

Alibaba Cloud Apsara Stack Enterprise

Security Whitepaper

Version: 0818..

Issue: 20180831

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.









1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified,

reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

- 6.** Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Note: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other contents.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	It is used for commands.	Run the <code>cd /d C:/windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand slave}</code>

Contents

Legal disclaimer	1
Generic conventions	1
1 Introduction to the security white paper	1
2 Sharing of security responsibilities	2
2.1 Security responsibilities of Alibaba Cloud.....	2
2.2 Security responsibilities of users.....	3
3 Security compliance and privacy	4
3.1 Security compliance.....	6
3.2 Privacy protection.....	8
4 Apsara Stack security architecture	9
4.1 Cloud platform security architecture.....	9
4.1.1 Infrastructure security.....	9
4.1.1.1 Physical security.....	9
4.1.1.2 Server security.....	10
4.1.1.3 Network device security.....	10
4.1.1.4 Basic network security.....	11
4.1.2 Cloud operating system security.....	11
4.1.2.1 Virtualization security.....	11
4.1.2.2 Security of basic system services.....	13
4.1.2.3 Security of system management and scheduling.....	14
4.1.2.4 Cloud server security.....	14
4.1.3 Network service security.....	15
4.1.3.1 Server Load Balancer.....	15
4.1.3.2 Virtual Private Cloud.....	15
4.1.3.3 Distributed firewall.....	16
4.1.3.4 DDoS attack protection.....	16
4.1.4 ApsaraDB security.....	16
4.1.4.1 Tenant layer isolation.....	16
4.1.4.2 Database accounts.....	17
4.1.4.3 IP address whitelist.....	17
4.1.4.4 VPC isolation.....	17
4.1.5 Cloud storage security.....	17
4.1.5.1 Identity verification.....	17
4.1.5.2 Access control.....	18
4.1.5.3 Tenant layer isolation.....	18
4.1.6 Application security.....	18
4.1.7 Data security.....	19
4.1.7.1 Data security system.....	19
4.1.7.2 Data ownership.....	19
4.1.7.3 Multi-copy redundancy storage.....	19

4.1.7.4 Full-stack encryption.....	19
4.1.7.5 Image management.....	19
4.1.7.6 Residual data cleanup.....	20
4.1.7.7 O&M data security.....	20
4.1.8 Security of cloud product codes.....	20
4.1.9 Security audit.....	22
4.1.10 Security operation service on the cloud platform.....	22
4.2 Cloud user (tenant) security.....	23
4.2.1 Account security.....	23
4.2.2 Host security.....	23
4.2.3 Application security.....	24
4.2.4 Data security.....	24
4.2.5 Security product (Apsara Stack Security).....	25
4.2.6 Security operation service.....	25
4.2.7 Best security practices.....	25
5 Apsara Stack product security.....	27
5.1 Account security.....	27
5.1.1 Apsara Stack account.....	27
5.1.2 Super administrator.....	27
5.1.3 Identity credential.....	27
5.2 OAM.....	28
5.2.1 OAM permission model.....	28
5.2.2 OAM authorization.....	28
5.3 Apsara Infrastructure Management Framework permission management (data center management).....	29
5.4 RAM.....	30
5.4.1 RAM user identity types.....	30
5.4.2 Permissions.....	30
5.4.3 Authorization policies.....	31
5.5 Analysis of security risks.....	31
5.6 Design of security features.....	32
5.6.1 Security isolation.....	32
5.6.2 Authentication and authorization.....	33
5.6.2.1 Identity authentication.....	33
5.6.2.2 Authority management.....	34
5.6.2.3 RAM and STS.....	35
5.6.3 Data security.....	35
5.6.3.1 Triplicate technology.....	35
5.6.3.2 ECS disk encryption.....	37
5.6.4 Transfer encryption.....	38
5.6.5 Log auditing.....	38
5.6.6 Other security capabilities.....	38
5.7 Object Storage Service (OSS).....	39
5.7.1 Security Isolation.....	39

5.7.2 Authentication.....	39
5.7.2.1 User Authentication.....	39
5.7.2.2 Resource Access Management.....	40
5.7.2.3 RAM and STS support.....	40
5.7.3 Data Security.....	41
5.7.4 Transmission Encryption.....	41
5.7.4.1 Server-Side Encryption.....	41
5.7.4.2 Client Encryption.....	41
5.7.4.3 KMS Encryption.....	42
5.7.5 Logging Audit.....	42
5.7.6 Anti-Leech.....	42
5.8 What is Table Store.....	42
5.8.1 Security Isolation.....	43
5.8.2 Authentication.....	43
5.8.2.1 ID Authentication.....	43
5.8.2.2 RAM and STS Support.....	43
5.8.2.3 VPC Access Control.....	43
5.8.3 Data Security.....	44
5.9 Security Isolation.....	44
5.10 Authentication.....	44
5.11 Data Security.....	46
5.12 Logging audit.....	47
5.13 ApsaraDB for RDS.....	47
5.13.1 Security isolation.....	47
5.13.2 Authentication.....	48
5.13.2.1 Identity authentication.....	48
5.13.2.2 Permission control.....	48
5.13.2.3 RAM and STS support.....	48
5.13.3 Data security.....	49
5.13.4 Transmission encryption.....	49
5.13.4.1 SSL.....	49
5.13.4.2 TDE.....	49
5.13.5 SQL server audit.....	50
5.13.6 IP whitelist.....	50
5.13.7 Software upgrade.....	50
5.13.8 Anti-DDoS protection.....	50
5.14 Tenant isolation.....	51
5.15 Permission control.....	51
5.16 Network isolation.....	52
5.17 Backup and recovery.....	53
5.18 RAM and STS support.....	53
5.19 Software upgrade.....	53
5.20 Data transmission encryption.....	53
5.21 ApsaraDB for MongoDB.....	54

5.22 Security isolation.....	54
5.23 Authentication.....	54
5.23.1 Identity authentication.....	54
5.23.2 Permission control.....	55
5.23.3 RAM and STS support.....	55
5.24 Data security.....	55
5.25 Log audit.....	56
5.26 IP address whitelist.....	56
5.27 Anti-DDoS protection.....	56
5.28 Tenant isolation.....	56
5.29 Access control.....	56
5.30 Network isolation.....	57
5.31 Backup and recovery.....	58
5.32 RAM and STS support.....	58
5.33 Software upgrade.....	58
5.34 Server Load Balancer.....	58
5.34.1 Access control.....	58
5.34.2 HTTPS listeners.....	59
5.34.3 RAM and STS support.....	59
5.35 Virtual Private Cloud.....	59
5.35.1 Security Isolation.....	59
5.35.2 Access control.....	60
5.35.3 RAM and STS support.....	60
5.36 Log Service.....	60
5.36.1 Security isolation.....	60
5.36.2 Authentication.....	61
5.36.3 Data security.....	61
5.36.4 Transmission security.....	62
5.36.5 Service monitoring.....	63
5.37 Key Management Service (KMS).....	63
5.37.1 Security risk analysis.....	63
5.37.2 Security functions.....	64
5.37.3 Security isolation.....	64
5.37.4 Authentication.....	64
5.37.4.1 Identity verification.....	64
5.37.4.2 Permission control.....	64
5.37.4.3 RAM and STS support.....	65
5.37.5 Data security.....	65
5.37.6 Encrypted transmission.....	65
5.37.7 Log auditing.....	65
5.38 Security Isolation.....	65
5.39 User Authentication.....	66
5.40 Permission control.....	67
5.41 Account Security.....	68

5.42 Business Security.....	69
5.43 Data Security.....	70
6 Apsara Stack Security.....	71
6.1 Apsara Stack Security Basic Edition.....	71
6.2 Apsara Stack Security Advanced Edition.....	73

1 Introduction to the security white paper

Data security and user privacy are top priorities of Apsara Stack. We are committed to providing a public, open, and secure Apsara Stack cloud computing service platform. With technical innovation, Apsara Stack is constantly improving its computing capability and achieving greater cost advantages to turn cloud computing into cutting-edge infrastructure in its true sense.

Apsara Stack is designed to provide users with stable, reliable, secure, and well-regulated cloud computing infrastructure services and protect their systems, and availability, confidentiality, and integrity of data.

This white paper introduces the Apsara Stack security system in the following parts:

- Sharing of security responsibilities
- Security compliance and privacy
- Security of the Apsara Stack platform architecture
- Security features provided by Apsara Stack products
- Security services provided by Apsara Stack Security

This white paper also provides the best practices for secure use of Apsara Stack products and Apsara Stack Security, which helps you make better use of the Apsara Stack platform and get an insight into the overall security environment.

2 Sharing of security responsibilities

Alibaba Cloud and users share security responsibilities for Apsara Stack-based user applications. Alibaba Cloud guarantees the security of the Apsara Stack platform architecture, and users guarantee the running of the Apsara Stack platform and the security of application systems built based on the Apsara Stack platform.

Alibaba Cloud

Alibaba Cloud is responsible for the security of the Apsara distributed cloud operating system of Apsara Stack and various cloud products running on the operating system, which provides users with an Apsara Stack platform featuring high availability and security. By leveraging Alibaba Group's years of expertise in anti-attack technologies, Apsara Stack provides users with Apsara Stack Security to further protect their Apsara Stack environments.

Users

Users must configure and use the Apsara Stack platform and cloud products such as ECS and RDS instances, and build their own applications based on such cloud products in a secure and controllable manner. In addition, users can use products of Apsara Stack Security to protect their Apsara Stack environments.

2.1 Security responsibilities of Alibaba Cloud

Alibaba Cloud is responsible for the security of distributed cloud operating systems and cloud products, and provides users with the technical measures required to protect the Apsara Stack platform, cloud applications, and data.

- Protects the security of the Apsara Stack platform architecture.
- Provides the security services and technologies that promptly detect and fix security vulnerabilities of the Apsara Stack platform without affecting the business availability.
- Provides services to help users cooperate with an independent third-party security supervision and audit institution to audit and evaluate the security compliance of Apsara Stack.
- Provides users with technical measures to protect cloud information systems.
- Provides users with security audit measures.
- Provides users with data encryption measures.
- Provides users with Apsara Stack Security services.

2.2 Security responsibilities of users

Users build their own cloud applications based on the Apsara Stack platform provided by Alibaba Cloud, and protect their own Apsara Stack environments by using the security features of Apsara Stack products and services and products of Apsara Stack Security.

Users must properly manage their Apsara Stack accounts, grant the minimum permissions required to each O&M administrator, and implement the separation of duties by means of group authorization. In addition, users must use the operation audit service to record the operations performed in the console and API call logs.

Users have full control of the ECS and VPC instances provided by Apsara Stack, and are responsible for managing these instances and performing security configurations. For example, users must reinforce the rented ECS operating system, upgrade patches, and configure security group firewall in time for network access control.

For other Apsara Stack services, such as RDS, users must manage the service accounts and authorization, and use the security features provided by such services, for example, configuring the source IP address whitelist for RDS.

3 Security compliance and privacy

The security process of Alibaba Cloud has been recognized by authorities inside and outside China. By leveraging Alibaba Group's years of expertise in defense against Internet security threats, Alibaba Cloud provides security protection for the Apsara Stack platform, and integrates multiple compliance standards into the internal control and product design of the cloud platform. In addition, Alibaba Cloud has participated in the development of standards for various cloud platforms, contributed best practices, and passed evaluation and verification by an independent third party. Certified by more than 10 agencies inside and outside China, Alibaba Cloud is the cloud service provider with the most complete range of certifications in Asia.

Alibaba Cloud has been awarded certifications listed in [Table 3-1: Certifications awarded to Alibaba Cloud](#).

Table 3-1: Certifications awarded to Alibaba Cloud

Certification	Description
ISO 27001	The international Information Security Management System (ISMS) Certification. It certifies Alibaba Cloud for fully performing its security duties in regard to data security, network security, communication security, and operation security.
CSA STAR	The international Cloud Security Management System Certification. The certification organization awarded the first cloud security gold medal to Alibaba Cloud.
ISO 20000	The IT Service Management System Certification. This certifies that Alibaba Cloud has established and strictly implemented a standard service process. The standardized cloud platform services improve efficiency and reduce the overall IT risk.
ISO 22301	The Business Continuity Management System Certification. This certifies that Alibaba Cloud meets the requirements for business continuity planning, disaster recovery, and regular drills to enhance the stability of the cloud platform.

Certification	Description
Classified protection (Class 4)	Alibaba Cloud's Finance Cloud is the first cloud platform in China that passed the Class 4 certification of classified cloud computing protection, which means that Finance Cloud is steadily becoming the key information infrastructure in China.
Cloud service network security audit by the party and government department of Office of the Central Leading Group for Cyberspace Affairs	Alibaba Cloud is the only cloud service provider that passed the audit for enhanced level (more than 500 checkpoints) among the first community cloud service providers in China that passed the security audit of the Central Leading Group for Cyberspace Affairs.
Cloud service capability standard test by Ministry of Industry and Information Technology (MIIT)	CNAS certification for cloud products is the only product-level classified certification based on national standards.
Payment Card Industry Data Security Standard (PCI DSS)	PCI DSS focuses on managing and controlling the lifecycle of payment card information within an organization, including the generation/entry, transfer, storage, processing, and destruction.
MTCS T3	The highest-level certification in Singapore for security of cloud service providers. This allows Alibaba Cloud to get involved in Singapore government projects.
Service Organization Control (SOC) audit certification	Alibaba Cloud has passed the TYPE I and TYPE II of SOC1 and SOC2, and SOC3.
TRUSTe	Alibaba Cloud international site has been certified by US corporate privacy standards. This marks the compliance of Alibaba Cloud in collecting, using, managing, and destroying personal information.
Health Insurance Portability and Accountability Act (HIPAA)	Alibaba Cloud complies with HIPAA's business associate agreement (BAA) to meet customer needs, and with US HIPAA to protect the privacy and security of health information.
MPAA	Alibaba Cloud complies with the best practices guidelines of Motion Picture Association of America (MPAA).

Certification	Description
PDPA	Alibaba Cloud complies with personal information protection requirements in Singapore.
Trusted Cloud membership	Alibaba Cloud is a member of Trusted Cloud promoted by German Federal Ministry of Economics and Energy.
Founding member of SCOPE Cloud Code	As a founding member, Alibaba Cloud is actively engaged in SCOPE EUROPE's efforts to develop cloud code and standards for implementation of GDPR.
Proposer of "Data Protection Initiative"	This is the first "Data Protection Initiative" launched for cloud computing service providers in China, which defines data ownership, and the responsibilities and obligations of Alibaba Cloud.
Released "Alibaba Cloud Data Security White Paper"	Alibaba Cloud fulfills its commitment to data security with sound data security management and advanced technologies.

3.1 Security compliance

Alibaba Cloud keeps improving its management and processes based on relevant standards and best practices in the industry, and gets certified in a series of standard certifications, third-party audits, and self-assessment, aiming to better demonstrate its compliance practices to users.

Given compliance requirements from different perspectives and for different industries and regions, the overall compliance architecture of Alibaba Cloud is divided into the following types:

Management system compliance

These compliance certifications demonstrate the mature management of Alibaba Cloud and the best industry practices that Alibaba Cloud complies with.

- ISO 27001: Information security management system
- ISO 20000: IT service management system
- ISO 22301: Business continuity management system
- CSA STAR: Maturity model of cloud service security
- Classified protection (Class 4)
- CNAS test for cloud computing standards in China

Systematized compliance reports

These compliance certifications demonstrate the integrity and effectiveness of Alibaba Cloud platform's management and control, including the continuous effectiveness of system control, accuracy of separation of duties, and completeness of O&M audit.

- Payment Card Industry Data Security Standard (PCI DSS)
- Best practices guidelines of Motion Picture Association of America (MPAA)
- TRUSTe corporate privacy certification
- SOC 1/2 TYPE II: The Service Organization Control (SOC) reports are a series of audit reports from independent third parties to indicate the continuous effectiveness of Alibaba Cloud's key compliance control and objectives. These reports aim to help users and their auditors learn the control measures behind operation and compliance. The SOC reports that Alibaba Cloud has are categorized into the following types:
 - SOC 1 TYPE II: Internal control report on financial reporting
 - SOC 2 TYPE II: Report on security, availability, and confidentiality
 - SOC 3: Report on security, availability, and confidentiality

Legal compliance

Compliance with local laws and regulations is the primary condition for cloud services to be implemented in different regions. However, legal compliance cannot be reflected in the form of certificates or audit reports because of its unique nature.

