Project Pacific
Technical Overview: Unifying vSphere and Kubernetes

Kit Colbert, VMware
Karim Awan, VMware
Disclaimer

This presentation may contain product features or functionality that are currently under development.

This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.

Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.

Technical feasibility and market demand will affect final delivery.

Pricing and packaging for any new features/functionality/technology discussed or presented, have not been determined.

This information is confidential.
Modern Application Deployments are Accelerating
A Modern Application Is Complex…
...Which Introduces Many Challenges...

- How do I deploy this app?
- How do I operate it on day 2?
- What tools can I use with it?
- How do I ensure the availability of this app?
- How do I ensure it’s security?
- How do I deliver quality of service?
- How do I control cost of our infrastructure?
VMware as the Platform That Connects Developers and Operations

Power the developer, Assure the admin

- Performance
- Security
- Availability
- Cost
- Diagnostics

Operations

Developers

Collaboration

Manage

Deploy

vSphere

Workloads

Code

Test

Deploy

Support

#vFORUMAU
Using Kubernetes to Manage Workloads!

**Kubernetes Cluster**
- kind: KubernetesCluster
- apiVersion: vks.vmware.com/v1
- metadata:
  - name: My Application
- spec:
  - topology:
    - workers:
      - count: 3
        class: small
distribution: v1.14.1

**My Application**

**Serverless**
- kind: Pod
- apiVersion: v1
- metadata:
  - name: Function 1
- spec:
  - containers:
    - name: func1
      image: func1
      ports:
        - containerPort: 80

**Legacy App**
- kind: VirtualMachine
- apiVersion: vms.vmware.com/v1
- metadata:
  - name: LegacyApp
- spec:
  - className: large
  - imageName: my-app.ova
  - powerState: poweredOn
  - policy:
    - restartPolicy: OnFailure

**Database**
- kind: HanaDatabase
- apiVersion: hana.sap.com/v1
- metadata:
  - name: ERP database
- spec:
  - nodes: 3
  - class: extra-large
Namespaces as the Unit of Management

My Application

Control Plane

Node

Node

Node

Legacy App

VM

VM

VM

Serverless

Function 1

Function 2

Database

VM

VM

VM

Quality of Service
- Priority: High
- Reserved vCPUs: 128
- Reserved Memory: 1 TB

Security
- Encrypt all persistent data
- Disallow all ports but 443
- Audit developer changes

Availability
- Failures to tolerate: 2
- Disaster recovery site: us-east
- Hourly snapshots to backup

Access controls
- Users in group app-admin: Write
- Users in group ops: Read Only
- Disallow MySQL
Project Pacific: Rearchitecting vSphere with Native Kubernetes

Transforming vSphere into the App Platform of the Future

vSphere with Native Kubernetes | App-focused Management | Dev & IT Ops Collaboration

vSphere

Supervisor Kubernetes Cluster

ESXi Cluster | Networking | Storage

App

Kubernetes cluster
Virtual machines
Native pods

Developer

IT Operator

Improved Economics | Control at Scale | Increased Velocity
vSphere with Native Kubernetes

- Embed Kubernetes into the control plane of vSphere, unifying control of compute, network and storage resources
- Deliver Kubernetes clusters as a service to developers
- Converge VMs and containers using the new vSphere Native Pods that are high performing, secure and easy to consume
Application-Focused Management

- App level control for applying policies, quota and role-based access to Developers
- Apply vSphere features (HA, vMotion, DRS) at the app level and to the containers
- Unified visibility in vCenter for Kubernetes clusters, containers and existing VMs
Dev & IT Ops Collaboration

- Developers use Kubernetes APIs to access the SDDC
- IT operators use vSphere tools to deliver Kubernetes clusters to developers
- Consistent view between Dev and Ops via Kubernetes constructs in vSphere
Enable Kubernetes in vSphere with Supervisor Clusters
Enable Kubernetes in vSphere with Supervisor Clusters

