数据加密服务

用户指南

文档版本 72

发布日期 2025-07-23

华为云计算技术有限公司

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

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，在您的华为账号中，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、高效的其他华为账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为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1-1**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 KMS系统策略**、**表 KPS系统策略**、**表 CSMS系统策略**所示。

如果您需要对除DEW之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

表 1-1 KMS 系统策略

系统角色/策略名称	描述	类别	依赖关系
KMS Administrator	密钥管理服务(KMS)管理员，拥有该服务下的所有权限。	系统角色	无
KMS CMKFullAccess	密钥管理服务(KMS)的加密密钥所有权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无

系统角色/策略名称	描述	类别	依赖关系
KMS CMKReadOnlyAccess	密钥管理服务(KMS)的加密密钥只读权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无

表 1-2 KPS 系统策略

系统角色/策略名称	描述	类别	依赖关系
DEW KeypairFullAccess	数据加密服务中密钥对管理服务(KPS)的所有权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无
DEW KeypairReadOnlyAccess	数据加密服务中密钥对管理服务(KPS)的查看权限。拥有该权限的用户仅能查看密钥对管理服务(KPS)数据。	系统策略	无

表 1-3 CSMS 系统策略

系统角色/策略名称	描述	类别	依赖关系
CSMS FullAccess	数据加密服务中凭据管理服务(CSMS)的所有权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无
CSMS ReadOnlyAccess	数据加密服务中凭据管理服务(CSMS)的只读权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无

表1-4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 1-4 常用操作与系统权限的关系

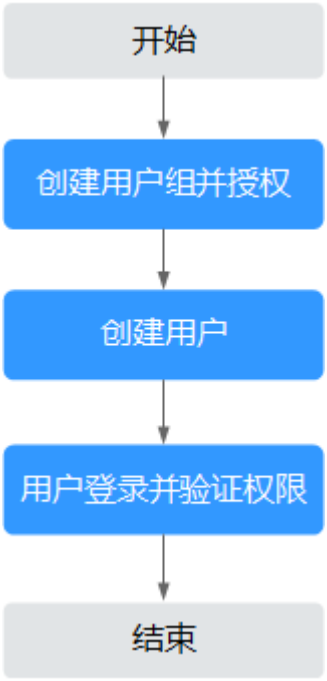
操作	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
创建密钥	√	√	x	x
启用密钥	√	√	x	x
禁用密钥	√	√	x	x
计划删除密钥	√	√	x	x

操作	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
取消计划删除密钥	√	√	x	x
修改密钥别名	√	√	x	x
修改密钥描述	√	√	x	x
创建随机数	√	√	x	x
创建数据密钥	√	√	x	x
创建不含明文数据密钥	√	√	x	x
加密数据密钥	√	√	x	x
解密数据密钥	√	√	x	x
获取密钥导入参数	√	√	x	x
导入密钥材料	√	√	x	x
删除密钥材料	√	√	x	x
创建授权	√	√	x	x
撤销授权	√	√	x	x
退役授权	√	√	x	x
查询授权列表	√	√	x	x
查询可退役授权列表	√	√	x	x
加密数据	√	√	x	x
解密数据	√	√	x	x
签名消息	√	√	x	x
验证签名	√	√	x	x
开启密钥轮换	√	√	x	x
修改密钥轮换周期	√	√	x	x
关闭密钥轮换	√	√	x	x
查询密钥轮换状态	√	√	x	x
查询密钥实例	√	√	x	x

操作	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
查询密钥标签	√	√	x	x
查询项目标签	√	√	x	x
批量添加删除密钥标签	√	√	x	x
添加密钥标签	√	√	x	x
删除密钥标签	√	√	x	x
查询密钥列表	√	√	x	x
查询密钥信息	√	√	x	x
查询公钥信息	√	√	x	x
查询实例数	√	√	x	x
查询配额	√	√	x	x
查询密钥对列表	x	x	√	√
创建或导入密钥对	x	x	√	x
查询密钥对	x	x	√	√
删除密钥对	x	x	√	x
更新密钥对描述	x	x	√	x
绑定密钥对	x	x	√	x
解绑密钥对	x	x	√	x
查询绑定任务信息	x	x	√	√
查询失败的任务	x	x	√	√
删除所有失败的任务	x	x	√	x
删除失败的任务	x	x	√	x
查询正在处理的任务	x	x	√	√

示例流程

图 1-1 给用户授权 DEW 权限流程



1. **创建用户组并授权**

   在IAM控制台创建用户组，并授予加密密钥所有权限“KMS CMKFullAccess”。

2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。

3. **用户登录**并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限。

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

Tenant Guest 系统角色说明

如果您已为IAM子账号配置了**Tenant Guest系统角色**权限时，除了拥有全部云服务只读权限外（除IAM），由于历史原因，还会额外拥有以下KMS相关的操作权限：

- **kms:cmk:create**：创建密钥
- **kms:cmk:createDataKey**：创建数据密钥
- **kms:cmk:createDataKeyWithoutPlaintext**：创建不含明文数据密钥
- **kms:cmk:encryptDataKey**：加密数据密钥
- **kms:cmk:decryptDataKey**：解密数据密钥
- **kms:cmk:retireGrant**：退役授权
- **kms:cmk:decryptData**：解密数据

- **kms:cmk:encryptData**：加密数据
- **kms::generateRandom**：生成随机数

如果您想为某个IAM子账号配置Tenant Guest系统角色权限，但不想拥有上述权限，您需要额外为该IAM子用户配置自定义的拒绝策略。配置自定义策略请参考**DEW自定义策略**。

2 密钥管理

2.1 密钥管理概述

密钥管理服务 KMS 提供密钥的全生命周期管理和数据加解密能力。

密钥管理服务中涉及的核心密钥组件包括**用户主密钥**CMK（Customer Master Key，CMK）、**数据加密密钥** DEK（Data Encryption Key，DEK）。其中 CMK 属于用户的一级密钥，CMK 用于对敏感数据的加解密以及 DEK 的派生。DEK 是信封加密流程中的二级密钥，用于加密业务数据的密钥，受用户主密钥 CMK 的保护。

密钥管理类型

KMS提供默认密钥、自定义密钥和外部密钥三种密钥管理类型，以满足不同业务场景、安全与合规要求。具体内容如下表所示。

表 2-1 密钥管理类型

密钥管理类型	应用场景	功能描述	算法类型	密钥规格	说明
默认密钥	被云服务集成用于服务端加密。 具体请参见**使用KMS加密的云服务**。	仅支持数据加密解密。	AES	AES_256	默认密钥由KMS代您创建和托管，其别名后缀为“/default”。

密钥管理类型	应用场景	功能描述	算法类型	密钥规格	说明
自定义密钥	• 被自建应用集成用于构建应用层密码技术方案。例如：创建AES算法的主密钥，用于自定义数据加密和解密方案；创建RSA/ECC算法的主密钥，用于数字签名计算和验证。 • 被云服务集成用于服务端加密。具体请参见使用KMS加密的云服务。	支持数据加密解密和数字签名。	AES SHA RSA ECC ML-DSA **说明** ML-DSA算法需提交工单申请开通。	• 对称密钥规格：AES_256 • 摘要密钥：HMAC_256、HMAC_384、HMAC_512 • 非对称密钥：RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384、ML-DSA-44、ML-DSA-65、ML-DSA-87 更多信息，请参见KMS支持的密钥算法类型和密钥规格。	由您在KMS创建和管理生命周期，密钥材料由KMS生成。

密钥管理类型	应用场景	功能描述	算法类型	密钥规格	说明
外部密钥	• 被自建应用集成用于构建应用层密码技术方案。例如：创建AES算法的主密钥，用于自定义数据加密和解密方案。 • 被云服务集成用于服务端加密。具体请参见使用KMS加密的云服务。	支持数据加密解密和数字签名。	AES RSA ECC	• 对称密钥规格：AES_256 • 非对称密钥：RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384 更多信息，请参见KMS支持的密钥算法类型和密钥规格。	由您在KMS创建和管理生命周期，密钥材料由您自主导入。

KMS 支持的密钥算法类型和密钥规格

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	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。

密钥类型	算法类型	密钥规格	说明	适用场景
摘要密钥	SHA	• HMAC_256 • HMAC_384 • HMAC_512	摘要密钥	• 数据防篡改 • 数据完整性校验
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。
非对称密钥	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
非对称密钥	ML-DSA **说明** ML-DSA算法需**提交工单**申请开通。	• ML-DSA-44 • ML-DSA-65 • ML-DSA-87	机器学习（ML）算法	抗量子数字签名和验签

KMS 创建的密钥材料和导入的密钥材料的区别

密钥包含密钥元数据（密钥ID、密钥名称、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，创建密钥材料来源为外部的自定义密钥，并将自己的密钥材料导入该自定义密钥中。

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
KMS创建的密钥材料	• 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。

密钥材料来源	区别
导入的密钥材料	• 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。 **说明** RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384算法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，只能永久有效。

2.2 创建密钥

2.2.1 创建自定义密钥

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”。同时为您介绍如下操作：

- **创建自定义密钥**
- **启用自定义密钥**
- **禁用自定义密钥**
- **计划删除密钥**
- **取消计划删除密钥**

前提条件

使用IAM用户创建密钥时，已授予该IAM用户KMS CMKFullAccess及以上权限策略，详细操作请参见**创建用户并授权使用DEW**。

约束条件

- 用户最多可创建100个自定义密钥，不包含默认密钥。创建副本密钥会占用该区域自定义密钥配额。
- 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，HMAC密钥用于数据完成性校验。
- 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”。
- 通过API接口方式调用KMS密钥时，每月每个密钥可免费调用20000次。

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。

创建自定义密钥

步骤1 **登录DEW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 单击界面右上角“创建密钥”。

步骤4 进入“创建密钥”页面，填写密钥参数。

图 2-1 创建密钥

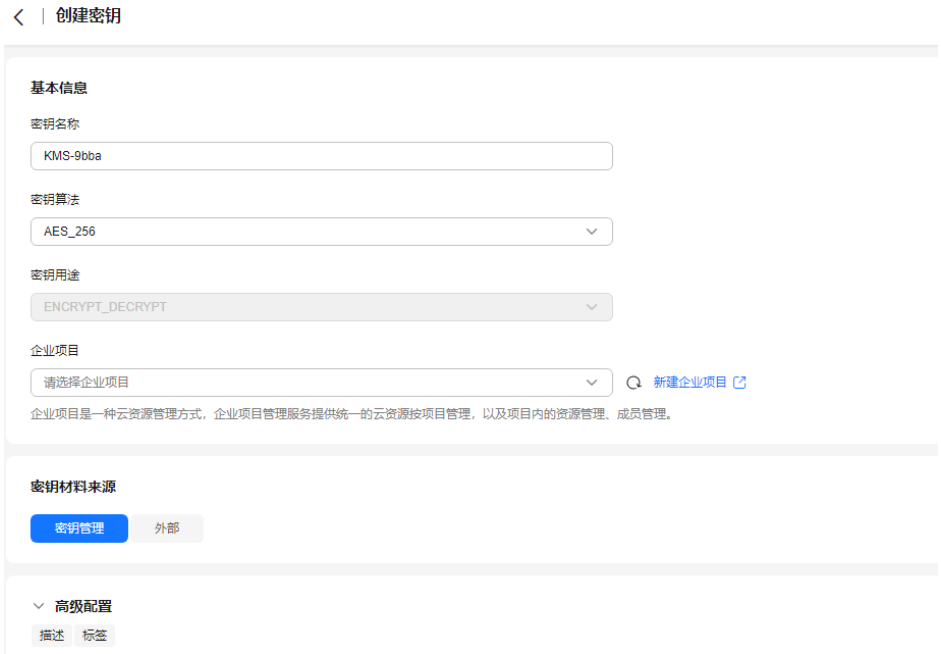


表 2-4 密钥参数配置

参数	描述
密钥名称	待创建的密钥的名称。 **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。
密钥用途	密钥的用途，密钥用途创建后不支持修改。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HMAC对称密钥，默认值“GENERATE_VERIFY_MAC”。 • 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”。
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。 **说明** • 企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。更多关于企业项目的信息，请参见**《什么是企业项目管理？》**。 • 如需开通企业项目，请参考**如何开通企业项目/企业多账号**。
密钥材料来源	• 密钥管理 • 外部
高级配置	• 描述信息 密钥的描述信息。 • 标签 可根据自己的需要为自定义密钥添加标签。更多标签相关操作请参见**标签管理**。 **说明** 最多可以给单个自定义密钥添加20个标签。

步骤5 单击“确定”，完成密钥创建。用户可在密钥列表上查看已完成创建的密钥，密钥材料来源为“密钥管理”时默认状态为“启用”；密钥材料来源为“外部”时默认状态为“等待导入”。

----结束

启用自定义密钥

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。

步骤1 在密钥列表中，在需要启用的密钥所在行的“操作”列，单击“启用”。

步骤2 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

禁用自定义密钥

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。

- 默认密钥不支持禁用操作。
- 密钥被禁用后，仍然会计费。只有删除密钥，才会停止计费。

步骤1 在密钥列表中，在需要启用的密钥所在行的“操作”列，单击“禁用”。

步骤2 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

计划删除密钥

KMS不支持直接删除密钥，仅支持计划删除密钥，即通过设置预删除周期（推迟时间范围为7天～1096天），在到期后删除密钥。

处于“启用”、“禁用”或“等待导入”状态的自定义密钥才支持删除，默认密钥不支持删除。

说明

- 系统会在推迟删除周期后删除密钥，使用该密钥加密的内容及产生的数据密钥也将无法解密。删除密钥前，请确认该密钥已不再使用，否则会导致您的业务不可用。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，详细操作请参见**查询审计事件**。
- 如果需要删除已创建副本密钥的主密钥，需要先删除副本密钥。

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”。以下为您介绍如何单个删除密钥。

步骤1 在需要删除的密钥所在行的“操作”列，单击“删除”，进入“删除密钥”界面。

步骤2 在“删除密钥”界面，填写“推迟删除”的时间。

步骤3 如果未开启删除验证，在确认删除提示框中输入“DELETE”后，单击“确定”，完成删除操作。

如果开启删除验证，选择验证方式后，单击“获取验证码”，在验证码对话框中输入获取的验证码，单击“确定”，完成删除操作。

说明

如果需要关闭操作保护，可以在账号的安全设置 > 敏感操作中关闭。也可以单击删除页面的“关闭操作保护”

步骤4 如果密钥用于加密数据库服务DDS、RDS、NOSQL，在单击“确认”后，会弹出提示“正在被XXX服务使用，请确认是否删除”，如**图 删除确认**所示，需单击“确认删除”，确认后才能完成密钥删除操作。

图 2-2 删除确认

----结束

取消计划删除密钥

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。

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”。以下为您介绍如何取消单个密钥的计划删除。

步骤1 在需要取消删除的密钥所在行的“操作”列，单击“取消删除”。

步骤2 在弹出的窗口中，单击“确定”，完成取消删除单个密钥操作。

取消删除后密钥状态为“禁用”，如需启用密钥，请参见**启用自定义密钥**操作。

----结束

相关操作

- 各云服务使用KMS加密的方法，请参见**使用KMS加密的云服务**。
- 创建DEK、不含明文的DEK方法，具体请参见《数据加密服务API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API参考》的“加密数据密钥”与“解密数据密钥”章节。

2.2.2 导入外部密钥

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。

约束条件

- 摘要密钥HMAC密钥算法不支持导入密钥材料，非对称密钥不支持删除密钥材料。
- 副本密钥在创建时会同步主密钥的密钥材料，密钥材料过期后，需在各区域重新独立导入密钥材料。

注意事项

导入的密钥材料需要注意以下事项：

- 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材料时，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。
- 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。

操作流程

场景	操作步骤
已有密钥材料	1. **创建密钥材料来源为外部的密钥**：创建一个密钥材料来源为外部的空密钥。 2. **导入密钥材料（导入已有密钥材料）**：导入密钥材料、导入令牌到创建的空密钥。
通过调用API接口下载密钥材料	1. **创建密钥材料来源为外部的密钥**：创建一个密钥材料来源为外部的空密钥。 2. **下载包装密钥和导入令牌（通过调用API接口下载）**：通过调用API接口下载包装密钥、导入令牌。 3. **使用包装密钥加密密钥材料**：使用HSM或OpenSSL，将包装密钥加密为密钥材料。 4. **导入密钥材料（导入已有密钥材料）**：导入密钥材料、导入令牌到创建的空密钥。

场景	操作步骤
通过KMS控制台下载密钥材料	1. **创建密钥材料来源为外部的密钥**：创建一个密钥材料来源为外部的空密钥。 2. **下载包装密钥和导入令牌（通过KMS控制台下载）**：通过KMS控制台下载包装密钥。导入令牌由控制台自动引导。 **须知** 下载包装密钥后，请勿关闭或中途退出“导入密钥材料”对话框，加密密钥材料后，需要继续在该对话框，执行**导入密钥材料（继续导入密钥材料）**。 3. **使用包装密钥加密密钥材料**：使用HSM或OpenSSL，将包装密钥加密为密钥材料。 4. **导入密钥材料（继续导入密钥材料）**：导入密钥材料到创建的空密钥。

步骤一：创建密钥材料来源为外部的密钥

步骤1 **登录DEW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 单击界面右上角“创建密钥”，创建一个“密钥材料来源”为“外部”的空密钥。更多参数说明，请参见**步骤4**。

----结束

步骤二：下载包装密钥和导入令牌

密钥管理提供两种下载方式：

- 通过调用API接口下载：获取到包装密钥、导入令牌。
- 通过KMS控制台下载：获取到包装密钥。导入令牌将由控制台自动传递。因此，下载密钥材料后，请勿关闭或中途退出“导入密钥材料”对话框，否则将导致导入的令牌自动失效。

