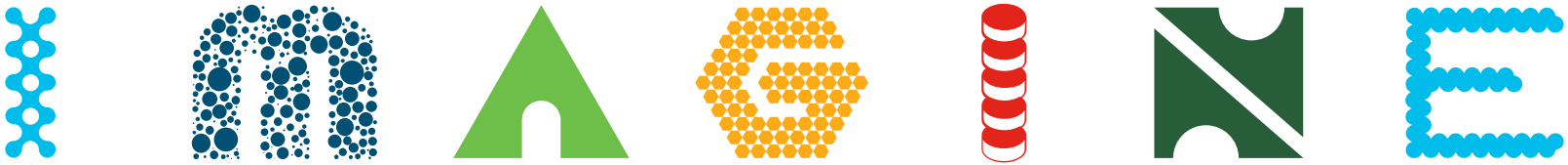


INTUITIVE

Cisco live!

June 10-14, 2018 • Orlando, FL

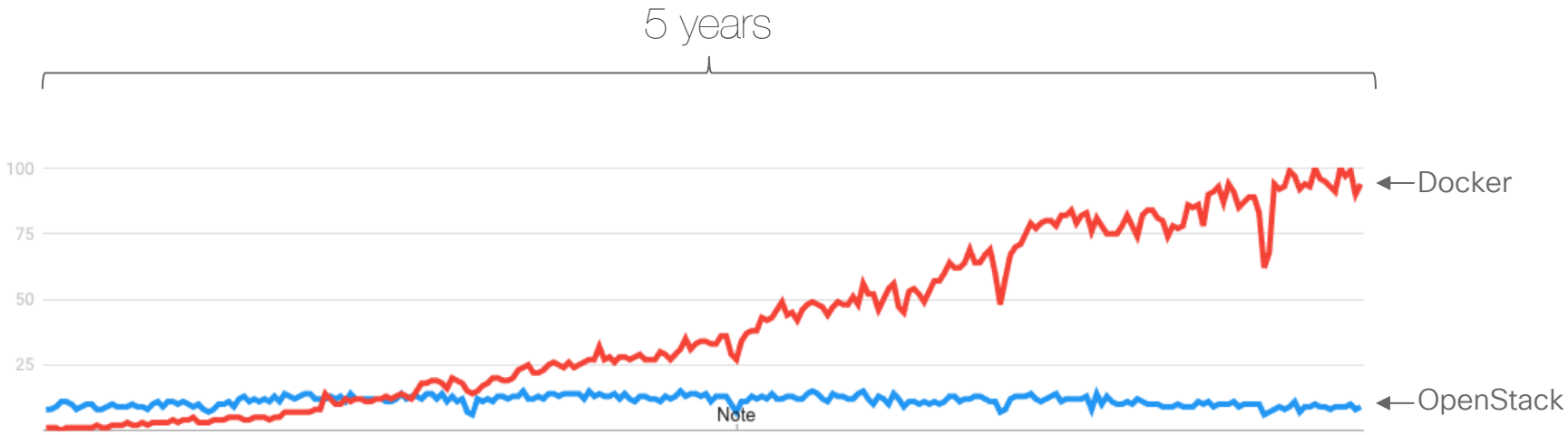
#CLUS

ACI with Kubernetes to create a private devops cloud

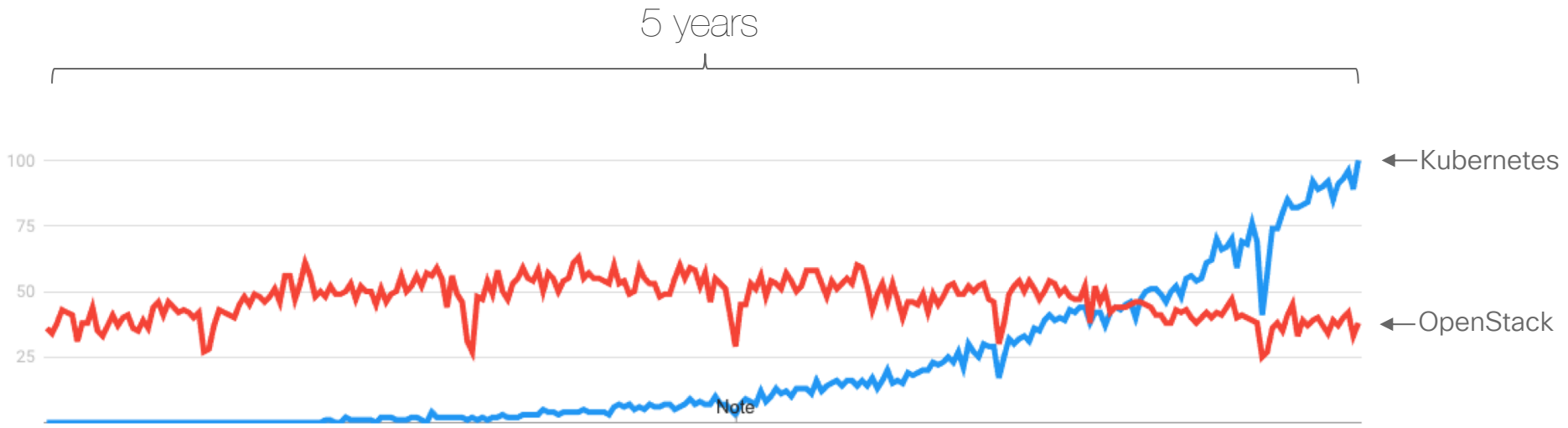
Luis Flores
Rafael Muller
Cesar Obediente

