ALIBABA CLOUD

Alibaba Cloud

Elasticsearch

RAM

Document Version: 20200902

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Resource types

This topic describes the types of resources that are supported by Elasticsearch. You can grant different permissions to different users.

Resource types and ARNs

The following table lists the resource types and ARNs that are supported by Elasticsearch.

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/*

- *$regionId*: The region ID of the Elasticsearch instance. This field can be replaced with an asterisk (*).
- *$accountId*: The ID of your Alibaba Cloud account. This field can be replaced with an asterisk (*).
- *$instanceId*: The ID of the Elasticsearch instance. This field can be replaced with an asterisk (*).

For more information about how to grant permissions on Elasticsearch resources, see the examples in Permission policies.

Permissions to access Elasticsearch instances

> Note The following ARNs are shortened. For more information about the full names, see Resource types and ARNs.

- Actions on Elasticsearch instances

Action	Description	ARN
elasticsearch:CreateInstance	Creates an Elasticsearch instance.	instances/*
elasticsearch:ListInstance	Queries Elasticsearch instances.	instances/*
elasticsearch:DescribeInstance	Queries the description of an Elasticsearch instance.	instances/* or instances/*$instanceId*

Action	Description	ARN
elasticsearch:DeleteInstance	Deletes an Elasticsearch instance.	instances/* or instances/*$instanceId*
elasticsearch:RestartInstance	Restarts an Elasticsearch instance.	instances/* or instances/*$instanceId*
elasticsearch:UpdateInstance	Updates an Elasticsearch instance.	instances/* or instances/*$instanceId*

- Actions on plug-ins

Action	Description	ARN
elasticsearch:ListPlugin	Queries plug-ins.	instances/*$instanceId*
elasticsearch:InstallSystemPlugin	Installs a system plug-in.	instances/*$instanceId*
elasticsearch:UninstallPlugin	Uninstalls a system plug-in.	instances/*$instanceId*

- Actions on networks

Action	Description	ARN
elasticsearch:UpdatePublicNetwork	Specifies whether to allow access from public IP addresses.	instances/*$instanceId*
elasticsearch:UpdatePublicIps	Modifies the whitelist of public IP addresses.	instances/*$instanceId*
elasticsearch:UpdateWhiteIps	Modifies the VPC whitelist.	instances/*$instanceId*
elasticsearch:UpdateKibanaIps	Modifies the Kibana whitelist.	instances/*$instanceId*

- Actions on dictionaries

Action	Description	ARN
elasticsearch:UpdateDict	Modifies the IK analyzer and synonym dictionary.	instances/*$instanceId*

Permissions to access CloudMonitor

> **Note** The following ARNs are shortened by using an asterisk (*).

Action	Description	ARN
cms:ListProductOfActiveAlert	Queries services that have enabled CloudMonitor.	*
cms:ListAlarm	Queries a specific or all alert rule settings.	*
cms:QueryMetricList	Queries the metric data of a specific instance over a period of time.	*

Permissions to query VPCs and VSwitches on the Elasticsearch purchase page

Note The following ARNs are shortened. For more information about the full names, see Resource types and ARNs.

Action	Description	ARN
DescribeVpcs	Queries VPCs.	vpc/*
DescribeVswitches	Queries VSwitches.	vswitch/*

Permissions to perform intelligent O&M

Note The following ARNs are shortened. For more information about the full names, see Resource types and ARNs.

