Cloud OS Security Specification v2.0

cloud security alliance®

The permanent and official location for Software Defined Perimeter Working Group is
https://cloudsecurityalliance.org/research/working-groups/cloud-component-specifications/

Acknowledgments

Initiative Lead:

Xiaoyu Ge

Key Contributors:

Dez Blanchfield
Robert Bolton
Shobharani Jagathpal
Matt Kaufman
Humayun Khan
Alan Leffingwell
Edgar Pimenta
K.S Reddy
Michael Roza
Justin Stoner
Srinivas Tatipamula
Cedric Thibault
Yu Zhang

CSA Global Staff:

Ekta Mishra
AnnMarie Ulskey (Design)
Haojie Zhuang

Table of Contents

1. Scope

This Cloud Security Alliance (CSA) specification defines cloud operating systems' security specifications, specifically their technical requirements. Information security management systems (ISMS) are out of the scope of this specification.

Cloud Security Alliance's Cloud Component Specifications Working Group first published the Cloud OS Security Specification v1[1] in July 2019. Some of the key changes and updates made in this revised version are:

1. The document structure was adjusted to be more in-line with logical architecture. Corresponding contents in version 1 are also moved/combined /removed according to the structural adjustment.
2. New requirements were added in response to cloud security technology developments, including micro-segmentation, hardware-based encryption, virtual machine (VM) high availability, backup and recovery capability, key management service, and a cloud bastion host.
3. Several requirements are improved and revised to be more precise and instructive, such as protocol related to processing/saving sensitive information, identity management, and log functions.

2. Normative References

The following recommendations and international standards contain provisions which, through reference in this text, constitute provisions of this specification.

- *CSA Research - Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*
- *ISO/IEC 17788 Information technology – Cloud computing – Overview and vocabulary*
- *ISO/IEC 19941 Information technology – Cloud computing – Interoperability and portability*
- *ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary*
- *ISO/IEC 27017 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- *NIST SP 500-299- Cloud Computing Security Reference Architecture*
- *NIST SP 800-144 - Guidelines on Security and Privacy in Public Cloud Computing*

[1] https://cloudsecurityalliance.org/artifacts/cloud-os-security-specification/

3. Definitions

3.1 Terms Defined Elsewhere

Definitions have been derived from *ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary*[2].

3.1.1 Cloud computing: Cloud computing, also referred to as "the cloud," is the paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

Note: Examples of resources include: servers, operating systems, networks, software, applications, and storage equipment.

Requirements include:

3.1.2 Component: A functional building block needed to engage in a cloud computing activity, backed by an implementation.

3.1.3 Cloud service: One or more capabilities offered via cloud computing (3.1.1), invoked using a defined interface.

3.1.4 Cloud service product: A cloud service allied to the set of business terms under which the cloud service is offered.

3.1.5 Cloud service provider (CSP): A party making cloud service (3.1.3) available.

3.1.6 Cloud service customer (CSC): A party in a business relationship for the purpose of using cloud services (3.1.3).

3.1.7 Cloud service user: A person, or entity acting on their behalf, associated with a cloud service customer (3.1.6) that uses cloud services (3.1.3).

3.1.8 Tenant: One or more cloud service users (3.1.7) sharing access to a set of physical and virtual resources.

3.2 Terms Defined in This Specification

3.2.1 Cloud operating system: A type of operating system (OS) designed to operate within cloud computing and virtualization environments. A cloud operating system manages the operation, execution, and processes of virtual machines, virtual servers, and virtual infrastructure, as well as back-end hardware and software resources.

[2] ISO/IEC 17788:2014(E) Information technology — Cloud computing — Overview and vocabulary

4. Abbreviations

API	Application programming interface	IP	Internet protocol
CBH	Cloud bastion host	KMS	Key management service
CPU	Central processing unit	LAN	Local area network
CSA	Cloud Security Alliance	LAN	Local area network
CSC	Cloud service customer	NIC	Network interface card
CSRF	Cross-site request forgery	NIST	National Institute of Standards and Technology
CVE	Common vulnerabilities and exposure	OS	Operating system
DEK	Data encryption key	O&M	Operations and maintenance
DHCP	Dynamic host configuration protocol	PaaS	Platform as a service
DPI	Deep packet inspection	SaaS	Software as a service
HSM	Hardware security module	SQL	Structured query language
HTTPS	Hypertext transfer protocol over secure socket layer	SSA	Security situation awareness
IaaS	Infrastructure as a service	SSL	Secure sockets layer
IAM	Identity and access management	TLS	Transmission layer security
IDS	Intrusion detection system	VFR	Virtual firewall/router
IPS	Intrusion protection systems	VM	Virtual machine
IEC	International Electrotechnical Commission	VLAN	Virtual local area network
ISMS	Information security management system	VPC	Virtual private cloud
ISO	International Organization for Standardization	WAF	Web application firewall
IT	Information technology	WTP	Web tamper protection
I/O	Input/output		

5. Goals and Objectives

From a user perspective, the cloud is a service. However, for cloud service providers, integrators, and channel partners who construct or build the cloud, it is a system that may comprise many separate components. The most basic cloud component is the cloud OS—a feature with functionality that closely resembles the relationship between Linux and a computer. Through the utilization of virtualization technology, cloud OS virtualizes hardware resources of physical servers and storage area network devices and supports software-defined networking. Along with virtualization, cloud OS also provides management and configuration capabilities on virtualized hardware resources. Furthermore, it affords many other capabilities and functions like disaster recovery, firewalls, load balancers, access control, and backup control to enhance the performance and security of cloud computing systems as well as the user experience of administrators and users.

