ALIBABA CLOUD

Alibaba Cloud

Security White Paper

International Edition

February 2021

Version: 2.1

阿里云

Legal disclaimer

Alibaba Cloud reminds you to carefully read the terms and conditions of this legal disclaimer in full before you read or use Alibaba Cloud Security Whitepaper (“White Paper”). If you have read or used this White Paper, it shall be deemed as your total acceptance of the terms and conditions of this legal disclaimer.

1. You shall download and obtain this White Paper from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this White Paper for your own legal business activities only. The content of this White Paper is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this White Paper 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 White Paper may be changed from time to time due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this White Paper without notice and the updated versions of this White Paper will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this White Paper as they occur and download and obtain the most up-to-date version of this White Paper from Alibaba Cloud-authorized channels.
4. This White Paper serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this White Paper 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 White Paper, 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 of, or trust in this White Paper. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages,

including lost profits arising from the use of or trust in this White Paper, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 brands and 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 brands and 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.

   Please contact Alibaba Cloud directly if you discover any errors in this White Paper.

Contents

1. Overview

Data security and user privacy are the top priorities of Alibaba Cloud. Alibaba Cloud is committed to building a public, open, and secure cloud computing service platform. Alibaba Cloud aims to turn cloud computing into a state-of-the-art computing infrastructure by investing heavily in technical innovation to continually improve the computing capabilities and economies of scale of its services.

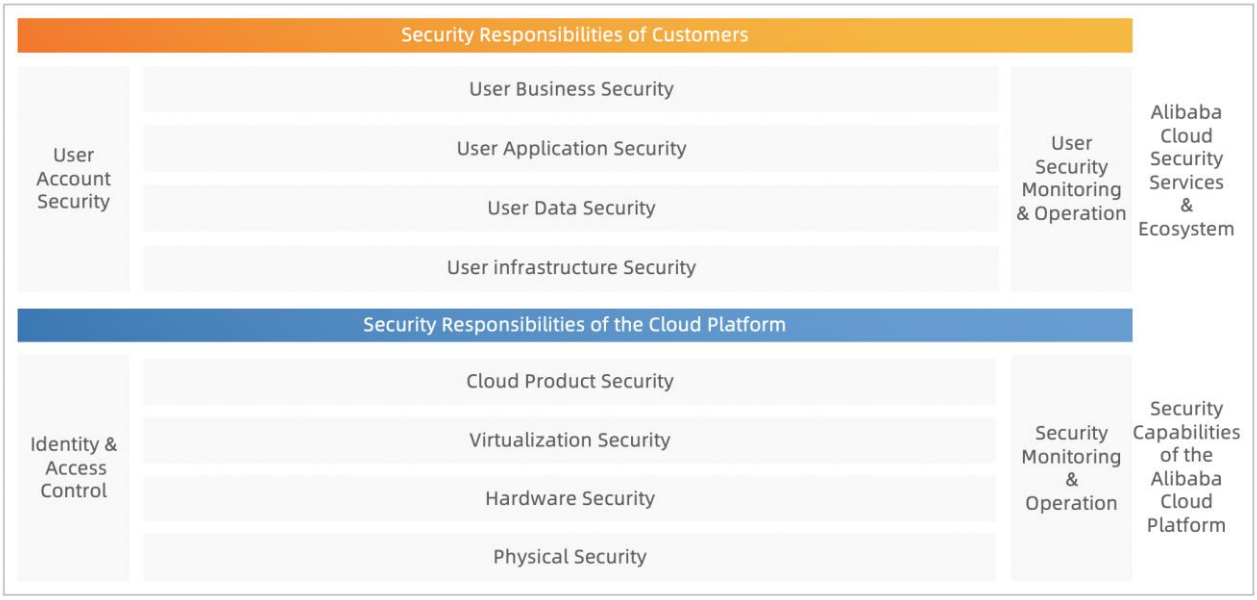
Alibaba Cloud strives to provide customers with consistent, reliable, secure, and compliant cloud computing services, helping customers ensure the confidentiality, integrity, and availability of their systems and data.

This white paper introduces the public cloud security system of Alibaba Cloud, specifically for Alibaba Cloud’s security capabilities and offerings for regions outside of Mainland China, and is divided into the following parts:

- Shared security responsibilities
- Security compliance and privacy
- Alibaba Cloud infrastructure
- Alibaba Cloud security architecture
- Security capabilities provided by Alibaba Cloud products
- Security services provided by Alibaba Cloud Security
- Alibaba Cloud data security system

2. Shared security responsibilities

The security of applications built on Alibaba Cloud is the joint responsibility of Alibaba Cloud and its customers. Alibaba Cloud is responsible for the security of the underlying cloud service platform and providing security services and capabilities to customers, while customers are responsible for the security of applications built based on Alibaba Cloud services.



Security Responsibilities of Customers

User Account Security

User Business Security

User Application Security

User Data Security

User infrastructure Security

User Security Monitoring & Operation

Alibaba Cloud Security Services & Ecosystem

Security Responsibilities of the Cloud Platform

Identity & Access Control

Cloud Product Security

Virtualization Security

Hardware Security

Physical Security

Security Monitoring & Operation

Security Capabilities of the Alibaba Cloud Platform

Alibaba Cloud must ensure the security of infrastructure (including but not limited to data centers deployed across regions and zones, and Alibaba backbone networks), physical devices (including computing, storage, and network devices), virtualization solutions, and cloud products running on top of the Apsara distributed cloud OS. Alibaba Cloud is also responsible for identity management and access control, monitoring, and operations of the platform to provide customers with a highly available and secure cloud service platform.

Customers must configure and use cloud products based on security best practices, and build applications on these securely configured cloud products. Alibaba Cloud offers Alibaba Cloud Security, which leverages the years of expertise in attack prevention technologies to help customers protect their applications and systems. Customers can choose to use Alibaba Cloud Security or any third-party security products in the Alibaba Cloud security ecosystem to protect their applications and business systems.

Alibaba Cloud employs a shared security responsibility model between itself and its customers, where Alibaba Cloud secures the cloud platform and provides integrated cloud security products and capabilities to customers. This relieves much of the underlying security burdens while allowing customers to focus more on their core business needs. Note that the Apsara Stack security responsibility model is somewhat different from the aforementioned public cloud security model. For more information, see Alibaba Cloud Apsara Stack Security White Paper.

2.1. Security responsibilities of Alibaba Cloud

Alibaba Cloud is responsible for the security of its infrastructure, physical devices, Apsara OS, and cloud products and services, and provides customers with necessary technical capabilities to protect their cloud applications and data.

Alibaba Cloud secures its cloud platform from several aspects, including but not limited to:

- Protecting the physical security of cloud data centers.
- Protecting the security of hardware, software, and network of the cloud platform by means of OS and database patch management, network access control, Anti-DDoS, disaster recovery, etc.
- Identifying and fixing security vulnerabilities of the cloud platform in a timely manner without affecting customers' service availability.
- Cooperating with independent third-party security regulation and audit agencies to audit and evaluate the security and compliance stance of Alibaba Cloud.

Alibaba Cloud provides customers with the technical means to protect cloud information systems, including but not limited to:

- Providing multihomed BGP access networks and cloud data centers distributed across multiple regions and zones, and allowing customers to build high availability cloud applications based on Alibaba Cloud infrastructure.
- Providing secure hardware infrastructure and equipment.
- Providing Alibaba Cloud account security management capabilities, including but not limited to the use of two-level account credentials (Alibaba Cloud accounts and RAM user accounts) for segregation of duties, multi-factor authentication (MFA), grouped authorization, fine-grained authorization control, and temporary authorization tokens.
- Providing security monitoring and operations capabilities, including security audits.

- Providing data encryption capabilities.
- Providing various Alibaba Cloud Security services.
- Working with third-party security vendors to provide customers with security solutions tailored to their needs.

2.2. Security responsibilities of customers

Customers who build cloud applications on Alibaba Cloud are responsible for protecting their own systems by using the security features provided by Alibaba Cloud services, Alibaba Cloud Security, and third-party security products in the Alibaba Cloud security ecosystem.

Customers must manage security configurations for cloud products to ensure infrastructure security and data security on the cloud. Customers have full control over infrastructure services such as ECS instances provided by Alibaba Cloud, and are responsible for managing these instances and performing the necessary security configurations. Customers must harden the OS on their ECS instances, install security patches in a timely manner, and properly configure security groups for network access control. For other Alibaba Cloud services, such as platform and cloud native services, customers do not need to maintain the underlying computing instances, such as keeping the OS updated, hardened, and patched. Instead, customers are only responsible for managing the service account authentication and resource authorization, and using the security features available with these services. For example, MaxCompute provides various levels of access control capabilities. Customers only need to configure security features in such products according to their business needs.

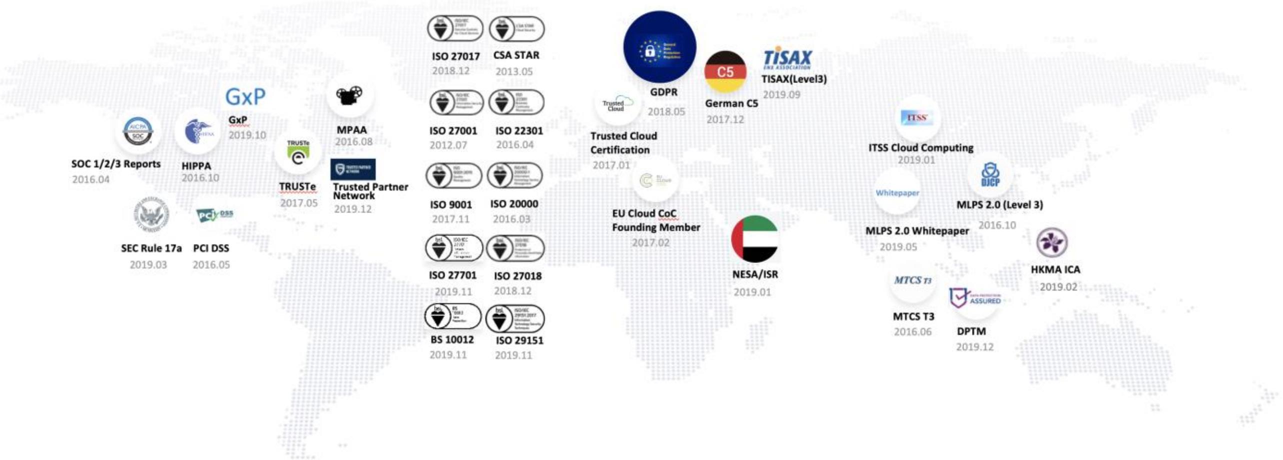
Customers can also use the native encryption capabilities of Alibaba Cloud products or Alibaba Cloud Data Encryption Service for security-sensitive data encryption, and use the managed Hardware Security Module (HSM) feature integrated with Key Management Service (KMS) for encryption key management.

Customers' applications and business systems on Alibaba Cloud need to be protected by Alibaba Cloud Security services and any third-party security products in the Alibaba Cloud security ecosystem. Customers can also use Alibaba Cloud Security services to monitor and manage the security of applications and business systems on the cloud. Customers must protect their Alibaba Cloud account credentials by taking such measures as enabling MFA, granting only the minimum permissions required, and ensuring a separation of duties by means of assigning permissions by group. Furthermore, customers can use Alibaba Cloud ActionTrail to record OpenAPI calls and operations performed on the console, and audit account operations.

Alibaba Cloud provides customers with a variety of security services and capabilities. In turn, customers are responsible for properly configuring and using these security services and capabilities to ensure the security of their applications and business systems on the cloud.

3. Security and compliance

By leveraging years of experience and professional expertise in defense against Internet security threats, Alibaba Cloud provides security protection for the cloud platform, and implements various compliance requirements into the internal control program and product design of the cloud platform. In addition, Alibaba Cloud has participated and contributed in the development of multiple standards and best practices for the cloud industry.



Alibaba Cloud adopts industry standards and best practices to safeguard customer data. We have received multiple industry standard certifications and regularly complete third-party audits. Our compliance credentials include, but are not limited to:

Credentials	Description
ISO 27001	ISO27001 is a widely adopted global security standard that outlines the requirements for information security management systems. As the first cloud service provider to pass this certification in China, Alibaba Cloud proves that it has fulfilled security responsibilities in such aspects as data security, network security, communication security, and operational security.
ISO 27017	ISO 27017 provides a set of information security control guidelines for the use of cloud services, including additional implementation guidelines for ISO/IEC 27002-based controls, as well as additional controls and implementation guidelines related to cloud service features.
ISO 27018	ISO 27018 is an international standard for personal data protection that applies to cloud service providers. ISO 27018 provides a set of guidelines to protect personally identifiable

	information (PII) in public clouds. It is widely regarded as the strictest, most authoritative, and most widely accepted and applied information security system certification in the world.
CSA STAR	CSA STAR certification was developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI). Alibaba Cloud is the first company in the world to obtain the CSA STAR gold medal certification.
ISO 9001	ISO 9001 is an authoritative certification for quality management systems. It is designed to help organizations ensure that they meet the needs of customers and other stakeholders while meeting statutory and regulatory requirements related to a product or service.
ISO 20000	ISO 20000 is the first internationally recognized IT service management standard. As the first cloud service provider in China to obtain the ISO/IEC 20000-1:2011 certification, Alibaba Cloud has established and strictly implemented a standard service process. Standardized cloud services can improve efficiency and reduce the overall risk.
ISO 22301	A standard for a Business Continuity Management (BCM) system, this certifies Alibaba Cloud as meeting the requirements for business continuity planning, disaster recovery and regular drills to enhance the stability of the cloud platform.
ISO27701	ISO/IEC 27701:2019 is an extension of the ISO/IEC 27001 information security management system and ISO/IEC 27002 information security control measures. It has considered the mapping of GDPR clauses and other privacy-related standards from the very beginning and is an authoritative guideline for the construction of a privacy management system.
SOC1/2/3	Service Organization Control (SOC) Reports are internal control reports on the services provided by a service organization. The reports provide valuable information that users need to assess and address the risks associated with an outsourced service.
Multi-Level Protection Scheme (MLPS) 2.0 issued by the Ministry of Public Security	Alibaba Cloud complies with the MLPS 2.0 standards in China. Alibaba Cloud's Finance Cloud is the first cloud platform that has passed the MLPS level-4 certification, and Alibaba Cloud's Government Cloud is the first cloud platform that has passed the MLPS 2.0 certification.
C5	Alibaba Cloud meets the C5 standard, showing its commitment to applying the highest level of

	compliance in control and security. The C5 standard serves not only as a benchmark for the German market, but also increasingly as a benchmark for institutions across Europe. With the attestation, German customers can leverage the work performed to comply with stringent local requirements and use Alibaba Cloud services to run secure workloads. C5 is intended for professional cloud service providers and their auditors and customers. It has 17 distinct control requirements that cloud service providers have to comply with or meet the defined minimum standards. It is a required assessment for working with the public sector in Germany and is increasingly adopted by the private sector.
MTCS	The Singapore certification organization Certification International has awarded Alibaba Cloud the Multi-Tier Cloud Security (MTCS) T3 certification, the highest of three available certification levels. The MTCS standard was initiated by the Infocomm Development Authority of Singapore (IDA) and launched by SPRING Singapore.
NESA/ISR	The National Electronic Security Authority (NESA) is a government body tasked with protecting the UAE's critical information infrastructure and improving national cybersecurity. Alibaba Cloud meets the set of standards and follows the guidance that NESA has produced for government entities in critical sectors, and was audited by a qualified third-party independent auditor for the P1 level compliance. The Dubai Government Information Security Regulation (ISR) formulated by the Dubai Government encompasses several information security domains composed of various controls and is similar to the ISO 27001 standard. The ISR also includes distinctive items reflecting specific requirements of the Dubai Government. Alibaba Cloud was audited by a qualified third-party independent auditor for the compliance of ISR requirements.
PCI DSS	PCI DSS is an important security standard for the card payment industry to evaluate the security of payment card data such as credit card number and CVV2 code. It also focuses on the security of account or password transfer and storage. Alibaba Cloud is the first cloud service provider in China to pass the PCI DSS certification.
SEC Rule-17a	Alibaba Cloud has completed the assessment related to the ability of OSS to comply with the broker-dealer media requirements promulgated by the Securities and Exchange Commission (SEC) Rule 17a-4(f) and Financial Industry Regulatory Authority (FINRA) Rule 4511. This assessment allows Alibaba Cloud to serve more customers in the financial industry worldwide,

	because these regulatory requirements have been widely adopted by many other countries outside of the US as part of the measurement of the financial support capability of a product.
TRUSTe	Alibaba Cloud is certified by TRUSTe Enterprise Privacy Certification. This marks the compliance of Alibaba Cloud in collecting, using, managing, and destroying personal information.
HIPAA/HITECH	Alibaba Cloud fully supports the Business Associate Agreement (BAA) for customers that require strict compliance with the US Health Insurance Portability and Accountability Act (HIPAA) to protect the privacy and security of healthcare information. For detailed information, please refer to our HIPAA whitepaper, which covers compliance of multiple Alibaba Cloud products and services under HIPAA security requirements.
GxP	Alibaba Cloud has completed the GxP readiness assessment of our platform and products under the US Food and Drug Administration (FDA) Regulations on Electronic Records and Electronic Signatures (ERES) Part 11 of Title 21 Code of Federal Regulations (21 CFR Part 11).
TPN	As a “trusted partner” vendor, Alibaba Cloud is the first public cloud service provider to obtain the entertainment industry’s TPN (Trusted Partner Network) certification to ensure customers’ content security.
MPAA	Alibaba Cloud complies with the best practices and common guidelines of the Motion Picture Association of America (MPAA).
TISAX	Alibaba Cloud Germany passed the European automotive industry's TISAX (Trusted Information Security Assessment Exchange) certification with the highest level, level 3
PDPA	Alibaba Cloud complies with the requirements of Singapore's Personal Data Protection Act (PDPA). The compliance is validated by third-party assessment organizations.
Trusted Cloud Label	Alibaba Cloud is a member of Trusted Cloud promoted by German Federal Ministry of Economics and Energy, and has obtained their quality label of reliable cloud services.
Founding member of EU Cloud Code of Conduct	As a founding member of the EU Cloud Code of Conduct and a member of the General Assembly, Alibaba Cloud is actively involved in formulating a code of conduct for EU cloud services in accordance with the requirements of GDPR article 40. Alibaba Cloud engages in

	constructive collaboration with the EU Data Protection bodies, and ensures that their expectations and future guidance for the GDPR are fully considered while drafting the code. Alibaba Cloud is committed to maintaining a high standard of data protection throughout the Alibaba Cloud ecosystem and contributing to the development of the technology industry. Alibaba Cloud supports improved transparency in the cloud computing industry and helps cloud customers understand how cloud service providers address data protection issues.

For additional information, please visit us at Alibaba Cloud Security and Compliance Center https://alibabacloud.com/trust-center

3.1. Privacy

Privacy by Design

Privacy by Design promotes privacy and data protection from the beginning. All of our newly released Alibaba Cloud products have been through a security review and a privacy design assessment to ensure security and privacy considerations are embedded in the product.

Privacy Policy

Alibaba Cloud is committed to protect customer personal information and guarantees that such information is only used for the purposes disclosed to or agreed to (as applicable) by customers. Alibaba Cloud's privacy policy is completely transparent to the public and can be found on our official website.

3.2. Transparency

At Alibaba Cloud, we are committed to our customers around the world. We understand the importance of international data protection standards and will help ensure that security interests for countries globally are respected.

Similar to other companies around the world, at times we are required by law to provide records to the government and law enforcement during an investigation or in the course of litigation. As a cloud service provider, we operate and ensure we meet the ever-changing regulations and standards set by government agencies, industry groups, and our own board of governance.

4. Alibaba Cloud infrastructure

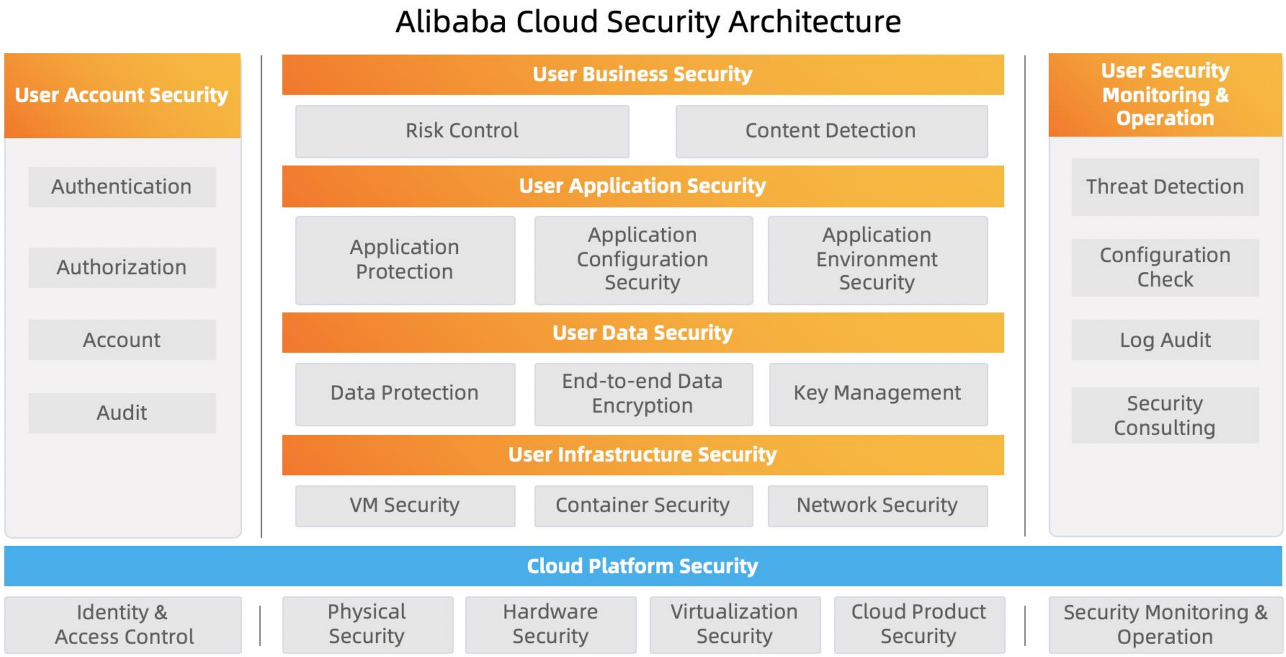
Alibaba Cloud offers highly available, secure, and reliable cloud computing infrastructure by taking the following measures: setting up cloud data centers across multiple regions and zones globally, delivering a better network access experience with multihomed BGP networks, providing cloud products with high availability infrastructure and multi-replica data redundancy based on the Apsara distributed cloud OS, upgrading products and fixing vulnerabilities through the world's leading hotfix dynamical patching technology, and ensuring O&M security while achieving world-leading compliance.

Alibaba Cloud data centers are deployed across multiple regions worldwide, with each region supporting multiple zones. Customer workloads can be deployed across regions and zones to implement a high availability architecture, such as zone active-active architecture, geo-disaster recovery architecture, active geo-redundancy architecture, and disaster recovery architecture that spans three data centers across two regions. For more information, see Alibaba Cloud global infrastructure at https://www.alibabacloud.com/global-locations.

Region		Number of zones
Regions in Mainland China	China (Qingdao)	2
	China (Beijing)	8
	China (Zhangjiakou)	3
	China (Hohhot)	2
	China (Hangzhou)	8
	China (Shanghai)	7
	China (Shenzhen)	5
	China (Chengdu)	2
	China (Heyuan)	2
Regions outside Mainland China	China (Hong Kong)	2
	Singapore	3
	Australia (Sydney)	2
	Malaysia (Kuala Lumpur)	2
	Indonesia (Jakarta)	2
	India (Mumbai)	2
	Japan (Tokyo)	2
	US (Virginia)	2
	US (Silicon Valley)	2

	Germany (Frankfurt)	2
	UK (London)	2
	UAE (Dubai)	1

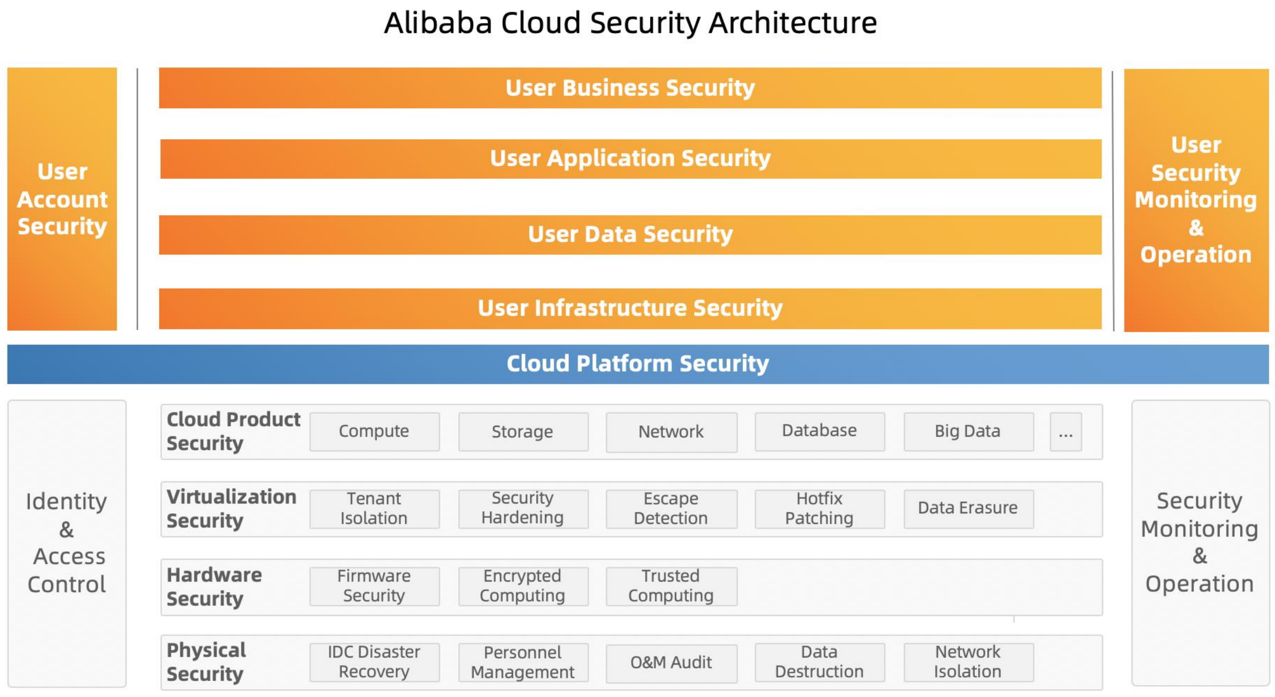
5. Alibaba Cloud security architecture



Alibaba Cloud provides a security architecture that offers protection in five horizontal dimensions and two vertical dimensions. The two vertical dimensions include account security (identity and access control) and security monitoring and operations. Note that these vertical dimensions include different implementations for both user security and cloud platform security. The five horizontal dimensions include cloud platform security at the bottom layer, as well as infrastructure security, data security, application security, and business security for cloud users.

This chapter introduces the overall security architecture and describes the key features of each layer that covers various Alibaba Cloud products and security services. For more information about the capabilities of each product, see the relevant sections of this white paper.

5.1. Cloud platform security



The cloud platform security architecture includes the basic security capabilities provided by the Alibaba Cloud platform. In the two vertical dimensions, identity and access control and security monitoring and operations are invisible to customers. Similarly, customers can enjoy the high-level protection capabilities of Alibaba Cloud without performing configurations at the physical security, hardware security, and virtualization security layers. The cloud product security layer includes the security capabilities provided by the cloud platform for customers. Some capabilities such as tenant isolation are enabled by default. Some capabilities such as data encryption must be enabled and properly configured by customers to function properly.

5.1.1. Physical security

Alibaba Cloud data centers are all in compliance with the requirements for Class A in the GB 50174 Code for Design of Electronic Information System Room and the T3+ standards in the TIA-942 Telecommunications Infrastructure Standard for Data Centers, including the following requirements for physical and environmental security control:

5.1.1.1. Data center disaster recovery

Fire detection and response

Alibaba Cloud data centers are equipped with fire detection systems that utilize thermal and smoke sensors. The sensors are fitted to the ceiling and floor and give audible and visual alarms when triggered. Each data center is equipped with an integrated gas extinguishing system and fire extinguishers. Data center personnel also undergo fire detection and response training on a regular basis.

Power

To achieve a 24/7 uninterrupted service, Alibaba Cloud data centers are powered by dual main supplies and redundant power systems. The primary and secondary power supplies and systems have the same power supply capabilities. In case of a power failure, redundant battery packs and diesel generators are enabled to power data center devices, thus allowing the data center to run continuously for a certain period of time.

Temperature and humidity

Alibaba Cloud data centers are fitted with precision air conditioners to ensure constant temperature and humidity levels, which are electronically monitored. In case of any fluctuation in temperature or humidity outside of the normal range, an alarm is triggered and corrective actions are immediately taken. All air conditioning units work in hot standby mode.

5.1.1.2. Personnel management

Access management

At each Alibaba Cloud data center, long-term access permissions are assigned only to corresponding maintenance personnel. If an employee is transferred to another position or leaves the company, access permissions of the employee are cleared immediately. If it is necessary for any other person to enter the data center, the person must submit a formal application in advance, and is granted temporary permission only upon the approval of the corresponding department heads. For each entry to or exit from the data center, such persons must display their ID to check in, and be escorted by the data center's maintenance personnel for the entire duration of the visit.

An Alibaba Cloud data center consists of equipment rooms, electrical measurement areas, warehouses, and other areas, with each area equipped with an independent access control system. Two-factor authentication (such as biometric verification) is employed for sensitive areas, and special areas are physically isolated by metal cages.

All Alibaba Cloud data centers and office areas have access control, with visitor areas marked out separately. Visitors are required to carry entry pass and be escorted by Alibaba Cloud staff when visiting Alibaba Cloud premises.

Account management and identity authentication

Alibaba Cloud uses a central account management and identity authentication system to manage employee accounts throughout their lifecycle. For more information, see 5.1.5. Identity and access control.

Authorization management

Alibaba Cloud grants minimum resource access permissions to employees based on their positions and roles while ensuring separation of duties. An employee can log on to the central permission management platform to apply for access permissions to VPN Gateway, Bastion Host, control platforms, and production systems as needed. The requested permissions are granted to the employee upon the approvals of the supervisor, data or system owner, security administrator, and relevant departments.

Separation of duties

Alibaba Cloud separates duties between O&M permissions by role to prevent permission violations and audit failures. Duties are separated between O&M and audit staff, with the security team being responsible for the audit. Duties are also separated between the database and system administrators.

5.1.1.3. O&M audit

Surveillance

Alibaba Cloud data centers and server rooms are equipped with security surveillance systems covering all the areas and passages, and staffed with security guards for 24/7 patrol. All the surveillance videos and documents are saved and reviewed by dedicated personnel on a regular basis.

Audit

All the maintenance operations on the production system can only be performed with Bastion Host. The entire operation process is recorded in logs, which are then transferred to a central logging platform in real time. Alibaba Cloud defines audit rules for violations in accordance with its Account Usage Specifications and Data Security Specifications. Any violations will be handled by security personnel accordingly.

Internally, all the sensitive operations are logged in the management system that has a browser/server (B/S) structure, as stated in Alibaba Cloud log audit specifications, and such logs are transferred to the central logging platform. The central logging platform provides only the APIs for collecting and reading, not for modifying and deleting logs.

5.1.1.4. Storage Device Management

Alibaba Cloud has established a security management system for the full lifecycle of devices, including reception, storage, placement, maintenance, transfer, reuse, or decommissioning. For devices involving storage media (such as HDD, SDD, flash memory cards, equipment containing storage chips), asset management is refined to the component level (for example, to the storage medium or the unique hardware identification information of the device containing the storage medium.)

The security management process is specified to the SOP operation level and documented in the on-site operating guidelines. Device-level operations follow a “work order specific” protocol for process and online systems. This means unless a work order is being fulfilled, no device-level operation can be conducted. The work order contains unique hardware identification information of the operating device.

SOP and asset management are cross-examined by different teams. The IDC risk management team implements both regular and unscheduled inspections. Joint audit of internal risk is carried out by multiple departments, such as the safety compliance and internal control departments, to ensure the consistency of online records/offline operations and the reliability of process safety control. Equipment access control and operating status monitoring are strictly managed, and equipment maintenance and inventory checks occur regularly.

For storage media, Alibaba Cloud has established a bottom line requirement that storage media are not allowed to leave a site or a physically controlled area without data destruction or physical media destruction to prevent data security issues in the production environment.

5.1.1.5. Data destruction

Secure erasure

Alibaba Cloud follows NIST SP800-88 to establish the storage media sanitization process. The data stored in the storage media will be erased multiple times to ensure the data is sanitized permanently. The unneeded storage media will be physically shredded. The media disposal and data sanitization process are tracked through records retained. Each device is assigned a unique ID for tracking the record throughout the whole process. The evidence can be traced using the unique ID to check the sanitization status, such as data destruction logs and surveillance videos.

Disposal of cloud service customer data

Alibaba Cloud deletes data assets of the customers promptly or returns the data assets according to relevant agreements. Alibaba Cloud uses data erasure techniques that meet industry standards. The erasure operations are logged to prevent unauthorized access to customer data.

Alibaba Cloud O&M personnel are not allowed to access customer data without prior consent from the customers. In line with the principle of keeping production data within the production cluster, any channels for production data to flow out of the production cluster are blocked via technical means, thus preventing O&M personnel from copying data from the production system.

5.1.1.6. Network isolation

Alibaba Cloud isolates production networks from non-production networks. Direct access from a non-production network to any servers and network devices in a production network is not allowed. Alibaba Cloud isolates the cloud service network that provides services to external users from the physical networks that supports the underlying cloud service functionalities. Network ACLs are configured to prohibit access from cloud service network to physical network. Alibaba Cloud also takes network control measures to prevent unauthorized devices from connecting to the internal network of the cloud platform and prevent the physical servers of the cloud platform from initiating external connections.

Alibaba Cloud deploys Bastion Host on production network boundaries. The O&M personnel in the office network can access the production network for O&M only through Bastion Host. When logging on to Bastion Host, O&M personnel must perform multi-factor authentication, namely a one-time password is required apart from the regular domain account name and password. Bastion Host uses advanced encryption algorithms to ensure the confidentiality and integrity of data transmitted through O&M channels.

5.1.2. Hardware security

5.1.2.1. Firmware security

Secure firmware is one of the foundations for overall cloud computing security. The firmware used within the Alibaba Cloud infrastructure is securely hardened. Such hardening techniques include firmware baseline scanning, high-performance GPU instance protection, BIOS secure update, and BMC firmware protection.

- Firmware baseline scanning: The version and other related information of hardware and firmware are scanned on a regular basis for any potential exceptions.
- High-performance GPU instance protection: This technique provides protection to critical GPU registers that the GPU flash cannot be modified by the users' virtual machines, and sensitive assets such as the GPU's firmware cannot be tampered with.
- BIOS secure update: This technique ensures that only the BIOS images signed by Alibaba Cloud are flashed to the servers to avoid BIOS-level attacks such as malicious BIOS flashing.
- BMC firmware protection: This technique prevents unauthorized BMC firmware flashing in the host operating system.

5.1.2.2. Encrypted computing

Alibaba Cloud platform uses Intel® Software Guard Extensions (Intel® SGX) to provide a hardware-trusted execution environment. Users can establish a trusted execution environment to protect their sensitive data such as encryption/decryption keys. The root of trust in cryptographic computing is based on the processor chip, not on the underlying software. Therefore, all encrypted information can only be computed and run in a trusted execution environment, providing a high level of hardware-based data protection.

5.1.2.3. Trusted computing

Alibaba Cloud uses trusted computing technology to provide trust at the system and application level. Specifically, security critical servers use TPM 2.0-based security measurement and verification to ensure a secure computing environment. Furthermore, to ensure the security of trusted applications, Alibaba Cloud monitors and manages a trusted application whitelist on security critical applications.

TPM 2.0 and vTPM technologies are used to measure the underlying software stack on physical machines and VMs during the boot up process, and the trusted computing technology is used to verify the measurement results. The underlying software being measured includes BIOS, BootLoader, OS kernel, and loaded system modules and applications. Security O&M personnel can determine whether the system can be trusted by verifying the measurement results and taking the corresponding security responses such as reinstalling the correct software version or performing business migration.

The trusted computing technology can also record and analyze the execution behaviors of an application, such as process startup, file access, and network access, and creates its behavior whitelist and model. When the application is running, the service dynamically measures the collected application behaviors and compares the measurement results with the permissible actions in the whitelist to determine whether the application can be trusted. Based on the verification results, the security O&M personnel can take measures such as reinstalling the correct application version.

5.1.3. Virtualization security

Virtualization technology is the foundation of cloud computing. It ensures isolation between multiple tenants in a cloud computing environment by means of virtualized computing, storage, and network. Alibaba Cloud virtualization security technology mainly involves five security features, namely tenant isolation, security hardening, escape detection, hotfix patching, and data erasure.

5.1.3.1. Tenant isolation

Virtualization plays a crucial role in tenant isolation. Based on the hardware virtualization technology, VMM allows VMs on multiple computing nodes to be isolated from each other at the system layer. It prevents unauthorized access to system resources between tenants and guarantees basic computing isolation between computing nodes. The virtualization management layer also provides storage isolation and network isolation. For more information about tenant isolation, see 6.1.1.1. Tenant isolation.

- **Computing isolation**

  Alibaba Cloud provides a variety of cloud-based computing instances and services that allow automatic scaling to meet application or business needs. These computing instances and services provide computing isolation at multiple levels to protect data while ensuring configuration flexibility. The key isolation boundaries are between the management system and VMs, and between VMs themselves. Such isolation is provided by the hypervisor. Alibaba Cloud platform uses a virtualized environment where ECS instances run as standalone VMs and the isolation is enforced by using different permission levels (i.e. ring levels) of physical processors to avoid unauthorized access of a user's VM to the host and to another VM.

- **Storage isolation**

  In the basic design of cloud computing virtualization, Alibaba Cloud separates VM-based computing from storage. This separation allows computing and storage to be scaled independently, and makes it easier to provide multi-tenant services. At the virtualization layer, the hypervisor substitutes a virtual device for its physical equivalent storage device. All the I/O operations of a VM are intercepted by the hypervisor to ensure that the VM can only access the physical disk space allocated to it, thus implementing security isolation of hard disk space between different VMs.

- **Network isolation**

  To provide network connections for ECS instances, Alibaba Cloud connects the instances to the Alibaba Cloud virtual network. Alibaba Cloud’s virtual network is a logical structure built on top of the physical network structure. All the logical virtual networks are isolated from each other. Such isolation prevents network traffic data from being snooped or intercepted by other malicious instances.

