阿里云
Elasticsearch

监控报警

文档版本：20190711

法律声明

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

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	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，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	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。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 阿里云Elasticsearch云监控报警

阿里云Elasticsearch已支持对实例进行监控，并允许通过短信接收报警。您可以根据需求，自定义报警阈值。本文档为您介绍阿里云Elasticsearch云监控报警的配置方法，帮助您快速地使用云监控报警对实例进行实时监控。

监控报警项

> **注意:**
> 强烈建议您配置监控报警。

以下三个报警项较为重要，强烈建议您进行配置。

- 集群状态。

  主要监控集群状态为绿色还是红色。
- 节点磁盘使用率(%)。

  报警阀值控制在75%以下，不要超过80%。
- 节点HeapMemory使用率(%)。

  报警阀值控制在85%以下，不要超过90%。

建议您同时配置以下几个报警项。

- 节点CPU使用率(%)。

  报警阀值控制在95%以下，不要超过95%。
- 节点load_1m。

  以CPU核数的80%为参考值。
- 集群查询QPS(Count/Second)。

  以实际测试结果作为参考。
- 集群写入QPS(Count/Second)。

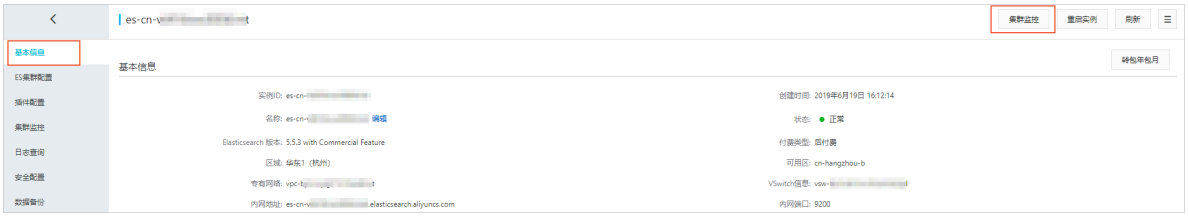
  以实际测试结果作为参考

进入云监控报警控制台

阿里云Elasticsearch为您提供以下两种方式进入云监控报警控制台。

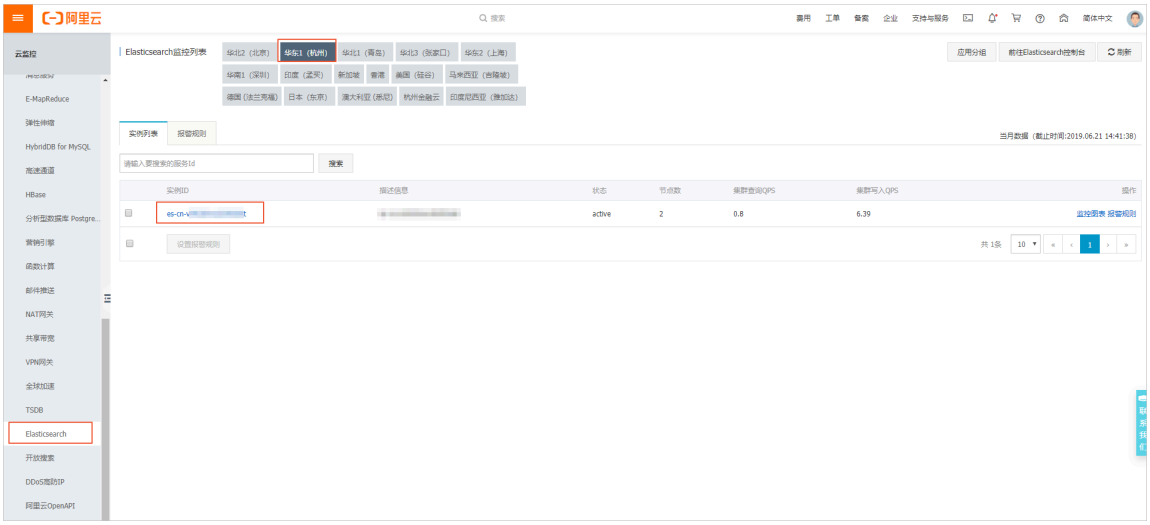
- Elasticsearch控制台。

  登录阿里云Elasticsearch控制台，单击实例ID。在实例的基本信息页面，单击右上角的集群监控，即可进入对应Elasticsearch实例的云监控控制台页面。



