IBM Tivoli Netcool OMNIbus v7.1 with IBM Tivoli Netcool Webtop™ v2.0

Security Target

Version 2.9
Ref: OMNIbus_ST
July 28, 2008

Document Control

Note: Micromuse, Inc was acquired by IBM Corporation on February 15, 2006.

Acknowledgements
TOE Distributor
The distributor of the TOE is:
IBM Corp.

Contact:
Evaluation Sponsor
The evaluation sponsor is:
IBM Corp.
12120 Sunset Hills Road
Suite 202
Reston, VA 20190
USA

Phone: 703-464-6082
FAX: 703-464-6099

Contents

References

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004

1. Introduction

This section contains document management and overview information necessary to allow the ST to be registered. The ST identification provides the labelling and descriptive information necessary to identify, catalogue, register, and cross-reference the ST. The ST overview summarises the Target of Evaluation (TOE) in narrative form and provides sufficient information for a potential user to determine whether the TOE is of interest. The conventions section provides an explanation of how this document is organised and the terms section gives a basic definition of terms which are specific to this ST.

1.1. Security Target Identification

Title: IBM Tivoli Netcool OMNIbus v7.1 with IBM Tivoli Netcool Webtop v2.0 Security Target

ST Version: 2.9

Target of Evaluation: IBM Tivoli Netcool OMNIbus v7.1 with IBM Tivoli Netcool Webtop v2.0

IBM Tivoli Netcool OMNIbus Version: v7.1

IBM Tivoli Netcool Webtop Version: v2.0

Evaluation Assurance Level: EAL2

1.2. Overview

IBM Tivoli Netcool OMNIbus v7.1 is an enterprise network and service level management (NMS-SLM) system that collects enterprise-wide event information from many different network data sources and presents a simplified view of this information to operators and administrators. IBM Tivoli Netcool Webtop v2.0 is a web server application that processes network alert information and presents the data output to users so that they can monitor events in their IBM Tivoli Netcool OMNIbus environment. The server publishes alert data from one or more IBM Tivoli Netcool OMNIbus datasources in real-time so that operatives can view pages that display this information in a web browser.

IBM Tivoli Netcool OMNIbus v7.1 with IBM Tivoli Netcool Webtop v2.0 may hereafter also be referred to as Netcool OMNIbus with Netcool Webtop or the TOE in this document. Each component may be referenced as a standalone term when referring to the respective component.

1.3. CC Conformance Claims

This TOE and ST are consistent with the following specifications:

- Conformant to Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, January 2004
- Conformant (at EAL2 with SOF-basic) to Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, January 2004
- Conformant with all International interpretations with effective dates on or before October 27, 2004, including NIAP Interpretation: I-0432.

1.4. Conventions

This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the reader.
The CC identifies four operations to be performed on requirements; assignment, iteration, refinement, and selection. These are defined in paragraph 169 of Part 1 of the CC (section 4.4.1.3.2).

a) The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

b) The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*.

c) The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value]. Curly braces are used to denote attributes of assignments {attributes of assignments}.

d) The **iteration** operation is used when a component is repeated with varying operations. Showing the iteration number in parenthesis following the component identifier and element identifier (iteration_number) denotes iteration.

1.5. List of Abbreviations

ACL Access Control List
AEL Active Event List
CC Common Criteria
NCO Netcool OMNIbus
DAC Discretionary Access Control
DES Data Encryption Standard
EAL Evaluation Assurance Level
GID Group Identifier
ICMP Internet Control Message Protocol
LEL Lightweight Event List
PAM Pluggable Authentication Module
SOF Strength of Function
SFP Security Function Policy
SFR Security Functional Requirement
SLM Service Level Management
SSL Secure Sockets Layer
ST Security Target
TCP Transport Control Protocol
TOE Target of Evaluation
TSC TOE Scope of Control
TSF TOE Security Functions
TSP TOE Security Policy
UID User Identifier
NMS Network Management System
SLM Service Level Management

1.6. Terminology

Netcool OMNIbus Term	Function
OMNIbus	IBM core product
Object Server	Data aggregation and consolidation component
Probe	Data capture component
Gateway	Data exchange component
Datasources	Devices/products being monitored
Operatives	Users of the TOE
Operator(s)	"Operator(s)" is used to mean TOE user(s) with limited permissions.
Authorized Administrator(s)	"Authorized Administrator(s)" is used to mean TOE user(s) with full access.
User(s)	"User(s)" is used to mean all TOE users, both the "Operator(s)" and "Authorized Administrator(s)".

Table 1 – IBM Terminology

2. TOE Description

2.1. Introduction

The TOE is made up of several (eight) components. Netcool OMNIbus is an enterprise network and service level management (NMS-SLM) system that collects enterprise-wide event information from many different network data sources and presents a simplified view of this information to operators and administrators. Netcool OMNIbus tracks alert information in a high-performance, in-memory database and presents information of interest to specifically identified and authenticated users through individually configurable filters and views. User activity can be accounted for and audited using the administration facilities provided by Netcool OMNIbus. Users can access the event information assigned to them from a client application or via a Java-enabled browser connecting to Netcool Webtop (an applet is available for greater functionality). Netcool Webtop is a web server application that processes network alert information and presents the data output to users so that they can monitor events in their Netcool OMNIbus environment. The server publishes alert data from one or more Netcool OMNIbus datasources in real-time so that operatives can view pages that display this information in a web browser. Further details about the components of the TOE follow.

Note: The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

2.1.1. ObjectServer

The ObjectServer is a proprietary relational database server at the core of Netcool OMNIbus. Alert information is forwarded to the ObjectServer from external programs such as probes and gateways, stored and managed in database tables, and displayed in the event list. In a standard configuration, alerts are forwarded directly to the ObjectServer. The TOE is run in “secure” mode. The “secure” mode forces encryption and authentication among remote TOE components. Whilst secure mode is running the ObjectServer authenticates probe and gateway connection requests by requiring a username and a password which are encrypted during transmission. The ObjectServer supports replication and persistence of data using disk-based checkpoints and logs. Checkpoints write all data to disk at system-defined intervals to enable data recovery if the server stops unexpectedly. Between checkpoints, additional modifications to the database are logged to disk. The ObjectServer stores administrator passwords in ciphertext, and they are encrypted with UNIX *crypt*, which provides Data Encryption Standard (DES) encryption of the password.

2.1.2. Webtop

Netcool Webtop is an Apache Tomcat-based web server application that processes network alert information and presents the data output to users so that they can monitor events. The server publishes alert data from one or more Netcool OMNIbus ObjectServer datasources in real-time so that users can view this information in a web browser.

The Webtop users must go through the I&A mechanism to gain access. When they connect to Netcool Webtop they are presented with pages, defined by an administrator, that allow them to view alert data in a number of ways. The main event display components are described below:

a) The Java-based active event list (AEL) allows clients to execute actions such as acknowledging alerts, viewing alert journals, taking ownership of alerts, running tools, and so forth.

b) The dynamic HTML lightweight event list (LEL) provides clients with the data filtering, data sorting, and information drill-down capabilities of the AEL.

c) The HTML tableview component provides clients with a static event list in the form of a table showing a defined set of alerts. The non-interactive tableview provides an immediate snapshot of alert status within a monitored system.

2.1.3. ObjectServer Gateway

ObjectServer gateways are used to replicate table data (for example, alert-related data) between different Netcool OMNIbus ObjectServers. ObjectServer gateways consist of readers and writers.
Readers extract alerts from a source ObjectServer. Writers send the alert data to a target ObjectServer.
A reader extracts alerts from an ObjectServer. There is only type of reader: the ObjectServer reader. Once the reader is started and the gateway attempts to open a connection to the source ObjectServer. If the gateway succeeds in opening the connection, it immediately starts to read alerts from the ObjectServer.

Writers send the alerts acquired by a reader to the destination application or ObjectServer. Once the writer is started, the gateway attempts to establish the connection to the alert destination ObjectServer. The writer sends alerts received from the source ObjectServer.

Routes create the link between readers and writers. Once the route has been created, the connection between a reader and writer is established. Any alerts received by the source ObjectServer are read by the reader, passed through the route to the writer, and written into the destination ObjectServer.

2.1.4. Administration Client

This TOE component is also known as “Administrator” during installation and appears as “Administrator Config” after installation.

The Administrator provides a simple graphical user interface from which to configure and manage the ObjectServers.

2.1.5. User Client

This TOE component is also known as “Desktop” during installation and appears as “Even List” after installation.

The desktop User Client is an integrated suite of graphical tools used to view and manage alerts and to configure how alert information is presented.

Alert information is delivered in a format that allows users to quickly determine the availability of services on a network. When an alert cause has been identified, desktop tools enable users to resolve problems quickly.

2.1.6. Probes

Probes detect and acquire event data, and forward the data to the ObjectServer as alerts. Probes use the logic specified in a rules file to manipulate the event elements before converting them into an alert, which is sent to the ObjectServer and populates the fields of the alerts.status table.

Each probe is uniquely designed to acquire event data from a specific source. Probes can acquire data from any stable data source, including devices, databases, and log files. The probes can be installed on the ObjectServer or on a remote host.

Caution: It should be noted that the probes included in this evaluation only use protocols listed here, Syslog, SNMPv1, SNMPv2c, & SNMPv3 for collecting raw data from monitored devices. The non-secure (clear-text) protocols are Syslog, SNMPv1, & SNMPv2c. No other probes were tested. The customer assumes the risk of using non-evaluated probes in an operational environment. The ST section 5 enumerates functional and security requirements that non-evaluated probes have to meet in order to

securely authenticate and communicate with the TOE. For example, the probes must be capable of authenticating and using an encrypted communication channel to the ObjectServer.

2.1.7. Flex License Server

Flex Licensing is a standalone server component that provides licensing functionality for the Netcool suite of products. This component is based on the premise that license administration and maintenance can be simplified by centralizing license data on one or more designated license servers, with licenses being drawn from a server as necessary.

Before running any Netcool product, Flex Licensing must be installed and configured on at least one license server in your environment. Customers must ensure that the requisite license files containing license feature codes for the Netcool products and related components are added. A license server can be shared between multiple Netcool products.

2.1.8. Security Manager

The Security Manager is the repository for role and group information for Webtop. The Webtop uses the Security Manager as its only source of authentication. In this evaluation, the Security Manager points to ObjectServer for user authentication.

2.2. TOE Architecture

The diagrams below show how the TOE components are interconnected in a number of possible deployment configurations. These diagrams also illustrate the secure connections between different TOE components, and the separation between TOE components and the IT Environment.

This is software only TOE. The underlying hosts' hardware and OS of any of the TOE components are not part of the TOE. The monitored devices are not part of the TOE either. The TOE components shown in below diagram are the User Client, Administration Client, Webtop Server, ObjectServer, Gateway, Flex License Server and Probes.

