ALIBABA CLOUD

Alibaba Cloud

Elasticsearch

RAM

Document Version: 20220428

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.RAM-based Access Control

1.1. Objects supported for authorization

Elasticsearch objects supported for authorization

Custom policies can be used to manage user permissions in a fine-grained manner. You can use custom policies to control the access permissions of RAM users, RAM roles, or other Alibaba Cloud services or to authenticate team or department members. When you create a custom policy, you must configure the Action and Resource elements. This topic describes the objects that you can specify in the Action and Resource elements.

Background information

You can use your Alibaba Cloud account or RAM users within your Alibaba Cloud account to manage your Elasticsearch resources in the Elasticsearch console or by calling Elasticsearch API operations. Authorization is required in the following scenarios:

- A new RAM user within your Alibaba Cloud account does not have permissions to perform operations on the resources of the Alibaba Cloud account.
- You want to access Elasticsearch resources from other Alibaba Cloud services, or Elasticsearch needs to access the resources of other Alibaba Cloud services.
- You want to perform operations on Elasticsearch resources that require resource and API operation permissions to be granted by the resource owners.

Custom policies

You can create a custom policy in the RAM console or by calling the RAM API operation CreatePolicy.

If you use the **Script** configuration mode to create a custom policy in the RAM console, you must specify the **policy document** based on the JSON template that is provided in the console. The objects that you can specify in the Action and Resource elements are provided in the Objects supported for authorization section. For more information, see Create a custom policy and Policy elements.

```
{
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
                "elasticsearch:[Elasticsearch RAM Action]",
                "elasticsearch:ListInstance"
            ],
    "Resource": [
                "[Elasticsearch RAM Action Resource]",
                "acs:elasticsearch:cn-hangzhou:133071096032****:instances/es-cn-2r42b7uyg00
3k****"
            ]
  }
  ],
  "Version": "1"
}
```

Objects supported for authorization

- Manage clusters

Action	Resource	Action description
elasticsearch:CreateInstance	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/*	Creates a cluster.
elasticsearch:ListInstance		Queries the details of all clusters.
elasticsearch:DescribeInstance	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Queries the details of a cluster.
elasticsearch:EstimatedRestartTime		Queries the estimated time that is required to restart a cluster.
elasticsearch:RestartInstance		Restarts a cluster.
elasticsearch:UpdateInstanceChargeType		Switches the billing method of a cluster from pay-as-you-go to subscription.
elasticsearch:UpdateDescription		Changes the name of a cluster.
elasticsearch:DeleteInstance		Releases a pay-as-you-go cluster.
elasticsearch:CancelDeletion		Restores the released cluster that is frozen.
elasticsearch:RenewInstance		Renews a subscription cluster.
elasticsearch:ActivateZones		Restores disabled zones.
elasticsearch:DeactivateZones		Disables one or more zones if a cluster is deployed in multiple zones, and migrates the nodes in the disabled zones to other zones.
elasticsearch:InterruptElasticsearchTask		Pauses a task for a cluster.
elasticsearch:ResumeElasticsearchTask		Resumes a task for a cluster.
elasticsearch:DescribeElasticsearchHealth		Queries the health status of a cluster.
elasticsearch:ListInstanceIndices		Queries the indexes of a cluster.
elasticsearch:MigrateToOtherZone		Migrates nodes across zones.
elasticsearch:MoveResourceGroup		Migrates a cluster to a specified resource group.

Action	Resource	Action description
elasticsearch:ModifyInstanceMaintainTime		Enables or modifies the maintenance window of a cluster.
elasticsearch:ListShardRecoveries		Queries the progress of ongoing and completed data restoration tasks on shards.

- Manage tags

Action	Resource	Action description
elasticsearch:ListTags	acs:elasticsearch:<yourRegionId>:<yourAccountId>:tags/<yourInstanceId>	Queries all visible user tags.
elasticsearch:CreateTags		Creates or updates tags.
elasticsearch:RemoveTags		Removes tags.
elasticsearch:ListTagResources	○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:tags/* ○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:tags/<yourInstanceId>	Queries the relationships between visible tags and resources.

- Migrate data

Action	Resource	Action description
elasticsearch:ListDataTasks	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Queries the information of data migration tasks.
elasticsearch:CancelTask		Cancels a data migration task.
elasticsearch:CreateDataTasks		Creates a data migration task to migrate data to a specified cluster.
elasticsearch:DeleteDataTask		Deletes a data migration task.
elasticsearch:GetClusterDataInformation	○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/* ○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Queries the data information of a cluster.

- Upgrade or downgrade cluster configurations

Action	Resource	Action description
elasticsearch:UpgradeEngineVersion	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Upgrades the version or kernel version of a cluster.
elasticsearch:UpdateInstance		Modifies the configuration of a cluster.
elasticsearch:DowngradeInstance		○ Checks whether the data on some nodes in a cluster can be migrated before a cluster scale-in. ○ Migrates data before a cluster scale-in. ○ Checks whether some nodes in a cluster can be removed. ○ Scales in a cluster.

- Configure clusters

Action	Resource	Action description
elasticsearch:UpdateInstanceSettings	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Modifies the YML configuration file of a cluster.
elasticsearch:UpdateHotIkDicts		Performs a rolling update on the analysis-ik plug-in, including the IK main dictionary and stopword list of the plug-in.
elasticsearch:UpdateSynonymsDicts		Updates the synonym dictionary of a cluster.
elasticsearch:UpdateDict		Performs a standard update on the analysis-ik plug-in, including the IK main dictionary and stopword list of the plug-in.
elasticsearch:UpdateAliwsDict		Updates the dictionary file of the analysis-aliws plug-in.
elasticsearch:ListDictInformation		Queries and checks the information of the dictionary file that is stored in Object Storage Service (OSS) when the file is uploaded to a cluster.
elasticsearch:UpdateAdvancedSetting		Modifies the garbage collector configuration of a cluster.

Action	Resource	Action description
elasticsearch:DescribeTemplates		Queries the scenario-based configuration templates of a cluster.
elasticsearch:ListDicts		Queries the details of a specified type of dictionary and the link that is generated based on the related signature to download the dictionary.

- Manage plug-ins

Action	Resource	Action description
elasticsearch:ListPlugins	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Queries the plug-ins that are installed for a cluster.
elasticsearch:InstallSystemPlugin		Installs a built-in plug-in.
elasticsearch:UninstallPlugin		Removes a built-in plug-in.
elasticsearch:InstallUserPlugins		Installs a custom plug-in that is uploaded to the Elasticsearch console.

- Query logs

Action	Resource	Action description
elasticsearch:ListSearchLogs	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Queries the logs of a cluster.

- Configure security settings

Action	Resource	Action description
elasticsearch:TriggerNetwork		Enables or disables the Public Network Access or Private Network Access feature for Elasticsearch or Kibana.
elasticsearch:UpdatePrivateNetworkWhiteIps		Modifies the private IP address whitelist of a cluster.
elasticsearch:UpdatePublicWhiteIps		Modifies the public IP address whitelist of a cluster.

Action	Resource	Action description
elasticsearch:UpdatePublicNetwork	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Enables or disables the Public Network Access feature for a cluster.
elasticsearch:UpdateWhiteIps		Modifies the private IP address whitelist of a cluster.
elasticsearch:ModifyWhiteIps		Modifies the whitelists of a cluster.
elasticsearch:UpdateAdminPassword		Changes the password that corresponds to the elastic username of a cluster.
elasticsearch:OpenHttps		Enables HTTPS.
elasticsearch:CloseHttps		Disables HTTPS.
elasticsearch:AddConnectableCluster		Connects clusters.
elasticsearch:DeleteConnectedCluster		Disconnects clusters.
elasticsearch:DescribeConnectableClusters		Queries the clusters that can be connected to a specified cluster. The clusters that are connected to the specified cluster are excluded.
elasticsearch:ListConnectedClusters		Queries the clusters that are connected to a specified cluster.
elasticsearch:DeleteVpcEndpoint		Deletes an endpoint in the service virtual private cloud (VPC).
elasticsearch:ListVpcEndpoints		Queries the status of an endpoint in the service VPC.

- Back up data

Action	Resource	Action description
elasticsearch:CreateSnapshot	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Creates a snapshot for a cluster.
elasticsearch:AddSnapshotRepo		Adds a shared OSS repository to a cluster.

Action	Resource	Action description
elasticsearch:DeleteSnapshotRepo	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/*	Deletes a shared OSS repository.
elasticsearch:ListSnapshotReposByInstanceId		Queries the shared OSS repositories that are added to a cluster.
elasticsearch:ListAlternativeSnapshotRepos	acs:elasticsearch:<yourRegionId>:<yourAccountId>:snapshotrepository/*	Queries the shared OSS repositories that can be added to a cluster.
elasticsearch:DescribeSnapshotSetting	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Queries the data backup configurations of a cluster.
elasticsearch:UpdateSnapshotSetting		Modifies the data backup configurations of a cluster.

- Perform intelligent O&M

Action	Resource	Action description
elasticsearch:OpenDiagnosis	○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/* ○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Enables intelligent health diagnostics.
elasticsearch:CloseDiagnosis		Disables intelligent health diagnostics.
elasticsearch:UpdateDiagnosisSettings		Modifies health diagnostic settings.
elasticsearch:DiagnoseInstance		Starts intelligent health diagnostics.
elasticsearch:ListDiagnoseReport		Queries the details of diagnostic reports.
elasticsearch:ListDiagnoseReportIds		Queries the IDs of diagnostic reports.
elasticsearch:ListDiagnoseIndices		Queries cluster indexes.
elasticsearch:DescribeDiagnoseReport		Queries the details of a diagnostic report.
elasticsearch:DescribeDiagnosisSettings		Queries health diagnostic settings.

