ALIBABA CLOUD

阿里云

阿里云Elasticsearch

访问控制

文档版本：20220419

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.RAM访问控制 05
1.1. 授权资源 05
1.2. 创建自定义权限策略 17
1.3. 通过资源组授权特定实例 25
1.4. 为RAM用户授权 31
2.Elasticsearch集群访问控制 34
3.Elasticsearch服务关联角色 36
4.访问控制FAQ 41

1.RAM访问控制

1.1. 授权资源

es授权资源类型

当您需要精细化地管理用户权限时，可通过创建自定义权限策略实现。创建时，需要配置Action（操作）和Resource（资源）。本文提供了阿里云Elasticsearch通过访问控制实现团队或者部门成员鉴权、RAM用户授权、RAM角色授权以及跨云服务授权的Action和Resource列表。

背景信息

默认情况下，阿里云主账号或者RAM用户均能使用Elasticsearch控制台或Elasticsearch API操作自己创建的Elasticsearch资源。在以下场景中，会涉及到操作授权问题：

- 刚创建的RAM用户没有权限操作阿里云主账号的资源时。
- 从其他阿里云服务访问Elasticsearch资源，或者Elasticsearch访问其他阿里云服务时。
- 操作具有权限控制的Elasticsearch资源前，需要资源拥有者授权目标资源和目标API行为权限。

自定义策略

您可以通过RAM控制台或者调用RAM API CreatePolicy创建一个自定义权限策略。

使用控制台的**脚本配置**方式，在自定义策略中，根据JSON模板文件填写**策略内容**。其中的Action和Resource参数取值为本文授权资源列表中对应的参数值。详细信息，请参见创建自定义权限策略和权限策略基本元素。

```
{
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
                "elasticsearch:[Elasticsearch RAM Action]",
                "elasticsearch:ListInstance"
            ],
    "Resource": [
                "[Elasticsearch RAM Action Resource]",
                "acs:elasticsearch:cn-hangzhou:133071096032****:instances/es-cn-2r42b7uyg003k****"
            ]
  }
  ],
  "Version": "1"
}
```

授权资源列表

- 实例管理

Action	Resource	Action描述
elasticsearch:CreateInstance	acs:elasticsearch:<yourRegionId>:	创建实例。
elasticsearch:ListInstance		查看所有实例的详细信息。

Action	Resource	Action描述
	<yourRegionId>:<yourAccountId>:instances/*	
elasticsearch:DescribeInstance	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	查询指定实例的详细信息。
elasticsearch:EstimatedRestartTime		获取重启实例的预估时间。
elasticsearch:RestartInstance		重启指定实例。
elasticsearch:UpdateInstanceChargeType		将按量付费实例转换为包年包月实例。
elasticsearch:UpdateDescription		更新指定实例的名称。
elasticsearch:DeleteInstance		释放指定按量付费类型的阿里云Elasticsearch实例。
elasticsearch:CancelDeletion		恢复释放后被冻结的Elasticsearch实例。
elasticsearch:RenewInstance		为包年包月实例续费。
elasticsearch:ActivateZones		恢复已下线的可用区。
elasticsearch:DeactivateZones		在有多个可用区的情况下，下线部分可用区。并将下线的可用区中的节点迁移到其他可用区。
elasticsearch:UpdateReadWritePolicy		开启或关闭实例的写入高可用特性。
elasticsearch:InterruptElasticsearchTask		中断变更中的实例。
elasticsearch:ResumeElasticsearchTask		恢复中断变更的实例。
elasticsearch:DescribeElasticsearchHealth		获取指定实例的健康情况。
elasticsearch:GetElastictask		获取集群的弹性扩缩容规则。
elasticsearch:ModifyElastictask		更新实例的弹性扩缩容规则。
elasticsearch:ListInstanceIndices		获取实例的索引列表。
elasticsearch:MigrateToOtherZone		迁移对应可用区下的节点到目标可用区。
elasticsearch:MoveResourceGroup		迁移实例到指定资源组。

Action	Resource	Action描述
elasticsearch:ModifyInstanceMaintainTime		更改并开启实例的可维护时间。
elasticsearch:ListShardRecoveries		查看正在进行和已完成的分片恢复的数据进度列表。

- 标签管理

Action	Resource	Action描述
elasticsearch:ListTags	acs:elasticsearch:<yourRegionId>:<yourAccountId>:tags/<yourInstanceId>	查询所有可见的用户标签。
elasticsearch:CreateTags		创建或更新标签。
elasticsearch:RemoveTags		删除标签。
elasticsearch:ListTagResources	○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:tags/* ○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:tags/<yourInstanceId>	查询可见资源标签关系。

- 数据迁移

Action	Resource	Action描述
elasticsearch:ListDataTasks	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	查看数据迁移任务信息。
elasticsearch:CancelTask		取消数据迁移任务。
elasticsearch:CreateDataTasks		创建索引迁移任务，将所选实例中的数据迁移到当前实例。
elasticsearch:DeleteDataTask		删除索引迁移任务。
elasticsearch:GetClusterDataInformation	○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/* ○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	获取实例的数据信息。

- 实例升降配

Action	Resource	Action描述
elasticsearch:UpgradeEngineVersion	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	升级实例版本或内核补丁版本。
elasticsearch:UpdateInstance		变更实例配置。
elasticsearch:DowngradeInstance		○ 缩容前，校验是否可以迁移指定实例中某些节点上的数据。 ○ 缩容前，执行数据迁移任务。 ○ 校验指定实例中的某些节点是否可以缩容。 ○ 执行实例节点缩容操作。

