密钥管理服务

接口参考（阿布扎比）

文档版本 03

发布日期 2022-11-28

华为技术有限公司

版权所有 © 华为技术有限公司 2022。 保留一切权利。

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

商标声明


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

注意

您购买的产品、服务或特性等应受华为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。

目 录

 版权所有 © 华为技术有限公司

 版权所有 © 华为技术有限公司

1 使用前必读

1.1 概述

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

您可以使用本文档提供的API对密钥进行相关操作，如创建、查询、删除密钥等。支持的全部操作请参见**API概览**。

1.2 调用说明

密钥管理服务提供了REST（Representational State Transfer）风格API，支持您通过HTTPS请求调用，调用方法请参见**如何调用API**。

1.3 终端节点

终端节点（Endpoint）即调用API的**请求地址**，不同服务不同区域的终端节点不同，您可以从**地区和终端节点**中查询所有服务的终端节点。

1.4 约束与限制

更详细的限制请参见具体API的说明。

1.5 基本概念

- 帐号

  用户注册时的帐号，帐号对其所拥有的资源及云服务具有完全的访问权限，可以重置用户密码、分配用户权限等。由于帐号是付费主体，为了确保帐号安全，建议您不要直接使用帐号进行日常管理工作，而是创建用户并使用他们进行日常管理工作。

- 用户

版权所有 © 华为技术有限公司

由帐号在IAM中创建的用户，是云服务的使用人员，具有身份凭证（密码和访问密钥）。

通常在调用API的鉴权过程中，您需要用到帐号、用户和密码等信息。

- 区域（Region）

  从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。

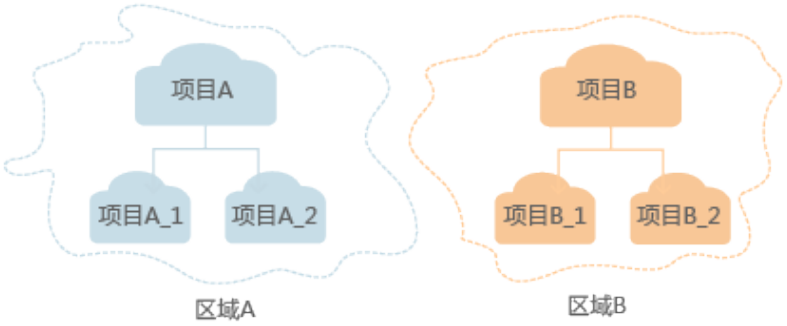
- 可用区（AZ，Availability Zone）

  一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

- 项目

  区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您帐号中该区域的所有资源。如果您希望进行更加精细的权限控制，可以在区域默认的项目中创建子项目，并在子项目中创建资源，然后以子项目为单位进行授权，使得用户仅能访问特定子项目中资源，使得资源的权限控制更加精确。

  图 1-1 项目隔离模型



- 企业项目

  企业项目是项目的升级版，针对企业不同项目间资源的分组和管理，是逻辑隔离。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。

版权所有 © 华为技术有限公司

2 如何调用 API

2.1 构造请求

本节介绍如何构造REST API的请求，并以调用IAM服务的**获取用户Token**说明如何调用API，该API获取用户的Token，Token可以用于调用其他API时鉴权。

请求 URI

请求URI由如下部分组成。

{URI-scheme} :// {Endpoint} / {resource-path} ? {query-string}

尽管请求URI包含在请求消息头中，但大多数语言或框架都要求您从请求消息中单独传递它，所以在此单独强调。

- **URI-scheme**：

  表示用于传输请求的协议，当前所有API均采用**HTTPS**协议。

- **Endpoint**：

  指定承载REST服务端点的服务器域名或IP，不同服务不同区域的Endpoint不同，您可以从**地区和终端节点**获取。

  例如IAM服务在“ae-ad-1”区域的Endpoint为“iam.ae-ad-1.myhuaweicloud.com”。

- **resource-path**：

  资源路径，也即API访问路径。从具体API的URI模块获取，例如“获取用户Token”API的resource-path为“/v3/auth/tokens”。

- **query-string**：

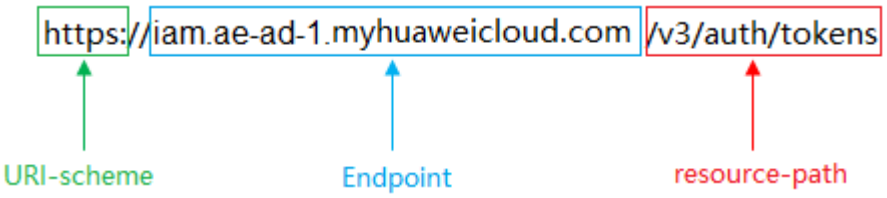
  查询参数，是可选部分，并不是每个API都有查询参数。查询参数前面需要带一个“？”，形式为“参数名=参数取值”，例如“limit=10”，表示查询不超过10条数据。

例如您需要获取IAM在“ae-ad-1”区域的Token，则需使用“ae-ad-1”区域的Endpoint（iam.ae-ad-1.myhuaweicloud.com），并在**获取用户Token**的URI部分找到resource-path（/v3/auth/tokens），拼接起来如下所示。

```
https://iam.ae-ad-1.myhuaweicloud.com/v3/auth/tokens
```


版权所有 © 华为技术有限公司

图 2-1 URI 示意图



说明

为查看方便，在每个具体API的URI部分，只给出resource-path部分，并将请求方法写在一起。这是因为URI-scheme都是HTTPS，同一个服务的Endpoint在同一个区域也相同，所以简洁起见将这两部分省略。

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务你正在请求什么类型的操作。

- **GET**：请求服务器返回指定资源。
- **PUT**：请求服务器更新指定资源。
- **POST**：请求服务器新增资源或执行特殊操作。
- **DELETE**：请求服务器删除指定资源，如删除对象等。
- **HEAD**：请求服务器资源头部。
- **PATCH**：请求服务器更新资源的部分内容。当资源不存在的时候，PATCH可能会去创建一个新的资源。

在**获取用户Token**的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://iam.ae-ad-1.myhuaweicloud.com/v3/auth/tokens
```

请求消息头

附加请求头字段，如指定的URI和HTTP方法所要求的字段。例如定义消息体类型的请求头“Content-Type”，请求鉴权信息等。

如下公共消息头需要添加到请求中。

- **Content-Type**：消息体的类型（格式），必选，默认取值为“application/json”，有其他取值时会在具体接口中专门说明。
- **X-Auth-Token**：用户Token，可选，当使用Token方式认证时，必须填充该字段。用户Token也就是调用**获取用户Token**接口的响应值，该接口是唯一不需要认证的接口。

  说明

  API同时支持使用AK/SK认证，AK/SK认证是使用SDK对请求进行签名，签名过程会自动往请求中添加Authorization（签名认证信息）和X-Sdk-Date（请求发送的时间）请求头。

  AK/SK认证的详细说明请参见**AK/SK认证**。

对于**获取用户Token**接口，由于不需要认证，所以只添加“Content-Type”即可，添加消息头后的请求如下所示。

```
POST https://iam.ae-ad-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```


版权所有 © 华为技术有限公司

请求消息体

请求消息体通常以结构化格式发出，与请求消息头中Content-type对应，传递除请求消息头之外的内容。若请求消息体中参数支持中文，则中文字符必须为UTF-8编码。

每个接口的请求消息体内容不同，也并不是每个接口都需要有请求消息体（或者说消息体为空），GET、DELETE操作类型的接口就不需要消息体，消息体具体内容需要根据具体接口而定。

对于**获取用户Token**接口，您可以从接口的请求部分看到所需的请求参数及参数说明。将消息体加入后的请求如下所示，加粗的斜体字段需要根据实际值填写，其中***username***为用户名，***domainname***为用户所属的帐号名称，*********为用户登录密码，***xxxxxxxxxxxxxxxxxx***为project的名称，您可以从**地区和终端节点**获取。

说明

scope参数定义了Token的作用域，下面示例中获取的Token仅能访问project下的资源。您还可以设置Token作用域为某个帐号下所有资源或帐号的某个project下的资源，详细定义请参见**获取用户Token**。

```
POST https://iam.ae-ad-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json

{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxxxxxxxxxxxx"
            }
        }
    }
}
```

到这里为止这个请求需要的内容就具备齐全了，您可以使用**curl**、**Postman**或直接编写代码等方式发送请求调用API。对于获取用户Token接口，返回的响应消息头中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

2.2 认证鉴权

调用接口有如下两种认证方式，您可以选择其中一种进行认证鉴权。

- Token认证：通过Token认证调用请求。
- AK/SK认证：通过AK（Access Key ID）/SK（Secret Access Key）加密调用请求。推荐使用AK/SK认证，其安全性比Token认证要高。

版权所有 © 华为技术有限公司

Token 认证

> **说明**
>
> Token的有效期为24小时，需要使用一个Token鉴权时，可以先缓存起来，避免频繁调用。

Token在计算机系统中代表令牌（临时）的意思，拥有Token就代表拥有某种权限。Token认证就是在调用API的时候将Token加到请求消息头，从而通过身份认证，获得操作API的权限。

Token可通过调用**获取用户Token**接口获取，调用本服务API需要project级别的Token，即调用**获取用户Token**接口时，请求body中auth.scope的取值需要选择project，如下所示。

```
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxx"
            }
        }
    }
}
```

获取Token后，再调用其他接口时，您需要在请求消息头中添加“X-Auth-Token”，其值即为Token。例如Token值为“ABCDEFJ....”，则调用接口时将“X-Auth-Token: ABCDEFJ....”加到请求消息头即可，如下所示。

```
POST https://iam.ae-ad-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK 认证

> **说明**
>
> AK/SK签名认证方式仅支持消息体大小12MB以内，12MB以上的请求请使用Token认证。

AK/SK认证就是使用AK/SK对请求进行签名，在请求时将签名信息添加到消息头，从而通过身份认证。

- AK(Access Key ID)：访问密钥ID。与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
- SK(Secret Access Key)：与访问密钥ID结合使用的密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

使用AK/SK认证时，您可以基于签名算法使用AK/SK对请求进行签名，也可以使用专门的签名SDK对请求进行签名。详细的签名方法和SDK使用方法请参见**API签名指南**。

版权所有 © 华为技术有限公司

须知

签名SDK只提供签名功能，与服务提供的SDK不同，使用时请注意。

2.3 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

状态码是一组从1xx到5xx的数字代码，状态码表示了请求响应的状态，完整的状态码列表请参见**状态码**。

对于**获取用户Token**接口，如果调用后返回状态码为“201”，则表示请求成功。

响应消息头

对应请求消息头，响应同样也有消息头，如“Content-type”。

对于**获取用户Token**接口，返回如**图2-2**所示的消息头，其中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

图 2-2 获取用户 Token 响应消息头

响应消息体（可选）

响应消息体通常以结构化格式返回，与响应消息头中Content-type对应，传递除响应消息头之外的内容。

对于**获取用户Token**接口，返回如下消息体。为篇幅起见，这里只展示部分内容。

```
{
    "token": {
        "expires_at": "2019-02-13T06:52:13.855000Z",
```


版权所有 © 华为技术有限公司

```
        "methods": [
            "password"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "region_id": "xxxxxxxx",
.....
```

当接口调用出错时，会返回错误码及错误信息说明，错误响应的Body体格式如下所示。

