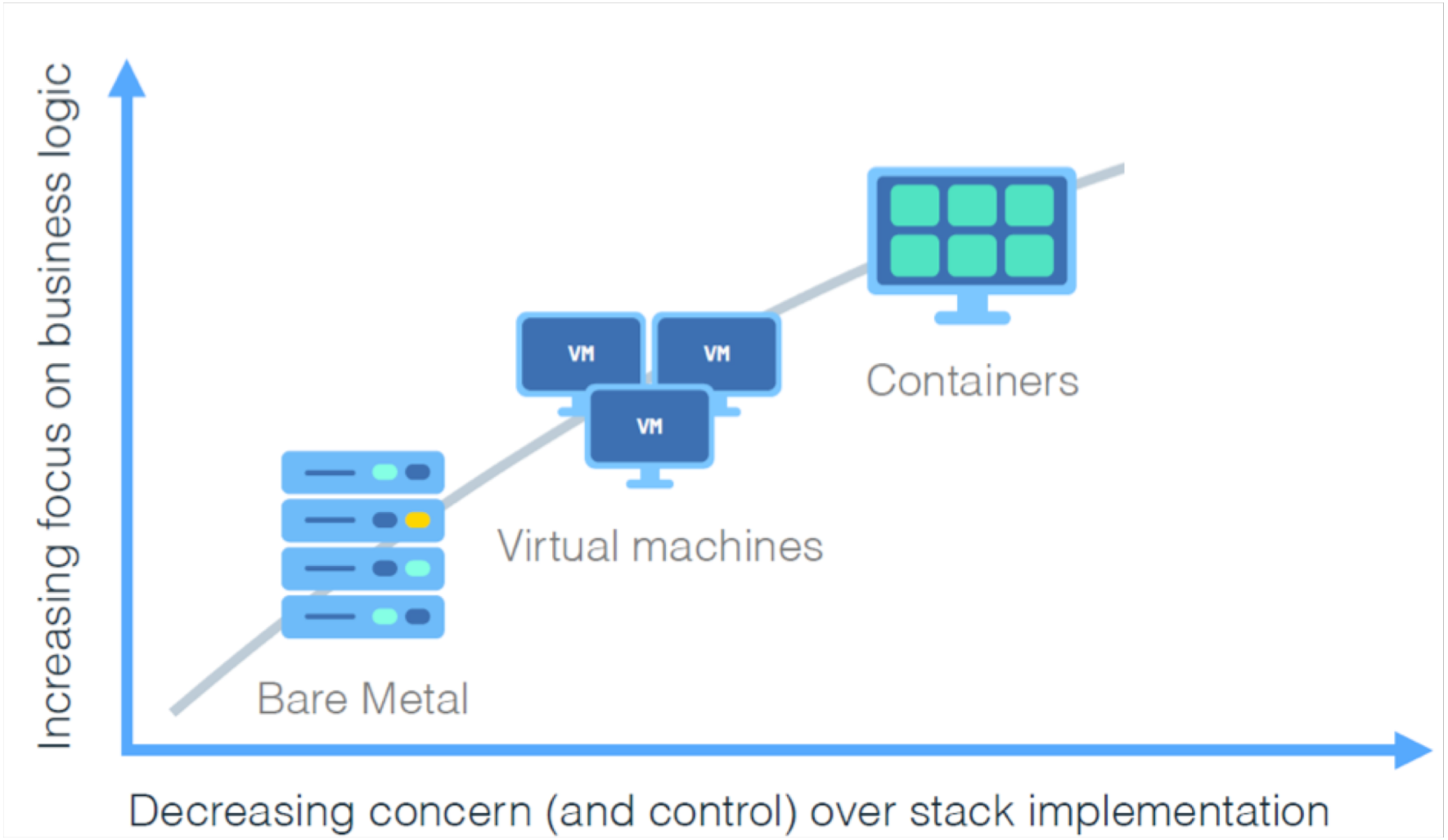
Quick overview of Container

IBM CODE

Evolution Of Containers



The challenge

Multiplicity of Stacks

Static website:
- Nginx
- OpenSSL
- Bootstrap 2
- ModSecurity

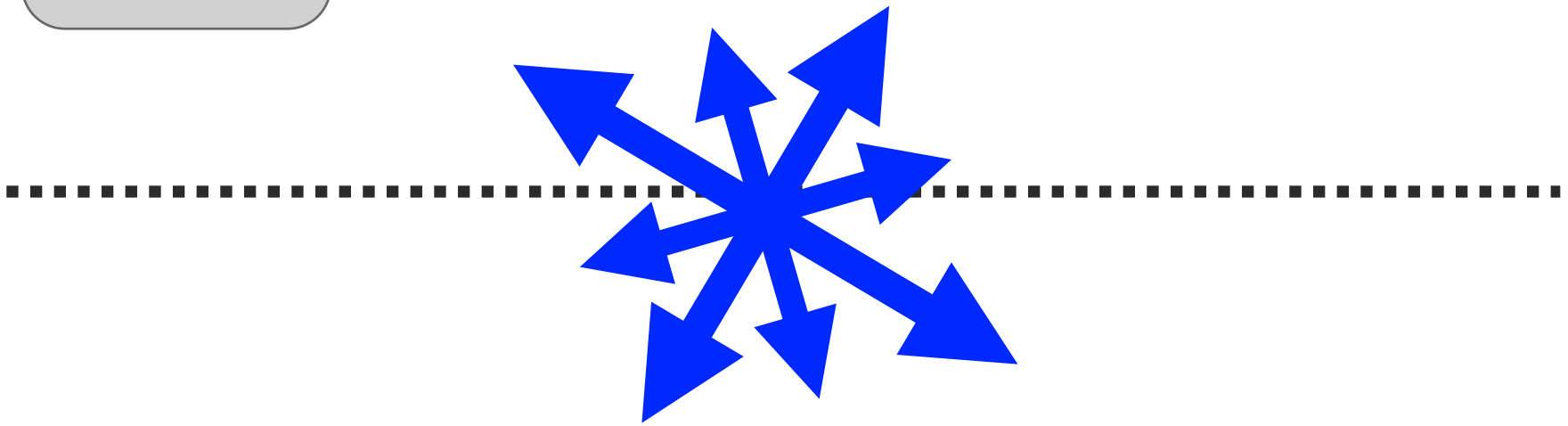
User DB:
- PostgreSQL
- pgv8
- v8

Web front end:
- Ruby
- Rails
- Sass
- Unicom

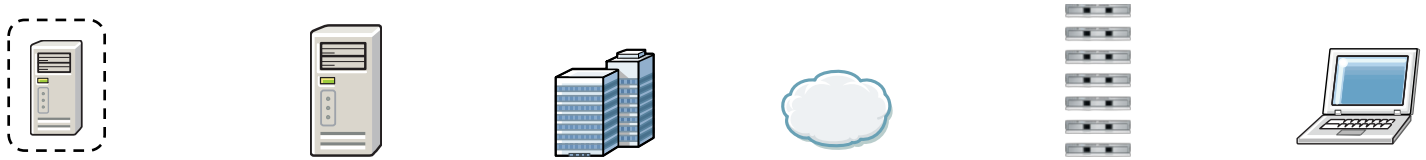
Queue:
- Redis
- Redis-sentinel

Analytics DB:
- Hadoop
- Hive
- Thrift
- OpenJDK

Do services and apps interact appropriately?



Multiplicity of hardware environments



Can I migrate smoothly and quickly?

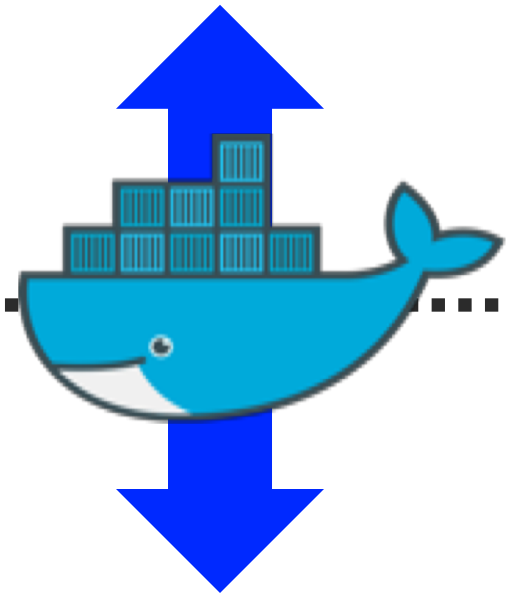
Docker: A shipping container for code

Multiplicity of Stacks

Static website | User DB | Web front end | Queue | Analytics DB

Do services and apps interact appropriately?

An engine that enables any payload to be encapsulated as a lightweight, portable, self-sufficient container…



…that can be manipulated by using standard operations, and run consistently on virtually any hardware platform.

Multiplicity of hardware environments

Development VM

QA server

Customer Data Center

Public Cloud

Production Cluster

Contributor's laptop

Can I migrate smoothly and quickly?

IBM CODE

What are Containers?

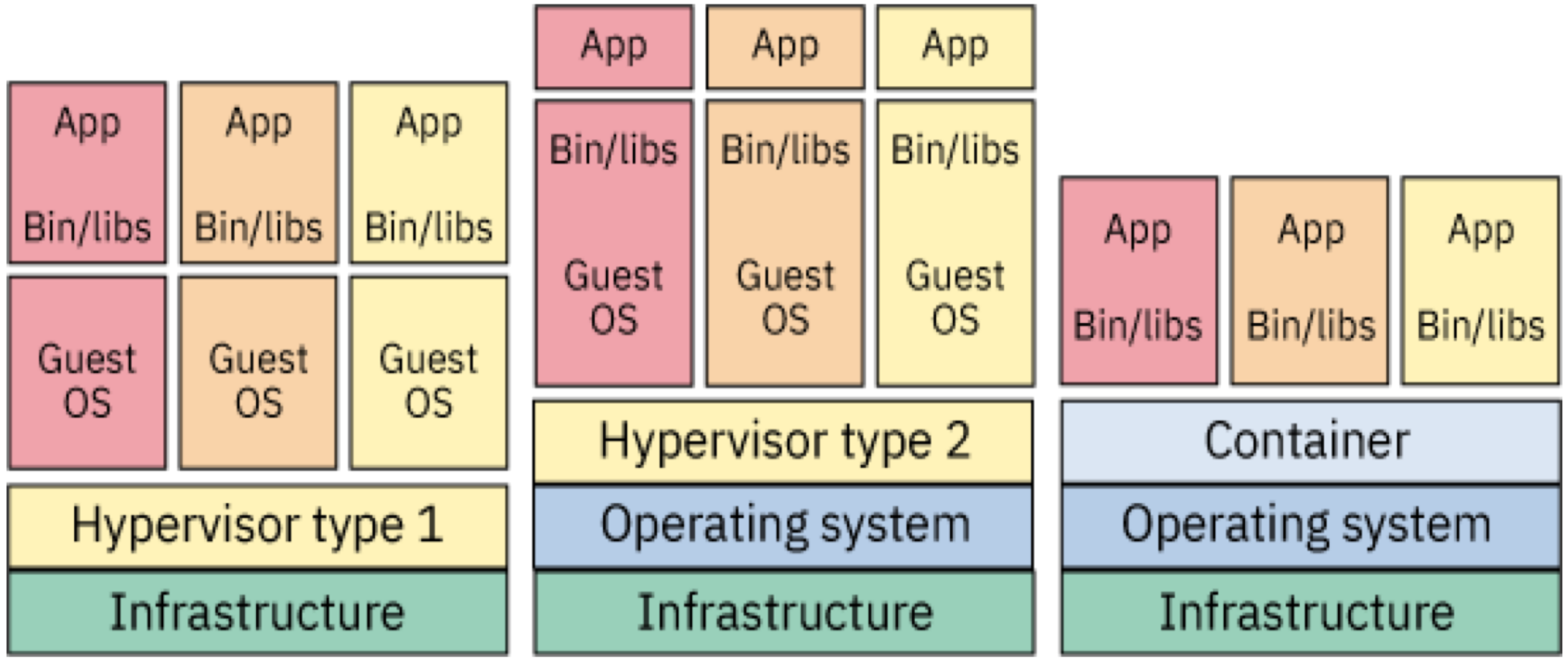
A group of processes run in isolation

- Similar to VMs but managed at the process level
- All processes MUST be able to run on the shared kernel

Each container has its own set of "namespaces" (isolated view)

- **PID** - process IDs
- **USER** - user and group IDs
- **UTS** - hostname and domain name
- **NS** - mount points
- **NET** - Network devices, stacks, ports
- **IPC** - inter-process communications, message queues
- **cgroups** - controls limits and monitoring of resources

VM vs Container



Each VM has its own OS

Containers share the same base Kernel

App, bins/libs/OS must all be runnable on the shared kernel

If OS files aren't needed they can be excluded.