通过调用 API 接口下载

步骤1 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
}
```

步骤2 保存包装密钥，包装密钥需要按照以下步骤转换格式。使用转换格式后的包装密钥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

步骤3 保存导入令牌，复制导入令牌“import_token”的内容，粘贴到“.txt”文件中，并保存为“ImportToken.b64”。

----结束

通过 KMS 控制台下载

步骤1 **登录DEW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 在“自定义密钥”页签，定位到**步骤一：创建密钥材料来源为外部的密钥**创建的密钥，单击“操作”列的“导入密钥材料”。

步骤4 在“获取包装密钥和导入令牌”配置项，根据**表 密钥包装算法说明**，选择密钥包装算法。

图 2-3 获取包装密钥和导入令牌

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。

步骤5 单击“下载密钥材料”，下载的文件为包装密钥，如图 下载文件所示。

图 2-4 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。

控制台将自动传递导入令牌。因此，下载密钥材料后，请勿关闭或中途退出“导入密钥材料”对话框，否则将导致导入的令牌自动失效。

下载包装密钥后，需要**使用包装密钥加密密钥材料**，然后继续在“导入密钥材料”对话框，导入密钥材料。具体操作，请参见**继续导入密钥材料**。

----结束

步骤三：使用包装密钥加密密钥材料

对称密钥和非对称密钥加密方式不同，生成的密钥材料也不同：

- 对称密钥：密钥材料为“EncryptedKeyMaterial.bin”。
- 非对称密钥：密钥材料为“EncryptedKeyMaterial.bin”临时密钥材料、“out_rsa_private_key.der”私钥密文。

对称密钥

- **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. 在已安装OpenSSL工具的客户端上，执行以下命令，生成密钥材料（256位对称密钥），并将生成的密钥材料以“PlaintextKeyMaterial.bin”命名保存。

     - AES256对称密钥

       openssl rand -out *PlaintextKeyMaterial.bin* 32

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

     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**

非对称密钥

- **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. 在已安装OpenSSL工具的客户端上，执行以下命令，生成密钥材料（256位对称密钥），并将生成的密钥材料以“PlaintextKeyMaterial.bin”命名保存。

  - RSA、ECC非对称密钥

    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。

  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 2-7 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. 导入非对称密钥时，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”。

  - 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。

步骤四：导入密钥材料

密钥材料下载方式不同，导入操作方式不同：

- 如果通过调用API接口下载密钥材料，或已有密钥材料，执行**导入已有密钥材料**。
- 如果通过KMS控制台下载密钥材料，执行**继续导入密钥材料**。

导入已有密钥材料

步骤1 **登录DEW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 在“自定义密钥”页签，定位到**步骤一：创建密钥材料来源为外部的密钥**创建的密钥，单击“操作”列的“导入密钥材料”。

步骤4 在“获取包装密钥和导入令牌”配置项，根据**表 密钥包装算法说明**，选择密钥包装算法。

图 2-5 获取包装密钥和导入令牌

表 2-8 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。

步骤5 单击“已有密钥材料”，在“导入密钥材料”配置项，填写“密钥材料”内容。

图 2-6 导入密钥材料

表 2-9 密钥材料说明

场景	说明
对称密钥	使用包装密钥加密后的密钥材料。 例如：**步骤三：使用包装密钥加密密钥材料**中的“EncryptedKeyMaterial.bin”文件。
非对称密钥	使用包装密钥加密后的临时密钥材料、私钥密文。 例如：**步骤三：使用包装密钥加密密钥材料**中的临时密钥材料“EncryptedKeyMaterial.bin”、私钥密文“out_rsa_private_key.der”。

步骤6 单击“下一步”，在“密钥导入令牌”配置项，根据**表2-10**设置参数。

图 2-7 导入密钥令牌

表 2-10 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	填写**通过调用API接口下载**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7 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

继续导入密钥材料

步骤1 返回控制台“导入密钥材料”对话框（**步骤5**），在“导入密钥材料”配置项，添加“密钥材料”文件。

图 2-8 导入密钥材料

表 2-11 密钥材料说明

场景	说明
对称密钥	使用包装密钥加密后的密钥材料。 例如：**步骤三：使用包装密钥加密密钥材料**中的“EncryptedKeyMaterial.bin”文件。
非对称密钥	使用包装密钥加密后的临时密钥材料、私钥密文。 例如：**步骤三：使用包装密钥加密密钥材料**中的临时密钥材料“EncryptedKeyMaterial.bin”、私钥密文“out_rsa_private_key.der”。

步骤2 单击“下一步”，进入“密钥导入令牌”页面。根据**表2-12**设置参数。

图 2-9 导入密钥令牌

表 2-12 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。

参数	操作说明
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3 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

删除密钥材料

导入的密钥材料过期或者被删除后，其密钥将无法使用，且当前密钥的状态切换为“等待导入”，需要**重新导入相同的密钥材料**才可以正常使用。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。

说明

非对称密钥不支持删除密钥材料。

KMS支持两种删除密钥材料的方法：

- **方法一**：过期后由KMS删除
  在导入密钥材料时，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。
- **方法二**：通过控制台直接删除密钥材料
  a. 在需要删除的密钥材料所在行，单击“更多 > 删除密钥材料”。
  b. 在弹出的对话框中输入“DELETE”后单击“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。

重新导入相同的密钥材料

密钥材料过期或删除后，您可以再次导入相同的密钥材料，密钥才可继续使用。

1. 重新下载包装公钥和导入令牌。具体操作，请参见**步骤二：下载包装密钥和导入令牌**。

   说明

   密钥包装过程不会影响密钥材料的内容，因此，您可以使用不同的包装公钥和不同的包装算法来导入相同的密钥材料。

2. 使用包装公钥加密密钥材料。具体操作，请参见**步骤三：使用包装密钥加密密钥材料**。

说明

密钥材料必须与之前过期的密钥材料为同一个。

3. 使用导入令牌，导入加密后的密钥材料。具体操作，请参见**步骤四：导入密钥材料**。

2.3 使用密钥

2.3.1 如何使用 KMS 加密

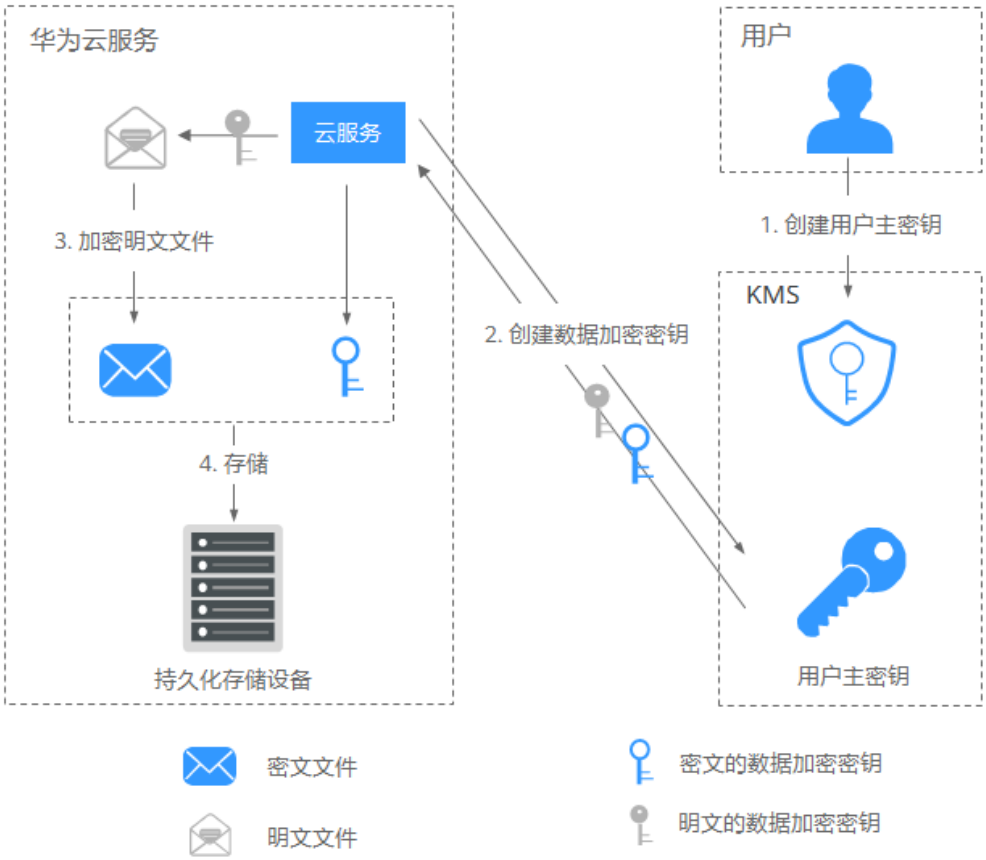
前提条件

本章节涉及的“自定义密钥”均为“对称密钥”。对称密钥和非对称密钥的介绍，请参见**密钥概述**章节。

与华为云服务配合使用

华为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，华为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。使用KMS加密的云服务请参见**使用KMS加密的云服务**。

图 2-10 华为云服务使用 KMS 加密原理



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. 华为云服务调用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. 华为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. 华为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

用户通过华为云服务下载数据时，华为云服务通过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。

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API参考》**。

使用 KMS 加密的云服务

KMS为各云服务提供主密钥管理控制能力，为各云服务提供加密能力。

表 2-13 使用 KMS 加密的云服务列表

服务名称	如何使用	参考文档
对象存储服务 OBS	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。	**OBS服务端加密**
云硬盘 EVS	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。	**EVS服务端加密**
镜像服务 IMS	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。	**IMS服务端加密**
弹性文件服务 SFS	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。	**SFS服务端加密**
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。	**RDS数据库加密**
文档数据库服务 DDS	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。	**DDS数据库加密**
弹性云服务器 ECS	弹性云服务器是通过镜像加密或者数据盘加密来实现ECS资源加密。 • 在创建弹性云服务器时，您如果选择加密镜像，弹性云服务器的系统盘会自动开启加密功能，加密方式与镜像保持一致。镜像加密请参见**IMS服务端加密**。 • 在创建弹性云服务器时，您也可以对添加的数据盘进行加密。 数据盘加密请参见**IMS服务端加密**。	**ECS服务端加密**
高性能弹性文件服务 SFS Turbo	创建SFS Turbo文件系统时，选择KMS提供的密钥对文件系统进行加密，使核心数据更安全。	**创建SFS Turbo文件系统**
专属主机 DeH	用户加密，是指用户通过提供的加密特性，对弹性云服务器资源进行加密，从而提升数据的安全性。用户加密功能包括镜像加密和云硬盘加密。	**专属主机加密**

服务名称	如何使用	参考文档
函数工作流 FunctionGraph	若需在函数运行时解密敏感数据（如数据库密码、API密钥），可通过KMS SDK动态操作密钥。用户可以将加解密密钥托管在KMS，并在IAM服务为函数创建委托授权FunctionGraph访问KMS。	用户配置安全
云硬盘备份 VBS	云硬盘备份的加密功能依赖于密钥管理服务。加密云硬盘的备份数据会以加密方式存放。	创建云硬盘备份
云容器引擎 CCE	可以使用KMS密钥对CCE中存储的Kubernetes Secret对象进行信封加密，为应用程序的敏感数据提供安全保护。	使用KMS进行Secret落盘加密
专属分布式存储服务 DSS	当您由于业务需求从而需要对存储在磁盘的数据进行加密时，EVS为您提供加密功能，可以对新创建的磁盘进行加密。加密磁盘使用的密钥由数据加密服务（DEW，Data Encryption Workshop）中的密钥管理（KMS，Key Management Service）功能提供，无需您自行构建和维护密钥管理基础设施，安全便捷。	磁盘加密
云容器实例 CCI	云容器实例支持将云硬盘（EVS）挂载到容器中，将通过KMS对云硬盘进行加密。	云硬盘存储卷
容器镜像服务 SWR	容器镜像服务企业版支持使用数据加密服务（DEW）中创建的密钥对镜像进行签名，保障镜像分发部署过程中的一致性，避免中间人攻击和非法镜像更新及运行。	镜像签名
云数据库 TaurusDB	透明数据加密（Transparent Data Encryption，简称TDE），对数据文件执行实时I/O加密和解密，数据在写入磁盘之前进行加密，从磁盘读入内存时进行解密，能有效保护数据库及数据文件的安全。	开启TaurusDB透明数据加密
云运维中心 COC	为了更加安全地保护您的主机账号密码，云运维中心会使用KMS来加密您的主机账号密码。在使用密钥管理之前，请先在KMS创建好密钥。	密钥管理
数据仓库服务 GaussDB(DWS)	在DWS中，可以为集群启用数据库加密，以保护静态数据。当您为集群启用加密时，该集群及其快照的数据都会得到加密处理。	DWS数据库加密
云数据迁移 CDM	在迁移文件到文件系统时，CDM支持通过KMS提供的密钥对文件加解密。	迁移文件时加解密
数据安全中心 DSC	通过加密算法和加密主密钥生成一种加密配置，达到数据脱敏的效果。	加密脱敏
云桌面 Workspace	购买云桌面时，可以使用KMS提供的密钥对磁盘进行加密。	购买桌面
云数据库 GeminiDB	购买云数据库实例时，可以使用KMS提供的密钥对数据库中静态数据加密。	购买并连接集群版实例

2.3.2 使用自定义密钥在线加解密小数据

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。
- 调用API进行数据加密后，无法使用在线工具解密。

加密数据

步骤1 登录DEW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 单击目标自定义密钥的名称，进入密钥信息页面后，单击“工具”页签。

步骤4 在“加密”文本框中输入待加密的数据，如图2-11所示。

图 2-11 加密数据

步骤5 单击“执行”，在“加解密结果”栏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。
- 单击“清除”，清除已输入的数据。
- 在“加密结果”栏，单击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

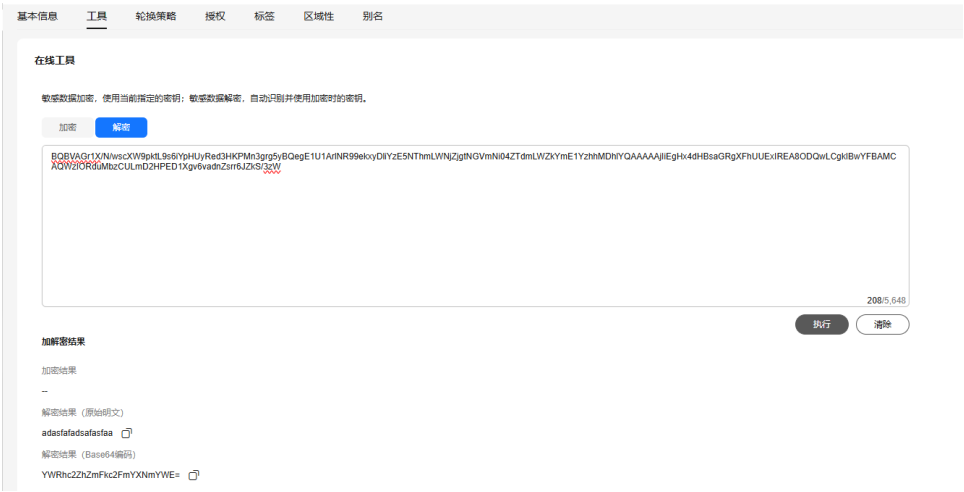
步骤1 在密钥列表中，单击任意“启用”状态的非默认密钥名称，进入该密钥的在线工具页面。

步骤2 单击“解密”，在文本框中输入待解密的密文数据，如图2-12所示。

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。

图 2-12 解密数据



步骤3 单击“执行”，在“加解密结果”栏显示解密后的密文数据。

说明

- 在“解密结果”栏，单击拷贝解密后的明文数据，并保存到本地文件中。
- 通过命令行或者API加密的信息，不能包含特殊字符，可能会导致控制台解密结果无法显示。
- 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

2.4 管理密钥

2.4.1 查看密钥详细信息

该任务指导用户通过KMS界面查看自定义密钥的信息，包括密钥名称/ID、状态创建时间。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DEW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 在密钥列表中，查看密钥信息，密钥列表参数说明，如表2-14所示。

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。

图 2-13 自定义密钥列表

图 2-14 默认密钥列表

表 2-14 密钥列表参数说明

参数	操作说明
密钥名称/ID	密钥的名称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”。
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。

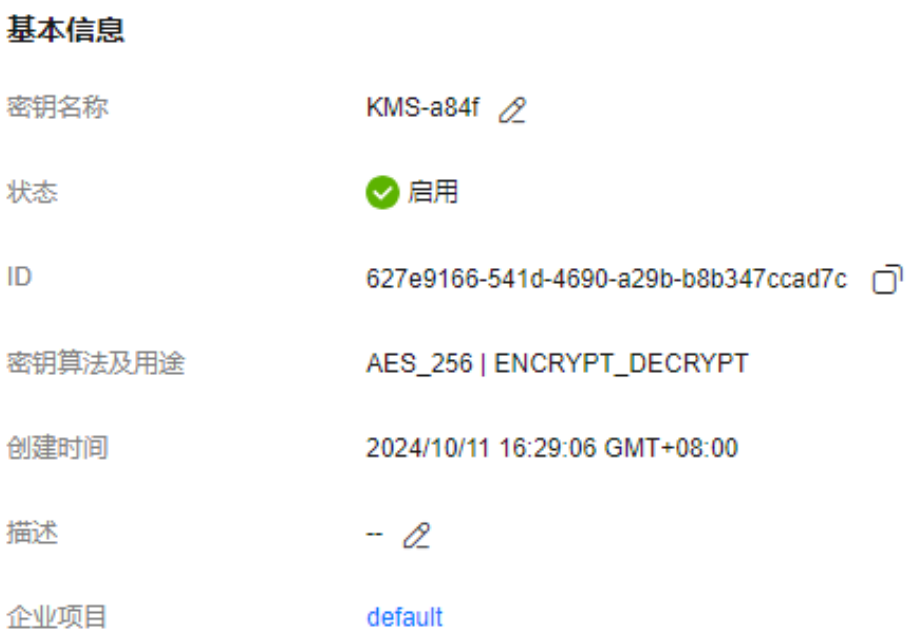
参数	操作说明
密钥材料来源	密钥材料的来源，包含： • 外部 用户从外部导入到KMS。 • 密钥管理 用户通过KMS创建的密钥，或默认密钥。
企业项目	创建密钥时，给密钥绑定企业项目ID。

步骤4 用户可单击密钥名称，查看密钥详细信息，如**图 密钥详细信息**所示。

用户可单击该密钥的“名称”或“描述”所在行的，修改密钥的名称或描述信息。

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

图 2-15 密钥详细信息



----结束

2.4.2 为自定义密钥创建别名

别名是为用户密钥设置的简称，是密钥的一种标识。您可以在API接口的调用中使用别名代替密钥ID。原有密钥别名修改为密钥名称。

该任务指导用户为密钥添加、删除别名。

约束条件

- 一个别名仅支持关联一个密钥，但一个密钥可以关联多个别名。

- 别名在区域中拥有唯一性，不同区域下的别名可以相同。
- 别名创建成功后不支持修改。
- 单个密钥最多支持创建50个密钥别名。

为自定义密钥创建别名

步骤1 **登录DEW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 单击目标自定义密钥名称，进入密钥信息页面后，默认进入基本信息页签，单击“别名”页签。

步骤4 单击“创建别名”，在弹出的对话框中输入别名，单击“确定”完成别名创建操作。

说明

别名支持使用数字、英文字符及“_”、“-”、“:”、“/”符号。

----结束

删除别名

步骤1 **登录DEW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 单击目标自定义密钥名称，进入密钥信息页面后，默认进入基本信息页签，单击“别名”页签。

步骤4 在目标别名所在行的“操作”列，单击“删除”。

步骤5 如果未开启删除验证，在确认删除提示框中输入“DELETE”后，单击“确定”，完成删除操作。

如果开启删除验证，选择验证方式后，单击“获取验证码”，在验证码对话框中输入获取的验证码，单击“确定”，完成删除操作。

说明

如果需要关闭操作保护，可以在账号的安全设置 > 敏感操作中关闭。也可以单击删除页面的“关闭操作保护”

----结束

2.4.3 为自定义密钥添加标签

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。

为自定义密钥添加标签

步骤1 登录DEW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 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤4 单击“标签”，进入标签管理页面。

步骤5 单击“添加标签”，弹出添加标签对话框，如图2-16所示，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2-15所示。

图 2-16 添加标签

说明

- 如果需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，用户可在TMS中创建预定义标签。更多关于预定义标签的信息，请参见《标签管理用户指南》。
- 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 2-15 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。 • 不能以_sys_开头。 • 可以包含以下字符： – 中文 – 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： – 中文 – 英文 – 数字 – 空格 – 特殊字符“_”、“.”、“:”、“/”、“=”、“+”、“-”、“@”	100

步骤6 单击“确定”，完成标签的添加。

----结束

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。

步骤1 在“密钥管理”列表中，单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤2 选择“标签”页签，进入标签管理页面。

步骤3 在目标标签所在行的“操作”列，单击“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

删除标签

该任务指导用户通过密钥管理界面删除标签。

步骤1 在“密钥管理”列表中，单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤2 选择“标签”页签，进入标签管理页面。

步骤3 在目标标签所在行的“操作”列，单击“删除”，弹出删除标签对话框。

步骤4 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

2.4.4 为自定义密钥创建副本密钥

副本密钥是指在数据加密服务中，通过对主密钥进行复制而生成的密钥。副本密钥是与主密钥具有相同密钥材料的密钥。它通常用于跨区域的数据加解密操作，以便在不同区域中使用相同的密钥进行数据处理。副本密钥在数据加密服务中提供了灵活性和高可用性，但需要合理管理以确保安全性和合规性。

约束条件

- 仅自定义密钥支持创建副本密钥，默认密钥不支持创建副本密钥。
- 仅支持对华北-北京四、华南-广州、西南-贵阳一、华东-上海一、亚太-新加坡、中东-利雅得区域的主密钥创建副本密钥。

  同一个主密钥可以在多个不同区域创建副本密钥，但每个区域仅能创建一个主密钥对应的副本密钥。

表 2-16 主密钥与副本密钥区域

主密钥区域	副本密钥支持区域
华北-北京四	• 华东-上海一 • 华南-广州 • 西南-贵阳一
华南-广州	• 华北-北京四 • 华东-上海一 • 西南-贵阳一
西南-贵阳一	• 华东-上海一 • 华南-广州 • 华北-北京四

主密钥区域	副本密钥支持区域
华东-上海一	• 华北-北京四 • 华南-广州 • 西南-贵阳一
亚太-新加坡	中东-利雅得
中东-利雅得	亚太-新加坡

- 副本密钥计费模式与主密钥计费模式一致。收取密钥实例费用以及API调用费用，具体计费可参见**计费项**。
- 副本密钥不支持密钥轮换。副本密钥的轮换需由区域主密钥发起。

为自定义密钥创建副本密钥

步骤1 **登录DEW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 单击目标自定义密钥的密钥名称，进入密钥详细信息页面。

步骤4 单击“区域性”，进入密钥区域性页面。

步骤5 单击“创建副本密钥”，进入“创建副本密钥”界面，如**图 创建副本密钥**所示。

图 2-17 创建副本密钥

步骤6 在弹出的对话框中，选择创建副本密钥区域，输入密钥别名。参数说明参见**表 副本密钥参数说明**。

表 2-17 副本密钥参数说明

参数	参数说明
区域	创建的副本密钥存储区域。
密钥名称	待创建密钥的别名。
企业项目	创建副本密钥绑定企业项目ID。 **说明** 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。
描述信息	副本密钥的描述信息。
标签	（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”。

步骤7 单击“确定”，完成创建副本密钥。预计1分钟刷新副本密钥所在区域，即可查看创建的副本密钥。

----结束

查看副本密钥

通过控制台直接查看：

步骤1 **登录DEW管理控制台**。

步骤2 单击管理控制台左上角，选择副本密钥所在区域。

步骤3 在密钥列表中，单击目标密钥查看密钥信息。

----结束

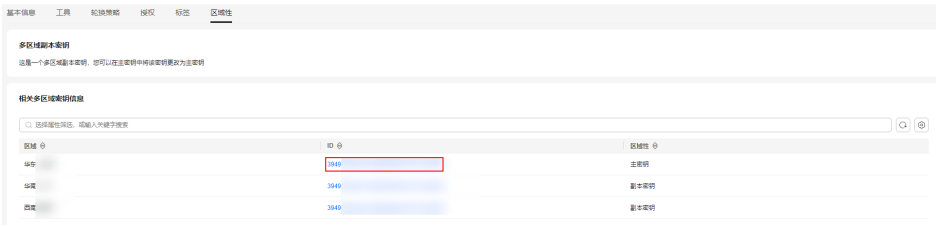
通过主密钥区域跳转查看：

步骤1 在密钥列表中，单击目标自定义密钥的密钥名称，进入密钥详细信息页面。

步骤2 单击“区域性”，进入密钥区域性页面。

步骤3 单击需要跳转区域的密钥ID，即可跳转至该区域密钥详情页面。

图 2-18 通过 ID 跳转



----结束

使用副本密钥

副本密钥的使用方式与主密钥一致，具体使用方式请参见**创建自定义密钥**章节。

2.4.5 为自定义密钥创建授权

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。
  - 用户ID：在“用户名 > 我的凭证 > API凭证”中的“IAM用户ID”。
  - 账号ID：在“用户名 > 我的凭证 > API凭证”中的“账号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。

为自定义密钥创建授权

步骤1 **登录DEW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 单击目标自定义密钥的名称，进入密钥详细信息授权页面。

步骤4 单击“授权”，进入授权管理界面。

步骤5 单击“创建授权”，弹出“创建授权”对话框。

图 2-19 创建授权（用户）

图 2-20 创建授权（账号）

步骤6 在弹出的对话框中，输入被授权用户/账号ID，并勾选授权操作的权限。参数说明请参见**表2-18**。

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 2-18 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

