ALIBABA CLOUD

阿里云

阿里云Elasticsearch

ES访问控制

文档版本：20201223

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.授权资源类型

es授权资源类型

本文提供了阿里云Elasticsearch支持的授权资源类型，帮助您为不同的用户配置不同的权限。

资源类型及描述

阿里云Elasticsearch支持资源类型及完整资源描述如下。

资源类型	完整资源描述
instances	acs:elasticsearch:$regionId:$accountId:instances/*
instances	acs:elasticsearch:$regionId:$accountId:instances/$instanceId
vpc	acs:elasticsearch:$regionId:$accountId:vpc/*
vswitch	acs:elasticsearch:$regionId:$accountId:vswitch/*
tags	acs:elasticsearch:$regionId:$accountId:tags/*

- $regionId：阿里云Elasticsearch实例的区域ID，可使用 * 代替。
- $accountId：您阿里云账号的主账号ID，可使用 * 代替。
- $instanceId：阿里云Elasticsearch的实例ID，可使用 * 代替。

配置阿里云Elasticsearch资源的方式，请参见创建自定义权限策略。

实例授权列表

> **说明** 以下资源描述为简写形式，已省略相同部分内容，完整资源描述请参见资源类型及描述。

- 实例基本操作

Action	Action描述	资源描述
elasticsearch:CreateInstance	创建实例	instances/*
elasticsearch:ListInstance	查看实例列表	instances/*
elasticsearch:DescribeInstance	查看实例描述	instances/* 或 instances/$instanceId
elasticsearch:DeleteInstance	删除实例	instances/* 或 instances/$instanceId

Action	Action描述	资源描述
elasticsearch:RestartInstance	重启实例	instances/* 或 instances/$instanceId
elasticsearch:UpdateInstance	更新实例	instances/* 或 instances/$instanceId
elasticsearch:UpdateInstanceSettings	更新实例的YML文件配置	instances/$instanceId
elasticsearch:UpdateDescription	更新实例名称	instances/$instanceId
elasticsearch:UpdateAdminPwd	更新实例访问账号的密码	instances/$instanceId
elasticsearch:ListSearchLogs	查询实例日志	instances/$instanceId
elasticsearch:DowngradeInstance	缩容集群数据节点	instances/$instanceId
elasticsearch:CancelTask	取消数据迁移任务	instances/$instanceId
elasticsearch:UpdateKibanaSettings	修改集群Kibana节点的配置	instances/$instanceId
elasticsearch:DescribeKibanaSettings	查看集群Kibana节点的配置	instances/$instanceId
elasticsearch:DescribeElasticsearchHealth	查看集群健康状态	instances/$instanceId
elasticsearch:DeactivateZones	对多可用区实例中的某个可用区进行切流	instances/$instanceId
elasticsearch:ActivateZones	恢复切流过的可用区	instances/$instanceId
elasticsearch:MigrateToOtherZone	迁移可用区节点	instances/$instanceId
elasticsearch:ResumeElasticsearchTask	恢复实例的变更状态	instances/$instanceId
elasticsearch:InterruptElasticsearchTask	中断实例的变更状态	instances/$instanceId
elasticsearch:UpdateAdvancedSetting	更新集群的垃圾回收器配置	instances/$instanceId
elasticsearch:ListPipelineIds	允许实例获取Logstash管道	instances/$instanceId

Action	Action描述	资源描述
elasticsearch:UpdateInstanceChargeType	更改实例的付费模式	instances/$instanceId
elasticsearch:RenewInstance	为包年包月实例续费	instances/$instanceId
elasticsearch:UpdateReadWritePolicy	开启或者关闭集群写入高可用	instances/$instanceId
elasticsearch:UpgradeInstanceEngineVersion	升级集群版本	instances/$instanceId
elasticsearch:ModifyInstanceMaintainTime	更新实例的可维护时间段	instances/$instanceId
elasticsearch:DescribeTemplates	获取当前集群的场景模板配置	instances/$instanceId
elasticsearch:UpdateTemplate	更新当前集群的场景模板配置	instances/$instanceId
elasticsearch:UpdateExtendConfig	修改集群扩展配置	instances/$instanceId
elasticsearch:ModifyElastictask	修改集群弹性扩缩容规则配置	instances/$instanceId
elasticsearch:GetElastictask	获取集群弹性扩缩容规则配置	instances/$instanceId

- 插件相关

Action	Action描述	资源描述
elasticsearch:ListPlugin	获取插件列表	instances/$instanceId
elasticsearch:InstallSystemPlugin	安装系统插件	instances/$instanceId
elasticsearch:UninstallPlugin	卸载插件	instances/$instanceId

- 网络相关

Action	Action描述	资源描述
elasticsearch:UpdatePublicNetwork	开启或关闭实例的公网地址	instances/$instanceId
elasticsearch:UpdatePublicIps	修改实例的公网访问白名单	instances/$instanceId
elasticsearch:UpdateWhiteIps	修改实例的VPC私网访问白名单	instances/$instanceId
elasticsearch:UpdateKibanaIps	修改Kibana白名单	instances/$instanceId

