

<u>IIIO</u>

## Plataformas com possibilidades ilimitadas

## Lisboa

23 de Maio de 2024



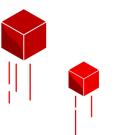
# Red Hat OpenShift Virtualization

Carlos Cornejo

Senior Architect

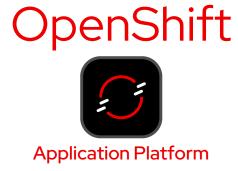
Sérgio Seabra

**Senior Solutions Architect** 





## What we'll discuss today



Modern Platform for Application Development and Deployment across the hybrid cloud.

## Virtualization



#### **Containers and VMs**

Single pane of glass. VMs can benefit from kubernetes. Lower barriers for modernization.



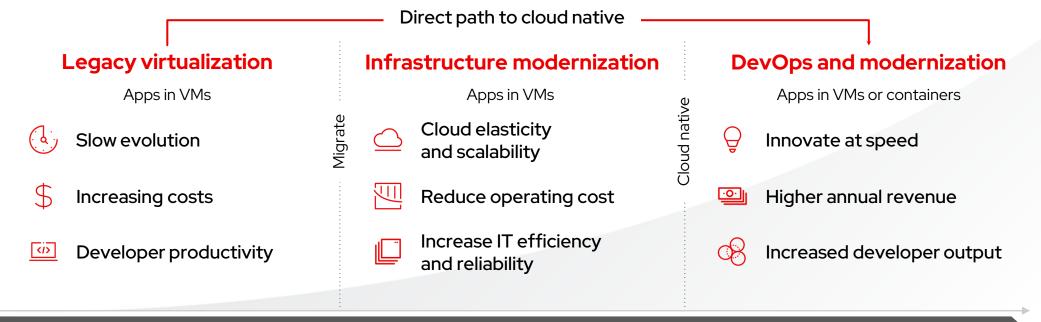
Warm migration of VMs at scale. Network and Storage mapping. From vSphere, RHV or OpenStack.





## Modernize at your own pace

(and only as much as you want)

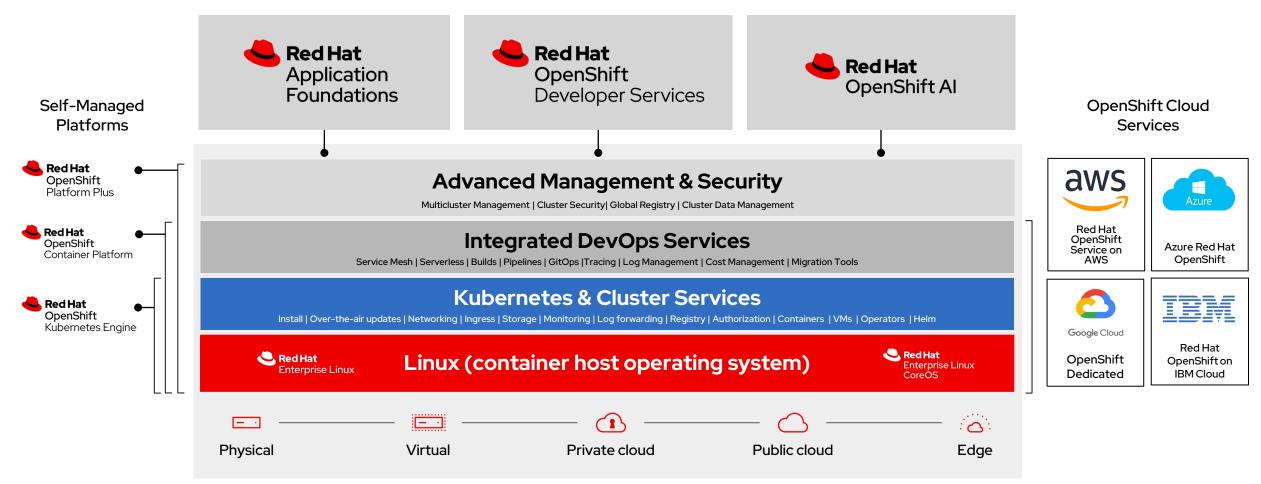


Speed of Infrastructure Deployment | Speed of Application Development





### Red Hat open hybrid cloud platform





## **OpenShift Virtualization**



Modernize workloads, bring VMs to Kubernetes

#### Enterprise Virtualization Enhancements

- Windows 11, 201x and RHEL 9 Guest Support
- Intuitive UI for VM admins
- Robust applications with *RHEL High Availability*