- Health Insurance Portability and Accountability Act (HIPAA): Alibaba Cloud complies with HIPAA's business associate agreement (BAA) to meet customer needs, and with US HIPAA to protect the privacy and security of health information.
- GDPR: Alibaba Cloud strives to provide supports for users and partners while complying with the EU data protection laws.

Others

Some compliance certifications cannot be demonstrated in the preceding three forms.

Alibaba Cloud strives to assist regulators in different regions in establishing and improving standards by sharing its best practices.

Multi-Tier Cloud Security (MTCS): MTCS is the cloud security standard proposed by the Info-communications Development Authority of Singapore and released by Singapore Standards,

Productivity and Innovation Board. MTCS security certification has three levels. Alibaba Cloud has been awarded Level-3 certification, the highest security level.

3.2 Privacy protection

Personal information processing principles of Alibaba Cloud: Users own and control all the personal information provided for Alibaba Cloud.

Users provide their personal information for Alibaba Cloud out of trust when using Alibaba Cloud services. Alibaba Cloud is committed to protecting users' personal information and guarantees that such information is used only for the intended purposes agreed by users. Alibaba Cloud's privacy policy is completely open to the public. For more information, see the privacy policy published on the official website. At the same time, Alibaba Cloud takes various technical measures to make sure that users' personal information is used only for Alibaba Cloud business.

Alibaba Cloud provides comprehensive compliance information in Trust Center in a hope that users can better understand Alibaba Cloud's compliance practices, and that users trust Alibaba Cloud as always while gaining experience in compliance from Alibaba Cloud practices to improve the global compliance capability together with Alibaba Cloud. Alibaba Cloud also works with TrustArc to provide the privacy compliance services for cloud customers.

Again, Alibaba Cloud undertakes that it is committed to protecting the personal information of users worldwide, and complying with applicable laws of countries/regions where Alibaba Cloud's business is operated.

Alibaba Cloud's privacy policies are available on the official website. If you have any questions about privacy, contact us by submitting questions on the Trust Center page.

Alibaba Cloud official privacy policies: <https://www.alibabacloud.com/help/faq-detail/42425.html>

4 Apsara Stack security architecture

Apsara Stack is designed with a multi-layer in-depth security defense system, providing security assurance at the cloud platform layer (including infrastructure, cloud operating system, network service, cloud database, cloud storage, application, big data computing, data, cloud product code , security audit, and cloud platform operation) and at the cloud users (tenants) layer (including accounts, hosts, applications, data, and operations).

4.1 Cloud platform security architecture

4.1.1 Infrastructure security

4.1.1.1 Physical security

The requirements for the physical security of Apsara Stack data centers include, but are not limited to, the following security measures: dual-circuit power supply, access control, video monitoring, fire detection, and hot standby data centers.

Dual-circuit power supply

To guarantee 24/7 non-stop services, each load in the Apsara Stack data center must be connected to two power supplies that support mutual switchover. If one power supply fails, the load is connected to the other power supply.

Access control

Access control must be set for the Apsara Stack data center and the physical devices in the data center. For example, the access control policies must be set for entry/exit of personnel and devices in the data center, and configuration, startup, shutdown, and fault recovery of physical devices.

Video monitoring

A video monitoring system or dedicated persons must monitor the channels or other important locations in the Apsara Stack data center around the clock. For example, the video monitoring system must monitor the entry and exit, and the alarm device must collaborate with the video monitoring system or access control device to effectively monitor the monitoring sites.

Fire detection

The Apsara Stack data center must be equipped with an automatic fire alarm system, including the automatic fire detector, regional alarm, and centralized alarm and controller. The automatic

fire alarm system sends alarm signals by sound, light, or point on the fire location, starts the automatic fire extinguishing device, cuts off the power, and turns off the air conditioners.

Hot standby data centers

When a fault occurs, the faulty unit is automatically replaced by a hot standby unit based on the preset fault recovery plan to achieve automatic fault recovery.

4.1.1.2 Server security

Alibaba Cloud reinforces the security of Apsara Stack physical servers in terms of account security , file permission, system service, host intrusion detection, and other aspects.

Account security

Sets the security policies for the password length, complexity, and lifecycle of the physical server accounts, deletes accounts with empty passwords, and sets the logon timeout.

File permission

Monitors integrity of important directories to immediately detect intrusions when hackers tamper and write files.

System service

Disables unnecessary system services on the physical servers to reduce attack surfaces on the servers.

Host intrusion detection

Deploys the host intrusion detection system (HIDS) on the servers to detect abnormal processes, ports, and operations.

4.1.1.3 Network device security

Account security

Reinforces the storage encryption of the account password policies and password configuration files for network devices.

- Provides network devices with read-only accounts that can only view configurations to separate accounts from reading and changing configurations.
- Uses the centralized control policy to manage accounts in a centralized manner.
- Uses multi-factor authentication to guarantee the account security for network devices.

Services

Disables services on network devices to reduce attack surfaces on the network devices, and disables features unrelated to the network devices.

Log centralization

Collects and manages logs generated by network devices in a centralized manner.

4.1.1.4 Basic network security

Micro isolation

The Apsara Stack platform adopts security isolation for the management network (OPS), business network, and physical network in the Apsara Stack network environment. The OPS, business, and physical networks are logically isolated from each other by using network access control policies to prevent mutual access. In addition, Apsara Stack takes network control measures to prevent unauthorized devices from connecting to the internal network of the cloud platform and prevent the physical servers of the cloud platform from connecting to external devices.

Anti-IP/MAC/ARP spoofing

IP/MAC/ARP spoofing severely challenges traditional networks. Hackers use IP/MAC/ARP spoofing to disturb the network environment and intercept network secrets. The Apsara Stack platform completely solves the address spoofing problem by using the underlying network technology on the physical server.

The Apsara Stack platform isolates the abnormal protocol access initiated by a server to external targets on the data link layer of the physical server, blocks the MAC/ARP spoofing from the server, and avoids IP spoofing from the server on the network layer of the host.

Network intrusion detection

A network intrusion detection system is deployed on the Apsara Stack platform to detect abnormal operations in the network in real time and send alarm notifications. The network intrusion detection system can detect HTTP intrusions and HTTP vulnerabilities. In addition, the system detects security vulnerabilities of some system services, including but not limited to Redis, MongoDB, and MySQL.

4.1.2 Cloud operating system security

4.1.2.1 Virtualization security

Virtualization lays the foundation for the cloud computing platform, and guarantees isolation between multiple tenants in a cloud computing environment by means of virtualized computing

, storage, and network. Alibaba Cloud virtualization security technology involves basic security features of tenant isolation, hotfix patches, and escape detection to guarantee the security of the virtualization layer of the Apsara Stack platform.

Tenant isolation

The virtualization management layer plays a vital role in tenant isolation. Based on the hardware virtualization technology, virtual machine management allows virtual machines on multiple computing nodes to be isolated from each other at the system layer, preventing unauthorized access to system resources between tenants to guarantee basic computing isolation between computing nodes. Meanwhile, the virtualization management layer provides storage isolation and network isolation.

- **Computing isolation**

The Apsara Stack platform provides various cloud-based computing instances and services, and allows automatic scaling to meet the requirements of applications and users. These computing instances and services provide computing isolation at multiple levels to protect data and guarantee flexible configuration to meet user needs. The key isolation boundaries in computing isolation are between the management system and virtual machines, and between virtual machines, which are directly provided by Hypervisor. The Apsara Stack platform uses a virtualized environment where user instances run as standalone virtual machines and the isolation is enforced with physical processor-level permissions to avoid unauthorized access of a user's virtual machine to physical hosts and the system resources on another user's virtual machine.

- **Storage isolation**

In the basic design of cloud computing virtualization, Alibaba Cloud separates virtual machine-based computing from storage. This separation allows computing and storage to be extended independently, and makes it easier to provide multi-tenant services. At the virtualization layer, Hypervisor uses the separation device driver model to implement I/O virtualization. Hypervisor intercepts and processes all I/O operations of a virtual machine to make sure that the virtual machine can only access the physical disk space allocated to it, thus realizing security isolation of hard disk space between virtual machines. After a user instance server is released, the original disk space is reliably cleared to guarantee the user data security.

- **Network isolation**

To guarantee the network connections of ECS instances, Alibaba Cloud connects virtual machines to the Apsara Stack virtual network. A virtual network is a logical structure built on the physical network structure. Each logical virtual network is isolated from all other virtual networks. This isolation prevents the network traffic from being accessed by another ECS instance during deployment.

Escape detection

A virtual machine escape attack first places the virtual machine controlled by the attacker on the same physical host as one of the target virtual machines. Then, it destroys the isolation boundary to steal sensitive information of the target or perform operations that compromise the functions of the target.

The Apsara Stack virtualization management program uses the advanced virtual machine layout algorithm to prevent virtual machines of malicious users from running on specific physical machines. At the virtualization management software level, Alibaba Cloud also provides reinforcement, attack detection, and hotfix for virtualization management programs to prevent attacks from malicious virtual machines.

Hotfix patches

The Apsara Stack virtualization platform supports the hotfix patch technology, which can fix system defects or vulnerabilities without restarting the system or affecting a user's business.

4.1.2.2 Security of basic system services

Apsara system

- **Apsara Distributed File System security**

Apsara Distributed File System uses the triple-copy technology to store three copies of data in the system. If one of the copies is lost, the system automatically copies another one to make sure that three copies always exist in the system. In addition, according to the security policy, three copies are not stored in the same physical storage medium to guarantee separated storage operations.

All the accesses to Apsara Distributed File System must pass the Capability authentication. Only those with the authorized Capability can communicate with the system to prevent unauthorized access.

Data is stored in Apsara Distributed File System in binary format to prevent information leakage caused by plaintext.

- **Remote Procedure Call security**

Remote Procedure Call uses the specified binary format for communication in the Apsara system. This guarantees transmission efficiency and security, and prevents data from being restored even if the data is hacked by a man-in-the-middle.

- **Job Scheduler security**

Job Scheduler uses a sandbox to isolate programs.

Infrastructure

DDoS attack protection, DNS region transfer, DNS amplification attack protection, NTP amplification attack protection, and other security measures are taken for NTP and DNS services to guarantee security of NTP and DNS servers.

4.1.2.3 Security of system management and scheduling

The management system of the Apsara Stack platform uses Docker containers for deployment. Alibaba Cloud security experts review the security development lifecycle (SDL) of the cloud platform management system, and perform code review, online test, requirement analysis, and threat modeling to guarantee the overall security of the cloud platform management system.

4.1.2.4 Cloud server security

Host operating system

The operating system of the Apsara Stack platform cloud server host uses a reinforced operating system that is customized, modified, and compiled by Alibaba Cloud based on the cloud characteristics. In addition, the security policy and security access of the operating system are greatly reinforced.

Guest operating system

Users have full control over the operating systems of their ECS instances. Alibaba Cloud does not have any permission to access users' instances and operating systems on them. Meanwhile, Alibaba Cloud strongly recommends that users access and operate the operating systems on their ECS instances in a secure way. For example, a user must use the SSH public key and private key pairs and properly keep the private key. (The user must at least use a complex password, which can be set when the user creates the instance.) In addition, the user must use SSHv2, a safer way, for remote logon and use the sudo command to temporarily escalate the permission.

Images

Alibaba Cloud basic images integrate patches for all known high-risk vulnerabilities to keep the ECS instances away from the high-risk status after these instances go online. Alibaba Cloud uses the data check algorithm and one-way hash algorithm to guarantee image integrity and prevent the images from malicious tampering. After detecting a new high-risk vulnerability, users must promptly update their basic images. Moreover, users can upgrade the operating system or fix vulnerabilities of their ECS instances by themselves.

We strongly recommend that users use Alibaba Cloud basic images as the first step for cloud migration without affecting the business deployment.

4.1.3 Network service security

4.1.3.1 Server Load Balancer

Server Load Balancer is a load balancing service that distributes traffic among multiple ECS instances. It can scale up the service capability of an application by distributing traffic, and enhance availability of the application by eliminating single points of failure.

Access control

Server Load Balancer supports access control by the IP address whitelist. After a whitelist of IP addresses listened by Server Load Balancer is added, only specific IP addresses are allowed to access Server Load Balancer.

Certificate management

Server Load Balancer provides centralized certificate management based on HTTPS. Certificates are not required to be uploaded to backend ECS instances. Decryption is performed on Server Load Balancer to reduce the CPU usage of backend ECS instances.

4.1.3.2 Virtual Private Cloud

Virtual Private Cloud (VPC) helps users establish an isolated network environment based on Apsara Stack. It supports the custom IP address range, CIDR block, route table, and gateway. In addition, VPC can be connected to a traditional data center by using leased lines or VPN to build the hybrid cloud.

Security isolation

By using the tunneling technology, VPC isolates networks to the same effect as the traditional VLAN. VPC isolates broadcast domains at the NIC level, thoroughly blocks network communication by VLAN isolation, and classifies different security domains for access control.

Access control

VPC supports flexible access control rules based on the security group firewall.

4.1.3.3 Distributed firewall

The distributed virtual firewall provided by Alibaba Cloud is a security group that provides the status detection and packet filtering features.

A security group is a logical group that consists of instances in the same region with the same security requirements and mutual trust. Security groups are used to set network access control rules for one or more ECS instances. As an important network security isolation measure, security groups are used to divide network security domains on the cloud.

Each instance must belong to at least one security group. Instances in the same security group can communicate with each other between networks. By default, instances in different security groups cannot communicate with each other by using the intranet, but a certain origin security group or CIDR block can be authorized to access a target security group to implement the interworking.

4.1.3.4 DDoS attack protection

Apsara Stack Security automatically detects, schedules, and mitigates DDoS attacks. It completes attack detection, traffic redirection, and traffic mitigation within five seconds, guaranteeing the stability of the cloud platform network. Meanwhile, the anti-DDoS system of Apsara Stack triggers protection by depending on the traffic threshold value, and statistics and judgment of network behaviors, which precisely identifies DDoS attacks and guarantees the business availability of users in case of a DDoS attack.

4.1.4 ApsaraDB security

4.1.4.1 Tenant layer isolation

ApsaraDB in the Apsara Stack environment isolates tenants by using the virtualization technology, allowing each tenant to have their own database permissions. Alibaba Cloud also reinforces the security of the server on which databases run. For example, users cannot access system files by

reading from or writing to databases, which makes sure that users cannot access data of other users.

4.1.4.2 Database accounts

After a user creates an ApsaraDB instance, the system does not create any initial database account for the user. The user must create a common database account in the console or by using APIs, and configure database-level read/write permissions. If the user requires more fine-grained permission control, such as table/view/field-level permission control, the user can also create a super database account in the console or by using APIs, use the database client and super database account to create a common database account, and use the super database account to configure table-level read/write permissions for the common database account.

4.1.4.3 IP address whitelist

By default, ApsaraDB instances are set to be inaccessible from any IP addresses, that is, the IP address whitelist contains only 127.0.0.1. To add IP address whitelist rules, users can use the data security module in the console or by using APIs. An IP address whitelist rule can take effect without restarting RDS instances and does not affect the usage. Multiple groups can be configured in the IP address whitelist, and each group can contain up to 1,000 IP addresses or IP address segments.

4.1.4.4 VPC isolation

Besides the IP address whitelist, ApsaraDB supports advanced network access control by using VPC. VPC is a private network environment that the user sets in the cloud platform. It strictly isolates network packets by using underlying network protocols and controls access at layer 2 of the network. Meanwhile, users can connect server resources of self-built data centers to the Apsara Stack platform by using VPN or leased lines, and solve possible IP resource conflicts by using the IP address segments of ApsaraDB instances defined by VPC, to allow self-owned servers and ECS instances to access ApsaraDB instances simultaneously.

By using VPC and the IP address whitelist, users can dramatically improve the security of their ApsaraDB instances.

