Cisco Container Networking Overview and Roadmap

Cisco Knowledge Network

Nov 2017

Phil Lowden, Consulting Systems Engineer

What Is A Container?

Virtual Machine

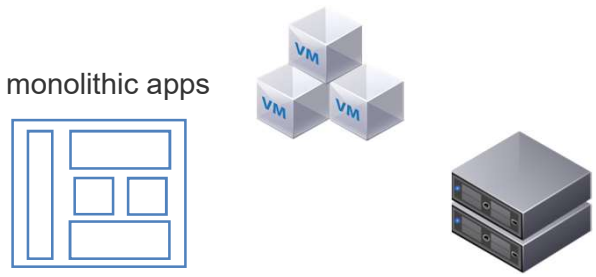
Container

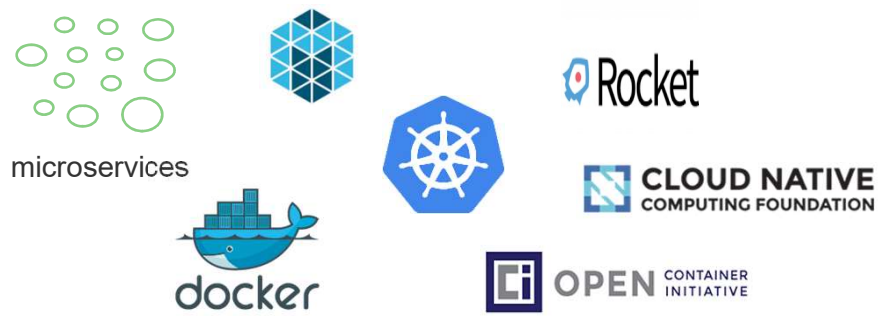
Containers vs VMs

Containers	Virtual Machines
Shared resources	Isolated resources
Lighter weight	Full OS + application
Faster installation	Several minutes to boot
No hypervisor	Hypervisor-based
Linux and Windows	No underlying OS
Microservices	Monolithic

Why: New Application Architectures

Monolithic Apps	Cloud Native Apps
server / hypervisor	server clusters, containers
dependencies	easy upgrade
stateful	microservices
waterfall development	agile devops teams





Linux Containers

- .Group of processes on a Linux machine
  - Isolated environment
  - Linux system within another Linux system
- Inside the container, it looks like a VM
- Outside the container, it looks like normal processes running on the machine

solaris Zones

OpenVZ

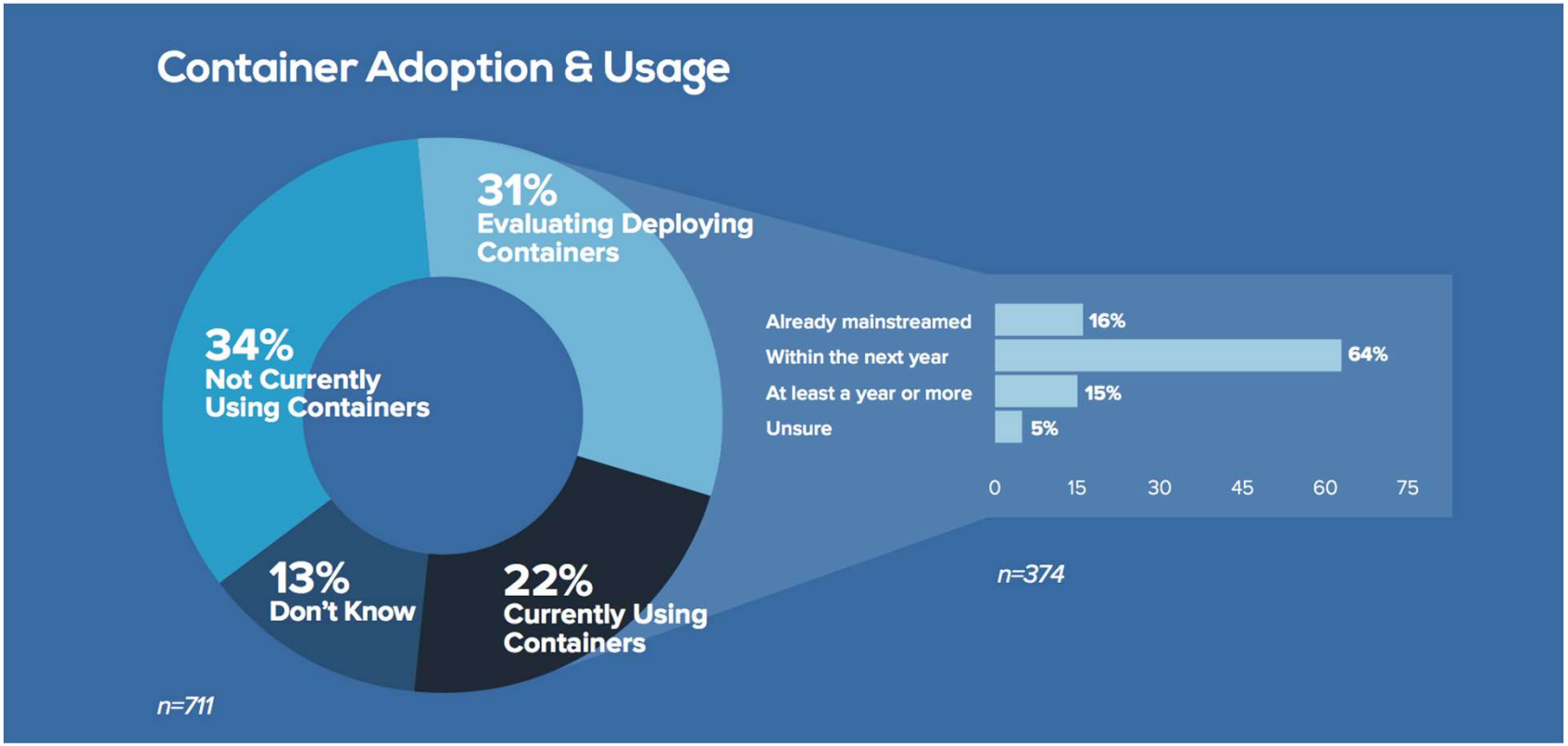
OPEN CONTAINER INITIATIVE

docker

Rocket

7

Industry trends



What Is Docker?