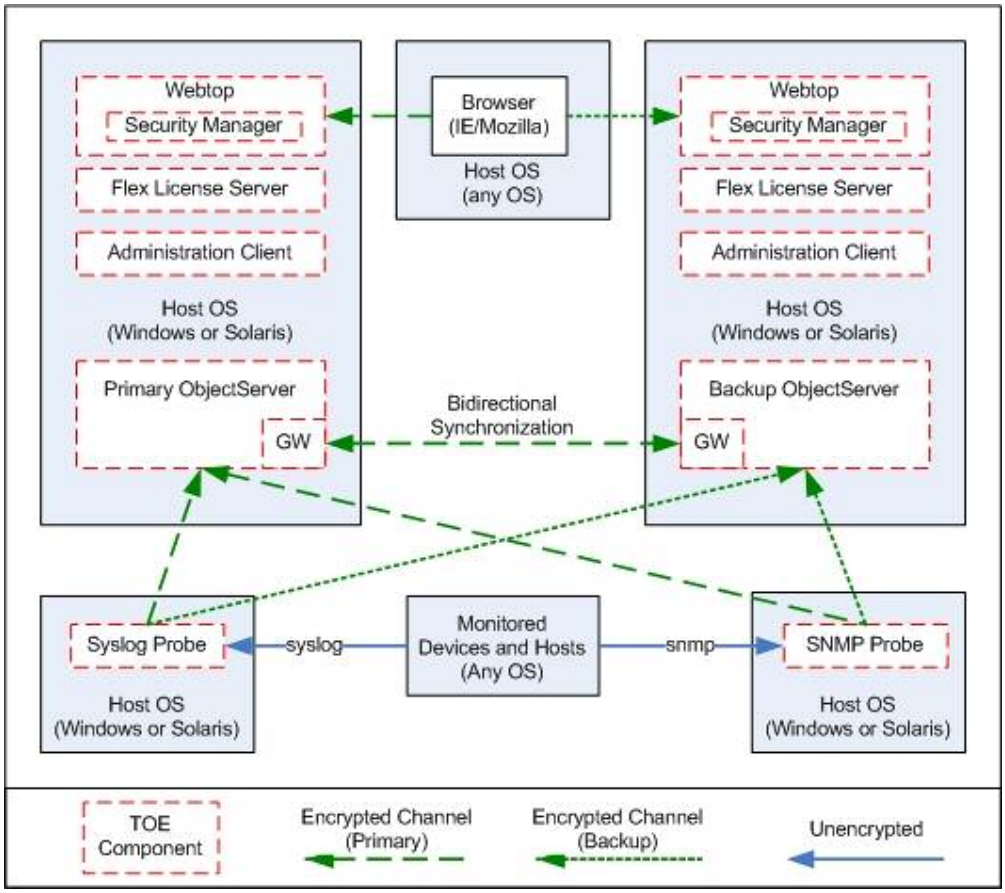

Figure 1: Deployment Scenario 1 & TOE Boundary

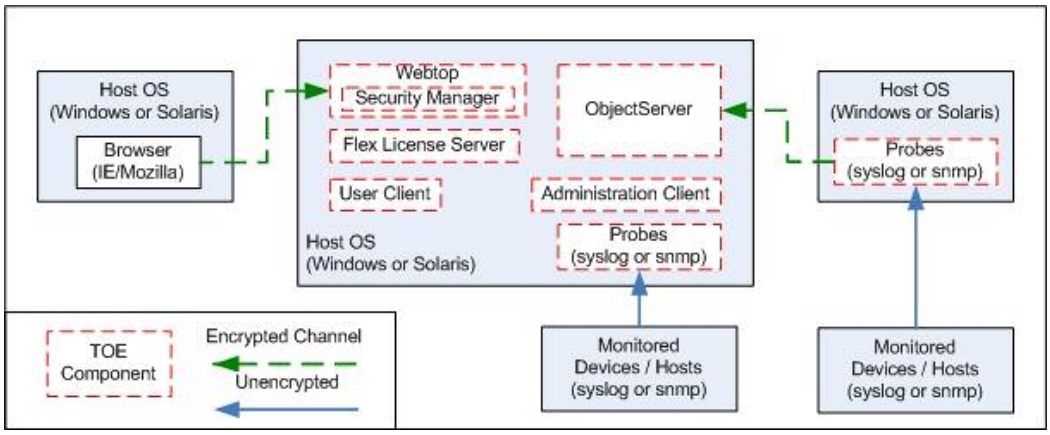

Figure 2: Deployment Scenario 2 & TOE Boundary

2.3. TOE Components, TOE Environment and Evaluated Configuration

2.3.1. ObjectServer

TOE Components	
Software	Netcool OMNIbus v7.1, Flex License Server v1.0.31
Non-TOE Components	
Software	JRE v1.5
Operating System	Solaris 8, 9, 10 SPARC, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2003 Server Note: Vendor recommends that operating system has all the recommended patches, including the latest patch levels, installed.
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Hard Disk Space	Minimum 500Mb
Network Interface Card	Any capable of handling TCP/IP connections.

Table 2 – ObjectServer Evaluated Configuration

2.3.2. Webtop

Server	
TOE Components	
Software	Netcool Webtop v2.0, Netcool Security Manager v1.3.939.0
Non-TOE Components	
Software	JRE v1.4.2 or 1.5
Operating System	Solaris 8, 9, 10 SPARC, Windows 2000 Professional, Windows 2000 Advanced Server, Windows XP Professional, Windows 2003 Note: Vendor recommends that operating system has all the recommended patches, including the latest patch levels, installed.
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Hard Disk Space	Minimum 500Mb
Client	

Software	Windows: MS Internet Explorer 6 or Mozilla Firefox 1.5 and 1.07 Solaris: Mozilla Firefox 1.5 and 1.07
Java Version	Java Virtual Machine Plug-in 1.4.2 or 1.5
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Network Interface Card	Any capable of handling TCP/IP connections.

Note: If Webtopv2.0 is installed on the same machine as ObjectServer, the minimum requirements listed for both components must be added up/combined. The OS options will be restricted to the common OS listed.

Table 3 – Webtop Evaluated Configuration

2.3.3. Gateway

Gateway is part of Netcool OMNIbus v7.1 software package and is installed with ObjectServer, see Table 2. There is no other additional hardware or software needed for this piece of TOE.

Note:
1- The Gateway is installed with ObjectServer installation. The term ObjectServer is used in this document to mean ObjectServer + Gateway.

2.3.4. Administration Client

TOE Components	
Software	Netcool OMNIbus v7.1
Non-TOE Components	
Software	JRE v1.5
Operating System	Solaris 8, 9, 10 SPARC, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2003 Server Note: Vendor recommends that operating system has all the recommended patches, including the latest patch levels, installed.
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Hard Disk Space	Minimum 500Mb
Network Interface Card	Any capable of handling TCP/IP connections.

Note: If Administration Client is installed on the same machine as ObjectServer, the minimum requirements listed for ObjectServer component must be followed and are sufficient for both components.

Table 4 – Administration Client Evaluated Configuration

2.3.5. User Client

TOE Components	
Software	Netcool OMNIbus v7.1
Non-TOE Components	
Software	JRE v1.5
Operating System	Solaris 8, 9, 10 SPARC, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Professional, Windows 2000 XP, Windows 2003 Server Note: Vendor recommends that operating system has all the recommended patches, including the latest patch levels, installed.
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Hard Disk Space	Minimum 500Mb
Network Interface Card	Any capable of handling TCP/IP connections.

Note: If User Client is installed on the same machine as ObjectServer, the minimum requirements listed for ObjectServer component must be followed and are sufficient for both components.

Table 5 – User Client Evaluated Configuration

2.3.6. Probes

The TOE includes only the common library (libopl), which is shared by the majority of the probes. Any probes not using libopl will be outside the scope of the evaluation. These Probes can be installed on the same machine on which one of the Netcool OMNIbus v7.1 software components are installed or on a remote machine. The only probes included in this evaluation are the ones that use Syslog and SNMP protocols to collect raw data from monitored devices.

2.3.7. Flex License Server

Flex License Server v1.0.31 is installed with ObjectServer, see Table 2. There is no other additional hardware or software needed for this piece of TOE.

2.3.8. Security Manager

The Netcool Security Manager v1.3 (with Interim Fix 1) is installed with the Webtop, see Table 3. There is no additional hardware or software needed for this piece of the TOE. The Security Manager works with the Webtop to authenticate Webtop users via ObjectServer.

Notes:
1- The term Security Manager v1.3 is used in this document to mean Security Manager v1.3 + Interim Fix-1.
2- The Security Managers is installed with the Webtop installation. The term Webtop is used in this document to mean Webtop + Security Manager.

2.4. Physical Boundary

The TOE physical boundary includes the TOE components (software) listed in section 2.3 and sub-sections. Figure 1 above illustrates the physical boundary of the TOE, and the TOE boundary is denoted with the dotted line. The figure also illustrates the interfaces between each of the TOE components and devices.

The TOE does not include the security devices from which data is collected, the operating system and the underlying hardware hosting any Netcool OMNIbus component, the network, the NICs, Probes not implementing the common library (libopl), Process Control (nco_pa & nco_pad utility & commands) product component, and the System Utilities "OMNIbus Settings". The Product components "Process Control" (also known as "Process Agent") must not be installed. The System Utilities "OMNIbus Settings" must not be used in the evaluated configuration.

2.4.1. TOE Physical Boundary, TOE Components, TOE Environment and Deployment Examples

To explain the TOE physical boundary, TOE components and TOE Environment, following three deployment examples are provided. These are examples only and not all possible deployment scenarios for the TOE. The TOE can be deployed in distributed environment as described in sections 2.2 and 2.3.

2.4.1.1. Minimum Possible Deployment Example

The following example explains what will be required for a minimum possible deployment of the TOE.

- One ObjectServer
- One Flex License Server
- One User Client
- One Administration Client
- Probes allowed in the evaluated configuration

Note: All of these TOE components can be installed on 1 machine.

TOE Components	
Software	Netcool OMNIbus v7.1, Flex License Server v1.0.31

Non-TOE Components	
Software	JRE v1.5
Operating System	Solaris 8, 9, 10 SPARC, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2003 Server Note: Vendor recommends that operating system has all the recommended patches, including the latest patch levels, installed.
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Hard Disk Space	Minimum 500Mb
Network Interface Card	Any capable of handling TCP/IP connections.

2.4.1.2. Minimum Possible Deployment Example with Webtop

The following example explains what will be required for a minimum possible deployment with Webtop for the TOE. Webtop is an additional web based GUI interface for the TOE and makes it easier for the user to manage the TOE using a browser.

- One ObjectServer
- One Flex License Server
- One User Client
- One Administration Client
- Probes allowed in the evaluated configuration
- One Webtop

Note: All of these TOE components can be installed on 1 machine.

TOE Components	
Software	Netcool OMNIbus v7.1, Flex License Server v1.0.31, Netcool Webtop v2.0, Netcool Security Manager v1.3
Non-TOE Components	
Software	JRE v1.5
Operating System	Solaris 8, 9, 10 SPARC, Windows 2000 Advanced Server, Windows 2003 Note: Vendor recommends that operating system has all the recommended patches, including the latest patch levels, installed.
CPU	Minimum 600MHz
Memory	Minimum 1024Mb
Hard Disk Space	Minimum 1024Mb
Network Interface Card	Any capable of handling TCP/IP connections.
Minimum Requirements for Webtop Client (Web/Internet Browser)	
Software	Windows: MS Internet Explorer 6 or Mozilla Firefox 1.5 and 1.07 Solaris: Mozilla Firefox 1.5 and 1.07
Java Version	Java Virtual Machine Plug-in 1.4.2 or 1.5
CPU	Minimum 300MHz
Memory	Minimum 512Mb
Network Interface Card	Any capable of handling TCP/IP connections.

