Alibaba Cloud Security Whitepaper

Version: 2.0
2017.01

MORE THAN JUST CLOUD | Alibaba Cloud

Table of Contents

OVERVIEW

Established in September 2009, Alibaba Cloud was initially designed to handle the data management needs resulting from the large scale of transactions and data on Alibaba Group's online platforms. Today, Alibaba Cloud is one of the world's leading cloud computing service providers, and the leading cloud computing service provider in China, providing services for innovative enterprises and organizations around the world. We are dedicated to providing stable and reliable computing and data processing, serving the public interest, and providing continuous new energy to build an interconnected world. Our datacenters currently operate in mainland China (North China, East China and South China), Hong Kong, Australia, Germany, Japan, Singapore, the United States of America (East Coast and West Coast) and the United Arab Emirates.

Alibaba Cloud is also dedicated to providing cloud computing infrastructure for small and medium-sized enterprises, developers and business partners to provide ease of access to cloud computing and a diverse suite of related services. We have solutions for customers in various industries, including E-Commerce, Finance, Gaming, Medical Services, Mobile Applications and Services, Multimedia, Internet of Things (IoT) and Online to Offline (O2O).

PRODUCTS AND SERVICES

Alibaba Cloud offers a suite of cloud products and services, including but not limited to Elastic Compute Service ("ECS"), Virtual Private Cloud ("VPC"), Server Load Balancer ("SLB"), Relationship Database System ("RDS"), Object Storage Service ("OSS"), and Key Management Service ("KMS") to meet a wide range of business needs.

CONTROL ENVIRONMENT

Alibaba Cloud is supported by different business departments that form our organizational structure. Each of the departments has its own responsibilities, such as product design and engineering, security, architecture, marketing, business development, technical support, service operations and training. We also work with partners around the world.

We have established policies and procedures for governance and risk management, information security management, IT operations, etc. and are accessible through internal websites. We also

provide learning and awareness training for all employees including company culture, vision, customer service, career development and teamwork. Professional training offered by internal and external experts are also available to employees.

RISK ASSESSMENT

Alibaba Cloud has established a risk management framework to identify, analyze and manage risks within the company and those related to services provided. The risk management framework involves management and various teams, and covers strategic and operational risks, such as security and availability. Our comprehensive risk management system is created in accordance with the ISO27001:2013 Standard, which requires an information security risk assessment to be carried out annually. In addition, a risk rating for changes based on potential impact and likelihood of occurrence is also performed to ensure more additional resources and control measures are dedicated to higher risks. We conduct information security risk assessment at least once a year, and update our security policies according to the assessment results.

INFORMATION AND COMMUNICATION

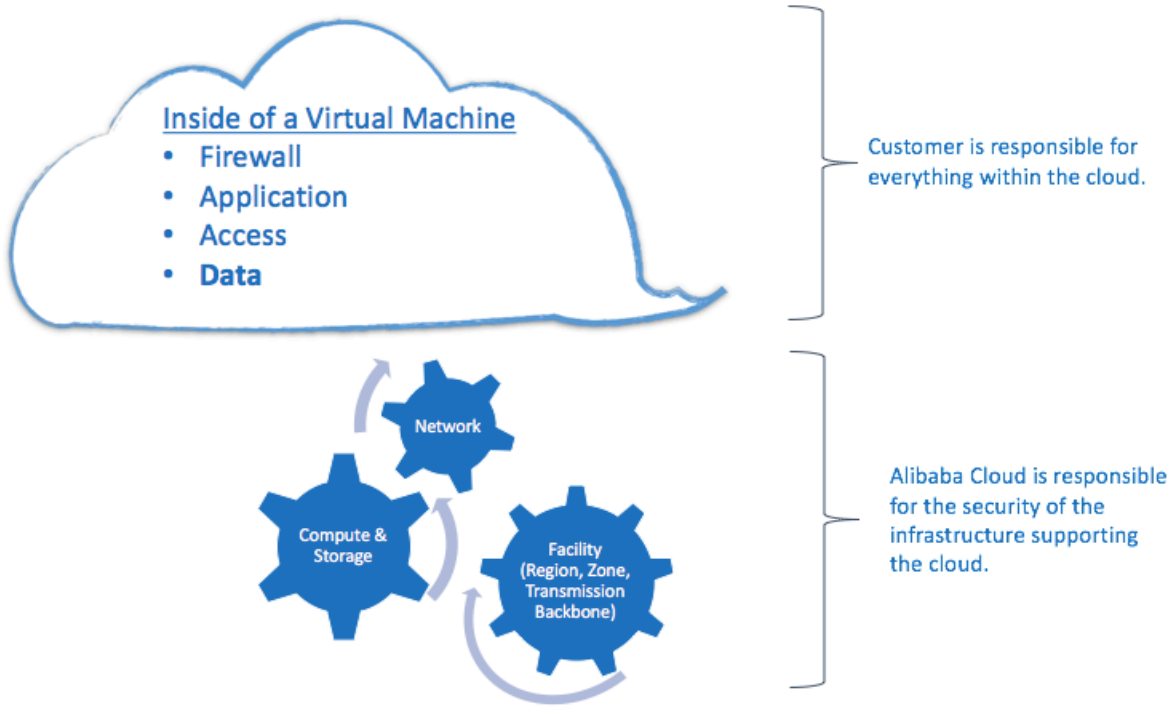
Alibaba Cloud has established communication channels to ensure effective communication between our employees and our customers. Internally, meetings such as project progress and review, reports and technical seminars are held frequently. New and updated policies are communicated on a timely basis. Externally, Alibaba Cloud has delineated responsibilities and obligations of customers and Alibaba Cloud in relevant membership agreements, product terms of use and other agreements under which we provide our services, and which include service levels, confidentiality and data disclosure provisions. We communicate our privacy policy to customers, providers and other third parties through our official international website (intl.aliyun.com). Customers can also report problems through telephone hotline, management console, email etc. Reported problems are handled by the respective account manager, after-sales, technical support and cloud service team. We also offer training and support to assist customers setting up their cloud applications.