Action	Resource	Action description
elasticsearch:DescribeKibanaSettings	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	Queries the configuration of Kibana.
elasticsearch:UpdateKibanaSettings		Modifies the configuration of Kibana.
elasticsearch:ListKibanaPlugins		Queries the plug-ins that are installed for Kibana.
elasticsearch:InstallKibanaSystemPlugin		Installs a plug-in for Kibana.
elasticsearch:UninstallKibanaPlugin		Removes a plug-in for Kibana.
elasticsearch:UpdateKibanaWhiteIps		Modifies the IP address whitelists that allow access to the Kibana console of a cluster.

- Manage clusters

Action	Resource	Action description
elasticsearch:CreateLogstash	○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/* ○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	Creates a cluster.
elasticsearch:ListLogstash		Queries the details of a specified cluster or all clusters.
elasticsearch:DescribeLogstash	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	Queries the details of a cluster.
elasticsearch:UpdateLogstash		Modifies some information of a cluster, such as the number of nodes, quota, name, and hard disk size.
elasticsearch:RenewLogstash		Renews a cluster.
elasticsearch:RestartLogstash		Restarts a cluster.
elasticsearch:EstimatedLogstashRestartTime		Queries the estimated time that is required to restart a cluster.
elasticsearch:UpdateLogstashDescription		Changes the name of a cluster.

Action	Resource	Action description
elasticsearch:UpdateLogstashChargeType		Switches the billing method of a cluster from pay-as-you-go to subscription.
elasticsearch:DeleteLogstash		Releases a pay-as-you-go cluster.
elasticsearch:CancelLogstashDeletion		Restores a released cluster that is frozen.

- Configure clusters

Action	Resource	Action description
elasticsearch:UpdateLogstashSettings	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	Modifies the configuration of a cluster.
elasticsearch:ListExtendfiles		Queries the third-party libraries that are configured for a cluster.
elasticsearch:UpdateExtendfiles		Updates the third-party libraries that are configured for a cluster.

- Manage plug-ins

Action	Resource	Action description
elasticsearch:ListPlugin	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	Queries plug-ins.
elasticsearch:InstallSystemPlugin		Installs a built-in plug-in.
elasticsearch:UninstallSystemPlugin		Removes a built-in plug-in.

- Monitor clusters and query logs

Action	Resource	Action description
elasticsearch:ListAvailableEsInstanceIds	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	Queries the Elasticsearch clusters that have X-Pack monitoring capabilities and can be associated with a Logstash cluster.
elasticsearch:ValidateConnection		Checks the connectivity between a Logstash cluster and the associated Elasticsearch clusters.

Action	Resource	Action description
elasticsearch:UpdateXpackMonitorConfig		Modifies the X-Pack monitoring configuration of a cluster.
elasticsearch:DescribeXpackMonitorConfig		Queries the X-Pack monitoring configuration of a cluster.
elasticsearch:ListLogstashLog		Queries the logs of a cluster.

- Manage tasks

Action	Resource	Action description
elasticsearch:InterruptLogstashTask	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	Pauses a task of a cluster.
elasticsearch:ResumeLogstashTask		Resumes a task of a cluster.

- Manage pipelines

Action	Resource	Action description
elasticsearch:CreatePipelines	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	Creates a pipeline.
elasticsearch:ListPipeline		Queries pipelines.
elasticsearch:DescribePipeline		Queries the configuration of a pipeline.
elasticsearch:UpdatePipelines		Modifies the configuration of a pipeline.
elasticsearch:RunPipelines		Immediately deploys a pipeline.
elasticsearch:StopPipelines		Stops a pipeline.
elasticsearch:UpdatePipelineManagementConfig		Updates the pipeline management method.
elasticsearch:DescribePipelineManagementConfig		Queries pipeline management configurations.
elasticsearch:ListPipelineIds		Checks the connectivity between a Logstash cluster and the Kibana console of an Elasticsearch cluster and queries the IDs of pipelines that are created in the Kibana console of the Elasticsearch cluster.
elasticsearch:DeletePipelines		Deletes a pipeline.

Action	Resource	Action description
elasticsearch:CreateCollector	acs:elasticsearch:<yourRegionId>:<yourAccountId>:collectors/<yourCollectorId>	Creates a shipper.
elasticsearch:DescribeCollector		Queries the details of a shipper.
elasticsearch:ReinstallCollector		Reinstalls a shipper that fails to be installed when it is created.
elasticsearch:ListCollectors	acs:elasticsearch:<yourRegionId>:<yourAccountId>:collectors/*	Queries shippers.
elasticsearch:ListDefaultCollectorConfigurations		Queries the default configuration file of a shipper.
elasticsearch:UpdateCollectorName	acs:elasticsearch:<yourRegionId>:<yourAccountId>:collectors/<yourCollectorId>	Changes the name of a shipper.
elasticsearch:UpdateCollector		Modifies the information of a shipper.
elasticsearch:StartCollector		Starts a shipper.
elasticsearch:RestartCollector		Restarts a shipper.
elasticsearch:StopCollector		Stops a shipper.
elasticsearch:DeleteCollector		Deletes a shipper.
elasticsearch:ListEcsInstances		Queries Elastic Compute Service (ECS) instances.
elasticsearch:ModifyDeployMachine		Changes the ECS instances on which a shipper is installed.
elasticsearch:ListNodes		Queries the status of ECS instances on which a shipper is installed.
elasticsearch:ListAckClusters	acs:elasticsearch:<yourRegionId>:<yourAccountId>:ackClusters/*	Queries Container Service for Kubernetes (ACK) clusters.
elasticsearch:ListAckNamespaces	acs:elasticsearch:<yourRegionId>:<yourAccountId>:ackClusters/<yourClusterId>	Queries all namespaces of an ACK cluster.
elasticsearch:DescribeAckOperator		Queries the information of ES-operator that is installed for an ACK cluster.
elasticsearch:InstallAckOperator		Installs ES-operator for an ACK cluster.

Action	Resource	Action description
elasticsearch:InitializeOperationRole	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/*	Creates a service-linked role.

Action	Resource	Action description
cms:ListProductOfActiveAlert	acs:elasticsearch:<yourRegionId>:<yourAccountId>:*	Queries the services for which CloudMonitor is activated.
cms:ListAlarm		Queries the settings of a specified alert rule or all alert rules.
cms:QueryMetricList		Queries the monitoring data of a cluster over a specific period of time.

Action	Resource	Action description
elasticsearch:DescribeVpcs	acs:elasticsearch:<yourRegionId>:<yourAccountId>:vpc/*	Queries VPCs.
elasticsearch:DescribeVswitches	acs:elasticsearch:<yourRegionId>:<yourAccountId>:vswitch/*	Queries vSwitches.

Elasticsearch

Kibana

Logstash

Beats

Access control

CloudMonitor

VPCs and vSwitches displayed on the Elasticsearch buy page

Parameters

This section describes the parameters that are contained in the Resource element in the preceding section.

- <yourRegionId>: Set this parameter to the region ID of your Elasticsearch or Logstash cluster. You can also set this parameter to an asterisk (*) to indicate all regions. The following table lists the IDs of all regions where Elasticsearch and Logstash are available.

Region	Region ID	
	China (Shanghai)	cn-shanghai

Region	Region ID	
China	China (Shenzhen)	cn-shenzhen
	China (Qingdao)	cn-qingdao
	China (Zhangjiakou)	cn-zhangjiakou
	China (Beijing)	cn-beijing
	China (Hangzhou)	cn-hangzhou
	China (Hong Kong)	cn-hongkong
Asia Pacific	Singapore (Singapore)	ap-southeast-1
	Malaysia (Kuala Lumpur)	ap-southeast-3
	Japan (Tokyo)	ap-northeast-1
	Australia (Sydney)	ap-southeast-2
	Indonesia (Jakarta)	ap-southeast-5
Europe & Americas	US (Virginia)	us-east-1
	US (Silicon Valley)	us-west-1
	Germany (Frankfurt)	eu-central-1
	UK (London)	eu-west-1
Middle East & India	India (Mumbai)	ap-south-1

- <yourAccountId>: Set this parameter to the ID of your Alibaba Cloud account. You can also set this parameter to an asterisk (*) to indicate all accounts.
- <yourInstanceId>: Set this parameter to the ID of your Elasticsearch or Logstash cluster. You can also set this parameter to an asterisk (*) to indicate all clusters.
- <yourCollectorId>: Set this parameter to the ID of your Beats shipper.
- <yourClusterId>: Set this parameter to the ID of the ACK cluster for which your Beats shipper is installed.

1.2. Create a custom policy

Create a custom policy in Elasticsearch

If the system policies provided by Alibaba Cloud Elasticsearch do not meet your requirements, you can create custom policies. Custom policies enable finer-grained permission management than system policies. This topic describes how to create a custom policy and provides policy examples.

Context

Elasticsearch supports the following system policies:

- AliyunElasticsearchReadOnlyAccess: grants the read-only permissions on Elasticsearch or Logstash

- AliyunElasticsearchReadOnlyAccess: grants the read-only permissions on Elasticsearch or Logstash clusters. This policy can be attached to read-only users.
- AliyunElasticsearchFullAccess: grants the management permissions on Elasticsearch clusters, Logstash clusters, or Beats shippers. This policy can be attached to administrators.

> Note
>
> - The preceding policies contain only permissions on Elasticsearch clusters, Logstash clusters, or Beats shippers. The policies do not contain permissions on CloudMonitor or tags. If you want to grant permissions on CloudMonitor or tags, you must create the related custom policies and attach the policies to RAM users. For more information about how to grant permissions on CloudMonitor or tags, see Policy examples in this topic.
> - By default, Elasticsearch clusters are created in the default resource group. After you attach a custom policy for a specific cluster to a RAM user and use the RAM user to log on to the Elasticsearch console, all the clusters of your Alibaba Cloud account rather than the specific cluster are displayed in the console. If you want the console to display only the specific cluster, you can use a resource group to grant the permissions on the cluster to the RAM user. For more information, see Use a resource group to grant permissions on a specific cluster.