Action	Description	ARN
elasticsearch:OpenDiagnosis	Enables health diagnosis.	instances/* or instances/*$instanceId*
elasticsearch:CloseDiagnosis	Disables health diagnosis.	instances/* or instances/*$instanceId*
elasticsearch:UpdateDiagnosisSettings	Updates the health diagnosis settings.	instances/* or instances/*$instanceId*
elasticsearch:DescribeDiagnosisSettings	Queries the health diagnosis settings.	instances/* or instances/*$instanceId*
elasticsearch:ListInstanceIndices	Queries instance indexes.	instances/* or instances/*$instanceId*

Action	Description	ARN
elasticsearch:DiagnoseInstance	Starts health diagnosis.	instances/* or instances/$instanceId
elasticsearch:ListDiagnoseReportIds	Queries diagnosis report IDs.	instances/* or instances/$instanceId
elasticsearch:DescribeDiagnoseReport	Queries the details of a diagnosis report.	instances/* or instances/$instanceId
elasticsearch:ListDiagnoseReport	Queries diagnosis reports.	instances/* or instances/$instanceId

Supported regions

Region supported by Elasticsearch	Region ID
China (Hangzhou)	cn-hangzhou-b
China (Beijing)	cn-beijing
China (Shanghai)	cn-shanghai
China (Shenzhen)	cn-shenzhen
India (Mumbai)	ap-south-1
Singapore	ap-southeast-1
China (Hong Kong)	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-Beijing Winter Olympics)	cn-zhangjiakou

2.Create a custom policy

Create a custom policy in Elasticsearch

This topic describes how to create a custom policy in Elasticsearch. Custom policies enable finer-grained access control than system policies.

Elasticsearch custom policy

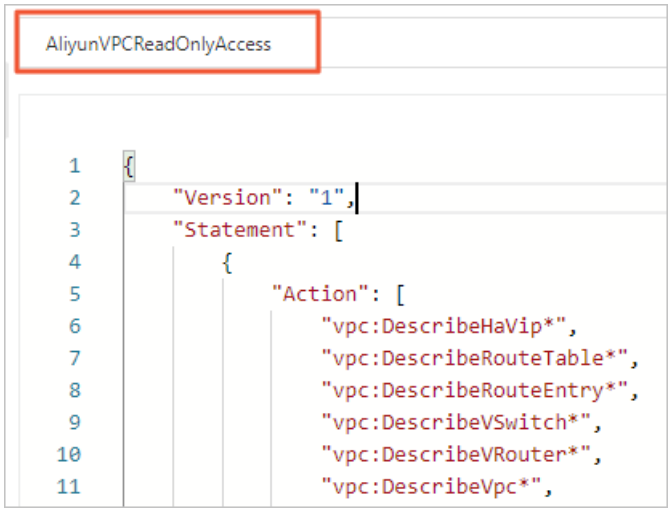
Prerequisites

You have understood the policy structure and syntax. For more information, see Policy structure and syntax.

Context

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Policies** under **Permissions**.
3. On the page that appears, click **Create Policy**.
4. On the Create Custom Policy page, specify the **Policy Name** and **Note** parameters.
5. Under **Configuration Mode**, select **Script**.
6. In the **Policy Document** section, select an existing system policy and edit the script.



Note You can enter keywords into the search box to perform fuzzy search.

Enter a permission script as required.

- Permission to access the Virtual Private Cloud (VPC) to which the Elasticsearch cluster belongs

```
"vpc:DescribeVSwitch*","vpc:DescribeVpc*"
```

> **Note** For more information, see the template for the **AliyunVPCReadOnlyAccess** policy.

- **Permission to purchase clusters**

```
["bss:PayOrder"]
```

> **Note** For more information, see the template for the **AliyunBSSOrderAccess** policy.

- **Permission to call API operations**

Method	URI	Resource	Operation
GET	/instances	instances/*	ListInstance
POST	/instances	instances/*	CreateInstance
GET	/instances/$instanceId	instances/$instanceId	DescribeInstance
DELETE	/instances/$instanceId	instances/$instanceId	DeleteInstance
POST	/instances/$instanceId/actions/restart	instances/$instanceId	RestartInstance
PUT	/instances/$instanceId	instances/$instanceId	UpdateInstance

Examples:

> **Notice** If tags are bound to your Elasticsearch cluster, you must grant operation permissions on the tags to RAM users. For more information, see Grant permissions on tags to a RAM user.