LTRACI-2967

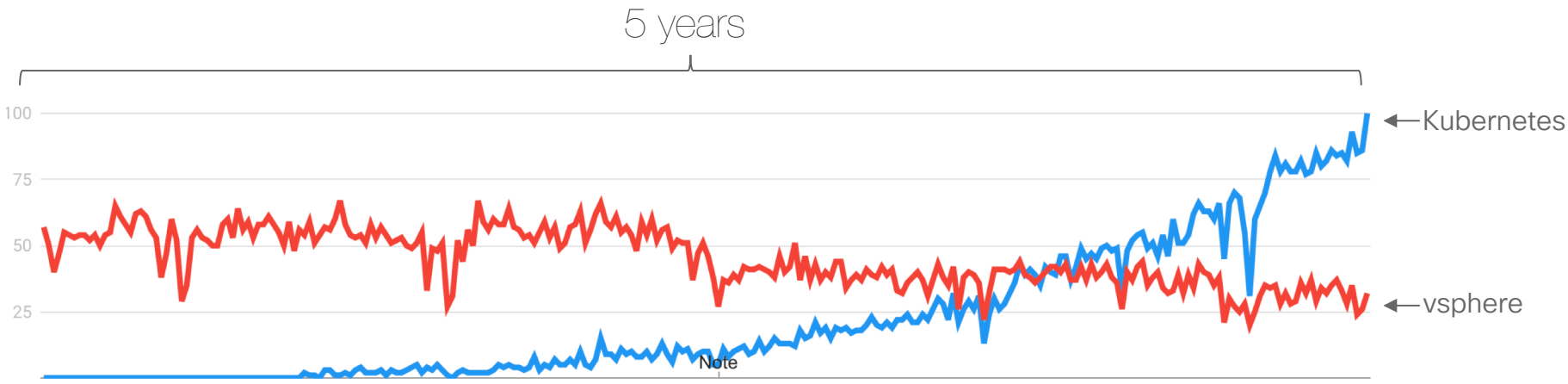
Google trends



Google trends



Google trends



Why this trend?

Applications

- Containers and orchestrators like Kubernetes are focused on application development and deployment as services
- Creates a mechanism for developers to operationalize what they work on (Dev-Ops)

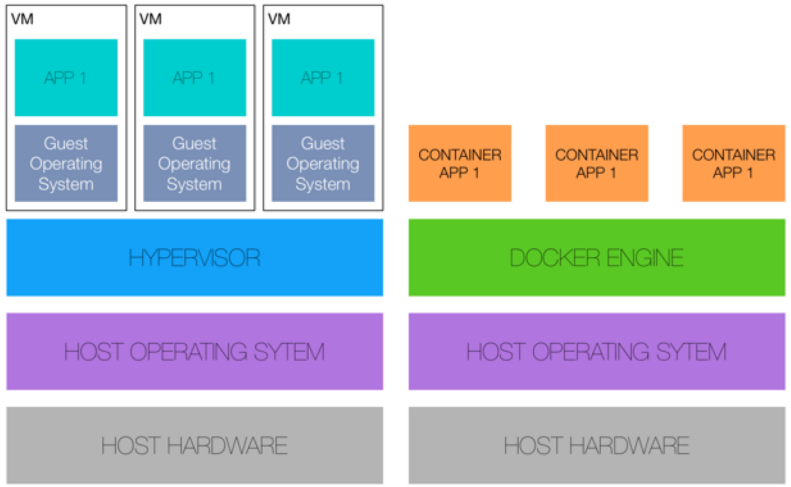
What are containers?

> **Containers are a solution to the problem of how to get software to run reliably when moved from one computing environment to another**. This could be from a developer's laptop to a test environment, from a staging environment into production, and perhaps from a physical machine in a data center to a virtual machine in a private or public cloud.

Paul Rubens
cio.com

But Technically?

- A container is a binary executable, packaged with dependencies and intended for execution in a private namespace with optional resource constraints.
- This provides the containers multiple isolated operating system environments with their own file system, network, process and block I/O space on the same host



What is Kubernetes?

- Kubernetes is an open source Container Orchestration system for automating deployment, scaling and management of containerized applications.
- Real production apps span multiple containers. Kubernetes gives you the orchestration and management capabilities required to deploy containers, at scale, for these workloads.
- It was inspired by the Google Borg System and with its v1.0 release in July 2015, Google donated it to the Cloud Native Computing Foundation (CNCF).
- Generally, Kubernetes has new releases every three months. The current stable version is 1.9 (as of Jan 2018).