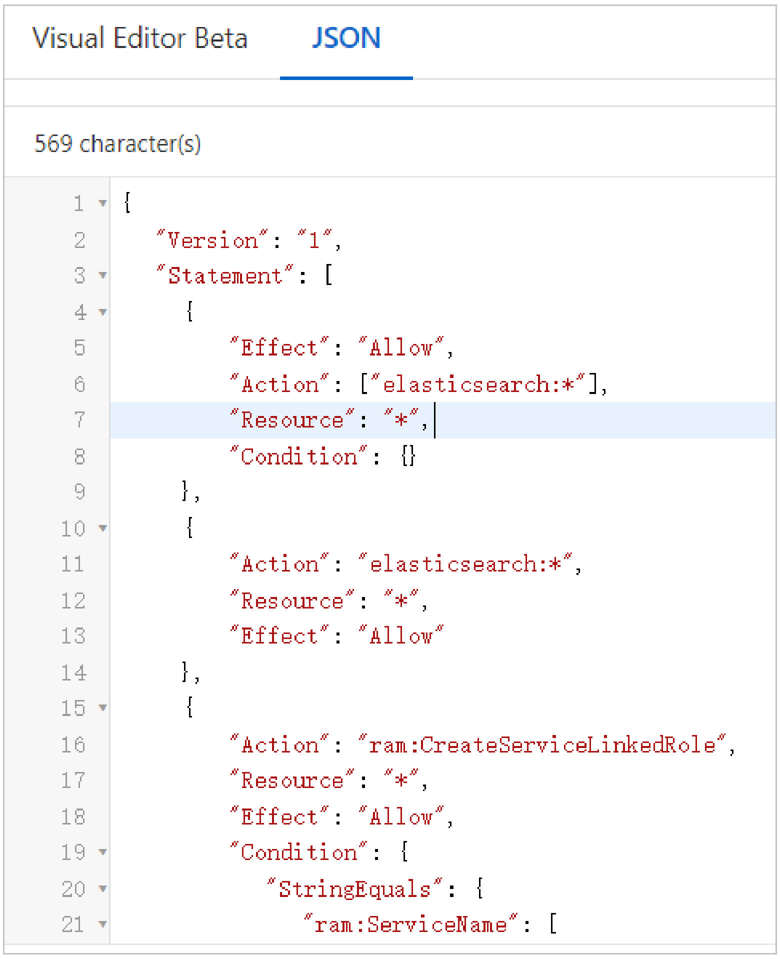
Prerequisites

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

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. On the **Create Policy** page, click the **JSON** tab.
5. On the JSON tab, enter the policy document and click **Next Step**.

   You can also click **Import System Policy** on the right, import an existing system policy as prompted in the Import System Policy dialog box, and then modify the policy to use the modified policy as a custom policy.



```
{
  "Version": "1",
  "Statement": [
    {
        "Effect": "Allow",
        "Action": ["elasticsearch:*"],
        "Resource": "*",
        "Condition": {}
    },
    {
        "Action": "elasticsearch:*",
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": "ram:CreateServiceLinkedRole",
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
          "StringEquals": {
            "ram:ServiceName": [
```

Enter a script for the permission that you want to grant. Examples:

- Permission to access the virtual private clouds (VPCs) that belong to your Alibaba Cloud account

  ```
  "elasticsearch:DescribeVpcs","elasticsearch:DescribeVSwitches"
  ```

  > Note For more information about the related policy document, see the document of the **AliyunVPCReadOnlyAccess** policy.

- Permission to pay for orders

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

  > Note For more information about the related policy document, see the document of the **AliyunBSSOrderAccess** policy.

- Permission to call API operations

Method	URI	Resource	Action
GET	/instances	instances/*	ListInstance
POST	/instances	instances/*	CreateInstance

Method	URI	Resource	Action
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

For more information, see Policy examples in this topic.

6. Configure the **Name** and **Note** parameters.
7. Check and optimize the content of the custom policy.
   - Basic optimization

     The system automatically optimizes the policy statement. The system performs the following operations during basic optimization:

     - Delete unnecessary conditions.
     - Delete unnecessary arrays.
   - (Optional)Advanced optimization

     You can move the pointer over **Optional: Advanced Optimize** and click **Perform**. The system performs the following operations during advanced optimization:

     - Split resources or conditions that are incompatible with actions.
     - Narrow down resources.
     - Deduplicate or merge policy statements.
8. Click **OK**.

Policy examples

> **Notice**
>
> Before you use the sample code provided in this section, you must replace the following information with your actual information:
>
> - *133071096032*****: Replace this ID with the ID of your Alibaba Cloud account. You can move the pointer over the profile picture in the upper-right corner of the console to obtain the ID of your Alibaba Cloud account.
> - *es-cn-tl32awopr002h*****: Replace this ID with the ID of the Elasticsearch cluster whose permissions you want to grant. For more information about how to obtain the ID, see View the basic information of a cluster.

- Policy for an administrator

  In this example, all the operation permissions on all Elasticsearch clusters are granted to a RAM user of the Alibaba Cloud account whose ID is *133071096032*****.

```
{
    "Statement": [
        {
            "Action": [
                "elasticsearch:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "cms:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "bss:PayOrder",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "ram:CreateServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "collector.elasticsearch.aliyuncs.com"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

- Policy for operation permissions on a specific cluster

  In this example, the following permissions are granted to a RAM user of the Alibaba Cloud account whose ID is *133071096032*****:

  - Permissions on CloudMonitor
  - Permission to perform all Elasticsearch-related operations on a specific cluster
  - Permission to view clusters
  - Permission to view all the tags that are added to clusters
  - Permission to view shippers

> **Note** External interfaces that are used to call some services, such as Beats, Advanced Monitoring and Alerting, and Tag, are integrated into the cluster management page of the Elasticsearch console. Therefore, when you grant the permissions on a specific cluster, you must refer to the following sample policy document.

```
{
    "Statement": [
        {
            "Action": [
                "elasticsearch:*"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:133071096032****:instances/es-cn-2r42b7uyg003k*****"
        },
        {
            "Action": [
                "cms:DescribeActiveMetricRuleList",
                "cms:ListAlarm",
                "cms:QueryMetricList"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "elasticsearch:ListTags"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:133071096032****:tags/*"
        },
        {
            "Action": [
                "elasticsearch:ListInstance",
                "elasticsearch:ListSnapshotReposByInstanceId"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:133071096032****:instances/*"
        },
        {
            "Action": [
                "elasticsearch:ListLogstash"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:133071096032****:logstashes/*"
        },
        {
            "Action": [
                "elasticsearch:ListCollectors"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:133071096032****:collectors/*"
        }
    ],
    "Version": "1"
}
```

Action element

Action	Description

`[`
`"cms:DescribeActiveMetricRuleList",`
`"cms:ListAlarm",`
`"cms:QueryMetricList"`
`]`
	The permissions on CloudMonitor.
	- `cms:DescribeActiveMetricRuleList` : the permission to query the services for which CloudMonitor is activated within the Alibaba Cloud account.
	- `cms:ListAlarm` : the permission to query all or specific alert rules.
	- `cms:QueryMetricList` : the permission to query the monitoring data of instances or clusters of a specific service within a period.

`"bss:PayOrder"`	The permission to pay for orders. After the RAM user is granted the permission, you can use the RAM user to pay for the purchase orders of resources.

`[`
`"elasticsearch:DescribeVpcs",`
`"elasticsearch:DescribeVSwitches"`
`]`
	The permissions to access the VPCs and vSwitches that belong to the Alibaba Cloud account. After the RAM user is granted the permissions, the VPC and vSwitch that belong to the Alibaba Cloud account can be selected when you use the RAM user to purchase resources.
	Notice When you authorize a RAM user to purchase resources, you must also specify `["bss:PayOrder"]` in the Action element. If you do not specify ["bss:PayOrder"], the system displays a message that indicates insufficient permissions when you use the RAM user to purchase resources.

`[`
`"elasticsearch:*"`
`]`
	All operation permissions on Elasticsearch clusters. After the RAM user is granted the permissions, you can use the RAM user to perform operations on all or specific clusters.
	Notice The permissions specified by `elasticsearch:*` do not include permissions on the Advanced Monitoring and Alerting, CloudMonitor, or Tag service. You must separately specify permissions on these services. If you do not specify permissions on these services, the system displays a message that indicates insufficient permissions after you use the RAM user to go to a related page. However, authorized features on this page can be used.

`[`
`"elasticsearch:ListTags"`
`]`
	The permission to query all the tags that are added to Elasticsearch clusters. After the RAM user is granted the permission, you can use the RAM user to view all the tags that are added to Elasticsearch clusters.

Action	Description

`[`
`"elasticsearch:ListInstance",`
`"elasticsearch:ListSnapshotReposByInstanceId"`
`]`
	- `elasticsearch:ListInstance`: the permission to query Elasticsearch clusters.
	- `elasticsearch:ListSnapshotReposByInstanceId`: the permission to query shared Object Storage Service (OSS) repositories.

`[`
`"elasticsearch:ListCollectors"`
`]`
	The permission to query Beats shippers. After the RAM user is granted the permission, you can use the RAM user to view all the created Beats shippers in the Elasticsearch console.

`[`
`"elasticsearch:ListLogstash"`
`]`
	The permission to query Logstash clusters. After the RAM user is granted the permission, you can use the RAM user to view all the Logstash clusters in the related region on the Logstash Clusters page.

Effect element

Effect	Description
Allow	Indicates that the RAM user can be used to perform the operations that are specified in the Action element.
Deny	Indicates that the RAM user cannot be used to perform the operations that are specified in the Action element.

Resource element

For more information, see Objects supported for authorization.

Resource	Description
*	Indicates all clusters.
*es-cn-tl32awopr002h*** *	Indicates a specific cluster. You must replace the ID with the ID of the cluster whose permissions you want to grant. For more information about how to obtain the ID, see View the basic information of a cluster.

What's next

After a custom policy is created, use your Alibaba Cloud account to attach the policy to a RAM user in the RAM console or by using a RAM SDK. For more information, see Grant permissions to a RAM user.

1.3. Use a resource group to grant permissions on a specific cluster

This topic describes how to use a resource group to grant permissions on a specific cluster to a RAM user in the RAM console.

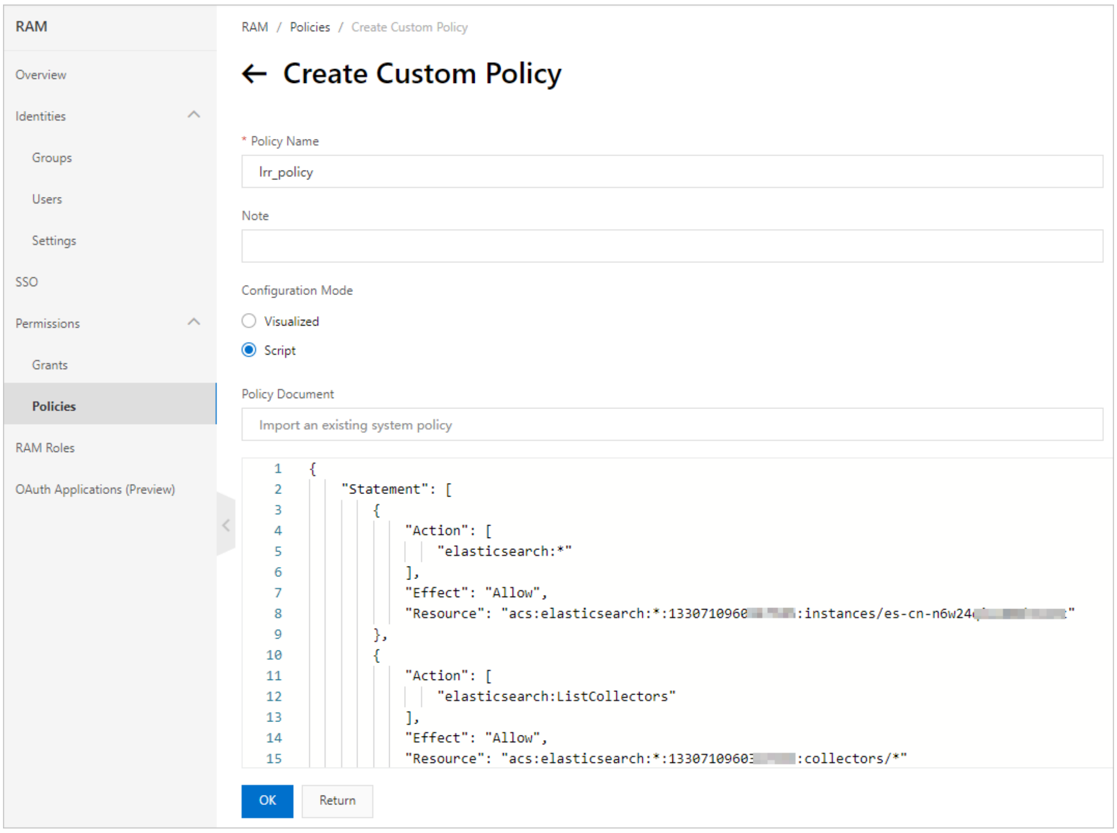
Background information

By default, Alibaba Cloud Elasticsearch clusters are created in the default resource group. After you attach a custom policy for a specific cluster to a RAM user and use the RAM user to log on to the Elasticsearch console, all the clusters of your Alibaba Cloud account rather than the specific cluster are displayed in the console. If you want the console to display only the specific cluster, you can use a resource group to grant the permissions on the cluster to the RAM user.

Step 1: Attach a custom policy whose effective scope is the entire Alibaba Cloud account to a RAM user of the account

1. Log on to the RAM console by using an Alibaba Cloud account.
2. Create a custom policy.
   i. In the left-side navigation pane, choose **Permissions > Policies**.
   ii. On the **Policies** page, click **Create Policy**.
   iii. Enter a name in the **Policy Name** field.

iv. Set **Configuration Mode** to **Script**.



Create Custom Policy

* Policy Name

lrr_policy

Note

Configuration Mode

○ Visualized

● Script

Policy Document

Import an existing system policy

