Elasticsearch Service

数据应用指南

腾讯云

文档目录

数据应用指南
数据应用概述

最近更新时间：2024-10-30 17:12:01

数据应用是构建在腾讯云 Elasticsearch Service（ES）中的一站式数据接入与管理服务，能够帮助您实现数据链路可视化接入以及云端的索引可视化管理，相对于传统的数据接入、手工索引创建与管理而言，可以大大的降低使用与维护成本。
数据接入提供了 CVM 与 TKE、MySQL 等数据源的接入，只需在界面上填写链路中相关组件的配置信息或者遵循相关指引，即可快速完成整个链路的创建。
数据管理提供了索引创建、检索分析、索引监控、配置管理等多项服务，协助用户通过简单易用的可视化界面进行数据管理。同时，数据管理特别推出由腾讯云自研的 自治索引，自治索引能够提供**自动化的索引生命周期管理和分片自动调优，并有效提高读写效率，降低管理与维护成本**，适用于时序数据（例如日志分析、运维监控等）场景。

功能概览

数据接入主要提供以下功能，详情请参考 数据接入：

- 日志接入：支持 CVM 以及 TKE 等数据源的日志采集。
- 指标接入：支持 CVM 等数据源的指标采集。
- 数据同步：指引您进行 MySQL 等数据源的同步。

数据管理主要提供以下功能：

- 索引创建：提供简单易用的**可视化界面**以及灵活的 **JSON 编辑模式**，有效降低索引创建成本。详情请参考 新建自治索引 。
- 索引检索分析：支持通过索引列表一键跳转到对应的 Kibana 页面，快速实现索引的检索与分析。详情请参考 索引检索与分析 。
- 索引基础信息：支持在控制台查看索引的相关信息，以及进行后备索引的管理。详情请参考 索引基础信息 。
- 索引监控：提供了索引粒度的丰富的监控指标，可以帮助在索引使用过程中查看索引的实时监控数据。详情请参考 索引监控 。
- 索引配置管理：索引管理中心支持在控制台灵活地进行索引配置信息的修改，以适应业务的变化。详情请参考 索引配置管理 。

数据接入

最近更新时间：2025-04-21 17:41:12

前提条件

已创建腾讯云账号，创建账号可参考 注册腾讯云 。

操作步骤

进入新建页面

1. 登录 ES 控制台，单击**数据接入**，进入数据链路列表。
2. 单击**新建数据链路**，进入新建页面。

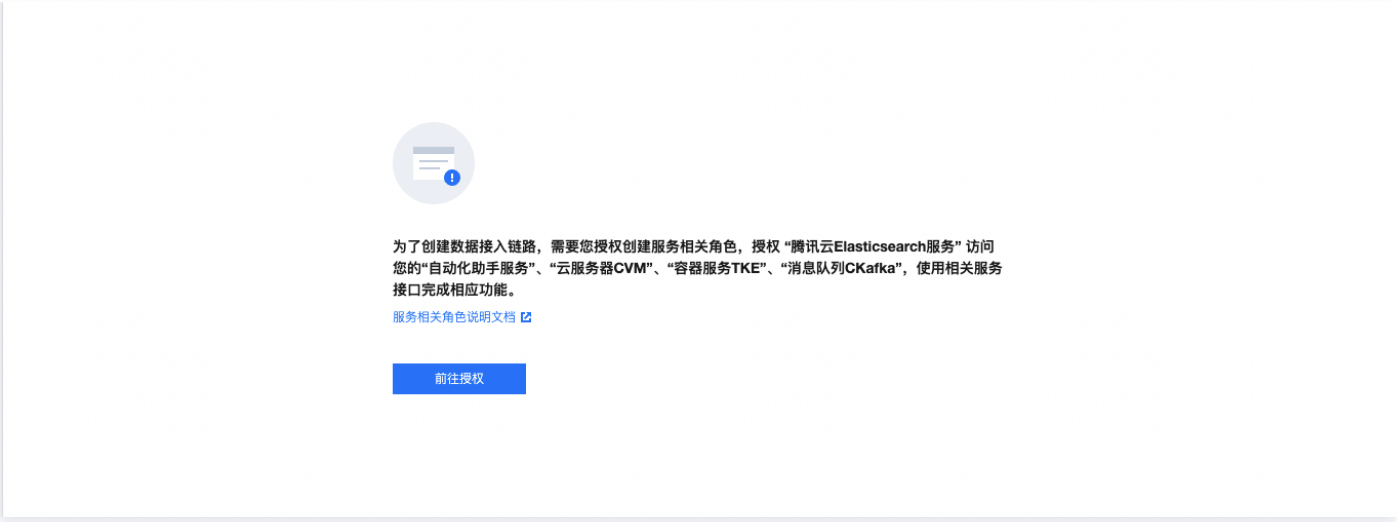
数据链路配置

填写数据链路基本信息

1. 填写数据链路名称，将根据该名称自动生成数据链路 ID。
2. 选择地域，后续数据链路的相关组件与资源，都将来自该地域。
3. 选择数据源，当前日志场景支持 CVM 与 TKE 等数据源、指标场景支持 CVM，后续将支持更多的数据源，其他数据同步配置如 MySQL 等可通过相关文档指引进行。
4. 单击**开始创建**，将进入数据链路组件配置页面。

进行数据链路组件配置

1. 建议数据链路各个组件在同一个 VPC 以保证网络互通，否则您需要自行打通网络连接。详情可参见 云联网 CCN 。
2. 通过选择**数据链路模式**，可切换该链路组件配置。
3. 为了创建数据接入链路，通过助手下发配置时，要使用用户密钥，初次点击“新建数据链路”时，需要您授权创建服务相关角色，授权“腾讯云 Elasticsearch 服务”访问您的“自动化助手服务”、“云服务器 CVM”、“容器服务 TKE”、“消息队列 CKafka”，使用相关服务接口完成相应功能。



