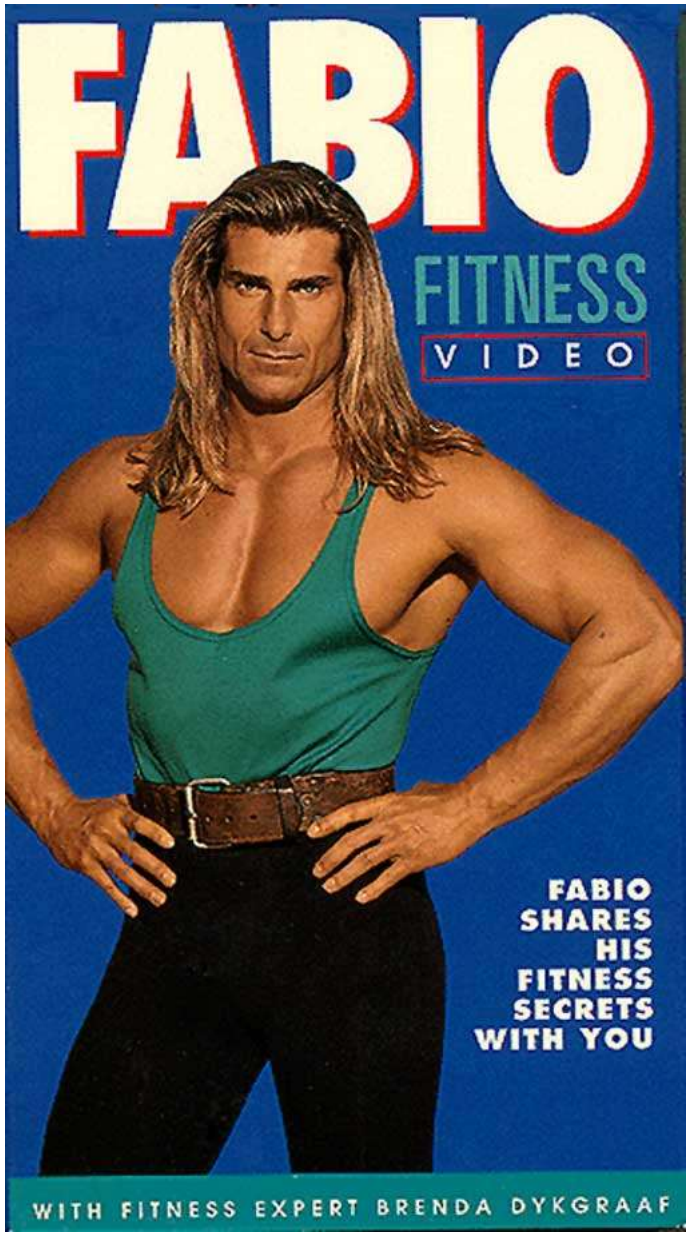
VMware & Pivotal's
Pivotal Container Service (PKS)

vmware®

whoami

- Fabio Rapposelli
- Staff Engineer 2 a VMware
- https://github.com/frapposelli

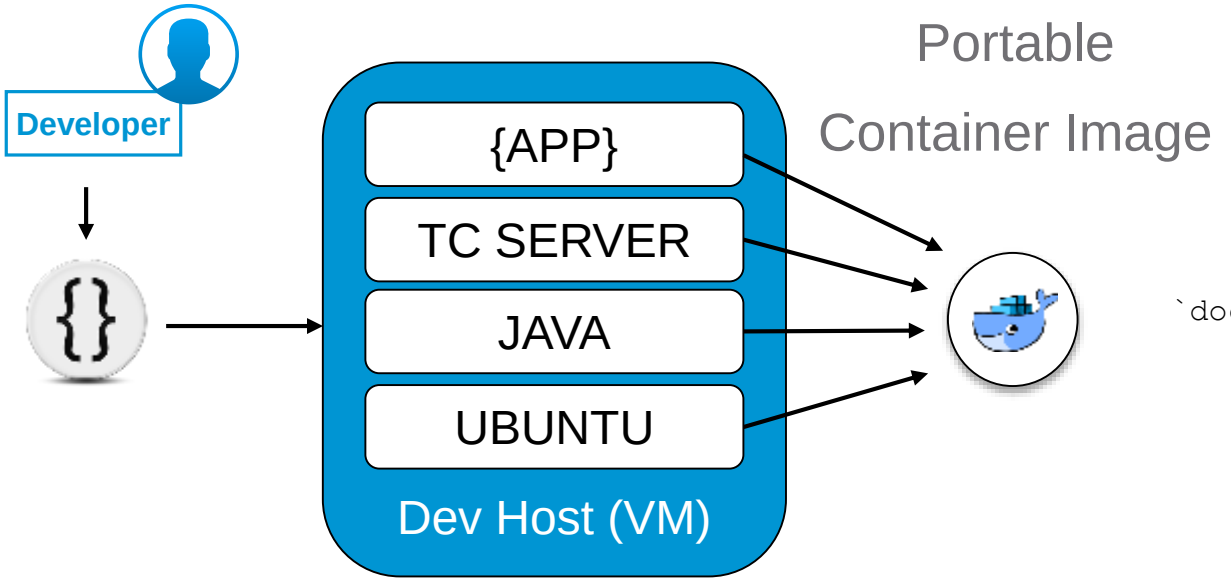


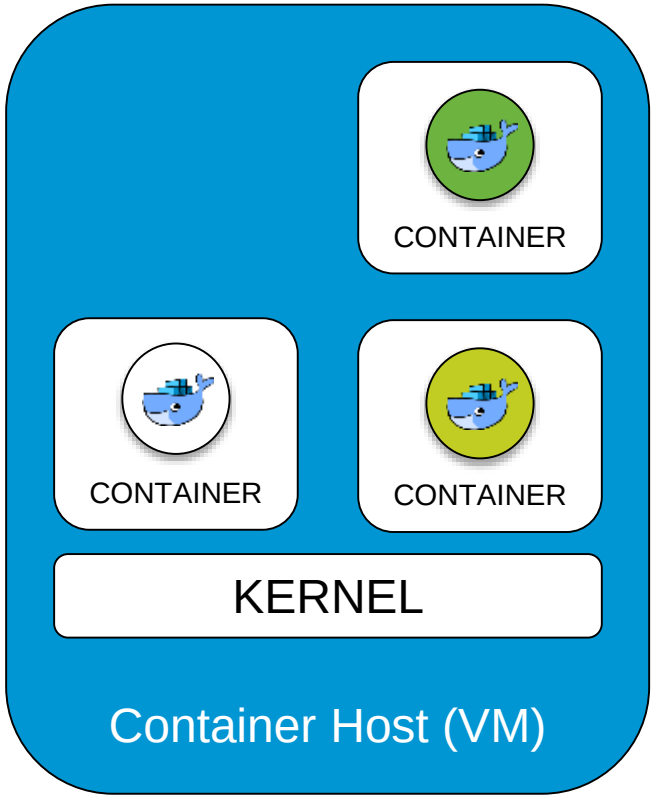
vmware

Agenda

1	**Containers, CaaS, & PaaS 101**
2	Why PKS
3	PKS Technical Overview
4	Packaging & Support

Containers 101





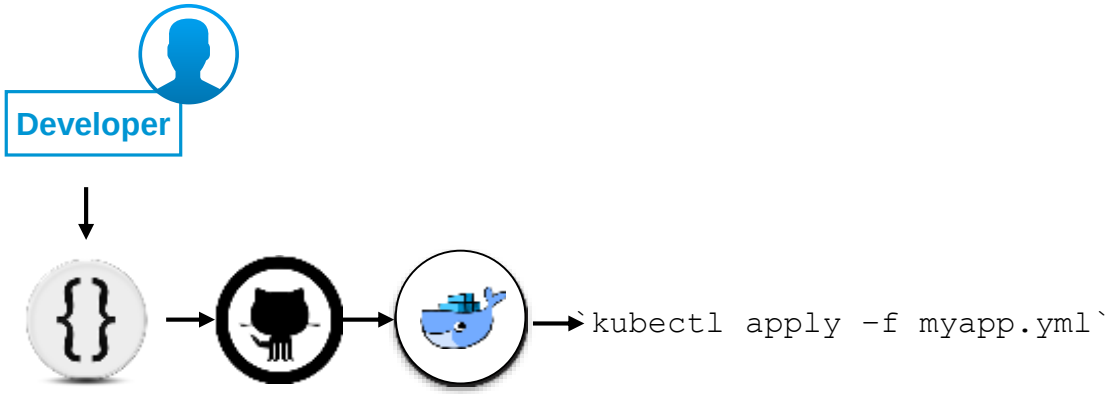
- **Reliable Packaging**
- **Server/VM Density**
- **Fast Time To Launch**
- **Built for CI/CD**

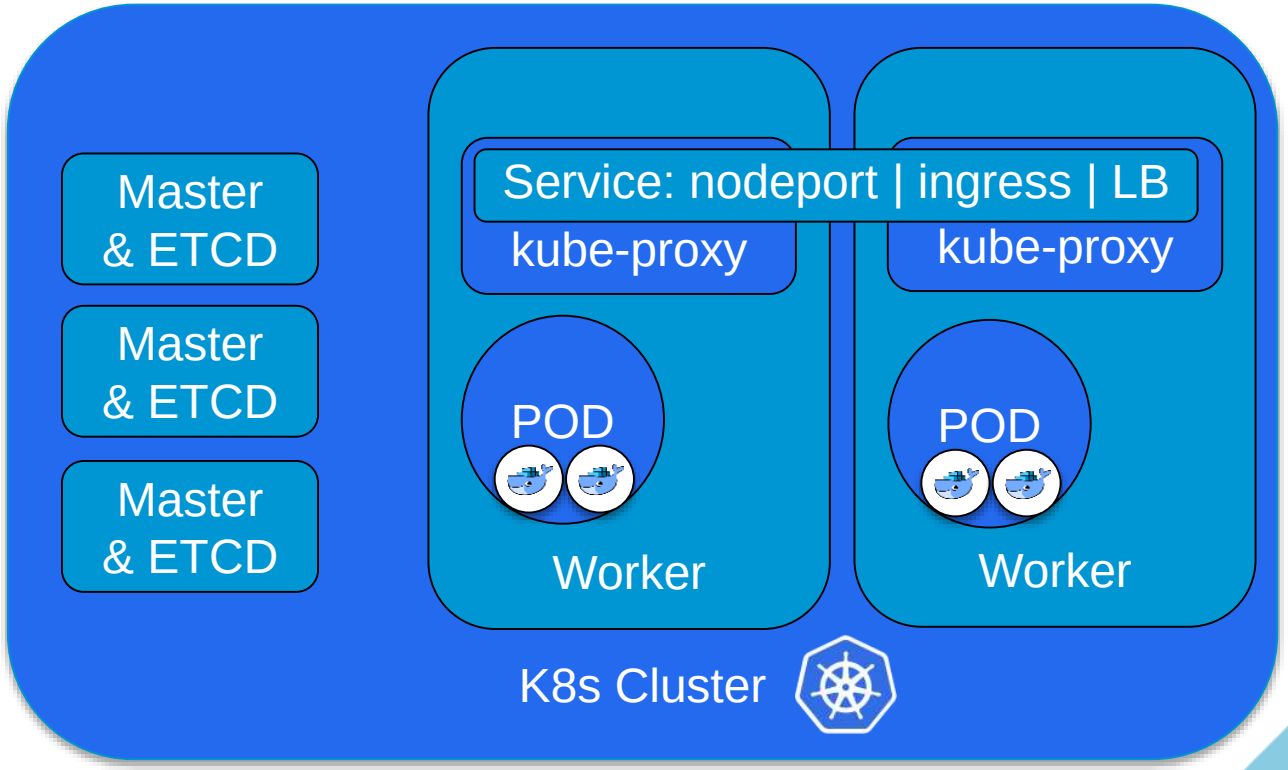
Kubernetes 101 (CaaS)

Containers @ Scale

URL Request:
myapp.foo.com/k8siscool

Load Balancer



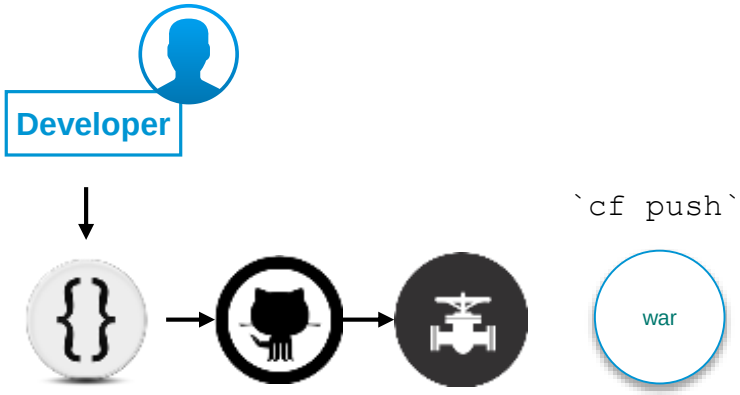


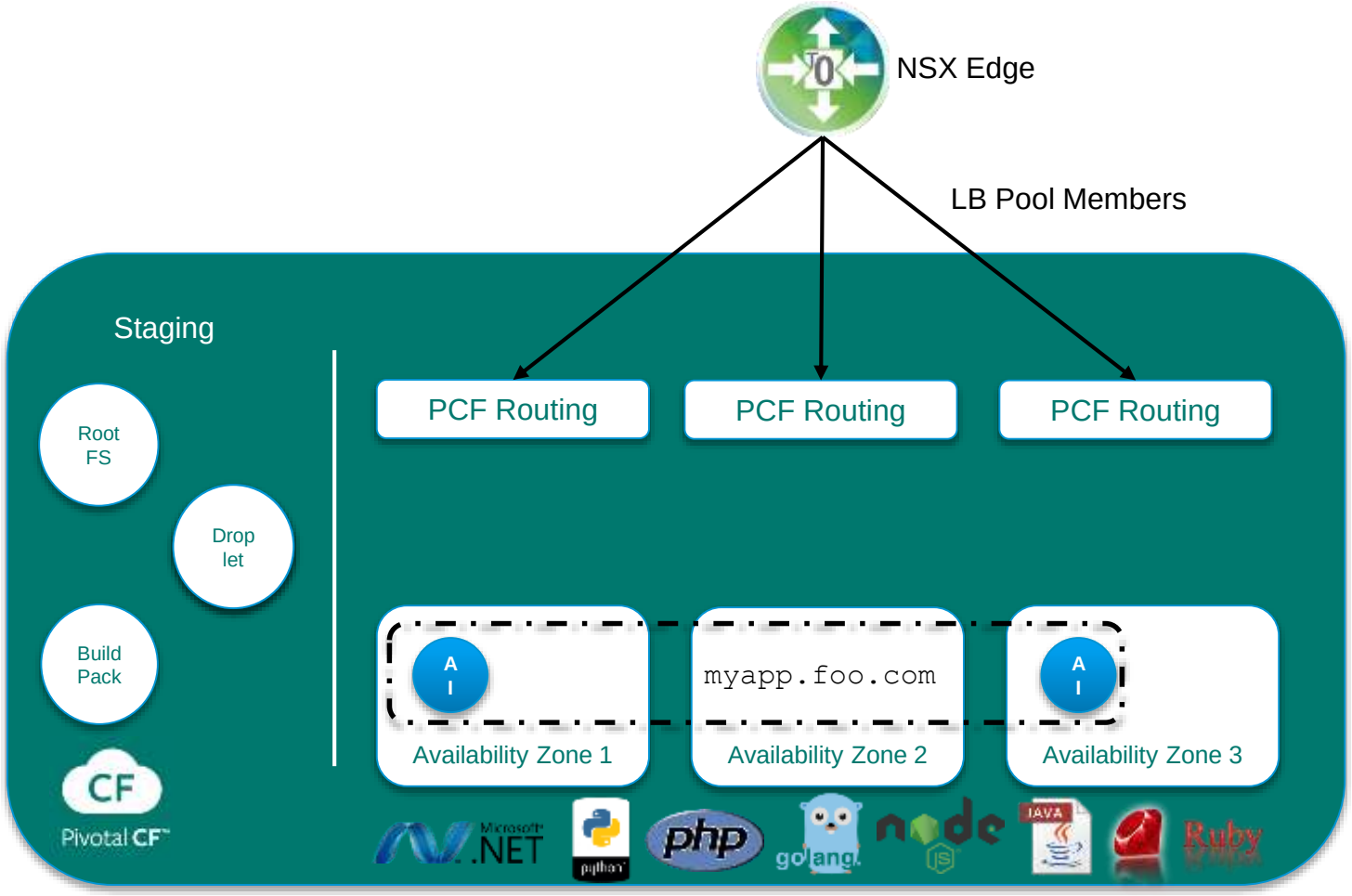
vmware

Pivotal Cloud Foundry 101 (PaaS)

URL Request:
myapp.foo.com

*.foo.com = NSX Edge Vip





“Here is my source code

Run it on the cloud for me

I do not care how”

Agenda

1	Containers, CaaS, & PaaS 101
2	**Why PKS**
3	PKS Technical Overview
4	Packaging & Support

75%

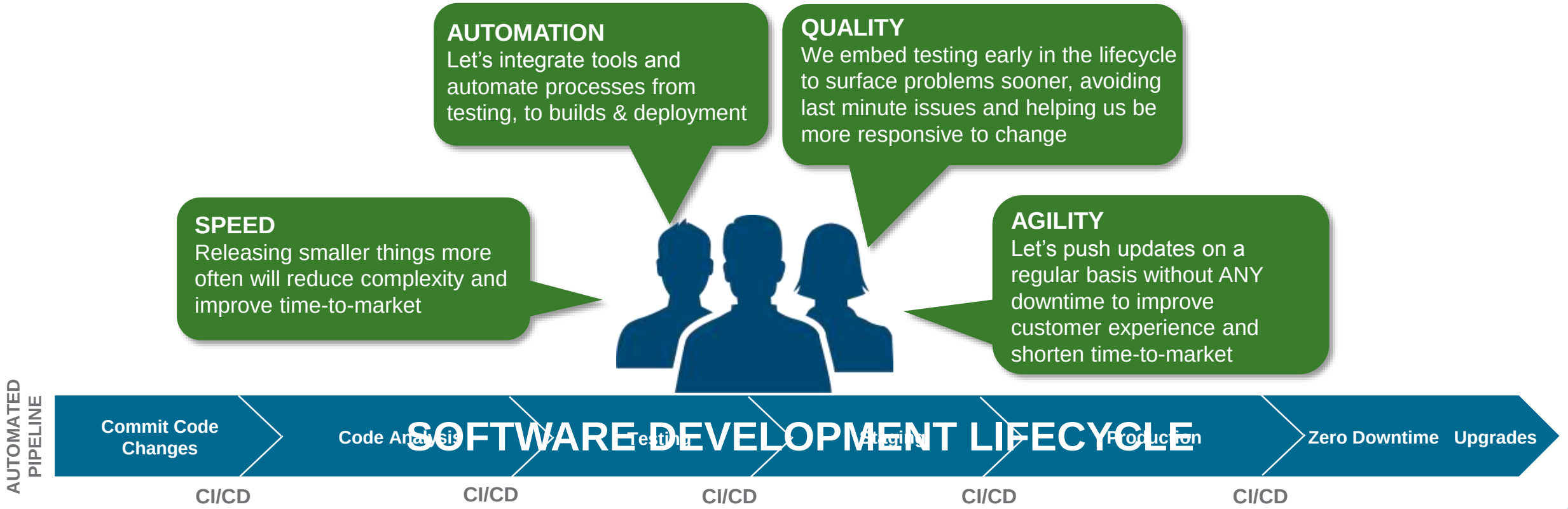
Of Applications will be “Built”, not “Bought” by 2020

