

阿里云 阿里云Elasticsearch

实例

文档版本：20191112

法律声明

阿里云提醒您在使用或阅读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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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
	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。	 禁止： 重置操作将丢失用户配置数据。
	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。
	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。
	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。	执行cd /d C:/window命令，进入Windows系统文件夹。
##	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

法律声明.....	I
通用约定.....	I
1 增强版实例介绍.....	1
2 实例列表.....	4
3 实例管理.....	6
4 基本信息.....	9
4.1 基本信息概览.....	9
4.2 节点可视化.....	11
4.3 配置列表.....	13
4.4 集群数据节点缩容.....	14
4.5 集群升配.....	22
5 ES集群配置.....	28
5.1 ES集群配置概述.....	28
5.2 同义词配置.....	28
5.3 高级配置.....	37
5.4 YML文件配置.....	38
5.5 Head插件安装 (Chrome)	47
6 插件配置.....	52
6.1 插件配置概述.....	52
6.2 自定义插件列表.....	53
7 集群监控.....	56
7.1 集群告警.....	56
7.2 集群监控.....	57
8 日志查询.....	65
9 安全配置.....	67
10 配置实例网络互通.....	74
11 数据备份.....	80
11.1 数据备份.....	80
11.2 自动备份指南.....	82
11.3 查看备份状态.....	85
11.4 快照备份及恢复.....	88
11.5 跨集群OSS仓库设置.....	97
12 可视化控制.....	100
12.1 Kibana.....	100
12.1.1 登录Kibana控制台.....	100
12.1.2 基本配置 (6.7.0)	102
12.1.3 访问配置.....	104

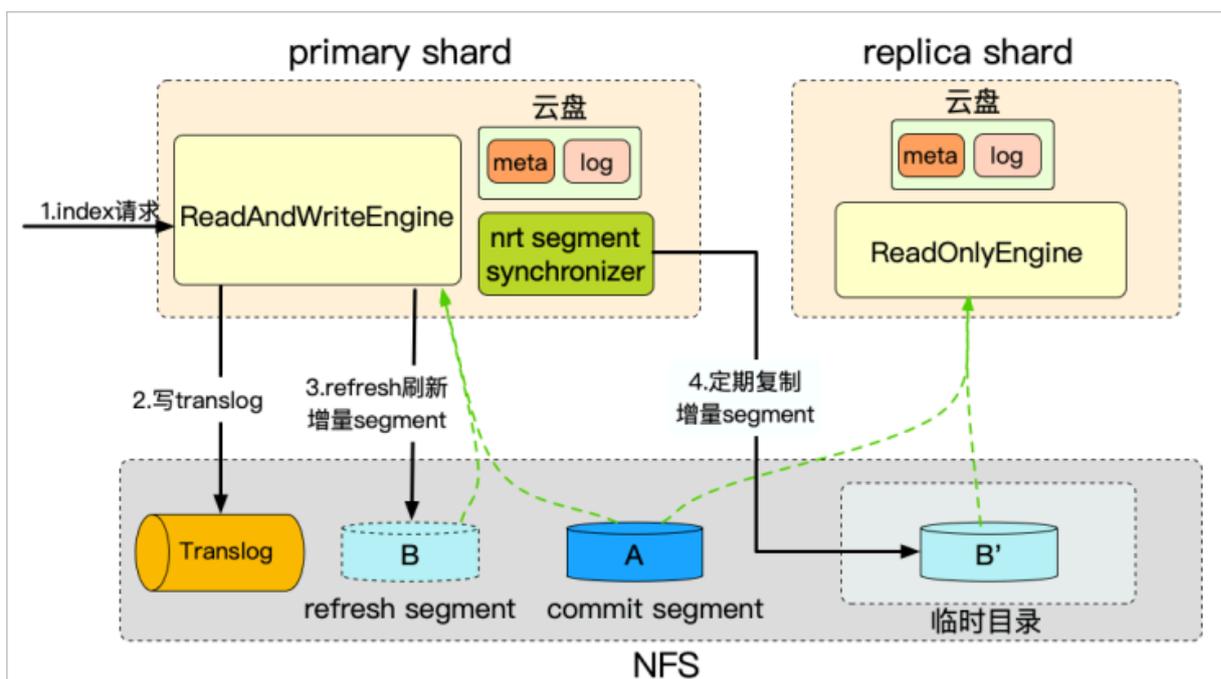
12.1.4 插件配置.....	106
12.1.5 BSearch-QueryBuilder插件使用介绍.....	108
12.1.6 BSearch-Label插件使用介绍.....	118
12.2 使用DataV大屏展示Elasticsearch数据.....	121

1 增强版实例介绍

阿里云Elasticsearch支持商业版和增强版两种类型的实例。商业版ES实例包含了阿里云ES的全部高级特性，增强版ES实例在全部高级特性的基础上，优化和增加了内核及插件，可以提供更好的性能、更高的稳定性和更低成本。本文为您介绍增强版ES实例的相关内容。

增强版Elasticsearch实例，是阿里云Elasticsearch（简称ES）团队基于社区6.7.0版本设计的，基于共享存储CPFS和读写分离架构的Elasticsearch数据模型。

架构



- 索引分片一写多读，数据只保存一份。
- 依赖云存储多副本，保证数据可靠性。
- IO fence机制，保证数据一致性。
- 内存物理复制，降低主备可见性延迟（毫秒可见）。

优势

- 写入性能提升100%，避免了副本写入的开销。
- 存储成本倍数级降低，数据只存一份。
- 副本秒级快速扩缩容和故障迁移，轻松应对高峰流量。

适用场景

- 日志分析场景。日志分析场景具有高吞吐写入、数据存储数据量大的特点，使用增强版ES能成倍提升写入性能，存储成本降低一倍。

- 高并发查询场景。高并发场景对稳定性要求高，当高峰流量远高于低峰时，会有弹性扩缩副本的需求。使用增强版ES不仅能快速扩缩副本，而且能在故障时快速恢复和迁移。

规格选择

目前支持5T/10T的CPFS共享存储空间，实例规格仅支持8核及以上的规格，建议搭配3~10个实例。

 **说明:**
如果需要更大的集群，请在控制台中提交工单。

存储 CPFS存储空间 5TB 10TB
CPFS存储空间暂不支持扩容，请考虑您所需的存储大小后选择

性能测试

数据集为官方esrally提供的nyc_taxis。

16核配置

- 阿里云增强版ES 6.7.0: 5*数据节点 (16核64G) + 3*主节点 (2核8G) + 10TSSD CPFS。
- 原生ES 6.7.0: 5*数据节点 (16核64G) + 3*主节点 (2核8G) + 2000GB SSD。

场景	副本	原生ES 6.7.0 (doc/s)	阿里云ES 6.7.0 (doc/s)	阿里云ES主副本同步延时 (ms)	性能对比
translog异步	1	265358	600044	476	226%
	2	185366	594015	600	320%
	4	103815	585316	854	564%
translog同步	1	177570	414562	286	223%
	2	114547	414278	308	362%
	4	69204	392661	610	567%

8核配置

- 阿里云增强版ES 6.7.0: 5*数据节点 (8核32G) + 3*主节点 (2核8G) + 10TSSD CPFS。
- 原生ES 6.7.0: 5*数据节点 (8核32G) + 3*主节点 (2核8G) + 2000GB SSD。

场景	副本	原生ES 6.7.0 (doc/s)	阿里云ES 6.7.0 (doc/s)	阿里云ES主副同步延时 (ms)	性能对比
translog异步	1	168554	324747	277	193%
	2	118957	317801	534	267%
	4	71125	326974	744	460%
translog同步	1	118500	242234	193	204%
	2	81681	246673	339	302%
	4	47886	239752	555	500%



说明:

- 以上测试过程中，在不同场景下分别调整了副本数，测试对原生ES 6.7.0和阿里云ES 6.7.0写入性能的影响。本测试过程中主shard的改变对写入性能没有影响，故在测试过程中没有体现主shard。
- 以上测试通过index.translog.durability参数，设置translog同步和异步请求状态，详情请参见官方[Translog](#)

性能测试结论

- 单副本情况下，阿里云增强版ES在16核配置下，相对原生提升了126%。8核配置下，相对原生提升93%。
- 阿里云增强版ES相比原生，在8核和16核下的性能提升，随副本数成线性提升。
- 阿里云增强版ES增加副本的的开销非常小，在纯写入场景下的主备延迟均小于1s。

2 实例列表

阿里云Elasticsearch（简称ES）的实例列表中展示了实例的基本信息，并提供了创建实例、一键报警、刷新实例状态以及管理实例等功能入口。

ES实例创建完成后，系统直接返回实例列表页面。实例列表页面展示了您账号下当前区域的所有ES实例，并提供了以下操作功能。

- 查看实例的列表信息

包括实例ID/名称、状态、版本、数据节点数、规格、可用区、付费类型、网络类型和创建时间。

- 查看实例的基本信息

单击实例ID/名称链接，在基本信息页面查看实例的基本信息，详情请参见[基本信息概览](#)。

- 创建实例

单击创建，可在购买页面创建实例，详情请参见[#unique_6](#)。

- 一键报警

单击一键报警，可跳转至云监控控制台上开启ES的一键报警功能（默认为关闭）。开启后，云监控会创建集群状态异常、节点磁盘使用率异常（>75%），节点JVM Heap异常（>85%）等报警规则，作用于主账号下全部Elasticsearch实例，详情请参见[#unique_7](#)。

- 刷新实例

单击刷新，可获取实例的实时状态。实例创建后，默认为生效中状态，可单击刷新查看实例的最新状态，当状态变为正常时，即可正常使用实例。

- 管理实例

单击右侧操作栏下的管理，可在实例管理页面进行集群升配、日志查询、安全配置、插件配置等操作，详情请参见[实例管理](#)。

- 转包年包月

单击右侧操作栏下的  > 转包年包月，可在确认订单页面，变更付费类型，详情请参

见[#unique_9](#)。

- 变更配置

单击右侧操作栏下的  > 变更配置，可在变配页面，修改集群的配置，详情请参见[集群升配](#)。

- 释放实例



警告:

实例释放后，数据将不可恢复，请谨慎操作。

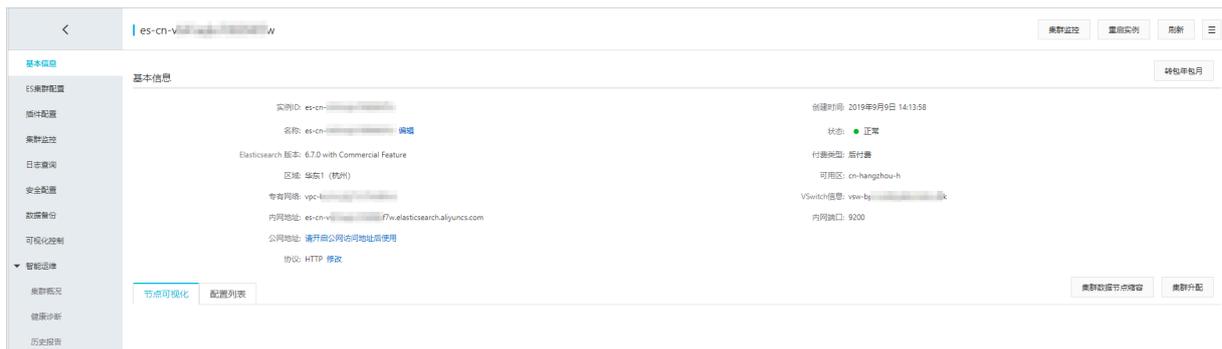
单击右侧操作栏下的  > 释放实例，在释放实例页面确认后，即可释放实例。

3 实例管理

阿里云Elasticsearch（简称ES）的实例管理模块，提供了集群监控、重启实例、刷新实例、任务列表等功能。

进入实例管理页面

ES实例创建成功后，在[实例列表](#)页面单击实例名称/ID链接，进入实例管理页面。



重启实例

当您修改了集群的配置或进行其他操作时，可能需要重启阿里云ES实例才能生效。

前提条件

在重启阿里云ES实例前，您需要确保实例的状态为正常（显示为绿色）、索引至少包含1个副本、资源使用率不是很高（可在[集群告警](#)页面查看，例如节点CPU使用率为80%左右或以下，节点HeapMemory使用率为50%左右，节点load_1m低于当前数据节点的CPU核数）。

1. [进入实例管理页面](#)，单击右上角的重启实例。
2. 在重启实例弹出框中选择重启方式。

阿里云ES支持重启和强制重启两种重启实例的方式。

· 重启

阿里云ES实例在重启过程中可持续提供服务（需要首先满足以上[前提条件](#)），但耗时较长。



注意:

- 在进行重启前，请确保实例的状态为正常（显示为绿色），否则需要进行[强制重启](#)。
- 节点在重启期间，对应的CPU和内存使用率会存在临时突增的情况，您的服务可能会出现抖动，正常情况下过一段时间后会恢复正常。

- 目前阿里云Elasticsearch实例重启耗时与实例的数据总量、节点数量、总索引数量和分片数量等因素有关，暂无法预估具体的耗时长短。您可以在任务列表中查看实例的重启进度。

- 强制重启

强制重启操作可能会导致阿里云Elasticsearch实例在重启阶段的服务不稳定，但耗时较短。

 **注意:**

当磁盘的使用率超过85%时，阿里云Elasticsearch实例的状态可能显示为非健康状态（黄色/红色），此时将不支持重启操作，需要进行强制重启。

- 如果创建的阿里云Elasticsearch实例处于非健康状态（黄色/红色），此时不建议对实例进行节点扩容、磁盘扩容、重启、修改密码或其他变更配置类的操作，请务必保证集群状态变为绿色后再进行这些操作。
- 当您的阿里云Elasticsearch实例包括了两个及两个以上节点，在上述情况下进行变更配置时，如果集群一直处于生效中的状态，您可以[提交工单](#)，联系阿里云Elasticsearch技术工程师处理。

3. 单击确认开始重启实例。

重启过程中，实例状态显示为生效中（黄色），可在任务列表中查看实例变更详情。重启成功后，实例状态显示为正常（绿色）。



刷新实例

当控制台中实例的信息没有及时更新时，例如刚创建完成的阿里云Elasticsearch（简称ES）实例状态显示失败，可以通过刷新功能，手动刷新页面中的状态信息。

[进入实例管理页面](#)，单击右上角的刷新。刷新成功后，实例信息显示正常。如果依然存在异常信息，请联系阿里云Elasticsearch技术工程师处理。

查看任务进度详情

您可以通过任务列表查看正在进行中的任务信息，例如实例的创建进度和重启进度。

1. [进入实例管理页面](#)，单击右上角的任务列表（）图标。

2. 在任务列表页面中，查看实例变更进度。

3. 单击展开详情，查看各任务的进度详情。



集群监控

阿里云Elasticsearch实例已支持对实例进行监控，并允许通过短信的方式报警。

[进入实例管理页面](#)，单击右上角的集群监控，在云监控控制台中根据需求自定义报警阈值，详情请参见[Elasticsearch云监控报警](#)。

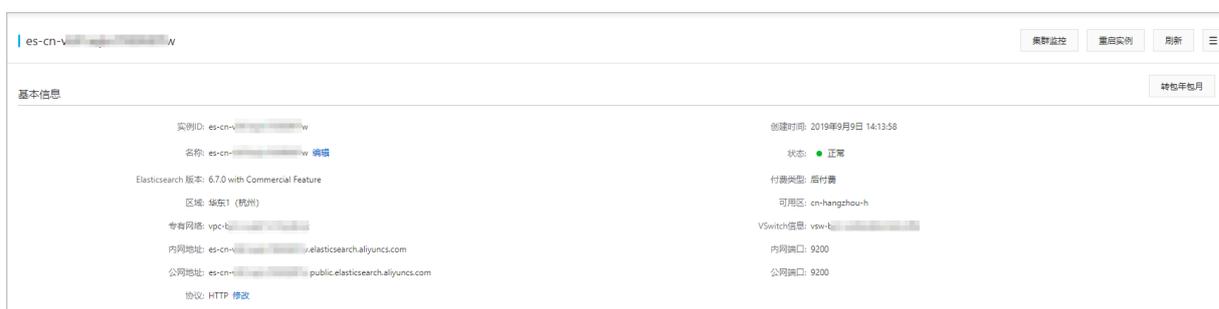
4 基本信息

4.1 基本信息概览

本文档为您介绍阿里云Elasticsearch（简称ES）实例的基本信息页面的相关内容。

登录[阿里云Elasticsearch控制台](#)，在实例列表页面，单击实例ID/名称，直接进入实例的基本信息页面。

在实例的基本信息页面，您可以查看实例基本信息。



名称	描述
实例ID	阿里云ES实例的ID，实例的唯一标识。
名称	阿里云ES实例的名称默认与实例ID相同，支持自定义实例名称，也支持按照名称搜索实例。
Elasticsearch 版本	支持5.5.3、6.3.2和6.7.0版本。不支持各版本之间的平滑升级，需要通过新建实例后迁移数据，详情请参见 #unique_16 。
区域	实例所在的区域。
专有网络	实例所属的专有网络（VPC）。
内网地址	支持在专有网络（VPC）下，通过指定内网地址访问阿里云ES实例服务，依赖阿里云ECS实例。 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> 注意： 通过公网访问阿里云ES实例的安全性较差。如果您对访问环境的安全性有要求，可以购买一个与阿里云Elasticsearch实例在同一VPC下的ECS实例，通过专有网络（VPC）指定内网地址来访问阿里云ES实例。 </div>
公网地址	支持在公网环境下，通过指定公网地址访问阿里云ES实例。需要在 安全配置 页面进行开启。

名称	描述
公网端口	<p>需要开启公网地址后才显示。主要支持的端口如下。</p> <ul style="list-style-type: none"> 支持9200端口，基于HTTP/HTTPS。 支持9300端口，基于TCP。主要支持阿里云Elasticsearch 5.5.3 with Commercial Feature版本。 <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> 说明:</p> <ul style="list-style-type: none"> 阿里云ES 6.3.2和阿里云ES 6.7.0版本不支持通过Transport Client访问9300端口。 需要添加公网地址访问白名单，默认禁止所有地址访问。 </div>
协议	默认使用HTTP协议，您可以单击修改进行切换。目前支持HTTP和HTTPS协议之间的切换，详情请参见 使用HTTPS协议 。
创建时间	实例创建的时间。
状态	实例的状态。支持正常（绿色）、生效中（黄色）、和失效（灰色）。
付费类型	支持预付费（包年包月）和后付费（按量付费）类型。
可用区	实例所在的可用区。
VSwitch信息	实例所属的交换机。
内网端口	<p>主要支持的端口如下。</p> <ul style="list-style-type: none"> 9200端口，基于HTTP/HTTPS。 9300端口，基于TCP。主要支持阿里云ES 5.5.3版本。 <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> 说明:</p> <p>阿里云ES 6.3.2和阿里云ES 6.7.0版本不支持通过Transport Client访问9300端口。</p> </div>
续费	<p>仅当付费类型为预付费时显示。</p> <p>单击基本信息右侧的续费，对实例进行续费。续费以月为单位，至少续费1个月。</p>

名称	描述
转包年包月	<p>仅当付费类型为后付费时显示。</p> <p>单击基本信息右侧的转包年包月，按照界面提示进行开通。通过转包年包月功能，您可以将ES实例的付费类型由后付费（按量付费）转为预付费（包年包月），转换时不支持折扣优惠。</p>

4.2 节点可视化

阿里云Elasticsearch（简称ES）实例的节点可视化页面，可视化地展示了ES集群中的节点信息。

在实例的基本信息页面，单击下方节点可视化。在节点可视化页面，您可以完成以下操作。

- 将鼠标移到集群节点上，在弹出框中可查看集群状态。单击智能运维可跳转到智能运维模块，引导您开通智能运维功能或对集群进行诊断。



- 根据颜色判断集群各节点的健康状态。

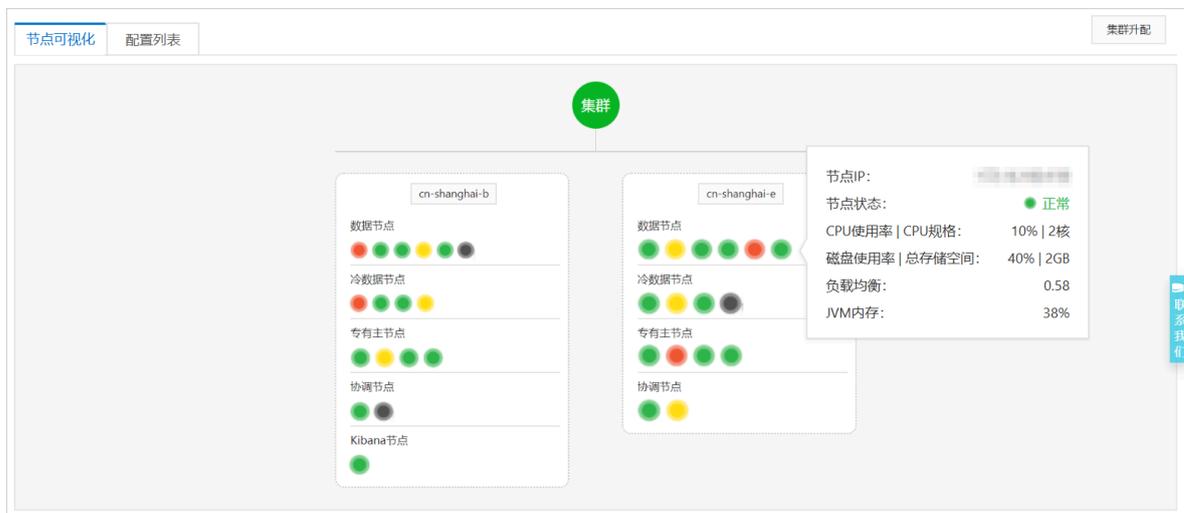


说明:

系统按照节点的使用阈值区分颜色, 与云监控的指标一致。

- 红色: 警告状态。
- 黄色: 预警状态。
- 绿色: 正常状态。
- 灰色: 未知状态 (长时间未获取到信息)。

- 查看节点的信息，包括节点IP，节点状态，CPU使用率 | CPU规格，磁盘使用率 | 总存储空间，负载均衡、JVM内存。



当节点状态为红色、黄色或灰色时，系统会提示节点失联或节点状态不佳，建议使用智能运维诊断。可单击智能运维诊断，跳转到智能运维 > 健康诊断页面，对集群进行诊断。



4.3 配置列表

阿里云Elasticsearch（简称ES）实例的配置列表展示了ES实例的配置信息，例如数据节点规格和数量、Kibana节点规格和数量等。

在基本信息页面，单击下方的配置列表，可查看阿里云ES实例的配置信息。

节点可视化	配置列表
数据节点规格: elasticsearch.n4.small(1核 2G)	数据节点数量: 3
存储规格: SSD云盘	存储容量: 20 GiB
冷数据节点规格: elasticsearch.sn2ne.large(2核 8G)	冷数据节点数: 2
冷数据节点存储类型: 高效云盘	冷数据节点存储空间: 500 GiB
专有主节点规格: elasticsearch.sn2ne.large(2核 8G)	专有主节点数: 3
专有主节点存储类型: SSD云盘	专有主节点存储空间: 20 GiB
协调节点规格: elasticsearch.sn2ne.large(2核 8G)	协调节点数: 2
协调节点存储类型: 高效云盘	协调节点存储空间: 20 GiB
Kibana节点规格: elasticsearch.n4.small(1核 2G)	Kibana节点数: 1

相关参数说明请参见#unique_20。

4.4 集群数据节点缩容

通过阿里云Elasticsearch（简称ES）的数据节点缩容功能，可以完成数据节点数量的变更。

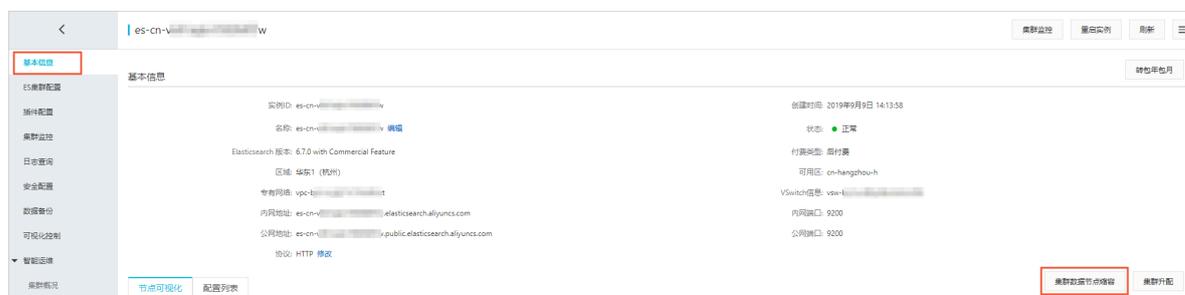


注意：

- 集群数据节点缩容功能目前适用于后付费和单可用区部署的阿里云Elasticsearch（简称ES）实例，暂不支持预付费和跨可用区部署的阿里云ES实例。并且只支持数据节点数量的变更，不支持专有主节点、协调节点、Kibana节点等类型的节点规格和磁盘缩容。
- 集群数据节点缩容会触发集群重启，为保证您的业务不受影响，请确认后操作。

数据节点缩容

1. 登录[阿里云Elasticsearch控制台](#)。
2. 在实例列表页面，单击列表中的实例ID/名称链接。
3. 在实例的基本信息页面，单击集群数据节点缩容。



4. 在集群数据节点缩容页面的缩容配置模块中，选择节点类型，并在节点列表中单击选择需要缩容的数据节点。

缩容配置

请选择节点类型：

当前节点个数：13

缩节点个数：

<input checked="" type="checkbox"/> 192.168.100.100	<input checked="" type="checkbox"/> 192.168.100.101	<input checked="" type="checkbox"/> 192.168.100.102	<input checked="" type="checkbox"/> 192.168.100.103	<input type="checkbox"/> 192.168.100.104
<input type="checkbox"/> 192.168.100.105	<input type="checkbox"/> 192.168.100.106	<input type="checkbox"/> 192.168.100.107	<input type="checkbox"/> 192.168.100.108	<input type="checkbox"/> 192.168.100.109
<input type="checkbox"/> 192.168.100.110	<input type="checkbox"/> 192.168.100.111	<input type="checkbox"/> 192.168.100.112		

