Data Encryption Workshop

API Reference

Issue 24

Date 2025-12-17

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions

and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Before You Start 1

2 Calling APIs 4

2.1 Making an API Request 4

2.2 Authentication 7

2.3 Response 8

3 API Overview 11

4 APIs 21

4.1 Key Management APIs 21

4.1.1 Key Lifecycle Management 21

4.1.1.1 Creating a Key 21

4.1.1.2 Enabling a Key 31

4.1.1.3 Disabling a Key 40

4.1.1.4 Scheduling the Deletion for a Key 48

4.1.1.5 Canceling the Scheduled Deletion for a Key 57

4.1.1.6 Modifying a Key Alias 65

4.1.1.7 Modifying a Key Description 74

4.1.2 DEK Management 82

4.1.2.1 Generating a Random Number 82

4.1.2.2 Creating a DEK 90

4.1.2.3 Creating a Plaintext-free DEK 101

4.1.2.4 Creating an RSA Data Key Pair 111

4.1.2.5 Creating an EC Data Key Pair 119

4.1.2.6 Encrypting a DEK 128

4.1.2.7 Decrypting a DEK 138

4.1.2.8 Creating a PIN 147

4.1.3 Small-Size Data Encryption and Decryption 156

4.1.3.1 Encrypting Data 156

4.1.3.2 Decrypting Data 165

4.1.4 Signature and Verification 174

4.1.4.1 Signature Data 175

4.1.4.2 Verifying a Signature 184

4.1.5 Key Tag Management 194

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.1.5.1 Querying the Key Instance 194
4.1.5.2 Querying Key Tags 207
4.1.5.3 Adding Tags to a Key 215
4.1.5.4 Querying Project Tags 224
4.1.5.5 Batch Adding or Deleting Key Tags 231
4.1.5.6 Deleting Key Tags 240
4.1.6 Querying Key API Versions 248
4.1.6.1 Querying the Version List 248
4.1.6.2 Querying a Specified Version 251
4.1.7 Multi-Region Key 257
4.1.7.1 Changing the Primary Region for a Key 257
4.1.7.2 Copying a Key to a Specified Region 266
4.1.7.3 Querying the Regions Supported by a Cross-Region Key 276
4.1.8 MAC 283
4.1.8.1 Generating a MAC 283
4.1.8.2 Verifying a MAC 288
4.1.9 Alias Management 294
4.1.9.1 Associating Key Alias 294
4.1.9.2 Querying the Alias Associated with a Key 299
4.1.9.3 Creating a Key Alias 304
4.1.9.4 Deleting a Key Alias 309
4.1.10 Key Import Management 314
4.1.10.1 Obtaining Key Import Parameters 314
4.1.10.2 Importing Key Materials 323
4.1.10.3 Deleting Key Materials 332
4.1.11 Querying Keys 340
4.1.11.1 Querying the Key List 340
4.1.11.2 Querying Key Details 352
4.1.11.3 Querying a Public Key 363
4.1.11.4 Querying the Instance Quantity 371
4.1.11.5 Querying Quotas 378
4.1.12 Key Grant Management 386
4.1.12.1 Creating a Grant 386
4.1.12.2 Revoking a Grant 396
4.1.12.3 Retiring a Grant 404
4.1.12.4 Querying the Grant List 412
4.1.12.5 Querying Retirable Grants 422
4.1.13 Key Rotation Management 432
4.1.13.1 Enabling Key Rotatioin 432
4.1.13.2 Disabling Key Rotation 440
4.1.13.3 Modifying the Key Rotation Interval 447
4.1.13.4 Querying the Key Rotation Status 456

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.1.14 Dedicated Keystore Management 464
4.1.14.1 Creating a Dedicated Keystore 464
4.1.14.2 Querying the List of Dedicated Keystores 473
4.1.14.3 Obtaining a Dedicated Keystore 480
4.1.14.4 Deleting a Dedicated Keystore 488
4.1.14.5 Enabling a Dedicated Keystore 495
4.1.14.6 Disabling a Dedicated Keystore 502
4.2 Key Pair Management APIs 509
4.2.1 Key Pair Management 509
4.2.1.1 Creating and Importing an SSH Key Pair 510
4.2.1.2 Accessing the page for clearing private keys 514
4.2.1.3 Querying the SSH Key Pair List 516
4.2.1.4 Querying SSH Key Pair Details 520
4.2.1.5 Deleting an SSH Key Pair 524
4.2.1.6 Updating SSH Key Pair Description 526
4.2.1.7 Accessing the page for importing private keys 529
4.2.1.8 Exporting a private key 533
4.2.1.9 Importing SSH Key Pairs in Batches 536
4.2.1.10 Exporting Private Keys of Key Pairs in Batches 541
4.2.2 Key pair task management 544
4.2.2.1 Binding an SSH Key Pair 544
4.2.2.2 Unbind an SSH Key Pair 549
4.2.2.3 Binding SSH Key Pairs in Batches 554
4.2.2.4 Querying Task Information 560
4.2.2.5 Querying Running Tasks 563
4.2.2.6 Querying Task Failure Information 566
4.2.2.7 Delete all failed tasks 569
4.2.2.8 Delete a failed task 571
4.3 Secret Management APIs 573
4.3.1 Lifecycle Management 573
4.3.1.1 Importing Secrets in Batches 573
4.3.1.2 Deleting Secrets in Batches 579
4.3.1.3 Creating a Secret 583
4.3.1.4 Querying the Secret List 593
4.3.1.5 Querying a Secret 600
4.3.1.6 Updating a Secret 607
4.3.1.7 Deleting a Secret Immediately 615
4.3.1.8 Restoring a Secret Object 619
4.3.1.9 Downloading Secret Backup 625
4.3.1.10 Creating a Scheduled Secret Deletion Task 629
4.3.1.11 Canceling a Scheduled Secret Deletion Task 636
4.3.1.12 Rotating a Secret 642

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.3.2 Secret Version Management 648
4.3.2.1 Creating a Secret Version 648
4.3.2.2 Querying the Secret Version List 653
4.3.2.3 Updating the Secret Version 659
4.3.2.4 Querying the Secret Version and Value 664
4.3.3 Secret Version Status Management 669
4.3.3.1 Updating the Version Status of a Secret 670
4.3.3.2 Querying the Version Status of a Secret 674
4.3.3.3 Deleting the Version Status of a Secret 678
4.3.4 Secret Tag Management 682
4.3.4.1 Querying a Secret Instance 682
4.3.4.2 Adding or Deleting Secret Tags in Batches 693
4.3.4.3 Querying Secret Tags 699
4.3.4.4 Querying Secret Tags 705
4.3.4.5 Deleting a Secret Tag 711
4.3.4.6 Querying Project Tags 716
4.3.5 Event Management 721
4.3.5.1 Creating an Event 721
4.3.5.2 Querying Events 729
4.3.5.3 Querying the Event List 735
4.3.5.4 Update an Event 742
4.3.5.5 Deleting an Event Immediately 749
4.3.5.6 Querying Triggered Event Notification Records 754
4.3.6 Secret Rotation Management 761
4.3.6.1 Querying the Task List 761
4.3.6.2 Creating a Service Agency 766
4.3.6.3 Checking Whether a Service Agency Exists 769
4.3.6.4 Obtaining the Secret Rotation Function Template 773
4.3.7 User Management 776
4.3.7.1 Enabling a User 776
4.3.7.2 Changing a User Password 778
4.3.7.3 Importing Users in Batches 780
4.3.7.4 Disabling a User 784
4.3.7.5 User Management 786
4.3.7.6 Querying the User List 791
4.3.7.7 Updating a User 794
4.3.7.8 Deleting a User 799
4.3.7.9 Obtaining User Details 800
4.3.8 Secret Detection Management 803
4.3.8.1 Checking the Imported Secret Strength 803
4.3.8.2 Obtaining the Tenant Secret Detection Configuration 805
4.3.8.3 Changing the Tenant Secret Detection Configuration 807

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.3.9 Authorization Management 810
4.3.9.1 Authorization Operations 810
4.3.9.2 Deleting an Authorization 814
4.3.9.3 Authorization List 817
4.3.9.4 Updating an Authorization 823
4.3.10 Password Management 827
4.3.10.1 Generating a Random Password 828
5 Historical APIs 832
5.1 Managing SSH Key Pairs (V2.1) 832
5.1.1 Querying the List of SSH Key Pairs (V2.1) 832
5.1.2 Querying Details About an SSH Key Pair (V2.1) 834
5.1.3 Creating and Importing an SSH Key Pair (V2.1) 836
5.1.4 Deleting an SSH Key Pair (V2.1) 842
5.1.5 Modifying the Description of a Key Pair (V2.1) 843
5.2 Managing SSH Key Pairs (V2) 844
5.2.1 Querying the List of SSH Key Pairs (V2) 844
5.2.2 Querying Details About an SSH Key Pair (V2) 845
5.2.3 Creating and Importing an SSH Key Pair (V2) 847
5.2.4 Deleting an SSH Key Pair (V2) 851
5.2.5 Copying an SSH Key Pair (V2) 851
6 Application Examples 854
6.1 Example 1: Encrypting or Decrypting Small Volumes of Data 854
6.2 Example 2: Encrypting or Decrypting Large Volumes of Data 856
6.3 Example 3: Querying Information About Keys 859
7 Permissions Policies and Supported Actions 863
7.1 Introduction to Permissions Policies and Supported Actions 863
7.2 Actions Supported by Policy-based Authorization 865
7.3 Actions Supported by Identity Policy-based Authorization 870
7.3.1 Actions Supported by Identity Policy-based Authorization (KMS) 871
7.3.2 Actions Supported by Identity Policy-based Authorization (KPS) 903
7.3.3 Actions Supported by Identity Policy-based Authorization (CSMS) 912
7.3.4 Actions Supported by Identity Policy-based Authorization (DHSM) 924
A Appendix 931
A.1 Status Codes 931
A.2 Error Code 932
A.3 Obtaining a Project ID 950

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1 Before You Start

Overview

Data Encryption Workshop (DEW) is a comprehensive cloud data encryption service. It provides Key Management Service (KMS), Dedicated HSM (DHSM), and Key Pair Service (KPS). DEW uses hardware security modules (HSMs) to protect your keys, and can be integrated with other Huawei cloud services to address data security, key security, and key management issues. Additionally, DEW allows you to develop customized encryption applications.

Before calling DEW APIs, ensure that you have understood the concepts related to DEW. For more information, see **What Is DEW?**

NOTICE

When interconnecting with KMS, retry is required. Error code such as 504, 502, 500, and 429 are included. Retry three to five times. For error codes 502 and 504, the timeout interval should be 5 to 8 seconds. Do not configure a long timeout interval. Otherwise, the client cannot respond.

API Calling

DSC supports Representational State Transfer (REST) APIs, allowing you to call APIs using HTTPS. For details, see **Making an API Request**.

Endpoints

An endpoint is the **request address** for calling an API. Endpoints vary depending on services and regions. For the endpoints of all services, see **Regions and Endpoints**.

Constraints

The number of keys that you can create is determined by your quota. For details, see **Service Quota**.

In KMS, TPS (the number of API operations that can be performed by a user per second) is set to **20**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Concepts

- Accounts

  An account is created upon successful registration with the cloud platform. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used directly to perform routine management. For security purposes, create Identity and Access Management (IAM) users and grant them permissions for routine management.

- User

  An IAM user is created by an account in IAM to use cloud services. Each IAM user has its own identity credentials (password and access keys).

  The account name, username, and password will be required for API authentication.

- Region

  Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.

- Availability Zone (AZ)

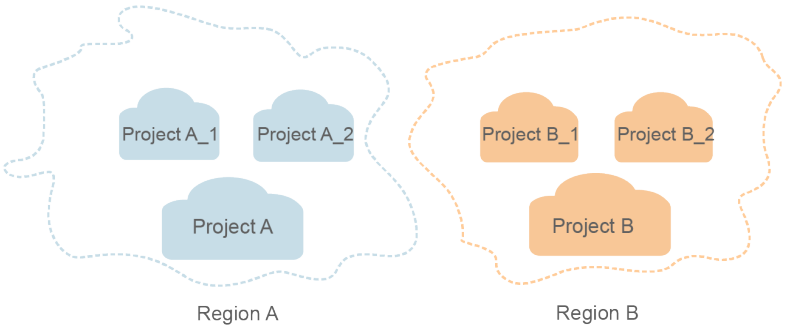
  An AZ comprises one or multiple physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Compute, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.

- Project

  A project corresponds to a region. Projects group and isolate resources (including compute, storage, and network resources) across physical regions. Users can be granted permissions in a default project to access all resources in the region associated with the project. For more refined access control, create subprojects under a project and create resources in the subprojects. Users can then be assigned permissions to access only specific resources in the subprojects.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 1-1 Project isolation model



- Enterprise Project

  Enterprise projects group and manage resources across regions. Resources in enterprise projects are logically isolated from each other. An enterprise project can contain resources in multiple regions, and resources can be directly transferred between enterprise projects.

  For details about how to obtain enterprise project IDs and features, see **Applicable Scenarios**.

Selecting an API Type

For SSH key pairs, V3, V2.1, and V2 APIs are available. V3 APIs are recommended.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 Calling APIs

Making an API Request

Authentication

Response

2.1 Making an API Request

This section describes the structure of a REST API request, and uses the IAM API for **creating an IAM user as the administrator** as an example to demonstrate how to call an API. The obtained token can then be used to authenticate the calling of other APIs.

Request URI

A request URI is in the following format:

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

Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be transmitted separately.

- **URI-scheme**:

  Protocol used to transmit requests. All APIs use HTTPS.

- **Endpoint**:

  Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**.

  For example, the endpoint of IAM in region **CN-Hong Kong** is **iam.ap-southeast-1.myhuaweicloud.com**.

- **resource-path**:

  Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.

- **query-string**:

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain an IAM token in the **CN-Hong Kong** region, obtain the endpoint of IAM (**iam.ap-southeast-1.myhuaweicloud.com**) for this region and the resource-path (**/v3.0/OS-USER/users**) in the URI of the API used for **creating an IAM user**. Then, construct the URI as follows:

```
https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
```

Figure 2-1 Example URI

NOTE

To simplify the URI display in this document, each API is provided only with a **resource-path** and a request method. The **URI-scheme** of all APIs is **HTTPS**, and the endpoints of all APIs in the same region are identical.

Request Methods

The HTTP protocol defines the following request methods that can be used to send a request to the server:

- **GET**: requests the server to return specified resources.
- **PUT**: requests the server to update specified resources.
- **POST**: requests the server to add resources or perform special operations.
- **DELETE**: requests the server to delete specified resources, for example, an object.
- **HEAD**: same as GET except that the server must return only the response header.
- **PATCH**: requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API used to **obtain a user token**, the request method is POST. The request is as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
```

Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request header fields are as follows:

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**. Other values of this field will be provided for specific APIs if any.
- **Authorization**: specifies signature authentication information. This field is optional. When AK/SK authentication is enabled, this field is automatically specified when SDK is used to sign the request.
- **X-Sdk-Date**: specifies the time when a request is sent. This field is optional. When AK/SK authentication is enabled, this field is automatically specified when SDK is used to sign the request.
- **X-Auth-Token**: specifies a user token only for token-based API authentication. The user token is a response to the API used to **obtain a user token**. This API is the only one that does not require authentication.
- **X-Project-ID**: specifies subproject ID. This field is optional and can be used in multi-project scenarios. The **X-Project-ID** field is mandatory in the request header for accessing resources in a subproject through AK/SK-based authentication.
- **X-Domain-ID**: account ID, which is optional. When you call APIs of global services using AK/SK-based authentication, **X-Domain-ID** needs to be configured in the request header.

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
Content-Type: application/json
X-Sdk-Date: 20240416T095341Z
Authorization: SDK-HMAC-SHA256 Access=**********, SignedHeaders=content-type;host;x-sdk-date,
Signature=**********
```

NOTE

In addition to supporting token-based authentication, APIs also support authentication using access key ID/secret access key (AK/SK). During AK/SK-based authentication, an SDK is used to sign the request, and the **Authorization** (signature information) and **X-Sdk-Date** (time when the request is sent) header fields are automatically added to the request.

For more information, see **AK/SK-based Authentication**.

Request Body

The body of a request is often sent in a structured format as specified in the **Content-Type** header field. The request body transfers content except the request header.

The request body varies between APIs. Some APIs do not require the request body, such as the APIs requested using the GET and DELETE methods.

In the case of the API used to **obtain a user token**, the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Replace the italic fields in bold with the actual values.

- **accountid**: ID of the account to which the IAM user belongs.
- **username**: IAM username to be created.
- **email**: email address of the IAM user.
- **************: password of the IAM user.

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users

Content-Type: application/json
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
X-Sdk-Date: 20240416T095341Z
Authorization: SDK-HMAC-SHA256 Access=**********, SignedHeaders=content-type;host;x-sdk-date,
Signature=**********

{
    "user": {
        "domain_id": "accountid",
        "name": "username",
        "password": "**********",
        "email": "email",
        "description": "IAM User Description"
    }
}
```

If all data required for the API request is available, you can send the request to call the API through **curl**, **Postman**, or coding.

2.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

- Token-based authentication: Requests are authenticated using a token.
- AK/SK authentication: Requests are encrypted using AK/SK pairs. This method is recommended because it provides higher security than token-based authentication.

Token-based Authentication

NOTE

- The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the IAM API used to obtain a user token.
- Ensure that the token is valid when you use it. Using a token that will soon expire may cause API calling failures.

A token specifies temporary permissions in a computer system. During API authentication using a token, the token is added to requests to get permissions for calling the API.

You can **obtain a token** by calling an API. A project-level token is required for calling DEW APIs. When calling an API to obtain a user token, set **project** in **auth.scope** in the request body, as shown in the following example.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            "name": "xxxxxxxx"
        }
    }
  }
}
```

After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when calling other APIs. For example, if the token is **ABCDEFG....**, add **X-Auth-Token: ABCDEFG....** to a request as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
Content-Type: application/json
X-Auth-Token: ABCDEFG....
```

AK/SK-based Authentication

NOTE

- AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.
- You can use the AK/SK in a permanent or temporary access key. The **X-Security-Token** field must be configured if the AK/SK in a temporary access key is used, and the field value is **security_token** of the temporary access key.

In AK/SK-based authentication, AK/SK is used to sign requests and the signature is then added to the requests for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests. For details about how to sign requests and use the signing SDK, see **API Request Signing Guide**.

NOTICE

The signing SDK is only used for signing requests and is different from the SDKs provided by services.

2.3 Response

After sending a request, you will receive a response, including a status code, response header, and response body.

Status Codes

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see **Status Codes**.

For example, if status code **201** is returned for calling the API used to **obtain a user token**, the request is successful.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Header

A response header corresponds to a request header, for example, **Content-Type**.

If the API is used to **obtain a user token**, the response header shown in **Figure 2-2** is returned.

Figure 2-2 Header of the response to the request for obtaining a user token


```
"X-Frame-Options": "SAMEORIGIN",
"X-IAM-ETag-id": "2562365939-d8f6f12921974cb097338ac11fceac8a",
"Transfer-Encoding": "chunked",
"Strict-Transport-Security": "max-age=31536000; includeSubdomains;",
"Server": "api-gateway",
"X-Request-Id": "af2953f2bcc67a42325a69a19e6c32a2",
"X-Content-Type-Options": "nosniff",
"Connection": "keep-alive",
"X-Download-Options": "noopen",
"X-XSS-Protection": "1; mode=block;",
"X-IAM-Trace-Id": "token_[redacted]_null_af2953f2bcc67a42325a69a19e6c32a2",
"Date": "Tue, 21 May 2024 09:03:40 GMT",
"Content-Type": "application/json; charset=utf8"
```


Response body

A response body is generally returned in a structured format, corresponding to the **Content-Type** in the response header, and is used to transfer content other than the response header.

The following shows part of the response body for the API to **obtain a user token**. For the sake of space, only part of the content is displayed here.


```
{
    "user": {
        "id": "c131886aec...",
        "name": "IAMUser",
        "description": "IAM User Description",
        "areacode": "",
        "phone": "",
        "email": "***@***.com",
        "status": null,
        "enabled": true,
        "pwd_status": false,
        "access_mode": "default",
        "is_domain_owner": false,
        "xuser_id": "",
        "xuser_type": "",
        "password_expires_at": null,
        "create_time": "2024-05-21T09:03:41.000000",
        "domain_id": "d78cbac1.....",
        "xdomain_id": "30086000.....",
        "xdomain_type": "",
        "default_project_id": null
    }
}
```


If an error occurs during API calling, the system returns an error code and a message to you. The following shows the format of an error response body:


```
{
    "error_msg": "Request body is invalid.",
```


 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "error_code": "IAM.0011"
}
```

In the preceding information, **error_code** is an error code, and **error_msg** describes the error.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 API Overview

You can use all functions of DEW by using the APIs provided by DEW and the performance parameters corresponding to the APIs.

Performance parameter types include shared traffic control and basic traffic control.

- Shared traffic control: APIs share the traffic.
- Basic traffic control: Only the current APIs can use the traffic.

NOTE

Generally, APIs share the traffic unless labeled as basic traffic control. For example, secret version creation APIs share the traffic.

Type	Description
Key Management APIs	Create, query, modify, and delete keys.
Secret management APIs	Create, query, modify, and delete secrets.
Key Pair Management APIs	(Latest API version) Create, query, modify, and delete key pairs.
Historical Global	(V2.1 and V2 API versions) Create, query, modify, and delete key pairs.

Key Management APIs

Type	Name	Description	Performance
Global API version query	Querying all API versions	Obtain the API version list.	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Name	Description	Performance
	Querying a specified API version	Query a specified API version.	
Lifecycle management	Creating a key	Create a CMK, which can be symmetric or asymmetric.	20 times per second for a single user 100 times per second globally
	Enabling a key	Enable a key, which can only be used after being enabled.	
	Disabling a key	Disable a CMK. A disabled CMK cannot be used.	
	Scheduling the deletion of a key	Schedule a deletion task for a specified key. The deletion can be scheduled 7 to 1,096 days in advance. After a key is deleted, the data encrypted using the key cannot be decrypted.	
	Canceling the scheduled deletion of a key	Cancel a scheduled deletion of a key. Once the deletion is cancelled, the key can be used.	
	Modifying the key alias	Change the alias of a CMK.	
	Modifying the key description	Change the description of a CMK.	
Data encryption key (DEK) management	Generating a random number	Generate a random number that is 8 bits to 8,192 bits long.	800 times per second for a single user 1,000 times per second globally
	Creating a DEK	Create a DEK. The returned result includes the plaintext and the ciphertext of a DEK.	
	Creating a plaintext-free DEK	Create a plaintext-free DEK. The returned result includes only the plaintext of a DEK.	
	Encrypting a DEK	Use a specified CMK to encrypt a DEK.	
	Decrypting a DEK	Use a specified CMK to decrypt a DEK.	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Name	Description	Performance
Key import management	Obtaining parameters for importing a key	Obtain necessary parameters to import a key, including an import token and a public key.	20 times per second for a single user 100 times per second globally
	Importing key materials	Import the material of a key.	
	Deleting key materials	Delete the material of a key.	
Authorization management	Creating a grant	Grant a user with key operation permissions.	20 times per second for a single user 100 times per second globally
	Revoking a grant	Revoke the key operation permissions granted to a user.	
	Retiring a grant	Retire the granted key operation permissions.	
	Obtaining the grants	Obtain the grants on a key.	
	Obtaining the grants that can be retired	Obtain the grants that can be retired.	
Small-volume data encryption and decryption	Data encryption	Use a specified CMK to encrypt data.	20 times per second for a single user 100 times per second globally
	Data decryption	Decrypt data.	
Signature and verification	Signing data	Digitally sign a message or message digest using the private key of an asymmetric key.	300 times per second for a single user 500 times per second globally
	Signature verification	Verify the signature of a message or message digest using the public key of an asymmetric key.	
Rotation management	Enabling key rotation	Enable the rotation of a CMK. Default master keys and imported keys cannot be rotated.	20 times per second for a single user 100 times per second globally
	Disabling key rotation	Disable the rotation of a CMK.	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Name	Description	Performance
	Modifying the rotation interval	Change the rotation interval for a CMK.	
	Querying the key rotation status	Query the rotation status of a CMK.	
Tag management	Querying key instances	Use tag filtering to query the detailed information of a CMK.	20 times per second for a single user 100 times per second globally
	Querying key tags	Query tags of a specified key.	
	Querying project tags	Query all tag sets of a project.	
	Adding or deleting key tags in batches	Add or delete key tags in batches.	
	Adding key tags	Add tags to a key.	
	Deleting key tags	Delete tags from a key.	
Query	Obtaining the key list	Obtain the list of all keys.	160 times per second for a single user 200 times per second globally
	Obtaining key details	Obtain details of a specified key.	
	Obtaining the number of instances	Obtain the number of created CMKs, excluding the default master keys.	80 times per second for a single user 200 times per second globally
	Querying quotas	Query the total quota of CMKs available and the usage information, excluding the default master keys.	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

CSMS APIs

Type	Name	Description	Quota
Lifecycle management	Creating a secret	Create a secret and stores the secret value in the initial secret version.	300 times per minute for a single user 4,800 times per minute globally
	Obtaining the secret list	Obtain all the secrets created by the current user in the current project.	100 times per second for a single user 200 times per second globally
	Querying a secret	Query a specified secret.	1,200 times per minute for a single user 4,800 times per minute globally
	Updating a secret	Update the metadata of a specified secret.	300 times per minute for a single user 4,800 times per minute globally
	Deleting a secret immediately	Delete a specified secret. The deleted secret cannot be restored.	
	Restoring a secret	Restore a secret by uploading the secret backup file.	
	Downloading a secret backup	Download the backup file of a specified secret.	
	Creating a scheduled secret deletion task	Create a scheduled task to delete a secret after 7 to 30 days.	
	Canceling a scheduled secret deletion task	Cancel the scheduled deletion task of a secret. The secret will be changed to the available state.	
	Secret rotation	Execute rotation for a secret immediately. Create a new version for the specified secret to encrypt and store the generated random secret values. The created secret version is in **SYSCURRENT** state.	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Name	Description	Quota
Secret version management	Creating a secret version	Create a new version for the specified secret to encrypt and store the new value of the secret. By default, the created secret version in **SYSCURRENT** state. The previous version is in **SYSPREVIOUS** state. You can configure **VersionStage** to overwrite the default settings.	Basic traffic control: 80 times per second for a single user 200 times per second globally 80 times per second for applications 80 times per second for IP addresses
	Obtaining the secret version list	Obtain the version list of a specific secret.	300 times per minute for a single user 4,800 times per minute globally
	Updating the secret version	Currently, only the version validity period of a secret whose status is **ENABLED** can be updated. If the associated subscription events include version expired events, only one notification is triggered each time the version validity period is updated.	
	Querying the secret version and value	Query the information about a specified secret version and the plaintext secret value in the version. Only secrets in **Enabled** state can be queried. The value of the latest secret version can be obtained via **/v1/{project_id}/secrets/{secret_name}/versions/latest**. (Set the **{version_id}** in the URL of the current API to **latest**).	Basic traffic control: 160 times per second for a single user 200 times per second globally 160 times per second for applications 160 times per second for IP addresses
Secret version status management	Updating the version status of a secret	Update the version status of a secret.	300 times per minute for a single user 4,800 times per minute globally

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Name	Description	Quota
	Querying the version status of a secret	Query the version of a specified secret version status tag.	
	Deleting the version status of a secret	Delete the status of a specified secret version.	
Secret tag management	Querying a secret instance	Query a secret instance. Filter user secrets by tag and returns the secret list.	300 times per minute for a single user 4,800 times per minute globally
	Adding or deleting secret tags in batches	Add or delete secret tags in batches.	
	Querying secret tags	Query secret tags.	
	Adding a secret tag	Add a secret tag.	
	Deleting a secret tag	Delete a secret tag.	
	Querying project tags	Query all secret tags of a user in a specified project.	
Event management	Creating an event	Create an event that can be configured on one or more secrets. When an event is enabled and the basic event type contained in the event is triggered on the secret, the cloud service sends the corresponding event notification to the notification topic specified by the event.	300 times per minute for a single user 4,800 times per minute globally
	Querying an event	Query information about a specified event.	
	Obtaining the event list	Obtain all events created by the current user in the project.	
	Updating an event	Update the metadata of a specified event. The following metadata can be updated: event enabling status, basic type list, and notification topic.	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Name	Description	Quota
	Deleting an event immediately	Delete a specified event. The deleted event cannot be restored. An event cannot be deleted if it is referenced by a secret. Disassociate the event from the secret.	
	Querying the record of triggered event notifications	Query all event notification records triggered in the last three months.	

SSH Key Pair Management APIs

Type	Name	Description	Quota
Key pair management	Creating and importing an SSH key pair	Create and import an SSH key pair.	300 times per minute for a single user 4,800 times per minute globally
	Clearing a private key	Delete the private key of an SSH key pair.	
	Obtaining SSH key pairs	Obtain the list of SSH key pairs.	Basic traffic control: 160 times per second for a single user 200 times per second globally 160 times per second for applications 160 times per second for IP addresses
	Obtaining details about an SSH key pair	Obtain details about an SSH key pair.	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Name	Description	Quota
	Deleting an SSH key pair	Delete an SSH key pair.	300 times per minute for a single user 4,800 times per minute globally
	Updating the description about an SSH key pair	Update the description about an SSH key pair.	
	Importing a private key	Import a private key to a specified key pair.	
	Exporting a private key	Export the private key of a specified key pair.	
Key pair task management	Binding an SSH key pair	Bind an SSH key pair to a specified VM. The private key of the SSH key pair for the VM is required if you want to replace the key pair, but not required if you want to reset the key pair.	300 times per minute for a single user 4,800 times per minute globally
	Unbinding an SSH key pair	Unbind an SSH key pair from a specified VM and restores SSH password login.	
	Binding SSH key pairs in batches	Bind SSH key pairs in batches to a specified VM.	Basic traffic control: 10 times per minute for a single user 20 times per minute globally 10 times per minute for applications 10 times per minute for IP addresses
	Obtaining task information	Obtain the execution status of the current task based on the task ID returned by the SSH key pair API.	300 times per minute for a single user 4,800 times per minute globally
	Querying running tasks	Query running tasks.	
	Querying failed tasks	Query information about failed tasks, such as binding and unbinding tasks.	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Type	Name	Description	Quota
	Deleting all failed tasks	Delete information about failed tasks.	
	Deleting failed tasks	Delete failed tasks.	

Global History

Global Type	Description
Key pair management APIs (V2.1)	Query the list of key pairs.
	Query details of a key pair.
	Create and import a key pair. You can manage the private keys on the cloud.
	Delete an SSH key pair based on the key pair name.
	Modify description of a key pair of a specified name.
Key pair management APIs (V2.0)	Query the list of key pairs.
	Query a key pair by its name.
	Create a key pair or import a public key to the cloud to generate a key pair. After an SSH key pair is created, you need to download the private key to a local directory. Then, you can use the private key to log in to an ECS. For ECS security purposes, the private key can be downloaded only once. Keep it secure.
	Delete an SSH key pair based on the key pair name.
	A tenant may contain multiple users. This API is used to copy the key pair from the target user to the current user under the same tenant account.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4 APIs

Key Management APIs

Key Pair Management APIs

Secret Management APIs

4.1 Key Management APIs

4.1.1 Key Lifecycle Management

4.1.1.1 Creating a Key

Function

This API is used to create a symmetric or asymmetric CMK.

A symmetric key is a 256-bit AES key or a 128-bit SM4 key. It can be used to encrypt a small amount of data or DEKs.

An asymmetric key is a RSA key or an ECC key pair (including SM2 key pair). It can be used for data encryption and decryption, digital signature, and signature verification.

Constraints

The alias of the default CMK automatically created by the service ends with **/default**. To avoid a conflict with the default CMK's alias, do not create a CMK whose alias also ends with **/default**. If you have created an enterprise project, the default CMKs can only be stored in the enterprise project. Enterprise resources cannot be moved around. Default CMKs can be used for cloud encryption in non-default enterprise projects to meet compliance requirements. If you need to manage enterprise resources, create a key and use it.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:create	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage	-	-
		-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys		

URI

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

Table 4-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-2 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-3 Request body parameters

Parameter	Mandatory	Type	Description
key_alias	Yes	String	Alias of a non-default master key. The value is a string of 1 to 255 characters that match the regular expression ^[a-zA-Z0-9:/_-]{1,255}$ and must be different from the alias of the Default Master Key.
key_spec	No	String	Key generation algorithm. The default value is **AES_256**. Possible values are as follows: **AES_256** **SM4** **RSA_2048** **RSA_3072** **RSA_4096** **EC_P256** **EC_P384** **SM2**
key_usage	No	String	Key usage. The default value of the symmetric key is **ENCRYPT_DECRYPT** and the default value of the asymmetric key is **SIGN_VERIFY**.
key_description	No	String	Key description. It can contain 0 to 255 characters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
origin	No	String	Key source. The default value is **kms**. Possible values are as follows: **kms**: The key is generated by KMS. **external**: The key is imported.
enterprise_project_id	No	String	Enterprise project ID If you haven't created any enterprise project, do not configure this field. If you have created an enterprise project, configure this field during resource creation. If this field is not configured, newly created resources are listed in the default enterprise project whose ID is **0**. Note: If you do not have the permission to create resources in the default enterprise project whose ID is **0**, an API error is reported.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**
keystore_id	No	String	Keystore ID. The default KMS keystore is used by default.
vm_id	No	String	ID of the VM created using a key. This parameter is valid only in the level-4 cryptography testing scenario.

Response Parameters

Status code: 200

Table 4-4 Response body parameters

Parameter	Type	Description
key_info	**KeKInfo** object	Key details.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-5 KeKInfo

Parameter	Type	Description
key_id	String	Key ID.
domain_id	String	User domain ID.

Status code: 400

Table 4-6 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-7 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-8 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-9 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-10 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-11 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-12 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-13 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-14 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-15 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-16 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-17 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-18 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-19 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

Create a key whose alias is **test**.

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

Example Responses

Status code: 200

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

Create a key whose alias is **test**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CreateKeySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateKeyRequest request = new CreateKeyRequest();
        CreateKeyRequestBody body = new CreateKeyRequestBody();
        body.withKeyAlias("test");
        request.withBody(body);
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        try {
            CreateKeyResponse response = client.createKey(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Create a key whose alias is **test**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateKeyRequest()
        request.body = CreateKeyRequestBody(
            key_alias="test"
        )
        response = client.create_key(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Create a key whose alias is **test**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateKeyRequest{}
    request.Body = &model.CreateKeyRequestBody{
        KeyAlias: "test",
    }
    response, err := client.CreateKey(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.1.2 Enabling a Key

Function

This API is used to enable a key. Only enabled keys can be used.

Note: Only keys that are disabled can be enabled.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:enable	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

URI

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

Table 4-20 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-21 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-22 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-23 Response body parameters

Parameter	Type	Description
key_info	**KeyStatusInfo** object	Key status.

Table 4-24 KeyStatusInfo

Parameter	Type	Description
key_id	String	Key ID
key_state	String	Key status. Possible values are as follows: **2**: Enabled **3**: Disabled **4**: To be deleted **5**: To be imported **7**: Frozen

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-25 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-26 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-27 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-28 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-29 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-30 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-31 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-32 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-33 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-34 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-35 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-36 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-37 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-38 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Enable the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

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

Example Responses

Status code: 200

Request succeeded.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
{
  "key_info" : {
    "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "key_state" : "2"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Enable the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class EnableKeySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        EnableKeyRequest request = new EnableKeyRequest();
        OperateKeyRequestBody body = new OperateKeyRequestBody();
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            EnableKeyResponse response = client.enableKey(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Python

Enable the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = EnableKeyRequest()
        request.body = OperateKeyRequestBody(
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.enable_key(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Enable the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.EnableKeyRequest{}
    request.Body = &model.OperateKeyRequestBody{
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.EnableKey(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.1.1.3 Disabling a Key

Function

This API is used to disable a key. A disabled key cannot be used. Only an enabled key can be disabled.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:disable	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

URI

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-39 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-40 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-41 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-42 Response body parameters

Parameter	Type	Description
key_info	**KeyStatusInfo** object	Key status.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-43 KeyStatusInfo

Parameter	Type	Description
key_id	String	Key ID
key_state	String	Key status. Possible values are as follows: **2**: Enabled **3**: Disabled **4**: To be deleted **5**: To be imported **7**: Frozen

Status code: 400

Table 4-44 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-45 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-46 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-47 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-48 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-49 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-50 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-51 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-52 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-53 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-54 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-55 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-56 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-57 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Disable the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_info" : {
    "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "key_state" : "3"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Disable the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class DisableKeySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        DisableKeyRequest request = new DisableKeyRequest();
        OperateKeyRequestBody body = new OperateKeyRequestBody();
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            DisableKeyResponse response = client.disableKey(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Disable the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DisableKeyRequest()
        request.body = OperateKeyRequestBody(
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.disable_key(request)
        print(response)
    except exceptions.ClientRequestException as e:
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Disable the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DisableKeyRequest{}
    request.Body = &model.OperateKeyRequestBody{
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.DisableKey(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.1.4 Scheduling the Deletion for a Key

Function

This API is used to set the number of days after which a key will be deleted. The value ranges from **7** to **1,096** days.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:scheduleKeyDeletion	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:update	-
		-	kms:ScheduleKeyDeletionPendingWindowInDays		

URI

POST /v1.0/{project_id}/kms/schedule-key-deletion

Table 4-58 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-59 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-60 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
pending_days	Yes	String	Number of days after which a CMK is scheduled to be deleted. The value can be from 7 to 1,096 days.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-61 Response body parameters

Parameter	Type	Description
key_id	String	Key ID
key_state	String	Key status. Possible values are as follows: **2**: Enabled **3**: Disabled **4**: To be deleted **5**: To be imported **7**: Frozen

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-62 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-63 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-64 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-65 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-66 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-67 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-68 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-69 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-70 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-71 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-72 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-73 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-74 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-75 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Delete the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** after seven days.

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

Example Responses

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "key_state" : "4"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Delete the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** after seven days.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class DeleteKeySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteKeyRequest request = new DeleteKeyRequest();
        ScheduleKeyDeletionRequestBody body = new ScheduleKeyDeletionRequestBody();
        body.withPendingDays("7");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            DeleteKeyResponse response = client.deleteKey(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        }
    }
}
```

Python

Delete the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** after seven days.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteKeyRequest()
        request.body = ScheduleKeyDeletionRequestBody(
            pending_days="7",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.delete_key(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Delete the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** after seven days.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteKeyRequest{}
    request.Body = &model.ScheduleKeyDeletionRequestBody{
        PendingDays: "7",
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.DeleteKey(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.1.1.5 Canceling the Scheduled Deletion for a Key

Function

This API is used to cancel the scheduled deletion of a key. Only keys that are scheduled a deletion task can be deleted by this API.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:cancelKeyDeletion	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:update	-

URI

POST /v1.0/{project_id}/kms/cancel-key-deletion

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-76 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-77 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-78 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-79 Response body parameters

Parameter	Type	Description
key_id	String	Key ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
key_state	String	Key status. Possible values are as follows: **2**: Enabled **3**: Disabled **4**: To be deleted **5**: To be imported **7**: Frozen

Status code: 400

Table 4-80 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-81 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-82 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-83 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-84 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-85 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-86 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-87 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-88 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-89 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-90 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-91 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-92 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-93 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Cancel the scheduled deletion task of the key whose status ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "key_state" : "3"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Cancel the scheduled deletion task of the key whose status ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CancelKeyDeletionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CancelKeyDeletionRequest request = new CancelKeyDeletionRequest();
        OperateKeyRequestBody body = new OperateKeyRequestBody();
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            CancelKeyDeletionResponse response = client.cancelKeyDeletion(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Cancel the scheduled deletion task of the key whose status ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CancelKeyDeletionRequest()
        request.body = OperateKeyRequestBody(
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.cancel_key_deletion(request)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Cancel the scheduled deletion task of the key whose status ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CancelKeyDeletionRequest{}
    request.Body = &model.OperateKeyRequestBody{
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.CancelKeyDeletion(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.1.6 Modifying a Key Alias

Function

This API is used to modify the alias of a CMK.

The aliases of the following keys cannot be modified:

Service default CMKs that end with **/default**

Keys that are scheduled to be deleted

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:updateKeyAlias	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:update	-

URI

POST /v1.0/{project_id}/kms/update-key-alias

Table 4-94 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-95 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-96 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
key_alias	Yes	String	Alias of a non-default CMK. The value can contain 1 to 255 strings and matches the regular expression **^[a-zA-Z0-9:/_-]{1,255}$**. The suffix cannot be **/default**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-97 Response body parameters

Parameter	Type	Description
key_info	**KeyAliasInfo** object	Key alias.

Table 4-98 KeyAliasInfo

Parameter	Type	Description
key_id	String	Key ID.
key_alias	String	Key alias.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-99 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-100 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-101 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-102 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-103 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-104 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-105 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-106 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-107 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-108 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-109 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-110 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-111 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-112 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Change the alias of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to **test**.

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

Example Responses

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

Change the alias of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to **test**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class UpdateKeyAliasSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateKeyAliasRequest request = new UpdateKeyAliasRequest();
        UpdateKeyAliasRequestBody body = new UpdateKeyAliasRequestBody();
        body.withKeyAlias("test");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            UpdateKeyAliasResponse response = client.updateKeyAlias(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Change the alias of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to **test**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateKeyAliasRequest()
        request.body = UpdateKeyAliasRequestBody(
            key_alias="test",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.update_key_alias(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Change the alias of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to **test**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateKeyAliasRequest{}
    request.Body = &model.UpdateKeyAliasRequestBody{
        KeyAlias: "test",
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.UpdateKeyAlias(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Error Codes

See **Error Codes**.

4.1.1.7 Modifying a Key Description

Function

This API is used to modify the CMK details.

The details of the following keys cannot be modified:

Service default CMKs that end with **/default**

Keys that are scheduled to be deleted

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:updateKeyDescription	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:update	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

URI

POST /v1.0/{project_id}/kms/update-key-description

Table 4-113 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-114 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-115 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
key_description	Yes	String	Key description. It can contain 0 to 255 characters.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-116 Response body parameters

Parameter	Type	Description
key_info	**KeyDescriptionInfo** object	Key description.

Table 4-117 KeyDescriptionInfo

Parameter	Type	Description
key_id	String	Key ID.
key_description	String	Key description.

Status code: 400

Table 4-118 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-119 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-120 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-121 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-122 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-123 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-124 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-125 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-126 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-127 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-128 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-129 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-130 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-131 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Change the description of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to **test**.

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

Example Responses

Status code: 200

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

Change the description of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to **test**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class UpdateKeyDescriptionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateKeyDescriptionRequest request = new UpdateKeyDescriptionRequest();
        UpdateKeyDescriptionRequestBody body = new UpdateKeyDescriptionRequestBody();
        body.withKeyDescription("test");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            UpdateKeyDescriptionResponse response = client.updateKeyDescription(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Change the description of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to **test**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateKeyDescriptionRequest()
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        request.body = UpdateKeyDescriptionRequestBody(
            key_description="test",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.update_key_description(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Change the description of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to **test**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateKeyDescriptionRequest{}
    request.Body = &model.UpdateKeyDescriptionRequestBody{
        KeyDescription: "test",
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.UpdateKeyDescription(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.2 DEK Management

4.1.2.1 Generating a Random Number

Function

This API is used to generate an 8-bit to 8,192-bit random number.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms::generateRandom	Write	-	kms:RecipientAttestation	• kms:cmk:generate	-

URI

POST /v1.0/{project_id}/kms/gen-random

Table 4-132 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-133 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-134 Request body parameters

Parameter	Mandatory	Type	Description
random_data_length	Yes	String	Bit length of a random number. The value must be a multiple of 8 and ranges from **8** to **8192**, for example, **512**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 200

Table 4-135 Response body parameters

Parameter	Type	Description
random_data	String	Random number in hexadecimal format. Two characters represent 1 byte. The length of the random number must be the same as that of the user input parameter **random_data_length**.

Status code: 400

Table 4-136 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-137 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-138 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-139 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-140 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-141 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-142 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-143 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-144 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-145 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-146 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-147 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-148 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-149 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Generate a 512-bit random number.

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "random_data" : "5791C223E87120BE4B98D168F47A58BB2A88834EEADC"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Generate a 512-bit random number.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CreateRandomSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

    KmsClient client = KmsClient.newBuilder()
            .withCredential(auth)
            .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
            .build();
    CreateRandomRequest request = new CreateRandomRequest();
    GenRandomRequestBody body = new GenRandomRequestBody();
    body.withRandomDataLength("512");
    request.withBody(body);
    try {
        CreateRandomResponse response = client.createRandom(request);
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
  }
}
```

Python

Generate a 512-bit random number.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateRandomRequest()
        request.body = GenRandomRequestBody(
            random_data_length="512"
        )
        response = client.create_random(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        print(e.error_code)
        print(e.error_msg)
```

Go

Generate a 512-bit random number.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateRandomRequest{}
    request.Body = &model.GenRandomRequestBody{
        RandomDataLength: "512",
    }
    response, err := client.CreateRandom(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.2.2 Creating a DEK

Function

This API is used to create a DEK. The returned result contains both plaintext and ciphertext.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:createDataKey	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:dek:create	-
		-	• kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext		

URI

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

Table 4-150 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-151 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-152 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
key_spec	No	String	Bit length of the generated key. The value can be **AES_256**, **AES_128**, **SM4**, **HMAC_256**, **HMAC_384**, **HMAC_512**, or **HMAC_SM3**. • **AES_256**: A 256-bit symmetric key • **AES_128**: A 128-bit symmetric key • **SM4**: An SM4 key • **HMAC_256**: An HMAC_256 key • **HMAC_384**: An HMAC_384 key • **HMAC_512**: An HMAC_512 key • **HMAC_SM3**: An HMAC_SM3 key • If neither of them is specified, a 256-bit key is generated by default. • If both of them are specified, only **datakey_length** takes effect. Notes: Set either **datakey_length** or **key_spec**.
datakey_length	No	String	Key length by bit. The value ranges from **8** to **8,192** and must be a multiple of 8. Note: You must configure either **datakey_length** or **key_spec**. If both are empty, a 256-bit key is generated by default. If both are specified, only **datakey_length** takes effect.
additional_authenticated_data	No	String	Non-sensitive extra data used for authentication. The value is a random string with at most 128 bytes.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
pin	No	String	PIN code, which is used to authenticate the data key. This parameter is valid only in the level-4 cryptography testing scenario.
pin_type	No	String	PIN code type. The default value is **CipherText**. The value can be: • **PlainText**: plaintext PIN • **CipherText**: ciphertext PIN
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-153 Response body parameters

Parameter	Type	Description
key_id	String	Key ID.
plain_text	String	Plaintext DEK in hexadecimal format. Two characters represent 1 byte.
cipher_text	String	Ciphertext DEK in hexadecimal format. Two characters represent 1 byte.

Status code: 400

Table 4-154 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-155 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-156 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-157 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-158 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-159 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 404

Table 4-160 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-161 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-162 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-163 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-164 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-165 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-166 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-167 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Create a 512-bit plaintext DEK and encrypt it using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**. Return the plaintext key and add **123add** as the associated data.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "datakey_length" : "512",
  "additional_authenticated_data" : "123aad"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "plain_text" : "8151014275E426C72EE7D44267XXXXX...",
  "cipher_text" : "020098009EEAFCE122CAA5927D2XXX..."
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

SDK Sample Code

The SDK sample code is as follows.

Java

Create a 512-bit plaintext DEK and encrypt it using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**. Return the plaintext key and add **123add** as the associated data.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CreateDatakeySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateDatakeyRequest request = new CreateDatakeyRequest();
        CreateDatakeyRequestBody body = new CreateDatakeyRequestBody();
        body.withAdditionalAuthenticatedData("123aad");
        body.withDatakeyLength("512");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            CreateDatakeyResponse response = client.createDatakey(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Python

Create a 512-bit plaintext DEK and encrypt it using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**. Return the plaintext key and add **123add** as the associated data.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateDatakeyRequest()
        request.body = CreateDatakeyRequestBody(
            additional_authenticated_data="123aad",
            datakey_length="512",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.create_datakey(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Create a 512-bit plaintext DEK and encrypt it using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**. Return the plaintext key and add **123add** as the associated data.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateDatakeyRequest{}
    additionalAuthenticatedDataCreateDatakeyRequestBody:= "123aad"
    datakeyLengthCreateDatakeyRequestBody:= "512"
    request.Body = &model.CreateDatakeyRequestBody{
        AdditionalAuthenticatedData: &additionalAuthenticatedDataCreateDatakeyRequestBody,
        DatakeyLength: &datakeyLengthCreateDatakeyRequestBody,
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.CreateDatakey(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Error Codes

See **Error Codes**.

4.1.2.3 Creating a Plaintext-free DEK

Function

This API is used to create a data encryption key (DEK). The returned result contains only ciphertext.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:createDataKeyWithoutPlaintext	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:dek:create	-

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
		-	• kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext		

URI

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

Table 4-168 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-169 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-170 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
key_spec	No	String	Bit length of the generated key. The value can be **AES_256**, **AES_128**, **SM4**, **HMAC_256**, **HMAC_384**, **HMAC_512**, or **HMAC_SM3**. • **AES_256**: A 256-bit symmetric key • **AES_128**: A 128-bit symmetric key • **SM4**: An SM4 key • **HMAC_256**: An HMAC_256 key • **HMAC_384**: An HMAC_384 key • **HMAC_512**: An HMAC_512 key • **HMAC_SM3**: An HMAC_SM3 key • If neither of them is specified, a 256-bit key is generated by default. • If both of them are specified, only **datakey_length** takes effect. Notes: Set either **datakey_length** or **key_spec**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
datakey_length	No	String	Key length by bit. The value ranges from **8** to **8,192** and must be a multiple of 8. Note: You must configure either **datakey_length** or **key_spec**. If both are empty, a 256-bit key is generated by default. If both are specified, only **datakey_length** takes effect.
additional_authenticated_data	No	String	Non-sensitive extra data used for authentication. The value is a random string with at most 128 bytes.
pin	No	String	PIN code, which is used to authenticate the data key. This parameter is valid only in the level-4 cryptography testing scenario.
pin_type	No	String	PIN code type. The default value is **CipherText**. The value can be: • **PlainText**: plaintext PIN • **CipherText**: ciphertext PIN
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-171 Response body parameters

Parameter	Type	Description
key_id	String	Key ID.
cipher_text	String	Encrypted ciphertext in Base64 format

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-172 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-173 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-174 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-175 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-176 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-177 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-178 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-179 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-180 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-181 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-182 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-183 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-184 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-185 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Create a 512-bit plaintext DEK and encrypt it using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**. Do not return the plaintext key and add **123add** as the associated data.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "datakey_length" : "512",
  "additional_authenticated_data" : "123aad"
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "cipher_text" : "020098009EEAFCE122CAA5927D2XXX..."
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create a 512-bit plaintext DEK and encrypt it using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**. Do not return the plaintext key and add **123add** as the associated data.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CreateDatakeyWithoutPlaintextSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateDatakeyWithoutPlaintextRequest request = new CreateDatakeyWithoutPlaintextRequest();
        CreateDatakeyRequestBody body = new CreateDatakeyRequestBody();
        body.withAdditionalAuthenticatedData("123aad");
        body.withDatakeyLength("512");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            CreateDatakeyWithoutPlaintextResponse response = client.createDatakeyWithoutPlaintext(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Create a 512-bit plaintext DEK and encrypt it using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**. Do not return the plaintext key and add **123add** as the associated data.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateDatakeyWithoutPlaintextRequest()
        request.body = CreateDatakeyRequestBody(
            additional_authenticated_data="123aad",
            datakey_length="512",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.create_datakey_without_plaintext(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Create a 512-bit plaintext DEK and encrypt it using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**. Do not return the plaintext key and add **123add** as the associated data.

```
package main

import (
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateDatakeyWithoutPlaintextRequest{}
    additionalAuthenticatedDataCreateDatakeyRequestBody:= "123aad"
    datakeyLengthCreateDatakeyRequestBody:= "512"
    request.Body = &model.CreateDatakeyRequestBody{
        AdditionalAuthenticatedData: &additionalAuthenticatedDataCreateDatakeyRequestBody,
        DatakeyLength: &datakeyLengthCreateDatakeyRequestBody,
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.CreateDatakeyWithoutPlaintext(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.2.4 Creating an RSA Data Key Pair

Function

This API is used to create an RSA data key pair. The returned result contains the plaintext public key and ciphertext private key. You can determine whether to return the plaintext private key based on the parameter.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

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

Table 4-186 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-187 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-188 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	Key ID, which is 36-byte long and matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
key_spec	Yes	String	The algorithm, length, and curve information are included. The value can be **RSA_2048**, **RSA_3072**, or **RSA_4096**.
with_plain_text	No	Boolean	Whether to return the plaintext private key. The default value is **true**.
additional_authenticated_data	No	String	Additional information for authentication and encryption. Do not enter sensitive information.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**.

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-189 Response body parameters

Parameter	Type	Description
key_id	String	Key ID.
key_spec	String	The algorithm, length, and curve information are included. The value can be **RSA_2048**, **RSA_3072**, **RSA_4096**, **ECC_NIST_P256**, **ECC_NIST_P384**, **ECC_NIST_P521**, **ECC_SECG_P256K1**, or **SM2**.
public_key	String	Plaintext public key information.
private_key_cipher_text	String	Ciphertext private key.
private_key_plain_text	String	Plaintext private key. Only one of **private_key_plain_text**, **wrapped_private_key**, and **ciphertext_recipient** can have a value.
wrapped_private_key	String	Ciphertext private key encrypted using the custom private key. Only one of **private_key_plain_text**, **wrapped_private_key**, and **ciphertext_recipient** can have a value.
ciphertext_recipient	String	Ciphertext private key encrypted using the QingTian public key. Only one of **private_key_plain_text**, **wrapped_private_key**, and **ciphertext_recipient** can have a value.

Status code: 400

Table 4-190 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-191 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 401

Table 4-192 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-193 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-194 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-195 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-196 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-197 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-198 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-199 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-200 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-201 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-202 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-203 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "key_spec" : "RSA_2048",
  "with_plain_text" : true,
  "additional_authenticated_data" : "aad",
  "sequence" : "sequence"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "key_spec" : "RSA_2048",
  "public_key" : "public_key",
  "private_key_cipher_text" : "private_key_cipher_text",
  "private_key_plain_text" : "private_key_plain_text",
  "wrapped_private_key" : "wrapped_private_key",
  "ciphertext_recipient" : "ciphertext_recipient"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CreateRsaDatakeyPairSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateRsaDatakeyPairRequest request = new CreateRsaDatakeyPairRequest();
        CreateRsaDatakeyPairRequestBody body = new CreateRsaDatakeyPairRequestBody();
        body.withSequence("sequence");
        body.withAdditionalAuthenticatedData("aad");
        body.withWithPlainText(true);
        body.withKeySpec(CreateRsaDatakeyPairRequestBody.KeySpecEnum.fromValue("RSA_2048"));
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            CreateRsaDatakeyPairResponse response = client.createRsaDatakeyPair(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateRsaDatakeyPairRequest()
        request.body = CreateRsaDatakeyPairRequestBody(
            sequence="sequence",
            additional_authenticated_data="aad",
            with_plain_text=True,
            key_spec="RSA_2048",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.create_rsa_datakey_pair(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateRsaDatakeyPairRequest{}
    sequenceCreateRsaDatakeyPairRequestBody:= "sequence"
    additionalAuthenticatedDataCreateRsaDatakeyPairRequestBody:= "aad"
    withPlainTextCreateRsaDatakeyPairRequestBody:= true
    request.Body = &model.CreateRsaDatakeyPairRequestBody{
        Sequence: &sequenceCreateRsaDatakeyPairRequestBody,
        AdditionalAuthenticatedData: &additionalAuthenticatedDataCreateRsaDatakeyPairRequestBody,
        WithPlainText: &withPlainTextCreateRsaDatakeyPairRequestBody,
        KeySpec: model.GetCreateRsaDatakeyPairRequestBodyKeySpecEnum().RSA_2048,
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.CreateRsaDatakeyPair(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Request failed. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.2.5 Creating an EC Data Key Pair

Function

This API is used to create an EC data key pair. The returned result contains the plaintext public key and ciphertext private key. You can determine whether to return the plaintext private key based on the parameter.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

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

Table 4-204 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-205 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-206 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	Key ID, which is 36-byte long and matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
key_spec	Yes	String	The algorithm, length, and curve information are included. The value can be **ECC_NIST_P256**, **ECC_NIST_P384**, **ECC_NIST_P521**, **ECC_SECG_P256K1**, or **SM2**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
with_plain_text	No	Boolean	Whether to return the plaintext private key. The default value is **true**.
additional_authenticated_data	No	String	Additional information for authentication and encryption. Do not enter sensitive information.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**.

