HUAWEI

扫码添加小助手，发送“CKA”加群

HUAWEI

CloudNative Lives

Kubernetes管理员实训

K8S存储管理实训

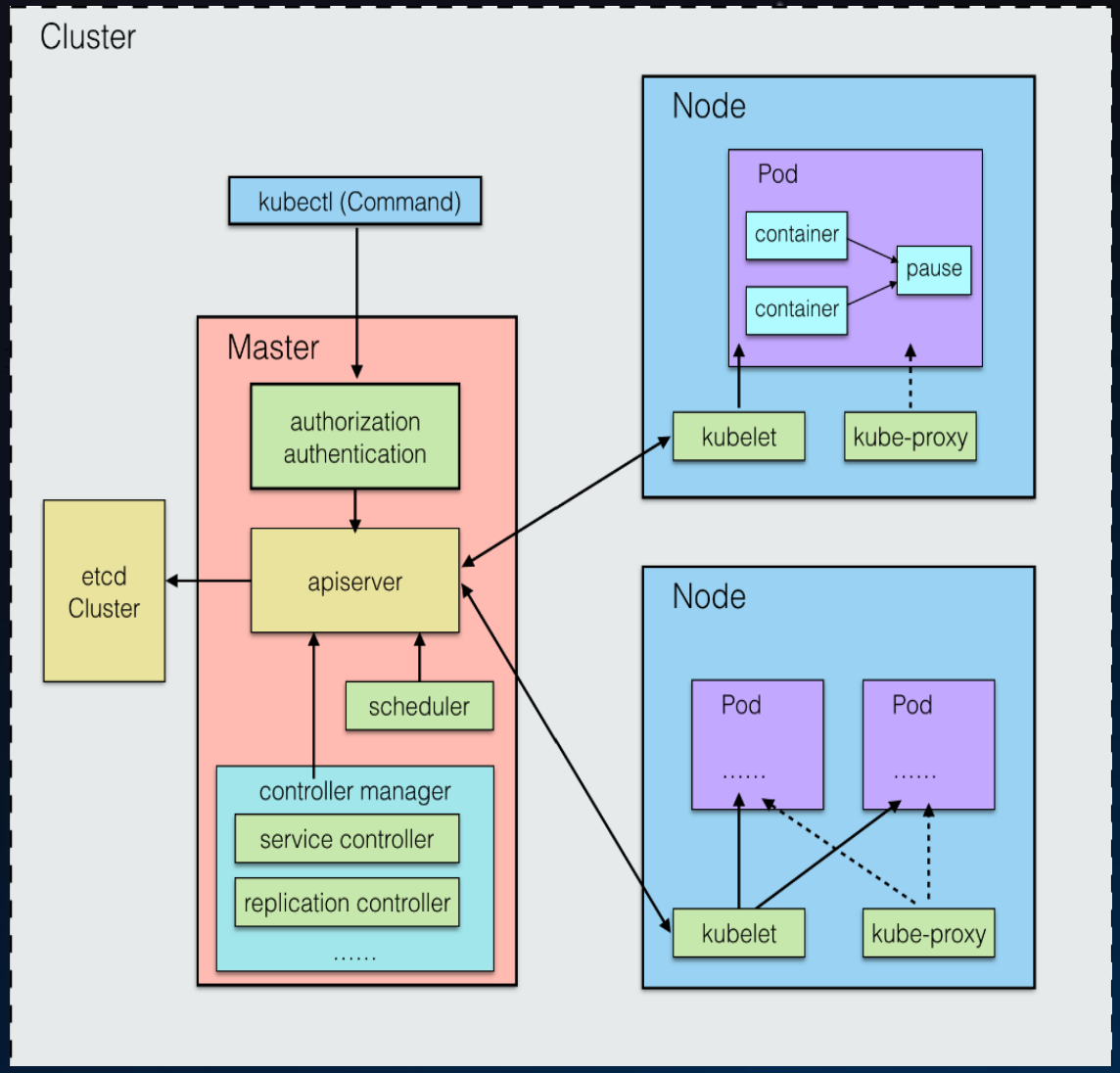
华为云容器团队核心架构师 & CNCF社区主要贡献者倾力打造

HUAWEI

大 纲

- 集群部署及安全配置
- 节点证书签发
