 - Security Objectives for the TOE

Name	Description
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 audit events of actions on the TOE with security relevance which may be indicative of misuse.
O.IDAUTH	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.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.SECURE	The TOE must ensure the security of all audit and system data.
O.MONITOR	The TOE must gather, analyze, and present information about all events that are indicative of unavailability or poor performance of IP networks, servers, and networked storage.
O.ROOTANL	The TOE must be able to perform root cause analysis to detect conditions that affect the availability or performance of monitored resources.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 9 - IT Security Objectives

Name	Description
OE.PLATFORM	The TOE hardware and OS must support all required TOE functions.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.AVAIL	The TOE environment must be implemented such that the TOE is available and reachable from the monitored network in order to perform its intended function.
OE.SUPPORT	The TOE environment must support the applicable protocols necessary for protection of TOE data across hostile networks.

4.2.2 Non-IT Security Objectives

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

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 TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

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_INX_MDC.1	Monitored Resource Data Collection
EXT_INX_RCA.1	Root Cause Analysis
EXT_INX_ARP.1	Resource Availability Alarms
EXT_INX_RDR.1	Restricted Data Review

5.1.1 Class INX: IT Operations Intelligence

IT Operations Intelligence functions involve collecting information from managed devices, analyzing and correlating the data for possible indications of service availability violations, and producing alarms based on the root cause and impact analysis performed.. The EXT_INX: IT Operations Intelligence functionality class was modeled after the CC FAU: Security audit class. The extended family EXT_INX_MDC: Monitored Resource Data Collection and related components were modeled after the family FAU_GEN: Audit Data Generation. The extended family and related components for EXT_INX_RCA: Root Cause Analysis was modeled after the family FAU_SAA: Security Audit Analysis. The extended family EXT_INX_ARP: Security alarms was modeled after the CC family FAU_ARP: Security Alarms. The extended family EXT_INX_RDR: Restrictive Data Review was modeled after the CC family FAU_SAR: Security Audit Review.

Figure 3 - EXT_INX: IT Operations Intelligence Class Decomposition

5.1.1.1 Monitored Resource Data Collection (EXT_INX_MDC)

Family Behaviour

This family defines the requirements for recording the occurrence of events that take place under TSF control. This family identifies the level of monitored resource data collection, enumerates the types of events that shall be collected by the TSF, and identifies the minimum set of event-related information that should be provided within various record types.

Component Leveling

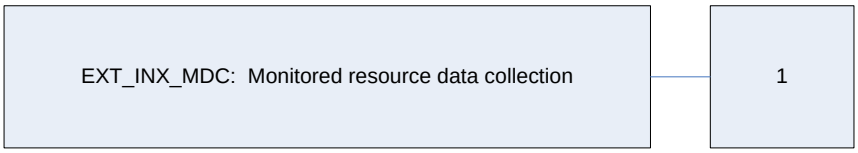

Figure 4 - EXT_INX_MDC Monitored Resource Data Collection family decomposition

EXT_INX_MDC.1: Monitored resource data collection, defines the level of events and specifies the list of data that shall be captured in each event recorded.

Management: EXT_INX_MDC.1

- There are no auditable events foreseen.

Audit: EXT_INX_MDC.1

- There are no auditable events foreseen.

EXT_INX_MDC.1 Monitored resource data collection
Hierarchical to: No other components
EXT_INX_MDC.1.1
The TSF shall be able to perform dynamic discovery of and create event records corresponding to the following information gathered from the monitored resource:
[assignment: *specifically defined events*.]
EXT_INX_MDC.1.2
At a minimum, the TSF shall collect and record the following information:
- Date and time of the event, type of event, monitored resource, and the outcome (success or failure) of the event.

Dependencies: FPT_STM.1 Reliable time stamps

5.1.1.2 Root Cause Analysis (EXT_INX_RCA)

Family Behaviour

This family defines requirements for automated means that analyze monitored resource data looking for possible or real violations of resource availability. This family enumerates the types of analysis functions that shall be performed on data collected by the TSF. The actions to be taken based on the detection can be specified using the EXT_INX_ARP: Resource availability alarms family.

