数据加密服务

用户指南

文档版本 01

发布日期 2023-12-30

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2024。 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


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云计算技术有限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，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

 版权所有 © 华为云计算技术有限公司

 版权所有 © 华为云计算技术有限公司

 版权所有 © 华为云计算技术有限公司

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）、凭据管理（CSMS），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，HSM模块满足FIPS 140-2 Level 3安全要求。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。
云凭据管理服务 （Cloud Secret Management Service，CSMS）	凭据管理是一种安全、可靠、简单易用的凭据托管服务。 用户或应用程序通过凭据管理服务，创建、检索、更新、删除凭据，轻松实现对敏感凭据的全生命周期和统一管理，有效避免程序硬编码或明文配置等问题导致的敏感信息泄密以及权限失控带来的业务风险。

版权所有 © 华为云计算技术有限公司

1.2 基本概念

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

表 1-2 通用加密术语

名称	定义
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。

表 1-3 密钥管理服务术语

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。 用户主密钥分为自定义密钥和默认密钥。
默认密钥（Default Key）	默认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）。

版权所有 © 华为云计算技术有限公司

名称	定义
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。

1.3 密钥管理

1.3.1 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。并且HSM模块满足FIPS 140-2 Level 3安全要求。

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
  - 创建、撤销、查询授权
- 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加解密算法。KMS创建的非对称密钥支持RSA、ECC算法。

 版权所有 © 华为云计算技术有限公司

表 1-4 KMS 支持的密钥算法类型

密钥类型	算法类型	密钥规格	说明	适用场景
对称密钥	AES	AES_256	AES对称密钥	• 数据的加解密 • 加解密数据密钥 **说明** 小量数据的加解密可通过控制台在线工具进行。 大量数据的加解密需要调用API接口进行。
非对称密钥	RSA	• RSA_2048 • RSA_3072 • RSA_4096	RSA非对称密钥	• 数字签名和验签 • 数据的加解密 **说明** 非对称密钥适用于签名和验签场景，加密数据效率不高，加解密数据推荐使用对称密钥。
	ECC	• EC_P256 • EC_P384	椭圆曲线密码，使用NIST推荐的椭圆曲线	数字签名和验签

通过外部导入的密钥支持的密钥包装加解密算法如**表 密钥包装算法说明**所示。

表 1-5 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。

1.3.2 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。
- 与CTS服务集成，用户可以通过CTS服务查看近期KMS的操作记录。

版权所有 © 华为云计算技术有限公司

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。

高易用性

无需购买硬件加密设备，通过控制台或者API的方式实现密钥易用、易管理。

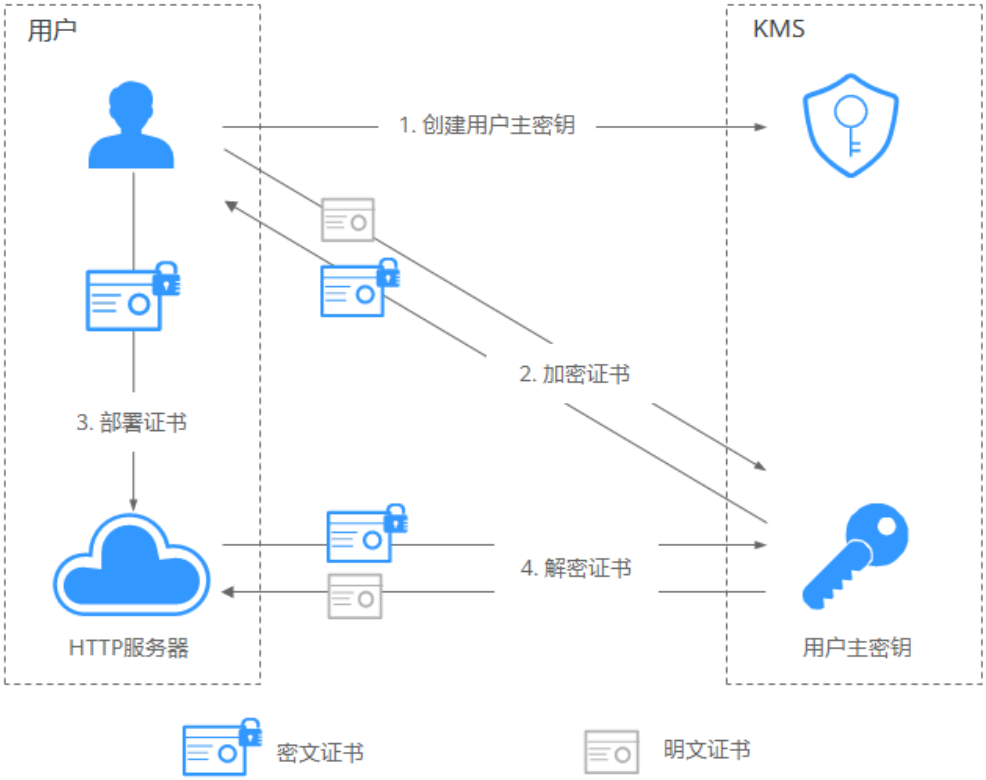
1.3.3 使用场景

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。

版权所有 © 华为云计算技术有限公司

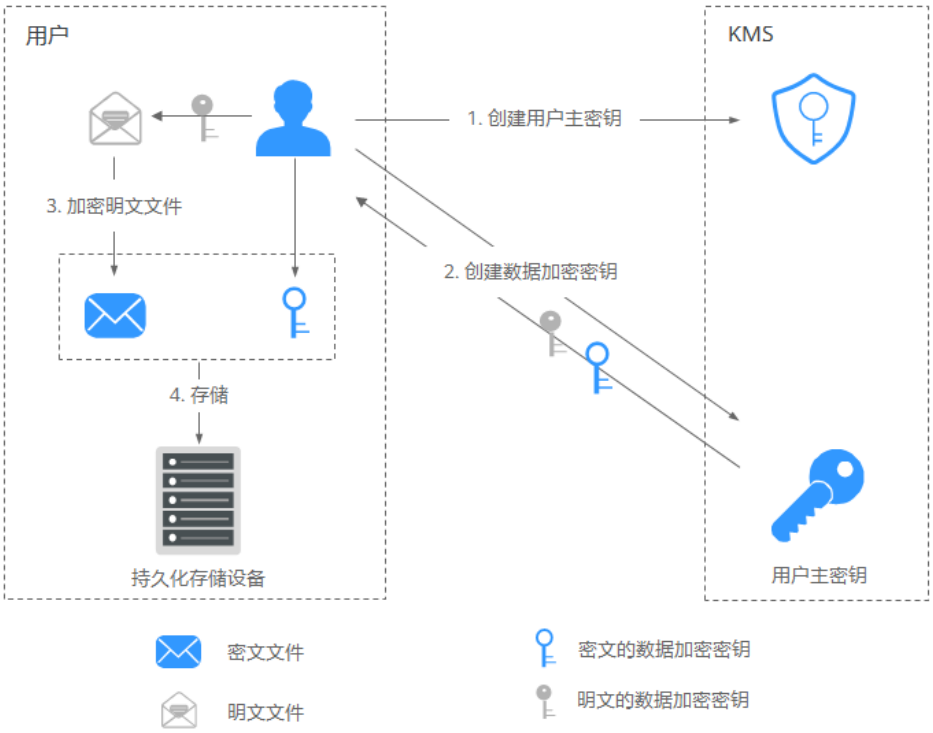
4. 当服务器需要使用证书时，调用KMS的“decrypt-data”接口，将密文证书解密为明文证书。

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**自定义密钥**加密**明文的数据加密密钥**生成的。