参数	参数说明	配置样例
授权名称	用户可选择为授权命名。 **说明** • 输入字符支持数字、字母、“_”、“-”、“:”和“/”。	test
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 用户可以选择多种授权操作。以下为各类型密钥通用授权操作： • 查询密钥信息 • 创建授权 • 退役授权 各类型密钥算法及用途，具有对应专属授权操作，具体请参见**表 授权操作**。	-

表 2-19 授权操作

密钥算法	密钥类型	密钥用途	授权操作
• AES_256	对称密钥	ENCRYPT_DECRYPT	• 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 • 加密数据 • 解密数据
• RSA_2048 • RSA_3072 • RSA_4096 • EC_P256 • EC_P384	非对称密钥	SIGN_VERIFY	• 查询公钥信息 • 签名 • 验签
• RSA_2048 • RSA_3072 • RSA_4096	非对称密钥	ENCRYPT_DECRYPT	• 查询公钥信息 • 加密数据 • 解密数据
• HMAC_256 • HMAC_384 • HMAC_512	摘要密钥	GENERATE_VERIFY_MAC	• 生成HMAC • 校验HMAC

步骤7 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

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。

步骤1 在“密钥管理”列表中，单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤2 选择“授权”页签，用户可查看当前自定义密钥下创建的授权。自定义密钥的授权信息如**表2-20**所示。

表 2-20 授权信息参数说明

参数	参数说明
授权名称	创建授权时为授权进行命名。
被授权ID	被授权的ID。
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。

步骤3 单击目标授权，页面右侧显示授权详情，如**图 授权详情**所示。

图 2-21 授权详情

----结束

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。

步骤1 在“密钥管理”列表中，单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤2 选择“授权”页签，在目标授权ID所在行的“操作”列，单击“撤销授权”。

步骤3 如果未开启验证，在确认删除提示框中输入“DELETE”后，单击“确定”，完成撤销授权操作。

如果开启验证，选择验证方式后，单击“获取验证码”，在验证码对话框中输入获取的验证码，单击“确定”，完成撤销授权操作。

说明

如果需要关闭操作保护，可以在账号的“安全设置 > 敏感操作”中关闭。也可以单击删除页面的“关闭操作保护”。

----结束

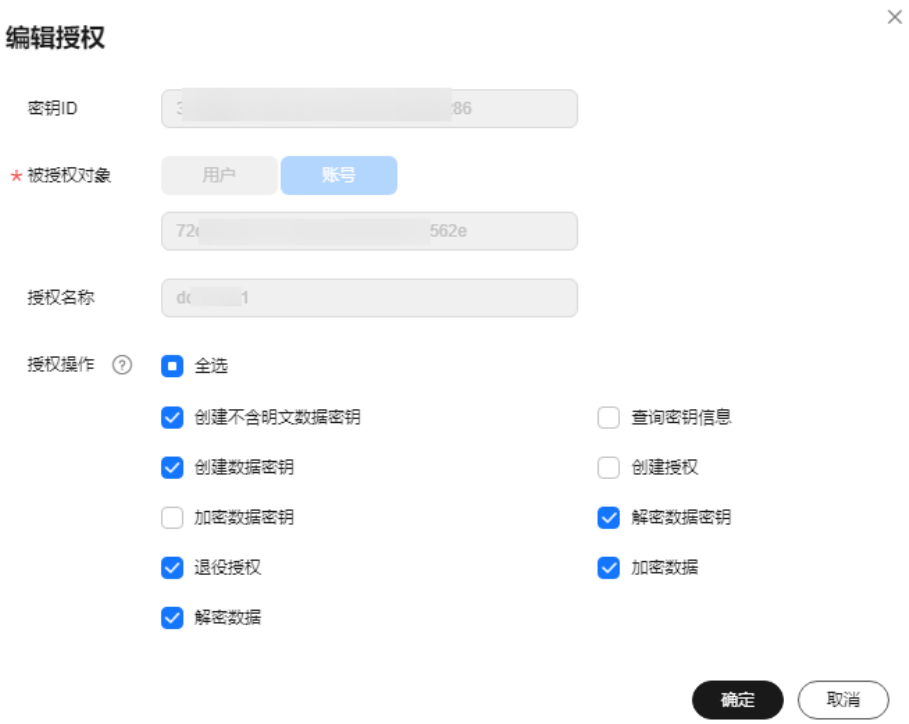
编辑授权

为其他IAM用户或账号创建授权后，可对已授权操作进行编辑，更改授权对象的操作权限范围。

步骤1 在“密钥管理”列表中，单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤2 选择“授权”页签，在目标授权ID所在行“操作”列，单击“编辑授权”，在弹出页面对授权操作进行勾选，如图 编辑授权所示。

图 2-22 编辑授权



步骤3 单击“确定”，完成编辑授权操作。

----结束

2.4.6 将自定义密钥迁入企业项目

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迁移至其他企业项目。

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。如需开通企业项目，请参考**如何开通企业项目/企业多账号**。
- 默认密钥不支持切换企业项目。

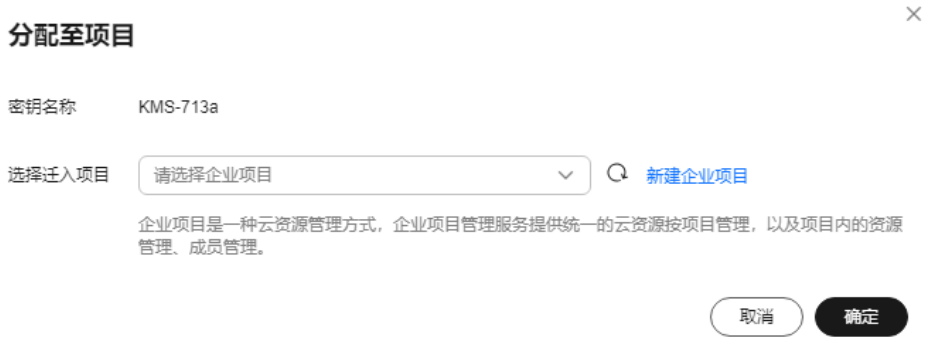
将自定义密钥迁入企业项目

步骤1 **登录DEW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 在目标密钥所在行，选择“更多 > 分配至项目”，弹出对话框。

图 2-23 分配至项目



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。

如需开通企业项目，请参考**如何开通企业项目/企业多账号**。

步骤4 在弹出的对话框中，选择迁入项目。单击“确定”，完成操作。

----结束

2.4.7 查看密钥计费请求次数

通过云监控服务 CES对当前用户的所有密钥进行数据监控，支持查询密钥请求计费次数、密钥详情请求次数等常用调用的请求次数。本章节指导通过查看监控功能进密钥计费请求次数查询。

约束条件

- 仅支持查看已启用或禁用状态的密钥，计划删除或已删除的密钥不支持查看计费请求次数。
- 默认密钥支持查看计费请求次数。

查看单个密钥监控详情

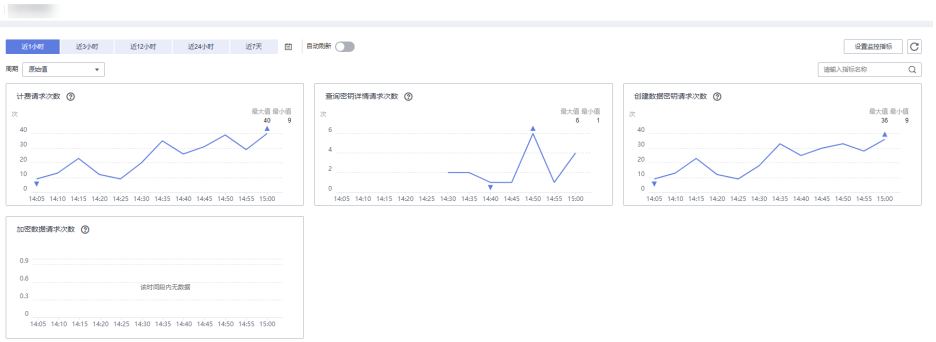
步骤1 登录DEW管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 在目标密钥所在行操作列，选择“更多 > 查看监控”，进入对应密钥的监控指标详情页面。

步骤4 通过密钥详情页面，可以看到当前密钥在不同时间范围内的密钥调用情况，查询内容如图 单个密钥监控详情所示。

图 2-24 单个密钥监控详情



说明

默认展示所有指标类型，通过设置监控指标以及时间范围选择，查询您需要的目标密钥的指标。

----结束

查看批量密钥监控详情

步骤1 登录DEW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 单击页面左侧，选择“管理与监管 > 云监控服务”，进入“监控概览”页面。

步骤4 在左侧导航栏中选择“云服务监控 > 密钥管理服务”，进入服务监控页面。

步骤5 勾选多个目标密钥，单击页面左上角“导出监控数据”，配置参数后，单击“导出”。

图 2-25 导出监控数据

步骤6 导出完成后，选择左侧导航栏“任务中心”，默认进入“监控数据导出”页签。

步骤7 在目标任务名称所在行，单击“下载”，即可获取导出的密钥数据的监控信息。

----结束

2.4.8 开启密钥轮换

KMS提供了密钥轮换功能，您可以通过定期轮转来加强密钥使用的安全性，有效地提升业务数据的安全性。本文介绍KMS密钥轮转的原理和配置方法。

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。开启密钥轮换后会产生一定费用，具体费用计算可参见**开通密钥轮转如何收费？**。

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

华为云服务提供了两种密钥轮换方法：

- 手动轮换密钥

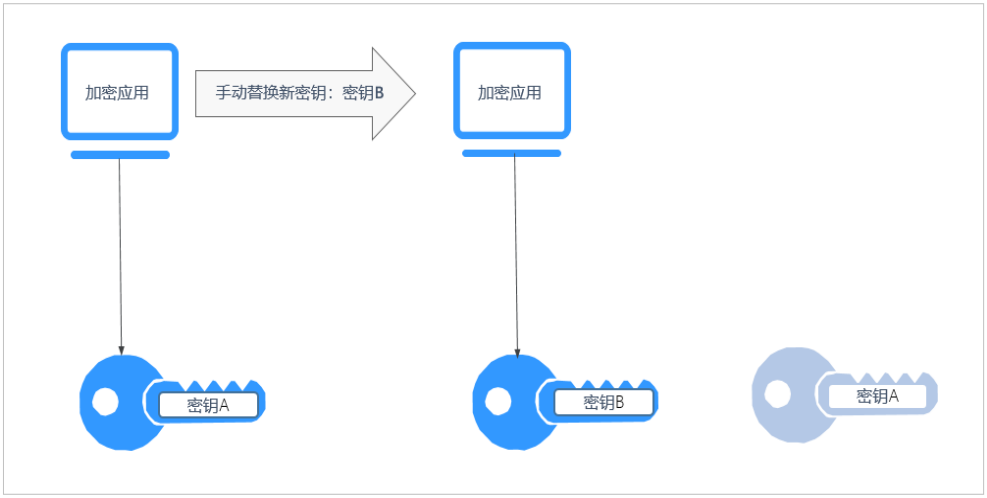
  方式一：创建一个新的密钥B，使用密钥B替换当前正在使用的密钥A。

  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。

图 2-26 手动轮换密钥工作原理



- 自动轮换密钥

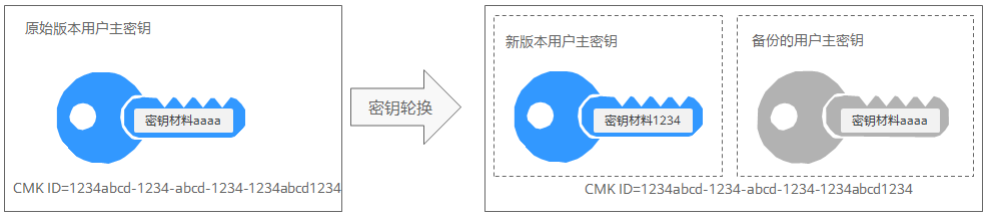
  KMS会根据设置的轮换周期（默认365天）自动轮换密钥，系统自动生成一个新的密钥B，并替换当前使用的密钥A。自动轮换密钥只会更改主密钥的密钥材料，即加密操作中所使用的加密材料。不管密钥材料有没有变更或变更了多少次，该主密钥仍是相同的逻辑资源。主密钥的属性（密钥ID、别名、描述、权限）不会发生变化。

  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 2-27 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 2-21 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。
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。

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。

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，副本密钥不支持进行密钥轮转。
- 仅对称密钥支持开启密钥轮换。
- 密钥必须处于“启用”状态，且“密钥材料来源”为“密钥管理”，才支持开启密钥轮换，导入的密钥材料不支持自动轮转。
- 启用密钥轮换可能会生成额外的费用。费用详情查阅**计费说明**。

启用密钥轮换

步骤1 **登录DEW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 单击目标自定义密钥的名称，进入密钥详细信息页面。

步骤4 单击“轮换策略”页签，进入“轮换策略”页面。

步骤5 单击，将“密钥轮换”设置为，弹出“启用轮换策略”对话框。

步骤6 设置轮换周期（天），单击“确定”。如图2-28所示。参数说明如表2-22所示。

图 2-28 开启密钥轮换

表 2-22 密钥轮换参数说明

参数	说明
密钥轮换	密钥轮换开关，默认。 ：关闭。 ：开启。 开启密钥轮换后，密钥在设置的轮换周期到达后开始轮换。 **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。
轮换周期（天）	轮换周期。取值范围为“30~365”的整数，默认“365”天。 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。

步骤7 开启后，页面显示密钥轮换详情，如图 密钥轮换详情所示。

图 2-29 密钥轮换详情

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

关闭密钥轮换

步骤1 单击目标自定义密钥的名称，进入密钥详细信息页面。

步骤2 单击“轮换策略”页签，进入“轮换策略”页面。

步骤3 单击  ，关闭密钥轮换。

步骤4 在弹出的确认是否关闭密钥轮换提示框中，单击“确定”，完成关闭密钥轮换操作。

----结束

3 密钥对管理

3.1 密钥对概述

密钥对通常用于非对称加密（也称为公钥加密）场景中，由公钥（Public Key）私钥（Private Key）组成。**公钥**可以公开分发给任何人，用于加密数据或验证签名；**私钥**必须严格保密，只有密钥所有者知道，用于解密或生成签名。

工作原理

- **加密与解密**
  - 当使用公钥加密数据时，只有对应的私钥才能解密。例如，A想安全地向B发送信息，A使用B的公钥对信息加密，然后B使用自己的私钥解密。
  - 如果使用私钥加密数据，公钥可以用来解密。这种方式主要用于数字签名，以证明信息的来源和完整性。
- **数字签名**：
  - A使用自己的私钥对数据生成签名，然后将数据和签名一起发送给B。
  - B使用A的公钥验证签名，如果验证通过，则说明数据未被篡改且确实来自A。

使用流程

操作	说明
创建密钥对	提供了创建密钥对的操作指导，以及删除密钥对的方法。
使用密钥对	提供了如何为弹性云服务器绑定密钥对、使用私钥登录Linux ECS、使用私钥获取Windows ECS的登录密码的操作指导。

操作	说明
管理密钥对	该章节为您提供如下操作指导： • 将私有密钥对升级为账号密钥对 • 下载公钥 • 导入私钥 • 导出私钥 • 清除私钥

3.2 创建密钥对

为安全起见，用户登录弹性云服务器时建议使用密钥对方式进行身份认证。用户可以新建一个密钥对，在登录弹性云服务器时进行鉴权。

说明

如果用户已有密钥对，可重复使用，无需多次创建。

创建密钥对的方式

创建密钥对的方式如表3-1所示。

表 3-1 创建密钥对的方式

创建密钥对的方式	区别

通过管理控制台创建密钥对
说明
• **账号密钥对**：
  • 首次创建时，需要具有Tenant Administrator系统角色的用户才能创建。
  • 账号密钥对可以由本账号下的多个IAM用户使用。
• **私有密钥对**：IAM用户通过管理控制台创建的私有密钥对，仅能自己使用。如果多个IAM用户需要使用相同的密钥对，可以将私有密钥对升级为账号密钥对，详见将私有密钥对升级为账号密钥对。
	• 公钥保存在华为云中，私钥可以由用户下载保存在本地，也可以将私钥托管在华为云中，由华为云统一管理。华为云采用KMS提供的加密密钥对私钥进行加密，确保托管私钥的安全存储与访问。
	• 通过管理控制台创建的密钥对支持的加解密算法为：
	  – SSH-ED25519
	  – ECDSA-SHA2-NISTP256
	  – ECDSA-SHA2-NISTP384
	  – ECDSA-SHA2-NISTP521
	  – SSH_RSA有效长度为：2048，3072，4096

通过PuTTYgen工具创建密钥对 **说明** PuTTYgen是一款公钥私钥生成工具，获取路径：https://www.putty.org/。	公钥和私钥均保存在用户本地。

创建密钥对的方式	区别
导入密钥对 **说明** 如果多个IAM用户需要使用相同的密钥对时，用户可以先通过其他工具（例如，PuTTYgen工具）创建密钥对，然后分别在两个IAM用户的资源中导入您创建的密钥对。	• 通过外部导入的SSH密钥对支持的加解密算法为： – SSH-DSS（不推荐） – SSH-ED25519 – ECDSA-SHA2-NISTP256 – ECDSA-SHA2-NISTP384 – ECDSA-SHA2-NISTP521 – SSH_RSA有效长度为：2048，3072，4096 • 导入的私钥支持PKCS8格式，如果使用PKCS1格式则需要进行转换。

创建密钥对

KPS支持三种方式创建密钥对，可根据需要进行选择：

通过管理控制台创建密钥对

步骤1 登录DEW管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤4 默认进入“账号密钥对”页签，根据用户使用需求，自主选择创建私有密钥对或者账号密钥对。

步骤5 单击“创建密钥对”，进入“创建密钥对”页面，输入密钥对名称，如图3-1所示。

图 3-1 创建密钥对

步骤6 （可选）选择“密钥对类型”。

说明

- 创建私有密钥对时，必须保证该账号下已有账号密钥对（创建的账号密钥对或私有密钥对升级的账号密钥对），该参数才会生效。否则，该参数无效，默认只会创建SSH_RSA_2028的密钥对。
- 当前仅RSA算法支持windows系统。

步骤7 如果需要托管私钥，请阅读并勾选“我同意将密钥对私钥托管”。在“KMS加密”中选择加密密钥。如果不需要托管私钥，请跳过此步骤。

- “列表选择”：适用于使用本账号的密钥或共享密钥的场景。
  - “默认密钥”：KPS采用KMS提供的加密密钥对私钥进行加密，KMS为KPS提供的默认密钥为“kps/default”。
  - “自定义密钥”：您也可以通过KMS平台创建自定义密钥来对私钥加密，具体操作请参见**创建密钥**。如果想使用RAM创建的共享密钥，确认接受共享后，可以在KMS加密的下拉框最下方选择共享密钥，密钥名称后会显示来自共享。
- “手工输入”：适用于使用授权的密钥场景，仅支持对称算法密钥ID，请勿输入非对称算法密钥ID。创建授权后，用户可以通过切换手工输入方式，输入密钥ID后使用被授权密钥加密。授权密钥操作可参见**创建授权**。

图 3-2 托管私钥

步骤8 请阅读《密钥对管理服务免责声明》并勾选“我已阅读并同意《密钥对管理服务免责声明》”。

步骤9 单击“确定”，浏览器自动执行下载任务，私钥文件将自动下载到本地。

须知

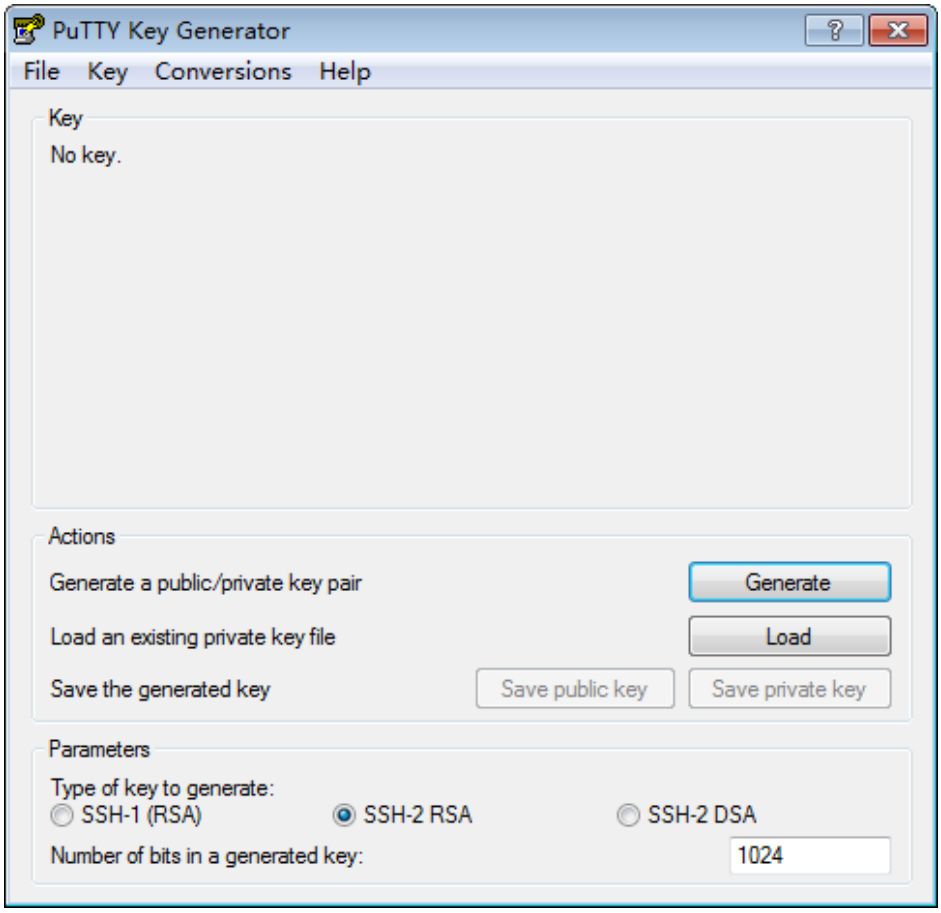
- 如果用户没有进行私钥托管，为保证安全，私钥只能下载一次，请妥善保管。如果不慎遗失，您可以通过重置密码或重置密钥对的方式，重新给弹性云服务器绑定密钥对，具体可参照**解绑密钥对后用户无法登录ECS时如何处理?** 进行处理。
- 如果用户已授权华为云托管私钥，可根据需要将托管的私钥导出使用。

----结束

通过 PuTTYgen 工具创建密钥对

步骤1 生成公钥和私钥文件，双击“PUTTYGEN.exe”，打开“PuTTY Key Generator”。如图3-3所示。

图 3-3 PuTTY Key Generator



步骤2 请根据表3-2设置参数。

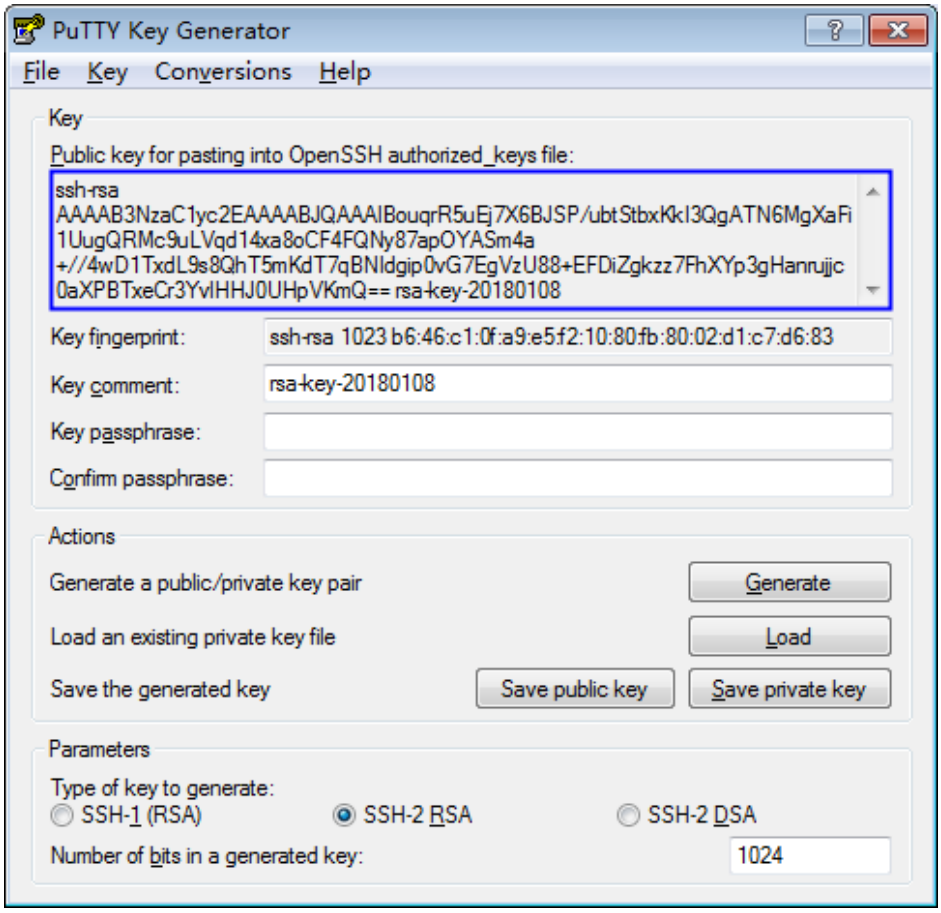
表 3-2 生成密钥对参数说明

参数	参数说明
Type of key to generate	• 通过外部导入的SSH密钥对支持的加解密算法为： – SSH-DSS（不推荐） – SSH-ED25519 – ECDSA-SHA2-NISTP256 – ECDSA-SHA2-NISTP384 – ECDSA-SHA2-NISTP521 – SSH_RSA有效长度为：2048，3072，4096 • 导入的私钥支持PKCS8格式，如果使用PKCS1格式则需要进行转换。
Number of bits in a generated key	

步骤3 单击“Generate”，生成一个公钥和一个私钥，如图3-4所示。

蓝框中标记的内容为生成的公钥内容。

图 3-4 生成公钥和私钥文件



步骤4 复制蓝框中的公钥内容，并将其粘贴在文本文档中，以“.txt”格式保存在本地。

须知

请勿直接单击“Save public key”保存公钥文件。如果用户使用“Save public key”保存公钥，公钥内容的格式会发生变化，不能直接导入管理控制台使用。

步骤5 根据以下方式，选择保存私钥的格式，可保存为“.ppk”或者“.pem”格式的私钥。

须知

为保证安全，私钥只能下载一次，请妥善保管。

表 3-3 私钥文件格式

私钥文件格式	私钥使用场景	保存方法
“.pem”格式	• 使用**Xshell**工具登录Linux操作系统云服务器 • 将私钥托管在管理控制台	1. 选择“Conversions > Export OpenSSH key”。 2. 保存私钥到本地。例如：kp-123.pem。
	获取Windows操作系统云服务器的密码	1. 选择“Conversions > Export OpenSSH key”。 **说明** 请勿填写“Key passphrase”信息，否则会导致获取密码失败。 2. 保存私钥到本地。例如：kp-123.pem。
“.ppk”	使用**PuTTY**工具登录Linux操作系统云服务器	1. 在“PuTTY Key Generator”界面，选择“File > Save private key”。 2. 保存私钥到本地。例如：kp-123.ppk。

根据需要正确保存公钥和私钥文件后，可将密钥对导入管理控制台使用。

----结束

导入密钥对

确保已有IAM用户下没有相同名称的私有密钥对，如果已经创建了相同名称的私有密钥对，导入账号密钥对时会提示密钥对名称已存在。导入的私钥支持PKCS8格式，如果使用PKCS1格式则需要进行转换。

步骤1 **登录DEW管理控制台**。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤4 默认进入“账号密钥对”页签，根据用户使用需求，自主选择导入私有密钥对或者账号密钥对。

步骤5 单击“导入密钥对”，在弹出“导入密钥对”对话框中，单击，导入公钥文件，如图3-5所示。

图 3-5 导入密钥对

说明

- 当前支持批量导入，最多一次支持导入10个公钥。
- 用户可自定义导入密钥对的名称。
- 如果提示名称已存在，是由于其他IAM用户创建了同名的私有密钥对，需修改密钥对名称。

步骤6 如果需要托管私钥，请确认并勾选“我同意将密钥对私钥托管”，如图 托管私钥所示。如果不需要托管私钥，请跳过此步骤。

图 3-6 托管私钥

1. 将私钥内容复制并粘贴至“私钥内容”文本框中。
2. 在“KMS加密”下拉列表中选择加密密钥。
   - “列表选择”：适用于使用本账号的密钥或共享密钥的场景。
     - “默认密钥”：KPS采用KMS提供的加密密钥对私钥进行加密，KMS为KPS提供的默认密钥为“kps/default”。
     - “自定义密钥”：您也可以通过KMS平台创建自定义密钥来对私钥加密，具体操作请参见**创建密钥**。如果想使用RAM创建的共享密钥，确认接受共享后，可以在KMS加密的下拉框最下方选择共享密钥，密钥名称后会显示来自共享。
   - “手工输入”：适用于使用授权的密钥场景，仅支持对称算法密钥ID，请勿输入非对称算法密钥ID。创建授权后，用户可以通过切换手工输入方式，输入密钥ID后使用被授权密钥加密。授权密钥操作可参见**创建授权**。

步骤7 请阅读《密钥对管理服务免责声明》后，勾选“我已阅读并同意《密钥对管理服务免责声明》”。

步骤8 单击“确定”，导入密钥对。

----结束

删除密钥对

如果创建或导入的密钥对不再使用时，可以删除密钥对。

- 执行删除操作后，密钥对将被彻底删除，不可恢复，请谨慎操作。
- 如果用户已导入私钥，执行删除操作时，会将该私钥一起删除。
- 如果用户删除控制台上已配置到弹性云服务器的公钥，而用户本地已保存私钥，用户可正常使用私钥登录弹性云服务器，删除操作对弹性云服务器的登录没有任何影响。

步骤1 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤2 在目标密钥对所在行，单击“删除”。

说明

如果您已经将密钥对升级为账号密钥对，请在“账号密钥对”列表中，执行以下操作。

步骤3 如果未开启删除验证，在确认删除提示框中输入“DELETE”后，单击“确定”，完成删除操作。

如果开启删除验证，选择验证方式后，单击“获取验证码”，在验证码对话框中输入获取的验证码，单击“确定”，完成删除操作。

说明

如果需要关闭操作保护，可以在账号的安全设置 > 敏感操作中关闭。也可以单击删除页面的“关闭操作保护”

----结束

3.3 使用密钥对

3.3.1 为弹性云服务器绑定密钥对

当用户购买Linux操作系统的弹性云服务器使用的是“密码方式”登录弹性云服务器时，如果用户需要将“密码方式”修改为“密钥对方式”，可通过管理控制台绑定密钥对，KPS将使用密钥对配置弹性云服务器。绑定完成后，用户可直接使用对应的私钥登录该弹性云服务器。

操作指导

本章节为您提供的操作指导如**表3-4**所示。

表 3-4 操作指导

操作	使用场景	前提条件	约束条件
绑定密钥对 • **单个绑定密钥对** • **批量绑定密钥对**	使用密钥对方式登录弹性云服务器。	• 弹性云服务器的状态处于“运行中”或者“关机”状态。 • 待重置密钥对的弹性云服务器使用的是华为云提供的公共镜像。 • 执行密钥对绑定操作是通过修改服务器的“/root/.ssh/authorized_keys”文件的方式来写入用户公钥。请确保绑定密钥对前，该文件没有被修改过，否则，绑定密钥对会失败。 • 弹性云服务器安全组SSH端口（默认22）需对网段100.125.0.0/16提前放通。	• 在管理控制台上，不支持对Windows操作系统的弹性云服务器进行密钥对的绑定操作。 • 公共镜像上，不支持CoreOS、openEuler、FreeBSD（Other）、Kylin V10 64bit、UnionTech OS Server 20、Euler 64bit和CentOS Stream 8 64bit系统进行密钥对的绑定操作。 • 用户最多可同时选择10个弹性云服务器绑定密钥对。
查看密钥对	通过密钥对管理界面查看密钥对的信息，包括密钥对的“名称”、“指纹”、“私钥”。	-	-
重置密钥对	用户私钥丢失，使用新的密钥对重新绑定弹性云服务器。	• 待重置密钥对的弹性云服务器使用的是华为云提供的公共镜像。 • 执行密钥对重置操作是通过修改服务器的“/root/.ssh/authorized_keys”文件的方式来替换用户公钥。请确保重置密钥对前，该文件没有被修改过，否则，重置密钥对会失败。 • 弹性云服务器的状态处于“关机”状态。	-

操作	使用场景	前提条件	约束条件
替换密钥对	用户私钥泄露，使用新的密钥对替换弹性云服务器内的公钥，替换完成后，用户需要使用本地保存的新密钥对的私钥登录该弹性云服务器，无法使用替换前的私钥登录该弹性云服务器。	• 待替换密钥对的弹性云服务器使用的是华为云提供的公共镜像。 • 执行密钥对替换操作是通过修改服务器的“/root/.ssh/authorized_keys”文件的方式来替换用户公钥。请确保替换密钥对前，该文件没有被修改过，否则替换公钥会失败。 • 弹性云服务器的状态处于“运行中”状态。	-

操作	使用场景	前提条件	约束条件
解绑密钥对	用户不想使用密钥对方式登录弹性云服务器，需要将登录方式改回“密码方式”。	• 弹性云服务器的状态处于“运行中”或者“关机”状态。 • 待解绑密钥对的弹性云服务器使用的是华为云提供的公共镜像。 • 执行密钥对解绑操作是通过修改服务器的“/root/.ssh/authorized_keys”文件的方式来清除用户公钥。请确保解绑密钥对前，该文件没有被修改过，否则，解绑密钥对会失败。	• 如果用户未设置登录弹性云服务器的密码，或者忘记登录密码，可以到弹性云服务器管理控制台重置该弹性云服务器的登录密码，详细信息请参见《弹性云服务器用户指南》。 • 当用户创建弹性云服务器使用的是“密钥对方式”登录时，用户解绑密钥对后，如果需要重新绑定密钥对，需要关机重新绑定密钥对。 • 为了能正常登录弹性云服务器，解绑密钥对后，请在弹性云服务器界面及时重置密码，详细信息请参见《弹性云服务器用户指南》。 • 支持通过KPS控制台解绑的操作系统：EulerOS、CentOS、RedHat、SUSE、Debian、OpenSUSE、Oracle Linux、Fedora、Ubuntu、Huawei Cloud EulerOS、AlmaLinux、Rocky Linux、CentOS Stream、openEuler。

单个绑定密钥对

步骤1 登录DEW管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤4 单击“云服务器列表”，显示云服务器列表页面。

步骤5 单击目标虚拟机所在行的“绑定”，弹出“绑定密钥对”对话框。

- 如果弹性云服务器处于“关机”状态，绑定密钥对的对话框，如图3-7所示。

图 3-7 绑定密钥对（一）

- 如果弹性云服务器处于“运行中”状态，需要提供“root密码”，如图3-8所示。

图 3-8 绑定密钥对（二）

说明

- 如果用户已有弹性云服务器的“root密码”，可直接输入root密码，直接进行密钥对绑定操作。
- 如果用户没有弹性云服务器的“root密码”，可将弹性云服务器关机，在弹性云服务器关机状态执行密钥对绑定操作。

步骤6 在“新密钥对”下拉列表中，选择新的密钥对。

步骤7 “端口”的默认参数为22，可进行自定义修改。

说明

使用自定义端口参数，需确认以下内容：

