# Alibaba Cloud
# Apsara Stack Agility SE

## Security Whitepaper

**Version: 1912, Internal: V3.1.0**

**Issue: 20200311**

# 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, consequent**

ial, 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.

# Document conventions

| Style | Description | Example |
| --- | --- | --- |
|  | A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results. |  **Danger:**<br>Resetting will result in the loss of user configuration data. |
|  | A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results. |  **Warning:**<br>Restarting will cause business interruption. About 10 minutes are required to restart an instance. |
|  | A caution notice indicates warning information, supplementary instructions, and other content that the user must understand. |  **Notice:**<br>If the weight is set to 0, the server no longer receives new requests. |
|  | A note indicates supplemental instructions, best practices, tips, and other content. |  **Note:**<br>You can use Ctrl + A to select all files. |
| > | Closing angle brackets are used to indicate a multi-level menu cascade. | Click Settings > Network > Set network type. |
| **Bold** | Bold formatting is used for buttons, menus, page names, and other UI elements. | Click **OK**. |
| `Courier font` | Courier font is used for commands. | Run the `cd /d C:/window` command to enter the Windows system folder. |
| *Italic* | Italic formatting is used for parameters and variables. | `bae log list --instanceid`<br>*`Instance_ID`* |
| [] or [a\|b] | This format is used for an optional value, where only one item can be selected. | `ipconfig [-all\|-t]` |

| Style | Description | Example |
| --- | --- | --- |
| **{} or {a\|b}** | **This format is used for a required value, where only one item can be selected.** | `switch {active\|stand}` |

# Contents

# 1 Overview

**Data security and user privacy are top priorities of Alibaba Cloud Apsara Stack. Alibaba Cloud is 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 economies of scale to turn cloud computing into the infrastructure of true sense.**

**Apsara Stack is designed to provide users with stable, reliable, secure, and compliant cloud computing basic services and protect the availability, confidenti ality, and integrity of users' systems and data.**

**This document introduces the Apsara Stack security system in the following parts:**

- **Attribution of security power and responsibilities and security capacity co-construction**
- **Security compliance**
- **Security of the Apsara Stack platform architecture**
- **Security features provided by Apsara Stack products**
- **Security services provided by Apsara Stack Security**

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

# 2 Attribution of Apsara Stack security power and responsibilities and construction of Apsara Stack security capabilities

## 2.1 Attribution of security power

**The products, design, model algorithm, programs, and its relevant intellectual property provided by Alibaba Cloud in various types of Apsara Stack environment all belong to Alibaba Cloud unless the contract stipulates clearly otherwise. Users have the access rights within the time period authorized by License.**

**The national standard** *GBT 31167-2014 Information Security Technology - Cloud Computing Service Security Guide* **(this document puts forward the national standard of the security control solution for the government to use cloud service. It has four deployment forms of cloud computing including Apsara Stack (private cloud). Other customers can also regard this standard as a reference when using Apsara Stack service) stipulates that "the customer owns the data, device, and other resources that the customer submits to cloud provider. The customer also owns the data and document collected, produced, and stored by customer business system on the cloud computing platform. The right of the customer to visit, use, and dominate these resources must not be limited."**

**In Apsara Stack environment, users are entitled to the ownership of the user data of project planning and implementation, the operation data produced during operations, and the business data that are transferred to the cloud environment . Alibaba Cloud can access the data within the scope of users' authorization, and cloud users must avoid authorizing business data to Alibaba personnel.**

## 2.2 Construction of Apsara Stack security capabilities

### 2.2.1 Security responsibilities of Alibaba Cloud

**In Apsara Stack environment, Alibaba Cloud is responsible to provide users with cloud computing products and solutions, help users with customized deployment**

**, or facilitates operations within the scope of the contract. Alibaba Cloud takes the following responsibilities:**

- **Provides users with security testimonial for compliance requirement of Alibaba Cloud Apsara Stack.**
- **Provides the vulnerability recognition service and technology for Apsara Stack products and helps users fix Apsara Stack on the product side.**
- **Protects users' Apsara Stack information system or infrastructure and provides relevant solutions and techniques, including authorization management, encryption, and auditing feature. Based on the preceding solutions and methods , Alibaba Cloud provides best practices of security management for users and puts forward the security capacity building.**
- **According to Alibaba Cloud security regulation and customer's requirement, the Alibaba Cloud personnel is required to sign the confidential agreement and receive proper security training and education.**

## 2.2.2 Security responsibilities of users

**The national standard** *GBT 31167-2014 Information Security Technology - Cloud Computing Service Security Guide* **stipulates that "the responsibility of information security control must not transfer to the outsourcing service partner. No matter the customer data and business are placed in the customer internal information system or on the cloud computing platform of the cloud service provider, the customer holds the responsibility for the information security." In Apsara Stack environment, the user exercises the security control based on the security solutions and technology provided by Alibaba Cloud or the third party and takes the following responsibilities for the results:**

- **Establishes the security control personnel, organization, security system, and operation system, which all support the Apsara Stack environment. The control object includes relevant project members of Alibaba Cloud.**
- **Practices admittance examination, confidentiality agreement, security training and education for relevant project members of Alibaba Cloud in the Apsara Stack environment, according to the national law, regulation, and customer requirements.**

- **Executes the transfer control for code and program in the Apsara Stack environment and takes responsibility for data leakage that is caused by users' fault.**
- **Leads the vulnerability fix process for Apsara Stack products, reviews the relevant implementation plan, and authorizes the change of plan during the upgrade process.**
- **Implements the account assignment, authorization, and log audit in each console in the Apsara Stack environment. Manages to achieve minimized authorization and normalized audit.**
- **Implements the security configuration of each console and products in the Apsara Stack environment, or authorizes the Alibaba Cloud field personnel to perform the security configuration.**
- **Users must perform backup and recovery drills for key data on regular basis to guarantee the business data is backed up and can be restored.**

# 3 Security compliance

## 3.1 Overview

**The security process of Alibaba Cloud has been recognized by authorities inside and outside China. By using years of expertise in defense against Internet security threats of Alibaba Group, 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. Alibaba Cloud also participates in the development of standards for various cloud platforms and contributes the best practices. Certified by more than 10 agencies inside and outside China currently, Alibaba Cloud is a cloud service provider with the most complete scope of certifications in Asia.**

**Certified by more than 10 agencies in and outside China, Alibaba Cloud is the cloud service provider with the most complete range of certifications in Asia. Alibaba Cloud has certifications as listed inAlibaba Cloud has the following qualifications.**

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. |

| Certification | Description |
| --- | --- |
| 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 can improve IT 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. |
| Classified protection (level 4) | Alibaba Cloud Apsara Stack platform complies with the security and technology capabilities that are requested by Cloud computing platform classified protection 2.0 compliance specifications (level 4), which is formulated in accordance with GB/T22239 - 2019 *Information security technology - Baseline for classified protection of cybersecurity*. |
| 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. |
| Service Organization Control (SOC) audit certification | Alibaba Cloud has passed SOC3 audit, and the TYPE II of SOC1 and SOC2. |

Table 3-2: List of domestic Apsara stack qualifications

| Qualifications/certification | Certification authority |
| --- | --- |
| ITSS cloud computing service capability (private cloud IaaS service/level 1) | Chinese Electronics Standardization Association |
| Trusted cloud - the protection of the user data of cloud service (private cloud) | China Academy of Information and Communications Technology |

| Qualifications/certification | Certification authority |
| --- | --- |
| Security level assessment report of the information system of the Ministry of Public Security(level 4, private cloud) | Information security rating center of the Ministry of Public Security |
| Security classified protection evaluation report of the Ministry of Public Security Information System Apsara stack V3.0 | Information security rating center of the Ministry of Public Security |
| Security assessment report of big data simple Apsara Stack platform of the security of the information system of Ministry of Public Security | China Academy of Information and Communications Technology |
| Cloud evaluation certificate-Cloud computing reference architecture-cloud solution | China Electronics Standardization Institute |
| Trusted cloud-open-source solutions ( agile private cloud version)/virtualization and virtualization management software | China Academy of Information and Communications Technology |

## 3.2 Security compliance

**Alibaba Cloud keeps improving its management and system based on relevant standards and best practices in the industry. It is certified in a series of standard certifications, third-party audits, and self-assessment, which aims to better demonstrate its compliance practices to users.**

**The overall compliance architecture of Alibaba Cloud is divided into the following parts according to compliance requirements from different perspectives, industries , and regions:**

