VMware Cloud-Native Applications

Container Challenges, que propose VMware

Corfdir francois @fcorfdir fcorfdir@syscom.nc
SYSCOM

vmware

vSphere Integrated Containers

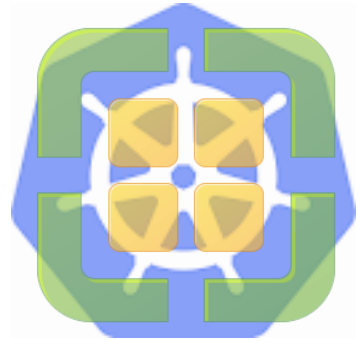
PHOTON CONTROLLER™

HARBOR

ADMIRAL™

Docker Volume Driver for vSphere

PHOTON OS™



Kubernetes on vSphere

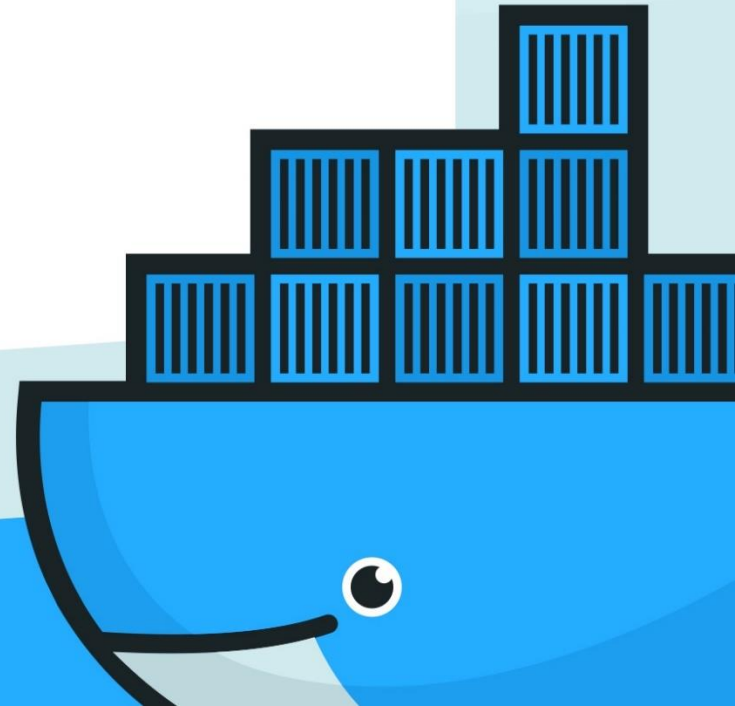
vmware

Problème #1

- Vos développeurs veulent utiliser des **Containers**
- En temps qu'administrateur vSphere vous pouvez fournir des machines virtuelles dans lesquelles vos développeurs peuvent déployer des containers
- Mais…
  - Les développeur veulent aussi du stockage **persistent** et **redondant** pour les données des containers
  - Dockers nous a dit que les containers sont **stateless**

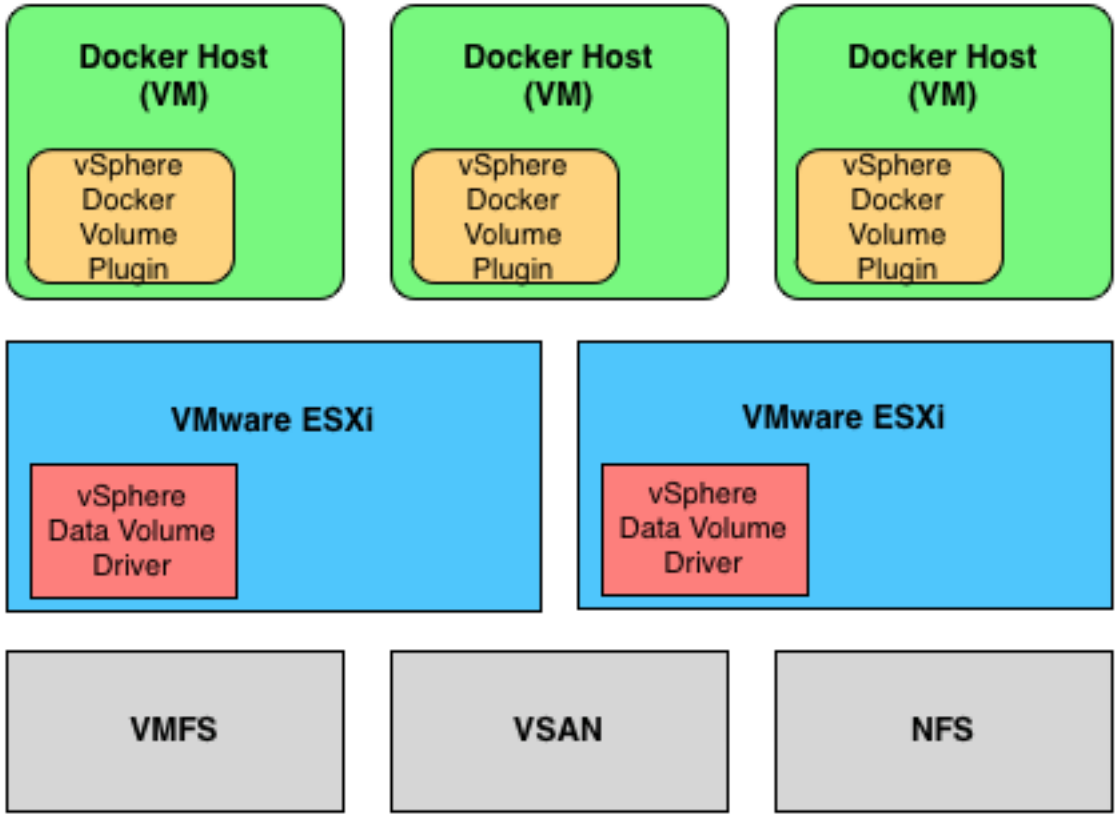
- Quelles sont mes options en temps qu'administrateur vSphere ?

“Docker is for stateless applications!”



Docker Volume Driver pour vSphere

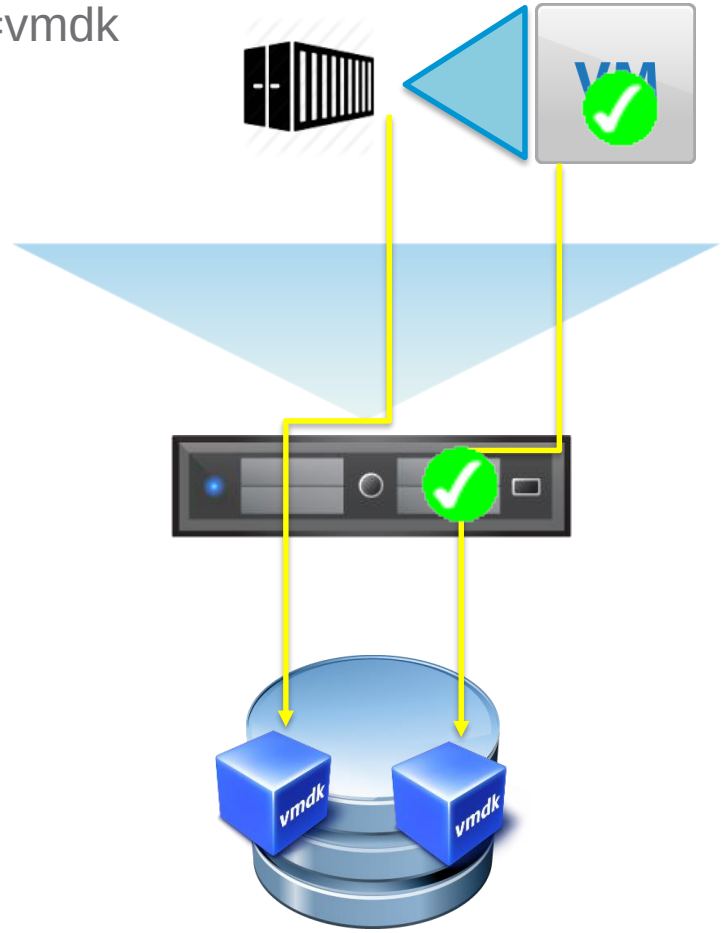
- Permet de créer des volumes “**stateful**” pour vos containers sous VMware
  - Repose sur votre stockage actue VMFS, NFS and vSAN
- 2 composants à installer :
  - VIB pour ESXi
  - RPM (docker VMDK plugin) pour les VM Docker
- Disponible sur tout les environnement VMware



https://github.com/vmware/docker-volume-vsphere

Docker Volume Driver for vSphere

```
# docker volume create --driver=vmdk
# docker run --volume <image>
```



RPM installed in VM

VIB installed on ESXi host

Docker Volume Driver for vSphere

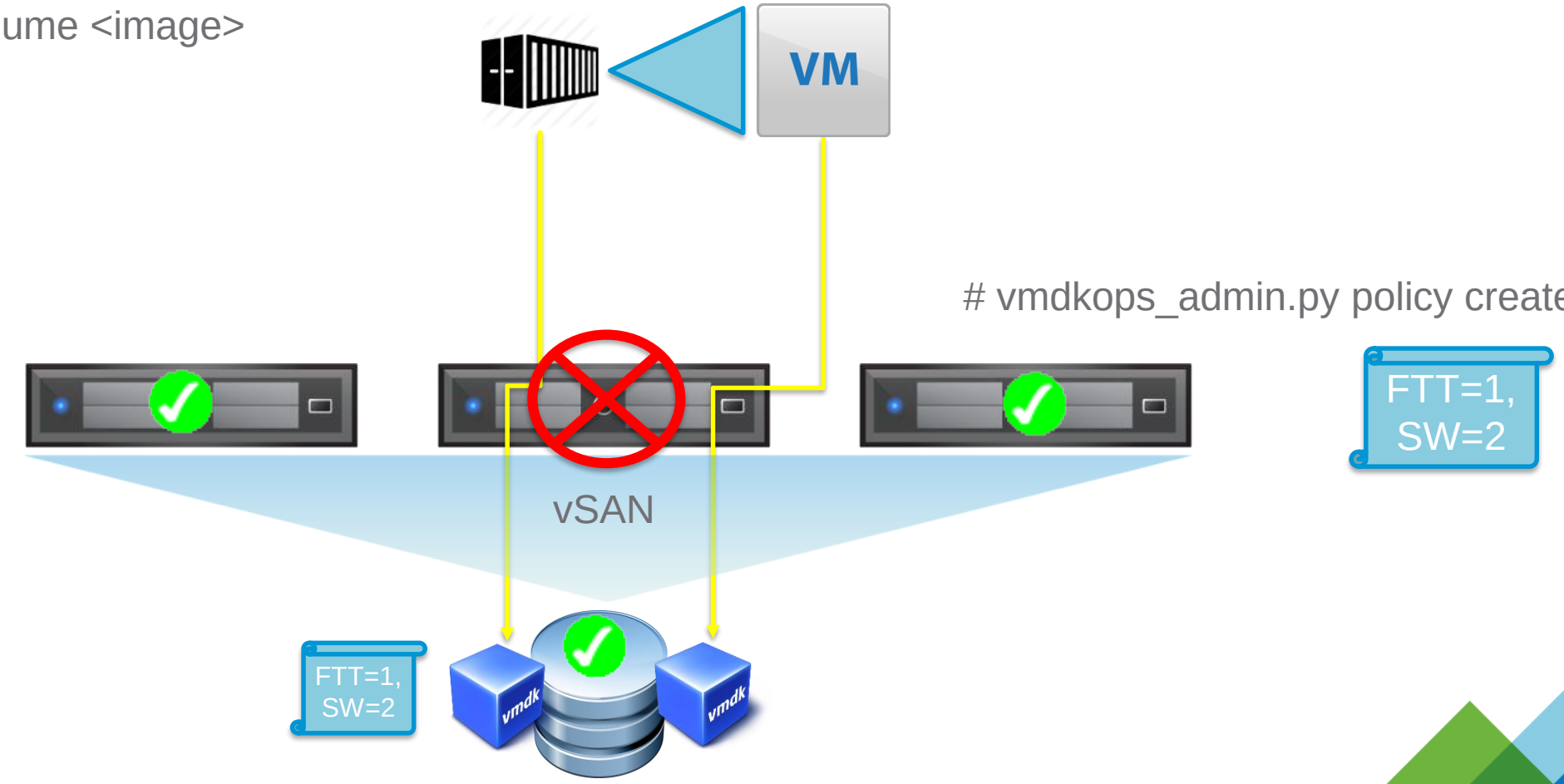

```
root@photon-machine [ ~ ]# docker volume create --driver=vmdk --name=MyVol -o size=20gb
MyVol
root@photon-machine [ ~ ]#
root@photon-machine [ ~ ]# docker volume ls
DRIVER              VOLUME NAME
vmdk                MyVol
root@photon-machine [ ~ ]#

root@photon-machine [ ~ ]# docker run -it -v MyVol:/MyVolume ubuntu bash

root@bd9410fb4c1d:/#
root@bd9410fb4c1d:/# ls
Myvolume  bin   boot  dev   etc   home  lib   lib64  media  mnt   opt   proc  \
root  run   sbin  srv   sys   tmp   usr   var
root@fe8c21d003fa:/#
```