As a result, it is vital to specify the security requirements of cloud OS technically. Currently, most of the standards related to cloud computing security focus on information security management systems (ISMS), and corresponding certifications only concentrate on cloud services rather than specific cloud components. There is a lack of internationally recognized technical security specifications and certifications for cloud components such as the cloud OS. The CSA believes the guidance provided in this paper will be useful to help regulate security requirements for the cloud OS to prevent security threats and improve the security capabilities of cloud OS products.

6. Overview

This document builds on the foundation provided by *ISO/IEC 17788, ISO/IEC 19941, ISO/IEC 27000, NIST SP 500-299,* and *NIST SP 800-144* in the context of cloud computing security. Security property and functionality presented by cloud service providers—such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and Huawei—are referenced in this report. Additionally, CSA research artifact *Security Guidance for Critical Areas of Focus in Cloud Computing* is one of the central baseline references for this paper. However, this publication differs from these respective resources by focusing on a specific cloud computing component: the cloud OS. Specifically, this report aims to clarify the security functions and requirements of the cloud OS needed to maintain the system's smooth operation, protect cloud data, and provide secure and trusted cloud computing services to the CSC.

A cloud OS serves as a computing platform between infrastructure devices and service applications, manages, operates, and executes virtual infrastructure processes such as virtual machines, virtual servers, and hardware and software resources within the cloud environment. The cloud OS also grants interfaces through which the CSC can manage tasks on mobile internet devices, tablets, and netbooks wherever and whenever they prefer. While cloud OS affords convenient, fast access to cloud computing resources, various security challenges may accompany this access that can affect cloud computing systems' regular operation and threaten the confidentiality, integrity, and availability of user data. This document provides guidelines for security functions and requirements cloud OSs should possess to respond to security risks and threats. Adherence to this report's guidelines will help establish secure and reliable cloud computing services for the CSC and anyone involved in the design and development of cloud OSs.

7. Security Threats of Cloud OSs

The utilization and management modes of computing resources in cloud computing systems bring new risks and threats for both administrators and end users.

Risks and threats for administrators include:

- **The virtualization management layer becomes the new high-risk area.** Cloud computing systems enable computing resources for large numbers of users using virtualization technology. Therefore, the virtualization management layer becomes the new high-risk area.
- **Malicious users are difficult to track and isolate.** The on-demand and self-service allocation of resources within a cloud computing system make it much easier for malicious users to launch attacks. Unfortunately, these users are difficult to track and isolate due to dynamically varying resource allocation and network settings.
- **Open interfaces make the cloud computing system vulnerable to external attacks.** Administrators commonly use open interfaces to access the cloud computing system through networks, making the system vulnerable to attacks from external networks.

Risks and threats for end users include:

- **Risks cannot be controlled for data stored in the cloud.** Computing resources and data are retained and managed entirely by cloud service providers. The risks brought by this resource management mode are as follows:
  - Malicious cloud service provider administrators may invade CSC systems illegally.
  - Data security cannot be ensured after the computing resources or storage space is released.
  - The selection and formulation of laws and regulations used for data processing can be complex.
- **Multi-tenant resource sharing may cause data leakage and lead to attacks.**
- **Resources shared among multiple tenants pose the following security risks:**
  - User data may leak because of inappropriate isolation methods.
  - Users are susceptible to attacks by other malicious users within the same physical environment.
- **Open network interfaces carry security risks.** In a cloud computing environment, users operate and manage computing resources through the internet. The openness of network interfaces brings more security risks.
- **Hardware resource security can be challenging to control.** Since computing resources are allocated and utilized through virtualization technology, users have limited visibility and control of the original hardware resources which are actually in use.

