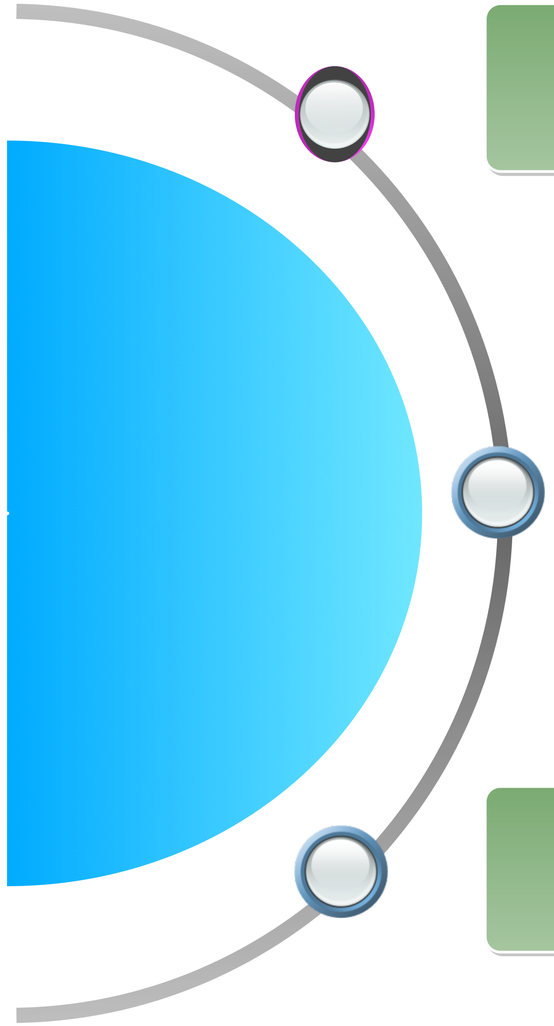
EYou—阿里云Elasticsearch智能诊断系统

张家杰（梵寞）

目录

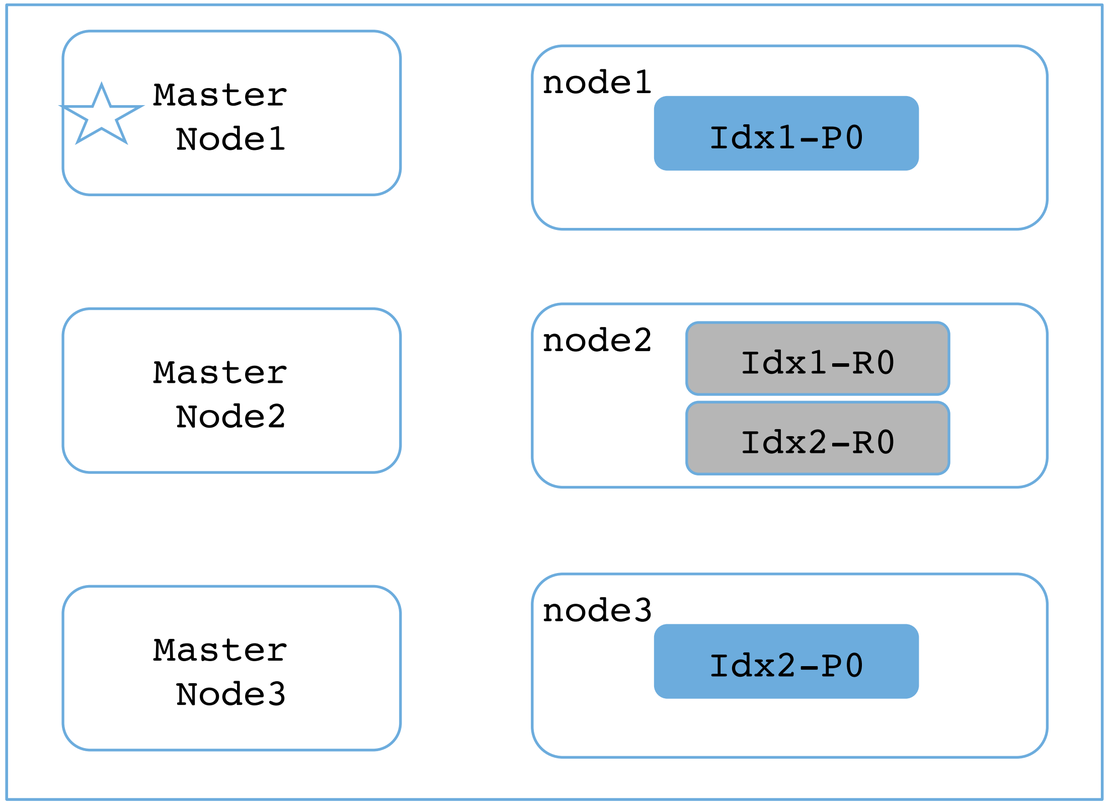


问题

- ✓ 用户多集群多
- ✓ 业务场景差异大
- ✓ 使用姿势异常丰富
- ✓ 用户问题多

- ✓ 如何让用户更自主高效的使用ES?
- ✓ 如何让用户全方位的了解自己的集群?

EYou | Green Is OK ?