Component Leveling

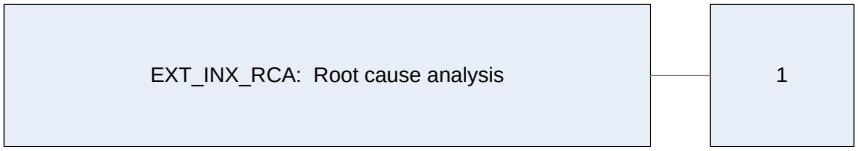

Figure 5 - EXT_INX_RCA Root Cause Analysis family decomposition

EXT_INX_RCA.1 Root cause analysis, specifies the list of analyses the TOE will perform on the collected resource data. The TSF shall be able to detect the occurrence of signature-based events that represent a significant threat to resource availability in the TOE environment, and assign severity levels based on business impact of events.

Management: EXT_INX_RCA.1

- Maintenance of the analysis functions by (adding, modifying, deletion) of signatures from the set of signatures.

Audit: EXT_INX_RCA.1

- Minimal: Enabling and disabling any of the root cause analysis mechanisms.

EXT_INX_RCA.1 Root cause analysis
Hierarchical to: No other components
EXT_INX_RCA.1.1
The TSF shall be able to perform the following analysis functions *[assignment: analytical functions]* in order to maintain an internal representation of behavior-based signatures that represent real problem scenarios in the TOE environment.
EXT_INX_RCA.1.2
The TSF shall be able to compare the signature events and event sequences against the record of resource activity.
EXT_INX_RCA.1.3
The TSF shall be able to indicate a potential violation of monitored resource availability when collected resource data is found to match a signature event or event sequence that indicates a potential violation of monitored resource availability.
EXT_INX_RCA.1.4
The TSF shall be able to assign a weighted value to monitored objects, which shall be used to determine the severity or business impact of violations.

Dependencies: EXT_INX_MDC.1

5.1.1.3 Resource Availability Alarms (EXT_INX_ARP)

Family Behaviour

This family defines the requirements for the response to be taken in case of a detected violation of monitored resource availability.

Component Leveling

Figure 6 - EXT_INX_ARP Resource Availability Alarms family decomposition

EXT_INX_ARP.1 Resource availability alarms, the TSF shall take actions in the case of a detected resource availability violation.

Management: EXT_INX_ARP.1

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

- Management (addition, removal, or modification) of alarm.

Audit: EXT_INX_ARP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Actions taken due to a detected resource availability violation.

EXT_INX_ARP.1 Resource availability alarms
Hierarchical to: No other components
EXT_INX_ARP.1.1
The TSF shall take [*assignment: list of actions*] upon the trigger of a programmable alarm.

Dependencies: EXT_INX_MDC.1

5.1.1.4 Restricted Data Review (EXT_INX_RDR)

Family Behaviour

This family defines the requirements for resource monitoring tools that should be available to authorized users to assist in the review of collected resource data.

Component Leveling

Figure 7 - EXT_INX_RDR Restricted Data Review family decomposition

EXT_INX_RDR.1 Restricted data review, the TSF shall ensure that no other users other than those identified can read the collected resource data.

Management: EXT_INX_RDR.1

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

- There are no management activities foreseen.

Audit: EXT_INX_RDR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Unsuccessful attempts to read information from the resource data.

EXT_INX_RDR.1 Restricted data review
Hierarchical to: No other components
EXT_INX_RDR.1.1
The TSF shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of events*] from the collected resource data.
EXT_INX_RDR.1.2
The TSF shall provide the resource data in a manner suitable for the user to interpret the information.
EXT_INX_RDR.1.3

The TSF shall prohibit all users read access to the resource data, except those users that have been granted explicit read-access.

Dependencies: No dependencies

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components.

