

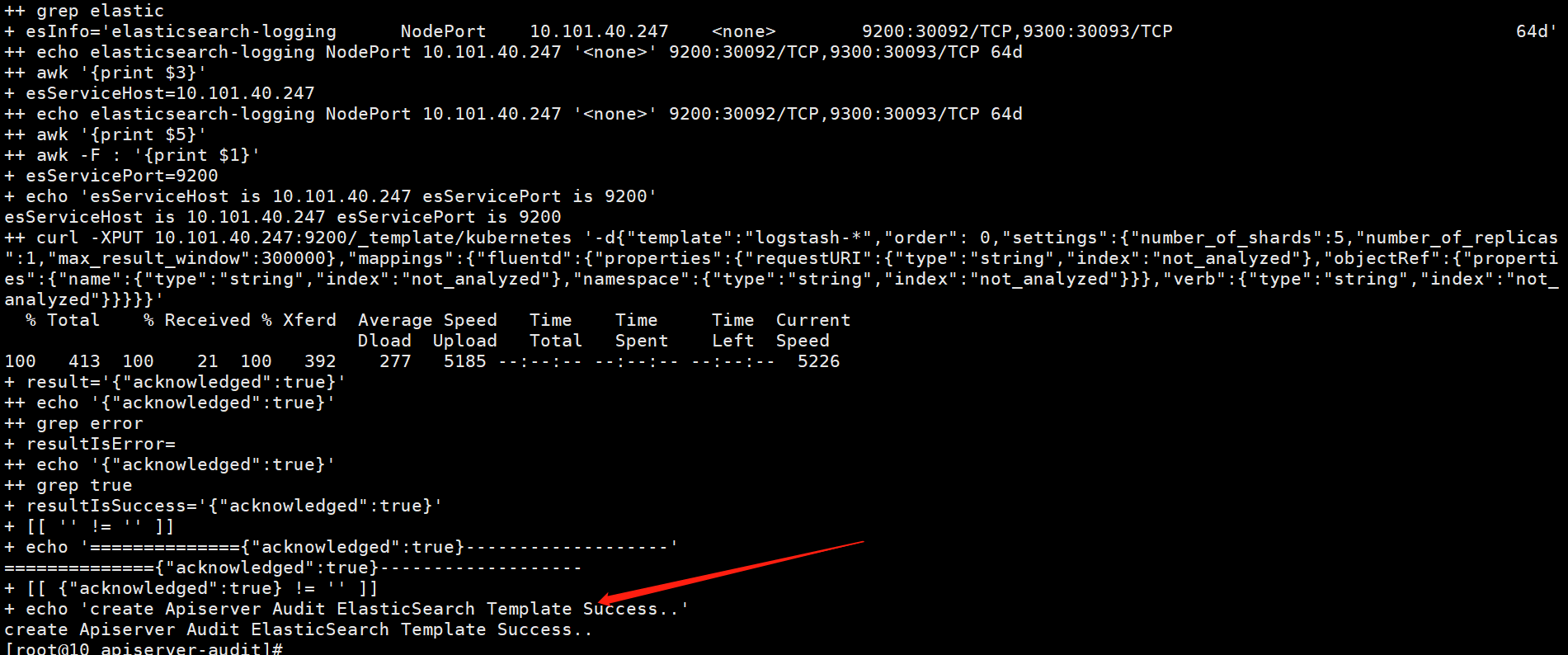
1、首先点击apiserver-audit.zip下载到本地，并上传到master节点。

