

# ELK CI/CD 部署实践

黄鑫 ( @dreampuf )

# Agenda

使用 SaltStack 对 ELK 维护、配置管理、持续集成和持续部署的设计与实施。

- 背景介绍
- 可用性设计
- 配置管理和持续集成
- 持续部署
- 发现的问题和未来展望

# 背景介绍

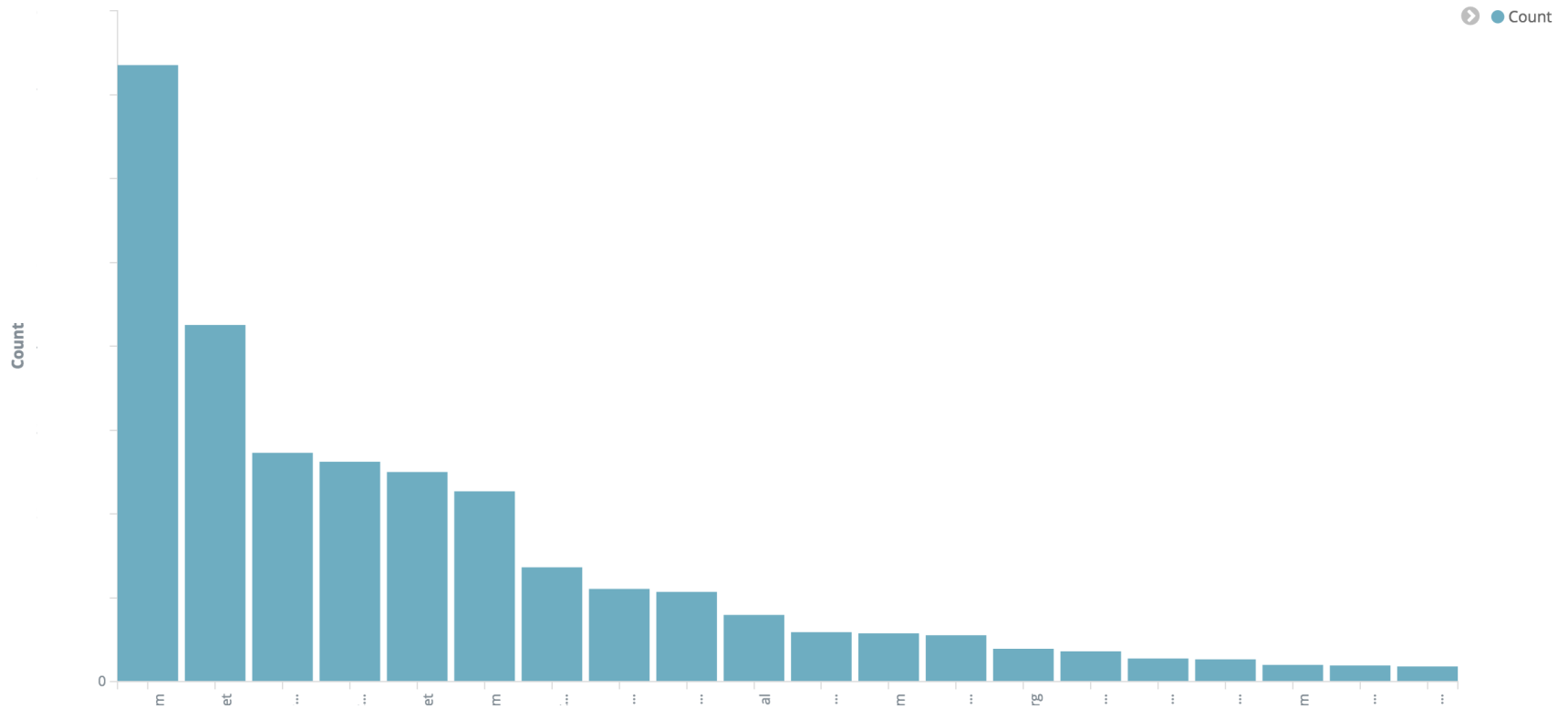
- 应用场景
- 多部门协作
- 日志收集为主 (Filebeat)
- 历史演进 (1.75 -> 5.3.2)
- 使用 SaltStack 进行状态管理 (安装, 更新, 维护)