IBM CODE

Why Containers?

Fast startup time - only takes milliseconds to:

- Create a new directory
- Lay-down the container's filesystem
- Setup the networks, mounts, ...
- Start the process

Better resource utilization

- Can fit far more containers

	CONTAINER BENEFITS	VIRTUAL MACHINE BENEFITS
Consistent Runtime Environment	✓	✓
Application Sandboxing	✓	✓
Small Size on Disk	✓	
Low Overhead	✓	

IBM CODE

Docker :

Why we need Docker

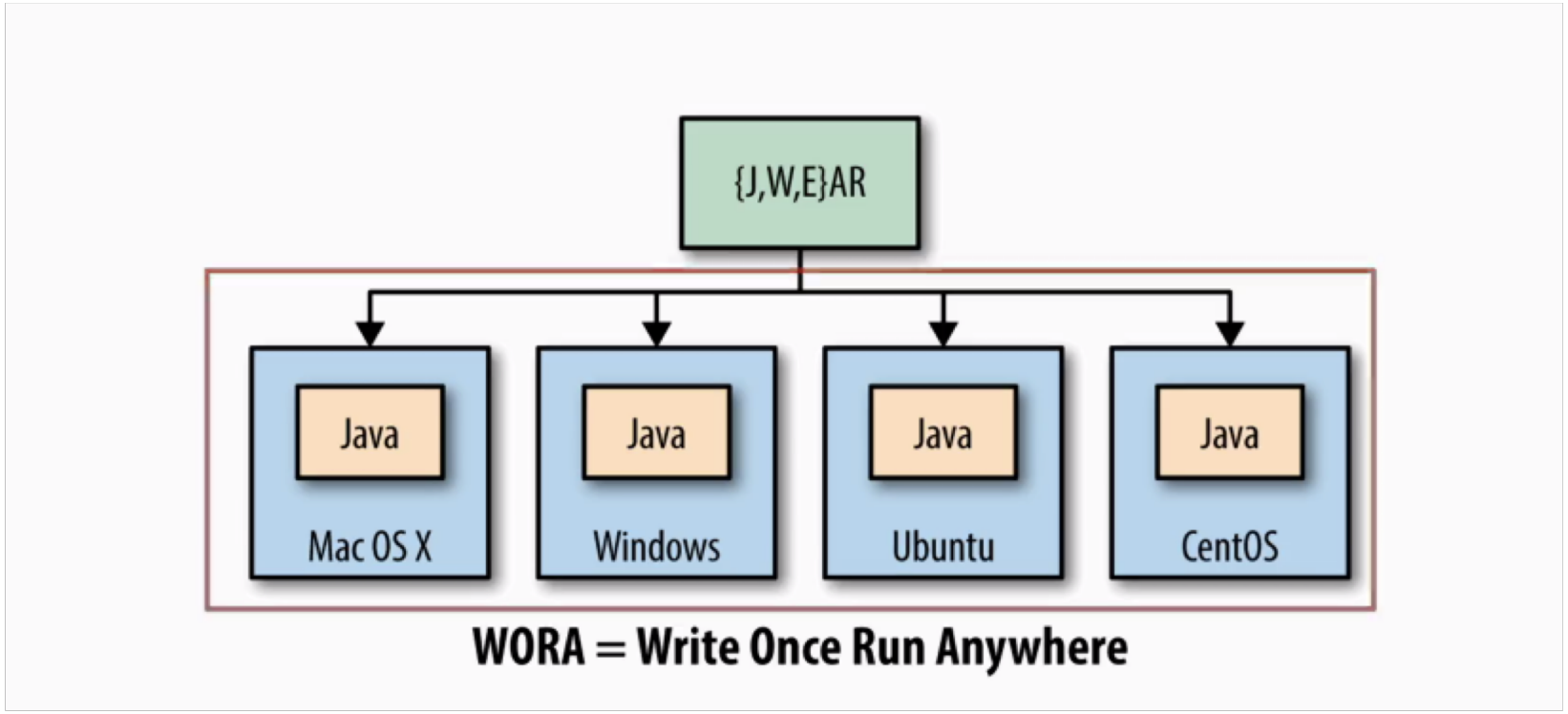
Package Once and Deploy Anywhere

Docker Concepts

Containerization

Isolation

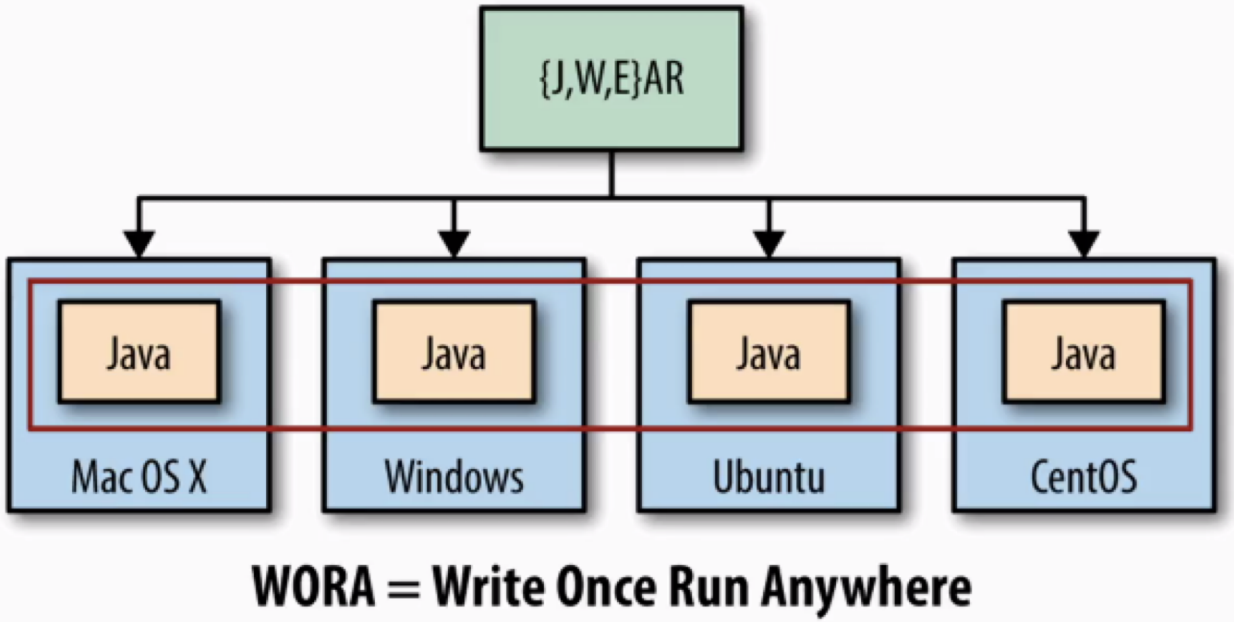
Java Application



- Each OS has its Java Software
- With same version of Software

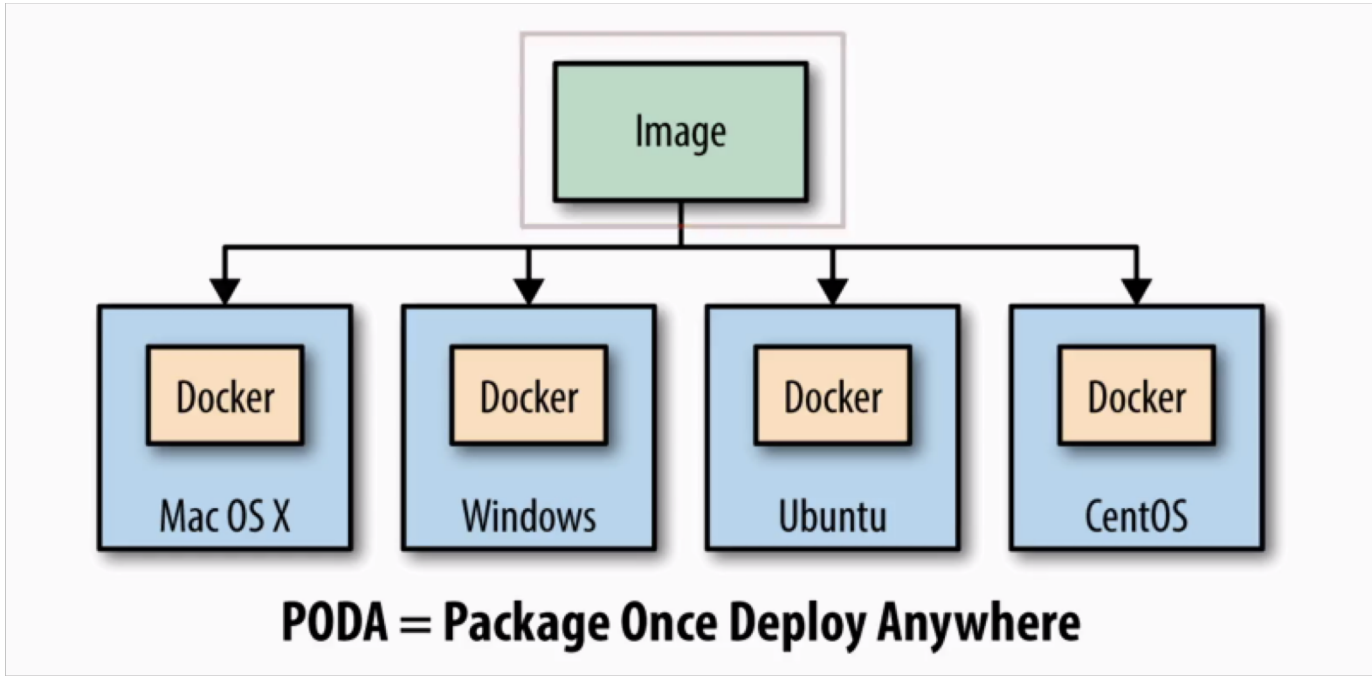
IBM CODE

Dependencies



Java installed (Proper version)
–

One Step Ahead : Docker



- No installation of software
- Docker Image using Docker Platform
- (so one step ahead)