2.4.1.3. Other Deployment Options

Other possible deployment for this TOE can take any of the forms described in sections 2.2 and 2.3. In which case it can have following TOE components.

- One or more ObjectServer
- One or more Flex License Server
- One or more User Client
- One or more Administration Client
- Probes allowed in the evaluated configuration
- One or more Webtop

Note: Any distributed deployment as long as it is within the physical boundary described in sections 2.2, 2.3 and 2.4 will be compliant with the evaluated TOE.

2.5. Logical Boundary

The logical boundary of the TOE includes the security functionality described in the following sections.

Keys: E=Enforcing & S=Supporting

Security Functions to TOE Components mapping	ObjectServer	Administration Client	User Client	Webtop	Probes
IA	E	S	S	S	
AC	E	S			
AU	E	S	S	S	S
COM	E	S	S	S	S
MAN	E	S	S	S	S
REP	E				

Figure 3: Logical Boundary Security Functions to TOE Components Mappings

2.5.1. Identification/Authentication (IA)

The TOE supports two types of users: An “Authorized Administrator” with complete control over all aspects of configuration and TSF Data, and a “Operator" whose access is limited to viewing and managing alerts to determine the availability of services on a network. Both of these user types are maintain in the ObjectServer. The internal ObjectServer authentication mechanism is used to perform I&A. The Object Server stores unique usernames, application ID and encrypted passwords. Once these authentication parameters are collected, the ObjectServer compares it with the stored encrypted password, based on the result of this comparison, the authentication is either successful or denied. The Administration Client, the User Client and the Webtop require operators to identify and authenticate before accessing the system. The TOE maps the operator to a set of permissions defined by the Administrator.

2.5.2. Discretionary Access Control (AC)

When an operator authenticates, the TOE controls the level of access granted to that operator. These permissions are contained within the assigned group of the operator and are configured by the Administrator.

2.5.3. Audit (AU)

Actions taken by operators generate audit records. These records contain the date, time, event type, identity of the analyst, and outcome of the action. Only the Administrator has the ability to review and clear these records. Auditable events include the following: start-up and shutdown of audit functions; logon attempts; creation, deletion and modification of administrator / operator account; and other events discussed in the Security Functions section of this document.

2.5.4. Communications (COM)

The TOE provides robust, secure communications between components. Components must successfully identify and authenticate to an ObjectServer prior to transferring data. If a Probe cannot establish a connection with its primary ObjectServer, then it will attempt to establish a connection to a secondary ObjectServer. If a secure communications establishment to the primary and secondary ObjectServers, the Probe will store data locally and not transmit to the ObjectServer.

2.5.5. Management (MAN)

The TOE offers various methods of management of security functions, including user account management, accounting and audit management, cryptographic management and replication management.

2.5.6. Replication (REP)

The TOE replicates data between ObjectServers to ensure consistency of data. As a result, if a Probe fails to connect to its primary ObjectServer, the connection to the secondary ObjectServer will allow the operators to assume regular operations without downtime or loss of configuration.

3. Security Environment

3.1. Introduction

This section provides the statement of the TOE security environment, which identifies and explains all:

- known and personnel threats countered by either the TOE or by the security environment;
- organizational security policies the TOE must comply with;
- assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

3.2. Threats

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment.

NAME	DESCRIPTION
T.AUD	Activities of unauthorized personnel may go unnoticed.
T.COMPDATA	Event data may be compromised while being transferred between the probes and the ObjectServers.
T.DATABASEFAIL	Database failure may prevent event information from being noticed
T.INSECURE	The TOE may be installed and / or managed insecurely.
T.LOWEXP	An attacker with low attack potential may attempt to bypass the TSF to gain access to the TOE or the assets it protects.
T.NETSEC	Security relevant events occurring on network equipment may go unnoticed.
T.UNAUTH	Unauthorized personnel may attempt to gain access to the facilities and the data available in the TOE.
T.SEL_PRO	An unauthorized person may read, modify or destroy security critical TOE configuration Data.

Table 6 – Threats Countered by TOE

3.3. Organizational Security Policies

There are no organizational security policies or rules with which the TOE must comply.

3.4. Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. This includes information about the physical, personnel, and connectivity aspects of the environment.

The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The operational environment must be managed in accordance with assurance requirements documentation for delivery, operation, and user/administrator guidance. The following specific conditions are assumed to exist in an environment where the TOE is employed.

NAME	DESCRIPTION
A.INSTALL	The TOE is delivered, installed, managed and operated in a secure manner via an internal network only.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.PHYSEC	The ObjectServers, Webtop Server (if used) and Gateway

	components, and network connections between them, must be located in a physically secure environment.
A.PROBE	To enable a Probe to securely store network event data on their local platform in the event of a connectivity interruption between the Probe and the ObjectServer (when the Probe goes into "Store-and-Forward" mode), the Probe log destination must be on a separate, secure volume. This log is secured by the administrator with access controls.
A.SOLARIS	When PAM authentication is used, the ObjectServer will be able to connect to the PAM module on the Solaris machines hosting the ObjectServers.
A.TRUSTED	The TOE will be administered by competent and trusted personnel who will ensure that every user knows that all access credentials must be protected.
A.SEL_PRO	The TOE environment will be configured in such a manner as to prevent an unauthorized person from reading, modifying or destroying security critical TOE configuration data.
A.OSLOGIN	The TOE environment will be configured in such a way to require administrators and users to authenticate prior to performing security-relevant tasks.

Table 7 – Assumptions for Secure Use

4. Security Objectives

This section defines the security objectives of the TSF and its supporting environment. Security objectives, categorised as either security objectives for the TOE, (section 4.1) or security objectives for the environment (section 4.2), reflect the stated intent to counter identified threats. All of the identified threats are addressed under one of the categories below.

4.1. Security Objectives for the TOE

The following are the TOE security objectives:

NAME	DESCRIPTION
O.AUDITING	The TSF must record specified security relevant actions of users of the TOE. The TSF must clearly present this information to authorized administrators.
O.AUDITPROTECT	The TSF must prevent the unauthorized deletion or modification of audit records.
O.AUTHORIZATION	The TSF must ensure that users are identified and authenticated prior to any interaction with the TOE and its resources with the exceptions of Utilities/Startup-Commands. The Utilities/Startup-Commands are, nco_objserv –secure [-name *servername*] , nco_sql (on unix), `nco_sql_crypt,` nco_g_crypt ,nco_objserv -secauditlevel *info*, nco_ssladmin, nco_objserv, nco_ssladmin -> Generate self-signed certificate, setsslreg.exe (on windows) and Servers Editor.
O.DISCRETIONARY_ACCESS	The TSF must control access to resources based on identity of users. The TSF must allow authorized administrators to specify which resources may be accessed by which users.
O.MANAGE	The TSF must provide the IT functions necessary to support the authorized administrators that are responsible for the management of TOE security.
O.REPLICATION	The TSF must ensure that data is replicated consistently between databases.
O.SECURECOMMS	The TSF must securely transfer data between probes and ObjectServers, Administration Client and ObjectServers and User Client and ObjectServers.
O.SEL_PRO	The TSF must provide, in conjunction with the environment, means to prevent unauthorized persons from reading, modifying or destroying security critical TOE configuration Data.

Table 8 – TOE Security Objectives

4.2. Security Objectives for the Environment

The TOE is assumed to be complete and self-contained and, as such, is not dependent upon any other products to perform properly. However, certain objectives with respect to the general operating environment must be met.

NAME	DESCRIPTION
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner that maintains security objectives for the TOE.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains security objectives for the TOE.
OE.LOWEXP	The TOE's operating environment must protect itself against malicious attacks aimed at discovering exploitable

	vulnerabilities from an attacker with low attack potential
OE.PAM	Those responsible for the TOE must ensure that PAM, when deployed, is correctly installed on the Solaris machines hosting the ObjectServers.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to meeting the security objectives are protected from physical attack that might compromise the security objectives for the TOE.
OE.PROBE	Those responsible for the TOE must ensure that all probes can securely store data locally.
OE.SEL_PRO	The TOE environment will be configured in such a manner as to work in conjunction with the TOE to prevent an unauthorized person from reading, modifying or destroying security critical TOE configuration data.
OE.OSLOGIN	The TOE Environment will require authorized administrators to identify and authenticate themselves to the OS (Windows or Solaris)

Table 9 – Environment Security Objectives

5. Security Functional Requirements

The security functional requirements consist of components from Part 2 of the CC. They are listed in the following table. The SFRs for the IT Environment are Proceeded by (ENV) in table (Table 10) below, just for identification and making it easy for the readers of this ST. The explicitly stated SFR have "_EXP" (e.g. FAU_GEN_EXP.1) in the title of the SFR. The section 5.1 describes SFRs for the TOE and section 5.2 describes SFRs for the IT Environment.

Functional Components	
FAU_GEN_EXP.1	Audit data generation
FAU_SAR.1	Audit review
FAU_STG.1 (1)	Protected audit trail storage
FCS_CKM.1	Cryptographic key generation
FCS_COP.1 (1)	Cryptographic operation
FCS_COP.1 (2)	Cryptographic operation (Hashing)
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FIA_AFL.1 (1)	Authentication failure handling (Internal authentication mechanism)
FIA_AFL.1 (2) (ENV)	Authentication failure handling (PAM)
FIA_ATD.1	User attribute definition
FIA_SOS.1 (1)	Verification of secrets (Internal authentication mechanism)
FIA_SOS.1 (2) (ENV)	Verification of secrets (PAM)
FIA_UAU.1	Timing for authentication
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1(1)	Management of security attributes (information flow SFP)
FMT_MSA.1(2)	Management of security attributes (access control SFP)
FMT_MSA.3(1)	Static attribute initialization (information flow SFP)
FMT_MSA.3(2)	Static attribute initialization (access control SFP)
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_STM.1 (ENV)	Reliable time stamps
FPT_TRC.1	Internal TSF consistency
FPT_SEP_EXP.1	Domain separation
FPT_RVM_EXP.1	Reference mediation
FPT_SEP_OS.1 (ENV)	TSF domain separation
FPT_RVM_OS.1 (ENV)	Non-bypassability of the TSP
FIA_UAU_OS.1 (ENV)	User Authentication
FIA_UID_OS.2 (ENV)	User Identification
FAU_STG.1 (2) (ENV)	Protected audit trail storage

Table 10 – Security Functional Requirements

5.1. TOE Security Functional Requirements

5.1.1. Security Audit (FAU)

Audit Data Generation FAU_GEN_EXP.1

FAU_GEN_EXP.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Stop/Start of the audit functions; b) All auditable events for the *not specified* level of audit and; c) [use of authentication mechanism, loss of connection between ObjectServers, creation / deletion / modification of user account].
FAU_GEN_EXP.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event (incl First and Last occurrence), type of event, severity, summary, identifier of event; and b) For each audit event type, based on the auditable event definition of the functional components included in the ST, [none].

