INTERNATIONAL STANDARD

ISO/IEC 21878

First edition
2018-11

Information technology — Security techniques — Security guidelines for design and implementation of virtualized servers

Technologies de l'information — Techniques de sécurité — Lignes directrices pour la conception et l'implémentation sécurisées des serveurs virtualisés

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 21878:2018
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af9607c8725b/iso-iec-21878-2018

Reference number
ISO/IEC 21878:2018(E)

© ISO/IEC 2018

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 21878:2018
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af9607c8725b/iso-iec-21878-2018

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

 © ISO/IEC 2018 – All rights reserved

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Symbols and abbreviated terms ... **2**

5 Overview of server virtualization ... **3**
5.1 Types of server virtualization ... 3
5.2 Components of a VS ... 3
5.3 Technical considerations ... 4
5.3.1 General ... 4
5.3.2 Exclusions ... 4

6 Overview of security threats and risks ... **5**
6.1 General ... 5
6.2 Common threats ... 5
6.3 VS-specific risks ... 6
6.3.1 General ... 6
6.3.2 VM risks ... 6
6.3.3 Hypervisor risks ... 7
6.3.4 Operational risks related to implementation ... 8
6.3.5 Cloud Services risks ... 8

7 Recommendations for secure VS lifecycle ... **9**
7.1 General ... 9
7.2 Initial preparation phase ... 9
7.3 Planning and design phase ... 10
7.4 Implementation phase ... 10
7.5 Disposition phase ... 10

8 Planning and design phase: security considerations ... **10**
8.1 General ... 10
8.2 Security considerations and satisfying requirements ... 11

9 Implementation phase: security checklist ... **11**
9.1 General ... 11
9.2 Security checklist and vulnerability exposure ... 12

Annex A (informative) **Risk assessment for VSs** ... **14**

Annex B (informative) **Guidelines for implementing security checklist items in Table 2** ... **17**

Bibliography ... **22**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 21878:2018
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af8607c8725b/iso-iec-21878-2018

© ISO/IEC 2018 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 21878:2018
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af9607c8725b/iso-iec-21878-2018

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

 © ISO/IEC 2018 – All rights reserved

Introduction

Data centre infrastructures are rapidly becoming virtualized due to increasing deployment of virtualized servers (VSs) for cloud computing services and for internal IT services. Since VSs are compute engines hosting many business-critical applications, they are key resources to be protected in virtualized data centre infrastructure. As VSs are becoming mainstream in typical data centre infrastructure setups, the secure design and implementation of VSs forms an important element in the overall security strategy.

The purpose of this document is to provide security guidelines for the design and implementation of VSs. The motivation for this document is the global trend in enterprises and government agencies deploying server virtualization technologies within their internal IT infrastructure as well as the use of VSs by cloud service providers. Hence the target audience is any organization using and/or providing VSs.

The intended goal of this document is to facilitate informed decisions with respect to architecting VS configurations. Such design and implementation configuration is expected to assure the appropriate protection for all virtual machines (VMs) and the application workloads running in them in the entire virtualized infrastructure of the organization.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 21878:2018
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af9607c8725b/iso-iec-21878-2018

© ISO/IEC 2018 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 21878:2018
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af9607c8725b/iso-iec-21878-2018

Information technology — Security techniques — Security guidelines for design and implementation of virtualized servers

1 Scope

This document specifies security guidelines for the design and implementation of VSs. Design considerations focusing on identifying and mitigating risks, and implementation recommendations with respect to typical VSs are covered in this document.

This document is not applicable to: (see also 5.3.2 Exclusions)

— desktop, OS, network, and storage virtualization; and

— vendor attestation.

This document is intended to benefit any organization using and/or providing VSs.

2 Normative references

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 21878:2018
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af9607c8725b/iso-iec-21878-2018

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17788 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org

3.1
domain
information domain
collection or cluster of *virtual machines* (3.7) hosted in one or more VSs

3.2
guest operating system
guest OS
operating system that runs within a *virtual machine* (3.7)

3.3
host operating system
host OS
operating system onto which virtualization software (hypervisor) is installed

Note 1 to entry: Host OS is an optional component of a virtualized server.