8. Security Requirement Architecture of Cloud OSs

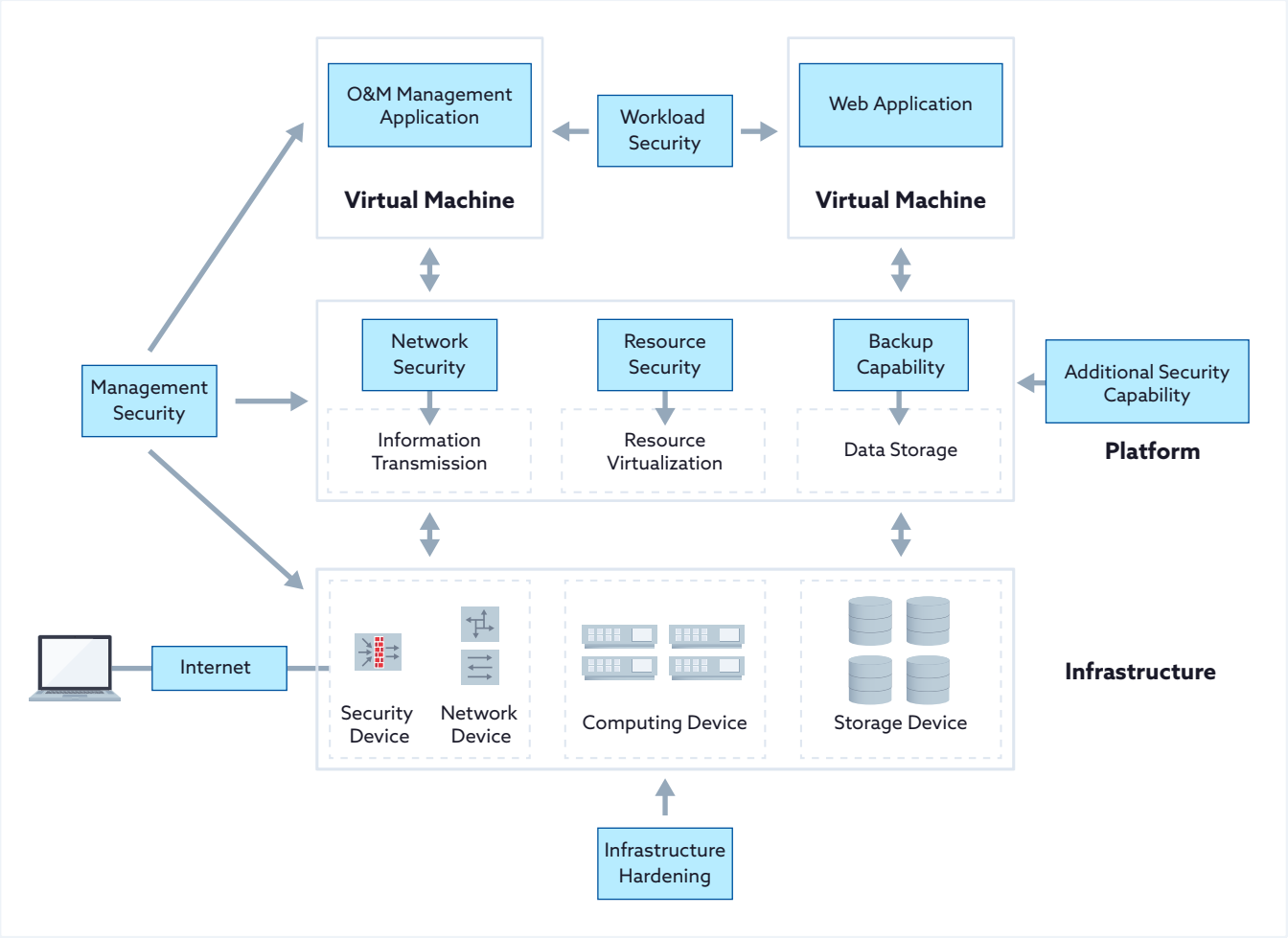

Figure 1: Cloud OS security requirement architecture

In response to the aforementioned threats faced by the cloud OS, this section lists and describes technical requirements for the cloud OS's security assurance. The cloud OS security requirement architecture is illustrated in Figure 1.

- **Infrastructure hardening** describes the necessary capabilities that cloud computing infrastructure should have to maintain a secure and reliable foundation for cloud OS (including host OS, web, and database).
- **Network security** characterizes the required capacity that cloud OS should possess to protect the communication network in cloud computing.
- **Virtualization security** outlines the necessary capabilities that cloud OS should include when virtualization technology is used.
- **Workload security** expresses the necessary capabilities that cloud OS should feature to help cloud customers protect the workloads they deploy or operate in a cloud system.

- **Management security** details the security requirements of the management module in the cloud OS.
- **Backup capability** specifies the means cloud OSs should have to protect data availability for tenants and systems.
- **Additional security** capability defines other functions that cloud OSs should employ to enhance security abilities.

The structure of this specification is illustrated in Figure 2 below, with all these security requirements factors.

9. Infrastructure Hardening

The infrastructure for cloud OS is the physical host on which cloud OS runs. Infrastructure security is critical, as it guarantees a stable and trustworthy environment for cloud OS functionality. Hence, infrastructure security should be highly valued. Infrastructure security directly impacts the host OS, host database, and host web service components, and security measures should satisfy the following requirements.

9.1 OS Hardening

The operating system on the physical host is one of the most basic and important components in cloud computing systems and has a significant impact on cloud OS. Therefore, the host OS must be hardened.

Security technology requirements include:

1. Basic security configurations are required, which include:
   - Unnecessary or unused service components and communication ports should be kept closed to reduce the potential attack surface.
   - Common services, such as secure shell (SSH), should be hardened according to best practices.
   - Kernel parameters should be modified to enhance OS security according to best practices, such as disabling IP forwarding, system responses to broadcast requests and internet control message protocol (ICMP) redirection/forwarding functions.
   - Account and password security should be enhanced by enabling password complexity checks, configuring password validity, and limiting unsuccessful login attempts.
   - Files permission should be minimized (per the principle of least privilege).
   - System access should be restricted, including the prevention of the remote login of user root and the avoidance of installing and running processes using the root account.
2. The logging function should be enabled to record the key operation of the OS. The logging function should be able to connect to a remote log server for centralized log management.
3. Trusted boot and trusted measurements for host OS should be implemented to guarantee the dependable operating environment for cloud OS.

9.2 Database Hardening

Cloud OS can use database functions. As a result, hardening is required.

Security technology requirements include:

1. Database identity and access functions should be hardened by limiting unsuccessful login attempts and utilizing SSL for remote access.
2. Strong passwords: the password must contain at least eight characters and should follow a strong password policy that requires users to enlist two of the following four variables in password creation (uppercase letter/s, lowercase letter/s, special character/s, and numeral/s).
3. Accounts and passwords should be saved in a hash with salt using a secure algorithm.
4. The operation permission of the files/data in the database should be carefully granted according to the principle of least privilege.
5. The database's logging function should be enabled to record the key state/parameter changes and the key operation of administrators and users, such as login, logout, and data operations.