MyVolume mounted in container image

Docker Volume Driver and vSAN

- Select a vSAN policy when creating a container volume

```
# docker volume create --driver=vmdk –o vsan_policy
# docker run –volume <image>
```



Docker Volume Driver and vSAN

```
[root@esxi-hp-08:~]  /usr/lib/vmware/vmdkops/bin/vmdkops_admin.py policy create \
--name FTT=0 \
--content  '("hostFailuresToTolerate" i0)'
Successfully created policy: FTT=0
[root@esxi-hp-08:~]
[root@esxi-hp-08:~] /usr/lib/vmware/vmdkops/bin/vmdkops_admin.py policy ls
Policy Name  Policy Content                  Active
-----------  -----------------------------  ------
FTT=0        ("hostFailuresToTolerate" i0)  Unused
```

```
root@photon[~] # docker volume create --driver=vmdk --name=corvol -o size=20gb -o vsan-policy-
name=FTT=0
corvol
root@photon[~] #
root@photon[~] # docker run -it -v corvol:/MyVolume ubuntu bash
root@0684feae5a02:/#
root@0684feae5a02:/# df | grep MyVolume
/dev/disk/by-path/pci-0000:13:00.0-scsi-0:0:0:0  20642428   44992  19548860   1% /MyVolume
```

```
[root@esxi-hp-08:~] /usr/lib/vmware/vmdkops/bin/vmdkops_admin.py policy ls
Policy Name  Policy Content                   Active
-----------  ------------------------------  ------------------
FTT=0        (("hostFailuresToTolerate" i0))  In use by 1 volumes
```

Problème #2

- Nos développeurs utilisent maintenant des Containers dans des VM dans notre cluster vSphere, avec des volumes persistants
- Mais…
  - Ils envoient et tirent leur code depuis un dépôt public sur internet
- donc...
  - C'est lent
  - Ce n'est pas sécurisé
  - Comment protéger ces images et les rendre plus disponibles ?
  - Les données de mon entreprise (propriété intellectuelle) sont envoyées sur Internet

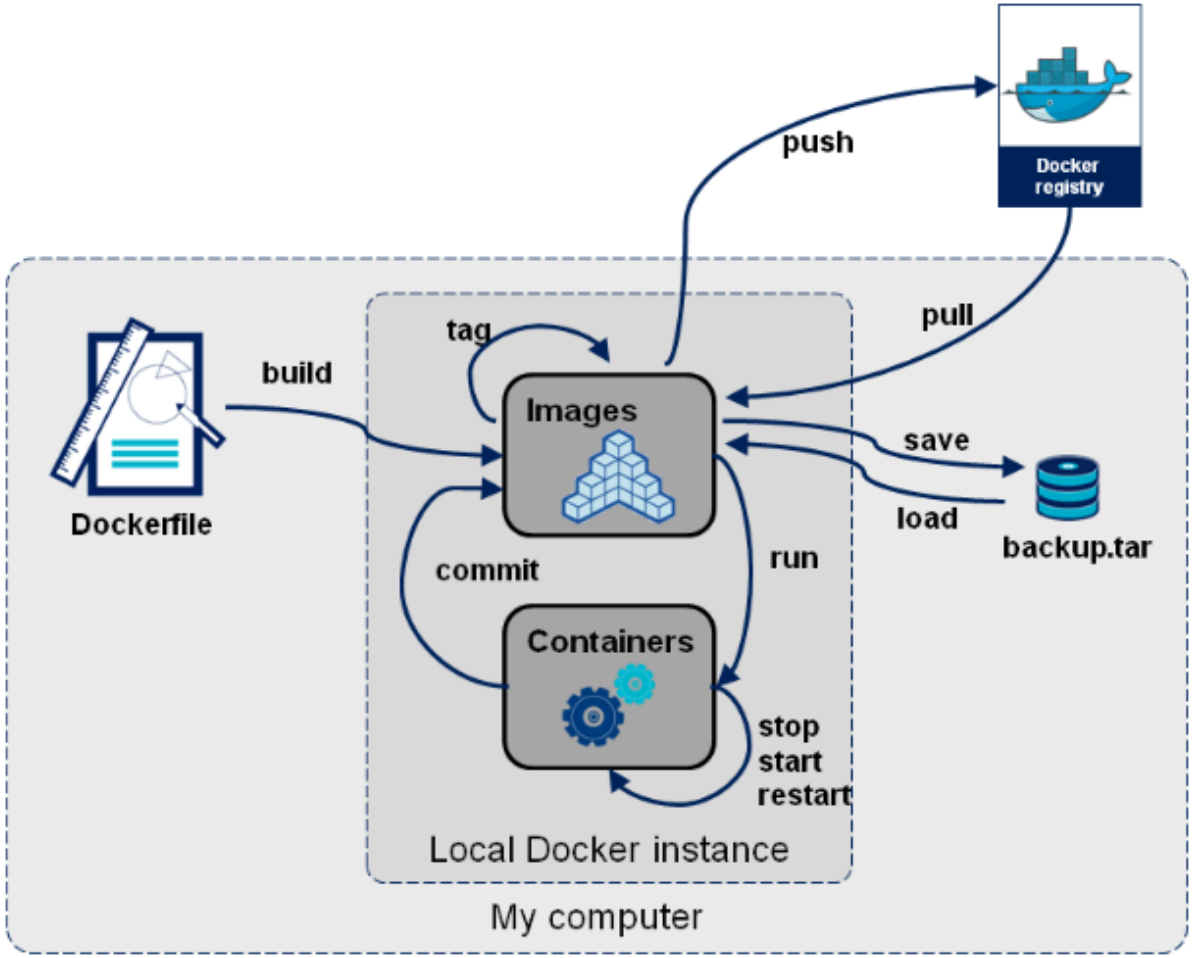
- On demande des solutions
- Qu'elle sont mes options en temps qu'administrateur vSphere?

Project Harbor

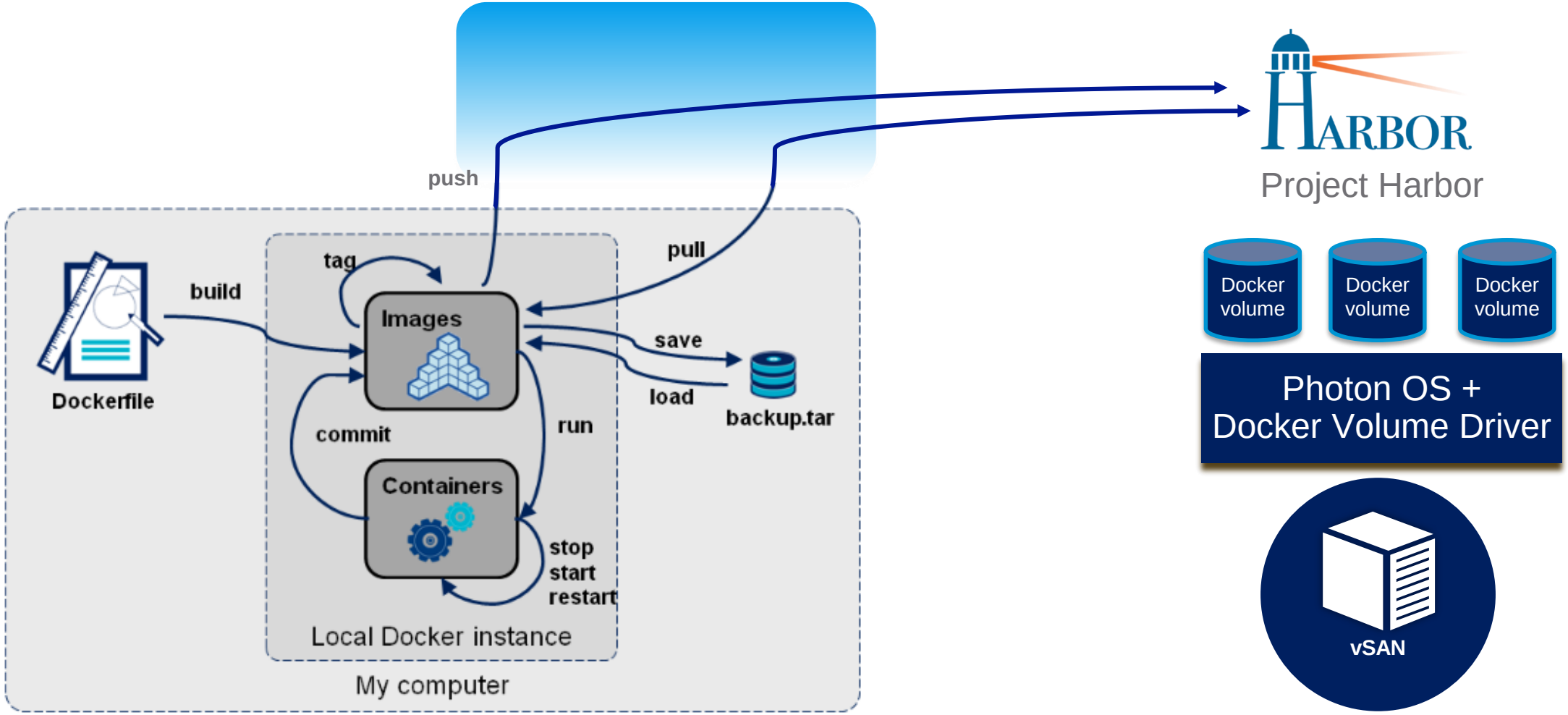
- Enterprise-class registry serveur pour Docker images
- Ajoute des fonctionnalités de management, audit, securité, performance, Role Base Access Contrôle
  - Améliore le transfert des environnements (registry is closer to the build/run environment)
  - La propriété intellectuelle reste dans l'entreprise derrière le Firewall
  - Contrôle du push/pull des images par des droits
  - Hautement disponible par la réplication des images

https://github.com/vmware/harbor

Déploiement typique – utilisant le docker Registry



Project Harbor + Docker Volume Driver + vSAN



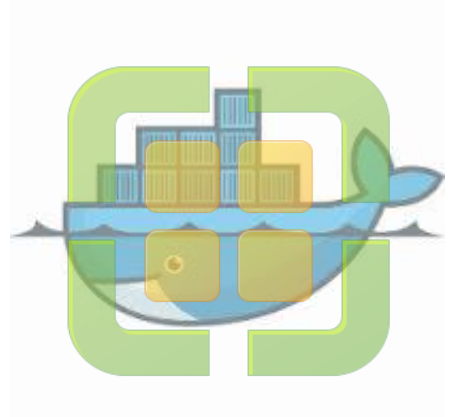
Highly available, persistent storage for container images

Problème #3

- Vos développeurs utilisent maintenant des containers dans des VM sur vSphere avec Harbor
- Mais …
  - **Je ne sais pas du tout ce qu'ils font dans leurs containers !!!**
- Quelles ressources consomment les containers ?
- Quel stockage consomment les containers ?
- Avec quel réseau ils communiquent ?
- Quels ports réseau utilisent- ils?

