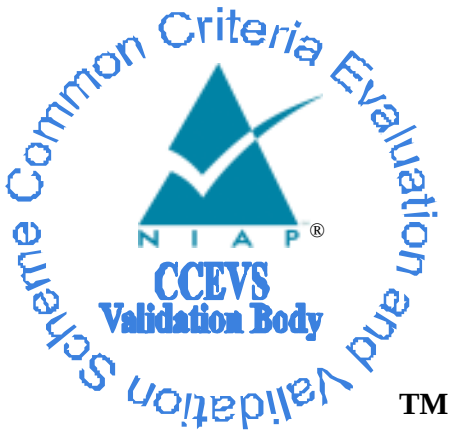
National Information Assurance Partnership



TM

Common Criteria Evaluation and Validation Scheme Validation Report

Infoblox Trinzic Appliances with NIOS v6.3 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010)

Report Number: CCEVS-VR-VID10465-2012
Dated: 17 December 2012
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

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Mario Tinto (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Computer Sciences Corporation
7231 Parkway Drive
Hanover, Maryland 21076

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10 where any restrictions are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Infoblox Trinzic Appliances with NIOS 6.4 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the Infoblox Trinzic Appliances with NIOS 6.4 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010) was performed by the Computer Sciences Corporation (CSC), the Common Criteria Testing Laboratory, in Hanover, Maryland USA and was completed in November 2012.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Computer Sciences Corporation on behalf of Infoblox. The ETR and test report used in developing this validation report were written by CSC. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, dated July 2009 at Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2 and ALC_DVS.1. The Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 3, dated July 2009 was used for this evaluation. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the Infoblox Trinzic Appliances with NIOS 6.4 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010) Security Target. The evaluation team determined the product to be both Part 2 extended and Part 3 augmented compliant, and meets the assurance requirements of EAL 2 augmented by ALC_FLR.2 and ALC_DVS.1. All security functional requirements are derived from Part 2 of the Common Criteria.

The Infoblox Trinzic Appliances with NIOS 6.4 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010) are a family of network appliances which consolidate the delivery and management of core IP network services historically provided by multiple general purpose operating systems and servers (core IP network services

include DNS, DHCP, IPAM, FTP, TFTP, and HTTP). The NIOS operating system is a hardened version of the Fedora Linux distribution optimized for security and network performance. The appliance models are differentiated by performance, capacity and availability to support various deployment scenarios such as a branch-office or large enterprise.

1.1 Interpretations

There are no applicable Common Criteria interpretations.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, 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 conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) 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 (if any); and
- 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	Infoblox Trinzic Appliances with NIOS 6.3 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010).
Protection Profiles	None.
Security Target	*Infoblox Trinzic Appliances with NIOS v.6.3 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010) Security Target*, Version 1.0, Revision 20, September 25, 2012
Dates of evaluation	May 2011 through November 2012
Evaluation Technical Report	*Evaluation Technical Report for Infoblox Trinzic Appliances with NIOS v.6.3 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010),* Version 1.0, September 29, 2012
Conformance Result	Part 2 extended conformant and EAL2 Part 3 augmented with ALC_FLR.2 and ALC_DVS.1
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009 and all applicable NIAP and International Interpretations effective on May 23, 2011
Common Evaluation Methodology (CEM) version	CEM version 3.1R3 dated July2009and all applicable NIAP and International Interpretations effective on May 23, 2011
Sponsor	Infoblox, 4750 Patrick Henry Drive, Santa Clara, CA 95054
Developer	Infoblox, 4750 Patrick Henry Drive, Santa Clara, CA 95054
Common Criteria Testing Lab	Computer Sciences Corporation, 7231 Parkway Drive, Hanover, MD 21076
Evaluators	John Daniels, Timothy R. Cochrane, Annette Nadeau
Validation Team	Mario Tinto and Mike Allen of the Aerospace Corporation

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

None

International Interpretations

None

3 Security Policy

The TOE enforces the following security policies:

- **Secure management.** Administrators manage the TOE via a TLS protected web GUI or via the CLI console port. The TOE implements role based access control, password based authentication and auditing of management functions. Communication with the TOE's API interface is protected by TLS.
- **High availability.** The TOE enforces quotas on exhaustible resources thereby preventing failover due to resource exhaustion.
- **Trusted updates.** The TOE uses digital signatures to verify updates prior to installation.
- **Self protection.** The TOE performs self-test at startup to verify the integrity of hardware components and the cryptographic module.
- **Secure DNS.** The TOE employs secure DNS protocols to verify and authenticate DNS updates.
- **Secure Grid.** The TOE uses an SSL/TLS VPN to protect communication between itself and other TOE instances when deployed in a grid.

A complete list of the security functions of the TOE is provided at section 5.1.

