

# Alibaba Cloud Elasticsearch

RAM

Issue: 20190919

# 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.	 <b>Danger:</b> 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.	 <b>Warning:</b> 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.	 <b>Notice:</b> 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.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click OK.
<code>Courier</code> font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand   slave}</code>



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
1 Authorized resources.....	1
2 Access authentication rules.....	6
3 Temporary access token.....	11
4 RAM.....	15



# 1 Authorized resources

## Resource types and descriptions

The following table lists the supported resource types and the corresponding Aliyun resource names (ARN).

Resource type	ARN
instances	acs:elasticsearch:\$regionId:\$accountId:instances/*
instances	acs:elasticsearch:\$regionId:\$accountId:instances/\$instanceId
vpc	acs:elasticsearch:\$regionId:\$accountId:vpc/*
vswitch	acs:elasticsearch:\$regionId:\$accountId:vswitch/*

- `$regionId`: the ID of the specified region. You can also enter an asterisk `*`.
- `$accountId`: the ID of your Alibaba Cloud account. You can also enter an asterisk `*`.
- `$instanceId`: the ID of a specified Alibaba Cloud Elasticsearch instance. You can also enter an asterisk `*`.

## Instance authorization



### Note:

The following ARNs are shortened. For the complete name information, see the preceding table.

- Common actions on instances

Action	Description	ARN
elasticsearch:CreateInstance	You can perform this action to create an instance.	instances /*
elasticsearch:ListInstances	You can perform this action to view instances.	instances /*

Action	Description	ARN
<b>elasticsearch:DescribeInstance</b>	You can perform this action to view instance description.	<code>instances /* or instances /\$ instanceId</code>
<b>elasticsearch&gt;DeleteInstance</b>	You can perform this action to delete an instance.	<code>instances /* or instances /\$ instanceId</code>
<b>elasticsearch:RestartInstance</b>	You can perform this action to restart an instance.	<code>instances /* or instances /\$ instanceId</code>
<b>elasticsearch:UpdateInstance</b>	You can perform this action to update an instance.	<code>instances /* or instances /\$ instanceId</code>

- Actions on plug-ins

Action	Description	ARN
<b>elasticsearch:ListPlugin</b>	You can perform this action to obtain the list of plug-ins.	<code>instances /\$ instanceId</code>
<b>elasticsearch:InstallSystemPlugin</b>	You can perform this action to install system plug-ins.	<code>instances /\$ instanceId</code>
<b>elasticsearch:UninstallPlugin</b>	You can perform this action to uninstall a plug-in.	<code>instances /\$ instanceId</code>

- Actions on networks

Action	Description	ARN
<b>elasticsearch:UpdatePublicNetwork</b>	You can perform this action to check whether access through the public address is allowed.	<code>instances /\$ instanceId</code>
<b>elasticsearch:UpdatePublicIps</b>	You can perform this action to modify the public network whitelist.	<code>instances /\$ instanceId</code>
<b>elasticsearch:UpdateWhiteIps</b>	You can perform this action to modify the VPC whitelist.	<code>instances /\$ instanceId</code>

Action	Description	ARN
elasticsearch:UpdateKibanaIps	You can perform this action to modify the Kibana whitelist.	instances /\$ instanceId

• Actions on dictionaries

Action	Description	ARN
elasticsearch:UpdateDict	You can perform this action to modify the IK analyzer and synonym dictionary.	instances /\$ instanceId

Authorized CloudMonitor actions (CloudMonitor console)



Note:

The following ARNs are shortened to a \* wildcard form.

Action	Description	ARN format
cms:ListProductOfActiveAlert	You can perform this action to view services that have CloudMonitor enabled.	*
cms:ListAlarm	You can perform this action to query the specified or all alarm rule settings.	*
cms:QueryMetricList	You can perform this action to query the monitoring data of a specified instance.	*

VPC and VSwitch authorization



Note:

The following ARNs are shortened. For the complete name information, see the preceding table.