```
{
    "error": {
        "message": "The request you have made requires authentication.",
        "title": "Unauthorized"
    }
}
```

其中，error_code表示错误码，error_msg表示错误描述信息。

版权所有 © 华为技术有限公司

3 API 概览

通过使用密钥管理服务提供的接口，您可以完整的使用密钥管理服务的所有功能。

管理加密密钥

API	说明
创建密钥	创建一个用户主密钥。
启用密钥	启用密钥，密钥启用后才可以使用。
禁用密钥	禁用密钥，密钥禁用后不可以使用。
计划删除密钥	计划删除一个指定密钥，可设置7天～1096天内删除密钥。密钥将被彻底删除后，使用该密钥加密的数据将无法解密。
取消计划删除密钥	取消计划删除密钥，取消后，用户可以正常使用该密钥。
查询密钥列表	查询用户所有密钥列表。
查询密钥信息	查询指定密钥的详细信息。
创建随机数	生成8~8192bit范围内的随机数，且须为8的倍数。
创建数据密钥	创建数据密钥，返回结果包含明文和密文。
创建不含明文数据密钥	创建数据密钥，返回结果只包含密文。
加密数据密钥	使用指定的用户主密钥加密数据密钥。
解密数据密钥	使用指定的用户主密钥解密数据密钥。
查询实例数	获取用户已经创建的用户主密钥数量，不包含默认主密钥。
查询配额	查询用户可以创建的用户主密钥配额总数及当前使用量信息，不包含默认主密钥。
修改密钥别名	修改用户主密钥别名。
修改密钥描述	修改用户主密钥描述信息。

版权所有 © 华为技术有限公司

API	说明
加密数据	使用指定的用户主密钥加密数据。
解密数据	解密数据。
获取密钥导入参数	获取导入密钥的必要参数，包括密钥导入令牌和密钥加密公钥。
导入密钥材料	导入指定密钥的密钥材料。
查询密钥实例	通过标签过滤，查询指定用户主密钥的详细信息。
查询密钥标签	查询指定密钥的标签信息。
查询项目标签	查询用户在指定项目下的所有标签集合。
批量添加删除密钥标签	批量添加或删除密钥标签。
添加密钥标签	添加密钥标签。

版权所有 © 华为技术有限公司

4 API 说明

4.1 管理密钥

4.1.1 创建密钥

功能介绍

创建用户主密钥，可用来加密数据密钥。

说明

别名“/default”为服务默认主密钥的后缀名，由服务自动创建。因此用户创建的主密钥别名不能与服务默认主密钥的别名相同，即后缀名不能为“/default”。

对于开通企业项目的用户，服务默认主密钥属于且只能属于默认企业项目下，且不支持企业资源的迁入迁出。服务默认主密钥为用户提供基础的云上加密功能，满足合规要求。因此，在企业多项目下，其他非默认企业项目下的用户均可使用该密钥。若客户有企业管理资源诉求，请自行创建和使用密钥。

URI

- URI格式

  POST /v1.0/{project_id}/kms/create-key

- 参数说明

  表 4-1 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

版权所有 © 华为技术有限公司

请求消息

表 4-2 请求参数

参数	是否必选	参数类型	描述
key_alias	是	String	非默认主密钥别名，取值范围为1到255个字符，满足正则匹配“^[a-zA-Z0-9:/_-]{1,255}$”，且不与系统服务创建的默认主密钥别名重名。
enterprise_project_id	否	String	企业多项目ID。 ● 用户未开通企业多项目时，不需要输入该字段。 ● 用户开通企业多项目时，创建资源可以输入该字段。 若用户不输入该字段，默认创建属于默认企业多项目ID（ID为“0”）的资源。 注意：若用户没有默认企业多项目ID（ID为“0”）下的创建权限，则接口报错。
key_description	否	String	密钥描述，取值0到255字符。
origin	否	String	密钥来源，默认为“kms”，枚举如下： ● kms：表示密钥材料由kms生成。 ● external：表示密钥材料由外部导入。
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-3 响应参数

参数	是否必选	参数类型	描述
key_info	是	Array of objects	密钥信息，详情请参见表4-4。

表 4-4 key_info 字段结构说明

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。
domain_id	是	String	用户域ID。

版权所有 © 华为技术有限公司

示例

如下以创建别名为“test”的密钥为例。

- 请求样例

```
{
   "key_alias": "test"
}
```

- 响应样例

```
{
   "key_info": {
      "key_id": "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
      "domain_id": "b168fe00ff56492495a7d22974df2d0b"
   }
}
```

或

```
{
   "error": {
      "error_code": "KMS.XXXX",
      "error_msg": "XXX"
   }
}
```

状态码

表4-5描述的是API返回的正常状态码。

表 4-5 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.2 启用密钥

功能介绍

启用密钥，密钥启用后才可以使用。

说明

密钥为禁用状态才能启用密钥。

URI

- URI格式

  POST /v1.0/{project_id}/kms/enable-key

- 参数说明

版权所有 © 华为技术有限公司

表 4-6 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

表 4-7 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-8 响应参数

参数	是否必选	参数类型	描述
key_info	是	Array of objects	密钥信息，详情请参见表4-9。

表 4-9 key_info 字段结构说明

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。
key_state	是	String	密钥状态： • 2为启用状态 • 3为禁用状态 • 4为计划删除状态

示例

如下以启用密钥ID为“0d0466b0-e727-4d9c-b35d-f84bb474a37f”的密钥为例。

版权所有 © 华为技术有限公司

- 请求样例

```
{
    "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

- 响应样例

```
{
    "key_info": {
        "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
        "key_state": "2"
    }
}
```

或

```
{
    "error": {
        "error_code": "KMS.XXXX",
        "error_msg": "XXX"
    }
}
```

状态码

表4-10描述的是API返回的正常状态码。

表 4-10 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.3 禁用密钥

功能介绍

禁用密钥，密钥禁用后不可以使用。

说明

密钥为启用状态才能禁用密钥。

URI

- URI格式

  POST /v1.0/{project_id}/kms/disable-key

- 参数说明

表 4-11 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

版权所有 © 华为技术有限公司

请求消息

表 4-12 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-13 响应参数

参数	是否必选	参数类型	描述
key_info	是	Array of objects	密钥信息，详情请参见表4-14。

表 4-14 key_info 字段结构说明

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。
key_state	是	String	密钥状态： • 2为启用状态 • 3为禁用状态 • 4为计划删除状态

示例

如下以禁用密钥ID为“0d0466b0-e727-4d9c-b35d-f84bb474a37f”的密钥为例。

- 请求样例

```
{
    "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

- 响应样例

```
{
    "key_info": {
```


版权所有 © 华为技术有限公司

```
        "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
        "key_state": "3"
    }
}
```

或

```
{
    "error": {
        "error_code": "KMS.XXXX",
        "error_msg": "XXX"
    }
}
```

状态码

表4-15描述的是API返回的正常状态码。

表 4-15 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.4 计划删除密钥

功能介绍

计划多少天后删除密钥，可设置7天～1096天内删除密钥。

URI

- URI格式
  POST /v1.0/{project_id}/kms/schedule-key-deletion
- 参数说明

  表 4-16 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

版权所有 © 华为技术有限公司

请求消息

表 4-17 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
pending_days	是	String	计划多少天后删除密钥，取值为7到1096。
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-18 响应参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。
key_state	是	String	密钥状态： ● 2为启用状态 ● 3为禁用状态 ● 4为计划删除状态

示例

如下以删除密钥ID为“0d0466b0-e727-4d9c-b35d-f84bb474a37f”的密钥为例。

- 请求样例

```
{
   "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
   "pending_days": "7"
}
```

- 响应样例

```
{
   "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
   "key_state": "4"
}
```

或

```
{
   "error": {
```


版权所有 © 华为技术有限公司

```
    "error_code": "KMS.XXXX",
    "error_msg": "XXX"
  }
}
```

状态码

表4-19描述的是API返回的正常状态码。

表 4-19 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.5 取消计划删除密钥

功能介绍

取消计划删除密钥。

说明

密钥处于“计划删除”状态才能取消计划删除密钥。

URI

- URI格式
  POST /v1.0/{project_id}/kms/cancel-key-deletion
- 参数说明

  表 4-20 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

版权所有 © 华为技术有限公司

请求消息

表 4-21 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥id，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-22 响应参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。
key_state	是	String	密钥状态： ● 2为启用状态 ● 3为禁用状态 ● 4为计划删除状态

示例

如下以取消删除密钥ID为“0d0466b0-e727-4d9c-b35d-f84bb474a37f”的密钥为例。

- 请求样例

```
{
   "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

- 响应样例

```
{
   "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
   "key_state": "3"
}
```

或

```
{
   "error": {
      "error_code": "KMS.XXXX",
      "error_msg": "XXX"
   }
}
```


版权所有 © 华为技术有限公司

状态码

表4-23描述的是API返回的正常状态码。

表 4-23 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.6 查询密钥列表

功能介绍

查询用户所有密钥列表。

URI

- URI格式
  POST /v1.0/{project_id}/kms/list-keys
- 参数说明

表 4-24 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

表 4-25 请求参数

参数	是否必选	参数类型	描述
limit	否	String	指定查询返回记录条数，如果指定查询记录条数小于存在的条数，响应参数“truncated”将返回“true”，表示存在分页。取值在密钥最大个数范围以内。例如：100
marker	否	String	分页查询起始位置标识。分页查询收到的响应参数“truncated”为“true”时，可以发送连续的请求获取更多的记录条数，“marker”设置为响应的next_marker的值。例如：10

版权所有 © 华为技术有限公司

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业多项目ID。 • 用户未开通企业多项目时，不需要输入该字段。 • 用户开通企业多项目时，查询资源可以输入该字段。 若用户不输入该字段，默认查询租户所有有权限的企业多项目下的资源。此时“enterprise_project_id”取值为“all”。 若用户输入该字段，取值满足以下任一条件。 – 取值为“all” – 取值为“0” – 满足正则匹配：“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”
key_state	否	String	密钥状态，满足正则匹配“^[1-5]{1}$”，枚举如下： • “1”表示待激活状态 • “2”表示启用状态 • “3”表示禁用状态 • “4”表示计划删除状态 • “5”表示等待导入状态
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-26 响应参数

参数	是否必选	参数类型	描述
keys	是	Array of strings	key_id列表。
key_details	是	Array of objects	密钥详情列表，详情请参见**表4-31**。
next_marker	是	String	获取下一页所需要传递的“marker”值。当“truncated”为“false”时，“next_marker”为空。

版权所有 © 华为技术有限公司

参数	是否必选	参数类型	描述
total	是	Integer	密钥总条数。
truncated	是	String	是否还有下一页： ● “true”表示还有数据。 ● “false”表示已经是最后一页。

示例

如下以查询返回记录条数为“2”，分页为“1”为例。

- 请求样例

```
{
   "limit": "2",
   "marker": "1"
}
```

- 响应样例

```
{
   "keys": [
      "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
      "2e258389-bb1e-4568-a1d5-e1f50adf70ea"
   ],
   "key_details": [
      {
      "key_id":"0d0466b0-e727-4d9c-b35d-f84bb474a37f",
      "domain_id":"00074811d5c27c4f8d48bb91e4a1dcfd",
      "key_alias":"caseuirpr",
      "realm":"aaaa",
      "key_description":"123",
      "creation_date":"1502799822000",
      "scheduled_deletion_date":"",
      "key_state":"2",
      "default_key_flag":"0",
      "key_type":"1",
      "expiration_time":"1501578672000",
      "origin":"kms"
},
      {
      "key_id":"2e258389-bb1e-4568-a1d5-e1f50adf70ea",
      "domain_id":"00074811d5c27c4f8d48bb91e4a1dcfd",
      "key_alias":"casehvniz",
      "realm":"aaaa",
      "key_description":"234",
      "creation_date":"1502799820000",
      "scheduled_deletion_date":"",
      "key_state":"2",
      "default_key_flag":"0",
      "key_type":"1",
      "expiration_time":"1501578673000",
      "origin":"kms"
}
    ],
   "next_marker": "",
   "truncated": "false",
   "total":2
}
```

或

```
{
   "error": {
      "error_code": "KMS.XXXX",
```


版权所有 © 华为技术有限公司

```
    "error_msg": "XXX"
  }
}
```

状态码

表4-27描述的是API返回的正常状态码。

表 4-27 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见**状态码**。

4.1.7 查询密钥信息

功能介绍

查询密钥详细信息。

URI

- URI格式
  POST /v1.0/{project_id}/kms/describe-key
- 参数说明

  表 4-28 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

表 4-29 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f

版权所有 © 华为技术有限公司

参数	是否必选	参数类型	描述
sequence	否	String	请求消息序列号，36字节序列号。 例如： 919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-30 响应参数