### Management system compliance

**These compliance authentications demonstrate the mature management system of Alibaba Cloud and the best industry practices that Alibaba Cloud complies with:**

- **ISO 27001: Information Security Management Standard**
- **ISO 20000: IT Service Management Standard**
- **ISO 22301: Business Continuity Management Standard**
- **CSA STAR: maturity model of cloud service security**
- **Classified protection (level four)**

- **CNAS test for cloud computing standards in China**

Systematized compliance reports

**These compliance authentications demonstrate the integrity and effectiveness of control in Alibaba Cloud platform, including the continuous effectiveness of system control, accuracy of separation of duties, and completeness of operations audit.**

**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 the key compliance control and objectives of Alibaba Cloud. 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 three types:**

- **SOC 1 TYPE II: internal control report over financial reporting**
- **SOC 2 TYPE II: reports over security, availability, and confidentiality**
- **SOC 3: report over security, availability, and confidentiality**

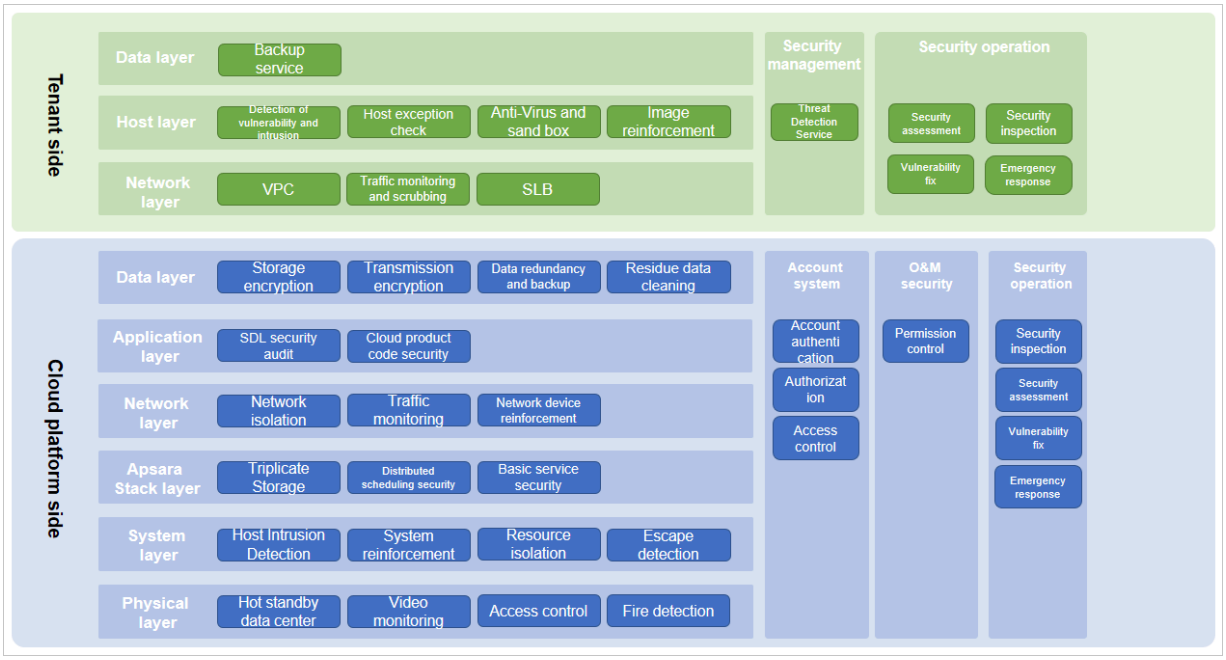
## 3.3 Alibaba Apsara Stack classified protection 2.0 compliance whitepaper

**According to** *Cloud Computing Security Classified Protection Compliance Capability Framework* **, and under the guidance of China's technology community of the cloud computing security classified protection compliance capacity specification system, Information security rating center of the Ministry of Public Security and Alibaba Cloud Computing Co., LTD. jointly compiled and issued** *Apsara Stack Network Security Classified Protection 2.0 Compliance Capability Whitepaper* **. The whitepaper explains in details from the technical verification architecture of classified protection capability, the compliance status of Apsara stack classified protection 2.0 to the usage recommendations for the whitepaper. With this whitepaper, customers can quickly obtain compliance protection on the Apsara stack platform side in multiple delivery scenarios. It also integrates customer-side application, security management, and protection measures such as physical environment, to jointly construct an overall security defense system of information systems to meet the needs of classified protection and customers.**

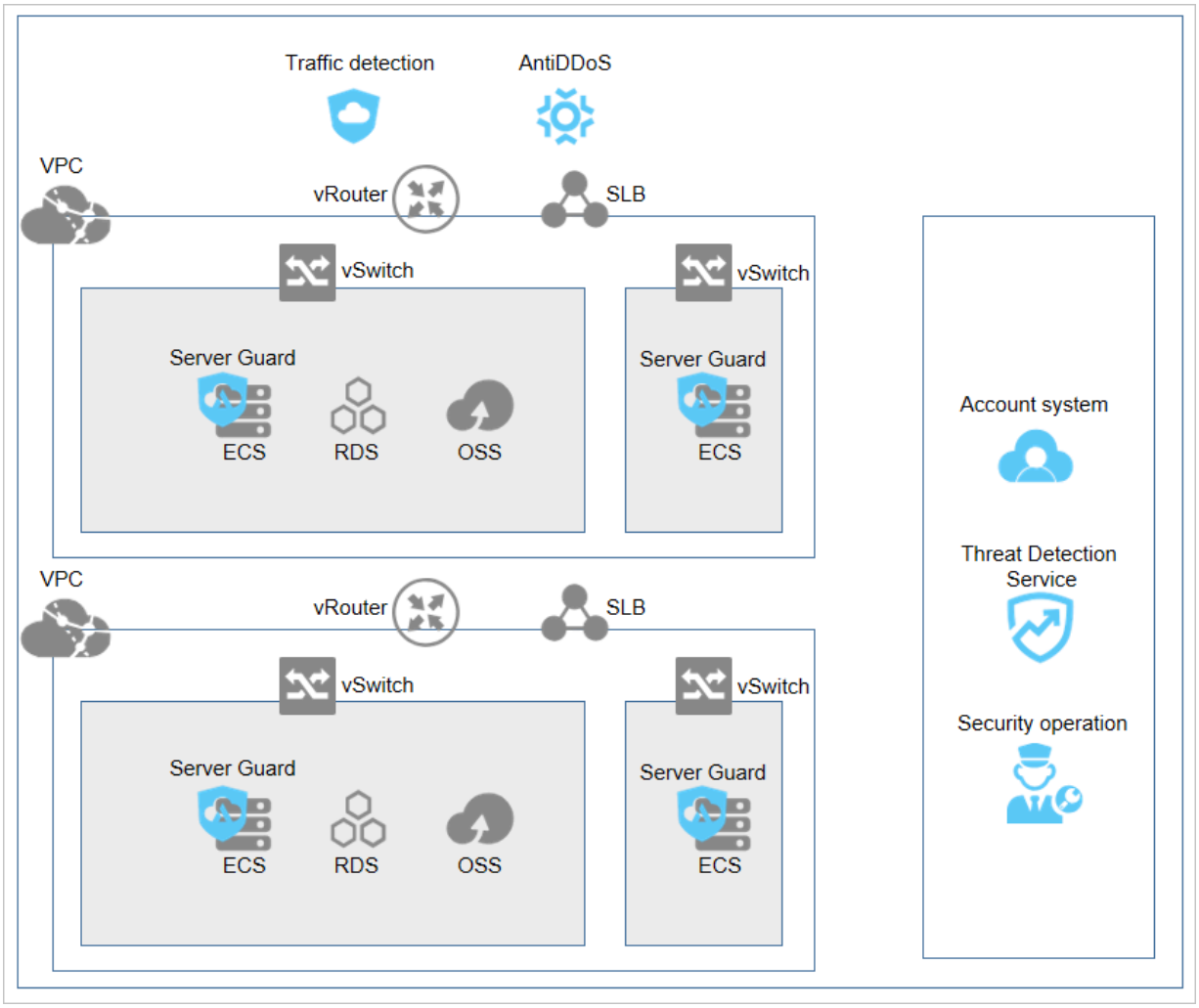
# 4 Apsara Stack security architecture

## 4.1 Apsara Stack security architecture

**Apsara Stack is designed with an in-depth multi-layer security defense system and provides security assurance of architecture on the cloud platform side, including infrastructure, system, distributed Apsara system security, network, application, database, cloud platform account, O&M, and operation service, and also on the cloud users (tenants) side, including network, host, application, data, and operation service.**