- ✓ 监控指标多且分散

  —指标意义不明确

- ✓ 问题发现滞后

  —无法提前预防

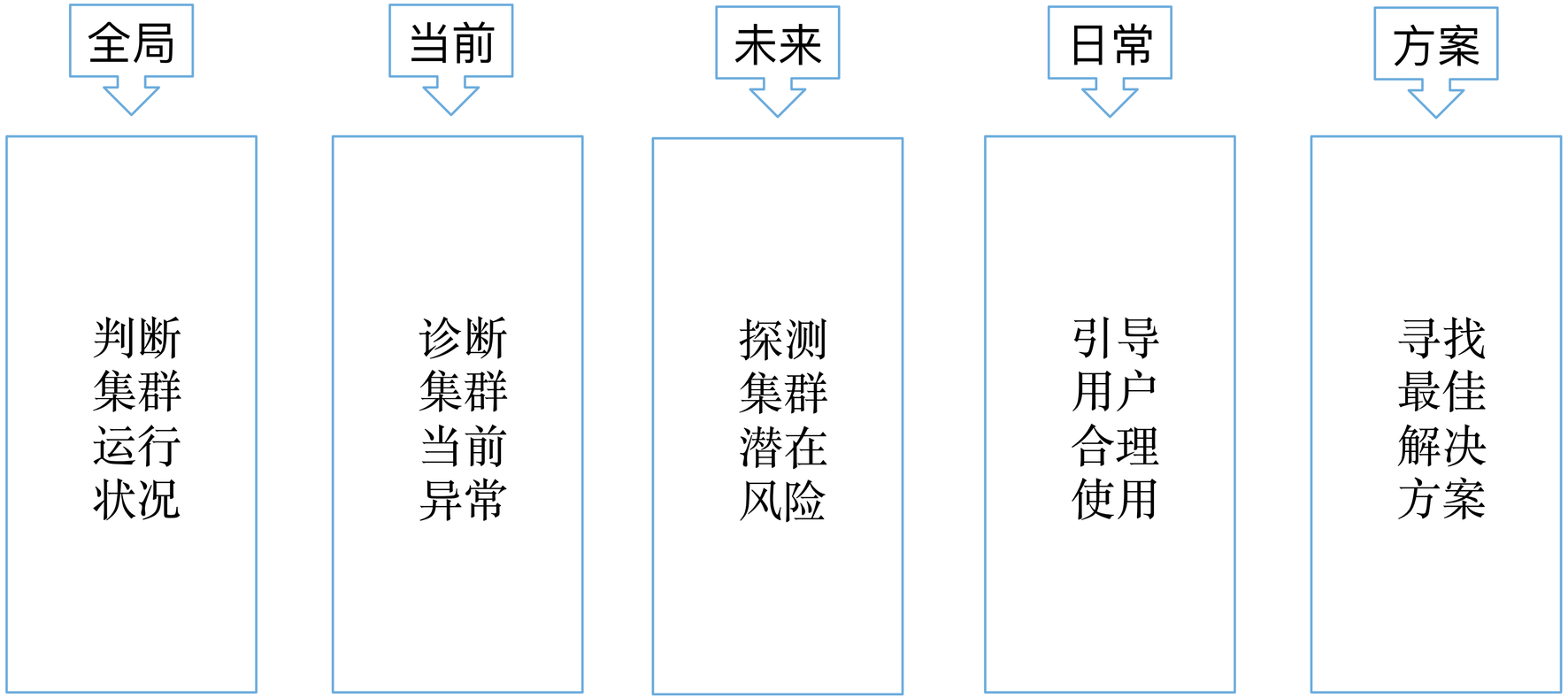
- ✓ 问题分析定位门槛高

  —需要有一定的专业知识

EYou |EYou ?

EYou是阿里云Elasticsearch智能诊断系统。

目标：更全方面的了解ES集群健康，寻找更佳的使用方式



EYou | 诊断项

诊断项是可以直接反馈ES集群某一个状态或行为是否合理的指标。

华东1 (杭州)

es-c[redacted]

立刻诊断

历史诊断报告

索引名称:

请输入要诊断的索引名，多个索引用逗号,分隔；默认全部索引

诊断项:

- [x] 集群颜色状态诊断
- [x] 集群master分配诊断
- [x] 集群存储资源诊断
- [x] 集群计算资源诊断
- [x] 索引shard合理性诊断

- scheduled__2018-07-[redacted] 16 03:31:13)
- scheduled__2018-07-[redacted] 15 03:31:10)
- scheduled__2018-07-[redacted] 14 03:31:10)
- scheduled__2018-07-[redacted] 13 03:31:10)
- scheduled__2018-07-12T03:30:00 (2018-07-12 03:31:08)
- scheduled__2018-07-11T03:30:00 (2018-07-11 03:31:10)
- scheduled__2018-07-10T03:30:00 (2018-07-10 03:31:06)
- scheduled__2018-07-09T03:30:00 (2018-07-09 03:31:09)

索引shard数可能需要调整。按照当前索引大小计算，给出了参考方案，但实际操作时且要尽可能匹配节点数。

Action:

参考方案:

[redacted]18-07-05 [1GB] [3 -> 1]
[redacted]18-07-04 [size < 1GB] [3 -> 1]
[redacted]18-07-03 [size < 1GB] [3 -> 1]
[redacted]s-2018-07-03 [size < 1GB] [3 -> 1]
[redacted]s-2018-07-02 [size < 1GB] [3 -> 1]

诊断结果

查看原始文件

集群整体诊断结果

实例ID: [redacted] 诊断时间: 2018-07-03 20:43:10

集群颜色状态诊断

诊断集群基本颜色状态，检查副本分配情况
颜色不正常的索引会影响数据读写。黄色索引副本丢失，会影响到数据的可靠性和读写性能；红色索引会引起数据丢失或者kibana加载异常，最高优处理

诊断结果及建议:

磁盘空间不足导致集群颜色异常[RED]，丢失索引分片，如: [[redacted], .kibana, .security, [redacted]]。建议扩充磁盘空间至少到 9000GB，或者参考<集群存储资源诊断>

Action:

GET /_cluster/allocation/explain GET /_cluster/health GET /_cat/indices?v

集群存储资源诊断

诊断集群存储空间是否充足
磁盘使用超过85%的时候将不允许创建新索引，超过90%就会尝试重新分配分片。空间不足时可能会导致新索引创建不出来，分片丢失，kibana加载异常，负载增加等，高优处理

诊断结果及建议:

磁盘空间不足，最大使用率为 94.92，报警次数 WARN[2726次] CRITICAL[1364次]

Action:

建议集群总体磁盘扩容到 9000 GB，单节点容量[1500 -> 1800 GB]，节点个数[4 -> 5]

EYou | 产品

集群计算资源诊断

诊断集群节点和规格是否充足
计算资源不足会全方面影响到集群稳定性，读写性能

诊断结果及建议：

计算资源不足。
报警次数 CPU[99次] JVM[0次]
系统资源使用情况：CPU.AVG[12.93] JVM.AVG[57.9] LOAD.AVG[1.8] CPU.MAX[100.0] JVM.MAX[100.0] LOAD.MAX[16.06]

Action:

建议增加一个数据节点

集群状态频繁变更诊断

诊断集群状态变更是否合理
短时间频繁变更集群状态会给master节点带来很高的负担，GC频繁，负载突增，甚至阻塞相关索引的读写，影响性能

诊断结果及建议：

集群状态变更频繁，过去24小时内状态发生频繁变更
2018-07-03 19:24 -- 2018-07-03 20:42 连续变更358次
2018-07-02 20:43 -- 2018-07-03 19:21 连续变更1376次
2018-07-03 19:24 -- 2018-07-03 19:25 连续变更30次

Action:

请确认是否有频繁创建，删除，打开，关闭索引，如有请尽量在低峰期操作
请确认是否有频繁增加type，动态增加字段，如有请提前创建完整的mapping，尽量不使用动态映射
请确认是否有频繁修改索引或集群配置，如有请尽量在低峰期操作
请确认是否有集群变更，重启，节点上下线等操作

节点负载偏差过大诊断

诊断集群当天节点负载偏差是否过大
节点间负载不一致会使得某个节点成为系统瓶颈，影响集群稳定性

诊断结果及建议：

数据节点 负载相对较高。以下索引可能存在shard不均匀 [[...]]