5.1.3.2. Security hardening

Security hardening refers to the use of various technical means to reduce the possible attack surface in the hypervisor. Alibaba Cloud uses a lightweight KVM-based hypervisor developed specifically for cloud computing. The hypervisor combines the needed hardware and software capabilities by design, and focuses on supporting only hardware virtualization for the cloud infrastructure underneath. To reduce the potential impact of zero-day vulnerabilities, the Alibaba Cloud hypervisor limits the number of calls to system-level dynamic libraries without affecting functionality or performance. In summary, Alibaba Cloud minimizes the amount of code that is not related to devices on the cloud at the hypervisor level, therefore reducing the attack surface. In addition, all virtualization software must be compiled and run in a trusted execution environment to ensure that each binary file is not maliciously altered or replaced during runtime. Alibaba Cloud uses a series of trusted computing technologies to ensure the security of the entire virtualization software stack, and provides a complete set of control mechanisms to ensure that these virtualization software binary files are not accessible by external malicious parties.

Alibaba Cloud also hardens security at the hypervisor and host OS/kernel levels. For example, hypervisor permissions are downgraded during dynamic runtime, and the kernel is prevented from executing user space code. This increases the difficulty of permission escalation after an escape. Memory address layout randomization, restricted kernel symbol access, and memory page protection features are implemented to increase the difficulty of memory overflow type attacks. Alibaba Cloud continues to introduce new security features into the hypervisor and host OS/kernel, including the latest security features developed by Alibaba Cloud and the open source community.

5.1.3.3. Escape detection

Intrusions at the virtualization level mainly include VM escape attacks. VM escape typically involves two steps: First, the VM controlled by the attacker is placed on the same physical host as the target VM. Next, the attacker escapes the isolation boundary to intercept any sensitive information from the target VM or perform operations that compromise the functionality of the target VM.

The Alibaba Cloud hypervisor uses advanced VM distribution algorithms to prevent malicious VMs from running on a targeted physical machine. VMs cannot proactively detect the physical host environment in which they are located. At the hypervisor level, Alibaba Cloud also detects abnormal VM behaviors (i.e. potential attack events) by performing the following operations: analyze and monitor Coredump files in real time, detect suspicious code snippets loaded and executed by the hypervisor in real time, audit VM calls to system functions and abnormal VM Exit behaviors, monitor and analyze possible abnormal behaviors such as irregular process execution and network behaviors of hosts.

When an attack is detected, Alibaba Cloud locates and discards the VM that initiated the attack, reconstructs the attack chain in a timely manner, and performs hotfix patching on any discovered vulnerabilities.

5.1.3.4. Hotfix patching

Alibaba Cloud virtualization platform supports hotfix patching technology, which can fix system defects or vulnerabilities without user intervention, thus keeping any negative effects on user business operations to a minimum.

5.1.3.5. Data erasure

Data erasure is an extension of storage virtualization. After an ECS instance is released, its original disk space and memory space are reliably scrubbed to ensure user data security.

5.1.4. Cloud product security

Alibaba Cloud provides a variety of cloud products, such as Elastic Compute Service (ECS), Object Storage Service (OSS), Virtual Private Cloud (VPC), Relational Database Service (RDS), and MaxCompute. For more information about security features and capabilities of cloud products, see 6. Cloud product security.

5.1.5. Identity and access control

5.1.5.1. Identity management

Alibaba Cloud uses an identity authentication system to provide account lifecycle management for internal users such as regular employees, interns, outsourced employees, and partner employees. Each user is assigned a unique account, and the user must use such an account when dealing with corporate data. Once an account is assigned, the account cannot be shared, and unified logon management, password management, and access control of the account are enforced. When internal users leave Alibaba Cloud, move to new positions, or change their job responsibilities, the account resources used or managed by them must be revoked and/or transferred to proper Alibaba Cloud personnel.

5.1.5.2. Password management

Alibaba Cloud assigns each user a unique account, and each account has a clear owner. A unified password policy is employed. It requires users to configure a password that meets certain length and complexity requirements and to change the password on a regular basis (further, users are prevented from reusing their previous password). Multiple logon authentication modes are supported, such as account and password logon, one-time password logon, and digital certificate logon.

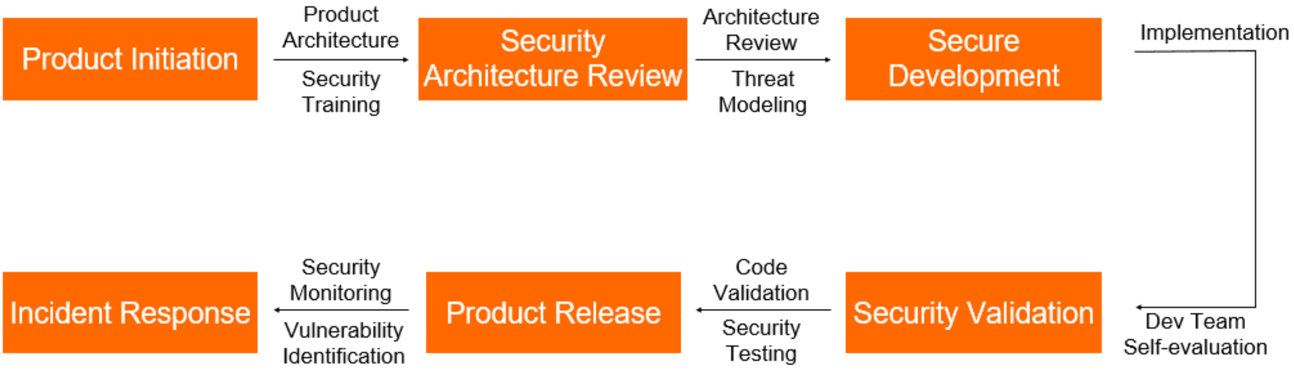
5.1.5.3. Permission management

Alibaba Cloud assigns permissions based on business needs, and centrally manages permissions by role, user group, department, and user. Each internal user can apply for and use permissions through the permission management system, and the permissions can also be revoked through the system. To strengthen permission management and reduce the risk of using incorrect permissions, Alibaba Cloud sets different levels of permissions and roles according to risks, and implements different approval processes accordingly at different permission levels. The system automatically freezes permissions that have not been used for a certain period of time. For users who leave Alibaba Cloud, the system automatically freezes their accounts and reclaims their permissions. For users who move to new positions, the system automatically revokes their permissions.

5.1.6. Security monitoring and operations

5.1.6.1. SPLC

Secure Product Lifecycle (SPLC) is a solution tailored for cloud products, designed to integrate security into the entire product development lifecycle. With SPLC, a complete security development mechanism is put into place at each stage, from product architecture review, development, validation, all the way up to incident response, to ensure that the products meet the rigorous security requirements for cloud computing. As a result, SPLC helps to greatly improve security capabilities and reduce security risks in cloud products.



As shown in the preceding figure, the entire security lifecycle of a cloud product can be divided into six stages: product initiation, security architecture review, secure development, security validation, product release, and incident response.

In the product initiation stage, the security architect works together with the product team to establish a functional requirement document (FRD) and a detailed architecture diagram based on business requirements and technical frameworks, and also extract the security baseline requirements applicable to a product. Meanwhile, applicable security training courses and exams are arranged for the product team at this stage to prevent security risks in the subsequent development stage of the product.

In the security architecture review stage, the security architect evaluates the security architecture of the product based on the FRD and architecture diagram established in the previous stage, and creates threat models for the product. In the process of threat modeling, the security architect creates detailed models for every asset that requires protection, security requirements of assets, and attack scenarios, and then proposes corresponding security solutions. Based on the preceding security baseline requirements and the security solutions proposed in threat modeling, the security architect then works with the product team to determine all the security requirements for the product.

In the secure development stage, the product team must develop the product in accordance with the security requirements, and implement the relevant security features and requirements of the product. To ensure the rapid and continuous development, release, and deployment of cloud products, the product team carries out self-testing at this stage to confirm that the security requirements have been implemented, and provides corresponding test information such as code implementations and test reports to prepare for the next stage of security validation.

In the security validation stage, the security team implements comprehensive security reviews on the architecture, design, and server environment of the product according to the security requirements, and also performs code review and penetration testing on the product. Any product with security problems found in this stage must be amended.

In the product release stage, only after the product passes the security validation and obtains the security approval, can it be deployed to the production environment through a standard deployment system.

In the incident response stage, the incident response team constantly monitors the cloud platform to discover possible security problems, and identifies security vulnerabilities through external channels such as Alibaba Security Response Center (ASRC) or internal channels such as internal security scan and self security testing. Once a security vulnerability is detected, the incident response team quickly rates the vulnerability and determines its priority and schedule for fixing. The incident response team ensures a rational allocation of resources in order to efficiently fix vulnerabilities to guarantee the security of Alibaba Cloud and its users.

5.1.6.2. Cloud platform security monitoring

The main purpose of security monitoring on the cloud platform is to promptly discover security incidents in which platform resources such as applications, hosts, and networks are attacked, and then trigger the internal incident response process to properly handle the incidents and eliminate potential impact.

Security monitoring mainly consists of three parts: log collection, anomaly analysis and detection, and alerting. Log collection aims to collect logs of hosts, networks, applications, and cloud products on the cloud platform, and import them into online real-time (such as Blink) and offline (such as MaxCompute) computing platforms. Anomaly analysis and detection aims to process and analyze the logs through security monitoring algorithms in each computing platform to monitor and identify risks. Once a security incident is discovered, an alert will be displayed on the security monitoring platform of Alibaba Cloud, and security emergency personnel will be notified via DingTalk (IM), SMS, or email to immediately handle the incident.

5.1.6.3. Penetration testing on the cloud platform

Alibaba Cloud has developed plans to conduct attack-and-defense drills on the cloud platform. During a drill, Alibaba Cloud organizes a specialized team of cyber penetration and attack experts to conduct security tests against Alibaba Cloud by means of periodic attack-defense confrontation. The drill is designed to objectively test the defense and threat detection capabilities of Alibaba Cloud, enhance the core security capabilities of Alibaba Cloud, and improve the security defense system.

Such security attack drills are performed to test the security status of the cloud platform in the following aspects:

- Whether the current defense measures are effective
- Whether the current intrusion detection measures are effective
- Whether there are any blind spots in the current defense measures
- Determines the effectiveness of the current security protection mechanisms, and

identifies areas that require further improvement

5.1.6.4. Cloud platform incident response

Cloud platform incident response refers to actions taken by Alibaba Cloud in response to internally detected and externally reported vulnerabilities and security incidents. Internally, Alibaba Cloud discovers possible security incidents through log collection, anomaly analysis and detection, and alert generation. The external reporting channels include Alibaba Security Response Center (ASRC), Alibaba Cloud Crowdsourced Security Testing Platform, externally reported Common Vulnerabilities and Exposures (CVE) vulnerabilities of open source third-party components, and threat intelligence information from third parties.

Alibaba Cloud will respond to security incidents and vulnerabilities as soon as they are discovered. The first step in incident response is to verify the authenticity of the reported vulnerabilities and security incidents. Once the vulnerabilities and security incidents are confirmed, Alibaba Cloud security team will initiate the incident response process and follow the standard protocols. The security severity level and impact scope of a vulnerability will be confirmed, and the response team will ensure resources are properly allocated so that the vulnerability can be fixed and the affected Alibaba Cloud product can be brought online within the corresponding SLA time. The steps to handle a security incident include confirming the impact scope of the incident, eliminating the impact, reviewing the incident, and making subsequent improvements. Meanwhile, the incident response team will promptly notify users of security issues through online announcements. Alibaba Cloud has a rigorous incident response process in place to ensure that every security incident is handled rigorously and quickly.

To ensure the effectiveness of the incident response process, Alibaba Cloud has set up a dedicated team to conduct attack drills from time to time. Alibaba Cloud also regularly invites third-party teams to conduct penetration testing on the Alibaba Cloud platform to verify the effectiveness of the Alibaba Cloud security protection system and the reliability of the incident response process.

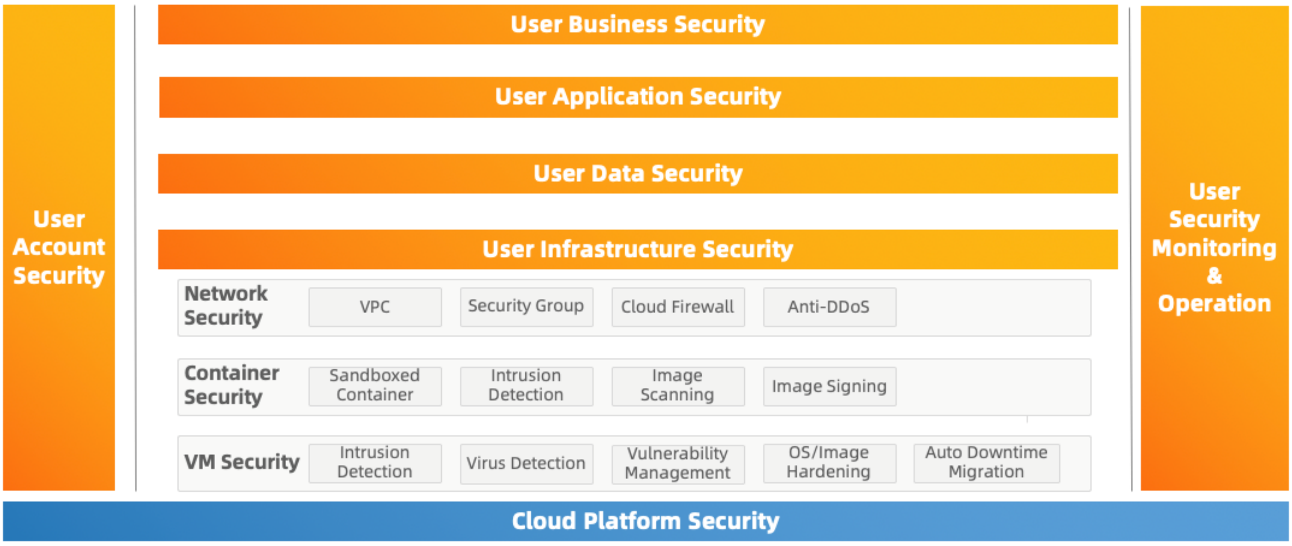
5.1.6.5. Change management

The virtualization system is the foundation of cloud computing. Any changes to the virtualization system can directly affect cloud operations. Alibaba Cloud has established a comprehensive change management process based on ISO/IEC 20000, where changes are classified based on the degree of emergency and are managed by category based on their sources and targets. The criteria for judging possible outcomes from various changes are also clearly defined. The whole change process is standardized and is supported by automatic systems and tools. Any changes need to go through a series of phases from application, evaluation, approval, test, implementation, and finally to verification. The responsibilities of various personnel involved in the process are clearly defined.

- Application phase of change: Key actions, including application submission, documentation, reception, and approval, are clearly defined.
- Implementation phase of change: including the change scheme, plan, assessment, and implementation. All the changes are tested before being implemented. The change time window and change scheme are subject to strict review. In addition, Alibaba Cloud will send a change notice to customers who may be affected by such change. Important change operations must be reviewed and confirmed by two persons.
- Verification phase of change: including change verification, configuration item review, and change result notification. Alibaba Cloud records all the information throughout the change process and deploys an automatic configuration check tool to verify the configurations of infrastructure and information systems after a change.

5.2. User infrastructure security

Alibaba Cloud Security Architecture



The user infrastructure security capabilities and requirements of cloud users focus on three aspects: host security, container security, and network security. These aspects involve the use of networks to isolate and protect the most important computing resources. Cloud applications and services of users are directly or indirectly built (through upper-layer cloud services) and run on the basic computing and network service modules. Therefore, the user infrastructure security and cloud platform security capabilities mentioned in the previous chapter together lay a solid foundation for users' upper-layer business security on the cloud.

In addition to computing and network resources, storage resources are also crucial to users, especially in the protection of user data. This will be explained in detail in the User data security section. The user-side security architecture also includes two vertical dimensions: user account security and user security monitoring and operations. These vertical dimensions are involved in each horizontal dimension, such as configuration security check for VM hosts during security monitoring and control over permissions of various cloud resources for account security. For more information, see the relevant sections.

5.2.1. VM security

5.2.1.1. Intrusion detection

Alibaba Cloud users can install the lightweight Security Center agent on their VMs. The agent is integrated as part of the Alibaba Cloud Security Center product, and can detect intrusion attempts in real time. The intrusion detection for VMs includes remote logon detection, Webshell detection and removal, anomaly detection (detection of abnormal process behaviors and abnormal network connections), and detection of changes in key files and suspicious accounts in systems and applications. Security Center can also intelligently learn application whitelists. It can identify trusted and suspicious and malicious applications and create application whitelists to prevent applications that are not authorized by the whitelists from running undetected and prevent VMs from being compromised by untrusted or malicious applications.

5.2.1.2. Virus detection

Security Center can also intercept mainstream viruses such as ransomware, mining scripts, and DDoS trojans in real time. It monitors and analyzes files and processes at the VM’s system kernel level in real time, and can effectively overcome the anti-detection technologies of trojans and malware. Based on application behavior analysis, Security

Center can also discover and intercept threats that are not included in blacklists. Its cloud virus database integrates leading-edge technologies that allow real-time virus update, such as mainstream anti-virus engines inside and outside China. Additionally, Security Center also integrates with technologies such as sandbox and machine learning engines that are developed by Alibaba Cloud, which can avoid losses caused by failures to update the virus database in time.

5.2.1.3. Vulnerability management

Alibaba Cloud users can install the lightweight Security Center agent on their VMs to scan for any vulnerabilities. Based on the cross-platform vulnerability scanning and repair engine developed by Alibaba Cloud, Security Center can help users scan and fix multiple systems and applications simultaneously during O&M. Currently, Security Center can detect mainstream vulnerabilities in Windows, Linux, and Web-CMS systems and applications. It can also offer vulnerability detection and patching capabilities in applications for which official patches are unavailable.

5.2.1.4. OS and image hardening

An OS security benchmark certified by the international third-party organization Cyber Internet Security (CIS) has been published for Aliyun Linux 2 OS. Users can follow the security best practices (i.e. remediations) in the CIS Benchmark to enhance OS security, or use the CIS Benchmark Remediation Kit to automatically harden Aliyun Linux 2. The CIS Benchmark documentation and the Remediation Kit are available through the CIS official website.

An image is an operating environment template for ECS instances. It generally includes an operating system and preinstalled software. Alibaba Cloud ECS tenants can use an image to create ECS instances and change system disks of ECS instances. The security enhancement of Alibaba Cloud public images (available in various Linux and Windows release versions, including Aliyun Linux 2) contains three parts: image security configuration, image vulnerability fixing, and default security software in an image. Alibaba Cloud monitors the vulnerabilities in Alibaba Cloud public image continuously to ensure that all high-risk vulnerabilities in Alibaba Cloud public images are fixed in a timely manner. In addition, all Alibaba Cloud public images include the Security Center agent by default (users can choose to opt-out) to guarantee the security of instances upon startup.

5.2.1.5. Automatic downtime migration

ECS instances are deployed on physical hosts (physical servers) that may fail due to performance anomalies or due to hardware failures. After detecting a fault on a host, the system will trigger a protective migration to migrate the ECS instances on the host to a normal host automatically to ensure the normal operations and high availability of instances and applications.

5.2.2. Container security

5.2.2.1. Sandboxed containers

Alibaba Cloud Container Service for Kubernetes (ACK) provides a secure container version based on Alibaba Cloud ECS Bare Metal Instance. The entire framework is implemented based on Alibaba Cloud sandbox technology. Unlike the traditional shared kernel architecture of Docker containers, each secure container has an exclusive kernel that maintains independent memory, network, and I/O resources. Based on this framework, multi-tenant security isolation can be enforced more efficiently on a single host.

5.2.2.2. Intrusion detection

Alibaba Cloud Container Service supports Security Center based intrusion detection. Security Center can monitor process startup logs and network connection logs in containers, and detect and fix Web-CMS vulnerabilities, Webshell, malware and trojan, suspicious process behavior, and abnormal network connections.

5.2.2.3. Image scanning

Alibaba Cloud Container Registry provides secure scanning of some Linux-based images. This feature can discover the latest CVE vulnerability information related to scanned images and, if applicable, offer vulnerability fixing suggestions to users.

5.2.2.4. Image signing

Signing and verifying container images can ensure that only container images that have been confirmed with the signature of container users are deployed in ACK. With image signing and binary authorization, container users can require images to be signed by trusted authorities during the development process and then enforce signature validation when deploying the images. By enforcing validation, container users can ensure that only verified images are integrated into the build-and-deploy process and thus can gain tighter control over their container environment. Container users can also use binary authorization for further security policy configuration.

5.2.3. Network security

5.2.3.1. VPC

Based on tunneling technology, Virtual Private Cloud (VPC) can help build an isolated virtual network environment. The intranet communication within a VPC is completely isolated from other VPCs. Users can customize IP address ranges, CIDR blocks, routing tables, and gateways within their VPCs, and connect on-premises data centers to VPCs through services such as VPN Gateway, Express Connect, and Smart Access Gateway. Users can also use Cloud Enterprise Network (CEN) to connect network resources across the globe to facilitate communications including VPC to VPC and VPC to IDC communications, and form an on-demand network environment that enables smooth migration of applications to the cloud, as well as expansion of data centers.

5.2.3.2. Security group

A security group is a virtual firewall provided by Alibaba Cloud for ECS instances. It provides Stateful Packet Inspection (SPI) and packet filtering functions, and can be used to isolate security domains between ECS instances (or container clusters in Container Service) on the cloud. Security groups are logically isolated groups of instances that are located within the same region and share the same security requirements while also being mutually accessible. Security groups are used for network access control over one or more ECS instances. As an important means of security isolation, security groups logically isolate security domains on the cloud.

Each instance belongs to at least one security group. Instances in the same security group can communicate through the network. By default, instances in different security groups cannot communicate with each other. Security group rules can be configured to authorize mutual access between basic security groups. However, mutual access between advanced security groups is not allowed.

5.2.3.3. Cloud Firewall

Alibaba Cloud Firewall is the industry's first firewall as a service (FWaaS) solution targeted for public clouds. It centrally manages control policies for the access traffic from the Internet to ECS instances (Internet traffic), and provides micro-isolation policies for the access traffic between ECS instances (intranet traffic). This is because in a cloud environment, users not only need to manage boundaries between the Internet and the intranet, but also need to manage network boundaries between cloud products, between VPCs, and even between ECS instances. With Cloud Firewall, users can analyze Internet and intranet traffic, gain full visibility into network-wide traffic such as traffic between security groups and Internet access traffic, and analyze and block external connections.

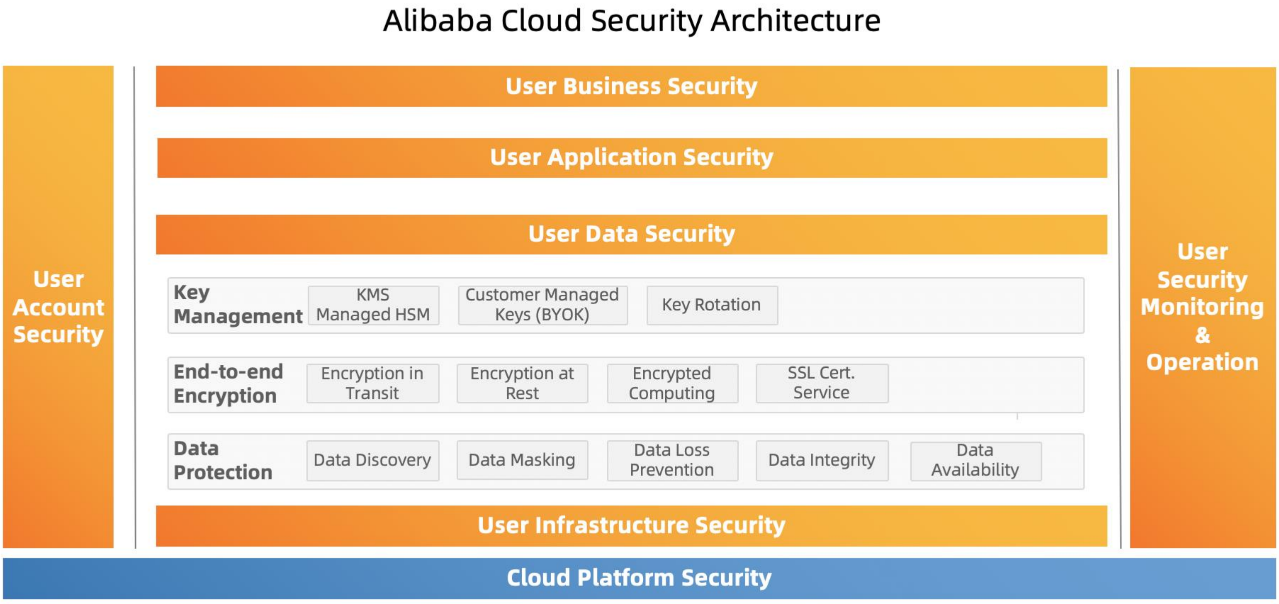
Based on traffic analysis, Cloud Firewall provides isolation and control at all levels of the entire network, including centralized control over public IP addresses, domain name-based access control, VPC-based isolation, and isolation of leased lines between Alibaba Cloud and on-premises data centers.

Cloud Firewall also integrates Intrusion Prevention Service (IPS) and threat intelligence capabilities for intrusion detection and analysis. By default, Cloud Firewall can also store network traffic and security event logs and firewall operation logs for six months.

5.2.3.4. Anti-DDoS

Alibaba Cloud secures all data centers with a self-developed Anti-DDoS service that provides protection against all types of DDoS attacks. It uses an AI protection engine to accurately identify attack behaviors and automatically load protection rules, ensuring network stability. Alibaba Cloud Anti-DDoS allows users to monitor risks and protection status in real time through security reports. Alibaba Cloud Anti-DDoS not only supports mitigating DDoS threats for users' business on Alibaba Cloud, but also allows them to use Alibaba Cloud's globally distributed scrubbing centers and AI protection engine for on premise businesses, in order to mitigate high-volume DDoS attacks and provide fine-grained protection against resource exhaustion attacks at the web application layer.

5.3. User data security



User data security on the cloud is one of the most critical security requirements of users and one of the most important representational attributes of the overall cloud security capability. The data of all developers, companies, governments, and social institutions on cloud computing platforms belongs only to these users. Cloud computing platforms cannot use the data for other purposes. Cloud service providers have responsibilities and obligations to help users ensure the confidentiality, integrity, and availability of their data.

The requirements for data security can be summarized as CIA - Confidentiality, Integrity, and Availability, which is considered the core underpinning of information security. Confidentiality means that protected data can only be accessed by authorized (or intended) users. Ways to achieve confidentiality include data access control, data loss prevention, data encryption, and key management. Integrity means that only authorized (or intended) users can modify data, which is mainly achieved through access control. The integrity of user data can also be ensured through integrity verification algorithms during data transmission and storage. Data availability is related to the overall security capability, disaster tolerance capability, reliability, and normal operating of all relevant cloud systems in such areas as storage, network access, authentication, and authorization verification. Alibaba Cloud data security capabilities help users prevent data breaches and meet compliance requirements such as personally identifiable information (PII) protection and GDPR.

5.3.1. Data protection

5.3.1.1. Data discovery

Large amounts of data are generated every day in the cloud. Discovering and classifying sensitive data that requires protection is essential to allow data protection mechanisms to operate effectively and efficiently. The first step in data discovery is to discover and detect sensitive data such as Personally Identifiable Information (PII). The second step is to further classify the data based on users' business scenarios and compliance and security requirements so that users are aware of their data assets and can choose targeted data protection mechanisms properly.

Alibaba Cloud Sensitive Data Discovery and Protection (SDDP) can discover and classify user data on the cloud. After being authorized by the users, SDDP can automatically scan and discover data within cloud products such as RDS, OSS, and MaxCompute. SDDP uses keywords, rules, and machine learning algorithms to accurately identify sensitive data within the cloud environment, and allows users to customize sensitive data discovery policies based on their needs. Based on the identification results of sensitive data, SDDP can classify user data on the cloud based on business content and sensitivity level and then implement relevant protection mechanisms for the data according to the discovery and classification results.

5.3.1.2. Data masking

After the sensitive data is discovered and classified, users often need to mask relevant sensitive data in order to protect data privacy. For example, users often want to be able to mask production data without changing data structures and distribution, and use it in scenarios such as testing, development, analysis, and data exchange with third parties.

SDDP provides nearly 30 built-in masking algorithms in six categories including hash, encryption, masking, replacement, shuffling, and transformation, and supports user-defined masking algorithms or parameters. SDDP ensures that data is masked without changing the original data distribution and the corresponding business system logic, and ensures the validity and availability of the data. Users can protect their data while accomplishing business needs at a low cost and high efficiency.

5.3.1.3. Data loss prevention

User data loss prevention involves the complete control over permissions on data and the monitoring and detection of data in use. To prevent data loss, users must first implement effective control over the permissions on storage and transmission products on the cloud. SDDP supports instant querying of data, users, and permissions, and provides centralized query capabilities against all applicable data permissions, SDDP can also resolve the mappings between Alibaba Cloud account permissions and relevant roles. SDDP can generate alerts for data permission configuration and usage exceptions that do not comply with the security best practices in the cloud environment.

It is also necessary to have comprehensive monitoring and detection capabilities in place during data transmission and processing, and to discover possible abnormal behaviors during data use in a timely manner. SDDP can effectively monitor exceptions that occur during the data transmission process, display the data flow lifecycle dynamically, and ensure compliant and orderly export and transmission of data. Based on log analysis, SDDP can effectively identify manual operations and API calls. Based on machine learning and big data analysis capabilities, SDDP can monitor and generate alerts for abnormal behaviors that arise during various data flows and operations.

Finally, after data loss is discovered and alerts are sent, SDDP analyzes suspicious events for subsequent data loss handling processes. The event analysis feature centrally collects various types of alert events, and uses time series analysis to restore the behavior baseline of responsible parties and display the historical baseline trajectory in real time, effectively improving analysis efficiency. SDDP can handle tenant events in isolation and feedback the handling results to the machine learning model, which makes anomaly detection increasingly accurate.

5.3.1.4. Data integrity

During data transmission and storage, Alibaba Cloud products provide end-to-end data integrity verification and scan data in the storage medium on a regular basis to ensure data integrity and reliability. Currently, OSS can return the CRC64 value of objects uploaded using any of the uploading methods provided. The client can compare the CRC64 value with that calculated locally to verify data integrity. An error-checking code is also generated and used throughout the storage process for fine-grained data integrity protection.

Data integrity is also guaranteed by the access authorization feature of Alibaba Cloud. For more information, see 5.6.2. Access authorization.

5.3.1.5. Data availability

Alibaba Cloud employs distributed storage. Files are split into multiple data segments and stored on different devices. Each data segment is stored in multiple replicas. Distributed storage improves data reliability and security. Based on product types/tiers and business needs, Alibaba Cloud products also provide multiple protection capabilities such as multi-copy redundancy, system backup, live migration, load balancing, and anti-DDoS to ensure high data availability. For example, OSS provides zone-redundant storage and can back up user data in three different AZs, ensuring 99.9999999999% (12 nines) durability and 99.95% availability.

5.3.2. End-to-end encryption

Alibaba Cloud uses end-to-end encryption to ensure data security, including encryption in transit, encryption at rest, and hardware-based encrypted computing service using Intel® Software Guard Extensions (Intel® SGX). Alibaba Cloud also provides HSM-based Data Encryption Service and SSL Certificates Service as part of a complete set of data encryption solutions.

5.3.2.1. Encryption in transit

Cloud products use the SSL/TLS protocol to ensure data transmission security while users read and upload data. The Alibaba Cloud console uses HTTPS encryption for data transmission. Alibaba Cloud products provide API access points that have HTTPS encryption enabled with 256-bit key length to address the need for encrypted transmission of sensitive data.

Alibaba Cloud gateway products also provide end-to-end encryption during data transmission. VPN Gateway securely and reliably connects on-premises data centers to Alibaba Cloud VPC over encrypted channels. VPN Gateway can establish an IPsec-VPN connection to connect an on-premises data center to a VPC. It can also establish an SSL-VPN connection to connect a remote client to a VPC. Alibaba Cloud also provides Smart Access Gateway (SAG) that allows enterprise users to access the nearest cloud resources through encrypted connections and encrypt the transmitted data with the Internet Key Exchange (IKE) and Internet Protocol Security (IPsec) protocols to secure data.

5.3.2.2. Encryption at rest

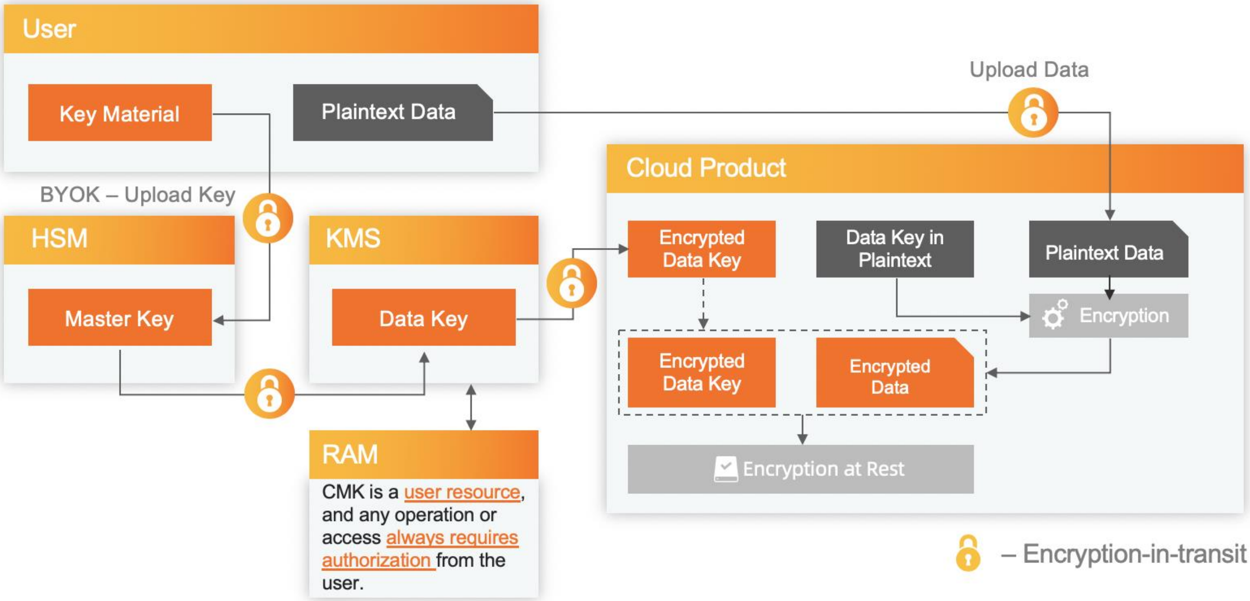
Alibaba Cloud allows users to encrypt data stored at rest in Alibaba Cloud services with integration of Alibaba Cloud Key Management Service (KMS). Alibaba Cloud supports the Advanced Encryption Standard with 256-bit key length ((AES256) for encrypting sensitive data at rest.

The encryption design varies with Alibaba Cloud services based on product features and business needs. Generally, a key hierarchy consisting of at least two layers is used, and data is encrypted using the envelope encryption mechanism. The first layer is the Customer Master Key (CMK), and the second layer is the Data Encryption Key (DEK). The CMK is used to encrypt and decrypt the DEK, while the DEK is used to encrypt and decrypt data. When a user stores data to a persistent storage medium, an Alibaba Cloud service writes both the ciphertext of the DEK (encrypted by KMS using the CMK) and the ciphertext of the data (encrypted by the Alibaba Cloud service using the DEK) to the persistent storage medium. This mechanism is known as envelope encryption. The ciphertext of the DEK and the ciphertext of the data are packaged together in an "envelope." When reading the encrypted data, the Alibaba Cloud service reads both the ciphertext of the DEK and the ciphertext of the data. The Alibaba Cloud service must decrypt the ciphertext of the DEK before using the decrypted DEK to decrypt the ciphertext of the data.

In envelope encryption, the CMK is protected by the key management infrastructure of KMS. Strict physical and logical security controls are implemented to prevent unauthorized access. The key management infrastructure of Alibaba Cloud conforms to the recommendations in (NIST) 800-57 and uses cryptographic algorithms and hardware security modules (HSMs) that comply with relevant compliance requirements. For example, the HSMs used outside of mainland China regions conform with FIPS 140-2 Level 3 standard. During the envelope encryption process, the plaintext of the CMK is stored and used inside the managed HSM of KMS. KMS also supports software-protected keys and protects these keys through its software cryptographic module. By hardening the software cryptographic module, KMS ensures that the plaintext materials of software-protected keys stay within the software cryptographic module and can only be loaded into memory within the boundary of the module. Moreover, the plaintext of the DEK never leaves the memory of the host where the Alibaba Cloud service instance in use resides. That is, the DEK will never be stored in plaintext in any persistent storage medium.

Encryption at rest allows users to use service managed keys as CMKs. Specifically, when a user uses the data encryption feature of an Alibaba Cloud service for the first time, the system automatically creates a CMK exclusively for the service in the user's KMS for the specific region in which the service is being used. This CMK is used as a service managed key and its lifecycle is managed by the cloud service. The user can query the CMK in the KMS console, but cannot delete it.

Several Alibaba Cloud services also support customer managed keys, including customer supplied keys (also known as Bring Your Own Key or BYOK) and customer generated keys through KMS. A user can use these keys as CMKs to encrypt data and manage the CMKs throughout their lifecycle. It is important to note that a customer managed CMK is the asset of a user. Alibaba Cloud services must obtain the authorization of the user through RAM before they can use the CMK to encrypt and decrypt data. The user can also cancel the corresponding CMK authorization at any time, thus gaining full control of the data encryption and decryption process.



For the sake of simplicity, unless otherwise specified, the rest of this white paper will use customer managed keys to refer to the use of customer supplied keys or customer generated keys as CMKs to encrypt data at rest.

Data encryption is enabled in different Alibaba Cloud services. For more information, see the corresponding section for each service in the rest of the white paper.

- EBS: encrypts block storage devices (cloud disks) used inside VMs to ensure that data is securely stored in a distributed system, and uses service managed keys and customer managed keys as CMKs to encrypt data.
- OSS: supports both server-side and client-side storage and encryption. In server-side encryption, OSS uses service managed keys and customer managed keys as CMKs to encrypt data. In client-side encryption, OSS allows the users to use on-premises self-managed keys or CMKs generated in Alibaba Cloud KMS to encrypt data on the client side.
- ApsaraDB for RDS: Multiple versions of ApsaraDB for RDS provide Transparent Data Encryption (TDE) or DB instance disk encryption mechanism. RDS uses service managed keys and customer managed keys as CMKs to encrypt data.
- Table Store: uses service managed keys or customer managed keys as CMKs to encrypt data.
- NAS: uses service managed keys as CMKs to encrypt data.
- MaxCompute: uses service managed keys as CMKs to encrypt data.