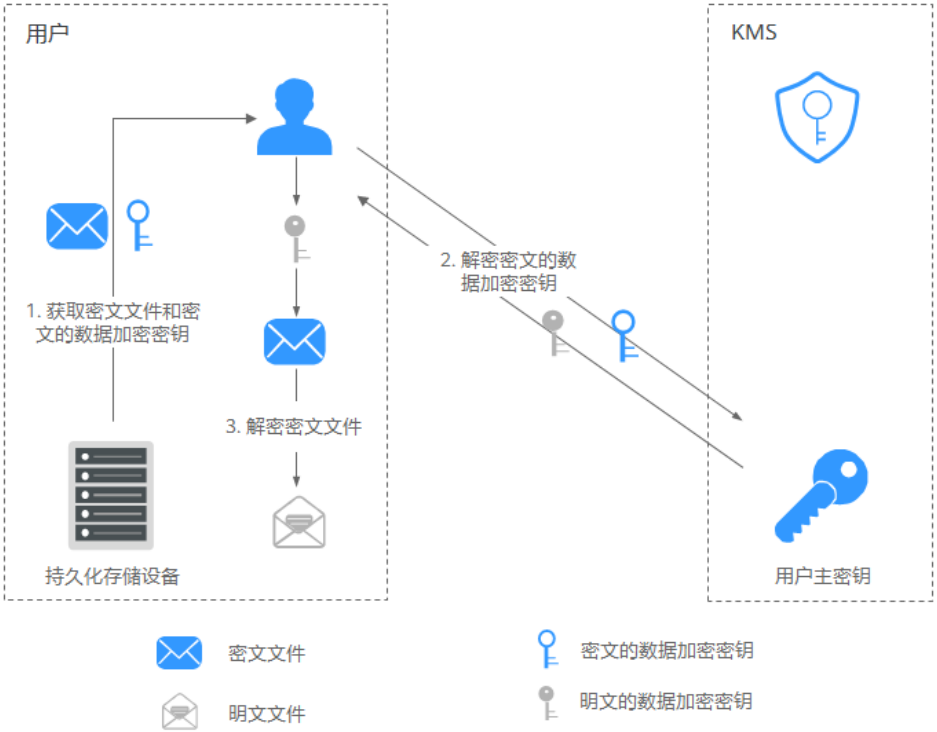
c. 用户使用明文的数据加密密钥来加密明文文件，生成密文文件。

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。

版权所有 © 华为云计算技术有限公司

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。

   如果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。

1.3.4 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。由用户管理自己的自定义密钥，云服务在拥有用户授权的情况下，使用用户指定的自定义密钥对数据进行加密。

加密流程说明如下：

1. 用户需要在KMS中创建一个自定义密钥。
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。

版权所有 © 华为云计算技术有限公司

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指定的自定义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 1-6 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《弹性文件服务用户指南》。
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《云数据库RDS用户指南》。
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《文档数据库服务用户指南》。

版权所有 © 华为云计算技术有限公司

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”接口创建一个自定义密钥。
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》。

1.3.5 使用 KMS 加密的云服务

1.3.5.1 OBS 服务端加密

- 用户使用OBS（Object Storage Service，OBS）服务端加密方式上传时，可以选择“SEE-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《对象存储服务用户指南》。

  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密钥“obs/default”。
  - 用户通过KMS界面创建的自定义密钥。
- 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》。

1.3.5.2 EVS 服务端加密

- 用户创建磁盘时，可以选择“高级配置 > 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密钥“evs/default”。
  - 用户通过KMS界面创建的自定义密钥。

版权所有 © 华为云计算技术有限公司

- 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 》。

1.3.5.3 IMS 服务端加密

- 用户使用OBS桶中已上传的外部镜像文件创建私有镜像时，可以选择“KMS加密”，使用KMS提供的密钥来加密镜像，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密钥“ims/default”。
  - 用户通过KMS界面创建的自定义密钥。
- 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 》。

1.3.5.4 SFS 服务端加密

- 用户通过弹性文件服务（ Scalable File Service，SFS ）创建文件系统时，可以选择“KMS加密”，使用KMS提供的密钥来加密文件系统。更多信息请参见《 弹性文件服务用户指南 》。

  用户可选择通过KMS界面创建的自定义密钥进行加密。
- 用户也可以通过调用SFS API接口创建加密的文件系统，详情请参考《 弹性文件服务API参考 》。

1.3.5.5 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 》。

  用户可选择通过KMS界面创建的自定义密钥进行加密。
- 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 》。

1.3.5.6 DDS 服务端加密

- 用户在通过文档数据库服务（ Document Database Service，DDS ）创建文档数据库实例选择自定义购买时，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 》。

  用户可选择通过KMS界面创建的自定义密钥进行加密。
- 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 》。

1.4 凭据管理

1.4.1 功能特性

凭据管理，即云凭据管理服务（ Cloud Secret Management Service，CSMS ），是一种安全、可靠、简单易用的凭据托管服务。用户或应用程序通过凭据管理服务，创

版权所有 © 华为云计算技术有限公司

建、检索、更新、删除凭据，轻松实现对敏感凭据的全生命周期的统一管理，有效避免程序硬编码或明文配置等问题导致的敏感信息泄露以及权限失控带来的业务风险。

凭据统一管理

应用系统中存在大量的敏感凭据信息，且分散到不同业务部门及系统，管理混乱，缺乏集中管理工具。

通过凭据管理服务对敏感凭据进行统一的存储、检索、使用等全生命周期管控。

解决方案说明如下：

1. 用户或管理员对应用敏感凭据进行收集。
2. 将收集的敏感凭据上传托管到凭据管理服务。

凭据安全检索

应用程序访问数据库或其他服务时，需要提供如密码、令牌、证书、SSH 密钥、API 密钥等各种类型的凭据信息进行身份校验，通常是直接使用明文方式将上述凭据嵌入在应用程序的配置文件中。该场景存在凭据信息硬编码、明文存储易泄露和安全性较低等风险问题。

通过凭据管理服务，用户可以将代码中的硬编码替换为对API 的调用，以便用编程的方式动态查询凭据，由于该凭据中不包含敏感信息，保证凭据不被泄露。

解决方案说明如下：

应用读取配置时，调用凭据管理服务API检索读取凭据（代替硬编码和明文凭据）。

凭据管理基本功能

表 1-7 凭据管理基本功能

功能	服务内容
凭据全生命周期管理	● 创建、查看、定时删除、取消删除凭据 ● 修改凭据的加密密钥和描述信息
凭据版本管理	● 创建、查看凭据版本 ● 查看凭据值
凭据版本状态管理	更新、查询、删除凭据版本状态
凭据标签管理	添加、搜索、编辑、删除标签

1.4.2 产品优势

凭据加密保护

凭据通过集成KMS进行加密存储，加密密钥基于第三方认证的硬件安全模块（HSM）来生成和保护。凭据检索时，通过 TLS 安全传输到服务器本地。

版权所有 © 华为云计算技术有限公司

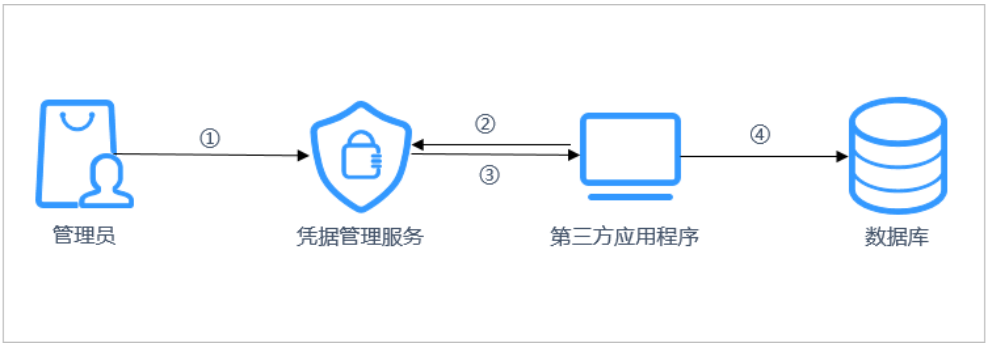
凭据安全检索

使用CSMS服务，将应用程序代码中的硬编码凭据替换为对凭据的API调用，以便以编程方式动态检索和管理凭据，实现凭据安全管理。同时对分散在各个应用程序中的敏感凭据统一集中管理，降低暴露风险。