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 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_SAA.1	*Potential violation analysis*		✓		
FAU_SAR.1	*Audit review*		✓		
FAU_STG.1	*Protected audit trail storage*	✓			
FIA_ATD.1	*User attribute definition*		✓		
FIA_UAU.1	*User authentication before any action*		✓		
FIA_UID.1	*User identification before any action*		✓		
FMT_MOF.1	*Management of security functions behaviour*	✓	✓	✓	
FMT_MTD.1(a)	*Management of TSF data*	✓	✓		✓
FMT_MTD.1(b)	*Management of TSF data*	✓	✓		✓
FMT_SMF.1	*Specification of management functions*		✓		
FMT_SMR.1	*Security roles*		✓		
FTA_TAB.1	*TOE access banner*				

Name	Description	S	A	R	I
EXT_INX_ARP.1	Resource availability alarms		✓		
EXT_INX_MDC.1	Monitored resource data collection		✓		
EXT_INX_RCA.1	Root cause analysis		✓		
EXT_INX_RDR.1	Restricted data review		✓		

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) [*The auditable events specified in Table 13*].

Table 13 - Auditable Events

Auditable Event
Unsuccessful logins
User responses to notifications

FAU_GEN.1.2
The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].
Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAA.1 Potential violation analysis
Hierarchical to: No other components.
FAU_SAA.1.1
The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2
The TSF shall enforce the following rules for monitoring audited events:
Accumulation or combination of [*the system events specified in Table 15*] known to indicate a potential security violation;
[*No other rules*].
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1 Audit review
Hierarchical to: No other components.
FAU_SAR.1.1
The TSF shall provide [the "*All" and "Monitor" roles*] 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 unauthorized deletion.
FAU_STG.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

6.2.2 Class FIA: Identification and Authentication

FIA_ATD.1 User attributes definition
Hierarchical to: No other components.
FIA_ATD.1.1
The TSF shall maintain the following list of security attributes belonging to individual users: [*user name, password, and role*].
Dependencies: No dependencies

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.
FIA_UAU.1.1
The TSF shall allow [*the viewing of active TOE components*] 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_UID.1 Timing of identification
Hierarchical to: No other components.
FIA_UID.1.1
The TSF shall allow [*the viewing of active TOE components*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: No dependencies

6.2.3 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 [**perform the actions listed in Table 14**] the functions [*the functions listed in Table 14*] to [*the roles listed in Table 14*].

Table 14 - Management Functions

Actions	Security Functions	Roles
Determine the behaviour of, Disable, Enable, Modify the behavior of	*Audit*	*All*
Determine the behaviour of, Disable, Enable, Modify the behavior of	*Identification & Authentication*	*All*
Determine the behaviour of, Disable, Enable, Modify the behavior of	*Notifications*	*All*
Determine the behaviour of, Disable, Enable, Modify the behavior of	*Discovery*	*All*
Determine the behaviour of, Disable, Enable, Modify the behavior of	*Monitoring*	*All*
Determine the behaviour of	*Monitoring*	*All,* *Monitor*

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

FMT_MTD.1(a) Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1(a)

The TSF shall restrict the ability to [query] the [*audit data and TOE configuration*] to [*the Monitor and All roles*].

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

FMT_MTD.1(b) Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1(b)

The TSF shall restrict the ability to [modify, delete] the [*audit data and TOE configuration*] to [*the All role]*.

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: [*TSF data management, and security functions behaviour management*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Ping, Monitor, All*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.4 Class FTA: TOE Access

FTA_TAB.1 Default TOE access banners

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

6.2.5 Class INX: IT Operations Intelligence

EXT_INX_ARP.1 **Resource availability alarms**
Hierarchical to: **No other components**
EXT_INX_ARP.1.1

The TSF shall take [*actions to send an alert to the console or email*] upon the trigger of a programmable alarm.

Dependencies: **EXT_INX_MDC.1**

EXT_INX_MDC.1 **Monitored resource data collection**
Hierarchical to: **No other components**
EXT_INX_MDC.1.1

The TSF shall be able to perform dynamic discovery of and create event records corresponding to the following information gathered from the monitored resource:
[*the system events specified in Table 15*]

Table 15 - System Events

Auditable Event
A monitored layer 2 or 3 device: • *Is unavailable* • *Has high processor utilization* • *Has a hard drive failure* • *Has insufficient free memory*
A monitor server: • *Is unavailable* • *Has high processor utilization* • *Has a hard drive failure* • *Has insufficient free memory* • *Processor is unavailable or unresponsive* • *Hardware has failed* • *Cluster node is down* • *Virtual machine resource has failed*
A monitored network adaptor: • *Is unavailable* • *Has a high failure rate*
A monitored storage resource: • *Is unavailable* • *Has file system errors* • *Is becoming exhausted of free space* • *Is performing poorly*
A monitored router: • *Route is unavailable* • *Interface is down* • *Hardware has failed* • *Network performance is degraded* • *Is misconfigured*

Auditable Event
A monitored load balancer: • *Node is down* • *Performance is degraded* • *Interface is down* • *Is misconfigured* • *Hardware has failed*

EXT_INX_MDC.1.2

At a minimum, the TSF shall collect and record the following information:

- Date and time of the event, type of event, monitored resource, and the outcome (success or failure) of the event.