```
{
    "Statement": [
        {
            "Action": [
                "elasticsearch:*"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:1330710960[redacted]:instances/es-cn-n6w24[redacted]"
        },
        {
            "Action": [
                "elasticsearch:ListCollectors"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:1330710960[redacted]:collectors/*"
```

v. Configure **Policy Document**. The following code provides an example.

```
{
    "Statement": [
        {
            "Action": [
                "elasticsearch:*"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:<yourAccountId>:instances/<yourInstanc
eId>"
        },
        {
            "Action": [
                "elasticsearch:ListCollectors"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:<yourAccountId>:collectors/*"
        },
        {
            "Action": [
                "elasticsearch:ListInstance",
                "elasticsearch:ListSnapshotReposByInstanceId"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:<yourAccountId>:instances/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cms:ListAlarm",
                "cms:DescribeActiveMetricRuleList",
                "cms:QueryMetricList"
            ],
            "Resource": "*"
        },
        {
            "Action": [
                "elasticsearch:ListTags"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:*:tags/*"
        },
        {
            "Action": [
                "elasticsearch:GetEmonProjectList"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:*:emonProjects/*"
        },
        {
            "Action": [
                "elasticsearch:getEmonUserConfig"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:*:emonUserConfig/*"
        },
       {
          "Action": "ims:*",
          "Effect": "Allow",
          "Resource": "acs:ims::<yourAccountId>:application/*"
       }
    ],
    "Version": "1"
}
```

Before you use the preceding code, you must replace the variables in the code with the desired values.

Variable	Description
<yourAccountId>	Replace this variable with the ID of your Alibaba Cloud account. You can move the pointer over the profile picture in the upper-right corner of the console to obtain the ID of your Alibaba Cloud account.
<yourInstanceId>	Replace this variable with the ID of the cluster whose permissions you want to grant. For more information about how to obtain the ID, see View the basic information of a cluster.

External interfaces that are used to call some services, such as Beats, Advanced Monitoring and Alerting, and Tag, are integrated into the cluster management page of the Elasticsearch console. Therefore, if you want to manage only the clusters in a specific resource group in the console, you must configure a custom policy whose effective scope is the entire Alibaba Cloud account and attach the policy to the RAM user. This way, the RAM user can pass permission verification on the cluster management page.

> **Note** After the policy for a specific Elasticsearch or Logstash cluster is created and attached to a RAM user, you can use the RAM user and one of the following URLs to directly access the Elasticsearch or Logstash cluster:
>
> - https://elasticsearch.console.aliyun.com/{regionId}/instances/{instanceId}/base
> - https://elasticsearch.console.aliyun.com/{regionId}/logstashes/{instanceId}/base

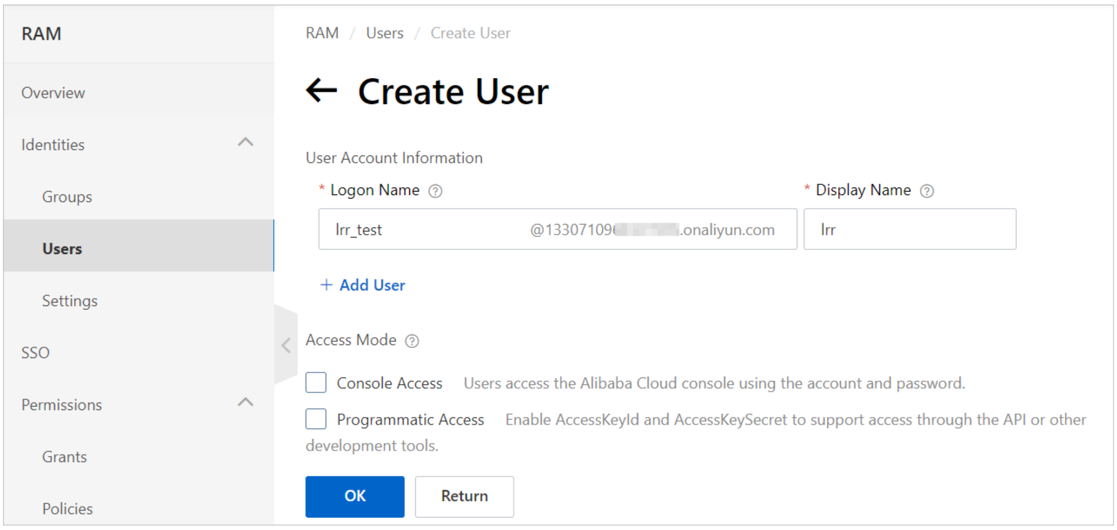
vi. Click **OK**.

3. Create a RAM user.

   i. In the left-side navigation pane, choose **Identities > Users**.

   ii. Click **Create User**.

   iii. On the **Create User** page, configure the **Logon Name** and **Display Name** parameters.



RAM / Users / Create User

Create User

User Account Information

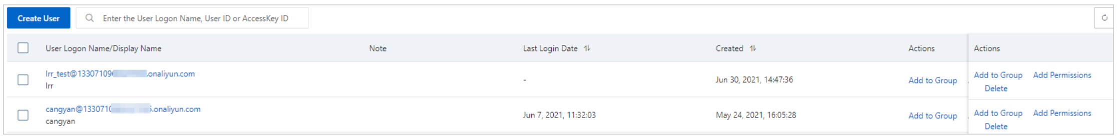
* Logon Name: lrr_test @1330710[redacted].onaliyun.com

* Display Name: lrr

□ Console Access Users access the Alibaba Cloud console using the account and password.

□ Programmatic Access Enable AccessKeyId and AccessKeySecret to support access through the API or other development tools.

   iv. Click **OK**. The newly created RAM user appears on the Users page.



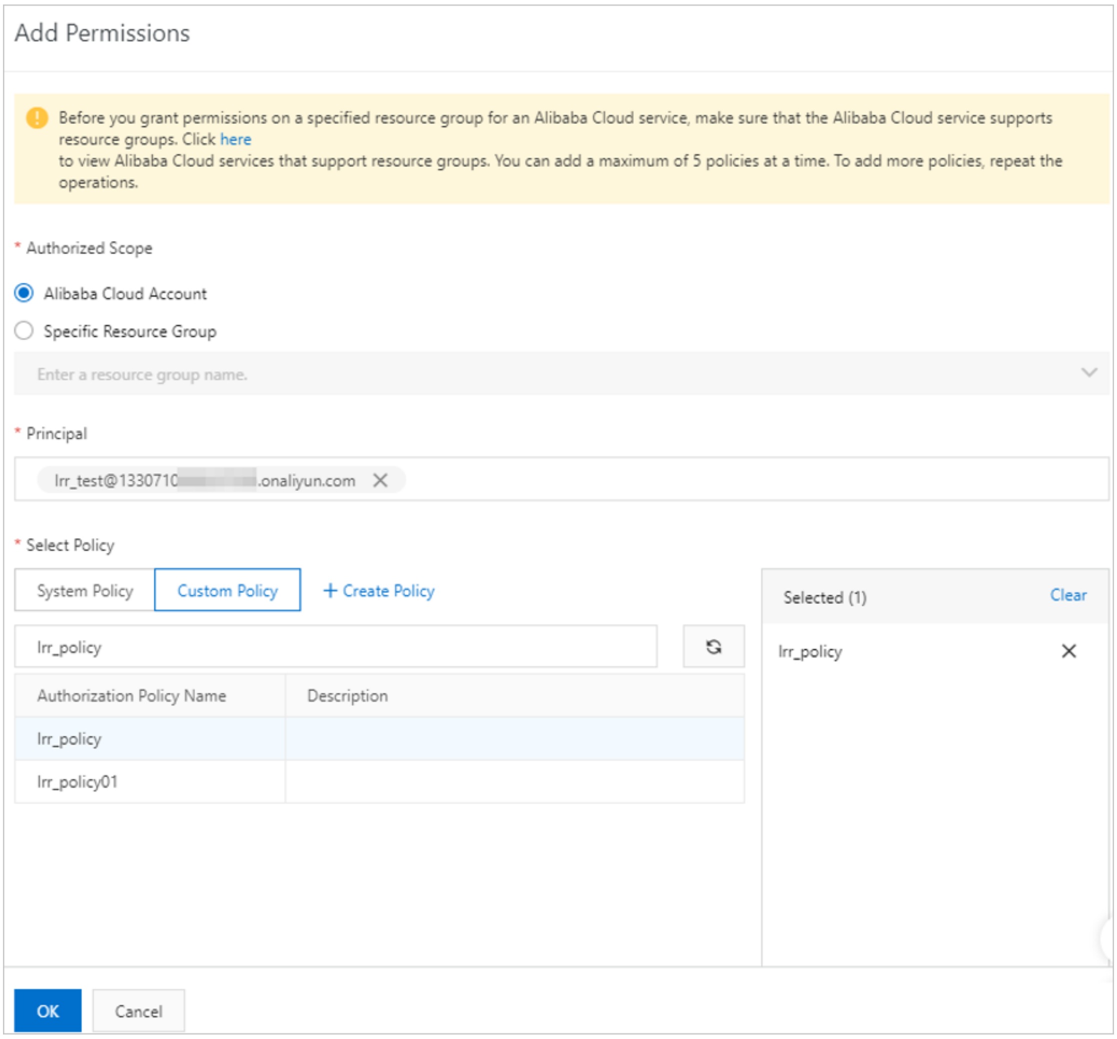
□	User Logon Name/Display Name	Note	Last Login Date	Created	Actions	Actions
□	lrr_test@1330710[redacted].onaliyun.com lrr		-	Jun 30, 2021, 14:47:36	Add to Group	Add to Group Add Permissions Delete
□	cangyan@1330710[redacted].onaliyun.com cangyan		Jun 7, 2021, 11:32:03	May 24, 2021, 16:05:28	Add to Group	Add to Group Add Permissions Delete

4. Attach the newly created custom policy whose effective scope is the entire Alibaba Cloud account to the RAM user.

   i. Find the RAM user on the **Users** page.

   ii. Click **Add Permissions** in the **Actions** column that corresponds to the RAM user.

iii. In the **Add Permissions** panel, click **Custom Policy** in the Select Policy section and click the name of the newly created custom policy in the Authorization Policy Name column.Use a resource group to grant permissions on a specific cluster



Add Permissions

Before you grant permissions on a specified resource group for an Alibaba Cloud service, make sure that the Alibaba Cloud service supports resource groups. Click here
to view Alibaba Cloud services that support resource groups. You can add a maximum of 5 policies at a time. To add more policies, repeat the operations.

* Authorized Scope

● Alibaba Cloud Account

○ Specific Resource Group

Enter a resource group name.

* Principal

lrr_test@1330710[redacted].onaliyun.com ✕

* Select Policy

lrr_policy

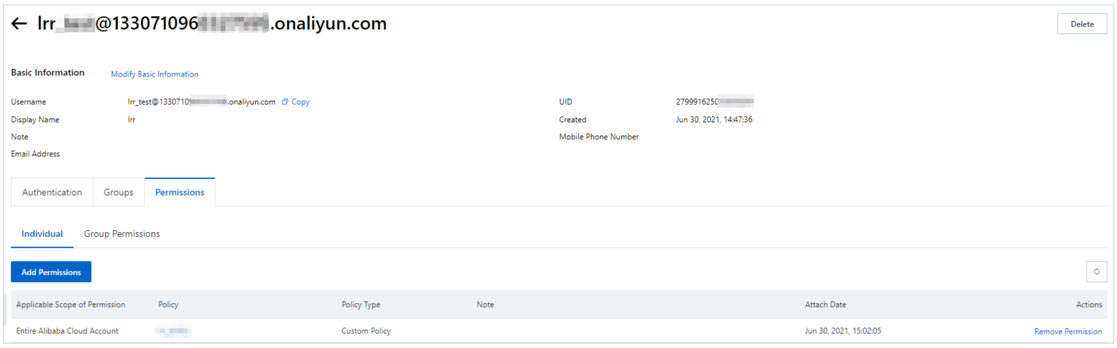
Authorization Policy Name	Description
lrr_policy	
lrr_policy01	

Selected (1) Clear