9.3 Web Hardening

Security technology requirements should protect web interfaces offered natively by the cloud OS and the underlying physical server.

Security technology requirements include:

1. Input validation should be carried out as a control against SQL injection or cross-site scripting (XSS).
2. Strong ciphers and/or hashes should protect sensitive data.
3. Validate user accounts—ensuring that identity is properly authenticated—and capture detailed audit trails for access information. This validation will harden the web application against attacks such as cross-site request forgery (CSRF).
4. Hypertext transfer protocol over secure socket layer (HTTPS) should be used to protect the connection between the web server and the client.
5. Each user type should be allowed specific permissions to prevent unauthorized access to the data beyond their permissions via a uniform resource locator (URL).

10. Network Security

Network security applies to the security of devices and management activities related to the devices, applications/services, and end users. Network security also encompasses the protection of information being transferred across the networks. Network security protocols in the cloud OS should satisfy the following requirements.

10.1 Network Plane Isolation

Security technology requirements include:

1. The communication network planes should be divided into independent networks such as the management network, tenant network, and storage network (as follows):
2. Management network: The management network works as the communication plane for cloud computing system management, service deployment, and system loading.
3. Tenant network: The tenant network provides service channels for users and works as the communication plane of VMs to provide services. Virtual machines of the tenant can connect to the tenant networks to communicate with one another.
4. Storage network: The storage network works as the communication plane for storage over block storage devices and provides storage resources for VMs.
5. These networks are isolated from each other.

Illustrative explanation

A network plane isolation example is presented in Figure 2 below.

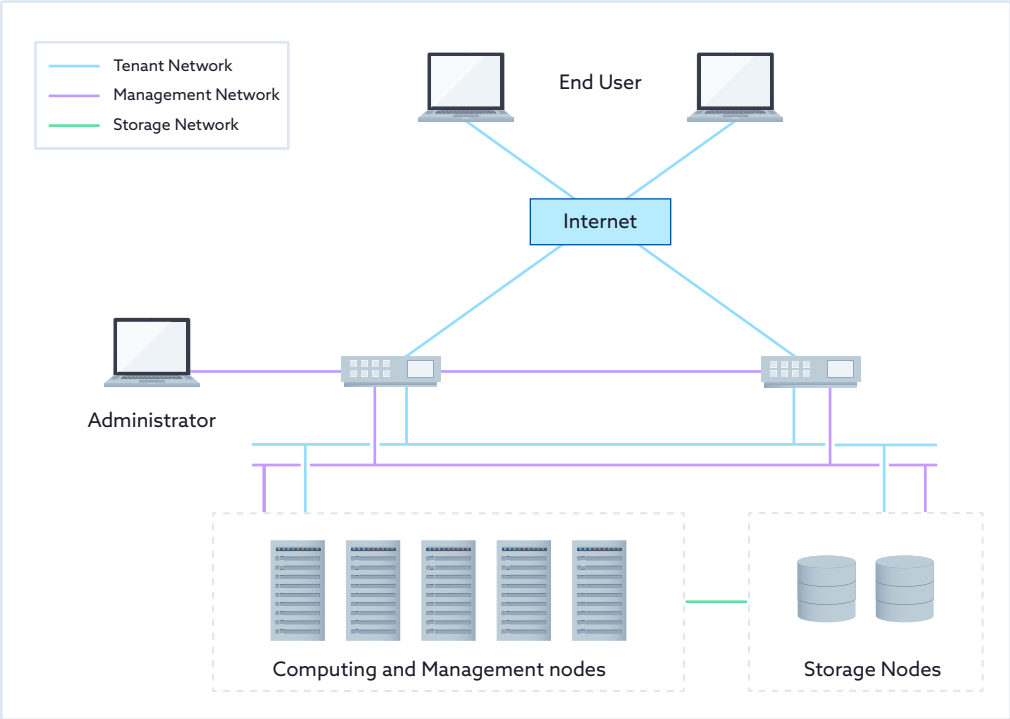

Figure 2: Network plane isolation

10.2 VLAN Isolation

Security technology requirements include:

1. A virtual network bridge should be supported to serve as a virtual switch, and the VLAN tagging function should be provided to isolate VLANs for VM security.
2. A virtual bridge should connect all VMs running on the same physical server.
3. These VMs can tag data frames using VLAN tagging.

