Bootstrapping HA Kubernetes Cluster on AWS using KOPS

Kubernetes Pune Meetup 102 | 19 August 2017 | Jakir Patel

Agenda

Kubernetes and its growth

Available Solutions for creating Kubernetes cluster

KOPS Introduction

Get Started with KOPS

KOPS CLI

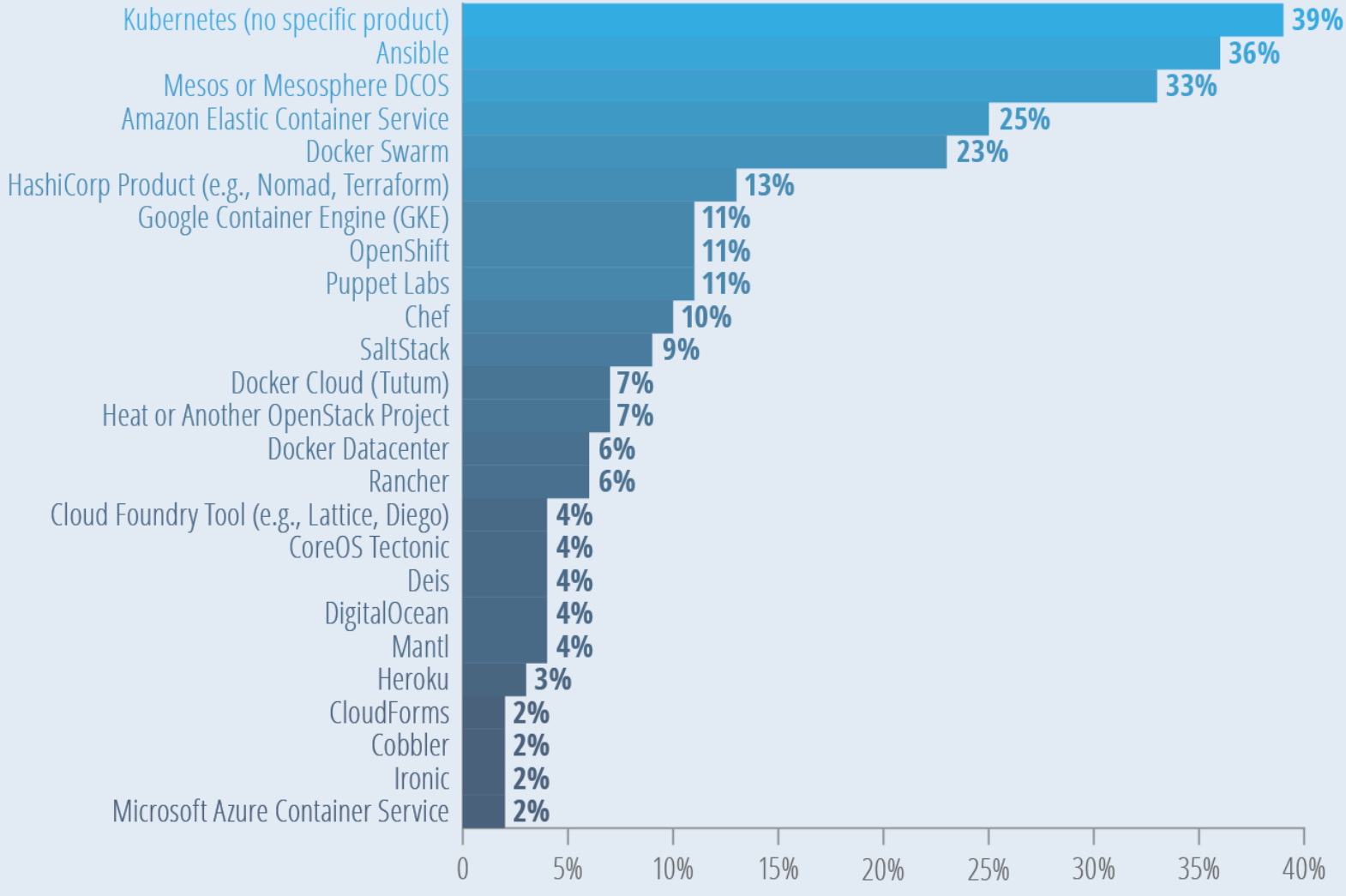
\

Networking, Security and Higher Availability with KOPS

Kubernetes is one of the most adopted tool in container orchestration.