lrr_policy ✕

iv. Click **OK**.

v. Click **Complete**.



← lrr_[redacted]@133071096[redacted].onaliyun.com

Basic Information Modify Basic Information

Username lrr_test@1330710[redacted].onaliyun.com Copy

Display Name lrr

Note

Email Address

UID 2799916250[redacted]

Created Jun 30, 2021, 14:47:36

Mobile Phone Number

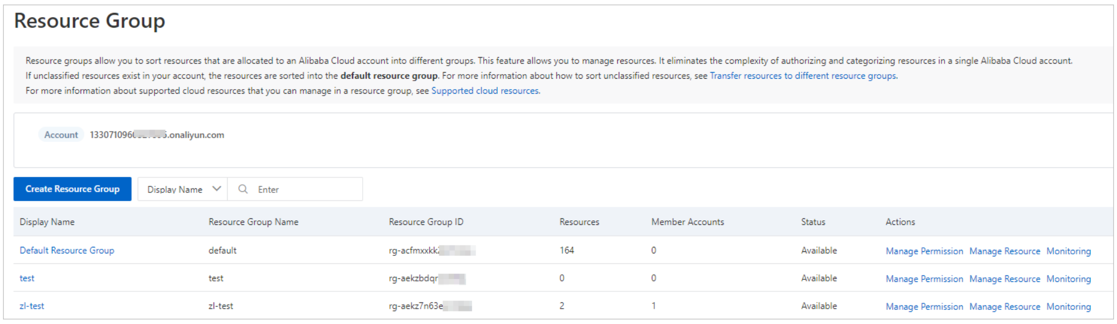
Applicable Scope of Permission	Policy	Policy Type	Note	Attach Date	Actions
Entire Alibaba Cloud Account	[redacted]	Custom Policy		Jun 30, 2021, 15:02:05	Remove Permission

Step 2: Create a resource group and attach a policy to the resource group

1. Log on to the Resource Management console.
2. Create a resource group.

i. In the left-side navigation pane, click **Resource Group**.

ii. On the Resource Group page, click **Create Resource Group**.



Resource Group

Resource groups allow you to sort resources that are allocated to an Alibaba Cloud account into different groups. This feature allows you to manage resources. It eliminates the complexity of authorizing and categorizing resources in a single Alibaba Cloud account.
If unclassified resources exist in your account, the resources are sorted into the **default resource group**. For more information about how to sort unclassified resources, see Transfer resources to different resource groups.
For more information about supported cloud resources that you can manage in a resource group, see Supported cloud resources.

Account 13307109[redacted].onaliyun.com

Display Name	Resource Group Name	Resource Group ID	Resources	Member Accounts	Status	Actions
Default Resource Group	default	rg-acfmxxkk[redacted]	164	0	Available	Manage Permission Manage Resource Monitoring
test	test	rg-aekzbdqr[redacted]	0	0	Available	Manage Permission Manage Resource Monitoring
zl-test	zl-test	rg-aekz7n63e[redacted]	2	1	Available	Manage Permission Manage Resource Monitoring

iii. In the **Create Resource Group** panel, configure the **Resource Group Name** and **Display Name** parameters.

iv. Click **OK**.

3. Move the desired cluster from the default resource group to the newly created resource group.

i. On the Resource Group page, click **Default Resource Group** in the Display Name column.

ii. On the Default Resource Group page, click the **Resources** tab.

iii. Select the desired cluster and click **Transfer Out** in the lower part of the page.

iv. In the **Transfer Out** panel, select the newly created resource group.

v. Click **OK**.

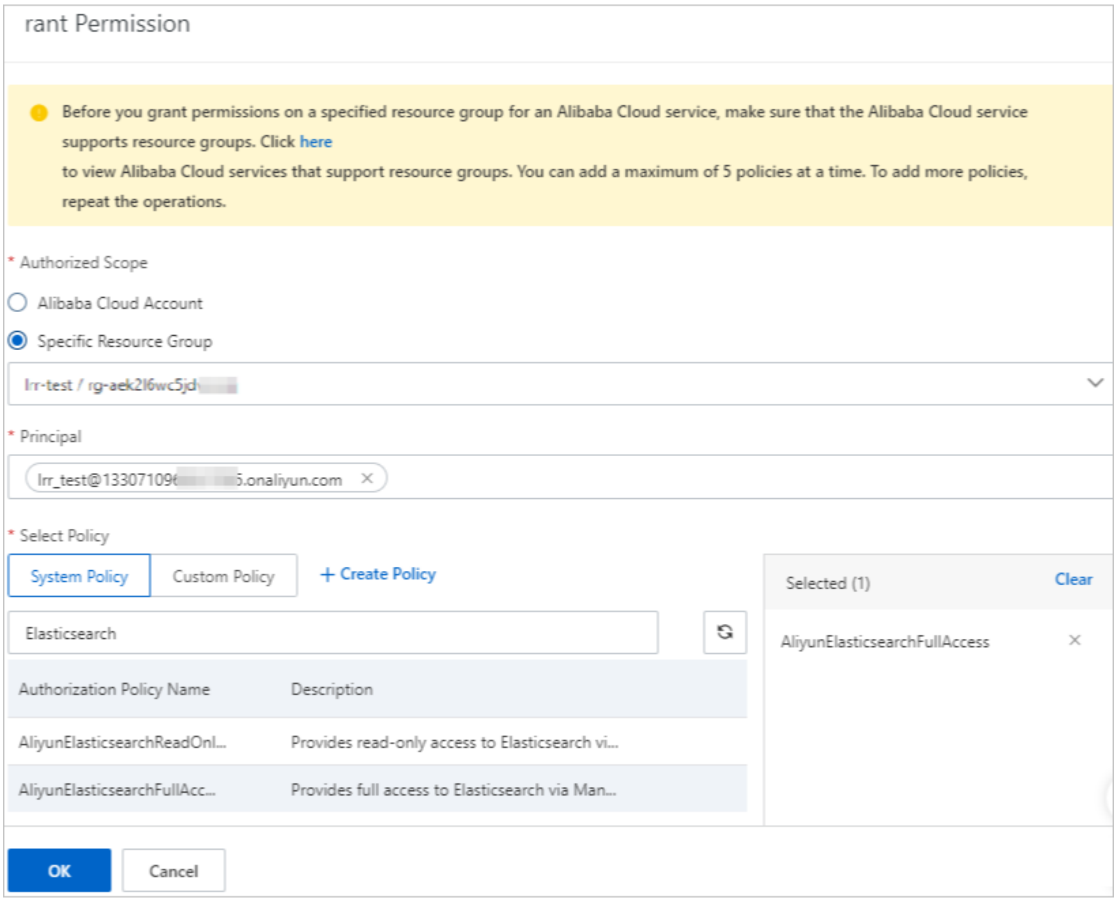
4. Attach a policy to the newly created resource group.

i. In the left-side navigation pane, click **Resource Group**.

ii. Find the newly created resource group and click **Manage Permission** in the **Actions** column.

iii. On the page that appears, click **Grant Permission**.

iv. In the **Grant Permission** panel, configure the parameters.



rant Permission

Before you grant permissions on a specified resource group for an Alibaba Cloud service, make sure that the Alibaba Cloud service supports resource groups. Click here
to view Alibaba Cloud services that support resource groups. You can add a maximum of 5 policies at a time. To add more policies, repeat the operations.

* Authorized Scope

○ Alibaba Cloud Account

● Specific Resource Group

lrr-test / rg-aek2l6wc5jd[redacted]

* Principal

lrr_test@13307109[redacted]5.onaliyun.com ×

* Select Policy

System Policy | Custom Policy | + Create Policy

Elasticsearch

Authorization Policy Name	Description
AliyunElasticsearchReadOnl...	Provides read-only access to Elasticsearch vi...
AliyunElasticsearchFullAcc...	Provides full access to Elasticsearch via Man...

Selected (1) Clear

AliyunElasticsearchFullAccess ×

OK Cancel

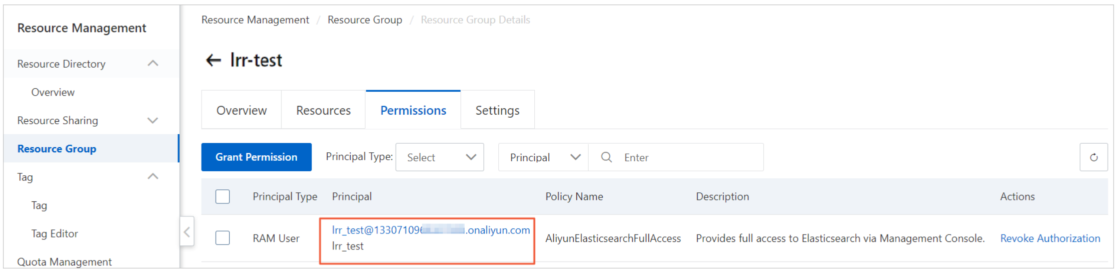
v. Click **OK**.

vi. Click **Complete**.

5. View the authorization information of the RAM user.

i. Click the **Permissions** tab.

ii. Click the name of the RAM user in the **Principal** column.



Resource Management / Resource Group / Resource Group Details

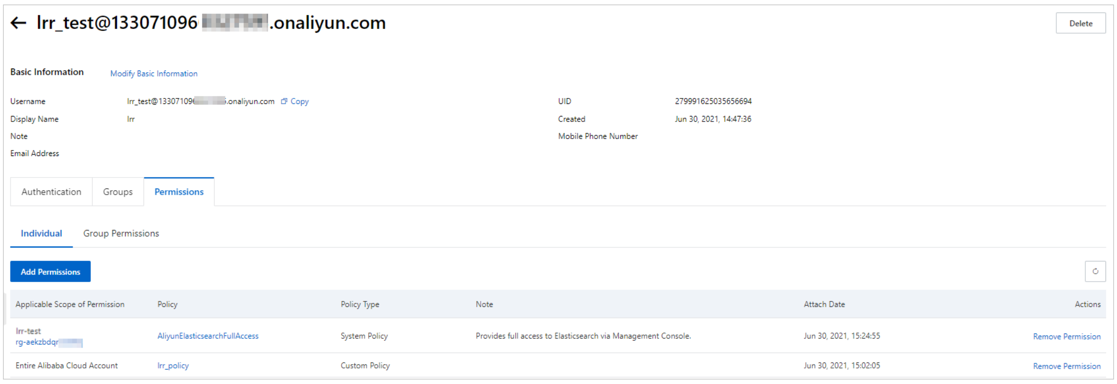
← lrr-test

Overview | Resources | Permissions | Settings

Grant Permission | Principal Type: Select | Principal | Enter

Principal Type	Principal	Policy Name	Description	Actions
RAM User	lrr_test@13307109[redacted].onaliyun.com lrr_test	AliyunElasticsearchFullAccess	Provides full access to Elasticsearch via Management Console.	Revoke Authorization

iii. On the page that appears, click the **Permissions** tab and view the authorization information of the RAM user.



← lrr_test@133071096[redacted].onaliyun.com

Basic Information

Username	lrr_test@133071096[redacted].onaliyun.com	UID	279991625035656694
Display Name	lrr	Created	Jun 30, 2021, 14:47:36
Note		Mobile Phone Number	
Email Address			

Applicable Scope of Permission	Policy	Policy Type	Note	Attach Date	Actions
lrr-test rg-aekzbdqr[redacted]	AliyunElasticsearchFullAccess	System Policy	Provides full access to Elasticsearch via Management Console.	Jun 30, 2021, 15:24:55	Remove Permission
Entire Alibaba Cloud Account	lrr_policy	Custom Policy		Jun 30, 2021, 15:02:05	Remove Permission

Step 3: Log on to the Elasticsearch console by using the RAM user

1. Log on to the Elasticsearch console by using the RAM user.
2. In the top navigation bar, select the region where the desired cluster resides.
3. In the left-side navigation pane, click **Elasticsearch Clusters**.
4. In the top navigation bar, select the newly created resource group and view the information of the cluster.

1.4. Grant permissions to a RAM user

Grant permissions to a RAM user