CONTROL ACTIVITIES AND PROCESSES

Shared Responsibility Model

Base on the cloud service model, a delineation of responsibilities exists between the customer and the cloud service provider. Proper controls should be implemented by both parties in order to provide a “multilayer” approach to data protection.

For an IaaS deployment, Alibaba Cloud maintains security of the infrastructure that supports the cloud, and the customer is responsible for ensuring the security of the cloud resources and applications which the customer uses.



Alibaba Cloud secures, manages and operates the infrastructure, including datacenters deployed across regions and zones and Alibaba’s backbone transmission network, computing and storage equipment, network devices, Apsara distributed cloud operating system, and various cloud services and products based on the operating system.

Customers should evaluate their own controls on a regular basis in order to determine if appropriate controls, processes and procedures are in place, such as implementing access controls to prevent unauthorized access to their content.

Physical Security

Access Controls

Alibaba Cloud has established access management processes, including an access card system and fingerprint access control system. Visitor access to a datacenter and/or server room areas must be requested and approved prior to the visit. An official identification document (ID) must be presented and validated at the front desk during registration. Visitors must be accompanied by an on-site operator during the visit to the server room areas. Datacenter managers perform a monthly review of the access card system and fingerprint access control system to ensure that only authorized personnel are granted access.

Environmental Controls

Dual power supply is required at our datacenters, and a hot standby system is implemented for network devices. A temperature monitoring system is in place to monitor the temperature of servers in the datacenters. If any exception occurs, an alert is triggered automatically by the temperature monitoring system to notify on-site operators for action. On-site operators perform daily inspection and maintenance of IT equipment, with documented inspection and maintenance results.

Decommissioning

Data storage media that are discarded or damaged must be demagnetized and bent for data removal before being removed from a datacenter. To ensure data security, our agreements with hardware providers require that no storage media be returned to them.

Security Monitoring

Datacenter facility management is responsible for monitoring the intercom and emergency communication systems, smoke detectors, lightning protection and grounding devices, fire alarms and sprinkler systems, power supply, electrical circuit system and control panels, ventilation and air conditioning systems, etc. In addition, personnel on duty monitor the operation of datacenters 24x7. Video surveillance is also installed at the entrance, equipment delivery areas and dedicated areas within the datacenters. Security personnel at datacenters perform inspections to ensure safe operation of datacenters.

Alibaba Cloud maintains the risk inventory of each datacenter, and communicates the risk inventory to the corresponding risk manager. The risk manager conducts risk assessment and periodic contingency drill testing, and requires suppliers to issue an improvement plan for any operational risks.

Logical Security

Access Provisioning

Alibaba Cloud has policies and procedures established for logical access management of employee access rights.

Operation personnel manage cloud products or services through the operations platform. Access is granted with role-based access controls (RBAC) and following the rule of the least privileges necessary for the operations platform. Controls are in place to ensure segregation of duties and access rights. Alibaba Cloud enforces two-factor authentication to authenticate users of the operations platform.

Upon employment termination, the Human Resource system automatically synchronizes users' termination information with other systems, and terminates accounts in the operation platform and infrastructure.

