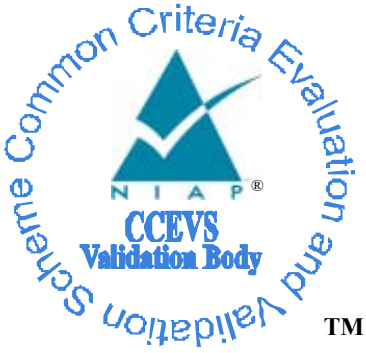
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



TM

Validation Report

Protection Profile for Server Virtualization, Version 1.1, 14 September 2015

Report Number: CCEVS-VR-PP-0043
Dated: 26 January 2018
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

Common Criteria Testing Laboratory

Leidos Common Criteria Testing Laboratory
Columbia, Maryland

Table of Contents

Table of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for Server Virtualization, Version 1.1, also referred to as the Server Virtualization Protection Profile (SVPP). It presents a summary of the SVPP and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the SVPP was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) was the Microsoft hypervisor and virtualization subsystem, known as "Hyper-V for Windows Server 2016, Windows Server 2012 R2, and Windows 10." The evaluation was performed by the Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in November 2017. This evaluation addressed the base requirements of the SVPP, as well as a few of the additional requirements contained in Appendices B through D.

An additional review of the PP was performed independently by the Validation Report (VR) author as part of the completion of this VR, to confirm that it meets the claimed APE assurance requirements.

The evaluation determined that the SVPP is both Common Criteria Part 2 Extended and Part 3 Extended. The PP identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). Because the ST contains only material drawn directly from the SVPP, the majority of the ASE work units serve to satisfy the APE work units as well.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the SVPP meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the Assurance Activity Report (AAR) are consistent with the evidence produced.

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, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against PPs that contain Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

To be thorough and efficient, the evaluation of the SVPP was performed concurrent with the first product evaluation against the PP. The Target of Evaluation (TOE) was the Microsoft "Hyper-V for Windows Server 2016, Windows Server 2012 R2, and Windows 10" server

virtualization product. The evaluation was performed by The Leidos CCTL in Columbia, Maryland, United States of America, and was completed in November 2017.

The SVPP contains a set of "base" requirements that all conformant STs must include, and additionally contains "Optional," "Selection-based," and "Objective" requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in the base requirements and the capabilities of the TOE. Objective requirements are those that specify security functionality that is desirable but is not explicitly required by the PP. The vendor may choose to include such requirements in the ST and still claim conformance to this PP.

Because these discretionary requirements may not be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the SVPP that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the PP subject of the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP and any subsequent evaluations that address additional optional requirements in the SVPP.

Protection Profile	Protection Profile for Server Virtualization, Version 1.1, 14 September 2015
ST (Base)	Microsoft Hyper-V Security Target, Version 0.07, November 17, 2017
Assurance Activity Report (Base)	Microsoft Windows Server 2016, Windows Server 2012 R2, and Windows 10 Hyper-V Assurance Activity Report, Version 1.0, December 7, 2017
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	Leidos Common Criteria Testing Laboratory, Columbia, MD, USA
CCEVS Validators	Paul Bicknell, MITRE
	Sheldon Durrant, MITRE
	Jerome Myers, Aerospace Corporation

3 SVPP Description

The SVPP specifies information security requirements for server virtualization systems, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

Server Virtualization in the context of this PP relates to a virtualization system that implements virtualized hardware components on server-class hardware. It creates a virtualized hardware environment for each instance of an operating system (virtual machines or VMs) permitting these environments to execute concurrently while maintaining the appearance of isolation and exclusive control over assigned computing resources. Each VM instance supports applications such as file servers, web servers, and mail servers. Server virtualization may also support client operating systems in a virtual desktop or thin-client environment.

A Virtualization System (VS) is a software product that enables multiple independent computing systems to execute on the same physical hardware platform without interference from one other. For purposes of this document, the VS consist of a Virtual Machine Manager (VMM), Virtual Machine (VM) abstractions, and other components.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
A.PLATFORM_INTEGRITY	The platform has not been compromised prior to installation of the Virtualization System.
A.PHYSICAL	Physical security commensurate with the value of the TOE and the data it contains is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance.