参数	是否必选	参数类型	描述
key_info	是	Array of objects	密钥信息，详情请参见表4-31。

表 4-31 key_info 字段结构说明

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。
domain_id	是	String	用户域ID。
key_alias	是	String	密钥别名。
realm	是	String	密钥区域。
key_description	是	String	密钥描述。
creation_date	是	String	密钥创建时间，时间戳，即从1970年1月1日至该时间的总秒数。
scheduled_deletion_date	是	String	密钥计划删除时间，时间戳，即从1970年1月1日至该时间的总秒数。
key_state	是	String	密钥状态： • “1”表示待激活状态 • “2”表示启用状态 • “3”表示禁用状态 • “4”表示计划删除状态 • “5”表示等待导入状态
default_key_flag	是	String	默认主密钥标识，默认主密钥标识为1，非默认标识为0。
key_type	是	String	密钥类型。

版权所有 © 华为技术有限公司

参数	是否必选	参数类型	描述
origin	是	String	密钥来源，默认为“kms”，枚举如下：
sys_enterprise_project_id	是	String	企业项目ID，默认为“0”。 对于开通企业项目的用户，表示资源处于默认企业项目下。 对于未开通企业项目的用户，表示资源未处于企业项目下。

示例

如下以查询密钥ID为“0d0466b0-e727-4d9c-b35d-f84bb474a37f”为例。

- 请求样例

```
{
   "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

- 响应样例

```
{
   "key_info": {
      "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
      "domain_id": "b168fe00ff56492495a7d22974df2d0b",
      "key_alias": "kms_test",
      "realm": "aaa",
      "key_description": "",
      "creation_date": "1472442386000",
      "scheduled_deletion_date": "",
      "key_state": "2",
      "default_key_flag": "0",
      "key_type": "1",
      "expiration_time":"1501578672000",
      "origin":"kms"
      ,
      "sys_enterprise_project_id ": "0",
   }
}
```

或

```
{
   "error": {
      "error_code": "KMS.XXXX",
      "error_msg": "XXX"
   }
}
```

状态码

表4-32描述的是API返回的正常状态码。

表 4-32 状态码

状态码	编码	状态说明
200	OK	请求已成功。

版权所有 © 华为技术有限公司

异常状态码，请参见**状态码**。

4.1.8 创建随机数

功能介绍

生成8~8192bit范围内的随机数。

URI

- URI格式
  POST /v1.0/{project_id}/kms/gen-random
- 参数说明

表 4-33 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

表 4-34 请求参数

参数	是否必选	参数类型	描述
random_data_length	是	String	取值为8的倍数，取值范围为8~8192。
sequence	否	String	请求消息序列号，36字节序列号。 例如： 919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-35 响应参数

参数	是否必选	参数类型	描述
random_data	是	String	随机数16进制表示，两位表示1byte。随机数的长度与用户传入的参数“random_data_length”的长度保持一致。

版权所有 © 华为技术有限公司

示例

如下以创建长度“512”bit的随机数为例。

- 请求样例

```
{
   "random_data_length": "512"
}
```

- 响应样例

```
{
   "random_data":
"5791C223E87124AB9FC29B5A8AC60BE4B98D168F47A58BB2A88833E40D6ED32D57E2AAB5410492EB
25096873F9CE3D45E0D22F820A5AB4EEADC33A1A6AE780F1"
}
```

或

```
{
   "error": {
      "error_code": "KMS.XXXX",
      "error_msg": "XXX"
   }
}
```

状态码

表4-36描述的是API返回的正常状态码。

表 4-36 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.9 创建数据密钥

功能介绍

创建数据密钥，返回结果包含明文和密文。

URI

- URI格式

  POST /v1.0/{project_id}/kms/create-datakey

- 参数说明

表 4-37 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

版权所有 © 华为技术有限公司

请求消息

表 4-38 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$”。例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f。
encryption_context	否	Object	一系列key-value键值对，用于记录资源上下文信息，用于保护数据的完整性，不应包含敏感信息，最大长度为8192。 当在加密时指定了该参数时，解密密文时，需要传入相同的参数，才能正确的解密。 例如： {"Key1":"Value1","Key2":"Value2"}
datakey_length	否	String	密钥bit位长度。 取值为8的倍数，取值范围为8~8192。
sequence	否	String	请求消息序列号，36字节序列号。 例如： 919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-39 响应参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。
plain_text	是	String	DEK明文16进制，两位表示1byte。
cipher_text	是	String	DEK密文16进制，两位表示1byte。

示例

如下以创建密钥ID为“0d0466b0-e727-4d9c-b35d-f84bb474a37f”，密钥长度为“512”bit的数据密钥为例。

- 请求样例

```
{
    "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    "datakey_length": "512"
}
```


版权所有 © 华为技术有限公司

- 响应样例

```
{
    "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    "plain_text":
"8151014275E426C72EE7D44267EF11590DCE0089E19863BA8CC832187B156A72A5A17F17B5EF0D525
872C59ECEB72948AF85E18427F8BE0D46545C979306C08D",
    "cipher_text":
"020098009EEAFCE122CAA5927D2E020086F9548BA1675FDB022E4ECC01B96F2189CF4B85E78357E73
E1CEB518DAF7A4960E7C7DE8885ED3FB2F1471ABF400119CC1B20BD3C4A9B80AF590EFD0AEDABFDB
B0E2B689DA7B6C9E7D3C5645FCD9274802586BE63779471F9156F2CDF07CD8412FFBE923064303436
3662302D653732372D346439632D623335642D663834626234373461333766000000045B05321483B
D9F9561865EE7DFE9BE267A42EB104E98C16589CE46940B18E52"
}
```

或

```
{
    "error": {
        "error_code": "KMS.XXXX",
        "error_msg": "XXX"
    }
}
```

状态码

表4-40描述的是API返回的正常状态码。

表 4-40 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.10 创建不含明文数据密钥

功能介绍

创建不含明文数据密钥，返回结果只包含密文。

URI

- URI格式

  POST /v1.0/{project_id}/kms/create-datakey-without-plaintext

- 参数说明

表 4-41 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

版权所有 © 华为技术有限公司

请求消息

表 4-42 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
encryption_context	否	Object	一系列key-value键值对，用于记录资源上下文信息，用于保护数据的完整性，不应包含敏感信息，最大长度为8192。 当在加密时指定了该参数时，解密密文时，需要传入相同的参数，才能正确的解密。 例如：{"Key1":"Value1","Key2":"Value2"}
datakey_length	否	String	密钥bit位长度。 取值为8的倍数，取值范围为8~8192。
key_spec	否	String	指定生成的密钥bit位长度。 有效值：AES_256、AES_128。 ● AES_256：表示256比特的对称密钥。 ● AES_128：表示128比特的对称密钥。 **说明** datakey_length和key_spec二选一。 ● 若datakey_length和key_spec都为空，默认生成256bit的密钥。 ● 若datakey_length和key_spec都指定了值，仅datakey_length生效。
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-43 响应参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。

版权所有 © 华为技术有限公司

参数	是否必选	参数类型	描述
cipher_text	是	String	DEK密文16进制，两位表示1byte。

示例

如下以创建密钥ID为“0d0466b0-e727-4d9c-b35d-f84bb474a37f”的不含明文数据密钥为例。

- 请求样例

```
{
    "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    "datakey_length": "512"
}
```

- 响应样例

```
{
    "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    "cipher_text":
"020098005CDC28E29EC3230AA42E8985FBABA095037D6474C64519C9B564AB28B15739C88E7E887500D1094973C2DC16353DB7ED3946C73339517AB1E983D521F9E9D700DC5D9C42F557EBF3F608E3CBBEE0BC68136EE7D2A49117E00332BAC4AE4ED805EB6068FA900C5A8019BFE2C2651BE3E130643034363662302D653732372D346439632D623335642D663834626234373461333766000000000F160727EBDB83400C21D80D713B49D3A2C37F24AE160E7BB3DAC025ADC0C45E3"
}
```

或

```
{
    "error": {
        "error_code": "KMS.XXXX",
        "error_msg": "XXX"
    }
}
```

状态码

表4-44描述的是API返回的正常状态码。

表 4-44 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.11 加密数据密钥

功能介绍

加密数据密钥，用指定的主密钥加密数据密钥。

版权所有 © 华为技术有限公司

URI

- URI格式
  POST /v1.0/{project_id}/kms/encrypt-datakey
- 参数说明

表 4-45 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

表 4-46 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
encryption_context	否	Object	一系列key-value键值对，用于记录资源上下文信息，用于保护数据的完整性，不应包含敏感信息，最大长度为8192。 当在加密时指定了该参数时，解密密文时，需要传入相同的参数，才能正确的解密。 例如： {"Key1":"Value1","Key2":"Value2"}
plain_text	是	String	DEK明文以及DEK明文的摘要（SHA256算法生成的32字节的字符串）拼接而成的16进制字符串。 具体请参见**示例**。
datakey_plain_length	是	String	DEK明文字节长度，取值范围为1~1024。
sequence	否	String	请求消息序列号，36字节序列号。 例如： 919c82d4-8046-4722-9094-35c3c6524cff

版权所有 © 华为技术有限公司

响应消息

表 4-47 响应参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。
cipher_text	是	String	DEK密文16进制，两位表示1byte。
datakey_length	是	String	DEK字节长度。

示例

如下以密钥ID为“0d0466b0-e727-4d9c-b35d-f84bb474a37f”的用户主密钥生成的512bit的数据密钥明文值为“7549d9aea901767bf3c0b3e14b10722eaf6f59053bbd82045d04e075e809a0fe6ccab48f8e5efe74e4b18ff0512525e527b10331100f357bf42125d8d5ced94f”，该数据密钥明文可通过调用**创建数据密钥**接口得到。

该数据密钥明文的摘要为“fbc8ac72b0785ca7fe33eb6776ce3990b11e32b299d9c0a9ee0305fb9540f797”，计算摘要的方法如下所示：

```
//计算摘要
public static byte[] sha256(byte[] cmkData) {
    byte[] digest = new byte[0];
   try {
       MessageDigest md = MessageDigest.getInstance("SHA-256");
         md.update(cmkData);
        digest = md.digest();
     } catch (Exception e) {
        System.out.println("calculate digest failure, exception is " + e.toString());
    }
     return digest;
}
//将所得的摘要，转换成十六进制字符串
public static String bytesToHexString(byte[] digest) {
        ...
}
```

加密明文数据密钥明文值（**plain_text**参数），为数据密钥明文及其摘要拼接而成的十六进制字符串为“7549d9aea901767bf3c0b3e14b10722eaf6f59053bbd82045d04e075e809a0fe6ccab48f8e5efe74e4b18ff0512525e527b10331100f357bf42125d8d5ced94f
fbc8ac72b0785ca7fe33eb6776ce3990b11e32b299d9c0a9ee0305fb9540f797”

- 请求样例

  ```
  {
     "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
     "plain_text":
  "7549d9aea901767bf3c0b3e14b10722eaf6f59053bbd82045d04e075e809a0fe6ccab48f8e5efe74e4b18ff
  0512525e527b10331100f357bf42125d8d5ced94f
  fbc8ac72b0785ca7fe33eb6776ce3990b11e32b299d9c0a9ee0305fb9540f797",
     "datakey_plain_length": "64"
  }
  ```

- 响应样例

  ```
  {
     "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  ```


版权所有 © 华为技术有限公司

```
    "cipher_text":
"020098005273E14E6E8E95F5463BECDC27E80AF820B9FC086CB47861899149F67CF07DAFF2810B7D2
7BDF19AB7632488E0926A48DB2FC85BEA905119411B46244C5E6B8036C60A0B0B4842FFE6994518E89
C19B1C1D688D9043BCD6053EA7BA0652642CE59F2543C80669139F4F71ABB9BD9A243306430343636
62302D653732372D346439632D623335642D663834626234373461333766000000000D34457984F9730
D57F228C210FD22CA6017913964B21D4ECE45D81092BB9112E",
    "datakey_length": "64"
}
```