Illustrative explanation

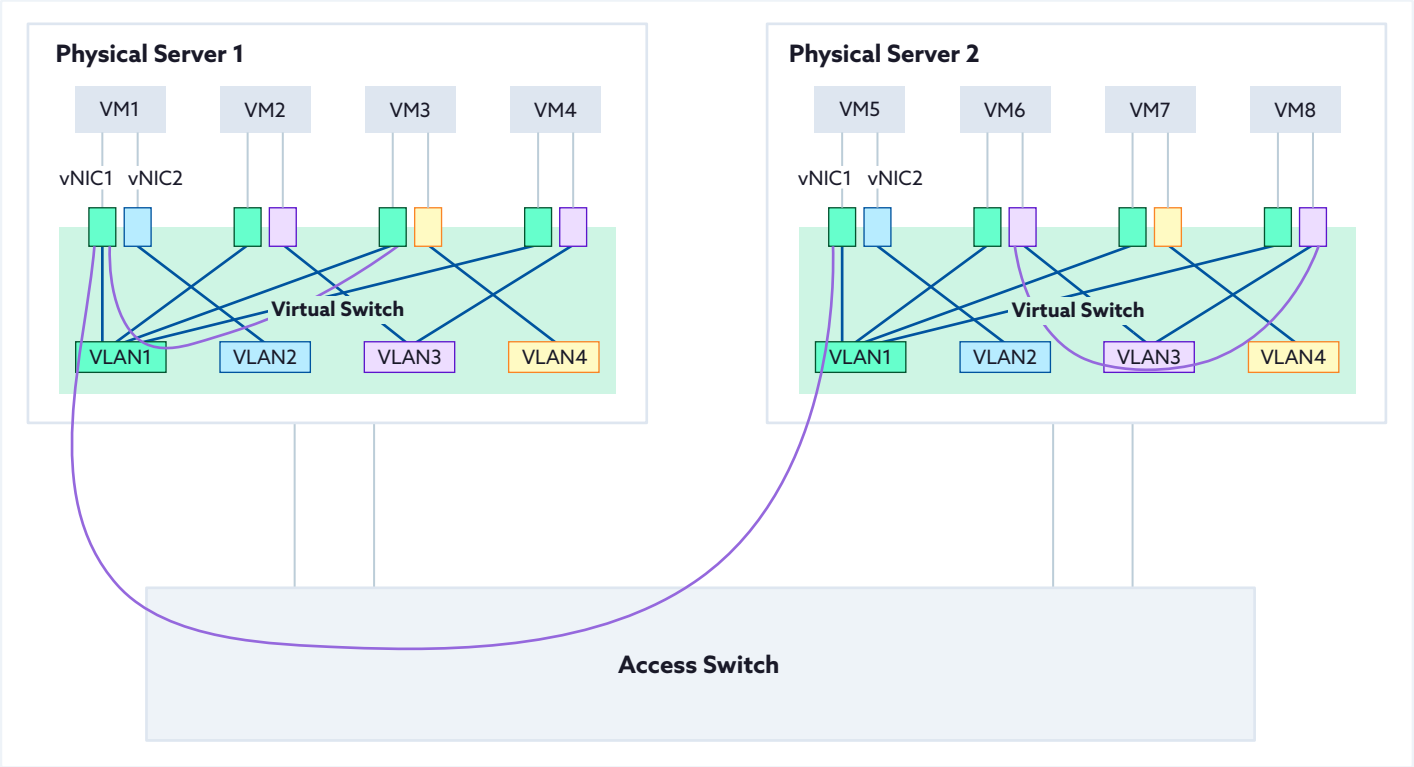

Figure 3 An example of VLAN isolation

A VLAN isolation example is shown in Figure 3. The VMs distributed on different physical servers can be deployed on the same LAN using VLAN technology. The VMs on a server's VLAN communicate with each other through the virtual switch. In contrast, the VMs on a VLAN of different servers communicate through the physical switch—ensuring that VMs of different LANs are isolated and forbidden to exchange data.

10.3 Security Groups

Security groups should be utilized to isolate different VMs based on different tenants and their varying security requirements and to satisfy security assurance for these VMs.

Security technology requirements should include:

1. Security group function should be supported, allowing admins to create security groups based on VM security requirements.
2. Admins should be able to add VMs to security groups when creating VMs.
3. Virtual machines in the same security group should be distributed on different physical servers.
4. The VMs in a security group should communicate with each other, while those in different security groups are (by default) not allowed to communicate with each other. However, the VMs in varying security groups can be configured to communicate with each other.

Illustrative explanation

An example of security groups in multi-tenants is shown in Figure 4.

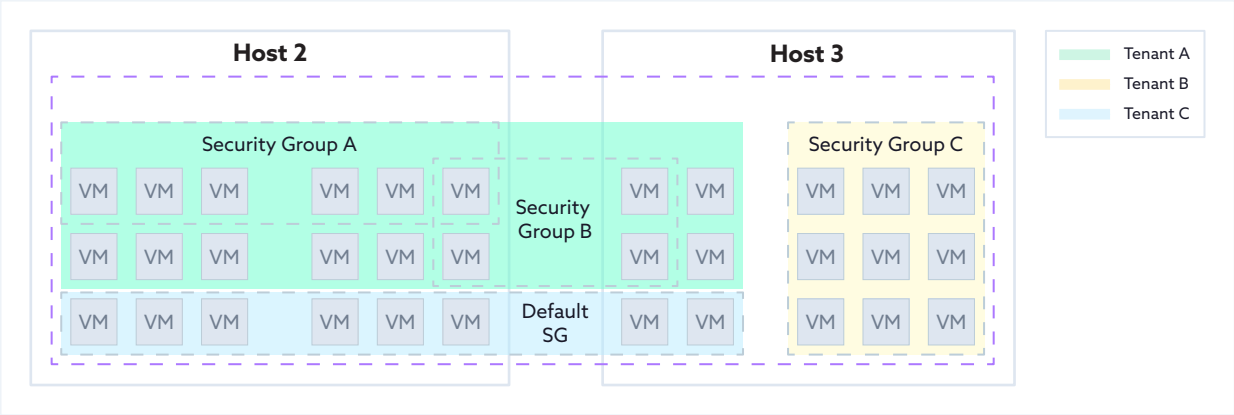

Figure 4: Security groups in multi-tenants

10.4 VPC Supporting

Virtual private cloud (VPC) can create a completely isolated network environment for tenants. Virtual machines in a VPC can't be accessed from the outside except for dedicated network configurations.