- In the following example, a RAM user of the Alibaba Cloud account whose account ID is 1234 is granted the operation permissions (except the cluster creation permission) on all Elasticsearch clusters in the China (Hangzhou) region. In addition, the policy allows only specified IP addresses to access the clusters.

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

- In the following example, a RAM user of the Alibaba Cloud account whose account ID is 1234 is granted the operation permissions (except the cluster creation permission) on specified Elasticsearch clusters in the China (Hangzhou) region. In addition, the policy allows only specified IP addresses to access the clusters.

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

- In the following example, a RAM user of the Alibaba Cloud account whose account ID is 1234 is granted all the operation permissions on Elasticsearch clusters in all regions.

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

- In the following example, a RAM user of the Alibaba Cloud account whose account ID is 1234 is granted the operation permissions (except the cluster creation and query permissions) on Elasticsearch clusters in all regions.

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

7. Click **OK**.

What's next

You can attach the created custom policy to a RAM user for authorization. For more information, see Grant permissions to a RAM user.

3.Grant permissions on tags to a RAM user

Grant a RAM user permissions on tags bound to Elasticsearch clusters

This topic describes how to grant a RAM user operation permissions specified in a custom policy on the tags that are bound to Elasticsearch clusters.

permission policies for tags bound to Elasticsearch clusters operation permissions on tags bound to Elasticsearch clusters

> **Notice** For information about how to create a custom policy, see Create a custom policy. After you create a policy in the RAM console with your Alibaba Cloud account, you must use the RAM console or the RAM SDK to grant the required permissions to a RAM user. For more information, see Grant permissions to a RAM user.

Authorize a RAM user to create or update tags for specified Elasticsearch clusters

In the following example, a RAM user of the Alibaba Cloud account whose account ID is 1234 is granted the permissions to create tags for Elasticsearch clusters `es-instance1` and `es-instance2` in the China (Hangzhou) region.

```
{
"Statement": [
{
"Action": [
"elasticsearch:CreateTags"
],
"Effect": "Allow",
"Resource": [
"acs:elasticsearch:cn-hangzhou:1234:tags/es-instance1",
"acs:elasticsearch:cn-hangzhou:1234:tags/es-instance2",
]
}
],
"Version": "1"
}
```

Authorize a RAM user to delete the tags of specified Elasticsearch clusters

In the following example, a RAM user of the Alibaba Cloud account whose account ID is 1234 is granted the permissions to delete the tags of Elasticsearch clusters `es-instance1` and `es-instance2` in the China (Hangzhou) region.

```
{
"Statement": [
{
"Action": [
"elasticsearch:RemoveTags"
],
"Effect": "Allow",
"Resource": [
"acs:elasticsearch:cn-hangzhou:1234:tags/es-instance1",
"acs:elasticsearch:cn-hangzhou:1234:tags/es-instance2",
]
}
],
"Version": "1"
}
```

Authorize a RAM user to query the tags of specified Elasticsearch clusters

In the following example, a RAM user of the Alibaba Cloud account whose account ID is 1234 is granted the permissions to query the tags of Elasticsearch clusters `es-instance1` and `es-instance2` in the China (Hangzhou) region.

```
{
"Statement": [
{
"Action": [
"elasticsearch:ListTags"
],
"Effect": "Allow",
"Resource": [
"acs:elasticsearch:cn-hangzhou:1234:tags/es-instance1",
"acs:elasticsearch:cn-hangzhou:1234:tags/es-instance2",
]
}
],
"Version": "1"
}
```

Authorize a RAM user to query the tags of all Elasticsearch clusters

In the following example, a RAM user of the Alibaba Cloud account whose account ID is 1234 is granted the permissions to query the tags of all Elasticsearch clusters in the China (Hangzhou) region.

```
{
"Statement": [
{
"Action": [
"elasticsearch:ListTags"
],
"Effect": "Allow",
"Resource": "acs:elasticsearch:cn-hangzhou:1234:tags/*"
}
],
"Version": "1"
}
```

