天翼云·数据加密服务

用户使用指南

天翼云科技有限公司

目 录

1 产品介绍

1.1 什么是数据加密服务

数据加密服务

数据是企业的核心资产，每个企业都有自己的核心敏感数据。这些数据都需要被加密，从而保护它们不会被他人窃取。

数据加密服务（Data Encryption Workshop, DEW）是一个综合的云上数据加密服务。它提供密钥管理（KMS）、专属加密(DHSM)，安全可靠的为您解决数据安全、密钥安全、密钥管理复杂等问题。其密钥由硬件安全模块（Hardware Security Module，HSM） 保护，并与多个云服务集成。您也可以借此服务开发自己的加密应用。

表1-1 服务介绍

名称	定义
密钥管理服务 （Key Management Service, KMS）	密钥管理是一种安全、可靠、简单易用的密钥托管服务，帮助您轻松创建和管理密钥，保护密钥的安全。 KMS 通过使用硬件安全模块（Hardware Security Module，HSM）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。
专属加密 （Dedicated Hardware Security Module，Dedicated HSM）	专属加密是一种云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。 Dedicated HSM 为您提供经国家密码管理局检测认证的加密硬件，帮助您保护弹性云服务器上数据的安全性和完整性，满足监管合规要求。同时，用户能够对专属加密实例生成的密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。

概念介绍

本文解释了数据加密服务（Data Encryption Workshop, DEW）的基本概念，帮助您正确理解和使用 DEW。

表1-2 基本概念

名称	定义
硬件安全模块 （Hardware Security Module，HSM）	硬件安全模块是一种用于保护和管理强认证系统所使用的密钥同时提供相关密码学操作的计算机硬件设备。
用户主密钥 （Customer Master Key，CMK）	用户主密钥是用户或云服务通过密钥管理创建的密钥，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。
默认主密钥 （Default Master Key）	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为用户创建的用户主密钥，其别名后缀为“/default”。
密钥材料 （Key Material）	密钥材料是密码运算操作的重要输入之一，与密钥ID、基本元数据共同组成用户主密钥（Customer Master Key，CMK）。
信封加密 （Envelope Encryption）	信封加密是一种加密手段，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。
数据加密密钥 （Data Encrypt Key，DEK）	数据加密密钥是用于加密数据的密钥。
对称密钥加密	对称密钥加密又称专用密钥加密。信息的发送方和接收方使用相同密钥去加密和解密数据。 优点：加密和解密速度快。 缺点：每对密钥需保持唯一性，所以用户量大时密钥管理困难。 适用场景：加密大量数据。
非对称密钥加密	非对称密钥加密又称公开密钥加密。它需要使用一对密钥来分别完成加密和解密的操作，一个公开发布，即公开密钥，另一个由用户自己秘密保存，即私用密钥。 优点：加密和解密使用密钥不同，所以安全性高。 缺点：加密和解密速度较慢。 适用场景：对敏感信息加密。

1.2 密钥管理

1.2.1 功能特性

密钥管理，即密钥管理服务（Key Management Service, KMS），是一种安全、可靠、简单易用的密钥托管服务，帮助您轻松创建和管理密钥，保护密钥的安全。

KMS 通过使用硬件安全模块 HSM（Hardware Security Module, HSM）保护密钥的安全，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。

功能介绍

- 用户可通过密钥管理界面，对用户主密钥进行以下操作：
  - 创建、查看、启用、禁用、计划删除、取消删除用户主密钥
  - 修改用户主密钥的别名和描述
  - 在线工具加解密小数据
  - 导入密钥、删除密钥材料
  - 添加、搜索、编辑、删除标签
- 用户可通过密钥管理的接口执行以下操作：
  - 对数据加密密钥进行创建、加密或解密操作。
  - 对授予的权限进行退役授权操作

  具体请参见《数据加密服务接口参考》。
- 生成硬件真随机数

  用户可通过密钥管理的接口生成 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《数据加密服务接口参考》。

KMS 支持的密钥算法

KMS 创建的对称密钥使用的是 AES-256 加解密算法。KMS 创建的非对称密钥支持 RSA 和 ECC 算法。

表1-3 KMS 支持的密钥算法类型

密钥类型	算法类型	密钥规格	说明	用途
对称密钥	AES	AES_256	AES 对称密钥	小量数据的加解密或用于加解密数据密钥。
对称密钥	SM4	SM4	国密 SM4 对称密钥	小量数据的加解密或用于加解密数据密钥。

密钥类型	算法类型	密钥规格	说明	用途
非对称密钥	RSA	• RSA_2048 • RSA_3072 • RSA_4096	RSA 非对称密钥	小量数据的加解密或数字签名。
	ECC	• EC_P256 • EC_P384	椭圆曲线密码，使用 NIST 推荐的椭圆曲线	数字签名
非对称密钥	SM2	SM2	国密 SM2 非对称密钥	小量数据的加解密或数字签名。

通过外部导入的密钥支持的密钥包装加解密算法如表 1-4 所示。

表1-4 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。	请您根据自己的 HSM 功能选择加密算法。 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。 **须知** **“RSAES_OAEP_SHA_1”加密算法已经不再安全，请谨慎选择。**
RSAES_OAEP_SHA_1	具有“SHA-1”哈希函数的 OAEP 的 RSA 加密算法。	

1.2.2 产品优势

- 服务集成广泛

  与 OBS、EVS、IMS 等服务集成，用户可以通过 KMS 管理这些服务的密钥，还可以通过 KMS API 完成用户本地数据的加解密。

- 合规遵循

  密钥由经过安全认证的第三方硬件安全模块（HSM）产生，对密钥的所有操作都会进行访问控制及日志跟踪，符合国际法律合规的要求。

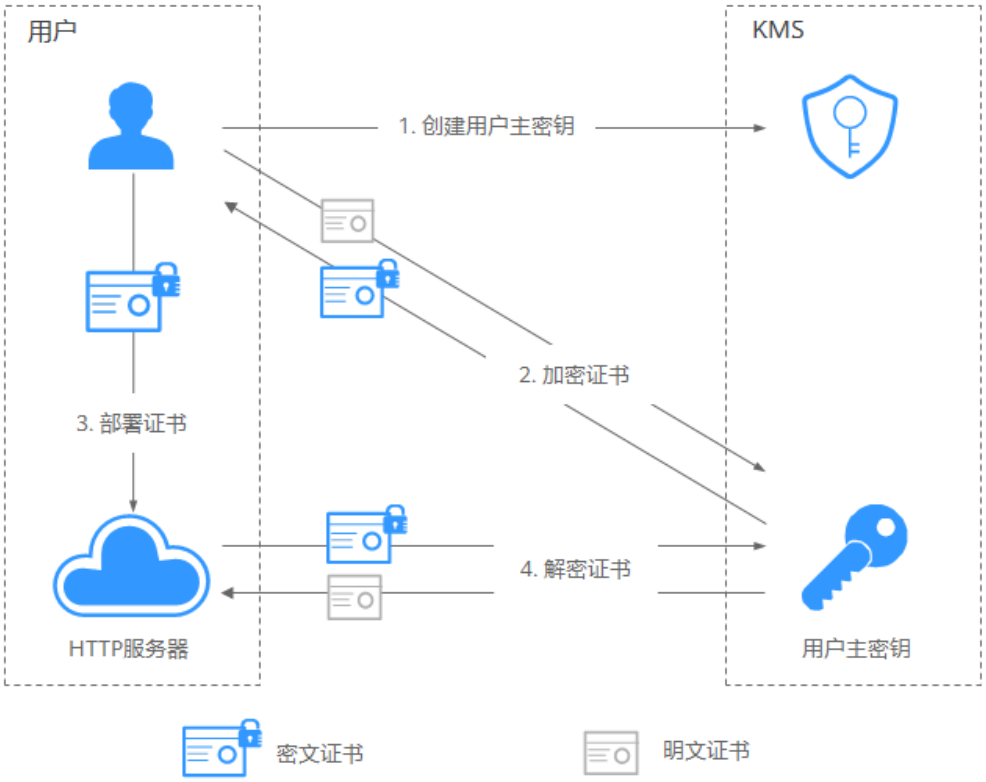
1.2.3 使用场景

小数据加解密

当您有少量数据（例如：密码、证书、电话号码等）需要加解密时，用户可以通过 KMS 界面使用在线工具加解密数据，或者调用 KMS 的 API 接口使用指定的用户主密钥直接加密、解密数据。当前支持不大于 4KB 的小数据加解密。

以保护服务器 HTTPS 证书为例，采用调用 KMS 的 API 接口方式进行说明，如图 1-1 所示。

图1-1 保护服务器 HTTPS 证书



流程说明如下：

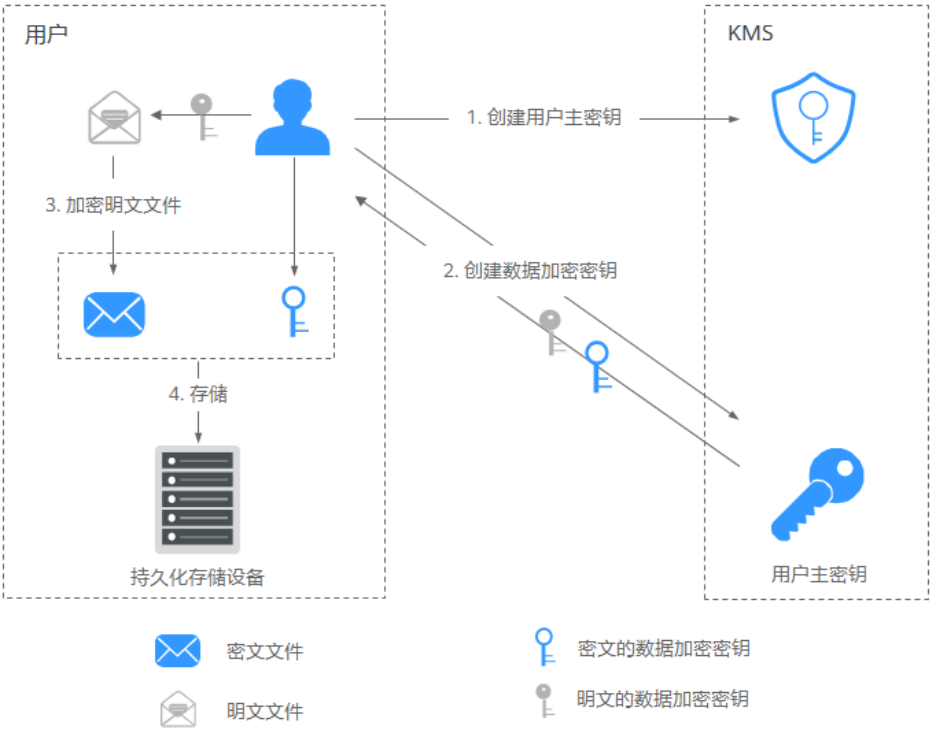
1. 用户需要在 KMS 中创建一个用户主密钥。
2. 用户调用 KMS 的“encrypt-data”接口，使用指定的用户主密钥将明文证书加密为密文证书。
3. 用户在服务器上部署密文证书。
4. 当服务器需要使用证书时，调用 KMS 的“decrypt-data”接口，将密文证书解密为明文证书。

