阿里云
对象存储

白皮书

文档版本：20190921

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

法律声明.....I
通用约定.....I
1 安全白皮书..... 1

1 安全白皮书

本文介绍如何通过对象存储OSS提供的加密、访问控制、日志与监控及数据保护等多种方式来保障OSS的数据安全性。

加密

OSS提供服务器端加密、客户端加密以及数据传输加密三种数据加密方式。

- 服务器端加密

  OSS通过服务器端加密机制，提供静态数据保护。适合于对于文件存储有高安全性或者合规性要求的应用场景。例如，深度学习样本文件的存储、在线协作类文档数据的存储。

  > 说明:
  > 有关服务器端加密原理的更多信息，请参考原理介绍。

  针对不同的应用场景，OSS有如下三种服务器端加密方式：

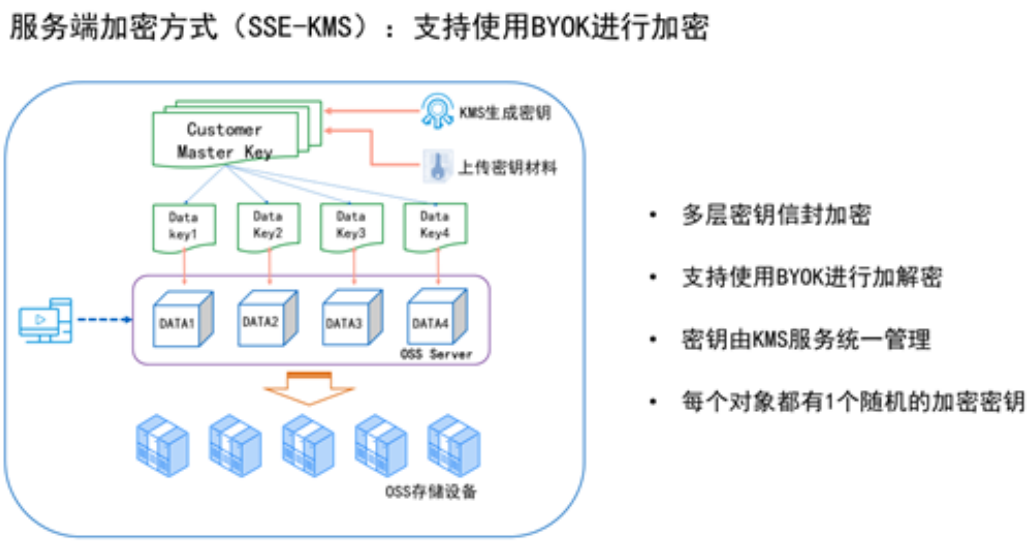
  - 使用OSS默认托管的KMS密钥（SSE-KMS）

    您可以将Bucket默认的服务器端加密方式设置为KMS且不指定具体的CMK ID，也可以在上传Object或修改Object的meta信息时，在请求中携带`X-OSS-server-side-encryption`并指定其值为KMS且不指定具体的CMK ID。OSS将使用默认托管的CMK生成不同的密钥来加密不同的对象，并且在下载时自动解密。

  - 使用BYOK进行加密（SSE-KMS BYOK）

    服务器端加密支持使用BYOK进行加密，您可以将Bucket默认的服务器端加密方式设置为KMS并指定具体的CMK ID，也可以在上传Object或修改Object的meta信息时，在请求中携带`X-OSS-server-side-encryption`，指定其值为KMS，并指定`X-OSS-server-side-encryption-key-id`为具体的CMK ID。OSS将使用指定的CMK生成不同的密钥来