Source: Gartner

vmware

Problem to Solve, Faster Time To Value …

Agile methods help drive Digital Transformation



Drive Business Value into Production Faster and Safer

Multiple Use Cases Dictate Multiple Workloads and Approaches

The Goal:
Pick the Right Approach for the Workload

CONTAINERS

BATCHES

MONOLITHIC APPLICATIONS

DATA SERVICES

MICROSERVICES

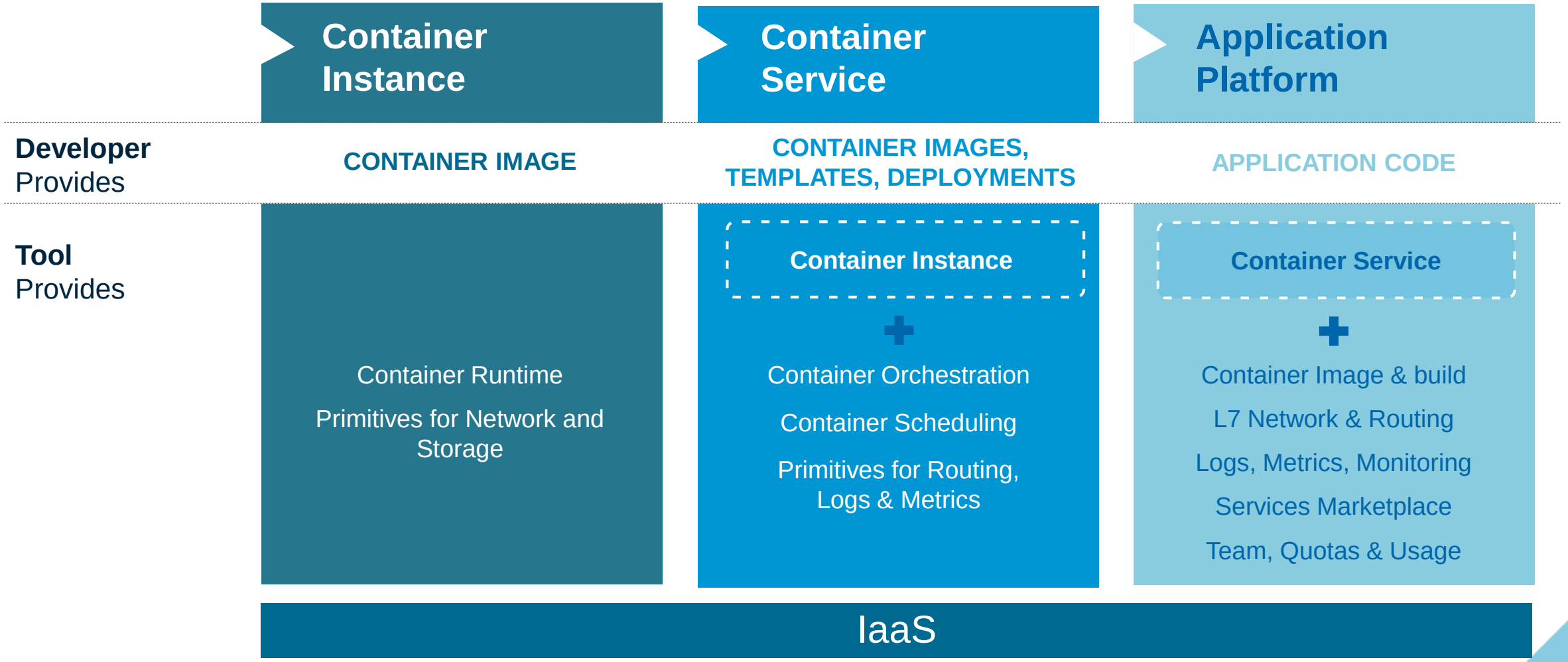
Container Instance (CI)

Container Service (CaaS)

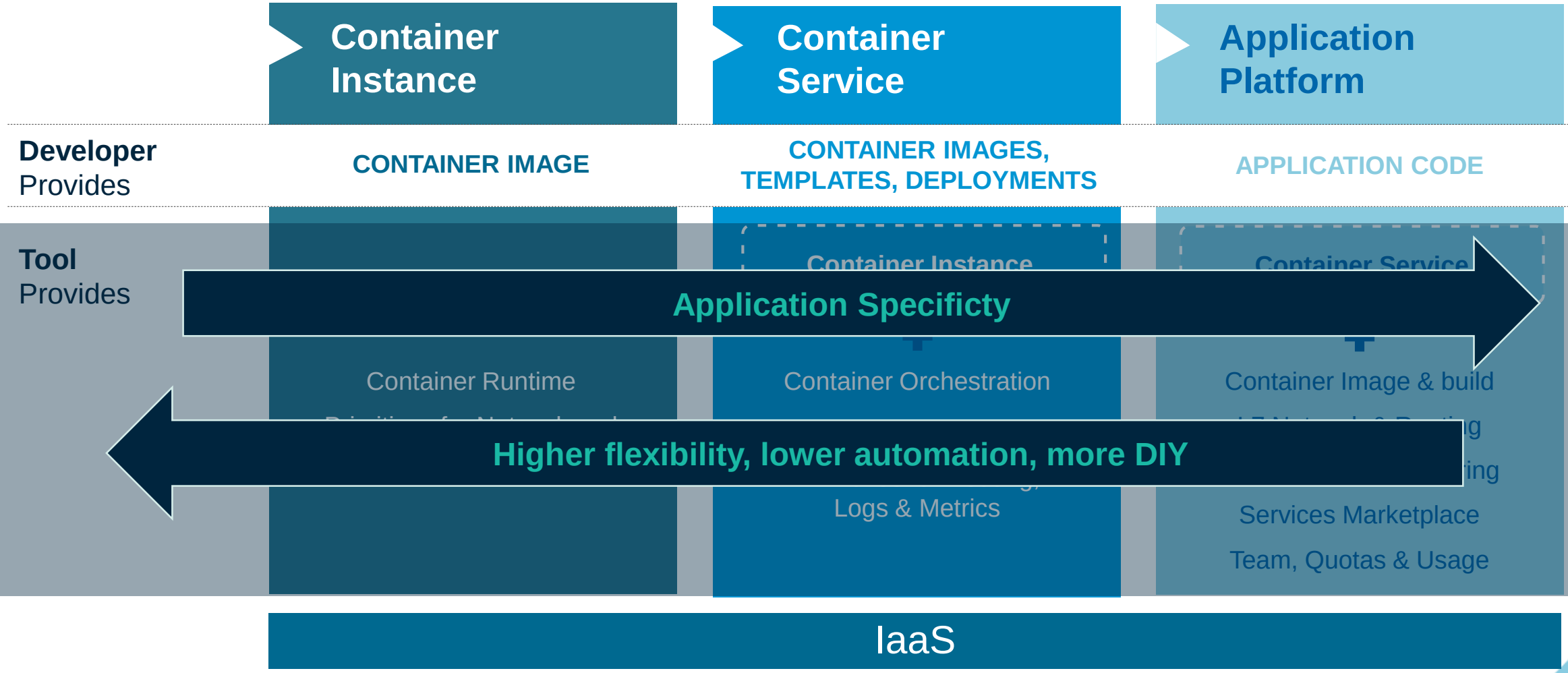
Application Platform (PaaS)

IaaS

Choosing the Right Tool for the Job



Choosing the Right Tool for the Job



Choosing the Right Tool for the Job

	Container Instance	Container Service	Application Platform
Abstraction	CONTAINER IMAGE	CONTAINER IMAGES, TEMPLATES, DEPLOYMENTS	APPLICATION CODE

Pivotal Container Service

Pivotal Cloud Foundry
Elastic Runtime

CLOUDFOUNDRY

BOSH

IaaS

Agenda

1	Containers, CaaS, & PaaS 101
2	Why PKS
3	**PKS Technical Overview**
4	Packaging & Support

VMware and Pivotal Collaborate to Deliver
VMware Pivotal Container Service (VMware PKS)

Purpose-built container service to operationalize Kubernetes for the multi-cloud enterprises and service providers

Fully Supported Kubernetes

Deep Integration with NSX

Runs on vSphere and VMC

Hardened, Production-grade

Unified VM + Containers on SDDC

HA, Security, Multi-tenancy, Tools

vmware

VMware PKS – Solving Day-2 Operational Challenges

High Availability

Fault-tolerance for masters, workers, and etcd nodes

Scaling

Auto-scaling of masters, workers, and etcd nodes

Health Checks & Healing

Routine health checks and self-healing of cluster

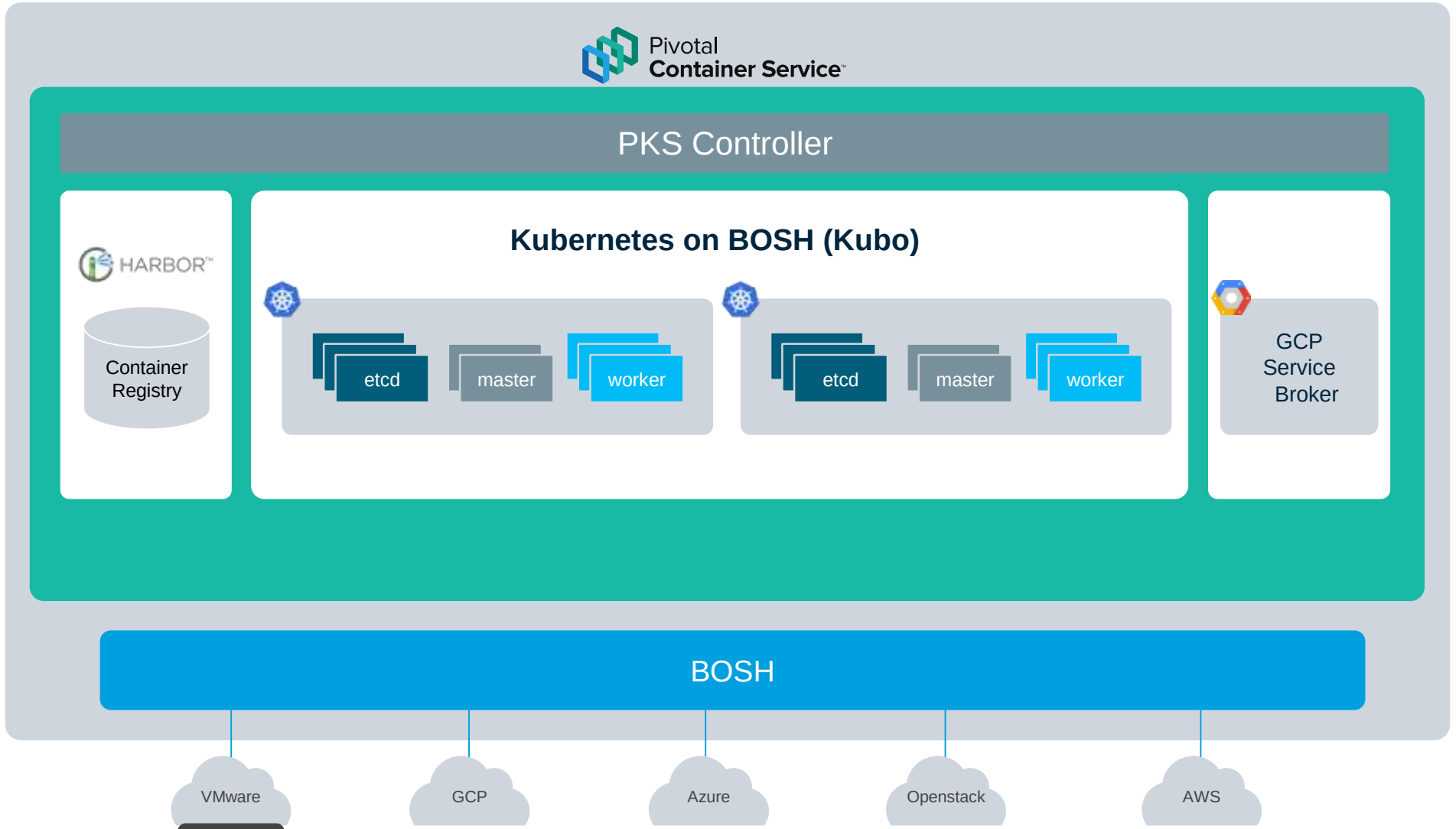
Lifecycle Management

LCM includes rolling upgrades to ensure workload uptime & application of CVEs

vmware

Container Infrastructure for Cloud-Native Apps

Rapidly deliver and operationalize next generation apps



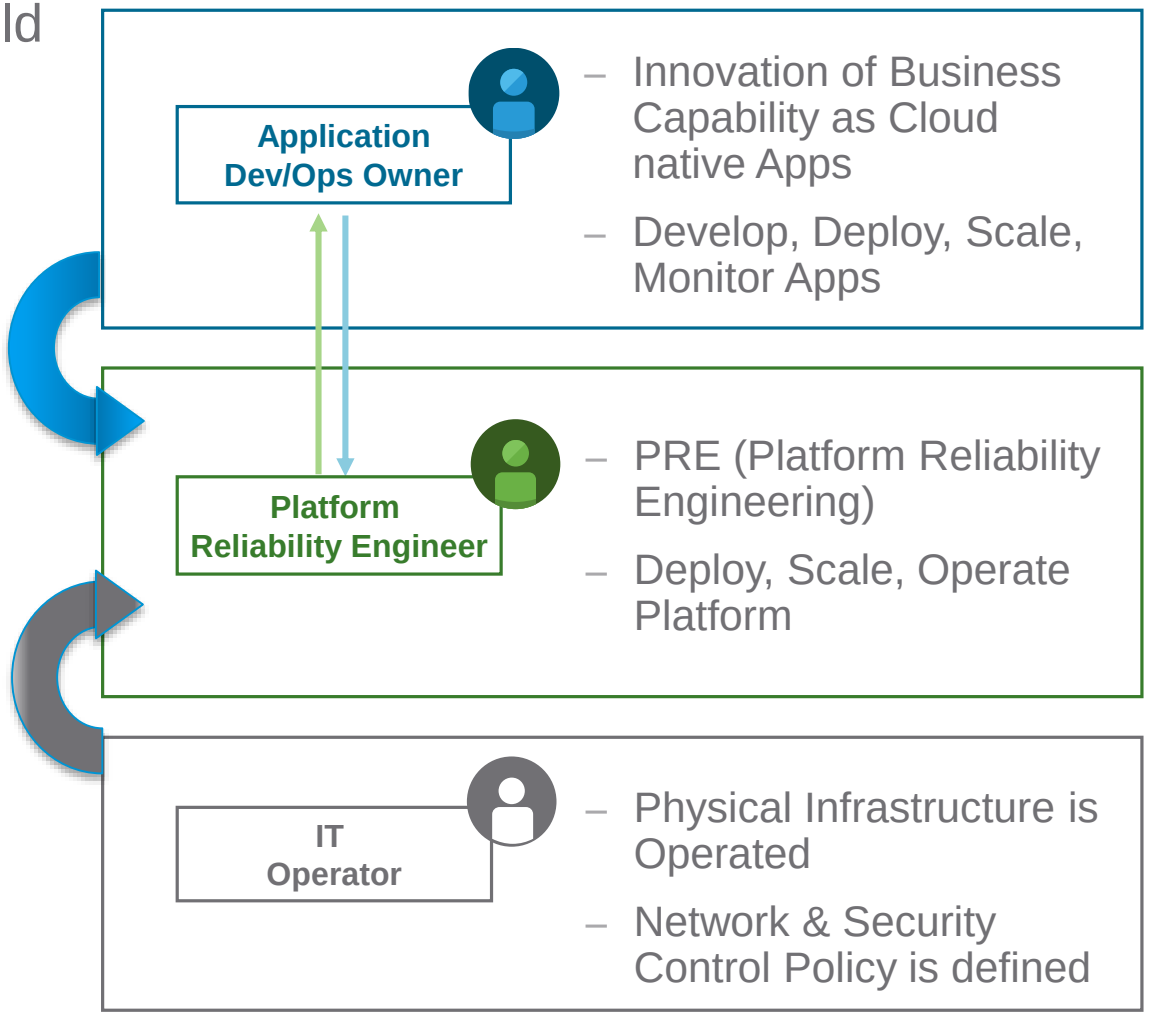
Who is PKS built for?

