

# CKA-14日志管理

讲师：老段 RHCE/RHCA/COA/CKA

# 架构

## ELK

Elasticsearch #是个开源分布式搜索引擎，存储日志及提供查询接口。

Logstash #是一个完全开源的工具，他可以对日志进行收集 发送给Elasticsearch.

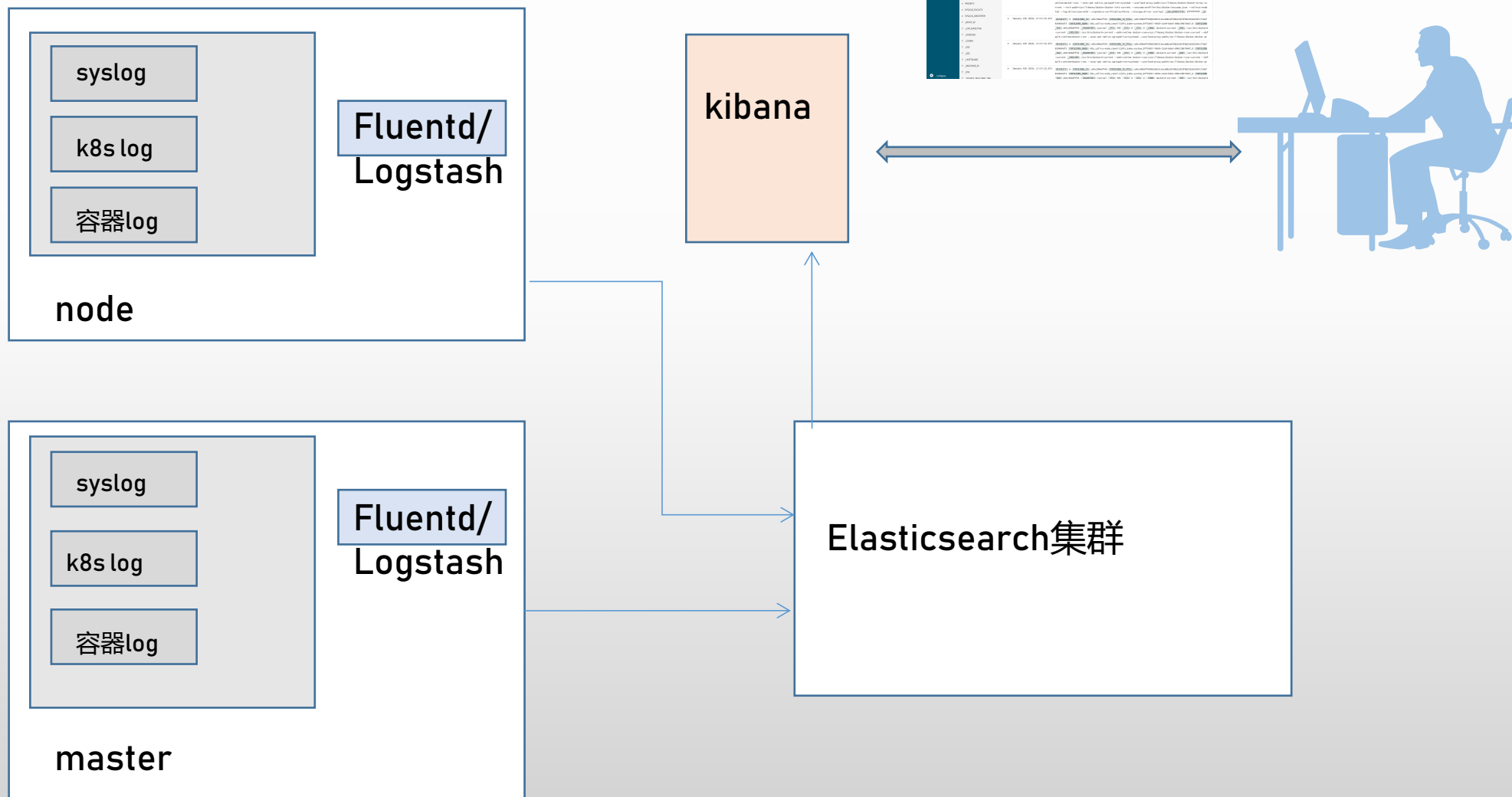
Kibana #是一个开源和免费的，web界面的工具，可以让用户浏览Elasticsearch里的日志.