2、在数据库中执行k8s-apiserver-audit-upgrade.sql文件中的sql；

3、创建索引：

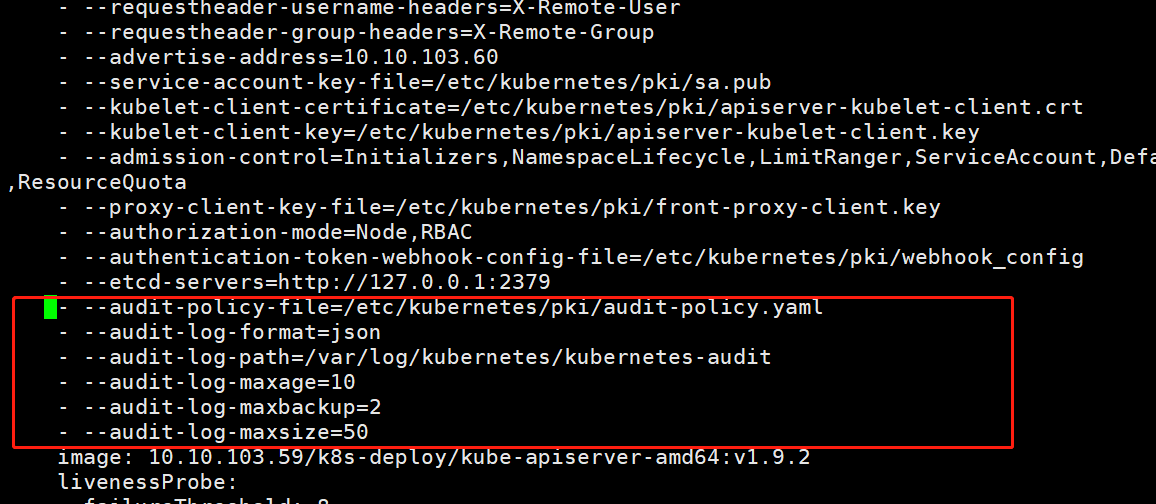
sh -x createApiserverAuditElasticSearchTemplate.sh

