National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

PP-Configuration for Virtualization and Server Virtualization Systems

Version 1.0

04 June 2021

Report Number: CCEVS-VR-PP-0084
Dated: 03 February 2023
Version: 1.1

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGMENTS

Common Criteria Testing Laboratory
Base and Additional Requirements
Leidos Common Criteria Testing Laboratory
Columbia, MD

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 PP-Configuration for Virtualization and Server Virtualization Systems, Version 1.0 (CFG_Virtualization-SV_V1.0). This PP-Configuration defines how to evaluate a TOE that claims conformance to the Protection Profile for Virtualization, Version 1.1 (PP_Virtualization_V1.1) Base-PP, and the PP-Module for Server Virtualization Systems, Version 1.1 (MOD_SV_V1.1). It presents a summary of the CFG_Virtualization-SV_V1.0 and the evaluation results.

The Leidos Common Criteria Testing Laboratory, located in Columbia, Maryland, performed the evaluation of the PP_Virtualization_V1.1 and MOD_SV_V1.1, contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was VMware ESXi 7.0 Update 3d.

This evaluation addressed the base security functional requirements of PP_Virtualization_V1.1 and MOD_SV_V1.1 as part of CFG_Virtualization-SV_V1.0. This evaluation also addressed several of the additional requirements contained in the appendices of PP_Virtualization_V1.1.

The Validation Report (VR) author independently performed an additional review of the PP-Configuration, Base-PP, and PP-Module as part of the completion of this VR, to confirm they meet the claimed APE and ACE requirements.

The evaluation determined the CFG_Virtualization-SV_V1.0 is both Common Criteria Part 2 extended and Part 3 extended. An accredited Information Technology Security Evaluation Facility (ITSEF) evaluated the PP-Configuration and PP-Module identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 5). The Security Target (ST) includes material from the PP_Virtualization_V1.1 and MOD_SV_V1.1; completion of the ASE workunits satisfied the APE workunits for this PP and ACE workunits for this PP-Module, but only for the materials defined in this PP-Module, and only when the PP-Module is in the defined PP-Configuration.

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 Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles (PPs) and PP-Modules that have Evaluation Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 workunits specific to the technology described by the PP or PP-Modules. Products may only be evaluated against PP-Modules when a PP-Configuration is defined to include the PP-Modules with at least one corresponding Base-PP.

To promote thoroughness and efficiency, the evaluation of the CFG_Virtualization-SV_V1.0, PP_Virtualization_V1.1, and MOD_SV_V1.1, was performed concurrent with the first product evaluation to claim conformance to the PP-Configuration. In this case, the Target of Evaluation (TOE) was VMware, performed by the Leidos Common Criteria Testing Laboratory in Columbia, MD.

This evaluation addressed the base security functional requirements of PP_Virtualization_V1.1, and MOD_SV_V1.1 as part of CFG_Virtualization-SV_V1.0. PP_Virtualization_V1.1 also defines additional requirements, some of which the VMware product evaluation claimed.

PP_Virtualization_V1.1 and MOD_SV_V1.1 contain a set of base requirements that all conformant STs must include. PP_Virtualization_V1.1 additionally contains strictly optional, objective, and selection-based requirements. Strictly 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. Objective requirements are optional in the present version of the PP but are being considered for inclusion as base requirements in future revisions. Vendors planning to have evaluations performed against future products are encouraged to plan for these objective requirements to be met. Selection-based requirements are those that must be included based on the selections made in other requirements and the abilities of the TOE.

The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ workunits performed against the Base-PP and the ACE_REQ workunits performed against the PP-Module. 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 reference to this as additional evidence that the corresponding portions of the CFG_Virtualization-SV_V1.0 were evaluated.

The following identifies the Base-PP and the PP-Module in the PP-Configuration evaluated by this VR. It also includes supporting information from the initial product evaluation performed against these PP-Modules.

