

密钥管理服务

用户指南（阿布扎比）

文档版本 02
发布日期 2021-06-03



版权所有 © 华为技术有限公司 2021。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 简介	1
1.1 概念	1
1.1.1 密钥管理服务	1
1.1.2 用户主密钥	1
1.1.3 默认主密钥	1
1.1.4 数据加密密钥	2
1.1.5 硬件安全模块	2
1.1.6 信封加密方式	2
1.1.7 真随机数生成器	2
1.2 使用场景	2
1.3 功能介绍	3
1.4 访问与使用	4
1.4.1 如何访问	4
1.4.2 如何使用	4
1.4.3 与其他云服务的关系	5
1.4.4 KMS 权限管理	6
2 管理	10
2.1 创建密钥	10
2.2 导入密钥	12
2.2.1 概述	12
2.2.2 导入密钥材料	13
2.2.3 删除密钥材料	18
2.3 计划删除密钥	19
2.4 在线工具加解密小数据	20
2.5 管理标签	22
2.5.1 添加标签	22
2.5.2 搜索标签	24
2.5.3 修改标签值	25
2.5.4 删除标签	25
2.6 管理密钥	26
2.6.1 查看密钥	26
2.6.2 修改密钥别名和描述	28
2.6.3 启用密钥	29

2.6.4 禁用密钥.....	30
2.6.5 取消删除密钥.....	30
2.7 权限管理.....	31
2.7.1 创建用户并授权使用 KMS.....	31
2.7.2 KMS 自定义策略.....	33
3 常见问题.....	35
3.1 什么是密钥管理服务?	35
3.2 什么是用户主密钥?	35
3.3 什么是数据加密密钥?	35
3.4 为什么不能马上删除用户主密钥?	35
3.5 哪些云服务使用 KMS 加密数据?	35
A 修订记录.....	36

1 简介

1.1 概念

1.1.1 密钥管理服务

密钥管理服务，即KMS（Key Management Service），是一种安全、可靠、简单易用的密钥托管服务，帮助用户集中管理密钥，保护密钥安全。

KMS通过使用硬件安全模块HSM（Hardware Security Module）保护密钥安全，帮助用户轻松创建和管理密钥，所有的用户密钥都由HSM中的根密钥保护，避免密钥泄露。KMS对密钥的所有操作都会进行访问控制及日志跟踪，提供所有密钥的使用记录，满足审计和合规性要求。

1.1.2 用户主密钥

用户主密钥，即CMK（Customer Master Key），是用户使用密钥管理服务创建的密钥，是一种密钥加密密钥，主要用于加密并保护数据加密密钥。一个用户主密钥可以加密多个数据加密密钥。

1.1.3 默认主密钥

默认主密钥，是对象存储服务（Object Storage Service，OBS）等其他云服务自动通过密钥管理服务为用户创建的用户主密钥，其别名后缀为“/default”。

默认主密钥可通过密钥管理服务界面进行查询，不支持禁用、计划删除操作。

表 1-1 默认主密钥列表

密钥别名	对应云服务
obs/default	对象存储服务
evs/default	云硬盘（Elastic Volume Service，EVS）
ims/default	镜像服务（Image Management Service，IMS）
sfs/default	弹性文件服务（Scalable File Service，SFS）

密钥别名	对应云服务
rds/default	关系型数据库（Relational Database Service, RDS）

说明

默认主密钥是在用户第一次通过对应云服务使用KMS加密时自动生成的。

1.1.4 数据加密密钥

数据加密密钥，即DEK（Data Encryption Key），是用户加密数据的加密密钥。

1.1.5 硬件安全模块

硬件安全模块，即HSM（Hardware Security Module），一种安全产生、存储、管理及使用密钥并提供加密处理服务的硬件设备。

1.1.6 信封加密方式

信封加密方式，是一种加密手段，将加密数据的数据密钥封入信封中存储、传递和使用，不再使用用户主密钥直接加解密数据。

1.1.7 真随机数生成器

真随机数生成器，即TRNG（True Random Number Generator），是一种通过物理过程而不是计算机程序来生成随机数字的设备，用以生成完全不可预测的随机数。

1.2 使用场景

密钥管理服务为对象存储（Object Storage Service, OBS）、云硬盘（Elastic Volume Service, EVS）、镜像服务（Image Management Service, IMS）、关系型数据库（Relational Database Service, RDS）和用户的应用程序提供用户主密钥管理控制能力，应用于数据加解密场景。

- 密钥管理服务与对象存储服务配合使用，应用于对象存储服务中对象的服务端加密场景。

说明

对象存储服务是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力，包括：创建、修改、删除桶，上传、下载、删除对象等。OBS适合存放任意类型的文件，适合普通用户、网站、企业和开发者使用。对象存储服务的更多信息请参见《对象存储服务用户指南》。

- 密钥管理服务与云硬盘配合使用，应用于云硬盘中的数据加密场景。

说明

云硬盘是一种基于分布式架构的、可弹性扩展的虚拟块存储设备。用户可在线进行操作，使用方式与传统服务器硬盘完全一致。同时，云硬盘具有更高的数据可靠性，更高的I/O吞吐能力和更加简单易用等特点，适用于文件系统、数据库或者其他需要块存储设备的系统软件或应用。云硬盘的更多信息请参见《云硬盘用户指南》。

- 密钥管理服务与镜像服务配合使用，应用于加密私有镜像的创建场景。

📖 说明

镜像服务提供简单方便的镜像自助管理功能。用户可以灵活便捷的使用公共镜像、私有镜像或共享镜像申请弹性云服务器。同时，用户还能通过已有的云服务器或使用外部镜像文件创建私有镜像。镜像服务的更多信息请参见《镜像服务用户指南》。