logstash性能低，消耗资源，且存在不支持消息队列缓存及存在数据丢失的问题

所以logstash一般可以用fluentd或者filebeat替代

## EFK框架

# 架构



# 下载所需要的镜像

```
docker pull registry.cn-hangzhou.aliyuncs.com/elasticsearch/elasticsearch:6.7.2
```

```
docker pull registry.cn-hangzhou.aliyuncs.com/google_containers/fluentd-elasticsearch:v2.4.0
```

```
docker pull registry.cn-hangzhou.aliyuncs.com/middle_ware/kibana:6.7.2
```

```
docker pull alpine:3.6
```

# 下载所需要的yaml文件

wget

<https://raw.githubusercontent.com/kubernetes/kubernetes/master/cluster/addons/fluentd-elasticsearch/es-statefulset.yaml>

wget

<https://raw.githubusercontent.com/kubernetes/kubernetes/master/cluster/addons/fluentd-elasticsearch/es-service.yaml>

wget

<https://raw.githubusercontent.com/kubernetes/kubernetes/master/cluster/addons/fluentd-elasticsearch/fluentd-es-configmap.yaml>

wget

<https://raw.githubusercontent.com/kubernetes/kubernetes/master/cluster/addons/fluentd-elasticsearch/fluentd-es-ds.yaml>

wget

<https://raw.githubusercontent.com/kubernetes/kubernetes/master/cluster/addons/fluentd-elasticsearch/kibana-service.yaml>

wget

<https://raw.githubusercontent.com/kubernetes/kubernetes/master/cluster/addons/fluentd-elasticsearch/kibana-deployment.yaml>

# 部署

修改kibana-deployment.yaml, 注释掉2行

37 ~~#- name: SERVER\_BASEPATH~~

38 ~~# value: /api/v1/namespaces/kube-system/services/kibana-logging/proxy~~

~~#为节点打标签~~

~~#kubectl label nodes --all beta.kubernetes.io/fluentd-ds-ready=true~~

先部署elasticsearch, 确保pod正常运行

再部署 fluentd, 确保pod正常运行

最后部署 kibana

把所有节点重启

稍等一会即可

Kibana

←

→

↺

🏠

192.168.26.10:30813/app/kibana#/management/kibana/index?\_g=0

🔍

⋮

★

📊

📄

💬

↶

🔔

🌐

👤

☰

kibana

🕒

Discover

📈

Visualize

📊

Dashboard

🛡️

Timelion

🏠

Canvas

📍

Maps

🧠

Machine Learning

🏢

Infrastructure

📄

Logs

📁

APM

🕒

Uptime

🔧

Dev Tools

Elasticsearch

Index Management

Index Lifecycle Policies

Rollup Jobs

Cross Cluster Replication

Remote Clusters

License Management

7.0 Upgrade Assistant

Create index pattern

No default index pattern. You must select or create one to continue.

Kibana

Index Patterns

Saved Objects

Spaces

Reporting

Advanced Settings

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

×

Include system indices

Step 1 of 2: Define index pattern

Index pattern

\*

You can use a \* as a wildcard in your index pattern.

You can't use spaces or the characters \, /, ?, ", <, >, |.

Next step

✓ Success! Your index pattern matches 1 index.

logstash-2019.10.09

Rows per page: 10

# 创建index

index fluentd-k8s-\*

Management / Kibana

Index Patterns Saved Objects Advanced Settings

★ fluentd-k8s-\*

### Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations. ☐ Include system indices

Step 1 of 2: Define index pattern

Index pattern

fluentd-k8s-\*

You can use a \* as a wildcard in your index pattern.  
You can't use empty spaces or the characters \, /, ?, ", <, >, |.

✓ **Success!** Your index pattern matches **3 indices**.

fluentd-k8s-2018.12.23

> Next step



