Certification Report

HP Server Automation Ultimate v10.10.002

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-328-CR
Version: 1.0
Date: 22 December 2015
Pagination: i to iii, 1 to 9

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI IT Security Evaluation & Test Facility.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 22 December 2015, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

TABLE OF CONTENTS

Executive Summary

HP Server Automation Ultimate v10.10.002 (hereafter referred to as HP SA), from Hewlett Packard Enterprise Development, LP, is the Target of Evaluation. The results of this evaluation demonstrate that HP SA meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

The TOE is an automation software solution, which centralizes and automates server configuration and lifecycle management for the hybrid data center. The TOE scans network to discover servers, and bring them under the TOE management. The TOE installs SA Agent software on the SA Managed Servers to patch, audit, monitor, and maintain those servers.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 22 December 2015 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for HP SA, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the CCS Certification Body, declares that the HP SA evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is HP Server Automation Ultimate v10.10.002 (hereafter referred to as HP SA), from Hewlett Packard Enterprise Development, LP.

2 TOE Description

The TOE is an automation software solution, which centralizes and automates server configuration and lifecycle management for the hybrid data center. The TOE scans network to discover servers, and bring them under the TOE management. The TOE installs SA Agent software on the SA Managed Servers to patch, audit, monitor, and maintain those servers.

A diagram of the HP SA architecture is as follows:

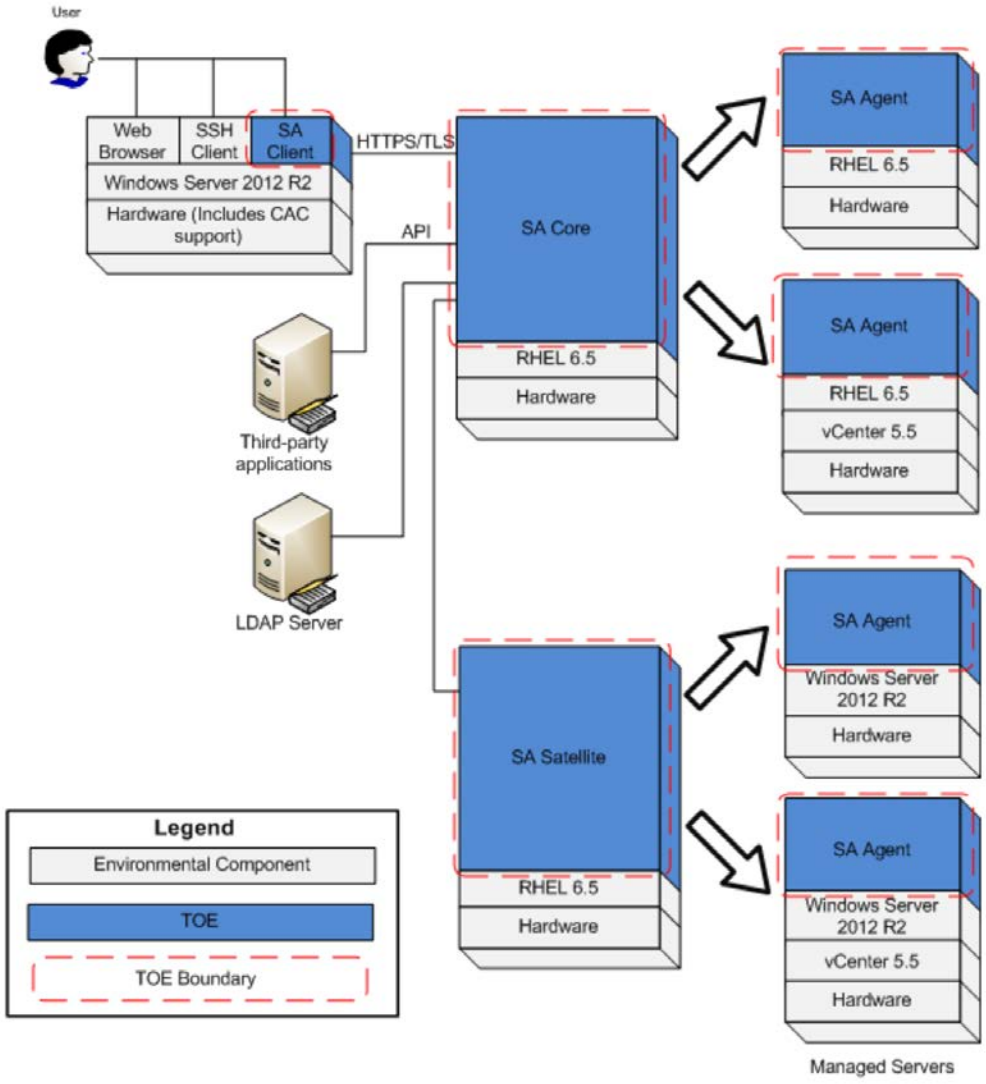

Figure 2 Physical TOE Boundary

3 Security Policy

HP SA implements a role-based access control policy to control administrative access to the system. In addition, HP SA implements policies pertaining to the following security functional classes:

- *Security Audit;*
- *Cryptographic Support;*
- *User Data Protection;*
- *Identification and Authentication;*
- *Security Management;*
- *Protection of the TOE Security Functionality;*
- *TOE Access; and*
- *Trusted Path/Channels.*

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate**
OpenSSL FIPS Object Module, Software Version 2.0.5	1747
RSA Crypto-J Software Module, Software Version 6.1	2057

4 Security Target

The ST associated with this Certification Report is identified below:

Hewlett-Packard Enterprise Development, LP, Server Automation Ultimate v10.10.002 Security Target December 17, 2015, v1.9.