1.4.3 使用场景

以最基础的数据库用户名及密码管理为示例，为您介绍凭据管理服务基本的使用场景。

图 1-4 凭据登录流程



流程说明如下：

步骤1 您首先需要在凭据管理服务中使用控制台或者API创建一个凭据，用来存储数据库的相关信息（例如：数据库地址、端口、密码）。

步骤2 当您使用应用程序访问数据库时，凭据管理服务会去查询步骤1所创建的凭据存储的内容。

步骤3 凭据管理服务检索并解密凭据密文，将凭据中保存的信息通过凭据管理API安全地返回到应用程序中。

步骤4 应用程序获取到解密后的凭据明文信息，使用这些安全的信息访问数据库。

----结束

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，您可以在账号中给员工创建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。

如果系统账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。

版权所有 © 华为云计算技术有限公司

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1-8所示，包括了DEW的所有系统权限。

表 1-8 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 CMK Admin	加密密钥所有权限	系统策略

表1-9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 1-9 常用操作与系统权限的关系

操作	KMS Administrator
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	√

版权所有 © 华为云计算技术有限公司

操作	KMS Administrator
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	√
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	√

 版权所有 © 华为云计算技术有限公司

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。如果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

- 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。

与云数据库关系型数据库的关系

云数据库关系型数据库（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关系型数据库服务。

版权所有 © 华为云计算技术有限公司

KMS为RDS提供用户主密钥管理控制能力，应用于云数据库关系型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。

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 1-10 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
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
创建授权	cmk	createGrant
退役授权	cmk	retireGrant

版权所有 © 华为云计算技术有限公司

操作名称	资源类型	事件名称
撤销授权	cmk	revokeGrant
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
创建凭据	csms	createSecret
更新凭据	csms	updateSecret
删除凭据	csms	forceDeleteSecret
计划删除凭据	csms	scheduleDelSecret
取消计划删除凭据	csms	restoreSecretFromDeletedStatus
创建凭据状态	csms	createSecretStage
更新凭据状态	csms	updateSecretStage
删除凭据状态	csms	deleteSecretStage
创建凭据版本	csms	createSecretVersion
下载凭据备份	csms	backupSecret
恢复凭证备份	csms	restoreSecretFromBackupBlob

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》。

版权所有 © 华为云计算技术有限公司

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1-11**所示：

表 1-11 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。

版权所有 © 华为云计算技术有限公司

2 用户指南

2.1 密钥管理

2.1.1 密钥概述

用户主密钥包括自定义密钥和默认密钥。本章节涉及创建、查看、启用、禁用、计划删除、取消删除等操作均为自定义密钥。

自定义密钥分为“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，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。
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

版权所有 © 华为云计算技术有限公司

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。

自定义密钥包括“对称密钥”和“非对称密钥”。

前提条件

账号拥有KMS CMKFullAccess及以上权限。

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算法密钥，AES-256密钥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。
- 云数据库中数据库实例的磁盘加密。
- 自定义密钥直接加解密小数据。
- 用户应用程序的DEK加解密。
- 消息认证码生成与校验。
- 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 单击页面左侧 ☰，选择“安全 > 数据加密服务”，默认进入“密钥管理”界面。

步骤3 单击界面右上角“创建密钥”。

步骤4 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。

 版权所有 © 华为云计算技术有限公司

- 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。
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

- 密钥用途：可选择“SIGN_VERIFY”、“ENCRYPT_DECRYPT”、“GENERATE_VERIFY_MAC”。
  - 对于AES_256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”。

  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。

  说明

  支持长度为1 ~ 255个字符。
- 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5 （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

- 当用户在创建密钥完成后，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。

版权所有 © 华为云计算技术有限公司

步骤6 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。
- 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。

 版权所有 © 华为云计算技术有限公司

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。 • 不支持密钥轮换功能。 • 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。 • 仅对称密钥支持密钥轮换功能。 • 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。

2.1.3.2 导入密钥材料

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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击“导入密钥”，弹出“导入密钥”对话框。

步骤3 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。

- 密钥算法：选择密钥算法。KMS支持的密钥算法说明如表2-4所示。

 版权所有 © 华为云计算技术有限公司

表 2-4 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。
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

- 密钥用途：可选择“SIGN_VERIFY”、“ENCRYPT_DECRYPT”、“GENERATE_VERIFY_MAC”。
  - 对于AES_256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”。

  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。

  说明

  支持长度为1 ~ 255个字符。

步骤4 （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。如果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5 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6 单击“下一步”，进入“获取包装密钥和导入令牌”页面。根据选择密钥包装算法。

 版权所有 © 华为云计算技术有限公司

表 2-5 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。

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7 获取“包装密钥”和“导入令牌”，并加密密钥材料，如果您已有密钥材料，可跳过本步骤。

1. 获取“包装密钥”和“导入令牌”。
   - 方法一：单击“下载并继续”，下载的文件为包装密钥，如图 下载文件所示。

     图 2-1 下载文件

     - 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：引导程序自动传递导入令牌，无需下载，如果中途退出引导程序，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，如果创建密钥过程中，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。

 版权所有 © 华为云计算技术有限公司

- 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

如果用户需要使用**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：

版权所有 © 华为云计算技术有限公司

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。

如果“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 2-6 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**

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 pkcs1_rsa_private_key.pem 4096

  2) 格式转换成pkcs8格式

     openssl pkcs8 -topk8 -inform PEM -in pkcs1_rsa_private_key.pem -outform pem -nocrypt -out rsa_private_key.pem

  3) pkcs8格式转换成der格式

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

  4) 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8 已有密钥材料时，单击“已有密钥材料”，进入“导入密钥材料”页面。

 版权所有 © 华为云计算技术有限公司

表 2-7 导入密钥材料参数说明（对称密钥场景）

参数	说明
密钥ID	创建密钥时，随机生成的密钥ID。
密钥材料	导入密钥材料。 例如：使用**步骤7.2.b**中“EncryptedKeyMaterial.bin”文件。

表 2-8 导入密钥材料参数说明（非对称密钥场景）

参数	说明
密钥ID	创建密钥时，随机生成的密钥ID。
临时密钥材料	选择导入临时密钥材料。 例如：选择**步骤7.2.b**中“EncryptedKeyMaterial.bin”文件。
私钥密文	选择导入私钥密文。 例如：选择**步骤7.2.c**中“out_rsa_private_key.der”文件。

步骤9 单击“下一步”，进入“密钥导入令牌”页面。根据**表2-9**设置参数。

表 2-9 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10 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

版权所有 © 华为云计算技术有限公司

2.1.3.3 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，如果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，如果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**删除密钥**功能。

操作步骤

步骤1 登录管理控制台。

步骤2 在需要删除的密钥材料所在行，单击“删除密钥材料”。

步骤3 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。

版权所有 © 华为云计算技术有限公司

步骤2 在密钥列表中，查看密钥信息，密钥列表参数说明。

表 2-10 密钥列表参数说明

参数	操作说明
别名/ID	密钥的别名以及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。
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”。
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： ● 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。
企业项目	创建密钥时，给密钥绑定企业项目ID。
操作	用户可以在操作栏中，执行禁用、删除、分配至项目、导入密钥材料、取消删除密钥等操作。

步骤3 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。

版权所有 © 华为云计算技术有限公司

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 在需要启用的密钥所在行，单击“启用”。

步骤3 在弹出窗口中，单击“确定”，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**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 在需要禁用的密钥所在行，单击“禁用”。

步骤3 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“确定”，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。