- Comment je gère mes containers en production on day#2 opérations?
  - Monitor/Manage/Backup/Recover/Security/Auditing
- Quelles sont mes options en temps qu'administrateur vSphere?

vSphere Integrated Containers



- Pour les **Dev** : Docker API endpoint sans Docker
- Pour les **Ops** : container tournent comme des VM dans vSphere
- App Team et IT team utilisent maintenant le même système de “virtualization”

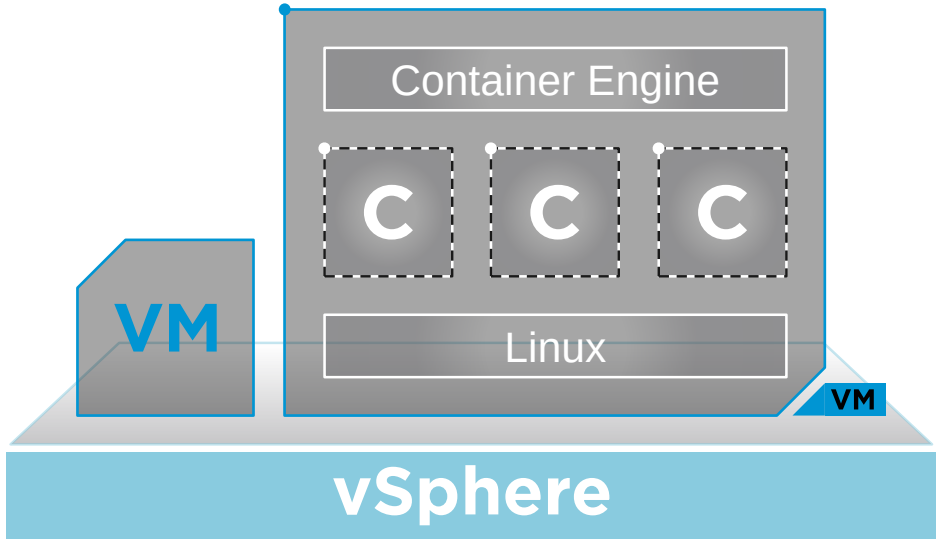
- VIC (dans vSphere) nous permet d’avoir de la visibilité de nos ressources, du réseau et du stockage
- Sécurité et audit font partie de la VM et peuvent être appliqués sur le “container as VMs”.

- VIC fait partie de **vSphere 6.5** et du support.

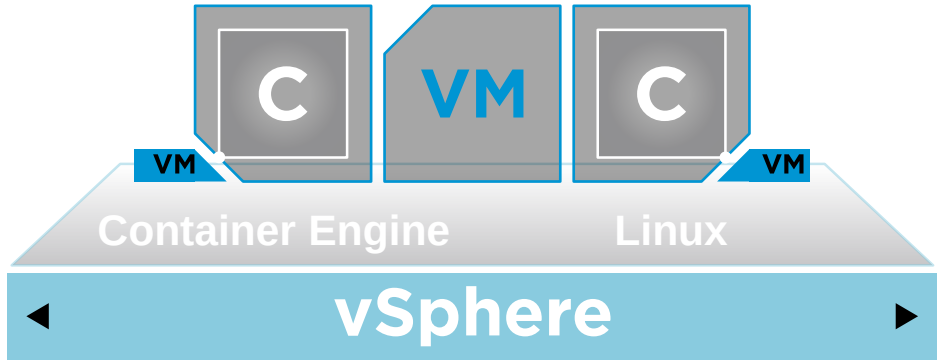
https://github.com/vmware/vic

Intégration des containers dans le noyaux de vSphere

Basic VM Approach

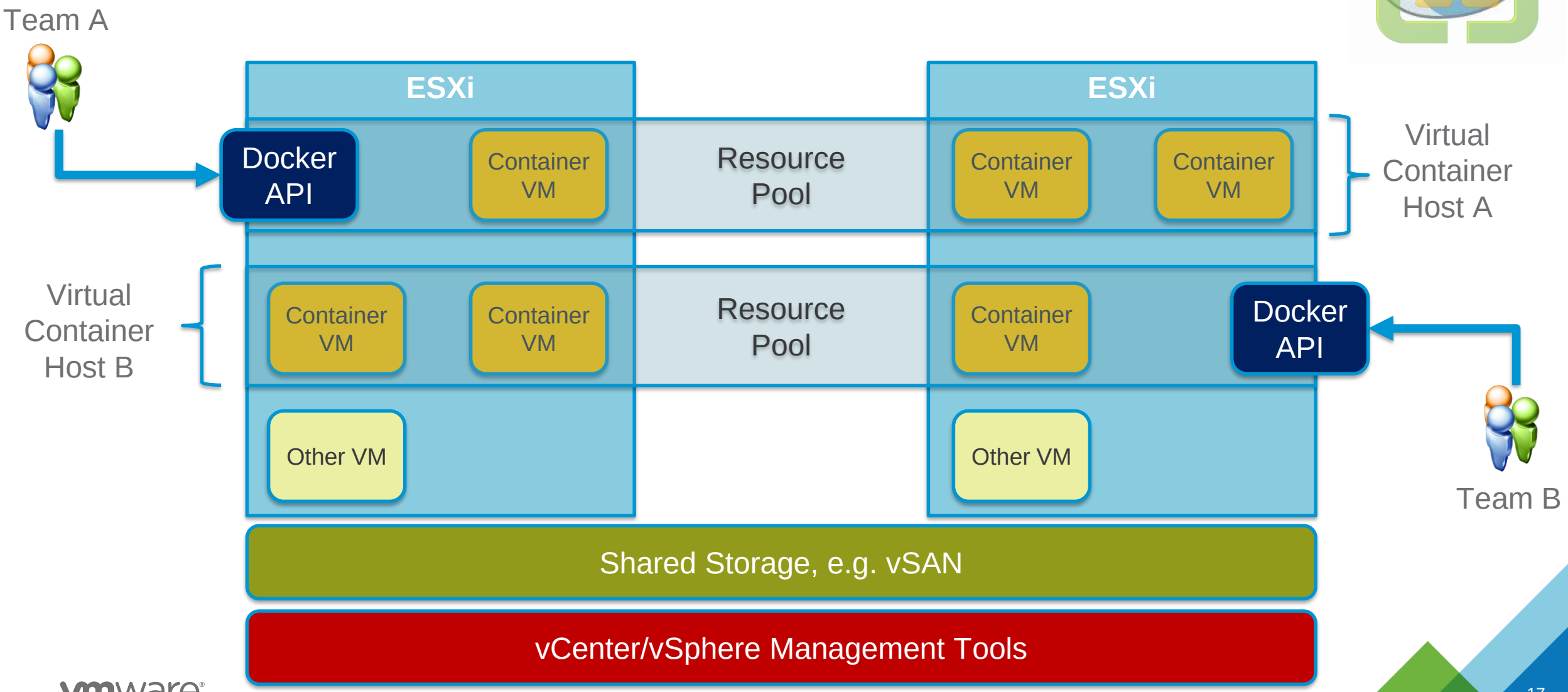


vSphere Integrated Containers



Developers + Operators use the same abstraction

vSphere Integrated Containers – Docker without Docker



vSphere Integrated Containers – VCH deploy (1 of 2)

```
root@photon-NaTv5i8IA [ /workspace/vic27 ]# vic-machine-linux create  \
--bridge-network Bridge-DPG \
--image-store isilion-nfs-01 \
-t 'administrator@vsphere.local:VMware123!@10.27.51.103'  \
--compute-resource Mgmt/COR_RP
INFO[2016-07-11T11:58:36Z] ### Installing VCH ####
INFO[2016-07-11T11:58:36Z] Generating certificate/key pair - private key in ./virtual-container-
host-key.pem
INFO[2016-07-11T11:58:37Z] Validating supplied configuration
INFO[2016-07-11T11:58:37Z] Firewall status: DISABLED on /CNA-DC/host/Mgmt/10.27.51.8
INFO[2016-07-11T11:58:37Z] Firewall configuration OK on hosts:
INFO[2016-07-11T11:58:37Z]   /CNA-DC/host/Mgmt/10.27.51.8
INFO[2016-07-11T11:58:37Z] License check OK on hosts:
INFO[2016-07-11T11:58:37Z]   /CNA-DC/host/Mgmt/10.27.51.8
INFO[2016-07-11T11:58:37Z] DRS check OK on:
INFO[2016-07-11T11:58:37Z]   /CNA-DC/host/Mgmt/Resources/COR_RP
```

vSphere Checks

vSphere Integrated Containers – VCH deploy (2 of 2)

VCH deploy

Docker API

```
INFO[2016-07-11T11:58:38Z] Creating Resource Pool virtual-container-host
INFO[2016-07-11T11:58:38Z] Creating appliance on target
INFO[2016-07-11T11:58:38Z] Network role client is sharing NIC with external
INFO[2016-07-11T11:58:38Z] Network role management is sharing NIC with external
INFO[2016-07-11T11:58:39Z] Uploading images for container
INFO[2016-07-11T11:58:39Z]     bootstrap.iso
INFO[2016-07-11T11:58:39Z]     appliance.iso
INFO[2016-07-11T11:58:44Z] Registering VCH as a vSphere extension
INFO[2016-07-11T11:58:50Z] Waiting for IP information
INFO[2016-07-11T11:59:09Z] Waiting for major appliance components to launch
INFO[2016-07-11T11:59:09Z] Initialization of appliance successful
INFO[2016-07-11T11:59:09Z]
INFO[2016-07-11T11:59:09Z] SSH to appliance (default=root:password)
INFO[2016-07-11T11:59:09Z] ssh root@10.27.32.87
INFO[2016-07-11T11:59:09Z]
INFO[2016-07-11T11:59:09Z] Log server:
INFO[2016-07-11T11:59:09Z] https://10.27.32.87:2378
INFO[2016-07-11T11:59:09Z]
INFO[2016-07-11T11:59:09Z] DOCKER_HOST=10.27.32.87:2376
INFO[2016-07-11T11:59:09Z]
INFO[2016-07-11T11:59:09Z] Connect to docker:
INFO[2016-07-11T11:59:09Z] docker -H 10.27.32.87:2376 --tls info
INFO[2016-07-11T11:59:09Z] Installer completed successfully
```