IBM CODE

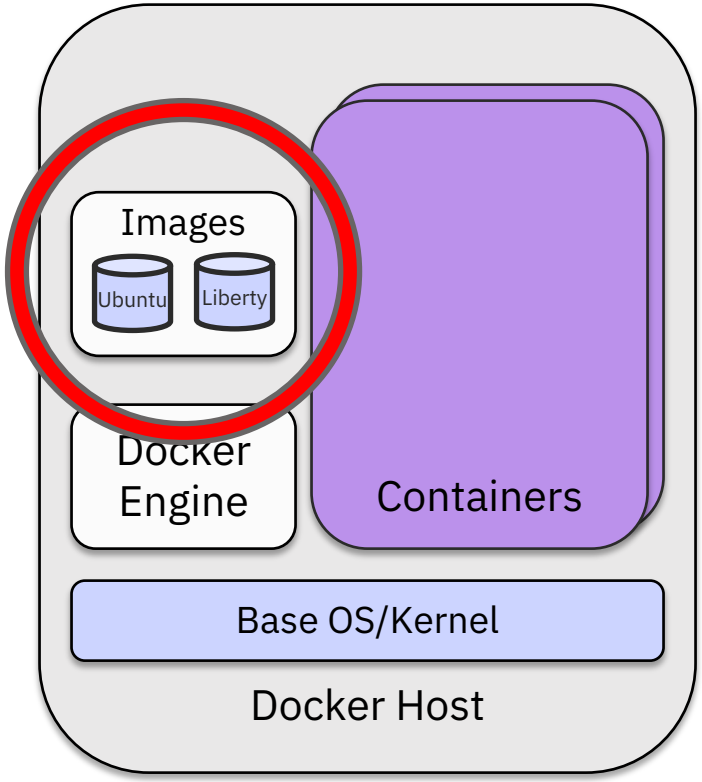
Docker Images

Tar file containing a container's filesystem + metadata

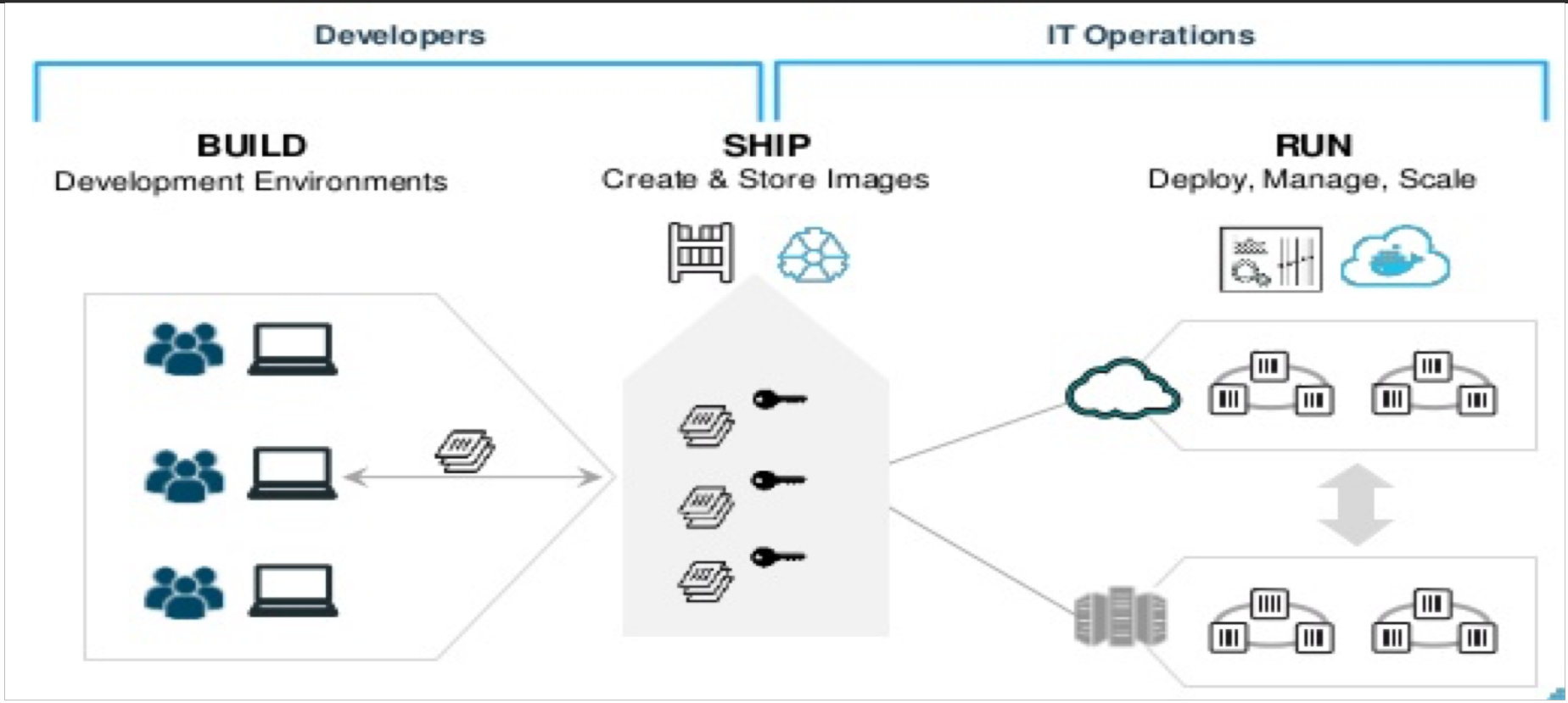
For sharing and redistribution

– Global/public registry for sharing: DockerHub

Similar, in concept, to a VM image



Phases : Build , Ship, Run



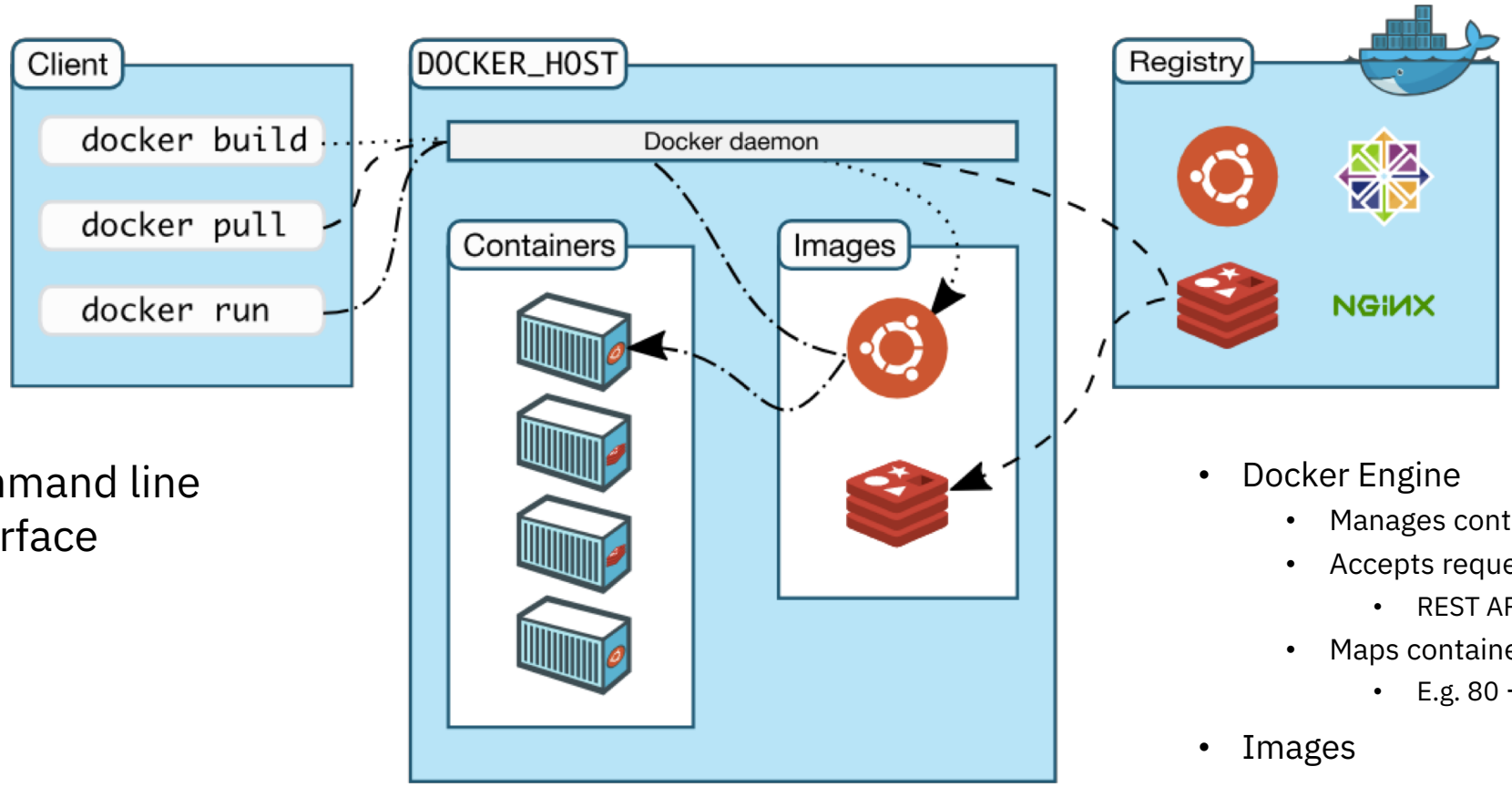
- Tools to create containerized application
- Package App – dependencies, infra as template – This is called Image

- Share Apps in Secure and collaboration manner
- Docker images stored, shared & managed in **Docker Registry**
- **Docker Hub(Public)** default registry for all

- Deploy, manage and scale apps
- Container is runtime representation of image
- Lifecycle of container – run, start, scale, stop, move, delete

IBM CODE

Docker Architecture



Command line Interface

Docker Engine

Images

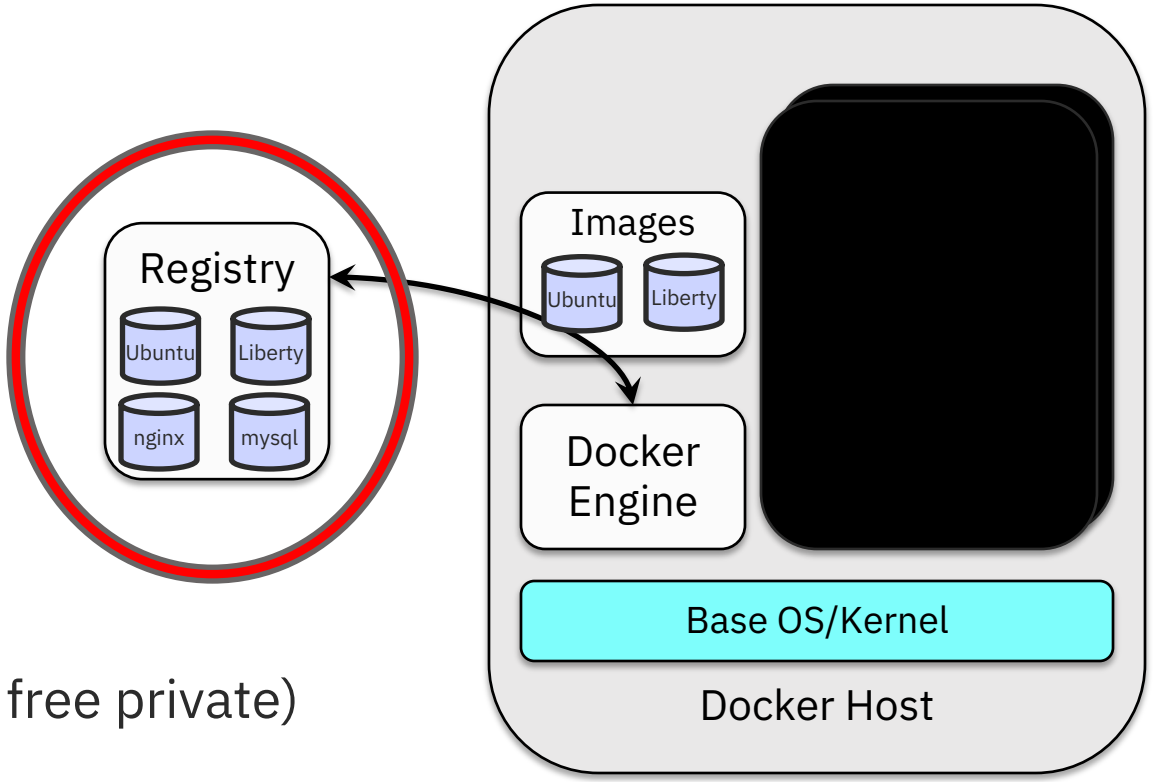
- Docker Engine
  - Manages containers on a host
  - Accepts requests from clients
    - REST API
  - Maps container ports to host ports
    - E.g. 80 → 3582
- Images
- Docker Client
  - Drives daemon
  - Drives "builder" of Images
- Docker Registry
  - Image DB