- 检查CMK权限以确定潜在使用范围，详细操作请参见**查询授权**。
- 检查审计日志以确定实际使用情况。

版权所有 © 华为云计算技术有限公司

前提条件

- 待删除的密钥需处于“启用”、“禁用”或“等待导入”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，如果需要重新使用该密钥，可以执行取消删除密钥操作。如果超过推迟时间，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 在需要删除的密钥所在行，单击“删除”,，进入“删除密钥”界面。

步骤3 在“删除密钥”界面，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，如果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4 勾选“我已知晓删除以上密钥产生的影响”。单击“是”“确定”，完成删除单个密钥操作。

----结束

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”。

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 在需要取消删除的密钥所在行，单击“取消删除”。

版权所有 © 华为云计算技术有限公司

步骤3 在弹出的窗口中，单击“确定”，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**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**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**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

2.1.4.6 分配至企业项目

企业项目为用户提供企业组织架构以及和业务管理模型匹配的云治理平台，帮助企业以公司、部门、项目等组织架构分级管理和项目业务结构来实现企业在云上的管理，提供企业项目管理、资源管理、人员管理、财务管理、应用管理能力。

如果您开通了企业项目管理，可以通过密钥管理界面对指定的自定义密钥分配至企业项目。

约束条件

- 已开通企业项目管理。

  未开通企业项目管理的用户，或者权限为非企业账号的用户，控制台默认不显示“企业项目”选项，不涉及“分配至企业项目”功能。
- 默认密钥不支持切换企业项目。

操作步骤

步骤1 登录管理控制台。

步骤2 在目标密钥所在行，单击“分配至项目”，弹出对话框。

说明

如果用户为非企业用户，操作列不显示“分配至项目”按钮。

步骤3 在弹出的对话框中，选择迁入项目。

步骤4 单击，完成操作。

----结束

2.1.5 搜索密钥

该任务指导用户在密钥管理界面，通过指定属性查找当前满足条件的自定义密钥。

操作步骤

步骤1 登录管理控制台。

版权所有 © 华为云计算技术有限公司

步骤2 单击搜索栏，选择筛选密钥的条件，通过指定属性搜索自定义密钥。

说明

- 可根据别名、密钥ID、状态、创建时间、密钥用途、密钥材料来源、企业项目进行筛选。

----结束

2.1.6 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。
- 在线工具不支持非对称密钥加解密小数据。
- 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API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3 在“加密”文本框中输入待加密的数据。

步骤4 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 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3 单击“解密”，在左侧文本框中数据待解密的密文数据。

版权所有 © 华为云计算技术有限公司

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。
- 如果该密钥已被删除，会导致解密失败。

步骤4 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。
- 在控制台输入的明文，会进行base64编码得到加密后的字符。

  如果直接调用API接口进行解密，得到的解密结果是进行了base64编码的内容。需再进行一次base64解码才能得到与控制台输入明文一致的内容。

----结束

2.1.7 管理标签

2.1.7.1 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 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤3 单击“标签”，进入标签管理页面。

步骤4 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2-11**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。

版权所有 © 华为云计算技术有限公司

表 2-11 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128个字符。 • 首尾不能包含空格。 • 可以包含以下字符： – 英文 – 数字 – 空格 – 特殊字符“_”、“-”、“@”	cost
标签值	标签的值。	• 可以为空。 • 长度不超过255个字符。 • 可以包含以下字符： – 英文 – 数字 – 空格 – 特殊字符“_”、“-”、“@”	100

步骤5 单击“确定”，完成标签的添加。

----结束

2.1.7.2 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 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤3 单击“标签”，进入标签管理页面。

步骤4 单击目标标签所在行的“编辑”，弹出编辑标签对话框。

步骤5 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

版权所有 © 华为云计算技术有限公司

2.1.7.3 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 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤3 单击“标签”，进入标签管理页面。

步骤4 单击目标标签所在行的“删除”，弹出删除标签对话框。

步骤5 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

2.1.8 轮换密钥

2.1.8.1 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

  方式一：创建一个新的密钥B，使用密钥B替换当前正在使用的密钥A。

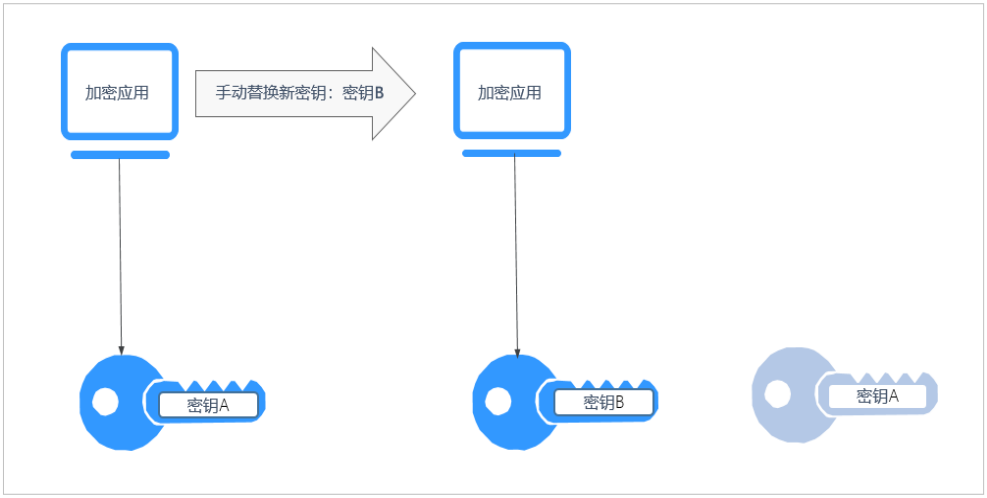
  方式二：对密钥A的密钥材料进行更改，继续使用密钥A。

  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。

版权所有 © 华为云计算技术有限公司

图 2-2 手动轮换密钥工作原理



- 自动轮换密钥

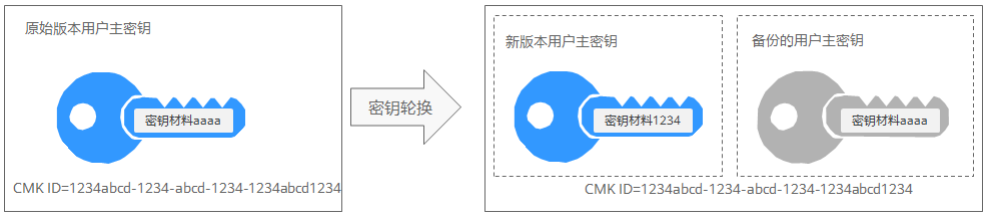
  KMS会根据设置的轮换周期（默认365天）自动轮换密钥，系统自动生成一个新的密钥B，并替换当前使用的密钥A。自动轮换密钥只会更改主密钥的密钥材料，即加密操作中所使用的加密材料。不管密钥材料有没有变更或变更了多少次，该主密钥仍是相同的逻辑资源。主密钥的属性（密钥ID、别名、描述、权限）不会发生变化。

  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 2-3 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。

版权所有 © 华为云计算技术有限公司

密钥支持的轮换方式

表 2-12 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	支持自动轮换密钥或手动轮换密钥，根据密钥算法类型决定。 ● 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**已禁用的主密钥**。
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**计划删除的主密钥**。

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。

2.1.8.2 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”。
- 仅对称密钥支持开启密钥轮换。

约束条件

- 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。
- 只有区域主密钥可以进行轮转，副本密钥不允许进行密钥密钥轮转。

版权所有 © 华为云计算技术有限公司

操作步骤

步骤1 登录管理控制台。

步骤2 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤3 单击“轮换策略”，进入“密钥轮换管理”页签。

步骤4 单击，将“密钥轮换”设置为，弹出“启用轮换策略”对话框。

步骤5 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，如果密钥使用频率高，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。