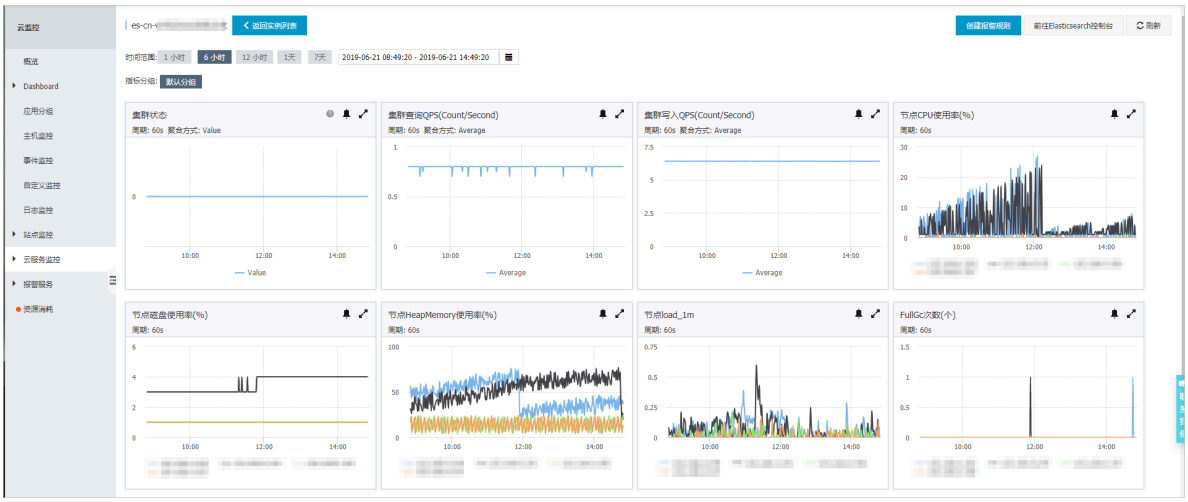
- 云监控控制台。

  1. 登录阿里云控制台，选择产品导航栏下的云监控。
  2. 在云监控控制台中，单击左侧菜单栏的云服务监控 > Elasticsearch。
  3. 选择实例所在区域，并单击实例ID，即可进入对应Elasticsearch实例的云监控控制台页面。