- 密钥对可以通过端口参数连接到弹性云服务器。修改弹性云服务器中的安全组配置具体操作请参见**配置安全组规则**。
- 弹性云服务器中的默认端口参数修改并确认端口开放。具体操作请参见**Linux云服务器SSH登录的安全加固**

步骤8 用户可根据自己的需要选择是否勾选“关闭密码登录方式”，默认勾选“关闭密码登录方式”。

说明

- 如果不关闭密码登录方式，用户既可使用密码登录弹性云服务器，也可以使用密钥对登录弹性云服务器。
- 如果关闭了密码登录方式，用户只能使用密钥对登录弹性云服务器，如果用户仍然需要使用密码登录弹性云服务器，可再次开启密码登录方式，具体操作请参见**关闭弹性云服务器的密码登录方式后如何重新开启？**。

步骤9 请阅读并勾选“我已阅读并同意《密钥对管理服务免责声明》”。

步骤10 单击“确定”，完成密钥对绑定操作。

- 如果弹性云服务器处于非关机状态，直接使用“root密码”方式绑定密钥对，等待约30秒可绑定成功。
- 如果弹性云服务器处于“关机”状态时绑定密钥对，等待约5分钟可绑定成功。

----结束

批量绑定密钥对

当多个弹性云服务器需要绑定同一个密钥对时，且弹性云服务器处于“运行中”状态时，可采用批量绑定密钥对的方式。

- 场景一：当多个需要绑定密钥对的弹性云服务器root密码相同时，使用“一键绑定”的方式，即选择要绑定的密钥对，并输入弹性云服务器的root密码即可。
- 场景二：当多个需要绑定密钥对的弹性云服务器root密码不同时，使用“单独绑定”的方式，即选择要绑定的密钥对，并分别输入弹性云服务器的root密码即可。

步骤1 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤2 单击“云服务器列表”，显示云服务器列表页面。

步骤3 勾选需要进行批量绑定的服务器，单击搜索框上方的“绑定”，弹出绑定对话框。

- 如果多个需要绑定的弹性云服务器密码相同，可一键选择密钥对并输入密码进行绑定，如**图 一键绑定**所示。

图 3-9 一键绑定

- 如果多个需要绑定的弹性云服务器密码不同，可选择单独绑定，如图 **单独绑定**所示。

图 3-10 单独绑定

说明

选择一键绑定时，只允许使用同一密钥对进行绑定。

----结束

查看密钥对

该任务指导用户通过密钥对管理界面查看密钥对的信息，包括密钥对的“名称”、“指纹”、“私钥”。

步骤1 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

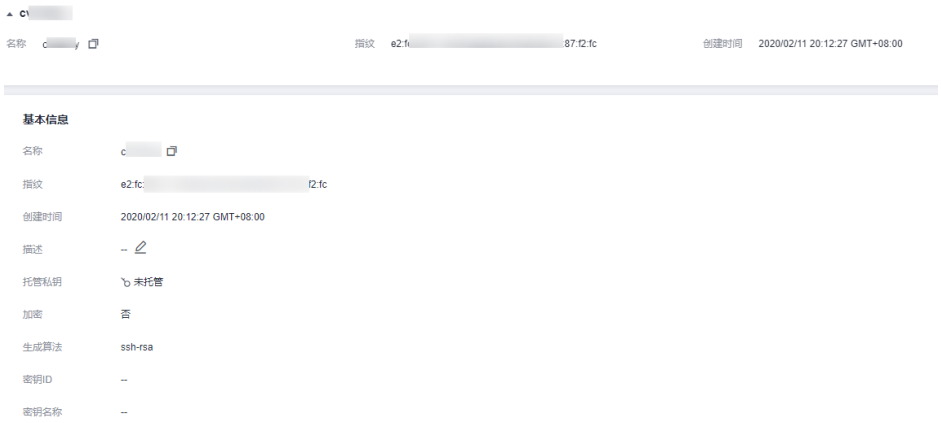
步骤2 单击“私有密钥对”，在密钥对列表中查看密钥对的信息。

说明

密钥对列表中包含创建和导入的密钥对的“名称”、“指纹”、“私钥”以及“状态”。

步骤3 单击目标密钥对的名称，显示密钥对详细信息以及使用该密钥对的弹性云服务器列表，如图3-11所示。

图 3-11 密钥对详细信息



说明

当用户购买弹性云服务器，选择的是使用“密钥对方式”登录时，购买成功后，选择的密钥对即与弹性云服务器绑定。

绑定密钥对的弹性云服务器，参数说明如表3-5所示。

表 3-5 弹性云服务器参数说明

参数名	参数说明
ECS 名称/ID	弹性云服务器的名称与ID。
状态	弹性云服务器的状态： • 运行中 • 创建中 • 故障 • 关机
私有IP地址	私有IP地址。
弹性IP	弹性IP地址。

参数名	参数说明
绑定密钥对	绑定弹性云服务器的密钥对。

步骤4 单击“云服务器列表”，显示云服务器列表页面。

图 3-12 云服务器列表

步骤5 单击任务状态旁边的数字，查看密钥对执行失败记录，如图3-13所示。

密钥对执行重置或者替换的状态：

：正在执行

：执行失败

说明

- 单击指定密钥对执行失败记录所在行的“删除”，删除失败记录；或者单击“删除所有失败记录”，删除所有的失败记录。
- 单击“了解更多”，查看相关文档。

图 3-13 密钥对执行失败记录

----结束

重置密钥对

如果用户私钥丢失，用户可通过管理控制台使用新的密钥对重新配置弹性云服务器，重置完成后，用户需要使用本地保存的新密钥对的私钥登录该弹性云服务器，无法使用重置前的私钥登录该弹性云服务器。

- 待重置密钥对的弹性云服务器使用的是华为云提供的公共镜像。

- 执行密钥对重置操作是通过修改服务器的“/root/.ssh/authorized_keys”文件的方式来替换用户公钥。请确保重置密钥对前，该文件没有被修改过，否则，重置密钥对会失败。
- 弹性云服务器的状态处于“关机”状态。

步骤1 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤2 单击“云服务器列表”页签，单击目标弹性云服务器所在行的“重置”，弹出重置密钥对的对话框，如图3-14所示。

图 3-14 重置密钥对

步骤3 在“新密钥对”下拉列表中选择新的密钥对。

步骤4 单击“确定”，等待约10分钟后，完成该弹性云服务器密钥对的重置操作。

----结束

替换密钥对

如果用户私钥泄露，用户可通过管理控制台使用新的密钥对替换弹性云服务器内的公钥，替换完成后，用户需要使用本地保存的新密钥对的私钥登录该弹性云服务器，无法使用替换前的私钥登录该弹性云服务器。

- 待替换密钥对的弹性云服务器使用的是华为云提供的公共镜像。
- 执行密钥对替换操作是通过修改服务器的“/root/.ssh/authorized_keys”文件的方式来替换用户公钥。请确保替换密钥对前，该文件没有被修改过，否则替换公钥会失败。
- 弹性云服务器的状态处于“运行中”状态。

步骤1 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤2 单击“云服务器列表”页签，单击目标弹性云服务器所在行的“替换”，弹出“替换密钥对”对话框，如图3-15所示。

图 3-15 替换密钥对

步骤3 在“新密钥对”下拉框中选择新的密钥对。

步骤4 单击“选择文件”，上传原密钥对的私钥（“.pem”格式），或者将原密钥对的私钥拷贝至文本框中。

说明

- 上传或者拷贝至文本框的私钥必须是“.pem”格式文件，如果是“.ppk”格式文件，请参考**如何将“.ppk”格式的私钥文件转化为“.pem”格式**进行转换。

步骤5 单击“确定”，等待约1分钟后，完成该弹性云服务器密钥对的替换操作。

----结束

解绑密钥对

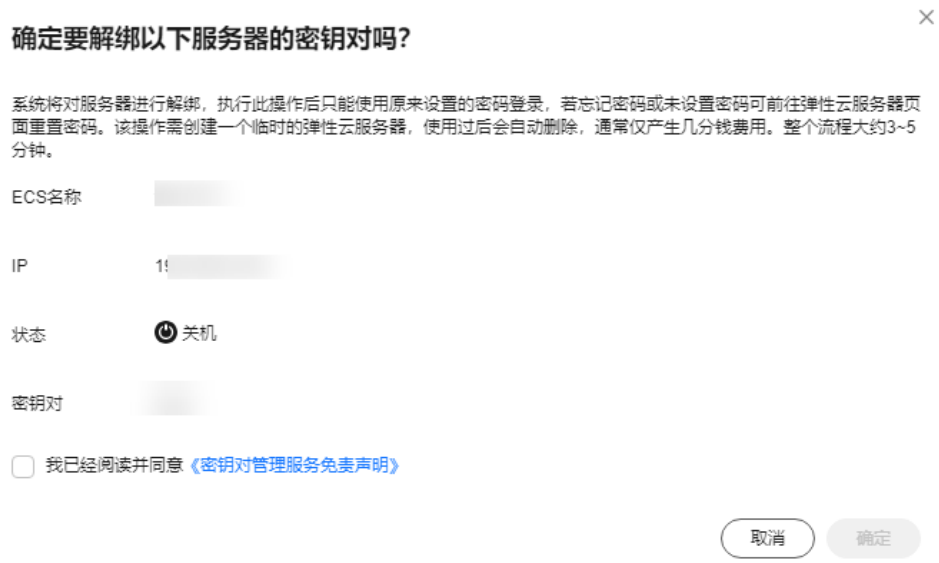
如果用户需要将“密钥对方式”修改为“密码方式”，可通过密钥对管理界面解绑密钥对。

步骤1 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤2 单击“云服务器列表”页签，单击目标弹性云服务器所在行的“解绑”，弹出解绑密钥对的对话框。

- 如果弹性云服务器处于“关机”状态，解绑密钥对的对话框，如**图3-16**所示。

图 3-16 解绑密钥对（一）



- 如果弹性云服务器处于“运行中”状态，解绑密钥对的对话框，如图3-17所示。

图 3-17 解绑密钥对（二）

步骤3 如果在弹性云服务器处于“运行中”状态时解绑密钥对，需要上传私钥。单击“选择文件”，上传现有密钥对的私钥（“.pem”格式），或者将私钥拷贝至文本框中。如果在弹性云服务器处于“关机”状态，请跳过此步骤。

说明

- 上传或者拷贝至文本框的私钥必须是“.pem”格式文件，如果是“.ppk”格式文件，请参考**如何将“.ppk”格式的私钥文件转化为“.pem”格式**进行转换。

步骤4 单击“确定”，等待约1分钟后，完成该弹性云服务器密钥对的解绑操作。

说明

为了能正常登录弹性云服务器，解绑密钥对后，请在弹性云服务器界面及时重置密码，详细信息请参见《弹性云服务器用户指南》。

----结束

3.3.2 使用私钥登录 Linux ECS

用户通过管理控制台创建或者导入密钥对后，在购买弹性云服务器时，“登录方式”选择“密钥对”，并选择创建或者导入的密钥对。

用户购买弹性云服务器成功后，可使用密钥对的私钥登录弹性云服务器。

前提条件

- 使用的登录工具（如PuTTY、Xshell）与待登录的弹性云服务器之间网络连通。
- 弹性云服务器已经绑定弹性IP地址。
- 已获取该弹性云服务器的私钥文件。

约束条件

弹性云服务器的私钥文件必须满足以下格式要求：

表 3-6 选择私钥文件格式

本地使用的操作系统	登录Linux弹性云服务器使用的工具	私钥文件格式
Windows操作系统	**Xshell**	“.pem”
	PuTTY	“.ppk”
Linux操作系统	-	“.pem”或“.ppk”

如果私钥文件格式不满足要求，请参考**如何转换私钥文件格式?** 进行转换。

本地使用 Windows 操作系统

如果您本地使用Windows操作系统登录Linux弹性云服务器，可以按照以下方式登录弹性云服务器。

方式一：使用PuTTY登录

步骤1 双击“PuTTY.EXE”，打开“PuTTY Configuration”。

步骤2 选择“Connection > data”，在“Auto-login username”处输入镜像的用户名。

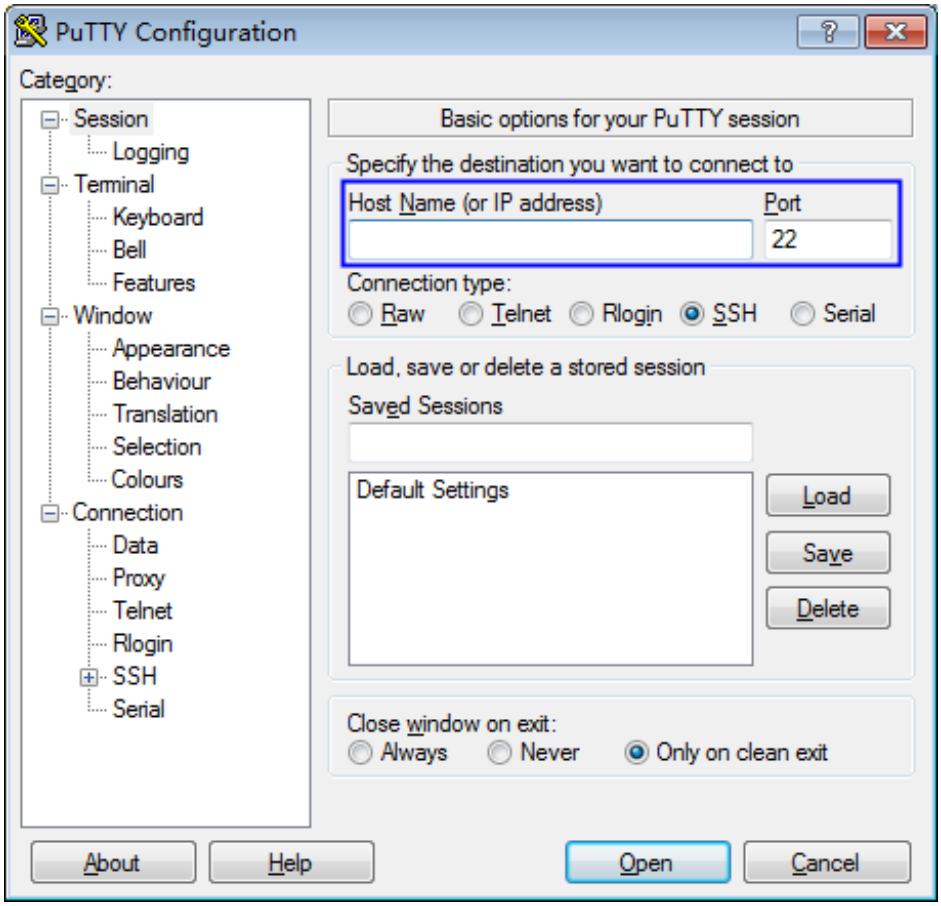
说明

- 如果是“CoreOS”的公共镜像，镜像的用户名为“core”。
- 如果是“非CoreOS”的公共镜像，镜像的用户名为“root”。

步骤3 选择“Connection > SSH > Auth”，在“Private key file forauthentication”配置项中，单击“Browse”，选择私钥文件（“.ppk”格式）。

步骤4 单击“Session”，在“Host Name (or IP address)”下的输入框中输入弹性云服务器的弹性IP地址。

图 3-18 配置弹性 IP



步骤5 单击“Open”，登录弹性云服务器。

----结束

方式二：使用Xshell登录

步骤1 打开Xshell工具。

步骤2 执行以下命令，SSH远程连接弹性云服务器。

ssh *用户名@弹性IP*

示例：

ssh *root@192.168.1.1*

步骤3 （可选）如果系统弹窗提示“SSH安全警告”，此时，需要单击“接受并保存”。

步骤4 选择“Public Key”，并单击“用户密钥(K)”栏的“浏览”。

步骤5 在“用户密钥”窗口中，单击“导入”。

步骤6 选择本地保存的私钥文件（“.pem”格式），并单击“打开”。

步骤7 单击“确定”，登录弹性云服务器。

----结束

本地使用 Linux 操作系统

如果您是在Linux操作系统上登录Linux弹性云服务器，可以按照下面方式登录。下面步骤以私钥文件是“kp-123.ppk”为例进行介绍。

步骤1 在您的Linux计算机的命令行中执行以下命令，变更权限。

chmod 600 *[/path/kp-123.ppk](#)*

说明

*path*为密钥文件的存放路径。

步骤2 执行以下命令登录弹性云服务器。

ssh -i *[/path/kp-123](#)* root@*弹性IP地址*

说明

- *path*为密钥文件的存放路径。
- *弹性IP地址*为弹性云服务器绑定的弹性IP地址。

----结束

3.3.3 使用私钥获取 Windows ECS 的登录密码

登录Windows操作系统的弹性云服务器时，需要使用密码方式登录。此时，用户需要先根据购买弹性云服务器时下载的私钥文件，获取该弹性云服务器初始安装时系统生成的管理员密码（Administrator账户或Cloudbase-init设置的账户）。该密码为随机密码，安全性高，请放心使用。

用户可以通过管理控制台获取Windows弹性云服务器的登录密码。

前提条件

已获取登录弹性云服务器的私钥文件（“.pem”格式）。

约束条件

- 为安全起见，建议用户获取初始密码后，执行清除密码操作，清除系统中记录的初始密码信息。

  该操作不会影响弹性云服务器的正常登录与运行。清除密码后，系统不能恢复获取密码功能，因此，请在执行清除密码操作前，记录弹性云服务器密码信息。详细信息请参见《弹性云服务器用户指南》。
- 用户也可以通过调用API接口的方式获取Windows弹性云服务器的初始密码，请参考《弹性云服务器API参考》。

- 获取的弹性云服务器的私钥文件必须是“.pem”格式。
  如果是“.ppk”格式文件，请参考**如何将“.ppk”格式的私钥文件转化为“.pem”格式**进行转换。

操作步骤

步骤1 **登录DEW管理控制台**。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击，选择“计算 > 弹性云服务器”。

步骤4 在弹性云服务器列表，选择待获取密码的弹性云服务器。

步骤5 选择“操作 > 更多”，单击“获取密码”。

步骤6 通过密钥文件获取密码，有以下两种方式：

- 单击“选择文件”，从本地上传密钥文件。
- 将密钥文件内容复制粘贴在空白文本框中。

步骤7 单击“获取密码”，获取随机密码。

----结束

3.4 管理密钥对

3.4.1 将私有密钥对升级为账号密钥对

如果用户希望本账号下的所有用户都能查看或使用本账号下已创建的密钥对，可将创建的密钥对升级为账号密钥对。

前提条件

- 已创建密钥对或者已导入密钥对。
- 需要具有Tenant Administrator系统角色的用户至少执行一次升级，升级密钥对个数不限。
- 已成功申请升级密钥对。

约束条件

- 如果密钥对名称与其他子用户的私有密钥对重名，将无法升级。
- 私有密钥对升级为账号密钥对时，不会占用账号密钥对配额。
- 私有密钥对升级为账号密钥对后，不支持回退为私有密钥对。

操作步骤

步骤1 **登录DEW管理控制台**。

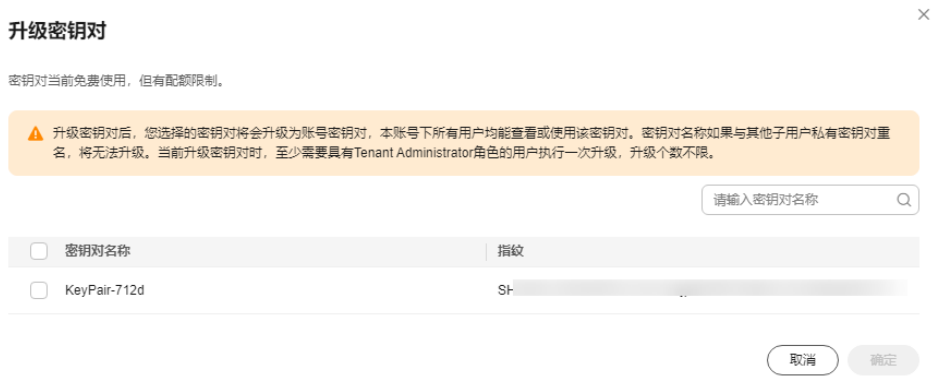
步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤4 单击“私有密钥对”页签，单击“升级密钥对”。

步骤5 在弹出的页面中，勾选需要升级为账号密钥对的密钥对名称，单击“确定”，如图3-19所示。

图 3-19 升级密钥对



说明

已升级的密钥对，在“账号密钥对”列表中可以查看。

----结束

3.4.2 管理公钥和私钥

通过KPS控制台创建密钥对后，公钥自动保存在华为云中，私钥由用户下载保存在本地。用户也可以根据自己的需要将私钥托管在华为云中，由华为云统一管理。华为云采用KMS提供的加密密钥对私钥进行加密，确保托管私钥的安全存储与访问。

该章节为您提供如下操作指导：

- **下载公钥**
- **导入私钥**
- **导出私钥**
- **清除私钥**

约束条件

- 一个公钥下只能导入与这个公钥匹配的私钥。
- 上传或者拷贝至文本框的私钥必须是“.pem”格式文件，如果是“.ppk”格式文件，请参考**如何将“.ppk”格式的私钥文件转化为“.pem”格式**进行转换。

下载公钥

KPS支持将公钥下载到本地，该任务指导用户通过密钥对管理界面下载公钥。

步骤1 **登录DEW管理控制台**。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤4 在目标密钥对所在行操作列，单击“下载公钥”，获得公钥的“.txt”格式文件。

----结束

导入私钥

为了方便用户管理本地的私钥，用户可将私钥导入管理控制台，由KPS统一管理。导入的私钥由KMS提供的密钥加密，保证用户私钥的存储、导入或者导出安全。当用户需要使用私钥时，可从管理控制台多次下载，为了保证私钥的安全，请妥善保管下载的私钥。

步骤1 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤2 单击目标公钥所在行的“导入私钥”，弹出的“导入私钥”界面，如**图3-20**所示。

图 3-20 导入私钥

步骤3 单击“选择文件”，选择本地保存的私钥文件（“.pem”格式），或者将私钥内容复制并粘贴至“私钥内容”文本框中。

说明

- 一个公钥下只能导入与这个公钥匹配的私钥。
- 上传或者拷贝至文本框的私钥必须是“.pem”格式文件，如果是“.ppk”格式文件，请参考**如何将“.ppk”格式的私钥文件转化为“.pem”格式**进行转换。

步骤4 在“KMS加密”下拉列表中选择加密密钥。

说明

- KPS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“kps/default”。
- 用户使用KMS创建的自定义密钥，具体操作请参见**创建密钥**。

步骤5 单击“确定”，完成私钥托管。

----结束

导出私钥

如果用户已将私钥托管在管理控制台上，用户可根据自己的需要多次下载托管的私钥，为了保证私钥的安全，请妥善保管下载的私钥。

用户导出私钥时，使用的是托管私钥时加密私钥的加密密钥进行解密。如果加密密钥已被彻底删除，那么导出私钥将会失败。

步骤1 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤2 单击目标密钥对所在行的“导出私钥”，弹出“导出私钥”对话框，如**图3-21**所示。

图 3-21 导出私钥对话框

说明

当前支持批量导出私钥，勾选多个待导出私钥后，单击“导出私钥”，完成批量导出操作。

步骤3 单击“确定”，浏览器自动执行下载任务，下载私钥文件。

须知

用户导出私钥时，使用的是托管私钥时加密私钥的加密密钥进行解密。如果加密密钥已被彻底删除，那么导出私钥将会失败。

----结束

清除私钥

如果用户不需要使用托管在管理控制台的私钥时，可通过“密钥对管理”界面将托管的私钥清除。

清除私钥后，用户无法再从华为云获取私钥，请谨慎操作。如果需要再次托管私钥，可将私钥再导入管理控制台。

步骤1 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤2 单击目标密钥对所在行“操作”列的“更多 > 清除私钥”。

步骤3 在弹出的对话框中，单击“确定”，清除私钥。

说明

清除私钥后，用户无法再从华为云获取私钥，请谨慎操作。如果需要再次托管私钥，可将私钥再导入管理控制台。

----结束

4 凭据管理

4.1 凭据管理概述

“凭据”用于验证身份和授权访问的证明信息。在信息安全和身份认证领域，凭据是确保只有授权用户才能访问系统、资源或服务的关键机制。凭据的类型包括：用户名和密码、数字证书、密钥对（公钥和私钥）、令牌、生物识别信息、一次性密码、智能卡等。

通用凭据

通用凭据支持在各场景下进行自定义凭据的全生命周期管理，用户可以通过凭据管理服务实现对数据库账号口令、服务器口令、SSH Key、访问密钥等各类型凭据的统一管理、检索与安全存储，且支持多个版本管理，方便用户实现凭据轮转。

轮转凭据

数据库凭据泄露是导致数据泄露的主要途径。凭据管理服务支持托管RDS、TaurusDB凭据，能够全自动的定期轮转与手动立即轮转，满足各类数据库凭据管理场景，降低业务数据面临的安全风险。

表 4-1 轮转凭据支持凭据类型

凭据类型	数据库类型\实例
RDS凭据	MySQL、PostgreSQL、SQLServer、MariaDB、TaurusDB。
TaurusDB凭据	TaurusDB实例

通用凭据与轮转凭据差异

表 4-2 凭据差异

凭据类型	通用凭据	轮转凭据

使用场景	各场景下自定义凭据的全生命周期管理	• RDS凭据：自动托管华为云RDS数据库凭据 • TaurusDB凭据：自动托管华为云TaurusDB数据库凭据
是否支持自动轮转	否，需要用户自行触发轮转	是，支持单双用户两种经典轮转模型

轮转凭据使用流程

流程说明：

1. 创建一个轮转凭据。
   - 设置凭据名称、标签等。
   - 配置自动轮转策略。
2. 应用系统在使用过程中需要访问数据库时，可以向CSMS服务请求访问凭据，获取凭据值，调用API接口详情请参见**查询凭据版本和凭据值**。
3. 应用系统通过访问返回的凭据值解析明文数据，获取账号和密码后，可以访问该用户对应的目标数据库。

⚠ 注意

- 开启自动轮转后，数据库实例所托管的密码将定时轮转更新，请确认使用该数据库实例的应用端已完成代码适配，可在数据库连接建立时，动态获取最新凭据。
- 不要轻易缓存凭据中的任何信息，避免账号密码轮转后失效，导致数据库连接失败。

4.2 轮转策略

单用户轮转

单用户轮转策略适用于单一用户场景，多用于低频次轮转、可靠性要求不高的账号，这是最简单的轮换策略，适用于大多数用例。但是在密码重置切换的瞬间，凭据的当前版本可能暂时无法使用。

您可以使用单用户轮换来实现：

- 在创建时选择或者新建一个数据库账户作为凭据值储存。
- 访问数据库。密钥轮换时不会删除数据库连接，轮换后的新连接使用新凭据。

双用户轮转

双用户轮转多用于轮转频次较高、轮转可靠性要求高的账号，托管两个相同权限的账号，每次轮转SYSPREVIOUS的凭据版本，保证密码重置切换的瞬间，程序访问不被中断。在轮转时先将新版本的凭据改为SYSPENDING状态，通过调用RDS接口重置密

码，重置完成后新版本凭据的SYSPENDING状态会改为SYSCURRENT，之前SYSCURRENT状态的凭据变为SYSPREVIOUS，即视为完成整个轮转流程。

- 在创建时选择或者新建两个数据库账户作为凭据值储存
- 两个凭据值交替轮转，用户每次都是去获取的SYSCURRENT的凭据值

4.3 创建凭据

通过凭据管理管理服务创建凭据实现凭据托管服务，新创建的凭据，会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”。

凭据值是凭据的具体内容，用于在身份验证过程中证明用户的身份或授权。它可以是多种形式的数据，具体取决于所使用的身份验证机制。常见的凭据值包括：

- **用户名和密码**：用户名是用户的身份标识，密码是用户身份验证的关键凭据值。
- **数字证书**：证书中的公钥和身份信息是凭据值，用于验证用户或设备的身份。
- **密钥对**：私钥是凭据值，用于签名和解密操作。
- **令牌（Token）**：令牌是一个临时的凭据值，用于验证用户的身份。
- **生物识别信息**：指纹、面部识别、虹膜识别等生物特征数据是凭据值。
- **一次性密码（OTP）**：通过短信、邮件或专门的应用程序生成的一次性密码是凭据值。

约束条件

- CSMS最多支持创建500个凭据。
- 凭据大小最大限制为64kb。
- 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。
- RDS凭据支持的数据库引擎为：MySQL、PostgreSQL、SQLServer、MariaDB、TaurusDB。
- TaurusDB凭据支持选择TaurusDB类型数据库。
- 首次开启轮转时，当用户确认授权后，CSMS会在当前区域当前项目下，帮助用户自动创建委托授权。因此，用户需要确认账号拥有IAM相关权限：iam:permissions:grantRoleToAgencyOnProject、iam:agencies:listAgencies、iam:roles:listRoles、iam:agencies:createAgency、iam:permissions:checkRoleForAgencyOnProject、iam:roles:createRole。

  根据轮转凭据类型不同，创建的委托不同：

  - **RDS凭据**
    - 创建一个名为**CSMSAccessFunctionGraph**的委托 ，账号是**op_svc_kms**，权限名称是**CSMSAccessFunctionGraph**，使用项目级服务策略，包含**函数工作流服务（FunctionGraph）**的同步执行函数的权限（functiongraph:function:invoke）。
    - 创建一个名为**FunctionGraphAgencyForRotateRDSByCSMSV3**委托 ，云服务是**FunctionGraph**，权限名称是**FunctionGraphAgencyForRotateRDSByCSMSV3**，使用项目级服务策略，包含：
      - **凭据管理服务（CSMS）**的相关权限：csms:secret:getVersion、csms:secret:listVersion、csms:secret:createVersion、

csms:secret:getStage、csms:secret:get、csms:secret:updateStage。

- **虚拟私有云云服务（VPC）**的相关权限：vpc:ports:create、vpc:vpcs:get、vpc:ports:get、vpc:ports:delete、vpc:subnets:get。
- **密钥管理服务（KMS）**的相关权限：kms:cmk:createDataKey、kms:cmk:decryptDataKey。
- **云数据库（RDS）**的相关权限：rds:password:update。

– **TaurusDB凭据**

- 创建一个名为**CSMSAccessFunctionGraph**的委托，账号是**op_svc_kms**，权限名称是**CSMSAccessFunctionGraph**，使用项目级服务策略，包含**函数工作流服务（FunctionGraph）**的同步执行函数的权限（functiongraph:function:invoke）。
- 创建一个名为**FunctionGraphAgencyForRotateGaussDBByCSMSV3**委托，云服务是**FunctionGraph**，权限名称是**FunctionGraphAgencyForRotateGaussDBByCSMSV3**，使用项目级服务策略，包含：
  - **凭据管理服务（CSMS）**的相关权限：csms:secretVersion:get、csms:secretVersion:list、csms:secretVersion:create、csms:secretStage:get、csms:secret:get、csms:secretStage:update。
  - **虚拟私有云云服务（VPC）**的相关权限：vpc:ports:create、vpc:vpcs:get、vpc:ports:get、vpc:ports:delete、vpc:subnets:get。
  - **密钥管理服务（KMS）**的相关权限：kms:dek:create、kms:dek:decrypt。
  - **云数据库TaurusDB**的相关权限：gaussdb:user:modify。

创建凭据

CSMS支持创建通用凭据和轮转凭据，可根据需要进行选择。

创建通用凭据

步骤1 **登录DEW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 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

步骤4 单击“创建凭据”。弹出“创建凭据”页面，如**图 创建凭据**所示，填写参数，参数说明如**表4-3**所示。

图 4-1 创建凭据

表 4-3 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，默认选择“通用凭据”。支持“通用凭据”和“轮转凭据”两种凭据类型，两种凭据的区别请参见**凭据概述**。
