Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership (NIAP)

Title: Server Virtualization Essential Security Requirements

Maintained by: National Information Assurance Partnership

Unique Identifier: 42

Version: 1.0

Status: final

Date of issue: 19 October 2016

Approved by:

Supersedes:

Status

This Essential Security Requirements (ESR) document specifies the essential requirements for server virtualization software.

Background and Purpose

Server Virtualization, for the purposes of this EP, refers to a virtualization system (VS) that implements virtualized hardware components on server-class hardware. It creates a virtualized hardware environment for each instance of a guest 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 and are generally not directly accessible by non-administrative users.

This EP does not address client virtualization, application virtualization, or containers.

Use Cases

- Virtualized Servers – Virtualized instances of network services traditionally executed on separate hardware platforms, such as web servers, file servers, and mail servers.
- Virtualized Network Infrastructure – Virtualized instances of routers, switches, and other network infrastructure.
- Virtualized Enterprise User Environments – The server back-end of virtual desktop (VDI) or thin-client implementations where actual computation occurs in a server-based VM and the user interacts through a client. The client application is not covered by this EP.

Resources to be protected

- The platform onto which the Virtualization System is installed including the hardware, firmware, and host operating system
- The Virtual Machine Manager (VMM) including the Hypervisor and Service VMs
- The Management Subsystem (if applicable)
- The VMs and their contents

Attacker access

An attacker has access to either:

- One or more Guest VMs, and
- Its operational network

TOE Boundary

- The Virtual Machine Manager (VMM)
    - The Hypervisor

    - Service VMs
    - VM abstractions (but not Guest VM workloads)
- The Management Subsystem (if applicable)

Essential Security Requirements

The following are the essential security requirements that are expected to be implemented by any application that is compliant with the Server Virtualization EP. Note that these security requirements are conditional on that functionality being present. For example, a product that does not require an external network connection for any purpose is considered to satisfy any security requirements that pertain to the secure use of external network connections.

Any other conditional requirements that depend on whether or not the product implements a certain capability are listed in the “Optional Extensions” section below.

The Virtualization System shall:

- Maintain isolation between its VMs (and their resources)
- Maintain the integrity of the VMM
- Protect the platform from VMs and remote users of the VS
- Protect the Management Subsystem (if applicable) from unauthorized access
- Be capable of being updated/patched in a secure and timely manner
- Provide the VMs access to sufficient sources of entropy (or necessary platform resources)
- Provide audit capabilities for security-relevant events

Assumptions

- The VS relies on a trustworthy computing platform for its execution, and it is assumed that the platform has not been compromised prior to the installation of the VS.
- Physical security appropriate to the value of the VS and the data it contains is provided.
- Administrators of the VS are trusted follow and apply all Administrator guidance.
- The VMs will have assurance sufficient to outweigh the risk that they will violate the security policy of the TOE by using covert channels.
- 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.

Optional Extensions

The following requirements may already be realized in some products in this technology class, but the ESR is not mandating these capabilities exist in “baseline” level products:

- Automatic response to certain security events
- Verifying VM Integrity

Objective Requirements

Requirements captured in this section specify security-relevant behavior that is not expected to be realized currently in products of this type, but they are capabilities that may be mandated in future versions of the ESR and resulting PPs.

- Device Driver Isolation
- Support for Software Identification Tags
- Support for VM Introspection
- Support for Measured Launch of Platform and VMM

Outside the TOE's Scope

- The platform onto which the Virtualization System is installed including the hardware, firmware, and non-VS-essential portions of the host operating system (if any)
- Software installed inside VMs that is unrelated to the functioning of the Virtualization System
- Application virtualization
- Containers