# 应用场景

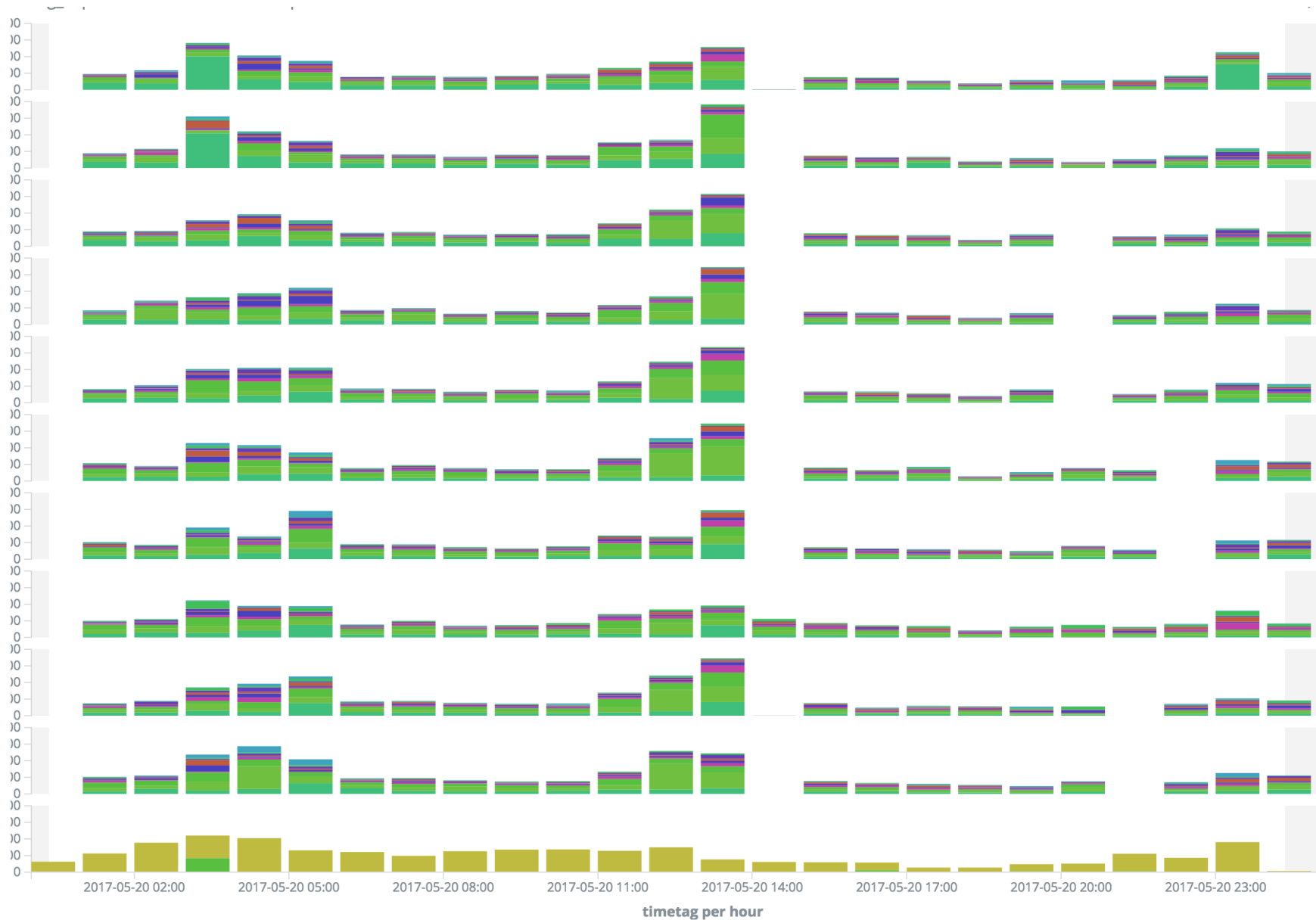
- 广告投放记录
- 访问日志
- 离线计算任务追踪
- 内部服务监控

# 广告投放记录

Most Visited 20 Host of Access Log



# 离线计算任务追踪



# 多部门协作

- 前端、后端.....
- 部门之间相对隔离