Customer Authentication and Access Management:

The Management Console is a control center for customers to manage and control cloud resource. When a customer registers a cloud account, the system automatically checks the uniqueness of the user name selected. When a customer subsequently logs into the Management Console, identity authentication information is transmitted via HTTPS protocol. Customers can centrally manage cloud services and data via our Open API.

Network Security

A network configuration scanning tool is deployed to scan network device configurations within the network security domains on a daily basis. Our security team follows up on the scan results, and documents the results together with any action items. Network device configuration is backed up to ensure timely recovery of network device configurations if needed.

DDoS Protection:

Alibaba Cloud Anti-DDoS automatically detects and prevents various types of attacks including those at the application level and volumetric attacks. It also supports two-way protection to prevent cloud resources from being abused for attacks.

Data Transmission

Alibaba Cloud supports secure communication channels with strong cryptographic protocols for data transmission. Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS) is deployed in the Management Console and Open API gateway of Alibaba Cloud. Alibaba Cloud also offers

Alibaba Cloud Security Certificate Service by which tenants can purchase and deploy digital certificates directly through Alibaba Cloud's platform in order to replace Hyper Text Transfer Protocol (HTTP) with HTTPS to implement transmission encryption. We also support IPSec VPN and leased line connections. Tenants can apply for IPSec VPN or leased line connections by submitting tickets in order to access the cloud environment for service management and data transmission, and to establish secure communication channels.

Key Management Service

Alibaba Cloud offers Key Management Service ("KMS") for customers. Customers are granted full control over key management and are able to use keys generated by KMS to encrypt/decrypt data on the Alibaba Cloud platform.

Product Security Features:

1) ECS:

Alibaba Cloud ECS supports two kinds of hypervisors - Xen and KVM ("Hypervisor"), which achieve CPU hardware segregation -- in the virtualization layer, segregation of memory, as well as differentiation of virtual machine hard disks is achieved through Hypervisor. Our security team tracks vulnerabilities in the virtualization platform where any exceptions are reported for review.

Network traffic of different ECS instances is isolated. We enforce controls over the communication mode for data exchange, to ensure an ECS instance cannot access or be commingled with network traffic of other instances.

Customers are able to manage network access controls for single or multiple ECS instances via the use of security groups. In creating an ECS instance, customers are required to select a security group; ECS instances in different security groups cannot communicate with each other by default. Customers are able to enforce access controls among ECS instances in different security groups by configuring group rules.

2) RDS:

Customer isolation relies on the instance isolation mechanism of the database. Security protections are deployed on database servers to prohibit customers from loading dynamic link libraries to execute commands in the host operating systems, for the purpose of preventing unauthorized access to other customer database instances running in the same host. Intranet connection mode is set up for RDS where customers can set up IP whitelists for RDS to prevent unauthorized access.

3) OSS:

Data files are uploaded into OSS buckets as objects. Tenants can create one or more buckets for storage and add one or more objects into each bucket. Tenants can share and download objects by use of the link of uploaded files. OSS provides bucket-based and object-based access controls for tenants. Only authorized tenants can operate buckets and objects.

When a tenant creates a new bucket, OSS will automatically set up the access control type as “private” for the bucket, if not specified otherwise. Objects in a bucket inherit the authority of its container by default.

4) SLB:

ECS resources in the same region can be virtualized as an application service pool with high performance and high availability by setting up virtual IP addresses in SLB. Access requests from clients are distributed into the pool according to the configuration of applications. SLB hides IP addresses of back-end servers, and only reveals virtual IP addresses externally in order to achieve unified load balancing and access controls.

5) VPC:

Only instances bound with elastic IP ("EIP") can access the Internet. ECS instances of different tenants are located in different VPCs. Different VPCs are isolated internally and can only be accessed from one another by use of the IP addresses mapped externally.

Change Management

Alibaba Cloud has established policies for change control and configuration management. A change control system is utilized to initiate and approve change requests. The applicant is required to specify change type, risk level, risk description, change reason, change plan, rollback plan, and validation method in the application form. Changes must pass quality tests prior to migration into the production environment, with testing results documented. New equipment must pass environment tests, server pressure tests and delivery inspection prior to deployment. Additional approval from management must be obtained prior to migration of emergency changes.

System changes that affect Alibaba Cloud and customer responsibilities are communicated to customers through announcements on Alibaba Cloud's official international website.

Configuration Management

Alibaba Cloud has established configuration baseline standards that specify baseline requirements for physical servers, operating systems, database management systems, network

devices and virtual images. Configuration baseline standards are reviewed and updated at least annually. In addition, a configuration detection system is deployed to scan system components. Deviations from standard configurations defined in the baseline documents are detected and automatically restored to the standard by the configuration detection system.

