National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report
for
Protection Profile for Virtualization, Version 1.0, 06 December 2019

Report Number:	**CCEVS-VR-PP-0065**
Dated:	**28 January 2021**
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 6982
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base and Additional Requirements

CGI IT Security Labs
Fairfax, Virginia

Table of Contents

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 Virtualization, Version 1.0 (PP_BASE_VIRTUALIZATION_V1.0). It presents a summary of the PP_BASE_VIRTUALIZATION_V1.0 and the evaluation results.

CGI IT Security Labs, located in Fairfax, Virginia, performed the evaluation of PP_BASE_VIRTUALIZATION_V1.0 concurrent with the first product evaluation against the PP's requirements. The evaluated product was VMware ESXi 6.7 Update 2.

This evaluation addressed the base requirements of PP_BASE_VIRTUALIZATION_V1.0 and several of the additional requirements contained in Appendices A, B, and C. The Validation Report (VR) author independently performed an additional review of the PP as part of the completion of this VR, to confirm it meets the claimed APE assurance requirements. During the evaluation, it was determined that some APE work units failed due to missing rationales and dependencies. NIAP issued a Technical Decision to update the Security Objective Rationale, add an SFR Rationale, and add an Implicitly Satisfied SFR Appendix. After further review, it was verified that these issues resolved all PP deficiencies and had no impact on the product evaluation.

The evaluation determined that PP_BASE_VIRTUALIZATION_V1.0 is both Common Criteria Part 2 Extended and Part 3 Extended. The PP identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the Common Methodology for IT Security Evaluation (Version 3.1, Release 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 4). The Security Target (ST) includes material from the PP_BASE_VIRTUALIZATION_V1.0 and completion of the ASE work units satisfied the APE work units for PP_BASE_VIRTUALIZATION_V1.0, but only for those parts of the Security Target that were relevant to this PP.

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

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 Evaluation Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of PP_BASE_VIRTUALIZATION_V1.0 was performed concurrent with the first product evaluation against the PP's requirements. In this case, the Target of Evaluation (TOE) was VMware ESXi 6.7 Update 2, evaluated by CGI IT Security Labs in Fairfax, Virginia, United States of America.

These evaluations addressed the base requirements of PP_BASE_VIRTUALIZATION_V1.0, and several of the additional requirements contained in Appendices A, B, and C.

PP_BASE_VIRTUALIZATION_V1.0 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 specify optional functionality that the PP authors consider candidates for becoming mandatory requirements in the future.

The initial use of the PP addresses (in terms of the PP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors have evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ work units performed against PP_BASE_VIRTUALIZATION_V1.0. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include references to this as additional evidence that the corresponding portions of PP_BASE_VIRTUALIZATION_V1.0 were evaluated.

The following identifies the PP subject of the evaluation or validation, as well as the supporting information from the evaluation performed against this PP and any subsequent evaluations that address additional optional or selection-based requirements in the PP_BASE_VIRTUALIZATION_V1.0.

Protection Profile	Protection Profile for Virtualization, Version 1.0, 17 November 2016.
ST (Base)	VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001 Security Target, Version 1.12, 05 November 2019
Assurance Activity Report (Base)	Assurance Activities Report VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001, Version 0.5, 05 November 2019
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	CGI IT Security Labs

12601 Fair Lakes Circle
Fairfax, VA 22033

3 PP_BASE_VIRTUALIZATION_V1.0 Description

The PP_BASE_VIRTUALIZATION_V1.0 specifies information security requirements for virtualization, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

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. A VS creates a virtualized hardware environment (virtual machines or VMs) for each instance of an operating system permitting these environments to execute concurrently while maintaining isolation and the appearance of exclusive control over assigned computing resources. For the purposes of this document, the VS consists of a Virtual Machine Manager (VMM), Virtual Machine (VM) abstractions, a management subsystem, and other components.

This Protection Profile (PP) describes security requirements for a VS, which is the Target of Evaluation (TOE). The VS is only one component of an enterprise deployment of virtualization devices which would additionally include Client or Server Virtualization capabilities as described separately in corresponding Extended Packages (EP).