- 密钥管理服务与关系型数据库配合使用，应用于关系型数据库中数据库实例的磁盘加密场景。

📖 说明

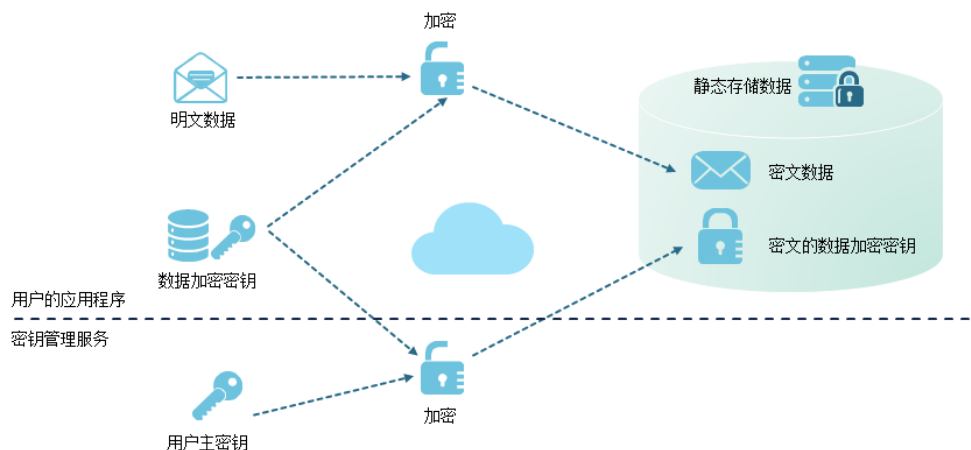
关系型数据库是一种基于云计算平台的即开即用、稳定可靠、弹性伸缩、便捷管理的在线关系型数据库服务。关系型数据库的更多信息请参见《关系型数据库用户指南》。

- 密钥管理服务与用户的应用程序配合使用。

用户的应用程序需要对明文数据进行加密时，可通过调用密钥管理服务的接口来产生数据加密密钥，再使用数据加密密钥将明文数据进行加密，得到密文并进行存储。同时，用户的应用程序可通过调用密钥管理服务的接口来创建对应用户主密钥，对数据加密密钥进行加密保护，并对密文的数据加密密钥进行存储。信封加密基本原理如图1-1所示。

为确保用户加密数据的安全，密钥管理服务不保存明文或密文的数据加密密钥，通过对用户主密钥的管理，以确保用户能安全获取和使用数据加密密钥。

图 1-1 信封加密基本原理



1.3 功能介绍

密钥管理服务提供如下功能：

- 管理用户主密钥
用户可通过密钥管理服务的界面或接口，对用户主密钥进行以下操作：
 - 创建、查询、启用、禁用、计划删除、取消删除用户主密钥
 - 导入密钥、删除密钥材料
 - 修改用户主密钥别名和描述
- 创建、加密、解密数据加密密钥
用户可通过密钥管理服务的接口对数据加密密钥进行创建、加密或解密操作，具体请参见《密钥管理服务接口参考》。


- 生成硬件真随机数
用户可通过密钥管理服务的接口生成512bit的随机数，为加密系统提供基于硬件真随机数的密钥材料和加密参数，具体请参见《密钥管理服务接口参考》。

1.4 访问与使用

1.4.1 如何访问

公有云提供了Web化的服务管理平台，即管理控制台管理方式和基于HTTPS请求的API（Application Programming Interface）管理方式。

- 管理控制台方式

如果用户已注册公有云，可直接登录管理控制台，单击管理控制台左上角的，选择区域或项目后，选择“安全 > 密钥管理服务”。

- API方式

用户可通过接口方式访问密钥管理服务，具体操作请参见《密钥管理服务接口参考》。

1.4.2 如何使用

与对象存储服务配合使用

对象存储服务支持普通方式和服务端加密方式上传和下载对象。当用户使用服务端加密方式上传对象时，数据会在服务端加密成密文后安全地存储在对象存储服务中；用户下载加密对象时，存储的密文会先在服务端解密为明文，再提供给用户。对象存储服务支持KMS托管密钥的服务端加密方式（即SSE-KMS加密方式），该加密方式是通过密钥管理服务提供密钥的方式进行服务端加密。

用户如何使用对象存储服务的SSE-KMS加密方式上传对象，具体操作请参见《对象存储服务用户指南》。

与云硬盘配合使用

在创建云硬盘时，用户启用云硬盘的加密功能，选择密钥管理服务提供的用户主密钥对云硬盘进行加密，则在使用该云硬盘时，存储到云硬盘的数据将会自动加密。

用户如何使用云硬盘加密功能，具体操作请参见《云硬盘用户指南》。

与镜像服务配合使用

用户通过外部镜像文件创建私有镜像时，可启用私有镜像加密功能，选择密钥管理服务提供的用户主密钥对镜像进行加密。

用户如何使用镜像服务的私有镜像加密功能，具体操作请参见《镜像服务用户指南》。

与弹性文件服务配合使用

用户通过弹性文件服务创建文件系统时，选择密钥管理服务提供的用户主密钥对文件系统进行加密，当使用该文件系统时，存储到文件系统的文件将会自动加密。

用户如何使用弹性文件服务的文件系统加密功能，具体操作请参见《弹性文件服务用户指南》。

与关系型数据库配合使用

在创建数据库实例时，用户启用数据库实例的磁盘加密功能，选择KMS提供的用户主密钥对数据库实例的磁盘进行加密，选择磁盘加密后会提高数据的安全性。

用户如何使用关系型数据库的磁盘加密功能，具体操作请参见《关系型数据库用户指南》。

与用户的应用程序配合使用

当用户的应用程序需要对明文数据进行加密时，可通过调用密钥管理服务的接口来产生数据加密密钥，再使用数据加密密钥将明文数据进行加密，得到密文并进行存储。同时，用户的应用程序调用密钥管理服务的接口创建对应用户主密钥，对数据加密密钥进行加密保护，得到密文的数据加密密钥并进行存储。具体操作请参见《密钥管理服务接口参考》。

1.4.3 与其他云服务的关系

与对象存储服务的关系

密钥管理服务为对象存储服务提供用户主密钥管理控制能力，应用于对象存储服务的服务端加密功能（SSE-KMS加密方式）。

与云硬盘的关系

密钥管理服务为云硬盘提供用户主密钥管理控制能力，应用于云硬盘的加密功能。

与镜像服务的关系

密钥管理服务为镜像服务提供用户主密钥管理控制能力，应用于镜像服务的私有镜像加密功能。

与弹性文件服务的关系

密钥管理服务为弹性文件服务提供用户主密钥管理控制能力，应用于弹性文件服务的文件系统加密功能。

与关系型数据库的关系

密钥管理服务为关系型数据库提供用户主密钥管理控制能力，应用于关系型数据库中数据库实例的磁盘加密功能。

与云审计服务的关系

云审计（Cloud Trace Service, CTS）记录密钥管理服务相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计用户指南》。

