数据加密服务

用户指南

文档版本 34

发布日期 2024-04-30

华为技术有限公司

版权所有 © 华为技术有限公司 2024。 保留一切权利。

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

商标声明

HUAWEI和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 密钥管理.....1
1.1 密钥概述.....1
1.2 创建密钥.....2
1.3 导入密钥.....5
1.3.1 概述.....5
1.3.2 导入密钥材料.....6
1.3.3 删除密钥材料.....14
1.4 管理密钥.....15
1.4.1 查看密钥.....15
1.4.2 启用密钥.....17
1.4.3 禁用密钥.....17
1.4.4 删除密钥.....18
1.4.5 取消删除密钥.....20
1.4.6 分配至企业项目.....20
1.5 搜索密钥.....21
1.6 在线工具加解密小数据.....22
1.7 管理标签.....23
1.7.1 添加标签.....23
1.7.2 修改标签值.....25
1.7.3 删除标签.....26
1.8 轮换密钥.....27
1.8.1 密钥轮换概述.....27
1.8.2 开启密钥轮换.....29
1.8.3 关闭密钥轮换.....31
1.9 管理授权.....32
1.9.1 创建授权.....32
1.9.2 查询授权.....36
1.9.3 撤销授权.....37
2 凭据管理.....38
2.1 凭据概述.....38
2.2 轮转策略.....40
2.3 创建凭据.....40
2.3.1 创建通用凭据.....40

2.3.2 创建 RDS 凭据 42
2.4 管理凭据 47
2.4.1 查看凭据 47
2.4.2 通过事件搜索凭据 48
2.4.3 删除凭据 48
2.5 管理凭据版本 50
2.5.1 存入和查看凭据值 50
2.5.2 管理版本状态 51
2.6 管理标签 53
2.6.1 添加标签 53
2.6.2 通过标签搜索凭据 54
2.6.3 修改标签值 55
2.6.4 删除标签 56
2.7 创建事件 57
2.8 管理事件 58
2.8.1 查看事件 58
2.8.2 编辑事件 60
2.8.3 启用事件 60
2.8.4 禁用事件 61
2.8.5 删除事件 62
2.9 通知记录 63
3 密钥对管理 64
3.1 创建密钥对 64
3.2 导入密钥对 69
3.3 升级密钥对 72
3.4 删除密钥对 73
3.5 管理密钥对 73
3.5.1 绑定密钥对 73
3.5.2 批量绑定密钥对 76
3.5.3 查看密钥对 78
3.5.4 重置密钥对 80
3.5.5 替换密钥对 82
3.5.6 解绑密钥对 84
3.6 管理私钥 86
3.6.1 导入私钥 86
3.6.2 导出私钥 88
3.6.3 清除私钥 89
3.7 使用私钥登录 Linux ECS 89
3.8 使用私钥获取 Windows ECS 的登录密码 92
4 专属加密 94
4.1 操作指引 94
4.2 购买专属加密实例 96

4.2.1 创建专属加密实例 96
4.2.2 激活专属加密实例 99
4.3 查看专属加密实例 102
4.4 管理标签 105
4.4.1 添加标签 105
4.4.2 通过标签搜索专属加密实例 107
4.4.3 修改标签值 108
4.4.4 删除标签 108
4.5 使用专属加密实例 109
5 审计日志 112
5.1 支持云审计的操作列表 112
5.2 查询审计事件 114
6 共享 118
6.1 共享 VPC 118
6.2 更新共享 120
6.3 退出共享 121
7 权限管理 122
7.1 创建用户并授权使用 DEW 122
7.2 DEW 自定义策略 127
A 修订记录 129

1 密钥管理

1.1 密钥概述

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

自定义密钥分为“对称密钥”和“非对称密钥”。

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

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

表 1-1 KMS 支持的密钥算法类型

密钥类型	算法类型	密钥规格	说明	用途
对称密钥	AES	● AES_256	AES对称密钥	小量数据的加解密或用于加解密数据密钥。
摘要密钥	SHA	● HMAC_256 ● HMAC_384 ● HMAC_512	SHA摘要密钥	● 数据防篡改 ● 数据完整性校验
摘要密钥	SM3	● HMAC_SM3	国密SM3摘要密钥	● 数据防篡改 ● 数据完整性校验

版权所有 © 华为技术有限公司

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

1.2 创建密钥

该任务指导用户通过密钥管理界面创建自定义密钥。

自定义密钥包括“对称密钥”和“非对称密钥”。

前提条件

账号拥有KMS CMKFullAccess及以上权限。

约束条件

- 用户最多可创建100个自定义密钥，不包含默认密钥。
- 创建的对称密钥使用的是AES算法密钥，AES-256密钥可用于小量数据的加解密或用于加解密数据密钥，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”。
- 数据加密服务密钥通过接口每月可免费调用次数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。

创建密钥

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击界面右上角“创建密钥”。

步骤5 在弹出的“创建密钥”对话框中，填写密钥参数。

图 1-1 创建密钥

- 别名：待创建密钥的别名。

  说明

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

- 密钥算法：选择密钥算法。KMS支持的密钥算法说明如**表1-2**所示。

表 1-2 KMS 支持的密钥算法类型

密钥类型	算法类型	密钥规格	说明	用途
对称密钥	AES	– AES_256	AES对称密钥	小量数据的加解密或用于加解密数据密钥。
摘要密钥	SHA	– HMAC_256 – HMAC_384 – HMAC_512	SHA摘要密钥	– 数据防篡改 – 数据完整性校验
摘要密钥	SM3	– HMAC_SM3	国密SM3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	小量数据的加解密或数字签名。
	ECC	– EC_P256 – EC_P384	椭圆曲线密码，使用NIST推荐的椭圆曲线	数字签名

- 密钥用途：可选择“SIGN_VERIFY”、“ENCRYPT_DECRYPT”、“GENERATE_VERIFY_MAC”。
  - 对于AES_256对称密钥，默认值“ENCRYPT_DECRYPT”。
  - 对于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”。

  说明

  创建密钥时请选择“密钥用途”，密钥创建后不可修改。

- （可选）描述：可根据自己的需要为自定义密钥添加描述。

  说明

  支持长度为1 ~ 255个字符。

- 企业项目：该参数针对企业用户使用。

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

  未开通企业管理的用户页面则没有“企业项目”参数项，无需进行配置。

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

说明

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

步骤7 单击“确定”，在页面右上角弹出“创建密钥成功”，则说明密钥创建完成。

用户可在密钥列表上查看已完成创建的密钥，密钥默认状态为“启用”。

----结束

相关操作

- 对象存储服务中对象的服务端加密方法，具体请参见《对象存储服务控制台指南》的“使用服务端加密方式上传文件”章节。
- 云硬盘中数据加密方法，具体请参见《云硬盘用户指南》的“购买云硬盘”章节。
- 私有镜像的加密方法，具体请参见《镜像服务用户指南》的“加密镜像”章节。
- 云数据库中数据库实例的磁盘加密方法，具体请参见《云数据库RDS快速入门》的“购买实例”章节。
- 创建DEK、不含明文的DEK方法，具体请参见《数据加密服务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。

1.3 导入密钥

1.3.1 概述

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

- 当用户使用KMS管理控制台创建自定义密钥时，KMS系统会自动为该自定义密钥生成密钥材料。
- 当用户希望使用自己的密钥材料时，可通过KMS管理控制台的“导入密钥”功能创建密钥材料为空的自定义密钥，并将自己的密钥材料导入该自定义密钥中。

注意事项

- 安全性

  用户需要确保符合自己安全要求的随机源生成密钥材料。用户在使用导入密钥时，需要对自己密钥材料的安全性负责。请保存密钥材料的原始备份，以便在意外删除密钥材料时，能及时将备份的密钥材料重新导入KMS。

- 可用性与持久性

  在将密钥材料导入KMS之前，用户需要确保密钥材料的可用性和持久性。

  导入的密钥材料与通过KMS创建密钥时自动生成的密钥材料的区别，如**表1-3**所示。

  表 1-3 导入的密钥材料与通过 KMS 创建密钥时自动生成的密钥材料的区别

密钥材料来源	区别
导入的密钥	● 可以手动删除密钥材料，但不能删除该自定义密钥及其元数据。 ● 不支持密钥轮换功能。 ● 在导入密钥材料时，可以设置密钥材料失效时间，密钥材料失效后，KMS将在24小时以内自动删除密钥材料，但不会删除该自定义密钥及其元数据。 建议用户在本地密钥管理基础设施中安全地备份一份密钥材料，以便密钥材料失效或误删除时重新导入该密钥材料。 **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。
KMS创建的密钥	● 不能手动删除密钥材料。 ● 仅对称密钥支持密钥轮换功能。 ● 不能设置密钥材料的失效时间。

- 关联性

  当用户将密钥材料导入自定义密钥时，该自定义密钥与该密钥材料永久关联，不能将其他密钥材料导入该自定义密钥中。

- 唯一性

  当用户使用导入的密钥加密数据时，加密后的数据必须使用加密时采用的自定义密钥（即自定义密钥的元数据及密钥材料与导入的密钥匹配）才能解密数据，否则解密会失败。

1.3.2 导入密钥材料

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

该任务指导用户通过密钥管理界面导入密钥材料。

约束条件

- HMAC密钥算法不支持导入密钥材料。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击“导入密钥”，弹出“导入密钥”对话框。

步骤5 在弹出的对话框中填写密钥参数。

图 1-2 创建空密钥

- 别名：待创建密钥的别名。

  说明

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

- 密钥算法：选择密钥算法。KMS支持的密钥算法说明如表1-4所示。

版权所有 © 华为技术有限公司

表 1-4 KMS 支持的密钥算法类型

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

- 密钥用途：可选择“SIGN_VERIFY”、“ENCRYPT_DECRYPT”、“GENERATE_VERIFY_MAC”。
  - 对于AES_256对称密钥，默认值“ENCRYPT_DECRYPT”。
  - 对于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”。

  说明

  创建密钥时请选择“密钥用途”，密钥创建后不可修改。

- （可选）描述：可根据自己的需要为自定义密钥添加描述。

  说明

  支持长度为1 ~ 255个字符。

- 企业项目：该参数针对企业用户使用。

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

  未开通企业管理的用户页面则没有“企业项目”参数项，无需进行配置。

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

说明

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

步骤7 单击“安全性与持久性”阅读并了解导入密钥的安全性和持久性。

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

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

图 1-3 获取包装密钥和导入令牌

表 1-5 密钥包装算法说明

密钥包装算法	说明	设置
RSAES_OAEP_SHA_256	具有“SHA-256”哈希函数的OAEP的RSA加密算法。	请您根据自己的HSM功能选择加密算法。 如果您的HSM支持“RSAES_OAEP_SHA_256”加密算法，推荐使用“RSAES_OAEP_SHA_256”加密密钥材料。

说明

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

步骤10 获取“包装密钥”和“导入令牌”，并加密密钥材料，如果您已有密钥材料，可跳过本步骤。

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

图 1-4 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。

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

– 方法二：通过调用API接口的方式获取包装密钥和导入令牌。

i. 调用“get-parameters-for-import”接口，获取包装密钥和导入令牌。
   - public_key：调用API接口返回的base64编码的包装密钥内容。
   - import_token：调用API接口返回的base64编码的导入令牌内容。

   以获取密钥ID为“43f1ffd7-18fb-4568-9575-602e009b7ee8”，加密算法为“RSAES_OAEP_SHA_256”的包装密钥和导入令牌为例。
   - 请求样例
     ```
     {
       "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
       "wrapping_algorithm":"RSAES_OAEP_SHA_256"
     }
     ```
   - 响应样例
     ```
     {
       "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
       "public_key":"public key base64 encoded data",
       "import_token":"import token base64 encoded data",
       "expiration_time":1501578672
     }
     ```

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

      openssl enc -d -base64 -A -in PublicKey.b64 -out PublicKey.bin

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

2. 使用“包装密钥”加密密钥材料。

说明

执行完此步骤后可获得以下文件：

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

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

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

方法二：使用OpenSSL生成密钥材料，并用下载的“包装密钥”对密钥材料进行加密。

说明

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

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

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

  openssl rand -out *PlaintextKeyMaterial.bin* 32

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

  1) 生成16进制AES256密钥：

     openssl rand -out 0xPlaintextKeyMaterial.bin -hex 32

  2) 将16进制AES256密钥转换成二进制格式：

     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 1-6 使用下载的包装密钥加密生成的密钥材料

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

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

- 执行以下命令（以配套算法为“RSA4096算法”为例）：
  1) 生成私钥

     openssl genrsa -out pkcs1_rsa_private_key.pem 4096
  2) 格式转换成pkcs8格式

     openssl pkcs8 -topk8 -inform PEM -in pkcs1_rsa_private_key.pem -outform pem -nocrypt -out rsa_private_key.pem
  3) pkcs8格式转换成der格式

     openssl pkcs8 -topk8 -inform PEM -outform DER -in rsa_private_key.pem -out rsa_private_key.der -nocrypt
  4) 使用临时密钥材料对私钥进行加密

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

     说明

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

步骤11 已有密钥材料时，单击“已有密钥材料”，进入“导入密钥材料”页面。

表 1-7 导入密钥材料参数说明（对称密钥场景）

参数	说明
密钥ID	创建密钥时，随机生成的密钥ID。
密钥材料	导入密钥材料。 例如：使用**步骤10.2.b**中“EncryptedKeyMaterial.bin”文件。