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.
A.COVERT_CHANNELS	If the TOE has covert storage or timing channels, then for all VMs executing on that TOE, it is assumed that relative to the IT assets to which they have access, those VMs will have assurance sufficient to outweigh the risk that they will violate the security policy of the TOE by using those covert channels.
A.NON_MALICIOUS_USER	The user of the VS is not willfully negligent or hostile, and uses the VS in compliance with the applied enterprise security policy and guidance. At the same time, malicious applications could act as the user, so requirements which confine malicious applications are still in scope.

4.2 Threats

The following table contains applicable threats.

Table 2: Threats

Threat Name	**Threat Definition**
T.DATA_LEAKAGE	It is a fundamental property of VMs that the domains encapsulated by different VMs remain separate unless data sharing is permitted by policy. For this reason, all Virtualization Systems shall support a policy that prohibits information transfer between VMs. It shall be possible to configure VMs such that data cannot be moved between domains from VM to VM, or through virtual or physical network components under the control of the VS. When VMs are configured as such, it shall not be possible for data to leak between domains, neither by the express efforts of software or users of a VM, nor because of vulnerabilities or errors in the implementation of the VMM or other VS components. 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 personally identifiable information to be made accessible to unauthorized entities.
T.UNAUTHORIZED_UPDATE	It is common for attackers to target outdated versions of software containing known flaws. This means it is extremely important to update Virtualization System software as soon as possible when updates are available. But the source of the updates and the updates themselves must be trusted. If an attacker can write their own update containing malicious code they can take control of the VS.
T.UNAUTHORIZED_MODIFICATION	System integrity is a core security objective for Virtualization Systems. To achieve system integrity, the integrity of each VMM component must be established and maintained. Malware running on the platform must not be able to undetectably modify Virtualization System components while the system is running or at rest. Likewise, malicious code running within a virtual machine must not be able to modify Virtualization System components.
T.USER_ERROR	If a Virtualization System is capable of simultaneously displaying VMs of different domains to the same user at the same time, there is always the chance that the user will become confused and unintentionally leak information between domains. This is especially likely if VMs belonging to different domains are indistinguishable. Malicious code may also attempt to interfere with the user's ability to distinguish between domains. The VS must take measures to minimize the likelihood of such confusion.
T.3P_SOFTWARE	In some VS implementations, critical functions are by necessity performed by software not produced by the virtualization vendor. Such software may include Host Operating Systems and physical device drivers. Vulnerabilities in this software can be exploited by an adversary and result in VMM compromise. Where possible, the VS should mitigate the results of potential vulnerabilities or malicious content in third-party code.

Threat Name	Threat Definition
T.VMM_COMPROMISE	The Virtualization System is designed to provide the appearance of exclusivity to the VMs and is designed to separate or isolate their functions except where specifically shared. Failure of security mechanisms could lead to unauthorized intrusion into or modification of the VMM, or bypass of the VMM altogether. This must be prevented to avoid compromising the Virtualization System.
T.PLATFORM_COMPROMISE	The VS must be capable of protecting the platform from threats that originate within VMs and operational networks connected to the VS. The hosting of untrusted—even malicious—domains by the VS cannot be permitted to compromise the security and integrity of the platform on which the VS executes. If an attacker can access the underlying platform in a manner not controlled by the VMM, the attacker might be able to modify system firmware or software—compromising both the Virtualization System and the underlying platform.
T.UNAUTHORIZED_ACCESS	Functions performed by the management layer include VM configuration, virtualized network configuration, allocation of physical resources, and reporting. Only certain authorized system users (administrators) are allowed to exercise management functions. Virtualization Systems are often managed remotely over communication networks. Members of these networks can be both geographically and logically separated from each other, and pass through a variety of other systems which may be under the control of an adversary, and offer the opportunity for communications to be compromised. An adversary with access to an open management network could inject commands into the management infrastructure. This would provide an adversary with administrator privilege on the platform, and administrative control over the VMs and virtual network connections. The adversary could also gain access to the management network by hijacking the management network channel.
T.WEAK_CRYPTO	To the extent that VMs appear isolated within the Virtualization System, a threat of weak cryptography may arise if the VMM does not provide good entropy to support security-related features that depend on entropy to implement cryptographic algorithms. For example, a random number generator keeps an estimate of the number of bits of noise in the entropy pool. From this entropy pool random numbers are created. Good random numbers are essential to implementing strong cryptography. Cryptography implemented using poor random numbers can be defeated by a sophisticated adversary.
T.UNPATCHED_SOFTWARE	Vulnerabilities in outdated or unpatched software can be exploited by adversaries to compromise the Virtualization System or platform.
T.MISCONFIGURATION	The Virtualization System may be misconfigured, which could impact its functioning and security. This misconfiguration could be due to an administrative error or the use of faulty configuration data.
T.DENIAL_OF_SERVICE	A VM may block others from system resources (e.g., system memory, persistent storage, and processing time) via a resource exhaustion attack.