Authorize a RAM user to perform operations on Elasticsearch clusters bound with specified tags

In the following example, a RAM user of the Alibaba Cloud account whose account ID is 1234 is granted the permissions to perform operations only on Elasticsearch clusters bound with tags `name:liumi`, `env:test`, and `env:pre`.

```
{
"Statement": [
{
"Action": [
"elasticsearch:ListTags"
],
"Effect": "Allow",
"Resource": "acs:elasticsearch:cn-hangzhou:1234:tags/*"
}
],
"Version": "1"
}
```

4.Grant permissions to a RAM user

Grant permissions to a RAM user

This topic describes how to grant a RAM user operation permissions on Elasticsearch, such as the cluster creation and query permissions. Elasticsearch supports system and custom policies.

grant permissions to a RAM user grant permissions to a RAM user

Prerequisites

- A RAM user is created. For more information, see Create a RAM user.
- A custom policy is created.

  If system policies do not meet your requirements, create a custom policy. For more information, see Create a custom policy.

  > Note Elasticsearch supports the following system policies:
  >
  > - `AliyunElasticsearchReadOnlyAccess`: the read-only permission to access Elasticsearch or Logstash clusters. This permission can be granted to read-only users.
  > - `AliyunElasticsearchFullAccess`: the permission to manage Elasticsearch or Logstash clusters. This permission can be granted to administrators.

Context

This topic describes how to grant permissions to a RAM user on the Grants page of the RAM console. You can also grant permissions to a RAM user on the Users page. For more information, see Grant permissions to a RAM user.

> Note

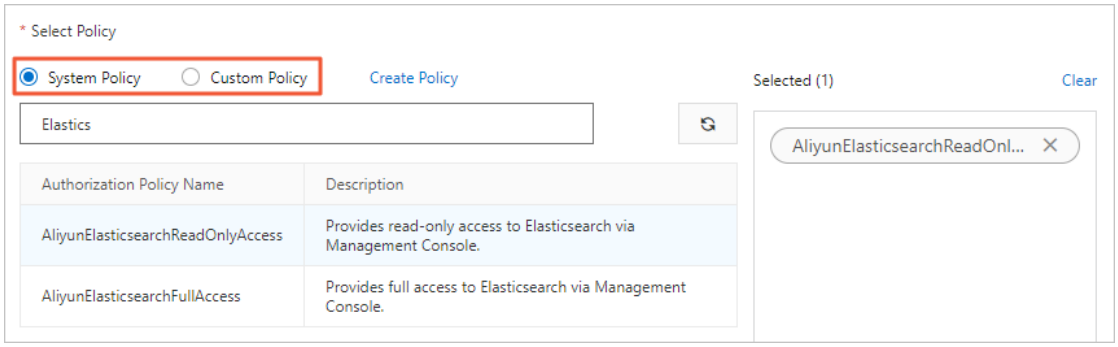
Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Grants** under **Permissions**.
3. Click **Grant Permission**.
4. Under **Principal**, enter a principal name and click the target principal.

   > Note You can enter a name of the RAM user, user group, or role for a fuzzy search.

5. In the **Select Policy** section, grant permissions to the principal.

i. Select **System Policy** or **Custom Policy**.



ii. Find the target policy.

> **Note** You can also enter the policy name in the search box to perform fuzzy search.

iii. In the **Authorization Policy Name** column, click the target policy.

6. Click **OK**.
7. Click **Finished**.

What's next

If a RAM user no longer requires a permission, you can remove the permission for the user. For more information, see Remove permissions from a RAM user.

