Red Hat CoE in PaaS

About The Course

Red Hat Certificate of Expertise in Platform-as-a-Service

About the Course

Red Hat CoE in PaaS

Certificate of Expertise Rebranding

Red Hat CoE in PaaS

Certificate of Expertise Rebranding

Certificate of Expertise Rebranding

Effective December 1, 2017, all Red Hat Certificates of Expertise will be rebranded as Red Hat Certified Specialist. For example, the Red Hat Certificate of Expertise in Deployment and Systems Management will become Red Hat Certified Specialist in Deployment and Systems Management."

Certificate of Expertise Rebranding

Effective December 1, 2017, all Red Hat Certificates of Expertise will be rebranded as Red Hat Certified Specialist. For example, the Red Hat Certificate of Expertise in Deployment and Systems Management will become Red Hat Certified Specialist in Deployment and Systems Management."

Red Hat CoE in PaaS

OpenShift Overview

Why Containers Are Awesome – pt. 1

Why Containers Are Awesome – pt. 2

OpenShift Overview

What Is OpenShift?

- Enterprise Kubernetes + Docker
- Source code management
- Image management and promotion
- Application management at scale
- Team and user tracking
- Cluster networking infrastructure
- REST APIs
- Controllers

OpenShift Overview

Main Features

- Self-service platform
- Polyglot, multi-lingual support
- Automation
- User Interfaces
- Scalability
- Container portability
- Choice of platform
- Open source

OpenShift Overview

K8s

kubernetes

OpenShift Overview

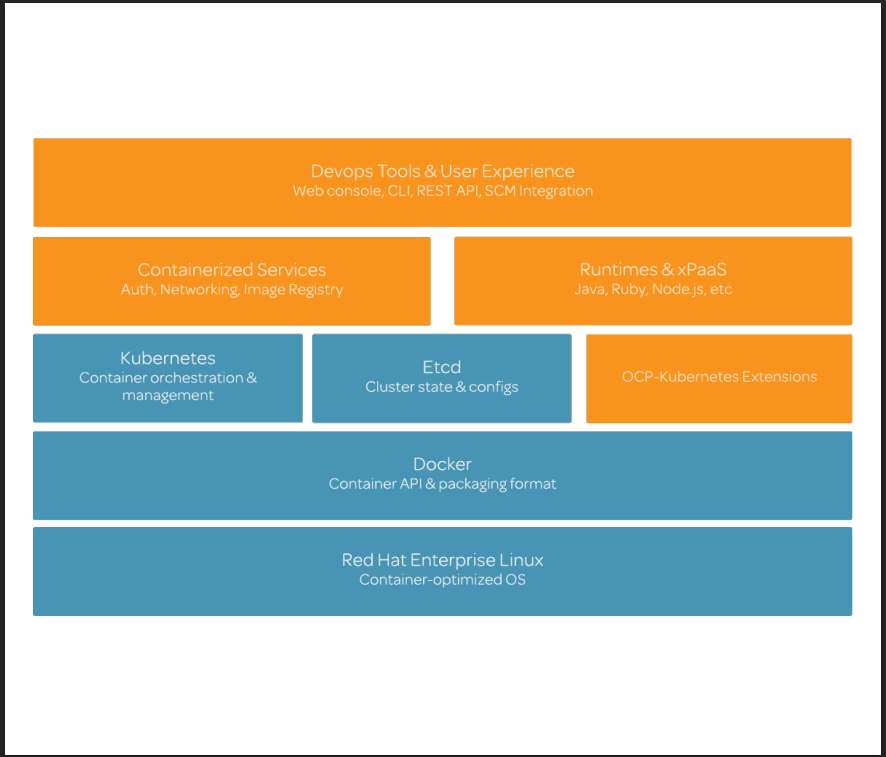
Core Concepts

- Containers and images
- Pods and services
- Projects and users
- Builds and image streams
- Deployments
- Routes
- Templates

Why Use OpenShift?

OpenShift Overview

- Source code management, builds, and deployments for developers
- Managing and promoting images at scale
- Application management at scale
- Team and user tracking
- Networking infrastructure



Red Hat CoE in PaaS

OpenShift Overview

Why Containers Are Awesome – pt. 1

Why Containers Are Awesome – pt. 2

OpenShift Overview

What Is OpenShift?

- Enterprise Kubernetes + Docker
- Source code management
- Image management and promotion
- Application management at scale
- Team and user tracking
- Cluster networking infrastructure
- REST APIs
- Controllers

OpenShift Overview

Main Features

- Self-service platform
- Polyglot, multi-lingual support
- Automation
- User Interfaces
- Scalability
- Container portability
- Choice of platform
- Open source