Additional services support encryption at rest and can use service managed keys or customer managed keys as CMKs to encrypt data. For more information, see the official web page for each cloud service at www.alibabacloud.com.

5.3.2.3. Encrypted computing

Alibaba Cloud platform uses Intel® Software Guard Extensions (Intel® SGX) to provide a hardware-based encrypted computing environment. Users can create a trusted execution environment through software to protect sensitive data such as encryption and decryption keys and account credentials. Based on ECS Bare Metal Instances that support encrypted computing, users can protect their data by writing code that supports the trusted execution environment. This ensures that their sensitive data can be accessed and manipulated only through the code that they write. With Alibaba Cloud encrypted computing technologies, Alibaba Cloud provides an additional data encryption capability at runtime through the SGX based trusted execution environment.

5.3.2.4. SSL Certificates Service

Alibaba Cloud Certificates Service can issue SSL certificates issued by well-known third-party certification authorities on the cloud to enable HTTPS for websites so that the websites are protected against traffic hijacking, tampering, and interception. The service also provides integrated certification lifecycle management on the cloud to simplify certificate deployment. Users can deploy the certificates to Alibaba Cloud services such as CDN, SCDN, DCDN, and SLB at the click of a button.

5.3.3. Key Management Service

Key Management Service (KMS) is a secure and easy-to-use management service provided by Alibaba Cloud. KMS provides functions such as secure hosting of keys and cryptographic operations, and implements security practices such as key rotation. KMS can be integrated into other cloud services to encrypt user data managed by these services. KMS's secure and reliable key management is an important prerequisite for data encryption capabilities in cloud services.

5.3.3.1. Managed HSM

In addition to the software cryptographic module that hosts customer managed keys in KMS, Alibaba Cloud KMS allows users to manage keys in HSMs and use HSMs for cryptographic and security management operations, providing a higher level of protection for CMKs.

Users can manage CMKs in HSMs that use hardware mechanisms to keep plaintext key materials within the boundary of HSMs. When users perform cryptographic operations in an HSM, the process of cryptographic operations only occurs in the HSM, ensuring the privacy of the CMKs. HSM managed CMKs can meet the relevant security and compliance requirements, while greatly reducing user management overhead through the built-in HSM management capabilities of KMS.

5.3.3.2. Customer managed keys

Each cloud service can manage a default service managed key in KMS for users and use the key to encrypt data. Users can audit the behaviors of cloud services that use KMS to encrypt and decrypt data. Although service managed keys can provide the most basic data protection capabilities, a few shortcomings exist for users who have a clear requirement for key management. For example, users are not allowed to manage the lifecycle of keys or set automatic rotation, and the service managed keys are only protected in the software cryptographic module of KMS.

With the support for customer managed keys (CMKs), users can choose to create or upload CMKs into KMS, and choose to use customer managed CMKs through supported cloud services. The users would in turn directly manage the lifecycle of these CMKs. After the authorization through RAM, customer managed keys can be used for data encryption of cloud services, and can empower users with stronger security capabilities:

- Users can disable or enable keys to control the capability of cloud services to encrypt and decrypt data.
- Users can configure authorization policies to control the capability of cloud services to encrypt and decrypt data.
- Users can import customer supplied keys to KMS (BYOK), further enhancing the capabilities of managing the lifecycle of keys and controlling the data encryption and decryption capabilities of cloud services.

When using customer managed keys and the preceding security capabilities, users are responsible for managing the authorization and lifecycle of the keys.

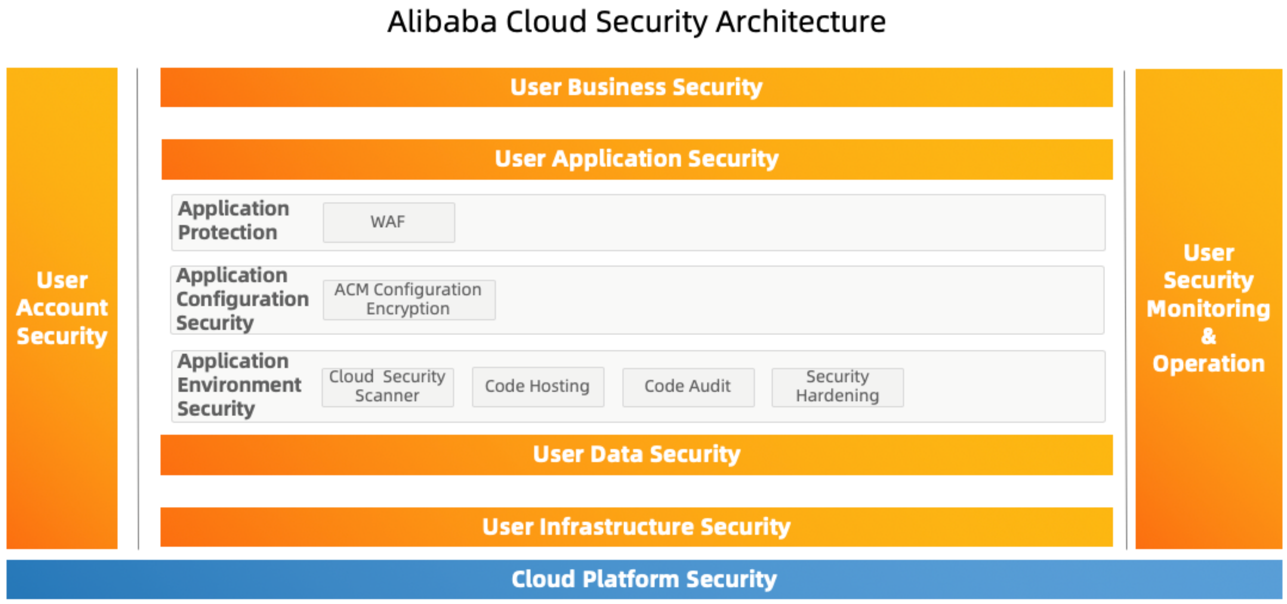
5.3.3.3. Key rotation

KMS integrates automatic key rotation based on the capability of supporting multiple versions of a CMK. With automatic key rotation, KMS automatically generates a new version of a CMK based on the configured schedule. All older versions are used to decrypt historical data. This reduces the attack surface for keys and protected data.

In certain scenarios, users may also re-encrypt historical data to convert the ciphertext generated with an older version of a CMK into the ciphertext encrypted with the new version.

Users can also manually rotate CMKs one or more times beyond the automatic rotation schedule when needed.

5.4. User application security


Alibaba Cloud Security Architecture
User Account Security
User Business Security
User Application Security
Application Protection
WAF
Application Configuration Security
ACM Configuration Encryption
Application Environment Security
Cloud Security Scanner
Code Hosting
Code Audit
Security Hardening
User Data Security
User Infrastructure Security
User Security Monitoring & Operation
Cloud Platform Security

Applications built on Alibaba Cloud also need to be properly secured. At the application security level, Alibaba Cloud provides users with security capabilities in three aspects: application environment security, application configuration security, and application protection.

5.4.1. Application environment security

5.4.1.1. Cloud Security Scanner

Cloud Security Scanner is a best practice in any digital transformation process. Cloud Security Scanner automatically discovers assets that are associated with a user’s website and performs automated penetration tests and detects sensitive content with high efficiency and accuracy. This guarantees a secure environment for the user’s website and applications. Cloud Security Scanner generates professional scanning reports after scanning tasks are completed. Cloud Security Scanner classifies detected risks into different types and offers troubleshooting solutions. It can help the user verify and fix vulnerabilities with professional assistance.

5.4.1.2. Code hosting

For cloud users, especially those who develop applications directly on the cloud, code protection is an important part of asset protection. Alibaba Cloud DevOps solution provides Git repositories for storing source code, and provides strict authorization control mechanisms. With the authorization management function, users can view their permissions on a specific Git repository or group. When users have authorization on a specific Git repository or group as a master or owner role, they can also view and modify the permissions of other members on the Git repository or group, and manage the permissions of other members based on the principle of least privilege.

5.4.1.3. Code audit

In the SPLC of cloud products, Alibaba Cloud security experts strictly review and validate source code security to ensure a high level of code security for Alibaba Cloud products. Alibaba Cloud also constantly performs code security scanning for software in Alibaba Cloud Marketplace to effectively reduce security risks. Meanwhile, Alibaba Cloud strongly recommends that enterprise users perform blackbox and whitebox code security validation and testing on their applications to prevent security vulnerabilities and enhance the security of their businesses.

5.4.2. Application configuration security

5.4.2.1. ACM configuration encryption

Application Configuration Management (ACM), formerly known as Taobao's internal configuration center Diamond, is now open-sourced as the configuration center module of the open source project Nacos. ACM is a product that centrally manages and pushes application configurations in a distributed architecture environment. With ACM, users can greatly reduce the workload of configuration management and enhance service capabilities in scenarios such as microservices, DevOps, and big data. To ensure the security of sensitive configurations such as data sources, tokens, usernames, and passwords and reduce the risk of user configuration information leakage, ACM provides the ability to create encrypted configurations. The configuration encryption methods provided by ACM include:

- Encryption through KMS: The configuration content cannot exceed 6 KB in size. The plaintext of the configuration content is transmitted to KMS to be encrypted.
- KMS-based AES-128 encryption: The configuration content must be 6 KB to 100 KB in size. It is recommended that the content does not exceed 10 KB in size. The plaintext of the configuration content is not transmitted to KMS. Instead, the configuration content is encrypted locally in ACM by using encryption keys managed by KMS, thus ensuring a higher level of security.

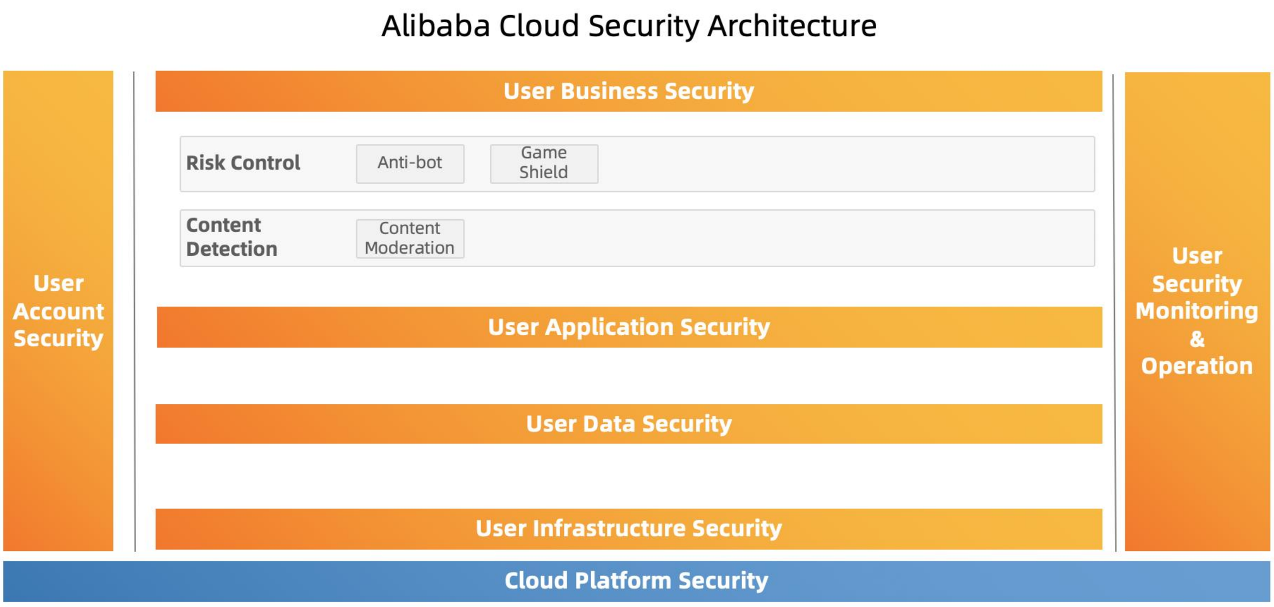
5.4.3. Application protection

5.4.3.1. WAF

Based on the big data and intelligent computing capabilities of Alibaba Cloud Security, Web Application Firewall (WAF) filters out a large number of malicious access attempts by defending against common security threats reported by OWASP, such as SQL injection, XSS, common vulnerabilities in Web server plug-ins, Webshell uploads, and unauthorized access to core resources. This prevents website asset leakage, thus safeguarding website security and availability.

It is worth mentioning that WAF relies on the powerful data computing and processing capabilities of Alibaba Cloud. By leveraging an industry-leading deep learning model, WAF reduces the false alarm rate while effectively improving the detection rate. WAF can also process high-risk requests in near real time based on big data collection and analysis capabilities by collaborating with client-side SDK. WAF also provides the capability of simultaneously deploying and upgrading of alerts and global response rules.

5.5. User business security



After a user's application has been built and run on the Alibaba Cloud platform, Alibaba Cloud provides corresponding security capabilities for different user business scenarios of the user. At the business security level, Alibaba Cloud provides security features in two aspects, namely content detection and risk control.

5.5.1. Content detection

5.5.1.1. Content Moderation

Alibaba Cloud provides the Content Moderation service. Based on the deep learning technology and years of big data analysis experience of Alibaba Cloud, Content Moderation provides intelligent risk identification of pictures, videos, texts, and other multimedia content. This service can help users identify adult, extremist, violence, terrorism, and other illegal or inappropriate content. It also helps minimize invasive advertising, abuse, and other factors that affect user experience, while greatly reducing manual audit costs. Content Moderation relies on the online computing and processing capabilities of Alibaba Cloud for real-time automated and accurate detection.

5.5.2. Business risk control

5.5.2.1. Anti-Bot Service

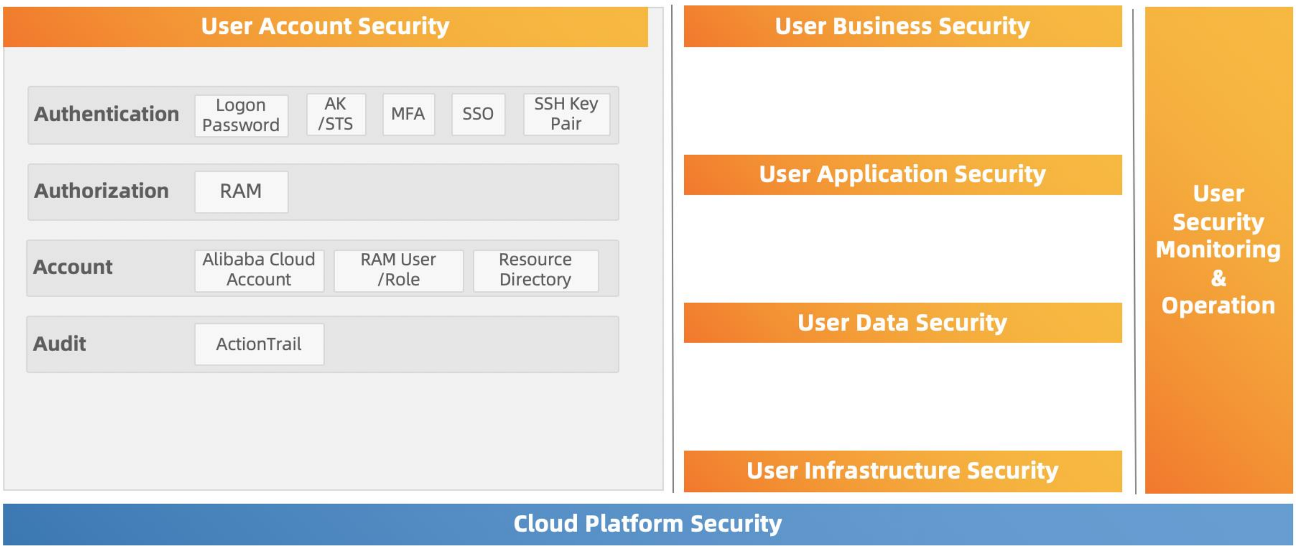
Preventing malicious bots on the cloud can effectively reduce and even eliminate the business impact of external malicious automation tools on users' websites. Anti-Bot Service can be used in the following scenarios: flight seating occupancy, online scalping, credential stuffing, core API exploitation, and vote count or reward point manipulation. Alibaba Cloud Anti-Bot Service provides comprehensive protection for webpages, H5 pages, applications, and APIs. It also provides large amounts of security threat information on the cloud and updates protection policies against bot attacks in a timely manner. Without changing the server-side code, users only need to change the CNAME record to seamlessly connect to Anti-Bot Service. All malicious bot traffic will be detected and filtered on the cloud, and normal traffic will be forwarded to the source server. This ensures that the business is protected from security issues such as data breaches and business fraud caused by malicious bot traffic.

5.5.2.2. GameShield

Alibaba Cloud provides the GameShield service for the gaming business on the cloud. GameShield is a network security solution launched by Alibaba Cloud to protect the gaming industry against DDoS attacks. Compared with Anti-DDoS Pro, GameShield can defend against TB-grade high-traffic DDoS attacks and TCP resource exhaustion attacks (Layer-4 CC attacks) that commonly target the gaming industry. This service reduces protection costs and provides a more effective protection for gaming industry users.

5.6. User account security

Alibaba Cloud Security Architecture



User account security is an important dimension in the overall cloud security architecture design. User account security on the cloud involves authentication, authorization, account management, and audit management. It is important to note that in cloud-based businesses, there is often a cloud product or service (such as RAM) that actually provides capabilities spanning more than one of the aforementioned dimensions. This chapter describes Alibaba Cloud account security capabilities specific to each dimension. For more information about the account security capabilities of various products, see the relevant chapters of this white paper.

5.6.1. Authentication

Identity authentication refers to the use of account credentials to verify the real identity of a user. An account credential usually refers to a user's logon password or Access Key (AK). Note that the account credentials used for identity authentication are confidential and must be kept in secret by Alibaba Cloud users.

5.6.1.1. Logon password

A user can use the logon password and user name of its Alibaba Cloud account or those of its RAM users to log on to the Alibaba Cloud console and perform operations on cloud resources. The password specifications of Alibaba Cloud accounts and the associated risk control policies for logon security are managed by Alibaba Cloud. The password policies for RAM users can be defined by the Alibaba Cloud account owner, which include the required character combinations of a password, the number of logon retries, and password rotation cycle, etc. For example, A user can create password policies for RAM users in the RAM console to ensure that each RAM user uses a strong password rotated on a regular basis. This improves overall account security.

5.6.1.2. Access Key

An Access Key (AK) is the credential used for calling Alibaba Cloud service APIs. It is used to authenticate the identity of users who access Alibaba Cloud resources through APIs. API credentials are equivalent to logon passwords. The former is used to call the API of a cloud service, while the latter is used to log on to the console.

An Access Key consists of an AK ID and an AK secret. The AK ID is used to identify a user, and the AK secret is used to authenticate the user's identity. When calling a cloud resource API, a user will pass in an AK ID and use an AK secret to sign the request based on the HMAC-SHA1 algorithm. An Alibaba Cloud account owner can log on to the Alibaba Cloud User Center or RAM console to manage Access Keys. The account owner can create, freeze, enable, and delete Access Keys. Since the AKs can be used for API requests for a long period of time, it is recommended that the user should rotate AKs on a regular basis.

Based on security best practices, it is recommended that a user should create different Access Key credentials for each RAM user to effectively divide permissions and reduce risks by following the principle of least privilege. Furthermore, an Alibaba Cloud account can be viewed as a “root” account, which has full control permissions for all cloud products and resources under the account. Hence, to avoid the risk of exposing the Access Key of the root account, it is recommended that all users should operate resources at the RAM user level and not create Access Keys for the root account unless absolutely necessary.

5.6.1.3. STS

Alibaba Cloud Security Token Service (STS) is a cloud service that provides trusted entities such as RAM users, Alibaba Cloud services, and identity providers with authorization credentials for short-term resource access. Some scenarios involve users (persons or applications) that do not regularly access the resources of a cloud account but only need occasional access, such users are called "temporary users." For some other users such as applications running on untrusted mobile devices, it is undesirable to issue them long-term Access Keys due to the insecure nature of the execution environment. In these cases, STS can be used to issue temporary authorization credentials to these users. When issuing a token, the administrator can define the permissions and expiration time (default expiration time is one hour) for the token as needed.

An STS access token is a triplet that includes a security token, an AK ID, and an AK secret. When calling a resource API, a user will pass in the security token and AK ID and use the AK secret to sign the request similar to the API Access Key signing mentioned previously.

5.6.1.4. MFA

Multi-factor authentication (MFA) is a simple and effective security best practice that provides an extra level of protection on top of usernames and passwords. With MFA enabled, a user is asked to enter a username and password (first security factor), and then a variable verification code (second security factor) from an MFA device when logging on to the Alibaba Cloud console. These factors combine to provide a higher-level of protection for user accounts. Alibaba Cloud supports software-based virtual MFA devices. A virtual MFA device is an application that generates a 6-digit verification code, and complies with the time-based one-time password (TOTP) standard (RFC 6238). The virtual MFA application can run on mobile hardware devices (including smartphones).

5.6.1.5. SSO

Alibaba Cloud supports SAML 2.0-based Single Sign On (SSO), which enables enterprise users to access Alibaba Cloud (as the service provider) by using the logon service of the enterprise's identity system (as the identity provider).

To meet the logon requirements of different enterprise users, Alibaba Cloud provides the following SSO mechanisms based on the SAML 2.0 protocol:

- User-based SSO: Alibaba Cloud determines the RAM user account that an enterprise user can use through a SAML assertion issued by the identity provider. After logon, the enterprise user can use the RAM user account to access Alibaba Cloud resources, and the corresponding access permissions are restricted by the authorization policy of the RAM user.
- Role-based SSO: Alibaba Cloud determines the RAM role that an enterprise user can use through a SAML assertion issued by the identity provider. After logon, the enterprise

user can use the RAM role specified in the SAML assertion to access Alibaba Cloud resources, and the corresponding access permissions are restricted by the authorization policy of the RAM role.

5.6.1.6. SSH key pair

SSH key pair is a secure authentication method offered by Alibaba Cloud to remotely log on to ECS Linux instances. An SSH key pair is a pair of keys generated by using a cryptographic algorithm. One key is made public, known as the "public key", and the other is kept secret by its user, known as the "private key". If the public key is configured in an ECS Linux instance, a user can use the private key to connect to the instance without the need to enter a password. This is done by using SSH commands or other related tools. By default, a 2048-bit RSA key pair is used. Compared with traditional methods that use usernames and passwords, the SSH key pair is more secure and reliable for logon authentication, making it convenient to remotely log on to a large number of ECS Linux instances. Alibaba Cloud Container Service also allows the user to remotely log on to a container cluster through an SSH key pair.

5.6.2. Authorization

5.6.2.1. RAM

Alibaba Cloud provides a variety of tools and features to help customers securely authorize access to resources in different scenarios. Among them, the Resource Access Management (RAM) service is provided for user identity management and resource access control. RAM enables an Alibaba Cloud account (i.e. primary or root account) to have multiple independent RAM users (i.e. subaccounts). This eliminates the need for an account owner to share its Access Key or other credentials with other users, and the account owner can assign minimum operation permissions to different RAM users based on the principle of least privilege. RAM can be used to define fine-grained authorizations at an API operation or resource ID level. RAM also supports various restrictive conditions on permission granting, such as constraints on source IP address, required SSL/TLS channel, access time period, and MFA.

RAM is the basis for the security management and O&M of Alibaba Cloud accounts. RAM can assign a different password or API Access Key to each RAM user, which eliminates security risks arising from sharing of Alibaba Cloud account credentials. Assigning different work permissions to different RAM users also reduces the risks by following the principle of least privilege.

5.6.3. Account management

5.6.3.1. Alibaba Cloud account

RAM is a centralized user identity management and resource access control service provided by Alibaba Cloud. Each resource has only one owner (i.e. resource owner). The owner must be an Alibaba Cloud account (also known as the primary account, root account, or resource owner). This account pays for and has full control over the resource.

The resource owner is not necessarily the resource creator. For example, if a RAM user is granted only the permission to create resources, the resources created by this user belong to the Alibaba Cloud account of the RAM user. In this case, the RAM user is the resource creator, but is not the resource owner.

5.6.3.2. RAM user

With RAM, an Alibaba Cloud account owner can create independent RAM user accounts for its employees, systems, or applications and control their access to cloud resources. Each RAM user can log on to the Alibaba Cloud console or call service APIs by using an independent logon password or Access Key. RAM enables an Alibaba Cloud account to have multiple independent RAM users. RAM also supports such features as MFA, strong password policies, separation of console users from API users, custom fine-grained authorization policies, grouped authorization, and temporary authorization token. By default, a newly created RAM user account does not have any permissions on resources. Only an authorized RAM user can perform operations on resources on behalf of the corresponding Alibaba Cloud account.

5.6.3.3. RAM role

A RAM role can be viewed as a virtual RAM user. It does not have any long-term authentication credentials (such as logon password or AccessKey pair). A RAM role must be assumed by an authorized RAM user identity before it can take effect. RAM roles can be used in scenarios such as cross-cloud-account resource authorization, resource access authorization among different cloud services, issuance of temporary authorization tokens to mobile apps, and role-based SSO.

5.6.3.4. Resource Directory (multi-account management)

A cloud account is the smallest management granularity for Alibaba Cloud resources in terms of isolation, metering, and billing. To isolate resources or manage costs, enterprise users often need to use and manage multiple cloud accounts. To this end, Alibaba Cloud provides a hierarchical multi-account management service called Resource Directory for enterprise users.

Resource Directory allows the administrator to easily create a resource directory structure that reflects the business relationship based on the business or organizational environment, and distributes multiple accounts of the enterprise to corresponding positions in the directory structure, forming a multi-level relationship among resources. Enterprise users can rely on established organizational relationships to centrally manage resources and meet the management requirements of corporate resources in terms of finance, security, audit, and compliance.

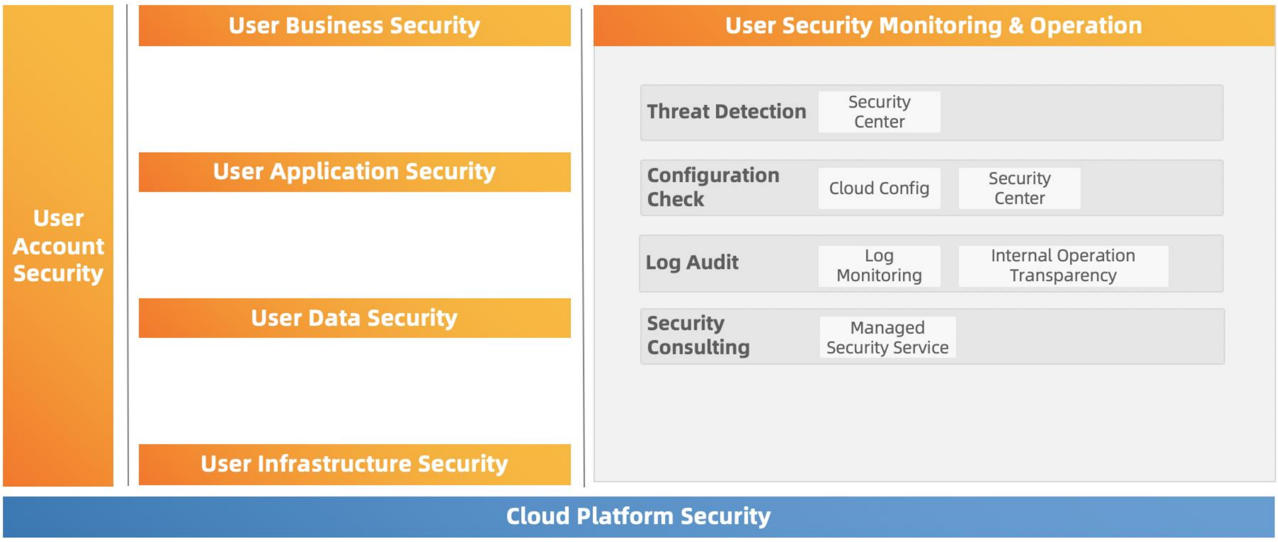
5.6.4. Audit

5.6.4.1. ActionTrail

User authentication credentials and authorization controls are designed to avoid security risks. On the other hand, operation logs can help Alibaba Cloud users better understand and diagnose a variety of security situations. Alibaba Cloud ActionTrail provides centralized log management for cloud resource operations. The logon and resource access operations performed under each account are recorded. An ActionTrail record includes information such as the operator, operation time, source IP address, resource object, operation name, and operation status. The operation records stored by ActionTrail can be used for security analysis, intrusion detection, resource change tracking, and compliance audit. In a compliance audit, users may need to provide detailed operation records for Alibaba Cloud accounts and RAM users. The operation events recorded by ActionTrail can meet these compliance audit requirements.

5.7. User security monitoring and operations

Alibaba Cloud Security Architecture



After a user's resources, applications, business, and accounts are properly protected on the cloud, the cloud platform needs to provide security monitoring and operations capabilities to detect security threats, monitor the configurations of cloud resources and logs, and provide security response and consulting services. In this way, the security monitoring and operations capabilities of Alibaba Cloud can effectively safeguard the user's business.

5.7.1. Threat detection and response

5.7.1.1. Security Center

Security Center is a unified security management system that identifies, analyzes, and produces alerts based on security threats in real time. With security capabilities such as anti-ransomware, anti-virus, tamper-proofing, and compliance assessment, users can automate security operations, response, and threat tracing to safeguard cloud and local servers and meet regulatory compliance requirements.

Security Center provides threat detection capabilities based on threat intelligence. Based on the huge amount of network infrastructure data and threat intelligence gathered by Alibaba Cloud, Security Center performs protocol feature analysis, detects abnormal network and server behaviors based on machine learning, detects malicious domain names by domain generation algorithms (DGAs), and produces indicator of compromise (IOC) for use in the detection model. Based on the threat intelligence data, the service also integrates a server abnormal behavior detection model to detect suspicious processes and malicious activities from various perspectives.

In addition to the host intrusion detection, virus detection, and vulnerability management capabilities mentioned in the User infrastructure security - VM security section, Security Center also provides such capabilities as cloud platform configuration check and server baseline check (see the User security monitoring and operations - Configuration check - Security Center section), threat detection, threat investigation and response, log analysis, and threat visualization.

5.7.2. Configuration check

5.7.2.1. Cloud Config

Cloud Config is an audit service for resources on the cloud. This service provides users with cross-region resource inventory and retrieval capabilities to record historical configuration snapshots of resources and form a configuration timeline. Cloud Config allows users to set compliance rules for the configuration of cloud resources. When a resource configuration change occurs, the compliance assessment is automatically triggered and an alert is issued for any "non-compliant" configuration. Cloud Config allows users to continuously monitor the compliance of large volumes of resources to address internal and external compliance requirements.

5.7.2.2. Security Center

Security Center allows users to perform baseline checks on their ECS instances. This service initiates tasks to scan VM instance security configurations in such aspects as account security, system configuration, database risks, and compliance requirements, and alerts users for items that do not meet the security and compliance standards. In addition, users can customize check policies by setting check items, check intervals, and target server groups.

Security Center also provides cloud platform secure configuration assessment based on security configuration best practices in five dimensions: identity authentication, network access control, data security, log audit, and basic security protection. With the deep integration of Security Center and the cloud platform, security risks from ECS instances to the cloud platform can be visualized with detailed information. This reduces risks caused by the cloud environment and cloud product misconfigurations.

5.7.3. Log audit

5.7.3.1. Log monitoring

In addition to the logging functions of ActionTrail and Bastion Host introduced in the User account security - Audit section, Alibaba Cloud Log Service can also collect and process logs of cloud products in the computing, storage, database, network, and security categories, such as ECS, OSS, and SLB. Log Service records operational information and operating status of cloud products. Log Service provides end-to-end capabilities across cloud products, including real-time log collection and consumption, delivery of logs to data warehouses and third party SIEM, and real-time log query and analysis, enabling users to monitor and audit different types of logs in real time.

5.7.3.2. Internal operation transparency

Traditionally, internal O&M operations done by the cloud platform are invisible to users. In other words, users are not aware of and cannot monitor or audit O&M actions performed by the cloud provider. Although Alibaba Cloud has obtained industry-leading third-party compliance certifications, efforts must also be made to give users the confidence that their data and resources are properly protected and managed within the cloud platform. To this end, Alibaba Cloud provides the ability to make relevant internal operations transparent to the users by providing internal operation logs in selected products (such as OSS). This allows users to monitor and audit internal cloud platform operations when using Alibaba Cloud products.

5.7.4. Security consulting

5.7.4.1. Managed Security Service

Managed Security Service is a security consulting and management service. Backed by the Alibaba Cloud Security service team, this service provides enterprise users with customized assessment and consulting services such as security protection strategy optimization, security protection for major events, and manual review and response. The service also provides real-time monitoring and detection, reinforcement strategy, vulnerability management, and incident response to fully protect the business environments of users. Therefore, enterprise users are protected even without a dedicated on-premises team of security engineers.

6. Cloud product security

This chapter describes featured products of Alibaba Cloud and their security functions. For more information about Alibaba Cloud products and services, please visit the official Alibaba Cloud website (www.alibabacloud.com).

6.1. Elastic computing

Alibaba Cloud provides a wide range of cloud-based elastic computing services based on Elastic Compute Service (ECS).

6.1.1. ECS

An ECS instance is a virtual computing environment that incorporates CPUs, disks, memory, operating system, network bandwidth, and other basic server components. An ECS instance is the operating entity offered by ECS, and is a virtual machine which users can log on to as an administrator to perform administrative operations, such as mounting a disk, creating a snapshot, creating an image, and establishing a computing environment.

6.1.1.1. Tenant isolation

ECS instances are assigned to different tenants. Isolation between ECS instances plays an important role in the security protection of each tenant. ECS instances are isolated based on hardware virtualization technology of the VMM (i.e. hypervisor). One ECS instance cannot access the system resources of another ECS instance unless authorized. This ensures isolation of computing resources between compute nodes. In addition, virtualization management layer provides storage isolation and network isolation.

In tenant isolation, it is critical to ensure isolation among virtual machines or between the virtual machine management system and virtual machines. Isolation between virtual machines (ECS instances) is guaranteed by CPU isolation, memory isolation, storage isolation, and network isolation. These isolation methods are described as follows:

- **CPU isolation**

  Based on the hardware virtualization technology Intel® VT-x, the hypervisor runs in VMX root mode and virtual machines run in VMX non-root mode. Different CPU privilege levels (i.e. ring levels) can effectively prevent unauthorized virtual machines from accessing system resources of the physical host and other virtual machines, thus ensuring isolation between virtual machines. The hypervisor controls resource interactions between the host and virtual machines by providing mutually isolated computing channels. This prevents a tenant from gaining read/write/execute access privileges of other tenants' or host’s resources, reduces risks associated with system resource sharing, and ensures computing isolation among tenants.

- **Memory isolation**

  The hypervisor isolates memory in hardware virtualization. During ECS instance execution, the hardware-assisted Extended Page Tables (EPT) technology is used to prevent a VM from accessing the memory space of other VMs. After an ECS instance is released, its memory is scrubbed by the hypervisor to prevent other ECS instances from accessing any residual data in the memory.

- **Storage isolation**

  In the virtualization design of cloud computing, Alibaba Cloud isolates computing from storage for virtual machines. This allows computing and storage to be scaled separately and makes it easier to provide services for multiple tenants. At the virtualization layer, the hypervisor substitutes a virtual device for its physical equivalent storage device. All the I/O operations of a VM are intercepted by the hypervisor to ensure that the VM can only access the physical disk space allocated to it, thus implementing security isolation of hard disk space between different VMs. After a virtual machine is released, its previously allocated disk space will be scrubbed to zeros to guarantee data security.

  Alibaba Cloud provides ECS disk encryption, which is an automatic encryption function designed for block storage devices in virtual machines. The ECS disk encryption function can encrypt data disk volumes, and can encrypt system disks via encrypted images to ensure the data security of tenants. With this function, tenants can symmetrically encrypt (AES256) their disks in a simple and secure manner to meet their specific business and certification needs. As a transparent encryption method, ECS disk encryption helps tenants eliminate the need to build, maintain, and protect their own key management infrastructure, change existing applications and O&M procedures, and perform any additional encryption and decryption operations. ECS disk encryption allows tenants to encrypt data by using KMS managed service keys and customer managed keys as the CMKs. A customer managed key refers to either a customer generated key through KMS or a customer supplied key (i.e. BYOK) uploaded to the KMS.

ECS disk encryption supports end-to-end encryption and encrypts data transmitted from ECS instances to cloud disks by default. The read and write operations of ECS instances are mapped to the corresponding physical files stored on the Alibaba Cloud data storage platform (i.e. cloud disks). Except for those who are authorized, no other tenants can access data from these files. The Alibaba Cloud data storage platform isolates data stored in the backend with high reliability and security assurance.

- **Network isolation**

  To establish network connections among ECS instances, Alibaba Cloud connects ECS instances to the Alibaba Cloud virtual network, which is a logical structure built on the Alibaba Cloud physical network structure. Virtual networks are isolated from each other to prevent traffic data snooping, interception, and other unauthorized access. In addition, all ECS instances can use the VPC and security group firewall function to segregate network access permissions.

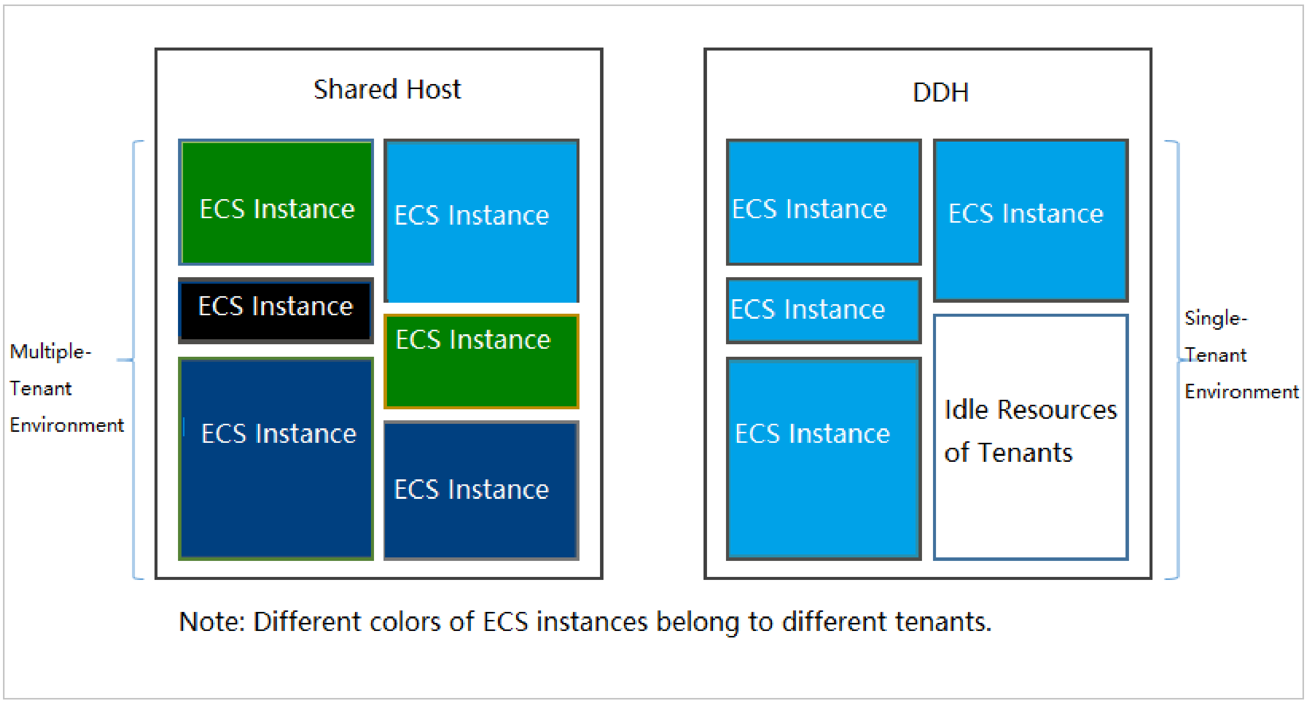
  During a packet transmission between two ECS instances, a packet from one ECS instance is sent to the VSwitch port corresponding to the virtual network interface controller (vNIC) of the destination ECS instance. Such packet is not visible to any other ECS instances. With network isolation provided by Alibaba Cloud, an ECS instance cannot receive or sniff traffic destined for other ECS instances even when the ECS instance runs in promiscuous mode. Although the vNIC can be set to the promiscuous mode, the hypervisor would not send any traffic destined for other destination addresses to the instance. Even if two ECS instances belong to the same tenant and run on the same physical server, they cannot sniff each other's traffic.