#### VMs and Containers in Private/Hybrid Cloud

- Provide self-tuned VM instances
- RBAC control on VM templates
- Easily share vGPU w/ NVIDIA operator

#### Ensure continuity of business critical applications.

- OpenShift Data Foundation / ACM Metro-DR
  - Support recovery of virtual machines

#### **Proven Performance**

 Large Scale Tuning and Performance whitepaper

<b>Overview</b> Mor	nitoring Settings				
	itering outings				
	77		364	4564	23,540 Storage (TiB)
	Machines		'U usage	Memory (MiB)	
.ast 7 days' trend		Last 7 days' trend		Last 7 days' trend	Last 7 days' trend
<sup>.5k VM:</sup> Aug 10, 2022 500	2, 4:28:38 PM	2.5k vCPU -	1	5k MiB	24k TiB
0 VMs		0 vCPU		О Мів	O TIB
Aug 31	Sept 3 Today	Aug 31	Sept 3 Today	Aug 31 Sept 3 Today	Aug 31 Sept 3 Tod
Alerts (4)				View all	Show virtualization health alerts 🔹
0 1 Critical	2 Warning 01 Info				
Critical alerts 1					
<ul> <li>Jul 3, 2022, 10</li> <li>Jul 3, 2022, 10</li> </ul>					View deta
VM etcdGR etcd cluster "e Warning alerts 2	PCRequestsSlow etcd":99th percentil of gRP	C requests is 0.429999	199999999995s on etcd inst	ance 10.35.141:9979.	View deta
VM etcdGR etcd cluster "e	PCRequestsSlow etcd":99th percentil of gRP	C requests is 0.429999	199999999995s on etcd inst	ance 10.35.141:9979.	View deta
VM etcdGR etcd cluster "e Warning alerts 2	IPCRequestsSlow	C requests is 0.429999	199999999995s on etcd inst	ance 10.35.141:9979. VirtualMachines by template	View deta
VM     etcdGR       etcd cluster "etcd     etcd       Warning alerts     2       Info alerts     1	IPCRequestsSlow	C requests is 0.429999	19999999995s on etcd inst		View deta
VM etcdGR etcd cluster "e Warning alerts 2 Info alerts 1 VirtualMachine s	IPCRequestsSlow etcd":99th percentil of gRP				View deta
VM etcdGR etcd cluster "e Warning alerts 2 Info alerts 1 VirtualMachine s	PCRequestsSlow etcd*:99th percentil of gRP statuses ctatuses Running	@ 7	<del>ن</del> 7	VirtualMachines by template	View deta
VM etcdGR etcd cluster "e Warning alerts 2 Info alerts 1 VirtualMachine s 0 1 Error Additional statuses	PCRequestsSlow atcd*:99th percentil of gRP statuses 2 1048 Running		نۍ 7 Migrating	VirtualMachines by template	177
VM etcdGR etcd cluster "e Warning alerts 2 Info alerts 1 VirtualMachine s 0 1 Error Additional statuses	PCRequestsSlow atcd*:99th percentil of gRP statuses 2 1048 Running 5 ;2 10	⊕ 7 Paused	:) 7 Migrating * ;) 7	VirtualMachines by template	177
VM etcdGR etcd cluster "e Warning alerts 2 Info alerts 1 VirtualMachine s 0 1 Error Additional statuses	PCRequestsSlow atcd*:99th percentil of gRP statuses 2 1048 Running		نۍ 7 Migrating	VirtualMachines by template	1777 VMs
VM etcdGR etcd cluster "e Warning alerts 2 Info alerts 1 VirtualMachine s 0 1 Error Additional statuses ; 2 83 Provisioning	PCRequestsSlow atcd*:99th percentil of gRP statuses 2 1048 Running 5 ;2 10	⊕ 7 Paused	:) 7 Migrating * ;) 7	VirtualMachines by template	1777 /Ms 100 rhel8-highperformance-large
VM etcdGR etcd cluster "e Warning alerts 2 Info alerts 1 VirtualMachine s 0 1 Error Additional statuses	PCRequestsSlow atcd*:99th percentil of gRP statuses 2 1048 Running 5 ;2 10	⊕ 7 Paused	:) 7 Migrating * ;) 7	VirtualMachines by template	1777 VMs