Cloud Native Applications at scale can & should be kept running by a 2 Pizza Team mentality (DevOps in Action)

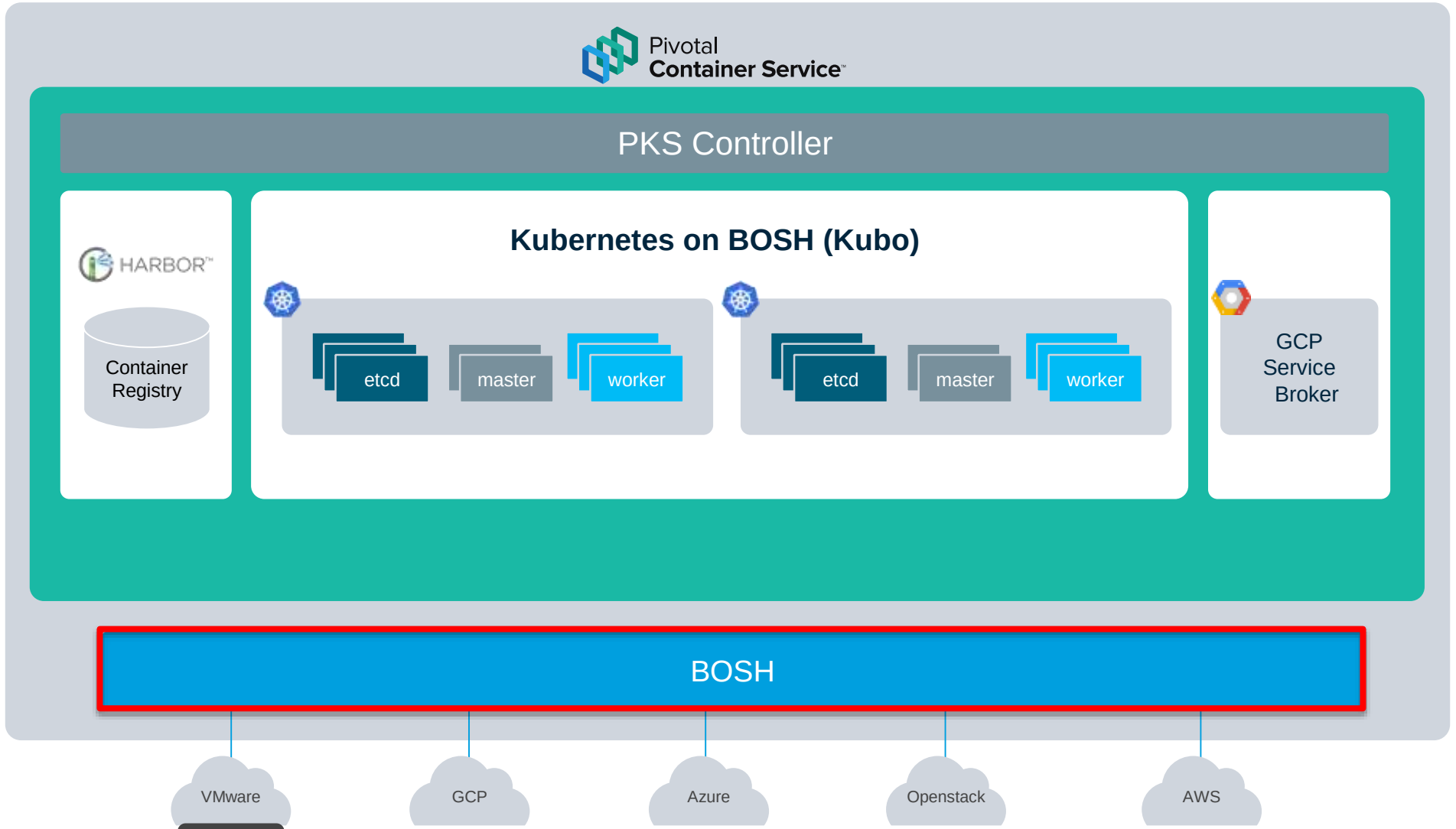
- **Platform Reliability Engineers**
  - Platform is **Reliable**
  - **Capacity** Is planned for
  - Platform is **Secured** & **Controlled**
  - Platform is **Auditable**
  - Application Dev/Ops owners are **Agile**
- **Application Dev/Ops owner**
  - Automate Everything
  - Agile

** Role Shift*

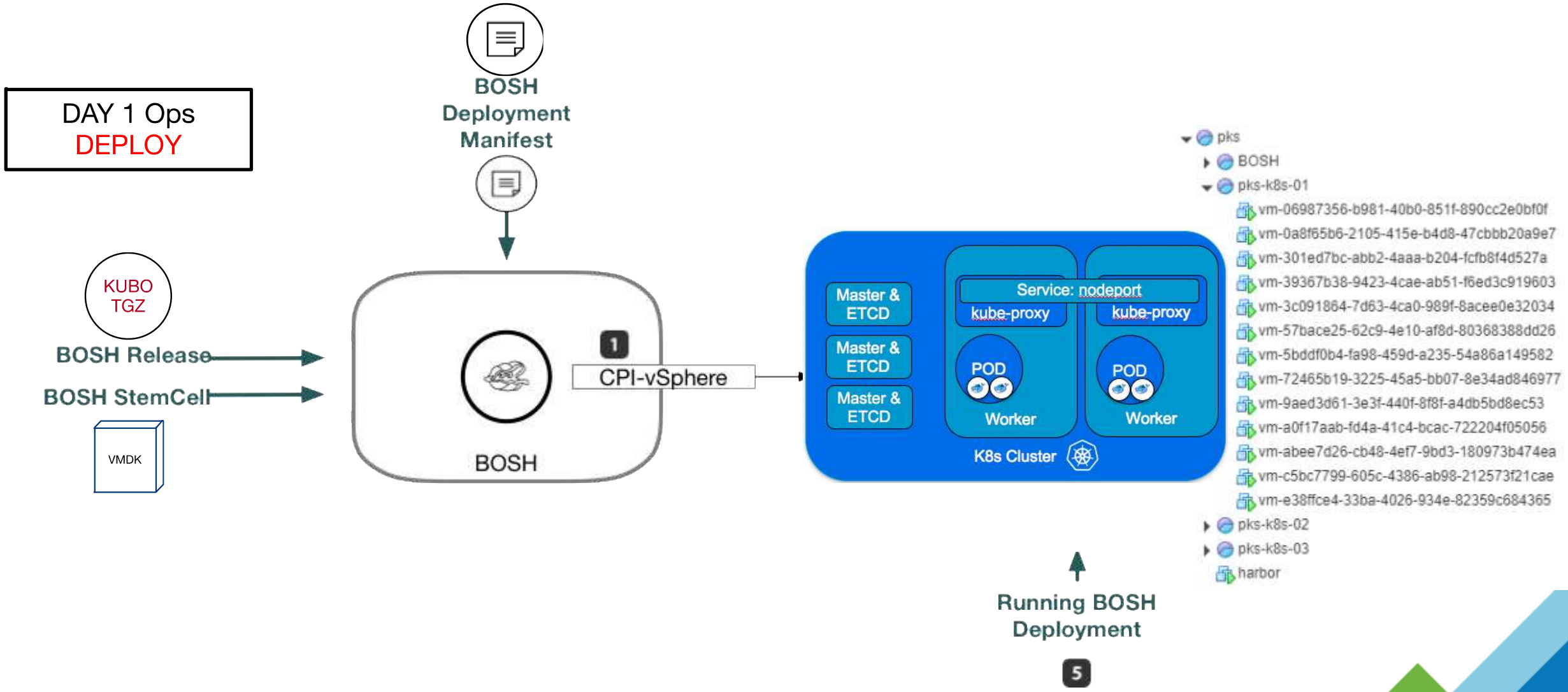
- *It is common to see the VI Admins (IT Ops), becoming the Platform Reliability Engineer*



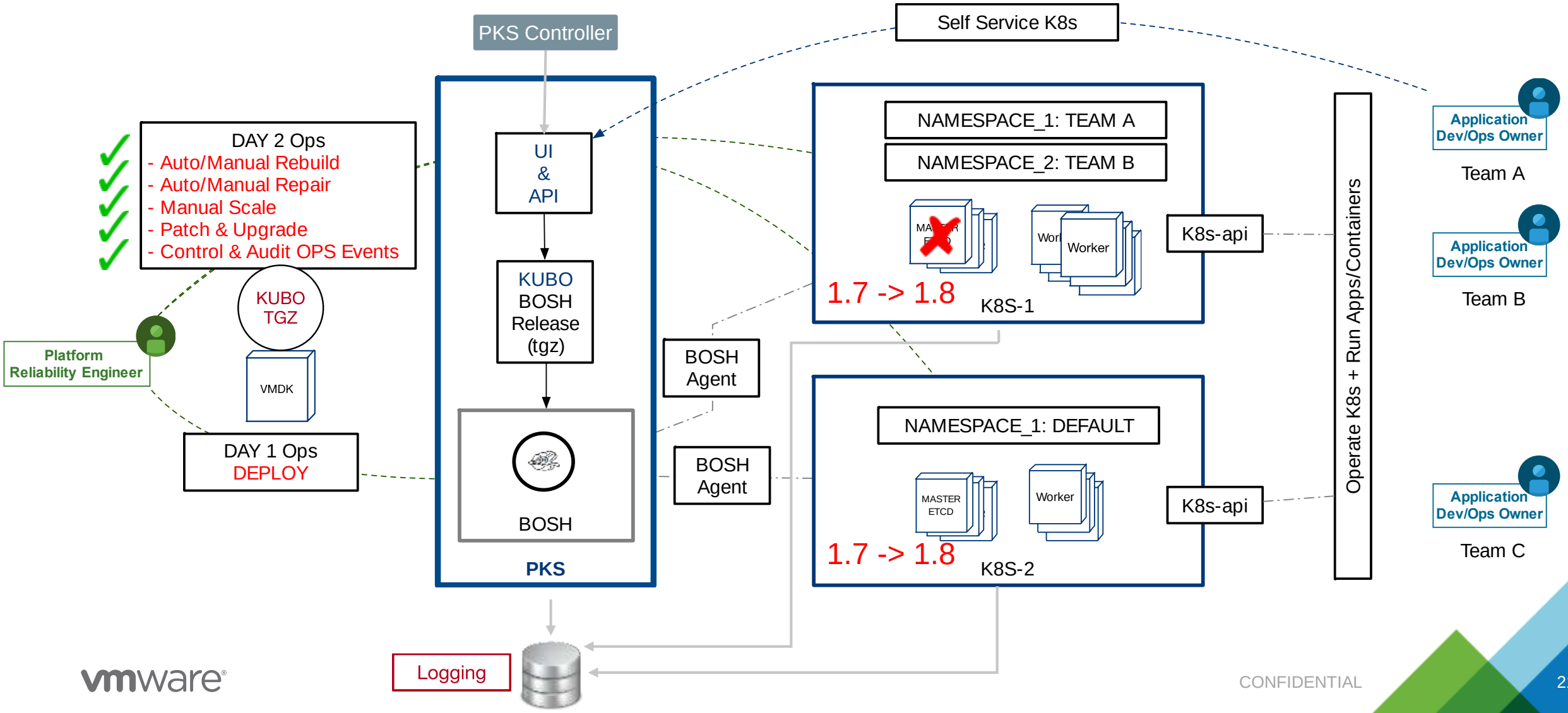
PKS Technical Overview



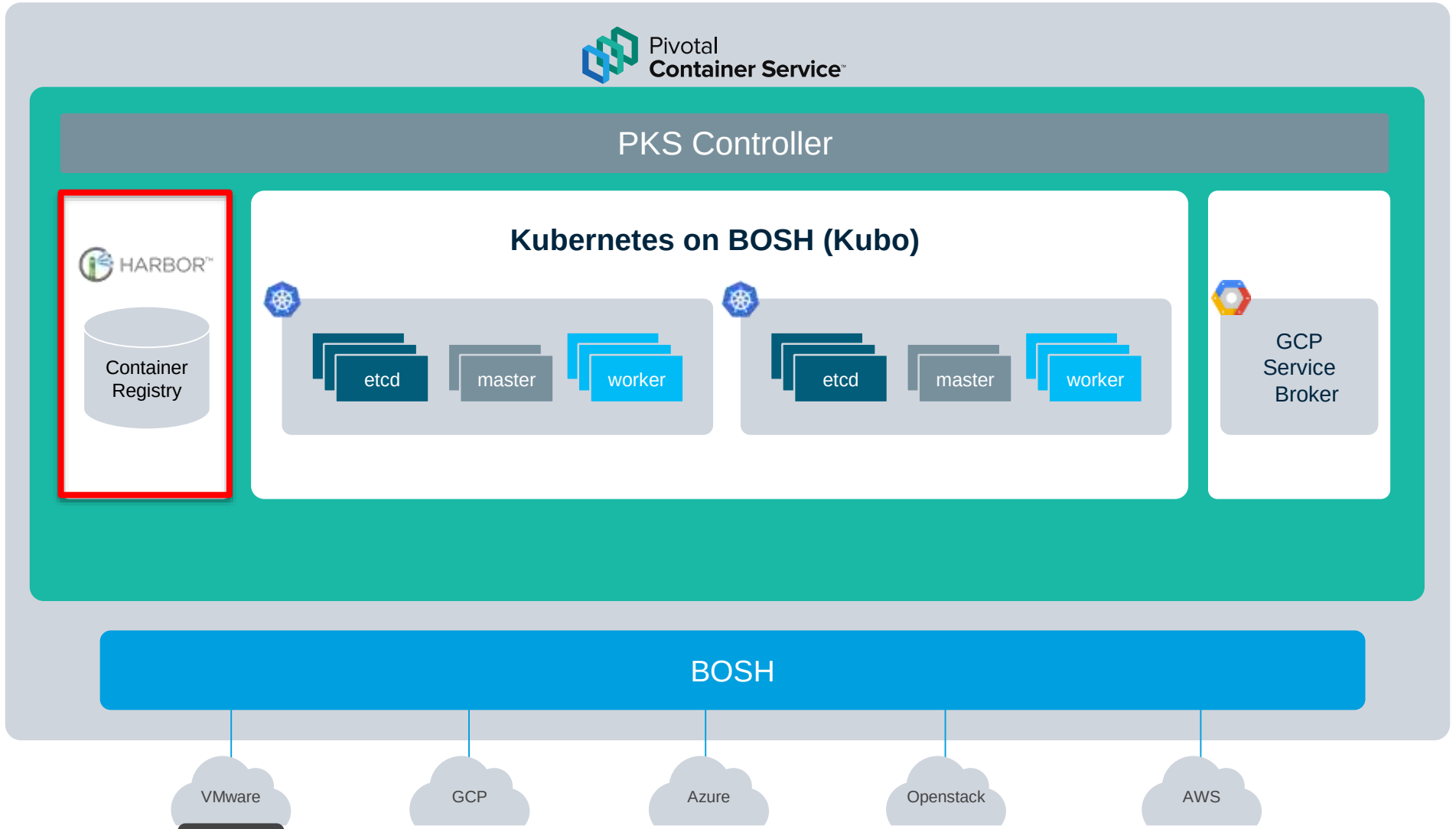
BOSH Day 1


DAY 1 Ops
DEPLOY
BOSH
Deployment
Manifest
KUBO
TGZ
BOSH Release
BOSH StemCell
VMDK
1
CPI-vSphere
BOSH
Master &
ETCD
Master &
ETCD
Master &
ETCD
Service: nodeport
kube-proxy
kube-proxy
POD
POD
Worker
Worker
K8s Cluster
pks
BOSH
pks-k8s-01
vm-06987356-b981-40b0-851f-890cc2e0bf0f
vm-0a8f65b6-2105-415e-b4d8-47cbbb20a9e7
vm-301ed7bc-abb2-4aaa-b204-fcfb8f4d527a
vm-39367b38-9423-4cae-ab51-f6ed3c919603
vm-3c091864-7d63-4ca0-989f-8acee0e32034
vm-57bace25-62c9-4e10-af8d-80368388dd26
vm-5bddf0b4-fa98-459d-a235-54a86a149582
vm-72465b19-3225-45a5-bb07-8e34ad846977
vm-9aed3d61-3e3f-440f-8f8f-a4db5bd8ec53
vm-a0f17aab-fd4a-41c4-bcac-722204f05056
vm-abee7d26-cb48-4ef7-9bd3-180973b474ea
vm-c5bc7799-605c-4386-ab98-212573f21cae
vm-e38ffce4-33ba-4026-934e-82359c684365
pks-k8s-02
pks-k8s-03
harbor
Running BOSH
Deployment
5

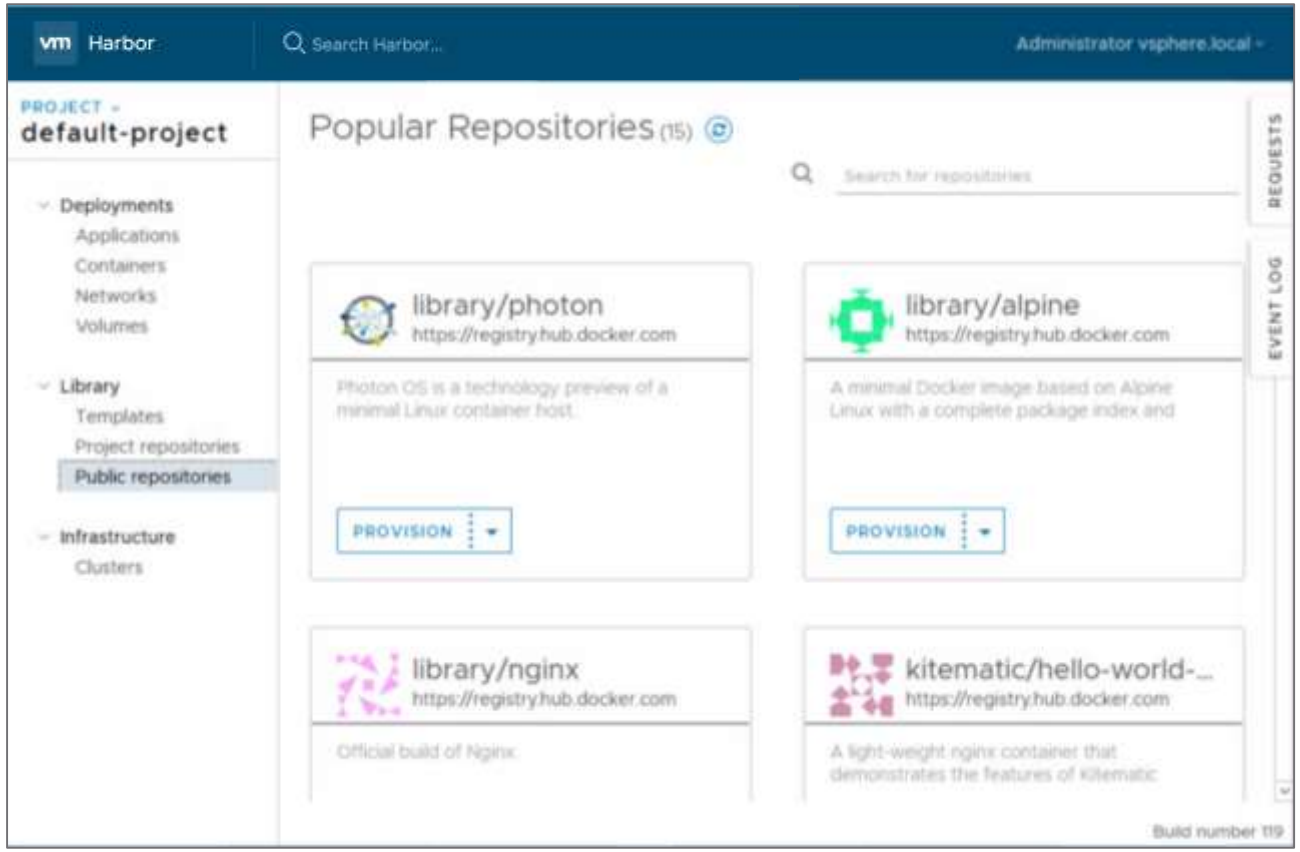
BOSH Day 2


PKS Controller
Self Service K8s
DAY 2 Ops
- Auto/Manual Rebuild
- Auto/Manual Repair
- Manual Scale
- Patch & Upgrade
- Control & Audit OPS Events
UI
&
API
KUBO
BOSH
Release
(tgz)
KUBO
TGZ
VMDK
Platform
Reliability Engineer
DAY 1 Ops
DEPLOY
BOSH
PKS
BOSH
Agent
BOSH
Agent
NAMESPACE_1: TEAM A
NAMESPACE_2: TEAM B
Worker
1.7 -> 1.8
K8S-1
K8s-api
NAMESPACE_1: DEFAULT
MASTER
ETCD
Worker
1.7 -> 1.8
K8S-2
K8s-api
Operate K8s + Run Apps/Containers
Application
Dev/Ops Owner
Team A
Application
Dev/Ops Owner
Team B
Application
Dev/Ops Owner
Team C
Logging