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

HP SA is:

a. *EAL 2 augmented*, containing all security assurance requirements listed, as well as the following:

   - ALC_FLR.2 – Flaw Reporting Procedures.

b. *Common Criteria Part 2 extended*, with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:

   - FAU_GEN_EXT - Security Audit Data Generation – SA Core and SA Client.

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of HP SA should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

6.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

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

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is installed on the appropriate, dedicated hardware and operating system;
- Those responsible for installing the TOE will ensure that the SA Core server is only used for the SA Core and have no other purpose. In addition, the users responsible for installing the TOE will protect the SA Core installation log;
- The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions;
- The TOE is located within a controlled access facility;
- The TOE software will be protected from unauthorized modification; and
- The TOE environment will provide the TOE with the necessary reliable timestamps.

7 Evaluated Configuration

The evaluated configuration for HP Server Automation Ultimate v10.10.002 Build 55.0.51417.0 comprises the following software binaries:

- SA Core; and
- SA Satellite.

Installed on a Red Hat Enterprise Linux 6.5 Base Server with

- SA Agent residing on a Red Hat Enterprise Linux 6.5 Base Server or a Microsoft Windows Server 2012 R2; and
- SA Client residing on a Microsoft Windows Server 2012 R2.

The publication entitled

- Hewlett-Packard Enterprise Development, L.P. Server Automation Ultimate v10.10.002 Guidance Documentation Supplement

describes the procedures necessary to install and operate HP SA in its evaluated configuration.

8 Documentation

The Hewlett Packard Enterprise Development, LP documents provided to the consumer are as follows:

- Hewlett-Packard Enterprise Development, L.P. Server Automation Ultimate v10.10.002 Guidance Documentation Supplement;
- HP Server Automation; Ultimate Edition; Software Version 10.10 Administration Guide;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Installation Guide;
- HP Server Automation; Ultimate Edition; Software Version 10.10; User Guide;
- HP Server Automation; Ultimate Edition; Software Version 10.10; User Guide: Server Automation;
- HP Server Automation; Ultimate Edition; Software Version 10.10; User Guide: Virtualization Management;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Platform Developer Guide;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Release Notes;
- HP Server Automation; Ultimate Edition; Software Version 10.10; FIPS 140-2 Compliance Statement;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Content Utilities;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Storage Visibility and Automation Installation & Administration Guide;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Overview and Architecture;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Reports Guide;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Storage Visibility and Automation Installation and Administration Guide;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Application Configuration;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Application Deployment Manager;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Audit & Compliance;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Server Patching;
- HP Server Automation; Ultimate Edition; Software Version 10.10; Server Automation Visualizer; and
- HP Server Automation; Ultimate Edition; Software Version 10.10; Software Management.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of HP SA, including the following areas:

Development: The evaluators analyzed the HP SA functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the HP SA security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the HP SA preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the HP SA configuration management system and associated documentation was performed. The evaluators found that the HP SA configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of HP SA during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the HP SA. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[1].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. External Authentication: The objective of this test goal is to test external authentication methods;

c. Super Administrator Role: The objective of this test goal is to demonstrate that users without Super Administrator powers cannot manage other users;

d. Audit Generation: The objective of this test goal is to ensure mandatory audit records are generated;

e. HTTP Inaccessible: The objective of this test goal is to show that using insecure channel/protocol HTTP will be blocked;

f. API Auditing: The objective of this test goal is to exercise the Application Programming Interface (API) powers and ensure the proper audit logs are generated; and

g. Move Managed Server: The objective of this test goal is to confirm that managed servers can be moved from CORE to Satellite.

10.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;

b. Open VAS and nmap: The objective of this test goal is to perform port scans and analyze the results;

c. Vulnerability Check: The objective of this test goal is to determine if the Heartbleed, Poodle, Shellshock, Ghost or Freak vulnerabilities are exploitable;

d. Extreme input values: The objective of this test case is to determine how the TOE reacts to extreme input values;

e. Weak Ciphers: The objective of this test goal is to determine if the SSH daemon accepts weak ciphers; and

f. Wireshark sniffer: The objective of this test goal is to confirm that communication to and from the HP SA Core is encrypted.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

10.4 Conduct of Testing

HP SA was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that HP SA behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
API	Application Programming Language
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HTTP	Hypertext Transfer Protocol

Acronym/Abbreviation/ Initialization	Description
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SAV	Service Automation Visualizer
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VAS	Vulnerability Assessment Scanner

13 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Hewlett-Packard Enterprise Development, LP, Server Automation Ultimate v10.10.002 Security Target December 17, 2015, v1.9.

e. Hewlett-Packard Enterprise Development, LP, Server Automation Ultimate v10.10.002 Evaluation Technical Report, December 22, 2015, v0.4.