阿里云 MVP

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

阿里云 MVP

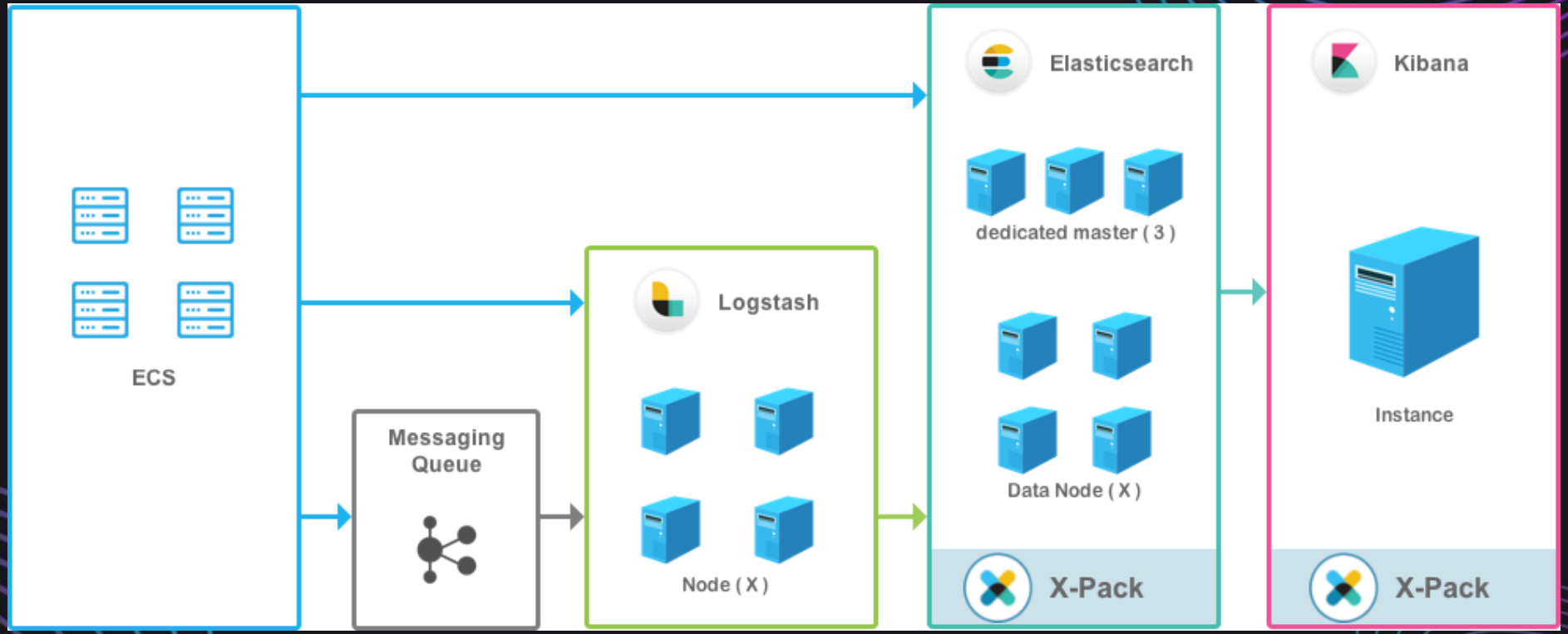
在线日志处理

离线日志处理

实时日志处理

阿里云 MVP

日志在线处理



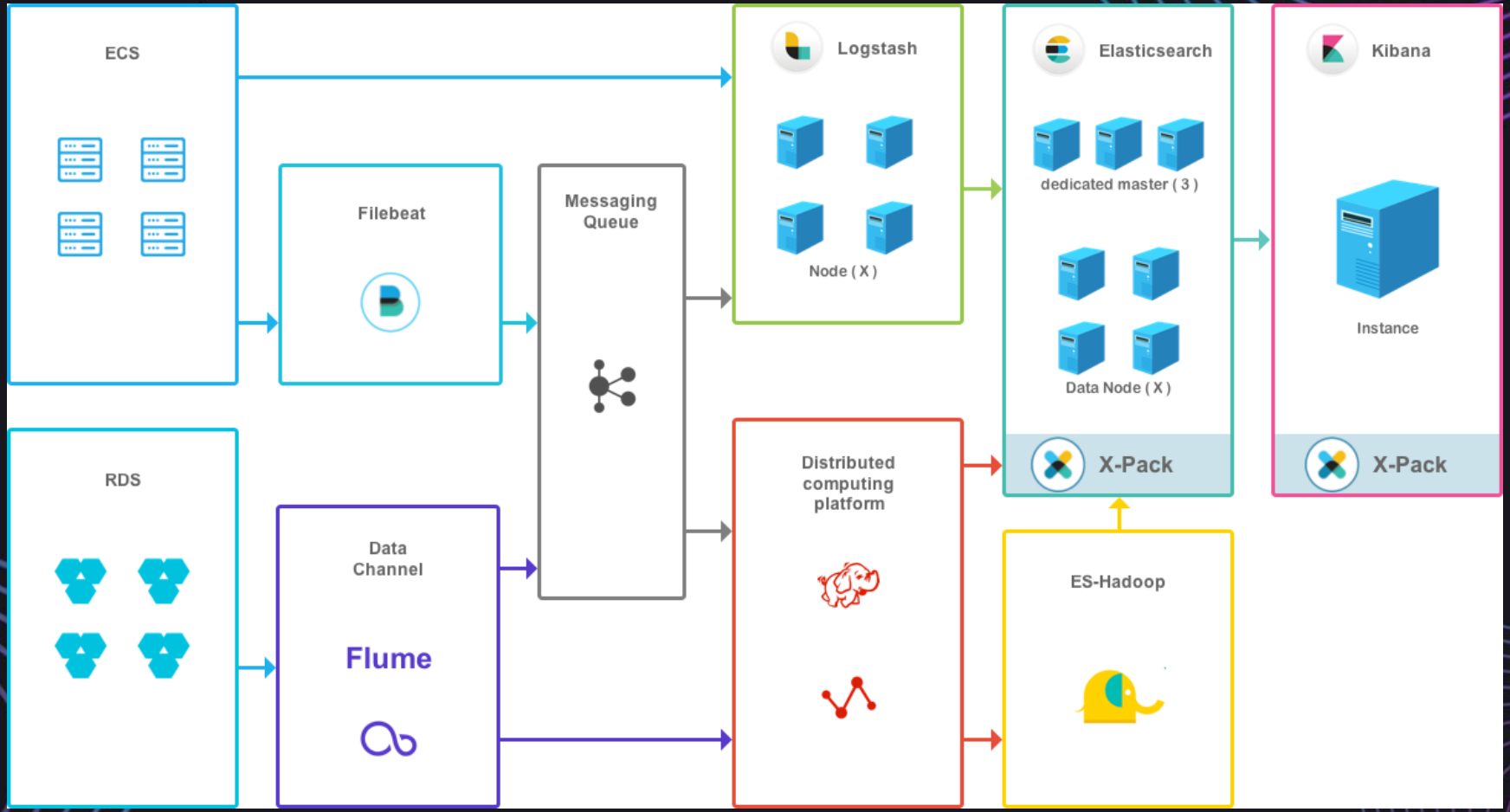
阿里云 MVP

Logstash订阅日志文件

```
nput {
    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]i.elasticsearch.aliyuncs.com:9200"]
        user => "elastic"
        password => "[redacted]"
        index => "serverlog"
    }
}
```

