National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

For

Opsware System 4.5 Patch 1

Report Number: CCEVS-VR-05-0133

Dated: December 12, 2005

Version: 2.3

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Nicole Carlson, Lead Validator

Dr. Deborah D. Downs, Senior Validator

The Aerospace Corporation

El Segundo, California

Common Criteria Testing Laboratory

Science Applications International Corporation (SAIC)

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Opsware's Opsware 4.5 Patch 1 product. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in October 2005. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 and Part 3 Conformant**, and meets the assurance requirements of EAL 2. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria.

During this validation, the Validator monitored the activities of the SAIC evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. The Validator determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

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 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;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Opsware System 4.5 Patch 1
Protection Profile	None
Security Target	*Opsware System 4.5 Patch 1, Version 1.0, October28, 2005*
Evaluation Technical Report	*Evaluation Technical Report for Opsware System 4.5 Patch 1:* • *Part 1 (Non-Proprietary), Version 4.0,* • *Part 2 (Proprietary), Version 1.0,*
Conformance Result	Part 2 and Part 3 Conformant, EAL 2
Sponsor	Opsware
Developer	Opsware
Evaluators	Science Applications International Corporation (SAIC)
Validator	The Aerospace Corporation

3. SECURITY POLICY [1]

User Data Protection

The TOE enforces a Management Access Control policy, which restricts access to the management functions of the TOE. This protection requires that users of the TOE be authenticated before any access to the management functions is granted. Once access is granted, user access to management functions is controlled by the assigned user privileges.

Identification and Authentication

The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. The TOE provides the ability to define levels of authority for users, providing administrative flexibility. Full administrators have the ability to define groups and their authority and they have complete control over the TOE. In Opsware security privileges are associated with Groups, and it is by assigning users to one or more groups that users get access to features within Opsware. Groups are managed by authorized administrators, and all discussion of "security privileges" in this document should be understood to mean Groups and their associated privileges to access various parts of the TOE.

3.1. Usage Assumptions

Administrators are assumed to be non-hostile, appropriately trained and follow all administrator guidance.

The TOE is managed through the Opsware Command Center, a web-based interface. Through this interface TOE management can be performed by providing the administrators the ability to manage user attributes and privileges, as well as assign roles for different levels of administrative access.

3.2. Environmental Assumptions

It is assumed that all components, except for the Agent, are installed on the same platform. The Agent must be installed on each server that is managed by the TOE. Therefore, the only disparate communication is between the Agent and the core components (e.g. Command Engine, Software Repository).

It is also assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

Lastly, it is assumed that the IT environment provides support commensurate with the expectations of the TOE. This is achieved by using evaluated products (or products in evaluation at the time of

[1] Some of this information is drawn from [7].

the writing of this VR) in the environment. The expectations of the TOE with respect to the security provided by the IT environment are captured in the ST in the environmental objectives. Users of this product should be clearly aware of the assumptions in the ST regarding the environment of use.

4. ARCHITECTURAL INFORMATION[2]

This section provides a high level description of the TOE and its components as described in the Security Target.

The TOE preserves management knowledge for system administrators, network engineers, and database administrators in a centralized knowledgebase (referred to as the Model Repository), which can then be tapped for future actions, allowing this knowledge to be preserved and used by all administrators in the system.

The TOE is comprised of the following components: Opsware Command Center, Data Access Engine, Model Repository, Software Repository, Command Engine, and the Opsware Agent installed on the managed servers.

These components communicate over encrypted channels using SSL (Secure Sockets Layer). SSL is FIPS-certified cryptography, but is not further evaluated here.

Opsware Command Center - The Opsware Command Center (OCC) is the primary user interface to the TOE. Users accessing the Opsware Command Center are authenticated before gaining access. Through the Opsware Command Center's web-based user interface (UI), the user can view and update the systems being managed by the TOE. The Opsware Command Center operates primarily via the Data Access Engine, though it talks directly to other backend services to implement some operations. These backend services are considered part of the TOE and are installed during TOE installation. These backend services are an Apache web server, BEA's WebLogic application server, and a Netscape Directory Server LDAP server. Opsware uses an Apache web-server to support protection of internal TOE communication by performing SSL encryption through Apache's OpenSSL-based cryptographic module. The Opsware Command Center server is implemented in Java using the BEA WebLogic platform as the application server. Opsware uses a LDAP directory server to store authentication data (e.g. usernames, passwords).