OpenShift Overview

K8s

kubernetes

OpenShift Overview

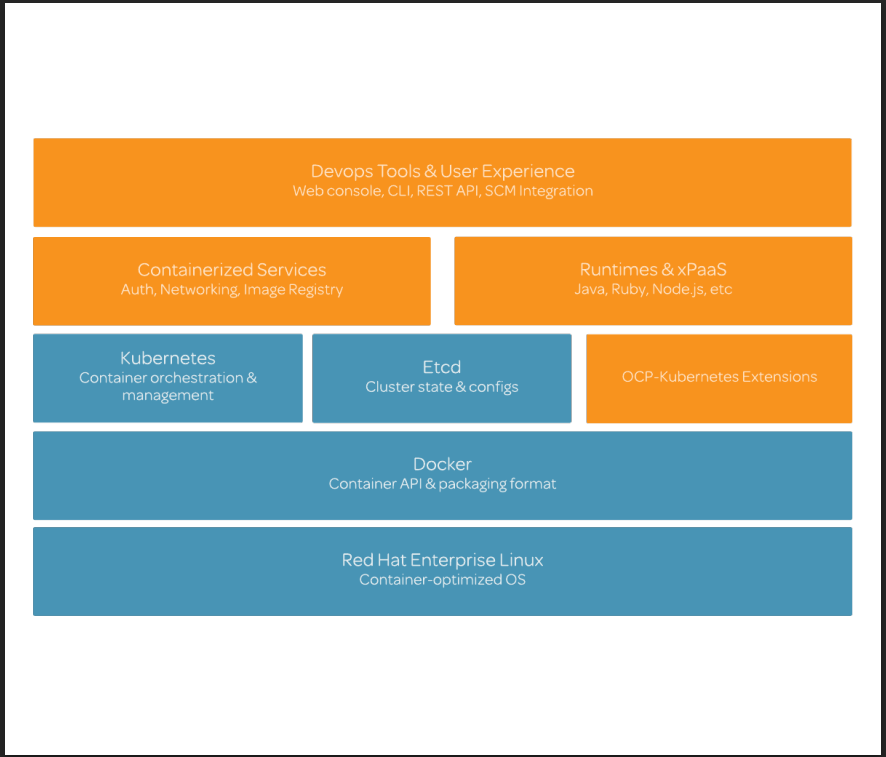
Core Concepts

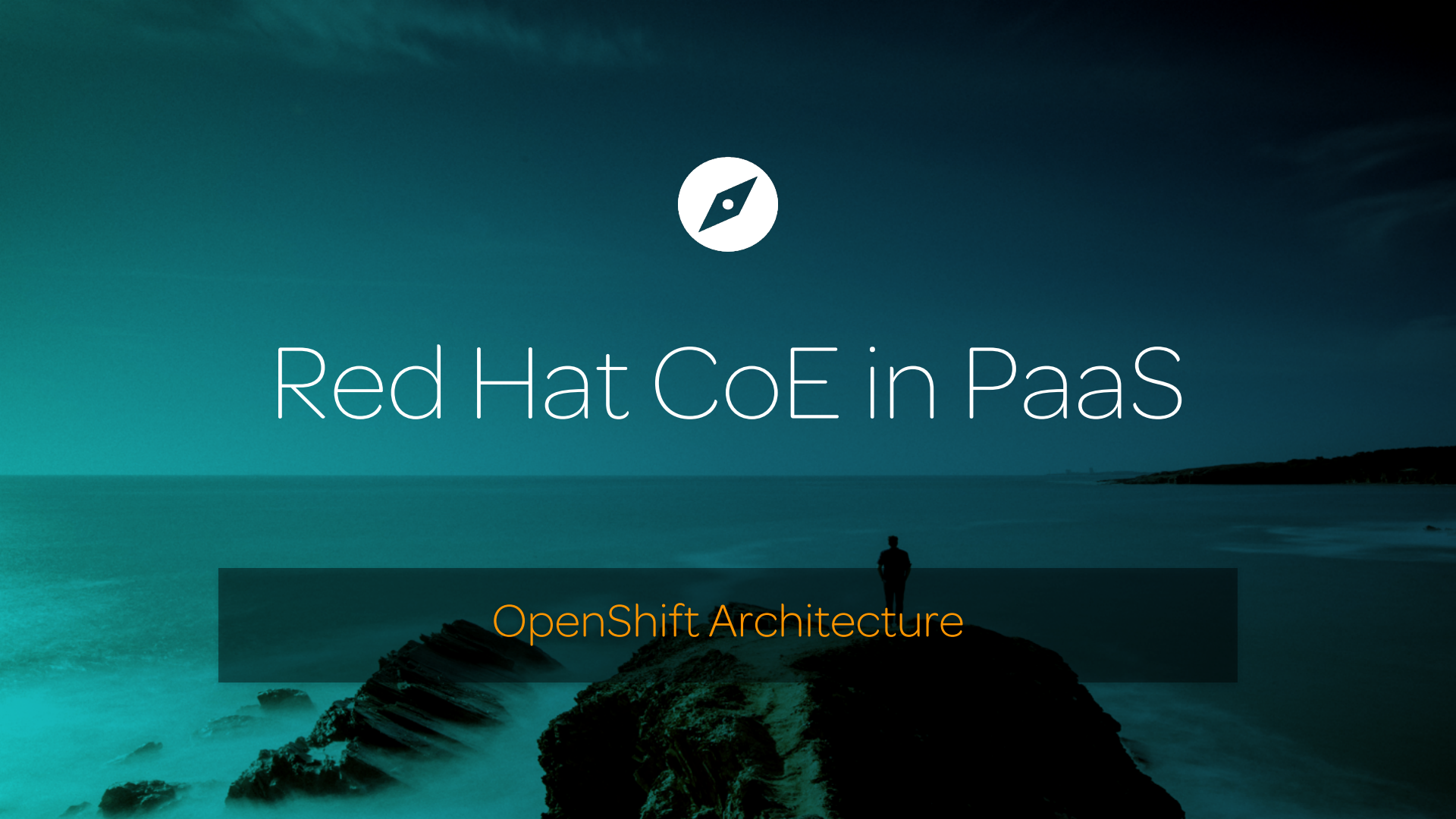
- Containers and images
- Pods and services
- Projects and users
- Builds and image streams
- Deployments
- Routes
- Templates

Why Use OpenShift?

OpenShift Overview

- Source code management, builds, and deployments for developers
- Managing and promoting images at scale
- Application management at scale
- Team and user tracking
- Networking infrastructure





Red Hat CoE in PaaS

OpenShift Architecture

OpenShift Architecture

OCP Masters

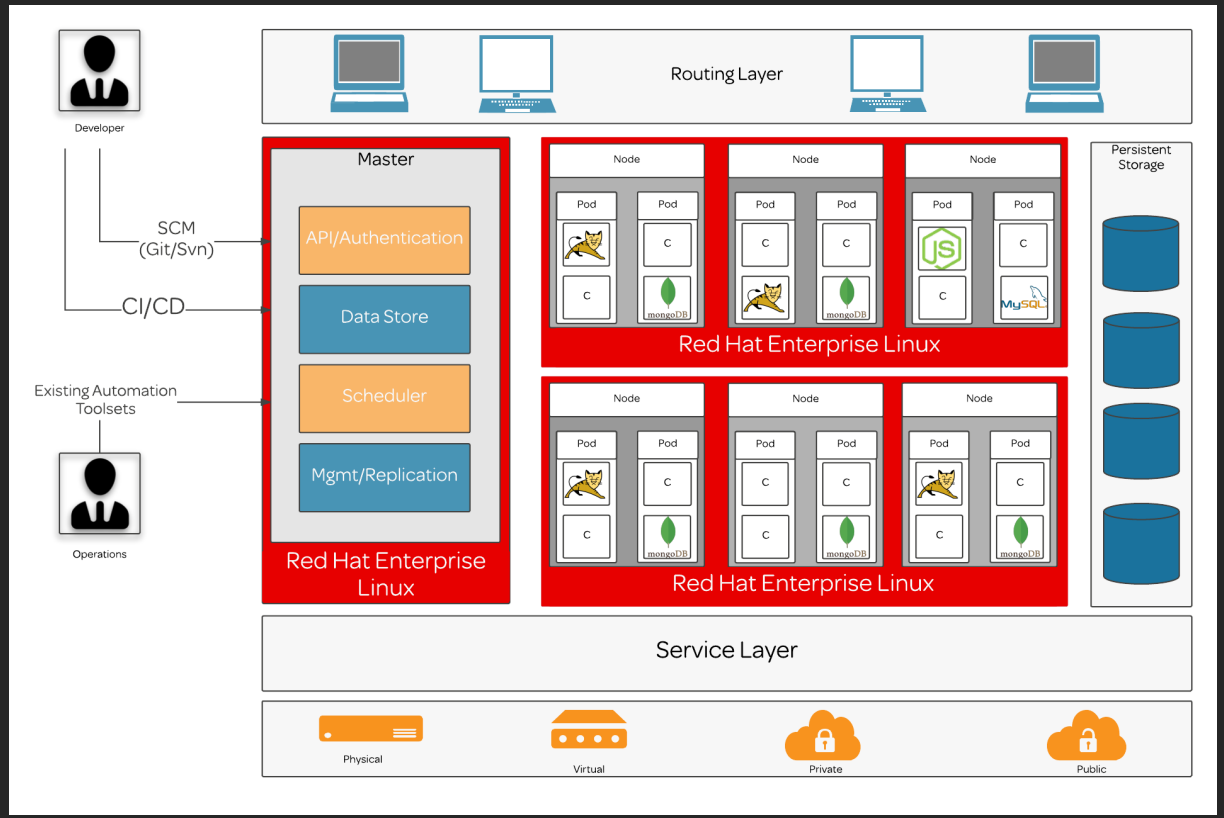
- API Server
- etcd
- Controller manager server
- HAProxy

OpenShift Architecture

Nodes

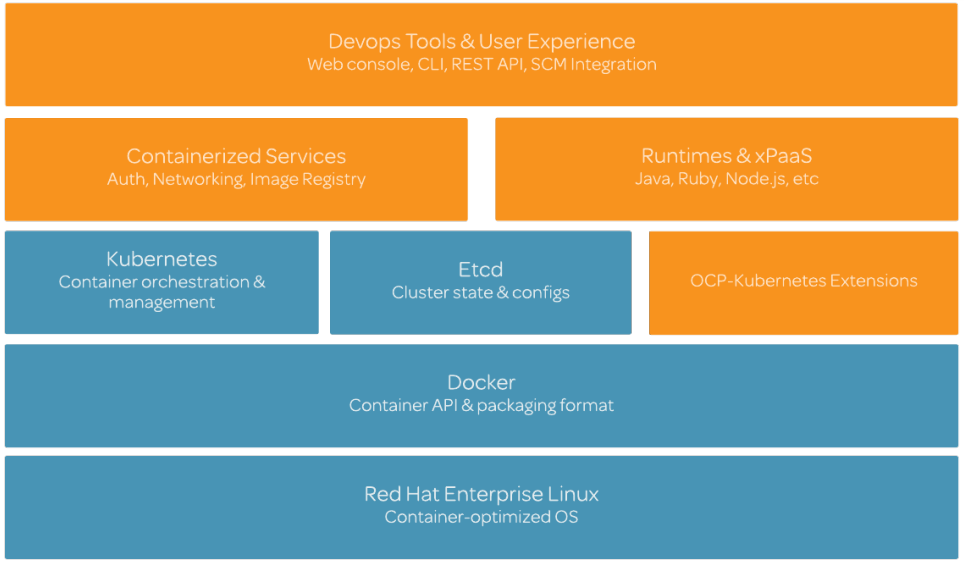
- Runtime environments
- Docker service
- Kubelet
- Service proxy