4.2 Threats

The following table contains applicable threats.

Table 2: Threats

Threat Name	Threat Definition
T.DATA_LEAKAGE	If it is possible for data to leak between domains when prohibited by policy, then an adversary on one domain or network can obtain data from another domain. Such cross-domain data leakage can, for example, cause classified information, corporate proprietary information, or medical data to be made accessible to unauthorized entities.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the Administrator with an update to the product that may compromise the security features of the TOE.
T.UNAUTHORIZED_MODIFICATION	Malware running on the physical host must not be able to undetectably modify Virtualization System components while the system is running or at rest. Likewise, malicious code running

Threat Name	Threat Definition
	within a virtual machine must not be able to modify Virtualization System components.
T.USER_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.3P_SOFTWARE	Vulnerabilities in 3rd party software can lead to VMM compromise. Where possible, the VS should mitigate the results of potential vulnerabilities or malicious content in third-party code.
T.VMM_COMPROMISE	Failure of security mechanisms could lead to unauthorized intrusion into or modification of the VMM or bypass of the VMM altogether.
T.PLATFORM_COMPROMISE	The hosting of untrusted or malicious domains by the VS cannot be permitted to compromise the security and integrity of the platform on which the VS executes.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.WEAK_CRYPTO	A threat of weak cryptography may arise if the VMM does not provide sufficient entropy to support security-related features that depend on entropy to implement cryptographic algorithms.
T.UNMANAGEABLE_NW	The Virtualization System itself is generally part of a larger enterprise network and must be updated and patched as a normal part of enterprise network operations. Such basic network hygiene is more difficult if the enterprise network is unmanageable.

4.3 Organizational Security Policies

No organizational policies have been identified that are specific to server virtualization.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 3: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.VM_ISOLATION	As basic functionality, the VMM must support a security policy that mandates no information transfer between VMs.
O.VMM_INTEGRITY	Integrity is a core security objective for Virtualization Systems. To achieve system integrity the integrity of each VMM component must be established and maintained. This objective concerns only the integrity of the Virtualization System—not the integrity of software running inside of VMs or of the physical platform. The overall objective is to ensure the integrity of critical components of a Virtualization System.
O.PLATFORM_INTEGRITY	The integrity of the VMM depends on the integrity of the hardware and software on which the VMM relies. Although the VS does not have complete control over the integrity of the platform, the VS should as much as possible try to ensure that no users or software

TOE Security Obj.	TOE Security Objective Definition
	hosted by the VS is capable of undermining the integrity of the platform.
O.DOMAIN_INTEGRITY	The VS is responsible for ensuring that software running in Guest VMs is not interfered with by VMs from other domains.
O.MANAGEMENT_ACCESS	Management functions must be exercised only by authorized Administrators.
O.MANAGEABLE_NETWORK	The VS must support standards and protocols that help enhance manageability of the VS as an IT product.
O.AUDIT	The purpose of audit is to capture and protect data about what happens on a system so that it can later be examined to determine what has happened in the past.

The following table contains objectives for the Operational Environment.

Table 4: Security Objectives for the Operational Environment

Environmental Security Obj.	TOE Security Objective Definition
OE.CONFIG	TOE administrators will configure the Virtualization System correctly to create the intended security policy.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5 Requirements

As indicated above, requirements in the SVPP are comprised of the "base" requirements and additional requirements that are conditionally optional. The following table contains the "base" requirements that were validated as part of the Microsoft Hyper-V evaluation activity referenced above.