Security technology requirements include:

1. Virtual private cloud should be supported to protect the virtual resources of tenants better.

10.5 IP/MAC Address Spoofing

Security technology requirements include:

1. Internet protocol (IP) address or MAC address spoofing prevention should be supported by IP-MAC address binding techniques, thereby enhancing network security of user VMs.

10.6 Port Access Control

Security technology requirements include:

1. The system service port can be set to listen to the service message on only the specified communication plane.
2. The system service ports can be bound to specified IP addresses to receive service messages from known/trusted sources.

10.7 DHCP Quarantine

Security technology requirements include:

1. Dynamic host configuration protocol (DHCP) quarantine should be supported to block users from unintentionally or maliciously enabling the DHCP server service for a VM, ensuring standard VM IP address assignment.

10.8 Anti-Dos/DDoS Attack

Security technology requirements include:

1. Cloud OS should have defensive capabilities against denial-of-service (Dos/DDoS) attacks, such as limiting the connection tracks to the virtual network ports of a VM running on it.

10.9 Micro-Segmentation

Micro-segmentation can provide more granular access control, as it is dependent on different attributes and tags rather than just subnet-level policy. It can provide better control capabilities for cloud systems.

Security technology requirements include:

1. Cloud OS should provide access control between VMs depending on the attributes or tags of different VMs.
2. Visualization of connection between VMs in cloud systems should be provided.

11. Virtualization Security

Virtualization security ensures virtualized objects can share a common set of infrastructure resources while maintaining full isolation. Data theft and malicious attacks can be prevented by utilizing hypervisors to isolate VMs running on the same host. Users can use VMs to access resources only belonging to their own VMs, such as hardware and software resources, and data. Figure 5 shows an example of VM resource isolation.

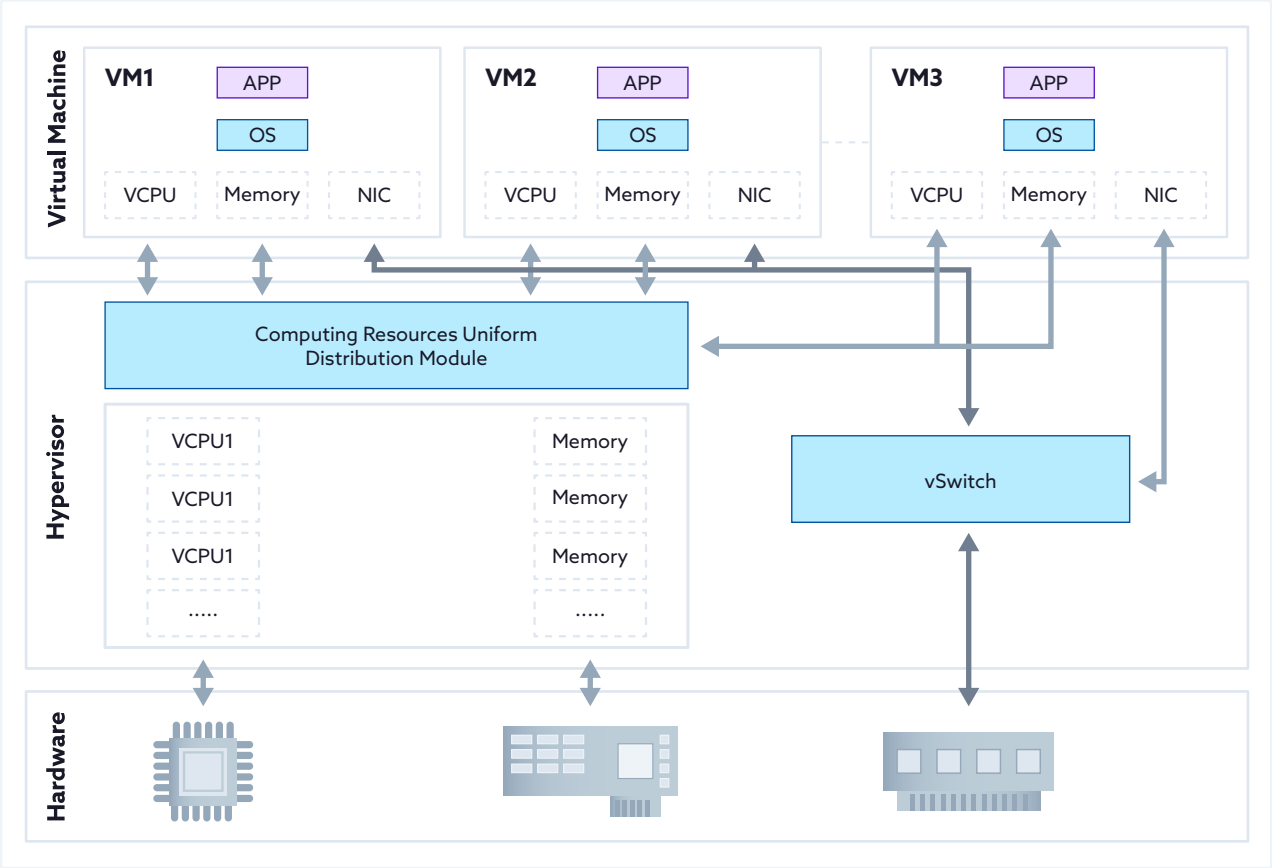

Figure 5: VM resource isolation

11.1 vCPU Scheduling Isolation

Security technology requirements include:

1. The guest OS of VMs should be prevented from executing all privileged instructions.
2. The OS and application should be isolated.

