阿里云 阿里云Elasticsearch

实例

文档版本: 20191112

为了无法计算的价值 | [-] 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。

- 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。
- 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
0	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。
Ê	用于补充说明、最佳实践、窍门 等,不是用户必须了解的内容。	送 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 listinstanceid
		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。	<pre>switch {active stand}</pre>

目录

通用约定
1 增强版实例介绍1 2 实例列表4 3 实例管理6
1 省 强派关闭并指 2 实例列表
2 头例列衣
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
5 ES集群配置
5.1 ES集群配置概述
5.2 同义词配置
5.3 高级配置
5.4 YML文件配置
5.5 Head插件安装(Chrome)
6 插件配置
6.1 插件配置概述
6.2 自定义插件列表53
7 集群监控
7.1 集群告警
7.2 集群监控
8 日志查询
9 安全配置
10 配置实例网络互通
11 数据各份 80
11 3从10 田 [J]····································
11.1 奴据审切 80 11 9 自动冬码指动
11.2 日初田以泪雨 02 11 3 杏看各份状态 85
11.5 呈有面份状态 11.4 快昭备份及恢复 88
11.5 跨集群OSS仓库设置
12 可视化控制
12 1 Kibana 100
12.1.1 登录Kibana控制台100
12.1.2 基本配置(6.7.0)
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	
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。



・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。

NFS

 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。

如 類	〕 说明: 県需要更大的	り集群,请在控	制台中提交工	`单 。
存储	CPFS存储空间	5TB CPFS存储空间暂不支持	10TB 寺扩容, 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

- ・阿里云増强版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 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

- ・阿里云増强版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

- ・ 単副本情况下,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<u>实例管理</u>。

・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。

・変更配置

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<mark>集群升配</mark>。

・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。

<	es-cn-v w		集群监控重度实例	刷新	≡
基本信息				转包年包月	
ES樂群配靈	基本信息				
插件配置	实例ID: es-cn-	创建时间: 2019年9月9日 14:13:58			
集群监控	名称: es-cn-编辑	状态: ● 正常			
日志査询	Elasticsearch 版本: 6.7.0 with Commercial Feature	付要與型:后付费			
*458	区域: 华东1 (杭州)	可用区: cn-hangzhou-h			
×±40 <u>用</u>	专有网络: vpc-l	VSwitch(回想: vsw-bg k			
数据备份	内阳地址: es-cn-vi F7w.elasticsearch.aliyuncs.com	内网端口: 9200			
可视化控制	公网地址 请开册公网访问地址居使用				
▼ 智能运進	协议: HTTP 傳改				
集群概况	节点可视化 配置列表		集群数据节点缩容	集群升配	3
健康诊断					
历史报告					

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<u>集群告警</u>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<mark>强制重启</mark>。
- 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)。

	集群监控	实例生效中	刷新 📃
	任务列表		×
创建时间: 2019年9月9日 1	实例变更		
状态: ● 生效中	55%		展开详情
▲ ▲ 付 書 送 型: 后 付 書	● 准备ECS资源		
可用区: cn-hangzhou-h	已完成节点数: 3/3,进度: 100%		
- VSwitch信息: vsw-b	 准备容器服务 进度: 100% 		
内网端口: 9200	 变更节点 (创建、重启, 扩节点, 扩规格)	
	已完成节点数: 0/3,进度: 22.5%		
	● 准备配置		
	进度: 0%		
		集群数据节点缩容	集群升配

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 实例生效中	刷新	1
任务列表	>	<
实例变更		
55%	展开详情	
● 准备ECS资源		
已完成节点数: 3/3,进度: 100%		
● 准备容器服务		
进度: 100%		
 变更节点(创建、重启,扩节点,扩规格) 		
已完成节点数: 0/3,进度: 22.5%		
● 准备配置		
进度: 0%		

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。

es-cn-v w	黄料盐拉 重点采州 用新 三
基本信息	转起年起月
实例UD: es-cn-v w	创建时间;2019年9月9日 14:13:58
名称 es-cn- w 编辑	秋志: ● 正常
Elasticsearch 版本: 6.7.0 with Commercial Feature	付機类型: 后付機
区域: 华东1 (杭州)	可用区: cn-hangzhou-h
参有网络: vpc-b	VSwitch值思: vsw-b
内网地址: es-cn-\	内网施口: 9200
公网结社: es-cn- public.elasticsearch.aliyuncs.com	公网颁曰: 9200
1933: HTTP 博改	

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降 级,需要通过新建实例后迁移数据,详情请参见# <i>unique_16</i> 。	
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。	
	 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。 	
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	需要开启公网地址后才显示。主要支持的端口如下。 ・ 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。	
	 [三] 说明: - 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。 	
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 <mark>使用<i>HTTPS</i>协</mark> 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	主要支持的端口如下。	
	・ 9200端口,基于HTTP/HTTPS。 ・ <u>9300</u> 端口,基于TCP。主要支持阿里云ES 5.5.3版本。	
	道 说明: 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。	
续费	仅当付费类型为预付费时显示。 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。	

名称	描述
转包年包月	仅当付费类型为后付费时显示。
	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。

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。

节点可视化 配置列表		集群	許升配
	集群	状态:正常 获取详细集群健康诊断请前往 <mark>智能运维</mark>	
	cn-shanghai-b 数据节点	cn-shanghai-e 数据节点	

・根据颜色判断集群各节点的健康状态。



门 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。

节点IP:	14.140.004	节点IP:	110,000,000,000
节点状态:	● 未知	节点状态:	● 警告
CPU使用率 CPU规格:	_	CPU使用率 CPU规格:	80% 8核
磁盘使用率 总存储空间:	_	磁盘使用率 总存储空间:	2GB 32GB
负载均衡:	_	负载均衡:	0.58
JVM内存:	_	JVM内存:	40%
• 节点失联,建议使用智能	运维诊断	• 节点状态不佳,建议使用	目智能运维诊断

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。

<	es-cn-v w		集群监控	重启实例	周新	≡
基本信息 ES集群配置	基本信息				转包年包月	月
浙件配置	說例D2 es-cn-v v	创建时间: 2019年9月9日 14:13:58				
集群监控	名称 ei-cn-v / 網續	状态:● 正常				
日志查询	Elasticsearch 版本: 6.7.0 with Commercial Feature	付張與型: 局付 勝				
安全配置	区域: 华东1 (杭州)	可用区: cn-hangzhou-h				
数据备份	专有内容: vpc-t t t	VSwitch(E) (2 vsw-)				
可视化物制	公网结战 e-cn-v x_public.elasticsearch.aliyuncs.com	公務調告: 9200				
▼ #255510	的论: HTTP 慘政					
集群概况	节点可 强化		#1877	数据节点编辑	樂群升春	R

 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: 数据节点 · · · · · · · · · · · · · · · · · · ·	
192.168.	192.168
192.168.	192.168.
192.168	

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。

择节点类型:	数据节点	\sim			
5点个数:4					
点个数: 1					
100.100	100.100	100.100	100.11	20	
192.168.	192.168.	192.168.	192.10	58.	

- 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。

集群数据节点迁移	×
迁移节点类型:数据节点 迁移节点个数: 1	
系统建议 自定义	
提示:系统根据数据分布和集群健康状况智能推荐迁移节点IP,无法盘点业务数据重要性,请二次确认数据 安全。	
192.168.3.152	
✓ 我同意《阿里云Flasticsearch数据迁移服务协议》、授权阿里云Flasticsearch服务协助迁移日标数据节点中的数据。	
确认	取消

・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: 1 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. 192.168. 192.168. 192.168. 192.168.	
✓ 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。	
确认	取消

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<mark>任务列表</mark>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。

	Kibana控制台	集群监控	重启实例	刷新	=
任务列表					×
集群数据重	新分布 100%		展开详情		
● 待迁移	节点选择中				
进度:	100%				
• 迁移数	据				
进度:	100%,迁移服务器IP歹	刂表(2台):			
192.16 192.16	8. 8.				

____ 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。

	Kibana控制台	集群监控	实例生效中	刷新
任务列表				
集群数据重	新分布	展开详情	唐 停止	
● 待迁移	节点选择中		а Ттт	
进度:	100%			
● 迁移数	据			
2# 庄.	0% 迁移肥冬岛回	川主 (04) .		

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。

}

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。

・回滚全部节点数据。

3. 校验是否完成数据回滚。

在*Kibana*控制合的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。



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<mark>集</mark> 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。

}

```
"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→
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。

<	es-cn-v		集群监控重定实例	刷新 ☰
基本信息				转包年包月
ES集群配置	基个信息			
播件配置	条例ID:	创建时间: 2019年6月24日 10:18:50		
集群监控	名称	秋志: • 正常		
日本要項	Elasticsearch 版本: 6.7.0 with Commercial Feature	付藤美型:后付赛		
HIGHER	区域: 华东1 (杭州)	可用区: cn-hangzhou-b		
安全配置	参有网络: 、	VSwitch信思: v		
数据备份	内网地址 e	内网端曰: 9200		
可提化控制	公网地址 请开启公网访问地址后使用			
▼ 智能运進	协议: HTTP 傳政			
集群概况	配置列表 节点可视化		集群数据节点编容	集群升配
健康诊断	数据节师规格: elasticsearch.n4.small(1核 2G)	数据节点数量: 2		
历史报告	存储现h: SSD 云曲	存储容量: 20 GiB		
	Kibana节点明h elasticsearch.n4.small(1核 2G)	Kibana节点数: 1		
				联系
				我们

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。

2凹C					
á前配置					
《例名称:					
洧主节点:否		协调节点 : 否	存储类型:SSD云盘	单节点存储空间:20	
本 : 6.7 with Commercial	Feature	网络类型:专有网络	数量:2	实例规格:1核2G	
域:华东1		规格族:云盘型	专有网络:v	虚拟交换机:v	
用区:杭州可用区B		冷数据节点:否	可用区数量:单可用区		
置变更					
雪子 地域	华东1(杭州)	•			
査 安 更 第 地域 可用区数量	华东1(杭州) <mark>单可用区</mark> 普通部署模式,适	■ 浦于非关键任务型工作负载			
(学文更) (学文)	华东1 (杭州) 单可用区 普通部署棋式,适 云盘型	■ 用于非关键任务型工作负载			

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。

当前配置			
实例名称: es-cn-(
专有主节点:是	协调节点:是	协调节点数:2	协调节点存储空间:20G
协调节点存储类型:高效云盘	协调节点规格:2核8G	存储类型:SSD云盘	单节点存储空间:20
版本 : 6.3 with Commercial Feature	强制变更:false	专有主节点数:3(默认)	专有主节点存储空间:20G
专有主节点存储类型:SSD云盘	专有主节点规格:2核8G	网络类型:专有网络	数量:3
实例规格:2核4G	地域:华东1	规格族:云盘型	专有网络:vpc-
虚拟交换机:vsw-	可用区:杭州可用区B	冷数据节点:是	冷数据节点数量:3
冷数据节点存储空间:500	冷数据节点存储类型:高效云盘	冷数据节点规格:2核8G	

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,那么在进行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。
- ・変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

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。

可 规 实 数 专 专 专类 专至 协 协 协型	U用区数量 の格族 に例规格 な量 学有主节点数 学有主节点双格 学有主节点可储 短期 学行主节点可储 2011 か调节点数	 単可用区 ● ●	2		
	R 格族 C 例規格 2 公 2 会 2 合 <p2 p="" 合<=""> 2 合 2 合 2</p2>	田田田中田山以, ADD J H-V WEILD ALLI 19382 1様20 1 1 1 1 1 1 1 1 1 1 1 1 1	3		
实 数 专 专 专类 专空 协 协 协型	Q例现格 Q例现格 皮量 皮有主节点 皮有主节点切り格 皮有主节点切り格 皮有主节点存储 QU型 内调节点 か调节点数	1枚20 ・ 1枚20規構用适合測試、不透用于生产环境、不在SLA集后保障范围 3 第 第 3(数以) 2枚80 SSD无盘 200	3		
数 安 安 安 安 安 安 安 安 安 安 安 一 数 物 数 物 数	安有主节点 テ有主节点数 テ有主节点初格 テ有主节点存储 空間 か调节点数	1歳2G規模用适合則試,不透用于生产环境,不在SLA售后保障范围 3 一 一 一 3(款以) 2(歳3(以)) 2(歳3(以)) 20G 否 夏 二	2		
 安 安 安 安美 安空 协 协 协型	专有主节点 等有主节点取 等有主节点现略 专有主节点存储 处理 空间 空间	两个石点集群有颜裂风险,谨慎选择 否			
· ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	字有主节点数 字有主节点规格 字有主节点存储 型 字有主节点存储 2回 か调节点。	3(康秋) 2(桂約G ← SSD云盘 200G 音 星			
专 专类 专空 协 协 协型	字有主节点规格 字有主节点存储 处型 字有主节点存储 2回 办调节点、	2株8G - SSD元曲 20G 否 星 2			
· ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	9有主节点存储 後型 9月主节点存储 20月 功调节点 办调节点数	SSD无意 20G 否 是 2			
专空 协 协 协型	9有主节点存储 2回 协调节点 か调节点数	20G 否 是 2 章			
	が调节点 か调节点数	2 ×			
□ □ □ ■ ● ● ● ● ●	协调节点数	2			
<u>高</u> 禄 协					
协型	协调节点规格	2核8G ▼			
	か调节点存储类 型	意效云盘			
协间	协调节点存储空 同	20G			
~	\$数据节点	否			
冷	令数据节点数量	2			
冷	令数据节点规格	2#28G 🔹			
冷美	◎数据节点存储 ≌型	高效云盘			
		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 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	莫数据量的日志及分析场景 封F容		
冷 空	令数据节点存储 2间	500			
кі	〔ibana节点	高效云曲扩容时最大支持扩容到2T,新购最大支持5120Gib(5T),超	12048Gib时,只能取:2560、3072、3584、	4096、4608、5120	
Ki	übana规格	2校4G *			
强	虽制变更				
	i	强制变更,忽略集群健康状态			
準	自节点存储空间	20 ◆ 単位为Glb, SSD 云曲最大存储空间支持2048Glb(2T) 高改云曲扩窗时最大支持扩容到27,新购时最大支持5120Glb/5T).	武之2048Gib时,只能取: 2560. 3072. 3584	4, 4096, 4608, 5120	

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	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。
	 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。
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	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。
	 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。

参数	说明
强制变更	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。
	(!) 注意:
	 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。
存储	单位为Gib, SSD云盘最大支持2048Gib(2T)的空间。 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 $_{\circ}$

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" : {
               "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "analyzer" : {
                "ananalyzer" : {
                "analyzer" : {
                "[analyzer" : {
                "[analyzer" : {
                "[analyzer" : [analyzer" : [ananalyzer" : [ananalyzer" : [ananalyzer" : [analyzer" : [anana
```

```
"synonym" : {
                         "tokenizer" : "whitespace",
                         "filter" : ["synonym"]
                         }
                    },
"filter" : {
                          "synonym" : {
                               "type" : "synonym",
                                "synonyms_path" : "analysis/synonym.txt
۳,
                                "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_p

ath),示例如下。

1 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定义会增加群集 大小。

WordNet同义词

```
示例格式声明如下。
```
}

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。
- 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。
- 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。

同义词配置	×
9 当前实例规格最大支持5M词典文件	
同义词配置 ₂	
aliyun_synonyms.txt $ imes$	
上传文件 ~ 上传文件	

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": {
    tfr":
      "by_tfr": {
    "type": "stop",
        "stopwords": [" "]
      },
      "by_sfr": {
    "type": "synonym",
        "synonyms_path": "analysis/aliyun_synonyms.txt"
      }
   "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."
      ...
      "title": [
           "I <red>start</red> work at nine."
         ٦
      }
   },
{
      "_index": "aliyun-index-test",
"_type": "doc",
"_id": "1",
      "_score": 0.39556286,
        _source": {
"title": "Shall I begin?"
      "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。
```

```
}
}
}
}
```

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."
      "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

0

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。

空间抑格	
1核2G规格只适合测试,不适用于生产环境,不在SLA	皆保障范围内
数量 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。



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。

<	es-cn-v	修改配置 ×
基本信息	分词能置	修改配置: C CMS回收器
ES集群配置 插件配置	同义词配置 實系	④ G1回收器
集群监控日志查询	高级配置	
安全配置	12次回收器: G 1回收器 🕢	
数据备份 可视化控制	YML文件配置	
▼ 智能运维	自动创建家号:不允许自动创建家号 🕢	
集群概況 健康诊断	MilliconfigureREE @	· · · · · · · · · · · · · · · · · · ·
历史报告		
		R032 R036

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 +.*,-* 	0
删除索引指定名称: 删除时明确索引名称 一 删除时索引名称支持通配符 	0
Auditlog索引: ● 不开启auditlog索引 ● 开启auditlog索引	0
开启Watcher:	0
其他configure配置:	0
	联
● □ 该操作会重启实例,请确认后操作。	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.watcherhistory*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
http.cors.enabled	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。
	 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。
http.cors.allow-origin	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。
	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 2.\///localbost(:「0-9]+)2/ 表示可响
	应符合此正则的请求信息。
	 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。
http.cors.max-age	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)。

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。

- ・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
Ł
  "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": {
        "nemote": {
            "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。

Auditlog索引:	\bigcirc	不开启auditlog索引
	0	开启auditlog素引

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



- · 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。
- · 当您将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
<pre>xpack.security.audit. index.bulk_size</pre>	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。
<pre>xpack.security.audit. index.flush_interval</pre>	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	<pre>access_denied, access_granted, anonymous_access_denied , authentication_faile d, connection_denied , tampered_request , run_as_denied, run_as_granted</pre>	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
<pre>xpack.security.audit. index.events.exclude</pre>		构建索引过程中排除的 Auditlog事件。
<pre>xpack.security.audit. index.events.emit_reque st_body</pre>	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。



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	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。
	 注意: 使用best_compression会导致写性能降低。

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"
    }
}
```


- ・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。

竖 要添加"ElasticSearch Head"吗?	×
该程序可以: 读取和更改您在访问的网站上的所有数据	
添加扩展程序取	消

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。

8	× "ElasticSearch Head"已添加到 Chrome	
	点击该图标, 即可使用此扩展程序。	
	您可以通过点击"工具"菜单中的"扩展程序",管理您的 扩展程序。	
要将您的所有扩展程序同步到您的所有设备上,请开启同步 功能。		
开启同步功能		

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。

<	es-cn-456w	Kibana控制给 集群监控 重启实例 刷新 三
基本信息	集群网络设置	
ES集群配置		
插件配置	ES实例访问密码: 已设置 重置	Kibana访问白名单: =1 修改
集群监控	VPC私网访问白名单: 修改	公网地址
日志查询	公网地址访问白名单: ::1 4 /16 修改	
安全配置		
数据备份		



- · 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。

🛿 elasticsearc	ch-head ×	+			٥	23	J
$\leftarrow \rightarrow c$	* ElasticSearch Head	chrome-extension://ffmkiejjmecolpfloofpjologoblkegm/elasticsearch-head/index.html	☆	ß	θ	:	

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。

B elasticsearch-head × +			• ×
\leftrightarrow \rightarrow C (* ElasticSearch Head chrome-extension://ffmkiejjmecolpfloofpjologoblkegm/elasticsearch-head/index.html	☆	ß	Θ :
Elasticsearch http://es-cn-45/6w.public.elastics 连接 集群健康值: 未连接			信息▼
概况 索引 数据测试 基本查询[+] 复合查询[+]			
集群概范 集群指弦 * Sort Indices * View Aliases * Index Filer			刷新 🔽

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-45xxxxxxx01xw6w.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。

登录 http://es 您与此网:	-cnpublic.elasticsearch.aliyuncs.com:9200 站的连接不是私密连接
用户名	elastic
密码	
	登录 取消



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。

 B elasticsearch-head ← → C 	× +	hrome-extension://ff	mkiejimecolofloofn	iologoblkegm/elast	icsearch-head/index h	itml		÷ (
Elasticsearc 概定 案引 数据浏览 集群概算 集群推变	ch http://es-cn- 基本查询 [+] 复合部	前回 [+]	lic.elastics 连接 es	5-cn-	Sector Heady Hacking	重值: green (155 of 155			
	test_sort size: 4.69ki (9.37ki) docs: 1 (2) 信息 • 动作 •	test_index size: 5.46ki (10.9ki) docs: 1 (2) 信息 ~ 动作 ~	my_index size: 95.7kl (188ki) docs: 750 (1,502) 信見 マ 初作 マ	my_array size: 7.16ki (14.3ki) docs: 1 (2) 信息。 动作。	logstash- 2019.02.14 size: 6.17ki (12.3ki) docs: 1 (2) 信意 マ 同作マ	jcj_index_test size: 14.1ki (28.2ki) docs: 4 (8) (信息) 创作)	iktest size: 5.40ki (10.8ki) docs: 1 (2) (信夏 、 (訪作 、	football size: 22.7ki (45.4ki) docs: 11 (22) 信息。 动作。	datete size: 4.71 (9.41ki) docs: 1 (; 信息 • 动作 •
★ 2FkVV0V 信息 • 动作 ●	23	23	1	23	0	12	23	3	[

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。

<	es-cn-v				集群监控重合实例	刷新 〓
基本信息 ES集群配置	插件配置					
揚件配置	系统默认插件列表 自定义插件列表					
集群监控	周新				请输入插件名称	Q
日志查询	插件名称	英型	状态	描述	操作	
安全配置	analysis-icu	系统默认	 已安装 	Elasticsearch ICU分析操件,集成了ICU模块,添加了ICU模关的分析组件。	卸数	
可视化控制	analysis-ik	系统默认	 E安装 	Elasticsearch IK分析關件。	冷更新	
▼ 智能器進 須許概況	analysis-kuromoji	驱统默认	● 已安装	Elasticsearch日语(kuromoji)分析操作, 集成了Lucene kuromoji分析模块。	50 <u>90</u>	
健康诊断	analysis-phonetic	系统默认	• 已安装	Elasticsearch 音标分析描件,集成了词元过滤器。	90 9 0	
历史报告	analysis-pinyin	系统默认	● 巳安岐	Elasticsearch 拼音分析插体。	卸戰	
	analysis-smartcn	系统默认	• 已废装	Elasticsearch 智能中文分析描件,集成了Lucene智能中文分析器。	卸载	
	analysis-stconvert	系统默认	 未安装 	STConvert is a analysis plugin that convert Chinese characters between traditional and simplified.	安装	联系我们
	elasticsearch-repository-oss	系统默认	 已安装 	支持使用同型云OSS存储Elasticsearch Snapshot		

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。

<	es-cn-v	
基本信息 ES集群配置	插件配置	
插件配置	系统默认插件列表 自定义插件列表	
集群监控	上传刷新	
日志查询		米刑
安全配置		XE
数据备份		

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。

插件上传		×
选择文件:	添加多个文件或将多个文件拖放到此区域	
	elasticsearch-sql-6.7.0.0.zip (4.44M) ×	
	自定义插件上传会触发集群重启安装,并且插件本身可能影响集群稳定,请 务必保证自定义插件的可用性和安全性。ES升级时插件不会自动升级更新, 需要重新上传。 上传安装 取	消

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。



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。

插件上传		×
选择文	件: 添加多个文件或将多个文件拖放到此区域	
	elasticsearch-sql-6.7.0.0.zip (4.44M)	
	✓ 自定义插件上传会触发集群重启安装,并且插件本身可能影响集群稳定,请 务必保证自定义插件的可用性和安全性。ES升级时插件不会自动升级更新, 需要重新上传。	
	上传安装 取消	

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。

系统默认插件列表 自定义插件列表					
上份 刷新				请输入插件名称	Q
□ 插件名称	英型	状态	描述	操作	
sql	自定义播件	 ● 已安装 	Query elasticsearch using SQL	卸載	

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)。

一键报警 × ×	
状态: 关闭	
Elasticsearch—键报警由云监控提供,开启后会创建: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。	
前往开启	

4. 在云监控控制台上,打开Elasticsearch服务的一键报警开关。

Elasticearch 开启后,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,作用于主张号下全部Elasticearch实例, 一種报警:

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。

<	es-cn-
基本信息	生丧生态
ES集群配置	
插件配置	一键报警: 开启 😮
集群监控	集群监控

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。

集群监控								
1 小时	3 小时	6 小时	12 小时	1天	3天	7天	14天	

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。

曽 自定义]	
开始时间:	2019-09-12	08
结束时间:	2019-09-12	09
30天内的重 最多连续重	查询提供分钟粒度 查询7天数据	的数据, 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)



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:

磁盘使用率报警阀值建议控制在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)



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*。



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。

<	es-xx-t	d	\$\$ \$
基本信息			
ES集群配置	主日志 searching慢日志	indexing慢日志 GC日志	
插件配置	host:172.16. AND conten	thealth AND level:info	② 2019年9月19日 1545:12 □ 至 2019年9月19日 1545:12 □ 1045
樂群监控	时间	节点IP	内容
日志登询			Tand Links
安全配置	2019年9月19日 15:40:36	172.16.	host : 172216
数据备份			content : [cie.cc.a.AllocationService] [2:3(59hC] Cluster health status changed from [PELCW] to [GREEN] (reason: [shards started [[monitoring-kibana-6-2019.08.19][0]]]).
可视化控制			level : info
▼ 智能运道	2019年9月19日 15:40:24	172.16.	host : 172.16 time : 2019-09-19715-40:24:364Z
集群概况			content : [o.e.c.r.a AllocationService] [2:3C9hC] Cluster health status changed from [YELLOW] to [SREEN] (reason: [shards started [[Albana][0]]]).
健康诊断			level : info
历史报告	2019年9月19日 15:28:57	172.16.	hest : 17216 time: 1096-09-091528257.052 context : : [0xcrx.Allocationdevice] [2:2596:] Cluster health status changed from (YELLOW) to [3REEN] (reason [shards started [].monitoring-es-6-2019.09.19][0]]]).

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	印点带	内容
2019年9月19日 15:40:36	172.16.	level : info host : 172.16 time : 2019-09-19TI5-40.36.324Z content : [o.c.r.a.AllocationService] [2:305HC] 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] [2:3C9hC] Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[Jobbana]]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.ra.AllocationService] [2r3C9hC] 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。
	前明: 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。
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。

<	es-cn-		
基本信息			
ES集群配置	集群网络设置		
插件配置	ES实例访问审码:已设置 置置 VPC私网访问白名单: 0.0.0.0 修改		
集群监控	公网始社:		
日志查询			
安全配置			
数据备份	配置实例网络互逐:未设置 修改		
可视化控制			

- · 重置ES实例访问密码。
- ・配置VPC私网访问白名单。
- ・ 开启<mark>公网地址</mark>。
- ・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。
- ・ 単击重置, 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	P		×
	! 您以后每次登录	ElasticSearch时都需要输入该信息,请妥善保存	
	用户名:	elastic	
	家码.	0/30	
	ш.,	8-30个字符, 月同时包含三项 (大写字母, 小写字母, 数字, 特殊	
		字符)	
	确认密码:	两次输入密码保持一致 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。



・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。 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



·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	6,您需要首先购买协计	调节点。	
数量	2	险,谨慎选择	
专有主节点	否	是	
协调节点	否	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	否	是	
Kibana节点	否	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。

= (-)阿里云	Q 搜索
<	Terror All Back Back Back
基本信息	集群网络设置
53来#HD国 插件配置	ES实例访问密码: 已设置 重置
集群监控	公网地址
日志查询	使用HTTPS协议:
安全配置	
数据备份	
可视化控制	

!) 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。



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。

	集群监控 实例生效中	刷新 ⊒
	任务列表	×
VPC私网访问白名单: 0.0.0.0/0	实例变更 55%	展开详情
	 准备ECS资源 已完成节点数: 5/5, 进度: 100% 准备容器服务 进度: 100% 变更节点(创建、重启,扩节点,扩规格) 已完成节点数: 0/5, 进度: 22.5% 准备配置 进度: 0% 	

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 BasicCrede
ntialsProvider();
       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.setHttpCli
entConfigCallback(
           new RestClientBuilder.HttpClientConfigCallback() {
              @Override
              public HttpAsyncClientBuilder customizeHttpClient(
sProvider(credentialsProvider);
              }
```

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

・开启HTTPS后的示例代码如下。

```
final CredentialsProvider credentialsProvider = new BasicCrede
ntialsProvider();
        credentialsProvider.setCredentials(AuthScope.ANY,
            new UsernamePasswordCredentials("elastic", "Your
password"));
RestClientBuilder restClientBuilder = RestClient.builder(
            new HttpHost("es-cn-xxxxx.elasticsearch.aliyuncs.com",
9200, "https"));
        RestClient restClient = restClientBuilder.setHttpCli
entConfigCallback(
            new RestClientBuilder.HttpClientConfigCallback() {
                @Override
                public HttpAsyncClientBuilder customizeHttpClient(
HttpAsyncClientBuilder httpClientBuilder) {
                    return httpClientBuilder.setDefaultCredential
sProvider(credentialsProvider);
                ł
            }).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", 9200, "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<mark>配置实例间网络互通</mark>。

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。

<	es-cn-o401b96v50002d3zd	修改	收配置			×
基本信息. 65株群配置	集計列的设置		 支持从同一地域同一账号下,1 功能,请注意:跨可用区实例 	B署在同一VPC内的实例进行网 [1单可用区VPC网络之间隔离,	络互通,从而实现跨集群撞索 不能配置跨集群访问。 详细参	
浙仲積2盟	ESEMINIER BAR 📷 VROUT		与当前实例打通的实例列表:			
集群监控			实例ID	网络美型	操作	
日志宣词		11				
安全配置				没有数据		
款 描 留份	就還與例例為且進,未设置 傳放	l c	- (81029)			
可視化控制		۲ ا				
▼ 智能意地						
集群概况						
建建设新						
历史报告						

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。

添加实例			×
请选择实例:	es-cn-o4	wm 🗸	Ø
		确认	取消
(!) 注意:			
・子账号需要List权限	才能获取相应主账号下的所	所有实例。	
・ 在满足 <mark>前提条件</mark> 后,	您可以在添加实例页面选	译多个符合条件的阿里z	SES实例。
· 当且用→/『EN弘///17	いぞう シンチュー・トリルホエトリト・トチ	-1900711110/G /H-95/128.S	
· 当其中一个ES头例起 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	o实例的配置实例网络 的。如果A实例配置了
 · 当兵中一个ES头例更 互通页面,也可以看 与B实例的网络打通, 	到刚才配置的ES实例ID, ,则B实例的网络也与A实	;例打地后,在另一个ES 即网络打通操作是双向 例进行了打通。	实例的配置实例网络 的。如果A实例配置了
· 当兵中一个ES头例更 互通页面,也可以看 与B实例的网络打通, 添加成功后,可在修改酌	到刚才配置的ES实例ID, 到刚才配置的ES实例ID, ,则B实例的网络也与A实 记置页面查看与当前实例打	;例打地后,在另一个ES 即网络打通操作是双向 例进行了打通。 通的实例列表。	S头例的配直头例网络 的。如果A实例配置了
· 当其中一个ES头例起 互通页面,也可以看 与B实例的网络打通, 添加成功后,可在修改面 修改配置	日平丁马另一个远柱的ESy 到刚才配置的ES实例ID, ,则B实例的网络也与A实 已置页面查看与当前实例打	;例打地后,在另一个ES 即网络打通操作是双向 例进行了打通。 通的实例列表。	S头例的配置头例网络的。如果A实例配置了
· 当具中一个ES头例更 互通页面,也可以看 与B实例的网络打通, 添加成功后,可在修改面 修改配置	到刚才配置的ES实例ID, ,则B实例的网络也与A实 已置页面查看与当前实例打	;例打地后,在另一个ES 即网络打通操作是双向 例进行了打通。 通的实例列表。	S头例的配置头例网络的。如果A实例配置了
· 当具中一个ES头例成 互通页面,也可以看 与B实例的网络打通, 添加成功后,可在修改面 修改配置 修改配置 ① 支持从同一地域的 功能。请注意: 第 考文档	到刚才配置的ES实例ID, 到刚才配置的ES实例ID, ,则B实例的网络也与A实 已置页面查看与当前实例打 已一账号下,部署在同一VPC内的 等可用区实例和单可用区VPC网络	。例打地后,在另一个ES 即网络打通操作是双向 例进行了打通。 通的实例列表。 ³ 实例进行网络互通,从而实 路之间隔离,不能配置跨集群	≫ 天 例 的 配 重 头 例 网 络 的。 如 果 A 实 例 配 置 了
 · 当其中一个ES实例成 互通页面,也可以看 与B实例的网络打通, 添加成功后,可在修改面 修改配置 修改配置 ① 支持从同一地域版 功能。请注意: 影 考文档 与当前实例打通的实 	到刚才配置的ES实例ID, 到刚才配置的ES实例ID, ,则B实例的网络也与A实 记置页面查看与当前实例打 同一账号下,部署在同一VPC内的 等可用区实例和单可用区VPC网络	(例打) 地后, 在 另一个 EX 即 网络打 通 操作 是 双 向 例 进 行 了 打 通 。 通 的 实 例 列 表 。 9 实 例 进 行 网络 互 通 , 从 而 实 路之间隔离, 不能配置跨集群	≫ 天例 的配 重 头 例 网络 的。如果 A 实 例 配 置 了
 · 当其中一个ES实例成 互通页面,也可以看 与B实例的网络打通, 添加成功后,可在修改面 修改配置 · 支持从同一地域际 功能。请注意: 影 考文档 与当前实例打通的实 实例D 	到刚才配置的ES实例ID, 到刚才配置的ES实例ID, ,则B实例的网络也与A实 记置页面查看与当前实例打 同一账号下,部署在同一VPC内的 等可用区实例和单可用区VPC网络	(例打) 地后, 在另一个ES。 即网络打通操作是双向 例进行了打通。 通的实例列表。 的实例进行网络互通,从而实路之间隔离,不能配置跨集群	≫ 天 例 的 配 重 头 例 网 络 的。 如 果 A 实 例 配 置 了

+ 添加实例

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实例右侧的移除。

修	改配置			\times
	支持从同一地域同一账号下,部署在 功能。请注意:跨可用区实例和单可 考文档	同一VPC内的实例进行网络互 用区VPC网络之间隔离,不能	通,从而实现跨集群搜索 配置跨集群访问。 <mark>详细参</mark>	
	与当前实例打通的实例列表:			
	实例ID	网络类型	操作	
	es-cn-o4 vm	专有网络	移除	
	+ 添加实例			

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 og	专有网络	移除			
	es-cn-o4 wm	专有网络	移除			
	+ 添加实例					

<u>!</u>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-o4xxxxxxx4f1.elasticsearch.aliyuncs.com:
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
9300"
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:
```

- ・単可用区实例,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<sup>"</sup>: 3,
      "skipped" : 0,
"failed" : 0
  },
"_clusters" : {
    "total" : 1,
    "cocful"
      "successful" : 1,
      "skipped" : 0
   },
"hits" : {
      "total" : 1,
      "max_score" : 1.0,
      "hits" : [
         {
            "_index" : "cluster_one:twitter",
"_type" : "doc",
"_id" : "qudxxxxxxxxx_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。

基本信息						
ES樂群配盟	数据备份 (免费试用)					修改配置
插件配置	开启自动舞(3:			自动暂份开始时间:每天 01:00 💡		
集群监控	部份 恢复:	白東音音動和		部份状态: 卢冉音要教程		
日志遭询				700-200 0002		
安全配置	跨集群OSS仓库设置					
数据备份	2005200	利用へまな許	制用人类中于			
	51/0940310	21/3 (2/#4410)	21/82/#4/23		3941 F	
可视化控制	es-cn-78 gp	aliyun_snapshot_from_es-cn-78 gp	✓ 生效		删除仓库	
▼ 智能送维						
集群概况	新増OSS合库引用					
健康诊断						
历史报告						

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。
	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。

参数	说明
修改配置	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。
	自动备份周期设置 ×
	备份周期:每天 备份时间点: 02:00 へ 00:00 01:00 01:00 02:00 √ 03:00 04:00 03:00 04:00 05:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05:00 06:00 05
	 注意: 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	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 <mark>跨集群OSS仓库设置</mark> 。
	 注意: 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。

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。

数据备份 (免费试用)				修改配置
开启自动备份:		自动备份开始时间。	每天 04:00 ⑦	
备份恢复:	点击查看教程	备份状态:	点击查看教程	

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。

自动备份周期设置		
备份周期:	每天	
备份时间点:	04:00	^
	00:00	A
	01:00	
	02:00	
	03:00	
	✓ 04:00	
	05:00	
	06:00	
	07:00	
	08:00	-

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_20180 627091600。 ・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

0

・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_20180 627091600。
- 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-abxxxxxxxlmn_20180628092236",
    "uuid": "n7YxxxxxxxxxxdA",
    "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": Ó.
       "successful": 1
    }
  },
{
    "snapshot": "es-cn-abxxxxxxxmn_20180628092500",
    "uuid": "frdxxxxxxxxxxKLA",
    "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1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-cnabxxxxxxxxxlmn_20180628092236。

返回内容如下:

```
{
  "snapshots": [
    {
      "snapshot": "es-cn-abxxxxxxxxlmn_20180628092236",
      "repository": "aliyun_auto_snapshot",
      "uuid": "n7YxxxxxxxxxxxydA",
      "state": "SUCCESS",
       "shards_stats": {
         "initializing": 0,
         "started": 0,
         "finalizing": 0,
         "done": 1,
         "failed": 0,
         "total": 1
      },
"stats": {
    "mer";
}
         "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
      ".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。

蕢 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
	6,65
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 <mark>存储包、流量包。</mark> 建议您购买资源包享受更多优惠,点 击 <mark>购买。</mark>
Endpoint	oss-cn-hangzhou.aliyuncs.com
存储类型	标准存储 低频访问 归档存储
	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 公共读 公共读写
	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	开通不开通
	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, <mark>了解详情</mark>

```
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",
        "bucket": "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_201 4_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
      }
   }
٦
```

}

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,会只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。

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,
            "shards_stats": 10,
            "state": 10,
            "st
```

```
"started": 1, <2>
                              "finalizing": 0,
                             "done": 4,
"failed": 0,
                              "total": 5
  },
"stats": {
    "bor
                            "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"
        "initialing"
        "initializing"

                                                                              "initializing": 0,
                                                                             "started": 0,
"finalizing": 0,
                                                                             "done": 5,
"failed": 0,
"total": 5
                                                   },
"stats": {
    "sumber"
}
                                                                             "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": {
    "ands": {
    "ands"
                                                                              "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

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"
  "total" : 73,
         "reused" : 0,
"recovered" : 69,
         "percent" : "94.5%" <3>
     },
"bytes" : {
    "total" : 79063092,
    "reused" : 0,
    "recovered" : 68891939,
    "sercent" : "87.1%"
      },
      "total_time_in_millis" : 0
   },
   "translog" : {
"recovered" : 0,
      "total_time_in_millis" : 0
   },
"start" : {
    tack in

      "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题。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。

基本信息			
ES集群配置	数据备份 (免费试用)		
插件配置		开启自动备份:	
集群监控		备份恢复: 点击查看教程	
日志查询			
安全配置	跨集群OSS仓库设置		
新捉条份			
50月田10	引用实例ID	引用仓库名称	引用仓库状态
可视化控制			
▼ 智能运進			未创建其他集群OSS仓库引用 立即添加

3. 在添加引用仓库页面,选择实例。

添加引用仓库			\times
 支持从当前地域 需要恢复数据的 快照仓库进行数 	城同一账号下,更低版本的其他实例 的实例名称,将会为您创建所选实例 如据恢复。详细参考文档	备份与恢复数据, 请选 快照的引用仓库, 您可	择您所 以从该
请选择实例:	es-cn-45 u	~	0
		确认	取消

🕛 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着仓库不存在。
- 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。

 Console
 Search Profiler
 Grok Debugger

 1
 GET /_cat/snapshots
 1
 id
 status start_epoch start_time end_epoch end_time duration indices successful_shards failed_shards total_shards total_shards

 /_aliyun_snapshot_from_pes_en
 1
 id
 status start_epoch start_time end_epoch end_time duration indices successful_shards failed_shards total_shards

 /_aliyun_snapshot_from_pes_en
 2
 es-cn-45
 ju_201910090100006 SUCCESS 1578554016
 17:00:10
 1578554012
 1.55
 3
 0
 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。

<	es-cn-v t
基本信息	
ES集群配置	Kibana
插件配置	
集群监控	
日志查询	
安全配置	QueryBuilder DSL
数据备份	
可视化控制	• 新省Querybuilder/面件,可在修改配置中宣者。 • 强大而便捷的开发工具。
▼ 智能运维	• 时序数据分析、数据图谱分析。
集群概况	相关文档参看Kibana官方介绍 修改配置 进入控制台

3. 在登录页面,输入用户名和密码,单击登录。

Welcome to Kibana Your window into the Elastic Stack	
Username	
Password	
Log in	

- ·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。

		DevTools History Settings Help
	kibana	Welcome to Console
佡	Visualize	Quick intro to the UI
50	Dashboard	The Console UI is split into two panes: an editor pane (left) and a response pane (right). Use the editor to type requests and submit them to Elasticsearch. The results will be displayed in the response pane on the right side.
₽	Timelion	Console understands requests in a compact format, similar to cURL:
寙	Canvas	While typing a request. Console will make suggestions which you can then accept by hitting Enter/Tab. These suggestions are made based on the request structure as well as your indices and types.
۹	Maps	A few quick tips, while I have your attention
۲	Machine Learning	Submit requests to ES using the green triangle button.
G	Infrastructure	Use the wrench menu to comer useful mings. You can paste requests in cURL format and they will be translated to the Console syntax.
J	Logs	You can resize the edulor and output panes by dragging the separation between them. Study the keyboard shortcuts under the Help button. Good stuff in there!
G	АРМ	Get to work
୍ତ	Uptime	Concolo – Sourch Brofiler – Grok Dohumor
÷	Graph	Cursole Search Fruitier Grok Depugger
ę	Dev Tools	1 [ET_search
æ	Monitoring	4 "match_all": {} 5* }
۲	Management	0° }
2	elastic	I I
B	Logout	
	Default	
÷	Collapse	

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、制作数据展示仪表板等操作。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。



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。

<	es-cn-vi 9		
基本信息			
ES集群配置	Kibana	🕎 DataV	
插件配置	•••		
集群监控			
日志查询			
安全配置	QueryBuilder DSL		
数据备份	• 新增Querybuilder插件,可在修改配置中查看,	• 天猫双11、阿里云城市大脑同款数据大屏。	
可视化控制	• 强大而便捷的开发工具。	• 高性能三维渲染引擎。	
▼ 智能运维	• 时序数据分析、数据图谱分析。	 多种图表组件,支撑多种数据类型的分析展示。 	
集群概况	相关文档参看Kibana官方介绍	提入控制台 相关文档参看DataV官方介绍	进入控制台
健康诊断			

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。

<	es-cn-ù k	集群监控	重启实例	刷新	Ξ
Kibana 🍋	基本設置			修改配	
	Kharaellin Ergion				

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。

修改Ki	bana基本配置	
		1
	修改语言: 💿 中文	
	🔿 English	
		-
~		

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。

K	kibana	◎ 吉蒙在 Kibana 中可現代和政府政策, S·用業的建築引模式, SJA, Elasticsearch 检索数据。			
Ø	Discover	Dev Tools	历史记录	设置	帮助
旈	可把化	欢迎使用 Console			0
50	仪表板	u ian			
₽	Timelion	Console UI 分成两个雪格:蝙蝠器雪格(左),他用蝙蝠器镶入谦求并将它们提交到 Elasticsearch,结果将显示在右髂的响应雪格中。			
寙	Canvas	Console 理解意赅推动的意志,类似于 cURL:			
2	Maps	键入请求时,Console 将提供建议、您可以通过按Enter/Flab 键来接受建议。这些建议基于请求结构以及忽的法书用关系回出,			
æ	Machine Learning	有几个需要郑注意的有用提示			
G	基础设施	 使用语色二角纹记术请求度交到 E5, 適用時に考慮的に考慮的意思 			
Ē	志	19回び以降市(以此)時式(約束)、反应要方用等時級にConcole 田田市式、 9回び以降市(以此)時式(約束)、反应要方用等時度の(19)(19)(19)(19)(19)(19)(19)(19)(19)(19)			
Ę	АРМ	● ○ ● 小田田市市で加加した。○ 小田市市市大部分に通知/ 「 ● 子写 考慮/ 旧石下の機会(場合) 元、 部国市市本大部分(通知)			
- 1	远行时间	Heire			
,	Curch				
***	Graph	Console Search Profiler Grok Debugger			
Ŷ	开发工具	1 Ef_search			
æ	Monitoring	3 [•]			
۲	管理	6-) ²			
2	elastic				
B	注销				
	Default				
÷	折叠				

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。

<	es-cn-vi 9		
基本信息			
ES集群配置	Kibana	🕎 DataV	
插件配置	***		R1-HAR
集群监控			
日志查询	· · · · · · · · · · · · · · · · · · ·		
安全配置	QueryBuilder	DSL	
数据备份	• 新增Querybuilder插件,可在修改配置中查看。	• 天猫双11、阿里云城市大脑间款数据大屏。	
可视化控制	• 强大而便捷的开发工具。	• 高性能三維渲染引擎。	
• 智能运维	• 时序数据分析、数据图谱分析。	 多种图表组件,支撑多种数据类型的分析展 	7 .
集群概况	相关文档参看Kibana盲方介绍	改配置 进入控制台 相关文档参看DataV官方介绍	进入控制台
健康诊断			

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。

<	es-cn-\	集群监控 重胆实例 見账 三
Kibana配置	基本配置	传达影漫
	Kibana语言配册: English	
	访问配置	
	Kibana公网访问:	Kibana访问白名单: 特数

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。



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。 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。

三〕 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	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。

<	es-cn-v(9	
基本信息		
ES集群配置	Kibana	🕎 DataV
插件配置		
集群监控		
日志童询		
安全配置	QueryBuilder DSL	
数据备份	• 新増Querybuilder插件,可在修改配置中查看。	• 天猫双11、阿里云城市大脑间款数据大屏。
可视化控制	• 强大而便捷的开发工具。	• 高性能三维渲染引擎。
* 智能运進	 时序数据分析、数据图谱分析。 	• 多种图表组件,支撑多种数据类型的分析展示。
集群概况	相关文档参看Kibena首方介绍 修改配置 进	进入控制台 相关文档参看DataV官方介绍 进入控制台
健康诊断		

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。



- ·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。

<	es-cn-v 9			
Kibana配置	访问配置			
	Kibana公网访问: C	C		Kibana访问白名单: 0.0.0.0/0 修改
	1411 1 Houses	40+	ente	48 14-
		· □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □		324T E 30383
	network_vis	 ● 未安装 	通过家引的两个字段,可以生成这两个字段的网络关系图	安装
门 说明	月:			

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。



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)。

	预付费	后付费					
	地域	华东1 (杭州) 香港	华北2 (北京) 美国 (硅谷)	华东2 (上海) 马来西亚 (吉隆坡)	华南1 (深圳) 德国 (法兰克福)	印度 (孟买) 日本 (东京)	新加坡 澳大利亚 (悉尼)
1999	可用区	印度尼西亚(雅加达) 上海可用区B	华北1 (青岛)	华北3 (张家口)			
资源组	资源组	全部	▼ 및	以资源组	•		
	版本	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<u>集群升配</u>。

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。

<	es-cn-vi 9			
基本信息				
ES集群配置	Kibana		🕎 DataV	
插件配置		•••		
集群监控				
日志查询	·····			
安全配置	QueryBuilder	DSL		haling and a second
数据备份	• 新增Querybuilder插件,可在修改配置中查看。		• 天猫双11、阿里云城市大脑同款数据大屏。	
可视化控制	• 强大而便捷的开发工具。		• 高性能三维渲染引擎。	
▼ 智能运维	• 时序数据分析、数据图谱分析。		• 多种图表组件,支撑多种数据类型的分析展示。	
集群概况	相关文档参看Kibana官方介绍	修改配置 进入控制台	相关文档参看DataV官方介绍	进入控制台
健康诊断				

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。



- ·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。

<	es-cn-v 9			
Kibana配置	访问配置			
	Kībana公网访问:			Kibana访问白名单: 0.0.0.0/0 修改
	插件配置			
	□ 插件名称	状态	描述	操作
	her had hit	● 已安装	Reference and the second	卸载
	network_vis	● 未安装	通过索引的两个字段,可以生成这两个字段的网络关系图	安装
道 说明	月:			
此过程可能	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。



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。

		2 hits				New	Save Ope	n Share Query	Reporting	C Auto-refresh
	kibana	email · 通配符(Wildcard)	v *iga*]				2		0
Ø	Discover	-+-=		3						
	Visualize	submit								
୍ଦ	Dashboard									
	Timelion	Search (e.g. status:200 AND extension:PHF	P)						c	ptions Q
65	Machine Learning	Querybuilder0 Add a filter +								Actions -
=	APM	All filters: Enable Disable Pin Unpin Invert Te	oggle Remove							
- 44	Granh	megacorp	_source							1
بر	Dev Tools	Selected Fields	• ensil: p2iga@123.com first_mane: p2	2 last_mane: Smith age: 27 about: I	love to go rock climbing inter	ests: sports, music _id: 5 _type	employee _	index: megacorp _se	tore: 1	4
	Monitoring	? source	• enail: John_igabbhg.com first_neme:	John last_nome: Smith age: 25 abou	t: I love to go rock climbing	interests: sports, music _id: 1	type: employ	ee _index: megacon	p_seere: 1	
٥	Management	Available Fields Ø								-
		t _id								
		t _index								
		# _score								
24	+++	15 LPAA	コンストロー 人 大く	治友体、公士		山よろう		–)-+M	+ 11	
単	古宣判	区或的	可添加一个鱼	削 涂忤; 単击	יר זי	」万宣判添加	→ ⁄[于过况	家们	;単
-										
击	<u> </u>	□可删除一个 杳	询或过滤条件。	, ,						
		4 ANALAN 1								
	× ×									

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。

email	•	通配符(Wildcard)	Y	*iga*]_	•	×
+ ====							
submit							

最终得到的匹配结果如下。

Add a filter +														Actions +
kibana_sample_data_ecommerce	• 0						2018-04-24 14:11:12 - 2	2019-04-24 14:11:12 - Auto	0					
Belisoted fields 1 custome_fing_name 1 custome_gendar 1 mmli	3	33 22 33 34 25 35 35 36 35 35 35 35 35 35 35 35 35 35 35 35 35	2010-06-01	2018-07-01	2018-08-01	2018-08-01	2018-10-01	2018-11-01	2018-12-01	2018-01-01	2019-02-01	2019-03-01	2019-04-01	
# takki_totai_price Available fields G	•							order_date per week						
t_id		Time	customer_gender		customer_first_name			email				taxful_total_price		
t _index		2019-03-09 11:33:07	FEMALE		Abigail			abigail@salazar-fam	ily.zzz			69.98		
# _score		2819-84-84 19:88:58	FEMALE		Abigail			abigail@banks-famil	y. 222			53.98		
t_type		2819-03-29 04:21:07	FEMALE		Abigail			abigail@potter-fami	ly.222			47.99		
t category		2819-03-22 04:38:24	FEMALE		Abigail			abigail@farmer-fami	ly.zzz			66.98		
t currency	1.5	2819-03-14 10:58:34	FEMALE		Abigeil			abigail@powell-fami	ly-222			93.98		
t customer_Ail_name	1.5	2819-04-06 17:08:38	FEMALE		Abigail			abigail@villis-fami	ly.zzz			117.98		
# customer_id	1.5													
t customer_last_name		2019-03-17 00:40:00	PERMIT		Abigait			801981(09008w1h-Tan	aty.222			110.96		
t customer_phone		2019-04-01 00:00:29	FEMALE		Abigail			abigail@webb-family	.222			147.98		
t day_of_week		2819-03-22 09:17:46	FEMALE		Abigail			abigail@webb-family	. 222			53.98		
# day_ot_week_i		2019-03-20 00:56:38	FEMALE		Abigail			abigail@perry-famil	y. 222			43.98		

・多条件组合查询

下图的查询条件表示index必须为tryme_book,同时要对type 进行过滤,要求type等于大学教辅、数学、对外汉语教学或大学教材。

		•	也留E(Match)	•	大学教辅	×
-[type	\$	匹配(Match)	\$	数学	×
-	type	\$	匹配(Match)	\$	对外汉语教学	×
-	type	\$	匹配(Match)	\$	大学教材	_ ×

最终得到的匹配结果如下。

_querybuilderAdd a filter +		Actions
tryme_book	• 0	6006
Selected fields		· Date: Concernent Apple Registrer Registrer Registrer and Registrer R
? _source Available fields	•	* James 1996 Jost type 7 8 8 moders 828 prior 0 Annali jon palate REBRING anno BERGEROUSE SECONFORCEDE Lake jon balle jon later CREDEROUSEREDEREDERED. ERECTRONOMENT, AFORDER CREDERED. Later 1 year too Lake 1990 Jost CREDERED.
Popular t author		* Inter Type, Dok type (XTEX Inter: LACKER, CARES, ATURN print # Mindi pro patient RTERIES and RTERIES and RTERIES for the CARE REAL CONTRACT SHE (M) Inter () [M M [M M [M M [M M [M M
t helo t index		* Jahre Type, 20 K Vanher, 80 price, 8 Jahre Jon Jahre Jahren Jon Jahren TRATADA Jane BATTRYTYPERUMMERSPEE STATES ACCOMPTENT LANS Jon Jahr Jon Jahr (Syletan) 2"ST-6764521" SUNDER, UN PALS, DS SUNDER, UN PALS, DS SUNDER, DS SUNDE
t info t label		* Dame Typezine Type (X T KT Hame) 20.7 FT prime (Tame) (To partial X TETATA Hame) XTETATA Hame) XTETATA Hame) XTETATA Hame) To Hame) Typezine (X T KT HAME) Typezine (X
t name # price		* Laine type, 24 type, 24 type, 24 type, 24 andre, 20 20 Derrol-P.) priori # Annel (FM paine AREFAULT ANNE AREFAULT ANNE AREFAULT AND ANNE AREFAULT
t publish t type		* Jahon Type, Dek Type, N. Maker, D.S. P.E. price, F Makel jon paking REFEASE mane EXTENTTHERMENTERP46 CIEF9930001088 DDD label jon Maker (RIF199300010886000 [ac] type; box
t Animal t .)d t .index		District Topellow Type: 2 8 M Instruct REALERS ADDRESS ADDRESS To ADDRESS TO ADDRESS ADDRES
# _score 1 _type		* Jaden: frymt, best type: 2,9 8.0 ander: 2010 prior: 0 Animal: jon publich: AVERTORS name: 2010/00/07 (2010) label: jon Jaden: jon Jaden: 100/05/00/07/828 [doi:10.10].paper box [laben: type,box [laben: type,box].01

・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。

- ×	days	240	最近几天(In the last) ♦	\$ utc_time
				+ 🔳
				+ - III

最终得到的匹配结果如下。

querybuilder Add a filter +													Actions	
kibana_sample_data_logs	•	0					2018-04-24 14:19:53 -	2019-04-24 14:19:53 - Auto	0					
Selected fields		1,500												
7 _source Available fields	۰	1,000 - 500 -												
t_id t_index		2018-05-01	2018-06-01 2018	07-01	2018-08-01	2018-09-01	2018-10-01	2018-11-01	2018-12-01	2019-01-01	2019-02-01	2018-03-01	2018-04-01	
# _score		Time -	source					timestamp per week						
t _type t agent		> 2819-04-24 14:08:49	referer: http://facebook.com/su	cess/lloyd-harmond	elientip: 230.114.	21.43 responses 28	0 tagas success, 1	nfo message: 230.114.21.43	[2018-09-12T05:00:	49.599Z] "GET /styles/	app.css HTTP/1.1" 200	8700 "-" "Mozilla/5.0	(X11; Linux 1686) AppleMebKit/	
# bytes			s wels https://cdn.elastic-elast like Geckp) Chrome/11.0.696.50 Su	ic-elastic.org/styl	es/opp.css memory: 0.114.21.43 bytes:	- host: cdn.elas 8,700 timestamp:	tic-elastic-elastic	.org utc_time: 2018-09-12 1	14:00:49 machine.ram:	7,516,192,768 machine.	osi ios agenti Mozil	la/5.0 DK11; Linux if	186) AppleWebKit/534.24 (KHTML,	
t extension		· 2019-04-24 13:53:53	referer: http://www.elastic-elas	tic-elastic.com/suc	cess/steven-lindsey	clientip: 158.64.	134.248 response:	200 tage: success, info me	ssager 158.64.134.248	[2018-09-12705:53:	53.1192] "GET / HTTP/1	.1" 200 5139 "-" "Mos	illa/4.0 (compatible; MSIE 6.0;	