Give this docker API endpoint o your developer

vmware

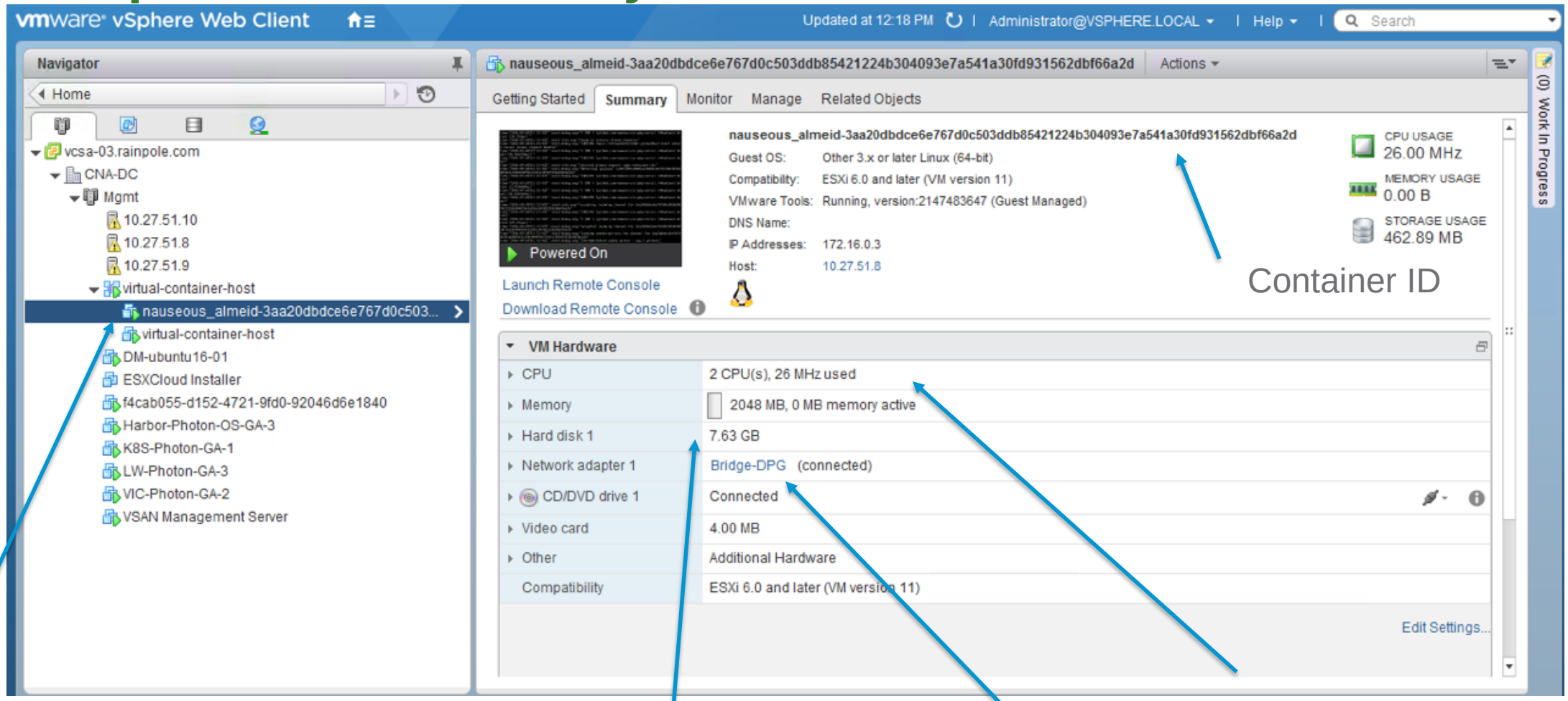
As far as a developer is concerned, this is docker!

```
root@photon-NaTv5i8IA [ /workspace/vic ]# docker -H 10.27.51.18:2376 --tls run -it ubuntu bash
Unable to find image 'ubuntu:latest' locally
Pulling from library/ubuntu
a3ed95caeb02: Pull complete
6bbedd9b76a4: Pull complete
fc19d60a83f1: Pull complete
de413bb911fd: Pull complete
2879a7ad3144: Pull complete
668604fde02e: Pull complete
Digest: sha256:312986132029d622ae65423ca25d3a3cf4510de25c47b05b6819d61e2e2b5420
Status: Downloaded newer image for library/ubuntu:latest
root@6c8d6a4add24:/#
root@6c8d6a4add24:/# ls
bin  boot  dev  etc  home  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv
sys  tmp  usr  var
root@6c8d6a4add24:/#
```

Ubuntu shell

vmware

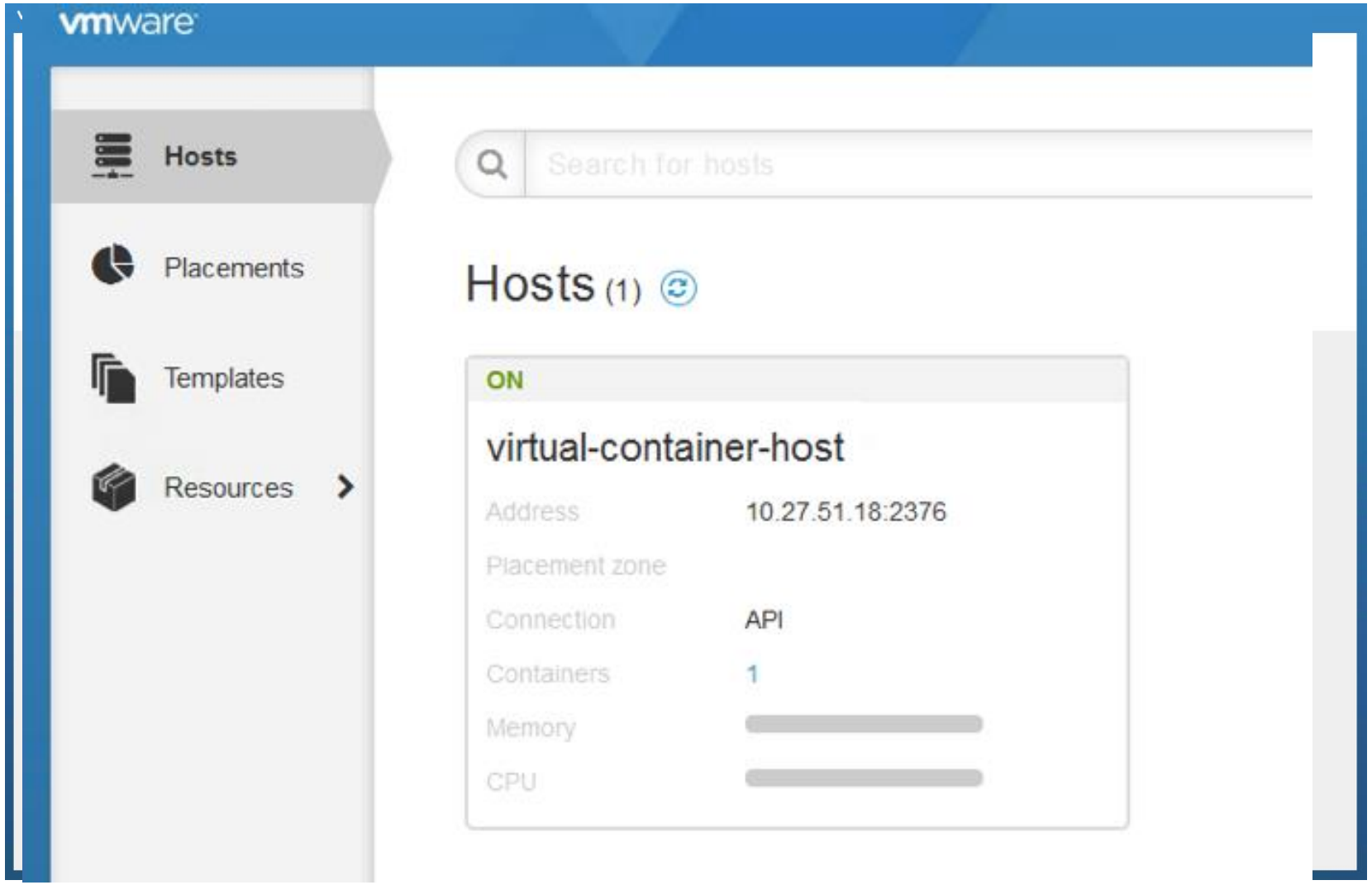
Admin/Ops have full visibility of Container as a VM



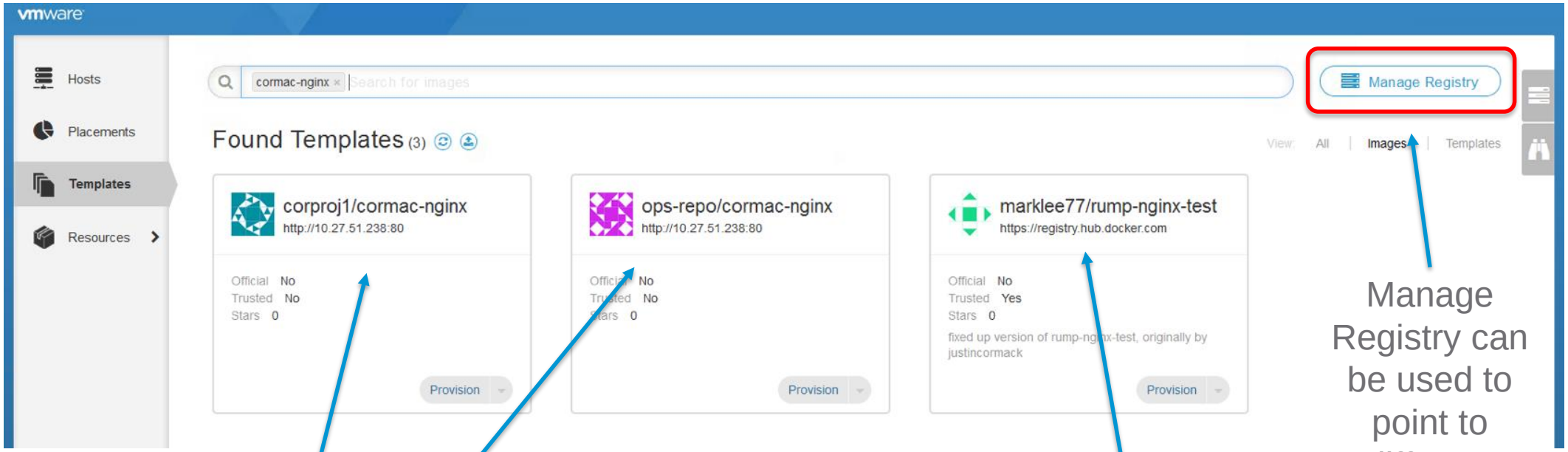
Problème #4

- Vos développeurs utilisent maintenant **vSphere Integrated Containers**
- Mais…
  - Ils veulent des outils d‘automatisation et d‘orchestration pour déployer les containers dans VIC
  - Ils veulent une repository local à la place de docker hub comme le propose « project Harbor »
- Quelles sont mes options en temps qu’administrateur vSphere?