5. (可选) 数据迁移。

为保证数据的安全，进行缩容的数据节点中不应该存在数据。如果所选数据节点中有数据，系统会提示您进行数据迁移。迁移后所选节点上不再有任何索引数据，新的索引数据也不会被写入该节点。

a. 单击提示栏中的数据迁移辅助工具。



b. 在集群数据节点迁移页面，选择节点迁移方式。

· 系统建议

通过系统建议自动选择需要缩容的数据节点，需要勾选同意数据迁移协议。



· 自定义

手动选择需要缩容的数据节点。

集群数据节点迁移

迁移节点类型：冷数据节点

迁移节点个数：

系统建议 自定义

提示：慎重自定义方式选择迁移数据节点，可能会影响集群健康状况。

192.168.1.100 192.168.1.101 192.168.1.102 192.168.1.103

我同意《[阿里云Elasticsearch数据迁移服务协议](#)》，授权阿里云Elasticsearch服务协助迁移目标数据节点中的数据。

c. 勾选同意数据迁移协议，并单击确认。

6. 数据迁移完成后，单击确定。

确定后，会触发集群重启。重启时，可在[任务列表](#)页面查看缩容任务的进度，重启成功后，即可完成集群数据节点的缩容。



说明:

数据迁移过程中，可以在任务列表页面单击停止，停止迁移任务。



迁移回滚

数据迁移是一个周期很长的过程，在此期间集群状态和数据的变更可能会导致迁移失败，具体可在[任务列表](#)中查看。当数据迁移失败或者迁移完成后，需要对迁移节点进行回滚时，可通过以下方式进行操作。

1. 获取迁移的节点IP列表。

可以在[任务列表](#)查找，或者在[Kibana控制台](#)的Console中，使用以下ES API命令查找。

```
// 获取集群配置信息。  
GET _cluster/settings
```

返回结果如下。

```
{  
  "transient": {  
    "cluster": {  
      "routing": {  
        "allocation": {  
          "exclude": {  
            "_ip": "192.168.***.***,192.168.***.***,192.168.***.***"  
          }  
        }  
      }  
    }  
  }  
}
```

```
}
```

2. 回滚迁移节点数据。

在Kibana控制台的Console中，使用以下命令进行数据回滚。

- 回滚部分节点数据，配置中去掉需要回滚的节点，但要保留不回滚的节点。

```
PUT _cluster/settings
{
  "transient": {
    "cluster": {
      "routing": {
        "allocation": {
          "exclude": {
            "_ip": "192.168.***.***,192.168.***.***"
          }
        }
      }
    }
  }
}
```

- 回滚全部节点数据。

```
PUT _cluster/settings
{
  "transient": {
    "cluster": {
      "routing": {
        "allocation": {
          "exclude": {
            "_ip": null
          }
        }
      }
    }
  }
}
```

3. 校验是否完成数据回滚。

在Kibana控制台的Console中，通过GET _cluster/settings进行IP地址的二次确认，判断回滚任务的完成情况。您也可以通过观察相应节点是否被重新分配shard来判断。



说明:

数据迁移或回滚时，均可以通过GET _cat/shards?v查看任务状态。

常见问题

- 该操作会导致当前集群资源（disk/cpu/mem）不足或shard分配异常。

原因：集群在迁移或者缩容后，磁盘、内存、CPU等资源不足，不足以承担当前系统数据或者负载。

解决方案：使用GET `_cat/indices?v`查看集群中索引的副本数是否超出缩容后的节点数，检查磁盘等资源是否可以在安全阈值内承担当前的数据量和请求量。如果不满足要求，需要进行[集群升配](#)。

- 集群当前状态异常或有未完成任务，请稍后再试。

解决方案：使用GET `_cluster/health`查看集群健康状况，或者在智能运维中查看集群异常原因。

- 集群节点有数据，请先执行迁移。

解决方案：进行数据迁移操作，详情请参见[数据节点缩容](#)章节的第六步。

- 保留节点数需大于2且大于当前节点数一半。

原因：为保证集群的可靠性，保留的节点数必须大于2；为保证集群的稳定性，每次迁移或者缩容节点数不得超过当前数据节点数的一半。

解决方案：如果不满足以上要求，需要重新选择迁移的节点或者进行[集群升配](#)。

- 当前ES集群配置不支持该操作，请检查ES配置。

解决方案：使用GET `_cluster/settings`查看集群配置，查看是否存在不允许数据分配的配置。

- `auto_expand_replicas`

原因：部分用户使用了X-Pack提供的权限管理功能，在早期版本中，该功能对应的`.security`或者`.security-6`索引默认会使用`"index.auto_expand_replicas" : "0-all"`，该配置会使得数据迁移或者节点缩容失败。

解决方案：当您使用`auto_expand_replicas`索引时，建议参考以下方式修改。

1. 查看索引配置。

```
GET .security/_settings
```

返回如下结果。

```
{
  ".security-6" : {
    "settings" : {
      "index" : {
        "number_of_shards" : "1",
```

```
"auto_expand_replicas" : "0-all",
"provided_name" : ".security-6",
"format" : "6",
"creation_date" : "1555142250367",
"priority" : "1000",
"number_of_replicas" : "9",
"uuid" : "9t2hotc7S50pPuKEIJ****",
"version" : {
  "created" : "6070099"
}
}
}
}
```

2. 选择其中一种方式修改配置。

```
//方式一
PUT .security/_settings
{
  "index" : {
    "auto_expand_replicas" : "0-1"
  }
}
```

```
//方式二
PUT .security/_settings
{
  "index" : {
    "auto_expand_replicas" : "false",
    "number_of_replicas" : "1"
  }
}
```



注意:

副本个数可以根据实际需要选择，但要保证至少有1个，且不大于可用数据节点数。

4.5 集群升配

本文档为您介绍阿里云Elasticsearch（简称ES）集群升配的相关说明、注意事项和操作方法。



注意:

目前阿里云ES不支持5.5.3、6.3.2和6.7.0三个版本间的平滑升降级，需要通过新建实例后迁移数据，详情请参见[#unique_16](#)。

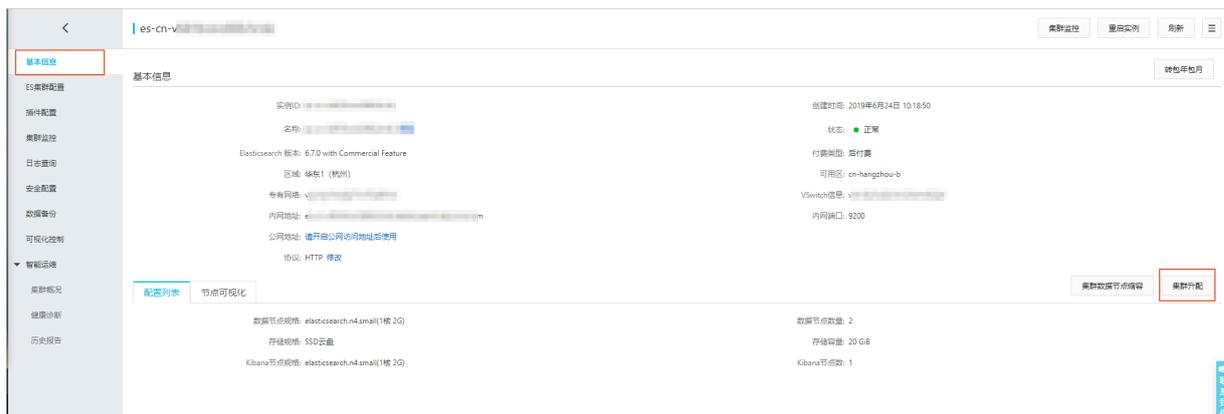
阿里云ES主要支持按照实例规格、节点数量、专有主节点规格、协调节点数、协调节点规格、冷数据节点数量、冷数据节点规格、冷数据节点存储空间及单节点存储空间等进行升级配置。



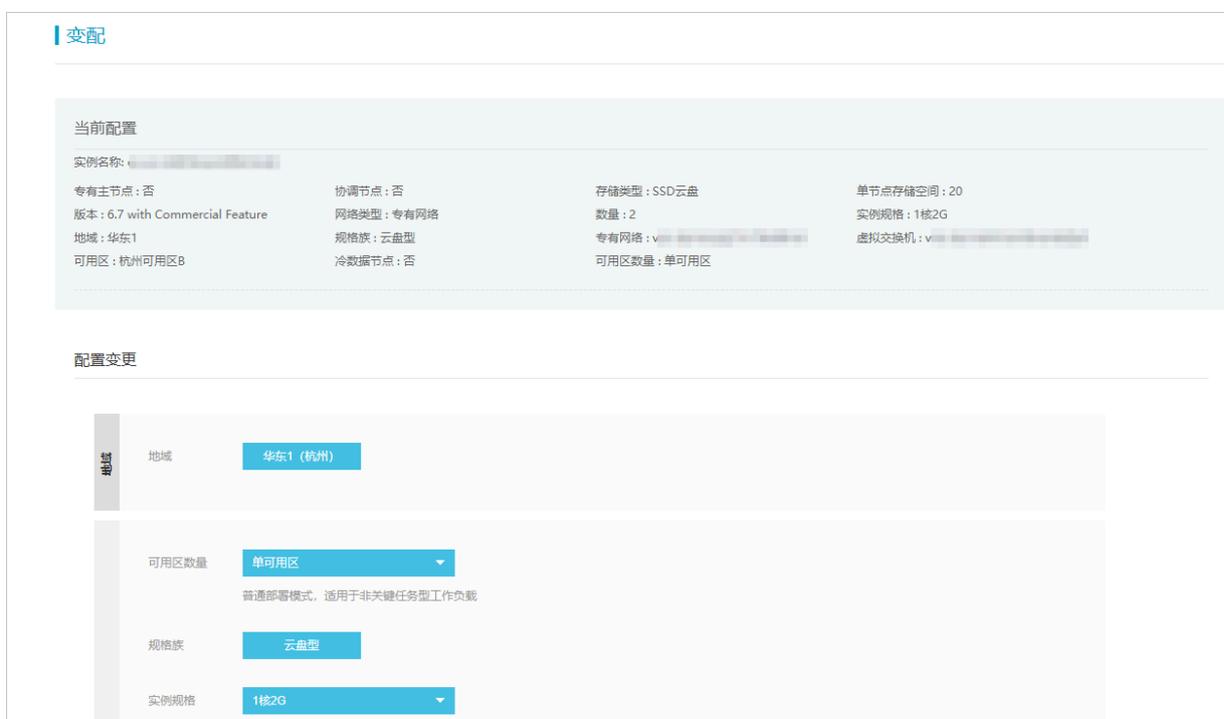
说明:

以上个别属性可能会受到关联条件限制而无法扩容，详情请参见下文的[配置变更](#)。

登录阿里云Elasticsearch控制台，单击实例ID > 基本信息 > 集群升配，进入实例的变配页面。



变配页面包括了当前配置和配置变更模块，相关说明请参见下文的当前配置和配置变更。



当前配置

当前配置模块展示了当前阿里云Elasticsearch实例的相关配置信息，便于您在进行升配操作时做参考。



注意事项

在进行变更配置操作前，您需要认真阅读以下注意事项。

- 如果您的业务有变更需求，请先进行评估后再进行变更。
- 每次变更操作只支持更新集群的其中一个**可变更的属性**。
- 一般情况下，升配操作会重启阿里云Elasticsearch实例。但是如果您已经购买过专有主节点，那么在变更节点数量的操作时不会重启阿里云Elasticsearch实例。
- 如果您的阿里云Elasticsearch实例的状态为非健康状态（黄色/红色），在进行变更操作时需要勾选强制变更，忽略集群健康状态，此操作可能会影响服务。
- 变更操作不支持更改节点的存储类型，但可以修改节点存储空间的大小。
- 阿里云Elasticsearch支持Kibana节点规格的升配，在进行升配时需要收费。
- 预付费类型的阿里云Elasticsearch实例暂不支持降配（例如减少节点个数、减少磁盘大小、减少节点规格）。
- 后付费类型的阿里云Elasticsearch实例目前降配功能只支持数据节点个数的变更（通过集群数据节点缩容实现，会有限制），暂不支持其它类型的降配（例如减少磁盘大小、减少节点规格）。
- 在变更配置的过程中，您可以在变配页面中实时观察更新后的订单消费金额。
- 当您提交了变更配置的订单后，阿里云Elasticsearch实例将按照更新后的订单计费。

配置变更



注意：

在进行变更配置操作前，请首先认真阅读上文的**注意事项**。

请根据实际业务需求，参考页面中的提示修改实例的配置。参数详情请参见[#unique_20](#)。

配置变更

地域	华东1 (杭州)
可用区数量	单可用区 <small>普通部署模式，适用于非关键任务型工作负载</small>
规格族	云盘型
实例规格	1核2G <small>1核2G规格只适合测试，不适用于生产环境，不在SLA售后保障范围内</small>
数量	3 <small>两个节点集群有脑裂风险，谨慎选择</small>
专有主节点	<input checked="" type="checkbox"/> 是
专有主节点数	3(默认)
专有主节点规格	2核8G
专有主节点存储类型	SSD云盘
专有主节点存储空间	20G
协调节点	<input checked="" type="checkbox"/> 是
协调节点数	2
协调节点规格	2核8G
协调节点存储类型	高效云盘
协调节点存储空间	20G
冷数据节点	<input checked="" type="checkbox"/> 是
冷数据节点数量	2
冷数据节点规格	2核8G
冷数据节点存储类型	高效云盘 <small>高效云盘最大存储空间支持5T，提供较为低廉的存储能力，适合大规模数据量的日志及分析场景 2.5TB以上的高效云盘通过磁盘阵列及RAID 0的方式提供服务，不支持扩容</small>
冷数据节点存储空间	500 <small>高效云盘扩容时最大支持扩容到2T，新购时最大支持5120Gib(5T)，超过2048Gib时，只能取：2560、3072、3584、4096、4608、5120</small>
Kibana节点	<input checked="" type="checkbox"/> 是
Kibana规格	2核4G
强制变更	<input type="checkbox"/> 强制变更，忽略集群健康状态
单节点存储空间	20 <small>单位为Gib，SSD云盘最大存储空间支持2048Gib(2T) 高效云盘扩容时最大支持扩容到2T，新购时最大支持5120Gib(5T)，超过2048Gib时，只能取：2560、3072、3584、4096、4608、5120</small>

一次升配变更资源过多，目前只能更新以下属性中的一个（各类节点的节点数量,存储空间,规格）或者没有某类节点的时候购买该节点

《阿里云Elasticsearch (按量付费) 服务协议》

部分参数说明如下。

参数	说明
规格簇/实例规格	规格簇不支持变更。如果规格簇为本地盘类型，则不支持实例规格的变更。
专有主节点	<p>在变配页面单击专有主节点右侧的是，可购买专有主节点。支持升配已购买的专有主节点的规格，默认为3个专有主节点，2核8G，云盘型存储类型，20GB存储空间。配置变更后，系统将按照新规格的定价进行重新计费。</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p> 说明： 如果您已经购买了1核2G规格的专有主节点，可在变配页面重新购买更高规格的专有主节点，系统将按照新规格的定价进行重新计费。如果之前的专有主节点是系统为您赠送的，变更后该专有主节点将变为计费模式。</p> </div>
协调节点	在变配页面单击协调节点右侧的是，可购买协调节点。支持升配已购买的协调节点的规格，默认为2个协调节点，2核8G，云盘型存储类型，20GB存储空间。配置变更后，系统将按照新规格的定价进行重新计费。
冷数据节点	在变配页面单击冷数据节点右侧的是，可购买冷数据节点。支持升配已购买的冷数据节点的规格，默认为2个冷数据节点，2核8G，云盘型存储类型，500GB存储空间。配置变更后，系统将按照新规格的定价进行重新计费。
Kibana节点	<p>在变配页面单击Kibana节点右侧的是，可购买Kibana节点。支持升配已购买的Kibana节点的规格，默认为2核4G。</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p> 注意： 当您购买了阿里云Elasticsearch实例后，系统默认会为您赠送一个1核2G的Kibana节点。您可以通过集群升配操作变更Kibana节点的规格，规格变更后，系统将按照新规格的定价进行计费。</p> </div>

参数	说明
强制变更	<p>如果您的阿里云Elasticsearch实例状态为非健康状态（红色/黄色），且您的服务已受到严重影响，急需扩容解决。此时可以勾选强制变更选项，忽略阿里云Elasticsearch的实例健康状态进行强制变更，耗时相对较短。</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p> 注意:</p> <ul style="list-style-type: none"> · 强制变更操作会重启阿里云Elasticsearch实例。 · 强制变更操作可能会导致阿里云Elasticsearch实例服务在重启阶段不稳定。 · 不勾选强制变更时，系统默认使用重启的方式进行集群升配，相关注意事项请参考#unique_8/unique_8_Connect_42_section_p5n_ccm_zgb。 · 如果您的阿里云Elasticsearch实例状态为非健康状态（红色/黄色），系统会自动勾选强制变更，将不支持通过重启方式进行集群升配。 </div>
存储	<p>单位为Gib，SSD云盘最大支持2048Gib（2T）的空间。</p> <p>高效云盘扩容时最大支持扩容到2T，新购时最大支持5120Gib（5T）。超过2048Gib时，只能取2560、3072、3584、4096、4608、5120。</p>

5 ES集群配置

5.1 ES集群配置概述

通过阿里云Elasticsearch的集群配置功能，您可以自定义分词配置、垃圾回收器配置以及YML文件配置。

进入ES集群配置页面

1. 登录[阿里云Elasticsearch控制台](#)。
2. 在实例列表页面，单击实例ID/名称。
3. 在实例管理页面，单击左侧导航栏的ES集群配置，进入ES集群配置页面。

在ES集群配置页面，您可以进行[同义词配置](#)、[高级配置](#)（垃圾回收器配置）和[YML文件配置](#)。

5.2 同义词配置

阿里云Elasticsearch（简称ES）的分词配置模块提供了同义词配置功能，通过同义词配置，您可以上传自定义的同义词词典文件，作用于ES的同义词库。新的索引将会采用更新后的词库进行搜索。

注意事项

- 阿里云Elasticsearch上传同义词词典操作不会重启节点，后台会进行同义词词典的下发，生效时间与节点数量相关。
- 假设现存索引index-aliyun使用了aliyun.txt同义词文件，当aliyun.txt文件内容变更并重新上传后，现存索引不会动态加载更新后的同义词词典。建议您在词典文件内容发生变化后进行索引重建操作，否则可能会造成只有新增数据使用新词典的情况。
- 同义词词典文件配置要求每行一个同义词表达式，保存为utf-8编码的.txt文件。例如：

```
西红柿,番茄 => 西红柿,番茄  
土豆,马铃薯 => 土豆,马铃薯
```

同义词配置说明

您可以使用filter过滤器配置同义词，示例代码如下。

```
PUT /test_index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
```

```

        "synonym" : {
          "tokenizer" : "whitespace",
          "filter" : ["synonym"]
        }
      },
      "filter" : {
        "synonym" : {
          "type" : "synonym",
          "synonyms_path" : "analysis/synonym.txt"
        },
        "tokenizer" : "whitespace"
      }
    }
  }
}

```

- **filter**: 配置一个synonym (同义词) 过滤器, 其中包含一个路径analysis/synonym.txt (路径是相对于config的位置)。
- **tokenizer**: 用于控制标记同义词的分词器, 默认为whitespace分词器, 其他设置有:
 - **ignore_case**: 默认值为false。
 - **expand**: 默认值为true。

目前同义词分词器支持Solr和WordNet两种同义词格式。

- Solr同义词

文件的示例格式如下。

```

# Blank lines and lines starting with pound are comments.
# Explicit mappings match any token sequence on the LHS of "=>"
# and replace with all alternatives on the RHS.  These types of
mappings
# ignore the expand parameter in the schema.
# Examples:
i-pod, i pod => ipod,
sea biscuit, sea biscit => seabiscuit
# Equivalent synonyms may be separated with commas and give
# no explicit mapping.  In this case the mapping behavior will
# be taken from the expand parameter in the schema.  This allows
# the same synonym file to be used in different synonym handling
strategies.
# Examples:
ipod, i-pod, i pod
foozball , foosball
universe , cosmos
lol, laughing out loud
# If expand==true, "ipod, i-pod, i pod" is equivalent
# to the explicit mapping:
ipod, i-pod, i pod => ipod, i-pod, i pod
# If expand==false, "ipod, i-pod, i pod" is equivalent
# to the explicit mapping:
ipod, i-pod, i pod => ipod

```

```
# Multiple synonym mapping entries are merged.
foo => foo bar
foo => baz
# is equivalent to
foo => foo bar, baz
```

您也可以在配置文件中直接给过滤器定义同义词（请注意使用`synonyms`而不是`synonyms_path`），示例如下。

```
PUT /test_index
{
  "settings": {
    "index": {
      "analysis": {
        "filter": {
          "synonym": {
            "type": "synonym",
            "synonyms": [
              "i-pod, i pod => ipod",
              "begin, start"
            ]
          }
        }
      }
    }
  }
}
```



说明:

建议您使用`synonyms_path`在文件中定义大型同义词集，因为使用`synonyms`定义会增加集群大小。

- WordNet同义词

示例格式声明如下。

```
PUT /test_index
{
  "settings": {
    "index": {
      "analysis": {
        "filter": {
          "synonym": {
            "type": "synonym",
            "format": "wordnet",
            "synonyms": [
              "s(100000001,1,'abstain',v,1,0).",
              "s(100000001,2,'refrain',v,1,0).",
              "s(100000001,3,'desist',v,1,0)."
            ]
          }
        }
      }
    }
  }
}
```

```
}
```

以上示例使用synonyms定义WordNet同义词，您也可以使用synonyms_path在文本中定义WordNet同义词。

同义词配置步骤

1. 在阿里云ES控制台上传同义词词典文件，保存并生效成功。
2. 在创建索引配置 setting时，配置 "synonyms_path": "analysis/your_dict_name.txt"，再为该索引配置 mapping，指定字段设置同义词。
3. 校验同义词，并上传测试数据进行搜索测试。

使用示例一

以下示例使用filter过滤器配置同义词，操作步骤如下。

1. 在ES集群配置页面，单击分词配置右侧的同义词配置。
2. 在同义词配置页面，单击上传文件，选择您要上传的同义词词典（按照同义词配置说明中的规则生成的txt文件），单击保存。
3. 等待阿里云Elasticsearch实例生效并提示状态正常后即可使用。

本示例中使用aliyun_synonyms.txt作为测试文件，内容为begin, start。



4. 配置并测试同义词。

a. 登录Kibana控制台。

b. 在Console中执行如下命令，创建索引。

```
PUT /aliyun-index-test
{
  "index": {
    "analysis": {
      "analyzer": {
        "by_smart": {
          "type": "custom",
          "tokenizer": "ik_smart",
          "filter": ["by_tfr","by_sfr"],
          "char_filter": ["by_cfr"]
        },
        "by_max_word": {
          "type": "custom",
          "tokenizer": "ik_max_word",
          "filter": ["by_tfr","by_sfr"],
          "char_filter": ["by_cfr"]
        }
      },
      "filter": {
        "by_tfr": {
          "type": "stop",
          "stopwords": [" "]
        },
        "by_sfr": {
          "type": "synonym",
          "synonyms_path": "analysis/aliyun_synonyms.txt"
        }
      },
      "char_filter": {
        "by_cfr": {
          "type": "mapping",
          "mappings": ["| => |"]
        }
      }
    }
  }
}
```

c. 执行以下命令，配置同义词字段title。

```
PUT /aliyun-index-test/_mapping/doc
{
  "properties": {
    "title": {
      "type": "text",
      "analyzer": "by_max_word",
      "search_analyzer": "by_smart"
    }
  }
}
```

d. 执行以下命令，校验同义词。

```
GET /aliyun-index-test/_analyze
{
```

```
"analyzer": "by_smart",
"text": "begin"
}
```

命令执行成功后，返回结果如下。

```
{
  "tokens": [
    {
      "token": "begin",
      "start_offset": 0,
      "end_offset": 5,
      "type": "ENGLISH",
      "position": 0
    },
    {
      "token": "start",
      "start_offset": 0,
      "end_offset": 5,
      "type": "SYNONYM",
      "position": 0
    }
  ]
}
```

e. 执行以下命令，添加数据，进行下一步测试。

```
PUT /aliyun-index-test/doc/1
{
  "title": "Shall I begin?"
}
```

```
PUT /aliyun-index-test/doc/2
{
  "title": "I start work at nine."
}
```

f. 执行以下命令，测试查询。

```
GET /aliyun-index-test/_search
{
  "query": { "match": { "title": "begin" } },
  "highlight": {
    "pre_tags": ["<red>", "<bule>"],
    "post_tags": ["</red>", "</bule>"],
    "fields": {
      "title": {}
    }
  }
}
```

命令执行成功后，返回结果如下。

```
{
  "took": 11,
  "timed_out": false,
  "_shards": {
    "total": 5,
    "successful": 5,
    "failed": 0
  }
}
```

```
},
"hits": {
  "total": 2,
  "max_score": 0.41048482,
  "hits": [
    {
      "_index": "aliyun-index-test",
      "_type": "doc",
      "_id": "2",
      "_score": 0.41048482,
      "_source": {
        "title": "I start work at nine."
      },
      "highlight": {
        "title": [
          "I <red>start</red> work at nine."
        ]
      }
    },
    {
      "_index": "aliyun-index-test",
      "_type": "doc",
      "_id": "1",
      "_score": 0.39556286,
      "_source": {
        "title": "Shall I begin?"
      },
      "highlight": {
        "title": [
          "Shall I <red>begin</red>?"
        ]
      }
    }
  ]
}
}
```