表 1-8 导入密钥材料参数说明（非对称密钥场景）

参数	说明
密钥ID	创建密钥时，随机生成的密钥ID。
临时密钥材料	选择导入临时密钥材料。 例如：选择**步骤10.2.b**中“EncryptedKeyMaterial.bin”文件。
私钥密文	选择导入私钥密文。 例如：选择**步骤10.2.c**中“out_rsa_private_key.der”文件。

版权所有 © 华为技术有限公司

图 1-5 导入密钥材料

步骤12 单击“下一步”，进入“密钥导入令牌”页面。根据**表1-9**设置参数。

图 1-6 导入密钥令牌

表 1-9 导入密钥令牌参数说明

参数	操作说明
密钥ID	创建密钥时，随机生成的密钥ID。
密钥导入令牌	选择**12.b**调用API获取的导入令牌。
密钥材料失效模式	• 永不失效：导入的密钥材料永久不失效。 • 失效时间：用户可指定导入的密钥材料的失效时间，默认失效时间为24小时。 密钥材料失效后，KMS会在24小时内自动删除密钥材料，删除后密钥将无法使用，且密钥状态变更为“等待导入”。

步骤13 单击“确定”，页面右上角弹出“密钥导入成功”，则说明导入密钥成功。

版权所有 © 华为技术有限公司

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

1.3.3 删除密钥材料

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

该任务指导用户通过密钥管理界面对外部导入的密钥材料进行删除操作。

说明

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

前提条件

- 用户已导入密钥材料。
- “密钥材料来源”为“外部”。
- 密钥“状态”为“启用”或“禁用”。

约束条件

- 删除密钥材料后，如果需要重新导入密钥材料，导入的密钥材料必须与删除的密钥材料完全相同，才能导入成功。
- 用户重新导入相同的密钥材料后，该自定义密钥可以解密删除密钥材料前加密的所有数据。
- 密钥材料删除后，密钥将无法使用，且当前密钥的状态切换为“等待导入”。
- 非对称密钥不支持删除密钥材料功能，如需删除，请使用删除密钥功能。

操作步骤

步骤1 登录管理控制台。

步骤2 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“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在需要删除的密钥材料所在行，单击“删除密钥材料”。

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

密钥材料删除后，密钥将无法使用，且当前密钥的状态切换为“等待导入”。

----结束

1.4 管理密钥

1.4.1 查看密钥

该任务指导用户通过KMS界面查看自定义密钥的信息，包括密钥别名、状态、ID和创建时间。密钥状态包括“启用”、“禁用”、“计划删除”和“等待导入”。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在密钥列表中，查看密钥信息，密钥列表参数说明，如表1-10所示。

图 1-7 自定义密钥列表

图 1-8 默认密钥列表

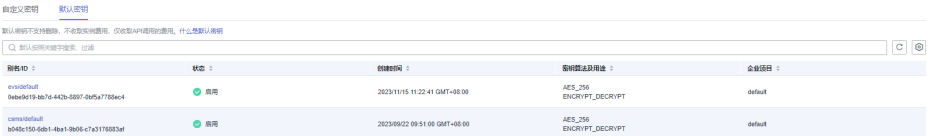


表 1-10 密钥列表参数说明

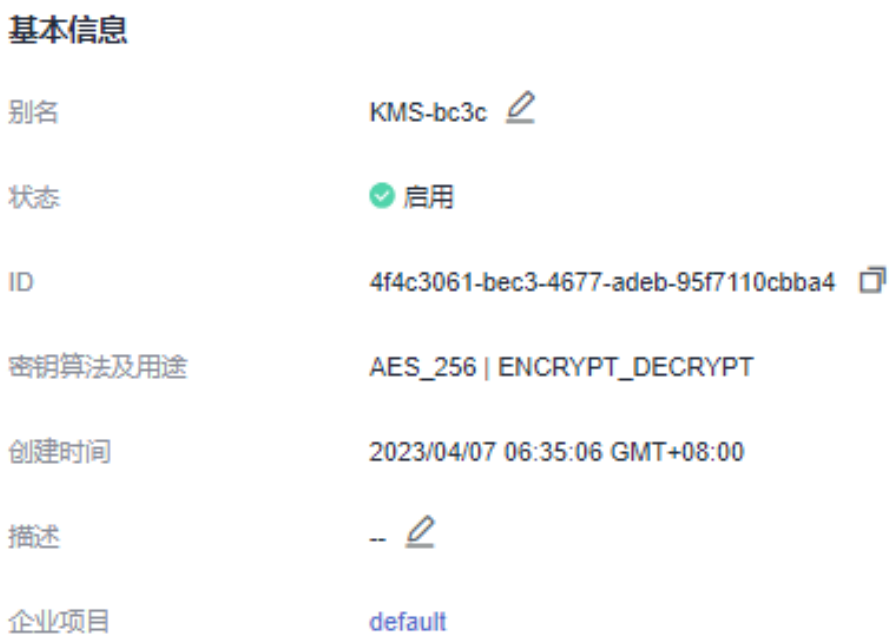
参数	操作说明
别名/ID	密钥的别名以及创建密钥时自动生成的密钥ID。 **说明** 在IAM中创建自定义策略时，添加资源路径中的“路径”填写此ID。

版权所有 © 华为技术有限公司

参数	操作说明
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。
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5 用户可单击密钥别名，查看密钥详细信息，如图 密钥详细信息所示。

图 1-9 密钥详细信息



说明

用户可单击该密钥的“别名”或“描述”所在行的 ，修改密钥的别名或描述信息。

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

----结束

1.4.2 启用密钥

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

前提条件

待启用的密钥需处于“禁用”状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ，选择区域或项目。

步骤3 单击页面左侧 ，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在需要启用的密钥所在行，单击“启用”。

图 1-10 启用单个密钥

步骤5 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

1.4.3 禁用密钥

该任务指导用户通过密钥管理界面对指定的自定义密钥进行禁用，以紧急保护数据。

自定义密钥被禁用后，用户将不能使用该密钥进行加解密任何数据。如果要使用该密钥进行加解密数据，用户需将该密钥重新启用，具体操作请参见启用密钥。

前提条件

待禁用的密钥需处于“启用”状态。

约束条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 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“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在需要禁用的密钥所在行，单击“禁用”。

图 1-11 禁用单个密钥

步骤5 在弹出窗口中，勾选“我已知晓禁用以上密钥产生的影响”，单击“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

1.4.4 删除密钥

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

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

前提条件

- 待删除的密钥需处于“启用”、“禁用”或“等待导入”状态。

约束条件

- 执行删除密钥操作后，密钥不会立即删除，密钥管理会将该操作按用户指定时间推迟执行，推迟时间范围为7天～1096天。

  在推迟删除时间未到时，如果需要重新使用该密钥，可以执行取消删除密钥操作。如果超过推迟时间，密钥将被KMS彻底删除，使用该密钥加密的数据将无法解密，请谨慎操作。
- 关于处于计划删除状态的密钥计费情况，请参见计划删除的密钥是否还计费？。
- 默认密钥为服务自动创建，不支持删除操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在需要删除的密钥所在行，单击“删除”,，进入“删除密钥”界面。

图 1-12 删除单个密钥

步骤5 在“删除密钥”界面，填写“推迟删除”的时间。

图 1-13 推迟删除时间

说明

- 密钥管理会将该操作按用户指定时间推迟执行，推迟时间范围为7天～1096天。在推迟删除时间未到时，如果需要重新使用该密钥，可以执行取消删除密钥操作。
- 关于处于计划删除状态的密钥计费情况，请参见计划删除的密钥是否还计费？。

步骤6 在确认删除提示框中输入“DELETE”后，单击“确定”，页面提示删除密钥任务下发成功，完成删除单个密钥操作。

步骤7 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 1-14 删除确认

----结束

说明

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

版权所有 © 华为技术有限公司

1.4.5 取消删除密钥

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

前提条件

待取消删除的密钥需处于“计划删除”状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在需要取消删除的密钥所在行，单击“取消删除”。

图 1-15 取消删除单个密钥

步骤5 在弹出的窗口中，单击“确定”，完成取消删除单个密钥操作。

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

说明

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

----结束

1.4.6 分配至企业项目

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

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

约束条件

- 已开通企业项目管理。

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 在目标密钥所在行，单击“分配至项目”，弹出对话框。

图 1-16 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。

步骤5 单击“确定”，完成操作。

----结束

1.5 搜索密钥

该任务指导用户在密钥管理界面，通过指定属性查找当前满足条件的自定义密钥。

操作步骤

步骤1 登录管理控制台。

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“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击搜索栏，选择筛选密钥的条件，如图 搜索栏所示，通过指定属性搜索自定义密钥。

图 1-17 搜索栏

说明

- 可根据别名、密钥ID、状态、创建时间、密钥算法、密钥用途、密钥材料失效时间、密钥材料来源、企业项目进行筛选。
- 可进行属性组合筛选，例如同时选择状态为启用，密钥算法为AES_256作为筛选条件，可查找出所有满足属性的自定义密钥。

----结束

1.6 在线工具加解密小数据

该任务指导用户通过密钥管理界面使用在线工具加解密不大于4KB的数据。

前提条件

自定义密钥处于“启用”状态。

约束条件

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

加密数据

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击目标自定义密钥的别名，进入密钥信息页面后，默认进入工具页签。

步骤5 在“加密”文本框中输入待加密的数据，如图1-18所示。

图 1-18 加密数据

版权所有 © 华为技术有限公司

步骤6 单击“执行”，右侧文本框显示加密后的密文数据。

说明

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

----结束

解密数据

步骤1 登录管理控制台。

步骤2 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤3 解密数据时，可单击任意“启用”状态的非默认密钥别名，进入该密钥的在线工具页面。

步骤4 单击“解密”，在左侧文本框中数据待解密的密文数据，如图1-19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 1-19 解密数据

步骤5 单击“执行”，右侧文本框中显示解密后的明文数据。

说明

- 用户可直接单击“复制到剪切板”拷贝解密后的明文数据，并保存到本地文件中。
- 在控制台输入的明文，会进行base64编码得到加密后的字符。

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

----结束

1.7 管理标签

1.7.1 添加标签

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

约束条件

KMS不支持为默认密钥添加标签。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤5 单击“标签”，进入标签管理页面。

步骤6 单击“添加标签”，弹出添加标签对话框，如图1-20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1-11所示。

图 1-20 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 1-11 标签参数说明

参数	参数说明	取值要求	样例
标签键	标签的名称。 同一个自定义密钥下，一个标签键只能对应一个标签值；不同的自定义密钥下可以使用相同的标签键。 用户最多可以给单个自定义密钥添加20个标签。	● 必填。 ● 对于同一个自定义密钥，标签键唯一。 ● 长度不超过128个字符。 ● 首尾不能包含空格。 ● 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7 单击“确定”，完成标签的添加。

----结束

1.7.2 修改标签值

该任务指导用户通过密钥管理界面修改标签值。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤5 单击“标签”，进入标签管理页面。

步骤6 单击目标标签所在行的“编辑”，弹出编辑标签对话框。

图 1-21 编辑标签

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

----结束

1.7.3 删除标签

该任务指导用户通过密钥管理界面删除标签。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤5 单击“标签”，进入标签管理页面。

步骤6 单击目标标签所在行的“删除”，弹出删除标签对话框。

步骤7 在弹出的删除标签对话框中单击“确定”，完成标签的删除。

----结束

1.8 轮换密钥

1.8.1 密钥轮换概述

为什么需要轮换密钥

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

定期轮换密钥有如下优点：

- 减少每个密钥加密的数据量

  一个密钥的安全性与被它加密的数据量呈反比。数据量通常是指同一个密钥加密的数据总字节数或总消息数。
- 增强应对安全事件的能力

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

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

密钥轮换的两种方法

华为云服务提供了两种密钥轮换方法：

- 手动轮换密钥

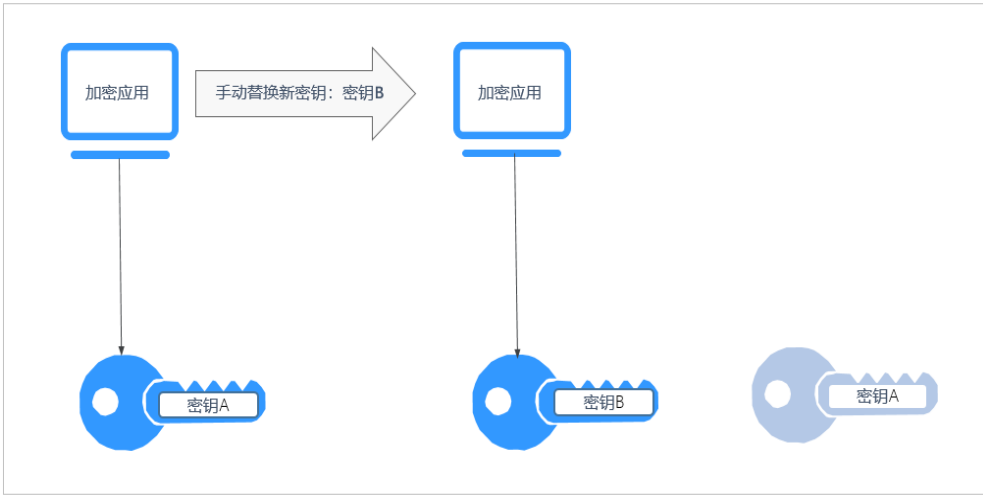
  方式一：创建一个新的密钥B，使用密钥B替换当前正在使用的密钥A。

  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 1-22 手动轮换密钥工作原理



版权所有 © 华为技术有限公司

- 自动轮换密钥

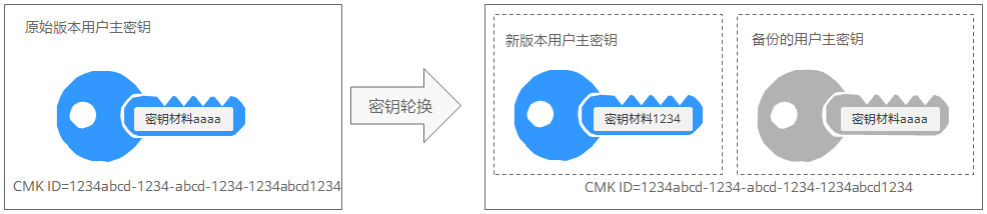
  KMS会根据设置的轮换周期（默认365天）自动轮换密钥，系统自动生成一个新的密钥B，并替换当前使用的密钥A。自动轮换密钥只会更改主密钥的密钥材料，即加密操作中所使用的加密材料。不管密钥材料有没有变更或变更了多少次，该主密钥仍是相同的逻辑资源。主密钥的属性（密钥ID、别名、描述、权限）不会发生变化。