表 1-2 云审计服务支持的 KMS 操作列表

操作名称	资源类型	事件名称
创建密钥	cmk	createKey
创建数据密钥	cmk	createDataKey
创建不含明文数据密钥	cmk	createDataKeyWithoutPlaintext
启用密钥	cmk	enableKey
禁用密钥	cmk	disableKey
加密数据密钥	cmk	encryptDataKey
解密数据密钥	cmk	decryptDataKey
计划删除密钥	cmk	scheduleKeyDeletion
取消计划删除密钥	cmk	cancelKeyDeletion
创建随机数	rng	genRandom
修改密钥别名	cmk	updateKeyAlias
修改密钥描述	cmk	updateKeyDescription
密钥删除风险提示	cmk	deleteKeyRiskTips
导入密钥材料	cmk	importKeyMaterial
删除密钥材料	cmk	deleteImportedKeyMaterial
添加标签	cmk	createKeyTag
删除标签	cmk	deleteKeyTag
批量添加标签	cmk	batchCreateKeyTags
批量删除标签	cmk	batchDeleteKeyTags

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为密钥管理服务提供了权限管理的功能。需要拥有KMS Administrator权限的用户才能使用KMS服务。如需开通该权限，请联系拥有Security Administrator权限的用户，详细内容请参考《统一身份认证服务用户指南》。

1.4.4 KMS 权限管理

如果您需要对云服务平台上购买的KMS资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在c帐号中给员工创建IAM用户，并使用策略来控制他们对云服务资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有KMS的使用

权限，但是不希望他们拥有删除KMS等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用KMS，但是不允许删除KMS的权限策略，控制他们对华为云资源的使用范围。

如果系统帐号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用KMS的其它功能。

IAM是华为云云服务平台提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。关于IAM的详细介绍，请参见[IAM产品简介](#)。

KMS 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

KMS部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问KMS时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云服务平台各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对KMS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，权限的最小粒度为API授权项（action）。

如表1-3所示，包括了KMS的所有系统权限。

表 1-3 KMS 系统权限

系统角色/策略名称	描述	类别	依赖关系
KMS Administrator	数据加密服务加密密钥的管理员权限。	系统角色	无。
KMS CMKFullAccess	数据加密服务加密密钥所有权限。	系统策略	无。

表1-4列出了KMS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 1-4 常用操作与系统权限的关系

操作	KMS Administrator	KMS CMKFullAccess
创建密钥	√	√
启用密钥	√	√
禁用密钥	√	√
计划删除密钥	√	√
取消计划删除密钥	√	√
修改密钥别名	√	√
修改密钥描述	√	√
创建随机数	√	√
创建数据密钥	√	√
创建不含明文数据密钥	√	√
加密数据密钥	√	√
解密数据密钥	√	√
获取密钥导入参数	√	√
导入密钥材料	√	√
删除密钥材料	√	√
创建授权	√	√
撤销授权	√	√
退役授权	√	√
查询授权列表	√	√
查询可退役授权列表	√	√
加密数据	√	√
解密数据	√	√
开启密钥轮换	√	√
修改密钥轮换周期	√	√
关闭密钥轮换	√	√
查询密钥轮换状态	√	√
查询密钥实例	√	√
查询密钥标签	√	√
查询项目标签	√	√

操作	KMS Administrator	KMS CMKFullAccess
批量添加删除密钥标签	√	√
添加密钥标签	√	√
删除密钥标签	√	√
查询密钥列表	√	√
查询密钥信息	√	√
查询实例数	√	√
查询配额	√	√

相关链接

- [IAM产品简介](#)
- 创建用户组、用户并授予KMS权限
- 权限支持的授权项
- 系统默认提供两种权限策略：系统策略和自定义策略。系统策略是IAM预置的策略，用户只能使用不能修改。若系统策略不满足授权要求，用户可以创建自定义策略，自由搭配需要授予的权限集。
- 用户组配置权限策略后，将用户加入用户组中，可以使该用户获得权限策略中定义的操作权限。

2 管理

2.1 创建密钥

操作场景

该任务指导用户通过密钥管理服务界面创建用户主密钥。用户最多可创建100个用户主密钥，不包含默认主密钥。

用户主密钥可用于如下场景：

- 对象存储服务中对象的服务端加密
- 云硬盘中数据的加密
- 私有镜像的加密
- 弹性文件服务中文件系统的加密
- 关系型数据库中数据库实例的磁盘加密
- 用户应用程序的DEK加解密

说明


因为默认主密钥的别名后缀为“/default”，所以用户创建的密钥别名后缀不能为“/default”。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤4 单击页面右上角“创建密钥”，在弹出的窗口中，填写密钥的“别名”、“企业项目”与“描述”。

图 2-1 创建密钥

- 别名：待创建密钥的别名。
- （可选）描述：可根据自己的需要为用户主密钥添加描述。
- 企业项目：该参数针对企业用户使用。

如果您是 enterprise 用户，且已创建企业项目，则请从下拉列表中为密钥选择需要绑定的企业项目，默认项目为“default”。

未开通企业管理的用户页面则没有“企业项目”参数项，无需进行配置。

步骤5 （可选）用户可根据自己的需要为用户主密钥添加标签，输入“标签键”和“标签值”。

📖 说明

- 当用户在创建密钥时，没有为该用户主密钥添加标签。若用户需要为该用户主密钥添加标签，可单击该用户主密钥的别名，进入密钥详情页面，为该用户主密钥添加标签。
- 同一个用户主密钥下，一个标签键只能对应一个标签值；不同的用户主密钥下可以使用相同的标签键。
- 用户最多可以给单个用户主密钥添加20个标签。
- 当同时添加多个标签，需要删除其中一个待添加的标签时，可单击该标签所在行的“删除”，删除标签。