## Migration Toolkit for Virtualization

Bringing traditional virtual machines into OpenShift

#### **Migration tooling**

- Migration Toolkit for Virtualization (MTV)
- Warm and parallel migration of VMs at scale
- VM Validation
- Network and Storage mapping
- Comes free with OpenShift Virtualization

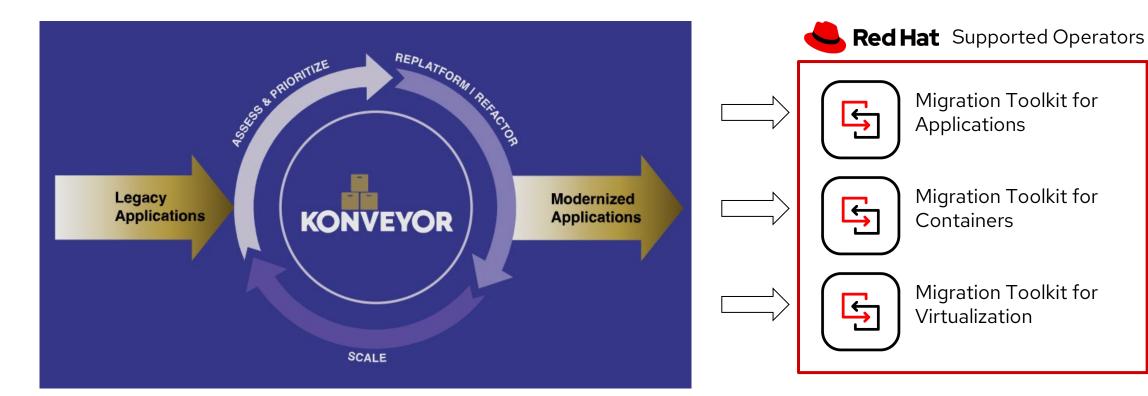
C	reate Migration Pla	an								
1	General VM selection Filter VMs Select VMs	S	elect		migration. The		sis column shows the risk associ risk assessment.	ated with migra	ting a VM as determi	ned by Red Hat's Migration Analytic
	Storage mapping		Name	e v Fi	lter by name	•	Name v JAZ			1-3 of 3 🤍 < 1 of 1 > >>
	Hooks		•		Migration analysis	VM name	Datacenter	Cluster	Host	Folder path
6	Review		►		A	VM1	datacenter1	cluster1	host1	folder1\folder2
			►		•	VM2	datacenter1	cluster1	host1	folder1\folder2
			►		6	VM3	datacenter1	cluster1	host1	folder1\folder2
			►		⊘	VM4	datacenter1	cluster1	host1	folder1\folder2
			•		0	VM5	datacenter1	cluster1	host1	folder1\folder2
				- VM - VM	shares a disk with uses remote devic	other VMs	it violates the following rules: an "r" in it			





## Konveyor Projects and Migration Toolkits by Red Hat

A community of **people** passionate about **helping others modernize** and migrate their **applications** to Kubernetes by **building tools and discovering patterns** of how to **break down monoliths, adopt containers, and embrace Kubernetes**.



Konveyor is a CNCF

Sandbox project

**CLOUD NATIVE** 

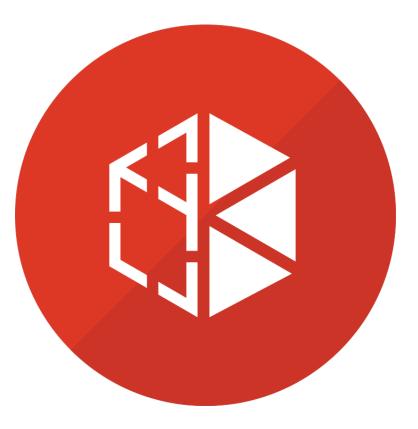
**COMPUTING FOUNDATION** 





## **OpenShift Virtualization**

- Virtual machines
  - Running in containers, managed as Pods
  - Using the KVM hypervisor
- Scheduled, deployed, and managed by Kubernetes
- Integrated with container orchestrator resources and services
  - Traditional Pod-like SDN connectivity and/or connectivity to external VLAN and other networks via multus
  - Persistent storage paradigm (PVC, PV, StorageClass)

