vSphere 7.0 Update 2

A new platform for the Developer, the Kubernetes Admin, and the vSphere Admin

Part 2 – the Kubernetes Admin

Cormac Hogan
Office of the CTO
Cloud Platform

vmware® Confidential | ©2021 VMware, Inc.

Agenda

What we will look at in this presentation

- ✓ Which **Tanzu** are we discussing?
- ✓ Compare **vSphere with Tanzu** to **VCF with Tanzu (vSphere with Tanzu on VCF)**
- ✓ Deployment steps: **HAProxy / Load Balancer Service**
- ✓ Deployment steps: **Workload Management / Supervisor cluster**
- ✓ Deployment steps: **TKG 'guest/workload' cluster**
- ✓ An introduction to the **vSAN Data Persistence platform (DPp)**

Let's clarify which Tanzu I will be talking about

TKGI – Tanzu Integrated

This is the product formerly known as **Enterprise PKS** (Pivotal Container Service)

This is now rebranded as **Tanzu Kubernetes Grid Integrated (TKGI)**

I will not be talking about this Tanzu

TKGm – Tanzu Multi-Cloud

This is the version of Tanzu Kubernetes Grid which can be deployed on public and private clouds

It uses a management cluster to manage create/scale/delete of Tanzu Kubernetes clusters

It is branded as **Tanzu Kubernetes Grid multi-cloud (TKGm)**

I will not be talking about this Tanzu

TKGS – Tanzu Service

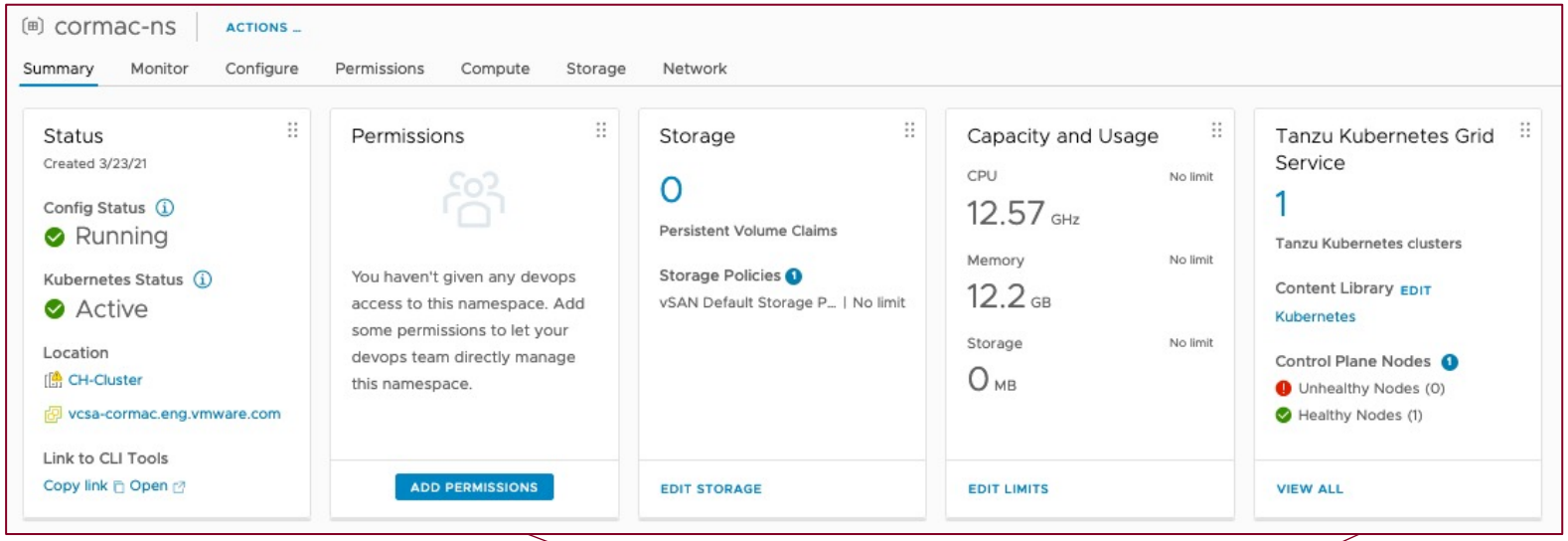
This is the version of Tanzu Kubernetes Grid which can be deployed on **vSphere with Tanzu**

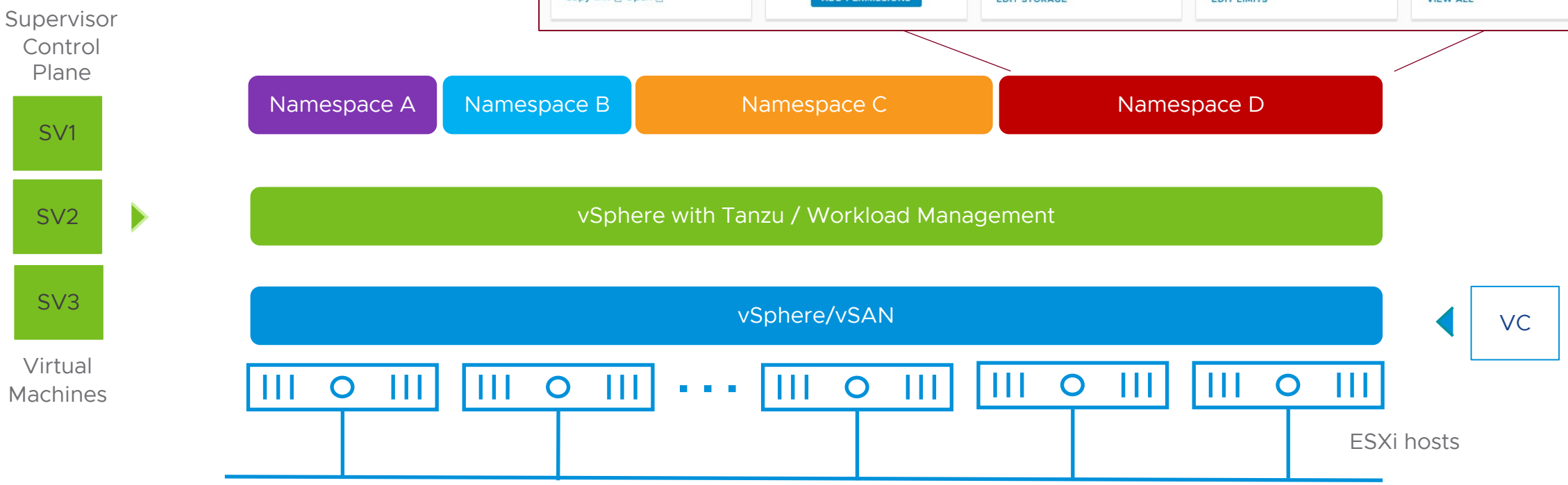
It is branded as **Tanzu Kubernetes Grid Service (TKGS)**

