What’s New in K8s 1.3

Carter Morgan
@_askcarter
Background: 3 Hurdles
The App

How do I write scalable apps?

How do I package and distribute?

What runtimes am I locked into?
The Infra

Can I scale?

Is it automatic?

Am I locked in?
The Wild

Where are my machines?

How do I update?
Kubernetes

Open Source Container Automation Framework

- Open API
- Based on Google’s experiences
3 Claims

Planet Scale
Designed on the same principles that allows Google to run billions of containers a week, Kubernetes can scale without increasing your ops team.

Never Outgrow
Whether testing locally or running a global enterprise, Kubernetes flexibility grows with you to deliver your applications consistently and easily no matter how complex your need is.

Run Anywhere
Kubernetes is open source giving you the freedom to take advantage of on-premise, hybrid, or public cloud infrastructure, letting you effortlessly move workloads to where it matters to you.
How does k8s hold up?
Kubernetes

Pre 1.3

(already had a lot)

Horizontal Scaling
Automated Rollbacks
Container Scheduling
Resource Quotas and Limits
Self-healing
Service Discovery and Load Balancing
Secret and Configuration Management
Daemon Sets
Secrets and Config Maps
Deployments
Monolith

Microservices

@_askcarter
Container Based

Photo © ptnimages via Canva.com
@_askcarter
Pods
Logical Application
• One or more containers and volumes
• Shared namespaces
• One IP per pod

Pod

10.1.0.100

nginx
monolith

GCE iSCSI NFS

@_askcarter
Labels

Arbitrary metadata attached to any API object

• Queryable by Selectors
• How Kubernetes does grouping

Pod

labels:
version: v1
track: stable

Pod

labels:
version: v1
track: test

@_askcarter
Labels

selector: version=v1
Labels

selector: track=stable
Services
Persistent IPs for Pods
• Uses Labels to Target Pods
• Internal or External IPs
Deployments

Drive current state towards desired state

@_askcarter
Deployments

Drive current state towards desired state

app: hello
replicas: 2

Node 1
Pod
hello

Node 2
Pod
hello
Deployments
Drive current state towards desired state

app: hello
replicas: 2

Node 1
Pod
hello

Node 2

@_askcarter
Deployments
Drive current state towards desired state

app: hello
replicas: 2

Node 1
Pod: hello
Pod: hello

Node 2
Rolling Update

@_askcarter
Rolling Update

@_askcarter
Rolling Update
Rolling Update
Rolling Update
Rolling Update

@_askcarter
Rolling Update
Rolling Update

@_askcarter
Rolling Update

Node 1

Pod

hello

Node

Pod

goodbye

Node

Pod

goodbye

Node

Pod

goodbye

@_askcarter
Rolling Update

Node 1
Pod goodbye
Pod hello
Node 2
Pod goodbye
Pod hello
Node 3
Pod goodbye

Service
Rolling Update
Rolling Update

Node 1

Node

Pod

Pod
goodbye

Pod
goodbye

Node

Node

Pod
goodbye

Service

@_askcarter
3 Claims: revisited

Planet Scale
Designed on the same principles that allows Google to run billions of containers a week, Kubernetes can scale without increasing your ops team.

Never Outgrow
Whether testing locally or running a global enterprise, Kubernetes flexibility grows with you to deliver your applications consistently and easily no matter how complex your need is.

Run Anywhere
Kubernetes is open source giving you the freedom to take advantage of on-premise, hybrid, or public cloud infrastructure, letting you effortlessly move workloads to where it matters to you.
Kubernetes 1.3

Highlights

- Authorization:
  - Alpha RBAC authorization API group
- Federation
  - federation api group is now beta
  - Services from all federated clusters are now registered in Cloud DNS (AWS and GCP).
- Stateful Apps:
  - alpha PetSets manage stateful apps
  - alpha Init containers provide one-time setup for stateful containers
- Updating:
  - Retry Pod/RC updates in kubectl rolling-update.
  - Stop "kubectl drain" deleting pods with local storage.
  - Add kubectl rollout status
- Security/Auth
  - L7 LB controller and disk attach controllers run on master, so nodes do not need those privileges.
  - Setting TLS1.2 minimum
  - kubectl create secret tls command
  - Webhook Token Authenticator
  - beta PodSecurityPolicy objects limits use of security-sensitive features by pods.
- Kubecf!
  - Display line number on JSON errors
  - Add flag -t as shorthand for --tty
- Resources
  - alpha: NVIDIA GPU support (#24836, @therec)
  - Adding loadBalancer services and nodeports services to quota system

Joseph Jacks @asynchio · Jul 2

@KubernetesIO 1.3.0 is out with *lots* of new goodies!
github.com/kubernetes/kub...
Kubernetes 1.3
Kubernetes 1.3