阿里云 MVP

离线在线日志架构



阿里云 MVP

周期性离线数据批量写入

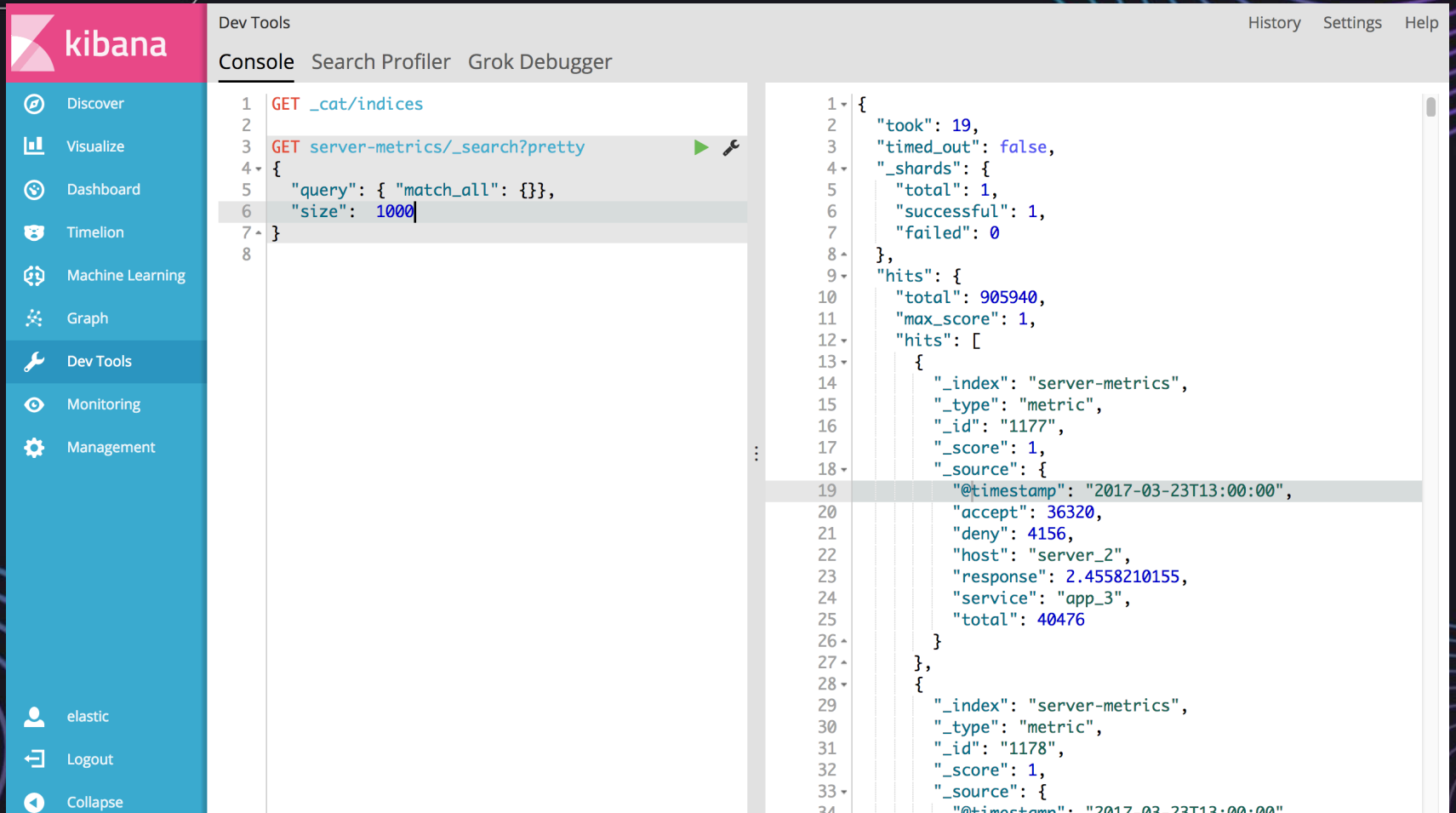
阿里云 MVP

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",
```

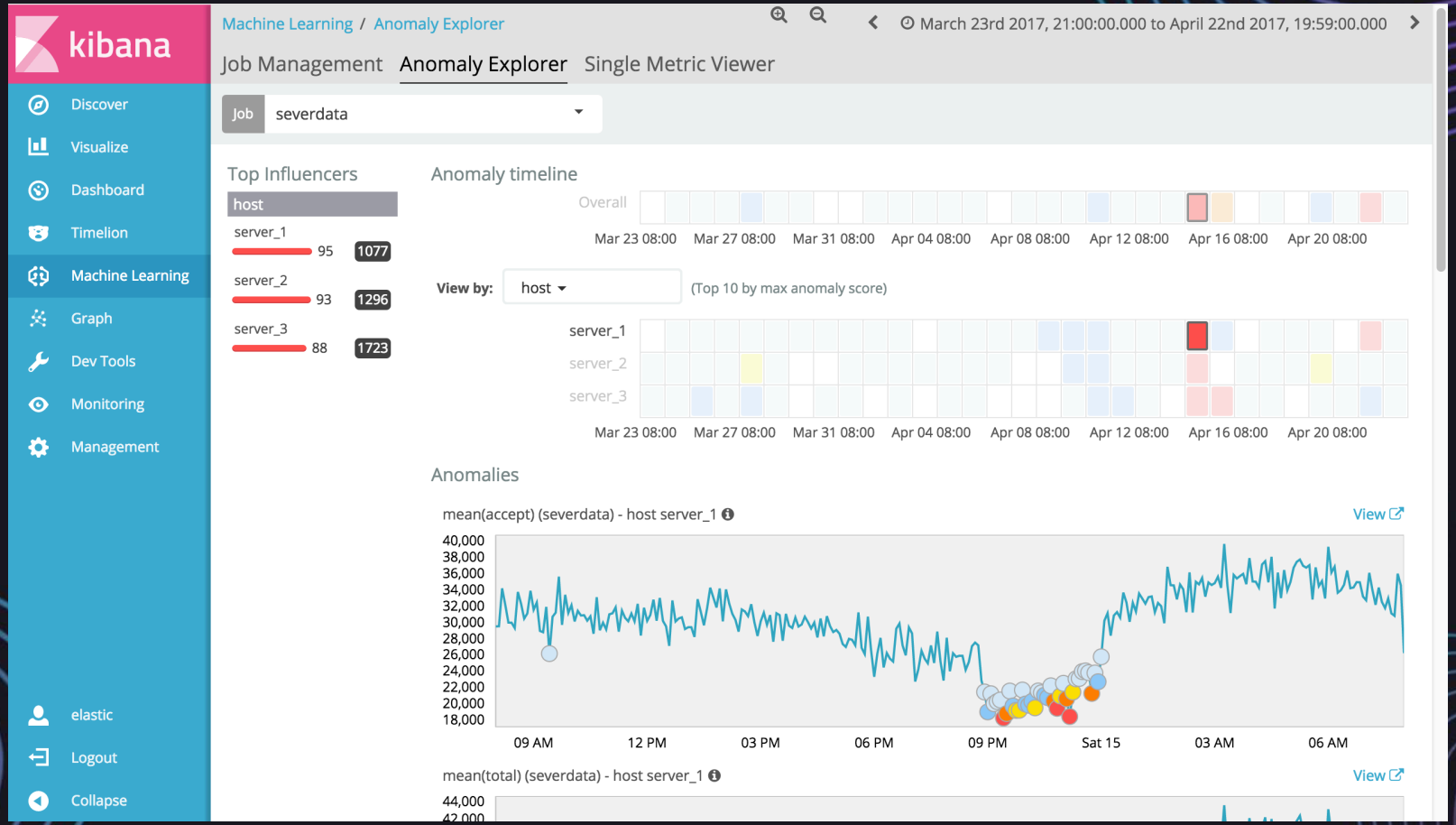
阿里云 MVP

通过Kibana查看日志



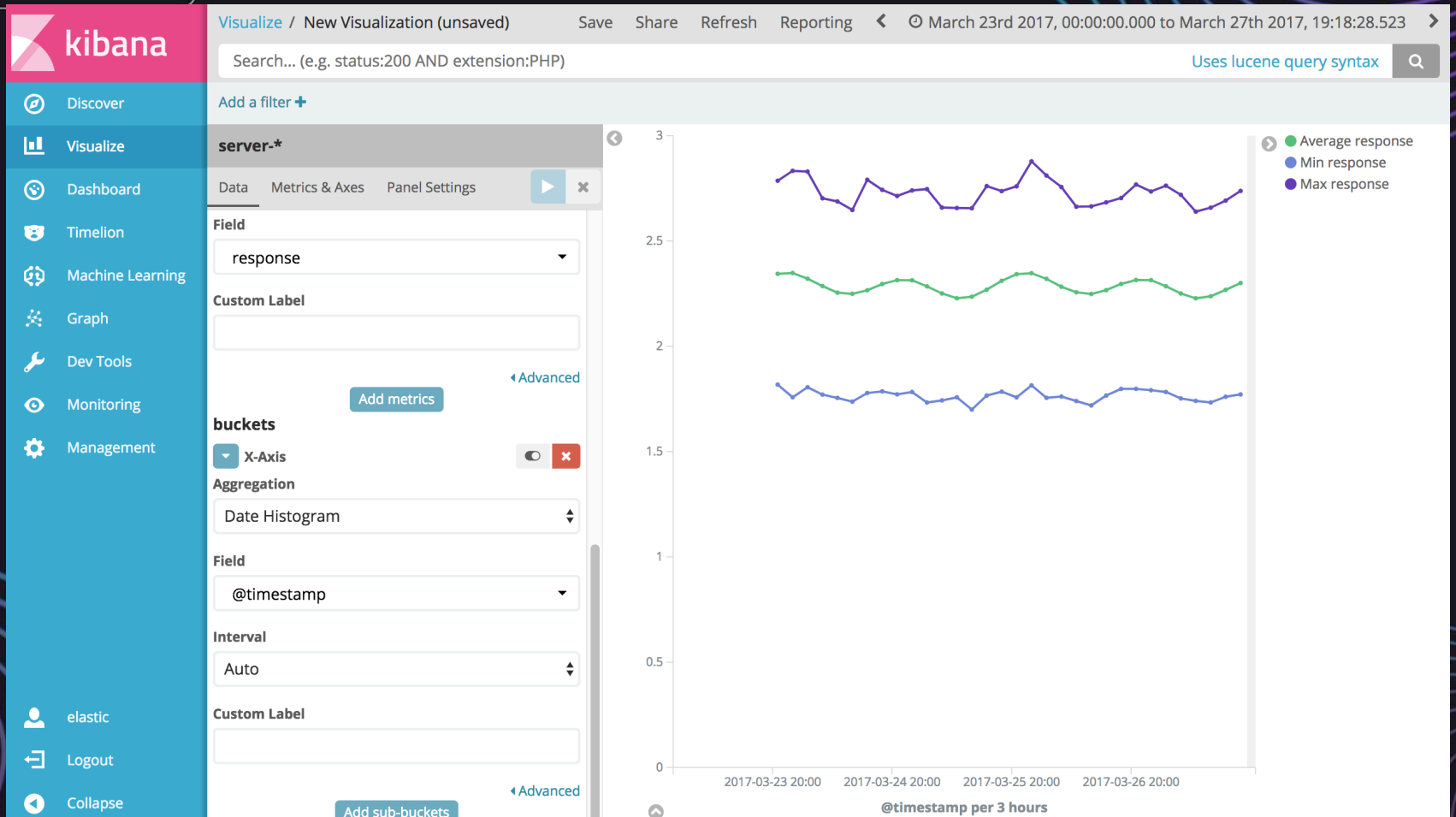
阿里云 MVP

通过Machine Learning模块分析



阿里云 MVP

可视化统计结果



阿里云 MVP