PP-Configuration	PP-Configuration for Virtualization and Server Virtualization Systems, Version 1.0, 04 June 2021 (CFG_Virtualization-SV_V1.0)
Base-PP	Protection Profile for Virtualization, Version 1.1, 14 June 2021 (PP_Virtualization_V1.1)
Modules in PP-Configuration	PP-Module for Server Virtualization Systems, Version 1.1, 14 June 2021 (MOD_SV_V1.1)

ST (Base)	VMware ESXi 7.0 Update 3d Security Target, Version 1.0, 22 July 2022
Assurance Activity Report (Base)	Assurance Activities Report for VMware ESXi 7.0 Update 3d, Version 1.0, 28 July 2022
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	Leidos Common Criteria Testing Laboratory Columbia, MD

3 CFG_Virtualization-SV_V1.0 Description

CFG_Virtualization-SV_V1.0 is a PP-Configuration that combines the following.

- Protection Profile for Virtualization, Version 1.1 (PP_Virtualization_V1.1)
- PP-Module for Server Virtualization Systems, Version 1.1 (MOD_SV_V1.1)

This PP-Configuration is for a virtualization system that includes server virtualization capabilities according to the requirements of the PP-Configuration.

Server Virtualization refers 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 isolation and the appearance of 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. Typically, virtualized servers provide services to remote clients from a data center, and are generally not directly accessible by non-administrative users.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_Virtualization-SV_V1.0.

Table 1: Assumptions

Assumption Name	Assumption Definition
From PP_Virtualization_V1.1	
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.
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.PLATFORM_INTEGRITY	The platform has not been compromised prior to installation of the VS.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance.
From MOD_SV_V1.1	
No additional assumptions defined in MOD_SV_V1.1.	

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_Virtualization-SV_V1.0.

Table 2: Threats

Threat Name	Threat Definition
From PP_Virtualization_V1.1	
T.3P_SOFTWARE	In some VS implementations, functions critical to the security of the TOE are by necessity performed by software not produced by the virtualization vendor. Such software may include physical device drivers, and even non-TOE entities such as Host Operating Systems. Since this software has the same or similar privilege level as the VS, vulnerabilities can be exploited by an adversary to compromise the VS and VMs. Where possible, the VS should mitigate the results of potential vulnerabilities or malicious content in third-party code on which it relies. For example, physical device drivers (potentially the Host OS) could be encapsulated within VMs in order to limit the effects of compromise.
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

Threat Name	Threat Definition
	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.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.
T.MISCONFIGURATION	The VS 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.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 VS 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 or obtain sensitive information from the TOE. 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 or extract sensitive information. 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.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 VS 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.UNAUTHORIZED_UPDATE	It is common for attackers to target outdated versions of software containing known flaws. This means it is extremely important to

Threat Name	Threat Definition
	update VS 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.UNPATCHED_SOFTWARE	Vulnerabilities in outdated or unpatched software can be exploited by adversaries to compromise the VS or platform.
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.VMM_COMPROMISE	The VS 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, by non-TOE software, such as that running in Guest or Helper VMs or on the host platform. This must be prevented to avoid compromising the VS.
T.WEAK_CRYPTO	To the extent that VMs appear isolated within the VS, 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. Such defeat can result in the compromise of Guest VM data and credentials, and of VS data and credentials, and can enable unauthorized access to the VS or VMs.
From MOD_SV_V1.1	
This PP defines no additional threats beyond those defined in the Base-PP. Note however that the SFRs defined in this PP-Module will assist in the mitigation of the following threats defined in the Base-PP: T.UNAUTHORIZED_ACCESS and T.UNAUTHORIZED_UPDATE	

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_Virtualization-SV_V1.0.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
From PP_Virtualization_V1.1	
No OSPs defined in PP_Virtualization_V1.1.	
From MOD_SV_V1.1	
No OSPs defined in MOD_SV_V1.1.	