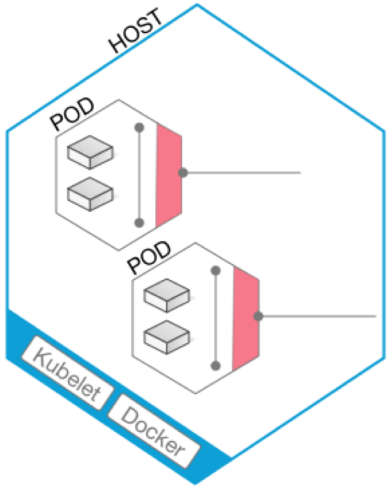
What is kubernetes?

- Orchestrate containers across large scale of compute resources
- Scale containerized applications automatically or via operations controls with simple commands
- Declarative configuration of services and deployments
- Manage storage and resources for all containers
- Health-check of containers and hosts

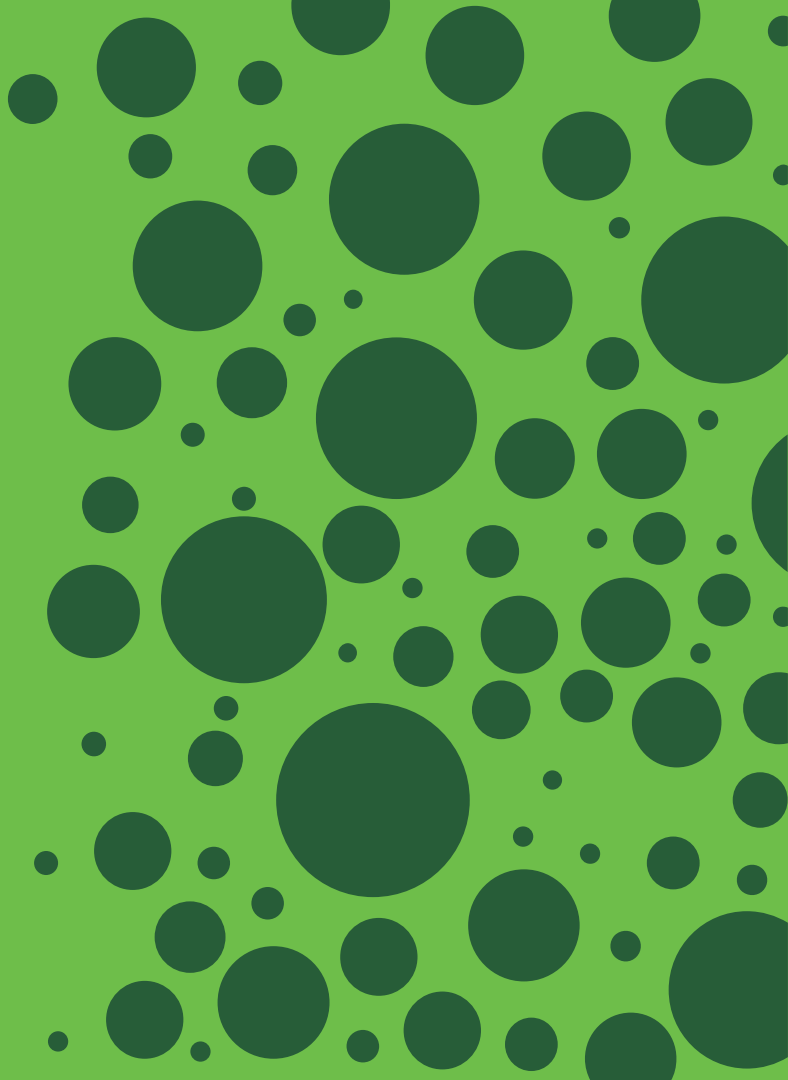
What is a Kubernetes POD?

A *pod* (as in a pod of whales or pea pod) is a group of one or more containers (such as Docker containers), with shared storage/network, and a specification for how to run the containers

A pod models an application-specific "logical host" - it contains one or more application containers which are relatively tightly coupled — in a pre-container world, they would have executed on the same physical or virtual machine.