大量数据加解密

当您有大量数据（例如：照片、视频或者数据库文件等）需要加解密时，用户可采用信封加密方式加解密数据，无需通过网络传输大量数据即可完成数据加解密。

- 加密本地文件流程，如图 1-2 所示。

图1-2 加密本地文件



流程说明如下：

a. 用户需要在 KMS 中创建一个用户主密钥。

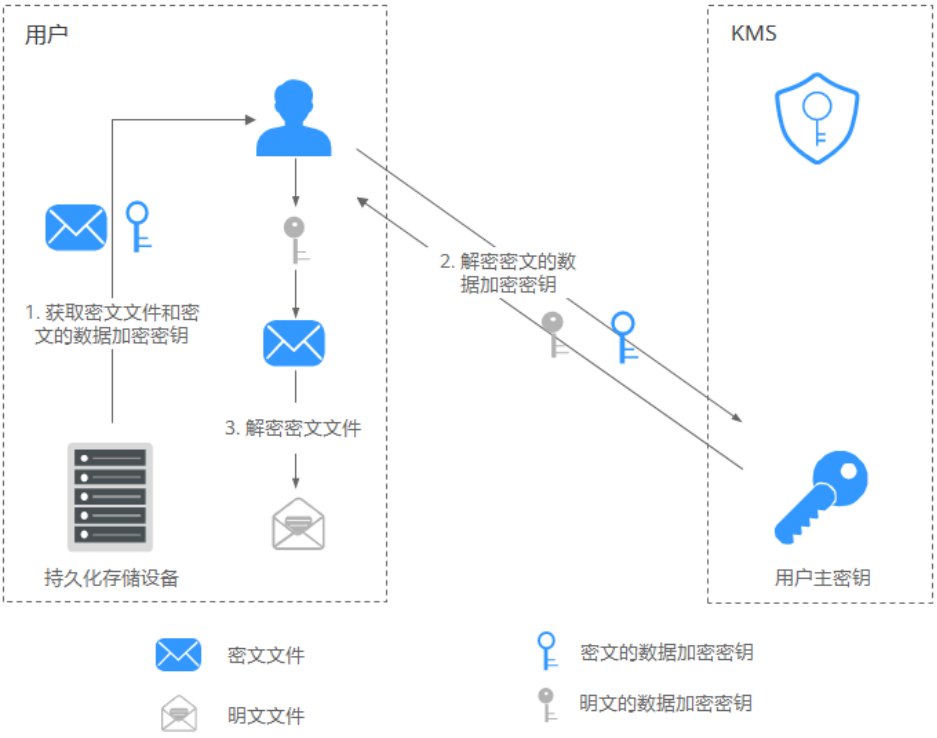
b. 用户调用 KMS 的“create-datakey”接口创建数据加密密钥。用户得到一个明文的数据加密密钥和一个密文的数据加密密钥。其中**密文的数据加密密钥**是由指定的**用户主密钥**加密**明文的数据加密密钥**生成的。

c. 用户使用明文的数据加密密钥来加密明文文件，生成密文文件。

d. 用户将密文的数据加密密钥和密文文件一同存储到持久化存储设备或服务中。

- 解密本地文件流程，如图 1-3 所示。

图1-3 解密本地文件



流程说明如下：

a. 用户从持久化存储设备或服务中读取密文的数据加密密钥和密文文件。

b. 用户调用 KMS 的“decrypt-datakey”接口，使用对应的用户主密钥（即生成密文的数据加密密钥时所使用的用户主密钥）来解密密文的数据加密密钥，取得明文的数据加密密钥。

若对应的用户主密钥被误删除，会导致解密失败。因此，需要妥善管理好用户主密钥。

c. 用户使用明文的数据加密密钥来解密密文文件。

1.2.4 如何使用

与云服务配合使用

云服务基于信封加密技术，通过调用 KMS 的接口来加密云服务资源。由用户管理自己的用户主密钥，云服务在拥有用户授权的情况下，使用用户指定的用户主密钥对数据进行加密。

加密流程说明如下：

1. 用户需要在 KMS 中创建一个用户主密钥。
2. 云服务调用 KMS 的“create-datakey”接口创建数据加密密钥。得到一个明文的数据加密密钥和一个密文的数据加密密钥。

说明

密文的数据加密密钥是由指定的用户主密钥加密明文的数据加密密钥生成的。

3. 云服务使用明文的数据加密密钥来加密明文文件，得到密文文件。
4. 云服务将密文的数据加密密钥和密文文件一同存储到持久化存储设备或服务中。

说明

用户通过云服务下载数据时，云服务通过 KMS 指定的用户主密钥对密文的数据加密密钥进行解密，并使用解密得到的明文的数据加密密钥来解密密文数据，然后将解密后的明文数据提供给用户下载。

表1-5 使用 KMS 加密的云服务列表

服务名称	如何使用
对象存储服务	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 KMS 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《对象存储服务控制台指南》。
云硬盘	在创建云硬盘时，用户启用云硬盘的加密功能，系统将使用用户主密钥产生的数据密钥对磁盘进行加密，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》 。
镜像服务	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 KMS 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》 。
弹性文件服务	用户通过弹性文件服务创建文件系统时，选择 KMS 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。
云数据库 RDS	在购买数据库实例时，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。 用户如何使用云数据库 RDS 的磁盘加密功能，具体操作请参见。
文档数据库服务	在购买文档数据库实例时，用户启用文档数据库实例的磁盘加密功能，选择 KMS 提供的用户主密钥对文档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。 用户如何使用文档数据库的磁盘加密功能，具体操作请参见。

与用户的应用程序配合使用

当您的应用程序需要对明文数据进行加密时，可通过调用 KMS 的接口来创建数据加密密钥，再使用数据加密密钥将明文数据进行加密，得到密文数据并进行存储。同时，用户的应用程序调用 KMS 的接口创建对应用户主密钥，对数据加密密钥进行加密，得到密文的数据加密密钥并进行存储。

基于信封加密技术，用户主密钥存储在 KMS 中，用户的应用程序只存储密文的数据加密密钥，仅在需要使用时调用 KMS 解密数据加密密钥。

加密流程说明如下：

1. 应用程序调用 KMS 的“create-key”接口创建一个用户主密钥。
2. 应用程序调用 KMS 的“create-datakey”接口创建数据加密密钥。得到一个明文的数据加密密钥和一个密文的数据加密密钥。

说明

密文的数据加密密钥是由 1 创建的用户主密钥加密明文的数据加密密钥生成的。

3. 应用程序使用明文的数据加密密钥来加密明文文件，生成密文文件。
4. 应用程序将密文的数据加密密钥和密文文件一同存储到持久化存储设备或服务中。

具体操作请参见《数据加密服务接口参考》。

1.2.5 使用 KMS 加密的云服务

1.2.5.1 OBS 服务端加密

- 用户使用 OBS（Object Storage Service，OBS）服务端加密方式上传文件时，可以选择“KMS 加密”，从而使用 KMS 提供的密钥来加密上传的文件。更多信息请参见《对象存储服务控制台指南》.。

  可供选择的用户主密钥包含以下两种：

  - KMS 为使用 OBS 的用户创建一个默认主密钥“obs/default”。
  - 用户通过 KMS 界面创建的非默认主密钥。
- 用户也可以通过调用 OBS API 接口，选择服务端加密 SSE-KMS 方式（SSE-KMS 方式是指 OBS 使用 KMS 提供的密钥进行服务端加密）上传文件，详情请参考《对象存储服务接口参考》。

1.2.5.2 EVS 服务端加密

- 用户创建磁盘时，可以选择“高级配置 > 现在配置 > 加密”，使用 KMS 提供的密钥来加密磁盘上的数据。更多信息请参见《云硬盘用户指南》。

说明

当用户需要使用磁盘加密功能时，需要授权云硬盘访问密钥管理。如果用户有授权资格，则可直接授权。如果权限不足，需先联系 Security Administrator 权限用户添加 Security Administrator 权限，然后重新操作。详细信息请参见《云硬盘用户指南》。

可供选择的用户主密钥包含以下两种：

- KMS 为使用 EVS（Elastic Volume Service，EVS）的用户创建一个默认主密钥“evs/default”。
- 用户通过 KMS 界面创建的非默认主密钥。

- 用户也可以通过调用 EVS API 接口创建加密磁盘，详情请参考《云硬盘接口参考》 。

1.2.5.3 IMS 服务端加密

- 用户上传镜像文件时，可以选择“KMS 加密”，使用 KMS 提供的密钥来加密上传的文件，更多信息请参见《镜像服务用户指南》 。

  可供选择的用户主密钥包含以下两种：

  - KMS 为使用 IMS（Image Management Service，IMS）的用户创建一个默认主密钥“ims/default”。
  - 用户通过 KMS 界面创建的非默认主密钥。

- 用户也可以通过调用 IMS API 接口创建加密镜像，详情请参考《镜像服务接口参考》。

1.2.5.4 RDS 服务端加密

- 用户在通过云数据库（Relational Database Service，RDS）购买数据库实例时，可以选择“磁盘加密”，使用 KMS 提供的密钥来加密数据库实例的磁盘，更多信息请参见《云数据库 RDS 用户指南》。

  图1-4 RDS 服务端加密

  可供选择的用户主密钥包含以下两种：

  - KMS 为使用 RDS（Relational Database Service，RDS）的用户创建一个默认主密钥“rds/default”。
  - 用户通过 KMS 界面创建的非默认主密钥。

- 用户也可以通过调用 RDS API 接口购买加密数据库实例，详情请参考《云数据库 RDS API 参考》。

1.2.5.5 DDS 服务端加密

- 用户在通过文档数据库服务（Document Database Service，DDS)购买文档数据库实例时，可以选择“磁盘加密”，使用 KMS 提供的密钥来加密文档数据库实例的磁盘，更多信息请参见《文档数据库服务用户指南》。

图1-5 DDS 服务端加密

可供选择的用户主密钥包含以下两种：

- KMS 为使用 DDS（Document Database Service，DDS）的用户创建一个默认主密钥“dds/default”。
- 用户通过 KMS 界面创建的非默认主密钥。

- 用户也可以通过调用 DDS API 接口购买加密数据库实例，详情请参考《文档数据库 API 参考》。

1.3 专属加密

1.3.1 功能特性

专属加密（Dedicated Hardware Security Module，Dedicated HSM）是一种云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。

Dedicated HSM 为您提供的加密硬件，帮助您保护弹性云服务器上数据的安全性与完整性，满足 FIPS 140-2 安全要求。同时，您能够对专属加密实例生成的密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。

功能介绍

Dedicated HSM 提供以下功能：

- 生成、存储、导入、导出和管理加密密钥（包括对称密钥和非对称密钥）。
- 使用对称和非对称算法加密和解密数据。
- 使用加密哈希函数计算消息摘要和基于哈希的消息身份验证代码。
- 对数据进行加密签名（包括代码签名）并验证签名。
- 以加密方式生成安全随机数据。