加密不同的对象，并将加密Object的CMK ID记录到对象的元数据中，因此具有解密权限的用户下载对象时会自动解密。



- 使用OSS完全托管加密（SSE-OSS）

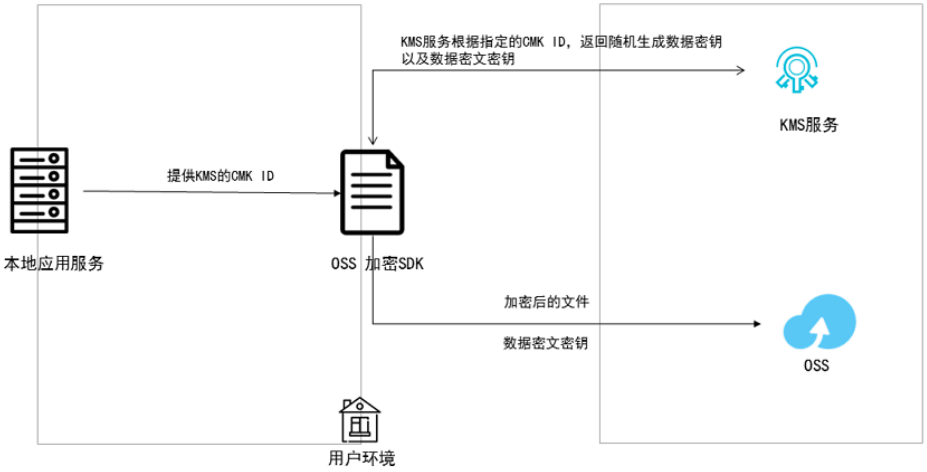
  基于OSS完全托管的加密方式，是Object的一种属性。OSS服务器端加密使用AES256加密每个对象，并为每个对象使用不同的密钥进行加密，作为额外的保护，它将使用定期轮转的主密钥对加密密钥本身进行加密。

- 客户端加密

  客户端加密是指将数据发送到OSS之前在用户本地进行加密，对于数据加密密钥的使用，目前支持如下两种方式：

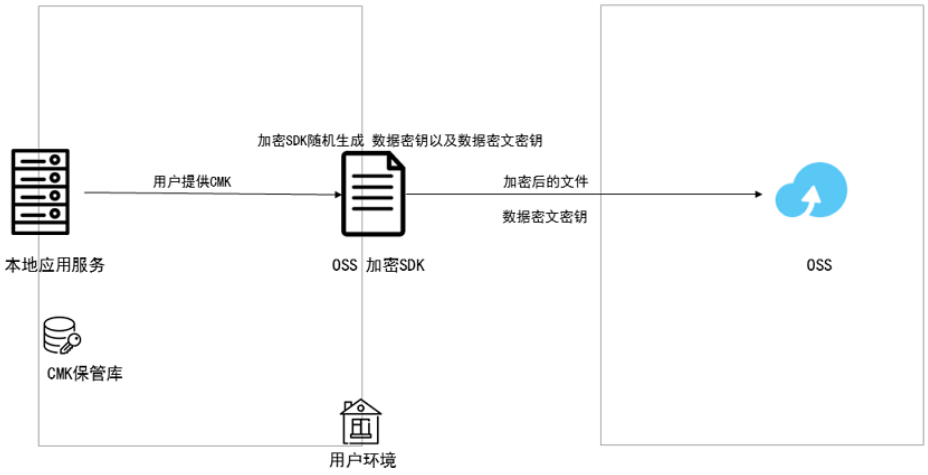
  - 使用KMS托管用户主密钥

    当使用KMS托管用户主密钥用于客户端数据加密时，无需向OSS加密客户端提供任何加密密钥。只需要在上传对象时指定KMS用户主密钥ID（也就是CMK ID）。其具体工作原理如下图所示。



  - 使用用户自主管理密钥

    使用用户自主管理密钥，需要用户自主生成并保管加密密钥。当用户本地客户端加密时，由用户自主上传加密密钥（对称加密密钥或者非对称加密密钥）至本地加密客户端。其具体加密过程如下图所示。



- 数据传输加密

  OSS支持通过HTTP或HTTPS的方式访问，但您可以在Bucket Policy中设置仅允许通过HTTPS (TLS)来访问OSS资源。安全传输层协议（TLS）用于在两个通信应用程序之间提供保密性和数据完整性。

访问控制

OSS提供了多种权限控制方式，包括ACL、RAM Policy和Bucket Policy。

- ACL：OSS 为权限控制提供访问控制列表（ACL）。ACL是基于资源的授权策略，可授予Bucket和Object访问权限。 您可以在创建Bucket或上传Object时设置ACL，也可以在创建Bucket或上传Object后的任意时间内修改ACL。
- RAM Policy：RAM （Resource Access Management）是阿里云提供的资源访问控制服务。RAM Policy是基于用户的授权策略。通过设置RAM Policy，您可以集中管理您的用户（比如员工、系统或应用程序），以及控制用户可以访问您名下哪些资源的权限。比如能够限制您的用户只拥有对某一个 Bucket 的读权限。子账号是从属于主账号的，并且这些账号下不能拥有实际的任何资源，所有资源都属于主账号。
- Bucket Policy：Bucket Policy是基于资源的授权策略。相比于RAM Policy，Bucket Policy操作简单，支持在控制台直接进行图形化配置，并且Bucket拥有者直接可以进行访问授权，无需具备RAM操作权限。Bucket Policy支持向其他账号的RAM用户授予访问权限，以及向匿名用户授予带特定IP条件限制的访问权限。

