

# 基于阿里云Elasticsearch构建网站日志处理系统

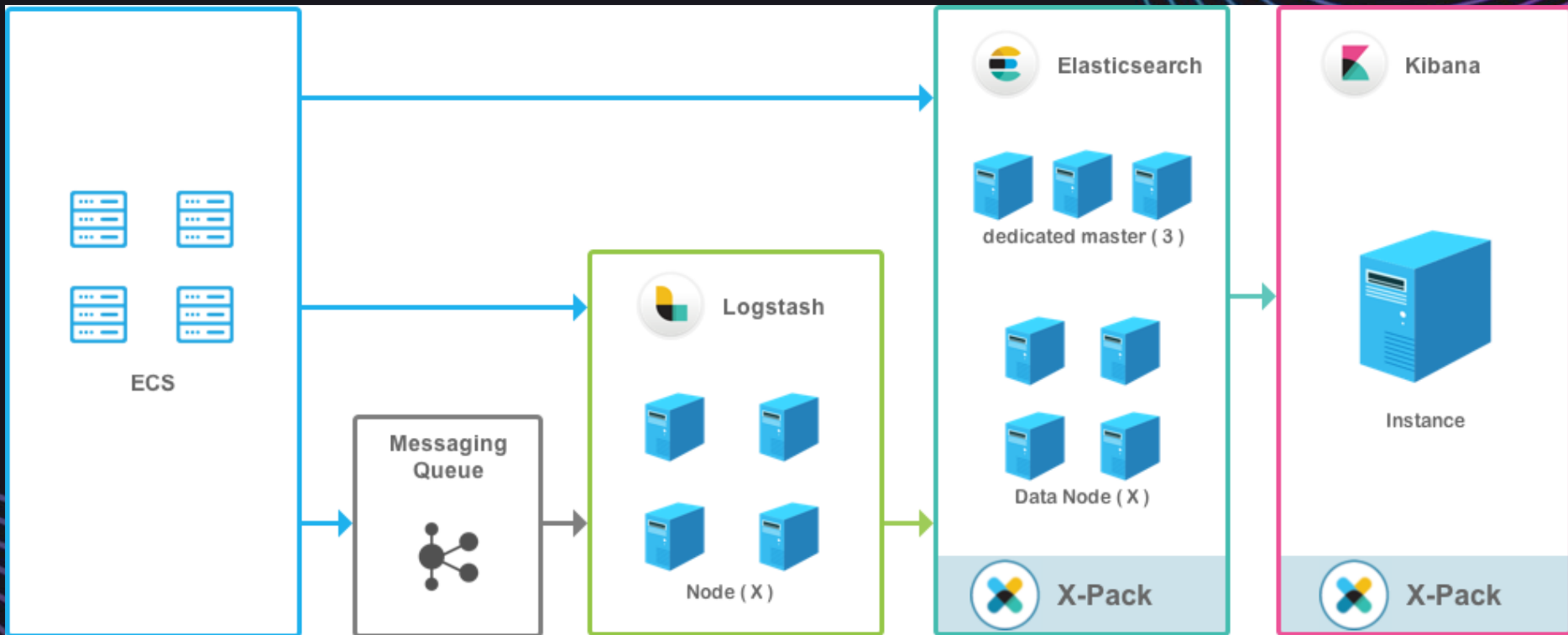
阿里云产品专家 赵弘扬

在线日志处理

离线日志处理

实时日志处理

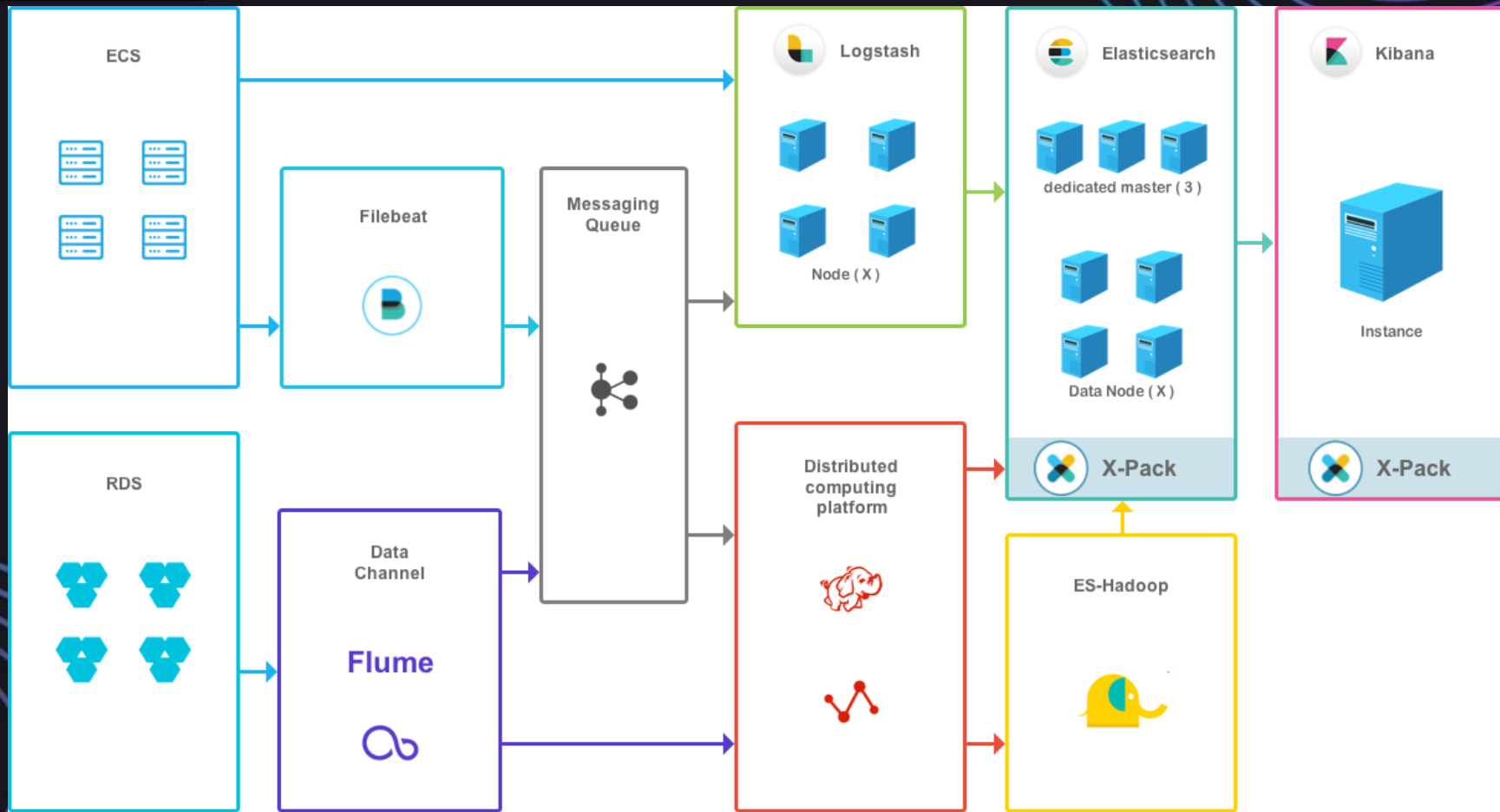
# 日志在线处理



# Logstash订阅日志文件

```
input {
  file {
    codec => json_lines{charset => ["UTF-8"]}
    path => "/root/server_metrics/*.json"
    start_position => beginning
  }
}
# 该部分被注释，表示filter是可选的
filter {
#   json {
#     source => "message"
#   }
}
output {
  elasticsearch {
    hosts => ["http://[redacted]:[redacted]@i.elasticsearch.aliyuncs.com:9200"]
    user => "elastic"
    password => "[redacted]"
    index => "serverlog"
  }
}
```