步骤6 单击“确定”，密钥创建完成。

用户可在密钥列表上查看已创建的密钥，密钥默认状态为“启用”。

----结束

相关操作

- 对象存储服务中对象的服务端加密方法，具体请参见《对象存储服务用户指南》的“使用服务端加密方式上传文件”章节。
- 云硬盘中数据加密方法，具体请参见《云硬盘用户指南》的“创建云硬盘”章节。

- 私有镜像的加密方法，具体请参见《镜像服务用户指南》的“加密镜像”章节。
- 弹性文件服务的文件系统加密方法，具体请参见《弹性文件服务用户指南》的“创建文件系统”章节。
- 关系型数据库中数据库实例的磁盘加密方法，具体请参见《关系型数据库用户指南》的“创建实例”章节。
- 创建DEK、不含明文的DEK方法，具体请参见《密钥管理服务接口参考》的“创建数据密钥”与“创建不含明文数据密钥”章节。
- 用户应用程序的DEK加解密方法，具体请参见《密钥管理服务接口参考》的“加密数据密钥”与“解密数据密钥”章节。

2.2 导入密钥

2.2.1 概述

用户主密钥包含密钥元数据（密钥ID、密钥别名、描述、密钥状态与创建日期）和用于加解密数据的密钥材料。

- 当用户使用KMS管理控制台创建用户主密钥时，KMS系统会自动为该用户主密钥生成密钥材料。
- 当用户希望使用自己的密钥材料时，可通过KMS管理控制台的导入密钥功能创建密钥材料为用户主密钥，并将自己的密钥材料导入该用户主密钥中。

注意事项

- 安全性
用户需要确保符合自己安全要求的随机源生成密钥材料。用户在使用导入密钥时，需要对自己密钥材料的安全性负责。请保存密钥材料的原始备份，以便在意外删除密钥材料时，能及时将备份的密钥材料重新导入KMS。
- 可用性与持久性
在将密钥材料导入KMS之前，用户需要确保密钥材料的可用性和持久性。
导入的密钥材料与通过KMS创建密钥时自动生成的密钥材料的区别，如表2-1所示。

表 2-1 导入的密钥材料与通过 KMS 创建密钥时自动生成的密钥材料的区别

密钥材料来源	区别
导入的密钥	<ul style="list-style-type: none">• 可以手动删除密钥材料，但不能删除该用户主密钥及其元数据。• 在导入密钥材料时，可以设置密钥材料失效时间，密钥材料失效后，KMS将在24小时以内自动删除密钥材料，但不会删除该用户主密钥及其元数据。 建议用户在本地密钥管理基础设施中安全地备份一份密钥材料，以便密钥材料失效或误删除时重新导入该密钥材料。
KMS创建的密钥	<ul style="list-style-type: none">• 不能手动删除密钥材料。• 不能设置密钥材料的失效时间。

- 关联性
当用户将密钥材料导入用户主密钥时，该用户主密钥与该密钥材料永久关联，不能将其他密钥材料导入该用户主密钥中。
- 唯一性
当用户使用导入的密钥加密数据时，加密后的数据必须使用加密时采用的用户主密钥（即用户主密钥的元数据及密钥材料与导入的密钥匹配）才能解密数据，否则解密会失败。

2.2.2 导入密钥材料

操作场景

当用户希望使用自己的密钥材料，而不是KMS生成的密钥材料时，可通过密钥管理服务界面将自己的密钥材料导入到KMS，由KMS统一管理。

该任务指导用户通过密钥管理服务界面导入密钥材料。

说明


- 导入的密钥与通过密钥管理服务创建的用户主密钥一样支持启用、禁用、计划删除和取消删除等操作。
- 用户仅能导入256位对称密钥。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已准备好待导入的密钥材料。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤4 单击页面右上角的“导入密钥”，弹出“导入密钥”对话框。

步骤5 在弹出的对话框中填写密钥的“别名”、“企业项目”与“描述”。

图 2-2 创建空密钥

导入密钥

1 创建密钥 — 2 获取包装密钥和导入令牌 — 3 导入密钥材料 — 4 导入密钥令牌

* 别名: KMS-ed42

企业项目: default

描述: 请输入密钥描述 (0/255)

标签: 标签键, 标签值

您还可以创建20个标签。

我已经了解导入密钥的安全性和持久性

取消 下一步

步骤6（可选）用户可根据自己的需要为用户主密钥添加标签，输入“标签键”和“标签值”。

说明

- 当用户在创建密钥时，没有为该用户主密钥添加标签。若用户需要为该用户主密钥添加标签，可单击该用户主密钥的别名，进入密钥详情页面，为该用户主密钥添加标签。
- 同一个用户主密钥下，一个标签键只能对应一个标签值；不同的用户主密钥下可以使用相同的标签键。
- 用户最多可以给单个用户主密钥添加20个标签。
- 当同时添加多个标签，需要删除其中一个待添加的标签时，可单击该标签所在行的“删除”，删除标签。

步骤7 单击“安全性与持久性”阅读并了解导入密钥的安全性和持久性。

步骤8 勾选“我已经了解导入密钥的安全性和持久性”，创建密钥材料为空的密钥。

步骤9 单击“下一步”，进入“获取包装密钥和导入令牌”页面。根据表2-2选择密钥包装算法。

图 2-3 获取包装密钥和导入令牌

导入密钥

1 创建密钥 — 2 获取包装密钥和导入令牌 — 3 导入密钥材料 — 4 导入密钥令牌

密钥ID: 72e2d1df-6bf4-4256-8fba-6172c6dff515

密钥包装算法: RSAES_OAEP_SHA_256

下载

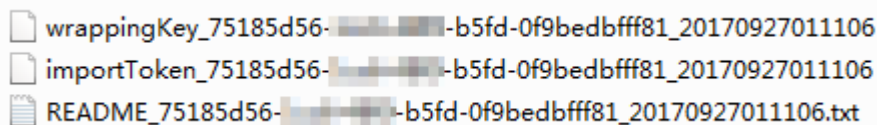
取消 下一步

表 2-2 密钥包装算法说明

密钥包装算法	说明	设置
RSAES_OAEP_SHA_256	具有“SHA-256”哈希函数的OAEP的RSA加密算法。	请用户根据自己的HSM功能选择加密算法。 1. 如果您的HSM支持“RSAES_OAEP_SHA_256”加密算法，推荐使用“RSAES_OAEP_SHA_256”加密密钥材料。 2. 如果您的HSM不支持“OAEP”选项，用户可以使用“RSAES_PKCS1_V1_5”加密密钥材料。 须知 “RSAES_OAEP_SHA_1”加密算法已经不再安全，请谨慎选择。
RSAES_PKCS1_V1_5	PKCS#1 v1.5版本的RSA加密算法。	
RSAES_OAEP_SHA_1	具有“SHA-1”哈希函数的OAEP的RSA加密算法。	