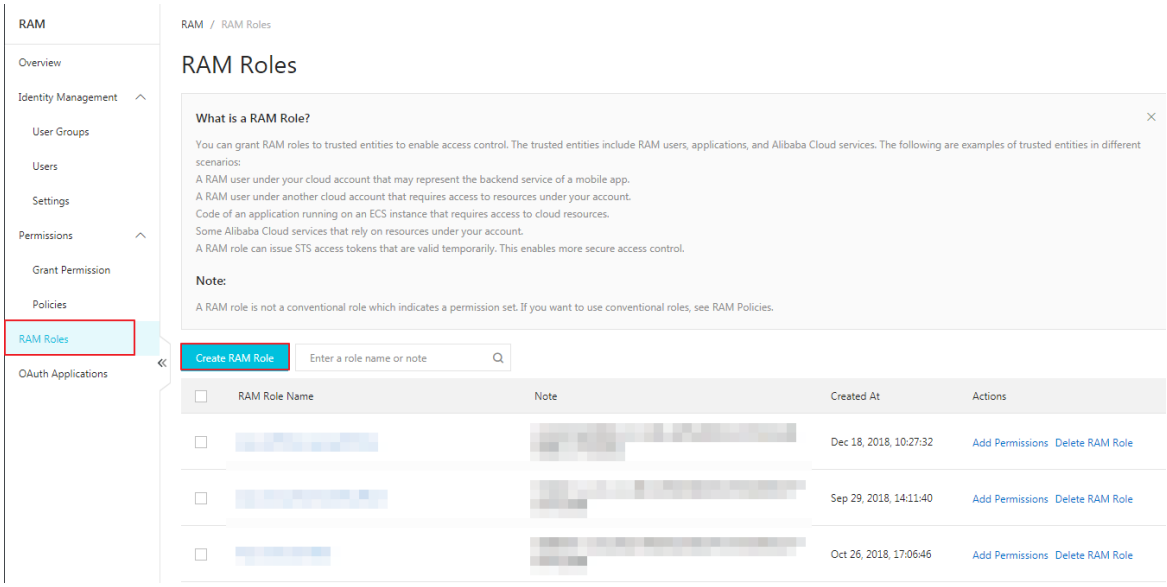
5.Temporary access token

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.

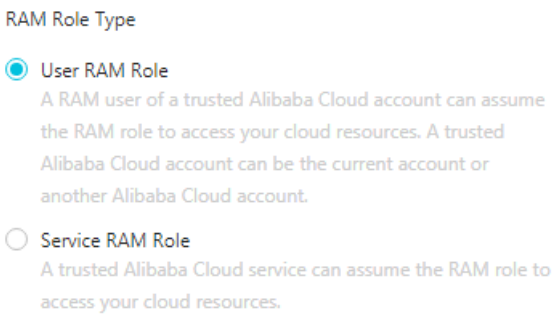
The advantage of using the STS access token to authorize temporary users is making the authorization more controllable. You do not need to create a RAM user account and key for the temporary users. The RAM user account and key are valid in the long term but the temporary users do not need to access the resources for long. For use cases, see Use an STS token for authorizing a mobile app to access Alibaba Cloud resources and Use a RAM role to grant permissions across Alibaba Cloud accounts.