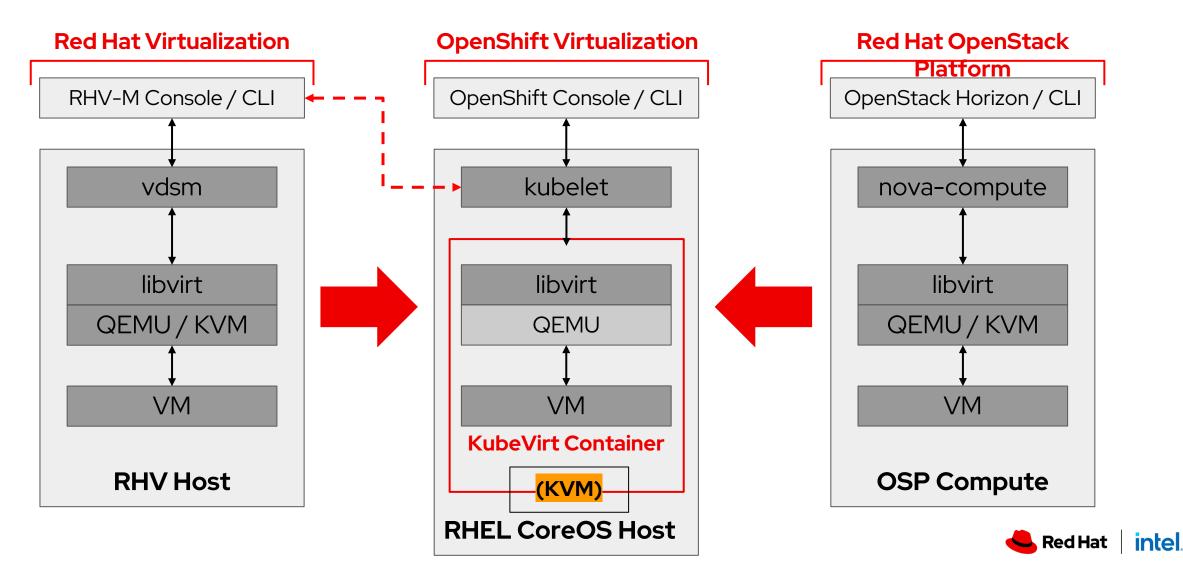






## Containerizing KVM

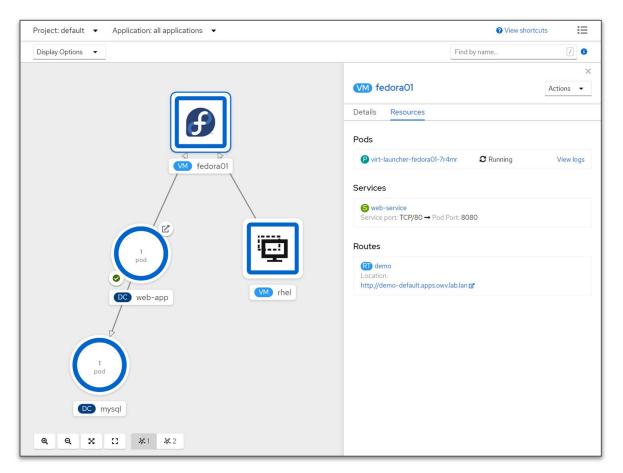
Trusted, mature KVM wrapped in modern management and automation





## Using VMs and containers together

- Virtual machines connected to pod networks are accessible using standard Kubernetes methods:
  - $\circ$  Service
  - Route
  - $\circ$  Ingress
- Network policies apply to VM pods the same as application pods
- VM-to-pod, and vice-versa, communication happens over SDN or ingress depending on network connectivity





## **OpenShift Virtualization - Cloud Native VMs**



Modernize your operations with comprehensive lifecycle and infrastructure management

#### Public cloud experience for VM creation using Instance Types

- $\cdot$  Streamlined VM creation: 3-click GUI experience, tuned for multiple purposes
- Simply specify boot source and InstanceType



## Ensure continuity of business critical applications.

- $\cdot$  OpenShift Data Foundation / ACM Metro-DR
  - Support recovery of declarative GitOps virtual machines