或


```
{
    "error": {
        "error_code": "KMS.XXXX",
        "error_msg": "XXX"
    }
}
```


状态码

表4-48描述的是API返回的正常状态码。

表 4-48 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.12 解密数据密钥

功能介绍

解密数据密钥，用指定的主密钥解密数据密钥。

说明

解密的数据为加密数据中的结果。

URI

- URI格式

  POST /v1.0/{project_id}/kms/decrypt-datakey
- 参数说明

表 4-49 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

版权所有 © 华为技术有限公司

请求消息

表 4-50 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
encryption_context	否	Object	一系列key-value键值对，用于记录资源上下文信息，用于保护数据的完整性，不应包含敏感信息，最大长度为8192。 当在加密时指定了该参数时，解密密文时，需要传入相同的参数，才能正确的解密。 例如： {"Key1":"Value1","Key2":"Value2"}
cipher_text	是	String	DEK密文及元数据的16进制字符串。取值为加密数据密钥结果中的cipher_text的值。
datakey_cipher_length	是	String	密钥字节长度，取值范围为1~1024。
sequence	否	String	请求消息序列号，36字节序列号。 例如： 919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-51 响应参数

参数	是否必选	参数类型	描述
data_key	是	String	DEK明文的16进制字符串。
datakey_length	是	String	DEK明文字节长度。
datakey_dgst	是	String	DEK明文的SHA256值对应的16进制字符串。

示例

如下以密钥ID为“0d0466b0-e727-4d9c-b35d-f84bb474a37f”的用户主密钥解密密钥字节长度为64字节，密文数据密钥为

版权所有 © 华为技术有限公司

“020098005273E14E6E8E95F5463BECDC27E80AF820B9FC086CB47861899149F67CF07DAFF2810B7D27BDF19AB7632488E0926A48DB2FC85BEA905119411B46244C5E6B8036C60A0B0B4842FFE6994518E89C19B1C1D688D9043BCD6053EA7BA0652642CE59F2543C80669139F4F71ABB9BD9A24330643034363662302D653732372D346439632D623335642D6638346262343734613376600000000D34457984F9730D57F228C210FD22CA6017913964B21D4ECE45D81092BB9112E”的数据密钥为例。

- 请求样例


```
{
    "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    "datakey_cipher_length": "64",
    "cipher_text":
"020098005273E14E6E8E95F5463BECDC27E80AF820B9FC086CB47861899149F67CF07DAFF2810B7D27BDF19AB7632488E0926A48DB2FC85BEA905119411B46244C5E6B8036C60A0B0B4842FFE6994518E89C19B1C1D688D9043BCD6053EA7BA0652642CE59F2543C80669139F4F71ABB9BD9A24330643034363662302D653732372D346439632D623335642D6638346262343734613376600000000D34457984F9730D57F228C210FD22CA6017913964B21D4ECE45D81092BB9112E"
}
```


- 响应样例


```
{
    "data_key":
"00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000",
    "datakey_length": "64",
    "datakey_dgst": "F5A5FD42D16A20302798EF6ED309979B43003D2320D9F0E8EA9831A92759FB4B"
}
```


或


```
{
    "error": {
        "error_code": "KMS.XXXX",
        "error_msg": "XXX"
    }
}
```


状态码

表4-52描述的是API返回的正常状态码。

表 4-52 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.13 查询实例数

功能介绍

查询实例数，获取用户已经创建的用户主密钥数量。

说明

用户已经创建的用户主密钥不包括服务自动创建的默认主密钥。

URI

- URI格式

  GET /v1.0/{project_id}/kms/user-instances

- 参数说明

  表 4-53 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

无

响应消息

表 4-54 响应参数

参数	是否必选	参数类型	描述
instance_num	是	Integer	非默认用户主密钥个数。

示例

- 请求样例

  无

- 响应样例

```
{
   "instance_num": 15
}
```

  或

```
{
   "error": {
      "error_code": "KMS.XXXX",
      "error_msg": "XXX"
   }
}
```

状态码

表4-55描述的是API返回的正常状态码。

表 4-55 状态码

状态码	编码	状态说明
200	OK	请求已成功。

版权所有 © 华为技术有限公司

异常状态码，请参见**状态码**。

4.1.14 查询配额

功能介绍

查询配额，查询用户可以创建的用户主密钥配额总数及当前使用量信息。

说明

用户可以创建的用户主密钥配额不包括服务自动创建的默认主密钥数量。

URI

- URI格式
  GET /v1.0/{project_id}/kms/user-quotas
- 参数说明

表 4-56 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

无

响应消息

表 4-57 响应参数

参数	是否必选	参数类型	描述
quotas	是	Object	配额列表，详情请参见**表4-58**。

表 4-58 quotas 字段数据结构说明

参数	是否必选	参数类型	描述
resources	是	Array of objects	资源配额列表，详情请参见**表4-59**。

版权所有 © 华为技术有限公司

表 4-59 resources 字段数据结构说明

参数	是否必选	参数类型	描述
type	是	String	配额类型。 枚举值说明： • CMK，用户主密钥 • grant_per_CMK，单个用户主密钥可创建授权数
used	是	Integer	已使用配额数。
quota	是	Integer	配额总数。

示例

- 请求样例

  无

- 响应样例

```
{
    "quotas": {
        "resources": [
            {
                "type": "CMK",
                "used": 15,
                "quota": 20
            },
            {
                "type": "grant_per_CMK",
                "used": 15,
                "quota": 100
            }

        ]
    }
}
```

  或

```
{
    "error": {
        "error_code": "KMS.XXXX",
        "error_msg": "XXX"
    }
}
```

状态码

表4-60描述的是API返回的正常状态码。

表 4-60 状态码

状态码	编码	状态说明
200	OK	请求已成功。

版权所有 © 华为技术有限公司

异常状态码，请参见**状态码**。

4.1.15 修改密钥别名

功能介绍

修改用户主密钥别名。

说明

- 服务默认主密钥（密钥别名后缀为“/default”）不可以修改。
- 密钥处于“计划删除”状态，密钥别名不可以修改。

URI

- URI格式
  POST /v1.0/{project_id}/kms/update-key-alias
- 参数说明

表 4-61 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

表 4-62 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
key_alias	是	String	非默认主密钥别名，取值1到255字符，满足正则匹配“^[a-zA-Z0-9:/_-]{1,255}$”且后缀不可以为“/default”。
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

版权所有 © 华为技术有限公司

响应消息

表 4-63 响应参数

参数	是否必选	参数类型	描述
key_info	是	Array of objects	密钥信息，详情请参见表4-64。

表 4-64 key_info 字段结构说明

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。
key_alias	是	String	密钥别名。

示例

如下以修改别名为“test”，密钥ID为“bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e”的密钥为例。

- 请求样例

```
{
   "key_alias": "test",
   "key_id": "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e"
}
```

- 响应样例

```
{
   "key_info": {
      "key_id": "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
      "key_alias": "test"
    }
}
```

或

```
{
   "error": {
      "error_code": "KMS.XXXX",
      "error_msg": "XXX"
   }
}
```

状态码

表4-65描述的是API返回的正常状态码。

表 4-65 状态码

状态码	编码	状态说明
200	OK	请求已成功。

版权所有 © 华为技术有限公司

异常状态码，请参见**状态码**。

4.1.16 修改密钥描述

功能介绍

修改用户主密钥描述信息。

说明

- 服务默认主密钥（密钥别名后缀为“/default”）不可以修改。
- 密钥处于“计划删除”状态，密钥描述不可以修改。

URI

- URI格式
  POST /v1.0/{project_id}/kms/update-key-description
- 参数说明

表 4-66 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。

请求消息

表 4-67 请求参数

参数名	参数类型	是否必选	说明
key_id	String	是	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
key_description	String	是	密钥描述，取值0到255字符。
sequence	String	否	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

版权所有 © 华为技术有限公司

响应消息

表 4-68 响应参数

参数	是否必选	参数类型	描述
key_info	是	Array of objects	密钥信息，详情请参见表4-69。

表 4-69 key_info 字段结构说明

参数	参数类型	是否必选	说明
key_id	String	是	密钥ID。
key_description	String	是	密钥描述。

示例

如下以修改密钥ID为“bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e”，描述为“test”的密钥为例。

- 请求样例

```
{
   "key_id": "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
   "key_description": "test"
}
```

- 响应样例

```
{
   "key_info": {
      "key_id": "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
      "key_description": "test"
    }
}
```

或

```
{
   "error": {
      "error_code": "KMS.XXXX",
      "error_msg": "XXX"
   }
}
```

状态码

表4-70描述的是API返回的正常状态码。

表 4-70 状态码

状态码	编码	状态说明
200	OK	请求已成功。

版权所有 © 华为技术有限公司

异常状态码，请参见**状态码**。

4.1.17 加密数据

功能介绍

加密数据，用指定的用户主密钥加密数据。

URI

- URI格式
  POST /v1.0/{project_id}/kms/encrypt-data
- 参数说明

表 4-71 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

表 4-72 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
encryption_context	否	Object	一系列key-value键值对，用于记录资源上下文信息，用于保护数据的完整性，不应包含敏感信息，最大长度为8192。 当在加密时指定了该参数时，解密密文时，需要传入相同的参数，才能正确的解密。 例如： {"Key1":"Value1","Key2":"Value2"}
plain_text	是	String	明文数据，1~4096字节，满足正则匹配“^.{1,4096}$”，且转化为byte数组后长度取值范围为1~4096字节。
sequence	否	String	请求消息序列号，36字节序列号。 例如： 919c82d4-8046-4722-9094-35c3c6524cff

版权所有 © 华为技术有限公司

响应消息

表 4-73 响应参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。
cipher_text	是	String	加密数据密文，base64格式。

示例

如下以密钥ID为“0d0466b0-e727-4d9c-b35d-f84bb474a37f”的用户主密钥加密明文数据为“12345678”为例。

- 请求样例

```
{
   "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
   "plain_text": "12345678"
}
```

- 响应样例

```
{
   "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
   "cipher_text": "AgDoAG7EsEc2OHpQxz4gDFDH54CqwaelpTdEl
+RFPjbKn5klPTvOywYIeZX60kPbFsYOpXJwkL32HUM50MY22Eb1fOSpZK7WJpYjx66EWOkJvO
+Ey3r1dLdNAjrZrYzQlxRwNS05CaNKoX5rr3NoDnmv+UNobaiS25muLLiqOt6UrStaWow9AUyOHSzl
+BrX2Vu0whv74djK
+3COO6cXT2CBO6WajTJsOgYdxMfv24KWSKw0TqvHe8XDKASQGKdgfI74hzI1YWJlNjlmLWFlMTAtNDRjZ
C1iYzg3LTFiZGExZGUzYjdkNwAAAACdcfNpLXwDUPH3023MvZK8RPHe129k6VdNIi3zNb0eFQ==="
}
```

或

```
{
   "error": {
      "error_code": "KMS.XXXX",
      "error_msg": "XXX"
   }
}
```

状态码

表4-74描述的是API返回的正常状态码。

表 4-74 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

版权所有 © 华为技术有限公司

4.1.18 解密数据

功能介绍

解密数据。

URI

- URI格式
  POST /v1.0/{project_id}/kms/decrypt-data
- 参数说明

  表 4-75 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

表 4-76 请求参数

参数	是否必选	参数类型	描述
cipher_text	是	String	被加密数据密文。取值为加密数据结果中的cipher_text的值，满足正则匹配“^[0-9a-zA-Z+/=]{188,5648}$”。
encryption_context	否	Object	一系列key-value键值对，用于记录资源上下文信息，用于保护数据的完整性，不应包含敏感信息，最大长度为8192。 当在加密时指定了该参数时，解密密文时，需要传入相同的参数，才能正确的解密。 例如： {"Key1":"Value1","Key2":"Value2"}
sequence	否	String	请求消息序列号，36字节序列号。 例如： 919c82d4-8046-4722-9094-35c3c6524cff