Table 5: Base Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Microsoft Hyper-V Security Target
	FAU_SAR.1: Audit Review	Microsoft Hyper-V Security Target
	FAU_STG.1: Protected Audit Trail Storage	Microsoft Hyper-V Security Target
	FAU_STG_EXT.1: Off-Loading of Audit Data	Microsoft Hyper-V Security Target
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	Microsoft Hyper-V Security Target
	FCS_CKM.2: Cryptographic Key Establishment	Microsoft Hyper-V Security Target
	FCS_CKM_EXT.4: Cryptographic Key Destruction	Microsoft Hyper-V Security Target
	FCS_COP.1(1): Cryptographic Operation (AES Data Encryption/Decryption)	Microsoft Hyper-V Security Target
	FCS_COP.1(2): Cryptographic Operation (Hashing)	Microsoft Hyper-V Security Target

Requirement Class	Requirement Component	Verified By
	FCS_COP.1(3): Cryptographic Operation (Signature Algorithms)	Microsoft Hyper-V Security Target
	FCS_COP.1(4): Cryptographic Operation (Keyed Hash Algorithms)	Microsoft Hyper-V Security Target
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)	Microsoft Hyper-V Security Target
	FCS_ENT_EXT.1: Extended: Entropy for Virtual Machines	Microsoft Hyper-V Security Target
FDP: User Data Protection	FDP_VMS_EXT.1: VM Separation	Microsoft Hyper-V Security Target
	FDP_PPR_EXT.1: Physical Platform Resource Controls	Microsoft Hyper-V Security Target
	FDP_VNC_EXT.1: Virtual Networking Components	Microsoft Hyper-V Security Target
	FDP_RIP_EXT.1: Residual Information in Memory	Microsoft Hyper-V Security Target
	FDP_RIP_EXT.2: Residual Information on Disk	Microsoft Hyper-V Security Target
	FDP_HBI_EXT.1: Hardware-Based Isolation Mechanisms	Microsoft Hyper-V Security Target
FTP: Trusted Path/Channel	FTP_TRP.1: Trusted Path for Remote Administration	Microsoft Hyper-V Security Target
	FTP_UIF_EXT.1: User Interface: I/O Focus	Microsoft Hyper-V Security Target
	FTP_UIF_EXT.2: User Interface: Identification of VM	Microsoft Hyper-V Security Target
FIA: Identification and Authentication	FIA_PMG_EXT.1: Extended: Password Management	Microsoft Hyper-V Security Target
	FIA_UIA_EXT.1: Administrator Identification and Authentication	Microsoft Hyper-V Security Target
	FIA_X509_EXT.1: X.509 Certificate Validation	Microsoft Hyper-V Security Target
	FIA_X509_EXT.2: X.509 Certificate Authentication	Microsoft Hyper-V Security Target
FMT: Security Management	FMT_SMR.2: Restrictions on Security Roles	Microsoft Hyper-V Security Target
	FMT_MSA_EXT.1: Default Data Sharing Configuration	Microsoft Hyper-V Security Target
	FMT_MOF_EXT.1: Management of Security Functions Behavior	Microsoft Hyper-V Security Target
	FMT_SMO_EXT.1: Separation of Management and Operational Networks	Microsoft Hyper-V Security Target
FPT: Protection of the TSF	FPT_TUD_EXT.1: Trusted Updates to the Virtualization System	Microsoft Hyper-V Security Target
	FPT_VIV_EXT.1: VMM Isolation from VMs	Microsoft Hyper-V Security Target
	FPT_HCL_EXT.1: Hypercall Controls	Microsoft Hyper-V Security Target
	FPT_VDP_EXT.1: Virtual Device Parameters	Microsoft Hyper-V Security Target

Requirement Class	Requirement Component	Verified By
	FPT_HAS_EXT.1: Hardware Assists	Microsoft Hyper-V Security Target
	FPT_EEM_EXT.1: Execution Environment Mitigations	Microsoft Hyper-V Security Target
	FPT_RDM_EXT.1: Removable Devices and Media	Microsoft Hyper-V Security Target
	FPT_DVD_EXT.1: Non-Existence of Disconnected Virtual Devices	Microsoft Hyper-V Security Target

The following table contains the "**Optional**" requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Table 6: Optional Requirements