步骤6 开启后，页面显示密钥轮换详情，如图 密钥轮换详情所示。

图 2-4 密钥轮换详情

 版权所有 © 华为云计算技术有限公司

说明

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

2.1.8.3 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 单击目标对称密钥的别名，进入密钥详细信息页面。

步骤3 单击“轮换策略”，进入密钥轮换管理界面。

步骤4 单击 ，关闭密钥轮换。

步骤5 在弹出的确认是否关闭密钥轮换提示框中，单击“确认”。

步骤6 关闭后，页面将显示密钥轮换管理界面。

----结束

2.1.9 管理授权

2.1.9.1 创建授权

用户可以为其他IAM用户或账号创建授权，授予其使用自身的自定义密钥的权限，一个自定义密钥下最多可创建100个授权。

前提条件

- 已获取被授权IAM用户或账号的ID。
- 自定义密钥需处于“启用”状态。

约束条件

- 自定义密钥的所有者可通过KMS界面或者调用API接口的方式为自定义密钥创建授权；被自定义密钥所有者授予了“创建授权”操作权限的IAM用户或账号仅能通过调用API接口的方式为自定义密钥创建授权。
- 一个自定义密钥下最多可创建100个授权。
- 授权仅支持用户以及账户，不能针对委托进行授权。

 版权所有 © 华为云计算技术有限公司

操作步骤

步骤1 登录管理控制台。

步骤2 单击目标自定义密钥的别名，进入密钥详细信息授权页面。

步骤3 单击“授权”，进入授权管理界面。

步骤4 单击“创建授权”，弹出“创建授权”对话框。

步骤5 在弹出的对话框中，输入被授权用户ID，并勾选授权操作的权限。参数说明请参见**表2-13**。

须知

被授权用户只有通过调用API接口的方式，才能使用“授权操作”的权限，详细信息请参考《数据加密服务API参考》。

表 2-13 创建授权参数说明

参数	参数说明	配置样例
被授权对象	支持对用户和账号进行授权。 • 用户 用户ID：请填写在“用户名 > 我的凭证 > API凭证”中的“IAM用户ID”。 授权完成后，该IAM用户能使用授权中指定的密钥 • 账号 账号ID：请填写在“用户名 > 我的凭证 > API凭证”中的“账号ID”。 授权完成后，该账号下所有的IAM用户均能使用授权中指定的密钥。	d9a6b2bdaedd4ba586cabe6372d1b312

版权所有 © 华为云计算技术有限公司

参数	参数说明	配置样例
授权操作	用户可选择以下授权操作： **说明** • 一个自定义密钥可以多次授权给同一个用户不同的权限，用户最终的权限为所有授权的并集。 • 授权操作选项不能为空。 • 不能仅授予“创建授权”操作。 • 创建不含明文数据密钥 • 创建数据密钥 • 加密数据密钥 • 解密数据密钥 • 查询密钥信息 • 创建授权 • 退役授权 – 当被授权用户不再使用授权用户授予的自定义密钥的操作权限时，被授权用户可退役该授权。 – 如果被授权用户在退役授权前，已将自定义密钥的操作权限授予给其他用户，那么被授权用户退役授权后，对其他用户操作自定义密钥的权限无影响。 • 加密数据 • 解密数据	-

步骤6 单击“确定”，页面右上角弹出“授权创建成功”，则说明授权成功。

授权列表中可查看到“授权名称”、“授权类型”、“被授权ID”、“授权操作”和“创建时间”。

----结束

2.1.9.2 查询授权

该任务指导用户通过KMS界面查看自定义密钥的授权信息，包括授权ID、被授权ID、授权操作、创建时间等。

前提条件

用户已创建授权。

操作步骤

步骤1 登录管理控制台。

步骤2 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤3 单击“授权”，用户可查看当前自定义密钥的授权信息。自定义密钥的授权信息如表2-14所示。

 版权所有 © 华为云计算技术有限公司

表 2-14 授权信息参数说明

参数	参数说明
授权ID	随机生成的授权的唯一标识。
授权类型	授权类型：用户和账号。
授权操作	被授予用户对自定义密钥的操作权限（例如：创建数据密钥）。
创建时间	创建该授权的时间。
操作	用户可以在操作栏中，执行撤销授权操作。

----结束

2.1.9.3 撤销授权

在以下两种情况下，授权用户可以通过密钥管理界面撤销授权：

- 当被授权用户不再使用授权用户的自定义密钥时，被授权用户可告知授权用户撤销授权，或者通过API接口直接退役授权。
- 当授权用户想收回自定义密钥的操作权限时，授权用户可强制撤销授权。

撤销授权后，被授权用户不再持有被授予的权限，而撤销授权前被授权用户已授予给其他用户的权限不受影响。

该任务指导用户通过KMS界面撤销授权。

前提条件

用户已创建授权。

操作步骤

步骤1 登录管理控制台。

步骤2 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤3 在目标授权ID所在行，单击“撤销授权”。

步骤4 在弹出的对话框中单击“确认”，页面右上角弹出“授权撤销成功”，则说明撤销授权成功。

----结束

2.2 凭据管理

2.2.1 创建凭据

2.2.1.1 创建通用凭据

该任务指导用户通过凭据管理界面创建凭据。

版权所有 © 华为云计算技术有限公司

创建新的凭据，并将凭据值存入凭据的初始版本，初始版本的状态被标记为“SYSCURRENT”。

约束条件

- 用户最多可创建200个凭据。
- 默认使用凭据管理为您创建的默认密钥“csms/default”作为当前凭据的加密密钥。您也可以前往KMS服务页面创建自定义对称密钥，并使用自定义密钥加密。

创建凭据

步骤1 登录管理控制台。

步骤2 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤3 单击“创建凭据”。弹出“创建凭据”对话框，填写参数，参数说明如**表 凭据配置参数说明**所示。

表 2-15 凭据配置参数说明

参数名称	参数说明
凭据类型	创建凭据类型，默认通用凭据。
凭据名称	待创建凭据的名称。 **说明** 仅支持输入英文字符、数字、“-”、“_”。
企业项目	创建凭据时，凭据绑定企业项目ID。
设置凭据值	待加密的用户凭据键/值和明文凭据。
描述信息	凭据的描述信息。
KMS加密	可选择默认密钥“csms/default”或用户在KMS已创建的自定义密钥 **说明** • CSMS采用KMS提供的加密密钥对私钥进行加密，用户使用密钥对的KMS加密功能时，可选择KMS创建的默认密钥“csms/default”。 • 用户在KMS创建的自定义密钥，具体操作请参见。

步骤4 单击“下一步”，设置轮转周期。

步骤5 单击“下一步”，确认创建的信息。

步骤6 单击“确定”，凭据创建完成。

用户可在凭据列表查看已完成创建的凭据，凭据默认状态为“启用”。

----结束

2.2.2 管理凭据

版权所有 © 华为云计算技术有限公司

2.2.2.1 查看凭据

该任务指导用户通过凭据管理界面查看凭据的信息，包括凭据名称、状态和创建时间。凭据状态包括“启用”和“待删除”。

操作步骤

步骤1 登录管理控制台。

步骤2 在凭据列表中，查看凭据信息，凭据列表参数说明，如表2-16所示。

表 2-16 凭据列表参数说明

参数	操作说明
凭据名称/ID	凭据的名称。
状态	凭据的状态，包含启用和待删除。
凭据类型	凭据的类型，包含通用凭据。
创建时间	创建该凭据的时间。
企业项目	创建凭据绑定的企业项目ID
操作	用户可以在操作栏中，执行下载凭据备份、删除和撤销删除凭据等操作。