使用示例二

以下示例直接引用同义词并使用IK过滤，操作步骤如下。

1. 登录Kibana控制台，在Console中执行如下命令。

```
PUT /my_index
{
  "settings": {
    "analysis": {
      "analyzer": {
        "my_synonyms": {
          "filter": [
            "lowercase",
            "my_synonym_filter"
          ],
          "tokenizer": "ik_smart"
        }
      },
      "filter": {
        "my_synonym_filter": {
          "synonyms": [
            "begin,start"
          ],
          "type": "synonym"
        }
      }
    }
  }
}
```

```
    }
  }
}
```

以上命令的原理为：

- a. 设置一个同义词过滤器`my_synonym_filter`，并配置同义词词库。
- b. 设置一个`my_synonyms`解释器，使用`ik_smart`分词。
- c. 经过`ik_smart`分词，把所有字母小写并作同义语查找。

2. 执行以下命令，设置同义词字段`title`。

```
PUT /my_index/_mapping/doc
{
  "properties": {
    "title": {
      "type": "text",
      "analyzer": "my_synonyms"
    }
  }
}
```

3. 执行以下命令，校验同义词。

```
GET /my_index/_analyze
{
  "analyzer": "my_synonyms",
  "text": "Shall I begin?"
}
```

命令执行成功后，返回数据如下。

```
{
  "tokens": [
    {
      "token": "shall",
      "start_offset": 0,
      "end_offset": 5,
      "type": "ENGLISH",
      "position": 0
    },
    {
      "token": "i",
      "start_offset": 6,
      "end_offset": 7,
      "type": "ENGLISH",
      "position": 1
    },
    {
      "token": "begin",
      "start_offset": 8,
      "end_offset": 13,
      "type": "ENGLISH",
      "position": 2
    },
    {
      "token": "start",
```

```
    "start_offset": 8,
    "end_offset": 13,
    "type": "SYNONYM",
    "position": 2
  }
]
}
```

4. 执行以下命令，添加数据，进行下一步测试。

```
PUT /my_index/doc/1
{
  "title": "Shall I begin?"
}
```

```
PUT /my_index/doc/2
{
  "title": "I start work at nine."
}
```

5. 执行以下命令，测试查询。

```
GET /my_index/_search
{
  "query" : { "match" : { "title" : "begin" }},
  "highlight" : {
    "pre_tags" : ["<red>", "<bule>"],
    "post_tags" : ["</red>", "</bule>"],
    "fields" : {
      "title" : {}
    }
  }
}
```

命令执行成功后，返回数据如下。

```
{
  "took": 11,
  "timed_out": false,
  "_shards": {
    "total": 5,
    "successful": 5,
    "failed": 0
  },
  "hits": {
    "total": 2,
    "max_score": 0.41913947,
    "hits": [
      {
        "_index": "my_index",
        "_type": "doc",
        "_id": "2",
        "_score": 0.41913947,
        "_source": {
          "title": "I start work at nine."
        },
        "highlight": {
          "title": [
            "I <red>start</red> work at nine."
          ]
        }
      }
    ]
  }
}
```

```
    },
    {
      "_index": "my_index",
      "_type": "doc",
      "_id": "1",
      "_score": 0.39556286,
      "_source": {
        "title": "Shall I begin?"
      },
      "highlight": {
        "title": [
          "Shall I <red>begin</red>?"
        ]
      }
    }
  ]
}
```

本文档部分内容参考了官方Elasticsearch文档，详情请参见[Synonym Token Filter](#)和[Using Synonyms](#)

。

5.3 高级配置

阿里云Elasticsearch（简称ES）6.7.0及以上版本的实例（要求规格大于等于32GB）提供了垃圾回收器的配置功能，支持CMS垃圾回收器和G1垃圾回收器的相互切换。

注意事项

- 垃圾回收器配置完成后，需要进行集群重启才能生效，请确认后操作。
- 只有6.7.0及以上版本的阿里云Elasticsearch实例才可以修改垃圾回收类型，5.5.3和6.3.x版本不支持修改。
- 6.7.0及以上版本的Elasticsearch实例，如果数据规格的内存大于等于32GB，支持CMS和G1垃圾回收器的相互切换，小于32GB只能使用CMS垃圾回收器。

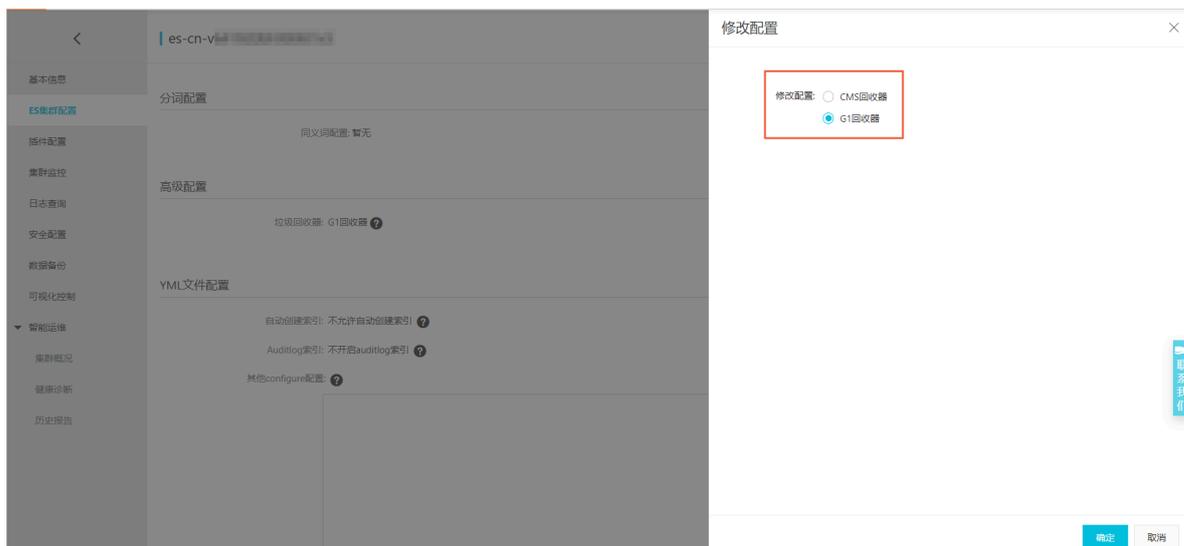
规格族	<input checked="" type="radio"/> 云盘型	<input type="radio"/> 本地SSD盘型	<input type="radio"/> 本地SATA盘型
实例规格	<input checked="" type="text" value="8核32G"/> ▼		
	1核2G规格只适合测试，不适用于生产环境，不在SLA售后保障范围内		
数量	<input type="text" value="3"/>	▲ ▼	

操作步骤

1. 在阿里云Elasticsearch实例的**ES集群配置**页面，单击高级配置右侧的修改配置。

 **警告：**
以下步骤会触发集群自动重启，请确认后操作。

2. 在修改配置页面，选择G1回收器，单击确定。



确定后，集群会自动重启。重启成功后，即可完成垃圾回收器的切换。

5.4 YML文件配置

通过阿里云Elasticsearch（简称ES）的YML文件配置功能，您可以自定义阿里云ES实例的配置。

操作步骤

 **警告：**
修改YML文件配置后，需要通过重启阿里云ES实例生效，为保证您的业务不受影响，请确认后操作。

1. 在**ES集群配置**页面，单击YML文件配置右侧的修改配置。

2. 在YML参数配置页面，按照以下说明进行配置。

YML参数配置
✕

自动创建索引: 不允许自动创建索引 ?

允许自动创建索引

自定义

删除索引指定名称: 删除时明确索引名称 ?

删除时索引名称支持通配符

Auditlog索引: 不开启auditlog索引 ?

开启auditlog索引

开启Watcher: 关闭 ?

开启

其他configure配置: ?

1

! 该操作会重启实例，请确认后操作。

联系我们

- **自动创建索引**：当阿里云ES实例在接收到新文档后，如果没有对应索引，是否允许系统自动新建索引。自动创建的索引可能不符合您的预期，不建议开启。
- **删除索引指定名称**：在删除索引时是否需要明确指定索引名称，如果选择删除时索引名称支持通配符，则可以使用通配符进行批量删除索引。索引删除后不可恢复，请谨慎使用此配置。

- **Auditlog索引**：开启后，系统会记录阿里云ES实例对应的增、删、改、查等操作产生的索引日志，该日志信息会占用您的磁盘空间，同时也会影响性能，不建议开启，请谨慎使用此配置。
- **开启Watcher**：开启后，可使用X-Pack的Watcher功能，请注意定时清理`.watcher-history*`索引，避免占用大量磁盘空间。
- **其他configure配置**：支持部分配置项如下，详情请参见[自定义CORS访问（跨域）](#)、[自定义远程索引重建（白名单）](#)、[自定义Auditlog](#)、[自定义queue大小](#)和[参数调优](#)。

**说明：**

以下配置项，如果没有标识具体适用于哪个ES版本，默认兼容ES 5.5.3和6.3.2版本。

- `http.cors.enabled`
- `http.cors.allow-origin`
- `http.cors.max-age`
- `http.cors.allow-methods`
- `http.cors.allow-headers`
- `http.cors.allow-credentials`
- `reindex.remote.whitelist`
- `action.auto_create_index`
- `action.destructive_requires_name`
- `thread_pool.bulk.queue_size`（只适用于Elasticsearch 5.5.3 with X-Pack版本）
- `thread_pool.write.queue_size`（只适用于Elasticsearch 6.3.2 with X-Pack版本）
- `thread_pool.search.queue_size`

3. 滑动到页面底部，勾选该操作会重启实例，请确认后操作，单击确认。

确认后，ES实例会进行重启，可在[任务列表](#)中查看进度。重启成功后即可完成YML文件的配置。

自定义CORS访问（跨域）

**注意：**

- 以下表格中的配置信息是阿里云ES为支持HTTP协议开放的自定义配置。
- 以下表格中的字段配置仅支持静态配置。如果您想使配置生效，请将配置信息写入`elasticsearch.yml`文件中。
- 以下配置依赖于集群网络设定（[Network settings](#)）。

配置项	描述
<p>http.cors.enabled</p>	<p>跨域资源共享配置项，即配置ES是否允许其他域资源下的浏览器向其发送请求。可设置为true或false。</p> <ul style="list-style-type: none"> • 设置为true，表示启用跨域资源访问。即可使ES处理OPTIONS CORS请求。如果发送请求中的域信息已在http.cors.allow-origin中声明，那么ES会在头信息中附加Access-Control-Allow-Origin以响应跨域请求。 • 设置为false（默认），表示禁止跨域资源访问。即可使ES忽略请求头中的域信息，ES将不会以Access-Control-Allow-Origin信息头应答，以达到禁用CORS目的。如果客户端不支持发送附加域信息头的pre-flight请求，或者不校验从服务端返回的报文的头信息中的Access-Control-Allow-Origin信息，那么跨域安全访问将受到影响。如果ES关闭CORS支持，则客户端只能尝试通过发送OPTIONS请求，以了解此响应信息是否存在。
<p>http.cors.allow-origin</p>	<p>域资源配置项，可设置接受来自哪些域名的请求。默认不允许且无配置。</p> <p>如果在该配置值前后添加/，则此配置信息会被识别为正则表达式。允许您使用正则方式兼容支持HTTP和HTTPs的域请求信息。例如/https?:\\/\\$/localhost(:[0-9]+)?/，表示可响应符合此正则的请求信息。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> 说明: *被认定为合法配置，可被识别为使集群支持来自任意域名的跨域请求，这将给ES集群带来安全风险，不建议使用。</p> </div>
<p>http.cors.max-age</p>	<p>浏览器可发送OPTIONS请求以获取CORS配置信息，此配置项可设置获取的信息在浏览器中的缓存时间，默认为1728000秒（20天）。</p>

配置项	描述
http.cors.allow-methods	请求方法配置项，默认为OPTIONS, HEAD, GET, POST, PUT, DELETE。
http.cors.allow-headers	请求头信息配置项，默认为X-Requested-With, Content-Type, Content-Length。
http.cors.allow-credentials	凭证信息配置项目，即是否允许响应头中返回Access-Control-Allow-Credentials信息。默认为false，表示不允许返回此信息。设置为true表示允许返回此信息。

自定义跨域访问配置示例如下。

```
http.cors.enabled: true
http.cors.allow-origin: "*"
http.cors.allow-headers: "X-Requested-With, Content-Type, Content-Length, Authorization"
```

如果需要了解更多设置，请参见ES官方文档，查看[HTTP](#)相关信息。

自定义远程索引重建（白名单）

索引重建组件支持用户在远程的ES集群中重建数据索引，适用于您所能找到的任意版本的远程ES服务。

您可以使用自定义远程索引重建功能，将旧版本的ES服务中的数据索引到当前发布版本中。使用示例如下，详情请参见[Reindex API](#)。

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "http://otherhost:9200",
      "username": "user",
      "password": "pass"
    },
    "index": "source",
    "query": {
      "match": {
        "test": "data"
      }
    }
  },
  "dest": {
    "index": "dest"
  }
}
```

```
}
```

- **host**: 远程主机的地址，必须包含支持协议、域名和端口等信息，例如`https://otherhost:9200`。

**注意:**

远程主机地址需要在`elasticsearch.yml`中使用`reindex.remote.whitelist`属性进行声明，才可以在远程使用此API功能。允许以`host`和`port`组合，并使用逗号分隔多个主机配置（例如`otherhost:9200, another:9200, 127.0.10.**:9200, localhost:**`）。白名单不识别协议信息，只使用主机和端口信息用于实现安全策略设定。

- `username`和`password`为可选参数，如果您所请求的远程ES服务需要使用Basic Authentication，请在请求中一并提供此参数信息。通过Basic Authentication鉴权需要使用HTTPS协议，否则密码信息将以文本形式进行传输。

**说明:**

- 如果机器地址信息已在白名单中设定，将不会验证和修改`query`，而是直接发送请求至远端服务。
- 从远端集群索引数据，不支持手动切片或自动切片。详情请参见[手动切片](#)或[自动切片](#)。

批量设定

远端服务使用堆缓存索引数据，默认最大设定值为100（MB）。如果远端索引中包含大文档，请您将批量设定值设置为较小值。

以下示例中，设置批量数值为10。

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "http://otherhost:9200"
    },
    "index": "source",
    "size": 10,
    "query": {
      "match": {
        "test": "data"
      }
    }
  },
  "dest": {
    "index": "dest"
  }
}
```

超时时间

- 使用`socket_timeout`设置socket读取超时时间，默认超时为30s。
- 使用`connect_timeout`设置连接超时时间，默认超时为1s。

以下示例中，设置socket读取超时为1分钟，连接超时为10秒。

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "http://otherhost:9200",
      "socket_timeout": "1m",
      "connect_timeout": "10s"
    },
    "index": "source",
    "query": {
      "match": {
        "test": "data"
      }
    }
  },
  "dest": {
    "index": "dest"
  }
}
```

自定义Auditlog

开启Auditlog索引

阿里云ES实例不支持查看Auditlog的相关log文件，因此如果您想了解阿里云ES实例请求的相关信息（例如`audit_log`），那么需要在控制台中开启阿里云ES实例对应的Auditlog索引功能。



修改生效后，Auditlog将输出到阿里云ES实例中，并且使用`.security_audit_log-*`开头的索引名称。

配置Auditlog索引



注意:

- 您无法实现对Auditlog索引过程中的信息进行过滤。当您的Auditlog事件中包含`request body`信息时，有可能在文本中暴露敏感信息。
- 当您把Auditlog日志计入索引中时，该日志将占用您阿里云ES实例的存储空间。因为阿里云ES不支持自动过期清除策略，需要您手动触发清除陈旧的Auditlog索引。

Auditlog索引配置项如下。

```
xpack.security.audit.index.bulk_size: 5000
xpack.security.audit.index.events.emit_request_body: false
xpack.security.audit.index.events.exclude: run_as_denied,anonymous_
access_denied,realm_authentication_failed,access_denied,connection
_denied
xpack.security.audit.index.events.include: authentication_failed,
access_granted,tampered_request,connection_granted,run_as_granted
xpack.security.audit.index.flush_interval: 180s
xpack.security.audit.index.rollover: hourly
xpack.security.audit.index.settings.index.number_of_replicas: 1
xpack.security.audit.index.settings.index.number_of_shards: 10
```

特性	默认设置	描述
xpack.security.audit.index.bulk_size	1000	控制将多个审核事件，分批处理到一个写入日志中，默认写入事件为1000个。
xpack.security.audit.index.flush_interval	1s	控制缓冲事件刷新到索引的频率。
xpack.security.audit.index.rollover	daily	控制滚动构建到新索引的频率，可以设置为hourly、daily、weekly或者monthly。
xpack.security.audit.index.events.include	access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted	控制何种Auditlog事件可以被计入到索引中。完整列单请参见 Accesslog事件类型
xpack.security.audit.index.events.exclude		构建索引过程中排除的Auditlog事件。
xpack.security.audit.index.events.emit_request_body	false	当触发明确的事件类型（例如authentication_failed），是否忽略或包含以REST发送的请求体。

您也可以对存储Auditlog的索引进行配置，将以xpack.security.audit.index.settings为命名空间，配置在elasticsearch.yml文件中。

以下设置构建Auditlog索引的分片和副本均为1。

```
xpack.security.audit.index.settings:
  index:
    number_of_shards: 1
    number_of_replicas: 1
```



说明:

如果您希望通过传入参数配置生成Auditlog索引，请在开启Auditlog索引的同时传入此配置。当阿里云ES实例完成变更后，Auditlog索引将会出现在您的阿里云ES实例中。否则，阿里云ES实例的Auditlog索引将以默认的`number_of_shards: 5, number_of_replicas: 1`进行设置。

更多详细信息请参见[Auditing Security Settings](#)。

自定义queue大小

可以通过自定义`thread_pool.bulk.queue_size`、`thread_pool.write.queue_size`和`thread_pool.search.queue_size`，分别调整文档写入和搜索queue大小。

以下设置文档写入和搜索queue大小为500，需要您根据实际业务情况自行调整合适参数值。



说明:

以下示例默认兼容阿里云ES 5.5.3和6.3.2版本。

```
thread_pool.bulk.queue_size: 500 (只适用于Elasticsearch 5.5.3 with X-Pack版本)
thread_pool.write.queue_size: 500 (只适用于Elasticsearch 6.3.2 with X-Pack版本)
```

```
thread_pool.search.queue_size: 500
```

参数调优

配置项	描述
index.codec	<p>ES的数据压缩算法默认为LZ4。当您使用高效云盘的warm或cold集群时，通常将该参数设置为best_compression，就可使用更高压缩率的DEFLATE算法。在更改压缩算法后，segment merge时会使用新的压缩算法。</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"><p> 注意： 使用best_compression会导致写性能降低。</p></div>

REST API设置

可以通过REST API设置index.codec参数，示例如下。