#### Flexibility

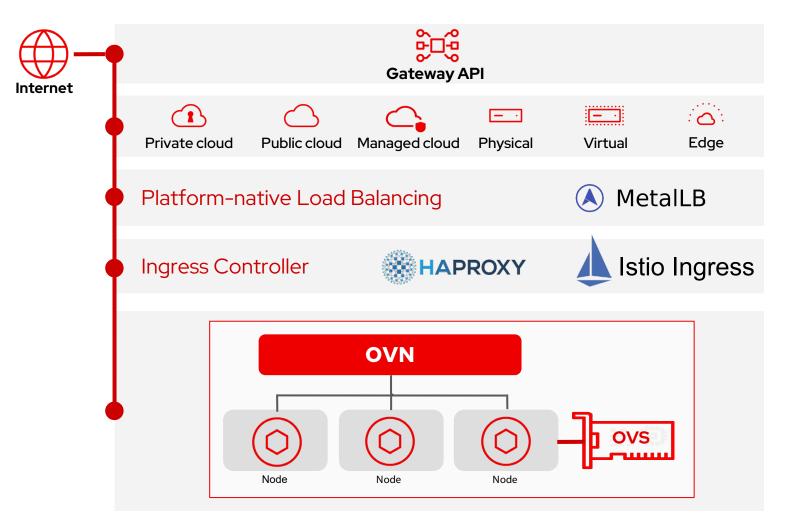
- $\cdot$  Dynamic reconfiguration Bridged and SRIOV NIC hotplug
- $\cdot$  Micro-segmentation on secondary networks
- Workload density improvements
  - kernel same page merging (KSM)
- free page reporting (FPR) can free memory not currently in use by the VM
  - OVN-Kubernetes and ipBlock filtering policies
- Create hosted OpenShift clusters on OpenShift with Advanced Cluster Manager.





## Multicluster End-to-End Networking

Supporting your most advanced workloads



- Unified traffic handling so you configure all your traffic the same way
- Any supported platform add or swap easily, hybrid scenarios
- Flexibility to use native traffic distribution for optimal performance
- OVN for advanced traffic workloads
- IPv6 single/dual for scale
- HW Offload (OVS, IPsec, ...) for performance
- Multi-NIC support to align host networking
- BGP-advertised services (FRR)
- Observability for improved understanding
- eBPF precision traffic control
- No-overlay option





## **Networking Observability**



#### **Network Traffic Metrics and**

Whether one cluster or one hundred, developers and cluster administrators require seamless connectivity across applications.

#### Network Policy and Governance

Security and regulatory compliance requires governance of traffic in, around, and out of networks.

## Platform Consistency

Security Everywhere

#### **Network Traffic Flow and**

TOPORTOPICS and administrators require a common understanding of their traffic within and across cluster boundaries.

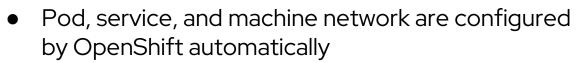
#### Network Flow Data – New Insight & Presentation

Tabular Netflow data, NOC Dashboard, Pod/Service/Node-specific Topology, New Metrics, Export options