看到输出success字样表示创建索引成功。



4、复制audit-policy.yaml到/etc/kubernetes/pki/目录下

在/etc/kubernetes/manifests目录的kube-apiserver.yaml中加：



- --audit-policy-file=/etc/kubernetes/pki/audit-policy.yaml

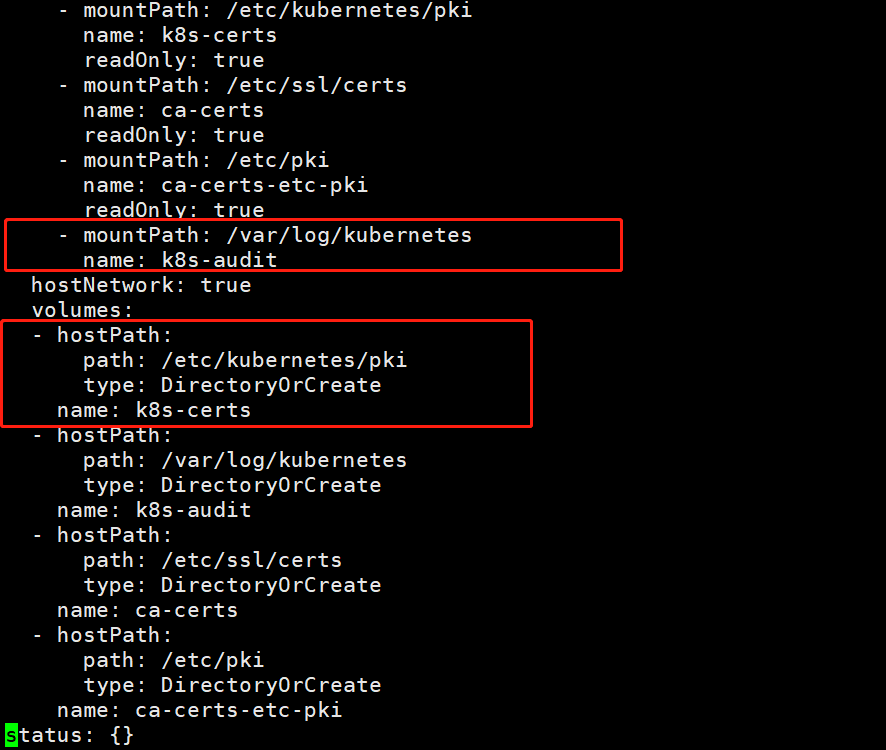
- --audit-log-format=json

- --audit-log-path=/var/log/kubernetes/kubernetes-audit

- --audit-log-maxage=10

- --audit-log-maxbackup=2

- --audit-log-maxsize=50



- mountPath: /var/log/kubernetes

name: k8s-audit

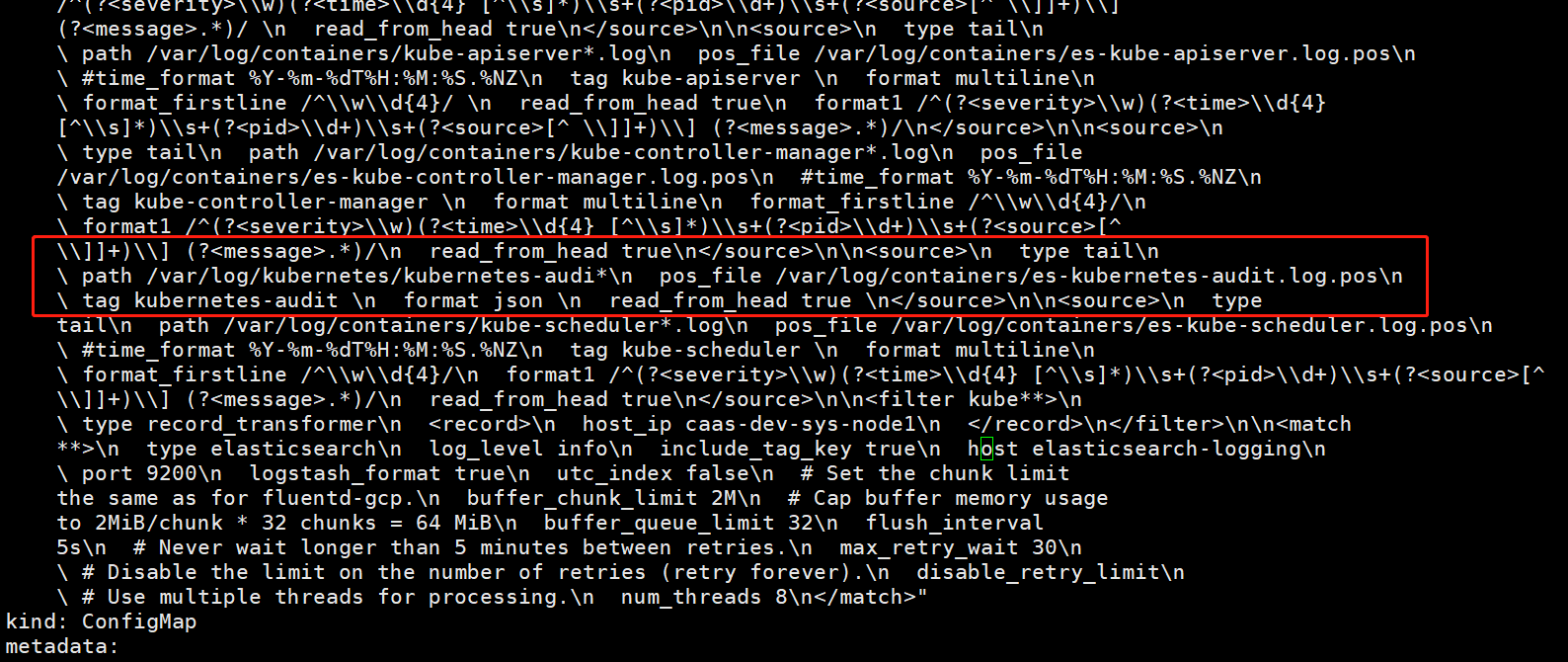
- hostPath:

path: /etc/kubernetes/pki

type: DirectoryOrCreate

name: k8s-certs

5、修改名为fluentd的comfigmaps：



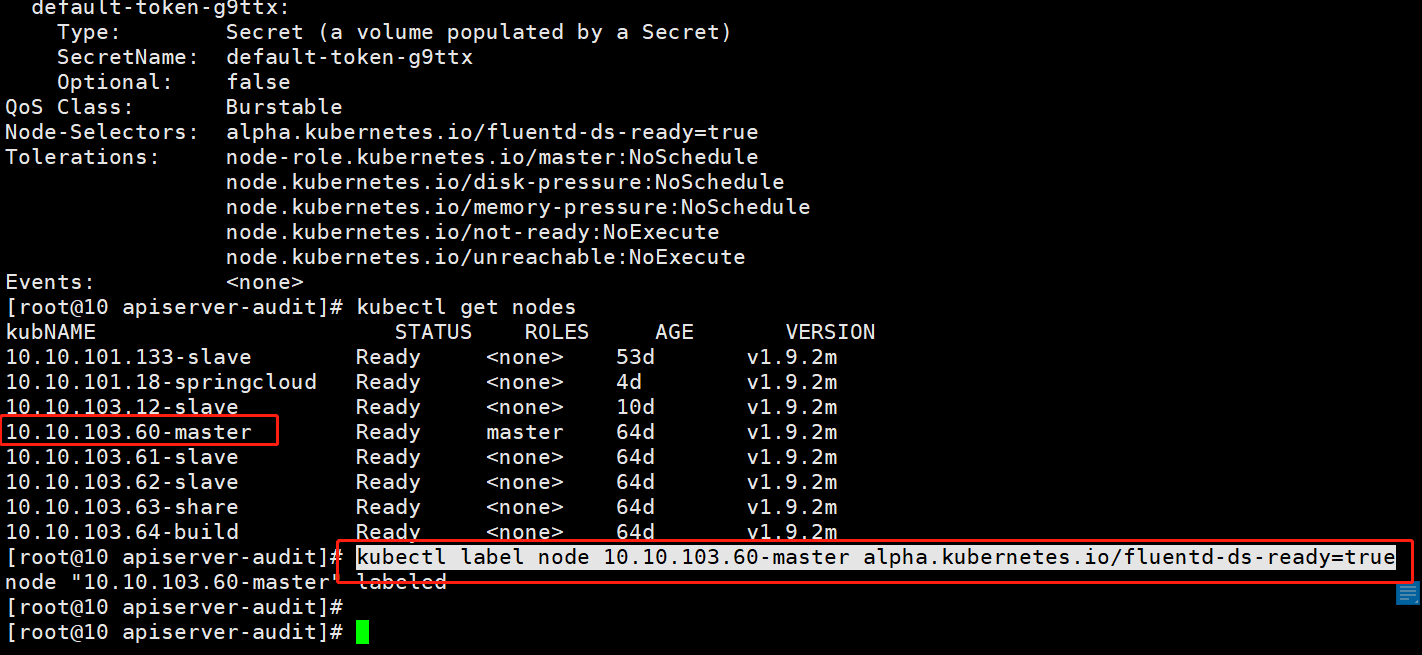
<source>\n type

tail\n path /var/log/kubernetes/kubernetes-audi\* \n pos\_file /var/log/containers/es-kubernetes-audit.log.pos\n

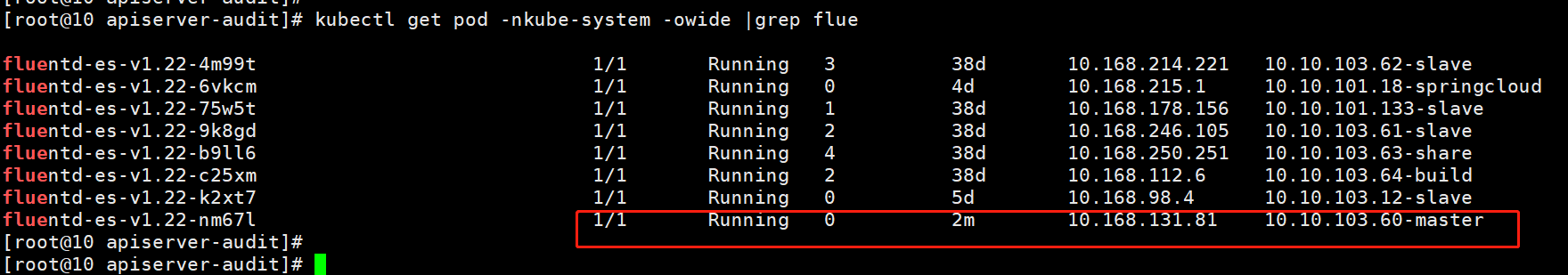
\ tag kubernetes-audit \n format json \n read\_from\_head true \n</source>\n\n