4.1.5 Cloud storage security

4.1.5.1 Identity verification

Users can create AccessKeys by themselves in the Apsara Stack console. An AccessKey consists of an AccessKey ID and an AccessKey Secret. The AccessKey ID is public and used to identify

users, and the AccessKey Secret is private and used to authenticate users. When a request is sent to OSS, a signature string is generated for the request in the specified format and then encrypted by using the AccessKey Secret (based on the HMAC algorithm) to generate a verification code. (The verification code contains a timestamp to avoid replay attacks.) After receiving the request, OSS locates the corresponding AccessKey Secret by using the AccessKey ID and obtains the signature string and verification code in the same way. If the calculated verification code is the same as the provided one, the request is assumed valid. If not, OSS rejects the request and returns an HTTP 403 error.

4.1.5.2 Access control

Access to OSS resources is divided into access by the owner and access by third-party users. An owner owns a bucket, while third-party users are other users who access resources in the bucket. A user can access OSS resources anonymously or with a signature. An anonymous access request does not contain any identification information. A signature-based access request carries signature information in the request header or URL according to the OSS API rules.

4.1.5.3 Tenant layer isolation

OSS slices user data, discretely stores the sliced data in the distributed file system in compliance with specific rules, and stores the user data and data indexes separately. OSS users are authenticated by using symmetric AccessKeys. The signature of each HTTP request is verified. After user verification is passed, OSS reassembles the discretely stored data to achieve data storage isolation between multiple tenants.

4.1.6 Application security

The Apsara Stack platform uses Web Application Firewall (WAF) to protect the security of middleware and platform applications. WAF blocks and intercepts OWASP Top 10 attacks, including SQL injection, XSS, and other attacks, on Web applications to guarantee the security of middleware and platform applications.

In addition, Alibaba Cloud security experts perform SDL security review and continuous red army-blue army confrontation exercises for middleware and platform applications in the Apsara Stack platform to guarantee the security of such applications.

4.1.7 Data security

4.1.7.1 Data security system

Alibaba Cloud develops its data security system comprehensively and systematically by taking management and technical measures based on the data security lifecycle. Data security is managed and controlled during the data lifecycle, from data production, data storage, data usage, data transmission, data distribution, to data destruction.

The Apsara Stack platform has appropriate security management systems and security technologies at each stage of data security lifecycle.

4.1.7.2 Data ownership

In July 2015, Alibaba Cloud initiated the first "Data Protection Proposal" among cloud computing service providers in China. This public proposal appeals that the ownership of data of all developers, companies, governments, and social institutions on the cloud computing platforms absolutely belongs to the users. The cloud computing platforms cannot use the data for other purposes. Platform providers have a responsibility and obligation to help users protect privacy, integrity, and availability of their data.

4.1.7.3 Multi-copy redundancy storage

Apsara Stack uses the distributed storage technology to divide a file into many data fragments, stores them on different devices, and creates multiple copies for each data fragment. Distributed storage improves both data reliability and security.

4.1.7.4 Full-stack encryption

Apsara Stack uses full-stack encryption to guarantee the data security, including sensitive data encryption in applications, transparent data encryption in RDS, block storage data encryption, object storage system encryption, hardware encryption modules, and network data transmission encryption. To encrypt sensitive data in applications, Apsara Stack uses encryption solutions in a hardware-trusted execution environment provided by the processor.

4.1.7.5 Image management

The ECS instances in the Apsara Stack platform provide snapshots and custom images. Snapshots can save the status of system data at a certain time point for data backup, which allows users to achieve quick disaster recovery. Users can create custom images by using snapshots to completely include the operating system and data environment information of the

snapshots in the images. Snapshots are incremental and only the data changed between two snapshots is copied.

4.1.7.6 Residual data cleanup

After memories and disks that once stored user data are released and recycled, all the residual data on them are automatically cleared.

4.1.7.7 O&M data security

Without the consent of users, O&M personnel cannot access unpublished data of users in any way.

Adhering to the principle that production data stays within the production clusters, the Apsara Stack platform technically controls the channels through which the production data flows out of the production clusters. This prevents the O&M personnel from copying data from the production system.

4.1.8 Security of cloud product codes

In the secure product lifecycle (SPLC) of cloud products, Alibaba Cloud security experts strictly review and evaluate the code security on each development node to guarantee the code security of Apsara Stack products.

SPLC is tailored by Alibaba Cloud for cloud products, aiming to integrate security into the entire product development lifecycle. With SPLC, complete security audit is implemented at each node from product architecture review, development, test, to emergency response. This makes sure that the products meet the strict cloud security requirements, effectively improve their security capabilities, and reduce security risks. The entire SPLC of a cloud product can be divided into the following six phases: product initiation, security architecture review, secure development, security testing and review, application release, and emergency response.

- **In the product initiation phase**, the security architect works together with the product team to establish a functional requirements document (FRD) and a detailed architecture diagram based on the business contents, business process, and technical frameworks. This also extracts the Security Baseline Requirements applicable to the product range from all the security baseline requirements for the release of Apsara Stack products. Meanwhile, specific security training courses and exams are arranged for the product team in this phase to avoid significant security risks in subsequent product development.

- **In the security architecture review phase**, the security architect evaluates the security architecture of products based on the FRD and architecture diagram established in the preceding phase, and creates threat models of the products. In the process of threat modeling, the security architect creates detailed models for every asset that requires protection, security requirements of assets, and scenarios where attacks may occur, and then proposes corresponding security solutions. The security architect then works with the product team to determine all the Security Requirements for the products, based on the preceding Security Baseline Requirements and the security solutions proposed during threat modeling.
- **In the secure development phase**, the product team must abide by the secure coding standards in product development in accordance with the Security Requirements, and achieve relevant security features and requirements of the products. To guarantee rapid and continuous development, release, and deployment of cloud products, the product team carries out self-evaluation in this phase to confirm that the Security Requirements have been implemented. Then, the team provides the security engineer who is responsible for testing with corresponding test information, such as the code implementation address and self-testing result report, to prepare for the security testing and review in the next phase.
- **In the security testing and review phase**, the security engineer implements comprehensive security reviews on the architecture design and server environment of the products according to their Security Requirements. The engineer also performs code review and penetration testing on the products. The product team must repair and reinforce products with security problems found in this phase.
- **In the application release phase**, only products that pass the security review and get the security approval can be deployed in the production environment by using a standard release system. This prevents products with security vulnerabilities from running in the production environment.
- **In the emergency response phase**, the security emergency team constantly monitors possible security problems in the cloud platform. They also identify security vulnerabilities by using external channels such as ASRC or internal channels, such as internal scanners and self-testing on security. If a security vulnerability is detected, the emergency team quickly rates it, determines its priority, and schedules it for fixing. The team appropriately allocates resources to quickly fix vulnerabilities. This guarantees the security of Apsara Stack and its users.

4.1.9 Security audit

Security audit is the systemic and independent inspection and verification of the activities and behaviors in the computer network environment. It is carried out by professional auditors who give their assessments based on relevant laws and regulations, as delegated by property owners and authorized by management authorities. Administrators can perform security audit when they want to backtrack system operations.

The security audit of Apsara Stack collects system security data, analyzes weaknesses in system operations, reports audit events, and classifies audit events into high, medium, and low risk levels. Administrators view and analyze audit events to continuously improve the system performance and guarantee the security and reliability of cloud services.

Security audit covers multiple businesses and physical hosts on the cloud computing platform. It collects behaviors from various aspects to guarantee full coverage of audit.

The audit log collection center allows centralized, quasi real-time, and synchronous collection of all behavior logs. Audit logs are stored based on cloud computing storage services and clustered in three copies. This guarantees the secure and stable storage. The storage space can be quickly expanded.

By creating a full-text index for massive log data, security audit provides fast retrieval and query capability for large volumes of data.

4.1.10 Security operation service on the cloud platform

Security inspection

Alibaba Cloud investigates and sorts lists of cloud platform services, including the number of physical machines and the version of each product.

In addition, Alibaba Cloud analyzes event logs of basic security products provided by the cloud platform, and defends against security risks of products.

Security evaluation and reinforcement

Alibaba Cloud evaluates the security of the cloud platform system, detects network, host, and application security risks on the cloud platform, and reinforces security against the detected risks.

Vulnerability repair

Alibaba Cloud repairs security vulnerabilities detected during cloud platform running, such as password and configuration problems.

Cloud product security policy sorting and reinforcement

Alibaba Cloud sorts and reinforces the default security policies of the cloud platform system and products.

Security emergency response

If a security emergency such as an intrusion occurs, Alibaba Cloud responds to the emergency in time and analyzes the event cause.

4.2 Cloud user (tenant) security

Apsara Stack provides users with multi-level security protection, including account security, host security, application security, data security, Apsara Stack Security, security operation service, and best security practices.

4.2.1 Account security

The Apsara Stack platform provides various security measures to help users protect their accounts and avoid operations of unauthorized users. These security measures include logon as a cloud account, RAM user creation, centralized management of RAM user permissions, data transmission encryption, and operation audit of RAM users. Users can use these measures to protect their cloud accounts.

4.2.2 Host security

Intrusion detection

Apsara Stack users can configure the Apsara Stack Security Server Guard client on their hosts to collaborate with the Apsara Stack Security center and acquire the security capability of intrusion detection. The intrusion detection for the hosts includes remote logon reminder, identification of brute force attack behaviors, Webshell detection and removal, and host exception detection.

Vulnerability management

Apsara Stack users can configure the Apsara Stack Security Server Guard client on their hosts to collaborate with the Apsara Stack Security center and acquire the security capability of vulnerability management. The vulnerability management for the hosts incorporates multiple scanning engines (network side, local side, and PoC verification) to detect all vulnerabilities in the system at a time. Features such as one-click fixing, fixing command generation, and one-click batch verification are provided to implement closed-loop vulnerability management.

Image reinforcement

An image is a running environment template for ECS instances. It generally includes an operating system and preinstalled softwares. ECS tenants can use images to create ECS instances or change the system disks of ECS instances. Security measures for Apsara Stack basic images (supporting various Linux/Windows release versions) include basic image security configurations , image vulnerability fixing, and default image host security software. In addition, Apsara Stack monitors the vulnerabilities in basic image operating system and third-party softwares in real time to make sure that all high-risk vulnerabilities in Apsara Stack basic images are fixed immediately. Basic images are configured with best security practices for the hosts by default. Besides, Apsara Stack host security software is added to all Apsara Stack basic images by default to guarantee the security of instances upon startup.

4.2.3 Application security

Web application protection

Web Application Firewall (WAF) defends against SQL injection, XSS, common Web server plug-in vulnerabilities, Trojan uploads, unauthorized access to core resources, and other common OWASP attacks. It filters out massive malicious access attempts to prevent leakage of website assets and data and guarantee the security and availability of website applications.

Code security

In the secure product lifecycle (SPLC) of cloud products, Alibaba Cloud security experts strictly review and evaluate the code security on each development node to guarantee the code security for Apsara Stack products. Meanwhile, Alibaba Cloud strongly recommends that enterprise users perform black-box and white-box code security testing on their online applications to prevent security vulnerabilities and improve the security robustness of their businesses.

4.2.4 Data security

Alibaba Cloud protects users' data on the cloud platform by means of data desensitization, data discovery, and data watermarking.

- **Data discovery** is the basis of data security. This feature detects sensitive data, such as ID card number, mobile phone number, bank card number, and address, and performs custom data security control based on the data type.
- **Data desensitization** desensitizes sensitive data and converts original data to data in a specific format but does not have any special meanings.

- **Data watermarking** inserts data in a database to original data by adding pseudo rows and columns. If massive data is stolen, the original data can be traced. Data in the pseudo rows and columns is simulated from actual data. In this way, hackers cannot visually distinguish data, delete data in the pseudo rows and columns, or clear data watermarks.

4.2.5 Security product (Apsara Stack Security)

Built on Alibaba Group's security technologies accumulated over the years, Apsara Stack Security provides users with one-stop security services, including the anti-DDoS, host intrusion protection, Web Application Firewall (WAF), and Situation Awareness by leveraging the powerful data analysis capability of Apsara Stack computing platform.

Apsara Stack Security is composed of traffic security monitoring, host intrusion detection, Server Guard, security audit, DDoS mitigation, WAF, Cloud Firewall, bastion host, and Situation Awareness. Together with Alibaba Cloud's professional security operation services, Apsara Stack Security provides cloud users with one-stop security assurance that covers intrusion protection, security audit, Situation Awareness, and centralized management.

4.2.6 Security operation service

Alibaba Cloud provides tenants with the security operation service to operate resources and management policies on the Apsara Stack platform, including security product configuration and hosting, security event response, accident tracking, security inspection, monitoring and scanning, and security process management. This service continuously guarantees consecutive and secure operation of tenants' services.

4.2.7 Best security practices

Tenants must migrate security policies during the cloud migration and configure the best security practices as follows to guarantee the security of their businesses:

- **Cloud resource security:** The security of cloud resources, which must be guaranteed by using VPC.
- **Apsara Stack Security:** Apsara Stack Security is used to guarantee the security of tenants' businesses. The synchronization center is used to synchronize the latest Apsara Stack Security rules. In addition, we recommend that users use WAF to protect Web applications.
- **Cloud product security configurations:**
 - Complex passwords must be used for ECS instances to prevent intrusions by brute force cracking.

- SSH and RDP management ports must be restricted by using security groups.
- If high-risk ports are enabled on ECS instances, the IP address whitelist must be configured for access control.
- Server Load Balancer is prohibited to enable access of SSH, RDP, MySQL, Redis, and other high-risk port services to the Internet.
- High-intensity passwords must be set for RDS instances, and the IP address whitelist must be configured for access control.
- The access to OSS instances must be restricted by using access control rules, and public read/write operations are disabled.
- **Application deployment security:** The compressed packages, .svn hidden directories, and .git hidden directories must be deleted during code deployment. Security of Linux, Windows, and other operating systems must be reinforced. Meanwhile, we recommend that users use WAF to protect Web applications.

5 Apsara Stack product security

5.1 Account security

5.1.1 Apsara Stack account

An Apsara Stack account is used to manage O&M operations on the Apsara Stack platform and resources of cloud tenants.

An Apsara Stack account is the owner of Apsara Stack resources and the basic unit for measuring the resource usage. A user must register an Apsara Stack account before using Apsara Stack services. An Apsara Stack account has full permissions to all the resources they own. By default, a resource can only be accessed by the ResourceOwner. Other users must be explicitly authorized by the owner to access the resource, that is, the owner must grant the object to other users. Therefore, from the perspective of permission management, the Apsara Stack account is similar to the root or admin account of an operating system, and the Apsara Stack account is sometimes called the root or primary account.

An authorized Apsara Stack account can manage cloud resources or maintain the cloud platform. The O&M permissions of the cloud platform are managed by using OAM, and the resource management permissions of the cloud tenants are managed by using RAM. RAM also supports the primary account and RAM users.

5.1.2 Super administrator

The Apsara Stack platform has a default super administrator who can create system administrators and notify them of the default password by SMS or email. You must modify the password of your username as instructed when you log on to the Apsara Stack console for the first time. To improve security, the password must meet minimum complexity requirements, that is, 8-20 characters long and containing at least two types of the following characters: English uppercase or lowercase letters (A-Z or a-z), numbers (0-9), or special characters (such as exclamation marks (!), at signs (@), number signs (#), dollar signs (\$), and percent signs (%)).

5.1.3 Identity credential

An identity credential is used to verify the real identity of a user. It usually refers to a user's logon password or AccessKey. Identity credentials are confidential, so users must keep their credentials secret.

- **Logon username/password**

Users can use the logon username and password to log on to the Apsara Stack console to apply for resources and perform operations on resources.

- **AccessKey**

Users can use the AccessKey to construct an API request (or use cloud service SDKs) to perform operations on resources.

5.2 OAM

Operation Administrator Manager (OAM) is a permission management platform for Apsara Stack Operation. OAM uses a simplified role-based access control (RBAC) model. Administrators can assign roles to O&M personnel by using OAM. The O&M personnel have different operation permissions to different O&M systems based on their roles.

5.2.1 OAM permission model

In RBAC, the administrator does not directly grant system operation permissions to specific users, but creates a role set between the sets of users and permissions. Each role corresponds to a group of permissions. A user that is assigned a role has all permissions of that role. Therefore, when creating a user, you are only required to assign a role to the user, without granting specific permissions to the user. In addition, role permission change is less frequent than user permission change, which simplifies permission management and reduces system overhead.

