PP-Module for Server Virtualization Systems

Version: 1.1 Draft
2021-03-09
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2016-11-17	Initial Publication as an Extended Package
1.1	2020-11-17	Converted to Module

Contents

1.1 Draft National Information Assurance Partnership 2021-03-09 Server Virtualization 1.0 2016-11-17 Initial Publication as an Extended Package 1.1 2020-11-17 Converted to Module

1 Introduction

1.1 Overview

The scope of this PP-Module is to define the security functionality of a Server Virtualization product in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is not complete in itself, but rather is intended for use with the following base PP:

- Protection Profile for Virtualization, Version 1.1.

This base PP is valid because Server Virtualization is a specific type of Virtualization System and is expected to implement security functionality that is not common to all Virtualization Systems. One additional SFR has been defined in this PP-Module to define security functionality that is unique to this particular type of Virtualization System.

1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory

Testing Laboratory	Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.
Target of Evaluation (TOE)	The product under evaluation.

1.2.2 Technical Terms

Administrator	Administrators perform management activities on the VS. These management functions do not include administration of software running within Guest VMs, such as the Guest OS. Administrators need not be human as in the case of embedded or headless VMs. Administrators are often nothing more than software entities that operate within the VM.
Domain	A Domain or Information Domain is a policy construct that groups together execution environments and networks by sensitivity of information and access control policy. For example, classification levels represent information domains. Within classification levels, there might be other domains representing communities of interest or coalitions. In the context of a VS, information domains are generally implemented as collections of VMs connected by virtual networks. The VS itself can be considered an Information Domain, as can its Management Subsystem.
Guest Operating System (OS)	An operating system that runs within a Guest VM.
Guest VM	A Guest VM is a VM that contains a virtual environment for the execution of an independent computing system. Virtual environments execute mission workloads and implement customer-specific client or server functionality in Guest VMs, such as a web server or desktop productivity applications.

Host Operating System (OS)	An operating system onto which a VS is installed. Relative to the VS, the Host OS is part of the Platform.
Hypercall	An API function that allows VM-aware software running within a VM to invoke VMM functionality.
Hypervisor	The Hypervisor is part of the VMM. It is the software executive of the physical platform of a VS. A Hypervisor's primary function is to mediate access to all CPU and memory resources, but it is also responsible for either the direct management or the delegation of the management of all other hardware devices on the hardware platform.
Management Subsystem	Components of the VS that allow VS Administrators to configure and manage the VMM, as well as configure Guest VMs. VMM management functions include VM configuration, virtualized network configuration, and allocation of physical resources.
Platform	The hardware, firmware, and software environment into which a VS is installed and executes.
User	Users operate Guest VMs and are subject to configuration policies applied to the VS by Administrators. Users need not be human as in the case of embedded or headless VMs, users are often nothing more than software entities that operate within the VM.
Virtual Machine (VM)	A Virtual Machine is a virtualized hardware environment in which an operating system may execute.
Virtual Machine Manager (VMM)	A VMM is a collection of software components responsible for enabling VMs to function as expected by the software executing within them. Generally, the VMM consists of a Hypervisor, Service VMs, and other components of the VS, such as virtual devices, binary translation systems, and physical device drivers. It manages concurrent execution of all VMs and virtualizes platform resources as needed.
Virtualization System (VS)	A software product that enables multiple independent computing systems to execute on the same physical hardware platform without interference from one other. For the purposes of this document, the VS consists of a Virtual Machine Manager (VMM), Virtual Machine abstractions, a management subsystem, and other components.

1.3 Compliant Targets of Evaluation

Server Virtualization, for the purposes of this Module, 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.

A TOE that claims conformance with this PP Module must also claim conformance to the Protection Profile for Virtualization. And a TOE that claims comformance with the Protection Profile for Virtualization must also claim conformance either to this Module or to the PP Module for Client Virtualization.

1.3.1 TOE Boundary

The TOE boundary is the same as that which is defined for a Virtualization System in the base Virtualization PP.

1.4 Use Cases

Requirements in this PP Module are designed to address the security problem in the following use cases. The description of these use cases provides examples for how the TOE and its Operational Environment could support the functionality required by this PP-Module.