Dependencies: **FPT_STM.1 Reliable time stamps**

EXT_INX_RCA.1 Root cause analysis

Hierarchical to: **No other components**

EXT_INX_RCA.1.1

The TSF shall be able to perform the following analysis functions *[dynamic discovery of network, server and storage topology, creation of failure behavior patterns and other analysis provided by EMC Codebook Correlation technology]* in order to maintain an internal representation of behavior-based signatures that represent real problem scenarios in the TOE environment.

EXT_INX_RCA.1.2

The TSF shall be able to compare the signature events and event sequences against the record of resource activity.

EXT_INX_RCA.1.3

The TSF shall be able to indicate a potential violation of monitored resource availability when collected resource data is found to match a signature event or event sequence that indicates a potential violation of monitored resource availability.

EXT_INX_RCA.1.4

The TSF shall be able to assign a weighted value to monitored objects, which shall be used to determine the severity or business impact of violations.

Dependencies: **EXT_INX_MDC.1**

EXT_INX_RDR.1 Restricted data review

Hierarchical to: **No other components**

EXT_INX_RDR.1.1

The TSF shall provide [*Monitor and All*] with the capability to read [*all resource events*] from the collected resource data.

EXT_INX_RDR.1.2

The TSF shall provide the resource data in a manner suitable for the user to interpret the information.

EXT_INX_RDR.1.3

The TSF shall prohibit all users read access to the resource data, except those users that have been granted explicit read-access.

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 16 - Assurance Requirements summarizes the requirements.

Table 16 - 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[20] 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

[20] Configuration Management

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 17 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.1	User authentication before any action
	FIA_UID.1	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1(a)	Management of TSF data
	FMT_MTD.1(b)	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
TOE Access	FTA_TAB.1	TOE access banner
IT Operations Intelligence	EXT_INX_ARP.1	Resource availability alarms
	EXT_INX_MDC.1	Monitored resource data collection
	EXT_INX_RCA.1	Root cause analysis
	EXT_INX_RDR.1	Restricted data review

7.1.1 Security Audit

The Service Assurance Manager records an audit event whenever a user login fails or when a user responds, or fails to respond promptly, to a notification. The Security Audit SFRs pertain only to security events generated by the Service Assurance Manager.

The TOE audit records contain the following information:

Table 18 - Audit Record Contents

Field	Content
Timestamp	Date and time of the event
Class	Type of event
Source	Subject identity
Event State	Outcome

The audit data can be viewed by TOE users with the roles All and Monitor through the Global Console and the web browser. The SAM performs analysis on the audit events and provides an indication that a potential security violation has occurred. Only users with the role "All" can delete audit events by rolling over the audit logs. The audit logs are stored in the file system of the underlying operating system. They are protected so that only authorized users can modify or delete these files.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAA.1, FAU_SAR.1, FAU_STG.1

7.1.2 Identification and Authentication

The Identification and Authentication function ensures that the TOE user that is requesting a service has provided a valid username and password. For each user, the TOE stores the following security attributes in the database: username, password, and role. When TOE users enter their username and password at the Global Console interface or the web browser interface, the information is passed to the Service Assurance Manager, where it is verified. If the provided username and password are valid, the TOE user is assigned the role associated with that username. Before identification and authentication, the TOE user is only able to view active TOE components. The Broker ensures that all components are authenticated with each other.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.1, FIA_UID.1

7.1.3 Security Management

The TOE maintains three roles: All, Monitor and Ping. The All role has full access to all elements of the TOE. The Monitor role can only view information. The Ping role can only discover which TOE components are active. Users perform all management of the TOE through the Global Console or the Web Console. A user can have a role of "None", but this is not a true role and simply denies all access.