  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 1-23 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 1-12 密钥轮换方式

密钥的来源或状态	支持的密钥轮换方式
默认密钥	不支持密钥轮换。
自定义密钥	支持自动轮换密钥或手动轮换密钥，根据密钥算法类型决定。 ● 对称密钥：支持自动轮换密钥和手动轮换密钥。 ● 非对称密钥：仅支持手动轮换密钥。
已禁用的主密钥	禁用主密钥后，KMS不会对它进行轮换。但是，密钥轮换状态不会发生改变，并且在主密钥处于禁用状态时不能对其进行更改。重新启用主密钥后，如果已禁用的自定义密钥已超过轮换周期，KMS会立即轮换。如果已禁用的自定义密钥少于轮换周期，KMS会恢复之前的密钥轮换计划。 关于禁用密钥的信息，请参见已禁用的主密钥。

密钥的来源或状态	支持的密钥轮换方式
计划删除的主密钥	对于计划删除的主密钥，KMS不会对它进行轮换。如果取消删除，将恢复之前的密钥轮换状态。如果计划删除的自定义密钥已超过轮换周期，KMS会立即轮换。如果计划删除的用户主密钥少于轮换周期，KMS会恢复之前的密钥轮换计划。 关于计划删除密钥的信息，请参见计划删除的主密钥。

说明

用户可在“轮换策略”页面查看轮换详情，例如：上次轮换时间、轮换次数。

轮换密钥的定价

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。

1.8.2 开启密钥轮换

该任务指导用户通过密钥管理界面开启自动轮换密钥。

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

前提条件

- 密钥处于“启用”状态。
- “密钥材料来源”为“密钥管理”。
- 仅对称密钥支持开启密钥轮换。

约束条件

- 如果自定义密钥开启密钥轮换以后，禁用了自定义密钥，KMS也不会轮换该自定义密钥。

  当自定义密钥恢复到“启用”状态时，密钥轮换将立即重新激活。如果刚恢复“启用”状态的自定义密钥距离上次轮换的时间已超过轮换周期，KMS将在24小时内轮换该自定义密钥。
- 只有区域主密钥可以进行轮转，副本密钥不允许进行密钥轮转。

操作步骤

步骤1 登录管理控制台。

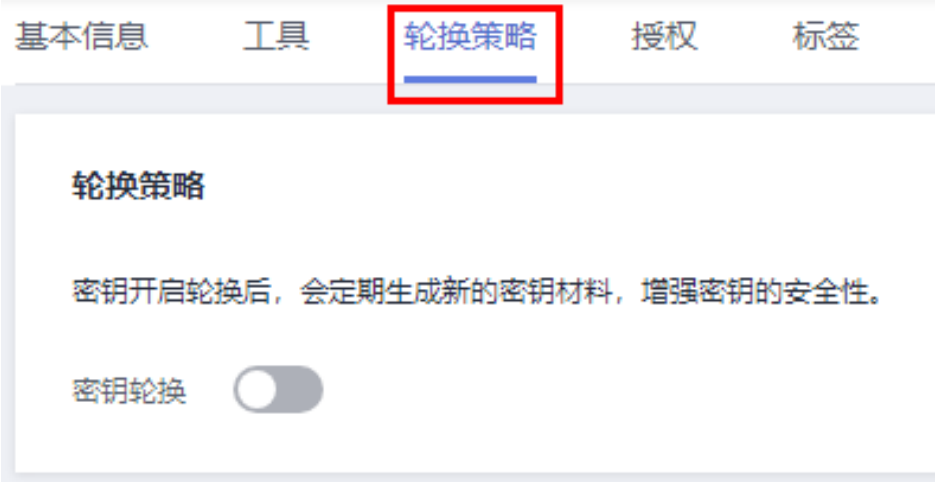
步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤5 单击“轮换策略”，进入“轮换策略”页面，如图1-24所示。

图 1-24 密钥轮换



步骤6 单击，将“密钥轮换”设置为，弹出“启用轮换策略”对话框。

步骤7 设置轮换周期（天），单击“确定”。如图1-25所示。参数说明如表1-13所示。

图 1-25 开启密钥轮换

表 1-13 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。

版权所有 © 华为技术有限公司

参数	说明
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8 开启后，页面显示密钥轮换详情，如图 密钥轮换详情所示。

图 1-26 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

1.8.3 关闭密钥轮换

该任务指导用户通过密钥管理界面关闭自动轮换密钥。

前提条件

- 密钥处于“启用”状态。
- “密钥材料来源”为“密钥管理”。
- 已开启密钥轮换。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击目标对称密钥的别名，进入密钥详细信息页面。

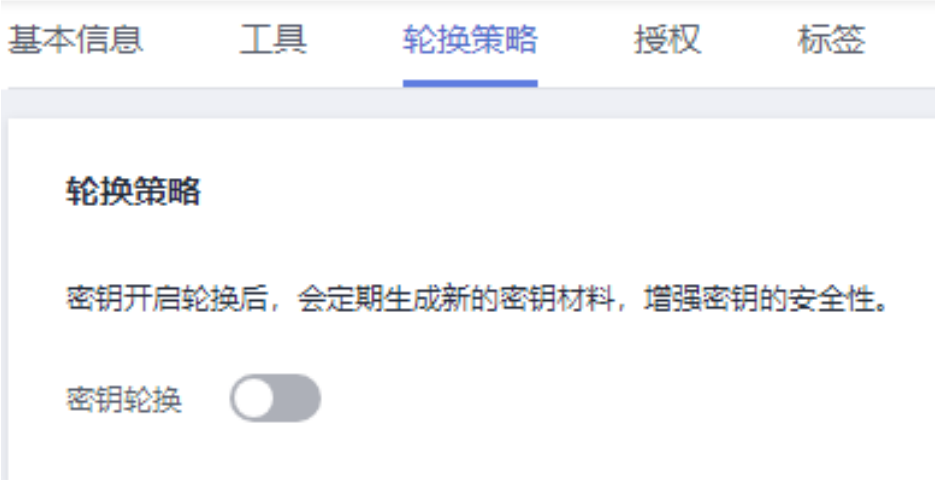
步骤5 单击“轮换策略”，进入密钥轮换管理界面。

步骤6 单击，关闭密钥轮换。

步骤7 在弹出的确认是否关闭密钥轮换提示框中，单击“确定”。

步骤8 关闭后，页面将显示密钥轮换管理界面，如图1-27所示。

图 1-27 关闭密钥轮换



----结束

1.9 管理授权

1.9.1 创建授权

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

前提条件

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

约束条件

- 自定义密钥的所有者可通过KMS界面或者调用API接口的方式为自定义密钥创建授权；被自定义密钥所有者授予了“创建授权”操作权限的IAM用户或账号仅能通过调用API接口的方式为自定义密钥创建授权。
- 一个自定义密钥下最多可创建100个授权。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击目标自定义密钥的别名，进入密钥详细信息授权页面。

步骤5 单击“授权”，进入授权管理界面。

步骤6 单击“创建授权”，弹出“创建授权”对话框。

图 1-28 创建授权（用户）

图 1-29 创建授权（账号）

步骤7 在弹出的对话框中，输入被授权用户ID，并勾选授权操作的权限。参数说明请参见表1-14。

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 1-14 创建授权参数说明

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

版权所有 © 华为技术有限公司

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 1-15 授权操作

密钥算法	密钥类型	密钥用途	授权操作
● AES_256 ● SM4	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 ● SM2	非对称密钥	SIGN_VERIFY	● 查询公钥信息 ● 签名 ● 验签
● RSA_2048 ● RSA_3072 ● RSA_4096 ● SM2	非对称密钥	ENCRYPT_DECRYPT	● 查询公钥信息 ● 加密数据 ● 解密数据

版权所有 © 华为技术有限公司

密钥算法	密钥类型	密钥用途	授权操作
• HMAC_256 • HMAC_384 • HMAC_512 • HMAC_SM3	摘要密钥	GENERATE_VERIFY_MAC	• 生成HMAC • 校验HMAC

步骤8 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

1.9.2 查询授权

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

前提条件

用户已创建授权。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤5 单击“授权”，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1-16所示。

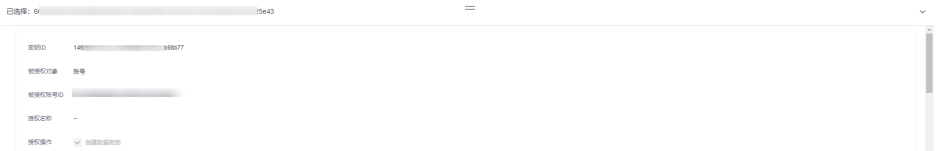
表 1-16 授权信息参数说明

参数	参数说明
授权名称	创建授权时为授权进行命名。
授权类型	授权类型：用户和账号。
被授权ID	被授权的ID。
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）。

参数	参数说明
创建时间	创建该授权的时间。
操作	用户可以在操作栏中，执行撤销授权操作。

步骤6 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 1-30 授权详情



----结束

1.9.3 撤销授权

在以下两种情况下，授权用户可以通过密钥管理界面撤销授权：

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

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

该任务指导用户通过KMS界面撤销授权。

前提条件

用户已创建授权。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 单击目标自定义密钥的别名，进入密钥详细信息页面。

步骤5 在目标授权ID所在行，单击“撤销授权”。

步骤6 在弹出的对话框中单击“确定”，页面右上角弹出“授权撤销成功”，则说明撤销授权成功。

----结束

2 凭据管理

2.1 凭据概述

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。

RDS 凭据

数据库凭据泄露是导致数据泄露的主要途径。针对华为云关系型数据库RDS，凭据管理服务支持托管RDS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。

通用凭据与 RDS 凭据差异

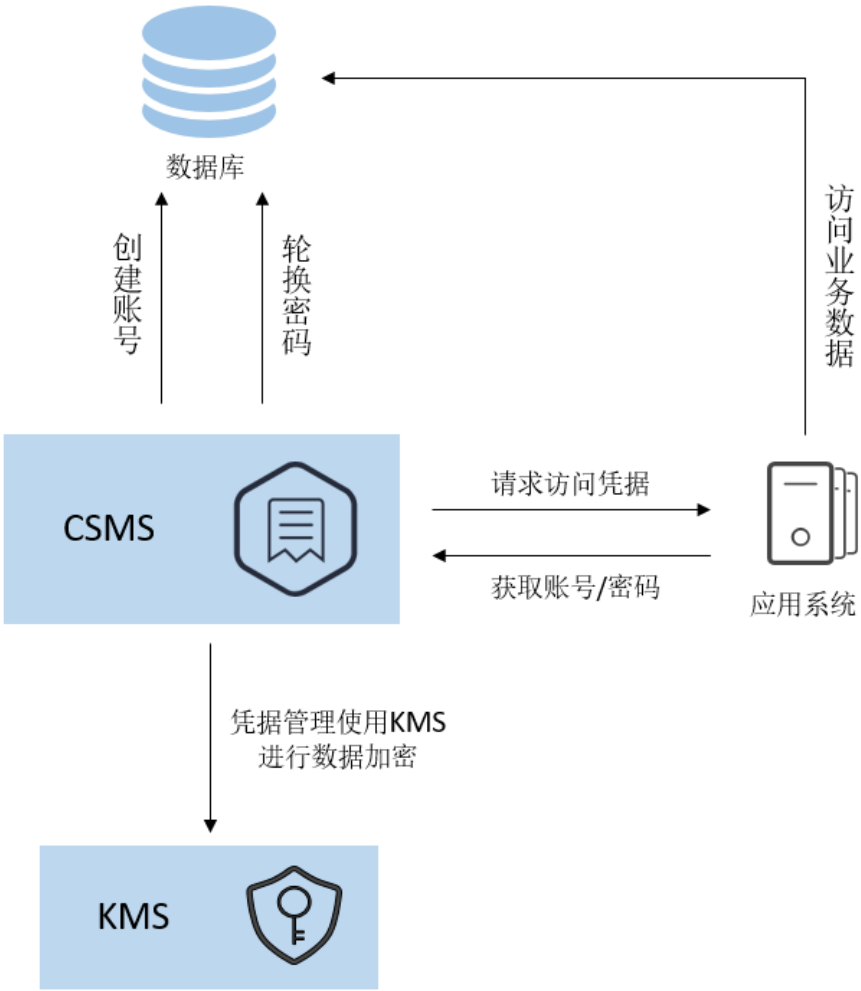
表 2-1 凭据差异

凭据类型	通用凭据	RDS凭据
使用场景	各场景下自定义凭据的全生命周期管理	自动托管华为云RDS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