- 集群配置

Action	Resource	Action描述
elasticsearch:UpdateInstanceSettings	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	更新指定实例的YML参数配置。
elasticsearch:UpdateHotIkDicts		热更新实例的IK分词插件，包括IK主分词词库和IK停用词词库。
elasticsearch:UpdateSynonymsDicts		更新实例的同义词词典。
elasticsearch:UpdateDict		冷更新实例的IK分词插件，包括IK主分词词库和IK停用词词库。
elasticsearch:UpdateAliwsDict		更新AliNLP分词插件（analysis-aliws）的词典文件。
elasticsearch:ListDictInformation		在添加用户OSS存储的词典文件时，获取和校验用户OSS词典文件的详情。
elasticsearch:UpdateAdvancedSetting		更改指定实例的垃圾回收器配置。
elasticsearch:DescribeTemplates		获取实例的场景化配置模板。
elasticsearch:UpdateExtendConfig		修改实例的场景化配置模板。
elasticsearch:UpdateTemplate		修改实例的场景化模板配置内容。
elasticsearch:RecommendTemplates		获取推荐的场景化模板配置。
elasticsearch:ListDicts		查看指定类型的词典详情以及签名生成的公网可下载链接。

- 索引管理

Action	Resource	Action描述
elasticsearch:CreateIndexTemplate	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	创建索引模板。
elasticsearch:DeleteIndexTemplate		删除索引模板。
elasticsearch:UpdateIndexTemplate		更新索引模版的组件化设置。
elasticsearch:DescribeIndexTemplate		获取索引模版的组件化设置。
elasticsearch:ListIndexTemplates		查看索引模板列表。
elasticsearch:DescribeILMPolicy		查询指定索引生命周期详情。
elasticsearch:ListILMPolicies		查看已有的索引生命周期策略列表。
elasticsearch:CreateILMPolicy		创建索引生命周期策略。
elasticsearch:DeleteILMPolicy		删除指定的生命周期策略定义。
elasticsearch:UpdateILMPolicy		修改索引生命周期策略。
elasticsearch:CreateDataStream		创建数据流。
elasticsearch:DeleteDataStream		删除数据流。
elasticsearch:RolloverDataStream		滚动更新数据流下的匹配索引。
elasticsearch:ListDataStreams		查看数据流列表。
elasticsearch:CloseManagedIndex		关闭Indexing Service实例中某个索引的云端托管功能。

- 插件管理

Action	Resource	Action描述
elasticsearch:ListPlugins	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	查看指定实例的插件列表。
elasticsearch:InstallSystemPlugin		安装系统预置插件。
elasticsearch:UninstallPlugin		卸载已安装的预置插件。

Action	Resource	Action描述
elasticsearch:InstallUserPlugins		安装用户自定义的已经上传至Elasticsearch控制台的插件。

- 集群监控和日志查询

Action	Resource	Action描述
elasticsearch:GetEmonMonitorData	acs:elasticsearch:<yourRegionId>:<yourAccountId>:emonProjects/<yourProjectId>	获取Grafana指标监控数据。
elasticsearch:GetEmonGrafanaDashboards		获取Grafana大盘列表。
elasticsearch:GetEmonGrafanaAlerts		获取Grafana报警列表。
elasticsearch:PostEmonTryAlarmRule	acs:elasticsearch:<yourRegionId>:<yourAccountId>:emonProjects/*	发送测试的报警消息。
elasticsearch:GetEmonAlarmGroupList		获取报警组列表。
elasticsearch:ListSearchLogs	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	查看实例日志。

- 安全配置

Action	Resource	Action描述
elasticsearch:TriggerNetwork	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yo	开启或关闭Elasticsearch或Kibana实例的公网或私网访问。
elasticsearch:UpdatePrivateNetworkWhiteIps		更新指定实例的VPC私网访问白名单。
elasticsearch:UpdatePublicWhiteIps		更新指定实例的公网地址访问白名单。
elasticsearch:UpdatePublicNetwork		开启或关闭指定实例的公网地址。
elasticsearch:UpdateWhiteIps		更新实例的VPC私网访问白名单。
elasticsearch:ModifyWhiteIps		更新指定实例的访问白名单。
elasticsearch:UpdateAdminPassword		更新指定实例的elastic账号的密码。
elasticsearch:OpenHttps		开启HTTPS协议。

Action	Resource	Action描述
elasticsearch:CloseHttps		关闭HTTPS协议。
elasticsearch:AddConnectableCluster		配置实例网络互通。
elasticsearch:DeleteConnectedCluster		移除互通实例。
elasticsearch:DescribeConnectableClusters		获取能够与当前实例进行网络互通的实例列表。不包括已经打通的实例。
elasticsearch:ListConnectedClusters		获取已经与当前实例进行了网络互通的实例列表。
elasticsearch:DeleteVpcEndpoint		删除服务VPC下的终端节点。
elasticsearch:ListVpcEndpoints		查看服务VPC下的终端节点状态。

- 数据备份

Action	Resource	Action描述
elasticsearch:CreateSnapshot	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	手动对实例进行快照备份。
elasticsearch:AddSnapshotRepo	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/*	在设置跨集群OSS仓库时，创建引用仓库。
elasticsearch:DeleteSnapshotRepo		删除一个跨集群OSS引用仓库。
elasticsearch:ListSnapshotReposByInstanceId		获取当前实例的跨集群OSS仓库设置列表。
elasticsearch:ListAlternativeSnapshotRepos	acs:elasticsearch:<yourRegionId>:<yourAccountId>:snapshotrepository/*	获取当前实例可添加的OSS引用仓库。
elasticsearch:DescribeSnapshotSetting	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	获取指定实例的数据备份配置。
elasticsearch:UpdateSnapshotSetting		更新指定实例的数据备份配置。

- 智能运维

Action	Resource	Action描述
elasticsearch:OpenDiagnosis	◦ acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/* ◦ acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	开启智能运维。
elasticsearch:CloseDiagnosis		关闭智能运维。
elasticsearch:UpdateDiagnosisSettings		更新智能运维场景设置。
elasticsearch:DiagnoseInstance		即刻诊断实例。
elasticsearch:ListDiagnoseReport		查看智能运维的历史报告。
elasticsearch:ListDiagnoseReportIds		查看智能运维历史报告的ID。
elasticsearch:ListDiagnoseIndices		查看指定实例智能运维模块中，健康诊断的诊断索引。
elasticsearch:DescribeDiagnoseReport		获取智能运维的历史报告。
elasticsearch:DescribeDiagnosisSettings		获取智能运维的场景设置。