- 数据存储统一，方便级联查询

# 数据源

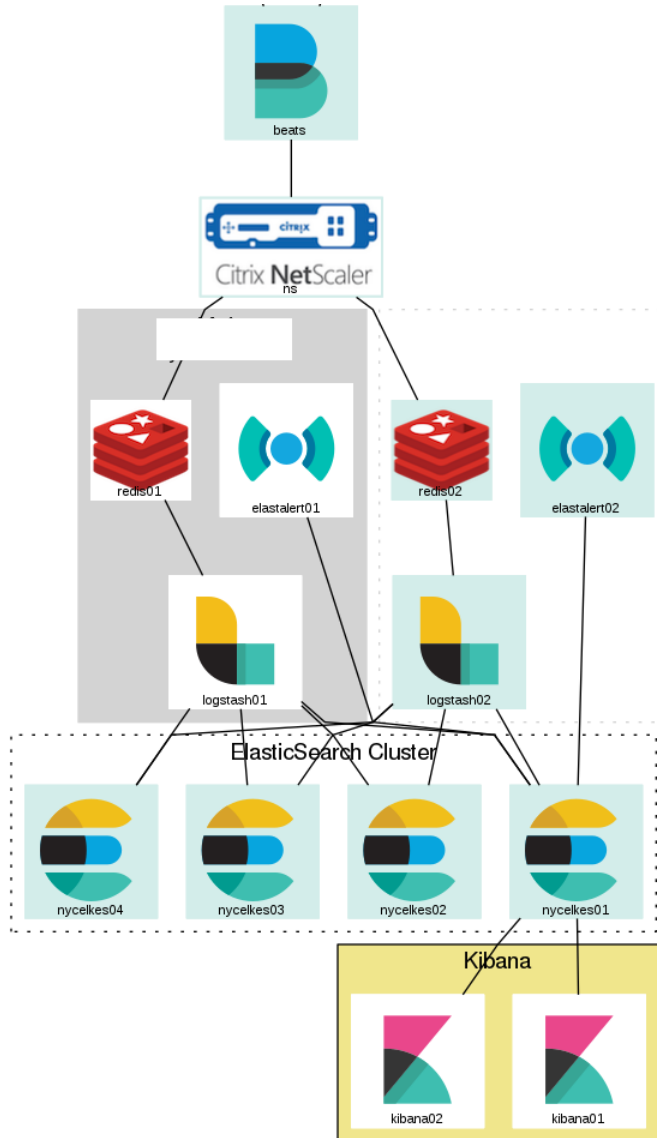
- 文件日志格式收集为主 (Filebeat)
- 少量网络数据 (Packetbeat)
- 系统指标数据 (Matricbeat/Collectd/NMon in Splunk)
- 容器日志 (TBD: Kafka Driver)