4.3 Organizational Security Policies

This protection profile contains no organizational security policies.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 3: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
O.VM_ISOLATION	VMs are the fundamental subject of the system. The VMM is responsible for applying the system security policy (SSP) to the VM and all resources. As basic functionality, the VMM must support a security policy that mandates no information transfer between VMs. The VMM must support the necessary mechanisms to isolate the resources of all VMs. The VMM partitions a platform's physical resources for use by the supported virtual environments. Depending on the use case, a VM may require a completely isolated environment with exclusive access to system resources, or share some of its resources with other VMs. It must be possible to enforce a security policy that prohibits the transfer of data between VMs through shared devices. When the platform security policy allows the sharing of resources across VM boundaries, the VMM must ensure that all access to those resources is consistent with the policy. The VMM may delegate the responsibility for the mediation of sharing of particular resources to select Service VMs; however in doing so, it remains responsible for mediating access to the Service VMs, and each Service VM must mediate all access to any shared resource that has been delegated to it in accordance with the SSP. Devices, whether virtual or physical, are resources requiring access control. The VMM must enforce access control in accordance to system security policy. Physical devices are platform devices with access mediated via the VMM per the O.VMM_Integrity objective. Virtual devices may include virtual storage devices and virtual network devices. Some of the access control restrictions must be enforced internal to Service VMs, as may be the case for isolating virtual networks. VMMs may also expose purely virtual interfaces. These are VMM specific, and while they are not analogous to a physical device, they are also subject to access control. The VMM must support the mechanisms to isolate all resources associated with virtual networks and to limit a VM's access to only those virtual networks for which it has been configured. The VMM must also support the mechanisms to control the configurations of virtual networks according to the SSP.
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 Guest VMs or of the physical platform. The overall objective is to ensure the integrity of critical components of a Virtualization System. Initial integrity of a VS can be established through mechanisms such as a digitally signed installation or update package, or through

TOE Security Objective	TOE Security Objective Definition
	integrity measurements made at launch. Integrity is maintained in a running system by careful protection of the VMM from untrusted users and software. For example, it must not be possible for software running within a Guest VM to exploit a vulnerability in a device or hypercall interface and gain control of the VMM. The vendor must release patches for vulnerabilities as soon as practicable after discovery. Only one VM has access to a physical USB device at a time.
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 hosted by the VS is capable of undermining the integrity of the platform.
O.DOMAIN_INTEGRITY	While the VS is not responsible for the contents or correct functioning of software that runs within Guest VMs, it is responsible for ensuring that the correct functioning of the software within a Guest VM is not interfered with by other VMs.
O.MANAGEMENT_ACCESS	VMM management functions include VM configuration, virtualized network configuration, allocation of physical resources, and reporting. Only certain authorized system users (administrators) are allowed to exercise management functions. Because of the privileges exercised by the VMM management functions, it must not be possible for the VMM's management components to be compromised without administrator notification. This means that unauthorized users cannot be permitted access to the management functions, and the management components must not be interfered with by Guest VMs or unprivileged users on other networks—including operational networks connected to the TOE. VMMs include a set of management functions that collectively allow administrators to configure and manage the VMM, as well as configure Guest VMs. These management functions are specific to the virtualization system, distinct from any other management functions that might exist for the internal management of any given Guest VM. These VMM management functions are privileged, with the security of the entire system relying on their proper use. The VMM management functions can be classified into different categories and the policy for their use and the impact to security may vary accordingly. The management functions might be distributed throughout the VMM (within the VMM and Service VMs). The VMM must support the necessary mechanisms to enable the control of all management functions according to the system security policy. When a management function is distributed among multiple Service VMs, the VMs must be protected using the security mechanisms of the Hypervisor and any Service VMs involved to ensure that the intent of the system security policy is not compromised. Additionally, since hypercalls permit Guest VMs to invoke the Hypervisor, and often allow the passing of data to the Hypervisor, it is important that the

