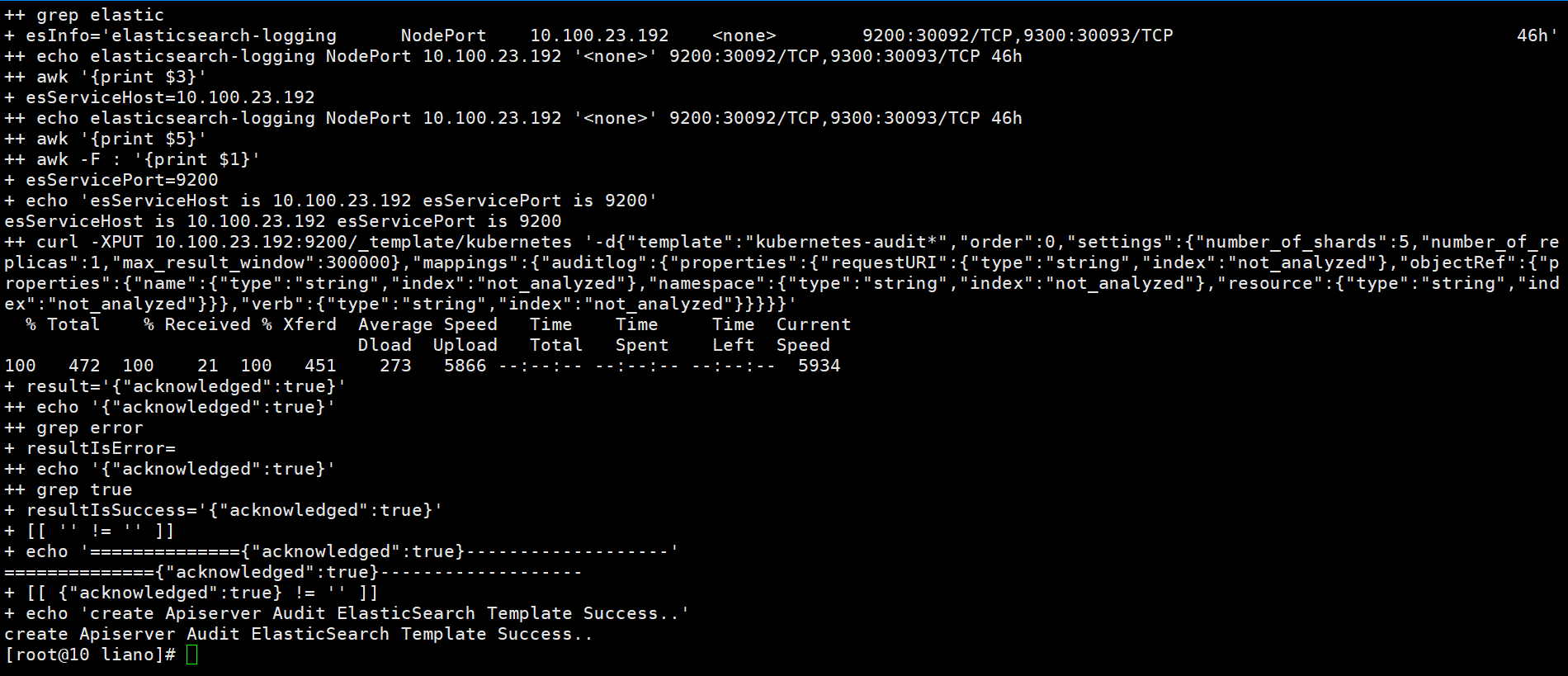
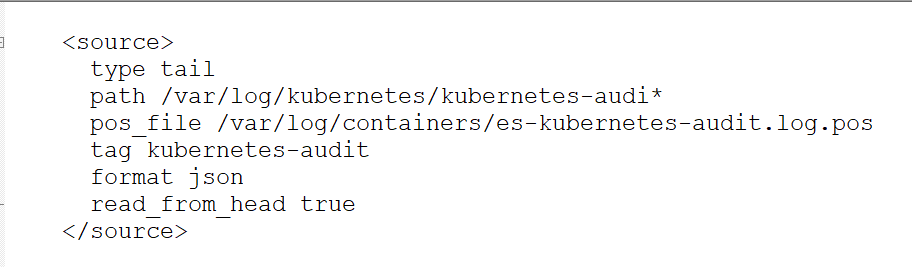
1、创建索引：