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_Virtualization-SV_V1.0.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From PP_Virtualization_V1.1	
O.AUDIT	An audit log must be created that captures accesses to the objects the TOE protects. The log of these accesses, or audit events, must be protected from modification, unauthorized access, and destruction. The audit log must be sufficiently detailed to indicate the date and time of the event, the identify of the user, the type of event, and the success or failure of the event.
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 a newly created Guest VM, 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.
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 authorized users (administrators) may 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 VS and are 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 are 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

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

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 customer requirements, a VM may need 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 resource sharing 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. Both virtual and physical devices are resources requiring access control. The VMM must enforce access control in accordance with 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 VS—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 VS. Initial integrity of a VS can be established through mechanisms such as a digitally signed installation or update package, or through 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.
From MOD_SV_V1.1	

TOE Security Objective	TOE Security Objective Definition
This Module defines no additional TOE security objectives beyond those defined in the Base-PP. Note however that the SFRs defined in this Module will assist in the achievement of the following objectives defined in the Base-PP: O.MANAGEMENT_ACCESS and O.VMM_INTEGRITY	

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_Virtualization-SV_V1.0.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From PP_Virtualization_V1.1	
OE.CONFIG	TOE administrators will configure the VS correctly to create the intended security policy.
OE.NON_MALICIOUS_USER	Users are trusted to not be willfully negligent or hostile and use the VS in compliance with the applied enterprise security policy and guidance.
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.
From MOD_SV_V1.1	
This PP-Module does not define any objectives for the Operational Environment. Because this Module does not define any additional assumptions or organizational security policies, there are no additional security objectives for the Operational Environment to satisfy.	

5 Functional Requirements

As indicated above, CFG_Virtualization-SV_V1.0 includes the PP_Virtualization_V1.1 and MOD_SV_V1.1.

Requirements in the PP_Virtualization_V1.1 and MOD_SV_V1.1 are comprised of the "base" requirements, additional requirements that are optional, selection-based, or objective, and in the case of the PP-Modules, additional requirements that are dependent on the Base-PP that the PP-Module is used with. The following table contains the "base" requirements that were validated as part of the VMware device evaluation activities referenced above as well as any additional requirements that depend on the Base-PP that is claimed.

Table 6: Bae-PP Security Function Requirements

Requirement Class	Requirement Component	Verified By
Modified when the Protection Profile for Protection Profile for Virtualization is the Base-PP		
There are no Modified SFRs in the MOD_SV_V1.1		
Additional when the Protection Profile for Protection Profile for Virtualization is the Base-PP		
There are no Additional SFRs in the MOD_SV_V1.1		

The following table contains the "base" requirements specific to the TOE.

Table 7: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
From PP_Virtualization_V1.1		
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	VMware ESXi 7.0 Update 3d
	FAU_SAR.1: Audit Review	VMware ESXi 7.0 Update 3d
	FAU_STG.1: Protected Audit Trail Storage	VMware ESXi 7.0 Update 3d
	FAU_STG_EXT.1: Off-Loading of Audit Data	VMware ESXi 7.0 Update 3d
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	VMware ESXi 7.0 Update 3d
	FCS_CKM.2: Cryptographic Key Distribution	VMware ESXi 7.0 Update 3d
	FCS_CKM_EXT.4: Cryptographic Key Destruction	VMware ESXi 7.0 Update 3d
	FCS_COP.1/Hash: Cryptographic Operation (Hashing)	VMware ESXi 7.0 Update 3d
	FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithms)	VMware ESXi 7.0 Update 3d
	FCS_COP.1/Sig: Cryptographic Operation (Signature Algorithms)	VMware ESXi 7.0 Update 3d
	FCS_COP.1/UDE: Cryptographic Operation (AES Data Encryption/Decryption)	VMware ESXi 7.0 Update 3d
	FCS_ENT_EXT.1: Entropy for Virtual Machines	VMware ESXi 7.0 Update 3d