PKS Technical Overview

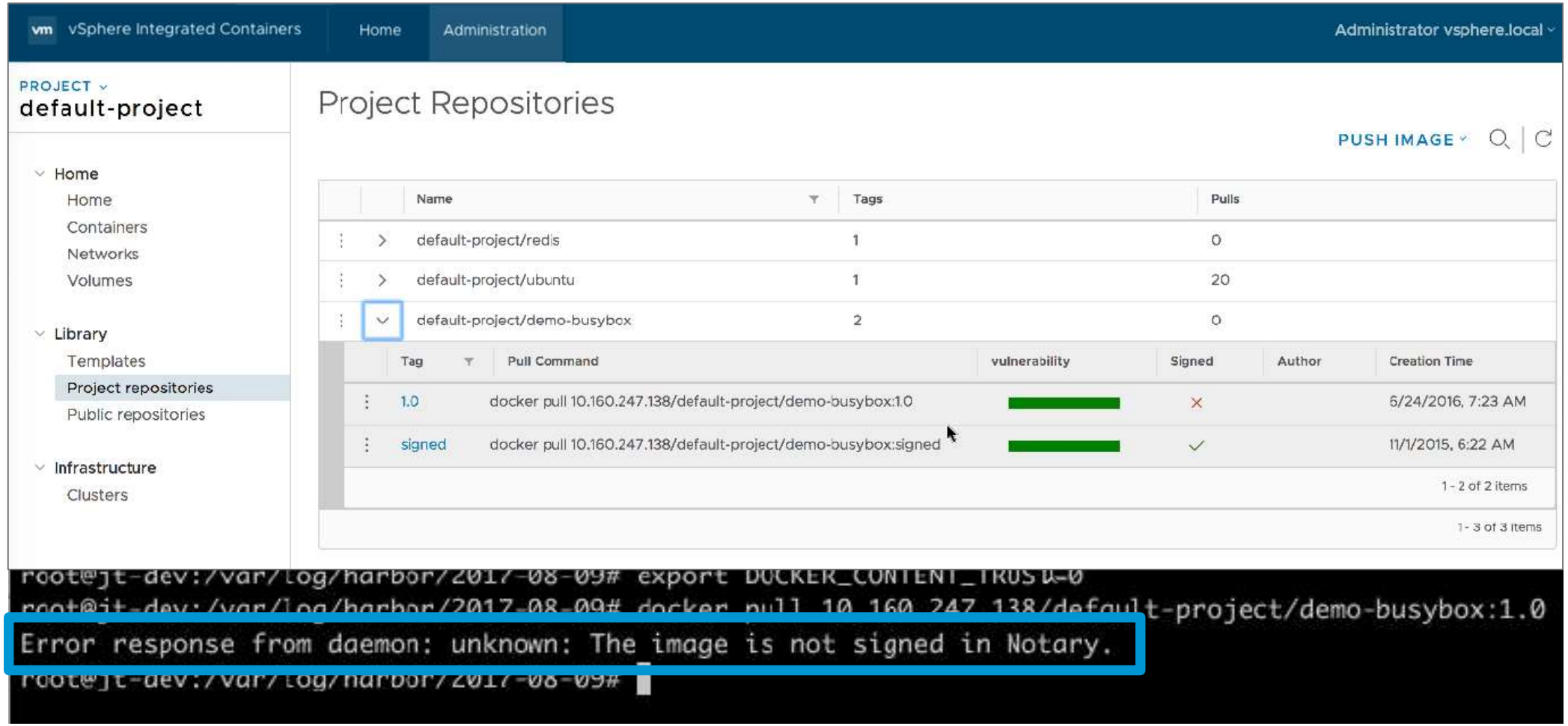


Harbor – Enterprise Grade Private Registry



- **user** management & access control
- role-based **access control**
- **AD/LDAP** integration
- Security **vulnerability scanning (Clair)**
- content trust - **image signing**
- policy based image **replication**
- **audit** and **logs**
- Restful **API**
- **open-source** under Apache 2 license

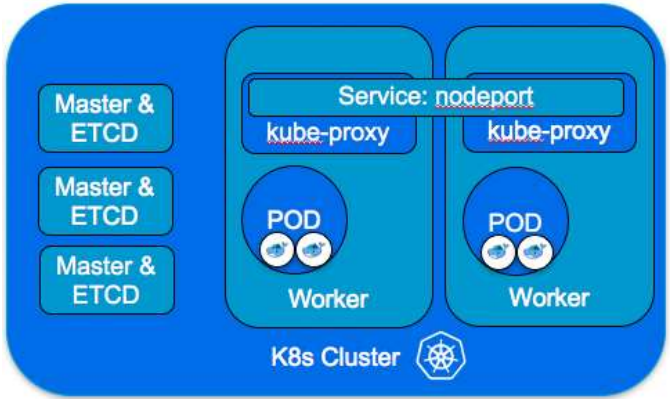
Harbor – Content Trust,
When Enabled Un-signed Images Can't Be Pulled



Harbor – Image Vulnerability Scanning Details (Clair)

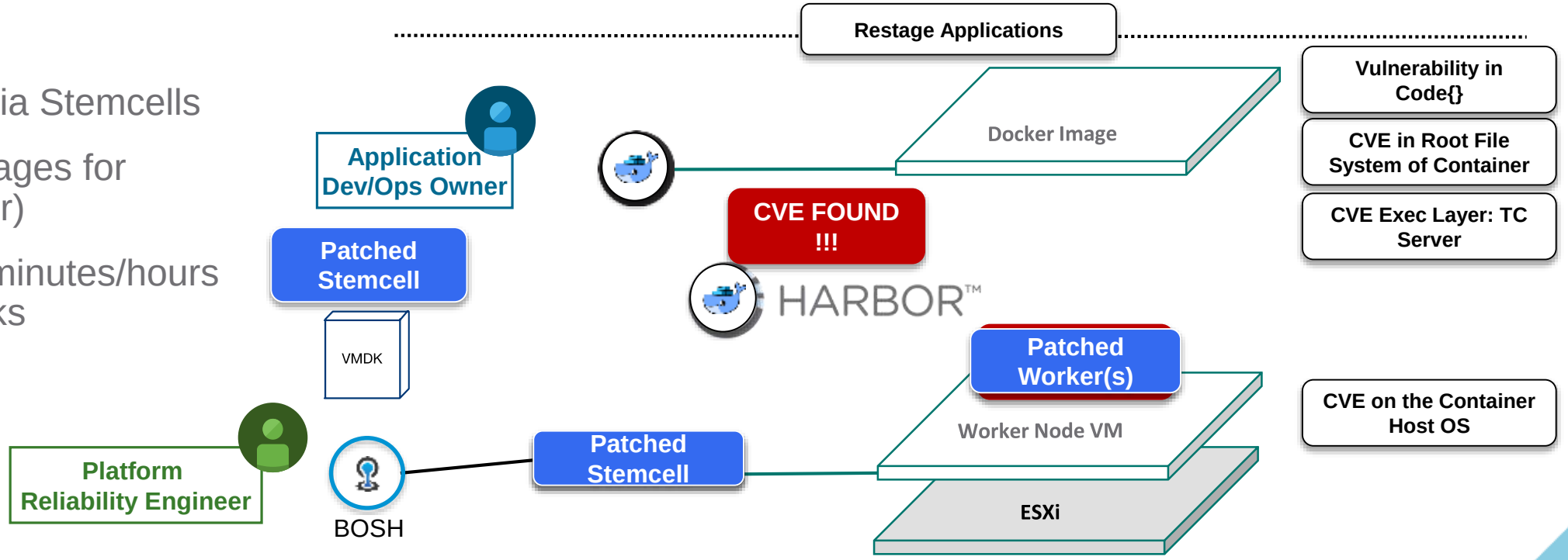
Vulnerability	Severity	Package	Current version	Fixed in version
CVE-2016-1252	high	apt	1.0.1ubuntu2.6	1.0.1ubuntu2.17
CVE-2016-5011	low	util-linux	2.20.1-5.1ubuntu20.3	
Description: The parse_dos_extended function in partitions/dos.c in the libblkid library in util-linux allows physically proximate attackers to cause a denial of service (memory consumption) via a crafted MSDOS partition table with an extended partition boot record at zero offset.				
CVE-2014-9114	low	util-linux	2.20.1-5.1ubuntu20.3	
CVE-2013-0157	low	util-linux	2.20.1-5.1ubuntu20.3	
CVE-2017-6350	low	vim	2:7.4.052-1ubuntu3	
CVE-2017-5953	low	vim	2:7.4.052-1ubuntu3	
CVE-2017-6349	low	vim	2:7.4.052-1ubuntu3	
CVE-2016-1248	medium	vim	2:7.4.052-1ubuntu3	2:7.4.052-1ubuntu3.1
CVE-2017-9525	low	cron	3.0pl1-124ubuntu2	
CVE-2017-10685	medium	ncurses	5.9+20140118-1ubuntu1	
CVE-2016-7543	medium	bash	4.3-7ubuntu1.5	4.3-7ubuntu1.7

Harbor – Use Cases

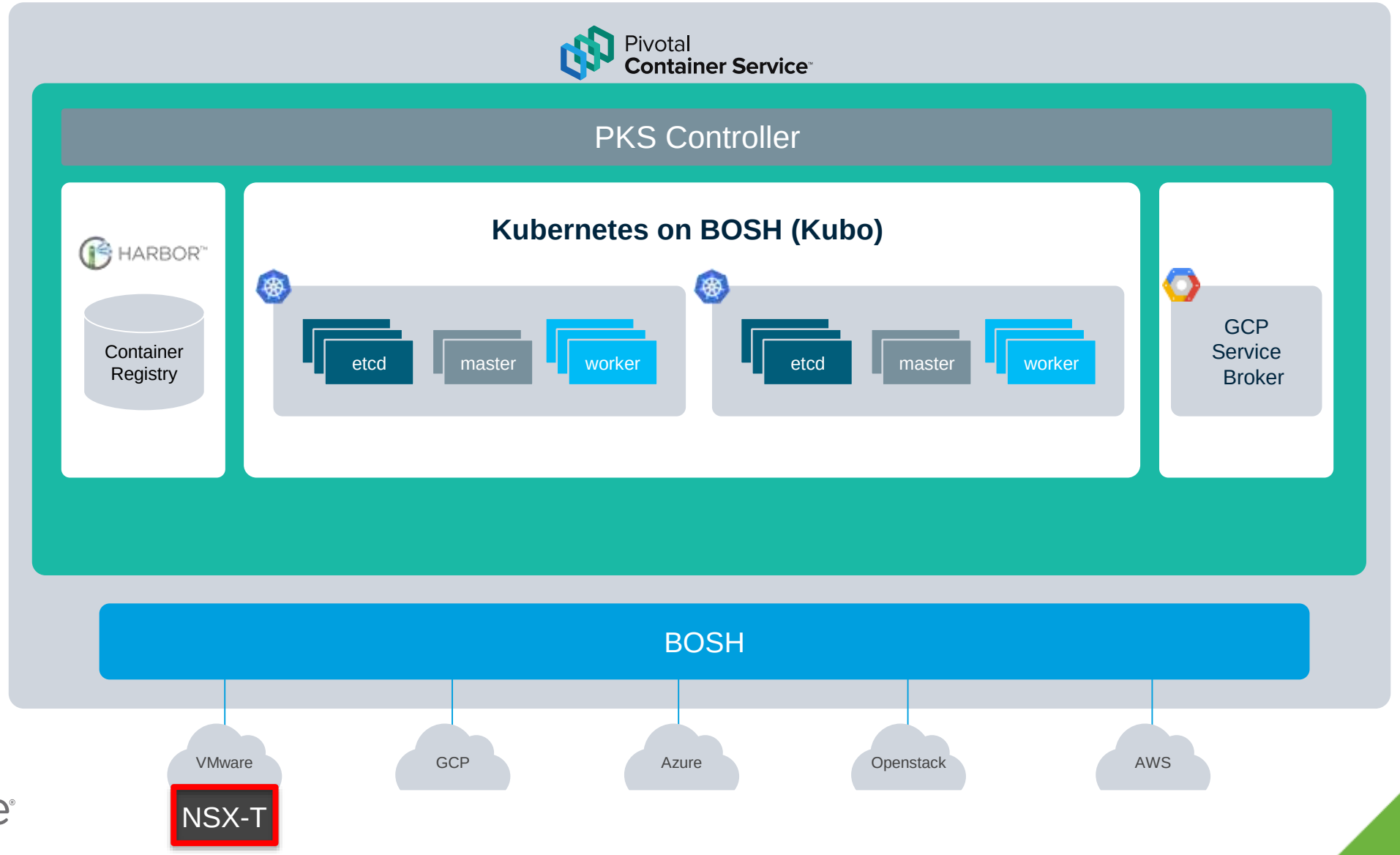


CVE & Update Patching

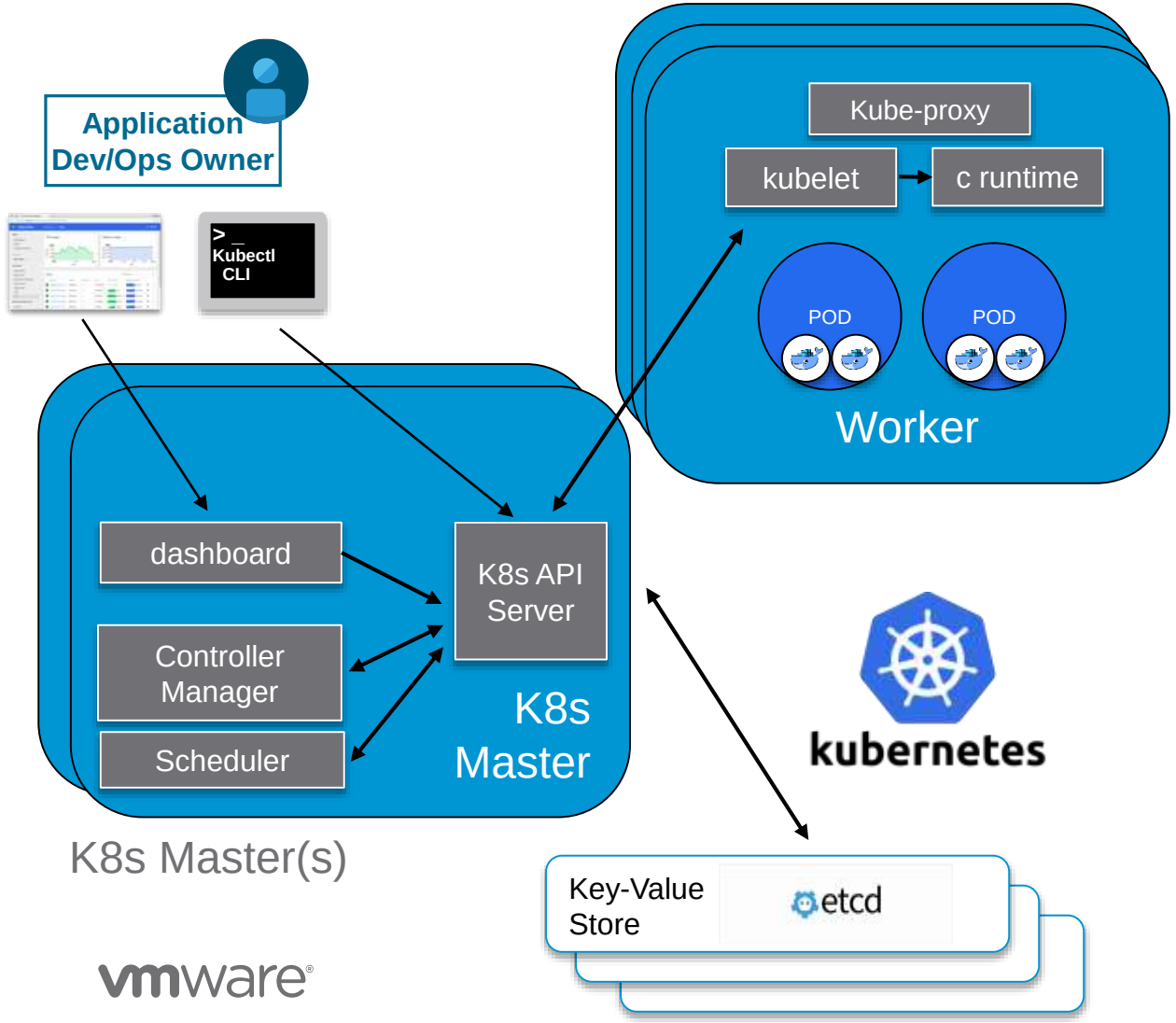
- Patch OS Level via Stemcells
- Harbor Scans Images for Vulnerability (Clair)
- Address CVE in minutes/hours versus days/weeks