版权所有 © 华为技术有限公司

响应消息

表 4-77 响应参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID。
plain_text	是	String	明文。

示例

如下以解密密文数据为“AgDoAG7EsEc2OHpQxz4gDFDH54CqwaelpTdEl+RFPjbKn5klPTvOywYIeZX60kPbFsYOpXJwkL32HUM50MY22Eb1fOSpZK7WJpYjx66EWOkJvO+Ey3r1dLdNAjrZrYzQlxRwNS05CaNKoX5rr3NoDnmv+UNobaiS25muLLiqOt6UrStaWow9AUyOHSzl+BrX2Vu0whv74djK+3COO6cXT2CBO6WajTJsOgYdxMfv24KWSKw0TqvHe8XDKASQGKdgfI74hzI1YWJlNjlmLWFlMTAtNDRjZC1iYzg3LTFiZGExZGUzYjdkNwAAAACdcfNpLXwDUPH3023MvZK8RPHe129k6VdNIi3zNb0eFQ==”为例。

- 请求样例
  ```
  {
      "cipher_text": "AgDoAG7EsEc2OHpQxz4gDFDH54CqwaelpTdEl+RFPjbKn5klPTvOywYIeZX60kPbFsYOpXJwkL32HUM50MY22Eb1fOSpZK7WJpYjx66EWOkJvO+Ey3r1dLdNAjrZrYzQlxRwNS05CaNKoX5rr3NoDnmv+UNobaiS25muLLiqOt6UrStaWow9AUyOHSzl+BrX2Vu0whv74djK+3COO6cXT2CBO6WajTJsOgYdxMfv24KWSKw0TqvHe8XDKASQGKdgfI74hzI1YWJlNjlmLWFlMTAtNDRjZC1iYzg3LTFiZGExZGUzYjdkNwAAAACdcfNpLXwDUPH3023MvZK8RPHe129k6VdNIi3zNb0eFQ=="
  }
  ```
- 响应样例
  ```
  {
     "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
     "plain_text": "12345678"
  }
  ```
  或
  ```
  {
     "error": {
        "error_code": "KMS.XXXX",
        "error_msg": "XXX"
     }
  }
  ```

状态码

表4-78描述的是API返回的正常状态码。

表 4-78 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

版权所有 © 华为技术有限公司

4.1.19 获取密钥导入参数

功能介绍

获取导入密钥的必要参数，包括密钥导入令牌和密钥加密公钥。

说明

返回的公钥类型默认为RSA_2048。

URI

- URI格式
  POST /v1.0/{project_id}/kms/get-parameters-for-import
- 参数说明

表 4-79 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

表 4-80 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
wrapping_algorithm	是	String	密钥材料加密算法，枚举如下： ● RSAES_PKCS1_V1_5 ● RSAES_OAEP_SHA_1 ● RSAES_OAEP_SHA_256
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

版权所有 © 华为技术有限公司

响应消息

表 4-81 响应参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，base64格式。
import_token	是	String	密钥导入令牌。
expiration_time	是	String	导入参数到期时间，时间戳，即从1970年1月1日至该时间的总秒数。
public_key	是	String	加密密钥材料的公钥，base64格式。

示例

如下以获取密钥ID为“bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e”，加密算法为“RSAES_OAEP_SHA_1”的导入参数为例。

- 请求样例

```
{
    "key_id": "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
     "wrapping_algorithm":"RSAES_OAEP_SHA_1"
}
```

- 响应样例

```
{
    "key_id": "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",

"import_token":"AACIBjY2ZTQxYjBmLTY3ZWItNDU4Ny04OTIxLWVhZTVhZjg5NDZmYQAAuihvPN7Hly3uhp7cWw4cfuwDIem9mGwaIl7/HTx10+8ENsRR4FB7DCR+zG1s7UIZMAZRLx7LD1lkXY
+rfN5ibDOOHZkoIiVSh+9u7xtC5m/
mNpIFeyqumxHei2I8CNdsNuJtjLV5bDU3tQrIkj72HCWpC0k9yf1ZSvi3yCwD4wyULXBsYwUa76bTK85MIZNGGtqfOyV6w74MT6m70gLhog8r7oWe6Gbof58uyYfFMbc
+s0OpkzMjvlvl1HApyOTijled26VgbgoGbPm9QvgjxC7mQEJpzQeg1/uNiziAG0YKo7wuD2mojwMBnr
+XGJrrFgmdO0pUaK+53KtDr8dtpGrVfJ+0zvebA45c4A4VfvaQQDCI5nJvB2Zz3LM4oiullVt
+0xrwDJYn9KRNZto2/zsGzrc/iBVASKE2UpIH7IikALJuDNrla8MVP5lzxdE0I
+905U2O7HLOsIwlDKMXx3CFao+4qLTb2O+Mq6xMQUwR2pwLcQA1cw
+BypJe4XE3z4fqFejO6VzjX5yd5pDVQ19eAzr9RgvSCi/IuyefFUci
+aX7xB4jx5MNwej3aePsOC9afsXBulhFyGgS/dZoPQ9kyG5TE2ELqAN6obERYoiZcyvq8RW9w/
uItLS99nGjwVe3U1yW4P6ColV+u7ygWxXm/Zs
+QTJHUDwl2ysbrebnN9PLNJSpHbBmuLjiMX02xtDAIt1meB2hGLqw+Mj/
n1jF5rnt5eXrNiG94pHZEvbp2BEDawJrRpaGj15C984WVw8ja/ZrTYfWklcNKW84cLvJXl9vxsuUp3/
ZYKh32M/ORUT46o6KtB/
xEltkaDJiSBBK4utuxQ8wO5UXW6FRkmAuV2naxhF6Obk7kEKYnuj4jxWAODtL9GcoNwq04ylSXj/
ZzaYbqXo1O34fjyz3QG5ZChXGgg52+wPj2LBDjUvlriuARg7cATgdqq9c6aifrGQAj0QgVp9Gv/
8c7PRzjzfH2vRwOZqpLSuCD5slWFSgc/RLxf1YNtNx98Jo
+PjRTWbyuZNiH2xOrpG0oKyk1giFITqOTuQ6UL768HgVJPRP4CgkgF7v65QpYaYgPvkJvwOb7j2VMr5VoykTipt7R2Xvh2LMy6wBW+HA0rw8V7ebc8/
KaH3CkGTdYL2MIfbOlxjyNplUeBKu8zYshFWfp7BUQsflAFMQyp2FhO7PGMygvqY0LLzDphVvBjpFCO4VqHZ/iOSDzL8vuEA
+OX8XLhZp9Kb7JPIJflfEz2lx3K8YvOJeRxUfOgvvBhpKu7KUDvnarW1R9rDX4adD4EC3mgP42SumAMYvFBKb6BgOkGAlTgHgLrKKsDw4DW56ANua30ZjeKJ1ZVftnyU0UJ34jsY0uJPi6QujBHqUzFbCp019Jx8Mi
+LtkN3e8Sl+4pvIfj7t+t9Xu03oDhD0J65qhHlpNP/NFrvP3KLmXFyXTWpGeczXxZvDp7Wmu5TnDSozN/
AbzBuyWASYZpLvgsf1xwevMmM1Gw/UX/
WVPQdN5lzWjhT1Dcy4ar8OozYtQeQ2ItSH1UaPJx0hW3BA1GYjW42+Vjy0VSLkliK/n6lN9KwTTTGAbW
+BvftImzGnfFM7fTCMJ3Jnx9nTn6+fbnhoXXfGHjOgPZ208VEIlG5YHS+HN/
JYyAkkj8G2+bSZmKfX9VMbYRGNTPrrghjAEY/Hh8V+/
ZhUSR3pPnblhr30SePGYgQPUGmnoTRHulCHRFOMcvu9nQ1P855DNpoE7fYi
+7N9xu1wFTB3DHtgUW8yuwtt
+q6LJZQMuGfmJLhBBf05FKlSxpR49IaJ0uQc7fsVYCpECL2aH8ueBqVGvQtEebWG6q0XTIrhqmaPtlQx9rVP
```


版权所有 © 华为技术有限公司

8oevPZ99yfB+8TZCT0B9WNqCotxijWqH3eyePY0Hb/AAXB34GjH1gni4NjwEI6LVX
+jSGb2ATy4Bd6ckonhGO9uwvW3WaPX214+GZvPdmv0pN60XfQ9B4Il/
RLIek6h6+2WEmB4i8qsvjgWfDD7DEhq6YN1Q/44NqUdDjrVCozBxXyDOab5tdsWCvfGXruGa/
wq7I1kH7K76s7TeL0a3pc0H5zt8qU/UT7uoLv0G7H+vVulGmqcl5pbsHYxTqNtSu2w9OBQ6PC8g+MCS/
fnXIcAhS7Lmvy8TFK4x0N+MhZqVbozVW37apCXFg6m1I9N0Sa4=",
"expiration_time":1501578672,

"public_key":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnJQqE9GorZ16XMlOQngJfU0Sg
kMKJpL9W+byIebeKgmDt2I6oVSPckk9y3JiaGjXKYlepawob9b61IRR97Bcr4Sf2p3J6J3gpiYGp1Ai3495rYF
+FSZAxW+VDOzbN3vig6SVxcP1PXtaKzQbtNfnlIh+rvSMJpVI3MFHh5lWjEn8L/
XpprLy1FqHSSvgB99qwiPw1ZGTL5XGSrIpCV3/ah8u+5VGoIUJZTtiZk6OQDkFH9fxwIahYvLI8/
yjrWFLtJuApr7aIrhRN0iDBINxddNh8M0A9sIFoS3D5RNKITjIKIMl/GVz+mHaPjK+91M/
b7JrNvinFCMQDGrb/1qoGQIDAQAB"
}

或

```
{
   "error": {
      "error_code": "KMS.XXXX",
      "error_msg": "XXX"
   }
}
```

状态码

表4-82描述的是API返回的正常状态码。

表 4-82 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.20 导入密钥材料

功能介绍

导入密钥材料。

URI

- URI格式

  POST /v1.0/{project_id}/kms/import-key-material
- 参数说明

  表 4-83 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

版权所有 © 华为技术有限公司

请求消息

表 4-84 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
import_token	是	String	密钥导入令牌，base64格式，满足正则匹配“^[0-9a-zA-Z+/=]{200,6144}$”。
encrypted_key_material	是	String	加密后的密钥材料，base64格式，满足正则匹配“^[0-9a-zA-Z+/=]{344,360}$”。
expiration_time	否	String	密钥材料到期时间，时间戳，即从1970年1月1日至该时间的总秒数，KMS会在该时间的24小时内删除密钥材料。 例如：1550291833
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

响应消息

无

示例

如下将密钥导入令牌和密钥材料导入密钥ID为“bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e”的密钥，并指定密钥材料过期时间为“1521578672”为例。

