阿里云 MVP

Elasticsearch 的监控与报警

阿里云技术专家 李靖威

阿里云 MVP

自建 ELASTICSEARCH 集群

阿里云 MVP

监控分类

- 资源
- 容器
- 应用
  - 集群
  - 索引
- 调用

阿里云 MVP

第三方监控

- ElasticHD
- Kopf
- Datadog
- Xpack Monitoring

阿里云 MVP

ES 监控接口

- GET /_nodes/stats
- GET /_cluster/stats
- GET /index_name/_stats
- GET /_cluster/health
- GET /_cluster/pending_tasks

阿里云 MVP

ELASTICSEARCH X-PACK

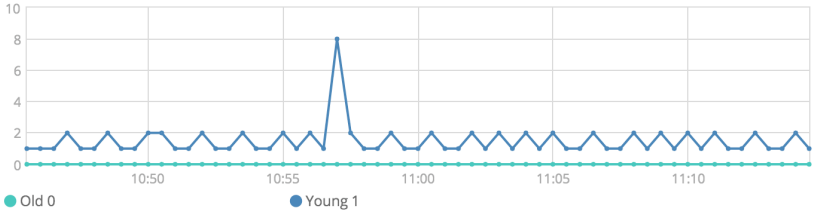
kibana

Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management

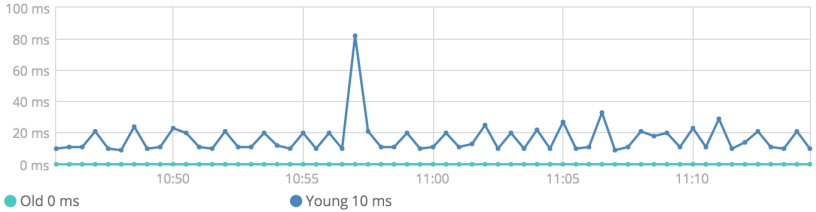
Overview Advanced

127.0.0.1:9300 JVM Heap: **33%** Free Disk Space: **208.1 GB** Documents: **1.8m** Data: **747.8 MB** Indices: **26** Shards: **43** Type: **Master Node** Health: Online

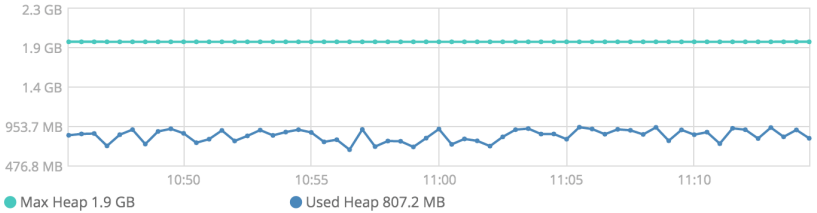
GC Count



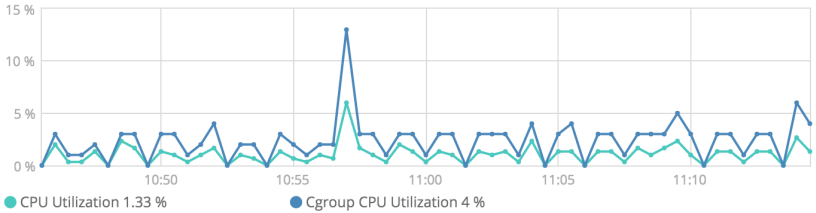
GC Duration (ms)



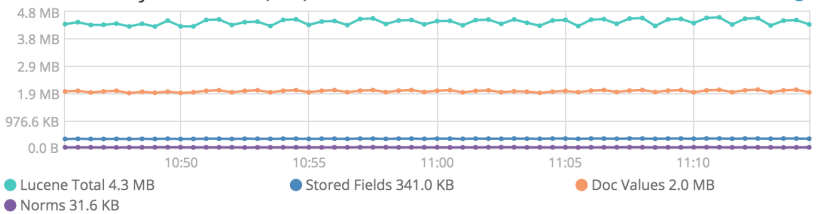
JVM Heap (GB)