- 安装network插件插件
- 高可用集群
- 集群升级与备份恢复
- E2E测试及结果分析

K8S集群工作原理



Master节点：负责整个集群的管理和控制

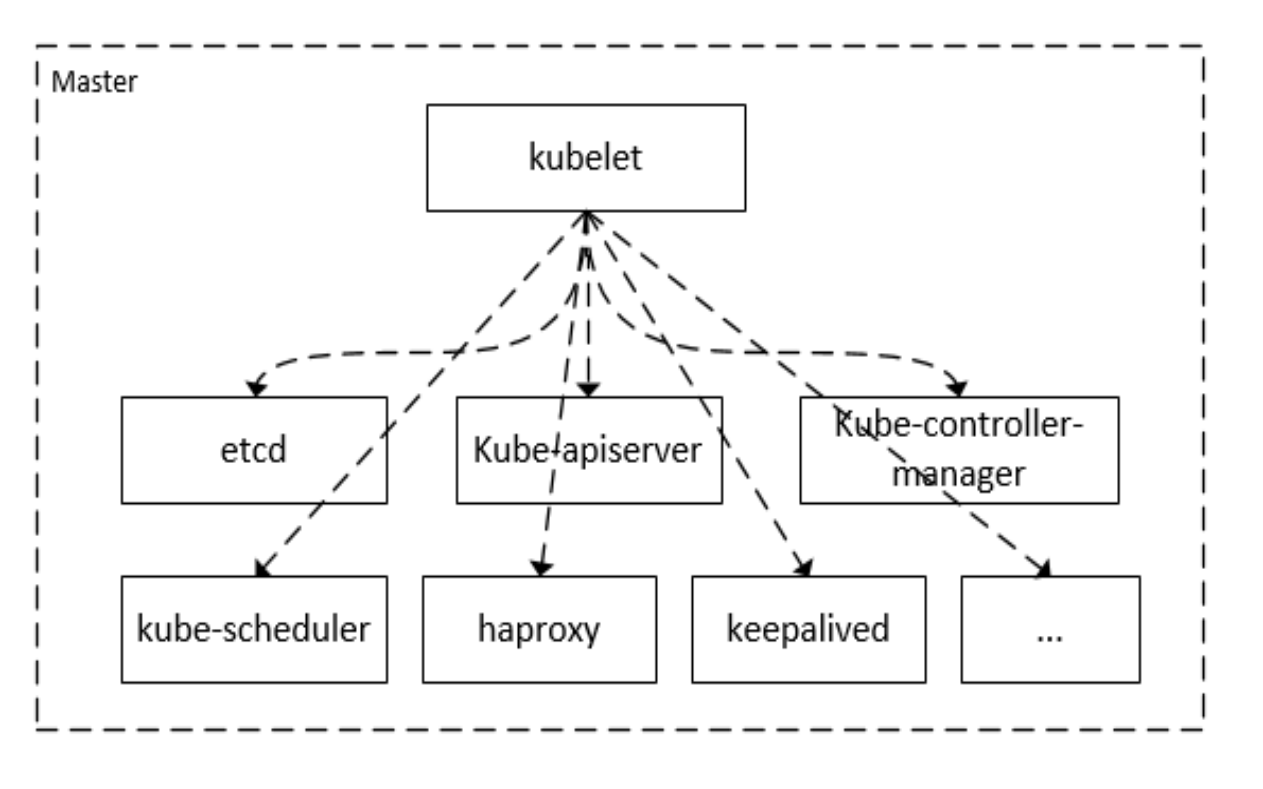
- etcd
- kube-apiserver
- kube-controller-manager
- kube-scheduler

Node节点:

- kubelet
- kube-proxy
- docker
- cni 插件

集群部署及安全配置

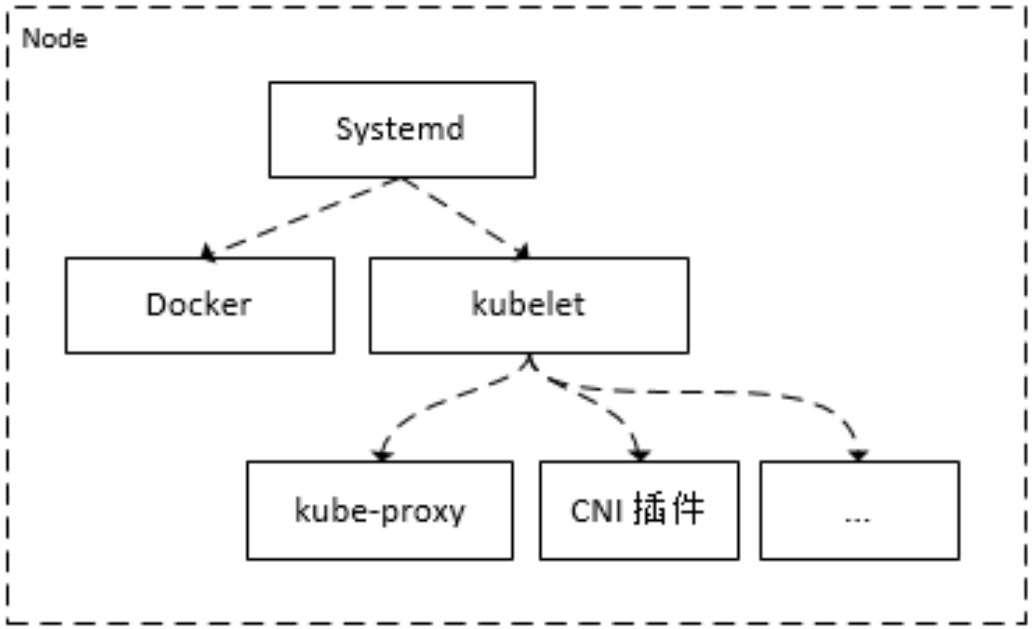
Kubelet manifest部署控制节点组件



manifest方式拉起管理面组件

Liveness、readiness配置组件健康检查

集群部署及安全配置



Systemd 管理docker、kubelet进程

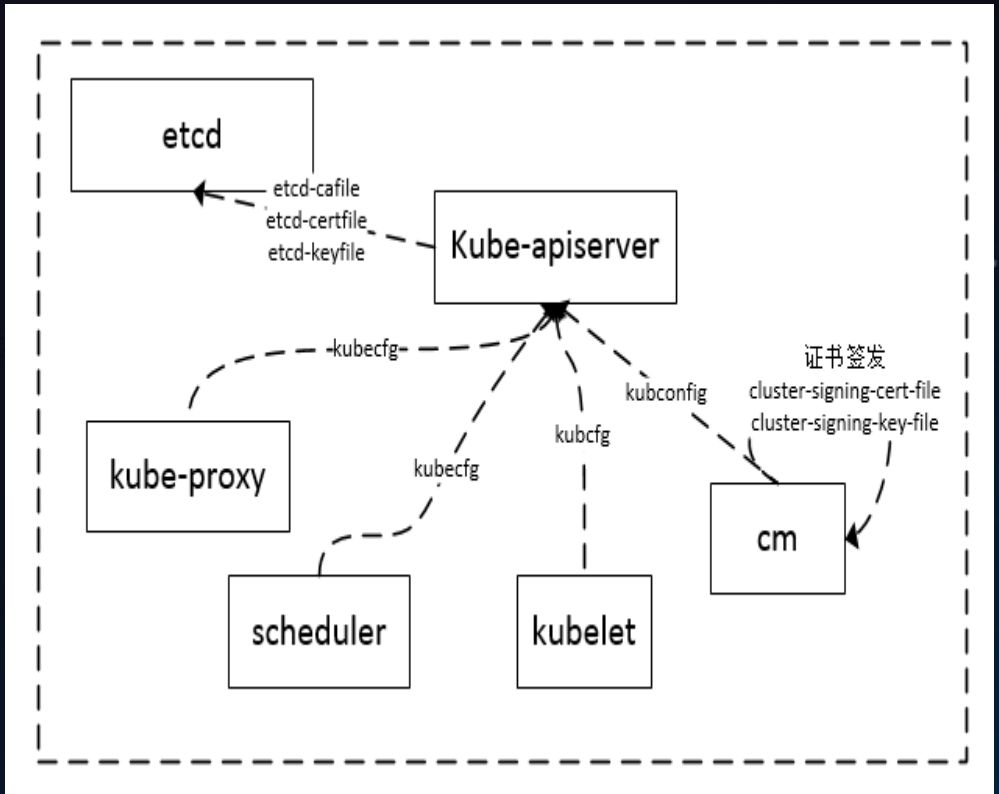
Daemonset方式部署插件

安装CNI插件

- 为pod分配IP
- 节点间podIP互通

```
kubectl apply -f
https://raw.githubusercontent.com/coreos/flannel/v0.9.1/Documentation/kube-flannel.yml
```