Action	Action描述	资源描述
elasticsearch:OpenHttps	开启HTTPS协议	instances/$instanceId
elasticsearch:CloseHttps	关闭HTTPS协议	instances/$instanceId
elasticsearch:DescribeConnectableClusters	查看同一专有网络下，能实现网络互通的实例列表	instances/$instanceId
elasticsearch:ListConnectedClusters	查看已配置的网络互通实例	instances/$instanceId
elasticsearch:AddConnectableCluster	配置实例网络互通	instances/$instanceId
elasticsearch:DeleteConnectedCluster	删除已配置的网络互通实例	instances/$instanceId
elasticsearch:ModifyWhiteIps	更新实例（包含Kibana）的访问白名单	instances/$instanceId
elasticsearch:TriggerNetwork	开启或关闭Elasticsearch、Kibana的公网或私网访问	instances/$instanceId

> **注意** 当Action中包含其他更新白名单相关参数时（例如UpdatePublicIps、UpdateWhiteIps、UpdateKibanaIps），都需要添加ModifyWhiteIps参数。

- 词典

Action	Action描述	资源描述
elasticsearch:UpdateDict	修改词典（IK、同义词）	instances/$instanceId

Tags授权列表

Action	Action描述	资源描述
elasticsearch:ListTags	允许子用户查询标签	tags/$instanceId
elasticsearch:CreateTags	允许子用户创建或更新标签	tags/$instanceId
elasticsearch:RemoveTags	允许子用户删除标签	tags/$instanceId

自定义标签权限策略，请参见实例标签权限策略示例。

底层云监控授权列表

> **说明** 以下资源描述为简写的 * 通配符形式。

Action	Action描述	资源描述
cms:ListProductOfActiveAlert	获取用户已开通云监控服务的产品	*
cms:ListAlarm	查询指定或全部报警规则设置	*
cms:QueryMetricList	查询一段时间内指定产品实例的监控数据	*

购买页VPC和VSwitch授权列表

> **说明** 以下资源描述为简写形式，已省略相同部分内容，完整资源描述请参见资源类型及描述。

Action	Action描述	资源描述
DescribeVpcs	获取VPC列表	vpc/*
DescribeVswitches	获取VSwitch列表	vswitch/*

智能运维授权列表

> **说明** 以下资源描述为简写形式，已省略相同部分内容，完整资源描述请参见资源类型及描述。

Action	Action 描述	资源描述
elasticsearch:OpenDiagnosis	开启智能诊断	instances/* 或 instances/$instanceId
elasticsearch:CloseDiagnosis	关闭智能诊断	instances/* 或 instances/$instanceId
elasticsearch:UpdateDiagnosisSettings	更新诊断配置	instances/* 或 instances/$instanceId
elasticsearch:DescribeDiagnosisSettings	获取诊断配置	instances/* 或 instances/$instanceId
elasticsearch:ListInstanceIndices	获取实例索引	instances/* 或 instances/$instanceId

Action	Action 描述	资源描述
elasticsearch:DiagnoseInstance	开始智能诊断	instances/* 或 instances/$instanceId
elasticsearch:ListDiagnoseReportIds	获取诊断报告标号列表	instances/* 或 instances/$instanceId
elasticsearch:DescribeDiagnoseReport	获取诊断报告详情	instances/* 或 instances/$instanceId
elasticsearch:ListDiagnoseReport	获取诊断报告详情列表	instances/* 或 instances/$instanceId

支持区域

地域	区域	区域ID
中国	华东 2（上海）	cn-shanghai
	华南 1（深圳）	cn-shenzhen
	华北1（青岛）	cn-qingdao
	华北3（张家口）	cn-zhangjiakou
	华北2（北京）	cn-beijing
	华东 1（杭州）	cn-hangzhou
	中国（香港）	cn-hongkong
亚太	新加坡	ap-southeast-1
	马来西亚（吉隆坡）	ap-southeast-3
	日本（东京）	ap-northeast-1
	澳大利亚（悉尼）	ap-southeast-2
	印度尼西亚（雅加达）	ap-southeast-5
欧洲与美洲	美国（弗吉尼亚）	us-east-1
	美国（硅谷）	us-west-1
	德国（法兰克福）	eu-central-1
	英国（伦敦）	eu-west-1

地域	区域	区域ID
中东与印度	印度（孟买）	ap-south-1

2.创建自定义权限策略

es自定义权限

如果阿里云Elasticsearch的系统策略无法满足您的需求，可以通过创建自定义策略实现精细化权限管理。本文介绍如何创建自定义权限策略，并提供实例和标签权限策略配置示例供您参考。

前提条件

了解权限策略语言的基本结构和语法。详细信息，请参见权限策略语法和结构。

背景信息

阿里云Elasticsearch支持以下两种系统策略：

- AliyunElasticsearchReadOnlyAccess：只读访问阿里云Elasticsearch或Logstash的权限，可用于只读用户。
- AliyunElasticsearchFullAccess：管理阿里云Elasticsearch或Logstash的权限，可用于管理员。