Admiral - Container Lifecycle Management



Harbor + Admiral + vSphere Integrated Containers



These are from a Harbor deployment

This is from docker hub

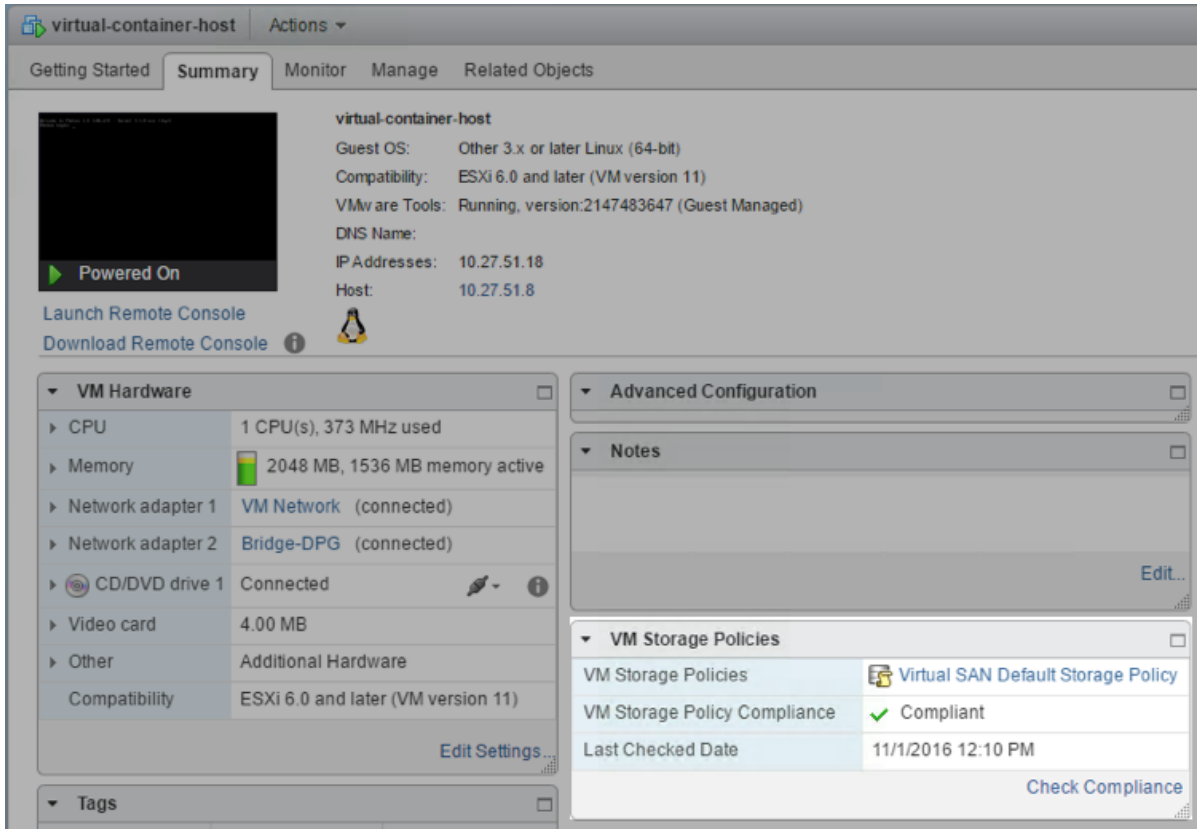
Manage Registry can be used to point to different registries, including Harbor

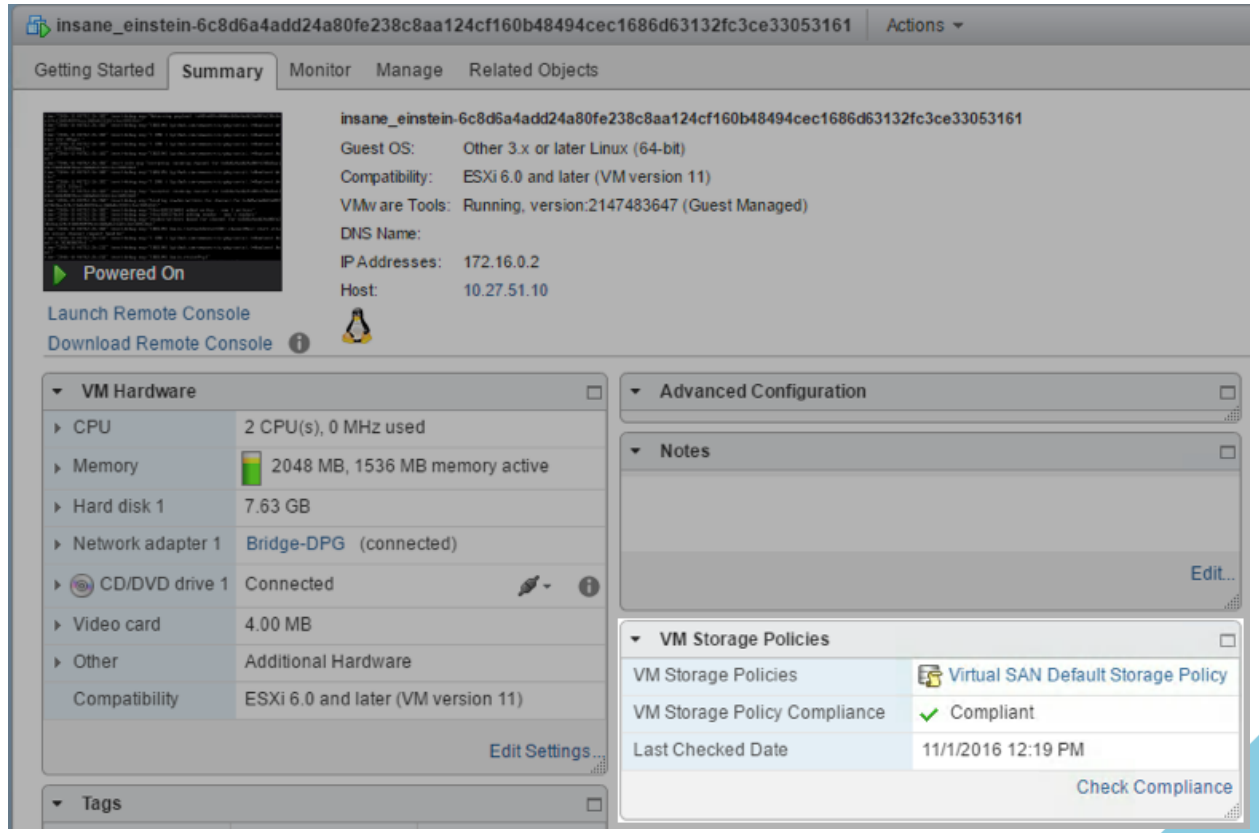
Problème #5

- Vos développeur utilisent **vSphere Integrated Containers + Admiral + Harbor**
- Mais …
  - J‘aimerais leur donner une solution de haute disponibilité, définie par des règles software, sur un stockage persistant.
- Quelles sont mes options en temps qu’administrateur vSphere?

vSAN for vSphere Integrated Containers

- Storage Policies peuvent être appliqué sur des VIC “Containers”, de la même façon que sur des VM





VCH

Container

Problème #6

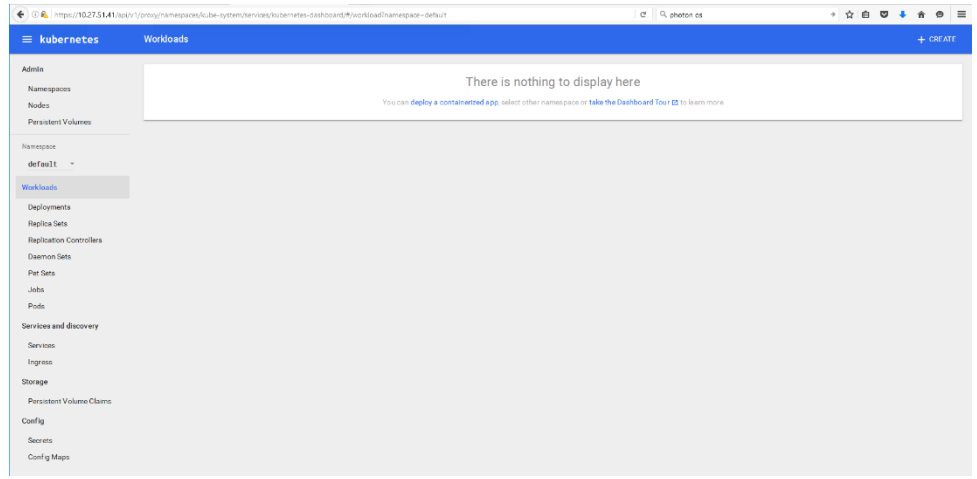
- Mes développeurs m'ont demandé de déployer **Kubernetes** sur mon Infrastructure vSphere
- Mais..
  - **Kuber #€!!@@ ? Longin c'est quoi ton machin**

- Kubernetes est une application populaire permettant la gestion automatisé du déploiement, l'extensibilité (scaling) de la gestion des applications containerisées sur des cluster.
- Cela semble compliqué !
- Quelles sont mes options en temps qu'administrateur vSphere?

Kubernetes (K8S) deployed natively on vSphere

- Depuis la version Kubernetes 1.4.5 (October 2016) via kube-up/kube-down
- Téléchargement de l'ova K8S et du VMDK image (Debian)
- Enregistrer K8S dans votre vSphere Infrastructure
- Auto déploiement des VMs et des containers associés, pour créer le K8S

```
root@photon-39BgfUQRO [ ~/kubernetes ]# KUBERNETES_PROVIDER=vsphere cluster/kube-up.sh
... Starting cluster using provider: vsphere
... calling verify-prereqs
... calling kube-up
Starting master VM (this can take a minute)...
Powering on VirtualMachine:vm-1228... OK
kubernetes-server-linux-amd64.tar.gz                                  100%  336MB
18.7MB/s   00:18
kubernetes-salt.tar.gz                                                100%   53KB
52.5KB/s   00:00
uploaded /tmp/kubernetes.k2DE84/master-start.sh to /tmp/master-start.sh
Using master: kubernetes-master (external IP: 10.27.51.41)

Starting node VMs (this can take a minute)...
Powering on VirtualMachine:vm-1229... Powering on VirtualMachine:vm-1230... Powering on
VirtualMachine:vm-1231... Powering on VirtualMachine:vm-1232... OK
OK
OK
OK
kubernetes-minion-2-ip                                                100%   69
0.1KB/s   00:00
kubernetes-minion-4-ip                                                100%   69
0.1KB/s   00:00
kubernetes-minion-3-ip                                                100%   69
0.1KB/s   00:00

uploaded /tmp/kubernetes.k2DE84/node-start-3.sh to /tmp/node-start-3.sh
uploaded /tmp/kubernetes.k2DE84/node-start-0.sh to /tmp/node-start-0.sh
uploaded /tmp/kubernetes.k2DE84/node-start-2.sh to /tmp/node-start-2.sh
uploaded /tmp/kubernetes.k2DE84/node-start-1.sh to /tmp/node-start-1.sh
Found kubernetes-minion-1 at 10.27.51.50
Found kubernetes-minion-2 at 10.27.51.47
Found kubernetes-minion-3 at 10.27.51.42
Found kubernetes-minion-4 at 10.27.51.49
```



Problème #7

- Nous avons de nombreux développeurs, chacun a ses préférence pour l'administration et le déploiement des containers
- Certains utilisent **Kubernetes**
- D'autres **Mesos + Marathon**
- D'autres **Pivotal Cloud Foundry**
- D'autres **Docker Swarm**

- Cela implique d'avoir des centaines de serveurs !!!

- Que me propose VMware ?

