kubeadm Bootstrap Kubernetes

CONCEPTS

kubeadm only bootstraps: it needs a container runtime and kubelet already installed, and you install a CNI plugin yourself afterwards.

Install runtime, kubelet, kubeadm
↓ `kubeadm init`
Control plane static pods, admin.conf
↓ apply a CNI
Network nodes become Ready
↓ `kubeadm join`
Workers kubelet joins

BOOTSTRAP A CLUSTER

`kubeadm init`
Initialise a control-plane node

`kubeadm init --pod-network-cidr=`*`<cidr>`*
Reserve the pod IP range for a CNI

`kubeadm init --apiserver-advertise-address=`*`<ip>`*
Choose the API server IP

`kubeadm init --control-plane-endpoint=`*`<dns>`***`:6443`**
Stable endpoint for HA control plane

`kubeadm init --config `*`<file>`*
Init from a config file

`mkdir -p $HOME/.kube && sudo cp /etc/kubernetes/admin.conf $HOME/.kube/config`
Let kubectl talk to the cluster

JOIN NODES

`kubeadm join `*`<host>`***`:6443 --token `***`<token>`*** `--discovery-token-ca-cert-hash sha256:`***`<hash>`***
Join a worker node

`kubeadm join `*`<host>`***`:6443 ... --control-plane --certificate-key `***`<key>`***
Join as a control-plane node

TOKENS

`kubeadm token create --print-join-command`
New token plus full join command

`kubeadm token list`
List bootstrap tokens

`openssl x509 -pubkey -in /etc/kubernetes/pki/ca.crt | openssl rsa -pubin -outform der 2>/dev/null | openssl dgst -sha256 -hex | sed 's/^.* //'`
Compute the CA cert hash

CERTIFICATES

`kubeadm certs check-expiration`
Show expiry of all certs

`kubeadm certs renew all`
Renew every certificate

UPGRADE

`kubeadm upgrade plan`
Show available versions and checks

`kubeadm upgrade apply v`*`<version>`*
Upgrade the first control plane

`kubeadm upgrade node`
Upgrade other nodes' local config

`kubectl drain `*`<node>`*** `--ignore-daemonsets`**
Evict pods before upgrading kubelet

`kubectl uncordon `*`<node>`*
Make the node schedulable again

CONFIG AND IMAGES

`kubeadm config print init-defaults`
Print the default init config

RESET

`kubeadm reset`
Revert init or join on this node

reset leaves CNI config, iptables rules and $HOME/.kube behind; clean them by hand before re-initialising.