The TOE enforces which roles have access to TSF data, such as events and notifications and configuration settings. All and Monitor roles have the ability to query TSF Data. Only the All role can modify or delete configuration settings. All is the only role that can modify or delete other users' usernames, passwords, or roles. Attempts by the user to query, modify, or delete security attributes (such as username, password, or role), TSF data (such as audit data, resource data and configuration settings), and security are mediated by the TOE.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MTD(a), FMT_MTD.1(b), FMT_SMF.1, FMT_SMR.1.

7.1.4 TOE Access

The TOE provides the capability of displaying what is referred to as a security message, or disclaimer, which is displayed when end users attempt to launch the Global Console, Business Dashboard, or the Web Console. This is not enabled by default, thus the TOE must be configured according to the CC configuration guidance in order to be compliant.

TOE Security Functional Requirements Satisfied: FTA_TAB.1.

7.1.5 IT Operations Intelligence

The IP Availability and IP Performance Manager components record events when a monitored layer 2 or 3 device or a network adaptor on a monitored layer 2 or 3 device is unavailable. The IP Server Performance Manager records an audit event if a monitored server: is unavailable, has high processor utilization, has a hard drive failure, or has insufficient free memory. The Network Protocol Manager monitors internetworking devices utilizing routing protocols such as BGP, EIGRP, IS-IS, and OSPF and records events when it detects a failure or configuration issue with a monitored device and the events generated as a result of the failure. The Server Manager monitors virtual machines, clusters, server processes, hardware objects, OS objects, and load balancing, and records events when a failure or availability issue occurs within the monitored server resources or if any of the monitored resources reaches a violation threshold. The SIA components record events received by EMC ControlCenter and other third party storage products, and performs root cause and impact analysis upon detection of a storage availability failure. The SAM Adapters extract information using SNMP and Syslog, and normalizes input for root cause analysis, enabling monitoring, root cause analysis and notification of events occurring in proprietary third-party systems. The Business Impact Manager associates monitored devices with business elements, assigning an impact value to each event that is related to a business entity, enabling operators to quickly identify and respond to issues which have a high business impact.

When audit events relating to the monitored network resources reach the Service Assurance Manager they are analyzed to determine the root cause of the event. The system uses patented Codebook Correlation Technology. This set of algorithms computes a correlation between the set of possible symptoms and the root cause that can best explain the symptoms, based on the nature of the symptoms and the network topology, which is gathered from the various discovery components. Upon detection of an availability violation, the SAM notifies network operators of the failure condition and monitors responses to the notifications to ensure that the failure conditions are corrected. It also automates response procedures using a predefined set of tools and escalation policies. Events, tools, and notifications are only displayed to authorized roles. The Business Dashboard, Global Console, and Web Console are used to view events and notifications, which are restricted to authorized operators.

TOE Security Functional Requirements Satisfied: EXT_INX_MDC.1, EXT_INX_RCA.1, EXT_INX_ARP.1, EXT_INX_RDR.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 extended and Part 3 of the Common Criteria Standard 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 19 - Threats:Objectives Mapping

Threats	Objectives	Rationale
T.PRIVIL An unauthorized individual may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	O.IDAUTH 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.IDAUTH satifies this threat.
	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.	O.PROTECT mitigates this threat by preventing unauthorized access to TOE functions and data.
T.TAMPERING A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	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 audit events of actions on the TOE with security relevance which may be indicative of misuse.	The objective O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded.
	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.