5.2.2 OAM authorization

- **Subject:** Operator of the access control system. OAM subjects include users and groups.
- **User:** Administrators and operators of the OAM system.
- **Group:** A set of multiple users.
- **Role:** Core of the OAM system. Generally, a role can be considered as a set of permissions. A role can contain multiple RoleCells and/or roles.
- **RoleHierarchy:** In the OAM system, a role can contain other roles to form a RoleHierarchy.
- **RoleCell:** Specific description about a permission. A RoleCell consists of resources, operation sets, and authorization options.
- **Resource:** Description about authorization objects. For resources on each O&M platform, see the permission list of each O&M platform.

- **ActionSet:** Description about authorized operations. An ActionSet can contain multiple operations. For operations on each O&M platform, see the permission list of each O&M platform.
- **WithGrantOption:** Maximum number of authorizations in cascaded authorization, which is an integer greater than or equal to zero. If the value is not zero, the permission can be granted. If the value is zero, the permission cannot be granted.

For example, when administrator A grants a permission to administrator B, the WithGrantOption value is 5, indicating that the permission can be granted for five times at most. When administrator B grants the permission to administrator C, the WithGrantOption value can be up to 4. If WithGrantOption is set to 0 when administrator B grants the permission to operator D, operator D can only use the permission but cannot grant the permission to others.

5.3 Apsara Infrastructure Management Framework permission management (data center management)

Apsara Infrastructure Management Framework is an automatic data center management system that manages the hardware lifecycles and various static resources in the Apsara Stack data center, including programs, configurations, operating system images, and data.

Apsara Infrastructure Management Framework provides a set of universal version management, deployment, and hot upgrade solutions for the Apsara system and applications and services of various Apsara Stack products. Services based on Apsara Infrastructure Management Framework can enjoy automatic O&M in a large-scale distributed environment, greatly improving the O&M efficiency and system availability.

Permission management

The permission management of Apsara Infrastructure Management Framework is based on the OAM system. The user permissions of Apsara Infrastructure Management Framework include the Admin permissions, Project permissions, and Service permissions.

- **Admin permissions:** Administrators can manage all pages on the Apsara Infrastructure Management Framework platform.
- **Project permissions:**
 - The administrator must grant users the Project permissions to view the project information in **Operations > Project Operations** on the Apsara Infrastructure Management Framework platform.

- The administrator must grant users the Project permissions to view the cluster information and perform operations on the cluster in **Operations > Cluster Operations** on the Apsara Infrastructure Management Framework platform.
- **Service permissions:** The administrator must grant users the Service permissions to view the service information and perform operations on the service in **Operations > Service Operations** on the Apsara Infrastructure Management Framework platform.

5.4 RAM

Cloud tenants can use Resource Access Management (RAM) to build a system of primary account and RAM users.

RAM is an Apsara Stack service designed for user identity management and access control. You can use RAM to create and manage user accounts (such as employees, systems, and applications) and grant them the operation permissions to their resources. If multiple users collaboratively work with resources, RAM allows you to avoid sharing the password or AccessKey Secret of your Apsara Stack account with other users. You can grant users the minimum permissions necessary for them to complete their work, reducing information security risks.

5.4.1 RAM user identity types

RAM supports two different user identity types: RAM-User and RAM-Role.

- **RAM-User**

A RAM-User is a real identity, with a fixed ID and authentication key. Generally, it corresponds to a specific person or application.

- **RAM-Role**

A RAM-Role is a virtual identity with a fixed ID, but no authentication key. A RAM-Role must be associated with one or more real identities before it becomes available. For example, it can be associated with RAM-Users under the current or another Alibaba Cloud account, Apsara Stack services such as EMR and MTS, and external real identities such as a local enterprise account.

5.4.2 Permissions

A permission is used to allow or deny a user's operation on a certain kind of resource.

Operations can be divided into two categories: resource control operations and resource use operations.

- **Resource control operations** are operations for lifecycle management and O&M management of cloud resources, such as creating, stopping, and restarting ECS instances, and creating, modifying, and deleting OSS buckets. Resource control is generally oriented to resource owners or O&M employees in an enterprise organization.
- **Resource use operations** are the use of the core functions of the resources, such as user operations in an ECS instance operating system, and uploads/downloads of OSS bucket data. Resource use is oriented to R&D employees or applications in an enterprise organization.

For elastic computing and database products, resource control operations are managed by using RAM and resource use operations are managed in each product instance, such as the permission control of ECS instance operating system or MySQL database. For storage products, such as OSS and Table Store, both resource control operations and resource use operations can be managed by using RAM.

5.4.3 Authorization policies

An authorization policy is a type of simple language specification that describes a permissions set.

RAM supports two types of authorization policies: system access policies managed by the Apsara Stack platform and custom access policies managed by users. For system access policies managed by the Apsara Stack platform, users can only use but cannot modify them, and the policy versions are automatically updated by the platform. For custom access policies managed by users, users can create or delete them and maintain the policy versions by themselves.

RAM allows users to create and manage multiple authorization policies under an Apsara Stack account. Each authorization policy is essentially a set of permissions. The administrator can allocate one or more authorization policies to a RAM user (including RAM-User and RAM-Role). The RAM authorization policy language expresses the authorization meaning in details. A policy can grant permissions to an API-Action and Resource-ID, and specify multiple restrictions such as source IP address and access time.

5.5 Analysis of security risks

The security risks of ECS mainly stem from five areas, that is, accounts, hosts, applications, networks and data.

Table 5-1: Security risks

Risk sources	Description
Accounts	Unauthorized operations exist due to loose control over accounts' identity and access.
Hosts	Intrusions to hosts must be prevented. Detection must be made in a timely manner to avoid vulnerabilities.
Applications	Common attacks defined by OWASP must be prevented, including SQL injection, XSS, ordinary Web server plugin loopholes, Trojan uploading, unauthorized access to core resources, etc. Malicious access must be filtered out and website asset data must be protected, thus safeguarding the security and availability of websites.
Networks	As a distributed virtual firewall, a security group features state detection and packet filtering. Hence, complete security group rules must be configured to ensure network security isolation.
Data	Risks exist in various areas of data such as production, storage and transfer.

5.6 Design of security features

5.6.1 Security isolation

Security isolation of instances includes:

CPU isolation

Based on the hardware virtualization technology of VT-x, Alibaba Cloud ECS supports the KVM Hypervisor. Hypervisor runs in the vmx root mode while ECS instances run in the vmx non-root mode. With hardware-based isolation, ECS instances are effectively prevented from accessing privileged resources and isolation among ECS instances is implemented.

Memory isolation

At the virtualization layer, Hypervisor isolates the memory. When ECS instances are running, the hardware-aided Extended Page Tables (EPT) technology ensures that ECS instances cannot access each other's memory.

When an ECS instance is released, all of its memory is cleared by Hypervisor, thus preventing other ECS instances from accessing the contents of physical memory pages after the release.

Memory isolation

At the virtualization layer, Hypervisor implements I/O virtualization by separating the device drivers . By doing so, ECS instances cannot access physical disks directly and all the I/O operations are intercepted and processed by Hypervisor. Hypervisor makes sure an ECS instance can only access the assigned virtual disks, thereby securely isolating the disks of different ECS instances.

Network isolation

ECS adopts virtual switches. When a packet is sent to an ECS instance, it is only sent to the virtual switch port that corresponds to the virtual network interface of that ECS instance so that other ECS instances cannot receive or sniff that packet.

When running in the hybrid mode, a virtual instance cannot receive or sniff the traffic toward other virtual instances either. Even if the network interface is set to the hybrid mode, Hypervisor does not send any traffic toward a destination address to other virtual instances.

Meanwhile, Alibaba Cloud adopts VPC and security groups to isolate networks.

As a distributed virtual firewall provided by Alibaba Cloud, a security group has such functions as state detection and packets filtering, presenting another line of network defense for ECS instances . Independent of the internal firewall of the operating system of an ECS instance, a security group is another protection mechanism outside the ECS instance. A security group allows configuring the inbound/outbound policies at the granularity of individual IPs/ports and can be used for security domain isolation.

As a logical group, a security group consists of the instances in the same region that have the same security demands and trust each other. By using security groups, you can configure network access control for one or more ECS instances. Security groups are an important network security isolation approach and can be used to divide network security domains on the cloud.

With the above isolation measures, instances cannot sniff each other's traffic even if two instances owned by the same user run on the same physical server.

In addition, it is recommended to encrypt your data before storing it on the disks of an ECS instance, for example, using encrypted file systems or disks. For details, see [ECS disk encryption](#).

5.6.2 Authentication and authorization

5.6.2.1 Identity authentication

Account authentication is to verify the authenticity of a user's identity via identity credentials.

Identity credentials usually refer to the login password or Access Key (AK). You can create an

AK on the cloud by yourself. An AK consists of AccessKeyId and AccessKeySecret. Of them, AccessKeyId is public and indicates a user's identity. AccessKeySecret is a key intended for encrypting the signature string and verifying it by the server. It is used for identity authentication and must be kept secure.

ECS performs identity authentication for each access request. Thus, whether a request is made via HTTP or HTTPS, a signature must be included in the request. ECS performs symmetric-key encryption to verify the identity of a sender by using AccessKeyID and AccessKeySecret. AccessKeyID and AccessKeySecret are officially issued to visitors by Alibaba Cloud (requested via and managed by the Alibaba Cloud website). Of them, AccessKeySecret is only known by Alibaba Cloud and its owner.

5.6.2.2 Authority management

Provided by Alibaba Cloud, Resource Access Management (RAM) is a centralized service for users management and resources access control. With RAM, you can create independent user accounts for employees, systems or applications and control such users' operation authority of your cloud resources. Each RAM user has an independent login password or Access Key and is able to log on to the cloud console or operate the cloud service API via a program. When created, a RAM user has no authority to access any resource by default. Only after explicitly authorized, can a RAM user operate resources by representing the cloud account.

With RAM, you can avoid sharing a cloud account key with other users and assign the minimum authority to different users according to the least privilege principle, thus reducing the information security risks. RAM allows one Alibaba Cloud account (primary account) to have multiple sub-accounts and supports such functions as multi-factor authentication, strong password policy, console users separated from API users, custom fine-granularity authorization, authorization by user groups, temporary authorization token, temporary account freeze, etc. RAM authorization can be implemented at such a granularity as an API-Action or Resource-ID. Moreover, various restrictions can be imposed, including the source IP address, SSL/TLS, access time period, multi-factor authentication, etc.

It is strongly recommended that you must exercise caution when accessing and operating ECS instances, for example, using the SSH public/private key pair and protecting the private key well (a complex password should be used at least and it can be set upon creating instances), logging in remotely via the safer SSHv2, increasing the authority via sudo instructions, etc.

5.6.2.3 RAM and STS

Provided by Alibaba Cloud, Resource Access Management (RAM) enables ECS users to manage users' access to resources by creating sub-accounts and groups.

RAM helps you control users' access to resources. For example, to enhance network security control, you can add an authorization policy to a group, providing that if the source IP is not from a certain enterprise website, requests from that IP are denied.

You can assign different authorities to different groups in a bid to manage ECS resources, for example:

- **SysAdmins:** This group requires the authority of creating and managing ECS images, instances, snapshots and security groups. You can add an authorization policy to this group, providing that all its members can perform all the ECS operations.
- **Developers:** This group only needs the authority of using ECS instances. You can add an authorization policy to this group, providing that all its members can make calls to such APIs as `DescribeInstances`, `StartInstance`, `StopInstance`, `CreateInstance` and `DeleteInstance`.

If a developer becomes a system administrator, you can easily move him/her from the Developers group to the SysAdmins group.

In addition, ECS supports the ECS instance RAM role by connecting to the STS access point. The instance RAM role is a type of RAM role and is used to make an ECS instance assume a role with some permissions, thereby assigning the instance some access authority.

The instance RAM role allows you to associate a RAM role with an ECS instance so that other cloud products can be accessed by using the temporary STS credentials (updated periodically) inside the instance. This way, the security of the Access Key is protected on one hand; on the other hand, authority can be controlled in a fine way with the help of RAM.

5.6.3 Data security

For the sensitive data required for the running of the cloud platform, such as authorization credentials, user passwords and keys, encrypted storage is implemented for them with the key management and encryption mechanism provided by the Alibaba Cloud Key Management Service (KMS).

5.6.3.1 Triplicate technology

ECS users' reads/writes to virtual disks are mapped to the reads/writes to the files on the file platform of VPC. The Distributed File System of VPC uses a flat design in which a linear address

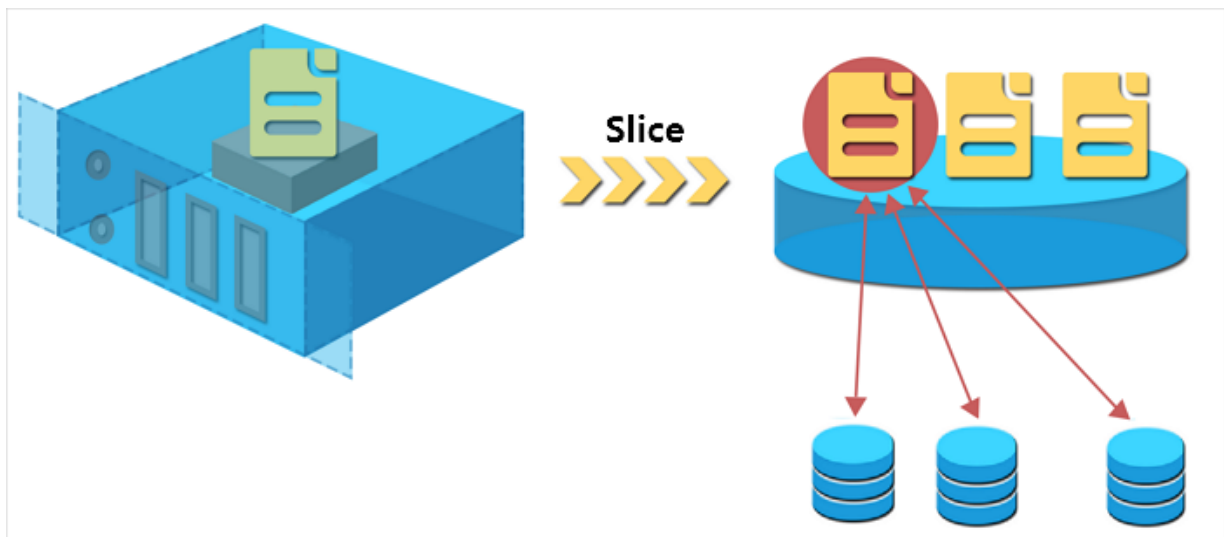
space is divided into slices, also called chunks. Each chunk has three copies stored on different server nodes on different racks, thus guaranteeing the data reliability.

Triplicate technology involves three key components: Master, Chunk Server, and Client. To demonstrate how triplicate technology works, in this example, the write operation of an ECS user undergoes several conversions before being executed by the Client. The process is as follows:

1. The Client determines the location of a chunk corresponding to one of your write operations.
2. The Client sends a request to the Master to query the storage locations (that is, the Chunk Servers) of the three copies of the chunk.
3. The Client sends write requests to the corresponding three Chunk Servers according to the results returned from the Master.
4. The Client returns a message to the user indicating whether the operation was successful.

The distribution strategy of the Master takes into account such factors as the disk usage of all the Chunk Servers in a rack, how they are distributed in different racks, availability of power supply and machine workloads, thereby guaranteeing that all the copies of a chunk are distributed on different Chunk Servers on different racks. This approach effectively reduces the potential of total data loss caused by failure of a Chunk Server or a rack.

Figure 5-1: Triple replication of data



If a system failure occurs because of a corrupted node or hard drive failure, some chunks may lose one or more of the three valid chunk copies associated with them. If this occurs and triplicate technology is enabled, the Master replicates data between Chunk Servers to restore the missing chunk copies across different nodes.

Figure 5-2: Auto syn. of data

As described above, whenever users add, modify or delete data on the cloud disks, their operations are synchronized to the three copies. By doing so, the reliability and consistency of users' data is guaranteed.

