

# Alibaba Cloud Object Storage Service

Security white paper

Issue: 20190912

## Legal disclaimer

---

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

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








or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the 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 names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.



## Generic conventions

Table -1: Style conventions

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

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand   slave}</code>



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
1 Security white paper.....	1



# 1 Security white paper

---

This topic describes how to secure data in OSS by using the security features provided by OSS, such as encryption, access control, logging, monitoring, and data protection.

## Encryption

The following encryption methods are available in OSS: server-side encryption, client-side encryption, and transmission encryption.

- Server-side encryption

OSS protects static data by encrypting it on the server side. This method is suitable for scenarios that require additional security or compliance for object storage. Examples of the scenarios include storage of deep learning samples and online collaborative documents.



Note:

For more information about the principle of server-side encryption, see [#unique\\_4/unique\\_4\\_Connect\\_42\\_section\\_c24\\_wbd\\_5gb](#).

OSS allows you to implement server-side encryption in any of the following methods:

- SSE-KMS: Customer master keys (CMKs) are hosted by OSS.

When sending a request to upload an object or modify the metadata of an object, you can include the `X - OSS - server - side - encryption` header in the request and specify its value as KMS without a specified CMK ID. In this method, OSS generates an individual key to encrypt each object by using the default managed CMK, and automatically decrypts the object when it is downloaded.

- SSE-KMS BYOK: This encryption method allows you to use bring your own key (BYOK).

OSS supports using BYOK material for encryption. When sending a request to upload an object or modify the metadata of an object, you can include the `X - OSS - server - side - encryption` header in the request, specify its value as KMS, and specify the value of `X - oss - server - side - encryption - key - id` to a specified CMK ID. In this method, OSS generates an individual key to encrypt each object by using the specified CMK, and adds the CMK ID

used to encrypt an object into the metadata of the object so that the object is automatically decrypted when it is downloaded by an authorized user

- SSE-OSS: This encryption method is fully hosted by OSS.

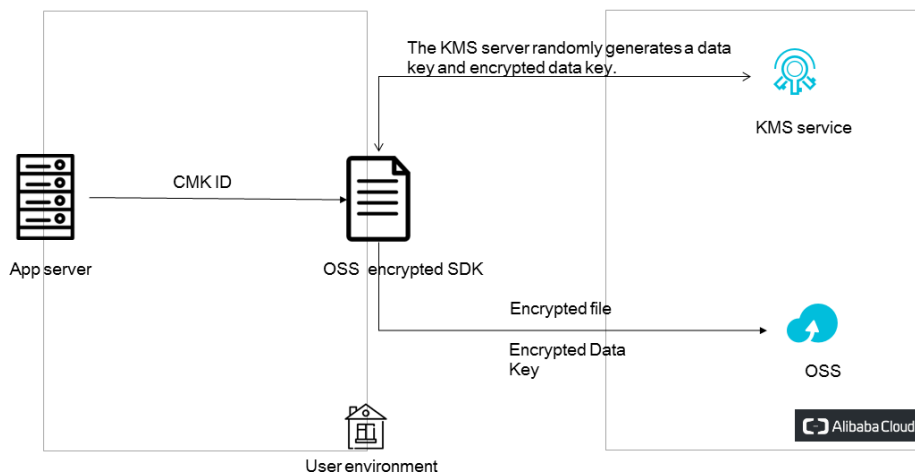
This encryption method is an attribute of objects. In this mode, OSS server-side encryption uses AES256 to encrypt objects with different data keys. AES256 uses master keys that are regularly rotated to encrypt data keys.

- Client-side encryption

Client-side encryption encrypts files on the client before they are uploaded to OSS. You can use either of the following methods to implement client-side encryption:

- Use CMKs hosted on KMS

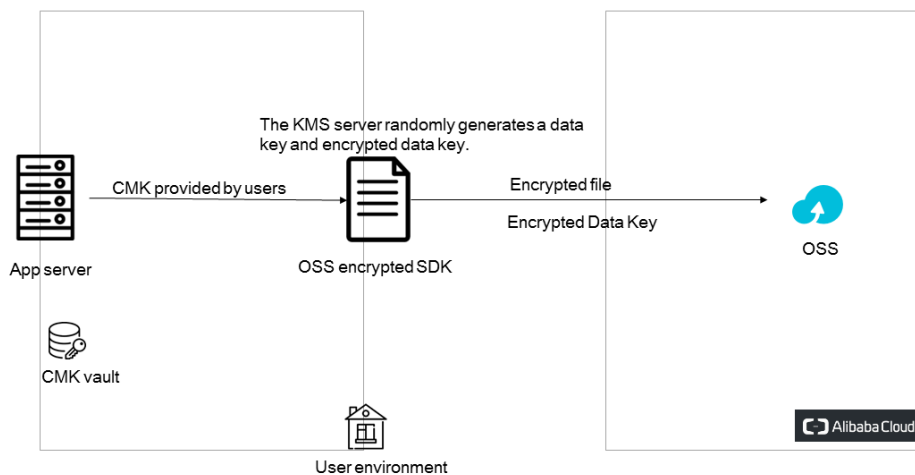
Encrypt files on the client using a CMK hosted on KMS. When using KMS, you need only to specify the CMK ID. You do not need to provide additional data keys. The following flow chart shows the encryption process in detail.



- Manually manage data keys

BYOK allows you to generate and manage data keys using your own tools. When you implement client-side encryption, you can upload your symmetric or

asymmetric key to the client. The following flow chart shows the encryption process in detail.