OpenShift Cluster Architecture



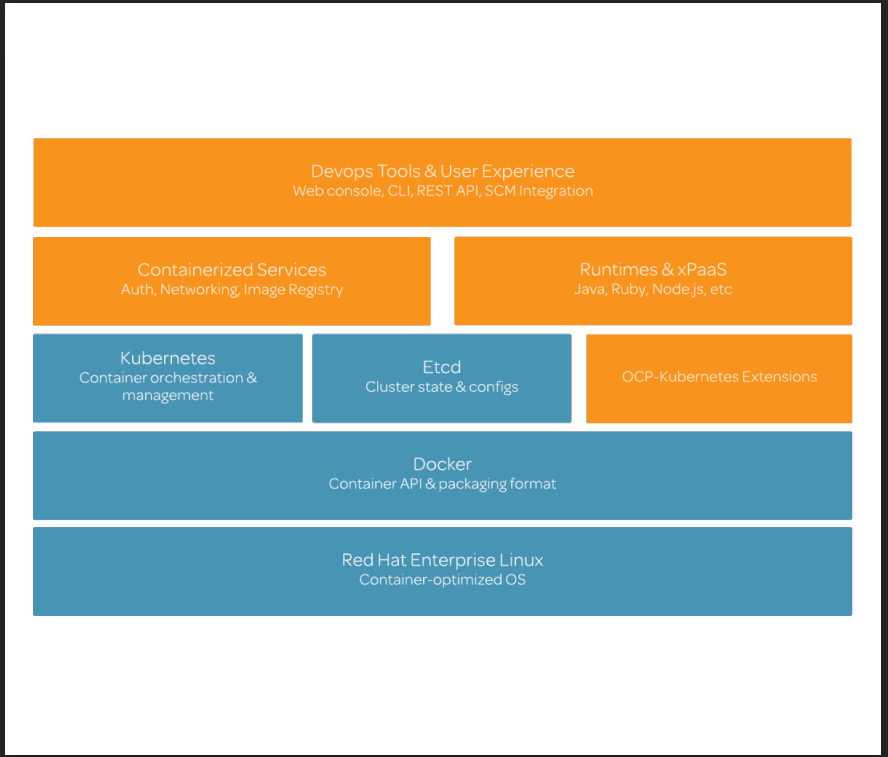
OpenShift Container Platform

Architecture



OpenShift Architecture

- OCP-Kubernetes Extensions
- Containerized Services
- Runtimes and xPaaS
- DevOps Tools and User Experience (UX)



OpenShift Container Registry

- Docker Hub
- Private Registries
- /registry/hosts/$(hostname -f)
- Listening for HTTP

Red Hat CoE in PaaS

Dnsmasq

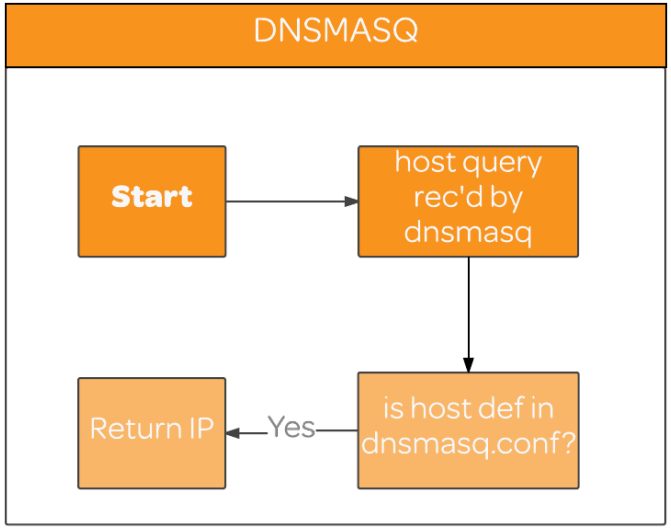
Red Hat Certificate of Expertise in Platform-as-a-Service

About Dnsmasq

- DNS
- TFTP
- PXE
- Router advertisement
- DHCP
- Static address assignments
- Multiple networks

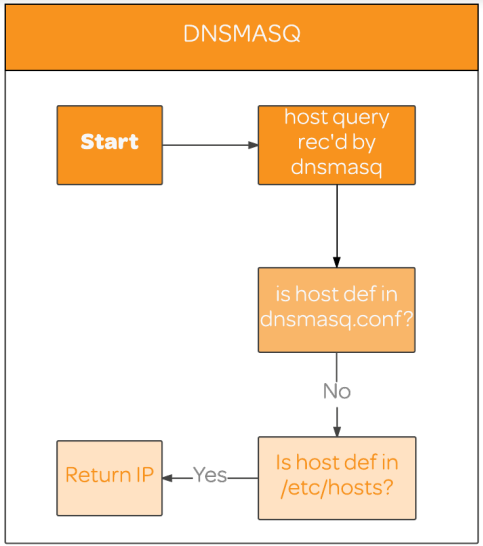
Red Hat Certificate of Expertise in Platform-as-a-Service

Dnsmasq

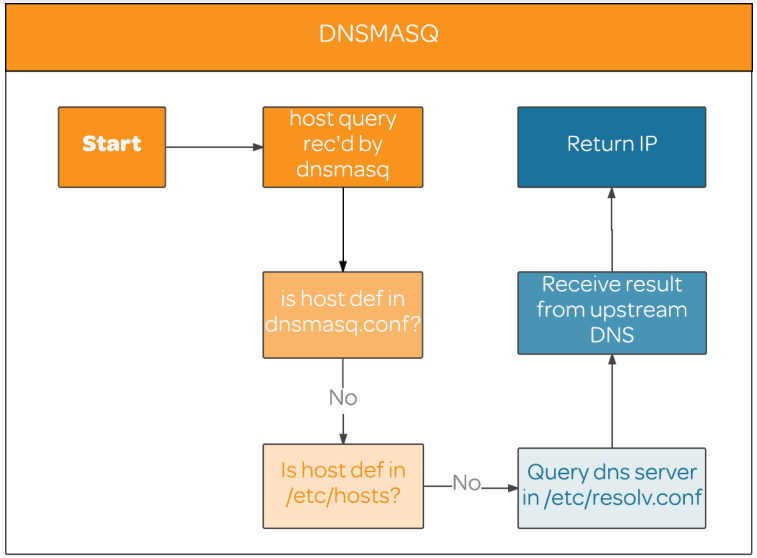


Red Hat Certificate of Expertise in Platform-as-a-Service

Dnsmasq



Dnsmasq


DNSMASQ
Start
host query rec'd by dnsmasq
Return IP
is host def in dnsmasq.conf?
Receive result from upstream DNS
No
Is host def in /etc/hosts?
No
Query dns server in /etc/resolv.conf

Red Hat Certificate of Expertise in Platform-as-a-Service

Installation :: master and node1

- Install packages: dnsmasq and bind-utils
- Add the following entries to /etc/dnsmasq.conf
  - address=/ocp.lab.example.com/<NODE1_IP>
  - resolv-file=/etc/resolv.dnsmasq