- 请求样例

```
{
   "key_id": "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",

"import_token":"AACIBjY2ZTQxYjBmLTY3ZWItNDU4Ny04OTIxLWVhZTVhZjg5NDZmYQAAuihvPN7Hly3uhp7cWw4cfuwDIem9mGwaIl7/HTx10+8ENsRR4FB7DCR+zG1s7UIZMAZRLx7LD1lkXY
+rfN5ibDOOHZkoIiVSh+9u7xtC5m/
mNpIFeyqumxHei2I8CNdsNuJtjLV5bDU3tQrIkj72HCWpC0k9yf1ZSvi3yCwD4wyULXBsYwUa76bTK85MIZNGGtqfOyV6w74MT6m70gLhog8r7oWe6Gbof58uyYfFMbc
+s0OpkzMjvlvl1HApyOTijled26VgbgoGbPm9QvgjxC7mQEJpzQeg1/uNiziAG0YKo7wuD2mojwMBnr
+XGJrrFgmdO0pUaK+53KtDr8dtpGrVfJ+0zvebA45c4A4VfvaQQDCI5nJvB2Zz3LM4oiullVt
+0xrwDJYn9KRNZto2/zsGzrc/iBVASKE2UpIH7IikALJuDNrla8MVP5lzxdE0I
+905U2O7HLOsIwlDKMXx3CFao+4qLTb2O+Mq6xMQUwR2pwLcQA1cw
+BypJe4XE3z4fqFejO6VzjX5yd5pDVQ19eAzr9RgvSCi/luyefFUci
+aX7xB4jx5MNwej3aePsOC9afsXBulhFyGgS/dZoPQ9kyG5TE2ELqAN6obERYoiZcyvq8RW9w/
uItLS99nGjwVe3U1yW4P6ColV+u7ygWxXm/Zs
+QTJHUDwl2ysbrebnN9PLNJSpHbBmuLJiMX02xtDAIt1meB2hGLqw+Mj/
```


版权所有 © 华为技术有限公司

n1jF5rnt5eXrNiG94pHZEvbp2BEDawJrRpaGj15C984WVw8ja/ZrTYfWklcNKW84cLvJXl9vxsuUp3/
ZYKh32M/ORUT46o6KtB/
xEltkaDJiSBBK4utuxQ8wO5UXW6FRkmAuV2naxhF6Obk7kEKYnuj4jxWAODtL9GcoNwq04ylSXj/
ZzaYbqXo1O34fjyz3QG5ZChXGgg52+wPj2LBDjUvlriuARg7cATgdqq9c6aifrGQAj0QgVp9Gv/
8c7PRzjzfH2vRwOZqpLSuCD5sIWFSgc/RLxf1YNtNx98Jo
+PjRTWbyuZNiH2xOrpG0oKyk1giFITqOTuQ6UL768HgVJPRP4CgkgF7v65QpYaYgPvkJvwOb7j2VMr5Voy
kTipt7R2Xvh2LMy6wBW+HA0rw8V7ebc8/
KaH3CkGTdYL2MIfbOlxjyNplUeBKu8zYshFWfp7BUQsflAFMQyp2FhO7PGMygvqY0LLzDphVvBjpFCO4V
qHZ/iOSDzL8vuEA
+OX8XLhZp9Kb7JPIJflfEz2lx3K8YvOJeRxUfOgvvBhpKu7KUDvnarW1R9rDX4adD4EC3mgP42SumAMYvF
BKb6BgOkGAlTgHgLrKKsDw4DW56ANua30ZjeKJ1ZVftnyU0UJ34jsY0uJPi6QujBHqUzFbCp019Jx8Mi
+LtkN3e8Sl+4pvIfj7t+t9Xu03oDhD0J65qhHlpNP/NFrvP3KLmXFyXTWpGeczXxZvDp7Wmu5TnDSozN/
AbzBuyWASYZpLvgsf1xwevMmM1Gw/UX/
WVPQdN5lzWjhT1Dcy4ar8OozYtQeQ2ItSH1UaPJx0hW3BA1GYjW42+Vjy0VSLkliK/n6lN9KwTTTGAbW
+BvftImzGnfFM7fTCMJ3Jnx9nTn6+fbnhoXXfGHjOgPZ208VEIlG5YHS+HN/
JYyAkkj8G2+bSZmKfX9VMbYRGNTPrrghjAEY/Hh8V+/
ZhUSR3pPnblhr30SePGYgQPUGmnoTRHulCHRFOMcvu9nQ1P855DNpoE7fYi
+7N9xu1wFTB3DHtgUW8yuwtt
+q6LJZQMuGfmJLhBBf05FKlSxpR49IaJ0uQc7fsVYCpECL2aH8ueBqVGvQtEebWG6q0XTIrhqmaPtlQx9rVP
8oevPZ99yfB+8TZCT0B9WNqCotxijWqH3eyePY0Hb/AAXB34GjH1gni4NjwEI6LVX
+jSGb2ATy4Bd6ckonhGO9uwvW3WaPX214+GZvPdmv0pN60XfQ9B4Il/
RLIek6h6+2WEmB4i8qsvjgWfDD7DEhq6YN1Q/44NqUdDjrVCozBxXyDOab5tdsWCvfGXruGa/
wq7I1kH7K76s7TeL0a3pc0H5zt8qU/UT7uoLv0G7H+vVulGmqcl5pbsHYxTqNtSu2w9OBQ6PC8g+MCS/
fnXIcAhS7Lmvy8TFK4x0N+MhZqVbozVW37apCXFg6m1I9N0Sa4=",
    "encrypted_key_material":"K+ixymtl90e
+B5Rdan89KjDslBIoOexrIwzkYHGz3odS7FDXDkogqbWwwJg5wQ6zjUbEvsR/+Fi
+A0SSkhhqtijivOKHu4Z86RWjOCBdrr9es+ZhJ0zYBNMN+7Rf2fd9vxbb873Q7VBkJRyH1hi3Wh
+kLmDW4rpWZm4+YGCtWylz7ZKbV1KBlhSNLDtZzT4nxUra0p7Die4HgUUxSjZTOr/0s71yF6o2eysreIzIl
+GbpCft0WpRsxN2Ng++ntgOcwOf2zOC9o/tjraxeAvgGw
+Dwt4cjF4znnFf0LPQ2YvpNUo248LjAGxdFvzUABNzfYSj3RZ0K3wQCNAcXU3HYw==",
    "expiration_time":1521578672
}

- 响应样例

  ```
  {
  }
  ```

  或

  ```
  {
     "error": {
        "error_code": "KMS.XXXX",
        "error_msg": "XXX"
     }
  }
  ```

状态码

表4-85描述的是API返回的正常状态码。

表 4-85 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.21 删除密钥材料

功能介绍

删除密钥材料信息。

 版权所有 © 华为技术有限公司

URI

- URI格式

  POST /v1.0/{project_id}/kms/delete-imported-key-material

- 参数说明

  表 4-86 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

表 4-87 请求参数

参数	是否必选	参数类型	描述
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

响应消息

无

示例

如下以删除密钥ID为“0d0466b0-e727-4d9c-b35d-f84bb474a37f”的密钥材料为例。

- 请求样例

```
{
   "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

- 响应样例

```
{
   "error": {
      "error_code": "KMS.XXXX",
      "error_msg": "XXX"
   }
}
```


版权所有 © 华为技术有限公司

状态码

表4-88描述的是API返回的正常状态码。

表 4-88 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.22 查询密钥实例

功能介绍

查询密钥实例。

通过标签过滤，查询指定用户主密钥的详细信息。

URI

- URI格式
  POST /v1.0/{project_id}/kms/resource_instances/action
- 参数说明

表 4-89 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

表 4-90 请求参数

参数	是否必选	参数类型	描述
tags	否	Array of objects	标签列表，key和value键值对的集合。 • key：表示标签键，一个密钥下最多包含10个key，key不能为空，不能重复，同一个key中value不能重复。key最大长度为36个字符。 • value：表示标签值。每个值最大长度43个字符，value之间为“与”的关系。

版权所有 © 华为技术有限公司

参数	是否必选	参数类型	描述
limit	否	String	查询记录数（“action”为“count”时，无需设置此参数），如果“action”为“filter”，默认为“10”。 limit的取值范围为“1-1000”。
offset	否	String	索引位置。从offset指定的下一条数据开始查询。查询第一页数据时，将查询前一页数据时响应体中的值带入此参数（“action”为“count”时，无需设置此参数）。如果“action”为“filter”，offset默认为“0”。 offset必须为数字，不能为负数。
action	是	String	操作标识（可设置为“filter”或者“count”）。 • filter：表示过滤。 • count：表示查询总条数。
matches	否	Array of objects	搜索字段。 • key为要匹配的字段，例如：resource_name等。 • value为匹配的值，最大长度为255个字符，不能为空。
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

响应消息

表 4-91 响应参数

参数	是否必选	参数类型	描述
resources	是	Array of objects	资源实例列表，详情请参见表4-92。
total_count	是	Integer	总记录数。

表 4-92 resource 字段数据结构说明

参数	是否必选	参数类型	描述
resource_id	是	String	资源ID。

版权所有 © 华为技术有限公司

参数	是否必选	参数类型	描述
resource_detail	是	Object	资源详情，详情请参见表4-31。
tags	是	Array of objects	标签列表，没有标签，数组默认为空。
resource_name	是	String	资源名称，默认为空字符串。

示例

以下以查询密钥实例为例。

- 请求样例

```
{
      "offset": "100",
      "limit": "100",
      "action": "filter",
      "matches":[
      {
            "key": "resource_name",
            "value": "resource1"
       }
      ],
      "tags": [
          {
            "key": "key1",
            "values": [
                  "value1",
                  "value2"
            ]
          }
      ]
  }
```

- 响应样例

```
{
 "resources": [{
      "resource_id": "90c03e67-5534-4ed0-acfa-89780e47a535",
      "resource_detail": {
            "key_id": "90c03e67-5534-4ed0-acfa-89780e47a535",
            "domain_id": "4B688Fb77412Aee5570E7ecdbeB5afdc",
            "key_alias": "tagTest_xmdmi",
            "key_description": "123",
            "creation_date": 1521449277000,
            "scheduled_deletion_date": "",
            "key_state": 2,
            "default_key_flag": 0,
            "key_type": 1
      },
      "resource_name": "tagTest_xmdmi",
      "tags": [{
            "key": "$",
            "value": "testValue!"
      }, {
            "key": "1",
            "value": "ccwZ"
      }, {
            "key": "1&",
            "value": "testValue!"
      }, {
            "key": "abcd",
```


版权所有 © 华为技术有限公司

```
            "value": "1&"
        }, {
            "key": "efg",
            "value": "1&"
        }, {
            "key": "faregbqer",
            "value": "AAaa00-99"
        }, {
            "key": "fcwefwq",
            "value": "$"
        }, {
            "key": "fwqegqwrg",
            "value": "1&"
        }, {
            "key": "haha",
            "value": "qzzahnzgoqbkabppdehnbrrgbrkvlxkkfoosqyhdylq"
        }, {
            "key": "quapxpysduboguiluwargcgmvcgxinianbhl",
            "value": "testValue!"
        }]
}]
"total_count": "1"}
```


或


```
{
    "error": {
    "error_code": "KMS.XXXX",
    "error_msg": "XXX"
     }
}
```


状态码

表4-93描述的是API返回的正常状态码。

表 4-93 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.23 查询密钥标签

功能介绍

查询指定密钥的标签信息。

标签管理服务需要使用该接口查询指定密钥的全部标签数据。

URI

- URI格式

  GET /v1.0/{project_id}/kms/{key_id}/tags
- 参数说明

版权所有 © 华为技术有限公司

表 4-94 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f

请求消息

无

响应消息

表 4-95 响应参数

参数	是否必选	参数类型	描述
tags	是	Array of objects	标签列表，key和value键值对的集合。 ● key：表示标签键，一个密钥下最多包含10个key，key不能为空，不能重复，同一个key中value不能重复。key最大长度为36个字符。 ● value：表示标签值。每个值最大长度43个字符，value之间为“与”的关系。
existTagNum	是	Integer	密钥的标签个数。

示例

如下以查询密钥标签为例。

- 请求样例

  无

- 响应样例

```
{       "tags": [
         {
          "key": "key1",
          "value": "value1"
         },
         {
          "key": "key2",
          "value": "value3"
         }
         ],
```


版权所有 © 华为技术有限公司