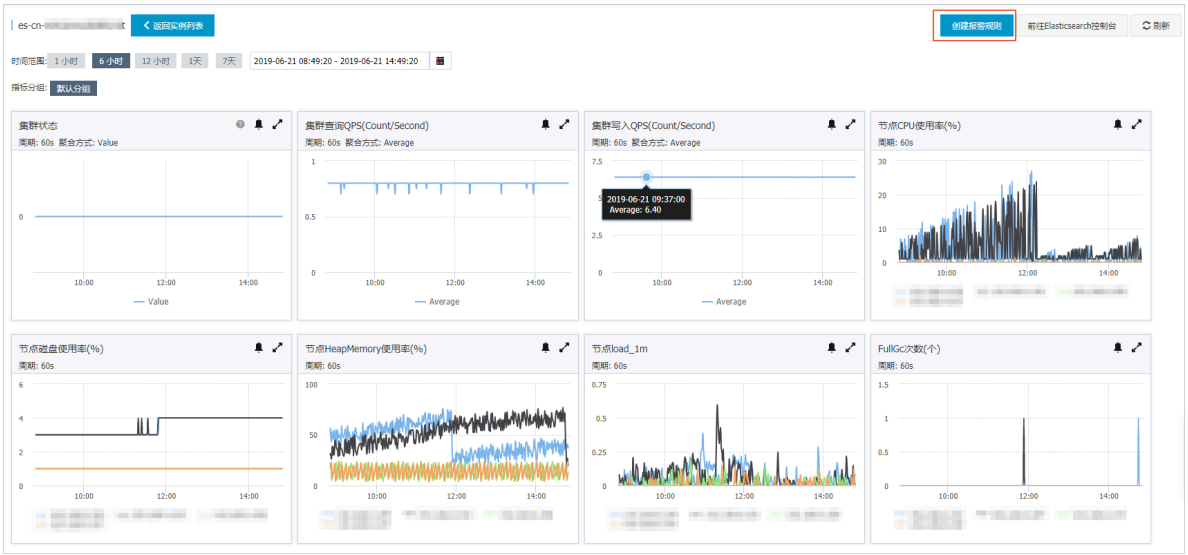
监控指标配置

1. 进入您阿里云Elasticsearch实例的云监控报警控制台。



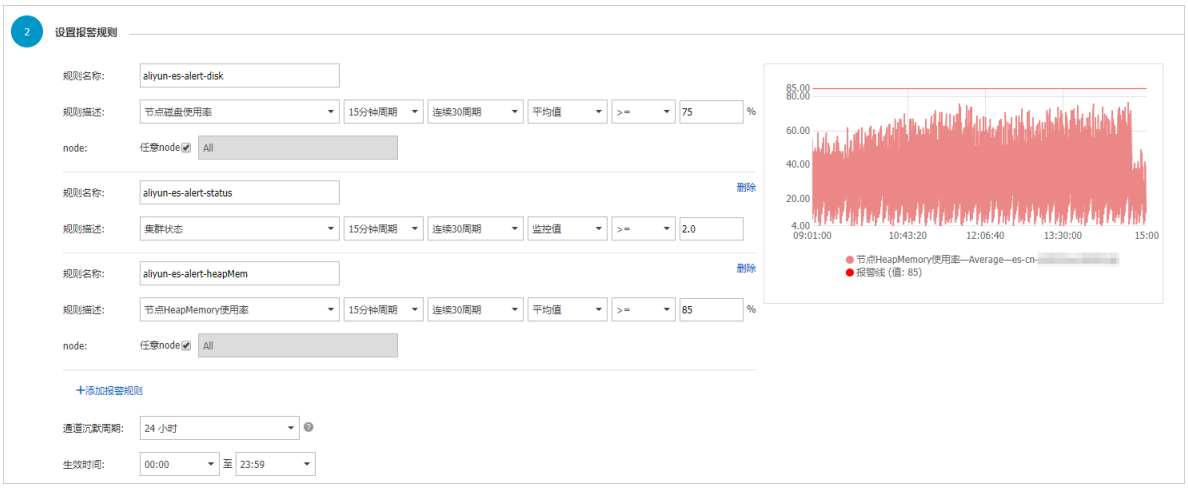
您可在此页面查看集群的历史监控数据，目前只保留一个月内的监控信息。通过创建报警规则，可对此实例配置报警监控。

2. 在实例的云监控控制台页面，单击右上角的创建报警规则 。



3. 在创建报警规则页面，设置报警规则。

以添加节点磁盘使用率监控、集群状态监控、节点HeapMemory使用率监控为例，添加方式如下图所示。



- 集群的状态对应Green、Yellow、Red，转换成数值对应0.0、1.0、2.0。所以在配置集群状态报警指标时，需要按照对应数值的大小进行报警配置。
- 通道沉默时间是指，同一个指标在一定时间范围内，只会触发一次报警。

> **说明:**
> 其他参数说明请参见报警规则参数说明。

4. 配置通知方式，选择云账号报警联系人。

   如果您还没有报警联系组，可以单击快速创建联系人组，进行创建。

5. 单击确认，保存报警配置，完成配置。

   配置完成后，Elasticsearch实例的监控信息将在实例正常生产后5分钟内开始采集，并提供监控数据展示。

2 XPack Watcher

本文档为您介绍XPack Watcher的配置方法。您可以通过添加XPack Watcher实现当满足某些条件时执行某些操作，比如当`logs`索引中出现`error`日志时，自动发送报警邮件或钉钉消息。可以简单的理解为Watcher是一个基于Elasticsearch实现的监控报警服务。

