Alibaba Cloud KeyManagementService

User Guide

Issue: 20190730

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
⚠	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
📋	This indicates warning informatio n, supplementary instructions, and other content that the user must understand.	Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 Use ActionTrail to record KMS events

KMS has been integrated with the ActionTrail service. You can view the events performed by all users (including the primary account and RAM users) on your resource instances in ActionTrail.

The KMS information recorded by ActionTrail includes all APIs except DescribeRegions. For more information, see KMS event log examples.

For event details, see ActionTrail event log syntax.

2 Use RAM to authorize KMS resources

KMS uses RAM to control access to KMS resources. This topic describes the resource types, actions, and policy conditions of KMS.

An Alibaba Cloud account has full operation permissions on its own resources. RAM users and roles are granted varying operation permissions on resources through RAM authorization. Before you use RAM to authorize and access CMKs, make sure that you have read ../../SP_65/DNRAM11820297/EN-US_TP_12331.dita#concept_oyr_zzv_tdb and API overview.

Resource types in KMS

The following table lists all resource types and corresponding Alibaba Cloud resource names (ARNs) in KMS. They can be used in the `Resource` parameter of an RAM policy.

Resource type	ARN
Key container	acs:kms:${region}:${account}:key
Alias container	acs:kms:${region}:${account}:alias
Key	acs:kms:${region}:${account}:key/${key-id}
Alias	acs:kms:${region}:${account}:alias/${ alias-name}

Actions in KMS

KMS defines actions used in RAM policies as access control for different APIs. They must be in the `kms :${ api - name }` format.

Note:
Access control is not required for `DescribeRegions`. DescribeRegions can be called by an Alibaba Cloud account, RAM user, or role and authenticated directly.

The following table lists the relationship between KMS APIs, RAM actions, and resource types.

KMS API	Action	Resource type
`ListKeys`	kms:ListKeys	Key container

KMS API	Action	Resource type
`CreateKey`	**kms:CreateKey**	Key container
`DescribeKey`	**kms:DescribeKey**	Key
`EnableKey`	**kms:EnableKey**	Key
`DisableKey`	**kms:DisableKey**	Key
`ScheduleKeyDeletion`	**kms:ScheduleKeyDeletion**	Key
`CancelKeyDeletion`	**kms:CancelKeyDeletion**	Key
`GetParametersForImport`	**kms:GetParametersForImport**	Key
`ImportKeyMaterial`	**kms:ImportKeyMaterial**	Key
`DeleteKeyMaterial`	**kms:DeleteKeyMaterial**	Key
`Encrypt`	**kms:Encrypt**	Key
`GenerateDataKey`	**kms:GenerateDataKey**	Key
`Decrypt`	**kms:Decrypt**	Key
`ListAliases`	**kms:ListAliases**	Alias container
`CreateAlias`	**kms:CreateAlias**	Alias and key
`UpdateAlias`	**kms:UpdateAlias**	Alias and key
`DeleteAlias`	**kms:DeleteAlias**	Alias and key
`ListAliasesByKeyId`	**kms:ListAliasesByKeyId**	Key
`TagResource`	**kms:TagResource**	Key
`UntagResource`	**kms:UntagResource**	Key
`ListResourceTags`	**kms:ListResourceTags**	Key

Policy conditions in KMS

You can add conditions to RAM policies to control their access to KMS. RAM authentication will only be successful when the specified conditions are met. For example, you can use `acs : CurrentTim e` to control the time period when a RAM policy is valid.

In addition to global conditions, you can use tags as filters to restrict the use of key-related APIs such as `Encrypt`, `Decrypt`, and `GenerateDataKey`. Filters must be in the `kms : tag /${ tag - key }` format.

For more information, see Policy elements.

Common RAM policy examples

- The RAM policy allowing users to access all KMS resources.

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Effect ": " Allow ",
      " Action ": [
        " kms :*"
      ],
      " Resource ": [
        "*"
      ]
    }
  ]
}
```

- The RAM policy allowing users to view keys, aliases, and key usage permissions.

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Effect ": " Allow ",
      " Action ": [
        " kms : List *", " kms : Describe *",
        " kms : Encrypt ", " kms : Decrypt ", " kms : GenerateDa
 taKey "
      ],
      " Resource ": [
        "*"
      ]
    }
  ]
}
```

- The RAM policy allowing users to operate keys that contain the following tags:
  - Tag key: `Project`
  - Tag value: `Apollo`

```
{
    " Version ": " 1 ",
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": [
                " kms : Encrypt ", " kms : Decrypt ", " kms :
 GenerateDa  taKey "
            ],
            " Resource ": [
                "*"
            ],
            " Condition ": {
                " StringEqua  lsIgnoreCa  se ": {
                    " kms : tag / Project ": [
                        " Apollo "
                    ]
                }
            }
        }
    ]
}
```

3 Managed HSM (preview)

3.1 Overview

Managed HSM is an important feature of Key Management Service (KMS) to enable easy access to certified Hardware Security Modules (HSMs) provided by Alibaba Cloud.

An HSM is a hardware device that performs cryptographic operations, and generates and stores keys. You can protect your most sensitive workloads and assets provided by Alibaba Cloud, by hosting keys in these highly secure hardware devices.

Supported regions

You can use Managed HSM in the following regions. This feature will be provided in more regions later.