Requirement Class	Requirement Component	Verified By
	FCS_RBG_EXT.1: Cryptographic Operation (Random Bit Generation)	VMware ESXi 7.0 Update 3d
FDP: User Data Protection	FDP_HBI_EXT.1: Hardware-Based Isolation Mechanisms	VMware ESXi 7.0 Update 3d
	FDP_PPR_EXT.1: Physical Platform Resource Controls	VMware ESXi 7.0 Update 3d
	FDP_RIP_EXT.1: Residual Information in Memory	VMware ESXi 7.0 Update 3d
	FDP_RIP_EXT.2: Residual Information on Disk	VMware ESXi 7.0 Update 3d
	FDP_VMS_EXT.1: VM Separation	VMware ESXi 7.0 Update 3d
	FDP_VNC_EXT.1: Virtual Networking Components	VMware ESXi 7.0 Update 3d
FIA: Identification and Authentication	FIA_AFL_EXT.1: Authentication Failure Handling	VMware ESXi 7.0 Update 3d
	FIA_UAU.5: Multiple Authentication Mechanisms	VMware ESXi 7.0 Update 3d
	FIA_UIA_EXT.1: Administrator Identification and Authentication	VMware ESXi 7.0 Update 3d
FMT: Security Management	FMT_SMO_EXT.1: Separation of Management and Operational Networks	VMware ESXi 7.0 Update 3d
FPT: Protection of the TSF	FPT_DVD_EXT.1: Non-Existence of Disconnected Virtual Devices	VMware ESXi 7.0 Update 3d
	FPT_EEM_EXT.1: Execution Environment Mitigations	VMware ESXi 7.0 Update 3d
	FPT_HAS_EXT.1: Hardware Assists	VMware ESXi 7.0 Update 3d
	FPT_HCL_EXT.1: Hypercall Controls	VMware ESXi 7.0 Update 3d
	FPT_RDM_EXT.1: Removable Devices and Media	VMware ESXi 7.0 Update 3d
	FPT_TUD_EXT.1: Trusted Updates to the Virtualization System	VMware ESXi 7.0 Update 3d
	FPT_VDP_EXT.1: Virtual Device Parameters	VMware ESXi 7.0 Update 3d
	FPT_VIV_EXT.1: VMM Isolation from VMs	VMware ESXi 7.0 Update 3d
FTA: TOE Access	FTA_TAB.1: TOE Access Banner	VMware ESXi 7.0 Update 3d
FTP: Trusted Path/Channels	FTP_ITC_EXT.1: Trusted Channel Communications	VMware ESXi 7.0 Update 3d
	FTP_UIF_EXT.1: User Interface: I/O Focus	VMware ESXi 7.0 Update 3d
	FTP_UIF_EXT.2: User Interface: Identification of VM	VMware ESXi 7.0 Update 3d

Requirement Class	Requirement Component	Verified By
From MOD_SV_V1.1		
FMT: Security Management	FMT_MOF_EXT.1: Management of Security Functions Behavior	VMware ESXi 7.0 Update 3d

The following table contains the "**Optional**" requirements contained in Appendix A.1 of the Base-PP and PP-Module, 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 and ACE workunits and has indicated its verification through "PP Evaluation" or "Module Evaluation."

Table 8: Optional Requirements

Requirement Class	Requirement Component	Verified By
From PP_Virtualization_V1.1		
FAU: Security Audit	FAU_ARP.1: Security Audit Automatic Response	PP Evaluation
	FAU_SAA.1: Potential Violation Analysis	PP Evaluation
FPT: Protection of the TSF	FPT_GVI_EXT.1: Guest VM Integrity	PP Evaluation
From MOD_SV_V1.1		
The MOD_SV_V1.1 does not define any additional optional requirements.		