集群部署及安全配置




```
current-context: federal-context
clusters:
- cluster:
    server: https://example.org:443
    certificate-authority: /path/to/my/cafile
    insecure-skip-tls-verify: true
  name: cluster1
contexts:
- context:
    cluster: cluster1
    namespace: chisel-ns
    user: green-user
  name: federal-context
users:
- name: blue-user
  user:
    token: blue-token
- name: green-user
  user:
    client-certificate: path/to/my/client/cert
    client-key: path/to/my/client/key
```

集群信息：访问方式、CA等

cluster、user、ns映射到关系

客户端认证凭据：token、password、证书等

生成kubecfg文件

- 修改cluster

```
kubectl config set-cluster kubernetes
        --certificate-authority=/path/to/ca
        --embed-certs=true
        --server=${KUBE_APISERVER}
        --kubeconfig=/kubeconfig/filename
```

- 修改user

```
kubectl config set-credentials testuser
      --client-certificate=/path/to/cert
      --client-key=/path/to/private_key
      --embed-certs=true
      --kubeconfig=/kubeconfig/filename
```

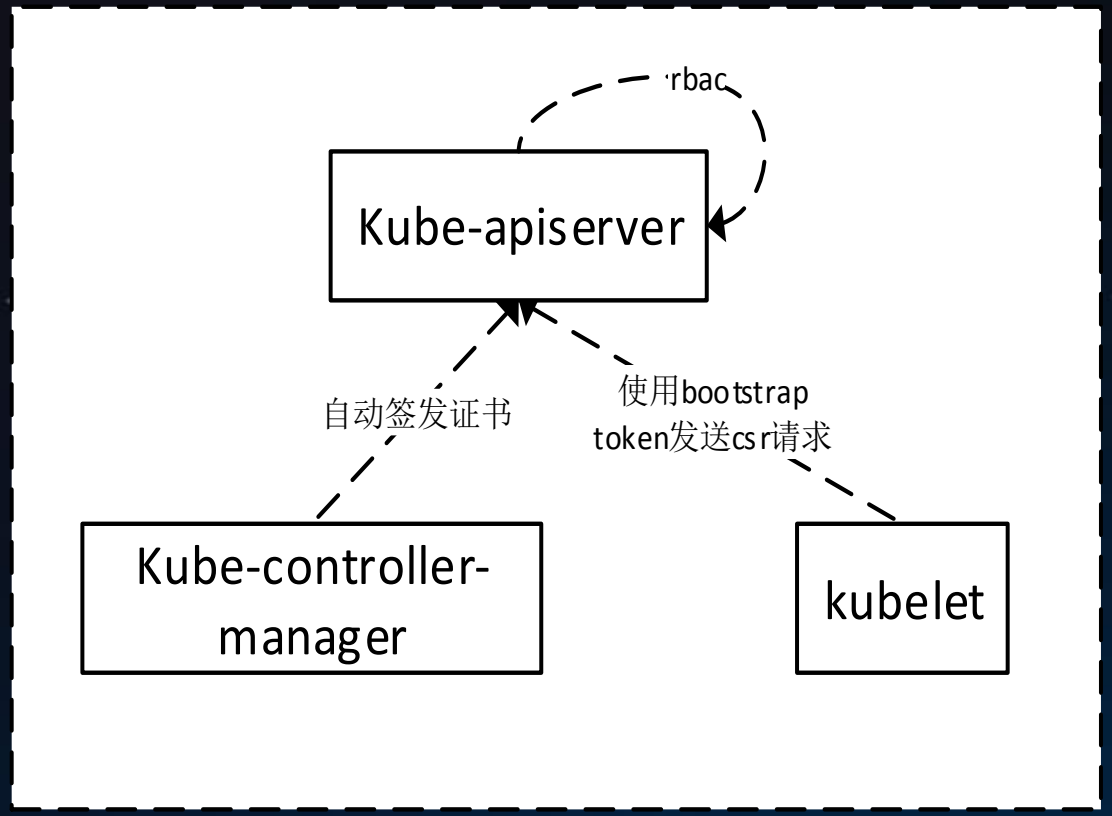
- 修改context

```
kubectl config set-context default
      --cluster=kubernetes
      --user=testuser
      --kubeconfig=test.kubeconfig
```