© ISO/IEC 2018 – All rights reserved

3.4
hypervisor
computer software that creates and runs one or more *virtual machines* (3.7)

3.5
management subsystem
component of a VS that enables administrators to configure the VS components

3.6
hardware
physical resources including processors, memory, devices, and associated firmware

3.7
virtual machine
VM
software-defined complete execution stack consisting of virtualized *hardware* (3.6), operating system (guest OS), and applications

3.8
virtualized server
VS
physical host on which a *hypervisor* (3.4) is installed to enable execution of multiple *virtual machines* (3.7)

3.9
virtualized server administrator
VS administrator
person with rights and responsibilities to configure and manage VS components

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.10
virtual machine manager
VMM
all software that enables VMs to run on a virtualized platform which includes the hypervisor, service VMs, virtual and physical device drivers

ISO/IEC 21878:2018
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af9607c8725b/iso-iec-21878-2018

3.11
golden image
golden VM image
master copy of disk image of a VM or server with a specific configuration

4 Symbols and abbreviated terms

API	Application programming interface
CLI	Command line interface
COBIT 5	Control objectives for information and related technologies
CSC	Cloud service customer
CSP	Cloud service provider
IT	Information technology
NFV	Network function virtualization
OASIS	Organization for the advancement of structured information systems
OS	Operating system

© ISO/IEC 2018 – All rights reserved

PII	Personally identifiable information
SDN	Software-defined networking,
SSD	Solid state drive
VLAN	Virtual local area network

5 Overview of server virtualization

5.1 Types of server virtualization

Server virtualization is the abstraction of the underlying hardware resources to enable multiple computing stacks (consisting of an OS, middleware and applications) to be run on a single physical host. A VS is commonly classified along two perspectives.

The first perspective addresses full virtualization versus para-virtualization.

— **Full virtualization:** The guest OS is unaware that it is in a virtualized platform. The hypervisor exposes the interface of a hardware device that is physically available to the VM and for which drivers are available for guest OS, and it completely emulates the behaviour of that device. Emulation allows the programs running in VMs to use the VM OS drivers that were designed to interact with the emulated device without installing any special driver or tool specified by the hypervisor vendor.

— **Para-virtualization**: In this implementation, the hypervisor exposes a device that does not physically exist, which is just software only, and presents a lightweight interface. However, this scenario calls for having special drivers in the VM, requiring modification to the guest OS which becomes para-virtualized-aware. This approach is intended to increase the performance level of the applications running in the VM, compared to the full emulation approach adopted in full virtualization.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af9607c8725b/iso-iec-21878-2018

The second perspective is based on the platform on which the hypervisor is installed. There are two types of hypervisors:

— **Type 1** hypervisors, also known as bare-metal hypervisors, are installed directly over computer hardware, with no need for an underlying host OS.

— **Type 2** hypervisors are hosted on top of a host OS. Type 2 hypervisors are started like a regular software application before any VMs can be run and controlled.