Response Parameters

Status code: 200

Table 4-207 Response body parameters

Parameter	Type	Description
key_id	String	Key ID.
key_spec	String	The algorithm, length, and curve information are included. The value can be **RSA_2048**, **RSA_3072**, **RSA_4096**, **ECC_NIST_P256**, **ECC_NIST_P384**, **ECC_NIST_P521**, **ECC_SECG_P256K1**, or **SM2**.
public_key	String	Plaintext public key information.
private_key_ciphertext	String	Ciphertext private key.
private_key_plaintext	String	Plaintext private key. Only one of **private_key_plain_text**, **wrapped_private_key**, and **ciphertext_recipient** can have a value.
wrapped_private_key	String	Ciphertext private key encrypted using the custom private key. Only one of **private_key_plain_text**, **wrapped_private_key**, and **ciphertext_recipient** can have a value.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
ciphertext_recipient	String	Ciphertext private key encrypted using the QingTian public key. Only one of **private_key_plain_text**, **wrapped_private_key**, and **ciphertext_recipient** can have a value.

Status code: 400

Table 4-208 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-209 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-210 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-211 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-212 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-213 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-214 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-215 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-216 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-217 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-218 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-219 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-220 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-221 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "key_spec" : "ECC_NIST_P256",
  "with_plain_text" : true,
  "additional_authenticated_data" : "aad",
  "sequence" : "sequence"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "key_spec" : "ECC_NIST_P256",
  "public_key" : "public_key",
  "private_key_cipher_text" : "private_key_cipher_text",
  "private_key_plain_text" : "private_key_plain_text",
  "wrapped_private_key" : "wrapped_private_key",
  "ciphertext_recipient" : "ciphertext_recipient"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CreateEcDatakeyPairSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateEcDatakeyPairRequest request = new CreateEcDatakeyPairRequest();
        CreateEcDatakeyPairRequestBody body = new CreateEcDatakeyPairRequestBody();
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        body.withSequence("sequence");
        body.withAdditionalAuthenticatedData("aad");
        body.withWithPlainText(true);
        body.withKeySpec(CreateEcDatakeyPairRequestBody.KeySpecEnum.fromValue("ECC_NIST_P256"));
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            CreateEcDatakeyPairResponse response = client.createEcDatakeyPair(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateEcDatakeyPairRequest()
        request.body = CreateEcDatakeyPairRequestBody(
            sequence="sequence",
            additional_authenticated_data="aad",
            with_plain_text=True,
            key_spec="ECC_NIST_P256",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.create_ec_datakey_pair(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateEcDatakeyPairRequest{}
    sequenceCreateEcDatakeyPairRequestBody:= "sequence"
    additionalAuthenticatedDataCreateEcDatakeyPairRequestBody:= "aad"
    withPlainTextCreateEcDatakeyPairRequestBody:= true
    request.Body = &model.CreateEcDatakeyPairRequestBody{
        Sequence: &sequenceCreateEcDatakeyPairRequestBody,
        AdditionalAuthenticatedData: &additionalAuthenticatedDataCreateEcDatakeyPairRequestBody,
        WithPlainText: &withPlainTextCreateEcDatakeyPairRequestBody,
        KeySpec: model.GetCreateEcDatakeyPairRequestBodyKeySpecEnum().ECC_NIST_P256,
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.CreateEcDatakeyPair(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Request failed. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.2.6 Encrypting a DEK

Function

This API is used to encrypt a DEK using a specified CMK.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:encryptDataKey	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:dek:crypto • kms:dek:encrypt	-
		-	• kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext		

URI

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

Table 4-222 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-223 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-224 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
plain_text	Yes	String	If AES is used for the customer master key (CMK), the value is the plaintext data encryption key (DEK) + the SHA256 value (32 bytes) of the plaintext DEK. If SM4 is used for the CMK, the value is the plaintext DEK + the SM3 value (32 bytes) of the plaintext DEK. The values are hexadecimal strings.
datakey_plain_length	Yes	String	Number of bytes of a DEK in plaintext. The value ranges from **1** to **1024**, for example, **64**.
additional_authenticated_data	No	String	Non-sensitive extra data used for authentication. The value is a random string with at most 128 bytes.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
pin	No	String	PIN code, which is used to authenticate the data key. This parameter is valid only in the level-4 cryptography testing scenario.
pin_type	No	String	PIN code type. The default value is **CipherText**. The value can be: • **PlainText**: plaintext PIN • **CipherText**: ciphertext PIN
key_spec	No	String	Type of the data key to be encrypted. This parameter is valid only in the level-4 cryptography testing scenario. The value can be **SM2** or **RSA**. • **SM2**: SM2 key • **RSA**: RSA key
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-225 Response body parameters

Parameter	Type	Description
key_id	String	Key ID
cipher_text	String	Ciphertext DEK in hexadecimal format. Two characters represent 1 byte.
datakey_length	String	Length of a DEK, in bytes.

Status code: 400

Table 4-226 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-227 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-228 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-229 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-230 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-231 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 404

Table 4-232 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-233 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-234 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-235 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-236 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-237 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-238 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-239 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Encrypt a 512-bit plaintext key using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123add** as the associated data.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "plain_text" :
"7549d9aea901767bf3c0b3e14b10722eaf6f59053bbd82045d04e075e809a0fe6ccab48f8e5efe74e4b18ff0512
525e527b10331100f357bf42125d8d5ced94ffbc8ac72b0785ca7fe33eb6776ce3990b11e32b299d9c0a9ee0305f
b9540f797",
  "datakey_plain_length" : "64",
  "additional_authenticated_data" : "123aad"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "datakey_length" : "64",
  "cipher_text" : "020098009EEAFCE122CAA5927D2XXX..."
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

SDK Sample Code

The SDK sample code is as follows.

Java

Encrypt a 512-bit plaintext key using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123add** as the associated data.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class EncryptDatakeySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        EncryptDatakeyRequest request = new EncryptDatakeyRequest();
        EncryptDatakeyRequestBody body = new EncryptDatakeyRequestBody();
        body.withAdditionalAuthenticatedData("123aad");
        body.withDatakeyPlainLength("64");

body.withPlainText("7549d9aea901767bf3c0b3e14b10722eaf6f59053bbd82045d04e075e809a0fe6ccab48f8e5efe74e4b18ff0512525e527b10331100f357bf42125d8d5ced94ffbc8ac72b0785ca7fe33eb6776ce3990b11e32b299d9c0a9ee0305fb9540f797");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            EncryptDatakeyResponse response = client.encryptDatakey(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Python

Encrypt a 512-bit plaintext key using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123add** as the associated data.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = EncryptDatakeyRequest()
        request.body = EncryptDatakeyRequestBody(
            additional_authenticated_data="123aad",
            datakey_plain_length="64",

plain_text="7549d9aea901767bf3c0b3e14b10722eaf6f59053bbd82045d04e075e809a0fe6ccab48f8e5efe74e4b18ff0512525e527b10331100f357bf42125d8d5ced94ffbc8ac72b0785ca7fe33eb6776ce3990b11e32b299d9c0a9ee0305fb9540f797",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.encrypt_datakey(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Encrypt a 512-bit plaintext key using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123add** as the associated data.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.EncryptDatakeyRequest{}
    additionalAuthenticatedDataEncryptDatakeyRequestBody:= "123aad"
    request.Body = &model.EncryptDatakeyRequestBody{
        AdditionalAuthenticatedData: &additionalAuthenticatedDataEncryptDatakeyRequestBody,
        DatakeyPlainLength: "64",
        PlainText:
"7549d9aea901767bf3c0b3e14b10722eaf6f59053bbd82045d04e075e809a0fe6ccab48f8e5efe74e4b18ff0512
525e527b10331100f357bf42125d8d5ced94ffbc8ac72b0785ca7fe33eb6776ce3990b11e32b299d9c0a9ee0305f
b9540f797",
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.EncryptDatakey(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Error Codes

See **Error Codes**.

4.1.2.7 Decrypting a DEK

Function

This API is used to decrypt DEKs using specified CMKs.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:decryptDataKey	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:dek:crypto • kms:dek:decrypt	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
		-	• kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext		

URI

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

Table 4-240 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-241 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-242 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
cipher_text	Yes	String	Hexadecimal string of the DEK ciphertext and the metadata. It is the value of cipher_text in the encryption result.
datakey_cipher_length	Yes	String	Number of bytes of a key. The value ranges from **1** to **1024**, for example, **64**.
additional_authenticated_data	No	String	Non-sensitive extra data used for authentication. The value is a random string with at most 128 bytes.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-243 Response body parameters

Parameter	Type	Description
data_key	String	Hexadecimal string of the plaintext of a DEK
datakey_length	String	Length of a plaintext DEK, in bytes.
datakey_dgst	String	Hexadecimal string corresponding to the SHA-256 hash value of the plaintext of a DEK.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-244 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-245 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-246 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-247 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-248 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-249 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-250 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-251 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-252 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-253 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-254 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-255 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-256 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-257 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Decrypt a ciphertext DEK into a 64-byte plaintext DEK using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123aad** as the associated data.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "cipher_text" : "020098005273E14E6E8E95F5463BECDC27E80AFxxxxxxxxxx...",
  "datakey_cipher_length" : "64",
  "additional_authenticated_data" : "123aad"
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Responses

Status code: 200

Request succeeded.

```
{
  "data_key" : "000000e724d9cb35df84bb474a37fXXX...",
  "datakey_length" : "64",
  "datakey_dgst" : "F5A5FD42D16A20302798EF6ED3099XXX..."
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Decrypt a ciphertext DEK into a 64-byte plaintext DEK using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123aad** as the associated data.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class DecryptDatakeySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        DecryptDatakeyRequest request = new DecryptDatakeyRequest();
        DecryptDatakeyRequestBody body = new DecryptDatakeyRequestBody();
        body.withAdditionalAuthenticatedData("123aad");
        body.withDatakeyCipherLength("64");
        body.withCipherText("020098005273E14E6E8E95F5463BECDC27E80AFxxxxxxxxxx...");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            DecryptDatakeyResponse response = client.decryptDatakey(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Decrypt a ciphertext DEK into a 64-byte plaintext DEK using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123aad** as the associated data.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DecryptDatakeyRequest()
        request.body = DecryptDatakeyRequestBody(
            additional_authenticated_data="123aad",
            datakey_cipher_length="64",
            cipher_text="020098005273E14E6E8E95F5463BECDC27E80AFxxxxxxxxxx...",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.decrypt_datakey(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Decrypt a ciphertext DEK into a 64-byte plaintext DEK using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123aad** as the associated data.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DecryptDatakeyRequest{}
    additionalAuthenticatedDataDecryptDatakeyRequestBody:= "123aad"
    request.Body = &model.DecryptDatakeyRequestBody{
        AdditionalAuthenticatedData: &additionalAuthenticatedDataDecryptDatakeyRequestBody,
        DatakeyCipherLength: "64",
        CipherText: "020098005273E14E6E8E95F5463BECDC27E80AFxxxxxxxxxx...",
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.DecryptDatakey(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.2.8 Creating a PIN

Function

This API is used to create a PIN, which is used to create and encrypt a DEK in the level-4 cryptography testing scenario.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:createDataKey	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:dek:create	-
		-	• kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext		

URI

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

Table 4-258 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-259 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-260 Request body parameters

Parameter	Mandatory	Type	Description
pin_type	No	String	PIN code type. The default value is **CipherText**. The value can be: • **PlainText** • **CipherText**
keystore_id	No	String	Keystore ID. If the ciphertext PIN is specified, the following content must be specified: **1**: shared cluster on the management plane **2**: shared cluster on the data plane (POD zone) **Others**: exclusive to tenants

Response Parameters

Status code: 200

Table 4-261 Response body parameters

Parameter	Type	Description
pin	String	Created PIN.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-262 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-263 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-264 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-265 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-266 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-267 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-268 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-269 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-270 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-271 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-272 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-273 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-274 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-275 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Specify the shared cluster on the management plane to create a PIN. The ciphertext PIN is returned.

```
{
  "pin_type" : "CipherText",
  "keystore_id" : "1"
}
```

Example Responses

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request succeeded.

```
{
  "pin" : "020098009EEAFCE122CAA5927D2XXX..."
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Specify the shared cluster on the management plane to create a PIN. The ciphertext PIN is returned.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CreatePinSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePinRequest request = new CreatePinRequest();
        CreatePinRequestBody body = new CreatePinRequestBody();
        body.withKeystoreId("1");
        body.withPinType(CreatePinRequestBody.PinTypeEnum.fromValue("CipherText"));
        request.withBody(body);
        try {
            CreatePinResponse response = client.createPin(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    }
}
```

Python

Specify the shared cluster on the management plane to create a PIN. The ciphertext PIN is returned.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePinRequest()
        request.body = CreatePinRequestBody(
            keystore_id="1",
            pin_type="CipherText"
        )
        response = client.create_pin(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Specify the shared cluster on the management plane to create a PIN. The ciphertext PIN is returned.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePinRequest{}
    keystoreIdCreatePinRequestBody:= "1"
    pinTypeCreatePinRequestBody:= model.GetCreatePinRequestBodyPinTypeEnum().CIPHER_TEXT
    request.Body = &model.CreatePinRequestBody{
        KeystoreId: &keystoreIdCreatePinRequestBody,
        PinType: &pinTypeCreatePinRequestBody,
    }
    response, err := client.CreatePin(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Request failed. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.1.3 Small-Size Data Encryption and Decryption

4.1.3.1 Encrypting Data

Function

This API is used to encrypt data using a specified CMK.

Constraints

If you use an asymmetric key for encryption, record the key ID and encryption algorithm, which are required for decryption. If the specified key ID and encryption algorithm do not match those used for encrypting data, the decryption fails.

If you use a symmetric key for decryption, you do not need to provide the key ID and encryption algorithm. KMS stores the information as ciphertext. KMS cannot store metadata in the ciphertext generated using an asymmetric key. A standard asymmetric key ciphertext does not contain configurable fields.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:encryptData	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:crypto • kms:cmk:encrypt	-
		-	• kms:EncryptionAlgorithm • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext		

URI

POST /v1.0/{project_id}/kms/encrypt-data

Table 4-276 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-277 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-278 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
plain_text	Yes	String	Plaintext data. It can be 1 to 4,096 bytes and should match the regular expression ^.{1,4096}$. After it is converted to a byte array, its length should still be 1 to 4096 bytes.
encryption_algorithm	No	String	Data encryption algorithm. Specify this parameter if only asymmetric keys are used. The default value is **SYMMETRIC_DEFAULT**. Possible values are as follows: **SYMMETRIC_DEFAULT** **RSAES_OAEP_SHA_256** **SM2_ENCRYPT**
additional_authenticated_data	No	String	Non-sensitive extra data used for authentication. The value is a random string with at most 128 bytes.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-279 Response body parameters

Parameter	Type	Description
key_id	String	Key ID.
cipher_text	String	Encrypted ciphertext in Base64 format

Status code: 400

Table 4-280 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-281 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-282 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-283 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-284 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-285 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-286 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-287 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-288 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-289 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-290 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-291 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-292 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-293 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Encrypt the plaintext **hello world** using the CMK whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123aad** as the associated data. The data encryption algorithm is **SYMMETRIC_DEFAULT**.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "plain_text" : "hello world",
  "encryption_algorithm" : "SYMMETRIC_DEFAULT",
  "additional_authenticated_data" : "123aad"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "cipher_text" : "AgDoAG7EsEc2OHpQxz4gDFDH54CqwaelpTdEl+RFXXX..."
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Encrypt the plaintext **hello world** using the CMK whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123aad** as the associated data. The data encryption algorithm is **SYMMETRIC_DEFAULT**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class EncryptDataSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        EncryptDataRequest request = new EncryptDataRequest();
        EncryptDataRequestBody body = new EncryptDataRequestBody();
        body.withAdditionalAuthenticatedData("123aad");

body.withEncryptionAlgorithm(EncryptDataRequestBody.EncryptionAlgorithmEnum.fromValue("SYMMETRIC_DEFAULT"));
        body.withPlainText("hello world");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            EncryptDataResponse response = client.encryptData(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Encrypt the plaintext **hello world** using the CMK whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123aad** as the associated data. The data encryption algorithm is **SYMMETRIC_DEFAULT**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = EncryptDataRequest()
        request.body = EncryptDataRequestBody(
            additional_authenticated_data="123aad",
            encryption_algorithm="SYMMETRIC_DEFAULT",
            plain_text="hello world",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.encrypt_data(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Encrypt the plaintext **hello world** using the CMK whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and add **123aad** as the associated data. The data encryption algorithm is **SYMMETRIC_DEFAULT**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.EncryptDataRequest{}
    additionalAuthenticatedDataEncryptDataRequestBody:= "123aad"
    encryptionAlgorithmEncryptDataRequestBody:= model.GetEncryptDataRequestBodyEncryptionAlgorithmEnum().SYMMETRIC_DEFAULT
    request.Body = &model.EncryptDataRequestBody{
        AdditionalAuthenticatedData: &additionalAuthenticatedDataEncryptDataRequestBody,
        EncryptionAlgorithm: &encryptionAlgorithmEncryptDataRequestBody,
        PlainText: "hello world",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.EncryptData(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.3.2 Decrypting Data

Function

This API is used to decrypt data.

Constraints

When decrypting the data encrypted using asymmetric keys, you need to specify the key ID and encryption algorithm. If the specified key ID and encryption algorithm do not match those used for encrypting data, the decryption fails.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:decryptData	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:crypto • kms:cmk:decrypt	-
		-	• kms:EncryptionAlgorithm • kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext		

URI

POST /v1.0/{project_id}/kms/decrypt-data

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-294 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-295 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling an IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-296 Request body parameters

Parameter	Mandatory	Type	Description
cipher_text	Yes	String	Ciphertext of encrypted data, which is the value of **cipher_text** in the data encryption output. The value matches the regular expression **^[0-9a-zA-Z+/=]{128,5648}$**.
encryption_algorithm	No	String	Data encryption algorithm. Specify this parameter if only asymmetric keys are used. The default value is **SYMMETRIC_DEFAULT**. Possible values are as follows: **SYMMETRIC_DEFAULT** **RSAES_OAEP_SHA_256** **SM2_ENCRYPT**
key_id	No	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
additional_authenticated_data	No	String	Non-sensitive extra data used for authentication. The value is a random string with at most 128 bytes.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-297 Response body parameters

Parameter	Type	Description
key_id	String	Key ID.
plain_text	String	Plaintext.
plain_text_base64	String	Base64 value of the plaintext. In asymmetric encryption scenarios, if the encrypted plaintext contains invisible characters, the value is used as the decryption result.

Status code: 400

Table 4-298 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-299 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 401

Table 4-300 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-301 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-302 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-303 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-304 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-305 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-306 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-307 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-308 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-309 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-310 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-311 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Decrypt the ciphertext **AgDoAG7EsEc2OHpQxz4gDFDH54Cqwaelxxxxxxx** and add **123aad** as the associated data. The data encryption algorithm is **SYMMETRIC_DEFAULT**.

```
{
  "cipher_text" : "AgDoAG7EsEc2OHpQxz4gDFDH54Cqwaelxxxxxxx",
  "encryption_algorithm" : "SYMMETRIC_DEFAULT",
  "additional_authenticated_data" : "123aad"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "plain_text" : "hello world",
  "plain_text_base64" : "aGVsbG8gd29ybGQ="
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Decrypt the ciphertext **AgDoAG7EsEc2OHpQxz4gDFDH54Cqwaelxxxxxxx** and add **123aad** as the associated data. The data encryption algorithm is **SYMMETRIC_DEFAULT**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class DecryptDataSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        DecryptDataRequest request = new DecryptDataRequest();
        DecryptDataRequestBody body = new DecryptDataRequestBody();
        body.withAdditionalAuthenticatedData("123aad");
        body.withEncryptionAlgorithm(DecryptDataRequestBody.EncryptionAlgorithmEnum.fromValue("SYMMETRIC_DEFAULT"));
        body.withCipherText("AgDoAG7EsEc2OHpQxz4gDFDH54Cqwaelxxxxxxx");
        request.withBody(body);
        try {
            DecryptDataResponse response = client.decryptData(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Decrypt the ciphertext **AgDoAG7EsEc2OHpQxz4gDFDH54Cqwaelxxxxxxx** and add **123aad** as the associated data. The data encryption algorithm is **SYMMETRIC_DEFAULT**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DecryptDataRequest()
        request.body = DecryptDataRequestBody(
            additional_authenticated_data="123aad",
            encryption_algorithm="SYMMETRIC_DEFAULT",
            cipher_text="AgDoAG7EsEc2OHpQxz4gDFDH54Cqwaelxxxxxxx"
        )
        response = client.decrypt_data(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Decrypt the ciphertext **AgDoAG7EsEc2OHpQxz4gDFDH54Cqwaelxxxxxxx** and add **123aad** as the associated data. The data encryption algorithm is **SYMMETRIC_DEFAULT**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            WithCredential(auth).
            Build())

    request := &model.DecryptDataRequest{}
    additionalAuthenticatedDataDecryptDataRequestBody:= "123aad"
    encryptionAlgorithmDecryptDataRequestBody:=
model.GetDecryptDataRequestBodyEncryptionAlgorithmEnum().SYMMETRIC_DEFAULT
    request.Body = &model.DecryptDataRequestBody{
        AdditionalAuthenticatedData: &additionalAuthenticatedDataDecryptDataRequestBody,
        EncryptionAlgorithm: &encryptionAlgorithmDecryptDataRequestBody,
        CipherText: "AgDoAG7EsEc2OHpQxz4gDFDH54Cqwaelxxxxxxx",
    }
    response, err := client.DecryptData(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.4 Signature and Verification

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.1.4.1 Signature Data

Function

This API is used to digitally sign a message or digest using the private key of an asymmetric key.

Constraints

Only the asymmetric key whose **key_usage** is **SIGN_VERIFY** can be used for signature.

SM2 keys can only be used to sign message digests.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:sign	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
		-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases		

URI

POST /v1.0/{project_id}/kms/sign

Table 4-312 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-313 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-314 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
message	Yes	String	Message digest or message to be signed. The message must be Base64-coded and smaller than 4,096 bytes.
signing_algorithm	Yes	String	Signature algorithm. Possible values are as follows: **RSASSA_PSS_SHA_256** **RSASSA_PSS_SHA_384** **RSASSA_PSS_SHA_512** **RSASSA_PKCS1_V1_5_SHA_256** **RSASSA_PKCS1_V1_5_SHA_384** **RSASSA_PKCS1_V1_5_SHA_512** **ECDSA_SHA_256** **ECDSA_SHA_384** **ECDSA_SHA_512** **SM2DSA_SM3**
message_type	No	String	Message type. The default value is **DIGEST**. Possible values are as follows: **DIGEST**: message digest **RAW**: message
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-315 Response body parameters

Parameter	Type	Description
key_id	String	Key ID
signature	String	Base64-coded signature value

Status code: 400

Table 4-316 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-317 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-318 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-319 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-320 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-321 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-322 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-323 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-324 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-325 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-326 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-327 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-328 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-329 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

Sign messages and digests using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and the **RSASSA_PKCS1_V1_5_SHA_256** algorithm.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "signing_algorithm" : "RSASSA_PKCS1_V1_5_SHA_256",
  "message" : "MmFiZWE0ZjI3ZGIxYTkzY2RmYmEzM2YwMTA1YmJjYw=="
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "signature" : "jFUqQESGBc0j6k9BozzrP9YL4qk8/W9DZRvK6XXX..."
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Sign messages and digests using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and the **RSASSA_PKCS1_V1_5_SHA_256** algorithm.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class SignSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        SignRequest request = new SignRequest();
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        SignRequestBody body = new SignRequestBody();

body.withSigningAlgorithm(SignRequestBody.SigningAlgorithmEnum.fromValue("RSASSA_PKCS1_V1_5_SHA_
256"));
        body.withMessage("MmFiZWE0ZjI3ZGIxYTkzY2RmYmEzM2YwMTA1YmJjYw==");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            SignResponse response = client.sign(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Sign messages and digests using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and the **RSASSA_PKCS1_V1_5_SHA_256** algorithm.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = SignRequest()
        request.body = SignRequestBody(
            signing_algorithm="RSASSA_PKCS1_V1_5_SHA_256",
            message="MmFiZWE0ZjI3ZGIxYTkzY2RmYmEzM2YwMTA1YmJjYw==",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.sign(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Go

Sign messages and digests using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and the **RSASSA_PKCS1_V1_5_SHA_256** algorithm.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.SignRequest{}
    request.Body = &model.SignRequestBody{
        SigningAlgorithm: model.GetSignRequestBodySigningAlgorithmEnum().RSASSA_PKCS1_V1_5_SHA_256,
        Message: "MmFiZWE0ZjI3ZGIxYTkzY2RmYmEzM2YwMTA1YmJjYw==",
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.Sign(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.4.2 Verifying a Signature

Function

This API is used to verify the signature of a message or digest using the public key of an asymmetric key.

Constraints

Only the asymmetric key whose **key_usage** is **SIGN_VERIFY** can be used for signature verification.

SM2 keys can only be used to sign message digests.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:verify	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-
		-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases		

URI

POST /v1.0/{project_id}/kms/verify

Table 4-330 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-331 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-332 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
message	Yes	String	Message digest or message to be signed. The message must be smaller than 4,096 bytes and in Base64 format.
signature	Yes	String	Value of signature to be valued, which is in Base64 format.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
signing_algorithm	Yes	String	Signature algorithm. Possible values are as follows: **RSASSA_PSS_SHA_256** **RSASSA_PSS_SHA_384** **RSASSA_PSS_SHA_512** **RSASSA_PKCS1_V1_5_SHA_256** **RSASSA_PKCS1_V1_5_SHA_384** **RSASSA_PKCS1_V1_5_SHA_512** **ECDSA_SHA_256** **ECDSA_SHA_384** **ECDSA_SHA_512** **SM2DSA_SM3**
message_type	No	String	Message type. The default value is **DIGEST**. Possible values are as follows: **DIGEST**: message digest **RAW**: message
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-333 Response body parameters

Parameter	Type	Description
key_id	String	Key ID
signature_valid	String	Whether the verification signature is valid. **true**: The signature is valid. **false**: The signature is invalid.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-334 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-335 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-336 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-337 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-338 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-339 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-340 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-341 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-342 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-343 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-344 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-345 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-346 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-347 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Verify the signatures of messages and digests using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and the **RSASSA_PKCS1_V1_5_SHA_256** algorithm.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "signing_algorithm" : "RSASSA_PKCS1_V1_5_SHA_256",
  "signature" : "jFUqQESGBc0j6k9BozzrP9YL4qk8/W9DZRvK6XXX...",
  "message" : "MmFiZWE0ZjI3ZGIxYTkzY2RmYmEzM2YwMTA1YmJjYw=="
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Responses

Status code: 200

Request succeeded.

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

SDK Sample Code

The SDK sample code is as follows.

Java

Verify the signatures of messages and digests using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and the **RSASSA_PKCS1_V1_5_SHA_256** algorithm.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ValidateSignatureSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ValidateSignatureRequest request = new ValidateSignatureRequest();
        VerifyRequestBody body = new VerifyRequestBody();

body.withSigningAlgorithm(VerifyRequestBody.SigningAlgorithmEnum.fromValue("RSASSA_PKCS1_V1_5_SHA_256"));
        body.withSignature("jFUqQESGBc0j6k9BozzrP9YL4qk8/W9DZRvK6XXX...");
        body.withMessage("MmFiZWE0ZjI3ZGIxYTkzY2RmYmEzM2YwMTA1YmJjYw==");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            ValidateSignatureResponse response = client.validateSignature(request);
            System.out.println(response.toString());
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Verify the signatures of messages and digests using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and the **RSASSA_PKCS1_V1_5_SHA_256** algorithm.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ValidateSignatureRequest()
        request.body = VerifyRequestBody(
            signing_algorithm="RSASSA_PKCS1_V1_5_SHA_256",
            signature="jFUqQESGBc0j6k9BozzrP9YL4qk8/W9DZRvK6XXX...",
            message="MmFiZWE0ZjI3ZGIxYTkzY2RmYmEzM2YwMTA1YmJjYw==",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.validate_signature(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Verify the signatures of messages and digests using the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** and the **RSASSA_PKCS1_V1_5_SHA_256** algorithm.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ValidateSignatureRequest{}
    request.Body = &model.VerifyRequestBody{
        SigningAlgorithm: model.GetVerifyRequestBodySigningAlgorithmEnum().RSASSA_PKCS1_V1_5_SHA_256,
        Signature: "jFUqQESGBc0j6k9BozzrP9YL4qk8/W9DZRvK6XXX...",
        Message: "MmFiZWE0ZjI3ZGIxYTkzY2RmYmEzM2YwMTA1YmJjYw==",
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.ValidateSignature(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.5 Key Tag Management

4.1.5.1 Querying the Key Instance

Function

This API is used to query a key instance. You can use tags to filter and check CMK details.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:listKeysByTag	List	KeyId *	-	• kms:cmkTag:listInstance	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

URI

POST /v1.0/{project_id}/kms/{resource_instances}/action

Table 4-348 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
resource_instances	Yes	String	Resource instance. The value is **resource_instances**.

Request Parameters

Table 4-349 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-350 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	String	Number of records to be queried. You do not need to specify this parameter if **action** is set to **count**. If **action** is set to **filter**, the default value of this parameter is **10**. The value of **limit** ranges from **1** to **1000**.
offset	No	String	Index location. The query starts from the next data specified by **offset**. If **action** is set to **count**, do not specify this parameter. If **action** is set to **filter**, the default value of **offset** is **0**. The value of **offset** must be a non-negative number.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
action	No	String	Operation type. The value can be **filter** or **count**. **filter**: filtering **count**: total number of queried records
tags	No	Array of **Tag** objects	Tag list, which is the value pairs of **key** and **value**. **key**: Tag key. A tag key can contain up to 10 values. This parameter cannot be left empty or repeated. The value of a **key** must be unique and contain up to 36 characters. **value**: Tag value. There can be multiple values and each value can contain up to 43 characters. Each pair contains one **key** and one **value**.
matches	No	Array of **TagItem** objects	Search field. Possible values are as follows: **key**: The field to be matched, for example, **resource_name**. **value**: The value to be matched. The value can contain up to 255 characters and cannot be blank.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Table 4-351 Tag

Parameter	Mandatory	Type	Description
key	No	String	Key. The value can contain up to 36 unicode characters. This parameter cannot be left empty. The following nonprintable characters are not supported: ASCII(0-31), *, <, >, , and =.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
values	No	Array of strings	Tag value set.

Table 4-352 TagItem

Parameter	Mandatory	Type	Description
key	Yes	String	Key. The value can contain up to 36 unicodes. This parameter cannot be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.
value	No	String	Key. The value can contain up to 43 unicodes. This parameter can be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.

Response Parameters

Status code: 200

Table 4-353 Response body parameters

Parameter	Type	Description
resources	Array of **ActionResources** objects	Resource instance list. For details, see the data structure description of the **resource** field.
total_count	Integer	Total number of records.

Table 4-354 ActionResources

Parameter	Type	Description
resource_id	String	Resource ID.
resource_detail	**KeyDetails** object	Key details.
resource_name	String	Specifies the resource name. This parameter is an empty string by default.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
tags	Array of **TagItem** objects	Tag list. If there is no tag in the list, an empty array is returned.

Table 4-355 KeyDetails

Parameter	Type	Description
key_id	String	Key ID.
domain_id	String	User domain ID.
key_alias	String	Key alias.
realm	String	Key realm.
key_spec	String	Key generation algorithm. Possible values are as follows: **AES_256** **SM4** **RSA_2048** **RSA_3072** **RSA_4096** **EC_P256** **EC_P384** **SM2**
key_usage	String	Key usage. Possible values are as follows: **ENCRYPT_DECRYPT** **SIGN_VERIFY**
key_description	String	Key description.
creation_date	String	Time when the key was created. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
scheduled_deletion_date	String	Time when the key was scheduled to be deleted. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
key_state	String	Key status which matches the regular expression **^[1-5]{1}$**. Possible values are as follows: **1**: To be activated **2**: Enabled **3**: Disabled **4**: To be deleted **5**: To be imported
default_key_flag	String	Master key identifier. The value is 1 for Default Master Keys and 0 for non-default master keys.
key_type	String	Key type.
expiration_time	String	Time when the key material expires. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
origin	String	Key source. The default value is **kms**. Possible values are as follows: • **kms**: The key material was generated by KMS. • **external**: The key material was imported.
key_rotation_enabled	String	Key rotation status. The default value is false, indicating that key rotation is disabled.
sys_enterprise_project_id	String	Enterprise project ID. The default value is **0**. If you have created an enterprise project, the resources are listed in the default enterprise project. If you haven't created an enterprise project, the resources are not listed in the enterprise project.
keystore_id	String	Keystore ID
keystore_type	String	Dedicated keystore cluster type. **1** indicates Dedicated HSM cluster, **2** indicates CDMS cluster, and **0** indicates the original KMS cluster.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-356 TagItem

Parameter	Type	Description
key	String	Key. The value can contain up to 36 unicodes. This parameter cannot be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.
value	String	Key. The value can contain up to 43 unicodes. This parameter can be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.

Status code: 400

Table 4-357 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-358 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-359 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-360 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-361 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-362 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-363 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-364 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-365 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-366 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-367 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-368 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-369 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-370 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Query the key instance whose tag key is **key1** and tag value is **value1** or **value2**. The start position is **100** and 100 results are displayed.

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "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,
      "key_rotation_enabled" : false,
      "expiration_time" : "",
      "origin" : "kms",
      "sys_enterprise_project_id" : "0",
      "realm" : "test"
    } ],
    "resource_name" : "tagTest_xmdmi",
    "tags" : [ {
      "key" : "key",
      "value" : "testValue!"
    }, {
      "key" : "haha",
      "value" : "testValue"
    } ]
  } ],
  "total_count" : 1
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

SDK Sample Code

The SDK sample code is as follows.

Java

Query the key instance whose tag key is **key1** and tag value is **value1** or **value2**. The start position is **100** and 100 results are displayed.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class ListKmsByTagsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ListKmsByTagsRequest request = new ListKmsByTagsRequest();
        request.withResourceInstances("{resource_instances}");
        ListKmsByTagsRequestBody body = new ListKmsByTagsRequestBody();
        List<String> listTagsValues = new ArrayList<>();
        listTagsValues.add("value1");
        listTagsValues.add("value2");
        List<Tag> listbodyTags = new ArrayList<>();
        listbodyTags.add(
            new Tag()
                .withKey("key1")
                .withValues(listTagsValues)
        );
        body.withTags(listbodyTags);
        body.withAction("filter");
        body.withOffset("100");
        body.withLimit("100");
        request.withBody(body);
        try {
            ListKmsByTagsResponse response = client.listKmsByTags(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Query the key instance whose tag key is **key1** and tag value is **value1** or **value2**. The start position is **100** and 100 results are displayed.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListKmsByTagsRequest()
        request.resource_instances = "{resource_instances}"
        listValuesTags = [
            "value1",
            "value2"
        ]
        listTagsbody = [
            Tag(
                key="key1",
                values=listValuesTags
            )
        ]
        request.body = ListKmsByTagsRequestBody(
            tags=listTagsbody,
            action="filter",
            offset="100",
            limit="100"
        )
        response = client.list_kms_by_tags(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Go

Query the key instance whose tag key is **key1** and tag value is **value1** or **value2**. The start position is **100** and 100 results are displayed.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListKmsByTagsRequest{}
    request.ResourceInstances = "{resource_instances}"
    var listValuesTags = []string{
        "value1",
        "value2",
    }
    keyTags:= "key1"
    var listTagsbody = []model.Tag{
        {
            Key: &keyTags,
            Values: &listValuesTags,
        },
    }
    actionListKmsByTagsRequestBody:= "filter"
    offsetListKmsByTagsRequestBody:= "100"
    limitListKmsByTagsRequestBody:= "100"
    request.Body = &model.ListKmsByTagsRequestBody{
        Tags: &listTagsbody,
        Action: &actionListKmsByTagsRequestBody,
        Offset: &offsetListKmsByTagsRequestBody,
        Limit: &limitListKmsByTagsRequestBody,
    }
    response, err := client.ListKmsByTags(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.5.2 Querying Key Tags

Function

This API is used to query key tags.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:getTags	Read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmkTag:list	-

URI

GET /v1.0/{project_id}/kms/{key_id}/tags

Table 4-371 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
key_id	Yes	String	Key ID

Request Parameters

Table 4-372 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 200

Table 4-373 Response body parameters

Parameter	Type	Description
tags	Array of **TagItem** objects	Tag list, which is the value pairs of **key** and **value**. **key**: Tag key. A tag key can contain up to 10 values. This parameter cannot be left empty or repeated. The value of a **key** must be unique and contain up to 36 characters. **value**: Tag value. There can be multiple values and each value can contain up to 43 characters. Each pair contains one **key** and one **value**.
existTagsNum	Integer	Number of key tags.

Table 4-374 TagItem

Parameter	Type	Description
key	String	Key. The value can contain up to 36 unicodes. This parameter cannot be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.
value	String	Key. The value can contain up to 43 unicodes. This parameter can be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.

Status code: 400

Table 4-375 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-376 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-377 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-378 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-379 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-380 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 404

Table 4-381 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-382 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-383 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-384 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-385 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-386 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-387 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-388 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value2"
  } ],
  "existTagsNum" : 2
}
```

SDK Sample Code

The SDK sample code is as follows.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ShowKmsTagsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowKmsTagsRequest request = new ShowKmsTagsRequest();
        request.withKeyId("{key_id}");
        try {
            ShowKmsTagsResponse response = client.showKmsTags(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowKmsTagsRequest()
        request.key_id = "{key_id}"
        response = client.show_kms_tags(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowKmsTagsRequest{}
    request.KeyId = "{key_id}"
    response, err := client.ShowKmsTags(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.5.3 Adding Tags to a Key

Function

This API is used to add a key tag.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:createTag	Tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmkTag:create	-
		-	• g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v1.0/{project_id}/kms/{key_id}/tags

Table 4-389 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
key_id	Yes	String	Key ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-390 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-391 Request body parameters

Parameter	Mandatory	Type	Description
tag	No	TagItem object	Tag.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Table 4-392 TagItem

Parameter	Mandatory	Type	Description
key	Yes	String	Key. The value can contain up to 36 unicodes. This parameter cannot be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.
value	No	String	Key. The value can contain up to 43 unicodes. This parameter can be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.

Response Parameters

Status code: 204

No Content

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-393 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-394 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-395 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-396 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-397 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-398 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-399 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-400 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-401 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-402 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-403 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-404 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-405 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-406 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Add a tag whose key is **DEV** and value is **DEV1**.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Add a tag whose key is **DEV** and value is **DEV1**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CreateKmsTagSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateKmsTagRequest request = new CreateKmsTagRequest();
        request.withKeyId("{key_id}");
        CreateKmsTagRequestBody body = new CreateKmsTagRequestBody();
        TagItem tagbody = new TagItem();
        tagbody.withKey("DEV")
            .withValue("DEV1");
        body.withTag(tagbody);
        request.withBody(body);
        try {
            CreateKmsTagResponse response = client.createKmsTag(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    }
}
```

Python

Add a tag whose key is **DEV** and value is **DEV1**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateKmsTagRequest()
        request.key_id = "{key_id}"
        tagbody = TagItem(
            key="DEV",
            value="DEV1"
        )
        request.body = CreateKmsTagRequestBody(
            tag=tagbody
        )
        response = client.create_kms_tag(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Add a tag whose key is **DEV** and value is **DEV1**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateKmsTagRequest{}
    request.KeyId = "{key_id}"
    valueTag:= "DEV1"
    tagbody := &model.TagItem{
        Key: "DEV",
        Value: &valueTag,
    }
    request.Body = &model.CreateKmsTagRequestBody{
        Tag: tagbody,
    }
    response, err := client.CreateKmsTag(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	No Content
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Error Codes

See **Error Codes**.

4.1.5.4 Querying Project Tags

Function

This API is used to query all tags in a specified project.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms::listAllTags	List	-	-	-	-

URI

GET /v1.0/{project_id}/kms/tags

Table 4-407 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-408 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-409 Response body parameters

Parameter	Type	Description
tags	Array of **Tag** objects	Tag list, which is the value pairs of **key** and **value**. **key**: Tag key. A tag key can contain up to 10 values. This parameter cannot be left empty or repeated. The value of a **key** must be unique and contain up to 36 characters. **value**: Tag value. There can be multiple values and each value can contain up to 43 characters. Each pair contains one **key** and one **value**.

Table 4-410 Tag

Parameter	Type	Description
key	String	Key. The value can contain up to 36 unicode characters. This parameter cannot be left empty. The following nonprintable characters are not supported: ASCII(0-31), *, <, >, , and =.
values	Array of strings	Tag value set.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-411 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-412 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-413 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-414 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-415 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-416 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-417 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-418 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-419 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-420 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-421 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-422 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-423 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-424 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "tags" : [ {
    "key" : "key1",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ListKmsTagsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ListKmsTagsRequest request = new ListKmsTagsRequest();
        try {
            ListKmsTagsResponse response = client.listKmsTags(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListKmsTagsRequest()
        response = client.list_kms_tags(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListKmsTagsRequest{}
    response, err := client.ListKmsTags(request)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.5.5 Batch Adding or Deleting Key Tags

Function

This API is used to add or delete key tags in batches.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:createTags	Tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmkTag:batch	-
		-	• g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v1.0/{project_id}/kms/{key_id}/tags/action

Table 4-425 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
key_id	Yes	String	Key ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-426 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-427 Request body parameters

Parameter	Mandatory	Type	Description
tags	Yes	Array of **TagItem** objects	Tag list, which is a collection of key-value pairs.
action	Yes	String	Operation type. The value can only be **create** or **delete**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Table 4-428 TagItem

Parameter	Mandatory	Type	Description
key	Yes	String	Key. The value can contain up to 36 unicodes. This parameter cannot be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.
value	No	String	Key. The value can contain up to 43 unicodes. This parameter can be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.

Response Parameters

Status code: 204

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

No Content

Status code: 400

Table 4-429 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-430 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-431 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-432 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-433 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-434 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-435 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-436 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-437 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-438 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-439 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-440 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-441 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-442 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Add multiple key tags. For tag 1, the key is **key1** and the value is **value1**. For tag 2, the key is **key** and the value is **value3**.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
 }]
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Add multiple key tags. For tag 1, the key is **key1** and the value is **value1**. For tag 2, the key is **key** and the value is **value3**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class BatchCreateKmsTagsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchCreateKmsTagsRequest request = new BatchCreateKmsTagsRequest();
        request.withKeyId("{key_id}");
        BatchCreateKmsTagsRequestBody body = new BatchCreateKmsTagsRequestBody();
        List<TagItem> listbodyTags = new ArrayList<>();
        listbodyTags.add(
            new TagItem()
                .withKey("key1")
                .withValue("value1")
        );
        listbodyTags.add(
            new TagItem()
                .withKey("key")
                .withValue("value3")
        );
        body.withAction("create");
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        body.withTags(listbodyTags);
        request.withBody(body);
        try {
            BatchCreateKmsTagsResponse response = client.batchCreateKmsTags(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Add multiple key tags. For tag 1, the key is **key1** and the value is **value1**. For tag 2, the key is **key** and the value is **value3**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchCreateKmsTagsRequest()
        request.key_id = "{key_id}"
        listTagsbody = [
            TagItem(
                key="key1",
                value="value1"
            ),
            TagItem(
                key="key",
                value="value3"
            )
        ]
        request.body = BatchCreateKmsTagsRequestBody(
            action="create",
            tags=listTagsbody
        )
        response = client.batch_create_kms_tags(request)
        print(response)
    except exceptions.ClientRequestException as e:
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Add multiple key tags. For tag 1, the key is **key1** and the value is **value1**. For tag 2, the key is **key** and the value is **value3**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchCreateKmsTagsRequest{}
    request.KeyId = "{key_id}"
    valueTags:= "value1"
    valueTags1:= "value3"
    var listTagsbody = []model.TagItem{
        {
            Key: "key1",
            Value: &valueTags,
        },
        {
            Key: "key",
            Value: &valueTags1,
        },
    }
    request.Body = &model.BatchCreateKmsTagsRequestBody{
        Action: "create",
        Tags: listTagsbody,
    }
    response, err := client.BatchCreateKmsTags(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	No Content
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.5.6 Deleting Key Tags

Function

This API is used to delete a key tag.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:deleteTag	Tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmkTag:delete	-
		-	g:TagKeys		

URI

DELETE /v1.0/{project_id}/kms/{key_id}/tags/{key}

Table 4-443 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
key_id	Yes	String	Key ID
key	Yes	String	Value of a tag key.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-444 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-445 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-446 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-447 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-448 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-449 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-450 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-451 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-452 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-453 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-454 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-455 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-456 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-457 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-458 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

None

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class DeleteTagSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteTagRequest request = new DeleteTagRequest();
        request.withKeyId("{key_id}");
        request.withKey("{key}");
        try {
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            DeleteTagResponse response = client.deleteTag(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteTagRequest()
        request.key_id = "{key_id}"
        request.key = "{key}"
        response = client.delete_tag(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteTagRequest{}
    request.KeyId = "{key_id}"
    request.Key = "{key}"
    response, err := client.DeleteTag(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	No Content
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.1.6 Querying Key API Versions

4.1.6.1 Querying the Version List

Function

This API is used to query the API version list.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms::getVersions	Read	-	-	-	-

URI

GET /

Request Parameters

None

Response Parameters

Status code: 200

Table 4-459 Response body parameters

Parameter	Type	Description
versions	Array of **ApiVersionDetail** objects	Related version object list. For details, see the data structure description of the **versions** field.

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-460 ApiVersionDetail

Parameter	Type	Description
id	String	Version number, for example, v1.0.
links	Array of **ApiLink** objects	JSON object. For details, see the data structure of the **links** field.
version	String	If the APIs of this version support microversions, the supported maximum microversion is returned. If microversions are not supported, an empty string is returned.
status	String	Version status. Possible values are as follows: **CURRENT**: The version is widely used. **SUPPORTED**: It is an earlier version which can still be used. **DEPRECATED**: The version is deprecated and may be deleted later.
updated	String	Version release time. The time must be in UTC format. For example, v1 is released on **2014-06-28T12:20:21Z**.
min_version	String	If the APIs of this version support microversions, the supported minimum microversion is returned. If microversions are not supported, an empty string is returned.

Table 4-461 ApiLink

Parameter	Type	Description
href	String	API URL.
rel	String	The default value is self.

Status code: 500

Table 4-462 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-463 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-464 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-465 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-466 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-467 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.


```
{
  "versions" : [ {
    "min_version" : "",
    "links" : [ {
      "rel" : "self",
      "href" : "https://kms.region_id.domain.com/v1.0/"
    } ],
    "id" : "v1.0",
    "version" : "",
    "updated" : "2016-10-29T02:00:00Z",
    "status" : "CURRENT"
  } ]
}
```


Status Codes

Status Code	Description
200	Request succeeded.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.6.2 Querying a Specified Version

Function

This API is used to query a specified API version.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms::getVersion	Read	-	-	-	-

URI

GET /{version_id}

Table 4-468 Path Parameters

Parameter	Mandatory	Type	Description
version_id	Yes	String	API version.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-469 Response body parameters

Parameter	Type	Description
version	Object	Version object list. For details, see the data structure description of the **ApiVersionDetail** field.

Table 4-470 ApiVersionDetail

Parameter	Type	Description
id	String	Version number, for example, v1.0.
links	Array of **ApiLink** objects	JSON object. For details, see the data structure of the **links** field.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
version	String	If the APIs of this version support microversions, the supported maximum microversion is returned. If microversions are not supported, an empty string is returned.
status	String	Version status. Possible values are as follows: **CURRENT**: The version is widely used. **SUPPORTED**: It is an earlier version which can still be used. **DEPRECATED**: The version is deprecated and may be deleted later.
updated	String	Version release time. The time must be in UTC format. For example, v1 is released on **2014-06-28T12:20:21Z**.
min_version	String	If the APIs of this version support microversions, the supported minimum microversion is returned. If microversions are not supported, an empty string is returned.

Table 4-471 ApiLink

Parameter	Type	Description
href	String	API URL.
rel	String	The default value is self.

Status code: 500

Table 4-472 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-473 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-474 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-475 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-476 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-477 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Query the V1.0 API information of the current site.

```
/v1.0
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Responses

Status code: 200

A specified API version is queried.

```
{
  "version" : {
    "min_version" : "",
    "links" : [ {
      "rel" : "self",
      "href" : "https://kms.region_id.domain.com/v1.0/"
    } ],
    "id" : "v1.0",
    "version" : "",
    "updated" : "2016-10-29T02:00:00Z",
    "status" : "CURRENT"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ShowVersionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowVersionRequest request = new ShowVersionRequest();
        request.withVersionId("{version_id}");
        try {
            ShowVersionResponse response = client.showVersion(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]

    credentials = BasicCredentials(ak, sk)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowVersionRequest()
        request.version_id = "{version_id}"
        response = client.show_version(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        WithSk(sk).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowVersionRequest{}
    request.VersionId = "{version_id}"
    response, err := client.ShowVersion(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	A specified API version is queried.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.7 Multi-Region Key

4.1.7.1 Changing the Primary Region for a Key

Function

Change the primary region to which the key belongs. After the modification, the current region becomes the backup region.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:updatePrimaryRegion	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-
		-	kms:PrimaryRegion		

URI

PUT /v2/{project_id}/kms/keys/{key_id}/update-primary-region

Table 4-478 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
key_id	Yes	String	ID of the key to be updated, which is 36-byte long and matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**

Request Parameters

Table 4-479 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-480 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	ID of the key to be updated, which is 36-byte long and matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**
primary_region	Yes	String	Code of the new primary region to which the key belongs, for example, **cn-north-4**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 200

Table 4-481 Response body parameters

Parameter	Type	Description
key_id	String	Key ID, which is 36-byte long and matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**
primary_region	String	Code of the primary region where the key is located, for example, **cn-north-4**

Status code: 400

Table 4-482 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-483 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-484 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-485 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-486 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-487 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-488 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-489 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-490 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-491 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-492 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-493 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-494 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-495 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

```
{
  "key_id" : "826314dd-1b5b-4037-b976-5f9b7a17df46",
  "primary_region" : "cn-north-4"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "primary_region" : "cn-north-4"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class UpdatePrimaryRegionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePrimaryRegionRequest request = new UpdatePrimaryRegionRequest();
        request.withKeyId("{key_id}");
        UpdatePrimaryRegionRequestBody body = new UpdatePrimaryRegionRequestBody();
        body.withPrimaryRegion("cn-north-4");
        body.withKeyId("826314dd-1b5b-4037-b976-5f9b7a17df46");
        request.withBody(body);
        try {
            UpdatePrimaryRegionResponse response = client.updatePrimaryRegion(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdatePrimaryRegionRequest()
        request.key_id = "{key_id}"
        request.body = UpdatePrimaryRegionRequestBody(
            primary_region="cn-north-4",
            key_id="826314dd-1b5b-4037-b976-5f9b7a17df46"
        )
        response = client.update_primary_region(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePrimaryRegionRequest{}
    request.KeyId = "{key_id}"
    request.Body = &model.UpdatePrimaryRegionRequestBody{
        PrimaryRegion: "cn-north-4",
        KeyId: "826314dd-1b5b-4037-b976-5f9b7a17df46",
    }
    response, err := client.UpdatePrimaryRegion(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
404	The resource does not exist.
500	Internal service error.
502	Request failed. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.7.2 Copying a Key to a Specified Region

Function

Copy the key in the current region to the target region.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:replicate	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

URI

POST /v2/{project_id}/kms/keys/{key_id}/replicate

Table 4-496 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
key_id	Yes	String	ID of the key to be copied, which is 36-byte long and matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-497 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-498 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	ID of the key to be copied, which is 36-byte long and matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**
replica_region	Yes	String	Target region code of the copied key, for example, **cn-north-4**
key_alias	Yes	String	Alias of the copied new key
key_description	No	String	Description of the copied new key

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise multi-project ID for the copied new key • If the enterprise project function is not enabled, you do not need to set this parameter. • If the enterprise project function is enabled, you can set this parameter when creating a resource. If this parameter is not specified, the resource you create will be put under the default enterprise project (whose project ID is **0**). If you do not have the permission to create resources under the default enterprise project, an error will be reported.
replica_project_id	Yes	String	Project ID of the copied new key
tags	No	Array of **TagItem** objects	Tag list, which is the value pairs of tag keys and values.

Table 4-499 TagItem

Parameter	Mandatory	Type	Description
key	Yes	String	Key. The value can contain up to 36 unicodes. This parameter cannot be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.
value	No	String	Key. The value can contain up to 43 unicodes. This parameter can be left empty. The following nonprintable characters cannot be included: ASCII(0-31), *, <, >, , and =.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 200

Table 4-500 Response body parameters

Parameter	Type	Description
key_id	String	ID of the copied key, which is 36-byte long and matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**
domain_id	String	User domain ID
region	String	Code of the region where the copied key is located, for example, **cn-north-4**

Status code: 400

Table 4-501 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-502 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-503 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-504 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-505 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-506 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-507 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-508 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-509 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-510 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-511 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-512 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-513 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-514 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

```
{
  "key_id" : "826314dd-1b5b-4037-b976-5f9b7a17df46",
  "replica_region" : "cn-north-4",
  "key_alias" : "replica_key_alias",
  "replica_project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "8e85c00f-f7d0-47c9-ac96-548f977d16ba",
  "domain_id" : "3bab8e245e854f68af5967c00dd43127",
  "region" : "cn-north-4"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ReplicateKeySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

    KmsClient client = KmsClient.newBuilder()
            .withCredential(auth)
            .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
            .build();
    ReplicateKeyRequest request = new ReplicateKeyRequest();
    request.withKeyId("{key_id}");
    ReplicateKeyRequestBody body = new ReplicateKeyRequestBody();
    body.withReplicaProjectId("2b31ed520xxxxxxebedb6e57xxxxxxxx");
    body.withKeyAlias("replica_key_alias");
    body.withReplicaRegion("cn-north-4");
    body.withKeyId("826314dd-1b5b-4037-b976-5f9b7a17df46");
    request.withBody(body);
    try {
        ReplicateKeyResponse response = client.replicateKey(request);
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
  }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ReplicateKeyRequest()
        request.key_id = "{key_id}"
        request.body = ReplicateKeyRequestBody(
            replica_project_id="2b31ed520xxxxxxebedb6e57xxxxxxxx",
            key_alias="replica_key_alias",
            replica_region="cn-north-4",
            key_id="826314dd-1b5b-4037-b976-5f9b7a17df46"
        )
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        response = client.replicate_key(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ReplicateKeyRequest{}
    request.KeyId = "{key_id}"
    request.Body = &model.ReplicateKeyRequestBody{
        ReplicaProjectId: "2b31ed520xxxxxxebedb6e57xxxxxxxx",
        KeyAlias: "replica_key_alias",
        ReplicaRegion: "cn-north-4",
        KeyId: "826314dd-1b5b-4037-b976-5f9b7a17df46",
    }
    response, err := client.ReplicateKey(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Request failed. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.7.3 Querying the Regions Supported by a Cross-Region Key

Function

- Function: Query the regions supported by a cross-region key.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

GET /v2/{project_id}/kms/regions

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-515 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-516 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of returned records. The default value is **10**.
offset	No	Integer	Index location. The query starts from the next data record specified by **offset**.

Request Parameters

Table 4-517 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-518 Response body parameters

Parameter	Type	Description
regions	Array of strings	Region information

Status code: 400

Table 4-519 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-520 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-521 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-522 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-523 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-524 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-525 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-526 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-527 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-528 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-529 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-530 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-531 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-532 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "regions" : [ "cn-north-2", "cn-north-4", "cn-north-1" ]
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ListSupportRegionsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ListSupportRegionsRequest request = new ListSupportRegionsRequest();
        try {
            ListSupportRegionsResponse response = client.listSupportRegions(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListSupportRegionsRequest()
        response = client.list_support_regions(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListSupportRegionsRequest{}
    response, err := client.ListSupportRegions(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Request failed. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.8 MAC

4.1.8.1 Generating a MAC

Function

This API is used to generate a MAC.