- Create /etc/resolv.dnsmasq with the following:
  - nameserver <YOUR_GW_IP>

Red Hat Certificate of Expertise in Platform-as-a-Service

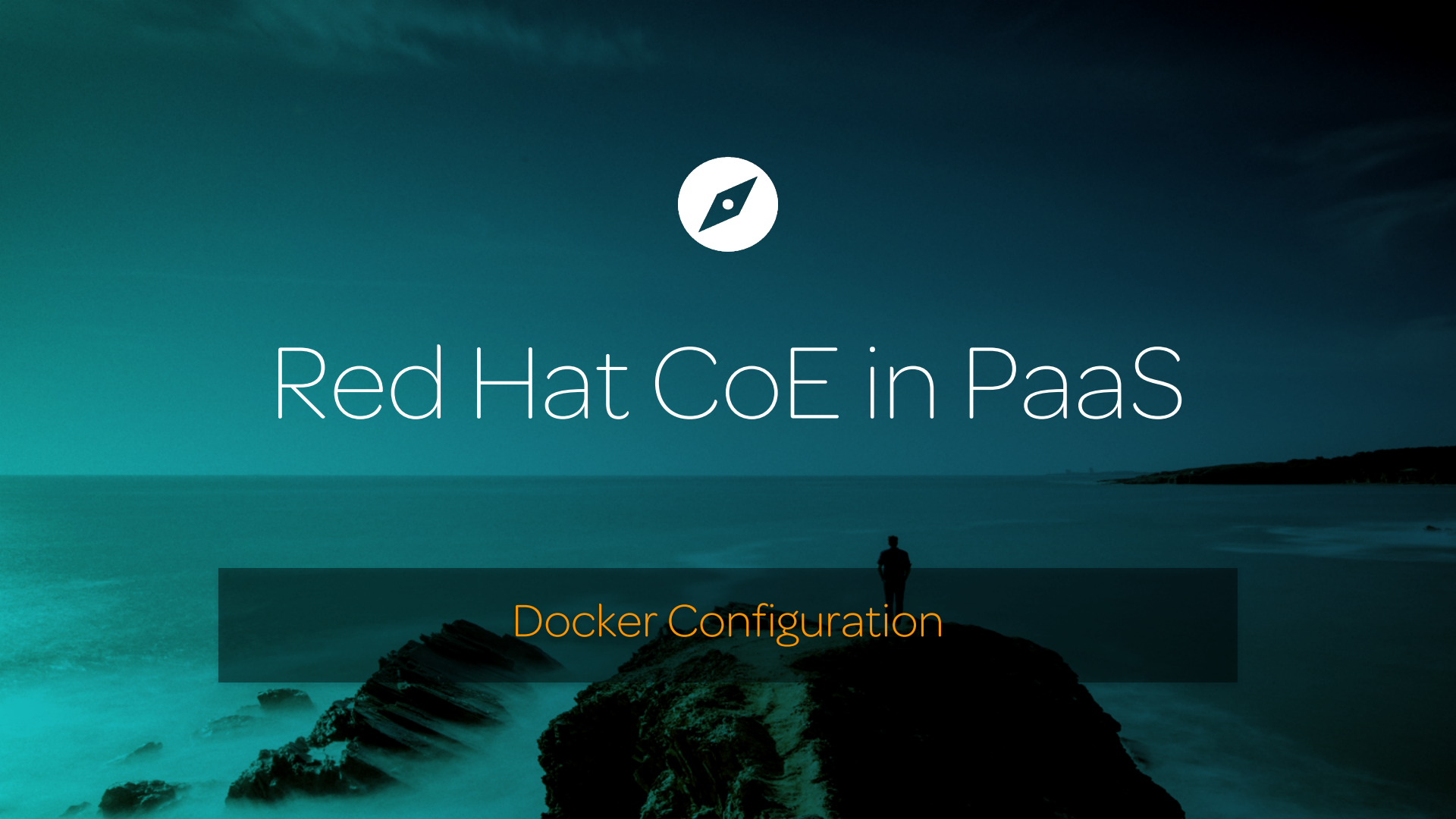
Installation :: master and node1 :: cont'd

- Edit /etc/resolv.conf
  - search example.com
  - nameserver 127.0.0.1
- Add entries to /etc/hosts for master and node1
  - <MASTER_IP> master master.example.com
  - <NODE1_IP> node1 node1.example.com
- Start and enable dnsmasq.service
  - systemctl enable dnsmasq
  - systemctl start dnsmasq

Red Hat Certificate of Expertise in Platform-as-a-Service

Testing

- Verify DNS resolution
  - host $(hostname)
  - Ping a non-existent subdomain under *.ocp.lab.example.com
  - Ping google.com to verify network access



Red Hat CoE in PaaS

Docker Configuration

Red Hat Certificate of Expertise in Platform-as-a-Service

Docker ::

Red Hat Certificate of Expertise in Platform-as-a-Service


Red Hat CoE in PaaS
OpenShift Container Platform Installation

Red Hat Certificate of Expertise in Platform-as-a-Service

OCP :: Dependencies

- bind-utils
- bridge-utils
- git
- iptables-services
- net-tools
- wget

Red Hat Certificate of Expertise in Platform-as-a-Service

OCP :: Packages

- atomic-openshift-excluder
- atomic-openshift-docker-excluder
- atomic-openshift-utils

Red Hat Certificate of Expertise in Platform-as-a-Service

OCP :: atomic-openshift-excluder

- atomic-openshift-excluder unexclude
- atomic-openshift-excluder exclude

Red Hat Certificate of Expertise in Platform-as-a-Service

OCP :: atomic-openshift-installer

- atomic-openshift-installer install
  - User for ssh access [root]
  - OCP variant
  - Set node hostname or IP
  - OpenShift master [y/n]
  - RPM or container-based [rpm]
  - Default subdomain

Red Hat CoE in PaaS

OpenShift Role Bindings

Red Hat Certificate of Expertise in Platform-as-a-Service

OCP :: Role Bindings

- Grants relevant access to user or group
- Per-project basis (-n)
- Per-cluster basis

Red Hat Certificate of Expertise in Platform-as-a-Service

OCP :: Default Roles

- admin
- basic-user
- cluster-admin
- cluster-status
- edit
- self-provisioner
- view

Red Hat Certificate of Expertise in Platform-as-a-Service

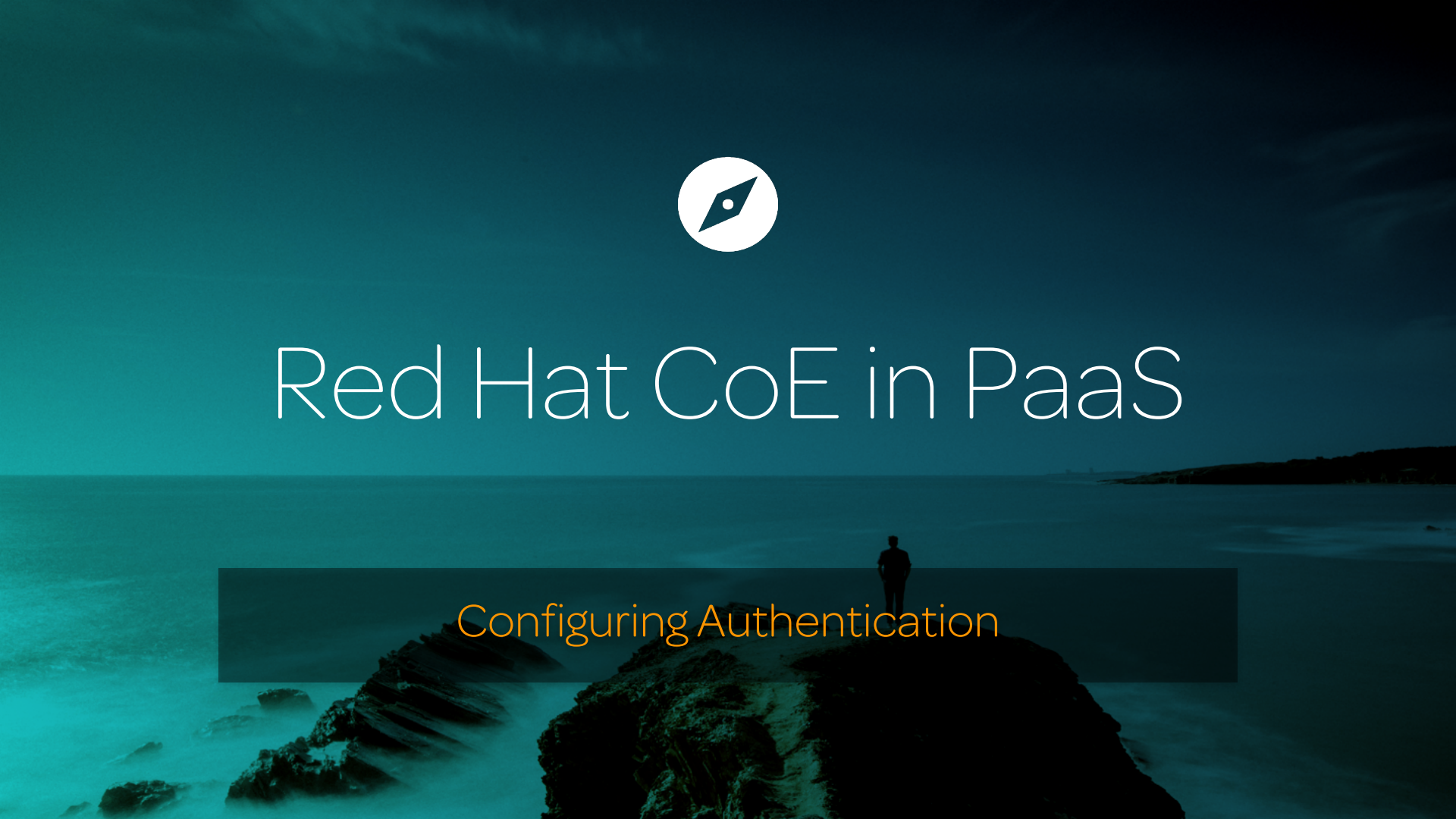
- oc adm policy who-can [action] [resource]
  - Ex: oc adm policy who-can show pods
- oc adm policy add-role-to-user [role] [username]
  - Ex: oc adm add-role-to-user admin dev
- oc adm policy remove-role-from-user [role] [username]
  - Ex: oc adm policy remove-role-from-user edit dev
- oc adm policy remove-user [username]
  - Ex: oc adm policy remove-user test