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

阿里云 MVP

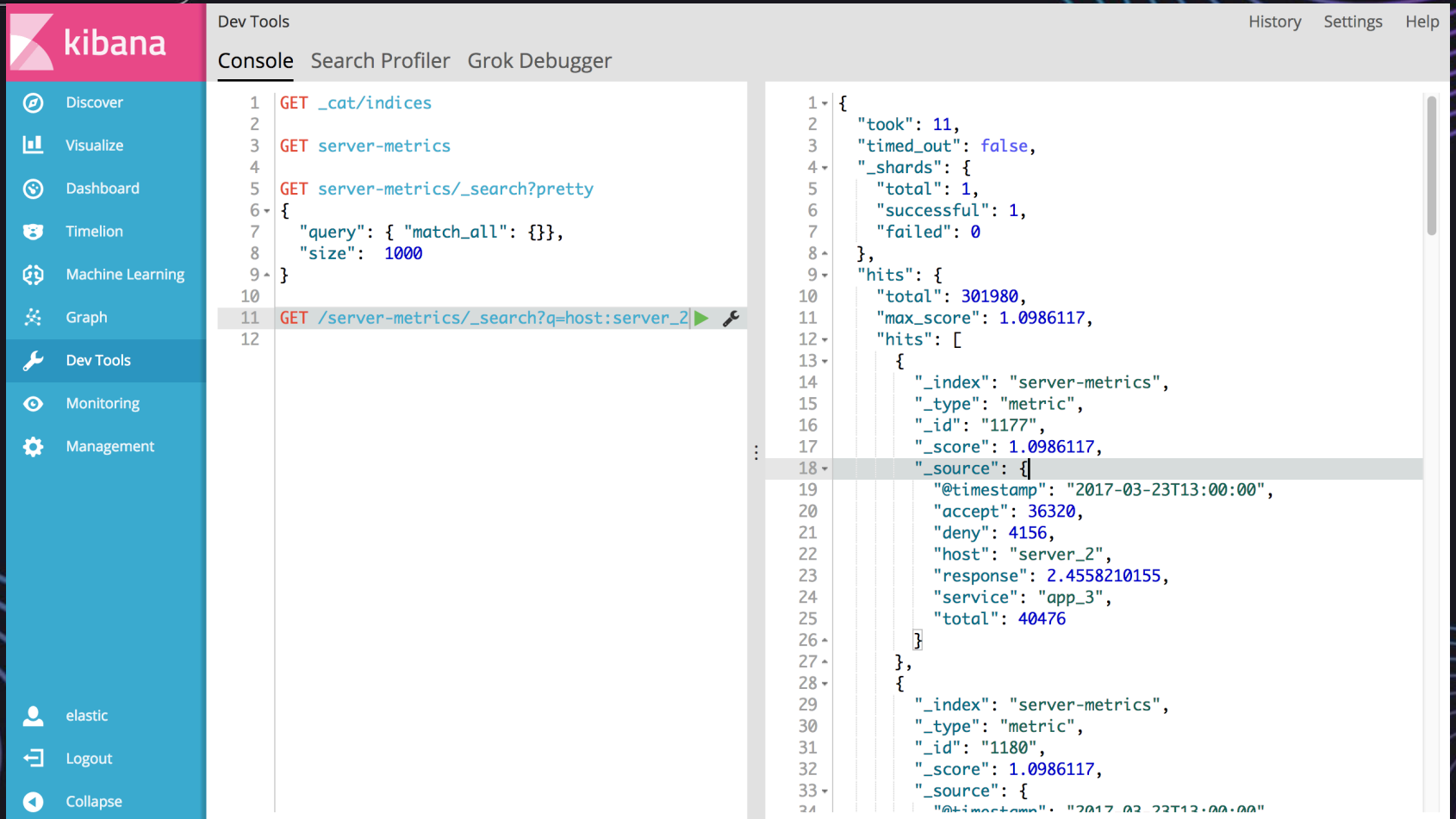
集中与存储

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*	3000	数百
最大吞吐量	300 MBps*	80 MBps	30–40 MBps
单盘性能计算公式**	IOPS = min{1200 + 30 * 容量, 20000}	IOPS = min{1000 + 6 * 容量, 3000}	无
	吞吐量 = min{80 + 0.5 * 容量, 300} MBps	吞吐量 = min{50 + 0.1 * 容量, 80} 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%