> **说明**
> - 以上两种权限仅为RAM用户授予阿里云Elasticsearch或Logstash的权限，不包括云监控和Tags权限，使用时需自定义对应权限。您也可参见管理员权限配置。
> - 授权范围仅支持云账号全部资源，不支持指定资源组。
> - 本文中的云账号是指阿里云主账号。

操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏的**权限管理**菜单下，单击**权限策略管理**。
3. 单击**创建权限策略**。
4. 填写**策略名称**和**备注**。
5. **配置模式**选择**脚本配置**。
6. 在**策略内容**区域，选择并导入已有系统策略后适当修改。

> **说明** 在搜索框输入关键字可以进行模糊搜索。

根据需求输入具体的权限脚本，例如：

- 访问主账号的专有网络VPC（Virtual Private Cloud）权限。

```
"elasticsearch:DescribeVpcs","elasticsearch:DescribeVswitches"
```

> 说明 策略内容可参见系统模板AliyunVPCReadOnlyAccess。

- RAM用户订单权限。

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

> 说明 策略内容可参见系统模板AliyunBSSOrderAccess。

- API对应权限。

Method	URI	Resource	Action
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

具体示例，请参见权限策略示例。

7. 单击**确定**。

权限策略示例

- 管理员权限策略

以下示例设置为账号ID为*<UID>*的主账号下的某个RAM用户授权，使该用户拥有所有Elasticsearch实例的所有操作权限。

```
{
  "Statement": [
    {
      "Action": [
        "elasticsearch:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
```

```
{
  "Action": [
    "elasticsearch:ListInstance",
    "elasticsearch:ListSnapshotReposByInstanceId"
  ],
  "Effect": "Allow",
  "Resource": "acs:elasticsearch:cn-hangzhou:<UID>:instances/*"
},
{
  "Action": [
    "elasticsearch:ListCollectors"
  ],
  "Effect": "Allow",
  "Resource": [
    "acs:elasticsearch:*:*:collectors/*"
  ]
},
{
  "Action": [
    "cms:ListProductOfActiveAlert",
    "cms:ListAlarm",
    "cms:QueryMetricList"
  ],
  "Effect": "Allow",
  "Resource": "*"
},
{
  "Action": [
    "elasticsearch:ListTags"
  ],
  "Effect": "Allow",
  "Resource": "acs:elasticsearch:*:*:tags/*"
},
{
  "Action": [
    "elasticsearch:ListLogstash"
  ],
  "Effect": "Allow",
  "Resource": "acs:elasticsearch:*:<UID>:logstashes/*"
},
{
```

```
    {
      "Effect": "Allow",
      "Action": [
        "elasticsearch:DescribeVpcs",
        "elasticsearch:DescribeVswitches"
      ],
      "Resource": [
        "acs:elasticsearch:*:<UID>:vswitch/*",
        "acs:elasticsearch:*:<UID>:vpc/*"
      ]
    },
    {
      "Action": "bss:PayOrder",
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

- 操作特定实例权限策略

  以下示例设置为账号ID为*<UID>*的主账号下的某个RAM用户授权，使该用户拥有以下权限：

  - 底层云监控权限
  - 指定实例，除安全配置（删除实例、配置公网和私网访问白名单等）外的所有Elasticsearch相关操作的权限
  - 查看实例列表的权限
  - 查看所有实例标签的权限
  - 查看采集器列表的权限

```
{
  "Statement": [
    {
      "Action": [
        "elasticsearch:*"
      ],
      "Effect": "Allow",
      "Resource": "acs:elasticsearch:*:<UID>:instances/<instanceId>"
    },
    {
      "Action": [
        "cms:ListProductOfActiveAlert",
        "cms:ListAlarm",
```

```
      "cms:QueryMetricList"
    ],
    "Effect": "Allow",
    "Resource": "*"
  },
  {
    "Action": [
      "elasticsearch:DeleteInstance",
      "elasticsearch:UpdatePublicNetwork",
      "elasticsearch:UpdateWhiteIps",
      "elasticsearch:ModifyWhiteIps",
      "elasticsearch:TriggerNetwork"
    ],
    "Effect": "Deny",
    "Resource": "acs:elasticsearch:*:<UID>:instances/*"
  },
  {
    "Action": [
      "elasticsearch:ListTags"
    ],
    "Effect": "Allow",
    "Resource": "acs:elasticsearch:*:<UID>:tags/*"
  },
  {
    "Action": [
      "elasticsearch:ListInstance",
      "elasticsearch:ListSnapshotReposByInstanceId"
    ],
    "Effect": "Allow",
    "Resource": "acs:elasticsearch:*:<UID>:instances/*"
  },
  {
    "Action": [
      "elasticsearch:ListCollectors"
    ],
    "Effect": "Allow",
    "Resource": "acs:elasticsearch:*:<UID>:collectors/*"
  },
  {
    "Action": [
      "elasticsearch:ListLogstash"
```