Audit Review FAU_SAR.1

FAU_SAR.1.1	The TSF shall provide [authorized administrators] with the capability to read [all audit information] from the audit records:
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Protected Audit Trail Storage FAU_STG.1 (1)

FAU_STG.1.1 (1)	The TSF shall protect the stored audit records from unauthorized deletion.
FAU_STG.1.2 (1)	The TSF shall be able to *prevent* unauthorized modifications to the audit records in the audit trail.

Application Note: There is an iteration of FAU_STG.1 on the TOE and one on the IT Environment. The TOE protects the audit records from unauthorized deletion through enforcing I&A and user access permissions via its interfaces to ObjectServer (Administration Client, User Client, and Webtop). The IT Environment protects the files stored on the underlying OS by enforcing access controls necessary to deny any unauthorized access.

5.1.2. Cryptographic Support (FCS)

Cryptographic Key Generation FCS_CKM.1

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [1024-bit] that meet the following [DES or 3-DES: FIPS PUB 46-2, or Diffie-Hellman: PKCS #3, or RSA: PKCS #1].

Cryptographic Operation FCS_COP.1 (1)

FCS_COP.1.1 (1)	The TSF shall perform [SSL Communication] in accordance with a specified algorithm [DES data encryption or 3-DES data encryption, Diffie-Hellman cryptographic key agreement] and cryptographic key sizes [56-bit DES or 168-bit 3-DES, 1024-bit RSA] that meet the following [DES or 3-DES: FIPS PUB 46-2, or Diffie-Hellman: PKCS #3, or RSA: PKCS #1].

Cryptographic Operation FCS_COP.1 (2) (Hashing)

FCS_COP.1.1 (2)	The TSF shall perform [Password Hashing] in accordance with a specified algorithm [Proprietary Hashing Algorithm generating 128 bit hash] and cryptographic key sizes [not applicable] that meet the following [no standard].

5.1.3. User Data Protection (FDP)

Subset Access Control FDP_ACC.1

FDP_ACC.1.1	The TSF shall enforce the [access control SFP] on [subject: o operators, o authorized administrators; object: o user accounts, o groups, o roles, o network event data tables, o accounting and audit data tables, o triggers, o procedures; operations: o view, o modify, o create, o delete].

Security Attribute Based Access Control FDP_ACF.1

FDP_ACF.1.1	The TSF shall enforce the [access control SFP] to objects based on the following: Subject security attributes: o [operators {userid, password}, o [authorized administrators {userid, password}], Object security attributes: o [user accounts {username, hashed password, groups, restrictions}, o groups {roles, restrictions, users}, o roles {permissions}, o network event data tables {name, row number}, o accounting and audit data tables {name, row number}, o triggers {name}, o procedures {name}].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: o [an operator or authorized administrator may view a network event data table if their user role allows view access to that table; o an operator or authorized administrator may modify a network event data table if their user role allows modify access to that table; o an authorized administrator may create a new network event data table if their user role allows table creation;

- an authorized administrator may view, modify, create or delete a user account/group/role if their user role allows access to user account management;
- an authorized administrator may view an accounting and audit data table if their user role allows view access to that table;
- an authorized administrator may view, modify, create or delete triggers if their user role allows access to that trigger;
- an authorized administrator may view, modify, create or delete procedures if their user role allows access to that procedure.]

FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the: [restrictions within a user account and/or group].

Subset Information Flow Control FDP_IFC.1

FDP_IFC.1.1 The TSF shall enforce the [information flow SFP] on
[subject:
- Administration Client,
- User Client,
- Webtop,
- Probes and
- ObjectServers;

information:
- network events;

operation:
- data transfer from probe to ObjectServer,
- data transfer from Administration Client to ObjectServer,
- data transfer from User Client to ObjectServer,
- data transfer from Webtop to ObjectServer, and
- data replication between ObjectServers].

Simple Security Attributes FDP_IFF.1

FDP_IFF.1.1 The TSF shall enforce the [information flow SFP] based on the following types of subject and information security attributes :
[Subject security attributes :
- (Probes): probe identification;
- (Administration Client): authorized administrator identification;
- (User Client): user identification;
- (Webtop): user identification;
- (ObjectServers): ObjectServer name.

Information security attributes:
- (Probes): probe password and ObjectServer public key;
- (Administration Client): authorized administrator password and ObjectServer public key;
- (User Client): user password and ObjectServer public key;
- (Webtop): user password;
- ObjectServers): all identification data, all password data and ObjectServer private key][1].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold :
[

[1] The ObjectServer public / private key pair is generated during installation.

- Probe to ObjectServer {ObjectServer status = on, probe identification, probe password, encrypted channel}If the ObjectServer is up, it requires probe to provide ID and password, before authenticating and establishing an encrypted channel with the probe ,
- ObjectServer to ObjectServer {ObjectServer status = data awaiting replication, gateway identification, gateway password}If the ObjectServer is waiting to replicate data, it requires the gateway to provide ID and password, before authenticating and starting replication,
- Webtop to ObjectServer {user identification, user password}The ObjectServer requires that the Webtop provide the user ID and password, before authenticating and allowing a session establishment,
- User Client to ObjectServer {user identification, user password, encrypted channel}The ObjectServer requires that the User Client provides the user ID and password, before authenticating and establishing an encrypted channel,
- Administration Client to ObjectServer { authorized administrator identification, authorized administrator password, encrypted channel} The ObjectServer requires that the Administrator Client provides the authorized administrator ID and password, before authenticating and establishing an encrypted channel.

].

FDP_IFF.1.3	The TSF shall enforce the [none].
FDP_IFF.1.4	The TSF shall provide the following [none].
FDP_IFF.1.5	The TSF shall explicitly authorize an information flow based on the following rules: [none].
FDP_IFF.1.6	The TSF shall explicitly deny an information flow based on the following rules [non availability of both ObjectServers will cause information flow to be denied and the information stored locally on the platform the probe is installed on].

5.1.4.Identification and Authentication (FIA)

Authentication Failure Handling FIA_AFL.1 (1)

FIA_AFL.1.1	The TSF shall detect when [a non-zero number, determined by the authorized administrator, of] unsuccessful authentication attempts occur related to [internal ObjectServer authentication mechanism].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the user from successfully authenticating until an authorized administrator takes action to unlock the user].

User-Attribute Definition FIA_ATD.1

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [username, password, group, restrictions, enabled].

Verification of secrets FIA_SOS.1 (1)

FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [a) For each attempt to use the internal ObjectServer authentication mechanism, the probability that a random attempt will succeed is less than one in 1,000,000; b) Any feedback given during an attempt to use the internal authentication mechanism will not reduce the probability below the above metrics].

Timing of authentication FIA_UAU.1

FIA_UAU.1.1	The TSF shall allow **use of Utilities/Startup-Commands*** (The Utilities/Startup-Commands are, a) nco_objserv –secure [-name *servername*] , b) nco_sql (on unix), c) `nco_sql_crypt,` d) nco_g_crypt , e) nco_objserv -secauditlevel *info*, f) nco_ssladmin, g) nco_objserv, h) nco_ssladmin -> Generate self-signed certificate, i) setsslreg.exe (on windows), and j) Servers Editor.) 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.

Timing of identification FIA_UID.1

FIA_UID.1.1	The TSF shall allow **use of Utilities/Startup-Commands*** (The Utilities/Startup-Commands are, a) nco_objserv –secure [-name *servername*] , b) nco_sql (on unix), c) `nco_sql_crypt,` d) nco_g_crypt , e) nco_objserv -secauditlevel *info*, f) nco_ssladmin, g) nco_objserv, h) nco_ssladmin -> Generate self-signed certificate, i) setsslreg.exe (on windows), and j) Servers Editor.) 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.

Note for FIA_UID.1 & FIA_UAU.1: The Utilities/Startup-Commands are, nco_objserv –secure [-name *servername*] , nco_sql (on unix), `nco_sql_crypt,` nco_g_crypt ,nco_objserv -secauditlevel *info*, nco_ssladmin, nco_objserv, nco_ssladmin -> Generate self-signed certificate, setsslreg.exe (on windows) and Servers Editor.

5.1.5. Security Management (FMT)

Management of Security Functions Behaviour FMT_MOF.1

FMT_MOF.1.1	The TSF shall restrict the ability to *disable, enable, modify the behaviour of,* the functions [user account management, accounting and audit, cryptographic management, replication, triggers] to [authorized administrator].

Static Attribute Initialization FMT_MSA.1 (1)

FMT_MSA.1.1	The TSF shall enforce the [information flow SFP] to restrict the ability to *modify, delete* the security attributes [all identification and password data] to [authorized administrator of ObjectServer].

Static Attribute Initialization FMT_MSA.1 (2)

FMT_MSA.1.1	The TSF shall enforce the [access control SFP] to restrict the ability to *modify, delete, create, view* the security attributes [user accounts, groups, roles, network event data tables, accounting and audit data tables, triggers, and procedures] to [authorized administrator and users (view only)].

Static Attribute Initialization FMT_MSA.3 (1)

FMT_MSA.3.1	The TSF shall enforce the [information flow SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

Static Attribute Initialization FMT_MSA.3 (2)

FMT_MSA.3.1	The TSF shall enforce the [access control SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

Specification of Management Functions FMT_SMF.1

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions o [user account management, o accounting and audit, o cryptographic management, o data replication between ObjectServers, o management of triggers].

Application Note: The data replication only applies when multiple ObjectServers have been deployed.

Security Management Roles FMT_SMR.1

FMT_SMR.1.1	The TSF shall maintain the roles [authorized administrator, operators].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Application Note: The “authorized administrators” are the TOE users assigned to the “System” group. The “operators” are the TOE users assigned to the “Normal” group. The “System” group users have “create, delete, update & view” permissions. The “Normal” group users have “view” permissions and limited update & delete permissions for network event data tables, alert.status & alert.journal and delete permission for alerts.detail.

5.1.6. Protection of the TSF (FPT)

Internal TSF Consistency FPT_TRC.1

FPT_TRC.1.1	The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.
FPT_TRC.1.2	When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [updates to data on an ObjectServer].

Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1	The TSF shall protect TSF data from *disclosure* when it is transmitted between separate parts of the TOE.

FPT_SEP_EXP.1 - Domain separation
Based on the CC requirement FPT_SEP.1

FPT_SEP_EXP.1.1	The TSF, **when invoked by the underlying host OS**, shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.
FPT_SEP_EXP.1.2	The TSF, **when invoked by the underlying host OS**, shall enforce separation between the security domains of subjects in the TSC.

FPT_RVM_EXP.1 - Reference mediation
Based on the CC requirement FPT_RVM.1

FPT_RVM_EXP.1.1	The TSF, **when invoked by the underlying host OS**, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2. Security Requirements for the IT Environment

5.2.1. Identification and Authentication (FIA)

Authentication Failure Handling FIA_AFL.1 (2)

FIA_AFL.1.1	The IT Environment shall detect when [a non-zero number, determined by the authorized administrator, of] unsuccessful authentication attempts occur related to [all PAM authentication attempts].

FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the IT Environment shall [prevent the user from successfully authenticating until an authorized administrator takes action to unlock the user].

Verification of Secrets FIA_SOS.1 (2)

FIA_SOS.1.1	The IT Environment shall provide a mechanism to verify that secrets meet [a) For each attempt to use the PAM authentication mechanism, the probability that a random attempt will succeed is less than one in 1,000,000; b) Any feedback given during an attempt to use the PAM authentication mechanism will not reduce the probability below the above metrics].