What is Docker?

Docker is a software technology providing containers, promoted by the company Docker, Inc. Docker provides an additional layer of abstraction and automation of operating-system-level virtualization on Windows and Linux.

[Source: Wikipedia]

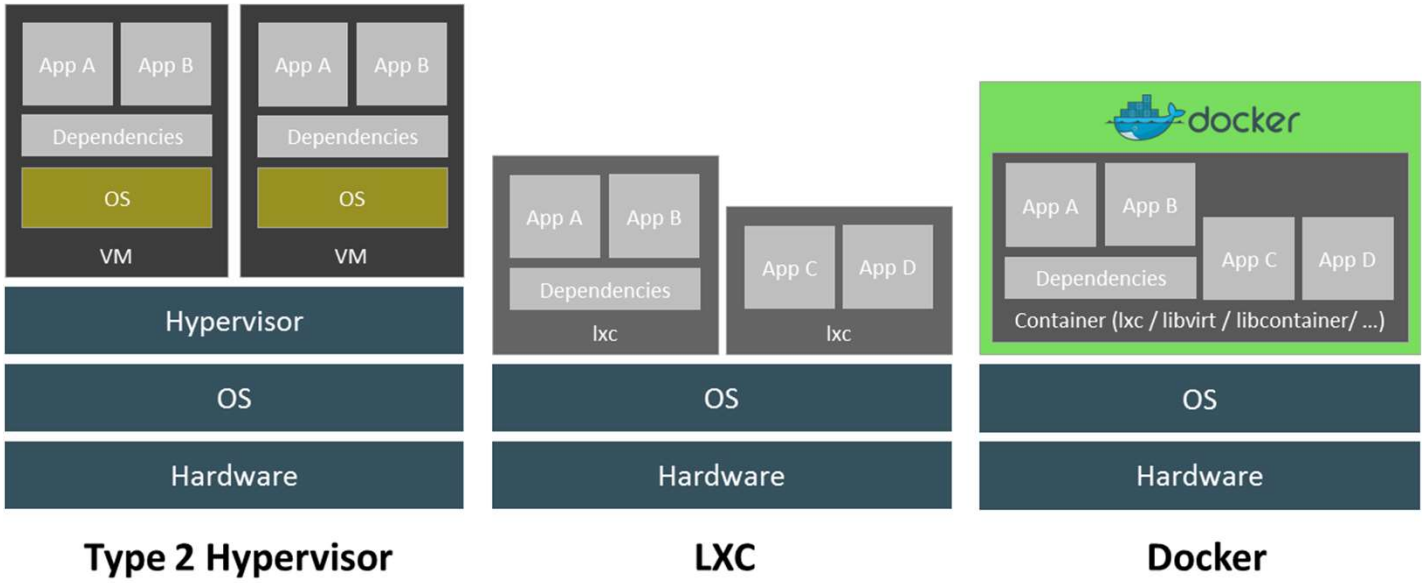
Docker is an open platform that helps companies build, ship and run their applications anywhere.

[Source: Docker, Inc]

Virtualization Technologies Comparison

- Docker provides a unified access to:
  - Linux container technology (cgroups, namespaces)
  - Various container implementations (lxc, libvirt, libcontainer, etc.)