```
        ],
        "Effect": "Allow",
        "Resource": "acs:elasticsearch:*:<UID>:logstashes/*"
      },
      {
        "Action": [
          "elasticsearch:GetEmonProjectList"
        ],
        "Effect": "Allow",
        "Resource": "acs:elasticsearch:*:*:emonProjects/*"
      },
      {
        "Action": [
          "elasticsearch:getEmonUserConfig"
        ],
        "Effect": "Allow",
        "Resource": "acs:elasticsearch:*:*:emonUserConfig/*"
      }
    ],
    "Version": "1"
}
```

Action说明

Action	说明
["cms:ListProductOfActiveAlert", "cms:ListAlarm", "cms:QueryMetricList"]	云监控权限，具体说明如下： • cms:ListProductOfActiveAlert：获取主账号已开通云监控服务的产品。 • cms:ListAlarm：查询指定或全部报警规则设置。 • cms:QueryMetricList：查询一段时间内指定产品实例的监控数据。
["bss:PayOrder"]	支付订单的权限。授权后，RAM用户可在购买实例时，支付订单。

Action	说明
["elasticsearch:DescribeVpcs", "elasticsearch:DescribeVswitches"]	访问主账号的专有网络和虚拟交换机列表权限。授权后，在购买实例时，RAM用户可选择主账号创建的的专有网络和虚拟交换机。 注意 设置RAM用户购买实例的权限时，需要同时配置 ["bss:PayOrder"] Action，否则购买时，会出现无权限的错误。
["elasticsearch:*"]	操作Elasticsearch实例的所有权限。授权后，RAM用户可对所有或指定实例执行任意操作。 注意 elasticsearch:* 不包括高级监控告警、云监控、Tags权限，这些权限需要单独设置。如果没有设置，进入包含这些功能的页面后，会出现无权限的错误。但确认后，可以在该页面中使用其他已授权的功能。
["elasticsearch:ListTags"]	查看Elasticsearch实例标签的权限。授权后，RAM用户可查看Elasticsearch实例的标签。
["elasticsearch:ListInstance", "elasticsearch:ListSnapshotReposByInstanceId"]	• elasticsearch:ListInstance：查看Elasticsearch实例列表的权限。 • elasticsearch:ListSnapshotReposByInstanceId：查看跨集群OSS仓库设置列表权限。
["elasticsearch:ListCollectors"]	查看Beats采集器列表的权限。授权后，RAM用户可查看控制台中包含的所有Beats采集器。

Action	说明
["elasticsearch:ListLogstash"]	查看Logstash实例列表的权限。授权后，RAM用户可在实例列表页面中，查看对应区域下包含的所有Logstash实例。
["elasticsearch:DeleteInstance", "elasticsearch:UpdatePublicNetwork", "elasticsearch:TriggerNetwork"]	• elasticsearch:DeleteInstance：删除实例的权限。 • elasticsearch:UpdatePublicNetwork：修改实例公网访问白名单的权限。 • elasticsearch:TriggerNetwork：开启或关闭Elasticsearch、Kibana的公网或私网访问。 说明 此部分的Effect设置为Deny，表示不允许RAM用户执行以上操作。
["elasticsearch:GetEmonProjectList"]	获取集群监控项目列表的权限。 注意 此Action需要与["elasticsearch:getEmonUserConfig"] Action一起使用，否则在进入集群监控页面时，会提示无权限。
["elasticsearch:getEmonUserConfig"]	获取集群监控用户配置的权限。

Effect说明

Effect	说明
Allow	允许RAM用户执行Action中设置的操作。
Deny	拒绝RAM用户执行Action中设置的操作。

说明

- *<UID>*：替换为您主账号的ID。将鼠标移至控制台右上角的用户头像上，单击**安全设置**，**安全设置**页面中的**账号ID**即为*<UID>*。
- *<instanceId>*：替换待授权的目标实例ID。获取方式，请参见查看实例的基本信息。
- Resource中，`*`表示所有实例资源，*<instanceId>*表示指定实例资源。详细说明，请参见授权资源类型。

后续步骤

自定义策略创建完成后，使用主账号在RAM控制台中或通过RAM SDK对子账号授权。具体操作，请参见为RAM用户授权。

3.实例标签权限策略示例

es tags权限策略

创建自定义权限策略时，如果您需要为某个子账号授予操作阿里云Elasticsearch（简称ES）实例标签的权限，可参考本文示例进行配置。

es tags权限策略 es tags操作权限

> **注意** 配置入口请参见创建自定义权限策略。配置完成后，需要使用主账号在RAM控制台中对子账号授权，或通过RAM SDK对子账号授权才能生效，详情请参见为RAM用户授权。

授权子账号为指定实例创建或更新标签

以下示例为账号ID为1234的主账号下的某个子账号授予权限。使该子账号拥有为华东1（杭州）区域下，名称为 `es-instance1` 和 `es-instance2` 的实例创建标签的权限。