TOE Security Objective	TOE Security Objective Definition
	hypercall interface is well-guarded and that all parameters be validated. The VMM maintains configuration data for every VM on the system. This configuration data, whether of Service or Guest VMs, must be protected. The mechanisms used to establish, modify and verify configuration data are part of the VS management functions and must be protected as such. The proper internal configuration of Service VMs that provide critical security functions can also greatly impact VS security. These configurations must also be protected. Internal configuration of Guest VMs should not impact overall VS security. The overall goal is to ensure that the VMM, including the environments internal to Service VMs, is properly configured and that all Guest VM configurations are maintained consistent with the system security policy throughout their lifecycle. Virtualization Systems are often managed remotely. For example, an administrator can remotely update virtualization software, start and shut down VMs, and manage virtualized network connections. If a console is required, it could be run on a separate machine or it could itself run in a VM. When performing remote management, an administrator must communicate with a privileged management agent over a network. Communications with the management infrastructure must be protected from Guest VMs and operational networks.
O.PATCHED_SOFTWARE	The Virtualization System must be updated and patched when needed in order to prevent the potential compromise of the VMM, as well as the networks and VMs that it hosts. Identifying and applying needed updates must be a normal part of the operating procedure to ensure that patches are applied in a timely and thorough manner. In order to facilitate this, the VS must support standards and protocols that help enhance the manageability of the VS as an IT product, enabling it to be integrated as part of a manageable network (e.g., reporting current patch level and patchability).
O.VM_ENTROPY	VMs must have access to good entropy sources to support security-related features that implement cryptographic algorithms. For example, in order to function as members of operational networks, VMs must be able to communicate securely with other network entities—whether virtual or physical. They must therefore have access to sources of good entropy to support that secure communication.
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.
O.CORRECTLY_APPLIED_CONFIGURATION	The TOE must not apply configurations that violate the current security policy. The TOE must correctly apply configurations and policies to newly created Guest VMs, as well as to existing Guest VMs when applicable configuration or policy changes are made. All changes to configuration and to policy must conform to the existing security policy. Similarly, changes made to the configuration of the TOE itself must not violate the existing security policy.

TOE Security Objective	TOE Security Objective Definition
O.RESOURCE_ALLOCATION	The TOE will provide mechanisms that enforce constraints on the allocation of system resources in accordance with existing security policy.

The following table contains security objectives for the Operational Environment.

Table 4: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental 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.
OE.COVERT_CHANNELS	If the TOE has covert storage or timing channels, then for all VMs executing on that TOE, it is assumed that those VMs will have sufficient assurance relative to the IT assets to which they have access, to outweigh the risk that they will violate the security policy of the TOE by using those covert channels.
OE.NON_MALICIOUS_USER	Users are trusted to be not willfully negligent or hostile and use the VS in compliance with the applied enterprise security policy and guidance.

5 Requirements

As indicated above, requirements in the PP_BASE_VIRTUALIZATION_V1.0 are comprised of the “base” requirements and additional requirements that are optional, selection-based, or objective. The following table contains the “base” requirements that were validated as part of the CGI IT Security Labs evaluation activities referenced above.