If you purchase an Alibaba Cloud Elasticsearch cluster and other personnel (such as O&M, development, or data analytics personnel) in your organization want to use RAM users to access the cluster, you can attach policies to the RAM users based on the features that are required by the personnel. This improves system security and availability. You can also create multiple user groups and attach different policies to the user groups. This way, you can manage user permissions by user group.

Background information

RAM is a resource access control service provided by Alibaba Cloud. For more information, see What is RAM?.

Policy description

Policies are categorized into system policies and custom policies.

- System policies

System policy	Description
AliyunElasticsearchReadOnlyAccess	The read-only permissions on Elasticsearch or Logstash clusters. You can attach this policy to users to whom you want to grant only read-only permissions.
AliyunElasticsearchFullAccess	The management permissions on Elasticsearch clusters, Logstash clusters, or Beats shippers. After you attach this policy to a user, the user becomes an administrator.

- Custom policies

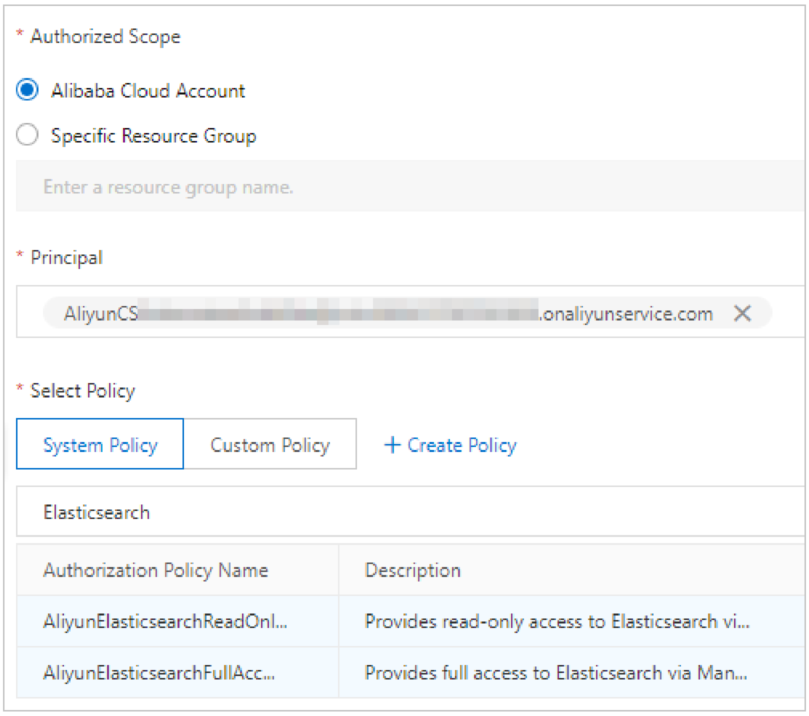
If system policies do not meet your business requirements, you can create custom policies. For more information, see Create a custom policy.

Prerequisites

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

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2.
3.
4. On the **Grant Permission** page, configure the following parameters based on your business requirements.



* Authorized Scope

● Alibaba Cloud Account

○ Specific Resource Group

Enter a resource group name.

* Principal

AliyunCS[redacted].onaliyunservice.com ✕

* Select Policy

System Policy | Custom Policy | + Create Policy

Elasticsearch

Authorization Policy Name	Description
AliyunElasticsearchReadOnl...	Provides read-only access to Elasticsearch vi...
AliyunElasticsearchFullAcc...	Provides full access to Elasticsearch via Man...

Parameter	Description
Authorized Scope	○ **Alibaba Cloud Account**: If you select this option, permissions take effect on the current Alibaba Cloud account. ○ **Specific Resource Group**: If you select this option, permissions take effect on a specific resource group.
Principal	The RAM user to which you want to grant permissions. You can enter the name of a RAM user, RAM user group, or RAM role to which you want to grant permissions. Fuzzy searches are supported.

Parameter	Description
Select Policy	○ **System Policy**: Enter Elasticsearch to search for Elasticsearch system policies and click the name of the policy that you want to attach to the RAM user. For more information about Elasticsearch system policies, see Policy description. ○ **Custom Policy**: If the system policies do not meet your business requirements, select an existing custom policy. Fuzzy searches are supported.

5.

6. Click **Complete**.
   The granted permissions then take effect. You can use the RAM user to log on to the Elasticsearch console and perform authorized operations.

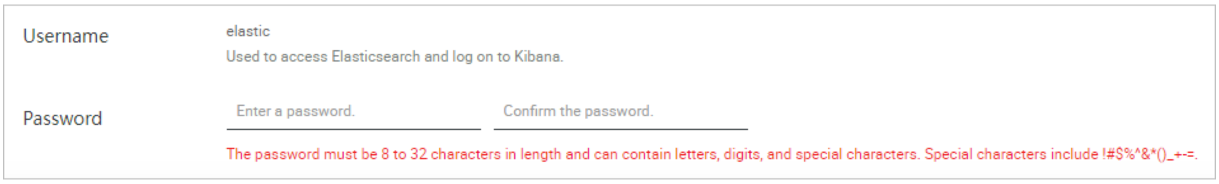
> **Note** If the RAM user no longer requires the permissions, you can revoke the permissions from the RAM user. For more information, see Revoke permissions from a RAM user.

2.Access control methods for Elasticsearch clusters

Alibaba Cloud Elasticsearch clusters are deployed in logically isolated virtual private clouds (VPCs). In addition, access control, authentication and authorization, encryption, and the advanced security features provided by X-Pack are used for the clusters. This ensures the high security of Alibaba Cloud Elasticsearch clusters. This topic describes the access control methods that can be used for Alibaba Cloud Elasticsearch clusters.

Specify a cluster access password or reset the password

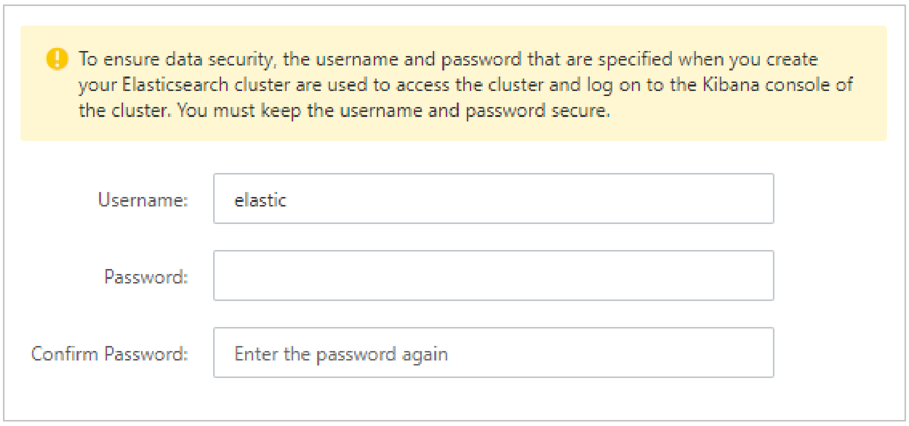
When you create an Elasticsearch cluster, you must specify a password for the default user elastic. The password is used to authenticate your identity when you use a client to access the cluster or when you log on to the Kibana console of the cluster. For more information, see Parameters on the buy page.



Username: elastic
Used to access Elasticsearch and log on to Kibana.

Password: Enter a password. Confirm the password.
The password must be 8 to 32 characters in length and can contain letters, digits, and special characters. Special characters include !#$%^&*()_+-=.

If you want to change the password, you can reset the password. For more information, see Reset the access password for an Elasticsearch cluster.



To ensure data security, the username and password that are specified when you create your Elasticsearch cluster are used to access the cluster and log on to the Kibana console of the cluster. You must keep the username and password secure.

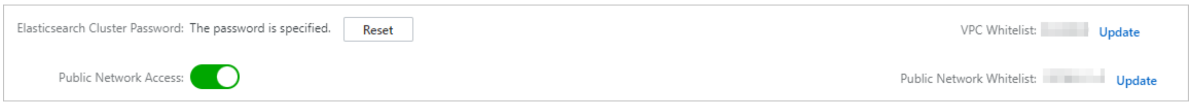
Username: elastic

Password:

Confirm Password: Enter the password again

Configure IP address whitelists for cluster access

- Public IP address whitelist: For security purposes, the Public Network Access feature is disabled for Elasticsearch clusters by default. If you want to access your Elasticsearch cluster over the Internet, you must enable the feature and add the IP address of the host that you use to access the cluster to the public IP address whitelist of the cluster. For more information, see Configure a public or private IP address whitelist for an Elasticsearch cluster.



Elasticsearch Cluster Password: The password is specified. Reset

VPC Whitelist: [redacted] Update

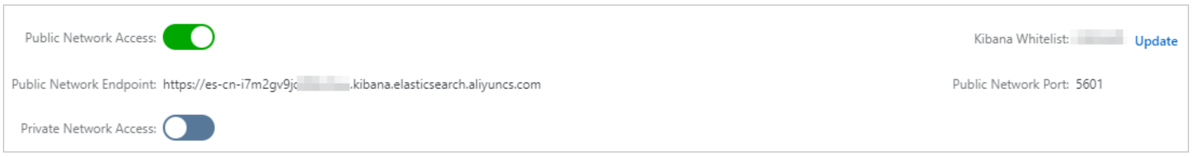
Public Network Access: ●

Public Network Whitelist: [redacted] Update

