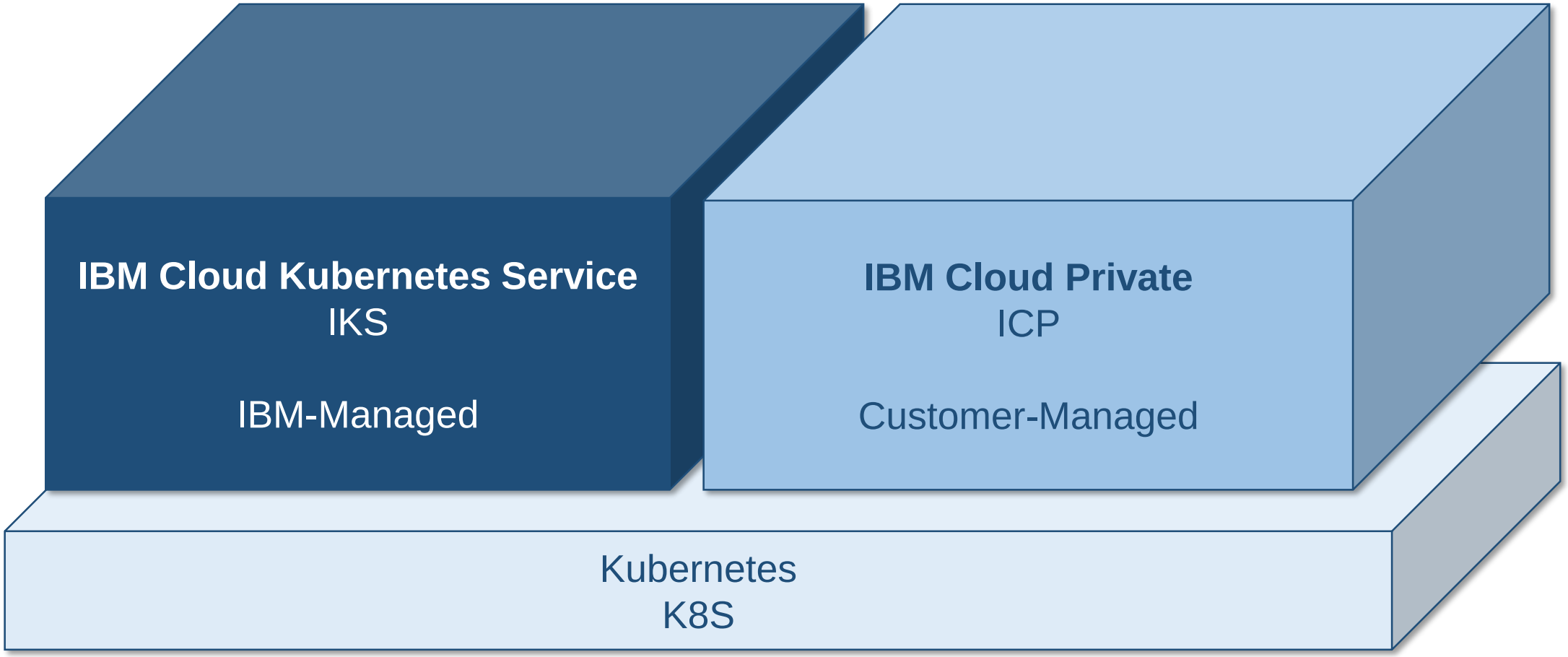
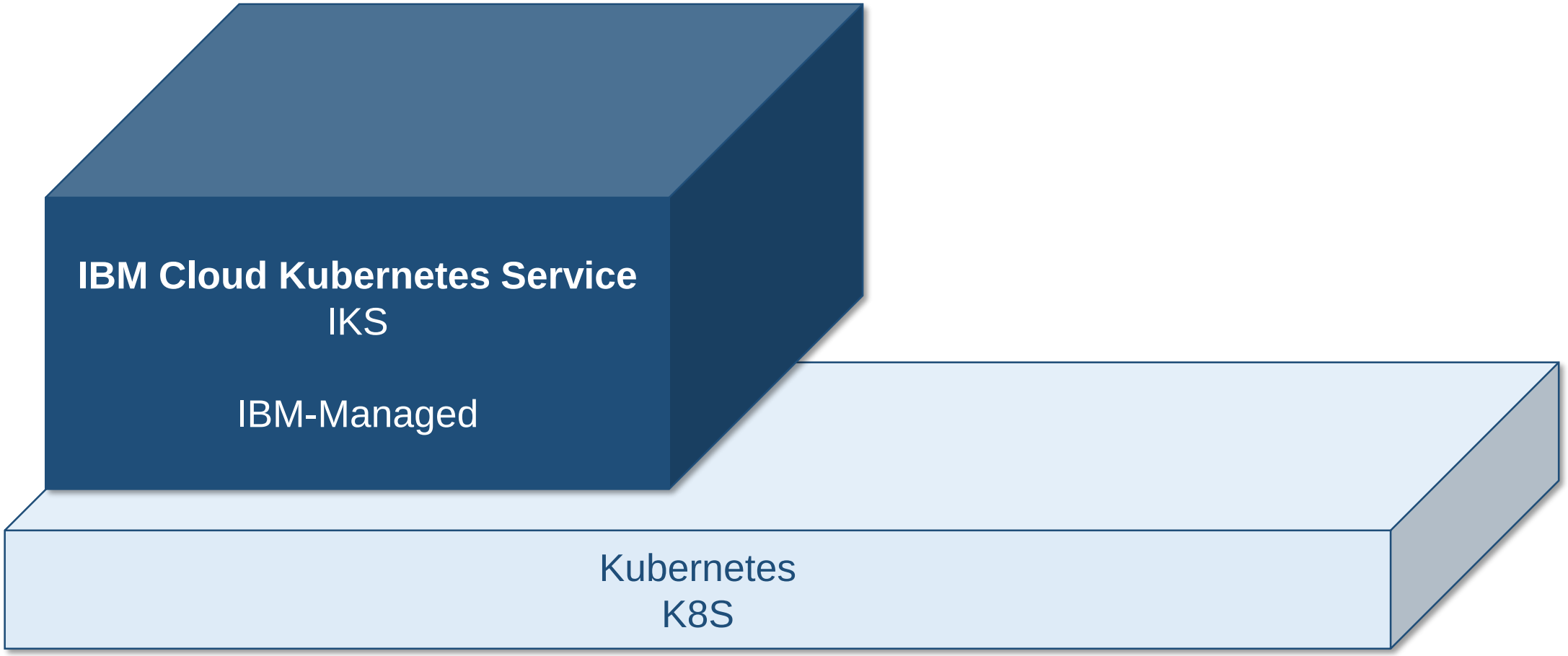
IBM Cloud Containers Workshop

IBM Cloud Kubernetes Services

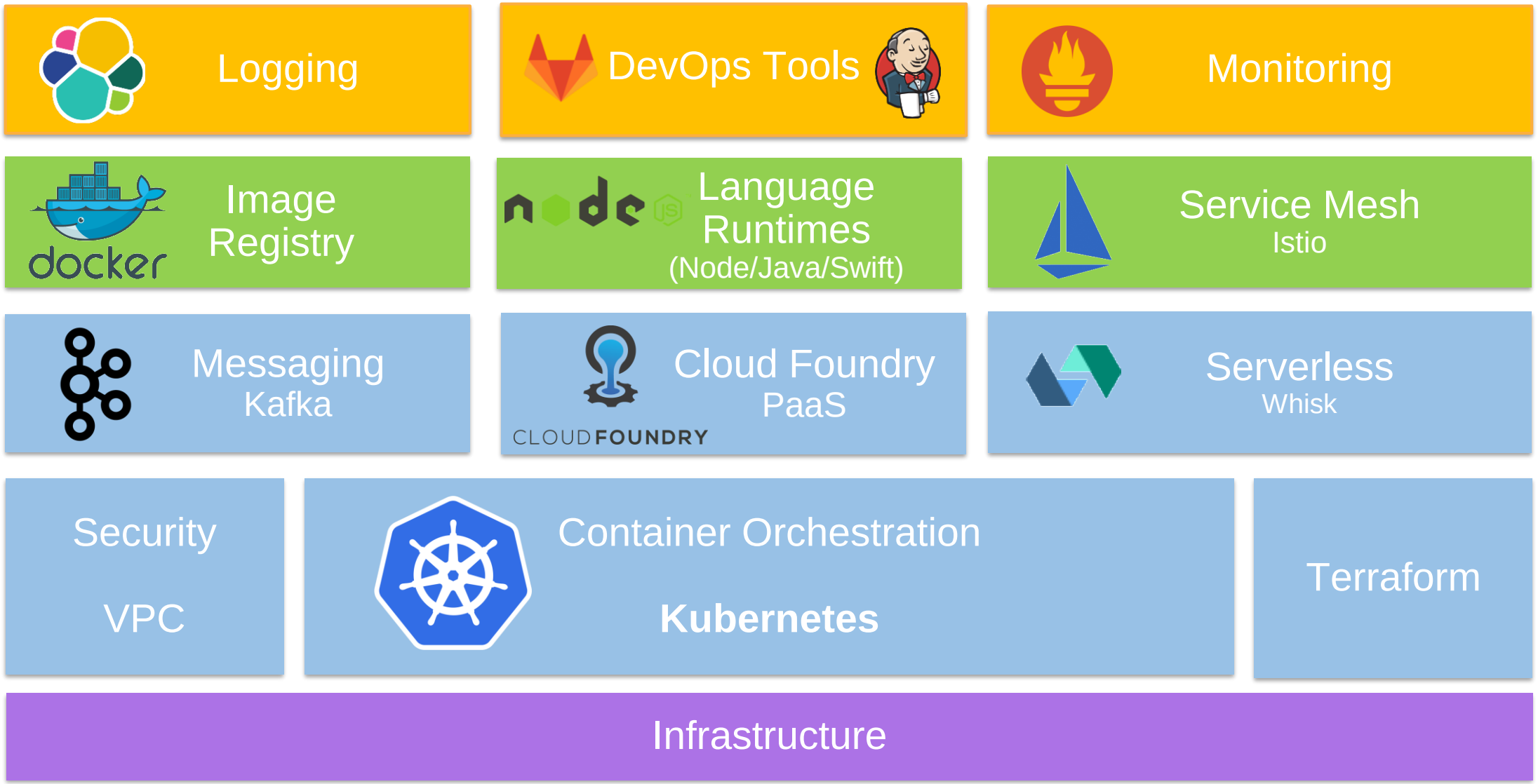
IBM Solutions based on Kubernetes



IBM Cloud Kubernetes Services



Architecture based on Open Technologies



IBM Cloud Container Registry

IBM **managed stand-alone Docker image registry**

Pre-integrated with our Kubernetes Service.

Secure with integration to IBM Identity and Access Manager.

No need to configure and maintain store for your images.

Advanced capabilities such as vulnerability scanning, malware detection, policy scanning, image signing, and deployment policy enforcement.

IBM Cloud Kubernetes Service

A **certified, managed Kubernetes service**

Built-in **security and isolation** to enable rapid delivery of apps.

Available in six IBM regions WW, including **20+ datacenters**.

Fully **dedicated, single tenant clusters** deployed within customer account and network

Seamless integration with IBM Cloud services

Portability with native Kubernetes experience and **full API support**

IBM **Cloud Kubernetes Service**

Kubernetes Capabilities

Intelligent Scheduling

Self-healing

Horizontal scaling

Service discovery & load balancing

Automated rollouts and rollbacks

Secret and configuration management

Cluster Management Capabilities

Simplified cluster management

Flexible cluster topologies

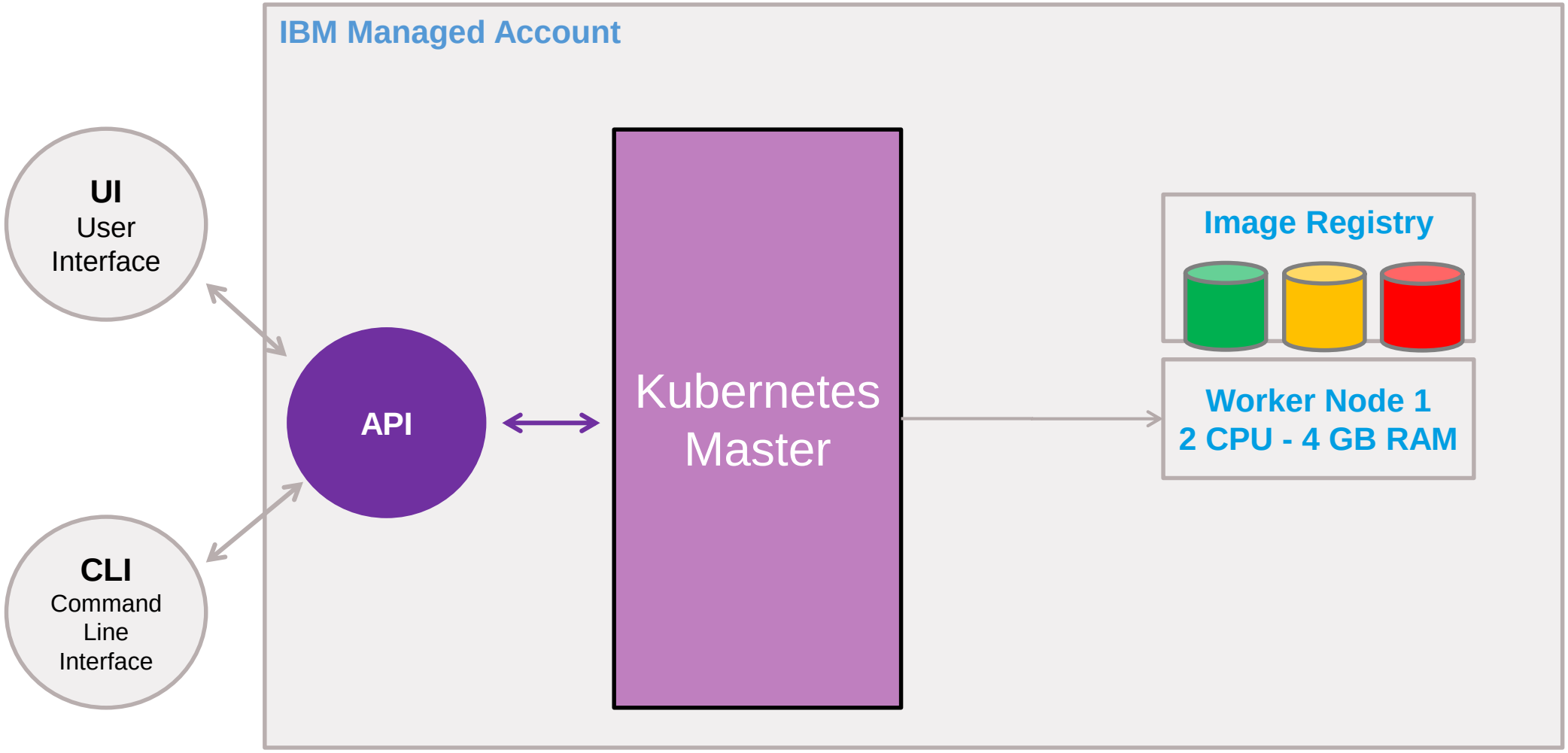
Container security & isolation

Extend with IBM Cloud & Watson

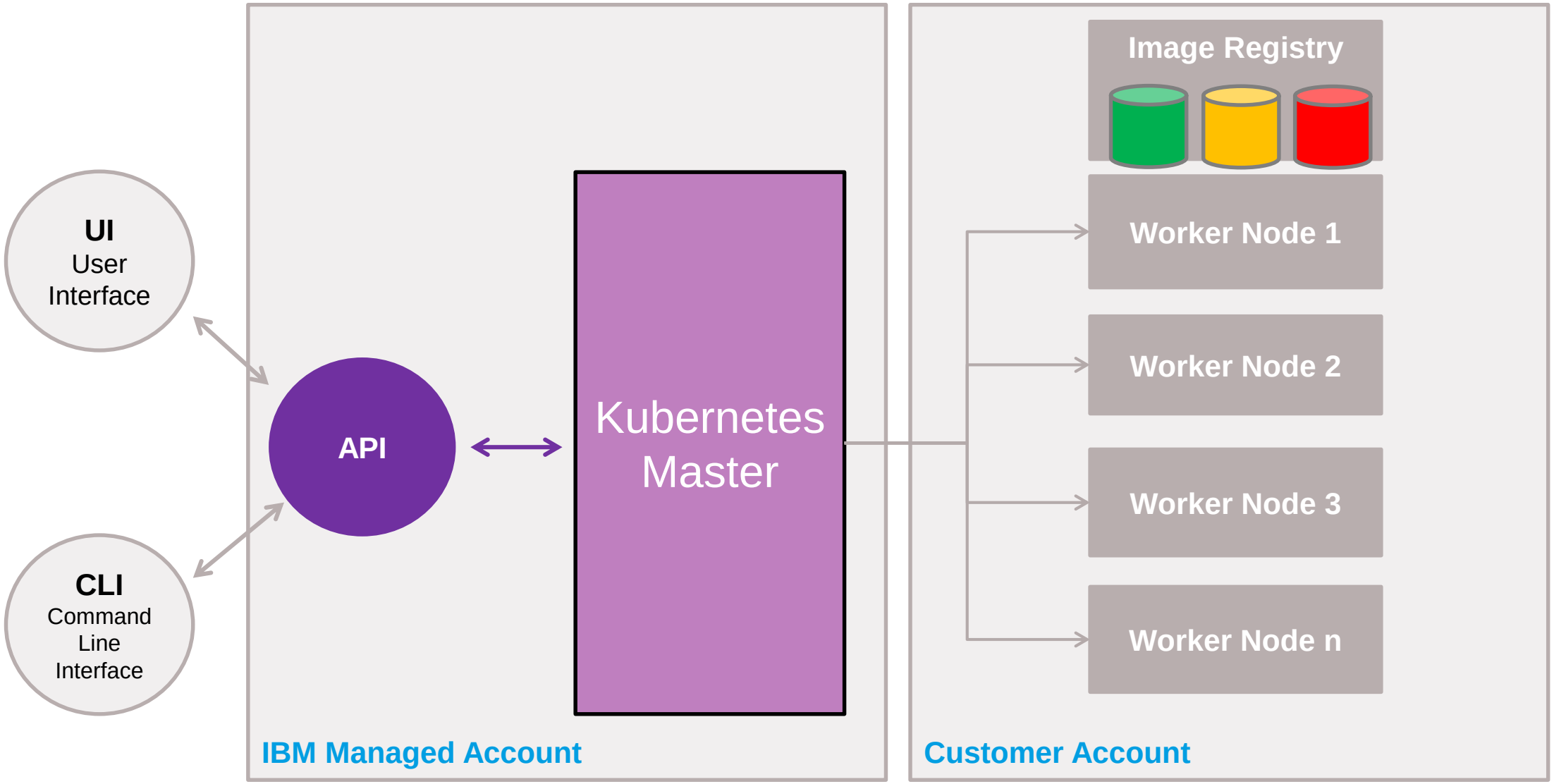
Native open-source experience

Integrated operational tools

Lite Cluster – Single Worker Node

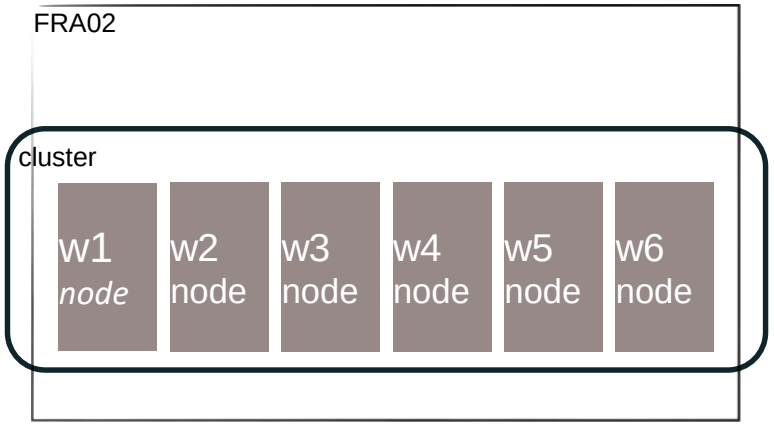


Standard Cluster - fully customizable, production-ready



Single Zone Cluster

EU-DE



- Cluster created in a single location (datacenter)
- Worker nodes provisioned in a single location
- Master managed by IKS runs in the same datacenter within the IKS account

Multizone Cluster

What is it?

A single Kubernetes cluster that has worker nodes spread across multiple failure domains (i.e., zones).

Why is it valuable?

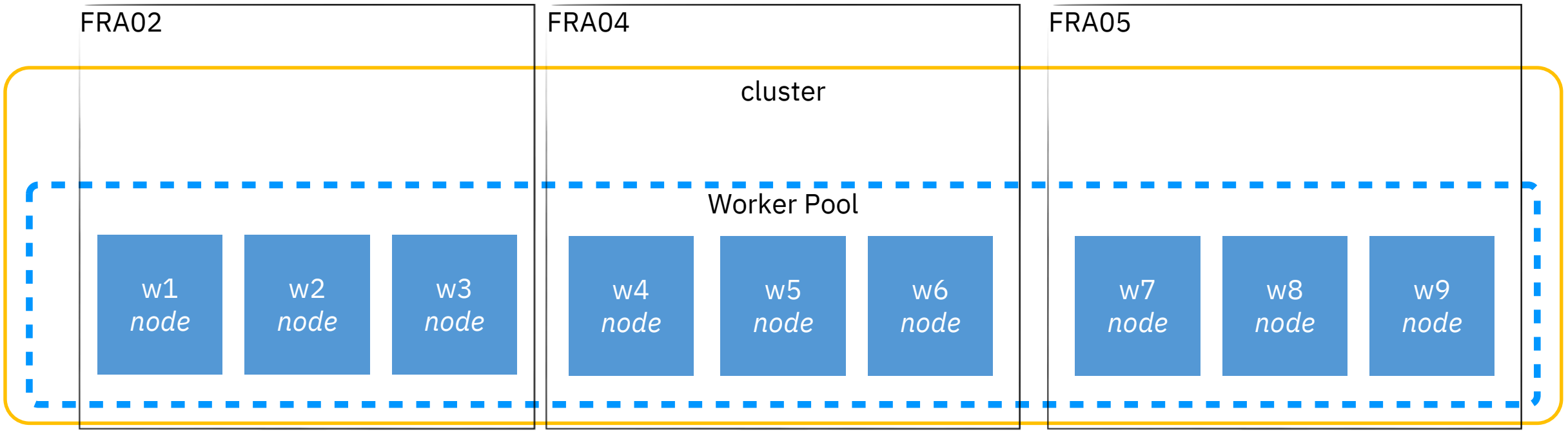
Enables customers to achieve higher availability of their services without an increased operational burden of having to run multiple clusters in separate zones.

https://console.bluemix.net/docs/containers/cs_internal_multi_az.html#cs_multi_az

Multizone Cluster

- Worker nodes are automatically provisioned in the other zones
- Three zones at 150% provides 100% capacity in event of a zone failure.
- Note, 200% capacity required if using two zones

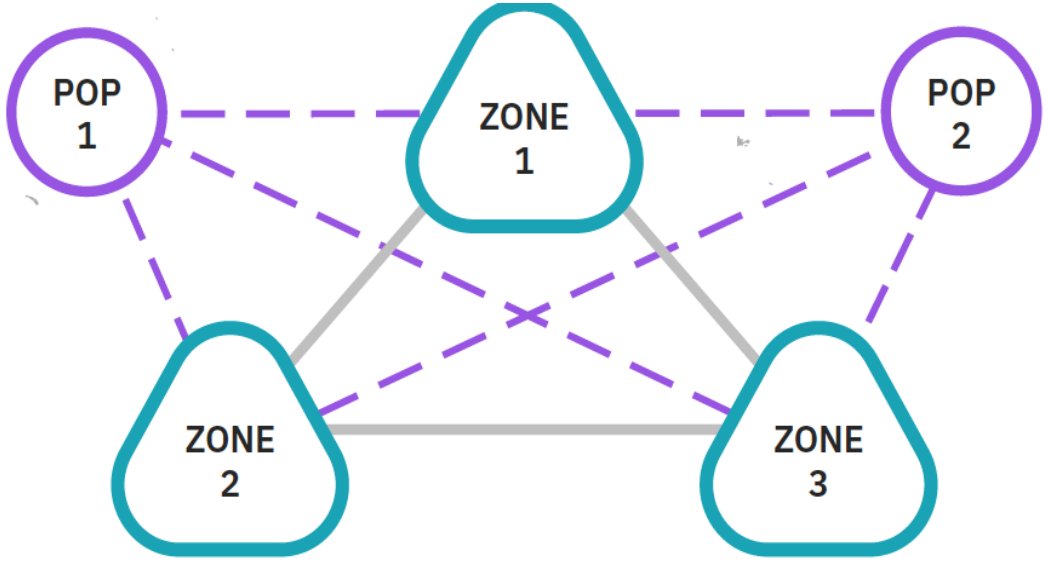
EU-DE



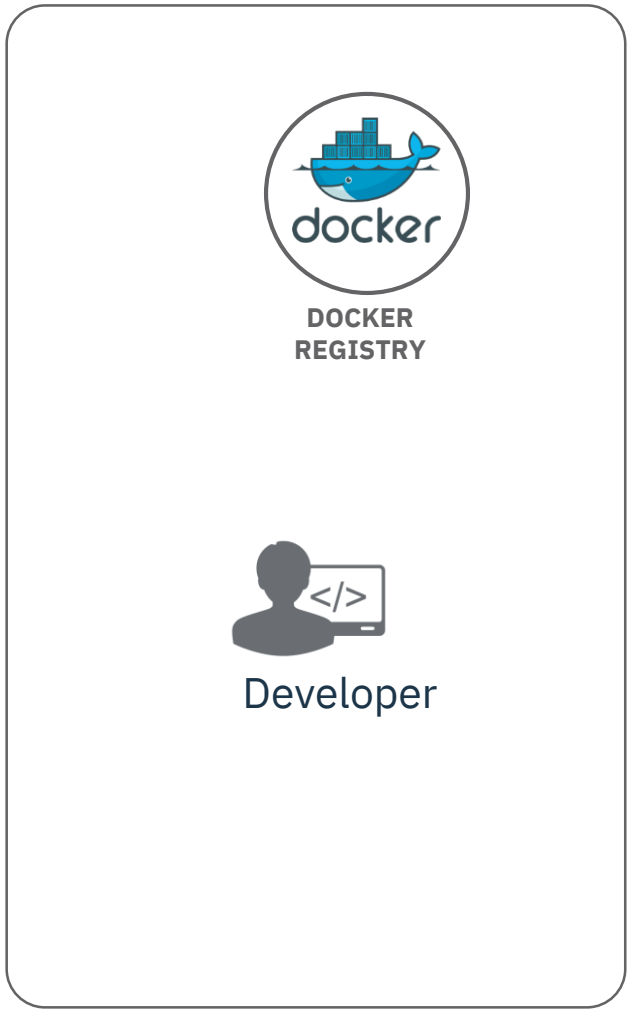
Where are Multizone Clusters available?

High Availability with Multi Zone Region (MZR)

- 3 AZ (Availability Zones) to separate failure domains per MZR (multi-zone region)
- Each AZ is a separate physical data center building.
- Data centers have high bandwidth, low latency redundant links with dual POPs.
- Zones built less than 2msec fiber distance from one another in a region.



Command Lines



ibmcloud login

ibmcloud target –r eu-de

ibmcloud cr images

docker push <my-image>

ibmcloud target –g <rg-name>

ibmcloud ks

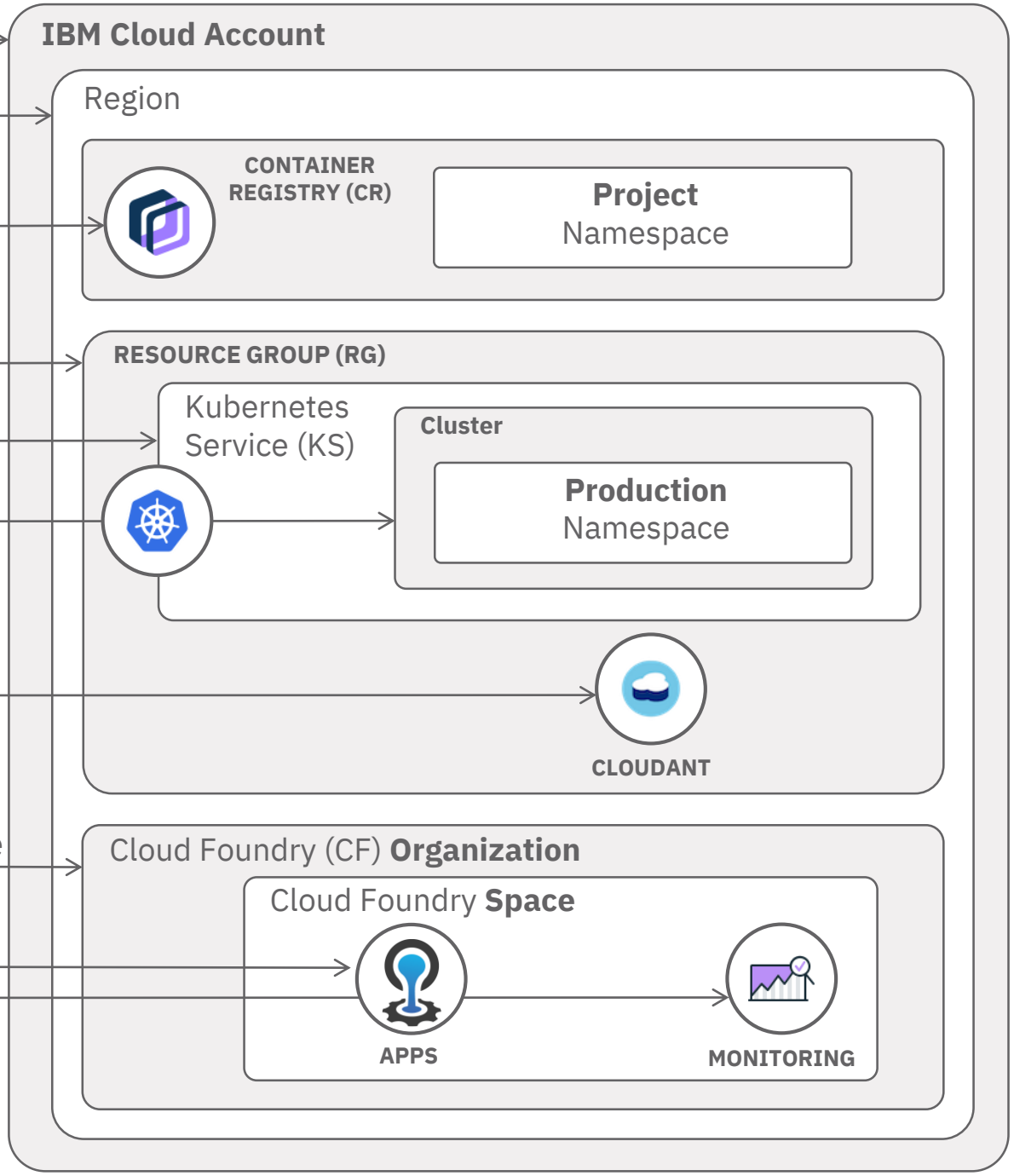
kubectl

ibmcloud resource

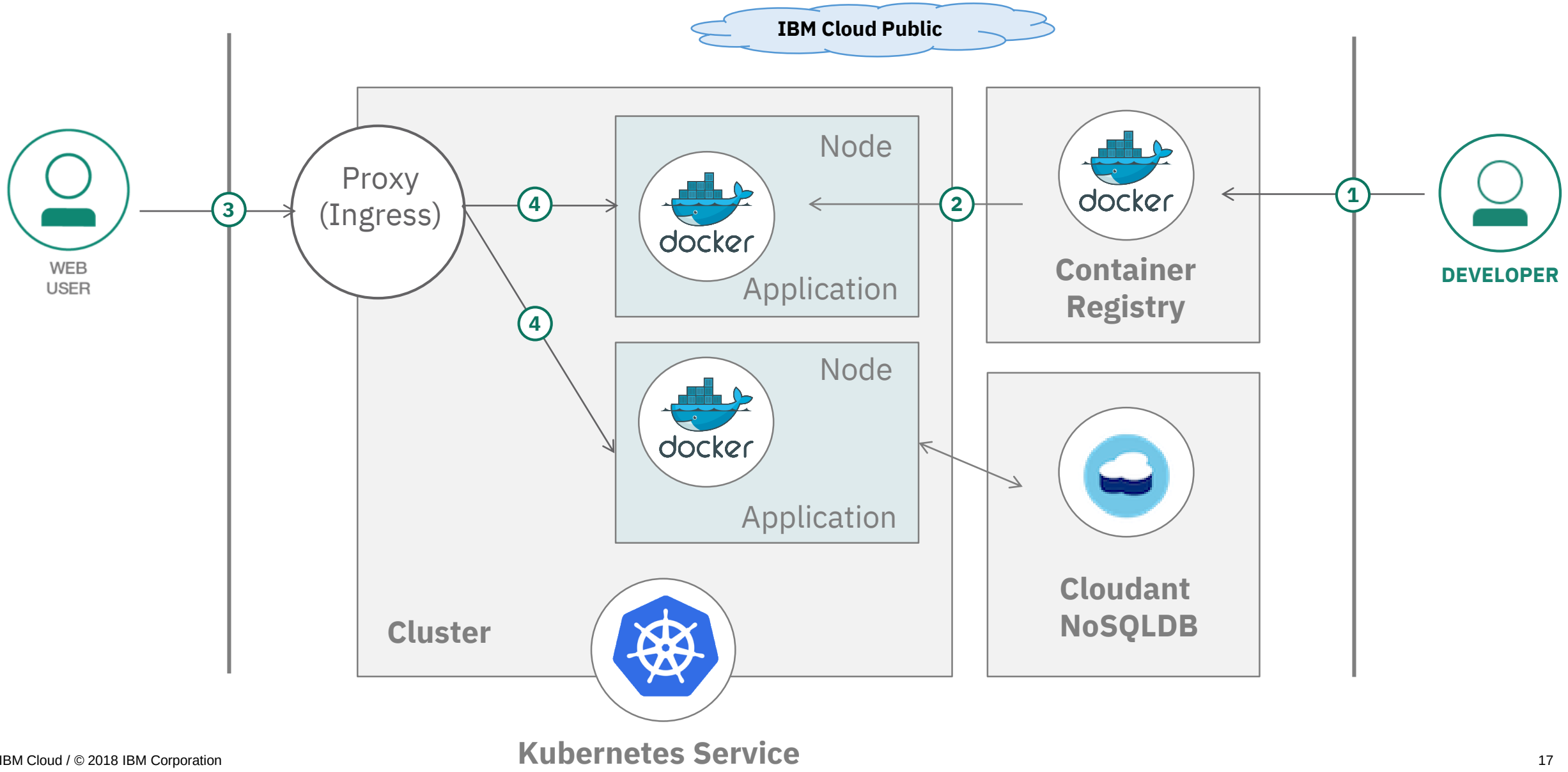
ibmcloud target –o org –s space

ibmcloud cf

ibmcloud service



Demonstration



Kubernetes Service

How to create a cluster?

Cluster IAM Access Policies

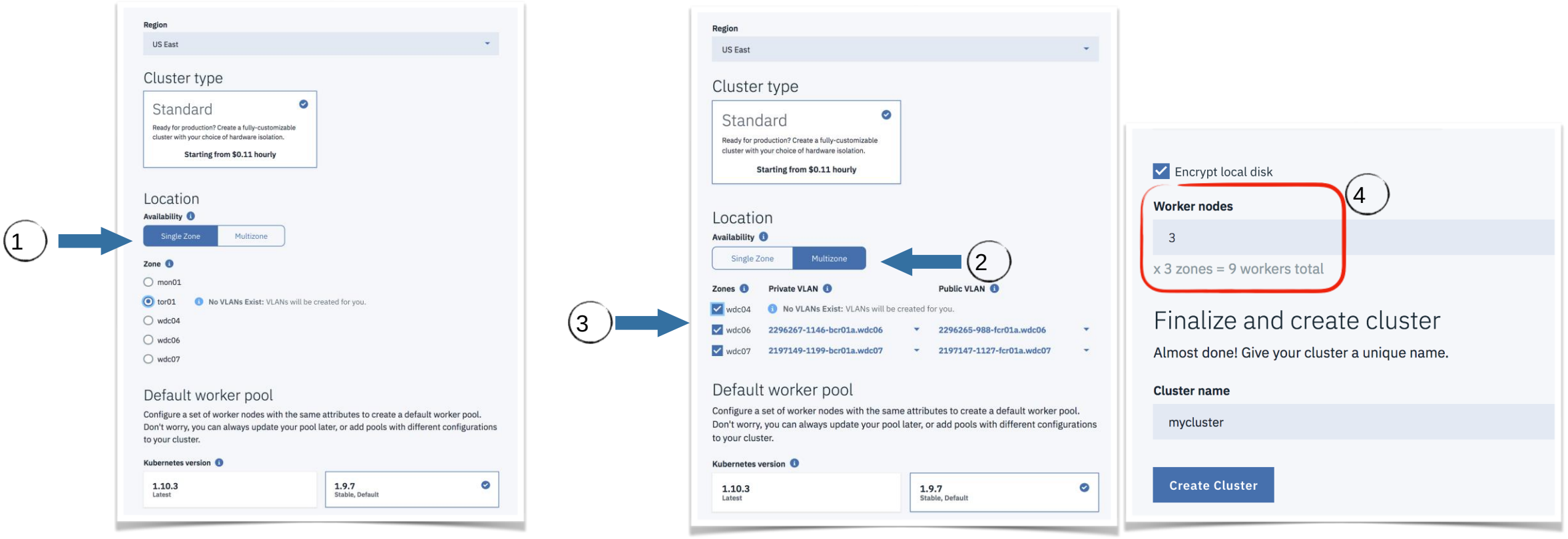
Cluster Management Permissions	Administrator	Operator	Editor	Viewer
Create / Remove a cluster	X			
Assign and change IKS access policies for other existing users in this account.	X			
Add additional worker nodes to a cluster	X	X		
Remove worker nodes from a cluster	X	X		
Reboot a worker node	X	X		
Reload a worker node	X	X		
Add a subnet to a cluster	X	X		
Bind / Unbind a Cloud Service to a cluster.	X	X	X	
View details for a secret	X	X	X	
List a cluster	X	X	X	X
View details for a cluster	X	X	X	X

***Tip**: Use the role Editor for app developers.*

Create Cluster

Single Zone Cluster

Multizone Cluster



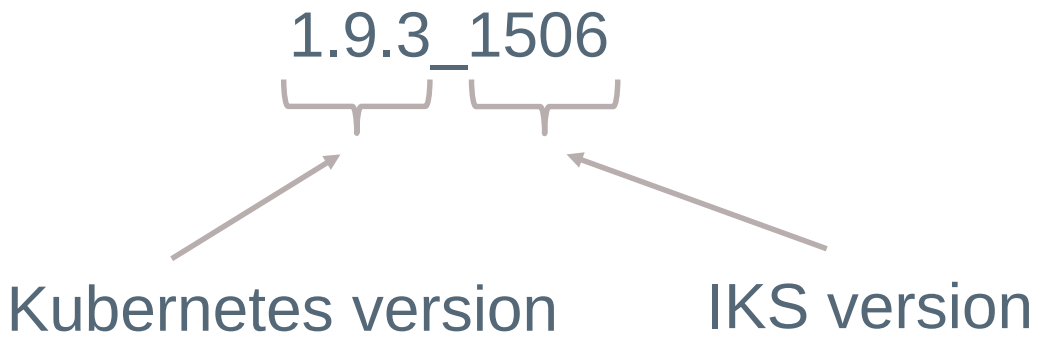
Select the Location where to provision your cluster

Region	Location	City
AP North	hkg02, seo01, sng01, tok02	Hong Kong S.A.R. of the PRC, Seoul, Singapore, Tokyo
AP South	syd01, syd04 mel01	Sydney Melbourne
EU Central	fra02, fra04, fra05 ams03, par01	Frankfurt Amsterdam, Paris
UK South	lon02, lon04, lon06	London
US East	wdc04, wdc06, wdc07 mon01, tor01	Washington DC Montreal, Toronto,
US South	dal10, dal12, dal13 sao01	Dallas São Paulo

Select the Kubernetes Version

Supported Kubernetes versions:

- Latest 1.13.4
- Stable, Default 1.12.6
- Stable 1.11.8
- Deprecated 1.9.10



Newest version supported is tagged **Latest**
The n-2 versions are marked **Stable**
The n-1 version also marked **Default**

DEVELOPER

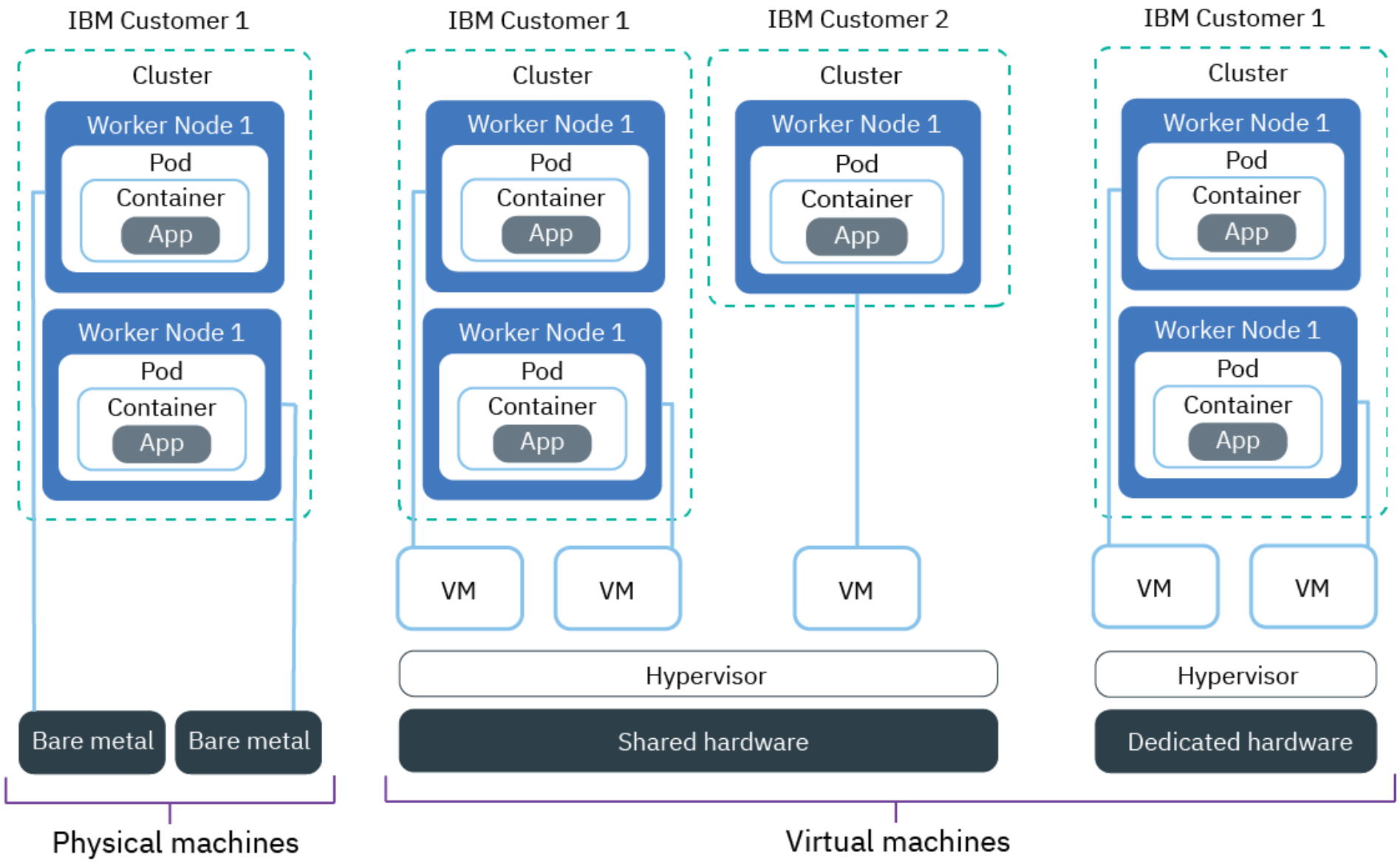
> ibmcloud ks kube-versions

Pace of evolution of Kubernetes

Supported?	Version	IBM Cloud Kubernetes Service release date	IBM Cloud Kubernetes Service unsupported date
✓	1.13	05 Feb 2019	Dec 2019 †
✓	1.12	07 Nov 2018	Sep 2019 †
✓	1.11	14 Aug 2018	Jun 2019 †
!	1.10	01 May 2018	30 Apr 2019 †
✗	1.9	08 Feb 2018	27 Dec 2018
✗	1.8	08 Nov 2017	22 Sep 2018
✗	1.7	19 Sep 2017	21 Jun 2018
✗	1.6	N/A	N/A
✗	1.5	23 May 2017	04 Apr 2018

Release history for IBM Cloud Kubernetes Service.

Select the type of machines



Select Local Disk Encryption

- Encryption by default
- /var/lib/docker is unlocked using LUKS encryption keys
- Each worker node in each cluster has its own unique LUKS encryption key

Kubernetes Service

Data Persistence

Persistent Data Storage

Option 1: EmptyDir

Pod

Container

Volume: /emptyDir

Disk space on worker node

Option 2: NFS based file storage

Pod

Container

Volume:
PersistentVolumeClaim

Persistent Volume

Option 3: IBM Cloud database service

Pod

Container

Volume:
IBM Cloud service secret

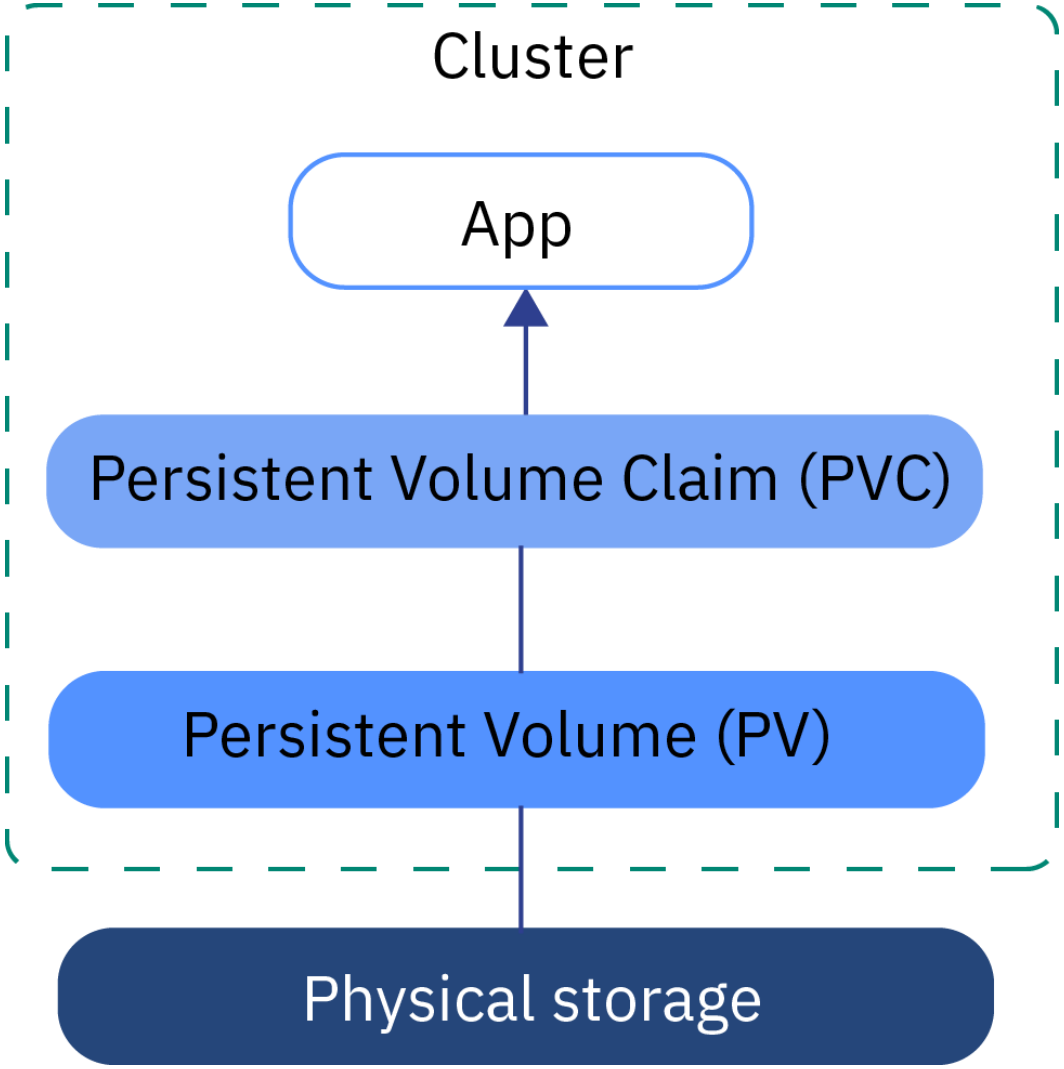
IBM Cloud service connected to external database

Persistent volumes and persistent volume claims

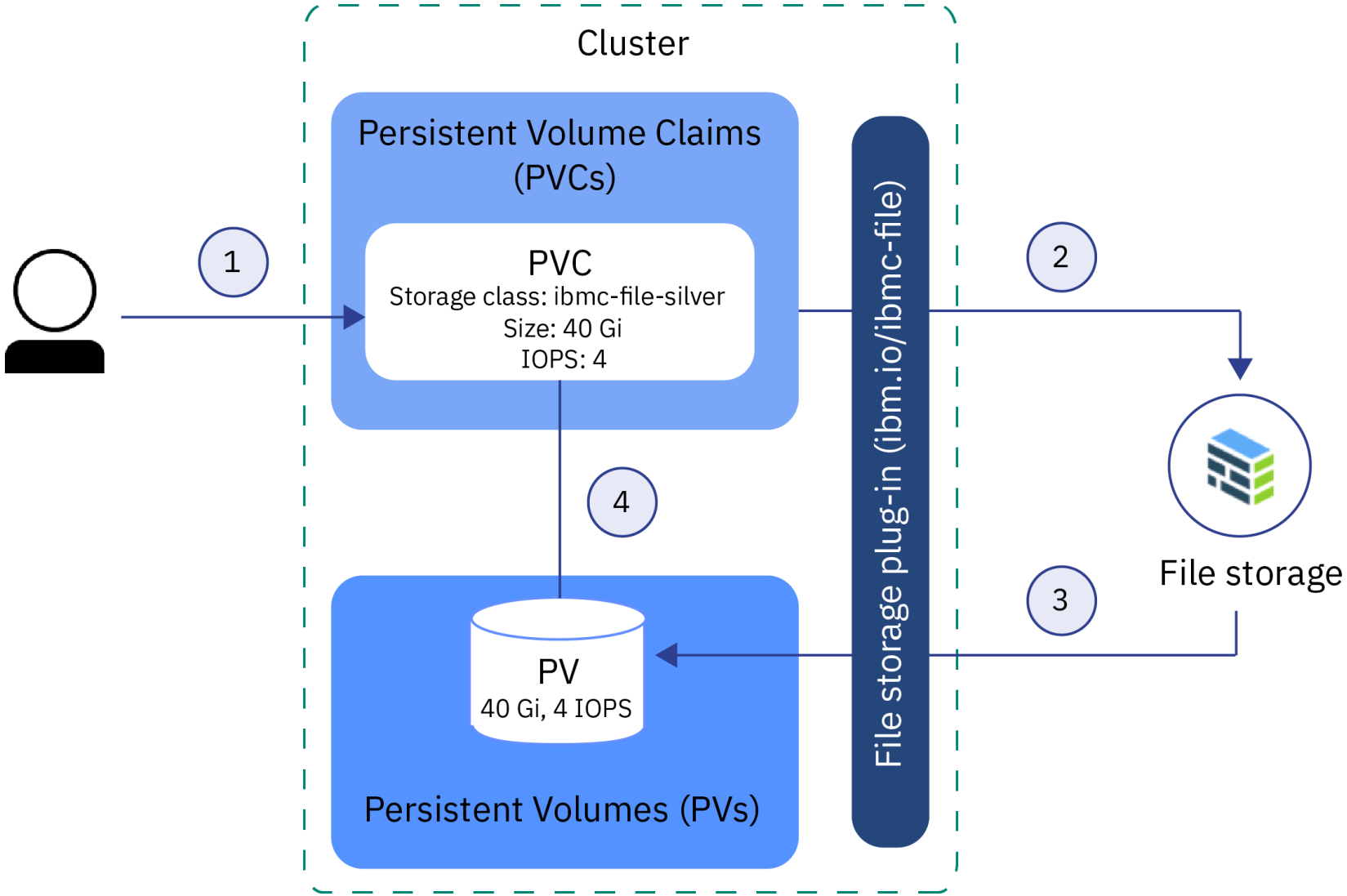
By default, every cluster is set up with a plug-in to provision file storage.

You can choose to install other add-ons, such as the one for block storage.

To use storage in a cluster, you must create a persistent volume claim, a persistent volume and a physical storage instance.



Option 2 - Sample flow for provisioning of file storage



Option 2 – Storage Classes – NFS 2, 4, 10 IOPS

Developer

kubectl get storageclasses

```
NAME                          PROVISIONER
default                       ibm.io/ibmc-file
ibmc-file-bronze              ibm.io/ibmc-file
ibmc-file-custom              ibm.io/ibmc-file
ibmc-file-gold                ibm.io/ibmc-file
ibmc-file-retain-bronze       ibm.io/ibmc-file
ibmc-file-retain-custom       ibm.io/ibmc-file
ibmc-file-retain-gold         ibm.io/ibmc-file
ibmc-file-retain-silver       ibm.io/ibmc-file
ibmc-file-silver              ibm.io/ibmc-file
```

Option 2 - Request a Persistence Volume Claim PVC

Developer

kubectl create –f mypvc.yml

kubectl describe persistentvolumeclaim/mypvc

mypvc.yml

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: mypvc
  annotations:
    volume.beta.kubernetes.io/storage-class: "ibmc-file-silver"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 20Gi
```

Option 3 - Connect Cloud Services using Kubernetes Secrets

ibmcloud ks cluster-service-bind <cluster_name> <namespace> <service-name>

kubectl get secret <service-name> –o yaml

secret.yml

```
apiVersion: v1
apiVersion: v1
data:
  binding: eyJkYl90eXBlIjoibW9uZ29kYiIsIm1hcHMiOltdLCJpbnN0YW5jZV9hZG1pbmlzdHJhdGlvbl9hcGkiOnsiaW5z…
RoU291cmNlPWFkbWluXHUwMDI2c3NsPXRydWUifQ==
kind: Secret
metadata:
  annotations:
    service-instance-id: 5d166698-c9b0-44b7-bce1-ffe72515f304
    service-key-id: 19b3e1b5-8a50-4fd8-93bc-ceb7879029fd
  creationTimestamp: 2018-09-04T17:47:50Z
  name: binding-mongodb-demo
  namespace: default
  resourceVersion: "354948"
  selfLink: /api/v1/namespaces/default/secrets/binding-mongodb-demo
  uid: a4258e87-b06a-11e8-8d71-120fbe0d22f8
type: Opaque
```

Option 3 - Kubernetes Secrets are encrypted

Summary

Cluster ID	6bed7717f94942c1ad2ac5f3d0
Kubernetes version	1.11.3_1524
Zones	fra02
Owner	lionel.mace@fr.ibm.com
Ingress subdomain	private-core-cluster-tbd.eu-de.containers.appdomain.cloud
Logs	Enable
Metrics	View
Key protect (Beta)	Enabled Update

Enable secret encryption

Be sure that your cluster secrets are secure by enabling encryption with the Key Protect service. With Key Protect, you can create, import, and manage encryption keys that ensure that any secrets you create going forward, are kept confidential. You can use only one root key per cluster at any time. Be sure to double check that any keys that were created prior to enabling key protect are encrypted.

Key Protect instance

secure-file-storage-kp

Encryption key

secure-file-storage-root-enckey

Option 3 – Connect to any IBM Cloud Platform Services

Compute
- Bare Metal
- Cloud Foundry Runtimes
- OpenStack VMs
- Docker Containers
- Event Driven Apps
- Blueprints (Patterns)
- CMS

Networking
- SDN
- Load Balancer
- VPN

Storage
- Block Storage
- Object Storage

Media
- CDN

Watson
- Concept Expansion
- Concept Insights
- Language Translation
- Natural Language Classifier
- Personality Insights
- Conversation
- Relationship Extraction
- Retrieve and Rank
- Speech To Text
- Text to Speech
- Visual Recognition

DevOps
- Active Deploy
- Auto-Scaling
- Delivery Pipeline
- Monitoring and Analytics
- Tracking and Plan GIT
- Image Builder
- Alert Notification

Data & Analytics
- Analytics for Apache Hadoop
- Apache Spark
- BigInsights for Apache Hadoop
- dashDB
- Cloudant NoSQL DB
- DataWorks
- Elasticsearch by Compose
- Geospatial Analytics
- IBM DB2 on Cloud
- Insights for Twitter
- Insights for Weather
- MongoDB by Compose
- PostgreSQL by Compose
- Predictive Analytics
- Redis by Compose
- SQL Database
- Streaming Analytics
- Time Series Database
- Embeddable Reporting

Private APIs
- User Defined Services
- User Defined APIs

Security
- Key Protect
- Security Groups
- IDaaS
- Firewall
- Access Trail
- Application Security Manager
- AppScan Dynamic Analyzer
- Mobile Analyzer for iOS
- AppScan Mobile Analyzer

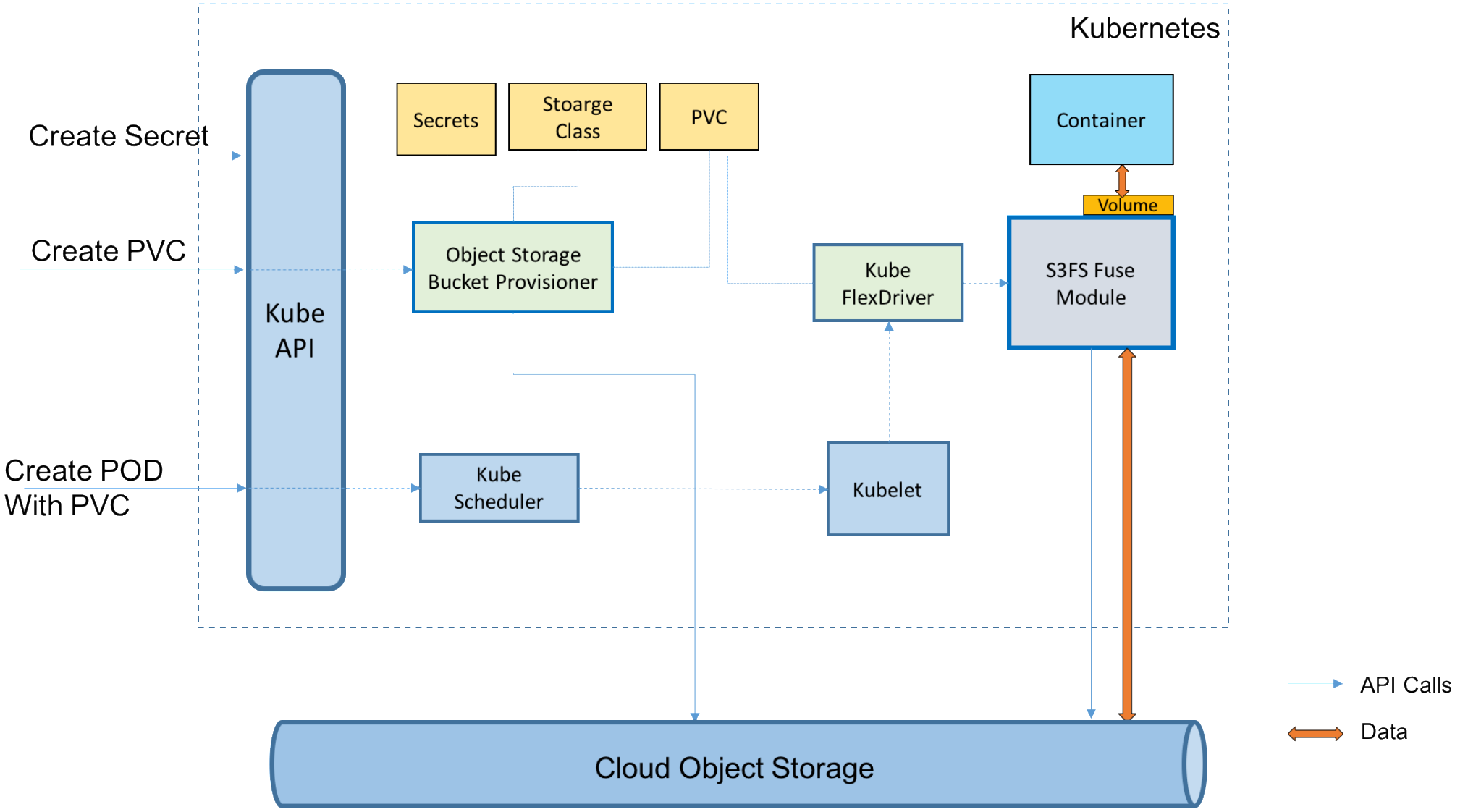
Integrate
- API Management
- Service Discovery
- Secure Gateway
- Service Proxy
- Service Broker
- Cloud Integration

IoT
- IoT Insights
- IoT Real Time Insights

Application
- Workflow
- Big Insights
- Application Server on Cloud
- Business Rules
- Data Cache
- Message Hub
- MQ Light
- Session Cache
- Workflow Scheduler

Mobile
- Push
- Mobile Client Access
- Mobile Data
- Quality Assurance
- IBM Push Notifications
- Mobile Application Security

Cloud Object Storage plug-in



https://github.com/IBM/ibmcloud-object-storage-plugin

Kubernetes Service

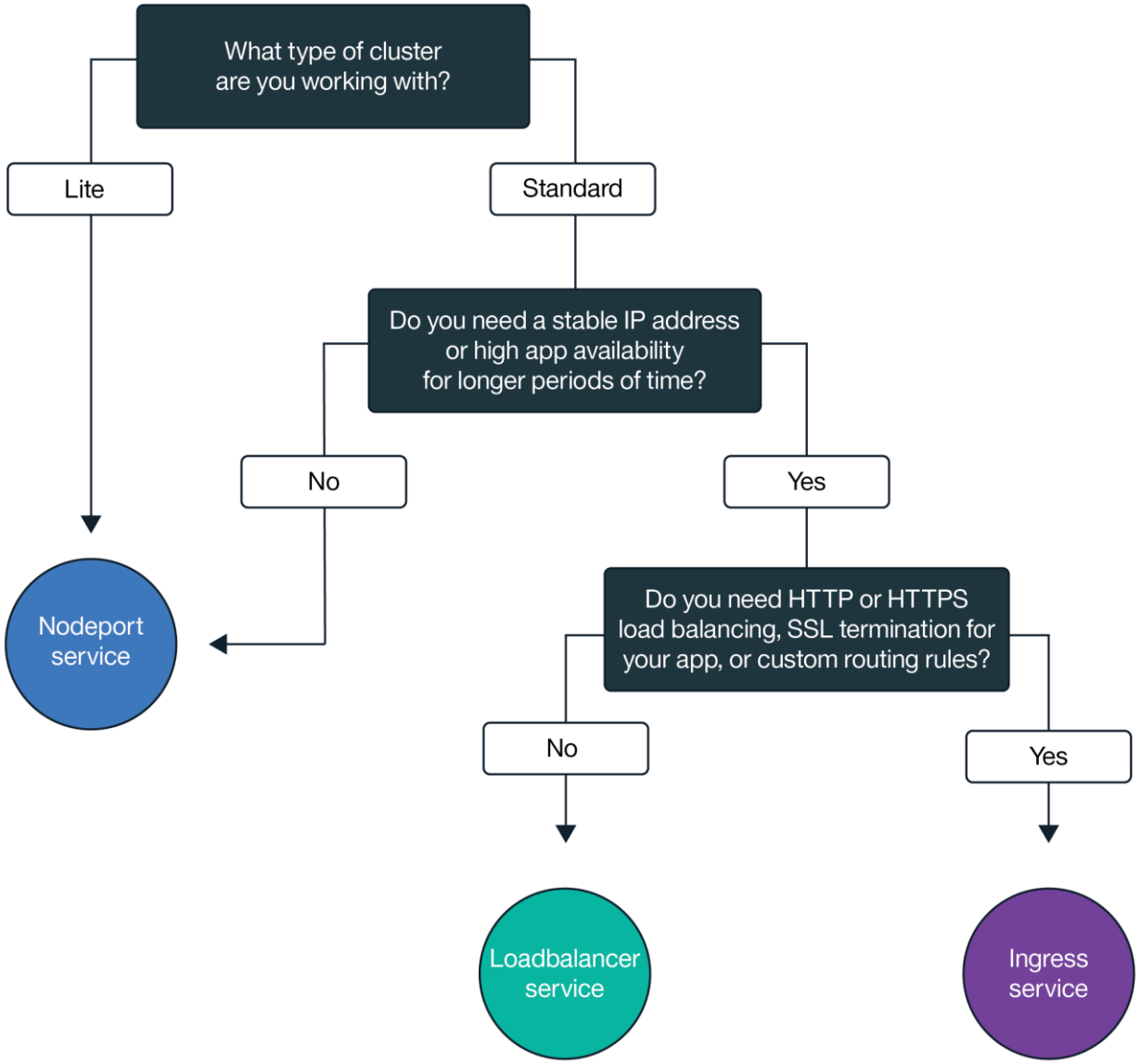
Expose your application

Kubernetes Service

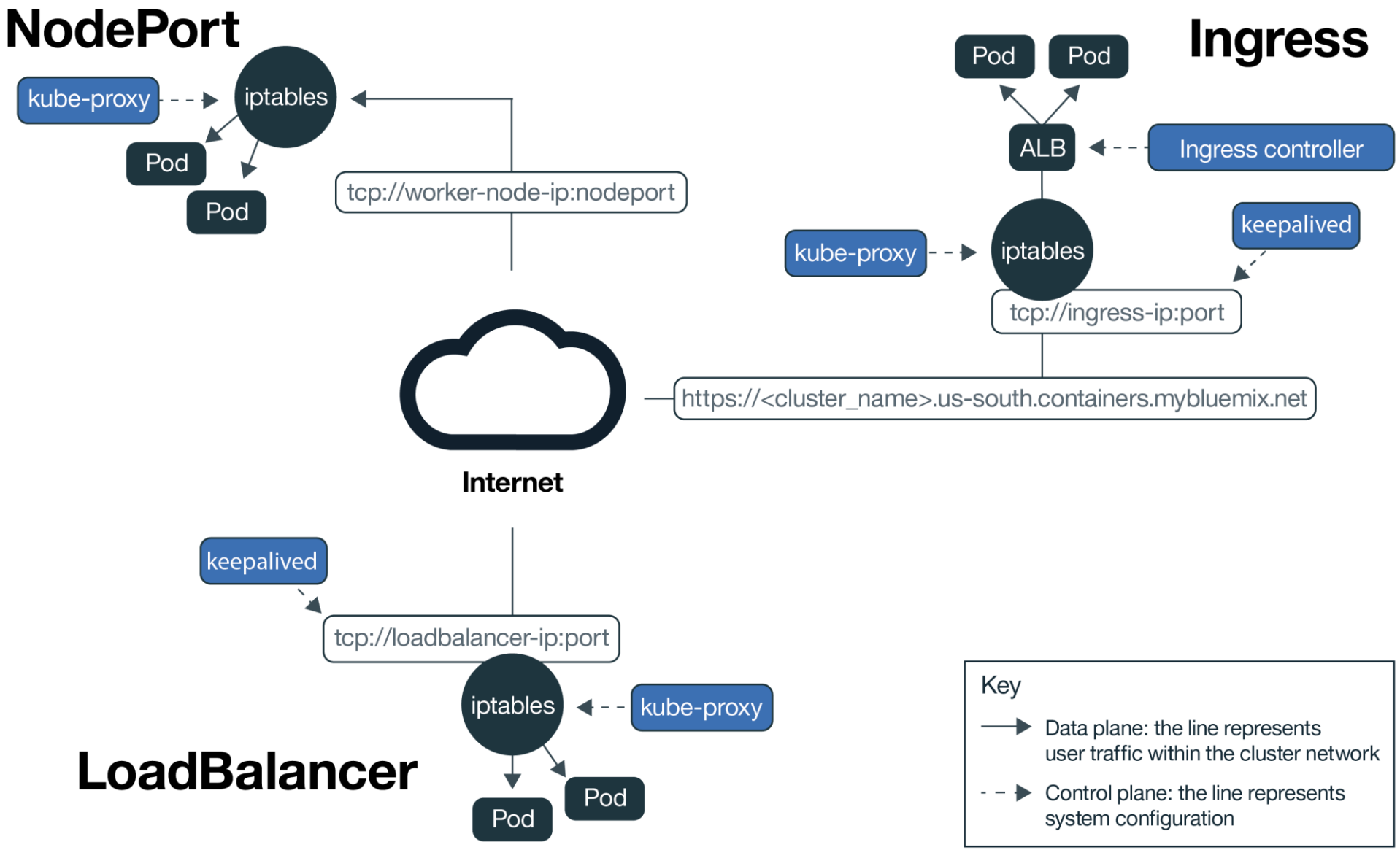
- An abstraction layer which defines a logical set of Pods and enables external traffic exposure, load balancing and service discovery for those Pods.
- Services enable a loose coupling between dependent Pods.
- Although Pods each have a unique IP address, those IPs are not exposed outside the cluster without a Service.
- Services match a set of Pods using labels and selectors, a grouping primitive that allows logical operation on objects in Kubernetes.

```
apiVersion: v1
kind: Service
metadata:
  name: mytodos
  labels:
    app: mytodos
    tier: frontend
spec:
  ports:
  - protocol: TCP
    port: 8080
  selector:
    app: mytodos
    tier: frontend
```

Choose the best networking option to expose service



Allowing public access to apps



Benefits of Ingress Controller

- Special **LoadBalancer-type** service automatically deployed with the cluster.
- Use the reserved public IP, making it highly available.
- Automatically register a **unique public DNS entry with CA signed certificate** that resolves to the public IP address for my Ingress controller, similar to <my-cluster-name>.<region>.containers.mybluemix.net.
- **NGINX-based container deployment** that can be used to expose one or more services to the Internet.
- Certificate stored as a Kubernetes secret in the “default” namespace and can be used to terminate TLS connections for L7 routing.

Use Ingress Annotations

- Levera Ingress Annotation
- Exemple: Force the use of https if the request is http

```
apiVersion: v1
kind: policy
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: mytodos-ingress
  annotations:
    ingress.bluemix.net/redirect-to-https: "True"
spec:
  tls:
  - hosts:
    - <cluster-name>.eu-de.containers.appdomain.cloud
    secretName: <cluster-name>.
  rules:
  - host: <cluster-name>.eu-de.containers.appdomain.cloud
    http:
      paths:
      - path: /
        backend:
          serviceName: mytodos
          servicePort: 8080
```

Securing Containers

Secure compute hosts

Built-in security and isolation

Hosted secured **Private image Registry**

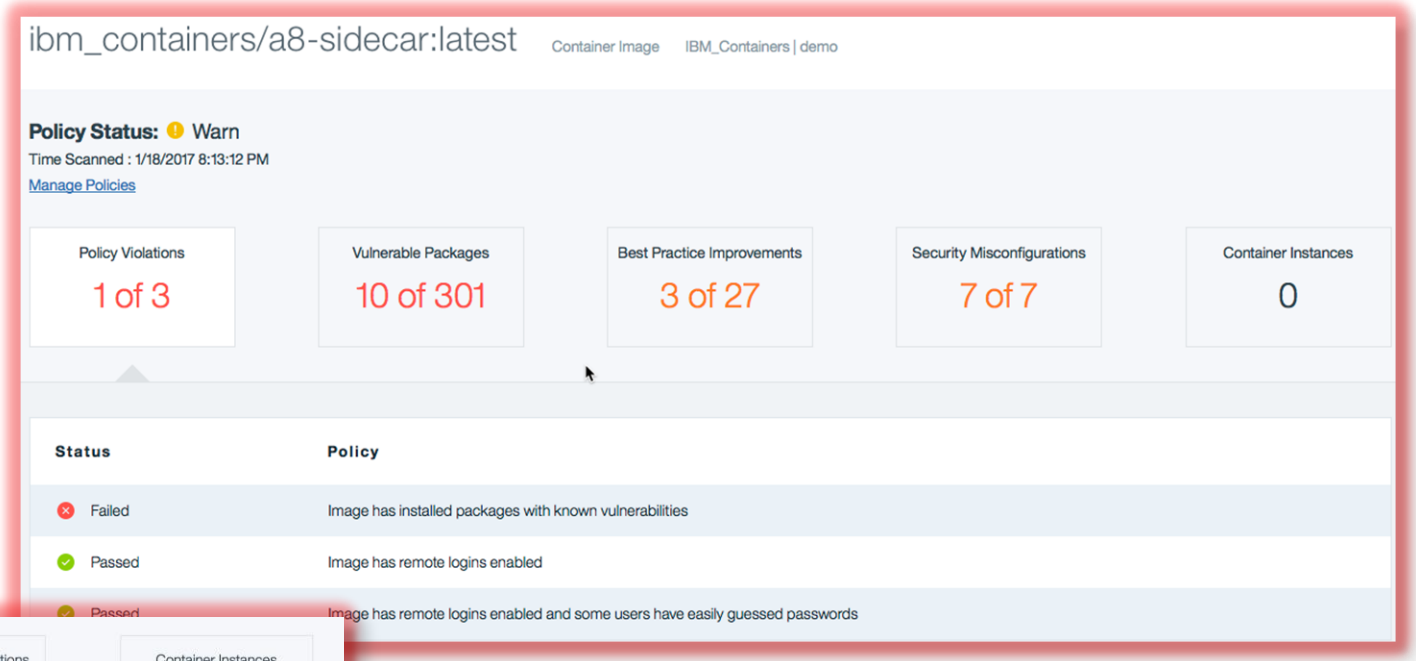
Private network overlays

Automatic **Vulnerability scanning**

https://console.bluemix.net/docs/services/Registry/registry_trusted_content.html#registry_trustedcontent

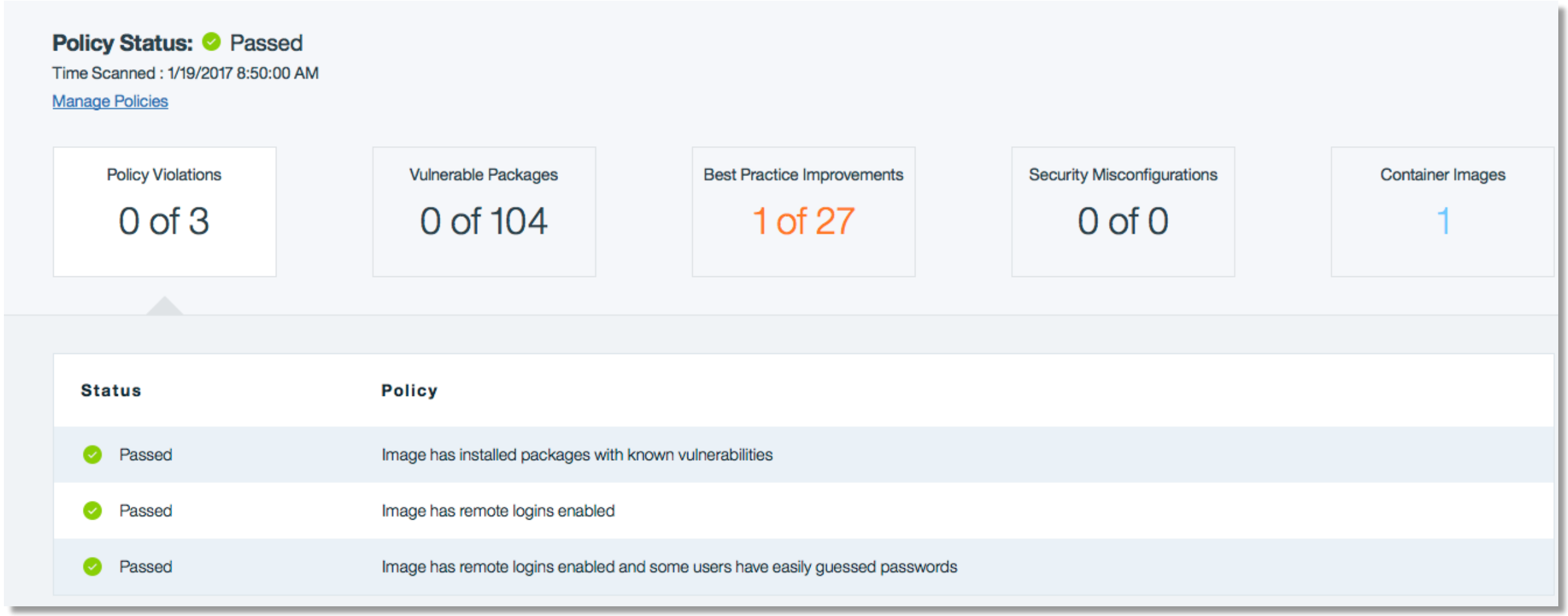
Vulnerability Advisor

Policy Violations



Vulnerable Packages

Vulnerability Advisor – Live Container Scanning



Integration between Vulnerability Advisor and IBM X-Force

				Description	Corrective Action
				Several security issues were fixed in curl.	Upgrade libcurl3 to at least version 7.35.0-1ubuntu2.10
				Several security issues were fixed in Python.	Upgrade libpython3.4-stdlib to at least version 3.4.3-1ubuntu1~14.04.5, Upgrade python3.4 to at least version 3.4.3-1ubuntu1~14.04.5, Upgrade libpython3.4-minimal to at least version 3.4.3-1ubuntu1~14.04.5, Upgrade python3.4-minimal to at least version 3.4.3-1ubuntu1~14.04.5
				The GD library could be made to crash or run programs if it processed aspecially crafted image file.	Upgrade libgd3 to at least version 2.1.0-3ubuntu0.5
Medium	apt	3156-1	CVE-2016-1252	An attacker could trick APT into installing altered packages.	Upgrade apt to at least version 1.0.1ubuntu2.17
Medium	vim-common	3139-1	CVE-2016-1248	Vim could be made run programs as your login if it opened a speciallycrafted file.	Upgrade vim-common to at least version 2:7.4.052-1ubuntu3.1
Medium	tar	3132-1	CVE-2016-6321	tar could be made to overwrite files.	Upgrade tar to at least version 1.27.1-1ubuntu0.1
Low	libdbus-1-3	3116-1	CVE-2015-0245	Several security issues were fixed in DBus.	Upgrade libdbus-1-3 to at least version 1.6.18-0ubuntu4.4

http://www-03.ibm.com/security/xforce/

Container Image Security Enforcement

ibmcloud-image-enforcement 0.2.2 IBM

Chart Details

Container Image Security Enforcement

This chart installs Container Image Security Enforcement for IBM Cloud Kubernetes Service in your cluster.

Prerequisites

- Kubernetes v1.9+
- Tiller v2.8+

https://console.bluemix.net/containers-kubernetes/solutions/helm-charts/ibm/ibmcloud-image-enforcement

Kubernetes Service

High Availability

Scaling Services

Scaling is accomplished by changing the number of replicas in a Deployment.

Scaling up a Deployment will ensure new Pods are created and scheduled to Nodes with available resources.

Scaling down will reduce the number of Pods to the new desired state. Kubernetes also supports autoscaling of Pods.

Services have an integrated load-balancer that will distribute network traffic to all Pods of an exposed Deployment.

kubectl scale
--replicas=2 deployment/mytodos

```
apiVersion: v1
kind: Deployment
metadata:
 name: mytodos
spec:
 replicas: 2
 template
  metadata:
   labels:
    app: mytodos
    tier: frontend
  spec:
   containers:
   - name: mytodos
    image: registry.eu-
de.bluemix.net/namespace/mytodos:1
    imagePullPolicy: Always
    resources:
     requests:
      cpu: 100m
      memory: 100Mi
```

Horizontal Pod Autoscaler HPA

kubectl apply –f hpa.yaml

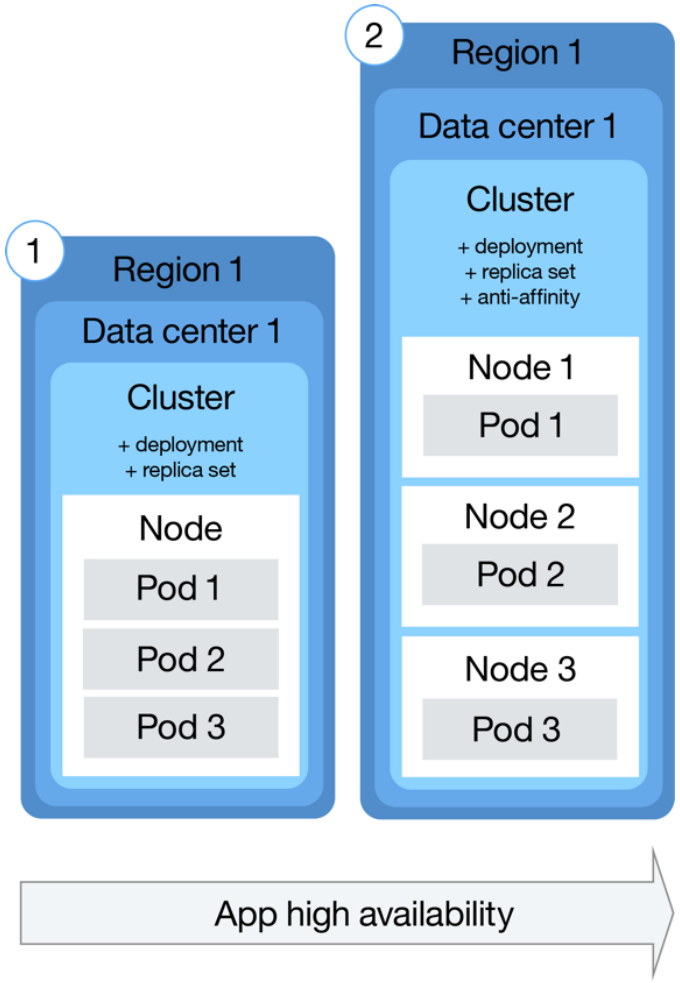
```
apiVersion: autoscaling/v2beta1
kind: HorizontalPodAutoscaler
metadata:
  name: mytodos-scaler
spec:
  scaleTargetRef:
    apiVersion: extensions/v1beta1
    kind: Deployment
    name: mytodos
  minReplicas: 2
  maxReplicas: 10
  metrics:
  - type: Resource
    resource:
      name: cpu
      targetAverageUtilization: 60
  - type: Resource
    resource:
      name: memory
      targetAverageUtilization: 55
```

High Availability

Scale Pods via Replica Sets
Use deployments and replica sets to deploy your app
Include enough replicas for your app's workload

Scale Nodes
Spread pods across multiple nodes (anti-affinity)
Access nodes via external load balancers

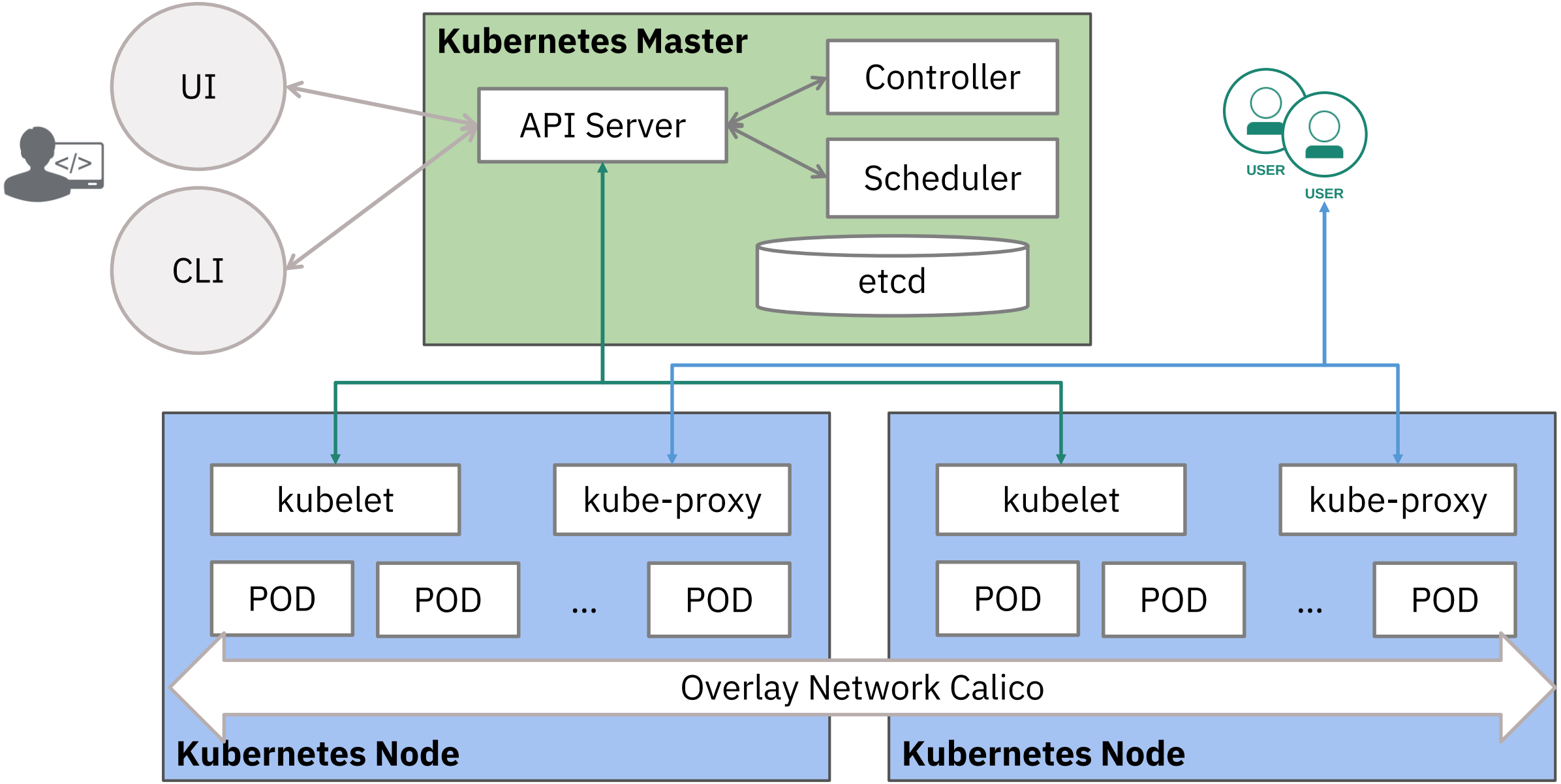
Use multiple zone cluster
Implement HA and DR use cases



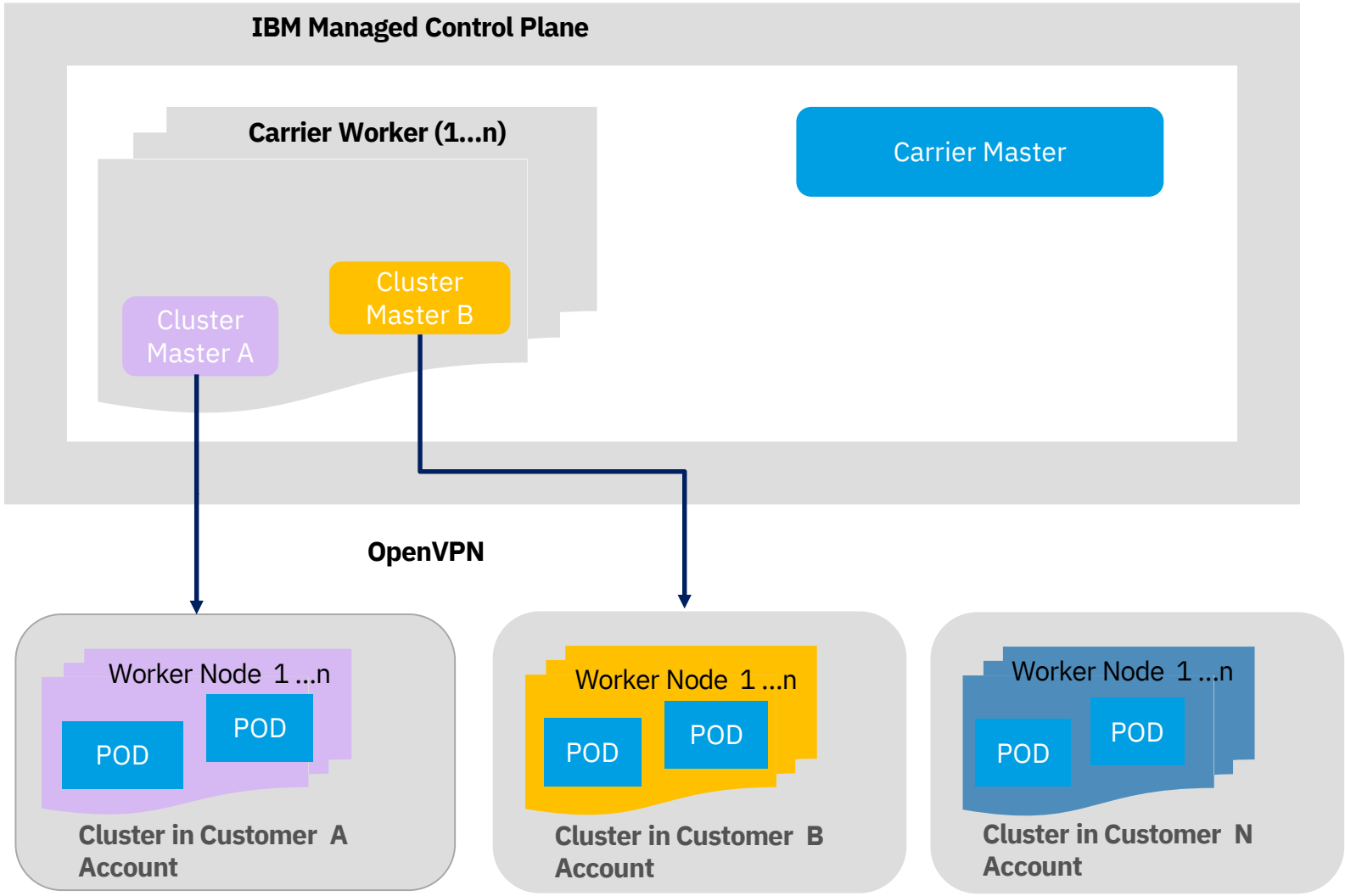
Kubernetes Service

Networking

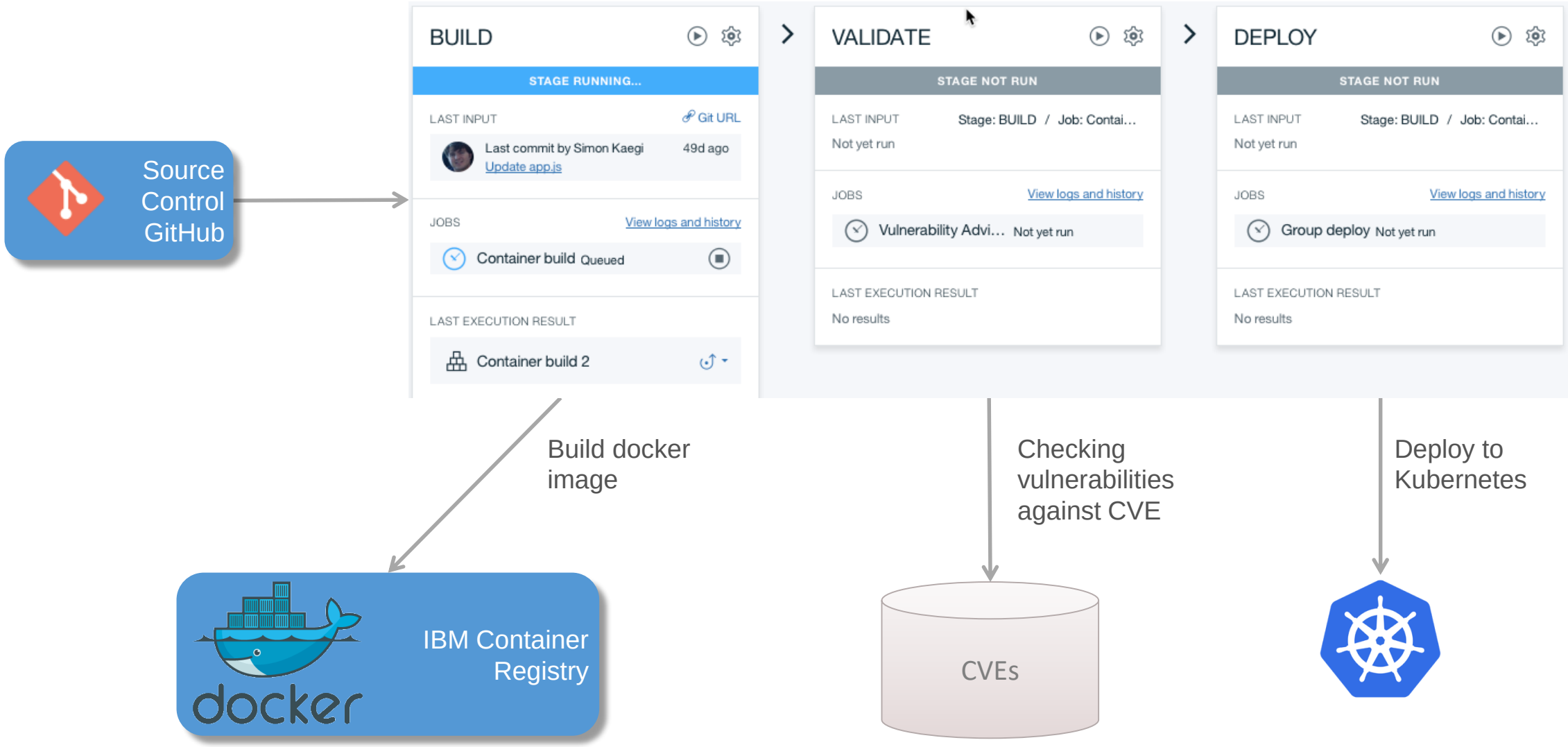
Kubernetes Architecture



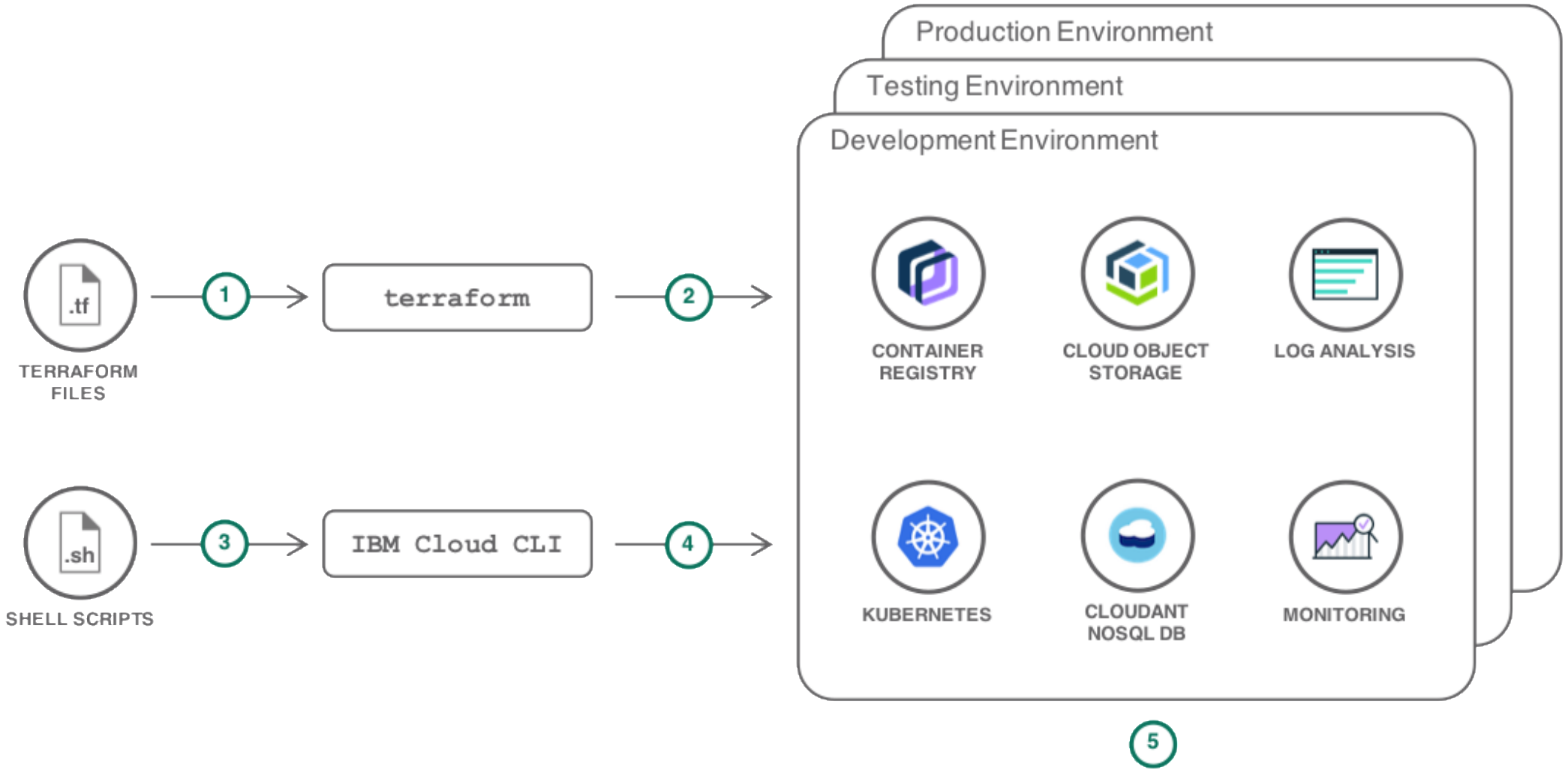
IBM Cloud Kubernetes Service – Topology



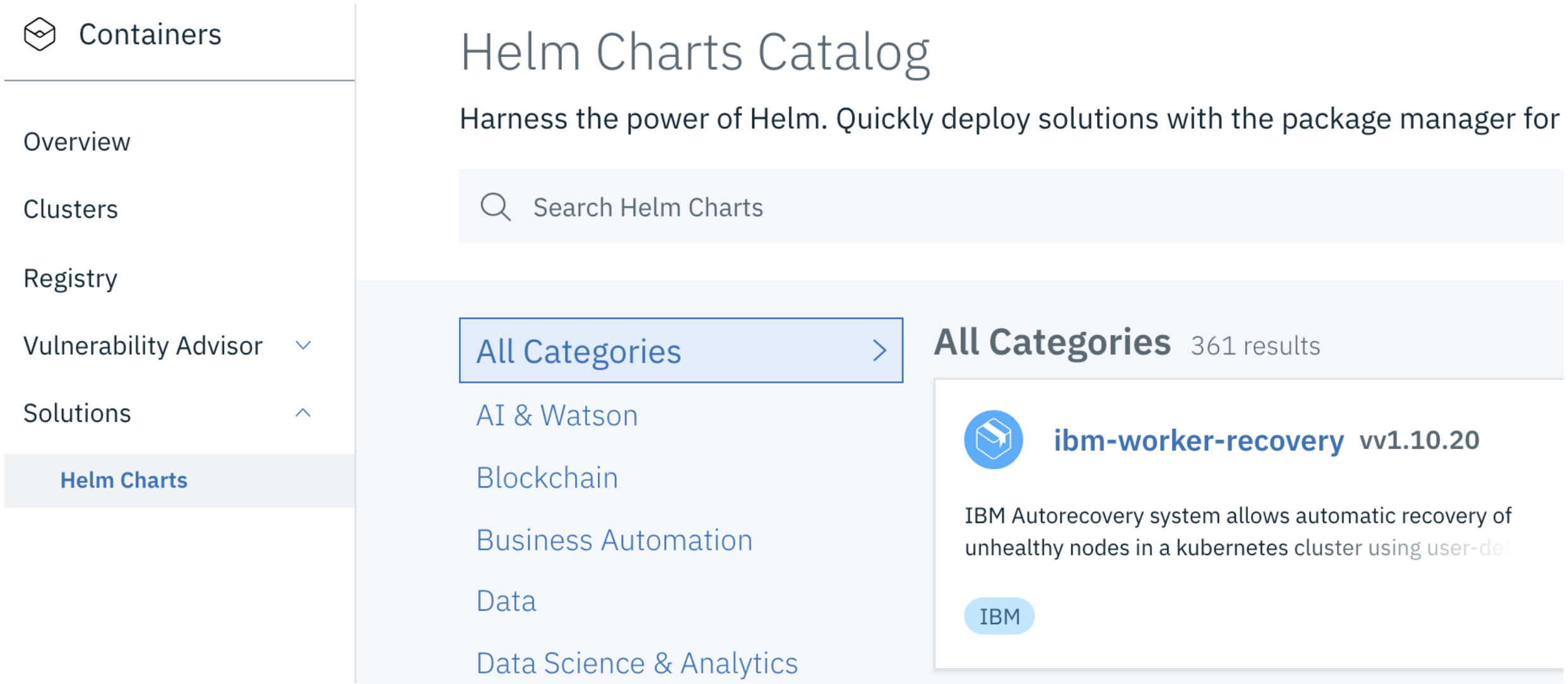
Open Toolchain with Delivery Pipeline for Kubernetes



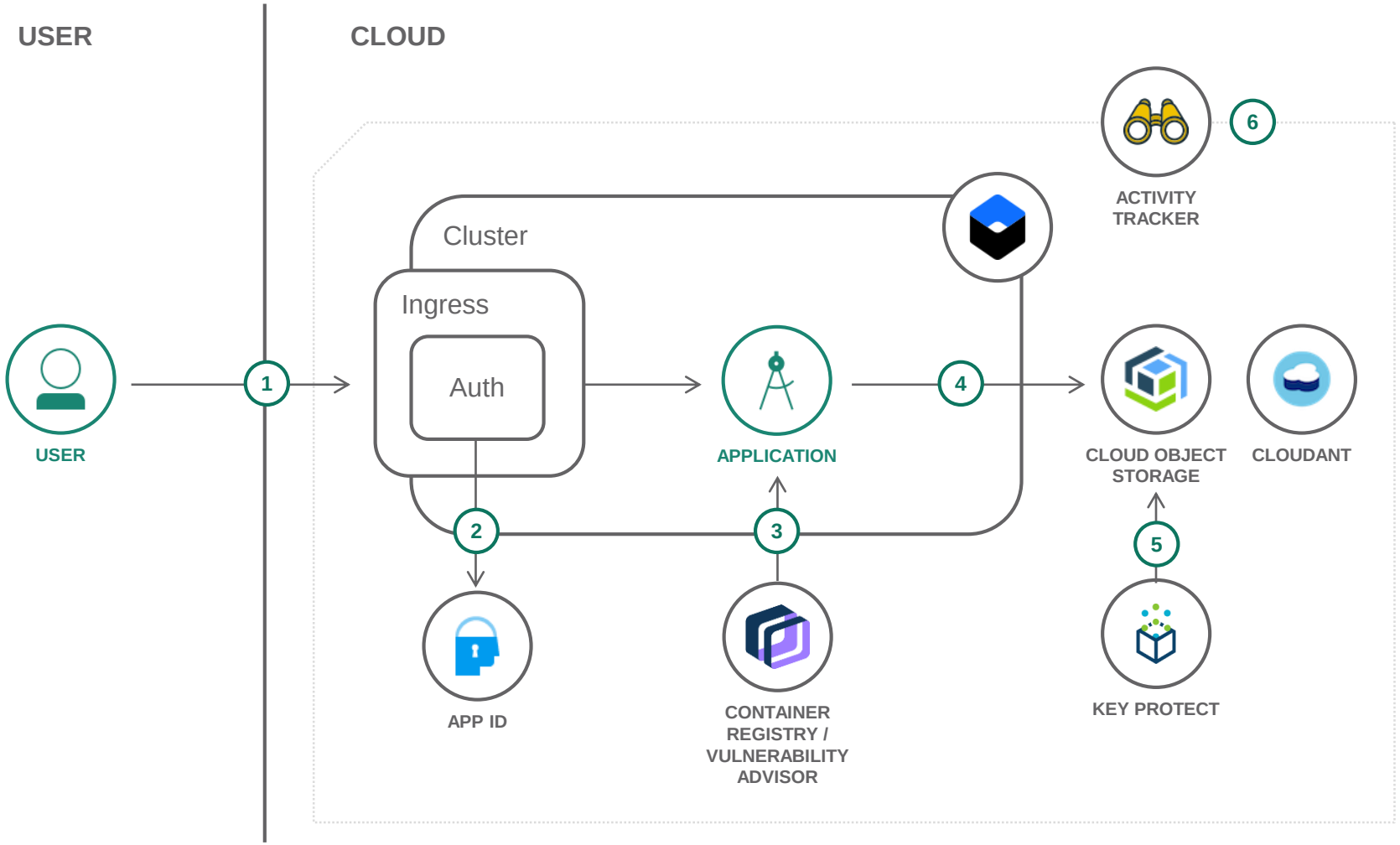
Terraform

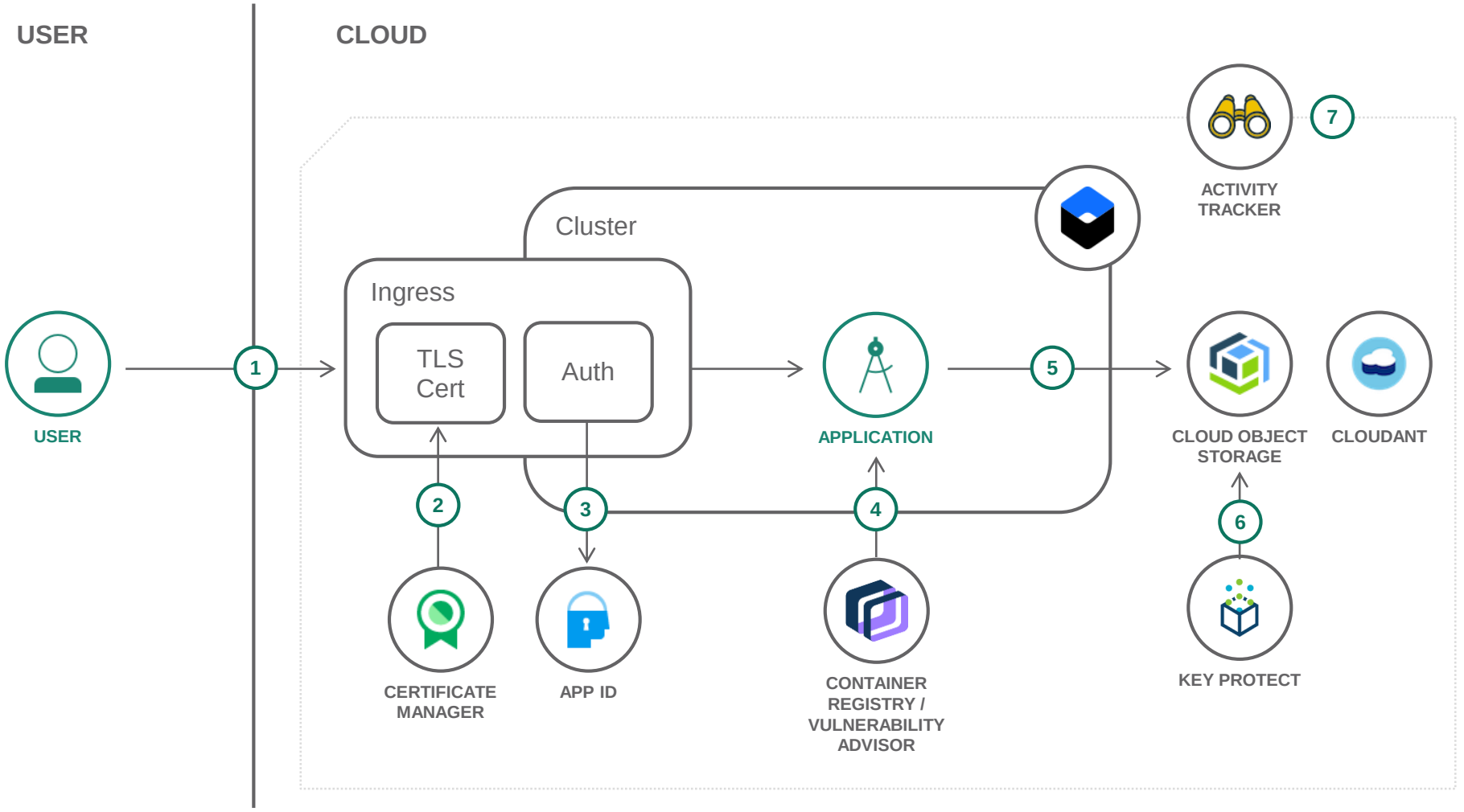

Production Environment
Testing Environment
Development Environment
.tf
TERRAFORM FILES
1
terraform
2
CONTAINER REGISTRY
CLOUD OBJECT STORAGE
LOG ANALYSIS
.sh
SHELL SCRIPTS
3
IBM Cloud CLI
4
KUBERNETES
CLOUDANT NOSQL DB
MONITORING
5

Helm Charts Catalog



https://console.bluemix.net/containers-kubernetes/solutions/helm-charts


USER
CLOUD
ACTIVITY TRACKER
6
Cluster
Ingress
Auth
USER
1
APPLICATION
4
CLOUD OBJECT STORAGE
CLOUDANT
2
3
5
APP ID
CONTAINER REGISTRY / VULNERABILITY ADVISOR
KEY PROTECT


USER
CLOUD
ACTIVITY TRACKER
7
Cluster
Ingress
TLS Cert
Auth
USER
1
APPLICATION
5
CLOUD OBJECT STORAGE
CLOUDANT
2
3
4
6
CERTIFICATE MANAGER
APP ID
CONTAINER REGISTRY / VULNERABILITY ADVISOR
KEY PROTECT

Kubernetes Service

Hands-on Labs

Pre-Requisites

1. Create an IBM Cloud account http://bluemix.net

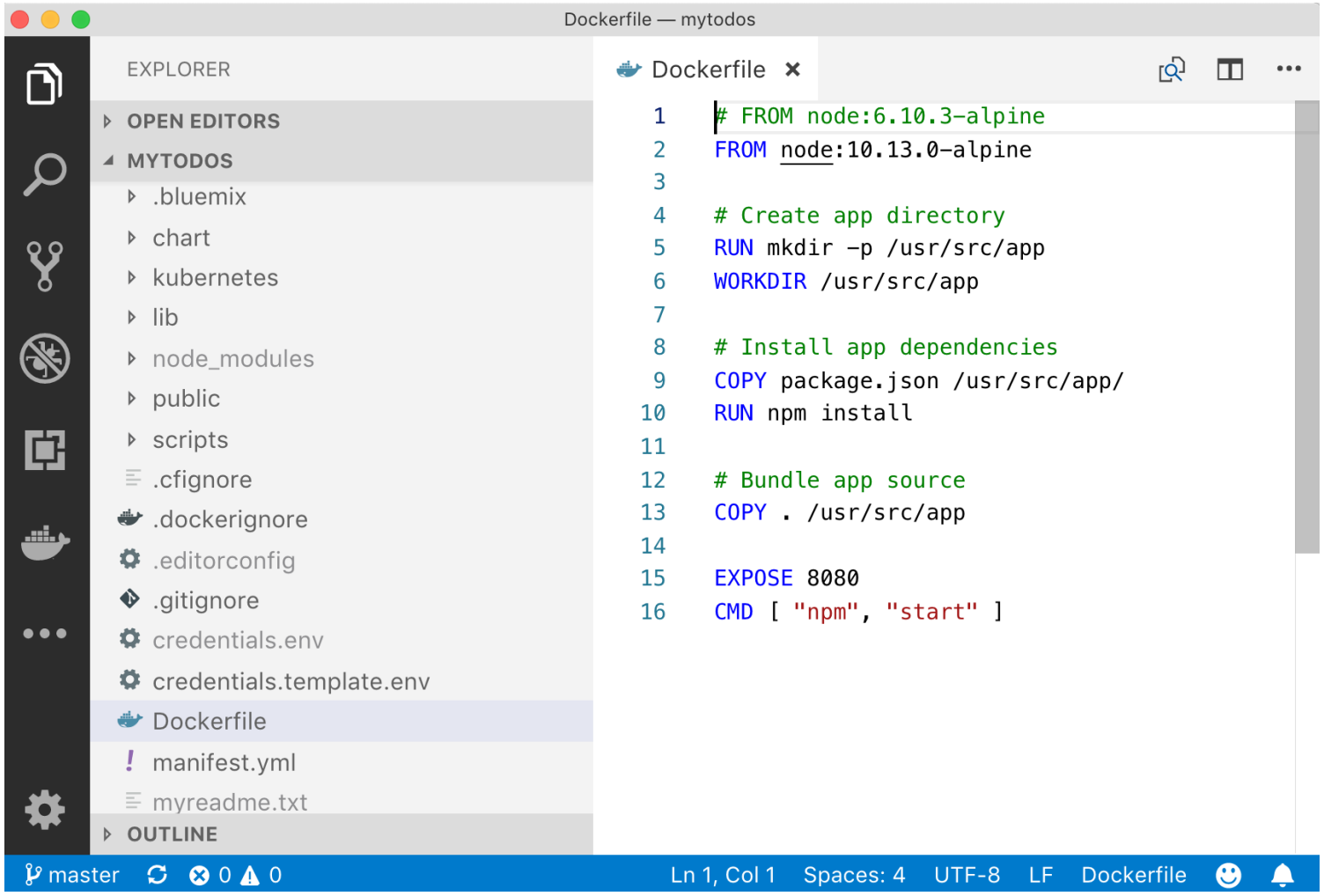
2. Create a free Kubernetes cluster in the Console
   https://console.bluemix.net/containers-kubernetes/clusters

3. Install Docker on the machine
   Mac (https://docs.docker.com/docker-for-mac/)
   Windows 10 (https://docs.docker.com/docker-for-windows/)
   Windows 7 (https://docs.docker.com/toolbox/overview/)
   OpenClient RedHat7 (https://docs.docker.com/install/linux/docker-ce/centos/)
   OpenClient RedHat6

4. Install the IBM Cloud Command Line (CLI)
   https://console.bluemix.net/docs/cli/reference/bluemix_cli/get_started.html#getting-started

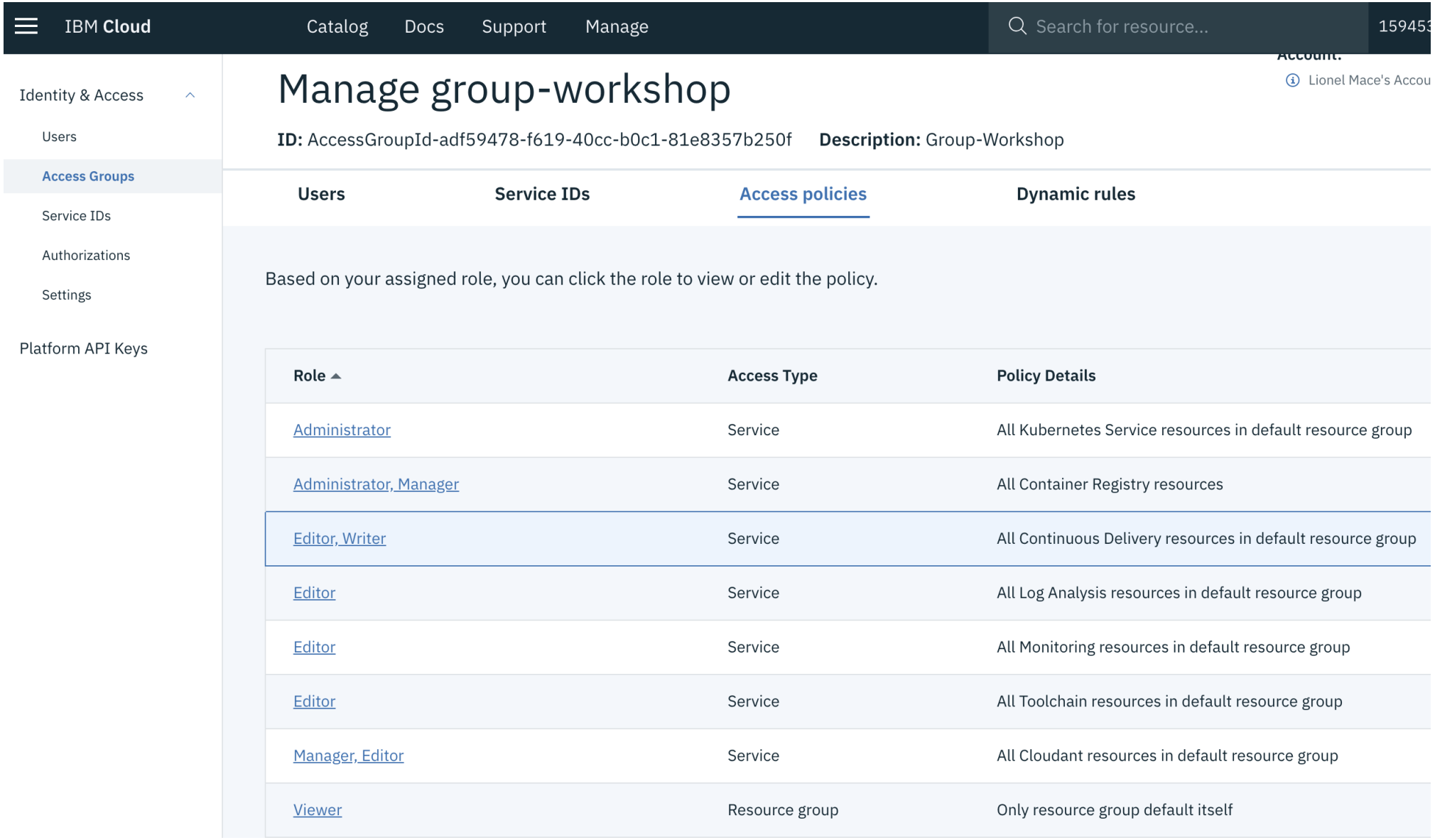
5. Install the kubectl command line
   https://kubernetes.io/docs/tasks/tools/install-kubectl/#install-kubectl-binary-via-curl

Recommendation: Use a proper IDE such as VS Code

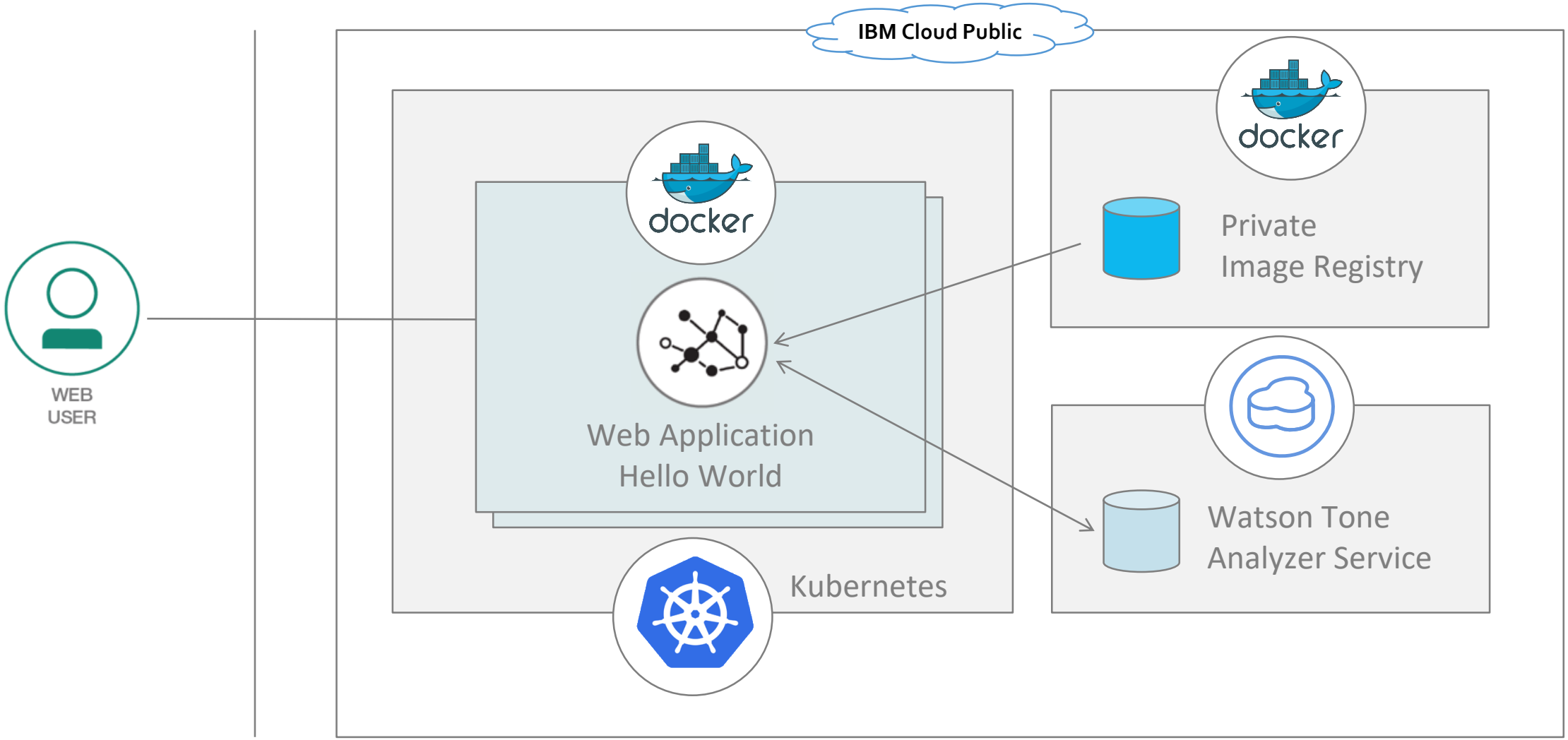


https://code.visualstudio.com/download

IAM Access


IBM Cloud
Catalog
Docs
Support
Manage
Search for resource...
Identity & Access
Users
Access Groups
Service IDs
Authorizations
Settings
Platform API Keys
Manage group-workshop
ID: AccessGroupId-adf59478-f619-40cc-b0c1-81e8357b250f
Description: Group-Workshop
Users
Service IDs
Access policies
Dynamic rules
Based on your assigned role, you can click the role to view or edit the policy.
Role
Access Type
Policy Details
Administrator
Service
All Kubernetes Service resources in default resource group
Administrator, Manager
Service
All Container Registry resources
Editor, Writer
Service
All Continuous Delivery resources in default resource group
Editor
Service
All Log Analysis resources in default resource group
Editor
Service
All Monitoring resources in default resource group
Editor
Service
All Toolchain resources in default resource group
Manager, Editor
Service
All Cloudant resources in default resource group
Viewer
Resource group
Only resource group default itself

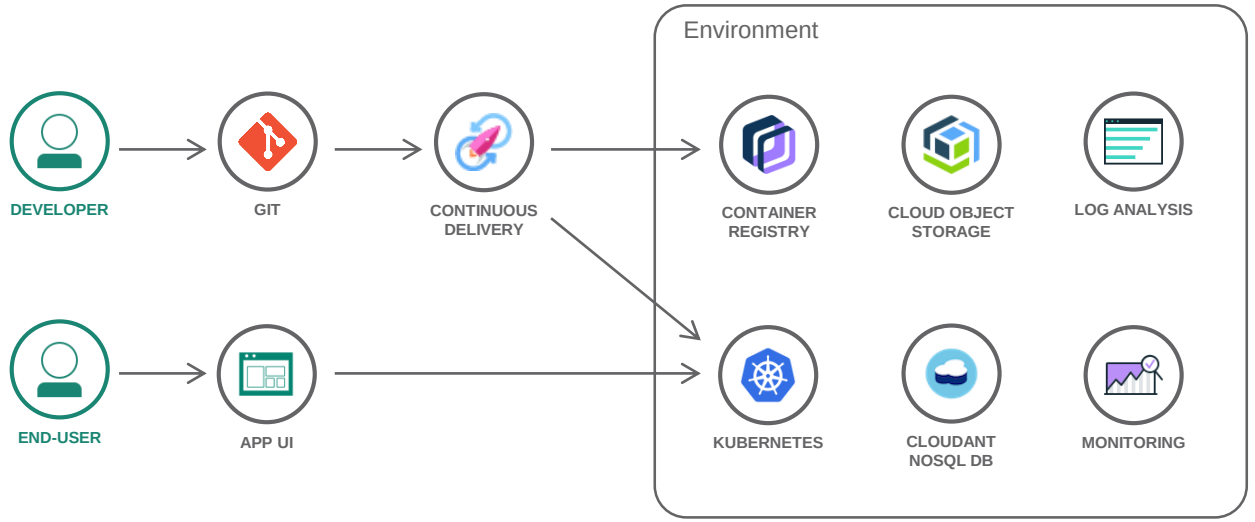
Lab 1 – Deploy Hello World… Watson in the Cluster



Tutorial: Creating Clusters
Tutorial: apps into clusters

ibm.biz/kubelabhello

Lab 2 – Deploy Apps with DevOps Continuous Delivery

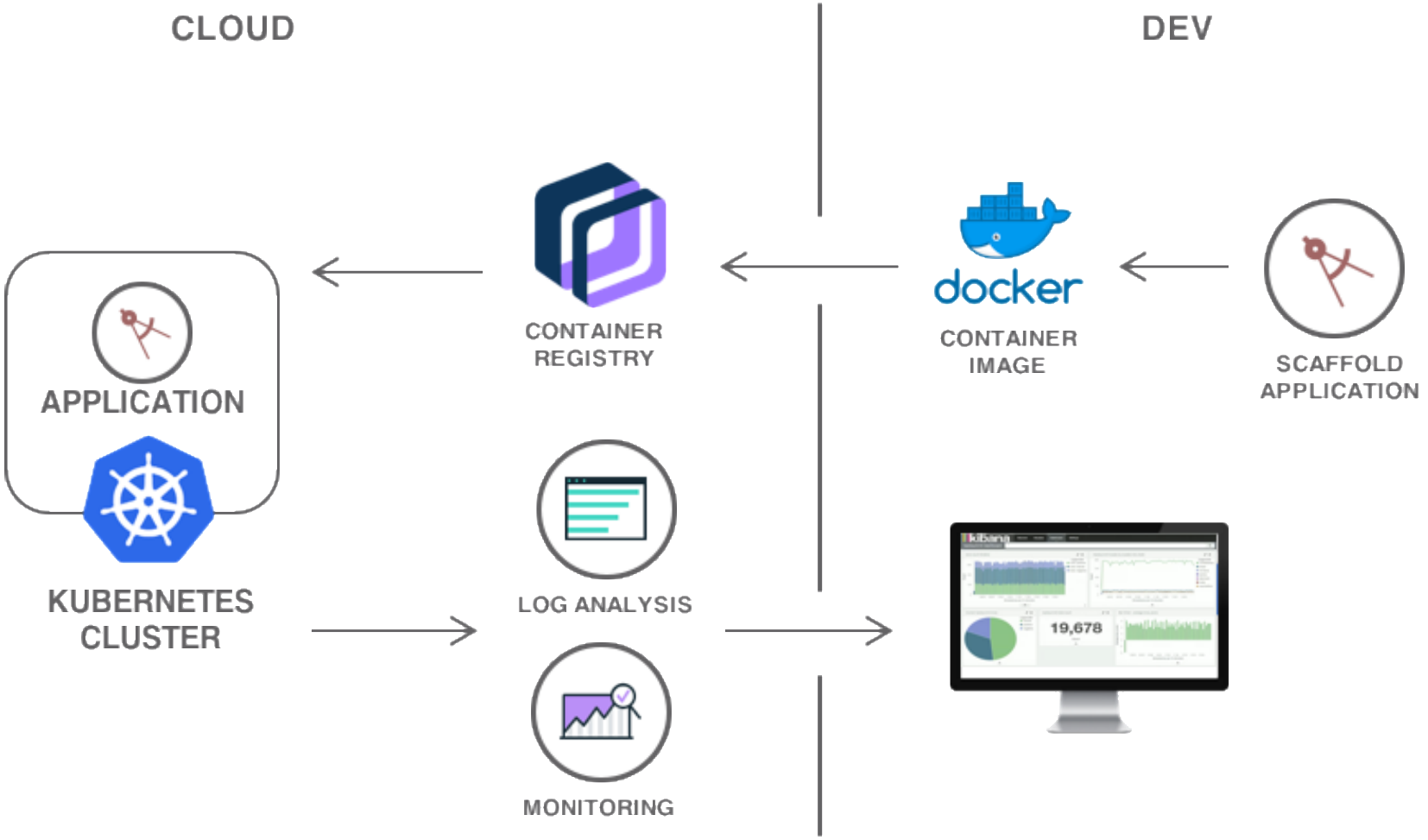


Task 1 Create Toolchain
Task 2 Run Toolchain
Task 3 Commit Changes
~~Task 4 Slack~~
Task 5 Clone Stage
~~Task 6 Cloud Private~~
~~Task 7 Cleanup~~

create an open toolchain to develop a simple "Hello World" Javascript app,
package it into a Docker container
deploy the app to a Kubernetes cluster using Helm charts.

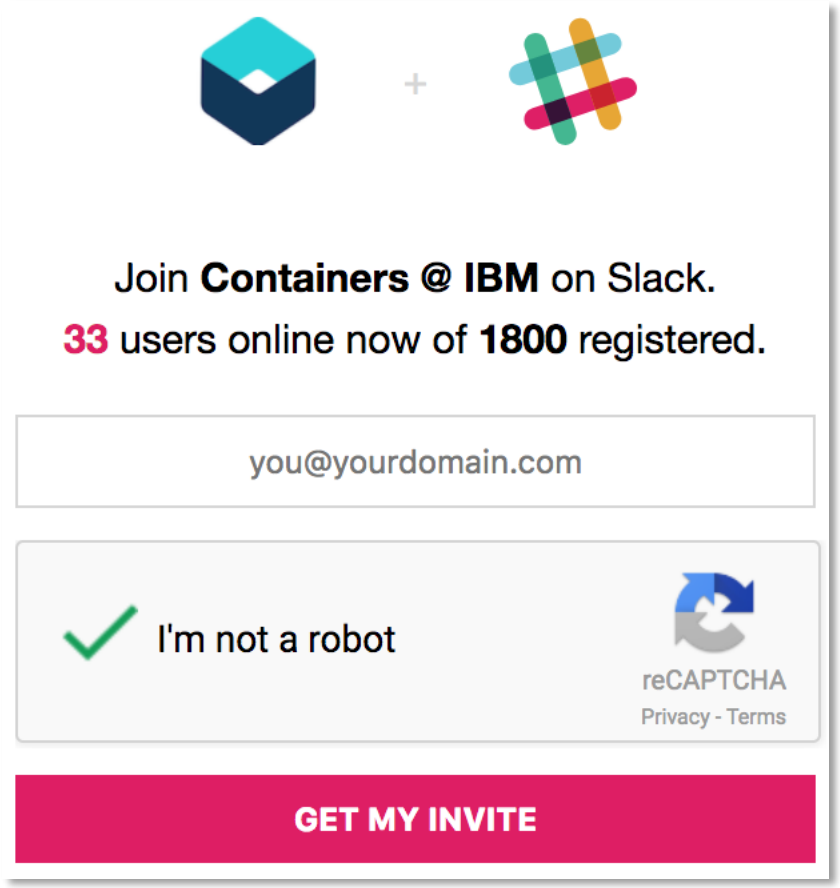
ibm.biz/kubelabdevops

Lab 3 - Analyze logs & monitor the health of Kubernetes Apps



ibm.biz/kubelabmonitoring

Reach out to the IKS community via Slack



Public IBM Slack to invite external developers

https://bxcs-slack-invite.mybluemix.net

slack

Great articles

Online Documentation
https://console.bluemix.net/docs/containers/container_index.html

5 Great Articles Kubernetes and Networking
https://www.ibm.com/blogs/bluemix/2017/05/kubernetes-and-bluemix-container-based-workloads-part1

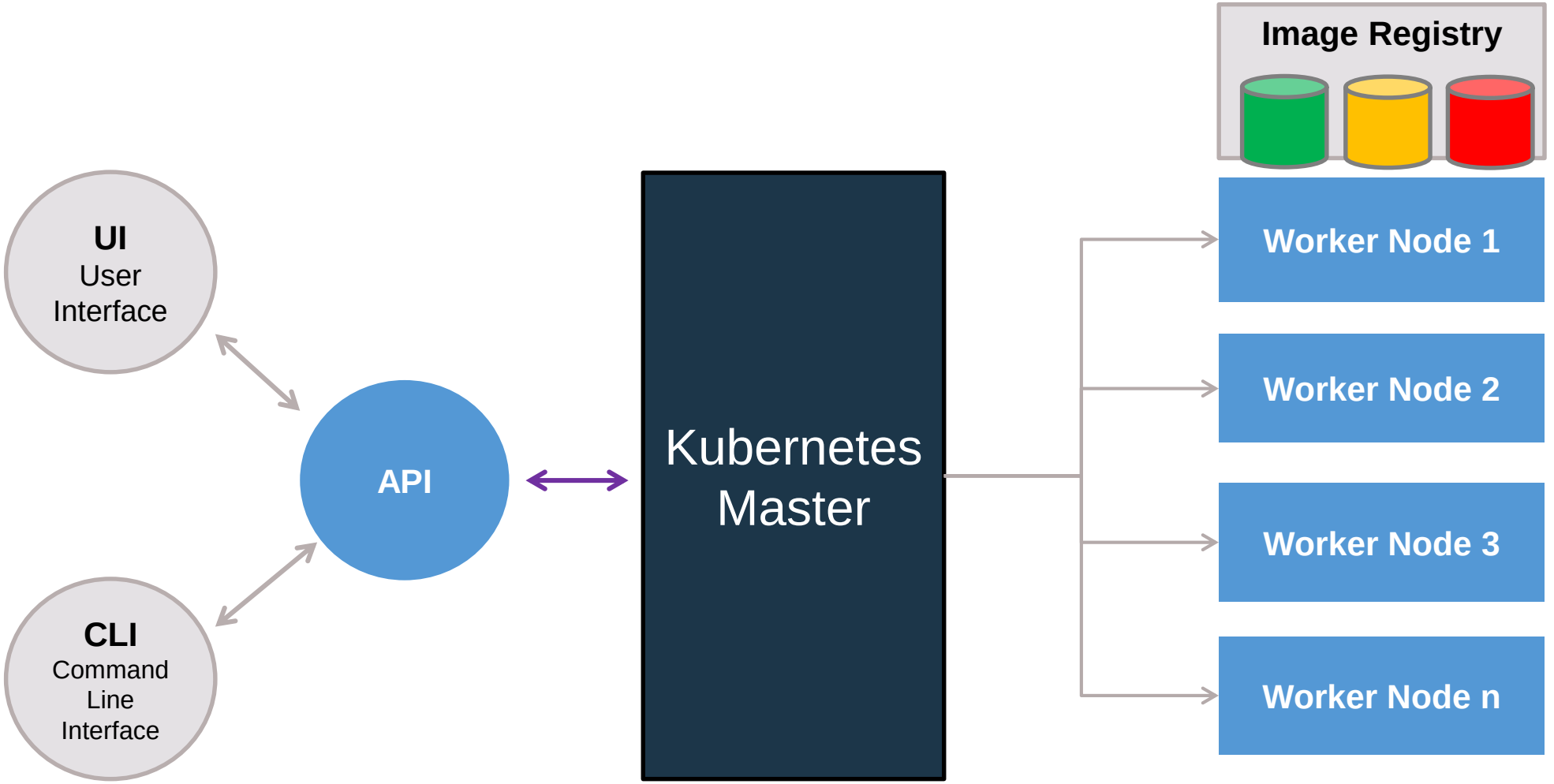
Securing Containers in IKS
https://developer.ibm.com/dwblog/2018/securing-containers-iks-kubernetes/
https://www.ibm.com/blogs/bluemix/2018/06/pod-security-policies-ibm-cloud-kubernetes-service/

Deployment Patterns for Maximizing Throughput and Availability
https://www.ibm.com/blogs/bluemix/2018/10/ibm-cloud-kubernetes-service-deployment-patterns-for-maximizing-throughput-and-availability

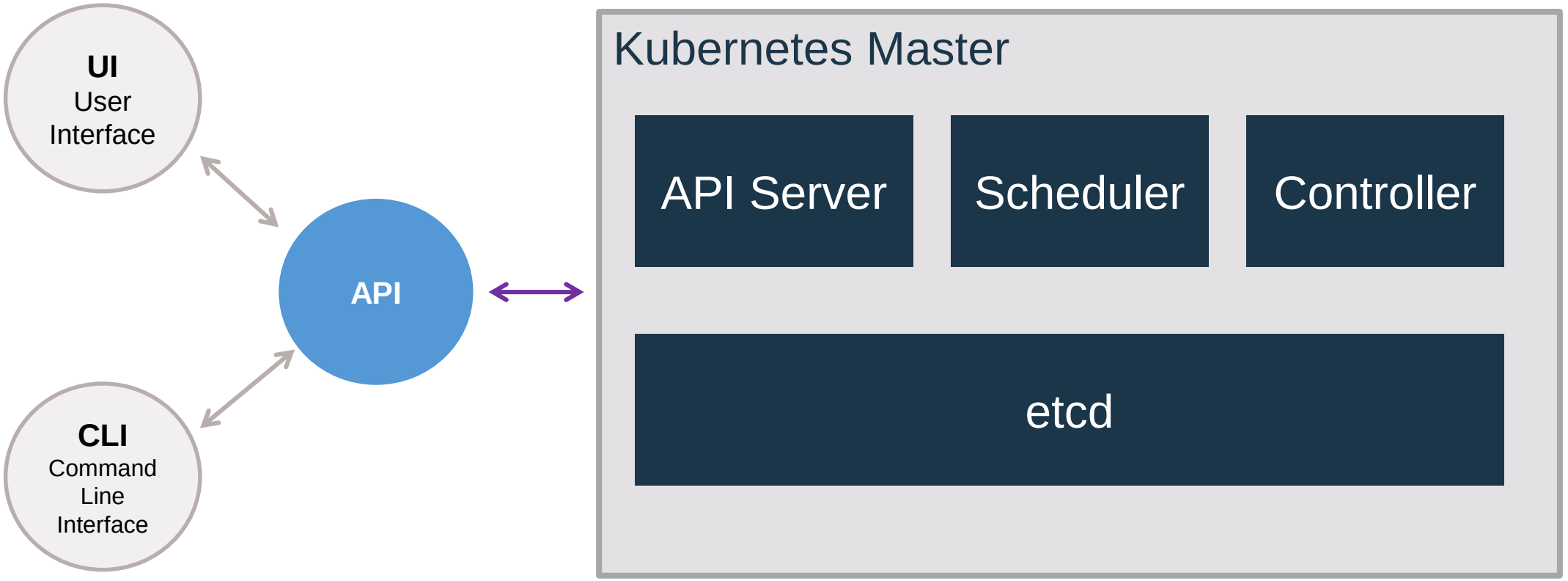
Ingress Useful commands

ibmcloud ks cluster-get <cluster-name> |grep Ingress	Get the ingress hostname
ibmcloud ks albs --cluster <cluster-name>	which ALB is listening on what IP address
kubectl get pods -n kube-system |grep alb	Get the IDs of the ALB pods in your cluster
kubectl logs <ingress_pod_ID> nginx-ingress -n kube-system	Pick the ALB you want to check the logs for
kubectl get ing	List ingress

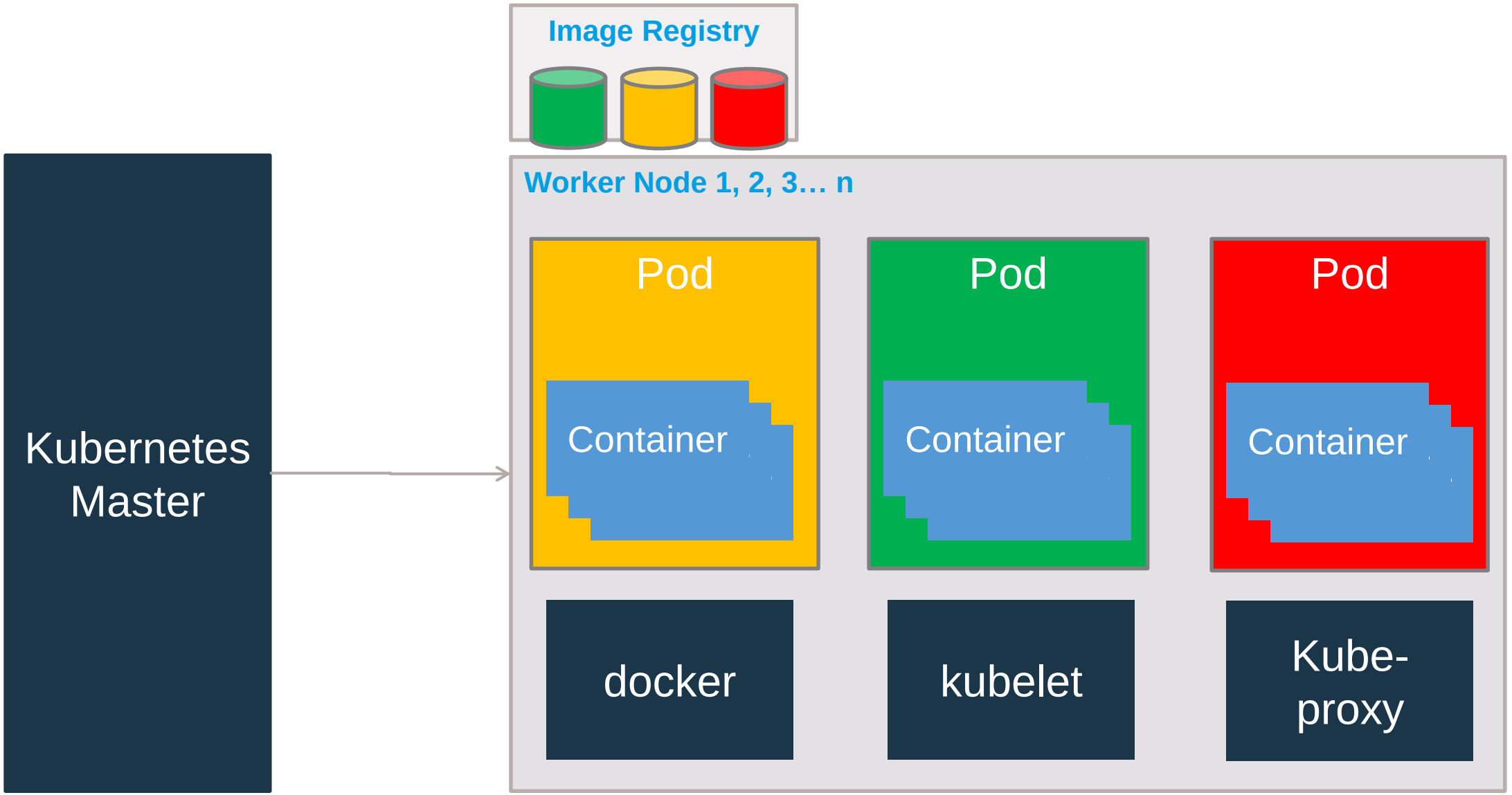
Kubernetes Architecture



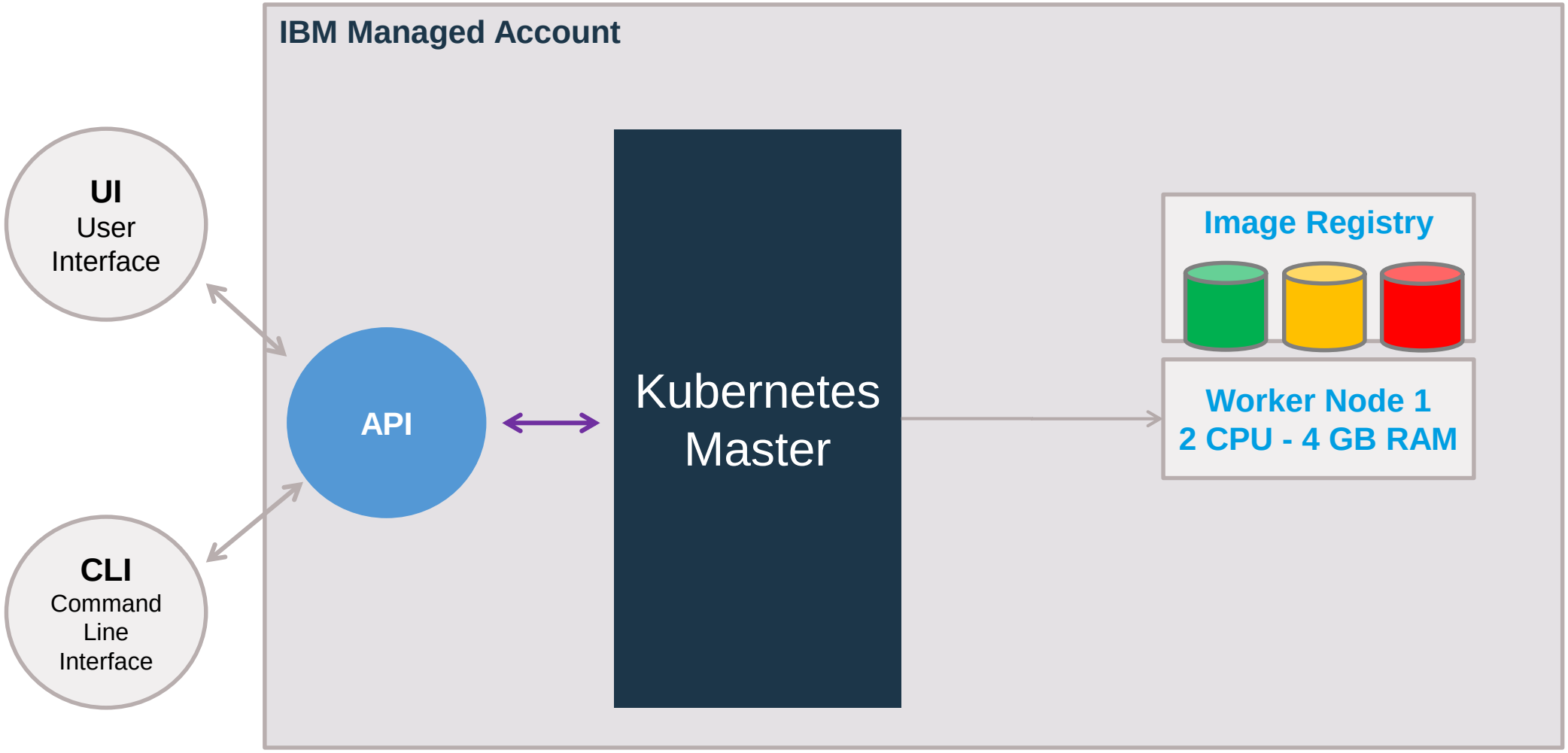
Kubernetes Architecture



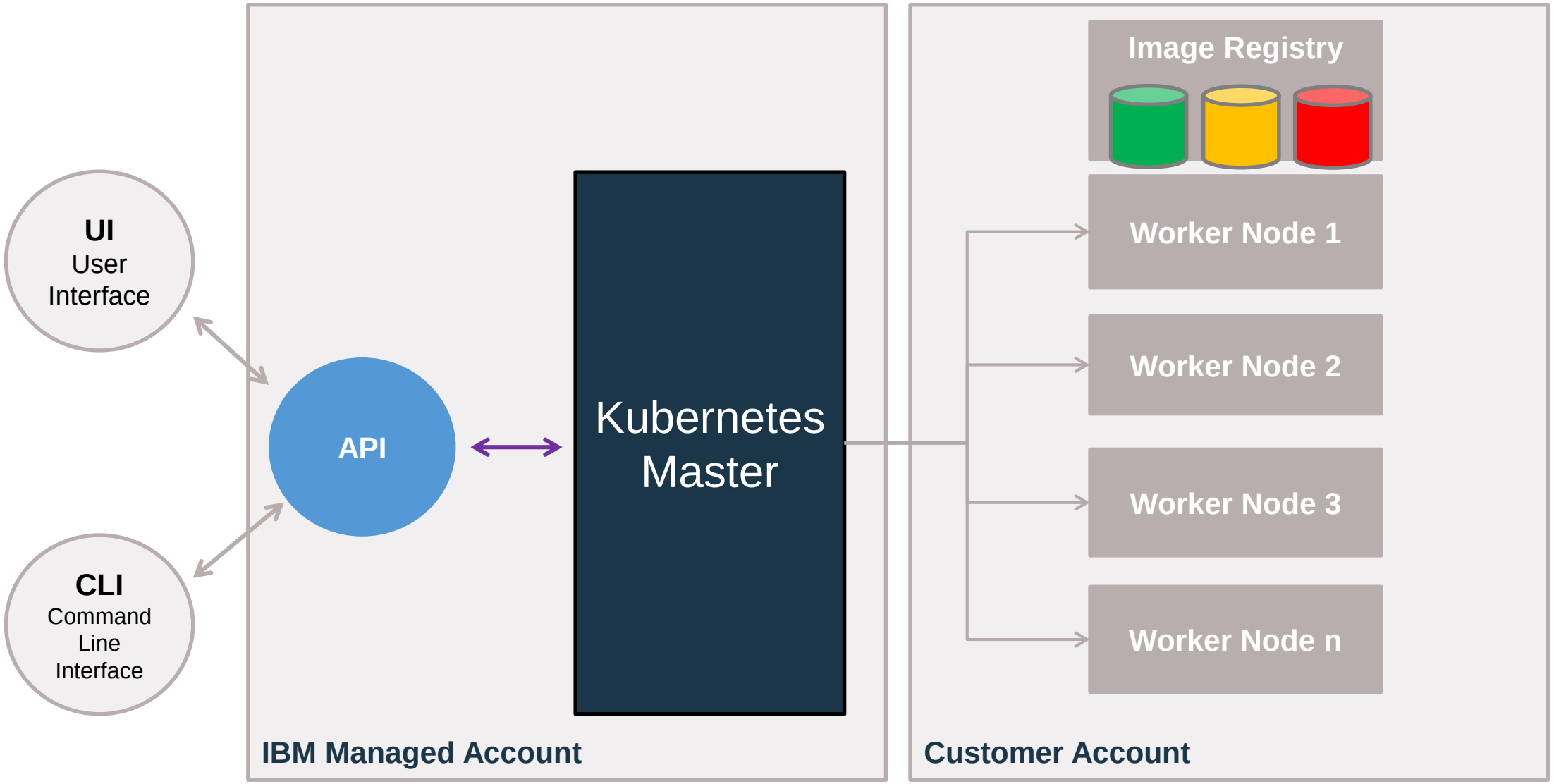
Kubernetes Architecture



Lite Cluster on IBM Cloud – Single Worker Node

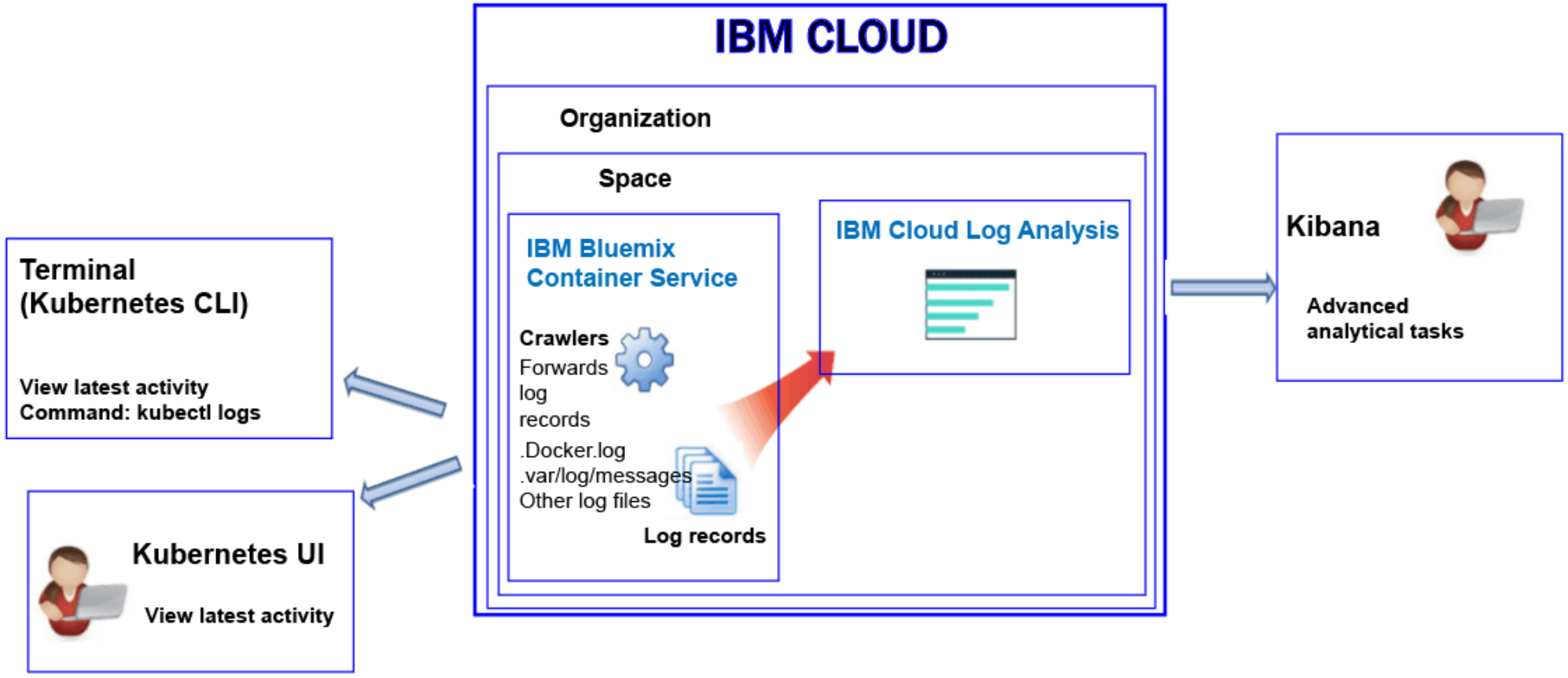


Standard Cluster - fully customizable, production-ready

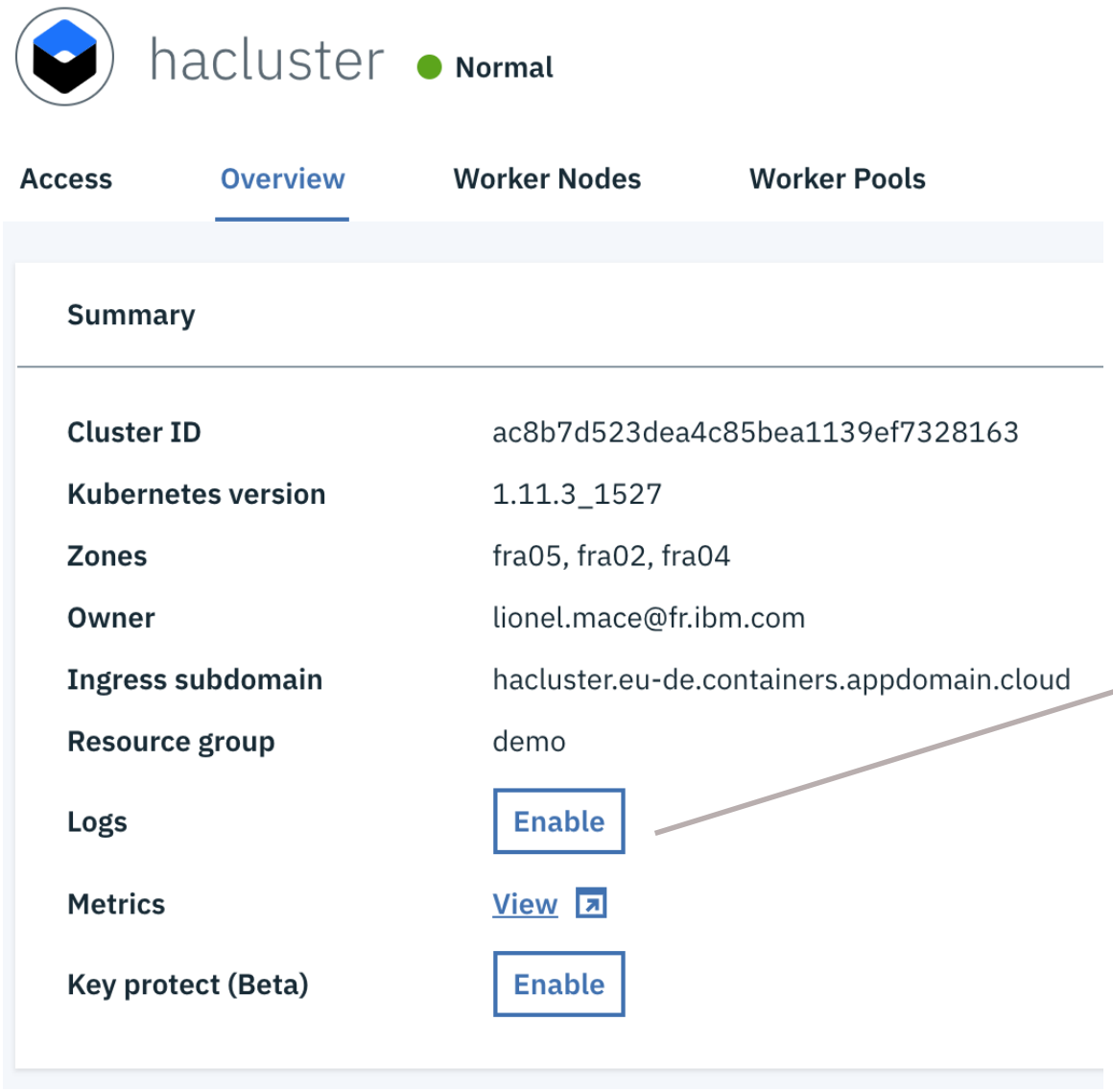


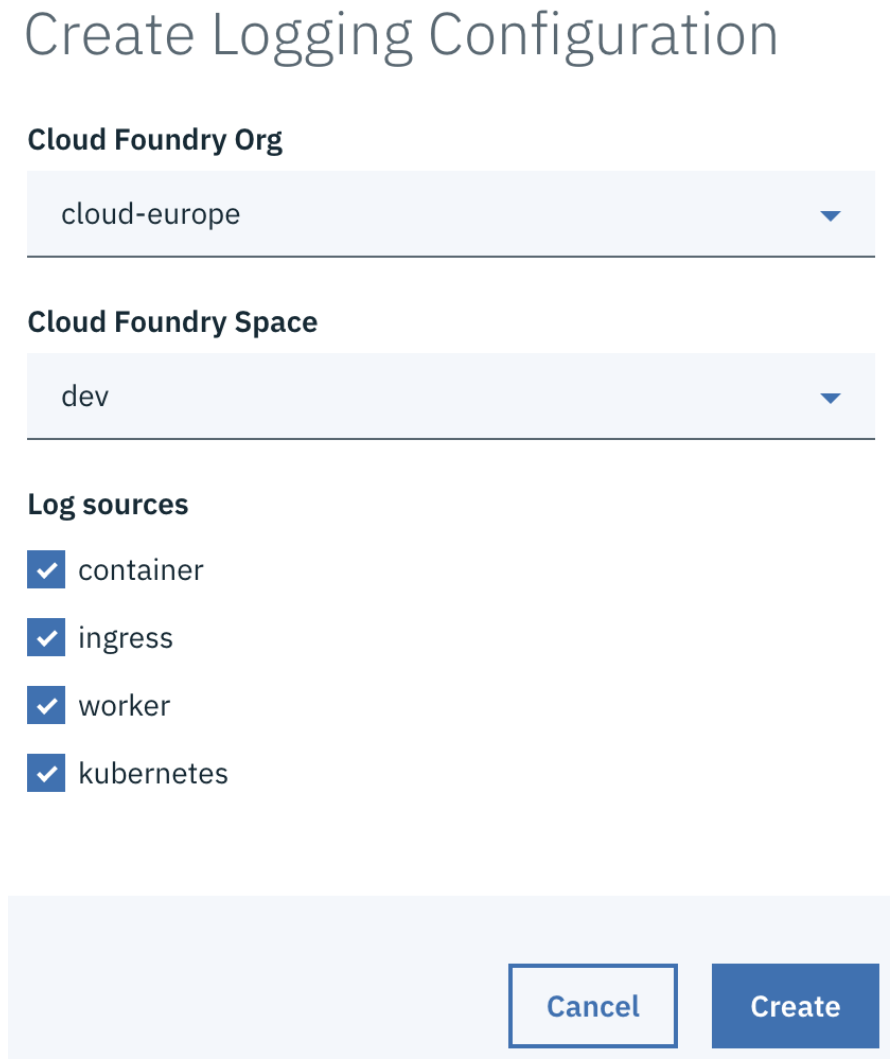
Logging with IBM Cloud Log Analysis

- Container logs are monitored and forwarded outside of the container.
- Logs for a container available in the Kibana dashboard.
- Enabling log forwarding to syslog



Enable Log Analysis in one click



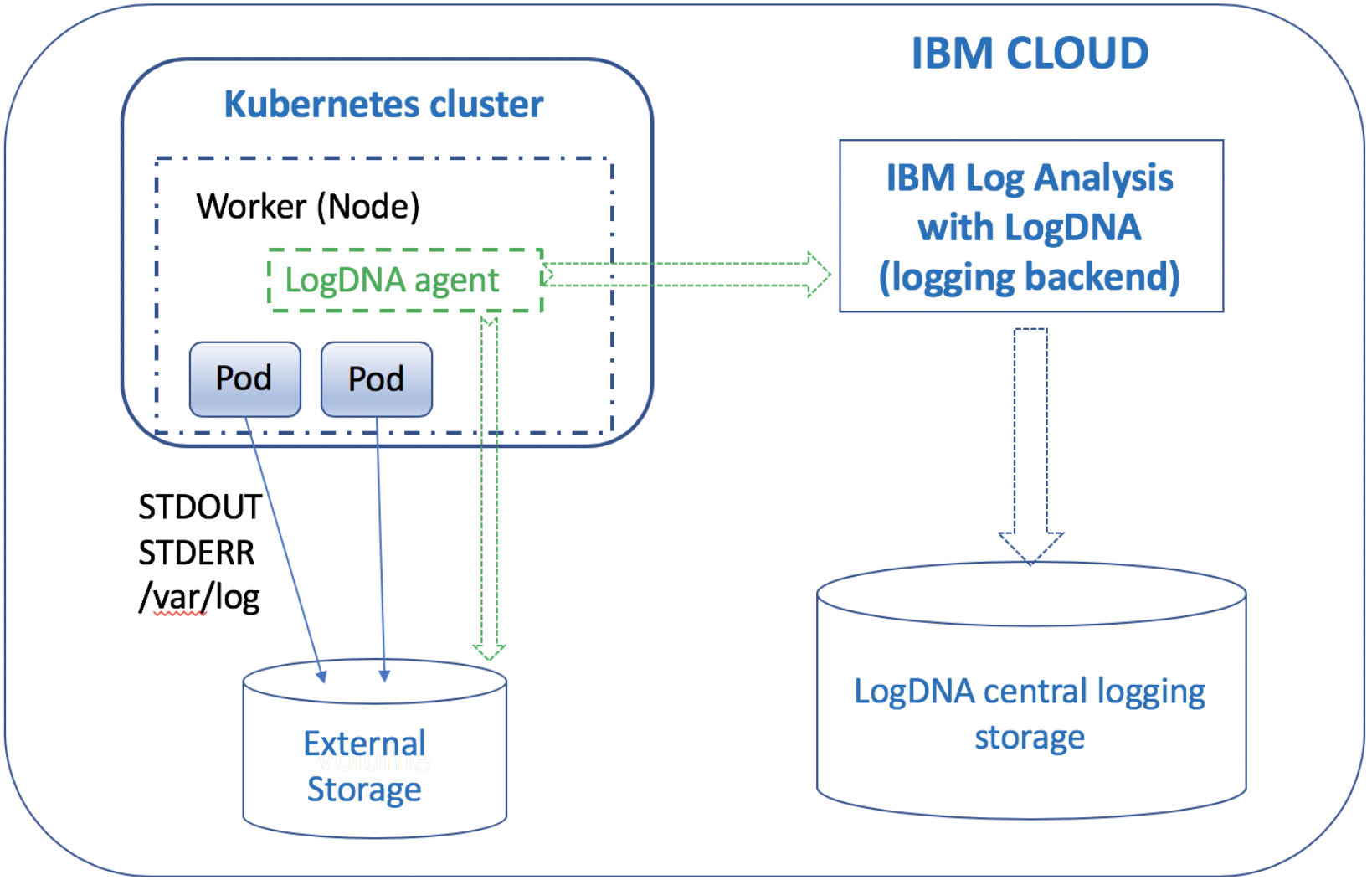


Log Analysis – Fluentd agent

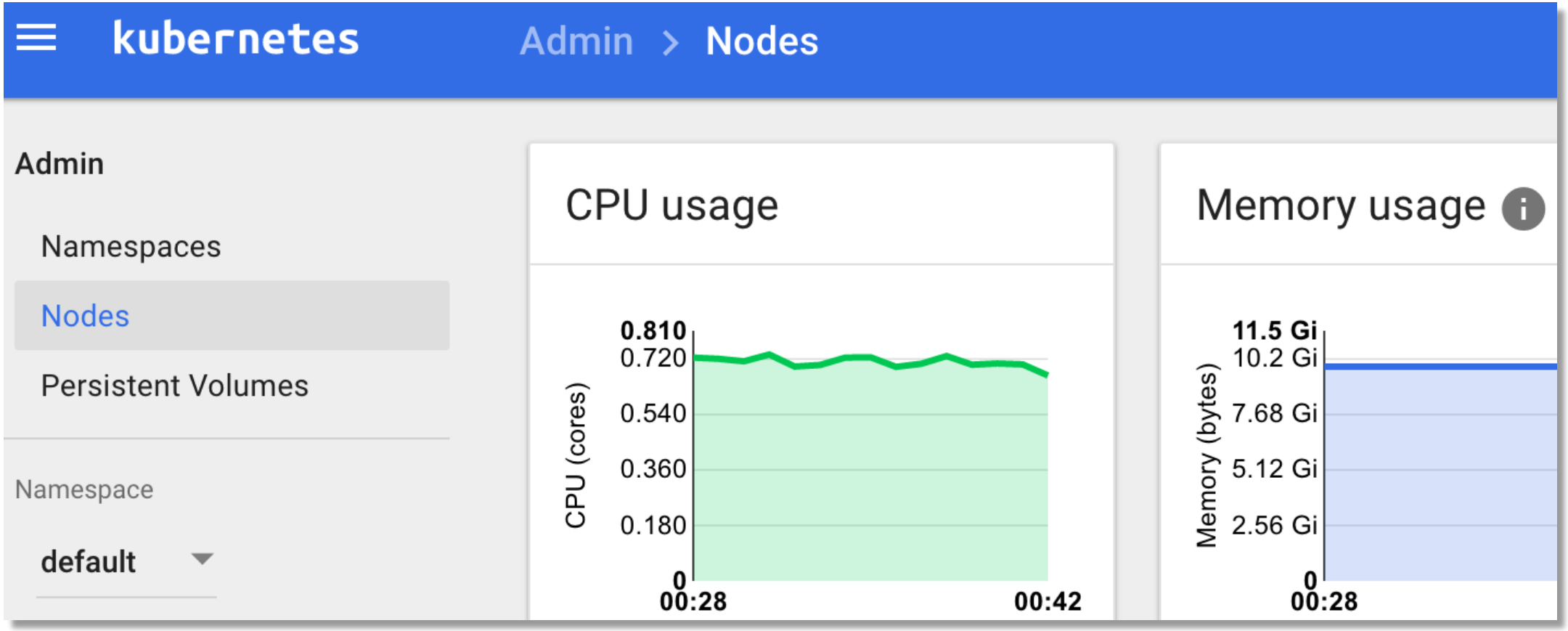
Fluentd is the agent responsible of forwarding logs from k8s pod to Log Analysis service:

```
kubectl -n kube-system top pods | grep fluent
```

Log Analysis with LogDNA



Cluster Monitoring with the Kubernestes Dashboard



Manager Cluster using REST API

clusters

Show/Hide | List Operations | Expand Operations

GET	/v1/clusters	List the clusters that you have access to.
POST	/v1/clusters	Create a cluster.
DELETE	/v1/clusters/{idOrName}	Delete a cluster.
GET	/v1/clusters/{idOrName}	View details for a cluster.
PUT	/v1/clusters/{idOrName}	Update the version of the Kubernetes cluster master node.
GET	/v1/clusters/{idOrName}/config	Download the cluster-specific configuration and certificates.
POST	/v1/clusters/{idOrName}/kms	Create a Key Protect configuration for a cluster.
PUT	/v1/clusters/{idOrName}/masters	Refresh the Kubernetes master.

https://eu-de.containers.bluemix.net/swagger-api/#/clusters

Monitoring Containers

- Monitoring based on Heapster and Grafana
- Native Kubernetes Dashboard or API
- Prometheus Monitoring