The New Stack Survey

Top Orchestration Products Based on Expected Usage Within Next Year



Source: The New Stack Survey, March 2016. Within the next year, what are the top three products or services you expect to utilize to manage or orchestrate containers? n=114.

THENEWSTACK

How to bootstrap Kubernetes Cluster?

Available Solutions

Independent Solutions:
1. Minikube
2. Kubeadm

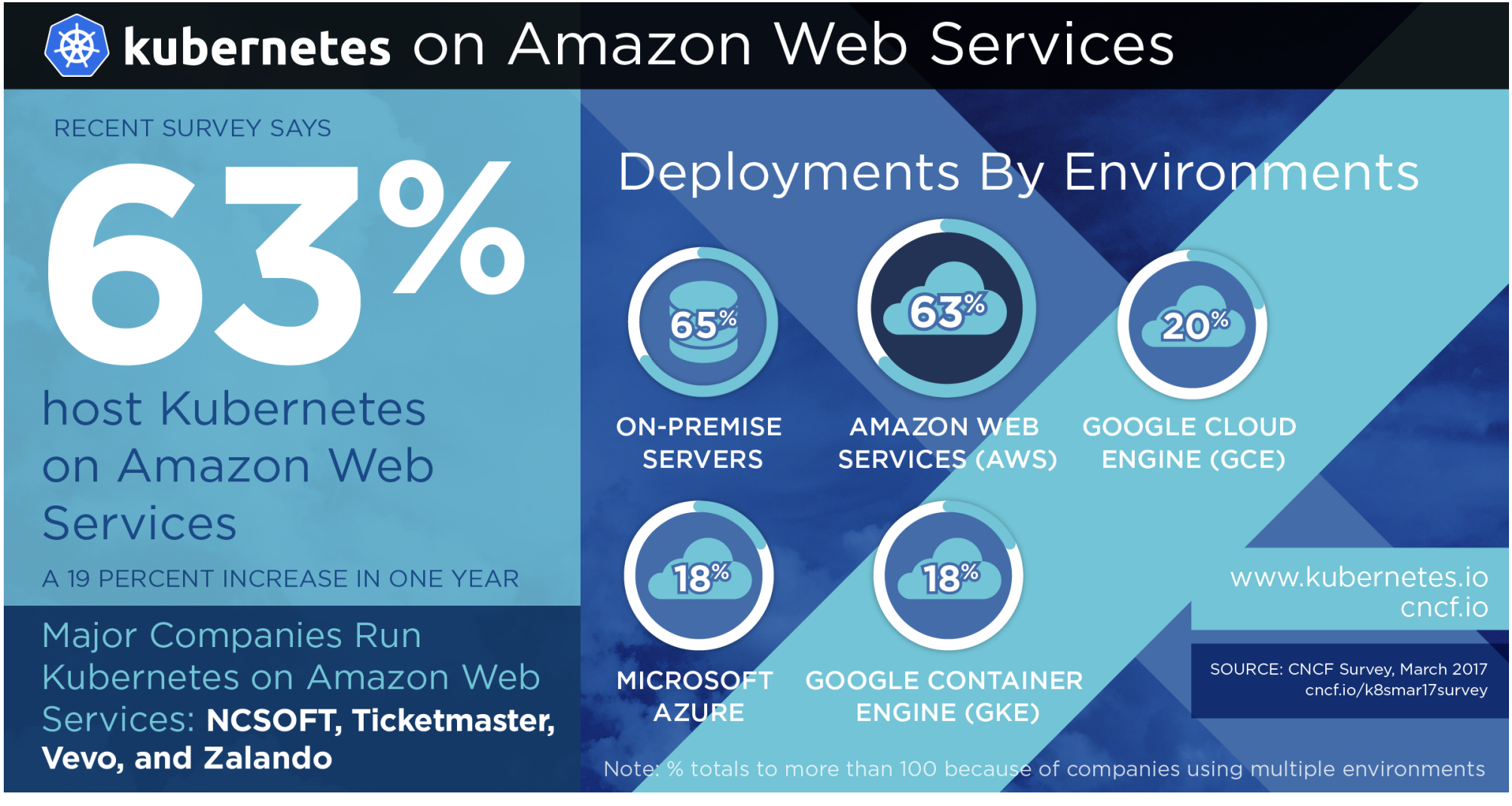
Hosted Solutions:
1. Google Container Engine
2. Azure Container Service
3. IBM Bluemix Container Service

Custom Solutions:
1. Kubernetes Operations (KOPS) for AWS
2.Kubespray formerly Kargo

And Much More.