4 Assumptions and Clarification of Scope

The assumptions, threats and policies in the following paragraphs were considered during the evaluation of the Infoblox Trinzic Appliances with NIOS 6.4 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010).

4.1 Assumptions

The ST identified the following security assumptions:

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- External authentication entities will be properly configured and operate correctly.

4.2 Threats

The ST identified the following threats addressed by the TOE:

- Persons who are not permitted to use the TOE who may attempt to use the TOE
- Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized
- Persons who are authorized to use the TOE who may attempt to access data in ways for which they not authorized
- Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats

4.3 Organizational Security Policies

The ST identified the following OSP addressed by the TOE:

- The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation and how the TOE needs to be configured to ensure it operates in the evaluated configuration.

The TOE's evaluated configuration consists of the following configuration settings:

- DNSSEC is enabled (zone policy configured according to user needs)
- TSIG is configured for dynamic DNS updates from ISC DHCP servers and DNS clients (if applicable to the environment)
- GSS-TSIG is configured for dynamic DNS updates from Microsoft DHCP servers and DNS servers and clients (if applicable to the environment)
- bloxTools is disabled
- SSH is disabled (CLI access is performed via the local consol port)
- RADIUS authentication is disabled
- TACACS+ authentication is disabled
- Secure Copy (SCP) is disabled / not used

5 Architectural Information

5.1 Logical Scope and Boundary

The TOE logical scope and boundary consists of the security functions provided/controlled by the TOE as follows:

- **Communication.** The TOE communicates with other network devices, as well as administrators, over the network. The critical communication paths and their related protection mechanisms are as follows:
    - **Grid communication.** The TOE may be configured to communicate with other TOE instances in a grid. This communication is protected via an SSL/TLS VPN
    - **Remote Administration.** Remote administrators configure the TOE via a web based GUI that is protected using TLS/HTTPS
    - **Application Programming Interface.** The TOE provides a Perl API to assist integration of the Infoblox device into network environments. The API is protected using TLS/HTTPS. The Perl API provides interfaces to DHCP, DNS, Grid and IPAM services
    - **DNS.** The TOE implements DNSSEC, TSIG (Transaction SIGnature) and GSS-TSIG (Generic Security Service Algorithm for Secret Key Transaction) to verify DNS updates between itself and other trusted IT products
- **Trusted Updates.** The TOE provides security administrators with the ability to query the current version of the TOE firmware/software and perform updates. The TOE verifies RSA digital signatures associated with TOE updates. The certificate used for validation is stored in a protected file on the appliance.
- **Audit.** The TOE generates audit records associated with use of the administrative functions. Audit records may be stored locally or on a Syslog server. The TOE deletes the oldest records if the audit trail exceeds a defined maximum. A local time source supports reliable time stamps for the audit function.
- **Access.** The TOE provides administrative access via a console port (local) and HTTPS (remote). The TOE provides a password-based logon mechanism for local and remote access and enforces a defined password complexity and expiration policy. The TOE optionally supports authentication against an Active Directory server. The TOE enforces Role Based Access Control (RBAC), session timeouts and displays an advisory banner at login.
- **Resource Exhaustion.** The TOE enforces maximum quotas on log files, uploaded files and number of simultaneous GUI and API sessions.

- **User Data Disclosure.** The TOE ensures that any previous information content of a resource is made unavailable upon the allocation of the resource to all objects by clearing the residual information before network packets are sent from the TOE.

- **Self-Test.** The TOE implements self-test, during initial startup, to verify the basic hardware components that the TOE is reliant upon, and also verify the integrity of the cryptographic module. The TOE will log to sys log (internal system log) when the test runs on power-up. In the event of failure, the TOE is not permitted to use cryptography services and the appliance will start in a broken state where the only permitted access is via the physical serial port. For appliances with an LCD panel on the front, they will display a failure message.

5.2 Physical Scope and Boundary

Infoblox Trinzic Appliances with NIOS 6.4 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010) is a network appliance which consolidate the delivery and management of core IP network services historically provided by multiple general purpose operating systems and servers (core IP network services include DNS, DHCP, IPAM, FTP, TFTP, and HTTP).

The NIOS operating system is a hardened version of the Fedora Linux distribution optimized for security and network performance.

The appliance models are differentiated by performance, capacity and availability to support various deployment scenarios such as a branch-office or large enterprise.

The following figure depicts the TOE.

Figure 1: Infoblox Trinzic Appliance with NIOS v6.3 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 andIB-4010)

The various software and firmware that comprise the TOE are listed in Table 1. A system administrator can ensure that they have a TOE by logging into the device as an administrator, pulling up the “Grid Manager”, clicking on the “Upgrade” tab, and comparing the version numbers reported on the sheet to the table below.