The preceding four isolation technologies provide a solution to tenant isolation when multiple tenants share physical resources. Furthermore, the physical resources of tenants can be isolated via dedicated physical resources, namely with dedicated hosts.

Dedicated hosts

Dedicated Host (DDH) is a cloud host service that allows a tenant to exclusively use the host’s underlying physical resources. As the only user on a host, the tenant does not need to share the physical resources of the host with other tenants. The tenant can obtain the physical attributes of the server, including the number of CPUs (number of sockets), number of physical CPU cores, and memory size. The tenant can also create ECS instances of an instance family that is compatible with the host specifications.

The following figure shows the difference between a dedicated host and a shared host.


Shared Host
DDH
ECS Instance
ECS Instance
ECS Instance
ECS Instance
ECS Instance
ECS Instance
ECS Instance
ECS Instance
ECS Instance
ECS Instance
Idle Resources of Tenants
Multiple-Tenant Environment
Single-Tenant Environment
Note: Different colors of ECS instances belong to different tenants.

6.1.1.2. Security group firewall

A security group is a virtual firewall provided by Alibaba Cloud for ECS instances. It provides Stateful Packet Inspection (SPI) and packet filtering functions.

A security group is a logical group that consists of mutually accessible ECS instances with the same security requirements in the same region. Security groups can be used to control access to one or more ECS instances and divide security domains for network isolation.

Each ECS instance must belong to at least one security group. Instances in the same security group can communicate through the network. By default, instances in different security groups cannot communicate with each other. Security group rules can be configured to authorize mutual access between basic security groups. However, mutual access between advanced security groups is not allowed.

Security groups can be divided into basic security groups and advanced security groups. Basic security groups apply to scenarios with fine-grained network control requirements, multiple ECS instance types, and moderate network connections. Advanced security groups apply to scenarios with high requirements for O&M efficiency, high ECS instance specifications, and a high number of computing nodes.

Feature	Basic security group	Advanced security group
Supports all instance types	Yes	No. Only ECS instances that support IPv6 are supported.
Supports VPC	Yes	Yes
Supports the classic network	Yes	No
Supports rule priority settings	Yes	No
Supports granting access permissions to other security groups	Yes	No
Supports manual setting of security group allow rules	Yes	Yes
Supports manual setting of security group deny rules	Yes	No. Advanced security groups deny all access requests by default.
Number of ENIs supported	The number of supported ENIs is limited by the number of ECS instances in the security group.	Up to 50,000 ENIs are supported.
Allows ENIs to be bound with ECS instance types	The network type of the ECS instance must be VPC.	ENIs can only be bound with instances that support IPv6.
Number of private IP addresses	2,000	No limit

ECS instances and associated ENIs must have the same security group type. ECS instances created before May 30, 2019 cannot be added to advanced security groups.

Security groups are stateful. States can be kept in the form of sessions. If outbound packets are allowed to flow out, the inbound response packets are also allowed to flow in. When a request is sent from an ECS instance, a security group allows bidirectional traffic in the same session by default (with a default session timeout).

6.1.1.3. SSH key pairs

Alibaba Cloud provides SSH key pairs for authentication of remote logon to Linux ECS instances. Compared with traditional logon using a username and password, logon using an SSH key pair is more secure and reliable, and is suitable for remote logon to a large number of Linux ECS instances.

SSH key pairs are generated by using a cryptographic algorithm. Each SSH key pair consists of a public key and a private key. If a user configures a public key for a Linux ECS instance, the user can use the corresponding private key to log on to this instance via SSH commands or other related tools from a local client or another Linux ECS instance without the need to enter the password.

6.1.1.4. Anti-IP/MAC/ARP spoofing

IP/MAC/ARP spoofing is a severe challenge for traditional networks. Through IP/MAC/ARP spoofing, attackers can disrupt the network environment and intercept confidential data.

Alibaba Cloud platform solves the IP/MAC/ARP spoofing problems by isolating any anomalous protocol requests initiated on the data link layer of the host and by avoiding IP spoofing on the network layer of the host.

6.1.1.5. High availability

High instance availability

The availability of a single instance is 99.975%. The availability of multiple ECS instances across regions is 99.995%.

Sever Load Balancer (SLB)

By using the SLB service, multiple ECS instances can be clustered to eliminate single points of failure and improve application availability. For more information, see 6.3.1. SLB.

High data reliability

By default, images and snapshots of ECS instances are stored in triplicate, distributed across physical servers to provide an availability of 99.9999999%.

Automatic failover and recovery

ECS instances are deployed on physical hosts (physical servers) that may fail due to performance anomaly or hardware failures. After detecting a fault on a host, the system will trigger a protective migration to migrate the ECS instances on the host to a normal host automatically to ensure the normal operation and high availability of instances and applications.

6.1.1.6. Snapshots and images

ECS allows users to create snapshots and custom images. A snapshot stores the state of data at a specific point in time, which can be used as back up data or to create an image. Users can create one or more automatic snapshot policies for a disk by specifying the creation time, frequency, and retention period.

Users can use a snapshot to create a custom image that contains the operating system and data of the snapshot. Then, users can use the custom image to create multiple ECS instances with the same environment, namely having the same operating system and data information. In two successive snapshots, the second snapshot only copies incremental data changes after the first snapshot is created. Snapshots apply to the following business scenarios:

- Users can use snapshots to back up important business data at regular intervals to avoid data loss caused by incorrect operations, attacks, or viruses.
- Users can create one or more snapshots before they perform critical and risky operations, such as replacing the operating system, updating applications, or migrating business data. By doing so, users can restore data if a fault occurs.
- Users can provide near-real-time data for applications such as data mining, report query, development, and testing by creating snapshots of production data.

Furthermore, users can create custom images and import them to Alibaba Cloud ECS.

6.1.1.7. Image security

Alibaba Cloud images are being updated to integrate patches for all known high-risk vulnerabilities to prevent the VMs from being exposed to high risk attacks. After detecting or discovering a new high-risk vulnerability, Alibaba Cloud will promptly update images and deliver them to customers. Alibaba Cloud will also protect image integrity against malicious tampering by using a data integrity verification algorithm.

6.1.1.8. Image encryption

If users need to encrypt data stored in images for security and compliance purposes, they can use the ECS image encryption function to protect data confidentiality and maintain control of data without the need to build or maintain their own key management infrastructure. Alibaba Cloud KMS supports customer generated keys as CMKs, and supports BYOK, by which users can upload key material to generate CMKs. To encrypt images, users can select CMKs generated by KMS, CMKs uploaded to KMS, or KMS managed service keys.

6.1.1.9. Hotfix patching

Alibaba Cloud's virtualization platform supports hotfix patching technology, which can fix system defects or vulnerabilities without user intervention, thus keeping any negative effects on user business operations to a minimum.

6.1.1.10.Support for RAM and STS

RAM is a resource access management service provided by Alibaba Cloud. ECS users can create RAM users and groups to manage access to cloud resources.

For example, to enhance the control of network security, users can assign an authorization policy to specific RAM user groups. Such a policy stipulates that, if the origin IP address is not from a specified corporate intranet, the access requests must be denied.

Different permissions can be granted to RAM user groups to manage ECS resources. Two example groups are described as follows:

- SysAdmins: This group requires permissions to create and manage ECS images, instances, snapshots, and security groups. A policy with full ECS permissions can be attached to the SysAdmins group.
- Developers: This group only requires permissions to use ECS instances. A policy that authorizes group members to call the *DescribeInstances*, *StartInstance*, *StopInstance*, *CreateInstance*, and *DeleteInstance* and other relevant APIs can be attached to the Developers group.

If a developer becomes a system administrator, the RAM user associated with the developer can be moved from the Developers group to the SysAdmins group.

ECS also supports STS and allows users to assume RAM roles to gain temporary resource access permissions across accounts. When a user assumes a role, the permissions associated with the role supersede the existing permissions of the user. This enables users to access resources across different accounts without sharing Access Keys.

6.1.1.11.Instance RAM role

ECS allows users to attach RAM roles to ECS instances to access cloud resources by using temporary tokens generated by Security Token Service (STS). An Instance RAM role allows the attached ECS instance to assume the role and gain specific access permissions. After successful role assumption, the ECS instance would receive a temporary Security Token Service (STS) credential, which can be used to access other cloud resources. This ensures the security of Access Keys (AKs) and allows users to apply fine-grained access control.

6.1.2. ECS Bare Metal Instance

An ECS Bare Metal Instance is an elastic and scalable computing service product, with the high-performance of a bare metal physical machine. It combines the benefits of virtual and physical machines to provide customers with secure, reliable, stable, and dedicated computing resources.

6.1.2.1. Dedicated computing resource

ECS Bare Metal Instances allow customers to use exclusive computing resources without virtualization overhead or feature loss. ECS Bare Metal Instances support 8, 32, 80, and 96 vCPUs with high CPU frequency. As an example, an ECS Bare Metal Instance with eight vCPUs can provide a core frequency of 3.7 GHz to 4.1 GHz. Compared with other computing products, ECS Bare Metal Instances provide better performance for gaming and finance workloads. In addition, ECS Bare Metal Instances are fully compatible with other Alibaba Cloud products. This helps customers build an integrated business system on Alibaba Cloud.

6.1.2.2. Encrypted computing

ECS Bare Metal Instances use a chip-level trusted execution environment (Intel ® SGX) to ensure that sensitive data is processed in a secure and trusted environment. Chip-level security provides a safe environment for sensitive data in the cloud and allows customers to create a trusted execution environment to protect encryption and decryption keys, account credentials, and other confidential information. Users can protect their data by writing code that supports the trusted execution environment. This ensures that their sensitive data can be accessed and manipulated only through the code that they write.

6.1.3. Auto Scaling

Auto Scaling is a service to automatically scale computing resources based on the volume of user requests and custom settings. It is suitable for applications with fluctuating workloads, as well as applications with stable traffic patterns.

Auto Scaling can monitor clusters and automatically replace unhealthy instances to reduce maintenance costs. It can also manage clusters, and automatically add or remove ECS instances as workloads fluctuate, thus reducing infrastructure costs. Auto Scaling is deeply integrated with SLB and RDS, and can automatically manage SLB instances and RDS whitelists to improve operational efficiency.

6.1.3.1. Authentication

Auto Scaling authenticates every request. Users need to include signature information in their requests. Auto Scaling uses Access Keys as the credentials for authentication. For more information about the AK authentication process, see 7.5.1.3. Authentication via AK.

6.1.3.2. Support for RAM and STS

Auto Scaling supports the RAM service. Users can grant access permissions to RAM users (i.e. subusers).

Auto Scaling also supports STS and allows users to assume RAM roles to gain temporary resource access permissions across accounts. When a user assumes a role, the permissions associated with the role supersede the existing permissions of the user. This enables users to access resources across different accounts without sharing Access Keys.

6.1.4. Resource Orchestration Service

Resource Orchestration Service (ROS) is an easy-to-use service for cloud resource management and automatic O&M. Users can create orchestration templates to define the needed resources, the dependencies between the resources, and the configuration details. ROS creates and configures resources for automatic deployment, operations, and maintenance based on the templates. The orchestration template also provides a standard method for resource and application delivery. and can be modified at any time. The ROS service can be used to make Infrastructure as Code (IaC) possible.

6.1.4.1. Support for RAM and STS

ROS supports the RAM service. Users can grant access permissions to RAM users (i.e. subusers).

ROS also supports STS and allows users to assume RAM roles to gain temporary resource access permissions across accounts. When a user assumes a role, the permissions associated with the role supersede the existing permissions of the user. This enables users to access resources across different accounts without sharing Access Keys.

6.1.5. Container Service for Kubernetes

Container Service for Kubernetes (ACK) is a high-performance and scalable containerized application management service that allows users to use Docker and Kubernetes to manage the lifecycle of containerized applications. It provides multiple methods for application deployment automation and continuous delivery, and supports microservice architectures.

6.1.5.1. Support for RAM and STS

Container Service for Kubernetes supports the RAM service. Users can authorize RAM users to read from or write to clusters. Besides, users can define RAM policies to allow or deny requests from certain IP addresses through whitelists or blacklists.

Container Service for Kubernetes also supports STS and allows users to assume RAM roles to gain temporary cluster access permissions across accounts. When a user assumes a role, the permissions associated with the role supersede the existing permissions of the user. This enables users to access clusters across different accounts without sharing Access Keys.

6.1.5.2. RBAC authorization for cluster resources

Alibaba Cloud account owners and authorized RAM users (i.e. admin users) can grant other RAM users RBAC permissions for access to cluster resources. After authorization, the RAM users can access certain resources in the cluster via the API server. Container Service for Kubernetes provides multiple built-in roles such as administrator, O&M engineer, developer, and restricted user to simplify the authorization process. It also supports custom roles and access control based on namespaces, and allows users to manage authorizations to cluster resources and users in batches.

6.1.5.3. Log auditing

Container Service for Kubernetes is integrated with Log Service and can automatically collect logs from API servers and Ingress accesses. It also provides visual interfaces to help users filter and retrieve logs.

6.1.5.4. Security hardening

Container Service for Kubernetes performs security hardening on cluster component configuration and runtime environment based on the CIS Kubernetes benchmark.

6.1.5.5. Runtime monitoring

Container Service supports Security Center based intrusion detection to monitor the applications running in clusters. It detects suspicious events and sends alerts to users in real time. Security Center can monitor process startup logs and network connection logs in containers, and detect and fix Web-CMS vulnerabilities, Webshell, malware and trojans, suspicious process behaviors, and abnormal network connections.

6.1.5.6. Sandboxed-container

Container Service for Kubernetes (ACK) provides a secure container version based on Alibaba Cloud ECS Bare Metal Instance. The entire framework is implemented based on Alibaba Cloud sandbox technology. Unlike the traditional shared kernel architecture of Docker containers, each secure container has an exclusive kernel that maintains independent memory, network, and I/O resources. Based on this framework, multi-tenant security isolation can be enforced more efficiently on a single host.

6.2. Storage

6.2.1. Block Storage

Block Storage is a storage service that provides low-latency, high-durability, high-reliability, and random-access block-level data storage for ECS instances. Block Storage automatically replicates data across different servers within a zone and prevents data unavailability due to unexpected hardware failures while ensuring business continuity. Block

Storage is similar to physical hard disks when in use (aka cloud disks). It allows users to perform operations such as creating and formatting disks when mounted on Elastic Compute Service (ECS) instances, and provides persistent data storage.

6.2.1.1. Data encryption

If users need to encrypt data stored in cloud disks for security and compliance purposes, they can use the cloud disk encryption function integrated with Alibaba Cloud KMS to protect data confidentiality and maintain control of data without the need to build or maintain their own key management infrastructure.

The cloud disk data encryption function uses KMS managed service keys as CMKs to encrypt user data by default. It also supports customer managed CMKs (i.e. BYOK or users generated CMKs) to encrypt user data. In the data encryption mechanism, a customer master key (CMK) and data encryption key (DEK) are specified for each disk. An envelope encryption method is used to encrypt data. For more information about envelope encryption, see 5.3.2.2. Encryption at rest.

The data encryption feature automatically encrypts data when data is transferred from ECS instances to disks, and decrypts data when the data is read from disks. Encryption and decryption operations are performed on the physical hosts where the ECS instances reside. During the encryption and decryption processes, cloud disks do not experience any noticeable performance reductions.

After an encrypted cloud disk is created and attached to an ECS instance, the following types of data are encrypted:

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

Data encryption is supported for all available cloud disk products (i.e. basic disks, ultra disks, standard SSD disks, and Enhanced SSD disks) and shared block storage products (i.e. ultra shared block storage and SSD shared block storage). All available ECS instance types support data encryption at rest in all regions.

6.2.1.2. High availability

Block storage uses a three-copy distributed mechanism and provides a data durability of 99.9999999%.

6.2.2. File Storage NAS

Apsara File Storage NAS (Network Attached Storage) provides file storage services for compute nodes, such as ECS instances, E-HPC clusters, and Docker containers. NAS is a distributed file system that provides shared-access, scalability, high availability, and high-performance. NAS is compatible with multiple standard protocols, such as NFS and SMB. With POXIS-based file APIs, NAS offers several benefits, including compatibility with operating systems, shared access, data consistency, and exclusive locks. By using NAS, users can enjoy unlimited capacity and performance scaling, single namespace, shared access, high durability, and high availability, all without the need to modify existing applications.

6.2.2.1. Access control

Apsara File Storage NAS supports standard directory/file permission operations on a file system, and supports read/write/execute permission settings for specific users/groups. NAS allows users to create mount targets within VPC or classic networks, and allows ECS instances within the same VPC or under the same account to access the file system. NAS also supports permission groups as a whitelist. Users can add rules to a permission group, allowing access to a file system from specific IP addresses or IP segments. Users can also assign different access permissions to different IP addresses or IP segments for fine-grained access control.

6.2.2.2. Support for RAM

Apsara File Storage NAS supports the RAM service. By enabling the RAM feature, users can grant console access permissions to RAM users (i.e. subusers).

6.2.2.3. High availability

The data that is stored in Apsara File Storage NAS within a specific zone is automatically replicated. This design prevents single point of failure (SPOF) risks and provide a data durability of 99.999999999%. Compared with user self-created NAS file systems, Apsara File Storage NAS can reduce maintenance costs and data loss risks.

6.2.2.4. Data encryption in transit via NFS

Apsara File Storage NAS can mount file systems by using an NFS client through the Transport Layer Security (TLS) protocol. users can use mount options that are recommended by Apsara File Storage NAS to mount file systems. The client also provides logs to allow easy troubleshooting of mount issues.

The NFS client defines a new network file type: *alinas*. This file type is fully compatible with the standard mount command. The client also supports automatic mounting on an operating system at system startup. Users can add related parameters to the /etc/fstab file to enable this feature. When the NFS client is used to mount the file system through TLS, the tool will start a stunnel process and a monitoring process named *aliyun-alinas-mount-watchdog*. Any read or write data between applications and NAS will be encrypted by the stunnel process using TLS and forwarded to the Apsara File Storage NAS servers on the cloud.

6.2.2.5. Data encryption at rest

If users need to encrypt data stored in Apsara File Storage NAS for security and compliance purposes, they can use the NAS encryption function integrated with Alibaba Cloud KMS to protect data confidentiality and maintain control of data without the need to build or maintain their own key management infrastructure.

The NAS data encryption function uses KMS managed service keys as CMKs to encrypt user data by default. In the data encryption mechanism, a customer master key (CMK) and data encryption key (DEK) are specified for each Volume. An envelope encryption method is used to encrypt data. For more information about envelope encryption, see 5.3.2.2. Encryption at rest.

6.2.3. Object Storage Service

Alibaba Cloud Object Storage Service is a secure and reliable storage service that helps users manage large amounts of data. OSS has the following benefits. Users can use RESTful APIs to access OSS anywhere on the Internet in a platform independent manner. Users can elastically scale the capacity and processing capabilities, and choose from a variety of storage types to optimize the storage costs.

6.2.3.1. Authentication

OSS authenticates each API request. Users need to include signature information in their requests (except for anonymous requests, see below). OSS uses Access Keys as the credentials for authentication. For more information about the AK authentication process, see 7.5.1.3. Authentication via AK.

6.2.3.2. Access control

Access to OSS resources by a user is sorted into owner access and third-party user access. The owner here refers to a bucket owner, also known as the developer. Third-party users are users other than the owner who access resources in a bucket. The method of access to OSS resources is divided into anonymous access and signature-based access. For OSS, an anonymous access request does not contain any authentication information. A signature-based access request is a request that contains signature information in the header or URL as described in the OSS API documentation.

For access to objects that are stored in buckets, OSS provides you with several access control methods. These methods include access control lists (ACLs), RAM policies, and bucket policies.

- ACLs: ACLs are resource-based authorization polices. You can specify access permissions for buckets and objects in ACLs. You can specify ACLs for a bucket or an object when you create the bucket or upload the object. You can also modify these ACLs at any time after you create the bucket or upload the object.
- RAM policies: RAM is a service that allows you to control access to resources. RAM policies are user-based authorization policies. With RAM polices, you can manage user identities and control their access to different resources. For example, you can grant a user read-only access to only one bucket.
- Bucket policies: Bucket policies are resource-based authorization policies. Compared with RAM policies, bucket policies can be configured directly in the OSS console. You can authorize users to access your bucket even when you do not have permissions for RAM operations. With bucket policies, you can grant permissions to RAM user accounts that are owned by other Alibaba Cloud accounts. You can control anonymous user access to resources from specified IP addresses or IP segments.

Access permissions for a bucket are sorted into the following types:

- public-read-write: All users (including anonymous users) can perform read, write, and delete operations on objects in the bucket. Use caution: expenses incurred for these operations are paid by the owner of the buckets.
- public-read: The bucket owner or authorized users can perform read/write and delete operations on objects in the bucket. The other users (including anonymous users) can perform read operations on objects in the bucket.
- private: The bucket owner or authorized users can perform read, write, and delete operations on the objects in the bucket. Unauthorized users cannot access objects in the bucket.

When a new bucket is created without any permission specified, OSS automatically sets the bucket permission to private.

Four Access permissions for an object are sorted into the following four types:

- public-read-write: All users can perform read/write operations on the object.
- public-read: The object owner can perform read/write operations on the object. Other users can perform read operations on the object.
- private: The object owner can perform read/write operations on the object. Other users cannot access the object.
- default: The object inherits the access permissions from the bucket where the object resides.

Use caution: If you do not specify an access permission for an object when uploading the object, OSS sets the access permission for the object to default. This means that the access permission for the object is the same as the bucket where the object resides if you do not specify the access permission. If you specify an access permission for an object, the specified access permission overrides the access permission of the bucket where the object resides. For example, you set the access permission for an object to public-read. The object is accessible by authenticated users and anonymous users regardless of the access permission for the bucket. If a RAM policy and bucket policy are applied for an object at the same time, the policies will be joined with a logical AND, and OSS will prioritize any DENY conditions ahead of ALLOW conditions.

6.2.3.3. Support for RAM and STS

OSS supports RAM. With RAM, users can grant access and management permissions for OSS resources under an Alibaba Cloud account to a RAM user.

OSS also supports Security Token Service (STS). With STS, users can provide RAM users with temporary authorization credentials that allow short-term access to resources.

6.2.3.4. High availability

With the “redundant storage across zones” mechanism, OSS replicates three copies of data to three different zones within the same region. The mechanism ensures data availability when one of the zones is unavailable. With this redundant storage mechanism, OSS achieves 99.9999999999% data durability (designed for) and 99.995% service availability (designed for).

The redundant storage mechanism provides OSS with the disaster recovery capability at the data center level, that is, OSS can provide services with strong consistency even if a data center is not available because of network disconnection, power outage, or other disaster events. During failover, services are switched without interruption or data loss, ensuring that the failover process is transparent to users. With this disaster recovery capability, OSS can meet the strict requirement that the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) must be zero for critical applications and services.

6.2.3.5. Tenant isolation

OSS helps you slice user data and tag each piece of data. These pieces of data are discretely stored on distributed file systems. OSS also stores user data and data indexes in separate locations. OSS performs identity authentication by using Access Key and symmetric cryptographic signature verification. OSS validates the signature of each request from a single user. After a user passes identity authentication, OSS then combines discrete pieces of data based on user tags. This mechanism isolates data storage among multiple tenants.

6.2.3.6. Access logging

OSS supports access logging. The owner of a bucket can enable access logging on the bucket in the OSS console. When access logging is enabled on the source bucket, an object that includes a list of OSS access log entries is automatically generated every one hour based on the specified naming rules. Each object is written to the specified target bucket. Users can use different methods to analyze these access logs. These methods include using Alibaba Cloud Data Lake Analytics and creating Spark compute clusters. Users can also convert log files to archives for long-term storage by configuring lifecycle management rules for the target bucket.

The real-time log retrieval function integrates OSS with Log Service. The function allows users to retrieve OSS access logs by using the OSS console. The function also helps users perform tasks such as auditing operations on OSS, collecting statistics for visits, backtracking abnormal events, and troubleshooting issues.

6.2.3.7. Hotlink protection

OSS is a service with the pay-as-you-go billing method. To prevent user data that is stored in OSS from being leeched, OSS supports hotlink protection to limit referrers in HTTP headers. A user can configure a referrer whitelist for a bucket or whether to allow empty referer requests by using the OSS console or API. For example, if a user adds http://www.alibabacloud.com/ to the referer whitelist of a bucket named oss-example, only requests with a value of http://www.alibabacloud.com/ in the referer field have access to objects in the oss-example bucket.

6.2.3.8. Cross-origin resource sharing

The same-origin policy is a restriction that is imposed by browsers for web security proposes. A browser will deny access to Website B when the access request originates from a JavaScript method on a page of Website A.

In actual practice, cross-origin access is a popular Web security feature. For example, OSS is adopted at the backend of a website named www.a.com. On the website, the upload function is implemented on a webpage by using JavaScript. However, requests on the webpage can only be sent to www.a.com, whereas all requests sent to other websites are rejected by the browser. As a result, user-uploaded data must be relayed to other sites through www.a.com. If JavaScript cross-origin resource sharing (CORS) is enabled, data can be directly uploaded to OSS, without the need to be transferred through www.a.com.

6.2.3.9. Server-side encryption

OSS supports server-side encryption for uploaded data. This means that when user data is uploaded, OSS encrypts the data and persistently stores the data. Then, when the data is downloaded by a user, OSS automatically decrypts the data, returns the original data to the user, and declares in the header of the returned HTTP request that the data has been encrypted on the server.

OSS provides the following server-side encryption methods:

- **Encryption by SSE-KMS**

  In order to use this method, a user can change the default server-side encryption method of a bucket to KMS without specifying a CMK ID. Alternatively, a user can include the x-oss-server-side-encryption header in the request and specify its value to KMS. In this method, OSS uses the KMS managed service key as the CMK, and has KMS generate different data encryption keys and perform envelop encryption for data objects. The objects are automatically decrypted when downloaded.

- **Encryption by SSE-KMS BYOK**

  Server-side encryption supports the Bring Your Own Key (BYOK) method to encrypt data. A user can change the default server-side encryption method of a bucket to KMS and specify a specific CMK ID. Alternatively, a user can include the x-oss-server-side-encryption header in the request and specify its value to KMS, and specify a CMK ID for the X-OSS-server-side-encryption-key-id parameter. In this method, OSS uses the specified CMK, and has KMS generate different data encryption keys and perform envelop encryption for data objects. The objects are automatically decrypted when downloaded. OSS also adds the CMK ID of an encrypted object to the metadata of the object. Therefore, these objects are automatically decrypted when downloaded by authorized users. Please note, this encryption method is applied when a user wants to specify a customer managed key as the CMK. Hence, a user can either specify a CMK that was uploaded to KMS or a CMK that was generated in KMS.

- **Encryption by SSE-OSS**

  This encryption method is an attribute of objects. In this method, OSS server-side encryption uses AES-256 to encrypt objects with different data keys. Master keys used to encrypt data keys are rotated regularly. A user can set the default server-side encryption method of the bucket to AES256. Alternatively, when sending a request to upload an object or modify the metadata of an object, a user can include the X-OSS-server-side-encryption field in the request and set its value to AES256.

6.2.3.10. Client-side encryption

Client-side encryption refers to encryption that is completed before user data is sent from a local client to a remote server. The plaintext of the data key that is used for encryption only resides on the local client. Other users cannot obtain the original data without the plaintext key, even if the data is leaked. This mechanism helps ensure data security.

- **Use KMS to manage master keys**

  When KMS is used to manage CMKs, users do not need to upload any data keys to the OSS client-side encryption SDK. Users only need to specify the CMK ID when uploading the data objects.

- **Manually manage keys**

  This method requires users to manually generate and manage data keys. During the client-side encryption process, users must upload a master key (symmetric or asymmetric key) to the client-side encryption SDK.

6.2.3.11. Compliance retention policy

OSS supports the Write Once Read Many (WORM) feature. This feature protects objects from being deleted or overwritten for a specified period of time. This feature can be used in cases that are subject to regulations of the U.S. Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority, Inc. (FINRA). OSS provides strong compliance policies. Users can configure time-based compliant retention policies for buckets. After a compliant retention policy is locked, users can read objects from or upload objects to buckets. However, no one can delete objects or revoke compliant retention policies within the retention period. Users can only delete objects after the specified retention period expires. The WORM feature is suitable for industries such as financing, insurance, health care, and security.

6.2.3.12. Versioning

OSS supports versioning. After versioning is enabled for a bucket, data that is overwritten or deleted is saved as a previous version. Versioning allows users to restore objects in a bucket to any previous point in time after you overwrite or delete the objects.

Versioning applies to all objects instead of specified objects in buckets. After a user enable versioning for a bucket, all objects in the bucket are subject to versioning. Each version has a unique version ID. After versioning is enabled for a bucket, the user can configure lifecycle rules to automatically delete expired object versions.

6.3. Networking

6.3.1. SLB

Server Load Balancer (SLB) is a load balancing service that distributes traffic among multiple ECS instances. It improves the service capabilities of applications. Users can use SLB to prevent single points of failure (SPOFs) and improve the availability of their applications.

6.3.1.1. High availability

SLB is designed with full redundancy to avoid SPOFs, and supports zone-disaster recovery. By integrating with Alibaba Cloud DNS, SLB can achieve geo-disaster recovery with an availability of up to 99.95%. SLB supports auto scaling based on application workloads and provides continuous services even when traffic fluctuates.

SLB is available in multiple zones in most regions to achieve zone-disaster recovery objectives. If the primary zone becomes unavailable, SLB can switch its service to a secondary zone in as little as 30 seconds and resume provisioning services. After the primary zone recovers, SLB would automatically switch back to the primary zone.

6.3.1.2. Health check

The SLB service inspects the health status of your Elastic Compute Service (ECS) instances. If an ECS instance is found in an abnormal state, the service will isolate the instance by not forwarding traffics to it until it recovers. In this way, SLB eliminates SPOFs and improves the service capabilities of applications.

6.3.1.3. Defend against DDoS attacks

Alibaba Cloud provides the layer-4 and layer-7 load balancing services. Layer 4 service uses an optimized and customized version of the open source software Linux Virtual Server (LVS) and Keepalived to achieve load balancing. Layer 7 service uses Tengine, a web server project based on Nginx, to achieve load balancing.

When combined with Alibaba Cloud Security, SLB can defend against distributed denial-of-service (DDoS) attacks in near real time. Additionally, the Layer 7 load balancing service provides the ability to defend against HTTP/S Flood attacks.

6.3.1.4. Access control

SLB can hide the IP addresses of the backend servers, and only expose virtual IP addresses instead.

SLB provides a source IP address whitelist feature, which allows only whitelisted source IP addresses to access services through SLB.

6.3.1.5. HTTPS

SLB supports HTTPS, SSL, and TLS load balancing:

- Provides centralized certificate and key management for services that require certificate authentication. This eliminates the need to deploy and manage the certificates on the backend ECS instances.
- Allows the decryption of ciphertext to be offloaded, thus reducing the CPU overhead on the backend ECS instances.

SLB provides a centralized certificate management system to store user certificates and keys. All private keys uploaded to the certificate management system are encrypted.

6.3.1.6. Logging

Operation logs are recorded in ActionTrail, and users can view the SLB operation logs by using the ActionTrail console. SLB also provides a log management feature that allows users to view any health check logs.

SLB integrates with Alibaba Cloud Log Service, and users can analyze the access logs of a SLB instance to understand the behavior and geographical distribution of client users and troubleshoot problems.

6.3.1.7. Support for RAM and STS

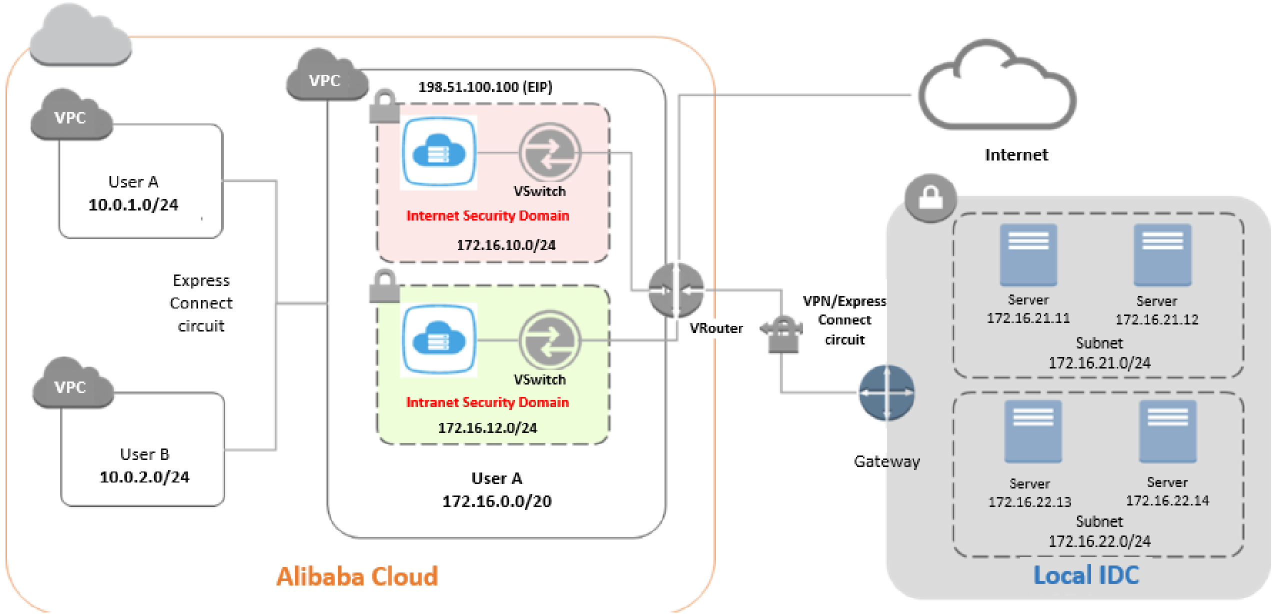
SLB supports RAM. With RAM, users can grant access and management permissions for SLB resources under an Alibaba Cloud account to a RAM user.

SLB also supports Security Token Service (STS). With STS, users can provide RAM users with temporary authorization credentials that allow short-term access to resources.

6.3.2. VPC

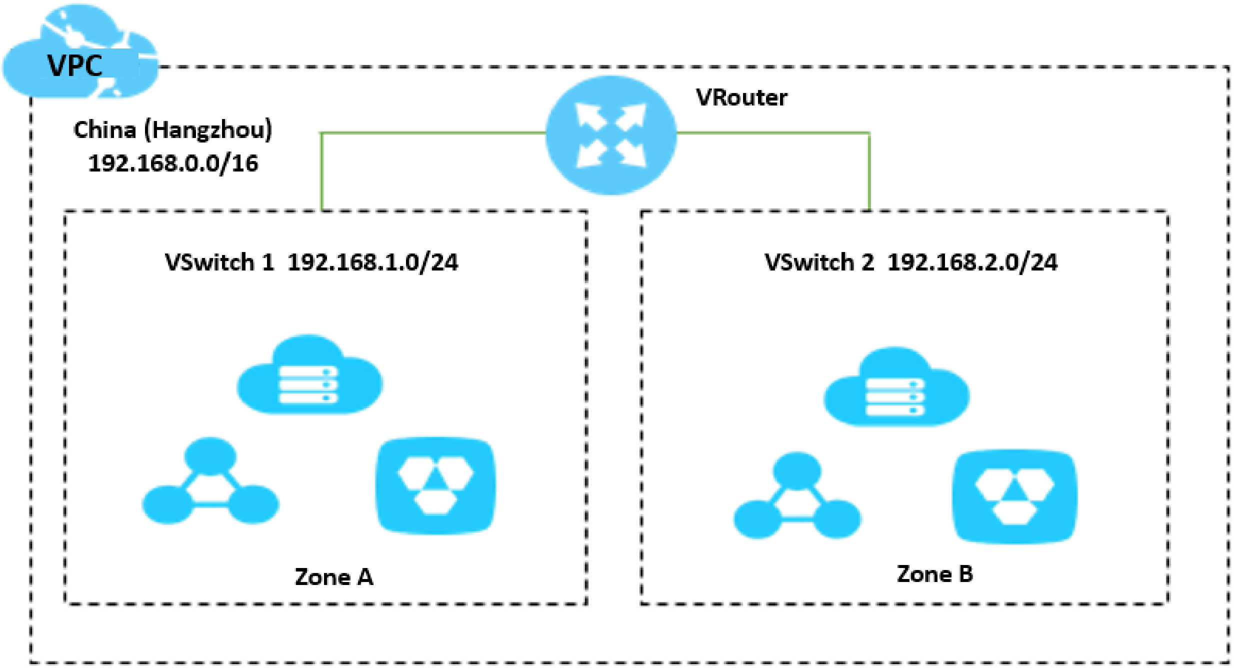
Virtual Private Cloud (VPC) is a recommended private network established by Alibaba Cloud. VPCs are logically isolated from each other in Alibaba Cloud. With Alibaba Cloud VPC, a user can build a virtual network that is logically isolated at layer 2 and define its IP address ranges, CIDR blocks, route tables, gateways, and other configurations. Furthermore, users can connect on-premises data centers to the VPCs through services such as VPN Gateway, Express Connect, and Smart Access Gateway. The Cloud Enterprise Network (CEN) can also be used to connect network resources across the globe to facilitate communications both between VPC groups and between VPC groups and off-cloud IDCs, and to form an on-demand network environment that enables smooth migration of applications to the cloud and expansion of data centers.