**In the Apsara Stack environment, the security deployment condition of each security product is shown as follows.**




## 4.2 Apsara Stack platform security

### 4.2.1 Apsara Stack infrastructure security

**The requirements for the physical security of Apsara Stack data centers include 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 the**

**entry/exit of personnel and devices in the data center and also for the configuration , start-up, 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 alert 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 alert system , including the automatic fire detector, regional alert, and centralized alert and controller. The automatic fire alert system sends alert 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.**

## 4.2.2 System security

### 4.2.2.1 Physical host system security

**Alibaba Cloud reinforces the security of Apsara Stack physical servers in many aspects such as account security, file permission, system service, and Host Intrusion Detection.**

Account security

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

File permission

**Monitors the 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 surface on the servers.**

Apsara Stack Security - Host Intrusion Detection

**Deploys the Host Intrusion Detection System (HIDS) module of Apsara Stack Security on the servers to detect abnormal processes, ports, and behaviors.**

**For more information about Host Intrusion Detection module, see Features > Apsara Stack Security Standard Edition > Server Intrusion Detection in** *Apsara Stack Security Technical Whitepaper* **.**

### 4.2.2.2 Virtualization system security

**Virtualization lays the technological 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. Virtualization security technology of Alibaba Cloud involves 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 isolates virtual machines that have multiple computing nodes at the system layer. Tenants cannot access unauthorized resources to guarantee the basic computing isolation between computing nodes. The virtualization management layer also provides storage isolation and network isolation.**

- **Computing isolation**

  **The Apsara Stack platform provides various cloud-based computing services including 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 users' needs. The computing isolation is directly provided by Hypervisor, and the key computing isolation boundaries are between the management system and users' virtual machines, and also between users' virtual machines. In the virtualized environment of Apsara Stack**

platform, user instances run as standalone virtual machines. The isolation is enforced with physical processor-level permissions to avoid unauthorized users ' virtual machines to access physical hosts and the system resources on other users' virtual machines.

- Storage isolation

  In the basic design of cloud computing virtualization, Alibaba Cloud separates computing based on virtual machine 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. This realizes security isolation of hard disk space between virtual machines. After the releasing of a user instance server, the original disk space is reliably cleared to guarantee the user data security.

- Network isolation

  To guarantee the network connections of virtual machine 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 other virtual networks. This isolation prevents the network traffic data being accessed by other instances during deployment.

Escape detection

A virtual machine takes two steps to perform escape attack: first it 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 virtualization management of Apsara Stack platform uses the advanced virtual machine layout algorithm to prevent virtual machines of malicious users from running on specific physical machines. At the software level of virtualization management, Alibaba Cloud also provides reinforcement, attack detection, and hotfix of 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 and then avoid affecting users' business.**

## 4.2.3 Distributed System (Apsara) Security

### 4.2.3.1 Security of distributed file system

**The distributed file system adopts triplicate technology to store data in the system . If one of the three copies is lost, system automatically performs copy operation to maintain the three copies in the system all the time. The three copies are stored in the same physical storage medium according to security policy. They are kept separatly for operation.**

**All the access operation of the distributed file system must be certified by the Capability. Only the access with approved Capability is allowed to communicate with the system, which avoids unauthorized access operation.**

**Data stored in the distributed file system adopts binary format to avoid information leakage caused by the direct access to the plain information.**

### 4.2.3.2 Security of remote process call module

**The remote process call module adopts binary format for remote communication in Apsara Stack operation system. This guarantees an efficient and secure transmissi on and also guarantees that even if data is hijacked by any intermediary, data cannot be restored.**

### 4.2.3.3 Security of job scheduling module

**The job scheduling module isolates programs by using the method of sand box.**

### 4.2.3.4 Security of basic service module

**Basic service module deploys specific security measures for NTP and DNS servers, such as DDos attack protection, DNS zone forward, DNS amplified attack defense, and NTP amplified attack defense.**

## 4.2.4 Network security

### 4.2.4.1 Basic network security

Logical 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. Apsara Stack platform also takes network control measures to prevent unauthorized devices from connecting to the internal network of the cloud platform and prevents the physical servers of the cloud platform from connecting to external devices.**

Anti-IP/MAC/ARP spoofing

**IP/MAC/ARP spoofing always challenge traditional networks. Hackers use IP/MAC /ARP spoofing to disturb the network environment and intercept network secrets . The Apsara Stack platform 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 of the server, and avoids IP spoofing of the server on the network layer of the host.**

Apsara Stack Security - Traffic Security Monitoring

**Traffic Security Monitoring module is a millisecond(ms)-level attack monitoring product that is developed independently by Alibaba Cloud security team. With an in-depth analysis of incoming image traffic packages in the Apsara Stack environment, this module can detect various attacks and abnormal behaviors in real time.**

**For more information about the Traffic Security Monitoring module, see Features > Apsara Stack Security Standard Edition > Traffic Security Monitoring in** *Apsara Stack Security Technical Whitepaper* **.**

### 4.2.4.2 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 the reading configuration accounts from changing configuration accounts.**
- **Uses the centralized control policy to manage accounts in a unified manner.**
- **Uses multi-factor authentication to guarantee the account security for network devices.**

Services

**Disables services on network devices to reduce attack surface of the network devices and disables features uncorrelated to the network devices.**

Log centralization

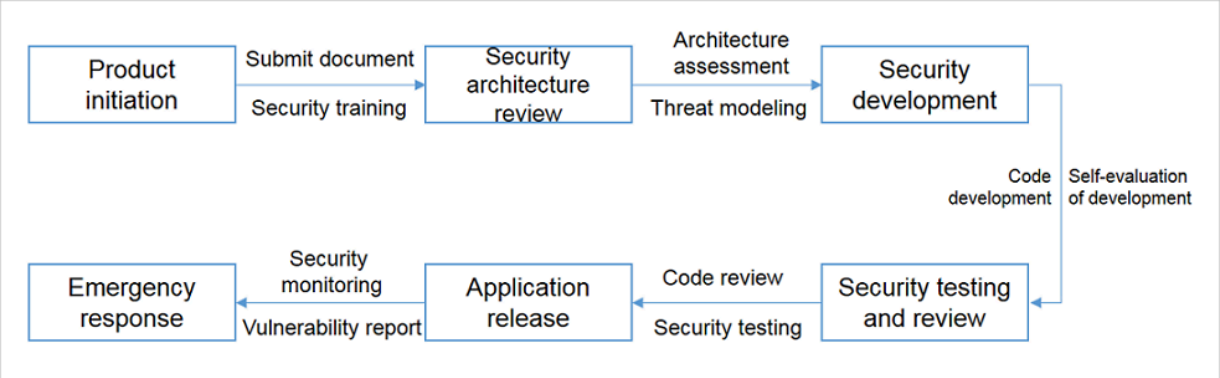
**Collects and manages logs generated by network devices in a centralized manner.**

## 4.2.5 Application security

### 4.2.5.1 Secure Product Lifecycle (SPLC)

**Secure Product Lifecycle (SPLC) is tailored by Alibaba Cloud for cloud products, which aims to integrate security into the entire product development lifecycle. With SPLC, a complete security review module is implemented at each node from product architecture review, development, test review, to emergency response. This makes sure that the product security performance can meet the strict cloud security requirements, effectively improves security capabilities of cloud products, and reduces security risks.**

**The entire SPLC of a cloud product can be divided into the following six phases: product initiation, security architecture review, security 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* **that is applicable to the product scope from all the security baseline requirements for the this Apsara Stack product. In this phase, specific security training courses and exams are also arranged for the product team memebers to avoid obvious security risks in subsequent product development.**
- **In the security architecture review phase, the security architect evaluates the security architecture of products and creates threat models of the products based on the FRD and architecture diagram established in the preceding phase. 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 security 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 a 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* **is 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 fix 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 vulnerabil ities 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 allocates resources appropriatly to quickly fix vulnerabilities. This guarantees the security of Alibaba Cloud and its users.**

## 4.2.6 Data security

### 4.2.6.1 Data security system

**Alibaba Cloud develops its data security system comprehensively and systematic ally 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 corresponding security management systems and security technologies at each stage of data security lifecycle.**

### 4.2.6.2 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 developers, companies, governments, and social institutions on the cloud computing platforms all belongs to the users. The cloud computing platforms cannot use the data for other purposes. Platform providers have responsibility and obligation to help users protect the privacy, integrity, and availability of their data.**

### 4.2.6.3 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 data reliability and security.**

#### 4.2.6.4 Full-stack encryption

**Apsara Stack provides full-stack encryption to guarantee the data security, namely sensitive data encryption in applications, transparent data encryption in ApsaraDB for 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.**

#### 4.2.6.5 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.**

#### 4.2.6.6 Operations data security

**Without the permission of users, operations personnel cannot access unpublished data of users in any way.**

**Complying with the principle that production data stays within the production clusters, the Apsara Stack platform technically controls the channels where the production data flows out of the production clusters. This prevents the operations personnel from copying data from the production system.**

### 4.2.7 Account system security

#### 4.2.7.1 Overview

**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 audit operation of RAM users. Users can use these measures to protect their cloud accounts.**

#### 4.2.7.2 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 to 20 characters in length and**

containing at least two types of the following characters: English uppercase or lowercase letters (A to Z or a to z), numbers (0 to 9), or special characters (such as exclamation marks (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%)).