Action:

请试着调整shard数或数据节点数，尽可能保证两者均衡

索引segment合理性诊断

诊断索引segment是否合理，是否需要优化
非大量写入情况下，过多的segment会降低查询性能，消耗内存，单条更新下性能极低

诊断结果及建议：

索引segment个数过多，索引列表如下：
[redacted] 期望segment数45 实际segment数71
[redacted] 期望segment数50 实际segment数77

Action:

建议可以在负载低峰时执行ES API：{indexName}/_forcemerge

索引shard合理性诊断

诊断索引的shard数和大小是否合理
shard不合理会极大的影响索引读写性能，meta信息过多会占用较高的系统资源

诊断结果及建议：

索引shard数可能需要调整。按照当前索引大小计算，给出了参考方案，但实际操作时需要考虑后续扩展且要尽可能匹配节点数。

Action:

参考方案:
[redacted] [1GB] [10 -> 1]
[redacted] [1GB] [10 -> 1]
[redacted] [size < 1GB] [10 -> 1]
[redacted] [size < 1GB] [10 -> 1]
[redacted] [size < 1GB] [10 -> 1]
[redacted] [size < 1GB] [10 -> 1]

EYou | 产品

节点shard数过多诊断

诊断集群当前节点shard数是否过多 单节点shard过多会大量消耗系统资源，读写失败，负载增加，索引加载异常等

诊断结果及建议：

部分节点shard个数过多，具体如下：[: 80311]

Action：

请考虑增加集群节点数到 [3 -> [illegible]]，或者提升规格到 [S2C8G -> S4C16G] 或者及时清理关闭无效索引，减少副本个数，减少shard个数

索引recovery过慢诊断

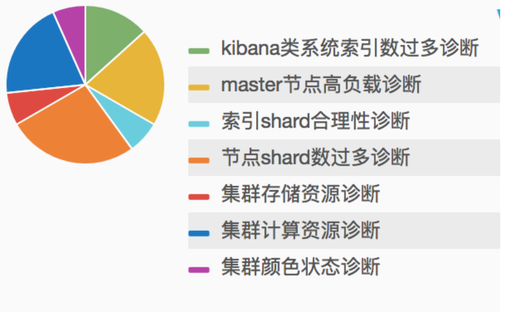
诊断集群当天索引recovery是否过慢

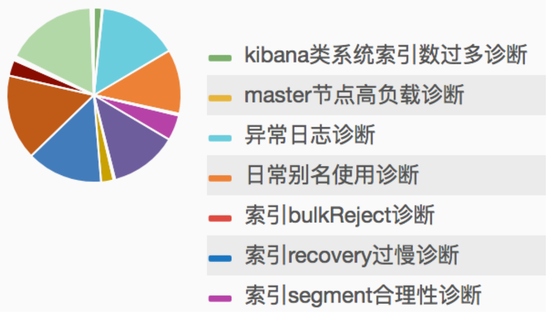
诊断结果及建议：

部分索引recovery过慢，最大耗时[190]min，最大任务数12582个，变更期间尽可能停止写操作，请考虑修改集群配置如Action

Action：

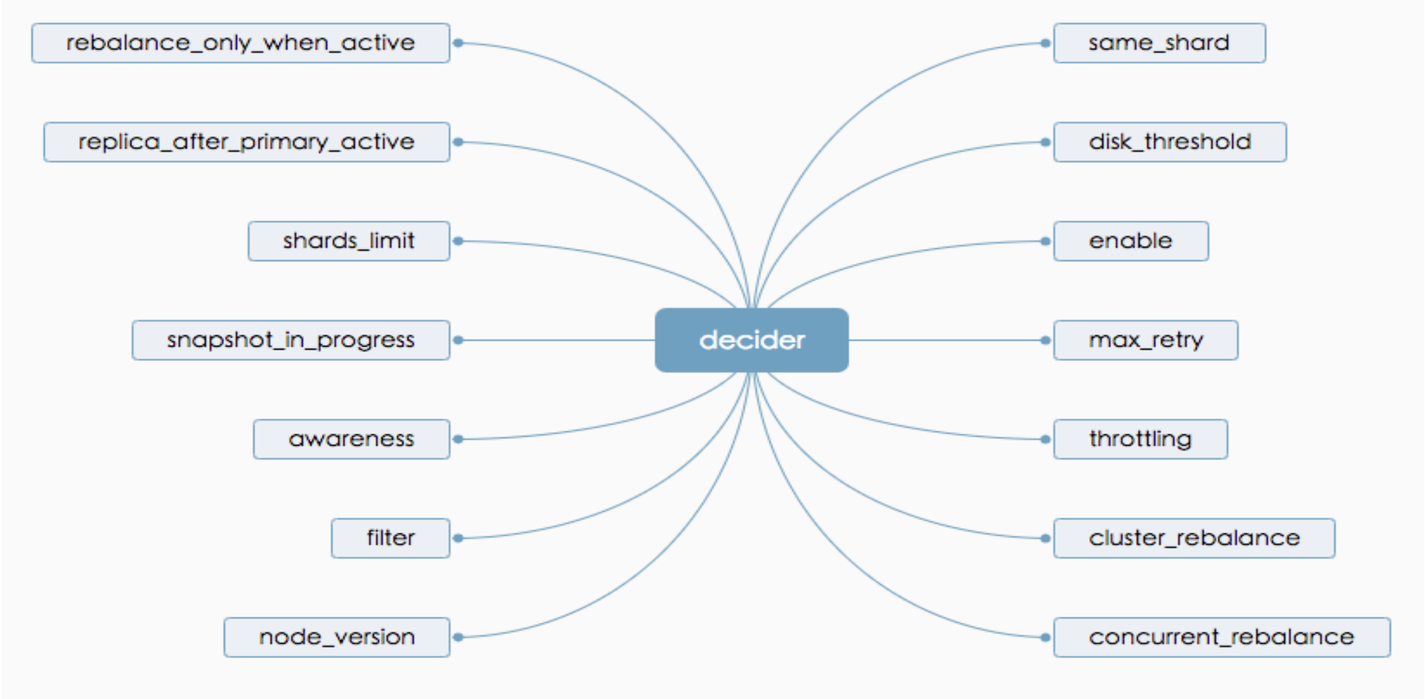
```
PUT _cluster/settings
{
  "transient" : {
    "cluster.routing.allocation.node_concurrent_recoveries":4,
    "cluster.routing.allocation.cluster_concurrent_rebalance":2,
    "indices.recovery.max_bytes_per_sec": "200mb"
  }
}
```





诊断项 | 集群颜色诊断

```
GET _cat/health?h=status
GET _cluster/allocation/explain
```




```
{
    "index": "ft2",
    "shard": 4,
    "primary": false,
    "current_state": "unassigned",
    "unassigned_info": {
        "reason": "REPLICA_ADDED",
        "at": "2018-06-27T11:51:17.670Z"
    },
    "can_allocate": "no",
    "allocate_explanation": "cannot allocate because allocation is not permitte
    "node_allocation_decisions": [
        {...},
        {
            "node_id": "RgmxR4vXSEuK32Dtnn8dyw",
            "node_attributes": {...},
            "node_decision": "no",
            "deciders": [
                {
                    "decider": "same_shard",
                    "decision": "NO",
                    "explanation": "the shard cannot be allocated to the same n
                },
                {
                    "decider": "disk_threshold",
                    "decision": "NO",
                    "explanation": "allocating the shard to this node will brin
                }
            ]
        },
        {...}
    ]
}
```