6、在apiserver所部署的节点上打标签：

kubectl label node 10.10.103.60-master alpha.kubernetes.io/fluentd-ds-ready=true

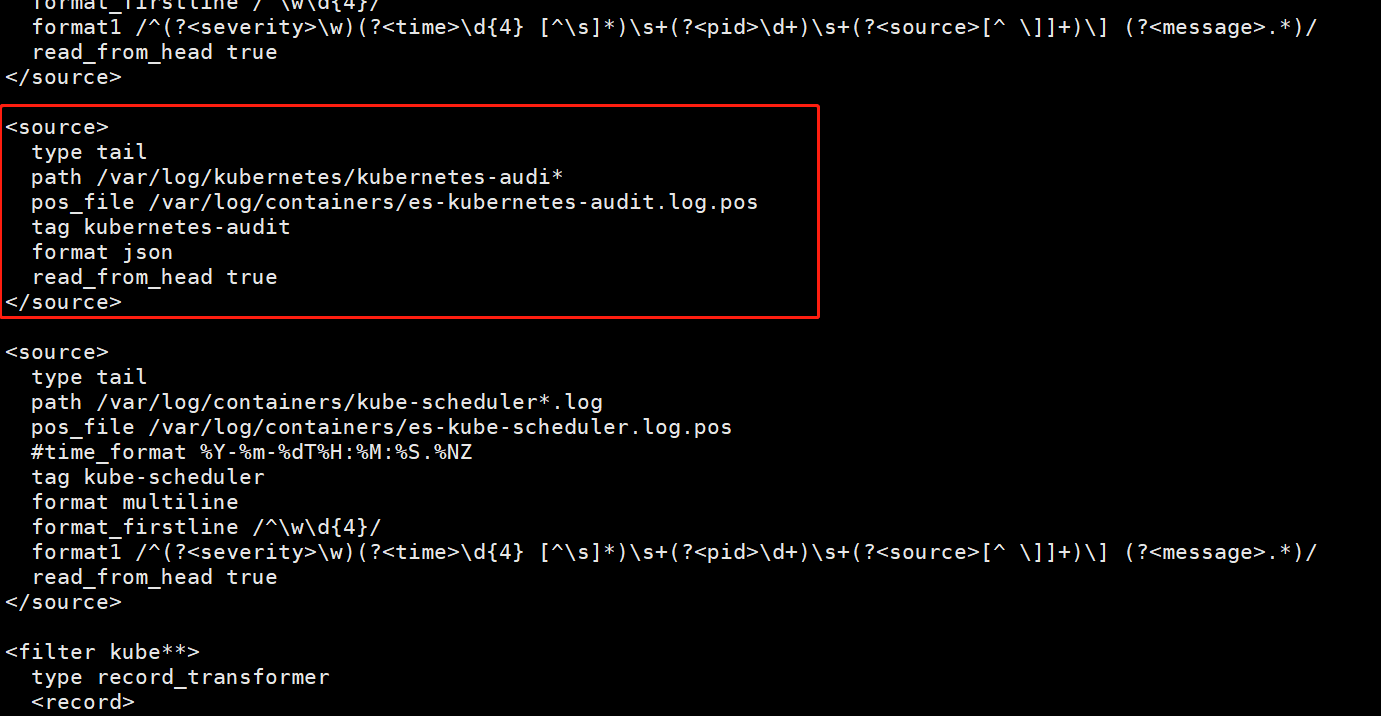


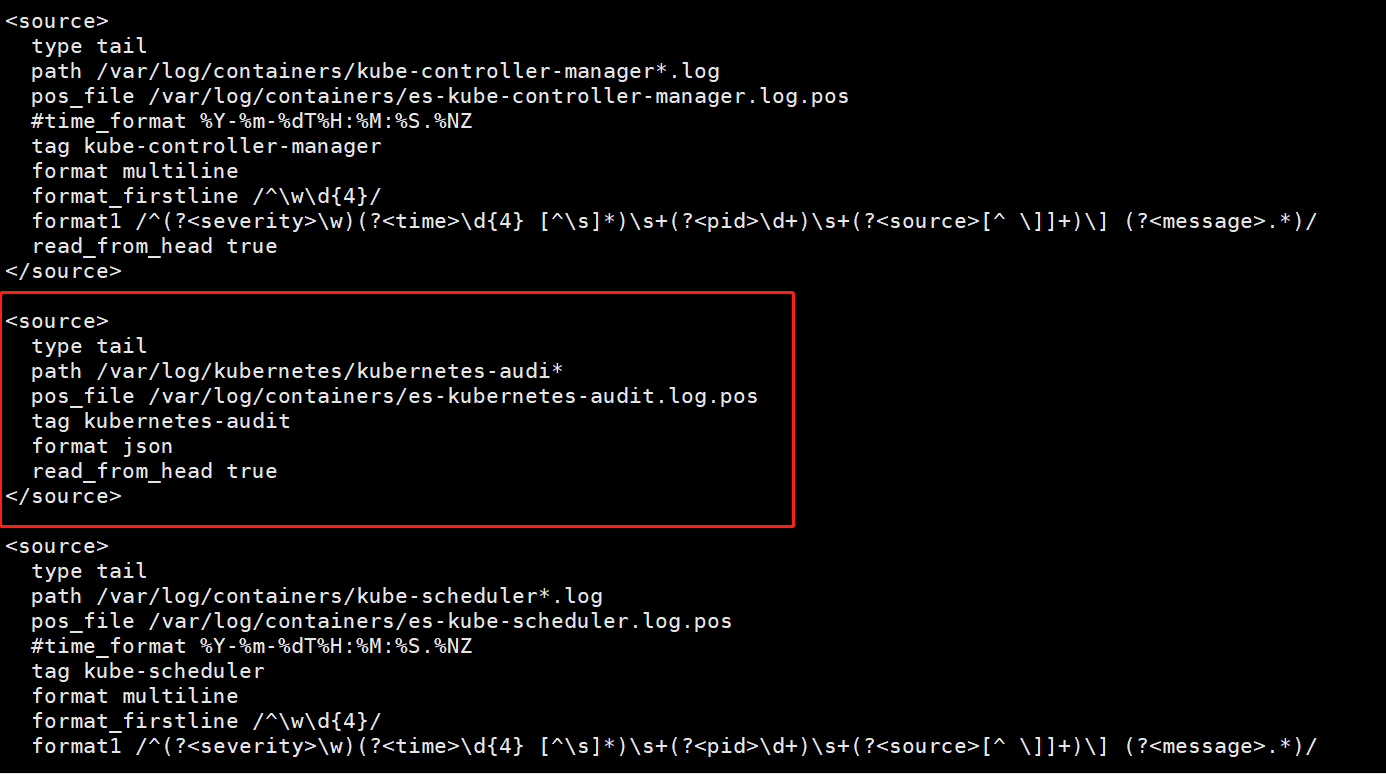
7、查看fluentd-es是否被调度到master节点，等待状态变为Running



8、重启以后看下master节点fluentd的配置：

kubectl exec -ti fluentd-es-v1.22-nm67l -nkube-system -- cat /etc/td-agent/td-agent.conf





9、安装完成，可登陆观云台->日志管理->集群审计查看日志