```
{
 "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"
}
```

授权子账号删除指定实例的标签

以下示例为账号ID为1234的主账号下的某个子账号授予权限。使该子账号拥有为华东1（杭州）区域下，名称为 `es-instance1` 和 `es-instance2` 的实例删除标签的权限。

```
{
 "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"
}
```

授权子账号查询指定实例的标签

以下示例为账号ID为1234的主账号下的某个子账号授予权限。使该子账号拥有查询华东1（杭州）区域下，名称为 `es-instance1` 和 `es-instance2` 的实例的标签的权限。

```
{
 "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"
}
```

授权子账号查询所有实例的标签

以下示例为账号ID为1234的主账号下的某个子账号授予权限。使该子账号拥有查询华东1（杭州）区域下所有实例的标签的权限。

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

授权子账号操作指定标签的实例

以下示例为账号ID为1234的主账号下的某个子账号授予权限。使该子账号拥有操作标签为 `name:liumi` 、 `env:test` 和 `env:pre` 的实例的权限，没有操作其他实例的权限。

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

4.为RAM用户授权

es 子账号授权

通过RAM用户授权，您可以为RAM用户授予操作阿里云Elasticsearch（简称ES）的权限，例如创建实例、查看实例列表等。权限策略支持系统策略和自定义策略两种类型。

es 子账号授权 es RAM用户授权

前提条件

您已完成以下操作：

- 创建RAM用户，详情请参见创建RAM用户。
- 创建自定义权限策略。

  如果系统策略无法满足您的需求，请自定义符合要求的权限策略，详情请参见创建自定义权限策略。

> **说明** 阿里云ES支持以下两种系统策略：
>
> - `AliyunElasticsearchReadOnlyAccess`：只读访问阿里云ES或Logstash的权限，可用于只读用户。
> - `AliyunElasticsearchFullAccess`：管理阿里云ES或Logstash的权限，可用于管理员。

背景信息

本文介绍在RAM控制台的授权页面下为RAM用户授权的方法，您也可以在用户页面下为RAM用户授权，详情请参见为RAM用户授权。

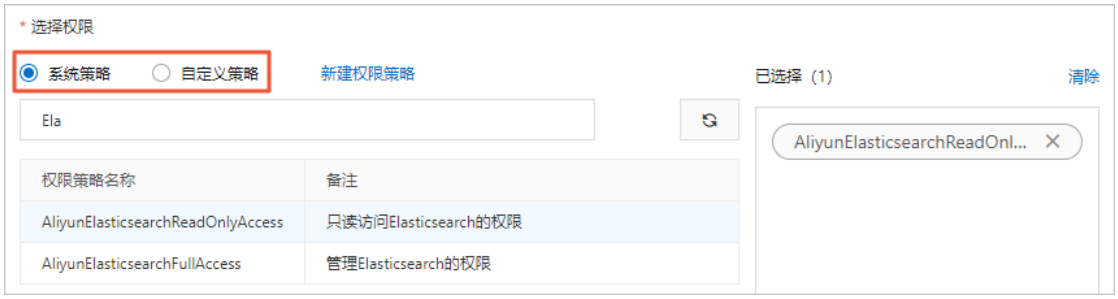
> **说明** 本文中的云账号是指阿里云主账号。

操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏的**权限管理**菜单下，单击**授权**。
3. 单击**新增授权**。
4. 在**被授权主体**区域下，输入目标授权主体名称后，单击需要授权的主体。

   > **说明** 输入RAM用户、用户组或RAM角色名称可以进行模糊搜索。

5. 在**选择权限**区域，为目标授权主体进行授权。
   i. 选择**系统策略**或**自定义策略**。



ii. 找到目标权限策略。

> **说明** 可在搜索框中输入权限策略名称进行查找，支持模糊匹配。

iii. 在左侧**权限策略名称**列表下，单击需要授予目标主体的权限策略。

6. 单击**确定**。
7. 单击**完成**。

> **说明** 如果RAM用户不再需要已授权的权限，可移除对应权限，详情请参见为RAM用户移除权限。

5.Kibana角色管理

5.1. 创建角色

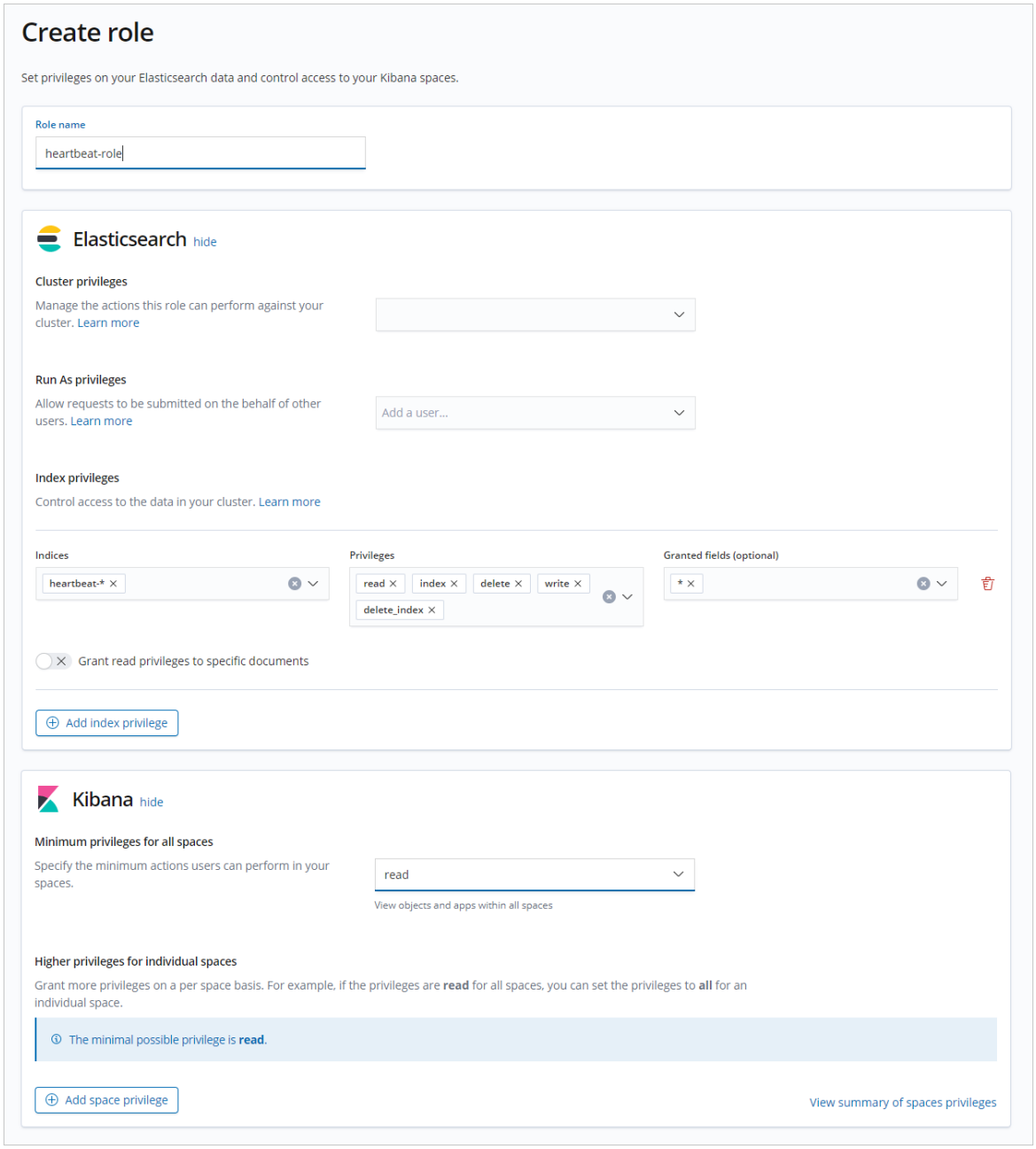
当您需要对自定义用户授予操作集群中某个索引的权限时，可在Kibana控制台中创建角色，并将该角色分配给对应用户。本文介绍在Kibana控制台中创建角色的方法。

前提条件

已创建阿里云Elasticsearch实例，详情请参见创建阿里云Elasticsearch实例。

操作步骤

1. 登录Kibana控制台。 登录控制台的具体步骤请参见登录Kibana控制台。
2. 在左侧导航栏，单击**Management**。
3. 在**Security**区域，单击**Roles**。
4. 单击**Create role**，然后输入相关参数配置。



参数	说明
Role name	角色名称，可自定义。