步骤3 用户可单击凭据名称，查看凭据详细信息。

说明

- 用户可单击“编辑”，修改凭据的“加密密钥”和“描述信息”。
- 单击“刷新”，刷新凭据信息。

----结束

2.2.2.2 删除凭据

在删除凭据前，您需要确保该凭据没有被使用或将来也不会被使用。

前提条件

待删除的凭据需处于“启用”状态。

约束条件

- “计划删除凭据”不会立即删除，凭据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～30天。在推迟删除时间未到时，如果需要重新使用该凭据，可以执行撤销删除凭据操作。如果超过推迟时间，凭据将被彻底删除，请谨慎操作。
- “立即删除”凭据，删除后如果需找回，需提前下载凭据备份用于恢复凭据，请谨慎操作。

版权所有 © 华为云计算技术有限公司

删除凭据

步骤1 登录管理控制台。

步骤2 在需要删除的凭据所在行，单击“删除”。

步骤3 在弹出的窗口中，选择“计划删除凭据”或“立即删除”。如果选择计划删除凭据，需填写“推迟删除”的时间。

步骤4 单击“确定”，完成删除凭据操作。

说明

- “计划删除凭据”不会立即删除，凭据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～30天。在推迟删除时间未到时，如果需要重新使用该凭据，可以执行撤销删除凭据操作。如果超过推迟时间，凭据将被彻底删除，请谨慎操作。
- “立即删除”凭据，删除后如果需找回，需提前下载凭据备份用于恢复凭据，请谨慎操作。

----结束

2.2.3 管理凭据版本

2.2.3.1 存入和查看凭据值

该任务指导用户通过凭据管理界面存入凭据值和查看凭据值。

在目标凭据中，存入凭据值即创建一个新的凭据版本，用于加密保管新的凭据值。默认情况下，新创建的凭据版本被标记为“SYSCURRENT”状态，而“SYSCURRENT”标记的前一个凭据版本被标记为“SYSPREVIOUS”状态。

约束条件

- 凭据管理服务的每个凭据中最多可支持20个版本。
- 每次存入新的凭据值时，凭据版本号按照为v1，v2，v3...的模式自动增加。

操作步骤

步骤1 登录管理控制台。

步骤2 单击凭据名称，进入凭据详细信息页面。

步骤3 在“版本列表”区，单击“存入凭据值”，弹出存入凭据值对话框。

步骤4 单击“确定”，在页面右上角弹出“版本凭据值添加成功”，则说明凭据值添加完成。

在凭据版本列表查看最新凭据值。

步骤5 在“版本列表”区，单击目标凭据版本所在行的“查看凭据值”，弹出查看凭据值对话框。

步骤6 查看凭据值，单击“确定”，关闭当前对话框。

----结束

版权所有 © 华为云计算技术有限公司

2.2.3.2 管理版本状态

该任务指导用户通过凭据管理界面，进行新增、更改和删除凭据版本状态的操作。

凭据管理服务将凭据值加密后，存储在凭据对象下的版本中。每个版本可与多个凭据版本状态相关联，凭据版本状态用于标识凭据版本处于的阶段，没有版本状态标记的版本视为已弃用，可用凭据管理服务自动删除。

约束条件

- 初始版本的状态被标记为“SYSCURRENT”。
- 您可以将凭据的版本状态标记上服务内创建或者自定义类型的状态标签。每个版本可以被标记上多个状态标签，但是每个状态标签只能标记一个版本。目标状态标签为凭据对象内已经存在的状态标签时，首先自动会将此状态标签从其它版本上移除，然后标记至目标版本上。
- 凭据管理服务的每个凭据中最多可支持12个凭据版本状态，每个凭据版本状态同时仅能标识一个凭据版本。
- “SYSCURRENT”和“SYSPREVIOUS”为服务内建的凭据状态，不可删除。

操作步骤

步骤1 登录管理控制台。

步骤2 单击凭据名称，进入凭据详细信息页面。

步骤3 在“版本列表”区，单击目标凭据版本所在行的“状态管理”。

步骤4 在“状态管理”对话框，用户可进行新增、更改、删除凭据版本状态的操作。

- 新增凭据版本状态

  在“状态管理”对话框，单击“新增”，填写“状态名称”。单击“确定”，完成凭据版本状态的新增。

  说明

  凭据管理服务的每个凭据中最多可支持12个凭据版本状态，每个凭据版本状态同时仅能标识一个凭据版本。

- 更改凭据版本状态

  在“状态管理”对话框，单击“更改”，在“已有版本状态”选择目标版本状态。单击“确定”，完成凭据版本状态的更改。

- 删除凭据版本状态

  在“状态管理”对话框，单击“删除”，在“当前版本状态”选择目标版本状态。单击“确定”，完成凭据版本状态的删除。

  说明

  “SYSCURRENT”和“SYSPREVIOUS”为服务内建的凭据状态，不可删除。

----结束

2.2.4 管理标签

 版权所有 © 华为云计算技术有限公司

2.2.4.1 添加标签

标签用于标识凭据。为凭据添加标签，可以方便用户对凭据进行分类和跟踪。

操作步骤

步骤1 登录管理控制台。

步骤2 单击凭据名称，进入凭据详细信息页面。

步骤3 在“标签”区，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2-17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 2-17 标签参数说明

参数	参数说明	取值要求
标签键	标签的名称。 同一个凭据，一个标签键只能对应一个标签值；不同的凭据可以使用相同的标签键。 用户最多可以给单个凭据添加20个标签。	• 必填。 • 对于同一个自定义密钥，标签键唯一。 • 长度不超过个字符。 • 首尾不能包含空格。 • 可以包含以下字符： – 中文 – 英文 – 数字 – 空格 – 特殊字符“_”、“-”、“@”
标签值	标签的值。	• 可以为空。 • 长度不超过个字符。 • 可以包含以下字符： – 中文 – 英文 – 数字 – 空格 – 特殊字符“_”、“-”、“@”

步骤4 单击“确定”，完成标签的添加。

----结束

版权所有 © 华为云计算技术有限公司

2.2.4.2 通过标签搜索凭据

该任务指导用户在凭据管理界面，通过标签搜索当前项目下满足标签搜索条件的凭据。

前提条件

已添加标签。

操作步骤

步骤1 登录管理控制台。

步骤2 单击“标签搜索”，展开搜索框。

步骤3 在搜索框中输入或选择“标签键”和“标签值”。

步骤4

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，如果进行多个标签组合搜索，则搜索结果的每个凭据均满足标签组合搜索条件。
- 如果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。
- 如果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

2.2.4.3 修改标签值

该任务指导用户通过凭据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 单击凭据名称，进入凭据详细信息页面。

步骤3 在“标签”区，单击目标标签所在行的“编辑”，弹出编辑标签对话框。

步骤4 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

2.2.4.4 删除标签

该任务指导用户通过凭据管理界面删除标签。

操作步骤

步骤1 登录管理控制台。

步骤2 单击凭据名称，进入凭据详细信息页面。

步骤3 在“标签”区，单击目标标签所在行的“删除”，弹出删除标签对话框。

版权所有 © 华为云计算技术有限公司

步骤4 在弹出的删除标签对话框中单击“确认”，完成标签的删除。

----结束

2.3 审计日志

2.3.1 支持云审计的操作列表

云审计服务记录数据加密服务相关的操作事件，如表2-18所示。

表 2-18 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
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
创建授权	cmk	createGrant
退役授权	cmk	retireGrant
撤销授权	cmk	revokeGrant
加密数据	cmk	encryptData
解密数据	cmk	decryptData
添加标签	cmk	createKeyTag
删除标签	cmk	deleteKeyTag

版权所有 © 华为云计算技术有限公司

操作名称	资源类型	事件名称
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
创建凭据	csms	createSecret
更新凭据	csms	updateSecret
删除凭据	csms	forceDeleteSecret
计划删除凭据	csms	scheduleDelSecret
取消计划删除凭据	csms	restoreSecretFromDeletedStatus
创建凭据状态	csms	createSecretStage
更新凭据状态	csms	updateSecretStage
删除凭据状态	csms	deleteSecretStage
创建凭据版本	csms	createSecretVersion
下载凭据备份	csms	backupSecret
恢复凭证备份	csms	restoreSecretFromBackupBlob