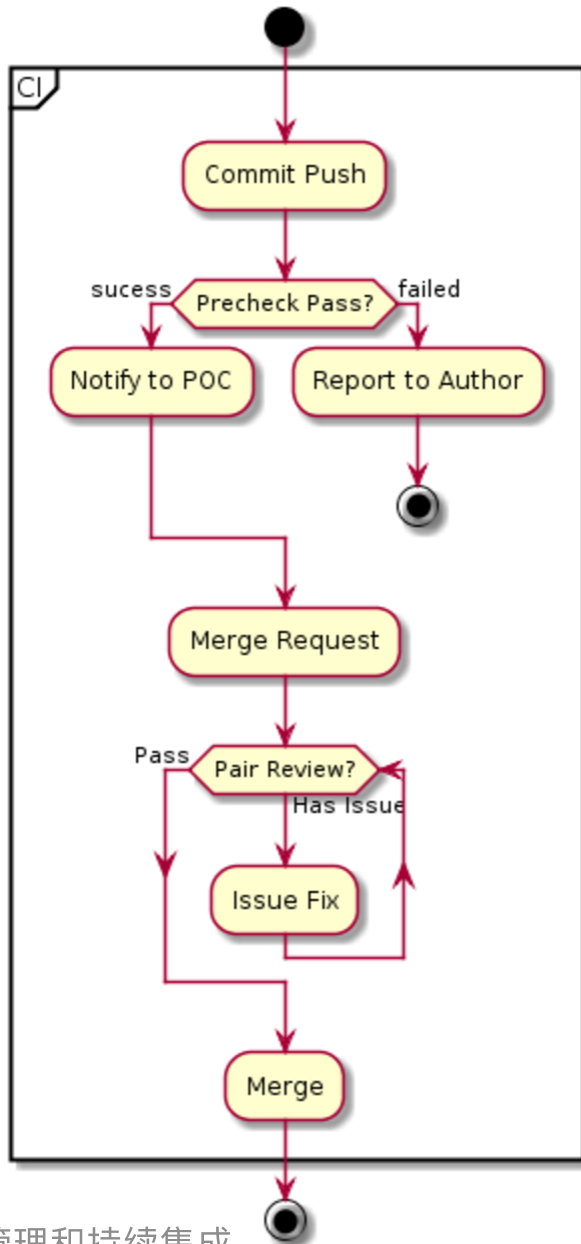
# 架构演进

- 单机原型
- ES 独立
- 跨机房数据收集 - Redis
- ES 分离 (Master/Data/Coordinating Node)

# 架构

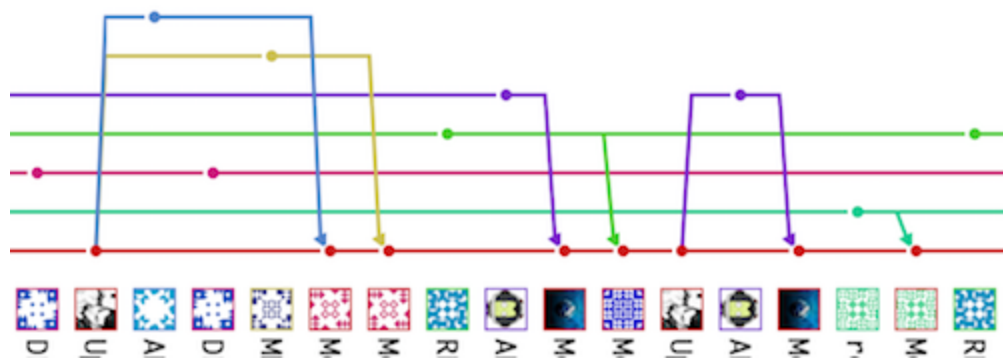


# 配置管理和持续集成



# 配置管理和持续集成

- 使用 Git 进行版本化
- Gitlab 作为持续集成套件



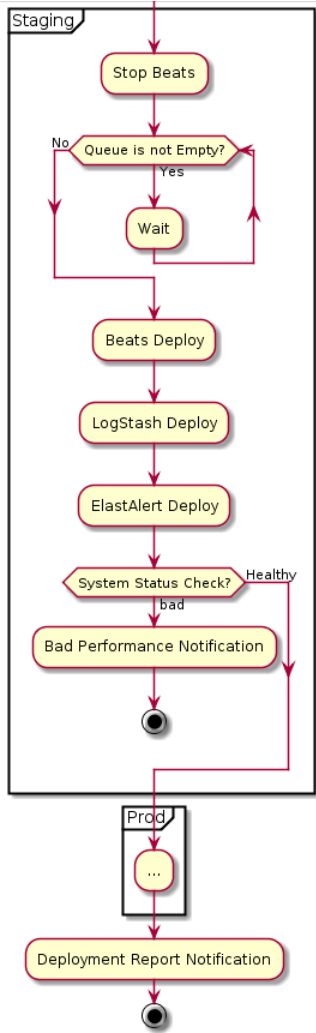
# Git 进行配置版本化

```
|_ config
|_|_ prd
|_|_|_ team_a
|_|_|_|_ filebeat-a-debug-log.yml
|_|_|_|_ filebeat-a-log-redis.yml
|_|_|_ team_b
|_|_|_|_ filebeat-c-mongo.yml
|_|_|_|_ filebeat-c-redis.yml
|_|_|_|_ filebeat-c-scheduler.yml
|_|_|_|_ filebeat-c-mysql.yml
|_|_|_|_ filebeat-c-postgresql.yml
|_|_|_ team_c
|_|_|_|_ filebeat-c-APP.yml
|_|_|_|_ filebeat-c-APP.yml
|_|_|_ team_d
|_|_|_|_ filebeat-d-service1.yml
|_|_|_|_ filebeat-d-service2.yml
|_|_|_|_ filebeat-d-service3.yml
```