Challenges running Kubernetes



Segmentation

- Network isolation amongst namespaces
- Control access to services

Outside Cluster Communication

- Communication to non-kubernetes services
  - Policy access outside cluster

Kubernetes

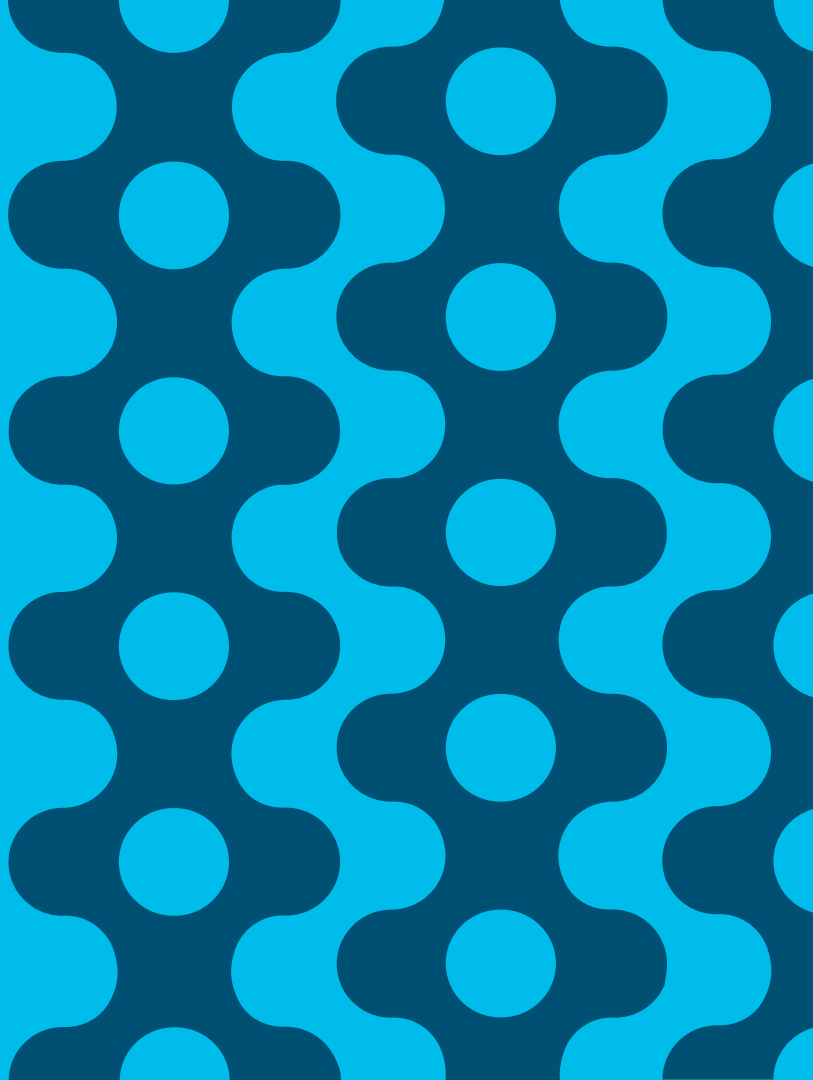
Storage across cluster

- Line rate access to storage from nodes

Operations

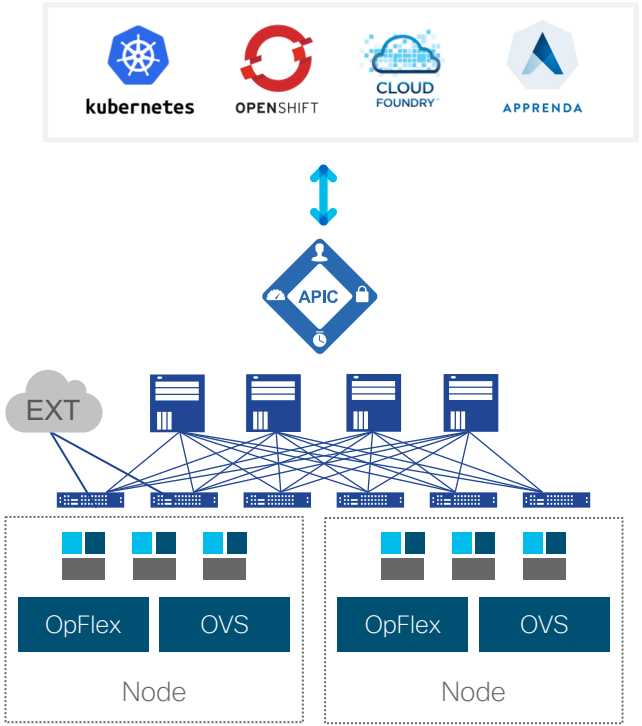
- Visibility and governance of policies
- Simpliied networks operations

ACI and Kubernetes Solution Overview



Cisco live!

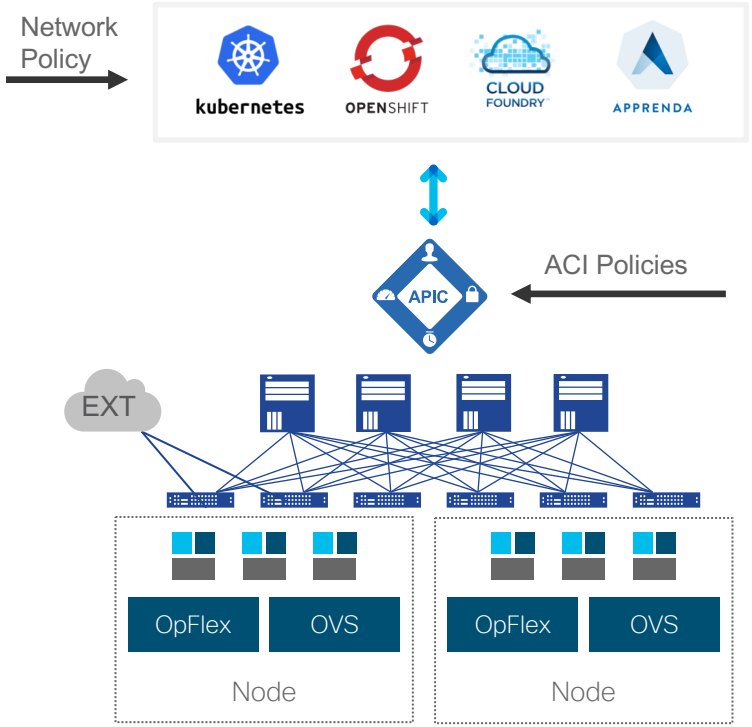
Cisco ACI Integration with Containers / PaaS