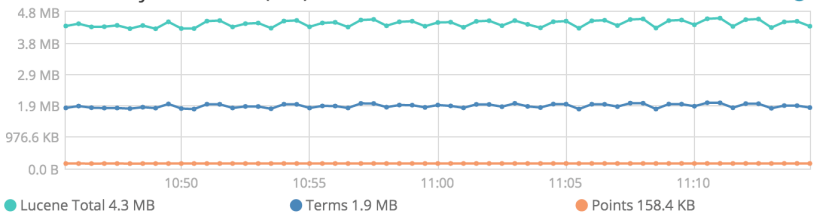
CPU Utilization (%)



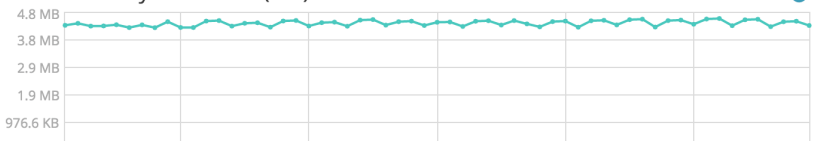
Index Memory - Lucene 1 (MB)



Index Memory - Lucene 2 (MB)



Index Memory - Lucene 3 (MB)



Index Memory - Elasticsearch (KB)

elastic
Logout
Collapse

Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management

Overview | Indices | Nodes

Nodes: **1** Indices: **26** Memory: **661MB / 2GB** Total Shards: **87** Unassigned Shards: **44** Documents: **1,826,800** Data: **748MB** Uptime: **41 minutes** Version: **5.4.0** Health: Red

Indices

Filter Indices

5 of 5 Show system indices

Name	Status	Document Count	Data	Index Rate	Search Rate	Unassigned Shards
metricbeat-2017.04.24	Red	79.9k	29.0 MB	0 /s	0 /s	3
metricbeat-2017.04.28	Yellow	113.5k	76.1 MB	28.03 /s	0 /s	5
metricbeat-2017.04.27	Yellow	502.8k	187.9 MB	0 /s	0 /s	5
metricbeat-2017.04.26	Yellow	638.6k	233.8 MB	0 /s	0 /s	5
metricbeat-2017.04.25	Yellow	261.8k	95.4 MB	0 /s	0 /s	5

elastic
Logout
Collapse

阿里云 MVP

X-Pack Monitoring 原理

- Collectors
- Watcher
- .monitoring 索引
- .monitoring-alerts 索引

阿里云 MVP

X-Pack Monitoring Collectors

- ClusterStatsCollector
- IndexRecoveryCollector
- IndexStatsCollector
- JobStatsCollector
- NodeStatsCollector
- ShardsCollector

