National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

IBM Tivoli

Netcool/OMNIbus Version 7.3.1

Report Number: CCEVS-VR-VID10355-2012

Dated: 2012-12-21

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of the IBM Tivoli Netcool/OMNIbus Version 7.3.1. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the information technology (IT) product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by the atsec information security corporation, and was completed during December 2012. atsec information security corporation is an approved NIAP Common Criteria Testing Laboratory (CCTL). The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 3.1. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by the CCTL. The evaluation determined the product to be Common Criteria Version 3.1 Revision 3, Part 2 and Part 3 conformant, and to meet the requirements of EAL4 augmented by ALC_FLR.3.

Netcool/OMNIbus is an enterprise network and service level management (NMS-SLM) system that uses software components called "probes" to collect enterprise-wide event information from many different network data sources and presents a simplified view of this information to administrators so that they can monitor events in their environment. Netcool/OMNIbus tracks alert information in a high-performance, in-memory database (the ObjectServer) 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 the Netcool Web GUI (Graphical User Interface). The TOE includes a probe to collect Simple Network Management Protocol (SNMP) data.

The validation team agrees that the CCTL presented appropriate rationales to support the Results of Evaluation presented in Section 4, and the Conclusions presented in Section 5 of the ETR. The validation team therefore concludes that the evaluation and the Pass result for the Netcool/OMNibus Version 7.3.1 is complete and correct.

2. IDENTIFICATION

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a National Security Agency (NSA) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary

Laboratory Assessment Program (NVLAP) accreditation granted by the National Institute of Standards and Technology (NIST).

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	IBM Tivoli Netcool/OMNIbus Version 7.3.1
Protection Profile	None.
Security Target	*IBM Tivoli Netcool/OMNIbus 7.3.1 Security Target Version 2.10, 2012-11-09*
Evaluation Technical Report	*Evaluation Technical Report for a Target of Evaluation* *IBM Tivoli Netcool/OMNIbus 7.3.1 ETR Version 1.0 as of 2012-10-02*
Conformance Result	CC V3.1, Part 2 conformant, Part 3 conformant, EAL 4 augmented by ALC_FLR.3
Sponsor	IBM Corporation
Developer	IBM Corporation
Evaluators	Alejandro Masino, Jeremy Powell, Trang Huynh atsec information security corporation

3. CLARIFICATION OF SCOPE

This section details the scope of the evaluation and describes the logical and physical boundaries of the TOE.

3.1. Physical Scope

The physical scope of the evaluated configuration consists of:

- Software:
  - Netcool/OMNIbus Version 7.3.1 with:
    - Core Fix Pack 3
    - WebGUI Fix Pack 3
    - iFix PM36620
    - iFix PM71389
- Hardware
  - None.

The TOE does not have any direct dependencies on hardware platforms. All environmental support for TOE Security Functionality (TSF) is provided by the TOE's runtime environments, which provide an abstraction layer from the physical (and, in the case of embedded WebSphere Application Server (eWAS), from the operating system layer of the systems,

- User documentation:
  - IBM Tivoli Netcool/OMNIbus Version 7.3.1 Common Criteria Guide
  - IBM Tivoli Netcool/OMNIbus Version 7.3.1 Administration Guide
  - IBM Tivoli Netcool/OMNIbus Version 7.3.1 Installation and Deployment Guide
  - IBM Tivoli Netcool/OMNIbus Version 7.3.1 Probe and Gateway Guide
  - IBM Tivoli Netcool/OMNIbus Version 7.3.1 User's Guide
  - IBM Tivoli Netcool/OMNIbus Version 7.3.1 Web GUI Administration and User's Guide
  - IBM Tivoli Netcool/OMNIbus Probe for SNMP Version 13.0 Reference Guide
  - IBM Tivoli Netcool/OMNIbus Socket Writer Gateway Version 10.0 Reference Guide

3.2. Logical Scope

The description of the security features of the product are described in further details in Section 4. In summary, these functions are:

- Identification and authentication
- Discretionary access control
- Auditing
- Communication security
- Fault tolerance
- Property encryption
- Security function management

4. SECURITY POLICY

4.1. Identification and Authentication

The **ObjectServer** performs authentication of users connecting to it using either an internal repository of users and their passwords, or an external authentication service in the environment. The ObjectServer can be set to use (Pluggable Authentication Module (PAM) (on platforms supporting PAM) or Lightweight Directory Access Protocol (LDAP) for external authentication, offering a variety of authentication methods depending on the PAM modules available. In addition, the ObjectServer implements direct support for authentication against LDAP servers, including Active Directory LDAP servers on Windows. If the ObjectServer is configured to use an external authentication provider, individual user accounts are still being maintained in the ObjectServer's user database, and must be individually configured to be authenticated against the external service.