It create similar Tanzu Kubernetes clusters to TKGm

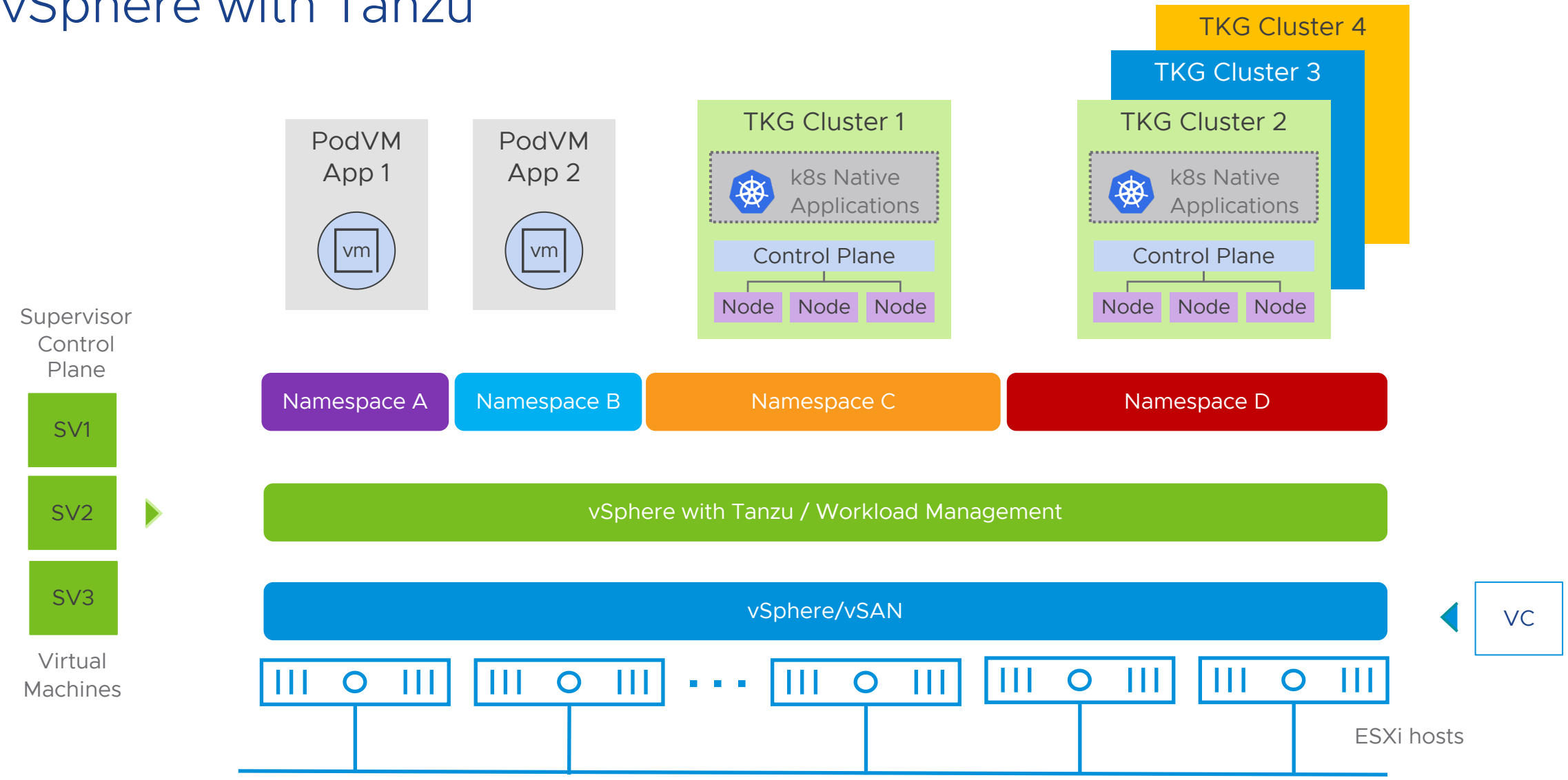
This is the version of Tanzu that I will be talking about

vSphere with Tanzu





vSphere with Tanzu



vSphere with Tanzu / VCF with Tanzu

Compare and Contrast

VMware Cloud Foundation (VCF) with Tanzu

App-focused Management | Dev & IT Ops Collaboration

Check out VMworld 2020 session KUB2469

Developer

VMware Cloud Foundation 4.0

vm

VMware Cloud Foundation Services

KUBERNETES & RESTful APIs

Tanzu Runtime Services

- Tanzu Kubernetes Grid Service

Hybrid Infrastructure Services

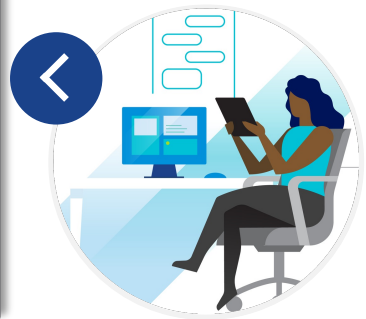
- PodVM Service
- Network Service
- Registry Service
- Storage Services

vCenter Server

vSphere | NSX-T | vSAN | vRealize

Intrinsic Security & Lifecycle Automation

Data Center | Edge | Service Provider | Public Cloud



vSphere Admin

7.0 Update 1/Update 2 Announcement - vSphere with Tanzu

App-focused Management | Dev & IT Ops Collaboration | Use existing vSphere

Developer

vSphere 7.0 U1/U2

vm

KUBERNETES & RESTful APIs

Runtime Services

Tanzu Kubernetes Grid Service

Infrastructure Services

Network Service

Storage Service

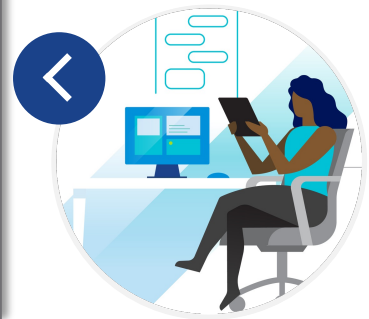
vCenter Server

vSphere

BYO Network

BYO Storage

BYO Load Balancer



vSphere Admin

The fastest way to get started with Kubernetes

vSphere with Tanzu Releases/Editions

vSphere 7.0 (VCF) with Tanzu – Designed for Production at Scale

VCF is required

NSX-T Load Balancer

NSX-T provides PodVM-PodVM traffic overlays

PodVM support

Calico CNI only for TKG cluster Pod to Pod Traffic

Integrated **Harbor** Image Registry, built on PodVMs

vSphere 7.0U1 with Tanzu – for smaller deployments

VCF is not required

NSX-T not required. **VDS** networking supported

HAProxy Load Balancer

No **PodVM** support (when **NSX-T** not used)

Antrea & **Calico CNI** for TKG Pod to Pod Traffic

No **Harbor** Image Registry (since no PodVM)

vSphere 7.0U2 with Tanzu – Production Ready

VCF is not required

NSX-T not required. **VDS** networking supported

NSX Advanced Load Balancer

No **PodVM** support (when **NSX-T** not used)

Antrea & **Calico CNI** for TKG Pod to Pod Traffic

No **Harbor** Image Registry (since no PodVM)