### 4.2.7.3 Apsara Stack account

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

An Apsara Stack account is the basic unit for the Apsara Stack resource ownership and the resource usage measurement. A user must register an Apsara Stack account before using Apsara Stack services. An Apsara Stack account has full permissions to all the resources it owns. By default, a resource can only be accessed by the Resource Owner. 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 administrator account of an operating system. Sometimes the Apsara Stack account is called the root or primary account.

An authorized Apsara Stack account can have management permissions of the cloud resources or operations permissions of the cloud platform. The operations 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 system of primary account and RAM users.

### 4.2.7.4 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.

### 4.2.7.5 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 the accounts operation permissions to their resources. If multiple users collaboratively work with resources, RAM allows you to avoid sharing the password or AccessKey of your Apsara Stack account with other users. You can grant users the minimum permissions as required to reduce information security risks.**

#### RAM user identity types

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

- **RAM-User**

  **A RAM-User is a physical 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 physical identities before it becomes available. For example, it can be associated with RAM-Users under the current or another Alibaba Cloud account, with Apsara Stack services such as Elastic Compute Service (ECS), and with external physical identities such as a local enterprise account.**

#### Permissions

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

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

- **Resource control operations are operations for lifecycle management and Operation and Maintenance (O&M) management of cloud resources, such as creating, pausing, and restarting Elastic Compute Service (ECS) instances, and creating, changing, and deleting Object Storage Service (OSS) buckets.**

**Resource control is generally oriented to resource owners or O&M personnel 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 applications or R&D personnel 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, resource control operations and resource use operations can be both managed by using RAM .**

Authorization policies

**An authorization policy is a type of simple language specification that describes a permission 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 and cannot change the policies, and the platform updates the policy versions automatically. For custom access policies managed by users, users can create and delete policies 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 permission s. The administrator can allocate one or more authorization policies to RAM users (namely RAM-User and RAM-Role). The RAM authorization policy language can convey the authorization meaning in details, which can grant permissions to a specified API-Action and Resource-ID and can also support multiple restrictions such as the source IP address and access time.**

## 4.2.8 O&M security

### 4.2.8.1 Overview

**Apsara Stack provides a set of centralized operations management system, the Apsara Stack Operations system, briefly called ASO. It enables various kinds**

**of operations roles for Apsara Stack, including field operations engineer, user operations engineer, cloud platform operations and management engineer, and operations security personnel or audit management personnel. ASO enables operations engineers to control the system operation status in time and perform corresponding operations actions.**

### 4.2.8.2 OAM permission and authorization

**Operation Administrator Manager (OAM) is a permission management platform for Apsara Stack Operations. OAM uses a simplified Role-Based Access Control (RBAC) model. Administrators can assign roles to operations personnel by using OAM. The operations personnel have different operation permissions to different operations systems based on their roles.**

#### 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. After being assigned a role, a user can have 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. The change of role permission is less frequent than that of the user permission, which simplifies permission management and reduces system overhead.**

#### OAM authorization system

**The administrator grants permissons to operations personnel of different roles by configuring the following parameters:**

- **Subject: operators to the access control system. OAM subjects include users and groups.**
- **User: administrators and operators of the operations system.**
- **Group: a set of multiple users.**
- **Role: core of the RBAC 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 more information about resources on each operations platform, see the permission list of each operations platform.**
- **ActionSet: description about authorized actions. An ActionSet can contain multiple actions. For more information about actions on each operations platform, see the permission list of each operations 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.**

### 4.2.8.3 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 realize automatic operations in a large-scale distributed environment, which makes the operations more efficient and the system more available.**

#### 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.**

### 4.2.9 Security operation service (on the platform side)

**Apsara Stack Security provides multiple platform security operation services that are specified on the platform side of Apsara Stack.**

Security inspection

**Apsara Stack Security investigates and sorts lists of cloud platform services, including the number of physical machines and the version of each product. Apsara Stack Security also analyzes event logs of basic security products that are provided by the cloud platform and defends against the security risks of products.**

Security evaluation and reinforcement

**Apsara Stack Security evaluates the security of the cloud platform system, detects security risks of network, host, and application on the cloud platform, and then reinforces security against the detected risks.**

Vulnerability fixing

**Apsara Stack Security fixes security vulnerabilities, such as password and configuration problems detected during the cloud platform running process.**

Security emergency response

**If a security emergency such as an intrusion occurs, Apsara Stack Security responds to the emergency in time and analyzes the event cause.**

# 4.3 Apsara Stack user (tenant) security

## 4.3.1 Host security

### 4.3.1.1 Apsara Stack Security - Server Guard

**Apsara Stack Security Server Guard module provides security protection measures such as vulnerability management, baseline check, intrusion detection, and asset management for Elastic Compute Service (ECS) by means of log monitoring, file analysis, and feature scanning. The Server Guard module is divided into client side and server side. Server Guard client side works with server side to monitor attack behavior and vulnerability at the host system layer and application layer, which protects the host security in real time.**

Vulnerability management

**The vulnerability management provided by Server Guard for ECS incorporates multiple scanning engines (namely 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.**

Baseline check

**The baseline check provided by Server Guard can automatically detect the risk points of system, database, and account configuration for ECS and provide suggestions for fixing the risks correspondingly.**

Intrusion detection

**The intrusion detection provided by Server Guard includes remote logon reminder, identification of brute force attack behaviors, Webshell detection and removal, and host exception detection.**

**For more information about the Server Guard module, see Features > Apsara Stack Security Standard Edition > Server Guard in** *Apsara Stack Security Technical Whitepaper* **.**

## 4.3.2 Application security

#### 4.3.2.1 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 Alibaba Cloud products. We recommend that enterprise users must perform black-box and white-box code security test for their online applications to prevent security vulnerabilities and improve the security robustness of their businesses.**

### 4.3.3 Data security

#### 4.3.3.1 ApsaraDB

Tenant layer isolation

**ApsaraDB in the Apsara Stack environment isolates tenants by using the virtualization technology, which allows each tenant to have independent 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.**

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, and use the database client and super database account to create a common database account. Then the user can use the super database account to configure table-level read/write permissions for the common database account.**

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. Users can add IP address whitelist rules by using the data security module in the console or APIs. An IP address whitelist rule can take effect without restarting ApsaraDB 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.**

VPC isolation

**Users can perform advanced network access control by using Virtual Private Cloud (VPC) in ApsaraDB. 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. Users also can connect server resources of self-built data centers to the Alibaba Cloud 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. This allows self-owned servers and ECS instances to access ApsaraDB instances simultaneously.**

**VPC and IP address whitelist guarantees a securer ApsaraDB instance.**

Data transfer encryption

**ApsaraDB supports Secure Sockets Layer (SSL) protocol. Users can use root certificate on the server side to verify whether the target address and port database service are provided by ApsaraDB to avoid Man-in-the-Middle (MITM) attack. ApsaraDB also provides the implementation and renovation capability of SSL certificate on the server side to allow users to change SSL cerficate as required, which guarantees the security and availability of the certificate.**

Primary node and standby node

**ApsaraDB adopts a high availability architecture with three nodes replica sets . Three data nodes locate in different physical servers and synchronize data automatically. Primary node and secondary node both provide service. When primary node encounters fault, the system selects new primary node automatically . When the secondary node is unavailable, the standby node takes charge.**