> 注意:
> XPack Watcher功能主要适用于单可用区的阿里云Elasticsearch实例，不支持跨多可用区的阿里云Elasticsearch实例。

功能介绍

XPack Watcher功能主要由`Trigger`、`Input`、`Condition`、`Actions`组成。

- `Trigger`

  确定何时检查，在配置Watcher时必须设置。支持丰富的时间计划方式，详情请参见Schedule Trigger。
- `Input`

  可以理解为您需要对监控的索引执行的筛选条件，详情请参见Inputs。
- `Condition`

  执行Actions的条件。
- `Actions`

  当条件发生时，执行的具体操作。

配置方式

阿里云Elasticsearch的Watcher功能不支持直接与公网进行通讯，需要基于阿里云Elasticsearch实例的内网地址来进行通讯（专有网络VPC环境）。如果您需要使用XPack Watcher，还需要购买一台能同时访问公网和阿里云Elasticsearch实例的阿里云ECS实例，作为代理去执行Actions。

以配置Webhook Action为例（Webhook采用钉钉群机器人）。

1. 购买阿里云ECS实例。

   购买的ECS要与阿里云Elasticsearch实例在同一个区域和VPC下，并且需要能够访问公网。

   > 注意:

- **阿里云ECS实例与阿里云Elasticsearch实例的VPC必须相同。**
- **阿里云ECS实例需要能访问公网。**

2. 配置安全组。

   a. 在阿里云ECS控制台的实例列表页面，单击对应实例右方的更多 > 网络和安全组 > 安全组配置。

   b. 在安全组列表右侧的操作栏下，单击配置规则。

   c. 在安全组规则页面，单击添加安全组规则。

   d. 填写相关参数，单击确定，即可完成配置。

   - 规则方向选择入方向。
   - 授权策略为默认的允许。
   - 协议类型选择自定义TCP。
   - 优先级通常默认即可。

- 端口范围填写您常用的端口（配置Nginx时需要用到，本文以8080为例）。
- 授权类型选择IPv4地址段访问。
- 授权对象添加您购买的阿里云Elasticsearch实例所有节点的IP地址。

> **说明:**
> 您可以通过以下方式获取阿里云Elasticsearch实例的IP地址列表。
>
> 登录您购买的阿里云Elasticsearch实例的Kibana控制台，单击左侧菜单栏的Monitoring，再单击Nodes。

3. 配置Nginx代理。

   详情请参见Nginx安装配置。

   a. 修改Nginx配置文件，参考以下配置替换Nginx安装配置中描述的`server`部分的配置。

```
server
  {
    listen 8080;#监听端口
    server_name localhost;#域名
    index index.html index.htm index.php;
    root /usr/local/webserver/nginx/html;#站点目录
      location ~ .*\.(php|php5)?$
    {
      #fastcgi_pass unix:/tmp/php-cgi.sock;
      fastcgi_pass 127.0.0.1:9000;
      fastcgi_index index.php;
      include fastcgi.conf;
    }
    location ~ .*\.(gif|jpg|jpeg|png|bmp|swf|ico)$
    {
      expires 30d;
  # access_log off;
    }
    location / {
      proxy_pass 钉钉机器人webhook地址，直接拷贝过来粘贴就行;
    }
    location ~ .*\.(js|css)?$
    {
      expires 15d;
   # access_log off;
    }
    access_log off;
  }
}
```

   b. 配置修改完成后，加载新配置文件并重启Nginx。

```
/usr/local/webserver/nginx/sbin/nginx -s reload            # 重新载入配置文件
/usr/local/webserver/nginx/sbin/nginx -s reopen            # 重启Nginx
```