日志与监控

OSS提供访问日志存储及实时日志查询服务，便于您从多个维度来对日志进行细化跟踪。此外，OSS提供的监控服务，帮助您更好的了解OSS服务的运行状态并进行自主诊断和故障排除。

- 访问日志查询

  您在访问OSS的过程中，会产生大量的访问日志。日志存储功能，可将OSS的访问日志，以小时为单位，按照固定的命名规则，生成一个Object写入您指定的Bucket（目标 Bucket，Target Bucket）。您可以使用阿里云DataLakeAnalytics或搭建Spark集群等方式对这些日志文件进行分析。同时，您可以配置目标Bucket的生命周期管理规则，将这些日志文件转成归档存储，长期归档保存。有关OSS访问日志的更多信息，请参考#unique_8。

- 实时日志查询

  实时日志查询功能将OSS与日志服务（LOG）相结合， 允许您在OSS控制台直接查询OSS访问日志，帮助您完成OSS访问的操作审计、访问统计、异常事件回溯和问题定位等工作，提升您的工作效率并更好地帮助您基于数据进行决策。有关实时日志查询的更多信息，请参考#unique_9。

- 监控服务

  OSS监控服务为您提供系统基本运行状态、性能以及计量等方面的监控数据指标，并且提供自定义报警服务，帮助您跟踪请求、分析使用情况、统计业务趋势，及时发现以及诊断系统的相关问题。有关监控服务的更多信息，请参考#unique_10。

数据保护

OSS提供合规保留策略、同城冗余存储及版本控制等特性来保障OSS的数据安全性。

- 合规保留策略

  OSS现已全面支持WORM（一次写入，多次读取）特性，允许用户以“不可删除、不可篡改”方式保存和使用数据。

  OSS提供强合规策略，用户可针对存储空间（Bucket）设置基于时间的合规保留策略。当策略锁定后，用户可以在Bucket中上传和读取文件（Object），但是在Object的保留时间到期之前，任何用户都无法删除Object和策略。Object的保留时间到期后，才可以删除Object。OSS支持的WORM特性，适用于金融、保险、医疗、证券等行业。您可以基于OSS搭建“云上数据合规存储空间”。

  有关合规保留策略的更多信息，请参考合规保留策略。

- 同城冗余存储

  OSS采用多可用区（AZ）机制，将用户的数据分散存放在同一地域（Region）的3个可用区。当某个可用区不可用时，仍然能够保障数据的正常访问。OSS 同城冗余存储（多可用区）是基于99.9999999999% (12个9）的数据可靠性设计，并且能够提供 99.95%的数据可用性SLA 。

  OSS的同城冗余存储能够提供机房级容灾能力。当断网、断电或者发生灾难事件导致某个机房不可用时，仍然能够确保继续提供强一致性的服务能力，整个故障切换过程用户无感知，业务不中断、数据不丢失，可以满足关键业务系统对于“恢复时间目标（RTO）”以及“恢复点目标（RPO）”等于0的强需求。

  有关同城冗余存储的更多信息，请参考同城冗余存储。

- 版本控制

  开启存储空间（Bucket）版本控制特性后，针对数据的覆盖和删除操作将会以历史版本的形式保存下来。通过文件（Object）的版本管理，用户在错误覆盖或者删除Object后，能够将Bucket中存储的Object恢复至任意时刻的历史版本。

  > 说明:
  > 版本控制特性将在近期推出，敬请期待。

  版本控制应用于Bucket内的所有Object。当第一次针对Bucket开启版本控制后，该Bucket中所有的Object将在之后一直受到版本控制，并且每个版本都具有唯一的版本ID。

  Bucket开启版本控制后，针对文件的每次覆盖都会生成一个历史版本，并且针对每个版本进行收费。您可以通过lifecycle自动删除过期版本。