FIA_UAU_OS.1 User Authentication

FIA_UAU_OS.1.1	The IT Environment shall allow **identification as stated in FIA_UID_OS.2** on behalf of the ***authorized administrator accessing the TOE*** to be performed before the ***authorized administrator*** is authenticated.
FIA_UAU_OS.1.2	The IT Environment shall require each ***authorized administrator*** to be successfully authenticated before allowing any other IT Environment-mediated actions on behalf of that ***authorized administrator***.

FIA_UID_OS.2 User Identification

FIA_UID_OS.2.1	The IT Environment shall require each user to identify itself before allowing any other IT Environment-mediated actions on behalf of that user.

5.2.2. Protection of the TSF (FPT)

Time Stamps FPT_STM.1

FPT_STM.1.1	The IT Environment shall be able to provide reliable time stamps for TOE's use.

FPT_SEP_OS.1 TSF domain separation

Based on the CC requirement FPT_SEP.1

FPT_SEP_OS.1.1	The ***security functions of the host OS*** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects ***in the scope of control of the host OS***.
FPT_SEP_OS.1.2	The ***security functions of the host OS*** shall enforce separation between the security domains of subjects in the ***scope of control of the host OS.***

FPT_RVM_OS.1 Non-bypassability of the TSP

Based on the CC requirement FPT_RVM.1

FPT_RVM_OS.1.1	The ***security functions of the host OS*** shall ensure that ***host OS security* policy** enforcement functions are invoked and succeed before each function within the **scope *of control of the host OS*** is allowed to proceed.

5.2.3. Security Audit (AU)

Protected Audit Trail Storage FAU_STG.1 (2)

FAU_STG.1.1 (2)	The IT Environment shall protect the stored audit records from

	unauthorized deletion.
FAU_STG.1.2 (2)	The IT Environment shall be able to ***prevent*** unauthorized modifications to the audit records in the audit trail.

Application Note: There is an iteration of FAU_STG.1 on the TOE and one on the IT Environment. The TOE protects the audit records from unauthorized deletion through enforcing I&A and user access permissions via its interfaces to ObjectServer (Administration Client, User Client, and Webtop). The IT Environment protects the files stored on the underlying OS by enforcing access controls necessary to deny any unauthorized access.

6. Assurance Requirements

This chapter defines the assurance requirements for the TOE. Assurance requirement components are Evaluation Assurance Level (EAL) 2, with no augmentation, from part 3 of the CC.

ASSURANCE CLASS	ASSURANCE COMPONENTS	
Configuration Management	ACM_CAP.2	Configuration items
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 11 – Security Assurance Requirements

7. PP Claims

There are no specific PP claims.

8. TOE Summary Specification

This section details the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

8.1. Security Functions

This section provides the Security Functions implemented by the TOE. See section 9.4 “TOE Summary Specification Rationale” for mappings and explanation from Security Functions to SFRs.

8.1.1. Identification/Authentication (IA)

This TSF provides support for FIA_AFL.1 (1), FIA_ATD.1, FIA_SOS.1 (1), FIA_UAU.1, FIA_UID.1, FCS_COP.1 (2) and FMT_SMR.1 SFRs.

IA.ENFORCE The TOE enforces individual identification and authentication to access any management functions with the exception of Utilities/Startup-Commands. The Utilities/Startup-Commands are, nco_objserv –secure [-name *servername*] , nco_sql (on unix), `nco_sql_crypt,` nco_g_crypt ,nco_objserv -secauditlevel *info*, nco_ssladmin, nco_objserv, nco_ssladmin -> Generate self-signed certificate, setsslreg.exe (on windows) and Servers Editor. The TOE supports two types of user roles: An “Authorized Administrator” with complete control over all aspects of configuration and TSF Data, and an “Operator” whose access is limited to viewing and managing alerts to determine the availability of services on a network. The “Authorized Administrators” are the TOE users assigned to the “System” group. The “Operators” are the TOE users assigned to the “Normal” group. The “System” group users have “create, delete, update & view” permissions. The users assigned to the “Normal” group have the following permissions. This role includes permissions to view information about system, tools, security, and desktop database tables. This role includes permissions to view, update, and delete entries in the alerts.status table; view, insert, and delete entries in the alerts.journal table; and view and delete entries in the alerts.details table. This role enables you to display and manipulate alerts, create filters and views, and run standard tools in the event list (User Client). There are two other groups “Probe” and “Gateway” that are only used for the relevant TOE components (Probes and Gateway) to authenticate with the ObjectServer. All of these user types/groups are maintain in the ObjectServer. The internal ObjectServer authentication mechanism is used to perform I&A. The Object Server stores unique usernames, application ID and encrypted passwords. Once these authentication parameters are collected, the ObjectServer compares it with the stored encrypted password, based on the result of this comparison, the authentication is either successful or denied. The Administration Client, the User Client and the Webtop require operators to identify and authenticate before accessing the system. The TOE maps the operator to a set of permissions defined by the Administrator. An administrator / operator must enter a correct username and password before configuring the TOE. The SOF-basic claim is related to this Security Function; see section 9.6 for more detail.

IA.PAM The TOE enforces authentication results received from PAM. For a Solaris environment, the PAM is also an option. If used, PAM verifies authentication parameters and passes the results to the ObjectServer. The SOF-basic claim is related to this Security Function; see section 9.6 for more detail.

IA.DISABLE The TOE disables an administrator / operator account when a defined number of logon attempts have failed. This parameter is set by the administrator during installation. Once the user account is locked, an administrator needs to take action and unlock the user account before user can log back in.

The default value is set to 5 for number of failed login tries before the account is locked. The value can be set / modified to a non-zero number by following; the “disable_user” trigger needs to be modified using Administrator GUI. To accomplish this task, start the Administrator GUI, navigate to the ObjectServer, login as an administrator to it, navigate to the “Automations” and then “Triggers”, double click on “disable_user” trigger, click on “Action” tab and in the SQL statement, change the number 5 in “set failurecount=5;” to the desired number, Click OK. It is strongly recommended that you keep this number at the default value of 5. It must be set to 5 or less to be compliant with

the evaluated configuration. The value set is step 2 above applies to all users in that ObjectServer in which the change was made.

IA.STORE The TOE stores administrator / operator passwords in encrypted form (via one-way hash). These parameters are stored in the ObjectServer component.

IA.ATTR The attributes of an administrator / operator account shall include username, password, role, group and restrictions. The attributes also include a Boolean value for whether or not the account is enabled.

8.1.2. Discretionary Access Control (AC)

This TSF Provides support for FDP_ACC.1, FDP_ACF.1, FMT_MSA.1 (1) and FMT_MSA.1 (2) SFRs.

AC.ACCESS "Authorized administrators" and "operators" can access TOE facilities based on their assigned group and restrictions. The "authorized administrator" = "Super User" user type in the TOE. The user account is a "Super User" if it has been assigned to "System" group. The "authorized administrators" have full access. The "operators" have limited access as granted by an authorized administrator based on their roles and assigned groups.

The ST SFR FMT_SMR.1 maps to actual user roles as described below. The compliance with evaluated configuration requires that only user groups defined below be used.

1- authorized administrator = "Super User" user type

   a. The user account is a "Super User" if it has been assigned to "System" group. These users have "create, delete, update & view" permissions. This role has all available permissions. You cannot modify the "SuperUser" role. The single user created by default, root, is assigned all permissions by virtue of being in the "System" group.

2- operator = "Normal" user type

   a. The operator account has "view" permissions and limited update/delete permissions to network event data tables as described here. This role includes permissions to view information about system, tools, security, and desktop database tables. This role includes permissions to view, update, and delete entries in the alerts.status table; view, insert, and delete entries in the alerts.journal table; and view and delete entries in the alerts.details table. This role enables you to display and manipulate alerts, create filters and views, and run standard tools in the event list (User Client).

3- There are two other groups "Probes" and "Gateway" that are only used for the relevant TOE components "Probes and Gateway" to authenticate with the ObjectServer.

   a. The Probe role includes permissions to insert and update entries in the alerts.status table and insert entries in the alerts.details table. This role provides the permissions that a probe needs to generate alerts in the ObjectServer.

   b. The Gateway role includes permissions to insert, update, and delete entries in the alerts.status, alerts.details, and alerts.journal tables, and the tables in the transfer database. The transfer database is used internally by the bidirectional ObjectServer Gateway to synchronize security information between ObjectServers. This role provides the permissions that a gateway needs to generate alerts in the ObjectServer.

8.1.3. Audit (AU)

This TSF Provides support for FAU_GEN_EXP.1, FAU_SAR.1 and FAU_STG.1 (1) SFRs.

AU.RECORD The TOE creates an audit record containing the following:

- Data and time of the First and Last occurrence of the event;

- Type;
- Manager;
- Identifier;
- Severity;
- Summary

1. Date and time of the event = First Occurrence, Last Occurrence
    a) The date and time an event occurs is the FirstOccurrence field. If it happens more than once, then the LastOccurrence will be the time it last happened.

Note: The TOE depends on the underlying OS of the ObjectServer for accurate timestamp. There is FPT_STM.1 requirement on the IT Environment.

2. Type of event = Manager, Identifier (Manager provides information on type of event, such as, ConnectionWatch, SecurityWatch, etc. The Identifier further identifies the (type of)command used)
3. Subject identity = Identifier
4. The outcome (success or failure) = Type, Severity, Summary, Identifier.

The following auditable events trigger an audit record:

- Alteration/Modification of audit functions;
- Logon attempts;
- Replication failure;
- Disablement of secure mode between probe and ObjectServer;
- Creation, deletion and modification of administrator / operator account.

AU.REVIEW The TOE provides the administrator with the means of reading the audit records. The administrator has access to GUIs (User Client and Webtop) and ObjectServer SQL command (SELECT) to review the audit records. The ObjectServer SQL Commands are part of ObjectServer TOE Component.

AU.PROTECT The TOE provides protection of audit data from unauthorized viewing, modification, or deletion. User accounts have no access to the audit record tables. In both Solaris and Windows environments, the ObjectServer provides audit protection (See Table 18, Security Functions to SFR Rationale). To further secure the TOE files that may contain audit records the FAU_STG.1 (2) was reiterated on the environment. This requirement enforces the IT Environment to make sure proper permissions are in place for all TOE directories and files to prevent unauthorized deletions or modifications of any files that may contain TOE audit records.

8.1.4.Communications (COM)

This TSF provides support for FCS_CKM.1, FCS_COP.1, FDP_IFC.1, FDP_IFF.1 and FPT_ITT.1 SFRs.

COM.IA The TOE requires a component to successfully identify and authenticate itself to an ObjectServer prior to transferring data. The components are identified based on the attributes listed in FDP_IFC.1 and FDP_IFF.1. Both these SFRs list in detail how and based on what attributes the communication between a component and ObjectServer is allowed.

COM.FAIL If a probe cannot contact ObjectServer it will not transfer any data. The data will be stored locally. Data will be transferred when a connection becomes available.

COM.PROTECT The TOE will use SSL to protect the transferring of data between Probes and ObjectServers, the Administration Client and ObjectServers and the User Client and ObjectServers.