- Lists who can perform an action on a resource.
  - Users: system:admin Groups: system:cluster-admins system:masters
- Binds a given role to a specified user
  - Grants admin privileges to 'dev' user
- Removes a role from specified users
  - Removes 'edit' privileges from 'dev' user
- Removes the specified user and all of their roles
  - Removes the 'test' user & all of their roles from current project

Red Hat Certificate of Expertise in Platform-as-a-Service

- oc adm policy add-cluster-role-to-user [role] [user]
    - Ex: oc adm policy add-cluster-role-to-user view student
- oc get clusterroles
- oc get / oc describe
    - roles
    - policy
    - clusterroles
    - clusterpolicy
    - clusterrolebindings
    - scc

- Add a role to user for all projects within the OpenShift cluster
    - Will grant viewing privileges to the 'student' user
- Print a full list of available cluster roles in the OCP environment.
- Can be used to print information on roles and policies within an OpenShift Environment



Red Hat CoE in PaaS

Configuring Authentication

Red Hat Certificate of Expertise in Platform-as-a-Service

OCP :: Supported Identity Providers

- Deny All (Default)
- Allow All
- HTPasswd
- GitHub/GitLab
- OpenID Connect
- Keystone v3
- LDAP v3
- Google

Red Hat Certificate of Expertise in Platform-as-a-Service

OCP :: Authentication

- "Secure by default" approach
- DenyAllPasswordIdentityProvider
- HTPasswdPasswordIdentityProvider

Red Hat Certificate of Expertise in Platform-as-a-Service

HTPasswd :: Installation

- Install httpd-tools package
- Create openshift-passwd file
- Edit /etc/origin/master/master-config.yaml
- htpasswd –b /path/to/openshift-passwd [user] [password]
- Restart atomic-openshift-master service

Red Hat Certificate of Expertise in Platform-as-a-Service

HTPasswd Configuration

- On master:
  - /etc/origin/master/master-config.yaml
  - If using vim, use `:set ai` to automatically set indentation
  - Find "oauthConfig:" section

```
oauthConfig:
  assetPublicURL: https://master:8443/console/
  grantConfig:
    method: auto
  identityProviders:
  - challenge: true
    login: true
    mappingMethod: claim
    name: deny_all
    provider:
      apiVersion: v1
      kind: DenyAllPasswordIdentityProvider
```

Red Hat Certificate of Expertise in Platform-as-a-Service

HTPasswd Configuration

- On master:
  - kind: HTPasswdPasswordIdentityProvider
  - file: /path/to/[htpasswd-file.txt]
  - Restart atomic-openshift-master.service

```
oauthConfig:
  assetPublicURL: https://master:8443/console/
  grantConfig:
    method: auto
  identityProviders:
  - challenge: true
    login: true
    mappingMethod: claim
    name: deny_all
    provider:
      apiVersion: v1
      kind: HTPasswdPasswordIdentityProvider
      file: /etc/origin/openshift-passwd
```

Red Hat CoE in PaaS

Routes

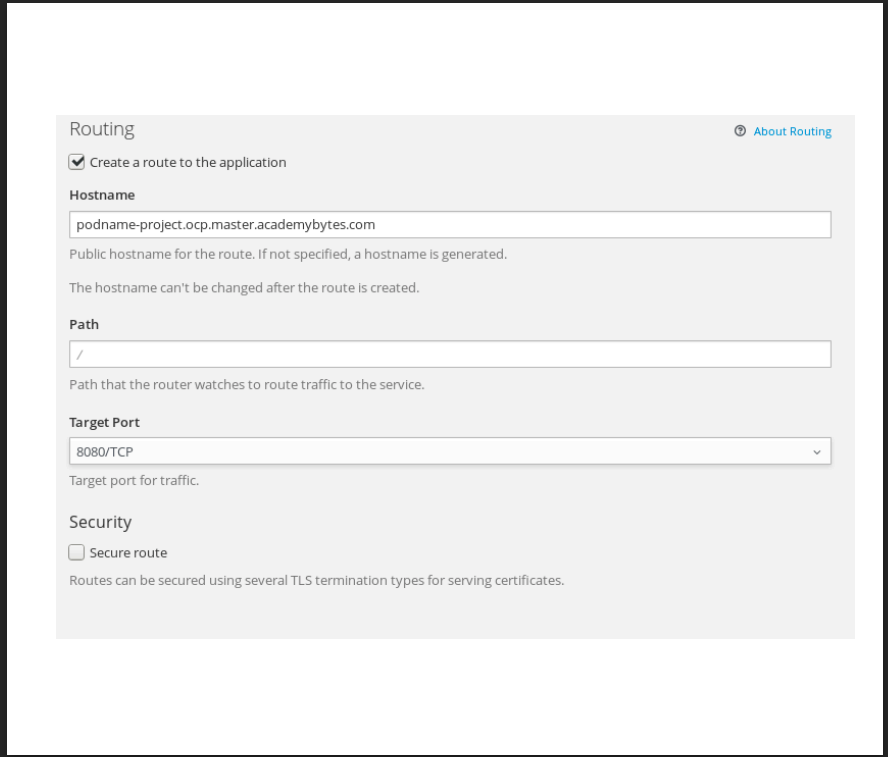
All About Routes

Supported Traffic Protocols

- HTTP
- HTTPS
- WebSockets
- TLS with SNI

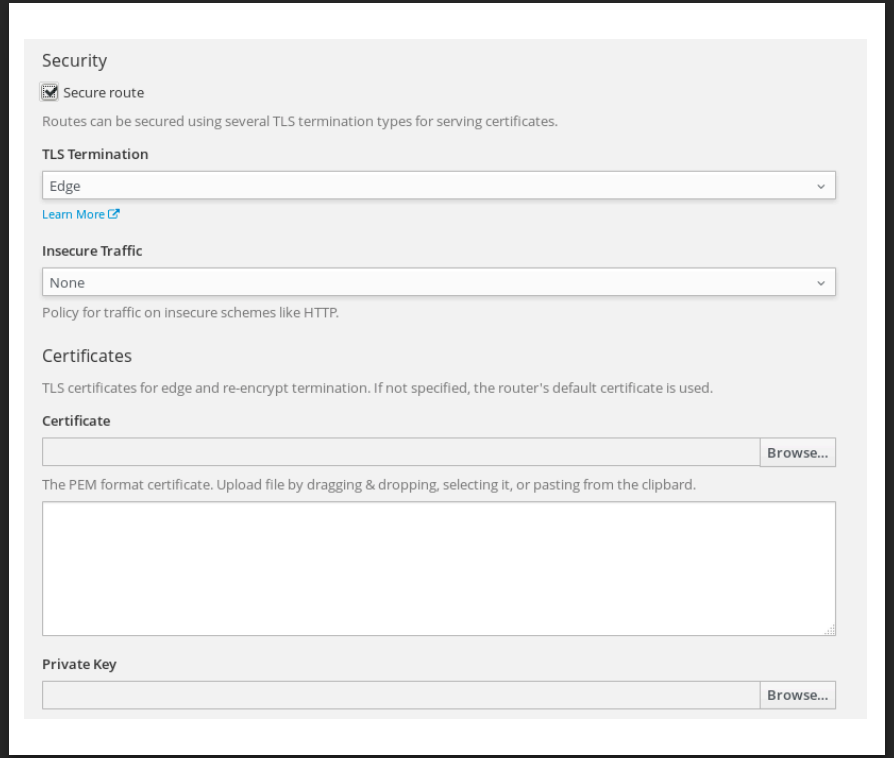
Routes

- Name
  - Pod-service.subdomain.hostname
- Service selector
- (Optional) Security configuration



