Red Hat Forum 2017
Cisco SDN pour OpenShift et sécurité des containers

Jaâfar CHRAÏBI
DevOps & PaaS Solution Architect

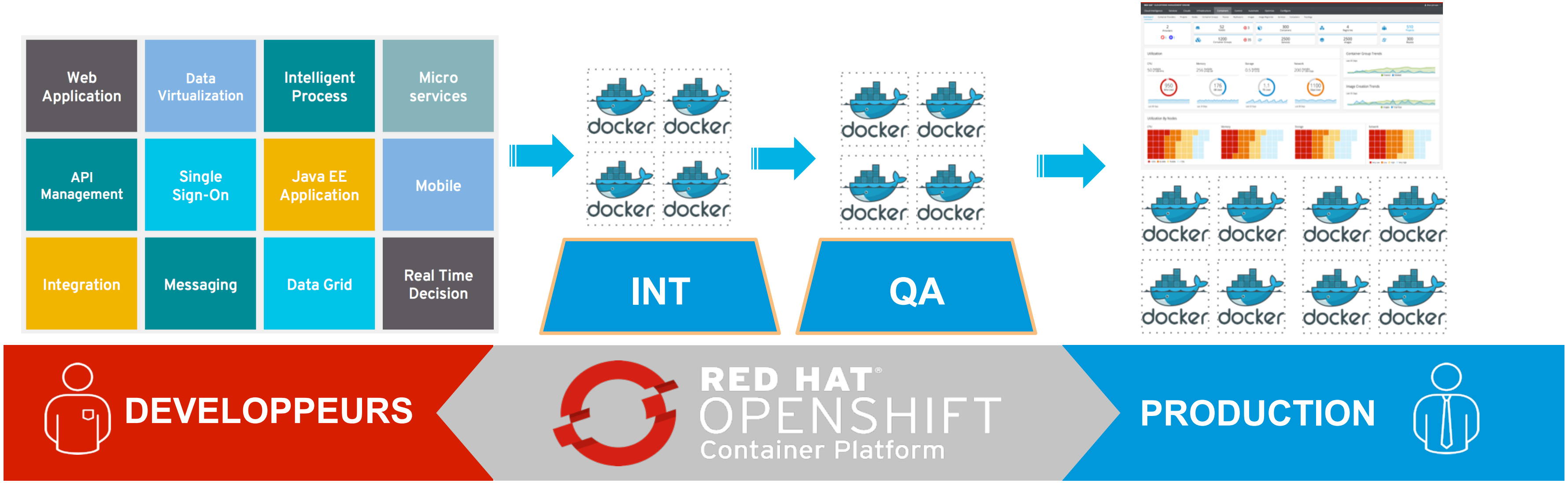
jchraibi@redhat.com

Guillaume Morini @GuillaumeMorini
Technology Solution Architect

gmorini@cisco.com

OpenShift Container Platform

Socle commun des études à la production



Web Application

Data Virtualization

Intelligent Process

Micro services

API Management

Single Sign-On

Java EE Application

Mobile

Integration

Messaging

Data Grid

Real Time Decision

INT

QA

DEVELOPPEURS

RED HAT® OPENSHIFT Container Platform

PRODUCTION

TRUE POLYGLOT PLATFORM

LANGUAGES	Java	NodeJS	Python	PHP	Perl	Ruby	.NET Core	Third-party Language Runtimes
DATABASES	MySQL	PostgreSQL	MongoDB	Redis				Third-party Databases
WEB SERVERS	Apache HTTP Server	nginx	Varnish	Phusion Passenger	Tomcat			Third-party App Runtimes
MIDDLEWARE	Spring Boot	Wildfly Swarm	Vert.x	JBoss Web Server	JBoss EAP	JBoss A-MQ	JBoss Fuse	Third-party Middleware
	3SCALE API mgmt	JBoss BRMS	JBoss BPMS	JBoss Data Virt	JBoss Data Grid	RH Mobile	RH SSO	Third-party Middleware

...and virtually any docker image out there!

CrunchyData

GitLab

Iron.io

Couchbase

Sonatype

EnterpriseDB

NuoDB

Fujitsu

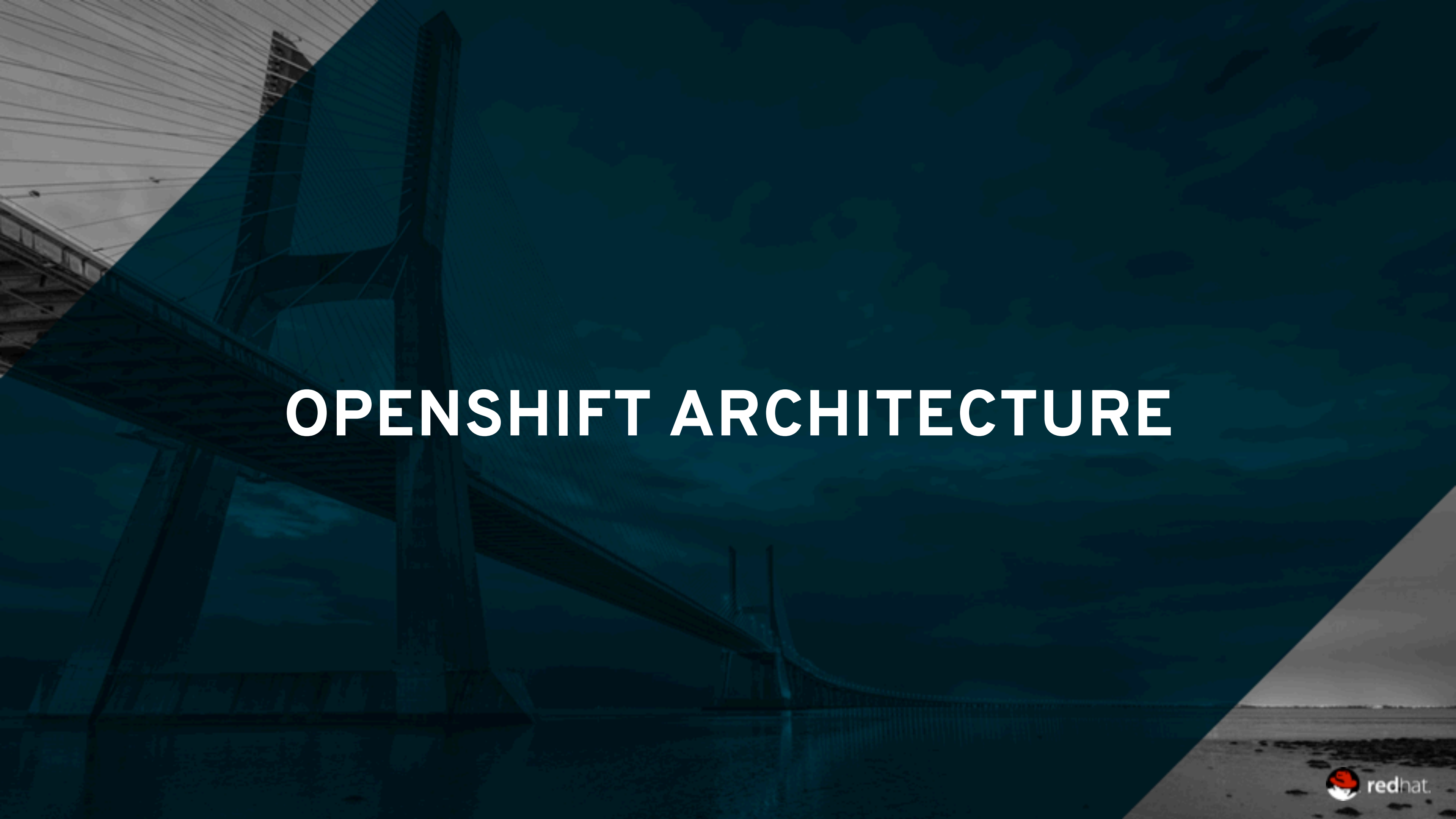
and many more

OPENSHIFT COMMONS

The community where users, partners, customers, upstream project leads and contributors come together to collaborate and work together on OpenShift.

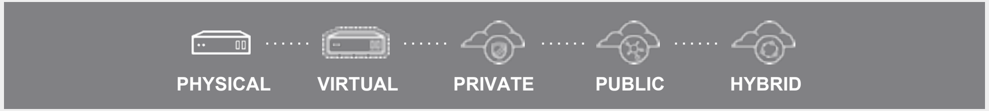
Learn more at https://commons.openshift.org

LIVEWYER kangaroot Zefflin OPENCONTRAIL SEAGATE produban FORSYTHE Iron.io electrical training redislabs Juniper RAPID transcirrus boondoc Walgreens Boots Alliance SBB CFF FFS S4 TECHNOLOGY cloudera vARMOUR EBSEMANTICS opensourcearchitect Fairfield UNIVERSITY ZTE Smals synnefo ciber NGINX OPENSHIFT StackRox mesosphere cloudsoft RAIFFEISEN INFORMATIK Datawise.io ConSol Consulting & Solutions NETENGINE hazelcast FUJITSU villamedia Couchbase ZEROTURNAROUND Hortonworks NODE4 IKANO Microsoft CRUNCHY RGen Solutions Cognizant VMTURBO On Center EUPRAXIALabs OpenCredo volk RocketBolt FEEDHENRY by Red Hat RASIA LEAVING A TRAIL DATADOG Intelligent Payments NEC UDig orange ELOS Codenvy kainos medisite ON YOUR SITE WEB RATIO Department for Work & Pensions JRebel SHADOW-SOFT ownCloud TREMOLO SECURITY ZABBIX BLACKDUCK ciber BLACKMESH CRYPTERON greenbird COLOSSEUM BIGLOBE MACROVIEW HITACHI Inspire the Next NS Solutions RHODIX thoughtbot CLOUDYLE Chuanhow Nextcloud getup KAAZING TIGERA LSD BlazeMeter KISMATIC mongoDB OUTRAIL Cognizant dynatrace EXVERSION leighton Green Peapod WIPRO worldline UOL MUDANO ContainerSolutions uakami PUZZLE ITC T-Systems rubiX COSCALE MIRACLE fedr8 NetApp NOVA Phase2 zend ThetisApps New Relic codearte TECH ANGELS IZURI IDC GitLab CITRIX SendGrid Twistlock neo4j puppet labs UC UNIVERSITY OF CANTERBURY Pega stamplay ICN.Bg Infosys CNPaaS PANTHEON USC catalyst ToMM OGIS-RI MIDDLEWARE360 OPERABLE Intelligent Payments Shippable MariaDB Skatteetaten CLOUDSSKY CloudBees OCTO Technology Unilogik ticketfly ebrc QUALICA cloudstrap NASA Symantec yeomani metabahn nuagenetworks Charter Pachyderm sapho Grid Dynamics UNIVA weave THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL cloudWerkstatt fasthosts peak 10 dreamfactory CSC NEOTYS videoNEXT ATOMIC REDAPT ITS4U L'labs