Threats	Objectives	Rationale
	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.	O.PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification.
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.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.AUDIT The TOE must record audit events of actions on the TOE with security relevance which may be indicative of misuse.	The objective O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	The objective O.IDAUTH ensures that users are identified and authenticated prior to gaining access to TOE security data.
T.AVAIL An unauthorized individual might disrupt the availability or performance of IP networks, servers or storage in the TOE environment.	O.MONITOR The TOE must gather, analyze, and present information about all events that are indicative of unavailability or poor performance of IP networks, servers, and networked storage.	O.MONITOR mitigates this threat by collecting resource data on monitored assets, which can be used to provide valuable incident response information.
	O.ROOTANL The TOE must be able to perform root cause analysis to detect conditions that affect the availability or performance of monitored resources.	O.ROOTANL mitigates this threat by performing analysis when availability conditions occur and can send alerts to the TOE operator or perform action on the operator's behalf.
T.AVAIL2 The root cause of an extended disruption of service provided by the TOE environment may not be immediately apparent, exhausting time and personnel resources to identify, troubleshoot, and correct the root condition, potentially incurring a financial loss or other collateral damage to the organization.	O.ROOTANL The TOE must be able to perform root cause analysis to detect conditions that affect the availability or performance of monitored resources.	O.ROOTANL mitigates this threat by performing advanced analysis on monitored resource data and can identify the root cause, supressing all other incident-related data, allowing the operator to quickly and effectively respond to the service disruption and minimize the troubleshooting efforts.

Threats	Objectives	Rationale
T.AVAIL3 Resources in the TOE environment might become over-allocated, causing a denial of service condition when resources are exhausted.	O.MONITOR The TOE must gather, analyze, and present information about all events that are indicative of unavailability or poor performance of IP networks, servers, and networked storage.	O.MONITOR mitigates this threat by monitoring resources in the TOE environment and can alert operators to potential denial of service conditions based on threshold values.
T.COMINT An unauthorized individual may attempt to compromise the security of the data collected and produced by the TOE by bypassing a security mechanism.	O.AUDIT The TOE must record audit events of actions on the TOE with security relevance which may be indicative of misuse.	O.AUDIT ensures that all accesses to the TOE are recorded, thus allowing for operators to detect unauthorized access.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.IDAUTH requires identification and authentication by authorized users, thus mitigating this threat.
	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.	O.PROTECT mitigates this threat by preventing unauthorized modifications of TOE functions.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS mitigates this threat by preventing access to unauthorized individuals.
	O.SECURE The TOE must ensure the security of all audit and system data.	O.SECURE mitigates this threat by preventing unauthorized modification of audit and system data.
T.EAVESDROP An external attacker might listen in on data communications traversing public networks, potentially exposing sensitive infrastructure information.	OE.SUPPORT The TOE environment must support the applicable protocols necessary for protection of TOE data across hostile networks.	OE.SUPPORT mitigates this threat by providing support for secure protocols which can be used to send sensitive resource information across public or hostile networks.

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

Table 20 - Policies:Objectives Mapping

Policies	Objectives	Rationale
P.MANAGE	O.ADMIN	O.ADMIN ensures that the TOE

Policies	Objectives	Rationale
The TOE may only be managed by authorized users.	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.	provides the necessary tools to support the P.MANAGE policy.
P.INTEGRITY Data collected and produced by the TOE must be protected from modification.	O.AUDIT The TOE must record audit events of actions on the TOE with security relevance which may be indicative of misuse.	O.AUDIT ensures that the TOE records events pertaining modifications to system 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.	O.PROTECT ensures that the TOE protects audit and system data to meet this policy.
P.ESCALATE The organization must have a defined incident escalation policy with procedures for responding to performance or availability conditions occurring within critical IT assets.	O.MONITOR The TOE must gather, analyze, and present information about all events that are indicative of unavailability or poor performance of IP networks, servers, and networked storage.	O.MONITOR ensures that all monitored resource data is made available to TOE operators.
	O.ROOTANL The TOE must be able to perform root cause analysis to detect conditions that affect the availability or performance of monitored resources.	O.ROOTANL ensures that performance and availability coniditions are detected appropriately.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 21 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.	OE.PLATFORM The TOE hardware and OS must support all required TOE functions.	OE.PLATFORM ensures that the TOE hardware and OS supports the TOE functions.
A.NETCON The TOE environment provides the network connectivity required	OE.AVAIL The TOE environment must be implemented such that the TOE is	OE.AVAIL satisfies the assumption that the TOE environment will provide the appropriate

Assumptions	Objectives	Rationale
to allow the TOE to monitor its resources.	available and reachable from the monitored network in order to perform its intended function.	connectivity to allow the TOE to perform its function.
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 satifies the assumption that the environment provides reliable timestamps to the TOE.
A.LOCATE The TOE is located within a controlled access facility.	OE.PHYSICAL The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	Physical security is provided within the TOE environment to provide appropriate protection to the 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 satifies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE	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.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.SECURE The communication between the TOE and its monitored resources will be protected from alteration or impersonation.	OE.SUPPORT The TOE environment must support the applicable protocols necessary for protection of TOE data across hostile networks.	OE.SUPPORT satisfies the assumption that communication between the TOE and its monitored resources cannot be tampered with or disclosed to unauthorized individuals by using secure protocols for communication across hostile networks.