Route Termination Types

- Edge
- Passthrough
- Re-encrypt



Edge Termination Policy :: HTTPS-only

- Object Name
- Termination type
- (Optional) Key

```
apiVersion: v1
kind: Route
metadata:
    name: route-edge-secured
spec:
    host: www.example.com
    to:
      kind: Service
      name: service-name
    tls:
     termination: edge
     key: |-
       -----BEGIN PRIVATE KEY-----
...
```

Edge Termination Policy :: Allow Insecure Traffic

- Object name
- Termination type
- (Optional) Insecure policy

```
apiVersion: v1
kind: Route
metadata:
    name: route-edge-secured-allow-insecure
spec:
    host: www.example.com
    to:
      kind: Service
      name: service-name
    tls:
      termination: edge
InsecureEdgeTerminationPolicy: Allow
[ ... ]
```

Edge Termination Policy :: Redirect

- Object name
- Termination type
- Insecure policy

```
apiVersion: v1
kind: Route
metadata:
    name: route-edge-secured-redirect-insecure
spec:
    host: www.example.com
    to:
      kind: Service
      name: service-name
    tls:
      termination: edge
InsecureEdgeTerminationPolicy: Redirect
[ ... ]
```

Load Balancing

- Roundrobin
- Each endpoint is used in turn, according to weight.
- Leastconn
- The endpoint with the least amount of connections receives the request.
- Source
- The source IP address is hashed & divided by the total weight of the running servers to designate which server will receive the request.

Red Hat CoE in PaaS

Storage Concepts

Storage Concepts :: Overview

- PersistentVolume – A specific resource
- PersistentVolumeClaim – A request for resource with specific attributes

PersistentVolumes

- Defined by a PV API object
- Cluster resource
- Independent lifecycle
- Captures storage implementation details

PersistentVolumeClaims

- Defined by a PVC API object
- Consumes PV resources

Access Modes

- ReadWriteOnce (RWO)
- ReadOnlyMany (ROX)
- ReadWriteMany (RWX)

- The volume can be mounted as read-write by a single node.
- The volume can be mounted read-only by many nodes.
- The volume can be mounted as read-write by many nodes.

Storage Concepts

PersistentVolume Types

- NFS
- HostPath
- GlusterFS
- Ceph RBD
- OpenStack Cinder
- AWS EBS
- GCE Persistent Disk
- iSCSI
- Fibre Channel
- Azure Disk
- Azure File

Requesting Storage

PersistentVolumes

- metadata:
  - name:
- spec:
  - storage:
  - accessModes:
  - persistentVolumeReclaimPolicy:
- nfs:
  - path:
  - server:

```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv0002
spec:
  capacity:
    storage: 5Gi
  accessModes:
    - ReadWriteOnce
  persistentVolumeReclaimPolicy: Recycle
  nfs:
    path: /tmp
    server: master.academybytes.com
```

Requesting Storage

PersistentVolumeClaims

- metadata:
  - name:
- spec:
  - accessModes:
  - storage:

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: claim-mysql
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 3Gi
```

PersistentVolume Phases

• Available	• A free resource that is not yet bound to a claim.
• Bound	• The volume is bound to a claim.
• Released	• The claim has been deleted, but the resource is not yet reclaimed by the cluster.
• Failed	• The volume has failed its automatic reclamation.

Red Hat CoE in PaaS

S2I

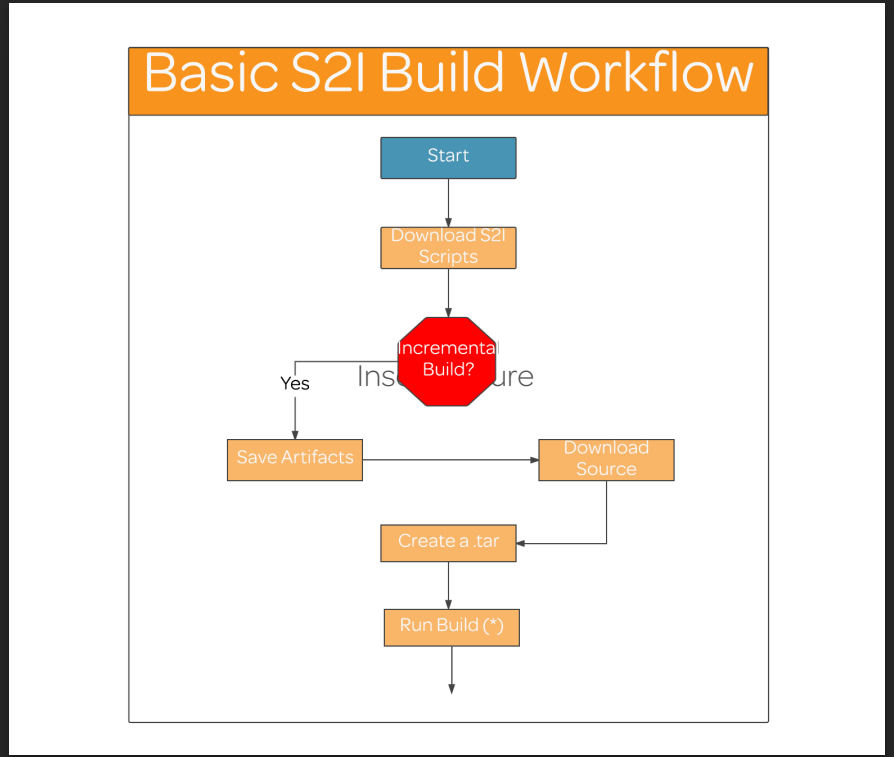
S2I

Build Process

- Sources
- S2I scripts
- Builder image

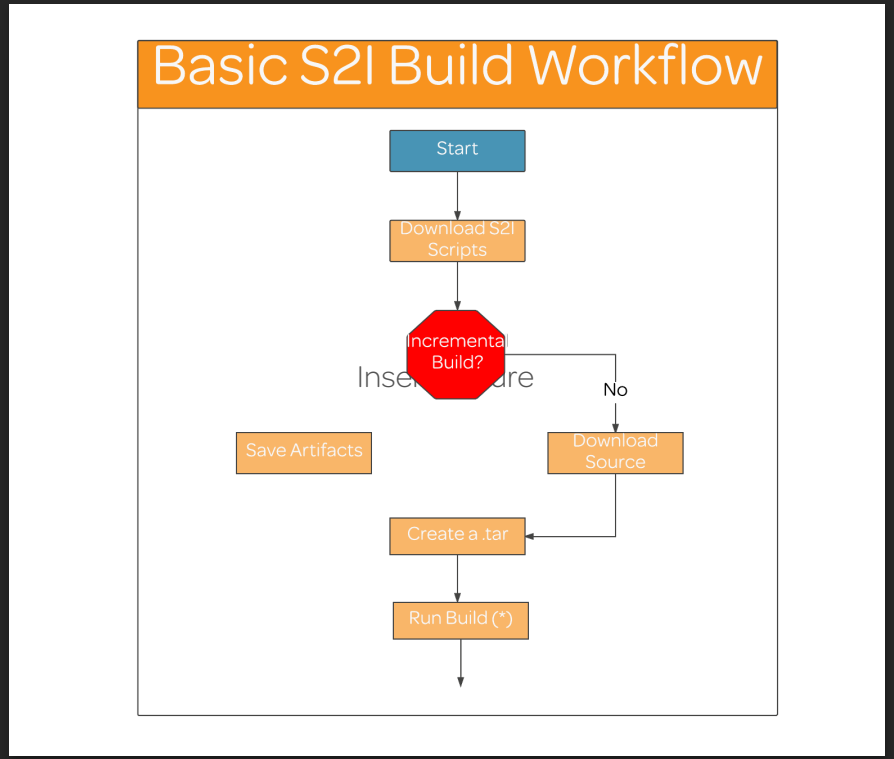
S2I :: Build Process

- Download S2I scripts
- Check for incremental build
    - If Yes:
- Save artifacts
- Download Source
- Create new .tar
- Run build



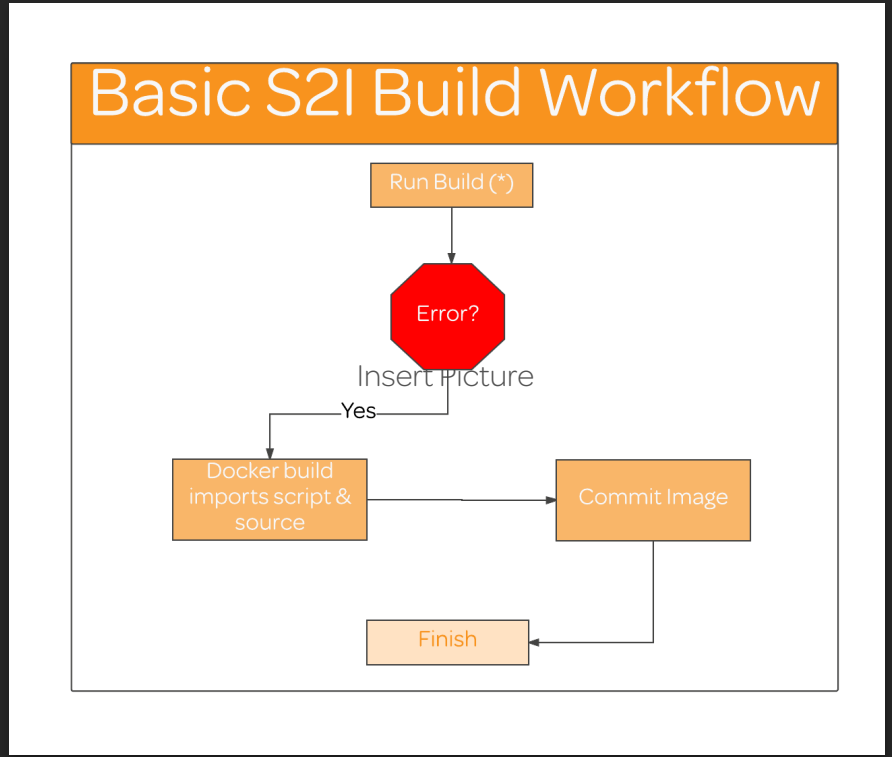
S2I :: Build Process

- Download S2I scripts
- Check for incremental build
    - If No:
- Download Source
- Create new .tar
- Run build



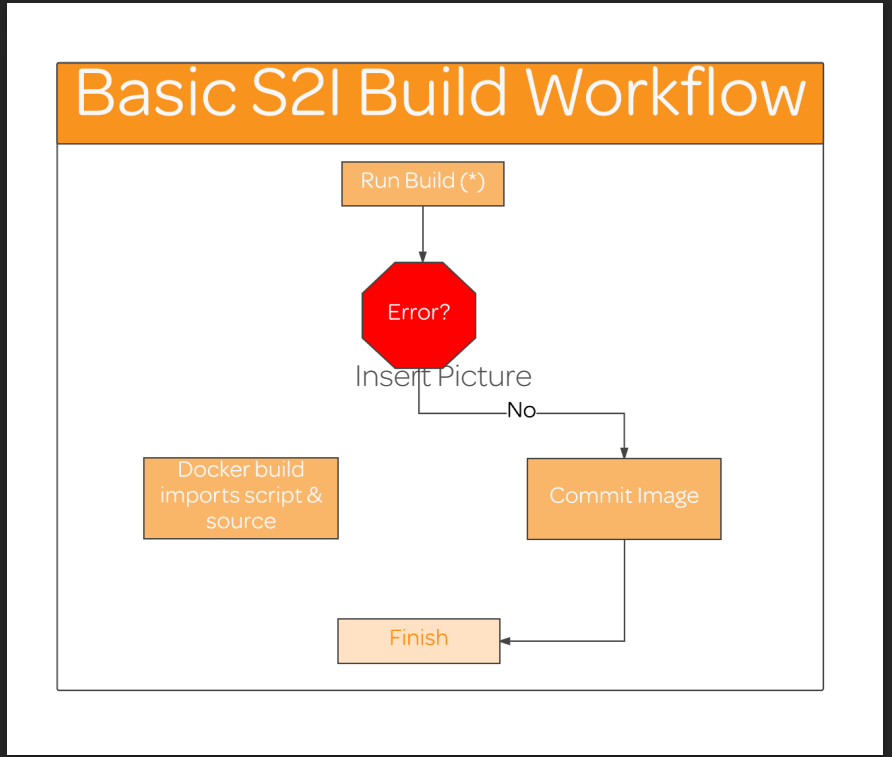
S2I Build Process

- Import script from source
- Commit image
- Build completes



S2I Build Process

- Import script from source
- Commit image
- Build completes



Red Hat CoE in PaaS

Managing Resource Quotas

Managing Resource Quotas

Compute Resources Managed by Quotas

- cpu
- memory
- requests.cpu
- requests.memory
- requests.storage
- limits.cpu
- limits.memory

Managing Resource Quotas

Storage Resources Managed by Quota

- requests.storage
- persistentvolumeclaims
- [storage-class-name].storageclass.storage.k8s.io/requests.storage
- [storage-class-name].storageclass.storage.k8s.io/persistentvolumeclaims

Object Counts Managed by Quota

- pods
- replicationcontrollers
- resourcequotas
- services
- secrets
- configmaps
- persistentvolumeclaims
- openshift.io/imagestreams

Range Object Definitions

1. The name of the limit range object.
2. The maximum amount of CPU that a pod can request on a node across all containers.
3. The maximum amount of memory that a pod can request on a node across all containers.
4. The minimum amount of CPU that a pod can request on a node across all containers.
5. The minimum amount of memory that a pod can request on a node across all containers.