Users in this authentication context can be both human users and other TOE components. Other TOE components that the ObjectServer authenticates in this way (when running in secure mode) are gateways, probes, Web GUI, and proxies (the latter not being part of the evaluated configuration).

Netcool/OMNIbus, when running on UNIX, also implements an ObjectServer PAM module that other components can use to authenticate against. This allows applications using PAM to authenticate against the user database maintained by the ObjectServer, and includes functionality to change user passwords via the PAM module.

In the evaluated configuration, the ObjectServer supports both PAM (on UNIX) and Active Directory (on Windows) for the authentication of users, as well as its internal authentication mechanism.

Configuration and management utilities that do not connect to the ObjectServer are not subject to the ObjectServer-enforced authentication.

ObjectServer Gateways and **Process Agents** running on UNIX authenticate users that connect to their command port, either via PAM, or against the local UNIX password database (users must be in the ncoadmin group). Process Agents (but not ObjectServer Gateways) running on Windows use the operating system to authenticate the requesting user. Every local or domain user account having access to the Windows host can therefore connect.

Managed processes that report their status back to a Process Agent are not authenticated.

The **TIP** server hosting the Web GUI does not implement authentication, but relies instead on its runtime environment for authentication (see below).

When Transport Layer Security (TLS) is being used (see Communications security below), certificate-based server authentication is employed in the following communication scenarios:

- Gateways, probes, administrative utilities, and the Web GUI authenticate ObjectServers they connect to.
- Clients (e.g., ObjectServers, Administrators) authenticate the Process Agents they connect to.

As a result, connecting clients will verify that the server certificate a) has been issued by a trusted Certificate Authority (CA) and b) contains the Common Name of the server that the client is trying to reach.

The use of TLS is mandatory in the evaluated configuration.

To support rapid deployment in test and secure environments, the ObjectServer, proxy server, and Process Agent will allow certain types of client application to connect without authentication. In the evaluated configuration, this feature must be disabled by running the ObjectServer and Process Agents in secure mode (use of the "SecureMode: TRUE" property on the ObjectServer). In this mode, probe, Socket Gateway, and integration gateway connections to an ObjectServer are authenticated with a user name and password. When the Process Agent is run in secure mode, connections are authenticated before external procedures are run. (Proxy servers are excluded from the evaluated configuration.)

4.2. Discretionary Access Control

The ObjectServer implements a fined-grained authorization system based on users, groups, permissions, and roles. As a result of the ObjectServer being first and foremost a database server, this authorization system primarily targets operations on the databases hosted by the server.

Permissions for individual actions (such as create, insert, alter) on individual objects (tables, rows, triggers, etc.) can be granted to users directly or combined into roles.

Administrators can further define groups that have several users as members, and associate roles defining specific permissions with individual users or groups.

In addition, so-called restriction filters can be defined and assigned to users or groups. Restriction filters are Structured Query Language (SQL) conditions that are being applied when a user accesses data in the database.

Permissions and restriction filters are also applied to queries that users send via the Web GUI, if the requesting user name matches a user name associated with such permissions and restrictions in the ObjectServer. If the user is unknown to the ObjectServer, only read-only access will be granted.(In this case, Web GUI users can read all data that is available to them on the GUI pages that the Virtual Member Manager in the environment grants them access to, as further explained below.)

4.3. Auditing

Actions taken by users generate audit records. These records contain the date, time, event type, identity of the user, and outcome of the action. Only administrators have the ability to review and clear these records.

4.4. Communications Security

Almost all network connections between remote components of the TOE can be (and, in the evaluated configuration, must be) encrypted using TLS.

In addition, remote entities authenticate their communication partners as described in the section on authentication above.

IDUC (insert, delete, update or control) communication is the only unsecured (not encrypted) communication channel in the evaluated configuration of the TOE. IDUC connections are used by ObjectServers to inform the gateways about event updates being available from the server, and are used for data sent through Accelerated Event Notification (AEN) channels.

4.5. Fault Tolerance

The TOE implements several mechanisms that contribute to the availability and correctness of event data:

1. The TOE can replicate data between multiple ObjectServers to ensure consistency of data, even if one of the servers is temporarily unavailable, using bi-directional configurations of ObjectServer Gateways.