- **Transmission encryption**

OSS allows you to access resources in OSS over HTTP or HTTPS. You can set bucket-based authorization policies to only allow access to resources in OSS over HTTPS. Transport Layer Security (TLS) is a cryptographic protocol that provides end-to-end communications security over networks.

#### Access control

OSS has a variety of methods to control access to resources, such as ACL, RAM, and bucket-based authorization policies.

- **ACL:** OSS provides Access Control List (ACL) for access control. An ACL is set based on resources. You can set ACLs for buckets or objects. You can set an ACL for a bucket when you create the bucket or for an object when you upload the object to OSS. You can also modify the ACL for a created bucket or an uploaded object at anytime.
- **RAM Policy:** Resource Access Management (RAM) is a service provided by Alibaba Cloud for resource access control. RAM policies are configured based on users. By configuring RAM policies, you can manage multiple users in a centralized manner and control the resources that can be accessed by the users. For example, you can control the permission of a user so that the user can only read a specified bucket. A RAM user belongs to the Alibaba Cloud account under which it was

created, and does not own any actual resources. That is, all resources belong to the corresponding Alibaba Cloud account.

- **Bucket Policy:** Bucket policies are configured based on resources. Compared with RAM policies, bucket policies can be directly configured on the graphical console. By configuring bucket policies, you can authorize users to access your bucket even you do not have permissions for RAM operations. By configuring bucket policies, you can grant access permissions to RAM users under other Alibaba Cloud accounts, and to anonymous users who access your resources from specified IP addresses or IP ranges.

## Logs and monitoring

OSS can store and query logs, allowing you to gain insight into resource access. Additionally, OSS provides the monitoring service to allow you to gain insights into the running status of OSS, perform diagnostics, and troubleshoot problems.

- Query access logs

A large number of logs are generated when OSS resources are accessed. After you enable and configure logging for a bucket, an object with a specified prefix is generated on an hourly basis to record access logs of the bucket. You can use Alibaba Cloud Data Lake Analytics or build a Spark cluster to analyze these access logs. You can also configure lifecycle management rules for the log object to convert its storage class to Archive. This way, the log can be retained for a long time. For more information about OSS access logs, see [#unique\\_8](#).

- Query logs in real time

Real-time log query integrates OSS with Log Service. This feature allows you to query and collect statistics on OSS access logs, audit access to OSS, track exception events, and troubleshoot problems in the OSS console. This way, you can improve efficiency at work and make better decisions based on logs. For more information about real-time log query, see [#unique\\_9](#).

- Monitoring

The monitoring service of OSS provides metrics that describe basic system operating statuses, performance, and metering. The monitoring service also provides a custom alert service to help you track requests, analyze usage, collect statistics on business trends, and promptly discover and diagnose system problems. For more information about the monitoring service, see [#unique\\_10](#).

## Data protection

OSS provides the compliance retention policy, zone-redundant storage, and versioning to guarantee data security of OSS.

- Compliance retention policy

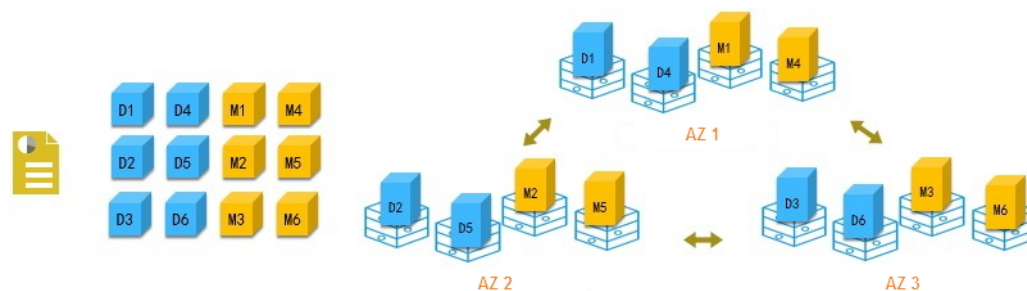
The Write Once Read Many strategy is supported in OSS. This feature prevents objects from being deleted or overwritten for a specified period of time.

OSS provides strong compliant policies. You can configure time-based compliant retention policies for buckets. After a compliant retention policy is locked, you can read objects from or upload objects to buckets. However, no one can delete the protected objects or compliant retention policies within the retention period. You can delete objects only after their retention period ends. The WORM strategy is suitable for industries such as the financing, insurance, health care, and security. OSS allows you to build a "compliant bucket in the cloud."

For more information about the compliance retention policy, see [#unique\\_11](#).

- Zone-redundant storage

OSS uses the multi-zone mechanism to distribute user data across three zones within the same region. If one zone becomes unavailable, the data will still be accessible. OSS zone-redundant storage provides durability of 99.999999999% (twelve 9's) and a guaranteed data availability of 99.95% in the SLA.



The redundant storage mechanism provides OSS with the disaster recovery capability in 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 and data loss, ensuring that the failover process is not perceived by users. With the disaster recovery capability, OSS can meet the strict

requirement that the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of key services must be 0.

For more information about zone-redundant storage, see [#unique\\_12](#).

- Versioning

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



Note:

Versioning will be available soon.

Versioning applies to all objects in buckets. After you enable versioning for a bucket, all objects in the bucket are subject to versioning. Each version has a unique version ID.

Fees are incurred when previous versions are generated for overwritten objects. You can configure lifecycle rules to automatically delete expired versions.