Future Looking

Photon Controller / Photon Platform

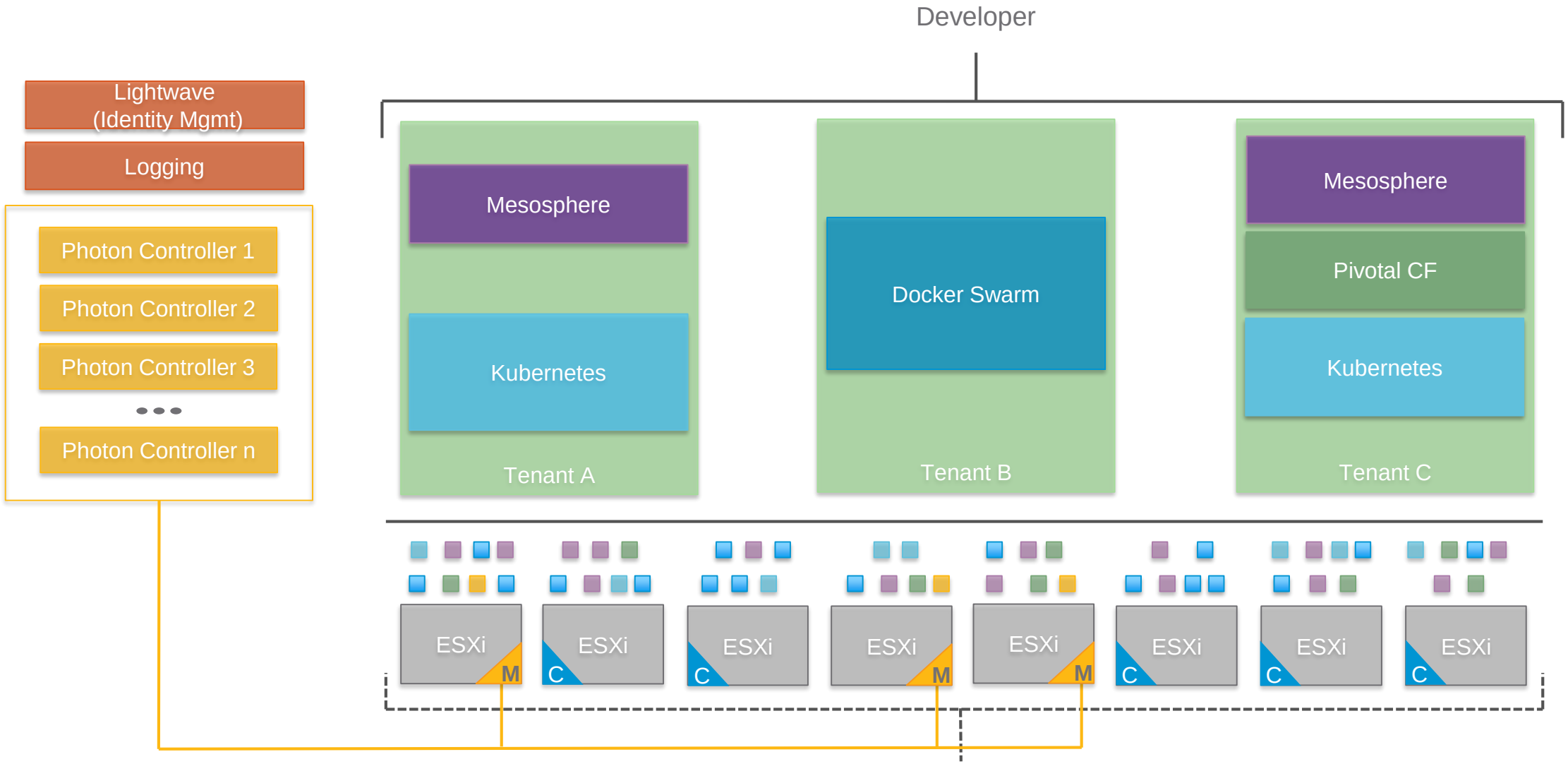
- Photon Platform est la suite qui inclus ESXi et Photon Controller technologies, comme vSphere est la suite qui inclus ESXi et vCenter.

- Il n'y a pas de vSphere/vCenter dans ce modèle. La philosophie de cette plateforme est de n'héberger que des containers

- Déployer un hyperviseur de containers (Photon Machine aka ESXi)
- Déployer un contrôleur de cluster (Photon Controller)
- Créer une VM comme Docker host (Photon OS)
- Faire fonctionner des containers à travers le Docker host

Container management and orchestration is out of scope for the Photon technologies

Photon Platform - Architecture

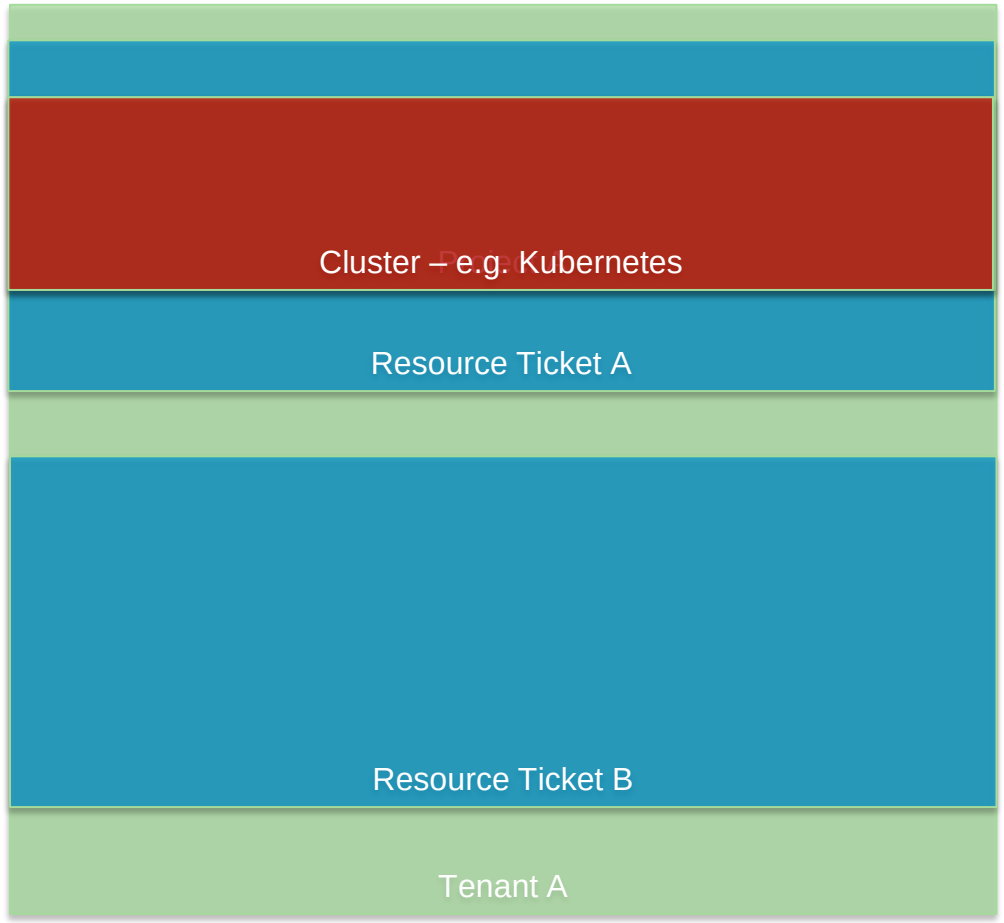


Tenants, Resource Tickets, Projects and Clusters

photon project create

photon cluster create

photon resource-ticket create



photon tenant create

Support

- Photon Platform supporter par Pivotal Cloud Foundry depuis **March 2016**

- Stand-alone Photon Platform for Kubernetes As A Service announced at VMworld 2016.

- Other container orchestration and clustering solutions, such as Mesos and Docker Swarm, are available but are not yet supported.

Photon Platform

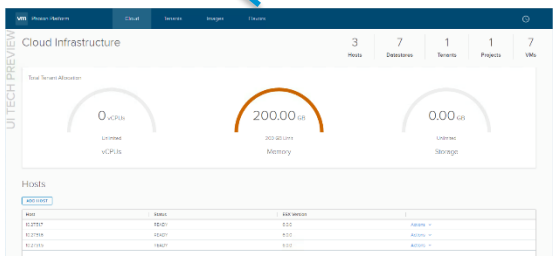
Management Infrastructure

installer OVA VM Controller(s)