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 EXT_INX requirements was created to specifically address availability of monitored resources. Resources include network devices, servers, and storage. The FAU: Security Audit family was used as a model for creating these requirements. The purpose of this family of requirements is to classify a new TSF which enforces the availability of TOE-monitored resources in the TOE environment. Because availability is a quality of the Confidentiality, Integrity, and Availability (CIA) Information Security Model, the enforcement of availability can be considered a security function. There exist SFRs that deal with resource utilization, fault tolerance, and protection of TOE functions, however, they pertain mainly to the TOE itself and not assets outside of the TOE boundary. Security audit SFRs apply to security actions performed on or by the TOE, but not devices the TOE monitors. This new family provides a set of criteria by which the enforcement of availability of monitored devices and resources can be measured. The only dependency of these requirements is the provisioning of reliable timestamps (FPT_STM.1). 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 Rationale for Extended Security Assurance Requirements

No extended Security Assurance Requirements were defined.

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 22 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
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(a) 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_MTD.1(b) 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	The requirement meets the objective by ensuring that the

Objective	Requirements Addressing the Objective	Rationale
	functions	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 audit events of actions on the TOE with security relevance which may be indicative of misuse.	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_SAA.1 Potential violation analysis	The requirement meets the objective by ensuring that a collection of security events that accummulate up to a specified threshold indicate a potential security violation.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensure that the TOE provides the ability to review logs.
O.IDAUTH 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 using security attributes to determine authorization for TOE functions based on the TOE authentication policy.
	FIA_UAU.1 User authentication before any action	The requirement meets the objective by requiring TOE operators to authenticate themselves prior to accessing TOE administrative functions.
	FIA_UID.1 User identification before any action	The requirement meets the objective by requiring authorized TOE operators to identify themselves prior to accessing TOE administrative functions.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE grants access only to TOE functions based on the role specified.
O.PROTECT The TOE must ensure the integrity of audit and system data by	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that only authorized administrators may

Objective	Requirements Addressing the Objective	Rationale
protecting itself from unauthorized modifications and access to its functions and data.		delete or alter information in the audit logs.
	FIA_ATD.1 User attribute definition	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by implementing security attribute-based access control.
	FIA_UAU.1 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_UID.1 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 unauthorized modification. The TOE does this by ensuring that only privileged users may manage the security behaviour of the TOE.
	FMT_MTD.1(a) 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.
	FMT_MTD.1(b) 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.
O.ACCESS The TOE must allow authorized	FIA_ATD.1 User attribute definition	The requirement meets the objective by requiring users to

Objective	Requirements Addressing the Objective	Rationale
users to access only appropriate TOE functions and data.		possess security attributes used to determine authorization based on the TOE authentication policy.
	FIA_UAU.1 User authentication before any action	The requirement meets the objective by ensuring that the TOE provides access to TOE functions and data only to users who have successfully authenticated.
	FIA_UID.1 User identification before any action	The requirement meets the objective by ensuring that the TOE provides access to TOE functions and data only to users who have successfully identified themselves.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE only allows authorized administrators to control behavior of TSFs.
	FMT_MTD.1(a) Management of TSF data	The requirement meets the objective by ensuring that the TOE only allows authorized users to query and modify TSF data.
	FMT_MTD.1(b) Management of TSF data	The requirement meets the objective by ensuring that the TOE only allows authorized users to query and modify TSF data.
	FTA_TAB.1 TOE access banner	The requirement meets this objective by providing individuals with a security warning implying that unauthorized access is prohibited.
O.SECURE The TOE must ensure the security of all audit and system data.	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by preventing unauthorized deletion of security audit records.
	FMT_MTD.1(a) Management of TSF data	The requirement meets the objective my ensuring that the TOE restricts modification of TOE data to authorized users.
	FMT_MTD.1(b) Management of TSF data	The requirement meets the objective my ensuring that the TOE restricts modification of TOE data to authorized users.
O.MONITOR	EXT_INX_ARP.1	The requirement meets the