- ‘libcontainer’ is Docker’s implementation of container technology

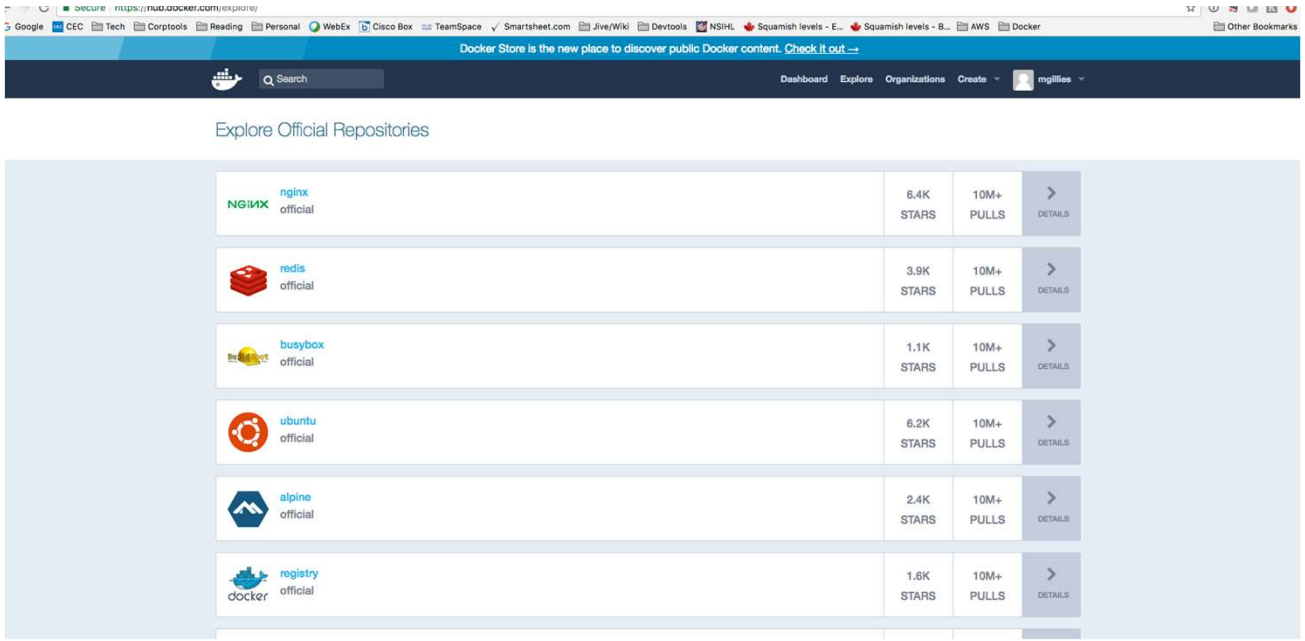


Type 2 Hypervisor **LXC** **Docker**

Why Docker Containers?

- **Standardization of the container format**
- **Development of an ecosystem for sharing containers**

Dockerhub



- Sign up for an account on dockerhub
- Public repository of Docker images
  - https://hub.docker.com/
  - docker search [term]

Docker+Cisco Partnership

Joint Engineering, Sales and Marketing

Contiv Network Plugin

Docker Datacenter On FlexPod CVD

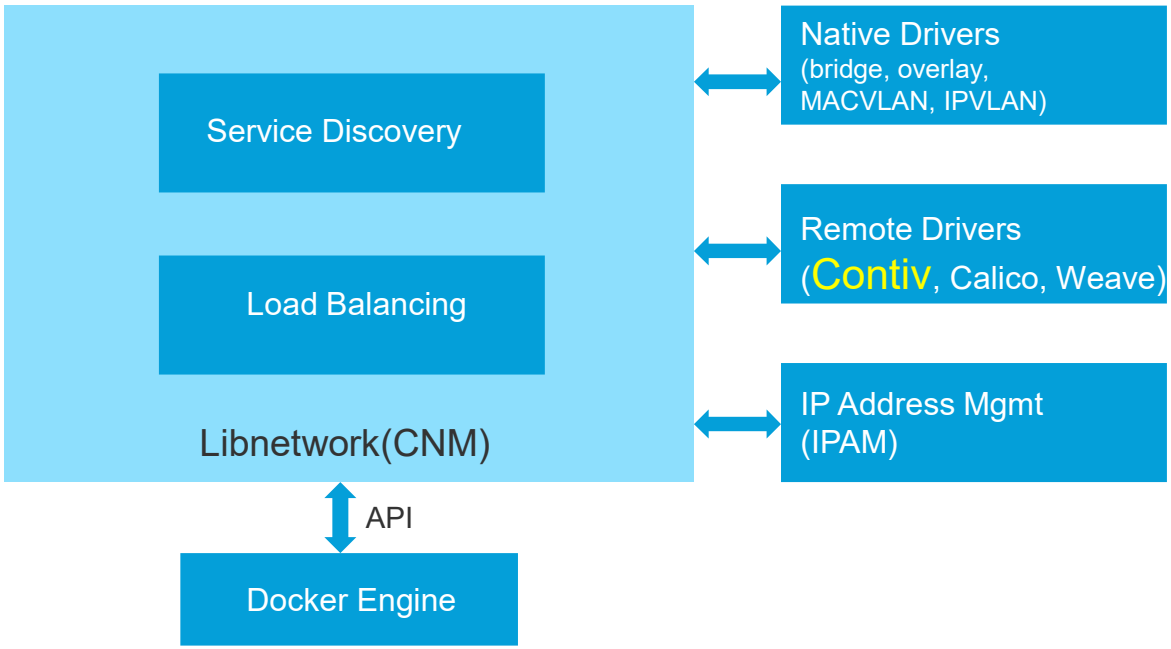
Docker Datacenter On Cisco UCS

Stronger Together

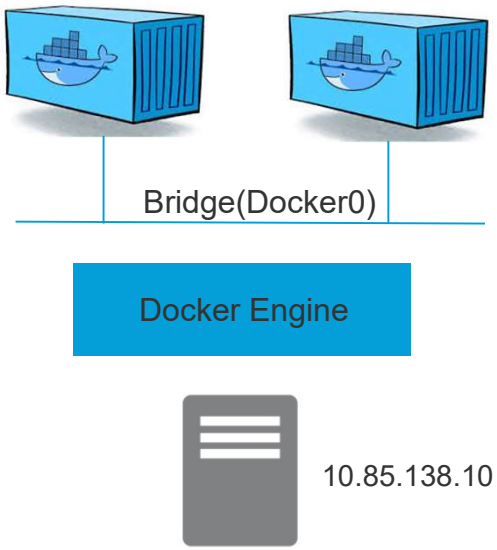
Open Source community and technology partners to build solutions

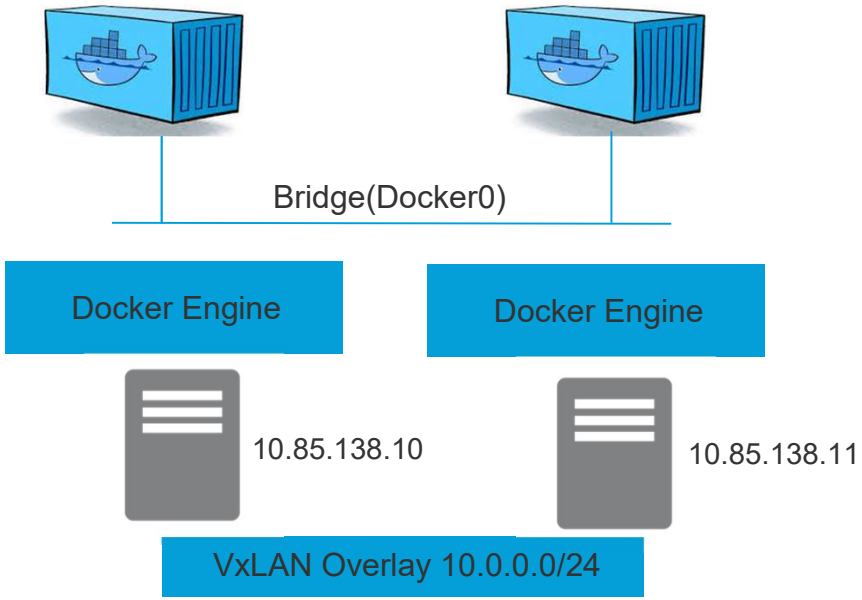
What Is Docker Networking?