```
PUT $index_name/_settings
{
  "index": {
    "codec": "best_compression"
  }
}
```



说明：

- 执行命令前需要先关闭对应索引，否则会报错。
- \$index_name：替换为需要设置的索引名。

5.5 Head插件安装（Chrome）

本文档为您介绍Elasticsearch Head插件的安装方法。通过在Chrome浏览器中安装Head插件，您可以使用阿里云Elasticsearch实例的公网地址来访问集群服务并执行相关操作。

前提条件

通过Chrome浏览器安装Head插件前，请确保您能够访问chrome.google.com域名。

背景信息

- Elasticsearch Head是第三方支持的服务/插件。
- 在公网环境下，Head插件只能通过阿里云Elasticsearch公网地址和端口访问集群服务。

操作步骤

1. 在Chrome浏览器中打开插件安装链接 (<https://chrome.google.com/webstore/detail/elasticsearch-head/ffmkiejjmecolpfloofpjologoblkegm>)，单击添加至 Chrome。



2. 在弹出的确认对话框中，单击添加扩展程序。



系统会自动下载并安装Head插件，安装成功后，系统会弹出安装成功的对话框。



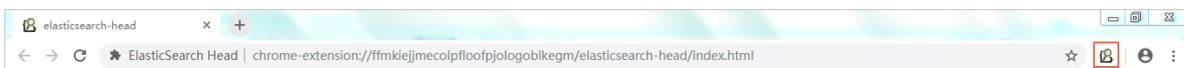
3. 进入**阿里云Elasticsearch控制台**，开启Elasticsearch实例的**公网地址**，然后将待访问Elasticsearch的设备的公网IP配置到**公网地址访问白名单**中。



说明:

- 获取访问设备的公网IP：打开百度首页输入IP，即可在IP地址查询网页链接处获取机器的公网IP。
- 开启阿里云Elasticsearch实例的公网地址后，默认禁止所有IPv4地址的访问。您可以通过配置公网访问白名单，为指定的设备开启访问权限。

4. 单击Chrome浏览器地址栏右侧的**放大镜图标**，进入Elasticsearch集群连接页面。



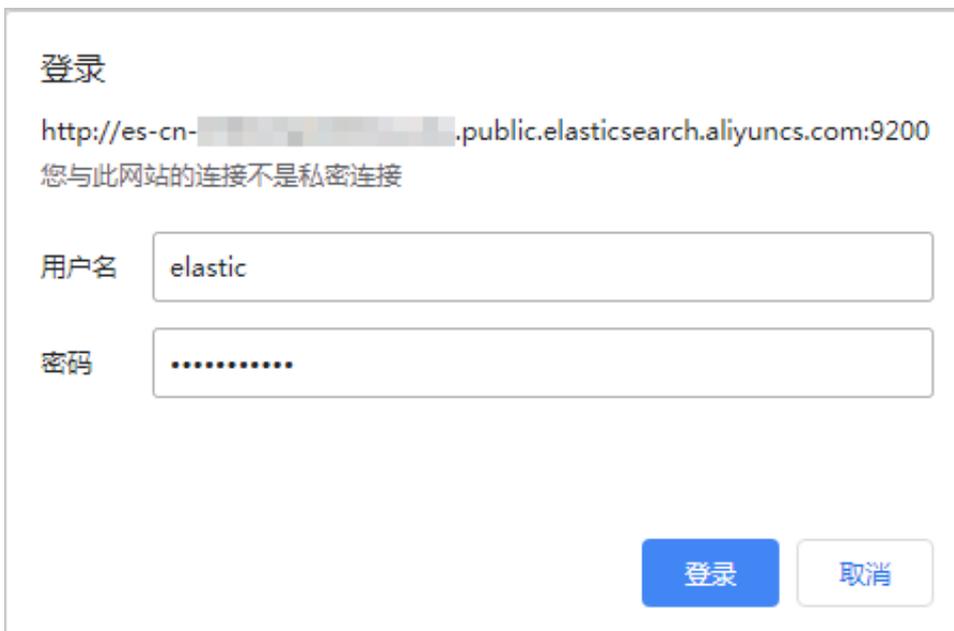
- 5. 在Elasticsearch集群连接页面的地址栏中输入http://<Elasticsearch实例的公网地址>:<端口号>/，单击连接。



您可以在Elasticsearch实例的基本信息页面获取Elasticsearch实例的公网地址和端口号，默认的端口号为9200，示例连接地址如下：

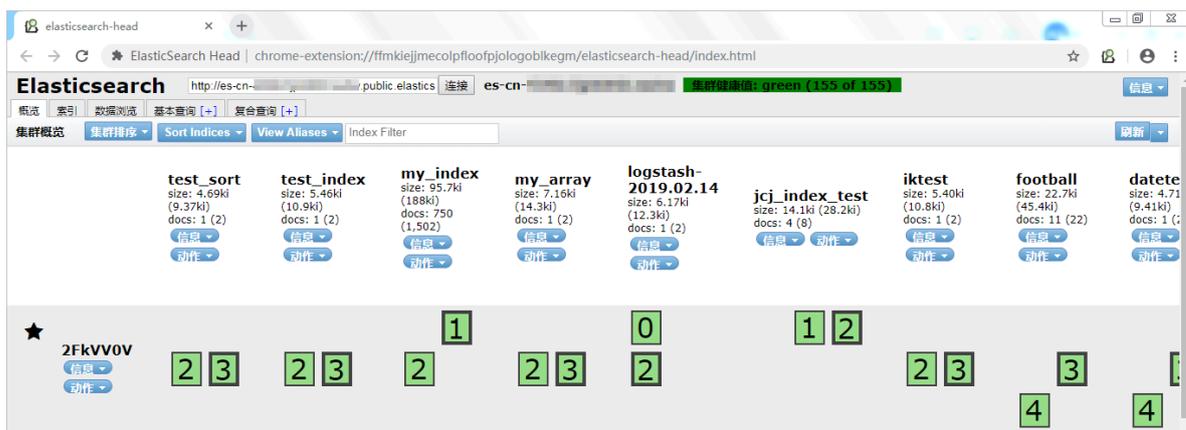
```
http://es-cn-45xxxxxxxxxx01xw6w.public.elasticsearch.aliyuncs.com:9200/
```

- 6. 在弹出的登录对话框中，输入Elasticsearch实例的访问用户名和密码（登录kibana控制台的用户名和密码），单击登录。



说明：
因阿里云Elasticsearch商业版本集成了X-Pack安全访问策略，需要在访问集群服务时输入授权信息。如果没有弹出登录对话框，请先检查阿里云Elasticsearch的公网地址访问白名单中是否包含了对应访问机器的公网IP，或者尝试清除浏览器缓存后重试。

7. 登录成功后，根据您的业务进行相关操作。



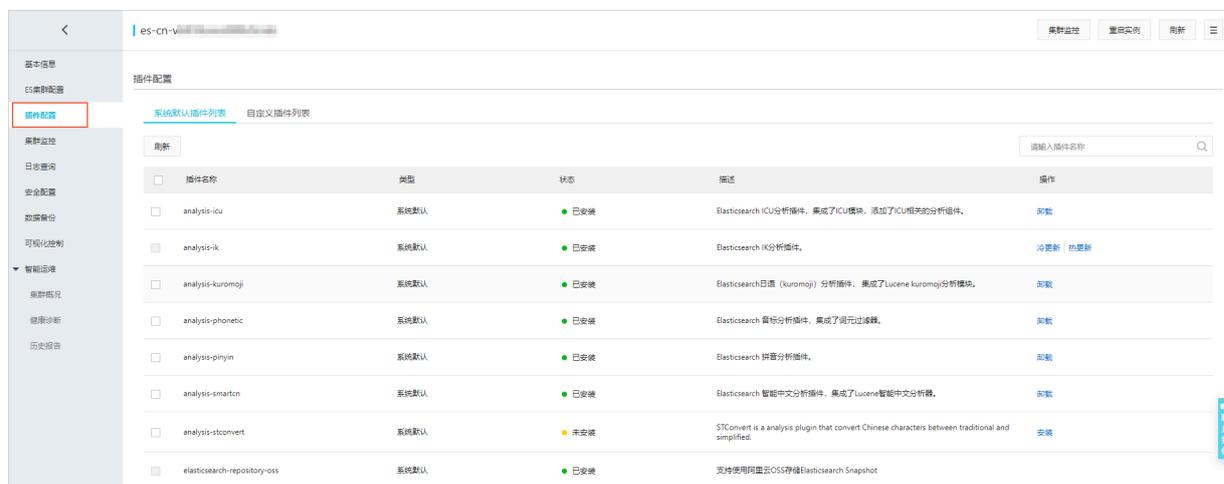
6 插件配置

6.1 插件配置概述

阿里云Elasticsearch在开源社区插件的基础上，提供了丰富的插件，在此基础上又扩展并丰富了部分插件提供给您使用。本章节为您介绍阿里云Elasticsearch的插件配置功能，帮助您快速使用阿里云Elasticsearch提供的插件完成特定的业务需求。

使用插件配置功能

登录[阿里云Elasticsearch控制台](#)，单击实例名称/ID > 插件配置。



在插件配置页面，您可以查看系统默认插件列表和自定义插件列表。

- 系统默认插件列表

系统默认插件列表中的analysis-ik和elasticsearch-repository-oss插件默认不能卸载。analysis-ik插件支持IK词典的冷更新和热更新操作，可以实现自定义扩展词典的更新功能。详情请参见[#unique_32](#)。

- 自定义插件列表

支持自定义标准类型的插件的上传、安装及卸载，以满足您特定场景的需求。详情请参见[自定义插件列表](#)。

6.2 自定义插件列表

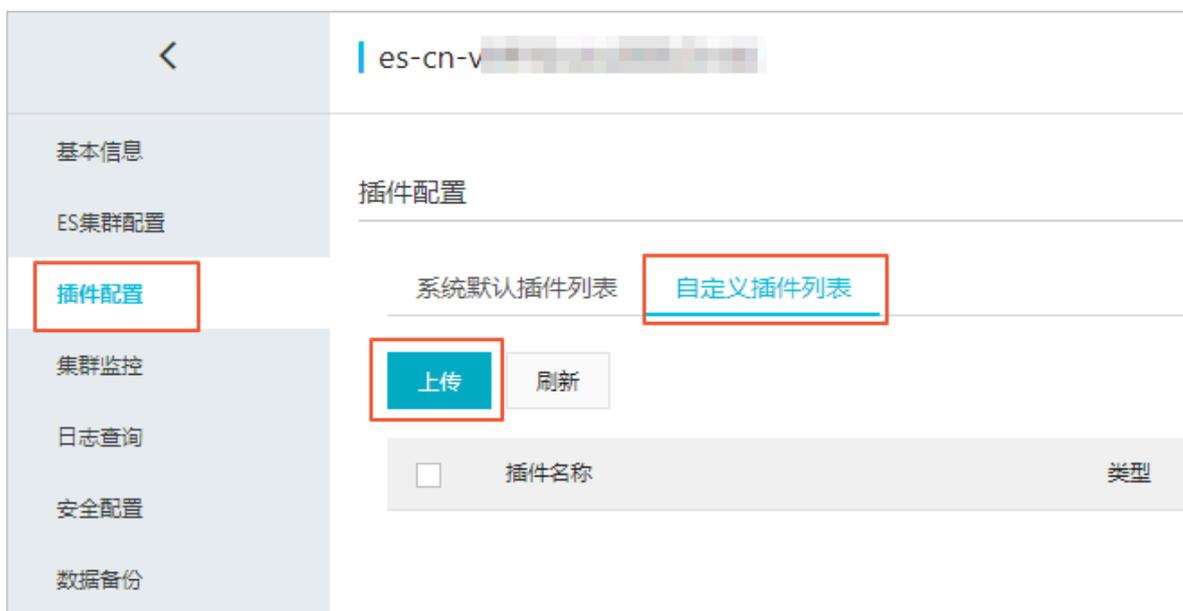
本文档为您介绍阿里云Elasticsearch自定义插件的上传、安装及卸载功能。

上传并安装自定义插件

注意:

- 上传自定义插件会触发Elasticsearch集群重启安装，并且插件本身可能影响Elasticsearch集群的稳定性，请务必保证自定义插件的可用性和安全性。
- Elasticsearch升级时插件不会自动升级更新，需要重新上传。
- 如果您的插件不涉及保密协议，我们也希望您能开源，一起共建和丰富开源社区的插件。

1. 在插件配置页面，单击自定义插件列表 > 上传。



2. 在弹出的插件上传对话框中，单击添加多个文件或将多个文件拖放到此区域，添加您需要上传的自定义插件。



您也可以将自定义的插件文件直接拖放到指定区域，完成添加。如上图成功添加了文件名为elasticsearch-sql-6.7.0.0的自定义插件。



说明:

使用同样的方式可添加多个自定义插件。

3. 仔细阅读并勾选对话框中的注意事项，单击上传安装。



插件的上传安装会触发集群重启。集群重启成功后，如果在自定义插件列表中看到您上传的插件，且状态显示为已安装，表示插件上传并安装成功。



如果您不需要再使用此插件，可单击插件右侧的卸载，卸载此插件。详细操作方法及注意事项请参见[#unique_32](#)。

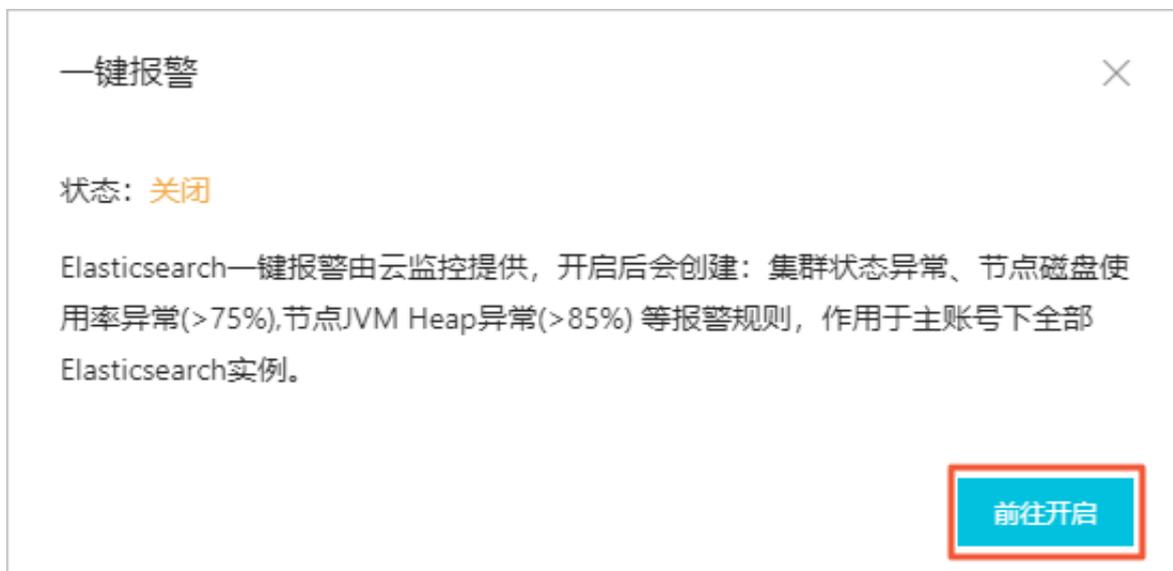
7 集群监控

7.1 集群告警

本文档为您介绍阿里云Elasticsearch的集群告警功能，包括一键报警和自定义报警。

开启一键报警

1. 登录[阿里云Elasticsearch控制台](#)。
2. 在实例列表页面，单击一键报警。
3. 在一键报警对话框中单击前往开启（默认为关闭状态）。



4. 在云监控控制台上，打开Elasticsearch服务的一键报警开关。



5. 开启后，刷新实例，单击实例ID/名称 > 集群监控，在集群告警模块中可以看到一键告警为开启状态。



自定义报警

在ES实例的集群监控页面，单击集群告警模块中的前往云监控配置。在云监控控制台中，可自定义报警规则，详情请参见[#unique_7](#)。

7.2 集群监控

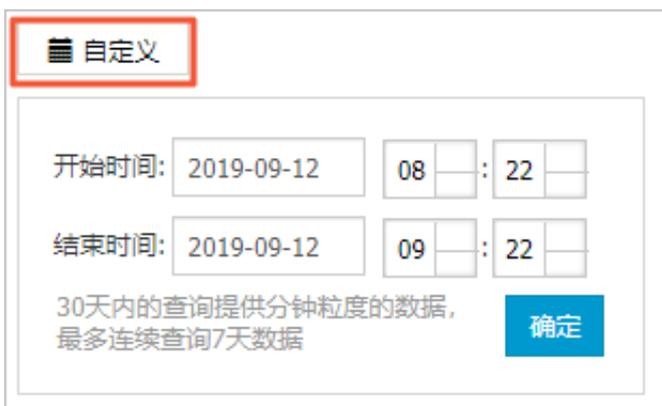
本文档为您介绍查看阿里云Elasticsearch（简称ES）集群监控状态的方法，同时为您提供了各监控指标的详细说明。

查看集群监控状态

1. 登录[阿里云Elasticsearch控制台](#)。
2. 单击实例ID/名称 > 集群监控。
3. 在集群监控页面的集群监控模块，单击监控时段，查看该时段内的监控详情。



4. 单击自定义图标，选择开始时间和结束时间，单击确定，可查看自定义时间段内的监控详情。



自定义

开始时间: 2019-09-12 08 : 22

结束时间: 2019-09-12 09 : 22

30天内的查询提供分钟粒度的数据，最多连续查询7天数据

确定

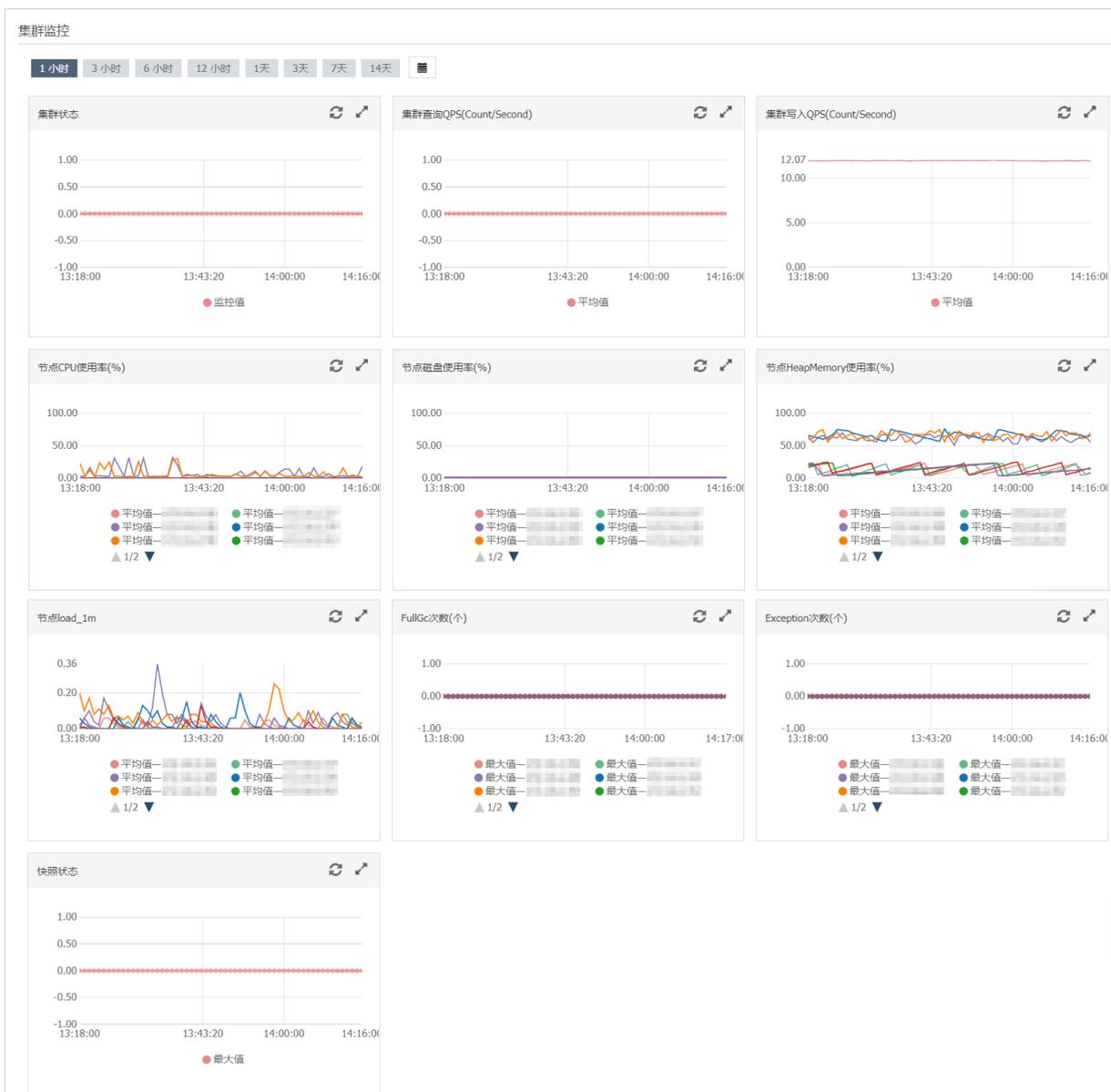


注意:

30天内的查询提供分钟粒度的数据，最多连续查询7天数据。

各监控指标详情请参见[集群监控指标说明](#)。

集群监控指标说明



阿里云ES集群的监控指标包含了**集群状态**、**集群查询QPS (Count/Second)**、**集群写入QPS (Count/Second)**、**节点CPU使用率 (%)**、**节点HeapMemory使用率 (%)**、**节点磁盘使用率 (%)**、**节点load_1m**、**FullGc次数 (个)**、**Exception次数 (个)** 以及**快照状态**。

集群状态

集群状态监控项，展示了对应阿里云ES的集群健康度，数值为0.00时表示正常。必须配置，配置方法请参见[#unique_7/unique_7_Connect_42_section_ffl_q1m_zgb](#)。

当监控项数值不为0（非绿色）时，表示集群状态异常，常见原因如下。

- 监控期间节点的CPU或HeapMemory使用率太高，或者达到100%。
- 监控期间节点的磁盘使用率太高（例如节点磁盘使用率超过85%），或者达到100%。

- 监控期间节点的load_1m负载太高。
- 监控期间ES集群中的索引健康度有出现非健康（非绿色）状态。

各监控项数值含义如下：

数值	颜色	状态	备注
2.00	Red	不是所有的主要分片都可用。	表示该集群中存在不可用的主分片。即某个或者某几个索引存在主分片丢失（unassigned）的情况。
1.00	Yellow	所有主要分片可用，但不是所有复制分片都可用。	表示该集群中某个或者某几个索引存在副本分片丢失（unassigned）的情况。
0.00	Green	所有主要分片和复制分片都可用。	表示集群中所有的索引都很健康，不存在丢失（unassigned）的分片。

集群查询QPS (Count/Second)

 **注意：**
如果查询QPS流量存在较大突增，可能引起CPU或HeapMemory使用率过高或load_1m负载过高，从而影响ES集群服务，业务上需要避免。

集群查询QPS监控项，展示了对应阿里云ES集群每秒执行的查询QPS个数。

查询QPS和需要查询索引的主分片个数有关。例如需要查询的索引有5个主分片，则一次查询请求对应5个QPS。

集群写入QPS (Count/Second)

 **注意：**
如果写入QPS流量存在较大突增，可能引起CPU或HeapMemory使用率过高或load_1m负载过高，从而影响ES集群服务，业务上需要避免。

集群写入QPS监控项，展示了对应阿里云ES集群每秒写入文档的数量。

如果在1秒内，客户端向阿里云ES集群发送1个只包含单个文档的写入请求，则对应1个写入QPS。如果1秒内发送了多个写入请求，则进行累加统计。

如果在1秒内通过_bulk API在一个写入请求中批量写入多个文档，则写入QPS参考该请求中批量推送的总文档个数。如果1秒内发送了多个_bulk API批量写入请求，则进行累加统计。

节点CPU使用率 (%)

节点CPU使用率监控项，展示了ES集群中各节点的CPU使用率百分比，当CPU使用率比较高或接近100%时会影响ES集群服务。

当监控项数值存在突增或波动比较大时，服务异常，常见原因如下。

- 监控期间查询QPS或写入QPS流量存在突增或波动比较大的情况。
- 监控期间存在个别慢查询或慢写入请求。

此情况下，查询和写入QPS流量波动比较小或不明显，可在ES控制台中的日志查询页面，单击searching慢日志进行查看分析。

- 监控期间该ES集群中存在大量索引或总分片数量非常多。

由于ES会监控集群中的索引并写入日志，因此当总索引或总分片个数过多时，容易引起CPU或HeapMemory或load_1m负载过高。

- 监控期间在该ES集群上执行过Merge操作。

Merge操作会消耗CPU资源，对应节点的Segment Count会出现突降，可在Kibana控制台中节点的Overview页面查看。

- 监控期间执行过GC操作。

GC操作会尝试释放内存（例如FULL GC），消耗CPU资源。可能会导致CPU使用率突增。

- 监控期间执行过定时任务，例如数据备份任务或其它自定义的任务。

节点HeapMemory使用率 (%)

节点HeapMemory使用率监控项，展示了对应ES集群中各节点的HeapMemory使用率百分比。当HeapMemory使用率比较高或存在比较大的内存对象时，会影响ES集群服务，也会自动触发GC操作。

当监控项数值存在突增或波动比较大时，服务异常，常见原因如下。

- 监控期间查询QPS或写入QPS流量存在突增或波动比较大的情况。
- 监控期间存在个别慢查询或慢写入请求。

此情况下，查询和写入QPS流量波动比较小或不明显，可在ES控制台中的日志查询页面，单击searching慢日志进行查看分析。

- 监控期间存在大量慢查询或慢写入请求。

此情况下，查询和写入QPS流量波动比较大或很明显，可在ES控制台中的日志查询页面，单击indexing慢日志进行查看分析。

- 监控期间该ES集群中存在大量索引或总分片数量非常多。

由于ES会监控集群中的索引并写入日志，因此当总索引或总分片个数过多时，容易引起CPU或HeapMemory或load_1m负载过高。

- 监控期间在该ES集群上执行过Merge操作。

Merge操作会消耗CPU资源，对应节点的Segment Count会出现突降，可在Kibana控制台中节点的Overview页面查看。

- 监控期间执行过GC操作。

GC操作会尝试释放内存（例如FULL GC），消耗CPU资源。可能会导致HeapMemory使用率突降。

- 监控期间执行过定时任务，例如数据备份任务或其它自定义的任务。

节点磁盘使用率（%）

节点磁盘使用率监控项，展示了对应ES集群中各节点的磁盘使用率百分比，节点磁盘使用率必须控制在85%以下，强烈建议您配置该监控项。否则可能会出现以下情况，影响ES服务。

- 默认数据节点的磁盘使用率超过85%，会导致新的shard无法分配，可能会影响ES服务。
- 默认数据节点的磁盘使用率超过90%，ES会尝试将对应节点中的shard迁移到其它磁盘使用率比较低的数据节点中，可能会影响ES服务。
- 默认数据节点的磁盘使用率超过95%，系统会对ES集群中的每个索引强制设置read_only_allow_delete属性，此时索引将无法写入数据，只能读取和删除对应索引，可能会影响ES服务。



注意：

磁盘使用率报警阈值建议控制在75%以下，不要超过80%。发生报警时，可以提前进行磁盘、节点扩容或清理索引数据等操作，防止影响ES服务。

节点load_1m

节点load_1m监控项，展示了对应ES集群中各节点在1分钟内的负载情况，表示各节点的系统繁忙程度。该监控项的正常数值应该低于当前ES节点规格的CPU核数。

当监控项数值超过当前ES节点规格的CPU核数时，服务异常，常见原因如下。

- 监控期间节点的CPU、HeapMemory使用率高或为100%。
- 监控期间查询QPS或写入QPS流量存在突增或上涨比较大的情况。

- 监控期间存在耗时比较大的慢查询。

可能存在个别慢查询或者大量慢查询，可在ES控制台中的日志查询页面，打开对应日志进行查看分析。

以单核的ES节点为例，监控项数值说明如下。

- Load<1：没有等待的进程。
- Load==1：系统无额外的资源运行更多的进程。
- Load>1：进程拥堵，等待资源。

FullGc次数（个）



警告：

当系统出现频繁FULL GC时，会影响ES集群服务。

FullGc次数监控项，展示了对应ES集群中1分钟内的GC总次数。

当监控项数值不为0时，服务异常，常见原因如下。

- 监控期间HeapMemory使用率比较高。
- 监控期间存在比较大的内存对象。

Exception次数（个）

Exception次数监控项，展示了对应ES集群的主日志中，一分钟内出现的警告级别日志的总个数。

当监控项数值不为0时，服务异常，常见原因如下。

- 监控期间查询请求可能存在异常。
- 监控期间写入请求可能存在异常。
- 监控期间ES执行任务时，可能遇到异常。
- 监控期间执行过GC。



说明：

- 在ES控制台中的日志查询页面，单击主日志。在主日志页面，根据时间点查看详细异常信息，并分析异常原因。
- 如果主日志中有GC记录，也会在Exception次数监控项中进行统计展示。

快照状态

快照状态监控项，展示了对应ES集群控制台中的自动备份功能的快照状态。当监控项数值为-1或0时，表示服务正常。

监控项数值为2时，服务异常，常见原因如下。

- 节点磁盘使用率很高或接近100%。
- ES集群不健康。

监控项的数值含义如下。

- 0：表示有快照。
- -1：表示没有快照。
- 1：表示正在进行快照。
- 2：表示快照任务失败。

8 日志查询

阿里云Elasticsearch（简称ES）提供了主日志、searching慢日志、indexing慢日志、GC日志的查询与展示。通过输入关键字和设置时间范围，可以快速锁定需要查询的日志内容。

阿里云ES最多支持查询7天内的日志，日志默认按时间倒序展示。支持基于Lucene的日志查询语法，详情请参见[Query string syntax](#)。



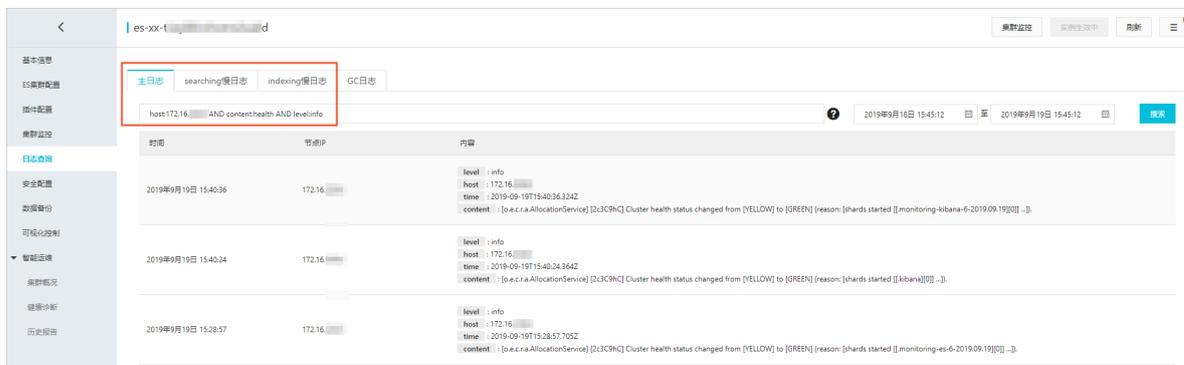
说明：

阿里云ES最大支持返回10000条日志，如果在返回的10000条日志中，未覆盖到您所需要的日志内容，可以通过缩短查询时间范围来获取您需要的日志。

查询样例

本文档以查询content包含关键字health，level为info，host为172.16.xx.xx的ES主日志为例。

1. 进入阿里云ES的实例管理页面。
2. 单击日志查询 > 主日志。
3. 在搜索框中输入查询条件。



本文档的查询条件为：`host:172.16.xx.xx AND content:health AND level:info`



注意：

查询条件中的AND必须为大写。

4. 选择开始时间和结束时间，单击搜索。



注意：

- 如果结束时间为空，那么结束时间默认为当前时间。

· 如果开始时间为空，那么开始时间默认为结束时间减去1小时。

搜索成功后，ES会根据您的查询条件返回日志查询结果，并展示在日志查询页面。日志查询结果主要包括时间、节点IP和内容三部分。

时间	节点IP	内容
2019年9月19日 15:40:36	172.16....	level : info host : 172.16. ... time : 2019-09-19T15:40:36.324Z content : [o.e.c.r.a.AllocationService] [2c3c9hc] Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[monitoring-kibana-6-2019.09.19][0]] ...]).
2019年9月19日 15:40:24	172.16. ...	level : info host : 172.16. ... time : 2019-09-19T15:40:24.364Z content : [o.e.c.r.a.AllocationService] [2c3c9hc] Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[kibana][0]] ...]).
2019年9月19日 15:28:57	172.16. ...	level : info host : 172.16. ... time : 2019-09-19T15:28:57.705Z content : [o.e.c.r.a.AllocationService] [2c3c9hc] Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[monitoring-es-6-2019.09.19][0]] ...]).

- 时间：日志产生时间。
- 节点IP：ES节点的IP地址。
- 内容：主要由level、host、time和content组成。

名称	描述
level	日志级别。包括trace、debug、info、warn、error等（GC日志没有level）。
host	ES节点的IP地址。 <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  说明： 可在Kibana控制台中的Monitoring页面中，单击Elasticsearch模块的Nodes，在节点列表中获取节点IP地址。 </div>
time	日志产生时间。
content	日志主要内容。

9 安全配置

本文档为您介绍阿里云Elasticsearch（简称ES）的安全配置功能，包括访问密码、公网/私网访问白名单以及HTTPS协议等。

进入阿里云ES的实例管理页面，单击左侧导航栏的安全配置，在集群网络设置中完成以下操作。



- 重置ES实例访问密码。
- 配置VPC私网访问白名单。
- 开启公网地址。
- 配置公网地址访问白名单。
- 使用HTTPS协议。

重置ES实例访问密码



注意:

- 密码重置后会影响到您使用elastic管理员账号访问阿里云ES实例，生效后的密码将作为新的管理密码，用来登录Kibana控制台以及访问阿里云ES实例。
- 重置ES实例访问密码不影响其它非elastic管理账号的账号访问该实例，不建议在程序中通过elastic管理账号来访问您的阿里云ES实例。
- 单击重置，密码修改完成并确认提交后，不会触发阿里云ES实例重启。

在ES安全配置页面，单击ES实例访问密码右侧的重置。输入elastic管理员账号的新密码，确认后即可重置您的密码。

重置

您以后每次登录ElasticSearch时都需要输入该信息，请妥善保管

用户名:

密码: 0/30
8-30个字符，且同时包含三项（大写字母，小写字母，数字，特殊字符）

确认密码: 0/30

密码重置后，新密码会在5分钟左右之后生效。

VPC私网访问白名单

当您需要通过内网来访问阿里云Elasticsearch实例时，可将待访问设备的IP加入到阿里云Elasticsearch实例的VPC私网访问白名单中。

单击修改，在VPC白名单输入框中输入您需要添加的IP地址，单击确认即可完成添加。

白名单支持配置为单个IP或IP网段的形式，格式为192.168.0.1或192.168.0.0/24，多个IP之间用英文逗号隔开。127.0.0.1代表禁止所有IPV4地址访问，0.0.0.0/0代表允许所有IPV4地址访问。



说明:

- 默认允许所有内网IPV4地址访问。
- 主要针对内网地址进行访问控制。

公网地址

单击公网地址开关，可开启公网地址。开启后开关显示为绿色，默认显示为灰色，即关闭状态。公网地址开启后，才可使用公网地址访问您的阿里云Elasticsearch实例。

公网地址访问白名单

在配置公网访问白名单前，请首先打开公网地址开关。打开公网地址后，默认禁止所有公网地址访问。

当您需要通过外网来访问阿里云Elasticsearch实例时，可将待访问设备的IP加入到阿里云Elasticsearch实例的公网地址访问白名单中。

白名单支持配置为单个IP或IP网段的形式，格式为192.168.0.1或192.168.0.0/24，多个IP之间用英文逗号隔开。127.0.0.1代表禁止所有IPV4地址访问，0.0.0.0/0代表允许所有IPV4地址访问。

目前杭州区域支持公网IPV6地址访问，并可以配置IPV6白名单，格式为2401:b180:1000:24::5或2401:b180:1000::/48。::1代表禁止所有IPV6地址访问，::/0代表允许所有IPV6地址访问。

使用HTTPS协议

HTTPS全称是Hyper Text Transfer Protocol over Secure Socket Layer，是一种能够保障数据安全的HTTP通道。它是 HTTP 协议的安全版，其保障数据传输安全的方式就是在HTTP协议的基础上增加了SSL（Secure Sockets Layer，安全套接层）。也就是说HTTPS 还是通过HTTP进行通信，只是传输的内容经过了SSL加密。

操作步骤



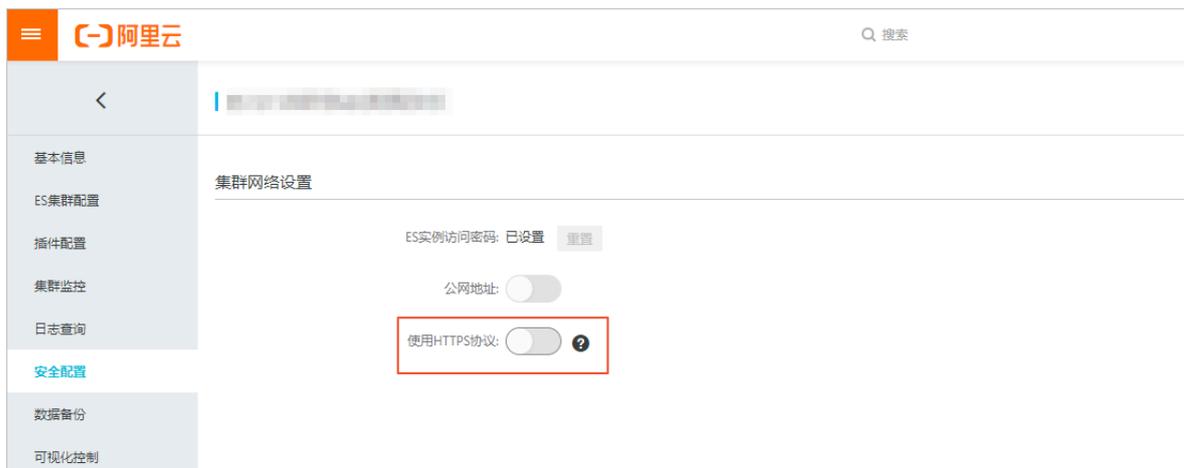
注意:

- 阿里云Elasticsearch支持HTTPS协议的开启和关闭能力，为了保障您数据的安全性，建议开启HTTPS协议。

· 在开启HTTPS协议前，您需要首先购买协调节点。

数量	<input type="text" value="2"/>	两个节点集群有脑裂风险，谨慎选择
专有主节点	<input checked="" type="radio"/> 否	<input type="radio"/> 是
协调节点	<input type="radio"/> 否	<input checked="" type="radio"/> 是
协调节点数	<input type="text" value="2"/>	
协调节点规格	<input type="text" value="2核8G"/>	
协调节点存储类型	<input type="text" value="高效云盘"/>	
协调节点存储空间	<input type="text" value="20G"/>	
冷数据节点	<input checked="" type="radio"/> 否	<input type="radio"/> 是
Kibana节点	<input checked="" type="radio"/> 否	<input type="radio"/> 是

1. 登录[阿里云Elasticsearch控制台](#)，单击实例ID > 安全配置，然后打开使用HTTPS协议开关。



注意:

- 启用HTTPS协议前，您需要首先对访问Elasticsearch的代码进行变更，否则会导致无法使用程序访问您的Elasticsearch实例。变更方式请参见[开启和关闭HTTPS协议代码变更示例](#)。
- 启用和关闭HTTPS服务会中断服务，并且会触发集群重启，为保证您的业务不受影响，请确认后操作。

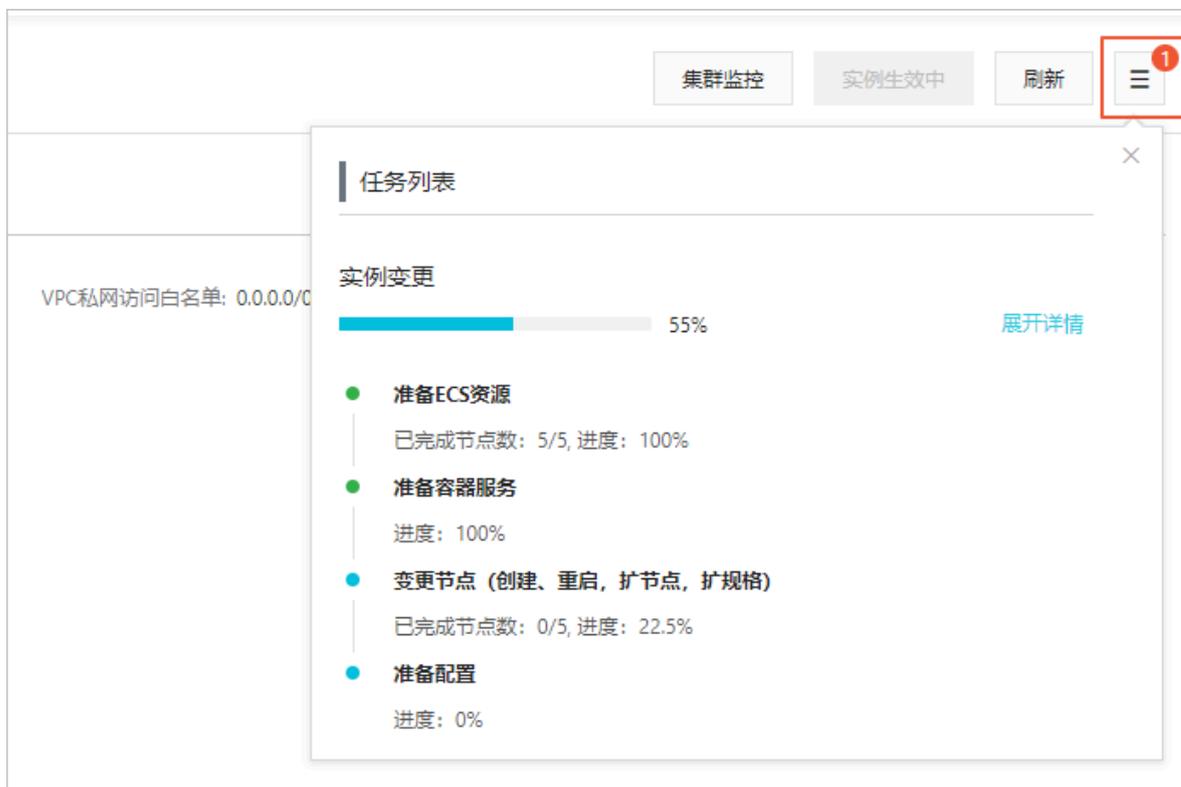
2. 在弹出的操作提示对话框中，勾选确认已经修改访问Elasticsearch实例的代码，单击确认。



说明:

如果您还未购买协调节点，在打开使用HTTPS协议开关后，系统会提示您购买协调节点。您可以按照提示购买协调节点后再进行操作。

确认后集群会进行重启，可单击右上角的图标查看实例变更进度。重启完成后，就可以使用HTTPS协议访问您的实例了。



开启和关闭HTTPS协议代码变更示例

下面以Elasticsearch官方Rest Client访问方式为例，为您介绍在开启HTTPS前后，客户端代码需要做的变更点。

- 开启HTTPS前的示例代码如下。