Cluster privileges	可选。选择此角色可以对集群执行的操作，详情请参见Security privileges。
Run As privileges	可选。选择用户，如果还没有创建用户，可不选，在创建用户时再分配该角色，详情请参见创建用户。

参数	说明
Index privileges	○ Indices：选择对应的索引模式。例如heartbeat-*。 说明 如果没有索引模式，请先在Management页面，单击Kibana中的Index Pattern，按照页面提示创建一个索引模式。 ○ Privileges：为角色分配索引权限。 ○ Granted fields (optional)：授权的字段，可选。
Minimum privileges for all spaces	选择所有空间的最低权限。建议设置为read，如果设置为none，通过对应用户进入Kibana控制台时会报错。 说明 您也可以通过设置单空间的权限，为指定空间授予特定权限。

5. 单击Create role。

5.2. 创建用户

角色创建完成后，您可以创建一个用户，并为该用户分配对应角色，使其具有操作集群中某个索引的权限。本文介绍通过Kibana控制台创建用户的方法。

前提条件

您已完成以下操作：

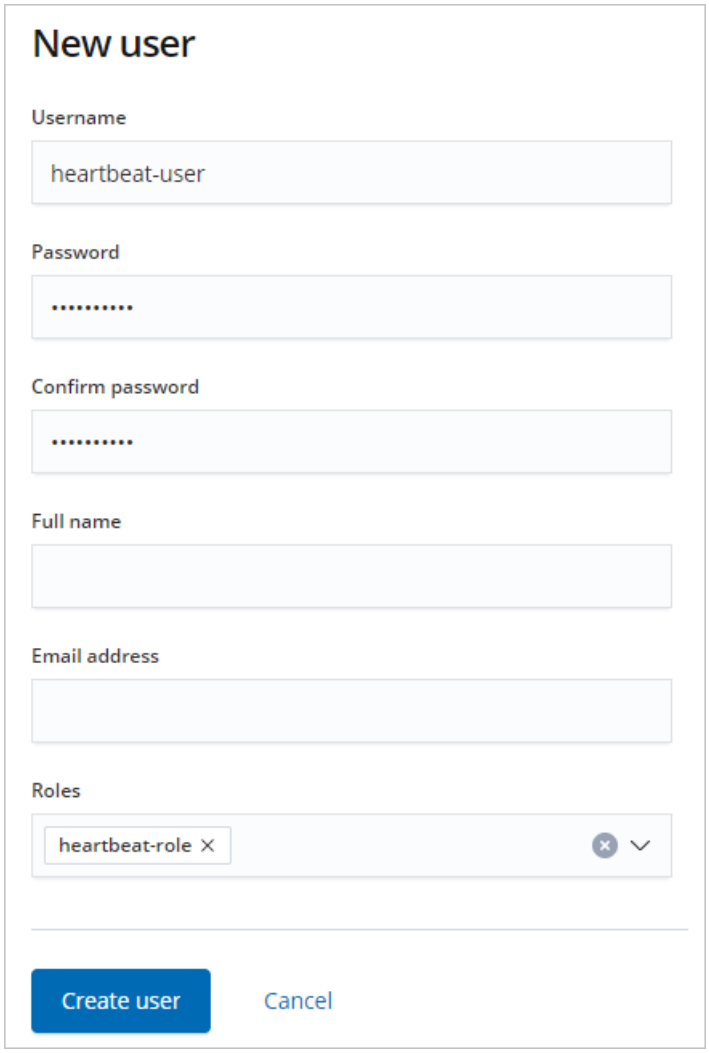
- 创建角色。

  该角色需要具有对应索引的操作权限，用来分配给用户，详情请参见创建角色。
- 创建阿里云Elasticsearch（简称ES）实例。

  详情请参见创建阿里云Elasticsearch实例。

操作步骤

1. 登录Kibana控制台。 登录控制台的具体步骤请参见登录Kibana控制台。
2. 在左侧导航栏，单击Management。
3. 在Security区域，单击Users。
4. 单击Create new user，然后输入相关参数配置。



参数	说明
Username	用户名称，用来登录Kibana控制台。自定义输入。
Password	该用户的密码，用来登录Kibana控制台。自定义输入。
Confirm password	确认密码，与Password保持一致。
Full name	用户全名，自定义输入。
Email address	用户的Email地址。
Roles	为用户分配角色。选择已创建的角色，或系统预置的角色，可选择多个。 **注意** 在创建角色时，如果已选择了对应用户，此处依然需要选择角色，否则登录时会报错。

5. 单击Create user。

6.Elasticsearch服务关联角色

Elasticsearch服务关联角色（包括AliyunServiceRoleForElasticsearchOps和AliyunServiceRoleForElasticsearchCollector角色）是为了使用集群弹性扩缩容、创建和管理Beats采集器功能，需要获取其他云服务的访问权限，而提供的RAM角色。本文介绍阿里云Elasticsearch服务关联角色的应用场景，以及如何删除服务关联角色。

背景信息

关于服务关联角色的详细信息，请参见服务关联角色。

应用场景

AliyunServiceRoleForElasticsearchOps和AliyunServiceRoleForElasticsearchCollector角色的应用场景如下：

- AliyunServiceRoleForElasticsearchOps

  执行集群弹性扩缩容任务时，需要通过服务关联角色功能，授权阿里云Elasticsearch后台调用集群弹性扩缩容的OpenAPI，按照您设定的时间对集群扩缩容。

- AliyunServiceRoleForElasticsearchCollector

  创建和管理Beats采集器时，需要通过服务关联角色功能，授权Beats采集器在云服务器ECS（Elastic Compute Service），或容器服务Kubernetes版ACK（Container Service for Kubernetes）的目标机器上，进行特定的管控操作。

AliyunServiceRoleForElasticsearchOps介绍

当执行集群弹性扩缩容任务时，如果不存在具有执行任务权限的角色，Elasticsearch将自动创建对应角色（服务关联角色），并为该角色授予相应的权限。Elasticsearch通过扮演该角色即可调用OpenAPI，完成定时扩缩容任务。该角色的相关说明如下：

- 角色名称：AliyunServiceRoleForElasticsearchOps
- 角色权限策略名称：AliyunServiceRolePolicyForElasticsearchOps
- 角色权限策略内容：