- 设置默认context

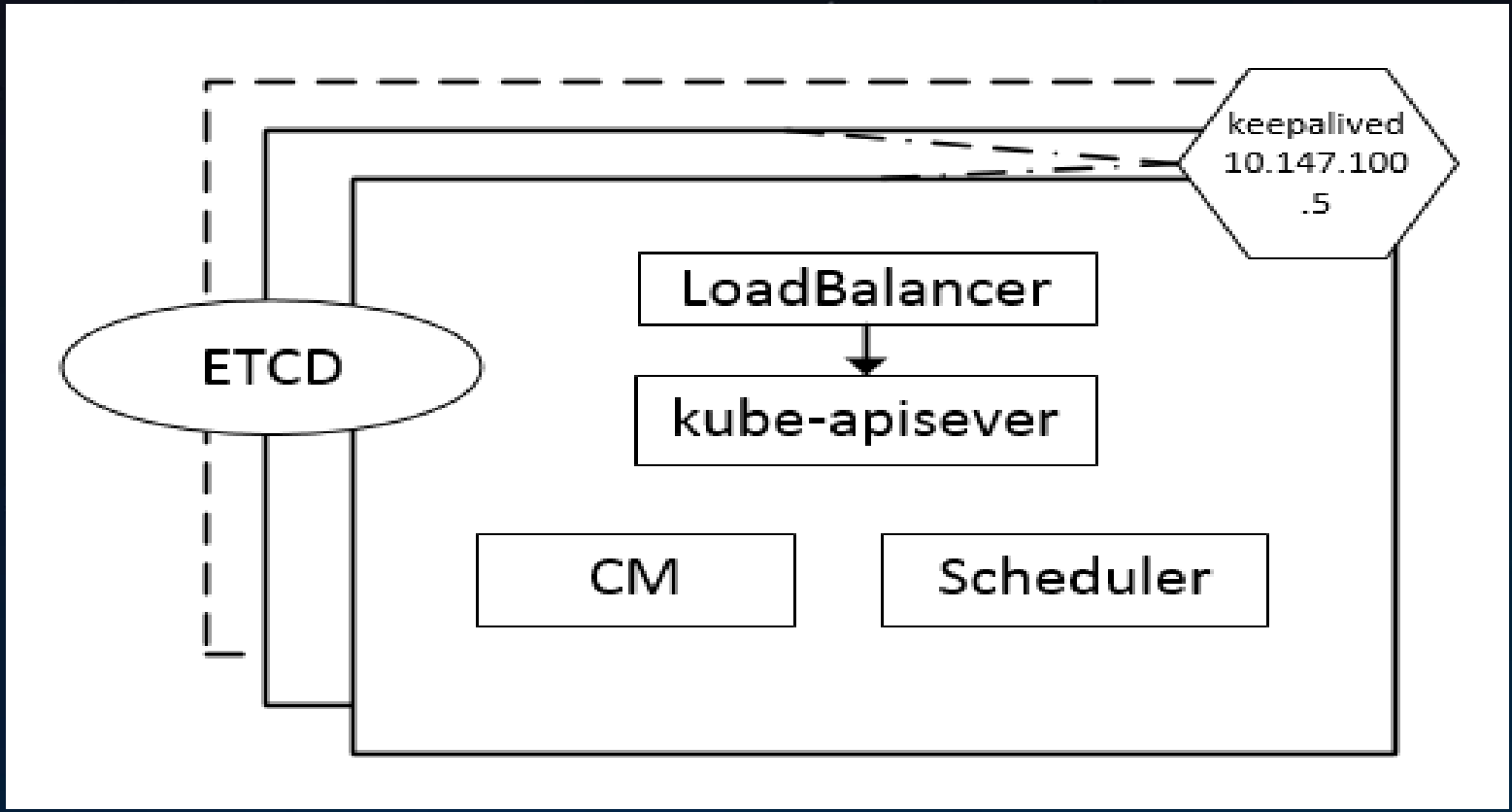
```
kubectl config use-context default
     --kubeconfig=/kubeconfig/filename
```

