

CKA-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，具有分布式，零配置，自动发现，索引自动分片，索引副本机制，restful风格接口，多数据源，自动搜索负载等特性。

Logstash #是一个完全开源的工具，他可以对日志进行收集、分析，并将其存储。

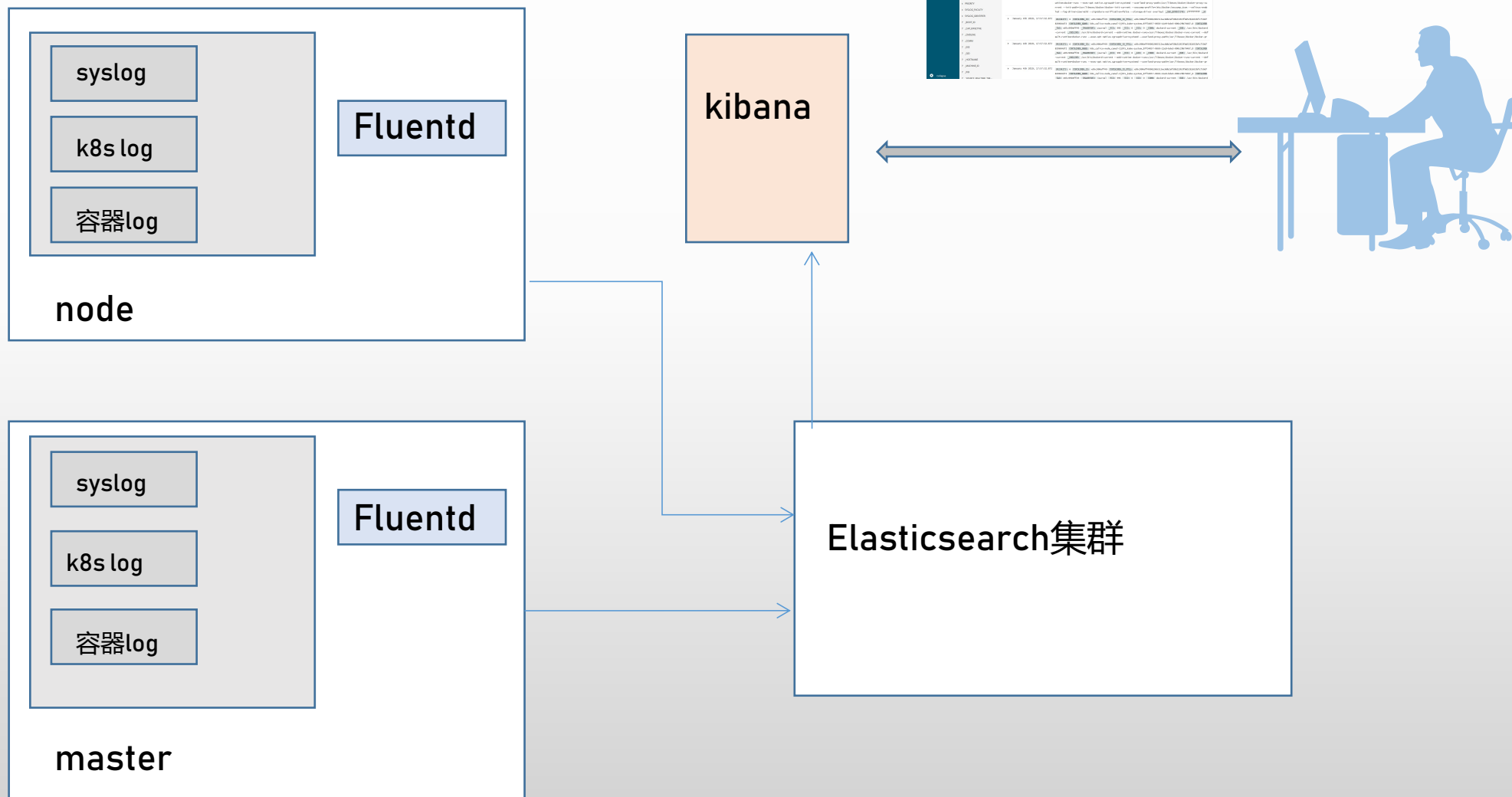
Kibana #是一个开源和免费的工具，可以为 Logstash 和 ElasticSearch 提供的日志分析友的 Web 界面。

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/google_containers/elasticsearch:v6.2.5
```

```
docker pull alpine:3.6
```

```
docker pull radial/busyboxplus:curl
```

```
docker pull registry.cn-shanghai.aliyuncs.com/k8s-log/kibana:6.2.4
```

```
docker pull registry.cn-hangzhou.aliyuncs.com/google_containers/fluentd-  
elasticsearch:v2.2.0
```

部署elasticsearch

下载yaml文件

```
git clone https://github.com/mgxian/k8s-log.git
```

```
kubectl create ns logging
```

部署elasticsearch

```
kubectl apply -f elasticsearch.yaml
```

验证

```
kubectl get pods,svc -n logging
```

```
kubectl run curl -n logging --image=radial/busyboxplus:curl -i --tty
```

```
nslookup elasticsearch-logging
```

```
curl 'http://elasticsearch-logging:9200/_cluster/health?pretty'
```

```
curl 'http://elasticsearch-logging:9200/_cat/nodes'
```

```
exit
```

部署kibana及fluentd

```
kubectl apply -f kibana.yaml
```

```
kubectl get pods,svc -n logging -o wide
```

在浏览器里打开kibana的服务查看

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

```
kubectl apply -f fluentd-es-configmap.yaml
```

```
kubectl apply -f fluentd-es-ds.yaml
```

```
kubectl get pods,svc -n logging -o wide
```

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