The following figure shows a typical architecture.



6.3.2.1. Custom networks

A VPC consists of a private IPv4 or IPv6 CIDR block, a VRouter, and one or more VSwitches. A VRouter is the hub of a VPC. It connects VSwitches in the VPC and serves as the gateway that connects the VPC to other networks. VSwitches are basic network devices of a VPC that are used to connect different resources in Alibaba Cloud. After a user creates a VPC, the user can create VSwitches to divide a VPC into one or more subnets.



Custom private CIDR blocks

VPC IPv4 address ranges fall within the private (non-publicly routable) IPv4 address ranges specified in RFC 1918, as shown in the following figure.

If the IPv6 feature is enabled, the VPC will be assigned an IPv6 CIDR block with a subnet mask of /56, and an IPv6 Gateway is automatically created. By default, only private network communication is supported.

CIDR blocks	Number of available private IP addresses (Private IP addresses reserved by the system are excluded.)
192.168.0.0/16	65,532
172.16.0.0/12	1,048,572
10.0.0.0/8	16,777,212

Custom routes

Route tables of a VPC consist of a system route table and a number of custom route tables. After you create a VPC, the system route table is automatically created to control the routes of the VPC. All VSwitches in the VPC use this route table by default. If you want to have more flexible control over your VPC, you can create custom route tables and attach them to

VSwitches to control the routes of subnets.

Both the system route table and custom route tables support custom route entries. You can access private or public networks by adding custom route entries to the following types of gateways.

- ECS instance: Traffic pointing to the destination CIDR block is forwarded to an ECS instance in the VPC.

  You can configure this type of route entry when you want to gain access to the Internet or other applications through an application running on the ECS instance.

- VPN gateway: Traffic pointing to the destination CIDR block is forwarded to a VPN Gateway.

  You can configure this type of route entry when you want to connect to the local IDC or other VPCs through a VPN gateway.

- NAT gateway: Traffic pointing to the destination CIDR block is forwarded to a NAT Gateway.

  You can configure this type of route entry when you want to gain access to the Internet through a NAT gateway.

- Router interface (To VPC): Traffic pointing to the destination CIDR block is forwarded to a VPC.

  You can configure this type of route entry when you want to connect two VPCs through an Express Connect circuit.

- Router interface (To VBR): Traffic pointing to the destination CIDR block is forwarded to a VBR.

  You can configure this type of route entry when you want to connect a VPC to an on-premises data center through Express Connect (physical connection access).

- Secondary ENI: Traffic pointing to the destination CIDR block is forwarded to a secondary ENI.

- IPv6 gateway: Traffic pointing to the destination CIDR block is forwarded to an IPv6 Gateway.

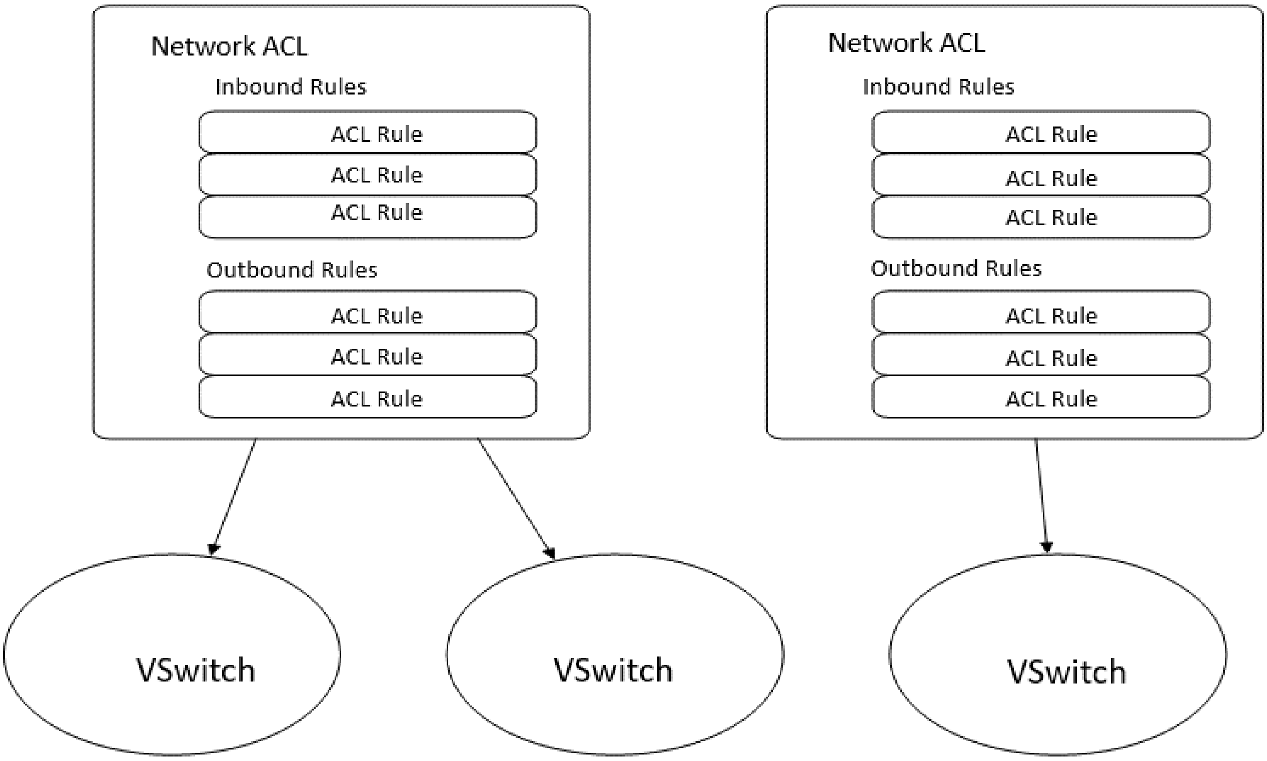
You can configure this type of route entry when you want to implement IPv6 communication through an IPv6 Gateway.

6.3.2.2. Access control

Alibaba Cloud provides two features for the security of your VPCs.

- Network ACLs

  A network access control list (ACL) controls inbound and outbound traffic of a VPC. You can associate a network ACL with VSwitches to control traffic. You can create a custom network ACL and add inbound and outbound rules to it. Network ACLs are stateless. For every rule that you configure to allow inbound traffic, you must configure a corresponding outbound rule that enables responses to inbound traffic. Otherwise, requests may not receive a response.



- ECS security groups

  A security group is a virtual firewall provided by Alibaba Cloud for ECS instances. It provides Stateful Packet Inspection (SPI) and packet filtering functions, and can be used to isolate security domains. By configuring security group rules, you can control public or private network access from ECS instances in a security group.

6.3.2.3. Logging and monitoring

The flow log feature of VPC allows users to capture the inbound and outbound traffic over the Elastic Network Interface (ENI) in their VPCs. It helps users check access control rules, monitor network traffic, and troubleshot network issues.

Users can use this feature to capture information about the inbound and outbound traffic of a specified ENI, VPC, or VSwitch. If you create a flow log for a VPC or a VSwitch, the inbound and outbound traffic of all the ENIs in the VPC or the ENIs connected with the VSwitch is captured.

The flow log data is stored in Log Service. Users can view and analyze the data in Log Service.

6.3.2.4. Tenant isolation

ECS instances of different tenants are launched in different VPCs, which are isolated from each other based on their Virtual Extensible LAN (VXLAN) tunnel IDs. Similar to traditional networks, VPCs can also be divided into subnets. ECS instances in the same subnet use the same VSwitch to communicate with each other, while the communication of ECS instances in different subnets requires VRouters.

It is recommended that users should use Cloud Enterprise Network (CEN) to enable communication across different VPCs. With CEN, users can interconnect VPCs that are in different regions and owned by different Alibaba Cloud accounts.

6.3.2.5. Network border control

Connect a VPC to the Internet

A VPC is a private network, and the ECS instances in VPC cannot access public networks by default. To connect to public networks, users can configure ECS public IP addresses, Elastic IP Addresses (EIPs), NAT gateways, or SLB instances for their ECS instances.

Product	Description	Benefit
ECS public IP address	When you create an ECS instance in a VPC, you can assign a public IPv4 address to your ECS instance. In this way, your ECS	An ECS instance with a static public IP address supports the Data Transfer Plan. If you replace the public IP address with

Product	Description	Benefit
	instance can access public networks.	an EIP, you can also use the Internet Shared Bandwidth feature.
Elastic IP (EIP)	You can attach an EIP to or detach an EIP from an ECS instance in a VPC based on your needs. An EIP allows source NAT (SNAT) for your instance to access the Internet and destination NAT (DNAT) for inbound traffic to access your instance, respectively.	You can attach an EIP to or detach an EIP from your ECS instance at any time. An EIP also supports Internet Shared Bandwidth and the Data Transfer Plan features to reduce the cost of accessing public networks.
NAT Gateway	NAT Gateways allow multiple VPC ECS instances to access the Internet (SNAT) and be accessed from the Internet (DNAT).	Different from an EIP that allows only one ECS instance in a VPC to communicate with public networks, a NAT gateway allows communication of multiple ECS instances in a VPC with public networks.
SLB	An SLB instance provides layer-4 and layer-7 load balancing services. You can access your ECS instances from a public network through an SLB instance.	In DNAT, SLB can forward an Internet request to multiple ECS instances. An SLB instance distributes traffic of multiple ECS instances to improve the service capabilities of your applications. You can use SLB instances to prevent single points of failure (SPOFs) and improve the availability of your applications. After you attach an EIP to an SLB instance, you can use the Internet Shared Bandwidth and the Data Transfer Plan features to reduce the cost of accessing public networks.

Connect two VPCs

You can interconnect your VPCs by using VPN gateways or Cloud Enterprise Network (CEN).

Product	Description	Benefit
VPN Gateway	You can create a VPN connection over IPsec to establish an encrypted communication channel between two VPCs.	• Security: Data encryption using the IKE and IPsec protocols ensures data security. • High availability: The hot-standby architecture of VPN Gateway ensures automatic failover within seconds. This ensures session and service continuity. • Low cost: The Internet-based encryption channel of VPN Gateway is more cost-effective than a connection over a leased line such as Express Connect. • Ease of use: VPN Gateway is ready for use after it is activated. All configurations immediately take effect. This allows you to quickly complete deployment.
CEN	CEN can interconnect VPCs that are in different regions and owned by different Alibaba Cloud accounts.	CEN allows global access for all of your Alibaba Cloud resources. • Low latency and fast transmission speed. • Nearest access based on proximity and shortest-path connection to Alibaba Cloud. • Redundancy and disaster recovery. • Systematic management.

Connect a VPC to an on-premises data center

You can connect your VPCs with an on-premises data center by using Express Connect, VPN Gateway, CEN, and Smart Access Gateway.

Product	Description	Benefit
Express Connect	You can connect a VPC to an on-premises data center through a physical connection.	• Low latency based on the backbone network. • Secure and reliable connections.
VPN Gateway	• You can create an IPsec-VPN connection between a VPC and an on-premises data center.	• High Security • High availability • Low cost

Product	Description	Benefit
	- You can create an SSL-VPN connection to connect local clients to your VPC.	- Easy to configure
CEN	- **Interconnection of a single VPC with local IDCs** You can interconnect your VPC with your local IDC by attaching a virtual border router (VBR) associated with the local IDC to a CEN instance. - **Interconnection of multiple VPCs with local IDCs** You can interconnect your networks by attaching multiple networks such as VPCs and VBRs to a CEN instance.	- A CEN instance allows you to connect all of your Alibaba Cloud resources with each other. - Low latency and high transmission speed. - Proximity access and shortest-path connection to Alibaba Cloud. - Redundancy and disaster recovery. - Systematic management.
Smart Access Gateway	- Smart Access Gateway allows you to build hybrid clouds by connecting your branch sites such as local IDCs, enterprise branches, or stores to Alibaba Cloud. - You can also interconnect your branch sites by using Smart Access Gateway.	- Smart Access Gateway is a highly automated and out-of-the-box service. It can quickly adapt to network topology changes. - You can connect to the VPC that is closest to your physical location. Active and standby SAG devices and links are used for failover to ensure that your on-premises business systems can establish reliable connections to the cloud. - The on-premises systems are connected to VPCs through encrypted connections. Data is encrypted for secure transmission over the Internet.

6.3.2.6. Support for RAM and STS

VPC supports RAM. With RAM, users can grant access and management permissions for VPC resources under an Alibaba Cloud account to a RAM user. VPC also supports Security Token Service (STS). With STS, users can provide RAM users with temporary authorization credentials that allow short-term access to resources.

For example, you can grant only permissions to manage route tables and their route entries in a specific region.

Assume that you create VPCs in multiple regions with your Alibaba Cloud account 11111111. You can grant permissions to manage VPCs only in a specific region, and the permissions only include deleting and adding route entries, creating subnet route entries and attaching them to VSwitches, and can only allow viewing of VPC instance information.

6.4. Databases

6.4.1. ApsaraDB for RDS

Alibaba Cloud ApsaraDB for Relational Database Service (RDS) offers stable, reliable, and scalable cloud database services. Based on the distributed file system and high-performance storage services of Alibaba Cloud, ApsaraDB for RDS supports multiple database engines, such as MySQL and SQL Server. In addition, ApsaraDB for RDS provides users with a set of database solutions, including disaster recovery, backup and restoration, monitoring, and migration.

To ensure data security, ApsaraDB for RDS provides multiple security protection features, including but not limited to:

- Network protection: IP address whitelists, Virtual Private Cloud (VPC) networks, SSL/TLS Protocol.
- Storage protection: Transparent Data Encryption (TDE), DB instance encryption at rest, and automatic backup.
- Disaster recovery: zone-disaster recovery and geo-disaster recovery.
- Audit: SQL Explorer, previously known as SQL audit function.

6.4.1.1. Tenant isolation

ApsaraDB for RDS uses virtualization techniques to isolate tenants. Tenants can only view and manage their own databases. Additionally, Alibaba Cloud implements security hardening on the servers where ApsaraDB for RDS instances are hosted. For example, tenants are not allowed to read from or write to operating system files by using their own

ApsaraDB for RDS instances. This ensures that tenants have no access to the data of other tenants.

6.4.1.2. High availability

A High-availability Edition instance provides a primary node and a secondary node. These nodes run in a hot standby configuration. The system switches workloads to the secondary node immediately after the primary node fails. This mechanism ensures a monthly service availability of 99.95%.

Users can create database backups at any time. To improve data traceability, ApsaraDB for RDS can restore a database to any earlier backup state by following a specified backup policy.

6.4.1.3. Access control

Database account

After you create an ApsaraDB for RDS instance, the instance does not provide any initial database accounts. You can create a standard database account and grant database-level read and write permissions in the ApsaraDB for RDS console or by calling the API. If you want to control more fine-grained permissions, such as permissions on tables, views, and fields, you can create a privileged Premier Account in the ApsaraDB for RDS console or by calling the API. Then, you can use a database client and the premier account to create standard accounts. You can also use the premier account to grant table-level read and write permissions to standard accounts.

IP address whitelist

By default, the IP address whitelist for an ApsaraDB for RDS instance is set to 127.0.0.1 to block connections from all IP addresses. You can go to the data security module in the ApsaraDB for RDS console or call the API to modify the IP address whitelist. You do not need to restart the ApsaraDB for RDS instance after you modify the IP address whitelist. Therefore, changes to the IP address whitelist do not interrupt your business. You can set multiple groups in the IP address whitelist. Each group can contain up to 1,000 IP addresses or IP address ranges. You can also enable the enhanced whitelist feature to specify the network type (classic or VPC network) when you create an IP whitelist group.

6.4.1.4. Network isolation

VPC

In addition to the IP address whitelist, ApsaraDB for RDS allows you to use Virtual Private Cloud (VPC) networks to enable advanced access control. A VPC network is a private network dedicated to your Alibaba Cloud account. The VPC isolates network packets by using underlying network protocols to achieve layer-2 access control. You can connect your servers in on-premises data centers to Alibaba Cloud over a virtual private network (VPN) or through a leased line. To avoid IP conflicts, you can configure CIDR blocks for ApsaraDB for RDS in the VPC console. In this way, you can connect to ApsaraDB for RDS from either on-premises servers or your Elastic Compute Service (ECS) instances.

The combination of VPCs and IP address whitelists is an ideal option for you to secure ApsaraDB for RDS instances.

Internet

By default, RDS instances deployed in a VPC network are only accessible from the ECS instances in the same VPC network. If necessary, you can also apply for a public IP address to allow access requests from the public network, such requests include but are not limited to:

- Connections from ECS Elastic IP Addresses (EIPs).
- Connections from public IP addresses of your on-premises IDCs.

IP address whitelists can be used for all connections to ApsaraDB for RDS instances. It is strongly recommended that you configure the IP address whitelist properly before requesting a public IP address.

6.4.1.5. Data encryption

SSL/TLS

ApsaraDB for RDS supports the SSL/TLS protocol for MySQL and SQL Server. ApsaraDB for RDS provides a server certificate when a user connects to the database service. With the certificate, the user can verify whether the database with the target IP address and port is provided by ApsaraDB for RDS. This helps to prevent man-in-the-middle (MITM) attacks. ApsaraDB for RDS also allows the user to enable and update server SSL certificates as needed.

TDE

ApsaraDB for RDS supports the Transparent Data Encryption (TDE) feature for MySQL and SQL Server. TDE in ApsaraDB RDS for MySQL is developed by Alibaba Cloud. TDE provided by ApsaraDB RDS for SQL Server is developed on the basis of the SQL Server Enterprise Edition. Key Management Service (KMS) provides and stores the keys used for TDE. With TDE enabled, ApsaraDB for RDS only needs to access the key once when an RDS instance is started or migrated. The following database services support TDE: ApsaraDB RDS for MySQL 5.6, 5.7 and 8.0, and ApsaraDB RDS for SQL Server 2008 R2. These products allow you to encrypt data by using service-managed keys as CMKs. ApsaraDB RDS for MySQL 5.6, 5.7 and 8.0 also allow you to use customer managed keys as CMKs to encrypt data. After you enable TDE for an ApsaraDB for RDS instance, you can specify the databases or tables that you want to encrypt. The data of the specified databases or tables is encrypted before you write the data to any device such as a hard disk, solid-state drive (SSD), or Peripheral Component Interconnect Express (PCIe) card, or to any services such as Object Storage Service (OSS). Therefore, data files and backups of the instance are encrypted.

DB instance encryption at rest

For ApsaraDB for RDS instances where cloud disks are attached, Alibaba Cloud provides encryption at rest for the RDS instance by using the block storage encryption capability.

Key Management Service (KMS) provides and stores the keys used for data encryption, and ApsaraDB for RDS only needs to access the key once when an RDS instance is started or migrated. The following database services support encryption at rest: ApsaraDB RDS for MySQL 5.7 and 8.0, ApsaraDB RDS for SQL Server 2012, 2014, 2016 and 2017, and ApsaraDB RDS for PostgreSQL 10 and 11. These services allow you to encrypt data by using service managed keys and customer managed keys as the CMKs for data encryption.

6.4.1.6. SQL Explorer

ApsaraDB for RDS supports the SQL Explorer feature. SQL Explorer uses SQL audit logs to record all database operations. SQL Explorer helps you efficiently manage databases, including failure analysis, behavior analysis, and security auditing. You can also use enhanced search function to retrieve data by database, user, client ID, thread ID, execution time, or number of scanned rows. The search results can be exported and downloaded. SQL Explorer supports SQL analysis, and allows you to analyze SQL log entries generated within the specified time frame in a visualized and interactive manner. Therefore, you can easily identify erroneous SQL statements and performance issues.

6.4.1.7. Backup and recovery

To ensure data integrity and reliability, ApsaraDB for RDS regularly backs up database data to guarantee data recoverability. ApsaraDB for RDS provides two types of backup functions, namely data backup and log backup.

6.4.1.8. Instance disaster recovery

Alibaba Cloud provides cloud computing services among multiple regions around the world. Each region covers multiple zones.

ApsaraDB for RDS supports multi-zone instances that are also known as zone-disaster recovery instances. These instances provide higher availability than single-zone instances. A multi-zone instance runs on physical servers deployed in different zones. When a failure occurs in a zone, the system immediately switches the workloads to another zone. The entire failover process is transparent to users, and requires no changes to application code.

ApsaraDB for RDS also supports cross-region data disaster recovery. For example, you can asynchronously replicate Instance A' in Region A to Instance B' in Region B by using the Data Transmission Service. Instance B' is a complete and independent ApsaraDB for RDS instance, and has different connection addresses, accounts, and permissions from Instance A'.

6.4.1.9. Software upgrade

ApsaraDB for RDS provides users with new versions of database software when applicable. In most cases, software upgrade is not mandatory. The database version of an ApsaraDB for RDS instance is upgraded only when restarted. In rare cases, for example, when critical bugs and security vulnerabilities occur, ApsaraDB for RDS enforces database upgrades during the maintenance period of the instance. Such mandatory upgrades only result in temporary database disconnections. These upgrades have no obvious adverse impact on the corresponding application if the database connection pool is correctly configured. Users can change the maintenance period in the ApsaraDB for RDS console or by calling the API to prevent mandatory upgrades at peak hours.

6.4.1.10. Support for RAM and STS

ApsaraDB for RDS supports RAM. With RAM, users can grant access and management permissions for RDS resources under an Alibaba Cloud account to a RAM user.

ApsaraDB for RDS also supports Security Token Service (STS). With STS, users can provide RAM users with temporary authorization credentials that allow short-term access to resources.

6.4.2. Table Store

Table Store is a NoSQL database service built on Alibaba Cloud's Apsara distributed system, enabling users to store and access large volumes of structured data in real time. Table Store organizes data into instances and tables that can seamlessly scale using data partitioning and load balancing. Applications use the Table Store service through the Table Store API/SDK or the Table Store console.

6.4.2.1. Authentication

Table Store authenticates each API request. Users need to include signature information in their requests. Table Store uses Access Keys as the credentials for authentication. For more information about the AK authentication process, see 7.5.1.3. Authentication via AK.

6.4.2.2. High availability

Table Store supports automatic failure detection and data migration. These features ensure the high availability of your applications in the case of server and network hardware failures. The service availability of Table Store can reach up to 99.9%.

Table Store creates multiple backups of data and distributes these backups among multiple servers on different racks, and enables quick recovery from a backup failure to provide high service reliability. This mechanism ensures data durability of 99.99999999%.

6.4.2.3. Strong consistency

Table Store ensures strong consistency for data writes. Applications can read the latest data immediately after the system indicates a successful write operation.

6.4.2.4. Data encryption

If users need to encrypt data stored in cloud disks for security and compliance purposes, they can use the Table Store encryption function integrated with Alibaba Cloud KMS to protect data confidentiality and maintain control of data without the need to build or maintain their own key management infrastructure.

Table Store data encryption function uses KMS managed service keys as CMKs to encrypt user data by default. It also supports customer managed CMKs (i.e. BYOK or user generated CMKs) to encrypt user data. In the data encryption mechanism, a customer master key (CMK) and data encryption key (DEK) are specified for each table. An envelope encryption method is used to encrypt data. For more information about envelope encryption, see 5.3.2.2. Encryption at rest.

6.4.2.5. Support for RAM and STS

Table Store supports RAM. With RAM, users can grant access and management permissions for Table Store resources under an Alibaba Cloud account to a RAM user.

Table Store also supports Security Token Service (STS). With STS, users can provide RAM users with temporary authorization credentials that allow short-term access to resources.

6.5. CDN

6.5.1. Overview

Alibaba Cloud Content Delivery Network (CDN) is a distributed network that is built on, and overlaying, the bearer network. CDN provides edge node clusters distributed across different regions. This architecture is a good substitute for the traditional data transmission mode that relies on centrally located web servers. CDN works with a precise scheduling system and caches content on edge nodes. If a client requests the contents, CDN redirects the request to the edge node nearest to the client, and the client can retrieve requested content from the edge node instead of the origin server. This mechanism enables efficient retrieval for a lower response time of required resources and also minimizes network congestion.

6.5.1.1. Authentication

CDN authenticates each API request. Users need to include signature information in their requests. CDN uses Access Keys as the credentials for authentication. For more information about the AK authentication process, see 7.5.1.3. Authentication via AK.

6.5.1.2. Tenant isolation

The content cached on CDN nodes is tagged with tenant information and separated among different tenants. The content is stored separately from data indexes. End users must pass authentication based on Access Keys when they request access to cached content. The requests are differentiated at the domain granularity. After the requests are authenticated, CDN redirects each request to the CDN node that is mapped to the requested domain. Then, the end users can only access content on the corresponding CDN nodes. This achieves the separation of content data storage among multiple tenants.

6.5.1.3. URL signing

The URL signing feature protects resources on an origin server from unauthorized download and access. With the hotlink protection feature, you can configure a referer blacklist or whitelist to prevent some hotlinking issues. However, hotlink protection cannot protect resources on the origin server in all scenarios because referer content can be forged. URL signing is a secure and effective measure to resolve this issue.

By working with the origin server, a CDN node implements URL signing to protect resources in a more reliable manner. The CDN node provides encrypted URLs that contain permission verification information. An end user can send a request to the CDN node by using the encrypted URL. The CDN node authenticates the permission information in the encrypted URL to determine whether the request is valid. If the request is valid, the CDN node returns a successful response. Otherwise, the CDN node rejects the request.

Alibaba Cloud CDN provides multiple authentication types. You can select an authentication type based on your business needs to protect the resources on your origin server.

6.5.1.4. HTTPS acceleration

As an extension of Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure

(HTTPS) is an HTTP channel designed to enhance security. Secure Sockets Layer (SSL) or Transport Layer Security (TLS) is used as a sublayer under the regular HTTP application to authenticate users and encrypt data.

Benefits:

- HTTPS encrypts sensitive information such as session IDs and cookies before transmission, and prevents security threats caused by sensitive information leakage.
- HTTPS checks data integrity during transmission to protect your DNS or content against man-in-the-middle (MITM) attacks such as hijacking and tampering.
- HTTPS is the new norm. An increasing number of major browsers such as Google Chrome and Mozilla Firefox have been identifying HTTP websites as insecure since 2018. If you insist on using HTTP, security vulnerabilities may occur. Furthermore, when end users visit your website using these browsers, they are prompted that the website is insecure. This may compromise user experience and reduce visits to your website.
- Google and Baidu prioritize HTTPS websites in search results. Additionally, major browsers must support HTTPS to support HTTP/2. HTTPS is a more reliable choice in terms of security, market presence, and user experience. Therefore, we recommend that you upgrade your communication protocol to HTTPS.

Alibaba Cloud CDN supports end-to-end secure acceleration over HTTPS. You can enable HTTPS secure acceleration and then upload the certificate and private key for a CDN domain. This feature also allows you to view, disable, enable, or modify certificates.

You can also configure HTTP Strict Transport Security (HSTS). This allows a client to only establish HTTPS connections to a CDN node. The CDN node returns the requested resources from the origin server to the client according to the configurations on the origin server. We recommend that you enable HTTPS on the origin server to support HTTP/2 and allow end-to-end HTTPS encryption. HTTP/2 is designed on the basis of HTTPS. HTTP/2 can be used to secure content and maintain network performance.

6.5.1.5. Hotlink protection

Alibaba Cloud CDN provides the hotlink protection feature.

Hotlink protection is implemented on the basis of the HTTP referer. The referer field is used to track and identify where requests come from. You can configure a referer blacklist or whitelist to identify and filter end users. This mechanism restricts access to CDN resources and improves CDN security.

Hotlink protection supports blacklist or whitelist configuration. When end users request resources, the requests are redirected to the CDN nodes nearest to the end users. Afterward, the CDN nodes identify the requests based on the specified blacklist or whitelist. A request with a referer in the whitelist is allowed. A request with a referer in the blacklist is rejected and HTTP status code 403 is returned.

6.5.1.6. HTTPDNS

For a traditional DNS service, an Internet service provider (ISP) provides a local DNS server to query domain name resolution results. During this process, the domain may be hijacked, domain name resolution errors may occur, and the resolution request may be forwarded across networks. These issues may slow down the connection to a target website, or even cause the connection to fail.

To solve these issues, CDN uses HTTPDNS to provide domain name resolution. HTTPDNS allows your request to bypass the local DNS server of the ISP and reach the HTTPDNS server of Alibaba Cloud CDN. Then, the HTTPDNS server works as a recursive DNS server and returns an up-to-date and accurate DNS resolution result. This mechanism helps to avoid domain hijacking.

The HTTPDNS server hosts DNS records that map CDN domains to IP addresses of L2 CDN nodes worldwide. When a client requests resources over the CDN network, the client sends a DNS resolution request to the HTTPDNS server. Then, the HTTPDNS server queries DNS records and returns the corresponding IP address to the client.

6.5.1.7. Support for RAM and STS

CDN supports RAM. With RAM, users can grant access and management permissions for CDN resources under an Alibaba Cloud account to a RAM user.

CDN also supports Security Token Service (STS). With STS, users can provide RAM users with temporary authorization credentials that allow short-term access to resources.

6.5.1.8. Content moderation

Content moderation is a value-added service of CDN. Based on Alibaba Cloud, content moderation detects illicit content in large volumes of data, and can cut human resource expenditure for content audits by 90%. With content moderation enabled, the system automatically detects illicit images delivered over the CDN network. The URLs of illicit images are recorded, so you can export or delete these images.

6.5.1.9. IP address blacklist or whitelist

You can specify an IP address blacklist or whitelist in the CDN console. Both the IP address blacklist and whitelist support IPv6 addresses and CIDR notation.

- IP address blacklist: Requests from IP addresses in the blacklist are rejected for retrieval of resources. If an IP address is added to the blacklist, a request from the IP address is still redirected to a CDN node. However, the CDN node rejects the request and returns HTTP status code 403. The requests from IP addresses in the blacklist are recorded in CDN logs.
- IP address whitelist: Only requests from IP addresses in the whitelist are allowed for retrieval of resources.

Please note the blacklist and whitelist functions are mutually exclusive, and only one of the two can be active at a given time.

6.5.1.10.User-Agent blacklist or whitelist

You can configure a User-Agent blacklist or whitelist to identify and filter visitors. This feature restricts requests for CDN resources and improves CDN security.

To enable access control based on the User-Agent field in a request, you must configure a User-Agent blacklist or whitelist to filter requests.

- User-Agent blacklist: The requests that include the User-Agent fields in the blacklist are rejected for retrieval of resources. If a User-Agent field is added to the blacklist, a request that includes the User-Agent field is still redirected to a CDN node. However, the CDN node rejects the request and returns HTTP status code 403. The requests that include the User-Agent fields in the blacklist are recorded in CDN logs.
- User-Agent whitelist: Only requests that include the User-Agent fields in the whitelist are allowed for retrieval of resources.

Please note the user-agent blacklist and whitelist functions are mutually exclusive, and only one of the two can be active at a given time.

6.6. Data and intelligence

6.6.1. MaxCompute

The Alibaba Cloud big data computing service, MaxCompute, is a fast, fully managed, petabyte-scale data warehousing solution. MaxCompute provides a complete data importing solution and a variety of classic distributed computing models to help customers tackle large-scale data computing problems while reducing business costs and maintaining data security.

6.6.1.1. Authentication

MaxCompute supports two types of accounts: Alibaba Cloud accounts and RAM user accounts. Note: MaxCompute only recognizes Alibaba Cloud accounts by default.

Resource Access Management (RAM) is an Alibaba Cloud service that helps customers manage user identities and access permissions of their cloud resources. MaxCompute is used together with RAM for the following two scenarios:

- When you use MaxCompute through DataWorks, you can use RAM for account management. After you activate the DataWorks service with your Alibaba account and create a project, you can create multiple RAM user accounts using your Alibaba account in RAM. You can then add the RAM user accounts as project members for collaborative development.
- When MaxCompute is used to process unstructured data, you must authorize the access permissions for the unstructured data through RAM. MaxCompute can directly process unstructured data, such as data from Object Storage Service (OSS) and Table Store. As a prerequisite, access permissions to access OSS or Table Store must be granted to MaxCompute in RAM.

MaxCompute authenticates each API request. Users need to include signature information in their requests. MaxCompute uses Access Keys as the credentials for authentication. For more information about the AK authentication process, see 7.5.1.3. Authentication via AK.

6.6.1.2. Access authorization

The multi-tenancy feature of MaxCompute is based on projects. A project is the basic unit for data management and computing, and the main measure for metering and billing. After a user creates a project, the user become the project owner. All objects that are created in the project, such as tables, instances, resources, and user-defined functions (UDFs), belong to the owner. Only the owner and users authorized by the owner can access objects in this project.

Before authorizing a user, the project owner must add the user to the project. Only users in a project can be authorized.

A role is a collection of access permissions. A role can be used to assign the same permissions to a group of users. Role-based authorization can simplify the authorization process and reduce authorization management overhead. To authorize users, you can choose to grant roles instead of granting permissions to users.

MaxCompute can grant different permissions to users or roles in the project. Users can have different access permissions for different objects, such as tables (please note views require separate authorization), functions, resources, and task instances. At the same time, MaxCompute supports column-level labeling, namely Label Security, for fine-grained access control.

Authorization mechanism

MaxCompute supports the authorization of users or roles through the access control list (ACL) authorization mechanism. ACL authorization is an object-based authorization. An access control list is regarded as a sub-resource of an object. ACL authorization can be performed only when the object exists. When the object is deleted, the access control list is automatically deleted. The ACL authorization supports the GRANT/REVOKE syntax similar to SQL92, and allows the users to grant or revoke the permissions to access an object in an existing project with a simple authorization statement.

The current MaxCompute permission model supports ACL access control at field (i.e. column) level. In other words, a field is also one of the objects supported by the ACL. Similar to a table, a field is an independent object that contains complete authorization information, such as the validity period. Example:

```
grant Alter on Table T1(c1,c2) to USER ALIYUN$bob@aliyun.com;
```

```
//Grant the permission to modify the two fields c1 and c2
revoke Alter on Table T1(c1,c2) from USER ALIYUN$bob@aliyun.com;
//Revoke the permissions to modify the two fields c1 and c2
```

Label Security is a mandatory access control (MAC) mechanism for the project. Label Security allows project owners to have controls that are more flexible in user access to sensitive data of different columns. Label Security provides data sensitivity classification at the column level. Owners can label columns in a table with sensitivity levels. A table can have columns with different sensitivity levels. The default sensitivity level of data is 0. The default access level of all users is also 0. After data and users are labeled with security levels, Label Security applies the following default security policies:

- No-ReadUp: Users are not allowed to read data that has a sensitivity level higher than their own, unless the users are given explicit authorization.
- Trusted-User: For trusted users, they are allowed to write data of all sensitivity levels. The default sensitivity level of newly written data is 0 (unclassified).

Separation of project ownership and administration operations

MaxCompute defines authorization permissions for administration-related operations. For example, users with the CreatePackage permission can create packages and users with the AddPackageResource permission can add resources to the package. Customers can use MaxCompute policies to authorize administrative operations. Specifically, MaxCompute define a new system role for managing administrative operations. This role has the same permissions in access control and project management as the project owner. This feature allows the separation of project ownership and administration operations. Subsequent MaxCompute versions will also allow customers to create custom administration roles for hierarchical management.

RAM user group

RAM provides the RAM User Group feature to manage a group of users. MaxCompute has also added support for RAM user groups. The authorization of a RAM user group is automatically applied to all members of the group. For example, after a RAM user group is authorized to access the project, all users of the group can access the project, without the need to authorize users individually.

6.6.1.3. Data protection

If a project contains sensitive data that cannot be shared with other projects, the owner can enable the ProjectProtection feature to disable any outbound data transfer.

MaxCompute allows users to set permissions for data download. In previous versions, if a user had the Select permission, the user could download data by using the MaxCompute Tunnel. In the current version, the Download permission is a separate permission, independent from the Select permission. Therefore, customers can use ACL to grant the Download permission specifically to achieve a more fine-grained control for data download.

6.6.1.4. Cross-project resource sharing

A package is a feature for data and resource sharing across projects. It is used to implement cross-project user authorization and resource sharing. For example, the owner of Project A can create a package that includes all objects required by Project B. Then, the owner of Project A can grant the owner of Project B the permissions to install the package. After the owner of Project B installs the package, the Project B owner can separately authorize the package or the resources in the package to the users under Project B.

6.6.1.5. Data isolation

MaxCompute can address security needs in multi-tenant scenarios. It uses the Alibaba Cloud account authentication system, which authenticates users based on Access Key using symmetric cryptographic signature operations. It also verifies the signature information in each HTTP request. MaxCompute stores user data separately and distributed in the Apsara Distributed File System to achieve data isolation between users. This allows MaxCompute to meet the requirements for multi-user collaboration, data exchange, data privacy, and data security, and implements complete resource isolation between tenants.

MaxCompute runs all computational tasks in isolated sandboxes. The sandboxes are structured in multiple layers, from the Kernel-based Virtual Machine (KVM) layer to the kernel layer. System sandboxes are combined with an authentication mechanism to ensure data security and prevent server failures caused by human errors and malicious operations.

6.6.1.6. Data encryption

Encryption in transit

MaxCompute provides RESTful APIs for transmission and uses HTTPS to ensure data transmission security.

Encryption at rest

If users need to encrypt data stored in MaxCompute for security and compliance purposes, they can use the MaxCompute encryption function integrated with Alibaba Cloud KMS to protect data confidentiality and maintain control of data without the need to build or maintain their own key management infrastructure.

MaxCompute data encryption function uses KMS managed service keys as CMKs to encrypt user data by default. MaxCompute manages encryption at the project level and supports table encryption. Only encryption of the entire table is supported. Each project corresponds to a customer master key (CMK) and multiple data encryption keys (DEKs). An envelope encryption method is used to encrypt data. For more information about envelope encryption, see 5.3.2.2. Encryption at rest.

6.6.1.7. Sensitive data protection

Data classification

By using Label Security, you can label table fields and classify them to enable flexible access control for sensitive data.

Data masking

MaxCompute can be integrated with various data masking applications and utilize the data masking algorithms provided by these applications. For example, Data Security Guard provides a data masking algorithm and MaxCompute can call this algorithm to generate the masked data.

6.6.1.8. Data backup and deletion

Backup

Alibaba Cloud uses a flat and linear design for storage. A storage address is divided into chunks. Each chunk is replicated into three copies. Each copy is stored on a different node in the cluster to ensure data reliability.

Deletion

After you delete data, the released storage is reclaimed by the Apsara Distributed File System. During this period, the storage space is not accessible by other users. Data erasure is performed before it is available for further usage. This mechanism provides a high level of protection for user data.

6.6.1.9. Log auditing

MaxCompute performs log auditing for different log data of different users, and provides log data storage for information such as static data, operation records, and security information.