- Init containers (alpha)
- Fixed PDs
- Cluster Federation (alpha)
- Optional HTTP2
- Pod Level QoS Policy
- Tls secrets
- kubectl set command
- UI
- Jobs
- RBAC (alpha, experimental)
- Garbage Collector (alpha)
- Pet Sets
- rkt Container runtime
- Network policies
  (and more)
Cluster Federation

Manage clusters across region and providers
Jobs

Pods *expected* to terminate

Creates 1...n Pods and ensures that a certain number of them run to completion

3 types: non-parallel, fixed count parallel, and parallel with a work queue
Job: Work Queue with Pod Per Work Item

```yaml
apiVersion: batch/v1
kind: Job
metadata:
  name: job-wq-1
spec:
  completions: 8
  parallelism: 2
  template:
    metadata:
      name: job-wq-1
    spec:
      containers:
        - name: c
          image: gcr.io/<project>/job-wq-1
      restartPolicy: OnFailure
```
Init Containers

Sequential Pod Initialization
Init Container: register pod to external service

```yaml
pod:
  spec:
    initContainers:
      - name: register
        image: centos:centos7
        command:
          - "/bin/sh"
          - "-c"
          - "curl -X POST http://$ADDR/register -d \"instance=${POD_NAME}&ip=${POD_IP}\""
        env:
          - name: POD_NAME
            valueFrom:
              field: metadata.name
          - name: POD_IP
            valueFrom:
              field: status.podIP
    containers:
      - name: run
        image: application-image
        command: ["/my_application_that_depends_on_myservice"]
```
Init Container: clone a git repo into a volume

```yaml
pod:
  spec:
    initContainers:
      - name: download
        image: image-with-git
        volumeMounts:
          - mountPath: /var/lib/data
            volumeName: git
    containers:
      - name: run
        image: centos:centos7
        command: ["/var/lib/data(binary)"
        volumeMounts:
          - mountPath: /var/lib/data
            volumeName: git
    volumes:
      - emptyDir: {}
Pet Sets

Pods with ego

Pods are fungible, stateless?

Pets are Pods with:
1. Stable hostname
2. A unique name
3. Stable storage
Pet Sets

Pods with ego
PetSet: example manifest

```yaml
apiVersion: apps/v1alpha1
kind: PetSet
metadata
  name: web
spec:
  serviceName: "nginx"
  replicas: 2
  template:
    metadata:
      labels:
        app: nginx
      annotations:
        pod.alpha.kubernetes.io/initialized: "true"
      spec:
        terminationGracePeriodSeconds: 0
        containers:
        - name: nginx
          image: gcr.io/google_containers/nginx-slim:0.7
          ports:
            - containerPort: 80
              name: web
            - name: nginx
              args: ["-g", "daemon off;"]
          volumeMounts:
            - name: www
              mountPath: /usr/share/nginx/html
          volumeClaimTemplates:
            - metadata:
                annotations:
                  volume.alpha.kubernetes.io/storage-class: anything
              spec:
                accessModes:
                - ReadWriteOnce
                resources:
                  requests:
                    storage: 1Gi
```
PetSet: headless service

```yaml
# A headless service to create DNS records
apiVersion: v1
kind: Service
metadata:
  name: nginx
  labels:
    app: nginx
spec:
  ports:
    - port: 80
      name: web
  clusterIP: None
  selector:
    app: nginx
```
Bonus
Google Container Engine (GKE)

- Cluster autoscaling (beta)
- IAM support
- Local SSD
- Container-VM Images (beta)
- Node pools
$ minikube start
Starting local Kubernetes cluster...
Running pre-create checks...
Creating machine...
Starting local Kubernetes cluster...

$ kubectl run hello-minikube --image=gcr.io/google_containers
deployment "hello-minikube" created
$ curl http://$(minikube ip):8000
CLIENT VALUES:
client_address=192.168.99.1
command=GET
real path=/
...
$ minikube stop
Stopping local Kubernetes cluster...
Stopping "minikubeVM"...

Ray Tsang @saturnism · Jun 28
easy local #kubernetes installation w/ minikube #devnation @aronchick
github.com/kubernetes/minikube
Kube UI

kubernetes.io/docs/user-guide/ui/
$ kubectl explain deployment.spec.minReadySeconds

FIELD: minReadySeconds <integer>

DESCRIPTION:
  Minimum number of seconds for which a newly created pod should be ready without any of its container crashing, for it to be considered available. Defaults to 0 (pod will be considered available as soon as it is ready)
Recap
3 Hurdles

The App
The Infra
The Wild
3 Claims

Planet Scale
Never Outgrow
Run Anywhere
Kubernetes 1.3

- Planet Scale - SLA 2000 nodes
- Never Outgrow - minikube to prod
- Run Anywhere - Cluster Federation
Scalable Microservice with Kubernetes
Learn more here!

Carter Morgan
@_askcarter