步骤10 单击“下载”，下载的文件包含包装密钥、导入令牌和说明文件，如图2-4所示。

图 2-4 下载文件



- wrappingKey_密钥ID_下载时间: 即包装密钥，用于加密密钥材料的包装密钥。
- importToken_密钥ID_下载时间: 即导入令牌，KMS导入密钥材料时需要使用。
- README_密钥ID_下载时间: 即说明文件，记录包装密钥序列号、密钥包装算法、包装密钥文件名称、令牌文件名称以及包装密钥和令牌的过期时间。

须知

包装密钥和导入令牌将在24小时后失效，失效后将不能使用。如果包装密钥和导入令牌失效，请重新下载包装密钥和导入令牌。

同时，用户也可以通过调用API接口的方式获取包装密钥和导入令牌。

1. 调用“get-parameters-for-import”接口，获取包装密钥和导入令牌。
 如下以获取密钥ID为“43f1ffd7-18fb-4568-9575-602e009b7ee8”，加密算法为“RSAES_PKCS1_V1_5”的包装密钥和导入令牌为例。
 “public_key”：调用API接口返回的base64编码的包装密钥内容。
 “import_token”：调用API接口返回的base64编码的导入令牌内容。

– 请求样例

```
{
  "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
  "wrapping_algorithm": "RSAES_PKCS1_V1_5"
}
```

- 响应样例

```
{
  "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
  "public_key": "public key base64 encoded data",
  "import_token": "import token base64 encoded data",
  "expiration_time": 1501578672
}
```

2. 保存包装密钥，包装密钥需要按照以下步骤转换格式。使用转换格式后的包装密钥进行加密的密钥材料才能成功导入管理控制台。
 - a. 复制包装密钥“public_key”的内容，粘贴到“.txt”文件中，并保存为“PublicKey.b64”。
 - b. 使用OpenSSL，执行以下命令，对“PublicKey.b64”文件内容进行base64转码，生成二进制数据，并将转码后的文件保存为“PublicKey.bin”。


```
openssl enc -d -base64 -A -in PublicKey.b64 -out PublicKey.bin
```
3. 保存导入令牌，复制导入令牌“import_token”的内容，粘贴到“.txt”文件中，并保存为“ImportToken.b64”。

步骤11 使用下载的“包装密钥”对待导入的密钥材料进行加密。

- 方法一：使用下载的包装密钥在自己的HSM中加密密钥材料，详细信息请参考您的HSM操作指南。
- 方法二：采用OpenSSL加密密钥材料。

 **说明**

若用户需要使用openssl pkeyutl命令，OpenSSL需要是1.0.2及以上版本。

如下以使用下载的包装密钥，加密生成的密钥材料（256位对称密钥）为例说明，操作步骤如下所示：

- a. 执行以下命令，生成密钥材料（256位对称密钥），并将生成的密钥材料以“PlaintextKeyMaterial.bin”命名保存。

```
openssl rand -out PlaintextKeyMaterial.bin 32
```

- b. 使用下载的包装密钥加密密钥材料，并将加密后的密钥材料按“EncryptedKeyMaterial.bin”命名保存。

以下命令中的**PublicKey.bin**参数请以**步骤10**下载的包装密钥名称 *wrappingKey_密钥ID_下载时间* 进行替换。

表 2-3 使用下载的包装密钥加密生成的密钥材料

包装密钥算法	加密生成的密钥材料
RSAES_OAEP_SHA_256	<pre>openssl pkeyutl -in PlaintextKeyMaterial.bin -inkey PublicKey.bin -out EncryptedKeyMaterial.bin -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256</pre>

包装密钥算法	加密生成的密钥材料
RSAES_PKCS1_V1_5	<code>openssl rsautl -encrypt -in PlaintextKeyMaterial.bin -pkcs -inkey PublicKey.bin -keyform der -pubin -out EncryptedKeyMaterial.bin</code>
RSAES_OAEP_SHA_1	<code>openssl pkeyutl -in PlaintextKeyMaterial.bin -inkey PublicKey.bin -out EncryptedKeyMaterial.bin -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha1</code>

步骤12 单击“下一步”，进入“导入密钥材料”页面。根据表2-4配置参数。

图 2-5 导入密钥材料

表 2-4 导入密钥材料参数说明

参数	操作说明
密钥ID	创建密钥时，随机生成的密钥ID。
密钥材料	1. 选择使用步骤10下载的“包装密钥”加密的密钥材料。 2. 单击“导入”，导入密钥材料。

步骤13 单击“下一步”，进入“导入密钥令牌”页面。根据表2-5设置参数。

图 2-6 导入密钥令牌

表 2-5 导入密钥令牌参数说明

参数	操作说明
密钥ID	创建密钥时，随机生成的密钥ID。
密钥导入令牌	选择 步骤10 “下载”的导入令牌。
密钥材料失效模式	<ul style="list-style-type: none">永不过期：导入的密钥材料永久不过期。失效时间：用户可指定导入的密钥材料的失效时间，默认失效时间为24小时。 密钥材料失效后，密钥管理服务会在24小时内自动删除密钥材料，删除后密钥将无法使用，且密钥状态变更为“等待导入”。

步骤14 单击“确定”，完成导入密钥。

须知

密钥ID、导入的密钥材料和导入的令牌需要全部匹配，密钥材料才能导入成功，否则会导入失败。

用户可在密钥列表中查看到导入的密钥信息，导入密钥的默认状态为“启用”。

----结束

2.2.3 删除密钥材料

操作场景

当用户导入密钥材料时，可以指定密钥材料的失效时间。当密钥材料失效后，KMS将删除密钥材料，用户主密钥的状态变为“等待导入”。用户也可以根据需求手动删除密钥材料。等待密钥材料到期失效与手动删除密钥材料所达到的效果是一样的。