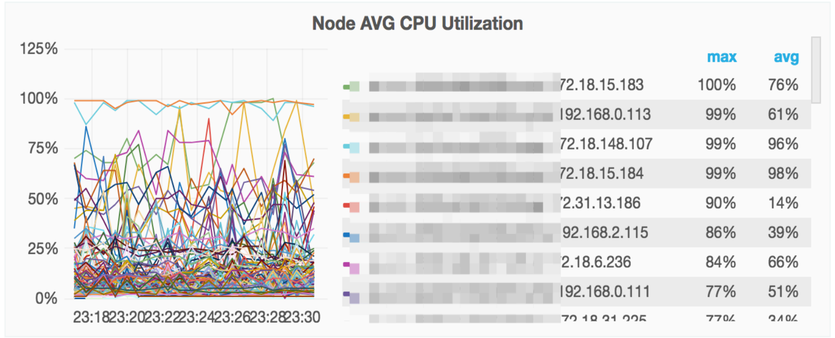
诊断项 | 集群计算/存储资源诊断

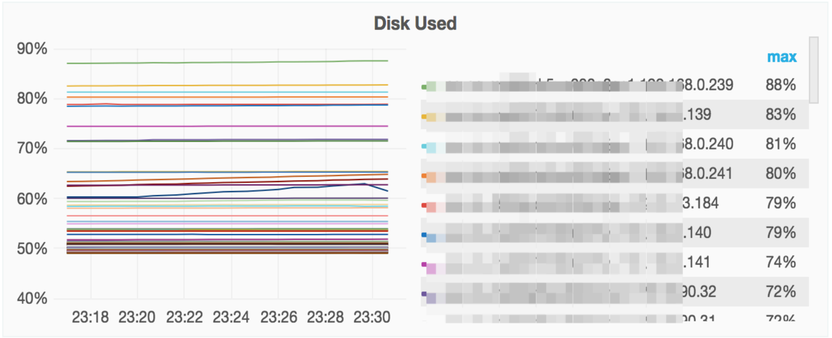
Monitor

Alarm

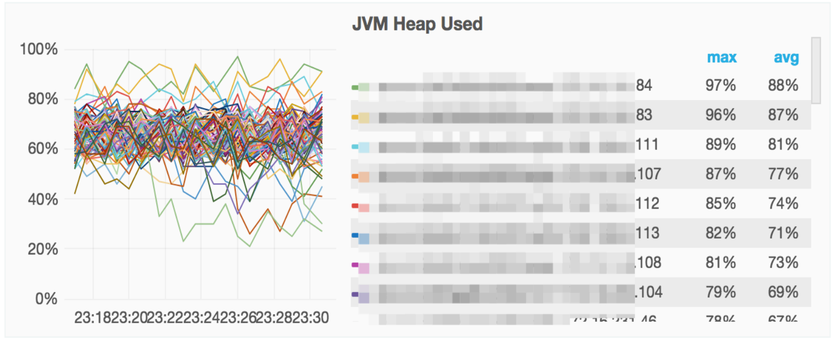
GET _cat/nodes

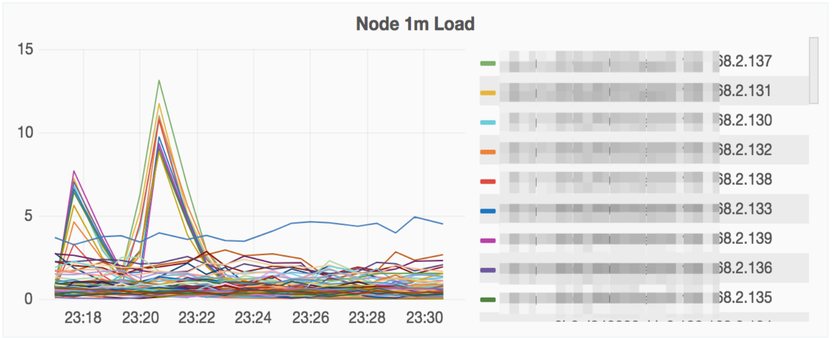
GET _cat/indices?h=h,pri.store.size





NODE STATES





诊断项 | 集群计算/存储资源诊断

使用场景不同，单节点最大承载数据量也会不同，具体如下：

```
数据加速，查询聚合等场景
    单节点最大数据量 = 单节点Mem(G) * 10
日志写入，离线分析等场景
    单节点最大数据量 = 单节点Mem(G) * 50
通常情况
    单节点最大数据量 = 单节点Mem(G) * 30
```

规格	最大节点数	单节点最大磁盘-查询	单节点最大磁盘-日志
2c4g	10	40 GB	200 GB
2c8g	10	80 GB	400 GB
4c16g	20	160 GB	800 GB
8c32g	40	320 GB	1.5 TB
16c64g	50	640 GB	2 TB

磁盘容量评估

影响ES集群磁盘空间因子大致如下：

```
1. 副本数量，至少1个副本
2. 索引开销，通常比源数据大10% ( _all等未计算)
3. 操作系统预留，默认操作系统会保留5%的文件系统供用户处理关键流程，系统恢复，磁盘碎片等
4. ES内部开销，段合并，日志等内部操作，预留20%
5. 安全阈值，通常至少预留15%的安全阈值
```

最小磁盘总大小 = **源数据 * 3.4**

```
磁盘总大小
= 源数据 * (1 + 副本数量) * (1 + 索引开销) / (1 - Linux预留空间)
    / (1 - ES开销) / (1 - 安全阈值)
= 源数据 * (1 + 副本数量) * 1.7
= 源数据 * 3.4
```

诊断项 | 索引shard合理性诊断

索引应该分配多少shard?

ES默认5个分片够用吗?

到底需不需副本呢?

单节点shard应该放多少?

每个节点应该放哪些shard?