> **说明:**

您可以通过以下方式获取钉钉群机器人的webhook地址。

创建一个钉钉报警接收群，在群的右上角找到群机器人，然后添加一个自定义通过webhook接入的机器人，并获取群机器人的webhook地址。详情请参见自定义机器人。

4. 设置报警。

登录阿里云Elasticsearch实例的Kibana控制台，单击左侧菜单栏的Dev Tools，在Console中使用API创建一个报警文档。

下文以创建`log_error_watch`为例，每隔`10s`查询`logs`索引中是否出现`error`日志，如果出现`0`次以上则触发报警。

```
PUT _xpack/watcher/watch/log_error_watch
{
  "trigger": {
    "schedule": {
      "interval": "10s"
    }
  },
  "input": {
    "search": {
      "request": {
        "indices": ["logs"],
        "body": {
          "query": {
            "match": {
              "message": "error"
            }
          }
        }
      }
    }
  },
  "condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gt": 0
      }
    }
  },
  "actions" : {
  "test_issue" : {
    "webhook" : {
      "method" : "POST",
      "url" : "http://您的ECS内网IP:8080",
      "body" : "{\"msgtype\": \"text\", \"text\": { \"content\": \"
error 日志出现了，请尽快处理\"}}"
    }
  }
}
}
```

 说明:

上述actions中配置的url必须是您购买的与阿里云Elasticsearch实例相同区域和VPC的阿里云ECS实例的内网IP地址，并且已经按照上述方式进行了安全组配置，否则不能进行通信。

如果您不再需要执行报警任务，可以使用以下命令删除该报警任务。

```
DELETE _xpack/watcher/watch/log_error_watch
```

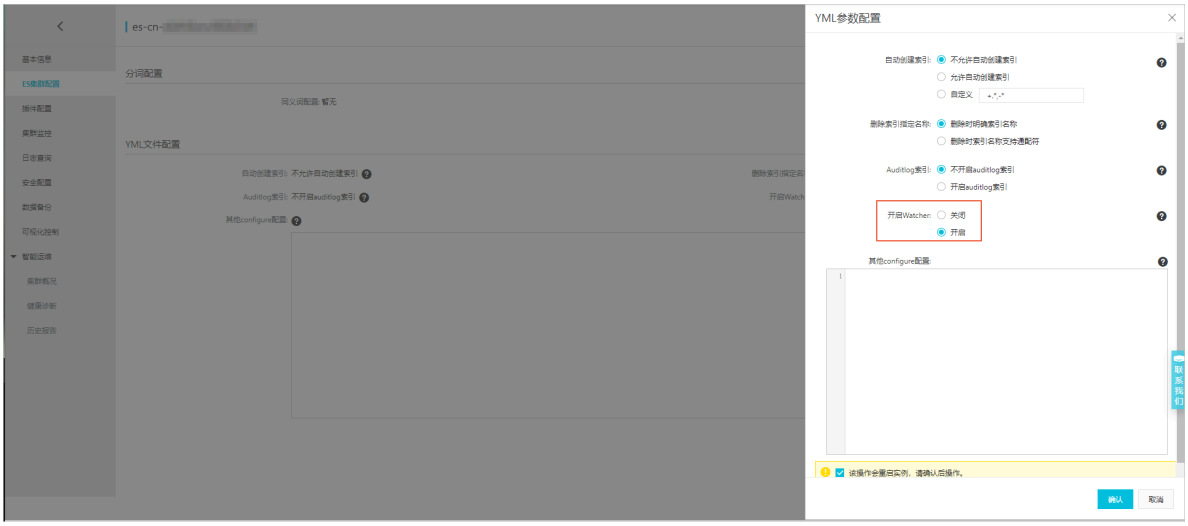
常见问题

问题：在设置报警时出现`No handler found for uri [/_xpack/watcher/watch/log_error_watch_2] and method [PUT]`异常。

解决方法：设置报警时以上异常，表示您购买的阿里云Elasticsearch实例未开启Watcher功能，可通过以下方式开启。

1. 登录阿里云Elasticsearch控制台，单击实例ID > ES集群配置。
2. 在ES集群配置页面，单击YML文件配置右侧的修改配置。
3. 在YML参数配置页面，将开启Watcher设置为开启。

> 注意:
> 开启Watcher操作会触发集群重启，为保证您的业务不受影响，请确认后操作。



4. 勾选该操作会重启实例，请确认后操作，然后单击确认。

   重启过程约持续30分钟，请耐心等待。重启完成后，即可完成Watcher的开启。

3 监控日志

阿里云Elasticsearch提供开源 Elasticsearch 5.5.3版本，及商业版 x-pack 插件服务，致力于数据分析、数据搜索等场景服务。在开源 Elasticsearch 基础上提供企业级权限管控、安全监控告警、自动报表生成等功能。