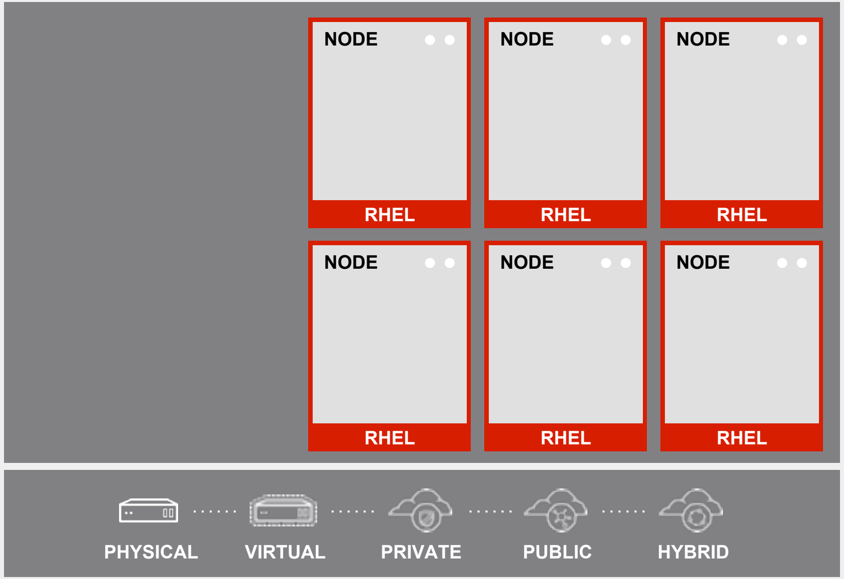
OPENSHIFT ARCHITECTURE

YOUR CHOICE OF INFRASTRUCTURE

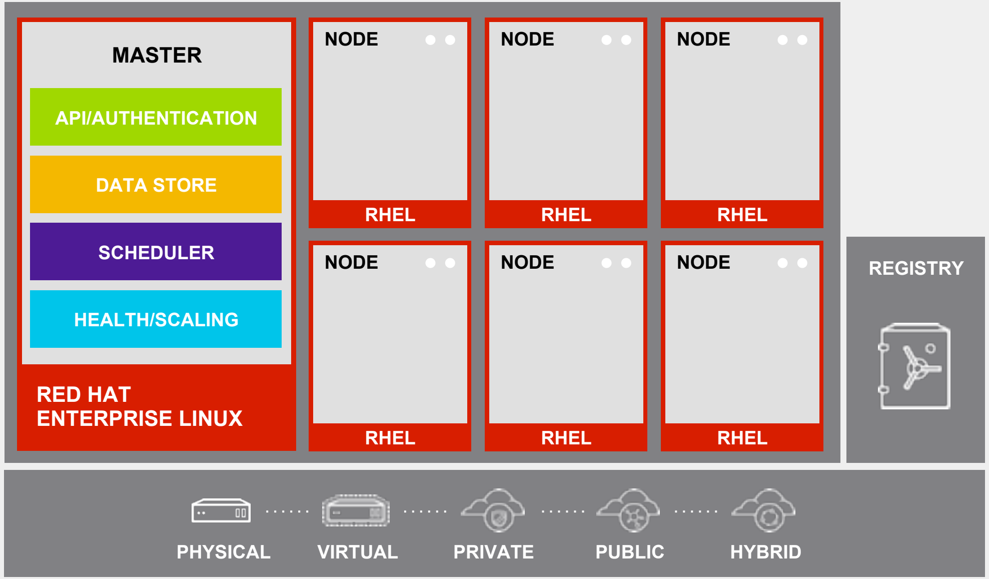


PHYSICAL VIRTUAL PRIVATE PUBLIC HYBRID

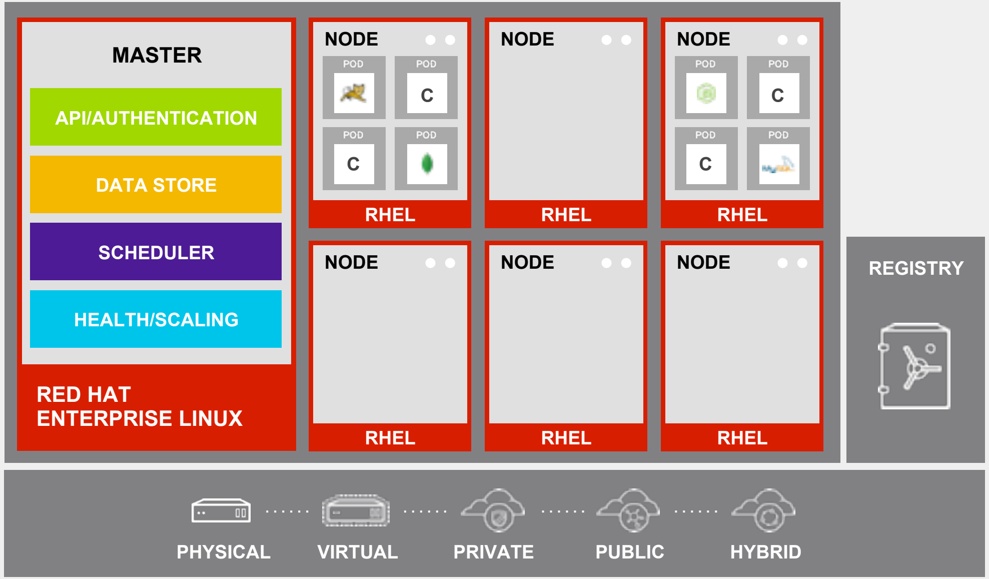
NODES RHEL INSTANCES WHERE APPS RUN



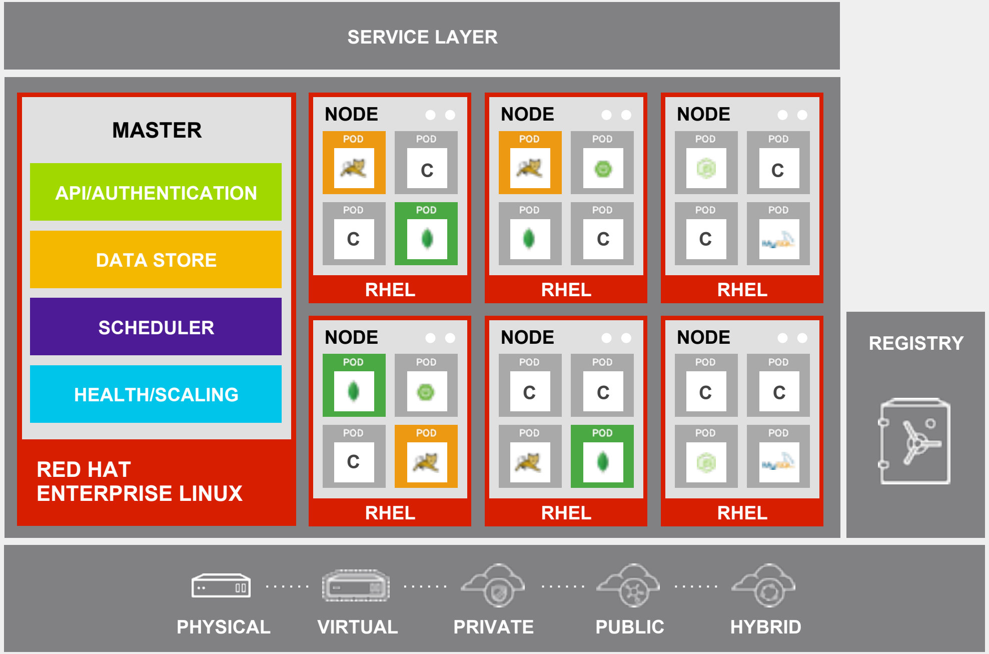
AUTOSCALING PODS



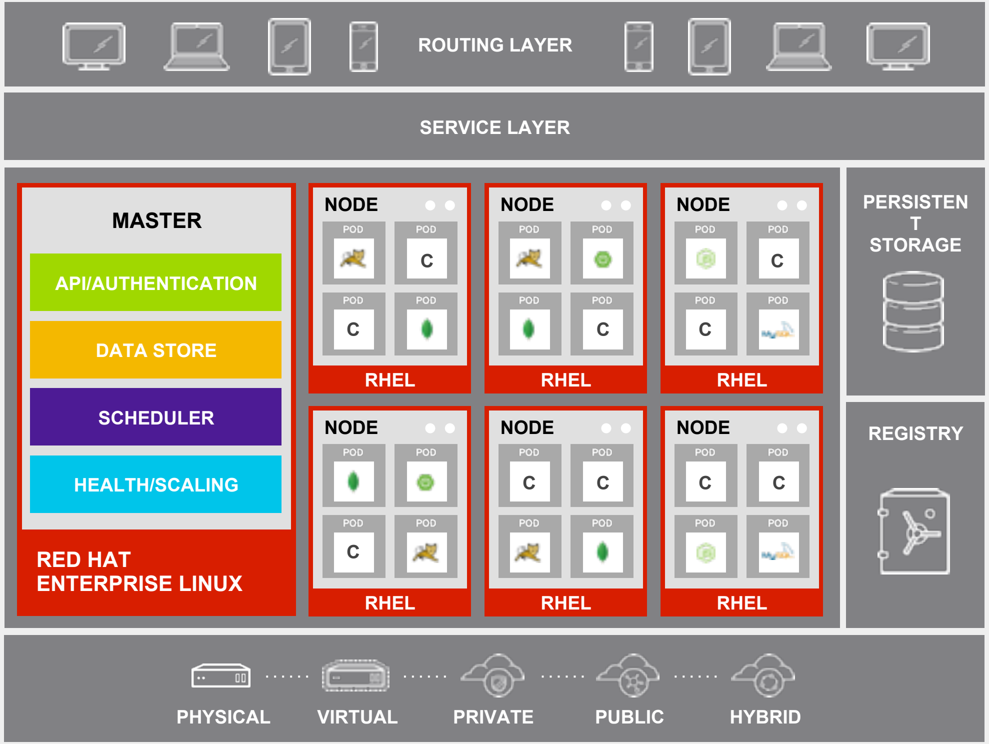
AUTOSCALING PODS



SERVICE DISCOVERY

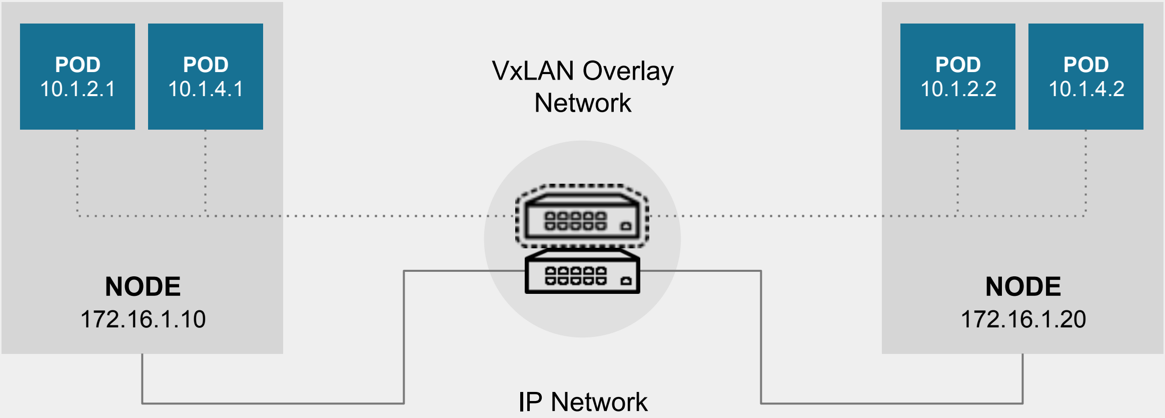


ROUTING AND LOAD-BALANCING

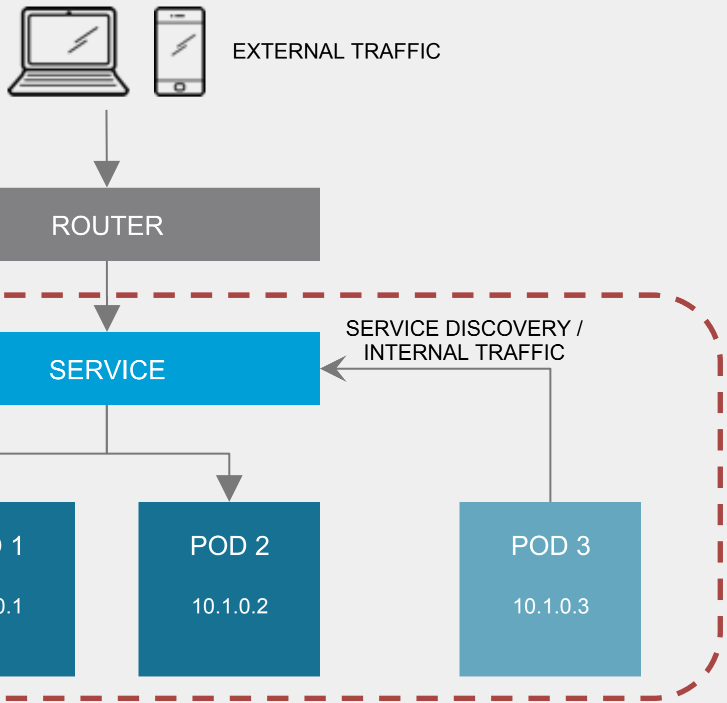


SOFTWARE DEFINED NETWORKING (SDN)

OPENSHIFT SDN

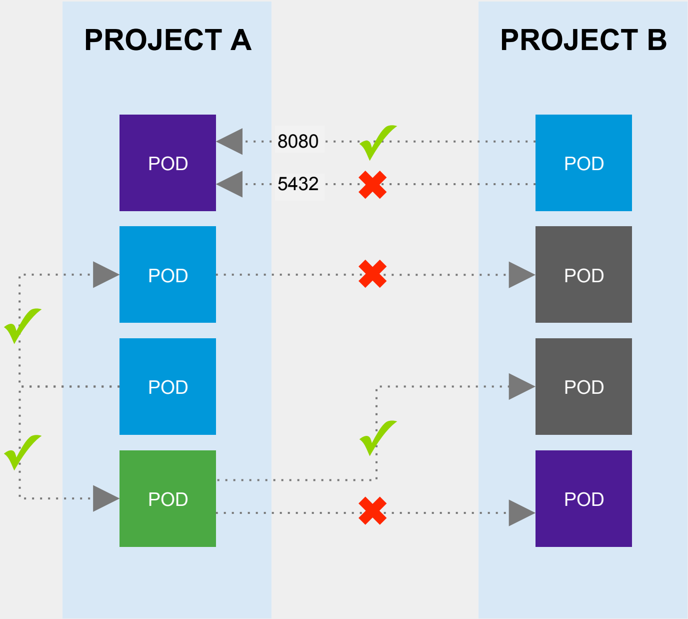


INTERNAL LOAD-BALANCING



Application