Constraints

- This API is supported only for keys whose **key_usage** is **GENERATE_VERIFY_MAC**.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:generateMac	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-
		-	• kms:MacAlgorithm • kms:RequestAlias • kms:ResourceAliases		

URI

POST /v1.0/{project_id}/kms/generate-mac

Table 4-533 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-534 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-535 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	Key ID
mac_algorithm	Yes	String	MAC algorithm. **HMAC_SM3** is supported only in China. Possible values are as follows: • HMAC_SHA_256 • HMAC_SHA_384 • HMAC_SHA_512 • HMAC_SM3
message	Yes	String	Message to be processed. The original message can contain 1 to 4,096 characters. Convert the original message to the Base64 format and import it.

Response Parameters

Status code: 200

Table 4-536 Response body parameters

Parameter	Type	Description
key_id	String	Key ID
mac_algorithm	String	MAC algorithm
mac	String	MAC

Example Requests

```
{
  "key_id" : "826314dd-1b5b-4037-b976-5f9b7a17df46",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
  "mac_algorithm" : "HMAC_SHA_256",
  "message" : "ZmRzYQ=="
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "mac_algorithm" : "HMAC_SHA_256",
  "key_id" : "826314dd-1b5b-4037-b976-5f9b7a17df46",
  "mac" : "9d266415acf82985bb44daf4990604f1931384c88fd21ef32b202396755dcfd7"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class GenerateMacSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        GenerateMacRequest request = new GenerateMacRequest();
        GenerateMacRequestBody body = new GenerateMacRequestBody();
        body.withMessage("ZmRzYQ==");

body.withMacAlgorithm(GenerateMacRequestBody.MacAlgorithmEnum.fromValue("HMAC_SHA_256"));
        body.withKeyId("826314dd-1b5b-4037-b976-5f9b7a17df46");
        request.withBody(body);
        try {
            GenerateMacResponse response = client.generateMac(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = GenerateMacRequest()
        request.body = GenerateMacRequestBody(
            message="ZmRzYQ==",
            mac_algorithm="HMAC_SHA_256",
            key_id="826314dd-1b5b-4037-b976-5f9b7a17df46"
        )
        response = client.generate_mac(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.GenerateMacRequest{}
    request.Body = &model.GenerateMacRequestBody{
        Message: "ZmRzYQ==",
        MacAlgorithm: model.GetGenerateMacRequestBodyMacAlgorithmEnum().HMAC_SHA_256,
        KeyId: "826314dd-1b5b-4037-b976-5f9b7a17df46",
    }
    response, err := client.GenerateMac(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See **Error Codes**.

4.1.8.2 Verifying a MAC

Function

This API is used to verify a MAC.

Constraints

- This API is supported only for keys whose **key_usage** is **GENERATE_VERIFY_MAC**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:verifyMac	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-
		-	• kms:MacAlgorithm • kms:RequestAlias • kms:ResourceAliases		

URI

POST /v1.0/{project_id}/kms/verify-mac

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-537 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-538 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-539 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	Key ID
mac_algorithm	Yes	String	MAC algorithm. **HMAC_SM3** is supported only in China. Possible values are as follows: • **HMAC_SHA_256** • **HMAC_SHA_384** • **HMAC_SHA_512** • **HMAC_SM3**
message	Yes	String	Message to be processed. The original message can contain 1 to 4,096 characters. Convert the original message to the Base64 format and import it.
mac	Yes	String	MAC to be verified

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-540 Response body parameters

Parameter	Type	Description
key_id	String	Key ID
mac_algorithm	String	MAC algorithm
mac_valid	Boolean	MAC verification result

Example Requests

```
{
  "key_id" : "826314dd-1b5b-4037-b976-5f9b7a17df46",
  "mac_algorithm" : "HMAC_SHA_256",
  "message" : "ZmRzYQ==",
  "mac" : "8549f9f5ef335184e23e6d477776f0fd338d02c59e48e52e8d81d158e2fc9262"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "mac_algorithm" : "HMAC_SHA_256",
  "key_id" : "826314dd-1b5b-4037-b976-5f9b7a17df46",
  "mac_valid" : false
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class VerifyMacSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

    KmsClient client = KmsClient.newBuilder()
            .withCredential(auth)
            .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
            .build();
    VerifyMacRequest request = new VerifyMacRequest();
    VerifyMacRequestBody body = new VerifyMacRequestBody();
    body.withMac("8549f9f5ef335184e23e6d477776f0fd338d02c59e48e52e8d81d158e2fc9262");
    body.withMessage("ZmRzYQ==");
    body.withMacAlgorithm(VerifyMacRequestBody.MacAlgorithmEnum.fromValue("HMAC_SHA_256"));
    body.withKeyId("826314dd-1b5b-4037-b976-5f9b7a17df46");
    request.withBody(body);
    try {
        VerifyMacResponse response = client.verifyMac(request);
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
  }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = VerifyMacRequest()
        request.body = VerifyMacRequestBody(
            mac="8549f9f5ef335184e23e6d477776f0fd338d02c59e48e52e8d81d158e2fc9262",
            message="ZmRzYQ==",
            mac_algorithm="HMAC_SHA_256",
            key_id="826314dd-1b5b-4037-b976-5f9b7a17df46"
        )
        response = client.verify_mac(request)
        print(response)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.VerifyMacRequest{}
    request.Body = &model.VerifyMacRequestBody{
        Mac: "8549f9f5ef335184e23e6d477776f0fd338d02c59e48e52e8d81d158e2fc9262",
        Message: "ZmRzYQ==",
        MacAlgorithm: model.GetVerifyMacRequestBodyMacAlgorithmEnum().HMAC_SHA_256,
        KeyId: "826314dd-1b5b-4037-b976-5f9b7a17df46",
    }
    response, err := client.VerifyMac(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See **Error Codes**.

4.1.9 Alias Management

4.1.9.1 Associating Key Alias

Function

This API is used to associate an alias.

You can associate an existing alias to another key.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:alias:associate	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-
		alias *	-		

URI

POST /v1.0/{project_id}/kms/alias/associate

Table 4-541 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-542 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-543 Request body parameters

Parameter	Mandatory	Type	Description
alias	Yes	String	Alias to be associated
target_key_id	Yes	String	ID of the key to be associated

Response Parameters

Status code: 200

Table 4-544 Response body parameters

Parameter	Type	Description
domain_id	String	Account ID
key_id	String	Key ID
alias	String	Alias
alias_urn	String	Alias resource locator
create_time	String	Creation time
update_time	String	Update time

Example Requests

Associate **kms-1234** to the **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

```
{
  "target_key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "alias" : "kms-1234"
}
```

Example Responses

Status code: 200

Response body for associating an alias

```
{
  "domain_id" : "3bab8e245e854f68af5967c00dd43127",
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "alias" : "kms-1234",
  "alias_urn" : "kms:cn-north-7:3bab8e245e854f68af5967c00dd43127:alias:kms-1234",
  "create_time" : "2024-04-01T00:00:00Z",
  "update_time" : "2024-04-01T00:00:00Z"
}
```

SDK Sample Code

The SDK sample code is as follows.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Java

Associate **kms-1234** to the **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class AssociateAliasSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        AssociateAliasRequest request = new AssociateAliasRequest();
        AssociateAliasRequestBody body = new AssociateAliasRequestBody();
        body.withTargetKeyId("bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e");
        body.withAlias("kms-1234");
        request.withBody(body);
        try {
            AssociateAliasResponse response = client.associateAlias(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Associate **kms-1234** to the **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = AssociateAliasRequest()
        request.body = AssociateAliasRequestBody(
            target_key_id="bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
            alias="kms-1234"
        )
        response = client.associate_alias(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Associate **kms-1234** to the **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    request := &model.AssociateAliasRequest{}
    request.Body = &model.AssociateAliasRequestBody{
        TargetKeyId: "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
        Alias: "kms-1234",
    }
    response, err := client.AssociateAlias(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Response body for associating an alias

Error Codes

See **Error Codes**.

4.1.9.2 Querying the Alias Associated with a Key

Function

This API is used to query all aliases associated with a key.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:alias:list	List	-	-	-	-

URI

GET /v1.0/{project_id}/kms/aliases

Table 4-545 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-546 Query Parameters

Parameter	Mandatory	Type	Description
key_id	No	String	Key ID
limit	No	String	Specify the number of returned records.
marker	No	String	Start position of pagination query

Request Parameters

Table 4-547 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-548 Response body parameters

Parameter	Type	Description
[items]	Array of **ListAliasResponseBody** objects	Response body for querying an alias

Table 4-549 ListAliasResponseBody

Parameter	Type	Description
aliases	Array of **AliasEntity** objects	All aliases associated with the key
page_info	**PageInfo** object	Pagination information

Table 4-550 AliasEntity

Parameter	Type	Description
domain_id	String	Account ID
key_id	String	Key ID
alias	String	Alias
alias_urn	String	Alias resource locator
create_time	String	Creation time
update_time	String	Update time

Table 4-551 PageInfo

Parameter	Type	Description
next_marker	String	Marker for querying the next page
current_count	Integer	Number of items returned on this page

Example Requests

None

Example Responses

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response body for querying an alias

```
{
  "aliases" : [ {
    "domain_id" : "3bab8e245e854f68af5967c00dd43127",
    "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "alias" : "kms-1234",
    "alias_urn" : "kms:cn-north-7:3bab8e245e854f68af5967c00dd43127:alias:kms-1234",
    "create_time" : "2024-04-01T00:00:00Z",
    "update_time" : "2024-04-01T00:00:00Z"
  } ],
  "page_info" : {
    "next_marker" : "",
    "current_count" : 1
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ListAliasesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAliasesRequest request = new ListAliasesRequest();
        try {
            ListAliasesResponse response = client.listAliases(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAliasesRequest()
        response = client.list_aliases(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAliasesRequest{}
    response, err := client.ListAliases(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Response body for querying an alias

Error Codes

See **Error Codes**.

4.1.9.3 Creating a Key Alias

Function

Associate a new alias for the specified key.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:alias:create	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-
		alias *	-		

URI

POST /v1.0/{project_id}/kms/aliases

Table 4-552 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Key ID

Request Parameters

Table 4-553 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-554 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	Key ID
alias	Yes	String	Alias. The alias of an account in the same region must be unique.

Response Parameters

Status code: 201

Table 4-555 Response body parameters

Parameter	Type	Description
domain_id	String	Account ID
key_id	String	Key ID
alias	String	Alias
alias_urn	String	Alias resource locator
create_time	String	Creation time
update_time	String	Update time

Example Requests

Associate a new alias **kms-1234** with the **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "alias" : "kms-1234"
}
```

Example Responses

Status code: 201

The alias is created.

```
{
  "domain_id" : "3bab8e245e854f68af5967c00dd43127",
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "alias" : "kms-1234",
  "alias_urn" : "kms:cn-north-7:3bab8e245e854f68af5967c00dd43127:alias:kms-1234",
  "create_time" : "2024-04-01T00:00:00Z",
  "update_time" : "2024-04-01T00:00:00Z"
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

SDK Sample Code

The SDK sample code is as follows.

Java

Associate a new alias **kms-1234** with the **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CreateAliasSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateAliasRequest request = new CreateAliasRequest();
        CreateAliasRequestBody body = new CreateAliasRequestBody();
        body.withAlias("kms-1234");
        body.withKeyId("bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e");
        request.withBody(body);
        try {
            CreateAliasResponse response = client.createAlias(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Python

Associate a new alias **kms-1234** with the **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateAliasRequest()
        request.body = CreateAliasRequestBody(
            alias="kms-1234",
            key_id="bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e"
        )
        response = client.create_alias(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Associate a new alias **kms-1234** with the **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateAliasRequest{}
    request.Body = &model.CreateAliasRequestBody{
        Alias: "kms-1234",
        KeyId: "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    }
    response, err := client.CreateAlias(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
201	The alias is created.

Error Codes

See **Error Codes**.

4.1.9.4 Deleting a Key Alias

Function

Delete an alias.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:alias:delete	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-
		alias *	-		

URI

DELETE /v1.0/{project_id}/kms/aliases

Table 4-556 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-557 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-558 Request body parameters

Parameter	Mandatory	Type	Description
aliases	Yes	Array of strings	Alias to be deleted
key_id	Yes	String	ID of the key associated with the alias

Response Parameters

Status code: 204

The alias is deleted.

None

Example Requests

Delete aliases **kms-1234** and **kms-4567** from the associated **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "aliases" : [ "kms-1234", "kms-4567" ]
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Delete aliases **kms-1234** and **kms-4567** from the associated **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class DeleteAliasSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteAliasRequest request = new DeleteAliasRequest();
        DeleteAliasRequestBody body = new DeleteAliasRequestBody();
        List<String> listbodyAliases = new ArrayList<>();
        listbodyAliases.add("kms-1234");
        listbodyAliases.add("kms-4567");
        body.withKeyId("bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e");
        body.withAliases(listbodyAliases);
        request.withBody(body);
        try {
            DeleteAliasResponse response = client.deleteAlias(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Delete aliases **kms-1234** and **kms-4567** from the associated **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteAliasRequest()
        listAliasesbody = [
            "kms-1234",
            "kms-4567"
        ]
        request.body = DeleteAliasRequestBody(
            key_id="bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
            aliases=listAliasesbody
        )
        response = client.delete_alias(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Delete aliases **kms-1234** and **kms-4567** from the associated **bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e** key.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteAliasRequest{}
    var listAliasesbody = []string{
        "kms-1234",
        "kms-4567",
    }
    request.Body = &model.DeleteAliasRequestBody{
        KeyId: "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
        Aliases: listAliasesbody,
    }
    response, err := client.DeleteAlias(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	The alias is deleted.

Error Codes

See **Error Codes**.

4.1.10 Key Import Management

4.1.10.1 Obtaining Key Import Parameters

Function

This API is used to obtain the parameters required for importing keys, including import passwords and encryption public keys.

An RSA_2048 public key is returned by default.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:getMaterial	Read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-
		-	kms:WrappingAlgorithm		

URI

POST /v1.0/{project_id}/kms/get-parameters-for-import

Table 4-559 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-560 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-561 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
wrapping_algorithm	Yes	String	Key material encryption algorithm. Possible values are as follows: **RSAES_OAEP_SHA_256** **SM2_ENCRYPT**. Some sites cannot be imported using this algorithm.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-562 Response body parameters

Parameter	Type	Description
key_id	String	Key ID.
import_token	String	Key import token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
expiration_time	Long	Import parameter expiration time. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
public_key	String	Public key of the DEK material, in Base64 format.

Status code: 400

Table 4-563 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-564 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-565 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-566 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 403

Table 4-567 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-568 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-569 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-570 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-571 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-572 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-573 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-574 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-575 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-576 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

Obtain the wrapping materials of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** using the **RSAES_OAEP_SHA_256** algorithm.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "wrapping_algorithm" : "RSAES_OAEP_SHA_256"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "import_token" : "AACIBjY2ZTQxYjBmLTY3ZWItNDU4Ny04OTIxLWVhZXXX...",
  "expiration_time" : 1501578672,
  "public_key" : "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCXXX..."
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Obtain the wrapping materials of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** using the **RSAES_OAEP_SHA_256** algorithm.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CreateParametersForImportSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        CreateParametersForImportRequest request = new CreateParametersForImportRequest();
        GetParametersForImportRequestBody body = new GetParametersForImportRequestBody();

body.withWrappingAlgorithm(GetParametersForImportRequestBody.WrappingAlgorithmEnum.fromValue("RSAES_OAEP_SHA_256"));
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            CreateParametersForImportResponse response = client.createParametersForImport(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Obtain the wrapping materials of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** using the **RSAES_OAEP_SHA_256** algorithm.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateParametersForImportRequest()
        request.body = GetParametersForImportRequestBody(
            wrapping_algorithm="RSAES_OAEP_SHA_256",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.create_parameters_for_import(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Go

Obtain the wrapping materials of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** using the **RSAES_OAEP_SHA_256** algorithm.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateParametersForImportRequest{}
    request.Body = &model.GetParametersForImportRequestBody{
        WrappingAlgorithm: model.GetGetParametersForImportRequestBodyWrappingAlgorithmEnum().RSAES_OAEP_SHA_256,
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.CreateParametersForImport(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.10.2 Importing Key Materials

Function

This API is used to import key materials.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:importMaterial	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-
		-	kms:ExpirationTime		

URI

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

Table 4-577 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-578 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-579 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
import_token	Yes	String	Key import token in Base64 format, which matches the regular expression ^[0-9a-zA-Z+/=]{200,6144}$.
encrypted_key_material	Yes	String	Encrypted symmetric key material. The value is in Base64 format and matches the regular expression **^[0-9a-zA-Z+/=]{344,360}$**. If an asymmetric key is imported, this parameter is used as a temporary intermediate key during private key encryption.
encrypted_privatekey	No	String	Private key encrypted using a temporary intermediate key. Specify this parameter if an asymmetric key is imported. The value is in Base64 format and matches the regular expression **^[0-9a-zA-Z+/=]{200,6144}$**.
expiration_time	No	Long	Expiration time of the key material. The value is a timestamp which indicates how many seconds it has been since January 1, 1970, for example, **1550291833**. The key material will be deleted by KMS in 24 hours after the expiration.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 200

Request succeeded.

Status code: 400

Table 4-580 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-581 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-582 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-583 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-584 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-585 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-586 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-587 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-588 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-589 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-590 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-591 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-592 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-593 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

Import ciphertext key materials to the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "import_token" : "AACIBjY2ZTQxYItNDU4Ny04OTIxLWVhZTVhZjg5NDZm....",
  "encrypted_key_material" : "e0wTU/YJT/HDxsEv2NE+3CKT1..."
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Import ciphertext key materials to the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ImportKeyMaterialSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ImportKeyMaterialRequest request = new ImportKeyMaterialRequest();
        ImportKeyMaterialRequestBody body = new ImportKeyMaterialRequestBody();
        body.withEncryptedKeyMaterial("e0wTU/YJT/HDxsEv2NE+3CKT1...");
        body.withImportToken("AACIBjY2ZTQxYItNDU4Ny04OTIxLWVhZTVhZjg5NDZm....");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            ImportKeyMaterialResponse response = client.importKeyMaterial(request);
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Import ciphertext key materials to the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ImportKeyMaterialRequest()
        request.body = ImportKeyMaterialRequestBody(
            encrypted_key_material="e0wTU/YJT/HDxsEv2NE+3CKT1...",
            import_token="AACIBjY2ZTQxYItNDU4Ny04OTIxLWVhZTVhZjg5NDZm....",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.import_key_material(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Import ciphertext key materials to the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ImportKeyMaterialRequest{}
    request.Body = &model.ImportKeyMaterialRequestBody{
        EncryptedKeyMaterial: "e0wTU/YJT/HDxsEv2NE+3CKT1...",
        ImportToken: "AACIBjY2ZTQxYItNDU4Ny04OTIxLWVhZTVhZjg5NDZm....",
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.ImportKeyMaterial(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.10.3 Deleting Key Materials

Function

This API is used to delete key materials.

Constraints

Materials of imported asymmetric keys cannot be deleted. To delete an asymmetric key, schedule a deletion task.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:deleteMaterial	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

URI

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

Table 4-594 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-595 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-596 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Request succeeded.

Status code: 400

Table 4-597 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-598 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-599 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-600 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-601 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-602 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-603 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-604 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-605 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-606 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-607 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-608 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-609 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-610 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Delete the materials of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

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

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Delete the materials of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class DeleteImportedKeyMaterialSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteImportedKeyMaterialRequest request = new DeleteImportedKeyMaterialRequest();
        OperateKeyRequestBody body = new OperateKeyRequestBody();
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            DeleteImportedKeyMaterialResponse response = client.deleteImportedKeyMaterial(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Delete the materials of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteImportedKeyMaterialRequest()
        request.body = OperateKeyRequestBody(
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.delete_imported_key_material(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Go

Delete the materials of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteImportedKeyMaterialRequest{}
    request.Body = &model.OperateKeyRequestBody{
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.DeleteImportedKeyMaterial(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.11 Querying Keys

4.1.11.1 Querying the Key List

Function

This API is used to query the key list.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:list	List	KeyId *	-	-	-
		-	g:EnterpriseProjectId		

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

URI

POST /v1.0/{project_id}/kms/list-keys

Table 4-611 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-612 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-613 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	String	Number of returned records. The default value is **2000**. The value should be no larger than the maximum number of keys, for example, **20**. If the number of retrieved results is greater than this value, **true** is returned for the response parameter **truncated**, indicating that multiple pages of results are returned.
marker	No	String	Start position of pagination query. If truncated is true in the response, you can send consecutive requests to obtain more records. Set marker to the value of next_marker in the response. Example: 10

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
key_state	No	String	Key status which matches the regular expression **^[1-5]{1}$**. Possible values are as follows: **1**: To be activated **2**: Enabled **3**: Disabled **4**: To be deleted **5**: To be imported
key_spec	No	String	Key generation algorithm. The default value is **AES_256**. Set this parameter to **ALL** to query all the keys (including asymmetric keys). Possible values are as follows: **AES_256** **SM4** **RSA_2048** **RSA_3072** **RSA_4096** **EC_P256** **EC_P384** **SM2** **ALL**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. If you haven't created any enterprise project, do not configure this field. If you have created an enterprise project, configure this field for resource querying. If you do not configure this field, all resources of enterprise projects that are granted are queried by default. If the value of **"enterprise_project_id** is **all**. The value must meet one of the following requirements: The value is **all**. The value is **0**. The value matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**.
keystore_type	No	String	Dedicated keystore cluster type. **1** indicates Dedicated HSM cluster, **2** indicates CDMS cluster, and **0** indicates the original KMS cluster.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-614 Response body parameters

Parameter	Type	Description
keys	Array of strings	Key ID list.
key_details	Array of **KeyDetails** objects	List of key details. For details, see **KeyDetails**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
next_marker	String	Value of marker used for obtaining the next page of results. If truncated is false, next_marker is left blank.
truncated	String	Whether there is another page. **true**: There is more data on the next page. **false**: This is the last page.
total	Integer	Total number of keys.

Table 4-615 KeyDetails

Parameter	Type	Description
key_id	String	Key ID.
domain_id	String	User domain ID.
key_alias	String	Key alias.
realm	String	Key realm.
key_spec	String	Key generation algorithm. Possible values are as follows: **AES_256** **SM4** **RSA_2048** **RSA_3072** **RSA_4096** **EC_P256** **EC_P384** **SM2**
key_usage	String	Key usage. Possible values are as follows: **ENCRYPT_DECRYPT** **SIGN_VERIFY**
key_description	String	Key description.
creation_date	String	Time when the key was created. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
scheduled_deletion_date	String	Time when the key was scheduled to be deleted. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
key_state	String	Key status which matches the regular expression **^[1-5]{1}$**. Possible values are as follows: **1**: To be activated **2**: Enabled **3**: Disabled **4**: To be deleted **5**: To be imported
default_key_flag	String	Master key identifier. The value is 1 for Default Master Keys and 0 for non-default master keys.
key_type	String	Key type.
expiration_time	String	Time when the key material expires. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
origin	String	Key source. The default value is **kms**. Possible values are as follows: ● **kms**: The key material was generated by KMS. ● **external**: The key material was imported.
key_rotation_enabled	String	Key rotation status. The default value is false, indicating that key rotation is disabled.
sys_enterprise_project_id	String	Enterprise project ID. The default value is **0**. If you have created an enterprise project, the resources are listed in the default enterprise project. If you haven't created an enterprise project, the resources are not listed in the enterprise project.
keystore_id	String	Keystore ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
keystore_type	String	Dedicated keystore cluster type. **1** indicates Dedicated HSM cluster, **2** indicates CDMS cluster, and **0** indicates the original KMS cluster.

Status code: 400

Table 4-616 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-617 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-618 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-619 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-620 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-621 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-622 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-623 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-624 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-625 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-626 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-627 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-628 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-629 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

Query the keys whose aliases start with **1**. At most two keys are returned.

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

Example Responses

Status code: 200

Request succeeded.


```
{
  "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" : "test",
    "realm" : "cn-north-7",
    "key_description" : "key_description",
    "creation_date" : "1502799822000",
    "scheduled_deletion_date" : "",
    "key_spec" : "AES_256",
    "key_usage" : "ENCRYPT_DECRYPT",
    "key_state" : "2",
    "default_key_flag" : "0",
    "key_type" : "1",
    "expiration_time" : "1501578672000",
    "origin" : "kms",
    "key_rotation_enabled" : "true",
    "sys_enterprise_project_id" : "0"
  }, {
    "key_id" : "2e258389-bb1e-4568-a1d5-e1f50adf70ea",
    "domain_id" : "00074811d5c27c4f8d48bb91e4a1dcfd",
    "key_alias" : "test",
    "realm" : "realm",
    "key_description" : "key_description",
    "creation_date" : "1502799822000",
    "scheduled_deletion_date" : "",
    "key_spec" : "AES_256",
    "key_usage" : "ENCRYPT_DECRYPT",
    "key_state" : "2",
    "default_key_flag" : "0",
    "key_type" : "1",
    "expiration_time" : "1501578672000",
    "origin" : "kms",
    "key_rotation_enabled" : "true",
    "sys_enterprise_project_id" : "0"
  } ],
  "next_marker" : "",
  "truncated" : "false",
  "total" : 2
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

Query the keys whose aliases start with **1**. At most two keys are returned.

```
package com.huaweicloud.sdk.test;
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ListKeysSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ListKeysRequest request = new ListKeysRequest();
        ListKeysRequestBody body = new ListKeysRequestBody();
        body.withMarker("1");
        body.withLimit("2");
        request.withBody(body);
        try {
            ListKeysResponse response = client.listKeys(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Query the keys whose aliases start with **1**. At most two keys are returned.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListKeysRequest()
        request.body = ListKeysRequestBody(
            marker="1",
            limit="2"
        )
        response = client.list_keys(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Query the keys whose aliases start with **1**. At most two keys are returned.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListKeysRequest{}
    markerListKeysRequestBody:= "1"
    limitListKeysRequestBody:= "2"
    request.Body = &model.ListKeysRequestBody{
        Marker: &markerListKeysRequestBody,
        Limit: &limitListKeysRequestBody,
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    }
    response, err := client.ListKeys(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.11.2 Querying Key Details

Function

This API is used to query key details.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:get	Read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-
		-	• kms:RequestAlias • kms:ResourceAliases		

URI

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

Table 4-630 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-631 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-632 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-633 Response body parameters

Parameter	Type	Description
key_info	**KeyDetails** object	Key details.

Table 4-634 KeyDetails

Parameter	Type	Description
key_id	String	Key ID.
domain_id	String	User domain ID.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
key_alias	String	Key alias.
realm	String	Key realm.
key_spec	String	Key generation algorithm. Possible values are as follows: **AES_256** **SM4** **RSA_2048** **RSA_3072** **RSA_4096** **EC_P256** **EC_P384** **SM2**
key_usage	String	Key usage. Possible values are as follows: **ENCRYPT_DECRYPT** **SIGN_VERIFY**
key_description	String	Key description.
creation_date	String	Time when the key was created. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
scheduled_deletion_date	String	Time when the key was scheduled to be deleted. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
key_state	String	Key status which matches the regular expression **^[1-5]{1}$**. Possible values are as follows: **1**: To be activated **2**: Enabled **3**: Disabled **4**: To be deleted **5**: To be imported
default_key_flag	String	Master key identifier. The value is 1 for Default Master Keys and 0 for non-default master keys.
key_type	String	Key type.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
expiration_time	String	Time when the key material expires. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
origin	String	Key source. The default value is **kms**. Possible values are as follows: • **kms**: The key material was generated by KMS. • **external**: The key material was imported.
key_rotation_enabled	String	Key rotation status. The default value is false, indicating that key rotation is disabled.
sys_enterprise_project_id	String	Enterprise project ID. The default value is **0**. If you have created an enterprise project, the resources are listed in the default enterprise project. If you haven't created an enterprise project, the resources are not listed in the enterprise project.
keystore_id	String	Keystore ID
keystore_type	String	Dedicated keystore cluster type. **1** indicates Dedicated HSM cluster, **2** indicates CDMS cluster, and **0** indicates the original KMS cluster.

Status code: 400

Table 4-635 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-636 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-637 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-638 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-639 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-640 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-641 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-642 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-643 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-644 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-645 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-646 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-647 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-648 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Query the details of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_info" : {
    "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    "domain_id" : "00074811d5c27c4f8d48bb91e4a1dcfd",
    "key_alias" : "test",
    "realm" : "test",
    "key_description" : "key_description",
    "creation_date" : "1502799822000",
    "scheduled_deletion_date" : "",
    "key_spec" : "AES_256",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "key_usage" : "ENCRYPT_DECRYPT",
    "key_state" : "2",
    "default_key_flag" : "0",
    "key_type" : "1",
    "expiration_time" : "1501578672000",
    "origin" : "kms",
    "key_rotation_enabled" : "false",
    "sys_enterprise_project_id" : "0"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Query the details of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ListKeyDetailSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ListKeyDetailRequest request = new ListKeyDetailRequest();
        OperateKeyRequestBody body = new OperateKeyRequestBody();
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            ListKeyDetailResponse response = client.listKeyDetail(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Query the details of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListKeyDetailRequest()
        request.body = OperateKeyRequestBody(
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.list_key_detail(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Query the details of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListKeyDetailRequest{}
    request.Body = &model.OperateKeyRequestBody{
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.ListKeyDetail(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Error Codes

See **Error Codes**.

4.1.11.3 Querying a Public Key

Function

This API is used to query the public key of a specified asymmetric key.

Constraints

This API cannot be used to obtain the public key of a symmetric key.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:getPublicKey	Read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
		-	• kms:RequestAlias • kms:ResourceAliases		

URI

POST /v1.0/{project_id}/kms/get-publickey

Table 4-649 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-650 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-651 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-652 Response body parameters

Parameter	Type	Description
key_id	String	Key ID
public_key	String	Public key information

Status code: 400

Table 4-653 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-654 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-655 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-656 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-657 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-658 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-659 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-660 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-661 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-662 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-663 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-664 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-665 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-666 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Query the public key of an asymmetric key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "public_key" : "-----BEGIN PUBLIC KEY-----\r\nMIICCgKCAgEA3RQAXXwya9k4zV1/
Q3AFr37GO8JgFobDKZioAklLQdgElHZ/uxmP\r\n4bveNHpY6OI0Okk/1Ov8oJf+9W10VqVxbzihWa5n/
RMN0720DzLV7KuH4YylCGDb\r\n3JH/+bMbhF2qRArrrKod0kR9rYHrdPkI7O5fYQQprZ3kWnPgrhDoDFC8ja
+OelOg\r\nn4MMOGGYA/DAOb0XyxPnGl26PnUtvvF7aZbMW5x/Yq2yAVFE1cjqLaH7/j1C8KYE\r
\naOSYtl2nOif28WoweFavXpgVsb/iICTfqgC91BtCSFC5pT8vqZCimfoHmJCAkZa5\r
\nZ8QIqkOOf9F6iMqqIz7pGKgQSUmoKKY9j6DK3OwXDOB5gKu0vyuz+gW3b4SZn+Xa\r
\nKkEN8ZpXsdQdEGpe4SwIzSVyUGYNBOCLrsydBcPR7jWgQ6gs56IJrV2pdAtmBwKd\r\n6l33z1tQ7+/
h3IrZxXuuej/fRRUMlbVcmhTS2l6vle7HXgZj/dWzPsLLg9MGHu0+\r\no9PRr+brxTbrf5e2Zdr1ad35X/
b86gx7Grg1sYPkly2aEI4fsnDGPgFrudG+Hzx/\r\nABHejYfJEI6P0SXCzB/oDMkjw6XKhTSojMzuncAP/AM
+0LVYQxQe750qkb3hjBT0\r\nq/HBl/
4zMXA03tMb9QySnLK63uo64JMJiBsEe7wPLhHB3VzBZk9SvvECAwEAAQ==\r\n-----END PUBLIC KEY-----\r\n"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Query the public key of an asymmetric key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
public class ShowPublicKeySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPublicKeyRequest request = new ShowPublicKeyRequest();
        OperateKeyRequestBody body = new OperateKeyRequestBody();
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            ShowPublicKeyResponse response = client.showPublicKey(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Query the public key of an asymmetric key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPublicKeyRequest()
        request.body = OperateKeyRequestBody(
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.show_public_key(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Query the public key of an asymmetric key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPublicKeyRequest{}
    request.Body = &model.OperateKeyRequestBody{
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.ShowPublicKey(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.11.4 Querying the Instance Quantity

Function

This API is used to query the number of instances, that is, the number of CMKs created by a user.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms::getInstance	Read	-	-	• kms:cmk:getInstance	-

URI

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

Table 4-667 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-668 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-669 Response body parameters

Parameter	Type	Description
instance_num	Integer	Number of non-default CMKs.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-670 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-671 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-672 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-673 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-674 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-675 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-676 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-677 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-678 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-679 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-680 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-681 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-682 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-683 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Query the number of instances created in the project whose ID is **0dea2644dc80d5d22ff1c01e3ebea6fc**.

```
/v1.0/0dea2644dc80d5d22ff1c01e3ebea6fc/kms/user-instances
```

Example Responses

Status code: 200

Request succeeded.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ShowUserInstancesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowUserInstancesRequest request = new ShowUserInstancesRequest();
        try {
            ShowUserInstancesResponse response = client.showUserInstances(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowUserInstancesRequest()
        response = client.show_user_instances(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowUserInstancesRequest{}
    response, err := client.ShowUserInstances(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.11.5 Querying Quotas

Function

This API is used to query quotas, including the total number of CMKs that can be created by a user and the current quota usage.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms::getQuota	Read	-	-	• kms:cmk:getQuota	-

URI

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

Table 4-684 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-685 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-686 Response body parameters

Parameter	Type	Description
quotas	**Quotas** object	Quota details.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-687 Quotas

Parameter	Type	Description
resources	Array of **Resources** objects	Resource quota list. For details, see **Resources**.

Table 4-688 Resources

Parameter	Type	Description
type	String	Quota type. Possible values are as follows: **CMK**: custom master key (CMK) **grant_per_CMK**: number of grants can be created by a single CMK
used	Integer	Used quotas.
quota	Integer	Total quotas.

Status code: 400

Table 4-689 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-690 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-691 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-692 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-693 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-694 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-695 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-696 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-697 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-698 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-699 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-700 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-701 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-702 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Query the quota usage of the project whose ID is **0dea2644dc80d5d22ff1c01e3ebea6fc**.

```
/v1.0/0dea2644dc80d5d22ff1c01e3ebea6fc/kms/user-quotas
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "quotas" : {
    "resources" : [ {
      "quota" : 20,
      "used" : 20,
      "type" : "CMK"
    }, {
      "quota" : 100,
      "used" : 0,
      "type" : "grant_per_CMK"
    } ]
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ShowUserQuotasSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowUserQuotasRequest request = new ShowUserQuotasRequest();
        try {
            ShowUserQuotasResponse response = client.showUserQuotas(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowUserQuotasRequest()
        response = client.show_user_quotas(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowUserQuotasRequest{}
    response, err := client.ShowUserQuotas(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.12 Key Grant Management

4.1.12.1 Creating a Grant

Function

This API is used to create a grant. Granted users can perform operations on the granted keys. The service default CMK whose suffix is **/default** cannot be granted.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:createGrant	Permission_management	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:grant:create	-
		-	• kms:GranteePrincipalType • kms:GrantOperations • kms:GranteePrincipal • kms:RetiringPrincipal		

URI

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

Table 4-703 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-704 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-705 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
grantee_principal	Yes	String	ID of the granted user. The value contains 1 to 64 bytes and matches the regular expression **^[a-zA-Z0-9]{1,64}$**, for example, **0d0466b00d0466b00d0466b00d0466b0**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
operations	Yes	Array of strings	List of granted operations. Possible values are as follows: **create-datakey**: Create a DEK. **create-datakey-without-plaintext**: Create a DEK that does not contain plaintext. **encrypt-datakey**: Encrypt DEK. **decrypt-datakey**: Decrypt DEK. **describe-key**: Query the key information. **create-grant**: Create the grant. **retire-grant**: Retire the grant. **encrypt-data**: Encrypt data. **decrypt-data**: Decrypt data. The value cannot be only **create-grant**.
name	No	String	Grant name. The value is a string of 1 to 255 characters and matches the regular expression ^[a-zA-Z0-9:/_-]{1,255}$.
retiring_principal	No	String	ID of the user whose grant can be retired. The value contains 1 to 64 bytes and matches the regular expression **^[a-zA-Z0-9]{1,64}$**, for example, **0d0466b00d0466b00d0466b00d0466b0**.
grantee_principal_type	No	String	Grant type. Values: user, domain. The default value is user.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-706 Response body parameters

Parameter	Type	Description
grant_id	String	Grant ID, which contains 64 bytes.

Status code: 400

Table 4-707 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-708 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-709 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-710 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-711 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-712 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-713 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-714 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-715 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-716 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-717 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-718 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-719 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-720 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

Grant user **13gg44z4g2sglzk0egw0u726zoyzvrs8** with permission to query, create, and encrypt a key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "operations" : [ "describe-key", "create-datakey", "encrypt-datakey" ],
  "grantee_principal" : "13gg44z4g2sglzk0egw0u726zoyzvrs8",
  "grantee_principal_type" : "user",
  "retiring_principal" : "13gg44z4g2sglzk0egw0u726zoyzvrs8"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "grant_id" : "7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Grant user **13gg44z4g2sglzk0egw0u726zoyzvrs8** with permission to query, create, and encrypt a key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreateGrantSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateGrantRequest request = new CreateGrantRequest();
        CreateGrantRequestBody body = new CreateGrantRequestBody();
        List<String> listbodyOperations = new ArrayList<>();
        listbodyOperations.add("describe-key");
        listbodyOperations.add("create-datakey");
        listbodyOperations.add("encrypt-datakey");

body.withGranteePrincipalType(CreateGrantRequestBody.GranteePrincipalTypeEnum.fromValue("user"));
        body.withRetiringPrincipal("13gg44z4g2sglzk0egw0u726zoyzvrs8");
        body.withOperations(listbodyOperations);
        body.withGranteePrincipal("13gg44z4g2sglzk0egw0u726zoyzvrs8");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            CreateGrantResponse response = client.createGrant(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Grant user **13gg44z4g2sglzk0egw0u726zoyzvrs8** with permission to query, create, and encrypt a key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateGrantRequest()
        listOperationsbody = [
            "describe-key",
            "create-datakey",
            "encrypt-datakey"
        ]
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        request.body = CreateGrantRequestBody(
            grantee_principal_type="user",
            retiring_principal="13gg44z4g2sglzk0egw0u726zoyzvrs8",
            operations=listOperationsbody,
            grantee_principal="13gg44z4g2sglzk0egw0u726zoyzvrs8",
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.create_grant(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Grant user **13gg44z4g2sglzk0egw0u726zoyzvrs8** with permission to query, create, and encrypt a key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateGrantRequest{}
    var listOperationsbody = []string{
        "describe-key",
        "create-datakey",
        "encrypt-datakey",
    }
    granteePrincipalTypeCreateGrantRequestBody:= model.GetCreateGrantRequestBodyGranteePrincipalTypeEnum().USER
    retiringPrincipalCreateGrantRequestBody:= "13gg44z4g2sglzk0egw0u726zoyzvrs8"
    request.Body = &model.CreateGrantRequestBody{
        GranteePrincipalType: &granteePrincipalTypeCreateGrantRequestBody,
        RetiringPrincipal: &retiringPrincipalCreateGrantRequestBody,
        Operations: listOperationsbody,
        GranteePrincipal: "13gg44z4g2sglzk0egw0u726zoyzvrs8",
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.CreateGrant(request)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.12.2 Revoking a Grant

Function

This API is used to revoke a grant.

Note: Only the key creator can revoke the grant of a key.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:revokeGrant	Permission_management	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:grant:revoke	-

URI

POST /v1.0/{project_id}/kms/revoke-grant

Table 4-721 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-722 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-723 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte Key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
grant_id	Yes	String	A 64-byte grant ID which matches the regular expression **^[A-Fa-f0-9]{64}$**, for example, **7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d**.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Request succeeded.

Status code: 400

Table 4-724 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-725 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 401

Table 4-726 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-727 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-728 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-729 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-730 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-731 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-732 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-733 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-734 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-735 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-736 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-737 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Revoke the grant (ID: **7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d**) for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "grant_id" : "7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d"
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Revoke the grant (ID: **7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d**) for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
public class CancelGrantSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CancelGrantRequest request = new CancelGrantRequest();
        RevokeGrantRequestBody body = new RevokeGrantRequestBody();
        body.withGrantId("7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            CancelGrantResponse response = client.cancelGrant(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Revoke the grant (ID: **7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d**) for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
client = KmsClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(KmsRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = CancelGrantRequest()
    request.body = RevokeGrantRequestBody(
        grant_id="7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d",
        key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
    )
    response = client.cancel_grant(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Revoke the grant (ID: **7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d**) for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CancelGrantRequest{}
    request.Body = &model.RevokeGrantRequestBody{
        GrantId: "7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d",
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.CancelGrant(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
  }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.12.3 Retiring a Grant

Function

This API is used to retire grants. After grants are retired, the granted users do not have the permission to operate keys.

For example, user A grants user B the permission to operate key **A** and grants user C the permission to revoke the grant. In this case, all users can retire the grant. After the grant is retired, user B cannot use key **A**.

Only the following users can retire a grant:

User who created the grant

User who has been granted the **retiring_principal** permission

User who has been granted the **grantee_principal** permission if **retire-grant** is contained in the grant list

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:retireGrant	Permission_management	KeyId *	g:ResourceTag/<tag-key>	• kms:grant:retire	-

URI

POST /v1.0/{project_id}/kms/retire-grant

Table 4-738 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-739 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-740 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte Key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
grant_id	Yes	String	A 64-byte grant ID which matches the regular expression **^[A-Fa-f0-9]{64}$**, for example, **7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d**.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Request succeeded.

Status code: 400

Table 4-741 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-742 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 401

Table 4-743 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-744 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-745 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-746 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-747 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-748 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-749 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-750 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-751 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-752 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-753 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-754 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Delete the grant (ID: **7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d**) for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "grant_id" : "7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d"
}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Delete the grant (ID: **7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d**) for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
public class CancelSelfGrantSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CancelSelfGrantRequest request = new CancelSelfGrantRequest();
        RevokeGrantRequestBody body = new RevokeGrantRequestBody();
        body.withGrantId("7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d");
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            CancelSelfGrantResponse response = client.cancelSelfGrant(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Delete the grant (ID: **7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d**) for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
client = KmsClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(KmsRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = CancelSelfGrantRequest()
    request.body = RevokeGrantRequestBody(
        grant_id="7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d",
        key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
    )
    response = client.cancel_self_grant(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Delete the grant (ID: **7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d**) for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CancelSelfGrantRequest{}
    request.Body = &model.RevokeGrantRequestBody{
        GrantId: "7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d",
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.CancelSelfGrant(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
  }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.12.4 Querying the Grant List

Function

This API is used to query the users who have been granted the permissions of a key.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:listGrants	List	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:grant:list	-

URI

POST /v1.0/{project_id}/kms/list-grants

Table 4-755 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-756 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-757 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
limit	No	String	Number of returned records. The default value is **1000**. The value cannot be larger than the maximum number of grants, for example, **100**. If the number of retrieved results is greater than this value, **true** is returned for the response parameter **truncated**, indicating that multiple pages of results are returned.
marker	No	String	Start position of the paginated query. If **truncated** is **true** in the response, you can send consecutive requests to obtain more records. Set **marker** to the value of **next_marker** in the response, for example, **10**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-758 Response body parameters

Parameter	Type	Description
grants	Array of **Grants** objects	Grant list. For details, see the data structure description of the **grants** field.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
next_marker	String	Value of **marker** used for obtaining the next page of results. If the value of **truncated** is **false**, **next_marker** is left empty.
truncated	String	Whether there is another page. **true**: There is more data on the next page. **false**: This is the last page.
total	Integer	Total number of grants.

Table 4-759 Grants

Parameter	Type	Description
key_id	String	Key ID.
grant_id	String	Grant ID, which contains 64 bytes.
grantee_principal	String	ID of the granted user. The value contains 1 to 64 bytes and matches the regular expression **^[a-zA-Z0-9]{1,64}$**, for example, **0d0466b00d0466b00d0466b00d0466b0**.
grantee_principal_type	String	Grant type. The value can be **user** or **domain**.
operations	Array of strings	List of granted operations. Possible values are as follows: **create-datakey**: Create a DEK. **create-datakey-without-plaintext**: Create a DEK that does not contain plaintext. **encrypt-datakey**: Encrypt DEK. **decrypt-datakey**: Decrypt DEK. **describe-key**: Query the key information. **create-grant**: Create the grant. **retire-grant**: Retire the grant. **encrypt-data**: Encrypt data. **decrypt-data**: Decrypt data. The value cannot be only **create-grant**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
issuing_principal	String	ID of the user who created the grant. The value contains 1 to 64 bytes and matches the regular expression **"^[a-zA-Z0-9]{1,64}$**, for example, **0d0466b00d0466b00d0466b00d0466b0**.
creation_date	String	Creation time. The value is a timestamp which indicates how many seconds it has been since January 1, 1970, for example, **1497341531000**.
name	String	Grant name. The value is a string of 1 to 255 characters and matches the regular expression ^[a-zA-Z0-9:/_-]{1,255}$.
retiring_principal	String	ID of the user whose grant can be retired. The value contains 1 to 64 bytes and matches the regular expression **^[a-zA-Z0-9]{1,64}$**, for example, **0d0466b00d0466b00d0466b00d0466b0**.

Status code: 400

Table 4-760 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-761 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-762 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-763 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-764 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-765 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-766 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-767 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-768 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-769 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-770 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-771 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-772 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-773 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Query the grant list of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "grants" : [ {
    "operations" : [ "create-datakey", "describe-key" ],
    "issuing_principal" : "8b961fb414344d59825ba0c8c008c815",
    "key_id" : "737fd52b-36c4-4c91-972e-f6e202de9f6e",
    "grant_id" : "dd3f03e9229a5e47a41be6c27a630e60d5cbdbad2be89465d63109ad034db7d8",
    "grantee_principal" : "13gg44z4g2sglzk0egw0u726zoyzvrs8",
    "name" : "13gg44z4g2sglzk0egw0u726zoyzvrs8",
    "creation_date" : "1597062260000",
    "grantee_principal_type" : "user"
  } ],
  "next_marker" : "",
  "total" : 1,
  "truncated" : "false"
}
```

SDK Sample Code

The SDK sample code is as follows.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Java

Query the grant list of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ListGrantsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ListGrantsRequest request = new ListGrantsRequest();
        ListGrantsRequestBody body = new ListGrantsRequestBody();
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            ListGrantsResponse response = client.listGrants(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Query the grant list of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListGrantsRequest()
        request.body = ListGrantsRequestBody(
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.list_grants(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Query the grant list of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        Build())

    request := &model.ListGrantsRequest{}
    request.Body = &model.ListGrantsRequestBody{
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.ListGrants(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.12.5 Querying Retirable Grants

Function

This API is used to query the list of grants that can be retired.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms::listRetirableGrants	List	-	-	• kms:grant:list	-

URI

POST /v1.0/{project_id}/kms/list-retirable-grants

Table 4-774 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-775 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-776 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	String	Number of returned records of grants that can be retired. If the number of retrieved results is greater than this value, **true** is returned for the response parameter **truncated**, indicating that multiple pages of results are returned.
marker	No	String	Start position of the paginated query. If **truncated** is **true** in the response, you can send consecutive requests to obtain more records. Set **marker** to the value of **next_marker** in the response, for example, **10**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-777 Response body parameters

Parameter	Type	Description
grants	Array of **Grants** objects	Grant list. For details, see the data structure description of the **grants** field.
next_marker	String	Value of **marker** used for obtaining the next page of results. If the value of **truncated** is **false**, **next_marker** is left empty.
total	Integer	Number of grants that can be retired
truncated	String	Whether there is another page. **true**: There is more data on the next page. **false**: This is the last page.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-778 Grants

Parameter	Type	Description
key_id	String	Key ID.
grant_id	String	Grant ID, which contains 64 bytes.
grantee_principal	String	ID of the granted user. The value contains 1 to 64 bytes and matches the regular expression **^[a-zA-Z0-9]{1,64}$**, for example, **0d0466b00d0466b00d0466b00d0466b0**.
grantee_principal_type	String	Grant type. The value can be **user** or **domain**.
operations	Array of strings	List of granted operations. Possible values are as follows: **create-datakey**: Create a DEK. **create-datakey-without-plaintext**: Create a DEK that does not contain plaintext. **encrypt-datakey**: Encrypt DEK. **decrypt-datakey**: Decrypt DEK. **describe-key**: Query the key information. **create-grant**: Create the grant. **retire-grant**: Retire the grant. **encrypt-data**: Encrypt data. **decrypt-data**: Decrypt data. The value cannot be only **create-grant**.
issuing_principal	String	ID of the user who created the grant. The value contains 1 to 64 bytes and matches the regular expression **"^[a-zA-Z0-9]{1,64}$**, for example, **0d0466b00d0466b00d0466b00d0466b0**.
creation_date	String	Creation time. The value is a timestamp which indicates how many seconds it has been since January 1, 1970, for example, **1497341531000**.
name	String	Grant name. The value is a string of 1 to 255 characters and matches the regular expression ^[a-zA-Z0-9:/_-]{1,255}$.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
retiring_principal	String	ID of the user whose grant can be retired. The value contains 1 to 64 bytes and matches the regular expression **^[a-zA-Z0-9]{1,64}$**, for example, **0d0466b00d0466b00d0466b00d0466b0**.

Status code: 400

Table 4-779 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-780 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-781 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-782 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 403

Table 4-783 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-784 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-785 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-786 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-787 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-788 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-789 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-790 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-791 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-792 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

Query grants that can be retired. At most 1,000 grants can be returned.

```
{
  "limit" : "1000"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "grants" : [ {
    "operations" : [ "create-datakey", "describe-key" ],
    "issuing_principal" : "8b961fb414344d59825ba0c8c008c815",
    "key_id" : "737fd52b-36c4-4c91-972e-f6e202de9f6e",
    "grant_id" : "dd3f03e9229a5e47a41be6c27a630e60d5cbdbad2be89465d63109ad034db7d8",
    "grantee_principal" : "13gg44z4g2sglzk0egw0u726zoyzvrs8",
    "name" : "13gg44z4g2sglzk0egw0u726zoyzvrs8",
    "creation_date" : "1597062260000",
    "grantee_principal_type" : "user"
  } ],
  "next_marker" : "",
  "total" : 1,
  "truncated" : "false"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Query grants that can be retired. At most 1,000 grants can be returned.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ListRetirableGrantsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ListRetirableGrantsRequest request = new ListRetirableGrantsRequest();
        ListRetirableGrantsRequestBody body = new ListRetirableGrantsRequestBody();
        body.withLimit("1000");
        request.withBody(body);
        try {
            ListRetirableGrantsResponse response = client.listRetirableGrants(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Query grants that can be retired. At most 1,000 grants can be returned.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListRetirableGrantsRequest()
        request.body = ListRetirableGrantsRequestBody(
            limit="1000"
        )
        response = client.list_retirable_grants(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Go

Query grants that can be retired. At most 1,000 grants can be returned.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListRetirableGrantsRequest{}
    limitListRetirableGrantsRequestBody:= "1000"
    request.Body = &model.ListRetirableGrantsRequestBody{
        Limit: &limitListRetirableGrantsRequestBody,
    }
    response, err := client.ListRetirableGrants(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.13 Key Rotation Management

4.1.13.1 Enabling Key Rotatioin

Function

This API is used to enable CMK rotation.

Note:

The default rotation period is 365 days.

Default CMKs and imported keys cannot be rotated.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:enableRotation	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

URI

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

Table 4-793 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-794 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-795 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Request succeeded.

Status code: 400

Table 4-796 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-797 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-798 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-799 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-800 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-801 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-802 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-803 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-804 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-805 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-806 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-807 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-808 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-809 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

```
Enable rotation for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

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

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class EnableKeyRotationSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        EnableKeyRotationRequest request = new EnableKeyRotationRequest();
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        OperateKeyRequestBody body = new OperateKeyRequestBody();
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            EnableKeyRotationResponse response = client.enableKeyRotation(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = EnableKeyRotationRequest()
        request.body = OperateKeyRequestBody(
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.enable_key_rotation(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.EnableKeyRotationRequest{}
    request.Body = &model.OperateKeyRequestBody{
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.EnableKeyRotation(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Error Codes

See **Error Codes**.

4.1.13.2 Disabling Key Rotation

Function

This API is used to disable CMK rotation.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:disableRotation	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

URI

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-810 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-811 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-812 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Request succeeded.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-813 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-814 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-815 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-816 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-817 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-818 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-819 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-820 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-821 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-822 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-823 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-824 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-825 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-826 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Disable rotation for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

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

Example Responses

None

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

SDK Sample Code

The SDK sample code is as follows.

Java

Disable rotation for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class DisableKeyRotationSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        DisableKeyRotationRequest request = new DisableKeyRotationRequest();
        OperateKeyRequestBody body = new OperateKeyRequestBody();
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            DisableKeyRotationResponse response = client.disableKeyRotation(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Disable rotation for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DisableKeyRotationRequest()
        request.body = OperateKeyRequestBody(
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.disable_key_rotation(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Disable rotation for the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DisableKeyRotationRequest{}
    request.Body = &model.OperateKeyRequestBody{
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.DisableKeyRotation(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.13.3 Modifying the Key Rotation Interval

Function

This API is used to change the CMK rotation period.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:updateRotation	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

URI

POST /v1.0/{project_id}/kms/update-key-rotation-interval

Table 4-827 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-828 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-829 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
rotation_interval	Yes	Integer	Rotation period. The value is an integer ranging from **30** to **365**. Set this parameter based on the key usage frequency. If the key is frequently used, set this parameter to a rather low value, vice versa.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Request succeeded.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-830 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-831 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-832 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-833 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-834 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-835 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-836 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-837 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-838 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-839 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-840 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-841 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-842 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-843 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Change the rotation period of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to 30 days.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "rotation_interval" : 30
}
```

Example Responses

None

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

SDK Sample Code

The SDK sample code is as follows.

Java

Change the rotation period of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to 30 days.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class UpdateKeyRotationIntervalSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateKeyRotationIntervalRequest request = new UpdateKeyRotationIntervalRequest();
        UpdateKeyRotationIntervalRequestBody body = new UpdateKeyRotationIntervalRequestBody();
        body.withRotationInterval(30);
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            UpdateKeyRotationIntervalResponse response = client.updateKeyRotationInterval(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Python

Change the rotation period of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to 30 days.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateKeyRotationIntervalRequest()
        request.body = UpdateKeyRotationIntervalRequestBody(
            rotation_interval=30,
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
        )
        response = client.update_key_rotation_interval(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Change the rotation period of the key whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f** to 30 days.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateKeyRotationIntervalRequest{}
    request.Body = &model.UpdateKeyRotationIntervalRequestBody{
        RotationInterval: int32(30),
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.UpdateKeyRotationInterval(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.1.13.4 Querying the Key Rotation Status

Function

This API is used to query the CMK rotation status.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:cmk:getRotation	Read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

URI

POST /v1.0/{project_id}/kms/get-key-rotation-status

Table 4-844 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-845 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-846 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	A 36-byte key ID which matches the regular expression **^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$**, for example, **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.
sequence	No	String	A 36-byte serial number of a request message, for example, **919c82d4-8046-4722-9094-35c3c6524cff**

Response Parameters

Status code: 200

Table 4-847 Response body parameters

Parameter	Type	Description
key_rotation_enabled	Boolean	Key rotation status. The default value is false, indicating that key rotation is disabled.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
rotation_interval	Integer	Rotation period. The value is an integer ranging from **30** to **365**. Set this parameter based on the key usage frequency. If the key is frequently used, set this parameter to a rather low value, vice versa.
last_rotation_time	String	Last key rotation time. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
number_of_rotations	Integer	Number of key rotations.