Action	Resource	Action描述
elasticsearch:DescribeKibanaSettings	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/<yourInstanceId>	查看Kibana配置。
elasticsearch:UpdateKibanaSettings		更新Kibana配置。
elasticsearch:ListKibanaPlugins		查看Kibana插件。
elasticsearch:InstallKibanaSystemPlugin		安装Kibana插件。
elasticsearch:UninstallKibanaPlugin		卸载Kibana插件。
elasticsearch:UpdateKibanaWhiteIps		修改Kibana白名单。

- 实例管理

Action	Resource	Action描述

Action	Resource	Action描述
elasticsearch:CreateLogstash	○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/* ○ acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	创建一个Logstash实例。
elasticsearch:ListLogstash		查看所有或指定Logstash实例的详细信息。
elasticsearch:DescribeLogstash	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	查询指定Logstash实例的详细信息。
elasticsearch:UpdateLogstash		修改指定Logstash实例的部分信息，例如节点数、配额、名称、硬盘大小等。
elasticsearch:RenewLogstash		为Logstash实例续费。
elasticsearch:RestartLogstash		重启指定的Logstash实例。
elasticsearch:EstimatedLogstashRestartTime		获取Logstash实例重启的预估时间。
elasticsearch:UpdateLogstashDescription		修改指定Logstash实例的名称。
elasticsearch:UpdateLogstashChargeType		将按量付费的Logstash实例转换为包年包月实例。
elasticsearch:DeleteLogstash		释放指定按量付费的Logstash实例。
elasticsearch:CancelLogstashDeletion		恢复释放后被冻结的Logstash实例。

- 集群配置

Action	Resource	Action描述
elasticsearch:UpdateLogstashSettings	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	更新指定Logstash实例的配置。
elasticsearch:ListExtendfiles		查看指定Logstash实例的扩展文件配置。
elasticsearch:UpdateExtendfiles		更新指定Logstash实例的扩展文件配置。

- 插件管理

Action	Resource	Action描述
elasticsearch:ListPlugin	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	查看插件列表。
elasticsearch:InstallSystemPlugin		安装系统预置插件。
elasticsearch:UninstallSystemPlugin		卸载系统预置插件。

- 集群监控和日志查询

Action	Resource	Action描述
elasticsearch:ListAvailableEsInstanceIds	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	在设置Logstash实例的X-Pack监控时，查看可用的Elasticsearch实例列表（具备X-Pack监控能力）。
elasticsearch:ValidateConnection		在Logstash实例的监控报警配置中，验证提供X-Pack监控的Elasticsearch实例的联通性。
elasticsearch:UpdateXpackMonitorConfig		更新Logstash实例的X-Pack监控报警配置。
elasticsearch:DescribeXpackMonitorConfig		获取Logstash实例的X-Pack监控配置。
elasticsearch:ListLogstashLog		查看Logstash实例的日志。

- 变更任务管理

Action	Resource	Action描述
elasticsearch:InterruptLogstashTask	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	中断实例变更任务。
elasticsearch:ResumeLogstashTask		恢复实例的变更中断任务。

- 管道管理

Action	Resource	Action描述
elasticsearch:CreatePipelines		创建管道。
elasticsearch:ListPipeline		查看管道列表。
elasticsearch:DescribePipeline		查看管道配置。
elasticsearch:UpdatePipelines		更新管道配置。
elasticsearch:RunPipelines		立即部署管道。

Action	Resource	Action描述
elasticsearch:StopPipelines	acs:elasticsearch:<yourRegionId>:<yourAccountId>:logstashes/<yourInstanceId>	停止运行管道。
elasticsearch:UpdatePipelineManagementConfig		更新管道管理方式。
elasticsearch:DescribePipelineManagementConfig		获取管道管理配置。
elasticsearch:ListPipelineIds		设置Kibana管道管理时，测试Logstash与Kibana连通性，并获取目标Kibana上创建的管道ID列表。
elasticsearch:DeletePipelines		删除管道。

Action	Resource	Action描述
elasticsearch:CreateCollector	acs:elasticsearch:<yourRegionId>:<yourAccountId>:collectors/<yourCollectorId>	创建采集器。
elasticsearch:DescribeCollector		获取采集器的详细信息。
elasticsearch:ReinstallCollector		重试安装在创建时没有安装成功的采集器。
elasticsearch:ListCollectors	acs:elasticsearch:<yourRegionId>:<yourAccountId>:collectors/*	获取采集器列表信息。
elasticsearch:ListDefaultCollectorConfigurations		获取采集器的默认配置文件。
elasticsearch:UpdateCollectorName	acs:elasticsearch:<yourRegionId>:<yourAccountId>:collectors/<yourCollectorId>	修改采集器名称。
elasticsearch:UpdateCollector		更新采集器信息。
elasticsearch:StartCollector		启动采集器。
elasticsearch:RestartCollector		重启采集器。
elasticsearch:StopCollector		停止运行中的采集器。
elasticsearch:DeleteCollector		删除采集器。
elasticsearch:ListEcsInstances		获取ECS机器列表。
elasticsearch:ModifyDeployMachine		更新采集器安装的ECS机器。
elasticsearch:ListNodes		查看安装采集器的ECS机器的状态。
elasticsearch:ListAckClusters	acs:elasticsearch:<yourRegionId>:<yourAccountId>:ackClusters/*	查看容器服务Kubernetes版ACK集群列表。

Action	Resource	Action描述
elasticsearch:ListAckNamespaces	acs:elasticsearch:<yourRegionId>:<yourAccountId>:ackClusters/<yourClusterId>	查看指定容器服务Kubernetes版ACK集群的所有命名空间。
elasticsearch:DescribeAckOperator		查看指定容器服务Kubernetes版ACK集群上安装的Elasticsearch Operator信息。
elasticsearch:InstallAckOperator		在指定容器服务Kubernetes版ACK集群上安装Elasticsearch Operator。

Action	Resource	Action描述
elasticsearch:InitializeOperationRole	acs:elasticsearch:<yourRegionId>:<yourAccountId>:instances/*	创建服务关联角色。