Dedicated HSM 支持的密码算法

支持国际通用密码算法，满足用户各种加密算法需求。

表1-6 Dedicated HSM 支持的密码算法

加密算法分类	通用密码算法	国密算法
对称密码算法	AES	SM1、SM4、SM7

加密算法分类	通用密码算法	国密算法
非对称密码算法	RSA（1024-4096）	SM2
摘要算法	SHA1、SHA256、SHA384	SM3

Dedicated HSM 支持的密码机类型

表1-7 Dedicated HSM 支持的密码机类型

密码机类型	功能	适用场景
服务器加密机	• 数据加密/解密 • 数据签名/验签 • 数据摘要 • 支持 MAC 的生成和验证	满足各种行业应用中的基础密码运算需求，比如身份认证、数据保护、SSL 密钥和运算卸载等。
金融加密机	• 支持 PIN 码的生成/加密/转换/验证 • 支持 MAC 生成及验证 • 支持 CVV 生成及验证 • 支持 TAC 生成及验证 • 支持常用 Racal 指令集 • 支持 PBOC3.0 常用指令集	满足金融领域密码运算需求，比如发卡系统、POS 系统等。
签名服务器	• 签名/验签 • 编码/解码数字信封 • 编码/解码带签名的数字信封 • 证书验证	满足签名业务相关需求，比如 CA 系统、证书验证、大量数据的加密传输和身份认证。

1.3.2 产品优势

- 云上使用

  Dedicated HSM 旨在满足用户将线下加密设备能力转移到云上的要求，降低运维成本。

- 弹性扩容

  灵活调整专属加密的数量，满足不同业务的加解密运算要求。

- 安全管理

  专属加密实例设备管理与内容（敏感信息）管理权限分离，用户作为设备使用者完全控制密钥的产生、存储和访问授权，Dedicated HSM 只负责监控和管理设备及其相关网络设施。即使 Dedicated HSM 的运维人员也无法获取到用户的密钥。

- 权限认证

  - 敏感指令支持分类授权控制，有效防止越权行为。
  - 支持用户名口令认证、数字证书认证等多种权限认证方式。
- 可靠性

  专属加密实例之间独享加密芯片，即使部分硬件芯片损坏也不影响使用。
- 安全合规

  Dedicated HSM 为您提供专属加密实例，帮助您保护弹性云服务器上数据的安全性和隐私性要求，满足监管合规要求。
- 应用广泛

  Dedicated HSM 可提供认证合规的金融加密机、服务器加密机以及签名验签服务器等，灵活支撑用户业务场景。

1.3.3 使用场景

若用户创建了专属加密实例，可通过 Dedicated HSM 提供的 **Ukey** 初始化并管控专属加密实例。用户作为设备使用者完全控制密钥的产生、存储和访问授权。

用户可通过专属加密实例加密用户业务系统（包含敏感数据加密、金融支付加密以及电子票据加密等），帮助用户加密企业自身的敏感数据（如合同、交易、流水等）以及企业用户的敏感数据（用户身份证号码、手机号码等），以防止黑客攻破网络、拖库导致数据泄露、内部用户非法访问或篡改数据等风险。

说明

用户需要将专属加密实例和业务系统部署在同一个 VPC 内，并选择合适的安全组规则。若您对此有疑问，请咨询技术支持人员。

敏感数据加密

应用领域：政府公共事业、互联网企业、包含大量敏感信息的系统应用。

数据是企业的核心资产，每个企业都有自己的核心敏感数据。通过专属加密服务对敏感数据进行完整性校验和加密存储，有效防止敏感数据被窃取、篡改，权限被非法获取。

金融支付

应用领域：交通卡支付、电商支付、各种预付费卡支付等系统应用

保证支付数据在传输和存储过程中的完整性、保密性和支付身份的认证、支付过程的不可否认性。

验伪

应用领域：交通、制造、医疗。

保证电子合同、电子发票、电子保单、电子病例在传输、存储过程中的保密性和完整性。

1.4 计费说明

计费项

DEW 根据您的使用情况和购买的版本计费。

表1-8 计费项说明

服务名称	计费模式	计费项	计费说明
密钥管理(KMS)	按需计费	密钥个数	按创建成功或导入成功的密钥实例进行按需计费，以小时为单位，不设最低消费标准。
	按需计费	API 请求次数	免费请求次数为 20000 次，超出的部分进行计费，以万次为单位。
专属加密(DHSM)	包年/包月	服务版本	按购买的版本：实行包月、包年的计费模式。 版本详情请参见。
	按需计费	API 请求次数	免费使用。

计费模式

- 密钥管理

  用户需要为自己创建或导入的所有用户主密钥，以及超出免费次数的 API 请求支付费用。
- 专属加密

  专属加密根据您购买的专属加密实例版本和设备型号进行包年/包月收费。

变更配置

数据加密服务暂不支持退订。

续费

包年/包月方式购买的 DEW 到期后，如果没有按时续费，公有云平台会提供一定的保留期。

为了防止造成不必要的损失，请您及时续费。

到期与欠费

- 服务到期

1.5 DEW 权限管理

如果您需要对云服务平台上购买的 DEW 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云服务资源的访问。

通过 IAM，您可以在帐号中给员工创建 IAM 用户，并使用策略来控制员工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，您希望这些开发人员拥有 DEW 的使用权限，但是不希望开发人员拥有删除 DEW 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 DEW，但是不允许删除 DEW 的权限策略，控制员工对云资源的使用范围。

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 DEW 的其它功能。

DEW 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。

DEW 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 1-9 所示，包括了 DEW 的所有系统权限。

表1-9 DEW 系统权限

系统角色/策略名称	描述	类别
KMS Administrator	加密密钥的管理员权限。	系统角色
KMS CMKFullAccess	加密密钥所有权限。	系统策略

表 1-10 列出了 DEW 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1-10 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	√	√
查询密钥实例	√	√
查询密钥标签	√	√
查询项目标签	√	√
批量添加删除密钥标签	√	√

操作	KMS Administrator	KMS CMKFullAccess
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

- 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。

1.6 如何访问

云服务提供了 Web 化的服务管理平台，即管理控制台管理方式。

- 管理控制台方式

  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，单击页面上方的“服务列表”，选择“安全 > 数据加密服务”。
- API 方式

  用户可通过接口方式访问数据加密服务，具体操作请参见《数据加密服务接口参考》。

1.7 与其他云服务的关系

与对象存储服务的关系

对象存储服务（Object Storage Service，OBS）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。KMS 为 OBS 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

云硬盘（Elastic Volume Service，EVS）可以为云服务器提供高可靠、高性能、规格丰富并且可弹性扩展的块存储服务，可满足不同场景的业务需求，适用于分布式文件系统、开发测试、数据仓库以及高性能计算等场景。KMS 为 EVS 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

镜像服务（Image Management Service，IMS）提供镜像的生命周期管理能力。KMS 为 IMS 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

弹性文件服务（Scalable File Service，SFS）提供按需扩展的高性能文件存储（NAS）。KMS 为 SFS 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。

与云数据库的关系

云数据库（Relational Database Service，RDS）是一种基于云计算平台的即开即用、稳定可靠、弹性伸缩、便捷管理的在线云数据库服务。KMS 为 RDS 提供用户主密钥管理控制能力，应用于云数据库的磁盘加密功能。

与弹性云服务器的关系

弹性云服务器（Elastic Cloud Server，ECS）是由 CPU、内存、操作系统、云硬盘组成的基础的计算组件。弹性云服务器创建成功后，您就可以像使用自己的本地 PC 或物理服务器一样，在云上使用弹性云服务器。

Dedicated HSM 提供的专属加密实例可以为部署在弹性云服务器内的业务系统加密敏感数据，用户可完全控制密钥的生成、存储和访问授权，保证数据在传输、存储过程中的完整性、保密性。

与文档数据库服务的关系

文档数据库服务（Document Database Service，DDS）完全兼容 MongoDB 协议，提供安全、高可用、高可靠、弹性伸缩和易用的数据库服务，同时提供一键部署、弹性扩容、容灾、备份、恢复、监控和告警等功能。KMS 为 DDS 提供用户主密钥管理控制能力，应用于文档数据库的磁盘加密功能。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录数据加密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《云审计服务用户指南》。

表1-11 云审计服务支持的 DEW 操作列表

操作名称	资源类型	事件名称

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
加密数据	cmk	encryptData
解密数据	cmk	decryptData
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
开启密钥轮换	cmk	enableKeyRotation
修改密钥轮换周期	cmk	updateKeyRotationInterval
关闭密钥轮换	cmk	disableKeyRotation

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management, IAM）为数据加密服务供了权限管理的功能。

需要拥有 KMS Administrator 权限的用户才能使用 DEW 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》。

1.8 个人数据保护机制

为了确保您的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，DEW 通过控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

DEW 收集及产生的个人数据如表 1-12 所示：

表1-12 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
租户 ID	• 在控制台进行任何操作时 Token 中的租户 ID • 在调用 API 接口时 Token 中的租户 ID	否	是，租户 ID 是用户的身份标识信息

存储方式

租户 ID 不属于敏感数据，明文存储。

访问权限控制

用户只能查看自己业务的相关日志。

日志记录

用户个人数据的所有操作，包括修改、查询和删除等，DEW 都会记录审计日志并上传至云审计服务（CTS），用户可以并且仅可以查看自己的审计日志。

1.9 快速入门

您可以通过 KMS 创建密钥，并使用创建的密钥对 OBS 服务端中上传的文件进行加密。

1.9.1 使用密钥进行 OBS 服务端加密

本章节以使用密钥进行 OBS 服务端加密为例，指导您快速上手使用密钥管理服务。

前提条件

账号拥有 KMS CMKFullAccess 及以上权限。

拥有已创建好的自定义密钥，创建密钥操作流程参见 2.1.2 创建密钥章节。

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“存储 > 对象存储 > 服务”，默认进入“对象存储”页面。

步骤 4 单击右上角“创建桶”，创建一个 OBS 桶，用于存储上传文件。

步骤 5 创建成功后，单击桶的名称，进入创 OBS 桶的详细信息页面。

步骤 6 在左侧导航栏中单击“对象”，进入默认页面。

步骤 7 单击“上传对象”，在上传对象对话框中，选择待上传的文件，并勾选“KMS 加密”。

说明

您可以使用自己创建的自定义密钥，也可以使用 KMS 系统创建的默认主密钥。

步骤 8 单击“上传”，完成文件上传后，密钥即开始对 OBS 桶中上传文件进行加密。

----结束

2 用户指南

2.1 密钥管理

2.1.1 密钥概述

用户主密钥包括“对称密钥”和“非对称密钥”。

对称密钥加密是最常用的数据加密保护方式，相比对称密钥加密，非对称密钥通常用于在信任程度不对等的系统之间，实现数字签名验签或者加密传递敏感信息。非对称密钥由一对公钥和私钥组成，他们互相关联，其中的公钥可以被分发给任何人，而私钥必须被安全的保护起来，只有受信任者可以使用。