Table 5: Base Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	VMware ESXi 6.7 Update 2
	FAU_SAR.1: Audit Review	VMware ESXi 6.7 Update 2
	FAU_STG.1: Protected Audit Trail Storage	VMware ESXi 6.7 Update 2
	FAU_STG_EXT.1: Off-Loading of Audit Data	VMware ESXi 6.7 Update 2
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	VMware ESXi 6.7 Update 2
	FCS_CKM.2: Cryptographic Key Establishment	VMware ESXi 6.7 Update 2
	FCS_CKM_EXT.4: Cryptographic Key Destruction	VMware ESXi 6.7 Update 2
	FCS_COP.1(1): Cryptographic Operation (AES Data Encryption/Decryption)	VMware ESXi 6.7 Update 2
	FCS_COP.1(2): Cryptographic Operation (Hashing)	VMware ESXi 6.7 Update 2
	FCS_COP.1(3): Cryptographic Operation (Signature Algorithms)	VMware ESXi 6.7 Update 2

Requirement Class	Requirement Component	Verified By
	FCS_COP.1(4): Cryptographic Operation (Keyed Hash Algorithms)	VMware ESXi 6.7 Update 2
	FCS_ENT_EXT.1: Entropy for Virtual Machines	VMware ESXi 6.7 Update 2
	FCS_RBG_EXT.1: Cryptographic Operation (Random Bit Generation)	VMware ESXi 6.7 Update 2
FDP: User Data Protection	FDP_HBI_EXT.1: Hardware-Based Isolation Mechanisms	VMware ESXi 6.7 Update 2
	FDP_PPR_EXT.1: Physical Platform Resource Controls	VMware ESXi 6.7 Update 2
	FDP_RIP_EXT.1: Residual Information in Memory	VMware ESXi 6.7 Update 2
	FDP_RIP_EXT.2: Residual Information on Disk	VMware ESXi 6.7 Update 2
	FDP_VMS_EXT.1: VM Separation	VMware ESXi 6.7 Update 2
	FDP_VNC_EXT.1: Virtual Networking Components	VMware ESXi 6.7 Update 2
FIA: Identification and Authentication	FIA_AFL_EXT.1: Authentication Failure Heading	VMware ESXi 6.7 Update 2
	FIA_UAU.5: Multiple Authentication Mechanisms	VMware ESXi 6.7 Update 2
	FIA_UIA_EXT.1: Administrator Identification and Authentication	VMware ESXi 6.7 Update 2
FMT: Security Management	FMT_MSA_EXT.1: Default Data Sharing Configuration	VMware ESXi 6.7 Update 2
	FMT_SMO_EXT.1: Separation of Management and Operational Networks	VMware ESXi 6.7 Update 2
FPT: Protection of the TSF	FPT_DVD_EXT.1: Non-Existence of Disconnected Virtual Devices	VMware ESXi 6.7 Update 2
	FPT_EEM_EXT.1: Execution Environment Mitigations	VMware ESXi 6.7 Update 2
	FPT_HAS_EXT.1: Hardware Assists	VMware ESXi 6.7 Update 2
	FPT_HCL_EXT.1: Hypercall Controls	VMware ESXi 6.7 Update 2
	FPT_RDM_EXT.1: Removable Devices and Media	VMware ESXi 6.7 Update 2
	FPT_TUD_EXT.1: Trusted Updates to the Virtualization System	VMware ESXi 6.7 Update 2
	FPT_VDP_EXT.1: Virtual Device Parameters	VMware ESXi 6.7 Update 2
	FPT_VIV_EXT.1: VMM Isolation from VMs	VMware ESXi 6.7 Update 2
FTA: TOE Access	FTA_TAB.1: TOE Access Banner	VMware ESXi 6.7 Update 2
FTP: Trusted Path/Channel	FTP_ITC_EXT.1: Trusted Channel Communications	VMware ESXi 6.7 Update 2
	FTP_UIF_EXT.1: User Interface: I/O Focus	VMware ESXi 6.7 Update 2
	FTP_UIF_EXT.2 User Interface: Identification of VM	VMware ESXi 6.7 Update 2

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation."