Status code: 400

Table 4-848 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-849 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-850 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-851 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-852 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-853 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-854 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-855 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-856 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-857 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-858 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-859 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-860 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-861 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Query the rotation status of the CMK whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "key_rotation_enabled" : true,
  "rotation_interval" : 30,
  "last_rotation_time" : "1501578672000",
  "number_of_rotations" : 3
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Query the rotation status of the CMK whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ShowKeyRotationStatusSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowKeyRotationStatusRequest request = new ShowKeyRotationStatusRequest();
        OperateKeyRequestBody body = new OperateKeyRequestBody();
        body.withKeyId("0d0466b0-e727-4d9c-b35d-f84bb474a37f");
        request.withBody(body);
        try {
            ShowKeyRotationStatusResponse response = client.showKeyRotationStatus(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Query the rotation status of the CMK whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowKeyRotationStatusRequest()
        request.body = OperateKeyRequestBody(
            key_id="0d0466b0-e727-4d9c-b35d-f84bb474a37f"
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        )
        response = client.show_key_rotation_status(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Query the rotation status of the CMK whose ID is **0d0466b0-e727-4d9c-b35d-f84bb474a37f**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowKeyRotationStatusRequest{}
    request.Body = &model.OperateKeyRequestBody{
        KeyId: "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    }
    response, err := client.ShowKeyRotationStatus(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.14 Dedicated Keystore Management

4.1.14.1 Creating a Dedicated Keystore

Function

Create a dedicated keystore. The keystore uses Dedicated HSM instances to store keys.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:keystore:create	Write	keystore *	-	-	-

URI

POST /v1.0/{project_id}/keystores

Table 4-862 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-863 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Table 4-864 Request body parameters

Parameter	Mandatory	Type	Description
keystore_alias	Yes	String	Alias of the dedicated keystore. The value contains 1 to 255 characters, matches the regular expression **^[a-zA-Z0-9:/_-]{1,255}$**, and must be unique.
hsm_cluster_id	No	String	ID of the Dedicated HSM cluster. Ensure that no dedicated keystores are created in the current cluster.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
hsm_ca_cert	No	String	CA certificate of the Dedicated HSM cluster
cluster_id	No	String	Cluster ID. If a Dedicated HSM is used, the **cluster_id** is **hsm_cluster_id**. If a CDMS is used, the **cluster_id** is **cdms_cluster_id**.
keystore_type	No	String	Dedicated keystore cluster type. **1** indicates Dedicated HSM cluster, **2** indicates CDMS cluster, and **0** indicates the original KMS cluster.

Response Parameters

Status code: 200

Table 4-865 Response body parameters

Parameter	Type	Description
keystore	**KeystoreInfo** object	Keystore information

Table 4-866 KeystoreInfo

Parameter	Type	Description
keystore_id	String	Keystore ID
domain_id	String	User domain ID

Status code: 400

Table 4-867 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-868 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-869 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-870 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-871 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-872 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 404

Table 4-873 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-874 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-875 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-876 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-877 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-878 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-879 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-880 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

Create a dedicated keystore whose alias is **keystore_alia1** and cluster ID is **hsm_cluster_id**.

```
{
  "keystore_alias" : "keystore_alia1",
  "hsm_cluster_id" : "hsm_cluster_id",
  "hsm_ca_cert" : "-----BEGIN CERTIFICATE---******----END CERTIFICATE-----"
}
```

Example Responses

Status code: 200

Request succeeded.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

SDK Sample Code

The SDK sample code is as follows.

Java

Create a dedicated keystore whose alias is **keystore_alia1** and cluster ID is **hsm_cluster_id**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class CreateKeyStoreSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateKeyStoreRequest request = new CreateKeyStoreRequest();
        CreateKeyStoreRequestBody body = new CreateKeyStoreRequestBody();
        body.withHsmCaCert("-----BEGIN CERTIFICATE---******----END CERTIFICATE-----");
        body.withHsmClusterId("hsm_cluster_id");
        body.withKeystoreAlias("keystore_alia1");
        request.withBody(body);
        try {
            CreateKeyStoreResponse response = client.createKeyStore(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Python

Create a dedicated keystore whose alias is **keystore_alia1** and cluster ID is **hsm_cluster_id**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateKeyStoreRequest()
        request.body = CreateKeyStoreRequestBody(
            hsm_ca_cert="-----BEGIN CERTIFICATE---******----END CERTIFICATE-----",
            hsm_cluster_id="hsm_cluster_id",
            keystore_alias="keystore_alia1"
        )
        response = client.create_key_store(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Create a dedicated keystore whose alias is **keystore_alia1** and cluster ID is **hsm_cluster_id**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateKeyStoreRequest{}
    hsmCaCertCreateKeyStoreRequestBody:= "-----BEGIN CERTIFICATE---******----END CERTIFICATE-----"
    hsmClusterIdCreateKeyStoreRequestBody:= "hsm_cluster_id"
    request.Body = &model.CreateKeyStoreRequestBody{
        HsmCaCert: &hsmCaCertCreateKeyStoreRequestBody,
        HsmClusterId: &hsmClusterIdCreateKeyStoreRequestBody,
        KeystoreAlias: "keystore_alia1",
    }
    response, err := client.CreateKeyStore(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.1.14.2 Querying the List of Dedicated Keystores

Function

This API is used to query the dedicated keystore list.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:keystore:list	List	keystore *	-	-	-

URI

GET /v1.0/{project_id}/keystores

Table 4-881 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-882 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of returned records. The default value is **10**.
offset	No	Integer	Index location. The query starts from the next data specified by **offset**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-883 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-884 Response body parameters

Parameter	Type	Description
total	Integer	Total number of keystores
keystores	Array of KeystoreDetails objects	List of keystore details. For details, see **KeystoreDetails**.

Table 4-885 KeystoreDetails

Parameter	Type	Description
keystore_id	String	Keystore ID
domain_id	String	User domain ID
keystore_alias	String	Keystore alias
keystore_type	String	Keystore type
hsm_cluster_id	String	Dedicated HSM cluster ID. Ensure that no dedicated keystores are created in the current cluster.
create_time	String	Keystore creation time, which is a UTC timestamp.
cluster_id	String	Cluster ID. If a Dedicated HSM is used, the **cluster_id** is **hsm_cluster_id**. If a CDMS is used, the **cluster_id** is **cdms_cluster_id**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 400

Table 4-886 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-887 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-888 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-889 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-890 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-891 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-892 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-893 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-894 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-895 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-896 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-897 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-898 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-899 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 1,
  "keystores" : [ {
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "keystore_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "domain_id" : "b168fe00ff56492495a7d22974df2d0b",
    "keystore_alias" : "test",
    "keystore_type" : "typetest",
    "hsm_cluster_id" : "cluster_id",
    "create_time" : 1581507580000
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ListKeyStoresSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ListKeyStoresRequest request = new ListKeyStoresRequest();
        try {
            ListKeyStoresResponse response = client.listKeyStores(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListKeyStoresRequest()
        response = client.list_key_stores(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        Build())

    request := &model.ListKeyStoresRequest{}
    response, err := client.ListKeyStores(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.14.3 Obtaining a Dedicated Keystore

Function

This API is used to obtain a dedicated keystore.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:keystore:get	Read	keystore *	-	-	-

URI

GET /v1.0/{project_id}/keystores/{keystore_id}

Table 4-900 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keystore_id	Yes	String	Keystore ID

Request Parameters

Table 4-901 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-902 Response body parameters

Parameter	Type	Description
keystore	**KeystoreDetails** object	Keystore details

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-903 KeystoreDetails

Parameter	Type	Description
keystore_id	String	Keystore ID
domain_id	String	User domain ID
keystore_alias	String	Keystore alias
keystore_type	String	Keystore type
hsm_cluster_id	String	Dedicated HSM cluster ID. Ensure that no dedicated keystores are created in the current cluster.
create_time	String	Keystore creation time, which is a UTC timestamp.
cluster_id	String	Cluster ID. If a Dedicated HSM is used, the **cluster_id** is **hsm_cluster_id**. If a CDMS is used, the **cluster_id** is **cdms_cluster_id**.

Status code: 400

Table 4-904 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-905 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-906 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-907 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-908 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-909 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-910 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-911 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-912 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-913 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-914 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-915 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-916 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-917 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "keystore" : {
    "keystore_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "domain_id" : "b168fe00ff56492495a7d22974df2d0b",
    "keystore_alias" : "test",
    "keystore_type" : "typetest",
    "hsm_cluster_id" : "cluster_id",
    "create_time" : 1581507580000
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ShowKeyStoreSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowKeyStoreRequest request = new ShowKeyStoreRequest();
        request.withKeystoreId("{keystore_id}");
        try {
            ShowKeyStoreResponse response = client.showKeyStore(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowKeyStoreRequest()
        request.keystore_id = "{keystore_id}"
        response = client.show_key_store(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowKeyStoreRequest{}
    request.KeystoreId = "{keystore_id}"
    response, err := client.ShowKeyStore(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Username and password are required for the requested page.
404	The resource does not exist.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.14.4 Deleting a Dedicated Keystore

Function

This API is used to delete a dedicated keystore.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:keystore:delete	Write	keystore *	-	-	-

URI

DELETE /v1.0/{project_id}/keystores/{keystore_id}

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-918 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keystore_id	Yes	String	Keystore ID

Request Parameters

Table 4-919 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 200

Deleted.

Status code: 400

Table 4-920 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-921 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-922 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-923 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-924 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-925 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-926 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-927 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-928 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-929 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-930 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-931 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-932 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-933 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

None

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class DeleteKeyStoreSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteKeyStoreRequest request = new DeleteKeyStoreRequest();
        request.withKeystoreId("{keystore_id}");
        try {
            DeleteKeyStoreResponse response = client.deleteKeyStore(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteKeyStoreRequest()
        request.keystore_id = "{keystore_id}"
        response = client.delete_key_store(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteKeyStoreRequest{}
    request.KeystoreId = "{keystore_id}"
    response, err := client.DeleteKeyStore(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Deleted.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.14.5 Enabling a Dedicated Keystore

Function

This API is used to enable a dedicated keystore.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:keystore:enable	Write	keystore *	-	-	-

URI

POST /v1.0/{project_id}/keystores/{keystore_id}/enable

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-934 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keystore_id	Yes	String	Keystore ID

Request Parameters

Table 4-935 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-936 Response body parameters

Parameter	Type	Description
keystore	**KeyStoreStateInfo** object	Keystore status information

Table 4-937 KeyStoreStateInfo

Parameter	Type	Description
keystore_id	String	Keystore ID
keystore_state	String	Keystore status

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-938 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-939 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-940 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-941 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

Table 4-942 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-943 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-944 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-945 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-946 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-947 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-948 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-949 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-950 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-951 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "keystore_state" : "2"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class EnableKeyStoreSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        EnableKeyStoreRequest request = new EnableKeyStoreRequest();
        request.withKeystoreId("{keystore_id}");
        try {
            EnableKeyStoreResponse response = client.enableKeyStore(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = EnableKeyStoreRequest()
        request.keystore_id = "{keystore_id}"
        response = client.enable_key_store(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.EnableKeyStoreRequest{}
    request.KeystoreId = "{keystore_id}"
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    response, err := client.EnableKeyStore(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.1.14.6 Disabling a Dedicated Keystore

Function

This API is used to disable a dedicated keystore.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kms:keystore:disable	Write	keystore *	-	-	-

URI

POST /v1.0/{project_id}/keystores/{keystore_id}/disable

Table 4-952 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keystore_id	Yes	String	Keystore ID

Request Parameters

Table 4-953 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-954 Response body parameters

Parameter	Type	Description
keystore	**KeyStoreStateInfo** object	Keystore status information

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-955 KeyStoreStateInfo

Parameter	Type	Description
keystore_id	String	Keystore ID
keystore_state	String	Keystore status

Status code: 400

Table 4-956 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-957 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 401

Table 4-958 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-959 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-960 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-961 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 404

Table 4-962 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-963 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 500

Table 4-964 Response body parameters

Parameter	Type	Description
error	Object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-965 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 502

Table 4-966 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-967 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

Status code: 504

Table 4-968 Response body parameters

Parameter	Type	Description
error	Object	Error message

Table 4-969 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned by the error request
error_msg	String	Error information returned by the error request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "keystore" : {
    "keystore_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "keystore_state" : "3"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class DisableKeyStoreSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        DisableKeyStoreRequest request = new DisableKeyStoreRequest();
        request.withKeystoreId("{keystore_id}");
        try {
            DisableKeyStoreResponse response = client.disableKeyStore(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DisableKeyStoreRequest()
        request.keystore_id = "{keystore_id}"
        response = client.disable_key_store(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DisableKeyStoreRequest{}
    request.KeystoreId = "{keystore_id}"
    response, err := client.DisableKeyStore(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Failed to complete the request. The server receives an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.2 Key Pair Management APIs

4.2.1 Key Pair Management

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.2.1.1 Creating and Importing an SSH Key Pair

Function

Creating and Importing an SSH Key Pair

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps:SSHKeyPair:create	Write	SSHKeyPair *	• kps:KmsKeyId • kps:Algorithm	• kps:domainKeypairs:create	• kms:cmk:createDataKey • kms:cmk:list

URI

POST /v3/{project_id}/keypairs

Table 4-970 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-971 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Table 4-972 Request body parameters

Parameter	Mandatory	Type	Description
keypair	Yes	**CreateKeypairAction** object	Parameter in the request body for creating a key pair

Table 4-973 CreateKeypairAction

Parameter	Mandatory	Type	Description
name	Yes	String	SSH key pair name. • The key pair name must be unique. • The SSH key pair name can contain at most 255 characters, including letters, digits, underscores (_), and hyphens (-).
type	No	String	SSH key pair type. The value can be **ssh** or **x509**.
public_key	No	String	String of an imported public key
scope	No	String	Tenant-level or user-level. The value can be **domain** or **user**.
user_id	No	String	User that an SSH key pair belongs to
key_protection	No	**KeyProtection** object	Private key hosting and protection for the SSH key pair.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-974 KeyProtection

Parameter	Mandatory	Type	Description
private_key	No	String	Private key of the imported SSH key pair.
encryption	Yes	**Encryption** object	How a private key is encrypted and stored.

Table 4-975 Encryption

Parameter	Mandatory	Type	Description
type	Yes	String	Value options: - default: The default encryption mode. Applicable to sites where KMS is not deployed. - kms: KMS encryption mode. If the KMS service is not available at the site, set this parameter to default.
kms_key_name	No	String	KMS key name. • If **type** is set to **kms**, you must enter the KMS key name or ID.
kms_key_id	No	String	KMS key ID. • If **type** is set to **kms**, you must enter the KMS key name or ID.

Response Parameters

Status code: 200

Table 4-976 Response body parameters

Parameter	Type	Description
keypair	**CreateKeypairResp** object	SSH key pair details

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-977 CreateKeypairResp

Parameter	Type	Description
name	String	SSH key pair name
type	String	SSH key pair type. The value can be **ssh** or **x509**.
public_key	String	Public key information about an SSH key pair
private_key	String	Private key information about an SSH key pair. - When an SSH key pair is created, the response contains private_key information. - When an SSH key pair is imported, the response does not contain private_key information.
fingerprint	String	Fingerprint information about an SSH key pair
user_id	String	User that an SSH key pair belongs to

Status code: 400

Table 4-978 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

Example Requests

```
{
  "keypair" : {
    "name" : "demo2"
  }
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "keypair" : {
    "name" : "demo",
    "type" : "ssh",
    "public_key" : "ssh-rsa AAAAB3NzaC1yc2EAAAADAQAB...",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "private_key" : "-----BEGIN RSA PRIVATE KEY-----...",
    "fingerprint" : "49:ef:73:2b:9b:7f:2e:0c:58:d3:e3:42:8e:28:04:3b",
    "user_id" : "e4f380899b1248918f3d37098dc63746"
  }
}
```

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Error response

Error Codes

See **Error Codes**.

4.2.1.2 Accessing the page for clearing private keys

Function

This API is used to delete the private key of an SSH key pair.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps:SSHKeyPair:clearPrivateKey	Write	SSHKeyPair *	-	• kps:domainKeypairs:clearpk	-

URI

DELETE /v3/{project_id}/keypairs/{keypair_name}/private-key

Table 4-979 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
keypair_name	Yes	String	Key pair name.

Request Parameters

Table 4-980 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

Request succeeded.

Status code: 404

Table 4-981 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.2.1.3 Querying the SSH Key Pair List

Function

Querying the SSH Key Pair List

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps:SSHKeyPair:list	List	SSHKeyPair *	-	• kps:domainKeypairs:list	-

URI

GET /v3/{project_id}/keypairs

Table 4-982 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-983 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	String	Number of records on each page. Default value: 50
marker	No	String	Specifies the resource ID of pagination query. If the parameter is left blank, only resources on the first page are queried.

Request Parameters

Table 4-984 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 200

Table 4-985 Response body parameters

Parameter	Type	Description
keypairs	Array of **Keypairs** objects	SSH key pair list
page_info	**PageInfo** object	Pagination information.

Table 4-986 Keypairs

Parameter	Type	Description
keypair	**Keypair** object	Key pair information

Table 4-987 Keypair

Parameter	Type	Description
name	String	SSH key pair name
type	String	Type of the SSH key pair. The value can be ssh or x509.
scope	String	Tenant-level or user-level. The value can be **domain** or **user**.
public_key	String	Public key information about an SSH key pair
fingerprint	String	Fingerprint information about an SSH key pair
is_key_protection	Boolean	Whether to host keys

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
frozen_state	String	Frozen Status - 0: normal, not frozen - 1: frozen due to common causes - 2: frozen by the public security bureau - 3: frozen due to common causes and by the public security bureau - 4: frozen due to violations - 5: frozen due to common causes and violations - 6: frozen by the public security bureau and due to violations - 7: frozen by the public security bureau and due to common causes and violations - 8: frozen due to lack of real-name authentication - 9: frozen due to common causes and lack of real-name authentication - 10: frozen by the public security bureau and due to lack of real-name authentication

Table 4-988 PageInfo

Parameter	Type	Description
next_marker	String	Query Address for Returning to the Next Page
previous_marker	String	Return to the query address of the previous page.
current_count	Integer	Number of returned items.

Status code: 400

Table 4-989 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "keypairs" : [ {
    "keypair" : {
      "name" : "1hprr3TI",
      "type" : "ssh",
      "scope" : "user",
      "public_key" : "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABjV8GvwpSs.....",
      "fingerprint" : "65:ca:87:0a:16:86:59:ea:57:ea:18:37:58:e2:04:b0",
      "is_key_protection" : false,
      "frozen_state" : 0
    }
  } ],
  "page_info" : {
    "next_marker" : "KeyPair-dxxx",
    "previous_marker" : "KeyPair-xxxx",
    "current_count" : 49
  }
}
```

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Error response

Error Codes

See **Error Codes**.

4.2.1.4 Querying SSH Key Pair Details

Function

Querying SSH Key Pair Details

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps:SSHKeyPair:get	Read	SSHKeyPair *	-	• kps:domainKeypairs:get	-

URI

GET /v3/{project_id}/keypairs/{keypair_name}

Table 4-990 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keypair_name	Yes	String	Key pair name.

Request Parameters

Table 4-991 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 200

Table 4-992 Response body parameters

Parameter	Type	Description
keypair	**KeypairDetail** object	Key pair details

Table 4-993 KeypairDetail

Parameter	Type	Description
name	String	SSH key pair name
id	Long	SSH key pair ID
type	String	SSH key pair type. The value can be **ssh** or **x509**.
scope	String	Tenant-level or user-level. The value can be **domain** or **user**.
public_key	String	Public key information about an SSH key pair
fingerprint	String	Fingerprint information about an SSH key pair
is_key_protection	Boolean	Whether to host keys
deleted	Boolean	Tag that indicates an SSH key pair is deleted
description	String	Description of an SSH key pair
user_id	String	User that an SSH key pair belongs to
create_time	Long	Time when the SSH key pair was created. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
delete_time	Long	Time when the SSH key pair was deleted. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
update_time	Long	Time when the SSH key pair was updated. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
frozen_state	Integer	Frozen Status - 0: normal, not frozen - 1: frozen due to common causes - 2: frozen by the public security bureau - 3: frozen due to common causes and by the public security bureau - 4: frozen due to violations - 5: frozen due to common causes and violations - 6: frozen by the public security bureau and due to violations - 7: frozen by the public security bureau and due to common causes and violations - 8: frozen due to lack of real-name authentication - 9: frozen due to common causes and lack of real-name authentication - 10: frozen by the public security bureau and due to lack of real-name authentication
key_id	String	Specifies the key pair ID.
algorithm	String	Generation algorithm.

Status code: 400

Table 4-994 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

Example Requests

None

Example Responses

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request succeeded.


```
{
  "keypair" : {
    "name" : "1hprr3TI",
    "id" : 116248,
    "type" : "ssh",
    "scope" : "user",
    "public_key" : "ssh-rsa AAAGenerated-by-Nova",
    "fingerprint" : "65:ca:87:0a:16:86:59:ea:57:ea:18:37:58:e2:04:b0",
    "is_key_protection" : false,
    "deleted" : false,
    "description" : "12345",
    "user_id" : "6c2a33b1b8474d0dbac0a24297127525",
    "create_time" : 1581507580000,
    "delete_time" : null,
    "update_time" : null,
    "frozen_state" : 0
  }
}
```


Status code: 400

Error response


```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```


Status Codes

Status Code	Description
200	Request succeeded.
400	Error response

Error Codes

See **Error Codes**.

4.2.1.5 Deleting an SSH Key Pair

Function

This API is used to delete an SSH key pair.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps:SSHKeyPair:delete	Write	SSHKeyPair *	-	• kps:domainKeypairs:delete	-

URI

DELETE /v3/{project_id}/keypairs/{keypair_name}

Table 4-995 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keypair_name	Yes	String	Key pair name.

Request Parameters

Table 4-996 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Response Parameters

Status code: 204

OK

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-997 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

Example Requests

None

Example Responses

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	OK
400	Error response

Error Codes

See **Error Codes**.

4.2.1.6 Updating SSH Key Pair Description

Function

This API is used to update the description of an SSH key pair.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps:SSHKeyPair:update	Write	SSHKeyPair *	-	• kps:domainKeypairs:update	-

URI

PUT /v3/{project_id}/keypairs/{keypair_name}

Table 4-998 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keypair_name	Yes	String	Key pair name.

Request Parameters

Table 4-999 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Table 4-1000 Request body parameters

Parameter	Mandatory	Type	Description
keypair	Yes	**UpdateKeypairDescriptionReq** object	Message body for updating the SSH key pair description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1001 UpdateKeypairDescriptionReq

Parameter	Mandatory	Type	Description
description	Yes	String	Description

Response Parameters

Status code: 200

OK

Status code: 400

Table 4-1002 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

Example Requests

```
{
  "keypair" : {
    "description" : "description"
  }
}
```

Example Responses

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	OK
400	Error response

Error Codes

See **Error Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.2.1.7 Accessing the page for importing private keys

Function

Import the private key to the specified key pair.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps:SSHKeyPair:importPrivateKey	Write	SSHKeyPair *	kps:KmsKeyId	• kps:domainKeypairs:importpk	• kms:cmk:createDataKey • kms:cmk:list

URI

POST /v3/{project_id}/keypairs/private-key/import

Table 4-1003 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1004 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Table 4-1005 Request body parameters

Parameter	Mandatory	Type	Description
keypair	Yes	**ImportPrivateKeyKeypairBean** object	Information about the key pair to be imported

Table 4-1006 ImportPrivateKeyKeypairBean

Parameter	Mandatory	Type	Description
name	Yes	String	SSH key pair name. - The name of a key pair must be unique. - The key pair name can contain letters, digits, underscores (_), and hyphens (-) and cannot exceed 64 bytes.
user_id	No	String	User that an SSH key pair belongs to
key_protection	Yes	**ImportPrivateKeyProtection** object	Private key hosting and protection for the SSH key pair.

Table 4-1007 ImportPrivateKeyProtection

Parameter	Mandatory	Type	Description
private_key	Yes	String	Private key of the imported SSH key pair.
encryption	Yes	**Encryption** object	How a private key is encrypted and stored.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1008 Encryption

Parameter	Mandatory	Type	Description
type	Yes	String	Value options: - default: The default encryption mode. Applicable to sites where KMS is not deployed. - kms: KMS encryption mode. If the KMS service is not available at the site, set this parameter to default.
kms_key_name	No	String	KMS key name. • If **type** is set to **kms**, you must enter the KMS key name or ID.
kms_key_id	No	String	KMS key ID. • If **type** is set to **kms**, you must enter the KMS key name or ID.

Response Parameters

Status code: 200

Table 4-1009 Response body parameters

Parameter	Type	Description
keypair	**ImportPrivateKeyKeypairBean** object	One

Table 4-1010 ImportPrivateKeyKeypairBean

Parameter	Type	Description
name	String	SSH key pair name. - The name of a key pair must be unique. - The key pair name can contain letters, digits, underscores (_), and hyphens (-) and cannot exceed 64 bytes.
user_id	String	User that an SSH key pair belongs to

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
key_protection	**ImportPrivateKeyProtection** object	Private key hosting and protection for the SSH key pair.

Table 4-1011 ImportPrivateKeyProtection

Parameter	Type	Description
private_key	String	Private key of the imported SSH key pair.
encryption	**Encryption** object	How a private key is encrypted and stored.

Table 4-1012 Encryption

Parameter	Type	Description
type	String	Value options: - default: The default encryption mode. Applicable to sites where KMS is not deployed. - kms: KMS encryption mode. If the KMS service is not available at the site, set this parameter to default.
kms_key_name	String	KMS key name. • If **type** is set to **kms**, you must enter the KMS key name or ID.
kms_key_id	String	KMS key ID. • If **type** is set to **kms**, you must enter the KMS key name or ID.

Status code: 400

Table 4-1013 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

```
{
  "keypair" : {
    "name" : "demo2",
    "key_protection" : {
      "private_key" : "-----BEGIN RSA PRIVATE KEY------...",
      "encryption" : {
        "type" : "kms",
        "kms_key_name" : "kps/default"
      }
    }
  }
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "keypair" : {
    "name" : "demo2"
  }
}
```

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Error response

Error Codes

See **Error Codes**.

4.2.1.8 Exporting a private key

Function

Export the private key of a specified key pair.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps:SSHKeyPair:exportPrivateKey	Write	SSHKeyPair *	-	• kps:domainKeypairs:exportpk	kms:cmk:decryptDataKey

URI

POST /v3/{project_id}/keypairs/private-key/export

Table 4-1014 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-1015 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1016 Request body parameters

Parameter	Mandatory	Type	Description
keypair	Yes	**KeypairBean** object	Information about the key pair whose private key is to be exported

Table 4-1017 KeypairBean

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the key pair.

Response Parameters

Status code: 200

Table 4-1018 Response body parameters

Parameter	Type	Description
keypair	**ExportPrivateKey KeypairBean** object	Information about the exported private key

Table 4-1019 ExportPrivateKeyKeypairBean

Parameter	Type	Description
name	String	SSH key pair name.
private_key	String	Private key of the SSH key pair

Status code: 400

Table 4-1020 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

```
{
  "keypair" : {
    "name" : "demo2"
  }
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "keypair" : {
    "name" : "demo2",
    "private_key" : "-----BEGIN RSA PRIVATE KEY-----..."
  }
}
```

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Error response

Error Codes

See **Error Codes**.

4.2.1.9 Importing SSH Key Pairs in Batches

Function

This API is used to batch import SSH key pairs. A maximum of 10 SSH key pairs can be selected at a time.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v3/{project_id}/keypairs/batch-import

Table 4-1021 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-1022 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-1023 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of **CreateKeypairRequestBody** objects	Request body for creating a key pair

Table 4-1024 CreateKeypairRequestBody

Parameter	Mandatory	Type	Description
keypair	Yes	**CreateKeypairAction** object	Parameter in the request body for creating a key pair

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1025 CreateKeypairAction

Parameter	Mandatory	Type	Description
name	Yes	String	SSH key pair name. • The key pair name must be unique. • The SSH key pair name can contain at most 255 characters, including letters, digits, underscores (_), and hyphens (-).
type	No	String	SSH key pair type. The value can be **ssh** or **x509**.
public_key	No	String	String of an imported public key
scope	No	String	Tenant-level or user-level. The value can be **domain** or **user**.
user_id	No	String	User that an SSH key pair belongs to
key_protection	No	**KeyProtection** object	Private key hosting and protection for the SSH key pair.

Table 4-1026 KeyProtection

Parameter	Mandatory	Type	Description
private_key	No	String	Private key of the imported SSH key pair.
encryption	Yes	**Encryption** object	How a private key is encrypted and stored.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1027 Encryption

Parameter	Mandatory	Type	Description
type	Yes	String	Value options: - default: The default encryption mode. Applicable to sites where KMS is not deployed. - kms: KMS encryption mode. If the KMS service is not available at the site, set this parameter to default.
kms_key_name	No	String	KMS key name. • If **type** is set to **kms**, you must enter the KMS key name or ID.
kms_key_id	No	String	KMS key ID. • If **type** is set to **kms**, you must enter the KMS key name or ID.

Response Parameters

Status code: 200

Table 4-1028 Response body parameters

Parameter	Type	Description
failed_keypairs	Array of **FailedKeypair** objects	Information about the SSH key pair that fails to be imported and the failure cause
succeeded_keypairs	Array of **CreateKeypairResponseBody** objects	Information about the imported SSH key pair

Table 4-1029 FailedKeypair

Parameter	Type	Description
keypair_name	String	SSH key pair name
failed_reason	String	Import failure cause

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1030 CreateKeypairResponseBody

Parameter	Type	Description
keypair	**CreateKeypairResp** object	SSH key pair details

Table 4-1031 CreateKeypairResp

Parameter	Type	Description
name	String	SSH key pair name
type	String	SSH key pair type. The value can be **ssh** or **x509**.
public_key	String	Public key information about an SSH key pair
private_key	String	Private key information about an SSH key pair. - When an SSH key pair is created, the response contains private_key information. - When an SSH key pair is imported, the response does not contain private_key information.
fingerprint	String	Fingerprint information about an SSH key pair
user_id	String	User that an SSH key pair belongs to

Example Requests

Import the **demo2** and **demo3** SSH key pairs in batches.

```
[ {
  "keypair" : {
    "name" : "demo2",
    "public_key" : "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAA... Generated-by-Nova"
  }
}, {
  "keypair" : {
    "name" : "demo3",
    "public_key" : "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAA... Generated-by-Nova"
  }
} ]
```

Example Responses

Status code: 200

The SSH key pairs are imported in batches.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
{
  "failed_keypairs" : [ {
    "keypair_name" : "demo3",
    "failed_reason" : "{\"error_code\":\"KPS.7004\", \"error_msg\":\"Key pair 'demo3' already exists.\"}"
  } ],
  "succeeded_keypairs" : [ {
    "keypair" : {
      "name" : "demo2",
      "fingerprint" : "SHA256:Wm91+h496cPk5JleSp4RdD2n4Z/5KdlDeD51lmiZ11M",
      "type" : "ssh",
      "public_key" : "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAA... Generated-by-Nova",
      "user_id" : "6c2a33b1b8474d0dbac0a24297127525"
    }
  } ]
}
```

Status Codes

Status Code	Description
200	The SSH key pairs are imported in batches.

Error Codes

See **Error Codes**.

4.2.1.10 Exporting Private Keys of Key Pairs in Batches

Function

This API is used to export private keys of key pairs in batches. A maximum of 10 private keys can be selected at a time.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v3/{project_id}/keypairs/private-key/batch-export

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1032 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-1033 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-1034 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of **Keypairs** objects	List of keys to be exported.

Table 4-1035 Keypairs

Parameter	Mandatory	Type	Description
keypair	Yes	**Keypair** object	Key pair information

Table 4-1036 Keypair

Parameter	Mandatory	Type	Description
name	No	String	SSH key pair name
type	No	String	Type of the SSH key pair. The value can be ssh or x509.
scope	No	String	Tenant-level or user-level. The value can be **domain** or **user**.
public_key	No	String	Public key information about an SSH key pair

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
fingerprint	No	String	Fingerprint information about an SSH key pair
is_key_protection	No	Boolean	Whether to host keys
frozen_state	No	String	Frozen Status - 0: normal, not frozen - 1: frozen due to common causes - 2: frozen by the public security bureau - 3: frozen due to common causes and by the public security bureau - 4: frozen due to violations - 5: frozen due to common causes and violations - 6: frozen by the public security bureau and due to violations - 7: frozen by the public security bureau and due to common causes and violations - 8: frozen due to lack of real-name authentication - 9: frozen due to common causes and lack of real-name authentication - 10: frozen by the public security bureau and due to lack of real-name authentication

Response Parameters

Status code: 200

Request succeeded.

None

Example Requests

Export the **demo2**, **demo3**, and **demo4** SSH key pairs in batches.

```
[ {
  "keypair" : {
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "name" : "demo2"
  }
}, {
  "keypair" : {
    "name" : "demo3"
  }
}, {
  "keypair" : {
    "name" : "demo4"
  }
} ]
```

Example Responses

Status code: 200

Request succeeded.

```
"keypairs.zip"
```

Status Codes

Status Code	Description
200	Request succeeded.

Error Codes

See **Error Codes**.

4.2.2 Key pair task management

4.2.2.1 Binding an SSH Key Pair

Function

Binds an SSH key pair to a specified VM. (The private key of the SSH key pair for the VM is required if you want to replace the key pair, but not required if you want to reset the key pair.)

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps:SSHKeyPair:bind	Write	SSHKeyPair *	-	• kps:domainKeypairs:bind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServer

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
					Quotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list

URI

POST /v3/{project_id}/keypairs/associate

Table 4-1037 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-1038 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Table 4-1039 Request body parameters

Parameter	Mandatory	Type	Description
keypair_name	Yes	String	SSH key pair name

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
server	Yes	**EcsServerInfo** object	Information about the VM that the key pair is to be bound to

Table 4-1040 EcsServerInfo

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the VM that the SSH key pair is to be bound to (in order to replace or reset the original key pair).
auth	No	**Auth** object	(Optional) Authentication type. This parameter is required for key pair replacement but not required for key pair reset.
disable_password	No	Boolean	• true: SSH login is disabled on the VM. - false: SSH login is enabled on the VM.
port	No	Long	SSH listening port.

Table 4-1041 Auth

Parameter	Mandatory	Type	Description
type	No	String	The value can be **password** or **keypair**.
key	No	String	• If type is set to password, key indicates the password. • If type is set to keypair, key indicates the private key.

Response Parameters

Status code: 202

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1042 Response body parameters

Parameter	Type	Description
task_id	String	ID returned when a task is delivered
server_id	String	Specifies the ID of the bound VM.
status	String	Indicates the delivery status of a task. SUCCESS or FAILED.
error_code	String	Error code returned when a task fails to be delivered.
error_msg	String	Error information returned when a task fails to be delivered.

Status code: 400

Table 4-1043 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

Example Requests

- ```
  {
    "keypair_name" : "newkeypair1",
    "server" : {
      "id" : "d76baba7-ef09-40a2-87ff-3eafec0696e7",
      "auth" : {
        "type" : "keypair",
        "key" : "-----BEGINRSAPRIVATEKEY-----M..."
      }
    }
  }
  ```
- ```
  {
    "keypair_name" : "newkeypair2",
    "server" : {
      "id" : "d76baba7-ef09-40a2-87ff-3eafec0696e7"
    }
  }
  ```

Example Responses

Status code: 202

OK

```
{
  "task_id" : "aee8d2fe-5484-4753-9177-5a38dc15546c"
}
```

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
202	OK
400	Error response

Error Codes

See **Error Codes**.

4.2.2.2 Unbind an SSH Key Pair

Function

Unbinds an SSH key pair from a specified VM and restores SSH password login.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps:SSHKeyPair:unbind	Write	SSHKeyPair *	-	• kps:domainKeypairs:unbind • ecs:serverKeypairs:unbind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServer

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
					Quotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list

URI

POST /v3/{project_id}/keypairs/disassociate

Table 4-1044 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-1045 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Table 4-1046 Request body parameters

Parameter	Mandatory	Type	Description
server	Yes	DisassociateEcsServerInfo object	Information about the VM that the key pair is to be bound to

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1047 DisassociateEcsServerInfo

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the VM that the SSH key pair is to be bound to (in order to replace or reset the original key pair).
auth	No	**Auth** object	(Optional) Authentication type. This parameter is required for key pair replacement but not required for key pair reset.

Table 4-1048 Auth

Parameter	Mandatory	Type	Description
type	No	String	The value can be **password** or **keypair**.
key	No	String	• If type is set to password, key indicates the password. • If type is set to keypair, key indicates the private key.

Response Parameters

Status code: 202

Table 4-1049 Response body parameters

Parameter	Type	Description
task_id	String	ID returned when a task is delivered
server_id	String	Specifies the ID of the bound VM.
status	String	Indicates the delivery status of a task. SUCCESS or FAILED.
error_code	String	Error code returned when a task fails to be delivered.
error_msg	String	Error information returned when a task fails to be delivered.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1050 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

Example Requests

- ```
  {
    "server" : {
      "id" : "d76baba7-ef09-40a2-87ff-3eafec0696e7",
      "auth" : {
        "type" : "keypair",
        "key" : "-----BEGINRSAPRIVATEKEY-----\nM..."
      }
    }
  }
  ```
- ```
  {
    "server" : {
      "id" : "x76baba7-ef09-40a2-87ff-3eafec0696e7"
    }
  }
  ```

Example Responses

Status code: 202

OK

```
{
  "task_id" : "aee8d2fe-5484-4753-9177-5a38dc15546c"
}
```

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
202	OK
400	Error response

Error Codes

See **Error Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.2.2.3 Binding SSH Key Pairs in Batches

Function

This interface is used to bind new SSH key pairs to specified VMs in batches.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps:SSHKeyPair:bind	Write	SSHKeyPair *	-	• kps:domainKeypairs:bind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServer

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
					Quotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list

URI

POST /v3/{project_id}/keypairs/batch-associate

Table 4-1051 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-1052 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1053 Request body parameters

Parameter	Mandatory	Type	Description
batch_keypairs	Yes	Array of **AssociateKeypairRequestBody** objects	You can select a maximum of 10 ECSs to bind key pairs at a time. Constraints: Only the same key pair can be selected. The ECS is in the Running state and has not been bound to any key pair.

Table 4-1054 AssociateKeypairRequestBody

Parameter	Mandatory	Type	Description
keypair_name	Yes	String	SSH key pair name
server	Yes	**EcsServerInfo** object	Information about the VM that the key pair is to be bound to

Table 4-1055 EcsServerInfo

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the VM that the SSH key pair is to be bound to (in order to replace or reset the original key pair).
auth	No	**Auth** object	(Optional) Authentication type. This parameter is required for key pair replacement but not required for key pair reset.
disable_password	No	Boolean	• true: SSH login is disabled on the VM. - false: SSH login is enabled on the VM.
port	No	Long	SSH listening port.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1056 Auth

Parameter	Mandatory	Type	Description
type	No	String	The value can be **password** or **keypair**.
key	No	String	• If type is set to password, key indicates the password. • If type is set to keypair, key indicates the private key.

Response Parameters

Status code: 202

Table 4-1057 Response body parameters

Parameter	Type	Description
tasks	Array of **TaskResponseBody** objects	Bind key pairs in batches.

Table 4-1058 TaskResponseBody

Parameter	Type	Description
task_id	String	ID returned when a task is delivered
server_id	String	Specifies the ID of the bound VM.
status	String	Indicates the delivery status of a task. SUCCESS or FAILED.
error_code	String	Error code returned when a task fails to be delivered.
error_msg	String	Error information returned when a task fails to be delivered.

Status code: 400

Table 4-1059 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
error_msg	String	Description

Example Requests

```
{
  "batch_keypairs" : [ {
    "keypair_name" : "1",
    "server" : {
      "id" : "fxxx16e3-74b8-4025-9852-1f451932c20c",
      "disable_password" : false,
      "auth" : {
        "type" : "password",
        "key" : "password"
      }
    }
  }, {
    "keypair_name" : "1",
    "server" : {
      "id" : "4xxxxfc4-b4bf-49c2-b983-a1811c9760c1",
      "disable_password" : false,
      "auth" : {
        "type" : "password",
        "key" : "password"
      }
    }
  } ]
}
```

Example Responses

Status code: 202

Request succeeded.

```
{
  "tasks" : [ {
    "server_id" : "xxx",
    "task_id" : "xxx",
    "status" : "SUCCESS"
  }, {
    "server_id" : "xxx",
    "status" : "Failed",
    "error_code" : "xxxx",
    "error_msg" : "xxxx"
  } ]
}
```

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
202	Request succeeded.
400	Error response

Error Codes

See **Error Codes**.

4.2.2.4 Querying Task Information

Function

Queries the execution status of the current task based on the task ID returned by the SSH key pair API.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps::getTask	List	-	-	• kps:domainKeypairs:gettask	-

URI

GET /v3/{project_id}/tasks/{task_id}

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1060 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
task_id	Yes	String	The task ID.

Request Parameters

Table 4-1061 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

Table 4-1062 Response body parameters

Parameter	Type	Description
server_id	String	Tenant VM ID
task_id	String	ID returned when a task is successfully delivered

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
task_status	String	Key pair processing state. It can be: - READY_RESET: Preparing for resetting the key pair. - RUNNING_RESET: Resetting the key pair. - FAILED_RESET: Reset failed. - SUCCESS_RESET: Reset succeeded. - READY_REPLACE: Preparing for replacing the key pair. - RUNNING_REPLACE: Replacing the key pair. - FAILED_RESET: Replacement failed. - SUCCESS_RESET: Replacement succeeded. - READY_UNBIND: Preparing for unbinding the key pair. - RUNNING_UNBIND: Unbinding the key pair. - FAILED_UNBIND: Unbinding failed. - SUCCESS_UNBIND: Unbinding succeeded.

Status code: 400

Table 4-1063 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "task_id" : "aee8d2fe-5484-4753-9177-5a38dc15546c",
  "task_status" : "RUNNING_RESET",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
  "server_id" : "c9aa197b-a6b6-4c33-b3a6-fa0b4ec50006"
}
```

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	OK
400	Error response

Error Codes

See **Error Codes**.

4.2.2.5 Querying Running Tasks

Function

Queries running tasks.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps::getRunningTask	List	-	-	• kps:domainKeypairs:getrunningtask	-

URI

GET /v3/{project_id}/running-tasks

Table 4-1064 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-1065 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of items displayed per page. Default value: 1000
offset	No	Integer	Offset of the first displayed task that is being processed.

Request Parameters

Table 4-1066 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1067 Response body parameters

Parameter	Type	Description
total	Integer	Total number of running tasks.
tasks	Array of **RunningTasks** objects	List of running tasks.

Table 4-1068 RunningTasks

Parameter	Type	Description
task_id	String	VM ID.
operate_type	String	Operation type - FAILED_RESET: reset - FAILED_REPLACE: replace - FAILED_UNBIND: unbind
task_time	String	Task time
server_name	String	VM Name
server_id	String	VM ID.
keypair_name	String	Key pair name.

Status code: 400

Table 4-1069 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
 "tasks" : [ {
   "task_id" : "aee8d2fe-5484-4753-9177-5a38dc15546c",
   "operate_type" : "RUNNING_RESET",
   "task_time" : "1523342130000",
   "server_name" : "Test",
   "server_id" : "c9aa197b-a6b6-4c33-b3a6-fa0b4ec50006",
   "keypair_name" : "KeyPair-xt"
 } ]
}
```

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	OK
400	Error response

Error Codes

See **Error Codes**.

4.2.2.6 Querying Task Failure Information

Function

Queries information about failed tasks, such as binding and unbinding tasks.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps::getFailedTask	List	-	-	• kps:domainKeypairs:getfailtask	-

URI

GET /v3/{project_id}/failed-tasks

Table 4-1070 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 4-1071 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of items displayed per page. Default value: 1000
offset	No	Integer	Offset of the failed task information list.

Request Parameters

Table 4-1072 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1073 Response body parameters

Parameter	Type	Description
total	Integer	Total number of failed tasks.
tasks	Array of **FailedTasks** objects	List of failed tasks.

Table 4-1074 FailedTasks

Parameter	Type	Description
task_id	String	VM ID.
operate_type	String	Operation type of a task. It can be: - FAILED_RESET: reset - FAILED_REPLACE: replace - FAILED_UNBIND: unbind
task_time	String	Task time
task_error_code	String	Error code of a task failure
task_error_msg	String	Error code of a task failure
server_name	String	VM Name
server_id	String	VM ID.
keypair_name	String	Key pair name

Status code: 400

Table 4-1075 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

Example Requests

None

Example Responses

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

OK

```
{
  "total" : 1,
  "tasks" : [ {
    "task_id" : "aee8d2fe-5484-4753-9177-5a38dc15546c",
    "operate_type" : "RUNNING_RESET",
    "task_time" : "1523342130000",
    "task_error_code" : null,
    "task_error_msg" : "Update public key error",
    "server_name" : "Test",
    "server_id" : "c9aa197b-a6b6-4c33-b3a6-fa0b4ec50006",
    "keypair_name" : "KeyPair-xt"
  } ]
}
```

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	OK
400	Error response

Error Codes

See **Error Codes**.

4.2.2.7 Delete all failed tasks

Function

Deletes information about failed tasks.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps::deleteFailedTask	Write	-	-	• kps:domainKeypairs:deletefailtask • kps:domainKeypairs:deletefailtasks	-

URI

DELETE /v3/{project_id}/failed-tasks

Table 4-1076 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-1077 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

OK

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1078 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

Example Requests

None

Example Responses

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	OK
400	Error response

Error Codes

See **Error Codes**.

4.2.2.8 Delete a failed task

Function

Deletes failed tasks.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
kps::deleteFailedTask	Write	-	-	• kps:domainKeypairs:deletefailtask • kps:domainKeypairs:deletefailtasks	-

URI

DELETE /v3/{project_id}/failed-tasks/{task_id}

Table 4-1079 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
task_id	Yes	String	Task ID.

Request Parameters

Table 4-1080 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. Can be obtained by calling the IAM API for obtaining the user token (the value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

OK

Status code: 400

Table 4-1081 Response body parameters

Parameter	Type	Description
error_code	String	Error Codes
error_msg	String	Description

Example Requests

None

Example Responses

Status code: 400

Error response

```
{
  "error_code" : "KPS.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	OK
400	Error response

Error Codes

See **Error Codes**.

4.3 Secret Management APIs

4.3.1 Lifecycle Management

4.3.1.1 Importing Secrets in Batches

Function

This API is used to import secrets in batches.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/{project_id}/secrets/batch-import

Table 4-1082 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-1083 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.

Table 4-1084 Request body parameters

Parameter	Mandatory	Type	Description
secrets	Yes	Array of **CreateSecretRequestBody** objects	Parameter for creating secrets in batches.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1085 CreateSecretRequestBody

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the secret to be created Constraint: The value can contain 1 to 64 characters and must match the regular expression **^[a-zA-Z0-9._-]{1,64}$**.
kms_key_id	No	String	ID of the KMS master key used to encrypt the protection secret value. If you do not specify this parameter, the secret management service uses the default master key named csms/default by default to encrypt the secret value created by your account. If the KMS you specified does not exist under your account, it will be automatically created.
description	No	String	Description of a secret. Constraint: It can contain up to 2,048 bytes.
secret_binary	No	String	Plaintext of a binary secret encoded using Base64. CSMS encrypts the plaintext and stores it in the initial version of the secret. Type: Base64-encoded binary data object Constraints: Either **secret_binary** or **secret_string** must be configured. The maximum size is 32 KB.
secret_string	No	String	Plaintext of a text secret. CSMS encrypts the plaintext and stores it in the initial version of the secret. Constraint: Either **secret_binary** or **secret_string** must be configured. The maximum size is 32 KB.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
secret_type	No	String	Secret type • **COMMON**: shared secret (default), which is used to store sensitive information in an application system. • **RDS**: RDS secret, which is used to store RDS account information. (no longer supported, replaced by **RDS-FG**) • **RDS-FG**: RDS secret, which is used to store RDS account information. • **GaussDB-FG**: TaurusDB secret, which is used to store TaurusDB account information.
auto_rotation	No	Boolean	Automatic rotation The value can be true (enabled) or false (disabled). The default value is false.
rotation_period	No	String	Rotation period Constraints: 6 hours - 8,760 hours (365 days) Type: Integer[unit]. Integer indicates the time length. unit indicates the time unit, which can be d (day), h (hour), m (minute), or s (second). For example, 1d indicates one day, and 24h also indicates one day. Note: This parameter is mandatory when automatic rotation is enabled.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
rotation_config	No	String	Rotation configuration Constraints: The value can contain a maximum of 1,024 characters. This parameter is mandatory when **secret_type** is **RDS-FG** or **GaussDB-FG**. The parameter format is {"InstanceId":"","SecretSubType":""}. Description: **InstanceId** indicates the instance ID, and **SecretSubType** indicates the rotation subtype. The value can be **SingleUser** or **MultiUser**. **SingleUser**: Single-user rotation is used. A new password is created for the account for each rotation. **MultiUser**: Dual-user rotation is used. The users are labeled as **SYSCURRENT** and **SYSPREVIOUS**, respectively. During secret rotation, the password of the account who is labeled as **SYSPREVIOUS** is reset, and a random password is generated. Then, the labels are switched for the users.
event_subscriptions	No	Array of strings	List of events subscribed to by secrets. Currently, only one event can be subscribed to. When a basic event contained in an event is triggered, a notification message is sent to the notification topic corresponding to the event.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	This parameter is provided for enterprise users. If you are an enterprise user and have created an enterprise project, select the enterprise project to be bound to the key from the drop-down list. The default project is default. For users who have not enabled Enterprise Management, the Enterprise Project parameter is not displayed on the page and does not need to be configured.
rotation_func_urn	No	String	URN of the FunctionGraph function

Response Parameters

Status code: 200

Table 4-1086 Response body parameters

Parameter	Type	Description
error_list	Array of **ErrorInfo** objects	Failure description.
total	Integer	Total number of records.
success	Integer	Number of successful records.
failed	Integer	Number of failed records.

Table 4-1087 ErrorInfo

Parameter	Type	Description
name	String	Name.
error_msg	String	Failure cause.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1088 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error details.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.

Error Codes

See **Error Codes**.

4.3.1.2 Deleting Secrets in Batches

Function

This API is used to delete secrets in batches immediately. The operation cannot be undone.

Constraints

Secrets deleted in batches via this API cannot be restored.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/{project_id}/secrets/batch-delete

Table 4-1089 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-1090 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-1091 Request body parameters

Parameter	Mandatory	Type	Description
instance_id	No	String	ID of the Huawei Cloud service instance associated with the secret, for example, the RDS instance ID. The request will delete all secrets associated with the instance ID in batches. This operation cannot be undone.
instance_type	No	String	Type of the Huawei Cloud service, which can be RDS, TaurusDB, GaussDB, or APIG.

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1092 Response body parameters

Parameter	Type	Description
total	Integer	Number of secrets that meet the request parameter conditions.
success_secrets	Array of strings	Secrets that meet the request parameter conditions and are deleted.
failed_secrets	Array of **FailedDeletedSecrets** objects	Secrets that meet the request parameter conditions but fail to be deleted, and the failure cause.

Table 4-1093 FailedDeletedSecrets

Parameter	Type	Description
secret_name	String	Secret name.
error_msg	String	Cause of the secret deletion failure.

Status code: 400

Table 4-1094 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1095 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1096 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1097 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1098 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1099 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1100 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 3,
  "success_secrets" : [ "secretName1", "secretName2" ],
  "failed_secrets" : [ {
    "secret_name" : "secretName3",
    "error_msg" : "CSMS.0107: Secret is already in the **Pending deletion** state."
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal server error.
502	Failed to complete the request. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.1.3 Creating a Secret

Function

You can create a secret and store its value in its original version.

Secret values are encrypted and stored in secret versions. A version can have multiple statuses. Versions without any statuses are regarded as deprecated versions and can be automatically deleted by CSMS.

The initial version is marked by the **SYSCURRENT** status tag.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Constraints

You can specify a symmetric CMK to encrypt secrets. If the **kms_key_id** parameter is not specified, the default master key **csms/default** will be used to encrypt the secrets created under your account in a project. If the CMK you specified does not exist under your account, it will be automatically created.

