International Standard

ISO/IEC 23167

Information technology — Cloud computing — Common technologies and techniques

First edition
2026-07

Sample Document

get full document from standards.iteh.ai

Reference number
ISO/IEC 23167:2026(en)

© ISO/IEC 2026

Sample Document

get full document from standards.iteh.ai

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols and abbreviated terms **4**
5 Overview of common technologies and techniques used in cloud computing **5**
5.1 General 5
5.2 Technologies 5
5.2.1 General 5
5.2.2 Infrastructure capabilities type of cloud services 5
5.2.3 Platform capabilities of cloud services 6
5.2.4 Application capabilities type of cloud services 6
5.3 Techniques 6
6 Virtual machines and hypervisors **6**
6.1 General 6
6.2 Virtual machines and system virtualization 7
6.3 Hypervisors 7
6.3.1 General 7
6.3.2 Type I hypervisors 8
6.3.3 Type II hypervisors 8
6.4 Security of VMs and hypervisors 8
6.5 VM images, metadata and formats 9
7 Containers and container management systems (CMSs) **10**
7.1 General 10
7.2 Containers and operating system virtualization 10
7.2.1 Description of containers 10
7.2.2 Container daemon 11
7.2.3 Container resources, isolation and control 12
7.3 Container images and filesystem layering 13
7.3.1 Image purpose and content 13
7.3.2 Filesystem layering 14
7.3.3 Container image repositories and registries 15
7.4 Container management systems (CMSs) 15
7.4.1 General 15
7.4.2 Common CMS capabilities 16
8 Serverless computing **17**
8.1 General 17
8.2 Functions as a service 18
8.2.1 Overview 18
8.2.2 Functions within FaaS 18
8.2.3 Serverless frameworks 19
8.2.4 FaaS relationship to microservices and containers 19
8.3 Serverless databases 20
9 Microservices architecture **20**
9.1 General 20
9.2 Advantages and challenges of microservices 21
9.3 Specification of microservices 23
9.4 Multi-layered architecture 23
9.5 Service mesh 25
9.6 Circuit breaker 27

Sample Document
iTeh Standards

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

9.7 API gateway ... 27
10 Automation ... 28
10.1 General ... 28
10.2 Automation of the development lifecycle ... 28
10.3 Tooling for automation ... 28
11 Architecture of PaaS systems ... 29
11.1 General ... 29
11.2 Relationship with ISO/IEC TS 7339:2024 ... 30
11.3 Characteristics of PaaS systems ... 30
11.4 Architecture of components running under PaaS system ... 32
12 Data storage as a service ... 34
12.1 General ... 34
12.2 Common features of DSaaS ... 34
12.3 Capabilities type of DSaaS ... 38
12.4 Significant additional capabilities of DSaaS ... 39
13 Networking in cloud computing ... 39
13.1 Key aspects of networking ... 39
13.2 Cloud access networking ... 40
13.3 Intra-cloud networking ... 40
13.4 Virtual private networks (VPNs) and cloud computing ... 41
14 Cloud computing scalability ... 43
14.1 Scalability approaches ... 43
14.2 Parallel instances and load balancing ... 44
14.3 Elasticity and automation ... 44
14.4 Database scaling ... 44
15 Security and the cloud common technologies ... 45
15.1 General ... 45
15.2 Firewalls ... 45
15.3 Endpoint protection ... 46
15.4 Identity and access management (IAM) ... 46
15.5 Data encryption ... 46
15.6 Encryption key management ... 46
Bibliography ... 48

Sample Document
Get full document from standards.iteh.ai

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

Sample Document

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Cloud computing and distributed platforms*.

get full document from standards.iteh.ai

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 and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

Introduction

Cloud computing is described at a high, conceptual level in the foundational standards ISO/IEC 22123-1, ISO/IEC 22123-2[1] and ISO/IEC 22123-3[2].