[USE CASE 1] Virtualized Servers
A platform for virtualized instances of network-based services traditionally executed on separate hardware platforms, such as web servers, file servers, and mail servers.

[USE CASE 2] Virtualized Network Infrastructure
A platform for virtualized instances of routers, switches, and other network infrastructure.

[USE CASE 3] Virtualized Enterprise User Environments
A platform for the server back-end of virtual desktop or thin-client implementations where actual computation occurs in server-based VMs and users interact through a client. The client application is not covered by this PP Module.

2 Conformance Claims

Conformance Statement

This PP-Module inherits exact conformance as required from the Virtualization PP and as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

There are no other PP-Modules that are allowed to be specified in a PP-Configuration with this PP-Module.

CC Conformance Claims

This PP Module is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Release 5 [CC].

3 Security Problem Description

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment, and any organizational security policies that the TOE is expected to enforce.

3.1 Threats

This PP defines no additional threats beyond those defined in the base Virtualization 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_UPDATE

See Virtualization PP, Section 3.1.

T.UNAUTHORIZED_ACCESS

See Virtualization PP, Section 3.1.

3.2 Assumptions

This document does not define any additional assumptions.

3.3 Organizational Security Policies

This PP-Module defines no additional Organizational Security Policies.

4 Security Objectives

4.1 Security Objectives for the TOE

This Module defines no additional TOE security objectives beyond those defined in the base Virtualization PP. Note however that the SFR defined in this Module will assist in the achievement of the following objectives defined in the base PP:

O.VMM_INTEGRITY

See Virtualization PP, Section 4.1.

O.MANAGEMENT_ACCESS

See Virtualization PP, Section 4.1.

4.2 Security Objectives for the Operational Environment

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.

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organization security policies map to the security objectives.

Table 1: Security Objectives Rationale

Threat, Assumption, or OSP	Security Objectives	Rationale
T.UNAUTHORIZED_UPDATE	O.VMM_INTEGRITY	Integrity of a Virtualization System can be maintained by ensuring that the only way to modify the VS is through a trusted update process initiated by an authorized Administrator as required by FMT_MOF_EXT.
T.UNAUTHORIZED_ACCESS	O.MANAGEMENT_ACCESS	Access to management functions must be limited to authorized Administrators as managed through controls required by FMT_MOF_EXT.1.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): is used to add details to a requirement (including replacing an assignment with a more restrictive selection) or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

In a PP-Configuration that includes the Virtualization PP, the TOE is expected to rely on some of the security functions implemented by the Virtualization System as a whole and evaluated against the base PP. This section describes any modifications that the ST author must make to base PP SFRs to satisfy the required VS functionality. When this PP-Module is used to extend the Virtualization PP, the TOE type for the overall TOE is still a Virtualization System. The TOE boundary does not change. This threat applies to functionality that is described in the base PP, but is managed through functionality described in this PP-module. This threat applies to functionality that is described in the base PP, but is managed through functionality described in this PP-module.

5.1 Auditable Events for Mandatory SFRs

Table 2: Auditable Events for Mandatory Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MOF_EXT.1	Attempts to invoke any of the management functions listed in Table 3	Success or failure of attempt Identity of actor

5.1.1 Security Management (FMT)

FMT_MOF_EXT.1 Management of Security Functions Behavior

FMT_MOF_EXT.1.1

The TSF shall be capable of supporting [**selection**: *local*, *remote*] administration.

Application Note: Selection of “remote” requires the selection-based requirement FTP_TRP.1 defined in the base PP to be included in the ST.