2. The ObjectServer maintains a transaction journal file to avoid loss of event data that has not been written to permanent storage yet.
3. Probes can be configured to use a backup ObjectServer if the primary ObjectServer is not available, and store event data in local files for later forwarding if no ObjectServer is available.

4.6. Property Encryption

The TOE implements functionality that can, in addition to the protection measures already in place in the operational environment, be used to further prevent unauthorized access to configuration and TSF data by encrypting it. This functionality is available for:

- property values stored in configuration files for ObjectServers, Probes, and Gateways
- passwords stored on the Web GUI servers
- passwords stored in ObjectServer databases

4.7. Security Function Management

The TOE offers various methods to administrate and configure security functions, including GUI-based standalone and web-based clients, and command line interfaces, as described above.

5. ASSUMPTIONS

The evaluation makes the following assumptions on the TOE environment and personnel managing the TOE:

- The TOE configured and operated in its evaluated configuration as defined in the Security Target and the TOE guidance.

- The machine(s) providing the runtime environment for the TOE are protected against unauthorized physical access and modification.

- The administrator of the TOE, of the TOE's underlying systems, and of the systems in the TOE's operational environment who are involved in safeguarding TSF data or providing functionality that the TOE depends on are assumed not to be careless, willfully negligent, or hostile. They will follow and abide by the instructions provided in the administrator guidance that is part of the TOE. They are well trained to securely and trustworthy administer all aspects of the TOE operation in accordance with the Security Target.

- The machines providing the runtime environment for the server components of the TOE (i.e., all components other than those running on user hosts) are assumed to be used solely for this purpose and not to run other application software except as required for the support of the TOE and for the management and maintenance of the underlying system and hardware.

Especially it is assumed that the underlying systems for all TOE components are configure in a way that prevents unauthorized access – either locally or via any network-based connections – to security functions, TSF and user data, including audit records generated by the TSF.

- The protection of communication over inherently insecure protocols between the TOE and the remote IT entities is assumed to be protected by environmental means as appropriate for the operational environment. This also includes unencrypted communication between probes and any Hypertext Transfer Protocol (HTTP) server that may be used to serve rules files to probes, communication between TOE components over the unencrypted IDUC protocol, and communication between the TOE and authentication providers.

6. PRODUCT TESTING

6.1. Developer Testing

6.1.1. Testing results

The test results provided by the developer were in the form of spreadsheets, where the tester recorded for each test case, the test date, tester name, and test result for each of the platforms. The test result also indicated the build number that was tested as a way to also distinguish the builds used for the regression tests that were performed to fix the discovered defects. Test results from all tested configurations show that the expected test results are consistent with the actual results.

6.1.2. Test coverage

The test coverage analysis provided by the developer shows that the coverage of the TSFIs is complete. The test cases provide coverage of the following TSFI groups:

- **Network - TDS protocol**: identification and authentication of clients connecting to TOE elements (Object Server, Object Server gateway, Socket Writer Gateway and Process Agent);secure communication using the TLS protocol.
- **Network - IDUC**: notification of events to IDUC aware clients.
- **Network - p2p heartbeat connection**: communication between SNMP probes to provide failover capability.
- **Network - SNMP**: encrypted communication with SNMP probe based on SNMP v3.
- **TDS - Object Server SQL**: access control policy on Object Server objects; audit capability.
- **TDS - Object Server RPC**: communication with IDUC aware clients and process agents.
- **TDS - Process Agent RPC**: communication with utilities.
-
- **Process Agent Utilities**: provides access to Process Agent.
- **Database Utilities**: provides management functions on the Object Server database.

- **Crypto Utilities**: encrypt and decrypt property values.
- **Object Server PAM Module**: authentication to a centralized Object Server.
- **Configuration Files**: configuration of secure communication; identification and authentication between TOE elements.
- **Administrator**: secure communication using the TLS protocol; security management functions on the Object Server.
- **SQL interface**: secure communication using the TLS protocol.
- **AEN client**: secure communication using the TLS protocol.

6.1.3. Test depth

Test coverage of all subsystems implementing SFR-enforcing functionality is also ensured by the same set of test cases. The depth analysis provided by the developer shows that the security functionality implemented in the subsystems is covered by the test cases.

6.2. Evaluator Testing

6.2.1. TOE test configuration

The evaluator independently installed the test systems according to the documentation in the Evaluated Configuration Guide and the test plan. The hardware is located at the CCTL in Austin, Texas.