*CNI – Container Network Interface

vSphere 7.0U1/U2 with Tanzu Requirements

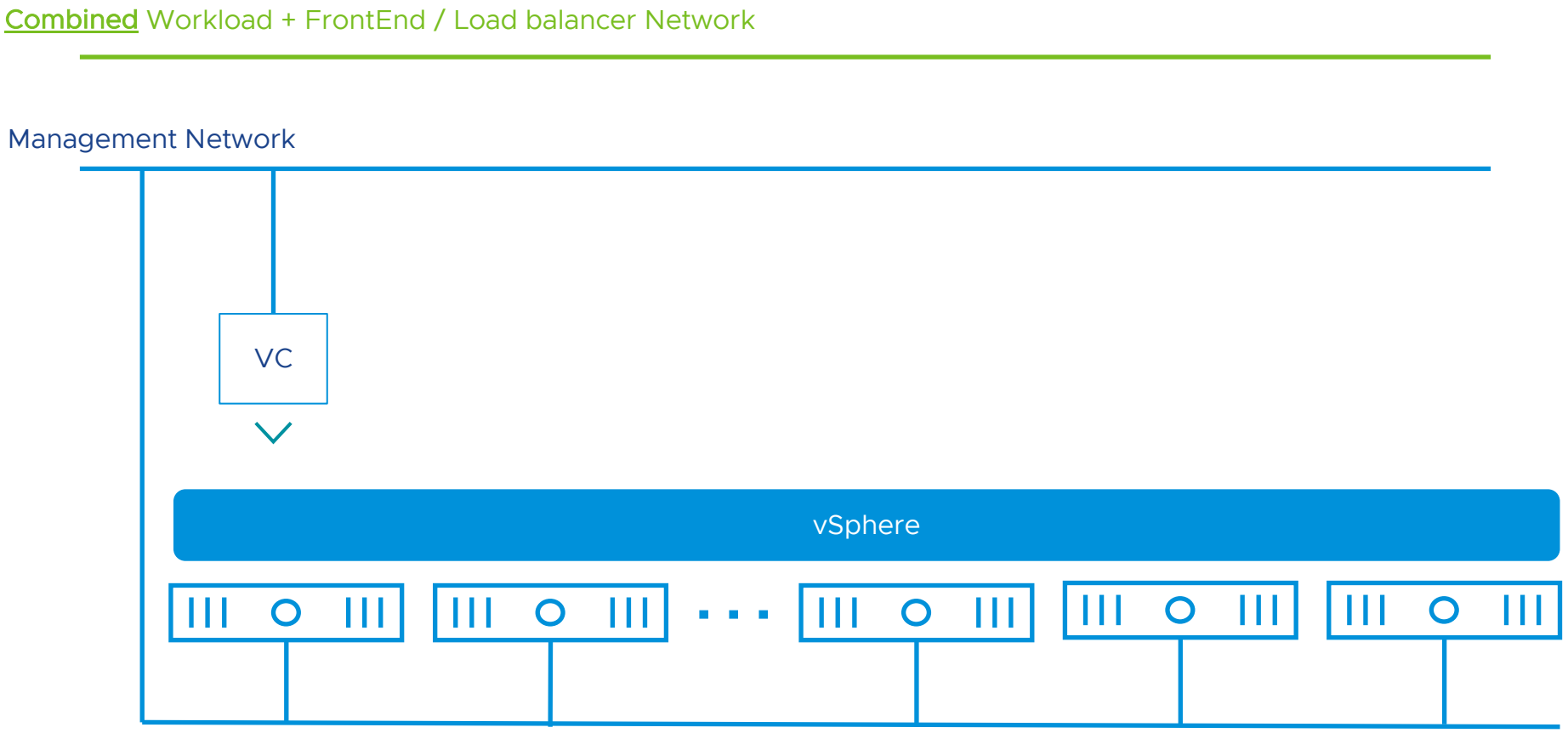
- vSphere 7.0 Update 1 / Update 2
- 3-node or higher vSphere cluster to accommodate 3-node Supervisor cluster control plane
- Shared storage across all ESXi hosts in the cluster
- DRS & HA must be enabled on the cluster
- Appropriate Storage Policies should be created
- HAProxy or NSX ALB for Load Balancer IP range
- A Content Library with a subscription for TKG images
- Network requirements, such as valid IP address ranges
- Enterprise Plus with Tanzu Edition Licenses

Step 1. HAProxy Load Balancer

Deployment Steps

Option 1 – Combined FrontEnd & Workload Networking

Check out VMworld 2020 session KUB2469

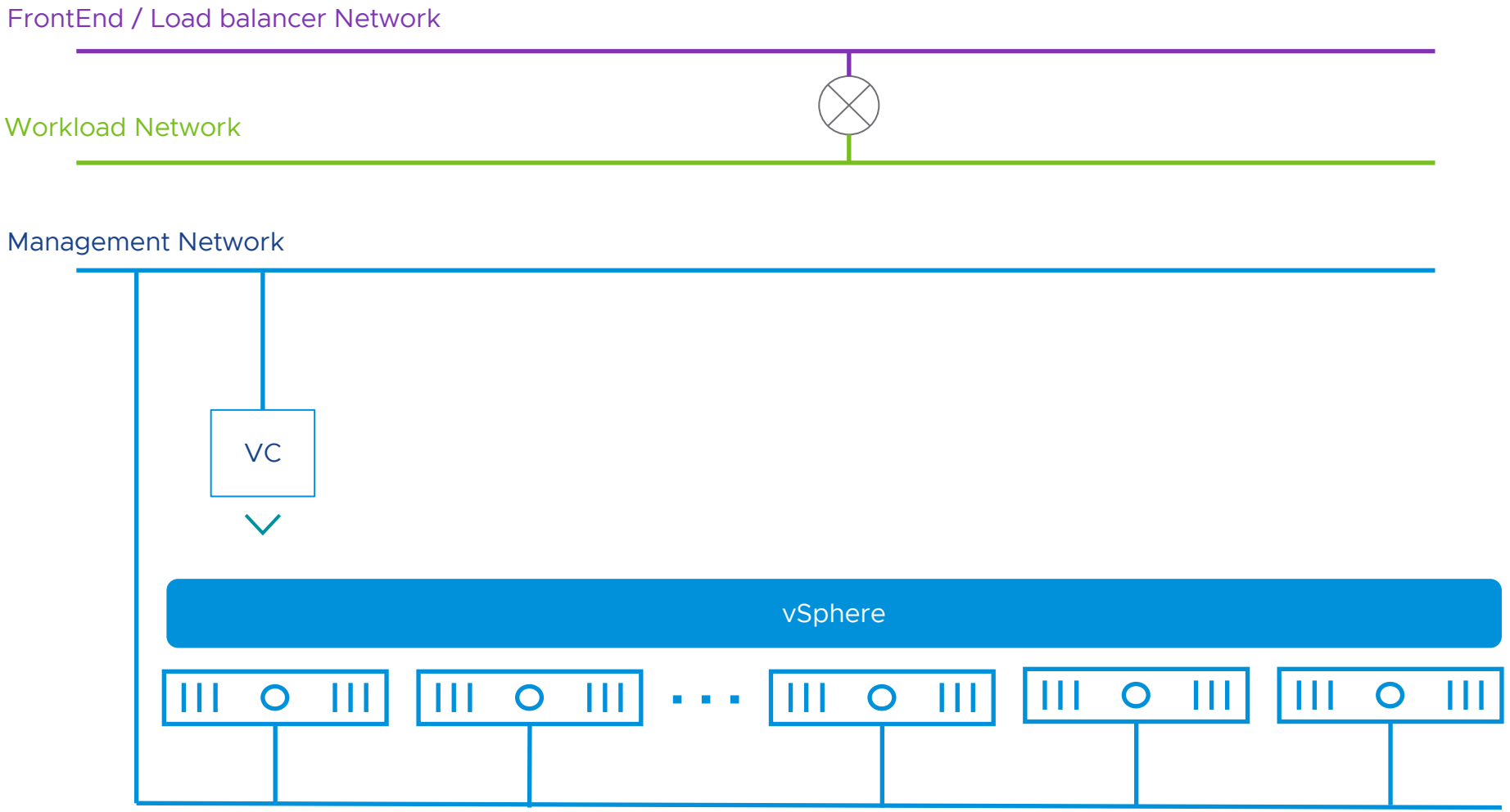


2 NIC approach

The FrontEnd / Load Balancer network are on the same segment

Extra care needs to be taken when selecting IP address ranges for each network

Option 2 – Separate FrontEnd Networking



3 NIC approach

A **route** is required between the FrontEnd / Load Balancer network and the Workload network if the HA-Proxy is deployed with 3 NICs