Create a role

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

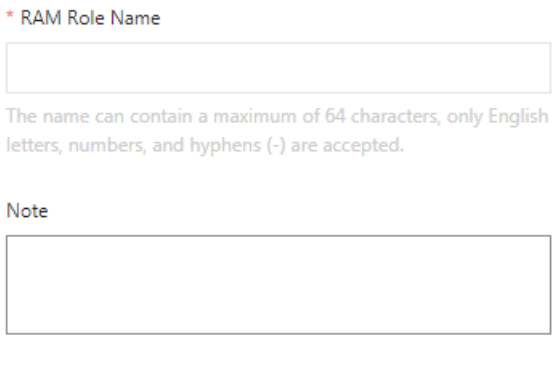


2. Select the role type. Here, the role **User** is selected.



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

4. Enter the role name.



5. After a role is created, authorize the role. For details, see Permission granting in RAM and Resource types.

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

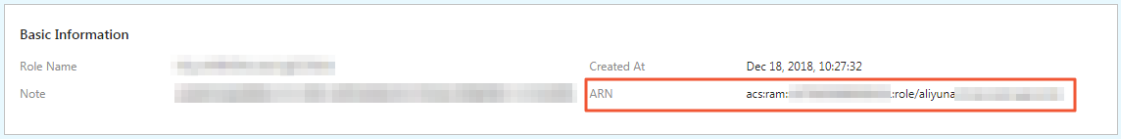
1. Click **Policy Management** on the left side of the page to go to the **Policy Management** page.
2. Click **Create Authorization Policy** on the right side of the page to go to the **Create Authorization Policy** page.
3. Select a **blank template** to go to the **Create Custom Authorization Policy** 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.



5. On the **User Management** page, authorize the permission of the role created for the subaccount. For details, see Permission granting in RAM.

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.

6.Manage Kibana role

6.1. Create a role

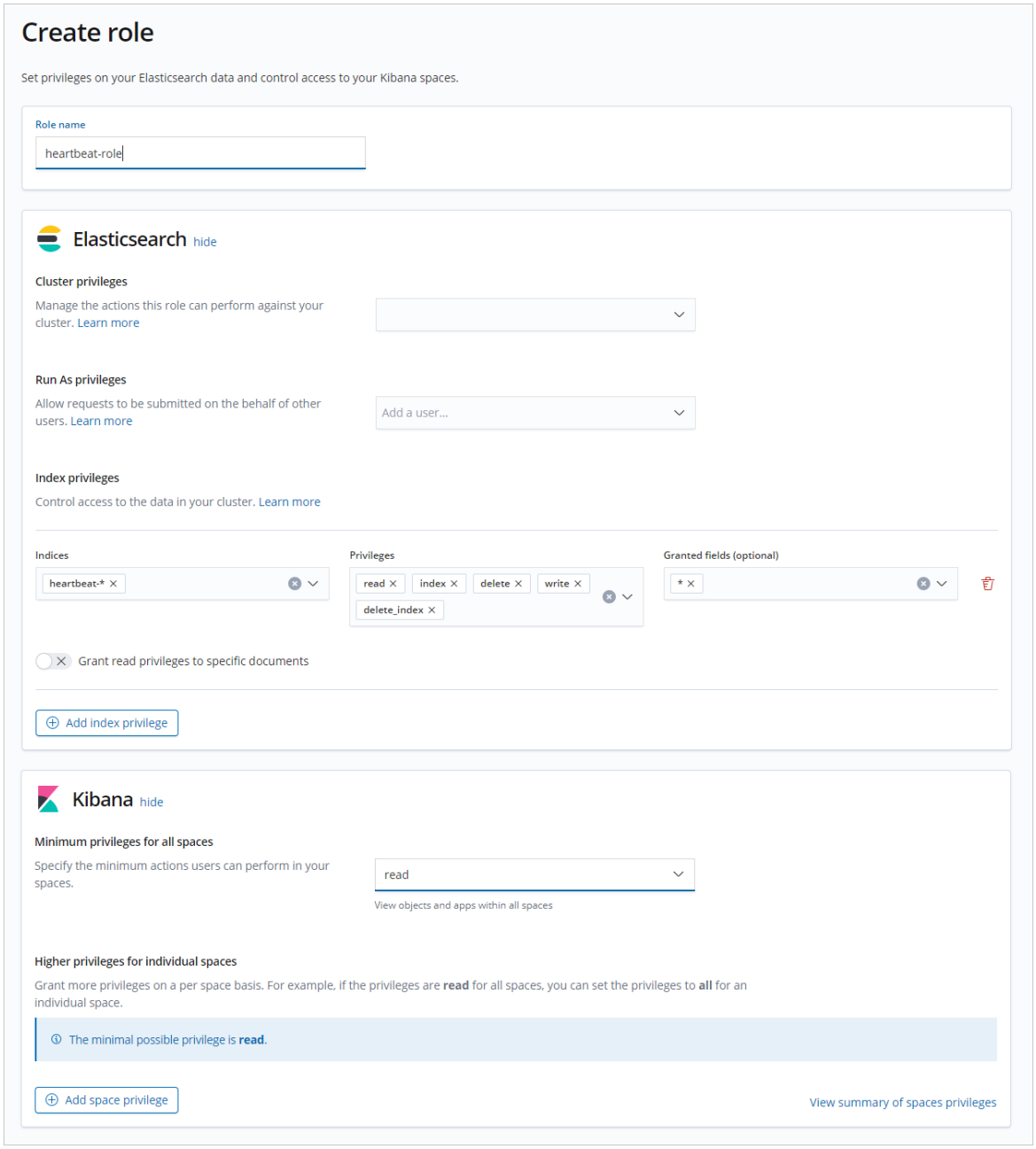
To authorize a custom user to manage a specific index in your cluster, you can create a role in the Kibana console and assign the role to the user. This topic describes how to create a role in the Kibana console.