IBM CODE

Docker Registry

Creating and using images is only part of the story

Sharing them is the other

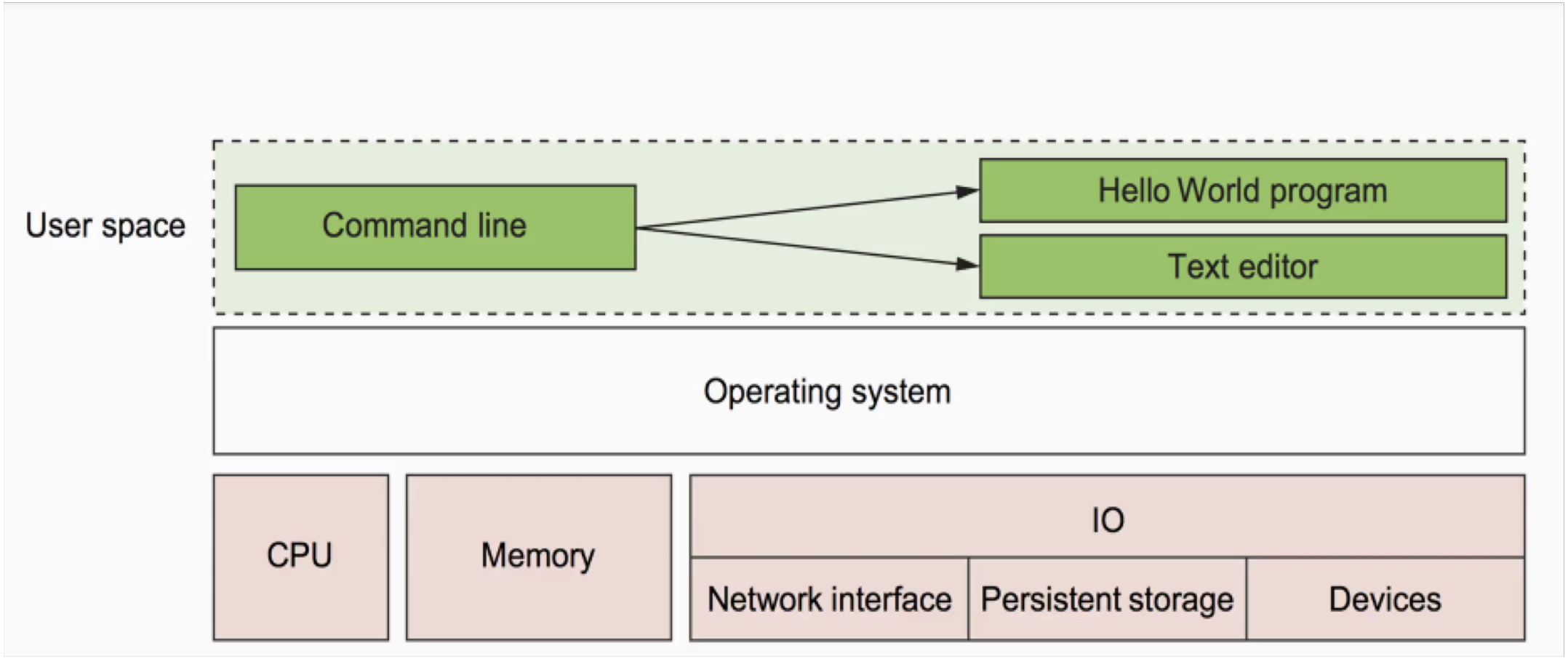


DockerHub - http://hub.docker.com

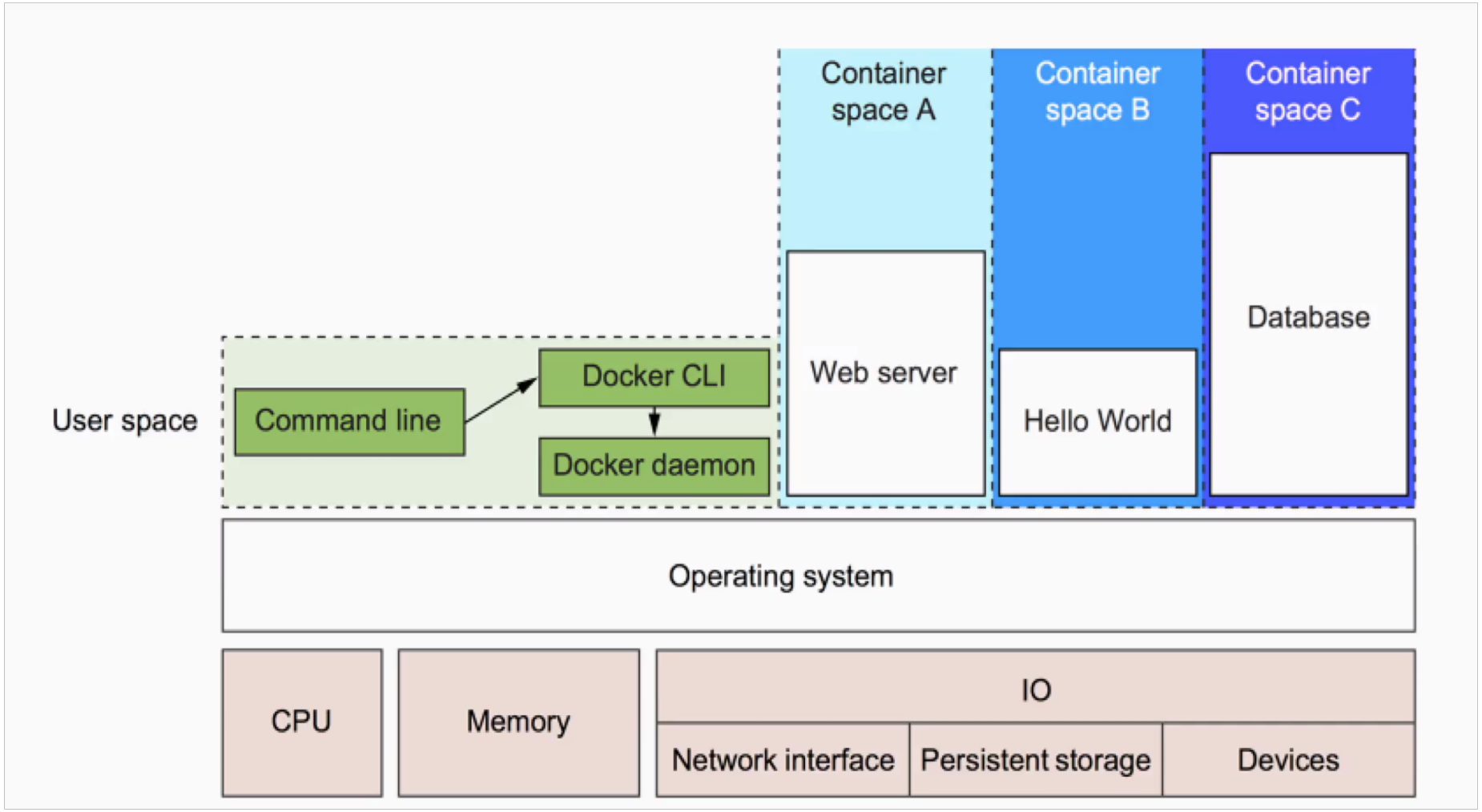
- Public registry of Docker Images
- Hosted by Docker Inc.
- Free for public images, pay for private ones (one free private)
- By default docker engines will look in DockerHub for images
- Web interface for searching, descriptions of images

IBM CODE

Isolation : Linux

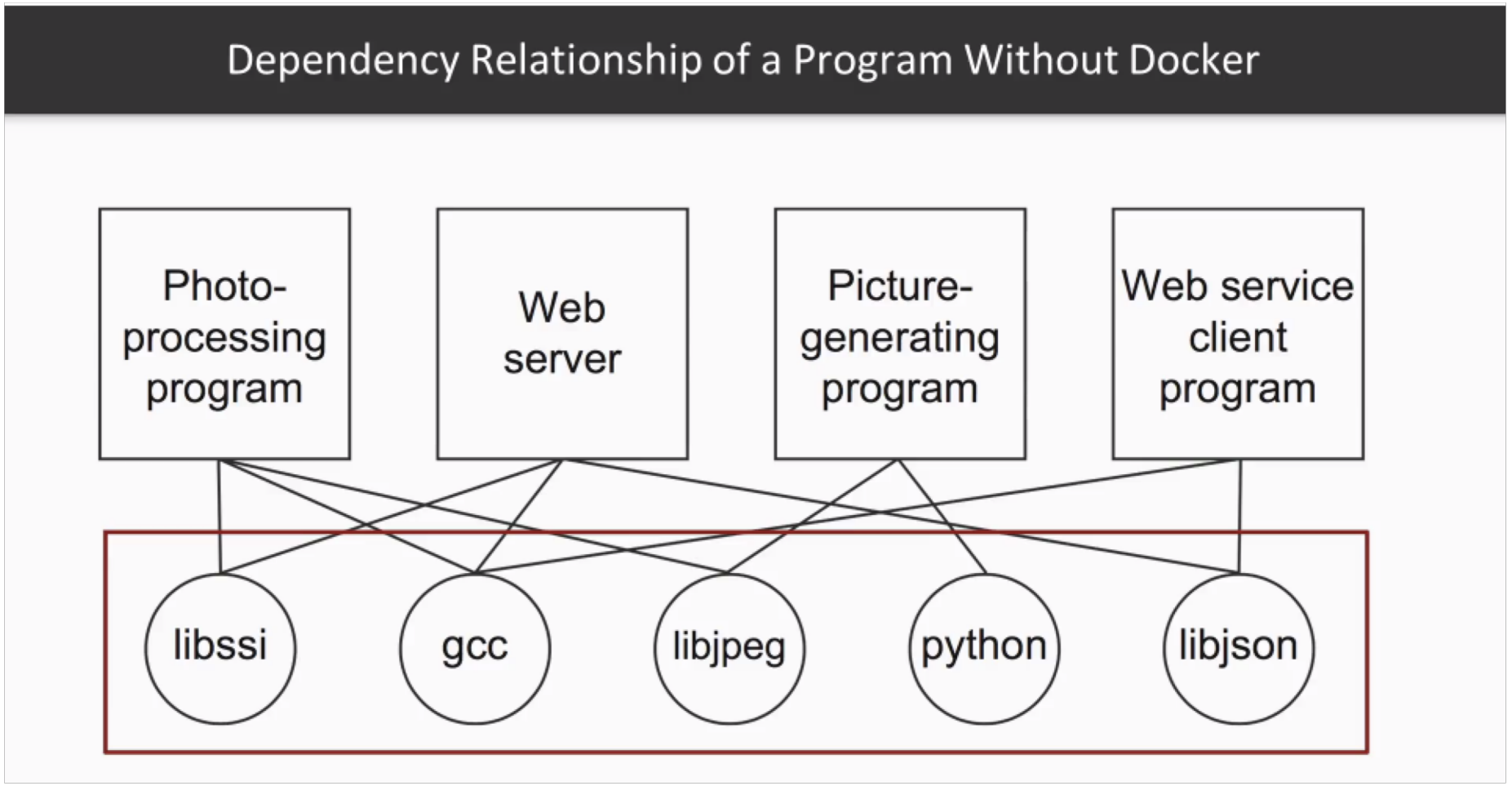


Docker Isolation : Process Level

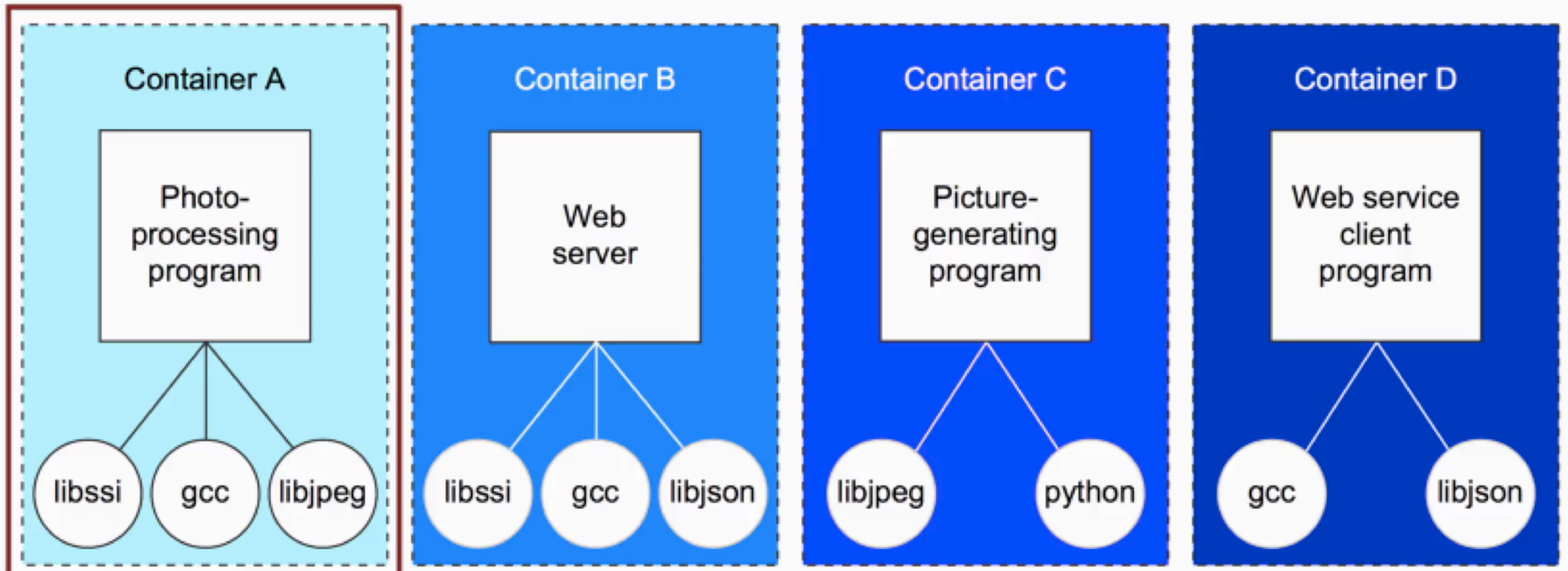


IBM CODE

Running programs without docker



Each App : With needed Dependencies



So : What is Docker?