**ApsaraDB also provides automatic backup feature that supports one-click data recovery to make sure that the data is integral and reliable.**

## 4.3.4 Security operation service (on the tenant side)

**Alibaba Cloud provides cloud tenants with the security operation service to operate resources and management policies on the Apsara Stack platform, including configuration and hosting of security product, response of security event, accident tracking, security inspection, monitoring and scanning, and security process**

**management. This service continuously guarantees the consecutive and secure operation of tenants' businesses.**

# 5 Security of Apsara Stack products

## 5.1 Object Storage Service (OSS)

### 5.1.1 Platform security

#### 5.1.1.1 Security isolation

**OSS slices user data and discretely stores the sliced data in a distributed file system based on specific rules. The user data and its indexes are stored separately. OSS users are authenticated using symmetric AccessKeys. The signature in each HTTP request is verified. If verification is successful, OSS reassembles the distributed data. This implements data storage isolation between multiple tenants.**

#### 5.1.1.2 Authentication and access control

#### 5.1.1.2.1 Authentication

**You can create an AccessKey on Apsara Stack Management Console. An AccessKey consists of AccessKey ID and AccessKey Secret. AccessKey ID is public and used to identify a user. AccessKey Secret is private and used to authenticate a user.**

**Before a request is sent to OSS, a signature string must be generated in the format specified by OSS for the request. Then, the signature string is encrypted using AccessKey Secret and the HMAC algorithm, to form a verification code. The verification code carries a timestamp to prevent replay attacks. After receiving the request, OSS finds the corresponding AccessKey Secret using AccessKey ID and extracts the signature string and verification code using the same method. If the calculated verification code matches the one provided, the request is valid. Otherwise, OSS rejects the request and returns an HTTP 403 error.**

#### 5.1.1.2.2 ACL settings

**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. Access can be either anonymous or signature-based . If the access is initiated with an OSS request without any identification informatio**

n, the access is considered to be an anonymous access. Based on the rules in the OSS API documentation, if the access is initiated with a request that contains signature information in its header or carried URL, the access is signature-based.

OSS provides access control for buckets and objects.

Three kinds of bucket access permissions are available: public read/write, public read, and private.

- Public read/write: All users (including anonymous users) can perform write (Put , Get, and Delete) operations on objects in the bucket.
- Public read: Only the bucket creator can perform write (Put, Get, and Delete) operations on objects in the bucket. All users (including anonymous users) can perform read (Get) operations on objects in the bucket.
- Private: Only the bucket creator can perform read/write operations on objects in the bucket. The other users cannot access objects in the bucket.

 Note:
When you create a new bucket without configuring bucket permissions, OSS automatically sets its access permission to private.

Four kinds of object access permissions are available: public read/write, public read, private, and default.

- Public read/write: All users can perform read/write operations on the object.
- Public read: Only the object owner can perform read/write operations on the object. Others can perform read operations on the object.
- Private: Only the object owner can perform read/write operations on the object. Others cannot access the object.
- Default: The object inherits the access permissions of the bucket.

 Note:
If you do not configure any bucket permission when uploading an object, the object will use the default access permission set by the OSS.

## 5.1.1.2.3 Support for RAM and STS

OSS supports Resource Access Management (RAM) and Security Token Service (STS ) authentication.

**RAM is a resource access control service provided by Alibaba Cloud. RAM allows you to create sub-accounts under a primary account. All resources belong to the primary account. The primary account can grant access permissions on resources to sub-accounts.**

**Alibaba Cloud STS provides temporary access credentials and short-term access permission management. STS can generate a temporary access credential for users . The access permission and expiration date of the credential are user-defined. The access credential expires automatically upon the expiration date.**

#### 5.1.1.3 Data security

**An error may occur when data is transferred between the client and server. OSS supports CRC and MD5 verification to secure data.**

CRC

**OSS can return the CRC64 value of objects uploaded through any of the methods provided. The client can compare the CRC64 value with the locally calculated value to verify data integrity.**

**OSS calculates the CRC64 value for newly uploaded objects and stores the result as metadata of the object. OSS then adds the `x-oss-hash-crc64ecma` header to the returned response header, indicating its CRC64 value. This CRC64 value is calculated based on *Standard ECMA-182*.**

MD5 verification

**To check whether the object uploaded to OSS is consistent with the local file, attach the Content-MD5 field value to the upload request. The OSS server verifies the MD5 value. The upload can succeed only when the MD5 value of the object received by the OSS server is the same as the Content-MD5 field value. This method can ensure the consistency between objects.**

#### 5.1.1.4 Data encryption

#### 5.1.1.4.1 Server-side encryption

**OSS supports server-side encryption for the data uploaded by users. When you upload data, OSS encrypts the data using AES256 and permanently stores the encrypted data. When you download the data, OSS automatically decrypts the data , returns the original data to you, and declares in the header of the returned HTTP request that the data had been encrypted on the server.**

**When creating an object, you only need to add the HTTP header of x-oss-server-side -encryption to the Put Object request and set its value to AES256. Then, the object can be encrypted on the server side before it is stored.**

#### 5.1.1.4.2 Client-side encryption

**OSS allows you to use client-side encryption to encrypt data before the data is sent to the remote server while the data encryption key (DEK) used is kept only on the local client. Other users cannot obtain the raw data without the DEK and Enveloped Data Key (EDK), even if the data is leaked. OSS uses functions in the SDK to encrypt the data locally before the data is uploaded to the OSS bucket.**

#### 5.1.1.4.3 KMS-based encryption

**Apsara Stack Key Management Service (KMS) is a secure and highly available service that integrates hardware and software, and provides a key management system that can be extended to the cloud. KMS uses customer master keys (CMKs) to encrypt OSS objects. It uses the KMS API operation to generate data encryption keys (DEKs) in a centralized manner, ActionTrail to check key usage, and RAM to define policies and control key usage. You can use these keys to secure data in OSS buckets.**

### 5.1.2 Tenant security

#### 5.1.2.1 Log audit

**OSS automatically saves access logs. After access logging is enabled for a source bucket, OSS generates an object that contains access logs for that bucket (by hour ), names the object based on predefined naming rules, and writes the object into the bucket specified by the user. These logs are used for later auditing and behavior analysis. Request logs contain information such as the request time, source IP address, request object, return code, and processing duration.**

#### 5.1.2.2 Hotlink protection

**To prevent your data in OSS from being leeched, you can configure hotlink protection through the following parameters:**

- **Referer Whitelist: Only specified domain names are allowed to access OSS resources.**

- **Allow Empty Referer: If this parameter is disabled, a request is allowed to access OSS resources only if the request includes the Referer field configured in the HTTP or HTTPS header.**

**For example, for a bucket named oss-example, you can add** `http://www.aliyun.com/` **to the Referer whitelist. Then, requests with a Referer of** `http://www.aliyun.com/` **can access objects in this bucket.**

# 5.2 ApsaraDB for RDS

## 5.2.1 Platform security

### 5.2.1.1 Secure isolation

Tenant isolation

**ApsaraDB for RDS uses virtualization technology to isolate tenants. Each tenant can maintain their own database permissions independently. Alibaba Cloud also implements increased security for servers that run databases to prevent other users from accessing your data. For example, databases cannot read or write system files.**

### 5.2.1.2 Authentication

**ApsaraDB for RDS secures data through authentication.**

Identity authentication

**Account authentication uses your logon password or AccessKey pair to verify your identity. You can create an AccessKey pair from Apsara Stack Management Console. An AccessKey pair consists of AccessKey ID and AccessKey Secret. AccessKey ID is a public key used for identification. AccessKey Secret is used to encrypt signature strings sent from the client and verify signature strings sent by the server. You must keep your AccessKey Secret confidential.**

**The ApsaraDB for RDS server authenticates the sender identity of each access request. Because of this, each request must contain signature information, regardless of whether it is sent using HTTP or HTTPS. ApsaraDB for RDS uses AccessKey ID and AccessKey Secret to implement symmetric-key encryption and authenticate the identity of a request sender. AccessKey pairs can be applied for**

**and managed from the Apsara Stack. The AccessKey Secret will only be known to you, so it is necessary to take precautions to keep it confidential.**

Permission control

**ApsaraDB for RDS does not automatically create initial database accounts for a newly created instance. You can use the console or API to create a standard database account and configure database-level read and write permissions. To implement fine-grained permission control, such as table-level, view-level, or field-level permissions, you can use the console or API to create a master database account. You can then use the database client and master database account to create standard database accounts. A master database account can configure table-level read/write permissions for standard database accounts.**