You need the **kms:dek:create** permission of the specified CMK to encrypt secret values.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:create	Write	secretName *	• csms:Type • csms:KmsKeyId	-	kms:cmk:createDataKey
		-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v1/{project_id}/secrets

Table 4-1101 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1102 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1103 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the secret to be created Constraint: The value can contain 1 to 64 characters and must match the regular expression **^[a-zA-Z0-9._-]{1,64}$**.
kms_key_id	No	String	ID of the KMS master key used to encrypt the protection secret value. If you do not specify this parameter, the secret management service uses the default master key named csms/default by default to encrypt the secret value created by your account. If the KMS you specified does not exist under your account, it will be automatically created.
description	No	String	Description of a secret. Constraint: It can contain up to 2,048 bytes.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
secret_binary	No	String	Plaintext of a binary secret encoded using Base64. CSMS encrypts the plaintext and stores it in the initial version of the secret. Type: Base64-encoded binary data object Constraints: Either **secret_binary** or **secret_string** must be configured. The maximum size is 32 KB.
secret_string	No	String	Plaintext of a text secret. CSMS encrypts the plaintext and stores it in the initial version of the secret. Constraint: Either **secret_binary** or **secret_string** must be configured. The maximum size is 32 KB.
secret_type	No	String	Secret type • **COMMON**: shared secret (default), which is used to store sensitive information in an application system. • **RDS**: RDS secret, which is used to store RDS account information. (no longer supported, replaced by **RDS-FG**) • **RDS-FG**: RDS secret, which is used to store RDS account information. • **GaussDB-FG**: TaurusDB secret, which is used to store TaurusDB account information.
auto_rotation	No	Boolean	Automatic rotation The value can be true (enabled) or false (disabled). The default value is false.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
rotation_period	No	String	Rotation period Constraints: 6 hours - 8,760 hours (365 days) Type: Integer[unit]. Integer indicates the time length. unit indicates the time unit, which can be d (day), h (hour), m (minute), or s (second). For example, 1d indicates one day, and 24h also indicates one day. Note: This parameter is mandatory when automatic rotation is enabled.
rotation_config	No	String	Rotation configuration Constraints: The value can contain a maximum of 1,024 characters. This parameter is mandatory when **secret_type** is **RDS-FG** or **GaussDB-FG**. The parameter format is {"InstanceId":"","SecretSubType":""}. Description: **InstanceId** indicates the instance ID, and **SecretSubType** indicates the rotation subtype. The value can be **SingleUser** or **MultiUser**. **SingleUser**: Single-user rotation is used. A new password is created for the account for each rotation. **MultiUser**: Dual-user rotation is used. The users are labeled as **SYSCURRENT** and **SYSPREVIOUS**, respectively. During secret rotation, the password of the account who is labeled as **SYSPREVIOUS** is reset, and a random password is generated. Then, the labels are switched for the users.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
event_subscriptions	No	Array of strings	List of events subscribed to by secrets. Currently, only one event can be subscribed to. When a basic event contained in an event is triggered, a notification message is sent to the notification topic corresponding to the event.
enterprise_project_id	No	String	This parameter is provided for enterprise users. If you are an enterprise user and have created an enterprise project, select the enterprise project to be bound to the key from the drop-down list. The default project is default. For users who have not enabled Enterprise Management, the Enterprise Project parameter is not displayed on the page and does not need to be configured.
rotation_func_urn	No	String	URN of the FunctionGraph function

Response Parameters

Status code: 200

Table 4-1104 Response body parameters

Parameter	Type	Description
secret	**Secret** object	Secret object

Table 4-1105 Secret

Parameter	Type	Description
id	String	Resource identifier of a secret
name	String	Secret name

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
state	String	Secret status. Its value can be: **ENABLED** **DISABLED** **PENDING_DELETE** **FROZEN**
kms_key_id	String	ID of the KMS CMK used to encrypt a secret value.
description	String	Description of a secret
create_time	Long	Secret creation time. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
update_time	Long	Time when a secret was last updated. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
scheduled_delete_time	Long	Time when a secret is scheduled to be deleted. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time. If the secret is not in the deletion plan, the value of this parameter is null.
secret_type	String	Secret type • **COMMON**: shared secret (default), which is used to store sensitive information in an application system. • **RDS**: RDS secret, which is used to store RDS account information. (no longer supported, replaced by **RDS-FG**) • **RDS-FG**: RDS secret, which is used to store RDS account information. • **GaussDB-FG**: TaurusDB secret, which is used to store TaurusDB account information.
auto_rotation	Boolean	Automatic rotation The value can be true (enabled) or false (disabled). The default value is false.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
rotation_period	String	Rotation period Constraints: 6 hours - 8,760 hours (365 days) Type: Integer[unit]. Integer indicates the time length. unit indicates the time unit, which can be d (day), h (hour), m (minute), or s (second). For example, 1d indicates one day, and 24h also indicates one day. Note: This parameter is mandatory when automatic rotation is enabled.
rotation_config	String	Rotation configuration Constraints: The value can contain a maximum of 1,024 characters. If **secret_type** is set to **RDS-FG** or **GaussDB-FG**, set this parameter to **{"InstanceId":"","SecretSubType":""}**. Note: This parameter is mandatory when **secret_type** is set to **RDS-FG** or **GaussDB-FG**. **InstanceId** indicates the instance ID, and **SecretSubType** indicates the rotation subtype. The value can be **SingleUser** or **MultiUser**. **SingleUser**: Single-user rotation is used. A new password is created for the account for each rotation. **MultiUser**: Dual-user rotation is used. The users are labeled as **SYSCURRENT** and **SYSPREVIOUS**, respectively. During secret rotation, the password of the account who is labeled as **SYSPREVIOUS** is reset, and a random password is generated. Then, the labels are switched for the users.
rotation_time	Long	Rotation timestamp
next_rotation_time	Long	Next rotation timestamp
event_subscriptions	Array of strings	List of events subscribed to by secrets. Currently, only one event can be subscribed to. When a basic event contained in an event is triggered, a notification message is sent to the notification topic corresponding to the event.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
enterprise_project_id	String	Enterprise project ID
rotation_func_urn	String	URN of the FunctionGraph function

Status code: 400

Table 4-1106 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1107 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1108 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1109 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-1110 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1111 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1112 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

Create a secret named demo and use KMS key ID 0d0466b0-e727-4d9c-b35d-f84bb474a37f to encrypt the value of this is a demo secret string.

```
{
  "name" : "demo",
  "kms_key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "secret_string" : "this is a demo secret string"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "secret" : {
    "id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "name" : "test",
    "state" : "ENABLED",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
  "kms_key_id" : "b168fe00ff56492495a7d22974df2d0b",
  "description" : "description",
  "create_time" : 1581507580000,
  "update_time" : 1581507580000,
  "scheduled_delete_time" : 1581507580000,
  "secret_type" : "RDS-FG",
  "auto_rotation" : true,
  "rotation_config" : "{'InstanceId':'63616bceef2c45409575d762a498318bin01','SecretSubType':'MultiUser'}",
  "rotation_period" : "1d",
  "rotation_time" : 1668567940000,
  "next_rotation_time" : 1668629140000,
  "event_subscriptions" : [ "pocEvent" ],
  "rotation_func_urn" : "urn:fss:{region}:46b6f338fc3445b8846c71dfb1fbxxxx:function:default:test2-0:latest"
 }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.1.4 Querying the Secret List

Function

This API is used to query all secrets created by the current user in the current project.

Constraints

The information returned by this API is secret metadata, which does not contain secret values.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:list	List	secretName *	g:EnterpriseProjectId	-	-

URI

GET /v1/{project_id}/secrets

Table 4-1113 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-1114 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	String	Specifies the number of records on each page. Default value: 50
marker	No	String	Start secret name of pagination query. If this parameter is left blank, only the first page is queried.
event_name	No	String	When an event name is specified, only the secrets associated with the event are returned.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1115 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1116 Response body parameters

Parameter	Type	Description
secrets	Array of **Secret** objects	Secret details list
page_info	**PageInfo** object	Pagination information.

Table 4-1117 Secret

Parameter	Type	Description
id	String	Resource identifier of a secret
name	String	Secret name
state	String	Secret status. Its value can be: **ENABLED** **DISABLED** **PENDING_DELETE** **FROZEN**
kms_key_id	String	ID of the KMS CMK used to encrypt a secret value.
description	String	Description of a secret
create_time	Long	Secret creation time. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
update_time	Long	Time when a secret was last updated. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
scheduled_delete_time	Long	Time when a secret is scheduled to be deleted. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time. If the secret is not in the deletion plan, the value of this parameter is null.
secret_type	String	Secret type • **COMMON**: shared secret (default), which is used to store sensitive information in an application system. • **RDS**: RDS secret, which is used to store RDS account information. (no longer supported, replaced by **RDS-FG**) • **RDS-FG**: RDS secret, which is used to store RDS account information. • **GaussDB-FG**: TaurusDB secret, which is used to store TaurusDB account information.
auto_rotation	Boolean	Automatic rotation The value can be true (enabled) or false (disabled). The default value is false.
rotation_period	String	Rotation period Constraints: 6 hours - 8,760 hours (365 days) Type: Integer[unit]. Integer indicates the time length. unit indicates the time unit, which can be d (day), h (hour), m (minute), or s (second). For example, 1d indicates one day, and 24h also indicates one day. Note: This parameter is mandatory when automatic rotation is enabled.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
rotation_config	String	Rotation configuration Constraints: The value can contain a maximum of 1,024 characters. If **secret_type** is set to **RDS-FG** or **GaussDB-FG**, set this parameter to **{"InstanceId":"","SecretSubType":""}**. Note: This parameter is mandatory when **secret_type** is set to **RDS-FG** or **GaussDB-FG**. **InstanceId** indicates the instance ID, and **SecretSubType** indicates the rotation subtype. The value can be **SingleUser** or **MultiUser**. **SingleUser**: Single-user rotation is used. A new password is created for the account for each rotation. **MultiUser**: Dual-user rotation is used. The users are labeled as **SYSCURRENT** and **SYSPREVIOUS**, respectively. During secret rotation, the password of the account who is labeled as **SYSPREVIOUS** is reset, and a random password is generated. Then, the labels are switched for the users.
rotation_time	Long	Rotation timestamp
next_rotation_time	Long	Next rotation timestamp
event_subscriptions	Array of strings	List of events subscribed to by secrets. Currently, only one event can be subscribed to. When a basic event contained in an event is triggered, a notification message is sent to the notification topic corresponding to the event.
enterprise_project_id	String	Enterprise project ID
rotation_func_urn	String	URN of the FunctionGraph function

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1118 PageInfo

Parameter	Type	Description
next_marker	String	Query address of the next page (name of the secret at the end of the current page, name of the secret at the start of the next page).
previous_marker	String	Name of the start secret on the current page and name of the end secret on the previous page.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-1119 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1120 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1121 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1122 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1123 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1124 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1125 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "secrets" : [ {
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "name" : "secret-name-test",
    "state" : "ENABLED",
    "kms_key_id" : "b168fe00ff56492495a7d22974df2d0b",
    "description" : "description",
    "create_time" : 1581507580000,
    "update_time" : 1581507580000,
    "scheduled_delete_time" : 1581507580000,
    "secret_type" : "RDS-FG",
    "auto_rotation" : true,
    "rotation_config" : "{'InstanceId':'indstance id','SecretSubType':'MultiUser'}",
    "rotation_period" : "1d",
    "rotation_time" : 1668567940000,
    "next_rotation_time" : 1668629140000,
    "event_subscriptions" : [ "pocEvent" ]
  } ],
  "page_info" : {
    "next_marker" : "secret-name-test",
    "previous_marker" : "secret-name-test",
    "current_count" : 1
  }
}
```


Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.1.5 Querying a Secret

Function

This API is used to query information about a specified secret.

Constraints

The information returned by this API is secret metadata, which does not contain secret values.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:get	Read	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

URI

GET /v1/{project_id}/secrets/{secret_name}

Table 4-1126 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1127 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1128 Response body parameters

Parameter	Type	Description
secret	**Secret** object	Secret object

Table 4-1129 Secret

Parameter	Type	Description
id	String	Resource identifier of a secret
name	String	Secret name
state	String	Secret status. Its value can be: **ENABLED** **DISABLED** **PENDING_DELETE** **FROZEN**
kms_key_id	String	ID of the KMS CMK used to encrypt a secret value.
description	String	Description of a secret
create_time	Long	Secret creation time. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
update_time	Long	Time when a secret was last updated. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
scheduled_delete_time	Long	Time when a secret is scheduled to be deleted. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time. If the secret is not in the deletion plan, the value of this parameter is null.
secret_type	String	Secret type • **COMMON**: shared secret (default), which is used to store sensitive information in an application system. • **RDS**: RDS secret, which is used to store RDS account information. (no longer supported, replaced by **RDS-FG**) • **RDS-FG**: RDS secret, which is used to store RDS account information. • **GaussDB-FG**: TaurusDB secret, which is used to store TaurusDB account information.
auto_rotation	Boolean	Automatic rotation The value can be true (enabled) or false (disabled). The default value is false.
rotation_period	String	Rotation period Constraints: 6 hours - 8,760 hours (365 days) Type: Integer[unit]. Integer indicates the time length. unit indicates the time unit, which can be d (day), h (hour), m (minute), or s (second). For example, 1d indicates one day, and 24h also indicates one day. Note: This parameter is mandatory when automatic rotation is enabled.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
rotation_config	String	Rotation configuration Constraints: The value can contain a maximum of 1,024 characters. If **secret_type** is set to **RDS-FG** or **GaussDB-FG**, set this parameter to **{"InstanceId":"","SecretSubType":""}**. Note: This parameter is mandatory when **secret_type** is set to **RDS-FG** or **GaussDB-FG**. **InstanceId** indicates the instance ID, and **SecretSubType** indicates the rotation subtype. The value can be **SingleUser** or **MultiUser**. **SingleUser**: Single-user rotation is used. A new password is created for the account for each rotation. **MultiUser**: Dual-user rotation is used. The users are labeled as **SYSCURRENT** and **SYSPREVIOUS**, respectively. During secret rotation, the password of the account who is labeled as **SYSPREVIOUS** is reset, and a random password is generated. Then, the labels are switched for the users.
rotation_time	Long	Rotation timestamp
next_rotation_time	Long	Next rotation timestamp
event_subscriptions	Array of strings	List of events subscribed to by secrets. Currently, only one event can be subscribed to. When a basic event contained in an event is triggered, a notification message is sent to the notification topic corresponding to the event.
enterprise_project_id	String	Enterprise project ID
rotation_func_urn	String	URN of the FunctionGraph function

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1130 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1131 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1132 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1133 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1134 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-1135 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1136 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "secret" : {
    "id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "name" : "test",
    "state" : "ENABLED",
    "kms_key_id" : "b168fe00ff56492495a7d22974df2d0b",
    "description" : "description",
    "create_time" : 1581507580000,
    "update_time" : 1581507580000,
    "scheduled_delete_time" : 1581507580000,
    "secret_type" : "RDS-FG",
    "auto_rotation" : true,
    "rotation_config" : "{'InstanceId':'63616bceef2c45409575d762a498318bin01','SecretSubType':'MultiUser'}",
    "rotation_period" : "1d",
    "rotation_time" : 1668567940000,
    "next_rotation_time" : 1668629140000,
    "event_subscriptions" : [ "pocEvent" ],
    "rotation_func_urn" : "urn:fss:{region}:46b6f338fc3445b8846c71dfb1fbxxxx:function:default:test2-0:latest"
  }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.1.6 Updating a Secret

Function

Updates the metadata of a specified secret.

Constraints

This API can only be used to modify secret metadata. It cannot modify the secret value.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:update	Write	secretName *	• csms:Type • csms:KmsKeyId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

URI

PUT /v1/{project_id}/secrets/{secret_name}

Table 4-1137 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name

Request Parameters

Table 4-1138 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1139 Request body parameters

Parameter	Mandatory	Type	Description
kms_key_id	No	String	ID of the KMS CMK used to encrypt a secret value. If the CMK of a secret is updated, only the secret versions created after the update will be encrypted using the new CMK. The secret versions earlier than the update are still decrypted using the old CMK ID.
description	No	String	Description of a secret. Constraint: It can contain up to 2,048 bytes.
auto_rotation	No	Boolean	Automatic rotation The value can be true (enabled) or false (disabled).
rotation_period	No	String	Rotation period Constraints: 6 hours - 8,760 hours (365 days) Type: Integer[unit]. Integer indicates the time length. unit indicates the time unit, which can be d (day), h (hour), m (minute), or s (second). For example, 1d indicates one day, and 24h also indicates one day. Note: This parameter is mandatory when automatic rotation is enabled.
event_subscriptions	No	Array of strings	List of events subscribed to by secrets. Currently, only one event can be subscribed to. When a basic event contained in an event is triggered, a notification message is sent to the notification topic corresponding to the event.
rotation_func_urn	No	String	URN of the FunctionGraph function

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 200

Table 4-1140 Response body parameters

Parameter	Type	Description
secret	**Secret** object	Secret object

Table 4-1141 Secret

Parameter	Type	Description
id	String	Resource identifier of a secret
name	String	Secret name
state	String	Secret status. Its value can be: **ENABLED** **DISABLED** **PENDING_DELETE** **FROZEN**
kms_key_id	String	ID of the KMS CMK used to encrypt a secret value.
description	String	Description of a secret
create_time	Long	Secret creation time. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
update_time	Long	Time when a secret was last updated. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
scheduled_delete_time	Long	Time when a secret is scheduled to be deleted. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time. If the secret is not in the deletion plan, the value of this parameter is null.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
secret_type	String	Secret type • **COMMON**: shared secret (default), which is used to store sensitive information in an application system. • **RDS**: RDS secret, which is used to store RDS account information. (no longer supported, replaced by **RDS-FG**) • **RDS-FG**: RDS secret, which is used to store RDS account information. • **GaussDB-FG**: TaurusDB secret, which is used to store TaurusDB account information.
auto_rotation	Boolean	Automatic rotation The value can be true (enabled) or false (disabled). The default value is false.
rotation_period	String	Rotation period Constraints: 6 hours - 8,760 hours (365 days) Type: Integer[unit]. Integer indicates the time length. unit indicates the time unit, which can be d (day), h (hour), m (minute), or s (second). For example, 1d indicates one day, and 24h also indicates one day. Note: This parameter is mandatory when automatic rotation is enabled.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
rotation_config	String	Rotation configuration Constraints: The value can contain a maximum of 1,024 characters. If **secret_type** is set to **RDS-FG** or **GaussDB-FG**, set this parameter to **{"InstanceId":"","SecretSubType":""}**. Note: This parameter is mandatory when **secret_type** is set to **RDS-FG** or **GaussDB-FG**. **InstanceId** indicates the instance ID, and **SecretSubType** indicates the rotation subtype. The value can be **SingleUser** or **MultiUser**. **SingleUser**: Single-user rotation is used. A new password is created for the account for each rotation. **MultiUser**: Dual-user rotation is used. The users are labeled as **SYSCURRENT** and **SYSPREVIOUS**, respectively. During secret rotation, the password of the account who is labeled as **SYSPREVIOUS** is reset, and a random password is generated. Then, the labels are switched for the users.
rotation_time	Long	Rotation timestamp
next_rotation_time	Long	Next rotation timestamp
event_subscriptions	Array of strings	List of events subscribed to by secrets. Currently, only one event can be subscribed to. When a basic event contained in an event is triggered, a notification message is sent to the notification topic corresponding to the event.
enterprise_project_id	String	Enterprise project ID
rotation_func_urn	String	URN of the FunctionGraph function

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1142 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1143 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1144 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1145 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1146 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-1147 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1148 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

Updating the secret KMS key ID to **test** and description to **update description**

```
{
  "kms_key_id" : "test",
  "description" : "update description",
  "event_subscriptions" : [ "pocEvent2" ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "secret" : {
    "id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "name" : "test",
    "state" : "ENABLED",
    "kms_key_id" : "b168fe00ff56492495a7d22974df2d0b",
    "description" : "description",
    "create_time" : 1581507580000,
    "update_time" : 1581507580000,
    "scheduled_delete_time" : 1581507580000,
    "secret_type" : "RDS-FG",
    "auto_rotation" : true,
    "rotation_config" : "{'InstanceId':'indstance id','SecretSubType':'MultiUser'}",
    "rotation_period" : "1d",
    "rotation_time" : 1668567940000,
    "next_rotation_time" : 1668629140000,
    "event_subscriptions" : [ "pocEvent" ],
    "rotation_func_urn" : "urn:fss:{region}:46b6f338fc3445b8846c71dfb1fbxxxx:function:default:test2-0:latest"
  }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.1.7 Deleting a Secret Immediately

Function

The specified secret is deleted immediately and cannot be restored.

Constraints

Secrets deleted via this API cannot be restored.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:delete	Write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	-

URI

DELETE /v1/{project_id}/secrets/{secret_name}

Table 4-1149 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name

Request Parameters

Table 4-1150 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Request succeeded.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1151 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1152 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1153 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1154 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1155 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-1156 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1157 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Error Codes

See **Error Codes**.

4.3.1.8 Restoring a Secret Object

Function

Restore the secret object by uploading the secret backup file.

Constraints

The information returned by this API is secret metadata, which does not contain secret values.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:create	Write	secretName *	• csms:Type • csms:KmsKeyId	-	kms:cmk:decryptDataKey
		-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v1/{project_id}/secrets/restore

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1158 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-1159 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1160 Request body parameters

Parameter	Mandatory	Type	Description
secret_blob	Yes	String	Secret backup file obtained after a specified secret object is backed up. The backup file contains all secret version information. The backup file is encrypted and encoded and cannot be directly read.

Response Parameters

Status code: 200

Table 4-1161 Response body parameters

Parameter	Type	Description
secret	**Secret** object	Secret object

Table 4-1162 Secret

Parameter	Type	Description
id	String	Resource identifier of a secret

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
name	String	Secret name
state	String	Secret status. Its value can be: **ENABLED** **DISABLED** **PENDING_DELETE** **FROZEN**
kms_key_id	String	ID of the KMS CMK used to encrypt a secret value.
description	String	Description of a secret
create_time	Long	Secret creation time. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
update_time	Long	Time when a secret was last updated. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
scheduled_delete_time	Long	Time when a secret is scheduled to be deleted. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time. If the secret is not in the deletion plan, the value of this parameter is null.
secret_type	String	Secret type • **COMMON**: shared secret (default), which is used to store sensitive information in an application system. • **RDS**: RDS secret, which is used to store RDS account information. (no longer supported, replaced by **RDS-FG**) • **RDS-FG**: RDS secret, which is used to store RDS account information. • **GaussDB-FG**: TaurusDB secret, which is used to store TaurusDB account information.
auto_rotation	Boolean	Automatic rotation The value can be true (enabled) or false (disabled). The default value is false.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
rotation_period	String	Rotation period Constraints: 6 hours - 8,760 hours (365 days) Type: Integer[unit]. Integer indicates the time length. unit indicates the time unit, which can be d (day), h (hour), m (minute), or s (second). For example, 1d indicates one day, and 24h also indicates one day. Note: This parameter is mandatory when automatic rotation is enabled.
rotation_config	String	Rotation configuration Constraints: The value can contain a maximum of 1,024 characters. If **secret_type** is set to **RDS-FG** or **GaussDB-FG**, set this parameter to **{"InstanceId":"","SecretSubType":""}**. Note: This parameter is mandatory when **secret_type** is set to **RDS-FG** or **GaussDB-FG**. **InstanceId** indicates the instance ID, and **SecretSubType** indicates the rotation subtype. The value can be **SingleUser** or **MultiUser**. **SingleUser**: Single-user rotation is used. A new password is created for the account for each rotation. **MultiUser**: Dual-user rotation is used. The users are labeled as **SYSCURRENT** and **SYSPREVIOUS**, respectively. During secret rotation, the password of the account who is labeled as **SYSPREVIOUS** is reset, and a random password is generated. Then, the labels are switched for the users.
rotation_time	Long	Rotation timestamp
next_rotation_time	Long	Next rotation timestamp
event_subscriptions	Array of strings	List of events subscribed to by secrets. Currently, only one event can be subscribed to. When a basic event contained in an event is triggered, a notification message is sent to the notification topic corresponding to the event.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
enterprise_project_id	String	Enterprise project ID
rotation_func_urn	String	URN of the FunctionGraph function

Status code: 400

Table 4-1163 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1164 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1165 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1166 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-1167 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1168 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1169 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

Upload the secret backup file.

```
{
  "secret_blob" :
")CloudSecretManagementBackupV1.comeyJraWQiOiI5ZjNlZmRjNS0zZjVlLTRiZWQtYThkMS05NjE2ZTUwNDQzYWIiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiUlNBLU9BRVAtMjU2In0.CtrOcFMSeW_qMdQjgKzNaWtC6hkSTdjOSMSr2IOKNa8OpbJH8rOaCt9l4LYLHKw8CF70YLWOODgaYrLiWuHgdR-O9hlALkT6CbXxJ-Cbmf6qpJF61kXKHX4TBe6-oV8t4PaPaSDDR_oeyt4Xl2EOOlHxs9PnU1st9Fkd7wOHNa4ueM16Ze5ICEdQK3cN1hnelid0zlb1qq58KhsSroNeI8B5RnoYDB-0eiFWD0XWJLppgkLnewXpuPLmLN_c558yUQ0u0VoUyBGB6EFePPbbT-Z1_LUCSRyiP9Y2S0Vz5jzzeabWZ4vZkW8JX57Wc-onHplUpsUUpIqcdHLjp40NEQ.VtA6Sg--jeA1QavYxY9z7Q.Mr6dLyontoJCaDaRFMAYg_qUdEPzd-aIIrCHWH7wvYayNpSFUjR5QJd3XPpGGy93y22jN-DoHZHclgMeureQwKq39QQF0xIdRqhOR2Lxy69PkgRaNtpz7ikLOlsbjh1wd7mbSmyolsK_0t1X9OlvOSmUMjxUXpXLzqLXxPY0R_MUxEanHb3V_vsLArF9sN1X7Km-fdUKXTV1EzVUq1eC5aSYqg3rGkLHPHG6lPXOetPWNsVCE1bX0Voh0XnlyFLSSoYzX45l04hR8JXgcP42FXfD7GugcNi7jTKuvxu4l2Q2v7wnk"
}
```

Example Responses

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request succeeded.

```
{
  "secret" : {
    "id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "name" : "test",
    "state" : "ENABLED",
    "kms_key_id" : "b168fe00ff56492495a7d22974df2d0b",
    "description" : "description",
    "create_time" : 1581507580000,
    "update_time" : 1581507580000,
    "scheduled_delete_time" : 1581507580000
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.1.9 Downloading Secret Backup

Function

Download the backup file of a specified secret.

Constraints

This API returns a string indicating the secret backup file. The content is encrypted and cannot be read.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:get	Read	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	• kms:cmk:createDataKey • kms:cmk:decryptDataKey • kms:cmk:list

URI

POST /v1/{project_id}/secrets/{secret_name}/backup

Table 4-1170 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name

Request Parameters

Table 4-1171 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 200

Table 4-1172 Response body parameters

Parameter	Type	Description
secret_blob	String	Secret backup file contains all secret version information. The backup file is encrypted and encoded and cannot be directly read.

Status code: 400

Table 4-1173 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1174 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1175 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1176 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1177 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1178 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1179 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "secret_blob" :
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

")CloudSecretManagementBackupV1.comeyJraWQiOiI5ZjNlZmRjNS0zZjVlLTRiZWQtYThkMS05NjE2ZTUwNDQzYWIiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiUlNBLU9BRVAtMjU2In0.CtrOcFMSeW_qMdQjgKzNaWtC6hkSTdjOSMSr2IOKNa8OpbJH8rOaCt9l4LYLHKw8CF70YLWOODgaYrLiWuHgdR-O9hlALkT6CbXxJ-Cbmf6qpJF61kXKHX4TBe6-oV8t4PaPaSDDR_oeyt4Xl2EOOlHxs9PnU1st9Fkd7wOHNa4ueM16Ze5ICEdQK3cN1hnelid0zlb1qq58KhsSroNeI8B5RnoYDB-0eiFWD0XWJLppgkLnewXpuPLmLN_c558yUQ0u0VoUyBGB6EFePPbbT-Z1_LUCSRyiP9Y2S0Vz5jzzeabWZ4vZkW8JX57Wc-onHplUpsUUpIqcdHLjp40NEQ.VtA6Sg--jeA1QavYxY9z7Q.Mr6dLyontoJCaDaRFMAYg_qUdEPzd-aIIrCHWH7wvYayNpSFUjR5QJd3XPpGGy93y22jN-DoHZHclgMeureQwKq39QQF0xIdRqhOR2Lxy69PkgRaNtpz7ikLOlsbjh1wd7mbSmyolsK_0t1X9OlvOSmUMjxUXpXLzqLXxPY0R_MUxEanHb3V_vsLArF9sN1X7Km-fdUKXTV1EzVUq1eC5aSYqg3rGkLHPHG6lPXOetPWNsVCE1bX0Voh0XnlyFLSSoYzX45l04hR8JXgcP42FXfD7GugcNi7jTKuvxu4l2Q2v7wnk"
}

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.1.10 Creating a Scheduled Secret Deletion Task

Function

Specify the deletion delay time and create a scheduled task for deleting secrets. You can set the deletion delay time to 7 to 30 days.

Constraints

For a secret in the **Scheduled deletion** state, its metadata cannot be updated and its secret cannot be checked.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:scheduleDeletion	Write	secretName *	• csms:Type • csms:RecoveryWindowInDays • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secret:deleteScheduled	-

URI

POST /v1/{project_id}/secrets/{secret_name}/scheduled-deleted-tasks/create

Table 4-1180 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1181 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1182 Request body parameters

Parameter	Mandatory	Type	Description
recovery_window_in_days	Yes	Integer	Delay in deleting a secret in a scheduled task. Constraint: The value range is 7 to 30 days. Default value: 30

Response Parameters

Status code: 200

Table 4-1183 Response body parameters

Parameter	Type	Description
secret	**Secret** object	Secret object

Table 4-1184 Secret

Parameter	Type	Description
id	String	Resource identifier of a secret
name	String	Secret name
state	String	Secret status. Its value can be: **ENABLED** **DISABLED** **PENDING_DELETE** **FROZEN**

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
kms_key_id	String	ID of the KMS CMK used to encrypt a secret value.
description	String	Description of a secret
create_time	Long	Secret creation time. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
update_time	Long	Time when a secret was last updated. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
scheduled_delete_time	Long	Time when a secret is scheduled to be deleted. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time. If the secret is not in the deletion plan, the value of this parameter is null.
secret_type	String	Secret type • **COMMON**: shared secret (default), which is used to store sensitive information in an application system. • **RDS**: RDS secret, which is used to store RDS account information. (no longer supported, replaced by **RDS-FG**) • **RDS-FG**: RDS secret, which is used to store RDS account information. • **GaussDB-FG**: TaurusDB secret, which is used to store TaurusDB account information.
auto_rotation	Boolean	Automatic rotation The value can be true (enabled) or false (disabled). The default value is false.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
rotation_period	String	Rotation period Constraints: 6 hours - 8,760 hours (365 days) Type: Integer[unit]. Integer indicates the time length. unit indicates the time unit, which can be d (day), h (hour), m (minute), or s (second). For example, 1d indicates one day, and 24h also indicates one day. Note: This parameter is mandatory when automatic rotation is enabled.
rotation_config	String	Rotation configuration Constraints: The value can contain a maximum of 1,024 characters. If **secret_type** is set to **RDS-FG** or **GaussDB-FG**, set this parameter to **{"InstanceId":"","SecretSubType":""}**. Note: This parameter is mandatory when **secret_type** is set to **RDS-FG** or **GaussDB-FG**. **InstanceId** indicates the instance ID, and **SecretSubType** indicates the rotation subtype. The value can be **SingleUser** or **MultiUser**. **SingleUser**: Single-user rotation is used. A new password is created for the account for each rotation. **MultiUser**: Dual-user rotation is used. The users are labeled as **SYSCURRENT** and **SYSPREVIOUS**, respectively. During secret rotation, the password of the account who is labeled as **SYSPREVIOUS** is reset, and a random password is generated. Then, the labels are switched for the users.
rotation_time	Long	Rotation timestamp
next_rotation_time	Long	Next rotation timestamp
event_subscriptions	Array of strings	List of events subscribed to by secrets. Currently, only one event can be subscribed to. When a basic event contained in an event is triggered, a notification message is sent to the notification topic corresponding to the event.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
enterprise_project_id	String	Enterprise project ID
rotation_func_urn	String	URN of the FunctionGraph function

Status code: 400

Table 4-1185 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1186 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1187 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1188 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-1189 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1190 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1191 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

Create a scheduled secret deletion task and delete the secret 15 days later.

```
{
  "recovery_window_in_days" : 15
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "secret" : {
    "id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "name" : "test",
    "state" : "ENABLED",
    "kms_key_id" : "b168fe00ff56492495a7d22974df2d0b",
    "description" : "description",
    "create_time" : 1581507580000,
    "update_time" : 1581507580000,
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "scheduled_delete_time" : 1581507580000
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.1.11 Canceling a Scheduled Secret Deletion Task

Function

The scheduled secret deletion task is canceled, and the secret object is restored to the available state.

Constraints

This API can only be called to delete secrets in the **Scheduled deletion** state.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:restoreSecret	Write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secret:deleteCancelled	-

URI

POST /v1/{project_id}/secrets/{secret_name}/scheduled-deleted-tasks/cancel

Table 4-1192 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name

Request Parameters

Table 4-1193 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1194 Response body parameters

Parameter	Type	Description
secret	Secret object	Secret object

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1195 Secret

Parameter	Type	Description
id	String	Resource identifier of a secret
name	String	Secret name
state	String	Secret status. Its value can be: **ENABLED** **DISABLED** **PENDING_DELETE** **FROZEN**
kms_key_id	String	ID of the KMS CMK used to encrypt a secret value.
description	String	Description of a secret
create_time	Long	Secret creation time. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
update_time	Long	Time when a secret was last updated. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
scheduled_delete_time	Long	Time when a secret is scheduled to be deleted. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time. If the secret is not in the deletion plan, the value of this parameter is null.
secret_type	String	Secret type • **COMMON**: shared secret (default), which is used to store sensitive information in an application system. • **RDS**: RDS secret, which is used to store RDS account information. (no longer supported, replaced by **RDS-FG**) • **RDS-FG**: RDS secret, which is used to store RDS account information. • **GaussDB-FG**: TaurusDB secret, which is used to store TaurusDB account information.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
auto_rotation	Boolean	Automatic rotation The value can be true (enabled) or false (disabled). The default value is false.
rotation_period	String	Rotation period Constraints: 6 hours - 8,760 hours (365 days) Type: Integer[unit]. Integer indicates the time length. unit indicates the time unit, which can be d (day), h (hour), m (minute), or s (second). For example, 1d indicates one day, and 24h also indicates one day. Note: This parameter is mandatory when automatic rotation is enabled.
rotation_config	String	Rotation configuration Constraints: The value can contain a maximum of 1,024 characters. If **secret_type** is set to **RDS-FG** or **GaussDB-FG**, set this parameter to **{"InstanceId":"","SecretSubType":""}**. Note: This parameter is mandatory when **secret_type** is set to **RDS-FG** or **GaussDB-FG**. **InstanceId** indicates the instance ID, and **SecretSubType** indicates the rotation subtype. The value can be **SingleUser** or **MultiUser**. **SingleUser**: Single-user rotation is used. A new password is created for the account for each rotation. **MultiUser**: Dual-user rotation is used. The users are labeled as **SYSCURRENT** and **SYSPREVIOUS**, respectively. During secret rotation, the password of the account who is labeled as **SYSPREVIOUS** is reset, and a random password is generated. Then, the labels are switched for the users.
rotation_time	Long	Rotation timestamp
next_rotation_time	Long	Next rotation timestamp

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
event_subscriptions	Array of strings	List of events subscribed to by secrets. Currently, only one event can be subscribed to. When a basic event contained in an event is triggered, a notification message is sent to the notification topic corresponding to the event.
enterprise_project_id	String	Enterprise project ID
rotation_func_urn	String	URN of the FunctionGraph function

Status code: 400

Table 4-1196 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1197 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1198 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1199 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1200 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1201 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1202 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "secret" : {
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "name" : "test",
    "state" : "ENABLED",
    "kms_key_id" : "b168fe00ff56492495a7d22974df2d0b",
    "description" : "description",
    "create_time" : 1581507580000,
    "update_time" : 1581507580000,
    "scheduled_delete_time" : 1581507580000
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.1.12 Rotating a Secret

Function

Executes rotation secrets immediately. Creates a new secret version in the specified secret to encrypt and store secret values randomly generated in the background. At the same time, the newly created secret version is marked as SYSCURRENT.

Constraints

The RotateSecret API does not support rotation of common secrets.

A user account has the following rights:

Change the RDS database password

Query key details

Query the key list

Create a DEK

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Decrypt the DEK

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:rotate	Write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-	• rds:password:update • kms:cmk:createGrant • kms:cmk:retireGrant

URI

POST /v1/{project_id}/secrets/{secret_name}/rotate

Table 4-1203 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1204 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1205 Response body parameters

Parameter	Type	Description
version_id	String	Version identifier of a secret.
secret_name	String	Secret name.
rotation_task_id	String	ID of the secret rotation task

Status code: 400

Table 4-1206 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1207 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1208 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1209 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

Table 4-1210 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1211 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 404

Table 4-1212 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1213 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1214 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1215 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 502

Table 4-1216 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1217 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-1218 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1219 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "rotation_task_id" : "a71a4b47-6cac-4f11-92c1-21a165bb6401"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Error Codes

See **Error Codes**.

4.3.2 Secret Version Management

4.3.2.1 Creating a Secret Version

Function

Creates a new secret version in the specified secret to encrypt and keep the new secret value. By default, The latest secret version in **SYSCURRENT** state. The previous version is in the **SYSPREVIOUS** state. You can overwrite the default behavior by specifying the **VersionStage** parameter.

Constraints

- On the CSMS console, only the **secret_string** field can be configured. To add binary secrets to the **secret_binary** field, use an SDK or API.
- A secret can have up to 20 versions.
- You can only add versions to enabled secrets.
- Secret versions are numbered v1, v2, v3, and so on based on their creation time.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:createVersion	Write	secretName *	• csms:TypeTag • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretVersion:create	kms:cmk:createDataKey

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

URI

POST /v1/{project_id}/secrets/{secret_name}/versions

Table 4-1220 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name

Request Parameters

Table 4-1221 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1222 Request body parameters

Parameter	Mandatory	Type	Description
secret_binary	No	String	Value of a new secret. The value is encrypted and stored in the initial version of the secret. Type: Base64-encoded binary data object Constraint: Either **secret_binary** or **secret_string** must be configured. The maximum size is 32 KB.
secret_string	No	String	Value of a new secret. The value is encrypted and stored in the initial version of the secret. Constraint: Either **secret_binary** or **secret_string** must be configured. The maximum size is 32 KB.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
version_stages	No	Array of strings	Version status added to a secret version when the version is stored. If you do not specify this parameter, secret manager defaults to SYSCURRENT for the new version. Constraint: The array can contain up to 12 elements. The stage length can be up to 64 bytes.
expire_time	No	Long	Expiration time of the secret version. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the current time. Value based on which the validity period is determined when the secret subscribes to the version expiration event type. This parameter is left blank by default.

Response Parameters

Status code: 200

Table 4-1223 Response body parameters

Parameter	Type	Description
version_metadata	**VersionMetadata** object	Status of a secret version.

Table 4-1224 VersionMetadata

Parameter	Type	Description
id	String	Secret version ID, which is unique under a secret object.
create_time	Long	Time when a secret version was created. The timestamp indicates the total seconds since January 1, 1970.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
expire_time	Long	Expiration time of the secret version. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time. When the secret subscribes to the version expiration event type, the validity period is determined based on this parameter. This parameter is left blank by default.
kms_key_id	String	ID of the KMS CMK used to encrypt a secret version value.
secret_name	String	Secret name
version_stages	Array of strings	Secret version status list. Each status tag is unique for a secret version. If a status tag in use is added to a new version, the tag will be automatically removed from the original version. If **version_stage** is not specified, the temporary tag **SYSCURRENT** will be added to this version.

Status code: 400

Table 4-1225 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1226 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1227 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1228 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1229 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1230 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1231 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

Create a secret version. The secret value is secret_string.

```
{
  "secret_string" : "secret_string"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "version_metadata" : {
    "id" : "v1",
    "kms_key_id" : "b168fe00ff56492495a7d22974df2d0b",
    "create_time" : 1581507580000,
    "secret_name" : "secret-name-demo",
    "version_stages" : [ "SYSCURRENT" ]
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.2.2 Querying the Secret Version List

Function

This API is used to query the version list of a specified secret.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Constraints

The information returned by this API is the metadata of secret versions, which does not contain secret values.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:listVersion	List	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretVersion:list	-

URI

GET /v1/{project_id}/secrets/{secret_name}/versions

Table 4-1232 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1233 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Pagination parameter. The value is the version number of the last record on the previous page.
limit	No	Integer	Specifies the number of items displayed per page. The default value is 50.

Request Parameters

Table 4-1234 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1235 Response body parameters

Parameter	Type	Description
version_metadatas	Array of **VersionMetadata** objects	**version_metadata** object.
page_info	**PageInfo** object	Pagination information.

Table 4-1236 VersionMetadata

Parameter	Type	Description
id	String	Secret version ID, which is unique under a secret object.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
create_time	Long	Time when a secret version was created. The timestamp indicates the total seconds since January 1, 1970.
expire_time	Long	Expiration time of the secret version. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time. When the secret subscribes to the version expiration event type, the validity period is determined based on this parameter. This parameter is left blank by default.
kms_key_id	String	ID of the KMS CMK used to encrypt a secret version value.
secret_name	String	Secret name
version_stages	Array of strings	Secret version status list. Each status tag is unique for a secret version. If a status tag in use is added to a new version, the tag will be automatically removed from the original version. If **version_stage** is not specified, the temporary tag **SYSCURRENT** will be added to this version.

Table 4-1237 PageInfo

Parameter	Type	Description
next_marker	String	Query address of the next page (name of the secret at the end of the current page, name of the secret at the start of the next page).
previous_marker	String	Name of the start secret on the current page and name of the end secret on the previous page.
current_count	Integer	Number of records returned on this page.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1238 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1239 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1240 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1241 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1242 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-1243 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1244 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "version_metadatas" : [ {
    "id" : "v1",
    "kms_key_id" : "b168fe00ff56492495a7d22974df2d0b",
    "create_time" : 1581507580000,
    "secret_name" : "secret-name-demo",
    "version_stages" : [ "SYSCURRENT" ]
  } ],
  "page_info" : {
    "next_marker" : "v10",
    "previous_marker" : "v1",
    "current_count" : 10
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.2.3 Updating the Secret Version

Function

Currently, the validity period of a specified secret version can be updated. Only secrets in the ENABLED state can be updated. If the associated subscription events contain the basic event type Version Expiration, only one event notification is triggered each time the version validity period is updated.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:updateVersion	Write	secretName *	• csms:Type • csms:VersionId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretVersion:update	-

URI

PUT /v1/{project_id}/secrets/{secret_name}/versions/{version_id}

Table 4-1245 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name
version_id	Yes	String	Version identifier of a secret.

Request Parameters

Table 4-1246 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1247 Request body parameters

Parameter	Mandatory	Type	Description
expire_time	Yes	Long	Expiration time of the secret version. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time. When the secret subscribes to the version expiration event type, the validity period is determined based on this parameter. This parameter is left blank by default.

Response Parameters

Status code: 200

Table 4-1248 Response body parameters

Parameter	Type	Description
version_metadata	VersionMetadata object	Status of a secret version.

Table 4-1249 VersionMetadata

Parameter	Type	Description
id	String	Secret version ID, which is unique under a secret object.
create_time	Long	Time when a secret version was created. The timestamp indicates the total seconds since January 1, 1970.
expire_time	Long	Expiration time of the secret version. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time. When the secret subscribes to the version expiration event type, the validity period is determined based on this parameter. This parameter is left blank by default.
kms_key_id	String	ID of the KMS CMK used to encrypt a secret version value.
secret_name	String	Secret name

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
version_stages	Array of strings	Secret version status list. Each status tag is unique for a secret version. If a status tag in use is added to a new version, the tag will be automatically removed from the original version. If **version_stage** is not specified, the temporary tag **SYSCURRENT** will be added to this version.

Status code: 400

Table 4-1250 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1251 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1252 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1253 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1254 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1255 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1256 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

Update the secret version. The expiration date is 1696838472000.

```
{
  "expire_time" : 1696838472000
}
```

Example Responses

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request succeeded.

```
{
  "version_metadata" : {
    "id" : "v3",
    "kms_key_id" : "b168fe00ff56492495a7d22974df2d0b",
    "create_time" : 1581507580000,
    "secret_name" : "secret-name-demo",
    "version_stages" : [ "SYSCURRENT" ]
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.2.4 Querying the Secret Version and Value

Function

This API is used to query information about a specified secret version and plaintext secret values in the version. Only secrets in the ENABLED state can be queried.

You can use /v1/{project_id}/secrets/{secret_name}/versions/latest (that is, set {version_id} in the URL of the current interface to latest) to access the secret value of the latest version.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:getVersion	Read	secretName *	• csms:Type • csms:VersionId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretVersion:get	kms:cmk:decryptDataKey

URI

GET /v1/{project_id}/secrets/{secret_name}/versions/{version_id}

Table 4-1257 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name
version_id	Yes	String	Version identifier of a secret.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1258 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1259 Response body parameters

Parameter	Type	Description
version	**Version** object	Secret version

Table 4-1260 Version

Parameter	Type	Description
version_metadata	**VersionMetadata** object	Status of a secret version.
secret_binary	String	Plaintext of a binary secret encoded using Base64. CSMS encrypts the plaintext and stores it in the initial version of the secret. Type: Base64-encoded binary data object
secret_string	String	Plaintext of a text secret. CSMS encrypts the plaintext and stores it in the initial version of the secret.

Table 4-1261 VersionMetadata

Parameter	Type	Description
id	String	Secret version ID, which is unique under a secret object.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
create_time	Long	Time when a secret version was created. The timestamp indicates the total seconds since January 1, 1970.
expire_time	Long	Expiration time of the secret version. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time. When the secret subscribes to the version expiration event type, the validity period is determined based on this parameter. This parameter is left blank by default.
kms_key_id	String	ID of the KMS CMK used to encrypt a secret version value.
secret_name	String	Secret name
version_stages	Array of strings	Secret version status list. Each status tag is unique for a secret version. If a status tag in use is added to a new version, the tag will be automatically removed from the original version. If **version_stage** is not specified, the temporary tag **SYSCURRENT** will be added to this version.

Status code: 400

Table 4-1262 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1263 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 403

Table 4-1264 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1265 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1266 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1267 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1268 Response body parameters

Parameter	Type	Description
error_code	String	Error codes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
error_msg	String	Error description

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "version" : {
    "version_metadata" : {
      "id" : "v6",
      "kms_key_id" : "b168fe00ff56492495a7d22974df2d0b",
      "create_time" : 1581507580000,
      "secret_name" : "secret-name-demo",
      "version_stages" : [ "SYSCURRENT" ]
    },
    "secret_string" : "\\\"demo_key\\\":\\\"demo_value\\\""
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.3 Secret Version Status Management

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.3.3.1 Updating the Version Status of a Secret

Function

Update the version status of a secret.

Constraints

- The version status of a secret can uniquely identify only one version under the same secret. If you add a status in use to a new version, the status will be automatically removed from the old version. A version without any version status identifier is considered deprecated and can be automatically deleted by CSMS.

* A secret can have up to 12 version statuses. A status can be used for only one version. **SYSCURRENT** and **SYSPREVIOUS** are built-in secret statuses.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:updateStage	Write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretStage:update	-

URI

PUT /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1269 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name
stage_name	Yes	String	Name of a secret version status that match the regular expression **^[a-zA-Z0-9_-]{1,64}$**

Request Parameters

Table 4-1270 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1271 Request body parameters

Parameter	Mandatory	Type	Description
version_id	Yes	String	Version identifier of a secret.

Response Parameters

Status code: 200

Table 4-1272 Response body parameters

Parameter	Type	Description
stage	**Stage** object	Secret status

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1273 Stage

Parameter	Type	Description
name	String	Status of a secret version. Constraint: The value can contain up to 64 characters.
update_time	Long	Time when a secret version status was updated. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
secret_name	String	Secret name.
version_id	String	Version identifier of a secret

Status code: 400

Table 4-1274 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1275 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1276 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1277 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1278 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1279 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1280 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

Updates the version status of a secret. The version is version_id.

```
{
  "version_id" : "version_id"
}
```

Example Responses

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request succeeded.

```
{
  "stage" : {
    "name" : "name",
    "version_id" : "v1",
    "update_time" : 1581507580000,
    "secret_name" : "secret-name-demo"
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.3.2 Querying the Version Status of a Secret

Function

Queries the version information of a specified secret version status flag.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:getStage	Read	secretName *	• csms:Type • csms:VersionStage • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretStage:get	-

URI

GET /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}

Table 4-1281 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Secret name
stage_name	Yes	String	Name of a secret version status.

Request Parameters

Table 4-1282 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1283 Response body parameters

Parameter	Type	Description
stage	**Stage** object	Secret status

Table 4-1284 Stage

Parameter	Type	Description
name	String	Status of a secret version. Constraint: The value can contain up to 64 characters.
update_time	Long	Time when a secret version status was updated. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
secret_name	String	Secret name.
version_id	String	Version identifier of a secret

Status code: 400

Table 4-1285 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1286 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1287 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1288 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1289 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1290 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1291 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "stage" : {
    "name" : "name",
    "version_id" : "v20",
    "update_time" : 1581507580000,
    "secret_name" : "secret-name-demo"
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.3.3 Deleting the Version Status of a Secret

Function

Deletes the status of a specified secret version.

Constraints

SYSCURRENT and **SYSPREVIOUS** are built-in statuses and cannot be deleted.

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:deleteStage	Write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretStage:delete	-

URI

DELETE /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}

Table 4-1292 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_name	Yes	String	Resource identifier of a secret.
stage_name	Yes	String	Name of a secret version status.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1293 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

Request succeeded.

Status code: 400

Table 4-1294 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1295 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1296 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 404

Table 4-1297 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1298 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1299 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1300 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

None

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
204	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.4 Secret Tag Management

4.3.4.1 Querying a Secret Instance

Function

This API is used to query secret instances. Filters user secret by tag and returns the secret list.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:getSecretsByTag	List	secretName *	-	• csms:tag:getSecretByTag	-

URI

POST /v1/{project_id}/csms/{resource_instances}/action

Table 4-1301 Path Parameters

Parameter	Mandatory	Type	Description
resource_instances	Yes	String	Its value is **resource_instances**.
project_id	Yes	String	Project ID

Request Parameters

Table 4-1302 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1303 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	String	Specifies the number of records to be queried. This parameter does not need to be set when action is set to count. If action is set to filter, the default value is 10. The value of limit is in the ranges 1 to 1,000.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
offset	No	String	The index location. The query starts from the next resource of the specified location. When querying data on the first page, set this parameter to the value in the response body of the previous page. If action is set to count, you do not need to set this parameter. If the **action** is set to **filter**, **offset** defaults to **0**. The value of offset must be a number and cannot be negative.
action	Yes	String	Operation type. It can be: - filter - count: Count total records.
tags	No	Array of **Tag** objects	Tag list, which is the value pairs of tag keys and values. There can be at most 10 value pairs on one page.
matches	No	Array of **TagMatches** objects	Key-value pair to be matched - **key** indicates the search field. Currently, its value is **resource_name**, indicating that only the secret name can be searched. - **value** indicates the field for fuzzy match. It can contain up to 255 characters. If it is left blank, a null value is returned.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff.

Table 4-1304 Tag

Parameter	Mandatory	Type	Description
key	No	String	Tag key

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
values	No	Array of strings	Tag value set. Constraints: A tag can contain at most 10 values, which are unique. If the tag list is empty, any value can be matched. A search result matches only one value.

Table 4-1305 TagMatches

Parameter	Mandatory	Type	Description
key	No	String	Is the field to be matched. Constraints: The value can only be resource_name.
value	No	String	Value for fuzzy match. Constraints: The value can contain a maximum of 255 characters. If the value is empty, an empty value is returned.

Response Parameters

Status code: 200

Table 4-1306 Response body parameters

Parameter	Type	Description
resources	Array of **ActionResources** objects	Resource instance list. For details, see the data structure of the **resource** field.
total_count	Integer	Total number of records.

Table 4-1307 ActionResources

Parameter	Type	Description
resource_id	String	Resource ID
resource_detail	**Secret** object	Secret object

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
resource_name	String	Resource name, which is a null string by default.
tags	Array of **TagItem** objects	Lists of tags. If there is no tag, the array is empty by default.
sys_tags	Array of **SysTag** objects	System tag list. If there is no tag, the list is empty by default.

Table 4-1308 Secret

Parameter	Type	Description
id	String	Resource identifier of a secret
name	String	Secret name
state	String	Secret status. Its value can be: **ENABLED** **DISABLED** **PENDING_DELETE** **FROZEN**
kms_key_id	String	ID of the KMS CMK used to encrypt a secret value.
description	String	Description of a secret
create_time	Long	Secret creation time. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
update_time	Long	Time when a secret was last updated. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time.
scheduled_delete_time	Long	Time when a secret is scheduled to be deleted. The value is a timestamp, that is, the total number of seconds on January 1, 1970 to the current time. If the secret is not in the deletion plan, the value of this parameter is null.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
secret_type	String	Secret type • **COMMON**: shared secret (default), which is used to store sensitive information in an application system. • **RDS**: RDS secret, which is used to store RDS account information. (no longer supported, replaced by **RDS-FG**) • **RDS-FG**: RDS secret, which is used to store RDS account information. • **GaussDB-FG**: TaurusDB secret, which is used to store TaurusDB account information.
auto_rotation	Boolean	Automatic rotation The value can be true (enabled) or false (disabled). The default value is false.
rotation_period	String	Rotation period Constraints: 6 hours - 8,760 hours (365 days) Type: Integer[unit]. Integer indicates the time length. unit indicates the time unit, which can be d (day), h (hour), m (minute), or s (second). For example, 1d indicates one day, and 24h also indicates one day. Note: This parameter is mandatory when automatic rotation is enabled.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
rotation_config	String	Rotation configuration Constraints: The value can contain a maximum of 1,024 characters. If **secret_type** is set to **RDS-FG** or **GaussDB-FG**, set this parameter to **{"InstanceId":"","SecretSubType":""}**. Note: This parameter is mandatory when **secret_type** is set to **RDS-FG** or **GaussDB-FG**. **InstanceId** indicates the instance ID, and **SecretSubType** indicates the rotation subtype. The value can be **SingleUser** or **MultiUser**. **SingleUser**: Single-user rotation is used. A new password is created for the account for each rotation. **MultiUser**: Dual-user rotation is used. The users are labeled as **SYSCURRENT** and **SYSPREVIOUS**, respectively. During secret rotation, the password of the account who is labeled as **SYSPREVIOUS** is reset, and a random password is generated. Then, the labels are switched for the users.
rotation_time	Long	Rotation timestamp
next_rotation_time	Long	Next rotation timestamp
event_subscriptions	Array of strings	List of events subscribed to by secrets. Currently, only one event can be subscribed to. When a basic event contained in an event is triggered, a notification message is sent to the notification topic corresponding to the event.
enterprise_project_id	String	Enterprise project ID
rotation_func_urn	String	URN of the FunctionGraph function

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1309 TagItem

Parameter	Type	Description
key	String	Tag name The tag keys of a secret cannot have duplicate values. A tag key can be used for multiple secrets. A secret can have up to 20 tags. Constraints: The value can contain 1 to 128 characters and must match the regular expression **^((?!\s)(?!*sys*)[\p{L}\p{Z}\p{N}_.:=+\-@]*)(?<!\s)$**.
value	String	Tag value. Constraints: The value can contain a maximum of 255 characters and must match the regular expression **^ ([\p{L}\p{Z}\p{N}_.:\/=+\-@]*) $**.

Table 4-1310 SysTag

Parameter	Type	Description
key	String	The tag key.
value	String	Tag value

Status code: 400

Table 4-1311 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1312 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1313 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1314 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

Table 4-1315 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1316 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 404

Table 4-1317 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1318 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1319 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1320 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 502

Table 4-1321 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1322 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-1323 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1324 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Example Requests

Filters user secrets by tag and returns the secret list.

```
{
  "action" : "filter",
  "tags" : [ {
    "key" : "key1",
    "values" : [ "val1" ]
  } ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total_count" : 1,
  "resources" : [ {
    "resource_id" : "2d1152f2-290d-4756-a1d2-e12c14992416"
  }, {
    "resource_detail" : {
      "id" : "2d1152f2-290d-4756-a1d2-e12c14992416",
      "name" : "example_name",
      "state" : "ENABLED",
      "description" : "",
      "kms_key_id" : "1213d410-ass1-1254-1a2d-3cca2sa2w554",
      "create_time" : 1581507580000,
      "update_time" : 1581507580000,
      "scheduled_delete_time" : 1581507580000
    }
  }, {
    "tags" : [ {
      "key" : "key1",
      "value" : "value1"
    }, {
      "key" : "key2",
      "value" : "value2"
    } ]
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
  }, {
    "sys_tags" : null
  }, {
    "resource_name" : "example_name"
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	Failed to complete the request because the server receives an invalid response from an upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.4.2 Adding or Deleting Secret Tags in Batches

Function

This API is used to add or delete secret tags in batches.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:batchCreateOrDeleteTags	Tagging	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:tag:batch	-
		-	• g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v1/{project_id}/csms/{secret_id}/tags/action

Table 4-1325 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_id	Yes	String	Secret ID

Request Parameters

Table 4-1326 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1327 Request body parameters

Parameter	Mandatory	Type	Description
tags	Yes	Array of **TagItem** objects	List of tags, including tag keys and tag values.
action	Yes	String	Operation type. It can be: create or delete
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff.

Table 4-1328 TagItem

Parameter	Mandatory	Type	Description
key	Yes	String	Tag name The tag keys of a secret cannot have duplicate values. A tag key can be used for multiple secrets. A secret can have up to 20 tags. Constraints: The value can contain 1 to 128 characters and must match the regular expression **^((?!\s)(?!*sys*)[\p{L}\p{Z}\p{N}_.:=+\-@]*)(?<!\s)$**.
value	No	String	Tag value. Constraints: The value can contain a maximum of 255 characters and must match the regular expression **^([\p{L}\p{Z}\p{N}_.:\/=+\-@]*) $**.

Response Parameters

Status code: 204

No Content

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1329 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1330 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

Table 4-1331 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1332 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

Table 4-1333 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1334 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 404

Table 4-1335 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1336 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1337 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1338 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-1339 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1340 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 504

Table 4-1341 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1342 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Example Requests

This API is used to add secret tags in batches.

```
{
  "action" : "create",
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value2"
  } ]
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Responses

None

Status Codes

Status Code	Description
204	No Content
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.4.3 Querying Secret Tags

Function

This API is used to query secret tags.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:listTags	List	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:tag:getBySecret	-

URI

GET /v1/{project_id}/csms/{secret_id}/tags

Table 4-1343 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_id	Yes	String	Secret ID

Request Parameters

Table 4-1344 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1345 Response body parameters

Parameter	Type	Description
tags	Array of **TagItem** objects	Tag list, which is the value pairs of tag keys and values. • **key**: Tag key. A secret can contain up to 20 keys. This value cannot be left blank or repeated. The value of a **key** must be unique and can contain up to 128 characters. • **value**: Tag value. Each tag value can contain up to 255 characters. A search result matches all the values.
sys_tags	Array of **SysTag** objects	System tags

Table 4-1346 TagItem

Parameter	Type	Description
key	String	Tag name The tag keys of a secret cannot have duplicate values. A tag key can be used for multiple secrets. A secret can have up to 20 tags. Constraints: The value can contain 1 to 128 characters and must match the regular expression **^((?!\s)(?!*sys*)[\p{L}\p{Z}\p{N}_.:=+\-@]*)(?<!\s)$**.
value	String	Tag value. Constraints: The value can contain a maximum of 255 characters and must match the regular expression **^ ([\p{L}\p{Z}\p{N}_.:\/=+\-@]*) $**.

Table 4-1347 SysTag

Parameter	Type	Description
key	String	The tag key.
value	String	Tag value

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1348 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1349 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

Table 4-1350 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1351 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

Table 4-1352 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1353 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 404

Table 4-1354 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1355 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1356 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1357 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-1358 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1359 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 504

Table 4-1360 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1361 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "tags" : [ {
    "key" : "key1",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value2"
  } ],
  "sys_tags" : null
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.4.4 Querying Secret Tags

Function

Add a secret tag.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:createTag	Tagging	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:tag:create	-
		-	• g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v1/{project_id}/csms/{secret_id}/tags

Table 4-1362 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_id	Yes	String	Secret ID

Request Parameters

Table 4-1363 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1364 Request body parameters

Parameter	Mandatory	Type	Description
tag	Yes	**TagItem** object	Tag information

Table 4-1365 TagItem

Parameter	Mandatory	Type	Description
key	Yes	String	Tag name The tag keys of a secret cannot have duplicate values. A tag key can be used for multiple secrets. A secret can have up to 20 tags. Constraints: The value can contain 1 to 128 characters and must match the regular expression **^((?!\s)(?!*sys*)[\p{L}\p{Z}\p{N}_.:=+\-@]*)(?<!\s)$**.
value	No	String	Tag value. Constraints: The value can contain a maximum of 255 characters and must match the regular expression **^([\p{L}\p{Z}\p{N}_.:\/=+\-@]*) $**.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 4-1366 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1367 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

Table 4-1368 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1369 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

Table 4-1370 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1371 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 404

Table 4-1372 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1373 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1374 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1375 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 502

Table 4-1376 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1377 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 504

Table 4-1378 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1379 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Example Requests

Add a secret tag.