使用非对称密钥生成数字签名以及验证签名：签名者将验签公钥分发给消息接收者，使用签名私钥，对数据产生签名，并将数据以及签名传递给消息接收者。消息接收者获得数据和签名后，使用公钥针对数据验证签名的合法性。

表2-1 KMS 支持的密钥算法类型

密钥类型	算法类型	密钥规格	说明	用途
对称密钥	AES	AES_256	AES 对称密钥	小量数据的加解密或用于加解密数据密钥。
对称密钥	SM4	SM4	国密 SM4 对称密钥	小量数据的加解密或用于加解密数据密钥。
非对称密钥	RSA	• RSA_2048 • RSA_3072 • RSA_4096	RSA 非对称密钥	小量数据的加解密或数字签名。
	ECC	• EC_P256 • EC_P384	椭圆曲线密码，使用 NIST 推荐的椭圆曲	数字签名

密钥类型	算法类型	密钥规格	说明	用途
			线	
非对称密钥	SM2	SM2	国密 SM2 非对称密钥	小量数据的加解密或数字签名。

2.1.2 创建密钥

该任务指导用户通过密钥管理界面创建自定义密钥。

约束条件

- 用户最多可创建 20 个自定义密钥，不包含默认密钥。
- 创建的对称密钥使用的是 AES-256 加解密算法，密钥长度为 256bit，可用于小量数据的加解密或用于加解密数据密钥。
- 创建的非对称密钥使用的是 RSA 密钥或 ECC 密钥，RSA 密钥可用于加解密、数字签名及验签，ECC 密钥仅用于数字签名及验签。
- 因为默认密钥的别名后缀为“/default”，所以用户创建的密钥别名后缀不能为“/default”。
- 数据加密服务不限定主密钥的调用次数。

应用场景

- 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。
- 自定义密钥直接加解密小数据。
- 用户应用程序的 DEK 加解密。
- 非对称密钥可用于数字签名及验签。

创建密钥

步骤 1 登录管理控制台。

步骤 2 单击管理控制台左上角  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 单击界面右上角“创建密钥”。

步骤 5 在弹出的“创建密钥”对话框中，填写密钥参数。

- 别名：待创建密钥的别名。

说明

- 输入字符支持数字、字母、“_”、“-”、“:”和“/”。
- 支持长度为 1 ~ 255 个字符。

- 密钥算法：选择密钥算法。KMS 支持的密钥算法说明如表 2-2 所示。

表2-2 KMS 支持的密钥算法类型

密钥类型	算法类型	密钥规格	说明	用途
对称密钥	AES	AES_256	AES 对称密钥	小量数据的加解密或用于加解密数据密钥。
对称密钥	SM4	SM4	国密 SM4 对称密钥	小量数据的加解密或用于加解密数据密钥。
非对称密钥	RSA	• RSA_2048 • RSA_3072 • RSA_4096	RSA 非对称密钥	小量数据的加解密或数字签名。
	ECC	• EC_P256 • EC_P384	椭圆曲线密码，使用 NIST 推荐的椭圆曲线	数字签名
非对称密钥	SM2	SM2	国密 SM2 非对称密钥	小量数据的加解密或数字签名。

- 密钥用途：可选择“SIGN_VERIFY”或“ENCRYPT_DECRYPT”。
  - 对于对称密钥，默认值“ENCRYPT_DECRYPT”。
  - 对于 RSA 非对称密钥，可选择“ENCRYPT_DECRYPT”或“SIGN_VERIFY”，省略参数为默认值“SIGN_VERIFY”。
  - 对于 ECC 非对称密钥，默认值“SIGN_VERIFY”。
  - 对于 SM2 非对称密钥，可选择“ENCRYPT_DECRYPT”或“SIGN_VERIFY”，省略参数为默认值“SIGN_VERIFY”。

说明

创建密钥时请选择“密钥用途”，密钥创建后不可修改。

- （可选）描述：可根据自己的需要为自定义密钥添加描述。
- 企业项目：该参数针对企业用户使用。

  如果您是企业用户，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 6 （可选）用户可根据自己的需要为自定义密钥添加标签，输入“标签键”和“标签值”。

说明

- 当用户在创建密钥时，没有为该自定义密钥添加标签。若用户需要为该自定义密钥添加标签，可单击该自定义密钥的别名，进入密钥详情页面，单击“标签”， 为该自定义密钥添加标签。
- 同一个自定义密钥下，一个标签键只能对应一个标签值；不同的自定义密钥下可以使用相同的标签键。
- 用户最多可以给单个自定义密钥添加 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“确定”，在页面右上角弹出“创建密钥成功”，则说明密钥创建完成。

用户可在密钥列表上查看已完成创建的密钥，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《对象存储服务控制台指南》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。
- 云数据库中数据库实例的磁盘加密方法，具体请参见《云数据库 RDS 快速入门》的“购买实例”章节。
- 创建 DEK、不含明文的 DEK 方法，具体请参见《数据加密服务接口参考》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《数据加密服务接口参考》的“加密数据密钥”与“解密数据密钥”章节。

2.1.3 导入密钥

2.1.3.1 概述

自定义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 管理控制台创建自定义密钥时，KMS 系统会自动为该自定义密钥生成密钥材料。
- 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空的自定义密钥，并将自己的密钥材料导入该自定义密钥中。

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 2-3 所示。

表2-3 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	• 可以手动删除密钥材料，但不能删除该自定义密钥及其元数据。 • 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，但不会删除该自定义密钥及其元数据。 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	• 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自定义密钥时，该自定义密钥与该密钥材料永久关联，不能将其他密钥材料导入该自定义密钥中。

- 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自定义密钥（即自定义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。

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自定义密钥一样支持启用、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。

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 单击“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参数。

- 别名：待创建密钥的别名。

  说明

  - 输入字符支持数字、字母、“_”、“-”、“:”和“/”。
  - 支持长度为 1 ~ 255 个字符。
- （可选）描述：可根据自己的需要为自定义密钥添加描述。
- 企业项目：该参数针对企业用户使用。

  如果您是企业用户，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 6 （可选）用户可根据自己的需要为自定义密钥添加标签，输入“标签键”和“标签值”。

说明

- 当用户在创建密钥时，没有为该自定义密钥添加标签。若用户需要为该自定义密钥添加标签，可单击该自定义密钥的别名，进入密钥详情页面，单击“标签”，为该自定义密钥添加标签。
- 同一个自定义密钥下，一个标签键只能对应一个标签值；不同的自定义密钥下可以使用相同的标签键。
- 用户最多可以给单个自定义密钥添加 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自定义密钥。

步骤 9 单击“下一步”，进入“获取包装密钥和导入令牌”页面。

表2-4 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。	请您根据自己的 HSM 功能选择加密算法。

密钥包装算法	说明	设置
RSAES_OAEP_SHA_1	具有“SHA-1”哈希函数的 OAEP 的 RSA 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。
SM2_ENCRYPT	国密推荐的 SM2 椭圆曲线公钥密码算法。	请在支持国密的局点使用 SM2 加密算法。

说明

当用户执行“导入密钥”操作，但未成功导入密钥材料便退出操作过程时，可在待导入密钥材料的自定义密钥所在行单击“导入密钥材料”，页面会弹出“导入密钥材料”对话框，用户可继续执行导入密钥材料的操作。

步骤 10 获取“包装密钥”和“导入令牌”，并加密密钥材料。

1. 获取“包装密钥”和“导入令牌”。
   - 方法一：单击“下载”，下载的文件为包装密钥。
     - wrappingKey_*密钥 ID*：即包装密钥，编码为二进制格式，用于加密密钥材料的包装密钥。
     - 导入令牌：引导程序已自动传递导入令牌，无需下载，若中途退出引导程序，导入令牌将自动失效。

须知

包装密钥将在 24 小时后失效，失效后将不能使用。如果包装密钥失效，请重新下载包装密钥。

引导程序将自动传递导入令牌，若创建密钥过程中，关闭或者退出设置则导入令牌失效。重新发起导入密钥材料操作时，导入令牌引导程序自动启动。

   - 方法二：通过调用 API 接口的方式获取包装密钥和导入令牌。
     i. 调用“get-parameters-for-import”接口，获取包装密钥和导入令牌。
        - 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。

以获取密钥 ID 为“43f1ffd7-18fb-4568-9575-602e009b7ee8”，加密算法为“RSAES_OAEP_SHA_256”的包装密钥和导入令牌为例。

- 请求样例

```
{
    "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
    "wrapping_algorithm":"RSAES_OAEP_SHA_256"
}
```