阿里云 MVP

X-Pack Monitoring

- 可监控 Kibana、Logstash
- 只有邮件报警通知

阿里云 MVP

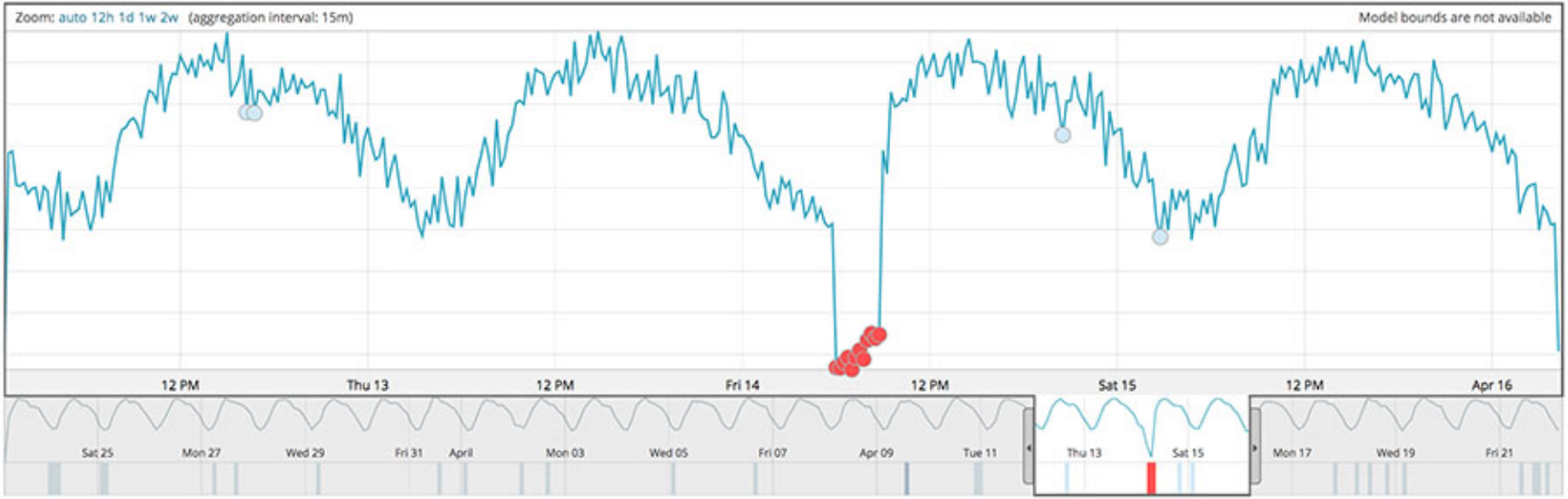
X-Pack Watcher

- 报警基础组件
- xpack monitoring 内置 watcher：
  - Cluster Stats
  - Elasticsearch Version Mismatch
  - Kibana Version Mismatch
  - Logstash Version Mismatch
- 内置 watcher 通过写入 .alerts 索引，kibana 读取此索引展示在界面上

阿里云 MVP

Machine Learning

- 基于索引
- 异常值检测



Anomalies

Severity threshold: warning Interval: Auto

time	max severity	detector	found for	influenced by	actual	typical	description	job ID
April 14th 2017	98	sum(total) (mm-job-4)	app_1	service: app_1	938905	1705380	2x lower	mm-job-4

Description:
critical anomaly in sum(total) (mm-job-4) found for service app_1

Details on highest severity anomaly:

service:	app_1
time:	April 14th 2017, 06:00:00 to April 14th 2017, 06:15:00
function:	sum
fieldName:	total
actual:	938905
typical:	1705380
job ID:	mm-job-4
probability:	4.84657e-20

Influenced by:

service	app_1

April 15th 2017	< 1	sum(total) (mm-job-4)	app_1	service: app_1	1564560	1789200	1.1x lower	mm-job-4
April 12th 2017	< 1	sum(total) (mm-job-4)	app_1	service: app_1	2156840	2353140	1.1x lower	mm-job-4

阿里云 MVP

DEMO

阿里云 MVP

阿里云 ELASTICSEARCH

云监控
弹性伸缩
HybridDB for MySQL
高速通道
HBase
HybridDB
营销引擎
函数计算
邮件推送
NAT网关
共享带宽
VPN网关
全球加速
HiTSDB
Elasticsearch
报警服务

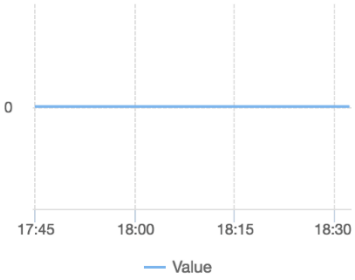
es-cn-4590f7jgq000nrxyi 返回实例列表

创建报警规则 | 前往Elasticsearch控制台 | 刷新

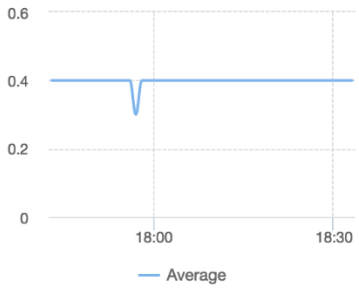
时间范围: 1小时 | 6小时 | 12小时 | 1天 | 7天 | 2018-01-16 12:35:15 - 2018-01-16 18:35:15