The following table contains the "**Objective**" requirements contained in Appendix A.2 of the Base-PP and PP-Module, 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 objective requirement, the VR author has evaluated it through the completion of the relevant APE and ACE workunits and has indicated its verification through "PP Evaluation" or "Module Evaluation."

Table 9: Objective Requirements

Requirement Class	Requirement Component	Verified By
From PP_Virtualization_V1.1		
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
From MOD_SV_V1.1		
The MOD_SV_V1.1 does not define any additional objective requirements.		

The following table contains the "**Selection-Based**" requirements contained in Appendix B of the Base-PP and PP-Module, 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

selection-based requirement, the VR author has evaluated it through the completion of the relevant APE and ACE workunits and has indicated its verification through "PP Evaluation" or "Module Evaluation."

Table 10: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
From PP_Virtualization_V1.1		
FCS: Cryptographic Support	FCS_HTTPS_EXT.1: HTTPS Protocol	VMware ESXi 7.0 Update 3d
	FCS_IPSEC_EXT.1: IPsec Protocol	PP Evaluation
FIA: Identification and Authentication	FIA_PMG_EXT.1: Password Management	VMware ESXi 7.0 Update 3d
	FIA_X509_EXT.1: X.509 Certificate Validation	VMware ESXi 7.0 Update 3d
	FIA_X509_EXT.2: X.509 Certificate Authentication	VMware ESXi 7.0 Update 3d
FPT: Protection of the TSF	FPT_TUD_EXT.2: Trusted Update Based on Certificates	VMware ESXi 7.0 Update 3d
FTP: Trusted Path/Channels	FTP_TRP.1: Trusted Path	VMware ESXi 7.0 Update 3d
From MOD_SV_V1.1		
The MOD_SV_V1.1 does not define any additional selection-based requirements.		

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by PP_Virtualization_V1.1. The SARs defined in that PP are applicable to MOD_SV_V1.1, as well as CFG_Virtualization-SV_V1.0 as a whole.

7 Results of the Evaluation

Note that for APE and ACE elements and workunits identical to ASE elements and workunits, the lab performed the ACE workunits concurrent to the ASE workunits.

Table 11: Evaluation Results: PP_Virtualization_V1.1

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	PP Evaluation
ACE_CCL.1	Pass	PP Evaluation
ACE_SPD.1	Pass	PP Evaluation
ACE_OBJ.1	Pass	PP Evaluation
ACE_ECD.1	Pass	PP Evaluation
ACE_REQ.1	Pass	PP Evaluation

Table 12: Evaluation Results: MOD_SV_V1.1

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module Evaluation
ACE_CCL.1	Pass	Module Evaluation
ACE_SPD.1	Pass	Module Evaluation
ACE_OBJ.1	Pass	Module Evaluation
ACE_ECD.1	Pass	Module Evaluation
ACE_REQ.1	Pass	Module Evaluation

Table 13: Evaluation Results: CFG_Virtualization-SV_V1.0

ACE Requirement	Evaluation Verdict	Verified By
ACE_MCO.1	Pass	PP-Config Evaluation
ACE_CCO.1	Pass	PP-Config Evaluation

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 unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the PP_Virtualization_V1.1 and MOD_SV_V1.1 Evaluation Activities to determine whether 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 the CCEVS Validation Body uses that leads to the issuance 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] CC and CEM addenda – Exact Conformance, Selection-Based SFRs, Optional SFRs, Version 0.5, dated: May 2017.

[6] Protection Profile for Virtualization, Version 1.1, 14 June 2021.

[7] PP-Module for Server Virtualization Systems, Version 1.1, 14 June 2021.

[8] PP-Configuration for Virtualization and Server Virtualization Systems, Version 1.0, 04 June 2021.

[9] VMware ESXi 7.0 Update 3d Security Target, Version 1.0, 22 July 2022.

[10] Assurance Activities Report for VMware ESXi 7.0 Update 3d, Version 1.0, 28 July 2022