However, as the use of cloud computing has developed, a set of commonly used technologies has emerged to support, simplify and extend the use of cloud computing alongside sets of commonly used techniques which enable the effective exploitation of the capabilities of cloud services. Many of these common technologies and techniques are aimed at developers and operations staff, increasingly linked together in a unified approach called DevOps (see 10.2). The aim is to speed and simplify the creation and operation of solutions based on the use of cloud services.

This document describes common technologies and techniques in cloud computing and their relationships. It also specifies how these are applied by roles associated with cloud computing.

This document addresses areas that are still developing in the industry and will be of primary interest to service developers in cloud service providers.

Sample Document

get full document from standards.iteh.ai

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

Information technology — Cloud computing — Common technologies and techniques

1 Scope

This document provides a description of a set of common technologies and techniques used in conjunction with cloud computing. These include:

— virtual machines (VMs) and hypervisors;

— containers and container management systems (CMSs);

— serverless computing;

— microservices architecture;

— automation;

— platform as a service systems and architecture;

— storage services;

— security, scalability and networking as applied to the above cloud computing technologies.

Sample Document

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 TS 5928, *Information technology — Cloud computing and distributed platforms — Taxonomy for digital platforms*

ISO/IEC TS 7339:2024, *Information technology — Cloud computing — Overview of platform capabilities type and platform as a service*

ISO/IEC 22123-1:2023, *Information technology — Cloud computing — Part 1: Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22123-1, ISO/IEC TS 5928, ISO/IEC TS 7339 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 https://www.electropedia.org/

3.1
guest operating system
guest OS
operating system that runs within a virtual machine

[SOURCE: ISO/IEC 21878:2018, 3.2]

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

3.2
host operating system
host OS
operating system onto which virtualization software is installed

Note 1 to entry: "virtualization software" can include both hypervisor and virtual machines as well as *container daemon* (3.4) and containers.

3.3
serverless computing
cloud service category in which the cloud service customer can use different cloud capabilities types without the cloud service customer having to provision, deploy and manage either hardware or software resources, other than providing cloud service customer application code or providing cloud service customer data

Note 1 to entry: Serverless computing provides automatic scaling with dynamic elastic allocation of resources by the cloud service provider, automatic distribution across multiple locations, and automatic maintenance and backup.

Note 2 to entry: Serverless computing functionality is triggered by one or more cloud service customer defined events and can execute for a limited time period as required to deal with each event.

Note 3 to entry: Serverless computing functionality can be invoked by direct invocation from web and mobile applications.

3.4
container daemon
software service that executes on a *host operating system* (3.2) and is responsible for creating, starting and stopping containers on that system

Note 1 to entry: Container daemon directly interacts with containers for lifecycle management.

Note 2 to entry: Container daemons are also known as container runtimes in some applications.

Sample Document

3.5
container management system
CMS
get full document from standards.iteh.ai
software that provides for management and orchestration of container instances

Note 1 to entry: Capabilities include initial creation and placement, scheduling, monitoring, scaling, update and the parallel deployment of capabilities such as load balancers, firewalls, virtual networks and logging.

Note 2 to entry: The acronym CMS refers to container management system, not content management system.

3.6
functional decomposition
type of modular decomposition in which a system is broken down into components that correspond to system functions and subfunctions

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.1695-modified — cf. hierarchical decomposition, stepwise refinement deleted]

3.7
continuous deployment
CD
automated process of deploying changes to production by verifying intended features and validations to reduce risk

[SOURCE: ISO/IEC/IEEE 32675:2022, modified — The abbreviated term "CD" has been added.]

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

3.8
continuous delivery
CD
software engineering practices that allow for frequent releases of new systems (including software) to staging or various test environments through the use of automated tools

[SOURCE: ISO/IEC/IEEE 32675:2022, modified — The abbreviated term "CD" has been added.]

3.9
DevOps
methodology which combines together software development and IT operations in order to shorten the development and operations lifecycle

3.10
DevSecOps
DevOps (3.9) extended to include security capabilities as an essential and integral part of the development and operations processes

3.11
orchestration
type of composition where one particular element is used by the composition to oversee and direct the other elements

Note 1 to entry: The element that directs an orchestration is not part of the orchestration (composition instance) itself.