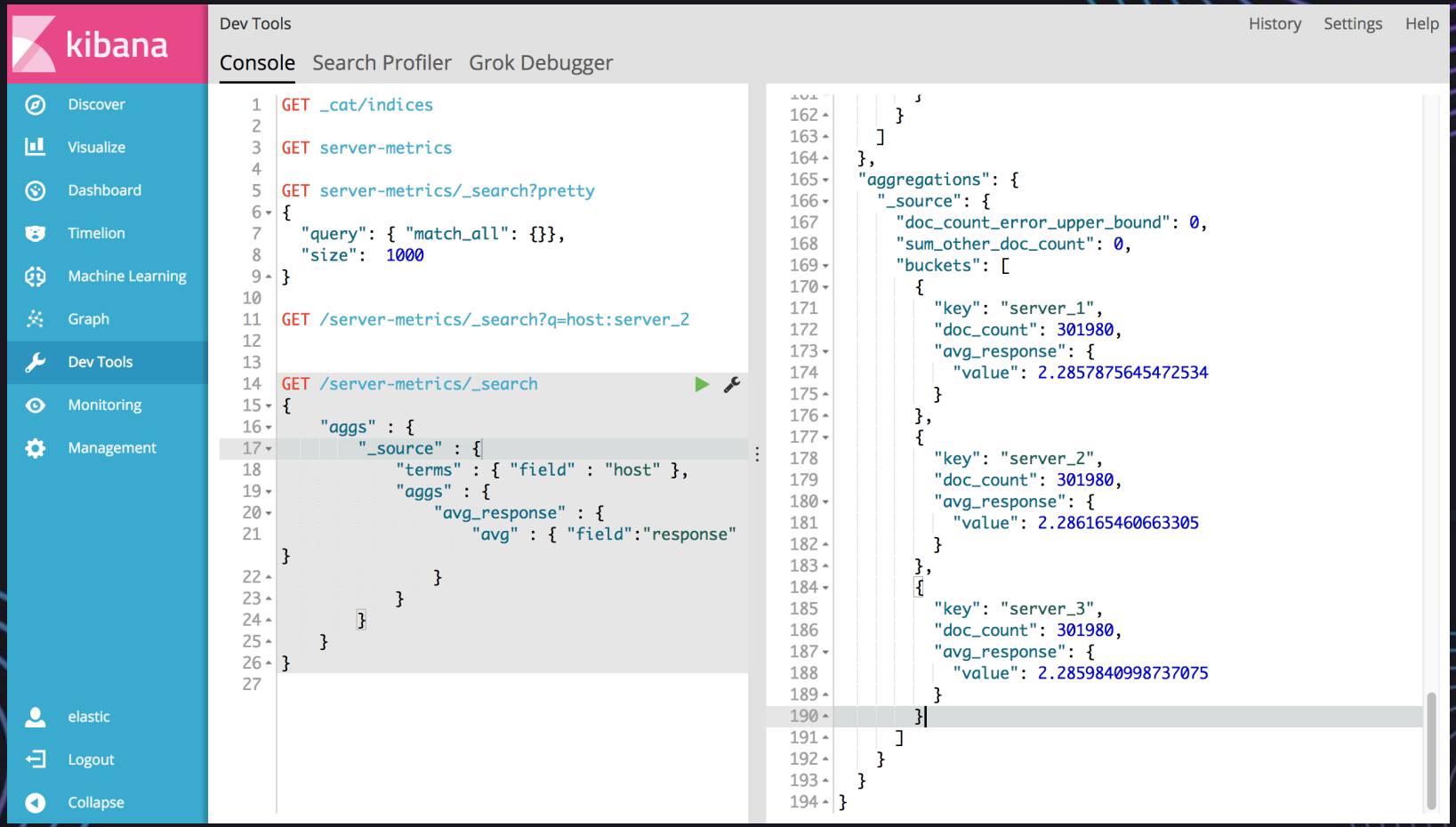
阿里云 MVP

日志搜索


kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management
elastic
Logout
Collapse
Dev Tools
History
Settings
Help
Console
Search Profiler
Grok Debugger
GET _cat/indices
GET server-metrics
GET server-metrics/_search?pretty
{