Docker Networking Architecture

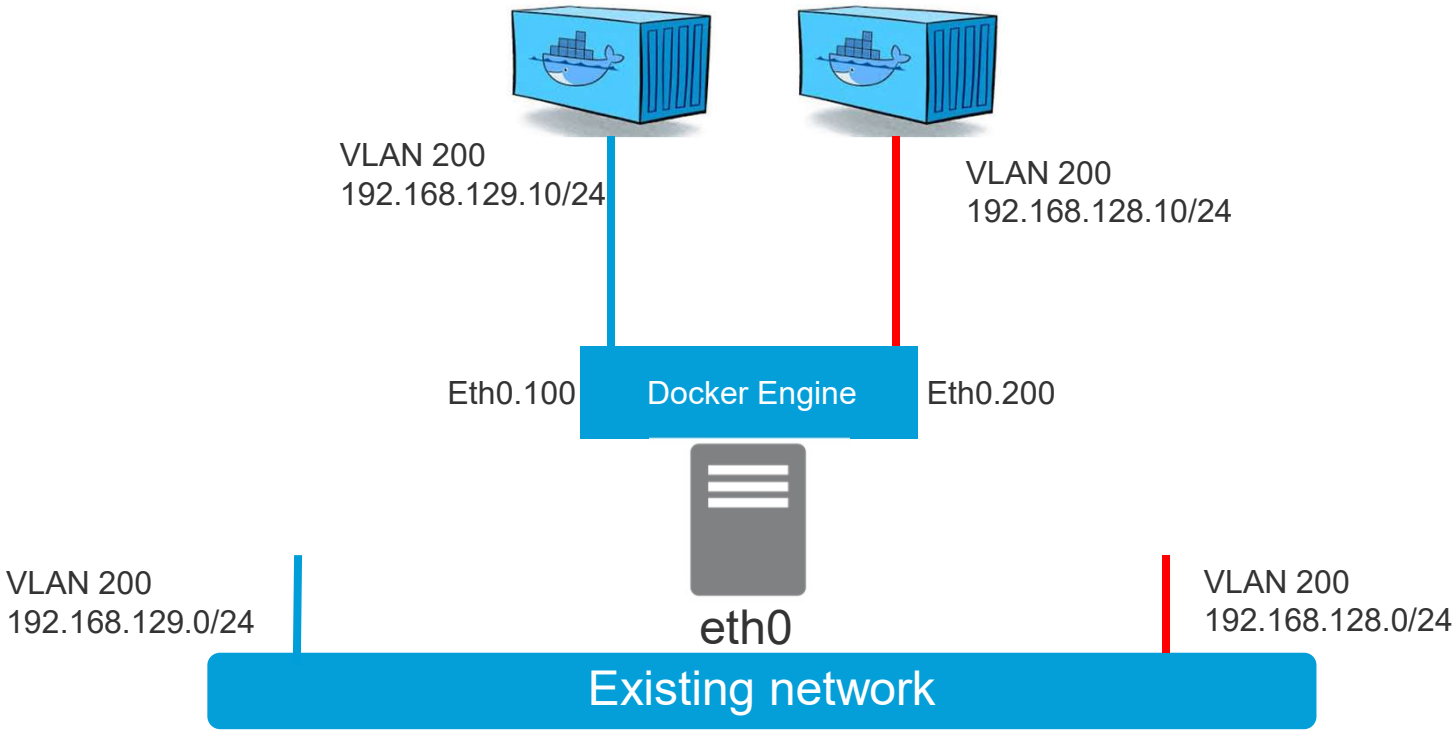


Docker networking: single host versus multi host



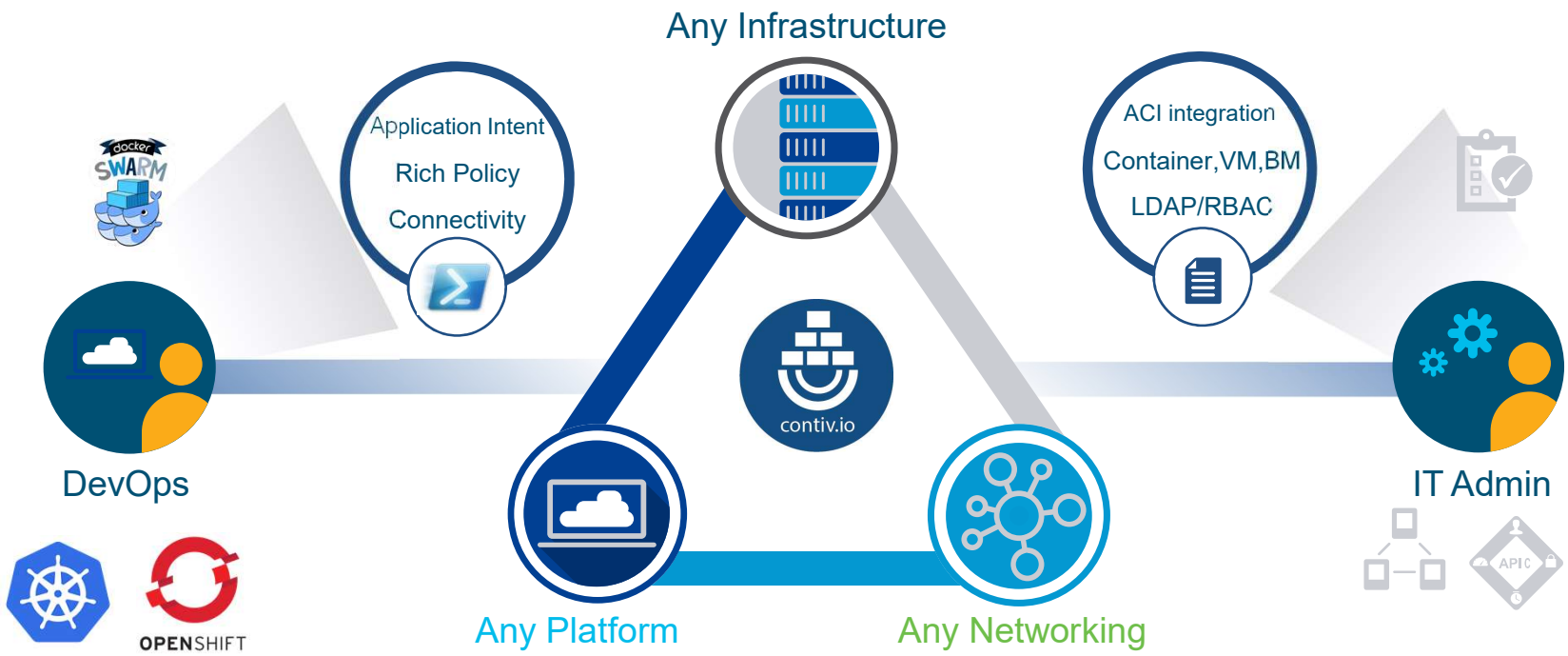


Docker Networking: MACVLAN Driver



What Is Contiv?

What is Contiv



100% Open Source	The Most Powerful Container Networking Fabric **L2, L3, Overlay or ACI**	Rich Policy Model

Production-Grade Network and Security Policies

Multi-Tenant, Multi-Host
Network Connectivity

Network Security
and Isolation
(White/Black List Rules)

Traffic Prioritization and
Bandwidth Allocation

Network Monitoring
(Live Connectivity
Graphs and Stats)

Integration with
External Network
(Cloud | Nexus | Cisco ACI)

Micro-Services
Load Balancing

Integrated IPAM,
Service Discovery

Performance and Scale

Available at https://github.com/contiv/netplugin

Contiv Integration with Cisco Products