该任务指导用户通过密钥管理服务界面对外部导入的密钥材料进行删除操作。

说明

- 删除密钥材料后，若需要重新导入密钥材料，导入的密钥材料必须与删除的密钥材料完全相同，才能导入成功。
- 用户重新导入相同的密钥材料后，该用户主密钥可以解密删除密钥材料前加密的所有数据。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 用户已导入密钥材料。
- “密钥材料来源”为“外部”。
- 密钥“状态”为“启用”或“禁用”。

操作步骤

步骤1 登录管理控制台。

步骤2 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤3 在需要删除的密钥材料所在行，单击“删除密钥材料”。

步骤4 在弹出的对话框中单击“是”。

密钥材料删除后，密钥将无法使用，且当前密钥的状态切换为“等待导入”。

----结束

2.3 计划删除密钥

操作场景

该任务指导用户通过密钥管理服务界面对不再使用的用户主密钥进行有计划删除。

用户执行删除密钥操作后，密钥不会立即删除，密钥管理服务会将该操作按用户指定时间推迟执行，推迟时间范围为7天~1096天。在推迟删除时间未到时，若需要重新使用该密钥，可以执行取消删除密钥操作。若超过推迟时间，密钥将被KMS彻底删除，使用该密钥加密的数据将无法解密，请谨慎操作。

在删除密钥前，用户需要确保该密钥没有被使用或将来也不会被使用。

说明


默认主密钥为服务自动创建，不支持删除操作。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 待删除的密钥需处于“启用”、“禁用”或者“等待导入”状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤4 在需要删除的密钥所在行，单击“删除”。

图 2-7 删除单个密钥

<input type="checkbox"/>	别名 备注	状态	ID	创建时间 备注	操作
<input type="checkbox"/>	KMS-a975	● 启用	6aa54ba5-f790-47f1-91d7-f8e3f5ef4f28	2020/09/21 16:15:22 GMT+08:00	禁用 删除

步骤5 在弹出的窗口中，填写“推迟删除”的时间。

图 2-8 推迟删除时间



步骤6 单击“是”，完成删除单个密钥操作。

📖 说明

如果您需要批量删除密钥，勾选所有需要删除的密钥，然后在列表的左上角，单击“删除”。

----结束

2.4 在线工具加解密小数据

该任务指导用户通过密钥管理界面使用在线工具加解密不大于4KB的数据。

📖 说明

- 在线工具不支持通过默认主密钥加解密小数据。
- 用户可使用调用API接口的方式，使用默认主密钥加解密小数据，详细信息请参考《密钥管理服务接口参考》。

📖 说明

用户可直接单击“复制到剪切板”拷贝解密后的明文数据，并保存到本地文件中。

----结束

2.5 管理标签

2.5.1 添加标签

操作场景

标签用于标识用户主密钥。为用户主密钥添加标签，可以方便用户对用户主密钥进行分类和跟踪，并按标签汇总用户主密钥的使用情况。

须知

KMS不支持为默认主密钥添加标签。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤


- 步骤1** 登录管理控制台。
- 步骤2** 单击管理控制台左上角的，选择区域或项目。
- 步骤3** 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。
- 步骤4** 单击目标用户主密钥的别名，进入密钥详细信息页面。
- 步骤5** 单击“标签”，进入标签管理页面。

图 2-10 标签页面



- 步骤6** 单击“添加标签”，在弹出的“添加标签”对话框中输入“标签键”和“标签值”，参数说明如表2-6所示。

图 2-11 添加标签



说明

当同时添加多个标签，需要删除其中一个待添加的标签时，可单击该标签所在行的“删除”，删除标签。

表 2-6 标签参数说明

参数	参数说明	取值要求	样例
标签键	<p>标签的名称。</p> <p>同一个用户主密钥下，一个标签键只能对应一个标签值；不同的用户主密钥下可以使用相同的标签键。</p> <p>用户最多可以给单个用户主密钥添加20个标签。</p>	<ul style="list-style-type: none"> ● 必填。 ● 对于同一个用户主密钥，标签键唯一。 ● 长度不超过36个字符。 ● 只能包含以下4种字符： <ul style="list-style-type: none"> - 大写字母 - 小写字母 - 数字 - 特殊字符，包括“-”和“_” 	cost

参数	参数说明	取值要求	样例
标签值	标签的值。	<ul style="list-style-type: none">可以为空。长度不超过43个字符。只能包含以下4种字符：<ul style="list-style-type: none">大写字母小写字母数字特殊字符，包括“-”和“_”	100

步骤7 单击“确定”，完成标签的添加。

----结束

2.5.2 搜索标签

操作场景


该任务指导用户通过密钥管理服务搜索标签，可搜索当前项目下满足标签搜索条件的所有的用户主密钥。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已添加标签。

操作步骤

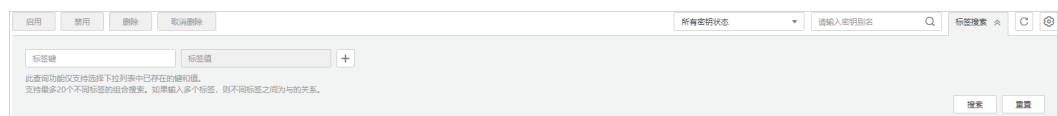
步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。


步骤3 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤4 单击“标签搜索”，展开搜索框。


图 2-12 标签搜索框



步骤5 在搜索框中输入“标签键”和“标签值”。

步骤6 单击，添加到搜索条件中，并单击“搜索”，显示满足搜索条件的用户主密钥列表。

说明

- 可添加多个标签进行组合搜索，最多支持20个不同标签的组合搜索，若进行多个标签组合搜索，则搜索结果的每个用户主密钥均满足标签组合搜索条件。
- 若需要在搜索条件中删除添加的标签，可在搜索条件中单击指定标签后的 ，删除添加的标签。
- 若需要重新添加搜索条件，可单击“重置”，重新添加搜索条件。