Kubernetes Operations (KOPS)

Kubernetes and AWS



KOPS

Tool to deploy highly available, production-grade Kubernetes cluster.

AWS is officially supported.

GCP and **VSphere** are in the initial support.

Generates **Terraform** and **Cloudformation** configuration files.

Supports custom Kubernetes Addons:

1. **Dashboard**
2. **Monitoring with Heapster**
3. **RBAC (Role Based Access Control)**

Maintained and supported by **CNCF** community.

Get Started

Kubectl: Install the latest stable version of Kubectl.

KOPS: Install the latest stable version of KOPS (Kubernetes Operations)

Install Via:

https://github.com/kubernetes/kops/blob/master/docs/install.md

Setting up Environment

AWS **Secret Key** and **Access Key** with following IAM roles:

AmazonEC2FullAccess
AmazonRoute53FullAccess
AmazonS3FullAccess
IAMFullAccess
AmazonVPCFullAccess

DNS Configuration

State Store for KOPS

DNS Configuration

Optional for **KOPS 1.6.2 <**

Gossip based cluster (KOPS 1.6.2 <):
Cluster name end with **.k8s.local**

Domain Name Scenarios:

1. Domain purchased/hosted on AWS

2. Subdomain under domain purchased/hosted on AWS

3.Domain purchased on another registrar

4. Subdomain under domain purchased on another registrar

Private DNS and State Store

Private / Public DNS: Available in KOPS 1.5 +

Private DNS of AWS used with:
--dns flag

KOPS stores the state of the cluster with AWS S3.

Uses **KOPS_STATE_STORE** environment variable.

KOPS CLI

kops create cluster <clustername>
Create the cloud specifications but not the actual resources. To create actual resources pass --**yes** flag.
kops create cluster <clustername> --yes

kops update cluster <clustername>
Creates or updates the cloud resources to match the cluster spec.
kops update cluster <clustername> --yes

kops delete cluster <clustername>
Delete the resources of the cluster also the cloud specification
kops delete cluster <clustername> --yes

Modes in KOPS CLI

--target: Gives the terraform / cloud formation manifest.
Example: --target=terraform

--kubernetes-version: Specific K8S version
Example: --kubernetes-version=1.6.0

--zones and --master-zones: Launch master and nodes in multi AZ environment
Example: --zones=us-east-1b,us-east-1c

--node-size and --master-size: Specify the type of instances wrt AWS.
Example: --master-size=m4.large

--dns-zone: Change default DNS Zone
Example: --dns-zone=<my.hosted.zone>

Whats more important for Production grade Kubernetes Cluster?

1. Networking
2. Security
3. Higher Availability

Security in KOPS

Limit **AdminAccess** from public to specific IP's

Limit**IAMRole** Policies for Pods

Turn Off **AnonymousAuth** for Kubelet API

Using secrets for **API Bearer Token** and **Admin Access**

Networking in KOPS

Kubenet: Default, limited with AWS 50 Nodes.
Native with CNI Plugin.

CNI: Container Network Interface

1. Weave
2. Flannel
3. Calico
4. Canal (Flannel + Calico)

Requires: --topology=private , --networking=<CNI-networking>

Classic: Native in a process.

External: Custom. With **daemonsets**.

HA with KOPS

Multi-AZ Master Nodes

Multi-AZ Nodes

Multi-master cluster（Odd number)

Cluster of etcd

Federation with KOPS

Some Best Practices with KOPS

Versioning the S3 Bucket

Using preview mode for KOPS CLI

Using KOPS IAM user

Using Bastion Host

Get Involved.

Tweet about your experience with Kubernetes Pune- @kubernetespune

Post questions (or answer questions) on Stack Overflow

Join the community portal for advocates on K8sPort

Follow us on Twitter @Kubernetesio for latest updates

Connect with the community on Slack
Share your Kubernetes story.

Thank you.

Please don't hesitate to contact us if
you have any questions

jakirpatel@outlook.com