Application-Centric Infrastructure (ACI)

- Containers integrated with APIC policies
- Physical services integration

Nexus Standalone or Any Network

- BGP interop (standard routing protocol)
- EVPN-based multi-tenancy and automation

Unified Compute Systems: B and C Series

- Leveraging vNICs for control, data, management, and storage traffic
- Offload encapsulation function

Contiv Leverages Underlying Infrastructure Capabilities for Applications

Cisco Container Solutions

Cisco Integrated Infrastructure for Containers

Cisco UCS with Docker Datacenter 1.x

Enterprise Ready

Design choices

Scalable Architecture

Jointly Engineered

Delivered by Partners

FlexPod with Docker Datacenter 2.x

NetApp Docker Vol Plugin

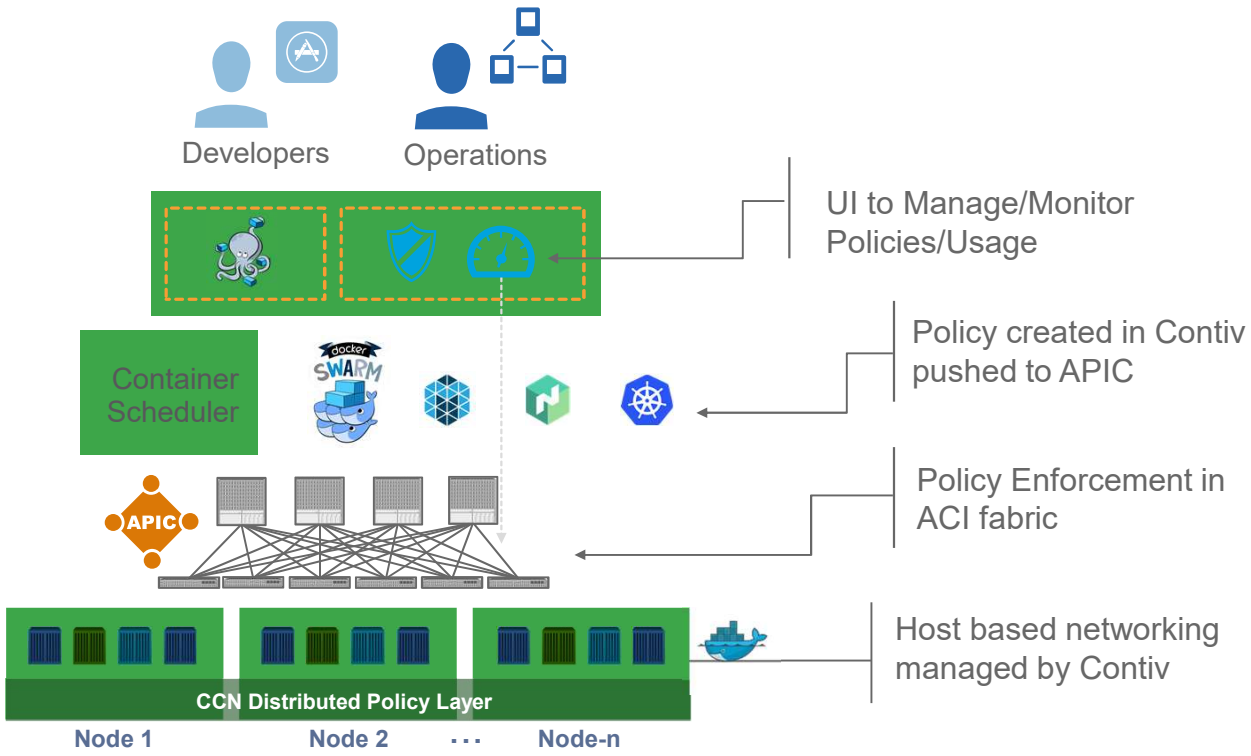
Container and Microservices Solutions on Cisco UCS Integrated Infrastructure