Note 2 to entry: See ISO/IEC 18384-3:2016, 8.3.

[SOURCE: ISO/IEC 18384-1:2016, 2.16]

Sample Document

3.12
virtual machine image
VM image
information and executable code required to run a virtual machine

get full document from standards.iteh.ai

3.13
virtual machine metadata
VM metadata
information about a virtual machine configuration and startup

3.14
microservice
independently deployable artefact providing a service implementing a specific functional part of an application

3.15
microservices architecture
design approach that divides an application into a set of *microservices* (3.14)

3.16
function as a service
FaaS
cloud service category in which the capability provided to the cloud service customer is the execution of cloud service customer application code, in the form of one or more functions that are each triggered by a cloud service customer specified event

3.17
serverless database
a form of serverless computing in which the capability used by the cloud service customer is a database, where the database is provisioned, managed and operated by the cloud service provider

Note 1 to entry: See ISO/IEC TS 7339 for further explanation of the cloud service developer.

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

3.18
container registry
component that provides the capability to store and to access container images

4 Symbols and abbreviated terms

API	application programming interface
CMS	container management system
CSC	cloud service customer
CSD	cloud service developer
CSP	cloud service provider
DDoS	distributed denial of service
DNS	domain name service
GUI	graphical user interface
HTTP	hypertext transfer protocol
IaaS	infrastructure as a service
IAM	identity and access management
IP	internet protocol
JSON	javascript object notation
MAC	media access control
OCI	open containers initiative
OS	operating system
OVF	open virtualization format
PaaS	platform as a service
REST	representational state transfer
SaaS	software as a service
SCM	source control management
SSL	secure sockets layer
TLS	transport layer security
VM	virtual machine
VPN	virtual private network
YAML	YAML ain't markup language

Sample Document
get full document from standards.iteh.ai

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

5 Overview of common technologies and techniques used in cloud computing

5.1 General

This document provides a description of a set of common technologies and techniques used in conjunction with cloud computing.

A common technology is one that is used to implement one or more of the functional components of cloud computing described in ISO/IEC 22123-3:2023,9.2,[2] cloud computing reference architecture. The common technologies often form part of a cloud service or are employed by the CSC when using a cloud service.

A common technique is a methodology or an approach to performing some of the activities associated with cloud computing, as described in ISO/IEC 22123-3:2023,10.2.2.[2] It is typical of the common techniques to either reduce the effort needed to make use of cloud services or to enable full use of the capabilities provided by cloud services.

Many of the common technologies and techniques are used in conjunction when developing and operating cloud native applications.

Many of the common technologies for cloud computing described in this document can also be applied to nodes and systems that are located near to the user (i.e., at or near the edge). ISO/IEC TR 23188[3] provides more details on the use of cloud computing technologies when cloud solutions include edge computing.

The various common technologies and techniques are described in detail in the following clauses.

NOTE Throughout this document, the term “platform” refers to a “digital technology platform” as defined in ISO/IEC TS 5928:2023.

Sample Document

5.2 Technologies

5.2.1 General

get full document from standards.iteh.ai

The common technologies principally relate to the virtualization and to the control and management of virtualized resources in the development and operation of cloud native applications. A cloud native application is an application that is explicitly designed to run within and to take advantage of the capabilities and environment of cloud services. These technologies address the three primary hardware resources of processing, storage and networking as identified in ISO/IEC 22123-3:2023,9.2.5.3.[2] They also address the platform capabilities type of cloud service. These technologies include:

— virtualized processing is addressed by virtual machines (see Clause 6), by containers (see Clause 7), by serverless computing (see Clause 8);

— virtualized storage is addressed by means of a variety of Data Storage as a Service (see Clause 12);

— virtualized networking is one of the primary groups of technologies for the provision and use of networking capabilities in relation to cloud services (see Clause 13);

— the PaaS category of cloud services are designed to enable more rapid development, testing and production of cloud native applications (see Clause 11 and ISO/IEC TS 7339).