----结束

2.5.3 修改标签值

操作场景


该任务指导用户通过密钥管理服务修改标签值。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤4 单击目标用户主密钥的别名，进入密钥详细信息页面。

步骤5 单击“标签”，进入标签管理页面。

图 2-13 标签页面



步骤6 单击目标标签所在行的“编辑”，弹出编辑标签对话框。

步骤7 在弹出的编辑标签对话框中修改标签值，单击“确定”，完成标签值的修改。

----结束

2.5.4 删除标签

操作场景


该任务指导用户通过密钥管理服务删除标签。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤4 单击目标用户主密钥的别名，进入密钥详细信息页面。

步骤5 单击“标签”，进入标签管理页面。

图 2-14 标签页面



步骤6 单击目标标签所在行的“删除”，弹出删除标签对话框。

步骤7 在弹出的删除标签对话框中单击“是”，完成标签的删除。

----结束

2.6 管理密钥

2.6.1 查看密钥

操作场景


该任务指导用户通过密钥管理服务界面查看用户主密钥的信息，包括密钥别名、状态、ID和创建时间。密钥状态包括“启用”、“禁用”、“计划删除”和“等待导入”。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤1 登录管理控制台。



步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤4 在密钥列表中查看密钥信息。

图 2-15 密钥列表

说明

- 在“所有密钥状态”搜索栏选择密钥状态，“密钥列表”界面将只显示对应状态的密钥。
- 在密钥列表右上角的搜索框中输入密钥的别名，单击  或按“Enter”，可以搜索指定的密钥。
- 可单击“标签搜索”，搜索符合标签搜索条件的用户主密钥。
- 可单击密钥列表右上角的 ，设置密钥列表展示的列。

密钥列表参数说明，如表2-7所示。

表 2-7 密钥列表参数说明

参数	操作说明
别名	密钥的别名。
状态	密钥的状态，包含： <ul style="list-style-type: none">启用 密钥处于启用状态禁用 密钥处于禁用状态计划删除 密钥处于计划删除状态等待导入 如果密钥没有密钥材料，那么密钥的状态为“等待导入”。
ID	创建密钥时自动生成的密钥ID。
创建时间	创建该密钥的时间。
密钥材料失效时间	密钥材料失效的时间，密钥材料失效后，当前密钥为空密钥。
密钥材料来源	密钥材料的来源，包含： <ul style="list-style-type: none">外部 用户从外部导入到密钥管理服务。密钥管理服务 用户通过密钥管理服务创建。

步骤5 用户可单击密钥别名，查看密钥详细信息。

图 2-16 查看密钥详细信息



----结束

2.6.2 修改密钥别名和描述

操作场景

密钥别名就是用户主密钥的名称，用户可根据密钥的别名更快捷的查找到密钥。

该任务指导用户通过密钥管理服务界面更改用户主密钥的别名和描述。

须知


- 默认主密钥（密钥别名后缀为“/default”），别名和描述不可以修改。
- 密钥状态处于“计划删除”时，别名和描述不可修改。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 非默认主密钥的“状态”为“启动”、“禁用”或者“等待导入”。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的, 选择区域或项目。

步骤3 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤4 单击待更改密钥别名或描述信息的密钥的别名，进入密钥详细信息页面。



步骤5 单击该密钥的“别名”或“描述”所在行的, 修改密钥的别名或描述信息。

图 2-17 密钥详细信息



说明

- 别名由字母、数字或者特殊字符“:”、“/”、“_”、“-”组成，长度为1-255个字符。
- 描述信息长度不能超过255个字符。

步骤6 修改完成后，单击  保存修改。

---结束

2.6.3 启用密钥

操作场景


该任务指导用户通过密钥管理服务对单个或多个用户主密钥进行启用操作，使被禁用的密钥恢复到数据加解密能力。新建的用户主密钥默认为“启用”状态。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 待启用的密钥需处于“禁用”状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤4 在需要启用的密钥所在行，单击“启用”。

图 2-18 启用单个密钥

名称	状态	ID	创建时间	操作
<input type="checkbox"/> KMS-8515	等待导入	a048370f-a013-421f-944c-b59faa9093ef	2020/09/21 16:19:03 GMT+08:00	删除
<input type="checkbox"/> KMS-a975	禁用	6aa54ba5-f790-47f1-91d7-f8e3f5e4f28	2020/09/21 16:15:22 GMT+08:00	<input type="button" value="启用"/> 删除

步骤5 在弹出窗口中，单击“是”，完成启用单个密钥操作。

说明

如果您想批量启用密钥，可以勾选所有需要启用的密钥，然后在列表左上角，单击“启用”。

----结束

2.6.4 禁用密钥

操作场景

该任务指导用户通过界面对指定的用户主密钥进行禁用，以紧急保护数据。

用户主密钥被禁用后，用户将不能使用该密钥进行加解密任何数据。如果要使用该密钥进行加解密数据，用户需将该密钥重新启用，具体操作请参见[启用密钥](#)。

说明


默认主密钥为密钥管理服务自动创建，不支持禁用操作。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 待禁用的密钥需处于“启用”状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤4 在需要禁用的密钥所在行，单击“禁用”。

图 2-19 禁用单个密钥

名称	状态	ID	创建时间	操作
<input type="checkbox"/> KMS-8515	等待导入	a048370f-a013-421f-944c-b59faa9093ef	2020/09/21 16:19:03 GMT+08:00	删除
<input type="checkbox"/> KMS-a975	禁用	6aa54ba5-f790-47f1-91d7-f8e3f5e4f28	2020/09/21 16:15:22 GMT+08:00	<input type="button" value="禁用"/> 删除

----结束

2.6.5 取消删除密钥

操作场景


该任务指导用户未超出删除密钥的推迟时间，通过密钥管理服务界面对用户主密钥进行取消删除操作。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 待取消删除的密钥需处于“计划删除”状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 选择“安全 > 密钥管理服务”，进入密钥管理服务界面。