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

Example Responses

None

Status Codes

Status Code	Description
204	No Content

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.4.5 Deleting a Secret Tag

Function

This API is used to delete a secret tag.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms:secret:deleteTag	Tagging	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:tag:delete	-
		-	g:TagKeys		

URI

DELETE /v1/{project_id}/csms/{secret_id}/tags/{key}

Table 4-1380 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
secret_id	Yes	String	Secret ID
key	Yes	String	Value of a tag key.

Request Parameters

Table 4-1381 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 204

No Content

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1382 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1383 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

Table 4-1384 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1385 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

Table 4-1386 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1387 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 404

Table 4-1388 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1389 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1390 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1391 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-1392 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1393 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 504

Table 4-1394 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1395 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Example Requests

None

Example Responses

None

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
204	No Content
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	The request failed to be fulfilled because the server received an invalid response from the upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.4.6 Querying Project Tags

Function

This API is used to query all secret tags of a user in a specified project.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms::listProjectTags	List	-	-	• csms:tag:getAll	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

URI

GET /v1/{project_id}/csms/tags

Table 4-1396 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-1397 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1398 Response body parameters

Parameter	Type	Description
tags	Array of **TagResponse** objects	Tag list, which is the value pairs of tag keys and values. • **key**: Tag key. A secret can contain up to 20 keys. This value cannot be left blank or repeated. The value of a **key** must be unique and can contain up to 128 characters. • **value**: Tag value. Each tag value can contain up to 255 characters. A search result matches all the values.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1399 TagResponse

Parameter	Type	Description
key	String	Tag key,
values	Array of strings	Tag value set.

Status code: 400

Table 4-1400 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1401 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

Table 4-1402 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1403 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1404 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1405 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 404

Table 4-1406 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1407 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1408 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1409 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 502

Table 4-1410 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1411 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 504

Table 4-1412 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1413 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "tags" : [ {
    "key" : "key1",
    "values" : [ "val1" ]
  }, {
    "key" : "key2",
    "values" : [ "val2" ]
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	Failed to complete the request because the server receives an invalid response from an upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.5 Event Management

4.3.5.1 Creating an Event

Function

Creates an event that can be configured on one or more secret objects. When an event is enabled and the basic event type contained in the event is triggered on the secret object, the cloud service sends the corresponding event notification to the notification topic specified by the event.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Constraints

The created event notification cannot be used independently and needs to be configured on a specific secret object. The service does not check the validity of the notification object in the event notification. If the notification object does not exist under the user account, the event notification fails when the event is triggered.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms::createEvent	Write	-	-	• csms:event:create	-

URI

POST /v1/{project_id}/csms/events

Table 4-1414 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1415 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-1416 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the created event notification. Constraint: The value can contain 1 to 64 characters and must match the regular expression **^[a-zA-Z0-9._-]{1,64}$**.
event_types	Yes	Array of strings	Basic event list of the notification. The event types are as follows: • **SECRET_VERSION_CREATED**: Version created. • **SECRET_VERSION_EXPIRED**: Version expired. • **SECRET_ROTATED**: Secret rotated. • **SECRET_DELETED**: Secret deleted. • **SECRET_ROTATED_FAILED**: The secret fails to be rotated. The basic event types in the list must be unique.
state	Yes	String	Indicates whether an event takes effect. Basic event types can be triggered only when the event is enabled. Enabled Disabled

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
notification	Yes	**Notification** object	Notification topic object.

Table 4-1417 Notification

Parameter	Mandatory	Type	Description
target_type	Yes	String	Type of the object to which an event notification is sent.
target_id	Yes	String	ID of the object to which the event notification is sent.
target_name	Yes	String	Name of the object to which the event notification is sent.

Response Parameters

Status code: 200

Table 4-1418 Response body parameters

Parameter	Type	Description
event	**Event** object	Event notification object

Table 4-1419 Event

Parameter	Type	Description
name	String	Event notification name.
event_id	String	Indicates the resource identifier of the event notification.
event_types	Array of strings	Set the basic event type list. **Constraints**: The array can contain up to 12 elements.
state	String	Event notification status. The options are as follows: **ENABLED** **DISABLED**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
create_time	Long	Time when an event notification is created. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time specified by this parameter.
update_time	Long	Last update time of the event notification. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time.
notification	**Notification** object	Notification topic object.

Table 4-1420 Notification

Parameter	Type	Description
target_type	String	Type of the object to which an event notification is sent.
target_id	String	ID of the object to which the event notification is sent.
target_name	String	Name of the object to which the event notification is sent.

Status code: 400

Table 4-1421 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1422 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1423 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1424 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

Table 4-1425 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1426 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 404

Table 4-1427 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1428 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1429 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1430 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 502

Table 4-1431 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1432 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-1433 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1434 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Example Requests

Create an event.

```
{
  "name" : "demo-event",
  "event_types" : [ "SECRET_VERSION_CREATED", "SECRET_VERSION_EXPIRED" ],
  "state" : "ENABLED",
  "notification" : {
    "target_type" : "SMN",
    "target_id" : "urn:smn:cn-north-4:dc3b7c85759141a991da17423c0f2068:test-poc",
    "target_name" : "demo-smn-name"
  }
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "event" : {
    "name" : "event-test",
    "event_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "state" : "ENABLED",
    "event_types" : [ "SECRET_VERSION_CREATED", "SECRET_VERSION_EXPIRED" ],
    "create_time" : 1581507580000,
    "update_time" : 1581507580000,
    "notification" : {
      "target_type" : "SMN",
      "target_id" : "urn:smn:cn-north-4:SecertExpirationTest",
      "target_name" : "SecertExpirationNotificationTest"
    }
  }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	Failed to complete the request because the server receives an invalid response from an upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.5.2 Querying Events

Function

This API is used to query information about a specified event.

Constraints

The information returned by this API is the metadata information value of the secret event notification.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms::getEvent	Read	-	-	• csms:event:get	-

URI

GET /v1/{project_id}/csms/events/{event_name}

Table 4-1435 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
event_name	Yes	String	Name of an event notification.

Request Parameters

Table 4-1436 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1437 Response body parameters

Parameter	Type	Description
event	**Event** object	Event notification object

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1438 Event

Parameter	Type	Description
name	String	Event notification name.
event_id	String	Indicates the resource identifier of the event notification.
event_types	Array of strings	Set the basic event type list. **Constraints**: The array can contain up to 12 elements.
state	String	Event notification status. The options are as follows: **ENABLED** **DISABLED**
create_time	Long	Time when an event notification is created. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time specified by this parameter.
update_time	Long	Last update time of the event notification. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time.
notification	**Notification** object	Notification topic object.

Table 4-1439 Notification

Parameter	Type	Description
target_type	String	Type of the object to which an event notification is sent.
target_id	String	ID of the object to which the event notification is sent.
target_name	String	Name of the object to which the event notification is sent.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1440 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1441 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

Table 4-1442 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1443 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

Table 4-1444 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1445 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 404

Table 4-1446 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1447 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1448 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1449 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-1450 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1451 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 504

Table 4-1452 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1453 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "event" : {
    "name" : "event-test",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
  "event_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "state" : "ENABLED",
  "event_types" : [ "SECRET_VERSION_EXPIRED" ],
  "create_time" : 1581507580000,
  "update_time" : 1581507580000,
  "notification" : {
    "target_type" : "SMN",
    "target_id" : "urn:smn:cn-north-4:SecertExpirationTest",
    "target_name" : "SecertExpirationNotificationTest"
  }
 }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	Failed to complete the request because the server receives an invalid response from an upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.5.3 Querying the Event List

Function

This API is used to query all events created by the current user in the project.

Constraints

The information returned by this API is the metadata information of the event notification, excluding the secret value.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms::listEvents	List	-	-	• csms:event:list	-

URI

GET /v1/{project_id}/csms/events

Table 4-1454 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-1455 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	String	Specifies the number of records on each page. Default value: 50
marker	No	String	Start event name of pagination query. If this parameter is left blank, only the first page is queried.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1456 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-1457 Response body parameters

Parameter	Type	Description
events	Array of **Event** objects	Event details list
page_info	**PageInfo** object	Pagination information.

Table 4-1458 Event

Parameter	Type	Description
name	String	Event notification name.
event_id	String	Indicates the resource identifier of the event notification.
event_types	Array of strings	Set the basic event type list. **Constraints**: The array can contain up to 12 elements.
state	String	Event notification status. The options are as follows: **ENABLED** **DISABLED**
create_time	Long	Time when an event notification is created. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time specified by this parameter.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
update_time	Long	Last update time of the event notification. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time.
notification	**Notification** object	Notification topic object.

Table 4-1459 Notification

Parameter	Type	Description
target_type	String	Type of the object to which an event notification is sent.
target_id	String	ID of the object to which the event notification is sent.
target_name	String	Name of the object to which the event notification is sent.

Table 4-1460 PageInfo

Parameter	Type	Description
next_marker	String	Query address of the next page (name of the secret at the end of the current page, name of the secret at the start of the next page).
previous_marker	String	Name of the start secret on the current page and name of the end secret on the previous page.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-1461 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1462 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

Table 4-1463 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1464 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

Table 4-1465 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1466 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 404

Table 4-1467 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1468 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1469 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1470 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 502

Table 4-1471 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1472 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 504

Table 4-1473 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1474 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.


```
{
  "events" : [ {
    "state" : "ENABLED",
    "name" : "TestEvent1",
    "event_id" : "120eeafd-eca5-4098-8733-c1b369f3a450",
    "event_types" : [ "SECRET_VERSION_CREATED", "SECRET_VERSION_EXPIRED",
"SECRET_VERSION_NEAR_EXPIRY", "SECRET_DELETED" ],
    "create_time" : 1669042498000,
    "update_time" : 1669042498000,
    "notification" : {
      "target_type" : "SMN",
      "target_id" : "urn:smn:cn-north-4:dc3b7c85759141a991da17423c0f2068:smn-target-name",
      "target_name" : "smn-target-name"
    }
  }, {
    "state" : "ENABLED",
```


 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "name" : "TestEvent2",
    "event_id" : "1d251c99-37d2-4396-86ce-f000d3aa9850",
    "event_types" : [ "SECRET_VERSION_CREATED", "SECRET_VERSION_EXPIRED",
"SECRET_VERSION_NEAR_EXPIRY", "SECRET_DELETED" ],
    "create_time" : 1669041491000,
    "update_time" : 1669041491000,
    "notification" : {
      "target_type" : "SMN",
      "target_id" : "urn:smn:cn-north-4:dc3b7c85759141a991da17423c0f2068:smn-target-name",
      "target_name" : "smn-target-name"
    }
  } ],
  "page_info" : {
    "next_marker" : "TestEvent2",
    "previous_marker" : "TestEvent3",
    "current_count" : 2
  }
}
```


Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	Failed to complete the request because the server receives an invalid response from an upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.5.4 Update an Event

Function

This API is used to update the metadata of a specified event. Metadata that can be updated includes the event enabling status, basic type list, and notification topic.

Constraints

This API can be used to modify only the metadata of secret event notifications.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms::updateEvent	Write	-	-	• csms:event:update	-

URI

PUT /v1/{project_id}/csms/events/{event_name}

Table 4-1475 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
event_name	Yes	String	Event notification name

Request Parameters

Table 4-1476 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1477 Request body parameters

Parameter	Mandatory	Type	Description
state	No	String	Event notification status. The options are as follows: **ENABLED** **DISABLED**
event_types	No	Array of strings	Basic event list of the notification. The event types are as follows: • **SECRET_VERSION_CREATED**: Version created. • **SECRET_VERSION_EXPIRED**: Version expired. • **SECRET_ROTATED**: Secret rotated. • **SECRET_DELETED**: Secret deleted. • **SECRET_ROTATED_FAILED**: The secret fails to be rotated. The basic event types in the list must be unique.
notification	No	**Notification** object	Notification topic object.

Table 4-1478 Notification

Parameter	Mandatory	Type	Description
target_type	Yes	String	Type of the object to which an event notification is sent.
target_id	Yes	String	ID of the object to which the event notification is sent.
target_name	Yes	String	Name of the object to which the event notification is sent.

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1479 Response body parameters

Parameter	Type	Description
event	**Event** object	Event notification object

Table 4-1480 Event

Parameter	Type	Description
name	String	Event notification name.
event_id	String	Indicates the resource identifier of the event notification.
event_types	Array of strings	Set the basic event type list. **Constraints**: The array can contain up to 12 elements.
state	String	Event notification status. The options are as follows: **ENABLED** **DISABLED**
create_time	Long	Time when an event notification is created. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time specified by this parameter.
update_time	Long	Last update time of the event notification. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time.
notification	**Notification** object	Notification topic object.

Table 4-1481 Notification

Parameter	Type	Description
target_type	String	Type of the object to which an event notification is sent.
target_id	String	ID of the object to which the event notification is sent.
target_name	String	Name of the object to which the event notification is sent.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 400

Table 4-1482 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1483 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

Table 4-1484 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1485 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

Table 4-1486 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1487 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 404

Table 4-1488 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1489 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1490 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1491 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 502

Table 4-1492 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1493 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 504

Table 4-1494 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1495 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Example Requests

This API is used to update a specified event.

```
{
  "notification" : {
    "target_type" : "SMN",
    "target_id" : "demo-smn-id",
    "target_name" : "demo-smn-name"
  }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Responses

Status code: 200

Request succeeded.

```
{
  "event" : {
    "name" : "event-test",
    "event_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "state" : "ENABLED",
    "event_types" : [ "SECRET_VERSION_EXPIRED" ],
    "create_time" : 1581507580000,
    "update_time" : 1581507580000,
    "notification" : {
      "target_type" : "SMN",
      "target_id" : "urn:smn:cn-north-4:SecertExpirationTest",
      "target_name" : "SecertExpirationNotificationTest"
    }
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	Failed to complete the request because the server receives an invalid response from an upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.5.5 Deleting an Event Immediately

Function

The specified event is deleted immediately and cannot be restored. If an event is referenced by a secret, the event cannot be deleted. Disassociate the event from the secret first.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Constraints

Secrets deleted via this API cannot be restored.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms::deleteEvent	Write	-	-	• csms:event:delete	-

URI

DELETE /v1/{project_id}/csms/events/{event_name}

Table 4-1496 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
event_name	Yes	String	Name of an event notification.

Request Parameters

Table 4-1497 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 204

Request succeeded.

Status code: 400

Table 4-1498 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1499 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 401

Table 4-1500 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1501 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1502 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1503 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 404

Table 4-1504 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1505 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1506 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1507 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 502

Table 4-1508 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1509 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 504

Table 4-1510 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1511 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
204	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	Failed to complete the request because the server receives an invalid response from an upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.5.6 Querying Triggered Event Notification Records

Function

Query all event notification records that have been triggered in the last three months.

Constraints

Only event notification records generated within three months are stored.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms::listNotificationRecords	List	-	-	• csms:event:listNotificationRecords	-

URI

GET /v1/{project_id}/csms/notification-records

Table 4-1512 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-1513 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1514 Response body parameters

Parameter	Type	Description
records	Array of **Record** objects	Record object
page_info	**PageInfo** object	Pagination information.

Table 4-1515 Record

Parameter	Type	Description
event_name	String	Secret name.
trigger_event_type	String	Event type. • **SECRET_VERSION_CREATED**: Version created. • **SECRET_VERSION_EXPIRED**: Version expired. • **SECRET_ROTATED**: Secret rotated. • **SECRET_DELETED**: Secret deleted. • **SECRET_ROTATED_FAILED**: The secret fails to be rotated.
create_time	Long	Time when an event notification record is created. The value is a timestamp, that is, the total number of seconds from January 1, 1970 to the time specified by this parameter.
secret_name	String	Secret name
secret_type	String	Secret type • **COMMON**: shared secret (default), which is used to store sensitive information in an application system. • **RDS**: RDS secret, which is used to store RDS account information. (no longer supported, replaced by **RDS-FG**) • **RDS-FG**: RDS secret, which is used to store RDS account information. • **GaussDB-FG**: TaurusDB secret, which is used to store TaurusDB account information.
notification_target_name	String	Name of the object to which the event notification is sent.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
notification_target_id	String	ID of the object to which the event notification is sent.
notification_content	String	Event notification
notification_status	String	Event notification status. • **SUCCESS**: Event notification succeeded. • **FAIL**: Event notification failed. • **INVALID**: Failed to send the event notification because the topic is invalid or incorrect.

Table 4-1516 PageInfo

Parameter	Type	Description
next_marker	String	Query address of the next page (name of the secret at the end of the current page, name of the secret at the start of the next page).
previous_marker	String	Name of the start secret on the current page and name of the end secret on the previous page.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-1517 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1518 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
error_msg	String	Error information returned for an error request.

Status code: 401

Table 4-1519 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1520 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 403

Table 4-1521 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1522 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 404

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1523 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1524 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 500

Table 4-1525 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1526 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 502

Table 4-1527 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1528 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Status code: 504

Table 4-1529 Response body parameters

Parameter	Type	Description
error	**ErrorDetail** object	Error message

Table 4-1530 ErrorDetail

Parameter	Type	Description
error_code	String	Error code returned for an error request.
error_msg	String	Error information returned for an error request.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.


```
{
  "records" : [ {
    "event_name" : "demo-event",
    "trigger_event_type" : "SECRET_VERSION_EXPIRED",
    "create_time" : 1581507580000,
    "secret_name" : "demo-secret",
    "secret_type" : "COMMON",
    "notification_target_name" : "SecertExpirationNotificationTest",
    "notification_target_id" : "urn:smn:cn-north-4:SecertExpirationTest",
    "notification_content" : "{\"eventName\":\"TestEvent20221112\",\"eventType
\":\"SECRET_VERSION_EXPIRED\",\"eventTime\":\"2023-04-14T20:25:10.126Z\",\"data\":{\"secretId
\":\"fde3d6ba-cb31-40b0-b6c4-78757050f8c8\",\"secretName\":\"Secret20230325\",\"createTime
\":\"2023-03-22T20:43:04.000Z\",\"updateTime\":\"2023-04-14T20:18:29.000Z\",\"versionId
\":\"v18\",\"versionExpireTime\":\"2023-03-29T17:07:23.000Z\"}}",
    "notification_status" : "SUCCESS"
```


 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
 }]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	A username and password are required.
403	Authentication failed.
404	The requested resource does not exist or is not found.
500	Internal service error.
502	Failed to complete the request because the server receives an invalid response from an upstream server.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.6 Secret Rotation Management

4.3.6.1 Querying the Task List

Function

Query the task list.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
csms::listTasks	List	-	-	• csms:task:list	-

URI

GET /v1/{project_id}/csms/tasks

Table 4-1531 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-1532 Query Parameters

Parameter	Mandatory	Type	Description
secret_name	No	String	Secret name
status	No	String	Task status. The value can be: • **SUCCESS**: Task rotated. • **FAILED**: Task rotation failed.
task_id	No	String	Task ID. If this parameter is specified, other search criteria cannot be specified.
limit	No	Integer	Number of records returned on each page. The default value is **50**.
marker	No	String	Start task ID of pagination query. If this parameter is left blank, only the first page is queried.

Request Parameters

None

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 200

Table 4-1533 Response body parameters

Parameter	Type	Description
total	Integer	Number of tasks
tasks	Array of SecretTask objects	Secret tasks
next_marker	String	Address for querying the next page (ID of the last task on the current page).

Table 4-1534 SecretTask

Parameter	Type	Description
task_id	String	Task ID
secret_name	String	Secret name
rotation_func_urn	String	URN of the FunctionGraph function
task_status	String	Task status
operate_type	String	Rotation type
task_time	Long	Task creation time
attempt_nums	Integer	Number of rotation attempts
task_error_code	String	Task error code
task_error_msg	String	Task error message

Status code: 400

Table 4-1535 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1536 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1537 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1538 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1539 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1540 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-1541 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

- Query the secret task whose ID is xxxxx.

  ```
  /v1/xxxxx/csms/tasks?task_id=xxxxx
  ```

- Query the secret task whose name is xx. The task status is **FAILED**. There are 10 returned records on each page. The start task ID of each page is xxxx.

  ```
  /v1/xxxxx/csms/tasks?secret_name=xx&status=FAILED&limit=10&marker=xxxx
  ```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 1,
  "tasks" : [ {
    "task_id" : "xxxx",
    "secret_name" : "xxxx",
    "rotation_func_urn" : "urn:fss:cn-north-4:xxxxxxxx:function:default:xxxx:xxxxx",
    "task_status" : "SUCCESS",
    "attempt_nums" : 3,
    "operate_type" : "MULTI_USER",
    "task_time" : 1715436899000
  } ],
  "next_marker" : "xxxxxx"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Request failed. The server has received an invalid response.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.6.2 Creating a Service Agency

Function

Create a service agency for CSMS and FunctionGraph.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/csms/agencies

Request Parameters

Table 4-1542 Request body parameters

Parameter	Mandatory	Type	Description
secret_type	Yes	String	Secret type

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1543 Response body parameters

Parameter	Type	Description
agencies	Array of **Agency** objects	Agency details list

Table 4-1544 Agency

Parameter	Type	Description
agency_name	String	Agency name
agency_id	String	Agency ID
error_msg	String	Error message. Returned error message when the agency fails to be created.

Status code: 400

Table 4-1545 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1546 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1547 Response body parameters

Parameter	Type	Description
error_code	String	Error codes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
error_msg	String	Error description

Status code: 404

Table 4-1548 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1549 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1550 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1551 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

Create an agency for **RDS-FG** secrets.

```
{
  "secret_type" : "RDS-FG"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "agencies" : [ {
    "agency_name" : "xxxx1",
    "agency_id" : "xxxxxxx"
  }, {
    "agency_name" : "xxxxx2",
    "error_msg" : "xxxxxxxx"
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Request failed. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.6.3 Checking Whether a Service Agency Exists

Function

Check whether a service agency exists.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

GET /v1/csms/agencies

Table 4-1552 Query Parameters

Parameter	Mandatory	Type	Description
secret_type	Yes	String	Secret type

Request Parameters

None

Response Parameters

Status code: 200

Table 4-1553 Response body parameters

Parameter	Type	Description
agency_granted	String	Whether an agency exists.

Status code: 400

Table 4-1554 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1555 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1556 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1557 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1558 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1559 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-1560 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

Query the agency of **RDS-FG** secrets.

```
/v1/csms/agencies?secret_type=RDS-FG
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "agency_granted" : "true"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Request failed. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.3.6.4 Obtaining the Secret Rotation Function Template

Function

Obtain the secret rotation function template.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

GET /v1/csms/function-templates

Table 4-1561 Query Parameters

Parameter	Mandatory	Type	Description
secret_type	Yes	String	Secret type
secret_sub_type	Yes	String	Secret rotation account type • **SingleUser**: single-user rotation • **MultiUser**: dual-user rotation
engine	No	String	Database type. This parameter is mandatory if the secret type is **RDS-FG**. The value can be **mysql**, **postgresql**, or **sqlserver**. Other secret types are not supported.

Request Parameters

None

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1562 Response body parameters

Parameter	Type	Description
function_templates	String	Secret rotation function template

Status code: 400

Table 4-1563 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1564 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1565 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1566 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 500

Table 4-1567 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1568 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1569 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

Obtain the rotation template of **RDS-FG** secrets. The account type is **SingleUser** and the database type is **mysql**.

```
/v1/csms/function-templates?secret_type=RDS-FG&secret_sub_type=SingleUser&engine=mysql
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "function_templates" : "xxxxxx"
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.
404	The resource does not exist.
500	Internal service error.
502	Request failed. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.7 User Management

4.3.7.1 Enabling a User

Function

This API is used to enable a user.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/csms/users/{user_id}/enable

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1570 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	User ID.

Request Parameters

Table 4-1571 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	It can be obtained by calling the IAM API. The token is the value of **X-Subject-Token** in the response header.

Response Parameters

Status code: 200

Table 4-1572 Response body parameters

Parameter	Type	Description
user_id	String	User ID.

Status code: 400

Table 4-1573 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error details.

Example Requests

Enable a user based on the imported user ID.

```
/api/v1/tenant/users/{user_id}/enable
```

Example Responses

Status code: 200

Request succeeded.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
{
  "user_id" : "20210621095935811-5E16-6B3060..."
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.

Error Codes

See **Error Codes**.

4.3.7.2 Changing a User Password

Function

This API is used to change user passwords.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/csms/users/change-password

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1574 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The token is the value of **X-Subject-Token** in the response header.

Table 4-1575 Request body parameters

Parameter	Mandatory	Type	Description
password	Yes	String	New password.
old_password	Yes	String	Old password.

Response Parameters

Status code: 200

Table 4-1576 Response body parameters

Parameter	Type	Description
user_id	String	User ID.

Status code: 400

Table 4-1577 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error details.

Example Requests

Change the user password. The new password is **huawei@321**, and the old password is **huawei@123**.

```
{
  "password" : "12345678",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
  "old_password" : "234567"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "user_id" : "20210621095935811-5E16-6B3060..."
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.

Error Codes

See **Error Codes**.

4.3.7.3 Importing Users in Batches

Function

This API is used to import users in batches.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/csms/users/batch-import

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request Parameters

Table 4-1578 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The token is the value of **X-Subject-Token** in the response header.

Table 4-1579 Request body parameters

Parameter	Mandatory	Type	Description
total	Yes	Integer	Number of imported records.
users	Yes	Array of **CreateUserRequest** objects	User list.

Table 4-1580 CreateUserRequest

Parameter	Mandatory	Type	Description
user_name	Yes	String	Username, which is a unique identifier in an enterprise.
mobile	Yes	String	Mobile number, which is unique in an enterprise.
password	No	String	Password, which must be in the format defined by the enterprise.
org_code	No	String	Main organization code. Enter an existing organization code in an enterprise. If the value is left empty, the organization is under the first root organization.
name	No	String	Real name. If the value is null, **user_name** is used. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
email	No	String	Email address. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.
employee_id	No	String	Employee ID. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.
first_name	No	String	Name. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.
middle_name	No	String	Middle name. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.
last_name	No	String	Last name. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.
pwd_must_modify	No	Boolean	Whether the password must be changed upon first login. The default value is **true**.
attr_gender	No	String	Gender.
attr_birthday	No	String	Date of birth, in yyyy-mm-dd format
attr_nick_name	No	String	Alias.
attr_identity_type	No	String	Certificate type.
attr_identity_number	No	String	Certificate number.
attr_area	No	String	Country or region code.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
attr_city	No	String	City.
attr_manager_id	No	String	Immediate superior.
attr_user_type	No	String	Personnel type. The value can be **regular** (formal), **intern** (internship), **dispatch** (labor dispatch), or **outsourcing** (labor outsourcing).
attr_hire_date	No	String	Onboarding date, in yyyy-MM-dd format.
attr_work_place	No	String	Work location.
user_org_relation_list	No	Array of **UserOrgRelationListOption** objects	Relationships between users and organizations. The main organization information must be included if this parameter is set.
extension	No	Object	Custom extended attribute.

Table 4-1581 UserOrgRelationListOption

Parameter	Mandatory	Type	Description
orgCode	Yes	String	Organization code.
relationType	Yes	String	Ownership. A user can only belong to one organization and can be mounted to at most nine organizations. The value can be **0** (mounting) or **1** (belonging).

Response Parameters

Status code: 200

Table 4-1582 Response body parameters

Parameter	Type	Description
error_list	Array of **ErrorInfo** objects	Failure description.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
total	Integer	Total number of records.
success	Integer	Number of successful records.
failed	Integer	Number of failed records.

Table 4-1583 ErrorInfo

Parameter	Type	Description
name	String	Name.
error_msg	String	Failure cause.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Import status.

Error Codes

See **Error Codes**.

4.3.7.4 Disabling a User

Function

This API is used to disable a user.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/csms/users/{user_id}/disable

Table 4-1584 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	User ID.

Request Parameters

Table 4-1585 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	It can be obtained by calling the IAM API. The token is the value of **X-Subject-Token** in the response header.

Response Parameters

Status code: 200

Table 4-1586 Response body parameters

Parameter	Type	Description
user_id	String	User ID.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1587 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error details.

Example Requests

Disable a user based on the imported user ID.

```
/api/v1/tenant/users/{user_id}/disable
```

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.

Error Codes

See **Error Codes**.

4.3.7.5 User Management

Function

This API is used to create a user.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

URI

POST /v1/csms/users

Request Parameters

Table 4-1588 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The token is the value of **X-Subject-Token** in the response header.

Table 4-1589 Request body parameters

Parameter	Mandatory	Type	Description
user_name	Yes	String	Username, which is a unique identifier in an enterprise.
mobile	Yes	String	Mobile number, which is unique in an enterprise.
password	No	String	Password, which must be in the format defined by the enterprise.
org_code	No	String	Main organization code. Enter an existing organization code in an enterprise. If the value is left empty, the organization is under the first root organization.
name	No	String	Real name. If the value is null, **user_name** is used. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.
email	No	String	Email address. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
employee_id	No	String	Employee ID. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.
first_name	No	String	Name. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.
middle_name	No	String	Middle name. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.
last_name	No	String	Last name. You can modify the mandatory attributes. To do so, log in to the administrator portal, and access the **User Attributes** page under the **Users** menu.
pwd_must_modify	No	Boolean	Whether the password must be changed upon first login. The default value is **true**.
attr_gender	No	String	Gender.
attr_birthday	No	String	Date of birth, in yyyy-mm-dd format
attr_nick_name	No	String	Alias.
attr_identity_type	No	String	Certificate type.
attr_identity_number	No	String	Certificate number.
attr_area	No	String	Country or region code.
attr_city	No	String	City.
attr_manager_id	No	String	Immediate superior.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
attr_user_type	No	String	Personnel type. The value can be **regular** (formal), **intern** (internship), **dispatch** (labor dispatch), or **outsourcing** (labor outsourcing).
attr_hire_date	No	String	Onboarding date, in yyyy-MM-dd format.
attr_work_place	No	String	Work location.
user_org_relation_list	No	Array of **UserOrgRelationListOption** objects	Relationships between users and organizations. The main organization information must be included if this parameter is set.
extension	No	Object	Custom extended attribute.

Table 4-1590 UserOrgRelationListOption

Parameter	Mandatory	Type	Description
orgCode	Yes	String	Organization code.
relationType	Yes	String	Ownership. A user can only belong to one organization and can be mounted to at most nine organizations. The value can be **0** (mounting) or **1** (belonging).

Response Parameters

Status code: 201

Table 4-1591 Response body parameters

Parameter	Type	Description
user_id	String	User ID.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1592 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error details.

Example Requests

Create a user whose username is **zhangsan**, mobile number is **12345678901**, and email address is **zhangsan@example.com**.

```
{
  "user_name" : "zhangsan",
  "password" : "p******d",
  "org_code" : "10000",
  "name" : "zhangsan",
  "mobile" : "12345678901",
  "email" : "zhangsan@example.com",
  "employee_id" : "123456789",
  "pwd_must_modify" : false,
  "first_name" : "F",
  "middle_name" : "M",
  "last_name" : "L",
  "attr_gender" : "male",
  "attr_birthday" : "1990-02-01",
  "attr_nick_name" : "zhangsan",
  "attr_identity_type" : "id_card",
  "attr_identity_number" : "123456789",
  "attr_area" : "CN",
  "attr_city" : "xxx",
  "attr_manager_id" : "123456789",
  "attr_user_type" : "regular",
  "attr_hire_date" : "2021-04-01",
  "attr_work_place" : "xxx",
  "user_org_relation_list" : [ {
    "orgCode" : "10000",
    "relationType" : 1
  }, {
    "orgCode" : "TestOrg1",
    "relationType" : 0
  }, {
    "orgCode" : "TestOrg2",
    "relationType" : 0
  } ],
  "extension" : {
    "age" : "18"
  }
}
```

Example Responses

Status code: 201

Request succeeded.

```
{
  "user_id" : "20210621095935811-5E16-6B3060..."
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

Status Code	Description
201	Request succeeded.
400	Request failed.

Error Codes

See **Error Codes**.

4.3.7.6 Querying the User List

Function

This API is used to query users.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

GET /v1/csms/users

Table 4-1593 Query Parameters

Parameter	Mandatory	Type	Description
org_id	No	String	Organization ID. If this parameter is left empty, all users are queried.
offset	Yes	Integer	Page number. Minimum value: **0**.
limit	Yes	Integer	Number of data records on each page. Minimum value: **10**. Maximum value: **100**.

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
user_info	No	String	Username, which can contain at most 64 characters. Fuzzy search is supported.

Request Parameters

Table 4-1594 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The token is the value of **X-Subject-Token** in the response header.

Response Parameters

Status code: 200

Table 4-1595 Response body parameters

Parameter	Type	Description
total	Long	Total number of users.
users	Array of **UsersDetailsResult** objects	User list.

Table 4-1596 UsersDetailsResult

Parameter	Type	Description
user_id	String	User ID.
org_id	String	Organization to which the user belongs.
user_name	String	Username.
name	String	Name.
mobile	String	Mobile number.
email	String	Email address.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
pwd_must_modify	Boolean	Whether the password must be changed upon first login.
pwd_change_at	String	Password change time.
created_at	String	Creation time.
updated_at	String	Last modification time.
disabled	String	Disabled or not.
grade	String	Trust level.
locked	String	Locked or not.
extension	String	Custom extended attribute.
user_org_relation_list	Array of **UserOrgRelation-ListResult** objects	Relationships between users and organizations.

Table 4-1597 UserOrgRelationListResult

Parameter	Type	Description
org_id	String	Organization ID.
relation_type	String	Relationship type.

Status code: 400

Table 4-1598 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error details.

Example Requests

Query the user list of the first 10 organizations.

```
/api/v1/tenant/users?org_id=&offset=0&limit=10
```

Example Responses

Status code: 200

Request succeeded.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
{
  "total" : 1,
  "users" : [ {
    "extension" : { },
    "user_name" : "zhangsan",
    "mobile" : "12345678901",
    "created_at" : "2022-03-31 16:46:02.964",
    "pwd_must_modify" : false,
    "updated_at" : "2022-03-31 16:48:44.073",
    "user_id" : "20220331164602949-904C-D475B60AE",
    "org_id" : "20220331135144180-0FA5-EE3B69068",
    "grade" : 1,
    "name" : "zhangsan",
    "disabled" : false,
    "pwd_change_at" : "2022-03-31 16:47:51.481",
    "locked" : false,
    "user_org_relation_list" : [ {
      "org_id" : "20220331135144180-0FA5-EE3B69068",
      "relation_type" : 1
    }, {
      "org_id" : "20220415103506608-AF59-5CC9081B9",
      "relation_type" : 0
    } ]
  } ]
}
```


Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.

Error Codes

See **Error Codes**.

4.3.7.7 Updating a User

Function

This API is used to modify a user.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

URI

PUT /v1/csms/users/{user_id}

Table 4-1599 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	User ID.

Request Parameters

Table 4-1600 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	It can be obtained by calling the IAM API. The token is the value of **X-Subject-Token** in the response header.

Table 4-1601 Request body parameters

Parameter	Mandatory	Type	Description
user_name	No	String	Username, which is a unique identifier in an enterprise.
mobile	No	String	Mobile number, which is unique in an enterprise.
org_code	No	String	Organization code.
name	No	String	Name.
email	No	String	Email address.
employee_id	No	String	Employee ID.
first_name	No	String	Name.
middle_name	No	String	Middle name.
last_name	No	String	Last name.
pwd_must_modify	No	String	Whether the password must be changed upon first login. The default value is **true**.
attr_gender	No	String	Gender. The value can be **unknown**, **male**, or **female**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
attr_birthday	No	String	Date of birth, in yyyy-mm-dd format
attr_nick_name	No	String	Alias.
attr_identity_type	No	String	Certificate type. The value can be: **id_card**: ID card **HongKong_Macau_Taiwan_residence_permit**: Residence permit for Hong Kong, Macao, and Taiwan residents **mainland_travel_permit_for_HongKong_Macao**: Chinese mainland travel permits for Hong Kong and Macao residents **mainland_travel_permit_for_Taiwan**: Chinese mainland travel permits for Taiwan residents **chinese_passport**: Chinese passport *__overseas_passport__: Foreign passport **overseas_driver_license**: Foreign driver license **officer_id: Military ID card **foreigner_residence_permit**: Residence permit for foreigners **other**: others
attr_identity_number	No	String	Certificate number.
attr_area	No	String	Country or region code.
attr_city	No	String	City.
attr_manager_id	No	String	Immediate superior.
attr_user_type	No	String	Personnel type. The value can be **regular** (formal), **intern** (internship), **dispatch** (labor dispatch), or **outsourcing** (labor outsourcing).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
attr_hire_date	No	String	Onboarding date, in yyyy-MM-dd format.
attr_work_place	No	String	Work location.
user_org_relation_list	No	Array of UserOrgRelationListOption objects	Relationships between users and organizations. The main organization information must be included if this parameter is set.
extension	No	String	Custom extended attribute.

Table 4-1602 UserOrgRelationListOption

Parameter	Mandatory	Type	Description
orgCode	Yes	String	Organization code.
relationType	Yes	String	Ownership. A user can only belong to one organization and can be mounted to at most nine organizations. The value can be **0** (mounting) or **1** (belonging).

Response Parameters

Status code: 200

Table 4-1603 Response body parameters

Parameter	Type	Description
user_id	String	User ID.

Status code: 400

Table 4-1604 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error details.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

Modify the username to **zhangsan**, mobile number to **12345678901**, and email address to **zhangsan@example.com**.

```
{
  "user_name" : "zhangsan",
  "org_code" : "10000",
  "name" : "zhangsan",
  "mobile" : "12345678901",
  "email" : "zhangsan@example.com",
  "employee_id" : "123456789",
  "pwd_must_modify" : false,
  "first_name" : "F",
  "middle_name" : "M",
  "last_name" : "L",
  "attr_gender" : "male",
  "attr_birthday" : "1990-02-01",
  "attr_nick_name" : "zhangsan",
  "attr_identity_type" : "id_card",
  "attr_identity_number" : "123456789",
  "attr_area" : "CN",
  "attr_city" : "xxx",
  "attr_manager_id" : "123456789",
  "attr_user_type" : "regular",
  "attr_hire_date" : "2021-04-01",
  "attr_work_place" : "xxx",
  "user_org_relation_list" : [ {
    "orgCode" : "10000",
    "relationType" : 1
  }, {
    "orgCode" : "TestOrg1",
    "relationType" : 0
  }, {
    "orgCode" : "TestOrg2",
    "relationType" : 0
  } ],
  "extension" : {
    "age" : "18"
  }
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "user_id" : "20210621095935811-5E16-6B3060..."
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Error Codes

See **Error Codes**.

4.3.7.8 Deleting a User

Function

This API is used to delete a user.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

DELETE /v1/csms/users/{user_id}

Table 4-1605 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	User ID.

Request Parameters

Table 4-1606 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The token is the value of **X-Subject-Token** in the response header.

Response Parameters

Status code: 204

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1607 Response body parameters

Parameter	Type	Description
-	String	-

Status code: 400

Table 4-1608 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error details.

Example Requests

Delete a specified user based on the imported user ID.

```
/api/v1/tenant/users/{user_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	Request succeeded.
400	Request failed.

Error Codes

See **Error Codes**.

4.3.7.9 Obtaining User Details

Function

This API is used to query user details based on the user ID.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

GET /v1/csms/users/{user_id}

Table 4-1609 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	User ID.

Request Parameters

Table 4-1610 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The token is the value of **X-Subject-Token** in the response header.

Response Parameters

Status code: 200

Table 4-1611 Response body parameters

Parameter	Type	Description
user_id	String	User ID.
org_id	String	Organization to which the user belongs.
user_name	String	Username.
name	String	Name.
mobile	String	Mobile number.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
email	String	Email address.
pwd_must_modify	Boolean	Whether the password must be changed upon first login.
pwd_change_at	String	Password change time.
created_at	String	Creation time.
updated_at	String	Last modification time.
disabled	Boolean	Disabled or not.
grade	Integer	Trust level.
locked	String	Locked or not.
extension	Object	Custom extended attribute.
user_org_relation_list	Array of **UserOrgRelation-ListResult** objects	Relationships between users and organizations.
domain_id	String	Tenant ID.

Table 4-1612 UserOrgRelationListResult

Parameter	Type	Description
org_id	String	Organization ID.
relation_type	String	Relationship type.

Status code: 400

Table 4-1613 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error details.

Example Requests

Query user details based on the imported user ID.

```
/v1/csms/users/{user_id}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Responses

Status code: 200

Request succeeded.


```
{
  "user_id" : "20220413165737132-3BA0-91FCA2CB7",
  "org_id" : "20220117125622909-9346-35755733F",
  "domain_id" : "d4e559b49b3b403da5279723299ed4a6",
  "user_name" : "zhangsan",
  "name" : "zhangsan",
  "mobile" : "12345678901",
  "email" : "zhangsan@example.com",
  "pwd_must_modify" : true,
  "pwd_change_at" : "2022-04-14 10:14:01.988",
  "created_at" : "2022-04-13 16:57:36.532",
  "updated_at" : "2022-04-14 10:14:01.979",
  "disabled" : false,
  "grade" : 1,
  "locked" : false,
  "extension" : { },
  "user_org_relation_list" : [ {
    "org_id" : "20220117125622909-9346-35755733F",
    "relation_type" : 1
  }, {
    "org_id" : "20220415103506608-AF59-5CC9081B9",
    "relation_type" : 0
  } ]
}
```


Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.

Error Codes

See **Error Codes**.

4.3.8 Secret Detection Management

4.3.8.1 Checking the Imported Secret Strength

Function

This API is used to check the imported secrets. It is used only in the secret vault scenario.

Calling Method

For details, see **Calling APIs**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/{project_id}/secrets/checker/check

Table 4-1614 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-1615 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-1616 Request body parameters

Parameter	Mandatory	Type	Description
type	Yes	String	Secret detection type.
data	Yes	Object	Request data body corresponding to secret detection.

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1617 Response body parameters

Parameter	Type	Description
type	String	Secret detection type.
data	Object	Response data body corresponding to secret detection.

Status code: 400

Table 4-1618 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.

Error Codes

See **Error Codes**.

4.3.8.2 Obtaining the Tenant Secret Detection Configuration

Function

This API is used to obtain the secret detection configuration of a tenant. It is used only in the secret vault scenario.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

GET /v1/{project_id}/secrets/checker/config

Table 4-1619 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-1620 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-1621 Response body parameters

Parameter	Type	Description
checking_secret_strength	Boolean	Whether secret strength detection is enabled.

Status code: 400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1622 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1623 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Response body of the tenant secret detection configuration.
400	Invalid request parameter.
500	Internal server error.

Error Codes

See **Error Codes**.

4.3.8.3 Changing the Tenant Secret Detection Configuration

Function

This API is used to change the secret detection configuration of a tenant. It is used only in the secret vault scenario.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/{project_id}/secrets/checker/config

Table 4-1624 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-1625 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of **X-Subject-Token** in the response header is the user token.

Table 4-1626 Request body parameters

Parameter	Mandatory	Type	Description
checking_secret_strength	No	Boolean	Whether secret strength detection is enabled.

Response Parameters

Status code: 200

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1627 Response body parameters

Parameter	Type	Description
checking_secret_strength	Boolean	Whether secret strength detection is enabled.

Status code: 400

Table 4-1628 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1629 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Response body of the tenant secret detection configuration.
400	Invalid request parameter.
500	Internal server error.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Error Codes

See **Error Codes**.

4.3.9 Authorization Management

4.3.9.1 Authorization Operations

Function

This API is used to authorize operations.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/{project_id}/csms/grants

Table 4-1630 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-1631 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Token of the authenticated user.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1632 Request body parameters

Parameter	Mandatory	Type	Description
resource_id	Yes	String	Resource ID.
type	Yes	String	Resource type, which can be **SECRET** or **GROUP**.
grantee_type	Yes	String	Authorized type, which can be **0** (user) or **2** (group).
grantee_target_id	Yes	String	Authorized ID.
validity_time	No	String	Expiration time.

Response Parameters

Status code: 200

Table 4-1633 Response body parameters

Parameter	Type	Description
uuid	String	Authorization ID, which is available when the authorization is granted to an individual.
resourceId	String	Resource ID.
type	String	Authorization type, which can be **SECRET** or **GROUP**.
granteeUser	String	Authorized user ID.
createTime	Long	Creation time.
updateTime	Long	Update time.
validityTime	Long	Validity period.
state	Integer	Status.
signature	String	Signature.

Status code: 400

Table 4-1634 Response body parameters

Parameter	Type	Description
error_code	String	Error codes

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Type	Description
error_msg	String	Error description

Status code: 401

Table 4-1635 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1636 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1637 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1638 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1639 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1640 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

```
{
  "resource_id" : "demo",
  "type" : "group",
  "grantee_type" : "0",
  "grantee_target_id" : "user_01"
}
```

Example Responses

Status code: 200

Authorization response.

```
{
  "data" : {
    "uuid" : "1c087a48-0d48-4222-9d34-ae43d30b27d2",
    "type" : "SECRET",
    "resourceId" : "43d643d2-95ec-4b0f-8020-a84f3ce931cc",
    "granteeUser" : "user_01",
    "state" : 0,
    "signature" : "",
    "createTime" : "2022-11-09 16:37:24",
    "updateTime" : "2022-11-09 16:37:24",
    "validityTime" : null
  }
}
```

Status Codes

Status Code	Description
200	Authorization response.
400	Invalid request parameter.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Description
401	Username and password are required for the requested page.
403	Authentication failed.
404	Resource not found.
500	Internal server error.
502	Failed to complete the request. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.9.2 Deleting an Authorization

Function

This API is used to delete an authorization.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

DELETE /v1/{project_id}/csms/grants

Table 4-1641 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1642 Query Parameters

Parameter	Mandatory	Type	Description
grantee_user	No	String	Authorized user ID.
resource_id	Yes	String	Authorized resource ID.

Request Parameters

Table 4-1643 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.

Response Parameters

Status code: 204

Deleted successfully.

Status code: 400

Table 4-1644 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1645 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1646 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1647 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1648 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1649 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1650 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
204	Deleted successfully.
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.
404	Resource not found.
500	Internal server error.
502	Failed to complete the request. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.9.3 Authorization List

Function

This API indicates the authorization list.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

URI

GET /v1/{project_id}/csms/grants

Table 4-1651 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 4-1652 Query Parameters

Parameter	Mandatory	Type	Description
resource_id	Yes	String	Resource ID.

Request Parameters

Table 4-1653 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.

Response Parameters

Status code: 200

Table 4-1654 Response body parameters

Parameter	Type	Description
id	String	Authorization ID, which is available when the authorization is granted to an individual.
name	String	Authorization name.
type	String	Authorization type, which can be **SECRET** or **GROUP**.
grantee_user	Array of **GrantUserInfo** objects	Authorized user information.
create_time	Long	Creation time.
update_time	Long	Update time.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1655 GrantUserInfo

Parameter	Type	Description
user_id	String	Resource ID.
user_name	String	Name.
create_time	Long	Creation time.
validity_time	Long	Validity period.

Status code: 400

Table 4-1656 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1657 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1658 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1659 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1660 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1661 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1662 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

Status code: 200

Authorization list.

```
{
  "data" : {
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "id" : "43d643d2-95ec-4b0f-8020-a84f3ce931cc",
    "grantee_user" : [ {
      "user_id" : "111",
      "user_name" : "null",
      "create_time" : "2022-11-09 16:37:24",
      "validity_time" : null
    } ],
    "create_time" : "2022-11-09 16:37:24",
    "update_time" : "2022-11-09 16:37:24"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.kms.v2.region.KmsRegion;
import com.huaweicloud.sdk.kms.v2.*;
import com.huaweicloud.sdk.kms.v2.model.*;


public class ListGrantsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
                .withProjectId(projectId)
                .withAk(ak)
                .withSk(sk);

        KmsClient client = KmsClient.newBuilder()
                .withCredential(auth)
                .withRegion(KmsRegion.valueOf("<YOUR REGION>"))
                .build();
        ListGrantsRequest request = new ListGrantsRequest();
        try {
            ListGrantsResponse response = client.listGrants(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkkms.v2.region.kms_region import KmsRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkkms.v2 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = KmsClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(KmsRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListGrantsRequest()
        response = client.list_grants(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    kms "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/kms/v2/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := kms.NewKmsClient(
        kms.KmsClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        Build())

    request := &model.ListGrantsRequest{}
    response, err := client.ListGrants(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in **API Explorer**. SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Authorization list.
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.
404	Resource not found.
500	Internal server error.
502	Failed to complete the request. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.9.4 Updating an Authorization

Function

This API is used to update an authorization.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

PUT /v1/{project_id}/csms/grants

Table 4-1663 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 4-1664 Query Parameters

Parameter	Mandatory	Type	Description
resource_id	Yes	String	Resource ID.

Request Parameters

Table 4-1665 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.

Table 4-1666 Request body parameters

Parameter	Mandatory	Type	Description
resource_id	Yes	String	Resource ID.
type	Yes	String	Resource type, which can be **SECRET** or **GROUP**.
grantee_type	Yes	String	Authorized type, which can be **0** (user) or **2** (group).
grantee_target_id	Yes	String	Authorized ID.
validity_time	No	String	Expiration time.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Response Parameters

Status code: 200

Table 4-1667 Response body parameters

Parameter	Type	Description
uuid	String	Authorization ID, which is available when the authorization is granted to an individual.
resourceId	String	Resource ID.
type	String	Authorization type, which can be **SECRET** or **GROUP**.
granteeUser	String	Authorized user ID.
createTime	Long	Creation time.
updateTime	Long	Update time.
validityTime	Long	Validity period.
state	Integer	Status.
signature	String	Signature.

Status code: 400

Table 4-1668 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

Table 4-1669 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1670 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1671 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1672 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1673 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 504

Table 4-1674 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Example Requests

```
{
  "resource_id" : 21,
  "type" : "SECRET",
  "grantee_type" : "0",
  "grantee_target_id" : 5
}
```

Example Responses

Status code: 200

Authorization update response.

```
{
  "data" : {
    "uuid" : "1c087a48-0d48-4222-9d34-ae43d30b27d2",
    "type" : "SECRET",
    "resourceId" : "43d643d2-95ec-4b0f-8020-a84f3ce931cc",
    "granteeUser" : "user_01",
    "state" : 0,
    "signature" : "",
    "createTime" : "2022-11-09 16:37:24",
    "updateTime" : "2022-11-09 16:37:24",
    "validityTime" : null
  }
}
```

Status Codes

Status Code	Description
200	Authorization update response.
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.
404	Resource not found.
500	Internal server error.
502	Failed to complete the request. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

4.3.10 Password Management

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.3.10.1 Generating a Random Password

Function

This API is used to generate a random password.

Calling Method

For details, see **Calling APIs**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see **Permissions Policies and Supported Actions** for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/{project_id}/csms/generate-password

Table 4-1675 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-1676 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.

Table 4-1677 Request body parameters

Parameter	Mandatory	Type	Description
password_policy_name	No	String	Policy name.
length	No	Integer	Length. The default value is **32**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
exclude_characters	No	String	Character to be excluded.
exclude_lowercase	No	Boolean	Exclude lowercase letters. The default value is **false**.
exclude_uppercase	No	Boolean	Exclude uppercase letters. The default value is **false**.
exclude_numbers	No	Boolean	Exclude digits. The default value is **false**.
exclude_punctuation	No	Boolean	Exclude symbols. The default value is **false**.
include_space	No	Boolean	Spaces are included. The default value is **false**.
require_each_included_type	No	Boolean	Types that must be included. The default value is **false**.

Response Parameters

Status code: 200

Table 4-1678 Response body parameters

Parameter	Type	Description
-	String	-

Status code: 400

Table 4-1679 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 401

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-1680 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 403

Table 4-1681 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 404

Table 4-1682 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 500

Table 4-1683 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Status code: 502

Table 4-1684 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status code: 504

Table 4-1685 Response body parameters

Parameter	Type	Description
error_code	String	Error codes
error_msg	String	Error description

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	password
400	Invalid request parameter.
401	Username and password are required for the requested page.
403	Authentication failed.
404	Resource not found.
500	Internal server error.
502	Failed to complete the request. The server has received an invalid response.
504	Gateway timed out.

Error Codes

See **Error Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5 Historical APIs

Managing SSH Key Pairs (V2.1)
Managing SSH Key Pairs (V2)

5.1 Managing SSH Key Pairs (V2.1)

5.1.1 Querying the List of SSH Key Pairs (V2.1)

Function

This API is used to query the list of SSH key pairs.

URI

- URI format
  GET /v2.1/{project_id}/os-keypairs
- Parameter description

Table 5-1 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Requests

None

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Responses

Table 5-2 Response parameters

Parameter	Mandatory	Type	Description
keypairs	Yes	Array of objects	SSH key pair information list. For details, see **Table 5-3**.

Table 5-3 keypairs field description

Parameter	Mandatory	Type	Description
keypair	Yes	Object	SSH key pair information, see **Table 5-4**.

Table 5-4 keypair field description

Parameter	Mandatory	Type	Description
fingerprint	Yes	String	Fingerprint information about an SSH key pair
name	Yes	String	Name of an SSH key pair
public_key	Yes	String	Public key information about an SSH key pair
is_key_protection	Yes	Boolean	Whether the private key of the SSH key pair is managed and protected.

Examples

- Example request

  None

- Example response

```
{
 "keypairs": [{
   "keypair": {
    "fingerprint": "15:b0:f8:b3:f9:48:63:71:cf:7b:5b:38:6d:44:2d:4a",
    "name": "keypair-601a2305-4f25-41ed-89c6-2a966fc8027a",
    "public_key": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQC+Eo/
RZRngaGTkFs7I62ZjsIlO79KklKbMXi8F+KITD4bVQHHn+kV
+4gRgkgCRbdoDqoGfpaDFs877DYX9n4z6FrAIZ4PES8TNKhatifpn9NdQYWA+IkU8CuvlEKGuFpKRi/
k7JLos/gHi2hy7QUwgtRvcefvD/vgQZOVw/mGR9Q== Generated-by-Nova\n",
    "is_key_protection": true
   }
 }
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
 ]
}
```

or

```
{
    "error_code": "KPS.XXXX",
    "error_msg": "XXXX"
}
```

Status Codes

For details, see **Status Codes**.

5.1.2 Querying Details About an SSH Key Pair (V2.1)

Function

This API is used to query details about an SSH key pair.

URI

- URI format

  GET /v2.1/{project_id}/os-keypairs/{keypair_name}
- Parameter description

  Table 5-5 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keypair_name	Yes	String	Name of an SSH key pair

Requests

None

Responses

Table 5-6 Response parameters

Parameter	Mandatory	Type	Description
keypair	Yes	Object	SSH key pair information. For details, see **Table 5-7**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-7 keypair field description

Parameter	Mandatory	Type	Description
public_key	Yes	String	Public key information about an SSH key pair
name	Yes	String	Name of an SSH key pair
fingerprint	Yes	String	Fingerprint information about an SSH key pair
created_at	Yes	String	Time when an SSH key pair is created The value is a timestamp expressed in the number of seconds since 00:00:00 UTC on January 1, 1970.
deleted	Yes	Boolean	Tag that indicates an SSH key pair is deleted
deleted_at	Yes	String	Time when an SSH key pair is deleted The value is a timestamp expressed in the number of seconds since 00:00:00 UTC on January 1, 1970.
id	Yes	String	ID of an SSH key pair
updated_at	Yes	String	Time when an SSH key pair is updated The value is a timestamp expressed in the number of seconds since 00:00:00 UTC on January 1, 1970.
user_id	Yes	String	User to whom an SSH key pair belongs
is_key_protection	Yes	Boolean	Whether the private key of the SSH key pair is managed and protected.
description	Yes	String	Description of an SSH key pair

Examples

- Example request

  None

- Example response

```
{
    "keypair": {
        "created_at": "2014-05-07T12:06:13.681238",
        "deleted": false,
        "deleted_at": null,
        "fingerprint": "9d:00:f4:d7:26:6e:52:06:4c:c1:d3:1d:fd:06:66:01",
        "id": 1,
        "name": "keypair-3582d8b7-e588-4aad-b7f7-f4e76f0e4314",
        "public_key": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDYJrTVpcMwFqQy/
oMvtUSRofZdSRHEwrsX8AYkRvn2ZnCXM+b6+GZ2NQuuWj+ocznlnwiGFQDsL/yeE+/
kurqcPJFKKp60mToXIMyzioFxW88fJtwEWawHKAclbHWpR1t4fQ4DS+/sIbX/
Yd9btlVQ2tpQjodGDbM9Tr9/+/3i6rcR+EoLqmbgCgAiGiVV6VbM2Zx79yUwd
+GnQejHX8BlYZoOjCnt3NREsITcmWE9FVFy6TnLmahs3FkEO/
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
QGgWGkaohAJlsgaVvSWGgDn2AujKYwyDokK3dXyeX3m2Vmc3ejiqPa/C4nRrCOlko5nSgV/
9IXRx1ERImsqZnE9usB Generated-by-Nova\n",
        "updated_at": null,
        "user_id": "fake",
        "is_key_protection": true,
        "description": "keypair test"
    }
}
```

or

```
{
    "error_code": "KPS.XXXX",
    "error_msg": "XXXX"
}
```

Status Codes

For details, see **Status Codes**.