Security and scalability technologies apply generally across all types of cloud services, although the explicit use of the technologies by the CSC is more common for some types of cloud service (see Clause 14 and Clause 15).

5.2.2 Infrastructure capabilities type of cloud services

Technologies commonly used with the infrastructure capabilities type of cloud services include:

— virtual machines;

— containers;

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

— virtualized storage;

— virtualized networking;

— security.

5.2.3 Platform capabilities of cloud services

Technologies commonly used with the platform capabilities type of cloud services include:

— containers;

— serverless computing;

— PaaS cloud services;

— virtualized storage;

— virtualized networking;

— security.

5.2.4 Application capabilities type of cloud services

Technologies commonly used with the application capabilities type of cloud services include:

— virtualized storage;

— virtualized networking;

— security.

Sample Document
get full document from standards.iteh.ai

5.3 Techniques

The common techniques typically apply to all cloud service categories, although some techniques are more useful with some categories of cloud service than others.

Orchestration and management of virtualized resources is achieved with tooling, including CMSs (see Clause 10 and 7.4).

Techniques commonly used with cloud computing include:

— automation of various kinds, applied throughout the DevOps processes (see Clause 10);

— scalability approaches such as parallel instances (see Clause 14);

— microservices design approach to applications and systems (see Clause 9);

— firewalls, encryption, and IAM techniques for security and protection of privacy (see Clause 15).

6 Virtual machines and hypervisors

6.1 General

Virtual machines and hypervisors are technologies that provide virtualized processing (also known as virtualized compute) for cloud services. These technologies primarily relate to cloud services of infrastructure capabilities type and IaaS as described in ISO/IEC 22123-2:2023[1].

One of the key characteristics of cloud computing is its ability to share resources. This is fundamental to its economics, but it is also important for cloud computing characteristics such as scalability and resilience. Sharing of processing resources requires some level of virtualization. Virtualization provides an abstraction of the underlying physical resource. The physical resource is converted into a software defined form, i.e. the

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

virtual resource, for use by other software entities, enabling multiple users to share the physical resource without interference. In other words, virtualization provides an abstraction of the underlying resource, being converted into a software defined form for use by other software entities. The software performing the virtualization enables multiple users to simultaneously share the use of a single physical resource without interfering with each other and usually without them being aware of each other (see ISO/IEC 22123-2:2023, Clause 9[1]).

One approach to the virtualization of processing resources is the use of virtual machines, which involves a hypervisor providing an abstraction of the system hardware and permitting multiple virtual machines to run on a given physical system, with each VM containing its own guest operating system (guest OS), as shown in Figure 1. This permits the system to be shared by the applications running in each VM.

The hypervisor is typically software that is installed and operated by the CSP. The cloud service that runs the VM offers the capability for the CSU to load software from a VM image and run the software within a VM on the CSP system. The VM is managed by the hypervisor, but this is not seen directly by the CSU. The CSU uses VMs to run software from VM images without direct interaction with the hypervisor.

6.2 Virtual machines and system virtualization

A virtual machine is a self-contained environment that runs software using emulated hardware. It virtualizes the underlying system so that each VM's software gets tightly managed access to real resources, allowing multiple VMs to share them without affecting one another. Often called system VMs, they can host full software stacks: an entire operating system plus the applications that run on it (see ISO/IEC 22123-2:2023, Clause 9). This is as depicted by the "Guest OS" and "App x" within each VM shown in Figure 1 and 2.

The purpose of VMs is to enable multiple applications to run at the same time on one hardware system, while those applications remain isolated from each other. The software running within each VM appears to have its own system hardware, such as processor, runtime memory, storage device(s) and networking hardware. Isolated means that the software running within one VM is separated from and unaware of software running within other VMs on the same system and is also separated from the host OS. Virtualization commonly means that a subset of the available physical resources can be made available to each VM, such as limited numbers of processors, limited RAM, limited storage space and controlled access to networking capabilities.