# 离线在线日志架构



# 周期性离线数据批量写入

MaxCompute

5min 一次全量写入

Elasticsearch

# 日志信息的Schema信息

```

"server-metrics":{
  "aliases":@Object{...},
  "mappings":{
    "metric":{
      "properties":{
        "@timestamp":{
          "type":"date"
        },
        "accept":{
          "type":"long"
        },
        "deny":{
          "type":"long"
        },
        "host":{
          "type":"keyword"
        },
        "response":{
          "type":"float"
        },
        "service":{
          "type":"keyword"
        },
        "total":{
          "type":"long"
        }
      }
    }
  }
},
"settings":{
  "index":{
    "creation_date":"1513612527792",
    "number_of_shards":"1",
    "number_of_replicas":"0",
    "uuid":"a58TKXThS7un IIzUQ64-A",
  }
}

```





- Discover
- Visualize
- Dashboard
- Timelion
- Machine Learning
- Graph
- Dev Tools
- Monitoring
- Management

- elastic
- Logout
- Collapse

Dev Tools

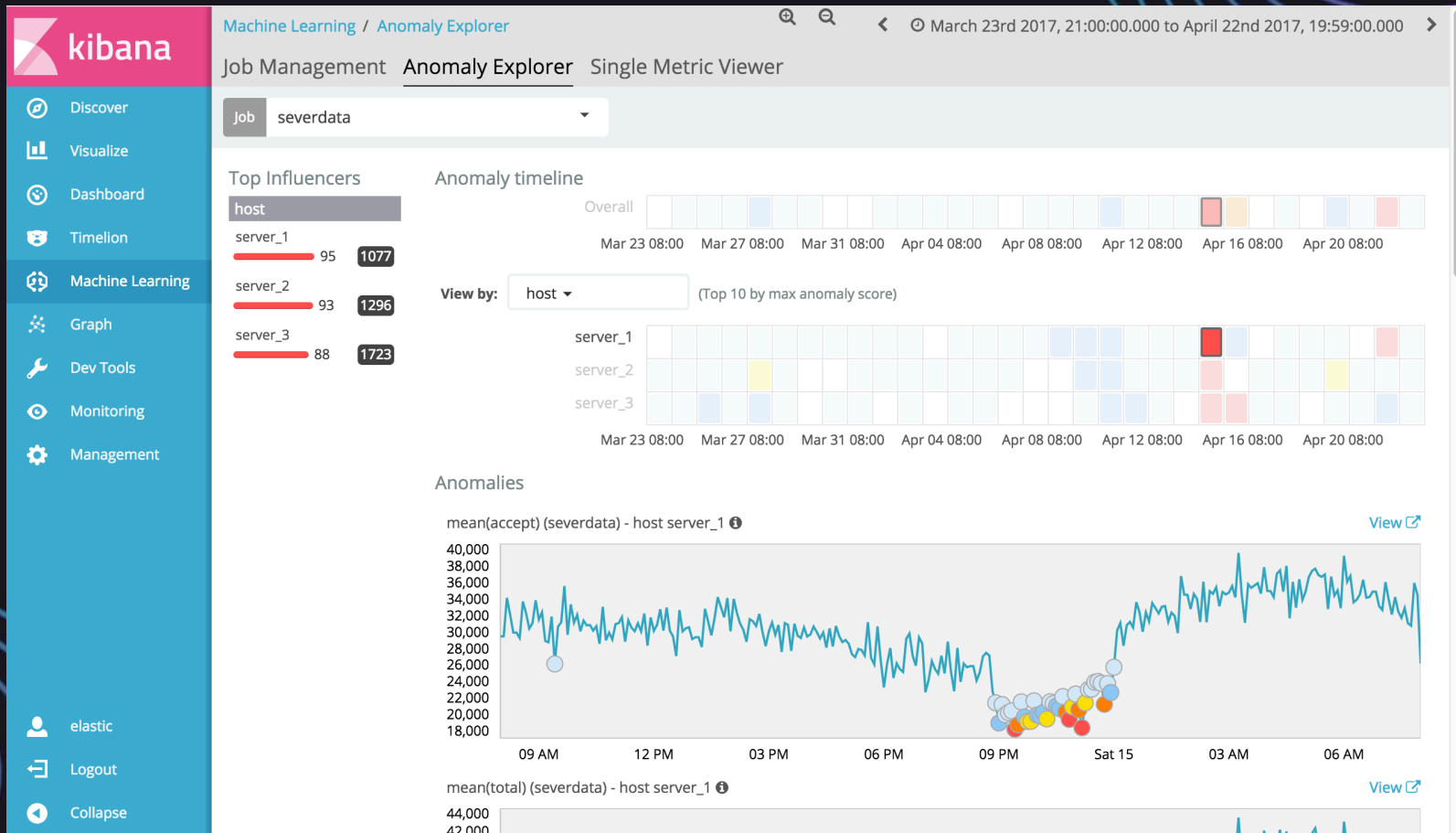
History Settings Help

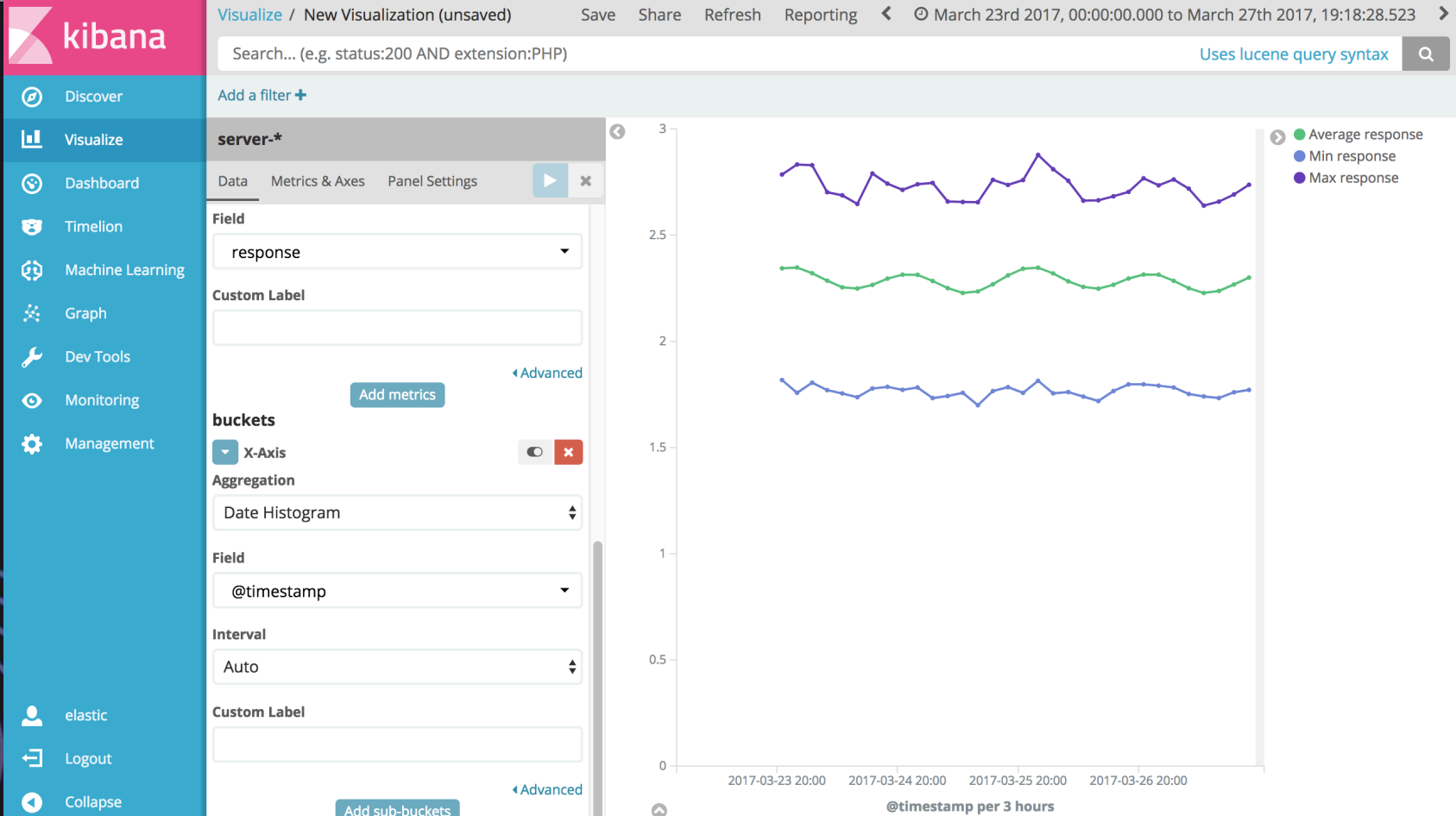
Console Search Profiler Grok Debugger

```
1 GET _cat/indices
2
3 GET server-metrics/_search?pretty
4 {
5   "query": { "match_all": {} },
6   "size": 1000
7 }
8
```

```
1 {
2   "took": 19,
3   "timed_out": false,
4   "_shards": {
5     "total": 1,
6     "successful": 1,
7     "failed": 0
8   },
9   "hits": {
10    "total": 905940,
11    "max_score": 1,
12    "hits": [
13      {
14        "_index": "server-metrics",
15        "_type": "metric",
16        "_id": "1177",
17        "_score": 1,
18        "_source": {
19          "@timestamp": "2017-03-23T13:00:00",
20          "accept": 36320,
21          "deny": 4156,
22          "host": "server_2",
23          "response": 2.4558210155,
24          "service": "app_3",
25          "total": 40476
26        }
27      },
28      {
29        "_index": "server-metrics",
30        "_type": "metric",
31        "_id": "1178",
32        "_score": 1,
33        "_source": {
34          "@timestamp": "2017-03-23T13:00:00",
35
```