- Information_Schema

  Adhering to the industry standards, MaxCompute allows users to access metadata and job history. Users can acquire the metadata at a low cost to meet the requirements for security management, job optimization, and cost analysis.

- Audit logs

  MaxCompute is integrated with Alibaba Cloud ActionTrail service to allow logging user operations and auditing the behaviors of users in real-time, as well as backtracking problems for analysis.

6.6.1.10.IP whitelist

MaxCompute supports multiple-level access control. For example, the multi-tenant authentication mechanism of the project ensures that only users who have the authorized AccessKey ID and AccessKey secret can pass authentication, and perform data operations according to the permissions granted by the owner. In addition to this authentication process, MaxCompute also supports an enhanced method for access control that is based on IP whitelisting. After configuration, only the IP addresses and IP segments specified in the configured rules can access the project. The IP rule check is performed on top of the Access Key authentication.

An IP whitelist can be applied to an entire VPC or specific IP addresses within a VPC.

6.6.2. AnalyticDB for MySQL

Developed by Alibaba Cloud, AnalyticDB for MySQL is a high-concurrency real-time online analytical processing (OLAP) service. AnalyticDB for MySQL enables users to query, explore, and analyze large amounts of data within milliseconds. AnalyticDB for MySQL allows rapid and customized computations of large amounts of data, allowing users to conduct flexible data exploration, discover the value of data, and integrate business processes to provide analytics services for end users.

AnalyticDB for MySQL is currently in version 3.0. The following security features are described based on version 3.0 unless otherwise specified.

6.6.2.1. Tenant isolation

AnalyticDB for MySQL allows users to connect to a database by using the MySQL protocol. APIs that are compatible with the MySQL protocol, such as JDBC and ODBC, are also supported. When a user connects to AnalyticDB for MySQL, the connection user name is the AnalyticDB for MySQL account name, and the connection password is the account password.

For AnalyticDB for MySQL version 2.0, based on the MySQL protocol, the AccessKey secret will be encrypted with a random salt during the transmission process to ensure the security of user credentials.

AnalyticDB for MySQL implements tenant isolation at the database level. The Alibaba Cloud account that creates the database is the owner of the database. The database owner must grant access permissions before other Alibaba Cloud accounts can access the database.

Databases run on separate instances and are isolated at the process level.

AnalyticDB for MySQL supports Virtual Private Cloud (VPC), and you can specify the VPC to which the cluster belongs when you create a cluster. VPC ensures secure isolation at the network layer to further protect user security.

6.6.2.2. Cluster whitelist

AnalyticDB for MySQL supports the cluster whitelist feature to further control access from external devices to the cluster. The default whitelist of the cluster only contains the default IP address of 127.0.0.1, which means that no device can access the cluster. Users can add IP addresses or IP segments to grant additional access. The cluster whitelist feature allows AnalyticDB for MySQL clusters to achieve a higher level of security control without affecting the operation of the cluster.

6.6.2.3. High availability

Based on high availability (HA) distributed storage, AnalyticDB for MySQL allows multiple data backups and dynamic resource management to provide highly available online service.

Alibaba Cloud Server Load Balancer (SLB) improves the availability and the fault tolerance capability of the access network from the Alibaba Cloud network endpoint to the AnalyticDB for MySQL product endpoint.

For internal designs, the multi-copy, active-active, primary/secondary instance deployment and dynamic patching capability ensure HA at the instance level.

6.6.2.4. Users and permissions

AnalyticDB for MySQL supports two types of database accounts: privileged accounts and standard accounts. A privileged account is equivalent to the root account in MySQL and can manage all standard accounts and databases.

AnalyticDB for MySQL supports a hierarchical model for permission management, similar to the ACL model of MySQL. AnalyticDB for MySQL supports four granularities of permission control: the GLOBAL cluster level, DB level, TABLE level, and COLUMN (field) level. Similar to MySQL, privileged accounts can use the GRANT/REVOKE statement for permission authorization and revocation. Each ACL permission entry includes an authorized user, authorization objects, and the permission allowed.

6.6.2.5. Support for RAM

AnalyticDB for MySQL supports using RAM user accounts to logon to AnalyticDB for MySQL, and using RAM to manage the permissions to connect to AnalyticDB for MySQL under different conditions.

Users can use their Alibaba Cloud account to create multiple RAM user accounts and authorize the RAM user accounts to connect to the service. When a RAM user connects the database using MySQL protocol, the user must use the database account and password created in the database instance as the connection user name and connection password. If a RAM user account is authorized to logon to the Alibaba Cloud console, the RAM user account can also logon to the AnalyticDB for MySQL console.

6.6.3. DataWorks

DataWorks is a one-stop big data intelligent cloud development platform that offers a complete solution for big data services such as data integration, development, monitoring, security, operations, quality, and administration. By using the DataWorks development platform, companies can focus on data exploration and value extraction.

6.6.3.1. Access Control

Logon control

An Alibaba Cloud account can be used to create multiple user accounts in the RAM console. You can use an Alibaba Cloud account to authorize permissions for the RAM user accounts so that RAM users can access DataWorks under the specified conditions. The conditions can be based on the IP address or IP segment of the incoming requests, whether the account has enabled multi-factor authentication (MFA), and whether the request is based on the HTTPS protocol, etc.

By specifying the IP addresses or IP segments that have access to DataWorks, you can further prevent unauthorized access and ensure data and business security. For example, when your Access Key is inadvertently lost or stolen, DataWorks can prevent access from unauthorized IP addresses (such as IP addresses that are not in your internal network) before you replace the lost Access Key.

Sandbox isolation

The workspace is the basic unit of DataWorks for user data isolation. All tasks in a workspace are run in a sandbox to ensure that data is not leaked. Furthermore, developers are prevented from accessing external resources. By default, DataWorks only allows the following types of access:

- Data development tasks can only access the specified compute engines.
- Data integration tasks can only access data sources that have been registered.

If developers need to access external resources outside the workspace in addition to the above two scenarios, the workspace administrator must add the resources to the sandbox whitelist in advance. To access resources in a VPC network, the resources need to in an exclusive resource group.

6.6.3.2. Separation of development and production permissions

DataWorks supports code and configuration management by workspace. Simple workspace and Standard workspace modes are available.

A standard workspace mode isolates the development environment and the production environment. Take the MaxCompute engine as an example. A standard workspace requires two MaxCompute projects: one for the development environment and the other for the production environment. Data in both environments are isolated from each other. Developers can only operate the data in the development environment. To apply changes to the production environment data, the O&M users need to “publish” the changes. A standard workspace allows users to strictly control table permissions. Developers are prohibited from operating tables in the production environment to ensure data security.

The development and production environments are integrated for a simple workspace mode. This type of workspace allows fast iterations where any code takes effect immediately after being submitted, without the need for a separate deployment. However, permissions of the development and production environments are not isolated.

6.6.3.3. Authorization

Role management

DataWorks provides seven roles for permission management, including the owner, administrator, developer, O&M engineer, deployment engineer, security administrator, and guest.

- The owner is the user who owns a workspace. The owner has all permissions within a workspace.
- An administrator is a user delegated by the owner. An administrator has all permissions within a workspace except for deleting the workspace.
- A developer is a user who operates the development environment. A developer has the permissions to the development nodes and workflows, and data operations in the development environment.
- An O&M engineer is a user who operates the production environment. An O&M engineer has the permissions to terminate, rerun, and deploy nodes in the production environment.

- A deployment engineer is a user who connects the development and production environments. A deployment engineer has the permissions to publish code from the development environment to the production environment.
- A security administrator is a data security manager. A security administrator has the permissions to manage the configurations in the Data Security Guard.
- A guest is a user with the minimum set of permissions. A guest can only view code and cannot perform any other operations.

Authorization

DataWorks allows users to manage data permissions on a workspace. users can authorize permissions by the table or field granularities, and perform permissions auditing.

Data download control

DataWorks provides users with full control over the download of configuration data to reduce the risk of data leakage and ensure data security.

6.6.3.4. Data encryption

All sensitive information of DataWorks, including the user code, workflow configurations, and data source configurations, are encrypted. Only authorized users can view, use, and modify the information. The data encryption function relies on the encryption capabilities of the MaxCompute storage encryption.

6.6.3.5. Sensitive data protection

DataWorks supports data identification, sensitive data discovery, data classification, data masking, access monitoring, risk discovery and alerting, and auditing.

- Data identification and discovery: automatically identifies sensitive data in a workspace based on preset rules.
- Data classification: allows users to define different levels of data sensitivity class and provide separate access control permissions for each level.
- Data masking: obfuscates sensitive data by masking, aliasing, and hashing.
- Access monitoring: monitors the access to and export of sensitive data.
- Risk discovery: monitors sensitive data access behavior in specific scenarios.

6.6.4. Realtime Compute

Alibaba Cloud Realtime Compute is a one-stop, high-performance platform that offers real-time big data processing platform built on Apache Flink. It is widely used in scenarios such as data stream processing and batch data processing.

6.6.4.1. Tenant isolation

Alibaba Cloud Realtime Compute supports two modes, shared mode and exclusive mode. In the shared mode, multiple tenants share the same physical resources for different clusters. In the exclusive mode, a separate computing cluster on the ECS instances is created for each user. The user can enjoy the exclusive physical resources of the computing cluster, such as the network, disk, CPU, and memory, independent of the resources used by other users. The user can run VPCs and exclusive computing resources in exclusive mode to ensure the isolation and security of the user data. The exclusive mode is isolated from other users at the network and computing resources level. It also supports lower levels of APIs such as using user-defined functions to meet the workload needs of the user.

6.6.4.2. Support for RAM

Realtime Compute is integrated with RAM. Users can customize the authorization through role-based management. If external services and resources are to be used, permissions can be granted to the AliyunStreamDefaultRole role of Realtime Compute.

In addition, if a user does not perform any job for a prolonged period of time, the system automatically initiate MFA authentication to improve account security.

6.6.4.3. Storage account protection

Realtime Compute allows users to register storage resources under the same Alibaba Cloud account. It does not require users to enter the Access Key in plain text to prevent AK leaking. Realtime Compute allows users to manage and reference input and output storage resources that have been registered with the Realtime Compute development platform. After a storage resource is registered, users can preview or sample the corresponding data, or obtain the DDL statements that are automatically generated for referencing the resource. This helps users manage their cloud-based storage resources in one-stop mode.

6.6.4.4. Data encryption

For data in transit, the data is encrypted by using upstream and downstream SDKs and shares the same level of security capabilities as the upstream and downstream services. For data at rest, Realtime Compute does not store user workload data, and the data is secured by the corresponding storage service provided by Alibaba Cloud.

6.6.4.5. Monitoring and auditing

For log auditing, Realtime Compute supports the download of logs. Users can configure the job parameters and customize the log type and output path.

For monitoring and alerting, Realtime Compute is integrated with CloudMonitor. CloudMonitor collects data on Alibaba Cloud resources or via user-defined metrics, detects service availability, and triggers rule-based alerts. Users can gain a complete view of resource usage and status of workloads, and can receive real-time alerts to ensure the stability of their applications.

6.7. Application services

6.7.1. ApsaraVideo Media Processing

ApsaraVideo Media Processing, formerly known as MTS, is a multimedia data processing service. It provides a flexible, highly scalable, and cost-effective service that converts multimedia data into formats that are compatible with various platforms. Based on deep learning on large datasets, ApsaraVideo Media Processing performs multi-modal analysis of text, audio, images, and other media formats, and provides capabilities such as intelligent auditing, content understanding, and intelligent editing.

6.7.1.1. Support for RAM and STS

ApsaraVideo Media Processing supports the RAM and Security Token Service (STS) services. Users can grant access permissions to RAM users. Users can also grant temporary access permissions through temporary authorization credentials provided by STS.

6.7.1.2. Authentication

API Gateway is integrated with ApsaraVideo Media Processing. ApsaraVideo Media Processing authenticates every request. Users need to include signature information in their requests. ApsaraVideo Media Processing uses Access Keys as the credentials for authentication. For more information about the AK authentication process, see 7.5.1.3. Authentication via AK.

ApsaraVideo Media Processing authenticates each request from applications to prevent unauthorized data access, thereby securing data access.

6.7.1.3. Monitoring and alerting

By integrating with the CloudMonitor service, ApsaraVideo Media Processing supports monitoring data including system properties and resource usage. Users can also specify custom alert settings to monitor service stability, analyze service usage, and detect and diagnose issues.

6.7.1.4. Video encryption

ApsaraVideo Media Processing supports video encryption. This feature allows users to encrypt and protect their videos from being compromised via avenues such as leakage and hotlinking. Available encryption methods include proprietary cryptography algorithms developed by Alibaba Cloud and HTTP-Live-Streaming (HLS) Encryption. Users can configure and manage these encryption settings by using the ApsaraVideo Media Processing console or API.

6.7.1.5. Intelligent auditing

ApsaraVideo Media Processing allows users to perform intelligent auditing of their video contents. It can also recognize audio, text, and image that involve adult-restricted materials, terrorist activity, and other inappropriate contents. This feature reduces the costs for manual auditing and lowers the risk of regulation breaches.

6.7.1.6. Video copyright protection

ApsaraVideo Media Processing uses digital rights management (DRM) and video fingerprint technologies to protect the copyright of video contents. Available DRM video encryption solutions include ChinaDRM and Widevine. More solutions based on widely used DRM protocols such as PlayReady and FairPlay are being developed to strengthen H5 content security. The video fingerprint feature helps users extract audio, images, and image sequence features from a video and generate a fingerprint for the video. Users can use this feature to detect any misuse and protect the authenticity of original content.

6.7.2. AlibabaMQ for Apache RocketMQ

Alibaba Cloud Message Queue for Apache RocketMQ is a powerful message-oriented middleware (MOM). It was first developed by Alibaba and was donated to the Apache Foundation. It is one of the key products of enterprise-level Internet architectures. Based on high availability cluster technology, AlibabaMQ for Apache RocketMQ allows users to send and subscribe to messages, query message tracing, schedule messages, etc. Users can also collect message production and consumption statistics, monitor and receive alerts for the consumption of messages, etc. AlibabaMQ for Apache RocketMQ provides asynchronous processing decoupling and load shifting for distributed application systems. It supports queuing of a large volume of messages, high throughput, reliable retries, and other features required by online applications. It is one of the core services that is used to support the Double 11 online shopping festival for Alibaba.

6.7.2.1. Support for RAM and STS

By default, AlibabaMQ for Apache RocketMQ only allows the creator of a message queue to access its data.

AlibabaMQ for Apache RocketMQ supports RAM. With RAM, users can grant access and management permissions for AlibabaMQ for Apache RocketMQ resources under an Alibaba Cloud account to a RAM user.

AlibabaMQ for Apache RocketMQ also supports Security Token Service (STS) and allows users to assume RAM roles to gain temporary resource access permissions across accounts. When a user assumes a role, the permissions associated with the role supersede the existing permissions of the user. This enables users to access resources across different accounts without sharing Access Keys.

6.7.2.2. Monitoring and alerting

Users can use the monitoring feature provided by AlibabaMQ for Apache RocketMQ to monitor message consumption status and receive real-time alerts about anomalies.

6.7.3. Alibaba Mail

Alibaba Mail provides an email mailbox service that can be customized with a user's enterprise domain name as a suffixes. This feature upholds the user's corporate and brand images, and simplifies the unified and secured management of business correspondence.

Alibaba Mail is built on the cloud computing technologies and platforms of Alibaba Cloud. With powerful server clusters deployed in multiple regions across the globe, Alibaba Mail ensures that users can send and receive emails from anywhere around the world. Featuring efficiency, security, and intelligence, Alibaba Mail integrates the features of DingTalk to offer efficient email services and support users' fast-paced expanding businesses. Currently, Alibaba Mail supports 5 million enterprises in both public and private sectors, making it one of the largest enterprise email service providers.

6.7.3.1. Authentication and permission management

Alibaba Mail allows you to set unified enterprise policies for password-based logons. For example, if an employee does not change the initial password, the system sends a notification as a reminder for the employee to change the password. This policy helps reduce security risks posed by a potentially low-strength of the initial password. Additionally, after multiple failed logon attempts, Alibaba Mail locks the account to prevent brute-force attacks. Alibaba Mail also supports two-factor authentication. The password and verification code are required if the user attempts to log on outside of the corporate network.

Alibaba Mail offers email clients for multiple operating systems, such as Windows, Mac OS, Android, and iOS to allow secure user logon. For web logons, the service supports two-factor authentication that requires the password and a verification code (such as a watermark verification code). Users can also scan the mobile APP QR code or DingTalk QR code for secure logons.

Alibaba Mail allows users to grant different levels of permissions to different administrators. For example, users can delegate the management of the mailboxes for a department to a specific administrator. User can also manage specific permissions separately to allow a finer granularity of permission control.

6.7.3.2. Email control

Alibaba Mail provides a comprehensive set of email control mechanisms. Admins can prevent emails from being sent to external recipients. Admins can also review and recall emails, restrict the number of emails that can be sent, and limit email sending frequency.

Alibaba Mail provides an anti-spam system that can support hundreds of millions of users. It automatically recognizes email spam by using the anti-attack and anomaly detection feature, the user behavior and email content inspection feature, and the identity recognition feature. Users can also design a whitelist or blacklist to filter inbound emails.

Additionally, analysis and detection are performed on specific phishing attacks and email viruses. These features are based on the phishing feature database and the antivirus engine that are maintained and updated by the Alibaba Cloud Security Team.

6.7.3.3. Transmission encryption

Alibaba Mail supports encryption in transit through SSL/TLS protocol.

6.7.3.4. Auditing and alerting

Your employees can view the status of their accounts and the emails sent and received. In addition, administrators can also view the mailbox usage of your employees on the domain administration page. You can also query the operations logs of an administrator on the domain administration page.

Alibaba Mail also supports export of email logs. To request the log export feature, submit a ticket to Alibaba Cloud Customer Services.

For suspicious logon activities, such as a logon with an unusual IP address, Alibaba Mail sends alerts to the affected users, so they can mitigate risks by modifying their password.

6.7.4. CloudMonitor

CloudMonitor is designed to monitor your Alibaba Cloud resources and applications.

CloudMonitor provides one-stop, out-of-the-box, and open monitoring solutions for Alibaba Cloud enterprise users. It allows users to monitor IT infrastructure, perform automated testing on network quality, and monitor business events, custom metrics, and logs. It is an efficient and cost-effective monitoring service. CloudMonitor offers users an application group feature that allows users to manage dozens of Alibaba Cloud services and tens of thousands of instances distributed across different regions. Additionally, it offers users an alert template feature that allows the users to monitor these services and instances. Users can create dashboards to devise their own strategy for monitoring their business. Users can use CloudMonitor to increase the availability of their system and reduce the O&M costs of their IT systems.

CloudMonitor collects monitoring metrics of users' Alibaba Cloud resources and custom metrics. Users can use it to detect the availability of their service and set alerts for specific metrics. In this way, users can have a real-time overview of their Alibaba Cloud resources and their usage, business operations and health status. When exceptions occur, alerts are sent to ensure the availability of applications.

6.7.4.1. Access control

CloudMonitor supports the RAM service. Users can grant RAM user permissions for the monitoring data and for the management of alert rules, alert contacts, and alert groups.

CloudMonitor also supports Security Token Service (STS). With STS, users can provide RAM users with temporary authorization credentials that allow short-term access to resources.

Please note, the read-only access to CloudMonitor provided by the RAM service allows a user to query monitoring data and alert data.

CloudMonitor allows users to grant permissions based on time limit, MFA, and IP address whitelists or blacklists.

7. Alibaba Cloud Security

Alibaba Cloud Security is built on Alibaba Group's security technologies and years of experience. By using the powerful data analysis capabilities of the Alibaba Cloud computing platform, it provides customers with security services that safeguard data, applications, businesses, accounts, and operations in addition to providing basic protection and security monitoring. This chapter covers only typical Alibaba Cloud Security products. For more information about other security products and services, visit the Alibaba Cloud official website at www.alibabacloud.com.

All products described in this chapter support Alibaba Cloud Resource Access Management (RAM).

7.1. Basic protection

7.1.1. Anti-DDoS

Anti-DDoS is provided for enterprises whose services on the Internet become unavailable due to distributed denial of service (DDoS) attacks.

7.1.1.1. Anti-DDoS Basic

By default, Anti-DDoS provides an anti-DDoS capacity of up to 5 Gbit/s for free. In addition, Alibaba Cloud has launched the Security Credibility plan. After becoming a member of Security Credibility, you can enjoy additional DDoS mitigation capacity on top of the default offering based on your security credibility score.

Alibaba Cloud provides a free Anti-DDoS service to a certain extent for all users. For more information about the threshold of the free Anti-DDoS service (the black-hole threshold), see the product specifications. The black-hole threshold varies with different regions. For startups and small-scale users who are rarely attacked, a feasible solution is to join the Security Credibility plan and maintain platform security and increase the security credibility score according to the suggestions provided by Security Credibility in order to receive higher Anti-DDoS capabilities free of charge.

7.1.1.2. DDoS protection package

The Anti-DDoS protection package is designed for large-scale enterprises on Alibaba

Cloud. It uses the native Alibaba Cloud network and transparent protection engine to mitigate DDoS attacks. The protection package can be used to protect various Alibaba Cloud products, such as Elastic Compute Service (ECS). Server Load Balancer (SLB), Web Application Firewall (WAF), and Elastic IP Address (EIP).

By default, the basic Anti-DDoS protection is provided free of charge. After a paid upgrade, the protection capability is directly improved for these Alibaba Cloud products without the need to change the IP address. In addition, there are no restrictions on numbers of layer-4 ports and layer-7 domain names supported, which simplifies deployment as you only need to bind the public IP addresses of these products in order to protect them.

Features

- **Default DDoS protection on Alibaba Cloud**

  Provides Anti-DDoS Basic, which has up to 5 Gbit/s Anti-DDoS capacity free of charge. This basic DDoS protection function is provided by default.

- **Easy purchase and deployment**

  Supports quick setup within one minute and directly enhances protection for Alibaba Cloud products without having to change IP addresses.

- **Alibaba Cloud's protection network for quick access**

  Leverages Alibaba Cloud's Border Gateway Protocol (BGP) bandwidth resources that cover multiple Internet service providers. With this feature, only one IP address is required for achieving quick access to the networks of these Internet service providers (ISPs).

- **Full protection without additional Pay-As-You-Go services**

  Employs the maximum DDoS protection capability of Alibaba Cloud in the current region to provide full protection against each DDoS attack.

- **Shared protection with full protection of enterprise assets**

  Supports sharing protection capabilities among public IP addresses belonging to the same enterprise, reducing configuration complexity.

- **Provides tiered protection capacities and defends against DDoS attacks at**

the Tbps level

You can use Anti-DDoS Pro or Anti-DDoS Premium to automatically direct traffic to the backup Anti-DDoS Pro instance when an attack with significant traffic volume occurs.

Scenarios

DDoS protection packages are suitable for customers whose services are deployed on Alibaba Cloud with a large business scale and demanding network quality requirements. Though the risk of DDoS attacks for such enterprises is low, once a service is interrupted or damaged due to DDoS attacks, tremendous business losses may occur. DDoS protection packages can improve the DDoS protection capability at the minimum cost to reduce the potential business risks caused by DDoS attacks.

Enterprises normally use DDoS protection packages in the following scenarios:

- Resources are deployed on Alibaba Cloud.
- A large number of public IP addresses need to be protected.
- The bandwidth or queries per second (QPS) is high.
- IPv6 traffic protection is required.

7.1.1.3. Anti-DDoS Pro and Anti-DDoS Premium

Anti-DDoS Pro and Anti-DDoS Premium are designed for enterprises who deploy their resources on or off Alibaba Cloud. By using the massive traffic scrubbing center resources of Alibaba Cloud, both products work together with the artificial intelligence (AI) protection engine and adopt full-traffic proxy to protect against high-volume traffic attacks and refined web application level resource exhaustion attacks such as HTTP flood attacks.

Features

Anti-DDoS Pro and Anti-DDoS Premium have the following features:

- **High-quality BGP Anti-DDoS network**

  Anti-DDoS Pro and Anti-DDoS Premium provide BGP bandwidth resources to help successfully mitigate massive DDoS attacks peaking at over 1 Tbps. This ensures both the network quality and large traffic protection. Both products can successfully mitigate DDoS attacks that peak at over 1 Tbps. The traffic scrubbing center supports BGP router redundancy and auto disaster recovery to ensure high availability.

- **Protection against all types of DDoS attacks**

  Anti-DDoS Pro and Anti-DDoS Premium provide protection against common traffic-based DDoS attacks, including malformed packet attacks and various flood attacks, such as SYN floods, ACK floods, ICMP floods, UDP floods, NTP floods, SSDP floods, DNS floods, and HTTP floods. Specifically, they support protection against common Challenge Collapsar (CC) attacks, such as HTTP GET floods and HTTP POST floods.

- **AI protection with zero concerns about complex attacks**

  Anti-DDoS Pro and Anti-DDoS Premium intelligently learn the service traffic baseline to accurately identify attack traffic and attack characteristics. Additionally, they can automatically defend against complex CC attacks such as TCP connection exhaustion and application-layer resource exhaustion attacks, and can automatically load precise matching protection rules. For example, you can specify HTTP header fields for interception, such as IP, URI, Cookie, Referer, User-Agent, X-Forwarded-for, Content-Type, Content-Length, Post-Body, HTTP-Method, Header, and Params. You can also set geo-blocking, blacklist and whitelist, or the smart combination of multi-dimensional protection policies to implement the high-precision blocking of complex attacks, with a false positive rate lower than one in ten thousand.

- **Rich security reports for monitoring network security risks in real time**

  DDoS protection security reports allow you to query and analyze multi-dimensional data in various time periods in real time, including normal business traffic and attack traffic, port connection data, attacked IP addresses, ports and domain names, attack source IP addresses, attack source regions and ISPs, website access response codes, the number of URI requests and response time, and cache hit rate, to help you learn about the health of your businesses and attack protection conditions.

Scenarios

Anti-DDoS Pro and Anti-DDoS Premium protect enterprise resources deployed on Alibaba Cloud or in local Internet data centers (IDCs). They are suitable for industries suffering from frequent DDoS attacks.

Enterprises normally use Anti-DDoS Pro and Anti-DDoS Premium in the following scenarios:

- Occurrence of a DDoS ransom attack by malicious attackers.
- DDoS attacks have overwhelmed your business systems and urgent protection is required to restore them to a working state.
- DDoS attacks occur frequently, requiring continuous DDoS protection to ensure service stability.

7.1.1.4. GameShield

GameShield is a network security solution presented by Alibaba Cloud for protecting the gaming industry against DDoS attacks. Compared with Anti-DDoS Pro, GameShield can defend against high-traffic DDoS attacks at Tbps level and TCP resource exhaustion attacks (Layer-4 CC attacks) that are especially applicable to the gaming industry. This solution reduces protection costs and provides better protection.

GameShield consists of two modules:

- Distributed Anti-DDoS nodes: Through these nodes, GameShield can defend against DDoS attacks.
- Game Security Gateway: Through the decoding of proprietary protocols, GameShield can defend against connection floods that are unique to the game industry.

Features

- **Protection against massive DDoS attacks**

  Unlike the Anti-DDoS Pro data center, GameShield does not combat the attack by using massive bandwidth but uses distributed Anti-DDoS nodes, effectively splitting and scattering hacker attacks to different focal points. In addition, based on SDK data and traffic data, attackers can be accurately located and isolated by dynamic scheduling policies to actively limit risk to the origin and defend against attacks.

- **Protection against CC attacks**

  In general, CC attacks in the gaming industry are different from those targeting websites. Site-targeted CC attacks are mainly based on the HTTP or HTTPS protocols. These protocols are standardized, so it is relatively easy to perform data analysis and protocol analysis on them. However, most of the protocols in the gaming industry are proprietary or uncommon. Therefore, to defend against game-targeted CC attacks, Alibaba Cloud launched a professional cloud-based defensive gateway, that is, Game Security Gateway (formerly known as NetGuard, or NG for short).

- Game Security Gateway establishes a game service firewall between the user's services and the attacker. It can accurately identify real players and hackers according to the attacker's TCP connection behavior, post-connection dynamic information, and full-flow data.
- Game Security Gateway supports big data analysis. It analyzes normal player behaviors based on the characteristics of real user services and directly intercepts abnormal clients (with invalid protocols). It can also accurately block traffic from provinces in China and overseas countries at any time through million-item-level blacklists and whitelists.
- Game Security Gateway can establish an encrypted communication tunnel with the SDK, fully supervising the network communications between the client and the server. It only allows the traffic authenticated by the SDK and the Cloud Gaming Security gateway, thus solving TCP-layer CC attacks such as protocol-stimulated attacks.

7.1.2. Security Center

Security Center is a unified security management system that recognizes, analyzes, and triggers alerts based on security threats in real time. With security capabilities such as ransomware protection, anti-virus protection, web tampering protection, and compliance assessment, users can automate security operations, responses, and threat tracing to safeguard cloud and local servers and meet regulatory compliance requirements.

7.1.2.1. Features

Proactive security model

- Anti-virus: As part of the in-depth threat detection architecture of Security Center, Alibaba Cloud's self-developed AliHIPS, a real-time interception component, is used to intercept mainstream ransomware, mining, DDoS trojans, and other viruses in real time. Security Center monitors and analyzes files and processes in the cloud in real time at the system kernel level, effectively bypassing the anti-detection and anti-removal capabilities of trojans and malicious programs. Based on program behavior analysis results, the anti-virus module detects unidentifiable malicious threats in blacklists and proactively intercepts them. On the other hand, the virus database in the cloud is updated in real time and integrates various advanced technologies such as mainstream anti-virus engines in and outside China, Alibaba Cloud Sandbox, and the machine learning engine. This prevents the losses caused by timely updates of the virus database.

- Webpage defacement prevention: It is a value-added service provided by Security Center. This service monitors website directories in real time and backs up and restores tampered files or directories. It prevents drive-by downloads, hidden links, and the uploading of undesirable content.
- Application whitelisting: By intelligently learning the application whitelist, the system can identify trustworthy and suspicious or malicious programs to build an application whitelist, preventing the running of unauthorized programs. This prevents your servers from being compromised by untrusted or malicious programs that consume server resources.

Threat prevention

- Cloud platform configuration check: It provides users with security configuration best practices along five dimensions: identity authentication, network access control, data security, log auditing, and basic security protection. With the deep integration of Security Center and cloud computing platforms, you can oversee security risks from ECS instances to the platform. This reduces risks caused by cloud environment and cloud product configuration errors.
- Vulnerability detection and repair: Based on the self-developed cross-platform vulnerability scanning and repair engine, this service helps you scan and maintain multiple systems and applications at the same time. Currently, it supports Windows systems, third-party Linux versions for Alibaba Cloud, and mainstream CMS systems. In addition, it can detect emergency vulnerabilities in systems or applications without relevant patches.

- Baseline check: This module allows you to deliver a task for scanning host security configurations, including account security, system configuration, database risks, and compliance requirements, alerting you for items that do not meet the standards. In addition, you can customize a check policy by setting the check items, check cycle, and target server group.

Threat detection

Security Center adopts machine learning, deep learning, UEBA, threat intelligence, AV engine, and other security capabilities to build an in-depth three-dimensional threat detection architecture, so that threats can be detected and attacks can be tracked. Its main functions include intrusion detection, the detection of suspicious cloud service calls, Access Key leakage monitoring, and attack analysis.

Investigation response

- The asset fingerprint feature periodically collects and records server running processes, system accounts, open ports, software versions, and website background information. It helps you fully understand the running status of your assets and provides the backtracking and analysis capabilities.
- Automatic attack tracing helps you automatically identify the source and cause of the attack, provides security suggestions, and quickly develops stop-loss actions to reduce the loss to your business.

Log analysis

This module provides the host and log analysis feature to help you manage logs on your cloud computing systems. You can easily identify the causes of problems that occur on your servers.

Dashboards

Based on big data visualization technology, Security Center analyzes threats based on the collected network, application, and host information and displays the results visually on dashboards. It also displays the network security situation of your assets from the perspective of assets, businesses, and threats. As a critical supporting module for security decision making on the cloud platform, this module supports custom scenarios. It can be flexibly used for real-time security monitoring and work reporting, including the real-time monitoring dashboard for global business operations, the business security situation and scoring, the host security situation dashboard, the overview of site visitors, the network-layer security situation, and the security defense system dashboard.

7.1.2.2. Technical capabilities

In-depth and three-dimensional threat detection model

- Security Center monitors and analyzes files and processes in the cloud in real time at the server system kernel level through the Security Center agent, effectively bypassing the anti-detection and anti-removal capabilities of trojans and malicious programs. It can also analyze program behaviors, and detect unidentifiable malicious threats in blacklists to actively intercepts them. The virus database in the cloud is updated in real time and integrates advanced technologies such as mainstream anti-virus engines in and outside China, Alibaba Cloud Sandbox, and the machine learning engine. Timely updates to the virus database from these multiple sources help further reduce the risk of losses caused by malicious software.
- With the machine learning and deep learning technologies, over 200 security threat detection models are already available for detecting potential security threats.
- With the UEBA capability, it can detect threats based on user behaviors and identify internal and external security threats. For example, it can detect threats for cloud products. For instance, detecting Access Key usage is a typical scenario. In addition, Security Center has officially cooperated with GitHub. If an Access Key is leaked accidentally on GitHub, an alert is generated.
- At the network layer, threat detection is performed on traffic to detect hackers' actions on the network. The attack analysis function is used to display attacks in real time to prevent potential hacker intrusions.
- In addition to threat intelligence provided by Alibaba Cloud, Internet threat intelligence provided by third-party partners is introduced to provide you with security services.

In-depth defense system

Security Center consists of multilevel security protection modules, including network security, server security, application security, and threat analysis. It provides an in-depth defense system on the cloud network perimeter, in the cloud network, and on ECS instances. By using a management center that can integrate the security information from all modules, this service can accurately detect and block attacks. Security Center can effectively protect your business systems in the cloud against intrusions.

Security solutions completely integrated with the cloud platform

Security Center brought together the rich experience of the Alibaba Cloud Security team to develop an attack protection product specific to cloud computing platforms. This product can effectively protect the security of users' cloud network environments and business systems on public clouds and hybrid clouds. With all software components virtualized, Security Center is compatible with a broad range of hardware and can be quickly deployed, scaled up, and brought online. In this way, this product is a perfect fit for the elastic nature of cloud computing. The protection modules situated on cloud borders and in cloud networks use a bypass architecture designed for cloud businesses to minimize the impact on cloud platform services. The virtualized protection modules deployed on ECS instances perfectly suit the flexibility of these virtual machines.

Leveraging Alibaba Cloud's security capabilities

Security Center is built on years of accumulated protection policies and rich attack data sources. Each day, millions of users on Alibaba Cloud encounter hundreds of thousands of attacks. The Alibaba Cloud Security team makes full use of the accumulated security attack and defense data, analyzing more than 10 TB of security data in the public cloud every day. Basic security capabilities such as the malicious IP library, malicious behavior library, malicious sample library, and security vulnerability library are developed and applied to the protection modules of Security Center in a timely manner to enhance protection capabilities and ensure better security.

7.1.2.3. Scenarios

Security Center identifies malicious attacks at the network layer through the traffic security monitoring module, and blocks these attacks in real time. At the VM layer, Security Center detects and removes Webshell and malicious files to prevent attackers from exploiting the web server. Security Center also blocks brute-force attacks and sends alerts upon abnormal logon attempts. This prevents attackers from stealing or destroying your business data by taking advantage of weak passwords to log on.

7.1.3. Cloud Firewall

Cloud Firewall is the industry's first firewall as a service (FWaaS) solution for public cloud environments. This product manages the access control policy for north-south traffic from the Internet to ECS instances and the micro-isolation policy for east-west traffic between ECS instances in a centralized manner. Cloud Firewall comprehensively checks the exposure of your assets to the Internet in the cloud environment, and manages the access policies for public network IP addresses in a centralized manner. With one-click access, Cloud Firewall is the primary network security infrastructure for ensuring the network security of your systems on Alibaba Cloud. With a built-in intrusion prevention system (IPS), this product provides intelligent prevention, detects victim hosts, blocks external connections launched by hosts, and visualizes network-wide traffic and access relationships among ECS instances.

7.1.3.1. Features

Traffic analysis

- Internet access: Cloud Firewall uses traffic visualization technology to analyze open public network IP addresses, open ports, open applications, and risks, and it also provides relevant solutions.
- External connections: Cloud Firewall identifies your assets with external connections and the connected domain names. It also determines whether the domain names are at risk.
- Security group-based traffic visualization: Cloud Firewall displays traffic access relationships between security groups without the need for any configuration. It also uses a red line to highlight access events that occurred in the last three days. Traffic monitoring helps the administrator to identify suspicious internal hosts. For example, a malicious ECS instance scans other ECS instances, or an ECS instance is set as a malicious proxy server to the Internet.

Network-wide isolation control

- Centralized control over public network IP addresses: This feature comprehensively checks the exposure of assets to the Internet in the cloud environment, manages access policies for public network IP addresses in a centralized manner, and provides one-click access to Cloud Firewall.

- Domain name-based resource access control: External connections can be very dangerous to servers. Therefore, we recommend that you only permit your internal server to access authorized domain names and IP addresses. Other unauthorized domain names and IP addresses are prohibited by default.
- VPC-based isolation: The isolation is implemented based on the risk level of business applications. Business applications at different risk levels are allocated to different VPCs, for which Cloud Firewall controls resource access.

Intelligent intrusion prevention

Cloud Firewall integrates real-time IPS and threat intelligence. Therefore, it can intelligently block intrusions without the need to install software patches for your system. It also supports intrusion detection and analysis, lists intrusions detected by IPS, and supports IPS blocking analysis. Additionally, you can quickly query all the traffic blocked by IPS.

Logging

Cloud Firewall supports the storage of network traffic and security event logs. By default, security event logs, network traffic logs, and firewall operation logs are stored for six months.

7.1.3.2. Technical capabilities

Cloud-specific security protection

The security protection boundary in the cloud environment is more blurred than that in traditional Internet data centers (IDCs). In the cloud environment, security protection is required between the Internet and VPCs, between VPCs or SaaS-based cloud products, and even between virtual machines. Cloud Firewall provides the industry's first FWaaS solution in the cloud environment by using virtualization techniques and the service function chain based on the Software Defined Network (SDN). With traffic visualization, threat intelligence, and micro-isolation, Cloud Firewall manages all traffic in a centralized manner, controls traffic between VPCs, and provides micro-isolation between ECS instances. In this way, it provides you with a complete defense-in-depth system.

Transparent deployment methods

Traditional firewalls are usually deployed on the public cloud through a software image. For this method, you have to undergo a complicated configuration process that includes image installation, routing configuration, and high-availability system deployment. This does not satisfy the demand for quick deployment and elastic performance. In contrast, Cloud Firewall is completely transparent. You can start using it with just one click. It relieves you of worries about installation, disaster recovery, resizing, and access, allowing you to focus more on your core business.