8.1.5.Management (MAN)

This TSF provides support for FMT_MOF.1, FMT_SMF.1, FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_MSA.3 (1) and FMT_MSA.3 (2) SFRs.

MAN.ACCESS Only the authorized administrator can access the facilities to perform user account management, accounting and audit management, cryptographic management and replication management.

MAN.SECVAL Authorized administrators are required to enter secure values[2] when creating and modifying security attributes.

8.1.6. Replication (REP)

This TSF provides support for FPT_TRC.1 SFR.

REP.DATA The TOE replicates data between ObjectServers to ensure consistency of data. ObjectServer gateways are used to replicate table data (for example, alert-related data) between different Netcool OMNIbus ObjectServers. ObjectServer gateways consist of readers and writers. Readers extract alerts from a source ObjectServer. Writers send the alert data to a target ObjectServer.
A reader extracts alerts from an ObjectServer. There is only type of reader: the ObjectServer reader. Once the reader is started and the gateway attempts to open a connection to the source ObjectServer. If the gateway succeeds in opening the connection, it immediately starts to read alerts from the ObjectServer.
Writers send the alerts acquired by a reader to the destination application or ObjectServer. Once the writer is started, the gateway attempts to establish the connection to the alert destination ObjectServer. The writer sends alerts received from the source ObjectServer.
Routes create the link between readers and writers. Once the route has been created, the connection between a reader and writer is established. Any alerts received by the source ObjectServer are read by the reader, passed through the route to the writer, and written into the destination ObjectServer.

8.1.7. Protection of TOE Functions (PTF)

This TSF provides support for FPT_RVM_EXP.1 and FPT_SEP_EXP.1 SFRs.

PTF.SEP The TOE (through the Probes) maintains a domain for its own execution separate from the Enterprise Event traffic that it analyzes. Threats to the TOE via the local host are mediated by security functions on the IT Environment and by assumptions regarding the non-IT Environment. The TSF is protected from interference that would prevent it from performing its functions. Protection of the TOE from physical tampering is ensured by its environment. It is assumed that the device will remain physically connected to the network in such a way that the TOE device cannot be bypassed. All processes on the TOE are trusted. The communication channels between ObjectServer and User Client, ObjectServer and Probes, Webtop and browser, ObjectServer and ObjectServer (via Gateway) are all protected using encryption. The encryption between all TOE components takes place entirely within the TOE software. The underlying OS of the TOE systems are not used for general purpose operations and non-administrative users are not allowed to directly access the TOE. Non-administrative users can only interact with the TOE indirectly via User Client or Webtop Client. The underlying OS maintains separate memory allocation for the use of TOE software. The SFRs on IT Environment require that no access to the underlying OS be granted without proper I&A, and that proper permission setup is used to protected TOE audit log files. Therefore domain separation is maintained.

PTF.RVM The TOE ensures that all functions are invoked and succeed before each function may proceed. The communication channels between ObjectServer and User Client, ObjectServer and Probes, Webtop and browser, ObjectServer and ObjectServer (via Gateway) are all protected using encryption. The encryption between all TOE components takes place entirely within the TOE software. Additionally, IT environment requirements and assumptions ensure that untrusted subjects in the host OS cannot interfere with TOE operation or bypass its checks. The SFRs on IT Environment require that no access to the underlying OS be granted without proper I&A, and that proper permission setup is used to protected directories containing TOE audit log files. Hence the TSF in-conjunction with the IT Environment ensures complete non-bypassability of TOE.

[2] The specification for secure values will be stated in the evaluated configuration guide.

8.2. Assurance Measures

This section identifies the Configuration Management, Delivery/Operation, Development, Guidance Documents, Test, and Vulnerability Assessment measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
ACM_CAP.2	CM_DOC	Configuration items: The implementation and documentation of procedures for the development of the TOE, including a configuration list of uniquely identified items. Evidence Title: IBM/Micromuse Configuration Management Plan and Delivery Procedures for Netcool OMNIbus v7.1 with Netcool Webtop v2.0, Version 0.9
ADO_DEL.1	DEL_DOC	Delivery procedures: The implementation and documentation of procedures for delivering the TOE to a customer in a secure manner. Evidence Title: IBM/Micromuse Configuration Management Plan and Delivery Procedures for Netcool OMNIbus v7.1 with Netcool Webtop v2.0, Version 0.9
ADO_IGS.1	IGS_DOC	Installation, generation, and start-up procedures: Documentation provided to the end users instructing the end users how to install and configure the TOE in a secure manner. Evidence Title: TOE (IGS/ADM) ReadMe for Netcool\OMNIbus v7.1 with Webtop v2.0 & Cisco Info Center v7.1 with Webtop v2.0, Version 1.2
ADV_FSP.1	FUN_SPEC	Informal functional specification: Functional Specification for the TOE describing the TSF and the TOE's external interfaces. Evidence Title: Informal Functional Specification for IBM Netcool\OMNIbus v7.1 with Webtop v2.0 & Cisco Info Center v7.1 with Webtop v2.0, Version 1.5
ADV_HLD.1	HLD_DOC	Descriptive high-level design: System Design for the TOE providing descriptions of the TSF structure in the form of subsystems and the functionality of each subsystem. Evidence Title: High Level Design for IBM Netcool\OMNIbus v7.1 with Webtop v2.0 & Cisco Info Center v7.1 with Webtop v2.0, Version 1.2
ADV_RCR.1	RCR_DOC	Informal correspondence demonstration: The documentation of the correspondence between the TSS, FSP and HLD in specifically provided deliverables. Evidence Title: Same as FSP and HLD above.
AGD_ADM.1	ADMIN_GUIDE	Administrator guidance: Documentation provided to the customers instructing the customer how to configure the TOE in a secure manner. Evidence Title: TOE (IGS/ADM) ReadMe for IBM Netcool\OMNIbus v7.1 with Webtop v2.0 & Cisco Info Center v7.1 with Webtop v2.0, Version 1.2

AGD_USR.1	USER_GUIDE	User guidance: Documentation provided to the customers instructing the users how to use the TOE. Note: There are no non-admin users of the TOE. Evidence Title: N/A
ATE_COV.1	TEST_COV	Evidence of coverage: Documented correspondence between the security functions and tests. Evidence Title: Test Plan and Coverage Analysis for IBM Netcool\OMNIbus v7.1 with Netcool Webtop v2.0 & Cisco Info Center v7.1 with Cisco Webtop v2.0, Version 0.6
ATE_FUN.1	TEST_DOC	Functional testing: The implementation and documentation of the test procedures including expected and actual results. Evidence Title: Test Plan and Coverage Analysis for IBM Netcool\OMNIbus v7.1 with Netcool Webtop v2.0 & Cisco Info Center v7.1 with Cisco Webtop v2.0, Version 0.6
AVA_SOF.1	SOF_DOC	Strength of TOE security function evaluation: The documentation for the Strength of Function Assessment. Evidence Title: Strength of Function for IBM Netcool\OMNIbus v7.1 with Netcool Webtop v2.0 & Cisco Inco Center v7.1 with Cisco Webtop v2.0, Version 0.7
AVA_VLA.1	VLA_DOC	Developer vulnerability analysis: Vulnerability Assessment of the TOE and its deliverables is performed and documented to ensure that identified security flaws are countered. Evidence Title: Vulnerability Analysis for IBM Netcool\OMNIbus v7.1 with Netcool Webtop v2.0 & Cisco Info Center v7.1 with Cisco Webtop v2.0, Version 0.6

Table 12 – Assurance Measures

The above table includes all of the assurance requirements for the target level of assurance EAL2. Documented evidence covering each of the detailed security assurance requirements in EAL2 has been provided in the supporting documentation listed above against each EAL2 component.

9. Rationale

This section provides a rationale for the existence of each threat, security objective, and security function that comprises the Security Target.

9.1. Security Objectives Rationale

9.1.1. Complete Coverage – Threats

This section provides evidence that demonstrates coverage of the threats by the TOE security objectives. The following table shows this threat to objective mapping. It should be noted that there are no availability requirements and hence no attempt has been made to address the threats if the TOE, or some part of the TOE, is not working.

OBJECTIVES	THREATS
O.AUTHORIZATION	This security objective is necessary to counter the threats T.UNAUTH and T.LOWEXP. This threat relates to unauthorized personnel gaining accessing to the TOE. This objective ensures that only authorized users can gain access to the TOE.
O.DISCRETIONARY_ACCESS	This security objective counters the threats T.UNAUTH and T.LOWEXP. This objective ensures that only users with the required level of access can gain access to the parts of the TOE specific to that user.
O.AUDITING	This security objective is necessary to counter the threats T.NETSEC, T.AUD and T.DATABASEFAIL. This objective ensures that no activities for unauthorized personnel will go unnoticed and any user action that causes a database failure will be noticed from the audit records.
O.MANAGE	This security objective is necessary to counter the threats T.NETSEC, T.INSECURE and T.DATABASEFAIL. This objective ensures that the TSF provides all the functions and facilities necessary to support the authorized administrators. Additionally, this objective provides administrators the ability to reduce the risk of T.DATABASEFAIL.
O.AUDITPROTECT	This security objective is necessary to counter the threats T.NETSEC and T.AUD. This objective ensures that audit records cannot be deleted or modified.
O.REPLICATION	This security objective is necessary to counter the threats T.NETSEC, T.COMPDATA, and T.DATABSEFAIL. This objective ensures that all data is consistently replicated between ObjectServers.
O.SEL_PRO	To counter the threat of T.LOWEXP and T.SEL_PRO the TOE (In concert with the environment) must protect itself against attempts by unauthorized users to bypass, deactivate or temper with the TOE Security functions.
O.SECURECOMMS	This security objective is necessary to counter the threats T.NETSEC and T COMPDATA. This objective ensures that data is transferred securely between physically separate components.
OE.INSTALL	This security objective is necessary to counter the threats T.NETSEC and T.INSECURE. This objective ensures that the TOE is delivered, installed, managed and operated in a secure manner.

OBJECTIVES	THREATS
OE.PHYSICAL	This security objective is necessary to counter the threats T.INSECURE and T.COMPDATA. This objective ensures that the parts of the TOE critical to security policies are protected from physical attack.
OE.CREDEN	This security objective is necessary to counter the threats T.NETSEC and T.UNAUTH. This objective ensures that all access credentials are protected in a manner which maintains IT security objectives.
OE.PROBE	This security objective is necessary to counter the threat T.NETSEC. This objective ensures that security relevant events are not lost if a probe cannot transfer it to an ObjectServer immediately.
OE.PAM	This security objective is necessary to counter the threat T.UNAUTH. This objective ensures that PAM is correctly installed on the Solaris machines hosting the ObjectServers.
OE.LOWEXP	This security objective is necessary to counter the threat T.LOWEXP. This objective ensures that the TOE's operating environment protects itself against malicious attacks.

Table 13 – Mapping of TOE Security Objectives to Threats

9.1.2. Complete Coverage - Environmental Assumptions

This section provides evidence that demonstrates coverage of the environmental security objectives by the environmental assumptions. The following table shows this assumption to objective mapping.