Region	City	Region ID
Hong Kong	Hong Kong	cn-hongkong
Singapore	Singapore	ap-southeast-1

Regulatory compliance

Managed HSM can help you meet stringent regulatory requirements. Based on different regulatory requirements in each local market, Alibaba Cloud offers HSMs certified by different third-party organizations to meet your localization and internationalization requirements.

For regions outside mainland China,

- FIPS validation for hardware: Alibaba Cloud HSMs, including their hardware and firmware, have passed FIPS 140-2 Level 3 validation. For more information, see Certificate #3254.
- FIPS 140-2 Level 3 Compliance: Alibaba Cloud Managed HSM runs under FIPS Approved Level 3 mode of operation.
- PCI DSS: Alibaba Cloud Managed HSM complies with PCI SS requirements.

High security assurance

- Hardware protection

  Managed HSM helps you protect keys in KMS through hardware mechanisms. The plaintext key material of CMKs is only processed inside HSMs for key operations. It is kept within the hardware security boundary of HSMs.
- Secure key generation

  Randomness is crucial to the encryption strength of keys. Managed HSM uses a random number generation algorithm that is secure and licensed and has high system entropy seeds to generate key material. This protects keys from being recovered or predicted by attackers.

Ease of operation

Alibaba Cloud fully manages HSM hardware. This eliminates the costs otherwise incurred by the following hardware management operations:

- Hardware lifecycle management
- HSM cluster management
- High availability and scalability management
- System patching
- Most disaster recovery operations

Ease of integration

Native key management capabilities allow you to use the following features:

- Key version management
- Automatic key rotation
- Resource tag management
- Controlled authorization

These features enable rapid integration of your applications with HSMs, as well as integration of ECS, RDS, and other cloud services with Managed HSM. You can implement static encryption of cloud data without paying any R&D costs.

Key control

Managed HSM allows you to better control encryption keys on the cloud and move the most sensitive computing tasks and assets to the cloud.

When using both Managed HSM and Bring Your Own Key (BYOK), you can have full control over the following items:

- How key material is generated
- The key material that you import to the managed HSM cannot be exported, but can be destroyed.
- Key lifecycle
- Key persistence

Low cost

You can benefit from the pay-as-you-go billing method of cloud computing. Compared with user-created key infrastructure by using local HSMs, Managed HSM eliminates hardware procurement costs, as well as subsequent R&D and O&M costs.

3.2 Using Managed HSM

This topic describes how to create and use keys through Managed HSM.

Enable free-trial version of Managed HSM

You can contact your pre-sales or after-sales consultant to enable the free-trial version of Managed HSM.

Create a key in Managed HSM

You can only use Managed HSM in some regions. For more information about supported regions, see Supported regions.

Create a key in the console

1. Log on to the KMS console.
2. Select a region in the upper-left corner of the page. Click Create Key.
3. Select HSM from the Protection Level drop-down list.
4. Enter a description and click OK.

After a key is created, its Protection Level is displayed on the Key Details and Keys pages.

Create a key by using Alibaba Cloud CLI

```
 aliyun   kms   CreateKey  -- Protection  Level   HSM  -- Descriptio  n
" Key1   in   Managed   HSM "
```

The protection level of the key is displayed in the output after the key is created or in the output of DescribeKey called by using Alibaba Cloud CLI. Example:

```
{
  " KeyMetadat  a ": {
    " CreationDa  te ": " 2019 - 07 - 04T13 : 14 : 15Z ",
    " Descriptio  n ": " Key1   in   Managed   HSM ",
    " KeyId ": " 1234abcd - 12ab - 34cd - 56ef - 12345678 ****",
    " KeyState ": " Enabled ",
    " KeyUsage ": " ENCRYPT / DECRYPT ",
    " DeleteDate ": "",
    " Creator ": " 1111222233  33 ",
    " Arn ": " acs : kms : cn - hongkong : 1111222233  33 : key /
 1234abcd - 12ab - 34cd - 56ef - 12345678 ****",
    " Origin ": " Aliyun_KMS ",
    " MaterialEx  pireTime ": "",
    " Protection  Level ": " HSM "
  },
  " RequestId ": " 8eaeaa8b - 4491 - 4f1e - a51e - f95a4e5462  0c "
}
```

Import external keys to Managed HSM

You can also import keys from user-created key infrastructure to Managed HSM. You only need to set Protection Level to HSM in the first step of the import key material process. This step is to create external keys. Keep the remaining steps unchanged.

The actions on the Alibaba Cloud side:

- When you call `GetParametersForImport`, Alibaba Cloud generates a key pair for importing external keys in Managed HSM based on the HSM protection level, and returns the public key of the key pair.
- When you call `ImportKeyMaterial`, Alibaba Cloud imports the encrypted external key material to Managed HSM, and obtains the key material by unwrapping the HSM key. The imported plaintext key material will never be exported.

Manage and use keys

All management and cryptographic features supported by KMS are applicable to keys created in Managed HSM. Specifically, you can:

- Enable and disable keys.
- Manage key lifecycle.
- Manage key aliases.
- Manage key tags.
- Call key operations.

Integration with other cloud products

Keys created in Managed HSM can be used in other cloud products such as ECS, RDS, and OSS through standard APIs of KMS, to protect your native Alibaba Cloud data. In this case, cloud products must support server-side encryption by using custom keys . You only need to select keys created in Managed HSM when configuring CMKs for server-side encryption on cloud products.