7.1.3.3. Scenarios

User services generally fall into services connected to the Internet, services not connected to the Internet, testing services, and access to a data center over a leased line. The services that are connected to the Internet and the services that are not connected to the Internet are deployed in different VPCs to meet the need for secure isolation.

- Through Cloud Firewall, VPCs with Internet access are managed in a centralized manner, and Internet access is managed with fine-grained controls.
- Cloud Firewall enables strict resource access control between VPCs with and without Internet access.
- Traffic visualization and timely detection of abnormal traffic are available for different security groups within a VPC through Cloud Firewall.
- The security of core off-premises assets is protected by the combination of Cloud Firewall, dedicated leased line, and VPN.
- Cloud Firewall can also be used for isolation control over cross-region access.

7.2. Data security

7.2.1. Sensitive Data Discovery and Protection

Alibaba Cloud Sensitive Data Discovery and Protection (SDDP) can discover, classify, and protect user data on the cloud. SDDP enables data permission monitoring, data masking, global flow monitoring, and anomaly detection based on precise data discovery and classification. This service can discover, detect, and analyze the usage of sensitive data from large amounts of data. It can also promptly detect data leakage and warn of risks. Therefore, it helps users prevent data leakage and meet compliance requirements, such as PII protection and General Data Protection Regulation (GDPR).

7.2.1.1. Features

Sensitive data discovery and classification

With user authorization, this feature automatically scans and discovers different sensitivity levels of data, such as newly added data from new instances, databases, tables and columns, OSS buckets and objects. This feature precisely identifies sensitive data in the cloud environment by using keywords, rules, and machine learning-based models and algorithms. It also supports using custom sensitive data detection policies . Based on sensitive data identification results and your business attributes, this feature allows content-based discovery and classification of data sensitivity levels. The data sensitivity levels can later be used as part of your business system applications.

Sensitive data access control

This feature helps control permissions to access various data storage and data transmission products in the cloud environment. It supports the real-time query of "data, users, and permissions" and maps permissions between Roles and Accounts. This feature supports the centralized query of global data permissions. It also alerts you to permissions assignments and abnormal permissions usage that do not meet security best practices in the cloud environment.

Data exchange and access monitoring

This feature effectively monitors exceptions in data exchange and access processes, enables the dynamic display of the data flow, and ensures compliant and orderly data export and transmission. SDDP can effectively identify manual operations and API calls by monitoring access logs. In addition, SDDP alerts you to exceptions that occur during the exchange and use of various data, based on machine learning and big data analysis.

Data masking

This feature provides nearly 30 built-in masking algorithms in six categories including hash, encryption, masking, replacement, shuffling, and transformation, and supports user-defined masking algorithms or parameters to meet various business scenarios.

Exception handling

This feature enables the efficient disposal of and emergency response to exceptions, collects exceptions in a centralized manner, and supports the tenant isolation of exception events. It also uses time series analysis to reconstruct the behavioral baseline of the responsible entities. This feature dynamically displays historical baseline traces and effectively improves emergency response. It automatically feeds back any results to the machine learning model library to improve future detection accuracy. The feature also supports log analysis for various products and the centralized handling of events from the permission management and control system, as well as events from the data exchange and monitoring system.

7.2.1.2. Technical capabilities

Identify sensitive data by using AI

SDDP uses AI techniques that Alibaba Group has polished for years, such as cluster analysis and machine learning. Based on natural language processing and artificial neutral network models, this service precisely identifies sensitive personal data, critical system configuration files, and confidential documents from large amounts of documents, pictures, and data. SDDP also provides the capability of new data learning based on your existing identified data, and automatically improves sensitive data identification accuracy.

Ensure data usability after data masking

SDDP provides data masking capabilities for various business scenarios, and ensures that data is masked without changing the original data distribution and the corresponding business system logic, and ensures the validity and availability of the data. The desensitized data can be used in testing, development, analysis, and third-party usage scenarios. Compared with using the original data and simulated production data, users can use the masked data securely while accomplishing business needs at a low cost with high efficiency.

Improve anomaly detection accuracy through multi-layer filtering

SDDP provides a multi-layer filtering mechanism that analyzes the baseline results of behavioral learning on data objects, and the baseline results of historical behaviors of accounts. This mechanism also analyzes the returned samples of event handling, and anomaly detection models from multiple dimensions. With these features, SDDP can accurately identify and effectively reduce false positives to ensure that detection results can improve your operational capabilities.

7.2.1.3. Scenarios

The SDDP cluster is deployed in the monitoring area of the Apsara Infrastructure Management Framework. This non-intrusive, flexible, and distributed deployment method enables authorization and management of data services, such as MaxCompute, ApsaraDB for RDS (RDS), OSS, and Table Store. Through effective data isolation, SDDP ensures that security auditors or administrators from different departments can check the data of their own departments. Therefore, SDDP ensures that the data security control process itself is secure and controllable.

7.2.2. Key Management Service

Alibaba Cloud Key Management Service (KMS) is a secure and easy-to-use cryptographic service that provides key management functions, such as key hosting and cryptographic operations. KMS also provides built-in security best practices such as key rotation, and integrates with many other cloud products, allowing users to encrypt and protect sensitive data.

By using KMS, users can obtain a highly available and reliable key management service without the need to build or maintain their own key management infrastructure, which can be costly and time consuming. With KMS, users can focus on their business scenario usage cases, such as data encryption, data decryption, and digital signature verification.

7.2.2.1. Authentication and access control

When users access KMS to manage and use keys, authentication and authorization are required. The authentication and authorization authority of KMS is the RAM service of Alibaba Cloud. The RAM service determines whether the initiator of a request is a legitimate user and has the permission to access specific resources. According to the result, KMS accepts or denies this request.

- **User authentication**

  A user uses an Access Key based on a hash-based message authentication code (HMAC_SHA1) algorithm to seek authentication from KMS. This ensures the authenticity and integrity of a request. KMS denies a request that fails to pass the HMAC-based authentication. For more information about the AK authentication process, see 7.5.1.3. Authentication via AK.

- **KMS service authentication**

  KMS provides services based on the HTTPS protocol, and therefore the client can verify the service identity of KMS by checking server certificates. Authentication for the service prevents attackers from masquerading as KMS.

- **Access control**

  If a request passes authentication, KMS considers the initiator to be a legitimate user and then checks the current user's permissions and the attributes of this request by using RAM. The administrator of the current user's organization needs to grant permissions to access specific resources in KMS to the current user in advance using the RAM service. This is necessary for this user to pass the permissions check. Failing to pass the permissions check leads to a denial of the request.

7.2.2.2. Transmission security

Your request to access KMS and the communication between internal systems of KMS may include sensitive data. Secure channels and their end-to-end authentication ensure transmission security.

- **KMS endpoints**

  All user requests for KMS must use HTTPS. KMS only allows the use of industry standard high security cipher suites in TLS.

- **Internal communication security**

  KMS includes different service modules, each of which has an identity certificate. The TLSv1.2 protocol that features two-way TLS authentication based on the identity certificate is used in all inter-module communications to protect secure communications between internal nodes.

7.2.2.3. Key security

Key security is one of the core values of KMS. KMS ensures key security by containing keys within certain security boundaries and forbidding cross-boundary key distribution, and provides a cryptographic function through a specific interface for cryptographic operations.

KMS provides two key security specifications of different protection levels through Software Cryptographic Modules (SCMs) and Hardware Security Modules (HSMs),

Confidentiality

KMS guarantees the confidentiality of the keys managed by KMS.

- Users can manage their keys in HSMs, which use a hardware mechanism to prevent the plaintext of keys from ever leaving the security boundaries of the HSM. When users use the HSM-managed keys for cryptographic operations, the operations occur only in HSM to ensure the confidentiality of keys. Based on the management capabilities built into KMS and key protection via the HSM, KMS meets the needs for high security with low management overhead.
- KMS also supports software-protected key hosting by using SCMs to protect your keys. By reinforcing SCMs, KMS prevents the plaintext of software-protected keys from crossing the security boundaries of the SCM. That is, a key can be loaded in memory only within the security boundary of an SCM. SCMs can meet basic security needs, for example, in handling service managed keys. If you do not want to manage keys yourself at all, Alibaba Cloud provides you with built-in basic key protection and data encryption capabilities.

Randomness

Randomness is crucial to key strengths.

- When using an HSM, the creation of HSM-protected keys is based on secure and certified random number generation algorithms that use high entropy values as seeds, with a much higher strength than keys generated by pseudo-random number generation algorithms in software. HSM-protected keys cannot cross the security boundaries of the HSMs, hence users do not need to worry that the keys may be predicted or maliciously recovered by attackers.
- Software-protected keys adopt pseudo-random number generation algorithms that are recommended by industry standards and best practices while conforming to cryptography standards. The keys are generated based on seeds, with entropy values provided by the CPUs and hardware servers.

Key versions and automatic key rotation

KMS has a built-in key version management capabilities. While supporting multiple key versions, KMS can also rotate CMKs regularly through configuration. Automatic key rotation allows periodic generation of new versions of CMKs, whereas the earlier versions can be used only to decrypt previously encrypted data. In this way, automatic key rotation reduces the attack surface on keys and protected data.

In some scenarios, it may be necessary to re-encrypt data to replace the ciphertext of an earlier version of a CMK with the ciphertext of a new version.

For specific business needs, users can manually rotate key versions one or more times beyond the automatic rotation cycle.

7.2.2.4. Compliance and security levels

- For regions outside of mainland China
    - Certification: HSMs offered by Alibaba Cloud, including their hardware and firmware, in these regions have passed the FIPS 140-2 Level 3 validation.
    - Operating mode: HSMs outside of mainland China operate under FIPS 140-2 Level 3 standard.

Additionally, the system and mechanism of Alibaba Cloud KMS, including the Managed HSM that it uses, also complies with PCI-DSS. Therefore, KMS helps users' applications and IT facilities to quickly meet the compliance requirements of their business and industry.

7.2.2.5. O&M security

DevOps process

The DevOps of KMS adopts the strictest standards of Alibaba Cloud to ensure the security of your keys.

- Based on the universal DevOps process of Alibaba Cloud, the deployment of every line of code in KMS is reviewed and approved by the DevOps, O&M audit, and security audit teams.
- In addition, KMS introduces a multi-person operating mechanism that requires multiple people with different roles and from different departments to jointly complete service deployment and O&M.

Technical security measures

- Trusted execution environment: The operation of KMS is based on trusted computing technology. After the enforced multi-person initialization operations, a trusted execution environment is established. Moreover, KMS can only start providing services once the controlled root of trust and the measured trusted environment are confirmed.

- Secure access to HSMs: HSMs are not subject to manual O&M. There is no O&M mechanism available for the initial deployment of an HSM, subsequent O&M operation, or direct access. KMS is the only operator of HSMs. This ensures that no undefined or illegitimate access occurs during the operations of HSMs.
- Access control reinforcement: Additional security measures are used to reinforce security during the operation of HSMs. Every HSM within the security boundary of KMS is initialized to undergo multi-party authentication. Every party that authenticates an HSM will separately generate random access credentials for this HSM and register the credentials in this HSM.

By using multiple reinforcement measures, KMS provides a secure HSM execution environment to ensure key security. This also ensures that the use of keys is consistent with user requests only.

Strict internal audit

Every system call in KMS, every O&M event, and every change in the operating system are all recorded in the internal auditing system and separately checked by the Alibaba Cloud audit team.

7.2.3. SSL Certificates Service

Alibaba Cloud SSL Certificates Service allows users to apply, purchase, and manage SSL certificates from well-known third-party certificate authorities (CAs) on the Alibaba Cloud platform. This service implements HTTPS for websites to make them more secure, and protects against hijacking, tampering, and snooping. This service also performs unified lifecycle management of certificates, simplifies certificate deployment, and allows one-click distribution of the certificates to other cloud products.

Alibaba Cloud SSL Certificates Service has the following features:

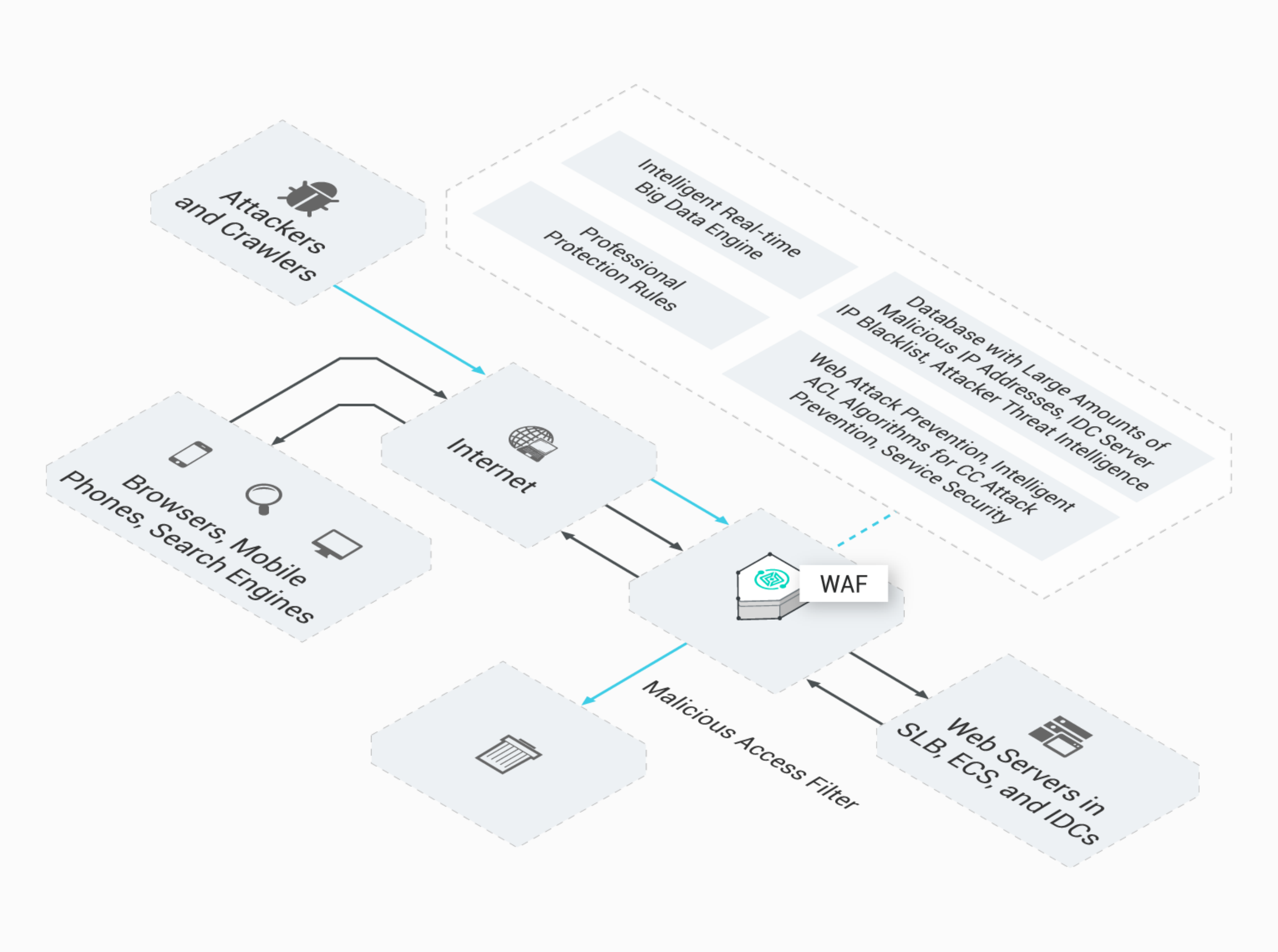
- It implements HTTPS for websites to enable encryption in transit. Therefore, it ensures that the information displayed is reliable, and protects the websites from hijacking, tampering, and snooping.

- It provides digital certificates issued by trusted CAs. It can issue different levels of digital certificates that have been verified by CAs.
- It provides unified management of SSL certificates in multiple channels. Users can view the certificates used by different cloud services and manage their certificate orders on a unified platform.
- It allows one-click deployment of SSL certificates to other Alibaba Cloud products, such as Content Delivery Network (CDN), SLB, Anti-DDoS Pro, and WAF. Therefore, it helps users deploy certificates at a low cost.
- It securely revokes SSL certificates according to standard revocation procedures reviewed by CAs.

7.3. Application security

7.3.1. WAF

Based on the big data and intelligent computing capabilities of Alibaba Cloud Security, Alibaba Cloud WAF defends against common security threats reported by OWASP. These threats include SQL injection, cross-site scripting (XSS), common vulnerabilities in web server plugins, Webshell upload, and unauthorized access to cloud resources. WAF also filters out massive numbers of malicious access attempts, prevents leakage of web assets and data, and ensures the security and availability of web applications.


Attackers and Crawlers
Intelligent Real-time Big Data Engine
Professional Protection Rules
Database with Large Amounts of Malicious IP Addresses, IDC Server IP Blacklist, Attacker Threat Intelligence
Web Attack Prevention, Intelligent ACL Algorithms for CC Attack Prevention, Service Security
Internet
Browsers, Mobile Phones, Search Engines
WAF
Malicious Access Filter
Web Servers in SLB, ECS, and IDCs

As shown in the figure above, WAF is installed at the outlet between web servers and the Internet. WAF identifies web threats and malicious web requests in real time by using the intelligent protection engine, expert protection rules, active protection and detection engine, and cloud threat intelligence. Based on pre-configured protection policies, WAF ensures the security and availability of web applications.

7.3.1.1. Features

Protection against web threats

WAF detects web traffic and defends against common threats reported by OWASP. These threats include SQL injection, XSS attacks, Webshell uploads, backdoor, command injection, illegal HTTP protocol requests, common web server vulnerabilities, unauthorized access to critical files, path traversal, and scanning attacks.

WAF quickly responds to zero-day vulnerabilities, and confirms and updates protection against these vulnerabilities in a timely manner. WAF promptly issues necessary targeted protection rules worldwide to ensure website security. This service also observes trends in targeted attack traffic and continuously observes ongoing attacks, thereby ensuring the completeness of protection capabilities.

Protection against HTTP flood attacks

WAF manages the access frequency from a single source IP address by using re-direction verification and human/machine identification.

WAF prevents massive and slow request attacks based on precise access control policies and recognition of response code and URL request distribution, abnormal Referer and User-Agent requests.

WAF builds threat intelligence and trusted access analysis models to quickly identify malicious requests by making full use of Alibaba Cloud’s big data-based security capabilities.

Precise access control

WAF provides a user-friendly GUI of the configuration console and supports the combination of conditions for 13 HTTP request fields, such as IP, URL, Referer, User-Agent, and Cookie. WAF also configures precise access control policies and supports scenarios such as anti-leech and back-end protection.

Combined with security modules that protect against HTTP flood attacks and common web threats, WAF builds a multi-layer comprehensive protection mechanism to easily identify trusted and malicious traffic as needed.

Log recording and real-time analysis

WAF automatically collects and stores website access logs in near-real time. It also uses Log Service to support features such as query output, analysis, reporting, alerting, and downstream log computation and delivery. Therefore, WAF allows users to focus on log analysis and relieves them from tedious basic querying and sorting operations.

WAF stores website access logs for more than six months.

Visualized security protection

- Security event identification and alerting: Based on big-data intelligent algorithms, WAF aggregates and identifies specific attacks from a massive pool of attacks and access logs, and analyzes the characteristics of these specific attacks. WAF also recommends solutions to handling these events and helps you create a closed-loop secure O&M process.

- Security report and service overview: WAF provides data visualization and statistics, so users can understand the overall threat situation of the website once it is connected to the WAF. Specifically, users can obtain an overview of attack protection and threats, and a detailed analysis of systems, attacks, and threats.
- Data visualization: WAF provides a data visualization service based on detailed logs collected by WAF for your website. By converting the data into a visual big screen, WAF enables you to monitor and understand the real-time attack and defense situations of your website. This provides you with visual and transparent data analysis and decision-making capabilities to keep your website secure.

Web asset identification

Upon your authorization, WAF obtains the configuration information of Alibaba Cloud products such as SSL Certificates Service and Domain Name System (DNS). WAF also obtains information about your website from its traffic. In this way, WAF actively detects the web assets under your Alibaba Cloud account, and provides one-click setup to protect your web assets.

7.3.1.2. Technical capabilities

Intelligent closed-loop defense-in-depth system

Based on the powerful storage and computing capabilities of Alibaba Cloud, WAF builds models for your normal business operations and outputs your business profile by using machine learning methods such as classification and anomaly detection. In this way, WAF avoids false positives caused by non-customized rules, and minimizes the rate of false positives. Based on supervised learning and the use of computer vision and deep neutral networks in text classification algorithms, WAF improves the traditional algorithms for convolutional neural networks. It also builds a deep learning-based attack detection engine that can directly extract attack payloads to provide real time protection and improve the attack detection rate. Based on these model collection and analysis capabilities, WAF rates every access request, and detects the threats that may bypass current policies as well as high-risk requests such as a zero-day attack request, in near-real time. WAF also automatically generates alerts based on these threats and requests. After combining this information with security experts' analyses, WAF updates protection rules across the Alibaba Cloud platform and therefore creates an efficient closed-loop from of early warning protection. Through all these measures, WAF establishes an intelligent closed-loop defense-in-depth system featuring data-driven security.

Modes to implement WAF

- DNS configuration mode: By changing the method of domain name resolution, this mode directs the requests that are sent to a protected domain name to WAF. WAF then forwards the processed requests to the origin server specified in the domain name configuration. Therefore, this mode enables your web server to be stealthy and prevents attackers from bypassing WAF to directly attack your origin servers.
- Transparent mode: WAF enables a fully transparent mode. If you are an Alibaba Cloud ECS user, you can activate this mode for your website with just one click. This mode automatically directs requests that are sent to web applications to WAF. You do not need to modify DNS records. This transparent mode ensures that your specific business operations will not be affected, and enables you to focus more on the businesses themselves.

7.4. Business security

7.4.1. Anti-Bot Service

Alibaba Cloud Security Anti-Bot Service detects and identifies web crawlers. It reduces the impact of web crawlers and automation tools on your website, and provides comprehensive protection for web pages, H5 pages, apps, and APIs. This service protects your business in scenarios such as scraping of airline tickets, scalping in e-commerce activities, credential stuffing, malicious calls to core APIs, and malicious ticket or credits brushing.

7.4.1.1. Features

Access control list

Through the access control list (ACL), you can configure custom protection policies for your business scenarios by combining common HTTP request fields, such as IP, URL, Referer, UA, and other parameters, to formulate filter conditions. These policies consist of matching conditions and matching actions.

Frequency limiting

A frequency limiting policy is used to limit the rate of a single field (i.e. IP, Cookie, Header, etc.) on a specific URL path that can access the server. In addition, you can set a certain threshold value for the number or proportion of response codes to limit access requests.

Permit legitimate bots

Anti-Bot provides a whitelist of crawlers used by legitimate search engines such as Google, Bing, Baidu, Sogou, 360, and Yandex. Anti-Bot can allow these search engine crawlers to access your entire website or specific directories.

Bot intelligence

Based on the powerful computing capabilities of the Alibaba Cloud platform, Anti-Bot provides information about suspicious IP addresses used by modem pools, data centers, and malicious scanners. Anti-Bot also maintains a malicious crawler library. Anti-Bot can prevent these IP addresses and crawlers from accessing your website or specific directories in real time.

Protection based on intelligent algorithms

Anti-Bot provides general algorithms for identifying typical crawler behaviors. You can also configure basic business parameters and a risk threshold for the machine learning algorithm, in order for Anti-Bot to prevent more advanced crawlers.

Enhanced app protection

Anti-Bot Service (Anti-Bot) provides a security solution, Anti-Bot SDK, for native apps. This provides security protection such as trusted communication, protection against scraping with bot scripts, and identification of suspicious IP addresses and modem pools. This feature can also effectively identify proxies, simulators, and illegal signing requests.

Human-machine identification

Through a multi-dimensional analysis of behavioral data, web data, and characteristics of devices, Anti-Bot determines the risk level of potential threats, such as simulation, the use of insecure devices, and brute-force replay, in a comprehensive and real-time manner. Based on simple interactive authentication logic, Anti-Bot enables a user to pass human-machine identification without much overhead. It can also accurately determine whether an access request is sent by a real user or a computer.

7.4.1.2. Technical capabilities

Anti-Bot can effectively reduce the impact of crawlers or automation tools on your website.

Multi-layer integrated intelligent protection

- The reverse proxy deployment architecture filters and intercepts bot traffic before the bot traffic reaches the server. This is the first-layer filtering of bot traffic. This deployment effectively reduces extra resource consumption brought by bot traffic reaching the server. Additionally, as the second-layer filtering of bot traffic, No-Captcha or JavaScript verification methods are used to deal with suspicious traffic.
- Anti-Bot provides multi-dimensional identification that includes targeted policies, high-frequency detection, bot intelligence, and crawler behavior analysis. These modules can deal with different levels of threats from low-level script-based crawling to high-level human behavior simulation.
- Anti-Bot supports independent access to the human-machine identification module that includes No-Captcha, non-invasive verification, and intelligent verification. The multiple modes effectively reduce the risk of logon, registration, SMS, and red envelope APIs being brushed.

Anti-Bot SDK

Anti-Bot SDK signs and validates requests, and identifies any risky devices. Therefore, this feature protects mobile apps against bots more effectively.

7.4.2. Content Moderation

Content Moderation is an intelligent multimedia content recognition service that supports the detection of objects, such as images, videos, texts, and audio. This service effectively helps you decrease the risk of content policy violations. Content Moderation is commonly used to recognize pornographic, violent, terroristic, and other sensitive content types. The service can also detect advertising images and text, logos, and QR codes. This service also supports text and image recognition with optical character recognition (OCR), and combats text, audio, and file spam. Content Moderation provides a site detection function that automatically detects high-risk and illegal or inappropriate content on your website on a regular basis. This service also detects sensitive content in the text and video objects that you specify in OSS buckets. You can also directly call the Content Moderation API and submit recognition tasks for specified scenarios.

Content moderation provides the following features:

- **Site detection**

  This feature detects your website homepage and all the content on your website on a regular basis for any possible risks. Some of these risks are homepage tampering, malicious code or script insertion, pornographic content, and violent, terroristic or other sensitive content. This feature also displays the specific IP addresses of illegal content to you, and helps you view and deal with these addresses. You can also set message notifications or choose to use email, SMS or direct message (DM) to obtain real-time risk reminders for your website homepage.

- **Detection of illegal content in OSS buckets**

  This feature uses AI to help you find whether images and videos stored in Alibaba Cloud OSS buckets contain high-risk content. This feature also automatically freezes the detected illegal content, preventing further distribution.

- **Content Moderation API**

  Based on advanced technologies and the big data capabilities provided by Alibaba Group, the Content Moderation API monitors multimedia content such as text, images, and video. This service is independent of other Alibaba Cloud services, and can filter and monitor all accessible images and texts on public sites. The following table describes some scenarios.

Scenario	Description
Detection of illegal content in images	This function detects illegal images or recognizes inappropriate content in images. It supports detection of the following content types: • Pornographic content • Violent, terroristic, or other sensitive content • Illegal text and images • QR codes • Inappropriate content • Logos

Scenario	Description
Illegal video content detection	This function detects illegal content or inappropriate information in videos. It supports the following scenarios: • Pornographic content • Violent, terroristic, or other sensitive content • Illegal text and images • Inappropriate content • Logos
Text spam detection	This function detects illegal or inappropriate content in text, and supports the following scenarios: • Advertising content • Violent, terroristic, or other sensitive content • Abusive content • Pornographic content • Flooding/spamming content • Meaningless content • Contraband-involved content • Custom (keyword filter)
Audio spam detection	This function detects illegal or inappropriate content in audio, and supports the following scenarios: • Advertising content • Violent, terroristic, or other sensitive content • Abusive content • Pornographic content • Flooding/spamming content • Meaningless content • Contraband-involved content • Custom (keyword filter)
Text and image recognition with OCR	This function identifies structured and unstructured text messages in images, including the following structured cards and credentials: • ID card • Passport • Bank card • Business license • Value-added tax invoice • Driver's license • License plate

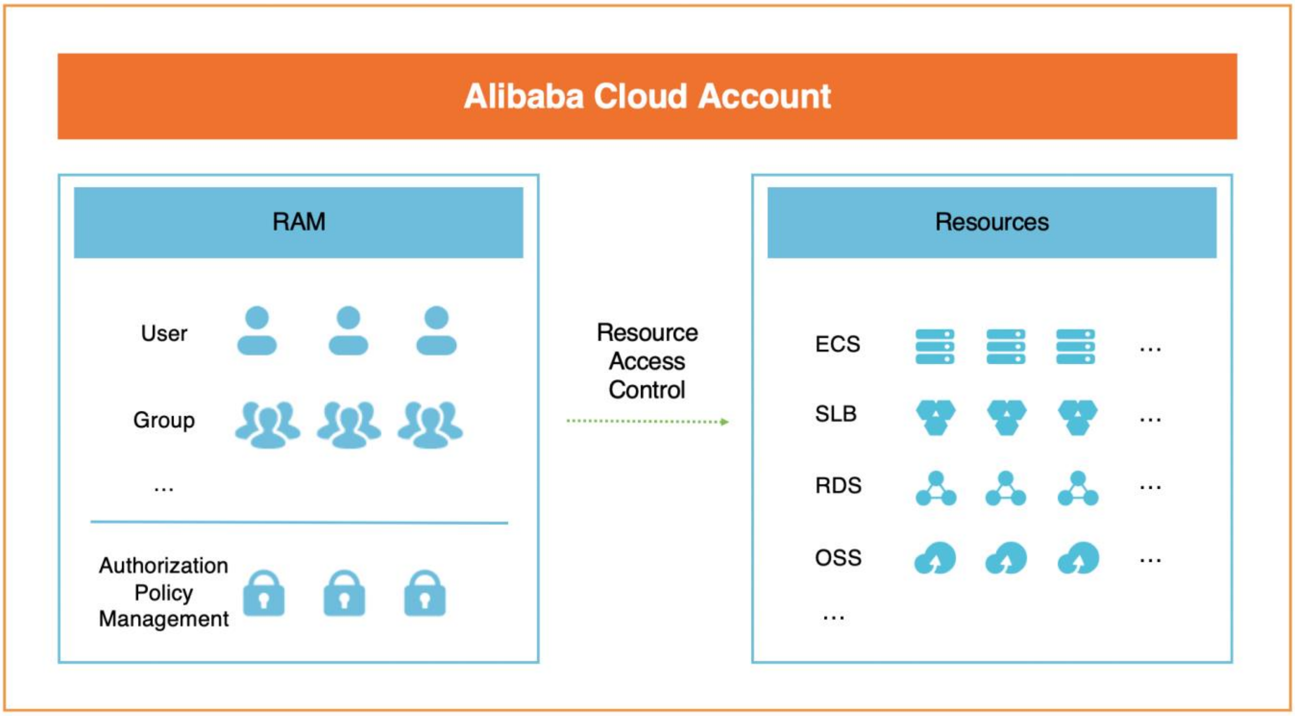
Scenario	Description
	- Vehicle identification number (VIN) **Note:** Text and image recognition with OCR supports the use of custom templates.
Face recognition	This function has the following capabilities: - Face attribute detection - Face comparison - Face retrieval - Recapture detection - Mobile biometric “liveness” detection (ensure the biometric check is being attempted by a real person) **Note:** Mobile biometric “liveness” detection is available in an offline Android SDK. Your client can call the Recapture Detection operation through the server API.
Similar image search	This function finds the top N images similar to the given image in your custom image library.
Image labeling	This function identifies the subject in an image and outputs a corresponding label.
Video fingerprinting	This function searches video libraries for videos with the same origin as the given video.

7.5. Account security and monitoring

7.5.1. RAM

Alibaba Cloud provides multiple tools and features to securely authorize access to resources in different scenarios. Among them, the Resource Access Management (RAM) service is provided for user identity management and resource access control. RAM enables an Alibaba Cloud account that can be regarded as a primary account to have multiple independent RAM users. RAM also supports features such as multi-factor authentication (MFA), strong password policies, the isolation of console users from API users, custom fine-grained authorization policies, grouped authorization, and temporary Security Token Service (STS) tokens. RAM authorization can be specific to an API action or resource ID. Users can specify authorization conditions, such as the source IP address, secure access channel (SSL or TLS), access time period, and MFA.

RAM provides centralized services for user identity and access control management. The following figure shows the relationships between RAM and other cloud services.



RAM is the basis for the security management and O&M of Alibaba Cloud accounts. RAM can assign a different password or Access Key to each RAM user, and therefore eliminates the security risks that arise from sharing Alibaba Cloud credentials among multiple people. Assigning different work permissions to different RAM users also reduces the risks associated with excessive permissions that come with the Alibaba Cloud account.

7.5.1.1. User management

An Alibaba Cloud account can create one or more independent RAM users through the RAM service. The Alibaba Cloud account and its RAM users have the following relationships:

- From the perspective of resource ownership, resources belong to the Alibaba Cloud account, which is the basic subject for the billing of used resources. RAM users can exist only under an Alibaba Cloud account. RAM users do not possess resources, and the resources they create under authorization belong to the Alibaba Cloud account. RAM users are not billed, so all expenses incurred by their authorized operations are also charged to the Alibaba Cloud account where they reside.

- From the perspective of permission management, the relationship between the Alibaba Cloud account and its RAM users is analogous to that of Root and User in Linux. The Alibaba Cloud account has all the permissions to manipulate and control resources, and RAM users only possess certain permissions authorized by the Alibaba Cloud account. In addition, the Alibaba Cloud account can revoke the permissions authorized to its RAM users at any time. Meanwhile, the Alibaba Cloud account can grant RAM users permission to manipulate RAM resources.

Each RAM user represents the identity of a security principal, such as some operational personnel or an application. If a new user or application wants to access the cloud resources under an Alibaba Cloud account, a RAM user must be created and must then be granted access to the relevant resources. If multiple RAM users are created under one Alibaba Cloud account, as a more convenient approach to manage RAM users and permissions, it is recommended to create groups to categorize RAM users based on job function and assign permissions to these groups rather than to individual users.

The administrator can also create a kind of users called "RAM role" through RAM. Both the RAM role and RAM users are identity objects for RAM management. The difference between the RAM role and RAM users is that the RAM role is, in a sense, a virtual user who does not have a long-term authentication Access Key and cannot be used without being assumed by a trusted RAM user identity.

7.5.1.2. Credentials

Credentials are used to verify the real identity of a user. This usually refers to a user's logon password or Access Key. Credentials are confidential. Users must keep them secure.

RAM users support the following credentials:

- **Logon name and password**

  A user can use the logon password and user name of its Alibaba Cloud account or those of its RAM users to log on to the Alibaba Cloud console and perform operations on cloud resources. The password policies and the associated risk control policies for logon security are managed by Alibaba Cloud. The password policies for RAM users can be defined by the Alibaba Cloud account owner, which include the required character combinations of a password, the number of logon retries, the password rotation cycle, and so on. For example, a user can create password policies for RAM users in the RAM console to ensure that each RAM user uses a strong password rotated on a regular basis. This improves overall account security.

- **AccessKey pair**

  An Access Key (AK) is the credential used for calling Alibaba Cloud service APIs. It is used to authenticate the identity of users who access Alibaba Cloud resources through APIs. API credentials are equivalent to logon passwords. The former is used to call the API of a cloud service, while the latter is used to log on to the console. An Access Key consists of an AK ID and an AK secret.

  Based on security best practices, Alibaba Cloud recommends that users create different Access Key credentials for each RAM user to effectively divide permissions and reduce risks by following the principle of least privilege. Furthermore, an Alibaba Cloud account can be viewed as a “root” account, which has full control permissions to all cloud products and resources under the account. Hence, to avoid the risk of exposing the Access Key of the root account, it is recommended that all users should operate resources at the RAM user level and not create Access Keys under the root account unless absolutely necessary.

- **MFA**

  Multi-factor authentication (MFA) is a simple and effective security best practice that provides an extra level of protection on top of username and password. With MFA enabled, a user is asked to enter their username and password (first security factor), and then a variable verification code (second security factor) from an MFA device when logging on to the Alibaba Cloud console. These factors combine to provide a higher-level of protection for user accounts. Alibaba Cloud supports software-based virtual MFA devices. A virtual MFA device is an application that generates a 6-digit verification code, and complies with the time-based one-time password (TOTP) standard (RFC 6238). The virtual MFA application can run on mobile hardware devices (including smartphones).

7.5.1.3. Authentication via AK

An Access Key (AK) is the credential used for calling Alibaba Cloud service APIs. It is used to authenticate the identity of users who access Alibaba Cloud resources through APIs. An Access Key consists of an AK ID and an AK secret. A user can apply for and manage AK ID and AK secret on the Alibaba Cloud console. An AK ID is used to identify a user, and an AK secret is used to authenticate the user's identity. When calling a cloud resource API, a user will pass in an AK ID and use an AK secret to sign the request based on the HMAC-SHA1 algorithm. The encrypted signature has a timestamp that can prevent replay attacks. When the service receives a user's request, it finds the corresponding AK secret according to the AK ID in the request. It then computes the encrypted signature in the same way and verifies the user identity.

An Alibaba Cloud account owner can log on to the Alibaba Cloud User Center or RAM console to manage Access Keys. The account owner can create, freeze, enable, and delete Access Keys. Since the AKs can be used for API requests for a long period of time, users should rotate their AKs on a regular basis.

7.5.1.4. User group management

If an Alibaba Cloud account owner has created multiple RAM users under their account, it is recommended that the account owner uses groups to better manage the users and their permissions. The account owner can create groups for RAM users who share the same responsibilities, such as Admins, Developers, and Accounting, and have permissions categorized and granted to these groups. When the responsibilities of a user change, one only needs to move the user to a different user group corresponding to their new responsibilities, without affecting other users. When the permissions of a group change, one only needs to modify the authorization policies for the group, and the new policies will immediately apply to all group members.

7.5.1.5. Permission and policy management

Permissions

Alibaba Cloud uses permissions to describe the ability of an operation security principal, such as a RAM user, user group, or RAM role, to access a specific resource. Permissions are used to allow or deny specific operations on specific resources under specific conditions.

- The Alibaba Cloud account, also known as the root account, primary account, or resource owner, controls all permissions.
  - Each resource has one owner. The owner must be an Alibaba Cloud account, which pays for and has full control over the resource.

    - The resource owner is not necessarily the resource creator. For example, if a RAM user is granted the permission to create resources, the resources created by this user belong to the user's Alibaba Cloud account. In this case, the RAM user is the resource creator, but not the resource owner.

- By default, a RAM user has no permissions.
    - A RAM user is an operator and must be explicitly granted permissions before performing any operations.
    - A new RAM user has no operation permissions by default, and can manipulate resources in the console or by calling API operations only after being granted permissions.
- A RAM user is not automatically granted permissions for the resources created by this user.
    - A RAM user can create resources if the user is granted the resource creation permission.
    - However, the RAM user is not automatically granted any permissions for the created resources, unless the resource owner explicitly grants permissions to the user.