凭据名称	待创建凭据的名称。 **说明** 仅支持输入大小写英文字母、数字、“.”“-”、“_”。
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”。 **说明** 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。

参数名称	参数说明
设置凭据值	配置为待加密的用户凭据键/值或明文凭据。 凭据值是凭据的具体内容，用于在身份验证过程中证明用户的身份或授权。它可以是多种形式的数据，具体取决于所使用的身份验证机制。常见的凭据值包括： • **用户名和密码**：用户名是用户的身份标识，密码是用户身份验证的关键凭据值。 • **数字证书**：证书中的公钥和身份信息是凭据值，用于验证用户或设备的身份。 • **密钥对**：私钥是凭据值，用于签名和解密操作。 • **令牌（Token）**：令牌是一个临时的凭据值，用于验证用户的身份。 • **生物识别信息**：指纹、面部识别、虹膜识别等生物特征数据是凭据值。 • **一次性密码（OTP）**：通过短信、邮件或专门的应用程序生成的一次性密码是凭据值。
KMS加密	支持以下两种KMS加密方式： • “列表选择”：适用于使用本账号的密钥或共享密钥的场景。可选择默认密钥“csms/default”或用户在KMS已创建的自定义密钥 • “手工输入”：输入授权密钥的ID。适用于使用授权的密钥场景，仅支持对称算法密钥ID，请勿输入非对称算法密钥ID。 **说明** • CSMS使用KMS提供的加密密钥对凭据值进行加密，使用KMS加密功能时，可选择KMS创建的默认密钥“csms/default”。 • 用户使用KMS创建的自定义密钥，具体操作请参见**创建密钥**。 • 用户使用授权密钥，创建授权后，用户可以通过切换手工输入方式，输入密钥ID后使用被授权密钥加密。授权密钥操作可参见**创建授权**。
高级配置	• 关联事件 为凭据选择关联事件，可以查看凭据轮转、版本过期等信息。 • 描述信息 凭据的描述信息。 • 标签 可根据自己的需要为凭据添加标签。 **说明** 最多可以给单个凭据添加20个标签。

步骤5 单击“下一步”。

步骤6 单击“下一步”，确认创建的信息。

步骤7 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

创建轮转凭据

步骤1 **登录DEW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 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

步骤4 单击“创建凭据”，选择轮转凭据。

图 4-2 创建轮转凭据

步骤5 在弹出的“创建凭据”对话框中，填写参数，参数说明如表4-4所示。

表 4-4 轮转凭据参数说明

参数名称	参数说明
凭据类型	创建轮转凭据类型，可选择以下类型凭据。 • RDS凭据 • TaurusDB凭据
凭据名称	待创建凭据的名称。
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”。 **说明** 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。
选择数据库类型	“凭据类型”选择“轮转凭据 > RDS凭据”时，需要选择数据库类型。 RDS凭据支持的数据库类型为：MySQL、PostgreSQL、SQLServer、MariaDB、TaurusDB。
选择RDS实例	选择目标数据库类型对应的RDS实例。
选择TaurusDB实例	“凭据类型”选择“轮转凭据 > TaurusDB凭据”时，需要选择TaurusDB类型数据库实例。 单击“查看TaurusDB实例”，可跳转到云数据库TaurusDB控制台购买数据库实例。
设置凭据值	待加密的账号名以及密码。 • 选择“单账号托管”时，需要填入一个可使用的数据库账号名及口令。 • 选择“双账号托管”时，填入一个可使用的数据库账号及口令后，会克隆一个具有一致权限的账号。需勾选“我已知晓风险”。 具体差异可以参考凭据概述中的**轮转策略**。
KMS加密	支持以下两种KMS加密方式： • “列表选择”：适用于使用本账号的密钥或共享密钥的场景。可选择默认密钥“csms/default”或用户在KMS已创建的自定义密钥 • “手工输入”：输入授权密钥的ID。适用于使用授权的密钥场景，仅支持对称算法密钥ID，请勿输入非对称算法密钥ID。 **说明** • CSMS使用KMS提供的加密密钥对凭据值进行加密，使用KMS加密功能时，可选择KMS创建的默认密钥“csms/default”。 • 用户使用KMS创建的自定义密钥，具体操作请参见**创建密钥**。 • 用户使用授权密钥，创建授权后，用户可以通过切换手工输入方式，输入密钥ID后使用被授权密钥加密。授权密钥操作可参见**创建授权**。

参数名称	参数说明
高级配置	• 关联事件 为凭据选择关联事件，可以查看凭据轮转、版本过期等信息。 • 描述信息 凭据的描述信息。 • 标签 可根据自己的需要为凭据添加标签。 **说明** 最多可以给单个凭据添加20个标签。

----结束

相关操作

查看凭据信息

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”。

步骤1 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

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4-5所示。

图 4-3 凭据列表

表 4-5 凭据列表参数说明

参数	操作说明
凭据名称/ID	凭据的名称和ID。
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、RDS凭据、TaurusDB凭据等。
关联事件	凭据创建时关联的事件通知。
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

步骤3 用户可单击凭据名称，查看凭据详细信息，如图4-4所示。

- 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。

图 4-4 凭据详细信息

----结束

下载凭据备份

该章节指导用户将凭据下载到本地进行备份。

步骤1 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

步骤2 在目标凭据所在行的“操作”列，单击“下载凭据备份”。

凭据文件将下载到本地，凭据文件样式为“凭据名称.secretbackup”。

----结束

恢复凭据备份

数据加密服务支持使用凭据备份，手动恢复凭据数据至凭据列表。恢复凭据备份后凭据ID与原凭据ID不同。

只能上传 secretbackup 文件，且不能超过5M。

步骤1 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

步骤2 单击“恢复凭证备份”，进入页面后，“添加文件”后，单击“确定”，完成恢复凭证备份。

图 4-5 恢复凭证备份

----结束

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。

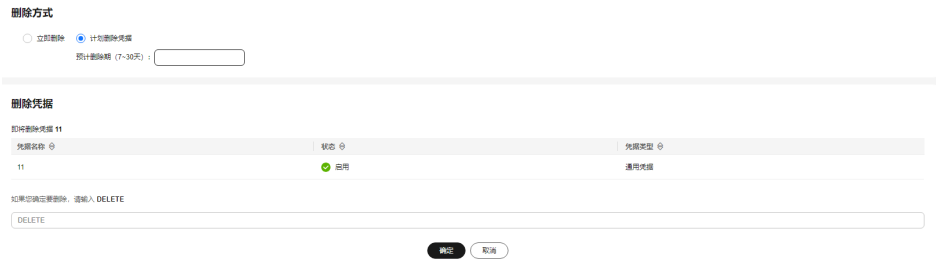
- “计划删除凭据”不会立即删除，凭据管理会将该操作按用户指定时间推迟执行，推迟时间范围为7天～30天。在推迟删除时间未到时，如果需要重新使用该凭据，可以执行撤销删除凭据操作。如果超过推迟时间，凭据将被彻底删除，请谨慎操作。
- 关于处于计划删除状态的凭据计费情况，请参见**计划删除的凭据是否还计费？**。
- “立即删除”凭据，删除后如果需找回，需提前下载凭据备份用于恢复凭据，请谨慎操作。

步骤1 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

步骤2 在需要删除的凭据所在行，单击“删除”。

步骤3 在“删除凭据”界面，选择删除方式，如果选择计划删除凭据，需填写“推迟删除”的时间。

图 4-6 推迟删除时间



步骤4 如果未开启删除验证，在确认删除提示框中输入“DELETE”后，单击“确定”，完成删除操作。

如果开启删除验证，选择验证方式后，单击“获取验证码”，在验证码对话框中输入获取的验证码，单击“确定”，完成删除操作。

说明

如果需要关闭操作保护，可以在账号的安全设置 > 敏感操作中关闭。也可以单击删除页面的“关闭操作保护”

----结束

4.4 管理凭据

4.4.1 轮转凭据版本

您如果长时间不更新凭据，凭据内保护的重要信息（例如：重要密码、令牌、证书、SSH密钥、API密钥等）的泄露风险也会增加，定期轮换凭据会增加所保护的明文信息安全性。该任务指导用户如何开启凭据轮转。

约束条件

- 凭据类型为轮转凭据。
- 最小轮转周期为4小时。
- 凭据账号必须是目标数据库里已存在的数据库账号。
- 首次开启轮转时，当用户确认授权后，CSMS会在当前区域当前项目下，帮助用户自动创建委托授权。因此，用户需要确认账号拥有IAM相关权限：iam:permissions:grantRoleToAgencyOnProject、iam:agencies:listAgencies、iam:roles:listRoles、iam:agencies:createAgency、iam:permissions:checkRoleForAgencyOnProject、iam:roles:createRole。

  根据轮转凭据类型不同，创建的委托不同：

  - **RDS凭据**
    - 创建一个名为**CSMSAccessFunctionGraph**的委托 ，账号是**op_svc_kms**，权限名称是**CSMSAccessFunctionGraph**，使用项目级服务策略，包含**函数工作流服务（FunctionGraph）**的同步执行函数的权限（functiongraph:function:invoke）。
    - 创建一个名为**FunctionGraphAgencyForRotateRDSByCSMSV3**委托 ，云服务是**FunctionGraph**，权限名称是**FunctionGraphAgencyForRotateRDSByCSMSV3**，使用项目级服务策略，包含：
      - **凭据管理服务（CSMS）**的相关权限：csms:secret:getVersion、csms:secret:listVersion、csms:secret:createVersion、csms:secret:getStage、csms:secret:get、csms:secret:updateStage。
      - **虚拟私有云云服务（VPC）**的相关权限：vpc:ports:create、vpc:vpcs:get、vpc:ports:get、vpc:ports:delete、vpc:subnets:get。
      - **密钥管理服务（KMS）**的相关权限：kms:cmk:createDataKey、kms:cmk:decryptDataKey。
      - **云数据库（RDS）**的相关权限：rds:password:update。
  - **TaurusDB凭据**
    - 创建一个名为**CSMSAccessFunctionGraph**的委托 ，账号是**op_svc_kms**，权限名称是**CSMSAccessFunctionGraph**，使用项目级服务策略，包含**函数工作流服务（FunctionGraph）**的同步执行函数的权限（functiongraph:function:invoke）。
    - 创建一个名为**FunctionGraphAgencyForRotateGaussDBByCSMSV3**委托 ，云服务是**FunctionGraph**，权限名称是**FunctionGraphAgencyForRotateGaussDBByCSMSV3**，使用项目级服务策略，包含：
      - **凭据管理服务（CSMS）**的相关权限：csms:secretVersion:get、csms:secretVersion:list、csms:secretVersion:create、csms:secretStage:get、csms:secret:get、csms:secretStage:update。
      - **虚拟私有云云服务（VPC）**的相关权限：vpc:ports:create、vpc:vpcs:get、vpc:ports:get、vpc:ports:delete、vpc:subnets:get。
      - **密钥管理服务（KMS）**的相关权限：kms:dek:create、kms:dek:decrypt。

- **云数据库TaurusDB**的相关权限：gaussdb:user:modify。

手动轮转

步骤1 **登录DEW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 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

步骤4 单击凭据名称，进入凭据详细信息页面。

步骤5 在“当前版本”区，单击“立即轮转”。

步骤6 在“立即轮转”页面，输入“ROTATE”后，单击“确认”。

步骤7 待右上角出现提示立即轮转成功，即为版本切换完成。

步骤8 版本轮转完成后，最新凭据版本的版本状态显示为SYSCURRENT。

----结束

自动轮转

步骤1 **登录DEW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 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

步骤4 单击凭据名称，进入凭据详细信息页面。

步骤5 单击右上角按钮“设置轮转策略”，在设置轮转策略页面，如**图 自动轮转开关**所示，打开自动轮转开关。

图 4-7 自动轮转开关

步骤6 选择自动轮转周期，勾选轮转提示，单击“确定”。待右上角出现提示设置轮转策略成功提示，即为设置成功。

步骤7 开启自动轮转后，若凭据版本轮转失败，在当前版本区域可查看轮转失败次数，单击轮转失败次数即可查看轮转失败记录。

说明

- 连续轮转3次失败，会关闭凭据的自动轮转按钮。
- 轮转失败记录不能手动执行删除，保存时间一个月，满一个月后会自动删除。

----结束

4.4.2 为凭据添加标签

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。

前提条件

已**创建凭据**。

为凭据添加标签

步骤1 **登录DEW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 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

步骤4 单击凭据名称，进入凭据详细信息页面。

步骤5 在“标签”区，单击“添加标签”，弹出添加标签对话框，如**图4-8**所示，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4-6**所示。

图 4-8 添加标签

说明

- 如果需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，用户可在TMS中创建预定义标签。更多关于预定义标签的信息，请参见《标签管理用户指南》。
- 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 4-6 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128个字符。 ● 首尾不能包含空格。 ● 不能以_sys_开头。 ● 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255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6 单击“确定”，完成标签的添加。

----结束

相关操作

- **修改标签值**：
  a. 在凭据列表中，单击凭据名称，进入凭据详细信息页面。
  b. 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。
  c. 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。
- **删除标签**：
  a. 在凭据列表中，单击凭据名称，进入凭据详细信息页面。

b. 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。
c. 在弹出的删除标签对话框中单击“确认”，完成标签的删除。

4.4.3 为凭据关联事件

通过事件通知，用户可以了解凭据放入版本相关变化等信息，通知的消息内容为JSON格式，主要适用于机机场景的自动化解析。该任务指导用户通过事件通知界面创建事件。

创建新的事件，可选择的事件类型包括新版本创建、版本过期、凭据轮转、凭据删除。

约束条件

- 用户最多可创建30个事件。
- 创建SMN消息类型时，需要依赖消息通知服务，该服务按实际用量付费，详见**SMN计费说明**。

  说明

  在设置告警通知前，建议您先在“消息通知服务”中创建“消息主题”。
- 创建EG消息类型时，需要在“事件网格 EG”控制台创建云服务事件订阅。详细操作请参见**创建事件订阅**。

为凭据关联事件

步骤1 **登录DEW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 在左侧导航树中，选择“凭据管理 > 事件通知”，进入“事件通知”页面。

步骤4 单击右上角“创建事件”，弹出创建事件页面。

图 4-9 创建事件

表 4-7 创建事件参数说明

参数名称	参数说明
事件名称	待创建事件的名称。 **说明** 仅支持输入英文字符、数字、“-”、“_”。
状态	启用、禁用。默认选择启用。
消息类型	支持两种消息类型： • SMN（消息通知服务）：每当凭据对象发生所选定的基础事件时，凭据管理服务（CSMS）通过事件通知中的SMN订阅主题发送通知消息。 • EG（事件网格）：每当凭据对象发生所选定的基础事件时，凭据管理服务（CSMS）通过事件网格服务中创建的云服务事件订阅来通知云服务。创建事件订阅时，“事件源”选择“HC.DEW.CSMS”。详细操作请参见**创建事件订阅**。

参数名称	参数说明
主题名称	消息类型选择“SMN”时，需要配置此参数。 单击下拉列表选择已创建的主题或者单击“查看SMN主题”创建新的主题，用于配置接收告警通知的终端。 单击“查看SMN主题”创建新主题的操作步骤如下： 1. 参见**创建主题**创建一个主题。 2. 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见**添加订阅**。 3. 确认订阅。添加订阅后，完成订阅确认。 更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。
消息模板	可选参数。可选择在SMN中创建的消息模板，或选择“暂不选择”。
通道名称	消息类型选择“EG”时，需要配置此参数。当前仅支持选择“default”，由事件网格自动创建且不可修改的一条默认的云服务事件通道，用于接收云服务事件源产生的事件。云服务事件源产生的事件只能发布到云服务事件通道。
事件类型	支持选择的事件类型。包含新版本创建、版本过期、凭据轮转、凭据删除等。

步骤5 单击“确定”，完成事件创建。

步骤6 在事件列表中查看已创建的事件。事件状态默认为“启用”。

图 4-10 事件列表

----结束

查看事件通知记录

步骤1 在左侧导航树中，选择“凭据管理 > 事件通知”，进入“事件通知”页面。

步骤2 单击“通知记录”页签，进入通知记录查看页面。

步骤3 在通知记录界面可看到已关联事件的凭据进行的变更。

----结束

相关操作

- **查看事件详细信息**：在事件列表中，单击事件名称，可查看事件详细信息。

- **编辑事件**：在目标事件所在行的“操作”列，单击“编辑”，进入编辑事件界面，根据需求修改“消息类型”、“事件类型”等配置。
- **启用事件**：
  a. 在目标事件所在行的“操作”列，单击“编辑”，进入编辑事件界面。
  b. “状态”选择“启用”，将禁用状态事件修改为启用状态。
  c. 单击“确定”，右上角提示更新事件状态成功，完成启用事件操作。
- **禁用事件**：
  a. 在目标事件所在行的“操作”列，单击“编辑”，进入编辑事件界面。
  b. “状态”选择“禁用”，将启用状态事件修改为启用状态。
  c. 单击“确定”，右上角提示更新事件状态成功，完成禁用事件操作。
- **删除事件**：在目标事件所在行的“操作”列，单击“删除”，弹出“删除事件”对话框，输入“DELETE”后，单击“确定”，完成删除操作。

说明

事件通知需要取消所有关联的凭据才能删除。如果未取消关联凭据，会导致删除失败。

4.4.4 管理凭据版本

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。

该章节为您提供如下操作指导：

- 存入和查看凭据值
- 管理凭据版本状态
- 设置凭据版本到期时间

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。
  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。
- RDS凭据、TaurusDB凭据不建议手动存入凭据值。
- “SYSCURRENT”和“SYSPREVIOUS”为服务内建的凭据状态，不可删除。

存入和查看凭据值

步骤1 登录DEW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 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

步骤4 单击凭据名称，进入凭据详细信息页面。

步骤5 在“当前版本”区，单击“存入凭据值”，弹出存入凭据值对话框，如图4-11所示，在弹出的“存入凭据值”对话框中输入“凭据键/值”或“明文凭据”。

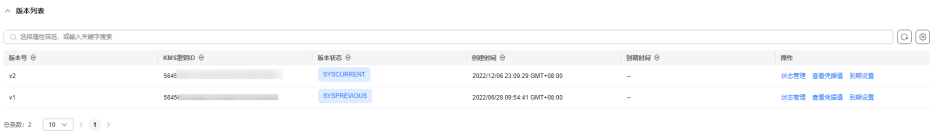
图 4-11 存入凭据值

步骤6 可以为存入的凭据值选择一个到期时间，时间可具体到秒。设置完成后可在凭据版本列表中查看到期时间。例如2023年6月30日19：52：59。

步骤7 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。

步骤8 在“版本列表”区，单击目标凭据版本所在行的“查看凭据值”，如图4-12所示，弹出查看凭据值对话框。

图 4-12 凭据版本列表



步骤9 如果开启敏感操作保护，在单击“查看凭据值”后，需要通过操作验证才可以查看凭据值。

说明

如果需开启敏感操作保护，具体操作参见**敏感操作保护**。

通常情况下，凭据值由应用程序调用API获取，如果您确实需要在服务控制台查看凭据值，建议开启敏感操作保护，在查看凭据值时进行信息确认，保证数据安全。请再次确认并单击“确定继续”。

步骤10 单击“确定”，关闭当前对话框。

----结束

管理凭据版本状态

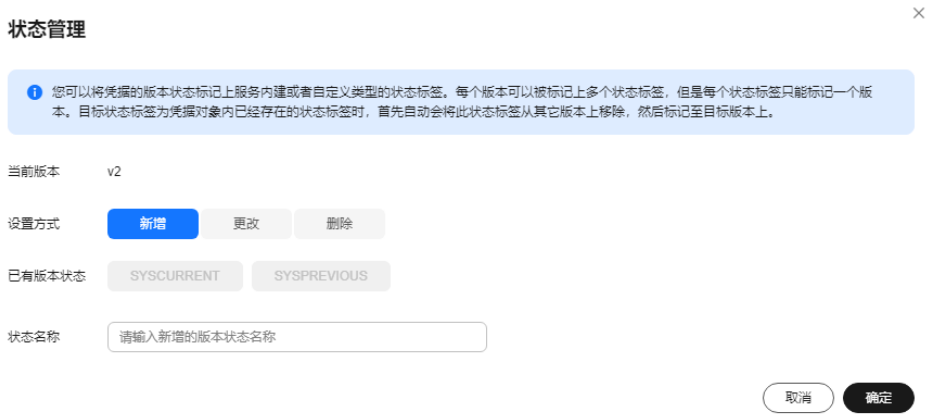
步骤1 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

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。

图 4-13 状态管理



- 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

设置凭据版本到期时间

该任务指导用户通过凭据详情页面进行凭据版本到期时间设置。

步骤1 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

步骤2 单击凭据名称，进入凭据详细信息页面。

步骤3 在“当前版本”区，单击目标凭据版本所在行的“到期设置”。

步骤4 在“到期设置”页面，选择当前凭据版本期望的到期时间，单击“确定”，完成凭据版本到期时间设置。

说明

到期时间可以设置日期或者设置天数。设置到期天数后，界面会提示具体到期日期。

图 4-14 到期时间设置

----结束

5 专属加密

5.1 专属加密概述

专属加密的核心在于为用户提供**独立的加密资源**和**定制化的加密服务**，以满足特定的业务需求和安全要求。它通常包括以下几个关键要素：

- **独立的加密资源**：用户可以独享加密硬件（如硬件安全模块HSM）、密钥管理系统（KMS）等资源，确保加密操作的独立性和安全性。
- **定制化的加密策略**：根据用户的具体需求，定制加密算法、密钥管理策略、访问控制策略等。
- **数据隔离**：通过物理或逻辑隔离，确保用户的数据与其他用户的数据完全分开，防止数据泄露。

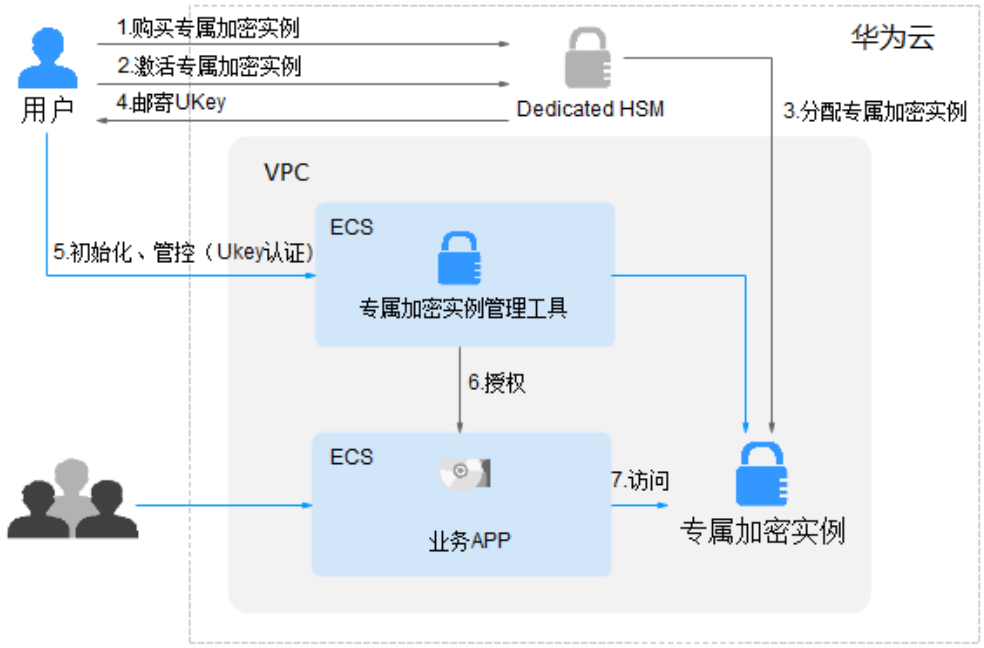
限制说明

- 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。
- 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5-1**所示。

图 5-1 操作指引



操作指引说明如表5-1所示。

表 5-1 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，华为云安全服务团队评估专属加密实例的使用场景，确认所购买的专属加密实例能够满足业务需求，即可下单付款。	用户
2	激活专属加密实例	您购买专属加密实例后，通过Dedicated HSM界面实例化专属加密实例。您需要选择专属加密实例所属的虚拟私有云，以及专属加密实例的功能类型，详细操作请参见**激活专属加密实例**。	用户
3	分配专属加密实例	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，如果满足要求，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

编号	操作步骤	说明	操作角色
4	获取UKey、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。 如果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。 **说明** 可通过提交**提交工单**方式提供Ukey收件地址以及联系安全专家指导。	专属加密服务安全专家
5	初始化、管控（UKey认证）	1. 在专属加密实例管理节点上安装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**。	用户
6	安装安全代理软件并授权	在业务APP节点上安装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
