While you’re waiting...

http://bit.ly/srecon-cake0
Kubernetes From
A Cake Mix

Liz Frost
Who am I?

Liz Frost

Twitter: @stillinbeta

slack.k8s.io: @liz
Who am I?
Who am I?
Who am I?

It’s pronounced “kube-cuddle”
Why should you listen to me?

- sig-cluster-lifecycle member
- kubernetes contributor
- kubeadm developer
What is Kubernetes?
Node

Pod

Pod

Pod

Node

Pod

Pod

Pod

User

@stillinbeta // #SREcon Americas 2019
Conformance Tests → Kubernetes API → Certified Kubernetes
Conformance Tests → Kubernetes API → certified kubernetes
We got Opinions
Kubeadm™ brand Kubernetes
kubeadm init
$ kubeadm init --help
Run this command in order to set up the Kubernetes master.

The "init" command executes the following phases:

```
preflight                  Run master pre-flight checks
kubelet-start              Writes kubelet settings and (re)starts the kubelet
certs                      Certificate generation
  /etcld-ca                   Generates the self-signed CA to provision identities for etcd
  /etcld-server               Generates the certificate for serving etcd
  /etcld-healthcheck-client   Generates the client certificate for liveness probes to healthcheck etcd
  /apiserver-etcd-client      Generates the client apiserver uses to access etcd
  /etcld-peer                 Generates the credentials for etcd nodes to communicate with each other
  /ca                        Generates the self-signed Kubernetes CA to provision identities for other Kubernetes components
  /apiserver                 Generates the certificate for serving the Kubernetes API
  /apiserver-kubelet-client   Generates the client certificate for the API server to connect to kubelet
  /front-proxy-ca             Generates the self-signed CA to provision identities for front proxy
  /front-proxy-client         Generates the client for the front proxy
  /sa                        Generates a private key for signing service account tokens along with its public key
kubeconfig                 Generates all kubeconfig files necessary to establish the control plane and the admin kubeconfig file
  /admin                     Generates a kubeconfig file for the admin to use and for kubeadm itself
  /kubelet                   Generates a kubeconfig file for the kubelet to use *only* for cluster bootstrapping purposes
  /controller-manager        Generates a kubeconfig file for the controller manager to use
  /scheduler                 Generates a kubeconfig file for the scheduler to use
control-plane              Generates all static Pod manifest files necessary to establish the control plane
  /apiserver                 Generates the kube-apiserver static Pod manifest
  /controller-manager        Generates the kube-controller-manager static Pod manifest
  /scheduler                 Generates the kube-scheduler static Pod manifest
  /etcd                      Generates static Pod manifest file for local etcd.
  /local                     Generates the static Pod manifest file for a local, single-node local etcd instance.
upload-config              Uploads the kubeadm and kubelet configuration to a ConfigMap
  /kubeadm                   Uploads the kubeadm ClusterConfiguration to a ConfigMap
  /kubelet                   Uploads the kubelet component config to a ConfigMap
mark-control-plane         Mark a node as a control-plane
addon                      Installs required addons for passing Conformance tests
  /coredns                   Installs the CoreDNS addon to a Kubernetes cluster
  /kube-proxy                Installs the kube-proxy addon to a Kubernetes cluster
```
$ kubeadm init --help
Run this command in order to set up the Kubernetes master.