"query": { "match_all": {}},
"size": 1000
}
GET /server-metrics/_search?q=host:server_2
{
"took": 11,
"timed_out": false,
"_shards": {
"total": 1,
"successful": 1,
"failed": 0
},
"hits": {
"total": 301980,
"max_score": 1.0986117,
"hits": [
{
"_index": "server-metrics",
"_type": "metric",
"_id": "1177",
"_score": 1.0986117,
"_source": {
"@timestamp": "2017-03-23T13:00:00",
"accept": 36320,
"deny": 4156,
"host": "server_2",
"response": 2.4558210155,
"service": "app_3",
"total": 40476
}
},
{
"_index": "server-metrics",
"_type": "metric",
"_id": "1180",
"_score": 1.0986117,
"_source": {

阿里云 MVP

分析聚合可视化



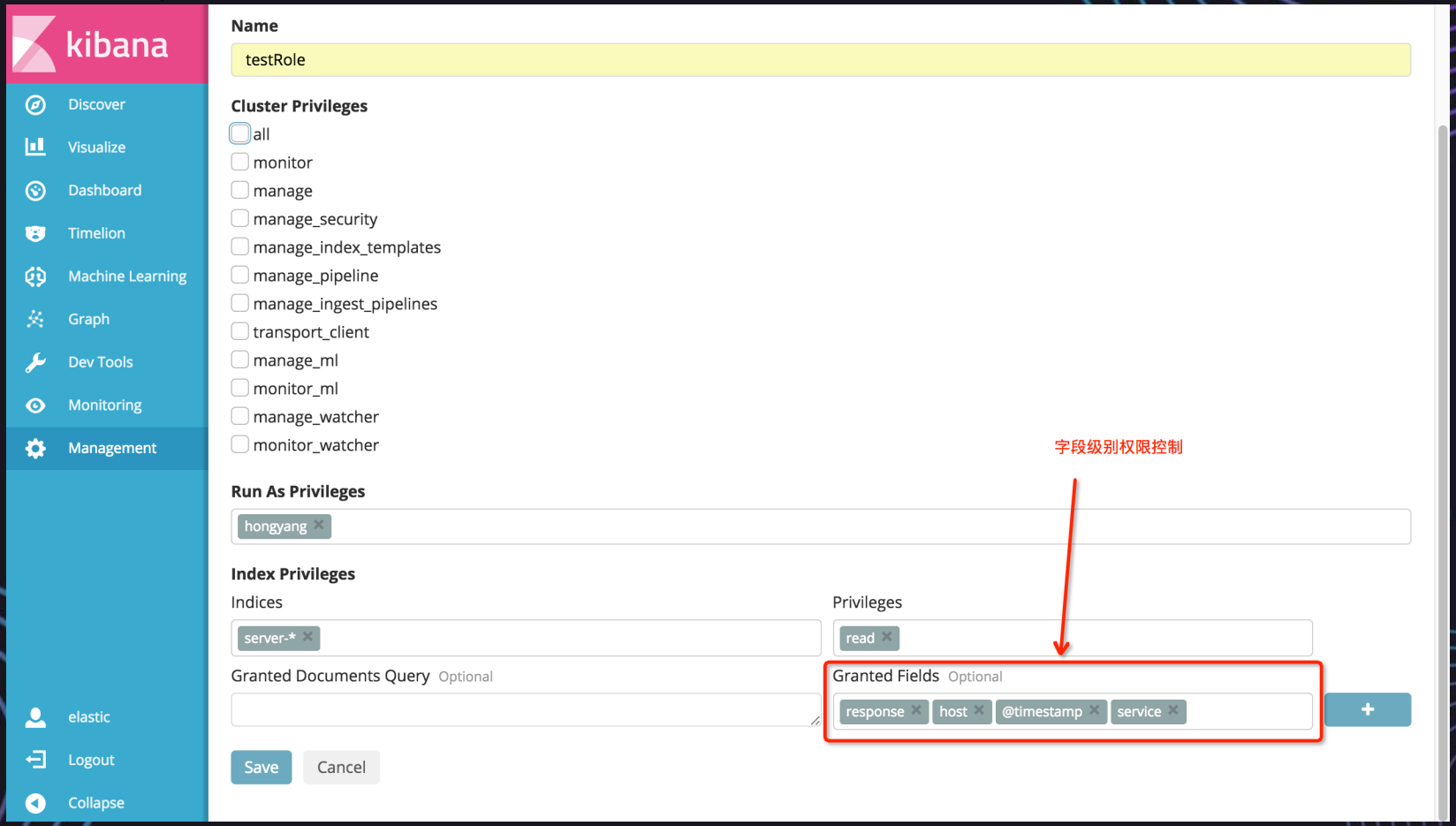
阿里云 MVP

安全角色管理

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "elasticsearch:Describe*"
      ],
      "Resource": "acs:elasticsearch:cn-hangzho
mp90fk3lk000192vw",
      "Effect": "Allow"
    },
    {
      "Action": [
        "elasticsearch:List*"
      ],
      "Resource": "acs:elasticsearch:cn-hangzhou:1818503459563647:instances/*",
      "Effect": "Allow"
    }
  ]
}
```