Policies

Permissions are defined in policies. A policy is a set of permissions described by using policy structure and grammar. By attaching policies to a RAM user or a RAM user group, the user or all users in the group can obtain the access permissions specified in the policies. By default, access denial takes priority.

RAM supports two types of policies: system policies and custom policies.

- **System policies**

  A system policy is a set of generic policies provided by Alibaba Cloud, which specify permissions for different products, such as read-only permission or full permission for ECS instances. System policies provided by Alibaba Cloud can only be used for granting permissions and cannot be edited and modified by users. These policies are automatically updated by Alibaba Cloud.

- **Custom policies**

RAM allows users to create custom policies and use these policies for fine-grained authorization control. The key components of a policy are the effect, resource, action, and condition components. For example, the following fine-grained authorization can be implemented: Read-only operations can be performed on SampleBucket in OSS on conditions that the requester's IP address is 42.160.1.0, and the access time is earlier than 9:00 Coordinated Universal Time (UTC+8) on September 30, 2019. Otherwise, the access is denied.

7.5.1.6. RAM role management

A RAM role can be regarded as a virtual RAM user. It does not have any long-term authentication credentials, such as logon passwords or Access Key. A RAM role can be used only after it is assumed by a trusted RAM user. RAM roles can be used in scenarios such as cross-cloud-account resource authorization, resource access authorization among various cloud services, the issuance of on-demand authorization tokens to mobile apps, and the implementation of role-based Single Sign-On (SSO).

The following types of RAM roles are available:

- **User role**

  Roles of this type can be assumed by RAM users. The RAM users can be under your own Alibaba Cloud account or other accounts. Roles of this type are mainly used to provide cross-account resource access and temporary authorization. Please note, after switching to a RAM role identity, the RAM user can only perform operations authorized to this role identity, but the access permissions of the user's real identity upon logon will not be available. When switching back to the logon identity, the RAM user has the access permissions of its own identity, but not those of the role identity.

- **Instance role**

  You can associate a RAM role with an ECS instance or Elastic Container Instance (ECI) to access other cloud services by using a temporary STS token within the instance. The temporary token is refreshed periodically. In this way, the security of your Access Key is ensured, and fine-grained permission control is implemented based on RAM.

- **Service role**

Roles of this type are assumed by Alibaba Cloud services. Such roles are used to authorize a cloud service to access the resources of other cloud services.

- **IdP role**

  Roles of this type can be assumed by users of a trusted IdP. These roles are mainly used to implement SSO to Alibaba Cloud.

7.5.1.7. SSO management

Alibaba Cloud supports SSO based on Security Assertion Markup Language 2.0 (SAML 2.0), and allows a user to use the enterprise's identity system (identity provider) to log on to Alibaba Cloud (service provider).

To meet the logon needs of different enterprises, Alibaba Cloud provides two SSO methods based on SAML 2.0:

- User-based SSO: The RAM user that you can use to log on to Alibaba Cloud can be determined through a SAML assertion issued by an IdP. After logon, you can use the RAM user to access Alibaba Cloud. The corresponding access permissions are restricted by the policies attached to the RAM user.
- Role-based SSO: The RAM role that you can use to log on to Alibaba Cloud can be determined through a SAML assertion issued by an IdP. After logon, you can use the role specified in the SAML assertion to access Alibaba Cloud. The corresponding access permissions are restricted by the policies attached to the RAM role.

7.5.1.8. Resource group management

Resource group management is a basic capability required by enterprises with the need to manage large sets of cloud resources. Alibaba Cloud provides two methods to help group resources: grouping based on resource tags and grouping based on managed resource groups.

- Resource tags

  Users can define and manage tags for massive sets of resources. Specifically, users can use the tags provided by cloud products to filter resources by tags, write RAM policies with tag specifications, and categorize bills by tags. In this way, users can implement basic resource grouping by using tag management.

- Resource groups

  Resource groups are an enhanced feature for resource group management within a single cloud account. It can help address the complexity of resource grouping and authorization management within a single cloud account. Compared with grouping resources by tags, resource groups are not only easy to use, but also support hierarchical authorization. That is, users can specify resource group administrators, which is not supported by resource tagging.

7.5.1.9. Multi-account management

A cloud account is the smallest management granularity for Alibaba Cloud resources in terms of isolation, metering, and billing. To isolate resources or manage costs, enterprise users often need to use and manage multiple cloud accounts. To this end, Alibaba Cloud provides a hierarchical multi-account management service called Resource Directory for enterprise users.

Resource Directory allows administrators to easily create a resource directory structure that reflects the organizational hierarchy of their enterprise, and allows Alibaba Cloud accounts to be placed into this structure (directory), forming a multi-level relationship among resources. Enterprise users can rely on established organizational relationships to centrally manage resources and meet the management requirements of their finance, security, audit, and compliance teams.

7.5.1.10.STS

Alibaba Cloud Security Token Service (STS) provides RAM users with authorization credentials for short-term resource access. In some cases, persons or applications require only occasional access to cloud resources, rather than the long term access granted by AccessKeys: such users are called "temporary users". In some other use cases, such as applications running on untrusted mobile devices, it is undesirable to issue them long-term AccessKeys due to the insecure nature of the execution environment. In these cases, STS can be used to issue temporary authorization credentials to these users. When issuing a token, the administrator can define the permissions and expiration time (one hour by default) for the token as needed.

An STS access token is a triplet that includes a security token, an AccessKey ID, and an AccessKey secret. The user passes in the security token and the AccessKey ID to call resource APIs, and uses the AccessKey secret to sign the request. Security tokens issued by STS are not used together with other Access Keys.

STS makes resource authorization more controllable because it eliminates the need to create and manage a long-term RAM user account and an Access Key for a temporary user or a user with a low security level. Moreover, the authorization credentials are automatically issued by STS, therefore they are not embedded in locations that are not secure locations such as client-side code. By default, tokens rotate automatically on an hourly basis to improve security.

7.5.2. Log Service

As a one-stop service for log data, Log Service is built based on the experiences of the massive big data scenarios of Alibaba Group. Log Service allows you to quickly complete the collection, consumption, shipping, querying, and analysis of log data without the need for low-level development, which improves maintenance and operational efficiency, and builds the processing capabilities to handle massive amounts of log data in the data technology (DT) era.

Note that although Log Service is not a security product in a traditional sense, its log collection, consumption querying, and shipping functions are closely related to cloud security monitoring and operations. Therefore, Log Service is also introduced here.

7.5.2.1. High availability

Log Service stores logs in a distributed file system, and uses a triplicate distributed storage mechanism to ensure data reliability and durability.

7.5.2.2. Read-only log system

Tampering resistance is an important feature of Log Service. Log Service provides an append-only log system. Additional information can only be appended to the logs, but existing logs cannot be modified, which effectively prevents log tampering.

7.5.2.3. Archiving

In addition to the real-time query and analysis functions, Log Service also provides the capability to store log archives to MaxCompute and OSS, so that users can analyze log data by using MaxCompute and other open source big data processing software.

7.5.2.4. Authentication

Log Service authenticates each API request. Users need to include signature information in their requests. Log Service uses Access Keys as the credentials for authentication. For more information about the AK authentication process, see 7.5.1.3. Authentication via AK.

7.5.2.5. Features

Real-time collection and consumption

- LogHub collects real-time log data such as metrics, events, binary logs, text logs, and clicks from ECS, containers, mobile terminals, open source software, and JS.
- A real-time consumption interface is provided to interconnect with real-time computing and other services.

Purposes: This feature can be used for ETL (extract, transform, load), stream computing, monitoring and alerting, machine learning, and iterative computing.

Query and real-time analysis

- Query: supports querying by keyword, fuzzy match, context, and range.
- Statistics: provides a variety of query methods including SQL aggregate queries.
- Visualization: provides dashboards and reports.
- Interconnection: supports Grafana, JDBC, and SQL-92.

Purposes: This feature can be used for DevOps and online O&M, real-time log data analysis, security diagnosis and analysis, and operations and customer service systems.

Authoritative data sources for profiling

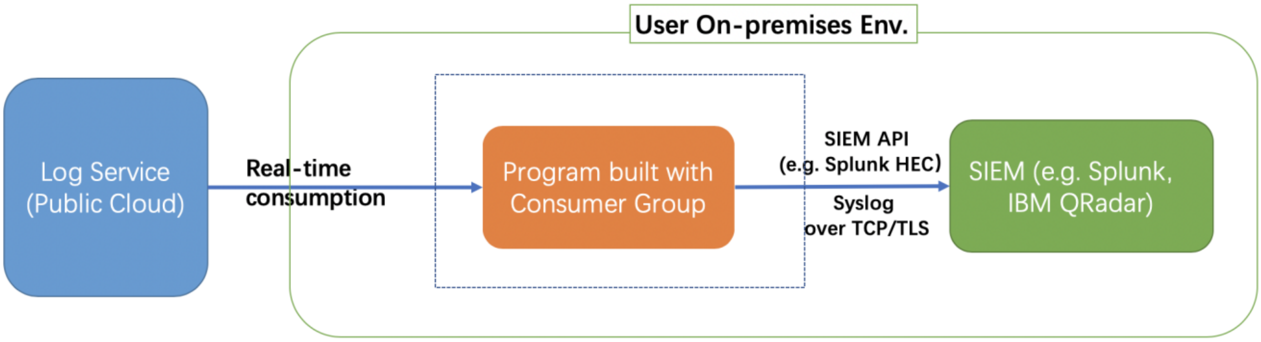
Stable and reliable log shipping is provided. Log Service ships collected logs to storage services for storage. Various storage methods are supported, such as compressed files, user-defined partitions, rows, and columns.

Purposes: This feature can be used for data warehousing and analysis, data auditing, product recommendation, and user profiling.

7.5.2.6. Integration with SIEM

Log Service supports shipping logs to a security information and event management (SIEM) system, such as Splunk or IBM QRadar. This ensures that all logs related to regulations and audits on Alibaba Cloud can be exported to a user's security operations center (SOC).

Log Service supports sending logs to SIEM over HTTPS. Take Splunk as an example. Generally, SIEM is located within a user on-premises environment. We recommend that you develop the required program based on consumer groups to consume logs from Log Service in real time. Then, you can call API operations provided by Splunk HEC to send logs to Splunk. Log Service also supports shipping logs to a SIEM system over Syslog. Syslog is a widely used logging standard, almost all SIEM systems, such as IBM QRadar and HP Arcsight, can receive logs over Syslog. As shown in the following figure, the program based on consumer groups is used to consume logs from Log Service in real time, and logs are sent to the SIEM system through Splunk HEC or Syslog over TCP or TLS. It is recommended to send Syslog messages over TCP or TLS if the SIEM system supports TCP or TLS.


User On-premises Env.
Log Service (Public Cloud)
Real-time consumption
Program built with Consumer Group
SIEM API (e.g. Splunk HEC)
Syslog over TCP/TLS
SIEM (e.g. Splunk, IBM QRadar)

7.5.2.7. RAM and STS support

Log Service supports RAM. With RAM, users can grant access and management permissions for Log Service resources under an Alibaba Cloud account to a RAM user.

Log Service also supports Security Token Service (STS). With STS, users can provide RAM users with temporary authorization credentials that allow short-term access to resources.

7.5.3. ActionTrail

ActionTrail records operations on Alibaba Cloud resources, supports operation record querying, and saves record files to specified OSS buckets or to Logstores in Log Service.

By using all the operation records saved by ActionTrail, users can perform security analysis, resource change tracking, and compliance audit.

ActionTrail records the operations performed through Alibaba Cloud APIs, including those triggered by using the Alibaba Cloud console. Then, ActionTrail processes the operation records and store them as logs in Log Service or as files in the specified OSS bucket. Users can manage the records files using all the management functions provided by OSS, such as authorization, enabling lifecycle management, and archiving management. Meanwhile, users can also use OSS data encryption and permission management functions to ensure the data security of event records. ActionTrail supports operation event queries along such dimensions as username (i.e. operator), operation time, source IP address, resource object, operation name, and operation status, and it can help to diagnose problems quickly or track security incidents.

Generally, ActionTrail records the operations that users perform when using Alibaba Cloud services. These operations include those performed in the Alibaba Cloud console, those for calling Alibaba Cloud APIs, and those triggered by Alibaba Cloud services through RAM roles. The operation records are saved to ActionTrail within 10 minutes. Users can use the ActionTrail console to view their operation records for the last 30 days.

ActionTrail is mainly applicable to the following scenarios:

- Security analysis

  Logs recorded by ActionTrail can be used for security analysis for any potential security issues. For example, ActionTrail records all account logon operations, including detailed records such as the logon time, which IP was used, whether multi-factor authentication logon was used, etc. With these records, Users can determine whether their accounts have any security issues.

- Resource change tracking

  When any cloud resources were changed unexpectedly, the operation logs recorded by ActionTrail can help users identify how the changes took place. For example, when a user noticed that an ECS instance had stopped, with the help of ActionTrail, the user can find out who initiated the operation, from which IP, and at what time, etc.

- Compliance audit

If a user's organization has multiple members and the Alibaba Cloud RAM service is used to manage the identities of members, it is generally required for the user to obtain the detailed operation records of each member to meet the compliance auditing requirements. The operation events recorded by ActionTrail can meet these compliance auditing requirements.

7.5.3.1. Internal operation transparency

Traditionally, internal O&M operations done by the cloud platform are invisible to users. In other words, users are not aware of and cannot monitor or audit O&M actions performed by the cloud provider. Although Alibaba Cloud has obtained industry-leading third-party compliance certifications, efforts must also be made to give users the confidence that their data and resources are properly protected and managed within the cloud platform. To this end, Alibaba Cloud provides the ability to make relevant internal operations transparent to users by providing internal operation logs in selected products (such as OSS). This allows users to monitor and audit internal cloud platform operations when using Alibaba Cloud products.

ActionTrail provides an Inner-ActionTrail feature that can automatically collect and store Alibaba Cloud platform-side operation events in near-real time. Based on Log Service, Inner-ActionTrail can output relevant internal operation logs for query analysis, reports, alerts, and downstream computing and delivery. Thus, users can perform analysis and audit of internal operations on the cloud platform.

7.5.4. Cloud Config

Cloud Config is a resource-oriented audit service. It provides cross-region resource configuration checklist and retrieval capabilities, records historical configuration snapshots of resources, and forms a configuration timeline. When a resource configuration change occurs, a compliance assessment is automatically triggered and an alert is generated for the non-compliant configuration. Cloud Config allows users to easily monitor the compliance status of massive sets of resources to meet internal and external compliance requirements.

When Cloud Config is used, the resources in each region under an Alibaba Cloud account are scanned to form a cross-region resource checklist, which supports simple retrieval. A user can set all or part of the account resources to be monitored. Cloud Config continuously monitors and records the configuration change details of resources, compares the changes in detail, and organizes the configuration timeline of resources. Therefore, a user can have a clear picture of the evolution of the resource configuration over time.

Cloud Config saves configuration snapshots of resources as files to specified OSS buckets. A user can use all the management functions provided by OSS to manage these record files, such as authorization, enabling lifecycle management, and enabling archival management. Meanwhile, the user can use OSS data encryption and permission management features to ensure the data security of event records. By using the historical configuration snapshots of resources together with the operation records from ActionTrail, the user can quickly locate the time when a problem occurred, list affected resources, see configuration changes, and find the accounts from which actions were initiated.

Cloud Config analyzes the results of resource changes. If a resource is changed or restored within the window period (10 minutes), Cloud Config cannot perceive the changes. Therefore, the corresponding configuration change snapshot cannot be generated. If a resource is changed several times within the window period (10 minutes), Cloud Config summarizes the results of multiple changes into a single configuration change record, displays it on the configuration timeline, and saves the snapshot to your OSS bucket.

Cloud Config uses functions in Function Compute as the editor and executor of compliance rules. A user can implement compliance rule by adding code to rule functions. Rules must be associated with specified resources in Cloud Config. When a configuration change record is generated for a resource, the rule function is automatically run to assess the compliance of the resource configuration, and sends notifications and alerts to relevant personnel based on user subscriptions if applicable. In addition to rule executions triggered by configuration changes, regular and manual rule execution is also supported. Based on actual compliance requirements, Cloud Config provides dozens of preset rule functions and supports custom rule functions.

Cloud Config is mainly applicable to the following scenarios:

- **Centralized resource configuration management**

  It is inconvenient to manage resources that are deployed across regions. To solve this problem, Cloud Config provides users with the cross-region resource checklist and retrieval capabilities. Users can use the resource checklist as a unified portal for resource management. Users can directly view the resource configuration timeline online, or manage resources in the console of an Alibaba Cloud product.

- **Continuous compliance audit**

  Provided with massive cloud resources, users can make frequent resource changes every day. Continuous self-monitoring is required to ensure that the specifications and configurations of the purchased resources are compliant. For example, a compliance requirement could be that access to storage space is prohibited from public networks, or that all disks must be encrypted. When non-compliance occurs, a notification about the non-compliant configuration can be sent quickly, and relevant resources can be quickly located and brought into compliance.

- **Problem detection and reproduction**

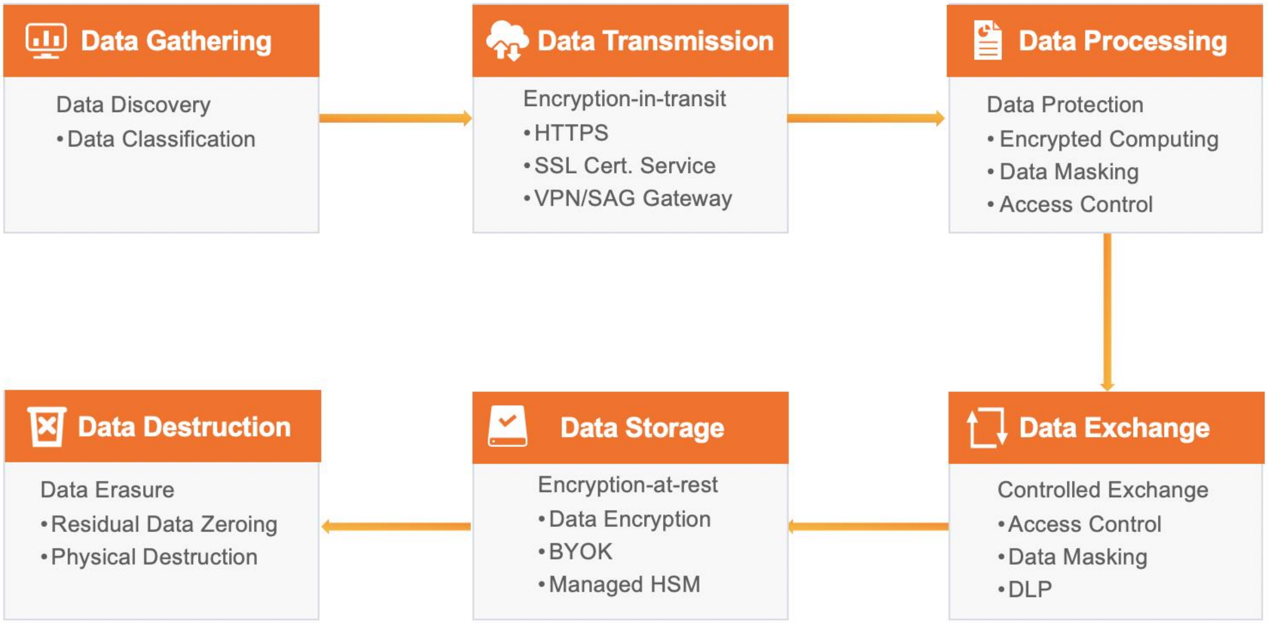
  When a problem occurs, the most important thing is to quickly locate and solve it. However, after the problem is solved, reproducing, recalling, and archiving the problem are of equal importance. By using the resource history configuration snapshots from Cloud Config together with the operation records from ActionTrail, a user can sort out the context of an entire event. One can find information including the initial location of the problem, related personnel, list of affected resources, list of rules violated, and related operation logs. Then, the user can quickly compose a report on the problem.

8. Cloud Data Security System

User data security on the cloud is one of the most critical security requirements of users and one of the most important representational attributes of the overall cloud security capability. The data of all developers, companies, governments, and social institutions on the cloud computing platforms belongs only to these users. Cloud computing platforms cannot use the data for other purposes. Cloud service providers have the responsibilities and obligations to help users ensure the confidentiality, integrity, and availability of their data.

Up to this point, this white paper has described Alibaba Cloud's capabilities and products for cloud data security protection in detail. This chapter intends to sort out the overall data security lifecycle on the cloud and describes how to use relevant capabilities and products on the cloud to build a comprehensive data security system.

Alibaba Cloud develops its data security system comprehensively and systematically by taking management and technical measures based on the data security lifecycle. Data security is managed and controlled throughout the data lifecycle that covers gathering, transmission, processing, exchange, storage, and destruction. Each stage of the data security lifecycle has its associated security management requirements and technologies.



8.1. Data gathering security

Data gathering security requires that data identification, classification, and categorization can be completed in a timely manner when data is created and gathered. In this way, subsequent cloud data protection techniques can be properly used. Proper data discovery can ensure the accuracy and efficiency of security protection in the future. Firstly, sensitive information in the data needs to be discovered, such as Personal Identifiable Information (PII). Secondly, the sensitive information in the data needs to be classified and categorized according to a user's application scenario, compliance requirements, and security requirements, so that the user can be aware of data assets and take appropriate protection actions later.

Alibaba Cloud Sensitive Data Discovery and Protection (SDDP) can discover and classify user data on the cloud. After being authorized by a user, SDDP can automatically scan and discover different sensitivity levels of data, such as newly added data from new instances, databases, tables and columns, OSS buckets and objects. SDDP uses keywords, rules, and machine learning algorithms to accurately identify sensitive data within the cloud environment, and allows users to customize sensitive data discovery policies based on their needs. Based on the identification results, SDDP can classify user data on the cloud based on business content and sensitivity level and then implement relevant protection mechanisms for the data according to the discovery and classification results.

Alibaba Cloud DataWorks also provides rules for automatic data identification, classification, and categorization. A user can also use the Label Security function in MaxCompute to label relevant sensitive data.

8.2. Data transmission security

8.2.1. HTTPS transmission encryption

Data transmission security is guaranteed by encryption in transit. Alibaba Cloud products use the SSL/TLS protocol to ensure data transmission security while users read and upload data. The Alibaba Cloud console uses HTTPS encryption for data transmission. Alibaba Cloud products provide API access points that have HTTPS encryption enabled with 256-bit key length to address the need for encrypted transmission of sensitive data.

8.2.2. VPN Gateway and Smart Access Gateway

Alibaba Cloud gateway products also provide end-to-end encryption during data transmission. VPN Gateway securely and reliably connects on-premises data centers to Alibaba Cloud VPC over encrypted channels. VPN Gateway can establish an IPsec-VPN connection to connect an on-premises data center to a VPC. It can also establish an SSL-VPN connection to connect a remote client to a VPC. Alibaba Cloud also provides Smart Access Gateway (SAG) that allows enterprise users to access the nearest cloud resources through encrypted connections and encrypt the transmitted data with the Internet Key Exchange (IKE) and Internet Protocol Security (IPsec) protocols to secure data.

8.2.3. SSL Certificates Service

Alibaba Cloud SSL Certificates Service allows users to apply for, purchase, and manage SSL certificates from well-known third-party certificate authorities (CAs) on the Alibaba Cloud platform. This service implements HTTPS for websites to make them more secure, and protects against hijacking, tampering, and snooping. This service also performs unified lifecycle management of certificates, simplifies certificate deployment, and allows one-click distribution of the certificates to various cloud products, such as Content Delivery Network (CDN), SLB, Anti-DDoS Pro, and WAF.

8.3. Data processing security

Data processing security is mainly implemented through the effective isolation and protection of data in use. The isolation can be implemented by using the encrypted computing environment of Intel® Software Guard Extensions (Intel®SGX) during runtime on the user side. Isolation methods, such as permission controls specific to each product, can also be used. Moreover, data masking of classified sensitive data can be used to ensure unauthorized users can not view sensitive information. In real world scenarios, multiple features and products are often used together to meet data isolation and protection requirements.

8.3.1. Encrypted computing

The Alibaba Cloud platform uses Intel® Software Guard Extensions (Intel® SGX) to provide a hardware-based encrypted computing environment. Users can create a trusted execution environment through software to protect sensitive data such as encryption and decryption keys and account credentials. Based on ECS Bare Metal Instances that support encrypted computing, users can protect their data by writing code that supports the trusted execution environment. This ensures that their sensitive data can be accessed and manipulated only through the code that they write. With Alibaba Cloud encrypted computing technologies, Alibaba Cloud provides an additional data encryption capability at runtime through the SGX based trusted execution environment.

8.3.2. Cloud product permission control

Alibaba Cloud products can provide data isolation and protection by using resource access control based on RAM and the additional control capabilities specific to these products. This section only describes the typical permission control mechanisms of products. For more information, see the sections for corresponding products.

8.3.2.1. Computing and network environment isolation

Users can implement the isolation of their cloud data processing environment by using ECS security groups, VPC, and Cloud Firewall.

A security group is a virtual firewall provided by Alibaba Cloud for ECS instances. It provides Stateful Packet Inspection (SPI) and packet filtering functions, and can be used to isolate security domains. By configuring security group rules, you can control public or private network access from ECS instances in a security group.

Based on tunneling technology, Virtual Private Cloud (VPC) can help build an isolated virtual network environment. The intranet communication within a VPC is completely isolated from other users and other VPCs even under the same account.

Alibaba Cloud Firewall is the industry's first firewall as a service (FWaaS) solution targeted for public clouds. It centrally manages control policies for the access traffic from the Internet to ECS instances (Internet traffic), and provides micro-isolation policies for the access traffic between ECS instances (intranet traffic). By default, Cloud Firewall can also store network traffic and security event logs and firewall operation logs for six months.

8.3.2.2. RAM

Alibaba Cloud provides RAM to manage user identities and control resource access permissions. RAM authorization can be specific to an API action or resource ID. RAM can be used to define fine-grained authorizations at an API operation or resource ID level. RAM also supports various restrictive conditions on permission granting, such as constraints on source IP address, required SSL/TLS channel, access time period, and MFA.

With RAM and its functions, such as RAM users, RAM roles, user groups, resource groups, and resource tags, you can use policies to control the access of an operation principle, such as a user, user group, or RAM role, to a specific resource. In a policy, you can specify whether to allow or deny specific operations on specific resources under specific conditions in order to implement the resource isolation of the data.

8.3.2.3. OSS access control

OSS provides multiple methods to control the access to objects stored in buckets, including ACLs, RAM policies, and bucket policies.

- ACLs: ACLs are resource-based authorization polices. You can specify access permissions for buckets and objects in ACLs. You can specify ACLs for a bucket or an object when you create the bucket or upload the object. You can also modify these ACLs at any time after you create the bucket or upload the object.
- RAM policies: RAM is a service that allows you to control access to resources. RAM policies are user-based authorization policies. With RAM polices, you can manage user identities and control their access to different resources. For example, you can grant a user read-only access to only one bucket.
- Bucket policies: Bucket policies are resource-based authorization policies. Compared with RAM policies, bucket policies can be configured directly in the OSS console. You can authorize users to access your bucket even when you do not have permissions for RAM operations. With bucket policies, you can grant permissions to RAM user accounts that are owned by other Alibaba Cloud accounts. You can control anonymous user access to resources from specified IP addresses or IP segments.

8.3.2.4. RDS access control

Database account

After you create an ApsaraDB for RDS instance, the instance does not provide any initial database accounts. You can create a standard database account and grant database-level read and write permissions in the ApsaraDB for RDS console or by calling the API. If you want to control more fine-grained permissions, such as permissions on tables, views, and fields, you can create a privileged Premier Account in the ApsaraDB for RDS console or by calling the API. Then, you can use a database client and the premier account to create standard accounts. You can also use the premier account to grant table-level read and write permissions to standard accounts.

IP address whitelist

By default, the IP address whitelist for an ApsaraDB for RDS instance is set to 127.0.0.1 to block connections from all IP addresses. You can go to the data security module in the ApsaraDB for RDS console or call the API to modify the IP address whitelist. You do not need to restart the ApsaraDB for RDS instance after you modify the IP address whitelist. Therefore, changes to the IP address whitelist do not interrupt your business. You can set multiple groups in the IP address whitelist. Each group can contain up to 1,000 IP addresses or IP address ranges. You can also enable the enhanced whitelist feature to specify the network type (classic or VPC network) when you create an IP whitelist group.

8.3.2.5. MaxCompute access control

The multi-tenancy feature of MaxCompute is based on projects. A project is the basic unit for data management and computing, and the main measure for metering and billing. After a user creates a project, the user become the project owner. All objects that are created in the project, such as tables, instances, resources, and user-defined functions (UDFs), belong to the owner. Only the owner and users authorized by the owner can access objects in this project.

Before authorizing a user, the project owner must add the user to the project. Only users in a project can be authorized.

A role is a collection of access permissions. A role can be used to assign the same permissions to a group of users. Role-based authorization can simplify the authorization process and reduce authorization management overhead. To authorize users, you can choose to grant roles instead of granting permissions to users.

MaxCompute can grant different permissions to users or roles in the project. Users can have different access permissions for different objects, such as tables (please note views require separate authorization), functions, resources, and task instances. At the same time, MaxCompute supports column-level labeling, namely Label Security, for fine-grained access control.

Authorization mechanism

- MaxCompute provides ACLs for authorizing users or roles. Authorization by using ACLs is based on objects. Permission data authorized by using ACLs is considered to be a type of sub-resource of the object. Authorization by using ACLs can be performed only when the object already exists. If the object is deleted, the permission data authorized by using the ACLs is automatically deleted.
- MaxCompute supports the authorization of users or roles through the access control list (ACL) authorization mechanism. ACL authorization is an object-based authorization. An access control list is regarded as a sub-resource of an object. ACL authorization can be performed only when the object exists. When the object is deleted, the access control list is automatically deleted.
- The MaxCompute permission model supports ACL access control at field (i.e. column) level. In other words, a field is also one of the objects supported by the ACL. Similar to a table, a field is an independent object that contains complete authorization information, such as the validity period. Example:
- MaxCompute supports security access control policies based on labels. After data and users are labeled with security levels, the Label Security feature applies the following default security policies:
    - No-ReadUp: A user is not allowed to read data with a sensitivity level higher than the user level unless the user is explicitly authorized.
    - Trusted-User: Trusted users are allowed to write data of all sensitivity levels. The default sensitivity level of new data is 0 (unclassified).
- MaxCompute defines authorization permissions for administration-related operations. For example, users with the CreatePackage permission can create packages and users with the AddPackageResource permission can add resources to the package. Customers can use MaxCompute policies to authorize administrative operations.

Sandbox isolation

MaxCompute runs all computational tasks in isolated sandboxes. The sandboxes are structured in multiple layers, from the Kernel-based Virtual Machine (KVM) layer to the kernel layer. System sandboxes are combined with an authentication mechanism to ensure data security and prevent server failures caused by human errors and malicious operations.

8.3.3. Data masking

Alibaba Cloud SDDP provides nearly 30 built-in masking algorithms in six categories including hash, encryption, masking, replacement, shuffling, and transformation, and supports user-defined masking algorithms or parameters. SDDP ensures that data is masked without changing the original data distribution and the corresponding business system logic, and ensures the validity and availability of the data. Users can protect their data while accomplishing business needs at a low cost with high efficiency.

Alibaba Cloud DataWorks provides the Data Security Guard feature, which provides a data masking algorithm and MaxCompute calls the algorithm to generate the masked data. In addition, MaxCompute can be connected to various masking applications and integrate with the associated masking algorithms for data computation and output of desensitized content.

8.4. Data exchange security

The value of data can be achieved through data exchange and sharing. The security requirements for data exchange can be partially implemented through the access control of cloud products and data masking of sensitive data protection products, as described in 8.3. Data processing security. Data exchange security also depends on the data loss prevention capability.

8.4.1. Data loss prevention

User data loss prevention involves the complete control over permissions on data and the monitoring and detection of data in use. To prevent data loss, users must first implement effective control over the permissions on storage and transmission products on the cloud. SDDP supports instant query of data, users, and permissions, and provides centralized query capabilities for all applicable permissions on data, and can resolve the mappings between Alibaba Cloud account permissions and relevant roles. SDDP can generate alerts for data permission configuration and usage exceptions that do not comply with security best practices in the cloud environment.

It is also necessary to have comprehensive monitoring and detection capabilities in place during data transmission and processing, and to discover possible abnormal behaviors during data use in a timely manner. SDDP can effectively monitor exceptions that occur during the data transmission process, display the data flow lifecycle dynamically, and ensure compliant and orderly export and transmission of data. Based on log analysis, SDDP can effectively identify manual operations and API calls. Based on machine learning and big data analysis capabilities, SDDP can monitor and generate alerts for abnormal behaviors that arise during various data flows and operations.

Finally, after data loss is discovered and alerts are generated, SDDP analyzes suspicious events for subsequent data loss handling processes. The event analysis feature centrally collects various types of alert events, and uses time series analysis to reconstruct the behavior baseline of responsible parties and display the historical baseline trajectory in real time, effectively improving analysis efficiency. SDDP can handle tenant events in isolation and feedback the handling results to the machine learning model, which makes anomaly detection more accurate.

The data loss prevention function of each product can also be used to prevent the leakage of sensitive data. For example, in DataWorks, users can configure risk identification rules to identify risks in daily access and use AI to automatically identify data risks. The identified data-at-risk is displayed on the data risks page and the data-at-risk can be audited. Similar functions in cloud products such as Log Service and Database Audit can also be used to perform regulation-defined auditing of relevant data usage.

8.5. Data storage security

8.5.1. Encryption at rest

Data storage security is mainly guaranteed by encryption at rest. Alibaba Cloud allows users to encrypt data stored at rest in Alibaba Cloud services with integration of Alibaba Cloud Key Management Service (KMS). Alibaba Cloud supports the Advanced Encryption Standard with 256-bit key length (AES256) for encrypting sensitive data at rest.

Data encryption is enabled in different Alibaba Cloud services. For more information, see the corresponding section for each service in the rest of the white paper.

- EBS: encrypts block storage devices (cloud disks) used inside VMs to ensure that data is securely stored in a distributed system, and uses service managed keys and customer managed keys as CMKs to encrypt data.
- OSS: supports both server-side and client-side storage and encryption. In server-side encryption, OSS uses service managed keys and customer managed keys as CMKs to encrypt data. In client-side encryption, OSS allows users to use on-premises self-managed keys or CMKs generated in Alibaba Cloud KMS to encrypt data on the client side.
- ApsaraDB for RDS: Multiple versions of ApsaraDB for RDS provide Transparent Data Encryption (TDE) or DB instance disk encryption mechanism. RDS uses service managed keys and customer managed keys as CMKs to encrypt data.
- Table Store: uses service managed keys or customer managed keys as CMKs to encrypt data.
- NAS: uses service managed keys as CMKs to encrypt data.
- MaxCompute: uses service managed keys as CMKs to encrypt data.

More additional services support encryption at rest and can use service managed keys or customer managed keys as CMKs to encrypt data. For more information, see the official website of each cloud service at www.alibabacloud.com.

8.5.2. Customer managed keys

The storage encryption function of cloud products supports using the key managed by the cloud products themselves as the CMK. Specifically, when you use the data encryption function of a cloud product for the first time in a region, the service system automatically creates a CMK in KMS for you to use the service. This key is used as a service-managed key and its lifecycle is managed by the cloud product. Specifically, you can query the CMK in the KMS console. However, you cannot delete it.

Although the keys managed by a cloud product can help users achieve basic data protection capabilities, users with clear requirements may need more fine-grained key management. The KMS keys auto-generated by cloud products when encryption is enabled for the first time don’t allow users to independently manage the key lifecycle, set automatic rotation, or change the protection level that is provided by the key.

Therefore, in cloud products that support the function, you can create or upload CMKs to KMS, and directly manage the lifecycle of the keys. When you create a CMK in KMS, it is referred to as a customer managed key. When you upload a key which you have generated yourself to KMS, it is often referred to as a customer supplied key or BYOK (Bring Your Own Key). With the authorization in RAM, these keys can also be used for the data encryption of cloud products, and provide users with additional security capabilities:

- You can disable or enable keys to control the data encryption and decryption capabilities of cloud products.
- You can configure policies to control the data encryption and decryption capabilities of cloud products.
- You can import keys into KMS to further enhance key lifecycle management and control the data encryption and decryption capabilities of cloud products.

User managed and supplied CMKs are a user's assets. Cloud products must be authorized by the user through RAM before they can be used to encrypt and decrypt data. You can also cancel the corresponding CMK authorization at any time to control data encryption and decryption. Note that when using these CMKs and the preceding security capabilities, you need to take into account your own responsibilities for the management of key authorization and lifecycle.

8.5.3. Managed HSM

Alibaba Cloud KMS allows users to manage their master keys in HSMs, which use a hardware mechanism to protect the plaintext of keys from ever leaving the security boundaries the HSM. When users use HSM-managed keys for cryptographic operations, the operations occur only in HSM to ensure the confidentiality of keys. Based on the management capabilities built into KMS and the key protection provided by an HSM, KMS meets the needs for high security with low management overhead.

8.6. Data destruction security

8.6.1. Physical destruction

Alibaba Cloud has established a security management system for the full lifecycle of devices, including reception, storage, placement, maintenance, transfer, and reuse or decommissioning. Access control and operation monitoring of devices are managed strictly, and maintenance and stocktaking of devices are conducted on a regular basis. When any device is recycled or decommissioned, Alibaba Cloud takes data erasure measures for the storage media. Prior to disposal of data assets, it is necessary to check whether the media containing sensitive data and genuine licensed software has been overwritten, degaussed, or physically destroyed to make sure that the data cannot be restored. When certain hard copy materials are no longer needed due to business or legal reasons, Alibaba Cloud physically destroys them or obtains proof of destruction from any third party data processors, to ensure that the data cannot be reconstructed.

8.6.2. Data erasure

Data erasure is an extension of storage virtualization. After an ECS instance is released, its original disk space and memory space are reliably scrubbed to ensure user data security.

8.6.3. Data clearing after service termination

On terminating a customer’s services, Alibaba Cloud deletes the customer’ data assets in a timely manner or returns the data assets according to relevant agreements. Alibaba Cloud uses data erasure techniques that meet industry standards. The erasure operations are logged to prevent unauthorized access to customer data.

9. Release history

February 2021: International Edition – Version 2.1 was released. The security mechanisms regarding storage device management and data erasure is supplemented in Section 5.1.1.4 and 5.1.1.5.

March 2020: International Edition – Version 2.0 was released. A comprehensive Alibaba Cloud security architecture was redefined. A cloud data security system section was added. Comprehensive product descriptions were updated.

April 2018: International Edition - Version 1.0 was released.