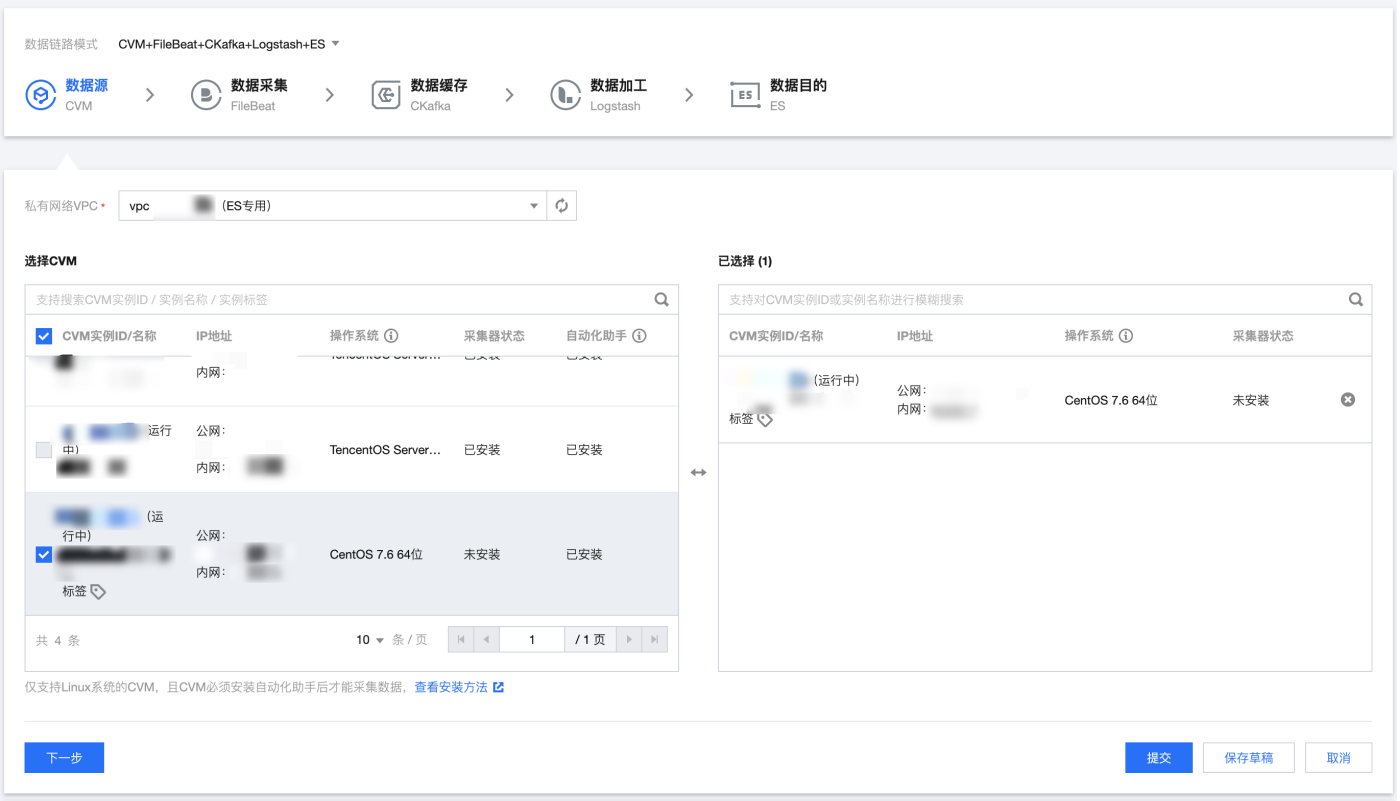
以下将通过 CVM 及 TKE 两个日志采集链路的配置进行相关说明。

CVM-Filebeat-CKafka-Logstash-ES

数据源

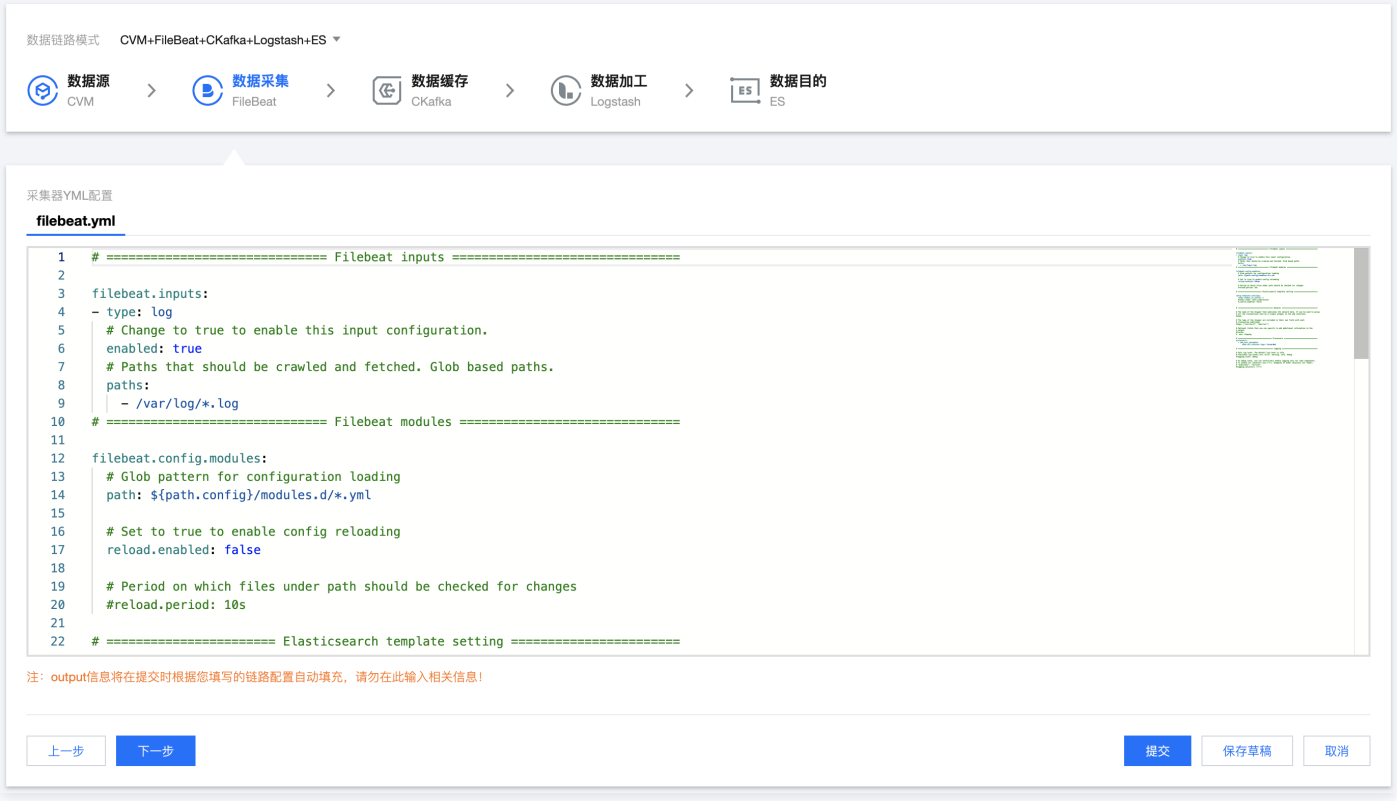
1. 选择 VPC。

2. 选择 CVM，仅支持 Linux 系统的 CVM，且 CVM 必须安装自动化助手后才能采集数据。查看安装方法 。



数据采集

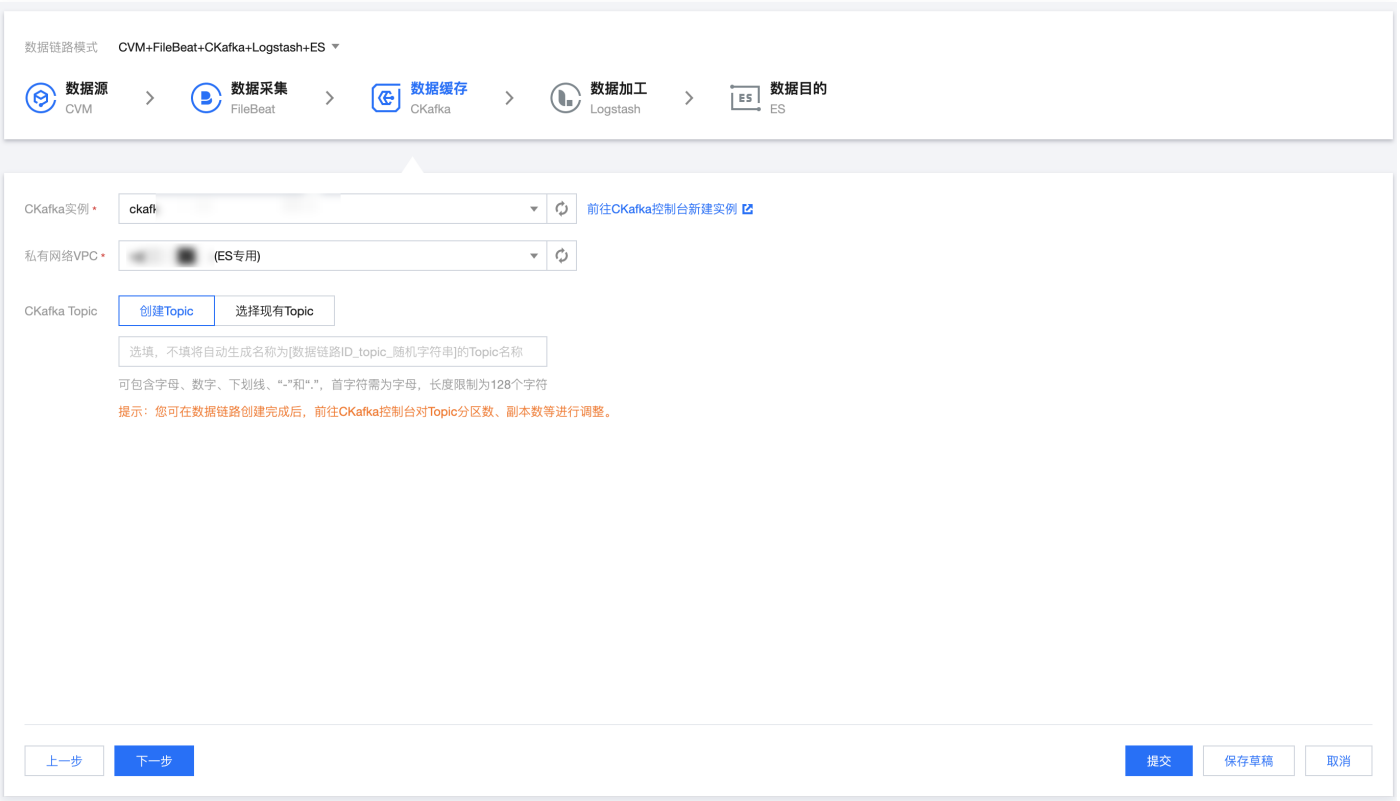
1. 填写采集配置相关内容。
2. output 信息将在提交时根据您填写的链路配置自动填充，请勿在此输入相关信息。



数据缓存

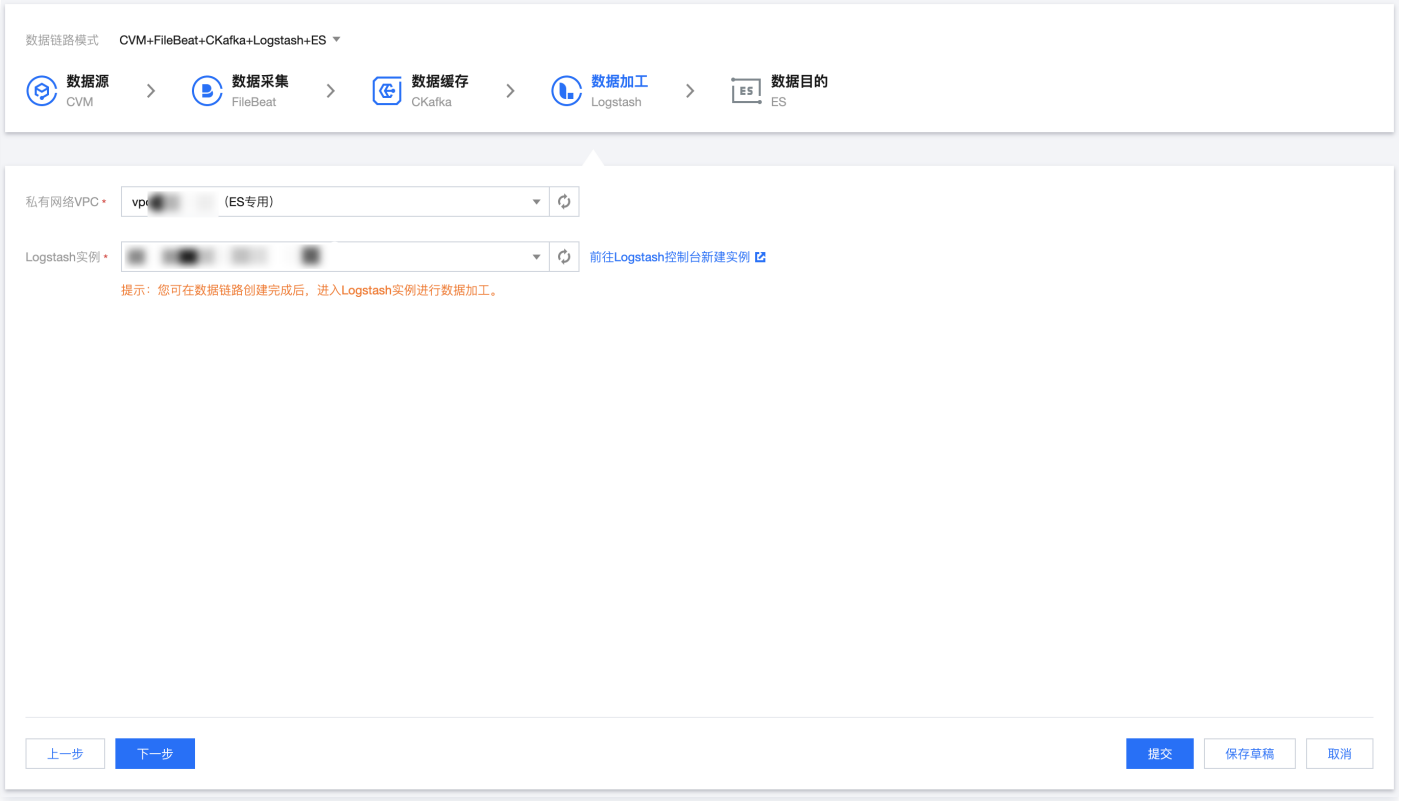
1. 选择 CKafka 实例。

2. 从 CKafka 实例已经路由打通的 VPC 中，选择跟当前链路组件有交集的 VPC。
3. 创建或者选择已有 Topic，当选择**创建 Topic** 时，如您未填写 Topic 名称，将自动生成格式为{数据链路 ID_topic_ 随机字符串}的 Topic 名称。



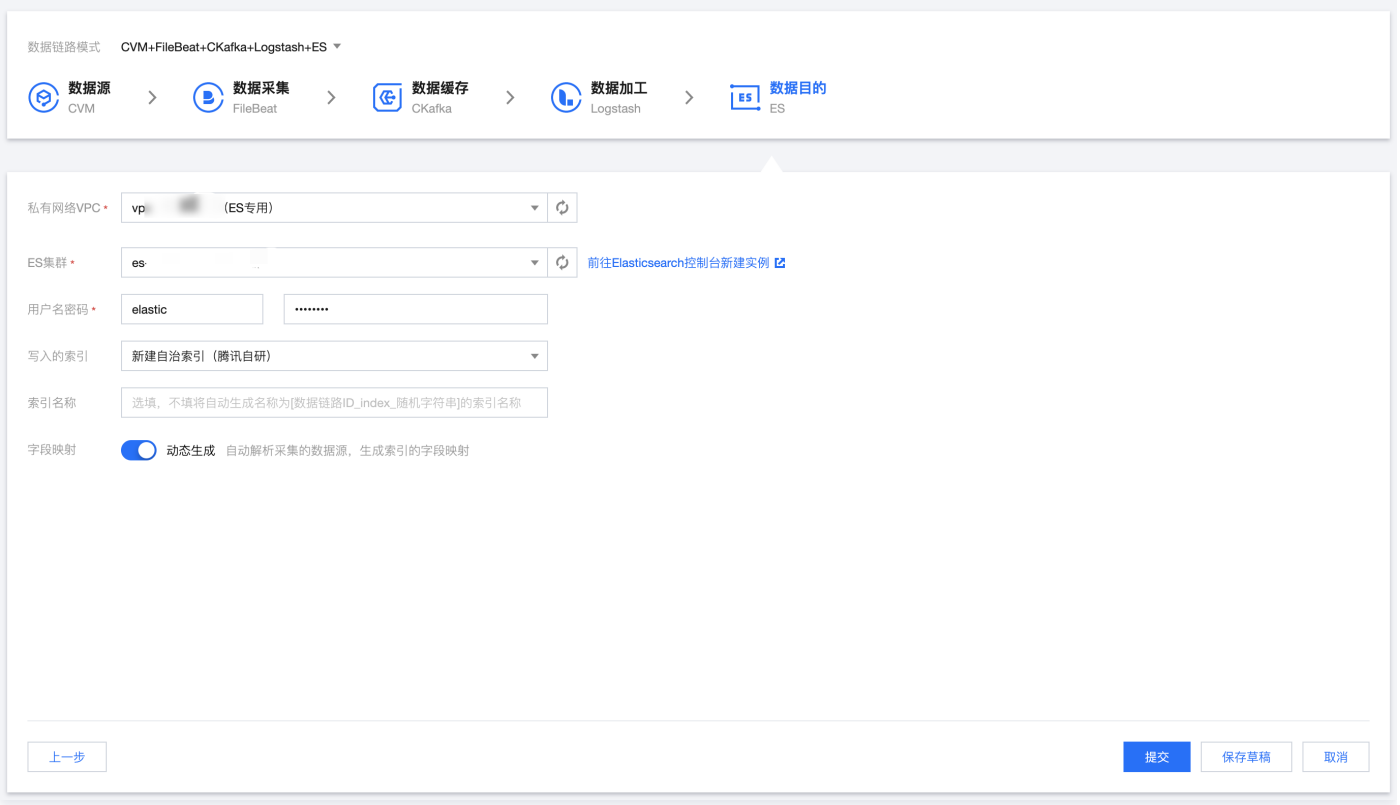
数据加工

1. 选择 VPC。
2. 选择 Logstash 实例。
3. 生成数据链路时，将自动在该实例下创建名称为{数据链路 ID_lgpipe_ 随机字符串}的管道，如需对数据进行加工，可在数据链路创建完成后到对应的 Logstash 实例下修改相关管道的配置。



数据目的

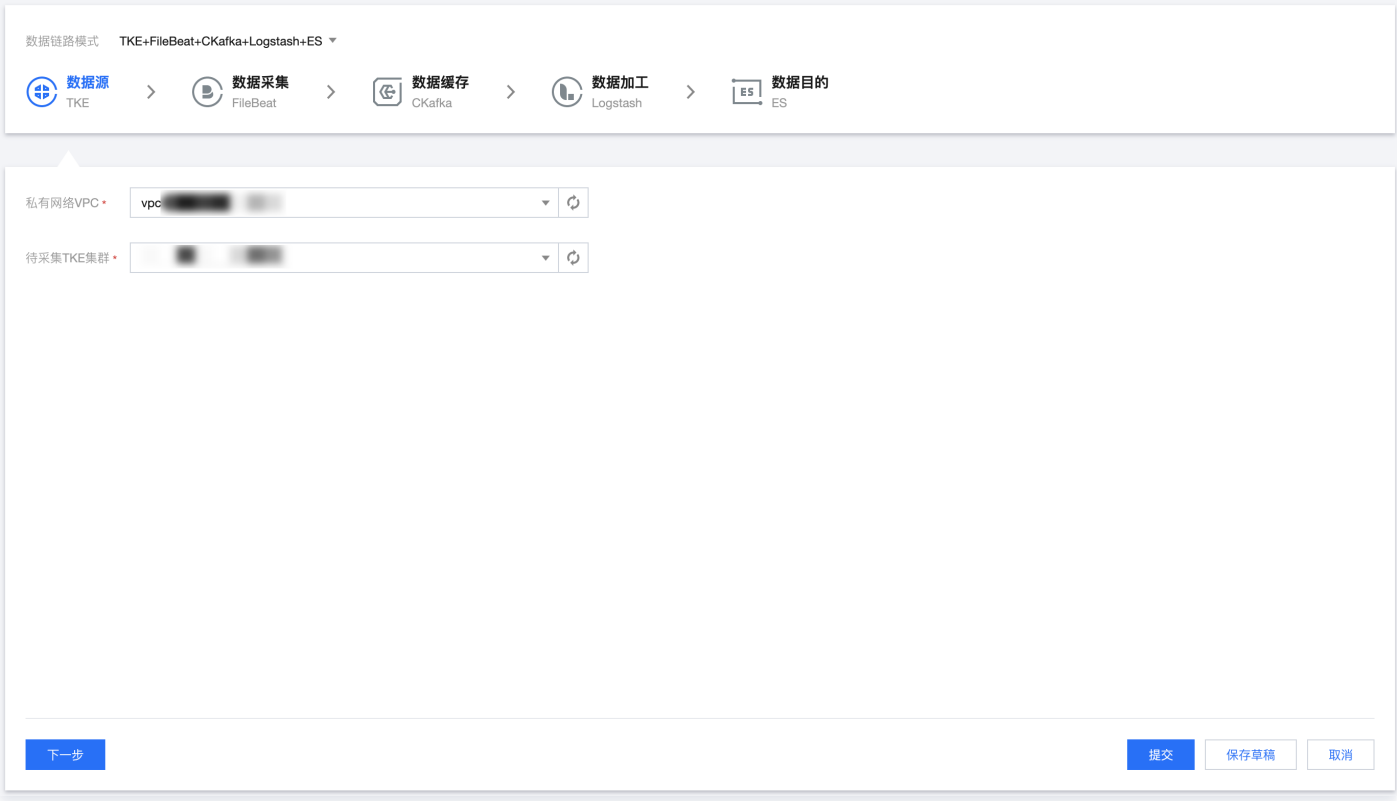
1. 选择 VPC。
2. 选择 ES 实例。
3. 选择写入的索引类型，自治索引 适用于2022年6月1日之后创建的7.14.2版本集群，早于此时间创建的7.14.2版本集群重启后可支持。低于7.14.2版本的集群需升级至7.14.2版本。
4. 填写索引名称，当写入的索引类型为普通索引时，该名称为索引别名，您可根据该别名访问您的数据。如您未填写索引名称，将自动生成格式为{数据链路 ID_index_ 随机字符串}的索引名称。
5. 在写入的索引类型中，如您选择的是**新建自治索引**，您可对字段映射进行预定义；如您选择的是**选择自治索引**，请确保采集的 "时间字段" 与所选自治索引的 "时间字段" 完全一致，否则将导致数据写入失败。