Monitoring日志配置

日志采集

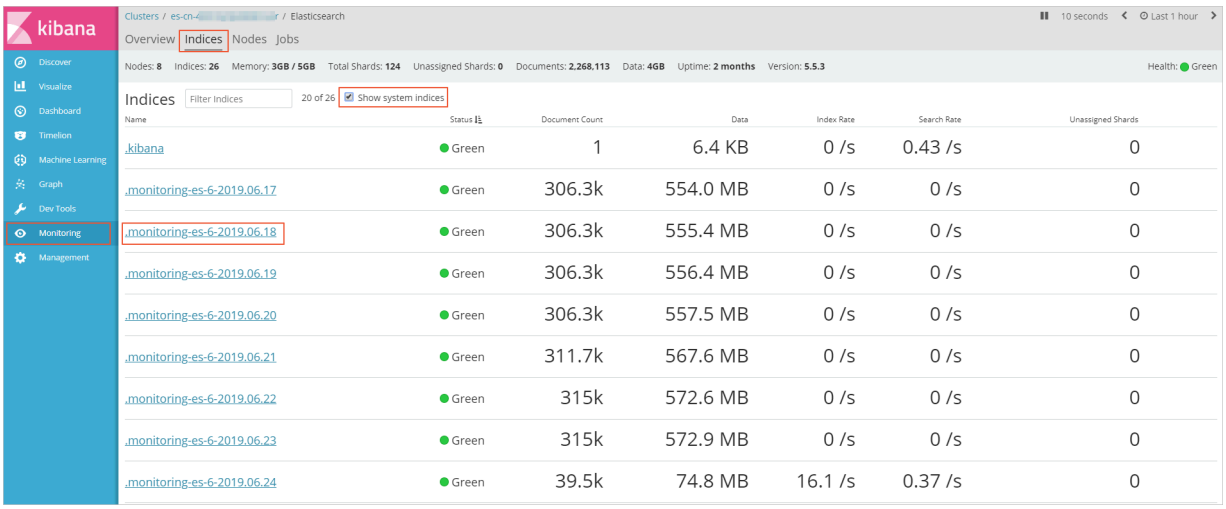
默认情况下 x-pack 监控客户端，会每隔10s采集集群的监控信息到您购买实例的以.monitoring-*为前缀的索引中。

目前主要有.monitoring-es-6-*、.monitoring-kibana-6-*这两种索引，以天为单位滚动创建。采集完的信息会保存在以.monitoring-es-6-为前缀，加当前日期为后缀的索引中。

其中.monitoring-es-6-*索引相对占用磁盘空间较大，主要存放了集群状态、集群统计、节点统计、索引统计等信息。

显示系统索引

可在Kibana页面中，选中Show system indices查看对应监控索引，占用空间大小。



日志保留设置

默认保留最近7天的监控索引，此类.monitoring-es-6-*索引会占用您购买的阿里云ES实例存储空间。索引的大小跟您集群中索引个数（包含系统索引）节点个数有关系。为了避免您购买的实例大部分空间被监控索引所占用，可通过以下两种方案优化。

1. 可通过以下 API 设置监控索引保留天数。

```
PUT _cluster/settings
{"persistent": {"xpack.monitoring.history.duration":"1d"}}
```

```
# 需要保留的天数按照您的需求而定，最少保留一天。
```

2. 设置需要采集监控的索引。

   可以通过 API 设置，哪些索引需要监控及哪些索引不需要监控。以减少.monitoring-es-6-*索引占用磁盘空间，本文以禁掉采集系统索引为例。

```
PUT _cluster/settings
{"persistent": {"xpack.monitoring.collection.indices": "*,-.*"}}
# 禁掉的索引监控信息将不会在Kibana页面中Montioring模块中看到，比如在索引列表及索引监控信息页面，都看不到禁掉的索引信息。就会出现_cat/indices获取的索引列表，跟在Kibana页面中Montioring模块中看到的索引列表不同的情况。
```

 说明:

实际使用中，您可以参考以上2种方案结合使用，以节省您购买的磁盘空间。