Cisco Container Solutions

- Infinite Video
- Mobile Evolved Packet Core (EPC)
- OpenStack Network Function Virtualization Infrastructure (NFVi) aka Project Mercury)
- Lindt (open network operating system)
- Virtual Managed Services (VMS)
- Digital Network Architecture Center (DNA-C) open, programmable architecture
- Installation Containers

Available as Open Source

Project Contiv and ACI

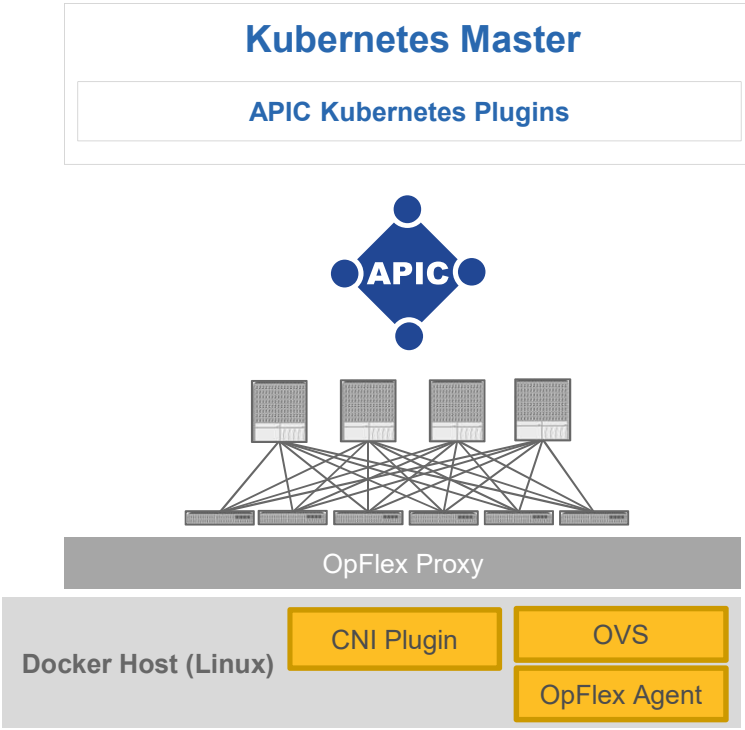


Project Contiv

- Provides policy-based container networking
- Multiple deployment options including overlay, L3, and ACI
- Integrates with multiple orchestration tools
- Support option to be made available from Cisco
- Learn more:
  - https://github.com/contiv

Contiv Enables Policy Based Distributed Container Networking

ACI + Kubernetes Integration



Kubernetes

Kubernetes is open source container mobility among on-premises, hybrid, or public cloud ("multicloud") infrastructure, letting you effortlessly move workloads to where it matters to you

ACI + Kubernetes Integration

- APIC GUI integration / VMM Domain specifically designed for Kubernetes
- Visibililty / statistics / health metrics for containers
- OVS + OpFlex provides Docker host datapath
- Flexible mapping of Kubernetes into ACI policies
  - Container teams set Kubernetes network policies
  - Network team retains control of ACI policies for EPGs / contracts
- Distributed load balancing
  - Symmetric PBR in ACI fabric for north south LB
  - OVS + OpFlex for distributed east-west LB

Solution Support for Contiv Open-source

How We Help	Engineer Expertise	What's Unique
• Our customers can rely on us to keep their container networking fabric environments operating • Fewer physical network devices to manage and operate • Easier to manage container networking services on demand • Container automation of security and application policies	• Container Networking Fabric • Virtual Network Per Tenant • Segment Per Microservice • Network-based Service Routing • Security Policies	• Solution Support Service for Cisco Contiv Open-source • Embedded Basic Support with Cisco Smart Account entitlement • Supports container networking fabric interoperability from solution partners

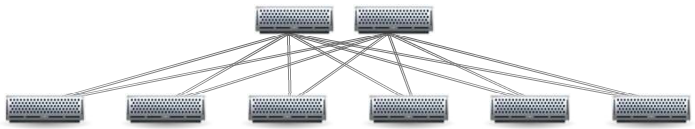
Service Provider Use Cases

Flexible Connectivity to Place Containers Anywhere

Native Connectivity

Use Case:
Private Cloud

Infra Policy: [Bridged | Routed]