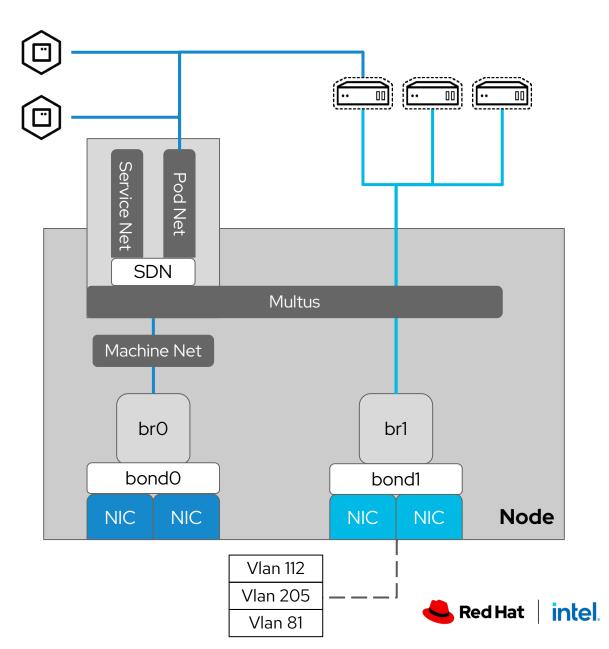
📽 Administrator	· ·		You are logge	ed in as a temporary administrative user. Up	date the <u>cluster OA</u>	uth configuration to	o allow others to log in.				
Home	~	Network Traffic									
Overview		Query Options 🔹	Names 💌	Q II II II				Last 5	i minute 💌 F	lefresh off 🔹	C
Projects			Specify a single kubernetes name. Learn more								
Search		Names "dns-default" 🗙	Clear all filters								
API Explorer		Date & time 1	Name 1	Namespace 1	Port 1	Name I	Namespace I	Port 1	Direction 1	Bytes I	Packets *
Events		Mon Mar 28 2022 3:50:19	P flowlogs-pipeline-7cc4668fd7-s7ckg	NS network-observability	40175	S dns	NS openshift	domain (53)	Ingress	90	1
		Mon Mar 28 2022 3:50:18	Pflowlogs-pipeline-7cc4668fd7-s7ckg	NS network-observability	56608	S dns	NS openshift	domain (53)	Ingress	90	1
Operators	<b>`</b>	Mon Mar 28 2022 3:50:18	Pflowlogs-pipeline-7cc4668fd7-s7ckg	NS network-observability	57159	S dns	NS openshift	domain (53)	Ingress	90	1
Workloads	>	Mon Mar 28 2022 3:50:17	B flowlogs-pipeline-7cc4668fd7-s7ckg	NS network-observ > Flows (a	) panels)						
		Mon Mar 28 2022 3:50:17	🕑 flowlogs-pipeline-7cc4668fd7-s7ckg	NS network-observ							
Networking	`	Mon Mar 28 2022 3:50:17		NS network-observ 200 ops/s							
Storage	>	Mon Mar 28 2022 3:50:17	P loki-ingest	180 ops/s							
		Mon Mar 28 2022 3:50:10		160 mm/m							
Builds	<u>``</u>	Mon Mar 28 2022 3:50:10	loki-ingester-lo	oki 🖌							<sup>1</sup>
Observe	~	Mon Mar 28 2022 3:50:16		140 ops/s							لىر
Alerting		Mon Mar 28 2022 3:50:16		120 ops/s	15:51:45 15:52	2:00 15:52:15	15:52:30 15:52:45	15:53:00	15:53:15 15	5:53:30 15:5	53:45 1
Metrics		Mon Mar 28 2022 3:50:16									
Dashboards				T T			Flows by source nar	nespace			
Targets			TO	P loki-querie 30 ops/s							
Network Traffic				20 ops/s ~				The second second			1
		<u>x</u>	P loki-compactor-loki-0	6 kBps 10 ops/s							
			loki-compactor-loki 🖌	0 ops/s	15:52:00 15:5	12:30 15:53:00	15:53:30 15:54:00	15:54:30 1	5:55:00 15:55:	30 15:56:00	15:56:3
							-"default") — {SrcK8S_Nami rcK8S_Namespace="openshift			espace-*network-	observability
				— (SrcK8	S_Namespace="opensit		<ul> <li>{SrcK8S_Namespace="oper</li> </ul>	nshift-authentication	- 1-operator"}		
					U						
			6 kBps	x B	loki-queri	erdd5fcb-					

## Multiple VLANs and Multus



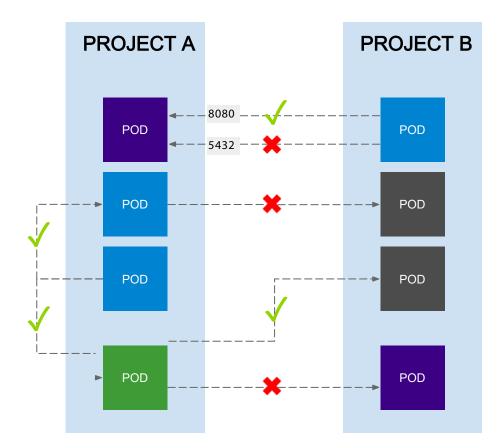


- Use kernel parameters (dracut) for configuration at install - bond0 in the example to the right
- Use kubernetes-nmstate, via the NMstate Operator, to configure additional host network interfaces
  - **bond1** and **br1** in the example to the right
- VM pods connect to one or more networks simultaneously