5.2 Components of a VS

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

© ISO/IEC 2018 – All rights reserved

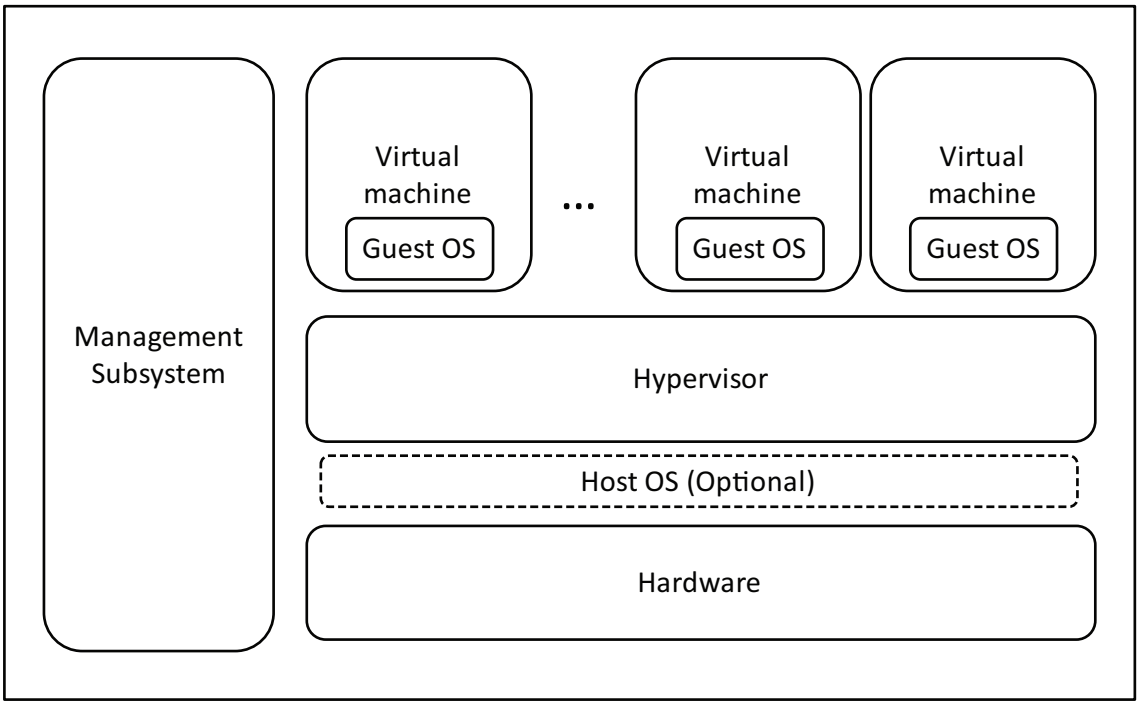

Figure 1 — Functional components of a VS

iTeh STANDARD PREVIEW
(standards.iteh.ai)

A VS comprises the following functional components as illustrated in Figure 1:

ISO/IEC 21878:2018
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af9607c8725b/iso-iec-21878-2018

— a hypervisor;

— virtual machine(s);

— hardware;

— host OS (optional);

— other components such as management subsystem(s) for the VS administrator to configure and manage the VS.

In general, for server virtualization products that are installed onto "bare metal," the entire set of installed components constitutes the VS, and the hardware constitutes the platform. Also for products that are hosted by or integrated into a commercial off-the-shelf (COTS) OS, the components installed expressly for implementing and supporting virtualization are in the VS, and the platform comprises of the hardware and host OS.

5.3 Technical considerations

5.3.1 General

This document's recommendations are applicable to both perspectives of server virtualization as described in 5.1. From this viewpoint, the security guidelines in this document can be replicated across a larger scale (for example, in environments with thousands of VS and more).

5.3.2 Exclusions

5.3.2.1 Vendor attestation

A manufacturer or vendor of a product can claim an attestation of conformance to a standard.

 © ISO/IEC 2018 – All rights reserved

This document provides guidance regarding the design and implementation of existing products and makes no specific requirements on the virtualization or associated products mentioned.

5.3.2.2 Operating environment

There are specific conditions that are assumed to exist in the operational environment where VS is deployed and hence not addressed in this document. These assumptions include both practical realities in the development of the VS security requirements and the essential environmental conditions on the use of the VS.

— **Physical security:** Physical security should be commensurate with the value of the VS and the data it contains.

— **Platform integrity**: The platform has not been compromised prior to installation of the VS.

— **Trusted administrators:** VS administrators are trusted to follow and apply all administrator guidance.

6 Overview of security threats and risks

6.1 General

The threats and risks in a virtualized infrastructure (where the computing nodes are predominantly VSs) can be classified into two types:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

— Common threats: Threats common to all types of IT infrastructures (virtualized or non-virtualized);

— VS-specific risks: Risks that impact the confidentiality, integrity and availability of VSs.

ISO/IEC 21878:2018
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af9607c8725b/iso-iec-21878-2018

6.2 Common threats

The following threats are commonly faced in virtualization setups in data centre infrastructures or cloud computing environments, but not specific to just for VSs technology per se.