版权所有 © 华为技术有限公司

RDS 凭据使用流程

图 2-1 产品架构



流程说明：

1. 创建一个RDS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。

版权所有 © 华为技术有限公司

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。

2.2 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

2.3 创建凭据

2.3.1 创建通用凭据

该任务指导用户通过凭据管理界面创建凭据。

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

约束条件

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

版权所有 © 华为技术有限公司

创建凭据

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤5 单击“创建凭据”。弹出“创建凭据”对话框，如图 创建凭据所示，填写参数，参数说明如表 凭据配置参数说明所示。

图 2-2 创建凭据

版权所有 © 华为技术有限公司

表 2-2 凭据配置参数说明

参数名称	参数说明
凭据类型	创建凭据类型，默认通用凭据。
凭据名称	待创建凭据的名称。 **说明** 仅支持输入英文字符、数字、“-”、“_”。
企业项目	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。
设置凭据值	待加密的用户凭据键/值和明文凭据。
描述信息（可选）	凭据的描述信息。
KMS加密	可选择默认密钥“csms/default”或用户在KMS已创建的自定义密钥 **说明** ● CSMS使用KMS提供的加密密钥对私钥进行加密，用户使用密钥对的KMS加密功能时，可选择KMS创建的默认密钥“csms/default”。 ● 用户使用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。
关联事件	创建凭据时可关联一个凭据事件，凭据版本的增删改查可通过事件通知界面查看。

步骤6 单击“下一步”，设置轮转周期。

步骤7 单击“下一步”，确认创建的信息。

步骤8 单击“确定”，凭据创建完成。

用户可在凭据列表查看已完成创建的凭据，凭据默认状态为“启用”。

----结束

2.3.2 创建 RDS 凭据

该任务指导用户通过凭据管理界面创建通RDS凭据

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

约束条件

- 用户最多可创建200个凭据。

- 默认使用凭据管理为您创建的默认密钥“csms/default”作为当前凭据的加密密钥。您也可以前往KMS服务页面创建自定义对称密钥，并使用自定义加密密钥。
- RDS凭据支持的数据库引擎为：MySQL。暂不支持SQL Server数据库。
- 当前RDS凭据支持在以下区域使用：华北-北京四、华东-上海一、华南-广州、中国-香港、亚太-新加坡、拉美-圣保罗一。

创建通用凭据

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤5 单击“创建凭据”，选择RDS实例凭据，如图 RDS实力凭据所示。

图 2-3 RDS 实力凭据

步骤6 在弹出的“创建凭据”对话框中，填写参数，参数说明如**表 RDS凭据参数说明**所示。

版权所有 © 华为技术有限公司

表 2-3 RDS 凭据参数说明

参数名称	参数说明
凭据类型	创建凭据类型，选择RDS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RDS实例	选择用户通过RDS控制台创建的实例名称。 **说明** 目前仅支持选择MySQL数据库。
设置凭据值	待加密的用户凭据键/值和明文凭据。 ● 选择单账号托管时，需要填入一个可使用的数据库账号及口令。 ● 选择双账号托管时，需要填入两个可使用的数据库账号及口令。 具体差异可以参考凭据概述中的**轮转策略**。
描述信息	凭据的描述信息
KMS加密	支持选择的密钥： 1. 可选择默认密钥“csms/default”。 2. 用户在KMS创建的自定义密钥，具体操作请参见**创建密钥**。 3. 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**。
标签（可选）	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。
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。

步骤7 单击“下一步”，选择轮转周期。

须知

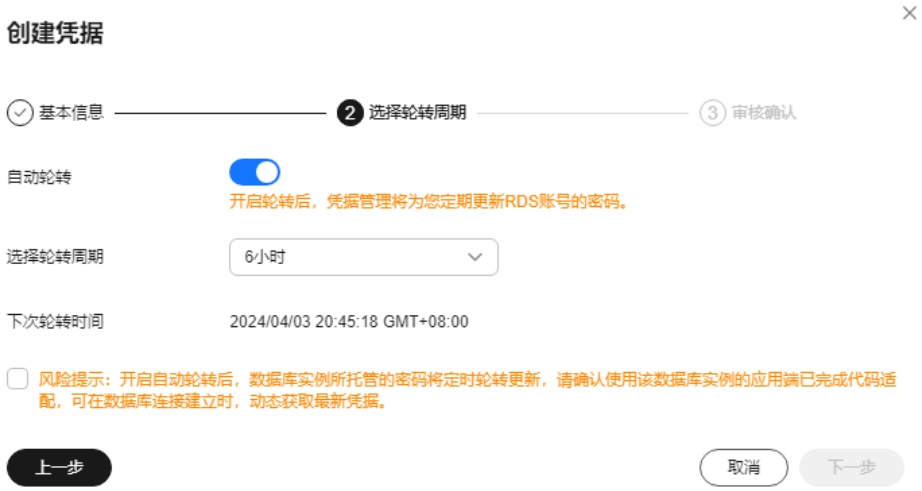
如果自动轮转开关未打开，凭据需进行手动轮转。后续如果需开启自动轮转，可在凭据详情页面单击“设置轮转策略”，开启自动轮转并设置轮转周期。

步骤8 打开自动轮转开关，选择轮转周期，可选择已有轮转周期或者自定义设置轮转周期。

自定义设置轮转周期的取值为6-8760小时，默认选择6小时。

版权所有 © 华为技术有限公司

图 2-4 选择轮转周期



步骤9 勾选“风险提示”，单击“下一步”，确认创建的信息。

图 2-5 凭据信息

步骤10 单击“确定”，凭据创建完成，页面右上角提示创建凭据成功。

步骤11 用户可在凭据列表查看已完成创建的凭据，如图 凭据列表所示，凭据默认状态为“启用”。

版权所有 © 华为技术有限公司

图 2-6 凭据列表

----结束

2.4 管理凭据

2.4.1 查看凭据

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

操作步骤

步骤1 登录管理控制台。

步骤2 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“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤5 在凭据列表中，查看凭据信息，凭据列表参数说明，如表2-4所示。

图 2-7 凭据列表

表 2-4 凭据列表参数说明

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

版权所有 © 华为技术有限公司

步骤6 用户可单击凭据名称，查看凭据详细信息，如图2-8所示。

图 2-8 凭据详细信息

说明

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

----结束

2.4.2 通过事件搜索凭据

该任务指导用户在凭据管理界面，通过关联事件搜索凭据。

前提条件

凭据已进行事件关联。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤5 单击搜索栏，选择“关联事件”作为凭据筛选的条件，如图 凭据搜索所示，通过指定关联事件搜索凭据。

图 2-9 凭据搜索

----结束

2.4.3 删除凭据

在删除凭据前，您需要确保该凭据没有被使用或将来也不会被使用。

前提条件

待删除的凭据需处于“启用”状态。

约束条件

- “计划删除凭据”不会立即删除，凭据管理会将该操作按用户指定时间推迟执行，推迟时间范围为7天～30天。在推迟删除时间未到时，如果需要重新使用该凭据，可以执行撤销删除凭据操作。如果超过推迟时间，凭据将被彻底删除，请谨慎操作。
- 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。

删除凭据

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

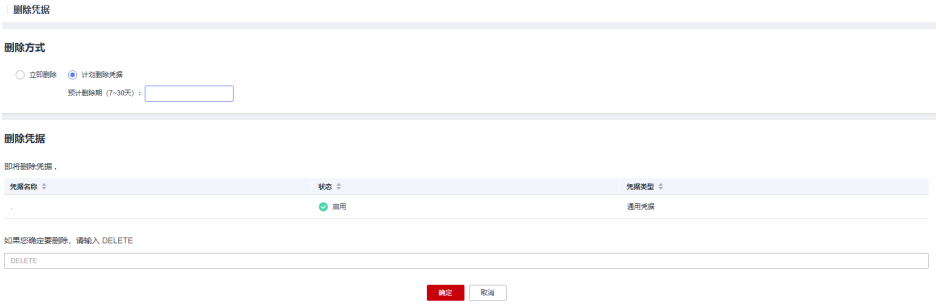
步骤4 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤5 在需要删除的凭据所在行，单击“删除”。

图 2-10 删除凭据

步骤6 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 2-11 推迟删除时间



步骤7 在确认删除提示框中输入“DELETE”后，单击“确定”，页面提示删除凭据成功，完成删除凭据操作。

版权所有 © 华为技术有限公司

说明

- “计划删除凭据”不会立即删除，凭据管理会将该操作按用户指定时间推迟执行，推迟时间范围为7天～30天。在推迟删除时间未到时，如果需要重新使用该凭据，可以执行撤销删除凭据操作。如果超过推迟时间，凭据将被彻底删除，请谨慎操作。
- 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。

----结束

2.5 管理凭据版本

2.5.1 存入和查看凭据值

该任务指导用户通过凭据管理界面存入凭据值和查看凭据值。

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

约束条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤5 单击凭据名称，进入凭据详细信息页面。

步骤6 在区，单击“存入凭据值”，弹出存入凭据值对话框，如图2-12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 2-12 存入凭据值

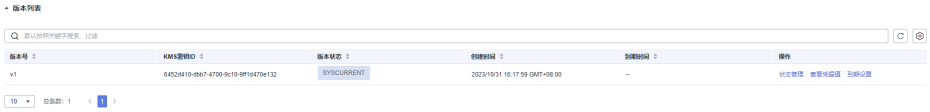
步骤7 可以为存入的凭据值选择一个到期时间，时间可具体到秒。设置完成后可在凭据版本列表中查看到期时间。例如2023年6月30日19：52：59。

步骤8 单击“确定”，在页面右上角弹出“版本凭据值添加成功”，则说明凭据值添加完成。

在凭据版本列表查看最新凭据值。

步骤9 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2-13所示，弹出查看凭据值对话框。

图 2-13 凭据版本列表



步骤10 查看凭据值，单击“确定”，关闭当前对话框。

----结束

2.5.2 管理版本状态

该任务指导用户通过凭据管理界面，进行新增、更改和删除凭据版本状态的操作。

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

约束条件

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

版权所有 © 华为技术有限公司

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤5 单击凭据名称，进入凭据详细信息页面。

步骤6 在“版本列表”区，单击目标凭据版本所在行的“状态管理”。

图 2-14 凭据版本列表

步骤7 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 2-15 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。

版权所有 © 华为技术有限公司

- 删除凭据版本状态

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

  说明

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

----结束

2.6 管理标签

2.6.1 添加标签

标签用于标识凭据。为凭据添加标签，可以方便用户对凭据进行分类和跟踪。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤5 单击凭据名称，进入凭据详细信息页面。

步骤6 在“标签”区，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2-5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 2-5 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7 单击“确定”，完成标签的添加。

----结束

2.6.2 通过标签搜索凭据

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

前提条件

已添加标签。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤5 单击“标签搜索”，展开搜索框，如图2-17所示。

图 2-17 标签搜索框

步骤6 在搜索框中输入或选择“标签键”和“标签值”。

步骤7 单击 +，添加到搜索条件中，并单击“搜索”，显示满足搜索条件的凭据列表，如图2-18所示。

图 2-18 搜索结果

说明

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

----结束

2.6.3 修改标签值

该任务指导用户通过凭据管理界面修改标签值。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤5 单击凭据名称，进入凭据详细信息页面。

步骤6 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。

图 2-19 编辑标签

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

----结束

2.6.4 删除标签

该任务指导用户通过凭据管理界面删除标签。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在左侧导航树中，选择“凭据管理”，进入“凭据管理”页面。

步骤5 单击凭据名称，进入凭据详细信息页面。

步骤6 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。

步骤7 在弹出的删除标签对话框中单击“确认”，完成标签的删除。

----结束

2.7 创建事件

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。

操作步骤

步骤1 登录管理控制台。

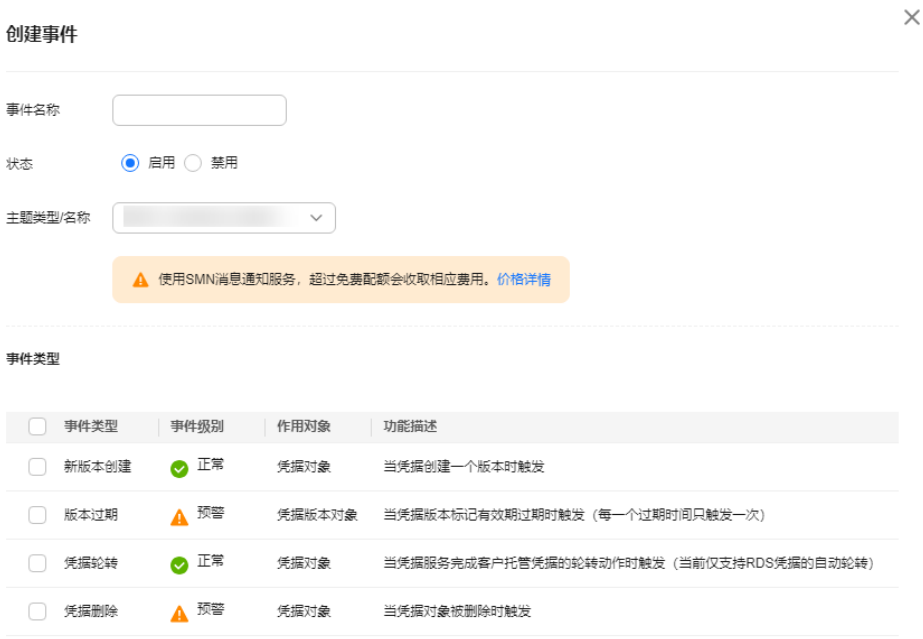
步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击右上角“创建事件”，弹出创建事件页面，如图 创建事件所示。