TKE-Filebeat-CKafka-Logstash-ES

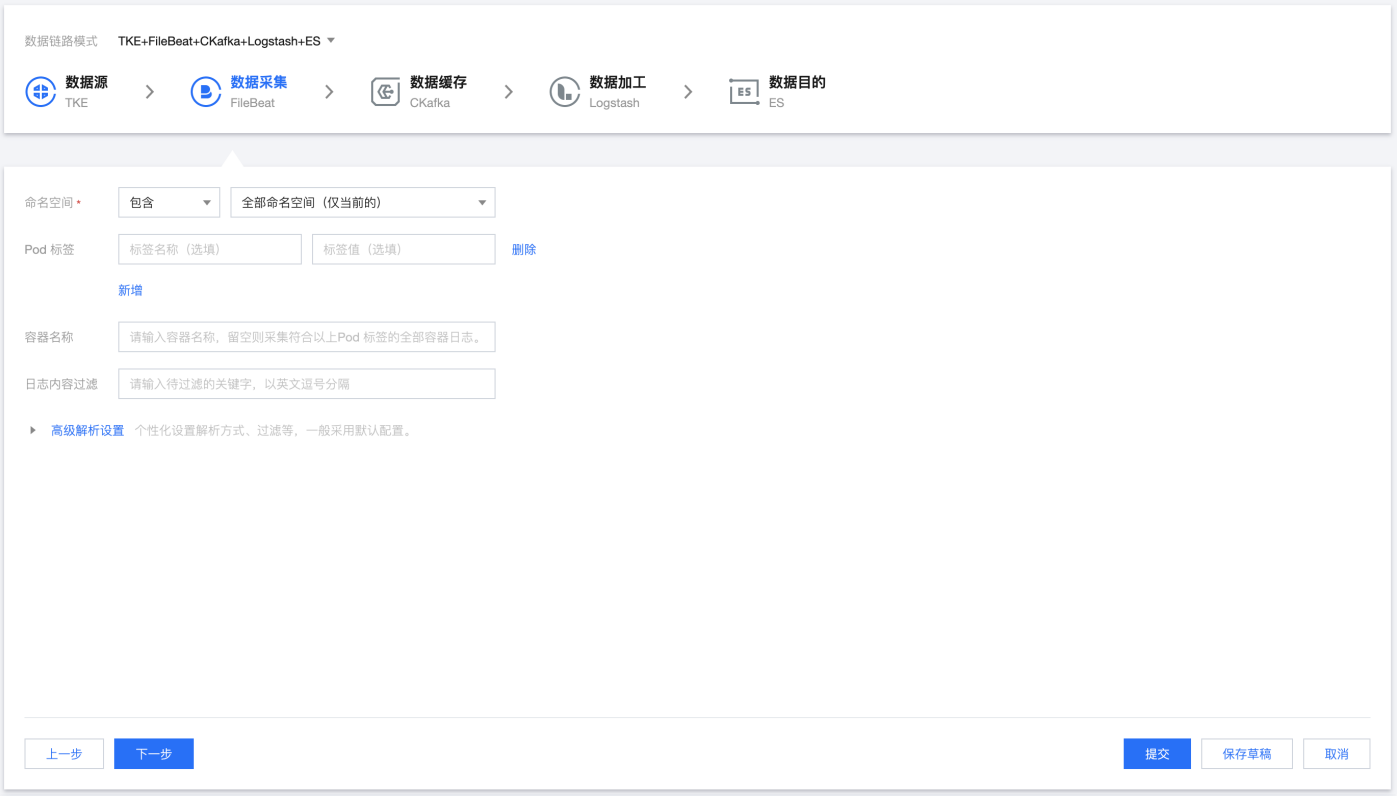
数据源

1. 选择 VPC
2. 选择 TKE 集群。



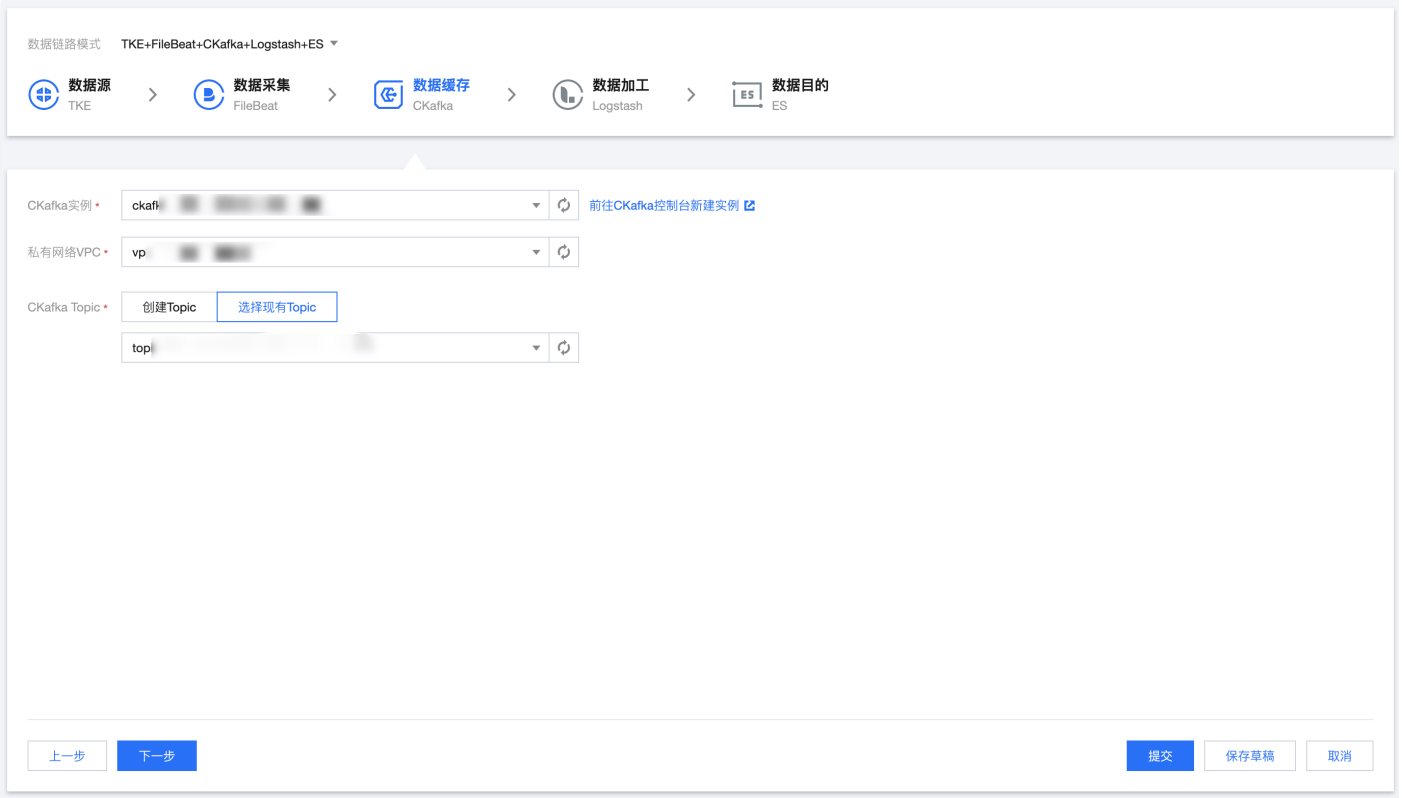
数据采集

1. 命名空间：必选。第一个下拉可选择 包含/不包含。第二个下拉可选择命名空间，支持多选，不支持选择不包含全部命名空间。
2. Pod 标签：选填。支持创建多个 Pod 标签，标签之间是逻辑与关系。
3. 容器名称：选填。填写的容器名称必须在采集目标集群及命名空间之下，为空时，Filebeat 会采集命名空间下符合 Pod 标签的全部容器。
4. 日志内容过滤：选填。根据关键字过滤日志，可填多个关键字，以逗号分隔。
5. 高级采集配置：选填。个性化设置解析方式、过滤等，一般采用默认配置，详情请参考 配置文件填写参考 。



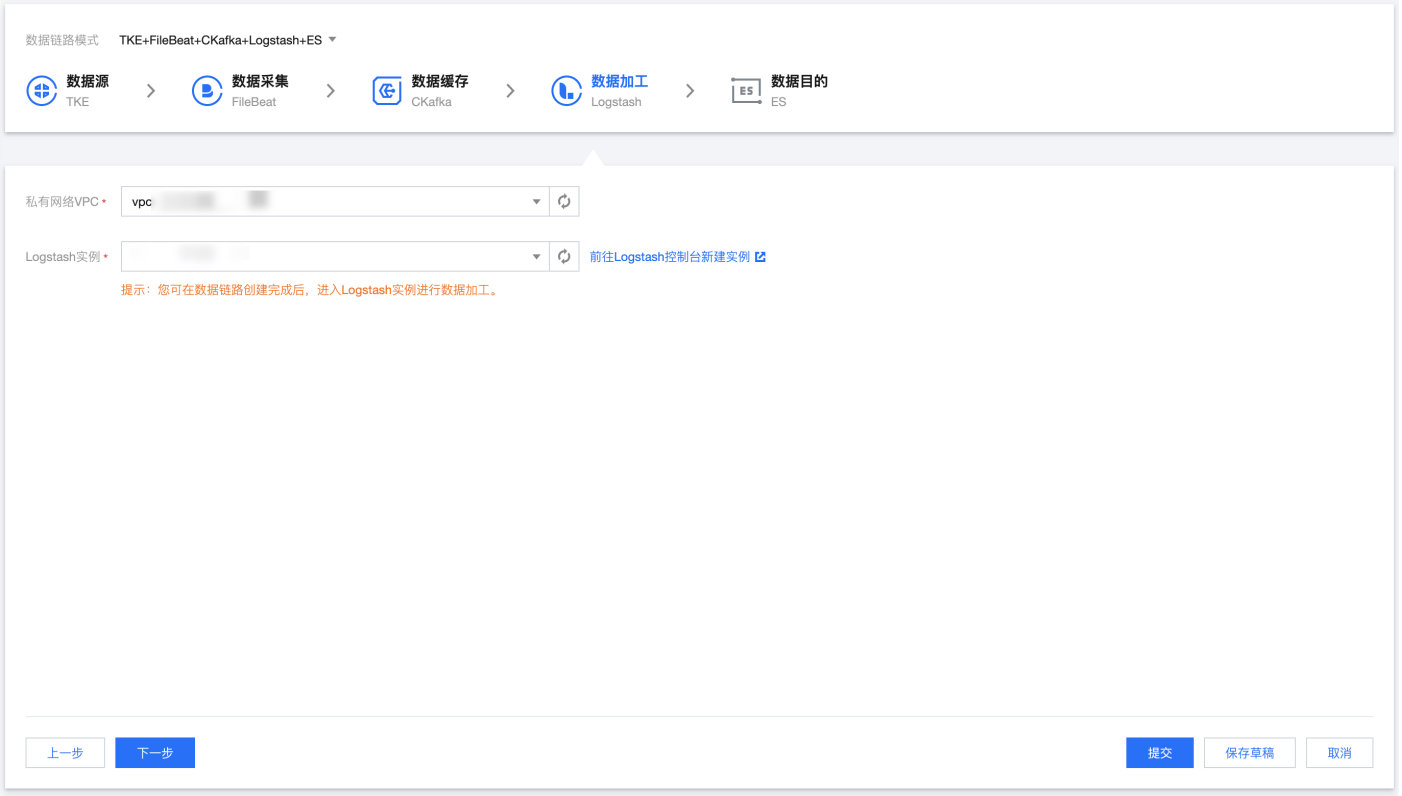
数据缓存

1. 选择 CKafka 实例。
2. 从 Ckakfa 实例已经路由打通的 VPC 中，选择跟当前链路组件有交集的 VPC。
3. 创建或者选择已有 Topic，当选择**创建 Topic** 时，如您未填写 Topic 名称，将自动生成格式为{数据链路 ID_topic_ 随机字符串}的 Topic 名称。