7	访问	业务APP通过API或者SDK的方式访问专属加密实例。	用户

专属加密与密码系统服务的关系

专属加密服务（Dedicated HSM）和密码系统服务（CPCS）在云平台中都用于提供加密和安全功能，但它们在功能、应用场景和管理方式上存在一定的区别和联系。具体如**表5-2**所示。

表 5-2 专属加密与密码系统服务的区别和联系

服务	专属加密服务（Dedicated HSM）	密码系统服务（CPCS）
功能对比	• 提供专属的硬件安全模块（HSM），用户可以独占使用加密硬件资源。 • 主要功能包括加解密、签名、验签、密钥生成和安全存储。 • 支持多种加密算法，并符合国家密码管理局认证。 • 适合对安全性和性能要求极高的场景，如金融支付、电子签名等。	• 提供一站式的密码服务管理平台，支持集群化部署。 • 功能更加广泛，包括加解密、签名验签、密钥管理、时间戳服务、电子签章服务、数据库加密等。

应用场景对比	• 适用于对数据安全性和性能有极高要求的场景，如金融支付、电子签名、证券业务等。 • 常用于满足监管合规要求的企业和机构。	• 适用于需要多种密码服务和快速通过密评的企业和机构。 • 适合电子合同、电子发票、电子病历等需要多种密码服务的场景。
管理方式对比	• 用户通过管理客户端进行初始化和权限管理。 • 提供高安全性的硬件资源，用户完全控制密钥的生成、存储和访问授权。	• 通过控制台集中管理，支持自动化部署和监控。 • 提供集群化部署能力，支持弹性伸缩和应用级隔离。
联系	• **共同目标**：两者都旨在提供安全的加密服务，保护数据的安全性和完整性。 • **集成与互补**：在某些场景下，两者可以集成使用。例如，专属加密服务（Dedicated HSM）可以作为密码系统服务（CPCS）的底层加密资源，提供高性能的加密运算支持。	

5.2 购买专属加密实例

5.2.1 创建专属加密实例

在创建专属加密实例时，您需要根据自己的需要选择专属加密实例的区域，并提供您的联系方式。

铂金版专属加密实例的费用由以下两部分组成：

- 初装费用：一次性收取，创建专属加密实例时支付。
- 包周期费用：按购买周期收取，**激活专属加密实例**时支付。

前提条件

已获取管理控制台的登录账号（ 拥有Ticket Administrator权限与KMS Administrator权限）与密码。

约束条件

创建成功后，您需要激活专属加密实例，激活后，系统会为您分配符合您业务需求的专属加密实例。

操作步骤

步骤1 **登录DEW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 单击页面右上方的“创建专属加密实例”。

步骤4 专属加密实例仅支持“包年/包月”的“计费模式”。

图 5-2 计费模式

步骤5 选择“当前区域”、“当前项目”。

图 5-3 选择区域

说明

- 当前区域选择确认后，当前项目选择默认。
- 当前项目仅支持使用默认项目，不支持自主创建。

步骤6 选择专属加密实例版本，如**图3 铂金版**所示，相关参数说明如**表5-3**所示。

图 5-4 铂金版

表 5-3 规格参数说明

参数名称	说明
服务版本	专属加密提供“铂金版”的专属加密实例。
加密算法	专属加密实例支持的加密算法。 • 对称算法：AES、DES • 非对称算法：RSA、DSA、ECDSA、ECDH • 摘要算法：SHA1、SHA256、SHA384
性能规格	铂金版专属加密实例支持的性能规格。 • 数据通讯协议：TCP/IP（最大并发链接：2048） • RSA2048签名运算性能：1500tps • RSA2048验签运算性能：25000tps • ECDSA256签名运算性能：23000tps • ECDSA256验签运算性能：9000tps • DSA2048签名运算性能：2800tps • DSA2048验签运算性能：3000tps
认证	通过FIPS 140-2 Level 3认证。

步骤7 设置“实例名称”。

图 5-5 实例名称

步骤8 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。

说明

- 企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。更多关于企业项目的信息，请参见**《什么是企业项目管理？》**。
- 如需开通企业项目，请参考**如何开通企业项目/企业多账号**。

步骤9 设置专属加密实例购买的时长和数量。

1. 选择“购买时长”。
   可以选择1个月～1年的购买时长。
2. 设置“购买数量”。
   您可以根据您的需要设置购买数量。
   为了保证业务的高可靠性，您至少需要购买2个及以上的专属加密实例。您最多可购买20个专属加密实例。

> **说明**
>
> 一个专属加密实例仅适用于测试，如需购买一个专属加密实例请联系华为云安全专家。

步骤10 （可选）用户可根据自己的需要为专属加密实例添加标签，输入“标签键”和“标签值”。

> **说明**
>
> - 当用户在创建专属加密实例完成后，需要为该实例添加标签，可在该实例所在行“操作”列，单击“标签”， 为该自定义密钥添加标签。更多修改、删除操作可参见**标签管理**。
> - 用户最多可以给单个实例添加20个标签。

步骤11 确认当前配置无误后，单击“立即购买”。如果您对价格有疑问，可以单击“了解计费详情”，了解产品价格。

步骤12 在“订单详情”页面，确认订单详情，阅读并勾选“我已阅读并同意《隐私政策声明》”。

步骤13 单击“去支付”，支付费用，在“付款”页面，选择付款方式进行付款。

步骤14 成功付款后，在专属加密实例列表界面，可以查看购买的专属加密实例信息。

当专属加密实例的“状态”为“安装中”时，表示专属加密实例购买成功。

----结束

5.3 激活并使用专属加密实例

5.3.1 激活专属加密实例

您需要激活专属加密实例才能使用。激活时需要支付专属加密实例的包周期费用。

该任务指导用户通过专属加密界面激活专属加密实例。

前提条件

专属加密实例的状态为“待激活”。

约束条件

- 实例名称只能由中文字符、英文字母、数字、下划线或者中划线组成。
- 每个专属加密实例会创建两个节点，用作访问后台加密机资源池；为了保障节点的高可用性，再给专属加密实例分配一个浮动IP。
- 如果创建专属加密实例失败，您可以单击该专属加密实例所在行的“删除”，删除专属加密实例，并以工单的形式申请退款。
- 成功创建专属加密实例后，不支持切换密码机类型。如果您想切换密码机类型，需要退订后重新购买。

操作步骤

步骤1 **登录DEW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 在左侧导航树中，选择“专属加密 > 实例列表”，进入“实例列表”页面。

步骤4 单击目标专属加密实例所在行的“激活”。

步骤5 选择“可用区”。

图 5-6 选择可用区

步骤6 填写实例化信息，如图5-7所示。相关参数说明如表5-4所示。

图 5-7 实例化专属加密实例

表 5-4 实例化参数说明

参数名称	说明	取值样例
实例名称	专属加密实例的名称。 **说明** 实例名称只能由中文字符、英文字母、数字、下划线或者中划线组成。	DedicatedHSM-3c98-0002
企业项目	为专属加密实例绑定对应企业项目。	default

参数名称	说明	取值样例
密码机类型	可选择的密码机类型，包含“金融密码机”、“服务器密码机”和“签名验证服务器”。 ● 金融密码机：提供密钥管理及密码运算服务，支持IC卡发卡、交易验证、数据加密、数字签名、动态口令认证等业务功能。 ● 服务器密码机：提供安全完善的密钥管理服务，提供高性能的、多任务并行处理的数据签名/验签、数据加密/解密等密码运算服务。 ● 签名验证服务器：通过数字签名、数字信封、数字摘要等密码技术手段，保障用户数据的完整性、机密性、抗抵赖性和事后追溯性。	金融密码机
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-test-dhsm
子网	界面显示所有可选择的子网，系统自动为专属加密实例分配3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》。 **说明** 每个专属加密实例会创建两个节点，用作访问后台加密机资源池；为了保障节点的高可用性，再给专属加密实例分配一个浮动IP。	subnet-test-dhsm（192.168.0.0/24）
是否支持绑定弹性公网	勾选后，可以为专属加密实例绑定弹性公网IP，开通公网访问专属加密实例。	-
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》。	WorkspaceUserSecurityGroup

步骤7 如果您购买的是“标准版”的专属加密实例：

请单击“立即激活”，回到专属加密实例列表界面，可以查看激活的专属加密实例信息。

当专属加密实例的“状态”为“创建中”时，表示专属加密实例激活成功。

步骤8 如果您购买的是“铂金版”的专属加密实例：

1. 选择“购买时长”。
   可以选择1个月～1年的购买时长。

   说明

   勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。
2. 确认当前配置无误后，单击“立即购买”。

如果您对价格有疑问，可以单击“了解计费详情”了解，了解产品价格。

3. 在“订单详情”页面，确认订单详情，阅读并勾选“我已阅读并同意《隐私政策声明》”。
4. 单击“去支付”，支付包周期费用。
5. 在“付款”页面，选择付款方式进行付款。

   成功付款后，在专属加密实例列表界面，可以查看激活的专属加密实例信息。

   当专属加密实例的“状态”为“创建中”时，表示专属加密实例已完成激活，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。

   分配后，分配状态有以下两种情况：

   - 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。

     说明

     如果创建专属加密实例失败，您可以单击该专属加密实例所在行的“删除”，删除专属加密实例，并以工单的形式申请退款。

   - 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”。

     说明

     成功创建专属加密实例后，不支持切换密码机类型，也不支持退订。如果您想切换密码机类型，需要重新购买。

----结束

5.3.2 使用专属加密实例

在您支付完成后，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 5-5 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》。	

名称	说明	来源
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。	请您根据自己的需要进行购买，详细操作请参见**购买弹性云服务器**。
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。

     说明

     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，具体操作参见**如何开通公网访问专属加密实例?**

     待初始化专属加密实例完成后，您可以解绑弹性公网IP。如果后续有需要，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、恢复密钥等操作。

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

5.4 管理专属加密实例

5.4.1 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DEW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 在左侧导航树中，选择“专属加密”，进入“专属加密”页面。

步骤4 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5-6所示。

表 5-6 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。

参数	参数说明
状态	专属加密实例的状态： ● 安装中 您支付了初装费用后，系统会对您购买的实例进行安装，专属加密实例处于“安装中”状态。 ● 待激活 系统已安装专属加密实例，您尚未对专属加密实例进行激活，专属加密实例处于“待激活”状态。 ● 创建中 您激活专属加密实例后，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 实例化专属加密实例后，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。
IP地址	专属加密实例的浮动IP地址。
到期时间	购买的专属加密实例的到期时间。

步骤5 用户可选择专属加密实例的名称，单击下方的^，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5-7所示。

表 5-7 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。

参数	参数说明
状态	专属加密实例的状态： ● 安装中 您支付了初装费用后，系统会对您购买的实例进行安装，专属加密实例处于“安装中”状态。 ● 待激活 系统已安装专属加密实例，您尚未对专属加密实例进行激活，专属加密实例处于“待激活”状态。 ● 创建中 您激活专属加密实例后，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 实例化专属加密实例后，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。
密码机类型	专属加密实例的密码机类型，包含“金融密码机”、“服务器密码机”和“签名服务器”。
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地址	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》。
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

5.4.2 为专属加密实例添加标签

标签用于标识专属加密实例。为加密实例添加标签，可方便用户对专属加密实例进行分类和查找。

为专属加密实例添加标签

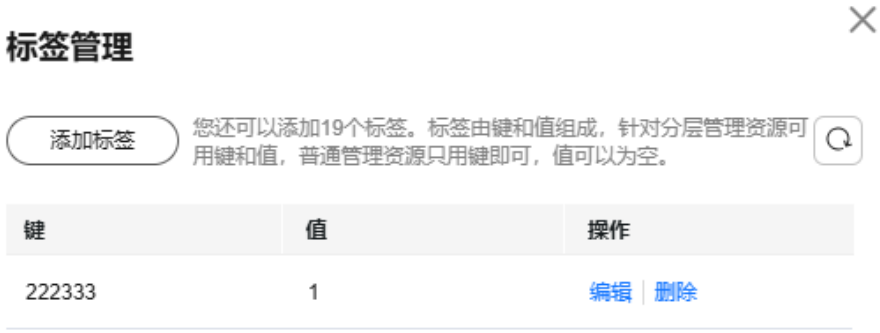
步骤1 登录DEW管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 在左侧导航树中，选择“专属加密”，进入“专属加密”页面。

步骤4 在右侧“操作”列，单击“标签管理”，弹出标签管理页面，如图 标签管理所示。

图 5-8 标签管理



步骤5 单击“添加标签”，在弹出的对话框中输入“标签键”和“标签值”，参数说明如表 标签参数说明所示。

图 5-9 添加标签

说明

- 如果需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，用户可在TMS中创建预定义标签。更多关于预定义标签的信息，请参见《标签管理用户指南》。
- 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 5-8 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128个字符。 ● 首尾不能包含空格。 ● 不能以_sys_开头。 ● 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255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6 单击“确定”，完成标签的添加。

----结束

修改标签值

步骤1 在左侧导航树中，选择“专属加密”，进入“专属加密”页面。

步骤2 单击目标专属加密实例所在行的“标签管理”，弹出“标签管理”对话框。

步骤3 单击“编辑”，弹出“编辑标签”对话框。修改标签值后单击“确定”，完成标签值修改。

----结束

删除标签

步骤1 在左侧导航树中，选择“专属加密”，进入“专属加密”页面。

步骤2 单击目标专属加密实例所在行的“标签管理”，弹出“标签管理”对话框。

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。

图 5-10 删除标签

步骤4 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

6 标签与配额

6.1 标签管理

6.1.1 标签概述

操作场景

标签是数据加密服务的标识。为数据加密服务添加标签，可以方便用户识别和管理拥有的数据加密资源。

您可以在创建资源时添加标签，也可以在资源创建完成后，在云资源的详情页添加标签。

标签命名规则

- 每个标签由一对键值对（Key-Value）组成。
- 每个数据加密服务资源最多可以添加20个标签。
- 对于每个资源，每个标签键（Key）都必须是唯一的，每个标签键（Key）只能有一个值（Value）。
- 标签共由两部分组成：“标签键”和“标签值”，其中，“标签键”和“标签值”的命名规则如**表 标签参数说明**所示。
- 标签以键值对的形式表示，用于标识存储库，便于对存储库进行分类和搜索。此处的标签仅用于存储库的过滤和管理。一个存储库最多添加10个标签。

  说明

  如您的组织已经设定数据加密服务的相关标签策略，则需按照标签策略规则为密钥、凭据等添加标签。标签如果不符合标签策略的规则，则可能会导致密钥、凭据创建失败，请联系组织管理员了解标签策略详情。

表 6-1 标签参数说明

参数	规则	样例
标签键	● 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。 ● 不能以_sys_开头。 ● 可以包含以下字符： – 中文 – 英文 – 数字 – 空格 – 特殊字符_.:=+-@	cost
标签值	● 可以为空。 ● 长度不超过255个字符。 ● 可以包含以下字符： – 中文 – 英文 – 数字 – 空格 – 特殊字符_.:=+-@	100

6.1.2 创建标签策略

标签策略简介

标签策略是策略的一种类型，可帮助您在组织账号中对资源添加的标签进行标准化管理。标签策略对未添加标签的资源或未在标签策略中定义的标签不会生效。

例如：标签策略规定为某资源添加的标签A，需要遵循标签策略中定义的大小写规则和标签值。如果标签A使用的大小写、标签值不符合标签策略，则资源将会被标记为不合规。

标签策略有如下两种应用方式：

1. 事后检查 —— 资源标签如果违反标签策略，则在资源在合规性结果中显示为不合规。

2. 事前拦截 —— 标签策略开启强制执行后，则会阻止在指定的资源类型上完成不合规的标记操作。

约束条件

只有组织管理员才可以创建标签策略，委托管理员无法执行此操作。

说明

在创建标签策略并将其附加到组织单元和账号之前，必须先启用标签策略，且只能使用组织的管理账号启用标签策略。具体操作请参见**启用和禁用标签策略**。

操作步骤

步骤1 以组织管理员或管理账号的身份登录华为云。

步骤2 单击页面左侧 ☰，选择“管理与监管 > 组织”，默认进入“组织管理”界面。

步骤3 单击左侧“策略管理”，进入策略管理页，单击“标签策略”，进入标签策略页面。

图 6-1 进入标签策略

步骤4 单击“创建”，进入标签策略创建页面。

图 6-2 创建策略

步骤5 输入策略名称。注意，创建的策略名称不能与已有策略名称重复。

步骤6 根据**标签策略语法**，标签策略内容。填写时，系统会自动校验语法。如不正确，请根据提示进行修正。

步骤7 （可选）为策略添加标签。在标签栏目下，输入标签键和标签值，单击添加。

步骤8 单击右下角“保存”后，如跳转到标签策略列表，则标签策略创建成功。

说明

如果需对标签策略进行修改、删除，可参见**修改、删除标签策略**。

具体绑定与解绑操作，参见**绑定和解绑标签策略**。

----结束

6.1.3 创建标签

本章节指导用户为已有密钥、凭据、专属加密实例添加标签。

约束条件

KMS不支持为默认密钥添加标签。

密钥管理

步骤1 登录DEW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 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤4 单击“标签”，进入标签管理页面。

步骤5 单击“添加标签”，弹出添加标签对话框，如图 添加标签所示，在弹出的“添加标签”对话框中输入“标签键”和“标签值”。

图 6-3 添加标签

说明

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

- 如果需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，用户可在TMS中创建预定义标签。更多关于预定义标签的信息，请参见《标签管理服务用户指南》。
- 当同时添加多个标签，需要删除其中一个待添加的标签时，可单击该标签所在行的“删除”，删除标签。

步骤6 单击“确定”，完成标签的添加。

----结束

凭据管理

步骤1 登录DEW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 在左侧导航树中，选择“凭据管理 > 凭据列表”，进入“凭据管理”页面。

步骤4 单击凭据名称，进入凭据详细信息页面。

步骤5 在“标签”区，单击“添加标签”，在弹出的“添加标签”对话框中输入“标签键”和“标签值”。

图 6-4 添加标签

说明

- 如果需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，用户可在TMS中创建预定义标签。更多关于预定义标签的信息，请参见《标签管理用户指南》。
- 当同时添加多个标签，需要删除其中一个待添加的标签时，可单击该标签所在行的“删除”，删除标签。

步骤6 单击“确定”，完成标签的添加。

----结束

专属加密

步骤1 单击管理控制台左上角，选择区域或项目。

步骤2 在左侧导航树中，选择“专属加密”，进入“专属加密”页面。

步骤3 在右侧“操作”列，单击“标签管理”，弹出标签管理页面。

步骤4 单击“添加标签”，在弹出的对话框中输入“标签键”和“标签值”。

说明

- 如果需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，用户可在TMS中创建预定义标签。更多关于预定义标签的信息，请参见《标签管理用户指南》。
- 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 单击“确定”，完成标签的添加。

----结束

6.1.4 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，如果进行多个标签组合搜索，则搜索结果的每个自定义密钥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。

操作步骤

步骤1 登录DEW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 单击搜索框，选择“资源标签”中的“标签键”和“标签值”后，显示满足搜索条件的自定义密钥列表。

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，如果进行多个标签组合搜索，则搜索结果的每个自定义密钥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。

----结束

6.1.5 修改标签值

本章节指导用户对已创建标签进行修改。

操作步骤

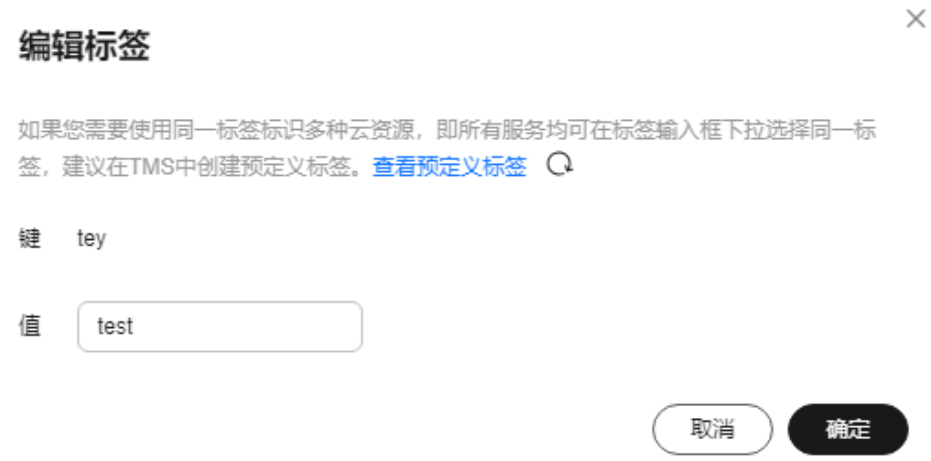
步骤1 登录DEW管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 在左侧选择对应服务进入页面，单击需要修改标签的实例，进入详情页面。

步骤4 选择对应的标签页签后，单击“编辑”，弹出“编辑标签”对话框。修改标签值后单击“确定”，完成标签值修改。

图 6-5 编辑标签



----结束

6.1.6 删除标签

本章节指导用户对已创建标签进行删除。

操作步骤

步骤1 登录DEW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 在左侧选择对应服务进入页面，单击需要删除标签的实例，进入详情页面。

步骤4 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。

图 6-6 删除标签

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

6.2 调整配额

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少个用户主密钥。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

查看配额

步骤1 登录DEW管理控制台。

步骤2 在页面右上角，选择“资源 > 我的配额”。

系统进入“服务配额”页面。

图 6-7 我的配额

步骤3 您可以在“服务配额”页面，查看各项资源的总配额、及使用情况。

步骤4 如果当前配额不能满足业务要求，请单击“申请扩大配额”。

----结束

申请扩大配额

步骤1 登录DEW管理控制台。

步骤2 在页面右上角，选择“资源 > 我的配额”。

系统进入“服务配额”页面。

图 6-8 我的配额

步骤3 单击“申请扩大配额”。

步骤4 在“新建工单”页面，根据您的需求，填写相关参数。

其中，“问题描述”请填写需要调整的内容和申请原因。

步骤5 填写完毕后，勾选协议并单击“提交”。

----结束

7 监控与审计

7.1 使用 CES 监控 DEW

7.1.1 DEW 服务支持的指标说明

功能说明

本节定义了数据加密服务上报云监控的基础监控指标的命名空间，监控指标列表，各项监控指标的具体含义与使用说明，用户可以通过云监控检索数据加密服务产生的监控指标和告警信息。

命名空间

密钥管理：SYS.KMS

凭据管理：SYS.CSMS

说明

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务，也能够互不干扰。

数据加密服务监控指标

表 7-1 密钥管理支持的监控指标

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
delkey_remaing_time	密钥剩余时间	该指标表示计划删除状态的密钥距离被删除还剩下的时间	≥ 0 小时	小时	不涉及	密钥	5分钟