PKS Technical Overview



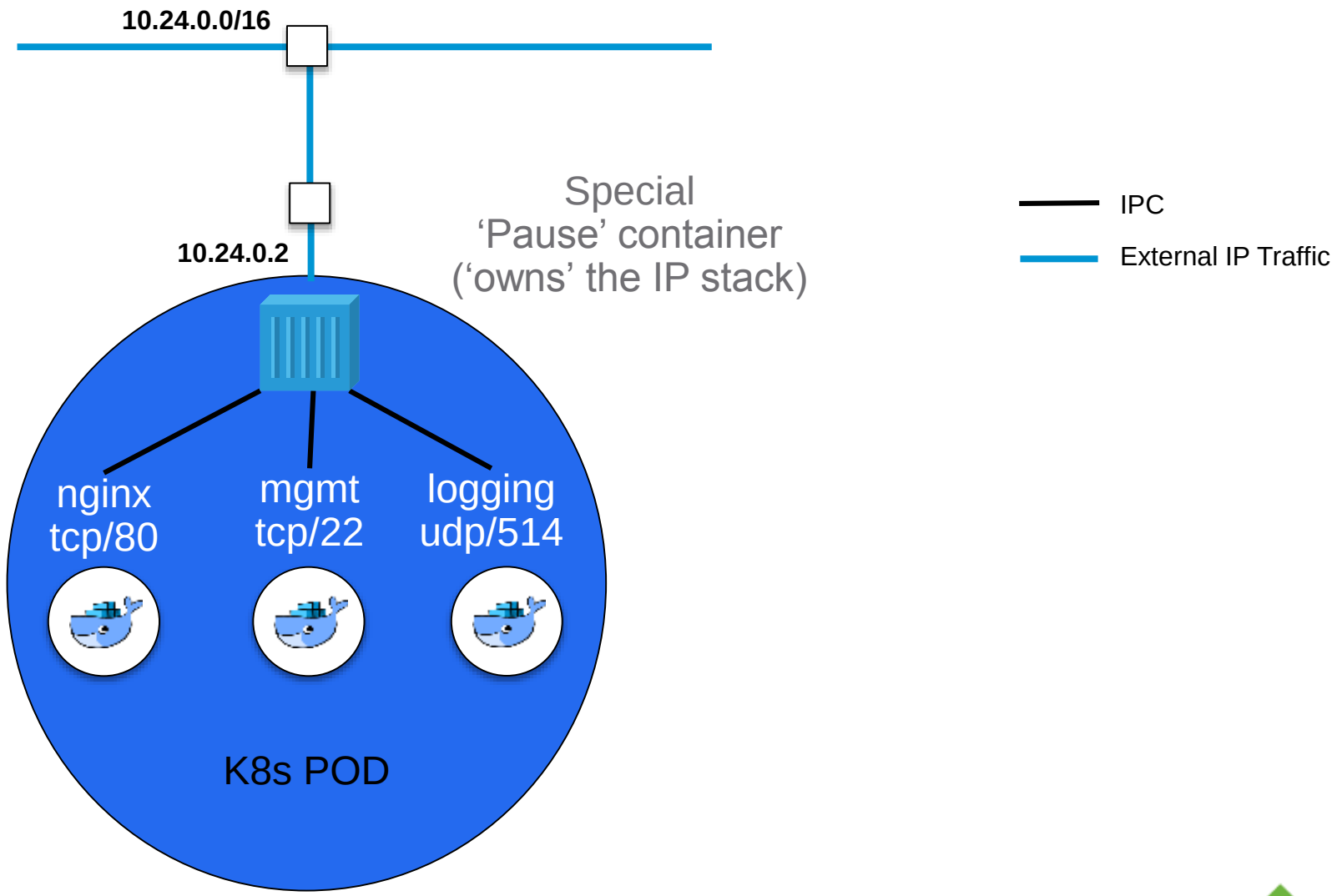
Kubernetes Components



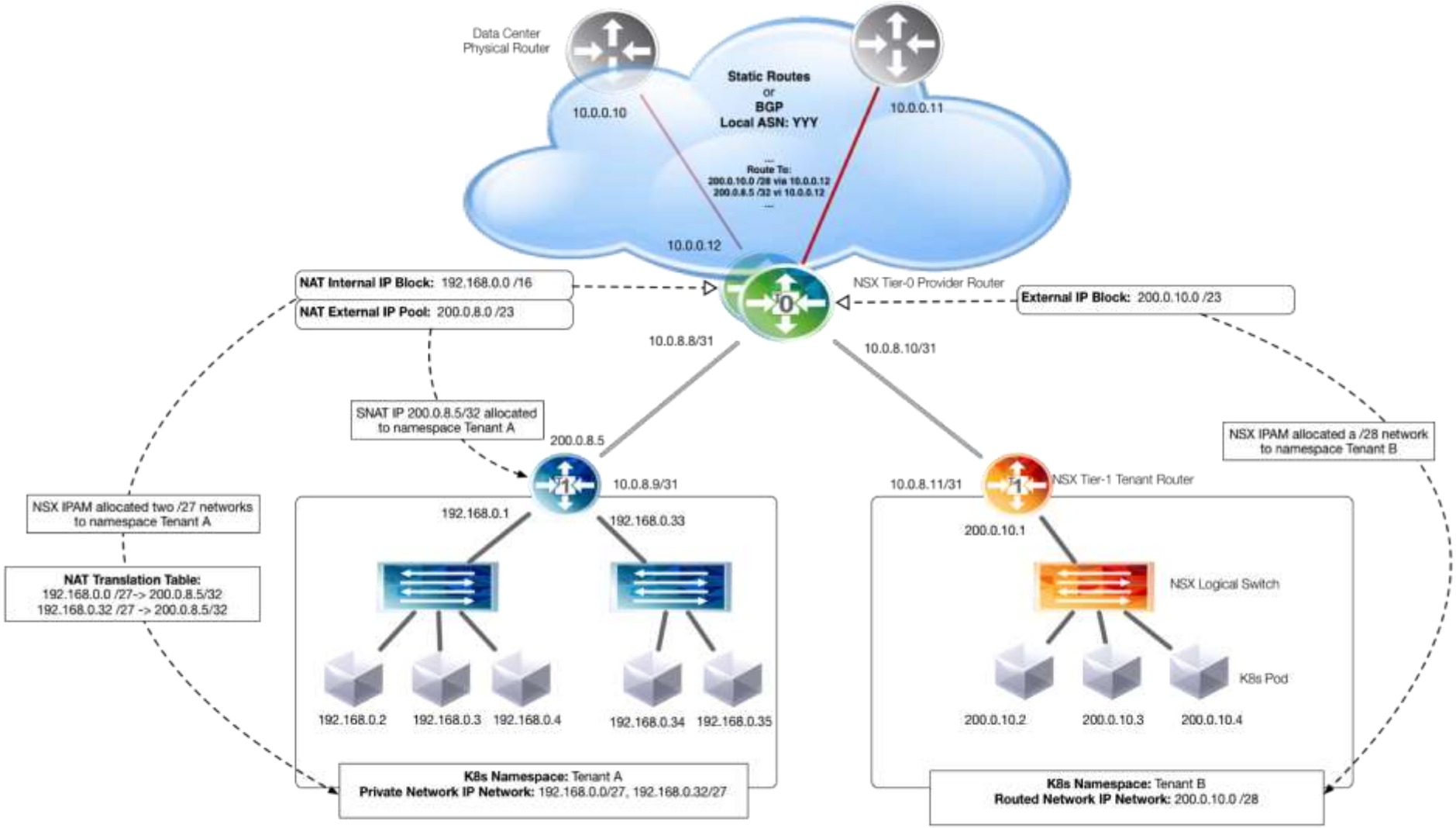
- K8s Cluster Consists of Master(s) and Nodes
- **K8s Master Components**
  - API Server
  - Scheduler
  - Controller Manager
  - Dashboard
- **K8s Node Components**
  - Kubelet
  - Kube-Proxy
  - Containers Runtime (Docker for PKS 1.0)

Kubernetes Pod – Networking Basics

- A Pod is a group of one or more co-located containers that share an IP address, PID namespace and/or Data Volumes

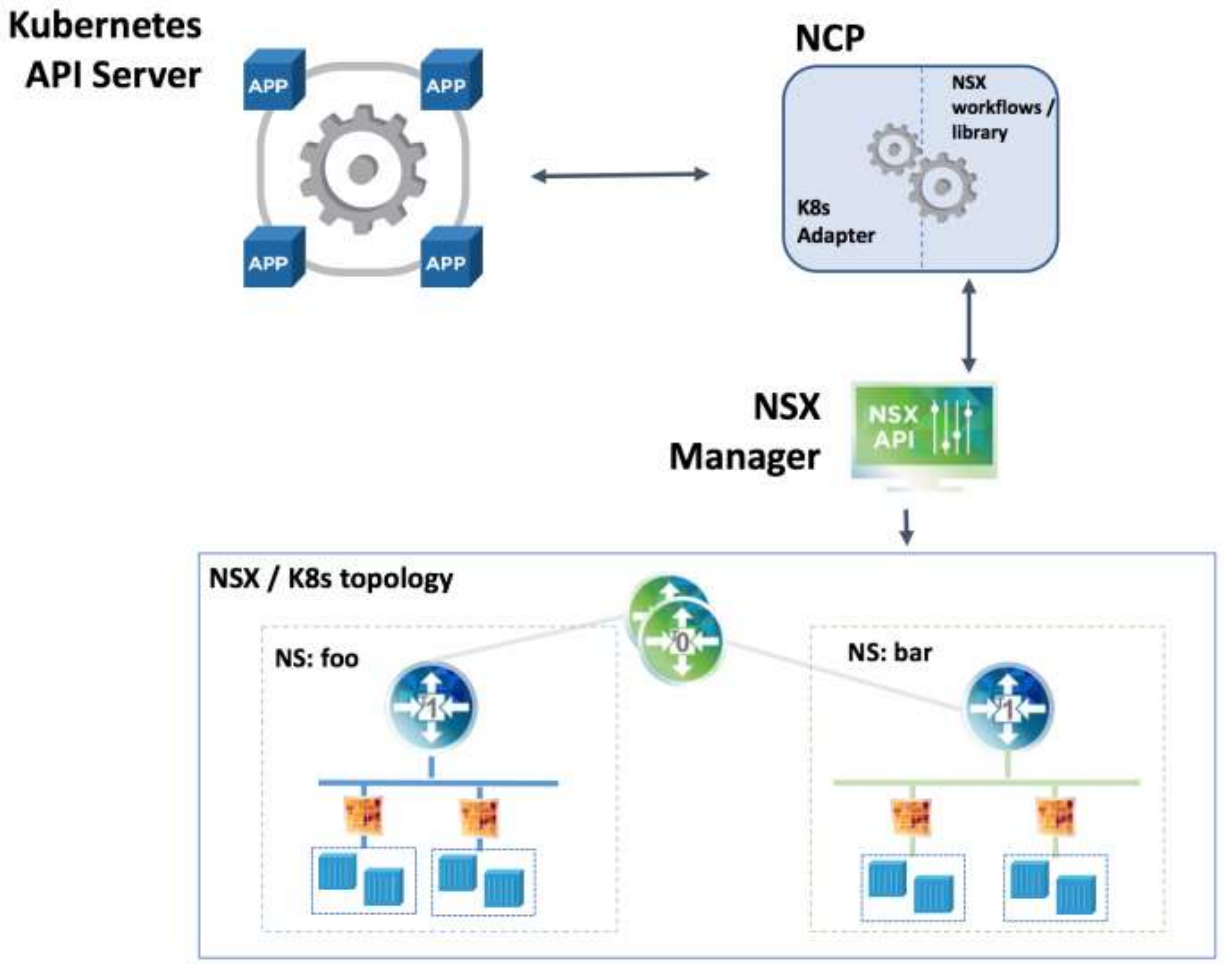


NSX-T & PKS Sample Topology



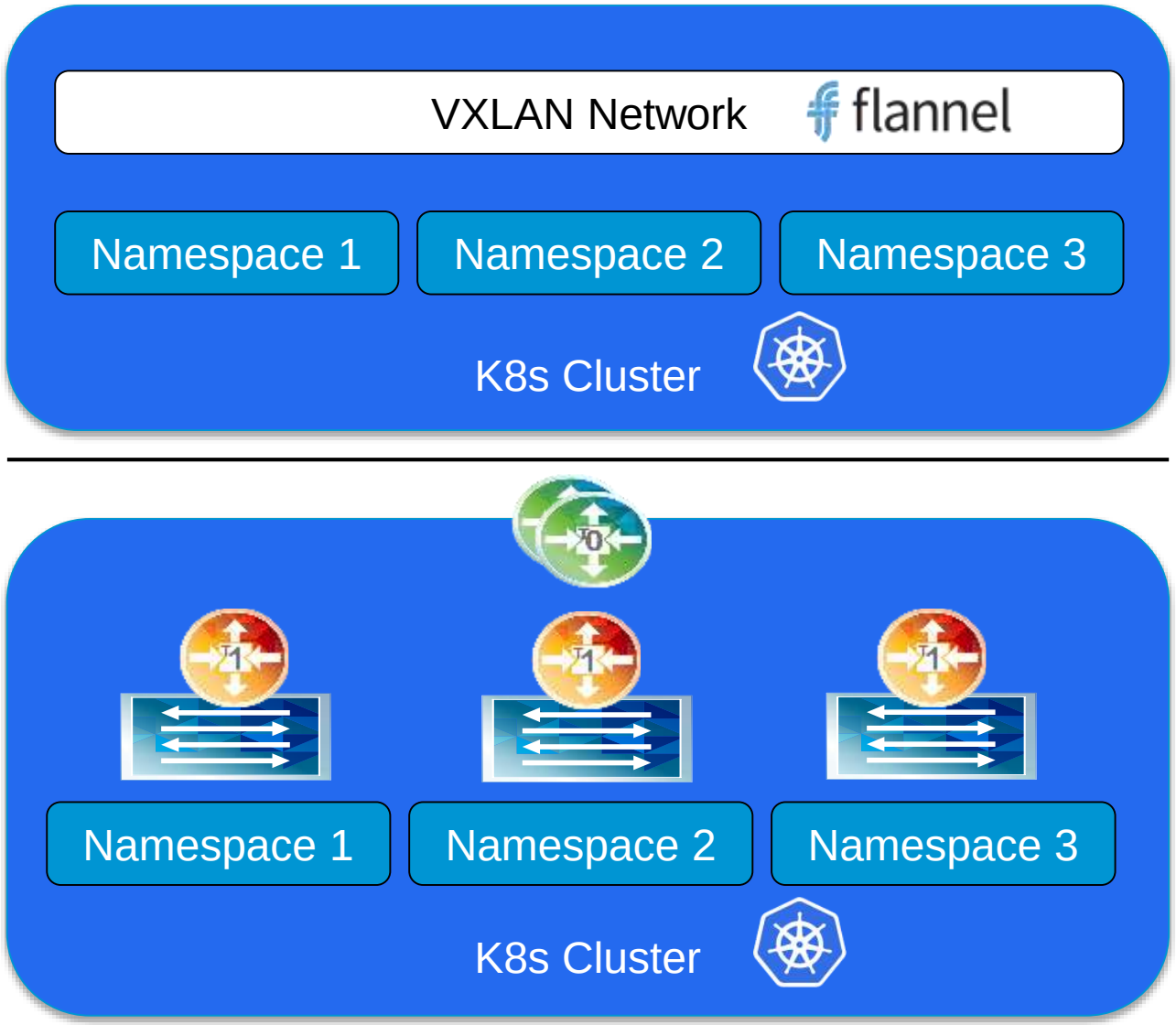
NSX-T & PKS Components

NSX Container Plugin (NCP)



- NCP is a software component provided by VMware in form of a container image, e.g. to be run as a K8s Pod.
- NCP is build in a modular way, so that individual adapters can be added for different CaaS and PaaS systems

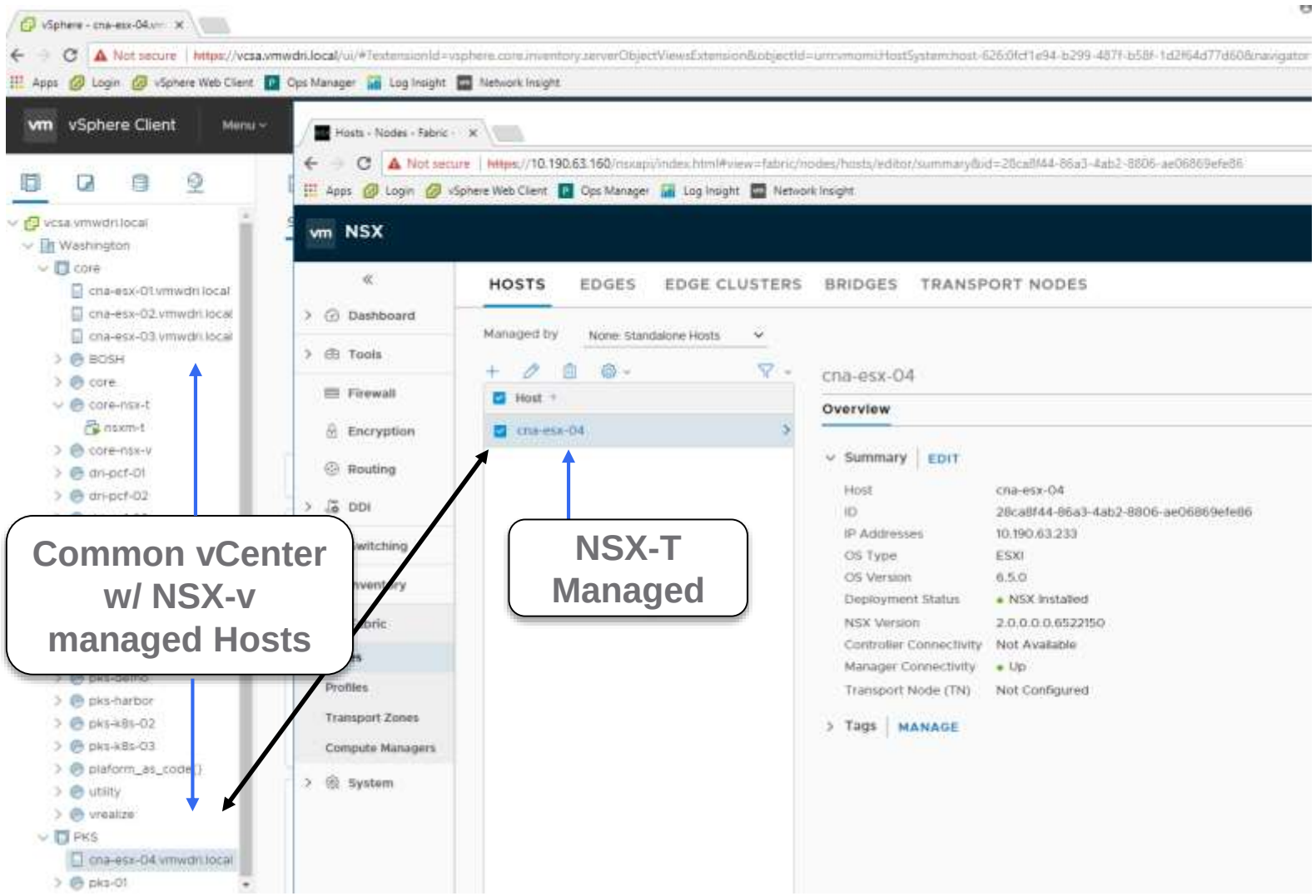
PKS & NSX-V



- PKS supported with NSX-V or without NSX
  - Flannel overlay.
    - 1 Flat SDN Overlay per Cluster
      - 1 Large CIDR “10.200.0.0/16”
      - Each worker node routes a subnet for Pods across
        - Example: 10.200.1.0/24
    - No integrated North South Load Balancing
    - No Integrated Security Policy