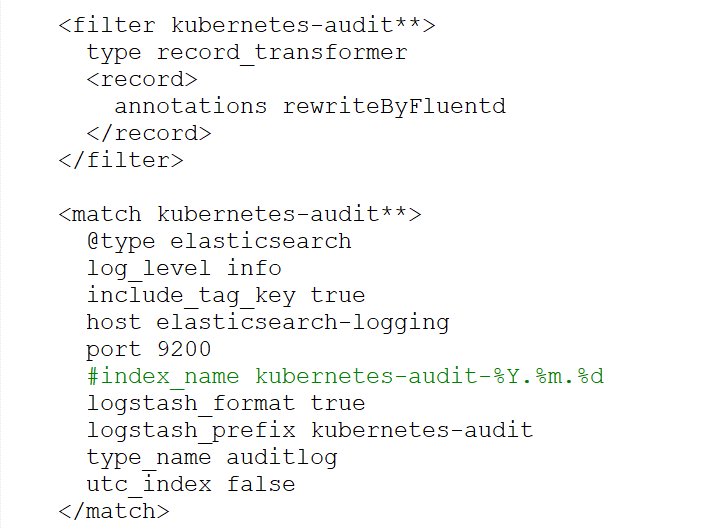
sh -x createApiserverAuditElasticSearchTemplate.sh