Action	Resource	Action描述
cms:ListProductOfActiveAlert	acs:elasticsearch:<yourRegionId>:<yourAccountId>:*	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实例的监控数据。

Action	Resource	Action描述
elasticsearch:DescribeVpcs	acs:elasticsearch:<yourRegionId>:<yourAccountId>:vpc/*	获取VPC列表。
elasticsearch:DescribeVswitches	acs:elasticsearch:<yourRegionId>:<yourAccountId>:vswitch/*	获取vSwitch列表。

Elasticsearch

Kibana

Logstash

Beats

访问控制

底层云监控

购买页专有网络和虚拟交换机

参数说明

本文Resource中包含的参数说明如下，请在使用时替换为实际值：

- <yourRegionId>：实例所在地域的ID，*表示所有地域下的资源。各地域对应的地域ID如下。

地域	地域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
中东与印度	印度（孟买）	ap-south-1

- <yourAccountId>：阿里云账号ID，*表示所有账号下的资源。
- <yourInstanceId>：实例ID，*表示所有实例资源。
- <yourProjectId>：高级监控报警项目ID。
- <yourCollectorId>：Beats采集器ID。
- <yourClusterId>：安装Beats采集器的容器服务Kubernetes版ACK集群ID。

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。

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、Logstash或Beats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、Logstash或Beats的权限，不包括云监控和Tags权限，使用时需自定义对应权限。您也可以参见权限策略示例配置。
> - 阿里云Elasticsearch实例默认创建在默认资源组下。当您为RAM用户授予指定的自定义权限策略后，通过该RAM用户登录阿里云Elasticsearch控制台，依旧会显示全量实例。如果您想对特定RAM用户仅显示控制台的特定资源，那么可以采用通过资源组授权特定实例的方式实现。

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。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**创建权限策略**页面，单击**脚本编辑**页签。
5. 输入权限策略内容，然后单击**下一步**。

   您也可以单击右侧的**导入系统策略**，根据页面提示导入已存在的系统权限策略，并在此基础上修改为自定义的权限策略。

根据需求输入具体的权限脚本，例如：

- 访问阿里云账号的专有网络VPC（Virtual Private Cloud）权限。

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

> 说明 策略内容请参见系统模板AliyunVPCReadOnlyAccess。

- RAM用户订单权限。

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

> 说明 策略内容请参见系统模板AliyunBSSOrderAccess。

- API对应权限。

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

Method	URI	Resource	Action
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。

6. 输入权限策略**名称**和**备注**。
7. 检查并优化权限策略内容。
   - 基础权限策略优化

     系统会对您添加的权限策略语句自动进行基础优化。基础权限策略优化会完成以下任务：
     - 删除不必要的条件。
     - 删除不必要的数组。
   - （可选）高级权限策略优化

     您可以将鼠标悬浮在**可选：高级策略优化**上，单击**执行**，对权限策略内容进行高级优化。高级权限策略优化功能会完成以下任务：
     - 拆分不兼容操作的资源或条件。
     - 收缩资源到更小范围。
     - 去重或合并语句。
8. 单击**确定**。

权限策略示例

> **注意**
>
> 在使用以下代码示例前，请将代码中的以下信息替换成您自己对应的信息：
>
> - 133071096032****：需要替换为您自己的阿里云账号ID。阿里云账号ID的获取方法：鼠标移至控制台右上角的用户头像上，即可查看到**账号ID**。
> - es-cn-tl32awopr002h****：需要替换为待授权的目标实例ID。获取方式，请参见查看实例的基本信息。

- 管理员权限策略

  以下示例用于为账号ID为133071096032****的阿里云账号下的某个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": [
                "cms:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "bss:PayOrder",
            "Effect": "Allow",
            "Resource": "*"
        },
       {
          "Action": "ims:*",
          "Effect": "Allow",
          "Resource": "acs:ims::133071096032****:application/*"
        },
        {
            "Action": "ram:CreateServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "collector.elasticsearch.aliyuncs.com",
                        "ops.elasticsearch.aliyuncs.com"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

- 操作特定实例权限策略

  以下示例用于为账号ID为133071096032****的阿里云账号下的某个RAM用户授权，使该用户拥有以下权限：

  - 底层云监控权限。
  - 给指定实例授予所有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。

说明 因为阿里云Elasticsearch控制台的实例管理页面，集成调用了Beats采集器、阿里云高级监控和标签Tags等外部依赖接口，所以在对特定实例授权时，需要参见以下配置示例，授予依赖权限。