The test environments used for the independent test consist of the systems shown in the table below:

ID	Platform	Hostname / IP address	TOE binaries	Purpose
Host 1	Microsoft Windows 2008	primary.ibm192.168.100.10	ObjectServer (NCOMS),ObjectServer Gateway(NCO_GATE), Socket Writer Gateway (NCO_SOGATE), WebGUI Server	Omnibus primary server
Host 2	Microsoft Windows 2008	secondary.ibm192.168.100.11	ObjectServer (NCOMS_BU),SNMP Probe	Omnibus secondary server
Workstation	Microsoft Windows 2008	workstation.ibm192.168.100.12	Administrator Client, AEN client, SQL client	Omnibus secondary server
Host 3	Ubuntu Linux	probed.ibm192.168.100.13	Not applicable	Helper system

The chosen configuration for the test machines matches one of the supported platforms specified in the Security Target, [ST], i.e., Microsoft Windows Server 2008.

The test cases were executed in the evaluated configuration which was setup and configured according to Security Target, [ST], and the Common Criteria Guide, [TNO-CCG].

The operational environment used for independent testing also included a helper system (Ubuntu Linux) which provides the following utilities:

- netcat: for receiving messages from the socket writer gateway.
- snmptrap: for sending SNMP v3 messages to the SNMP probe.

6.2.2. Subset size chosen

The test cases were either reproduced from the existing developer test cases or newly created concentrating in the specific areas where the evaluator considered that the developer's test scope could be enhanced. Emphasis was made on the security functionality aspects related to identification and authentication, password policy, and ObjectServer access control policy.

6.2.3. Evaluator tests performed

In addition to a subset of developer tests, the evaluator devised tests for a subset of the TOE. The tests are listed in the Evaluator Test Plan.

The evaluator has chosen these tests for the following reasons:

- **Selection criteria**

The tests were devised for functional areas that triggered the evaluation team’s attention during the evaluation of the developer's provided evidence including the ST, design documentation and guidance documentation. Also, new tests were derived in the cases where the evaluation team decided that the assurance provided by this evaluation would benefit from the augmentation of the developer's test scope.

- **Security functions tested**

The devised tests covered a broad range of security functionality, especially identification and authentication, password policy enforcement, and access control policy enforcement. Exercise of other security functionality aspects like audit generation, security management, and secure communications were also collateral to the test subset.

6.2.4. Evaluator Penetration Testing

The penetration testing effort was primarily focused on the web interface to the TOE, as the evaluator concluded that the web interface was the primary attack surface and, in general, tends to contain the most security flaws. The evaluator utilized two primary tools for the penetration testing that are not part of the TOE. He used the Firefox browser with the Firebug extension for examining the HTML, Javascript, and overall Document Object Model (DOM) structure of the web application.

He also used Burp Proxy, an interceptor proxy that allowed the evaluator to monitor, intercept, and edit requests and responses between the server and the client.

The configuration of the TOE was set up according the to the evaluated configuration guide. In actuality, it was the same set up used for the purposes of the independent testing. In summary, the TOE was configured on x86 virtual machines running Windows Server 2008 R2. One machine contained the primary ObjectServer and the WebGUI, one contained the secondary ObjectServer, one contained the Administrative client applications, and one was a machine monitored by the TOE. However, the evaluator primarily interacted with just the WebGUI. (He also touched the client software and viewed the audit trails for one or two small tests).

The penetration testing effort had a large amount of depth in testing the web application of the TOE. The Open Web Application Security Project (OWASP) Top Ten vulnerabilities for 2011 were used to focus the search for the most common vulnerabilities found in websites. The evaluator covered a significant portion of the web site navigable by a user, as well as used spidering tools in Burp Proxy to identify the less-known HTTP,

However, the evaluator does note that the complexity of the TOE is large. This complexity makes it difficult to delve very far past the attack surface into the TOE. Given that the time spent testing was about fifty person hours, exploitable vulnerabilities may exist that were not uncovered by this analysis.

The vulnerabilities that *were* uncovered include two HTML and Javascript injection attacks that can lead to Cross Site Scripting exploits. Such attacks could lead to privilege escalation within the TOE. However, the evaluator did not attempt to fully exploit the vulnerabilities, but only to prove that it exists. The developer was informed of the vulnerability and patched the system. After the patch was provided to the evaluator, the evaluator confirmed that the vulnerability no longer exists in the TOE.