SECURITY OBJECTIVES FOR THE ENVIRONMENT	ENVIRONMENTAL ASSUMPTIONS
OE.INSTALL	A.INSTALL This objective ensures that the TOE is delivered, installed, managed and operated in a manner which maintains the IT security objectives.
OE.PHYSICAL	A.PHYSEC This objective assumes that the ObjectServers, Webtop Server (if used) and Gateway components, and network connections between them, must be physically secure.
OE.CREDEN	A.TRUSTED This objective ensures that the TOE is administered by competent and trusted personnel who will ensure that all access credentials are protected.
OE.PROBE	A.PROBE This objective ensures that probes are able to securely store network event data on their local platform.
OE.PAM	A.SOLARIS This objective ensures that PAM is installed correctly on Solaris machines hosting the ObjectServers.
OE.LOWEXP	A.LOWEXP & A.SEL_PRO This objective assumes that the operating environment protects itself from malicious attacks from attackers with a low attack potential.
OE.SEL_PRO	A.SEL_PRO This covers the assumption A.SEL_PRO that states that the TOE Environment shall, in conjunction with the TOE, protect itself against attempts by unauthorized users to bypass, deactivate or temper with the TOE Security functions
OE.OSLOGIN	OE.OSLOGIN This covers the assumption A.OSLOGIN by ensuring that the TOE environment will require authorized administrators to successfully identify themselves to the OS.

Table 14 – Mapping of Environment Security Objectives to Environmental Assumptions

From the above table it can be seen that the objectives are suitable to cover all of the identified assumptions.

9.2. Security Requirements Rationale

9.2.1. Internal Consistency of Requirements

This section describes the mutual support and internal consistency of the components selected for this profile. These properties are discussed for both functional and assurance components. The functional components were selected from pre-defined CC components. The use of component refinement was accomplished in accordance with CC guidelines. Assignment, selection, and refinement operations were carried out among components using consistent computer security terminology. This helps to avoid the ambiguity associated with interpretations of meanings of terms between related components. Multiple instantiation of identical or hierarchically-related components was used to clearly state the required functionality that must exist in the TOE.

9.2.2. Complete Coverage - Objectives

This section demonstrates that the functional components selected for this profile provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the following table.

SECURITY OBJECTIVE FOR THE TOE	FUNCTIONAL REQUIREMENT (SFRs) FOR THE TOE	IT SECURITY FUNCTION (TSF) FOR THE TOE
O.AUTHORIZATION	FDP_IFC.1	COMM

	FDP_IFF.1	COMM
	FDP_ACC.1	AC
	FDP_ACF.1	AC
	FIA_AFL.1 (1)	IA
	FIA_ATD.1	IA
	FIA_SOS.1 (1)	IA
	FIA_UAU.1	IA
	FIA_UID.1	IA
	FCS_COP.1 (2) (Hashing)	IA
O.DISCRETIONARY_ACCESS	FDP_ACC.1	AC
	FDP_ACF.1	AC
	FMT_MSA.1 (2)	MAN
	FIA_ATD.1	IA
O.AUDITING	FAU_GEN_EXP.1	AU
	FAU_SAR.1	AU
	FAU_STG.1 (1)	AU
O.MANAGE	FAU_SAR.1	AU
	FMT_MOF.1	MAN
	FMT_SMF.1	MAN
	FMT_SMR.1	IA
	FMT_MSA.1 (1)	MAN, AC
	FMT_MSA.1 (2)	MAN, AC
	FMT_MSA.3 (1)	MAN
	FMT_MSA.3 (2)	MAN
O.AUDITPROTECT	FDP_ACC.1	AC
	FDP_ACF.1	AC
	FAU_STG.1 (1)	AU
O.REPLICATION	FPT_TRC.1	REP
	FDP_IFF.1	COMM
O.SECURECOMMS	FCS_CKM.1	COMM
	FCS_COP.1	COMM
	FDP_IFC.1	COMM
	FDP_IFF.1	COMM
	FPT_ITT.1	COMM
O.SEL_PRO	FPT_SEP_EXP.1	PTF
	FPT_RVM_EXP.1	PTF
SECURITY OBJECTIVE FOR THE ENVIRONMENT	**FUNCTIONAL REQUIREMENT (SFRs) FOR THE ENVIRONMENT**	**N/A**
OE.INSTALL	FPT_STM.1	These SFRs are for the Environment. Hence no mappings to TOE Security Functions.
OE.PAM	FIA_AFL.1 (2)	
	FIA_SOS.1 (2)	
OE.SEL_PRO	FPT_SEP_OS.1	
	FPT_RVM_OS.1	
	FAU_STG.1 (2)	
OE.OSLOGIN	FIA_UAU_OS.1	
	FIA_UID_OS.2	

Table 15 – Correspondence of security objectives to SFRs & SFRs to TSFs

The following discussion provides detailed evidence of coverage for each security objective for the TOE and IT Environment:

TOE OBJECTIVE	ARGUMENT TO SUPPORT SUFFICIENCY OF SECURITY

	REQUIREMENTS
O.AUTHORIZATION	The objective to ensure that only authorized operators can gain access to the TOE ensures is met by the following security requirements: • FDP_IFC.1, FDP_IFF.1, FDP_ACC.1 and FDP_ACF.1 ensure that no user action will be able to take place until the user has been identified and authenticated and no transfer of event data will take place until the probe or gateway has been identified and authenticated. • FIA_AFL.1(1) and FIA_ATD.1 provide the capability to detect when a defined number of attempts have been made to access the TOE and will prevent a user gaining access to the TOE until an authorized administrator takes actions to unlock the use account. • FIA_SOS.1 (1) requires the use of strong password/secretes to reduce the likelihood of password guessing • FIA_UAU.1 and FIA_UID.1 require the TOE to enforce identification and authentication of all users • FCS_COP.1 (2) specifies hashing requirements for hashing passwords.
O.DISCRETIONARY_ACCESS	The objective to ensure that only users with the required level of access can gain access to the parts of the TOE specific to that user is met by the following security requirements: • FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled • FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions, configuration data, audit logs, and account attributes is based on the user privilege level and their allowable actions • FMT_MSA.1(2) specifies that only privileged administrators can access the TOE security functions and related configuration data
O.AUDITING	The objective to ensure that no activities for unauthorized personnel will go unnoticed and any user action that causes a database failure will be noticed from the audit records is met by the following security requirements: • FAU_GEN_EXP.1 and FAU_SAR.1 define the auditing capability for information flow control and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs • FAU_STG.1 (1) ensures that stored audit records are not deleted by an unauthorized user
O.MANAGE	The objective to ensure that the TSF provides all the functions and facilities necessary to support the authorized administrators is met by the following security requirements: • FAU_SAR.1 requires that authorized users will have the capability to read and interpret data stored in the audit logs • FMT_MOF.1 stipulates that only an authorized administrator

	can modify account management, audit, cryptographic management, and accounting functions • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role • FMT_MSA.1(1) restricts the ability to modify or delete user identification and authentication details to an authorized administrator • FMT_MSA.3(1) allows an authorized administrator to change the default I&A attributes of objects or information • FMT_MSA.1(2) specifies that only privileged administrators can access the TOE security functions and related configuration data • FMT_MSA.3(2) ensures that the default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE
O.AUDITPROTECT	The objective to ensure that audit records cannot be deleted or modified is met by the following security requirements: • FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled • FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions, configuration data, audit logs, and account attributes is based on the user privilege level and their allowable actions • FAU_STG.1 (1) ensures that stored audit records are not deleted by an unauthorized user FAU_STG.1 (1) ensures that stored audit records are not deleted by an unauthorized user
O.REPLICATION	The objective to ensure that all data is consistently replicated between ObjectServers is met by the following security requirements: • FDP_IFF.1 ensures that each probe has a primary ObjectServer and only connects to its secondary ObjectServer when the primary ObjectServer is not available • FPT_TRC.1 ensures that data is consistent when replicated between TOE components (e.g., ObjectServers)
O.SECURECOMMS	The objective to ensure that data is transferred securely between physically separate components is met by the following security requirements: • FCS_CKM.1, FCS_COP.1 (1)specify cryptographic requirements for the secure communication between components • FDP_IFC.1 and FDP_IFF.1 ensure that no user action will be able to take place until the user has been identified and authenticated and no transfer of event data will take place until the probe or gateway has been identified and authenticated via secure SSL connection • FPT_ITT.1 requires that the TOE protects TSF data from one

	component to another
O.SEL_PRO	The objective to ensure that the TOE will provide, in conjunction with the environment, means to prevent unauthorized persons from reading, modifying or destroying security critical TOE configuration Data is met by the following security requirements. • FPT_RVM_EXP.1 Non-Bypassability of the TOE is required to meet the O.SEL_PRO objective by enforcing that the TOE in concert with the TOE environment is configured to ensure that all TSP enforcement functions and invoked and succeed before any function is allowed to proceed. • FPT_SEP_EXP.1 Domain Separation is required to meet the O.SEL_PRO objective by enforcing that the TOE in concert with the TOE environment maintains a security domain for its own execution to protect it from tampering by un-trusted subjects.
OE.INSTALL	The objective to ensure that those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains security objectives for the TOE. • FPT_STM.1 provides the reliable time stamp that is needed for correct operation of the TOE and keeping track of audit record in congenial order. The A.INSTALL covers the rest of this objective, see section 9.1.2, Table 14.
OE.PAM	The objective is to ensure that those responsible for the TOE must ensure that PAM, when deployed, is correctly installed on the Solaris machines hosting the ObjectServers. • FIA_AFL.1 (2) ensures that the IT Environment on Solaris is set to disable logging ability of a user who has surpassed the administrator configurable number for authentication attempts when PAM is used. • FIA_SOS.1 (2) ensures that the IT Environment on Solaris meets the SOF-basic standard set for the TOE I&A mechanism when PAM is used.
OE.SEL_PRO	The objective to ensure that the TOE will provide, in conjunction with the environment, means to prevent unauthorized persons from reading, modifying or destroying security critical TOE configuration Data. • FPT_RVM_OS.1 Non-Bypassability of the TSP is required to meet the environmental objective OE.SEL_PRO that states that TOE, in conjunction with the environment, protect itself against attempts by unauthorized users to bypass, deactivate or temper with the TOE Security functions. • FPT_SEP_OS.1 Domain Separation of the TSF is required to meet the environmental objective OE.SEL_PRO that states that the TOE, in conjunction

	with the environment, protect itself against attempts by unauthorized users to bypass, deactivate or temper with the TOE Security functions. • FAU_STG.1 (2) Audit Trail protection is required to meet the environmental objective OE.SEL_PRO that states that the TOE, in conjunction with the environment, protect itself against attempts by unauthorized users to delete or modify the audit records.
OE.OSLOGIN	The objective to ensure that the TOE utilities and tools that are available without authentication will be protected by requiring the authorized administrators to login to the IT Environment before they can access any other TSF mediated action or functionality. • FIA_UAU_OS.1 Identification is required to meet the environmental objective OE.OSLOGIN which states that the TOE environment shall require identification and authentication of authorized administrators • FIA_UID_OS.2 Authentication is required to meet the environmental objective OE.OSLOGIN which states that the TOE environment shall require identification and authentication of authorized administrators

Table 16 – Sufficiency of Security Requirements for the TOE and IT Environment

9.3. Dependencies

The following table shows the dependencies that exist between functional components. A box with an X in it indicates a dependency that has been satisfied in the ST. A box with an N in it indicates a dependency that has not been explicitly satisfied. The rationale for these dependencies not being satisfied is included below Table 17.