Access control

**All ApsaraDB for RDS instances that are created by an Apsara Stack tenant account are managed as resources by that account. By default, an Apsara Stack tenant account is granted full operation permissions on all resources belonging to the account.**

**ApsaraDB for RDS supports Resource Access Management (RAM). You can use RAM to allow RAM users to access and manage RDS resources under your account. ApsaraDB for RDS can also provide short-term access permissions with temporary credentials provided through STS.**

### 5.2.1.3 Data security

**ApsaraDB for RDS secures data through hot standby, data backups, and log backups.**

**High-availability ApsaraDB for RDS instances implement two database nodes for hot standby. When the primary node fails, the secondary node immediately takes over services. Database backups can be initiated anytime. To improve data traceability, ApsaraDB for RDS can restore data to any previous point in time based on the backup policy.**

**Automatic backup at regular intervals is required to guarantee the integrity, reliability, and restorability of databases. ApsaraDB for RDS provides two backup functions: data backup and log backup.**

### 5.2.1.4 Data encryption

SSL

**ApsaraDB for RDS provides Secure Sockets Layer (SSL) for MySQL and SQL Server . You can prevent man-in-the-middle attacks by using the server root certificate to verify whether the destination database service is provided by RDS. RDS also allows you to enable and update SSL certificates for servers to guarantee security and validity.**

**Although ApsaraDB for RDS can encrypt the connection between an applicatio n and a database, SSL cannot run properly until the application authenticates the server. SSL consumes extra CPU resources and affects the throughput and response time of instances. The severity of the impact depends on the number of user connections and frequency of data transfers.**

### 5.2.1.5 DDoS attack prevention

**ApsaraDB for RDS prevents DDoS attacks by using the traffic scrubbing and black hole filtering features.**

**When you access an ApsaraDB for RDS instance from the Internet, the instance is vulnerable to DDoS attacks. When a DDoS attack is detected, the RDS security system first scrubs inbound traffic. If traffic scrubbing is insufficient or if the black hole threshold is reached, black hole filtering is triggered.**

**Triggering conditions for traffic scrubbing and black hole filtering are listed as follows:**

- **Traffic scrubbing**

  **Traffic scrubbing only targets traffic from the Internet. Traffic is redirected from an IP address to the scrubbing device, which then checks whether the traffic is normal. Abnormal traffic is discarded and traffic to the server is limited by the**

scrubbing device to mitigate damage on the server. These operations may have an impact on normal traffic.

ApsaraDB for RDS triggers and stops traffic scrubbing automatically. Traffic scrubbing is triggered for a single ApsaraDB for RDS instance if any of the following conditions are 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 10,000.

· Black hole filtering

Black hole filtering only targets traffic from the Internet. If an RDS instance is undergoing black hole filtering, the instance cannot be accessed from the Internet and connected applications will not be available. Black hole filtering is triggered for a single ApsaraDB for RDS instance if any of the following conditions are met:

- BPS reaches 2 Gbit/s.
- Traffic scrubbing is ineffective.

Black hole filtering is automatically stopped 2.5 hours after being triggered. Then, the instance will undergo traffic scrubbing. If the DDoS attack is still occurring, black hole filtering is triggered again. Otherwise, the system restores the normal state.

## 5.2.2 Tenant security

### 5.2.2.1 Log audit

ApsaraDB for RDS can audit logs to identify security issues.

ApsaraDB for RDS allows you to view SQL transactions and periodically audit the SQL server to identify and resolve issues. RDS Proxy records all SQL statements sent to ApsaraDB for RDS, including the IP address, database name, user account used for execution, execution period, number of returned records, and execution time of each statement.

#### 5.2.2.2 IP address whitelist

**ApsaraDB for RDS uses the IP address whitelist to prevent access from invalid IP addresses.**

**ApsaraDB for RDS instances can be accessed from any IP address by default. Because of this, the IP address whitelist contains only the entry 0.0.0.0/0. You can add IP address whitelist rules through the data security module in the console or by calling an API. The IP address can be updated without restarting the ApsaraDB for RDS instance. Whitelist updates will not affect the normal operation of the instance. Multiple groups can be configured in the IP address whitelist. Each group can contain up to 1,000 IP addresses or IP address segments.**

#### 5.2.2.3 Software update

**ApsaraDB for RDS supports post-restart update and mandatory update for software.**

**ApsaraDB for RDS automatically provides you with new versions of installed database software. In most cases, it is not required to update software immediately. Only when you manually restart an ApsaraDB for RDS instance does the system update the database software to the latest compatible version.**

**In rare cases such as critical bugs and security vulnerabilities, ApsaraDB for RDS will force the database to update during the maintenance period of the instance. Such mandatory updates only result in temporary database disconnections, and will not have any adverse impact on the application if the database connection pool is configured properly.**

**You can use the console or API to change the maintenance schedule to prevent a mandatory update from occurring during peak hours.**

## 5.3 AnalyticDB for PostgreSQL

### 5.3.1 Platform security

#### 5.3.1.1 Security isolation

Network isolation

**In Apsara Stack, you can use IP address whitelists to control access. You can also use a VPC to control network access.**

A VPC is a private network environment that you can set in Apsara Stack to strictly isolate network packets at the network layer by using network protocols and control access.

By default, AnalyticDB for PostgreSQL instances deployed within a VPC are only accessible from the ECS instances within the same VPC. You can also apply for a public IP address to receive access requests from the Internet (not recommended). The requests include but are not limited to:

- Access requests from ECS EIPs.
- Access requests from the Internet egress of your on-premises IDC.

**Note:**

The IP address whitelists apply to all connections to AnalyticDB for PostgreSQL instances. We recommend that you configure whitelists before applying for a public IP address.

Tenant isolation

AnalyticDB for PostgreSQL uses virtualization to isolate tenants and grants each tenant their own database permissions. Alibaba Cloud also hardens security for database servers. For example, to prevent other users from accessing your data, users cannot use a database to read or write operating system files.

### 5.3.1.2 Authentication

AnalyticDB for PostgreSQL instances created by your Apsara Stack tenant account are also owned by the account. Alibaba Cloud tenant accounts have full access permissions on their resources.

AnalyticDB for PostgreSQL supports Resource Access Management (RAM) and Security Token Service (STS). You can use RAM to grant access and management permissions on the AnalyticDB for PostgreSQL resources of your account to other RAM users. You can use STS to issue temporary access credentials to RAM users for short-term access to resources.

### 5.3.1.3 Primary and secondary nodes

Each AnalyticDB for PostgreSQL instance consists of two components: the coordinator node and the compute node. Each node adopts a primary/secondary architecture. If the primary node fails, the service is quickly switched to the

**secondary node. You can back up databases at any time. AnalyticDB for PostgreSQL can restore data from backup sets based on backup policies to improve data traceability.**

## 5.3.2 Tenant security

### 5.3.2.1 Database account

**After you create an instance, you can create a superuser account in the console or by using an API operation. You can execute the `GRANT` statement to authorize other database accounts.**

### 5.3.2.2 IP address whitelist

**AnalyticDB for PostgreSQL instances cannot be accessed from any IP addresses by default. The default whitelist contains `127.0.0.1`. You can add IP addresses to a whitelist on the Security Controls page of the console or by using an API operation. Updating the IP address whitelist does not require an instance to restart nor affect operations on the instance. You can configure multiple IP address whitelists. Each whitelist can contain up to 1,000 IP addresses or CIDR block entries.**

### 5.3.2.3 SQL audit

**AnalyticDB for PostgreSQL allows you to view SQL details. You can audit SQL operations on a regular basis to locate problems in a timely manner. The Proxy module records the information of all SQL statements executed in AnalyticDB for PostgreSQL, including the IP address, the name of the accessed database, the account that executed the statement, the SQL statement, the execution duration, the number of returned records, and the execution time point.**

### 5.3.2.4 Backup and restoration

**To ensure data integrity and reliability, a database must automatically back up data on a regular basis to ensure that data can be restored. AnalyticDB for PostgreSQL allows you to restore instances from backup sets.**

### 5.3.2.5 Software update

- **New versions of database software are provided by AnalyticDB for PostgreSQL on a regular basis.**
- **Software updates are optional and only implemented when you request them.**