Prerequisites

An Alibaba Cloud Elasticsearch cluster is created. For more information, see Create an Elasticsearch cluster.

Procedure

1. Log on to the Kibana console of your Elasticsearch cluster.For more information, see Log on to the Kibana console.
2. In the left-side navigation pane, click **Management**.
3. In the **Security** section, click **Roles**.
4. In the Roles section, click **Create role**.



Parameter	Description
Role name	The name of the role, which can be customized.
Cluster privileges	Optional. The permissions of the role. For more information, see Security privileges.
Run As privileges	Optional. The user who assumes the role. If no users are available, leave this parameter empty. You can assign the role when you create a user. For more information, see Create a user.

Parameter	Description
Index privileges	○ **Indices**: the index pattern, such as heartbeat-*. Note If no index patterns are available, click **Index Pattern** in the **Kibana** section of the **Management** page and then create an index pattern as prompted. ○ **Privileges**: the permissions of the role on the index. ○ **Granted fields (optional)**: Optional. The fields on which you want to grant permissions.
Minimum privileges for all spaces	The minimum permissions on all spaces. We recommend that you set the value to **read**. If you set the value to **none**, an error is reported when the user logs on to the Kibana console. Note You can also specify permissions for a specific space.

5. Click **Create role**.

6.2. Create a user

After you create a role, you can create a user and assign the role to the user so that the user has permissions to perform operations on a specific index in your cluster. This topic describes how to create a user in the Kibana console.

Prerequisites

- A role is created.

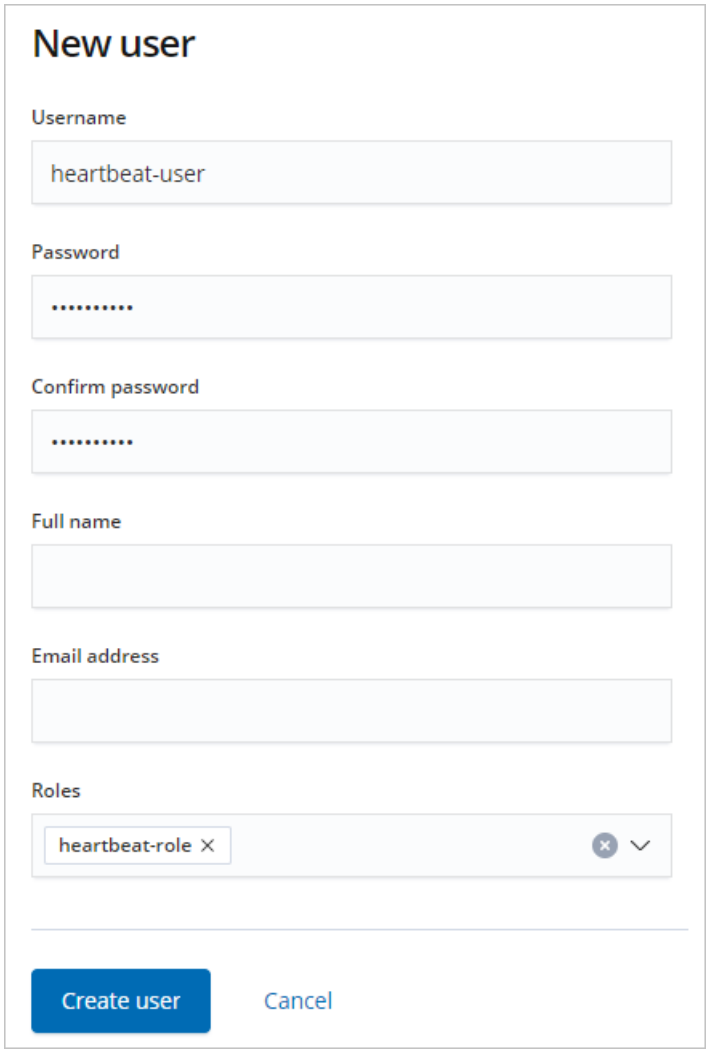
  The role must be granted the operation permissions on a specific index. For more information, see Create a role.

