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



Reference number
ISO/IEC 21878:2018(E)

© ISO/IEC 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

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**

© 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.

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

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.

© ISO/IEC 2018 – All rights reserved

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

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*

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

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

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