- **If the current database version that you are using contains critical security risks, the AnalyticDB for PostgreSQL team will notify you and recommend that you schedule an update. The AnalyticDB for PostgreSQL team can provide full support throughout the update process.**
- **AnalyticDB for PostgreSQL updates are usually completed within five minutes. During updates, instances may be disconnected several times and will become read-only for about a minute. There is minimal interruption to services if the database reconnection settings or connection pool are properly configured for your applications.**

## 5.4 Data Transmission Service (DTS)

### 5.4.1 Platform security

#### 5.4.1.1 Security isolation

**DTS uses independent processes and files to isolate instances and data between tenants. For example, users are not allowed to read/write OS files of instances so that users cannot access data of other users.**

#### 5.4.1.2 Authentication

**You can use your Alibaba Cloud account to create a DTS instance. The resources of the DTS instance are owned by the Alibaba Cloud account. The account has full access permissions on its DTS resources by default.**

**DTS supports RAM for Alibaba Cloud. You can assign permissions to access and manage DTS resources to RAM users. RAM enables you to assign permissions as needed and helps enterprises minimize information security risks.**

#### 5.4.1.3 Transmission security

**To enhance data transmission security, DTS-defined log formats are used.**

**In DTS, data is encrypted for secure transmission. For example, data is encrypted during incremental data synchronization between the data reading module and the data synchronization module.**

**DTS also supports HTTPS to effectively improve access security.**

#### 5.4.1.4 Data security

**When you use DTS to subscribe to incremental data, a large portion of incremental data is stored on the DTS server. The incremental data is serialized and stored based on the storage format defined in DTS. The DTS-defined storage format provides enhanced data security.**

> **Note:**
> **Data written to the DTS server is automatically deleted after it is stored for seven days.**

## 5.5 KVStore for Redis

### 5.5.1 Platform security

#### 5.5.1.1 Security isolation

Tenant isolation

**KVStore for Redis uses the virtualization technology to isolate tenants. Each tenant can maintain independent database permissions. Alibaba Cloud also increases security protections for the servers that run databases. For example, you cannot read from or write to system files by using the databases, so you cannot access other users' data.**

Network isolation

**In Apsara Stack, in addition to the whitelist, you can use Virtual Private Cloud (VPC ) to restrict connections.**

**A VPC is a private network that you specify in Apsara Stack. The VPC strictly isolates your network packets based on network protocols and restricts connection s at the network layer. You can use a virtual private network (VPN) or a leased line to connect server resources in your IDC to Alibaba Cloud, and use CIDR blocks in a VPC to prevent IP conflicts. In this way, your own servers and ECS instances can connect to KVStore for Redis instances at the same time. Protections based on the VPC and IP address whitelist improve the instance security.**

**By default, ECS instances in a VPC can only connect to KVStore for Redis instances in the same VPC. You can also request a public IP address to accept connections**

over a public network. We recommend that you do not use this connection method. The connection requests include but are not limited to:

- Those from ECS Elastic IP addresses (EIPs).
- Those from the public IP addresses in your own IDC.

**Notice:**

The IP whitelist is applicable to all types of connections to KVStore for Redis instances. We recommend that you set the whitelist before requesting the public IP address.

### 5.5.1.2 Authentication

The instances that you create by using your Alibaba Cloud account are the resources under this account. By default, the Alibaba Cloud account is granted full operation permissions on all the resources under the account.

KVStore for Redis supports Resource Access Management (RAM) and Security Token Service (STS) services. By using RAM, you can create and manage RAM users. You can grant access and management permissions on KVStore for Redis resources under your Alibaba Cloud account to the RAM users. By using STS, you can manage short-term permissions granted to RAM users. You can use STS to grant permissions to temporary users.

### 5.5.1.3 Transmission encryption

KVStore for Redis provides secure encryption based on the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. You can use the server root certificate from KVStore for Redis to verify that KVStore for Redis provides database services based on the target IP address and port. This can effectively prevent man-in-the-middle attacks (MITM). Also, KVStore for Redis allows you to enable and update SSL and TLS certificates for servers. Therefore, you can replace the SSL or TLS certificate to ensure security and validity.

**Note:**

- To use the transmission encryption feature, you must enable server verification in your application.

- **Transmission encryption consumes extra CPU resources and affects the throughput and response time of KVStore for Redis instances. The performance depends on the number of connections and the data transfer frequency.**

## 5.5.2 Tenant security

### 5.5.2.1 Database account

**To connect to KVStore for Redis, you must pass password authentication. The password is the access credential. KVStore for Redis optimizes the performance of transient connections. Therefore, when you enable password authentication, the performance of KVStore for Redis instances is not affected.**

### 5.5.2.2 IP address whitelist

**KVStore for Redis allows you to use an IP address whitelist to restrict connections and secure your data. You can set an IP address whitelist for each KVStore for Redis instance.**

**By default, KVStore for Redis instances block connections from all IP addresses or CIDR blocks. In this case, the IP address whitelist is set to `127.0.0.1`. To add an IP address or CIDR block to the whitelist, in the KVStore for Redis console, choose Instance Information > Change Whitelist. After you modify the IP address whitelist, you do not need to restart the instance, so you can still run the instance normally. You can specify multiple IP address groups for a whitelist. Each group contains a maximum of 1,000 IP addresses or CIDR blocks.**

### 5.5.2.3 Backup and recovery

**Databases require regular automatic backups to guarantee data integrity, reliability, and restorability. KVStore for Redis supports instance recovery based on backup sets.**

### 5.5.2.4 Software upgrade

- **KVStore for Redis regularly provides database upgrades.**
- **The upgrades are not mandatory. Databases upgrade to the specified version only when you request.**
- **When the KVStore for Redis team determines that your version has major security risks, KVStore for Redis notifies you to enable the upgrade. The KVStore for Redis team supports the whole upgrade process.**

- **KVStore for Redis completes the upgrade within five minutes. During the upgrade, temporary disconnections may occur, and the instance may stay in read-only status for one minute. If you have correctly configured the database reconnection or connection pool for your application, the upgrade does not affect your application.**

# 5.6 Distributed Relational Database Service (DRDS)

## 5.6.1 Platform security

### 5.6.1.1 Isolation

Network isolation

**Distributed Relational Database Service (DRDS) supports advanced network access control by using a Virtual Private Cloud (VPC).**

**A VPC is a private network environment that you set. It strictly isolates network packets over underlying network protocols and controls access at the network layer . The VPC and IP address whitelist together improve the security of DRDS instances greatly.**

### 5.6.1.2 Authentication

**Distributed Relational Database Service (DRDS) supports a MySQL-like account and permission system and supports commands and functions such as GRANT, REVOKE, SHOW GRANTS, CREATE USER, DROP USER, and SET PASSWORD.**

**When creating a DRDS database, you can specify an account with all permissions by default. You can use this account to create one or more accounts.**

- **Permissions can be granted at the database and table levels. Currently, global permissions and column permissions are not supported.**
- **Eight associated basic permissions are supported: CREATE, DROP, ALTER, INDEX , INSERT, DELETE, UPDATE, and SELECT.**
- **The `user@'host'` format can be used to match and verify access to a host.**

**Note:**

**However, if the business host is in the Virtual Private Cloud (VPC), the IP address cannot be obtained due to technical restrictions. In this case, we recommend that you change the format to `user@'%'`.**

## 5.6.2 Tenant security

### 5.6.2.1 IP address whitelist

**Distributed Relational Database Service (DRDS) provides an IP address whitelist to ensure secure access. Each DRDS database can be configured with an IP address whitelist.**

**By default, DRDS instances are set to be accessible from any IP address. You can add IP addresses to the DRDS whitelist on the Whitelist settings page in the console. Updating the IP address whitelist does not require restart of the DRDS instance, and does not affect operations on the instance. You can also set IP addresses or CIDR blocks in the IP address whitelist.**

**Note:**
**If the business host is in the Virtual Private Cloud (VPC), the IP address cannot be obtained due to technical restrictions. We recommend that you remove the IP address whitelist.**

### 5.6.2.2 Protection against high-risk SQL misoperations

**Distributed Relational Database Service (DRDS) prohibits high-risk operations such as full table deletion and update by default. You can temporarily skip this restriction by adding a hint. The following statements are prohibited by default:**

- **DELETE statements that do not contain the WHERE or LIMIT condition.**
- **UPDATE statements that do not contain the WHERE or LIMIT condition.**