5.1.3 Creating and Importing an SSH Key Pair (V2.1)

Function

This API is used to create and import an SSH key pair, and allows you to manage the private key in the cloud.

URI

- URI format

  POST /v2.1/{project_id}/os-keypairs
- Parameter description

  Table 5-8 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Requests

NOTE

When creating an SSH key pair, you only need to set the **name**. When importing an SSH key pair, you must set the **public_key** parameter.

Table 5-9 Request parameters

Parameter	Mandatory	Type	Description
keypair	Yes	Object	Information about the created or imported SSH key pair. For details, see **Table 5-10**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-10 keypair field description

Parameter	Mandatory	Type	Description
public_key	No	String	Character string of a public key to be imported
name	Yes	String	Name of an SSH key pair A new key pair cannot use the same name as an existing one. The value contains a maximum of 64 characters, including only letters, digits, underscores(_), and hyphens (-).
user_id	No	String	ID of the user to whom an SSH key pair belongs
key_protection	No	Object	Management and protection of the private key of an SSH key pair. For details, see **Table 5-11**.

Table 5-11 key_protection field description

Parameter	Mandatory	Type	Description
private_key	No	String	Character string of a private key to be imported
encryption	Yes	Object	Method to encrypt and store private keys. For details, see **Table 5-12**.

Table 5-12 encryption field description

Parameter	Mandatory	Type	Description
type	Yes	String	Value options: **kms** or **default** • **default** refers to the default encryption method. It is applicable to sites where the KMS service is unavailable. • **kms** indicates that the KMS service is leveraged for the encryption. If the KMS service is unavailable, set this parameter to **default**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
kms_key_name	No	String	Name of a KMS key. If **type** is set to **kms**, enter the name of the key obtained from KMS.

Responses

Table 5-13 Response parameters

Parameter	Mandatory	Type	Description
keypair	Yes	Object	SSH key pair information. For details, see **Table 5-14**.

Table 5-14 keypair field description

Parameter	Mandatory	Type	Description
fingerprint	Yes	String	Fingerprint information about an SSH key pair
name	Yes	String	Name of an SSH key pair
public_key	Yes	String	Public key information about an SSH key pair
private_key	Yes	String	Private key information about an SSH key pair. • The information about the private key is contained in the response for creating an SSH key pair. • The information about the private key is not contained in the response for importing an SSH key pair.
user_id	Yes	String	User to whom an SSH key pair belongs

Examples

- Creating an SSH key pair
  - Request example for creating an SSH key pair

```
{
    "keypair": {
        "name": "demo1"
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    }
}
```

  - Response example for creating an SSH key pair

```
{
    "keypair": {
        "public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCXKzohKbFOqubYNunFNsrEYlk9NEIJIFvbmTe/
LTeMzFIPKM53Zu2sYr/uuNcziPkWpFchXdkD+O/
Bf2ZzKaR1DYPMWss9TkaqU4RQ7CIBW7ChJF1Qzc1JPRBmKe6e8qs1QBBoS1QvXgSjbuf2Fb1yncSb
phmQV8+5KA8xkxz4XdM1/gSAZZ14rJrMjgp7jCdgxWiHNcDuKxaPt+0eO8rEG/gxR7J0b9Uk53ao/
xjLoKXYdLLiYUaha0fHdW3t6Lw1NdzUMmKnlLqN9O37Tbg7vM0nN4UJt0XXvM45KfnJiMx0HUKXd
WkUj9cE8VBDPw/gBbQzSpJHgQFG7mNDZubN Generated-by-Nova\n",
        "private_key": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEAlys6ISmxTqrm2DbpxTbKxGJZPTRCCSBb25k3vy03jMxSDyjO\nd2btrGK/
7rjXM4j5FqRXIV3ZA/jvwX9mcymkdQ2DzFrLPU5GqlOEUOwiAVuwoSRd
\nUM3NST0QZinunvKrNUAQaEtUL14Eo27n9hW9cp3Em6YZkFfPuSgPMZMc+F3TNf4E
\ngGWdeKyazI4Ke4wnYMVohzXA7isWj7ftHjvKxBv4MUeydG/VJOd2qP8Yy6Cl2HSy
\n4mFGoWtHx3Vt7ei8NTXc1DJip5S6jfTt+024O7zNJzeFCbdF17zOOSn5yYjMdB1C\nl3VpFI/
XBPFQQz8P4AW0M0qSR4EBRu5jQ2bmzQIDAQABAoIBAFwm1s3Gi7bICec+
\nOm2lhCAJUBs2UxcbKcQJd+lL2DQ1jcR9/LbfAP34SMZu2Ykp86Zw0kid3CBGzWko
\nj7yeYwmUDocxxfl+USedt+hYujYXvenNsDEE9CK0Xd3ZrAQrLGFOx3G8kfo6FxvG\nDRN/
lzhaorK7o5PRY+icWf6/joZ8Q96scHmm0ob5rtBkUYcek+ckf3mLVIpzzdKA
\ndkSi57M78zwDA89MpVABEoO1DPVxEqrrMQZy5UnAmeGHh16mPS4qMCokPVz36pSG
\nIWSqHnVKzsbxvw5Da9y69NmpSi2E1wqDaU9IzwnLyQpHnE1nXsWmxNqKTHlDBbnb
\nXPGFdcECgYEAxf4IMqYBeBiq
+7RVwcTcT4gpApJmywigwMFaaX35E3O53ja8hk1/\n5OCRnvK7yrt9wnWY8DIh8GPJptKzuTb/l/
14L4kE1MYm7Gpho5SwXV5BqtjgjfZm\nQVNpWruXEugXALcfbHiH+peO
+3AmwgIqgkOLPLxY1Duw6/miDB8bOfECgYEAw3VO\nl9edXExJvJvSzAopSNmw
+ExpUZTgS3L2Pyn21QhfwNHyxPH8fNNKv0/x9ZzBn25U
\nUxXTPPbLFV3cq7kfuYFW0OZkh8QjCPDkIE116E2QvacxqkBuW774xr5msfWdxpcp
\nwccgWKci1vEHLtqj3RTNMFKcXtj4QrCES4ZsPp0CgYEAhzYYux4LWszd188r0Yxz
\nOA0wlIUOlhFqVri02d4hv1sEz/Bphv5eHRwP1pDGFok8NRTCQSa7bsN27uptuksl\n
+e8rqKrWFcjMxB9SVrgwSVMZXWeG0uw2oN4p0MDTRyIgs2hbmWQm2Mev6Z6JmWyJ
\nQzSFXhDySN4K0NxGAiksGsECgYAJvZTXGFWtPdgG4DUXGgKIsOCS3yv4dtTerbH7\n39l/
MFWlRFE242BT0CvPcOp79P3pNhRZt6K5TQs921md7THZisqKypCD+5BLZ8XW\nnkWb
+BGYgfaFp4RYaiH3tZFkmPrt5KaeE5BXGq0vzP8wpJC5+cln+RX13BYzLJzL
\nLr3COQKBgDJjY0qop3aSG+1tSkMJtOFdb2+qXiqaE+Wxv03SOkPx8LBz+taNz+DE
\nR7THDNXSrS85WVc3ozE8hULBX12iIWpr5kb5lRaw3ZgX6wBnSSpdQu49v3nFoGJk\nUWY95pQ/
BWQaX0q4KxzRVxup+7gwT5sKFXU+ktFtsGMYoDoSzbZS\n-----END RSA PRIVATE KEY-----\n",
        "user_id": "e4f380899b1248918f3d37098dc63746",
        "name": "demo123",
        "fingerprint": "49:ef:73:2b:9b:7f:2e:0c:58:d3:e3:42:8e:28:04:3b"
    }
}
```

    or

```
{
    "error_code": "KPS.XXXX",
    "error_msg": "XXXX"
}
```

- Creating an SSH key pair and managing the private key in the cloud
  - Request example for creating an SSH key pair and managing the private key in the cloud

```
{
    "keypair": {
        "name": "demo2",
        "key_protection": {
            "encryption": {
                "type": "kms",
                "kms_key_name": "demo"
            }
        }
    }
}
```

  - Response example for creating an SSH key pair and managing the private key in the cloud

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
{
   "keypair": {
      "public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCXKzohKbFOqubYNunFNsrEYlk9NEIJIFvbmTe/
LTeMzFIPKM53Zu2sYr/uuNcziPkWpFchXdkD+O/
Bf2ZzKaR1DYPMWss9TkaqU4RQ7CIBW7ChJF1Qzc1JPRBmKe6e8qs1QBBoS1QvXgSjbuf2Fb1yncSb
phmQV8+5KA8xkxz4XdM1/gSAZZ14rJrMjgp7jCdgxWiHNcDuKxaPt+0eO8rEG/gxR7J0b9Uk53ao/
xjLoKXYdLLiYUaha0fHdW3t6Lw1NdzUMmKnlLqN9O37Tbg7vM0nN4UJt0XXvM45KfnJiMx0HUKXd
WkUj9cE8VBDPw/gBbQzSpJHgQFG7mNDZubN Generated-by-Nova\n",
      "private_key": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEAlys6ISmxTqrm2DbpxTbKxGJZPTRCCSBb25k3vy03jMxSDyjO\nd2btrGK/
7rjXM4j5FqRXIV3ZA/jvwX9mcymkdQ2DzFrLPU5GqlOEUOwiAVuwoSRd
\nUM3NST0QZinunvKrNUAQaEtUL14Eo27n9hW9cp3Em6YZkFfPuSgPMZMc+F3TNf4E
\ngGWdeKyazI4Ke4wnYMVohzXA7isWj7ftHjvKxBv4MUeydG/VJOd2qP8Yy6Cl2HSy
\n4mFGoWtHx3Vt7ei8NTXc1DJip5S6jfTt+024O7zNJzeFCbdF17zOOSn5yYjMdB1C\nl3VpFI/
XBPFQQz8P4AW0M0qSR4EBRu5jQ2bmzQIDAQABAoIBAFwm1s3Gi7bICec+
\nOm2lhCAJUBs2UxcbKcQJd+lL2DQ1jcR9/LbfAP34SMZu2Ykp86Zw0kid3CBGzWko
\nj7yeYwmUDocxxfl+USedt+hYujYXvenNsDEE9CK0Xd3ZrAQrLGFOx3G8kfo6FxvG\nDRN/
lzhaorK7o5PRY+icWf6/joZ8Q96scHmm0ob5rtBkUYcek+ckf3mLVIpzzdKA
\ndkSi57M78zwDA89MpVABEoO1DPVxEqrrMQZy5UnAmeGHh16mPS4qMCokPVz36pSG
\nIWSqHnVKzsbxvw5Da9y69NmpSi2E1wqDaU9IzwnLyQpHnE1nXsWmxNqKTHlDBbnb
\nXPGFdcECgYEAxf4IMqYBeBiq
+7RVwcTcT4gpApJmywigwMFaaX35E3O53ja8hk1/\n5OCRnvK7yrt9wnWY8DIh8GPJptKzuTb/l/
14L4kE1MYm7Gpho5SwXV5BqtjgjfZm\nQVNpWruXEugXALcfbHiH+peO
+3AmwgIqgkOLPLxY1Duw6/miDB8bOfECgYEAw3VO\nl9edXExJvJvSzAopSNmw
+ExpUZTgS3L2Pyn21QhfwNHyxPH8fNNKv0/x9ZzBn25U
\nUxXTPPbLFV3cq7kfuYFW0OZkh8QjCPDkIE116E2QvacxqkBuW774xr5msfWdxpcp
\nwccgWKci1vEHLtqj3RTNMFKcXtj4QrCES4ZsPp0CgYEAhzYYux4LWszd188r0Yxz
\nOA0wlIUOlhFqVri02d4hv1sEz/Bphv5eHRwP1pDGFok8NRTCQSa7bsN27uptuksl\n
+e8rqKrWFcjMxB9SVrgwSVMZXWeG0uw2oN4p0MDTRyIgs2hbmWQm2Mev6Z6JmWyJ
\nQzSFXhDySN4K0NxGAiksGsECgYAJvZTXGFWtPdgG4DUXGgKIsOCS3yv4dtTerbH7\n39l/
MFWlRFE242BT0CvPcOp79P3pNhRZt6K5TQs921md7THZisqKypCD+5BLZ8XW\nnkWb
+BGYgfaFp4RYaiH3tZFkmPrt5KaeE5BXGq0vzP8wpJC5+cln+RX13BYzLJzL
\nLr3COQKBgDJjY0qop3aSG+1tSkMJtOFdb2+qXiqaE+Wxv03SOkPx8LBz+taNz+DE
\nR7THDNXSrS85WVc3ozE8hULBX12iIWpr5kb5lRaw3ZgX6wBnSSpdQu49v3nFoGJk\nUWY95pQ/
BWQaX0q4KxzRVxup+7gwT5sKFXU+ktFtsGMYoDoSzbZS\n-----END RSA PRIVATE KEY-----\n",
      "user_id": "e4f380899b1248918f3d37098dc63746",
      "name": "demo123",
      "fingerprint": "49:ef:73:2b:9b:7f:2e:0c:58:d3:e3:42:8e:28:04:3b"
   }
}
```

- Importing the public key of the SSH key pair
  - Request example for importing the public key of an SSH key pair

    ```
    {
       "keypair": {
          "public_key": "ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAABAQCyNtFZM04PFxERvZU5OBKTKr3mtRZABe5/+zX81lTgDF
    CBfq6OXia47M4qXOa3ciBEKKZF+fMfs8U2UNB9aK1R/
    uORsoEFtxSgZnWG6p4Ct1vnrqwDD934VaDFPEn+h3JeAfvTB
    +Ag1YQ9zh9uYyE9Z3qZcC9+Ui93BDGdBtQeav4odxdwXcr2mT2jJV0nsocV0O4UcKM8BaIm8eqbcro
    ZEkyxqT3mUoSbmGx1hrngjBsP1ufgwJ6D85LFGQC1SjIOLvsR9i6v41BaLF8/
    kygvKOh2HlNVSMx38g52sTqoQ/xb3f8vR1VDXliAuD0frrG2Fy5wK4rOAnjuX9nh0bC9 Generated-
    by-Nova\n",
          "name": "demo3"
       }
    }
    ```

  - Response example for importing the public key of an SSH key pair

    ```
    {
       "keypair": {
          "public_key": "ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAABAQCyNtFZM04PFxERvZU5OBKTKr3mtRZABe5/+zX81lTgDF
    CBfq6OXia47M4qXOa3ciBEKKZF+fMfs8U2UNB9aK1R/
    uORsoEFtxSgZnWG6p4Ct1vnrqwDD934VaDFPEn+h3JeAfvTB
    +Ag1YQ9zh9uYyE9Z3qZcC9+Ui93BDGdBtQeav4odxdwXcr2mT2jJV0nsocV0O4UcKM8BaIm8eqbcro
    ZEkyxqT3mUoSbmGx1hrngjBsP1ufgwJ6D85LFGQC1SjIOLvsR9i6v41BaLF8/
    kygvKOh2HlNVSMx38g52sTqoQ/xb3f8vR1VDXliAuD0frrG2Fy5wK4rOAnjuX9nh0bC9 Generated-
    by-Nova\n",
          "user_id": "e4f380899b1248918f3d37098dc63746",
    ```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        "name": "demo1",
        "fingerprint": "b4:9a:c3:12:c4:90:bf:8e:7a:e2:70:10:c3:00:55:3f"
    }
}
```

or

```
{
    "error_code": "KPS.XXXX",
    "error_msg": "XXXX"
}
```

- Importing the public key of the SSH key pair and managing the private key in the cloud
  - Request example for importing the public key of an SSH key pair and managing the private key in the cloud

```
{
    "keypair": {
        "public_key": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDb26UrW0htRbE/
Ygf8EPhzanBCc+5yEhkgmeSb2hTe48YRE5FdJKH6tueyj+vw5guoKjAITLjqZCqffGYXz/
7aXpFt244b9tTzh2l43uNtEZC+XZtc6KiBgfWupFI8O2i9YjJqdadsr+4Ad4AtIBbF++qsSJN4YycPX//
Gl8ja6AGPy4sdv8DZ40Gr8d+dMQ4pAsnUEtZ3jJ6NLdQU2CE1JhBdg3hbVbeh44gqQtSjhxWaSTlr
+NbVxSERtXXpsQWsid6qM1RhqH2+02cqXq5oNs4JLdu56pcTgSO5azTsGYJi6j5qp5BAdjMrFtHjbaeV
VWtkO1XQxfpueCJ470lx Generated-by-Nova\n",
        "name": "demo4",
        "key_protection": {
            "private_key": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEpQIBAAKCAQEA29ulK1tIbUWxP2IH/BD4c2pwQnPuchIZIJnkm9oU3uPGEROR\nXSSh
+rbnso/r8OYLqCowCEy46mQqn3xmF8/+2l6RbduOG/bU84dpeN7jbRGQvl2b
\nXOiogYH1rqRSPDtovWIyanWnbK/uAHeALSAWxfvqrEiTeGMnD1//xpfI2ugBj8uL\nHb/A2eNBq/
HfnTEOKQLJ1BLWd4yejS3UFNghNSYQXYN4W1W3oeOIKkLUo4cVmkk5\na/
jW1cUhEbV16bEFrIneqjNUYah9vtNnKl6uaDbOCS3bueqXE4EjuWs07BmCYuo+
\naqeQQHYzKxbR422nlVVrZDtV0MX6bngieO9JcQIDAQABAoIBAAVSEXM1KFGMqDdy
\ndeMBviF85+6Tw6d7DKSfVMr4whyKwpZTNOdeJZVdq8nEdd9Eke+l5bets6PofKeT
\naR0WaYJ7W2WfNJc0p/6kvkawjixrimcw+LuM3dcUgA+T5nGStnwuzi2JX13f/BCC
\n09VDu4lbCVjWAMufCqjyl8wEjFXP0Amhu8fpDvqHuhGvDkoVWRm9vDEeyz71P25K\n/
UUs7kXw5Qv0VRcm15b+2jO6tii3RTo+JaTvkYXoI/qrOjiQhQD88geiOPQVuffa
\nzJhDw4/2GdHaCwEN6mzwKCYCfcPTRbM503F1YlceiP9w2qScToao
+5B2okN9cIE8\nTV4vmIkCgYEA+vo/TKqFep2D6DPY3dNRu2bHIYikBMtYMCIKJ1bgQ1xS/FjEJfSj
\notdDcBEik+0VEV05BCHNduTiMt6rTUD9fpqDduV8PfsskAAZZjndbyUEGP/KrCvS\nJsd2BFa2G7In/
3wz3zw+3P77Aegb+zHJfDyqYWReNkYy5tSsaZ9Oz38CgYEA4EH5\nIXQPhJt9683JmK/
INiyhW6WqKOAZkvjKpUpdUpGdVHJI/9dfUYI9wxnybgAkOZVL\noErxMTdRCDev8nVAq/OwC/
4jI5YnBGkN3ZRxIkCrepzwxIXgWeJiwWqsvdDbosfM
\nN0Q6PvUnPTXEly8RGcH9ABTQvQ9Nq4rQyjQvXw8CgYEAuK8hmWb55iq3AE32zfVM\n9ZxB
+Jk2KRkBghnqYtx5Fth/cJZZcJy/NXs2cucJDNWvZSG2bSX6rfzrvwdAAw9J\n
+rn0968TaADG4AhSqHj4S2tvwn2oRF3SvRqV68drJqJI8KYS/bi1gaZYSyTkQkp2\nu
+dgcV6MPWAW4OmrHeZO9j0CgYEAkY8Az4/vipkKkIWP9oUSJOevDDdpTQK4VscZ
\ncVPlYvSU8/0CGN2IRvWMdRhgXLnGyYF4BuDd0J4hAH50u6ETiwivGfmogS6ywJAX\nqdzx2dOz
+e/n7wceafkhNH2zBbmM9glNKgok7DxfbcF6is7IALoDJ4xbOHu4ZEHD
\n55sbrE0CgYEAuOuiISgfbujENFFPW0nvUmNqbkAH5YW1oUIWYA+64z7wcWyvzxRS
\nYml2XLWyrJy3JNzHpLoe4mCBxz+HGrftZ0/qfQ/WDZrY/Djp7/xIkPyI9EwsRTYC
\nr1PtWvVws3y3hgdo6WVQMaeUqtLSiTugyuuPqidH+/QtwxObunNH6Ns=\n-----END RSA
PRIVATE KEY-----\n",
            "encryption": {
                "type": "kms",
                "kms_key_name": "testName"
            }
        }
    }
}
```

  - Response example for importing the public key of an SSH key pair and managing the private key in the cloud

```
{
    "keypair": {
        "public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCyNtFZM04PFxERvZU5OBKTKr3mtRZABe5/+zX81lTgDF
CBfq6OXia47M4qXOa3ciBEKKZF+fMfs8U2UNB9aK1R/
uORsoEFtxSgZnWG6p4Ct1vnrqwDD934VaDFPEn+h3JeAfvTB
+Ag1YQ9zh9uYyE9Z3qZcC9+Ui93BDGdBtQeav4odxdwXcr2mT2jJV0nsocV0O4UcKM8BaIm8eqbcro
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

ZEkyxqT3mUoSbmGx1hrngjBsP1ufgwJ6D85LFGQC1SjIOLvsR9i6v41BaLF8/kygvKOh2HlNVSMx38g52sTqoQ/xb3f8vR1VDXliAuD0frrG2Fy5wK4rOAnjuX9nh0bC9 Generated-by-Nova\n",
        "user_id": "e4f380899b1248918f3d37098dc63746",
        "name": "demo1",
        "fingerprint": "b4:9a:c3:12:c4:90:bf:8e:7a:e2:70:10:c3:00:55:3f"
    }
}

or

{
    "error_code": "KPS.XXXX",
    "error_msg": "XXXX"
}

Status Codes

For details, see **Status Codes**.

5.1.4 Deleting an SSH Key Pair (V2.1)

Function

This API is used to delete a specified SSH key pair based on the key pair name.

URI

- URI format

  DELETE /v2.1/{project_id}/os-keypairs/{keypair_name}

- Parameter description

  Table 5-15 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keypair_name	Yes	String	Name of an SSH key pair

Requests

None

Responses

None

Status Codes

For details, see **Status Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5.1.5 Modifying the Description of a Key Pair (V2.1)

Function

This API is used to modify the description of a specified SSH key pair based on the name of the SSH key pair.

URI

- URI format

  PUT /v2.1/{project_id}/os-keypairs/{keypair_name}

- Parameter description

  Table 5-16 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keypair_name	Yes	String	Name of an SSH key pair

Requests

Table 5-17 Request parameters

Parameter	Mandatory	Type	Description
description	Yes	String	Description of the SSH key pair (The value ranges from 0 to 255 characters.)

Responses

None

Examples

- Example request

```
{
    "keypair": {
        "description": "keypair test"
    }
}
```

- Example response

  None

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

For details, see **Status Codes**.

5.2 Managing SSH Key Pairs (V2)

5.2.1 Querying the List of SSH Key Pairs (V2)

Function

This API is used to query the SSH key pair list.

URI

- URI format
  GET /v2/{project_id}/os-keypairs
- Parameter description

Table 5-18 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Requests

None

Responses

Table 5-19 Response parameters

Parameter	Mandatory	Type	Description
keypairs	Yes	Array of objects	SSH key pair information list. For details, see **Table 5-20**.

Table 5-20 keypairs field description

Parameter	Mandatory	Type	Description
keypair	Yes	Object	SSH key pair information, see **Table 5-21**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-21 keypair field description

Parameter	Mandatory	Type	Description
fingerprint	Yes	String	Fingerprint information about an SSH key pair
name	Yes	String	Name of an SSH key pair
public_key	Yes	String	Public key information about an SSH key pair

Examples

The following example describes how to query the SSH key pair list.

- Example request

  None

- Example response

```
{
   "keypairs": [
      {
         "keypair": {
            "fingerprint": "15:b0:f8:b3:f9:48:63:71:cf:7b:5b:38:6d:44:2d:4a",
            "name": "keypair-601a2305-4f25-41ed-89c6-2a966fc8027a",
            "public_key": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQC+Eo/
RZRngaGTkFs7I62ZjsIlO79KklKbMXi8F+KITD4bVQHHn+kV
+4gRgkgCRbdoDqoGfpaDFs877DYX9n4z6FrAIZ4PES8TNKhatifpn9NdQYWA+IkU8CuvlEKGuFpKRi/
k7JLos/gHi2hy7QUwgtRvcefvD/vgQZOVw/mGR9Q== Generated-by-Nova\n"
         }
      }
   ]
}
```

Status Codes

For details, see **Status Codes**.

5.2.2 Querying Details About an SSH Key Pair (V2)

Function

This API is used to query a specified SSH key pair based on the key pair name.

URI

- URI format

  GET /v2/{project_id}/os-keypairs/{keypair_name}

- Parameter description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-22 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keypair_name	Yes	String	Name of an SSH key pair

Requests

None

Responses

Table 5-23 Response parameters

Parameter	Mandatory	Type	Description
keypair	Yes	Object	SSH key pair information. For details, see **Table 5-24**.

Table 5-24 keypair field description

Parameter	Mandatory	Type	Description
public_key	Yes	String	Public key information about an SSH key pair
name	Yes	String	Name of an SSH key pair
fingerprint	Yes	String	Fingerprint information about an SSH key pair
created_at	Yes	String	Time when an SSH key pair is created The value is a timestamp expressed in the number of seconds since 00:00:00 UTC on January 1, 1970.
deleted	Yes	Boolean	Tag that indicates an SSH key pair is deleted
deleted_at	Yes	String	Time when an SSH key pair is deleted The value is a timestamp expressed in the number of seconds since 00:00:00 UTC on January 1, 1970.
id	Yes	String	ID of an SSH key pair

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
updated_at	Yes	String	Time when an SSH key pair is updated The value is a timestamp expressed in the number of seconds since 00:00:00 UTC on January 1, 1970.
user_id	Yes	String	User to whom an SSH key pair belongs

Examples

The following example describes how to query the SSH key pair details.

- Example request

  None

- Example response

```
{
    "keypair": {
        "created_at": "2014-05-07T12:06:13.681238",
        "deleted": false,
        "deleted_at": null,
        "fingerprint": "9d:00:f4:d7:26:6e:52:06:4c:c1:d3:1d:fd:06:66:01",
        "id": 1,
        "name": "keypair-3582d8b7-e588-4aad-b7f7-f4e76f0e4314",
        "public_key": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDYJrTVpcMwFqQy/
oMvtUSRofZdSRHEwrsX8AYkRvn2ZnCXM+b6+GZ2NQuuWj+ocznlnwiGFQDsL/yeE+/
kurqcPJFKKp60mToXIMyzioFxW88fJtwEWawHKAclbHWpR1t4fQ4DS+/sIbX/
Yd9btlVQ2tpQjodGDbM9Tr9/+/3i6rcR+EoLqmbgCgAiGiVV6VbM2Zx79yUwd
+GnQejHX8BlYZoOjCnt3NREsITcmWE9FVFy6TnLmahs3FkEO/
QGgWGkaohAJlsgaVvSWGgDn2AujKYwyDokK3dXyeX3m2Vmc3ejiqPa/C4nRrCOlko5nSgV/
9IXRx1ERImsqZnE9usB Generated-by-Nova\n",
        "updated_at": null,
        "user_id": "fake"
    }
}
```

Status Codes

For details, see **Status Codes**.

5.2.3 Creating and Importing an SSH Key Pair (V2)

Function

This API is used to create an SSH key pair or import a public key to HUAWEI CLOUD to generate a key pair.

After an SSH key pair is created, you need to download the private key to a local directory. Then, you can use this private key to log in to an ECS. For ECS security purposes, the private key can be downloaded only once. Keep it secure.

URI

- URI format

  POST /v2/{project_id}/os-keypairs

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- Parameter description

Table 5-25 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Requests

NOTE

When creating an SSH key pair, you only need to set the **name**. When importing an SSH key pair, you must set the **public_key** parameter.

Table 5-26 Request parameters

Parameter	Mandatory	Type	Description
keypair	Yes	Object	Information about the created or imported SSH key pair. For details, see **Table 5-27**.

Table 5-27 keypair field description

Parameter	Mandatory	Type	Description
public_key	No	String	Character string of a public key to be imported
type	No	String	Type of a key pair. The value is **ssh** or **x509**.
name	Yes	String	Name of an SSH key pair. A new key pair cannot use the same name as an existing one. The value contains a maximum of 64 characters, including only letters, digits, underscores(_), and hyphens (-).
user_id	No	String	ID of the user to whom an SSH key pair belongs

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Responses

Table 5-28 Response parameters

Parameter	Mandatory	Type	Description
keypair	Yes	Object	SSH key pair information. For details, see **Table 5-29**.

Table 5-29 keypair field description

Parameter	Mandatory	Type	Description
fingerprint	Yes	String	Fingerprint information about an SSH key pair
name	Yes	String	Name of an SSH key pair
public_key	Yes	String	Public key information about an SSH key pair
private_key	No	String	Private key information about an SSH key pair. • The information about the private key is contained in the response for creating an SSH key pair. • The information about the private key is not contained in the response for importing an SSH key pair.
user_id	Yes	String	ID of the user to whom an SSH key pair belongs

Examples

- Creating an SSH key pair
  - Request example for creating an SSH key pair

```
{    "keypair": {
        "type": "ssh",
        "name": "demo"
    }
}
```

  - Response example for creating an SSH key pair

```
{
   "keypair": {
      "public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCyNtFZM04PFxERvZU5OBKTKr3mtRZABe5/+zX81lTgDF
CBfq6OXia47M4qXOa3ciBEKKZF+fMfs8U2UNB9aK1R/
uORsoEFtxSgZnWG6p4Ct1vnrqwDD934VaDFPEn+h3JeAfvTB
+Ag1YQ9zh9uYyE9Z3qZcC9+Ui93BDGdBtQeav4odxdwXcr2mT2jJV0nsocV0O4UcKM8BaIm8eqbcro
ZEkyxqT3mUoSbmGx1hrngjBsP1ufgwJ6D85LFGQC1SjIOLvsR9i6v41BaLF8/
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

kygvKOh2HlNVSMx38g52sTqoQ/xb3f8vR1VDXliAuD0frrG2Fy5wK4rOAnjuX9nh0bC9 Generated-by-Nova\n",
"private_key": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEpAIBAAKCAQEAsjbRWTNODxcREb2VOTgSkyq95rUWQAXuf/s1/NZU4AxQgX6u
\njl4muOzOKlzmt3IgRCimRfnzH7PFNlDQfWitUf7jkbKBBbcUoGZ1huqeArdb566s\nAw/d
+FWgxTxJ/odyXgH70wfgINWEPc4fbmMhPWd6mXAvfllvdwQxnQbUHmr+KHcX
\ncF3K9pk9oyVdJ7KHFdDuFHCjPAWiJvHqm3K6GRJMsak95lKEm5hsdYa54IwbD9bn\n4MCeg/
OSxRkAtUoyDi77EfYur+NQWixfP5MoLyjodh5TVUjMd/
IOdrE6qEP8W93/\nL0dVQ15YgLg9H66xthcucCuKzgJ47l/Z4dGwvQIDAQABAoIBAQCdTjXL/
rVQLJQs\njKNDNnNu47NsCTvyl0nGPf+Rhb61ZSlKpH9/uyuC38O7MPWVx28jup3J9q7btNrG
\n7t6ZU+RpFAvbdyzb1pamXsoupLmEvESrZEsBCOhtY2fdsTG/Md+Ji0a1J6Z2VQG9\nbEviLC4S/
VwCRDwnzHOJInKIoJZroZv6SdK+KonQBS0Rq9bZrlvtBUUhaSGjBcJx\nmWKO78ikNOXP/
5Yl92SAw2vOYWhZdMZQrkp1EUFMG18Akuj+jC9QKXXfsLYYfzsQ
\nIGgpRdf6zYIV84QVMZ7NhQABM5DNmQfxrSIUSdbvOzOJzmShp41tH3sn9d+XS+bS
\nLloyuaQhAoGBAN7tpwgkcKddKI/Lp/CPqjkxP6lfO+xHEXjtnZd1Y//BavPSgq4v
\nWuFHgx1sPQK49KcSLZfF6UxkPw0KHBc5R9RkfYBAIdGNwENF2xyoYLLdnUtF4hRq
\n1q2DC3oklBZibH2tc6+hQ2aCWSeMvQbIvxTYV70EFzwR5f4O5LIskCm/AoGBAMyn
\nA7DOQdvcf4aexSYL4kGp70ERMOCtwr/d+O5RswARoyAQOxp4a7/TyFuGjnlT//bR
\nEYacXV1AieIdeJF3PgeUIR1QnUlNYD9Rufs14fs+5idQ7Evn1gvXv0HpBYTY7wNu
\nWTrWbsznY0fNIrGT4bQR6QpdvIuR5TBJf6HIAKyDAoGAFhKf3D2HbfraXkqC6V3A
\nNAN9Uy7bxwxOXZPha7Ky4QrspRGt4MNNk0q6X7ps3A0mJDi3jPSKoga2+3qJx37j
\nbtM4Xe97qb0IUWDkThUZ5fvtbBuSRAVEFlAIXeKrSwAZz+PRtY0ZGFhFrZXQzZAo
\n4058eXmjN05qYFpnKIEjEQ8CgYEAwELzW6oaAzR+dfk428p0UB4W0HkXAy0a9efS
\nUgpc8Oag6qF09SRGjdunshySQvegU78MCPtjVxUntE7dk0OD+di213SBn3jawAHG
\niHORjtkDndIPfCwcUdnpK0GAVtL6kK2dlIIZa9TB15WnT07Pzry4w21WkYSJ3Thf
\neJyNzYMCgYA8OvpKMdaEXFeNZWHDE1Q2VmpxvP/D6u6s4SBuyy8eac1qqku/s7zc\nsuFd/
o9wbBgzsf4eN8tNJ4bxrArRXvf9WyH7xd4PE3DvVJnz5S+8Nqj2Z0KCAqPD
\nibDbFxBYHcMIdwC2JBGQZIXpkST2jG9wZho5KghX4yiHSOPr2V25/g==\n-----END RSA PRIVATE KEY-----\n",
"user_id": "6fc0d2cbbfab40b199874b97097e913d",
"name": "demo",
"fingerprint": "b4:9a:c3:12:c4:90:bf:8e:7a:e2:70:10:c3:00:55:3f"
}
}

- Importing an SSH key pair
  - Request example for importing an SSH key pair

{
"keypair": {
"public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCyNtFZM04PFxERvZU5OBKTKr3mtRZABe5/+zX81lTgDF
CBfq6OXia47M4qXOa3ciBEKKZF+fMfs8U2UNB9aK1R/
uORsoEFtxSgZnWG6p4Ct1vnrqwDD934VaDFPEn+h3JeAfvTB
+Ag1YQ9zh9uYyE9Z3qZcC9+Ui93BDGdBtQeav4odxdwXcr2mT2jJV0nsocV0O4UcKM8BaIm8eqbcro
ZEkyxqT3mUoSbmGx1hrngjBsP1ufgwJ6D85LFGQC1SjIOLvsR9i6v41BaLF8/
kygvKOh2HlNVSMx38g52sTqoQ/xb3f8vR1VDXliAuD0frrG2Fy5wK4rOAnjuX9nh0bC9 Generated-by-Nova\n",
"type": "ssh",
"name": "demo1",
"user_id": "fake"
}
}

  - Response example for importing an SSH key pair

{
"keypair": {
"public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCyNtFZM04PFxERvZU5OBKTKr3mtRZABe5/+zX81lTgDF
CBfq6OXia47M4qXOa3ciBEKKZF+fMfs8U2UNB9aK1R/
uORsoEFtxSgZnWG6p4Ct1vnrqwDD934VaDFPEn+h3JeAfvTB
+Ag1YQ9zh9uYyE9Z3qZcC9+Ui93BDGdBtQeav4odxdwXcr2mT2jJV0nsocV0O4UcKM8BaIm8eqbcro
ZEkyxqT3mUoSbmGx1hrngjBsP1ufgwJ6D85LFGQC1SjIOLvsR9i6v41BaLF8/
kygvKOh2HlNVSMx38g52sTqoQ/xb3f8vR1VDXliAuD0frrG2Fy5wK4rOAnjuX9nh0bC9 Generated-by-Nova\n",
"user_id": "6fc0d2cbbfab40b199874b97097e913d",
"name": "demo1",
"fingerprint": "b4:9a:c3:12:c4:90:bf:8e:7a:e2:70:10:c3:00:55:3f"
}
}

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Codes

For details, see **Status Codes**.

5.2.4 Deleting an SSH Key Pair (V2)

Function

This API is used to delete a specified SSH key pair based on the key pair name.

URI

- URI format
  DELETE /v2/{project_id}/os-keypairs/{keypair_name}
- Parameter description

  Table 5-30 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
keypair_name	Yes	String	Name of an SSH key pair

Requests

None

Responses

None

Status Codes

For details, see **Status Codes**.

5.2.5 Copying an SSH Key Pair (V2)

Function

Copies a user's key pairs to the current user. The two users must belong to the same account.

URI

- URI format
  POST /v2/{project_id}/os-keypairs/copy
- Parameter description

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-31 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Requests

Table 5-32 Request parameters

Parameter	Mandatory	Type	Description
user_name	Yes	String	Name of the target user under the same tenant account
force	No	Boolean	Indicates whether to forcibly overwrite an existing key pair.

Responses

Table 5-33 Response parameters

Parameter	Mandatory	Type	Description
changed	Yes	Integer	Number of copied key pairs.
success	Yes	Array of objects	List of key pairs that were successfully copied. For details, see **Table 5-34**.
failed	Yes	Array of objects	List of key pairs that failed to be copied. For details, see **Table 5-34**.

Table 5-34 success/failed field description

Parameter	Mandatory	Type	Description
keypair	Yes	String	Key pair name
message	Yes	String	Task information

Examples

- Example request

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
{
 "user_name": "kpsuser"
}
```

- Example response

```
{
    "changed": 2,
    "success": [
        {
            "keypair": "KeyPair-test1",
            "message": "imported"
        },
        {
            "keypair": "KeyPair-test2",
            "message": "imported"
        }
    ],
    "failed": [
        {
            "keypair": "KeyPair-test3",
            "message": "exist"
        }
    ]
}
```

or

```
{
    "error_code": "KPS.XXXX",
    "error_msg": "XXXX"
}
```

Status Codes

For details, see **Status Codes**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6 Application Examples

Example 1: Encrypting or Decrypting Small Volumes of Data

Example 2: Encrypting or Decrypting Large Volumes of Data

Example 3: Querying Information About Keys

6.1 Example 1: Encrypting or Decrypting Small Volumes of Data

Scenario

Encrypt or decrypt data not larger than 4 KB, such as passwords, certificates, and phone numbers, by using a tool on the console or calling an API. This section describes how to call a KMS API and use a CMK to encrypt or decrypt data.

Process:

1. Create a CMK in KMS.
2. Call the encrypt-data API of KMS to encrypt plaintext data by using a CMK.
3. Deploy ciphertext certificates on your servers.
4. When your servers need to use a certificate, they call the decrypt-data API of KMS to decrypt the ciphertext data and obtain the ciphertext certificate.

Operations

APIs are called to perform the following operations:

- **Create a CMK**
- **Encrypt a DEK**
- **Decrypt a DEK**

Procedure

Step 1 Create a CMK.

- API information

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

URI format: POST /v1.0/*{project_id}*/kms/create-key

For details, see **Creating a CMK**.

NOTE

Default Master Keys are created by services integrated with KMS. Names of Default Master Keys end with **/default**. Do not end your CMK names with **/default**.

- Example request

  POST: https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/create-key

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

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

- Example response

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

Step 2 Encrypt data.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/encrypt-data

  For details, see **Encrypting Data**.

- Example request

  POST https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/encrypt-data

  Obtain *{endpoint}* from **Regions and Endpoints**.

  You can use the API for **Querying the List of CMKs** to check key information, including key_id.

  Body:

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

- Example response

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

Step 3 Decrypt data.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/decrypt-data

  For details, see **Decrypting Data**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- Example request

  POST https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/decrypt-data

  Obtain *{endpoint}* from **Regions and Endpoints**.

  You can use the API for **Querying the List of CMKs** to check key information, including key_id.

  Body:

  ```
  {     "cipher_text": "AgDoAG7EsEc2OHpQxz4gDFDH54CqwaelpTdEl
  +RFPjbKn5klPTvOywYIeZX60kPbFsYOpXJwkL32HUM50MY22Eb1fOSpZK7WJpYjx66EWOkJvO
  +Ey3r1dLdNAjrZrYzQlxRwNS05CaNKoX5rr3NoDnmv+UNobaiS25muLLiqOt6UrStaWow9AUyOHSzl
  +BrX2Vu0whv74djK
  +3COO6cXT2CBO6WajTJsOgYdxMfv24KWSKw0TqvHe8XDKASQGKdgfI74hzI1YWJlNjlmLWFlMTAtNDRjZ
  C1iYzg3LTFiZGExZGUzYjdkNwAAAACdcfNpLXwDUPH3023MvZK8RPHe129k6VdNIi3zNb0eFQ=="
   }
  ```

- Example response

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

----End

6.2 Example 2: Encrypting or Decrypting Large Volumes of Data

Scenario

Encrypt or decrypt a large amount of data.

- Encryption process:
  a. Create a CMK in KMS.
  b. Call the create-datakey API of the KMS to create a DEK. A plaintext DEK and a ciphertext DEK will be generated. The ciphertext DEK was generated by using a CMK to encrypt the plaintext DEK.
  c. Use the plaintext DEK to encrypt a plaintext file, generating a ciphertext file.
  d. Store the ciphertext DEK and the ciphertext file together in a permanent storage device or a storage service.
- Decryption process:
  a. Read the ciphertext DEK and the ciphertext file from the permanent storage device or storage service.
  b. Call the decrypt-datakey API and use the encryption CMK to decrypt the ciphertext DEK. The plaintext DEK will be generated.

     If the CMK is deleted, the decryption will fail. Properly keep your CMKs.
  c. Use the plaintext DEK to decrypt the ciphertext file.

Involved APIs

APIs used for the following operations are involved:

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- **Create a CMK**
- **Create a DEK**
- **Encrypt a DEK**
- **Decrypt a DEK**

Procedure

Step 1 Create a CMK.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/create-key

  For details, see **Creating a CMK**.

  NOTE

  Default Master Keys are created by services integrated with KMS. Names of Default Master Keys end with **/default**. Do not end your CMK names with **/default**.

- Example request

  POST: https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/create-key

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

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

- Example response

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

Step 2 Create a DEK.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/create-datakey

  For details, see **Creating a DEK**.

- Example request

  POST https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/create-datakey

  Obtain *{endpoint}* from **Regions and Endpoints**.

  You can use the API for **Querying the List of CMKs** to check key information, including key_id.

  Body:

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

- Example response

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

"8151014275E426C72EE7D44267EF11590DCE0089E19863BA8CC832187B156A72A5A17F17B5EF0D525872C59ECEB72948AF85E18427F8BE0D46545C979306C08D",
"cipher_text":
"020098009EEAFCE122CAA5927D2E020086F9548BA1675FDB022E4ECC01B96F2189CF4B85E78357E73E1CEB518DAF7A4960E7C7DE8885ED3FB2F1471ABF400119CC1B20BD3C4A9B80AF590EFD0AEDABFDBB0E2B689DA7B6C9E7D3C5645FCD9274802586BE63779471F9156F2CDF07CD8412FFBE9230643034363662302D653732372D346439632D623335642D663834626234373461333766000000045B05321483BD9F9561865EE7DFE9BE267A42EB104E98C16589CE46940B18E52"
}

Step 3 Encrypt the DEK.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/encrypt-datakey

  For details, see **Encrypting a DEK**.

- Example request

  POST https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/encrypt-datakey

  Obtain *{endpoint}* from **Regions and Endpoints**.

  You can use the API for **Querying the List of CMKs** to check key information, including key_id.

  Body:

{
"key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
"plain_text":
"0000000000

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


- Example response


```
{
   "data_key":
"000000000
```

```
    "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
}
```


Step 2 Query the information about keys.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/describe-key

  For details, see "Querying Key Details".

- Example request

  POST: https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/describe-key

  Obtain *{endpoint}* from **Regions and Endpoints**.

  You can use the API for **Querying the List of CMKs** to check key information, including key_id.

  Body:

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

- Example response


```
{
   "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",
```


 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "expiration_time":"1501578672000",
    "origin":"kms",
    "key_rotation_enabled":"false",
    "sys_enterprise_project_id ": "0",
  }
}
```

Step 3 Query CMK instances.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/resource_instances/action

  For details, see "Querying Key Instances".

- Example request

  POST: https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms//resource_instances/action

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

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

- Example response

```
{
 "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,
   "key_rotation_enabled" : false,
   "expiration_time" : "",
   "origin" : "kms",
   "sys_enterprise_project_id" : "0",
   "realm" :  "cn-hongkong-7"
  } ],
  "resource_name" : "tagTest_xmdmi",
  "tags" : [ {
   "key" : "key",
   "value" : "testValue!"
  }, {
   "key" : "haha",
   "value" : "testValue"
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    } ]
  } ],
  "total_count" : 1
}
```

Step 4 Query the tags of a key.

- API information

  URI format: GET /v1.0/{project_id}/kms/{key_id}/tags

  For details, see "Querying Key Tags".

- Example request

  GET: https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/94752282-805e-4032-ada8-34966f70e02f/tags

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

  None

- Example response

```
{
       "tags": [
        {
         "key": "key1",
         "value": "value1"
         },
         {
         "key": "key2",
         "value": "value3"
         }
         ],
         "existTagsNum":2
}
```

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

7 Permissions Policies and Supported Actions

Introduction to Permissions Policies and Supported Actions

Actions Supported by Policy-based Authorization

Actions Supported by Identity Policy-based Authorization

7.1 Introduction to Permissions Policies and Supported Actions

If fine-grained permission management is required for your DEW, you can use IAM. In other cases, skip this section.

With IAM, you can control access to specific Huawei Cloud resources from principals (IAM users, user groups, agencies, or trust agencies). There are two types of IAM authorization: role/policy authorization and identity policy authorization.

The differences and relationships between the two authorization models are as follows:

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 7-1 Differences between the two types of authorization

Name	Relationship	Permission	Authorization Method	Scenario
Role/Policy	User-permission-authorization scope	• System-defined role • System-defined policies • Custom policies	Grants a role or policy to principals.	To authorize a user, add it to a user group and specify the scope of authorization. It is hard to provide fine-grained permissions control using authorization granted by user groups and a limited number of condition keys. This method is suitable for small- and medium-sized enterprises.
Identity policy	User-policy	• System-defined policies • Custom identity policies	• Grants an identity policy to principals. • Attaches identity policies to principals.	To authorize a user, grant an identity policy to it. User-specific authorization and a variety of key conditions allow for more fine-grained permissions control. However, this model can be hard to set up. It requires a certain amount of expertise and is suitable for medium- and large-sized enterprises.

For example, if you want to grant an IAM user the permissions to create ECSs in CN North-Beijing4 and OBSs in CN South-Guangzhou, you need to use the administrator role to create two custom policies and assign them to the IAM user. In the policy-based authorization mode, the administrator only needs to create a custom policy and configure the condition key **g:RequestedRegion** in the policy to control the authorized regions. You can attach a subject to a policy or grant the policy to the subject to assign the corresponding permissions. This permission configuration mode is more fine-grained and flexible.

Policies and actions in the two authorization models are not interoperable. You are advised to use the policy-based authorization model.

If you use IAM users in your account to call an API, the IAM users must be granted the required permissions. The permissions required for calling an API are determined by the actions supported by the API. Only users who have been granted permissions allowing the actions can call the API successfully.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

7.2 Actions Supported by Policy-based Authorization

This section describes the actions supported by policy-based authorization in DEW.

Supported Actions

DEW provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: statements in a policy that allow or deny certain operations
- APIs: REST APIs that can be called by a user who has been granted specific permissions.
- Actions: Specific operations that are allowed or denied in a custom policy.
- Dependent actions: When assigning an action to users, you also need to assign dependent permissions for that action to take effect.
- IAM or enterprise projects: Type of projects for which an action will take effect. For example, if you set the authorization scope of a custom policy to both IAM projects and enterprise projects, the policy takes effect for user groups in either IAM or enterprise projects. If an action supports only IAM projects, the custom policy that contains this action will take effect only for user groups in IAM. Administrators can check whether an action supports IAM projects or enterprise projects in the action list. "√" indicates that the action supports the project and "×" indicates that the action does not support the project. For details about the differences between IAM and enterprise management, see **What Are the Differences Between IAM and Enterprise Management?**

The following content describes the custom policy authorization supported by DEW.

Lifecycle Management

Table 7-2 Lifecycle management

Permission	API	Action	IAM (Project)	Enterprise Project Name (Enterprise Project)
Create a key	/v1.0/{project_id}/kms/create-key	kms:cmk:create	√	√
Query the key list	/v1.0/{project_id}/kms/list-keys	kms:cmk:list	√	√

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Permission	API	Action	IAM (Project)	Enterprise Project Name (Enterprise Project)
Enable a key	/v1.0/{project_id}/kms/enable-key	kms:cmk:enable	√	√
Disable a key	/v1.0/{project_id}/kms/disable-key	kms:cmk:disable	√	√
Query details about a key	/v1.0/{project_id}/kms/describe-key	kms:cmk:get	√	√
Create a DEK	/v1.0/{project_id}/kms/create-datakey	kms:cmk:createDataKey	√	√
Create a plaintext-free DEK	/v1.0/{project_id}/kms/create-datakey-without-plaintext	kms:cmk:createDataKeyWithoutPlaintext	√	√
Encrypt a DEK	/v1.0/{project_id}/kms/encrypt-datakey	kms:cmk:encryptDataKey	√	√
Decrypt a DEK	/v1.0/{project_id}/kms/decrypt-datakey	kms:cmk:decryptDataKey	√	√
Encrypt data	/v1.0/{project_id}/kms/encrypt-data	kms:cmk:encryptData	√	√
Decrypt data	/v1.0/{project_id}/kms/decrypt-data	kms:cmk:decryptData	√	√

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Permission	API	Action	IAM (Project)	Enterprise Project Name (Enterprise Project)
Generate a random number	/v1.0/{project_id}/kms/gen-random	kms::generateRandom	√	×
Sign data	/v1.0/{project_id}/kms/sign	kms:cmk:sign	√	√
Authenticate a signature	/v1.0/{project_id}/kms/verify	kms:cmk:verify	√	√
Query a public key	/v1.0/{project_id}/kms/get-publickey	kms:cmk:getPublicKey	√	√
Query versions	/	kms::getVersions	√	×
Query key API version	/v1.0	kms::getVersion	√	×
Schedule key deletion	/v1.0/{project_id}/kms/schedule-key-deletion	kms:cmk:scheduleKeyDeletion	√	√
Cancel scheduled key deletion	/v1.0/{project_id}/kms/cancel-key-deletion	kms:cmk:cancelKeyDeletion	√	√
Query the number of key instances of a tenant	/v1.0/{project_id}/kms/user-instances	kms::getInstance	√	×
Query resource quotas	/v1.0/{project_id}/kms/user-quotas	kms::getQuota	√	×
Modify key information - update a key alias	/v1.0/{project_id}/kms/update-key-alias	kms:cmk:updateKeyAlias	√	√

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Permission	API	Action	IAM (Project)	Enterprise Project Name (Enterprise Project)
Modify key information - update key description	/v1.0/{project_id}/kms/update-key-description	kms:cmk:updateKeyDescription	√	√
Create a grant	/v1.0/{project_id}/kms/create-grant	kms:cmk:createGrant	√	√
Query the grant list	/v1.0/{project_id}/kms/list-grants	kms:cmk:listGrants	√	√
Query retirable grants	/v1.0/{project_id}/kms/list-retirable-grants	kms::listRetirableGrants	√	×
Retire a grant	/v1.0/{project_id}/kms/retire-grant	kms:cmk:retireGrant	√	×
Revoke a grant	/v1.0/{project_id}/kms/revoke-grant	kms:cmk:revokeGrant	√	√
Obtain parameters for importing a key	/v1.0/{project_id}/kms/get-parameters-for-import	kms:cmk:getMaterial	√	√
Import key materials	/v1.0/{project_id}/kms/import-key-material	kms:cmk:importMaterial	√	√
Delete key materials	/v1.0/{project_id}/kms/delete-imported-key-material	kms:cmk:deleteMaterial	√	√

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Permission	API	Action	IAM (Project)	Enterprise Project Name (Enterprise Project)
Enable key rotation	/v1.0/{project_id}/kms/enable-key-rotation	kms:cmk:enableRotation	√	√
Modify key rotation interval	/v1.0/{project_id}/kms/update-key-rotation-interval	kms:cmk:updateRotation	√	√
Disable key rotation	/v1.0/{project_id}/kms/disable-key-rotation	kms:cmk:disableRotation	√	√
Query key rotation status	/v1.0/{project_id}/kms/get-key-rotation-status	kms:cmk:getRotation	√	√
Create a keystore	/v1.0/{project_id}/keystores/	kms:keystore:create	√	×
Delete a dedicated keystore	/v1.0/{project_id}/keystores/{keystore_id}	kms:keystore:delete	√	×
Enable a dedicated keystore	/v1.0/{project_id}/keystores/{keystore_id}/enable	kms:keystore:enable	√	×
Disable a dedicated keystore	/v1.0/{project_id}/keystores/{keystore_id}/disable	kms:keystore:disable	√	×
Query the list of dedicated keystores	/v1.0/{project_id}/keystores/	kms:keystore:list	√	×

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Permission	API	Action	IAM (Project)	Enterprise Project Name (Enterprise Project)
Obtain a dedicated key store	/v1.0/{project_id}/keystores/{keystore_id}	kms:keystore:get	√	×
Add tags to a key	/v1.0/{project_id}/kms/{resource_id}/tags	kms:cmk:createTag	√	√
Batch add or delete key tags	/v1.0/{project_id}/kms/{resource_id}/tags/action	kms:cmk:createTags	√	√
Query key instances	/v1.0/{project_id}/kms/resource_instances/action	kms:cmk:listKeysByTag	√	×
Delete key tags	/v1.0/{project_id}/kms/{resource_id}/tags/{key}	kms:cmk:deleteTag	√	√
Query key tags	/v1.0/{project_id}/kms/{resource_id}/tags	kms:cmk:getTags	√	√
Query project tags	/v1.0/{project_id}/kms/tags	kms::listAllTags	√	×

7.3 Actions Supported by Identity Policy-based Authorization

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

7.3.1 Actions Supported by Identity Policy-based Authorization (KMS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the **Organizations** service also provides **Service Control Policies (SCPs)** to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see **How IAM Is Different from Organizations for Access Control?**.

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see **Creating a Custom Identity Policy**.
- For details about how to use these elements to edit a custom SCP, see **Creating an SCP**.

Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

  For details about the resource types defined by KMS, see **Resources**.
- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

  For details about the condition keys defined by KMS, see **Conditions**.

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see **Policies and Identity Policies**.

The following table lists the actions that you can define in identity policy statements for KMS.