The evaluator also identified a vulnerability where passwords that were rejected by the TOE are recorded in the audit logs. Although the passwords are not actual TSF data, they can be similar to the actual authentication tokens of the users.

This was considered a residual vulnerability due to the inaccessibility of attackers to the audit trail.

6.2.5. Summary of Evaluator Test Results

All tests passed successfully.

The test results demonstrate that the TOE behaved as expected and that the developer test execution were repeatable and the test results were reproducible.

1. PRODUCT GUIDANCE DOCUMENTATION

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- IBM Tivoli Netcool/OMNIbus Version 7.3.1 Common Criteria Guide
- IBM Tivoli Netcool/OMNIbus Version 7.3.1 Administration Guide
- IBM Tivoli Netcool/OMNIbus Version 7.3.1 Installation and Deployment Guide
- IBM Tivoli Netcool/OMNIbus Version 7.3.1 Probe and Gateway Guide
- IBM Tivoli Netcool/OMNIbus Version 7.3.1 User's Guide
- IBM Tivoli Netcool/OMNIbus Version 7.3.1 Web GUI Administration and User's Guide
- IBM Tivoli Netcool/OMNIbus Probe for SNMP Version 13.0 Reference Guide
- IBM Tivoli Netcool/OMNIbus Socket Writer Gateway Version 10.0 Reference Guide

7. RESULTS OF THE EVALUATION[1]

The evaluation team determined the product to be Common Criteria (CC) Part 2 conformant, CC Part 3 conformant, and to meet the requirements of EAL 4 augmented by ALC_FLR.3. In short, the product satisfies the security technical requirements specified in IBM Tivoli Netcool/OMNIbus Version 7.3.1 Security Target on platforms listed in Table 1: Evaluation Identifiers.

8. VALIDATOR COMMENTS

The Common Criteria Guide (Chapter 6, “Passwords” section) describes the detailed behavior of the password policy. The behavior might be confusing to end-users due to the rejection of passwords that contain certain special characters (e.g., ‘=’ and ‘%’) or that do not satisfy the password policy in the leading characters of passwords longer than the minimum characters required by the policy. A change request was submitted to update a future version of the TOE to support a password policy `that is less confusing (IBM defect number: alm00288001).

Section 6.2.4 of this report noted that actual passwords that were rejected during the time password creation are recorded in the audit logs. A change request was submitted to update a future version of the TOE to remove the logging of rejected passwords (IBM defect number: alm00270121).

9. SECURITY TARGET

IBM Tivoli Netcool/OMNIbus 7.3.1 Security Target Version 2.10 is included here by reference.

[1] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

10. LIST OF ACRONYMS

AEN	Advanced Encryption Mechanism
CA	Certificate Authority
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
DOM	Document Object Model
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
eWAS	embedded WebSphere Application Server
IDUC	Insert, Delete, Update, or Control
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
P2P	Peer-to-Peer
TLS	Transport Layer Security
ST	Security Target
TDS Protocol	Tabular Data Stream Protocol
TOE	Target of Evaluation
TIP	Tivoli Integrated Portal
TNO-CCG	Tivoli Netcool//OMNibus Common Criteria Guide
TSF	TOE Security Function

TSFI TOE Security Function Interface

11. BIBLIOGRAPHY

- Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1.
- Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1.
- Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1.
- Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, Version 3.1.
- Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, Version 3.1.Test Results
- Independent Test Plan, v1.4, 2012-10-02
- Evaluation Technical Report, ASE, v2.8, 2012-10-02
- Evaluation Technical Report, ADV, ADV_FSP.4, v2.2, 2012-10-02
- Evaluation Technical Report, ADV, ADV_TDS.3, v1.1, 2012-10-02
- Evaluation Technical Report, ADV, ADV_ARC.1, v1.1, 2012-10-02
- Evaluation Technical Report, ADV, ADV_IMP.1.1, v1.1, 2012-10-02
- Evaluation Technical Report, AGD, v2.0, 2012-09-26
- Evaluation Technical Report, ALC, v2.0, 2012-09-27
- Evaluation Technical Report, ATE, v2.4, 2012-10-02
- Evaluation Technical Report, AVA, v2.2, 2012-10-02
- Evaluation Technical Report, IND, v1.2, 2012-10-02
- Evaluation Technical Report for a Target of Evaluation, ETR, v1.0, 2011-10-02
- Site Visit Report, v1.0, 2012-10-02