```
final CredentialsProvider credentialsProvider = new BasicCredentialsProvider();
credentialsProvider.setCredentials(AuthScope.ANY,
    new UsernamePasswordCredentials("elastic", "Your password"));
RestClientBuilder restClientBuilder = RestClient.builder(
    new HttpHost("es-cn-xxxxx.elasticsearch.aliyuncs.com", 9200));
RestClient restClient = restClientBuilder.setHttpClientConfigCallback(
    new RestClientBuilder.HttpClientConfigCallback() {
        @Override
        public HttpAsyncClientBuilder customizeHttpClient(
            HttpAsyncClientBuilder httpClientBuilder) {
            return httpClientBuilder.setDefaultCredentialsProvider(credentialsProvider);
        }
    });
```

```
}).build();
```

- 开启HTTPS后的示例代码如下。

```
final CredentialsProvider credentialsProvider = new BasicCredentialsProvider();
credentialsProvider.setCredentials(AuthScope.ANY,
    new UsernamePasswordCredentials("elastic", "Your password"));
RestClientBuilder restClientBuilder = RestClient.builder(
    new HttpHost("es-cn-xxxxx.elasticsearch.aliyuncs.com",
6200, "https"));
RestClient restClient = restClientBuilder.setHttpClientConfigCallback(
    new RestClientBuilder.HttpClientConfigCallback() {
        @Override
        public HttpAsyncClientBuilder customizeHttpClient(
            HttpAsyncClientBuilder httpClientBuilder) {
            return httpClientBuilder.setDefaultCredentialsProvider(credentialsProvider);
        }
    }).build();
```

由以上示例可知，开启HTTPS后，`HttpHost`中需要加上`https`参数，即`new HttpHost("es-cn-xxxxx.elasticsearch.aliyuncs.com", 6200, "https");`。

配置实例网络互通

提供了跨集群搜索的功能，详情请参见[配置实例网络互通](#)。

10 配置实例网络互通

为了安全性，阿里云Elasticsearch（简称ES）实例间的网络默认是隔离的，若需要使用跨集群搜索功能，则需要将两个实例的网络进行打通。

前提条件

两个ES集群需要满足如下条件才能打通。

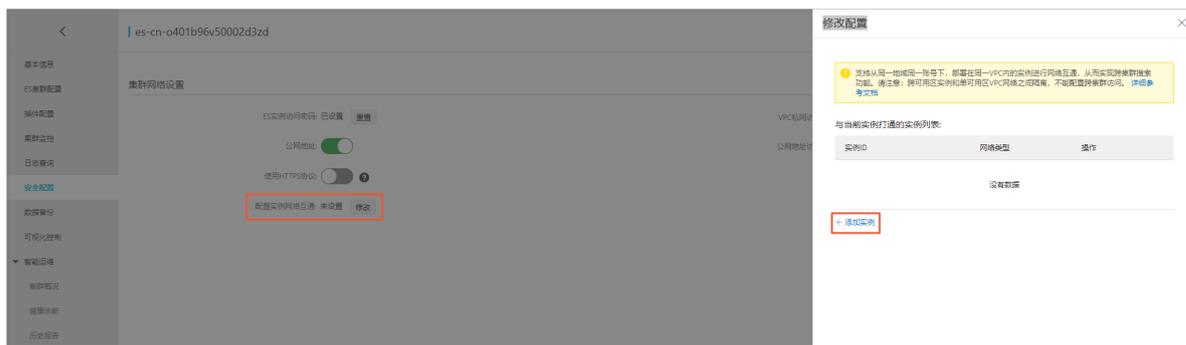
- 相同版本。
- ES集群都归属于当前账号。
- ES集群部署在同一个VPC中。
- 同为单可用区实例，或同为多可用区实例。

背景信息

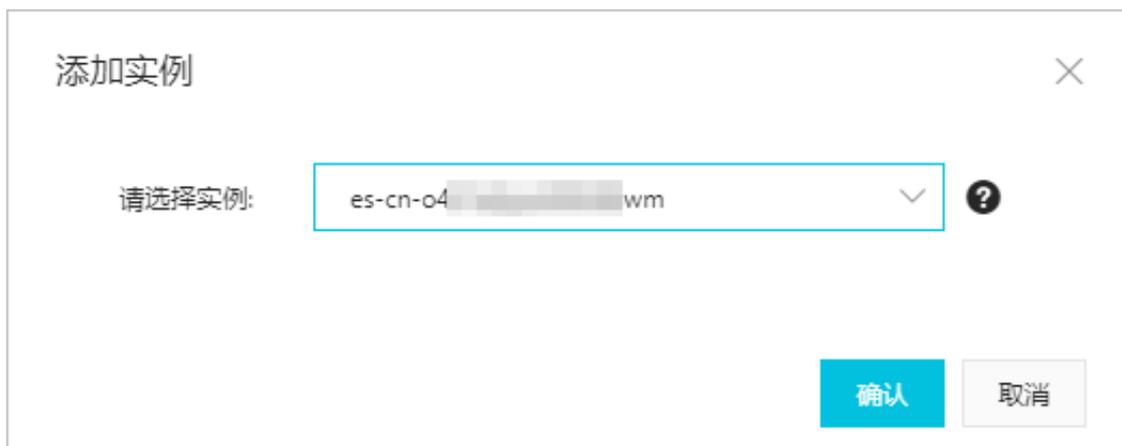
在满足前提条件后，对应各个阿里云ES实例的网络默认是没有打通的，需要您在配置实例网络互通页面进行配置后，才可打通，详情请参见[配置实例间网络互通](#)。

配置实例间网络互通

1. [进入阿里云ES的安全配置页面](#)。
2. 单击配置实例网络互通右侧的修改。
3. 在修改配置页面，单击+添加实例。



4. 在添加实例对话框中，选择需要进行网络互通的ES实例ID，单击确认。



注意:

- 子账号需要List权限才能获取相应主账号下的所有实例。
- 在满足前提条件后，您可以在添加实例页面选择多个符合条件的阿里云ES实例。
- 当其中一个ES实例选择了与另一个远程的ES实例打通后，在另一个ES实例的配置实例网络互通页面，也可以看到刚才配置的ES实例ID，即网络打通操作是双向的。如果A实例配置了与B实例的网络打通，则B实例的网络也与A实例进行了打通。

添加成功后，可在修改配置页面查看与当前实例打通的实例列表。



移除互通实例

1. 进入阿里云ES的安全配置页面。
2. 单击配置实例网络互通右侧的修改。

3. 在修改配置页面，单击与当前实例打通的实例列表中对应该实例右侧的移除。



4. 在确认移除对话框中，单击确认，完成互通实例的移除。

实例移除成功后，在修改配置页面的与当前实例打通的实例列表中不再显示该实例。

查询已打通的实例列表

1. 进入阿里云ES的安全配置页面。
2. 单击配置实例网络互通右侧的修改。

3. 在修改配置页面即可查看与当前实例打通的实例列表。

修改配置
✕

! 支持从同一地域同一账号下，部署在同一VPC内的实例进行网络互通，从而实现跨集群搜索功能。请注意：跨可用区实例和单可用区VPC网络之间隔离，不能配置跨集群访问。[详细参考文档](#)

与当前实例打通的实例列表:

实例ID	网络类型	操作
es-xx-65[redacted]pg	专有网络	移除
es-cn-04[redacted]wm	专有网络	移除

+ 添加实例

! **注意:**
 当删除实例时，如果该实例已经与其他实例打通，则会弹出当前实例已与其他实例实现网络互通，删除实例会同时解除网络打通，是否确认要删除实例的提示。

配置跨集群搜索

1. [登录远程ES集群的Kibana控制台](#)。
2. 执行以下命令，在远程ES集群中创建索引并添加文档。

```
PUT /twitter
{
  "settings" : {
    "index" : {
      "number_of_shards" : 3,
      "number_of_replicas" : 2
    }
  }
}
```

```
POST twitter/doc/
{
  "user" : "kimchy",
  "post_date" : "2009-11-15T14:12:12",
  "message" : "trying out Elasticsearch"
```

```
}
}
```



说明:

此步骤的作用是方便您对跨集群搜索进行验证。

3. 登录当前ES集群的Kibana控制台。

4. 执行以下命令，在当前ES集群中配置跨集群搜索。

以下为ES 6.7版本实例的配置，其他版本与此类似，详情请参见[ES 6.7版本实例配置官方文档](#)、[ES 6.3版本实例配置官方文档](#)、[ES 5.5版本实例配置官方文档](#)。

- 方法1：使用内网Endpoint配置。

```
PUT _cluster/settings
{
  "persistent": {
    "cluster": {
      "remote": {
        "cluster_one": {
          "seeds": [
            "es-cn-o4xxxxxxxxxxxx4f1.elasticsearch.aliyuncs.com:9300"
          ]
        }
      }
    }
  }
}
```

- 方法2：使用节点IP配置。

```
PUT _cluster/settings
{
  "persistent": {
    "cluster": {
      "remote": {
        "cluster_one": {
          "seeds": [
            "10.8.xx.xx:9300",
            "10.8.xx.xx:9300",
            "10.8.xx.xx:9300"
          ]
        }
      }
    }
  }
}
```



注意:

- 单可用区实例，可以使用方法1和2进行配置，并且支持配置多个远程阿里云ES实例。
- 多可用区实例，只能使用方法2进行配置，并且支持配置多个远程阿里云ES实例。

- 假如在A的ES实例中配置了需要访问的远程B的ES集群，只可在A的实例中查询远程B的ES实例中的用户索引，无法在远程B的ES实例中执行类似命令反向访问。如果需要反向访问，也需要在远程B的ES实例中配置A的实例的域名或IP。

5. 执行以下命令，验证跨集群搜索是否配置成功。

```
POST /cluster_one:twitter/doc/_search
{
  "query": {
    "match_all": {}
  }
}
```

验证成功后，返回如下结果。

```
{
  "took" : 78,
  "timed_out" : false,
  "_shards" : {
    "total" : 3,
    "successful" : 3,
    "skipped" : 0,
    "failed" : 0
  },
  "_clusters" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0
  },
  "hits" : {
    "total" : 1,
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "cluster_one:twitter",
        "_type" : "doc",
        "_id" : "qudxxxxxxxxxxx_7ie6J",
        "_score" : 1.0,
        "_source" : {
          "user" : "kimchy",
          "post_date" : "2009-11-15T14:12:12",
          "message" : "trying out Elasticsearch"
        }
      }
    ]
  }
}
```

11 数据备份

11.1 数据备份

本文档为您介绍阿里云Elasticsearch的数据备份功能。

进入阿里云Elasticsearch控制台，单击实例名称 > 数据备份，进入数据备份（免费试用）页面。



表 11-1: 数据备份

参数	说明
开启自动备份	开启自动备份开关为绿色时表示启用，默认为关闭状态。
自动备份开始时间	如果没有开启自动备份功能，会提示请开启自动备份后配置。 <div style="border: 1px solid gray; padding: 5px;"> <p>注意： 如果已经开启自动备份功能，则自动备份启动时间是当前Region的时间，请避免在自动数据备份时做集群Snapshot操作。</p> </div>

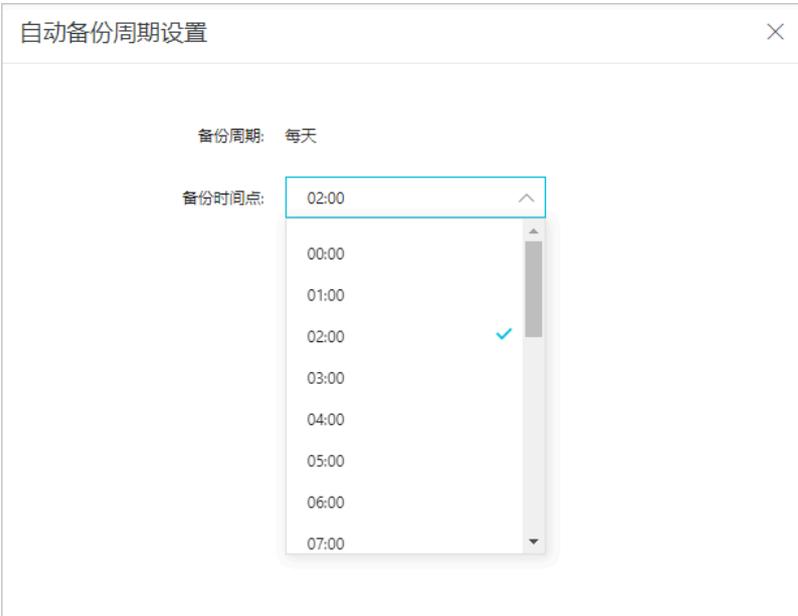
参数	说明
修改配置	<p>如果已经开启自动备份功能，可单击右上角的修改配置，在自动备份周期设置页面修改自动备份时间点。</p>  <p>注意：</p> <ul style="list-style-type: none"> · 备份周期是每天。 · 备份时间点单位是小时，可选时间范围为[0~23]。 · 自动备份只保存最近3天的快照数据。
备份恢复	可单击点击查看教程查看对应的文档。
备份状态	可单击点击查看教程查看对应的文档。

表 11-2: 跨集群OSS仓库设置

参数	说明
引用实例ID	被引用的ES实例的ID。
引用仓库名称	被引用的ES实例的仓库名称。
引用仓库状态	被引用的ES实例的仓库状态。
操作	提供了删除仓库的功能。
新增OSS仓库引用	<p>单击新增OSS仓库引用，可为当前ES实例添加一个OSS仓库引用，详情请参见跨集群OSS仓库设置。</p> <p>注意：</p> <p>首次新增OSS仓库引用时，不会显示新增OSS仓库引用按钮。需要单击立即添加，完成跨集群OSS仓库设置。</p>

11.2 自动备份指南

本文档为您介绍阿里云Elasticsearch（简称ES）实例的自动备份与自动备份恢复功能的使用方法。通过自动备份功能，您可以设置自动备份的时间，保证数据的安全性。

开启自动备份功能

1. [进入阿里云ES的实例管理页面](#)。
2. 单击左侧导航栏的数据备份。
3. 在数据备份页面，打开开启自动备份开关，开启自动备份功能。



4. 单击页面右侧的修改配置，选择每日自动备份触发的时间，单击保存即可定时触发ES自动备份。



从自动备份恢复数据

如果您对指定阿里云ES实例开启了自动备份功能，系统每天会自动为该Elasticsearch实例备份数据。您可以通过ES的snapshot API恢复数据到原阿里云Elasticsearch实例中。



说明:

- 您的第一个快照（即备份）是阿里云ES实例数据的完整拷贝，但后续所有的快照保留的是已存快照数据和新数据之间的增量，这意味着首次快照会耗时较长，后续快照会比较快。
- 快照不保存阿里云Elasticsearch实例自身的监控数据（例如以`.monitoring`和`.security_audit`为前缀的索引）。
- 快照只能用于恢复到原阿里云Elasticsearch实例。
- 自动快照仓库会在首次做快照时生成。

查看所有仓库

登录[Kibana控制台](#)，使用GET `_snapshot`命令查看所有仓库信息。

返回内容如下:

```
{
  "aliyun_auto_snapshot": {
    "type": "oss",
    "settings": {
      "compress": "true",
      "base_path": "xxxx",
      "endpoint": "xxxx"
    }
  }
}
```

- `aliyun_auto_snapshot`: 仓库名称。
- `type`: 快照存储介质，阿里云OSS。
- `compress:true`: 采用压缩模式，进行快照时会对索引的metadata信息进行压缩。
- `base_path`: 快照在OSS中的存储位置。
- `endpoint`: OSS所处区域的信息。

查看全部快照

通过GET `_snapshot/aliyun_auto_snapshot/_all`命令查看`aliyun_auto_snapshot`仓库内所有快照信息。

返回内容如下:

```
{
  "snapshots": [
```

```
{
  "snapshot": "es-cn-abcdefghijklmn_20180627091600",
  "uuid": "MMRniVLPRAiawSCm8D8Dug",
  "version_id": 5050399,
  "version": "5.5.3",
  "indices": [
    "index_1",
    ".security",
    ".kibana"
  ],
  "state": "SUCCESS",
  "start_time": "2018-06-27T01:16:01.009Z",
  "start_time_in_millis": 1530062161009,
  "end_time": "2018-06-27T01:16:05.632Z",
  "end_time_in_millis": 1530062165632,
  "duration_in_millis": 4623,
  "failures": [],
  "shards": {
    "total": 12,
    "failed": 0,
    "successful": 12
  }
}
```

默认参数

自动快照还有以下未显示的默认参数：

- `max_snapshot_bytes_per_sec:40mb`：单节点最大备份数据速度为40mb/秒。
- `max_restore_bytes_per_sec:40mb`：单节点最大恢复数据速度为40mb/秒。
- `chunk_size: Max 1Gb`：做快照过程中大文件会被拆分成若干个小文件，拆分出的文件最大为1GB。

从快照恢复索引数据

您可以通过ES的`_restore`命令从快照中恢复索引数据。

- 恢复`aliyun_auto_snapshot`仓库中指定快照的所有索引（后台执行）：

```
POST _snapshot/aliyun_auto_snapshot/<snapshot>/_restore
```

`<snapshot>`：替换为自动备份快照的名称，例如`es-cn-abcdefghijklmn_20180627091600`。

- 恢复aliyun_auto_snapshot仓库中指定快照的所有索引，并等待任务处理完成。

_restore为异步命令，Elasticsearch实例在确认可执行恢复操作后会立即返回，该恢复任务会在后台执行，可以通过追加wait_for_completion参数阻塞命令直到恢复完成再返回信息。

```
POST _snapshot/aliyun_auto_snapshot/<snapshot>/_restore?
wait_for_completion=true
```

<snapshot>: 替换为自动备份快照名称，例如es-cn-abcdefghijklmn_20180627091600

。

- 恢复aliyun_auto_snapshot仓库中指定快照的指定索引，并为恢复的索引重命名（后台执行）。

```
POST _snapshot/aliyun_auto_snapshot/<snapshot>/_restore
{
  "indices": "index_1",
  "rename_pattern": "index_(.+)",
  "rename_replacement": "restored_index_$1"
}
```

- <snapshot>: 替换为自动备份快照名称，例如es-cn-abcdefghijklmn_20180627091600。

- indices: 选择需要恢复的索引名称。

- rename_pattern: (可选) 正则匹配需要恢复索引的名称。

- rename_replacement: (可选) 为匹配上的索引按规则重命名。

11.3 查看备份状态

本文档为您介绍查看阿里云Elasticsearch（简称ES）实例自动备份的快照状态，帮助您实时了解快照的进度。

开启自动备份功能后，您可以登录该ES的Kibana控制台，在Dev Tools页面的Console中，通过snapshot API查看自动备份的快照状态。

查看所有快照

通过以下命令查看aliyun_auto_snapshot仓库中所有快照信息。

```
GET _snapshot/aliyun_auto_snapshot/_all
```

返回内容如下：

```
{
  "snapshots": [
```

```

{
  "snapshot": "es-cn-abxxxxxxxxxlmn_20180628092236",
  "uuid": "n7YxxxxxxxxxxxxdA",
  "version_id": 5050399,
  "version": "5.5.3",
  "indices": [
    ".kibana"
  ],
  "state": "SUCCESS",
  "start_time": "2018-06-28T01:22:39.609Z",
  "start_time_in_millis": 1530148959609,
  "end_time": "2018-06-28T01:22:39.923Z",
  "end_time_in_millis": 1530148959923,
  "duration_in_millis": 314,
  "failures": [],
  "shards": {
    "total": 1,
    "failed": 0,
    "successful": 1
  }
},
{
  "snapshot": "es-cn-abxxxxxxxxxmn_20180628092500",
  "uuid": "frdxxxxxxxxxxxxKLA",
  "version_id": 5050399,
  "version": "5.5.3",
  "indices": [
    ".kibana"
  ],
  "state": "SUCCESS",
  "start_time": "2018-06-28T01:25:00.764Z",
  "start_time_in_millis": 1530149100764,
  "end_time": "2018-06-28T01:25:01.482Z",
  "end_time_in_millis": 1530149101482,
  "duration_in_millis": 718,
  "failures": [],
  "shards": {
    "total": 1,
    "failed": 0,
    "successful": 1
  }
}
]
}

```

state: 显示快照状态, Elasticsearch快照共有5种状态。

快照状态	说明
IN_PROGRESS	快照正在执行。
SUCCESS	快照执行结束, 且所有shards都存储成功。
FAILED	快照执行结束, 但有数据存储不成功。
PARTIAL	Cluster级别的数据存储成功, 但至少有一个shard的数据没有存储成功。
INCOMPATIBLE	快照与阿里云ES实例版本不兼容。

查看指定快照

通过以下命令查看aliyun_auto_snapshot仓库中指定快照的详细信息。

```
GET _snapshot/aliyun_auto_snapshot/<snapshot>/_status
```

<snapshot>: 替换为自动备份快照名称, 可通过[查看所有快照](#)命令获取, 例如es-cn-abxxxxxxxxxxxlmn_20180628092236。

返回内容如下:

```
{
  "snapshots": [
    {
      "snapshot": "es-cn-abxxxxxxxxxxxlmn_20180628092236",
      "repository": "aliyun_auto_snapshot",
      "uuid": "n7YxxxxxxxxxxxxydA",
      "state": "SUCCESS",
      "shards_stats": {
        "initializing": 0,
        "started": 0,
        "finalizing": 0,
        "done": 1,
        "failed": 0,
        "total": 1
      },
      "stats": {
        "number_of_files": 4,
        "processed_files": 4,
        "total_size_in_bytes": 3296,
        "processed_size_in_bytes": 3296,
        "start_time_in_millis": 1530148959688,
        "time_in_millis": 77
      },
      "indices": {
        ".kibana": {
          "shards_stats": {
            "initializing": 0,
            "started": 0,
            "finalizing": 0,
            "done": 1,
            "failed": 0,
            "total": 1
          },
          "stats": {
            "number_of_files": 4,
            "processed_files": 4,
            "total_size_in_bytes": 3296,
            "processed_size_in_bytes": 3296,
            "start_time_in_millis": 1530148959688,
            "time_in_millis": 77
          },
          "shards": {
            "0": {
              "stage": "DONE",
              "stats": {
                "number_of_files": 4,
                "processed_files": 4,
                "total_size_in_bytes": 3296,
                "processed_size_in_bytes": 3296,

```

```
        "start_time_in_millis": 1530148959688,  
        "time_in_millis": 77  
      }  
    }  
  }  
} ]  
}
```

11.4 快照备份及恢复

您可以使用snapshot API来备份您的阿里云Elasticsearch集群。snapshot API会获取集群当前的状态和数据，然后保存到一个共享仓库里。这个备份过程是智能的。

第一次进行快照时，系统会备份您所有的数据，但后续所有的快照仅备份已存快照和新数据之间的差异。随着数据快照的不断进行，备份也在增量的添加和删除。这意味着后续备份会相当快速，因为它们只传输很小的数据量。



说明:

您可以参考[OSS快照迁移Elasticsearch](#)，使用快照方式完成自建Elasticsearch迁移至阿里云Elasticsearch。



注意:

本文代码中的<1>、<2>、<3>这三个标记用于标识位置，方便对指定位置代码描述。实际执行对应代码时，需去掉有包含这三个类型的标记。

前提条件

在进行快照备份前，您需要首先[#unique_46](#)并新建一个OSS Bucket（建议购买标准存储类型的OSS Bucket，不支持归档存储类型的OSS Bucket），且OSS Bucket的区域必须与您需要快照备份的阿里云Elasticsearch集群所在区域保持一致。

Bucket 名称 0/63

区域 华东1 (杭州) ▼

相同区域内的产品内网可以互通；订购后不支持更换区域，请谨慎选择

您在该区域下没有可用的 **存储包**、**流量包**。建议您购买资源包享受更多优惠，点击 [购买](#)。

Endpoint

存储类型 标准存储

标准：高可靠、高可用、高性能，数据会经常被访问到。
[如何选择适合您的存储类型？](#)

读写权限

私有：对文件的所有访问操作需要进行身份验证。

实时日志查询

OSS 与日志服务深度结合，免费提供最近7天内的 OSS 实时日志查询。开通该功能后，用户可对 Bucket 的访问记录进行实时查询分析，[了解详情](#)

创建仓库

```
PUT _snapshot/my_backup
{
  "type": "oss",
  "settings": {
    "endpoint": "http://oss-cn-hangzhou-internal.aliyuncs.com", <1>
  }
  "access_key_id": "xxxx",
  "secret_access_key": "xxxxxx",
  "bucket": "xxxxxx", <2>
  "compress": true,
  "base_path": "snapshot/" <3>
}
```

- <1>: `endpoint`为您的OSS Bucket对应的内网地址。详情请参见[#unique_48](#)中的ECS访问的内网Endpoint一栏。
- <2>: OSS Bucket的名称，需要一个已经存在的OSS Bucket。
- <3>: `base_path`设置仓库的起始位置，默认为根目录。

限制分块大小

当您上传的数据非常大时，可以限制snapshot过程中分块的大小，超过这个大小，数据将会被分块上传到OSS中。

```
POST _snapshot/my_backup/ <1>
{
  "type": "oss",
  "settings": {
    "endpoint": "http://oss-cn-hangzhou-internal.aliyuncs.com",
    "access_key_id": "xxxx",
    "secret_access_key": "xxxxxx",
    "bucket": "xxxxxx",
    "chunk_size": "500mb",
    "base_path": "snapshot/" <2>
  }
}
```

- <1>: 请求方式，注意使用POST而不是PUT，这会更新已有仓库的设置。
- <2>: `base_path`设置仓库的起始位置，默认为根目录。

列出仓库信息

```
GET _snapshot
```

您也可以使用GET `_snapshot/my_backup`获取指定仓库的信息。

备份快照迁移

按照以下步骤将当前快照迁移到另外一个集群。

1. 将当前快照备份到OSS。
2. 在新的集群上创建一个快照仓库（相同的OSS）。
3. 设置`base_path`为备份文件的路径。
4. 执行恢复备份的命令。

快照所有打开的索引

一个仓库可以包含多个快照，每个快照跟一系列索引相关（比如所有索引，一部分索引，或者单个索引）。当创建快照的时候，您可以指定感兴趣的索引，然后给快照取一个唯一的名字。

快照命令

最基础的快照命令如下。

```
PUT _snapshot/my_backup/snapshot_1
```

以上命令会备份所有打开的索引到`my_backup`仓库下，并保存在名称为`snapshot_1`的快照中。这个调用会立刻返回，然后快照会在后台运行。

如果您希望在脚本中一直等待到完成，可通过添加`wait_for_completion`实现。

```
PUT _snapshot/my_backup/snapshot_1?wait_for_completion=true
```

以上命令会阻塞调用直到快照完成。如果是大型快照，需要很长时间才能返回。

快照指定索引

系统默认会备份所有打开的索引。如果您在使用Kibana，并且考虑到磁盘空间大小因素，不想把所有诊断相关的`.kibana`索引都备份起来，那么可以在快照您的集群时，指定需要备份的索引。

```
PUT _snapshot/my_backup/snapshot_2
{
  "indices": "index_1,index_2"
}
```

以上快照命令只会备份名称为`index1`和`index2`的索引。

列出快照信息

有时您可能会忘记仓库里的快照细节，特别是快照按时间划分命名的时候（比如`backup_2014_10_28`）。

当您需要查看仓库中的某个快照时，可对仓库和快照名发起一个`GET`请求，获取单个快照信息。

```
GET _snapshot/my_backup/snapshot_2
```

返回结果中包括了快照相关的各种信息，如下所示。

```
{
  "snapshots": [
    {
      "snapshot": "snapshot_2",
      "indices": [
        ".marvel_2014_28_10",
        "index1",
        "index2"
      ],
      "state": "SUCCESS",
      "start_time": "2014-09-02T13:01:43.115Z",
      "start_time_in_millis": 1409662903115,
      "end_time": "2014-09-02T13:01:43.439Z",
      "end_time_in_millis": 1409662903439,
      "duration_in_millis": 324,
      "failures": [],
      "shards": {
        "total": 10,
        "failed": 0,
        "successful": 10
      }
    }
  ]
}
```

```
}
```

您也可以使用 `_all` 替换掉具体的快照名称，获取一个仓库中所有快照的完整列表。

```
GET _snapshot/my_backup/_all
```

删除快照

您可以对仓库和快照名发起一个 `DELETE` 请求，删除所有不再使用的快照。

```
DELETE _snapshot/my_backup/snapshot_2
```



注意:

- 请使用 `delete` API 来删除快照，而不能使用其他机制（比如手动删除）。因为快照是增量的，很多快照可能依赖于之前的备份数据。`delete` API 能够过滤出还在被其他快照使用的数据，只会删除不再被使用的备份数据。
- 如果您进行了一次人工文件删除，您将会面临备份严重损坏的风险，因为您删除的文件可能是还在使用中的数据。

监控快照进度

您可以使用 `wait_for_completion`，对快照进行监控，但其仅提供了基础的监控形式。如果您需要对中等规模的集群进行快照监控，可能会不够用。您可以通过以下两种方式获取详细的快照进度信息。

- 给快照ID发送一个 `GET` 请求。

```
GET _snapshot/my_backup/snapshot_3
```

如果您在执行这个命令时，快照还在进行中，那么您会看到它什么时候开始，运行了多久等信息。



注意:

这个API用的是与快照机制相同的线程池，当您在快照非常大的分片时，状态更新的间隔会很大，因为API在竞争相同的线程池资源。

- 使用 `_status` API 获取快照的状态信息。

```
{
  "snapshots": [
    {
      "snapshot": "snapshot_3",
      "repository": "my_backup",
      "state": "IN_PROGRESS", <1>
      "shards_stats": {
        "initializing": 0,
```

```
    "started": 1, <2>
    "finalizing": 0,
    "done": 4,
    "failed": 0,
    "total": 5
  },
  "stats": {
    "number_of_files": 5,
    "processed_files": 5,
    "total_size_in_bytes": 1792,
    "processed_size_in_bytes": 1792,
    "start_time_in_millis": 1409663054859,
    "time_in_millis": 64
  },
  "indices": {
    "index_3": {
      "shards_stats": {
        "initializing": 0,
        "started": 0,
        "finalizing": 0,
        "done": 5,
        "failed": 0,
        "total": 5
      },
      "stats": {
        "number_of_files": 5,
        "processed_files": 5,
        "total_size_in_bytes": 1792,
        "processed_size_in_bytes": 1792,
        "start_time_in_millis": 1409663054859,
        "time_in_millis": 64
      },
      "shards": {
        "0": {
          "stage": "DONE",
          "stats": {
            "number_of_files": 1,
            "processed_files": 1,
            "total_size_in_bytes": 514,
            "processed_size_in_bytes": 514,
            "start_time_in_millis": 1409663054862,
            "time_in_millis": 22
          }
        }
      }
    }
  },
}
```

```
...
```

- <1>: 快照的状态。一个正在运行的快照, 会显示为IN_PROGRESS。
- <2>: 正在快照传输的分片数量。为1时, 表示这个特定快照有一个分片还在传输 (另外四个已经完成)。

shards_stats响应不仅包括快照的总体状况, 也包括下钻到每个索引和每个分片的统计值。此参数为您展示了有关快照进度的非常详细的视图。分片可以在不同的完成状态:

- INITIALIZING: 分片在检查集群状态, 查看是否可以被快照。此过程一般是非常快的。
- STARTED: 数据正在被传输到仓库。
- FINALIZING: 数据传输完成, 分片正在发送快照元数据。
- DONE: 快照完成。
- FAILED: 快照过程中碰到了错误, 这个分片/索引/快照不可能完成。查看您的日志获取更多信息。

取消快照

如果您想取消一个快照, 可以在任务进行中的时候, 执行以下命令删除快照。

```
DELETE _snapshot/my_backup/snapshot_3
```

以上命令会中断快照进程并删除仓库中进行到一半的快照。

从快照恢复

在需要恢复索引的目标阿里云Elasticsearch实例上, 再执行和之前相同的[创建仓库](#)命令。您可以根据实际情况, 通过以下两种方式进行快照恢复。

- 如果您已经备份过数据, 可直接在需要恢复的快照ID后面加上_restore。

```
POST _snapshot/my_backup/snapshot_1/_restore
```

系统默认会恢复这个快照里的所有索引。例如snapshot_1包括五个索引, 那么这五个索引都会被恢复到您的集群中。您也可以指定需要恢复的索引, 具体请参考上文的[快照指定索引](#)。

- 恢复指定的索引, 并对恢复的索引进行重命名 (如果您需要在不替换现有数据的前提下, 恢复旧版本的数据来验证内容, 或者做其他处理, 可以使用此方式进行快照恢复)。

```
POST /_snapshot/my_backup/snapshot_1/_restore
{
  "indices": "index_1", <1>
  "rename_pattern": "index_(.+)", <2>
  "rename_replacement": "restored_index_$1" <3>
}
```

```
}
```

以上命令会恢复 `index_1` 到您集群里，并且重命名成了 `restored_index_1`。

- <1>: 只恢复 `index_1` 索引，忽略快照中的其他索引。
 - <2>: 查找正在恢复的索引，该索引名称需要与提供的模板匹配。
 - <3>: 重命名查找到的索引。
- 使用 `wait_for_completion`，查看恢复信息，直到恢复完成。

```
POST _snapshot/my_backup/snapshot_1/_restore?wait_for_completion=true
```

和快照类似，`_restore` API 会立刻返回，恢复进程会在后台进行。如果您更希望您的 HTTP 调用阻塞直到恢复完成，可以参考以上命令添加 `wait_for_completion`。

监控恢复操作



说明:

从仓库恢复数据借鉴了Elasticsearch里已有的现行恢复机制。在内部实现上，从仓库恢复分片和从另一个节点恢复是等价的。

您可以通过 `recovery` API 来监控恢复的进度。

- 监控指定索引的恢复状态。

```
GET restored_index_3/_recovery
```

`recovery` API 是一个通用的 API，可以用来展示您集群中移动着的分片状态。

- 查看您集群中的所有索引的恢复信息（可能包含跟您的恢复进程无关的其他分片的恢复信息）。

```
GET /_recovery/
```

示例输出结果如下（根据您的集群的活跃度，输出可能会非常多）。

```
{
  "restored_index_3" : {
    "shards" : [ {
      "id" : 0,
      "type" : "snapshot", <1>
      "stage" : "index",
      "primary" : true,
      "start_time" : "2014-02-24T12:15:59.716",
      "stop_time" : 0,
      "total_time_in_millis" : 175576,
      "source" : { <2>
        "repository" : "my_backup",
        "snapshot" : "snapshot_3",
        "index" : "restored_index_3"
      },
      "target" : {
```

```

    "id" : "ryqJ5l05S4-lSFbGntkEkg",
    "hostname" : "my.fqdn",
    "ip" : "10.0.1.7",
    "name" : "my_es_node"
  },
  "index" : {
    "files" : {
      "total" : 73,
      "reused" : 0,
      "recovered" : 69,
      "percent" : "94.5%" <3>
    },
    "bytes" : {
      "total" : 79063092,
      "reused" : 0,
      "recovered" : 68891939,
      "percent" : "87.1%"
    },
    "total_time_in_millis" : 0
  },
  "translog" : {
    "recovered" : 0,
    "total_time_in_millis" : 0
  },
  "start" : {
    "check_index_time" : 0,
    "total_time_in_millis" : 0
  }
} ]
}
}

```

- <1>: `type`字段定义了您恢复的类型。 `snapshot`表示这个分片是在从一个快照恢复的。
- <2>: `source`字段定义了作为恢复来源的特定快照和仓库。
- <3>: `percent`字段定义了恢复的状态。 `94.5%`表示这个特定分片目前已经恢复了94.5%的文件。

输出结果会展示所有正在恢复中的索引，并列出这些索引里的所有分片。同时每个分片中会显示启动/停止时间、持续时间、恢复百分比、传输字节数等统计值。

取消恢复

您可以通过删除正在恢复的索引，取消一个恢复（因为恢复进程其实就是分片恢复，发送一个DELETE API修改集群状态，就可以停止恢复进程）。

```
DELETE /restored_index_3
```

如果 `restored_index_3` 正在恢复中，以上删除命令会停止恢复，同时删除所有已经恢复到集群中的数据。

参考文档: [Snapshot And Restore](#)。

11.5 跨集群OSS仓库设置

阿里云Elasticsearch（简称ES）提供了跨集群OSS仓库设置的功能，帮助您在不同ES集群间进行数据的恢复。

背景信息

跨集群OSS仓库设置功能可以实现，某个实例从已经进行了自动快照备份的实例仓库中恢复数据。

例如，您有两个6.7.0版本的ES实例，ID分别为es-cn-a和es-cn-b，其中es-cn-a已经开通了自动快照的功能，且已经进行过一次快照。如果您的实例es-cn-b想从实例es-cn-a的自动快照恢复数据，那么需要使用阿里云ES的跨集群OSS仓库设置来实现。

兼容性说明

- 目前跨集群OSS仓库设置只支持同一个账号下同一个区域的ES实例间快照引用。
- 支持高版本的实例引用低版本的仓库，不支持低版本实例引用高版本仓库。



注意：

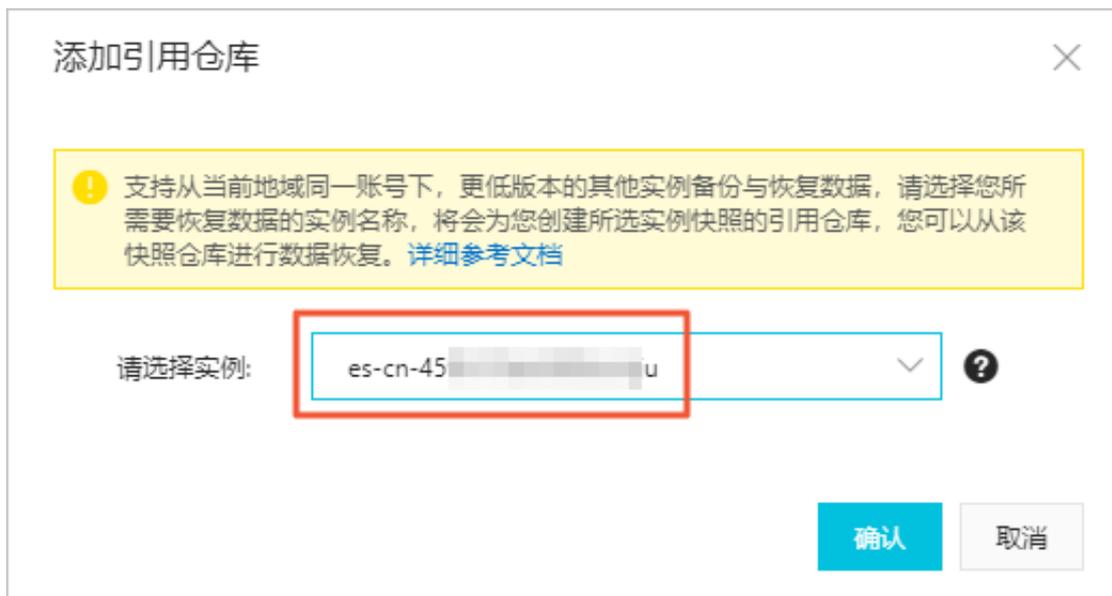
当高版本引用低版本的仓库时，需要注意高版本对低版本数据格式可能存在不兼容的情况。例如，从5.5.3版本的实例恢复数据到6.7.0的实例，对于单类型的索引，5.5.3的实例支持数据恢复到6.7.0。对于多类型索引，因为5.5.3版本的ES是支持多类型索引，而6.7.0不支持多类型索引，所以恢复可能会出现问題。此时需要根据您真实使用情况而定，恢复前需自行进行测试。

OSS仓库设置

1. 进入阿里云Elasticsearch控制台，单击实例名称 > 数据备份。
2. 在跨集群OSS仓库设置页面，单击立即添加。



3. 在添加引用仓库页面，选择实例。



注意:

所选实例需要与当前实例兼容，详情请参见[兼容性说明](#)。

4. 单击确认。

添加成功后，被引用的实例显示在当前页面，并显示引用仓库的状态。

引用实例ID	引用仓库名称	引用仓库状态	操作
es-cn-45...zju	aliyun_snapshot_from_es-cn-45...zju	生效	删除仓库



注意:

- 引用仓库会有两种状态，即生效和失效。生效状态表示该仓库可以正常引用，失效状态表示您引用的实例不存在或者仓库不存在。
- 由于仓库列表是通过访问您的实例获取到的，因此当您的实例在变更中、不健康或者负载特别高时，可能无法获取仓库列表。此时，您可以通过在Kibana控制台中，执行ES的原生命令GET _snapshot，获取所有的仓库地址。

恢复索引

跨集群OSS仓库设置只是帮您打通了实例间仓库的引用，并不会帮助您进行数据的恢复。您可以按需**在Kibana控制台上执行对应命令，恢复需要的索引数据。**

例如，您想从实例es-cn-a恢复file-2019-08-25索引，需要执行以下命令。

1. 查询指定实例仓库中的所有快照信息。

```
GET /_cat/snapshots/aliyun_auto_snapshot_from_a?v
```

该请求会返回该仓库下所存储的所有快照信息。

	id	status	start_epoch	start_time	end_epoch	end_time	duration	indices	successful_shards	failed_shards	total_shards
1	es-cn-45	ju_20191009010006	SUCCESS	1570554010	17:00:10	1570554012	17:00:12	1.5s	3	3	0
2											
3											

2. 根据上一步获取的快照id，恢复该快照下的指定索引。

 **注意：**
 请确保快照索引在恢复节点中处于close状态，或者没有该索引。如果在执行恢复之前，恢复节点已有相同名称的索引，并且处于open状态，使用索引恢复时会报错。

```
POST _snapshot/aliyun_snapshot_from_es-cn-a/es-cn-a_20190705220000/_restore
{"indices": "file-2019-08-25"}
```

```
POST _snapshot/aliyun_snapshot_from_es-cn-a/es-cn-a_20190705220000/_restore
{"indices": "kibana_sample_data_ecommerce,kibana_sample_data_logs"}
```

12 可视化控制

12.1 Kibana

12.1.1 登录Kibana控制台

本文档为您介绍登录阿里云Kibana控制台的方法。当您购买了阿里云Elasticsearch实例后，我们会为您赠送一个1核2G的Kibana节点。通过Kibana，您可以完成数据查询，数据可视化等操作。

前提条件

在登录Kibana控制台之前，您需要首先[购买一个Elasticsearch实例](#)。并且确保Kibana公网访问为开启状态。

背景信息

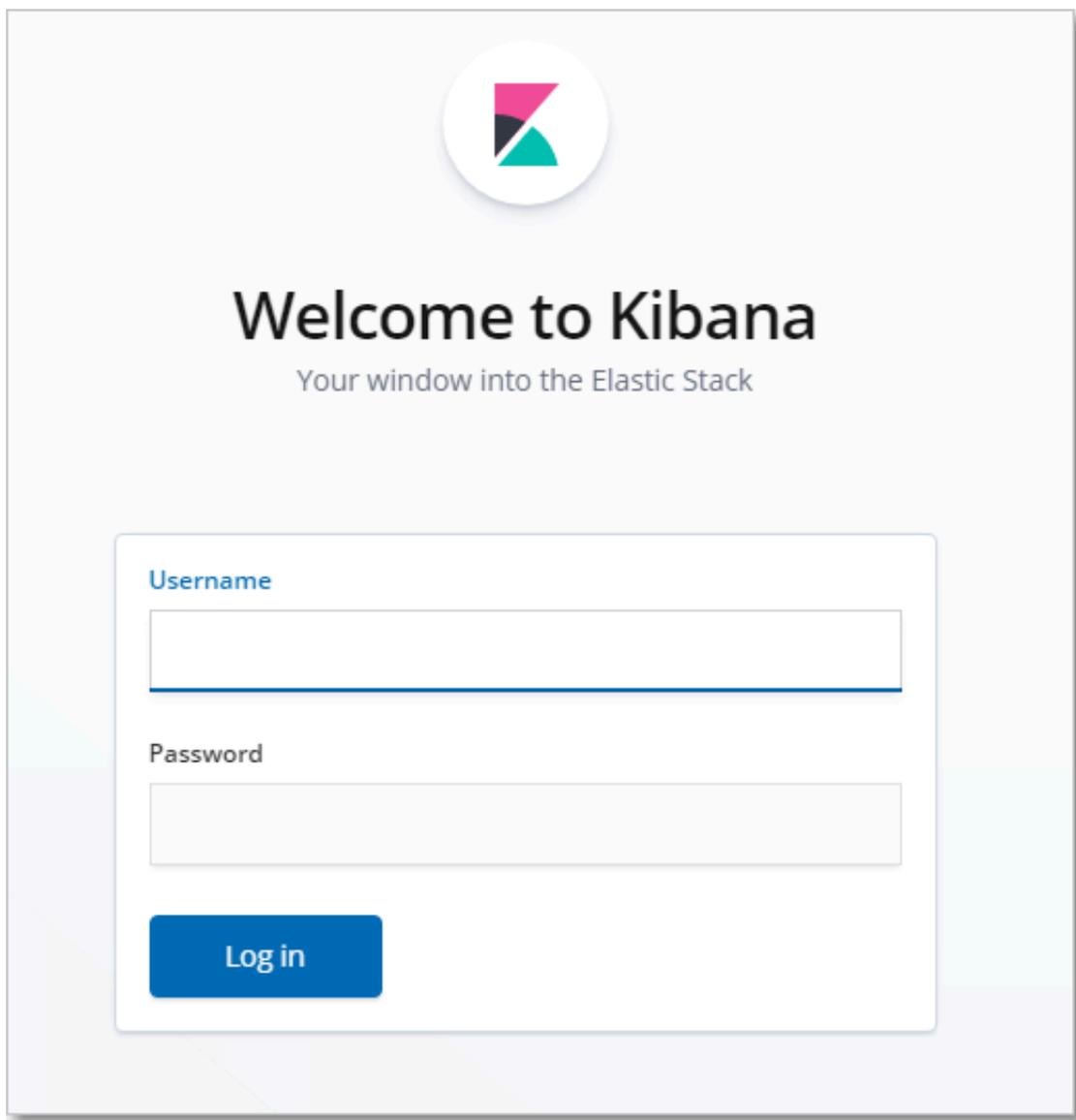
阿里云Elasticsearch实例提供Kibana控制台，为您的业务提供扩展的可能性。Kibana控制台作为Elastic生态系统的组成部分，支持无缝衔接Elasticsearch服务，可以让您实时了解阿里云Elasticsearch实例的运行状态并进行管理。

操作步骤

1. 登录[阿里云Elasticsearch控制台](#)，单击实例ID > 可视化控制。
2. 在可视化控制页面，单击Kibana模块中的进入控制台。

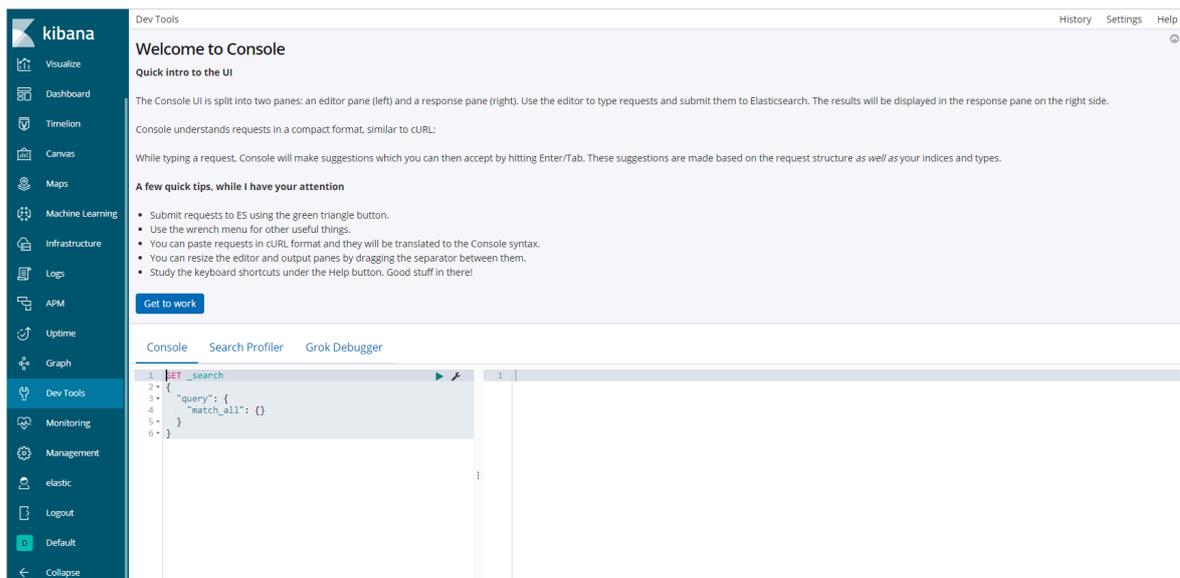


3. 在登录页面，输入用户名和密码，单击登录。



- 用户名：默认为elastic。
- 密码：您在购买Elasticsearch实例时设置的密码。

使用阿里云Elasticsearch 6.7版本（其他版本略有差异）登录成功后的页面如下图所示。



后续步骤

登录成功后，您就可以在Kibana控制台上完成数据查询、制作数据展示仪表盘等操作。详情请参见[官方文档](#)。

12.1.2 基本配置（6.7.0）

本文档为您介绍Kibana节点的基本配置功能。通过基本配置功能，您可以切换Kibana控制台的语言，包括中文和英文。



注意：

Kibana节点的基本配置功能仅适用于阿里云Elasticsearch 6.7.0 with Commercial Feature版本。

Kibana语言配置

1. 登录[阿里云Elasticsearch控制台](#)，单击实例ID > 可视化控制。

2. 在Kibana模块中，单击修改配置，进入Kibana配置页面。



在Kibana配置页面即可看到基本配置模块。在基本配置模块中，您可以继续执行以下步骤配置Kibana控制台的语言，默认为English。



3. 单击基本配置右侧的修改配置。

注意：
此配置需要重启Kibana节点才会生效。为避免影响您的Kibana操作，请确认后再执行以下步骤。

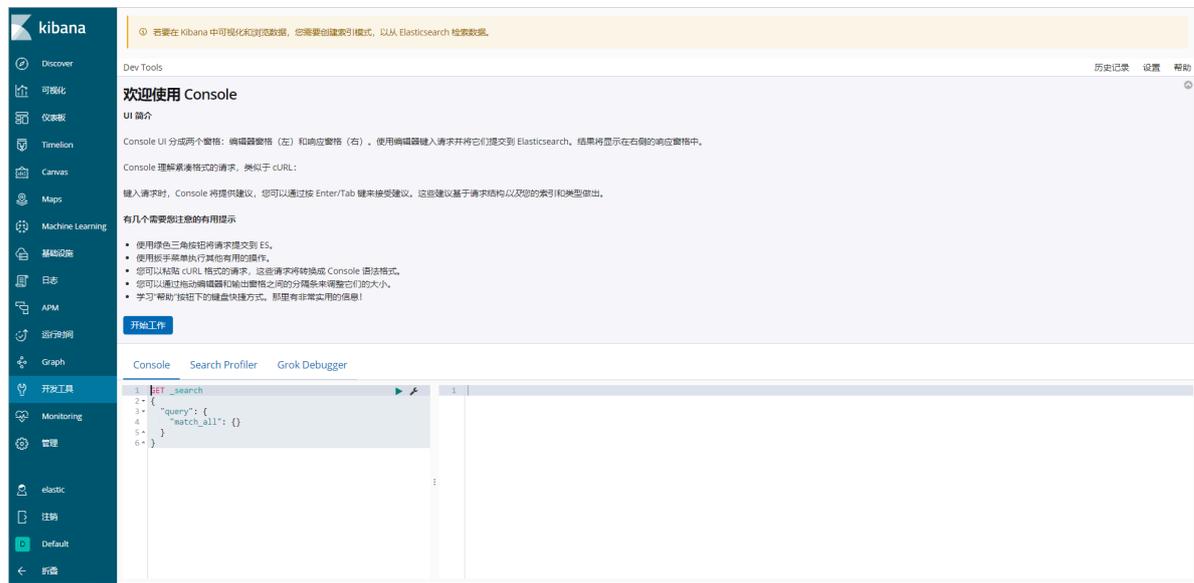
4. 在修改Kibana基本配置页面，选择修改语言，单击确定。



说明：

Kibana控制台支持English和中文两种语言，默认为English。

确认完成后，Kibana节点会自动进行重启。重启后，[登录Kibana控制台](#)，即可看到系统使用您设置的语言进行显示。



12.1.3 访问配置

本文档为您介绍Kibana集群的访问配置功能，包括开启公网访问和访问白名单配置。

进入Kibana访问配置页面

1. 登录[阿里云Elasticsearch控制台](#)，单击实例ID > 可视化控制。

2. 在Kibana模块中，单击修改配置，进入Kibana配置页面。



在Kibana配置页面即可看到访问配置模块。在访问配置模块中，您可以开启或关闭Kibana公网访问权限（默认开启），并配置Kibana访问白名单。



Kibana公网访问

Kibana公网访问开关默认显示为绿色，表示为开启状态。单击Kibana公网访问开关，可关闭Kibana公网访问权限，关闭后开关显示为灰色。Kibana公网访问关闭后，将无法通过外网进入Kibana控制台。

Kibana访问白名单

单击修改，在Kibana访问白名单输入框中输入您需要添加的IP地址，单击确认即可完成添加。

 **说明：**
默认允许所有公网地址访问。

Kibana访问白名单支持配置为单个IP或IP网段的形式，格式为192.168.0.1或192.168.0.0/24，多个IP之间用英文逗号隔开。127.0.0.1代表禁止所有IPV4地址访问，0.0.0.0/0代表允许所有IPV4地址访问。

目前杭州区域支持公网IPV6地址访问，并可以配置IPV6白名单，格式为2401:b180:1000:24::5或2401:b180:1000::/48。::1代表禁止所有IPV6地址访问，::/0代表允许所有IPV6地址访问。

12.1.4 插件配置

阿里云Kibana在开源社区插件的基础上，提供了丰富的插件。本文档为您介绍阿里云Kibana自定义插件的种类、安装和卸载方法及注意事项。

自定义插件列表

[BSearch-QueryBuilder](#)插件。

BSearch-QueryBuilder又称高级查询，是阿里内部纯自研的一个纯前端的工具插件，具有如下特性。

- 简单易用：BSearch-QueryBuilder插件提供了可视化的界面点选操作来构造Elasticsearch的DSL查询请求，无编码即可完成自定义条件的数据查询，减少了复杂的DSL的学习成本。也可辅助开发人员编写或验证DSL语句的正确性。
- 方便快捷：已经定义的复杂查询条件会保存在Kibana中，避免重复构造查询条件。
- 小巧轻盈：约占用14MB的磁盘空间，不会常驻内存运行，不影响Kibana和Elasticsearch的正常运行。
- 安全可靠：BSearch-QueryBuilder插件不会对用户的数据进行改写、存储和转发，源代码已经通过了阿里云安全审计。



说明：

BSearch-QueryBuilder插件仅支持6.3和6.7版本的阿里云Elasticsearch实例（不支持5.5.3）。

安装插件



注意：

当您购买了阿里云Elasticsearch实例后，我们会为您赠送一个1核2G的Kibana节点。由于插件需要耗费较多的资源，所以在安装插件前，您需要将该Kibana节点升级为2核4G或以上规格，详细请参见[集群升配](#)。

Kibana节点	<input checked="" type="checkbox"/>
Kibana节点规格	2核4GB

1. 登录[阿里云Elasticsearch控制台](#)，并购买一个[Elasticsearch实例](#)。
2. 单击实例ID > 可视化控制。

3. 在Kibana模块中，单击修改配置。



4. 在Kibana配置页面的插件配置区域，单击插件列表操作栏下的安装。

注意：

- 确认安装后会触发Kibana节点重启，所以在安装过程中Kibana不能正常提供服务，为避免影响您的Kibana操作，请确认后操作。
- 如果您的Kibana规格低于2核4G，系统会提示您进行集群升配，请按照提示将您的Kibana节点升级到2核4G或以上规格。

5. 确认安装并重启Kibana节点。

重启后即可完成插件的安装，安装成功后，插件的状态显示为已安装。



说明：
此过程可能耗时较长，请耐心等待。

卸载插件

1. 参考**安装插件**的操作步骤，在Kibana配置页面的插件配置区域，单击插件列表操作栏下的卸载。

注意：

确认卸载后会触发Kibana节点重启，所以在卸载过程中Kibana不能正常提供服务，为避免影响您的Kibana操作，请确认后操作。

2. 确认卸载并重启Kibana节点。

重启后即可完成插件的卸载，卸载成功后，插件的状态显示为未安装。

12.1.5 BSearch-QueryBuilder插件使用介绍

BSearch-QueryBuilder又称高级查询，是一个纯前端的工具插件。通过BSearch-QueryBuilder插件，您可以无需编写复杂的DSL语句，而是以可视化的方式完成复杂的查询请求。本文档为您介绍BSearch-QueryBuilder插件的使用方法，帮助您快速使用BSearch-QueryBuilder插件完成查询业务。

BSearch-QueryBuilder的特性

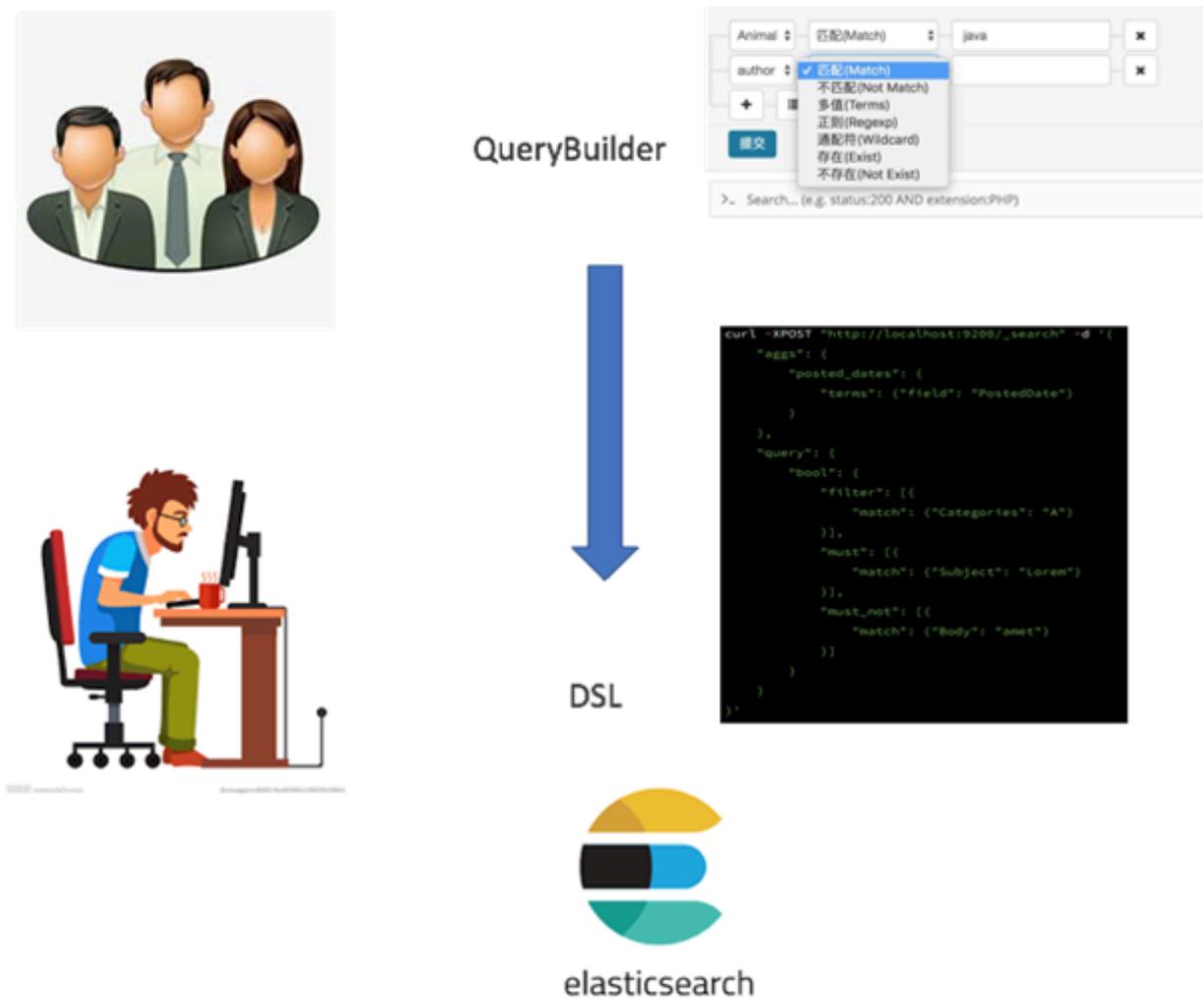
BSearch-QueryBuilder具有如下特性。

- 简单易用：BSearch-QueryBuilder插件提供了可视化的界面点选操作来构造Elasticsearch的DSL查询请求，无编码即可完成自定义条件的数据查询，减少了复杂的DSL的学习成本。也可辅助开发人员编写或验证DSL语句的正确性。
- 方便快捷：已经定义的复杂查询条件会保存在Kibana中，避免重复构造查询条件。
- 小巧轻盈：约占用14MB的磁盘空间，不会常驻内存运行，不影响Kibana和Elasticsearch的正常运行。
- 安全可靠：BSearch-QueryBuilder插件不会对用户的数据进行改写、存储和转发，源代码已经通过了阿里云安全审计。

背景信息

Query DSL是一个Java开源框架，用于构建安全类型的SQL查询语句，能够使用API代替传统的拼接字符串来构造查询语句。目前Query DSL支持的平台包括JPA、JDO、SQL、Java Collections、RDF、Lucene以及Hibernate Search。

Elasticsearch提供了一整套基于JSON的DSL查询语言来定义查询。Query DSL是由一系列抽象的查询表达式组成，特定查询能够包含其它的查询（如bool），部分查询能够包含过滤器（如constant_score），还有的可以同时包含查询和过滤器（如filtered）。您可以从ES支持的查询集合里面选择任意一个查询表达式，或者从过滤器集合里面选择任意一个过滤器进行组合，构造出复杂的查询。但编写DSL容易出错，仅有少数专业程序人员精通，QueryBuilder能够帮助对Elasticsearch DSL不甚了解或者想提升编写效率的用户快速生成DSL。



准备工作

在使用BSearch-QueryBuilder插件前，请先[购买一个Elasticsearch实例](#)，实例版本为6.3或6.7（不支持5.5.3）。

<input type="radio"/> 预付费 <input checked="" type="radio"/> 后付费																			
地域	<table border="1"> <tr> <td>华东1 (杭州)</td> <td>华北2 (北京)</td> <td style="background-color: #00a0e3; color: white;">华东2 (上海)</td> <td>华南1 (深圳)</td> <td>印度 (孟买)</td> <td>新加坡</td> </tr> <tr> <td>香港</td> <td>美国 (硅谷)</td> <td>马来西亚 (吉隆坡)</td> <td>德国 (法兰克福)</td> <td>日本 (东京)</td> <td>澳大利亚 (悉尼)</td> </tr> <tr> <td>印度尼西亚 (雅加达)</td> <td>华北1 (青岛)</td> <td>华北3 (张家口)</td> <td></td> <td></td> <td></td> </tr> </table>	华东1 (杭州)	华北2 (北京)	华东2 (上海)	华南1 (深圳)	印度 (孟买)	新加坡	香港	美国 (硅谷)	马来西亚 (吉隆坡)	德国 (法兰克福)	日本 (东京)	澳大利亚 (悉尼)	印度尼西亚 (雅加达)	华北1 (青岛)	华北3 (张家口)			
	华东1 (杭州)	华北2 (北京)	华东2 (上海)	华南1 (深圳)	印度 (孟买)	新加坡													
	香港	美国 (硅谷)	马来西亚 (吉隆坡)	德国 (法兰克福)	日本 (东京)	澳大利亚 (悉尼)													
印度尼西亚 (雅加达)	华北1 (青岛)	华北3 (张家口)																	
可用区	上海可用区B																		
资源组	全部																		
	默认资源组																		
版本	<table border="1"> <tr> <td style="border: 2px solid red;">6.7 with Commercial Feature</td> <td style="border: 2px solid red;">6.3 with Commercial Feature</td> <td>5.5.3 with Commercial Feature</td> </tr> </table>	6.7 with Commercial Feature	6.3 with Commercial Feature	5.5.3 with Commercial Feature															
6.7 with Commercial Feature	6.3 with Commercial Feature	5.5.3 with Commercial Feature																	



说明:

您也可以使用已经创建的实例，如果实例版本不符合要求，可进行版本升级。

安装BSearch-QueryBuilder插件



注意:

当您购买了阿里云Elasticsearch实例后，我们会为您赠送一个1核2G的Kibana节点。由于插件需要耗费较多的资源，所以在安装插件前，您需要将该Kibana节点升级为2核4G或以上规格，详细请参见[集群升配](#)。

Kibana节点	<input checked="" type="checkbox"/> 是
Kibana节点规格	2核4GB

1. 登录[阿里云Elasticsearch控制台](#)，并[购买一个Elasticsearch实例](#)。
2. 单击实例ID > 可视化控制。

3. 在Kibana模块中，单击修改配置。



4. 在Kibana配置页面的插件配置区域，单击插件列表操作栏下的安装。

注意:

- 确认安装后会触发Kibana节点重启，所以在安装过程中Kibana不能正常提供服务，为避免影响您的Kibana操作，请确认后操作。
- 如果您的Kibana规格低于2核4G，系统会提示您进行集群升配，请按照提示将您的Kibana节点升级到2核4G或以上规格。

5. 确认安装并重启Kibana节点。

重启后即可完成插件的安装，安装成功后，插件的状态显示为已安装。



说明:
此过程可能耗时较长，请耐心等待。

使用BSearch-QueryBuilder插件

1. 返回Elasticsearch实例的可视化控制页面，单击Kibana模块中的进入控制台。
2. 输入Kibana控制台的用户名和密码，单击登录。

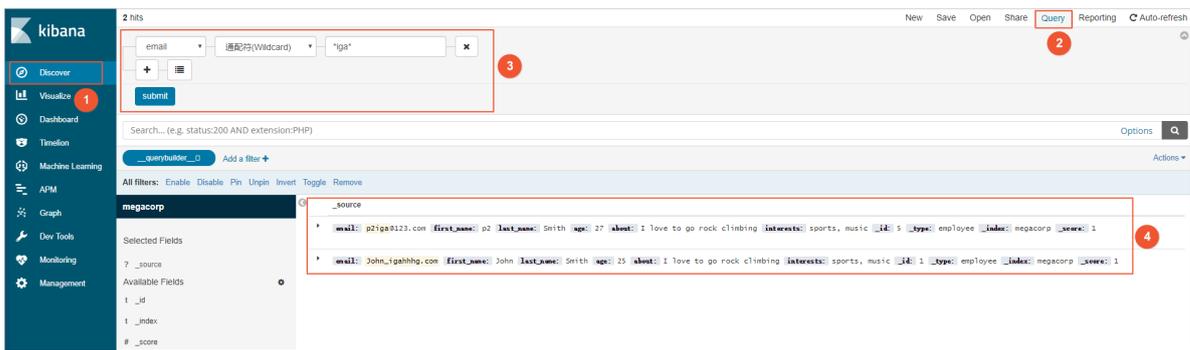
默认的用户名为elastic，密码为您购买实例时设置的密码。

3. 在Kibana控制台中，单击Discover > Query。

 **注意：**
 在查询前，请确保您已经创建了一个索引模式。否则需要在Kibana控制台中，单击Management，再单击Kibana模块中的Index Patterns > Create index pattern，按照提示创建一个索引模式。

4. 在查询区域选择查询和过滤条件，单击提交。

提交成功后，系统会显示查询结果。



单击查询区域的  可添加一个查询条件；单击  可为查询添加一个子过滤条件；单击  可删除一个查询或过滤条件。

具体的查询方式请参见下文的[BSearch-QueryBuilder插件使用示例](#)。

BSearch-QueryBuilder插件使用示例

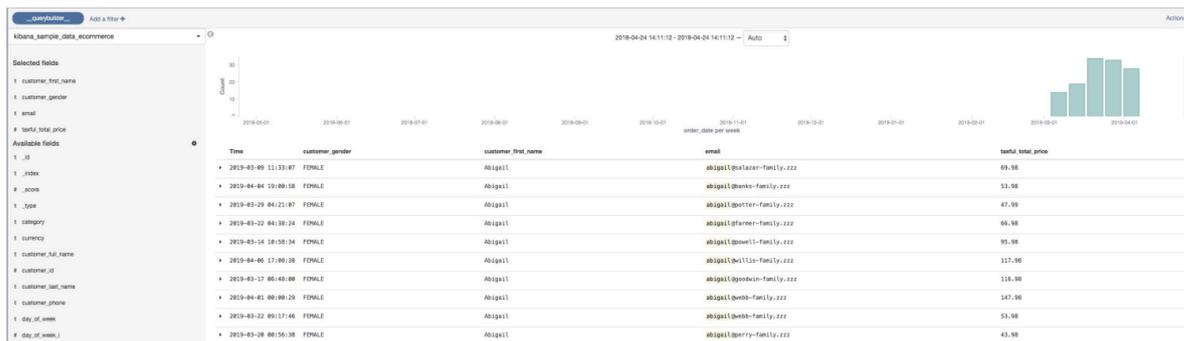
BSearch-QueryBuilder支持模糊查询、多条件组合查询和自定义时间范围查询等多种查询方式。

· 模糊查询

下图中表示对email这个条件进行模糊查询，并要求email中模糊匹配iga。

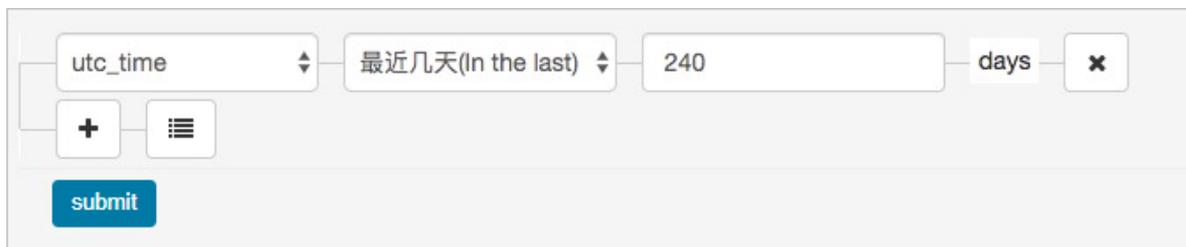


最终得到的匹配结果如下。

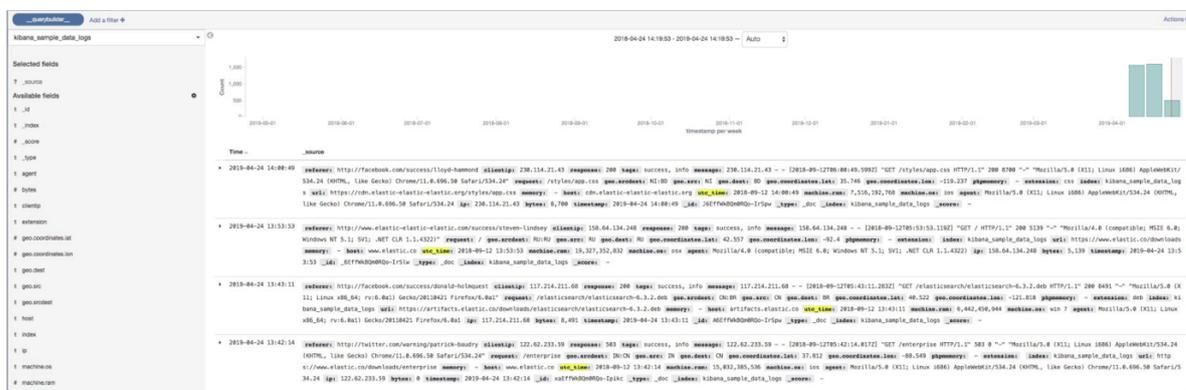


自定义时间范围查询

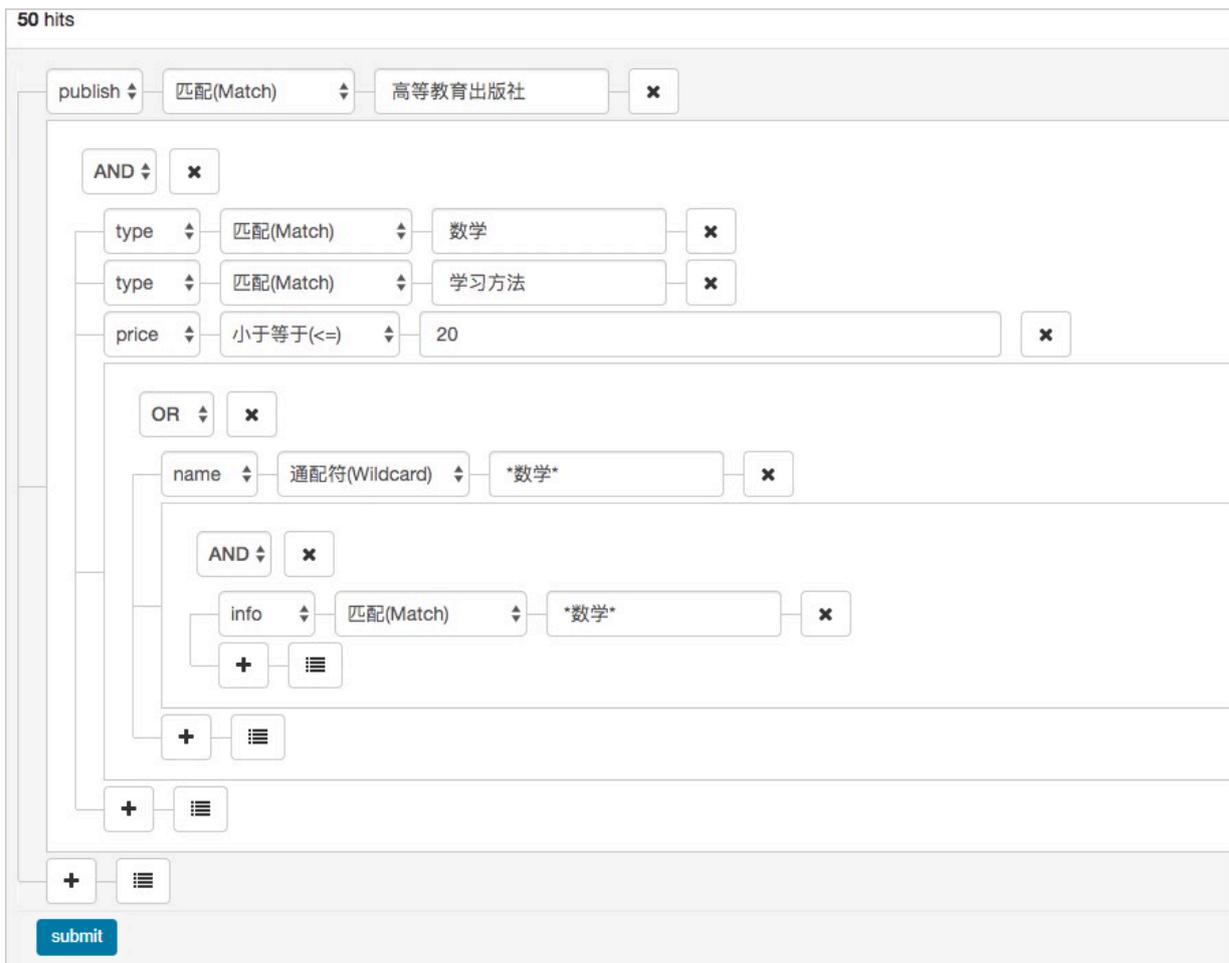
当您需要对时间字段进行筛选时，可使用时间类型的筛选功能。下图中对utc_time进行时间范围筛选，查询[当前时间-240天,当前时间]范围内的数据。



最终得到的匹配结果如下。



结合以上说明，构造一个复杂的查询条件，如下图所示。



而实际对应的DSL如下图所示。