matrial_remaing_time	密钥材料的剩余有效时间	该指标表示外部导入的密钥材料的剩余有效时间	≥ 0 小时	小时	不涉及	密钥	5分钟

表 7-2 凭据管理支持的监控指标

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
del_secret_remaining_time	计划删除凭据剩余时间	该指标表示计划删除凭据的剩余时间	≥ 0 小时	小时	不涉及	凭据	5分钟

维度

Key	Value
key_id	密钥ID
secret_id	凭据ID

7.1.2 DEW 服务支持的事件说明

功能说明

事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。

命名空间

密钥管理：SYS.KMS

凭据管理：SYS.CSMS

数据加密服务支持的事件列表

表 7-3 密钥管理服务支持监控的事件

事件名称	事件ID	事件级别	事件说明	处理建议	事件影响
禁用密钥	disableKey	重要	客户触发了禁用密钥的操作，密钥处于无法使用状态。	若客户因业务需要禁用密钥，无需处置。若客户误操作禁用了密钥，请登录DEW控制台重新启用密钥。	若密钥正在被客户业务使用，可能造成业务受损。
计划删除密钥	scheduleKeyDeletion	次要	客户触发了计划删除的操作，密钥处于无法使用状态。	若客户因业务需要删除密钥，无需处置。若客户误操作计划删除了密钥，请登录DEW控制台重新取消计划删除，并重新启用密钥。	若密钥正在被客户业务使用，可能造成业务受损。
退役授权	retireGrant	重要	客户触发了退役授权的操作，密钥处于无法使用的状态。	若客户因业务需要取消对密钥授权，无需处置。若客户误操作取消对密钥授权，请登录DEW控制台重新进行授权。	若密钥正在被客户业务使用，可能造成业务受损。
撤销授权	revokeGrant	重要	客户触发了撤销授权的操作，密钥处于无法使用的状态。	若客户因业务需要取消对密钥授权，无需处置。若客户误操作取消对密钥授权，请登录DEW控制台重新进行授权。	若密钥正在被客户业务使用，可能造成业务受损。

表 7-4 凭据管理服务支持监控的事件

事件名称	事件ID	事件级别	事件说明	处理建议	事件影响
操作待删除凭据	operateDeletedSecret	重要	用户调用接口操作计划删除状态凭据。	用户可以考虑取消删除该凭据。	到期删除的凭据无法恢复。

7.1.3 创建指标和事件监控告警规则

通过设置DEW告警规则，用户可自定义监控目标与通知策略，设置告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助您及时了解DEW使用状况，从而起到预警作用。

前提条件

已创建密钥或凭据实例。

操作步骤

步骤1 登录CES服务控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 在左侧导航树栏，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤4 在页面右上方，单击“创建告警规则”，进入“创建告警规则”界面。

步骤5 填写告警规则信息，如图 设置DEW监控告警规则所示，填写规则如表 设置DEW告警规则参数说明所示。

图 7-1 设置 DEW 监控告警规则

表 7-5 设置 DEW 告警规则参数说明

参数名称	参数说明	取值样例
名称	系统会随机产生一个名称，您也可以进行修改。	alarm-blc7
描述	告警规则描述。	-
告警类型	告警规则的类型，可选择指标或者事件。	指标
云产品	当告警类型选择指标时，需配置告警规则监控的服务名称。 在下拉列表框中选择“密钥管理服务”或“凭据管理服务”。	密钥管理服务

参数名称	参数说明	取值样例
资源层级	监控对象的资源层级。当告警类型选择指标时，需选择告警规则的资源层级，可选择云产品或子维度。推荐选择云产品。 **说明** 当资源层级选择云产品时，单条告警规则支持跨子维度指标（如磁盘使用率、CPU使用率），当资源层级选择子维度时，单条告警规则不支持跨子维度指标。	KMS密钥
监控范围	告警规则适用的资源范围。 ● 选择“全部资源”时，则当前云产品下任何资源满足告警策略时，都会触发告警。可单击“选择排除资源”排除不需要监控的资源。 ● 选择“资源分组”时，该分组下任何资源满足告警策略时，都会触发告警。可单击“选择排除资源”排除不需要监控的资源。 ● 选择“指定资源”时，在“监控对象”单击“选择指定资源”进行指定资源的选择。 **说明** ● 当告警类型选择指标时，监控范围可选择全部资源、资源分组或指定资源。 ● 当告警类型选择事件且事件类型为系统事件时，支持配置监控范围。	指定资源
分组	当监控范围选择资源分组时，需要选择分组。若当前已有的资源分组不满足使用条件时，可以单击“创建资源分组”进行创建。 在分组下拉框中选择资源分组名称后，可单击“查看组内资源详情”查看选择分组内的资源信息。告警规则配置完成后，不支持修改分组。	-

参数名称	参数说明	取值样例
监控对象	当监控范围选择指定资源时，需要选择告警规则的监控对象。 单击“选择指定资源”，在页面右侧的资源列表中选择需要监控的资源。	-
事件类型	当告警类型选择事件时，需要选择事件类型，可选择系统事件或自定义事件。	系统事件
事件来源	当告警类型选择事件时，需要设置事件来源。 ● 当事件类型选择系统事件时，在下拉列表中选择事件来源的云服务名称。 ● 当事件类型选择自定义事件时，事件来源需要与上报的字段一致，格式需要为service.item形式。	凭据管理服务
触发规则	根据需要可选择关联模板、导入已有模板或自定义创建。 **说明** 选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。	关联模板
模板	选择关联或导入的模板。	-
告警策略	当触发规则选择“自定义创建”时，需要设置触发告警规则的告警策略。 ● 当“告警类型”选择“指标”时，是否触发告警取决于连续周期的数据是否达到阈值。例如CPU使用率监控周期为5分钟，连续三个周期平均值≥80%，则触发告警。 ● 当告警类型为事件时，触发告警具体的事件为一个瞬间的事件。例如重启虚拟机，则触发告警。	-
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。	开启

参数名称	参数说明	取值样例
通知方式	发送告警通知的方式，可选择通知组或主题订阅。 ● 通知组：需要发送告警通知的通知组。 ● 主题：消息发布或客户端订阅通知的特定事件类型，如果此处没有需要的主题，需先创建主题并订阅该主题。	通知组
通知策略	当通知方式选择通知策略时，需要选择告警通知的策略。通知策略是包含通知组选择、生效时间、通知内容模板等参数的组合编排。	-
通知组	当通知方式选择通知组时，需要选择发送告警通知的通知组。	-
通知对象	当通知方式选择主题订阅时，需要选择发送告警通知的对象，可选择云账号联系人或主题。 ● 云账号联系人为注册时的手机和邮箱。 ● 主题是消息发布或客户端订阅通知的特定事件类型，若此处没有需要的主题则需先创建主题并添加订阅。	-
通知内容模板	当通知方式选择通知组或主题订阅时，需要选择发送告警通知时的内容模板，支持选择已有模板或创建通知内容模板。	-
生效时间	当通知方式选择通知组或主题订阅时，需要设置生效时间。 该告警仅在生效时间段发送通知消息，非生效时段则在隔日生效时段发送通知消息。	00:00-8:00
时区	告警生效时间的时区，默认为客户端浏览器所在时区，支持配置。	-
触发条件	可以选择“出现告警”、“恢复正常”两种状态，作为触发告警通知的条件。	出现告警

说明

“告警通知”功能触发产生的告警消息由消息通知服务SMN发送，可能产生少量费用，具体费用请参考**产品价格说明**。

步骤6 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

7.1.4 查看指标和事件监控数据

您可以通过管理控制台，查看DEW的相关指标，及时了解DEW使用状况，并通过指标设置防护策略。

前提条件

DEW已对接云监控，即已在云监控页面设置监控告警规则。有关设置监控告警规则的详细操作，请参见**设置监控告警规则**。

查看指标监控数据

步骤1 **登录CES服务控制台**。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 在左侧导航栏，选择“云服务监控”，进入“云服务监控”页面。

步骤4 在搜索框中，搜索“KMS”或“CSMS”，单击KMS或CSMS的看板名称，进入“云服务监控详情”页面。

步骤5 在目标密钥实例或凭据实例所在行的“操作”列中，单击“查看监控指标”，查看对象的指标详情。

----结束

查看事件监控数据

步骤1 **登录CES服务控制台**。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击业务左侧导航栏的“事件监控”，进入“事件监控”页面。

步骤4 在“事件监控”页面，默认展示近24小时的所有系统事件和自定义事件。

您也可以根据需要选择“近1小时”“近3小时”“近12小时”“近24小时”“近7天”“近30天”或自定义时间段，分别查看不同时段的事件。

表 7-6 事件监控列表

参数	说明
事件类型	上报的事件类型，支持系统事件和自定义事件。

参数	说明
事件名称	用户操作资源的动作，如用户登录，用户登出，是一个瞬间的操作动作。 DEW支持的系统事件请参见**DEW服务支持的事件说明**。
事件来源	事件来源的云服务名称。
事件数量	该事件在当前所选择的时间段内上报的次数。
最近发生时间	该事件最近一次发生的时间。
操作	目前支持查看监控图表和创建告警规则两种操作。

步骤5 单击待查看事件类型所在行“操作列”的“查看监控图表”，可以查看该事件类型的详情。

步骤6 单击具体事件右侧的操作列的“查看事件”，可查看具体事件的内容。

----结束

7.2 使用 CTS 审计 DEW

7.2.1 支持云审计的操作列表

云审计服务记录相关的操作事件，如**表 云审计服务支持的KMS操作列表**、**表 云审计服务支持的CSMS操作列表**、**表 云审计服务支持的KPS操作列表**、**表 云审计服务支持的DHSM操作列表**所示。

表 7-7 云审计服务支持的 KMS 操作列表

操作名称	资源类型	事件名称
创建密钥	cmk	createKey
创建数据密钥	cmk	createDataKey
创建不含明文数据密钥	cmk	createDataKeyWithoutPlaintext
启用密钥	cmk	enableKey
禁用密钥	cmk	disableKey
加密数据密钥	cmk	encryptDatakey
解密数据密钥	cmk	decryptDatakey
计划删除密钥	cmk	scheduleKeyDeletion
取消计划删除密钥	cmk	cancelKeyDeletion
创建随机数	rng	genRandom

操作名称	资源类型	事件名称
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	dealUnifiedTags
删除标签	cmk	dealUnifiedTags
批量添加标签	cmk	dealUnifiedTags
批量删除标签	cmk	dealUnifiedTags
开启密钥轮换	cmk	enableKeyRotation
修改密钥轮换周期	cmk	updateKeyRotationInterval

表 7-8 云审计服务支持的 CSMS 操作列表

操作名称	资源类型	事件名称
创建凭据	secret	createSecret
更新凭据	secret	updateSecret
删除凭据	secret	forceDeleteSecret
计划删除凭据	secret	scheduleDelSecret
取消计划删除凭据	secret	restoreSecretFromDeletedStatus
创建凭据状态	secret	createSecretStage
更新凭据状态	secret	updateSecretStage
删除凭据状态	secret	deleteSecretStage
创建凭据版本	secret	createSecretVersion

操作名称	资源类型	事件名称
下载凭据备份	secret	backupSecret
恢复凭证备份	secret	restoreSecretFromBackupBlob
更新凭据版本	secret	putSecretVersion
凭据轮转	secret	rotateSecret
创建凭据事件	secret	createSecretEvent
更新凭据事件	secret	updateSecretEvent
删除凭据事件	secret	deleteSecretEvent
创建资源标签	secret	createResourceTag
删除资源标签	secret	deleteResourceTag

表 7-9 云审计服务支持的 KPS 操作列表

操作名称	资源类型	事件名称
创建或导入SSH密钥对	keypair	createOrImportKeypair
删除SSH密钥对	keypair	deleteKeypair
导入私钥	keypair	importPrivateKey
导出私钥	keypair	exportPrivateKey
绑定SSH密钥对	keypair	bindKeypair
解绑SSH密钥对	keypair	unbindKeypair
清除私钥	keypair	clearPrivateKey

表 7-10 云审计服务支持的 DHSM 操作列表

操作名称	资源类型	事件名称
购买云加密实例	hsm	purchaseHsm
实例化云加密实例	hsm	createHsm
删除云加密实例	hsm	deleteHsm

7.2.2 在 CTS 事件列表查看云审计事件

场景描述

云审计服务能够为您提供云服务资源的操作记录，记录的信息包括发起操作的用户身份、IP地址、具体的操作内容的信息，以及操作返回的响应信息。根据这些操作记录，您可以很方便地实现安全审计、问题跟踪、资源定位，帮助您更好地规划和利用已有资源、甄别违规或高危操作。

什么是事件

事件即云审计服务追踪并保存的云服务资源的操作日志，操作包括用户对云服务资源新增、修改、删除等操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。

什么是管理类追踪器和数据类追踪器

管理追踪器会自动识别并关联当前租用户所使用的所有云服务，并将当前用户的所有操作记录在该追踪器中。管理追踪器记录的是管理类事件，即用户对云服务资源新建、修改、删除等操作事件。

数据追踪器会记录租户对OBS桶中的数据操作的详细信息。数据类追踪器记录的是数据类事件，即OBS服务上报的用户对OBS桶中数据的操作事件，例如上传数据、下载数据等。

约束与限制

- 管理类追踪器未开启组织功能之前，单账号跟踪的事件可以通过云审计控制台查询。管理类追踪器开启组织功能之后，多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。组织追踪器的详细介绍请参见**组织追踪器概述**。
- 用户通过云审计控制台只能查询最近7天的操作记录，过期自动删除，不支持人工删除。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务（OBS）或云日志服务（LTS），才可在OBS桶或LTS日志组里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。
- 用户对云服务资源做出创建、修改、删除等操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。

前提条件

1. **注册华为云并实名认证。**

   如果您已有一个华为账户，请跳到下一个任务。如果您还没有华为账户，请参考以下步骤创建。

   a. 打开**华为云官网**，单击“注册”。

   b. 根据提示信息完成注册，详细操作请参见**如何注册华为云管理控制台的用户？**。

      注册成功后，系统会自动跳转至您的个人信息界面。

   c. 参考**实名认证**完成个人或企业账号实名认证。

2. **为用户添加操作权限**。

   如果您是以主账号登录华为云，请跳到下一个任务。

   如果您是以IAM用户登录华为云，需要联系CTS管理员（主账号或admin用户组中的用户）对IAM用户授予CTS FullAccess权限。授权方法请参见**给IAM用户授权**。

查看审计事件

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。

在新版事件列表查看审计事件

步骤1 登录**CTS控制台**。

步骤2 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

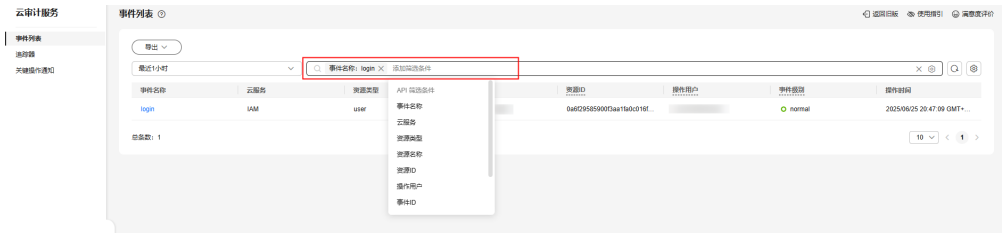
步骤3 在页面右上方，可以通过筛选时间范围，查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

步骤4 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件。

表 7-11 事件筛选参数说明

参数名称	说明
事件名称	操作事件的名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务支持审计的操作事件的名称请参见**支持审计的服务及详细操作列表**。 示例：updateAlarm
云服务	云服务的名称缩写。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 示例：IAM
资源名称	操作事件涉及的云资源名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。 示例：ecs-name
资源ID	操作事件涉及的云资源ID。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 当该资源类型无资源ID或资源创建失败时，该字段为空。 示例：*{虚拟机ID}*

参数名称	说明
事件ID	操作事件日志上报到CTS后，查看事件中的trace_id参数值。 输入的值需全字符匹配，不支持模糊匹配模式。 示例：01d18a1b-56ee-11f0-ac81-******1e229
资源类型	操作事件涉及的资源类型。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务的资源类型请参见**支持审计的服务及详细操作列表**。 示例：user
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的trace_type的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。 IAM身份与操作用户对应关系，以及操作用户名称的格式说明，请参见**IAM身份与操作用户对应关系**。
事件级别	下拉选项包含“normal”、“warning”、“incident”，只可选择其中一项。 ● normal代表操作成功。 ● warning代表操作失败。 ● incident代表比操作失败更严重的情况，如引起其他故障等。
企业项目ID	资源所在的企业项目ID。 查看企业项目ID的方式：在EPS服务控制台的“项目管理”页面，可以查看企业项目ID。 示例：b305ea24-c930-4922-b4b9-******1eb2
访问密钥ID	访问密钥ID，包含临时访问凭证和永久访问密钥。 查看访问密钥ID的方式：在控制台右上方，用户名下拉选项中，选择“我的凭证 > 访问密钥”，可以查看访问密钥ID。 示例：HSTAB47V9V*******TLN9



步骤5 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。

- 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
- 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx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。
- 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。

步骤6 （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

----结束

在旧版事件列表查看审计事件

步骤1 登录CTS控制台。

步骤2 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

步骤3 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。

步骤4 在页面右上方，可以通过筛选时间范围，查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

步骤5 事件列表支持通过筛选来查询对应的操作事件。

表 7-12 事件筛选参数说明

参数名称	说明
事件类型	事件类型分为“管理事件”和“数据事件”。 • 管理类事件，即用户对云服务资源新建、修改、删除等操作事件。 • 数据类事件，即OBS服务上报的OBS桶中的数据的操作事件，例如上传数据、下载数据等。
云服务	在下拉选项中，选择触发操作事件的云服务名称。
资源类型	在下来选项中，选择操作事件涉及的资源类型。 各个云服务的资源类型请参见支持审计的服务及详细操作列表。
筛选类型	筛选类型分为“资源ID”、“事件名称”和“资源名称”。 • 资源ID：操作事件涉及的云资源ID。 当该资源类型无资源ID，或资源创建失败时，该字段为空。 • 事件名称：操作事件的名称。 各个云服务支持审计的操作事件的名称请参见支持审计的服务及详细操作列表。 • 资源名称：操作事件涉及的云资源名称。 当事件所涉及的云资源无资源名称，或对应的API接口操作不涉及资源名称参数时，该字段为空。

参数名称	说明
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的trace_type的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。 IAM身份与操作用户对应关系，以及操作用户名称的格式说明，请参见**IAM身份与操作用户对应关系**。
事件级别	可选项包含“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。 • Normal代表操作成功。 • Warning代表操作失败。 • Incident代表比操作失败更严重的情况，如引起其他故障等。

步骤6 选择完查询条件后，单击“查询”。

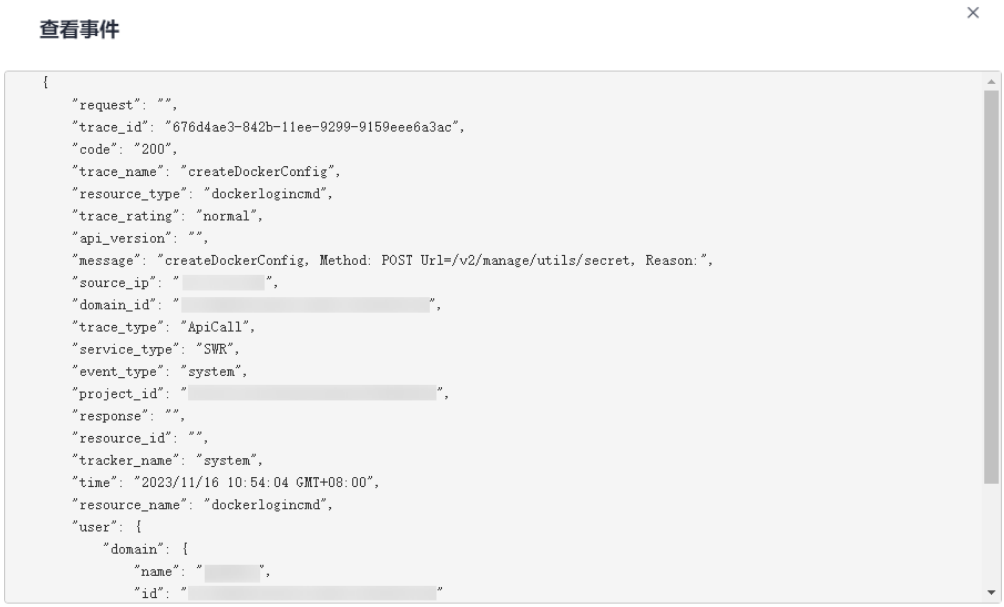
步骤7 在事件列表页面，您还可以导出操作记录文件和刷新列表。

- 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。

步骤8 在事件的“是否篡改”列中，您可以查看该事件是否被篡改：

步骤9 在需要查看的事件左侧，单击 展开该记录的详细信息。

步骤10 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。



步骤11 （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

----结束

相关文档

- 关于事件结构的关键字段详解，请参见**事件结构**和**事件样例**。
- 您可以通过以下示例，来学习如何查询具体的事件：
  - 使用云审计服务，审计最近两周内云硬盘服务的创建和删除操作。具体操作，请参见**安全审计**。
  - 使用云审计服务，定位现网某个弹性云服务器在某日上午发生的故障，以及定位现网创建弹性云服务器操作失败的问题。具体操作，请参见**问题定位**。
  - 使用云审计服务，查看某个弹性云服务器的所有的操作记录。具体操作，请参见**资源跟踪**。

7.3 使用 Config 审计 DEW

通过配置审计（Config）服务的资源合规特性，可以帮助您快速创建一组DEW合规规则，用于评估您的资源是否满足合规要求。合规规则创建后，有多种机制触发规则评估，然后查看合规规则的评估结果来了解资源的合规情况。更多信息请参见**资源合规概述**。

Config 支持的 DEW 预设策略

表 7-13 配置 Config 审计支持的 DEW 预设策略

预设策略	触发方式	评估资源
KMS密钥不处于“计划删除”状态	配置变更	kms.keys

预设策略	触发方式	评估资源
KMS密钥启用密钥轮换	配置变更	kms.keys
检查CSMS凭据轮转成功	配置变更	csms.secrets
CSMS凭据启动自动轮转	配置变更	csms.secrets
CSMS凭据使用指定KMS	配置变更	csms.secrets
CSMS凭据在指定时间内轮转	周期触发	csms.secrets

使用 Config 配置 DEW 审计

步骤1 登录DEW管理控制台。

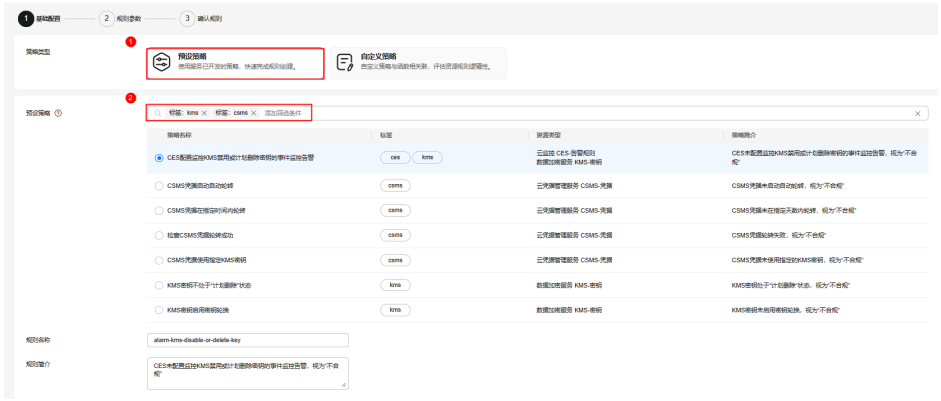
步骤2 单击页面左上角 ☰，在弹出的服务列表中，选择“管理与监管 > 配置审计 Config”，进入“资源清单”页面。

步骤3 在左侧导航树中，选择“资源合规”，进入“资源合规”页面。

步骤4 在“规则”页签下单击“添加规则”，进入“基础配置”页面，完成基础配置信息。

1. “策略类型”：选择“预设策略”。
2. “预设策略”：搜索框中搜索“标签：kms”或“标签：csms”，选择需要配置审计的策略名称。

图 7-2 添加审计规则



步骤5 单击“下一步”，配置“触发类型”和“周期频率”。

步骤6 单击“下一步”，确认信息无误后单击“提交”。

步骤7 规则添加成功后，在规则列表中可查看已添加的合规规则，单击规则名称，进入规则详情页可查看规则的合规评估结果。

----结束

8 权限管理

8.1 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**权限及授权项说明**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择策略内容，可自动生成策略。

  创建KMS自定义策略时：

  - “云服务”：数据加密服务（KMS）。
  - “操作”：根据您的需求进行选择。
  - “选择资源（可选）”：“资源”选择“特定资源”，“KeyId”选择“通过资源路径指定”时，“路径”为创建密钥时生成的ID，可参考“查看密钥”章节获取ID。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的DEW自定义策略样例。

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：拒绝用户删除密钥标签

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

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