2.3.2 查询审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录：

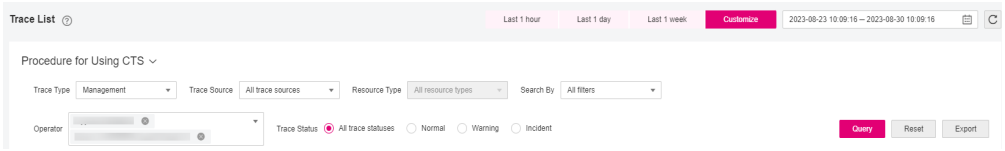
- **在事件列表查看审计事件**

在事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ☰，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过筛选来查询对应的操作事件，如**图2-5**所示。当前事件列表支持四个维度的组合查询，详细信息如下：

版权所有 © 华为云计算技术有限公司

图 2-5 筛选框

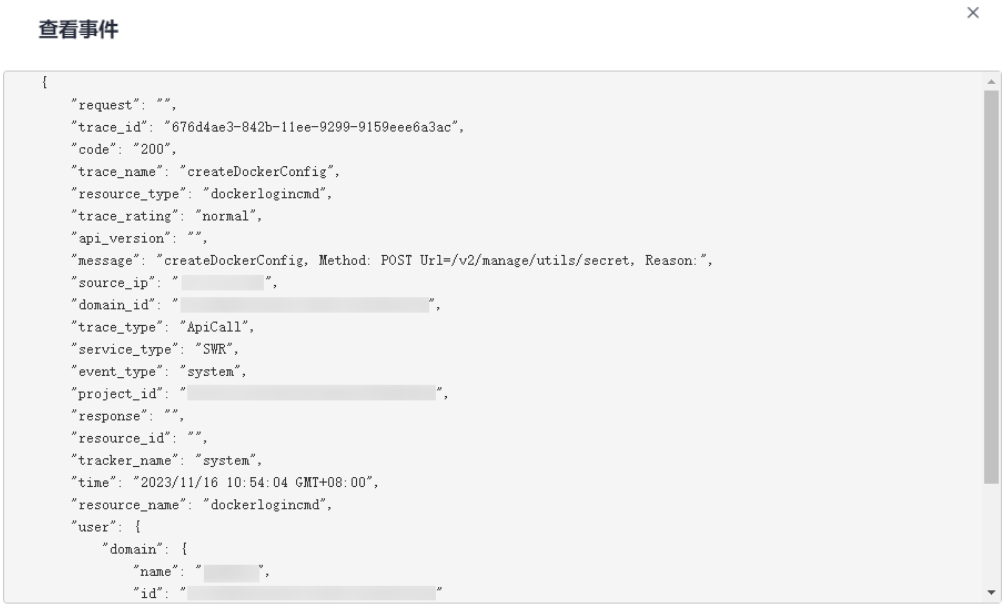


- 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
  - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
  - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
  - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
- 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
- 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
- 时间范围：可选择查询最近7天内任意时间段的操作事件。
- 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。

5. 选择完查询条件后，单击“查询”。
6. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
   - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击按钮，可以获取到事件操作记录的最新信息。
7. 在需要查看的事件左侧，单击 展开该记录的详细信息。

8. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。

版权所有 © 华为云计算技术有限公司



9. 关于事件结构的关键字段详解，请参见“云审计服务事件参考 > 事件结构”章节和“云审计服务事件参考 > 事件样例”章节。

2.4 权限管理

2.4.1 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DEW资源委托给更专业、高效的其他云账号或者云服务，这些账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2-6**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 系统权限**所示。

如果您需要对除KMS之外的其它服务授权，IAM支持服务的所有权限请参见。

表 2-19 DEW 系统权限

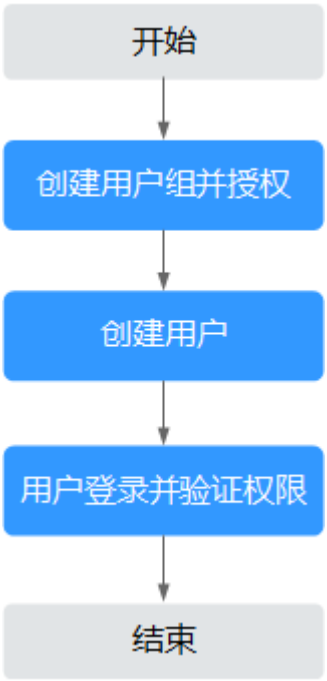
系统角色/策略名称	描述	类别
KMS Administrator	加密密钥的管理员权限。	系统角色

 版权所有 © 华为云计算技术有限公司

系统角色/策略名称	描述	类别
KMS CMK Admin	加密密钥所有权限	系统策略

示例流程

图 2-6 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 CMK Admin”。
2. 在IAM控制台创建用户，并将其加入1中创建的用户组。
3. 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。

2.4.2 DEW 自定义策略

如果系统预置的权限，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。

版权所有 © 华为云计算技术有限公司

  - “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：。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"
         ]
```

 版权所有 © 华为云计算技术有限公司