```
apiVersion: "v1"
kind: "LimitRange"
metadata:
  name: "core-resource-limits" (1)
spec:
  limits:
    - type: "Pod"
      max:
        cpu: "2" (2)
        memory: "1Gi" (3)
      min:
        cpu: "200m" (4)
        memory: "6Mi" (5)
    - type: "Container"
      max:
        cpu: "2" (6)
        memory: "1Gi" (7)
      min:
        cpu: "100m" (8)
        memory: "4Mi" (9)
      default:
        cpu: "300m" (10)
        memory: "200Mi" (11)
      defaultRequest:
        cpu: "200m" (12)
        memory: "100Mi" (13)
      maxLimitRequestRatio:
        cpu: "10" (14)
```

Range Object Definitions

6. The maximum amount of CPU that a single container in a pod can request.
7. The maximum amount of memory that a single container in a pod can request.
8. The minimum amount of CPU that a single container in a pod can request.
9. The minimum amount of memory that a single container in a pod can request.
10. The default amount of CPU that a container will be limited to use if not specified.

```
apiVersion: "v1"
kind: "LimitRange"
metadata:
  name: "core-resource-limits" (1)
spec:
  limits:
    - type: "Pod"
      max:
        cpu: "2" (2)
        memory: "1Gi" (3)
      min:
        cpu: "200m" (4)
        memory: "6Mi" (5)
    - type: "Container"
      max:
        cpu: "2" (6)
        memory: "1Gi" (7)
      min:
        cpu: "100m" (8)
        memory: "4Mi" (9)
      default:
        cpu: "300m" (10)
        memory: "200Mi" (11)
      defaultRequest:
        cpu: "200m" (12)
        memory: "100Mi" (13)
      maxLimitRequestRatio:
        cpu: "10" (14)
```

Range Object Definitions

11. The default amount of memory that a container will be limited to use if not specified.
12. The default amount of CPU that a container will request to use if not specified.
13. The default amount of memory that a container will request to use if not specified.
14. The maximum amount of CPU burst that a container can make as a ratio of its limit over request.