指标分组: 默认分组

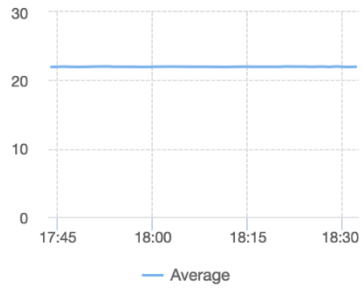
集群状态
周期: 60s 聚合方式: Value



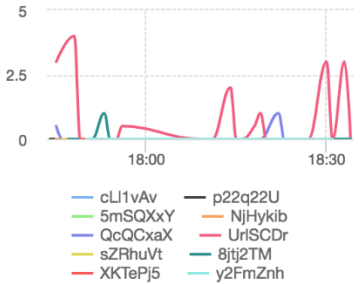
集群查询QPS(Count/Second)
周期: 60s 聚合方式: Average



集群写入QPS(Count/Second)
周期: 60s 聚合方式: Average

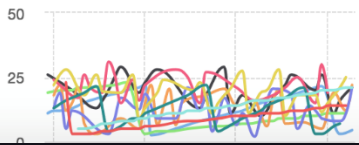


节点CPU使用率(%)

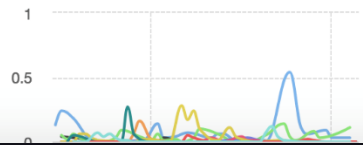


节点磁盘使用率(%)

节点HeapMemory使用率(%)



节点load_1m



云监控

1 关联资源

产品: ElasticSearch

资源范围: 实例 选择应用分组时，支持使用报警模板。点击 查看报警模板最佳实践

地域: 华东 1

实例: es-cn-4590f7jgq000nr... 共1个

2 设置报警规则

规则名称:

规则描述: 节点磁盘使用率 | 5分钟 | 平均值 | >= | 阈值 %

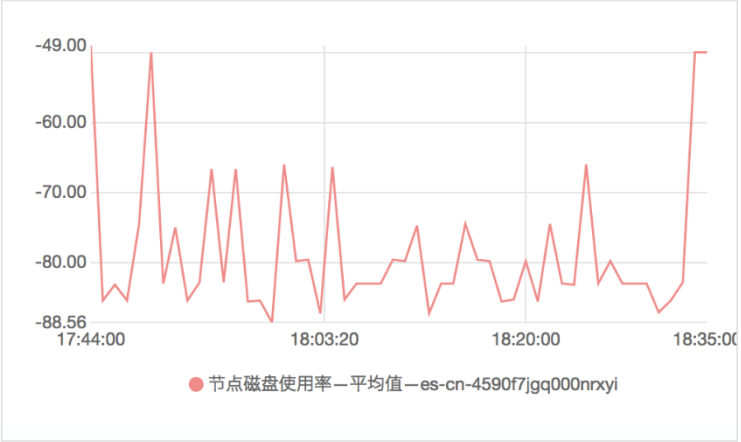
node: 任意node All

+添加报警规则

通道沉默时间: 24小时

连续几次超过阈值后报警: 1

生效时间: 00:00 至 23:59



阿里云 MVP

阿里云 Elasticsearch 监控报警

- 基于阿里云云监控
- 联系人分组
- 手机、邮箱、旺旺、钉钉
- 支持报警回调
- 数据来源于 xpack 生成的 .monitoring 索引

阿里云 MVP

DEMO

Thanks!