In addition, when data is deleted, the freed storage space is recycled by the Distributed File System and not accessible to any users. Moreover, the contents in the freed storage space are erased before that space is used again (including the contents on each cloud disk), thus safeguarding the data security to the maximum extent.

5.6.3.2 ECS disk encryption

As a simple and secure encryption method, ECS disk encryption encrypts newly created cloud disks. You do not have to create, maintain, or protect your own key management infrastructure, nor change any of your existing applications or O&M processes. In addition, no extra encryption /decryption operations are required, so your business is not impacted by the disk encryption function.

After an encrypted cloud disk is created and attached to an ECS instance, the data in the following list can be encrypted:

- Data on the cloud disk.
- Data transmitted between the cloud disk and the instance. However, data in the instance operating system is not encrypted.
- All snapshots created from the encrypted cloud disk, which are called encrypted snapshots.

Encryption and decryption are performed on the host that runs the ECS instance, so the data transmitted from the ECS instance to the cloud disk is encrypted.

ECS disk encryption supports all available cloud disks (basic cloud disks, ultra cloud disks, and SSD cloud disks) and shared block storage (ultra and SSD) in a VPC.

5.6.4 Transfer encryption

Alibaba Cloud ensures data transfer security via the HTTPS protocol. If you operate via the Alibaba Cloud platform, it transfers data via HTTPS. All the Alibaba Cloud services provide the HTTPS-ready API access points, allowing you to call the Alibaba Cloud service APIs in the form of program by using the Access Key. Alibaba Cloud supports the standard SSL/TLS protocols and offer the encryption of up to 256-bit keys, fully meeting the demands for encrypted transfer of sensitive data.

5.6.5 Log auditing

Identity authentication and authority management are intended for avoiding security issues while security logs are used to better understand and diagnose security status. Alibaba Cloud ActionTrail provides uniform management for security logs of cloud resources, recording the logins and access to resources under an account, including the operator, time, source IP, target resource, operation name and operation status. With the records saved by ActionTrail, you can carry out security analysis, intrusion detection, resource change track and compliance auditing. To meet the needs of compliance auditing, it is often needed to obtain the detailed operation records of the primary account and its sub-accounts, which can be retrieved easily from ActionTrail.

5.6.6 Other security capabilities

Block storage

Alibaba Cloud block storage is a low-latency, persistent, highly reliable, random block-level storage designed for ECS. Block storage can automatically replicate users' data in a zone, thus protecting the data from hardware failure and guaranteeing the business continuity. As with a hard disk, you can format the block storage attached to ECS instances, create a file system and store data for a long period of time.

Block storage supports auto encryption of the block storage devices used inside a virtual machine , making sure encrypted storage of block storage data in a distributed system.

Secure images

The Alibaba Cloud image integrates all the known high-risk vulnerability patches, preventing a host from being at high risk once online. Once a new high-risk vulnerability is found, Alibaba Cloud quickly updates the image and delivers it to the users. Meanwhile, Alibaba Cloud uses the data check algorithm to ensure the image integrity, preventing malicious tampering.

Once new high risk vulnerabilities are found, you can quickly update the base image. Meanwhile, you can upgrade the operating system on ECS instances or fix the vulnerabilities on your own.

It is strongly recommended that using Alibaba Cloud's base image as the first step of going cloud if your business deployment is not impacted.

Anti-ARP spoofing

In traditional network environments, ARP spoofing has been a severe challenge to the network. Through ARP spoofing, hackers can intercept secrets over the network and disturb the network.

To prevent ARP spoofing, VPC sets up an ARP firewall on the network interface. Normal communication is allowed only when the platform assigned MAC address is used, thus blocking the illegal traffic inside the attacker's instance.

5.7 Object Storage Service (OSS)

5.7.1 Security Isolation

OSS separates user data and discretely stores them in the distributed file system according to specified rules. User data and the data index are stored separately. OSS uses Access Key, a symmetric key authentication technology, for user authentication, to verify signatures for every HTTP request made by the user. When users are successfully authenticated, the user data that is stored discretely is reorganized to achieve data storage isolation among multiple tenants.

5.7.2 Authentication

5.7.2.1 User Authentication

Users can create Access Keys on the private cloud console. The Access Key consists of an AccessKey ID and AccessKey Secret. AccessKey ID is public, and is used to identify the user ID. AccessKey Secret is confidential, used to verify the user ID.

When a user sends a request to OSS, it first needs to generate a signature string for this request in accordance with the format specified by OSS. It then encrypts the signature string (based on the HMAC algorithm) with the AccessKey Secret to generate a digital signature. This is time stamped to prevent replay attacks. After receiving the request, OSS finds the corresponding AccessKey Secret using the AccessKey ID and extracts the signature string from the digital signature. If the calculated digital signature matches the provided one, the request is valid; otherwise, OSS will reject the request and return an HTTP 403 error.

5.7.2.2 Resource Access Management

Resource access to OSS is divided into owner access and third-party user access. Owner refers to the owner of the bucket, and third-party user refers to any other users who access the bucket. Access is divided into anonymous access and signed access. For OSS, if a request does not carry any identity information, it is regarded as anonymous access. Signed access is access that carries signature information in the request header or the request URL, as specified in the OSS API documentation.

OSS provides access control for buckets and objects.

Buckets have three kinds of access permissions: public-read-write, public-read, and private.

- Public-read-write: Anyone (including anonymous access) can PUT, Get and Delete objects in the bucket.
- Public-read: Only the creator of the bucket can write objects in the bucket (including PUT and Delete objects), and anyone (including anonymous access) can read objects in the bucket.
- Private: Only the creator of the bucket can write objects in the bucket (including PUT, Delete, and Get objects), and other users cannot access objects in the bucket.

When a user create a bucket, if they do not set a permission for the bucket, OSS will automatically configure the permission as private.

Objects have four kinds of access permissions: public-read-write, public-read, private, and default.

- Public-read-write: All users have the read-write access to this object.
- Public-read: The owner of another object has read access to this object, and only the owner of this object has the read-write access to this object.
- Private: The owner of this object has read-write access to this object, and other users have no read or write access to this object.
- Default: The object follows the access permissions of the bucket.

When a user uploads an object, if they do not set a permission for the object, OSS will automatically configure the permission as default.

5.7.2.3 RAM and STS support

OSS has integrated RAM/STS authentication.

Resource Access Management (RAM) is a resource access control service provided by Alibaba Cloud. Using RAM, the master account can create sub-accounts, which are subordinate to the

master account. All resources belong to the main account, and the main account can grant access permission for these resources to sub-accounts.

Security Token Service (STS) is a temporary access service provided by Alibaba Cloud to allow management of short-term access permissions. STS can generate a short-term access credential to the user. The access permission and expiration date of the credential are defined by the user, and the access credential expires automatically at the expiration date.

5.7.3 Data Security

Errors may occur during data transmission between the client and the server. OSS now supports the return of CRC64 values for objects uploaded in various ways. The client can compare the locally calculated CRC64 values to the returned CRC64 to verify data integrity.

OSS calculates the CRC64 value of the uploaded object, stores it in the metadata of the object, and then adds the `x-oss-hash-crc64ecma` head field in the returned response header to indicate the CRC64 value of the object. This value is calculated based on the [ECMA-182 standard](#).

5.7.4 Transmission Encryption

5.7.4.1 Server-Side Encryption

OSS supports server-side encryption for data uploaded by users. When users upload data, OSS encrypts the user data using AES256, and then saves the encrypted data. When users download data, OSS automatically decrypts the saved encrypted data and returns the original data to the user. It declares in the returned HTTP request header that this data has been encrypted on the server-side.

When users create objects and they want server-side encrypted storage for the object, only the HTTP header of `x-oss-server-side-encryption` is needed in the Put Object request, with its value set to AES256.

5.7.4.2 Client Encryption

Client encryption means that user data is encrypted before it is sent to the remote server. The secret key used for encryption is only stored in the user's local device. This guarantees user data security, ensuring that the original data cannot be decrypted even if it is leaked.

5.7.4.3 KMS Encryption

Alibaba Cloud Key Management Service (KMS) is a service that combines secure, highly available hardware and software to provide a key management system scaled for the cloud. KMS uses customer master keys (CMKs) to encrypt your OSS bucket objects. You can use KMS APIs to centrally create encryption keys, define the policies that control how keys can be used, and audit key usage to prove they are being used correctly. You can use these keys to protect your data in OSS buckets.

5.7.5 Logging Audit

OSS provides automatic access logging. After the user enables logging for the bucket, OSS automatically accesses the request log of this bucket. From this, it generates a request log, written as an object, in a user-specified target bucket according to a fixed naming rule. Hours are used as the unit of time for auditing or specific behavior analysis. The request log contains the request time, source IP, request object, return code, and processing time.

5.7.6 Anti-Leech

In order to prevent leeching of user data in OSS, OSS supports the anti-leech method based on the header field referer in the HTTP header. Users can configure a referer field's whitelist for a bucket and whether to allow the referer field to be empty through the OSS management console or the API. For example, for a bucket named oss-example, the user configures the referer's whitelist as `http://www.aliyun.com/`. Only requests with a referer of `http://www.aliyun.com/` can access objects in the bucket.

5.8 What is Table Store

Table Store is a NoSQL database service built on Alibaba Cloud's Apsara distributed file system that can store and access massive structured data in real time.

Table Store allows users to:

- Organize data into instances and tables that can seamlessly scale using data partitioning and load balancing.
- Shield applications from faults and errors that occur on the underlying hardware platform, providing fast recovery capability and high service availability.
- Manage data with multiple backups using solid state disks (SSDs), enabling quick data access and high data reliability.

5.8.1 Security Isolation

Table Store uses a shared storage mechanism, which allows multiple instances of different users to share the same cluster resource. Table Store uses the data partition as the smallest unit and supports the load balancing mechanism at the data partition level to isolate the impact between different instances.

5.8.2 Authentication

5.8.2.1 ID Authentication

Alibaba Cloud Table Store authenticates requests based on the AccessKey. Each valid table store request must carry the correct AccessKey information.

Table Store authenticates each request from applications to prevent unauthorized data access and ensure data access security.

5.8.2.2 RAM and STS Support

Alibaba Cloud Table Store supports RAM and STS services.

With RAM service, users can grant access and management permissions of the table store resources to sub-users.

Table Store also supports STS services, providing short-term access management through temporary access credentials. Users define access authority and validity of the credential. After the access credential expires, it will automatically become invalid.

Table Store supports the authorization granularity to both tables and APIs level.

5.8.2.3 VPC Access Control

Table store supports instance-level VPC access control with the following three types of VPC access settings:

- Allows arbitrary network access: Access from public networks and bound VPCs is allowed.
- Allows specific VPC access: Only access from bound VPCs is allowed and access from unbound VPCs is denied.
- Allows specific console or VPC access: Only access from bound VPCs and Table Store consoles is allowed and access from other sources is denied.

5.8.3 Data Security

Table Store is built on the Apsara Distributed File System and provides linear storage space. Linear addresses are sliced into chunks. For each chunk, three replicas are created and stored on different nodes in the cluster to ensure data reliability.

In Table Store, data is serialized before it is written to the disks. Each data block is written to one or multiple chunks.

The Apsara Distributed File System evaluates the disk usage of all nodes, the distribution of these nodes across different racks, the power supply, and the server loads to ensure the distribution of the chunk replicas on different servers on different racks. This ensures that failures on individual servers or racks do not impact data availability.

When a data node is damaged or a disk fault occurs on a data node, less than three chunk replicas are available.

In this case, the Apsara Distributed File System starts the automatic replication process to replicate data among different service nodes. This ensures that all chunks in the cluster have three valid replicas. Results of write operations are only returned after all the three replicas are written to the disks. This design ensures high data consistency.

5.9 Security Isolation

NAS splits user data into parts and discretely stores them in the distributed file system according to specified rules. In NAS, user data and the data index are stored separately and many authentication methods are applied. Before a user creates connections and sends requests, NAS checks the permission of the user. If the user passes the authentication, NAS reorganizes the splitted parts to achieve data storage isolation among multiple tenants.

5.10 Authentication

Permission control

Alibaba Cloud NAS supports standard file system directory/file permissions and supports user/user group read/write/execute permissions. NAS supports VPC mount points and classic network mount points. Only ECS instances within the same VPC or under the same account are allowed to access them.

In Alibaba Cloud NAS, access groups are a whitelist mechanism that allows specified IPs or network segments to access the file system. By adding rules to the access group, admins can grant different access permissions to different IPs or network segments.

Initially, each account automatically generates a **VPC default access group**. By default, it allows any IP in the VPC to access mount points with the highest permissions (read-write with no restrictions on the root user).



Note:

- Classic network type mount points do not provide a default access group.
- In addition, only single IP addresses can be added to Classic network access groups; network segments cannot be added.

An access group rule includes four attributes as shown in [Table 5-2: Access group attributes](#).

Table 5-2: Access group attributes

Attribute	Value	Description
Authorization address	Single IP addresses or network segment (classic network type only supports single IP addresses)	The authorization object of this rule.
Read-write permissions	Read-only, Read-Write	Allow the authorized object to perform read-only or read-write operations in the file system.
User privileges	No restrictions on the root user, Restrictions on the root user , Restrictions on all users	Whether to limit the privileges of Linux system users for the file system. When determining the file or directory access privileges: if restriction on the root user is selected, the root user will be treated as nobody; and if restriction on all users is selected, all users , including the root user, will be treated as nobody.
Priority	1-100, 1 is the highest priority	When an authorization object has multiple rules applied to it, higher priority rules will take priority over lower priority rules.

RAM Support

NAS applies the RAM service. You can configure RAM service on the Apsara Stack console to grant permissions to main account and sub-accounts.

With RAM service, you can authorize sub-users to store files in NAS.

Table 5-3: List of NAS operations that can be authorized by RAM

Operations	Description
DescriptFileSystems	List the file system instances
DescriptMountTargets	List the mount points for the file system
DescriptAccessGroup	List the access groups
DescriptAccessRule	List the rules for the access group
CreateFileSystem	Create file system instances
CreateMountTarget	Create mount points for the file system
CreateAccessGroup	Create access groups
CreateAccessRule	Create rules for the access group
DeleteFileSystem	Delete file system instances
DeleteMountTarget	Delete mount targets
DeleteAccessGroup	Delete access groups
DeleteAccessRule	Delete rules for the access group
ModifyMountTargetStatus	Disable or activate mount points
ModifyMountTargetAccessGroup	Modify mount target access group
ModifyAccessGroup	Modify access groups
ModifyAccessRule	Modify rules for the access group

5.11 Data Security

Multiple copy storage

NAS stores multiple copies of data to ensure data security.

Userdata: NAS stores three copies of userdata on the client, which allows it to afford the loss of two copies. The server side continuously monitors the copy number of the monitored data. If any data node is down or some disks on a data node are faulty, the copy number of some data in the cluster is less than 3. In this case, the server side starts the replication mechanism to ensure that the copy number of all data in the cluster is 3.

In addition, the server side compares the data and its checksum information to prevent occasional silent errors. If silent errors are detected, the server side replicates healthy copies of the data to ensure the copy number of all data is 3, guaranteeing the data reliability.

Data recycling

After you delete some data, the released storage space is recycled by the server side and is not allowed to be accessed. Before the storage space can be used again, the data stored in it is erased to ensure data security.

5.12 Logging audit

NAS system records logs related to file system instance operations, including creating and deleting.

Logs are automatically recorded at the server side after instance operations are performed, which include detailed information about the operations and can be used for fault analysis.

5.13 ApsaraDB for RDS

Alibaba Cloud ApsaraDB for RDS (Relational Database Service) is a stable, reliable, and scalable cloud database service. Based on Alibaba Cloud's distributed file system and high-performance storage, RDS supports the MySQL Redis database engine and provides an all-round database solution that includes disaster tolerance, backup, recovery, monitoring, migration, and more.

To ensure total user data security, RDS provides diversified functions to enhance security, such as:

- **Network:** IP whitelist, VPC
- **Storage:** automatic backup

5.13.1 Security isolation

Tenant isolation

RDS uses virtualization technology to isolate tenants. Each tenant can maintain their own database permissions independently. Alibaba Cloud also enhances security for servers running databases. For example, users cannot read or write system files using the database. This prevents users from accessing another user's data.