Step 1 - Deploy HAProxy

Providing Load Balancer services to vSphere with Tanzu

Deployed as OVA

- 2 NIC network - management with combined workload & frontend,

- 3 NIC network - separate workload & frontend

FrontEnd network == Load Balancer network == Virtual IP (VIP) network

Note CIDR formats

haproxy-v0.1.7 - New Virtual Machine from Content Library

- 1 Select a name and folder
- 2 Select a compute resource
- 3 Review details
- 4 License agreements
- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

2.6. Workload Gateway	The gateway address for the workload network 192.50.0.1
2.7. Frontend IP	(Optional) The static IP address for the appliance on the Frontend Port Group in CIDR format (Eg. ip/subnet mask bits). This IP must be outside of the Load Balancer IP Range 192.50.0.170/24
2.8. Frontend Gateway	(Optional) The gateway address for the frontend network 192.50.0.1
3. Load Balancing	4 settings
3.1. Load Balancer IP Ranges, comma-separated in CIDR format (Eg 1.2.3.4/28,5.6.7.8/28)	The IP ranges the load balancer will use for Kubernetes Services and Control Planes. The Appliance will currently respond to ALL the IPs in these ranges whether they're assigned or not. As such, these ranges must not overlap with the IPs assigned for the appliance or any other VMs on the network. 192.50.0.176/29
3.2. Dataplane API Management Port	Specifies the port on which the Dataplane API will be advertized on the Management Network. 5556
3.3. HAProxy User ID	Specifies the user ID used to authenticate to the Dataplane API. admin
3.4. HAProxy Password	Specifies the password used to authenticate to the Dataplane API. (6-128 characters) Password vmware Confirm Password vmware

CANCEL BACK NEXT

HAProxy Virtual Appliance Considerations

IP Addresses & Ranges

Static IP addresses required for HAProxy on Management **and** Workload networks

- The IP address format must be in CIDR format, e.g. 192.168.100.100/**24**

HAProxy **FQDN** is required on the Management network, so DNS must be present

3 distinct ranges of IP addresses are required for vSphere with Tanzu deployment

Front-End / Load Balancer Network	Management Network (Supervisor Nodes)	Workload Network (Supervisor and TKG Nodes)
Contiguous range of **N*** IP addresses, provided in a CIDR format. Required during HAProxy setup.	Contiguous range of **5** IP addresses, provided during Workload Management enablement. Required during Tanzu setup.	Contiguous range of **N*** IP addresses, provided during Workload Management enablement. Required during Tanzu setup.

* N is a number defined by the administrator, depending on environment requirements

Useful Tools

Verifying CIDR ranges start & end, and HA-Proxy Load Balancer IP Addresses

IPADDRESSGUIDE

HOME IPV4 TOOLS

CIDR to IPv4 Conversion

CIDR is the short for Classless Inter-Domain Routing, an IP addressing scheme that replaces the older system based on classes A, B, and C. A single IP address can be used to designate many unique IP addresses with CIDR. A CIDR IP address looks like a normal IP address except that it ends with a slash followed by a number, called the IP network prefix. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

CIDR to IP Range

Result

CIDR Range	192.50.0.176/29
Netmask	255.255.255.248
Wildcard Bits	0.0.0.7
First IP	192.50.0.176
First IP (Decimal)	3224502448
Last IP	192.50.0.183
Last IP (Decimal)	3224502455
Total Host	8

CIDR

192.50.0.176/29

Calculate

https://www.ipaddressguide.com/cidr

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 10.27.62.0 to 10.27.62.66 IP Range