Data Access Engine - The Data Access Engine provides the public API (Application Programming Interface) to the Model Repository. All clients of the Model Repository interact with the Model Repository via APIs defined by the Data Access Engine. Because interactions with the Model Repository go through the Data Access Engine, clients are sheltered from details of and changes to the Model Repository's implementation. The Data Access Engine abstraction also eliminates the need to bind database libraries into every program that implements Opsware System 4.5 Patch 1. The Data Access Engine is implemented as a server and hence its API is a network protocol. The protocol for transport of requests to the Data Access Engine is HTTP over the Secure Socket Layer protocol, sometimes referred to as "HTTPS" or "HTTP over SSL." The requests and responses are encoded in an XML dialect known as XML-RPC. This makes the Data Access Engine's network API language-independent.

[2] Information drawn from [8]

Model Repository - The TOE is model-based. Essentially all Opsware System 4.5 Patch 1 tools work from or record into a model of the systems that are being managed. The TOE component maintaining this model is known as the Model Repository. The Model Repository contains information about servers, network devices, data centers, etc. A data center (usually called Facility in the Opsware System 4.5 documentation) represents a customer site that contains managed servers and or network devices. The Model Repository contains essentially all of the information required to build, operate, and maintain all managed sites. Among other things the Model Repository maintains

- a list of all devices under management (servers, network devices and storage devices)
- the configuration of those devices
- the OS, system software and applications installed on servers
- the configuration of each data center
- authentication and security information

The Model Repository is implemented as an Oracle database.

Software Repository - The Software Repository is the TOE's central repository for all software managed by the TOE. It contains software packages for operating systems, application servers (e.g. WebLogic), databases, and customer code. Software is stored and pulled from the Software Repository via the Word Gateway. The Word Gateway enforces access control and checks for adherence to policies such as naming and versioning. Working with the Software Repository, an Opsware Agent can update the software running on the Opsware Agent's server. This process is often called reconciliation. The Software Repository is also the repository for software configuration information.

Command Engine - The Command Engine is a system for running distributed programs across many servers (usually Opsware Agents). The Command Engine executes scripts written in python, which can make RPC calls on Opsware Agents. These calls are delivered in a secure manner using SSL.

Opsware Agent - Each server managed by the TOE has an agent, named the Opsware Agent, which runs on that managed server. Whenever the Opsware System needs to make changes to servers it does so by sending requests to the Opsware Agent. Depending on the request, the Opsware Agent may use global Opsware System services (such as the Data Access Engine and Software Repository) in order to fulfill the request. Some functions that the Opsware Agent supports are software installation and removal, and configuration of software and hardware. The Opsware Agent is usually idle unless some part of the TOE is trying to effect some change on the server. Periodically the Opsware Agent wakes up and registers itself with the Model Repository. This allows the Model Repository to keep track of machines that have been disconnected from and reconnected to the network. The Opsware Agent is implemented as an HTTP/HTTPS server. As

described earlier in reference to the Data Access Engine, the protocol for communicating with the Opsware Agent is HTTPS and the requests and response are encoded in XML.

5. DOCUMENTATION

The following documentation was used as evidence for the evaluation of Opsware System 4.5 Patch 1:[3]

5.1. Design documentation

Document	Version	Date
Opsware System 4.5 Security Functional Specification, High Level Design, and Correspondence Maps	1.1	26 September 2004

5.2. Guidance documentation

Document	Version	Date
Opsware System 4.5 Administration Guide	Version is related to the Product/TOE version; hence 4.5	cr 2000 - 2004
Opsware System 4.5 User Guide	Version is related to the Product/TOE version; hence 4.5	cr 2000 - 2004
Opsware System 4.5 Documentation Addendum	Version 1.0 – Draft 2	20 September 2005

5.3. Configuration Management and Lifecycle documentation

Document	Version	Date
Opsware System 4.5 Configuration Management and Delivery for Common Criteria	Version 1.0, Draft 2	29 September 2005

[3] This documentation list is extracted from the Evaluation Technical Report, Part 1, developed by SAIC.

5.4. Delivery and Operation documentation

Document	Version	Date
Opsware System 4.5 Configuration Management and Delivery for Common Criteria	Version 1.0, Draft 2	29 September 2005
Opsware System 4.5 Installation Guide	Version is related to the Product/TOE version; hence 4.5	cr 2000 - 2004

5.5. Test documentation

Document	Version	Date
Opsware System 4.5 Security Test Documentation for Common Criteria	Version 1.1	9 March 2004
Test Cases Excel Spreadsheet	Version 1.0 draft 2	28 October 2005

The actual results are included with the test cases document. The tests are manual tests and the actual results are a pass/fail.