Standards Document
get full document from standards.iteh.ai

Each VM runs a complete software stack, from the operating system to the software to run the applications. Different VMs may run different operating systems, as long as the VM is compatible with the hardware architecture.

6.3 Hypervisors

6.3.1 General

A hypervisor, also called a virtual machine monitor, is software that abstracts the system's hardware so virtual machines can run. It controls how the underlying physical resources are presented and used, oversees VM operations, and assigns each VM its share of CPU, memory, storage, and network capacity (see ISO/IEC 22123-2:2023, 9.2.3[1]).

Hypervisors exist as one of two types:

— "Bare metal", "native" or "type I";

— "Embedded", "hosted" or "type II".

Type I hypervisors can be faster and more efficient, since they do not need to work via a host operating system. Type II hypervisors can be slower, but have the advantage of being typically easier to set up and are compatible with a broader range of hardware than type I hypervisors, since hardware variations have to be dealt with in the type I hypervisor code, whereas the type II hypervisors take advantage of the hardware support built in to the host operating system.

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

6.3.2 Type I hypervisors

Type I hypervisors run directly on the underlying system hardware and control that hardware directly as well as managing the VMs. The organization of a system using a type I hypervisor is shown in Figure 1.

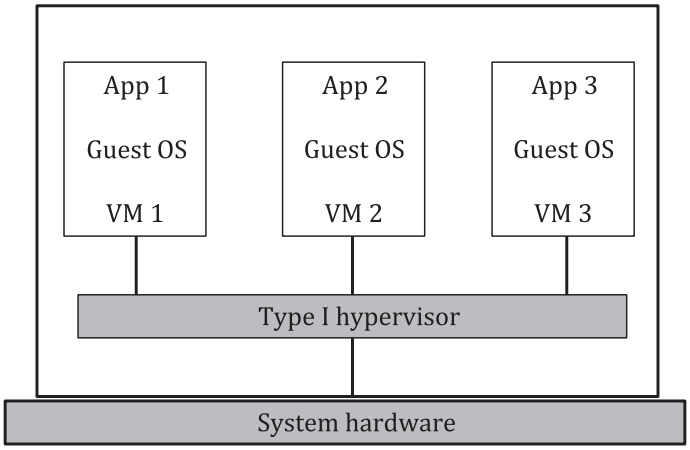

Figure 1 — Type I hypervisor for virtualization of system hardware

6.3.3 Type II hypervisors

Type II hypervisors run on top of a host operating system, more specifically the host OS kernel. It is the host operating system that controls the system hardware, while the hypervisor makes use of its capabilities to run and manage the VMs. The organization of a system with a type II hypervisor is shown in Figure 2.