Action	Description	ARN
DescribeVpcs	You can perform this action to obtain a VPC list.	vpc /*

Action	Description	ARN
DescribeVswitches	You can perform this action to obtain a VSwitch list.	vswitch /*

## Intelligent Maintenance authorization



### Note:

The following ARNs are shortened. For the complete name information, see the preceding table.

Action	Description	ARN
elasticsearch:OpenDiagnosis	You can perform this action to enable health diagnosis.	instances /* or instances /\$ instanceId
elasticsearch:CloseDiagnosis	You can perform this action to disable health diagnosis.	instances /* or instances /\$ instanceId
elasticsearch:UpdateDiagnosisSettings	You can perform this action to update the health diagnosis settings.	instances /* or instances /\$ instanceId
elasticsearch:DescribeDiagnosisSettings	You can perform this action to query the health diagnosis settings.	instances /* or instances /\$ instanceId
elasticsearch:ListInstanceIndices	You can perform this action to query instance indexes.	instances /* or instances /\$ instanceId
elasticsearch:DiagnoseInstance	You can perform this action to start health diagnosis.	instances /* or instances /\$ instanceId
elasticsearch:ListDiagnosisReportIds	You can perform this action to query diagnosis report IDs.	instances /* or instances /\$ instanceId
elasticsearch:DescribeDiagnoseReport	You can perform this action to view diagnosis report details.	instances /* or instances /\$ instanceId

Action	Description	ARN
elasticsearch:ListDiagnoseReport	You can perform this action to list diagnosis reports.	instances /* or instances /\$ instanceId

### Supported regions

Elasticsearch region	RegionId
China (Hangzhou)	cn-hangzhou-d
China (Beijing)	cn-beijing
China (Shanghai)	cn-shanghai
China (Shenzhen)	cn-shenzhen
India (Mumbai)	ap-south-1
Singapore	ap-southeast-1
cn-hongkong	cn-hongkong
US (Silicon Valley)	us-west-1
Malaysia (Kuala Lumpur)	ap-southeast-3
Germany (Frankfurt)	eu-central-1
Japan (Tokyo)	ap-northeast-1
Australia (Sydney)	ap-southeast-2
Indonesia (Jakarta)	ap-southeast-5
China (Qingdao)	cn-qingdao
China (Zhangjiakou)	cn-zhangjiakou

## 2 Access authentication rules

### General permission policies

The following two general permission policies are provided to meet the needs for common access, so that you can select a permission policy suitable for you. You can search for the policy name in the brackets from Optional Authorization Policy Names and select it.

- Read-only permissions for Elasticsearch instances, applicable for read-only users (AliyunElasticsearchReadOnlyAccess).
- Administrator permissions for Elasticsearch instances, applicable for the administrator (AliyunElasticsearchFullAccess).



**Note:**

If none of the above general permission policies can meet your needs, you can refer to the following description and customize a permission policy.

### Permission to buy instances (post-payment & prepayment)

Permission to access the VPC of the primary account

- [ “vpc:DescribeVSwitch\*”, “vpc:DescribeVpc\*” ]



**Note:**

You can refer to the system template AliyunVPCReadOnlyAccess.

### Subaccount order permission

- [ “bss:PayOrder” ]



**Note:**

You can refer to the system template AliyunBSSOrderAccess.

### API permissions

Method	URI	Resource	Action
GET	/instances	instances/*	ListInstance
POST	/instances	instances/*	CreateInstance
GET	/instances/\$instanceId	instances/\$instanceId	DescribeInstance

Method	URI	Resource	Action
DELETE	/instances/\$instanceId	instances/\$instanceId	DeleteInstance
POST	/instances/\$instanceId/actions/restart	instances/\$instanceId	RestartInstance
PUT	/instances/\$instanceId	instances/\$instanceId	UpdateInstance

### Authorization examples

- [#unique\\_5](#) (for example, \$regionid, \$accountid, and \$instanceId).
- Elasticsearch instances in the resource can be indicated by the wildcard `*`.