Network Isolation

NETWORK POLICIES TO CONTROL TRAFFIC



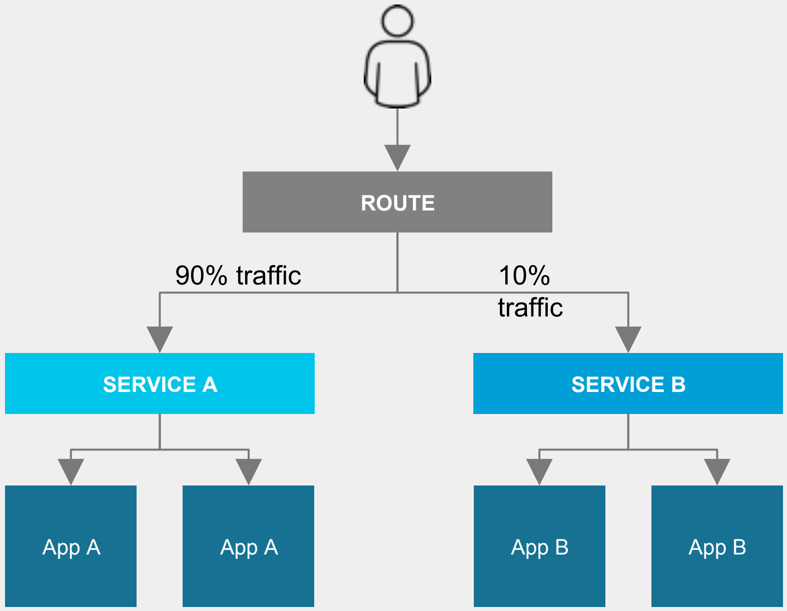
Example Policies

- Allow all traffic inside the project
- Allow traffic from green to gray
- Allow traffic to purple on 8080

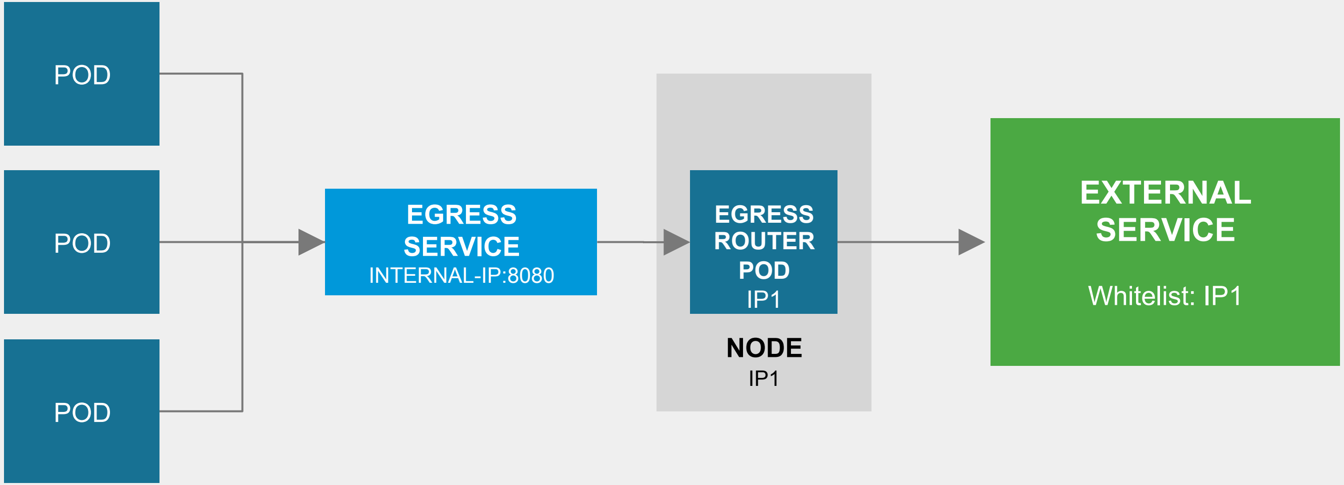
```
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: allow-to-purple-on-8080
spec:
  podSelector:
    matchLabels:
      color: purple
  ingress:
  - ports:
    - protocol: tcp
      port: 8080
```

ROUTE SPLIT TRAFFIC / AB Testing

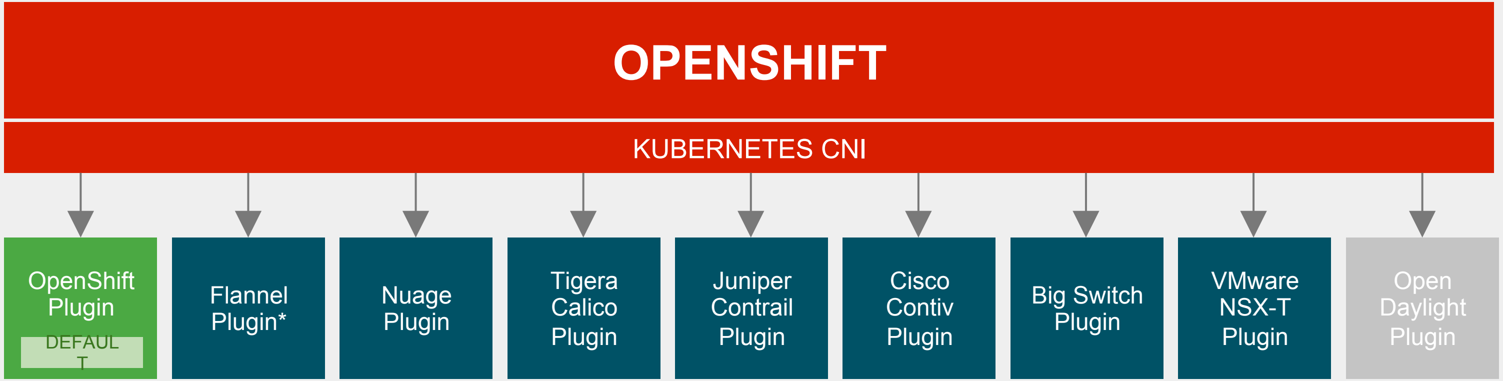
Split Traffic Between Multiple Services For A/B Testing, Blue/Green and Canary Deployments