CC IDENTIFIER	FAU_GEN_EXP.1	FCS_COP.1	FCS_CKM.1	FCS_CKM.4	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FPT_ITT.1	FMT_SMR.1	FMT_SMF.1	FPT_STM.1	FPT_SEP_EXP.1	FPT_RVM_EXP.1	FPT_SEP_OS.1	FPT_RVM_OS.1	FIA_UID_OS.2	FIA_UAU_OS.1
REQUIREMENT																							
FAU_GEN_EXP.1																	X						
FAU_SAR.1	X																						
FAU_STG.1 (1)	X																						
FCS_CKM.1		X		N								N											
FCS_COP.1 (1)			X	N								N											
FCS_COP.1 (2)																							
FDP_ACC.1						X																	
FDP_ACF.1					X								X										
FDP_IFC.1								X															
FDP_IFF.1							X						X										

FIA_AFL.1 (1)									X														
FIA_AFL.1 (2)									X														
FIA_ATD.1																							
FIA_SOS.1 (1)																							
FIA_SOS.1 (2)																							
FIA_UAU.1										X													
FIA_UID.1																							
FMT_MOF.1															X	X							
FMT_MSA.1(1)							X								X	X							
FMT_MSA.1(2)					X										X	X							
FMT_MSA.3(1)											X				X								
FMT_MSA.3(2)											X				X								
FMT_SMF.1																							
FMT_SMR.1										X													
FPT_ITT.1																							
FPT_STM.1																							
FPT_TRC.1														X									
FPT_SEP_EXP.1																				X			
FPT_RVM_EXP.1																					X		
FPT_SEP_OS.1																							
FPT_RVM_OS.1																							
FIA_UID_OS.2																							X
FIA_UAU_OS.1																							
FAU_STG.1 (2)																							

Table 17 – Satisfaction of Dependencies

Note that dependencies on FIA_UID.1 are met by the inclusion of FIA_UID.1, since FIA_UID.1 is hierarchical to FIA_UID.1. Similarly, dependencies on FIA_UAU.1 are met by the inclusion of FIA_UAU.1, since FIA_UAU.1 is hierarchical to FIA_UAU.1.

FCS_COP.1 (1) and FCS_CKM.1 both have a dependency on FMT_MSA.2. FMT_MSA.2.1 states “The TSF shall ensure that only secure values are accepted for security attributes.” All cryptographic security attributes are generated by the TSF and stored within the TOE. Consequently, all cryptographic security attributes have secure values by default when set by the administrator. When not set by an administrator, cryptographic security attributes have null values by default. No cryptographic security attributes are accepted from outside the TOE.

FCS_COP.1 (1) and FCS_CKM.1 both have a dependency on FCS_CKM.4. SSL session key functionality is based upon PKI protocols, whereby the active cryptographic keys are controlled, generated and destroyed as required by the activity of the protocols. Thus these dependencies are addressed by the correct implementation of the standard protocols, which is out of scope of the evaluation of this TOE. Ultimately the validity of the key management for these protocols is reliant upon the security of the private key data associated with published keys, and this is covered in part by the protocol standards and the fact that private keys are installed “out of band” by a process that requires direct access to a platform needing to communicate. The destruction of the TOE public/private key pair is also out of scope of the evaluation as once the keys are created they are data files controlled by operating systems.

9.4. TOE Summary Specification Rationale

This section demonstrates that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.

The specified TOE security functions work together to satisfy the TOE security functional requirements. The following Table 18 and Table15 show the security functional requirements that each security function addresses. The tables show that each security function is required to address at least one security functional requirement.

SECURITY FUNCTION	SECURITY FUNCTIONAL REQUIREMENTS	NOTES
IA.ENFORCE	FIA_UAU.1, FIA_UID.1	The administrator / operator shall be successfully identified and authenticated by the TOE before any functions are available. This function is realized by a probabilistic / permutational mechanism (specifically, a password greater than or equal to six characters); therefore the strength of function claim SOF-basic applies to this security function
IA.PAM	FIA_AFL.1 (1), FIA_SOS.1 (1)	The TOE can be configured to accept PAM identification and authentication (only for Solaris environments).
IA.DISABLE	FIA_AFL.1 (1)	The authorized administrator will determine how many attempts can be made to access the TOE before the TOE will then prevent the user from authenticating until the authorized administrator has taken some action.
IA.STORE	FIA_SOS.1 (1) , FCS_COP.1 (2)	The TOE will be configured to hash passwords before storing them. The algorithm used is a proprietary algorithm and generates 128 bit hashes. The ObjectServer stores administrator passwords in ciphertext, and they are encrypted with UNIX *crypt*, which provides Data Encryption Standard (DES) encryption of the password. They key is the password, and the digest is the key concatenated with salt. The keyspace consists of 2^{56} possible values. Since they key is derived from the password, this function is realized by a probabilistic / permutational mechanism (specifically, a password greater than or equal to six characters); therefore the strength of function claim SOF-basic applies to this security function.
IA.ATTR	FIA_ATD.1, FMT_SMR.1	The TOE shall recognise the roles authorized administrator and operator. When a user is assigned an account it shall contain username, password, role, group, restrictions and whether the account is enabled or not.
AC.ACCESS	FDP_ACC.1, FDP_ACF.1 FMT_MSA.1 (1), FMT_MSA.1 (2)	The TOE shall allow an authorized administrator to view, modify, create or delete user account data and ObjectServer tables based on the permission specified in his user account. The TOE shall allow a user to view network event data tables based on the permission specified in his user account.

SECURITY FUNCTION	SECURITY FUNCTIONAL REQUIREMENTS	NOTES
AU.RECORD	FAU_GEN_EXP.1	The TOE will generate audit records for security relevant events and store them in the error log and security audit log. The IT environment will provide capability for reliable time stamps.
AU.REVIEW	FAU_SAR.1	The audit records that are generated by the TOE will be in a format readable by the authorized administrator. The IT environment will provide capability for reliable time stamps.
AU.PROTECT	FAU_STG.1 (1)	The audit records will be protected against unauthorized deletion and prevented from unauthorized modification by preventing unauthorized personnel from viewing the log files. To further secure the TOE files that may contain audit records the FAU_STG.1 (2) was reiterated on the environment. This requirement enforces the IT Environment to make sure proper permissions are in place for all TOE directories and files to prevent unauthorized deletions or modifications of any files that may contain TOE audit records.
COM.IA	FDP_IFC.1, FDP_IFF.1	Only authenticated traffic is allowed to flow through the TOE.
COM.FAIL	FDP_IFF.1	Data will not be passed if ObjectServers are unavailable, the data will be locally stored on the originating probe.
COM.PROTECT	FPT_ITT.1, FCS_CKM.1, FCS_COP.1	The TOE will start an SSL session between the probes and the ObjectServers, Administration Client and ObjectServers and User Client and ObjectServers to protect data transfer using encryption. The information / parameters necessary for SSL will be created during installation.
MAN.ACCESS	FMT_MOF.1, FMT_SMF.1	The ability to perform a defined set of management functions on the TOE will be restricted to authorized administrators by reference to the permissions assigned to each user account.
MAN.SECVAL	FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_MSA.3 (1), FMT_MSA.3 (2)	The TOE will allow the administrator to populate all security attributes with secure values according to the evaluated configuration guide.
REP.DATA	FPT_TRC.1	The data will remain consistent between ObjectServers and if one or both of the ObjectServers are unavailable a consistency check will be undertaken before any new data is passed.

SECURITY FUNCTION	SECURITY FUNCTIONAL REQUIREMENTS	NOTES
PTF.SEP	PTF_SEP_EXP.1	The TOE (through the Probes) maintains a domain for its own execution separate from the Enterprise Event traffic that it analyzes. Threats to the TOE from the local host are mediated by security functions on the IT Environment and by assumptions regarding the non-IT Environment. The TSF is protected from interference that would prevent it from performing its functions. Protection of the TOE from physical tampering is ensured by its environment. It is assumed that the device will remain physically connected to the network so that a device cannot be bypassed. All processes on the TOE are trusted. The TOE systems are not used for general purpose operations and non-administrative users are not allowed to directly access the TOE. Non-administrative users can only interact with the TOE indirectly. Therefore domain separation is maintained.
PTF.RVM	FPT_RVM_EXP.1	The TOE ensures that all functions are invoked and succeed before each function may proceed. Non-bypassability of management functions is achieved by the identification and authentication mechanisms that ensure that the management functions are not bypassed. The TOE protects its management functions by isolating them through authentication of administrators. Additionally, IT environment requirements and assumptions ensure that untrusted subjects in the host OS cannot interfere with TOE operation or bypass its checks.

Table 18 – Security Functions to SFR Rationale

The rationale for the TOE security functional requirements given in Section 5 and elaborated in Section 9.2, demonstrates that the SFRs work together in a consistent manner and are mutually supportive. Given that the above tables show that the security functions completely instantiate the SFRs, and that they contain no conflicting or inconsistent requirements, it is determined that the security functions do not introduce any security weaknesses.

9.5. Rationale for Assurance Rating

This security target has been developed for a generalised environment with a low level of risk to the assets. It is intended that products used in these environments will be generally available, without modification to meet the security needs of the environment. As such it was determined that Evaluation Assurance Level 2 was the most appropriate.

9.6. Rationale for SOF Rating

The minimum Strength of Function for the TOE is SOF-Basic. Administrator passwords stored in the ObjectServers require a Strength of Function claim because they are inherently probabilistic. The security functional requirements FIA_UAU.1 and FIA_SOS.1 provide the basis for the password mechanism by via a probability of password guessing of less than 1 in 1,000,000. The strength of function claim is based on the functionality of the TOE. The TSF enforces restrictions on the password combinations. It requires that the TOE is correctly configured and administrated as instructed in the CC specific IGS guide. The

Assumptions to support the SOF claim are A.INSTALL and A.TRUSTED, which ensure that the TOE is configured securely and that administrators are trusted personnel.

The TSF enforces a minimum password length of 8 characters. If a password for an Administrator/Operator is only 8 characters, then the number of password permutation is as follows:

52 alphabets (26 capital alphabet characters +26 lower alphabet characters)
+10 numerical characters
=66 possible values

Since the password space is 8 characters at minimum, the total number of possible values is 4,160,000,000 (which equals 66^8). Assuming an attacker can enter one password every 1 second, that results in 60 attempts every minute (60/1=60), 3,600 attempts per hour, 216,000 attempts per day. It will take 19,260 days to try all possible values. Let's assume that attacker only need to go through 50% of the possible values to find the match that will take 9,630 days. This comes out to be 320 months or 26 years. However, the attacker will not have the opportunity to enter as many passwords for a particular user account because that account would be locked after an administrator settable number (required to be set to 5 or less) of failed authentication attempts.

The claim for SOF-Basic is appropriate for this TOE because it is sufficient to protect against an attacker with a low attack potential, (e.g.,. attackers with high resources, high skill and low motivation). Additionally, it is consistent with EAL 2 and the testing that is carried out for that level of assurance.