VPC

In addition to the IP whitelist, RDS also allows users to use VPCs for more advanced access control. A VPC is a logically isolated network environment in the private cloud. It uses underlying network protocols to strictly isolate users and provides access management at Layer 2. You can use VPN connections or leased lines to connect your own IDCs with Alibaba Cloud. You can

reserve IP segments for RDS instances in your VPCs, to avoid potential IP conflicts, and to allow both your own servers and ECS instances to access RDS.

The combined use of VPC and IP whitelist ensures overall security of RDS instances.

5.13.2 Authentication

5.13.2.1 Identity authentication

Account authentication uses your login password or access key (AK) to verify your identity. You can create your AK on the console. An AK consists of AccessKeyId and AccessKeySecret. AccessKeyId is public and indicates your identity, and the client uses AccessKeySecret to encrypt the signature string and the server uses AccessKeySecret to verify the signature string. You must keep your AK confidential.

The MongoDB server authenticates the identity of each access request, so the identity must contain signature information no matter whether the request is sent through HTTP or HTTPS. MongoDB services use AccessKeyId and AccessKeySecret to implement symmetric-key encryption for authenticating the identity of a request sender. AccessKeyId and AccessKeySecret are officially issued by Alibaba Cloud (you can apply for and manage them on the official website of Alibaba Cloud). Only you know the AccessKeySecret. Make sure to keep it confidential.

5.13.2.2 Permission control

After you create an instance, it has no initial database account. You can create a common database either on the console or using APIs, and set database-level read/write permissions. If more granular permission controls, such as table-, view-, or field-level permissions, are required, the user can use the console, or the API, to create a master database account. The user can use the database client and master database account to create a normal database account. A master database account can set read/write permissions for normal database accounts at the table level.

5.13.2.3 RAM and STS support

RDS instances which you create through an Alibaba Cloud primary account are managed as resources under that account. By default, a primary account has full permission for using resources under it.

RDS supports RAM. Using Alibaba Cloud's RAM service, a primary account user can permit RAM users under the account to access and manager primary account RDS resources. RDS also supports STS, granting temporary access permissions using temporary access tokens.

5.13.3 Data security

High-availability RDS instances have two database nodes to implement the master-standby architecture. The standby node immediately takes over services if the master node fails. To ensure data integrity and reliability, databases are automatically backed up. This ensures that data can be recovered. RDS supports automatic data and log backup. You can also initiate database backup whenever you want. RDS can restore data to any point in time according to the backup policy. This improves data traceability.

5.13.4 Transmission encryption

5.13.4.1 SSL

RDS provides Secure Sockets Layer (SSL) for MySQL and SQL Server. You can use the server root certificate provided by RDS to verify whether the database service with the target IP address and port is provided by RDS, which can effectively prevent man-in-the-middle attacks. To guarantee security and validity, RDS allows you to enable and update the SSL certificates for servers.

Though RDS can encrypt the connection between an application and a database, the SSL service can run properly only after the application enables authentication on the server. In addition, SSL results in extra CPU resource consumption and affects the throughput and response time of RDS instances to a certain degree. The specific impact varies depending on the number of user connection times and the data transfer frequency.

5.13.4.2 TDE

RDS provides transparent data encryption (TDE) for MySQL and SQL Server. The TDE function of RDS for MySQL is developed by Alibaba Cloud and the TDE function of RDS for SQL Server is based on the SQL Server Enterprise Edition.

You can specify the database or table to be encrypted in a TDE-enabled RDS instance. The data of the specified database or table is encrypted before being written to any device such as an HDD, SSD, or PCIe card, or to any service such as OSS or Archive Storage. Therefore, data files and backups of the instance are all ciphertext.

TDE adopts the Advanced Encryption Standard (AES) algorithm. The key length is 128 bits. The key for TDE is encrypted and stored by Key Management Service (KMS), and RDS dynamically reads the key only once when the instance is started or migrated. You can replace the key as needed on the KMS console.

5.13.5 SQL server audit

RDS allows users to review SQL transactions. You can regularly audit the SQL server to identify and resolve issues. RDS Proxy records all SQL statements sent to RDS, including details such as the IP address, database name, user account used for execution, SQL statement, execution time, number of returned records, and time point of execution.

5.13.6 IP whitelist

By default, the whitelist is set to only allow traffic from 127.0.0.1. It denies access to the RDS instance from any other IP addresses. To allow access for specific IPs, you can use the console, or the API, to configure whitelist access rules. Updates to a whitelist do not require restarting the RDS instance, and therefore do not affect instance services. You can sort IP whitelists into multiple groups, and each group can be configured with up to 1,000 IP addresses or IP segments.

5.13.7 Software upgrade

RDS provides you with new versions of database software.

Generally, upgrade is not mandatory. The database of an RDS instance is upgraded only when you restart the RDS instance.

In rare cases such as critical bugs and security vulnerabilities, RDS enforces database upgrade during the maintenance period of the instance. Such mandatory upgrade only results in transient database disconnection without any obvious adverse impact on the application when the database connection pool is correctly configured.

You can change the maintenance time on the console or using API to prevent mandatory upgrade during traffic peak periods.

5.13.8 Anti-DDoS protection

If the RDS instance is configured to be accessible from the Internet, the instance may suffer from DDoS attacks. If a DDoS attack is detected, the RDS security system enables traffic cleaning first. If traffic cleaning fails or the attack reaches the blackhole threshold, blackhole filtering is triggered.

Triggering conditions for traffic cleaning and blackhole filtering are listed as follows:

- Traffic cleaning

Traffic cleaning is only for traffic flows from external networks and does not affect running of your instance.

RDS automatically triggers and ends traffic cleaning. Traffic cleaning is triggered for a single RDS instance if any of the following conditions is met:

- Packets per second (PPS) reaches 30,000.
 - Bits per second (BPS) reaches 180 Mbit/s.
 - The number of new concurrent connections per second reaches 10,000.
 - The number of active concurrent connections reaches 10,000.
 - The number of inactive concurrent connections reaches 100,000.
- Blackhole filtering

Blackhole filtering is only for traffic flows from external networks. If an RDS instance is undergoing blackhole filtering, the instance cannot be accessed from external networks and the connected applications are unavailable. Blackhole filtering guarantees availability of RDS services.

Conditions for triggering blackhole filtering are listed as follows:

- BPS reaches 2 Gbit/s.
- Traffic cleaning cannot solve the problem.

A blackhole is automatically released 2.5 hours after being triggered.

5.14 Tenant isolation

RDS uses virtualization technology to isolate tenants. Each tenant can maintain their own database permissions independently. Alibaba Cloud also enhances security for servers running databases. For example, users cannot read or write system files using the database. This prevents users from accessing another user's data.

5.15 Permission control

Database account

When you log on to an ApsaraDB for Redis instance, you must pass the username and password authentication. ApsaraDB for Redis has optimized performance for short-lived connections. Therefore, enabling password authentication will not affect performance of Redis instances.

IP address whitelist

ApsaraDB for Redis provides the IP address whitelist feature to implement access control for network security. Each ApsaraDB for Redis instance can be configured with an IP address whitelist.

By default, ApsaraDB for Redis instances are set to be inaccessible from any IP addresses. Therefore, the IP address whitelist contains only 127.0.0.1. To add IP address whitelist rules, you can use the data security module on the console or Open APIs. The IP address whitelist can be updated without restarting ApsaraDB for Redis instances and does not affect the usage.

5.16 Network isolation

VPC

Alibaba Cloud provides different network isolation policies for different network environments.

In Apsara Stack, you can use an IP whitelist to control access. Furthermore, you can use the VPC to further control network access. A VPC is a private network environment you specified in the public cloud. A VPC strictly isolates your network data packets from others' through the bottom-layer network protocol to control access at the data link layer. You can use VPN or leased lines to enable your IDC server resources to access Alibaba Cloud. Additionally, you can use VPC-defined IP address segment to resolve IP address conflicts so that both your on-premises servers and ECS can access the cloud database. The VPC and IP whitelist provide full protection for instance security.

Internet

By default, instances deployed in a VPC can only be accessed by ECS instances belonging to the same VPC. Access from public network is acceptable in the following conditions if you have such a requirement and have applied for a public IP address. However, you are not recommended to do so.

- Access from ECS EIP.
- Access from your IDC public network.

**Note:**

An IP whitelist takes effect for all connection modes of instances. You are advised to set the whitelist before applying for a public IP address.

5.17 Backup and recovery

For the purpose of data integrity and reliability, databases are automatically backed up at a certain interval to ensure data restorability. Redis supports instance recovery based on backup sets.

5.18 RAM and STS support

Instances you have created through your cloud account are your resources. By default, your cloud account is granted full operation permissions on all your resources.

Memcache supports RAM and STS services. You can use RAM to grant Redis resource access and management permissions to sub-accounts of your cloud account. You can also use STS to grant short-term access permissions.

5.19 Software upgrade

- ApsaraDB for Memcache provides new database software releases on a regular basis.
- Software will be upgraded to the specified version only if you require.
- The ApsaraDB for Memcache development team will notify the service team to arrange the time for upgrade if your current version has critical security risks. The product development team provides full support throughout the upgrade.

Generally, ApsaraDB for Memcache is upgraded within 5 minutes. During the upgrade, the instance may be disconnected several times and will be read-only for about one minute. The impact is minor if the applications have correct automatic connection settings.

5.20 Data transmission encryption

ApsaraDB for Redis provides encryption based on Secure Sockets Layer (SSL) and Transport Layer Security (TLS). You can use the Redis server root license to check whether database services of destination IP addresses and ports are provided by Redis, thereby preventing man-in-the-middle attacks. Additionally, Redis allows you to enable and update SSL and TLS certificates on the server so that you can replace the SSL/TLS certificates as needed to enhance security.



Note:

- Transmission encryption requires authentication of applications running on the server.
- Transmission encryption increases CPU usage, affecting throughput and response time of instances. To which extent instances are affected depends on the number of connection times and data transmission frequency.

5.21 ApsaraDB for MongoDB

ApsaraDB for MongoDB is fully compatible with the MongoDB protocol and provides stable, reliable, and automatically scalable database services. It offers you a full range of database solutions in the areas of disaster tolerance, backup, recovery, monitoring, and alarms.

The three-node ReplicaSet architecture is deployed for ApsaraDB for MongoDB by default. The primary node supports read/write access, the secondary node provides routine read-only operations, and the hidden node ensures high availability.

ApsaraDB for MongoDB provides solutions to ensure secure and reliable services in multiple aspects, including but not limited to the following:

- RAM
- Network isolation
- Data backup

5.22 Security isolation

VPC

ApsaraDB for MongoDB allows you to use VPCs to achieve higher-level network isolation.

A VPC is a private network environment you specified in the public cloud. A VPC strictly isolates your network data packets from others' through the bottom-layer network protocol to control access at the network layer.

Tenant isolation

Tenants are isolated through virtualization technologies so that tenants have independent database permissions. In addition, Alibaba Cloud takes security hardening measures for database servers. For example, Alibaba Cloud forbids users to operate on system files through read/write operations, thereby preventing other users from contacting with your data.

5.23 Authentication

5.23.1 Identity authentication

Account authentication uses your login password or access key (AK) to verify your identity. You can create your AK on the console. An AK consists of AccessKeyId and AccessKeySecret. AccessKeyId is public and indicates your identity, and the client uses AccessKeySecret to encrypt the signature string and the server uses AccessKeySecret to verify the signature string. You must keep your AK confidential.

The MongoDB server authenticates the identity of each access request, so the identity must contain signature information no matter whether the request is sent through HTTP or HTTPS. MongoDB services use AccessKeyId and AccessKeySecret to implement symmetric-key encryption for authenticating the identity of a request sender. AccessKeyId and AccessKeySecret are officially issued by Alibaba Cloud (you can apply for and manage them on the official website of Alibaba Cloud). Only you know the AccessKeySecret. Make sure to keep it confidential.

5.23.2 Permission control

Database account

When you log on to an ApsaraDB for MongoDB instance, you must pass the username and password authentication. After an ApsaraDB for MongoDB instance is created, an initial root account is generated by default. You can set a password for the root account when creating an instance or reset the password after the instance is created.

The root account has all permissions on the ApsaraDB for MongoDB instance. You can log on to the database as the root user to add, delete, or grant permissions to other accounts.

5.23.3 RAM and STS support

ApsaraDB for MongoDB instances you create with your cloud account are resources of this account. By default, accounts have full operation permissions on their resources.

Alibaba Cloud Resource Access Management (RAM) allows you to assign the access and management permissions for ApsaraDB for MongoDB resources under your cloud account to RAM subaccounts.

5.24 Data security

ApsaraDB for MongoDB uses a three-node replica set highly available architecture. The three data nodes are located on different physical servers and synchronize data automatically. The primary and secondary nodes both provide service. When the primary node fails, the system automatically selects a new primary node. When the secondary node is unavailable, the standby node takes over services.

Apsara for MongoDB provides automatic backup and one-click recovery to resolve over 99.99% of system failures, ensuring data integrity and reliability.

ApsaraDB for MongoDB automatically backs up data to ensure data integrity and reliability. Users can specify the full physical backup frequency (at least twice per week) and the backup time window. Users can also initiate a full physical backup through the console or API at any time.

ApsaraDB for MongoDB also automatically backs up incremental logs. The full backup and incremental log backups allow users to restore data to a backup time point (accurate to seconds).

5.25 Log audit

The audit log function records operations performed on the databases in the instance. You can use the audit logs for fault analysis, behavior analysis, and security audit. Audit logs are generally becoming an essential regulatory requirement of Finance Cloud and other mission-critical services .

5.26 IP address whitelist

ApsaraDB for MongoDB provides the IP address whitelist feature to implement access control for network security. Each ApsaraDB for MongoDB instance can be configured with an IP address whitelist.

By default, ApsaraDB for MongoDB instances are set to be inaccessible from any IP addresses. Therefore, the IP address whitelist contains only 127.0.0.1. To add IP address whitelist rules, you can use the data security module on the console or Open APIs. The IP address whitelist can be updated without restarting ApsaraDB for MongoDB instances and does not affect the usage.

5.27 Anti-DDoS protection

Anti-DDoS protection provides real-time monitoring at the network entry point. When high-traffic attacks are identified, their source IP addresses are cleaned. If cleaning is ineffective, the black hole mechanism is triggered.

5.28 Tenant isolation

Tenants are isolated through virtualization technologies so that tenants have independent database permissions. In addition, Alibaba Cloud takes security hardening measures for database servers. For example, Alibaba Cloud forbids users to operate on system files through read/write operations, thereby preventing other users from contacting with your data.

5.29 Access control

Database account

Password authentication is required for access to ApsaraDB for Memcache. You can configure password-free access on the Memcache console if necessary.

ApsaraDB for Memcache has optimized performance for short-lived connections. Therefore, enabling password authentication will not affect performance of Memcache instances.

IP whitelist

ApsaraDB for Memcache provides IP whitelists to achieve secure network access control and allows you to set an IP whitelist for each ApsaraDB for Memcache instance.

By default, ApsaraDB for Memcache allows any IP address to access its instances. You can add IP addresses to the whitelist so that only these IP addresses can access your instance. Updating the IP whitelist does not require an instance restart, so services will not be affected. You can configure multiple whitelist groups, each of which can contain a maximum of 1000 IP addresses.

5.30 Network isolation

Alibaba Cloud provides different network isolation policies for different network environments.

VPC

In Apsara Stack, you can use an IP whitelist to control access. Furthermore, you can use the VPC to further control network access. A VPC is a private network environment you specified in the public cloud. A VPC strictly isolates your network data packets from others' through the bottom-layer network protocol to control access at the data link layer. You can use VPN or leased lines to enable your IDC server resources to access Alibaba Cloud. Additionally, you can use VPC-defined IP address segment to resolve IP address conflicts so that both your on-premises servers and ECS can access the cloud database. The VPC and IP whitelist provide full protection for instance security.

Internet

By default, instances deployed in a VPC can only be accessed by ECS instances belonging to the same VPC. Access from public network is acceptable in the following conditions if you have such a requirement and have applied for a public IP address. However, you are not recommended to do so.

- Access from ECS EIP
- Access from your IDC public network



Note:

An IP whitelist takes effect for all connection modes of instances. You are advised to set the whitelist before applying for a public IP address.