Table 1: Evaluated version

Software/Firmware Item	Infoblox with NIOS v6.3 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 andIB-4010)
System Software	6.3.15

6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Infoblox Trinzic Appliances with NIOS 6.4 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010). Note that not all evidence is available to customers. The following documentation is available to the customer:

- Infoblox Administrator Guide (6.3)
- Infoblox CLI Guide (NIOS 6.3)
- Infoblox API Documentation (NIOS 6.3)
- Infoblox CSV Import Reference (NIOS 6.3)
- Infoblox Installation Guide for the Trinzic 800 Appliances
- Infoblox Installation Guide for the Trinzic 1400 Appliances
- Infoblox Installation Guide for the Trinzic 2200 Appliances
- Infoblox Installation Guide for the IB-4010 Appliance
- Infoblox Installation Guide for the Trinzic Reporting 1400 Appliance
- Infoblox Installation Guide for the Trinzic Reporting 2200 Appliance
- Infoblox Installation Guide for the Trinzic Reporting 4000 Appliance
- NIOS 6.3.15 Release Notes
- Infoblox Safety Guide
-

The remaining evaluation evidence is described in the Evaluation Technical Report developed by Computer Sciences Corporation.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer testing

Test procedures were written by the developer and designed to be conducted using manual interaction with the TOE interfaces. The developer tested all of the interfaces to the TOE and in doing so tested all TSFs.

The developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included with each of the tests in the TOE Test Procedures. Each test case was assigned an identifier that was used to reference it throughout the testing evidence.

The evaluation team analyzed the developer's testing to ensure adequate coverage for EAL 2. The evaluation team determined that the developer's actual test results matched the developer's expected test results.

The evaluators assessed that the test environment used by the developers was appropriate and mirrored the test configuration during independent testing.

7.2 Evaluation team independent testing

The evaluation team conducted independent testing at the CCTL facility. The TOE was delivered in accordance with the documented delivery procedures. The evaluation team installed and configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while the associated ATE_IND work units. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the developer's test plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team repeated a sample of the developer's test cases and designed additional independent tests. The additional test coverage was determined based on the analysis of the developer test coverage and the ST.
The evaluators examined the design evidence and selected an appropriate test platform. Each TOE Security Function was exercised and the evaluation team verified that each test passed.

7.3 Vulnerability analysis

The evaluation team performed a vulnerability analysis of the TOE evidence and a search of publicly available information to identify potential vulnerabilities in the TOE. Based on the results of this effort, the evaluation team conducted penetration testing to determine if the identified potential vulnerabilities were indeed exploitable.

The evaluation team concluded that the TOE does not contain exploitable vulnerabilities in the intended environment and for the postulated attackers.

8 Evaluated Configuration

The TOE consists of one of several hardware devices and the installed software applications. The Infoblox Trinzic Appliances with NIOS 6.4 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010) must be configured in accordance with the guidance documents listed at section **Error! Reference source not found.**.

.

9 Results of the Evaluation

Computer Sciences Corporation (CSC) determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 augmented with ALC_FLR.2 and ALC_DVS.1. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation and validation efforts were finished on December 17, 2012.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Infoblox Trinzic Appliances with NIOS 6.4 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010) meet the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

- The user of this product should carefully review the restrictions on the evaluated configuration documented in the Clarification of Scope Section 4.3 of this report.
- The user should be aware that the product provides no alarms or warnings when the audit records are full. When the audit record limit is reached (i.e., 10 audit files of 100MB each) the oldest records are overwritten. If audit records are to be protected from loss, the administrator must follow the administrator guidance for management and maintenance of audit logs to move them to secure archival storage. The protection of these archival records is beyond the scope of the evaluated configuration.

11 Security Target

Infoblox Trinzic Appliances NIOS 6.3 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010) Security Target, Version 1.0, Revision 20, September 25, 2012.

12 Glossary

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Anything (manmade or act of nature) that has a potential to do harm to an IT system or product. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1 R3, July 2009.
- Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1 R3, July 2009.
- Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1 R3, July 2009.
- Common Criteria Project Sponsoring Organisations. *Common Methodology for Information Technology Security Evaluation*, Version 3.1 R3, July 2009.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 2.0, September 8, 2008.
- *Infoblox Trinzic Appliances with NIOS 6.3 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010) Security Target*, Version 1.0, Revision 20, September 25, 2012.
- *Computer Sciences Corporation (CSC) Evaluation Technical Report for Infoblox Trinzic Appliances with NIOS 6.3 (Models: IB-810, IB-820, IB-1400, IB-1410, IB-1420, IB-2200, IB-2210, IB-2220, IB-4000 and IB-4010)*, Version 1.1, September 29, 2012.