**The actual effect is as follows:**

```
mysql> delete from tt;
ERR-CODE: [TDDL-4620][ERR_FORBID_EXECUTE_DML_ALL] Forbid execute
DELETE ALL or UPDATE ALL sql. More: [http://middleware.alibaba-inc.com
/faq/faqByFaqCode.html?faqCode=TDDL-4620]
```

**After the hint is added, the statements are successfully executed.**

```
mysql> /*TDDL:FORBID_EXECUTE_DML_ALL=false*/delete from tt;
```

```
Query OK, 10 row affected (0.21 sec)
```

#### 5.6.2.3 Slow SQL audit

**In the Distributed Relational Database Service (DRDS) console, you can query the slow SQL statements sent by the client to DRDS. Slow SQL statements increase the response time (RT) of the entire link and reduce the DRDS throughput.**

**Contents of a slow SQL statement include the execution start time, database name , SQL statement, client IP address, and execution time. You can query slow SQL details in the DRDS console for optimization and adjustment.**

#### 5.6.2.4 Monitoring information

**The Distributed Relational Database Service (DRDS) console provides monitoring metrics in different dimensions. You can perform related operations based on the monitoring information.**

**DRDS monitoring information can be classified into two types:**

- **Resource monitoring information, including the CPU, memory, and network.**
- **Engine monitoring information, including the logical queries per second (QPS), physical QPS, logical response time (RT) (in ms), physical RT (in ms), number of connections, and number of active threads.**

**The QPS and CPU performance of a DRDS instance are in positive correlation. When DRDS encounters a performance bottleneck, the CPU usage of the DRDS instance remains high. If the CPU usage exceeds 90% or remains higher than 80%, the DRDS instance encounters a performance bottleneck. If there is no bottleneck in the DRDS instance, the current DRDS instance type cannot meet the QPS performance requirements of the business. In this case, upgrade the DRDS instance.**

## 5.7 AnalyticDB for MySQL

### 5.7.1 Platform security

#### 5.7.1.1 Security isolation

**In AnalyticDB for MySQL, databases are the basic unit of tenant isolation. The Apsara Stack tenant account used to create a database is the owner of the database . The database owner must grant access permissions before other users can access**

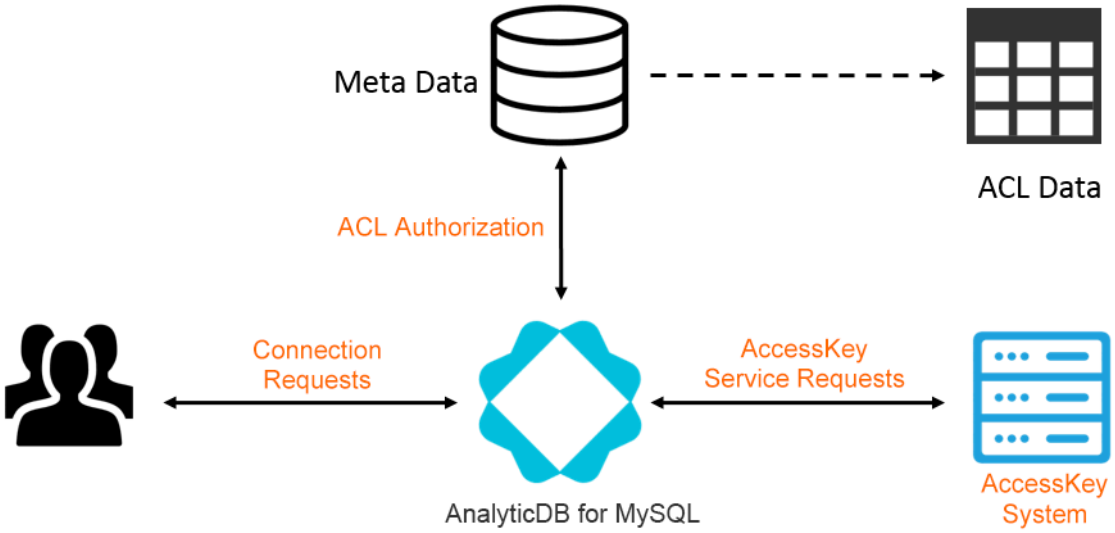
the database. Each database runs on an exclusive process for each user, isolating databases at the process level.

Each AnalyticDB for MySQL database uses a multi-tenancy mechanism to completely isolate each process. Physical resources, such as CPU, memory, and storage space, are isolated between databases.

AnalyticDB for MySQL allows you to manage the version of each database, scale database resources, and start and stop database services.

### 5.7.1.2 Authentication

The following figure shows the identity authentication and access control mechanisms of AnalyticDB for MySQL.




Identity authentication

AnalyticDB for MySQL provides a MySQL protocol-based identity authentication system with username and password authentication.

Like other Alibaba Cloud services, AnalyticDB for MySQL uses the AccessKey mechanism to implement identity authentication. You can connect to AnalyticDB for MySQL by using an AccessKey pair or a driver such as Connector/J or Connector /ODBC.

AccessKey pairs can be created in the Apsara Stack Cloud Management (ASCM) console. Each AccessKey pair consists of an AccessKey ID and an AccessKey secret , similar to the username and password. The AccessKey ID can be publicly shared

**and is used to identify a user. The AccessKey secret is used to authenticate the user identity and must be kept confidential.**

**You can connect to AnalyticDB for MySQL by using the AccessKey ID and AccessKey secret of your Apsara Stack tenant account or RAM user.**

Access control

**AnalyticDB for MySQL uses access control list (ACL) rules to provide table-level permission management similar to those of MySQL. However, unlike MySQL, AnalyticDB for MySQL ACL does not provide host-based authorization.**

**An ACL authorization lists authorized users as well as their authorization objects and operation permissions. ACL data is stored in the AnalyticDB for MySQL metadata system and uses RDS to ensure data persistence. AnalyticDB for MySQL caches metadata to accelerate authorizations for Data Manipulation Language ( DML) and Data Definition Language (DDL) operations.**

**After you connect to AnalyticDB for MySQL, AnalyticDB for MySQL uses the ACL metadata to control your operation permissions on database objects. AnalyticDB for MySQL defines whether you can perform SELECT, INSERT, DELETE, CREATE , SHOW, DROP, ALTER, DESCRIBE, LOAD DATA, or DUMP DATA operations on a specific table or column.**

**AnalyticDB for MySQL provides the following authorization objects:**

- **Database: specifies a database or all tables in a database, such as `db_name.*` or `*` (default database).**
- **Table: specifies a table, such as `db_name.table_name` or `table_name`.**
- **Column: specifies a column in a specified table. It is composed of `column_list` and `Table`.**

Access control

**AnalyticDB for MySQL supports resource access management (RAM), but not security token service (STS).**

**RAM allows you to create RAM users by using an Apsara Stack tenant account and grant resource access permissions to RAM users. All RAM users created by you are affiliated with your Apsara Stack tenant account, which means that all of their resources will also belong to your Apsara Stack tenant account.**

#### 5.7.1.3 Data security

Multi-tenancy

**AnalyticDB for MySQL provides tenant isolation. Resources (such as CPU, memory, disks, and network bandwidth) of different databases are completely isolated from each other to ensure tenant isolation.**

Data reliability

**All AnalyticDB for MySQL data is stored in Apsara Distributed File System using three-replica redundancy or erasure code (EC) to ensure high reliability and data persistence. After DML operations such as INSERT and DELETE are performed on the data of a real-time table, updates are synchronized to Apsara Distributed File System. Data is also written to Apsara Distributed File System during batch loading.**

Data consistency

**AnalyticDB for MySQL uses a multiversion concurrency control (MVCC) mechanism to store changes to real-time table data resulting from INSERT and DELETE operations. This ensures that query results returned during concurrent data updates are consistent with the data version at the time the query was initiated.**

> **Note:**
> **You can clear outdated data versions at regular intervals.**

### 5.7.2 Tenant security

#### 5.7.2.1 Log audit

**You can enable log audit to record all SQL operation information generated in AnalyticDB for MySQL. The information includes:**

- **Query time**
- **IP address of the client**
- **Executed SQL statements**

**You can then use SQL statements to query historical data.**

**Example of the audit log format:**

```
[2017-10-10 13:37:57,351] INFO [pool-31-thread-22] c.a.c.a.f.l.
AccessLog.info - Client=127.0.0.1 Total_time=1044 Exec_time=1043
Queue_time=1 - [2017-10-10 13:37:56 308] 1 SQL Statement \;process=
20171010133756010003163108099998380 42\;CLUSTER=ayads-bjyz
```