- 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
}
```

ii. 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加密的密钥材料才能成功导入管理控制台。

1) 复制包装密钥“public_key”的内容，粘贴到“.txt”文件中，并保存为“PublicKey.b64”。

2) 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

iii. 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”。

2. 使用“包装密钥”加密密钥材料。

说明

执行完此步骤后可获得以下文件：

对称密钥场景：**EncryptedKeyMaterial.bin** 密钥材料

非对称密钥场景：**EncryptedKeyMaterial.bin** 临时密钥材料和 **out_rsa_private_key.der** 私钥密文

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：使用 OpenSSL 生成密钥材料，并用下载的“包装密钥”对密钥材料进行加密。

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。

a. 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。

- 配套算法为 AES256 对称密钥时，在已安装 OpenSSL 工具的客户端上，执行以下命令。

openssl rand -out *PlaintextKeyMaterial.bin* 32

- 配套算法为 RSA、ECC 非对称密钥时，在已安装 OpenSSL 工具的客户端上，执行以下命令。

1) 生成 16 进制 AES256 密钥：

openssl rand -out 0xPlaintextKeyMaterial.bin -hex 32

2) 将 16 进制 AES256 密钥转换成二进制格式：

cat 0xPlaintextKeyMaterial.bin | xxd -r -ps > PlaintextKeyMaterial.bin

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。

若“包装密钥”由控制台下载，以下命令中的 ***PublicKey.bin*** 参数请以下载的包装密钥名称 *wrappingKey_密钥 ID* 进行替换。

表2-5 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	**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**
RSAES_OAEP_SHA_1	**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**
SM2_ENCRYPT	**gmssl pkeyutl** **-encrypt -pkeyopt ec_scheme:sm2** **-pkeyopt ec_encrypt_param:sm3** **-in *PlaintextKeyMaterial.bin*** **-pubin -inkey *PublicKey.bin*** **-keyform der** **-out EncryptedKeyMaterial.bin**

c. （可选）对于导入非对称密钥的场景，需要生成非对称私钥，并使用临时密钥材料（“ EncryptedKeyMaterial.bin”）对私钥进行加密，加密后的文件作为“私钥密文”导入。

- 执行以下命令（以配套算法为“RSA4096 算法”为例）：

1) 生成私钥

openssl genrsa -out rsa_private_key.pem 4096

2) 转换成 der 格式

openssl pkcs8 -topk8 -inform PEM -outform DER -in rsa_private_key.pem -out rsa_private_key.der -nocrypt

3) 使用临时密钥材料对私钥进行加密

openssl enc -id-aes256-wrap-pad -K $(cat 0xPlaintextKeyMaterial.bin) -iv A65959A6 -in rsa_private_key.der -out out_rsa_private_key.der

说明

默认情况下，OpenSSL 命令行工具中未启用包装密码算法-id-aes256-wrap-pad。您可以下载并安装最新版本的 OpenSSL，然后对其进行修补，以完成导入非对称密钥所需的信封包装。修补方式可以参考常见问题。

步骤 11 单击“下一步”，进入“导入密钥材料”页面。

步骤 12 单击“下一步”，进入“导入密钥令牌”页面。根据表 2-6 设置参数。

表2-6 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 12.b 调用 API 获取的导入令牌。
密钥材料失效模式	• 永不失效：导入的密钥材料永久不失效。 • 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，KMS 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 13 单击“确定”，页面右上角弹出“密钥导入成功”，则说明导入密钥成功。

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

2.1.3.2 删除密钥材料

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，自定义密钥的状态变为“等待导入”。用户也可以根据需要手动删除密钥材料。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，该自定义密钥可以解密删除密钥材料前加密的所有数据。

前提条件

- 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”。

约束条件

- 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，该自定义密钥可以解密删除密钥材料前加密的所有数据。
- 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”。
- 非对称密钥不支持删除密钥材料功能，如需删除，请使用 2.1.4.4 删除密钥功能。

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 在需要删除的密钥材料所在行，单击“删除密钥材料”。

步骤 5 在弹出的对话框中单击“确定”，页面右上角弹出“密钥材料删除成功”，则说明删除密钥材料的成功。

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

2.1.4 管理密钥

2.1.4.1 查看密钥

该任务指导用户通过 KMS 界面查看自定义密钥的信息，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”。

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 在密钥列表中，查看密钥信息，密钥列表参数说明。

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： • 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。 **说明** **在 IAM 中创建自定义策略时，添加资源路径中的“路径”填写此 ID。**
创建时间	创建该密钥的时间。
密钥算法及用途	创建密钥时选择的密钥算法及该算法的用途。
密钥材料来源	密钥材料的来源，包含： • 外部 用户从外部导入到 KMS。 • 密钥管理 用户通过 KMS 创建的密钥，或默认密钥。
操作	用户可以在操作栏中，执行禁用、删除、导入密钥材料、取消

参数	操作说明
	删除密钥等操作。

步骤 5 用户可单击密钥别名，查看密钥详细信息。

说明

用户可单击该密钥的“别名”或“描述”所在行的 ，修改密钥的别名或描述信息。

- 默认密钥（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。

----结束

2.1.4.2 启用密钥

该任务指导用户通过密钥管理界面对单个或多个自定义密钥进行启用操作，使被禁用的密钥恢复到数据加解密能力。新建的自定义密钥默认为“启用”状态。

前提条件

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 在需要启用的密钥所在行，单击“启用”。

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

2.1.4.3 禁用密钥

该任务指导用户通过密钥管理界面对指定的自定义密钥进行禁用，以紧急保护数据。

自定义密钥被禁用后，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 2.1.4.2 启用密钥。

前提条件

待禁用的密钥需处于“启用”状态。

约束条件

- 默认密钥为密钥管理自动创建，不支持禁用操作。
- 密钥被禁用后，仍然会计费。只有删除密钥，才会停止计费。

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 在需要禁用的密钥所在行，单击“禁用”。

步骤 5 在弹出窗口中，勾选“我已知晓禁用以上密钥产生的影响”，单击“是”，完成禁用单个密钥操作。

说明

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

----结束

2.1.4.4 删除密钥

在删除密钥前，您需要确保该密钥没有被使用或将来也不会被使用。您可以通过以下方式确定密钥的使用情况。

前提条件

- 待删除的密钥需处于“启用”、“禁用”、“等待导入”或“冻结”状态。

约束条件

- 执行删除密钥操作后，密钥不会立即删除，密钥管理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。
- 默认密钥为服务自动创建，不支持删除操作。
- 计划删除的密钥是不计费的，但是，如果您在密钥被彻底删除前的等待期内取消删除密钥，该密钥将恢复计费，并收取从计划删除开始到取消删除期间的费用。

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 在需要删除的密钥所在行，单击“删除”。

步骤 5 在弹出的窗口中，填写“推迟删除”的时间。

说明

- 密钥管理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。
- 计划删除的密钥是不计费的，但是，如果您在密钥被彻底删除前的等待期内取消删除密钥，该密钥将恢复计费，并收取从计划删除开始到取消删除期间的费用。

步骤 6 勾选“我已知晓删除以上密钥产生的影响”，单击“是”，完成删除单个密钥操作。

说明

如果您想批量计划删除密钥，可以勾选所有需要计划删除的密钥，然后在列表左上角，单击“删除”。

----结束

2.1.4.5 取消删除密钥

该任务指导用户在未超出删除密钥的推迟时间，通过密钥管理界面对自定义密钥进行取消删除操作，取消删除后密钥处于“禁用”状态。

前提条件

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 在需要取消删除的密钥所在行，单击“取消删除”。

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。

- 如果是通过 KMS 创建的密钥，取消删除后密钥状态为“禁用”，如需启用密钥，请参见 2.1.4.2 启用密钥操作。
- 如果是外部导入的密钥，且有密钥材料，取消删除后密钥状态为“禁用”，如需启用密钥，请参见 2.1.4.2 启用密钥操作。
- 如果是外部导入的密钥，且没有密钥材料，取消删除后密钥状态为“等待导入”，如需使用该密钥，请参见 2.1.3 导入密钥操作。