## **Network Policy** (network micro-segmentation)



**Example Policies** 

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

port: 8080





## MetalLB - The Problem

#### What Problem Are We Solving?

- Kubernetes Services of type: LoadBalancer
- On a cloud, this creates a cloud-native LB
- What about bare metal clusters?

```
apiVersion: v1
kind: Service
metadata:
  name: nginx
spec:
  ports:
  - name: http
    port: 80
    protocol: TCP
    targetPort: 80
  selector:
    app: nginx
  type: LoadBalancer
```







- Solve the problem by using standard network protocols
- MetalLB has two modes to announce reachability information for load balancer IP addresses:
  - Layer 2
  - BGP
- Two components:
  - Controller One per cluster
  - Speaker Per Node (DaemonSet)
- L2 mode: ARP (IPv4) or NDP (IPv6) announces location of a LB'd IP address from the Speaker, then relies on Service load balancing within the cluster

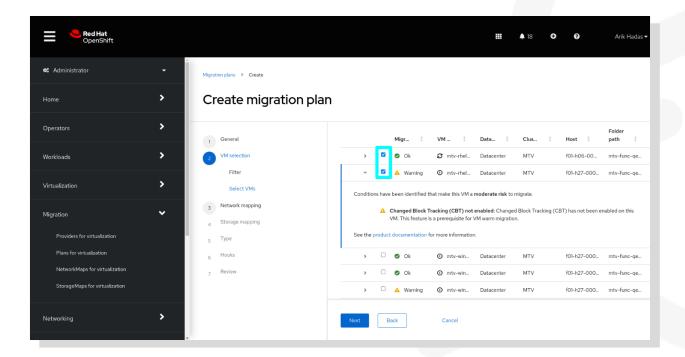
apiVersion: v1
kind: Service
metadata:
 name: nginx
spec:
 ports:
 name: http
 port: 80
 protocol: TCP
 targetPort: 80
 selector:
 app: nginx
type: LoadBalancer



# And now... (drum rool) *(Interpretent of the moment we've all been waiting for: Migrating VM based applications with minimal disruption!*

#### **Migration tooling**

- Migration Toolkit for Virtualization (MTV)
- Streamlined migration of virtual machines at scale
- Included with OpenShift







## OpenShift Virtualization - Services Journey

Strategy	Foundation	Expand	Evolve
Phase 1 - <u>Virtualization</u> <u>Migration Assessment</u>	Training & Certs – Discounted training bundle: <u>Mar</u> Phase 2 – Migrate: <u>OpenShift Virtualization Production Build + I</u>		App Modernization Accelerator (Optional)
<ul> <li>Analyze current VM Architecture</li> </ul>	<ul> <li>Deploy OpenShift cluster with optional container storage integration</li> </ul>	<ul> <li>Automated migration of VM batches with Ansible Automation Platform</li> </ul>	<ul> <li>Optional solution for customers that want to</li> </ul>
<ul> <li>Identify VM workloads</li> </ul>	• Enable & validate virtualization features	Automated configuration of	modernize apps to containers
• <b>Define</b> integrations	<ul> <li>Migration of initial VM workloads</li> </ul>	components like networking and	<ul> <li>Onboard initial app teams to</li> </ul>
<ul> <li>Understand Day 2 Ops</li> </ul>	Validate strategy for scale	storage with Ansible Automation Platform	platform functionality
<ul> <li>Propose high-level design and roadmap</li> </ul>	<ul> <li>Automate Day 2 Operations</li> </ul>	• <b>Repeat</b> migration patterns	provided by OpenShift
<ul> <li>Build lightweight business case</li> </ul>	(Optional Phase 1.5) - <u>OpenShift</u> <u>Virtualization Proof of Value</u>	<ul> <li>Validate migration</li> <li>Retire legacy platform</li> </ul>	Ansible Automation Acceleration (Optional)
	• <b>Proof of Value</b> of the virtualization platform, with meaningful workloads migrated	• Measure <b>value realized</b>	<ul> <li>Optional Services Map to accelerate Ansible Automation for the Enterprise</li> </ul>

**Technical Account Management -** Operational guidance & advisory services from an OpenShift TAM