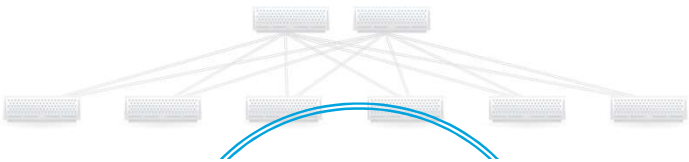


VLAN | IP (BGP) Handoff to Access Node

Overlay Connectivity

Use Case:
Private Cloud
Public Cloud

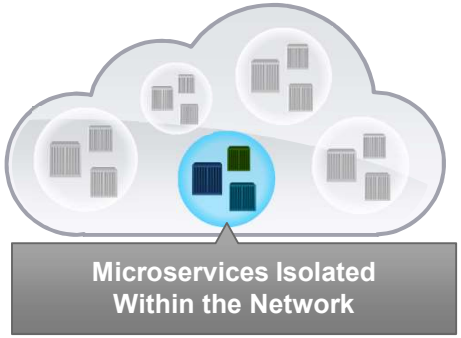
Infra Policy: [Overlay] [Bridge | Routed]

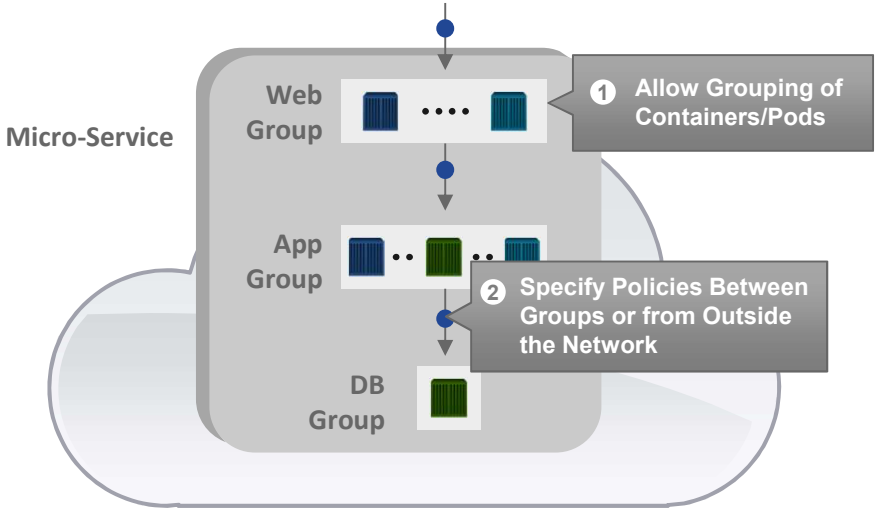


Overlays for Inter-Container Traffic

Any Network Topology and Container Visibility Across Physical Network

Scalable, Secure Microservices Deployments

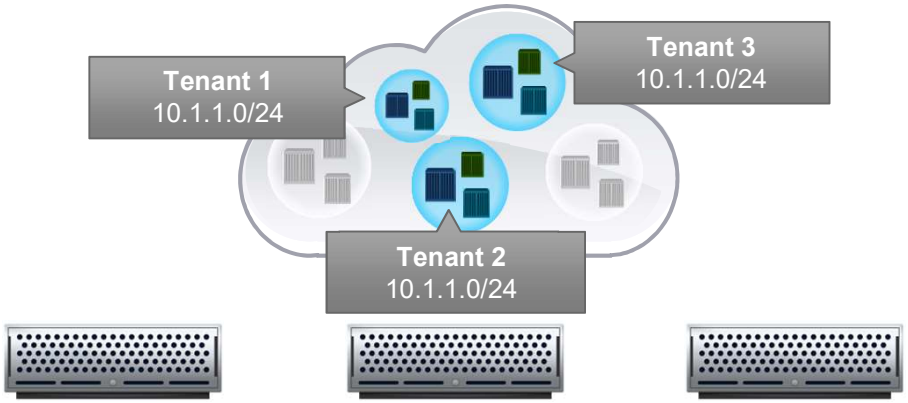




Ability to Provide Granular Micro-Service Security in a Scalable Way

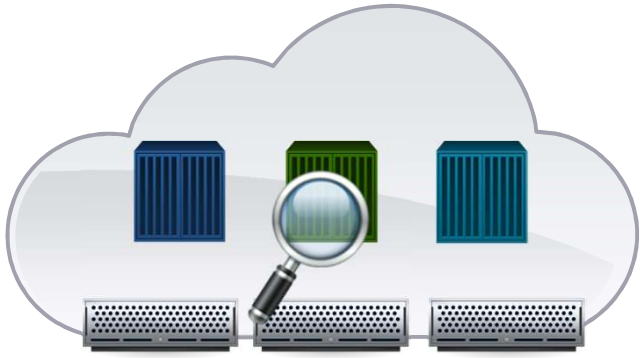
Multi-Tenancy

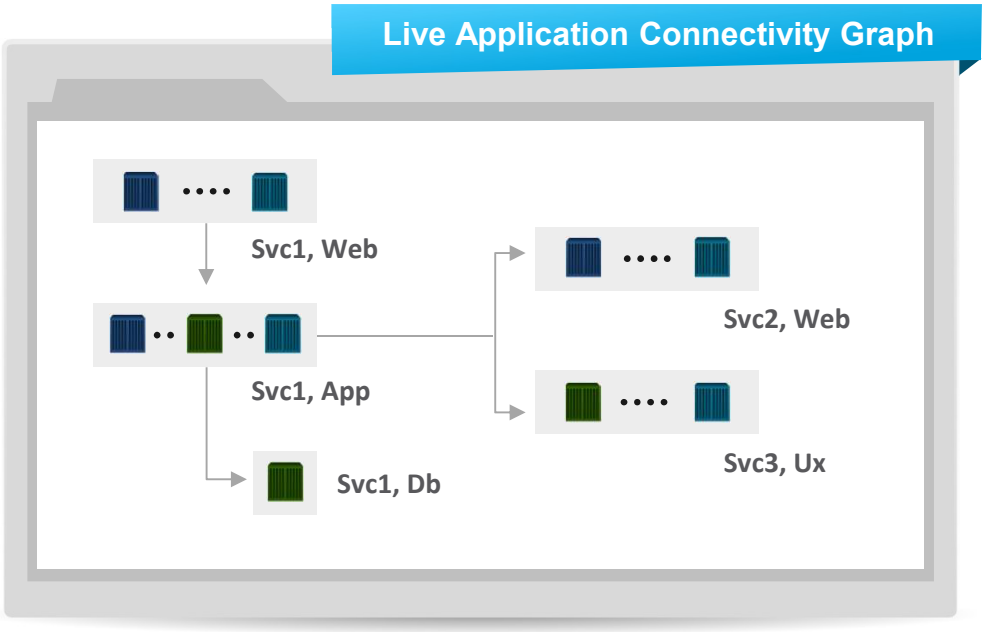
Separation of Policy/Network



Ability to Support Many Secure Tenants with Individual Policies or Overlapping IP