The "init" command executes the following phases:

```bash
preflight                  Run master pre-flight checks
kubelet-start              Writes kubelet settings and (re)starts the kubelet
certs                      Certificate generation
certificates               Generates all kubeconfig files necessary
coredns                    Installs the CoreDNS addon to a Kubernetes cluster
kubeconfig                 Generates all kubeconfig files necessary to establish the
                           kube-apiserver static Pod manifest
control-plane              Generates all static Pod manifest files necessary to establish the
                           kube-controller-manager static Pod manifest
/apiserver                 Generates the kube-apiserver static Pod manifest
/controller-manager         Generates the kube-scheduler static Pod manifest
/scheduler                 Generates static Pod manifest file for local etcd.
/create-etcd                Generates the static Pod manifest file for a local etcd instance.
upload-config              Uploads the kubeadm and kubelet configuration to a ConfigMap
/kubeadm                   Uploads the kubeadm ClusterConfiguration to a ConfigMap
/kubelet                    Uploads the kubelet component config to a ConfigMap
mark-control-plane         Mark a node as a control-plane
bootstrap-token            Generates bootstrap tokens used to join a node to a cluster
addon                      Installs required addons for passing Conformance tests
/coredns                   Installs the CoreDNS addon to a Kubernetes cluster
/kube-proxy                 Installs the kube-proxy addon to a Kubernetes cluster
```
preflight
kubelet-start
certs
cubeconfig
control-plane
  /apiserver
  /controller-manager
  /scheduler
etcfd
  /local
upload-config
  /kubeadm
  /kubelet
mark-control-plane
bootstrap-token
addon
  /coredns
  /kube-proxy
What are we making?

- kubelet
- etcd
- kube-apiserver
- kube-controller-manager
- kube-scheduler
kubelet ➔ docker ➔
  - etcd
  - kube-apiserver
  - kube-scheduler
  - kube-controller-manager

Node (VM / physical Machine)

@stillinbeta // #SREcon Americas 2019
kubelet
What will we need locally?

- kubelet
- kubeadm
- docker
kubelet connects to API server...

...but the API server is run by the kubelet
Kubelet boot

- Start static pods
- Try to connect to API server
Kubelet boot

Start static pods → Try to connect to API server
Kubelet boot

Start static pods
Tutorial 1!

http://bit.ly/srecon-cake1
kubeadm

REMOVE BEFORE FLIGHT
Preflight Checks

- Avoid common problems
- Handy guard-rails
- Ignore at your own peril!
Tutorial 2!

From the Website

- Simple: well-defined, user-facing API (gRPC)
- Secure: automatic TLS with optional client cert authentication
- Fast: benchmarked 10,000 writes/sec
- Reliable: properly distributed using Raft
What you care about

- Key/value store
- *Optionally* distributed
- Only stateful part of kubernetes
- Secured by client certificates
Where do we put it?

- External?
- HA?
- Self-Hosted
- Single Node
Setting up etcd

1. Generate Certificates
2. Create Pod Manifest
3. Run Healthcheck
Tutorial 3!

The centre of everything
kube-apiserver
kube-apiserver

- Exclusive control of etcd
- Handles all access control
- Stores some (but not all!) APIs
- Proxies everything
API Groups?

GET /apis/apps/v1/namespaces/default/deployments/myapp
Custom Resource Definitions

User (kubectl, curl) → kube-apiserver → CRD controller

- API Request
- MyCRD Response
- MyCRD Watch Notification
kubectl exec

User (kubectl, curl)  kube-apiserver  Running Pod

Command

Command Output

Command

Command output

@stillinbeta // #SREcon Americas 2019
Tutorial 4!

kube-controller-manager
...that could mean anything
Controller

State Changes

Desired State

Reactions
Pod Created / Destroyed

List of ReplicaSets

ReplicaSetController

Create / Destroy Pods

@stillinbeta // #SREcon Americas 2019
kube-controller-manager

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller goroutine

Controller gorouting
Tutorial 5!

Scheduler
kube-scheduler

Pods → kube-scheduler → Nodes

Assignments
I need a GPU

I'm out of disk

I can't be on Node17

I'm running Solaris

I want to be in us-east-1c

I'm in Europe
I prefer Europe

I prefer not to run on the same node as pod17
Bin Packing
Tutorial 6!

What would be next?

- DNS
- Container Networking
- Proxying
- Multiple Nodes
Your Cluster is *Not*: 

- Secure
- Production-Ready
- Resilient
- High-Availability
- Certified Kubernetes
But it is *yours*. 
Questions? Concerns?
Come find me! I’m the one with pink hair!

Twitter: @stillinbeta
slack.k8s.io: @liz
Github: github.com/stillinbeta