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

```
            "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:DescribeActiveMetricRuleList", "cms:ListAlarm", "cms:QueryMetricList" ]`	云监控权限，具体说明如下： • `cms:DescribeActiveMetricRuleList`：获取阿里云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。
`"ims:*"`	RAM用户使用高级监控报警时，需要授予ims权限。您也可以通过阿里云账号登录高级监控报警控制台，手动对RAM用户授权，具体操作请参见步骤一：查看和配置可视化监控。 **说明** IMS（Identity Management Service）为身份管理服务。主要管理的对象为阿里云RAM用户相关的身份Meta及认证相关的配置。同时，IMS提供了标准协议，能够应用于外部IDP控制台认证打通和用户数据同步的场景。

Action	说明
`[ "elasticsearch:DescribeVpcs", "elasticsearch:DescribeVSwitches" ]`	访问阿里云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用户可选择阿里云账号创建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，会出现无权限的报错。
`[ "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、云监控和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Beats采集器列表。

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，查看对应地域下包含的所有Logstash实例。
`[ "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。

Resource说明

Resource的详细说明请参见授权资源。

参数	说明
*	所有实例资源。
es-cn-tl32awopr002h****	指定的实例资源，需要替换为待授权的目标实例ID。获取方式，请参见查看实例的基本信息。

后续步骤

自定义策略创建完成后，使用阿里云账号在RAM控制台中或通过RAM SDK对RAM用户授权。具体操作，请参见为RAM用户授权。

1.3. 通过资源组授权特定实例

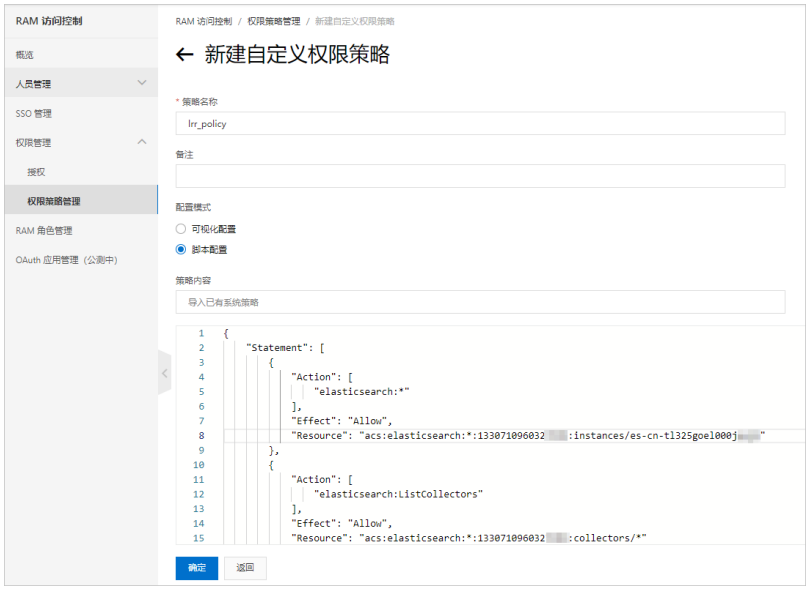
本文介绍如何在RAM控制台，通过资源组为RAM用户配置特定实例的管控权限。

背景信息

阿里云Elasticsearch实例默认创建在默认资源组下，以RAM用户身份对特定实例进行自定义权限策略授权后，阿里云Elasticsearch控制台依旧会显示全量实例。如果您想对特定RAM用户仅显示控制台的特定资源，那么您可以通过资源组管理方式进行授权配置。

步骤一：为RAM用户添加整个云账号的自定义策略权限

1. 使用阿里云账号登录RAM控制台。
2. 配置**新建自定义权限策略**。
   i. 在左侧导航栏，选择**权限管理 > 权限策略管理**。
   ii. 在**权限策略管理**页面，单击**创建权限策略**。
   iii. 输入**策略名称**。
   iv. 在**配置模式**中，选择**脚本配置**。



   v. 配置**策略内容**，详细信息请参见如下示例。

```
{
    "Statement": [
        {
            "Action": [
                "elasticsearch:*"
            ],
            "Effect": "Allow",
            "Resource": "acs:elasticsearch:*:<yourAccountId>:instances/<yourInstanceId>"
        },
        {
            "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"
}
```

使用示例时，您需要将替换以下变量值。

变量	说明
<yourAccountId>	替换为您的阿里云账号ID。阿里云账号ID的获取方法：鼠标移至控制台右上角的用户头像上，即可查看到**账号ID**。
<yourInstanceId>	替换为待授权的目标实例ID。获取方式，请参见查看实例的基本信息。

因为阿里云Elasticsearch控制台的实例管理页面，集成调用了Beats采集器、阿里云高级监控报警服务和标签Tags等外部依赖接口，所以，当控制台仅对特定资源组的实例进行管理时，需要配置整个阿里云账号下的自定义策略，才能保证控制台页面通过RAM用户权限的校验。

> **说明** 配置好访问特定实例的RAM权限后，您还可以通过Elasticsearch和Logstsah的接口直接访问特定的实例。直接访问特性实例的方式分别如下：
>
> - https://elasticsearch.console.aliyun.com/{regionId}/instances/{instanceId}/base
> - https://elasticsearch.console.aliyun.com/{regionId}/logstashes/{instanceId}/base

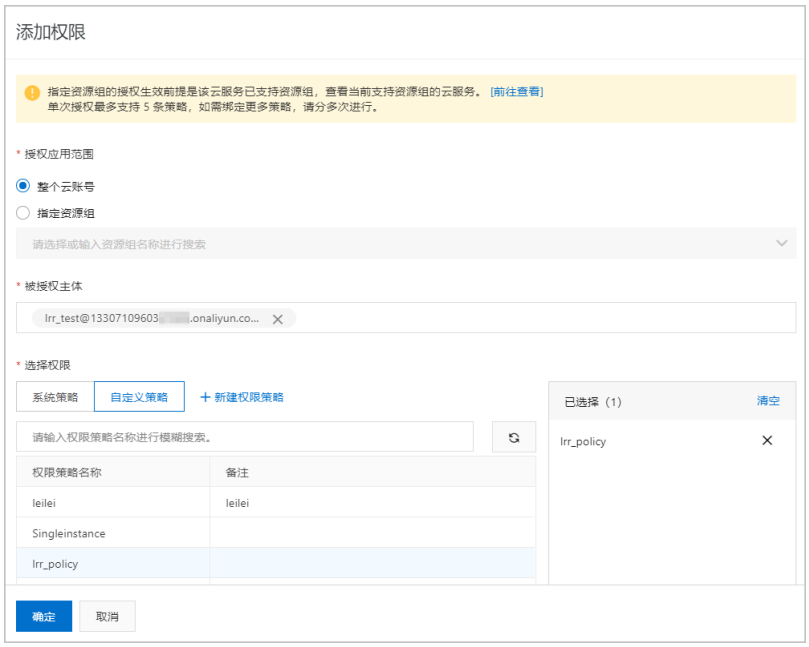
vi. 单击**确定**。

3. 创建RAM用户。
   i. 在左侧导航栏，选择**人员管理 > 用户**。
   ii. 单击**创建用户**。
   iii. 在**创建用户**页面，输入**登录名称**和**显示名称**。

iv. 单击**确定**，即可查看到创建的用户信息。

4. 为RAM用户添加整个云账号的自定义策略权限。
   i. 选择创建的目标**用户登录名称/显示名称**。
   ii. 单击**操作**列下的**添加权限**。

iii. 在**添加权限**面板中，**自定义策略**选择步骤2中创建的自定义策略名称。



iv. 单击**确定**。

v. 单击**完成**。

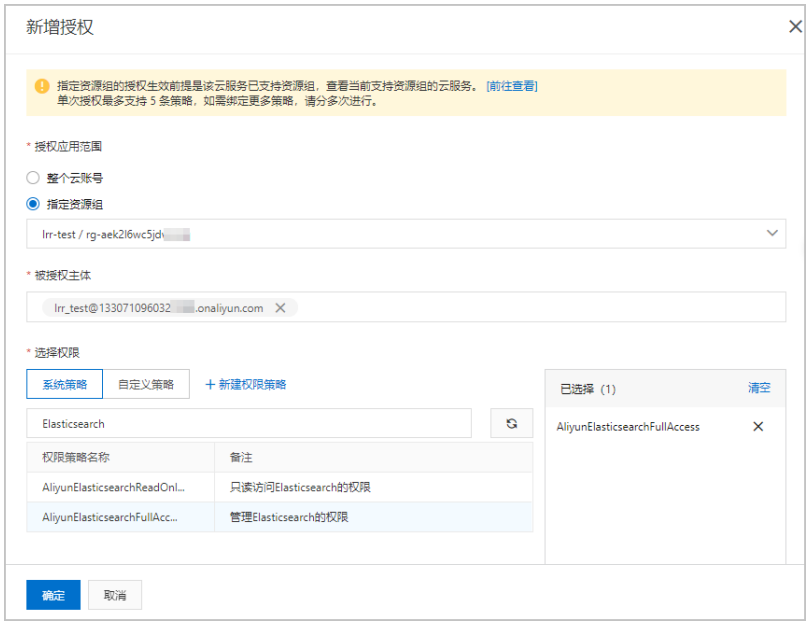
步骤二：创建资源组并关联特定资源组的权限策略

1. 登录资源管理控制台。
2. 创建资源组。
   i. 在左侧导航栏，单击**资源组**。
   ii. 单击**创建资源组**。

iii. 在**创建资源组**面板中，输入**资源组标识**和**资源组名称**。

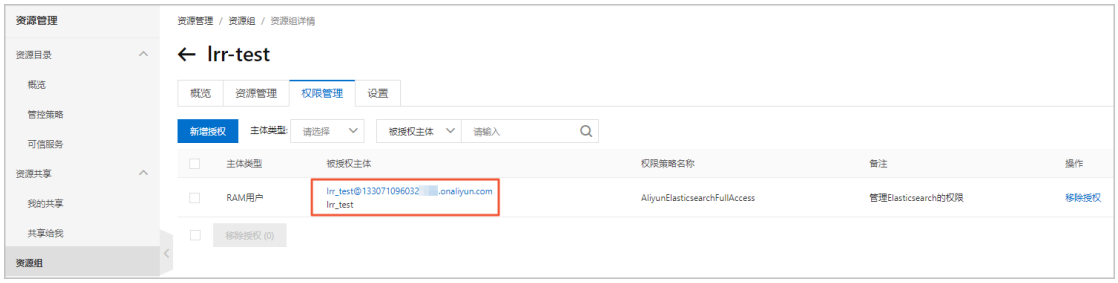
iv. 单击**确定**。

3. 将默认资源组下的特定实例转出到自定义资源组下。
   i. 单击**默认资源组**。
   ii. 单击**资源管理**页签。
   iii. 选择目标实例ID，单击**转出资源**。
   iv. 在**转出资源**面板，选择自定义的目标资源组。
   v. 单击**确定**。
4. 进行授权操作。
   i. 在左侧导航栏，单击**资源组**。
   ii. 找到之前自定义的目标资源组名称，单击**操作**列下的**权限管理**。
   iii. 单击**新增授权**。
   iv. 在**新增授权**面板，配置相关信息。

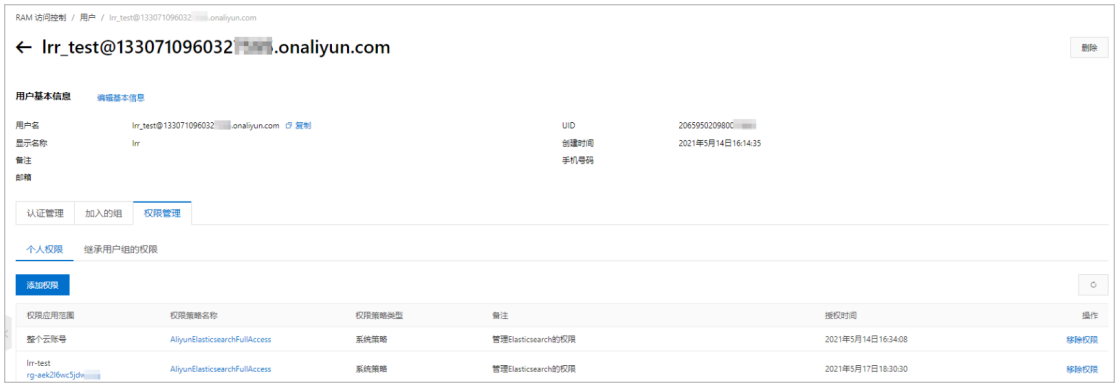


v. 单击**确定**。
vi. 单击**完成**。

5. 查看当前用户授权信息。
   i. 单击**权限管理**页签。
   ii. 单击**被授权主体**名称。



iii. 在**用户基本信息**页面，单击**权限管理**页签，查看当前用户授权信息。



步骤三：以RAM用户身份登录阿里云Elasticsearch控制台

1. 以RAM用户身份登录阿里云Elasticsearch控制台。
2. 在顶部菜单栏，选择地区。
3. 在左侧导航栏，单击**Elasticsearch实例**。
4. 在顶部菜单栏处，选择之前自定义的目标资源组，即可查看对应的实例信息。

1.4. 为RAM用户授权

es 子账号授权

如果您购买了阿里云Elasticsearch实例，您的组织中有多个RAM用户（例如运维、开发或数据分析）需要使用这些实例，您可以创建一个策略，允许特定用户只能使用特定功能，增强系统的安全性和可用性。您也可以创建多个用户组，并授予不同权限策略，实现批量管理用户权限。

背景信息

访问控制RAM是阿里云提供的资源访问控制服务。详细信息，请参见什么是访问控制。

权限策略说明

权限策略分为系统策略和自定义策略：

- 系统策略

系统策略名称	说明
AliyunElasticsearchReadOnlyAccess	只读访问阿里云Elasticsearch或Logstash的权限，用于只读用户。
AliyunElasticsearchFullAccess	管理阿里云Elasticsearch、Logstash或Beats的权限，用于管理员。

- 自定义策略

  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。具体操作，请参见创建自定义权限策略。

前提条件

已创建RAM用户。具体操作，请参见创建RAM用户。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户**操作**列的**添加权限**。
4. 在**添加权限**面板，根据需求选择授权范围、授权主体和权限，为RAM用户添加权限。

参数	描述
授权范围	○ **整个云账号**：权限在当前阿里云账号内生效。 ○ **指定资源组**：权限在指定的资源组内生效。
授权主体	被授权的RAM用户。需要输入RAM用户、用户组或RAM角色进行模糊搜索。
选择权限	○ **系统策略**：输入Elasticsearch搜索阿里云Elasticsearch相关权限策略，然后单击需要授予RAM用户的权限策略，选择该权限。各权限策略的详细说明，请参见权限策略说明。 ○ **自定义策略**：如果系统策略无法满足您的需求，请选择已创建的自定义策略，支持模糊搜索。

5. 单击**确定**。
6. 单击**完成**。
   完成授权后，权限立即生效，您可以以RAM用户身份登录阿里云Elasticsearch控制台，执行已被授权的操作。

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

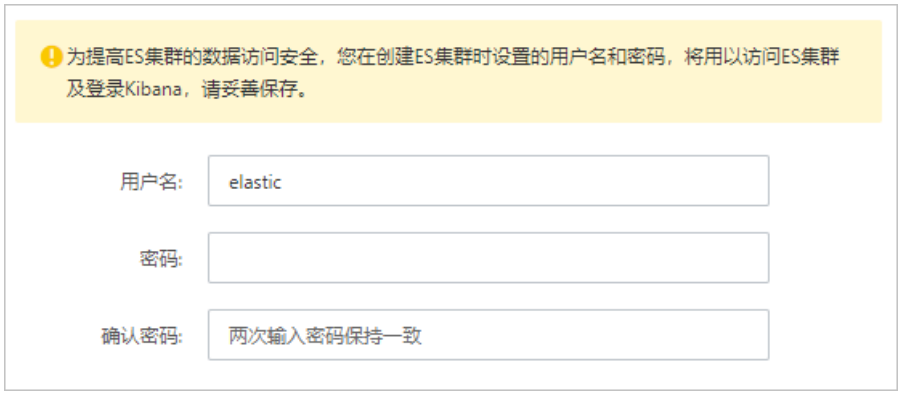
2.Elasticsearch集群访问控制

阿里云Elasticsearch部署在逻辑隔离的专有网络中，结合多种网络访问控制、认证授权、安全加密能力，以及商业插件X-Pack中的高级安全措施，确保云上集群的高安全性。本文介绍阿里云Elasticsearch的访问控制措施。

设置或重置集群访问密码

在创建阿里云Elasticsearch实例时，您需要设置默认用户elastic的密码，用于客户端访问集群、登录Kibana控制台等认证。详细信息，请参见购买页面参数（商业版）和购买页面参数（增强版）。

当您需要修改集群的访问密码时，可通过重置密码功能，重新设置elastic用户的密码。详细信息，请参见重置实例访问密码。



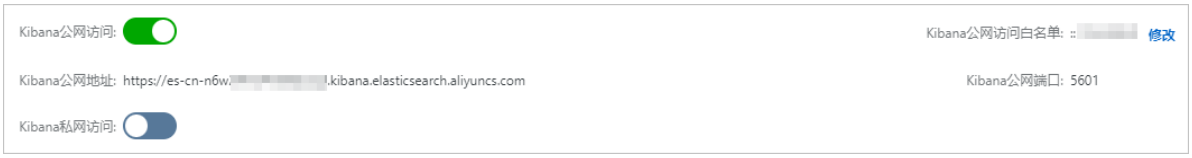
设置Elasticsearch集群访问白名单

- 公网访问白名单：出于安全考虑，阿里云Elasticsearch默认关闭公网访问功能。如果您需要通过公网访问阿里云Elasticsearch，需要手动开启公网访问，并将待访问设备的IP地址加入公网访问白名单组中。详细信息，请参见配置实例公网或私网访问白名单。

- 私网访问白名单：阿里云Elasticsearch默认开启私网访问功能，且支持修改私网访问白名单。如果您需要在私网环境中，通过指定设备访问阿里云Elasticsearch，可将待访问设备的IP地址加入私网访问白名单组中。详细信息，请参见配置实例公网或私网访问白名单。

设置Kibana访问白名单

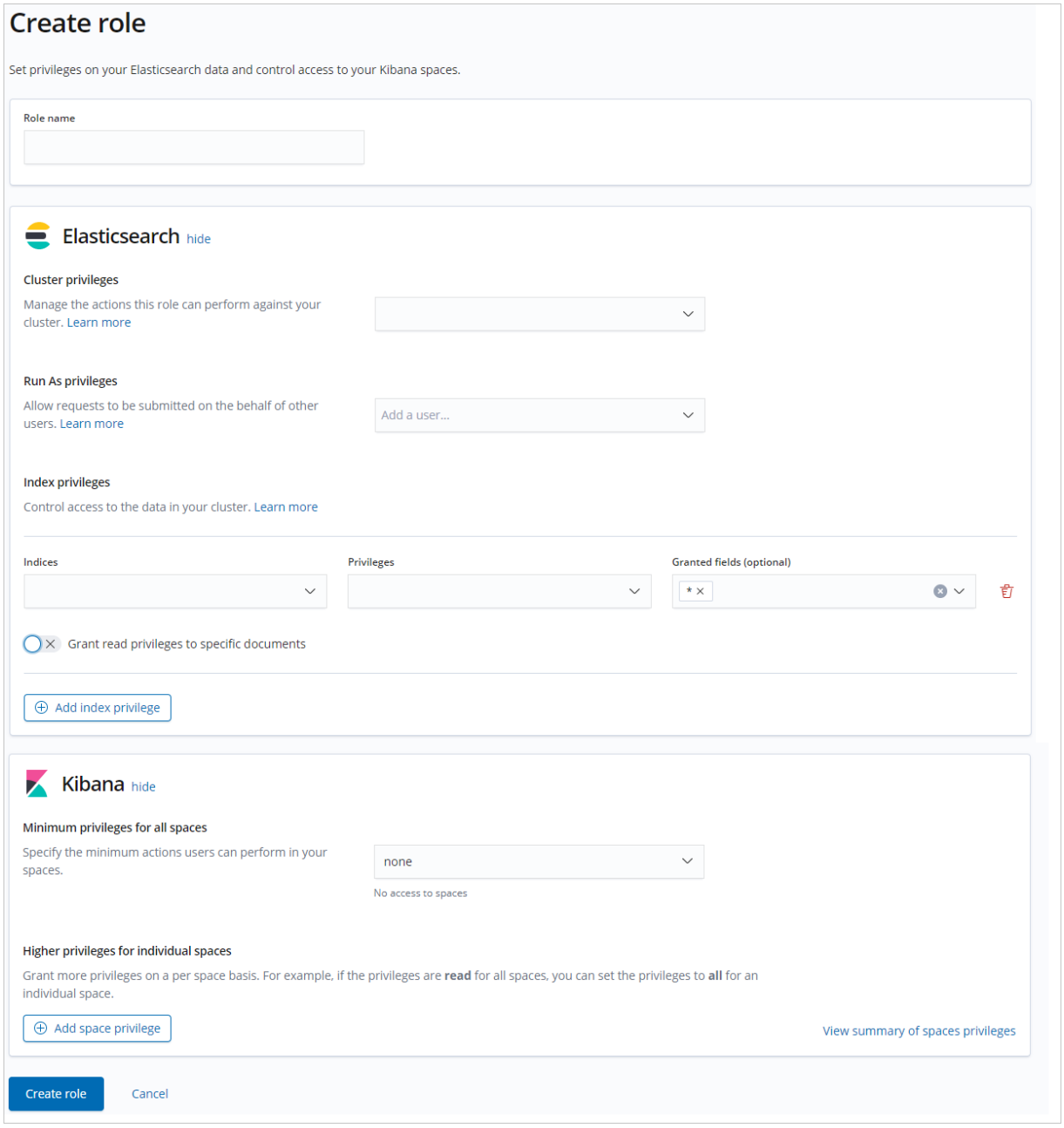
- 公网访问白名单：Kibana公网访问默认开启，但出于安全考虑，阿里云Elasticsearch默认将Kibana的公网访问白名单设置为127.0.0.1,::1，表示不允许任何IPv4和IPv6地址访问。首次进入Kibana控制台时，系统会提示您配置公网访问白名单，您需要将待访问设备的IP地址加入Kibana公网访问白名单中，才可以通过该设备登录Kibana控制台。详细信息，请参见配置Kibana公网或私网访问白名单。



- 私网访问白名单：阿里云Elasticsearch默认关闭Kibana的私网访问功能。如果您需要在私网环境中，通过指定设备登录Kibana控制台，可手动开启Kibana私网访问功能，并将对应设备的IP地址加入Kibana的私网访问白名单组中。详细信息，请参见配置Kibana公网或私网访问白名单。

X-Pack角色权限管控

当您需要设置集群、索引、字段或其他操作的访问权限时，可以通过Elasticsearch X-Pack的RBAC（Role-based Access Control）机制，在Kibana控制台中为自定义角色分配权限，并将角色分配给用户，实现权限管控。详细信息，请参见通过Elasticsearch X-Pack角色管理实现用户权限管控。



3.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用户无法创建Elasticsearch服务关联角色？

A：阿里云账号或拥有CreateServiceLinkedRole权限的RAM用户，才能创建或删除服务关联角色。因此当RAM用户无法创建服务关联角色时，需要通过阿里云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，Resource中的值 `1330710960 32****` 需要替换为您自己的阿里云账号ID。阿里云账号ID的获取方法：鼠标移至控制台右上角的用户头像上，即可查看到**账号ID**。

- RAM用户需要执行依赖服务关联角色AliyunServiceRoleForElasticsearchOps的Elasticsearch弹性扩缩容任务时，可为其添加以下权限策略。