1. At its core, Docker is tooling to manage containers

– Docker is not a technology, it’s a tool or platform

– Simplified existing technology to enable it for the masses

2. Tooling to manage containers

– Containers are not new

– Docker just made them easy to use

3. Docker creates and manages the lifecycle of containers

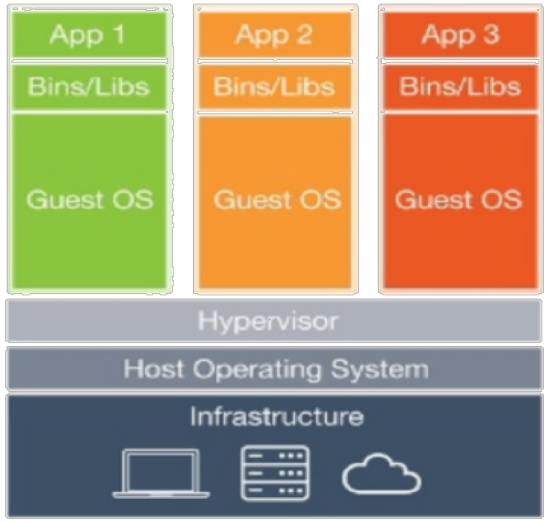
– Setup filesystem

– CRUD container

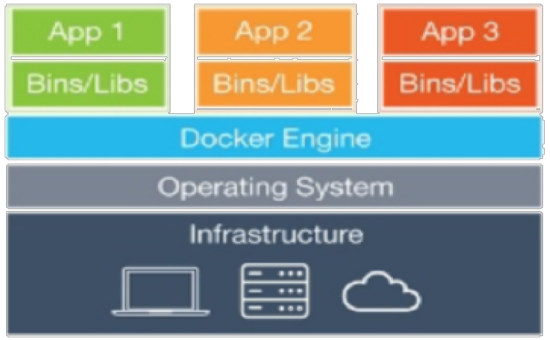
  - Setup networks
  - Setup volumes / mounts
  - Create: start new process telling OS to run it in isolation

IBM CODE

Docker Container Vs VMWare

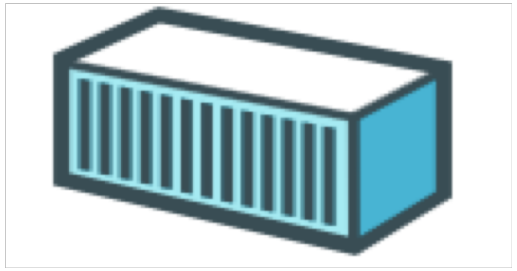


vmware

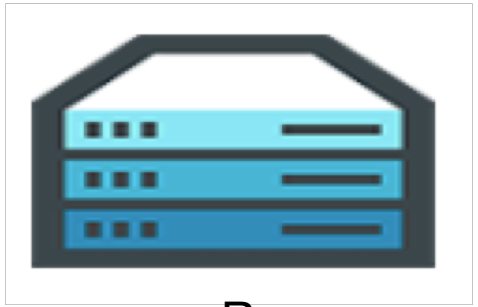


docker

Build



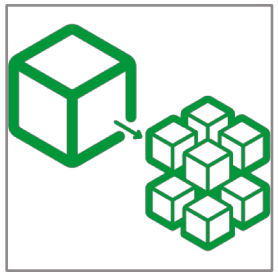
Ship

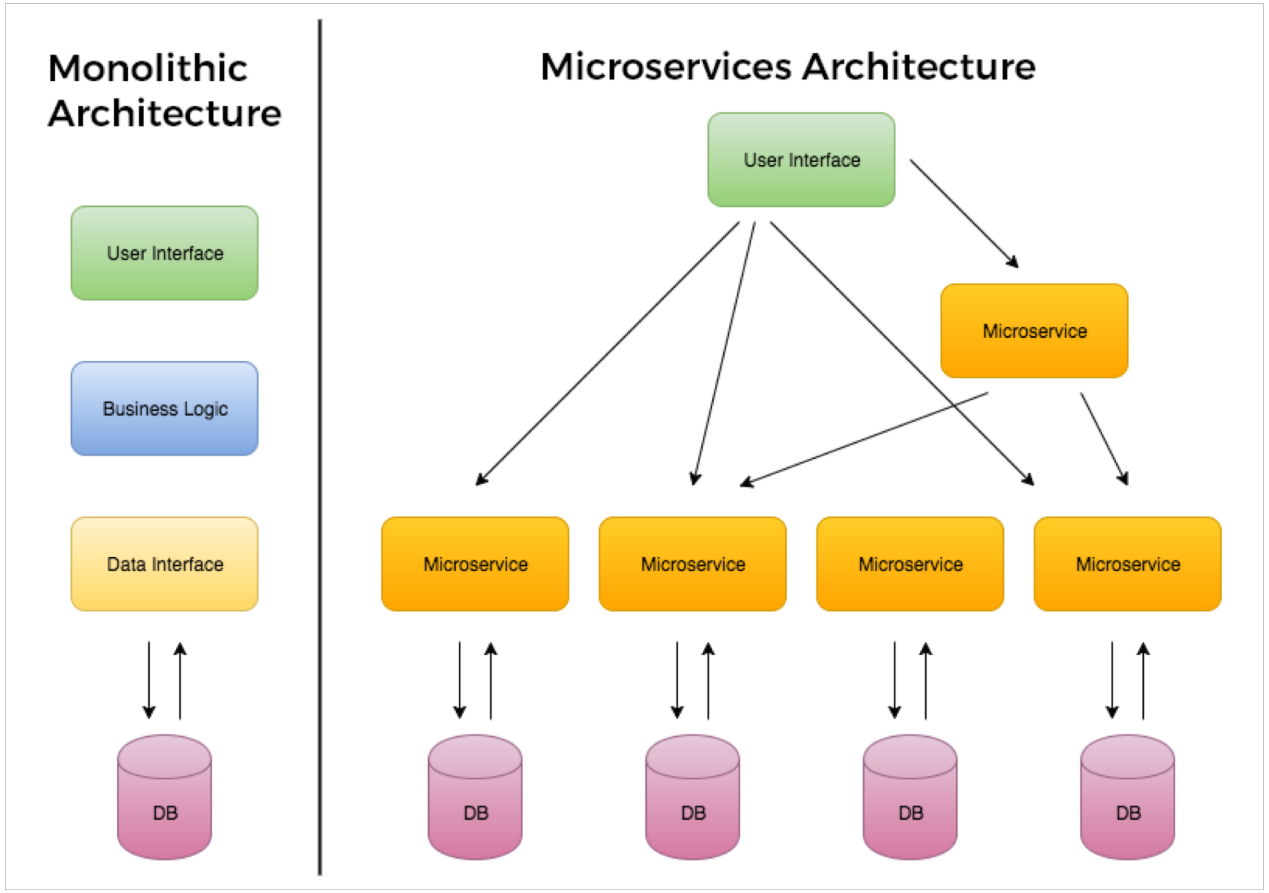


Run

IBM CODE

Microservices & Cloud Native Apps





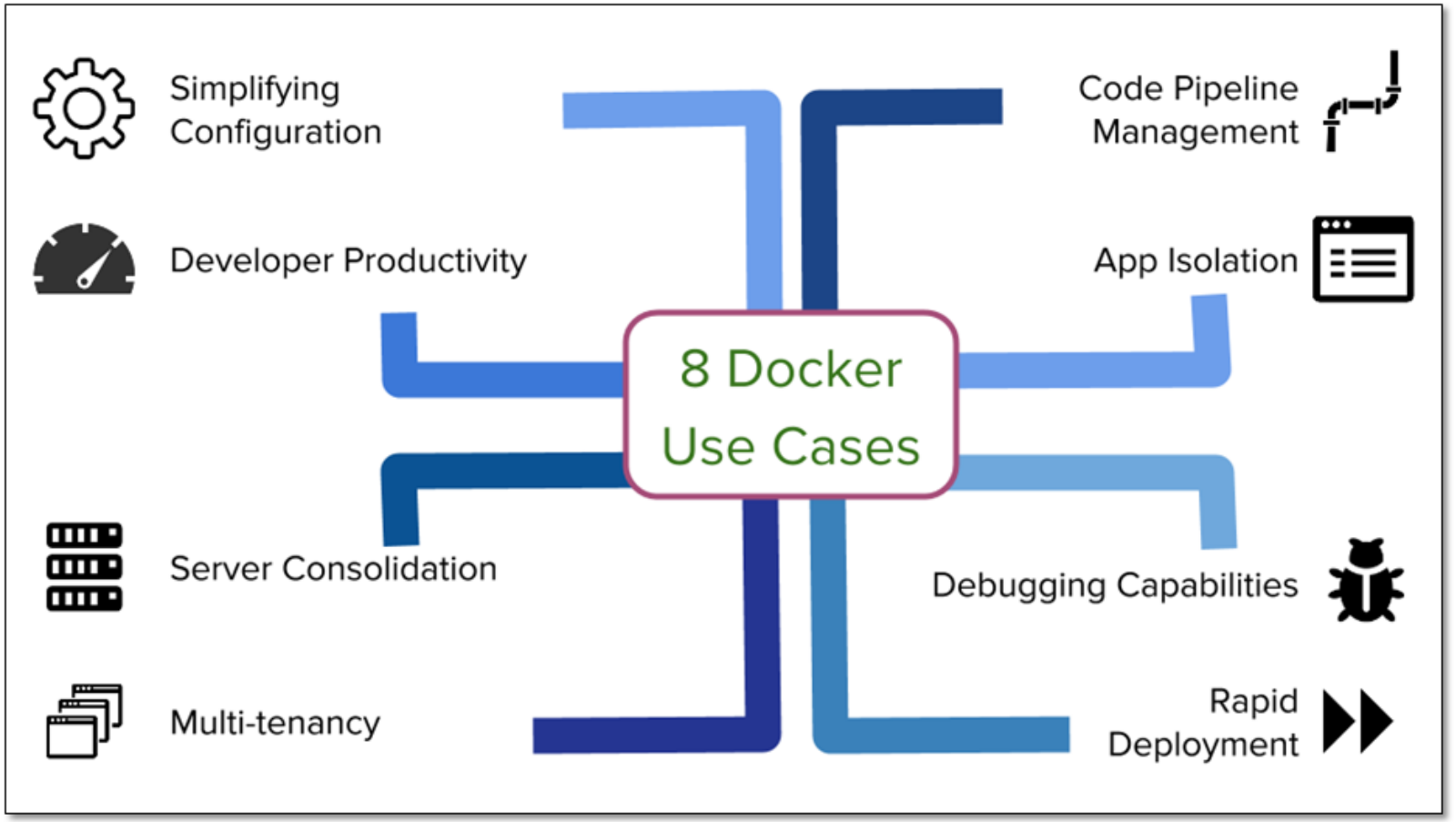
IBM CODE

Docker – Use cases

Server Apps like web servers, mail servers, databases, and proxies

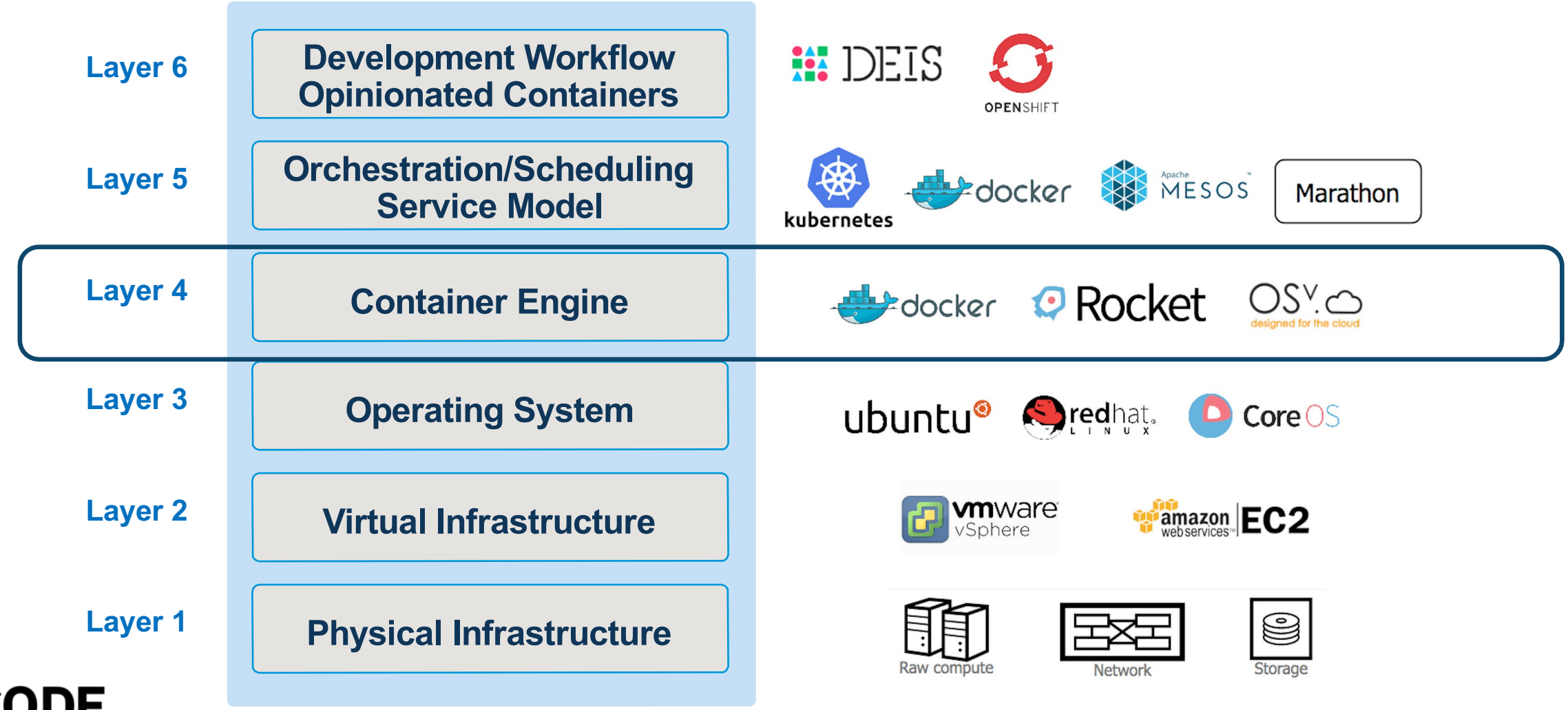
Desktop software's, tools , email clients etc