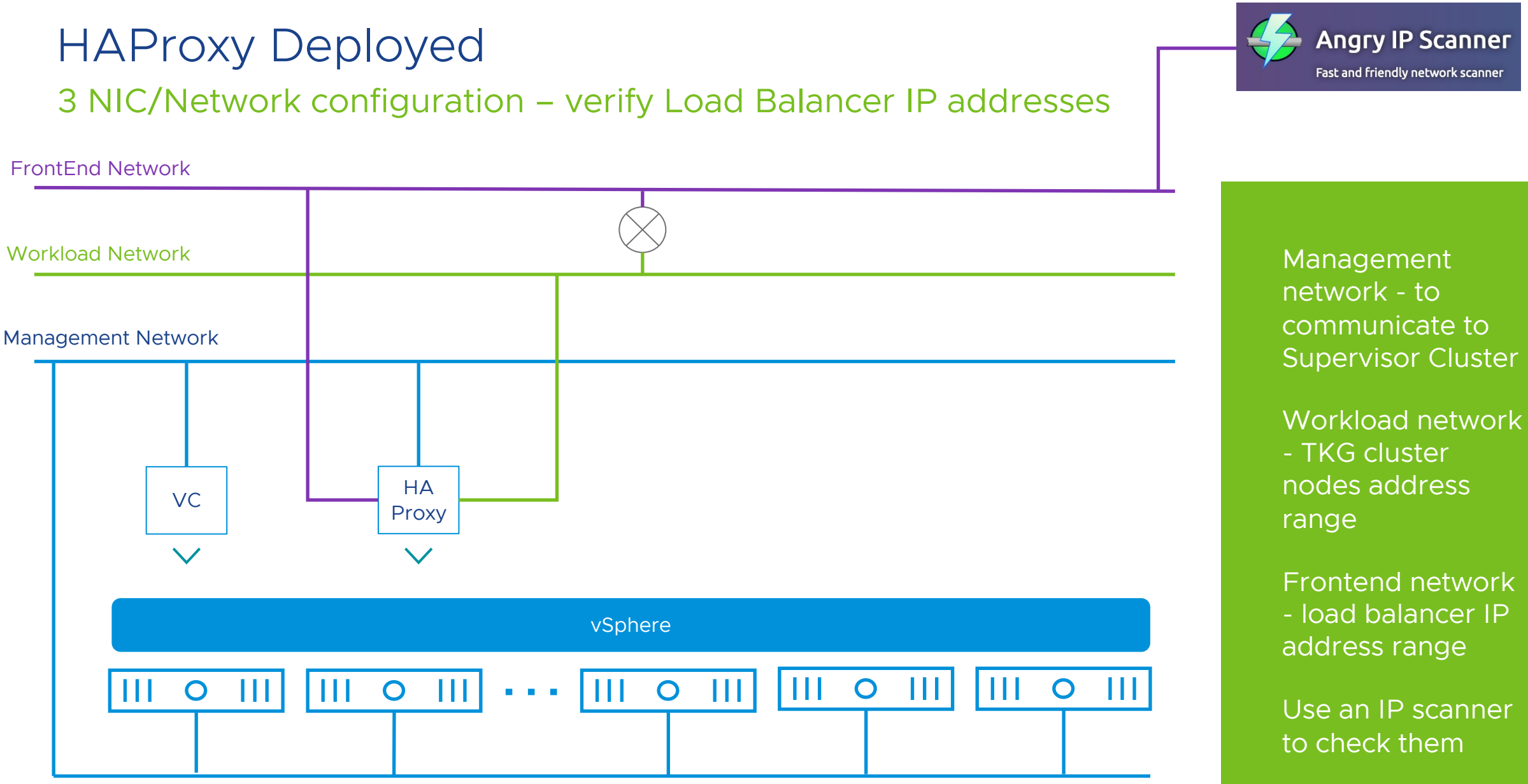
Hostname: ch-jump-02 IP↑ Netmask Start

IP	Ping	Hostname	Web detect	TTL	HTTP Sender	Packet Loss	MAC Address
10.27.62.1	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.2	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.3	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.4	0 ms	cs-tse-prd-dns.csl.vmware.com	Apache/2.2....	10	Mon, 16 No...	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.5	0 ms	[n/a]	lighttpd/1.4....	10	Mon, 16 No...	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.6	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.7	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.8	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.9	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.10	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.11	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.12	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.13	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.14	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.15	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.16	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.17	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.18	0 ms	[n/a]	nginx/1.19.3	10	Mon, 16 No...	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.19	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.20	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.21	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.22	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.23	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.24	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.25	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.26	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.27	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.28	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.29	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.30	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.31	0 ms	[n/a]	[n/a]	10	[n/a]	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.32	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.33	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.34	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
10.27.62.35	0 ms	[n/a]	nginx/1.16.1	10	Mon, 16 No...	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.36	0 ms	[n/a]	nginx/1.16.1	10	Mon, 16 No...	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.37	0 ms	[n/a]	nginx/1.16.1	10	Mon, 16 No...	0/3 (0%)	58:8D:09:EE:68:80
10.27.62.38	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]

https://angryip.org/

HAProxy Deployed

3 NIC/Network configuration – verify Load Balancer IP addresses



Management network - to communicate to Supervisor Cluster

Workload network - TKG cluster nodes address range

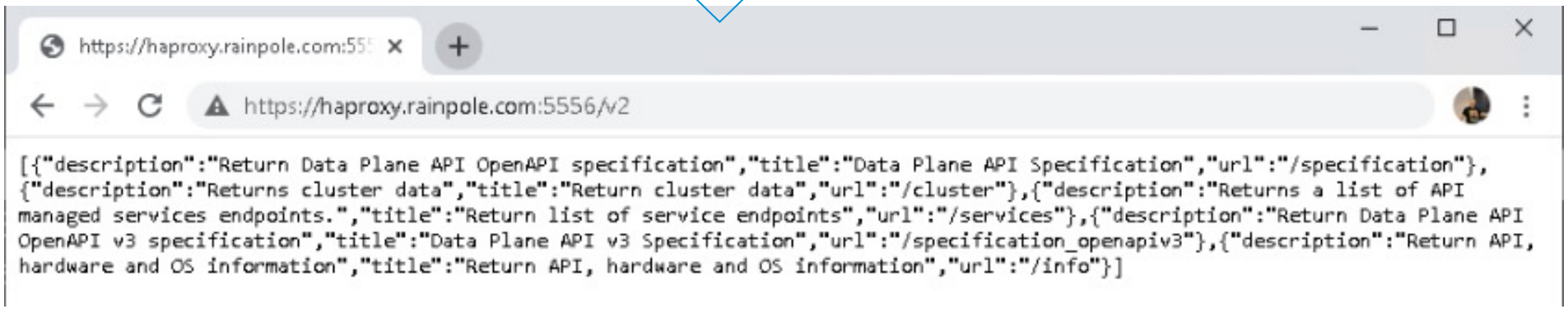
Frontend network - load balancer IP address range

Use an IP scanner to check them

https://<HA-PROXY-FQDN>:5556/v2

Verifying that HAProxy is responding on port 5556

Using the above URL, provide the admin credentials added during HA-Proxy deployment



Step 2. Workload Management (Enabling vSphere with Tanzu)

Deployment Steps

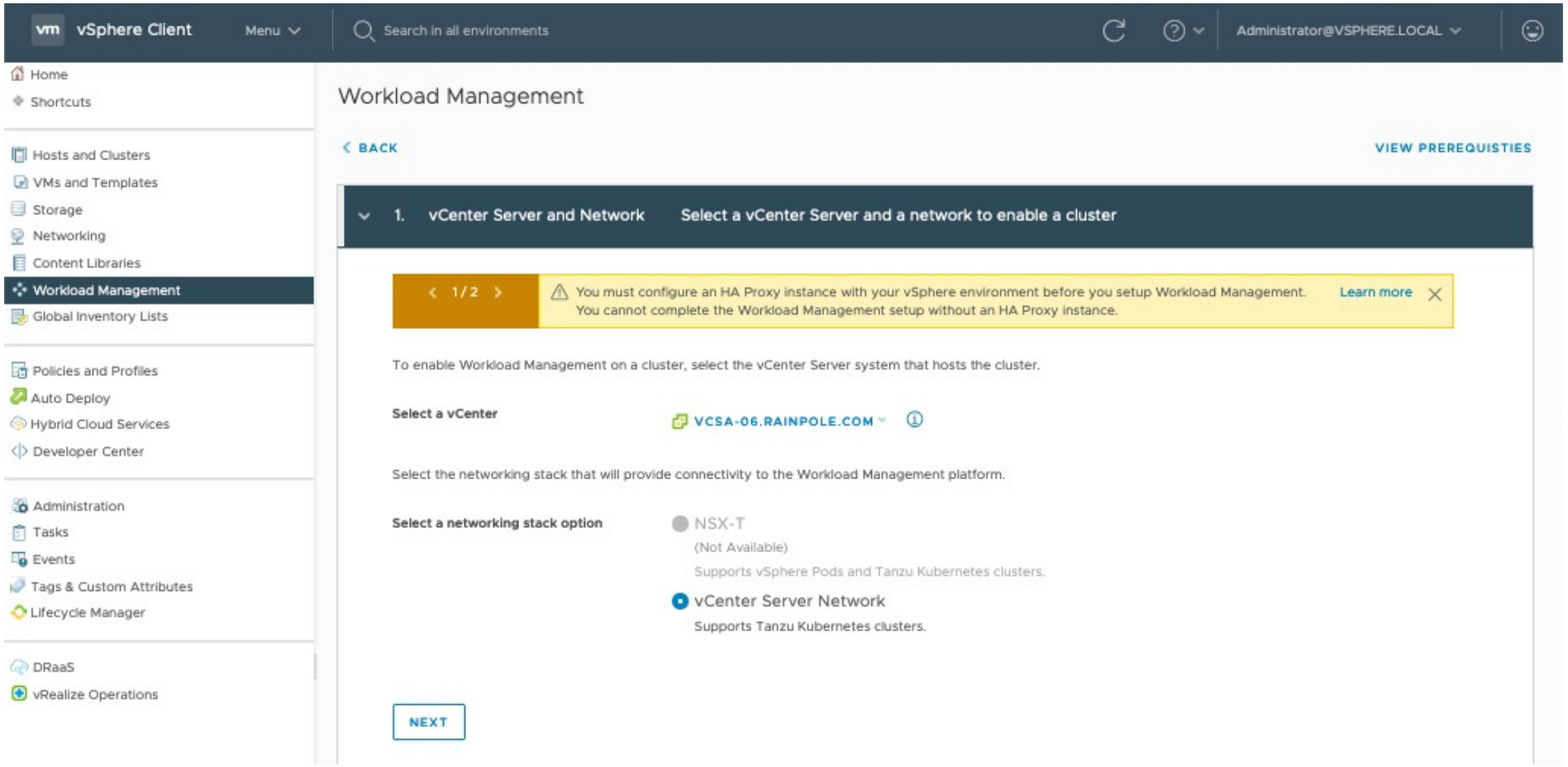
Step 2 - Deploy Workload Management/vSphere with Tanzu