```
{
  "query": {
    "bool": {
      "must": [
        {
          "match_phrase": {
            "publish": "高等教育出版社"
          }
        },
        {
          "bool": {
            "must": [
              {
                "match_phrase": {
                  "type": "数学"
                }
              },
              {
                "match_phrase": {
                  "type": "学习方法"
                }
              },
              {
                "range": {
                  "price": {
                    "lte": 20
                  }
                }
              }
            ],
            "should": [
              {
                "wildcard": {
                  "name": "*数学*"
                }
              },
              {
                "bool": {
                  "must": [
                    {
                      "match_phrase": {
                        "info": "*数学*"
                      }
                    }
                  ]
                }
              }
            ]
          }
        }
      ]
    }
  }
}
```

可以看出通过使用BSearch-QueryBuilder插件，可以极大地降低Elasticsearch查询的难度。

12.1.6 BSearch-Label插件使用介绍

BSearch-Label是一个纯前端的数据打标插件。通过BSearch-Label插件，您可以无需编写复杂的DSL语句，而是以可视化的方式完成数据打标。本文档为您介绍BSearch-Label插件的使用方法，帮助您快速使用BSearch-Label插件完成查询业务。

背景信息

通常情况下，在分析数据的时候，您可能不仅是单纯的浏览，而是希望通过某些查询条件对数据进行分析，并对某个字段（或者新增一个字段）赋予一个特殊的值（标签）来标注不同的数据，这一过程被称为“打标”。对数据打标后，您可以根据这个标签进行聚合分类统计，也可以根据标签的不同值进行快速过滤。标注的数据还可以直接为后续的流程所使用。

安装BSearch-Label插件

!
注意:

当您购买了阿里云Elasticsearch实例后，我们会为您赠送一个1核2G的Kibana节点。由于插件需要耗费较多的资源，所以在安装插件前，您需要将该Kibana节点升级为2核4G或以上规格，详细请参见[集群升配](#)。

Kibana节点

是

Kibana节点规格

2核4GB
▾

1. 登录[阿里云Elasticsearch控制台](#)，并[购买一个Elasticsearch实例](#)。
2. 单击实例ID > 可视化控制。
3. 在Kibana模块中，单击修改配置。



4. 在Kibana配置页面的插件配置区域，单击插件列表操作栏下的安装。

 **注意:**

- 确认安装后会触发Kibana节点重启，所以在安装过程中Kibana不能正常提供服务，为避免影响您的Kibana操作，请确认后操作。
- 如果您的Kibana规格低于2核4G，系统会提示您进行集群升配，请按照提示将您的Kibana节点升级到2核4G或以上规格。

5. 确认安装并重启Kibana节点。

重启后即可完成插件的安装，安装成功后，插件的状态显示为已安装。



 **说明:**

此过程可能耗时较长，请耐心等待。

使用BSearch-Label插件

1. 返回Elasticsearch实例的可视化控制页面，单击Kibana模块中的进入控制台。
2. 输入Kibana控制台的用户名和密码，单击登录。

默认的用户名为elastic，密码为您购买实例时设置的密码。

3. 在Kibana控制台中，单击Discover > 打标。

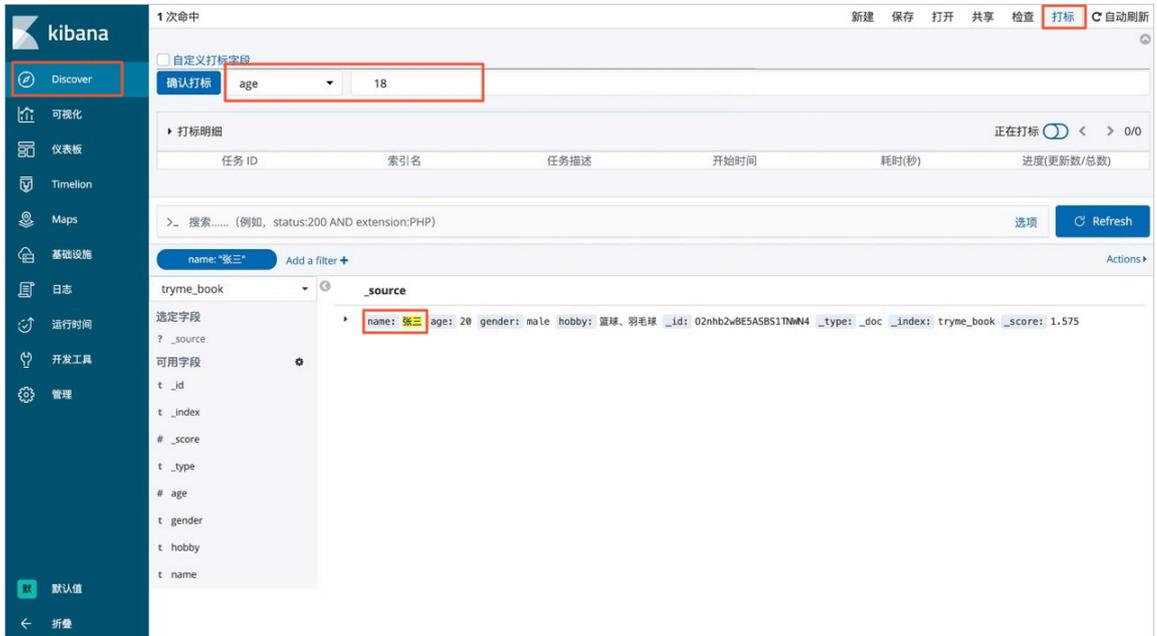
 **注意:**

在查询前，请确保您已经创建了一个索引模式。否则需要在Kibana控制台中，单击Management，再单击Kibana模块中的Index Patterns > Create index pattern，按照提示创建一个索引模式。

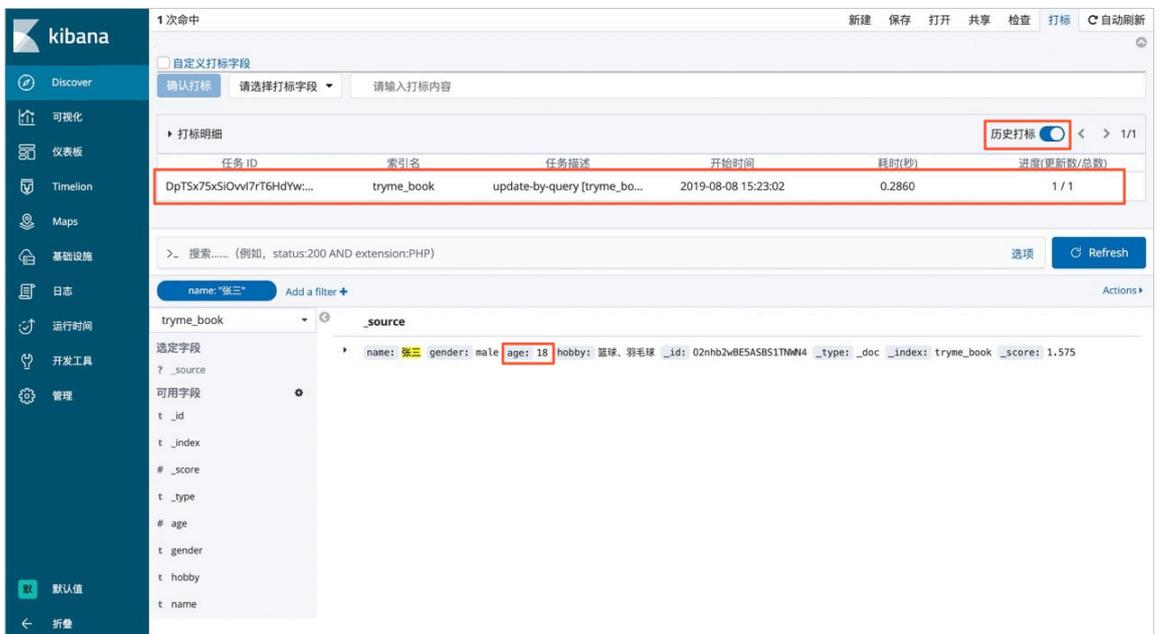
4. 根据您的需求，选择以下任意一种方式完成数据打标。

- 对已有字段进行打标。

如下示例，先查询到名字是张三的数据，然后选择age字段，将其标记为18，单击确认打标。

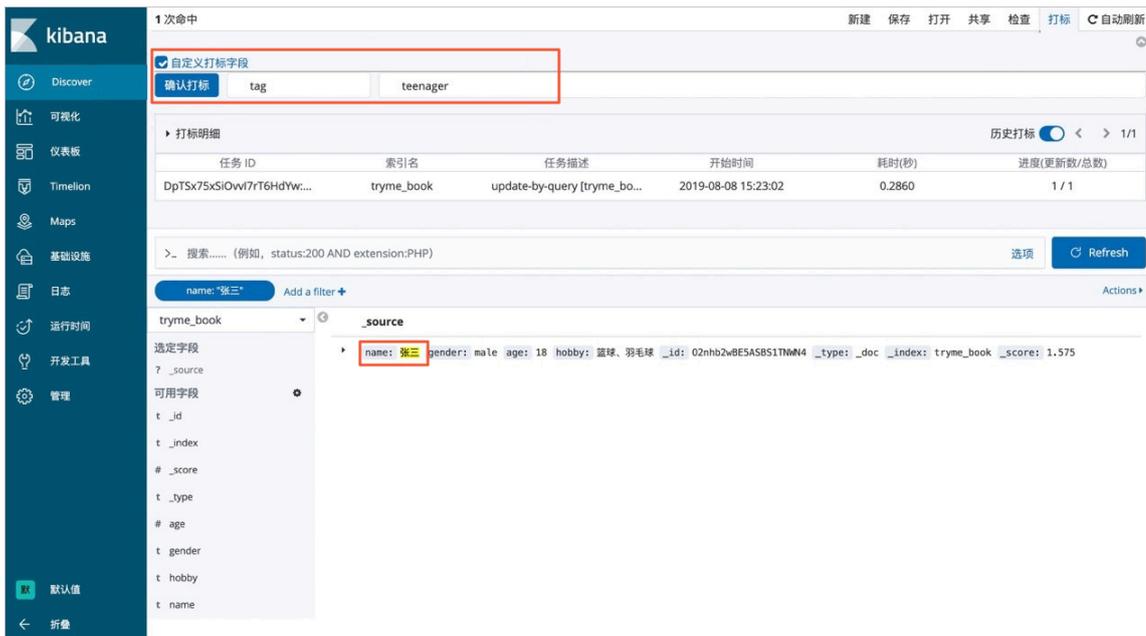


打开历史打标开关，可查看历史打标任务详情。

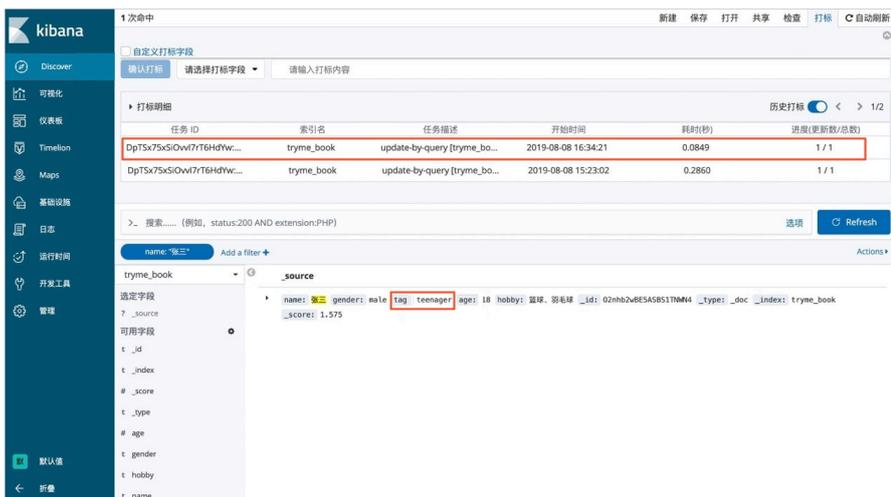


- 新增字段进行打标。

如下示例，先查询到名字是张三的数据，然后勾选自定义打标字段，新增一个字段tag，将其标记为teenager，单击确认打标。



查看打标结果。



12.2 使用DataV大屏展示Elasticsearch数据

您可以通过在DataV中添加阿里云Elasticsearch（简称ES）数据源，使用DataV访问阿里云ES服务，并在DataV中完成ES数据的查询与展示。

前提条件

已经完成以下任务：

- [#unique_6](#)。
- 开通DataV服务，必须为企业版或企业版以上版本，详情请参见[#unique_58/unique_58_Connect_42_section_ucc_3kj_p2b](#)。

在DataV中添加Elasticsearch数据源

1. 登录[阿里云Elasticsearch控制台](#)，单击实例ID > 可视化控制。
2. 在可视化控制页面，单击DataV模块中的进入控制台。
3. 在DataV控制台中，单击我的数据 > 添加数据。
4. 在添加数据对话框中，单击类型下拉箭头，选择Elastic Search并单击使用前请授权DataV访问。



注意：

DataV企业版及以上版本才支持添加Elastic Search数据源。

5. 在云资源访问授权页面，单击同意授权完成授权访问。



注意：

在使用ES数据源之前，需要先授权DataV对阿里云ES数据服务的访问。

6. 填写ES数据服务项目信息。

参数	说明
自定义数据源名称	数据源的显示名称，可以自由命名。
Region	ES实例的地域（默认选择华东1区）。

参数	说明
实例ID	用于查询可用的ES实例ID。授权DataV访问ES后，单击获取实例列表可以获取到ES的实例列表，单击右侧下拉框选择列表中某一实例（或直接输入数据库名称选择已有实例）。 可参见 基本信息概览 获取ES实例的ID。
密码	所选ES实例在被创建时设置的密码，不同实例的密码不同。

配置成功后，系统会自动进行测试连接。

7. 测试连接成功后，单击确定，完成数据源的添加。

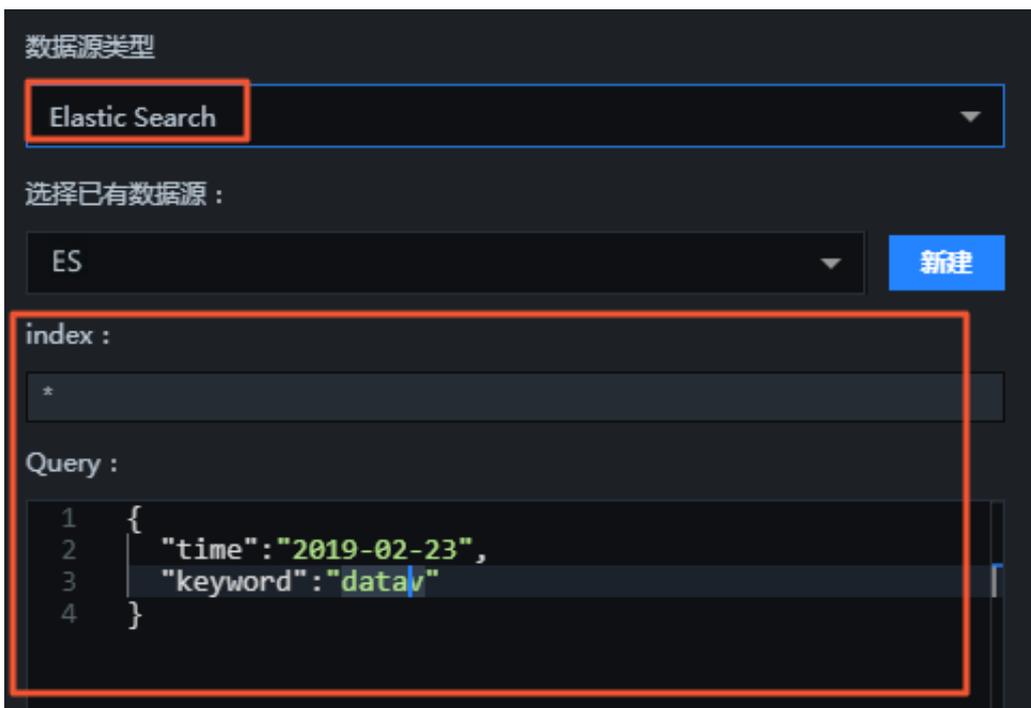
使用Elasticsearch数据源

在使用ES数据源之前，请首先在DataV中添加Elasticsearch数据源。



1. 在DataV控制台上，单击我的可视化。
2. 选择您的项目，单击编辑，进入大屏编辑界面。
3. 单击选择某一组件，在右侧的数据面板中，单击配置数据源。
4. 在设置数据源面板中，选择数据源类型为Elasticsearch。选择已有数据源为您已经添加的ES数据源。
5. 在index输入框中填写查询索引，通常是一个字符串。

6. 在Query输入框中填写查询体，查询体为JSON对象，默认是{}。



7. 单击查看数据响应结果，数据响应成功后即可看到效果。