Illustrative explanation

For example: in x86 architecture servers, four privilege levels are offered from Ring 0 (most privileged) to Ring 3 (least privileged). Ring 0 is used for the OS kernel, Ring 1 and Ring 2 for OS services, and Ring 3 for applications. The privilege levels separately restrict the commands that can be run, and the hypervisor schedules the vCPU context switch.

11.2 Virtual Memory Isolation

Security technology requirements include:

1. Virtual machines should have the ability to use memory virtualization technology to virtualize physical memory and isolate virtual memory.

Illustrative explanation

Physical addresses can be utilized in virtual memory isolation based on an existing mapping between virtual addresses and clients' machine addresses. Before sending the machine address to the physical server, the OS needs to translate the virtual address into the physical address, while the OS hypervisor should translate the client's physical address into a machine address.

11.3 Internal Network Isolation

Security technology requirements include:

1. The VFR function should be provided.
2. Each guest VM (GVM) has one or more virtual interfaces logically associated with the VFR.
3. The virtual firewall should allow workload, applications, VM, and other characteristics to define security policies.

Illustrative explanation

For example, data packets sent from a VM first arrive at domain 0. Domain 0 filters the data packets, checks the integrity of the data packets, adds or deletes rules, adds certificates, and sends the data packets to the destination VM. The destination VM then checks the certificates to determine whether to accept the data packets.

11.4 Disk I/O Isolation

Security technology requirements include:

1. Storage space isolation of multiple VMs should be implemented to ensure that the VMs access only the appointed space.

Illustrative explanation

An example implementation is to divide the device driver model into three parts: front-end driver, back-end driver, and native driver. The front-end driver runs in the guest OS while the latter two run in the host OS. The front-end driver transfers input-output device (I/O) requests from the guest OS to the host OS's back-end driver. The back-end driver parses the requests, maps them to the physical devices, and sends them to the corresponding device driver to control hardware I/O operations. Through the interception and processing of all I/O activities, the system realizes storage space isolation to ensure VMs can only access their self-appointed space.

12 Workload Security

12.1 VM Security

Security technology requirements include:

1. The integrity of VM images should be verified and protected before the VM is deployed.
2. When tenants log in their VMs, access control should be provided. Password and public/private key pair authentication modes should be supported.
3. Anti-virus software should be deployed in each VM to prevent virus invasion.
4. Intrusion detection and prevention system (IDPS) should be provided to avoid network invasion to VMs deployed in cloud systems.
5. The system should provide VM monitoring functionality to realize VM-level activity, including:
   - Resource utilization
   - Network I/O flow rate
   - Disk I/O rate
6. The system should implement alarm functionality when a particular monitored metric exceeds the setting threshold. Threshold values can be set differently in different conditions.

12.2 Application Security

1. A web application firewall (WAF) module should be provided.
2. A web tamper protection (WTP) module should be employed.

12.3 Data Security

12.3.1 Data Transmission Security

Security technology requirements include:

1. In untrusted network environments, sensitive data should be transmitted in the channel using the recommended secure version of transport layer security (TLS).

12.3.2 Data Storage Security

Security technology requirements include:

1. Data should be stored and protected utilizing backup technology and mechanisms (see Section 14 for more detail).
2. Sensitive data should be cryptographic and stored in the system via a secure encryption algorithm if needed.

12.3.3 Data Processing Security

Security technology requirements include:

1. The system should provide access control for each storage volume. Only users who get access permission can access a specific volume.

12.3.4 Residual Data Protection

The following requirements should be satisfied to prevent data leakage when the system reclaims resources.

Security technology requirements include:

1. By default, the system should support all the physically usable bits of logical volumes before they are formatted to ensure data security.
2. Documented disk recycle, or disposal procedures should be supported.
3. It should be guaranteed that all residual data in storage resources will be cleaned before resources are reallocated.

12.3.5 Tenant Database Security

Databases built by cloud service customers on their VM should also be protected as data stored in databases, as this is very important for the cloud service customers' workload.

Security technology requirements include:

1. The system should provide a logging audit function to help cloud service customers analyze access and operations occurring in their database.

12.4 Encryption Capability

Encryption is crucial in the IT system. It can protect sensitive information and configuration data in the VM of the cloud service customer. In addition to utilizing a self-built encryption module, cloud OS should provide a robust and efficient encryption capability for cloud service customers to efficiently and securely encrypt their valuable data.

Security technology requirements include:

1. The system should provide encryption capability to cloud service customers via API.
2. System-provided encryption algorithms should be secure and designed under best practices and related standards.
3. API-provided encryption capability should be implemented and realized by specific hardware rather than software-based encryption.

13. Management Security

Management security maintains the regular operation of O&M management systems. Furthermore, it protects the management information transferred in cloud computing systems while minimizing the potentially harmful impact of malicious administrators.

Management security in the cloud OS should satisfy the following requirements.

13.1 Identity Security

13.1.1 Identity Management

Security technology requirements include:

1. Role-based identity and access control should be supported to provide accurate and flexible management.
2. The system should feature the capacity to set admin account privileges to reduce admin role power and ensure orderly system maintenance.
3. Time-bounded account access should be provided. This type of access could be used for third-party engagements for application deployments over a few days to several weeks or months. Administrators should be able to define start and end dates on such accounts.

13.1.2 Account and Password Security

Account and password management tools are essential for securing the system for both cloud administrators and cloud consumers. The following requirements should be satisfied to support the secure management of accounts and passwords.