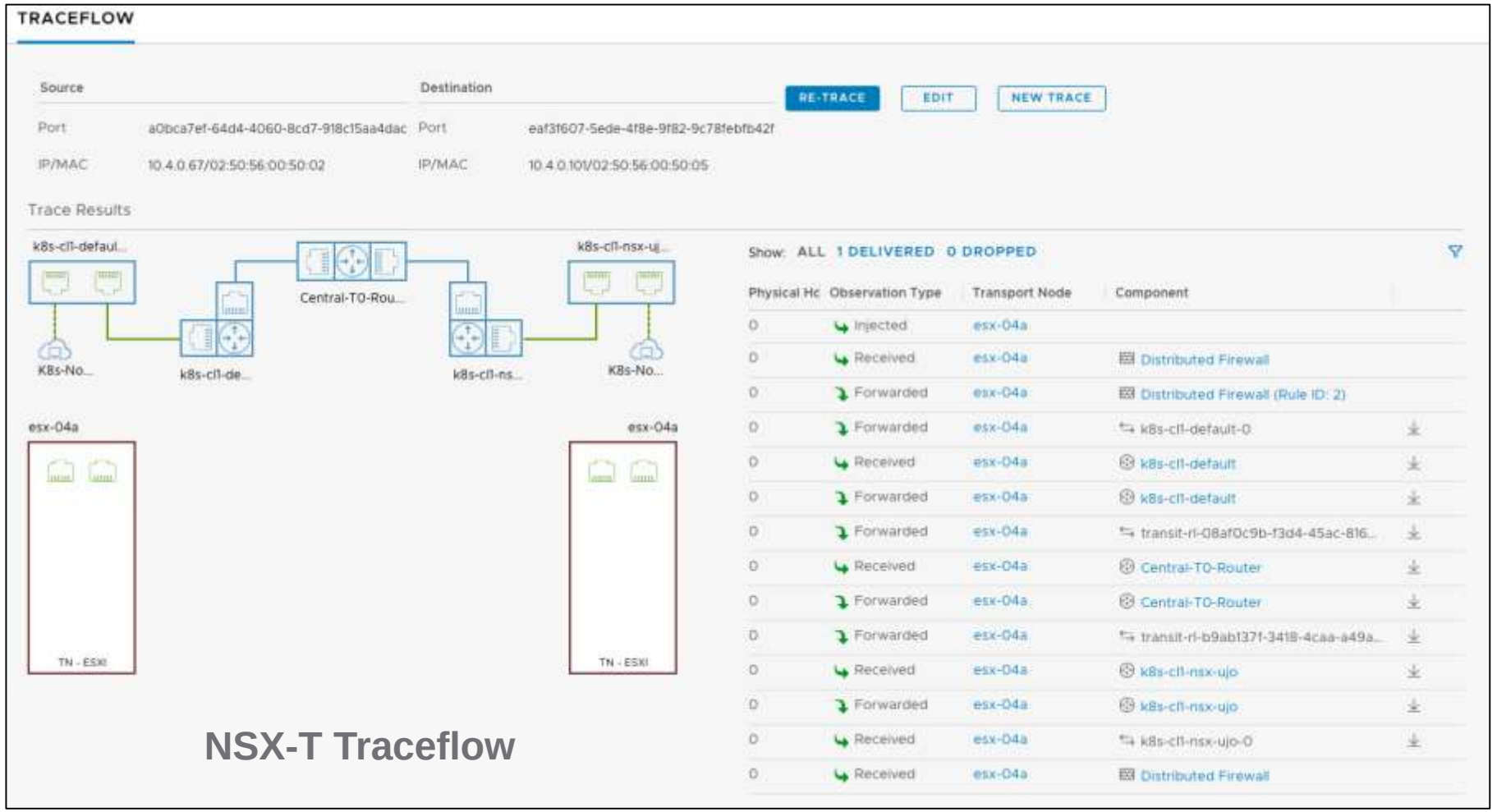
- NSX-T
  - Multiple Logical Switches (L2 Domain) per Namespace
  - Routable as NAT or No-NAT
  - Integrated Load Balancing (NSX-T 2.1)
  - Integrated Security Policy

PKS w/ NSX-T & NSX-V



- NSX-V and NSX-T Can coexist.
  - Dedicated Clusters for NSX-T Managed Hosts
  - Can Share a common vCenter backplane

NSX-T & PKS Operational Tools

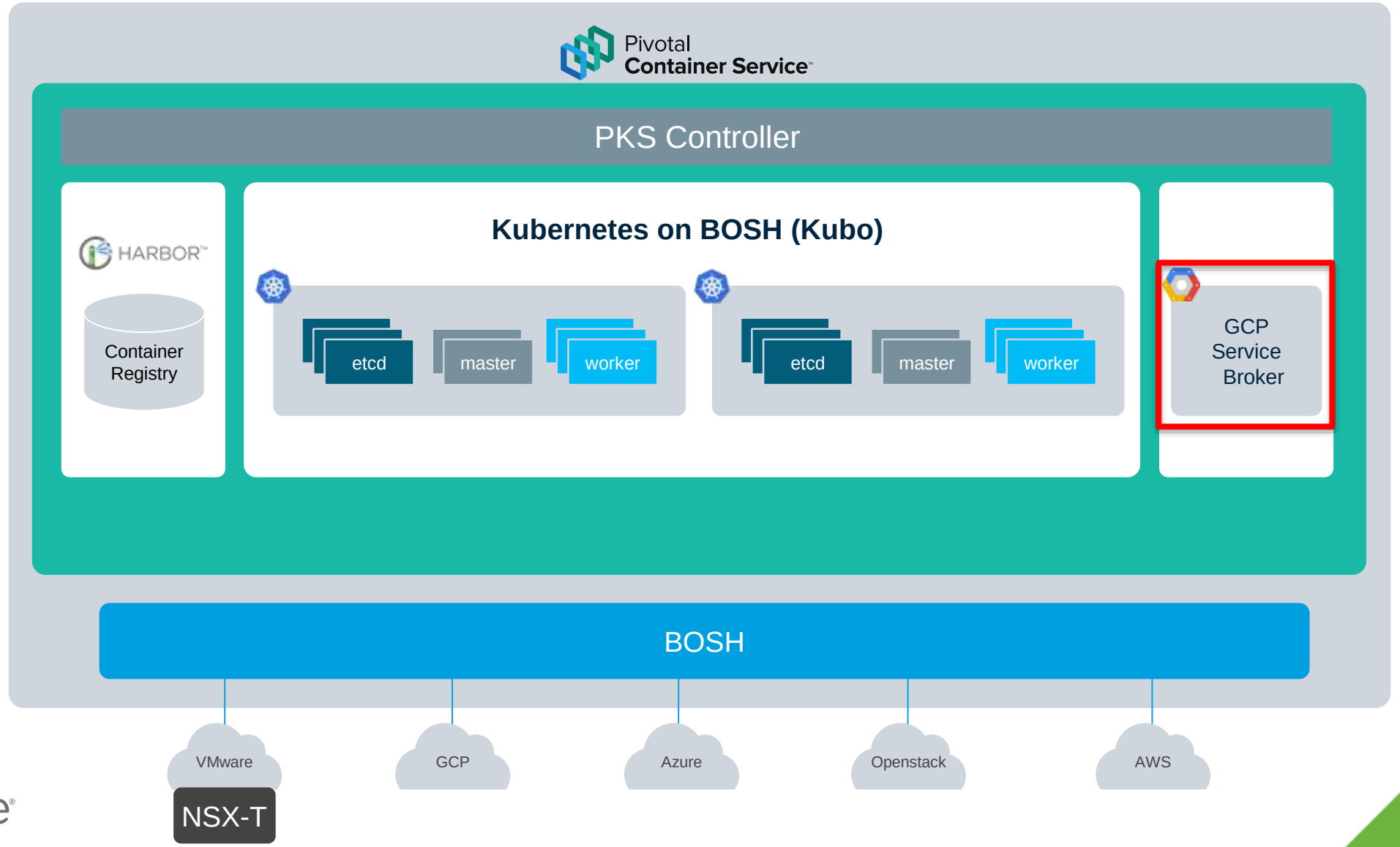


NSX-T Traceflow

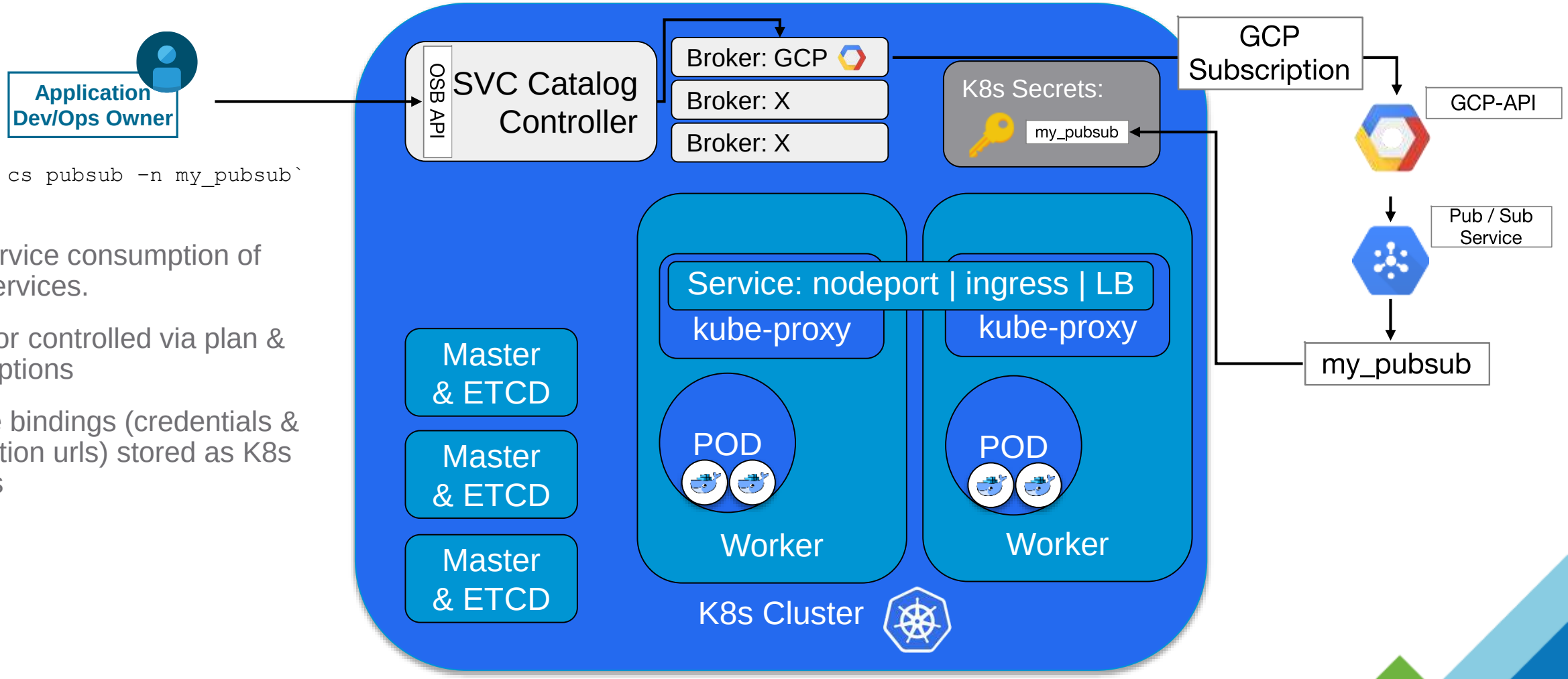
NSX-T Operational Tools

- Traceflow
- Port Mirroring
- Port Connection Tool
- Spoofguard
- Syslog
- Port Counters
- IPFIX

PKS Technical Overview



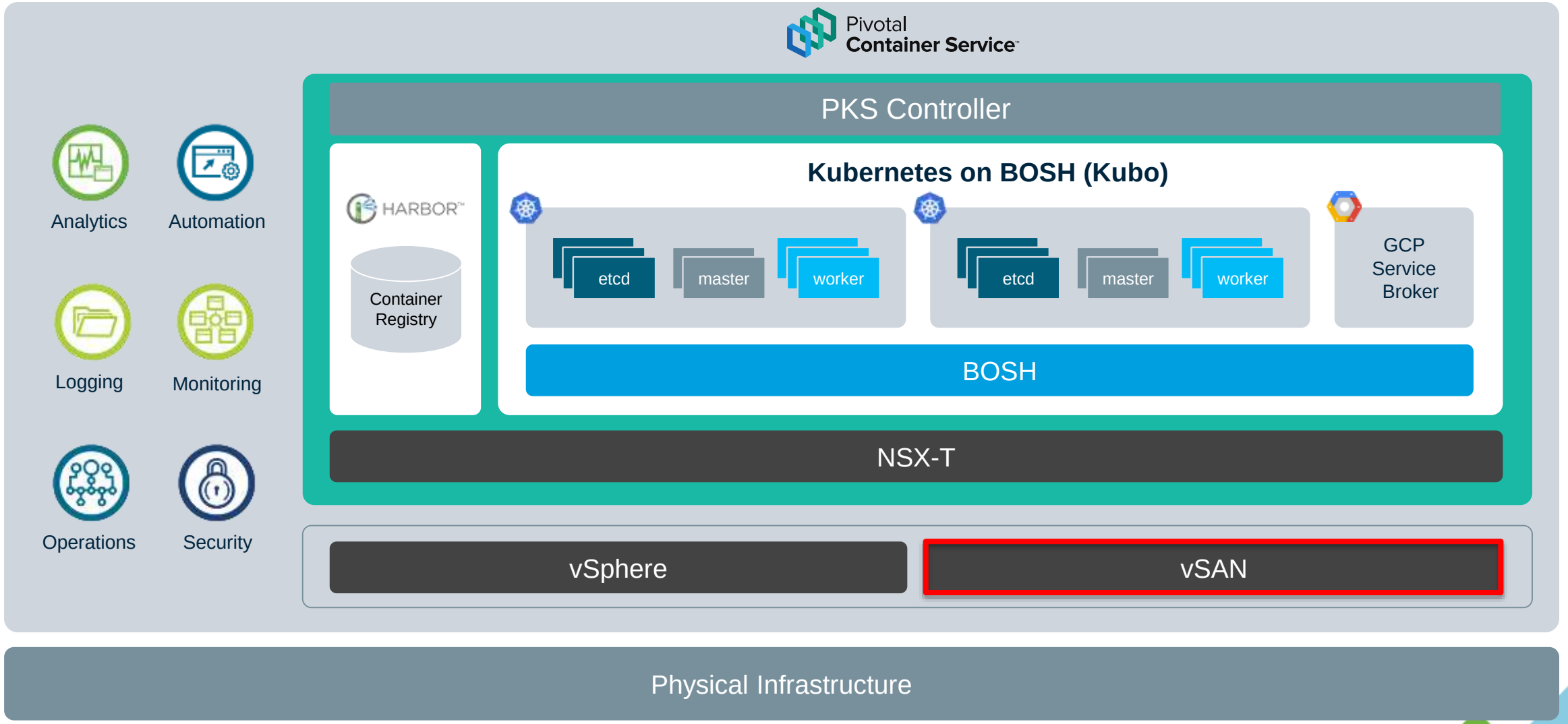
GCP Service Broker



- Self Service consumption of GCP services.
- Operator controlled via plan & subscriptions
- Service bindings (credentials & connection urls) stored as K8s Secrets