看到输出success字样表示创建索引成功。



2、查看fluentd-configmap.yaml文件，增加了以下内容：



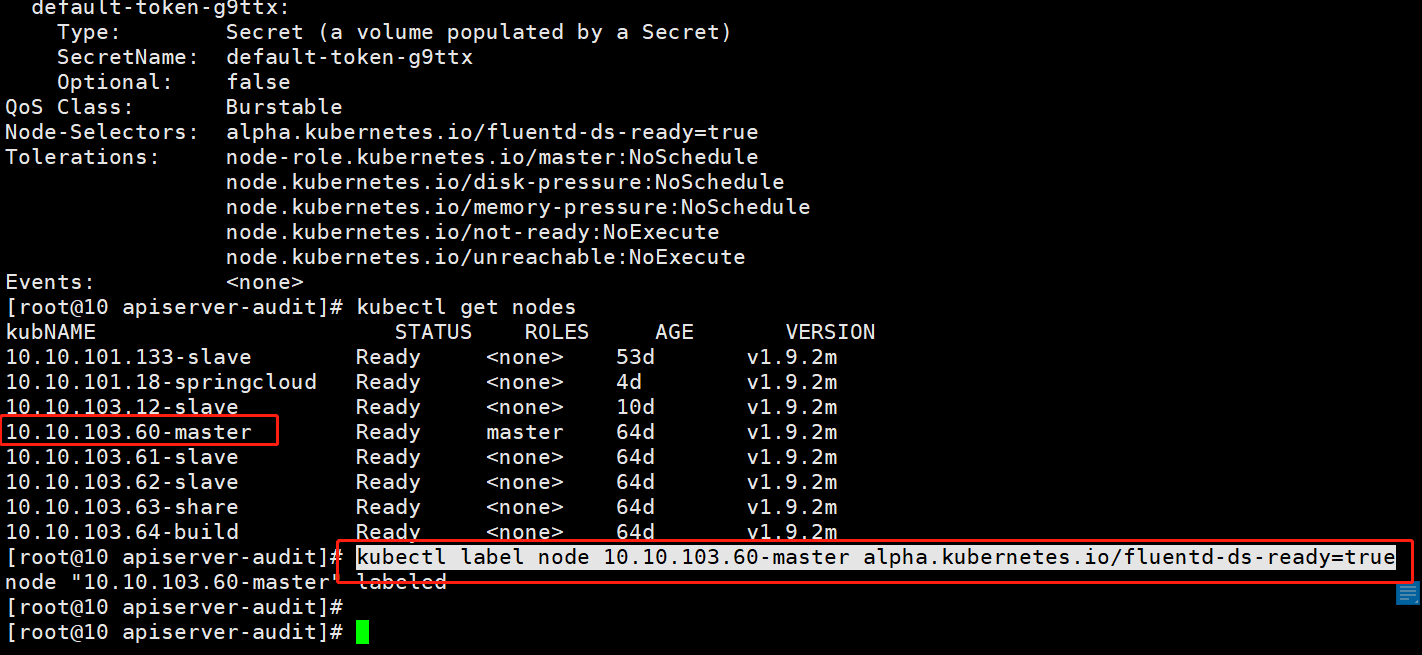


修改已有名为fluentd的comfigmaps：

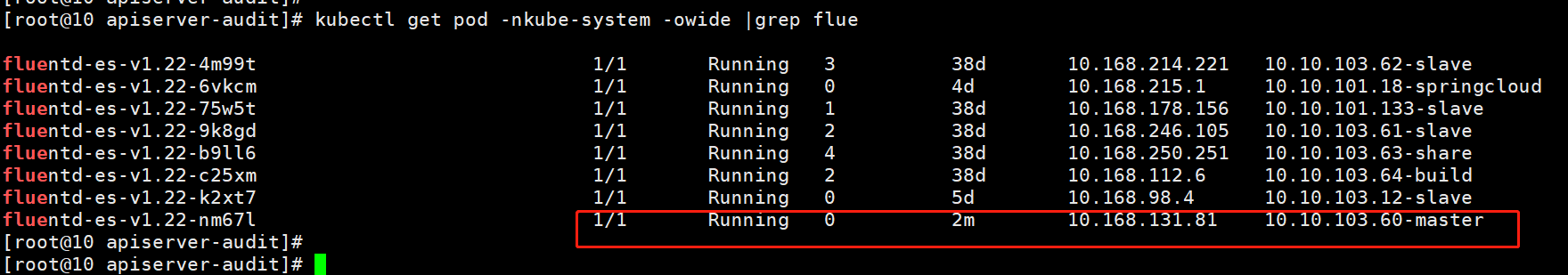
kubetl apply -f fluentd-configmap.yaml

5、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

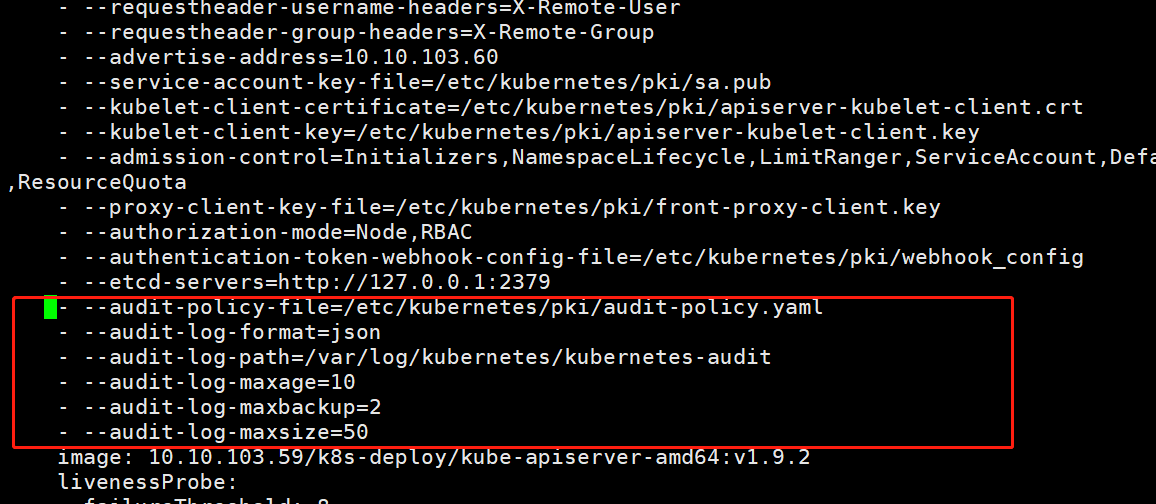


6、查看fluentd-es是否被调度到master节点，等待状态变为Running



7、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

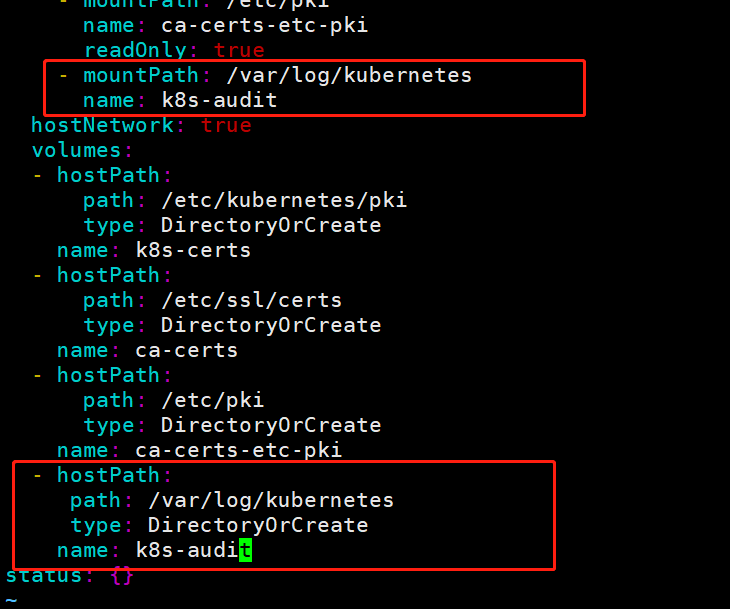
- --audit-log-format=json

- --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: /var/log/kubernetes

type: DirectoryOrCreate

name: k8s-audit

保存退出，等k8s Api-server pod重启成功，状态变为Running

8、安装完成，可登陆观云台->日志管理->集群审计查看日志