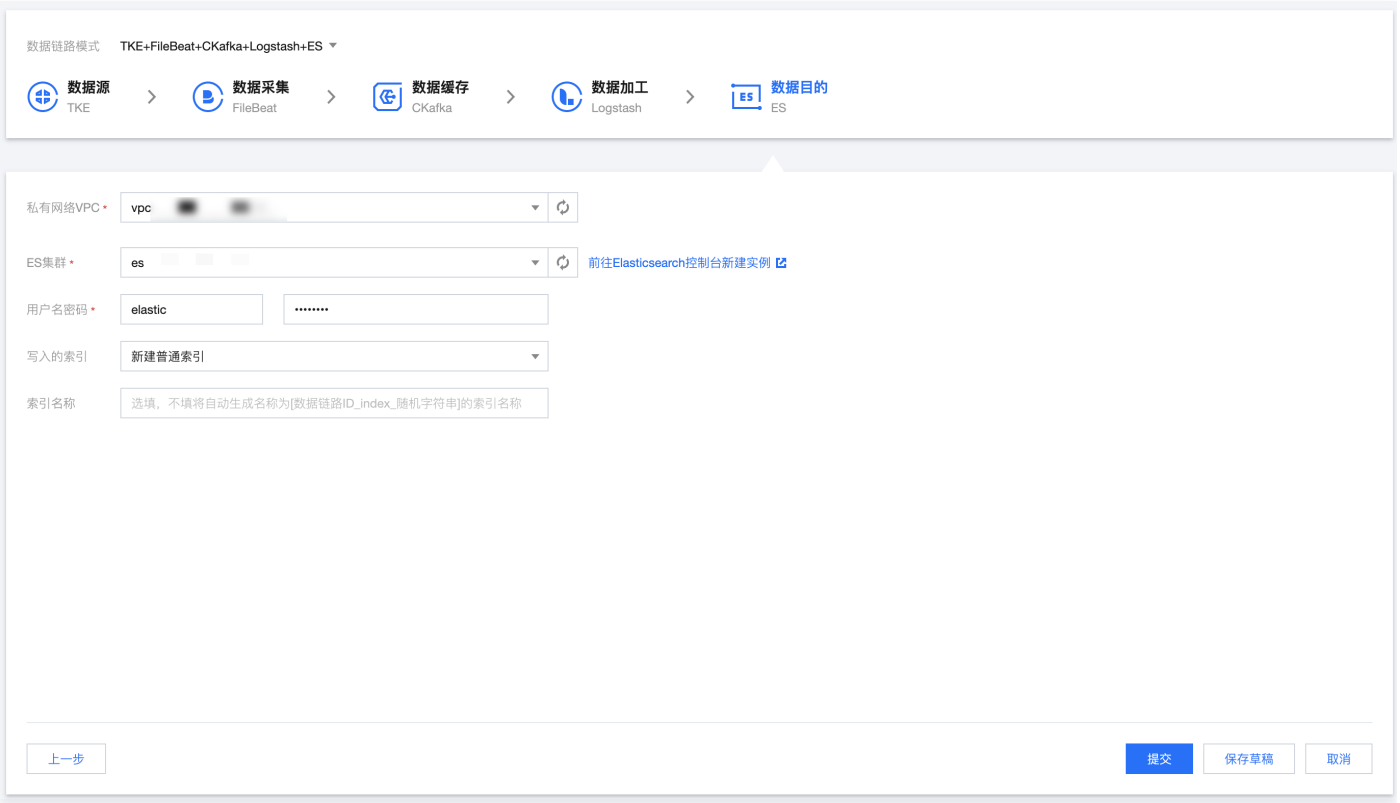
数据加工

1. 选择 VPC。
2. 选择 Logstash 实例。
3. 生成数据链路时，将自动在该实例下创建名称为{数据链路 ID_lgpipe_ 随机字符串}的管道，如需对数据进行加工，可在数据链路创建完成后到对应的 Logstash 实例下修改相关管道的配置。



数据目的

1. 选择 VPC。
2. 选择 ES 实例。
3. 选择写入的索引类型，自治索引 适用于2022年6月1日之后创建的7.14.2版本集群，早于此时间创建的7.14.2版本集群重启后可支持。低于7.14.2版本的集群需升级至7.14.2版本。
4. 填写索引名称，当写入的索引类型为普通索引时，该名称为索引别名，您可根据该别名访问您的数据。如您未填写索引名称，将自动生成格式为{数据链路 ID_index_ 随机字符串}的索引名称。
5. 在写入的索引类型中，如您选择的是**新建自治索引**，您可对字段映射进行预定义；如您选择的是**选择自治索引**，请确保采集的 "时间字段" 与所选自治索引的 "时间字段" 完全一致，否则将导致数据写入失败。



数据管理
自治索引简介

最近更新时间：2024-10-12 21:50:11

背景概述

当您有日志、监控等持续产生的时序数据存储需求时，通常通过滚动 Elasticsearch 索引的方式完成，该方式虽然能帮助您完成基本的数据管理功能，但是仍然需要结合索引模板、索引生命周期管理、索引别名等实现较完整的索引管理，有一定的使用门槛。另外也存在一定的索引维护成本，例如您需要在索引创建前进行分片数预估，避免索引分片数不足影响写入可用性、单副本索引在节点故障时需介入滚动新的索引，以及避免不合理的索引分片数预估，导致分片数过多，影响集群稳定性等。为了解决这些问题，腾讯云 Elasticsearch 自研了**自治索引**，自治索引是针对日志分析、运维监控等**时序数据**场景的一站式索引管理解决方案，您只需要通过简单的步骤创建自治索引，读写请求时指定单个自治索引对象即可，内置索引分片数自动调优、以及完整的索引生命周期管理。提升索引易用性的同时，降低索引的维护成本。本文主要介绍自治索引的适用场景、优势特性以及基本概念等。

适用场景

自治索引适用于日志分析、运维监控和其他时序数据场景，例如日志检索分析、Metric 监控分析、IoT 智能硬件数据收集以及监控分析等。

优势与特性

- 易使用：只需一条命令即可完成自治索引的创建，读写操作仅需关注单个自治索引，内置索引滚动、冷热数据搬迁、过期删除等功能，您只需在自治索引上配置即可，无需额外管理ILM策略和索引模板的成本。
- 易维护：内置索引分片数自动调整功能，实时跟踪业务写入压力变化，能够及时、稳定的调整索引分片数，以及故障自动滚动新的索引，大大降低索引维护成本。

前提条件

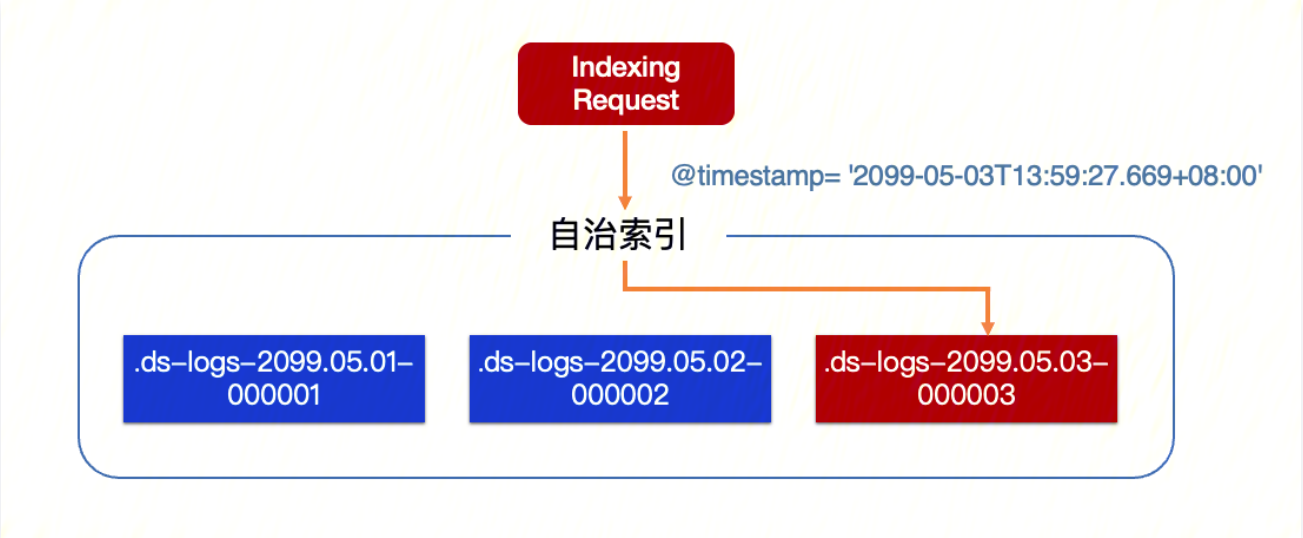
- 自治索引适用于2022年6月1日之后创建的7.14.2版本集群，早于此时间创建的7.14.2版本集群滚动重启后可支持，低于7.14.2版本的集群需升级至7.14.2版本。
- 写入到自治索引中的每个文档要求包含一个时间类型的字段，时间类型字段名称需与自治索引定义里的时间字段名称一致。如果创建自治索引时未指定时间字段名称，默认为 @timestamp。

基本概念

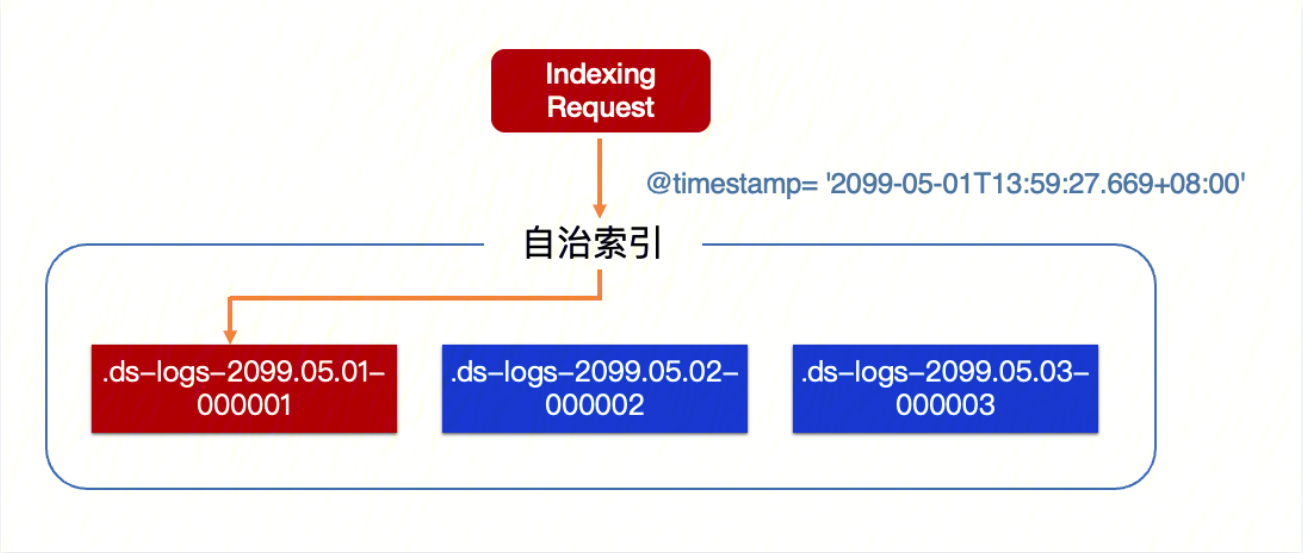
- 自治索引与后备索引
  自治索引通过Elasticsearch DataStream内核增强实现，内部关联一个或多个后备索引，后备索引即普通的Elasticsearch索引，后备索引处于隐藏状态，只需关注和操作自治索引即可。

- 写入模式
  自治索引支持追加写入和按时间分区写入两种数据写入模式。追加写入模式，数据将写到最新的后备索引，适用于日志场景；按时间分区写入模式，数据将根据时间字段写入到对应的后备索引，适用于指标场景。
- 写入请求
  向自治索引提交写请求时，会根据写入模式路由到对应的后备索引上。其中，追加写模式会路由到最新的后备索引，时间分区写模式会路由到数据时间对应的后备索引。

1.1 追加模式写入

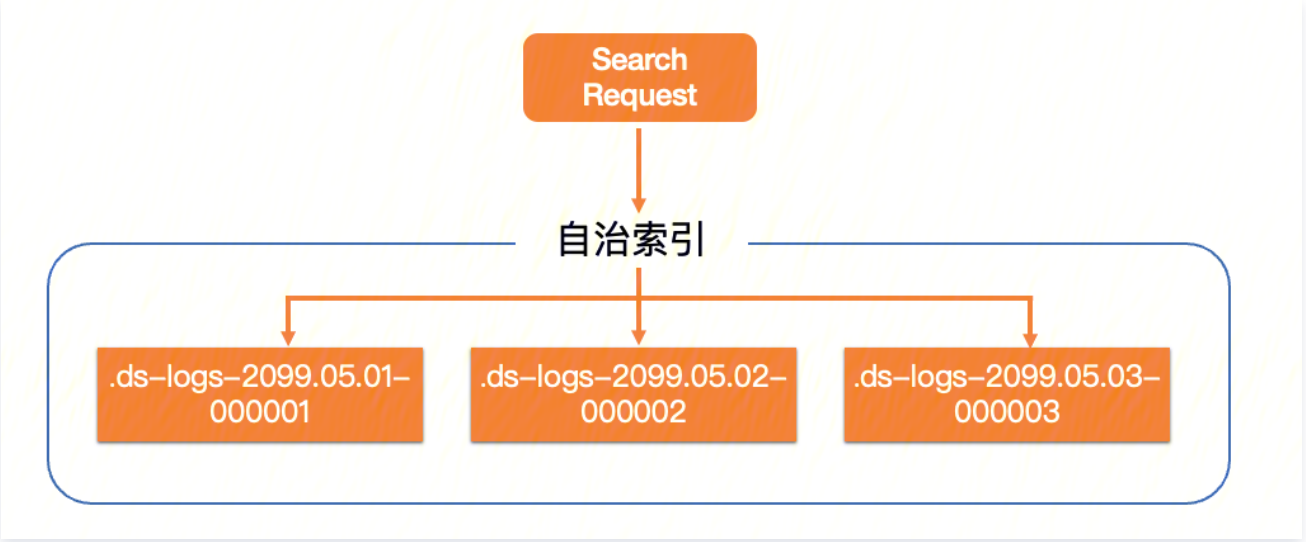


1.2 时间分区模式写入



- 查询请求

  向自治索引提交查询请求时，请求会转发到所有后备索引上。



- 滚动更新
  滚动更新将为自治索引新建一个新的后备索引，当前支持以下两种滚动方式：
  1.1 自动滚动更新：通过自治索引内置功能实现，当满足自治索引配置的滚动周期条件或者当前提供写入的后备索引所在节点故障时，自动滚动新的后备索引。
  1.2 手动滚动更新：通过 Rollover API 实现，操作方式详见 Rollover 。
- 索引生命周期管理
  通过 Elasticsearch ILM 索引生命管理实现，可直接在自治索引配置生命周期管理策略，无需额外管理生命周期管理策略和关联索引模板，策略类型支持 Elasticsearch 完整的索引生命周期管理策略。