阿里云 MVP

安全角色管理

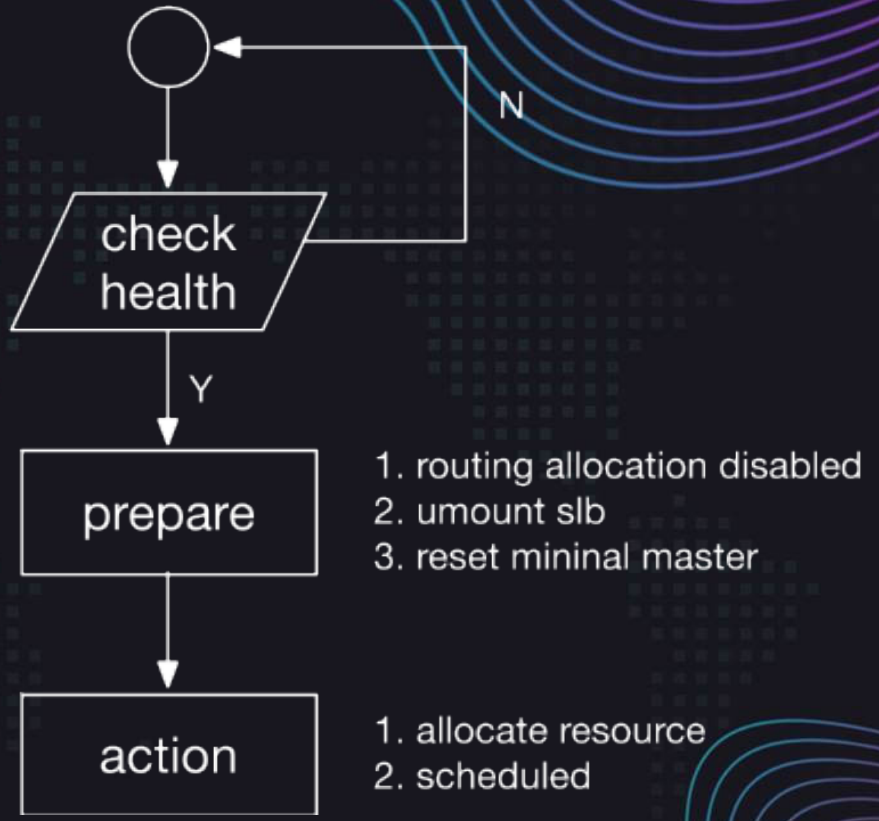


阿里云 MVP

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



Thanks!