Telemetry and Monitoring





Ability to Troubleshoot Micro-Service Application

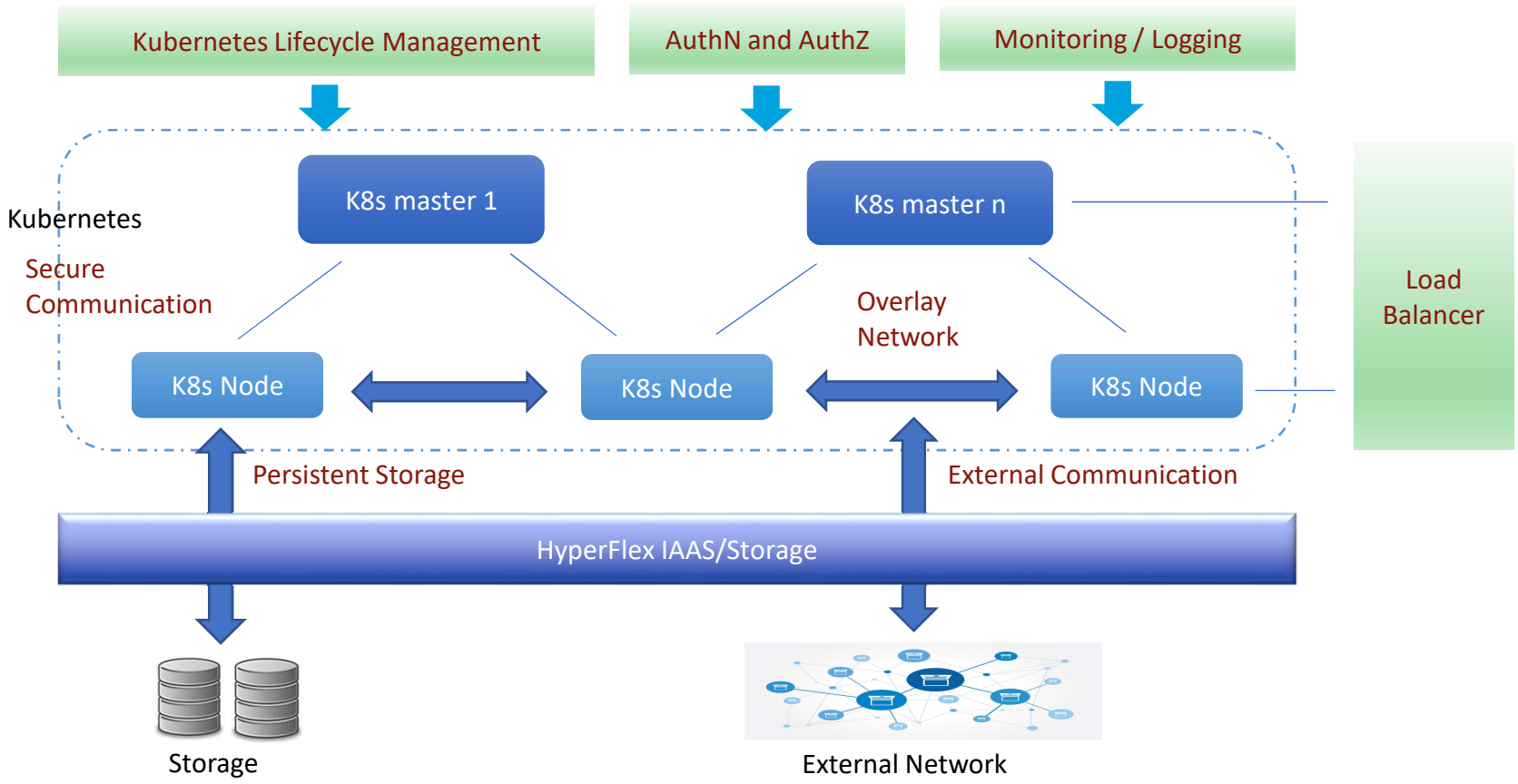
Roadmap

Cisco and Google: Best of Both Worlds

Oct 2017: Cisco's hyper-converged platform, Cisco HyperFlex, will provide a cloud-ready solution for Kubernetes and containers, and management tools to enforce security and consumption policies (Q2CY18).

Cisco	Google Cloud
Networking and Security	Cloud Services
Private Cloud Infrastructure	Microservices / Containers
Multicloud Management	API Gateway for Existing Services
Enterprise Class Sales and Support	Developer Community

Harmony Kubernetes Architecture



Nexus 9000 Container-based ISSU

- Software runs inside separate Linux container (LXC) for the supervisor and linecard
- A third container is created as part of the ISSU procedure and is brought up as a standby supervisor
- During enhanced ISSU: control plane downtime is < 3-5 seconds. No data plane traffic disruption
- Requires 16G memory on switch
- Requires switch reload when enabling enhanced ISSU for the first time
- The supervisor is upgraded first, then linecard is upgraded

CISCO