  ```
  {
     "Version": "1.1",
     "Statement": [
        {
           "Effect": "Deny",
           "Action": [
              "kms:cmkTag:delete"
           ]
        }
     ]
  }
  ```

- 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"
           ]
        }
     ]
  }
  ```


8.2 敏感操作保护

凭据管理支持敏感操作保护。在控制台进行敏感操作时，需要输入一种能证明身份的凭证，身份验证通过后方可进行相关操作。为了账号安全，建议开启操作保护功能，该功能对账号以及账号下的用户都生效。

约束条件

敏感操作保护仅影响通过管理控制台进行操作的用户。

开启操作保护

步骤1 登录DEW管理控制台。

步骤2 在“控制台”页面右上方的用户名处，在下拉列表中选择“安全设置”。

图 8-1 安全设置

步骤3 进入“安全设置”页面，单击“敏感操作”进入页面。在“操作保护”行，单击“立即启用”。

步骤4 进入“操作保护设置”页面，选择“开启”，单击“确定”后，开启操作保护。

开启后，您以及账号中的IAM用户进行敏感操作时，例如查看凭据值、删除密钥等，需要输入验证码进行验证，避免误操作带来业务风险与损失。

说明

- 用户如果进行敏感操作，将进入“操作保护”页面，选择认证方式，包括邮箱、手机和虚拟MFA三种认证方式。
  - 如果用户只绑定了手机，则认证方式只能选择手机。
  - 如果用户只绑定了邮箱，则认证方式只能选择邮件。
  - 如果用户未绑定邮箱、手机和虚拟MFA，进行敏感操作时，华为云将提示用户绑定邮箱、手机或虚拟MFA。
- 如需修改验证手机、邮箱、虚拟MFA设备，请在账号中修改。

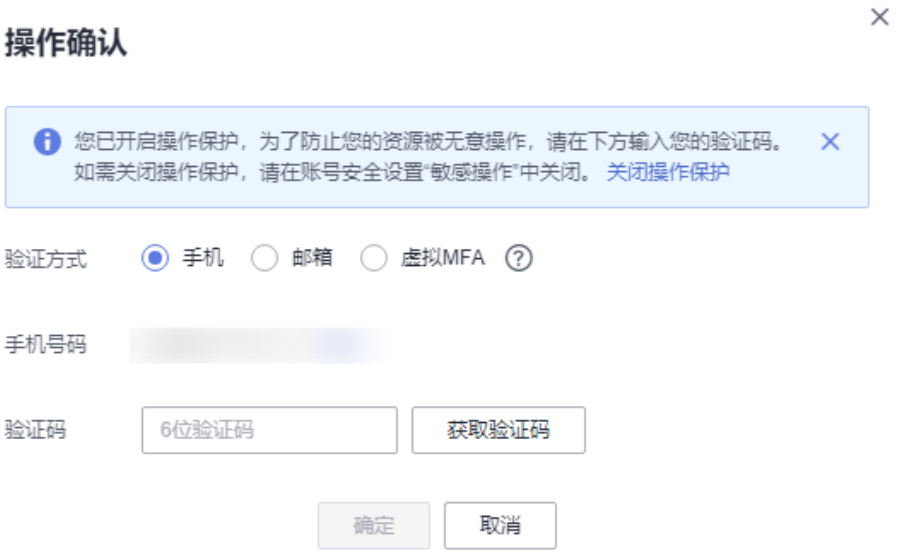
----结束

操作保护验证

当您已经开启操作保护，在进行敏感操作时，例如查看凭据值时，系统会先进行操作保护验证，根据您绑定的信息选择验证方式，如图 操作保护验证所示：

- 如果您绑定了邮箱，需输入邮箱验证码。
- 如果您绑定了手机，需输入手机验证码。
- 如果您绑定了虚拟MFA，需输入MFA设备上的6位动态验证码。

图 8-2 操作保护验证



关闭操作保护

步骤1 登录DEW管理控制台。

步骤2 在“控制台”页面右上方的用户名处，在下拉列表中选择“安全设置”。

图 8-3 安全设置

步骤3 进入“安全设置”页面，单击“敏感操作”进入页面。在“操作保护”行，单击“立即修改”。

步骤4 在“操作保护设置”页面中，选择“关闭”，单击“确定”后，通过验证后即可关闭操作保护。

----结束

相关链接

- 如何绑定虚拟MFA设备?
- 如何获取MFA验证码?

8.3 共享

8.3.1 共享概述

基于资源访问管理（Resource Access Manager，简称RAM）服务，资源所有者可以依据最小权限原则和不同的使用诉求，选择不同的共享权限，资源使用者只能对资源进行权限内的访问，保证共享资源在满足资源使用者业务诉求的同时，提升资源管理的安全性。关于RAM服务的更多信息请参见**什么是资源访问管理**。

当您的账号由华为云组织管理时，您还可以利用此优势更轻松地共享资源。如果您的账号在组织中，则您可以与单个账号共享，也可以与组织或OU中的所有账号共享，而不必枚举每个账号，具体请参见**启用与组织共享资源**。

约束条件

- 您的账号中必须拥有该KMS密钥资源，即您必须为该资源的所有者。您无法再次共享已与您共享的KMS密钥资源。
- 当您需要与您的组织或组织单元共享KMS密钥资源时，则您必须启用与组织共享资源功能。更多信息请参考**启用与组织共享资源**。

密钥所有者和接受者权限说明

密钥所有者可以对密钥执行任何操作，接受者仅可以执行部分操作，接受者支持的操作说明如**表 密钥接受者支持的操作列表**所示。

表 8-1 密钥接受者支持的操作列表

角色	支持的操作	操作说明
接受者	kms:cmk:get	通过控制台或API进行访问
	kms:cmk:createDataKey	仅能通过API访问
	kms:cmk:createDataKeyWithoutPlaintext	仅能通过API访问
	kms:cmk:encryptDataKey	仅能通过API访问
	kms:cmk:decryptDataKey	仅能通过API访问
	kms:cmk:encryptData	通过控制台或API进行访问
	kms:cmk:decryptData	通过控制台或API进行访问
	kms:cmk:sign	仅能通过API访问
	kms:cmk:verify	仅能通过API访问
	kms:cmk:generateMac	仅能通过API访问
	kms:cmk:verifyMac	仅能通过API访问
	kms:cmk:getPublicKey	通过控制台或API进行访问

角色	支持的操作	操作说明
	kms:cmk:getRotation	通过控制台或API进行访问
	kms:cmk:getTags	通过控制台或API进行访问

支持共享的资源类型和区域

当前DEW服务支持共享的资源类型和区域如**表 DEW服务支持共享的资源类型和区域**所示。

表 8-2 DEW 服务支持共享的资源类型和区域

云服务	资源类型	支持共享的区域
KMS	cmk：用户主密钥	所有Region都已支持共享。

支持使用共享密钥加密的服务和系统策略

在您购买包周期资源时，如果您选择共享密钥对创建的资源进行加密，需要给用户授予相应的策略才能使用共享密钥。支持使用共享密钥加密的服务和对应服务的系统策略见**表8-3**。

给IAM用户授权的详细操作请参见**给IAM用户授权**，系统策略选择**表8-3**中对应服务的系统策略即可。

表 8-3 支持使用共享密钥加密的服务和系统策略

服务	系统策略
云数据库 RDS	ServicePolicyForRDSFulfillment
云数据库 TaurusDB	ServicePolicyForGaussDBFulfillment
文档数据库服务 DDS	ServicePolicyForDDSFulfillment
高性能弹性文件服务 SFS Turbo	ServicePolicyForSFSTurboFulfillment
云桌面 Workspace	ServicePolicyForWorkspaceFulfillment
云数据库 GeminiDB	ServicePolicyForNosqlFulfillment

计费说明

关于KMS的计费可参见**计费项**。

共享密钥的计费，由密钥拥有者需支付密钥实例费用以及API调用费用。即所有共享资源发生费用均由资源拥有者账号产生。

8.3.2 共享 KMS

要共享您拥有的KMS资源给其他账号使用时，请创建共享。创建共享的流程分为指定共享资源、权限配置、指定使用者以及配置确认。

共享KMS可以用于DEW服务的凭据实例加密、密钥对加密等，也可以用于创建RDS、DDS、OBS实例加密。

前提条件

已给IAM用户授予对应服务的Billing系统策略，详见**支持使用共享密钥加密的服务和系统策略**。

创建共享 KMS 资源

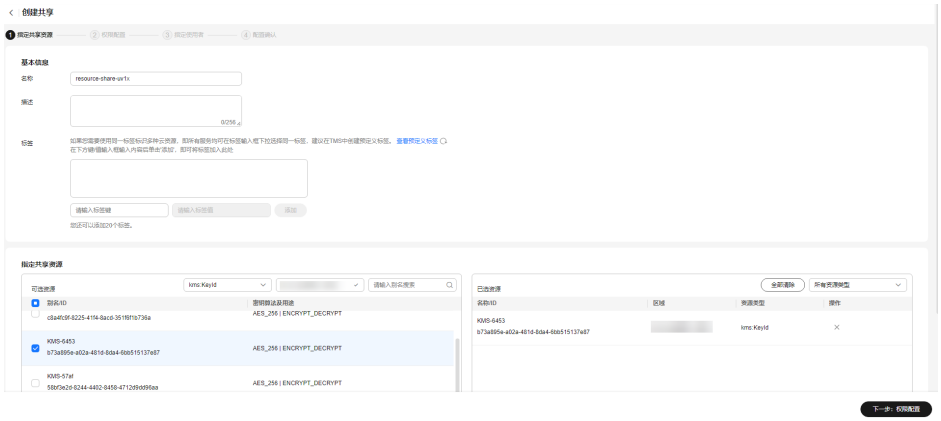
步骤1 **登录DEW管理控制台**。

步骤2 单击页面左上角的 ☰，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

步骤3 单击页面左侧“我的共享 > 共享管理”，进入“共享管理”页面。

步骤4 单击页面右上角的“创建共享”，进入“创建共享”页面。

图 8-4 指定共享资源



步骤5 选择资源类型为“kms:KeyId”，选择对应区域，勾选需进行共享的密钥。单击“下一步：权限配置”。

步骤6 进入“权限配置”页面，选择指定资源类型支持的共享权限，配置完成后，单击页面右下角的“下一步：指定使用者”。

步骤7 进入“指定使用者”页面，指定共享资源的使用者，配置完成后，单击页面右下角的“下一步：配置确认”。

表 8-4 参数说明

参数名称	参数说明
使用者类型	• 组织 关于组织创建相关操作可参见。 **说明** 如果您未打开“启用与组织共享资源”开关，使用者类型将无法选择“组织”。具体操作可参见。 • 华为云账号ID

步骤8 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确认”，完成资源共享实例的创建。

说明

创建共享实例后，组织会自动接收共享实例，华为云账号ID需要单独进行接受共享操作，具体请参见。

----结束

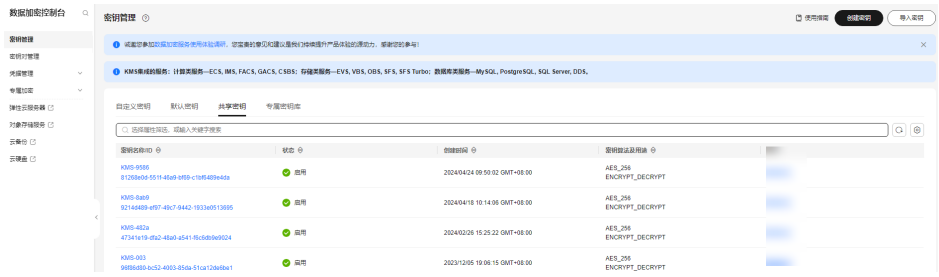
查看共享 KMS 资源

步骤1 登录DEW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 在密钥管理页面，单击“共享密钥”页签，查看当前共享中的密钥资源。

图 8-5 共享密钥



说明

通过共享密钥页签，可以复制密钥ID，用于手动输入ID的KMS加密密钥选择场景。

----结束

使用共享 KMS 资源

在通过共享密钥创建相关资源的时候，您仍然需要保证您当前的用户拥有操作密钥的相关权限。具体权限请参考密钥所有者和接受者权限说明。

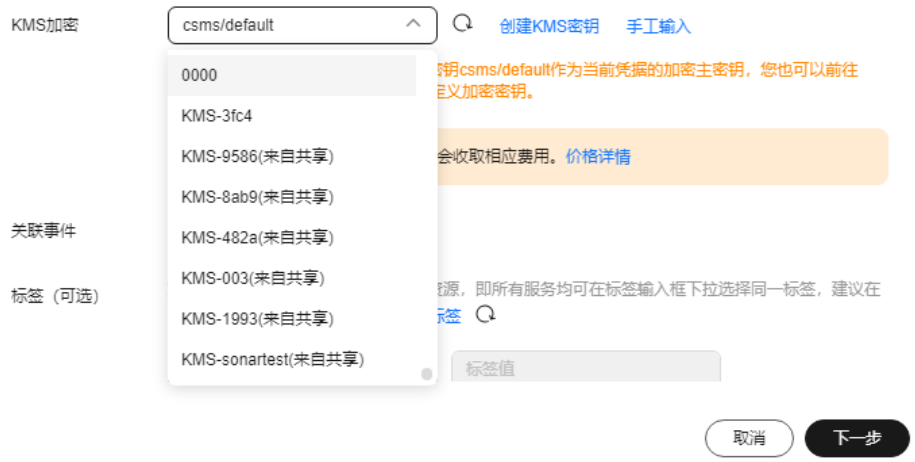
步骤1 登录DEW管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤4 在“创建凭据”页面的“KMS加密”选项中，通过选择或者手动输入方式选择来自共享的KMS密钥。

图 8-6 选择共享密钥



说明

- 创建密钥对支持选择来自共享的KMS密钥。
- 创建RDS、DDS、OBS等实例时，支持选择来自共享的KMS密钥，具体操作可参见**使用KMS加密的云服务**。

----结束

更新共享

您可以随时更新资源共享实例，支持更新共享实例的名称、描述、标签、共享的资源、共享权限以及共享使用者。

步骤1 **登录DEW管理控制台**。

步骤2 单击页面左上角的，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

步骤3 单击页面左侧“我的共享 > 共享管理”，进入“共享管理”页面。

步骤4 在共享管理列表中选择需要更新的共享，单击“操作”列的“编辑”。

步骤5 进入“指定共享资源”页面，您可根据需要更新共享的名称、描述、标签以及增加或删除共享的资源。

步骤6 更新完成后，单击页面右下角的“下一步：权限配置”。

步骤7 进入“权限配置”页面，您可根据需要增加或删除共享权限，更新完成后，单击页面右下角的“下一步：指定使用者”。

步骤8 进入“指定使用者”页面，您可根据需要增加或删除共享密钥的使用者，配置完成后，单击页面右下角的“下一步：配置确认”。

步骤9 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确认”，完成共享的更新。

----结束

退出共享

如果用户不再需要访问共享的密钥资源，可以随时退出共享。退出共享后，用户将失去对共享密钥对访问权限。

步骤1 登录DEW管理控制台。

步骤2 单击页面左上角的 ☰，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

步骤3 单击页面左侧“共享给我 > 共享管理”，进入“共享管理”页面。

步骤4 单击“已接收共享”页签，在列表选择需要退出的共享实例，单击“退出”。

步骤5 在弹出的对话框中，单击“退出”，即可完成退出共享实例。

----结束

8.3.3 使用共享 VPC 激活专属加密实例

在创建加密实例成功后，需要通过激活操作才可以使用该专属加密实例，激活专属加密实例时需要绑定VPC，可以通过申请VPC或者使用来自共享的VPC进行绑定。

创建共享 VPC 资源

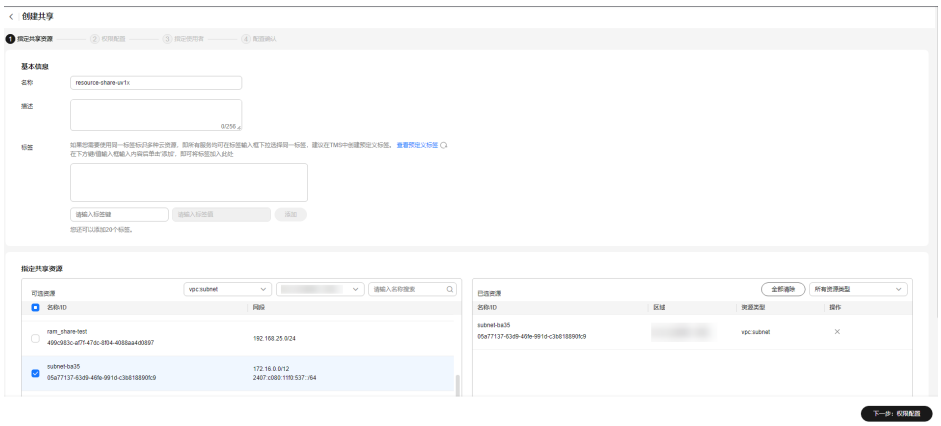
步骤1 登录DEW管理控制台。

步骤2 单击页面左上角的 ☰，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

步骤3 单击页面左侧“我的共享 > 共享管理”，进入“共享管理”页面。

步骤4 单击页面右上角的“创建共享”，进入“创建共享”页面。

图 8-7 指定共享资源



步骤5 选择资源类型为“vpc：subnet”，选择对应区域，勾选需进行共享的VPC。单击“下一步：权限配置”。

步骤6 进入“权限配置”页面，选择指定资源类型支持的共享权限，配置完成后，单击页面右下角的“下一步：指定使用者”。

步骤7 进入“指定使用者”页面，指定共享资源的使用者，配置完成后，单击页面右下角的“下一步：配置确认”。

表 8-5 参数说明

参数名称	参数说明
使用者类型	• 组织 关于组织创建相关操作可参见。 **说明** 如果您未打开“启用与组织共享资源”开关，使用者类型将无法选择“组织”。具体操作可参见。 • 华为云账号ID

步骤8 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确认”，完成资源共享实例的创建。

----结束

使用共享 VPC 资源

步骤1 **登录DEW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 在左侧导航树中，选择“专属加密 > 实例列表”，进入“实例列表”页面。

步骤4 在目标专属加密实例的“操作”列，单击激活，进入“激活专属加密实例”页面。

步骤5 在“虚拟私有云”下拉框中，选择来自共享的VPC实例，配置参数完成并单击“立即激活”。

图 8-8 选择共享 VPC

----结束