```
        "existTagsNum":2
}
```

或

```
{
    "error": {
        "error_code": "KMS.XXXX",
        "error_msg": "XXX"
    }
}
```

状态码

表4-96描述的是API返回的正常状态码。

表 4-96 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见状态码。

4.1.24 查询项目标签

功能介绍

查询用户在指定项目下的所有标签集合。

URI

- URI格式
  GET /v1.0/{project_id}/kms/tags
- 参数说明

  表 4-97 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求消息

无

版权所有 © 华为技术有限公司

响应消息

表 4-98 响应参数

参数	是否必选	参数类型	描述
tags	是	Array of objects	标签列表，key和value键值对的集合。 ● key：表示标签键，一个密钥下最多包含10个key，key不能为空，不能重复，同一个key中value不能重复。key最大长度为36个字符。 ● value：表示标签值。每个值最大长度43个字符，value之间为“与”的关系。

示例

如下以查询项目标签为例。

- 请求样例

  无

- 响应样例

```
{          "tags": [
           {
             "key": "key1",
             "values": [
                "value1",
                "value2"
              ]
            },
           {
             "key": "key2",
             "values": [
                "value1",
                "value2"
              ]
      }
]
}
```

  或

```
{
     "error": {
           "error_code": "KMS.XXXX",
           "error_msg": "XXX"
    }
}
```

状态码

表4-99描述的是API返回的正常状态码。

版权所有 © 华为技术有限公司

表 4-99 状态码

状态码	编码	状态说明
200	OK	请求已成功。

异常状态码，请参见**状态码**。

4.1.25 批量添加删除密钥标签

功能介绍

批量添加删除密钥标签。

URI

- URI格式

  POST /v1.0/{project_id}/kms/{key_id}/tags/action
- 参数说明

  表 4-100 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f

请求消息

表 4-101 请求参数

参数	是否必选	参数类型	描述
tags	是	Array of objects	标签列表，key和value键值对的集合。 ● key：表示标签键，一个密钥下最多包含10个key，key不能为空，不能重复，同一个key中value不能重复。key最大长度为36个字符。 ● value：表示标签值。每个值最大长度43个字符，value之间为“与”的关系。

版权所有 © 华为技术有限公司

参数	是否必选	参数类型	描述
action	是	String	操作标识： 仅限于“create”和“delete”。
sequence	否	String	请求消息序列号，36字节序列号。 例如： 919c82d4-8046-4722-9094-35c3c6524cff

响应消息

无

示例

如下以添加标签键为“key1”和“key”，标签值为“value1”和“value3”为例。

- 请求样例

```
{
   "action": "create",
   "tags": [
      {
         "key": "key1",
         "value": "value1"
      },
      {
         "key": "key",
         "value": "value3"
      }
   ]
}
```

或

```
{
   "action": "delete",
   "tags": [
      {
         "key": "key1",
         "value": "value1"
      },
      {
         "key": "key2",
         "value": "value3"
      }
   ]
}
```

- 响应样例

```
{
}
```

或

```
{
     "error": {
           "error_code": "KMS.XXXX",
           "error_msg": "XXX"
    }
}
```


版权所有 © 华为技术有限公司

状态码

表4-102描述的是API返回的正常状态码。

表 4-102 状态码

状态码	编码	状态说明
204	No Content	请求已成功，无内容返回。

异常状态码，请参见**状态码**。

4.1.26 添加密钥标签

功能介绍

添加密钥标签。

URI

- URI格式
  POST /v1.0/{project_id}/kms/{key_id}/tags
- 参数说明

表 4-103 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f

请求消息

表 4-104 请求参数

参数	是否必选	参数类型	描述
tag	是	Array of object	包含标签，详情请参见表4-105。

版权所有 © 华为技术有限公司

参数	是否必选	参数类型	描述
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

表 4-105 tag 字段数据结构说明

参数	是否必选	参数类型	描述
key	是	String	键。 最大长度36个unicode字符。 key不能为空。不能包含非打印字符“ASCII(0-31)”、“*”、“<”、“>”、“\”、“=”。
value	是	String	值。 每个值最大长度43个unicode字符，可以为空字符串。 不能包含非打印字符“ASCII(0-31)”、“*”、“<”、“>”、“\”、“=”。

响应消息

无

示例

如下以添加标签键为“DEV”，标签值为“DEV1”为例。

- 请求样例

```
{
  "tag":
    {
      "key":"DEV",
      "value":"DEV1"
    }
}
```

- 响应样例

```
{
}
```

或

```
{
      "error": {
            "error_code": "KMS.XXXX",
            "error_msg": "XXX"
    }
}
```


版权所有 © 华为技术有限公司

状态码

表4-106描述的是API返回的正常状态码。

表 4-106 状态码

状态码	编码	状态说明
204	No Content	请求已成功，无内容返回。

异常状态码，请参见状态码。

4.1.27 删除密钥标签

功能介绍

删除密钥标签。

URI

- URI格式
  DELETE /v1.0/{project_id}/kms/{key_id}/tags/{key}
- 参数说明

  表 4-107 参数说明

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。
key_id	是	String	密钥ID，36字节，满足正则匹配“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$”。 例如：0d0466b0-e727-4d9c-b35d-f84bb474a37f
key	是	String	标签key。

请求消息

表 4-108 请求参数

参数	是否必选	参数类型	描述
sequence	否	String	请求消息序列号，36字节序列号。 例如：919c82d4-8046-4722-9094-35c3c6524cff

版权所有 © 华为技术有限公司

响应消息

无

示例

响应样例