New Workload Management view in the vSphere client

Select cluster, control plane resources, storage policy

Provide network details for management, workload and frontend / load balancers

IP ranges for all 3 networks are provided during this step



From Configuring to Running

Control Plane address switches to Load Balancer IP address

Workload Management

Namespaces | Clusters | Updates

ADD CLUSTER

Filter

Management network IP address

Cluster	Namespaces	Hosts	Config Status	Control Plane Nod	CPU for namespa	Memory for name	Storage for name	Current Version	vCenter
OCTO-Cluster	0	4	Configuring (1)	10.27.51.191	0	0	552.11 TB		vcsa-06.rainpole.com

Workload Management

Namespaces | Clusters | Updates

ADD CLUSTER

Filter

Load Load Balancer IP address

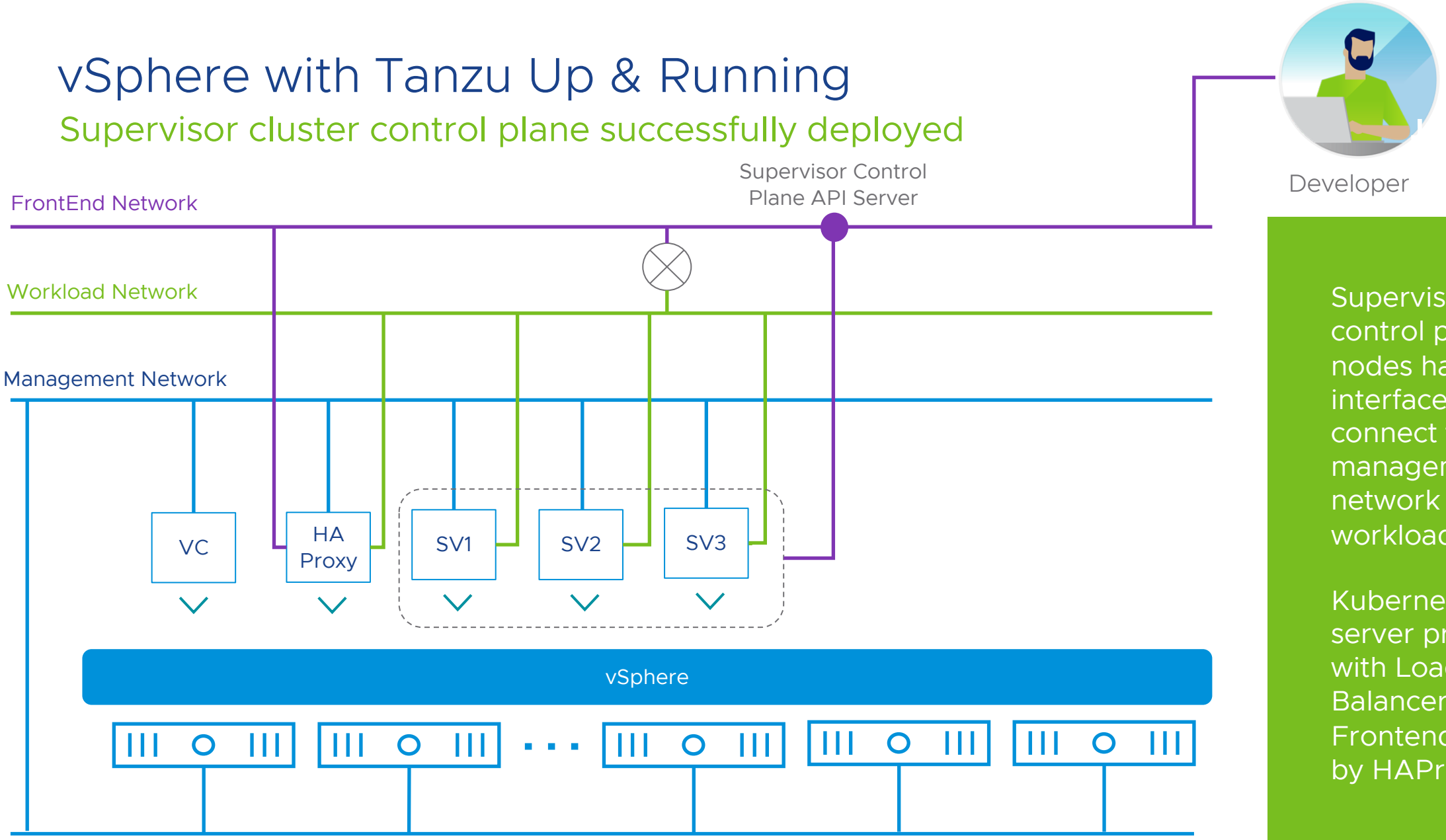
Cluster	Namespaces	Hosts	Config Status	Control Plane Nod	CPU for namespa	Memory for name	Storage for name	Current Version	vCenter
OCTO-Cluster	0	4	Running	192.50.0.176	0	0	552.1 TB	v1.18.2-vsc0.0.5-16762486	vcsa-06.rainpole.com

Note change from Management IP address to Load Balancer IP address

Load Balancer IP address provided by HA-Proxy

vSphere with Tanzu Up & Running

Supervisor cluster control plane successfully deployed



Supervisor cluster control plane nodes have interfaces that connect to management network and workload networks

Kubernetes API server provided with Load Balancer IP on Frontend network by HAProxy

vSphere with Tanzu Deployment Demo

Confidential | ©2021 VMware, Inc.

Cormac Desktop

vSphere - Shortcuts

https://vcsa-06.rainpole.com/ui/app/shortcuts

Search

vSphere Client | Menu | Search in all environments | Administrator@VSPHERE.LOCAL

- Home
- Shortcuts

- Hosts and Clusters
- VMs and Templates
- Storage
- Networking
- Content Libraries
- Workload Management
- Global Inventory Lists

- Policies and Profiles
- Auto Deploy
- Hybrid Cloud Services
- Developer Center

- Administration
- Tasks
- Events
- Tags & Custom Attributes
- Lifecycle Manager

- DRaaS
- vRealize Operations

Shortcuts

Inventories

Hosts and Clusters | VMs and Templates | Storage | Networking | Content Libraries | Global Inventory Lists | Workload Management | DRaaS

Monitoring

Task Console | Event Console | VM Customization Specifications | VM Storage Policies | Host Profiles | Lifecycle Manager