Requirement Class	Requirement Component	Verified By
FTA: TOE Access	FTA_TAB.1: TOE Access Banners	Microsoft Hyper-V Security Target

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Table 7: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1.1 Auditable Events Table	Microsoft Hyper-V Security Target
FCS: Cryptographic Support	FCS_HTTPS_EXT.1: HTTPS Protocol	Microsoft Hyper-V Security Target
	FCS_IPSEC_EXT.1: IPSec Protocol	Microsoft Hyper-V Security Target
	FCS_SSHC_EXT.1: SSH Client Protocol	PP Evaluation
	FCS_SSHS_EXT.1: SSH Server Protocol	PP Evaluation
	FCS_TLSC_EXT.1: TLS Client Protocol	Microsoft Hyper-V Security Target
	FCS_TLSS_EXT.1: TLS Server Protocol	Microsoft Hyper-V Security Target
FPT: Protection of the TSF	FPT_TUD_EXT.2: Trusted Update Based on Certificates	Microsoft Hyper-V Security Target

The following table contains the "**Objective**" requirements contained in Appendix D, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are not currently mandated by

the PP but specify security functionality that is desirable, and are expected to transition from objective requirements to baseline requirements in future versions of the PP.

Table 8: Objective Requirements

Requirement Class	Requirement Component	Verified By
FPT: Protection of the TSF	FPT_INT_EXT.1: Support for Introspection	PP Evaluation
	FPT_DDI_EXT.1: Device Driver Isolation	Microsoft Hyper-V Security Target
	FPT_CIM_EXT.1: Collection of Integrity Measurements	PP Evaluation
	FPT_IDV_EXT.1: Software Identification and Versions	PP Evaluation

6 Assurance Requirements

The following are the assurance requirements contained in the SVPP.

Table 9: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ADV: Development	ADV_FSP.1 Basic Functional Specification	Microsoft Hyper-V Security Target
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Microsoft Hyper-V Security Target
	AGD_PRE.1: Preparative Procedures	Microsoft Hyper-V Security Target
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	Microsoft Hyper-V Security Target
	ALC_CMS.1: TOE CM Coverage	Microsoft Hyper-V Security Target
	ALC_TSU_EXT.1: Timely Security Updates	Microsoft Hyper-V Security Target
ASE: Security Target	ASE_CCL.1: Conformance Claims	Microsoft Hyper-V Security Target
	ASE_ECD.1: Extended Components Definition	Microsoft Hyper-V Security Target
	ASE_INT.1: ST Introduction	Microsoft Hyper-V Security Target
	ASE_OBJ.1: Security Objectives for the Operational Environment	Microsoft Hyper-V Security Target
	ASE_REQ.1: Stated Security Requirements	Microsoft Hyper-V Security Target
	ASE_TSS.1: TOE Summary Specification	Microsoft Hyper-V Security Target
ATE: Tests	ATE_IND.1: Independent Testing - Sample	Microsoft Hyper-V Security Target
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Microsoft Hyper-V Security Target

7 Results of the evaluation

Note that for ASE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 10: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Microsoft Hyper-V Security Target
APE_ECD.1	Pass	Microsoft Hyper-V Security Target
APE_INT.1	Pass	Microsoft Hyper-V Security Target
APE_OBJ.1	Pass	Microsoft Hyper-V Security Target
APE_REQ.1	Pass	Microsoft Hyper-V Security Target

8 Glossary

The following definitions are used throughout this document:

- **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.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the SVPP Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **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.
- **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.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security Evaluation: Evaluation Methodology*, Version 3.1, Revision 4, dated: September 2012.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] Leidos Common Criteria Testing Laboratory, *Microsoft Windows Server 2016, Windows Server 2012 R2, and Windows 10 Hyper-V Assurance Activity Report*, Version 1.0, December 7, 2017.

[7] Leidos Common Criteria Testing Laboratory, *Microsoft Hyper-V Security Target,* Version 0.07, November 17, 2017.

[8] *Protection Profile for Server Virtualization*, Version 1.1, 14 September 2015.