#### Authorization example 1

To a subaccount under the primary account (accountId “1234” ), assign all operation permissions, except for CreateInstance, over all instances in China East 1 (Hangzhou ) on the console, and set the instances to be accessible from only the specified IP address.

After this policy is created on the console of the primary account, you need to use your primary account on the RAM console or the RAM SDK to authorize the subaccount.

#### 1. Create a policy

```
{
  "Statement": [
    {
      "Action": [
        "imagesearch : ListInstance ",
        "imagesearch : DescribeInstance ",
        "elasticsearch : DeleteInstance ",
        "elasticsearch : RestartInstance ",
        "elasticsearch : UpdateInstance "
      ],
      "Condition": {
        "IpAddress": {
          "acs:SourceIp": "xxx.x.x/xx"
        }
      },
      "Effect": "Allow",
      "Resource": "acs:imagesearch:cn-shanghai:1234:instance/*"
    }
  ],
  "Version": "1"
}
```

```
}

```

## 2. Authorize the current policy to your specified subaccount.

### Authorization example 2

For a subaccount under the primary account (accountId "1234" ), assign all operation permissions, except for CreateInstance, over the specified instances in China East 1 (Hangzhou) on the console, and set the instances to be accessible from only the specified IP address.

After this policy is created on the console of the primary account, you should authorize the subaccount through your primary account on the RAM console or use RAM SDK to authorize the subaccount.

### 1. Create a policy

```
{
  "Statement": [
    {
      "Action": [
        "elasticsearch : ListInstance "
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "xxx . xx . xxx . x / xx "
        }
      },
      "Effect": "Allow",
      "Resource": "acs : elasticsearch : cn - shanghai : 1234 : instance /*"
    },
    {
      "Action": [
        "elasticsearch : DescribeInstance ",
        "elasticsearch : DeleteInstance ",
        "elasticsearch : RestartInstance ",
        "elasticsearch : UpdateInstance "
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "xxx . xx . xxx . x / xx "
        }
      },
      "Effect": "Allow",
      "Resource": "acs : elasticsearch : cn - hangzhou : 1234 : instances /$ instanceId "
    }
  ],
  "Version": " 1 "
}
```

## 2. Authorize the current policy to your specified subaccount.

### Authorization example 3



To a subaccount under the primary account (accountId “1234” ), assign all operation permissions over all instances in all regions supported by Alibaba Cloud Elasticsearch on the console.

After this policy is created on the console of the primary account, you should authorize the subaccount through your primary account on the RAM console or use RAM SDK to authorize the subaccount.

### 1. Create a policy

```
{
  "Statement": [
    {
      "Action": [
        "elasticsearch:*"
      ],
      "Effect": "Allow",
      "Resource": "acs:elasticsearch:*:1234:instance/*"
    }
  ],
  "Version": "1"
}
```

### 2. Authorize the current policy to your specified subaccount.

#### Authorization example 4

To a subaccount under the primary account (accountId “1234” ), assign all operation permissions, except for CreateInstance and ListInstance, over specified instances in all regions supported by Alibaba Cloud Elasticsearch on the console.

After this policy is created on the console of the primary account, you should authorize the subaccount through your primary account on the RAM console or use RAM SDK to authorize the subaccount.

### 1. Create a policy

```
{
  "Statement": [
    {
      "Action": [
        "elasticsearch:DescribeInstance",
        "elasticsearch:DeleteInstance",
        "elasticsearch:UpdateInstance",
        "elasticsearch:RestartInstance"
      ],
      "Effect": "Allow",
      "Resource": "acs:elasticsearch:*:1234:instances/${instanceId}"
    }
  ],
  "Version": "1"
}
```

```
}
```

2. Authorize the current policy to your specified subaccount.

## 3 Temporary access token

Users (people or applications) that only access your cloud resources occasionally are called temporary users. You can use Security Token Service (STS, an extended authorization service of RAM) to issue an access token to these users (subaccounts). The permission and automatic expiration time of the token can be defined as required upon issuing.