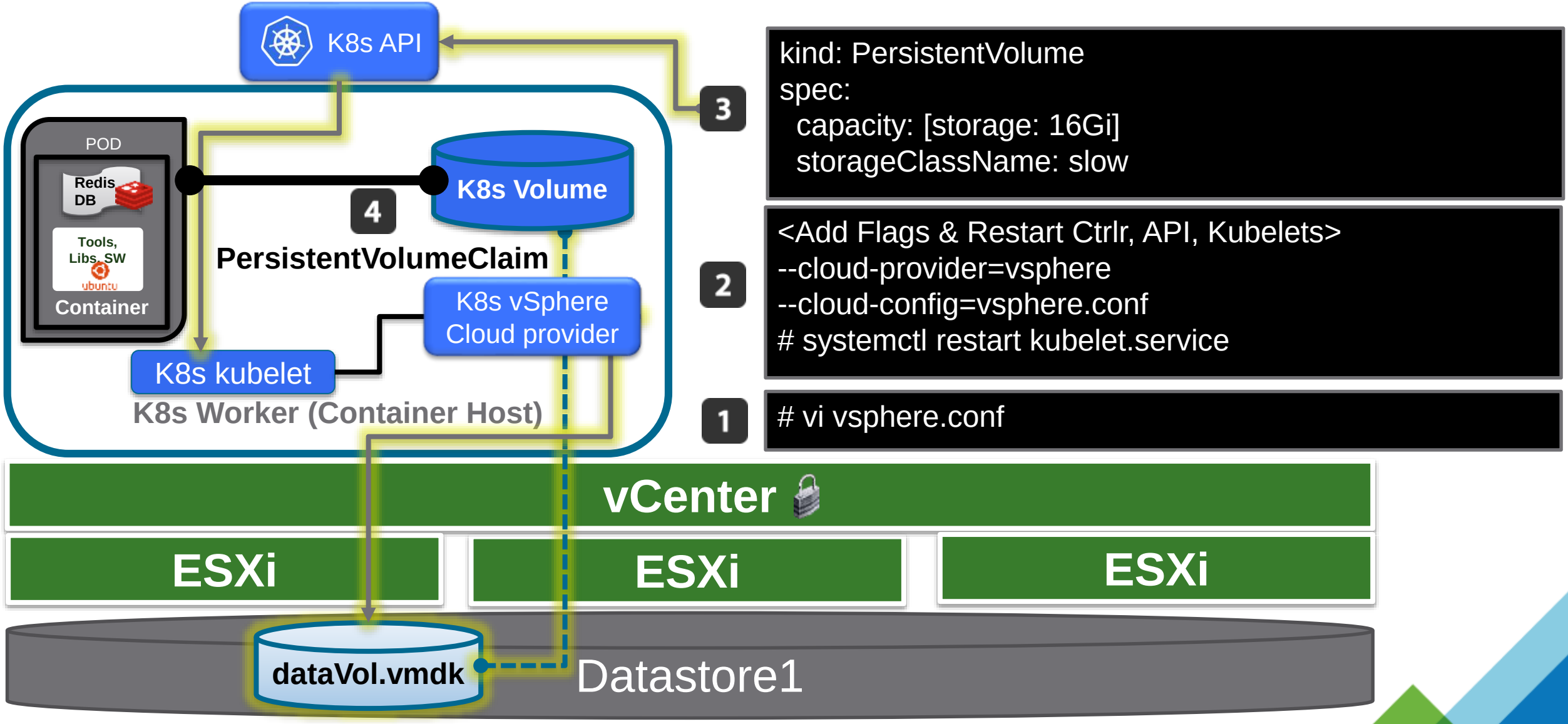
vmware

PKS Technical Overview w/ VMware Integrations

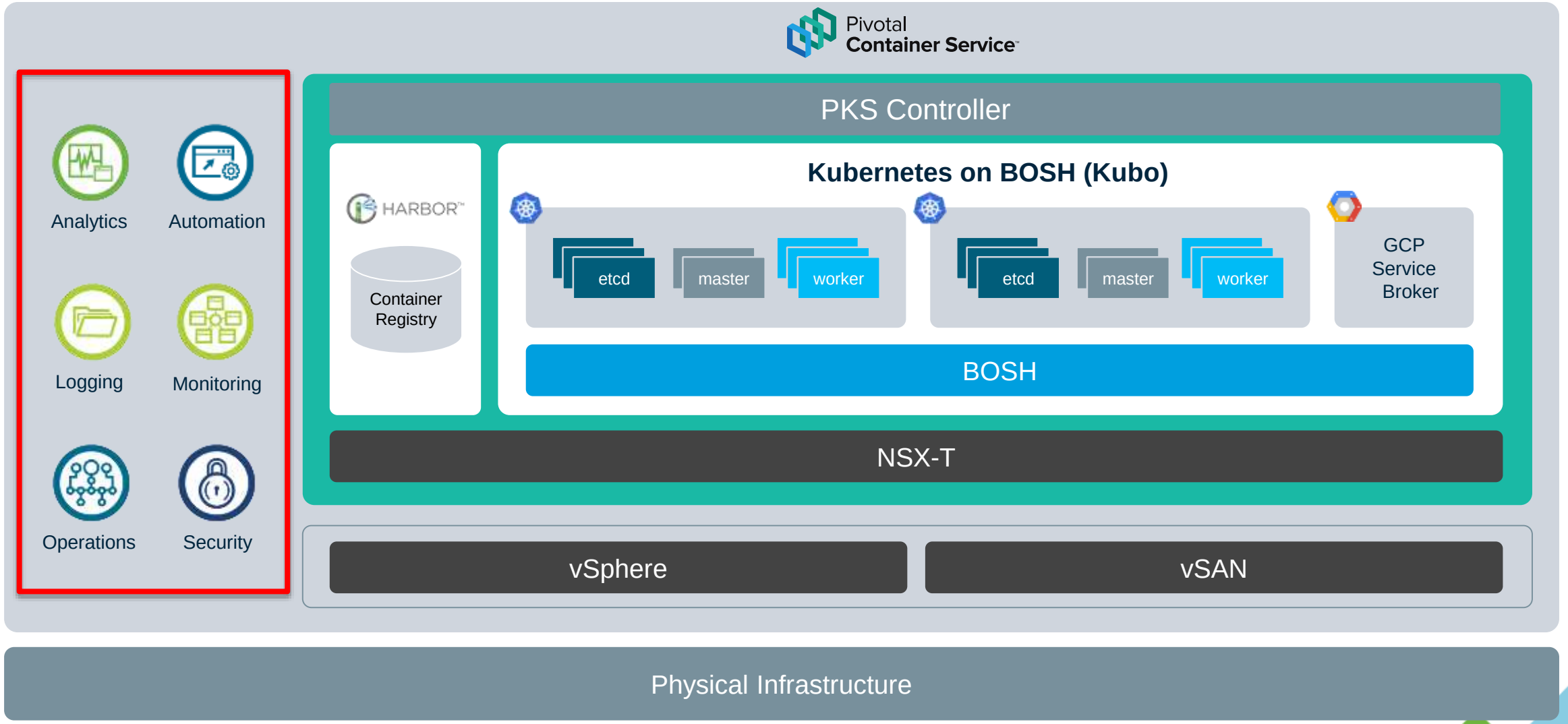


Project Hatchway : https://github.com/vmware/vsphere-storage-for-kubernetes

vSphere Storage for Kubernetes

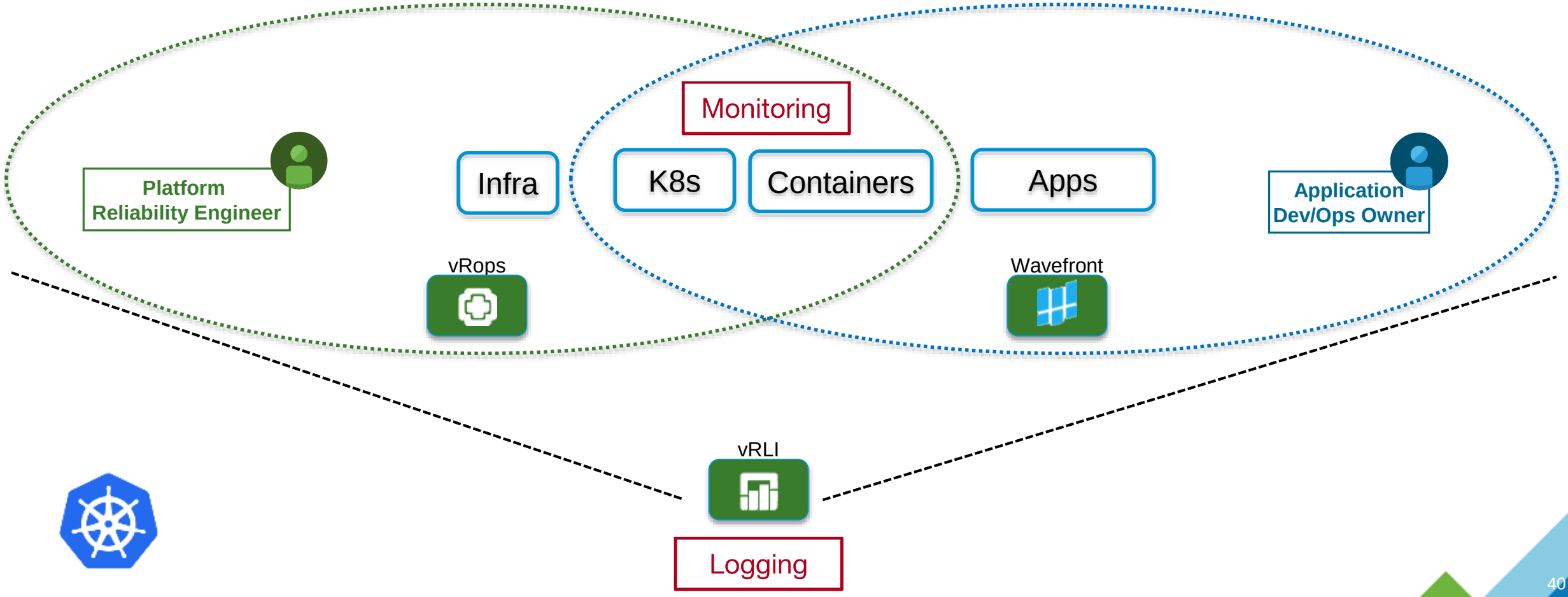


PKS Technical Overview w/ VMware Integrations



PKS Telemetry – On vSphere

Who needs what?

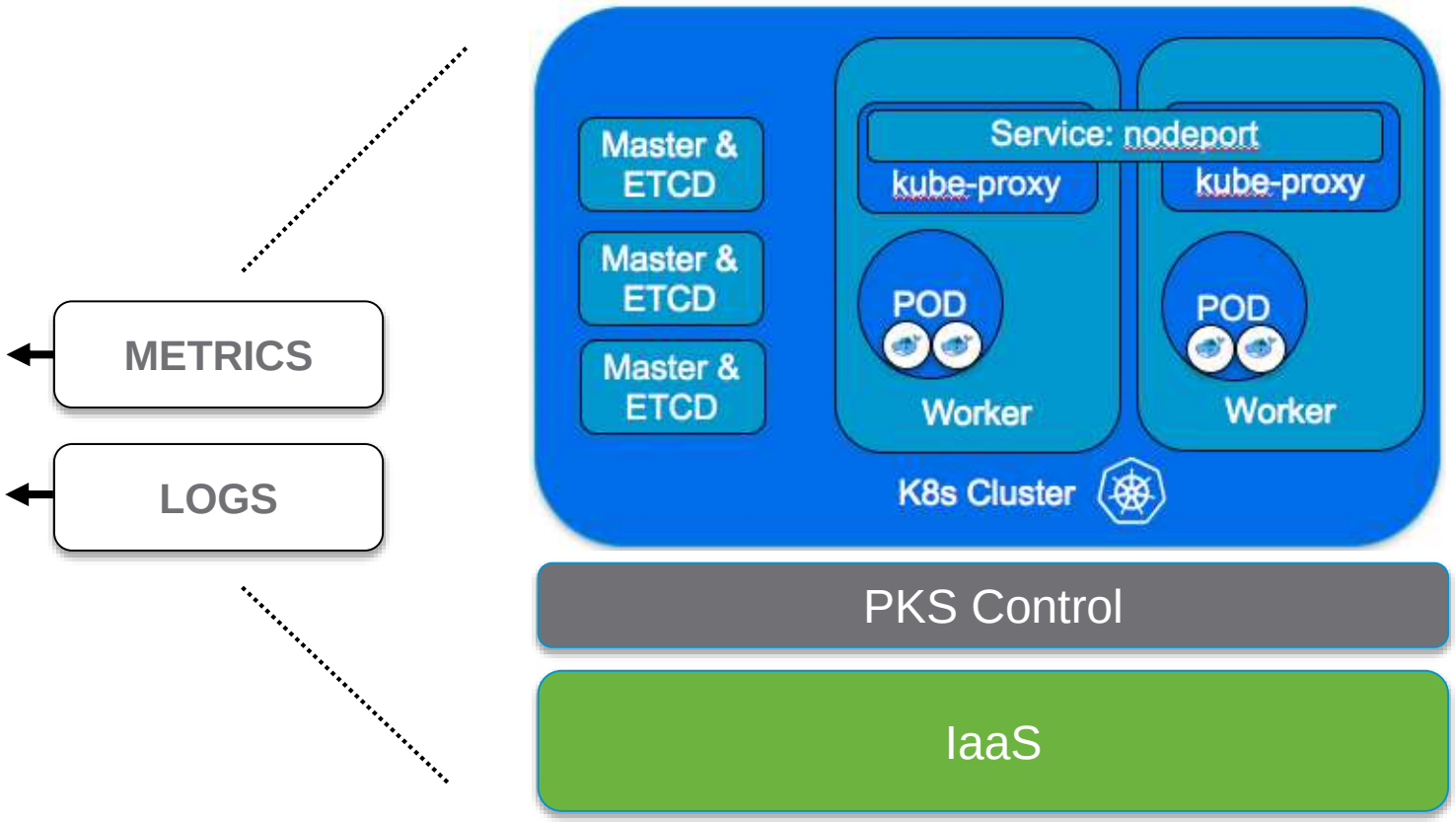


Monitoring & Logging

Metrics & Logs emit from many Sources:

- IaaS (vSphere)
- PKS K8s Platform
- Applications
- NSX
- Physical & Logical

Platform Reliability Engineer **MUST** leverage **ALL** of them



vRLI Logging w/ PKS

Application Dev/Ops Owner

&

Platform Reliability Engineer

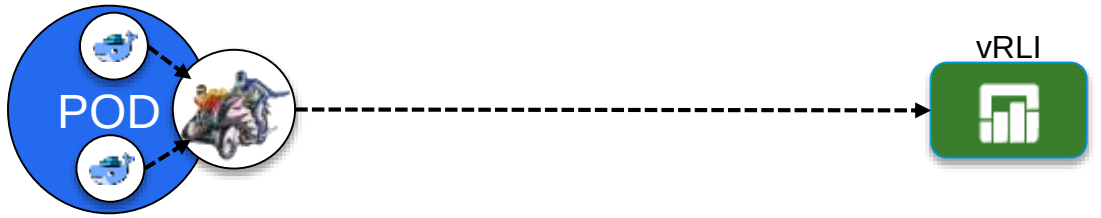
- App Logging
- System Logging
  - OS & Processes not run in Containers

App Logging

- Per App Only

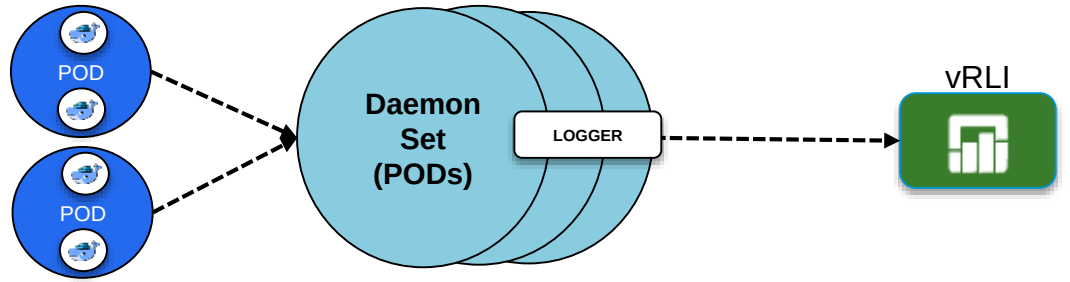
Sidecar

- App Logging @ Pod level



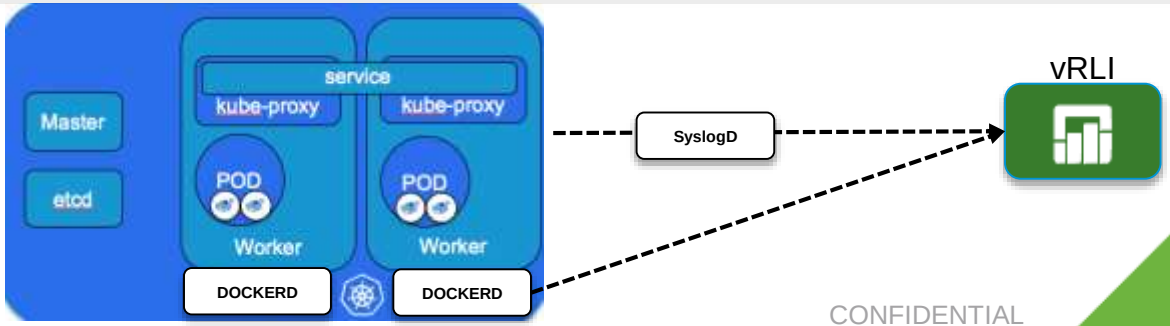
DaemonSet

- App Logging @ Cluster level
- Cluster Logging



Dockerd

- App Logging @ Cluster level
- Cluster Logging
- Not handled in K8s API ☹



Wavefront & PKS

K8s Monitoring Integration w/ Wavefront by VMware

Wavefront Integration can be deployed as containers within the K8s Cluster

- Proxy
- Heapster

- Comprehensive Dashboards
  - SaaS
- APM for the Developer
- Cluster KPIs for the Operator
- **Integrated with PKS**

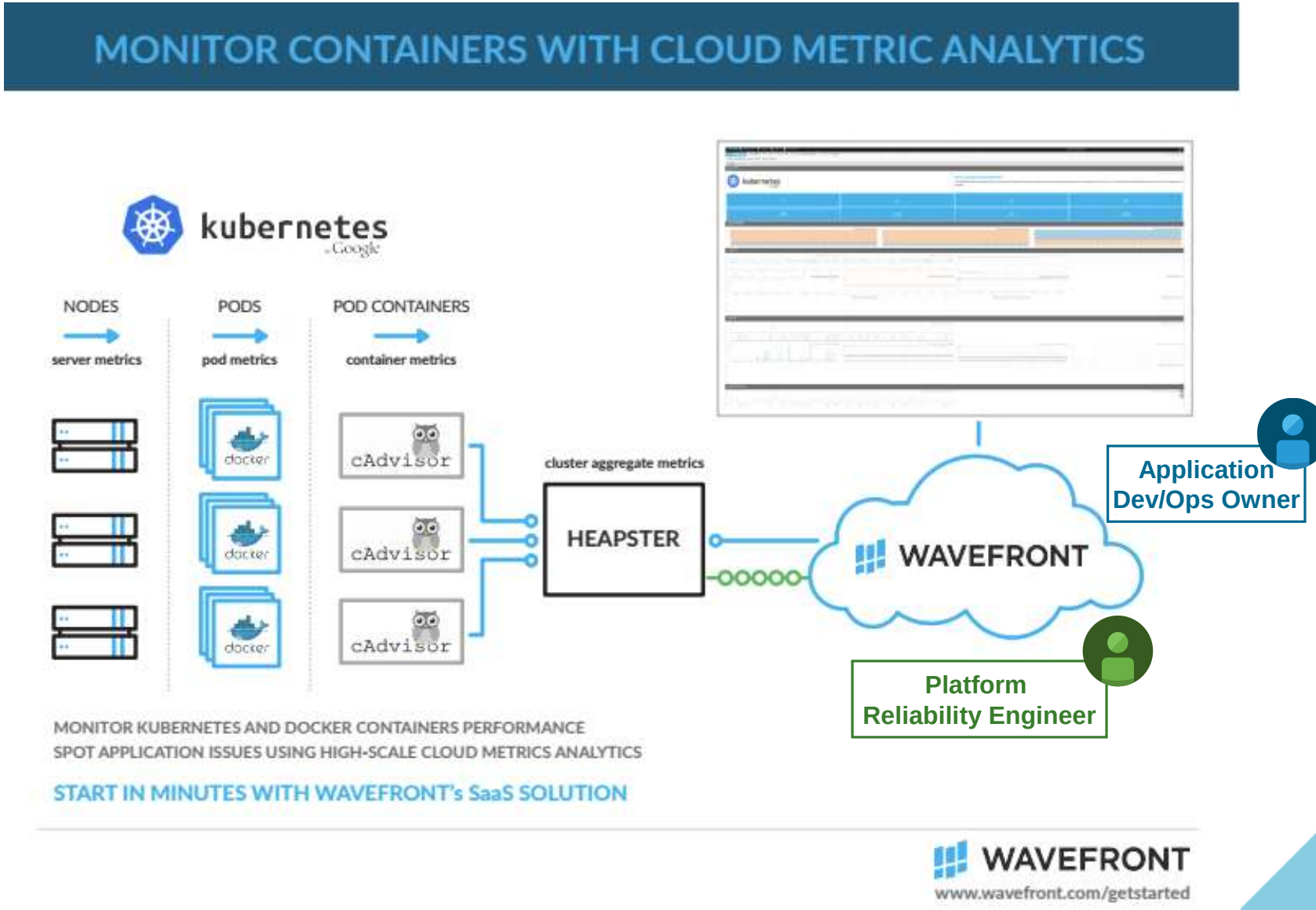
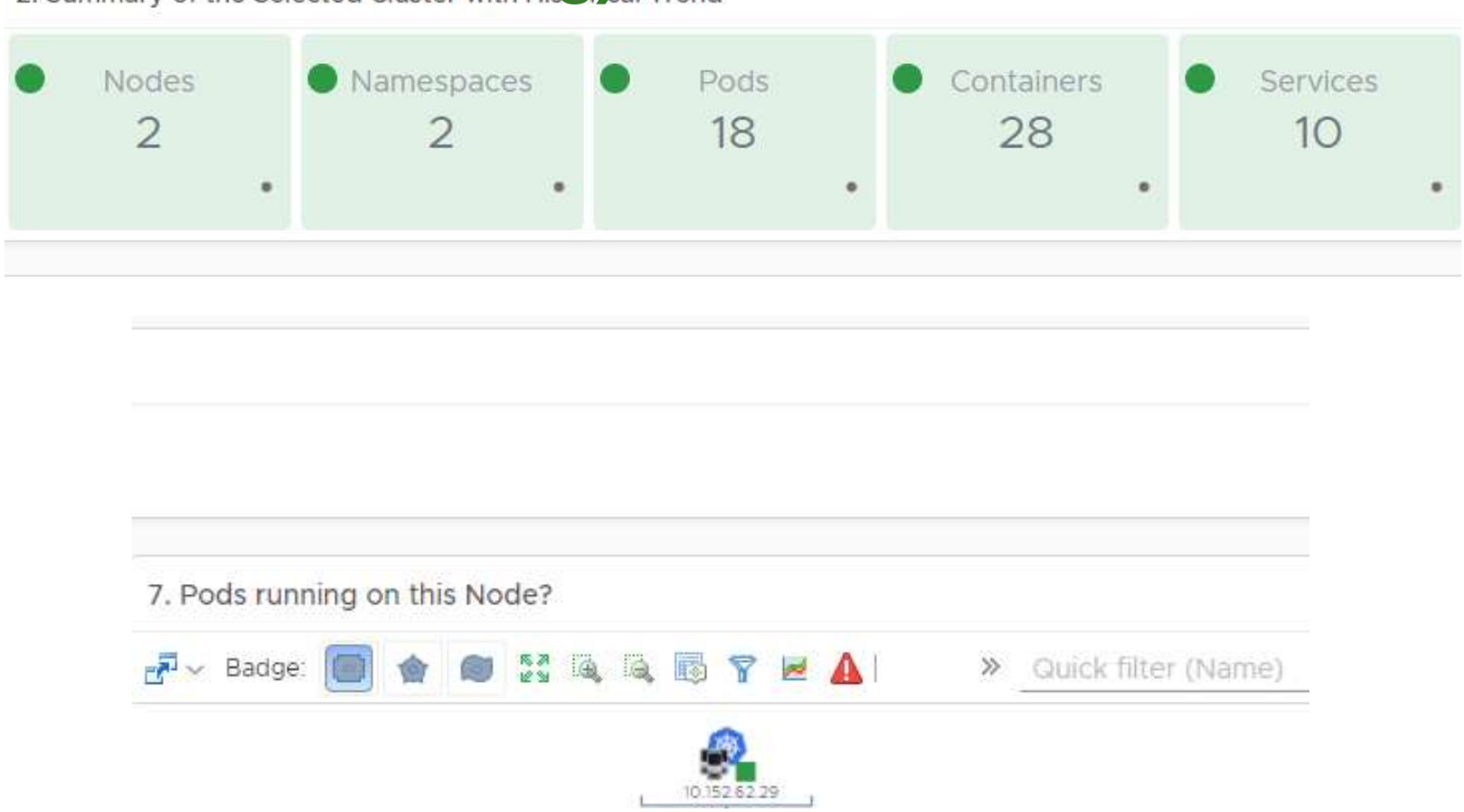