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

2.1.5 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。

前提条件

自定义密钥处于“启用”状态。

约束条件

- 在线工具不支持通过默认密钥加解密小数据。
- 用户可使用调用 API 接口的方式，使用默认密钥加解密小数据，详细信息请参考《数据加密服务接口参考》。
- 加密数据时，使用当前指定的密钥加密数据。
- 解密数据时，在线工具自动识别并使用数据被加密时使用的密钥解密数据，如果加密时使用的密钥已被删除，会导致解密失败。

加密数据

步骤 1 登录管理控制台。

步骤 2 单击管理控制台左上角  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 单击目标自定义密钥的别名，进入密钥详细信息在线工具加密数据页面。

步骤 5 在“加密”文本框中输入待加密的数据。

步骤 6 单击“执行”，右侧文本框显示加密后的密文数据。

说明

- 加密数据时，使用当前指定的密钥加密数据。
- 用户可单击“清除”，清除已输入的数据。
- 用户可单击“复制到剪切板”拷贝加密后的密文数据，并保存到本地文件中。

----结束

解密数据

步骤 1 登录管理控制台。

步骤 2 单击管理控制台左上角  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 解密数据时，可单击任意“启用”状态的非默认密钥别名，进入该密钥的在线工具页面。

步骤 5 单击“解密”，在左侧文本框中数据待解密的密文数据。

说明

- 在线工具自动识别并使用数据被加密时使用的密钥解密数据。
- 若该密钥已被删除，会导致解密失败。

步骤 6 单击“执行”，右侧文本框中显示解密后的明文数据。

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

2.1.6 管理标签

2.1.6.1 添加标签

标签用于标识自定义密钥。为自定义密钥添加标签，可以方便用户对自定义密钥进行分类和跟踪，并按标签汇总自定义密钥的使用情况。

约束条件

KMS 不支持为默认密钥添加标签。

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 单击目标自定义密钥的别名，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。

步骤 6 单击“添加标签”，弹出添加标签对话框，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 2-8 所示。

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2-8 标签参数说明

参数	参数说明	取值要求	样例
标签键	标签的名称。 同一个自定义密钥下，一个标签键只能对应一个标签值；不同的自定义密钥下可以使用相同的标签键。 用户最多可以给单个自定义密钥添加 20 个标签。	• 必填。 • 对于同一个自定义密钥，标签键唯一。 • 长度不超过 36 个字符。 • 可以包含以下 5 种字符： – 大写字母 – 小写字母 – 数字 – 特殊字符，包括“-”和“_” – 中文字符	cost
标签值	标签的值。	• 可以为空。 • 长度不超过 43 个字符。 • 可以包含以下 5 种字符： – 大写字母 – 小写字母 – 数字 – 特殊字符，包括“-”和“_” – 中文字符	100

步骤 7 单击“确定”，完成标签的添加。

----结束

2.1.6.2 通过标签搜索自定义密钥

该任务指导用户在密钥管理界面，通过标签搜索当前项目下满足标签搜索条件的自定义密钥。

前提条件

已添加标签。

约束条件

- 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。

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，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 单击“标签搜索”，展开搜索框。

步骤 5 在搜索框中输入或选择“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

2.1.6.3 修改标签值

该任务指导用户通过密钥管理界面修改标签值。

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，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 单击目标自定义密钥的别名，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。

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

2.1.6.4 删除标签

该任务指导用户通过密钥管理界面删除标签。

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 单击目标自定义密钥的别名，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。

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“确定”，完成标签的删除。

----结束

2.1.7 轮换密钥

2.1.7.1 密钥轮换概述

为什么需要轮换密钥

广泛重复的使用加密密钥，会对加密密钥的安全造成风险。为了确保加密密钥的安全性，建议您定期轮换密钥，更改原密钥的密钥材料。

定期轮换密钥有如下优点：

- 减少每个密钥加密的数据量

  一个密钥的安全性与被它加密的数据量呈反比。数据量通常是指同一个密钥加密的数据总字节数或总消息数。

- 增强应对安全事件的能力

  在系统安全设计的初期，设计密钥轮换功能并将其作为日常运维手段。这样可以使系统在特定安全事件发生时具备实际执行能力。

- 加强对数据的隔离能力

  轮换密钥使得轮换前后产生的密文数据形成隔离效果。特定密钥的安全事件可以被快速定义影响范围，从而采取进一步措施。

密钥轮换的两种方法

云服务提供了两种密钥轮换方法：

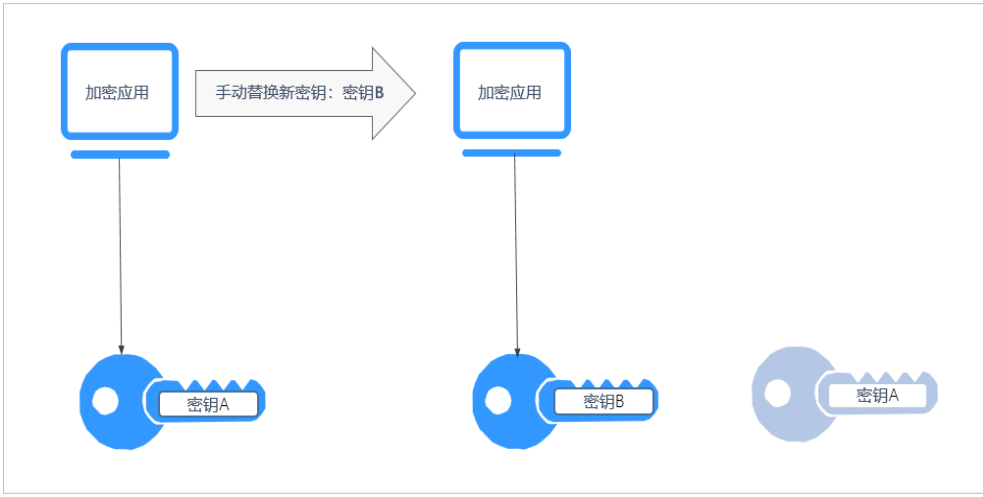
- 手动轮换密钥

  使用一个新的密钥替换使用中的密钥。即创建一个新的密钥 B，并使用密钥 B 替代当前使用的密钥 A，当密钥 B 使用的加密材料与密钥 A 使用的加密材料不相同时，使用密钥 B 与更改密钥 A 的密钥材料具有相同效果。

  示例：

  以 OBS 服务为例：需要手动轮换密钥时，用户先在 KMS 界面创建一个新的自定义密钥，后在 OBS 界面将原自定义密钥替换为新的自定义密钥。

  图2-1 手动轮换密钥工作原理

- 自动轮换密钥

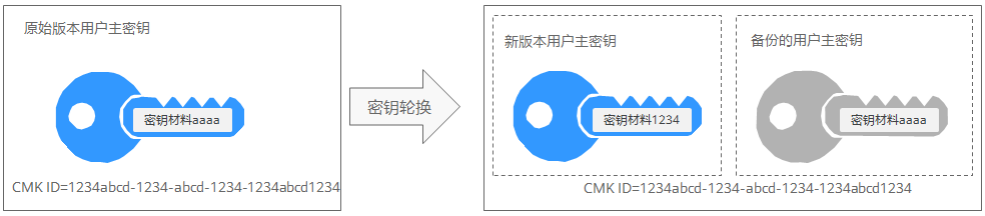
  KMS 会根据设置的轮换周期（默认 365 天）自动轮换密钥，系统自动生成一个新的密钥 B，并替换当前使用的密钥 A。自动轮换密钥只会更改主密钥的密钥材料，即加密操作中所使用的加密材料。不管密钥材料有没有变更或变更了多少次，该主密钥仍是相同的逻辑资源。主密钥的属性（密钥 ID、别名、描述、权限）不会发生变化。

  自动密钥轮换具有以下特点：

  a. 为现有的自定义密钥开启密钥轮换后，KMS 自动为该自定义密钥生成新的密钥材料。

  b. 自动密钥轮换对主密钥所保护的数据无效。它不会轮换主密钥生成的数据密钥，也不会对任何受主密钥保护的数据重新加密，并且它无法减轻数据密钥泄露的影响。

图2-2 自动密钥轮换工作原理



说明

KMS 会保留与该自定义密钥关联的所有版本的自定义密钥。这使得 KMS 可以解密使用该自定义密钥加密的任何密文。

- 加密数据时，KMS 会自动使用当前最新版本的自定义密钥来执行加密操作。
- 解密数据时，KMS 会自动使用加密时所使用的自定义密钥来执行解密操作。

密钥支持的轮换方式

表2-9 密钥轮换方式

密钥的来源或状态	支持的密钥轮换方式
默认密钥	不支持密钥轮换。
自定义密钥	仅支持手动轮换密钥。 关于自定义密钥的更多信息，请参见 2.1.3.1 概述。
对称密钥	支持自动轮换密钥和手动轮换密钥。
非对称密钥	仅支持手动轮换密钥。
已禁用的主密钥	禁用主密钥后，KMS 不会对它进行轮换。但是，密钥轮换状态不会发生改变，并且在主密钥处于禁用状态时不能对其进行更改。重新启用主密钥后，如果已禁用的自定义密钥已超过轮换周期，KMS 会立即轮换。如果已禁用的自定义密钥少于轮换周期，KMS 会恢复之前的密钥轮换计划。 关于禁用密钥的信息，请参见 2.1.4.3 禁用密钥。
计划删除的主密钥	对于计划删除的主密钥，KMS 不会对它进行轮换。如果取消删除，将恢复之前的密钥轮换状态。如果计划删除的自定义密钥已超过轮换周期，KMS 会立即轮换。如果计划删除的用户主密钥少于轮换周期，KMS 会恢复之前的密钥轮换计划。 关于计划删除密钥的信息，请参见 2.1.4.4 删除密钥。

说明

用户可在“轮换策略”页面查看轮换详情，例如：上次轮换时间、轮换次数。

2.1.7.2 开启密钥轮换

该任务指导用户通过密钥管理界面开启自动轮换密钥。

默认情况下，自定义密钥的自动密钥轮换处于禁用状态。当您启用（或重新启用）密钥轮换时，KMS 会根据您设置的轮换周期自动轮换自定义密钥。

前提条件

- 密钥处于“启用”状态。
- “密钥材料来源”为“密钥管理”。

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤 5 单击“轮换策略”，进入“密钥轮换管理”页签。

步骤 6 单击  ，开启密钥轮换。

步骤 7 在弹出的“开启密钥轮换”对话框中，设置密钥轮换周期，并单击“确定”。

- 轮换周期（天）：取值范围为“30~365”的整数，默认“365”天。
- 轮换周期从此次设置的时间开始计算。
- 轮换周期需要根据自定义密钥的使用频率进行设置，若密钥使用频率高，建议设置为短周期；反之，则设置为长周期。

说明

- 如果自定义密钥开启密钥轮换以后，禁用了自定义密钥，KMS 也不会轮换该自定义密钥。
- 当自定义密钥恢复到“启用”状态时，密钥轮换将立即重新激活。如果刚恢复“启用”状态的自定义密钥距离上次轮换的时间已超过轮换周期，KMS 将在 24 小时内轮换该自定义密钥。
- 用户可单击  ，修改轮换周期。修改轮换周期后，根据新设置的轮换周期进行轮换。

----结束

2.1.7.3 关闭密钥轮换

该任务指导用户通过密钥管理界面关闭自动轮换密钥。

前提条件

- 密钥处于“启用”状态。

- “密钥材料来源”为“密钥管理”。
- 已开启密钥轮换。

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  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 单击目标对称密钥的别名，进入密钥详细信息页面。

步骤 5 单击“轮换策略”，进入密钥轮换管理界面。

步骤 6 单击  ，关闭密钥轮换。

步骤 7 关闭后，页面将显示密钥轮换管理界面。

----结束

2.2 专属加密

2.2.1 操作指引

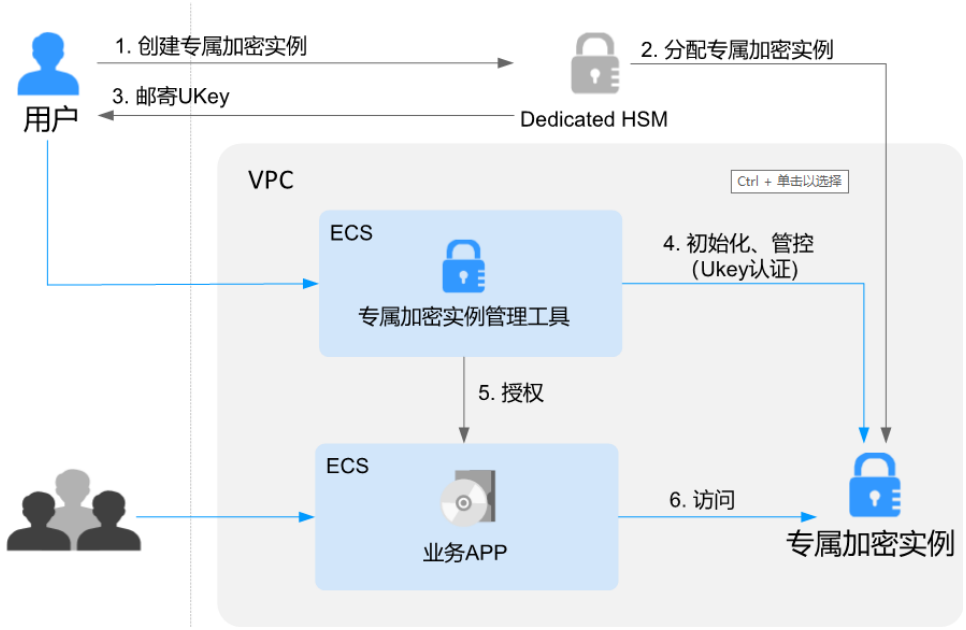
限制说明

- 专属加密实例需要配合虚拟私有云（VPC）一起使用。创建专属加密实例后，需要在管理控制台中实例化专属加密实例（配置 VPC 网络、安全组、网卡），才能正常使用。
- 专属加密实例出于安全性的考虑，不对公网提供服务，您需要将专属加密实例管理工具部署到与专属加密实例同一 VPC 网络中，才能对专属加密实例进行管理。

操作指引

当用户需要在云上使用专属加密服务时，可通过 Dedicated HSM 界面创建专属加密实例。创建专属加密实例后，当用户收到 Dedicated HSM 邮寄的 Ukey 后，通过 Ukey 初始化，并管控专属加密实例。用户通过专属加密实例管理工具授权业务 APP，允许业务用户通过业务 APP 访问专属加密实例。操作指引如图 2-3 所示。

图2-3 操作指引



操作指引说明如表 2-10 所示。

表2-10 操作指引说明

编号	操作步骤	说明	操作角色
1	创建专属加密实例	通过 Dedicated HSM 界面创建专属加密实例。	用户