5.31 Backup and recovery

For the purpose of data integrity and reliability, databases are automatically backed up at a certain interval to ensure data restorability. Memcache supports instance recovery based on backup sets.

5.32 RAM and STS support

Instances you have created through your cloud account are your resources. By default, your cloud account is granted full operation permissions on all your resources.

Memcache supports RAM and STS services. You can use RAM to grant Memcache resource access and management permissions to sub-accounts of your cloud account. You can also use STS to grant short-term access permissions.

5.33 Software upgrade

- ApsaraDB for Memcache provides new database software releases on a regular basis.
- Software will be upgraded to the specified version only if you require.
- The ApsaraDB for Memcache development team will notify the service team to arrange the time for upgrade if your current version has critical security risks. The product development team provides full support throughout the upgrade.

Generally, ApsaraDB for Memcache is upgraded within 5 minutes. During the upgrade, the instance may be disconnected several times and will be read-only for about one minute. The impact is minor if the applications have correct automatic connection settings.

5.34 Server Load Balancer

Apsara Stack Server Load Balancer distributes incoming traffic among multiple Elastic Compute Service (ECS) instances. It expands the service capabilities of the application through traffic distribution and improves the availability of the application by eliminating single points of failures (SPOF).

5.34.1 Access control

SLB masks the IP addresses of backend servers and only exposes the IP address of the SLB instance for use. Additionally, SLB provides the whitelist function. You can control which IP addresses can access the SLB service by adding a whitelist.

5.34.2 HTTPS listeners

SLB supports HTTPS load balancing to forward HTTPS requests:

- For services that require certificate authentication, you can manage certificates and keys on SLB in a centralized and unified manner and do not need to deploy them on ECS instances.
- All decryption operations are performed on SLB, reducing the CPU costs of backend ECS instances.

SLB offers the certificate management function, allowing you to store certificates and keys. All private keys uploaded to the certificate management system are encrypted.

5.34.3 RAM and STS support

SLB instances created by using a primary account are resources under the account. By default, the primary account has full permission on these resources.

SLB supports RAM. You can authorize a RAM account to access and manage SLB resources under the primary account. SLB also supports STS, which provides temporary accesses to SLB resources.

5.35 Virtual Private Cloud

Virtual Private Cloud (VPC) allows you to construct a fully isolated logical network environment where the IP address range, subnets, route tables, and gateways can be customized.

5.35.1 Security Isolation

By using the tunneling technology, the isolation effect between VPC networks is same as that of the traditional VLAN. Broadcast domain isolation can be achieved on the ECS instance and Network Interface Cards. Network communication between VPC networks is completed isolated like the VLAN isolation. At the same time, access controls are implemented by dividing different security domains.

Each VPC has a unique tunnel ID, and a tunnel ID corresponds to only one VPC. A tunnel encapsulation carrying a unique tunnel ID is added to each data packet transmitted between the ECS instances within a VPC. Then, the data packet is transmitted over the physical network. Because the tunnel IDs are different for ECS instances in different VPCs and the IDs are located on two different routing planes, the ECS instances from different VPCs cannot communicate with each other and are isolated by nature.

5.35.2 Access control

VPC divides the network security domain through a security group firewall with stateful detection packet filtering function, and implements access control of the three-layer network based on the security group. The internal networks of different VPCs are completely isolated and can be interconnected through router interfaces.

5.35.3 RAM and STS support

VPC supports RAM service. Using RAM service, a primary account can permit RAM users to access and manage VPC resources. VPC also supports STS, granting temporary access permissions using temporary access tokens.

5.36 Log Service

As a one-stop service for log data, Log Service (Log for short) experiences massive big data scenarios of Alibaba Group. Log Service allows you to quickly complete the collection, consumption, shipping, query, and analysis of log data without the need for development, which improves the Operation & Maintenance (O&M) efficiency and the operational efficiency, and builds the processing capabilities to handle massive logs in the DT (data technology) era.

Log Service collects multiple formats of log data (including Event, Binlog, and TextLog data) in real time by using the Logtail client, apps, JS, and more. It provides real-time consumption interfaces for log data collected to servers, such as real-time index and log analysis, and generates data reports of various patterns based on analysis scenarios and index results.

5.36.1 Security isolation

Logtail supports multi-tenant isolation. Compared with mainstream open source collection agents, Logtail has a more refined architecture. A fixed number of threads is used by Logtail to discover events, read data, resolve data, and send data. Parsing threads can be configured. The number of threads does not increase when the number of configuration increases. All configurations operate in the same execution environment. Log Service uses multiple technical methods to guarantee processing isolation of configurations, fairness of scheduling configurations, reliability and controllability of data collection, and high cost performance of resources.

Logtail has the following benefits in multi-tenant isolation:

- Supports data collection scheduling based on time slices to guarantee isolation and fairness of configuration data endpoints.

- Supports multi-level feedback queues for high and low resources usage to guarantee the isolation and fairness of processing flows and configurations with quite little resources consumption.
- Supports event processing without blocking mechanism to guarantee high reliability of log service even though file rotation occurs when blocking is configured or data collection stops.
- Supports different traffic controls, collection stop policies, and dynamic updates of configurations to guarantee high controllability of data collection.

5.36.2 Authentication

To ensure security of users' log data, all HTTP requests of the Log Service API must undergo security authentication. Currently, this security authentication is based on the Alibaba Cloud AccessKey and is completed by using the symmetric encryption algorithm.

This process is as follows:

1. The requester generates a SignString based on the API request content (including the HTTP Header and Body).
2. The requester uses Alibaba Cloud's access key pair (AccessKeyID and AccessKeySecret) to sign the signature string generated in the first step, forming a digital signature for this API request.
3. The requester sends both the API request content and digital signature to the server.
4. After receiving the request, Log Service repeats steps 1 and 2 and computes the expected digital signature for this request.



Note:

Log Service retrieves the AccessKey pair used by this request from the backend.

5. The server compares the expected digital signature to the digital signature sent with the request. If they are completely consistent, the request passes security authentication. Otherwise, the request is immediately rejected.

5.36.3 Data security

Apsara Stack uses a flat design in which a linear address space is divided into slices, also called chunks. Each chunk has three copies stored on different server nodes on different racks. This guarantees data reliability.

For the data on the cloud disk, all user operations, including addition, modification, and deletion of data, are synchronized to the three copies. This mode guarantees the reliability and consistency of user data.

The data storage system of Apsara Stack involves three key components: Master, Chunk Server, and Client. To demonstrate how triplicate technology works, in this example, the write operation of an ECS user undergoes several conversions before being executed by the Client. The process is as follows:

1. The Client determines the location of a chunk corresponding to one of your write operations.
2. The Client sends a request to the Master to query the storage locations (that is, the Chunk Servers) of the three copies of the chunk.
3. The Client sends write requests to the corresponding three Chunk Servers according to the results returned from the Master.
4. The Client returns a message to the user indicating whether the operation was successful.

This strategy guarantees that all the copies of a chunk are distributed on different Chunk Servers on different racks, effectively reducing the potential of total data loss caused by failure of a Chunk Server or a rack.

If a system failure occurs because of a corrupted node or hard drive failure, some chunks may lose one or more of the three valid chunk copies associated with them. If this occurs, the Master replicates data between Chunk Servers to reinstate the missing chunk copies across different nodes.

In addition, after a deletion operation is performed, the released storage space is recycled by the Distributed File System and denies any user access. Before the space is reused, the content on the space is erased to guarantee the security of your data.

5.36.4 Transmission security

Log Service guarantees your data security in transmission by using the following methods:

- To prevent data tampering during the transmission process, the Logtail client obtains your Alibaba Cloud AccessKey and provides a signature to all log data packets to be sent, and uses the HMAC SHA1 signature algorithm for authentication.



Note:

The Logtail client uses the HTTPS channel to obtain your Alibaba Cloud AccessKey, which guarantees the AccessKey security.

- The API uses signature and authorization to ensure the security and access permission of data .
- Log Service supports the HTTPS/SSL protocol. Applying HTTPS/SSL to the network connection between a user and a server, Log Service guarantees data is not listened or stolen in transmission. The data confidentiality of communication between the user and server is also protected by the HTTPS protocol.

5.36.5 Service monitoring

Log Service monitors machine group status and Logtail log collection status in real time.

- Monitor machine group status

Log Service monitors heartbeat status of all servers in your machine group in real time. The server status includes **OK** and **Fail**. The heartbeat state, **Fail**, indicates that the machine group is in abnormal state and cannot collect logs.

- Monitor log collection status

When you use Logtail to collect logs, Log Service sends alarms through **Log Collection Error** upon errors, such as log parsing failures with regular expression, false file paths, and traffic in excess of shard capability. Alarms contain the time of error occurrence, the IP address of the server on which errors occur, number of errors, and error types.

5.37 Key Management Service (KMS)

Key Management Service (KMS) is a secure and easy-to-use management service provided by Alibaba Cloud. The confidentiality, integrity, and availability of keys are guaranteed at a low cost.

With the help of KMS, you can use keys securely and conveniently, and focus on developing encryption/decryption scenarios for users.

KMS provides multiple strict security measures to help protect your data security.

5.37.1 Security risk analysis

KMS does not involve the deployment of instances. Due to its characteristics, KMS is exposed to the following external risks:

- Data keys generated from the CMK are leaked on the client.
- Encrypted data is decrypted under improper identity authentication and authorization.
- Cryptography vulnerabilities thoroughly disable specific encryption and decryption algorithms.

Risks of KMS itself lie in the data security of stored keys.

5.37.2 Security functions

5.37.3 Security isolation

KMS does not involve the deployment of instances. This eliminates the resource isolation problem caused by instance virtualization.

The resource of KMS is customer master key (CMK). You can only use an open API to access key resources indirectly. Security isolation is implemented at the network layer of an open API.

5.37.4 Authentication

5.37.4.1 Identity verification

You can create AccessKeys in the Apsara Stack console. An AccessKey is composed of AccessKey ID and AccessKey Secret. AccessKey ID is public and used to identify your identity. AccessKey Secret is secret and used to authenticate your identity.

When you send a request to KMS, you must generate a signature string in a format specified by KMS. Then, you use AccessKey Secret to encrypt the signature string (based on the HMAC algorithm) to generate a verification code. The verification code is timestamped to prevent replay attacks. After KMS receives the request, KMS locates the AccessKey Secret corresponding to the AccessKey ID, and uses the same method to extract the signature string and verification code. If the verification code is the same as the code that you provide, KMS considers that the request is valid. Otherwise, KMS rejects the request and returns an HTTP 403 error.

5.37.4.2 Permission control

The access control of KMS is implemented through RAM. Permission policies of RAM can be used to define different identity types and grant you with KMS permissions.

KMS permissions are described through the following RAM concepts:

- **Action:** The `Action` parameter of an open API involves addition, deletion, modification, and query of keys, as well as data encryption and decryption. Each API corresponds to an action, which can be independently granted to an identity.
- **Resource:** The resource of KMS is CMK, which is identified by CMK IDs.

5.37.4.3 RAM and STS support

KMS supports RAM/STS authentication.

Resource Access Management (RAM) is a resource access control service provided by Alibaba Cloud. RAM allows you to create a subaccount under a primary account. All resources of the subaccount belong to the primary account. The primary account can assign resources to the subaccount.

Security Token Service (STS) is a temporary access credential service provided by Alibaba Cloud, which provides short-term access permission management. You can use STS to generate short-term access credentials. The permissions and validity period of the credentials can be decided by you. The credentials become invalid upon expiration.

5.37.5 Data security

KMS data is the CMKs created and managed by you. CMKs are stored by redundant RDS servers (active/standby mode). Both active and standby RDS servers have their own redundancy and backup mechanisms. Therefore, RDS can implement hierarchical redundancy for your data.

Key materials of CMKs are encrypted by the KMS system before they are stored on disks. The KMS system implements a hierarchical key structure and automatically rotates the upper-layer keys. KMS can also access the trusted platform module (TPM) to protect the hardware of the root KMS key and ensure the privacy of your data.

5.37.6 Encrypted transmission

KMS implements data transmission encryption throughout the entire lifecycle. Requests must be initiated by you to KMS through HTTPS to ensure the privacy and integrity of exchanged information.

5.37.7 Log auditing

KMS uses Log Service of Alibaba Cloud to record KMS operations. You can audit KMS operations in Log Service.

5.38 Security Isolation

E-MapReduce supports using RAM to isolate the data of different sub-accounts. By authorizing different policies to different sub-accounts, the data access scope of different users can be

controlled. Users should use the corresponding sub-accounts to log on to the E-MapReduce console. There are several restrictions when E-MapReduce access the data stored in OSS:

- All buckets can be seen in the OSS selection interface for cluster, operation, and plan execution creations, but the authorized bucket can only be entered.
- The content under authorized bucket can only be seen, rather than those under other buckets.
- The authorized bucket can only be read and written. Otherwise, an error is reported.

5.39 User Authentication

E-MapReduce supports the Kerberos authentication system, that is, open source components in the cluster are started in the Kerberos security mode. In this mode, only authenticated clients can access the cluster service such as HDFS.

Kerberos is a safe authentication system. E-MapReduce uses HAS (Hadoop Authentication Service). Currently, open-source big data (Hadoop or Spark) only supports the built-in Kerberos for security authentication. HAS provides a new authentication method (Kerberos-based token authentication). By connecting to the existing authentication and authorization systems, Hadoop or Spark can support other authentication methods besides Kerberos and make the complex Kerberos simple and transparent to the end users.

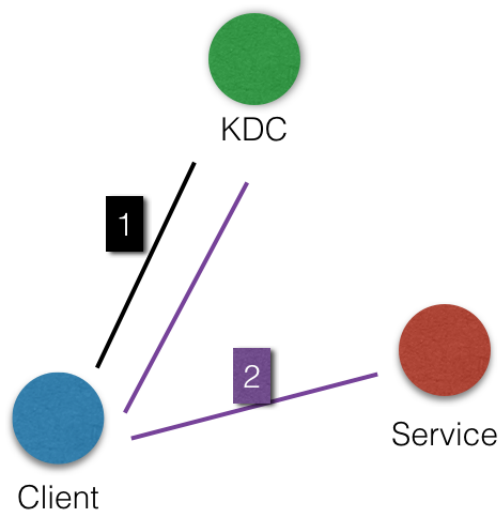
Currently, the new authentication mechanism (Kerberos-based token authentication) provided by HAS supports most components in the big data ecosystem and requires a few or no modifications on the components.

All components can use the original Kerberos authentication mechanism provided by HAS.

Kerberos Identity Authentication Principle

Kerberos is an identity authentication protocol based on the symmetric key technology. As an independent third-party identity authentication service, Kerberos can provide its ID authentication function for other services, and it supports SSO (the client can access multiple services, such as HBase and HDFS, after ID authentication).

The Kerberos protocol process is mainly divided into two stages where KDC authenticates the Client identity in the first stage, and the Service authenticates the Client identity in the second stage.

Figure 5-3: Kerberos Identity Authentication Principle

- KDC: Kerberos server.
- Client: If a user (principal) needs to access the service, KDC and Service authenticates the principal's identity.
- Service: Services that have integrated with Kerberos include HDFS, YARN, and HBase.

KDC ID authentication

Before a client user (principal) can access a service integrated with Kerberos, it must first pass the KDC ID authentication.

After passing the KDC ID authentication, the client receives a TGT (Ticket Granting Ticket), which can be used to access a service that has integrated Kerberos.

Service ID authentication

When a principal receives the TGT in step 2.1, it can access the Service. It uses the TGT and the name of the service that it must access (such as HDFS) to obtain an SGT (Service Granting Ticket) from KDC, and use the SGT to access Service, which uses the relevant information to conduct ID authentication on the client. After passing the ID authentication, the client can normally access the Service.

5.40 Permission control

After you create users, you can grant permissions on each component or to each user. Permission control is not highly related to authentication. Permission control is still effective without the authentication system.

- **HDFS authorization**

When permission control is enabled for HDFS, users need valid permissions to access HDFS for normal operations, such as reading data and creating a folder.

- **YARN authorization**

YARN authorization can be divided to service-level authorization and queue-level authorization based on the authorization entity.