- Private IP address whitelist: By default, Elasticsearch allows you to access your cluster over an internal network and modify the private IP address whitelist of the cluster. If you want to use a host to access your Elasticsearch cluster over an internal network, you must add the IP address of the host to the private IP address whitelist of the cluster. For more information, see Configure a public or private IP address whitelist for an Elasticsearch cluster.

Configure IP address whitelists for Kibana access

- Public IP access whitelist: The Public Network Access feature is enabled for Kibana by default. However, for security purposes, Elasticsearch adds `127.0.0.1,::1` to the public IP address whitelist of Kibana to deny requests from all IPv4 and IPv6 addresses. The first time you log on to the Kibana console, the system prompts you to configure a public IP address whitelist. You must add the IP address of your host to the public IP address whitelist of Kibana before you log on to the Kibana console by using the host. For more information, see Configure a public or private IP address whitelist for Kibana.



Public Network Access:

Kibana Whitelist: [redacted]

Public Network Endpoint: https://es-cn-i7m2gv9jc[redacted].kibana.elasticsearch.aliyuncs.com

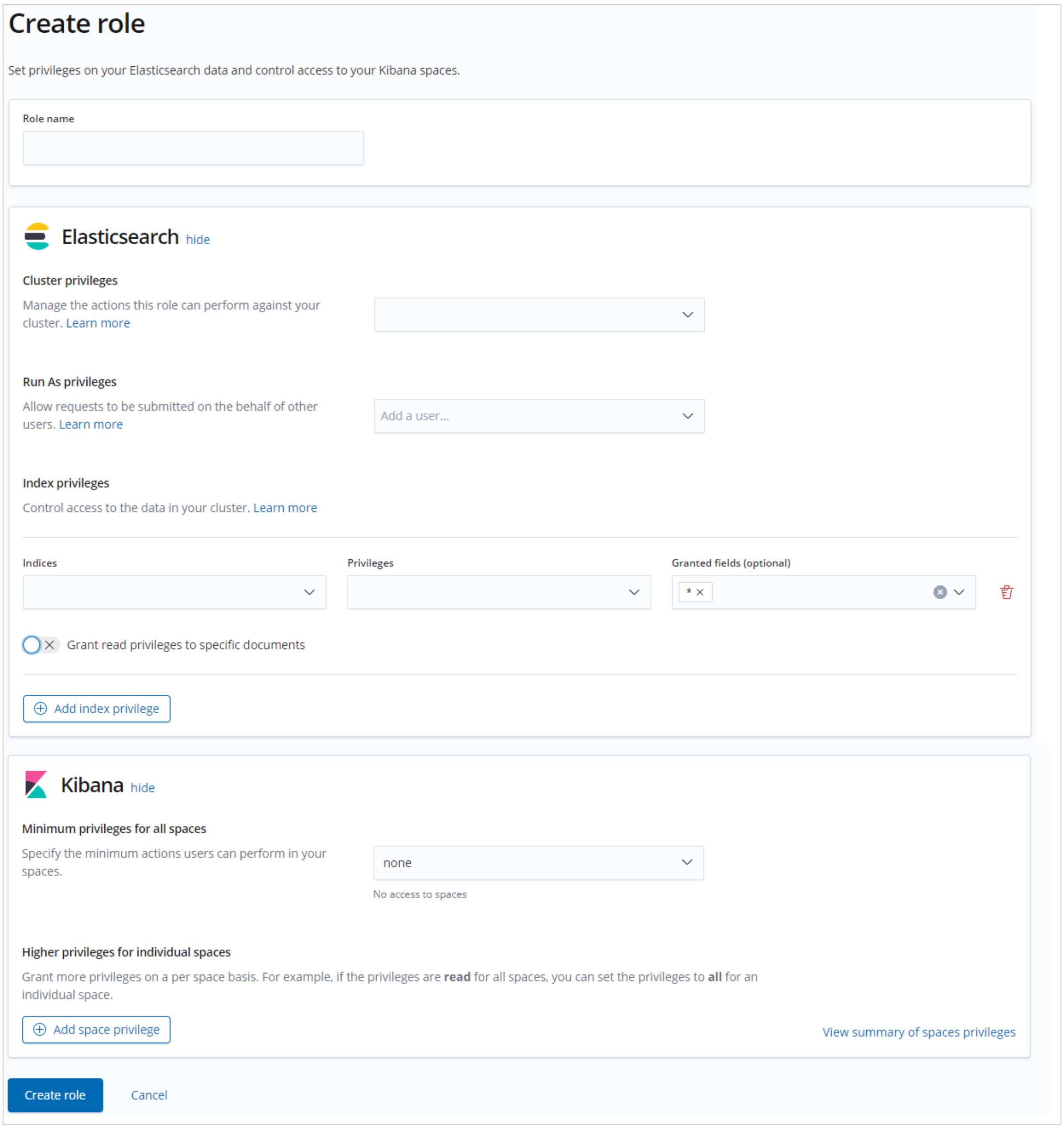
Public Network Port: 5601

Private Network Access:

- Private IP address whitelist: The Private Network Access feature is disabled for Kibana by default. If you want to use a host to log on to the Kibana console over an internal network, you must enable the feature and add the IP address of the host to the private IP address whitelist of Kibana. For more information, see Configure a public or private IP address whitelist for Kibana.

Use the RBAC mechanism provided by the X-Pack plug-in

If you want to grant access permissions on objects such as Elasticsearch clusters, indexes, and fields, you can use the role-based access control (RBAC) mechanism that is provided by the X-Pack plug-in of Elasticsearch. This mechanism allows you to grant permissions to custom roles and assign the roles to users in the Kibana console for access control. For more information, see Use the RBAC mechanism provided by Elasticsearch X-Pack to implement access control.



Create role

Set privileges on your Elasticsearch data and control access to your Kibana spaces.

Role name

Cluster privileges

Manage the actions this role can perform against your cluster. Learn more

Run As privileges

Allow requests to be submitted on the behalf of other users. Learn more

Index privileges

Control access to the data in your cluster. Learn more

Indices	Privileges	Granted fields (optional)
		*

Grant read privileges to specific documents

Minimum privileges for all spaces

Specify the minimum actions users can perform in your spaces.

none

No access to spaces

Higher privileges for individual spaces

Grant more privileges on a per space basis. For example, if the privileges are **read** for all spaces, you can set the privileges to **all** for an individual space.

3.Overview of the Elasticsearch service-linked role

The Elasticsearch service-linked role AliyunServiceRoleForElasticsearchCollector is a RAM role. It is used to create and manage Beats shippers and grant access permissions on other Alibaba Cloud services. This topic describes the use scenarios of the service-linked role and how to delete the role.

Background information

For more information about the service-linked role, see Service-linked roles.

Scenarios

When you create and manage a Beats shipper, you must use the service-linked role AliyunServiceRoleForElasticsearchCollector to authorize the shipper to perform specific operations on an Elastic Compute Service (ECS) instance or Container Service for Kubernetes (ACK) cluster.

Overview of AliyunServiceRoleForElasticsearchCollector

Elasticsearch can create and manage a Beats shipper only after it assumes a role that has the required permissions. If such a role does not exist, Elasticsearch automatically creates the service-linked role AliyunServiceRoleForElasticsearchCollector and grants the required permissions to the role. Elasticsearch assumes the role to call the related API operation and enables the Beats shipper to collect data from an ECS instance or ACK cluster. The following descriptions provide detailed information about the role:

- Role name: AliyunServiceRoleForElasticsearchCollector
- Name of the permission policy for the role: AliyunServiceRolePolicyForElasticsearchCollector
- Policy document:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "oos:CancelExecution",
        "oos:DeleteExecutions",
        "oos:GenerateExecutionPolicy",
        "oos:GetExecutionTemplate",
        "oos:ListExecutionLogs",
        "oos:ListExecutions",
        "oos:ListTaskExecutions",
        "oos:NotifyExecution",
        "oos:StartExecution",
        "oos:ListTagResources",
        "oos:TagResources",
        "oos:UntagResources",
        "oos:CreateTemplate",
        "oos:DeleteTemplate",
        "oos:GetTemplate",
        "oos:ListExecutionRiskyTasks",
        "oos:ListTemplates",
        "oos:UpdateTemplate"
      ],
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:DescribeInstances",
        "ecs:DescribeCloudAssistantStatus"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "cs:GetUserConfig",
        "cs:GetClustersByUid",
        "cs:GetClusterInfo"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "collector.elasticsearch.aliyuncs.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ram:PassRole",
      "Resource": "acs:ram:*:*:role/aliyunoosaccessingecs4esrole",
      "Condition": {
        "StringEquals": {
          "acs:Service": "oos.aliyuncs.com"
        }
      }
    }
  ]
}
```