— **Administrator error:** An administrator can unintentionally install or configure the VS incorrectly, resulting in ineffective security mechanisms.

— **Data leakage:** If it is possible for data to leak between domains when prohibited by policy, then an adversary on one domain or network can obtain data from another domain. Such cross-domain data leakage can, for example, cause classified information, corporate proprietary information, or PII data to be made accessible to unauthorized entities.

— **Insecure network configuration:** The VS is itself a node of a larger enterprise network and hence insecure network location and insecure host-level protection can have an impact on all the software and applications running in it.

— **Platform compromise:** The hosting of untrusted or malicious domains by the VS can compromise the security and integrity of the platform on which the VS executes.

— **Poor cryptography key management:** When the keys of the cryptographic applications are stored in insecure locations, the security of encrypted data can easily be compromised.

— **Third-party software:** Vulnerabilities in third-party software used as a VS component (e.g., device drivers) can compromise the security of an entire VS.

— **Unauthorized access:** A user can gain unauthorized access to the VS data and VS executable code. A malicious user, process, or external IT entity can masquerade as an authorized entity in order to gain unauthorized access to VS data or VS resources.

© ISO/IEC 2018 – All rights reserved

— **Unauthorized modification:** Malware running on the physical host can undetectably modify VS components while the components are in execution mode or at rest. Likewise, malicious code running within a VM can modify VS components.

— **Unauthorized update:** A malicious program can gain administrative privileges to perform an unauthorized update that can compromise the integrity of one or more VS functions.

— **VMM compromise:** Failure of security mechanisms can lead to unauthorized intrusion into or modification of the VMM or bypass of the VMM altogether.

— **Weak cryptography:** A threat of weak cryptography can arise if the VMM does not provide sufficient entropy to support security-related features that depend on entropy to implement cryptographic algorithms.

6.3 VS-specific risks

6.3.1 General

VS-specific risks are examined in further detail here. Moving to a virtualized environment brings a unique set of risks not present in traditional IT environment. These risks include:

— VM risks;

— hypervisor risks;

— operational risks related to implementation;

— cloud services risks.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

6.3.2 VM risks

ISO/IEC 21878:2018
https://standards.iteh.ai/catalog/standards/sist/ec958d3a-1a86-4534-9988-af9607c87258/iso-iec-21878-2018

The use of VMs can either introduce new and unique security risks or lead to more significant impacts for particular known risks. Consequently, as part of assessing the risks of virtualization, the following should be considered:

— **VM sprawl**: Uncontrolled proliferation of VMs can lead to an unmanageable condition of unpatched and unaccounted for machines. In a traditional IT environment, physical servers are procured. This requirement enforces effective controls, because change requests should be created and approved before hardware and software can be acquired and connected to the data centre. In the case of virtualized environments, however, VMs can be allocated quickly, self-provisioned, or moved between physical servers, bypassing the conventional change management process. Without an effective control process in place, VMs and other virtual systems with unknown configurations can quickly proliferate, consuming resources, degrading overall system performance, and increasing liability and risk of exposure. Because these machines are typically not readily detectable or visible, they cannot be effectively monitored or tracked for the application of security patches or effectively investigated when a security incident occur.

— **Sensitive data within a VM:** Data confidentiality within VMs can be easily compromised, because data can easily be transported and tampered with. Although VM images and snapshots provide a way to deploy or restore virtual systems quickly and efficiently across multiple physical servers, this capability means that copies of images and snapshots can be removed from a data centre easily. This removal includes current memory contents, which are not intended to be stored on the storage devices themselves. Therefore, in a virtualized environment, it is no longer possible to assure that sensitive data such as system password files is safe from unauthorized personnel. This sensitive information and the VM containing it can be moved easily, making it possible to compromise a VM and reintroduce it into the system later. Without proper controls, security loopholes can exist through the inadvertent capture, storage, and deployment of sensitive information, including rogue virtual instances of critical services. Potential hackers or disgruntled staff can gain access and insert malicious code into VM images and snapshots, which can then be rapidly deployed throughout the environment, resulting in its compromise.

 © ISO/IEC 2018 – All rights reserved