图 2-20 创建事件



版权所有 © 华为技术有限公司

表 2-6 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。
主题类型/名称	主题类型：默认选择SMN。 名称：在消息通知服务（SMN）中创建的主题名称。 **说明** 如果需创建自定义主题类型/名称，具体操作参见**创建主题**。
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。

步骤6 单击“确定”，完成事件创建。

步骤7 在事件列表中查看已创建的事件，如**图 事件列表**所示。事件状态默认为“启用”。

图 2-21 事件列表

----结束

2.8 管理事件

2.8.1 查看事件

该任务指导用户通过事件通知页面查看创建事件的信息，包括事件名称、状态、订阅事件类型、主题类型/名称、创建时间。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 在事件列表中，查看事件信息，事件列表参数如**表 事件列表参数说明**所示。

版权所有 © 华为技术有限公司

图 2-22 事件列表

表 2-7 事件列表参数说明

参数名称	参数说明
事件名称	创建事件的名称。
状态	事件的状态，包含 ● 启用 ● 禁用
订阅事件类型	创建事件时选择的事件类型，包含 ● 新版本创建 ● 版本过期 ● 凭据轮转 ● 凭据删除
主题类型/名称	主题类型：默认选择SMN类型。 名称：用户在SMN服务中创建的主题名称。
创建时间	创建该事件的时间。
操作	用户可在操作栏中，执行编辑、删除操作。

步骤6 单击“事件名称”，可查看事件详细信息，如图 事件详情所示

图 2-23 事件详情

----结束

版权所有 © 华为技术有限公司

2.8.2 编辑事件

该任务指导用户通过事件通知页面对已创建事件类型进行修改。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击目标事件所在列的“编辑”，进入编辑事件界面。

步骤6 勾选目标事件类型修改已创建事件，如图 编辑事件所示。

图 2-24 编辑事件

步骤7 单击“确定”，完成事件更新。

----结束

2.8.3 启用事件

该任务指导用户通过事件通知页面针对被禁用的事件，进行启用操作。

前提条件

待启用的事件需处于“禁用”状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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。

版权所有 © 华为技术有限公司

步骤5 单击需启用事件所在列的“编辑”，进入编辑事件界面。

步骤6 单击选择“启用”，将禁用状态事件修改为启用状态。

图 2-25 启用事件

步骤7 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

----结束

2.8.4 禁用事件

该任务指导用户通过事件通知页面针对已启用的事件，进行禁用操作。

前提条件

待禁用的事件需处于“启用”状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击需禁用事件所在列的“编辑”，进入编辑事件界面。

步骤6 单击选择“禁用”，将启用状态事件修改为禁用状态。

图 2-26 禁用事件

步骤7 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。

----结束

2.8.5 删除事件

该任务指导用户通过事件通知页面删除已创建的事件，删除前请确认事件已不使用。

约束条件

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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击目标事件所在行的“删除”，弹出“删除事件”对话框，如所示。

图 2-27 删除事件

步骤6 单击“确定”，完成删除事件操作。

----结束

2.9 通知记录

该任务指导用户查看事件通知状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面左侧 ，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击“通知记录”页签，进入通知记录查看页面。如图 通知记录所示。

图 2-28 通知记录

步骤6 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

版权所有 © 华为技术有限公司

3 密钥对管理

3.1 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，不需多次创建。

创建密钥对的方法如下：

- 通过管理控制台创建的密钥对。

  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。具体操作请参见**通过管理控制台创建密钥对**。

  说明

  - 通过管理控制台创建的密钥对使用的是“SSH-2（RSA，2048）”加解密算法。
  - IAM用户通过管理控制台创建的密钥对，仅能自己使用。如果多个IAM用户需要使用相同的密钥对，可以创建账号密钥对。

- 通过**PuTTYgen**工具创建密钥对。

  公钥和私钥均保存在用户本地，具体操作请参见**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/**。

前提条件

首次创建账号密钥对时，需要具有Tenant Administrator系统角色的用户完成一次账号密钥对创建。

版权所有 © 华为技术有限公司

约束条件

- IAM用户不支持创建账号密钥对。

通过管理控制台创建密钥对

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击“创建密钥对”，在弹出的“创建密钥对”对话框中，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。当您账号未开通账号密钥对时，默认创建SSH_RSA_2048的密钥对。

说明

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”下拉列表中选择加密密钥。如果不需要托管私钥，请跳过此步骤。

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。

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，下载私钥文件，并弹出提示对话框。

步骤10 用户需要根据提示对话框的提示信息，保存私钥文件。

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。

步骤11 单击“确定”，密钥对创建成功。密钥对创建成功后，用户可以在密钥对列表里看到新创建的密钥对信息，包括密钥对的“名称”、“指纹”、“状态”、“私钥”等。

说明

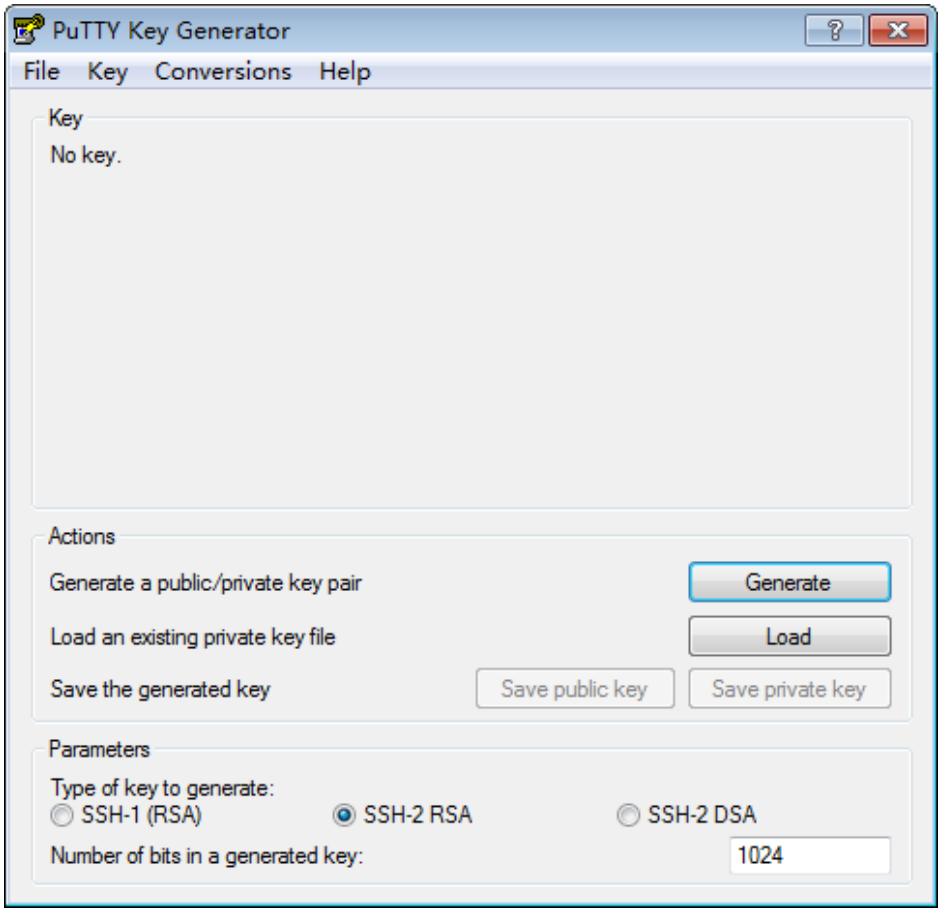
创建密钥对成功后，请确认私钥已成功下载到本地，并注意妥善保管私钥。

----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3-1设置参数。

表 3-1 生成密钥对参数说明

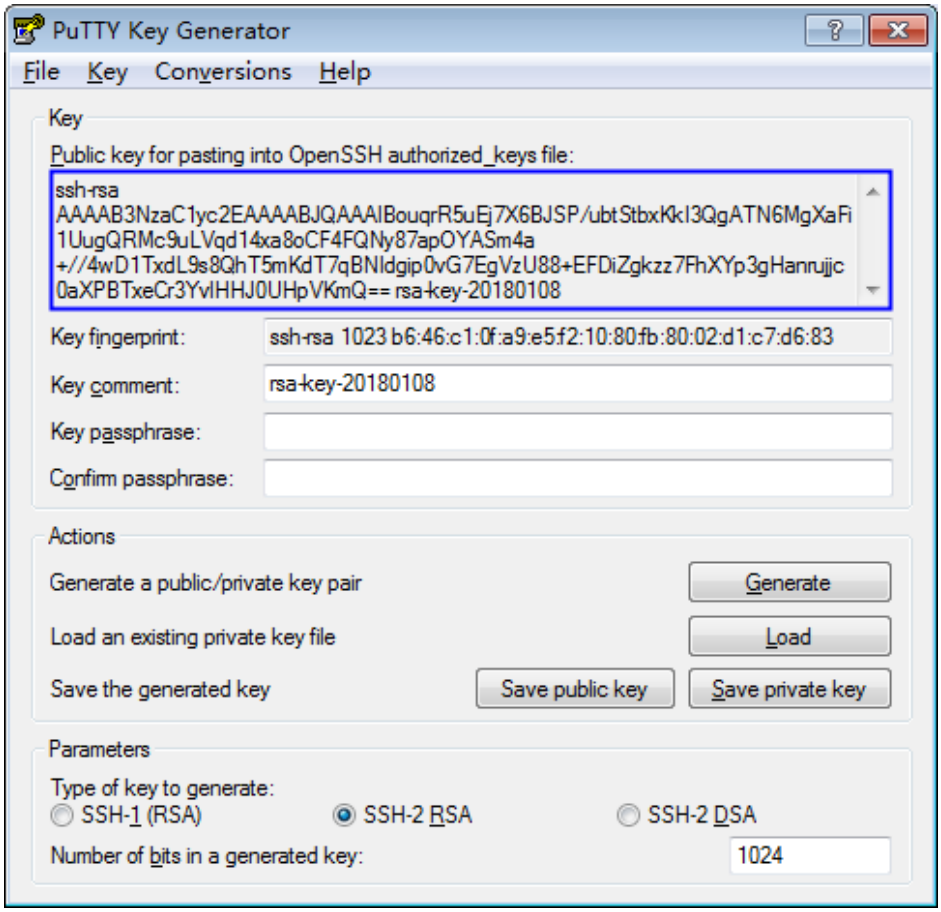
参数	参数说明
Type of key to generate	当前导入管理控制台的密钥对的加解密算法，仅支持“SSH-2 RSA”。
Number of bits in a generated key	当前支持导入管理控制台的密钥对的算法长度为：1024、2048、4096。

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。

版权所有 © 华为技术有限公司

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。

版权所有 © 华为技术有限公司

表 3-2 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

3.2 导入密钥对

如果用户需要使用自己的密钥对时（例如，使用**PuTTYgen**工具创建的密钥对），用户可以把密钥对的公钥文件导入管理控制台，使用对应的私钥远程登录弹性云服务器。用户也可根据需要将私钥托管在华为云中，由华为云统一管理。

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。

前提条件

- 已准备好待导入的密钥对公钥文件和对应的私钥文件。
- 导入的密钥对为账号密钥对，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。
- 每个IAM用户下没有相同名称的私有密钥对。
- 导入的私钥支持PKCS8格式，如果使用PKCS1格式则需要进行转换。

约束条件

- 通过外部导入的SSH密钥对支持的加解密算法为：
  - SSH-DSS

  - SSH-ED25519
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521
  - SSH_RSA有效长度为：2048，3072，4096
- 支持托管的私钥文件格式为“.pem”。
  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。
- 导入的私钥如果被加密，则会上传失败。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击“导入密钥对”，在弹出“导入密钥对”对话框中，单击“选择文件”，导入公钥文件，或将公钥内容复制并粘贴至“公钥内容”文本框中，如图3-5所示。

图 3-5 导入密钥对

说明

- 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. 单击“选择文件”，选择待导入的私钥文件（“.pem”格式），或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。

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

3.3 升级密钥对

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，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 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击“私有密钥对”页签，单击“升级密钥对”。

步骤6 在弹出的对话框中，勾选需要升级为账号密钥对的密钥对名称，单击“确定”，如图3-7所示。

图 3-7 升级密钥对

版权所有 © 华为技术有限公司

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 删除密钥对

如果创建或导入的密钥对不再使用时，用户可删除密钥对。

该任务指导用户通过密钥对管理界面删除密钥对。

约束条件

- 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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 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6 在弹出的“删除密钥对”对话框中，输入“DELETE”后，单击“确定”，页面右上角弹出“删除密钥对成功”提示信息，则说明删除密钥对成功。