```
    }
  ]
}
```


版权所有 © 华为云计算技术有限公司

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。并且HSM模块满足FIPS 140-2 Level 3安全要求。

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。

用户主密钥分为自定义密钥和默认密钥。

- 自定义密钥

  用户通过密钥管理界面自行创建或导入的密钥。

- 默认密钥

  在用户第一次通过对应云服务使用KMS加密时，云服务自动通过密钥管理为用户创建的密钥，其别名后缀为“/default”。

  默认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）

 版权所有 © 华为云计算技术有限公司

密钥别名	对应云服务
evs/default	云硬盘（Elastic Volume Service，EVS）
ims/default	镜像服务（Image Management Service，IMS）
csms/default	云凭据管理服务（Cloud Secret Management Service，CSMS）

3.1.3 什么是默认密钥?

默认密钥，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密钥，其别名后缀为“/default”。

默认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。

默认密钥托管不计费，仅收取API请求次数费用，超出免费请求次数后，超出部分会进行计费。

表 3-2 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）
kps/default	密钥对管理服务（Key Pair Service，KPS）
csms/default	云凭据管理服务（Cloud Secret Management Service，CSMS）

说明

默认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 自定义密钥与默认密钥有什么区别?

自定义密钥和默认密钥的区别，如表 自定义密钥和默认密钥的区别所示。

 版权所有 © 华为云计算技术有限公司

表 3-3 自定义密钥和默认密钥的区别

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。 一个自定义密钥可以加密多个DEK。	• 支持禁用、计划删除等操作。 • 创建或导入成功后进行按需计费。
默认密钥	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 3-4 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》。

 版权所有 © 华为云计算技术有限公司

服务名称	如何使用
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《弹性文件服务用户指南》。
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《云数据库RDS用户指南》。
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《文档数据库服务用户指南》。

3.1.8 云服务如何使用 KMS 加密数据?

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。

版权所有 © 华为云计算技术有限公司

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 中创建的自定义密钥的个数是否有限制?

有。

用户最多可以创建100个自定义密钥。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 如果自定义密钥被彻底删除，用户数据是否还可以解密?

不可以。

如果自定义密钥被彻底删除，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；如果自定义密钥没有被彻底删除，则可以通过KMS界面取消删除自定义密钥。

如果自定义密钥是通过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。如果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：

 版权所有 © 华为云计算技术有限公司

加密数据

步骤1 登录管理控制台。

步骤2 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3 在“加密”文本框中输入待加密的数据。

步骤4 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

说明

在控制台输入的明文，会进行base64编码得到加密后的字符。

如果直接调用API接口进行解密，得到的解密结果是进行了base64编码的内容。需再进行一次base64解码才能得到与控制台输入明文一致的内容。

解密数据

步骤1 登录管理控制台。

步骤2 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3 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。
- 如果该密钥已被删除，会导致解密失败。

步骤4 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。
- 在控制台输入的明文，会进行base64编码得到加密后的字符。

  如果直接调用API接口进行解密，得到的解密结果是进行了base64编码的内容。需再进行一次base64解码才能得到与控制台输入明文一致的内容。

----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。

 版权所有 © 华为云计算技术有限公司

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，用户可以在原自定义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 默认密钥如何生成?

默认密钥是自动生成的。

在用户第一次通过对应云服务使用KMS加密时，云服务自动通过密钥管理为用户创建的密钥，其别名后缀为“/default”。

默认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 3-5 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）
csms/default	云凭据管理服务（Cloud Secret Management Service，CSMS）

3.1.19 没有权限操作 KMS，该如何处理?

问题描述

用户在KMS中执行查看密钥信息、创建密钥、导入密钥等操作时，显示无法操作KMS。

版权所有 © 华为云计算技术有限公司

可能原因

该用户没有KMS系统策略，导致没有权限操作KMS。

解决方法

步骤1 检查该用户是否具有KMS系统策略，KMS Administrator和KMS CMKFullAccess权限。

查看用户所属用户组以及用户组已有的权限。具体操作请参见。

如无KMS系统策略，则继续执行**步骤2**。

步骤2 如无系统策略，则为该用户添加系统策略。

- 如需添加管理员权限，则请参见进行处理。
- 如需添加自定义策略，则请参见进行处理。

----结束

3.1.20 如何修补 OpenSSL 以使用-id-aes256-wrap-pad 包装非对称密钥?

问题描述

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。

解决方法

按照以下说明，使用bash命令创建已有OpenSSL的本地副本，而无需删除或更改OpenSSL的客户端默认安装。

步骤1 以**root**用户完成以下操作步骤，以确保您对使用此命令的目录和二进制文件拥有正确的权限。

sudo su -

步骤2 运行此命令并记下OpenSSL版本。

openssl version

步骤3 在/root/build目录中下载最新的OpenSSL二进制文件。运行以下命令以设置目录。

mkdir $HOME/build

mkdir -p $HOME/local/ssl

cd $HOME/build

步骤4 记住从下载页面(https://www.openssl.org/source/)下载的最新OpenSSL版本。

步骤5 使用以下命令下载并解压缩二进制文件。

步骤6 将openssl-1.1.1d.tar.gz替换为**步骤4**中的最新OpenSSL版本。

curl -O https://www.openssl.org/source/openssl-1.1.1d.tar.gz

 版权所有 © 华为云计算技术有限公司

tar -zxf openssl-1.1.1d.tar.gz

步骤7 安装修补程序，使gcc工具进行修补，然后编译已下载的二进制文件。

yum install patch make gcc -y

说明

如果您使用的版本与OpenSSL-1.1.1d不同，您可能需要更改目录。您可能需要为更新的OpenSSL的版本更新这些命令，否则此修补程序可能无法正常工作。

步骤8 复制并粘贴此数据块，然后在您的设备上选择输入。

```
sed -i "/BIO_get_cipher_ctx(benc, &ctx);/a\ EVP_CIPHER_CTX_set_flags(ctx,
EVP_CIPHER_CTX_FLAG_WRAP_ALLOW);" $HOME/build/openssl-1.1.1d/apps/enc.c
```

步骤9 运行此命令来编译OpenSSL enc.c文件。

cd $HOME/build/openssl-1.1.1d/

./config --prefix=$HOME/local --openssldir=$HOME/local/ssl

make -j$(grep -c ^processor /proc/cpuinfo)

make install

步骤10 成功安装最新版本的OpenSSL后，此版本的OpenSSL已与$HOME/local/ssl/lib/目录中的二进制文件动态链接，您的shell无法直接运行它。设置环境变量LD_LIBRARY_PATH，以确保有相关的库可用于OpenSSL。

步骤11 由于您需要多次运行修复版本的OpenSSL，请创建一个名为openssl.sh的脚本，以在运行二进制文件之前加载$HOME/local/ssl/lib/路径。

cd $HOME/local/bin/

echo -e '#!/bin/bash \nenv LD_LIBRARY_PATH=$HOME/local/lib/ $HOME/local/bin/openssl "$@"' > ./openssl.sh

步骤12 使用以下命令在脚本上设置执行位。

chmod 755 ./openssl.sh

步骤13 要启动修复版本的OpenSSL，请执行此命令。

$HOME/local/bin/openssl.sh

----结束

3.1.21 KMS 支持的密钥算法类型

表 3-6 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。

版权所有 © 华为云计算技术有限公司

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

3.1.22 请求 KMS 异常，错误码 401，应该如何处理?

问题现象

请求KMS报错或使用云服务加密功能报错。

报错信息为：httpcode=401,code=APIGW.0301,Msg=Incorrect IAM authentication information: current ip:xx.xx.xx.xx refused。

可能原因

用户在IAM服务中设置了访问控制。

IAM控制策略默认范围为全地址访问，如果用户设置了允许访问的IP地址或者网段，则未允许的IP地址/网段均无法访问KMS，或无法使用云服务加密特性。

解决方法

- 通过云服务控制台访问KMS（如OBS加密）：需要开放10.0.0.0/8、11.0.0.0/8、26.0.0.0/8网段。
- 通过API调用KMS接口：根据访问的源IP地址设置开放。

开放IP地址操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左侧 ☰，选择“管理与监督 > 统一身份认证服务 IAM”，默认进入“用户”界面。

步骤3 选择“安全设置 > 访问控制”，查看“允许访问的IP地址区间”和“允许访问的IP地址或网段”是否包含请求的源IP地址。

说明

需在“控制台访问”和“API访问”中都包含请求的源IP地址。

----结束

 版权所有 © 华为云计算技术有限公司

3.1.23 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的取值范围是(0,1]。

3.1.24 KMS 如何保护创建的密钥?

KMS的开发机制能够预防任何人以明文形式访问您的密钥。KMS使用加密机（HSM）确保密钥的机密性和完整性。明文KMS密钥由加密机加密并保护。仅在处理您的加密请求时，KMS才会在存储器中使用这些密钥。

3.2 凭据管理类

3.2.1 为什么凭据版本状态不能删除?

“SYSCURRENT”和“SYSPREVIOUS”为服务内建的凭据状态，不支持删除。

 版权所有 © 华为云计算技术有限公司

A 修订记录

发布日期	修改说明
2023-12-30	第七次正式发布。 上线凭据管理功能。 ● 新增产品介绍“凭据管理”章节。 ● 新增用户指南“凭据管理”章节。 ● 新增常见问题“为什么凭据版本状态不能删除？”章节。
2023-06-30	第六次正式发布。 ● 新增“审计日志”章节。
2023-05-30	第五次正式发布。 ● 新增“个人数据保护机制”章节。 ● 新增“功能介绍”章节中，密钥算法及密钥包装算法相关描述。 ● 新增“权限管理”章节。
2023-03-25	第四次正式发布。 ● 新增“什么是数据加密服务”章节。 ● 修改服务名称变更为“数据加密服务”。

版权所有 © 华为云计算技术有限公司

发布日期	修改说明
2022-10-25	第三次正式发布。 ● 新增“功能介绍”章节中，标签相关描述。 ● 新增“产品优势”章节。 ● 新增“如何使用”章节中，弹性文件服务相关描述。 ● 全文新增企业项目相关描述，并新增“分配至企业项目”章节。 ● 新增“自定义密钥与默认主密钥有什么区别”章节。 ● 新增“是否可以从KMS中导出用户主密钥”章节。
2020-10-29	第二次正式发布。 修改“创建密钥”章节，修改了可添加标签值的数量。
2020-09-20	第一次正式发布。

版权所有 © 华为云计算技术有限公司