Objective	Requirements Addressing the Objective	Rationale
The TOE must gather, analyze, and present information about all events that are indicative of unavailability or poor performance of IP networks, servers, and networked storage.	Resource availability alarms	objective by providing notifications to TOE operators when a threshold is met that indicates a violation of resource availability.
	EXT_INX_MDC.1 Monitored resource data collection	The requirement meets the objective by parsing collected resource data into a common event format.
	EXT_INX_RCA.1 Root cause analysis	The requirement meets the objective by performing analysis on event data to pinpoint root cause of a service disruption. This is done by comparing collected resource event data to a set of signatures based on known behavior models.
	EXT_INX_RDR.1 Restricted data review	The requirement meets the objective by restricting the collected resource data to authorized TOE operators.
O.ROOTANL The TOE must be able to perform root cause analysis to detect conditions that affect the availability or performance of monitored resources.	EXT_INX_ARP.1 Resource availability alarms	The requirement meets the objective by analyzing collected resource data and providing notifications to TOE operators when a threshold it met that indicates a violation of resource availability.
	EXT_INX_MDC.1 Monitored resource data collection	The requirement meets the objective by providing a mechanism for collecting monitored resource data.
	EXT_INX_RCA.1 Root cause analysis	The requirement meets the objective by performing root cause analysis. This is done by comparing the collected resource data to a set of signatures based on known event behavior models.

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.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 23 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 23 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	No	Provided by OE.TIME
FAU_SAA.1	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FIA_ATD.1	No dependencies	✓	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UID.1	No dependencies	✓	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MTD.1(a)	FMT_SMF.1	✓	
FMT_MTD.1(b)	FMT_SMF.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	
FTA_TAB.1	No dependencies	✓	
EXT_INX_ARP.1	EXT_INX_MDC.1	✓	
EXT_INX_MDC.1	FPT_STM.1	No	Provided by OE.TIME
EXT_INX_RCA.1	EXT_INX_MDC.1	✓	
EXT_INX_RDR.1	No dependencies	✓	

9 Acronyms and Terms

This section describes the acronyms and terms.

9.1 Acronyms

Table 24 - Acronyms

Acronym	Definition
API	Application Programming Interface
AS	Advanced Server
ARS	Action Request System
BGP	Border Gateway Protocol
CC	Common Criteria
CEM	Common Evaluation Methodology
CIA	Confidentiality, Integrity, Availability
CM	Configuration Management
CLI	Command Line Interface
CPU	Central Processing Unit
CVCLI	Command View Command Line Interface
EAL	Evaluation Assurance Level
EIGRP	Enhanced Interior Gateway Routing Protocol
EISM	EMC Ionix Server Manager
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICIM	Ionix Common Information Model
ICMP	Internet Control Message Protocol
ID	Identification
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface
IS-IS	Intermediate System to Intermediate System
IT	Information Technology
ITOps	IT Operations

Acronym	Definition
JDBC	Java Database Connectivity
MAC	Media Access Control
MB	Megabyte
NAS	Network Attached Storage
NOC	Network Operations Center
ODBC	Open Database Connectivity
OS	Operating System
OSI	Open Systems Interconnection
OSP	Organizational Security Policy
OSPF	Open Shortest Path First
PP	Protection Profile
RAM	Random Access Memory
SAM	Service Assurance Management/Manager
SAN	Storage area network
SAR	Security Assurance Requirement
SDI	SQL Data Interface
SFP	Security Function Policy
SFR	Security Functional Requirement
SIA	Storage Insight for Availability
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SP	Service Pack
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
WMI	Windows Management Instrumentation
XML	eXtensible Markup Language

9.2 Terminology

CIA Information Security Model – A basic model by which Information Security policies are developed. CIA, as defined in the table in section 9.1, is an acronym for Confidentiality, Integrity, and Availability.
Viewlet – A graphical representation of summary information presented in a modular format

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com