OUTGOING TRAFFIC - CONTROL SOURCE IP WITH EGRESS ROUTER



OPENSHIFT NETWORK PLUGINS



OPENSHIFT

KUBERNETES CNI

OpenShift Plugin DEFAUL T

Flannel Plugin*

Nuage Plugin

Tigera Calico Plugin

Juniper Contrail Plugin

Cisco Contiv Plugin

Big Switch Plugin

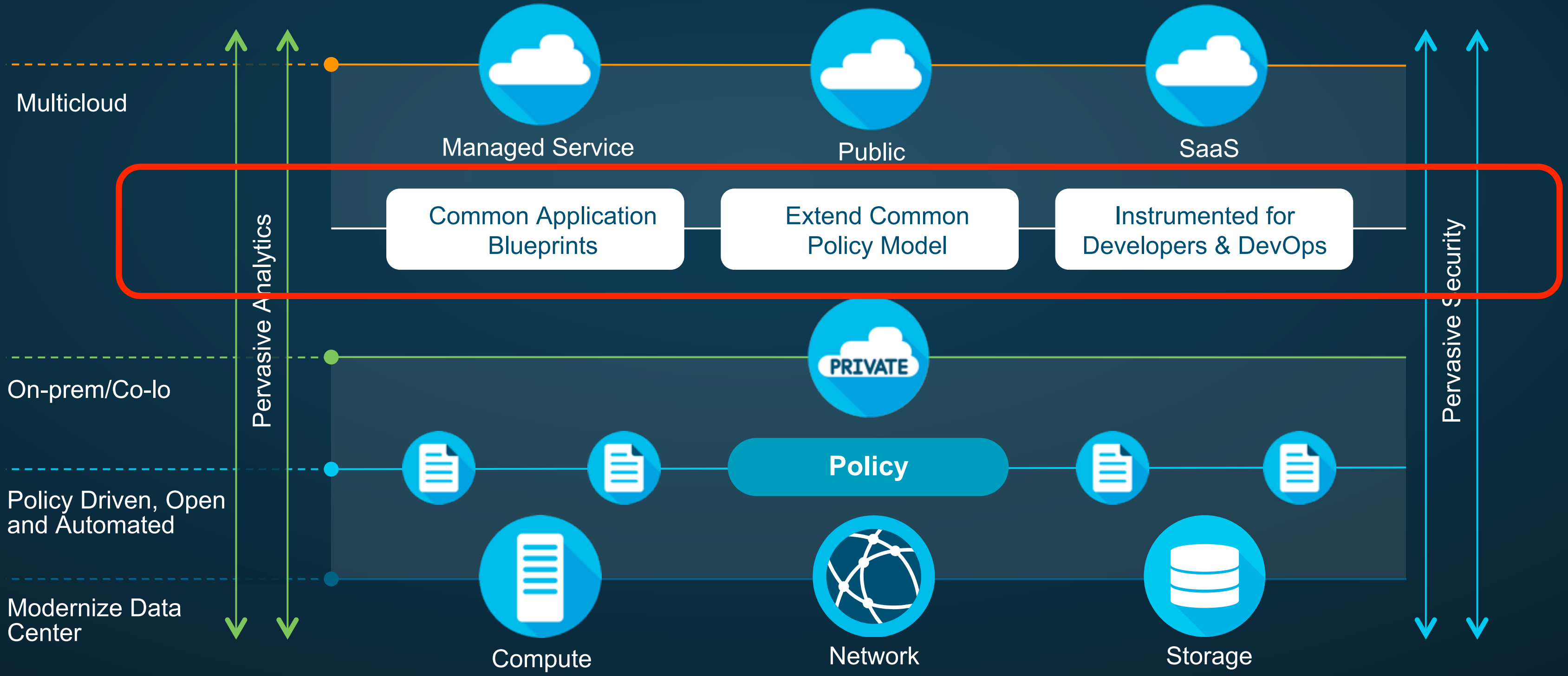
VMware NSX-T Plugin

Open Daylight Plugin

Certified Plugin | Validated Plugin | In-Progress

* Flannel is minimally verified and is supported only and exactly as deployed in the OpenShift on OpenStack reference architecture

Multicloud: The Customer Intent



This is an “AND” Story

- AppD
- CloudCenter
- Tetration
- Security
- Starship
- ACI

Compute

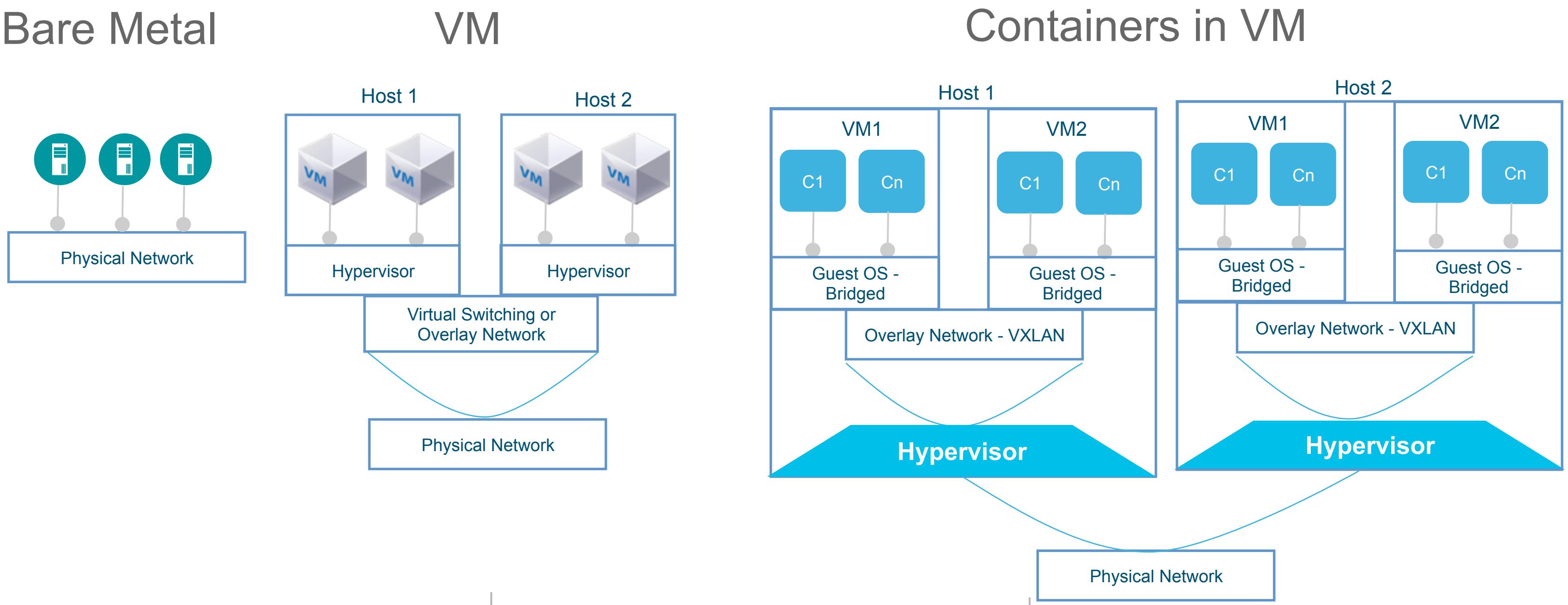
Network

Storage

Cisco
Data Center
$10B+
In FY17

What about containers & networking ?

Networking In The New Container World



✘ Connectivity

Network services, e.g. Load balancer, Firewall

✘ Performance

Encap over encap over encap affects performance

✘ HW Integration

Can not leverage performance and security by natively integrating with HW

Cisco’s Approach to Containers Networking & Security

Scale

Route and Policy Distribution

Speed

Automated Scale-out

Layer of Network

Flat Networks
High Performance

Application Centric

Integrated with App Blueprint

Shared Resources

Policies for Resource Acquisition

Hybrid Cloud

Consistent Policies

Security

Tenant Isolation
Security Policies

Telemetry /Diagnostics

Application Statistics
Data Export

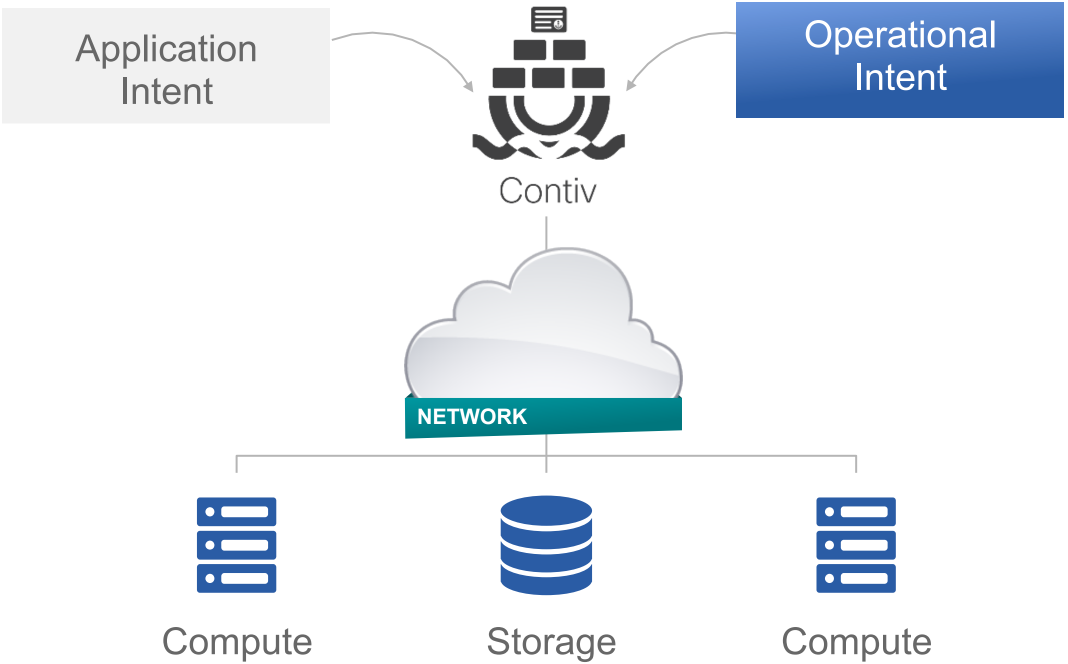
How can we achieve these goals?