资源消耗严重

读写性能下降

排序结果不理想

数据节点负载不一致

索引shard个数是否合理

单节点shard数是否过多

数据节点间负载是否偏差过大

```
GET _cat/shards
GET _cat/indices
GET _cat/nodes
```

shards装箱

诊断项 | segment不合理

Case:
负载很低，无大量的读写请求，但是出现BulkReject异常

频繁更新单条doc
segment碎片过多

```
GET _cat/nodes?h=n,*.percent,master,sm
GET _cat/segments?h=i,s,pr,size
```

```
public MergeSpecification findMerges(MergeTrigger mergeTrigger, SegmentInfos in
                                     IndexWriter writer) throws IOException {

    //这里主要拿到总bytes数，segments数
    minSegmentBytes = floorSize(minSegmentBytes);
    // Compute max allowed segs in the index
    long levelSize = minSegmentBytes;
    long bytesLeft = totIndexBytes;
    double allowedSegCount = 0;
    while(true) {
      final double segCountLevel = bytesLeft / (double) levelSize;
      if (segCountLevel < segsPerTier) {
        allowedSegCount += Math.ceil(segCountLevel);
        break;
      }
      allowedSegCount += segsPerTier;
      bytesLeft -= segsPerTier * levelSize;
      levelSize *= maxMergeAtOnce;
    }
    int allowedSegCountInt = (int) allowedSegCount;
    // ...
}
```

诊断项 | 集群meta合理性诊断

集群meta信息太多，短时间频繁更新，都会给集群带来极大的负担
可能造成GC频繁，负载突增，甚至阻塞相关索引的读写，影响性能

```
GET _cluster/state
GET .monitor*/_search?
filter_path=hits.hits.fields,hits.hits.sort
```

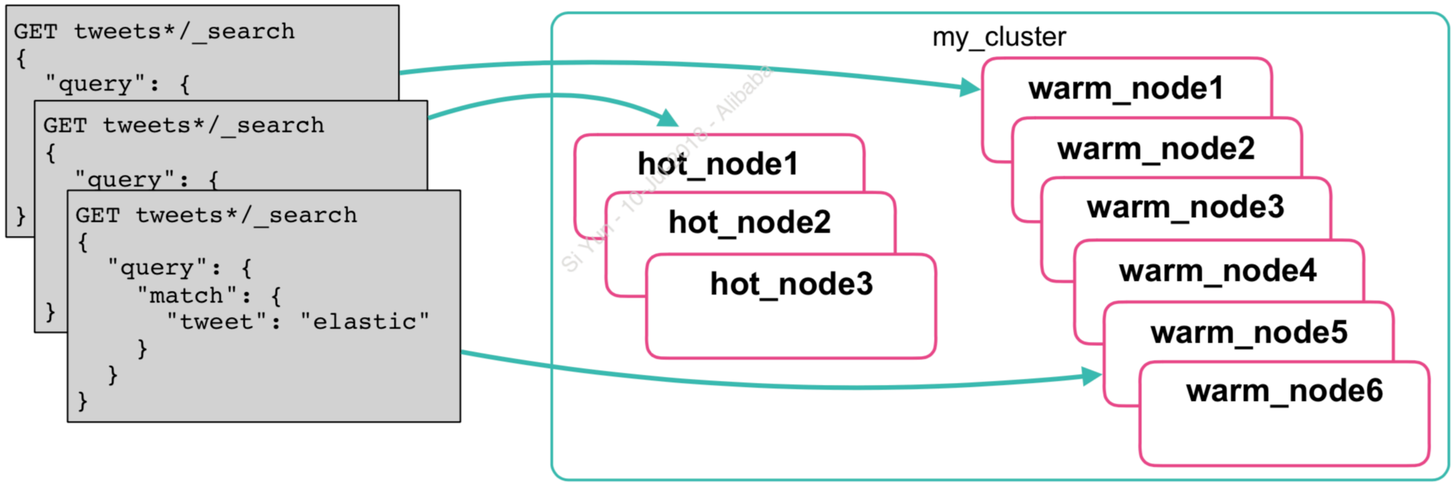
GET _cluster/state 结果如下


```
{
    "cluster_name": "es-cn-1[redacted]",
    "version": 329,
    "state_uuid": "HBwE531WRiem7ogiokGskA",
    "master_node": "1l0sVcAFTRCUNkDPJMVoGw",
    "blocks": {},
    "nodes": {
        "RgmxR4vXSEuK32Dtnn8dyw": {...},
        "YIvv3plRRJm4g0zYEuJcMQ": {...},
        "1l0sVcAFTRCUNkDPJMVoGw": {...}
    },
    "metadata": {...},
    "routing_table": {...},
    "routing_nodes": {...},
    "snapshot_deletions": {...},
    "snapshots": {...}
}
```