Key Benefits

- Unified networking: Containers, VMs, and bare-metal
- Micro-services load balancing integrated in fabric for HA / performance
- Secure multi-tenancy and seamless integration of Kubernetes network policies and ACI policies
- Visibility: Live statistics in APIC per container and health metrics

ACI and Container Integration – CNI Plugin



Technical Highlights

- POD IP addresses are visible as regular endpoints in the fabric – route/bridge to any other endpoint
- Kubernetes Network policies supported using standard upstream format enforced through OpFlex-OVS using APIC Host Protection Profiles
- Embedded fabric and virtual switch load balancing
  - ACI PBR in fabric for external service load balancing
  - OVS used for internal service load balancing
- VMM Domain for Kubernetes
  - Stats per namespace, deployment, service, pod
  - Physical to container correlation

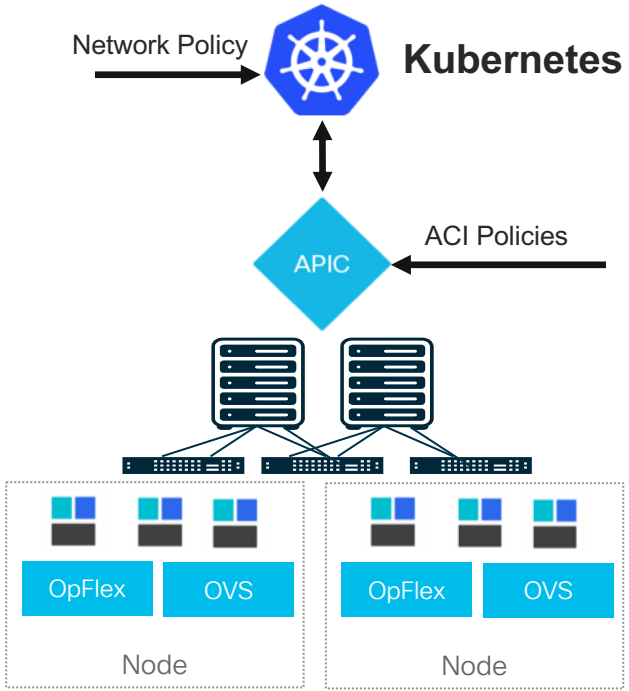
Leverage APIs, transparent to dev-ops

- Security Policies within and between PODs are defined using Kubernetes Network Security API.
- Kubernetes policies implemented on OVS by APIC, visible to ***fabric*** administrator.
- Kubernetes Services: the service IP is automatically managed by ACI + Opflex + OVS as an anycast service
- Kubernetes External Services (LoadBalancer) can be implemented by ACI PBR or an external LB.

Facilitate policy and connectivity to other workloads

- ACI admin can define EPGs and contracts that are exposed to Kubernetes users
- Kubernetes administrator can annotate objects, such as namespaces, deployments or even specific pods to map them into endpoint groups
- Enable Kubernetes Deployments/PODs to access other resources without bottlenecks and with conforming policy