- An Alibaba Cloud Elasticsearch cluster is created.

  For more information, see Create an Elasticsearch cluster.

Procedure

1. Log on to the Kibana console of your Elasticsearch cluster.For more information, see Log on to the Kibana console.
2. In the left-side navigation pane, click **Management**.
3. In the **Security** section, click **Users**.
4. In the Users section, click **Create new user** in the upper-right corner.



Parameter	Description
Username	The username, which is used to log on to the Kibana console. The username can be customized.
Password	The password of the user, which is used to log on to the Kibana console. The password can be customized.
Confirm password	The value must be the same as that of the **Password** parameter.
Full name	The full name of the user, which can be customized.
Email address	The email address of the user.

Parameter	Description
Roles	The role that is assigned to the user. You can specify one or more roles. The roles can be existing roles or roles that are preset in the system. **Notice** If you specify a user when you create a role, you still need to specify this parameter. Otherwise, an error is reported when the user logs on to the Kibana console.

5. Click **Create user**.

7.FAQ about access control

FAQ about Elasticsearch access control

This topic provides answers to commonly asked questions about the access control of Alibaba Cloud Elasticsearch clusters.

FAQ about Elasticsearch access control no VPC available for an Elasticsearch cluster to purchase delete Elasticsearch clusters created by a temporary user

When I use a RAM user to purchase an Elasticsearch cluster, no Virtual Private Clouds (VPCs) are available on the buy page. Why?

Check whether the RAM user has permissions to obtain the list of VPCs. For more information, see View the basic information of a RAM user. If the RAM user does not have the required permissions, grant the permissions to the RAM user. For more information, see Grant permissions to a RAM user.

If a temporary user is deleted, will Elasticsearch clusters or data that is created by the user be deleted?

If a temporary user is deleted, the Elasticsearch clusters that are created by this user will not be deleted. In addition, the changes made by this user to the Elasticsearch clusters will not be restored. Operations performed by a temporary user are equivalent to those performed by an Alibaba Cloud account.

When I use Elasticsearch, the system displays the "The specified RAM user is not authorized. Check the permission of the RAM user and try again." error message. What do I do?

Grant one of the following permissions to the RAM user. For more information, see Grant permissions to a RAM user.

- `AliyunElasticsearchReadOnlyAccess` : the read-only permission to access Elasticsearch or Logstash clusters. This permission can be granted to read-only users.
- `AliyunElasticsearchFullAccess` : the permission to manage Elasticsearch or Logstash clusters. This permission can be granted to administrators.

How do I create a user that has read-only permissions on resources, such as indexes, of an Elasticsearch cluster?

Create a role that has such permissions in the Kibana console. Then, assign the role to a user. For more information, see Grant permissions on indexes.

When I use a user to which the required role is assigned to log on to the Kibana console, the console displays no indexes. Only the elastic account can be used to view indexes. What do I do?

When you create a user, grant the kibana_system permission to the user.