```
{
    "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": [
                        "ops.elasticsearch.aliyuncs.com"
                    ]
                }
            }
        }
    ]
}
```

- RAM用户需要创建和管理依赖服务关联角色AliyunServiceRoleForElasticsearchCollector的Beats采集器时，可为其添加以下权限策略。

```
{
    "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.访问控制FAQ

es访问控制常见问题

本文介绍阿里云Elasticsearch访问控制相关的常见问题。

- 为什么RAM用户在阿里云Elasticsearch实例购买页面找不到VPC?
- 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？
- 使用Elasticsearch时报错“子账号无权限，请核对子账号权限”，如何处理？
- 如何创建一个对Elasticsearch实例中索引等资源的只读用户？
- 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？

为什么RAM用户在阿里云Elasticsearch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RAM用户授予了获取专有网络VPC（Virtual Private Cloud）列表的权限。如果没有授权，请参见创建自定义权限策略，为RAM用户授权。

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Elasticsearch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Elasticsearch实例的修改也不会随着临时用户的销毁而还原，相当于行使阿里云账号的权限进行操作。

使用Elasticsearch时报错“子账号无权限，请核对子账号权限”，如何处理？

参见创建自定义权限策略，为RAM用户授予Elasticsearch特定的操作权限。您也可以为RAM用户授予Elasticsearch所有的操作权限（不包括云监控和Tags权限），即将如下之一权限授权给您的子账号：

- 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、Logstash或Beats的权限，可用于管理员。

如何创建一个对Elasticsearch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。具体操作，请参见通过Elasticsearch X-Pack角色管理实现用户权限管控。

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。具体操作，请参见通过Elasticsearch X-Pack角色管理实现用户权限管控。