Key: Policy-based Container Networking

Declarative Tags (simpler)

Manage Groups instead of single objects (faster)

Cisco Enables Running Containerized Apps in Production Mode in a Shared Infrastructure



Contiv Is an Open Source Solution to Define and Enforce Distributed Policies Across Infrastructure

Application Intent with Operation Intent

App Intent

```
version: '2'
services:
web:
    build: .
    label:
          - tier: web
     volumes:
                - .:/code
     networks:
          -    front-tier
          -    back-tier
db:
   image: mysql
```

Ops Intent (e.g. Contiv Intent*)

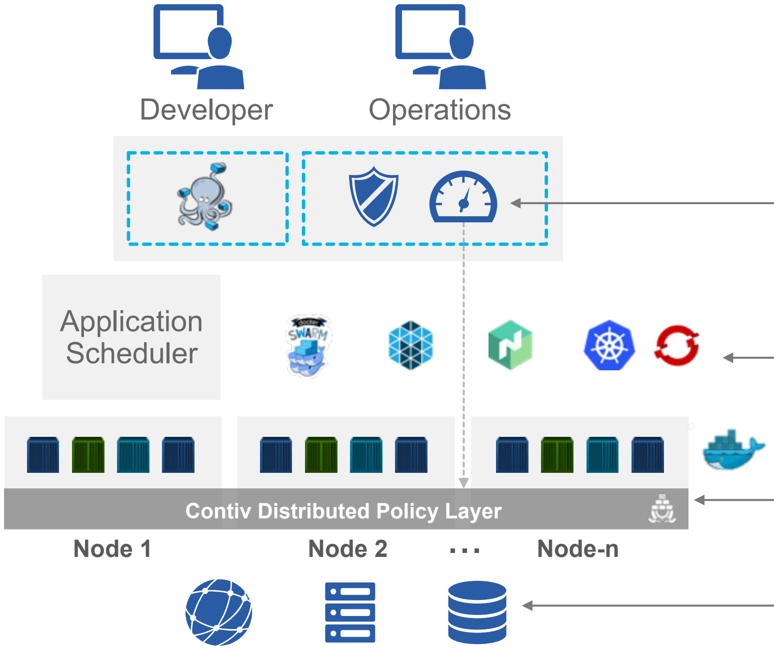
```
web:
  environment: prod
  networks:
    security: -
      allow ports: 5000, 443
    bandwidth: 5gbps
    lb selector:
           - tier: web
 db:
  networks:
    security:
     allow ports: 3306 from web
  volumes:
       pool:  SSD
       IOPS:  10000
```

* Shown in yaml for better visualization

Operation Intent Provides Operational Requirements and Policies for Applications

Contiv Architecture

Operational Policy Management



Contiv Elements

Contiv UI to manage/ monitor policies/usage

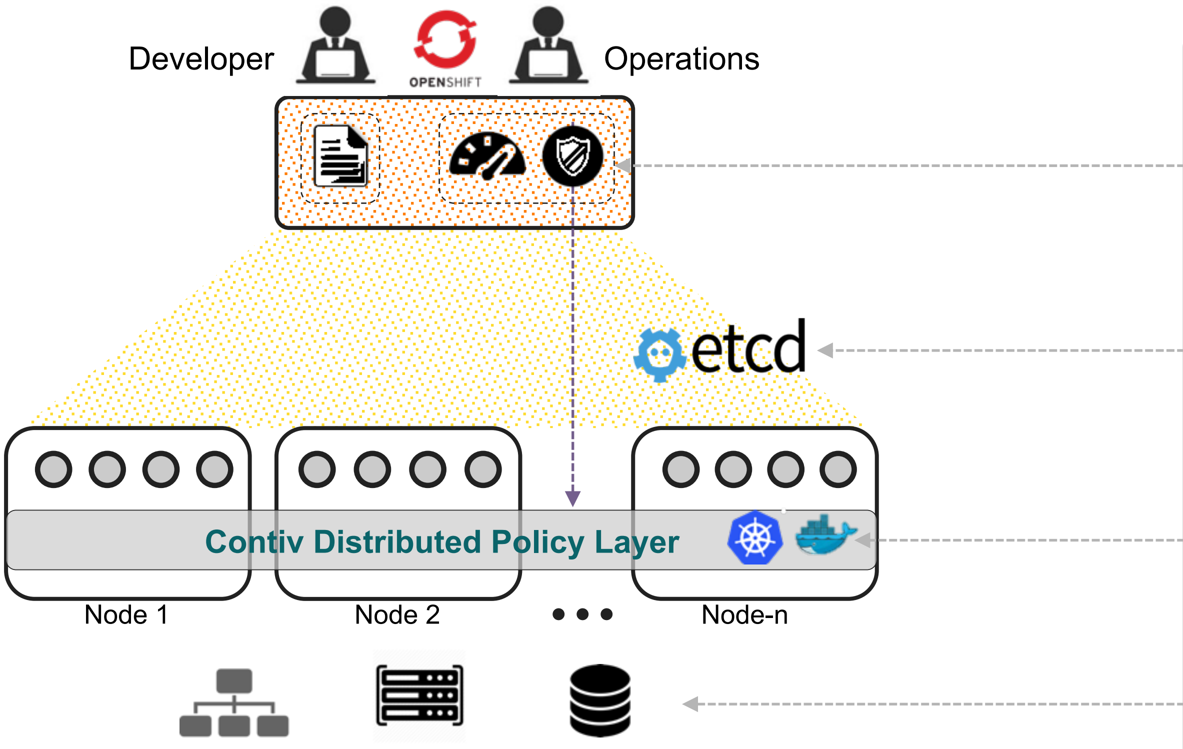
Integrated with popular container schedulers

Distributed policy enforcement for compute, network, and storage

Integration with physical infrastructure

Contiv Automatically Integrates and Enforces Developer and Operations Policies

Contiv Openshift – Integration Points



Contiv Elements

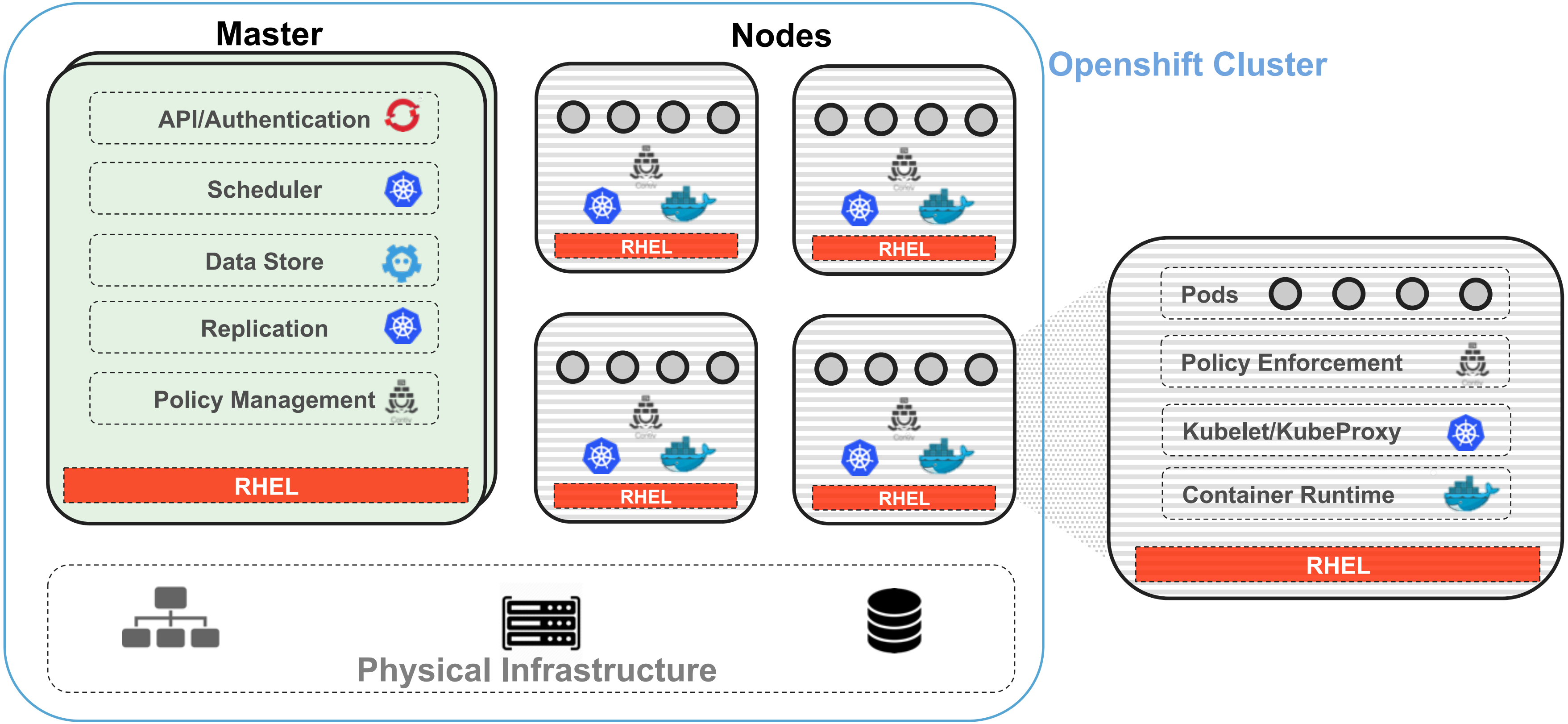
Contiv Ux to Manage/Monitor Policies/Usage

Contiv Policy Distribution using state store

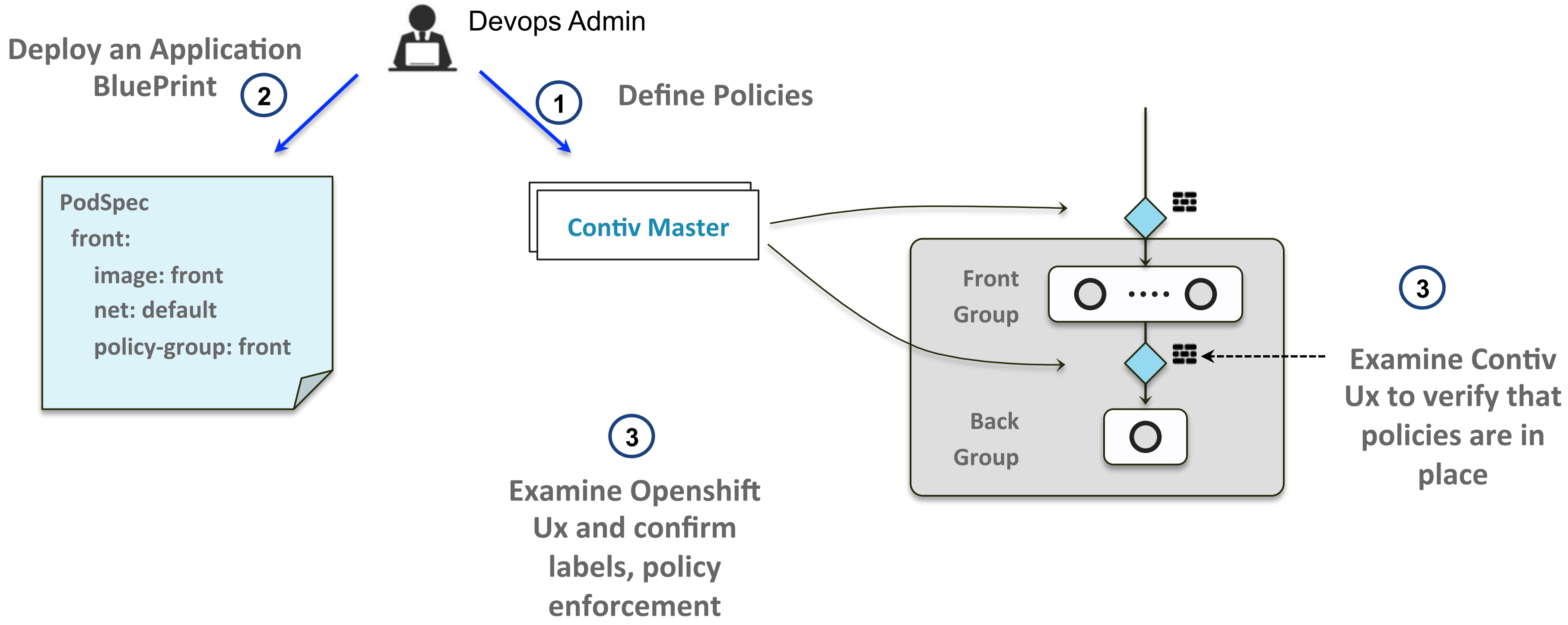
Policy Enforcement for compute, network and Storage