Image source: https://www.wavefront.com/surf-container-wave-join-wavefront-container-world-santa-clara/

vRops & PKS (Operations & Monitoring)

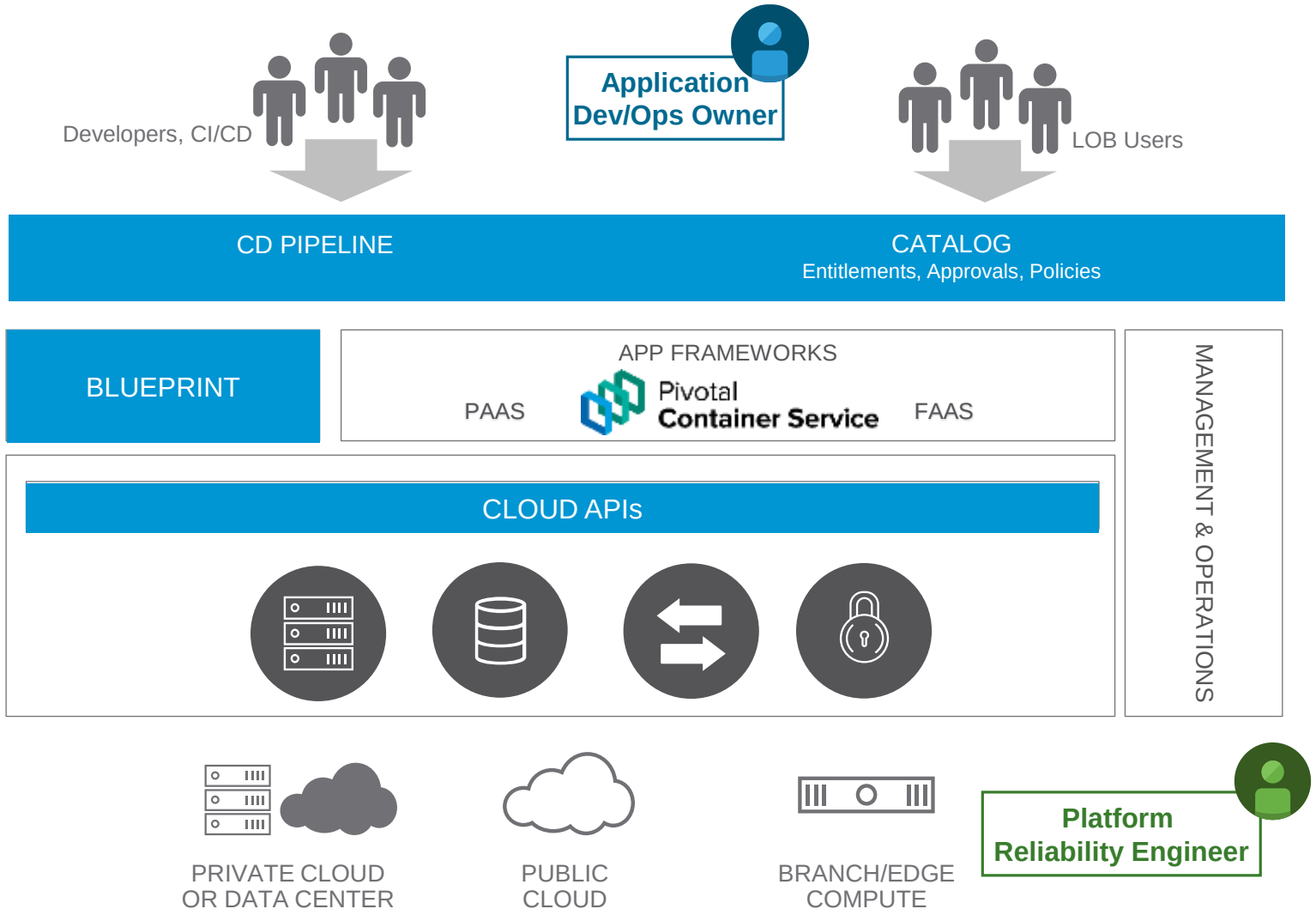
vRealize Operations & K8s

- Operator KPIs
- Single Pane for SDDC & K8s clusters monitoring
- vRLI Integrated
- Alert on K8s KPIs
- Entity Relationship
- Capacity Planning
- **Integrated with PKS**



Platform Reliability Engineer

vRA & PKS (Automation)



1

CLOUD APIs

Consume native K8s services from PKS

2

BLUEPRINTS & ITERATIVE DEVELOPMENT

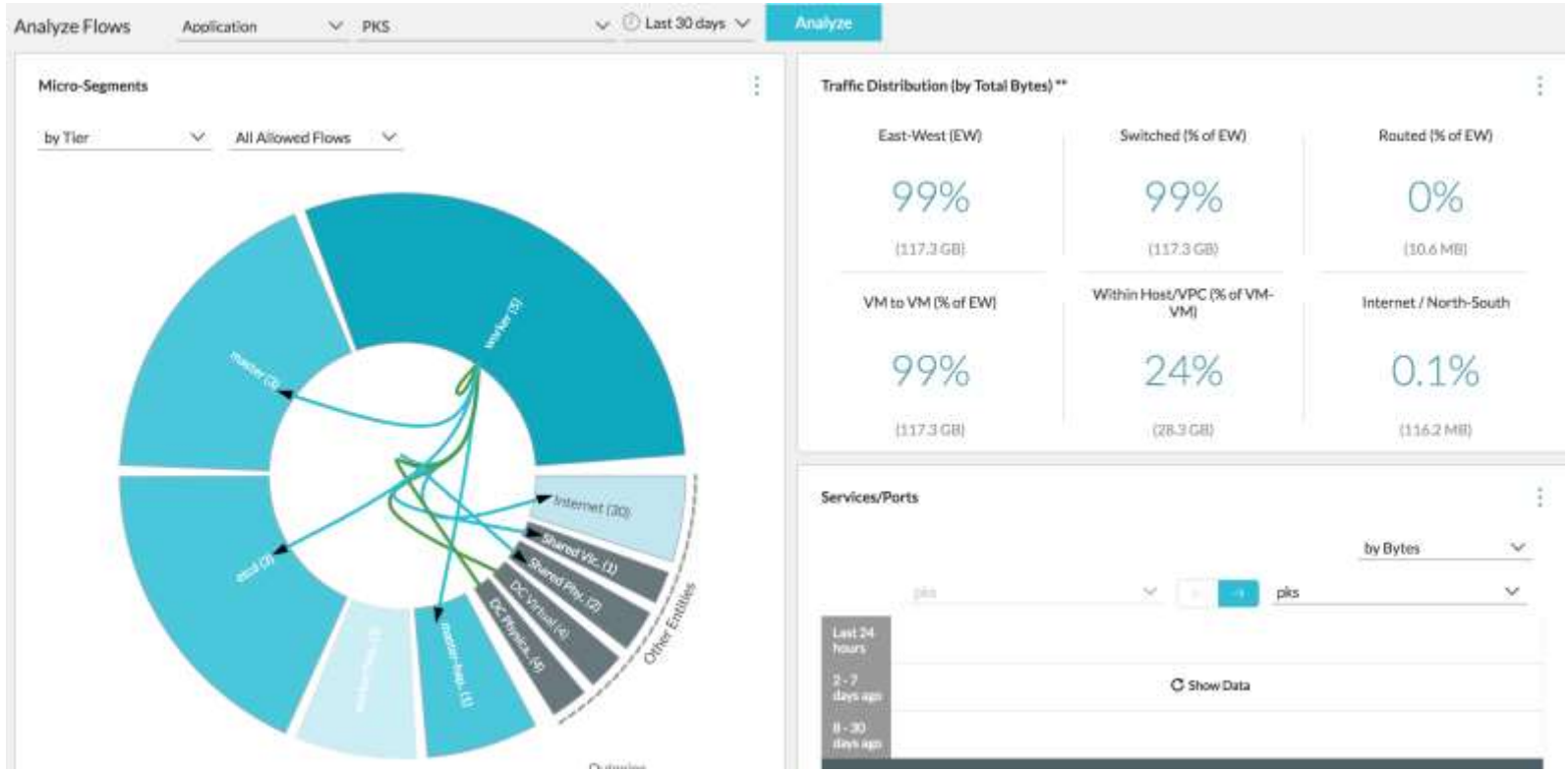
Compose applications using simplified YAML iteratively & Deploy to K8s

3

INTEGRATED CATALOG AND PIPELINE

Catalog for self-service provisioning of PKS K8s & applications pipelines for CI/CD

vRNI & PKS (Security & Analytics) – Post 1.1



vRealize Network Insight & K8s

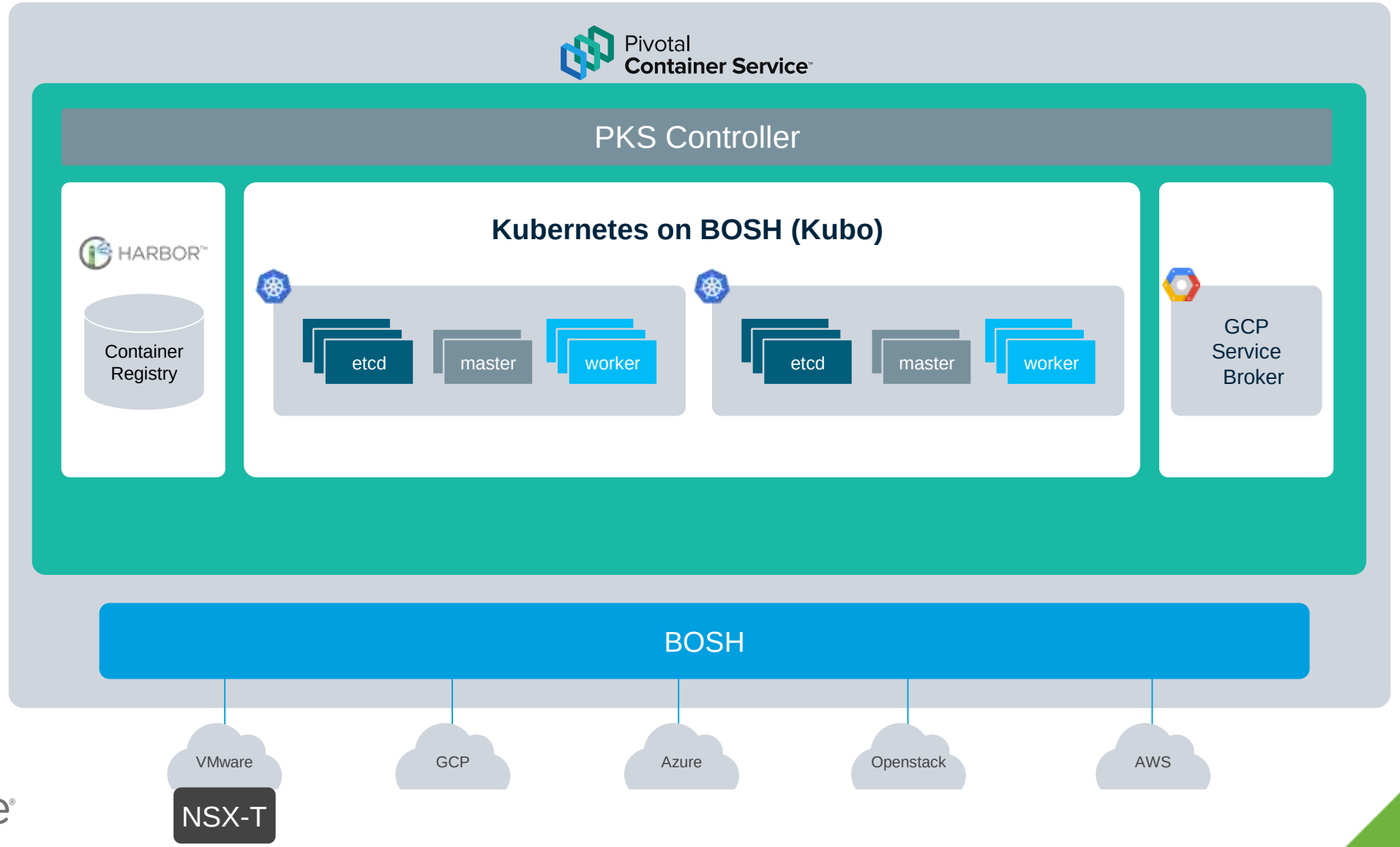
- Plan Security Policy based on knowledge of actual traffic patterns
- Continuously monitor & audit network security compliance
- Complete Network Visibility and Troubleshooting
- Accelerate micro-segmentation deployment

Platform Reliability Engineer

Agenda

1	Containers, CaaS, & PaaS 101
2	Why PKS
3	PKS Technical Overview
4	**Packaging & Support**

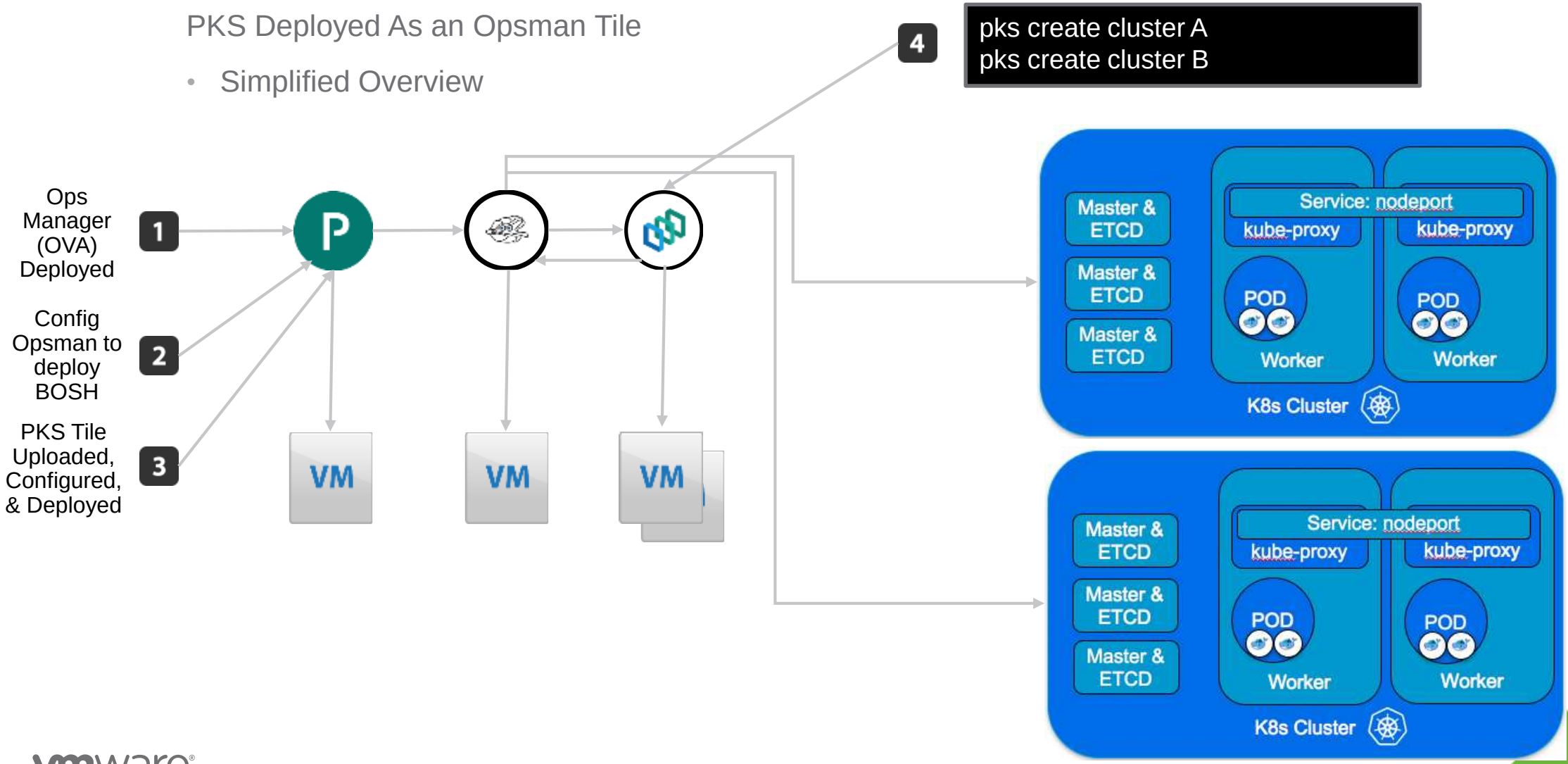
PKS Technical Overview



Packaging

PKS Deployed As an Opsman Tile

- Simplified Overview



vmware

Go To Market and Support

Available through VMware, Pivotal, and Dell EMC

Global Support Services

Product GA ~ Late Dec 2017

vmware®

Thank You!

VMware Pivotal Container Services (PKS)

@cloudnativeapps
#vmwcna
#vmwpks

vmware.github.io
blogs.vmware.com/cloudnative