Sample Document
get full document from standards.iteh.ai

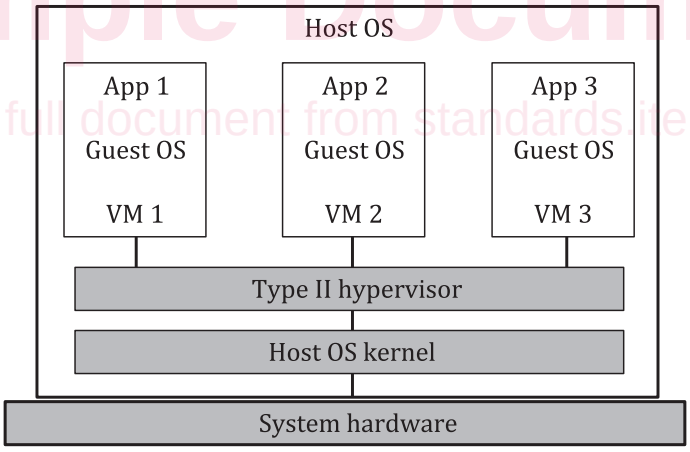

Figure 2 — Type II hypervisor for virtualization of system hardware

6.4 Security of VMs and hypervisors

For hardware systems, the operating system runs at the highest privilege level since it controls access to all hardware resources. However, in a hypervisor host, since the hypervisor controls all access to CPU and memory by guest VMs (providing processor and memory virtualization), it runs at a privilege level higher than all VMs. To facilitate this, hypervisors are installed on hardware systems that provide assistance for virtualization. Specifically, the hardware system provides two processor states: root (hypervisor) mode and non-root (guest) mode. All guest OSs run in non-root mode while the hypervisor alone runs in root mode.

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026

Despite the hardware support for virtualization, the runtime process isolation for VMs provided by the hypervisor can be subverted by rogue or compromised VMs which have gained access to areas of memory belonging to the hypervisor or other VMs.

— Rogue VM threat: rogue or compromised VMs exploit certain hypervisor design vulnerabilities with respect to certain software structures such as virtual machine control block (VMCB) and memory page tables which are used by the hypervisor to keep track of the execution state of VMs and memory mapping from VM addresses to host memory addresses respectively. These vulnerabilities of hypervisors have been known for some time and as a result, many of the vulnerabilities have been addressed or are being addressed. More recent hypervisor versions have been updated and hardened. The CSC and CSP should check that any hypervisors in use are up-to-date and hardened against known security vulnerabilities;

— Device virtualization vulnerabilities: another security implication in a hypervisor host platform stems from software used for providing device virtualization. Unlike instruction set and memory virtualization, device virtualization is not directly handled by the hypervisor but by using supporting software modules. Primary sources of vulnerabilities include:

  — code emulating physical hardware devices running in the hypervisor as a loadable kernel module and

  — device drivers for direct memory access (DMA) capable devices which can access memory regions belonging to other VMs or even the hypervisor.

Potential downstream impacts of a rogue VM taking control of the hypervisor include the installation of rootkits or attacks on other VMs on the same hypervisor host. All device virtualization software should be verified against security flaws before installation and use on a system using a hypervisor and VMs.

6.5 VM images, metadata and formats

A virtual machine image (VM image) is a package of data that contains the information and executable code necessary to run an instance of a VM. The VM image is used to instantiate a new instance of a VM, as required. The VM image can include the complete software stack required to run an application, starting with the operating system, libraries, runtimes, the application code itself, configuration files and other metadata used by the application. The VM image can also include metadata associated with the instantiation of the VM itself.

The VM metadata contains information about the configuration and startup of the VM. This may include properties of the VM such as RAM size, CPU requirements and so on. The VM metadata also typically references the disk images contained in the VM image, in particular indicating how they are deployed into a VM instance.

The concept of the VM image is that it should contain all the entities required to run an instance of a VM, where the VM image is used as input data to a hypervisor to enable it to create and start the VM. Broadly, the VM image consists of two sets of data – firstly, VM metadata and secondly disk images. It is important to understand that there are in existence many different formats of both VM metadata and disk images. A particular hypervisor used to instantiate a VM may only understand specific formats for the VM metadata and disk images. Some of the formats are proprietary, while others are open or standardized.

VM images are based on data held in files – files on filesystems, which are held in the VM image as one or more disk images. These files can be those of the operating system, the application and any other part of the software stack that is required. There is at least one disk image, but there can be multiple disk images if this is the organization of files that is used by the application and its software stack. It is often the case that the volume of data held in the disk images is very large and as a result, the formats used to store the data involve the use of compression in one form or another.

There are many VM image and disk image formats in use, a substantial proportion of which are proprietary or which are open source.

EXAMPLE Standardized VM image and disk image formats include:

— OVF ("Open Virtualization Format") (see ISO/IEC 17203:2017[11])

© ISO/IEC 2026 – All rights reserved

ISO/IEC 23167:2026 • https://standards.iteh.ai/catalog/standards/iso/1250c033-f164-422c-b6f1-648b118410aa/iso-iec-23167-2026