- **Service-level authorization**

- Control cluster service access by specific users, such as submitting jobs
 - Configures `hadoop-policy.xml`
 - Service level permission validation has a higher priority than other permission validation procedures (such as HDFS permission verification and YARN job submission control)

- **Queue-level authorization**

YARN supports permission control over resources through queues, and it provides two queue scheduling methods, namely `Capacity Scheduler` and `Fair Scheduler`.

- **Hive authorization**

Two authorization features are built in Hive, which can be configured at the same time without conflict.

- Storage Based Authorization

- SQL Standards Based Authorization

- **HBase authorization**

Without authorization, any account can perform any operations on the HBase cluster that includes `disable table/drop table/major compact` and so on. For clusters without Kerberos authentication, users can forge identities to access to the cluster service even when HBase authorization is enabled. Therefore, we recommend that you create a cluster with high security mode (i.e. supporting Kerberos).

5.41 Account Security

StreamCompute Account Security

StreamCompute account currently supports only Alibaba Cloud account system (including `username+password`, signing key). In addition to complying with Alibaba Cloud's existing security

system, the entire transmission link uses the HTTPS protocol to make sure full-link user account security.

Data Storage Account Security

Alibaba Cloud StreamCompute uses data storage connection accounts to store data. We provide a RAM/STS based approach to avoid the disclosure of business information caused by the loss of account information.

5.42 Business Security

Project Isolation Security

Different StreamCompute projects are strictly isolated based on permission. Access to and operations of another user/project (including all sub-products of the project) is not allowed.

Resources isolation at the project level ensures users use resources independently. For example, when you run your task and cause a sharp increase in data flow, you cause higher job CPU usage. Alibaba Cloud StreamCompute uses virtualization technologies at the bottom layer for resources isolation, ensuring that your higher CPU usage does not impact other users' jobs.

Business Process Security

StreamCompute strictly defines stream computing and development by separating data development and data operation and maintenance. This guarantees a complete and secure business process while minimizing adverse effects on user experience.

- Providing code version: supports version rollback and comparison for users to trace, compare, and identify errors in code.
- Providing single IDE debugging container: prevents running code offline from influencing actual online data. You can construct data yourself for input tables, dimension tables, and output tables, to prevent offline task debugging from impacting online production tasks.
- Providing release procedures: prevents offline code modification from directly impacting production. After debugging, you can start your task and submit your job to the data operation and maintenance system. The running StreamCompute task does not directly use the new code. You must first give confirmation, stop the running task, and start it again with the new code, forming a strict code release process.

5.43 Data Security

Data security can be divided into system data security and business data security.

System Data Security

StreamCompute takes responsibility for its own data security by implementing a series of measures.

- All access links use HTTPS to make sure transmission link security.
- High-security AES encryption is applied to data storage links to ensure that sensitive information is not leaked.
- Alibaba Cloud's security team ensures the security of StreamCompute by implementing comprehensive and in-depth attack testing.

Business Data Security

StreamCompute does not store business data of users, and various Alibaba Cloud storage systems are responsible for business data security. See different data storage security models and best security practices for more information.

6 Apsara Stack Security

Apsara Stack Security uses the powerful computing capacity of the Apsara Stack computing platform to provide one-stop security solutions to users, including defense against DDoS and host intrusion, Web Application Firewall, and Situation Awareness.

6.1 Apsara Stack Security Basic Edition

Apsara Stack Security Basic Edition provides traffic security monitoring, server guard basic edition, host intrusion detection, and security audit.

Traffic security monitoring

Traffic security monitoring is a millisecond(ms)-level attack monitoring product independently developed by Apsara Stack. With in-depth analysis of incoming traffic packages in the private cloud environment, this module can detect attacks and abnormal behaviors in real time. It then combines with other Apsara Stack Security modules to fully protect your system. Traffic security monitoring provides robust information and data support to the whole Apsara Stack Security defense.

Traffic security monitoring includes:

- **DDoS attack detection:** detects DDoS attacks in cloud boundary traffic using traffic mirroring.
- **Traffic statistics:** measures the inbound and outbound traffic of ISW and generates traffic graphs.
- **Network-layer web attacks interception:** interception and bypass blocking of common web attacks at the network layer based on the built-in web matching rules.

Best Practices

By reviewing the traffic over different periods for different zones, or IPs, you can identify the traffic distribution, including peak times, quiet periods, speed, and region. In addition, you can effectively mitigate attacks from malicious IP access using TOP5 IP traffic.

Host intrusion detection

Host intrusion detection, independently developed by Apsara Stack, provides security protection tailored for physical servers in the Apsara Stack environment. By default, Host intrusion detection agents deployed on the servers are linked with other security modules in the Apsara Stack Security security system to provide a variety of security protection functions.

Best Practices

Host intrusion detection allows you to check for host file tampering, abnormal processes, abnormal network connections, and abnormal port monitoring records. This provides timely identification and fixing of potential security risks at the host layer.

Server Guard Basic Edition

Through log monitoring, file analysis, and feature scanning, Server Guard Basic Edition provides brute force attack protection, webshell scanning and killing, and remote logon alarm for ECS servers. Server Guard Basic Edition consists of agents and server, and Server Guard agents work together with Server Guard server to monitor attacks at system-layer and application-layer, in order to discover intrusion behaviors.

Best Practices

Server Guard Basic Edition helps discover and block brute force attacks against ECS servers, which ensures the host security of ECS servers.

Security audit

Security audit is a systematic, independent process of inspecting and verifying relevant activities or behaviors in the Apsara Stack environment. It is followed by corresponding opinions from professional auditors entrusted by property owners and authorized by administrative authorities, based on relevant laws and regulations. Security audit can help a system administrator backtrack past operations in the system.

Apsara Stack's security audit collects system security-related data, analyzes the vulnerable points in system operations, and reports audit events. It classifies them into three groups: high risk, medium risk and low risk. The administrator can analyze audit events to constantly improve the system and ensure secure and reliable cloud service.

- Security audit covers multiple business and physical hosts in the Apsara Stack environment. It collects behaviors from a variety of sources to guarantee sufficient coverage for auditing. The log collection center collects and recovers logs in a centralized, real-time, and synchronized manner.
- Audit logs are stored using the cloud storage service. Three back-ups are kept to ensure security and stability. Storage space can also be rapidly expanded.
- By constructing full-text indexes for massive log data, the security audit module is able to quickly search for and query massive amounts of data.

Best Practices

Based on the defined audit strategy, administrators can receive warning emails in a timely manner. For example, if a high risk event-oriented audit strategy is set up for attempts to log in the ECS log, the set administrators will receive warning emails when relevant content appears in the ECS log.

6.2 Apsara Stack Security Advanced Edition

Apsara Stack Security Advanced Edition includes all the functions of the Basic Edition, in addition to Server Guard Advanced Edition, DDoS Cleaning, Web Application Firewall (WAF), Cloud Firewall, Bastion Host, and Situation Awareness. Together with Alibaba Cloud's professional security operations services, Apsara Stack Security provides you with an all-in-one security assurance product, combining intrusion protection, security audit, situation awareness, and centralized management.

Server Guard Advanced Edition

Server Guard Advanced Edition provides security protection measures such as vulnerability management, baseline test, intrusion detection, and asset management for ECS instances by means of log monitoring, file analysis, and feature scanning. Server Guard is divided into clients and servers. Server Guard clients work with Server Guard servers to monitor attack behavior, vulnerability information, and baseline configurations at the system layer and application layer, protecting the security of ECS instances in real time.

Server Guard Advanced Edition includes the following features:

- Uses log monitoring, file analysis, feature scanning, and other techniques to provide brute-force account cracking protection, webshell detection and removal, remote logon alerts, and other anti-intrusion measures.
- Provides targeted protection against brute-force cracking for SQL Server, MySQL, SSH, RDP, FTP, and other services.
- Provides remote host logon alerts.
- Provides high-risk host vulnerability detection and repair.
- Provides security baseline check for hosts.

Best practices

Use Server Guard to periodically perform baseline detection for ECS instances, detect security threats and vulnerabilities on hosts, and repair them promptly for higher host security.

DDoS cleaning

DDoS cleaning is an Apsara Stack Security product for protection against massive DDoS attacks . Alibaba Cloud relies on its self-developed, large-scale, distributed operating system and more than a decade of defense experience to provide a wide range of Apsara Stack platform users with DDoS cleaning, designed and developed based on its cloud computing architecture.

DDoS cleaning includes the following features:

- **Cleaning against DDoS attacks:** Defends against SYN flood, ACK flood, ICMP flood, UDP flood, NTP flood, DNS flood, and HTTP flood.
- **DDoS attack viewing:** Allows you to view DDoS attack events on the GUI and search for DDoS attack events by IP address, status, and event information.
- **DDoS traffic analysis:** Allows you to analyze the traffic of a DDoS attack, view the traffic protocol of the DDoS attack, and display the top 10 IP addresses of this attack event.

Best practices

The DDoS cleaning module automatically detects and protects against DDoS attacks targeted at public IP addresses on the Apsara Stack platform. When the platform is under DDoS attacks, the DDoS cleaning module works with the network traffic monitoring module for traffic detection and scheduling to channel, clean, and reinject network traffic, effectively cleaning the attack traffic. In addition, you can view the detailed information about a DDoS attack event to know the traffic elements of the attack event and analyze the attack source on the DDoS cleaning module.

Web Application Firewall

Based on the powerful big data capabilities of cloud security, WAF defends against SQL injection , XSS, common web server plug-in vulnerabilities, trojan uploads, unauthorized access to core resources, and other common OWASP attacks. It filters out massive numbers of malicious accesses to prevent the leakage of your website assets and data and safeguard website security and availability.

WAF is mainly used to distribute web traffic to WAF, where WAF detects, filters, and cleans the traffic and forwards it to the application server as a proxy to complete the web application protection.

Best practices

- **Prevent leakage of sensitive information with WAF**

The anti-leakage feature mainly protects against the leakage of sensitive information on websites, especially the filtering of information such as mobile numbers, ID numbers, and credit card numbers. WAF effectively defends against security threats such as the access by unauthorized URLs, unauthorized view of vulnerabilities, and malicious crawling of sensitive information on websites.

- **Prevent WordPress reflection attacks with WAF**

WAF prevents WordPress reflection attacks effectively with precision access control rules.

Cloud Firewall

Cloud Firewall is a firewall product used in cloud environments and solves the problem of vague security boundaries or failures to find security boundaries amid the rapid changes of cloud businesses. Cloud Firewall uses the groundbreaking techniques of business organization and business isolation based on visualized business results to implement secure access control on east-west traffic in the Apsara Stack environment.

Best practices

- **Implements micro-isolation:** Cloud Firewall supports fine-grained micro-isolation. It manages ports that must be enabled to prevent interrupted services in a more fine-grained manner through service partitioning and role grouping, reducing attacks and security risks.
- **Checks whether traffic is secure:** For example, information such as whether HTTP traffic has been changed to HTTPS traffic, or whether the traffic destined for TCP 3306 (service port of MySQL) includes traffic from the Internet is clearly displayed on the traffic view of Cloud Firewall.
- **Determines whether server changes affect services:** When servers are to be migrated or shut down, you can check whether the related traffic exists on Cloud Firewall and determine whether the servers can be securely changed.
- **Detects port misuse:** Different service development departments may use different ports of the same service (same applications and processes) provided by the server. In this case, port resources are wasted, and O&M becomes more difficult. Through visualized traffic, Cloud Firewall can clearly detect port misuse.

Situation Awareness

Situation Awareness uses machine learning and data modeling to find potential infiltration and attack risks. From the attacker's perspective, it effectively captures zero-day vulnerability attacks mounted by advanced attackers and new virus attacks, and displays ongoing security attacks. It

also effectively presents this information, keeping you aware of business security in a visual way. This solves the problem of data leaks due to cyberattacks and allows you to discover the hacker's identity using the tracing service.

- **Vulnerability analysis:** Vulnerability analysis is based on the stateless scan technology. In coordination with the network traffic security module, it relies on a combination of dynamic detection and static matching scanning modes to provide you with automated, high-performance, and precise web vulnerability scanning capabilities.
- **Big data security analysis platform:** Situation Awareness uses machine learning and data modeling to find potential infiltration and attack risks. From the attacker's perspective, it effectively captures zero-day vulnerability attacks mounted by advanced attackers and new virus attacks, and displays ongoing security attacks. It also effectively presents this information, keeping you aware of business security in a visual way. This solves the problem of data leaks due to cyberattacks and allows you to discover the hacker's identity using the tracing service.

Best practices

Situation Awareness provides features such as asset management, security monitoring, intrusion backtracking, hacker locating, and intelligence warning. We recommend that you use Situation Awareness to keep yourself aware of cloud service security in a visual way in the following scenarios:

- **Vulnerability scanning**

You can promptly detect host and application vulnerabilities by vulnerability scanning and fix the vulnerabilities in time. In the vulnerability scanning module, you can add custom weak password libraries to improve password strength on the Apsara Stack platform in a targeted way, enhancing the security of the platform accounts and application services.

- **Security situation awareness**

You can be fully aware of the security situation of cloud services, such as attacks, vulnerabilities, intrusions, protection effect, service weaknesses, and the security status of services available for external use on the host. Situation Awareness provides features like recognition of cyberattacks and host attacks, detection of abnormal network connections, recognition of advanced persistent threat (APT) attacks, recognition of security threats at the business layer, and sending of daily security reports.

- **Countermeasures against intrusions**

When your cloud business is intruded, for example, a sudden increase in host load and you are alerted by SMS that your ECS instance is being intruded, attacks initiated from your hosts, malicious advertisement links displayed on your webpages, or your data encrypted by a hacker asking for Bitcoins as a ransom, you can use the following features of Situation Awareness:

- **Intrusion detection:** Tens of intrusion behaviors can be detected, including WannaCry ransomware, intrusion through the webshell backdoor, one-statement Trojan horse, software viruses, and connection between the host and central control source.
- **Intrusion behavior analysis:** Situation Awareness can analyze the cause and process of intrusion and collect evidence of hackers' behaviors on the full link.
- **Details of security events:** You can view DDoS attack protocol analysis, backdoor addresses, process addresses, attack prevention effect, and other information.
- **Log analysis**

Situation Awareness provides a fully SaaS-based log retrieval platform, which is free of installation and maintenance and can be used out-of-the-box. The platform supports features such as logic-based (Boolean expression) retrieval, combinations of data logic in 50 dimensions, and a retrieval engine that outputs results in seconds to perform the following actions:

- **Log analysis:** Inspects the log evidence and evaluates the asset damaging scope and impact.
- **Operation audit:** Audits the operation logs of the host server and troubleshoots risky operations.
- **Service statistics:** Collects statistics on and analyzes web access logs and traces the environment and status of visitors.
- **Real-time monitoring on a big screen**

Situation Awareness provides multiple big visualized screens on which you can monitor the cloud security situation in real time, improve the teamwork efficiency, and display and report the security situation.

- **Code leakage awareness**

The intelligence collection system of Situation Awareness captures data on the code hosting websites using network crawlers and monitors and reports enterprise-related intelligence in real time. The system prevents data leakage caused by management problems of the enterprises (for example, the database connection address and password and server logon password

are directly leaked from the company's source code uploaded to a code hosting platform such as Github). In addition, Situation Awareness provides users with related intelligence content , including intelligence of data leakage, username and password leakage, the deep web, and attack plans from IM groups.

Bastion Hosts

Bastion Hosts provide complete audit playback and permission control services for O&M of ECS instances. Based on the AAAA solution that centrally manages accounts, authentication, authorization, and audit, bastion hosts improve the security of O&M management through features such as identity management, authorization management, two-factor authentication, monitoring and disconnection of real-time sessions, audit video playback, and risky command query.

Best practices

- **Scenarios that have strict audit requirements**
 - Isolation of department permissions: Effectively manages and audits O&M information about each department based on isolated department permissions.
 - Central O&M portal: Provides a central O&M portal for O&M personnel to centralize scattered logons.
 - Compliance with audit requirements: Builds a robust cloud-based O&M audit mechanism that meets the industrial monitoring requirements.
- **Efficient and stable O&M management scenarios**
 - Highly concurrent sessions: Supports concurrent sessions containing thousands of people.
 - Stable operation: Has a highly stable SLA-based assurance.
 - O&M fault backtrace: Builds O&M principles by backtracing operations when the O&M personnel have misoperations.