Development

Alibaba Cloud has established security development standards, including a variety of code and interface development standards, which cover applications and programming interface design, development, deployment and testing processes. Applications and programming interfaces must pass security assessment and code scanning prior to migration into the production environment. Development of new products must also be authorized.

Business Continuity & Operational Resilience

Alibaba Cloud has established business continuity plans. The business continuity management team performs business impact analysis and risk assessment, reviews and updates business continuity plans, as well as conducts business continuity drills every year.

The business impact analysis and risk assessment includes identification of critical business processes, maximum tolerable downtime, recovery time objective, minimum service levels and time needed to resume service. Threats that may trigger disruptions to Alibaba Cloud's business and resources are identified and documented, and corresponding strategies are designed according to different scenarios of cloud products and services. A business continuity drill covers data backup and recovery testing procedures and is updated when there are changes to products, services and the organizational environment.

Incident Management

Threat and Vulnerability Management

The Alibaba Cloud vulnerability management team is responsible for identifying, tracing, finding and fixing security vulnerabilities. We utilize a vulnerability scoring system to categorize and prioritize vulnerability fixing. Alibaba Cloud also keeps contact with members of security research communities and reviews reports about external vulnerabilities.

Security Incidents

Alibaba Cloud has established a security event management platform for security event reporting, status and notifications. In addition to security events, significant cloud failures will also be managed through this platform. Our security team will record and manage the events in order of

priority by severity, with events that directly impact customers assigned the highest priority. Post-event analysis and review is performed to prevent reoccurrence of similar events.

Alibaba Cloud notifies customers, media and the public of security incidents through the Alibaba Cloud's international website and other forums.

ONGOING REVIEW AND MONITORING ACTIVITIES

Alibaba Cloud carries out comprehensive assessment of information security management on an annual basis, including a review of information security policies, standards and requirements. Our legal and compliance departments monitor the legal, statutory and regulatory compliance obligations to ensure the company is aware of applicable compliance requirements in a timely manner.

Alibaba Cloud has applied guidance from the COBIT (Control Objectives for Information and Related Technologies) framework to build our internal control framework. Our internal audit team also performs inspection and evaluation of control activities periodically. Audit results are reported directly to the management for review and remediation. In addition, Alibaba Cloud engages external certification organizations to conduct audits of information security certificates and to assess our controls and processes.

Compliance

We adopt industry standards and best practices to safeguard customer data. We have received multiple industry standard certifications and regularly complete third party audits. Our certifications include:

- ISO/IEC 20000:2011 certificate for Information Technology Service Management System
- ISO/IEC 27001:2013 certificate for Information Security Management System
- ISO 22301:2012 certificate for Business Continuity Management System
- Cloud Security Alliance's Security Trust and Assurance Registry ("CSA STAR")
- Level III Information Security Technology – Testing and Evaluation for Classified Protection of Information System
- Trusted Cloud Certification by Datacenter Alliance of Information Center of Ministry of Industry and Information Technology ("IC-MIIT")
- Cloud Assessment recognized by China National Accreditation Service for Conformity Assessment ("CNAS")

- Singapore Multi-Tier Cloud Security (MTCS) standard Level 3
- Payment Card Industry Data Security Standard (PCI-DSS)
- Service Organization Control (SOC) Reports
- Compliant with Motion Picture Association of America (MPAA) Content Security Best Practice
- Provision of Business Associate Agreements (BAA) to assist customers in complying with the Health Insurance Portability and Accountability Act (HIPAA)

For additional information, please visit us at Alibaba Cloud Trust Center https://intl.aliyun.com/trust-center

Privacy

At Alibaba Cloud, we are committed to protecting the personal data of our customers around the world. We comply with applicable law in the markets in which we operate our business.

Our Privacy Policy can be find on our website, and any inquiry and privacy related questions can be submitted through our online Trust Center portal.

Transparency

Similar to other large internet companies around the world, at times Alibaba Cloud is required by law to provide records to government authorities during an investigation or in the course of litigation. We have established procedures to support litigation, court orders, discovery and other legal matters that may require disclosure of data. Each request is carefully reviewed and analyzed by our legal teams to ensure the validity of the request with consideration on means to minimize disclosure of personal data.

SUMMARY

At Alibaba Cloud, we strive for high standards and quality in our products and services, we are committed to providing stable, reliable, secure, and compliant cloud computing infrastructure services. For additional compliance information, please visit us at Alibaba Cloud Trust Center https://intl.aliyun.com/trust-center. To learn more about our cloud and services, please visit us at https://intl.aliyun.com, or get in touch with our Business Advisors.