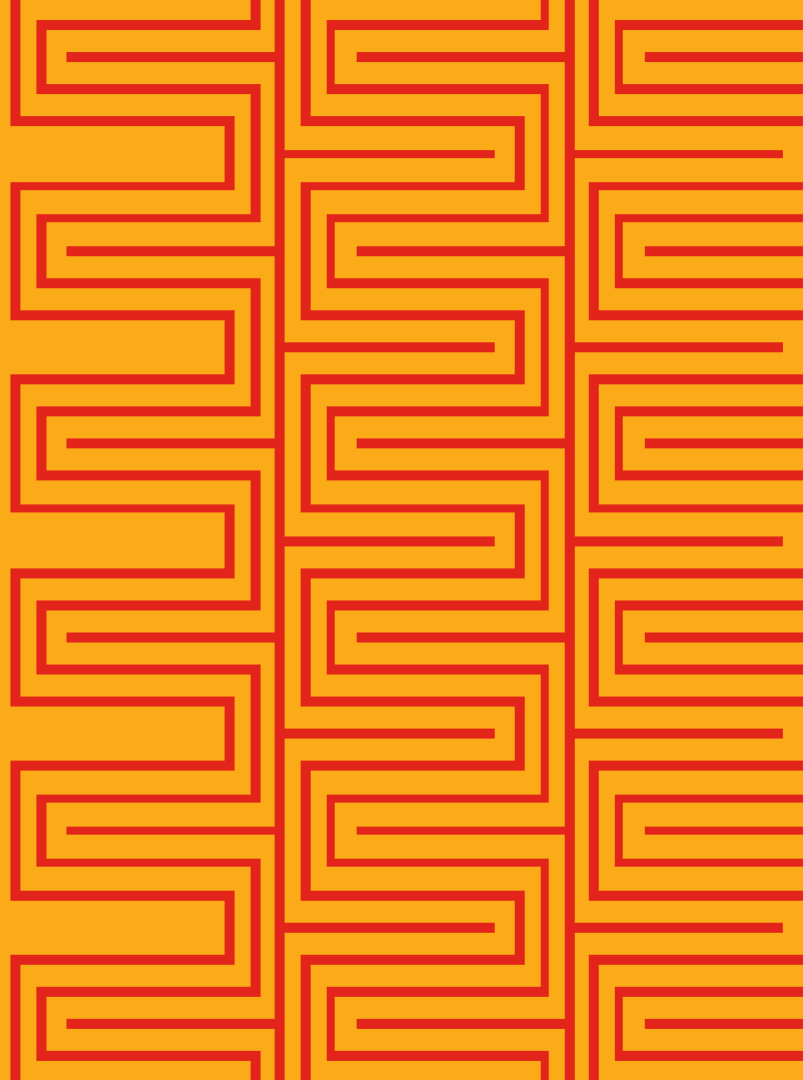
ACI VMM Domain for Kubernetes



Technical Description

- Network policies of Kubernetes supported using standard upstream format but enforced through OpFlex / OVS using APIC Host Protection Profiles
- Kubernetes app configurations can be moved without modification to/from ACI and non-ACI environments
- Embedded fabric and virtual switch load balancing
  - PBR in fabric for external service load balancing
  - OVS used for internal service load balancing
- VMM Domain for Kubernetes
  - Stats per namespace, deployment, service, pod
  - Physical to container correlation

Where can you use the ACI CNI Plugin?



Supported Container Application Platforms

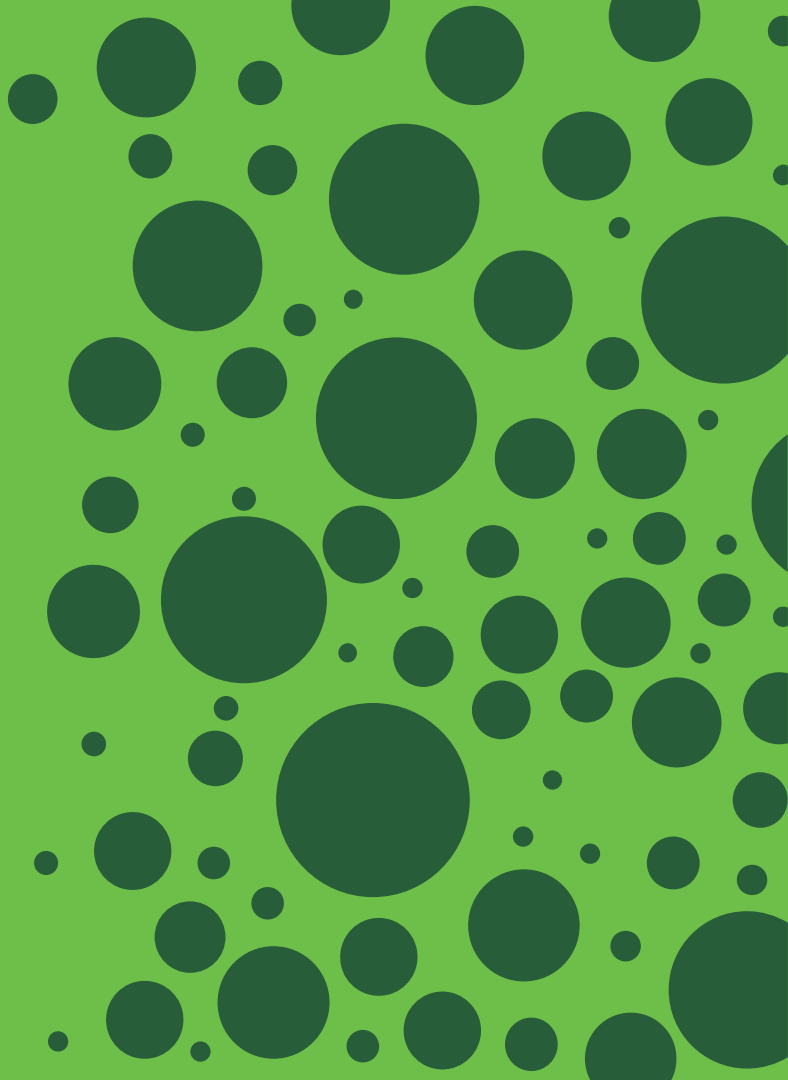
	Baremetal	ESXi	KVM
Open source Kubernetes 1.6-1.10	✓	✓	Future
Openshift 3.7-3.9	✓	✓	2HCY18
Pivotal Cloud Foundry 2.x	✓	✓	Future
Docker EE (Kubernetes)	Future	Future	Future
Mesosphere	Future	Future	Future

Cisco dev-test versions

	ACI 3.0(1)	ACI 3.0(2)	ACI 3.1(1)	ACI 3.1(2)	ACI 3.2(1)
Kubernetes 1.6	✓	✓	✓		
Kubernetes 1.7			✓	✓	✓
Kubernetes 1.10					✓