Security technology requirements include:

1. The system should support the configuration of a password strength policy.
2. Passwords should be stored after a hashing-plus-salting procedure.
3. Weak password verification should be supported to prevent weak character combinations. A weak combination of dictionaries' customization should be supported.
4. According to organizational policies, password recycling should be prevented based on specific thresholds.
5. The system should remind users to change their passwords on the first use within a particular period.

13.2 Access Control Management

Security technology requirements include:

1. Portal users' access control should be supported so that functions, such as rights- and domain-based management, can be utilized to ensure orderly system maintenance.
2. The administrator account should support multi-factor authentication, such as password and mobile prompts.
3. Administrators' and users' portal access should utilize HTTPS and its information transmission channel, which should be protected via the recommended secure version TLS protocol.
4. Service API calls must be authenticated, and the authentication session should have a validity period.
5. If the connection is initiated from an unknown source, this source's access control must be enforced.
6. The limitation of continuous erroneous login attempts should be provided to prevent brute-force cracking. If a user enters inaccurate password combinations a specific number of consecutive times, the account should be locked for a predefined period.

13.3 Key Management

Key management refers to the oversight of cryptographic key operations and technologies to ensure data is protected at rest, in transit, and in use. These key operations include key generation, storage, use, destruction, and replacement. Key management in the cloud OS should satisfy the following requirements.

Security technology requirements include:

1. The system should provide key management systems (KMS) for CSC to manage their key lifecycle or provide an interface for CSC to implement a third party KMS in the system. Key management systems and underlying support hardware should comply with related standards in the CSC's region or country.
2. The system should centrally manage the centralized management of certificates issued by the cloud system and third parties.
3. An automatic update of tenant keys should be supported.
4. Logs must support tracking key management operations, including the generation, distribution, storage, use and/or destruction, and recovery of key information. No sensitive data should be logged.
5. Secure methods should be selected and used for storing keys according to their systemic importance.
6. All keys need protection against modification, while secret and private keys also need protection against unauthorized disclosure.
7. Encryption keys must be generated using a true random number generator (TRNG).
8. Data encryption keys (DEK) should be rotated periodically.
9. Hardware security modules like HSM should protect some of the most important keys, such as the tenant's root key.

13.4 Log Management

Security technology requirements include:

1. The system should support operation logs that record the operations performed by O&M engineers. These logs should contain sufficient information for audit purposes.
   - The operation logs should feature the operator name, operation type, client IP address, operation time, and operation result to promptly locate malicious operations. Operation logs can also serve as non-repudiation evidence.
2. The system should support run logs that record the running status of each node.
   - The run logs should contain log level, thread name, and running information. Operations and maintenance engineers can understand and analyze the system's running status by viewing the run logs to detect and handle abnormalities.
3. The system should support black box logs that record location information about serious system faults. These logs are used to locate and handle severe system faults.
4. Logs can be written or transmitted in a standardized manner/format.
5. Logs can be sent to an external log manager.
6. Logs can be retained for at least a default time, the value of which can be configured by the administrator. Additionally, different kinds of logs can be set with varying values of default time by the administrator.
7. Sensitive information should not be recorded in logs.

14 Backup & Recovery Capability

14.1 Cloud Service Customer Data Backup & Recovery

The following requirements for CSC data backup should be satisfied.

Security technology requirements include:

1. The system should support one or more copies of backup to protect the stored system data.
2. The system should support the utilization of RAID (redundant array of independent disks) technology to guarantee high availability and provide the recovery capability of data stored in the system.
3. High availability (HA) of VMs that can quickly switch from a VM to a backup server when its located production server fails should be supported.

14.2 System Backup & Recovery

Cloud OS configuration data and databases should be protected through backup to bolster cloud OS service security. The following requirements for system data backup should be satisfied.

Security technology requirements include:

1. Local backup of system data should be supported and implemented automatically and periodically.
2. Remote backup of system data should be bolstered to store the backup copies on a third backup server.
3. The system should support hot failover, a scenario when the production server fails and the system can switch to a backup server and recover quickly without data loss.

15. Additional Security Capability

Additional security functions of the cloud OS can enhance system's total security performance. Accordingly, the following functions should be supported by the cloud OS.

Security technology requirements include:

1. The system should support the utilization and integration of third-party security software to enhance the security capability of the cloud OS through standardized and documented interfaces (e.g., APIs, and deep packet inspection (DPI) interface provided by the OS that can interface with DPI software to provide DPI capability for cloud OS).
2. The system should support functions for estimating and evaluating the security deployment condition of cloud computing systems. The function should provide a unified, visual, multi-dimensional security review for the CSC, allowing the CSC to check the cloud environment security conditions—including whether the environment is appropriately configured, if current security measures are sufficient, and if the system contains active and passive safety measures.
3. The system should support security situation awareness (SSA) functionality to help the CSC understand and analyze the OS and whole cloud system's security situation. This security feature utilizes all data and events/logs collected from every system component, analyzes each previous security incident, and presents this data in a centralized and comprehensive way. This process allows the CSC to better understand these security incidents and anticipate possible future issues.
4. The system should support weakness management functionality that can:
   - Scan for vulnerabilities in systems (including web/database/OS).
   - Scan for incorrect configuration weakness.
   - Scan for weak passwords.
   - Evaluate the severity and impact of detected weaknesses.
   - Report corresponding alerts in real-time.
5. The system should provide CBH to enhance the O&M access control and operation audit.