Integration with Physical Infrastructure (Nexus/ACI/UCS)

Contiv Openshift Integration



Security Policy - Steps



Devops Admin

Deploy an Application BluePrint

2

1

Define Policies

```
PodSpec
  front:
     image: front
     net: default
     policy-group: front
```

Contiv Master

3

Examine Openshift Ux and confirm labels, policy enforcement

3

Examine Contiv Ux to verify that policies are in place

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)

Microservices
Load Balancing

Integrated IPAM,
Service Discovery

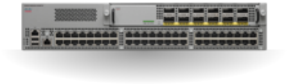
Performance and Scale

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

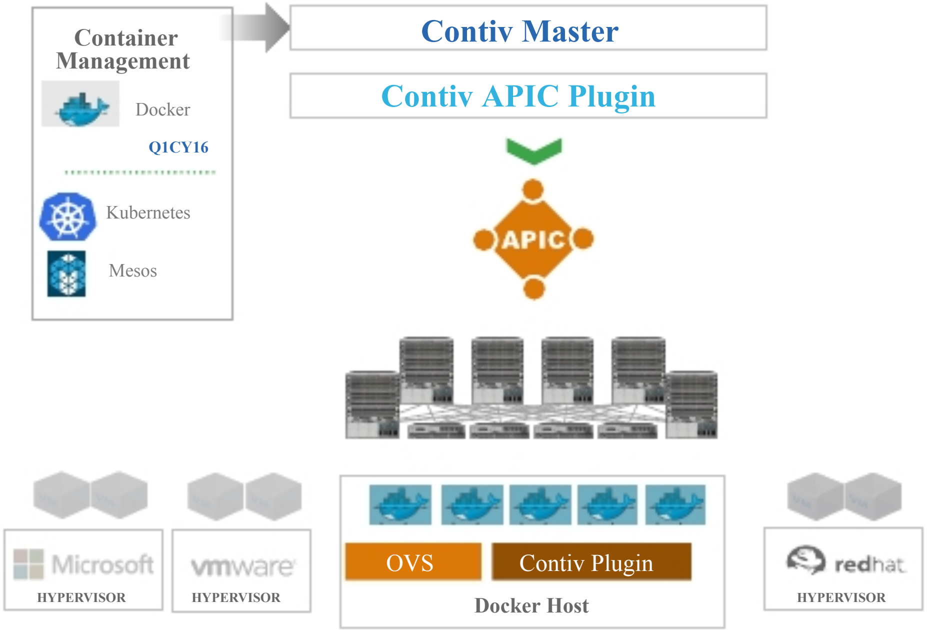
- BGP interop (standard routing protocol)
- EVPN-based multi-tenancy and automation

Unified Compute Systems: B and C Series

- Leveraging vNICs for control, data, management, and storage traffic
- NIC Offload function (future)

Contiv Leverages Underlying Infrastructure Capabilities for Applications

Cisco ACI + Contiv



Project Contiv

- Open source project for defining operational policies for container deployment
- Includes Docker networking plugin and APIC API integration

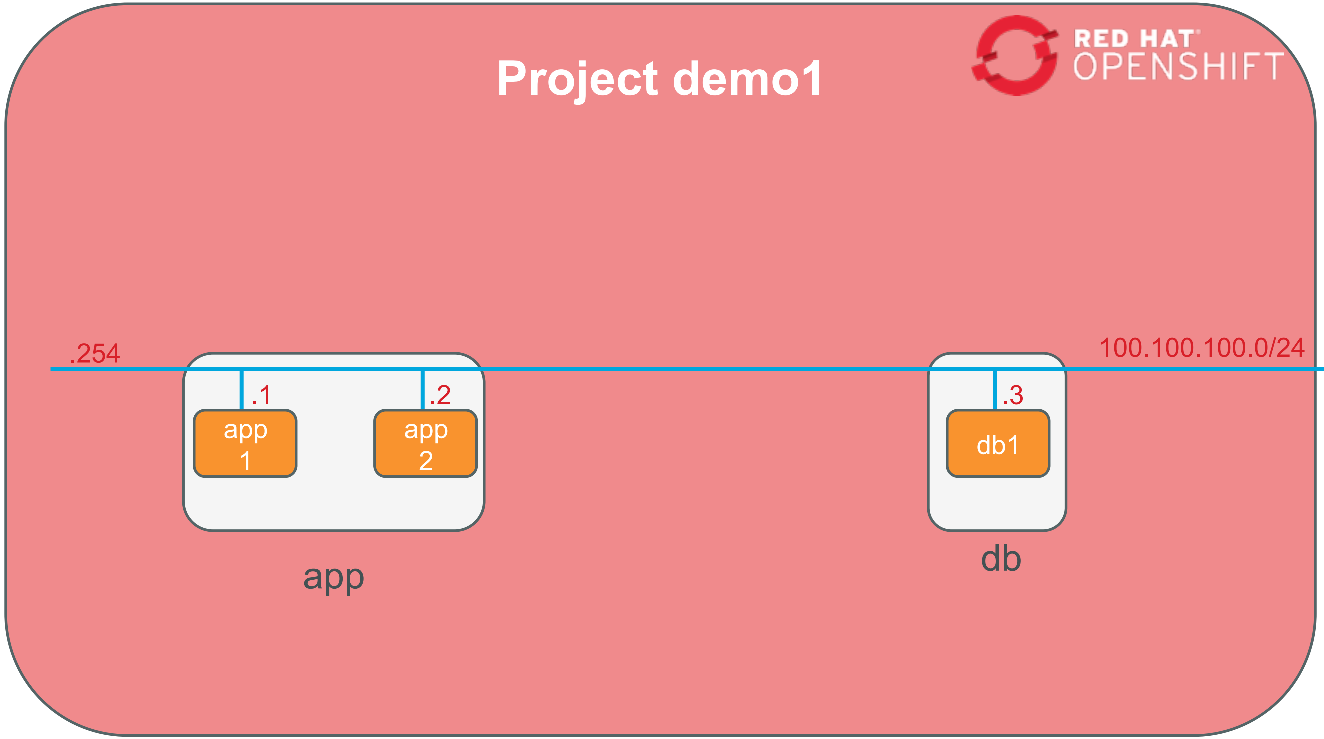
Solution Highlights

- ACI policies can be extended across physical, virtual machines, and Docker containers
- Open source Project Contiv can be used to integrate Docker containers with ACI

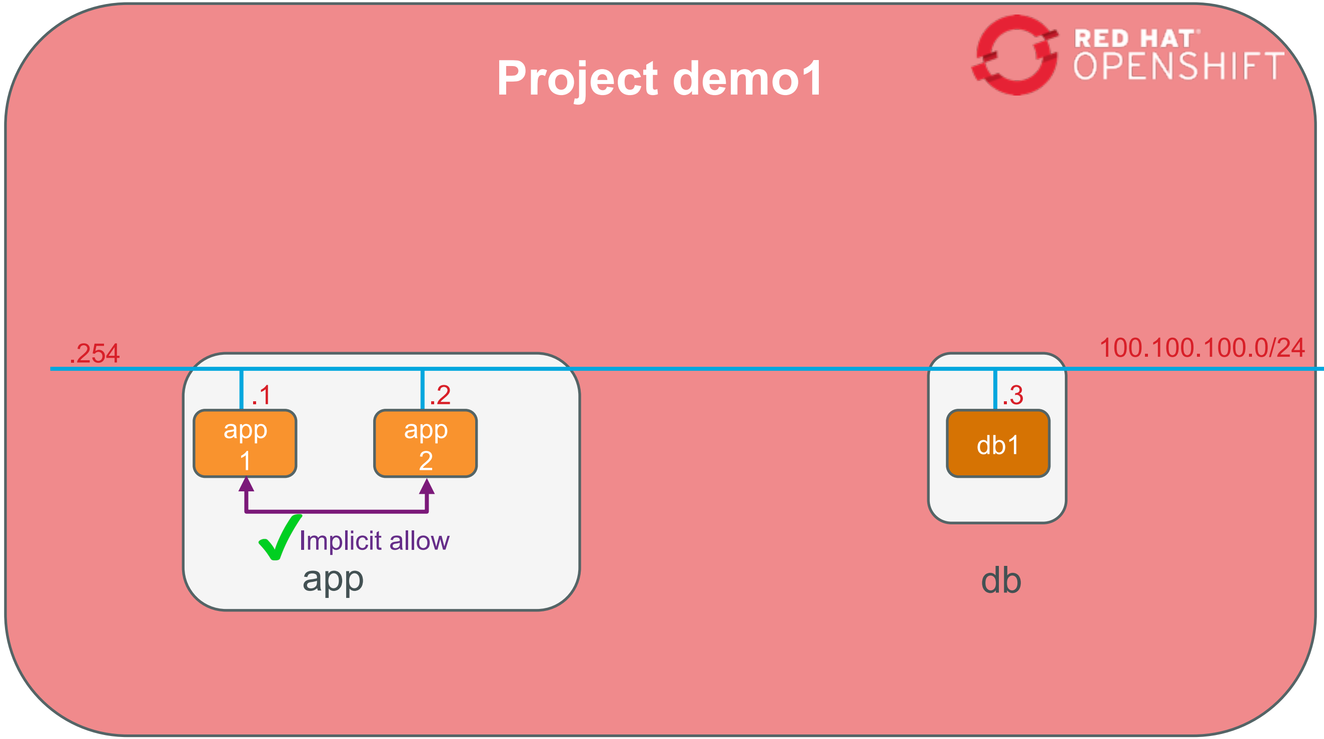
Unified Policy Automation and Enforcement Across Physical, Virtual, and Containers