# Gitlab-CI

- Feature branch workflow
- Gitlab-CI vs. Jenkins
- Precheck
  - `logstash -t`
  - `filebeat -configtest`

# 持续部署



# 持续部署

- ELK 的状态管理
- ELK 自身监控
- 性能观察 (系统监控/x-pack monitoring)



# 状态管理

```
{% set appname = "metricbeat" %}

{{ appname }}:
  pkg.installed:
    - require:
      - pkgrepo: {{ repo_name }}
  file.managed:
    - name: /etc/{{ appname }}/{{ appname }}.yml
    - source: salt://fw-{{ appname }}/{{ appconfig }}
    - template: jinja
```

# 状态管理

```
{{ appname }}-service:  
  service.running:  
    - name: {{ appname }}  
    - enable: True  
    - reload: True  
    - require:  
      - pkg: {{ appname }}  
      - file: {{ appname }}-permission  
      - file: {{ appname }}  
    - watch:  
      - file: {{ appname }}
```

# 状态管理

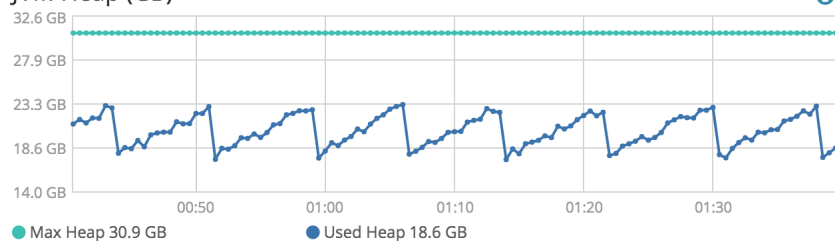
```
supervisor:
  pkg.installed: []
  file.managed:
    - name: /etc/supervisord.d/logstash.ini
    - contents: |+
      {% for path in paths %}{% set pname = get_filename
      [program:{{ pname }}]
      command=logstash --path.settings /opt/logstash/etc
      -f {{ path }} --path.data /opt/logstash,
      -n {{ grains['fqdn'] }}:{{ pname }}
      directory=/opt/logstash/
      user=logstash
      environment=LS_HEAP_SIZE=256m
      {% endfor %}
    - require:
      - file: logstash
```

# 状态管理

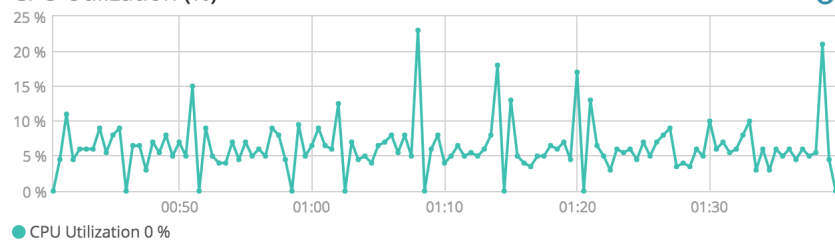
```
elasticsearch:
  file.managed:
    - name: /etc/elasticsearch/elasticsearch.yml
    - source: salt://es/elasticsearch-5.y/elasticsearch.yml
    - template: jinja
  cmd.run:
    - name: elasticsearch-plugin install x-pack
    - unless: elasticsearch-plugin list | grep x-pack
  service.running:
    - enable: True
    - reload: True
    - require:
      - pkg: elasticsearch-pkg
      - file: elasticsearch
      - file: elasticsearch-link
    - watch:
      - file: elasticsearch
```