Running these in a container and as a user with reduced previlgies will help protect your system from attack



IBM CODE

Layers : Containers



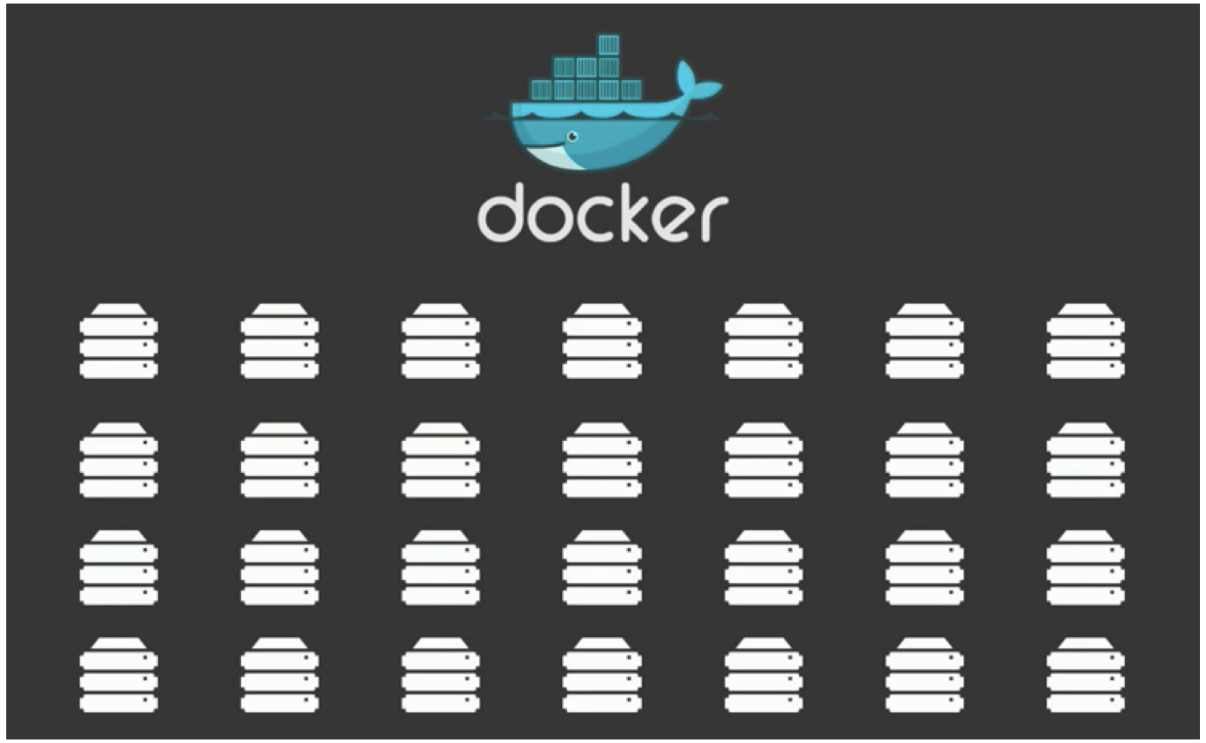
IBM CODE

Get Started with IBM Cloud

Create IBM Cloud Account

Deployed on 3 servers – Simple

Jump from 3 – 40,50 servers



- Scale out
- Keep track
- Where to put your containers
- What container – Where?
- May be containers other than docker as well

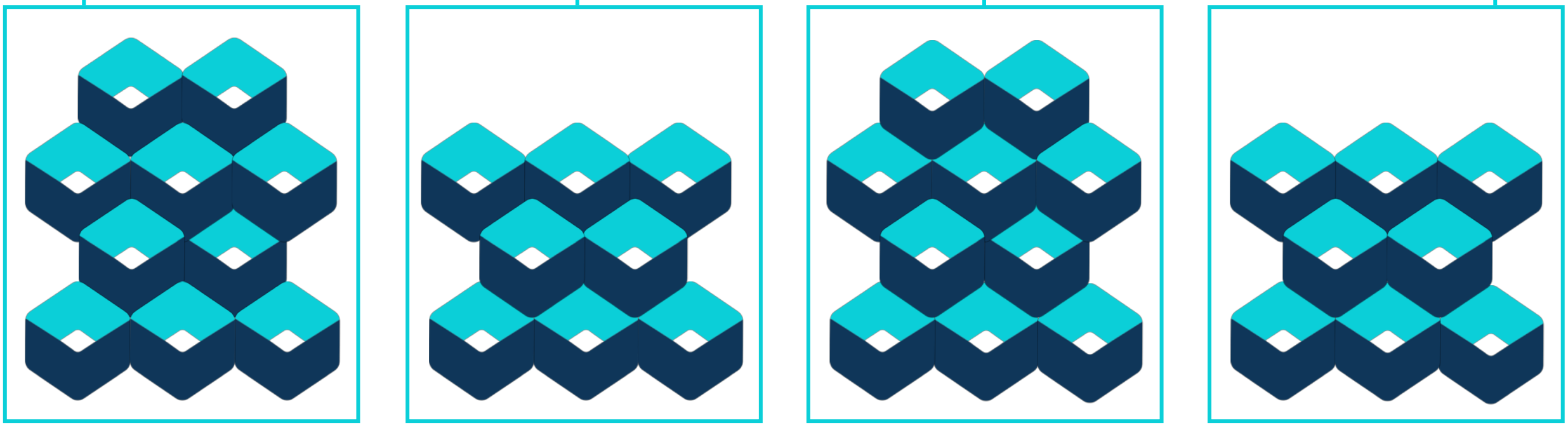
Containers are great but … can lead into lack of control & chaos

IBM CODE

Kubernetes – (Κυβερνήτης - Captain in Greek)

Regain control with Containers and Kubernetes

- Organize and Govern the Container Chaos



IBM CODE

What is K8s?

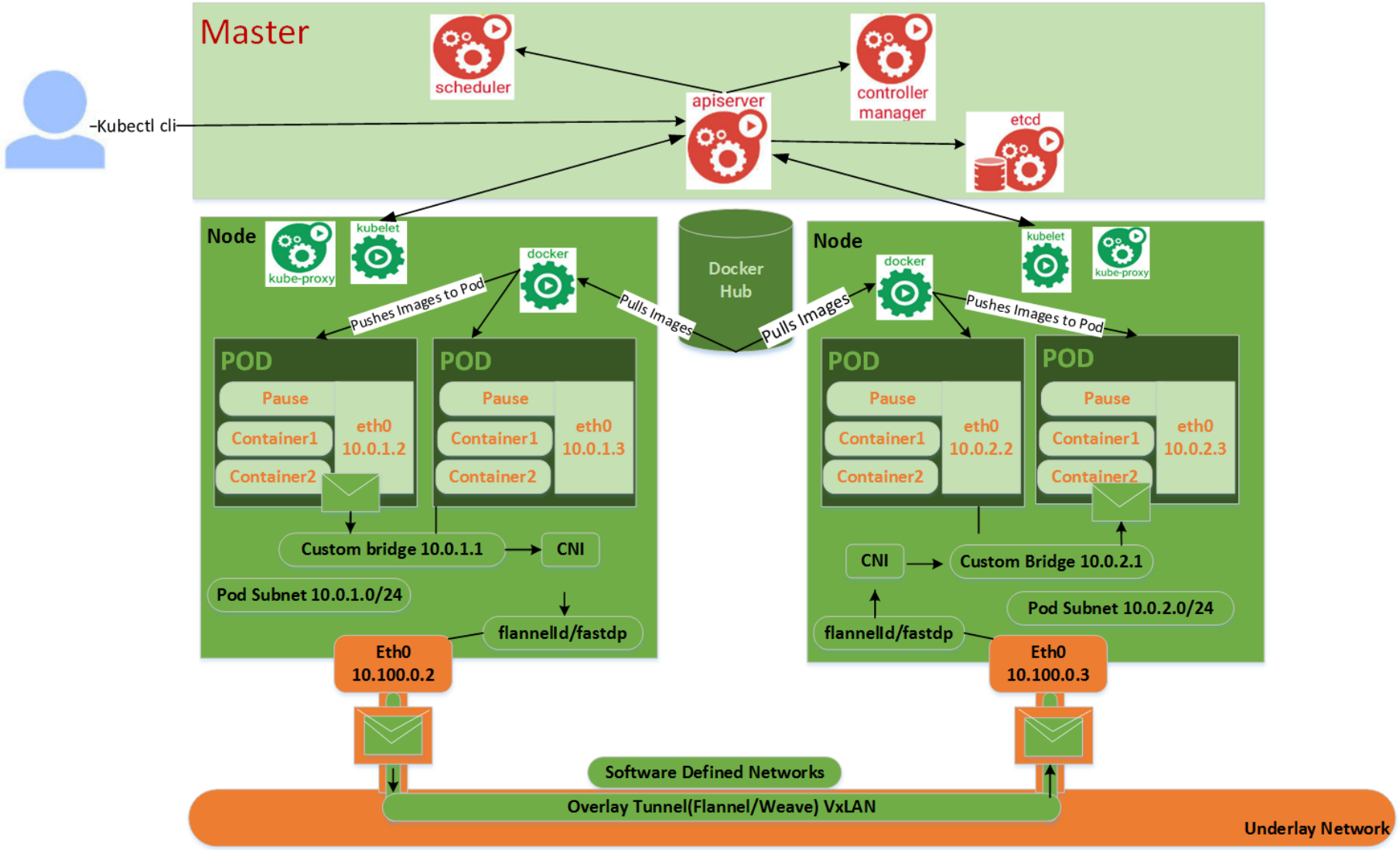
- Based on Google's Borg & Omega - Open Source - Container Orchestrator
- Open Governance

  Cloud Native Compute Foundation
- Adoption by Enterprise

  RedHat, Microsoft, IBM and Amazon

- Help to automate DevOps – Deployment, scaling and management of containerized apps
- Helps organize container in logical units(pods, nodes)
- Helps in resource monitoring and logging

Kubernetes Architecture



Kubernetes Capabilities

Intelligent Scheduling

Self-healing

Horizontal scaling

Service discovery & load balancing

Automated rollouts and rollbacks

Secret and configuration management

Intelligent Scheduling

- Automatically places containers based on required resources
- Supports mixed workloads to drive increased utilization

Self-healing

- Restarts containers that fail
- Replaces and reschedules containers when nodes die
- Kills containers that don't respond to your user-defined health check

Horizontal scaling

- Scale your application with a simple command
- Automatic scaling based on real-time usage

Service discovery and load balancing

- Simple discovery of services through a single DNS name
- Manage access to container applications through IP address or HTTP route.
- Automatically load balance traffic and route around failure

Automated rollouts and rollbacks

- Roll out changes to your application or its configuration, while monitoring application health to ensure things stay up
- If something goes wrong, Kubernetes will rollback the change for you

Secret and configuration management

- Safely store application credentials and secrets
- Deploy and update secrets and application configuration without rebuilding your image and without exposing secrets in your stack configuration.