Démo

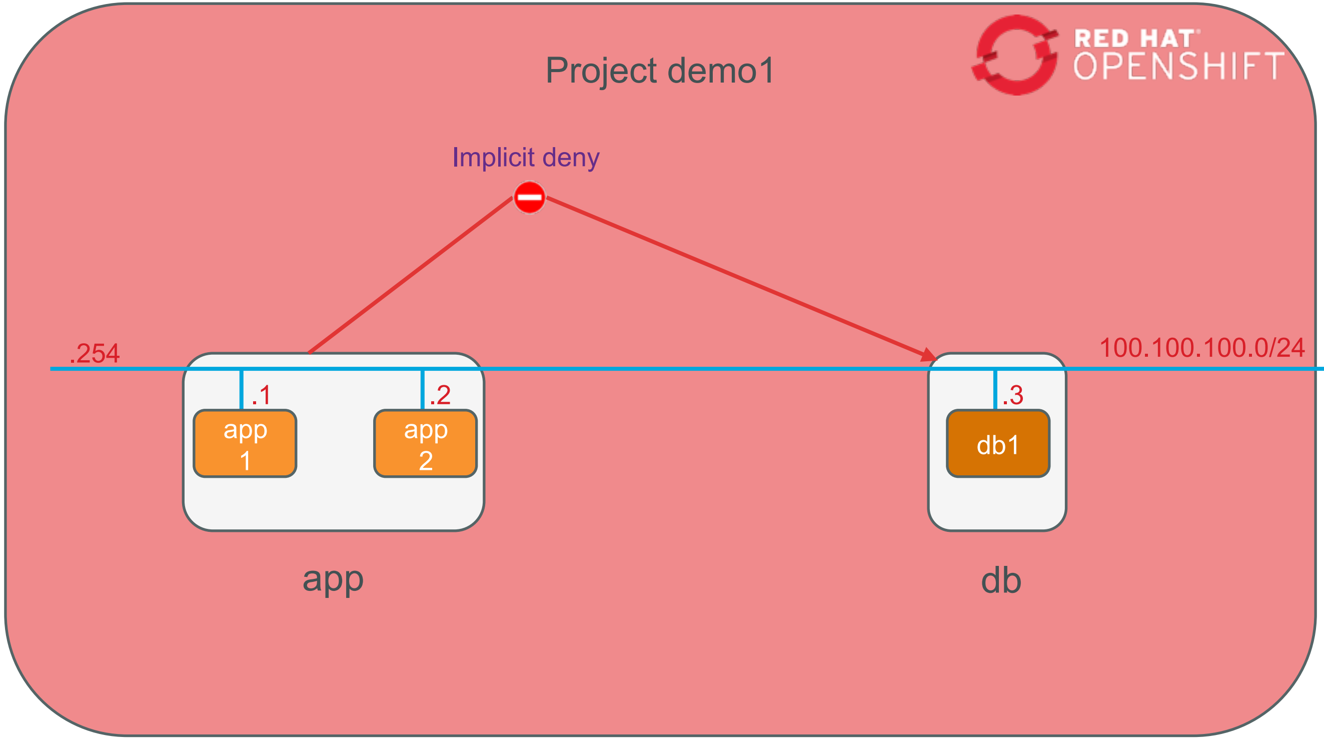
Démo:
initial setup



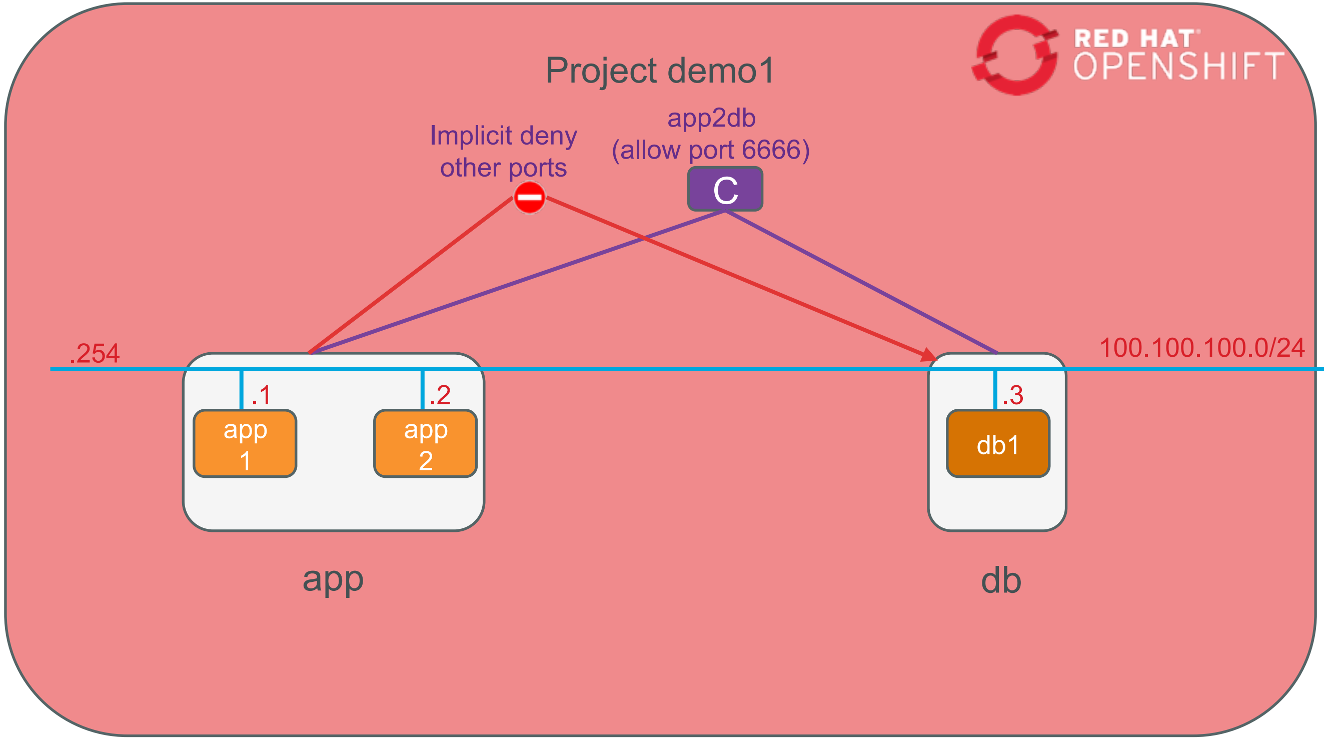
Démo:
Inter pods communications in a group



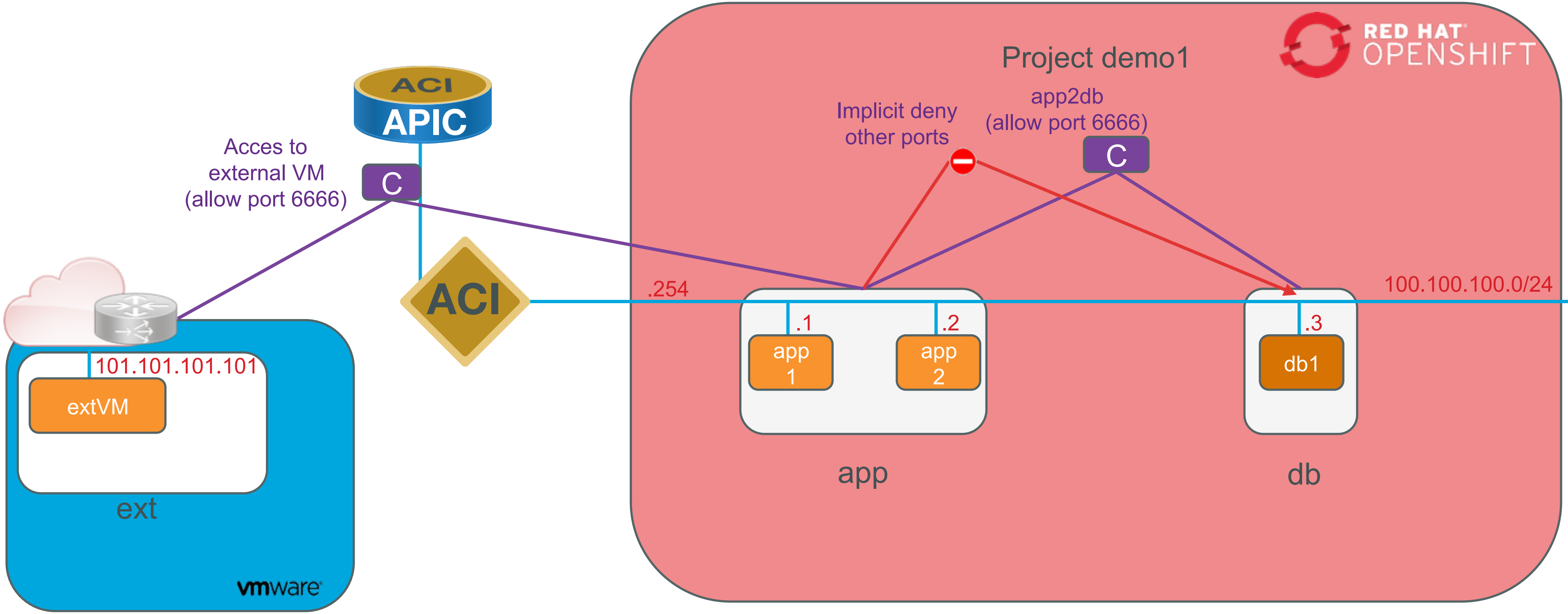
Démo:
Inter pods communications between groups



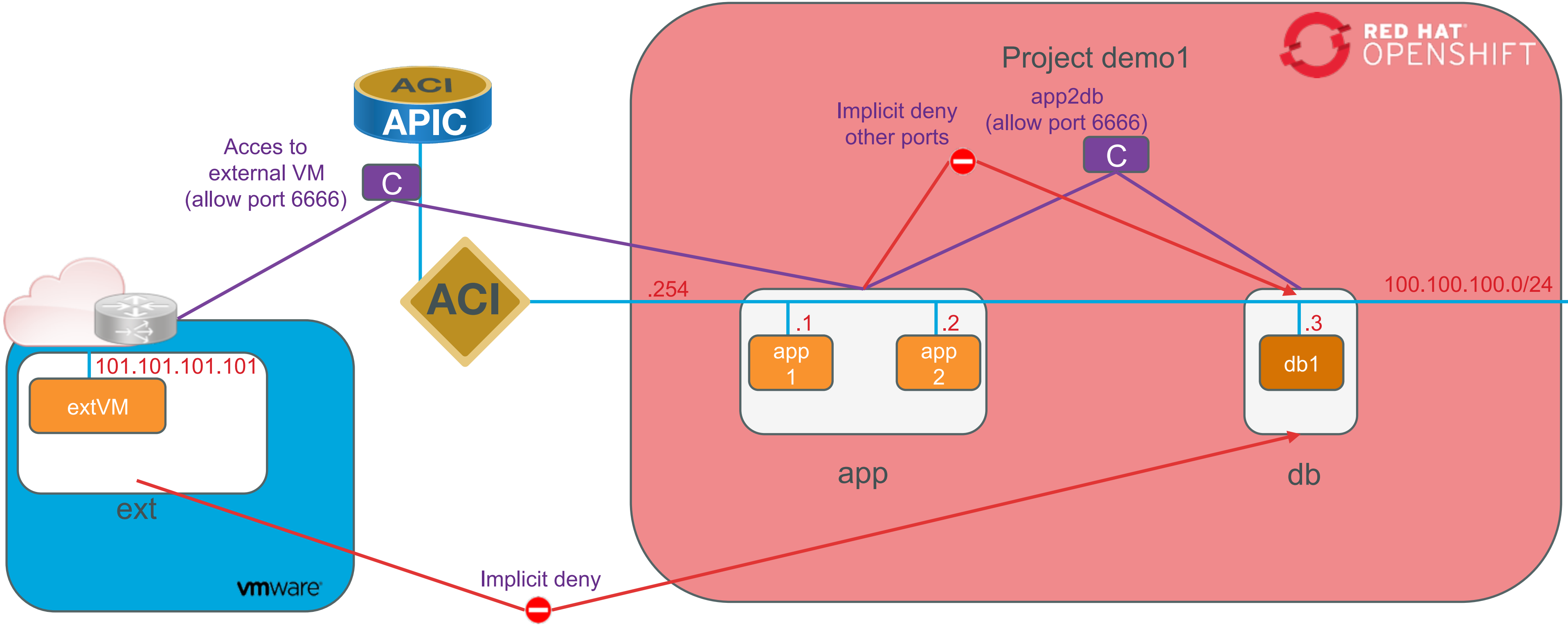
Démo
Inter pods communications between groups