> **说明：**
> 自治索引有类似回收站的机制，如果通过配置 expire.max_age 和 expire.max_size 字段的方式控制后备索引的删除，被删除的后备索引会首先被解除挂载并设置为隐藏，等到后备索引中的数据过期一天后才真正删除。目前可以通过提交工单来调整回收站的保留时间。

- 索引分片数管理
  通过自治索引内置功能实现，内部实时跟踪索引写入压力变化，及时、稳定，调整索引分片数。您无需关心索引分片数不足引起的写入可用性，以及集群分片数过多的问题。

使用方式

腾讯云 ES 支持用户通过简单易用的可视化界面使用与管理自治索引，详情请参考 新建自治索引 。

常见 API

1. 自治索引创建：

```
PUT /_data_stream/indexname
{
"mappings": {
   "properties": {
   }
},
"settings": {
},
"policy": {
  "warm.actions.migrate":{},
  "warm.min_age":"3d"
},
"options": {
   "timestamp_field": "@timestamp",
   "expire.max_age": "100d",
   "expire.max_size": "1TB",
   "pre_create.enable": true,
   "rollover.max_age": "1h",
   "rollover.dynamic": true,
   "shard_num.dynamic": true,
   "write_mode": "time_partition"
}
}
```

   - mappings
     与 ES index 中的 mapping 一致，用于设置 ES index mapping，可选填。
   - settings
     与 ES index 中的 settings 一致，用于设置 ES index settings，可选填。

- policy
  与 ES ilm 设置含义一致，配置方式做了简化，用于设置索引生命周期策略，可选填。
- options
  自治索引属性，其中：
  - timestamp_field：时间字段，支持用户自定义，可选填，不填默认为：@timestamp。
  - expire.max_age：时间范围分区过期最长保留时间，单位支持h(小时)、d(天)，最小单位为1小时，不填默认为0，即不删除历史范围分区。
  - expire.max_size：时间范围分区过期最大存储容量，超过则淘汰历史时间范围分区，单位支持b、kb、mb、gb、tb、pb，不填默认为0，即不淘汰历史范围分区。
  - precreate.enable：是否开启预创建时间范围分区，默认值为 true，表示自动预创建时间范围分区。
  - rollover.max_age：时间范围滚动周期，单位支持h(小时)、d(天)，可选填，默认值1d，最小单位为1h。-1表示不滚动时间范围分区。
  - rollover.dynamic：时间范围分区滚动周期动态调整开关，默认为 true，表示是否支持平台动态调整时间范围分区的滚动周期。
  - shard_num.dynamic：时间范围分区分片数动态调整开关，默认为 true，表示是否支持平台动态调整时间范围分区的分片数。
  - write_mode：时间范围分区写入模式，可选值为："append_only"：追加模式写入，表示数据会写入最新的时间范围分区、"time_partition"：时间分区模式写入，表示数据会写入数据时间对应的时间范围分区。默认为 append_only 模式。

2. 自治索引删除：

```
DELETE /_data_stream/index_name
```

3. 自治索引修改：

```
POST _data_stream/indexname/_update
{
  "options": {
    "expire.max_age": "30d"
  }
}

----
除options.timestamp_field和options.write_mode之外，其他属性均支持修改
修改配置成功后，生命周期的相关配置将在所有后备索引中生效，其他配置例如分片数、副本数、字段映射等仅在后续滚动出的后备索引中生效，已有的后备索引不会更新。
```

4. 自治索引查询，与普通索引查询用法一致：

```
GET indexname/_search
```

5. 写入，与普通索引写入用法一致，均支持 bulk 和 doc 方式写入：

```
PUT /indexname/_bulk
{"create":{ }}
{"@timestamp": "2022-03-13T03:07:34.348+08:00","field1": "a"}
{"create":{ }}
{"@timestamp": "2022-03-24T10:51:34.348+08:00","field1": "a"}
```

6. 自治索引滚动：

```
POST indexname/_rollover
```

7. 查询自治索引定义：

```
1.指定名称查询
GET _data_stream/indexname?include_define
2.查询所有自治索引
GET _data_stream?include_define
----
```

其中，include_define选项表示结果包含自治索引属性内容，不指定则和社区DataStream返回内容一致

新建自治索引

最近更新时间：2024-10-12 21:50:11

前提条件

- 已创建腾讯云账号，创建账号可参考 注册腾讯云 。
- 已创建 Elasticsearch Service 集群，且 Elasticsearch 版本为7.14.2，创建集群可参考 创建集群 。

> **注意**
> 当前仅支持新建 自治索引，自治索引由腾讯云自研，适用于时序数据（如日志分析、运维监控等）场景，能够实现索引生命周期管理和分片自动调优，并有效提高读写效率。自治索引适用于2022年6月1日之后创建的7.14.2版本集群，早于此时间创建的7.14.2版本集群重启后可支持。低于7.14.2版本的集群需升级至7.14.2版本。

操作步骤

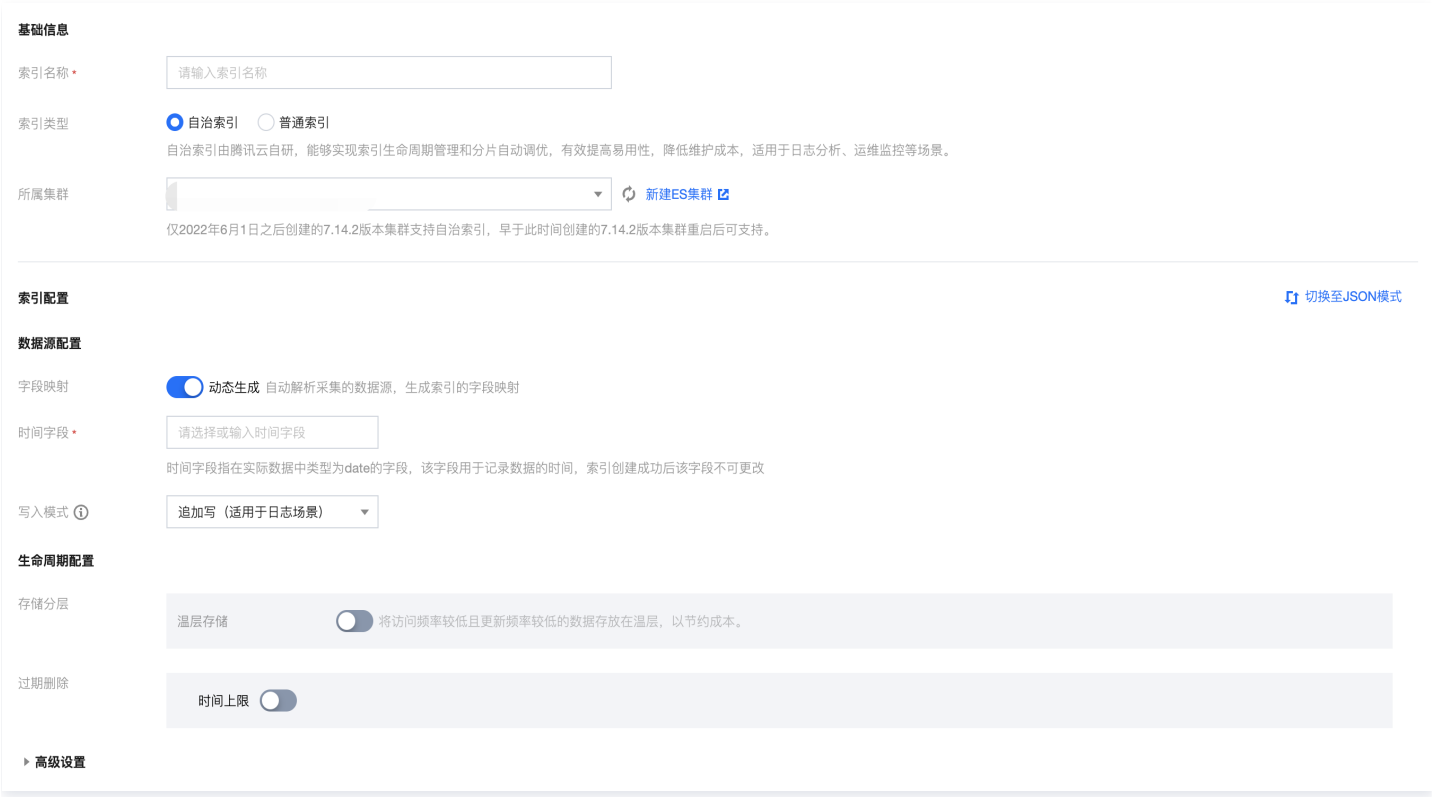
步骤一：进入新建页面

1. 登录 ES 控制台，单击 ES 索引管理进入索引列表。
2. 单击新建进入新建页面。

步骤二：填写配置信息

基础信息

- 索引名称：长度为1 - 255个字节，不支持中文，不能包含大写字母以及 \，/，*，?，"，<，>，|，#，:，空格，逗号，不能以 -，_，+，. 开头。
- 索引类型：选择自治索引。
- 所属集群：该索引所在的集群。



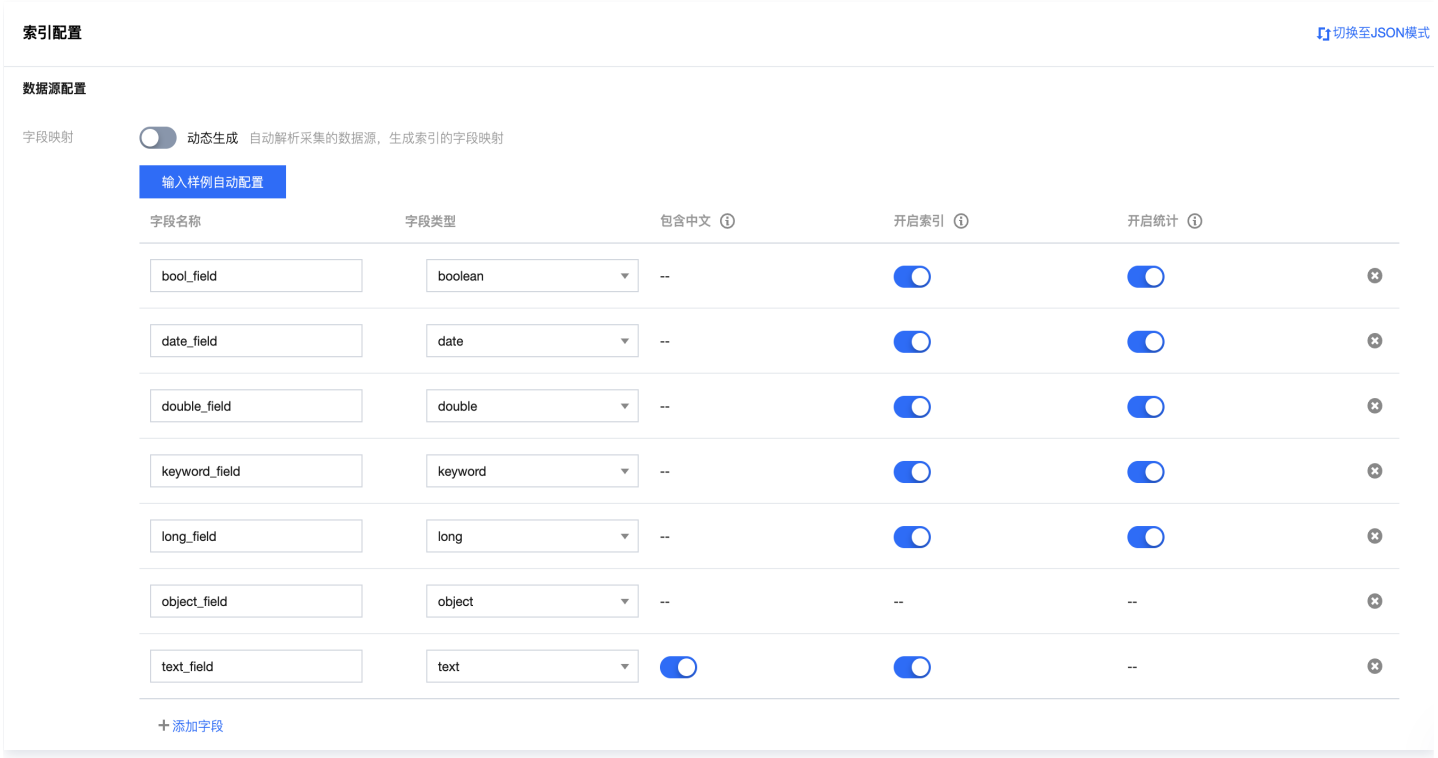
数据源配置

1. 字段映射

动态生成：默认开启，开启后将自动解析采集的数据源，生成索引的字段映射。
输入样例自动配置：关闭**动态生成**后，您可以通过**输入样例自动配置**来生成索引的字段映射，在输入框内输入一段 JSON 格式的数据样例，确定后平台将自动为您进行校验，校验无误后，相关字段将映射到字段映射的表格中。推导规则及样例如下：字段值为 true 或 false 映射类型为 boolean；字段值为整数映射类型为 long；字段值为浮点数映射类型为 double；字段值为字符串且长度小于等于36字符映射类型为 keyword；字段值为字符串且长度大于36字符映射类型为 text；字段值为日期格式字符串映射类型为 date；字段值支持嵌套映射类型为 object。我们在**输入样例自动配置**输入框中输入一段 JSON 格式的数据样例：

```
{
 "bool_field": true,
 "date_field": "2022/01/26 00:00:00",
 "double_field": 3.14,
 "keyword_field": "这是一行不需要分词的文本",
 "long_field": 126,
 "object_field": {
  "sub_field": 2022
 },
 "text_field": "这是一行需要分词的文本，文本长度超过36个字符的会被推断为需要分词，定义为text类型"
}
```