```
apiVersion: "v1"
kind: "LimitRange"
metadata:
  name: "core-resource-limits" (1)
spec:
  limits:
    - type: "Pod"
      max:
        cpu: "2" (2)
        memory: "1Gi" (3)
      min:
        cpu: "200m" (4)
        memory: "6Mi" (5)
    - type: "Container"
      max:
        cpu: "2" (6)
        memory: "1Gi" (7)
      min:
        cpu: "100m" (8)
        memory: "4Mi" (9)
      default:
        cpu: "300m" (10)
        memory: "200Mi" (11)
      defaultRequest:
        cpu: "200m" (12)
        memory: "100Mi" (13)
      maxLimitRequestRatio:
        cpu: "10" (14)
```

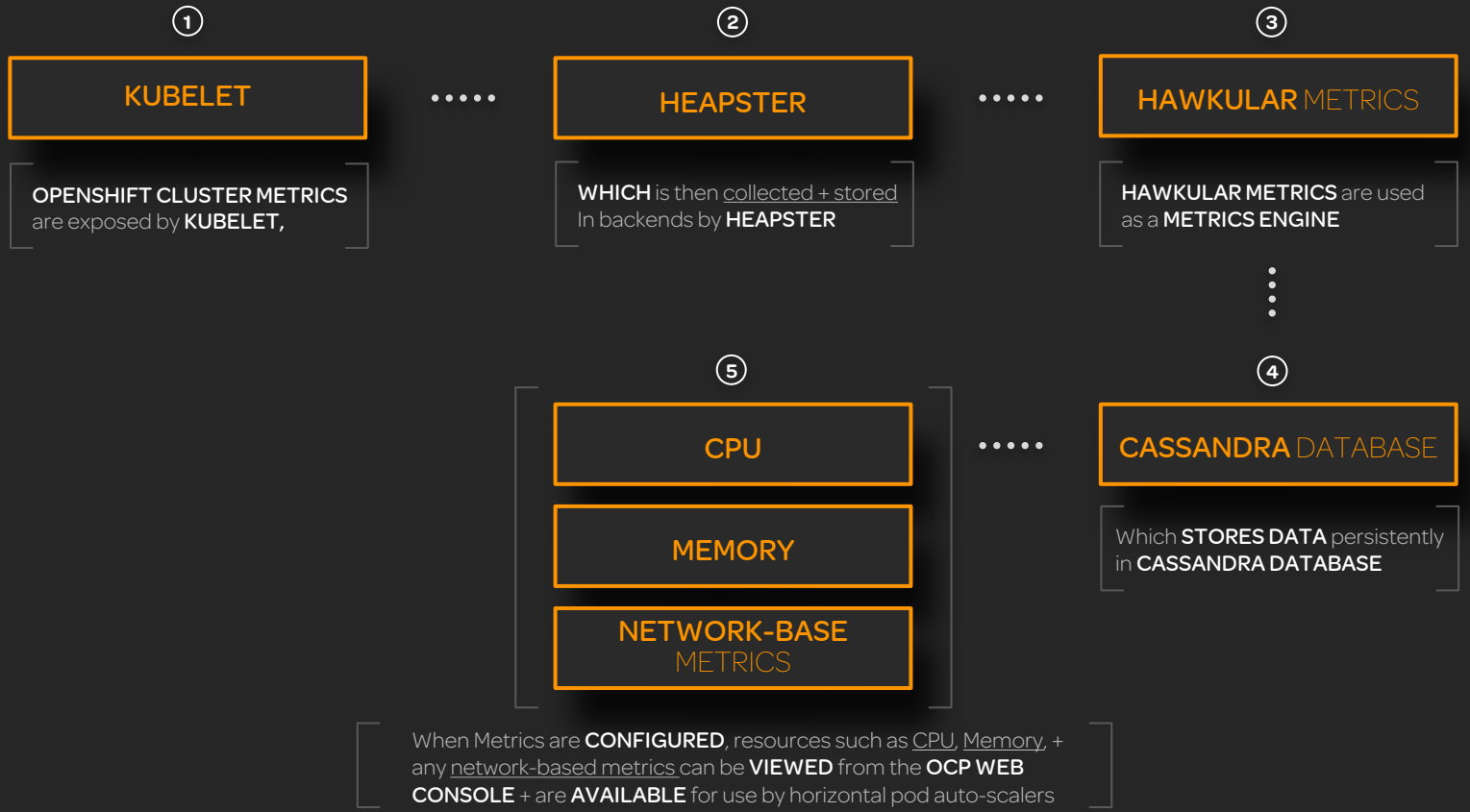
Example:: Resource Quota Definitions

- Total number of Pods (4)
- Total CPU requests (1)
- Sum of Memory Requests (2Gi)
- Sum of CPU limits (2)
- Sum of Memory Limits (4Gi)

```
apiVersion: v1
kind: ResourceQuota
metadata:
    name: compute
spec:
   hard:
     pods: "4"
     requests.cpu: "1"
     requests.memory: "2Gi"
     limits.cpu: "2"
     limits.memory: "4Gi"
```


Red Hat CoE in PaaS
OpenShift Metrics

OVERVIEW


1
KUBELET
OPENSHIFT CLUSTER METRICS are exposed by KUBELET,
2
HEAPSTER
WHICH is then collected + stored In backends by HEAPSTER
3
HAWKULAR METRICS
HAWKULAR METRICS are used as a METRICS ENGINE
4
CASSANDRA DATABASE
Which STORES DATA persistently in CASSANDRA DATABASE
5
CPU
MEMORY
NETWORK-BASE METRICS
When Metrics are CONFIGURED, resources such as CPU, Memory, + any network-based metrics can be VIEWED from the OCP WEB CONSOLE + are AVAILABLE for use by horizontal pod auto-scalers

HAWKULAR METRICS

Metric Data Storage Engine

HAWKULAR PROJECT provides java-based components for alerting **metrics storage** + **distributed tracing**

Apache Cassandra Backend

In **OPENSHIFT**, Hawkular is used as a metrics engine to persistently **STORE DATA** in a **CASSANDRA** database

Singular UI Access

Generic Monitoring System

REST/HTTP Interface

.....

③

HAWKULAR METRICS

HAWKULAR METRICS are used as a **METRICS ENGINE**

KUBELET

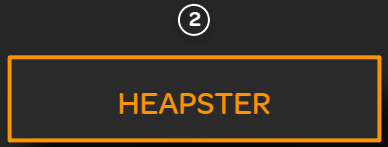
1

KUBELET

OPENSHIFT CLUSTER METRICS
are exposed by **KUBELET,**

File Path on command line	Checked **EVERY 20 SECONDS**
HTTP Endpoint passed...	on the Command Line that is checked **EVERY 20 SECONDS**
Kubelet **WATCHING**...	An **ETCD SERVER** such as /registry/hosts/$(hostname -f), and acting on any changes
Kubelet **LISTENING**...	For **HTTP** + responding to a **SIMPLE API** to submit a **NEW MANIFEST**

HEAPSTER



WHICH is then collected + stored
In backends by HEAPSTER

Heapster enables...	**CONTAINER CLUSTER MONITORING** and...
Performance analysis...	**for KUBERBETES** (v1.0.6 and up) + platforms which include it
Collect + Interpret various signals...	like **COMPUTE RESOURCE USAGE**, lifecycle events, etc.
Pluggable storage...	Heapster **SUPPORTS** many pluggable storage **BACKENDS**, or "sinks"
Multiple data sources...	**RETRIEVING** list, then **CONTACTING** nodes

CONFIGURATION :: NFS HOST GROUP

- openshift_metrics_install_metrics=true
- openshift_metrics_storage_kind=nfs
- openshift_metrics_storage_access_modes=['ReadWriteOnce']
- openshift_metrics_storage_nfs_directory=/exports
- openshift_metrics_storage_nfs_options='*(rw,root_squash)'
- openshift_metrics_storage_volume_name=metrics
- openshift_metrics_storage_volume_size=10Gi

CONFIGURATION :: NFS HOST GROUP

- openshift_metrics_install_metrics=true
- openshift_metrics_storage_kind=nfs
- openshift_metrics_storage_access_modes=['ReadWriteOnce']
- openshift_metrics_storage_nfs_directory=/exports
- openshift_metrics_storage_nfs_options='*(rw,root_squash)'
- openshift_metrics_storage_volume_name=metrics
- openshift_metrics_storage_volume_size=10Gi

CONFIGURATION :: EXTERNAL NFS HOST

- openshift_metrics_install_metrics=true
- openshift_metrics_storage_kind=nfs
- openshift_metrics_storage_access_modes=['ReadWriteOnce']
- openshift_metrics_storage_host=nfs.example.com
- openshift_metrics_storage_nfs_directory=/exports
- openshift_metrics_storage_volume_name=metrics
- openshift_metrics_storage_volume_size=10Gi

CONFIGURATION :: EXTERNAL NFS HOST

- openshift_metrics_install_metrics=true
- openshift_metrics_storage_kind=nfs
- openshift_metrics_storage_access_modes=['ReadWriteOnce']
- openshift_metrics_storage_host=nfs.example.com
- openshift_metrics_storage_nfs_directory=/exports
- openshift_metrics_storage_volume_name=metrics
- openshift_metrics_storage_volume_size=10Gi