步骤4 在需要取消删除的密钥所在行，单击“取消删除”。

图 2-20 取消删除单个密钥

<input type="checkbox"/>	别名 <small>⌵</small>	状态	ID	创建时间 <small>⌵</small>	操作
<input type="checkbox"/>	KMS-8515	计划删除	a048370f-a013-421f-944c-b59faa9093ef	2020/09/21 16:19:03 GMT+08:00	取消删除
<input type="checkbox"/>	KMS-a975	启用	6aa54ba5-f790-47f1-91d7-f8e3f5ef4f28	2020/09/21 16:15:22 GMT+08:00	禁用 删除

步骤5 在弹出的窗口中，单击“是”，完成取消删除单个密钥操作。

说明

如果您想批量取消删除密钥，可以勾选所有需要取消删除的密钥，然后在列表左上角，单击“取消删除”。

---结束

2.7 权限管理

2.7.1 创建用户并授权使用 KMS

如果您需要对您所拥有的KMS进行精细的权限管理，您可以使用[统一身份认证服务](#)（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用DEW资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将KMS资源委托给更专业、高效的其他账号或者云服务，这些帐号或者云服务可以根据权限进行代运维。

如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用KMS服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如[图2-21](#)所示。

前提条件

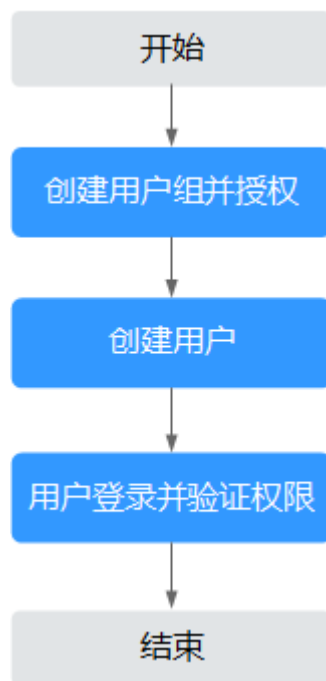
给用户组授权之前，请您了解用户组可以添加的KMS权限，并结合实际需求进行选择，KMS支持的系统权限如[表2-8](#)所示。若您需要对除KMS之外的其它服务授权，IAM支持服务的所有权限请参见[权限集](#)。

表 2-8 KMS 系统权限

系统角色/策略名称	描述	类别	依赖关系
KMS Administrator	数据加密服务加密密钥的管理员权限。	系统角色	无。
KMS CMKFullAccess	数据加密服务加密密钥所有权限。	系统策略	无。

示例流程

图 2-21 给用户授权 KMS 权限流程



1. **创建用户组并授权**

在IAM控制台创建用户组，并授予数据加密服务加密密钥所有权限“KMS CMKFullAccess”。

2. **创建用户并加入用户组**

在IAM控制台创建用户，并将其加入1中创建的用户组。

3. **用户登录并验证权限**

新创建的用户登录控制台，切换至授权区域，验证权限：

- 在“服务列表”中选择数据加密服务，进入KMS主界面，选择密钥对管理，若提示权限不足，表示“KMS CMKFullAccess”已生效。
- 在“服务列表”中选择除数据加密服务外的任一服务，若提示权限不足，表示“KMS CMKFullAccess”已生效。

2.7.2 KMS 自定义策略

如果系统预置的KMS权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见权限及授权项说明。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。

创建KMS自定义策略时：

- “云服务”：数据加密服务（KMS）。
- “操作”：根据您的需求进行选择。
- “选择资源（可选）”：“资源”选择“特定资源”，“KeyId”选择“通过资源路径指定”时，“路径”为创建密钥时生成的ID，可参考“查看密钥”章节获取ID。

- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：[创建自定义策略](#)。本章为您介绍常用的DEW自定义策略样例。

KMS 自定义策略样例

- 示例1：授权用户创建密钥

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:serverKMS:create"
      ]
    }
  ]
}
```

- 示例2：拒绝用户删除帐号密钥对

拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

如果您给用户授予“KMS Administrator”的系统策略，但不希望用户拥有“KMS Administrator”中定义的密钥对的删除权限（ecs:serverKeypairs:delete），您可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为Deny，然后同时将“KMS Administrator”和拒绝策略授予用户，根据Deny优先原则用户可以对密钥对执行除了删除外的所有操作。以下策略样例表示：拒绝用户删除密钥对。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ecs:serverKeypairs:delete"
      ]
    },
  ]
}
```

- 多个授权项策略

一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务。多个授权语句策略描述如下：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:serverKeypairs:create"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:cmk:*",
        "kms:dek:*",
        "kms:grant:*",
        "kms:tag:*"
      ]
    }
  ]
}
```

3 常见问题

3.1 什么是密钥管理服务？

密钥管理服务，即KMS（Key Management Service），是一种安全、可靠、简单易用的密钥托管服务，帮助用户集中管理密钥，保护密钥安全。

KMS通过使用硬件安全模块HSM（Hardware Security Module）保护密钥安全，帮助用户轻松创建和管理密钥，所有的用户密钥都由HSM中的根密钥保护，避免密钥泄露。KMS对密钥的所有操作都会进行访问控制及日志跟踪，提供所有密钥的使用记录，满足审计和合规性要求。

3.2 什么是用户主密钥？

用户主密钥，即CMK（Customer Master Key），是用户使用密钥管理服务创建的密钥，是一种密钥加密密钥，主要用于加密并保护数据加密密钥。一个用户主密钥可以加密多个数据加密密钥。

3.3 什么是数据加密密钥？

数据加密密钥是用于加密数据的密钥。

3.4 为什么不能马上删除用户主密钥？

删除密钥是一个需要非常谨慎的操作。操作前，用户需确保使用该密钥加密的相关数据都已完成迁移。因为密钥一旦被删除，所有使用该密钥加密的相关数据都无法解密。因此在删除密钥时，KMS会将该操作推迟7天到1096天执行，推迟时间由用户指定。超过推迟时间，密钥才会被真正删除。在密钥被真正删除之前，如果用户发现该密钥仍然有用，可取消删除操作。KMS通过这种方式来减少用户误操作所带来的损失。

3.5 哪些云服务使用 KMS 加密数据？

对象存储服务、云硬盘、镜像服务和关系型数据库借助KMS服务实现了加密特性。

A 修订记录

发布日期	修改说明
2021-06-03	第二次正式发布。 新增“KMS权限管理”章节。 新增“权限管理”章节。
2020-12-16	第一次正式发布。