```
{
}
```

或

```
{
    "error": {
        "error_code": "KMS.XXXX",
        "error_msg": "XXX"
    }
}
```

状态码

表4-109描述的是API返回的正常状态码。

表 4-109 状态码

状态码	编码	状态说明
204	No Content	请求已成功，无内容返回。

异常状态码，请参见状态码。

版权所有 © 华为技术有限公司

5 权限和授权项

5.1 权限及授权项说明

如果您需要对您所拥有的密钥管理服务（Key Management Service，KMS）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，IAM），如果帐号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用KMS的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为角色和策略。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略以API接口为粒度进行权限拆分，授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

说明

如果您要允许或是禁止某个接口的操作权限，请使用策略。

帐号具备所有接口的调用权限，如果使用帐号下的IAM用户发起API请求时，该IAM用户必须具备调用该接口所需的权限，否则，API请求将调用失败。每个接口所需要的权限，与各个接口所对应的授权项相对应，只有发起请求的用户被授予授权项所对应的策略，该用户才能成功调用该接口。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。策略支持的操作与API相对应，授权项列表说明如下：

- 权限：允许或拒绝某项操作。
- 对应API接口：自定义策略实际调用的API接口。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。
- 依赖的授权项：部分Action存在对其他Action的依赖，需要将依赖的Action同时写入授权项，才能实现对应的权限功能。

版权所有 © 华为技术有限公司

- IAM项目(Project)/企业项目(Enterprise Project)：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项对应的自定义策略，可以在IAM和企业管理两个服务中给用户组授权并生效。如果仅支持IAM项目，不支持企业项目，表示仅能在IAM中给用户组授权并生效，如果在企业管理中授权，则该自定义策略不生效。

  说明

  “√”表示支持，“x”表示暂不支持。

密钥管理服务（KMS）支持的自定义策略授权项如下所示：

加密密钥管理，包含密钥管理对应的授权项，如创建密钥、查询密钥等接口。

5.2 加密密钥管理

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
创建密钥	POST /v1.0/{project_id}/kms/create-key	kms:cmk:create	-	√	√
启用密钥	POST /v1.0/{project_id}/kms/enable-key	kms:cmk:enable	-	√	√
禁用密钥	POST /v1.0/{project_id}/kms/disable-key	kms:cmk:disable	-	√	√
计划删除密钥	POST /v1.0/{project_id}/kms/schedule-key-deletion	kms:cmk:update	-	√	√
取消计划删除密钥	POST /v1.0/{project_id}/kms/cancel-key-deletion	kms:cmk:update	-	√	√
查询密钥列表	POST /v1.0/{project_id}/kms/list-keys	kms:cmk:list	-	√	√
查询密钥信息	POST /v1.0/{project_id}/kms/describe-key	kms:cmk:get	-	√	√
创建随机数	POST /v1.0/{project_id}/kms/gen-random	kms:cmk:generate	-	√	√

版权所有 © 华为技术有限公司

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目 (Project)	企业项目 (Enterprise Project)
创建数据密钥	POST /v1.0/{project_id}/kms/create-datakey	kms:dek:create	-	√	√
创建不含明文数据密钥	POST /v1.0/{project_id}/kms/create-datakey-without-plaintext	kms:dek:create	-	√	√
加密数据密钥	POST /v1.0/{project_id}/kms/encrypt-datakey	kms:dek:crypto	-	√	√
解密数据密钥	POST /v1.0/{project_id}/kms/decrypt-datakey	kms:dek:crypto	-	√	√
查询实例数	GET /v1.0/{project_id}/kms/user-instances	kms:cmk:getInstance	-	√	√
查询配额	GET /v1.0/{project_id}/kms/user-quotas	kms:cmk:getQuota	-	√	√
修改密钥别名	POST /v1.0/{project_id}/kms/update-key-alias	kms:cmk:update	-	√	√
修改密钥描述	POST /v1.0/{project_id}/kms/update-key-description	kms:cmk:update	-	√	√
加密数据	POST /v1.0/{project_id}/kms/encrypt-data	kms:cmk:crypto	-	√	√
解密数据	POST /v1.0/{project_id}/kms/decrypt-data	kms:cmk:crypto	-	√	√
获取密钥导入参数	POST /v1.0/{project_id}/kms/get-parameters-for-import	kms:cmk:getMaterial	-	√	√
导入密钥材料	POST /v1.0/{project_id}/kms/import-key-material	kms:cmk:importMaterial	-	√	√
删除密钥材料	POST /v1.0/{project_id}/kms/delete-imported-key-material	kms:cmk:deleteMaterial	-	√	√

版权所有 © 华为技术有限公司

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目 (Project)	企业项目 (Enterprise Project)
查询密钥实例	POST /v1.0/{project_id}/kms/resource_instances/action	kms:cmkTag:listInstance	-	√	√
查询密钥标签	GET /v1.0/{project_id}/kms/{key_id}/tags	kms:cmkTag:list	-	√	√
查询项目标签	GET /v1.0/{project_id}/kms/tags	kms:cmkTag:list	-	√	√
批量添加删除密钥标签	POST /v1.0/{project_id}/kms/{key_id}/tags/action	kms:cmkTag:batch	-	√	√
添加密钥标签	POST /v1.0/{project_id}/kms/{key_id}/tags	kms:cmkTag:create	-	√	√
删除密钥标签	POST /v1.0/{project_id}/kms/{ key_id }/tags/{key}	kms:cmkTag:delete	-	√	√

版权所有 © 华为技术有限公司

A 附录

A.1 状态码

状态码	编码	状态说明
200	OK	请求已成功。
400	Bad Request	请求参数有误。
403	Forbidden	服务器已经理解请求，但是拒绝执行它。
404	Not Found	资源不存在，资源未找到。
500	Internal Server Error	服务内部错误。

A.2 错误码

状态码	错误码	错误信息	描述	处理措施
400	KMS.0201	Invalid request URL.	请求URL非法。	请传递正确的URL。
400	KMS.0202	Invalid JSON format of the request message.	请求消息JSON格式非法。	请传递正确的消息体。
400	KMS.0203	Request message too long.	请求消息长度超出限制。	请传递正确的消息体。
400	KMS.0204	Parameters missing in the request message.	请求消息缺少参数。	请传递正确的消息体。

版权所有 © 华为技术有限公司

状态码	错误码	错误信息	描述	处理措施
400	KMS.0205	Invalid key ID.	密钥key_id非法。	请传递正确的密钥id。
400	KMS.0206	Invalid sequence number.	sequence序号非法。	请传递正确的序列号。
400	KMS.0208	Invalid value of value encryption_context.	encryption_context参数非法。	请检查encryption_context字段是否合法。
400	KMS.0209	The key has been disabled.	密钥已被禁用，不能使用。	请启用该密钥。
400	KMS.0210	The key is in Scheduled deletion state and cannot be used.	密钥处于“计划删除”状态，不能使用。	请启用该密钥。
400	KMS.0211	Cannot perform this operation on Default Master Keys.	默认主密钥不支持该操作。	请使用普通主密钥操作该任务。
400	KMS.0308	Invalid parameter.	字段非法。	请传递正确的参数。
400	KMS.0309	External keys required.	密钥来源应为外部导入。	请使用外部导入密钥进行此操作。
400	KMS.0310	The key is not in Pending import state.	密钥未处于“等待导入”状态。	请确保密钥状态处于“等待导入”状态。
400	KMS.0311	Failed to decrypt data using the RSA private key.	RSA私钥解密数据失败。	请确保传入的密文的正确性，或联系技术支持。
400	KMS.0312	External keys cannot be rotated.	外部密钥不支持轮换操作。	请使用普通主密钥。
400	KMS.0313	Key rotation is not enabled.	密钥轮换未被启用。	请启用密钥轮换。
400	KMS.0401	Tag list cannot be empty.	标签列表不能为空。	请传递正确的参数。

版权所有 © 华为技术有限公司

状态码	错误码	错误信息	描述	处理措施
400	KMS.0402	Invalid match value.	match中value字段不合法。	请传递正确的参数。
400	KMS.0403	Invalid match key.	match中key字段不合法。	请传递正确的参数。
400	KMS.0404	Invalid action.	action字段不合法。	请传递正确的参数。
400	KMS.0405	Invalid tag value.	tag中value字段不合法。	请传递正确的参数。
400	KMS.0406	Invalid tag key.	tag中key字段不合法。	请传递正确的参数。
400	KMS.0407	Invalid tag list size.	tag列表长度不合法。	请传递正确的参数。
400	KMS.0408	Invalid resourceType.	resourceType字段不合法。	请传递正确的参数。
400	KMS.0409	Too many tags.	tag达到上限。	标签配额已达到上限，请删除部分标签后再重试。
400	KMS.0410	Invalid tag value length.	tag中value长度不合法。	请传递正确的参数。
400	KMS.0411	Invalid tag key length.	tag中key长度不合法。	请传递正确的参数。
400	KMS.0412	Invalid tag list.	tag list不合法。	请传递正确的参数。
400	KMS.0413	Too many tag values.	tag中values列表长度超过限制。	请传递正确的参数。
400	KMS.0415	Invalid matches.	matches字段不合法。	请传递正确的参数。
400	KMS.0417	Invalid offset.	offset不在有效数字范围内。	请传递正确的参数。
400	KMS.1101	Invalid key_alias.	key_alias密钥别名非法。	请传递正确的参数。
400	KMS.1102	Invalid realm.	realm密钥区域非法。	请传递正确的参数。
400	KMS.1103	Invalid key_description.	key_description密钥描述非法。	请传递正确的参数。

版权所有 © 华为技术有限公司

状态码	错误码	错误信息	描述	处理措施
400	KMS.1104	Duplicate key aliases.	密钥别名已经存在。	请更换别名。
400	KMS.1105	Too many keys.	密钥个数已达上限。	配额已达到上限，增加配额或者删除部分密钥。
400	KMS.1201	The key is not disabled.	密钥未被禁用。	请先禁用密钥。
400	KMS.1301	The key is not enabled.	密钥未被启用。	请先启用密钥。
400	KMS.1401	Set the pending deletion period between 7 to 1096 days.	计划删除密钥时间范围：7天～1096天。	请传递正确的参数。
400	KMS.1402	The key is already in Pending deletion state.	密钥已处于“计划删除”状态。	密钥已经处于“计划删除”状态，无需再操作。
400	KMS.1501	The key is not in Pending deletion state.	密钥未处于“计划删除”状态。	请先“计划删除”密钥。
400	KMS.1601	Invalid limit.	limit不在有效数字范围内。	请传递正确的参数。
400	KMS.1602	marker must be greater than or equals 0.	marker参数需大于等于0。	请传递正确的参数。
400	KMS.1801	random_data_length must be 512 bits.	random_data_length随机数长度需等于512位。	请传递正确的参数。
400	KMS.1901	datakey_length must be in the range 8 bits to 8,192 bits.	datakey_length必须介于8-8192比特之间。	请传递正确的参数。
400	KMS.2001	datakey_length must be 512 bits.	datakey_length数据密钥长度需等于512位。	请传递正确的参数。

版权所有 © 华为技术有限公司

状态码	错误码	错误信息	描述	处理措施
400	KMS.2101	Invalid plain_text.	plain_text数据密钥明文非法。	请传递正确的参数。
400	KMS.2102	datakey_plain_length must be 64 bytes.	datakey_plain_length数据密钥明文长度需等于64字节。	请传递正确的参数。
400	KMS.2103	Failed to verify the DEK hash.	数据密钥hash校验失败。	请确认数据密钥是否合法。
400	KMS.2201	Invalid cipher_text.	cipher_text数据密钥密文非法。	请传递正确的参数。
400	KMS.2202	datakey_cipher_length must be 64 bytes.	datakey_cipher_length数据密钥密文长度需等于64字节。	请传递正确的参数。
400	KMS.2203	Failed to verify the DEK hash.	数据密钥hash校验失败。	请确认数据密钥是否合法。
400	KMS.2601	Token expired.	令牌已失效。	请重新获取令牌。
400	KMS.2602	Key expiration time must be later than the current time.	导入密钥失效时间必须大于当前时间。	请重新选择导入密钥失效时间。
400	KMS.2603	Key IDs in the imported key and token do not match.	导入密钥key_id与令牌中key_id不匹配。	请确保导入密钥key_id与令牌中key_id匹配。
400	KMS.2604	The external key plaintext length must be 32 bits.	外部密钥明文长度必须为32位。	请传递正确的参数。
400	KMS.2605	Token verification failed.	令牌校验失败。	请重新获取令牌。

版权所有 © 华为技术有限公司

状态码	错误码	错误信息	描述	处理措施
400	KMS.2606	You are importing a deleted key again. The imported plaintext must be the same as the deleted key plaintext.	重新导入一个已删除的密钥材料时，外部密钥明文应与之前导入的一致。	请确保导入密钥明文与之前导入密钥明文数据一致。
400	KMS.2701	Key material is not in Enabled or Disabled state and cannot be deleted.	密钥材料只有在“启用”、“禁用”状态下方可被删除。	请确保密钥在“启用”、“禁用”状态。
403	KMS.0301	Invalid or null X-Auth-Token.	X-Auth-Token为null或字符非法。	请重新获取token，并在使用时确保token字符串的完整性。
403	KMS.0302	Invalid X-Auth-Token.	X-Auth-Token无效。	请重新获取token，并在使用时确保token字符串的完整性。
403	KMS.0303	X-Auth-Token expired.	X-Auth-Token过期。	请重新获取token，并在使用时确保token字符串的完整性。
403	KMS.0304	X-Auth-Token contains the OBT tag and cannot be used to access services.	X-Auth-Token包含公测标签，不能访问服务。	请重新获取token，并在使用时确保token字符串的完整性。
403	KMS.0305	Invalid X-Auth-Token project name.	X-Auth-Token Project Name区域非法。	请重新获取token，并在使用时确保token字符串的完整性。
403	KMS.0306	No access permissions.	用户无权限访问密钥。	请联系KMS管理员给帐户添加相应权限。
403	KMS.0307	No access permissions.	用户角色无权限访问接口。	请联系管理员给帐户添加相应权限。
500	KMS.0101	KMS error.	KMS错误。	请重试。

版权所有 © 华为技术有限公司

状态码	错误码	错误信息	描述	处理措施
500	KMS.0102	Abnormal KMS I/O.	KMS I/O异常。	请重试。

A.3 获取项目 ID

调用 API 获取项目 ID

项目ID可以通过调用IAM服务的“查询指定条件下的项目信息”API获取。

获取项目ID的接口为“GET https://{Endpoint}/v3/projects”，其中{Endpoint}为IAM的终端节点，可以从**地区和终端节点**获取。接口的认证鉴权请参见**认证鉴权**。

响应示例如下，其中projects下的“id”即为项目ID。

```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180d14e684b",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "xxxxxxxx",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
            },
            "id": "a4a5d4098fb4474fa22cd05f897d6b99",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```

从控制台获取项目 ID

在调用接口的时候，部分URL中需要填入项目编号，所以需要获取到项目编号。项目编号获取步骤如下：

1. 登录管理控制台。
2. 单击用户名，在下拉列表中单击“我的凭证”。
   在“我的凭证”页面的项目列表中查看项目ID。

A.4 API 授权项列表

版权所有 © 华为技术有限公司

A.4.1 加密密钥管理

API	API功能项	授权项
POST /v1.0/{project_id}/kms/create-key	创建密钥	kms:cmk:create
POST /v1.0/{project_id}/kms/enable-key	启用密钥	kms:cmk:enable
POST /v1.0/{project_id}/kms/disable-key	禁用密钥	kms:cmk:disable
POST /v1.0/{project_id}/kms/schedule-key-deletion	计划删除密钥	kms:cmk:update
POST /v1.0/{project_id}/kms/cancel-key-deletion	取消计划删除密钥	kms:cmk:update
POST /v1.0/{project_id}/kms/list-keys	查询密钥列表	kms:cmk:list
POST /v1.0/{project_id}/kms/describe-key	查询密钥信息	kms:cmk:get
POST /v1.0/{project_id}/kms/gen-random	创建随机数	kms:cmk:generate
POST /v1.0/{project_id}/kms/create-datakey	创建数据密钥	kms:dek:create
POST /v1.0/{project_id}/kms/create-datakey-without-plaintext	创建不含明文数据密钥	kms:dek:create
POST /v1.0/{project_id}/kms/encrypt-datakey	加密数据密钥	kms:dek:crypto
POST /v1.0/{project_id}/kms/decrypt-datakey	解密数据密钥	kms:dek:crypto
GET /v1.0/{project_id}/kms/user-instances	查询实例数	kms:cmk:getInstance
GET /v1.0/{project_id}/kms/user-quotas	查询配额	kms:cmk:getQuota
POST /v1.0/{project_id}/kms/update-key-alias	修改密钥别名	kms:cmk:update
POST /v1.0/{project_id}/kms/update-key-description	修改密钥描述	kms:cmk:update
POST /v1.0/{project_id}/kms/encrypt-data	加密数据	kms:cmk:crypto
POST /v1.0/{project_id}/kms/decrypt-data	解密数据	kms:cmk:crypto

版权所有 © 华为技术有限公司

API	API功能项	授权项
POST /v1.0/{project_id}/kms/get-parameters-for-import	获取密钥导入参数	kms:cmk:getMaterial
POST /v1.0/{project_id}/kms/import-key-material	导入密钥材料	kms:cmk:importMaterial
POST /v1.0/{project_id}/kms/delete-imported-key-material	删除密钥材料	kms:cmk:deleteMaterial
POST /v1.0/{project_id}/kms/resource_instances/action	查询密钥实例	kms:cmkTag:listInstance
GET /v1.0/{project_id}/kms/{key_id}/tags	查询密钥标签	kms:cmkTag:list
GET /v1.0/{project_id}/kms/tags	查询项目标签	kms:cmkTag:list
POST /v1.0/{project_id}/kms/{key_id}/tags/action	批量添加删除密钥标签	kms:cmkTag:batch
POST /v1.0/{project_id}/kms/{key_id}/tags	添加密钥标签	kms:cmkTag:create
POST /v1.0/{project_id}/kms/{ key_id }/tags/{key}	删除密钥标签	kms:cmkTag:delete

版权所有 © 华为技术有限公司

B 修订记录

发布日期	修改说明
2022-11-28	第三次正式发布。 新增： ● “创建密钥”章节，响应示例内容。 修改 ● “计划删除密钥”章节，优化内容。 ● “错误码”章节，优化错误码格式。 ● “创建密钥”章节，新增响应参数key_info及其说明。 ● “启用密钥”章节，新增响应参数key_info及其说明。
2021-06-03	第二次正式发布。 新增“权限和授权项”章节。
2021-01-27	第一次正式发布。

 版权所有 © 华为技术有限公司