The advantage of using the STS access token to authorize temporary users is making the authorization more controllable. You do not need to create a RAM user account and key for the temporary users. The RAM user account and key are valid in the long term but the temporary users do not need to access the resources for long. For use cases, see [#unique\\_7](#) and [#unique\\_8](#).

### Create a role

#### 1. On the RAM console, choose RAM Roles > Create RAM Role

The screenshot shows the RAM console interface. On the left, the 'RAM Roles' menu item is highlighted. The main panel displays the 'RAM Roles' page. A tooltip titled 'What is a RAM Role?' is visible, explaining that RAM roles are used to grant access to trusted entities like RAM users, applications, and Alibaba Cloud services. Below the tooltip, there is a 'Create RAM Role' button and a search bar. A table lists existing roles with columns for 'RAM Role Name', 'Note', 'Created At', and 'Actions'.

<input type="checkbox"/>	RAM Role Name	Note	Created At	Actions
<input type="checkbox"/>	[Redacted]	[Redacted]	Dec 18, 2018, 10:27:32	<a href="#">Add Permissions</a> <a href="#">Delete RAM Role</a>
<input type="checkbox"/>	[Redacted]	[Redacted]	Sep 29, 2018, 14:11:40	<a href="#">Add Permissions</a> <a href="#">Delete RAM Role</a>
<input type="checkbox"/>	[Redacted]	[Redacted]	Oct 26, 2018, 17:06:46	<a href="#">Add Permissions</a> <a href="#">Delete RAM Role</a>

2. Select the role type. Here, the role User is selected.

RAM Role Type

☒ User RAM Role

A RAM user of a trusted Alibaba Cloud account can assume the RAM role to access your cloud resources. A trusted Alibaba Cloud account can be the current account or another Alibaba Cloud account.

☐ Service RAM Role

A trusted Alibaba Cloud service can assume the RAM role to access your cloud resources.

3. Enter the type information. A subaccount of a trusted account can play the created role.

\* Select Alibaba Cloud Account

☒ Current Alibaba Cloud Account

☐ Other Alibaba Cloud Account

4. Enter the role name.

\* RAM Role Name

The name can contain a maximum of 64 characters, only English letters, numbers, and hyphens (-) are accepted.

Note

5. After a role is created, authorize the role. For details, see [#unique\\_9](#) and [#unique\\_5](#).

### Temporary access authorization

Before using STS for access authorization, authorize the role to be assumed by the subaccount of the trusted cloud account created in Step 3. If any subaccount could

assume these roles, unpredictable risks may occur. Therefore, in order to assume the corresponding role, a subaccount has to have explicitly configured permissions.

#### Authorization of the trusted cloud account

1. Click Policy Management on the left side of the page to go to the Policy Management page.
2. Click Create Authorization Policy on the right side of the page to go to the Create Authorization Policy page.
3. Select a blank template to go to the Create Custom Authorization Policy page.
4. Enter the authorization policy name and fill the following content to the policy content field.

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "acs:ram::${aliyunID}:role/${roleName}"
    }
  ]
}
```

`${aliyunID}` indicates the ID of the user that creates the role.

`${roleName}` indicates the role name in lowercase.



#### Note:

The resource details can be obtained from the Arn field in Role Details and Basic Information.

Basic Information			
Role Name		Created At	Dec 18, 2018, 10:27:32
Note		ARN	acsram:role/aliyuna

5. On the User Management page, authorize the permission of the role created for the subaccount. For details, see [#unique\\_9](#).

#### Role assumed by a subaccount

After logging on to the console through the subaccount, the subaccount can switch to the authorized role assumed by the subaccount to practise permissions of the role.

The steps are as follows:

1. Move the mouse to the profile picture on the upper-right corner of the navigation bar, and click Switch Role in the window.
2. Enter the enterprise alias of the account with which you intend to create a role. If the enterprise alias is not modified, the account ID is used by default. Enter the role name and then click Switch to switch to the specified role.

## 4 RAM

---