诊断项 | xpack类索引过多诊断

通用问题：冷/无效数据如何管理？

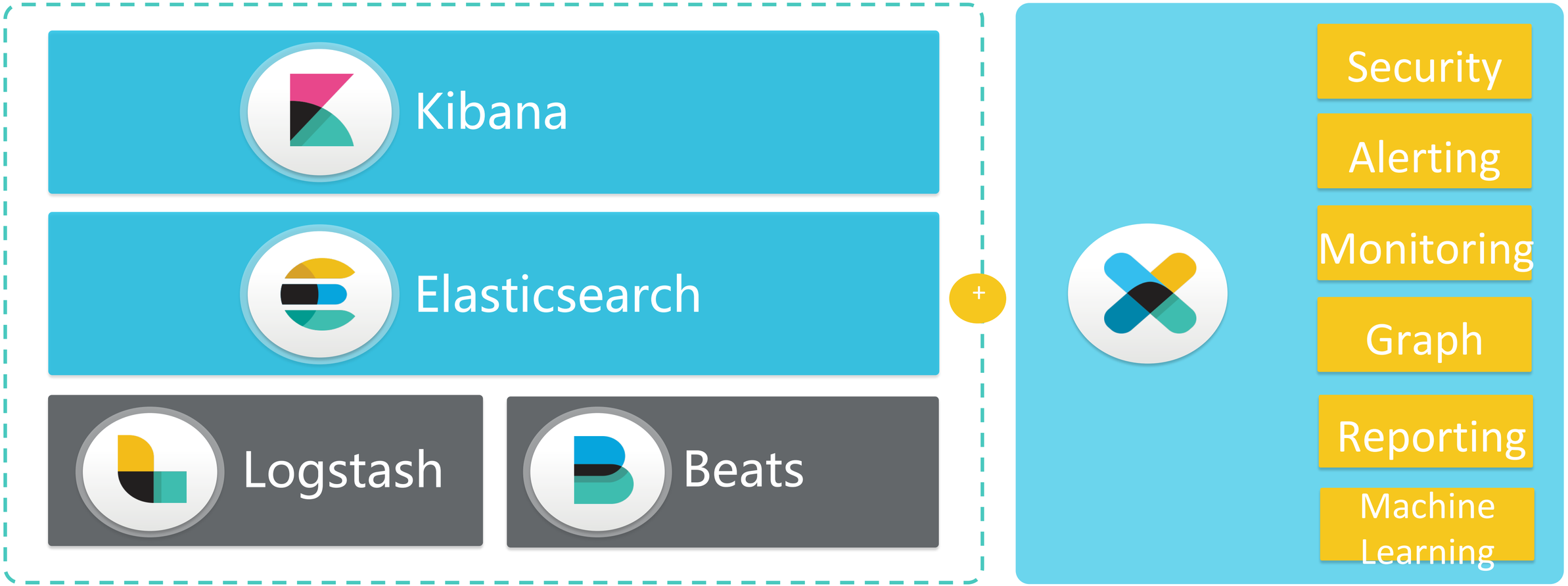
资 源 浪 费



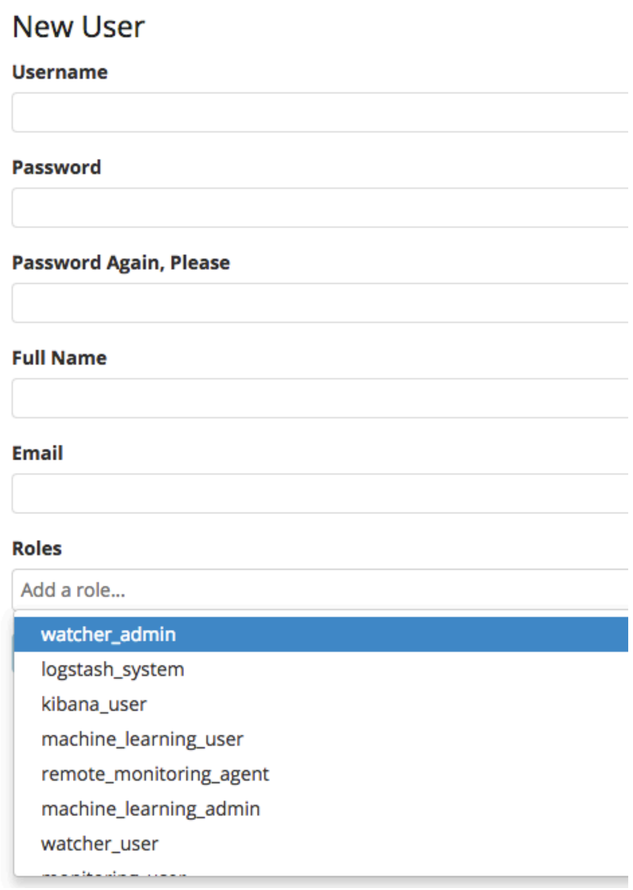
诊断项 | 日常使用规范诊断

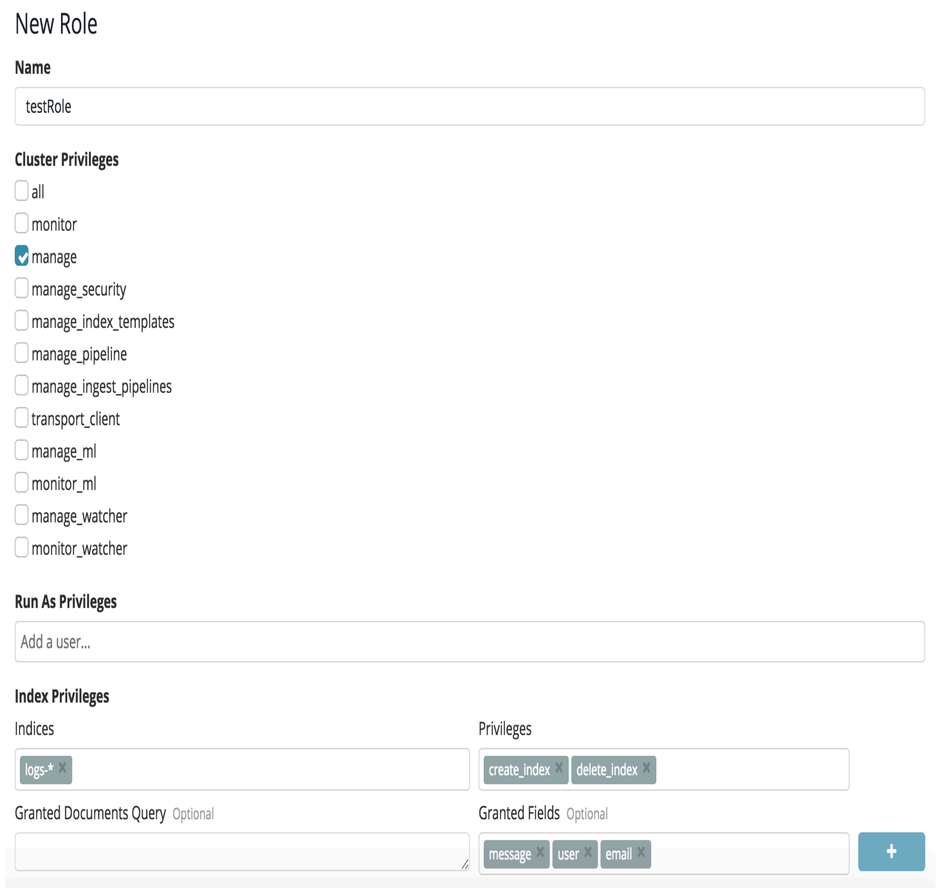
- 数据被删了还能不能恢复?
- Limit of total fields [1000], 不够用?
- 为啥这个数值字段会被映射成了text ?
- 重建索引了，还要改代码才能访问到新索引?
- 公网开启后，0.0.0.0/0 这个ip过滤规则很强大！
- ……

阿里云Elasticsearch



阿里云ES | X-Pack


New User
Username
Password
Password Again, Please
Full Name
Email
Roles
Add a role...
watcher_admin
logstash_system
kibana_user
machine_learning_user
remote_monitoring_agent
machine_learning_admin
watcher_user

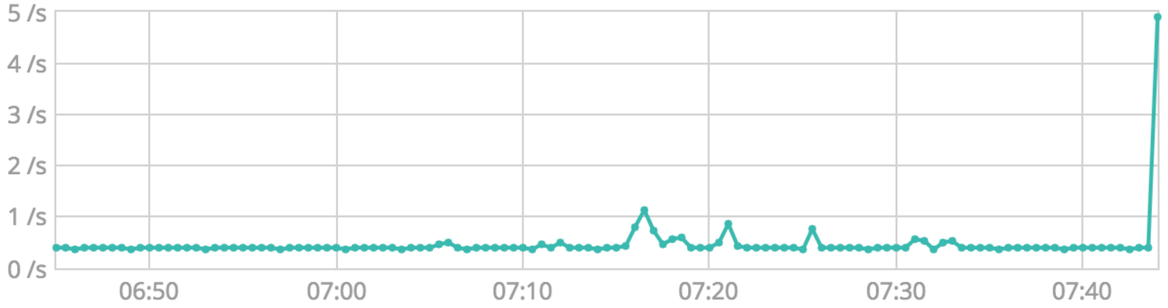

New Role
Name
testRole
Cluster Privileges
all
monitor
manage
manage_security
manage_index_templates
manage_pipeline
manage_ingest_pipelines
transport_client
manage_ml
monitor_ml
manage_watcher
monitor_watcher
Run As Privileges
Add a user...
Index Privileges
Indices
logs-*
Privileges
create_index
delete_index
Granted Documents Query Optional
Granted Fields Optional
message
user
email
+