Table 6: Optional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_ARP.1: Security Audit Automatic Response	PP Evaluation
	FAU_SAA.1: Security Audit Analysis	PP Evaluation
FPT: Protection of the TSF	FPT_GVI_EXT.1.1: Guest VM Integrity	PP Evaluation

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). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation."

Table 7: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_HTTPS_EXT.1: HTTPS Protocol	VMware ESXi 6.7 Update 2
	FCS_IPSEC_EXT.1 IPsec Protocol	PP Evaluation
	FCS_TLSC_EXT.1: TLS Client Protocol	VMware ESXi 6.7 Update 2
	FCS_TLSS_EXT.1: TLS Server Protocol	VMware ESXi 6.7 Update 2
	FCS_TLSS_EXT.2: TLS Server Protocol with Mutual Authentication	PP Evaluation
FIA: Identification and Authentication	FIA_PMG_EXT.1: Password Management	VMware ESXi 6.7 Update 2
	FIA_X509_EXT.1: X.509 Certificate Validation	VMware ESXi 6.7 Update 2
	FIA_X509_EXT.2: X.509 Certificate Authentication	VMware ESXi 6.7 Update 2
FPT: Protection of the TSF	FPT_TUD_EXT.2: Trusted Update Based on Certificates	VMware ESXi 6.7 Update 2
FTP: Trusted Path/Channel	FTP_TRP.1: Trusted Path	VMware ESXi 6.7 Update 2

The following table contains the "**Objective**" requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation."

Table 8: Objective Requirements

Requirement Class	Requirement Component	Verified By
FPT: Protection of the TSF	FPT_DDI_EXT.1: Device Driver Isolation	PP Evaluation
	FPT_IDV_EXT.1: Software Identification and Versions	PP Evaluation
	FPT_INT_EXT.1 Support for Introspection	PP Evaluation
	FPT_ML_EXT.1: Measured Launch of Platform and VMM	PP Evaluation

6 Assurance Requirements

The following are the assurance requirements contained in the PP_BASE_VIRTUALIZATION_V1.0.

Table 9: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target Evaluation	ASE_CCL.1: Conformance Claims ASE_ECD.1: Extended Components Definition ASE_INT.1: ST Introduction ASE_OBJ.2: Security Objectives for the Operational Environment ASE_REQ.1: Stated Security Requirements ASE_SPD.1: Security Problem Definition ASE_TSS.1: TOE Summary Specification	VMware ESXi 6.7 Update 2
ADV: Development	ADV_FSP.1 Basic Functional Specification	VMware ESXi 6.7 Update 2
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance AGD_PRE.1: Preparative Procedures	VMware ESXi 6.7 Update 2 VMware ESXi 6.7 Update 2
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE ALC_CMS.1: TOE CM Coverage ALC_TSU_EXT.1: Timely Security Updates	VMware ESXi 6.7 Update 2 VMware ESXi 6.7 Update 2
ATE: Tests	ATE_IND.1: Independent Testing – Conformance	VMware ESXi 6.7 Update 2
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	VMware ESXi 6.7 Update 2

7 Results of the Evaluation

Note that for APE elements and work units that are identical to ASE 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	VMware ESXi 6.7 Update 2
APE_ECD.1	Pass	VMware ESXi 6.7 Update 2
APE_INT.1	Pass	VMware ESXi 6.7 Update 2
APE_OBJ.2	Pass	VMware ESXi 6.7 Update 2
APE_REQ.2	Pass	VMware ESXi 6.7 Update 2
APE_SPD.1	Pass	VMware ESXi 6.7 Update 2

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 PP_BASE_VIRTUALIZATION_V1.0 Evaluation 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.
- **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 Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[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] Protection Profile for Virtualization, Version 1.0, 17 November 2016.

[7] VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001 Security Target, Version 1.12, 05 November 2019

[8] Assurance Activities Report VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001, Version 0.5, 05 November 2019