Cluster Management Capabilities

Simplified cluster management

Design your own cluster

Container security & isolation

Extend with IBM Cloud & Watson

Native open-source experience

Integrated operational tools

IBM Cloud
Kubernetes Service

Simplified Cluster Management

- Intuitive graphical user experience
- CLI and API alternatives
- Fully managed master nodes
- Highly available (HA) masters
- User controlled worker node management
- Worker node auto-recovery

IBM Cloud
Kubernetes Service

Design Your Own Cluster

- Tunable capacity
- Select between shared and dedicated compute using virtual server instances
- Bare metal worker nodes enabling Trusted Compute
- Multizone clusters in IBM Cloud multizone regions and single zone clusters in 25+ datacenters
- Edge nodes
- Configurable networking and storage
- Integrated VPN in-cluster providing IPSec tunnels

IBM Cloud
Kubernetes Service

Container Security & Isolation

- Isolated compute, networking, and storage
- Automatic encryption of secrets and volumes
- Customer managed keys using HSM backed IBM Key Protect
- Default LUKS encryption of /var/lib/docker
  - Every worker node in each cluster has a unique encryption key
- Store your images securely in your hosted private registry
- Vulnerability Advisor provides Docker image and running container scanning to detect vulnerabilities and configuration weaknesses
- Image signing by integrating with Docker Notary
- Image security deployment enforcement controls

IBM Cloud
Kubernetes Service

Extend IBM Cloud Services

- Enhance your application with Watson, IoT, Analytics and Data Services
- Persistent volumes using IBM Cloud storage (file, block, object)
- IP and application Load Balancing
- Integrated with IBM Cloud identity and access management
- Control access and billing using Resource Groups

IBM Cloud
Kubernetes Service

Native Kubernetes Experience

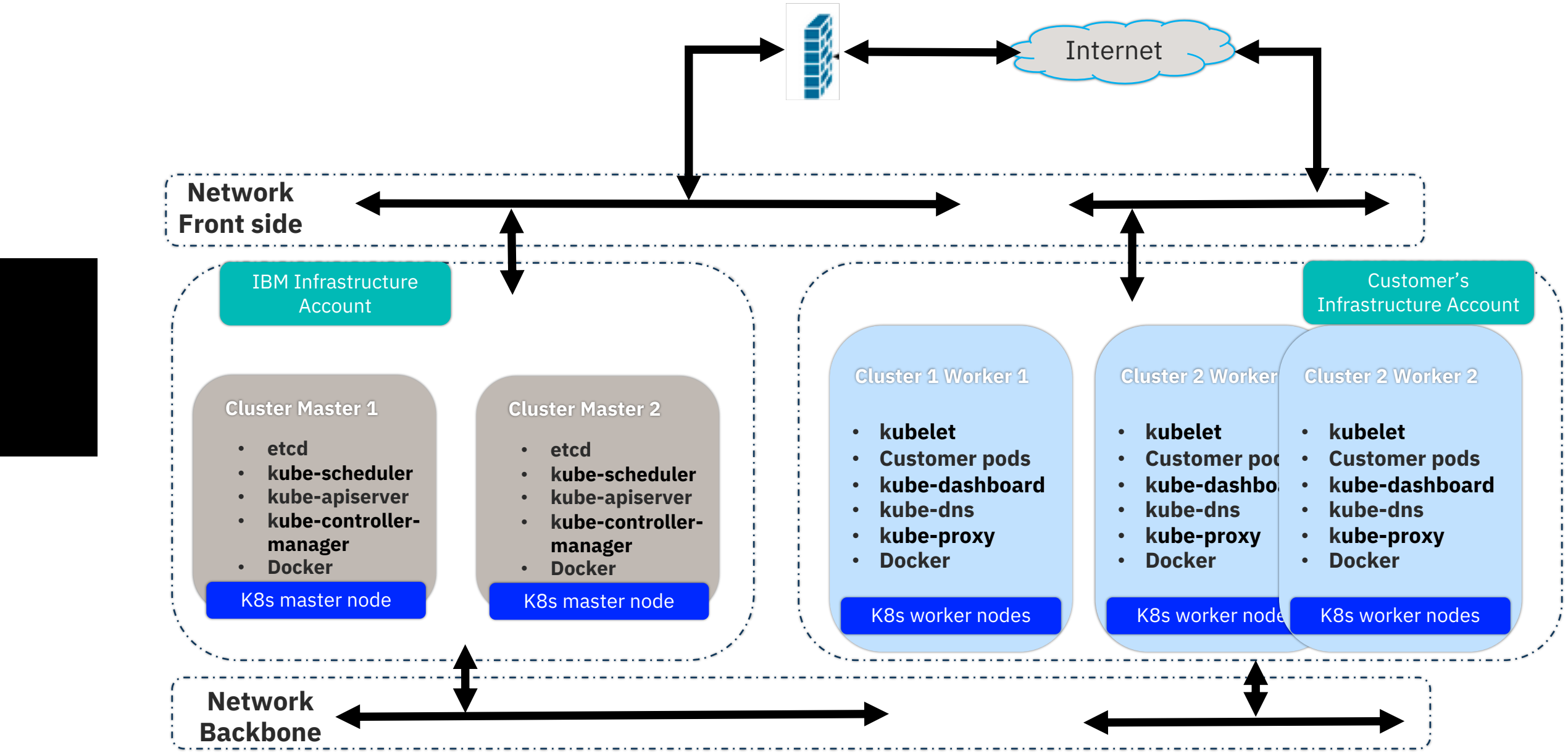
- Seamless experience moving from local development to IBM Cloud
- 100% Kubernetes API and tools
- Certified Kubernetes provider
- Conformance tested for Kubernetes 1.9, 1.10, 1.11
- Supports Kubernetes dashboard
- Leverage Docker images

IBM Cloud
Kubernetes Service

Integrated Operational Tools

- Built-in log and metrics collection with IBM Cloud log and monitoring services
- Use with IBM DevOps tools such as Delivery Pipeline
- Supports popular add-ons including Prometheus, Weave, Sysdig, fluentd and others

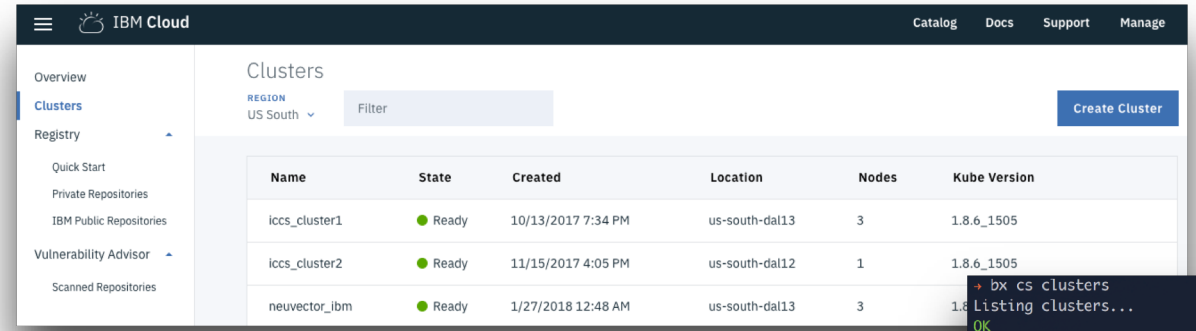
IBM Cloud Kubernetes Service



In-cluster Capabilities

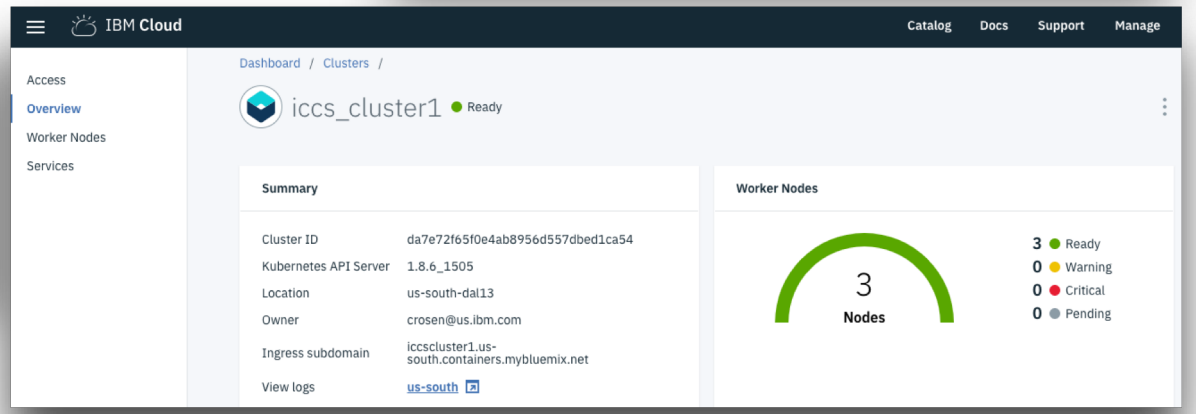
Create and Manage Kubernetes Clusters

Kubernetes Cluster Management Experience




```
→ bx cs clusters
Listing clusters...
OK
Name        ID                                State    Created                Workers
cj          337c42379cd044fb82070462bdb09215  normal   2017-05-03T12:28:46+0000  3
istio2      33ec4642167541ae9b902ab20dc6f8a7  normal   2017-05-10T18:20:45+0000  3
istiotest   2545b88130f7415cb8f2b0b8e90f97d7  normal   2017-05-05T04:15:07+0000  2
mycluster   79f5a344558a456e988dc8f1406b20f4  normal   2017-05-11T02:48:19+0000  1
trusted     395079b801364d7e83918ea94c4fd7ca  normal   2017-04-11T00:37:55+0000  3
```

```
→ bx cs cluster-get cj
Retrieving cluster cj...
OK
Name:           cj
ID:             337c42379cd044fb82070462bdb09215
Created:        2017-05-03T12:28:46+0000
State:          normal
Master URL:     https://169.47.234.18:10317
Ingress host:   cj.us-south.containers.mybluemix.net
Ingress secret: cj
Workers:        3
```



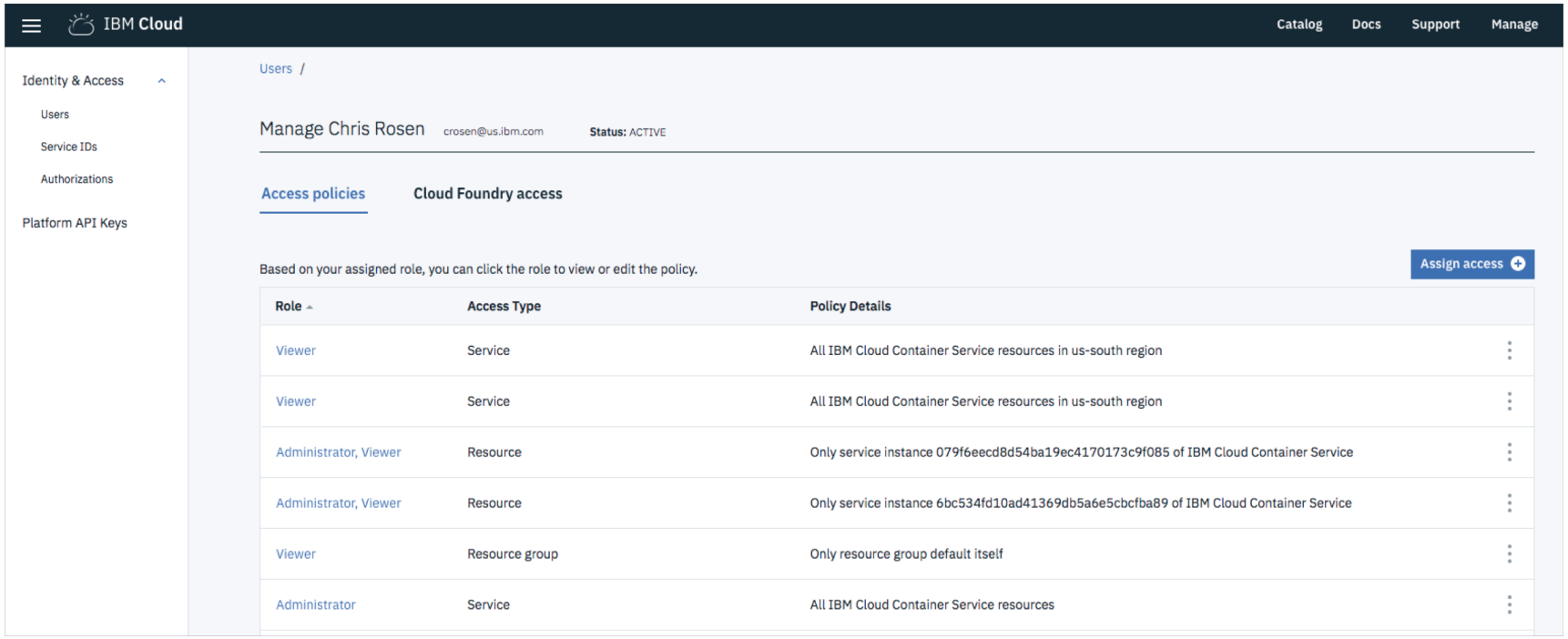

```
→ bx cs workers cj
Listing cluster workers...
OK
ID                                                  Public IP       Private IP      Machine Type  State   Status
kube-dal10-cr337c42379cd044fb82070462bdb09215-w1    169.47.220.231  10.171.61.21   u1c.2x4       normal  Ready
kube-dal10-cr337c42379cd044fb82070462bdb09215-w2    169.47.220.235  10.171.61.58   u1c.2x4       normal  Ready
kube-dal10-cr337c42379cd044fb82070462bdb09215-w3    169.47.220.201  10.171.61.51   u1c.2x4       normal  Ready
```