日志  
处理  
常见问题

- 集中收集与存储
- 日志搜索
- 分析聚合及可视化
- 安全，角色管理
- 可伸缩性

Filebeat

Logstash

其他...

参数	SSD云盘	高效云盘	普通云盘
单盘最大容量	32768 GB	32768 GB	2000 GB
最大IOPS	20000 <sup>*</sup>	3000	数百
最大吞吐量	300 MBps <sup>*</sup>	80 MBps	30-40 MBps
单盘性能计算公式 <sup>**</sup>	$IOPS = \min\{1200 + 30 * \text{容量}, 20000\}$	$IOPS = \min\{1000 + 6 * \text{容量}, 3000\}$	无
	$\text{吞吐量} = \min\{80 + 0.5 * \text{容量}, 300\} \text{ MBps}$	$\text{吞吐量} = \min\{50 + 0.1 * \text{容量}, 80\} \text{ MBps}$	无
访问时延	0.5-2 ms	1-3 ms	5-10 ms
数据可靠性	99.9999999%	99.9999999%	99.9999999%



- Discover
- Visualize
- Dashboard
- Timeline
- Machine Learning
- Graph
- Dev Tools
- Monitoring
- Management

- elastic
- Logout
- Collapse

Dev Tools

History Settings Help

Console Search Profiler Grok Debugger

```
1 GET _cat/indices
2
3 GET server-metrics
4
5 GET server-metrics/_search?pretty
6 {
7   "query": { "match_all": {}},
8   "size": 1000
9 }
10
11 GET /server-metrics/_search?q=host:server_2
12
```

```
1 {
2   "took": 11,
3   "timed_out": false,
4   "_shards": {
5     "total": 1,
6     "successful": 1,
7     "failed": 0
8   },
9   "hits": {
10    "total": 301980,
11    "max_score": 1.0986117,
12    "hits": [
13      {
14        "_index": "server-metrics",
15        "_type": "metric",
16        "_id": "1177",
17        "_score": 1.0986117,
18        "_source": {
19          "@timestamp": "2017-03-23T13:00:00",
20          "accept": 36320,
21          "deny": 4156,
22          "host": "server_2",
23          "response": 2.4558210155,
24          "service": "app_3",
25          "total": 40476
26        }
27      },
28      {
29        "_index": "server-metrics",
30        "_type": "metric",
31        "_id": "1180",
32        "_score": 1.0986117,
33        "_source": {
34          "@timestamp": "2017-03-23T13:00:00"
```