阿里云ES | X-Pack

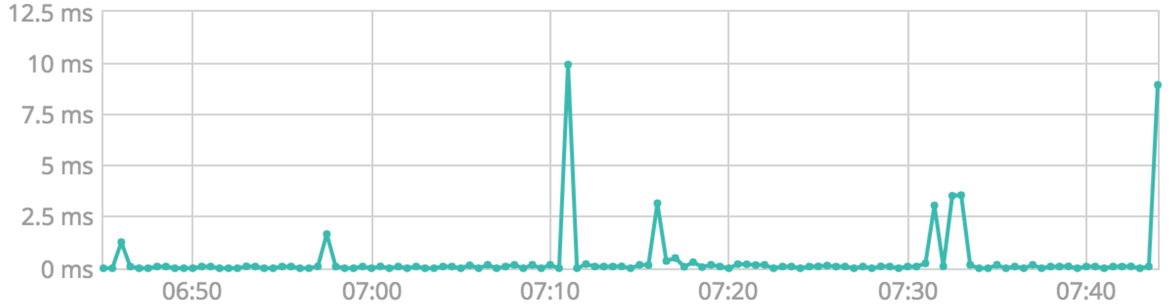
Alibaba Group 阿里巴巴集团

Nodes: **14** Indices: **12** Memory: **3GB / 9GB** Total Shards: **26** Unassigned Shards: **0** Documents: **1,024,472** Data: **2GB** Uptime: **5 days** Version: **5.5.3** Health: Green

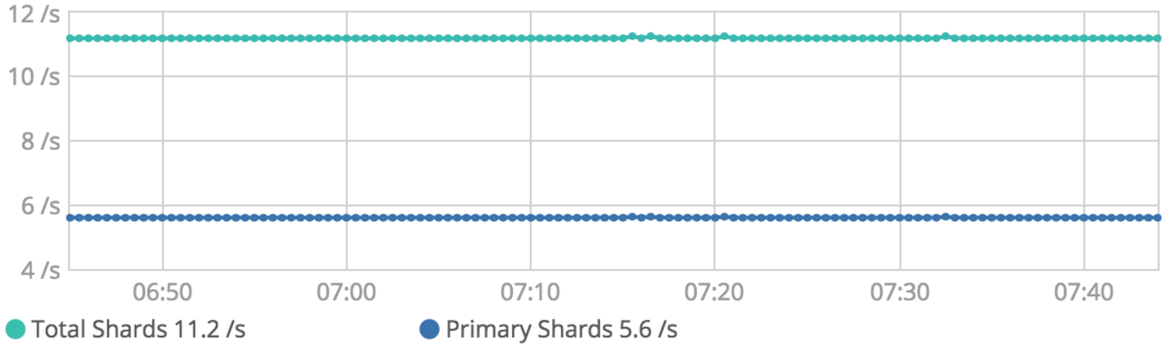
Search Rate (/s)



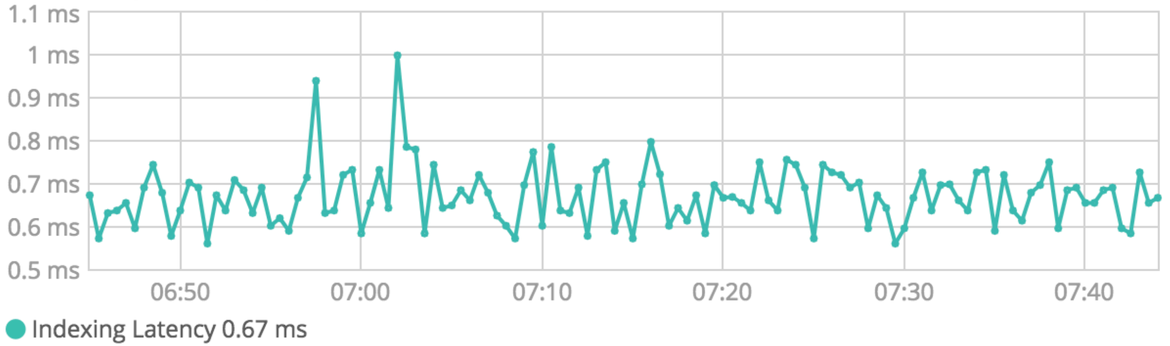
Search Latency (ms)



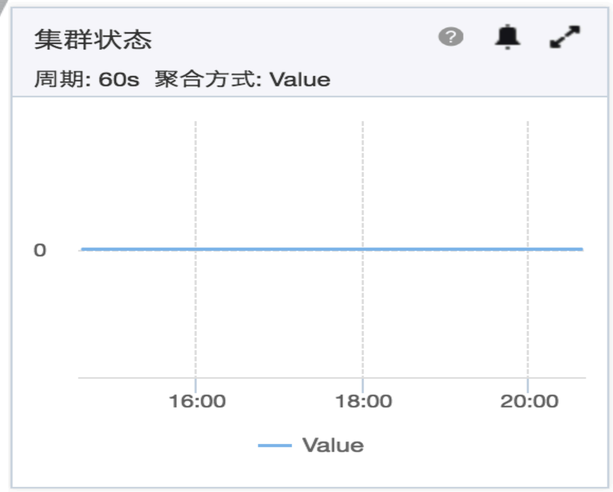
Indexing Rate (/s)

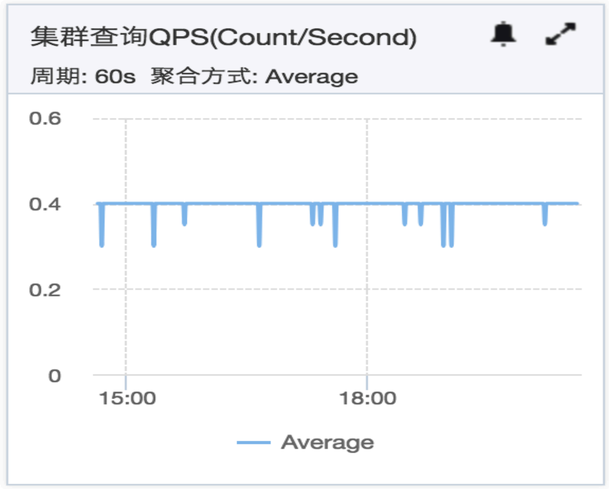


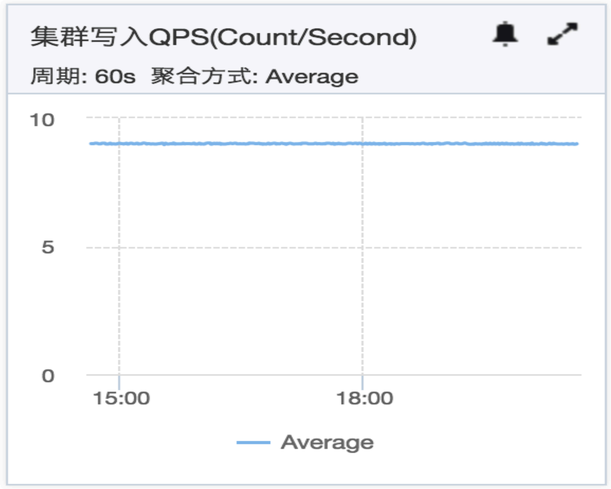
Indexing Latency (ms)