其解析后的结果如图所示：



字段映射将原始数据按字段（即 key:value ）分别切分为多个分词进行索引构建，检索时基于该映射进行检索。具体如下：

参数项	描述
字段名称	写入的数据中的字段名称
字段类型	字段的数据类型，包括 `boolean`、`keyword`、`long`、`double`、`date`、`text` 六种类型，更多字段类型可在 JSON 编辑模式中支持，参考 官方说明

包含中文	字段中包含中文且需要对中文进行检索时可开启该功能。开启后，将默认对该 text 字段使用 ik_max_word 分词器
开启索引	启用后，会对该字段构建索引用于检索，会增加索引存储
开启统计	启用后，可以对字段值做统计分析，会增加索引存储

2. 时间字段：指在实际数据中类型为 date 的字段，该字段用于记录数据的时间，索引创建成功后该字段不可更改。
   - 时间字段默认打开**开启索引**与**开启统计**，且不可关闭。
   - 关闭动态生成时，时间字段将把表格中为date类型的字段映射过来，您可下拉选择其中一个作为时间字段。
3. 写入模式：指数据写入到索引的模式，索引创建成功后不可更改。当前支持两种写入模式：
   - 追加写（适用于日志场景）：表示数据会写入到最新的后备索引。
   - 时间分区写（适用于监控场景）：表示会根据时间字段写入对应时间范围的后备索引。

生命周期配置

1. 存储分层
   存储分层表示您可将索引根据其访问频率存储到不同属性的节点上。例如，您可将访问频率较低且更新频率较低的数据移入温层，以节约成本。索引迁移到不同层级的时间，将从索引滚动更新开始计算。
2. 过期删除
   - 时间上限：当写入模式为**追加写**时，表示从后备索引的创建时间开始算起，当达到指定的值时，该后备索引将会被删除；当写入模式为**按时间分区写**时，表示从后备索引结束写入的时间开始算起，当达到指定值时，该后备索引将会被删除。

> **说明：**
> 自治索引有类似回收站的机制，如果通过配置expire.max_age 和 expire.max_size 字段的方式控制后备索引的删除，被删除的后备索引会首先被解除挂载并设置为隐藏，等到后备索引中的数据过期一天后才真正删除。目前可以通过提交工单来调整回收站的保留时间。

高级设置

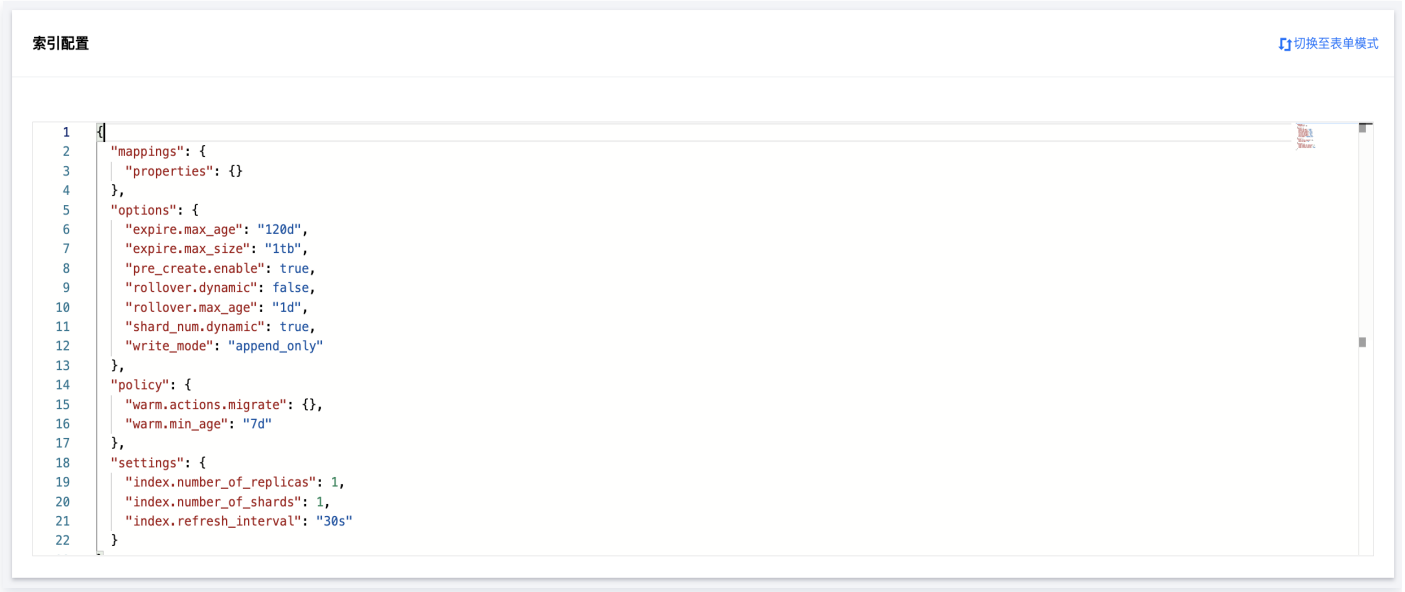
1. 创建参数
   - 分片数设置：分片是索引中存储数据的单元，若动态调整打开，这里的分片数仅作为初始的后备索引的分片值，后续算法会自动优化为最佳值。
   - 副本数：每个主分片拥有的副本分片的数量。
   - 刷新频率：数据写入索引后能够被搜索到的时间间隔。
2. 索引滚动
   - 滚动周期：从开始日期起，索引将以指定时间为周期，每一周期进行一次滚动。
   - 动态调整：平台将根据业务负载动态调整滚动周期，使得索引保持最佳状态。

JSON 编辑模式

1. 功能说明
   当前支持通过切换到 **JSON 编辑模式**创建索引，点击**索引配置**右上角**切换至 JSON 模式**即可进入 JSON 编辑页面。切换模式成功后，配置信息将自动同步到对应模式的界面中。
2. 常用参数说明
   自治索引通过提供 options 以及 policy，帮助用户快速进行滚动更新以及生命周期管理相关的设置，同时，兼容 Elasticsearch 社区中 settings 与 mappings 的原生语法，降低使用门槛，常见参数如下：

类别	参数项	参数描述	填写说明
settings	index.number_of_shards	主分片数	数值类型，该值需为大于等于1的整数
	index.number_of_replicas	副本数	数值类型，该值需为大于等于0的整数
	index.refresh_interval	刷新频率	字符串类型，单位当前支持设为d（天）、h（小时）、m（分钟）、s（秒）、ms（毫秒）、micros（微秒）、nanos（纳秒），例如“30s”表示将刷新频率设为30秒
mappings	field	字段名称	字符串类型，非中文且不可重复
	type	字段类型	字符串类型，可设为“boolean、keyword、long、double、date、text”，更多字段类型可参考 官方说明
	analyzer	分词器	字符串类型，支持ES集群中存在的分词器，例如“ik_max_word”
	index	开启索引	布尔类型，可设为“true”或者是“false”
	doc_values	开启统计	布尔类型，可设为“true”或者是“false”
options	pre_create.enable	索引预创建	布尔类型，默认开启，可设为“true”或者是“false”。请注意，写入模式为追加写的情况下，如关闭了索引预创建，后备索引将不会按照指定的滚动周期进行滚动
	rollover.dynamic	动态调整滚动周期	布尔类型，可设为“true”或者是“false”
	rollover.max_age	滚动周期	字符串类型，单位可设为“d”天或者“h”小时，例如“1d”表示将滚动周期设为1天
	shard_num.dynamic	动态调整分片	布尔类型，可设为“true”或者“false”
	write_mode	写入模式	字符串类型，“append_only”表示追加写，“time_partition”表示按时间分区写
	expire.max_age	过期删除时间上限	字符串类型，单位可设为“d”天或者“h”小时，例如“1d”表示将时间上限设为1天
	expire.max_size	过期删除空间上限	字符串类型，单位可设为“PB、TB、GB、MB、KB、B”，例如“1TB”表示将空间上限设为1TB
policy	warm.actions.migrate	温阶段索引迁移设置	请查看官方说明 Migrate 设置
	warm.min_age	移入温层存储时间	字符串类型，单位可设为“d”天或者“h”小时，例如“1d”表示从索引滚动更新开始，1天后移入温层
	cold.actions.migrate	冷阶段索引迁移设置	请查看官方说明 Migrate 设置

	cold.min_age	移入冷层存储时间	字符串类型，单位可设为“d”天或者“h”小时，例如“1d”表示从索引滚动更新开始，1天后移入冷层



创建完成

单击**确认创建**，索引创建成功后，将自动跳转到该索引所在的**索引列表**。

后续步骤

索引检索与分析

数据管理支持快速跳转到检索以及分析界面，实现索引检索与分析。详情请参考 索引检索与分析 。

索引基础信息

数据管理支持在控制台查看索引的相关信息，以及进行后备索引的管理。详情请参考 索引基础信息 。

索引监控

数据管理提供了索引粒度的丰富的监控指标，可以帮助在索引使用过程中查看索引的实时监控数据。详情请参考 索引监控 。

索引配置管理

数据管理支持在控制台灵活地进行索引配置信息的修改，以适应业务的变化。修改配置成功后，生命周期的相关配置将在所有后备索引中生效，其他配置仅在后续滚动出的后备索引中生效，已有的后备索引不会更新。详情请参考 索引配置管理 。

索引检索与分析

最近更新时间：2024-10-12 21:50:11

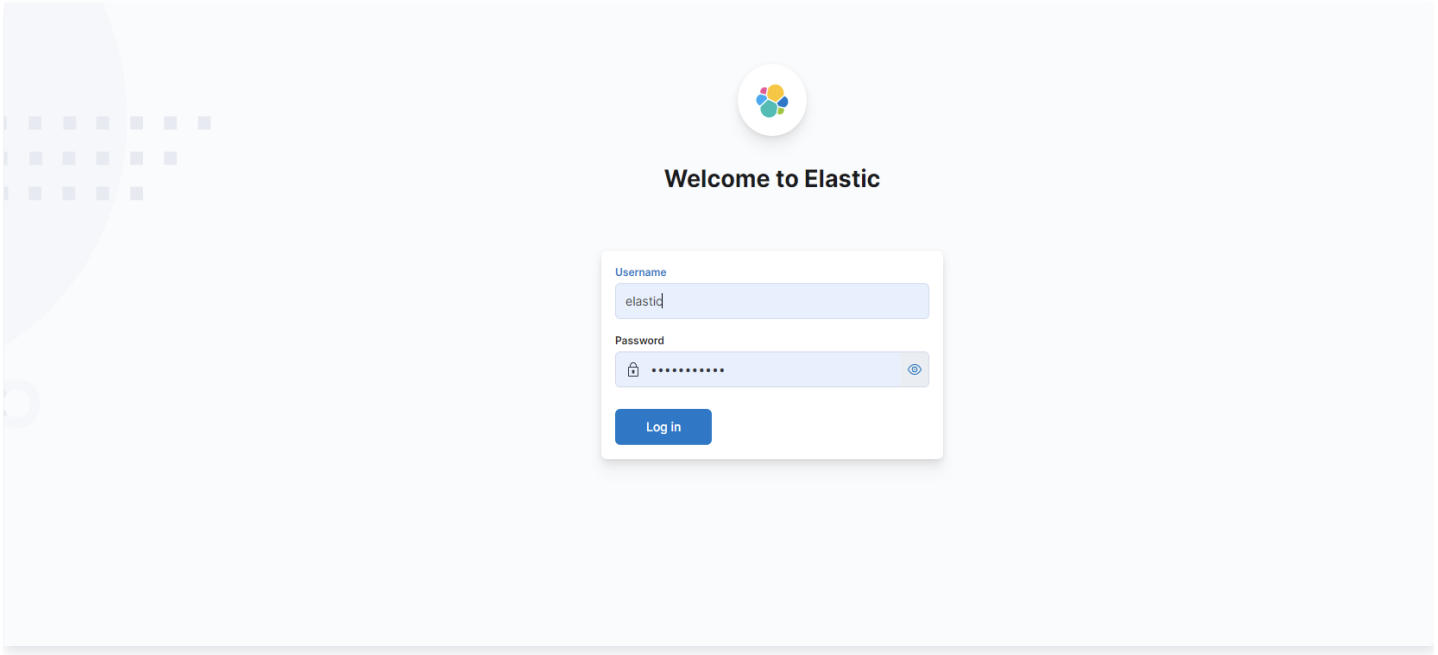
腾讯云 Elasticsearch Service（ES）包含 Kibana 模块，用户可以在 Kibana 中对索引中的数据进行检索与分析，您可以在索引列表中快速访问 Kibana，实现检索与分析。

检索与分析

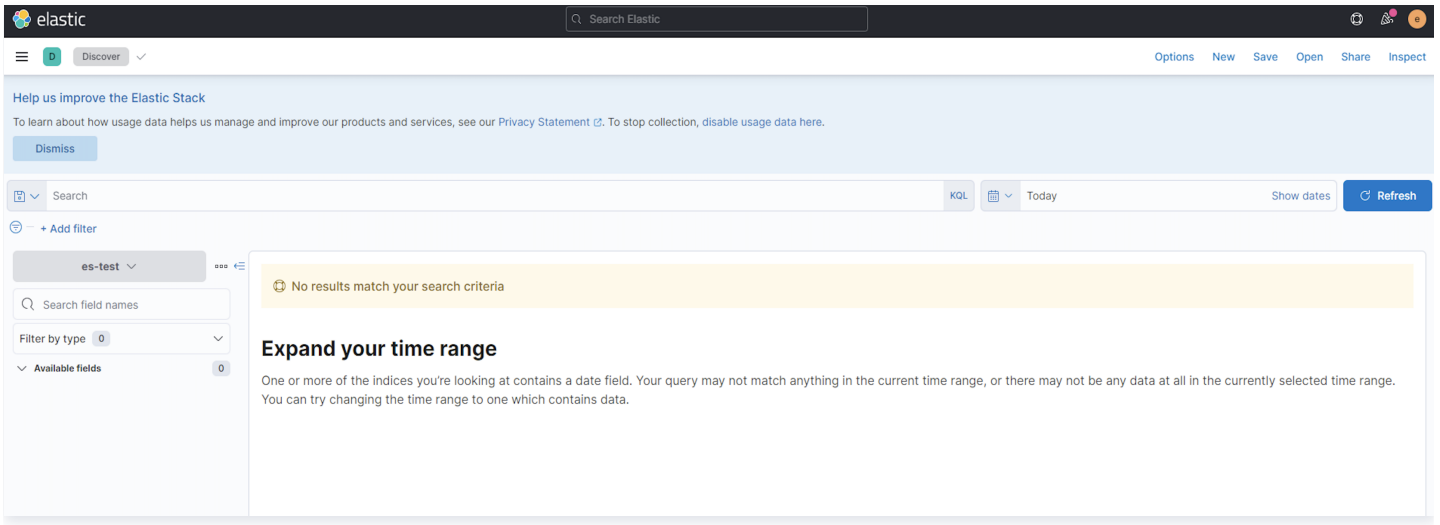
ES 控制台 提供快捷访问检索与分析页面的入口，在索引列表中，单击对应的入口，会跳转到 Kibana 登录页面，登录成功后即可进入对应界面。单击**kibana**，将进入对应索引的 discover 界面。

登录

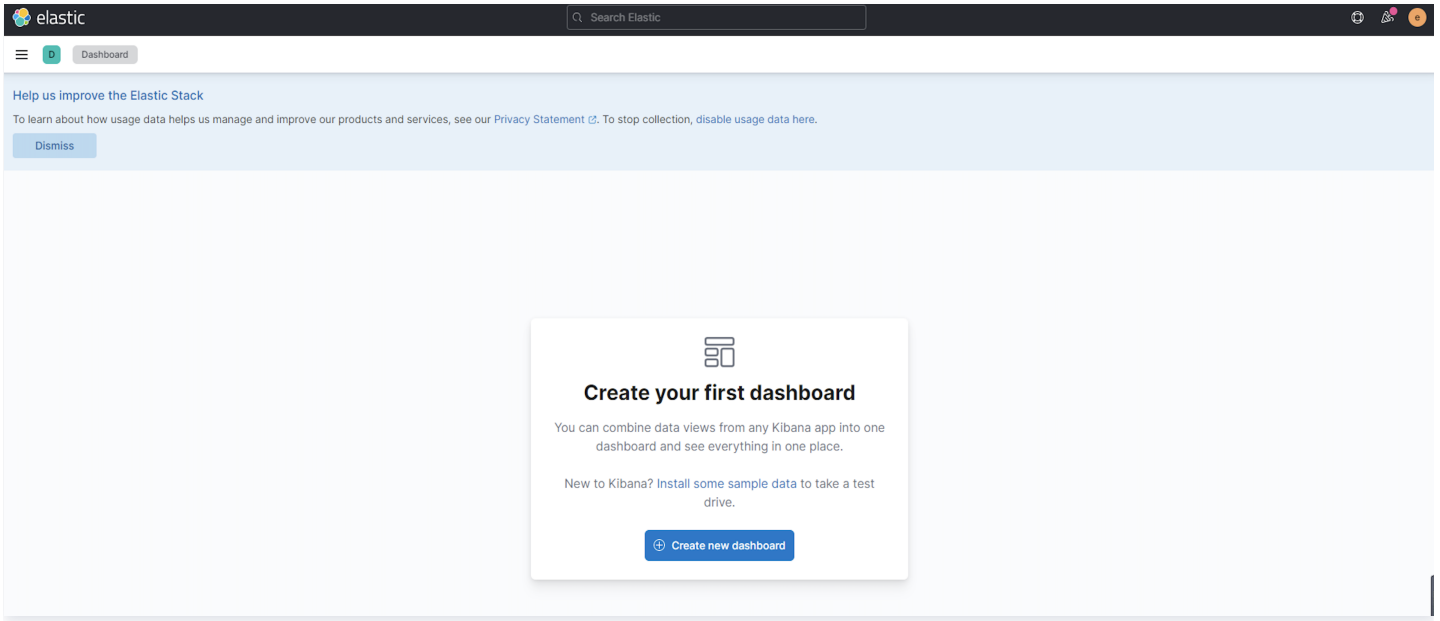
Kibana 页面访问需要登录，账号为 elastic，密码为用户创建集群时设置的 Kibana 密码。如果忘记密码，可以在集群详情页重置密码。出于安全考虑，用户可以配置 Kibana 公网地址的访问黑白名单来提高安全防护，详情请参见 ES 集群访问控制 。



登录成功后，进入**检索**界面，自治索引已默认根据索引名称建好Index Patterns，您可直接进行数据检索：



登录成功后，进入分析界面：



索引基础信息

最近更新时间：2024-10-12 21:50:11

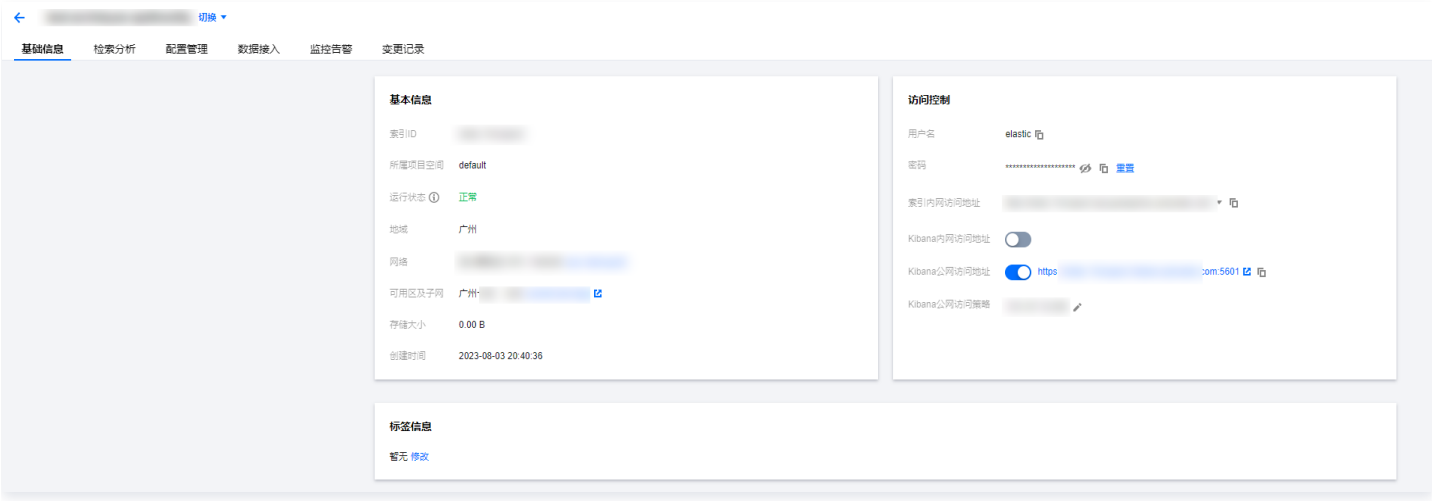
数据管理提供了包括索引状态、所属集群、Elasticsearch 版本等基础信息的查看以及后备索引的管理。

操作步骤

1. 登录 Elasticsearch Service 控制台。
2. 在**日志分析**选择对应的索引，在索引列表单击**索引名称/ID**，进入索引**基础信息**页面。

基本信息

基本信息模块提供对索引基本信息、访问控制和标签信息等的查看。其中，存储大小通过将该索引中所有后备索引的存储大小相加得出。



配置管理

用户可在**配置管理**模块查看索引配置中的字段映射、时间字段、数据存储时长等信息，也可按需修改配置。

后备索引管理

一般而言，您不需要关注后备索引，因为它是 自治索引 的底层实现逻辑，您可以完全不感知它。如果您希望对后备索引有更多的关注和操作，可以了解如下信息：

后备索引管理模块提供对后备索引的相关信息进行查看与管理的功能，包括对该后备索引的名称、索引状态、存储大小、当前生命周期阶段、创建时间的查看，以及对该后备索引进行删除的操作。

> **注意**
> 当该索引为自治索引中最新的后备索引或者是正在提供写入的后备索引时，无法删除。

滚动更新将为自治索引新建一个新的后备索引，当前支持以下两种滚动方式：

- 自动滚动更新：通过自治索引内置功能实现，当满足自治索引配置的滚动周期条件或者当前提供写入的后备索引所在节点故障时，自动滚动新的后备索引。
- 手动滚动更新：通过 Rollover API 实现，操作方式请参见 Rollover 。

索引监控

最近更新时间：2024-10-12 21:50:11

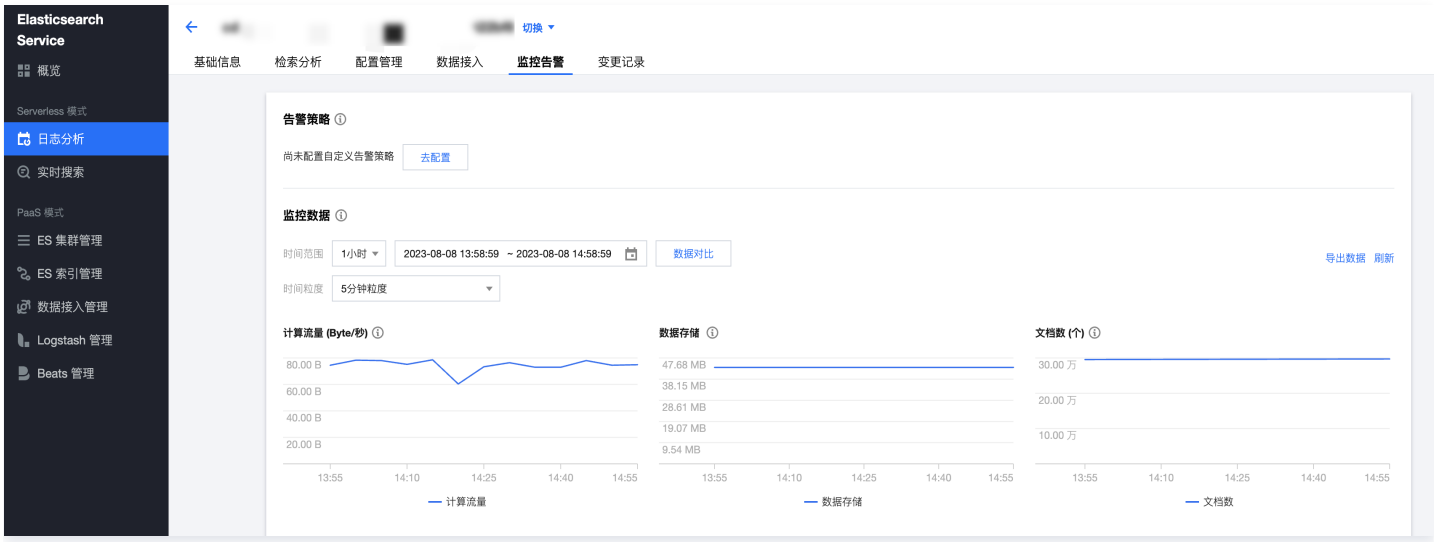
数据管理对 Elasticsearch Service 集群中的索引，提供了多项监控指标，用以监测索引的情况，如存储、写入、查询等。您可以根据这些指标实时了解索引的使用情况，针对可能存在的风险及时处理，保障索引的使用。本文为您介绍通过数据管理查看监控数据的操作。

操作步骤

1. 登录 Elasticsearch Service 控制台 。
2. 单击**日志分析**，在索引列表单击**索引名称/ID**，进入索引基础信息页。
3. 选择**监控告警**页面，可以查看索引的状态监控。

监控告警

监控数据涵盖计算流量、数据存储、文档数、写请求数和读请求数等维度。



指标含义及说明

所有指标的统计周期均为5分钟，即每5分钟对索引的指标采集1次。具体各指标含义说明如下：

监控指标	统计方式	详情
存储容量	每单位统计周期内，索引存储容量的平均值。	该值为单个索引或者自治索引所有后备索引存储容量总和，您可根据该值查看索引存储量变化。
总分片数	每单位统计周期内，索引中分片数量的平均值。	该值为单个索引或者自治索引所有后备索引所有分片数总和，包含主副分片
写入速度	每单位统计周期内，索引或自治索引接收到的每秒 index 次数的平均值。索引每秒 index 请求次数计算规则：每隔一个统计周期（5分钟）记录一次索引历史所有分片 index 总次数（_cat/shard?h=indexing.index_total），取相邻两次索引 index 总次数的差值，即一个周期内的绝对值并进行计算：index 次数 / 300秒，得出统计周期内每秒 index 请求次数的平均值。	-
查询速度	每单位统计周期内，索引或自治索引接收到的每秒 search 次数的平均值。索引每秒 search 请求次数计算规则：每隔一个统计周期（5分钟）记录一次索引历史所有分片 search 总次数（_cat/shard?h=search.query_total），取相邻两次索引 search 总次数的差值，即一个周期内的绝对值并进行计算：search 次数 / 300秒，得出统计周期内每秒 search 查询次数的平均值。	-

写入延迟	写入延迟（index_latency），指单次 index 请求平均耗时（ms/次）。单次 index 请求平均耗时计算规则：每隔一个统计周期（5分钟）记录一次索引的两个指标，索引历史所有分片 index 总耗时（_cat/shard?h=indexing.index_time）和 索引历史所有分片 index 总次数（_cat/shard?h=indexing.index_total），取相邻两次记录的差值，即一个周期内的绝对值并进行计算：index 耗时 / index 次数，得出统计周期内单次 index 平均耗时。	写入延迟，是指单个文档写入平均耗时。写入延迟过高时，建议调大索引分片数或增加集群节点规格或节点个数。
查询延迟	查询延迟（search_latency），指单次 query 请求平均耗时（ms/次）。单次 search 请求平均耗时计算规则：每隔一个统计周期（5分钟）记录一次索引的两个指标，索引历史所有分片 search 总耗时（_cat/shard?h=search.query_time）和 索引历史所有分片 search 总次数（_cat/shard?h=search.query_total），取相邻两次记录的差值，即一个周期内的绝对值并进行计算：search 耗时 / search 次数，得出统计周期内单次 search 平均耗时。	查询延迟，是指单个查询平均耗时。查询延迟过高时，建议结合查询profile做查询优化或增加集群节点规格或节点个数。

索引配置管理

最近更新时间：2024-10-12 21:50:11

操作场景

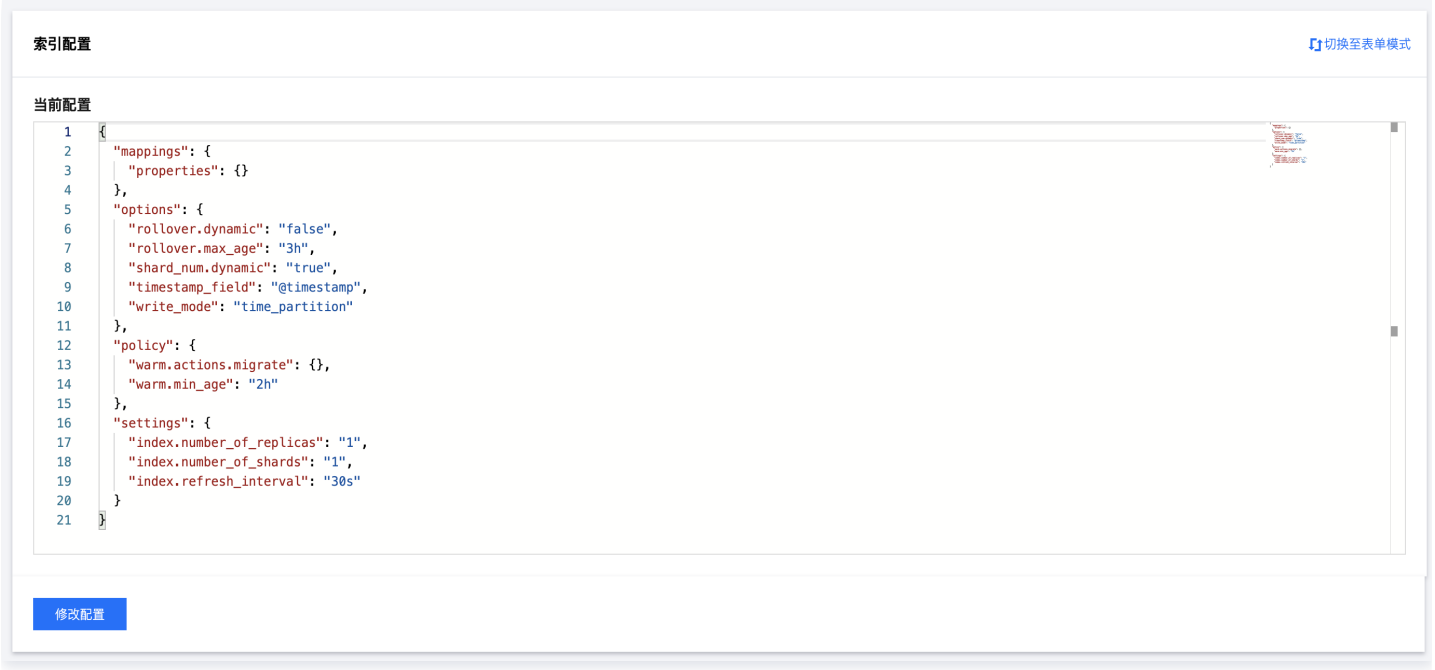
数据管理提供对索引进行配置管理的功能，您可通过**配置管理**页面，快速查看该索引的配置。同时，您可在配置管理页面，进行索引配置的修改，以快速适应业务发展。

操作步骤

1. 登录 Elasticsearch Service 控制台 。
2. 在 ES 索引管理选择对应的集群，在索引列表单击**更多**，下拉选择**配置管理**，进入索引配置管理页面。

查看模式

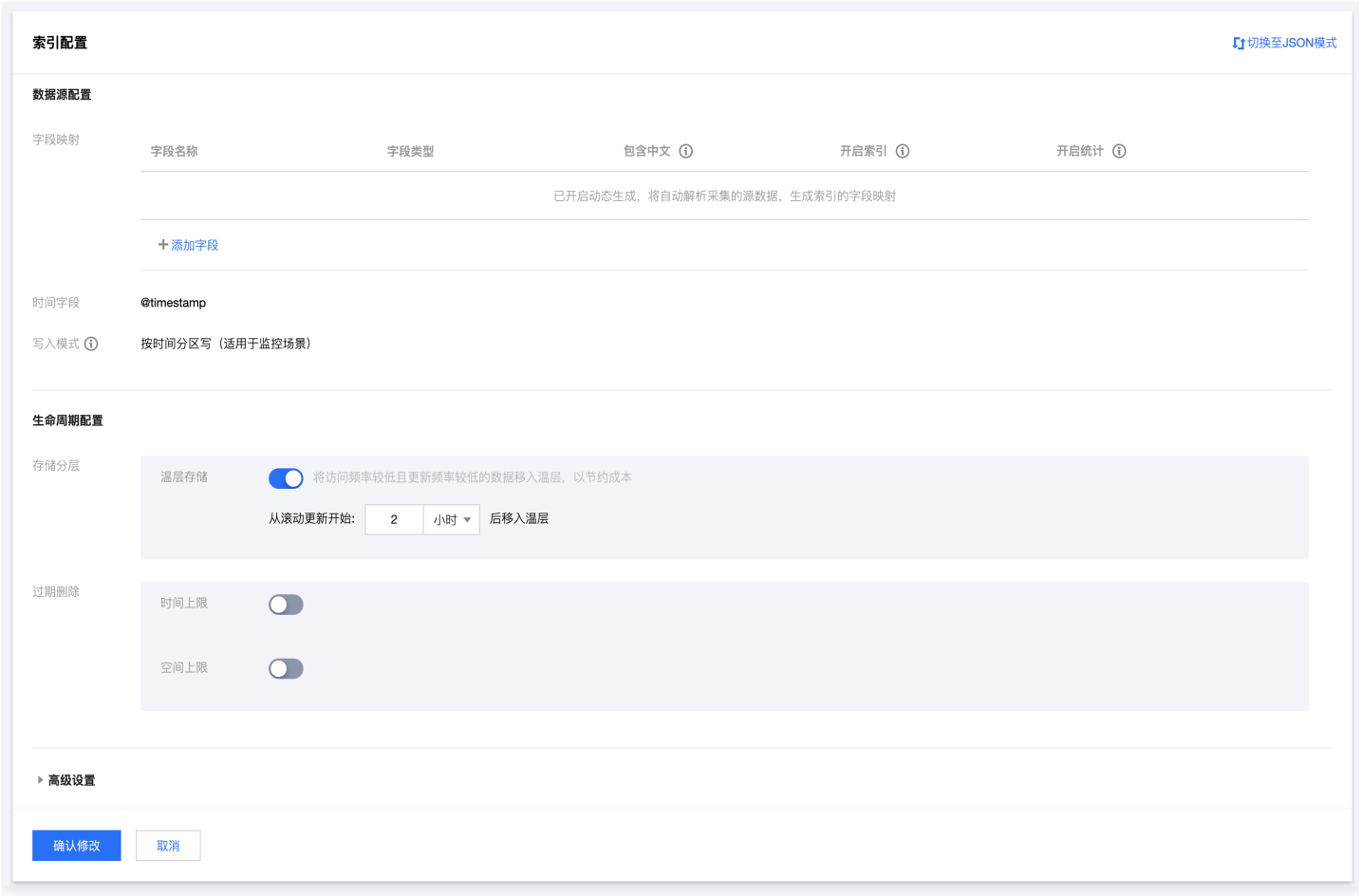
进入该页面后，默认为查看模式，包括数据源配置、生命周期配置以及高级设置的相关信息，同时，您可通过单击右上角**切换至 JSON 模式**，以 JSON 格式查看索引当前配置信息。



界面编辑模式

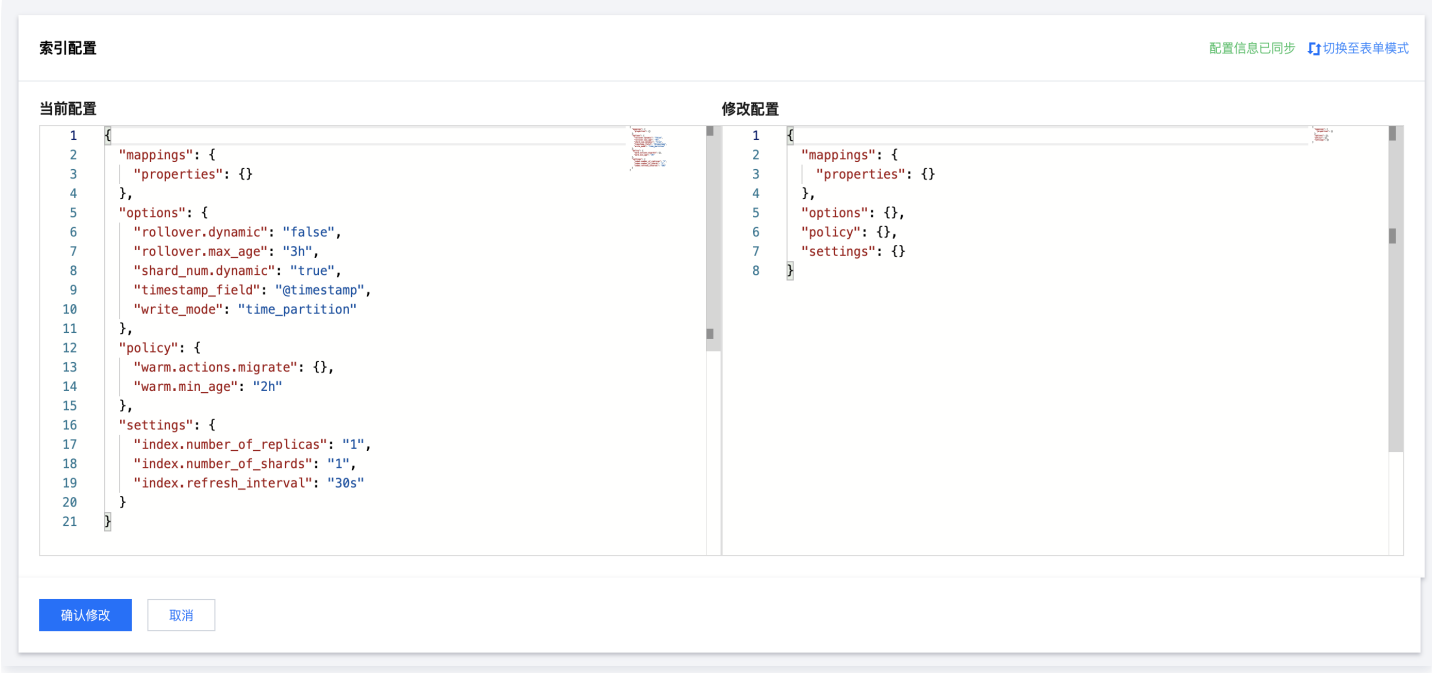
在查看模式下，单击左下角**修改配置**，可进入编辑模式，您可进行索引配置的信息的修改。修改配置成功后，生命周期的相关配置将在所有后备索引中生效，其他配置例如分片数、副本数、字段映射等仅在后续滚动出的后备索引中生效，已有的后备索引不会更新。

> **注意：**
> 时间字段与写入模式不可修改。



JSON 模式

切换至 JSON 编辑模式后，左侧为当前配置信息，方便您查看当前线上正在运行的索引的配置信息，右侧为修改配置输入框，在输入框中输入需修改的配置信息，配置修改成功后，对应的索引配置项即可更新。



如图样例所示，将移入温层存储的时间从2小时修改为了2天，单击**确认修改**，配置即可更新。