```
{
 "Version": "1",
 "Statement": [
  {
   "Action": [
    "elasticsearch:ListInstance",
    "elasticsearch:DescribeInstance",
    "elasticsearch:UpdateInstance",
    "elasticsearch:UpdateInstanceSettings",
    "elasticsearch:RestartInstance",
    "elasticsearch:RollbackInstance",
    "elasticsearch:DowngradeInstance",
    "elasticsearch:CancelTask",
    "elasticsearch:DeactivateZones",
    "elasticsearch:ActivateZones",
    "elasticsearch:MigrateToOtherZone",
    "elasticsearch:ResumeElasticsearchTask",
    "elasticsearch:InterruptElasticsearchTask",
    "elasticsearch:UpdateAdvancedSetting",
    "elasticsearch:UpgradeInstanceEngineVersion",
    "elasticsearch:UpdateWhiteIps",
    "elasticsearch:UpdatePublicIps",
    "elasticsearch:ModifyWhiteIps",
    "elasticsearch:TriggerNetwork",
    "elasticsearch:UpdateTemplate",
    "elasticsearch:DescribeLogstash",
    "elasticsearch:UpdateLogstash",
    "elasticsearch:RestartLogstash",
    "elasticsearch:UpdateLogstashSettings",
    "elasticsearch:InterruptLogstashTask",
    "elasticsearch:ResumeLogstashTask",
    "elasticsearch:DowngradeLogstash"
   ],
   "Resource": "*",
   "Effect": "Allow"
  }
 ]
}
```

- 服务名称：ops.elasticsearch.aliyuncs.com
- 执行服务关联角色操作所需的用户权限：ram:CreateServiceLinkedRole

AliyunServiceRoleForElasticsearchCollector介绍

创建和管理Beats采集器时，如果不存在具有执行任务权限的角色，Elasticsearch将自动创建对应角色（服务关联角色），并为该角色授予相应的权限。Elasticsearch通过扮演该角色即可调用OpenAPI，完成Beats采集器在ECS或ACK目标机器上的数据采集任务。该角色的相关说明如下：

- 角色名称：AliyunServiceRoleForElasticsearchCollector
- 角色权限策略名称：AliyunServiceRolePolicyForElasticsearchCollector
- 角色权限策略内容：