Table 7-3 Actions supported by KMS

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:create	Grants permission to create KMS keys.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
kms:cmk:list	Grants permission to View All KMS Key Information.	List	KeyId *	-	-
			-	g:EnterpriseProjectId	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:enable	Grants permission to change the status of a KMS key to Enabled.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
kms:cmk:disable	Grants permission to disable KMS keys.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:get	Grants permission to view details about KMS keys.	Read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• kms:RequestAlias • kms:ResourceAliases	
kms:cmk:createDataKey	Grants permission to use KMS keys to generate data keys.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:dek:create

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
			-	• kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	
kms:cmk:createDataKeyWithoutPlaintext	Grants permission to use KMS keys to generate data keys that do not contain plaintext versions.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:dek:create
			-	• kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:encryptDataKey	Grants permission to encrypt the data key.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:dek:crypto • kms:dek:encrypt
			-	• kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	
kms:cmk:decryptDataKey	Grants permission to decrypt the data key.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:dek:crypto • kms:dek:decrypt

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
			-	• kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	
kms:cmk:encryptData	Grants permission to use the specified KMS key to encrypt small data.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:crypto • kms:cmk:encrypt
			-	• kms:EncryptionAlgorithm • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:decryptData	Grants permission to decrypt data using the specified KMS key.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:crypto • kms:cmk:decrypt
			-	• kms:EncryptionAlgorithm • kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	
kms::generateRandom	Grants permission to generate secure random strings.	Write	-	kms:RecipientAttestation	• kms:cmk:generate

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:sign	Grants permission to generate digital signatures for.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases	
kms:cmk:verify	Grants permission to use the specified KMS key to verify the digital signature.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
			-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases	
kms:cmk:generateMac	Grants permission to generate a MAC.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• kms:MacAlgorithm • kms:RequestAlias • kms:ResourceAliases	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:verifyMac	Grants permission to verify a MAC using a specified KMS key.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• kms:MacAlgorithm • kms:RequestAlias • kms:ResourceAliases	
kms:cmk:getPublicKey	Grants permission to query the KMS key and public key.	Read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
			-	• kms:RequestAlias • kms:ResourceAliases	
kms::getVersions	Grants permission to query service versions.	Read	-	-	-
kms::getVersion	Grants permission to query the service key API version.	Read	-	-	-
kms::getInstance	Grants permission to query the number of key instances to the user.	Read	-	-	• kms:cmk:getInstance
kms::getQuota	Grants permission to query user quotas.	Read	-	-	• kms:cmk:getQuota
kms:cmk:scheduleKeyDeletion	Grants permission to periodically delete KMS keys.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:update

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
			-	kms:ScheduleKeyDeletionPendingWindowInDays	
kms:cmk:cancelKeyDeletion	Grants permission to cancel the scheduled deletion of KMS keys.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:update
kms:cmk:updateKeyAlias	Grants permission to change key aliases.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:update

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:updateKeyDescription	Grants permission to change the key description.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmk:update
kms:cmk:createGrant	Grants permission to a specific key creation authorization.	Permission_management	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:grant:create

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
			-	• kms:GranteePrincipalType • kms:GrantOperations • kms:GranteePrincipal • kms:RetiringPrincipal	
kms:cmk:listGrants	Grants permission to query the list of granted permissions for a specific key.	List	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:grant:list
kms::listRetirableGrants	Grants permission to query the list of authorizations that can be retired for keys.	List	-	-	• kms:grant:list
kms:cmk:retireGrant	Grants permission to a specific key retiring authorization.	Permission_management	KeyId *	g:ResourceTag/<tag-key>	• kms:grant:retire

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:revokeGrant	Grants permission to revoke authorization for a specific key.	Permission_management	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:grant:revoke
kms:cmk:getMaterial	Grants permission to obtain key import parameters.	Read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	kms:WrappingAlgorithm	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:importMaterial	Grants permission to import key materials.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	kms:ExpirationTime	
kms:cmk:deleteMaterial	Grants permission to delete key materials.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:enableRotation	Grants permission to enable rotation of a specified key.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
kms:cmk:updateRotation	Grants permission to change the specified key rotation period.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:disableRotation	Grants permission to disable key rotation.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
kms:cmk:getRotation	Grants permission to query the rotation status of a specified key.	Read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
kms:keystore:create	Grants permission to create a dedicated keystore.	Write	keystore *	-	-
kms:keystore:delete	Grants permission to delete the dedicated keystore.	Write	keystore *	-	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:keystore:enable	Grants permission to enable the dedicated keystore.	Write	keystore *	-	-
kms:keystore:disable	Grants permission to disable the dedicated keystore.	Write	keystore *	-	-
kms:keystore:list	Grants permission to query the list of dedicated keystore.	List	keystore *	-	-
kms:keystore:get	Grants permission to obtain the dedicated keystore.	Read	keystore *	-	-
kms:cmk:createTag	Grants permission to add tags to a specified CMK.	Tagging	KeyId *	• **kms:KeyOrigin** • **kms:KeySpec** • **kms:KeyUsage** • **kms:MultiRegionKeyType** • **g:EnterpriseProjectId** • **g:ResourceTag/<tag-key>**	• kms:cmkTag:create
			-	• **g:RequestTag/<tag-key>** • **g:TagKeys**	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:createTags	Grants permission to add or delete tags in batches for a specified CMK.	Tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmkTag:batch
			-	• g:RequestTag/<tag-key> • g:TagKeys	
kms:cmk:listKeysByTag	Grants permission to query a specified key instance.	List	KeyId *	-	• kms:cmkTag:listInstance
kms:cmk:deleteTag	Grants permission to delete a specified key tag.	Tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmkTag:delete

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
			-	g:TagKeys	
kms:cmk:getTags	Grants permission to query a specified key tag.	Read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• kms:cmkTag:list
kms::listAllTags	Grants permission to query the label of a specified key project.	List	-	-	-
kms:cmk:replicate	Grants permission to replicate KMS keys.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:cmk:updatePrimaryRegion	Grants permission to update primary region of KMS keys.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	kms:PrimaryRegion	
kms:alias:create	Grants permission to update primary region of KMS keys.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			alias *	-	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kms:alias:delete	Grants permission to update primary region of KMS keys.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			alias *	-	
kms:alias:list	Grants permission to update primary region of KMS keys.	List	-	-	-
kms:alias:associate	Grants permission to update primary region of KMS keys.	Write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			alias *	-	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Each API of KMS usually supports one or more actions. **Table 7-4** lists the supported actions and dependencies.

Table 7-4 Actions and dependencies supported by KMS APIs

API	Action	Dependencies
POST /v1.0/{project_id}/kms/create-key	kms:cmk:create	-
POST /v1.0/{project_id}/kms/list-keys	kms:cmk:list	-
POST /v1.0/{project_id}/kms/enable-key	kms:cmk:enable	-
POST /v1.0/{project_id}/kms/disable-key	kms:cmk:disable	-
POST /v1.0/{project_id}/kms/describe-key	kms:cmk:get	-
POST /v1.0/{project_id}/kms/create-datakey	kms:cmk:createDataKey	-
POST /v1.0/{project_id}/kms/create-datakey-without-plaintext	kms:cmk:createDataKeyWithoutPlaintext	-
POST /v1.0/{project_id}/kms/encrypt-datakey	kms:cmk:encryptDataKey	-
POST /v1.0/{project_id}/kms/decrypt-datakey	kms:cmk:decryptDataKey	-
POST /v1.0/{project_id}/kms/encrypt-data	kms:cmk:encryptData	-
POST /v1.0/{project_id}/kms/decrypt-data	kms:cmk:decryptData	-
POST /v1.0/{project_id}/kms/gen-random	kms::generateRandom	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

API	Action	Dependencies
POST /v1.0/{project_id}/kms/sign	kms:cmk:sign	-
POST /v1.0/{project_id}/kms/verify	kms:cmk:verify	-
POST /v1.0/{project_id}/kms/generate-mac	kms:cmk:generateMac	-
POST /v1.0/{project_id}/kms/verify-mac	kms:cmk:verifyMac	-
POST /v1.0/{project_id}/kms/get-publickey	kms:cmk:getPublicKey	-
GET /	kms::getVersions	-
GET /{version_id}	kms::getVersion	-
POST /v1.0/{project_id}/kms/schedule-key-deletion	kms:cmk:scheduleKeyDeletion	-
POST /v1.0/{project_id}/kms/cancel-key-deletion	kms:cmk:cancelKeyDeletion	-
GET /v1.0/{project_id}/kms/user-instances	kms::getInstance	-
GET /v1.0/{project_id}/kms/user-quotas	kms::getQuota	-
POST /v1.0/{project_id}/kms/update-key-alias	kms:cmk:updateKeyAlias	-
POST /v1.0/{project_id}/kms/update-key-description	kms:cmk:updateKeyDescription	-
POST /v1.0/{project_id}/kms/create-grant	kms:cmk:createGrant	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

API	Action	Dependencies
POST /v1.0/{project_id}/kms/list-grants	kms:cmk:listGrants	-
POST /v1.0/{project_id}/kms/list-retirable-grants	kms::listRetirableGrants	-
POST /v1.0/{project_id}/kms/retire-grant	kms:cmk:retireGrant	-
POST /v1.0/{project_id}/kms/revoke-grant	kms:cmk:revokeGrant	-
POST /v1.0/{project_id}/kms/get-parameters-for-import	kms:cmk:getMaterial	-
POST /v1.0/{project_id}/kms/import-key-material	kms:cmk:importMaterial	-
POST /v1.0/{project_id}/kms/delete-imported-key-material	kms:cmk:deleteMaterial	-
POST /v1.0/{project_id}/kms/enable-key-rotation	kms:cmk:enableRotation	-
POST /v1.0/{project_id}/kms/update-key-rotation-interval	kms:cmk:updateRotation	-
POST /v1.0/{project_id}/kms/disable-key-rotation	kms:cmk:disableRotation	-
POST /v1.0/{project_id}/kms/get-key-rotation-status	kms:cmk:getRotation	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

API	Action	Dependencies
POST /v1.0/{project_id}/keystores	kms:keystore:create	-
DELETE /v1.0/{project_id}/keystores/{keystore_id}	kms:keystore:delete	-
POST /v1.0/{project_id}/keystores/{keystore_id}/enable	kms:keystore:enable	-
POST /v1.0/{project_id}/keystores/{keystore_id}/disable	kms:keystore:disable	-
GET /v1.0/{project_id}/keystores	kms:keystore:list	-
GET /v1.0/{project_id}/keystores/{keystore_id}	kms:keystore:get	-
POST /v1.0/{project_id}/kms/{key_id}/tags	kms:cmk:createTag	-
POST /v1.0/{project_id}/kms/{key_id}/tags/action	kms:cmk:createTags	-
POST /v1.0/{project_id}/kms/{resource_instances}/action	kms:cmk:listKeysByTag	-
DELETE /v1.0/{project_id}/kms/{key_id}/tags/{key}	kms:cmk:deleteTag	-
GET /v1.0/{project_id}/kms/{key_id}/tags	kms:cmk:getTags	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

API	Action	Dependencies
GET /v1.0/{project_id}/kms/tags	kms::listAllTags	-
POST /v2/{project_id}/kms/keys/{key_id}/replicate	kms:cmk:replicate	-
PUT /v2/{project_id}/kms/keys/{key_id}/update-primary-region	kms:cmk:updatePrimaryRegion	-
POST /v1.0/{project_id}/kms/aliases	kms:alias:create	-
DELETE /v1.0/{project_id}/kms/aliases	kms:alias:delete	-
GET /v1.0/{project_id}/kms/aliases	kms:alias:list	-
POST /v1.0/{project_id}/kms/alias/associate	kms:alias:associate	-
POST /v1.0/{project_id}/kms/create-pin	kms:cmk:createDataKey	-

Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in **Table 7-5**, the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for KMS.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 7-5 Resource types supported by KMS

Resource Type	URN
KeyId	kms:<region>:<account-id>:KeyId:<cmk-id>
alias	kms:<region>:<account-id>:alias:<alias-name>
keystore	kms:<region>:<account-id>:keystore:<keystore-id>

Conditions

Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see **Global Condition Keys**.
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, kms) apply only to operations of the xx service. For details, see **Table 7-6**.
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see **operators**.

Service-specific condition keys supported by KMS

The following table lists the condition keys that you can define in identity policies for KMS. You can include these condition keys to specify conditions for when your identity policy is in effect.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 7-6 Service-specific condition keys supported by KMS

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
kms:EncryptionAlgorithm	string	Single-valued	Filters access to encryption/decryption operations based on the encryption/ decryption algorithm value in the request.
kms:GranteePrincipalType	string	Single-valued	Filters access to the CreateGrant operation based on the authorization principal type constraint in the request.
kms:GrantOperations	string	Multivalued	Filters access to the CreateGrant operation based on the operation to be authorized.
kms:GranteePrincipal	string	Single-valued	Filters access to the CreateGrant operation based on the authorized party principal in the authorization.
kms:KeyOrigin	string	Single-valued	Filters access to an API operation based on the origin attribute of the KMS key created or used for the operation.
kms:KeySpec	string	Single-valued	Filters access to API operations based on the key_spec attribute that created or used the operation KMS key.
kms:KeyUsage	string	Single-valued	Filters access to API operations based on the key_usage attribute of the KMS key created or used for the operation.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
kms:MessageType	string	Single-valued	Filters access to signing and verifying signature operations based on the value of the message_type parameter in the request.
kms:RetiringPrincipal	string	Single-valued	Filters access to CreateGrant operations based on retiring_principal in authorization.
kms:SigningAlgorithm	string	Single-valued	Filters access to signing and verifying operations based on signing_algorithm in the request.
kms:ExpirationTime	date	Single-valued	Filters access to the ImportKeyMaterial operation based on the value of the expiration_time parameter in the request.
kms:WrappingAlgorithm	string	Single-valued	Filters access to the CreateParametersFor-Import operation based on the value of the wrapping_algorithm parameter in the request.
kms:RecipientAttesta-tion	string	Single-valued	Filters access to the CreateDatakey, DecryptData, DecryptDatakey, and CreateRandom operations based on the Platform Configuration Register (PCR) value of the attestation document in the request.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
kms:MacAlgorithm	string	Single-valued	Filters access to MAC generation and verification operations based on mac_algorithm in the request.
kms:RequestAlias	string	Single-valued	Filters access to MAC generation and verification operations based on mac_algorithm in the request.
kms:ResourceAliases	string	Multivalued	Filters access to MAC generation and verification operations based on mac_algorithm in the request.
kms:MultiRegionKeyType	string	Single-valued	Filters access to API operations based on MultiRegionKeyType in the KMS key field.
kms:PrimaryRegion	string	Single-valued	Filters access to API operations based on primary_region in the request.
kms:EncryptionContext	string	Single-valued	Filters access to API operations based on additional_authenticated_data in the request.
kms:ScheduleKeyDeletionPendingWindowInDays	numeric	Single-valued	Filters access to API operations based on pending_days in the request.

7.3.2 Actions Supported by Identity Policy-based Authorization (KPS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

In addition to IAM, the **Organizations** service also provides **Service Control Policies (SCPs)** to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see **How IAM Is Different from Organizations for Access Control?**.

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see **Creating a Custom Identity Policy**.
- For details about how to use these elements to edit a custom SCP, see **Creating an SCP**.

Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

  For details about the resource types defined by KPS, see **Resources**.
- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

  For details about the condition keys defined by KPS, see **Conditions**.
- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see **Policies and Identity Policies**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

The following table lists the actions that you can define in identity policy statements for KPS.

Table 7-7 Actions supported by KPS

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kps:SSHKeyPair:create	Grants permission to create and import an SSH key pair.	Write	SSHKeyPair *	• **kps:KmsKeyId** • **kps:Algorithm**	• kps:domainKeypairs:create
kps:SSHKeyPair:delete	Grants permission to delete an SSH key pair.	Write	SSHKeyPair *	-	• kps:domainKeypairs:delete
kps:SSHKeyPair:get	Grants permission to query the details about an SSH key pair.	Read	SSHKeyPair *	-	• kps:domainKeypairs:get
kps:SSHKeyPair:list	Grants permission to query the SSH key pairs list.	List	SSHKeyPair *	-	• kps:domainKeypairs:list
kps:SSHKeyPair:update	Grants permission to update the description of an SSH key pair.	Write	SSHKeyPair *	-	• kps:domainKeypairs:update
kps:SSHKeyPair:bind	Grants permission to bind ECS to a new SSH key pair.	Write	SSHKeyPair *	-	• kps:domainKeypairs:bind

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kps::deleteFailedTask	Grants permission to delete failed tasks.	Write	-	-	• kps:domainKeypairs:deletefailtask • kps:domainKeypairs:deletefailtasks
kps:SSHKeyPair:unbind	Grants permission to unbind ECS from an SSH key pair.	Write	SSHKeyPair *	-	• kps:domainKeypairs:unbind • ecs:serverKeypairs:unbind
kps::getFailedTask	Grants permission to query information about failed tasks.	List	-	-	• kps:domainKeypairs:getfailtask
kps::getTask	Grants permission to query the current task execution status.	List	-	-	• kps:domainKeypairs:gettask
kps::getRunningTask	Grants permission to query information about ongoing tasks.	List	-	-	• kps:domainKeypairs:getrunningtask
kps:SSHKeyPair:importPrivateKey	Grants permission to import a private key to a key pair.	Write	SSHKeyPair *	**kps:KmsKeyId**	• kps:domainKeypairs:importpk

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
kps:SSHKeyPair:exportPrivateKey	Grants permission to export the private key of a key pair.	Write	SSHKeyPair *	-	• kps:domainKeypairs:exportpk
kps:SSHKeyPair:clearPrivateKey	Grants permission to clear the private key of a key pair.	Write	SSHKeyPair *	-	• kps:domainKeypairs:clearpk

Each API of KPS usually supports one or more actions. **Table 7-8** lists the supported actions and dependencies.

Table 7-8 Actions and dependencies supported by KPS APIs

API	Action	Dependencies
POST /v3/{project_id}/keypairs	kps:SSHKeyPair:create	• kms:cmk:createDataKey • kms:cmk:list
DELETE /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:delete	-
GET /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:get	-
GET /v3/{project_id}/keypairs	kps:SSHKeyPair:list	-
PUT /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:update	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

API	Action	Dependencies
POST /v3/{project_id}/keypairs/associate	kps:SSHKeyPair:bind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
DELETE /v3/{project_id}/failed-tasks	kps::deleteFailedTask	-
DELETE /v3/{project_id}/failed-tasks/{task_id}	kps::deleteFailedTask	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

API	Action	Dependencies
POST /v3/{project_id}/keypairs/disassociate	kps:SSHKeyPair:unbind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
GET /v3/{project_id}/failed-tasks	kps::getFailedTask	-
GET /v3/{project_id}/tasks/{task_id}	kps::getTask	-
GET /v3/{project_id}/running-tasks	kps::getRunningTask	-
POST /v3/{project_id}/keypairs/private-key/import	kps:SSHKeyPair:importPrivateKey	• kms:cmk:createDataKey • kms:cmk:list
POST /v3/{project_id}/keypairs/private-key/export	kps:SSHKeyPair:exportPrivateKey	kms:cmk:decryptDataKey

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

API	Action	Dependencies
POST /v3/{project_id}/keypairs/batch-associate	kps:SSHKeyPair:bind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
DELETE /v3/{project_id}/keypairs/{keypair_name}/private-key	kps:SSHKeyPair:clearPrivateKey	-

Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in **Table 7-9**, the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for KPS.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 7-9 Resource types supported by KPS

Resource Type	URN
SSHKeyPair	kps:<region>:<account-id>:SSHKeyPair:<keypair-name>

Conditions

Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see **Global Condition Keys**.
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, kps) apply only to operations of the xx service. For details, see **Table 7-10**.
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see **operators**.

Service-specific condition keys supported by KPS

The following table lists the condition keys that you can define in identity policies for KPS. You can include these condition keys to specify conditions for when your identity policy is in effect.

Table 7-10 Service-specific condition keys supported by KPS

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
kps:KmsKeyId	string	Single-valued	Filters access by the KMS key ID.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
kps:Algorithm	string	Single-valued	Filters access by SSH key algorithm.

7.3.3 Actions Supported by Identity Policy-based Authorization (CSMS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the **Organizations** service also provides **Service Control Policies (SCPs)** to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see **How IAM Is Different from Organizations for Access Control?**.

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see **Creating a Custom Identity Policy**.
- For details about how to use these elements to edit a custom SCP, see **Creating an SCP**.

Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

  - Required resources are marked with asterisks (*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

  For details about the resource types defined by CSMS, see **Resources**.

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

  For details about the condition keys defined by CSMS, see **Conditions**.
- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see **Policies and Identity Policies**.

The following table lists the actions that you can define in identity policy statements for CSMS.

Table 7-11 Actions supported by CSMS

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
csms:secret:create	Grants permission to create or recover a secret.	Write	secret Name *	• csms:Type • csms:KmsKeyId	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
csms:secret:delete	Grants permission to delete a secret immediately.	Write	secret Name *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
csms:secret:update	Grants permission to update the metadata of a secret.	Write	secretName *	• csms:Type • csms:KmsKeyId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
csms:secret:get	Grants permission to query or download the secret information.	Read	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
csms:secret:list	Grants permission to query all the secrets created by the current user under the current project.	List	secretName *	g:EnterpriseProjectId	-
csms:secret:createVersion	Grants permission to create a secret version in a specified secret.	Write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretVersion:create

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
csms:secret:getVersion	Grants permission to query information about a specified secret version and its plaintext secret value.	Read	secretName *	• csms:Type • csms:VersionId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretVersion:get
csms:secret:listVersion	Grants permission to list the available versions of a secret.	List	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretVersion:list
csms:secret:createStage	Grants permission to create a secret version stage.	Write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretStage:create
csms:secret:getStage	Grants permission to query version information about a specified secret version stage.	Read	secretName *	• csms:Type • csms:VersionStage • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretStage:get
csms:secret:updateStage	Grants permission to update a secret version stage.	Write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretStage:update

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
csms:secret:deleteStage	Grants permission to delete a specified secret version stage.	Write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretStage:delete
csms::getSecretQuota	Grants permission to query the secret quota of a specified project.	Read	-	-	• csms:secretQuota:get
csms:secret:scheduleDeletion	Grants permission to schedule the deletion of a secret.	Write	secretName *	• csms:Type • csms:RecoveryWindowInDays • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secret:deleteScheduled
csms:secret:restoreSecret	Grants permission to cancel the scheduled deletion of a secret.	Write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secret:deleteCancelled
csms:secret:rotate	Grants permission to start secret rotation.	Write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
csms:secret:getSecretsByTag	Grants permission to list secrets filtered by tags.	List	secret Name *	-	• csms:tag:getSecretByTag
csms:secret:batchCreateOrDeleteTags	Grants permission to batch add or remove secret tags.	Tagging	secret Name *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:tag:batch
			-	• g:RequestTag/<tag-key> • g:TagKeys	
csms:secret:createTag	Grants permission to add tags to a secret.	Tagging	secret Name *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:tag:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
csms:secret:deleteTag	Grants permission to remove tags from a secret.	Tagging	secret Name *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:tag:delete
			-	g:TagKeys	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
csms:secret:listTags	Grants permission to list secret tags.	List	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:tag:getBySecret
csms::listProjectTags	Grants permission to list the secret tags under a specified project.	List	-	-	• csms:tag:getAll
csms:secret:updateVersion	Grants permission to update the validity period of a secret version.	Write	secretName *	• csms:Type • csms:VersionId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• csms:secretVersion:update
csms::createEvent	Grants permission to create a secret event.	Write	-	-	• csms:event:create
csms::listEvents	Grants permission to list all secret event notifications created by the current user under the current project.	List	-	-	• csms:event:list

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
csms::getEvent	Grants permission to query a specified secret event notification.	Read	-	-	• csms:event:get
csms::updateEvent	Grants permission to update the metadata of a specified secret event notification.	Write	-	-	• csms:event:update
csms::deleteEvent	Grants permission to immediately delete a specified secret event notification.	Write	-	-	• csms:event:delete
csms::listNotificationRecords	Grants permission to list the records about triggered event notifications.	List	-	-	• csms:event:listNotificationRecords
csms::listTasks	Grants permission to list the secret rotation tasks.	List	-	-	• csms:task:list

Each API of CSMS usually supports one or more actions. **Table 7-12** lists the supported actions and dependencies.

Table 7-12 Actions and dependencies supported by CSMS APIs

API	Action	Dependencies
POST /v1/{project_id}/secrets	csms:secret:create	kms:cmk:createDataKey

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

API	Action	Dependencies
POST /v1/{project_id}/secrets/{secret_name}/backup	csms:secret:get	• kms:cmk:createDataKey • kms:cmk:decryptDataKey • kms:cmk:list
POST /v1/{project_id}/secrets/restore	csms:secret:create	kms:cmk:decryptDataKey
DELETE /v1/{project_id}/secrets/{secret_name}	csms:secret:delete	-
PUT /v1/{project_id}/secrets/{secret_name}	csms:secret:update	-
GET /v1/{project_id}/secrets/{secret_name}	csms:secret:get	-
GET /v1/{project_id}/secrets	csms:secret:list	-
POST /v1/{project_id}/secrets/{secret_name}/versions	csms:secret:createVersion	kms:cmk:createDataKey
GET /v1/{project_id}/secrets/{secret_name}/versions/{version_id}	csms:secret:getVersion	kms:cmk:decryptDataKey
GET /v1/{project_id}/secrets/{secret_name}/versions	csms:secret:listVersion	-
GET /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}	csms:secret:getStage	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

API	Action	Dependencies
PUT /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}	csms:secret:updateStage	-
DELETE /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}	csms:secret:deleteStage	-
POST /v1/{project_id}/secrets/{secret_name}/scheduled-deleted-tasks/create	csms:secret:scheduleDeletion	-
POST /v1/{project_id}/secrets/{secret_name}/scheduled-deleted-tasks/cancel	csms:secret:restoreSecret	-
POST /v1/{project_id}/secrets/{secret_name}/rotate	csms:secret:rotate	• rds:password:update • kms:cmk:createGrant • kms:cmk:retireGrant
POST /v1/{project_id}/csms/{resource_instances}/action	csms:secret:getSecretsByTag	-
POST /v1/{project_id}/csms/{secret_id}/tags/action	csms:secret:batchCreateOrDeleteTags	-
POST /v1/{project_id}/csms/{secret_id}/tags	csms:secret:createTag	-
DELETE /v1/{project_id}/csms/{secret_id}/tags/{key}	csms:secret:deleteTag	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

API	Action	Dependencies
GET /v1/{project_id}/csms/{secret_id}/tags	csms:secret:listTags	-
GET /v1/{project_id}/csms/tags	csms::listProjectTags	-
PUT /v1/{project_id}/secrets/{secret_name}/versions/{version_id}	csms:secret:updateVersion	-
POST /v1/{project_id}/csms/events	csms::createEvent	-
GET /v1/{project_id}/csms/events	csms::listEvents	-
GET /v1/{project_id}/csms/events/{event_name}	csms::getEvent	-
PUT /v1/{project_id}/csms/events/{event_name}	csms::updateEvent	-
DELETE /v1/{project_id}/csms/events/{event_name}	csms::deleteEvent	-
GET /v1/{project_id}/csms/notification-records	csms::listNotificationRecords	-
GET /v1/{project_id}/csms/tasks	csms::listTasks	-

Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in **Table 7-13**, the resource URN must be specified in the identity policy statements using that action, and the identity policy

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for CSMS.

Table 7-13 Resource types supported by CSMS

Resource Type	URN
secretName	csms:<region>:<account-id>:secretName:<secret-name>

Conditions

Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see **Global Condition Keys**.
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, csms) apply only to operations of the xx service. For details, see **Table 7-14**.
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see **operators**.

Service-specific condition keys supported by CSMS

The following table lists the condition keys that you can define in identity policies for CSMS. You can include these condition keys to specify conditions for when your identity policy is in effect.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 7-14 Service-specific condition keys supported by CSMS

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
csms:Type	string	Single-valued	Filters access by secret type.
csms:KmsKeyId	string	Single-valued	Filters access by KMS key ID.
csms:VersionId	string	Single-valued	Filters access by secret version ID.
csms:VersionStage	string	Single-valued	Filters access by secret version stage.
csms:RecoveryWindowInDays	numeric	Single-valued	Filters access by scheduled deletion time.

7.3.4 Actions Supported by Identity Policy-based Authorization (DHSM)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the **Organizations** service also provides **Service Control Policies (SCPs)** to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see **How IAM Is Different from Organizations for Access Control?**.

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see **Creating a Custom Identity Policy**.
- For details about how to use these elements to edit a custom SCP, see **Creating an SCP**.

Actions

Actions are specific operations that are allowed or denied in an identity policy.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

  For details about the resource types defined by DHSM, see **Resources**.
- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

  For details about the condition keys defined by DHSM, see **Conditions**.
- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see **Policies and Identity Policies**.

The following table lists the actions that you can define in identity policy statements for DHSM.

Table 7-15 Actions supported by DHSM

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
dhsm:hsm:list	Grants permission to query hsm list.	List	hsm *	-	-
			-	g:EnterpriseProjectId	
dhsm:hsm:get	Grants permission to view details about hsm.	Read	hsm *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
dhsm:hsm:delete	Grants permission to delete hsm.	Write	hsm *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dhsm:hsm:updateAlias	Grants permission to change hsm information.	Write	hsm *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dhsm:hsm:create	Grants permission to create hsm.	Write	hsm *	-	-
			-	g:EnterpriseProjectId	
dhsm:hsm:getJobInfo	Grants permission to query details about job.	Read	-	-	-
dhsm:hsm:updateHsm	Grants permission to operate hsm.	Write	hsm *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dhsm:cluster:create	Grants permission to create cluster.	Write	cluster *	-	-
dhsm:cluster:update	Grants permission to change cluster.	Write	cluster *	-	-
dhsm:cluster:delete	Grants permission to delete cluster.	Write	cluster *	-	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
dhsm:cluster:list	Grants permission to query cluster list.	List	cluster *	-	-
dhsm:cluster:addVsm	Grants permission to batch add hsm.	Write	cluster *	-	-
dhsm:cluster:getCsr	Grants permission to download a certificate request file.	Read	cluster *	-	-
dhsm:cluster:updateCert	Grants permission to configure certificate.	Write	cluster *	-	-
dhsm:cluster:getCert	Grants permission to view certificate.	Read	cluster *	-	-
dhsm:hsm:listHsmsByTag	Grants permission to query hsm instance.	List	hsm *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dhsm:hsm:createTags	Grants permission to add hsm tags.	Tagging	hsm *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dhsm:hsm:createResourceTag	Grants permission to add tags to a hsm.	Tagging	hsm *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dhsm:hsm:deleteResourceTag	Grants permission to remove tags from a hsm.	Tagging	hsm *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	g:TagKeys	
dhsm:hsm:getHsmTags	Grants permission to list hsm tags.	List	hsm *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dhsm::listTags	Grants permission to list tags.	List	-	-	-
dhsm::getPreCreatedInfo	Grants permission to query available hsm resources.	Read	-	-	-

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
dhsm::listChargeSpecCode	Grants permission to query specification codes.	List	-	-	-
dhsm:hsm:createInstallOrder	Grants permission to create install order.	Write	hsm *	-	-
			-	g:EnterpriseProjectId	
dhsm:hsm:createOrder	Grants permission to create order.	Write	hsm *	-	-
			-	g:EnterpriseProjectId	
dhsm:hsm:inquiryResource	Grants permission to order Inquiry.	Write	-	-	-

Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in **Table 7-16**, the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DHSM.

Table 7-16 Resource types supported by DHSM

Resource Type	URN
cluster	dhsm:<region>:<account-id>:cluster:<cluster-id>
hsm	dhsm:<region>:<account-id>:hsm:<hsm-id>

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Conditions

DHSM does not support service-specific condition keys in identity policies.It can only use global condition keys applicable to all services. For details, see **Global Condition Keys**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

A Appendix

A.1 Status Codes

Status Code	Status	Description
200	OK	Request processed successfully.
202	Accept	The job was successfully delivered. However, it will be postponed because the system is busy currently.
204	No Content	The request is processed successfully and no content is returned.
300	multiple choices	The requested resource has multiple available responses.
400	Bad Request	The request parameter is incorrect.
401	Unauthorized	You need to enter the username and password to access the requested page.
403	Forbidden	The server understood the request, but is refusing to fulfill it.
404	Not Found	The requested resource does not exist or not found.
405	Method Not Allowed	The method specified in the request is not allowed.
406	Not Acceptable	The response generated by the server cannot be accepted by the client.
407	Proxy Authentication Required	You must use the proxy server for authentication. Then, the request can be processed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Status	Description
408	Request Timeout	The request timed out.
409	Conflict	The request cannot be processed due to a conflict.
500	Internal Server Error	Internal service error.
501	Not Implemented	Failed to complete the request. The server does not support the requested function.
502	Bad Gateway	Failed to complete the request, because the server receives an invalid request.
503	Service Unavailable	Failed to complete the request due to system exception.
504	Gateway Timeout	A gateway timeout error occurs.

A.2 Error Code

Status Code	Error Code	Message	Description	Measure
400	CSMS.0002	The value of parameter is invalid.	The XX parameter is invalid.	Enter a valid parameter.
400	CSMS.0003	The request is invalid.	Invalid request.	Enter a valid URL.
400	CSMS.0004	The requested body format is wrong.	The request body format is incorrect.	Enter a valid body.
400	CSMS.0005	The resource does not exist.	The resource does not exist.	Enter valid secrets.
400	CSMS.0103	The secret is in the scheduled deletion state.	The secret is in Pending deletion state and cannot be used.	Ensure that the secret is in **Enabled** or **Disabled** state.
400	CSMS.0105	Can not delete the system internal stage.	Cannot delete the built-in version status of the system.	Do not delete the built-in version.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	CSMS.0106	The secret name not found int the db.	The secret name does not exist in the database.	Enter a valid secret name.
400	CSMS.0107	The secret is in schedule delete state.	The secret is in Pending deletion state.	Enter other secrets.
400	CSMS.0108	The secret is not in schedule delete state.	The secret is not in Pending deletion state.	Enter other secrets.
400	CSMS.0202	The number of secret has reached the upper limit.	The number of secrets reaches the upper limit.	Delete other secrets.
400	CSMS.0203	The number of stage has reached the upper limit.	The number of secret version statuses has reached the upper limit.	Delete other version statuses.
400	CSMS.0204	The number of stage is greater than the quota limit.	The number of secret version statuses has exceeded the upper limit.	Delete other version statuses.
400	CSMS.0301	Invalid X-Auth-Token.	Invalid **X-Auth-Token**.	Obtain the token again and ensure the token string is complete.
400	CSMS.0401	Can not get the protected secret value using the provided KMS key.	Failed to encrypt or decrypt the secret value by using KMS.	Ensure the key exists and is enabled.
403	CSMS.0109	The secret state is not enabled.	The secret is not enabled.	Enable the secret.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
403	CSMS.0302	The user role has no permission to access the interface.	The user role has no permission to access the API.	Contact the administrator to grant CSMS Fullaccess permissions.
404	CSMS.0205	Version quota not found for secret	No version quota is found for secret XX.	The secret has been deleted. Select another secret.
404	CSMS.0206	Stage quota not found for secret	No version status quota is found for secret XX.	The secret has been deleted. Select another secret.
404	CSMS.0207	Secret quota not found.	No secret quota found.	The secret has been deleted. Select another secret.
409	CSMS.0101	The secret name already exists.	The secret name is in use.	Enter another valid secret name.
409	CSMS.0102	The version id already exists.	The secret version number already exists.	Enter another valid secret version number.
409	CSMS.0104	The stage name already exists.	The version status name already exists.	Enter another valid version status name.
500	CSMS.0001	An internal error occurred.	Internal service error.	Try again later or contact customer support.
500	CSMS.0006	AES encrypt secret value occurred an error.	An error occurs while the secret value is encrypted using AES.	Try again later or contact customer support.
500	CSMS.0201	The number of secret has reached the upper limit.	The quota exceeds the upper limit.	Delete other secrets.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.0105	A system exception occurred. Contact technical support.	A system exception occurs. Contact technical support.	Contact technical support.
400	KMS.0106	It is replica service, readonly api allowed.	The replica service allows only read-only operations.	The replica service allows only read-only operations.
400	KMS.0201	Invalid request URL.	Invalid request URL.	Enter a valid URL.
400	KMS.0202	Invalid JSON format of the request message.	Invalid JSON format of the request message.	Enter a valid message.
400	KMS.0203	Request message too long.	Request message too long.	Enter a valid message.
400	KMS.0204	Parameters missing in the request message.	Parameters missing in the request message.	Enter a valid message.
400	KMS.0205	Invalid key ID.	Invalid key ID.	Enter a valid key ID.
400	KMS.0206	Invalid sequence number.	Invalid sequence number.	Enter a valid sequence number.
400	KMS.0208	Invalid value of value encryption_context.	Invalid value of value encryption_context.	Enter a valid value of encryption_context.
400	KMS.0209	The key has been disabled.	The key has been disabled.	Enable the key.
400	KMS.0210	The key is in Scheduled deletion state and cannot be used.	The key is scheduled to be deleted and is unavailable.	Enable the key.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.0211	Cannot perform this operation on Default Master Keys.	Cannot perform this operation on default master keys.	Perform this operation on a common CMK.
400	KMS.0212	Invalid resource type.	Invalid resource type.	Use the correct resource type.
400	KMS.0214	The request format is invalid.	Invalid request format.	Use the correct request format.
400	KMS.0308	Invalid parameter.	Invalid parameter.	Enter valid parameters.
400	KMS.0309	External keys required.	External keys required.	Use an imported key.
400	KMS.0310	The key is not in Pending import state.	The key is not pending to be imported.	Ensure the key is in **Pending import** state.
400	KMS.0311	Failed to decrypt data using the RSA private key.	Failed to decrypt data using the RSA private key.	Ensure the input ciphertext is correct and try again, or contact customer service.
400	KMS.0312	External keys cannot be rotated.	External keys cannot be rotated.	Use a common CMK.
400	KMS.0313	Key rotation is not enabled.	Key rotation is not enabled.	Enable key rotation.
400	KMS.0315	Invalid partition_id.	Invalid partition type.	Enter the correct partition type.
400	KMS.0317	The cmk partition is not enabled.	The key partition type is not enabled.	Enter the type of the partition to be enabled.
400	KMS.0318	Partition name has exist.	The partition type name already exists.	Enter a correct partition type name.
400	KMS.0319	Rotation not supported in the current KMS version.	Rotation is not supported in the current KMS version.	Try again later or contact customer support.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.0320	Resource frozen.	Resource frozen.	Renew the service and try again.
400	KMS.0323	Failed to obtain the partition of the key.	Failed to obtain the partition of the key.	Try again later or contact customer support.
400	KMS.0324	RSA keys cannot be rotated.	RSA keys cannot be rotated.	Use a common CMK.
400	KMS.0325	The asymmetric key is not support this operation.	This operation is not supported for asymmetric keys.	Try again using a symmetric key.
400	KMS.0327	Failed to obtain user permissions.	Failed to obtain user permissions.	Contact the administrator to grant the KMS CMKFullaccess permission to the account.
400	KMS.0329	Hash algorithm does not match the digest length.	Hash algorithm does not match the digest length.	Enter valid parameters or contact customer support.
400	KMS.0331	The symmetric key is not support this operation.	This operation is not supported for symmetric keys.	Use a correct key type and try again.
400	KMS.0332	This key is not support the signing algorithm.	The key does not support the signature algorithm.	Use a correct signature algorithm or contact technical support.
400	KMS.0333	The signing algorithm SM2DSA_SM3 not support RAW signing.	The signature algorithm SM2DSA_SM3 does not support RAW signatures.	Use a correct signature algorithm or contact technical support.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.0334	The cmk is used to encrypt and decrypt.	This key is used for encryption and decryption.	This key is used for encryption and decryption.
400	KMS.0335	The cmk is used to sign and verify.	This key is used for signature and verification.	This key is used for signature and verification.
400	KMS.0336	The current region does not support SM4.	SM4 is not supported in the current region.	Replace the algorithm or contact technical support.
400	KMS.0337	The current region does not support SM2.	SM2 is not supported in the current region.	Replace the algorithm or contact technical support.
400	KMS.0338	The custom keystore do not support rotation.	The user-defined keystore does not support rotation.	Contact technical support.
400	KMS.0339	The custom keystore do not support import key.	Keys cannot be imported to a custom keystore.	Contact technical support.
400	KMS.0340	not support keystore.	Currently, the keystore is not supported.	Contact technical support.
400	KMS.0341	The hmac key do not support this operation.	The HMAC key does not support this operation.	Enter valid parameters.
400	KMS.0401	Tag list cannot be empty.	Tag list cannot be empty.	Enter valid parameters.
400	KMS.0402	Invalid match value.	Invalid match value.	Enter valid parameters.
400	KMS.0403	Invalid match key.	Invalid match key.	Enter valid parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.0404	Invalid action.	Invalid action.	Enter valid parameters.
400	KMS.0405	Invalid tag value.	Invalid tag value.	Enter valid parameters.
400	KMS.0406	Invalid tag key.	Invalid tag key.	Enter valid parameters.
400	KMS.0407	Invalid tag list size.	Invalid tag list size.	Enter valid parameters.
400	KMS.0408	Invalid resourceType.	Invalid resourceType.	Enter valid parameters.
400	KMS.0409	Too many tags.	Too many tags.	Delete unnecessary tags and try again.
400	KMS.0410	Invalid tag value length.	Invalid tag value length.	Enter valid parameters.
400	KMS.0411	Invalid tag key length.	Invalid tag key length.	Enter valid parameters.
400	KMS.0412	Invalid tag list.	Invalid tag list.	Enter valid parameters.
400	KMS.0413	Too many tag values.	The length of the values list in the tag exceeded the upper limit.	Enter valid parameters.
400	KMS.0414	Invalid tags.	Invalid tags.	Enter valid parameters.
400	KMS.0415	Invalid matches.	Invalid matches.	Enter valid parameters.
400	KMS.0417	Invalid offset.	Invalid offset.	Enter valid parameters.
400	KMS.0418	Offset is not required.	No offset is required.	Enter valid parameters.
400	KMS.1101	Invalid key_alias.	Invalid key_alias.	Enter valid parameters.
400	KMS.1102	Invalid realm.	Invalid realm.	Enter valid parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.1103	Invalid key_description.	Invalid key_description.	Enter valid parameters.
400	KMS.1104	Duplicate key aliases.	The key alias already exists.	Use another alias.
400	KMS.1105	Too many keys.	Too many keys.	Increase key quota or delete unnecessary keys.
400	KMS.1108	Failed to create the default partition for the key.	Failed to create the default partition for the key.	Try again later or contact customer support.
400	KMS.1109	Failed to create the route for the key.	Failed to create the route for the key.	Try again later or contact customer support.
400	KMS.1110	Invalid alg_type.	The algorithm type is invalid.	Use a correct algorithm type.
400	KMS.1114	EC keys do not support to encrypt/ decrypt.	The key cannot be encrypted or decrypted.	Use the correct key for encryption and decryption.
400	KMS.1115	Symmetric keys do not support to sign/verify.	Signature verification is not supported for symmetric keys.	Try again using an asymmetric key.
400	KMS.1201	The key is not disabled.	The key is not disabled.	Disable the key.
400	KMS.1301	The key is not enabled.	The key is not enabled.	Enable the key.
400	KMS.1401	Set the pending deletion period between 7 to 1096 days.	The scheduled deletion time ranges from 7 days to 1,096 days.	Enter valid parameters.
400	KMS.1402	The key is already in Pending deletion state.	The key is already scheduled to be deleted.	No further operation required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.1404	This region is not the original region of the key, and it is not allowed to import-key-material.	The key material cannot be imported because this region is not the original region of the key.	Importing key materials is not supported for the current site.
400	KMS.1501	The key is not in Pending deletion state.	The key is not in **Pending deletion** state.	Create a scheduled deletion task for the key.
400	KMS.1601	Invalid limit.	Invalid limit.	Enter valid parameters.
400	KMS.1602	marker must be greater than or equals 0.	The value of **marker** must be greater than or equal to **0**.	Enter valid parameters.
400	KMS.1603	Invalid offset.	Invalid offset.	Enter valid parameters.
400	KMS.1801	random_data_length must be 512 bits.	random_data_length must be 512 bits.	Enter valid parameters.
400	KMS.1802	random_data_length must be a multiple of 8.	**random_data_length** must be a multiple of 8.	Enter valid parameters.
400	KMS.1901	datakey_length must be in the range 8 bits to 8,192 bits.	**datakey_length** must be in the range of 8 bits to 8,192 bits.	Enter valid parameters.
400	KMS.1902	key_spec can only be AES_128 or AES_256.	The value of **key_spec** must be **AES_128** or **AES_256**.	Enter valid parameters.
400	KMS.1903	datakey_length must be a multiple of 8.	**datakey_length** must be a multiple of 8.	Enter valid parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.1904	The rsa wrapping data key is over length 1520 bits.	The RSA wrapping data key exceeds 1,520 bytes.	Enter valid parameters.
400	KMS.2001	datakey_length must be 512 bits.	**datakey_length** must be 512 bits.	Enter valid parameters.
400	KMS.2101	Invalid plain_text.	The data key plaintext is invalid.	Enter valid parameters.
400	KMS.2102	datakey_plain_length must be 64 bytes.	**datakey_plain_length** must be 64 bytes.	Enter valid parameters.
400	KMS.2103	Failed to verify the DEK hash.	Failed to verify the DEK hash.	Ensure the data key is valid or contact customer support.
400	KMS.2104	The length of plain_text does not match datakey_plain_length.	The length of **plain_text** does not match **datakey_plain_length**.	Enter valid parameters.
400	KMS.2105	The symmetric key not support this encryption algorithm.	The symmetric key does not support this encryption algorithm.	Enter valid parameters.
400	KMS.2106	The rsa key not support this encryption algorithm.	The RSA key does not support this encryption algorithm.	Enter valid parameters.
400	KMS.2107	The sm2 key not support this encryption algorithm.	The SM2 key does not support this encryption algorithm.	Enter valid parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.2108	The rsa encryption plain_text is over length.	**rsa encryption plain_text** is too long.	Enter valid parameters.
400	KMS.2201	Invalid cipher_text.	The data key ciphertext is invalid.	Enter valid parameters.
400	KMS.2202	datakey_cipher_length must be 64 bytes.	datakey_cipher_length must be 64 bytes.	Enter valid parameters.
400	KMS.2203	Failed to verify the DEK hash.	Failed to verify the DEK hash.	Ensure the data key is valid or contact customer support.
400	KMS.2204	The length of cipher_text does not match datakey_cipher_length.	The length of **cipher_text** does not match **datakey_cipher_length**.	Enter valid parameters.
400	KMS.2301	The quota value is beyond the maximum configurable limit.	The quota value exceeds the upper limit.	Enter valid parameters.
400	KMS.2302	New quota value must not less than old.	The new quota cannot be smaller than the old quota.	Enter valid parameters.
400	KMS.2303	The quota type is not supported.	The quota type is not supported.	Enter valid parameters.
400	KMS.2304	Can not update grant quota when no grant has created.	If no grant is created, the grant quota cannot be updated.	Create a grant and try again.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.2305	Can not update cmk quota when no cmk has created.	The CMK quota cannot be updated if no CMK is created.	Create a key and try again.
400	KMS.2401	Specify an operation in addition to create-grant.	The operation cannot contain only **create-grant**.	Enter valid parameters.
400	KMS.2402	Invalid user ID.	Invalid user ID.	Enter valid parameters.
400	KMS.2403	Failed to create the grant.	Failed to create the grant.	Try again later or contact customer support.
400	KMS.2404	Too many CMK grants.	Too many CMK grants.	Increase grant quota or delete unnecessary grants.
400	KMS.2405	Too many grants.	Too many grants.	Increase grant quota or delete unnecessary grants.
400	KMS.2406	The basic partition has no right to create grant.	The basic partition does not have the permission to create a grant.	Contact technical support.
400	KMS.2501	Invalid grant ID.	Invalid grant ID.	Enter a valid grant ID.
400	KMS.2502	grant_id and key_id do not match.	grant_id and key_id do not match.	Ensure input grant_id matches key_id.
400	KMS.2601	Token expired.	Token expired.	Obtain a new token.
400	KMS.2602	Key expiration time must be later than the current time.	Key expiration time must be later than the current time.	Set a valid key expiration time.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.2603	Key IDs in the imported key and token do not match.	Key IDs in the imported key and token do not match.	Ensure the key ID in the imported key matches that in the token.
400	KMS.2604	The external key plaintext length must be 32 bits.	The external key plaintext length must be 32 bits.	Enter valid parameters.
400	KMS.2605	Token verification failed.	Failed to verify token.	Obtain a new token.
400	KMS.2606	You are importing a deleted key again. The imported plaintext must be the same as the deleted key plaintext.	You are importing a deleted key again. The imported plaintext must be the same as the deleted key plaintext.	Ensure the plaintext of the imported key is the same as that of the deleted key.
400	KMS.2607	The import sm4 plain key length must 16.	The length of the imported SM4 pure key must be 16.	Enter valid parameters.
400	KMS.2608	The imported asymmetric private key can not be null.	The imported asymmetric private key cannot be empty.	Enter valid parameters.
400	KMS.2609	The imported asymmetric private is invalid.	The imported asymmetric private key is invalid.	Enter valid parameters.
400	KMS.2610	The temporary key length must be 16 or 32.	The length of the temporary key must be 16 or 32.	Enter valid parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.2701	Key material is not in Enabled or Disabled state and cannot be deleted.	Key material is not in **Enabled** or **Disabled** state and cannot be deleted.	Ensure that the key is in **Enabled** or **Disabled** state.
400	KMS.2702	The imported private key material can not be deleted.	The imported private key material cannot be deleted.	The imported private key material cannot be deleted.
400	KMS.2801	End_time must bigger than start_time.	End time must be later than start time.	Enter valid parameters.
400	KMS.2901	Key rotation is not disabled.	Key rotation is not disabled.	Disable key rotation.
400	KMS.3001	Invalid rotation_interval.	Invalid rotation interval.	Enter valid parameters.
400	KMS.3103	Invalid id of tenant.	Invalid tenant ID.	Enter a valid tenant ID.
400	KMS.3201	Generate order id failed.	Failed to generate the order.	Try again or contact technical support.
400	KMS.3202	KMS error.	Incorrect order resources.	Try again or contact technical support.
400	KMS.3702	Invalid kms status parameter.	Invalid KMS status parameter.	Enter valid parameters.
400	KMS.3801	KMS key sync enable and configuration failed.	Failed to synchronize and configure KMS keys.	Try again or contact technical support.
400	KMS.3802	Failed to sync operation convert to born region.	Currently, the keystore is not supported.	Contact technical support.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
400	KMS.3803	The key of born region is turned off sync, so no operation can be performed.	Keystore is not supported.	Contact technical support.
400	KMS.3804	AttestationDocument parsing failed.	Failed to parse the document.	Try again or contact technical support.
400	KMS.3902	Invalid Service-Transaction-Id in request header.	Invalid value of **Service-Transaction-Id** in the request header.	Contact customer support.
400	KMS.3903	Service-Transaction-Id is missing in request header.	The request header does not contain the **Service-Transaction-Id** parameter.	Contact customer support.
400	KMS.4001	Service name to notify is illegal.	The service name used for notification is invalid.	Contact customer support.
400	KMS.4002	Service url to notify is illegal.	The service URL used for notification is invalid.	Contact customer support.
400	KMS.5022	Tags are not compliant.	The tags are not compliant.	Try again or contact technical support.
400	KMS.5023	Pdp5 Header is invalid.	Invalid value of **Header**.	Try again or contact technical support.
403	KMS.0301	Invalid or null X-Auth-Token.	Invalid or null X-Auth-Token.	Obtain the token again and ensure the token string is complete.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
403	KMS.0302	Invalid X-Auth-Token.	Invalid X-Auth-Token.	Obtain the token again and ensure the token string is complete.
403	KMS.0303	X-Auth-Token expired.	X-Auth-Token expired.	Obtain the token again and ensure the token string is complete.
403	KMS.0304	X-Auth-Token contains the OBT tag and cannot be used to access services.	X-Auth-Token contains the OBT tag and cannot be used to access services.	Obtain the token again and ensure the token string is complete.
403	KMS.0305	Invalid X-Auth-Token project name.	Invalid X-Auth-Token project name.	Obtain the token again and ensure the token string is complete.
403	KMS.0306	No access permissions.	The user has no permission to access the key.	Contact the administrator to grant the KMS CMKFullaccess permission to the account.
403	KMS.0307	No access permissions.	No access permissions.	Contact the administrator to grant the KMS CMKFullaccess permission to the account.
403	KMS.0314	Real-name authentication is required to access the API.	Real-name authentication is required to access the API.	Complete real-name authentication and try again.
403	KMS.0321	URIs in URL and X-Auth-Token do not match.	URIs in URL and X-Auth-Token do not match.	Ensure the URI in the URL matches that in X-Auth-Token.
403	KMS.0322	The user has no permission to access the partition.	The user does not have the permission on the partition type.	Configure the permission and try again.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
403	KMS.0326	No access permissions.	No access permissions.	Contact the administrator to grant the KMS CMKFullaccess permission to the account.
403	KMS.0328	KMS has been frozen. Renew it and try again.	KMS has been frozen. Renew it and try again.	Renew the service and try again.
403	KMS.0330	User has no permission.	The user does not have related permissions.	Configure the KMS CMKFullaccess permission and try again.
404	KMS.0207	The key does not exist.	The key does not exist.	Choose a valid key or create a key.
404	KMS.0316	No exist partition_id.	The partition type does not exist.	Enter the partition type.
404	KMS.0416	Invalid tag ID.	Invalid tag ID.	Enter a valid key tag.
404	KMS.3901	The requested jobId cannot be found.	Task ID not found.	Contact technical support.
405	KMS.0215	Request method not supported.	Invalid request method.	Use a supported request method.
500	KMS.0100	Get-status error.	Failed to obtain the service status.	Contact technical support.
500	KMS.0101	KMS error.	KMS service error.	Try again later or contact customer support.
500	KMS.0102	Abnormal KMS I/O.	Abnormal KMS I/O.	Try again later or contact customer support.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Status Code	Error Code	Message	Description	Measure
500	KMS.0103	A system exception occurred. Contact technical support.	A system exception occurs. Contact technical support.	Contact technical support.
500	KMS.3805	Failed to build digital envelope.	Failed to create a digital envelope.	Try again or contact technical support.
500	KMS.3806	Unable to obtain enclave root certificate, please contact technical support.	Failed to obtain the root certificate. Contact technical support.	Contact technical support.
500	KMS.5012	Request PDP service failed.	Failed to access the PDP service.	Try again or contact technical support.
500	KMS.5021	Check pdp5 auth failed.	PDP5 authentication fails.	Try again or contact technical support.
503	KMS.0104	A system exception occurred. Contact technical support.	A system exception occurs. Contact technical support.	Contact technical support.

A.3 Obtaining a Project ID

Obtaining a Project ID by Calling an API

You can obtain the project ID by calling the API used to **query project information based on the specified criteria**.

The API used to obtain a project ID is GET https://{Endpoint}/v3/projects. **{Endpoint}** is the IAM endpoint and can be obtained from **Regions and Endpoints**. For details about API authentication, see **Authentication**.

In the following example, **id** indicates the project ID.

```
{
    "projects": [
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

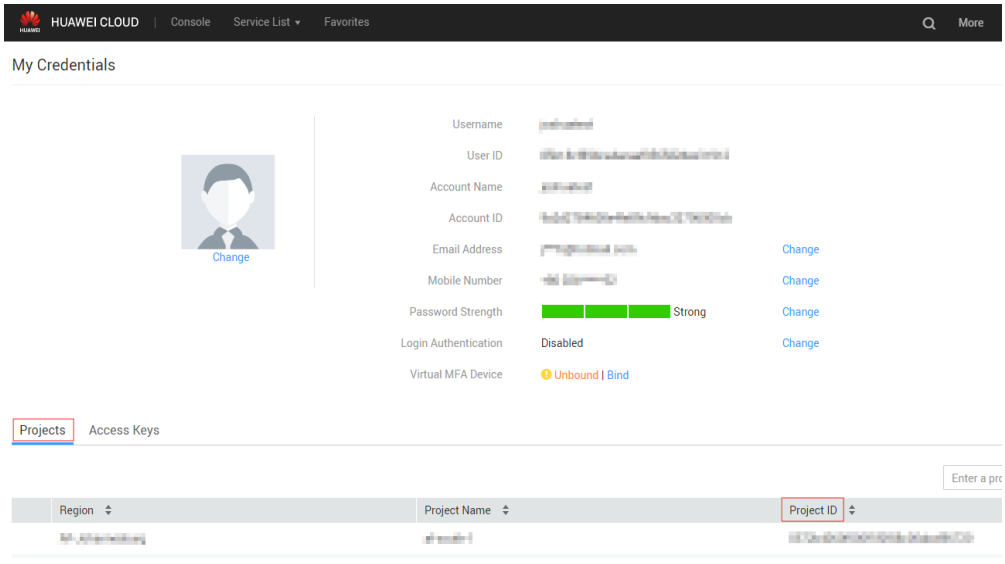
```
    {
        "domain_id": "65382450e8f64ac0870cd180d14e684b",
        "is_domain": false,
        "parent_id": "65382450e8f64ac0870cd180d14e684b",
        "name": "xxxxxxxx",
        "description": "",
        "links": {
            "next": null,
            "previous": null,
            "self":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


Obtaining a Project ID from the Console

A project ID is required for some URLs when an API is called. To obtain a project ID, perform the following operations:

1. **Log in to the management console**.
2. Click the username and choose **Basic Information** from the drop-down list.
3. On the **Account Info** page, click **Manage** next to **Security Credentials**.
   On the **My Credentials** page, view project IDs in the project list.

Figure A-1 Viewing project IDs



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.