API/CLI

UI

photon tenant
photon target
photon project
…



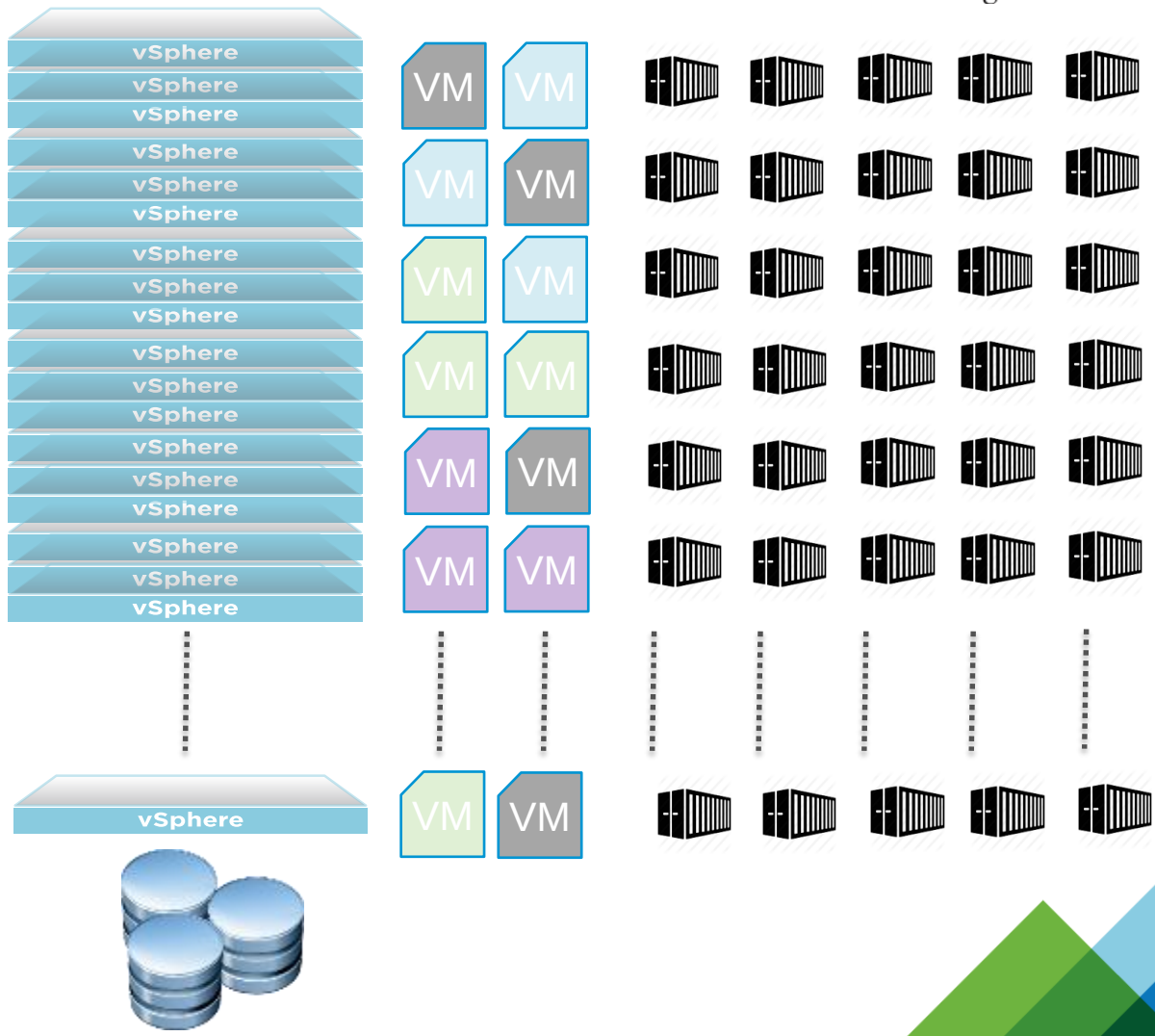
Cloud Infrastructure

Pivotal Cloud Foundry

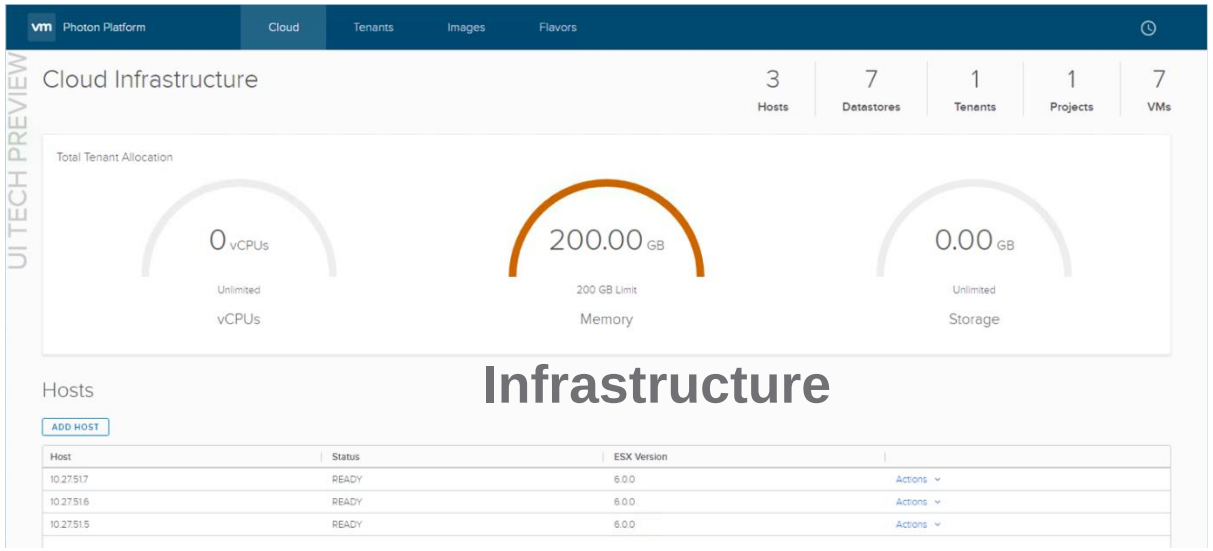
MESOS

kubernetes by Google

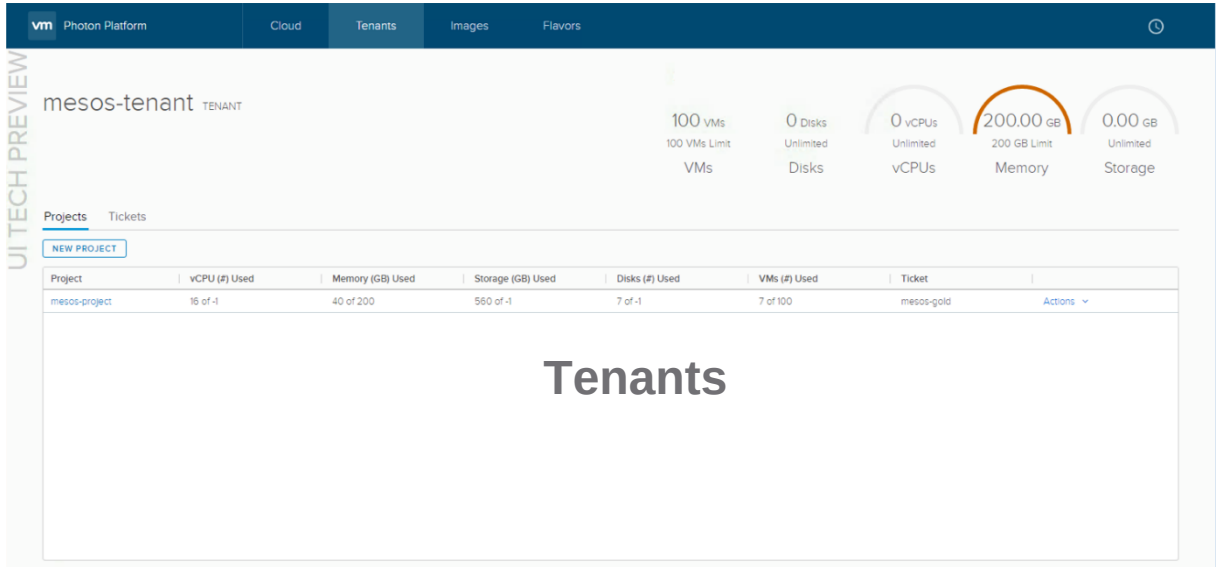
docker SWARM



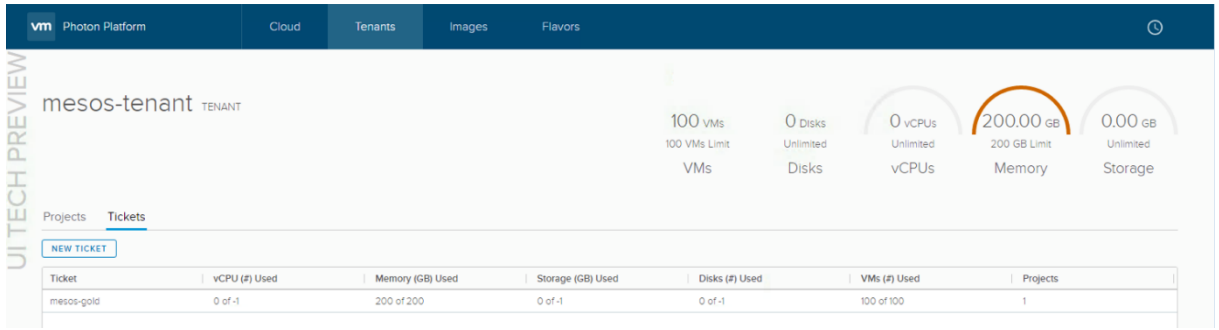
Photon Platform UI - IT Ops view



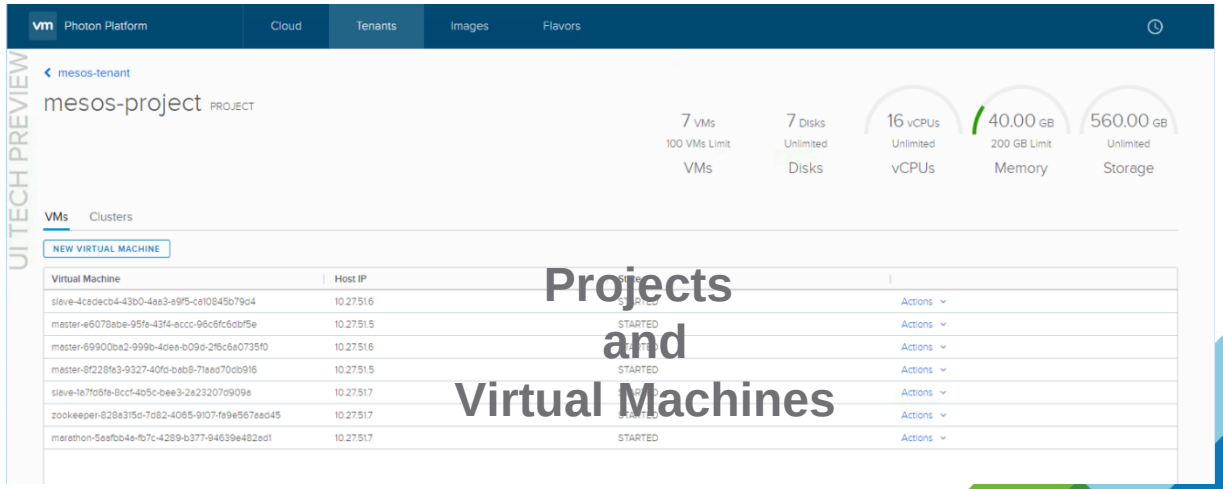
Infrastructure



Tenants

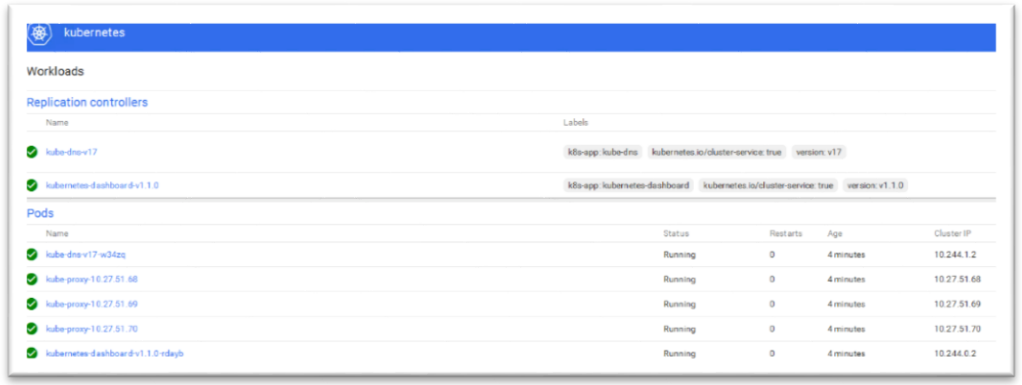


Resource Tickets

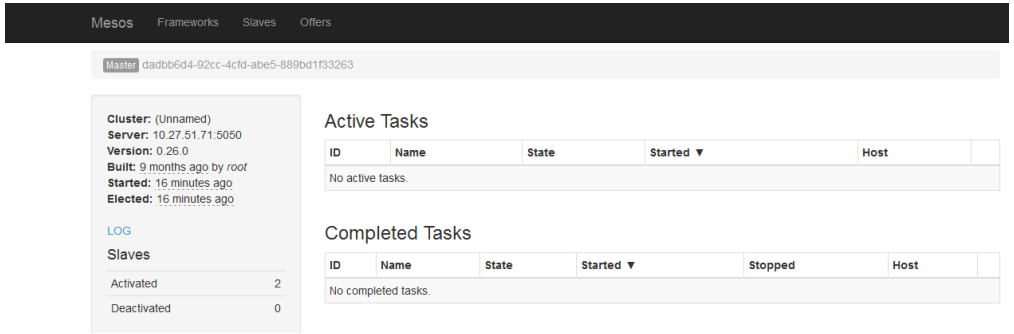


Projects and Virtual Machines

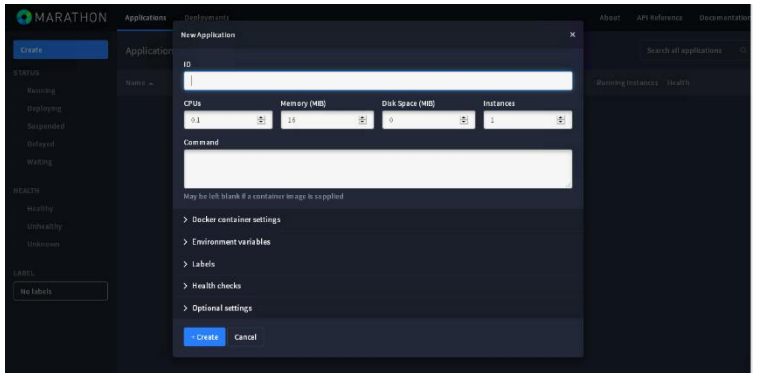
Developer View



Kubernetes



Mesos



Marathon

```
root@cs-dhcp32-29:~# docker-machine ls
NAME                 ACTIVE   DRIVER    STATE     URL                         SWARM                           DOCKER    ERRORS
consul-machine       -        photon    Running   tcp://10.27.51.53:2376                                      v1.11.2
swarm-node-1-master  *        photon    Running   tcp://10.27.51.54:2376      swarm-node-1-master (master)    v1.11.2
swarm-node-2         -        photon    Running   tcp://10.27.51.55:2376      swarm-node-1-master             v1.11.2
swarm-node-3         -        photon    Running   tcp://10.27.51.56:2376      swarm-node-1-master             v1.11.2
root@cs-dhcp32-29:~# eval $(docker-machine env swarm-node-1-master)
root@cs-dhcp32-29:~# docker ps -a
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS                      PORTS                                NAMES
87373378dfd0        hello-world         "/hello"                 8 weeks ago         Exited (0) 8 weeks ago                                           backstabbing_colden
ecbaa8600061        swarm:latest        "/swarm join --advert"   9 weeks ago         Up 9 weeks                  2375/tcp                             swarm-agent
a128e3b9145a        swarm:latest        "/swarm manage --tlsv"   9 weeks ago         Up 9 weeks                  2375/tcp, 0.0.0.0:3376->3376/tcp     swarm-agent-master