- Service name: collector.elasticsearch.aliyuncs.com
- Permission required to create or delete the service-linked role: ram:CreateServiceLinkedRole

Delete the service-linked role

Before you delete the AliyunServiceRoleForElasticsearchCollector service-linked role, you must delete all the Beats shippers that depend on the role.

For more information about how to delete a service-linked role, see Delete a service-linked role.

FAQ

Q: Why am I unable to use my RAM user to create the Elasticsearch service-linked role?

A: Only Alibaba Cloud accounts and RAM users that have the CreateServiceLinkedRole permission can be used to create or delete a service-linked role. Therefore, if your RAM user cannot be used to create the service-linked role, you must use your Alibaba Cloud account to attach the following policy to your RAM user.

> Note
>
> - For more information about how to grant permissions to a RAM user, see Grant permissions to a RAM user.
> - You must replace the ID `133071096032****` specified in the Resource element with the ID of your Alibaba Cloud account. To obtain the ID of your Alibaba Cloud account, perform the following operations: Log on to the Alibaba Cloud Management Console and move the pointer over the profile picture in the upper-right corner. Then, you can view the **ID** of your Alibaba Cloud account.

If you want to use a RAM user to create and manage a Beats shipper that depends on the AliyunServiceRoleForElasticsearchCollector service-linked role, you can attach the following policy to the RAM user:

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": "elasticsearch:InitializeOperationRole",
            "Resource": "acs:ram:*:133071096032****:role/*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:CreateServiceLinkedRole",
            "Resource": "acs:ram:*:133071096032****:role/*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "collector.elasticsearch.aliyuncs.com"
                    ]
                }
            }
        }
    ]
}
```

4.FAQ about access control

FAQ about Elasticsearch access control

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

- When I use a RAM user to purchase an Elasticsearch cluster, no VPCs are available on the buy page. Why?
- If a temporary user is deleted, will Elasticsearch clusters or data that is created by the user be deleted?
- When I use Elasticsearch, the error message "The specified RAM user is not authorized. Check the permission of the RAM user and try again." is displayed. What do I do?
- How do I create a user that has read-only permissions on resources, such as indexes, of an Elasticsearch cluster?
- 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 I use a RAM user to purchase an Elasticsearch cluster, no VPCs are available on the buy page. Why?

Check whether the Resource Access Management (RAM) user has the permissions to obtain the list of virtual private clouds (VPCs). For more information, see View the basic information about 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 error message "The specified RAM user is not authorized. Check the permission of the RAM user and try again." is displayed. What do I do?

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

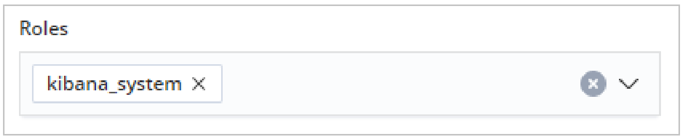
- `AliyunElasticsearchReadOnlyAccess` : the read-only permissions on Elasticsearch or Logstash clusters. This policy can be attached to read-only users.
- `AliyunElasticsearchFullAccess` : the management permissions on Elasticsearch or Logstash clusters. This policy can be attached to administrators.

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 Use the RBAC mechanism provided by Elasticsearch X-Pack to implement access control.

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. For more information, see Use the RBAC mechanism provided by Elasticsearch X-Pack to implement access control.



Roles

kibana_system