----结束

3.5 管理密钥对

3.5.1 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。

该任务指导用户通过密钥对管理界面绑定密钥对。

前提条件

- 弹性云服务器的状态处于“运行中”或者“关机”状态。
- 弹性云服务器未绑定密钥对。
- 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。请确保重置密钥对前，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。

约束条件

- 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和UnionTech OS Server 20 Euler 64bit系统进行密钥对的绑定操作。

绑定密钥对

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

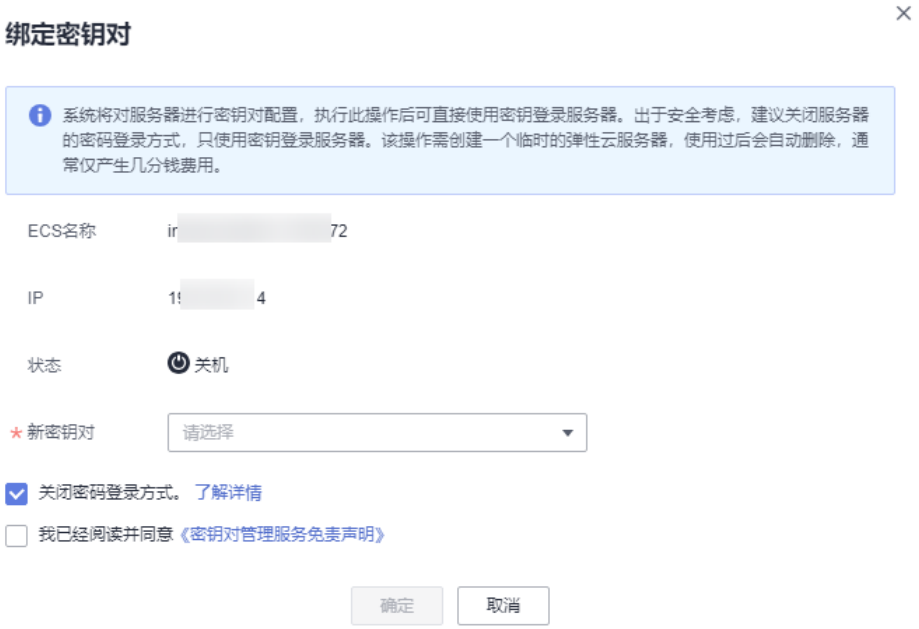
步骤4 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤5 单击“云服务器列表”，显示云服务器列表页面。

步骤6 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3-8所示。

图 3-8 绑定密钥对（一）



版权所有 © 华为技术有限公司

- 如果弹性云服务器处于“运行中”状态，需要提供“root密码”，如图3-9所示。

图 3-9 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7 在“新密钥对”下拉列表中，选择新的密钥对。

步骤8 “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配置安全规则组。
- 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9 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10 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11 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

3.5.2 批量绑定密钥对

当弹性云服务器处于“运行中”状态时，通过控制台可进行批量绑定密钥对操作。

该任务指导用户通过密钥对管理界面批量绑定密钥对。

适用场景

- 当多个需要绑定的弹性云服务器密码相同时，可输入密码并一键选择密钥。
- 当多个需要绑定的弹性云服务器密码不同时，输入弹性云服务器的密码后，需选择同一密钥对进行绑定。

前提条件

- 弹性云服务器的状态处于“运行中”状态。
- 弹性云服务器未绑定密钥对。

约束条件

- 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和UnionTech OS Server 20 Euler 64bit系统进行密钥对的绑定绑定操作。
- 用户最多可同时选择10个弹性云服务器绑定密钥对。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击“云服务器列表”，显示云服务器列表页面。

步骤6 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 3-10 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 3-11 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。

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配置安全规则组。
- 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”，完成批量绑定密钥对操作，等待约3-5分钟可绑定成功。

----结束

3.5.3 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”和“使用数量”。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

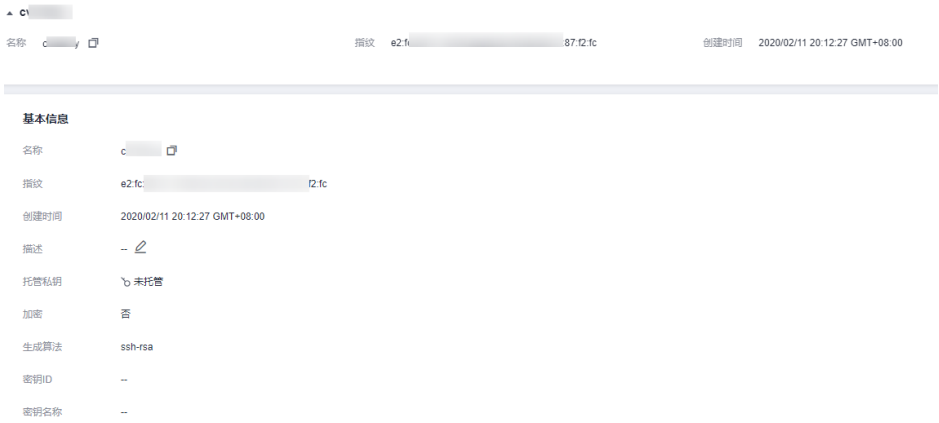
步骤5 单击“私有密钥对”，在密钥对列表中查看密钥对的信息。

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6 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3-12所示。

图 3-12 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3-3所示。

表 3-3 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 ● DELETE ● HARD_REBOOT ● MIGRATING ● REBOOT ● RESIZE ● REVERT_RESIZE ● SHELVED ● SHELVED_OFF ● LOADED ● UNKNOWN ● VERIFY_RESIZE
私有IP地址	私有IP地址。
弹性IP	弹性IP地址。

版权所有 © 华为技术有限公司

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7 单击“云服务器列表”，显示云服务器列表页面。

图 3-13 云服务器列表

步骤8 单击任务状态旁边的数字，查看密钥对执行失败记录，如图3-14所示。

说明

密钥对执行重置或者替换的状态：

：正在执行

：执行失败

图 3-14 密钥对执行失败记录

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。

----结束

3.5.4 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。

该任务指导用户通过密钥对管理界面重置密钥对。

前提条件

- 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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击“云服务器列表”。

步骤6 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3-15所示。

图 3-15 重置密钥对

步骤7 在“新密钥对”下拉列表中选择新的密钥对。

步骤8 “端口”的默认参数为22，可进行自定义修改。

版权所有 © 华为技术有限公司

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**配置安全规则组。
- 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”，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

3.5.5 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。

该任务指导用户通过密钥对管理界面替换密钥对。

前提条件

- 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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击“云服务器列表”。

步骤6 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3-16**所示。

图 3-16 替换密钥对

步骤7 在“新密钥对”下拉框中选择新的密钥对。

步骤8 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9 “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**配置安全规则组。
- 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10 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11 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

版权所有 © 华为技术有限公司

3.5.6 解绑密钥对

当用户使用的是“密钥对方式”登录弹性云服务器时，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，KPS将对弹性云服务器进行密钥对解绑操作。解绑完成后，用户可直接使用密码登录该弹性云服务器。

前提条件

- 弹性云服务器的状态处于“运行中”或者“关机”状态。
- 弹性云服务器已绑定密钥对。
- 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。

约束条件

- 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》。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

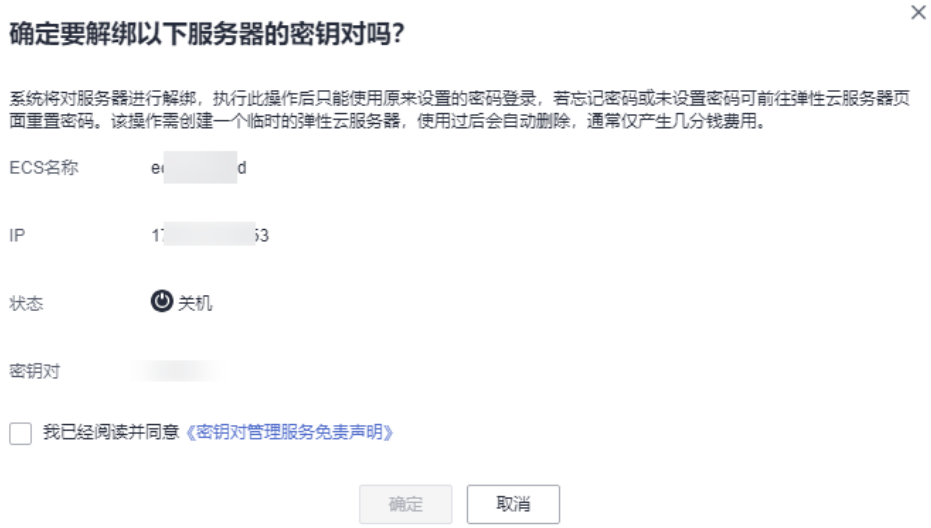
步骤4 在左侧导航树中，选择“密钥对管理”，进入“密钥对管理”页面。

步骤5 单击“云服务器列表”。

步骤6 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3-17所示。

图 3-17 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3-18所示。

图 3-18 解绑密钥对（二）

步骤7 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。

版权所有 © 华为技术有限公司

步骤8 “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**配置安全规则组。
- 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”，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

3.6 管理私钥

3.6.1 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。

该任务指导用户通过密钥对管理界面导入私钥。

前提条件

已获取与公钥匹配的私钥文件。

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。
- 用户使用密钥对的加密功能时，KMS会自动为密钥对创建一个“kps/default”默认密钥。
- 用户在选择加密密钥时，可选择已有的加密密钥，或者单击“查看密钥列表”，创建新的加密密钥。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击目标公钥所在行的“导入私钥”，弹出的“导入私钥”对话框，如图3-19所示。

图 3-19 导入私钥对话框

步骤6 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7 在“KMS加密”下拉列表中选择加密密钥。

说明

- 用户使用密钥对的加密功能时，KMS会自动为密钥对创建一个“kps/default”默认密钥。
- 用户在选择加密密钥时，可选择已有的加密密钥，或者单击“查看密钥列表”，创建新的加密密钥。

步骤8 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9 单击“确定”，完成私钥托管。

----结束

3.6.2 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。

前提条件

已将私钥托管在管理控制台。

约束条件

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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 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3-20所示。

图 3-20 导出私钥对话框

步骤6 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7 单击“确定”，浏览器自动执行下载任务，下载私钥文件。

版权所有 © 华为技术有限公司

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

3.6.3 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。

前提条件

已将私钥托管在管理控制台。

约束条件

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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击目标公钥所在行的“清除私钥”。

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6 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

3.7 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。

版权所有 © 华为技术有限公司

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 3-4 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

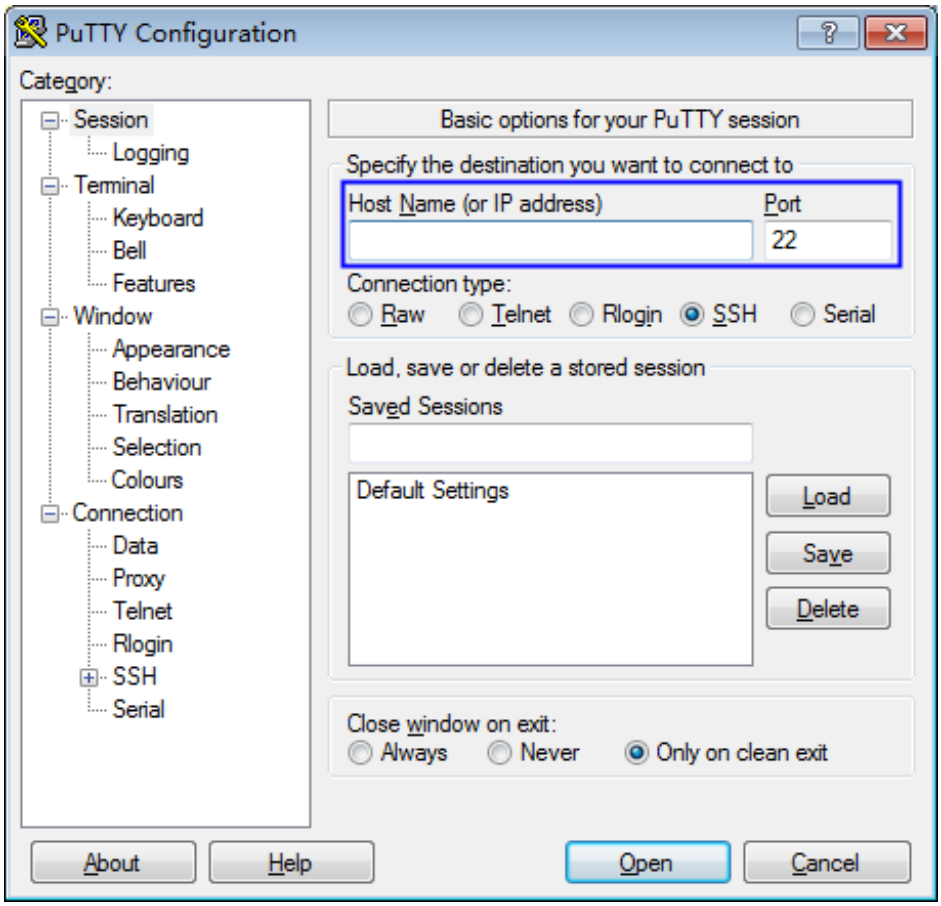
- 如果是“CoreOS”的公共镜像，镜像的用户名为“core”。
- 如果是“非CoreOS”的公共镜像，镜像的用户名为“root”。