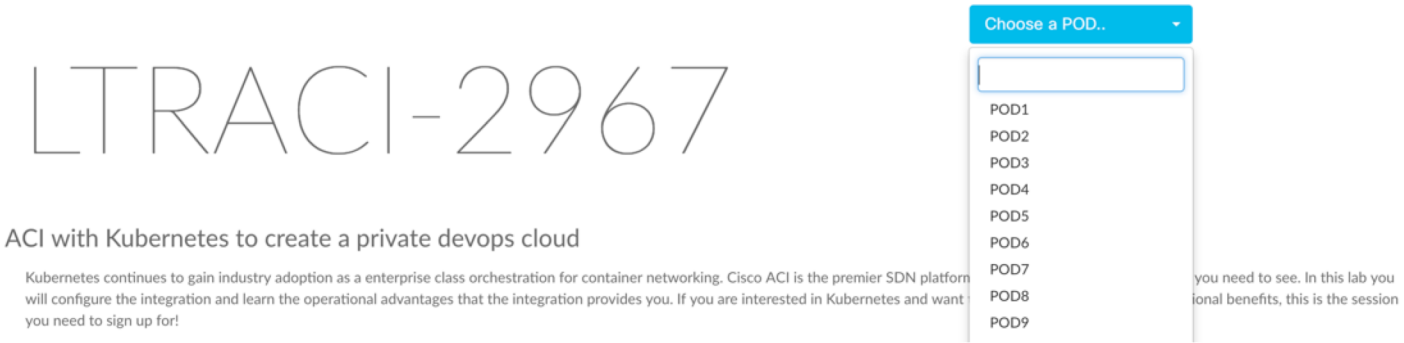
https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/aci/virtualization/matrix/virtmatrix.html