```
{
 "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"
     }
    }
   }
  ]
}
```

- 服务名称：collector.elasticsearch.aliyuncs.com
- 执行创建或删除服务关联角色操作所需的用户权限：ram:CreateServiceLinkedRole

删除服务关联角色

删除AliyunServiceRoleForElasticsearchOps服务关联角色，需要先停止依赖这个服务关联角色的Elasticsearch弹性扩缩容任务；删除AliyunServiceRoleForElasticsearchCollector服务关联角色，需要先删除依赖这个服务关联角色的所有Beats采集器。

删除服务关联角色的具体操作，请参见删除服务关联角色。

常见问题

Q：为什么我的RAM用户无法自动创建Elasticsearch服务关联角色？

A：主账号或拥有CreateServiceLinkedRole权限的RAM用户，才能自动创建或删除服务关联角色。因此当RAM用户无法自动创建服务关联角色时，需要通过主账号为其添加以下权限策略：

> **说明**
> - 具体操作，请参见为RAM用户授权。
> - 以下权限策略中的AccountId，需要替换为您的主账号ID。

- AliyunServiceRoleForElasticsearchOps

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

- AliyunServiceRoleForElasticsearchCollector

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

7.访问控制FAQ

es访问控制常见问题

本文介绍阿里云Elasticsearch（简称ES）访问控制相关的常见问题。

es访问控制常见问题 购买es找不到vpc 销毁临时用户创建的es

为什么使用子账号在阿里云ES实例购买页面找不到VPC？

请参见查看RAM用户基本信息，检查是否已经为对应子账号授予了获取专有网络VPC（Virtual Private Cloud）列表的权限。如果没有授权，请参见为RAM用户授权，为子账号进行授权。

临时用户创建的集群或数据等，会随着临时用户的销毁而销毁吗？

通过临时用户创建的阿里云ES实例不会随着临时用户的销毁而销毁，并且临时用户对阿里云ES实例的修改也不会随着临时用户的销毁而还原，相当于行使主账号的权限进行操作。

使用ES时报错“子账户无权限，请核对子账号权限”，如何处理？

对子账号授予ES的使用权限，将如下之一权限授权给您的子账号，详情请参见为RAM用户授权。

- `AliyunElasticsearchReadOnlyAccess`：只读访问阿里云ES或Logstash的权限，可用于只读用户。
- `AliyunElasticsearchFullAccess`：管理阿里云ES或Logstash的权限，可用于管理员。

如何创建一个对ES实例中索引等资源的只读用户？

需要在Kibana控制台中创建只读权限的角色，并将该角色分配给对应用户，详情请参见索引操作授权。

授权的角色用户登录Kibana看不到索引，只有管理员elastic账号能看到，怎么办？

在创建用户时，为用户分配kibana_system权限。