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。

版权所有 © 华为技术有限公司

图 3-21 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

版权所有 © 华为技术有限公司

本地使用 Linux 操作系统

如果您是在Linux操作系统上登录Linu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

3.8 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

4 专属加密

4.1 操作指引

限制说明

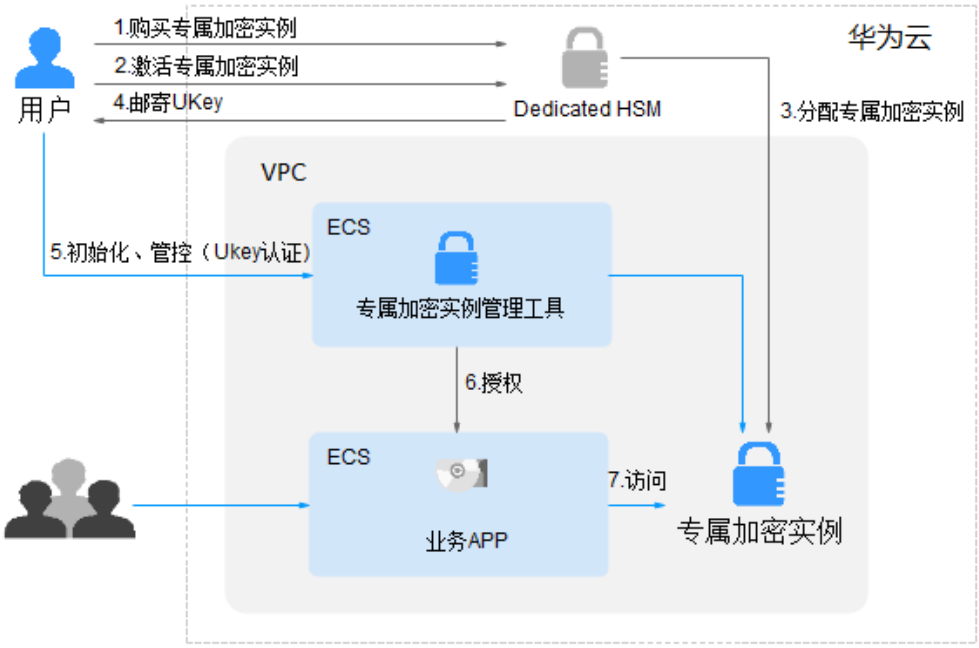
- 专属加密实例需要配合虚拟私有云（VPC）一起使用。创建专属加密实例后，需要在管理控制台中实例化专属加密实例（配置VPC网络、安全组、网卡），才能正常使用。
- 您需要将专属加密实例管理工具部署到与专属加密实例同一VPC网络中，才能对专属加密实例进行管理。

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4-1所示。

版权所有 © 华为技术有限公司

图 4-1 操作指引



操作指引说明如表4-1所示。

表 4-1 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

版权所有 © 华为技术有限公司

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我们为您提供的管理工具。 2. 使用Ukey和管理工具初始化专属加密实例，并注册相应的管理员，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节点上安装我们为您提供的安全代理软件并执行相关初始化操作。 详细操作请参见安装安全代理软件并授权。	用户
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

4.2 购买专属加密实例

4.2.1 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

- 购买专属加密实例时，需要通过提交工单的方式设置“UKey接收信息”。只有拥有“Ticket Administrator”权限的账号才可以提交工单。
- 创建成功后，华为云将按照您提供的Ukey收件地址将规划的Ukey邮寄给您，您可以使用Ukey初始化并授权您的业务APP访问专属加密实例。

同时，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“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击页面右上方的“创建专属加密实例”。

步骤6 专属加密实例仅支持“包年/包月”的“计费模式”。

图 4-2 计费模式

步骤7 选择“当前区域”、“当前项目”。

图 4-3 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8 选择专属加密实例版本，如图4-4所示，相关参数说明如表4-2所示。

版权所有 © 华为技术有限公司

图 4-4 铂金版（海外）

表 4-2 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（海外）”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 ● 非对称算法：RSA、DSA、ECDSA、DE、ECDH ● 摘要算法：SHA1、SHA256、SHA384
认证	通过FIPS 140-2 Level 3认证。

步骤9 单击“创建工单”，到工单系统中反馈联系信息，华为云安全专家将通过您提供的联系方式与您联系，确定购买和报价方案。

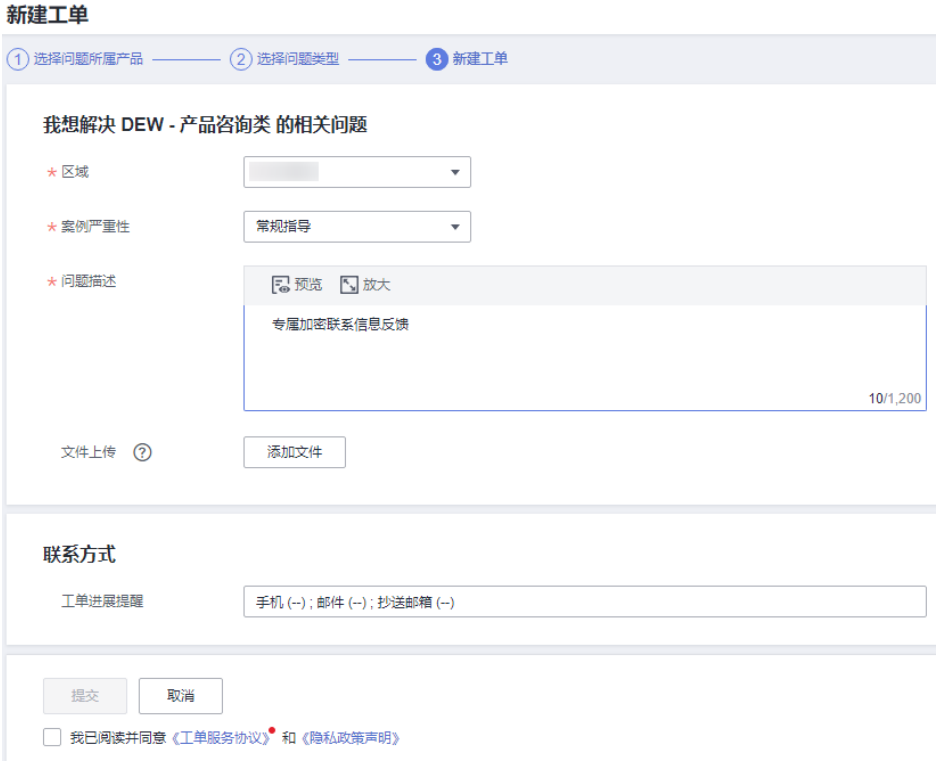
- “案例严重性”请选择“常规指导”。
- “问题描述”请填写为“专属加密联系信息反馈”。
- “联系方式”请填写电话、邮箱等用于接收工单进度信息。

须知

请确保您在工单里填写的姓名、电话、地址真实有效，以便安全专家能尽快与您取得联系。

版权所有 © 华为技术有限公司

图 4-5 新建工单



步骤10 信息填写完成后，单击“提交”，返回“我的工单”页面，可以查看到已经提交的工单列表。

说明

创建工单成功后，您可以单击工单所在行的“查看”，并根据工单的不同状态执行催单、提交留言、撤销工单、关闭工单等操作。

----结束

4.2.2 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。

版权所有 © 华为技术有限公司

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

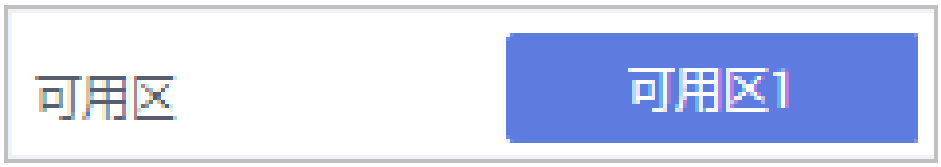
步骤3 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 单击目标专属加密实例所在行的“激活”。

步骤6 选择“可用区”。

图 4-6 选择可用区



步骤7 填写实例化信息，如图4-7所示。相关参数说明如表4-3所示。

图 4-7 实例化专属加密实例

表 4-3 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

版权所有 © 华为技术有限公司

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。 **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。 更多关于子网的信息，请参见《虚拟私有云用户指南》。	subnet-test-dhsm（192.168.0.0/24）
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8 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9 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

4.3 查看专属加密实例

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

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4-4所示。

表 4-4 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（海外）：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。
到期时间	购买的专属加密实例的到期时间。

步骤5 用户可单击专属加密实例的名称，查看实例化后专属加密实例的详细信息，如图4-8所示。

图 4-8 专属加密详细信息

版权所有 © 华为技术有限公司

专属加密实例详细信息参数说明，如表4-5所示。

表 4-5 专属加密实例详细信息参数说明

参数	参数说明
名称	专属加密实例的名称。
ID	专属加密实例的ID。
状态	专属加密实例的状态： ● 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（海外）：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》。

版权所有 © 华为技术有限公司

参数	参数说明
IP	专属加密实例的浮动IP地址。
安全组	专属加密实例所在的安全组。 更多关于安全组的信息，请参见《虚拟私有云用户指南》。
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

4.4 管理标签

4.4.1 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。

操作步骤

步骤1 单击管理控制台左上角，选择区域或项目。

步骤2 单击页面左侧 ，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

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 4-9 标签管理

版权所有 © 华为技术有限公司

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 4-10 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“_”、“.”、“:”、“/”、“=”、“+”、“-”、“@”

参数	参数说明	取值要求
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

4.4.2 通过标签搜索专属加密实例

该任务指导用户在实例列表（新版）界面，通过标签搜索当前项目下满足标签搜索条件的加密实例。

前提条件

已添加标签。

操作步骤

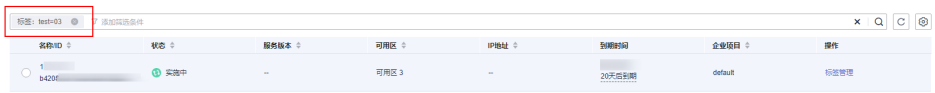
步骤1 单击管理控制台左上角，选择区域或项目。

步骤2 单击页面左侧 ☰，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

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 单击搜索框，选择标签作为筛选属性，搜索专属加密实例，如图 搜索专属加密实例所示。

图 4-11 搜索专属加密实例



----结束

版权所有 © 华为技术有限公司

4.4.3 修改标签值

该任务指导用户通过专属加密页面修改标签值。

操作步骤

步骤1 单击管理控制台左上角，选择区域或项目。

步骤2 单击页面左侧 ，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

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 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5 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 4-12 编辑标签

----结束

4.4.4 删除标签

该任务指导用户通过专属加密界面删除标签。

操作步骤

步骤1 单击管理控制台左上角，选择区域或项目。

步骤2 单击页面左侧 ，选择“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

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 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。

版权所有 © 华为技术有限公司

步骤5 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 4-13 删除标签

步骤6 在弹出的删除标签对话框中单击“是”，完成标签的删除。

----结束

4.5 使用专属加密实例

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

前提条件

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

表 4-7 信息获取

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

版权所有 © 华为技术有限公司

名称	说明	来源
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 审计日志

5.1 支持云审计的操作列表

云审计服务记录数据加密服务相关的操作事件，如**表 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 5-1 云审计服务支持的 KMS 操作列表

操作名称	资源类型	事件名称
创建密钥	cmk	createKey
创建数据密钥	cmk	createDataKey
创建不含明文数据密钥	cmk	createDataKeyWithoutPlaintext
启用密钥	cmk	enableKey
禁用密钥	cmk	disableKey
加密数据密钥	cmk	encryptDatakey
解密数据密钥	cmk	decryptDatakey
计划删除密钥	cmk	scheduleKeyDeletion
取消计划删除密钥	cmk	cancelKeyDeletion
创建随机数	rng	genRandom
修改密钥别名	cmk	updateKeyAlias
修改密钥描述	cmk	updateKeyDescription
密钥删除风险提示	cmk	deleteKeyRiskTips
导入密钥材料	cmk	importKeyMaterial

版权所有 © 华为技术有限公司

操作名称	资源类型	事件名称
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 5-2 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
下载凭据备份	secret	backupSecret
恢复凭证备份	secret	restoreSecretFromBackupBlob
更新凭据版本	secret	putSecretVersion

版权所有 © 华为技术有限公司

操作名称	资源类型	事件名称
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 5-3 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 5-4 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

5.2 查询审计事件

操作场景

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

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录：

- 在新版事件列表查看审计事件
- 在旧版事件列表查看审计事件

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。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。
- 用户通过云审计控制台只能查询最近7天的操作记录。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)，才可在OBS桶里面查看历史文件。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，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。

在新版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ☰ ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过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：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，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。
   - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
   - 云服务：在下拉框中选择对应的云服务名称。
   - 资源类型：在下拉框中选择对应的资源类型。
   - 操作用户：在下拉框中选择一个或多个具体的操作用户。
   - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
     - normal：表示操作成功。
     - warning：表示操作失败。
     - incident：表示比操作失败更严重的情况，例如引起其他故障等。
   - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近1周内任意时间段的操作事件。
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。

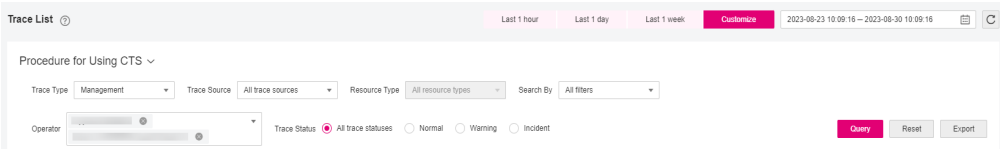
- 单击按钮，可以获取到事件操作记录的最新信息。
- 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。

6. 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**。
7. （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。

在旧版事件列表查看审计事件

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

图 5-1 筛选框

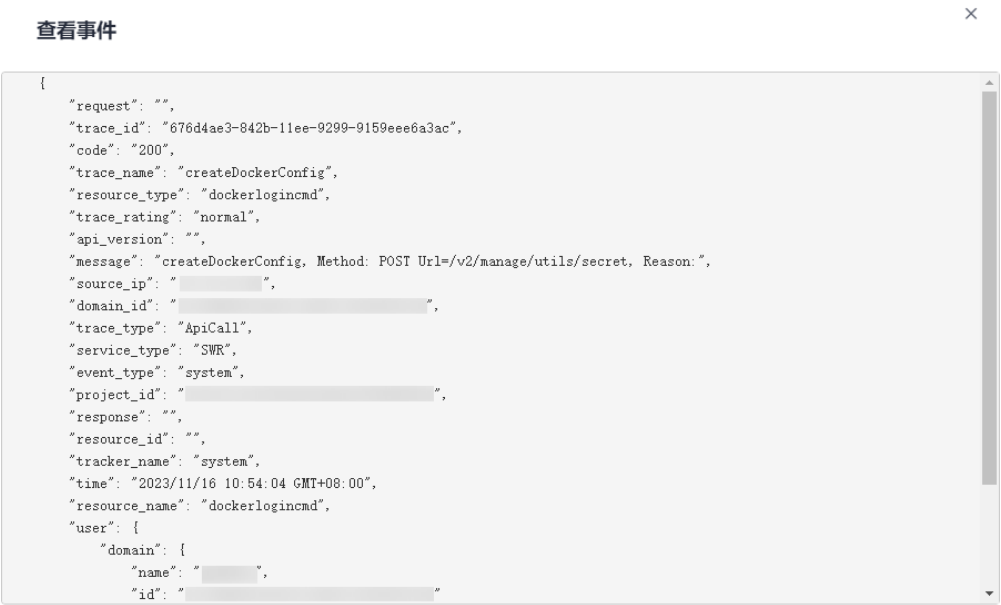


- 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
  - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
  - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
  - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
- 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
- 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
- 时间范围：可选择查询最近7天内任意时间段的操作事件。
- 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表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

6. 选择完查询条件后，单击“查询”。
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。

8. 在需要查看的事件左侧，单击 ﹀ 展开该记录的详细信息。

9. 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。



10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的**事件结构**“云审计服务事件参考 > 事件结构”章节和**事件样例**“云审计服务事件参考 > 事件样例”章节。
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。

版权所有 © 华为技术有限公司

6 共享

基于资源访问管理（Resource Access Manager，简称RAM）服务，DEW服务可以实现跨账号共享KMS密钥资源，资源所有者将KMS密钥资源同时共享给多个其他账号使用，资源使用者接受共享邀请后就可以访问和使用共享的KMS密钥资源，就像拥有它们一样。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。

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。

6.1 共享 VPC

操作场景

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。

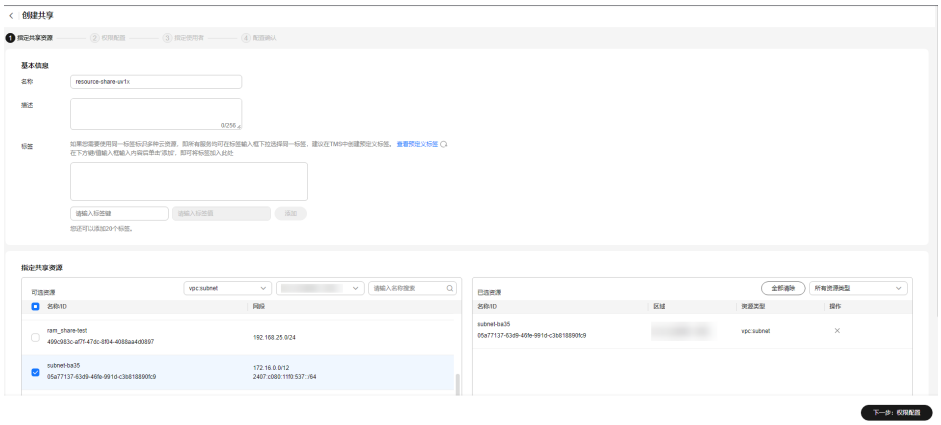
步骤2 单击页面左上角的 ☰，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

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。

版权所有 © 华为技术有限公司

图 6-1 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 6-1 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“安全与合规 > 数据加密服务”，默认进入“密钥管理”界面。

步骤4 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5 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6 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 6-2 选择共享 VPC

----结束

6.2 更新共享

用户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。

操作步骤

步骤1 登录管理控制台。

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的共享权限，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

6.3 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。

操作步骤

步骤1 登录管理控制台。

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

7 权限管理

7.1 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7-1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 7-1 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

版权所有 © 华为技术有限公司

系统角色/策略名称	描述	类别	依赖关系
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
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 7-2 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 7-3 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7-4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 7-4 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

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

版权所有 © 华为技术有限公司

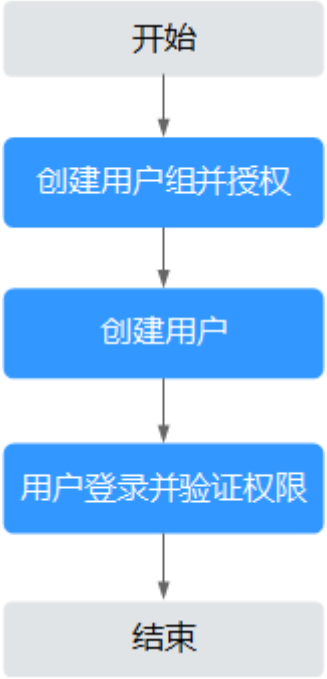
操作	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
查询密钥轮换状态	√	√	x	x
查询密钥实例	√	√	x	x
查询密钥标签	√	√	x	x
查询项目标签	√	√	x	x
批量添加删除密钥标签	√	√	x	x
添加密钥标签	√	√	x	x
删除密钥标签	√	√	x	x
查询密钥列表	√	√	x	x
查询密钥信息	√	√	x	x
查询公钥信息	√	√	x	x
查询实例数	√	√	x	x
查询配额	√	√	x	x
查询密钥对列表	x	x	√	√
创建或导入密钥对	x	x	√	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

版权所有 © 华为技术有限公司

操作	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
查询正在处理的任务	x	x	√	√

示例流程

图 7-1 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。

   在IAM控制台创建用户，并在“操作”列下选择“授权”，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。

7.2 DEW 自定义策略

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

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"
            ]
        }
    ]
}
```

A 修订记录

发布日期	修改说明
2024-04-30	第三十四次正式发布。 新增**共享VPC**章节，关于共享VPC创建、使用等操作。
2023-06-30	第三十三次正式发布。 新增**搜索密钥**章节，搜索方式更新。 新增2.5.1-凭据概述章节，通用凭据与RDS凭据介绍。 新增2.5.2-轮转策略章节，单用户轮转和双用户轮转策略。 新增2.5.3.2-创建RDS凭据章节，创建RDS凭据操作流程。 新增2.5.5.5-轮转凭据版本章节，RDS凭据自动轮转。 新增**创建事件**章节，事件通知创建。 新增**管理事件**章节，事件的查看、搜索、启用、禁用、删除等操作。 新增**通知记录**章节，事件触发后生成对应通知信息。 新增**批量绑定密钥对**章节，支持批量绑定密钥对。 新增**管理标签**章节，专属加密实例新增标签的增删改查功能。 修改**密钥概述**章节，增加关于HMAC密钥算法类型介绍。 修改**创建密钥**章节，HMAC密钥约束条件及用途。 修改**管理密钥对**章节，密钥对新增22端口描述。
2023-02-21	第三十二次正式发布。 新增**支持云审计的操作列表**章节，凭据管理操作事件。

版权所有 © 华为技术有限公司

发布日期	修改说明
2023-01-11	第三十一次正式发布。 修改导入密钥材料章节，优化加密密钥材料内容。
2022-11-22	第三十次正式发布。 “专属加密 > 版本说明”章节由“用户指南”更改至“产品介绍”中。
2022-11-15	第二十九次正式发布。 新增管理授权章节。
2022-07-22	第二十八次正式发布。 优化密钥轮换概述章节，调整内容。
2021-12-17	第二十七次正式发布。 修改 ● 导入密钥，支持导入非对称密钥。 ● 删除密钥材料，添加约束条件：非对称密钥不支持删除密钥材料功能。
2021-10-26	第二十六次正式发布。 新增凭据管理章节。
2021-09-30	第二十五次正式发布。 ● 修改创建密钥章节，新增国密算法相关描述。 ● 修改导入密钥章节，新增国密算法相关描述。 ● 修改管理密钥对章节，更新截图。
2021-08-30	第二十四次正式发布。 全文修改“专业版”为“铂金版”。
2021-07-20	第二十三次正式发布。 ● 数据加密服务入口由“安全”更改为“安全与合规”。 ● 修改创建密钥章节，修改创建密钥步骤和截图。 ● 修改管理密钥章节，优化内容和更新截图。 ● 修改管理密钥对章节，优化密钥对相关描述。 ● 新增密钥概述章节，增加密钥类型的相关描述。 ● 修改管理私钥章节，优化操作内容。 ● 修改专属加密章节，优化操作内容。
2021-06-30	第二十二次正式发布。 ● 新增分配至企业项目章节。 ● 修改绑定密钥对章节，增加约束条件。 ● 修改管理密钥章节，更新截图。

版权所有 © 华为技术有限公司

发布日期	修改说明
2021-02-22	第二十一次正式发布。 修改创建专属加密实例章节。
2020-12-21	第二十次正式发布。 文档Section优化。
2020-12-14	第十九次正式发布。 修改**创建密钥**章节。
2020-09-25	第十八次正式发布。 修改创建专属加密实例章节。
2020-08-24	第十七次正式发布。 修改**DEW自定义策略**，增加了关于获取KeyId的相关描述。
2020-08-12	第十六次正式发布。 ● 新增**升级密钥对**章节。 ● **创建密钥对**章节，更新了入口截图。 ● **导入密钥对**章节，更新了入口截图。 ● **查看密钥对**章节，更新了入口截图。 ● **删除密钥对**章节，更新了入口截图，增加了相关描述。 ● **导入私钥**章节，更新了入口截图，增加了相关描述。 ● **导出私钥**章节，更新了入口截图，增加了相关描述。 ● **清除私钥**章节，更新了入口截图，增加了相关描述。
2020-07-14	第十五次正式发布。 ● 新增**导入密钥**章节。 ● **创建密钥**、**导入密钥**、**查看密钥**章节，新增企业多项目功能及其描述。
2020-04-07	第十四次正式发布。 更新界面截图。
2020-02-10	第十三次正式发布。 修改**权限管理**章节。
2019-08-09	第十二次正式发布。 根据界面变化更新**密钥管理**章节的截图。

版权所有 © 华为技术有限公司

发布日期	修改说明
2019-07-19	第十一次正式发布。 ● 新增激活专属加密实例章节。 ● 新增查看专属加密实例章节。
2019-07-12	第十次正式发布。 新增购买专属加密实例章节。
2019-07-04	第九次正式发布。 ● 在删除密钥中新增查看密钥使用记录的方法。 ● 根据界面变化更新密钥对管理章节的截图。 ● 新增使用专属加密实例章节。 ● 云审计服务支持的DEW操作列表中新增“购买云加密实例”、“实例化云加密实例”、“删除云加密实例”的资源类型和事件名称。
2019-04-22	第八次正式发布。 优化流程图和架构图。
2018-10-25	第七次正式发布。 修改查看密钥对章节，增加密钥对详情页面描述。
2018-08-30	第六次正式发布。 ● 新增专属加密章节。 ● 新增“用户业务系统使用专属加密实例加密”章节。 ● 新增使用专属加密实例章节。
2018-07-05	第五次正式发布。 ● 修改创建密钥章节，增加添加标签的操作步骤。 ● 根据界面变化更新截图。
2018-05-30	第四次正式发布。 ● 新增绑定密钥对章节。 ● 新增解绑密钥对章节。 ● 新增重置密钥对章节。 ● 新增替换密钥对章节。 ● 修改查看密钥对章节，增加“删除失败信息”的描述。 ● 修改查看密钥对章节，新增绑定密钥对的弹性云服务器列表说明。

版权所有 © 华为技术有限公司

发布日期	修改说明
2018-04-30	第三次正式发布。 ● 新增添加标签章节。 ● 新增“搜索标签”章节。 ● 新增修改标签值章节。 ● 新增删除标签章节。 ● 根据界面变化更新截图。
2018-01-30	第二次正式发布。 ● 新增“SSH密钥对”概念说明章节。 ● 新增创建密钥对章节。 ● 新增导入密钥对章节。 ● 新增查看密钥对章节。 ● 新增删除密钥对章节。
2017-12-31	第一次正式发布。

版权所有 © 华为技术有限公司