About the lab

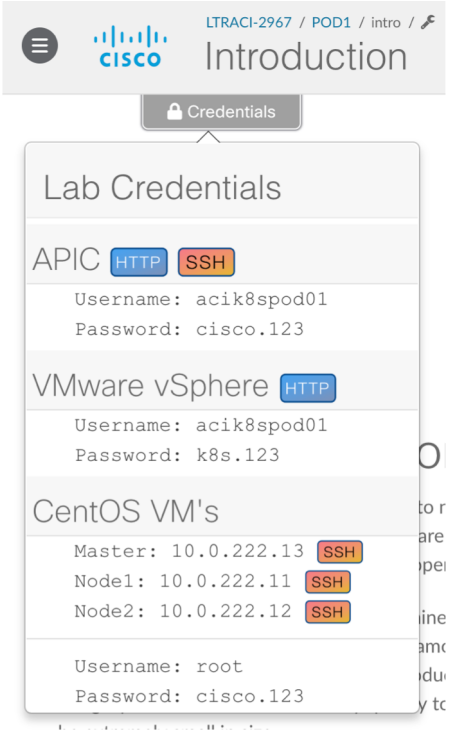


Web based Lab

http://aci-k8s-lab.ciscolive.com

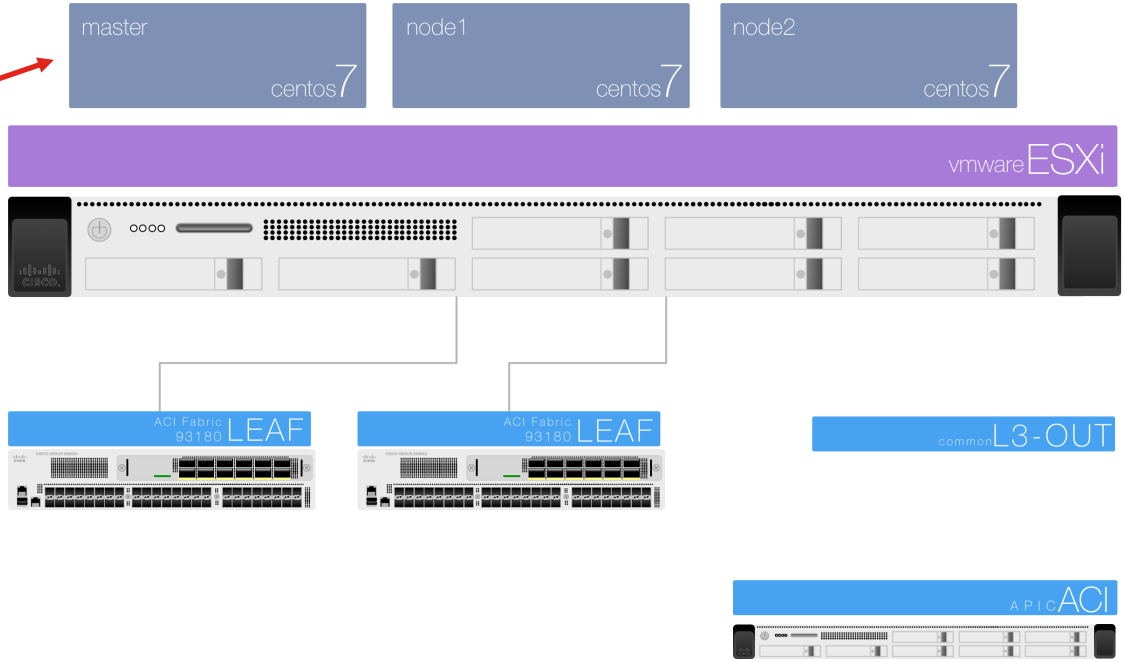


Devices and credentials



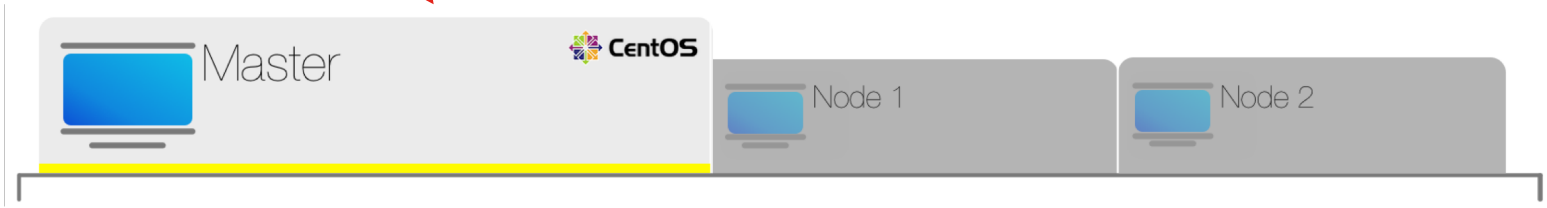
- Three virtual machines (VMware) for each Lab POD
- Will use a real ACI fabric with latest leaf hardware that is required for Kubernetes
- vShpere access
- Virtual machines are running CentOS 7
- Access to credentials always available on lab document with links to open each component
- SSH directly in browser

Three Virtual Machines



!

Document Indicator



Simplified steps

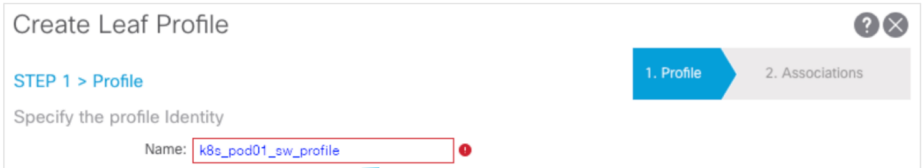
Lab doc provides step by step

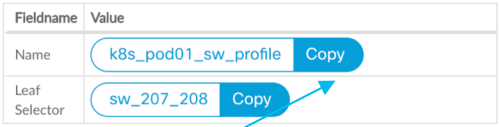
Easy to copy steps

```
[root@pod01-master ~]#
[root@pod01-master ~]#
[root@pod01-master ~]#
```

```
yum -y install epel-release
```

Bash Copy





paste

copy

You can start the lab!

Complete your online session evaluation

Give us your feedback to be entered into a Daily Survey Drawing.

Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don't forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.

Cisco Webex Teams

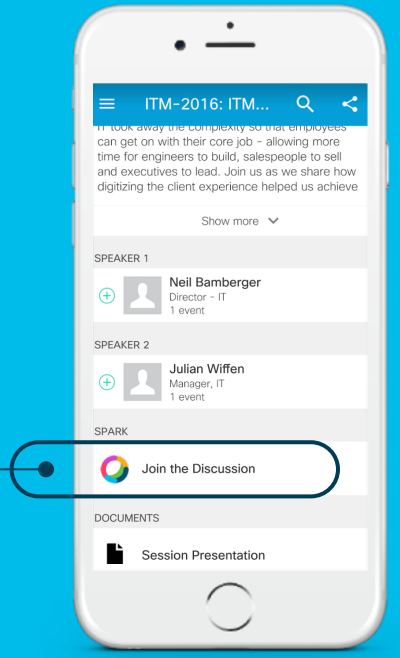
Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

How

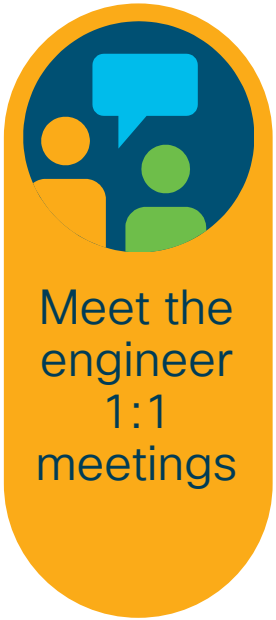
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

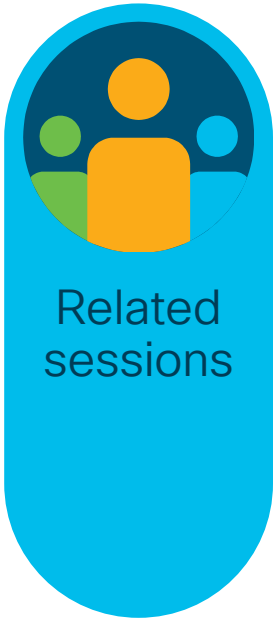
Webex Teams will be moderated by the speaker until June 18, 2018.



cs.co/ciscolivebot#BRKXXX-xxxx

Continue your education





Thank you

INTUITIVE