The screenshot displays the Kibana Dev Tools interface. The left sidebar contains navigation links: Discover, Visualize, Dashboard, Timelion, Machine Learning, Graph, Dev Tools (selected), Monitoring, and Management. At the bottom of the sidebar are links for elastic, Logout, and Collapse. The top of the Dev Tools panel has tabs for Console, Search Profiler, and Grok Debugger. The Console tab is active, showing a series of commands and their outputs.

**Commands:**

```
1 GET _cat/indices
2
3 GET server-metrics
4
5 GET server-metrics/_search?pretty
6 {
7   "query": { "match_all": {} },
8   "size": 1000
9 }
10
11 GET /server-metrics/_search?q=host:server_2
12
13
14 GET /server-metrics/_search
15 {
16   "aggs" : {
17     "_source" : {
18       "terms" : { "field" : "host" },
19       "aggs" : {
20         "avg_response" : {
21           "avg" : { "field": "response"
22         }
23       }
24     }
25   }
26 }
27
```

**Results:**

```
162 }
163 ]
164 },
165 "aggregations": {
166   "_source": {
167     "doc_count_error_upper_bound": 0,
168     "sum_other_doc_count": 0,
169     "buckets": [
170       {
171         "key": "server_1",
172         "doc_count": 301980,
173         "avg_response": {
174           "value": 2.2857875645472534
175       }
176     },
177     {
178       "key": "server_2",
179       "doc_count": 301980,
180       "avg_response": {
181         "value": 2.286165460663305
182     }
183   },
184   {
185     "key": "server_3",
186     "doc_count": 301980,
187     "avg_response": {
188       "value": 2.2859840998737075
189   }
190 }
191 ]
192 }
193 }
194 }
```

```
1 {
2   "Version": "1",
3   "Statement": [
4     {
5       "Action": [
6         "elasticsearch:Describe*"
7       ],
8       "Resource": "acs:elasticsearch:cn-hangzhou:1818503459563647:instances/es-cn-mp90fk3lk000192vw",
9       "Effect": "Allow"
10    },
11    {
12      "Action": [
13        "elasticsearch:List*"
14      ],
15      "Resource": "acs:elasticsearch:cn-hangzhou:1818503459563647:instances/*",
16      "Effect": "Allow"
17    }
18  ]
19 }
```

创建授权策略

STEP 1: 选择权限策略模板 STEP 2: 编辑权限并提交 STEP 3: 新建成功

\* 授权策略名称:

长度为1-128个字符，允许英文字母、数字，或“-”

备注:

策略内容:

```
9      "Resource": "acs:elasticsearch:cn-
10      hangzhou:1818503459563647:instances/es-cn-
11      mp90fk3lk000192vw",
12      "Effect": "Allow"
13    },
14    {
15      "Action": [
16        "elasticsearch:List*"
17      ],
18      "Resource": "acs:elasticsearch:cn-
19      hangzhou:1818503459563647:instances/*",
20      "Effect": "Allow"
21    }
22  ]
```

[授权策略格式定义](#)

上一步 新建授权策略 取消





- Discover
- Visualize
- Dashboard
- Timelion
- Machine Learning
- Graph
- Dev Tools
- Monitoring
- Management

- elastic
- Logout
- Collapse

## 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

hongyang

## Index Privileges

## Indices

server-\*

## Privileges

read

## Granted Documents Query Optional

## Granted Fields Optional

response host @timestamp service

Save

Cancel

字段级别权限控制

# 可伸缩性

管控组件shuttle:

- FSM设计
- 基于集群健康状态
- 多种资源分配
- 优化：双集群平滑升级



The background features a dark blue field with a faint, pixelated world map. The map is composed of small, light blue squares that form the outlines of continents. In the four corners of the image, there are decorative wavy lines in a light blue and purple hue, creating a modern, digital aesthetic.

**Thanks!**