Kubernetes In-Cluster Experience

RBAC with IBM Cloud IAM

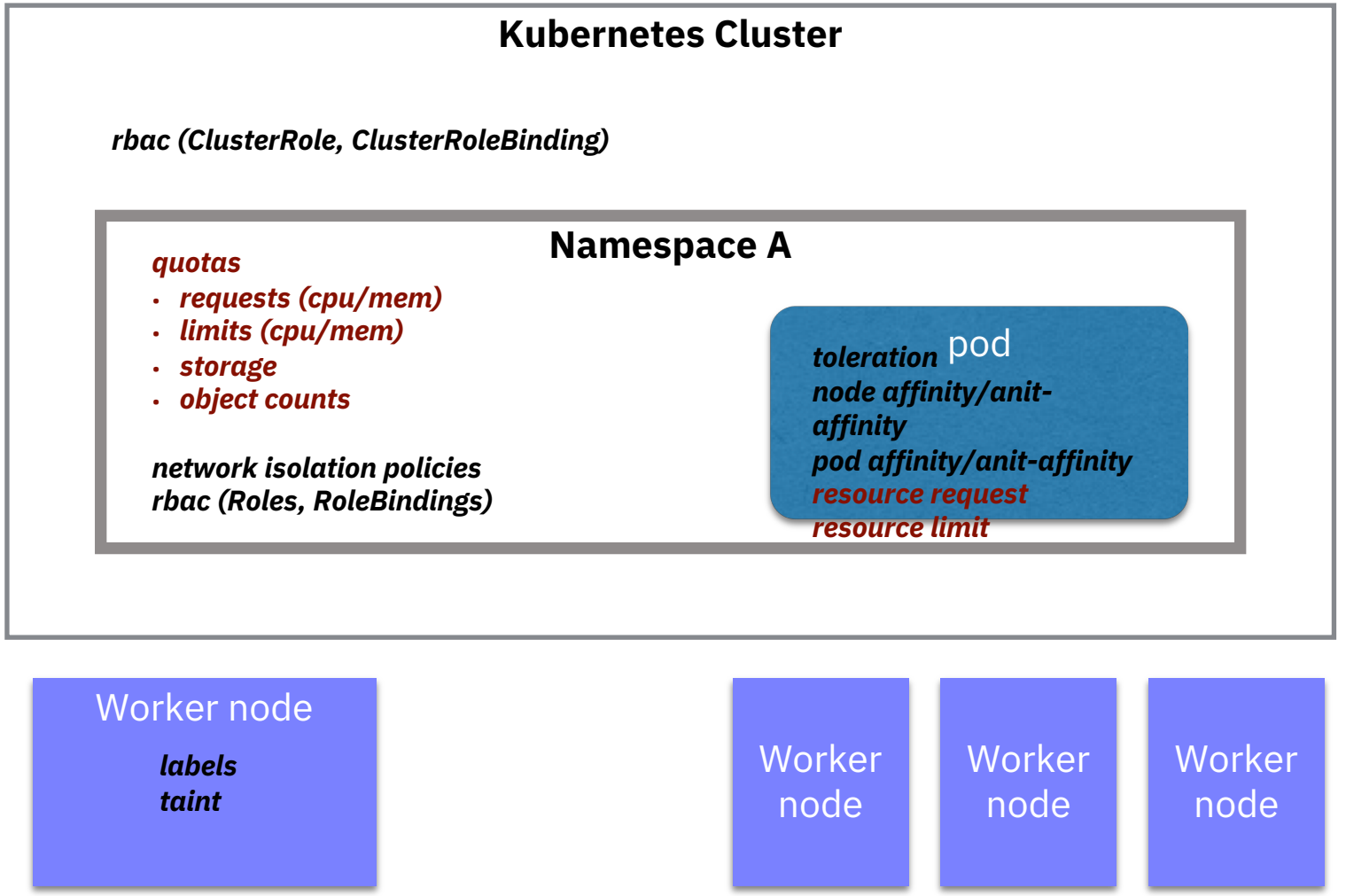
Use IBM Cloud authorization service (IAM) to set Kubernetes RBAC policies

Consistent way to set authorization across cloud resources



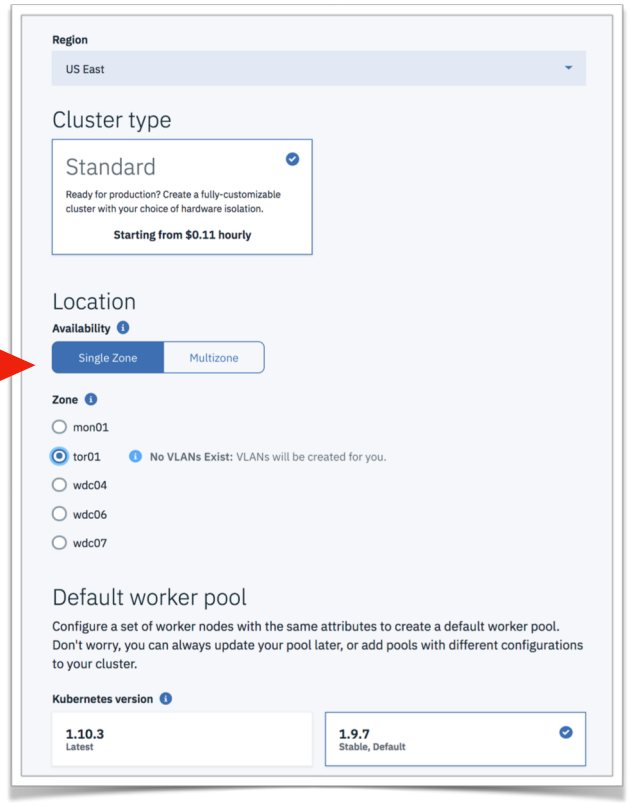
Isolation and scheduling control

Managing isolation within a Cluster

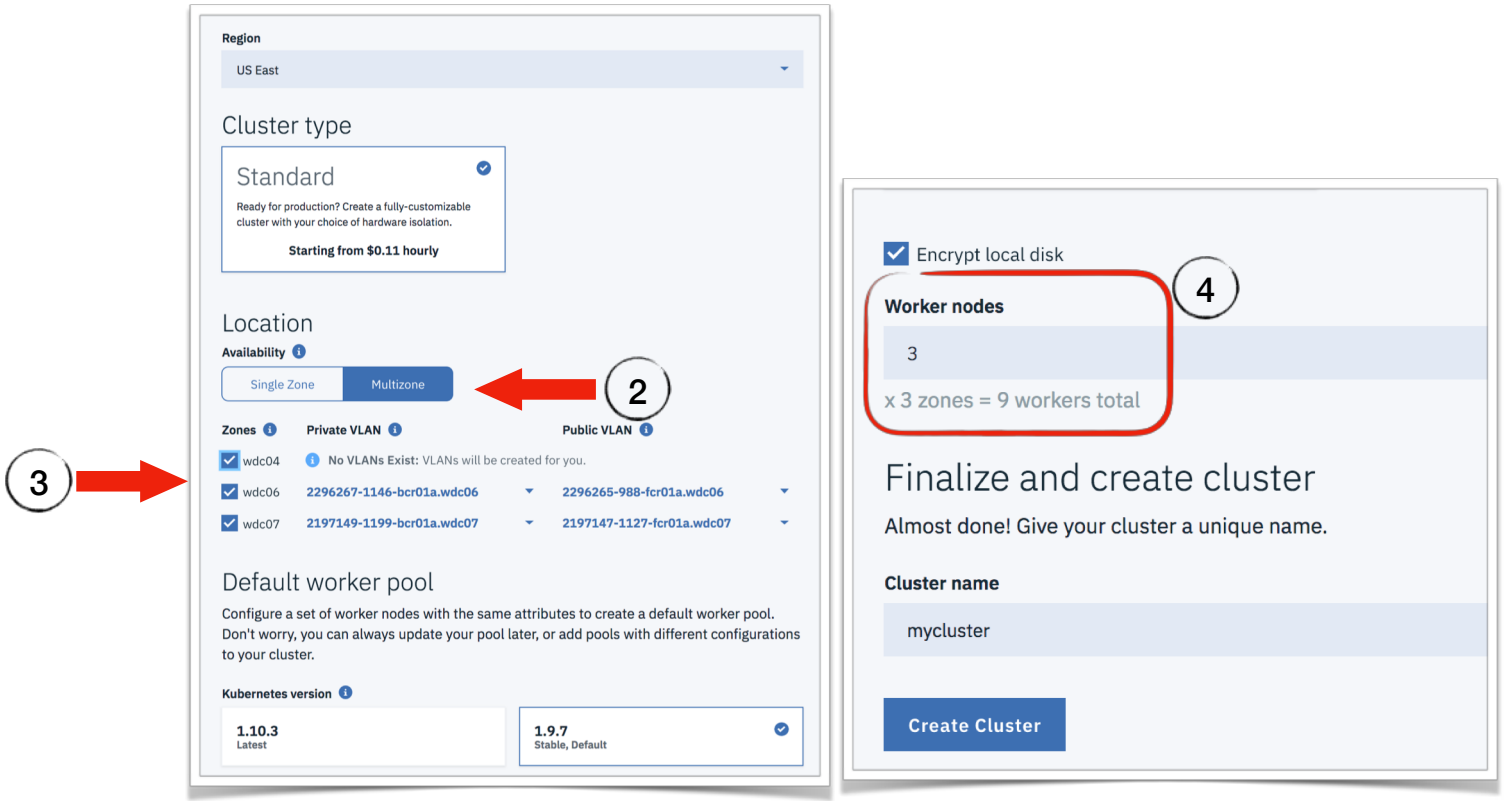


Create Cluster

Single Zone Cluster



Multizone Cluster



IBM CODE

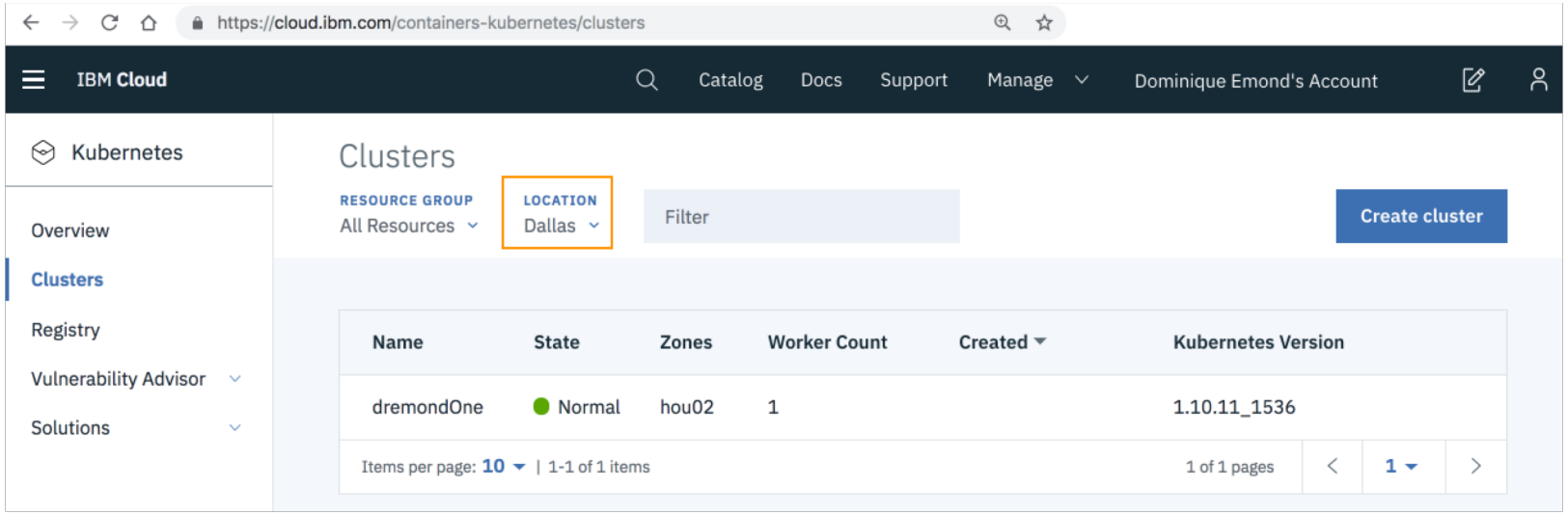
Hands On:
Create a Kubernetes Cluster

Flow:

1. Create IBM Account
2. Apply : Promo Code
3. Create Cluster

Technology stack:

- IBM Public Cloud
- Kubernetes



IBM CODE

Resources

Code Patterns

- https://developer.ibm.com/patterns/category/containers/

IBM Cloud Kubernetes Service

- https://cloud.ibm.com/docs/containers?topic=containers-getting-started