Administration

Licensing

Recent Tasks | Alarms

Steps 3 & 4. Namespace & TKG Cluster

Deployment Steps

Step 3 - Create a Namespace

Resource Allocation / Multi-Tenancy in vSphere with Tanzu

Create resources for developer

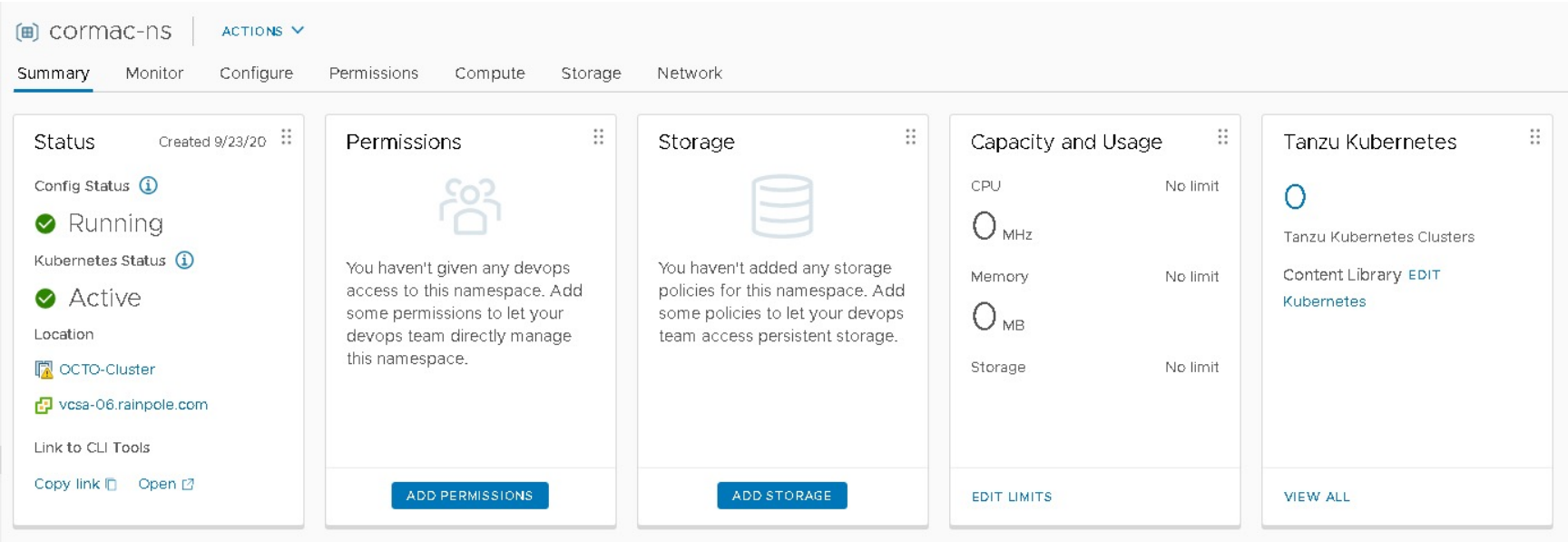
Set Permissions

Assign Storage Policies

Set Limits on Resource Usage

Monitor TKG clusters

Content Library details



Status and **Location** info, including links to **download** Kubernetes CLI Tools

Permissions to **Edit** or simply **View** in a namespace

Storage to select which Storage Policies become Kubernetes **Storage Classes** in this namespace

Capacity and Usage set **limits** on CPU, Memory and Storage in the namespace

Tanzu Kubernetes reports on any 'guest' cluster deployed in the namespace. **Content Library** holds available images

Working in the context of Supervisor Cluster Namespace

Login and Logout commands allow easy switching of contexts

```
> kubectl-vsphere login \
--insecure-skip-tls-verify \
--vsphere-username administrator@vsphere.local \
--server=https://192.50.0.176

Password:***********
Logged in successfully.

You have access to the following contexts:
   192.50.0.176
   cormac-ns

If the context you wish to use is not in this list, you may need to
try logging in again later, or contact your cluster administrator.

To change context, use `kubectl config use-context <workload name>`
```

K8s Admins (and developers) can login and work in the context of the vSphere Namespace to build Kubernetes objects, including guest TKG clusters

--server takes Supervisor cluster control plane IP address

Step 4 – Deploy a Tanzu Kubernetes "Guest/Workload" Cluster

Upstream, compliant, VMware engineered and VMware supported K8s distro

1 control plane node

2 worker nodes

Image to use, must be in content library

Node Resources

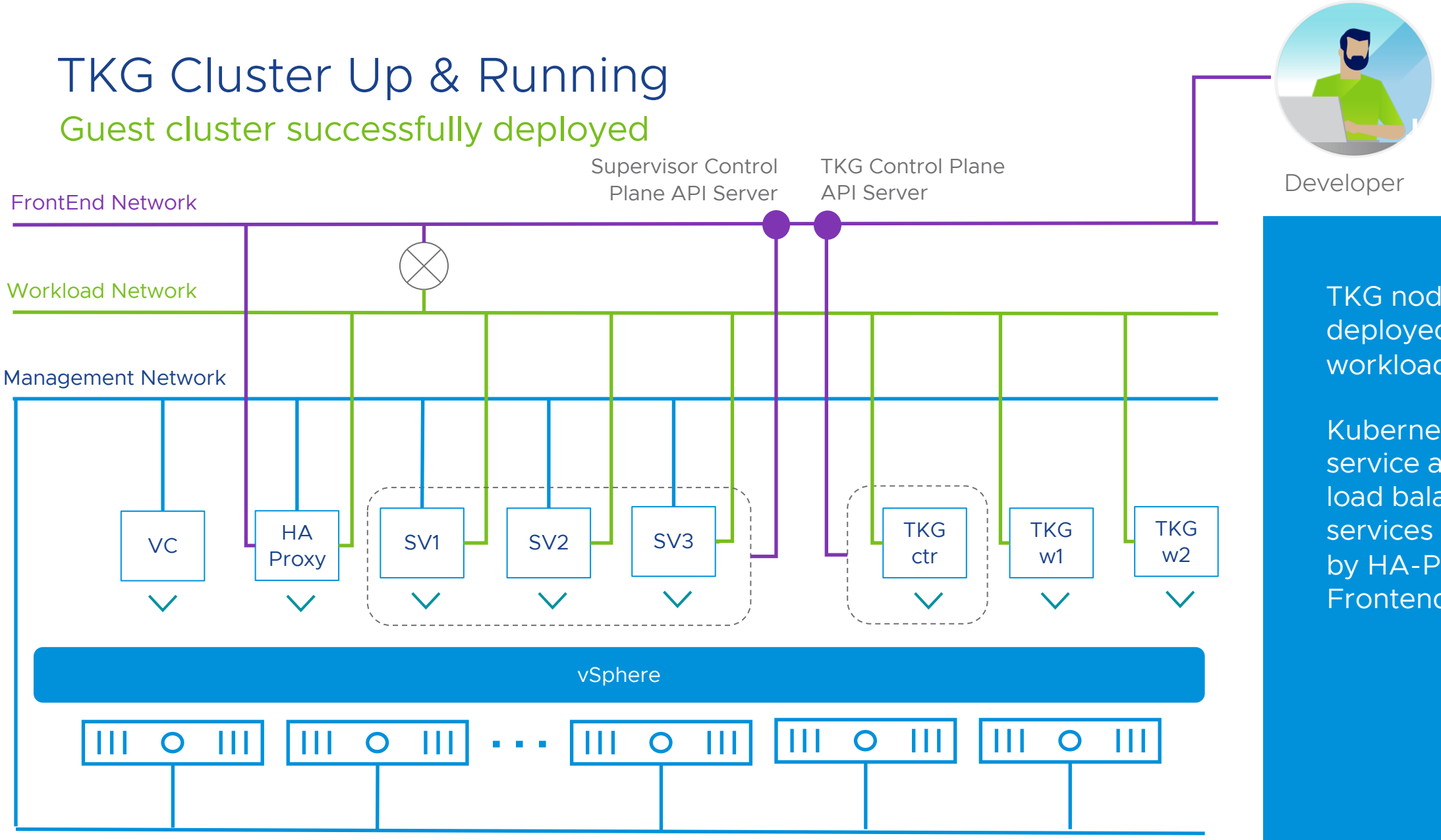
```yaml
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TanzuKubernetesCluster
metadata:
name: tkg-cluster-01
spec:
topology:
   controlPlane:
      count: 1
      class: guaranteed-small
      storageClass: vsan-default-storage-policy
   workers:
      count: 2
      class: guaranteed-small
      storageClass: vsan-default-storage-policy
distribution:
   version: v1.17.8
```

TKG "guest" or TKG "workload" clusters are deployed through a simple YAML manifest

Images available via synchronized content library

TKG Cluster Up & Running

Guest cluster successfully deployed



TKG nodes deployed on the workload network

Kubernetes API service and any load balancer services provided by HA-Proxy on Frontend network

Working in the context of Tanzu Kubernetes

Login and Logout commands allow easy switching of contexts

```
> kubectl-vsphere login \
--insecure-skip-tls-verify \
--vsphere-username administrator@vsphere.local \
--server=https://192.50.0.176 \
--tanzu-kubernetes-cluster-namespace cormac-ns \
--tanzu-kubernetes-cluster-name tkg-cluster-01

Password:***********
Logged in successfully.

You have access to the following contexts:
   192.50.0.176
   cormac-ns
   tkg-cluster-01

If the context you wish to use is not in this list, you may need to try
logging in again later, or contact your cluster administrator.

To change context, use `kubectl config use-context <workload name>`
```

Kubernetes cluster admins (or developers) can login and work in the context of the TKG cluster

TKG is a VMware engineered & supported Kubernetes distribution

TKG Cluster Deployment Demo

vSphere - Namespaces

https://vcsa-06.rainpole.com/ui/app/workload-platform/home/namespaces

New vCenter server updates are available VIEW UPDATES

vSphere Client | Menu | Search in all environments | Administrator@VSPHERE.LOCAL

Namespaces 1

cormac-ns

Workload Management

Namespaces | Clusters | Updates

NEW NAMESPACE

Filter

Namespaces	Cluster	Config Status	CPU (Used | Limit)	Memory (Used | Limit)	Storage (Used | Limit)	Description	vCenter
cormac-ns	OCTO-Cluster	Running	0 | No Limit	0 | No Limit	0 | No Limit		vcsa-06.rainpole.com

1 item

Recent Tasks | Alarms

Task Name	Target	Details	Status	Initiator	Queued For	Start Time	Comple
Fetch Content of a Library Item	ob-17010758-photon-3-k8s-v1.17.11---vmware.1-tkg.2.ad3d374		Completed	VSPHERE.LOCAL\wcp-vmop-use...	77 ms	02/25/2021, 12:08:24 PM	02/25/
Fetch Content of a Library Item	ob-15957779-photon-3-k8s-v1.16.8---vmware.1-tkg.3.60d2ffd		Completed	VSPHERE.LOCAL\wcp-vmop-use...	76 ms	02/25/2021, 12:08:18 PM	02/25/
Fetch Content of a Library Item	ob-17419070-photon-3-k8s-v1.18.10---vmware.1-tkg.1.3a6cd48		Completed	VSPHERE.LOCAL\wcp-vmop-use...	77 ms	02/25/2021, 12:08:12 PM	02/25/
Fetch Content of a Library Item	ob-17332787-photon-3-k8s-v1.17.13---vmware.1-tkg.2.2c133ed		Completed	VSPHERE.LOCAL\wcp-vmop-use...	84 ms	02/25/2021, 12:08:06 PM	02/25/

All

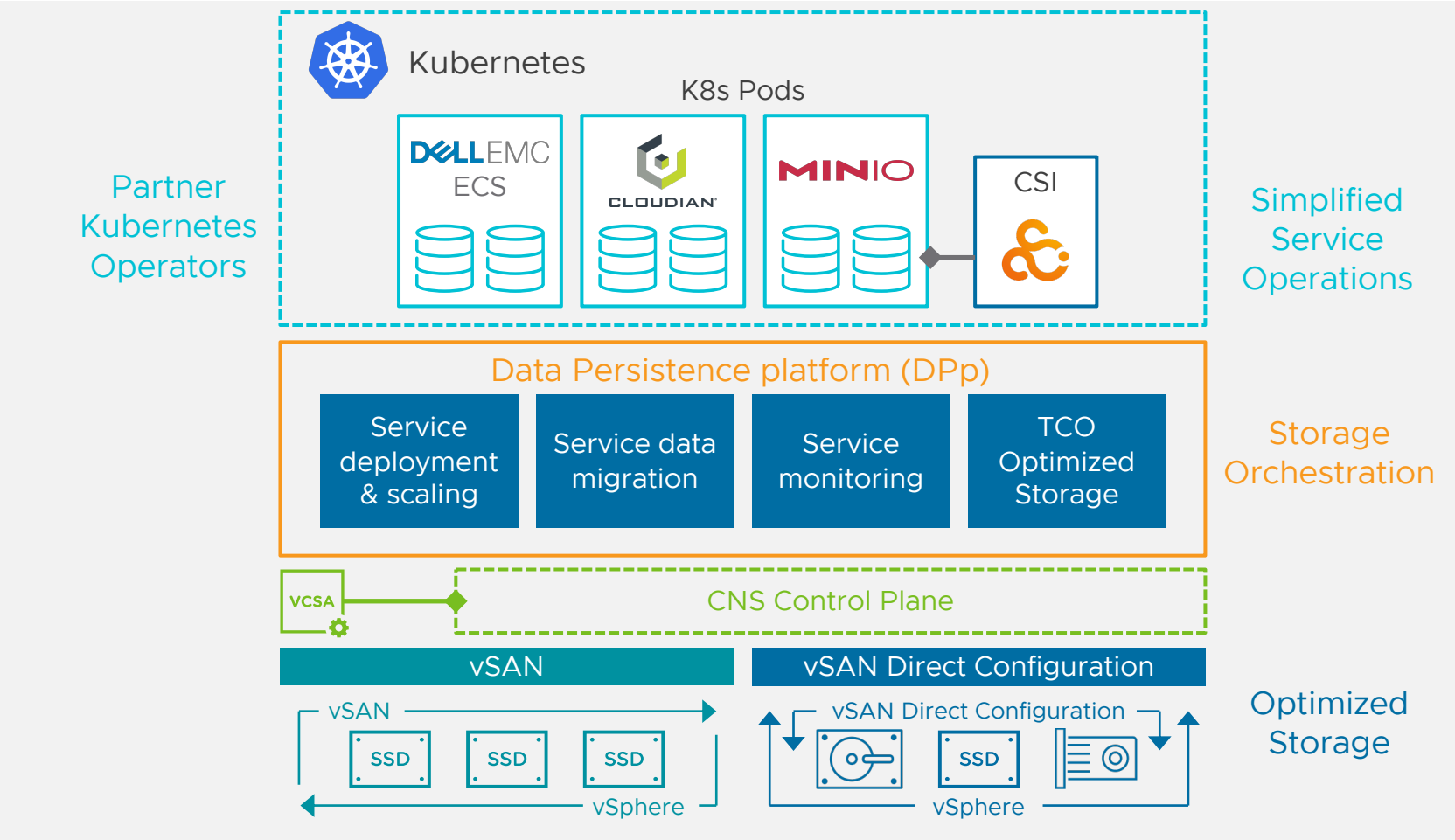
More Tasks

vSAN Data Persistence platform

vSphere with Tanzu

Consume Resources for Modern Apps in a More Efficient Way

VMware vSAN Data Persistence platform (DPp)



Framework for **integrating stateful apps** on vSAN*

Placement management for application resilient solutions

Awareness of vSphere management operations

Available with **VCF 4.2** with Tanzu

- Minio S3 Object Store
- Cloudian S3 Object Store

*Requires 3rd party plug-in

Any questions?

Thank You

Learn more at:

cormachogan.com