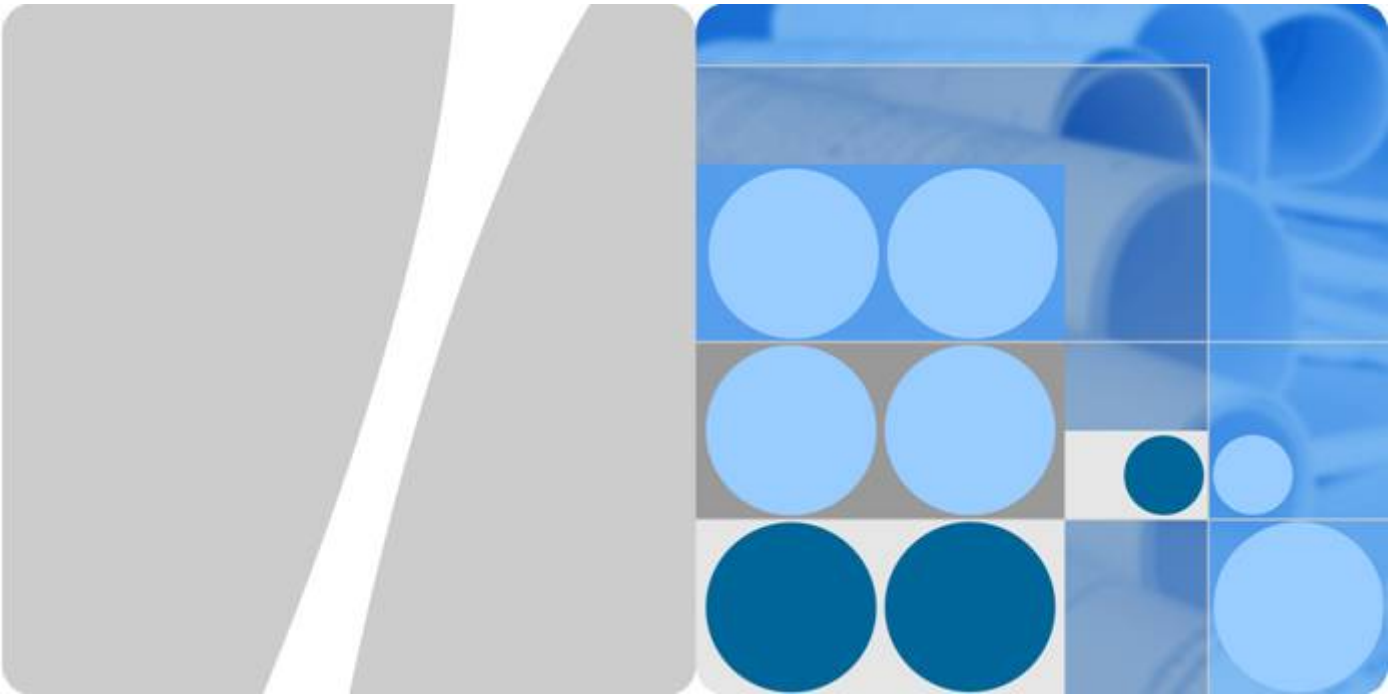


数据加密服务

用户指南

文档版本　16

发布日期　2018-07-05

华为技术有限公司

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://e.huawei.com

目 录

1 产品简介

1.1 数据加密服务

数据加密服务（Data Encryption Workshop）是一个综合的云上数据加密服务。它可以提供专属加密、密钥管理、密钥对管理等功能。其密钥由硬件安全模块（Hardware Security Module，HSM） 保护，并与许多华为云服务集成。用户也可以借此服务开发自己的加密应用。

- 密钥管理

  一种安全、可靠、简单易用的密钥托管服务，帮助用户集中管理密钥，保护密钥的安全。

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

- 密钥对管理

  一种安全、可靠、简单易用SSH密钥对托管服务，帮助用户集中管理SSH密钥对，保护SSH密钥对的安全。

  KPS是利用HSM产生的硬件真随机数来生成密钥对，并提供了一套完善和可靠的密钥对的管理方案，帮助用户轻松创建、导入和管理SSH密钥对。生成的SSH密钥对的公钥文件均保存在华为云中，私钥文件由用户自己下载保存在本地，从而保障了SSH密钥对的私有性和安全性。

- 专属加密

  专属加密服务为用户提供经国家密码管理局检测认证的专属加密实例，帮助用户保护弹性云服务器上数据的安全性和隐私性要求，满足监管合规要求。同时，用户能够对专属加密实例生成的密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。

1.2 密钥管理

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

KMS通过使用硬件安全模块HSM（Hardware Security Module）保护密钥安全，帮助用户轻松创建和管理密钥，所有的用户密钥都由HSM中的根密钥保护，避免密钥泄露。

KMS对密钥的所有操作都会进行访问控制及日志跟踪，提供所有密钥的使用记录，满足审计和合规性要求。

1.3 密钥对管理

密钥对管理，即密钥对管理服务（Key Pair Service），是一种安全、可靠、简单易用的SSH密钥对托管服务，帮助用户集中管理SSH密钥对，保护SSH密钥对的安全。

SSH密钥对，简称为密钥对，是为用户提供的远程登录Linux云服务器的认证方式，是一种区别于传统的用户名和密码登录的认证方式。

密钥对是通过加密算法生成的一对密钥，包含一个公钥和一个私钥，公钥自动保存在华为云中，私钥由用户保存在本地。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。

若用户将公钥配置在Linux云服务器中，则可以使用私钥登录Linux云服务器，而不需要输入密码。由于密钥对可以让用户无需输入密码登录到Linux云服务器，因此，可以防止由于密码被拦截、破解造成的帐户密码泄露，从而提高Linux云服务器的安全性。

1.4 专属加密

专属加密（Dedicated Hardware Security Module，Dedicated HSM）是华为云为用户提供的云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。

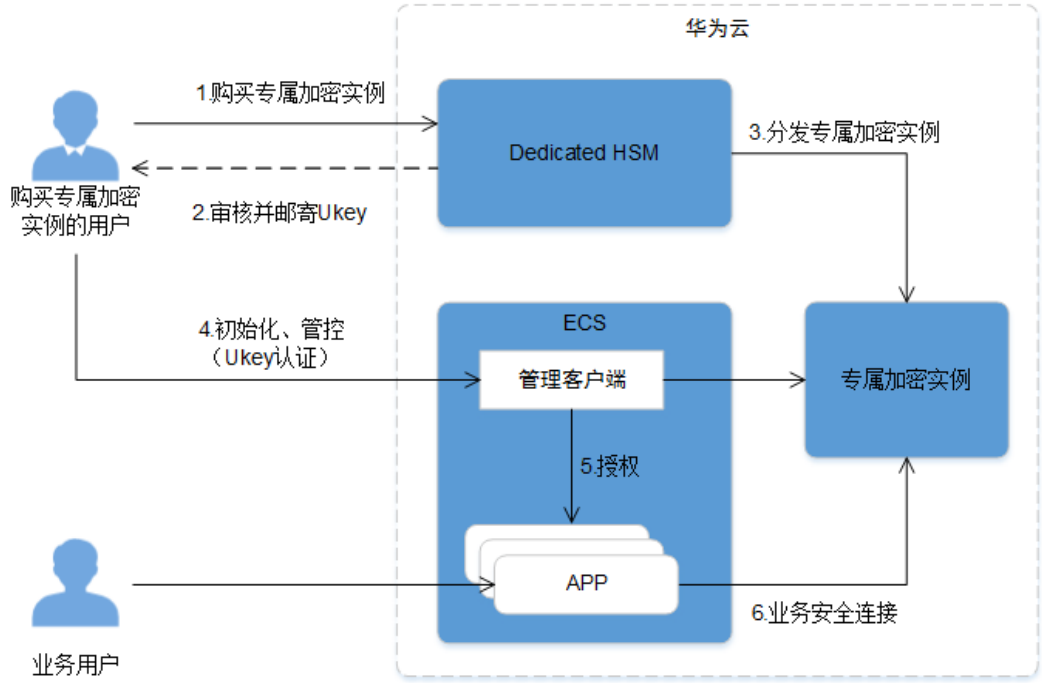
Dedicated HSM旨在满足用户将线下加密设备能力转移到云上的要求，提供可独占、高性能、安全合规的加密域计算资源。用户作为设备使用者完全控制密钥的产生、存储和访问授权。华为云只负责监控和管理设备及其相关网络设施。

同时，Dedicated HSM可提供认证合规的金融数据加密机、服务器加密机以及签名验签服务器等，灵活支撑用户业务场景。能够帮助用户满足数据安全方面的监管要求，以及云上业务数据的隐私性要求。

业务流程

当用户需要在云上使用专属加密服务时，可通过Dedicated HSM购买专属加密实例，并初始化专属加密实例，授权业务APP访问专属加密实例。业务流程如**图1-1**所示。

图 1-1 业务流程



业务流程说明如表1-1所示。

表 1-1 业务流程说明

编号	说明
1	用户通过Dedicated HSM购买专属加密实例，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。
2	Ukey是华为云提供给用户的身份识别卡，此卡仅购买专属加密实例的用户持有，请妥善保管。 华为云安全专家将通过您提供的联系方式与您联系，并确定您订购的专属加密实例是否满足您的业务要求，若满足要求，华为云安全专家将通过用户提供的Ukey收件地址将Ukey邮寄给用户。
3	用户付款后，华为云分配专属加密实例给用户。
4	用户使用Ukey和安全管理客户端初始化专属加密实例，并注册相应的管理员。
5	注册的管理员需要通过管理客户端授予业务APP访问专属加密实例的权限。
6	用户通过调用SDK与专属加密实例建立安全连接，并访问专属加密实例。

功能介绍

Dedicated HSM提供以下功能：

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

支持的密码算法

对称密码算法	SM1、SM4、DES、3DES、AES
非对称密码算法	SM2、 RSA（1024-2048）
摘要算法	SM3、 SHA1、SHA256、SHA384

权限认证

- 专属加密实例设备管理与内容（敏感信息）管理权限分离，即使华为云的运维人员也无法获取到用户的密钥。
- 可对敏感指令支持分类授权控制，有效防止越权行为。
- 支持用户名口令认证，数字证书认证等多种权限认证方式。

可靠性

专属加密实例之间独享加密芯片，即使部分硬件芯片损坏也不影响使用。

1.5 区域和可用分区

区域指DEW所在的物理位置。

同一区域内可用分区间内网互通，不同区域间内网不互通。

华为云在中国不同地区有数据中心。与此相应，华为云DEW可用于不同地区。通过在不同地区开启DEW服务，可以将应用程序设计的更接近特定客户的要求，或满足不同地区的法律或其他要求。

每个区域包含许多不同的称为“可用分区”的位置，即在同一区域下，电力、网络隔离的物理区域，可用分区之间内网互通，不同可用分区之间物理隔离。每个可用分区都被设计成不受其他可用分区故障的影响，并提供低价、低延迟的网络连接，以连接到同一地区其他可用分区。通过使用独立可用分区内的DEW，可以保护您的应用程序不受单一位置故障的影响。

1.6 项目

项目用于将OpenStack的资源（计算资源、存储资源和网络资源）进行分组和隔离。项目可以是一个部门或者一个项目组。

一个帐户中可以创建多个项目。

1.7 功能介绍

密钥管理

- 基础版

  用户可通过密钥管理界面，对用户主密钥进行以下操作：
  - 创建、查看、启用、禁用、计划删除、取消删除用户主密钥
  - 修改用户主密钥的别名和描述
  - 在线工具加解密小数据
  - 添加、搜索、编辑、删除标签
- 专业版
  - 用户可通过密钥管理界面或接口，对用户主密钥进行以下操作：
    - 包含基础版所有功能
    - 开启、修改、关闭密钥管理轮换周期
    - 创建、撤销、查询授权
  - 用户可通过密钥管理的接口执行以下操作：
    - 对数据加密密钥进行创建、加密或解密操作
    - 对授予的权限进行退役授权操作

    具体请参见《数据加密服务API参考》。
  - 生成硬件真随机数

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

密钥对管理

用户可通过密钥对管理界面或接口，对密钥对进行以下操作：

- 创建、导入、查看、删除密钥对
- 重置、替换、绑定、解绑密钥对
- 托管、导入、导出、清除私钥

专属加密

用户可通过专属加密界面，购买专属加密实例和查看专属加密实例信息。

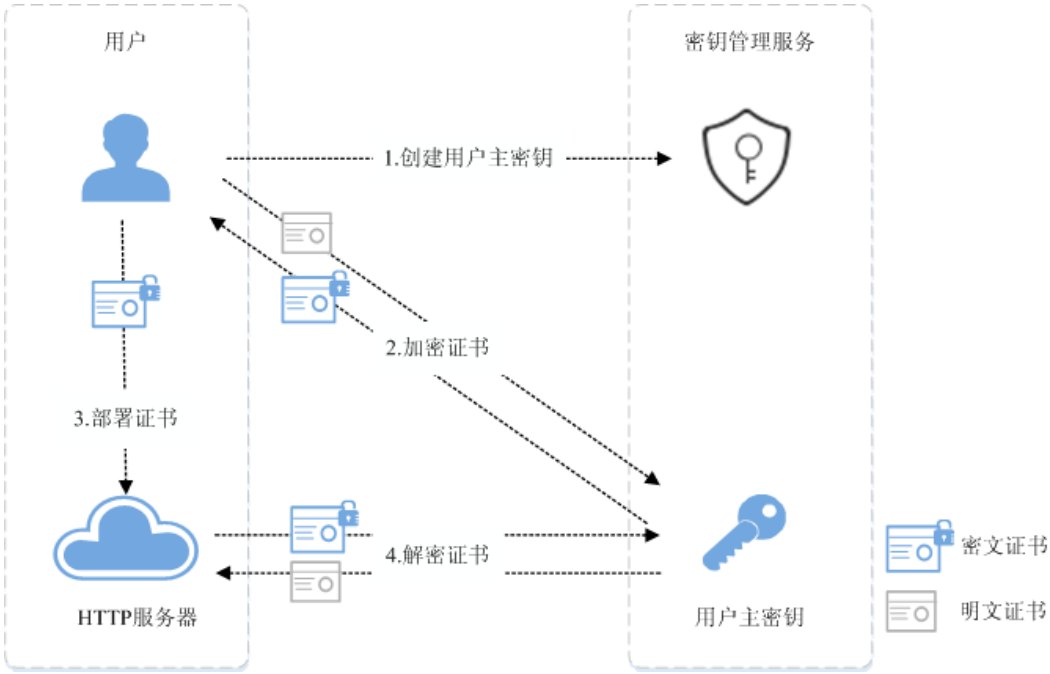
1.8 使用场景

1.8.1 小数据加密

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

以保护服务器HTTPS证书为例，采用调用KMS的API接口方式进行说明，如**图1-2**所示。

图 1-2 保护服务器 HTTPS 证书



流程说明如下：

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

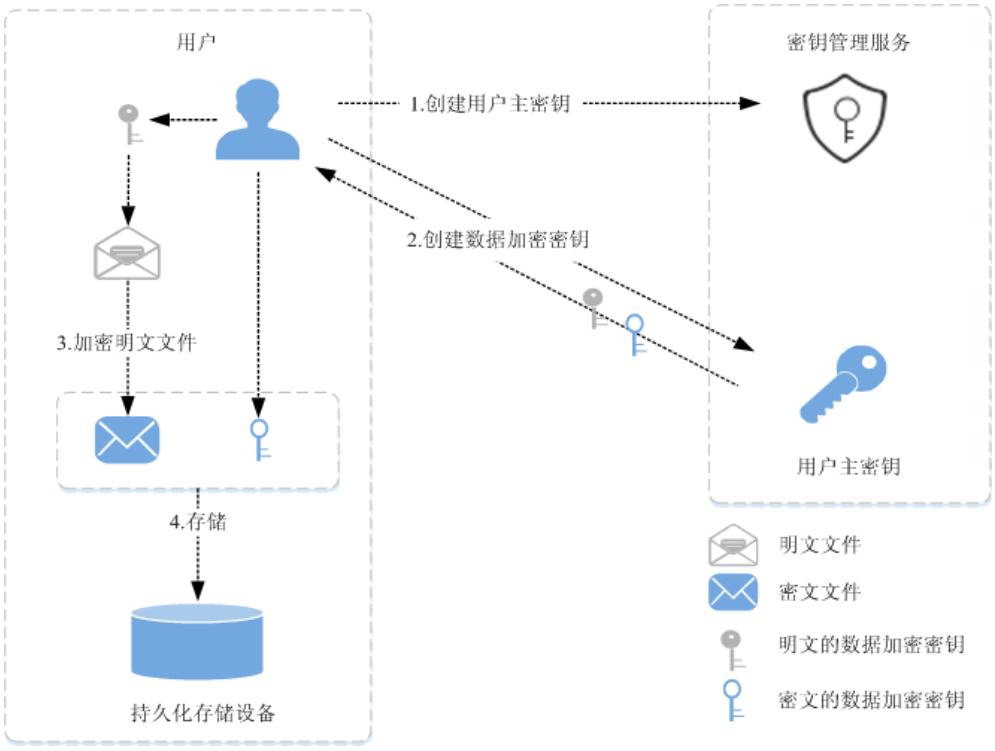
1.8.2 大量数据加密

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

加密本地文件

加密本地文件流程，如图1-3所示。

图 1-3 加密本地文件



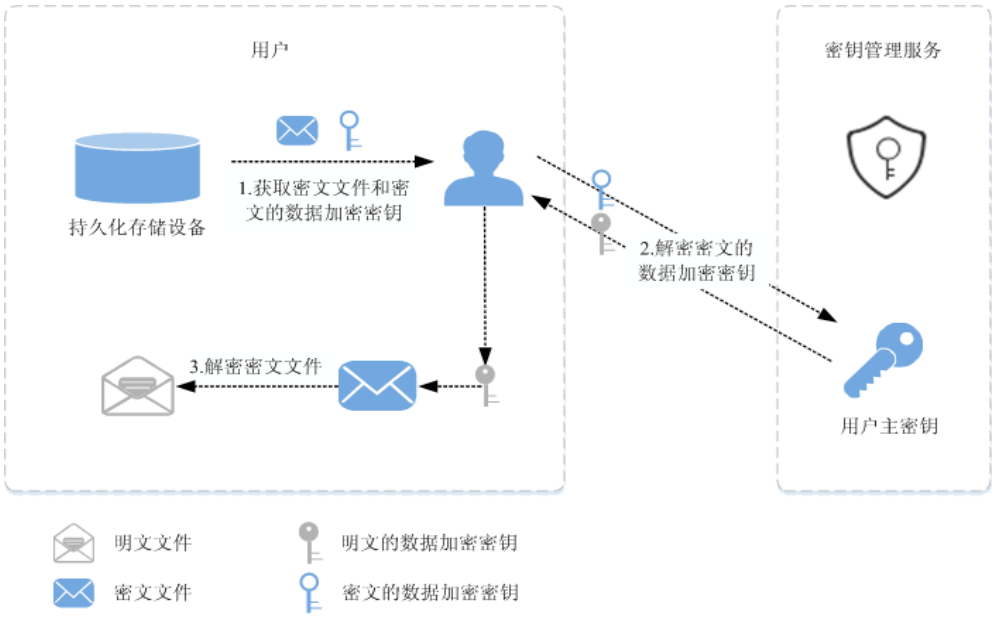
流程说明如下：

1. 用户需要在KMS中创建一个用户主密钥。
2. 用户调用KMS的“create-datakey”接口创建数据加密密钥。用户得到一个明文的数据加密密钥和一个密文的数据加密密钥。其中密文的数据加密密钥是由指定的用户主密钥加密明文的数据加密密钥生成的。
3. 用户使用明文的数据加密密钥来加密明文文件，生成密文文件。
4. 用户将密文的数据加密密钥和密文文件一同存储到持久化存储设备或服务中。

解密本地文件

解密本地文件流程，如图1-4所示。

图 1-4 解密本地文件



流程说明如下：

1. 用户从持久化存储设备或服务中读取密文的数据加密密钥和密文文件。
2. 用户调用KMS的“decrypt-datakey”接口，使用对应的用户主密钥（即生成密文的数据加密密钥时所使用的用户主密钥）来解密密文的数据加密密钥，取得明文的数据加密密钥。

   若对应的用户主密钥被误删除，会导致解密失败。因此，需要妥善管理好用户主密钥。
3. 用户使用明文的数据加密密钥来解密密文文件。

1.8.3 OBS 服务端加密

- 用户使用OBS（Object Storage Service，OBS）服务端加密方式上传文件时，可以选择“KMS 加密”，从而使用KMS提供的密钥来加密上传的文件，如图1-5所示。更多信息请参见《对象存储服务控制台指南》。

图 1-5 OBS 服务端加密

可供选择的用户主密钥包含以下两种：

- KMS为使用OBS的用户创建一个默认主密钥“obs/default”。
- 用户通过KMS界面创建的非默认主密钥。

- 用户也可以通过调用OBS API接口，选择服务端加密SSE-KMS方式（SSE-KMS方式是指OBS使用KMS提供的密钥进行服务端加密）上传文件，详情请参考《对象存储服务API参考》。

1.8.4 EVS 服务端加密

- 用户购买磁盘时，可以选择“磁盘加密”，使用KMS提供的密钥来加密磁盘上的数据，如图1-6所示。更多信息请参见《云硬盘用户指南》。

  说明

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

图 1-6 EVS 服务端加密

可供选择的用户主密钥包含以下两种：

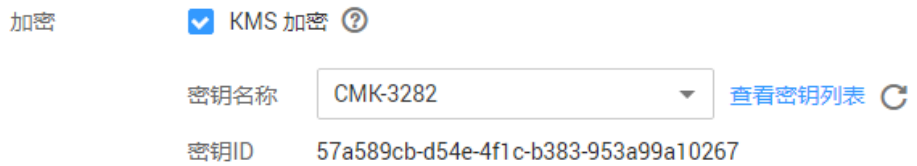
- KMS为使用EVS（Elastic Volume Service，EVS）的用户创建一个默认主密钥“evs/default”。
- 用户通过KMS界面创建的非默认主密钥。

- 用户也可以通过调用EVS API接口购买加密磁盘，详情请参考《云硬盘API参考》。

1.8.5 IMS 服务端加密

- 用户上传镜像文件时，可以选择“KMS加密”，使用KMS提供的密钥来加密上传的文件，如图1-7所示，更多信息请参见《镜像服务用户指南》。

图 1-7 IMS 服务端加密



可供选择的用户主密钥包含以下两种：

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

- 用户通过KMS界面创建的非默认主密钥。

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

1.8.6 RDS 服务端加密

- 用户购买数据库实例（Relational Database Service，RDS）时，可以选择“磁盘加密”，使用KMS提供的密钥来加密数据库实例的磁盘，更多信息请参见《关系型数据库用户指南》。

  可供选择的用户主密钥需要用户通过KMS界面购买专业版密钥管理，并在专业版密钥管理中创建用户主密钥，如图1-8所示。

  图 1-8 RDS 服务端加密

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

1.8.7 登录 Linux 操作系统的弹性云服务器

若用户购买的是Linux操作系统的弹性云服务器，可以选择“密钥对方式”登录，详细信息请参见《弹性云服务器用户指南》

购买弹性云服务器时，可供选择的密钥对包含以下两种：

- 用户通过云服务器控制台界面创建或者导入密钥对。
- 用户通过KPS界面创建或者导入密钥对。

1.8.8 获取 Windows 操作系统弹性云服务器的登录密码

若用户购买的是Windows操作系统的弹性云服务器，需要使用密钥对的私钥获取登录密码，详细信息请参见《弹性云服务器用户指南》。

购买弹性云服务器时，可供选择的密钥对包含以下两种：

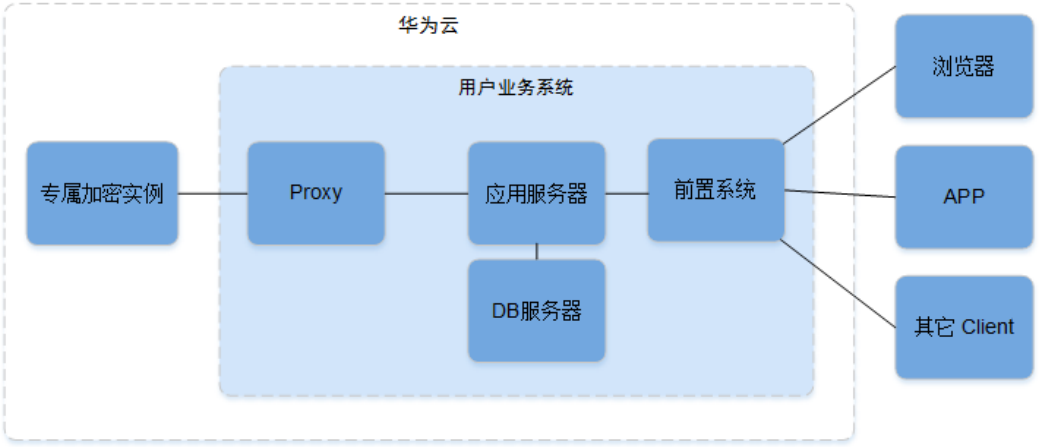
- 用户通过云服务器控制台界面创建或者导入密钥对。
- 用户通过KPS界面创建或者导入密钥对。

1.8.9 用户业务系统使用专属加密实例加密

若用户购买了华为云提供的专属加密实例，可通过华为云提供Ukey初始化并管控专属加密实例。用户作为设备使用者完全控制密钥的产生、存储和访问授权。用户可通过专属加密实例加密用户业务系统（包含敏感数据加密、金融支付加密以及电子票据加密），帮助用户加密企业自身的敏感数据（如合同、交易、流水等）以及企业用户的敏感数据（用户身份证号码、手机号码等），以防止黑客攻破网络、拖库导致数据泄露、内部用户非法访问或篡改数据等风险。

以敏感数据加密场景为例说明，如图1-9所示。

图 1-9 敏感数据加密场景



1.9 访问与使用

1.9.1 如何访问

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

- 管理控制台方式

  如果用户已注册公有云，可直接登录管理控制台，单击管理控制台左上角的，选择区域或项目后，单击页面上方的“服务列表”，选择“安全 > 数据加密服务”。

- API方式

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

1.9.2 如何使用

与对象存储服务配合使用

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

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

与云硬盘配合使用

在购买云硬盘时，用户启用云硬盘的加密功能，选择KMS提供的用户主密钥对云硬盘进行加密，则在使用该云硬盘时，存储到云硬盘的数据将会自动加密。

用户如何使用云硬盘加密功能，具体操作请参见《云硬盘用户指南》。

与镜像服务配合使用

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

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

与关系型数据库配合使用

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

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

与弹性云服务器配合使用

用户在购买弹性云服务器（Elastic Cloud Server，简称ECS）时，选择KPS提供的SSH密钥对对登录弹性云服务器的用户进行身份认证，或者通过提供的密钥对获取Windows操作系统弹性云服务器的登录密码。

用户如何通过SSH密钥对登录弹性云服务器，或者获取Windows操作系统弹性云服务器的登录密钥，具体操作请参见《弹性云服务器用户指南》。

用户可通过购买专属加密实例的方式，使用专属加密实例生成的密钥加解密部署在弹性云服务器内业务系统的敏感数据。

与用户的应用程序配合使用

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

1.9.3 与其他云服务的关系

与对象存储服务的关系

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

与云硬盘的关系

KMS为云硬盘提供用户主密钥管理控制能力，应用于云硬盘的加密功能。

与镜像服务的关系

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

与关系型数据库的关系

KMS为关系型数据库提供用户主密钥管理控制能力，应用于关系型数据库的磁盘加密功能。

与弹性云服务器的关系

KPS为弹性云服务器提供密钥对的管理控制能力，应用于用户登录弹性云服务器时，对用户身份认证的功能。

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

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录数据加密服务相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务用户指南》。

与统一身份认证服务的关系

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

需要拥有KMS Administrator权限的用户才能使用DEW服务。

需要拥有Server Administrator权限的用户才能使用密钥对功能。

如需开通该权限，请联系拥有Security Administrator权限的用户，详细内容请参考《统一身份认证服务用户指南》。

1.9.4 用户权限

系统默认提供两种权限：用户管理权限和资源管理权限。用户管理权限可以管理用户、用户组及用户组的权限。资源管理权限可以控制用户对云服务资源执行的操作。

数据加密服务的用户权限请参见**权限说明**。

2 审计

2.1 云审计服务支持的 DEW 操作列表

云审计服务记录数据加密服务相关的操作事件，如表2-1所示。

表 2-1 云审计服务支持的 DEW 操作列表

操作名称	资源类型	事件名称
创建密钥	cmk	createKey
创建数据密钥	cmk	createDataKey
创建不含明文数据密钥	cmk	createDataKeyWithoutPlaintext
启用密钥	cmk	enableKey
禁用密钥	cmk	disableKey
加密数据密钥	cmk	encryptDataKey
解密数据密钥	cmk	decryptDataKey
计划删除密钥	cmk	scheduleKeyDeletion
取消计划删除密钥	cmk	cancelKeyDeletion
创建随机数	rng	genRandom
修改密钥别名	cmk	updateKeyAlias
修改密钥描述	cmk	updateKeyDescription
密钥删除风险提示	cmk	deleteKeyRiskTips
创建授权	cmk	createGrant
退役授权	cmk	retireGrant
撤销授权	cmk	revokeGrant

操作名称	资源类型	事件名称
加密数据	cmk	encryptData
解密数据	cmk	decryptData
添加标签	cmk	createKeyTag
删除标签	cmk	deleteKeyTag
批量添加标签	cmk	batchCreateKeyTags
批量删除标签	cmk	batchDeleteKeyTags
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

2.2 查看审计日志

开启了云审计服务后，系统开始记录数据加密服务相关的操作。云审计服务管理控制台保存最近7天的操作记录。

查看 DEW 的云审计日志

步骤1 登录管理控制台。

步骤2 单击页面上方的“服务列表”，选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 单击事件列表右上方的“筛选”，设置对应的操作事件条件。

当前事件列表支持四个维度的组合查询，详细信息如下：

- “事件来源”、“资源类型”和“筛选类型”。
  - 在下拉框中选择查询条件。其中，“事件来源”选择“KMS”。
  - 筛选类型选择事件名称时，还需选择某个具体的事件名称。
  - 选择资源ID时，还需选择或者手动输入某个具体的资源ID。
  - 选择资源名称时，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。
- “起始时间”、“结束时间”：可通过选择时间段查询操作事件。

步骤5 单击“查询”，查看对应的操作事件。

步骤6 在需要查看的记录左侧，单击 展开该记录的详细信息，展开记录如图2-1所示。

图 2-1 展开记录

步骤7 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如图2-2所示，显示了该操作事件结构的详细信息。

图 2-2 查看事件

----结束

3 密钥管理

3.1 开启密钥管理

密钥管理为用户提供密钥创建与管理功能，密钥安全由硬件安全模块（HSM）保护。

该任务指导用户通过密钥管理界面开启密钥管理。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已购买密钥管理，且密钥管理处于“关闭”状态。

开启密钥管理

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行的“开启”，弹出“启用密钥管理”对话框。

步骤5 单击“确定”，在页面右上角弹出“开启密钥管理成功”，则说明密钥管理开启完成。

说明

当用户不需要使用密钥管理时，可单击目标密钥管理所在行的“关闭”，关闭密钥管理。关闭密钥管理后，密钥管理下的所有密钥及密钥功能均不能使用。

----结束

3.2 创建密钥

该任务指导用户通过密钥管理界面创建用户主密钥。

- 基础版的密钥管理中最多可创建或导入2个用户主密钥，不包含默认主密钥。

- 专业版的密钥管理中最多可创建或导入20个用户主密钥。

用户主密钥可用于如下场景：

- 对象存储服务中对象的服务端加密
- 云硬盘中数据的加密
- 私有镜像的加密
- 关系型数据库中数据库实例的磁盘加密
- 用户主密钥直接加解密小数据
- 用户应用程序的DEK加解密

说明

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

前提条件

已获取管理控制台的登录帐号与密码。

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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行的“创建密钥”。

步骤5 在弹出的“创建密钥”对话框中，填写密钥的“别名”与“描述”。

图 3-1 创建密钥

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

说明

- 当用户在创建密钥时，没有为该用户主密钥添加标签。若用户需要为该用户主密钥添加标签，可单击该用户主密钥的别名，进入密钥详情页面，为该用户主密钥添加标签。
- 同一个用户主密钥下，一个标签键只能对应一个标签值；不同的用户主密钥下可以使用相同的标签键。
- 用户最多可以给单个用户主密钥添加10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“密钥任务创建成功”，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。
- 关系型数据库中数据库实例的磁盘加密方法，具体请参见《关系型数据库快速入门》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。

3.3 导入密钥

3.3.1 概述

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

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

注意事项

- 安全性

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

- 可用性与持久性

  在将密钥材料导入KMS之前，用户需要确保密钥材料的可用性和持久性。

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

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

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

- 关联性

  当用户将密钥材料导入用户主密钥时，该用户主密钥与该密钥材料永久关联，不能将其他密钥材料导入该用户主密钥中。

- 唯一性

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

3.3.2 导入密钥材料

操作场景

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

该任务指导用户通过密钥管理界面导入密钥材料。

说明

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

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已准备好待导入的密钥材料。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行的“导入密钥”，弹出“导入密钥”对话框。

步骤5 在弹出的对话框中填写密钥的“别名”和“描述”信息。

图 3-2 创建密钥

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

说明

- 当用户在创建密钥时，没有为该用户主密钥添加标签。若用户需要为该用户主密钥添加标签，可单击该用户主密钥的别名，进入密钥详情页面，为该用户主密钥添加标签。
- 同一个用户主密钥下，一个标签键只能对应一个标签值；不同的用户主密钥下可以使用相同的标签键。
- 用户最多可以给单个用户主密钥添加10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用户主密钥。

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3-2选择密钥包装算法。

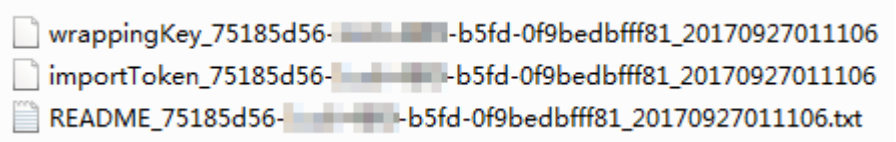
图 3-3 获取包装密钥和导入令牌

表 3-2 密钥包装算法说明

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

步骤10 单击“下载”，下载的文件包含包装密钥、导入令牌和说明文件，如图3-4所示。

图 3-4 下载文件



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

注意

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

同时，用户也可以通过调用API接口的方式获取包装密钥和导入令牌。

1. 调用“get-parameters-for-import”接口，获取包装密钥和导入令牌。

   如下以获取密钥ID为“43f1ffd7-18fb-4568-9575-602e009b7ee8”，加密算法为“RSAES_PKCS1_V1_5”的包装密钥和导入令牌为例。

   “public_key”：调用API接口返回的base64编码的包装密钥内容。

   “import_token”：调用API接口返回的base64编码的导入令牌内容。

   - 请求样例

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

   - 响应样例

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

2. 保存包装密钥，包装密钥需要按照以下步骤转换格式。使用转换格式后的包装密钥进行加密的密钥材料才能成功导入管理控制台。

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

   b. 使用OpenSSL，执行以下命令，对“PublicKey.b64”文件内容进行base64转码，生成二进制数据，并将转码后的文件保存为“PublicKey.bin”。

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

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

步骤11 使用下载的“包装密钥”对待导入的密钥材料进行加密。

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

  说明

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

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

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

     openssl rand -out *PlaintextKeyMaterial.bin* 32

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

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

- 若下载的是“RSAES_OAEP_SHA_256”算法的包装密钥，请执行以下命令，加密生成的密钥材料。

  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

- 若下载的是“RSAES_PKCS1_V1_5”算法的包装密钥，请执行以下命令，加密生成的密钥材料。

  openssl rsautl -encrypt

  -in *PlaintextKeyMaterial.bin*

  -pkcs

  -inkey *PublicKey.bin*

  -keyform der

  -pubin

  -out *EncryptedKeyMaterial.bin*

- 若下载的是“RSAES_OAEP_SHA_1”算法的包装密钥，请执行以下命令，加密生成的密钥材料。

  openssl pkeyutl

  -in *PlaintextKeyMaterial.bin*

  -inkey *PublicKey.bin*

  -out *EncryptedKeyMaterial.bin*

  -keyform der

  -pubin -encrypt

  -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha1

步骤12 单击“下一步”，进入“导入密钥材料”页面。根据表3-3配置参数。

图 3-5 导入密钥材料

表 3-3 导入密钥材料参数说明

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

步骤13 单击“下一步”，进入“导入密钥令牌”页面。根据表3-4设置参数。

图 3-6 导入密钥令牌

表 3-4 导入密钥令牌参数说明

参数	操作说明
密钥ID	创建密钥时，随机生成的密钥ID。
密钥导入令牌	选择步骤10中“下载”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，密钥管理服务会在24小时内自动删除密钥材料，删除后密钥将无法使用，且密钥状态变更为“等待导入”。

步骤14 单击“确定”，页面右上角弹出“密钥导入成功”，则说明导入密钥成功。

注意

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

3.3.3 删除密钥材料

操作场景

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

该任务指导用户通过密钥管理界面对外部导入的密钥材料进行删除操作。

说明

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

前提条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 在需要删除的密钥材料所在行，单击“删除密钥材料”。

步骤6 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

3.4 在线工具加解密小数据

该任务指导用户通过密钥管理界面使用在线工具加解密不大于4KB的数据。

说明

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

前提条件

- 已获取管理控制台的登录帐号与密码。
- 用户主密钥处于“启用”状态。

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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 单击目标用户主密钥的别名，进入密钥详细信息在线工具加密数据页面。

步骤6 在“加密”文本框中输入待加密的数据，如图3-7所示。

图 3-7 加密数据

步骤7 单击“执行”，右侧文本框显示加密后的密文数据。

说明

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

----结束

解密数据

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 解密数据时，可单击任意“启用”状态的非默认主密钥别名，进入该密钥的在线工具页面。

步骤6 单击“解密”，在左侧文本框中数据待解密的密文数据，如图3-8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。
- 若该密钥已被删除，会导致解密失败。

图 3-8 解密数据

步骤7 单击“执行”，右侧文本框中显示解密后的明文数据。

说明

用户可直接单击“复制到剪切板”拷贝解密后的明文数据，并保存到本地文件中。

----结束

3.5 轮换密钥

操作场景

该任务指导用户通过密钥管理界面开启密钥轮换。

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，用户需要为用户主密钥创建新的密钥材料。

用户可以通过以下两种方式创建新的密钥材料：

- 创建新的用户主密钥。
- 为现有的用户主密钥开启密钥轮换，KMS自动为用户主密钥生成新的密钥材料。

  密钥轮换只会更改用户主密钥的密钥材料，用户主密钥的属性（密钥ID、别名、描述、权限）不会发生变化。

开启密钥轮换后，密钥管理服务会根据设置的轮换周期（默认365天）自动轮换密钥，每次轮换都会生成一个新版本的用户主密钥，轮换的密钥加解密数据的方式如下所示：

- 加密数据时，KMS会自动使用当前最新版本的用户主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用户主密钥来执行解密操作。

密钥管理服务会保留与该用户主密钥关联的所有版本的用户主密钥。这使得KMS可以解密使用该用户主密钥加密的任何密文。

说明

默认主密钥和导入的密钥不支持密钥轮换。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 密钥处于“启用”状态。
- “密钥材料来源”为“密钥管理”。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 单击目标用户主密钥的别名，进入密钥详细信息页面。

步骤6 单击“密钥轮换”，进入密钥轮换管理界面，如图3-9所示。

图 3-9 密钥轮换

步骤7 单击  ，将“密钥轮换”设置为  ，如图3-10所示。参数说明如表3-5所示。

图 3-10 开启密钥轮换

表 3-5 用户主密钥轮换参数说明

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** 如果用户主密钥开启密钥轮换以后，禁用了用户主密钥，KMS也不会轮换该用户主密钥。 当用户主密钥恢复到“启用”状态时，密钥轮换将立即重新激活。如果刚恢复“启用”状态的用户主密钥距离上次轮换的时间已超过轮换周期，KMS将在24小时内轮换该用户主密钥。
轮换周期（天）	轮换周期。取值范围为“30~365”的整数，默认“365”天。 轮换周期需要根据用户主密钥的使用频率进行设置，若密钥使用频率高，建议设置为短周期；反之，则设置为长周期。

步骤8 单击“开启轮换”，页面显示密钥轮换详情，如图3-11所示。

图 3-11 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

3.6 管理授权

3.6.1 创建授权

操作场景

用户可以为其他用户创建授权，授予其使用自身的用户主密钥（CMK）的权限，一个用户主密钥下最多可创建100个授权。

用户主密钥的所有者可通过KMS界面或者调用API接口的方式为用户主密钥创建授权；被用户主密钥所有者授予了“创建授权”操作权限的用户仅能通过调用API接口的方式为用户主密钥创建授权。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已获取被授权用户的ID。
- 用户主密钥需处于“启用”状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

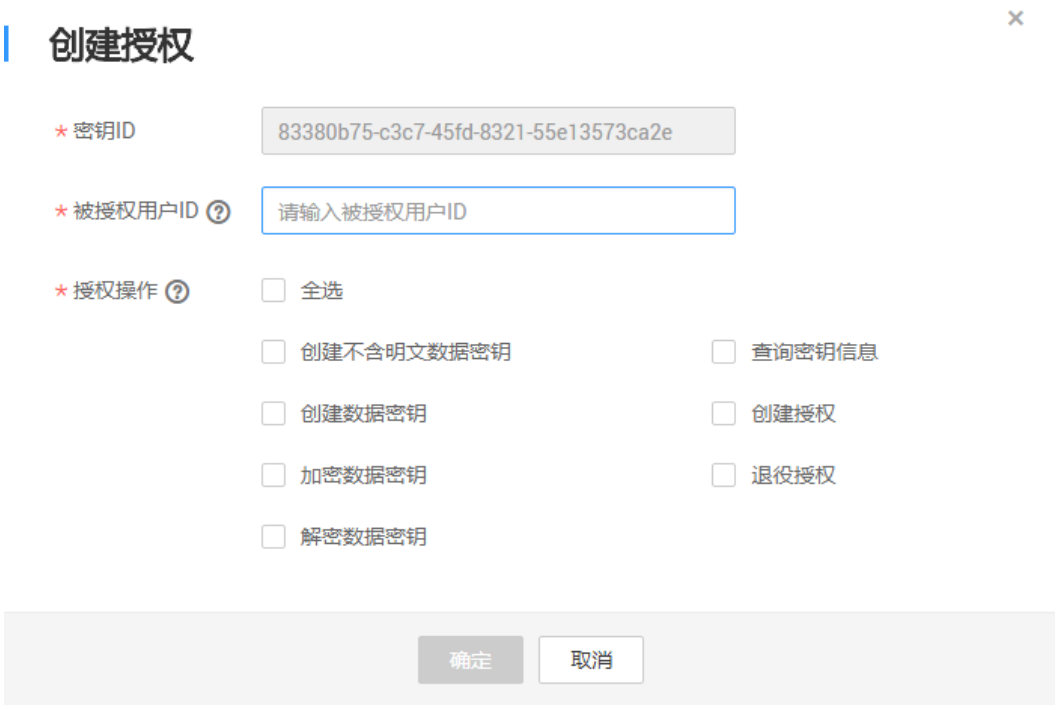
步骤5 单击目标用户主密钥的别名，进入密钥详细信息授权页面。

步骤6 单击“授权”，进入授权管理界面，如图3-12所示。

图 3-12 授权页面

步骤7 单击“创建授权”，弹出“创建授权”对话框。

图 3-13 创建授权



步骤8 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。

注意

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 3-6 创建授权参数说明

参数	参数说明	配置样例
密钥ID	自动读取用户主密钥的ID。	-
被授权用户ID	用户需要输入被授权用户的ID。 **说明** 被授权用户可在“用户名 > 我的凭证 > 用户ID”中查看并获取用户ID。	d9a6b2bdaedd4ba586cabe6372d1b312
授权操作	用户可选择以下授权操作： **说明** ● 一个用户主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用户主密钥的操作权限时，被授权用户可退役该授权。 – 如果被授权用户在退役授权前，已将用户主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，对其他用户操作用户主密钥的权限无影响。	-

步骤9 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ID”、“被授权用户ID”、“授权操作”和“创建时间”。

----结束

3.6.2 查询授权

操作场景

该任务指导用户通过密钥管理界面查看用户主密钥的授权信息，包括授权ID、被授权用户ID、授权操作、创建时间。

前提条件

- 已获取管理控制台的登录帐号与密码。

- 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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 单击目标用户主密钥的别名，进入密钥详细信息页面。

步骤6 用户可查看当前用户主密钥的授权信息，如图3-14所示。

图 3-14 查询授权

授权ID	被授权用户ID	授权操作	创建时间	操作
d7b6f90d20dca8d402bc7084...	[redacted]	创建授权/退役授权	2018/05/22 11:56:06 GMT+08:00	撤销授权
c55578c047852a68feafc865...	[redacted]	加密数据密钥/查询密钥信息	2018/05/22 11:55:27 GMT+08:00	撤销授权
aabc64758599399705e0b96...	[redacted]	创建不含明文数据密钥/创建授权	2018/05/22 11:55:14 GMT+08:00	撤销授权

用户主密钥的授权信息如表3-7所示。

表 3-7 授权信息参数说明

参数	参数说明
授权ID	随机生成的授权的唯一标识。
授权用户ID	被授权用户的ID。
授权操作	被授予用户对用户主密钥的操作权限（例如：创建数据密钥）。
创建时间	创建该授权的时间。

步骤7 单击“授权ID”，可以查看授权详情，如图3-15所示。

图 3-15 授权详情

----结束

3.6.3 撤销授权

操作场景

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用户主密钥时，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。
- 当授权用户想收回用户主密钥的操作权限时，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密钥管理界面撤销授权。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 单击目标用户主密钥的别名，进入密钥详细信息页面。

步骤6 在待撤销操作权限的授权用户ID所在行的“操作列”，单击“撤销授权”。

步骤7 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

3.7 管理标签

3.7.1 添加标签

标签用于标识密钥管理或用户主密钥。为密钥管理或用户主密钥添加标签，可以方便用户对密钥管理或用户主密钥进行分类和跟踪，并按标签汇总密钥管理或用户主密钥的使用情况。

注意

KMS不支持为默认主密钥添加标签。

前提条件

已获取管理控制台的登录帐号与密码。

添加标签

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 单击目标用户主密钥的别名，进入密钥详细信息页面。

说明

若用户需要为密钥管理添加标签，可直接单击密钥管理的名称，进入密钥管理详细信息页面，单击“添加标签”，添加标签。

步骤6 单击“标签”，进入标签管理页面，如图3-16所示。

图 3-16 标签页面

步骤7 单击“添加标签”，弹出添加标签对话框，如图3-17所示。

图 3-17 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。

步骤8 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3-8所示。

表 3-8 标签参数说明

参数	参数说明	取值要求	样例
标签键	标签的名称。 同一个用户主密钥下，一个标签键只能对应一个标签值；不同的用户主密钥下可以使用相同的标签键。 用户最多可以给单个用户主密钥添加10个标签。	● 必填。 ● 对于同一个用户主密钥，标签键唯一。 ● 长度不超过36个字符。 ● 只能包含以下4种字符： – 大写字母 – 小写字母 – 数字 – 特殊字符，包括“-”和“_”	cost
标签值	标签的值。	● 可以为空。 ● 长度不超过43个字符。 ● 只能包含以下4种字符： – 大写字母 – 小写字母 – 数字 – 特殊字符，包括“-”和“_”	100

步骤9 单击“确定”，完成标签的添加。

----结束

3.7.2 搜索标签

该任务指导用户通过密钥管理界面搜索标签，可搜索当前项目下满足标签搜索条件的所有的密钥管理或用户主密钥。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已添加标签。

搜索标签

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 单击“标签搜索”，展开搜索框，如图3-18所示。

图 3-18 标签搜索框

步骤6 在“密钥管理”下拉列表中，选择“密钥管理”或者“密钥”。

说明

- 如果选择的是“密钥管理”，那么可搜索出满足标签搜索条件的所有的密钥管理。
- 如果选择的是“密钥”，那么可搜索出满足标签搜索条件的所有的用户主密钥。

步骤7 在搜索框中输入“标签键”和“标签值”。

步骤8 单击 ，添加到搜索条件中，并单击“搜索”，显示满足搜索条件的用户主密钥列表，以搜索“密钥”的标签为例，如图3-19所示。

图 3-19 搜索结果

说明

- 可添加多个标签进行组合搜索，最多支持10个不同标签的组合搜索，若进行多个标签组合搜索，则搜索结果的每个用户主密钥均满足标签组合搜索条件。
- 若需要在搜索条件中删除添加的标签，可在搜索条件中单击指定标签后的，删除添加的标签。
- 若需要重新添加搜索条件，可单击“重置”，重新添加搜索条件。

----结束

3.7.3 修改标签值

该任务指导用户通过密钥管理界面修改标签值。

前提条件

已获取管理控制台的登录帐号与密码。

修改标签值

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行，展开密钥管理。

步骤5 单击目标用户主密钥的别名，进入密钥详细信息页面。

说明

若用户需要修改密钥管理的标签值，可直接单击目标密钥管理的名称，进入密钥管理详细信息页面，单击目标标签所在行的“编辑”，修改标签值。

步骤6 单击“标签”，进入标签管理页面，如图3-20所示。

图 3-20 标签页面

步骤7 单击目标标签所在行的“编辑”，弹出编辑标签对话框，如图3-21所示。

图 3-21 编辑标签

步骤8 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

3.7.4 删除标签

该任务指导用户通过密钥管理界面删除标签。

前提条件

已获取管理控制台的登录帐号与密码。

删除标签

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 单击目标用户主密钥的别名，进入密钥详细信息页面。

说明

若用户需要删除密钥管理的标签，可直接单击密钥管理的名称，进入密钥管理详细信息页面，单击目标标签所在行的“删除”，删除标签。

步骤6 单击“标签”，进入标签管理页面，如图3-22所示。

图 3-22 标签页面

步骤7 单击目标标签所在行的“删除”，弹出删除标签对话框。

步骤8 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

3.8 管理密钥

3.8.1 查看密钥

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

前提条件

已获取管理控制台的登录帐号与密码。

查看密钥

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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行，展开密钥管理。

步骤5 在密钥列表中，查看密钥信息，如图3-23所示。

图 3-23 密钥列表

说明

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

密钥列表参数说明，如表3-9所示。

表 3-9 密钥列表参数说明

参数	操作说明
别名	密钥的别名。

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”。
ID	创建密钥时自动生成的密钥ID。
创建时间	创建该密钥的时间。
密钥材料失效时间	密钥材料失效的时间，密钥材料失效后，当前密钥为空密钥。
密钥材料来源	密钥材料的来源，包含： ● 外部 用户从外部导入到密钥管理。 ● 密钥管理 用户通过密钥管理创建。

步骤6 用户可单击密钥别名，查看密钥详细信息，如图3-24所示。

图 3-24 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。

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

----结束

3.8.2 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用户主密钥进行启用操作，使被禁用的密钥恢复到数据加解密能力。新建的用户主密钥默认为“启用”状态。

前提条件

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

启用单个密钥

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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行，展开密钥管理。

步骤5 在需要启用的密钥所在行，单击“启用”。

图 3-25 启用单个密钥

别名	状态	ID	创建时间	密钥材料失效时间	密钥材料来源	操作
KMS-e973	禁用	a0070978-2060-4208-976c-5ee7c3407358	2018/05/22 15:26:04 GMT+08:00	-	密钥管理服务	启用 删除
KMS-a38b	等待导入	a0421a85-dba9-4373-81b4-f50c24e1ace6	2018/05/22 11:30:59 GMT+08:00	-	外部	删除 导入密钥材料
KMS-6a72	禁用	83380b75-c3c7-45fd-8321-55e13573ca2e	2018/05/22 11:08:40 GMT+08:00	-	密钥管理服务	启用 删除

步骤6 在弹出窗口中，单击“确定”，完成启用单个密钥操作。

----结束

批量启用密钥

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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行，展开密钥管理。

步骤5 在密钥列表中，勾选所有需要启用的密钥，单击“启用”。

图 3-26 批量启用密钥

步骤6 在弹出窗口中，单击“确定”，完成批量启用密钥操作。

----结束

3.8.3 禁用密钥

该任务指导用户通过密钥管理界面对指定的用户主密钥进行禁用，以紧急保护数据。

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

说明

默认主密钥为密钥管理服务自动创建，不支持禁用操作。

前提条件

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

禁用单个密钥

步骤1 登录管理控制台。

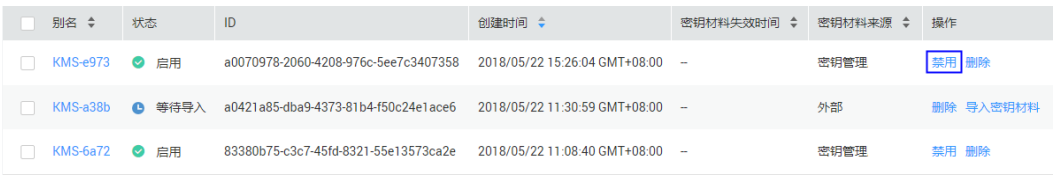
步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 在需要禁用的密钥所在行，单击“禁用”。

图 3-27 禁用单个密钥



步骤6 在弹出窗口中，单击“确定”，完成禁用单个密钥操作。

----结束

批量禁用密钥

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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 在密钥列表中，勾选所有需要禁用的密钥，单击“禁用”。

图 3-28 批量禁用密钥

步骤6 在弹出窗口中，单击“确定”，完成批量禁用密钥操作。

----结束

3.8.4 计划删除密钥

该任务指导用户通过密钥管理界面对不再使用的用户主密钥进行有计划删除。

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

在删除密钥前，用户需要确保该密钥没有被使用或将来也不会被使用。

说明

默认主密钥为服务自动创建，不支持删除操作。

前提条件

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

删除单个密钥

步骤1 登录管理控制台。

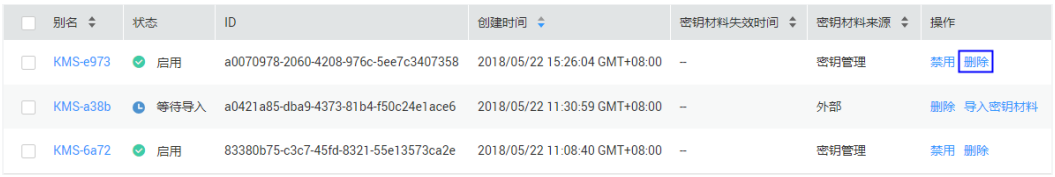
步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 在需要删除的密钥所在行，单击“删除”。

图 3-29 删除单个密钥



步骤6 在弹出的窗口中，填写“推迟删除”的时间。

图 3-30 推迟删除时间

步骤7 单击“确定”，完成删除单个密钥操作。

----结束

批量删除密钥

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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 在密钥列表中，勾选所有需要删除的密钥，单击“删除”。

图 3-31 批量删除密钥

步骤6 在弹出的窗口中，填写“推迟删除”的时间。

图 3-32 批量推迟删除时间

步骤7 单击“确定”，完成批量删除密钥操作。

----结束

3.8.5 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用户主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

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

取消删除单个密钥

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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 在需要取消删除的密钥所在行，单击“取消删除”。

图 3-33 取消删除单个密钥

步骤6 在弹出的窗口中，单击“确定”，完成取消删除单个密钥操作。

- 如果是密钥管理创建的密钥，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。

----结束

批量取消删除密钥

步骤1 登录管理控制台。

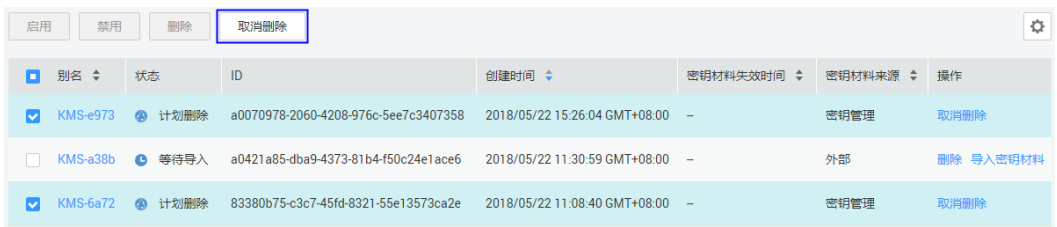
步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 在密钥列表中，勾选所有需要取消删除的密钥，单击“取消删除”。

图 3-34 批量取消删除密钥



步骤6 在弹出的窗口中，单击“确定”，完成批量取消删除密钥操作。

- 如果是密钥管理创建的密钥，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。

----结束

4 密钥对管理

4.1 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，并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**。

  注意

  通过管理控制台创建的密钥对默认使用“SSH-2（RSA，2048）”加解密算法。

- 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

已获取管理控制台的登录帐号与密码。

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  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

步骤5 单击“创建密钥对”。

步骤6 在弹出的“创建密钥对”对话框中，输入密钥对名称，如图4-1所示。

图 4-1 创建密钥对

步骤7 若需要托管私钥，请阅读并勾选“我同意将密钥对私钥托管到华为云”。在“KMS加密”下拉列表中选择加密密钥。若不需要托管私钥，请跳过此步骤。

说明

- 用户使用密钥对的KMS加密功能时，KMS会自动为密钥对创建一个“kps/default”默认主密钥。
- 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。

图 4-2 托管私钥

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”，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。

注意

- 若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。
- 若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 私钥保存完成后，单击“确定”，密钥对创建成功。

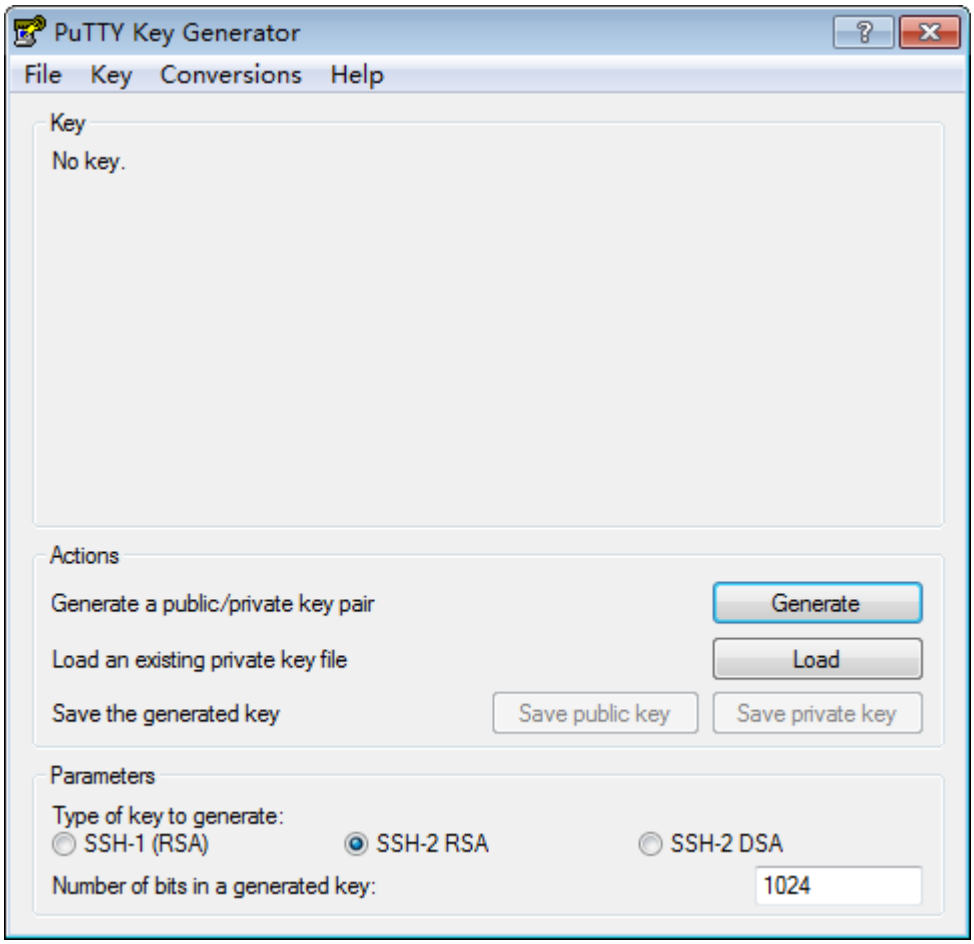
密钥对创建成功后，用户可以在密钥对列表里看到新创建的密钥对信息，包括密钥对的“名称”、“指纹”、“私钥”以及“使用数量”等。

----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4-3所示。

图 4-3 PuTTY Key Generator



步骤2 请根据表4-1设置参数。

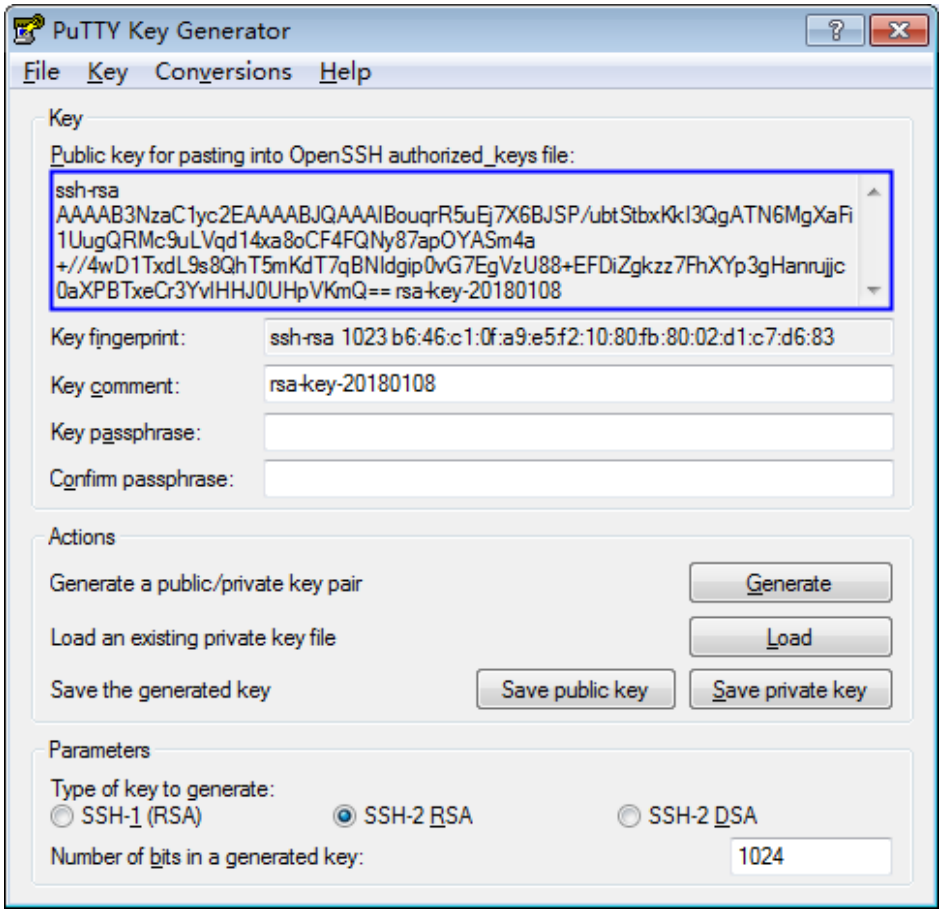
表 4-1 生成密钥对参数说明

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4-4所示。

蓝框中标记的内容为生成的公钥内容。

图 4-4 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。

注意

请勿直接单击“Save public key”保存公钥文件。若用户使用“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。

注意

为保证安全，私钥只能下载一次，请妥善保管。

- 当用户需要使用**PuTTY**工具登录Linux云服务器时，私钥文件保存为“.ppk”格式。保存方法如下所示：
  a. 在“PuTTY Key Generator”界面，选择“File > Save private key”。
  b. 保存私钥到本地。例如：kp-123.ppk。
- 当用户需要使用**Xshell**工具登录Linux操作系统云服务器，或者获取Windows操作系统云服务器的密码时，私钥文件保存为“.pem”格式。保存方法如下所示：
  a. 选择“Conversions > Export OpenSSH key”。

  说明

  如果该私钥文件用于Windows操作系统云服务器的获取密码操作，在选择“Export OpenSSH key”时，请勿填写“Key passphrase”信息，否则会导致获取密码失败。
  b. 保存私钥到本地。例如：kp-123.pem。

步骤6 根据需要正确保存公钥和私钥文件后，可将公钥导入管理控制台使用。

----结束

4.2 导入密钥对

若用户需要使用自己的密钥对（例如，使用**PuTTYgen**工具生成的密钥对），而不使用KMS生成的密钥对，用户可以把密钥对的公钥文件导入管理控制台使用，在远程登录弹性云服务器时，使用对应的私钥进行身份认证。用户也可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。

该任务指导用户通过密钥对管理界面导入密钥对。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 支持导入的公钥文件的加解密算法为：
  - SSH-2（RSA，1024）
  - SSH-2（RSA，2048）
  - SSH-2（RSA，4096）

导入密钥对

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

步骤5 单击“密钥对列表”页面右上角的“导入密钥对”，弹出“导入密钥对”对话框，如图4-5所示。

图 4-5 导入密钥对

步骤6 单击“选择文件”，选择本地保存的公钥文件，或者将公钥内容复制并粘贴至“公钥内容”文本框中。

说明

用户可自定义导入密钥对的名称。

步骤7 若需要托管私钥，请确认并勾选“我同意将密钥对私钥托管到华为云”，如图4-6所示。若不需要托管私钥，请跳过此步骤。

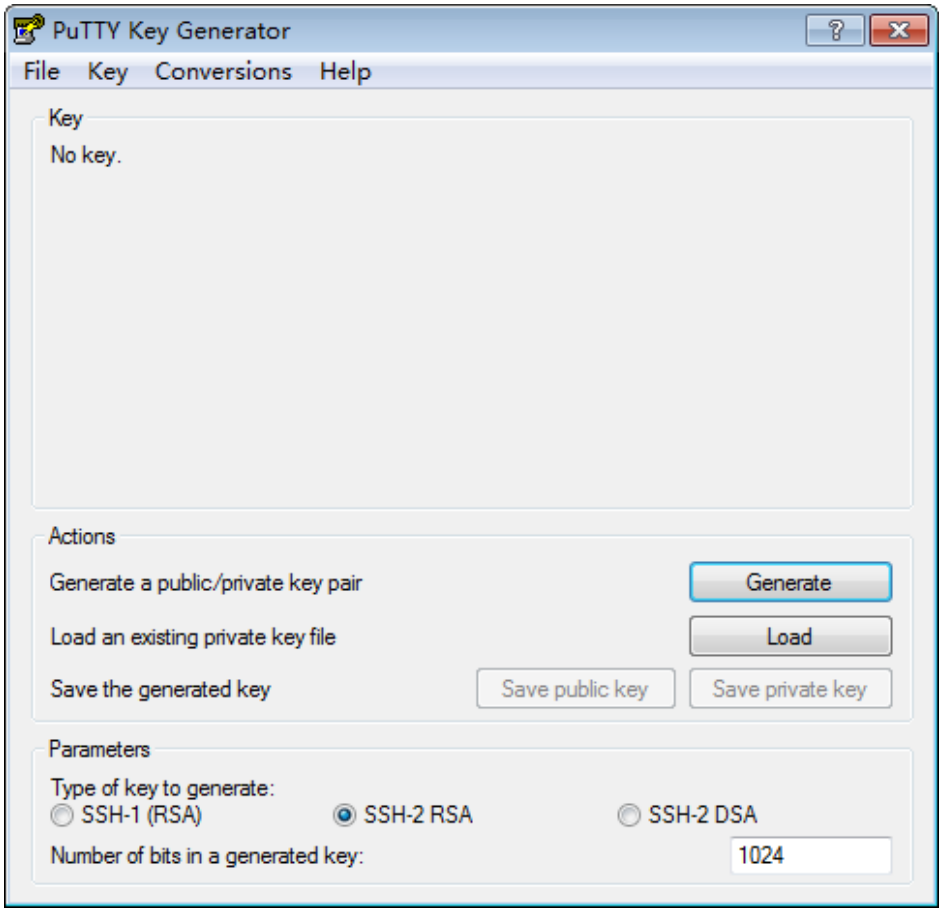
图 4-6 托管私钥

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

   上传或者拷贝至文本框的私钥必须是“.pem”格式文件，若是“.ppk”格式文件，需要通过以下步骤将“.ppk”格式文件转换为“.pem”格式文件。

   a. 双击“PUTTYGEN.exe”，打开“PuTTY Key Generator”，如图4-7所示。

图 4-7 PuTTY Key Generator



b. 选择“Conversions > Import Key”导入格式为“.ppk”的私钥文件。

c. 选择“Conversions > Export OpenSSH Key”，弹出“PuTTYgen Warning”对话框。

d. 单击“是”，将文件保存为“.pem”格式文件。

2. 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KMS加密功能时，KMS会自动为密钥对创建一个“kps/default”默认主密钥。
- 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”，导入密钥对。

----结束

4.3 使用私钥登录 Linux ECS

操作场景

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。

该任务指导用户使用私钥登录Linux弹性云服务器。

前提条件

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

本地使用 Windows 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

以PuTTY为例介绍如何登录弹性云服务器，使用PuTTY登录弹性云服务器前，需要先将私钥文件转化为“.ppk”格式。

步骤1 判断私钥文件是否为“.ppk”格式。

- 若是“.ppk”格式文件，请跳过此步骤。
- 若不是“.ppk”格式，请按以下步骤将私钥文件格式转换为“.ppk”格式。
  a. 在以下路径中下载PuTTY和PuTTYgen。
     http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
     说明
     PuTTYgen是密钥生成器，用于创建SSH密钥对，生成一个公钥和私钥供PuTTY使用。
  b. 运行PuTTYgen。
  c. 在“Actions”区域，单击“Load”，并导入购买弹性云服务器时保存的私钥文件。
     导入时注意确保导入的格式要求为“All files(*.*)”。
  d. 单击“Save private key”。
  e. 保存转化后的私钥到本地。例如：kp-123.ppk。

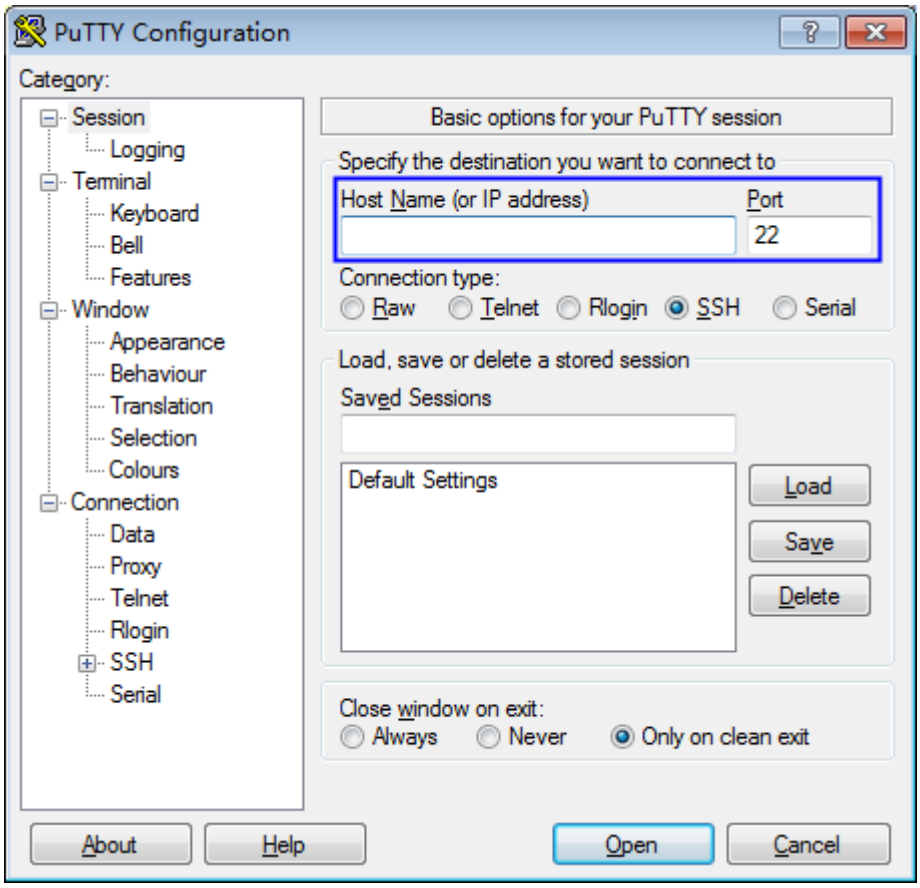
步骤2 双击“PuTTY.EXE”，打开“PuTTY Configuration”。

步骤3 选择“Connection > data”，在“Auto-login username”处输入镜像的用户名。

步骤4 选择“Connection > SSH > Auth”，在“Private key file forauthentication”配置项中，单击“Browse”，选择**步骤1**转化的私钥文件。

步骤5 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 4-8 配置弹性 IP



步骤6 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 选择本地保存的密钥文件，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/私钥文件名称*

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

4.4 使用私钥获取 Windows ECS 的登录密码

操作场景

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帐户或Cloudbase-init设置的帐户）。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。

说明

- 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》。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已购买Windows操作系统的弹性云服务器。

获取密码

步骤1 获取购买弹性云服务器时使用的私钥文件（.pem文件）。

步骤2 登录管理控制台。

步骤3 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

4.5 管理密钥对

4.5.1 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，若用户需要将“密码方式”修改为“密钥对方式”，可通过KMS管理控制台绑定密钥对，KMS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。

注意

在KMS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。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 弹性云服务器的状态处于“运行中”或者“关机”状态。

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  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

说明

用户也可以在“密钥对列表”页面，找到密钥对所对应的弹性云服务器，单击弹性云服务器所在行的“绑定”，绑定密钥对。

步骤5 单击“云服务器列表”，显示云服务器列表页面，如图4-9所示。

图 4-9 弹性云服务器列表

步骤6 单击目标虚拟机所在行的“绑定”，弹出绑定密钥对的对话框。

- 若弹性云服务器处于“关机”状态，绑定密钥对的对话框，如图4-10所示。

图 4-10 绑定密钥对（一）

- 若弹性云服务器处于“运行中”状态，需要提供“root密码”，如图4-11所示。

图 4-11 绑定密钥对（二）

说明

- 若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。
- 若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 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

若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。

若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，若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，操作步骤如下所示:

1. 登录弹性云服务器。
2. 执行以下命令，打开“/etc/ssh/sshd_config”文件。

   vi /etc/ssh/sshd_config
3. 按“i”进入编辑模式，开启密码登录。
   - 非SUSE操作系统，将“PasswordAuthentication”字段值修改为“yes”。
     ```
     PasswordAuthentication yes
     ```
   - SUSE操作系统，将“PasswordAuthentication”和“UsePAM”字段值修改为“yes”。
     ```
     PasswordAuthentication yes
     UsePAM yes
     ```
4. 按“Esc”，退出编辑模式。
5. 输入“:wq”，按“Enter”，保存退出。
6. 执行以下命令，重启SSH服务，使配置生效。
   - 非*Ubuntu14.xx*版本的操作系统。

     service sshd restart
   - *Ubuntu14.xx*版本的操作系统。

     service ssh restart

步骤9 请确认并勾选“该服务器使用华为云提供的公共镜像并未修改过SSH配置”。

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。

- 若在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。
- 若在弹性云服务器处于“关机”状态绑定密钥对，等待约5分钟可绑定成功。

----结束

4.5.2 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”。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

步骤5 在密钥对列表中查看密钥对的信息，用户可在右上角的搜索框中输入密钥对的名称，单击 ，搜索需要查看的密钥对。

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“使用数量”。

图 4-12 密钥对列表

步骤6 单击目标密钥对所在行的 展开密钥对，显示使用该密钥对的弹性云服务器列表，如图4-13所示。

图 4-13 弹性云服务器列表

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4-2所示。

表 4-2 弹性云服务器参数说明

参数名	参数说明
任务状态	重置或者替换密钥对的状态： ：正在执行 ：执行失败
ECS 名称/ID	弹性云服务器的名称与ID。

参数名	参数说明
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。
绑定密钥对	绑定弹性云服务器的密钥对。

步骤7 可单击，查看密钥对执行失败记录，如图4-14所示。

图 4-14 密钥对执行失败记录

说明

用户可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。

----结束

4.5.3 重置密钥对

若用户私钥丢失，用户可通过KMS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

- 已获取管理控制台的登录帐号与密码。
- 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。

重置密钥对

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

说明

用户也可以单击“云服务器列表”，进入云服务器列表页面，找到对应的弹性云服务器，单击弹性云服务器所在行的“重置”，重置密钥对。

步骤5 单击目标密钥对所在行的展开密钥对，显示绑定该密钥对的弹性云服务器列表，如图4-15所示。

图 4-15 弹性云服务器列表

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4-16所示。

图 4-16 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 请确认并勾选“该服务器使用华为云提供的公共镜像并未修改过SSH配置”。

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

4.5.4 替换密钥对

若用户私钥泄露，用户可通过KMS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

- 已获取管理控制台的登录帐号与密码。
- 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。

替换密钥对

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

说明

用户也可以单击“云服务器列表”，进入云服务器列表页面，找到对应的弹性云服务器，单击弹性云服务器所在行的“替换”，替换密钥对。

步骤5 单击目标密钥对所在行的展开密钥对，显示绑定该密钥对的弹性云服务器，如图4-17所示。

图 4-17 弹性云服务器列表

步骤6 单击目标弹性云服务器所在行的“替换”，弹出替换密钥对的对话框，如图4-18所示。

图 4-18 替换密钥对

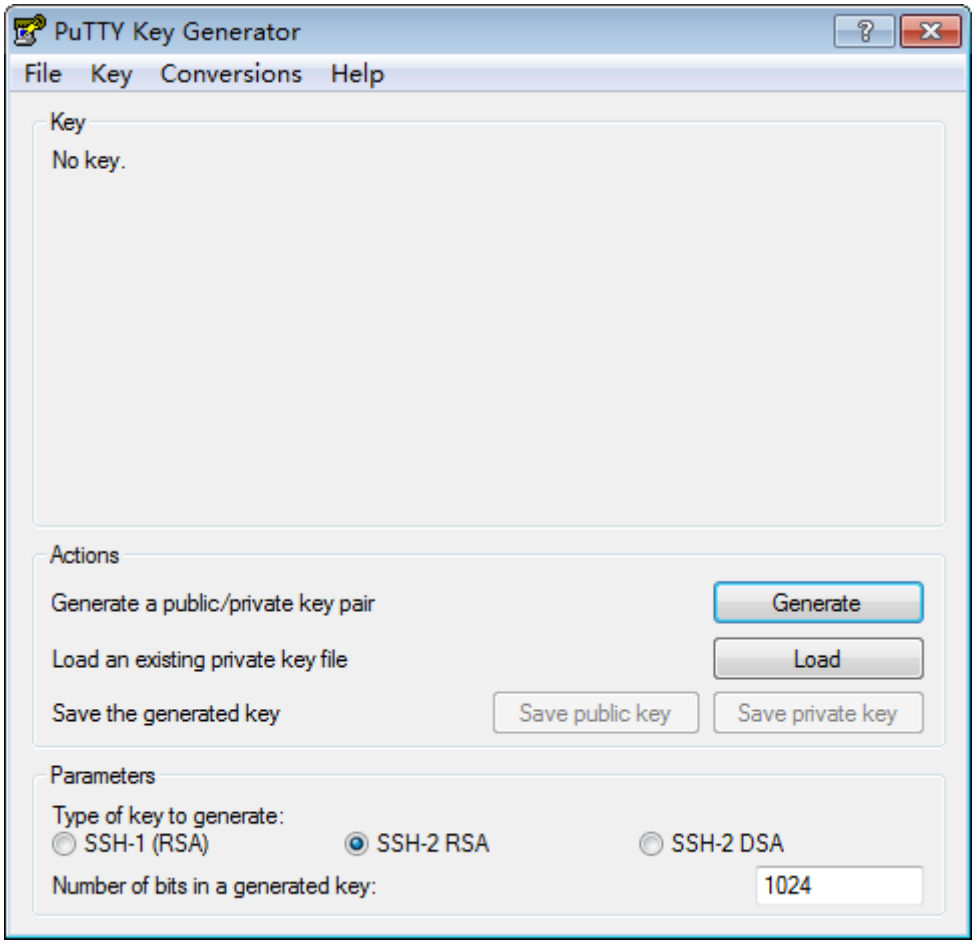
步骤7 在“新密钥对”下拉框中选择新的密钥对。

步骤8 单击“选择文件”，上传待替换密钥对的私钥，或者将私钥拷贝至文本框中。

上传或者拷贝至文本框的私钥必须是“.pem”格式文件，若是“.ppk”格式文件，需要通过以下步骤将“.ppk”格式文件转换为“.pem”格式文件。

1. 双击“PUTTYGEN.exe”，打开“PuTTY Key Generator”，如图4-19所示。

图 4-19 PuTTY Key Generator



2. 选择“Conversions > Import Key”导入格式为“.ppk”的私钥文件。
3. 选择“Conversions > Export OpenSSH Key”，弹出“PuTTYgen Warning”对话框。
4. 单击“是”，将文件保存为“.pem”格式文件。

步骤9 请确认并勾选“该服务器使用华为云提供的公共镜像并未修改过SSH配置”。

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

4.5.5 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，若用户需要将“密钥对方式”修改为“密码方式”，可通过密钥管理服务的SSH密钥对界面解绑密钥对，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。

注意

- 若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，若需要重新绑定密钥对，需要关机重新绑定密钥对。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 弹性云服务器已绑定密钥对。

解绑密钥对

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

说明

用户也可以在密钥对列表页面，找到密钥对所对应的弹性云服务器，单击弹性云服务器所在行的“解绑”，解绑密钥对。

步骤5 单击“云服务器列表”，显示云服务器列表页面，如图4-20所示。

图 4-20 弹性云服务器列表

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。

- 若弹性云服务器处于“关机”状态，解绑密钥对的对话框，如图4-21所示。

图 4-21 解绑密钥对（一）

- 若弹性云服务器处于“运行中”状态，解绑密钥对的对话框，如图4-22所示。

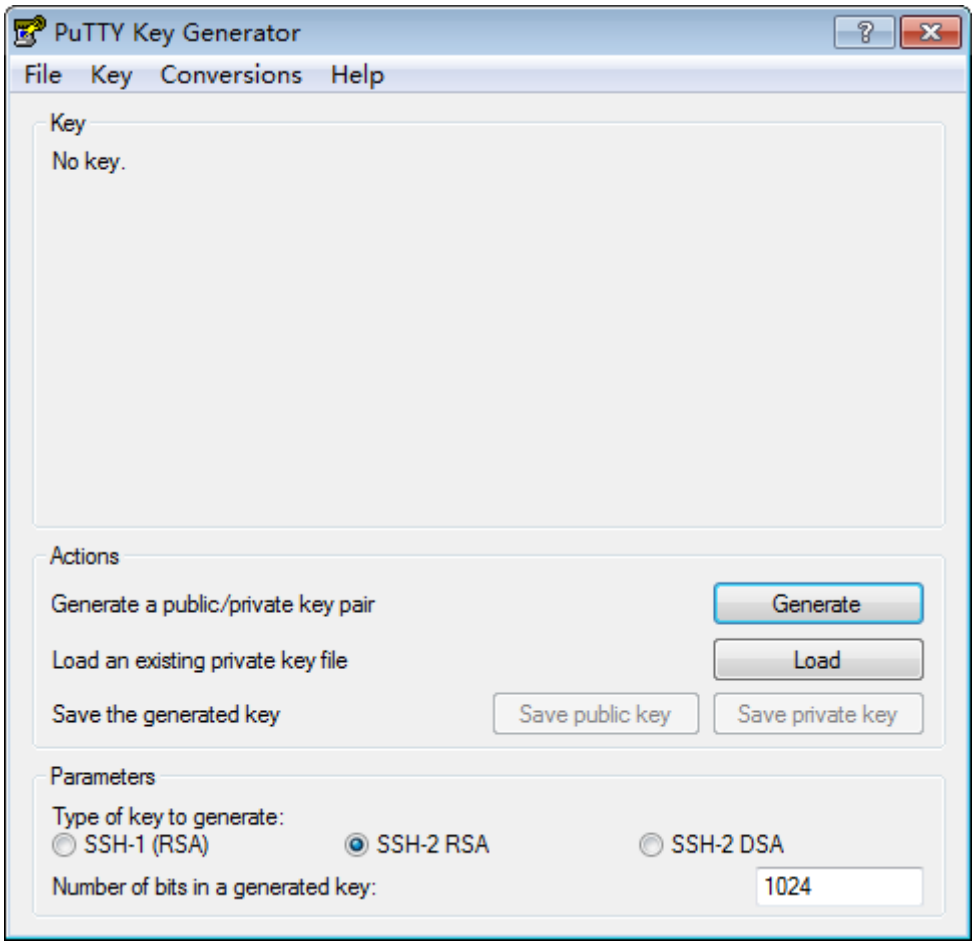
图 4-22 解绑密钥对（二）

步骤7 若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”，上传待替换密钥对的私钥，或者将私钥拷贝至文本框中。若在弹性云服务器处于“关机”状态，请跳过此步骤。

上传或者拷贝至文本框的私钥必须是“.pem”格式文件，若是“.ppk”格式文件，需要通过以下步骤将“.ppk”格式文件转换为“.pem”格式文件。

1. 双击“PUTTYGEN.exe”，打开“PuTTY Key Generator”，如图4-23所示。

图 4-23 PuTTY Key Generator



2. 选择“Conversions > Import Key”导入格式为“.ppk”的私钥文件。
3. 选择“Conversions > Export OpenSSH Key”，弹出“PuTTYgen Warning”对话框。
4. 单击“是”，将文件保存为“.pem”格式文件。

步骤8 请确认并勾选“该服务器使用华为云提供的公共镜像并未修改过SSH配置”。

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

4.5.6 删除密钥对

若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。

说明

- 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。
- 若用户删除KMS管理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。删除公钥后，用户无法使用新的密钥对对弹性云服务器进行密钥对的重置和替换操作。

前提条件

已获取管理控制台的登录帐号与密码。

删除密钥对

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

步骤5 在目标密钥对所在行，单击“删除”。

步骤6 在弹出的“删除密钥对”对话框中，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

4.6 管理私钥

4.6.1 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KMS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

已获取管理控制台的登录帐号与密码。

导入私钥

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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

步骤5 单击目标公钥所在行的“导入私钥”。

步骤6 在弹出的“导入私钥”对话框中，输入私钥的名称，如图4-24所示。

图 4-24 导入私钥

步骤7 单击“选择文件”，选择本地保存的私钥文件，或者将私钥内容复制并粘贴至“私钥内容”文本框中。

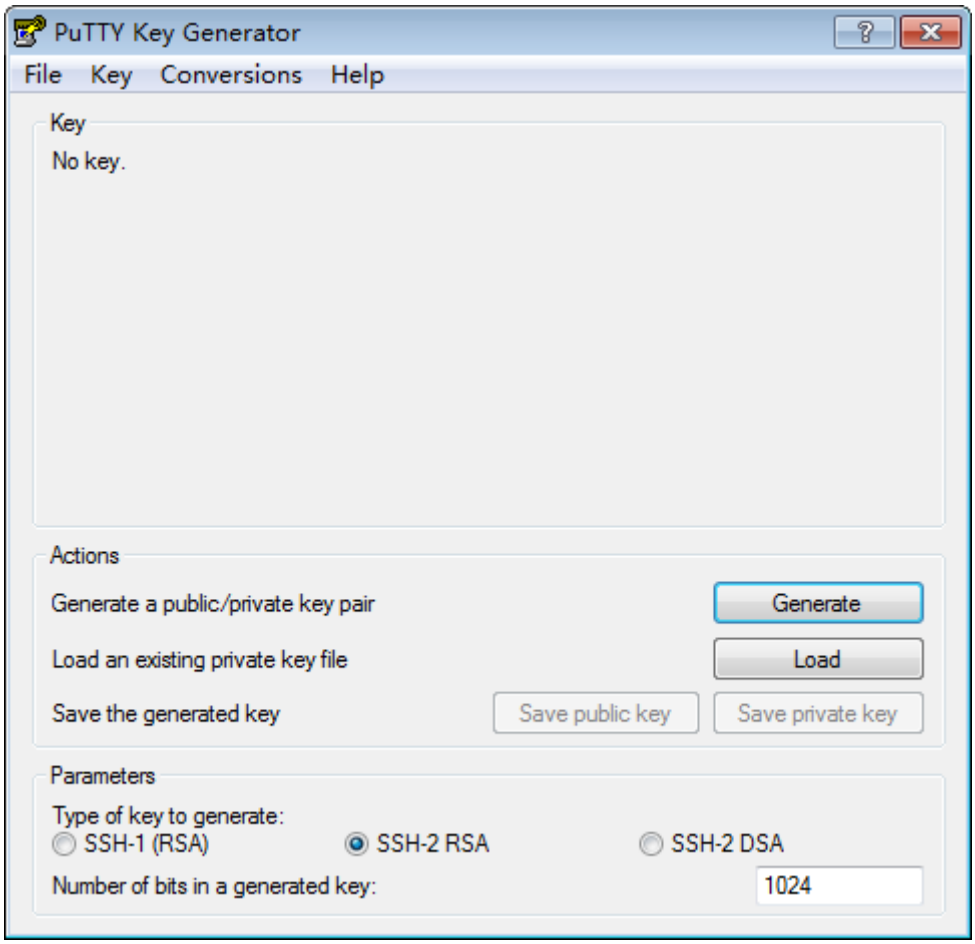
说明

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，若是“.ppk”格式文件，需要通过以下步骤将“.ppk”格式文件转换为“.pem”格式文件。

1. 双击“PUTTYGEN.exe”，打开“PuTTY Key Generator”，如图4-25所示。

图 4-25 PuTTY Key Generator



2. 选择“Conversions > Import Key”导入格式为“.ppk”的私钥文件。
3. 选择“Conversions > Export OpenSSH Key”，弹出“PuTTYgen Warning”对话框。
4. 单击“是”，将文件保存为“.pem”格式文件。

步骤8 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KMS加密功能时，KMS会自动为密钥对创建一个“kps/default”默认主密钥。
- 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”，完成私钥托管。

----结束

4.6.2 导出私钥

若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

- 已获取管理控制台的登录帐号与密码。
- 已将私钥托管在管理控制台。

导出私钥

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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”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4-26所示。

图 4-26 导出私钥

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。

注意

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

4.6.3 清除私钥

若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

- 已获取管理控制台的登录帐号与密码。
- 已将私钥托管在管理控制台。

删除私钥

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 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

步骤5 单击目标公钥所在行的“清除私钥”。

步骤6 在弹出的“清除私钥”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。若需要再次托管私钥，可将私钥再导入管理控制台。

----结束

5 专属加密

5.1 查看专属加密实例

该任务指导用户通过专属加密界面查看专属加密实例信息，包括专属加密实例的名称、状态、服务版本、设备厂商、设备型号、IP地址和到期时间。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 在左侧导航树中，选择“专属加密”，进入专属加密实例列表页面。

步骤5 在专属加密实例列表中，查看专属加密实例信息，如图5-1所示。

图 5-1 专属加密实例列表

说明

可在“名称”下拉列表中，选择“名称”或者“设备型号”，输入专属加密实例的名称或者设备型号，单击  ，搜索对应的专属加密实例。

专属加密实例列表参数说明，如表5-1所示。

表 5-1 专属加密实例参数说明

参数	参数说明
名称	专属加密实例的名称。
服务版本	基础版或者专业版。 ● 基础版：用户享有共享机框和电源，在密码运算上独占加密卡的虚拟化专属加密实例。 ● 专业版：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。
状态	购买的专属加密实例的状态： ● 审核中 用户购买专属加密实例提交审核后，处于“审核中”状态。 ● 审核未通过 华为安全专家通过与用户联系，确定用户订购的专属加密实例不满足用户的业务，审核不通过。 ● 待付款 用户购买的专属加密实例通过审核，等待用户付款，专属加密实例处于“待付款”状态。 ● 创建中 用户购买的专属加密实例通过审核，并付款成功，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。 ● 运行中 付款成功后，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。
设备厂商	设备厂商的名称，包含“江南天安”和“三未信安”。
设备型号	设备型号。
IP地址	IP地址。
到期时间	购买的专属加密实例的到期时间。

----结束

5.2 使用专属加密实例

在获取专属加密实例后需要初始化专属加密实例。初始化专属加密实例前，用户需要获取以下信息。

表 5-2 获取初始化专属加密实例的信息

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，由华为云邮寄到用户的Ukey收件地址。

名称	说明	来源
Ukey驱动	Windows驱动，识别Ukey。	华为云安全专家通过用户提供的联系方式联系用户，并提供软件包链接供用户下载。
Dedicated HSM管理工具	配合Ukey，远程管理专属加密实例。	
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。	
华为云Windows ECS实例	运行Dedicated HSM管理工具，与专属加密实例处于同一VPC组，并分配弹性IP地址用于远程连接。	
华为云Linux ECS实例	运行安全代理软件和用户的应用程序，与专属加密实例处于同一VPC组。	

初始化专属加密实例

步骤1 在用户本地Windows PC上安装Ukey驱动。

步骤2 远程连接华为云Windows ECS实例。

1. 运行本地Windows PC的**mstsc**远程连接工具，并通过华为云上Windows ECS实例的弹性IP地址远程连接ECS实例。
2. 在本地PC的USB口插入Ukey，通过远程连接功能将本地Ukey端口映射到华为云的Windows ECS实例。

步骤3 通过Dedicated HSM管理专属加密实例。

1. 在华为云Windows ECS实例上运行Dedicated HSM管理工具。
2. 通过与专属加密实例的VPC子网IP连接，配合Ukey初始化专属加密实例，并产生、备份、恢复密钥。

----结束

配置安全代理软件

步骤1 通过Dedicated HSM连接专属加密实例，给华为云Linux ECS实例上的安全代理签发许可文件。

步骤2 在Linux ECS实例上运行安全代理软件，将许可文件导入到安全代理软件，并与专属加密实例建立安全通道。

----结束

接口调用

应用程序通过SDK提供的接口与安全代理软件建立连接，通过安全代理软件调用专属加密实例。

6 常见问题

6.1 概念类

6.1.1 什么是密钥管理？

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

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

6.1.2 什么是用户主密钥？

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

6.1.3 什么是默认主密钥？

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

默认主密钥可通过密钥管理服务界面进行查询，不支持禁用、计划删除操作。

表 6-1 默认主密钥列表

密钥别名	对应云服务
obs/default	对象存储服务
evs/default	云硬盘（Elastic Volume Service，EVS）
ims/default	镜像服务（Image Management Service，IMS）

说明

默认主密钥是在用户第一次通过对应云服务使用KMS加密时自动生成的。

6.1.4 用户主密钥与默认主密钥有什么区别？

用户主密钥和默认主密钥的区别，如表6-2所示。

表 6-2 用户主密钥和默认主密钥的区别

名称	概念	区别
用户主密钥	即CMK，是用户通过KMS创建的密钥，是一种密钥加密密钥，主要用于加密并保护DEK。 一个用户主密钥可以加密多个DEK。	支持禁用、计划删除等操作。
默认主密钥	属于用户主密钥，是用户第一次通过对应云服务使用KMS加密时，系统自动生成的，其名称后缀为“/default”。 例如：evs/default	● 支持通过管理控制台的KMS页面查询默认主密钥详情。 ● 不支持禁用、计划删除等操作。

6.1.5 什么是数据加密密钥？

数据加密密钥是用于加密数据的密钥。

6.2 功能类

6.2.1 为什么不能立即删除用户主密钥？

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

6.2.2 哪些云服务使用 KMS 加密数据？

对象存储服务、云硬盘、镜像服务和关系型数据库借助KMS服务实现了加密特性。

6.2.3 KMS 提供了哪些功能？

密钥管理

- 基础版

  用户可通过密钥管理界面，对用户主密钥进行以下操作：
  - 创建、查看、启用、禁用、计划删除、取消删除用户主密钥
  - 修改用户主密钥的别名和描述
  - 在线工具加解密小数据
  - 添加、搜索、编辑、删除标签
- 专业版
  - 用户可通过密钥管理界面或接口，对用户主密钥进行以下操作：
    - 包含基础版所有功能
    - 开启、修改、关闭密钥管理轮换周期
    - 创建、撤销、查询授权
  - 用户可通过密钥管理的接口执行以下操作：
    - 对数据加密密钥进行创建、加密或解密操作
    - 对授予的权限进行退役授权操作

    具体请参见《数据加密服务API参考》。
  - 生成硬件真随机数

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

密钥对管理

用户可通过密钥对管理界面或接口，对密钥对进行以下操作：

- 创建、导入、查看、删除密钥对
- 重置、替换、绑定、解绑密钥对
- 托管、导入、导出、清除私钥

专属加密

用户可通过专属加密界面，购买专属加密实例和查看专属加密实例信息。

6.2.4 华为云服务如何使用 KMS 加密数据？

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

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

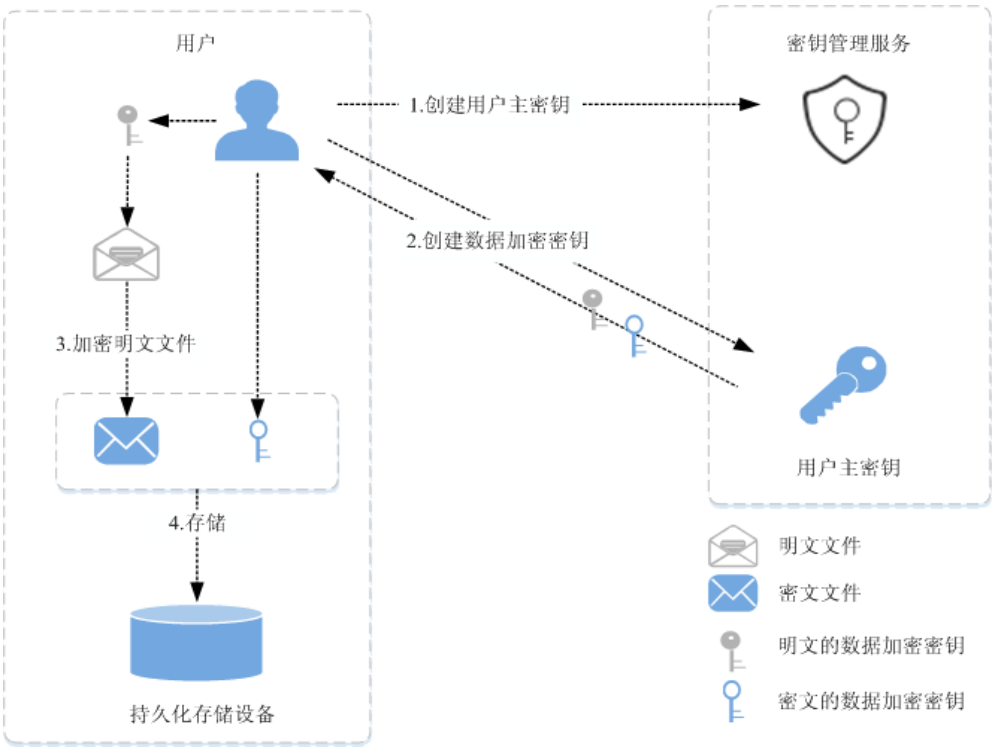
说明

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

- 用户通过华为云服务加密数据时，需要指定一个KMS用户主密钥。华为云服务会生成一个明文的数据加密密钥和一个密文的数据加密密钥，其中密文的数据加密密钥是由指定的用户主密钥加密明文的数据加密密钥生成的。华为云服务使用明

文的数据加密密钥来加密数据，然后将加密后的密文数据与密文的数据加密密钥一同存储在华为云服务中，如下图所示。

图 6-1 加密本地文件



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

6.2.5 信封加密方式有什么优势？

信封加密方式相对于使用KMS用户主密钥直接加密的优势如下：

使用KMS用户主密钥直接加解密数据仅适用于不大于4KB的小数据加解密场景；而信封加密方式可以在本地对大量数据进行加解密。信封加密方式加解密数据，只需要传输数据加密密钥到KMS服务端，无需通过网络传输大量数据。

6.2.6 在 KMS 中创建的用户主密钥的个数是否有限制？

有。

- 基础版的密钥管理中最多可创建或导入2个用户主密钥，不包含默认主密钥。
- 专业版的密钥管理中最多可创建或导入20个用户主密钥。

6.2.7 KMS 中创建的用户主密钥长度是多少？

通过KMS创建的用户主密钥长度为256bit。

6.2.8 用户是否可以从 KMS 中导出用户主密钥？

不可以。

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

6.2.9 如果用户主密钥被彻底删除，用户数据是否还可以解密？

不可以。

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

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

6.2.10 如何使用在线工具加解密数据？

使用在线工具加解密小数据的操作步骤如下所示：

加密数据

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 单击目标用户主密钥的别名，进入密钥详细信息在线工具加密数据页面。

步骤6 在“加密”文本框中输入待加密的数据，如图6-2所示。

图 6-2 加密数据

步骤7 单击“执行”，右侧文本框显示加密后的密文数据。

说明

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

----结束

解密数据

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤4 单击目标密钥管理所在行 ，展开密钥管理。

步骤5 解密数据时，可单击任意“启用”状态的非默认主密钥别名，进入该密钥的在线工具页面。

步骤6 单击“解密”，在左侧文本框中数据待解密的密文数据，如图6-3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。
- 若该密钥已被删除，会导致解密失败。

图 6-3 解密数据

步骤7 单击“执行”，右侧文本框中显示解密后的明文数据。

说明

用户可直接单击“复制到剪切板”拷贝解密后的明文数据，并保存到本地文件中。

----结束

6.2.11 是否可以更新 KMS 管理的密钥？

不可以。

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

6.2.12 在什么场景下推荐使用导入的密钥？

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

6.2.13 可以导入哪些类型的密钥？

用户可以导入256位对称密钥。

6.2.14 密钥材料被意外删除时如何处理？

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

注意

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

6.2.15 如何创建密钥对？

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，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

步骤5 单击“创建密钥对”。

步骤6 在弹出的“创建密钥对”对话框中，输入密钥对名称，如图6-4所示。

图 6-4 创建密钥对

步骤7 若需要托管私钥，请阅读并勾选“我同意将密钥对私钥托管到华为云”。在“KMS加密”下拉列表中选择加密密钥。若不需要托管私钥，请跳过此步骤。

说明

- 用户使用密钥对的KMS加密功能时，KMS会自动为密钥对创建一个“kps/default”默认主密钥。
- 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。

图 6-5 托管私钥

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”，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。

注意

- 若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。
- 若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 私钥保存完成后，单击“确定”，密钥对创建成功。

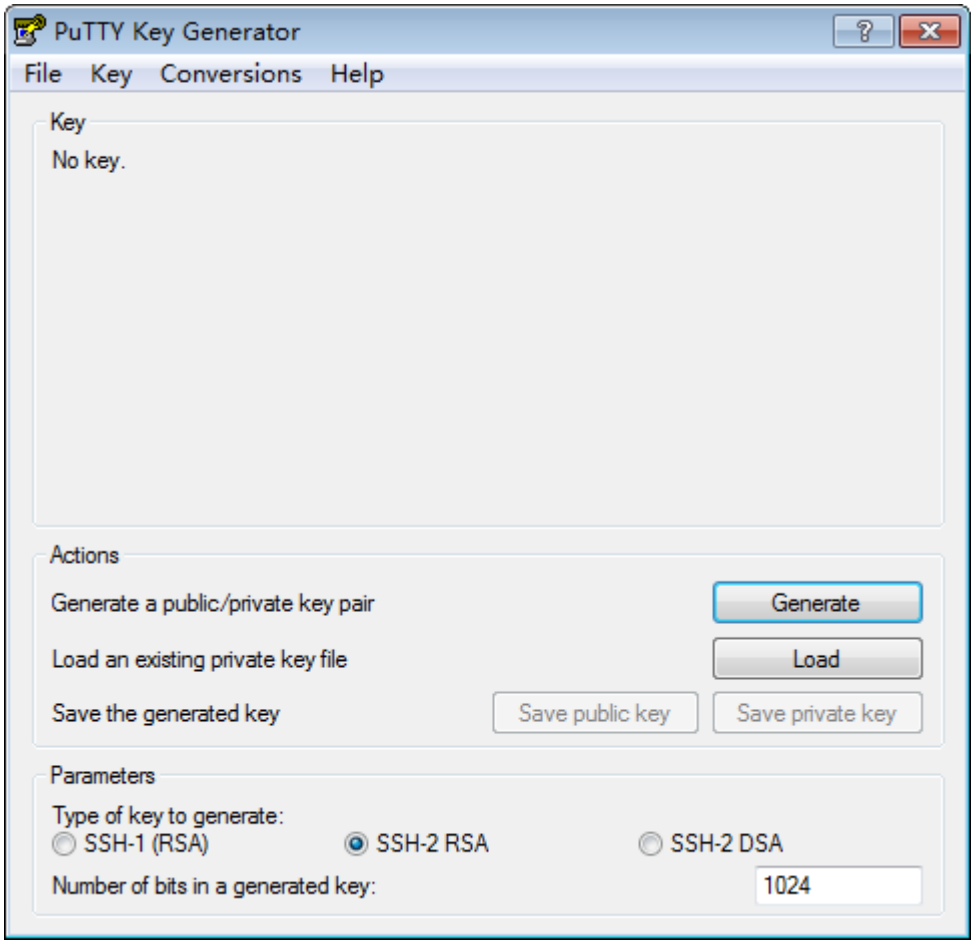
密钥对创建成功后，用户可以在密钥对列表里看到新创建的密钥对信息，包括密钥对的“名称”、“指纹”、“私钥”以及“使用数量”等。

----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6-6所示。

图 6-6 PuTTY Key Generator



步骤2 请根据表6-3设置参数。

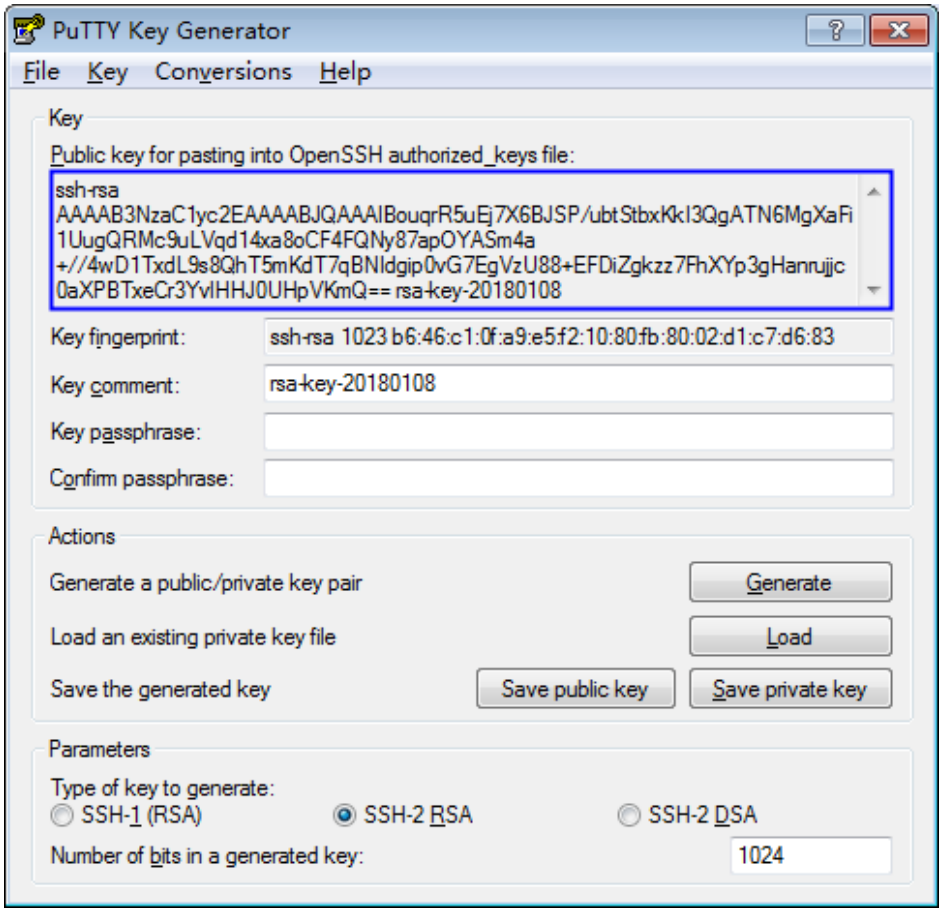
表 6-3 生成密钥对参数说明

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6-7所示。

蓝框中标记的内容为生成的公钥内容。

图 6-7 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。

注意

请勿直接单击“Save public key”保存公钥文件。若用户使用“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。

注意

为保证安全，私钥只能下载一次，请妥善保管。

- 当用户需要使用**PuTTY**工具登录Linux云服务器时，私钥文件保存为“.ppk”格式。保存方法如下所示：
  a. 在“PuTTY Key Generator”界面，选择“File > Save private key”。
  b. 保存私钥到本地。例如：kp-123.ppk。
- 当用户需要使用**Xshell**工具登录Linux操作系统云服务器，或者获取Windows操作系统云服务器的密码时，私钥文件保存为“.pem”格式。保存方法如下所示：

a. 选择“Conversions > Export OpenSSH key”。

说明

如果该私钥文件用于Windows操作系统云服务器的获取密码操作，在选择“Export OpenSSH key”时，请勿填写“Key passphrase”信息，否则会导致获取密码失败。

b. 保存私钥到本地。例如：kp-123.pem。

步骤6 根据需要正确保存公钥和私钥文件后，可将公钥导入管理控制台使用。

----结束

6.2.16 导入通过 PuTTYgen 工具创建的密钥对失败如何处理？

问题描述

通过**PuTTYgen**工具创建的密钥对，在导入管理控制台使用时，系统提示导入公钥文件失败。

可能原因

公钥内容的格式不符合系统要求。

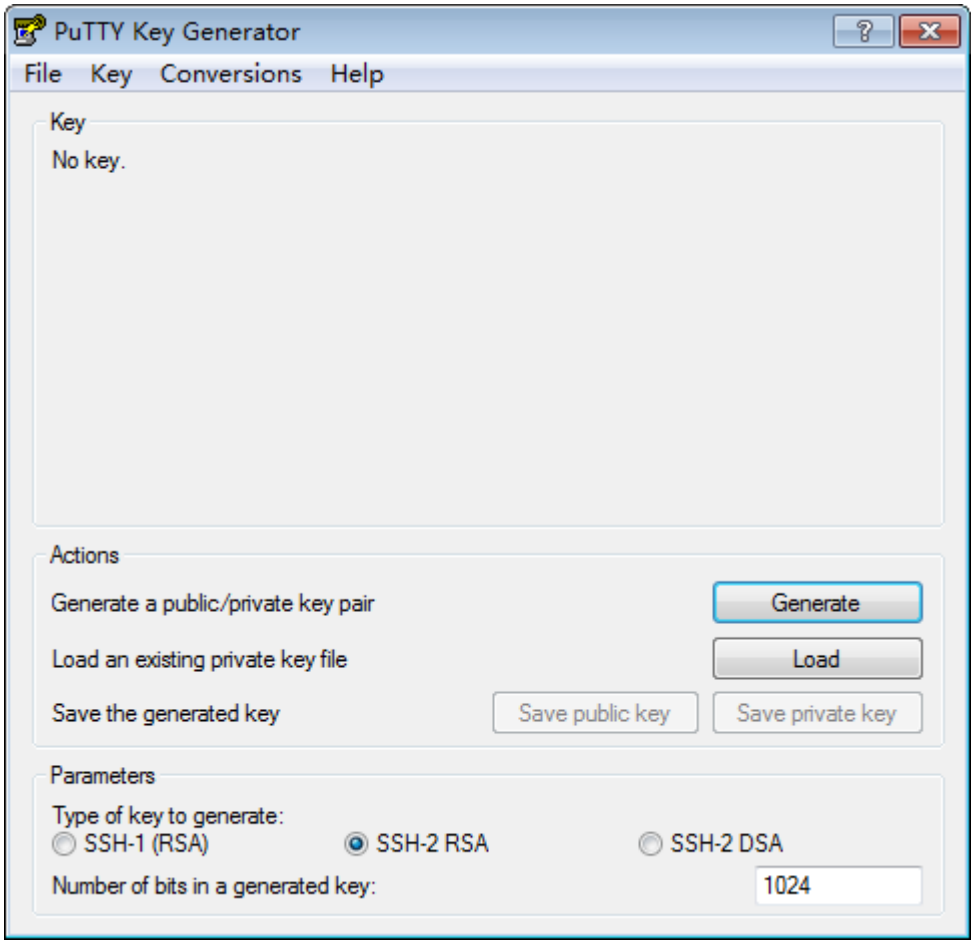
当用户使用**PuTTYgen**工具创建密钥对时，使用**PuTTYgen**工具的“Save public key”保存公钥，公钥内容的格式会发生变化。当用户将公钥内容导入管理控制台时，系统会校对公钥内容的格式，若校对不成功，则会导致导入失败。

处理方法

使用本地保存的私钥文件，在“PuTTY Key Generator”中恢复内容格式正确的公钥文件，然后再将该公钥文件导入管理控制台。

步骤1 双击“PUTTYGEN.exe”，打开“PuTTY Key Generator”，如图6-8所示。

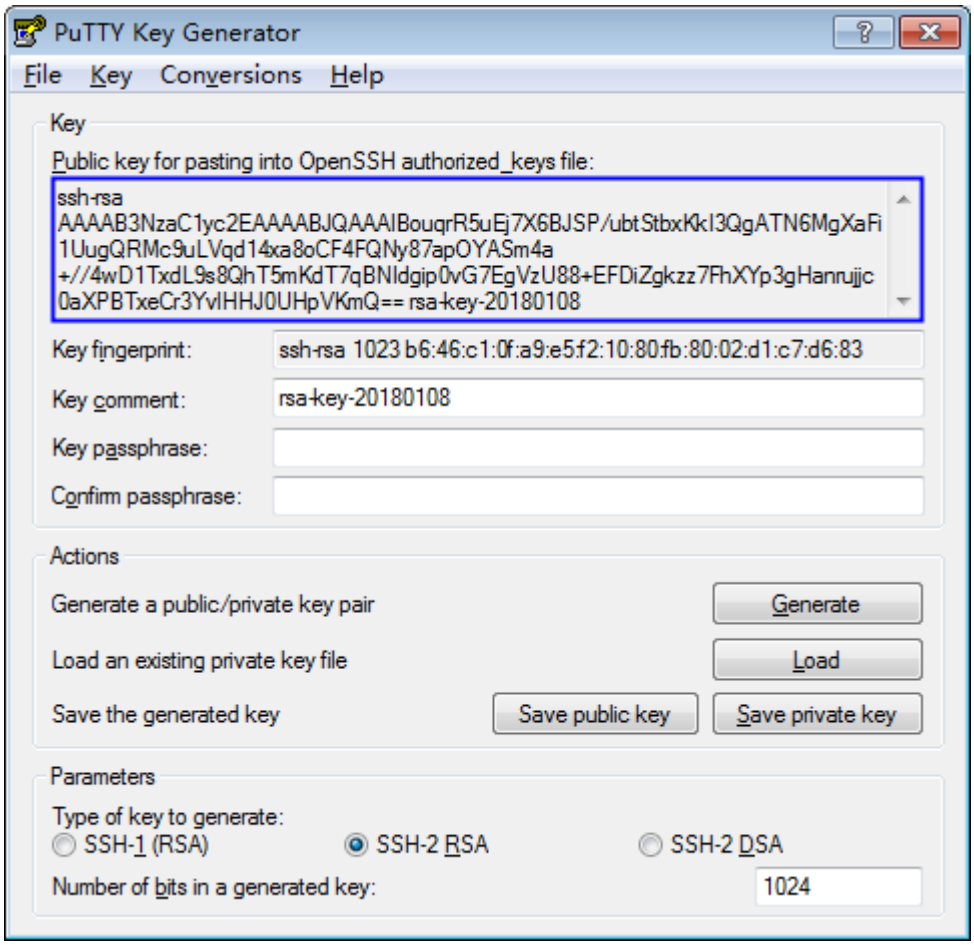
图 6-8 PuTTY Key Generator



步骤2 单击“Load”，并在本地选择该密钥对的私钥文件。

系统将自动加载该私钥文件，并在“PuTTY Key Generator”中恢复格式正确的公钥文件内容，如图6-9所示，蓝框中的内容即为符合系统要求的公钥文件。

图 6-9 恢复公钥文件内容



步骤3 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。

注意

请勿直接单击“Save public key”保存公钥文件。若用户使用“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4 将公钥文件导入管理控制台。

1. 登录管理控制台。
2. 选择“安全 > 数据加密服务”。
3. 在左侧导航树中，选择“密钥对管理”。
4. 在密钥对列表页面，单击“导入密钥对”。
5. 将“.txt”格式文本文档中的公钥内容粘贴至“公钥内容”的空白区域，并单击“确定”，导入公钥文件。或者单击“选择文件”，将保存的“.txt”格式文本文档的公钥文件导入管理控制台。

----结束

6.2.17 使用 IE9 浏览器无法导入密钥对，该如何处理？

问题描述

当使用的是IE9浏览器时，无法导入密钥对。

处理方法

步骤1 在浏览器主界面，单击  。

步骤2 选择“Internet选项”。

步骤3 在Inernet选项对话框中，单击“安全”。

步骤4 单击“Internet”。

步骤5 如果安全级别显示为“自定义”，单击“默认级别”，把设置还原为默认级别。

步骤6 滑动安全级别滑块，把安全级别调至“中”，单击“应用”。

步骤7 选择“自定义级别”。

步骤8 将“对未标记为可安全执行脚本的ActiveX控件初始化并执行脚本”设置为“提示”。

步骤9 单击“确定”。

----结束

6.2.18 如何使用私钥登录 Linux 弹性云服务器？

前提条件

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

本地使用 Windows 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

以PuTTY为例介绍如何登录弹性云服务器，使用PuTTY登录弹性云服务器前，需要先将私钥文件转化为“.ppk”格式。

步骤1 判断私钥文件是否为“.ppk”格式。

- 若是“.ppk”格式文件，请跳过此步骤。
- 若不是“.ppk”格式，请按以下步骤将私钥文件格式转换为“.ppk”格式。

  a. 在以下路径中下载PuTTY和PuTTYgen。

  http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

  说明

  PuTTYgen是密钥生成器，用于创建SSH密钥对，生成一个公钥和私钥供PuTTY使用。

b. 运行PuTTYgen。

c. 在“Actions”区域，单击“Load”，并导入购买弹性云服务器时保存的私钥文件。

导入时注意确保导入的格式要求为“All files(*.*)”。

d. 单击“Save private key”。

e. 保存转化后的私钥到本地。例如：kp-123.ppk。

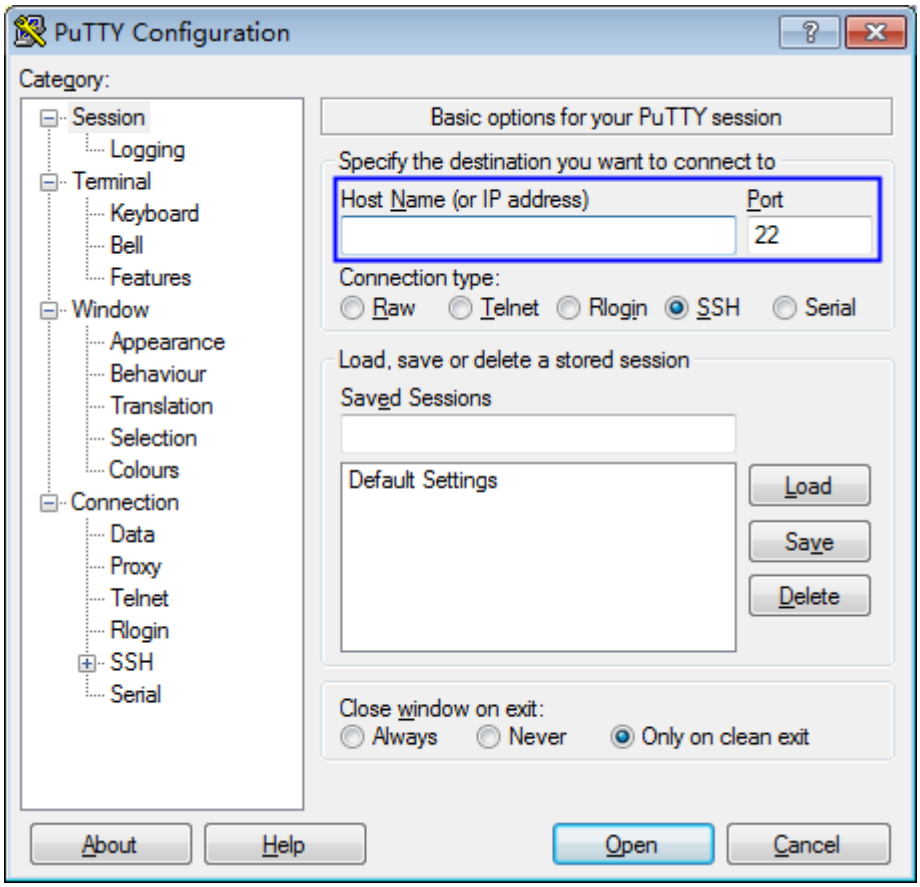
步骤2 双击“PuTTY.EXE”，打开“PuTTY Configuration”。

步骤3 选择“Connection > data”，在“Auto-login username”处输入镜像的用户名。

步骤4 选择“Connection > SSH > Auth”，在“Private key file forauthentication”配置项中，单击“Browse”，选择步骤1转化的私钥文件。

步骤5 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 6-10 配置弹性 IP



步骤6 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 选择本地保存的密钥文件，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/私钥文件名称***

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

6.2.19 如何通过私钥获取 Windows 弹性云服务器的登录密码？

问题描述

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帐户或Cloudbase-init设置的帐户）。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。

说明

- 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》。

处理步骤

步骤1 获取购买弹性云服务器时使用的私钥文件（.pem文件）。

步骤2 登录管理控制台。

步骤3 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

6.2.20 重置、替换、解绑或者绑定密钥对需要满足的条件？

若用户需要重置、替换或者绑定密钥对，需要满足以下条件：

- 重置密钥对
  - 弹性云服务器的状态处于“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。
- 替换密钥对
  - 弹性云服务器的状态处于“运行中”状态。
  - 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。
- 绑定密钥对
  - 若弹性云服务器处于“关机”状态，绑定密钥对是通过重置密钥对的方式实现绑定密钥对，因此，需要满足重置密钥对的条件。
  - 若弹性云服务器处于“运行中”状态，绑定密钥对是通过替换密钥对的方式绑定密钥对，因此，需要满足替换密钥对的条件。
- 解绑密钥对
  - 若弹性云服务器处于“关机”状态，解绑密钥对是通过重置密钥对的方式实现解绑密钥对，因此，需要满足重置密钥对的条件。
  - 若弹性云服务器处于“运行中”状态，解绑密钥对是通过替换密钥对的方式解绑密钥对，因此，需要满足替换密钥对的条件。

6.2.21 关闭弹性云服务器的密码登录方式后，如何重新开启？

当用户将密钥对绑定到弹性云服务器时，将密码登录方式关闭，若仍然需要使用密码登录弹性云服务器，可重新开启密码登录方式。

如下以PuTTY方式登录弹性云服务器开启密码登录方式为例进行说明。

步骤1 判断私钥文件是否为“.ppk”格式。

- 若是“.ppk”格式文件，请跳过此步骤。
- 若不是“.ppk”格式，请按以下步骤将私钥文件格式转换为“.ppk”格式。
  a. 在以下路径中下载PuTTY和PuTTYgen。
     http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
     说明
     PuTTYgen是密钥生成器，用于创建SSH密钥对，生成一个公钥和私钥供PuTTY使用。
  b. 运行PuTTYgen。
  c. 在“Actions”区域，单击“Load”，并导入购买弹性云服务器时保存的私钥文件。
     导入时注意确保导入的格式要求为“All files(*.*)”。
  d. 单击“Save private key”。
  e. 保存转化后的私钥到本地。例如：kp-123.ppk。

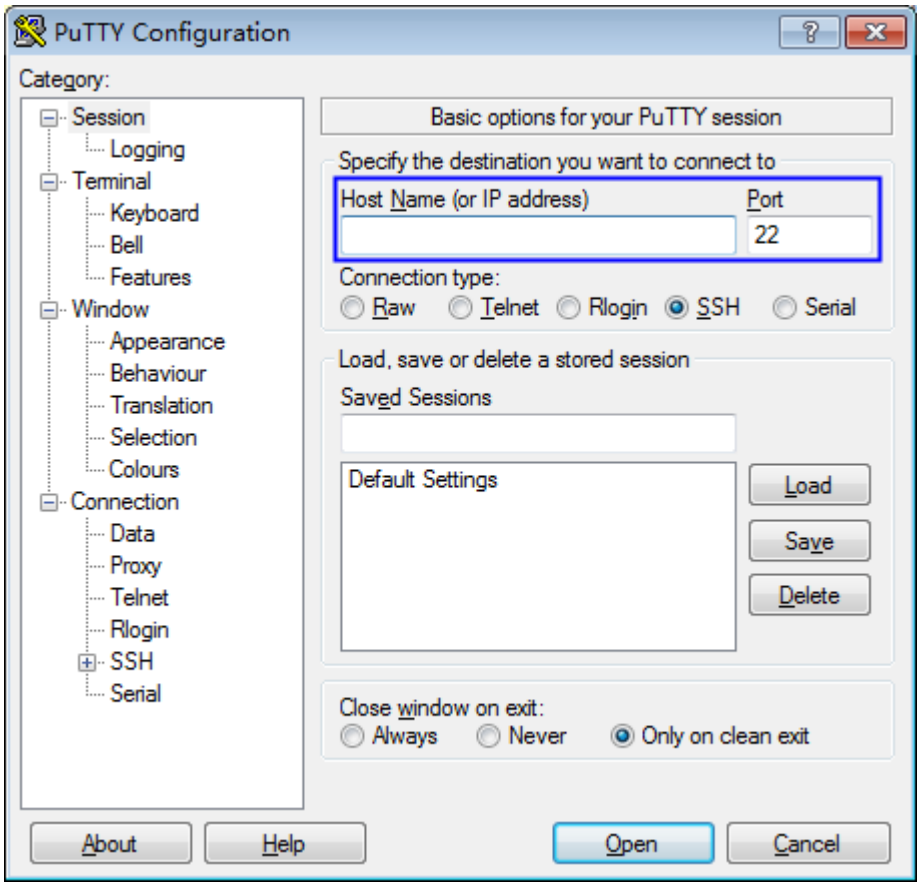
步骤2 双击“PuTTY.EXE”，打开“PuTTY Configuration”。

步骤3 选择“Connection > data”，在“Auto-login username”处输入镜像的用户名。

步骤4 选择“Connection > SSH > Auth”，在“Private key file forauthentication”配置项中，单击“Browse”，选择**步骤1**转化的私钥文件。

步骤5 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 6-11 配置弹性 IP



步骤6 单击“Open”，登录弹性云服务器。

步骤7 执行以下命令，打开“/etc/ssh/sshd_config”文件。

vi /etc/ssh/sshd_config

步骤8 按“i”进入编辑模式，开启密码方式登录。

- 非SUSE操作系统，将“PasswordAuthentication”字段值修改为“yes”。
  ```
  PasswordAuthentication yes
  ```
- SUSE操作系统，将“PasswordAuthentication”和“UsePAM”字段值修改为“yes”。
  ```
  PasswordAuthentication yes
  UsePAM yes
  ```

说明

- SUSE操作系统

  关闭密码登录需要将“PasswordAuthentication”和“UsePAM”字段值均修改为“no”。若文件中没有“PasswordAuthentication”和“UsePAM”参数，新增该参数并配置为“no”。
- 非SUSE操作系统

  关闭密码方式登录需要将“PasswordAuthentication”字段值修改为“no”。若“/etc/ssh/sshd_config”文件中没有“PasswordAuthentication”参数，新增该参数并配置为“no”。

步骤9 按“Esc”，退出编辑模式。

步骤10 输入“:wq”，按“Enter”，保存退出。

步骤11 执行以下命令，重启ssh服务，使配置生效。

service sshd restart

说明

Ubuntu14.xx版本的操作系统重启ssh服务，使用以下命令使配置生效。

service ssh restart

----结束

6.2.22 对 ECS 进行密钥对的绑定、重置或者替换操作时，失败怎么处理？

问题描述

当对弹性云服务器执行绑定、重置或者替换密钥对操作时，可能会失败，并在管理控制台显示执行失败的记录。

可能原因

1. 用户提供了错误或者失效的密码。
2. 用户提供了错误或者失效的私钥。
3. 网络发生故障。
4. 在弹性云服务器执行密钥对绑定、重置或者替换期间，用户对弹性云服务器进行关机、开启或者卸载磁盘等操作。

处理方法

说明

管理控制台上“密钥对执行失败记录”对话框中的失败记录只记录了弹性云服务器的操作历史，不会影响弹性云服务器的状态及后续操作，可单击失败记录所在行的“删除”，直接删除失败记录，或者单击“删除所有失败记录”，删除所有执行失败的记录。

步骤1 若弹性云服务器提供密码登录方式，使用密码登录弹性云服务器，检查密码是否正确。

- 正确，请执行**步骤2**。
- 错误，请提供正确的密码再次执行绑定、重置或者替换密钥对操作。

步骤2 若云服务器提供SSH密钥对登录方式，检查密钥对的私钥是否正确。

- 正确，请执行**步骤3**。
- 错误，请提供正确的私钥文件。

步骤3 检查网络是否发生故障。

- 是，请联系华为技术支持工程师查看并具体原因。
- 否，请执行**步骤4**。

步骤4 请检查执行密钥对绑定、重置或者替换操作的弹性云服务器是否可以正常开机、关机和登录使用等操作。

- 是，请再次执行密钥对的绑定、重置或者替换操作。
- 否，请联系华为技术支持工程师查看并定位原因。

----结束

6.2.23 解绑密钥对后，如果没有密码和密钥对登录 ECS，该如何处理？

问题描述

- 当用户购买弹性云服务器使用的是“密钥对方式”登录弹性云服务器时，解绑初始密钥对后，用户没有密码和密钥对登录弹性云服务器，该如何处理？
- 当用户在KMS管理控制台绑定密钥对时，勾选了“关闭密码登录方式”，解绑密钥对后，用户没有密码和密钥对登录弹性云服务器，该如何处理？

处理方法

方式一：

通过弹性云服务器界面重置密码，使用密码登录弹性云服务器，详细信息请参见《弹性云服务器用户指南》。

方式二：

将弹性云服务器关机，然后通过管理控制台重新绑定密钥对，使用密钥对登录弹性云服务器，操作步骤如下所示：

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角  ，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“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“密钥对列表”页面。

步骤5 单击“云服务器列表”，显示云服务器列表页面，如图6-12所示。

图 6-12 弹性云服务器列表

步骤6 单击目标弹性云服务器的名称，进入弹性云服务器详细信息界面。

步骤7 单击右上角“关机”，将弹性云服务器关机。

步骤8 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤9 单击“云服务器列表”，显示云服务器列表页面。

步骤10 单击目标弹性云服务器所在行的“绑定”，弹出绑定密钥对的对话框，如图6-13所示。

图 6-13 绑定密钥对

步骤11 在“新密钥对”下拉列表中，选择新的密钥对。

步骤12 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

若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。

若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，若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，操作步骤如下所示：

1. 登录弹性云服务器。
2. 执行以下命令，打开“/etc/ssh/sshd_config”文件。

   vi /etc/ssh/sshd_config
3. 按“i”进入编辑模式，开启密码登录。
   - 非SUSE操作系统，将“PasswordAuthentication”字段值修改为“yes”。
     ```
     PasswordAuthentication yes
     ```
   - SUSE操作系统，将“PasswordAuthentication”和“UsePAM”字段值修改为“yes”。
     ```
     PasswordAuthentication yes
     UsePAM yes
     ```
4. 按“Esc”，退出编辑模式。
5. 输入“:wq”，按“Enter”，保存退出。
6. 执行以下命令，重启SSH服务，使配置生效。
   - 非*Ubuntu14.xx*版本的操作系统。

     service sshd restart
   - *Ubuntu14.xx*版本的操作系统。

     service ssh restart

步骤13 请确认并勾选“该服务器使用华为云提供的公共镜像并未修改过SSH配置”。

步骤14 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15 单击“确定”，完成密钥对绑定操作，绑定完成后，可使用密钥对登录弹性云服务器。

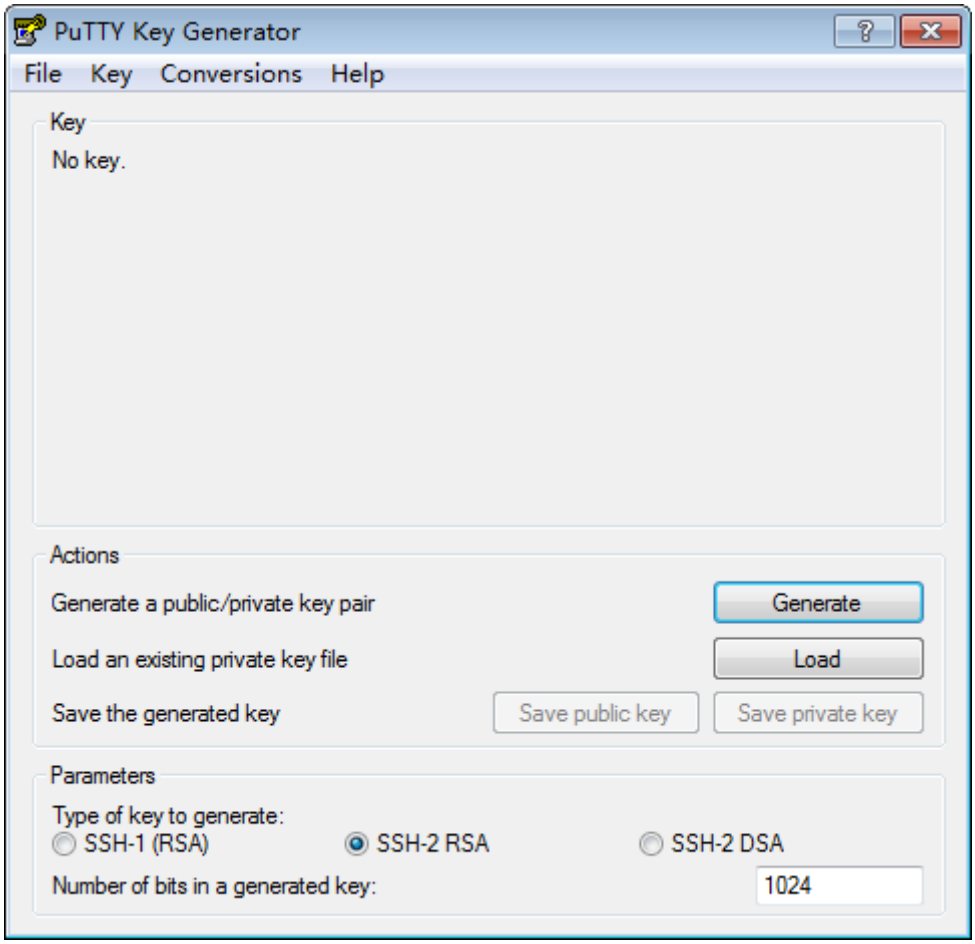
----结束

6.2.24 如何将“.ppk”格式的私钥文件转化为“.pem”格式？

上传或者拷贝至文本框的私钥必须是“.pem”格式文件，若是“.ppk”格式文件，需要通过以下步骤将“.ppk”格式文件转换为“.pem”格式文件。

1. 双击“PUTTYGEN.exe”，打开“PuTTY Key Generator”，如图6-14所示。

图 6-14 PuTTY Key Generator



2. 选择“Conversions > Import Key”导入格式为“.ppk”的私钥文件。
3. 选择“Conversions > Export OpenSSH Key”，弹出“PuTTYgen Warning”对话框。
4. 单击“是”，将文件保存为“.pem”格式文件。

6.3 地域类

6.3.1 哪些区域提供 DEW 服务？

- 密钥管理：华北-北京一、华东-上海二和华南-广州
- 密钥对管理：华北-北京一、华东-上海二、华南-广州和亚太-香港
- 专属加密：华北-北京一和华南-广州

6.4 计费类

6.4.1 如何收费和计费？

- 密钥管理的基础版实行按需计费，没有最低费用。用户创建密钥后，密钥会按小时计费。用户需要为自己创建的所有用户主密钥，以及超出免费次数的API请求支付费用。
- 密钥管理的专业版实行包年/包月付费。
- 密钥对管理的私钥不托管在华为云时，密钥对登录免费使用；私钥托管在华为云时，导入私钥成功后按照小时收费，当前阶段免费使用。
- 专属加密实例实行包年/包月付费。

详细的服务资费和费率标准，请参见**产品价格详情**。

6.4.2 密钥被禁用后，是否还计费？

计费。

禁用密钥只是数据加密服务提供的一个密钥管理功能。禁用密钥后，密钥仍然会计费。只有删除密钥，才会停止计费。

A 修订记录

发布日期	修改说明
2018-07-05	第十六次正式发布。 修改“查看专属加密实例”章节，修改专属加密实例参数说明。
2018-06-28	第十五次正式发布。 ● 修改“创建密钥”章节，增加添加标签的操作步骤。 ● 修改“导入密钥材料”章节，增加添加标签的操作步骤。 ● 根据界面变化更新截图。
2018-06-08	第十四次正式发布。 修改“导入密钥材料”章节，增加通过调用API接口获取的包装密钥转换格式的说明。

发布日期	修改说明
2018-05-25	第十三次正式发布。 ● 新增“RDS服务端加密”章节。 ● 新增“开启密钥管理”章节。 ● 新增“导入密钥”章节。 ● 新增“概述”章节。 ● 新增“导入密钥材料”章节。 ● 新增“删除密钥材料”章节。 ● 新增“密钥轮换”章节。 ● 新增“管理授权”章节。 ● 新增“创建授权”章节。 ● 新增“查询授权”章节。 ● 新增“撤销授权”章节。 ● 修改“如何使用”章节，增加“与关系型数据库配合使用”的说明。 ● 修改“与其他云服务的关系”章节，增加“与关系型数据库的关系”的说明。 ● 修改“查看专属加密实例”章节，新增基本版和专业版相关说明。
2018-05-17	第十二次正式发布。 ● 新增“使用私钥登录Linux ECS”章节。 ● 新增“使用私钥获取Windows ECS的登录密码”章节。 ● 新增“解绑密钥对”章节。 ● 新增“导入私钥”章节。 ● 新增“导出私钥”章节。 ● 修改“创建密钥对”章节，增加私钥托管的描述。 ● 修改“导入密钥对”章节，增加私钥托管的描述。 ● 修改“查看密钥对”章节，增加私钥托管的描述。 ● 修改“与其他云服务的关系”章节，新增导入私钥和导出私钥操作事件。 ● 新增以下常见问题： – 重置、替换、绑定或者解绑密钥对需要满足的条件？ – 解绑密钥对后，如果没有密码和密钥对登录ECS，该如何处理？ – 如何将“.ppk”格式的私钥文件转化为“.pem”格式？

发布日期	修改说明
2018-04-30	第十一次正式发布。 ● 新增“云审计服务支持的KMS操作列表”章节。 ● 新增“查看云审计日志”章节。 ● 新增“用户业务系统使用密码机加密”章节。 ● 新增“查看专属加密实例”章节。 ● 新增“使用专属加密实例”章节。 ● 新增以下常见问题：什么默认主密钥？
2018-04-12	第十次正式发布。 ● 新增“绑定密钥对”章节。 ● 修改“功能介绍”章节，增加绑定密钥对说明。 ● 修改“查看密钥对”章节，增加“删除失败记录”的描述。 ● 新增以下常见问题： – 绑定密钥对后，如何重新开启密码方式登录？ – 对ECS进行密钥对的绑定、重置或者替换操作时，失败怎么处理？

发布日期	修改说明
2018-03-30	第九次正式发布。 ● 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。 ● 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“重置密钥对”章节。 ● 新增“替换密钥对”章节。 ● 新增“删除密钥对”章节。 ● 修改“使用场景”，增加“登录Linux操作系统的弹性云服务器”。 ● 修改“功能介绍”，增加创建、导入和删除密钥对功能介绍。 ● 修改“如何使用”，增加与弹性云服务器配合使用的描述。 ● 修改“与其他云服务的关系”，增加与弹性云服务器的关系说明，新增添加标签、删除标签、创建和导入密钥对、删除密钥对操作事件。 ● 新增以下常见问题： – 如果用户主密钥被彻底删除，用户数据是否还可以解密？ – 如何创建密钥对？ – 导入通过PuTTYgen工具创建的密钥对失败如何处理？ – 使用IE9浏览器无法导入密钥对，该如何处理？ – 是否可以更新KMS管理的密钥？ – 如何使用SSH密钥对方式登录Linux弹性云服务器？ – 如何通过SSH密钥对的私钥文件获取Windows弹性云服务器的登录密钥？
2018-03-01	第八次正式发布。 根据界面变化更新截图。
2018-02-01	第七次正式发布。 新增“如果用户主密钥被彻底删除，用户数据是否还可以解密？”。

发布日期	修改说明
2017-12-15	第六次正式发布。 ● 新增“在线工具使用指导”章节。 ● 修改“功能介绍”章节，增加加解密小数据功能说明。 ● 删除“服务资费”章节。
2017-11-16	第五次正式发布。 ● 新增支持云硬盘。 ● 新增了“项目”的概念说明。 ● 新增了“选择项目”的操作步骤。 ● 新增以下常见问题： – 哪些区域提供KMS服务？ – KMS提供了哪些功能？ – 华为云服务如何使用KMS的加密数据？ – 信封加密方式有什么优势？ – 用户主密钥与默认主密钥有什么区别？ – 在KMS中创建用户主密钥的个数是否有限制？ – KMS中创建的用户主密钥长度是多少？ – 用户是否可以从KMS中导出用户主密钥？ ● 修改“使用场景”章节。 ● 修改“与其他云服务的关系”章节，增加云审计服务支持的KMS操作“加密数据”、“解密数据”的资源类型和事件名称。
2017-08-25	第四次正式发布。 ● “与云审计服务的关系”操作列表中新增“修改别名”、“修改密钥描述”、“密钥删除风险提示”、“退役授权”和“撤销授权”的资源类型和事件名称。 ● 新增“更改密钥别名和描述”章节。
2017-04-20	第三次正式发布。 新增“服务资费”章节。

发布日期	修改说明
2017-01-20	第二次正式发布。 ● 新增了密钥管理服务相关概念、访问与使用方法以及与其他云服务的关系。 ● 新增了密钥批量启用、禁用、删除、取消删除密钥操作描述。 ● 新增了默认主密钥说明。 ● 新增了OBS、EVS、IMS定义，并优化了使用场景相关描述。 ● 优化了SSE-KMS相关描述和“云审计服务支持的KMS操作列表”相关说明。 ● 新增了创建DEK、不含明文的DEK方法相关说明。 ● 新增了EVS、IMS与KMS的关系，如何配合使用等相关描述。 ● 新增加了私有镜像的加密方法相关说明。
2016-08-25	第一次正式发布。