- **vCenter**
- **ESXi**
- **Spherelet**
- **K8s Master VM**
- **ESXi Cluster**
- **hostd**
- **DevOps**
- **Superior Kubernetes Cluster**
A Kubernetes Control Plane for the SDDC

On-premises | Hybrid cloud | Public cloud
Kubernetes as a Service

On-premises | Hybrid cloud | Public cloud
Virtual Machine Service

On-premises | Hybrid cloud | Public cloud
Anything as a Service

![Diagram of Workload Platform]

- Kubernetes Service
- Virtual Machine Service
- Application Services
- Supervisor Kubernetes Cluster
- ESXi Cluster
- Networking
- Storage
- vCenter
- Ecosystem

On-premises | Hybrid cloud | Public cloud
Platform Architecture
What is Kubernetes Controller?

Reconciliation in action

- Database (etcd)
- API Server
- Controller Manager
- State of the world
What Is a Kubernetes Operator?

Kubernetes Operator

Custom Resource Definition (CRD)

Custom Controller

Operator Pattern

Custom Resource Definition = Definition of New Object Managed Thru Kubernetes API

Custom Controller = Manages the Lifecycle of Custom Resource defined by the CRD
What Is Cluster-API?

Cluster API Controllers deliver declarative, Kubernetes-style APIs for cluster creation, configuration, and management. They require a running Kubernetes Cluster to provide the Master API. Cluster API uses Custom Resource Definitions (CRDs) to manage Component Objects. Infrastructure Providers deliver "actuators" that implement VM lifecycle management. Kubeadm (another k8 lifecycle project) to actually bootstrap the individual Nodes.

Clusters

- Kubernetes Nodes
- AWS
- VMware
- Google Cloud
- Azure

Cluster Spec

- Cluster: Dev
- Machine Class: Small + Large VMs
- Machine Control Plane: 0/1/2...
- Machine Deployment: Mix of Small/Large VMs Possible

Cluster API

- Kubernetes Cluster
- Management Cluster
Workload platform architecture
Guest Kubernetes Clusters

Layered approach
Multi-tenancy with supervisor cluster namespaces

Each Namespace has its own Resource Pool

Resource Isolation with Quota for CPU/Memory/Storage

All Workloads in a Namespace are bounded by Namespace Quota
  - Guest Clusters
  - Native Pods
  - Virtual Machines
Supervisor Cluster Network Topology and Isolation

It leverages NSX network capabilities.

Supervisor Clusters are isolated with Tier-1 Routers and Distributed Firewalls.

Namespaces are isolated with vSwitches and Distributed Firewalls.

Inbound Traffic are denied for all namespaces by default.

Guest Clusters can use your preferred overlay (Calico by default).
Cloud Native Storage

Unified management of cloud native storage

vSphere SPBM policies become Storage Classes in Supervisor cluster

Works across local, hyperconverged and shared storage

Leverage full vSphere ecosystem of storage partners

Exposes persistent volumes as paravirtualized drivers in Supervisor Namespace
Native pods

Better security and resource isolation
Better performance
Provide serverless experience to DevOps
Provide workload visibility to VI Admins
Native pod technical details

- Native Pod runtime for ESXi
- Secure isolation of Pods
- Light weight and fast
- Advanced resource management
- Micro-segmented Pod network
Demo

Bringing IT Ops and Dev together!
Modern Apps Portfolio

Build

- bitnami
- Expert Services
- Pivotal

Run

- Project Pacific
- VMware PKS

Manage

- Tanzu Mission Control
  - Optimization
    [powered by CloudHealth]
  - Observability
    [powered by Wavefront]
Next Steps

1. Sign-up for Project Pacific Beta: [Link](#)
2. VMworld US & EU Session Recordings: [Link](#)
3. Project Pacific Website: [Link](#)
4. Project Pacific Architecture @ Tech Field Day: [Link](#)
5. Project Pacific Blog: [Link](#)
6. Project Pacific HOL – Coming Soon
Thank You!
Join the conversation

#vFORUMAU  
@VMwareAU