# geo.coordinates.lat # geo.coordinates.lat			Windows NT 5.1; SV1; .NET CLR 1.1 nemery: - bost: www.elastic.co	4322)" request: / utc_time: 2018-09	geo.srcdest: RU:R -12 13:53:53 machin	U geo.src: RU geo se.ram: 19,327,352,	dest: RU geo.coor 832 machine.os: 01	dinates.lat: 42.557 geo.coo x agest: Mozilla/4.0 (comp	atible; MSIE 6.0; Windo	tonemory: - extension ws NT 5.1; SV1; .NET C	un index: kibana_sam UR 1.1.4322) ip: 158.	ple_data_logs url: * 64.134.248 bytes: 5,	ttps://www.elastic.co/downloads 139 timestamp: 2019-04-24 13:5	
t pro.dest			3:53 _idi _6EffNkBQm0RQo-IrSlw	type: _doc _index	<pre>x kibana_sample_dat</pre>	a_logs _score: -								
t geo.arc		> 2019-04-24 13:43:11	referer: http://facebook.com/sur	cess/donald-holmque	st clientip: 117.2	14.211.68 response	200 tags: succes	s, info message: 117.214.21	11.68 (2018-09-1270	5:43:11.283Z] "GET /eb	asticsearch/elasticsea	rch-6.3.2.deb HTTP/1.	1" 200 8491 "-" "Mozilla/5.0 (X	
t geo.arcdest			bana_sample_data_logs wrls http:	//artifacts.elasti	c.co/downloads/elas	ticsearch/elasticse	arch-6.3.2.dtb men	ny: - host: artifacts.ela	istic.co uto_time: 201	8-09-12 13:43:11 machi	me.ram: 6,442,450,944	nachine.os: win 7	agent: Mozilla/5.0 (X11; Linux	
t host			x86_64; rv:6.@a1) Gecko/20110421	Firefox/6.0a1 ip:	117.214.211.68 byt	anı 8,491 timestam	pi 2019-04-24 13:43	:11 _14: A6EffNkBQmBRQo-Irt	Spy _type: _doc _inde	<pre>kibana_sample_data_</pre>	logs _score: -			
t ip		> 2019-04-24 13:42:14	referer: http://twitter.com/warn (KORDE. like Gerko) Chrome/11.8.6	ing/patrick-baudry	elientip: 122.62.2	33.39 responses 54	3 tage: success, 1	nfo message: 122.62.233.59	[2018-09-12705:42:	14.0172] "GET /enterpr	ise HTTP/1.1" 503 0 "-	" "Mozilla/5.0 (X11;	Linux 1686) AppleWebKit/534.24	
t machine.os			s://www.elastic.co/downloads/ente	rprise memorys -	host: www.elastic.	co ute_time: 2018-	09-12 13:42:14 mag	hime.rom: 15,032,385,536 mm	chine.os: ios agent:	Mozilla/5.0 (X11; Linz	x i686) AppleWebKit/53	4.24 (KHTNL, Like Geo	ks) Chrome/11.0.696.50 Safari/5	
# machine.ram			34.24 kpi 122.62.233.59 byteei	timestamp: 2019-	04-24 13:42:14 _64	<pre>xattwk8Qm8RQo-I;</pre>	Twc "alles "goc "	<pre>kmdex: kibana_sample_data_li</pre>	ogs _ecore: -					

结合以上说明,构造一个复杂的查询条件,如下图所示。

publi	ish \$ 匹配 AND \$ ×	(Match) \$ 高等	等教育出版社		
	type \$	匹配(Match) 💠	数学	×	
-	type \$	匹配(Match) \$	学习方法	×	
-	price \$	小于等于(<=) ◆	20		×
	name	e ◆ 通配符(Wildcard	d) ◆ - *数学*	- ×	
		e \$ 通配符(Wildcard AND \$ × info \$ 匹配(Mat	d)	X	
		e \$ 通配符(Wildcard AND \$ × info \$ 匹配(Mat + Ⅲ	d)	X	
		e \$ 通配符(Wildcard AND \$ × info \$ 匹配(Mat + Ⅲ	d)	X	

而实际对应的DSL如下图所示。



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<mark>集群升配</mark>。

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。

<	es-cn-v(9	
基本信息		
ES集群配置	Kibana	V DataV
插件配置		44120717717
集群监控		
日志查询		
安全配置	QueryBuilder DSL	
数据备份	• 新增Querybuilder插件,可在修改配置中查看,	 天猫双11、阿里云城市大脑同款数据大屏。
可视化控制	• 强大而便捷的开发工具。	 高性能三維道染引擎。
▼ 智能运進	 时序数据分析、数据图谱分析。 	• 多种图表组件,支撑多种数据类型的分析展示。
集群概况	相关文档参署Kibena直方介绍	相关文档参看DataV官方介绍进入控制台
健康诊断		

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。



<	es-cn-v 9								
Kibana配查	访问配置								
	Kībana公网访问:	Kibana公司访问 CO							
	插件配置								
	播件名称	状态	描述	操作					
	 Instantility 	 ● 已安装 	551.741-8181	印號					
	network_vis	● 未安装	通过索引的两个字段,可以生成这两个字段的网络关系图	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。



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。

	kibana	1 次命中				新建 保存 打开	共享 检查 打标 C 自动刷新
	KIDalla	()自定义打标字段					۵
Ø	Discover	确认打标 age 👻	18				
旈	可视化	. 471500/0					
50	仪表板	▶ 打标明細 (「タ」D	走り点	17 42 441-4	77-5449-323	25 0-1/20 V	正在打标 () 《 》 0/0
₩	Timelion	仕方し	添加面	性穷锢还	开始时间	*七中」(化少)	近度(更新致/忘数)
	Maps	> 埋委 (例加 status-200 AND	extension-PHP)				送面 C Refresh
	3# 2010 to	7- 按承 (四知, Status.200 AND	extension.rnr/				运动 C Refresh
	亚山 议派	name: "张三" Add a filter +					Actions >
E	日志	tryme_book • 0	_source				
3	运行时间	选定字段 ? source	name: 💥 age: 20	gender: male hobby: 篮球、羽毛球	_id: 02nhb2wBE5ASBS1TNWN4 _	type: _doc _index: tryme	e_book _score: 1.575
ę	开发工具	可用字段 •					
0	管理	t _id					
		t _index					
		# _score					
		t _type					
		# age					
		t gender					
		t name					
X	默认值						
÷	折叠						

打开历史打标开关,可查看历史打标任务详情。

	kibana	1 次命中				新建 保存 打开	共享 检查 打标 C 自动刷新
	RIDalla	自定义打标字段					0
Ø	Discover	确认打标 请选择打标字段 ▼	请输入打标内容				
旈	可视化						
50	仪表板	▶ 打标明细 (「タ」D	走过点	17 A2 441 34	77 4/4 (9+4/23)	\$5.0×7.5h	历史打标 () * 1/1
₩	Timelion	社会 ID DpTSx75xSiOwI7rT6HdYw:	家51名 tryme_book	位务细处 update-by-query [tryme_bo	2019-08-08 15:23:02	彩印(初)	出度(更新致/忌数) 1/1
,Q,	Maps						
Å	JILDHIG MA	>_ 搜索 (例如, status:200 AN	D extension:PHP)				洗顶 C Refresh
	日志	Add a filter +	•				Actions •
3	运行时间	tryme_book •	_source				
铅	开发工具	? _source	' name: <mark>%</mark> Ξ gender:	male age: 18 hobby: 篮球、羽毛球	_1d: 02nhb2wBE5ASBS1TNWN4 _	type: _doc _index: tryme_	book _score: 1.575
٩	管理	可用字段 •					
		t_id					
		t _index					
		* _score					
		# age					
		t gender					
	默认信	t hobby					
		t name					
÷	折叠						

・新増字段进行打标。

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。

	kihana	1次命中					新建 保存 打开	共享 检查	丁标 С自动刷新
	Ribana	■ 自定义打标字段							0
Ø	Discover	确认打标 tag		teenager					
£	可视化								
罰	仪表板	▶ 打标明细					descention of the form	历史打标) < > 1/1
57	Timelion	任务 ID DoTSx75xSiOwi7rT6HdW		索引名 to/me_book	任务描述	开始时间 2019-08-08 15:23:02	耗时(秒)	进度(更	新数/总数)
Ŵ	million	oproxisiowintender	•	dynie_book	update-by-query [if yme_bo	2019-00-00 15:25:02	0.2000		.,,,
\$	Maps								
â	基础设施	>_ 搜索(例如, statu	is:200 AND	extension:PHP)				选项	C Refresh
I	日志	name: "3K三" Ad	ld a filter 🕇						Actions >
্য	运行时间	tryme_book	• 0	_source					
<u>ب</u>	##T8	选定字段		name: 张三 gender:	male age: 18 hobby: 篮球、羽毛球	_id: 02nhb2wBE5ASBS1TNWN4 _	type: _doc _index: tryme	_book _score: 1	.575
	/////	? _source							
0	管理	可用字段	¢						
		t ju							
		t _index							
		# _score							
		t _type							
		# age							
		t gender							
-	默认值	t hobby							
-		t name							
÷	折叠								

查看打标结果。

		1 次命中					新建	保存	打开	共享	检查	打标	C自动刷新
	kibana												0
Ø		自定义打标字段 确认打标 请选择打标字段	Q •	请输入打标内容									
佡	可視化												
8	似夷垢	▶ 打标明细								D.	使打标		(> 1/2
80		任务 ID		索引名	任务描述	开始时间		耗时(秒)			进度	建更新数	/总数)
V	Timelion	DpTSx75xSiOvvl7rT6HdYw:		tryme_book	update-by-query [tryme_bo	2019-08-08 16:34:21		0.0849				1/1	_
٩	Maps	DpTSx75xSiOwI7rT6HdYw:		tryme_book	update-by-query [tryme_bo	2019-08-08 15:23:02		0.2860				1/1	
â	基础设施												
I	日志	>_ 搜索(例如, status:2	00 AND	extension:PHP)							选项	0	Refresh
1	运行时间	name: "號三" Add a	filter +										Actions •
e	开发工具	tryme_book •	0	_source									
		选定字段	•	name: 💥 gender:	male tag teenager age: 18 hob	by: 篮球、羽毛球 _id: 02nhb2wB	ESASBS1TN	N4 _ty	pe: _do	c _inde	ex: tryp	me_book	
0	管理	? _source		_score: 1.575									
		可用字段											
		t_id											
		t _index											
		# _score											
		t _type											
		# age											
	默认值	t gender											
-		t hobby											
÷	折叠	t name											

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_6₀
- · 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。
- 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。

😂 我的可视化	回我的数据 1 条 我的组件 合:数程	A	
数据源管理	+ 35008908	・ 発型 Elastic Search 3	査看数据源文档
[-] 代码片段管理	MySQL	自定义数据源各称	
		"Region 华东1	
		使用前请授权 DataV 访问 实例D	
		"密码	
			确定



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。

「云澄潭坊间接仅	
温馨描示:如雪修改角色fQIR、语前往RAM检制台角色管理中设置,雪蒙注意的是,情况的配置可能导致DataV无法获取到必要的仅用。	×
DataV请求获取访问您云资源的权限 下方是系统创建的可供Dutav使用的角色,接权后,Datav模构对你云资源相应的访问权用。	
AllyunData/AccessingElasticSearchkole	
mebi UNENVIKUU思想起的回题过发发展 乾限描述:用于Data收载面可吸化服务角色的接收策略,包含Elastix.Search的部分权限	
員感授祝 取消	

! 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 <u>基本信息概览</u> 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。

😂 我的可视化	奴 我的数据	& 我的 组件	合教科			- Jan Jack	
+ 添加数据						按类别筛选▼	按修改时间
Elastic Search		2019/5/17 下午6:52:51	1	csv 🖉	M3r	2019/5/16 上午11:0	
					,		
Elastic Search	rwerAA	2019/5/15 下午7:13:12	2	Elastic Search	234234	2019/5/15 下午7:1	

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{}。

数据源类型		
Elastic Search		-
选择已有数据源:		
ES	•	新建
index :		
*		
Query :		
1 { 2 "time":"2019-02-23",		
3 "keyword":"datav" 4 }		

7. 单击查看数据响应结果,数据响应成功后即可看到效果。