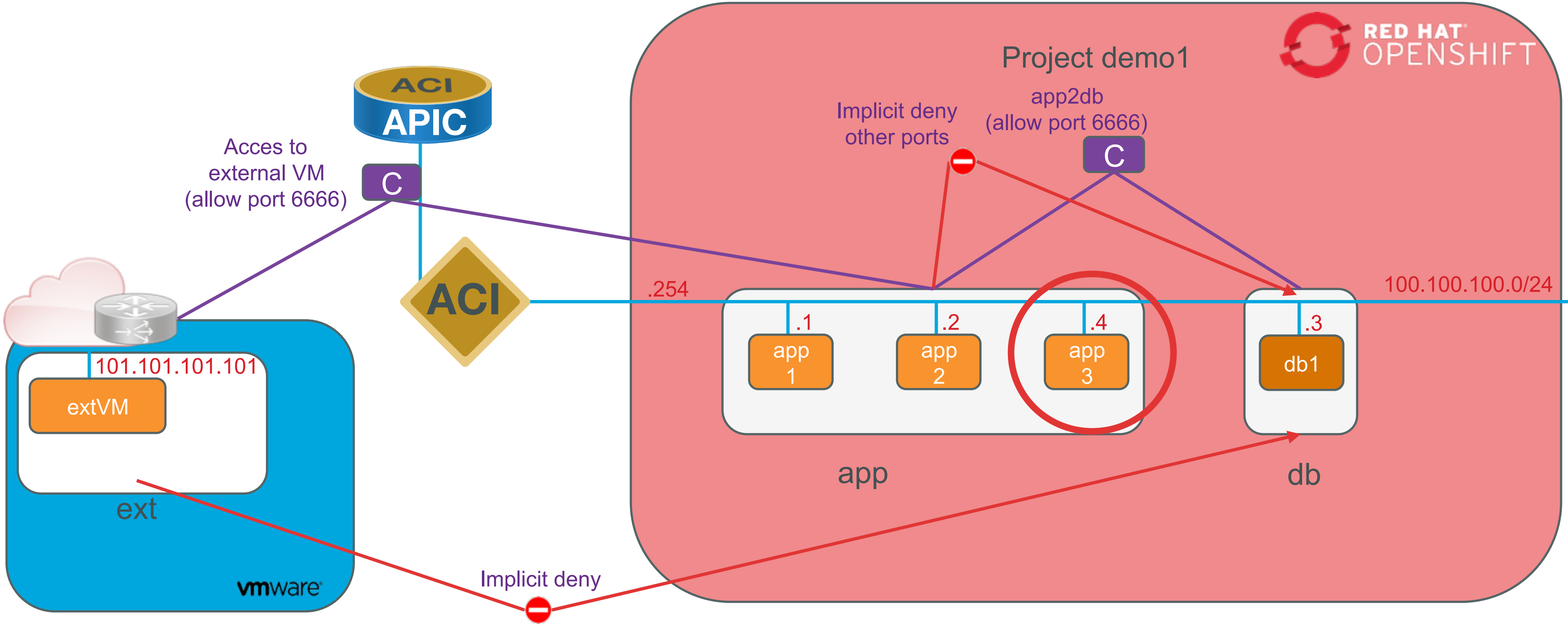
Démo
Pods communications outside of OpenShift

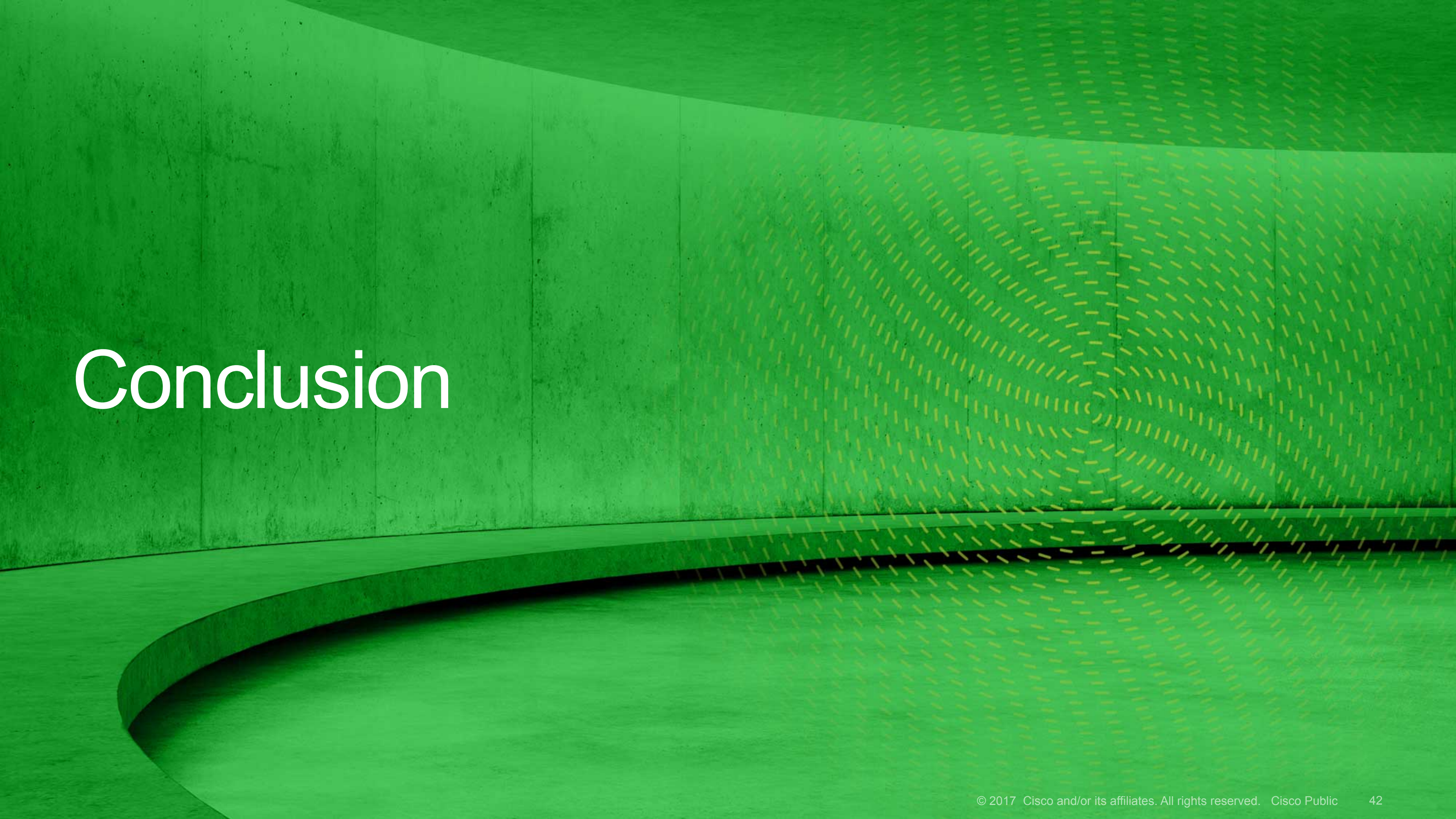


Démo
Pods communications outside of OpenShift



Démo
Add a pod and inherit connectivity

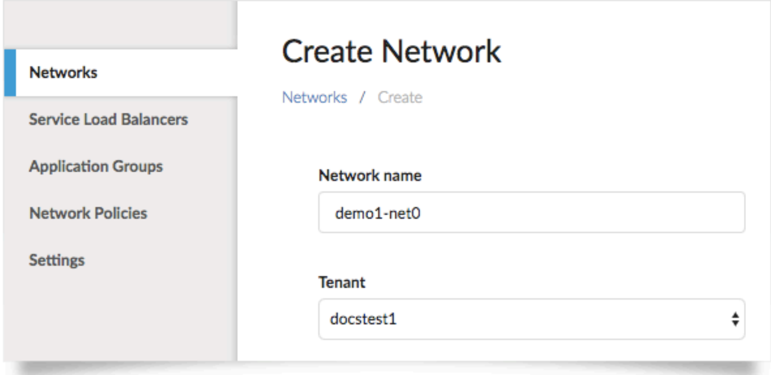




Conclusion

Contiv Value Proposition

Manage Container Networks



Create Network

Network name: demo1-net0

Tenant: docstest1

Why Contiv

Contiv unifies containers, VMs, and bare metal with a single networking fabric, allowing container networks to be addressable from VM and bare-metal networks.

Contiv combines strong network performance, support for industry-leading hardware, and an application-oriented policy that can move across networks with the application.

Rich Policy Framework

Set bandwidth and isolation policies in a multi-tenant environment.

Multi-Platforms

Docker, Kubernetes, OpenShift and more.

Multi-Infrastructure

VMs, containers, and bare metal.

Enterprise Grade

Rigorously tested for the cloud.

Networking Support

Layer 2, Layer 3, BGP, ACI

Open Source

Contiv is available through the Apache 2 License and our code is available on GitHub.

Contiv 1.0

What's New:

LDAP+ RBAC

All New User Experience and Workflow

Kubernetes Support

Docker Swarm Support

OpenShift Integration

Simple Install

Commercially Supported Contiv

Cisco Advanced Services Installation

Cisco Solutions Support

Go and test it (easy!): http://contiv.github.io

Contiv

The Most Powerful

Open Source Container Networking

Join Contiv Slack - **contiv.herokuapp.com**

Devnet Sandbox on Contiv and Kubernetes – http://cs.co/contiv

Come to see us on Cisco booth

Modules officiels Ansible pour infra. & réseau

Openstack : SDN / Pod

SDN pour Openshift (Contiv)

UCS 3260 & CEPH

AppDynamics

SAP HANA on RHEL

NFV (FD.io / VPP)

SDN pour RHEVM

redhat.

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos