Alibaba Cloud KeyManagementService

User Guide

Issue: 20190606

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 information, 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
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:GetParamet ersForImport	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:GenerateDataKey"
      ],
      "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:GenerateDataKey"
```

```
            ],
            " Resource ": [
                "*"
            ],
            " Condition ": {
                " StringEqua  lsIgnoreCa  se ": {
                    " kms : tag / Project ": [
                        " Apollo "
                    ]
                }
            }
        }
    ]
}
```