root@cs-dhcp32-29:~#
```

Docker swarm

VMworld 2016 Announcement – Kubernetes AAS

- Simplifie l'administration du frameworks on Photon Platform
- Annoncé au VMworld 2016 a Barcelone, Photon Platform permet au développeur de délivrer Kubernetes comme service pour l'administration de plusieurs tenants depuis un pool de ressource commun
- Les Tenants ont accès aux API, CLI et GUI pour créer leur cluster kubernetes dédier "on the fly".
- Les utilisateurs ont un cluster Kubernetes dédié isolé des autres tenants.
- Photon Platform automatise le "provisionnement" et la "haute disponibilité" de ce cluster, en automatisant le replacement des nœuds en panne sans intervention humaine.

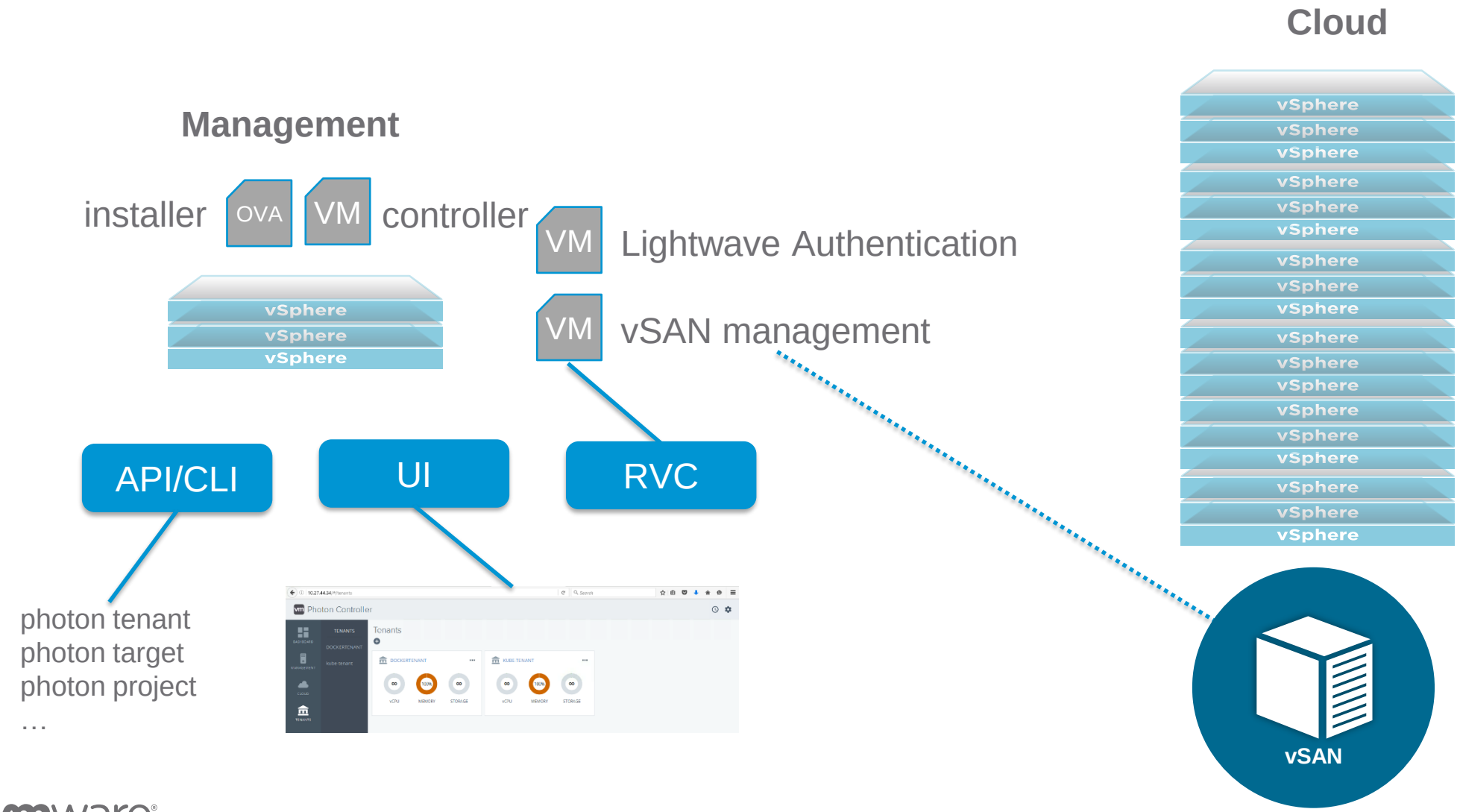
kubernetes by Google

Problème #8

- J’ai maintenant une plateforme photon déployée. J’ai de nombreux serveur ESXi, mais pas de vSphere
- Certains développeurs utilisent **Kubernetes**, **Mesos**, **Pivotal Cloud Foundry**, **Docker Swarm**…
- Mais...
  - Je dois fournir une solution de de stockage hautement disponible, administrée de façon logicielle et compatible avec tout
- Que me propose VMware ?

Future Looking

vSAN for Photon Platform



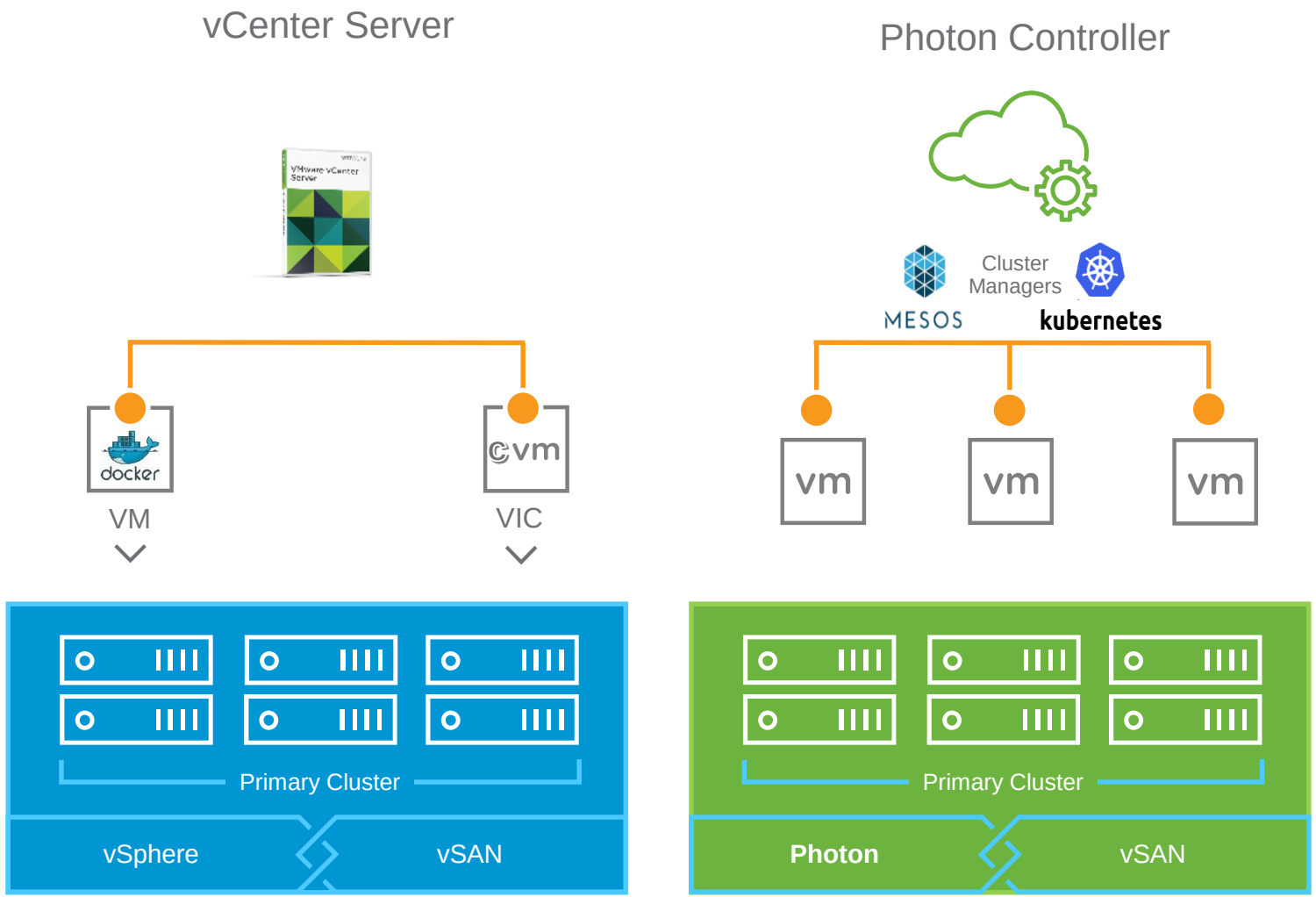
Problème #9

- J’ai de nombreuses applications “cloud Native Apps” proposées par VMware pour mes développeurs
- **Docker Volume Drive for vSphere**
- **Kubernetes running natively on vSphere**
- **vSphere Integrated Containers** avec **Admiral** et **Harbor**
- **Photon Platform**

- Quelle est ma meilleur option ?

Future Looking

vSAN – Hyper Converged Storage for Cloud Native Apps



Docker Volume driver for vSphere
Compatible directement avec Docker volumes
Politique de redondance par volume

---

vSphere Integrated Containers
Docker API Compatibility
VM-like container isolation
Politique de redondance par volume

DevOps Focus with Photon:
Native Container platform
Storage Operations: Managed solely via APIs for agile, scalable storage lifecycle operations

vmware


Q&A
Merci
vmware