2	分配专属加密实例	Dedicated HSM 分配专属加密实例给用户。 安全专家将通过您提供的联系方式与您联系，并确定您订购的专属加密实例是否满足您的业务要求，若满足要求，安全专家将分配专属加密实例给您。	专属加密服务安全专家
3	邮寄 UKey 并提供配套初始化文档及软件	• 安全专家将通过您提供的 Ukey 收件地址将 Ukey 邮寄给您。 Ukey 是 Dedicated HSM 提供给您的身份识别卡，此卡仅购买专属加密实例的用户持有，请妥善保管。 • 安全专家将会为您提供初始化专属加密实例的软件及相关指导文档。 若您对软件或指导文档的使用有疑问，请联系安全专家进行指导。	专属加密服务安全专家
4	初始化、管控	1. 在专属加密实例管理节点上安装我们为您提供的管理工具。 2. 使用 Ukey 和管理工具初始化专属加密实例，并注册	用户

编号	操作步骤	说明	操作角色
	（UKey 认证）	相应的管理员，管控专属加密实例，对密钥进行管理。 详细操作请参见初始化专属加密实例。	
5	安装安全代理软件并授权	在业务 APP 节点上安装我们为您提供的安全代理软件并执行相关初始化操作。 详细操作请参见安装安全代理软件并授权。	用户
6	访问	业务 APP 通过 API 或者 SDK 的方式访问专属加密实例。	用户

2.2.2 创建专属加密实例

该任务指导您通过专属加密服务创建专属加密实例。

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  ，选择区域或项目。

步骤 3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”。

步骤 4 在左侧导航树中，选择“专属加密”，进入专属加密实例列表页面。

步骤 5 在界面右上角，单击“创建专属加密实例”。

步骤 6 在弹出的“创建专属加密实例”窗口中，选择“当前区域”和“可用区”。

步骤 7 填写网络信息。相关参数说明如表 2-11 所示。

表2-11 网络参数说明

参数名称	说明	取值样例
虚拟私有云	可以选择使用已有的虚拟私有云（Virtual Private Cloud，VPC）网络，或者单击“申请虚拟私有云”创建新的虚拟私有云。 更多关于虚拟私有云的信息，请参见《虚拟私有云用户指南》。	vpc-sec
安全组	界面显示专属加密实例已配置的安全组。选择专属加密实例的安全组后，该专属加密实例将受到该安全组访问规则的保护。 更多关于安全组的信息，请参见《虚拟私有云用户指南》。	sg-533c

参数名称	说明	取值样例
网卡	界面显示所有可选择的子网，系统自动分配一个未使用的 IP 地址。 更多关于子网的信息，请参见《虚拟私有云用户指南》。	subnet1（10.1..0.0/16）
实例名称	专属加密实例的名称。	DedicatedHSM

步骤 8 配置完成后，单击“确定”，页面右上角弹出“专属加密实例开始创建”，则说明系统开始创建专属加密实例。

用户可在专属加密实例列表中查看到创建的专属加密实例信息，默认状态为“创建中”。专属加密实例包含以下三种状态：

- 创建中：系统正在分配专属加密实例给用户，等待 5-10 分钟，可分配完成。
- 创建失败：资源不够或网络故障等原因可能导致创建专属加密实例失败。
- 运行中：系统给用户分配专属加密实例已完成，专属加密实例处于“运行中”。

----结束

2.2.3 查看专属加密实例

该任务指导用户通过专属加密的实例列表查看专属加密实例信息，包括专属加密实例的名称/ID、状态、服务版本、设备厂商、设备型号、IP 地址和创建时间。

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  ，选择区域或项目。

步骤 3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”。

步骤 4 在左侧导航树中，选择“专属加密”，进入专属加密实例列表页面。

步骤 5 在专属加密实例列表中，查看专属加密实例信息。

专属加密实例列表参数说明，如表 2-12 所示。

表2-12 专属加密实例参数说明

参数	参数说明
名称/ID	专属加密实例的名称和 ID。
状态	专属加密实例的状态： • 创建中 用户创建的专属加密实例后，系统正在分配专属加密实例给用

参数	参数说明
	户，专属加密实例处于“创建中”状态。 • 创建失败 资源不够或网络故障等原因可能导致创建专属加密实例失败，专属加密实例处于“创建失败”状态。 • 运行中 系统已将专属加密实例分配给用户，专属加密实例处于“运行中”状态。 • 冻结 用户购买的专属加密实例到期，且没有续费，专属加密实例处于“冻结”状态。
服务版本	铂金版：用户独享硬件加密机机框、电源资源，独享硬件加密机网络带宽、接口资源。
可用区	显示设备的可用区域。
设备厂商	设备厂商的名称，包含“江南天安”和“三未信安”。
设备型号	设备型号。
IP 地址	专属加密实例的浮动 IP 地址。
创建时间	创建专属加密实例的时间。

步骤 6 用户可单击专属加密实例的名称，查看专属加密实例的详细信息。

专属加密实例详细信息参数说明，如表 2-13 所示。

表2-13 专属加密实例详细信息参数说明

参数	参数说明
名称	专属加密实例的名称。
ID	专属加密实例的 ID。
状态	专属加密实例的状态： • 创建中 用户创建的专属加密实例后，系统正在分配专属加密实例给用户，专属加密实例处于“创建中”状态。 • 创建失败 资源不够或网络故障等原因可能导致创建专属加密实例失败，专属加密实例处于“创建失败”状态。 • 运行中 系统已将专属加密实例分配给用户，专属加密实例处于“运行中”状态。

参数	参数说明
	• 冻结 用户购买的专属加密实例到期，且没有续费，专属加密实例处于“冻结”状态。
服务版本	铂金版：用户独享硬件加密机机框、电源资源，独享硬件加密机网络带宽、接口资源。
设备厂商	设备厂商的名称，包含“江南天安”和“三未信安”。
设备型号	设备型号。
虚拟私有云	专属加密实例所在虚拟私有云。 更多关于虚拟私有云的信息，请参见《虚拟私有云用户指南》。
子网	专属加密实例所在的子网。 更多关于子网的信息，请参见《虚拟私有云用户指南》。
IP	专属加密实例的浮动 IP 地址。
安全组	专属加密实例所在的安全组。 更多关于安全组的信息，请参见《虚拟私有云用户指南》。
可用区	专属加密实例所在的可用区。
创建时间	购买专属加密实例的时间。
到期时间	购买的专属加密实例到期的时间。
所属订单	购买专属加密实例的订单号，可单击订单号，查询订单详情。
计费模式	包年/包月计费。

----结束

2.2.4 使用专属加密实例

在您支付完成后，我们会根据您反馈的邮寄地址，将初始化专属加密实例的 Ukey 邮寄给您，请您耐心等待。同时，专属加密服务安全专家会通过您提供的联系方式，与您取得联系，将配套的软件及相关指导文档发送给您。软件分为两类，一类用于管理云加密实例；另一类是业务调用时依赖的安全代理软件和 SDK。

前提条件

在实例化专属加密实例后，用户需要获取以下信息，初始化专属加密实例、安装安全代理软件并授权。

表2-14 信息获取

名称	说明	来源
Ukey	保存专属加密实例的权限管理信息。	订单付款后，且实例化专属加密实例成功后，由专属加密服务邮寄到您的 Ukey 收件地址。
专属加密实例管理工具	配合 Ukey，远程管理专属加密实例。	安全专家会通过您提供的联系方式联系您，将配套的软件和相关指导文档发送给您。
专属加密实例配套文档	《专属加密实例用户手册》和《专属加密实例安装手册》。	
安全代理软件	与专属加密实例建立安全通道。	
SDK	用于提供专属加密实例的 API 接口，用户通过调用 SDK 与专属加密实例建立安全连接。	
专属加密实例管理节点（例如：ECS）	运行专属加密实例管理工具，与专属加密实例处于同一 VPC，并分配弹性 IP 地址用于远程连接。	
业务 APP 节点（例如：ECS）	运行安全代理软件和用户的业务 APP，与专属加密实例处于同一 VPC。	

初始化专属加密实例

说明

目前不支持 SSH 登录到 DHSM，需要通过专属加密实例管理工具管理 DHSM。

以使用 Windows 镜像的 ECS 作为专属加密实例管理节点为例，初始化专属加密实例操作步骤如下所示。

步骤 1 购买一台 Windows 镜像的 ECS 作为专属加密实例管理节点。

1. 登录管理控制台。
2. 单击页面左侧的 ☰，选择“计算 > 弹性云服务器”，进入弹性云服务器列表界面。
3. 单击“购买弹性云服务器”。
   - 区域、可用区：请与购买的专属加密实例保持一致。
   - 镜像：请选择 Windows 公共镜像。
   - VPC：请与专属加密实例所在 VPC 保持一致。
   - 弹性公网 IP：为方便在您本地实例化加密机，请绑定弹性公网 IP。

说明

待初始化专属加密实例完成后，您可以解绑弹性公网 IP。若后续有需要，可重复绑定、解绑操作。

- 其他参数请根据实际情况进行选择。

步骤 2 根据收到的专属加密实例管理工具及配套文档，初始化专属加密实例。

步骤 3 初始化完成后，可通过管理工具进行生成、销毁、备份、恢复秘钥等操作。

说明

初始化和管理过程中有任何问题，请咨询专属加密服务安全专家。

详细信息请参见专属加密实例配套文档《专属加密实例用户手册》和《专属加密实例安装手册》。

----结束

安装安全代理软件并授权

用户需要在业务 APP 节点上安装安全代理软件，使业务 APP 与专属加密实例建立安全通道。

步骤 1 在管理工具上下载访问专属加密实例的证书。

步骤 2 在业务 APP 节点上安装安全代理软件。

步骤 3 将证书导入到安全代理软件，授予业务 APP 访问专属加密实例的权限。

步骤 4 业务 APP 即可通过 SDK 或者 API 接口的方式访问专属加密实例。

说明

您可以在安全代理软件配置多个专属加密实例，实现负载均衡功能。

----结束

2.3 权限管理

2.3.1 创建用户并授权使用 DEW

如果您需要对您所拥有的 DEW 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，在您的帐号中，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 DEW 资源委托给更专业、高效的其他云帐号或者云服务，这些帐号或者云服务可以根据权限进行代运维。

如果帐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 DEW 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 2-4 所示。

前提条件

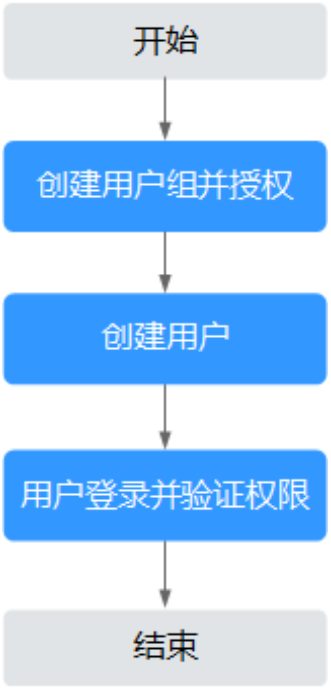
给用户组授权之前，请您了解用户组可以添加的 DEW 权限，并结合实际需求进行选择，DEW 支持的系统权限如表 2-15 所示。

表2-15 DEW 系统权限

系统角色/策略名称	描述	类别
KMS Administrator	加密密钥的管理员权限。	系统角色
KMS CMKFullAccess	加密密钥所有权限。	系统策略

示例流程

图2-4 给用户授权 DEW 权限流程



1. 在 IAM 控制台创建用户组，并授予加密密钥所有权限“KMS CMKFullAccess”。
2. 在 IAM 控制台创建用户，并将其加入 1 中创建的用户组。
3. 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。

2.3.2 DEW 自定义策略

如果系统预置的 DEW 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《数据加密服务接口参考》中“权限及授权项说明”章节。

目前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。本章为您介绍常用的 DEW 自定义策略样例。

DEW 自定义策略样例

- 示例：授权用户创建密钥

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:cmk:create",
                "kms:cmk:getMaterial",
                "kms:cmkTag:create",
                "kms:cmkTag:batch",
                "kms:cmk:importMaterial"
            ]
        }
    ]
}
```