tls bootstrap与节点证书签发

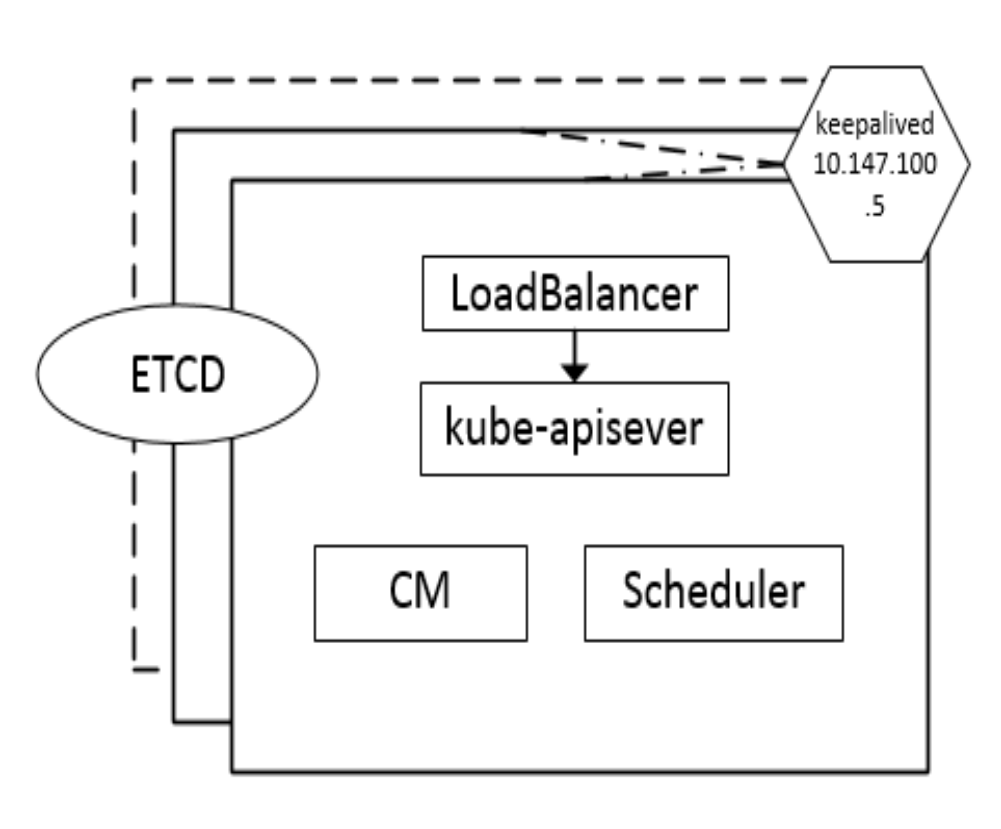


- kubelet启动时使用低权限token像kube-apiserver发送csr请求
- RBAC允许的CRS请求类型：
  nodeclient：签发证书
  selfnodeclient：更新证书
  selfnodeserver：更新kubelet server证书
- kube-controller-manager自动签发证书
- kubelet使用签发的证书、私钥访问kube-apiserver

高可用集群


keepalived
10.147.100
.5
LoadBalancer
ETCD
kube-apisever
CM
Scheduler

集群升级流程



- 控制节点滚动升级
  升级kubelet
  通过更新manifest升级控制组件

- 计算节点升级

  kubectl drain
  kubectl uncordon

备份恢复

- 周期性备份ETCD数据
- 生成snapshot

```
ETCDCTL_API=3 etcdctl --cacert /etc/kubernetes/pki/etcd/ca.crt --cert
/etc/kubernetes/pki/etcd/server.crt --key /etc/kubernetes/pki/etcd/server.key --
endpoints https://127.0.0.1:2379 snapshot save snapshotdb

ETCDCTL_API=3 etcdctl --cacert /etc/kubernetes/pki/etcd/ca.crt --cert
/etc/kubernetes/pki/etcd/server.crt --key /etc/kubernetes/pki/etcd/server.key --
endpoints https://127.0.0.1:2379 snapshot status snapshotdb -w table
```

课后作业

1. 使用kubeadm部署一个集群，部署一个cni插件，提供kube-system下所有pod截图

2. 手动配置TLS BootStrap:

   - 生成token文件
   - 为kube-apiserver配置token认证文件
   - 手动创建clusterrole、clusterrolebinding
   - 为kubelet-controller-manager配置cluster-signing-cert-file、cluster-signing-key-file
   - 为kubelet配置bootstrap kubeconfig、kubeconfig、rotateCertificates

   配置流程可参考 https://kubernetes.io/docs/reference/command-line-tools-reference/kubelet-tls-bootstrapping/

HUAWEI

HUAWEI

Thank You

直播 每周四 晚20:00

CloudNativeLives

Kubernetes Docker Istio