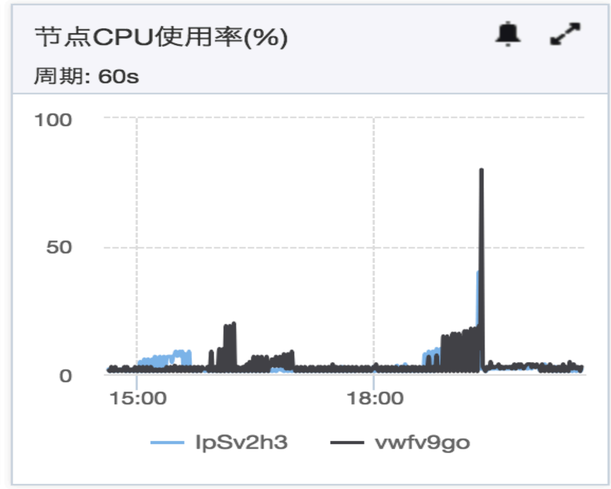


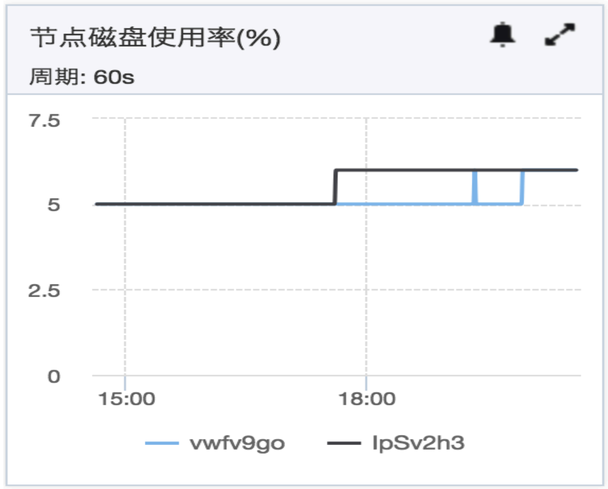
阿里云ES | 云监控

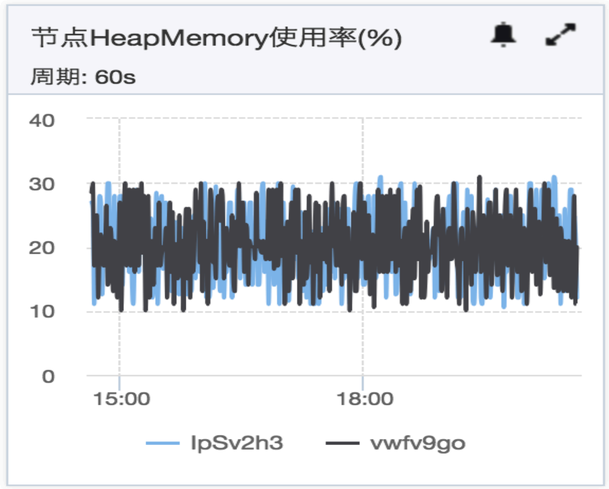


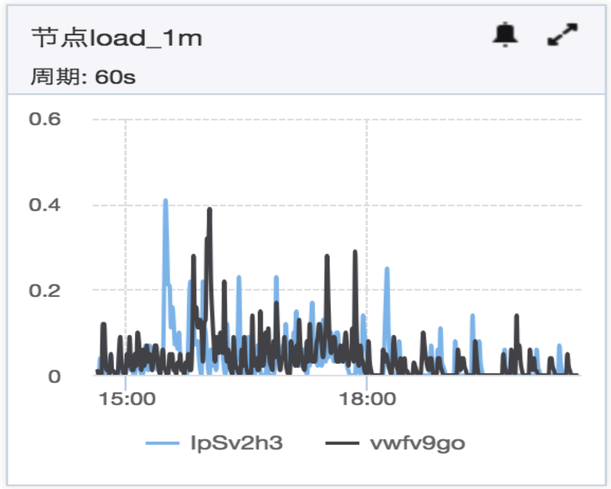












云监控

阿里云ES | ES日志可视化

Alibaba Group 阿里巴巴集团

[redacted]

kibana控制台 | 集群监控 | 重启实例 | 刷新

主日志 | searching慢日志 | indexing慢日志 | GC日志

Search... (e.g. status:200 AND extension:PHP)

2018-05-22 08:00:29 至 2018-05-23 08:00:29 搜索

时间	节点IP	内容
2018-05-23 08:00:05	[redacted]	level : info host : [redacted] time : 2018-05-23T08:00:05.007Z content : [o.e.c.r.a.AllocationService] [B9Mu1Qd] Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[.monitoring-es-6-2018.05.23][0]] ...]).
2018-05-23 00:30:00	[redacted]	level : info host : [redacted] time : 2018-05-23T00:30:00.002Z content : [o.e.x.m.a.DeleteExpiredDataAction$TransportAction] [B9Mu1Qd] Deleting expired data

阿里云ES | 弹性扩容

Alibaba Group 阿里巴巴集团

[redacted]

kibana控制台 | 集群监控 | 重启实例 | 刷新

转包年包月 | 节点扩容

基本信息

实例ID: [redacted]

名称: [redacted] 编辑

规格ID: elasticsearch.n4.small

Elasticsearch 版本: 5.5.3_with_X-Pack

付费类型: 后付费

内网地址: [redacted]

公网地址: 请开启公网访问地址后使用

区域: [redacted]

专有网络: [redacted]

创建时间: 2018-05-18 23:14:07

Dedicated master: 未开通

规格: CPU: 1核 内存: 2GB 存储: 20GB SSD

节点数: 2

状态: 正常

私网端口: [redacted]

公网端口: [redacted]

可用区: [redacted]

vswitch信息: [redacted]

EYou | 规划

- ✓ 引入更多的因子，对集群做到“千人千面”。
- ✓ 诊断项之间建立关系，从更高维去分析集群。
- ✓ 成为最了解集群的系统，给集群的调度，生命管理，运维等提供最佳策略。
- ✓ 挖掘集群日志，获取更多有效信息，结合具体的索引，推进集群的合理使用。
- ✓ 探索Machine Learning在EYou上的使用，优化诊断过程和结果。

Q&A

Alibaba Group 阿里巴巴集团

Elasticsearch技术...

682人

扫一扫群二维码，立刻加入该群。

elastic
中文社区

专业、垂直、纯粹的 Elastic 开源技术交流社区
https://elasticsearch.cn/