- 示例：授权用户使用密钥

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:dek:crypto",
                "kms:cmk:get",
                "kms:cmk:crypto",
```

```
                "kms:cmk:generate",
                "kms:cmk:list"
            ]
        }
    ]
}
```

- 示例：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": [
                "rds:task:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:dek:crypto",
                "kms:cmk:get",
                "kms:cmk:crypto",
                "kms:cmk:generate",
                "kms:cmk:list"
            ]
        }
    ]
}
```

3 常见问题

3.1 密钥管理类

3.1.1 什么是密钥管理？

密钥管理，即密钥管理服务（Key Management Service, KMS），是一种安全、可靠、简单易用的密钥托管服务，帮助您轻松创建和管理密钥，保护密钥的安全。

KMS 通过使用硬件安全模块 HSM（Hardware Security Module, HSM）保护密钥的安全，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。

3.1.2 什么是用户主密钥？

用户主密钥（Customer Master Key，CMK），是用户或云服务通过密钥管理创建的密钥，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。

3.1.3 什么是默认主密钥？

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界面进行查询，不支持禁用、计划删除操作。

表3-1 默认主密钥列表

密钥别名	对应云服务
obs/default	对象存储服务（Object Storage Service，OBS）
evs/default	云硬盘（Elastic Volume Service，EVS）
ims/default	镜像服务（Image Management Service，IMS）
vbs/default	云硬盘备份（Volume Backup Service，VBS）

密钥别名	对应云服务
dlf/default	数据湖工厂服务（Data Lake Factory，DLF）
kps/default	密钥对管理服务（Key Pair Service，KPS）

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。

3.1.4 自定义密钥与默认主密钥有什么区别？

自定义密钥和默认主密钥的区别，如表 3-2 所示。

表3-2 自定义密钥和默认主密钥的区别

名称	概念	区别
自定义密钥	是用户自行通过 KMS 创建或导入的密钥，是一种密钥加密密钥，主要用于加密并保护 DEK。 一个用户主密钥可以加密多个 DEK。	支持禁用、计划删除等操作。
默认主密钥	是用户第一次通过对应云服务使用 KMS 加密时，系统自动生成的，其名称后缀为“/default”。 例如：evs/default	不支持禁用、计划删除等操作。

3.1.5 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。

3.1.6 为什么不能立即删除用户主密钥？

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。

3.1.7 哪些云服务使用 KMS 加密数据？

对象存储服务、云硬盘和镜像服务借助 KMS 实现了加密特性。

表3-3 使用 KMS 加密的云服务列表

服务名称	如何使用
对象存储服务	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 KMS 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《对象存储服务控制台指南》。
云硬盘	在创建云硬盘时，用户启用云硬盘的加密功能，系统将使用用户主密钥产生的数据密钥对磁盘进行加密，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》 。
镜像服务	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 KMS 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》 。
弹性文件服务	用户通过弹性文件服务创建文件系统时，选择 KMS 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。
云数据库 RDS	在购买数据库实例时，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。 用户如何使用云数据库 RDS 的磁盘加密功能，具体操作请参见。
文档数据库服务	在购买文档数据库实例时，用户启用文档数据库实例的磁盘加密功能，选择 KMS 提供的用户主密钥对文档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。 用户如何使用文档数据库的磁盘加密功能，具体操作请参见。

3.1.8 云服务如何使用 KMS 加密数据？

云服务（包含 OBS、IMS、EVS、SFS、DDS 和 RDS）使用 KMS 提供的信封加密方式来保护用户的数据。

说明

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。

- 用户通过云服务加密数据时，需要指定一个 KMS 用户主密钥。云服务会生成一个明文的数据加密密钥和一个密文的数据加密密钥，其中密文的数据加密密钥是由指定的用户主密钥加密明文的数据加密密钥生成的。云服务使用明文的数据加密密钥来加密数据，然后将加密后的密文数据与密文的数据加密密钥一同存储在云服务中。
- 用户通过云服务下载数据时，云服务通过 KMS 指定的用户主密钥对密文的数据加密密钥进行解密，并使用解密得到的明文的数据加密密钥来解密密文数据，然后将解密后的明文数据提供给用户下载。

3.1.9 信封加密方式有什么优势？

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。

信封加密方式优势如下：

- 相对于 KMS 提供的另一种加密方式：KMS 用户主密钥直接加密

  使用 KMS 用户主密钥直接加密：是通过 KMS 界面使用在线工具加解密数据，或者调用 KMS 的 API 接口使用指定的用户主密钥直接加密、解密数据。

  使用 KMS 用户主密钥直接加解密数据仅适用于不大于 4KB 的小数据加解密场景；而信封加密方式可以在本地对大量数据进行加解密。

  信封加密方式加解密数据，只需要传输数据加密密钥到 KMS 服务端，无需通过网络传输大量数据。
- 相对于直接加解密的云服务
  - 安全性

    由云服务直接为用户加解密数据：通过因特网将敏感信息从客户手中传递到服务的过程中会存在诸多风险，例如：窃听、钓鱼。

    信封加密方式：KMS 通过使用硬件安全模块 HSM 保护密钥的安全，所有的用户密钥都由 HSM 中的根密钥保护，避免密钥泄露。
  - 信任和可信证明

    由云服务直接为用户加解密数据：信任和可信证明较难做。用户不一定信任云服务，愿意上传如此敏感的数据；云服务也难以证明自己不会误用和泄露这些数据。

    信封加密方式：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。
  - 性能、成本

    由云服务直接为用户加解密数据：大量数据需要通过安全信道传递到服务端，加密后再返回给用户，这一过程，对用户服务的性能影响很大。另外，大量的移动数据会带来巨大的成本。

    信封加密方式：可以通过 KMS 的密码运算 API 在线生成数据密钥，用离线数据密钥在本地加密大量数据。

3.1.10 在 KMS 中创建的用户主密钥的个数是否有限制？

有。

用户最多可以创建 20 个用户主密钥。启用、禁用和计划删除状态的用户主密钥都会被计入该限制，默认主密钥不计入该限制。

3.1.11 是否可以从 KMS 中导出用户主密钥？

不可以。

为确保用户主密钥的安全，用户只能在 KMS 中创建和使用用户主密钥，无法导出用户主密钥。

3.1.12 如果用户主密钥被彻底删除，用户数据是否还可以解密？

不可以。

若用户主密钥被彻底删除，KMS 将不再保留任何该密钥的数据，使用该密钥加密的数据将无法解密；若用户主密钥没有被彻底删除，则可以通过 KMS 界面取消删除用户主密钥。

若用户主密钥是通过 KMS 导入的密钥，且仅删除了密钥材料，则可以将本地备份的密钥材料再次导入原来的空密钥，回收用户数据。若密钥材料没有在本地备份，则无法回收用户数据。

3.1.13 如何使用在线工具加解密数据？

使用在线工具加解密小数据的操作步骤如下所示：

加密数据

步骤 1 登录管理控制台。

步骤 2 单击管理控制台左上角  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 单击目标自定义密钥的别名，进入密钥详细信息在线工具加密数据页面。

步骤 5 在“加密”文本框中输入待加密的数据。

步骤 6 单击“执行”，右侧文本框显示加密后的密文数据。

说明

- 加密数据时，使用当前指定的密钥加密数据。
- 用户可单击“清除”，清除已输入的数据。
- 用户可单击“复制到剪切板”拷贝加密后的密文数据，并保存到本地文件中。

----结束

解密数据

步骤 1 登录管理控制台。

步骤 2 单击管理控制台左上角  ，选择区域或项目。

步骤 3 单击“服务列表”，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤 4 解密数据时，可单击任意“启用”状态的非默认密钥别名，进入该密钥的在线工具页面。

步骤 5 单击“解密”，在左侧文本框中数据待解密的密文数据。

说明

- 在线工具自动识别并使用数据被加密时使用的密钥解密数据。
- 若该密钥已被删除，会导致解密失败。

步骤 6 单击“执行”，右侧文本框中显示解密后的明文数据。

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

3.1.14 是否可以更新 KMS 管理的密钥？

不可以。

通过 KMS 创建的密钥无法更新，用户只能通过 KMS 创建新密钥，使用新的密钥加解密数据。

3.1.15 在什么场景下推荐使用导入的密钥？

- 如果用户不想使用 KMS 中创建的密钥材料，而使用自己的密钥材料，并且可以随时删除密钥材料，或者密钥材料被意外删除，用户可以重新导入相同的密钥材料的情况下，推荐用户使用导入的密钥。
- 当用户把本地的加密数据迁移到云上时，想在云上云下共用一个密钥材料时，可以把云下的密钥材料导入到 KMS。

3.1.16 可以导入哪些类型的密钥？

用户可以导入 256 位对称密钥。

3.1.17 密钥材料被意外删除时如何处理？

如果密钥材料被意外删除，用户可以在原用户主密钥下将备份的密钥材料重新导入 KMS。

须知

导入密钥材料时需要及时备份，重新导入的密钥材料必须与被意外删除的密钥材料保持一致，否则导入会失败。

3.1.18 KMS 支持的密钥算法类型

表3-4 KMS 支持的密钥算法类型

密钥类型	算法类型	密钥规格	说明	用途
对称密钥	AES	AES_256	AES 对称密钥	小量数据的加解密或用于加解密数据密钥。
对称密钥	SM4	SM4	国密 SM4 对称密钥	小量数据的加解密或用于加解密数据密钥。
非对称密钥	RSA	• RSA_2048 • RSA_3072 • RSA_4096	RSA 非对称密钥	小量数据的加解密或数字签名。
	ECC	• EC_P256 • EC_P384	椭圆曲线密码，使用 NIST 推荐的椭圆曲线	数字签名
非对称密钥	SM2	SM2	国密 SM2 非对称密钥	小量数据的加解密或数字签名。

3.1.19 调用 encrypt-data 接口，返回的密文和明文有什么关系？

encrypt-data 接口返回的密文数据基础长度为 124 字节。密文数据由“密钥 ID”、“加密算法”、“密钥版本”、“密文摘要”等字段拼接组成。

明文按照每个分组 16 个字节进行处理，不足 16 字节的，补码至 16 字节。所以密文长度为 124+Ceil(明文长度/16)*16，并将结果进行 Base64 编码。

以 4 字节明文输入为例，先计算结果 124+Ceil(4/16)*16=140。140 字节进行 Base64 编码后为 188 字节。

说明

Ceil 为向上取整函数。 Ceil(a) = 1, a∈(0,1]。

3.2 专属加密类

3.2.1 什么是专属加密？

专属加密（Dedicated Hardware Security Module，Dedicated HSM）是一种云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。

Dedicated HSM 为您提供的加密硬件，帮助您保护弹性云服务器上数据的安全性与完整性，满足 FIPS 140-2 安全要求。同时，您能够对专属加密实例生成的密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。

3.2.2 专属加密如何保障密钥生成的安全性？

- 密钥是由用户自己远程创建，且创建过程需要仅用户持有的 Ukey 参与认证。
- 加密机的配置和内部密钥的准备，都必须要使用这一组 Ukey 作为鉴权凭证才能操作。

用户作为设备使用者完全控制密钥的产生、存储和访问授权，Dedicated HSM 只负责监控和管理设备及其相关网络设施。

3.2.3 机房管理员是否有超级管理权限，在机房插入特权 Ukey 窃取信息？

机房管理员没有超级管理权限，Ukey 是 Dedicated HSM 提供给您的身份识别卡，此卡仅创建专属加密实例的用户持有。

敏感数据（密钥）存储在硬件加密卡中，即使加密机制造商也无法读取内部密钥信息。

A 修订记录

表A-1

发布日期	修改说明
2023-05-24	第二次发布。 新增“计费说明”章节。
2019-09-09	第一次发布。