FMT_MOF_EXT.1.2

The TSF shall be capable of performing the following management functions, controlled by an Administrator or User as shown in Table 3, based on the following key:

X = Mandatory (TOE must provide that function to that role)

O = Optional (TOE may or may not provide that function to that role)

N = Not Permitted (TOE must not provide that function to that role)

S = Selection-Based (TOE must provide that function to that role if the TOE claims a particular selection-based SFR)

Table 3: Server Virtualization Management Functions

Number	Function	Administrator	User	Notes (all SFR references are from the base Virtualization PP
1	Ability to update the Virtualization System	X	N	See FPT_TUD_EXT.1
2	[**selection**: *Ability to*	S	N	Must be selected if ST includes

	configure Administrator password policy as defined in FIA_PMG_EXT.1, Not applicable.]			FIA_PMG_EXT.1.
3	Ability to create, configure and delete VMs	X	O	
4	Ability to set default initial VM configurations	X	N	
5	Ability to configure virtual networks including VM	X	O	See FDP_VNC_EXT.1
6	Ability to configure and manage the audit system and audit data	X	N	
7	Ability to configure VM access to physical devices	X	O	See FDP_PPR_EXT.1
8	Ability to configure inter-VM data sharing	X	O	See FDP_VMS_EXT.1 and FMT_MSA_EXT.1
9	~~Ability to enable/disable VM access to Hypercall functions~~	O	O	Management function 9 is no longer required
10	Ability to configure removable media policy	X	N	See FPT_RDM_EXT.1
11	Ability to configure the cryptographic functionality	X	N	See FCS_CKM.1, FCS_CKM.2, and FCS_COP.1/HASH. See also, the Functional Packages for Transport Layer Security (TLS) and for Secure Shell (SSH) if claimed for methods to configure their respective cryptographic functionality.
12	Ability to change default authorization factors	X	N	See FIA_PMG_EXT.1
13	Ability to enable/disable screen lock	O	O	
14	Ability to configure screen lock inactivity timeout	O	O	
15	Ability to configure remote connection inactivity timeout	X	N	
16	Ability to configure lockout policy for unsuccessful authentication	X	N	See FIA_AFL_EXT.1

	attempts through [**selection**: *timeouts between attempts, limiting number of attempts during a time period*]			
17	[**selection**: *Ability to configure name/address of directory server to bind with, Not applicable*]	S	O	Must be selected if "directory-based" is selected anywhere in FIA_UAU.5.1 in the base Virtualization PP.
18	Ability to configure name/address of audit/logging server to which to send audit/logging records	X	N	See FAU_STG_EXT.1
19	Ability to configure name/address of network time server	X	O	
20	Ability to configure banner	X	N	See FTA_TAB.1
21	Ability to connect/disconnect removable devices to/from a VM	O	O	See FPT_RDM_EXT.1
22	Ability to start a VM	O	O	
23	Ability to stop/halt a VM	O	O	
24	Ability to checkpoint a VM	O	O	
25	Ability to suspend a VM	O	O	
26	Ability to resume a VM	O	O	
27	[**selection**: *Ability to configure action taken if unable to determine the validity of a certificate, Not applicable*]	S	N	This function must be selected if "allow the administrator to choose whether to accept the certificate in these cases" in FIA_X509_EXT.2.2 in the base PP.

Application Note: The ST author is expected to update Table 3 with an indication as to whether any of the ‘optional’ or ‘selection-based’ functions are included as part of the TOE. The ST author may also omit the ‘Notes’ column as it is provided in this PP-Module as an aid to the ST author in constructing the table.

This SFR addresses the roles of the CC Part 2 SFRs FMT_MOF.1, FMT_SMF.1, and FMT_SMR.2.

Administration is considered “local” if the Administrator is physically present at the machine on which the VS is installed.

Administration is considered “remote” if communications between the Administrator and the Management Subsystem travel on a network.

There is no requirement to authenticate Users of the Virtualization System. Users that have access to VMs but not to the Management Subsystem need not authenticate to the Virtualization System in order to use Guest VMs. Requirements for authentication of VM users is determined by the policies of the

domains running within the Guest VMs.

Appendix A - Entropy

The TOE does not require any additional supplementary information to describe its entropy source(s) beyond the requirements outlined in the ‘Entropy Documentation and Assessment’ section of the Base Virtualization PP. As with other base PP requirements, the only additional requirement is that the entropy documentation also applies to the specific Server Virtualization capabilities of the TOE in addition to the functionality required by the base PP. [VirtPP]Protection Profile for Virtualization, Version: 1.1, 2020-11-17