5.6. Vulnerability Assessment documentation

Document	Version	Date
Opsware System 4.5 Vulnerability Assessment for Common Criteria	Version 1.0 Draft 8	27 October 2005

5.7. Security Target

Document	Version	Date
Opsware System 4.5 Security Target	1.0	28 October 2005

6. IT PRODUCT TESTING

6.1. Developer Testing

Evaluator analysis of the developer's test plans, test scripts, and test results indicate that the developer's testing is adequate to satisfy the requirements of EAL 2.

The developer's tests were non-automated, and consisted of a suite of manual tests that covered the security functions claimed in the ST, on both underlying operating systems; Solaris 8 and Red Hat Linux. These verified the basic functionality of the TOE, and exercised the parameters and verified the exception conditions documented in the user and administrative guidance.

For each of the developer tests, the evaluators analyzed the test procedures to determine whether the procedures were relevant to, and sufficient for the function being tested. They also verified that the test documentation showed results that were consistent with the expected results for each test case.

6.2. Evaluator Testing

6.2.1. Functional Testing

In addition to developer testing, the CCTL conducted its own suite of tests

6.2.2. Vulnerability Testing

The evaluators developed vulnerability test to address both management and TOE access security functions, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

7. EVALUATED CONFIGURATION

For Opsware System 4.5 Patch 1 Command Center, any of: Sun Solaris 8, Red Hat Linux Advanced Server (AS) 2.1

For Opsware System 4.5 Patch 1 Agent, any of: Red Hat Linux 6.2, 7.1, 7.2, 7.3, 8.0, AS 2.1, 3.0, Enterprise Server (ES) 2.1, ES 3.0, Workstation 3.0; Sun Solaris SunOS 5.6, 5.7, 5.8, 5.9; HP-UX 10.20, 11.00, 11.11/11i; Windows NT 4.0, Windows Server 2000, Windows Server 2003; AIX 4.3, 5.1, 5.2

8. RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3,4]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [6]; and all applicable International Interpretations in effect on 1 April 2004. The evaluation confirmed that the Opsware System 4.5 Patch 1 product is compliant with the Common Criteria Version 2.1, functional requirements (Part 2) and assurance requirements (Part 3) for EAL 2. The details of the evaluation are recorded in the CCTL's Evaluation Technical Report for the Opsware System 4.5 Patch 1, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the Opsware System 4.5 Patch 1 Security Target v1.0, 28 October 2005.

The Validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication #3 for Technical Oversight and Validation Procedures. The Validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

8.1. Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Opsware System 4.5 Patch 1 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

8.2. Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from Opsware.

8.3. Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification while in transit. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

8.4. Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

8.5. Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

8.6. Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed the entire set of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

8.7. Vulnerability Assessment Activity (AVA)

The Evaluation Team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer vulnerability analysis and the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

8.8. Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the vendor's test suite and the independent tests also demonstrated the accuracy of the claims in the ST.

9. VALIDATOR COMMENTS

The cryptography capabilities of this product were *not* evaluated

The Validator would like to note that this product uses OpenSSL. OpenSSL (a free and open-source implementation of the Secure Sockets Layer protocol) is FIPS-evaluated (140-2 Level 1, certificate #146 awarded May 10 2004), but it was not evaluated further during this evaluation.

10. SECURITY TARGET

Opsware System 4.5 Patch 1 Security Target, version 1.0, 28 October 2005

11. GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration Management
CMP	Configuration Management Plan
DoD	Department of Defense
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OCC	Opsware Command Center
PP	Protection Profile
SAIC	Science Applications International Corporation
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation

TSF	TOE Security Function
TSFI	TOE Security Function Interface
VR	Validation Report

12. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Opsware System 4.5 Patch 1 Security Target, v1.0, 28 October 2005

[8] Evaluation Technical Report for the Opsware System 4.5 Patch 1, Part 1 (Non-Proprietary), Version 4.0 7 December 2005; Part 2 (Proprietary), Version 1.0, 18 October 2005.

[9] Evaluation Team Test Plan For Opsware System 4.5 Patch 1 (SAIC and Opsware Proprietary), Version 2.0, 18 October 2005