# 自身监控

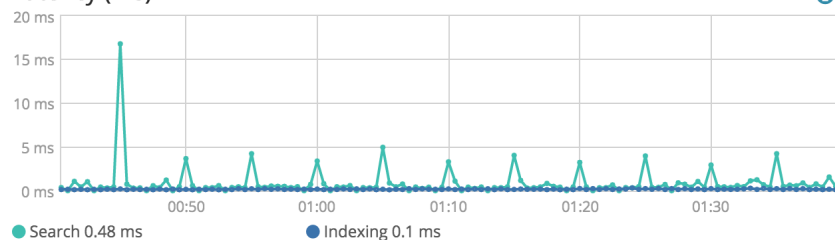
## JVM Heap (GB)



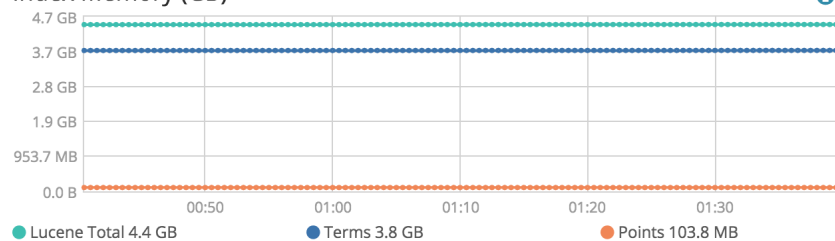
## CPU Utilization (%)



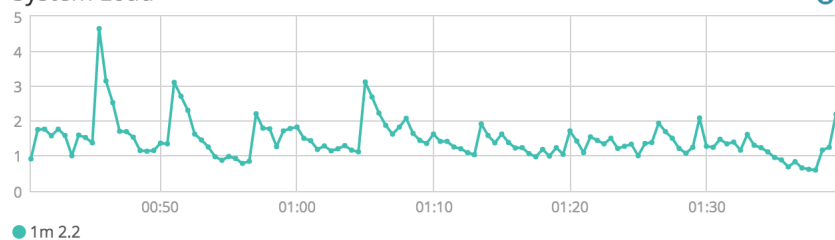
## Latency (ms)



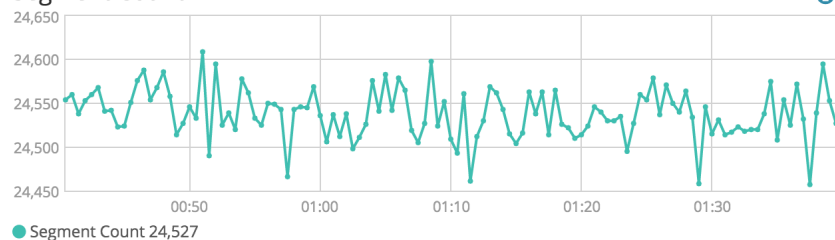
## Index Memory (GB)



## System Load



## Segment Count



# 发现的问题

- Salt-API timeout
- 新 LogStash 配置没有启动
- ElastAlert
- Filebeat 对 RHEL5 的支持

# Filebeat 对 RHEL5 的支持

```
diff -urpN output_orig/etc/init.d/filebeat output/etc/init.d/filebeat
--- output_orig/etc/init.d/filebeat
+++ output/etc/init.d/filebeat
@@ -27,8 +27,13 @@ pidfile=${PIDFILE-/var/run/filebeat.pid}
-wrapper="/usr/share/filebeat/bin/filebeat-god"
-wrapperopts="-r / -n -p $pidfile"
+if grep -q -i "release 7" /etc/redhat-release; then
+ wrapper="/usr/share/filebeat/bin/filebeat-god"
+else
+ wrapper="/usr/share/filebeat/bin/filebeat-god-el5"
+fi
+beat_user="monitor"
+wrapperopts="-r / -n -p $pidfile -u $beat_user"
  RETVAL=0

  test() {
-     $agent $args $test_args
+     runuser -s /bin/bash $beat_user -c "$agent $args $test_args"
  }
```

# 未来展望

- Kafka
- MetricBeat
- Container Monitoring
- ELK - Dockerize



# Q&A

We're hiring ❤️ [xhuang@freewheel.tv](mailto:xhuang@freewheel.tv)

