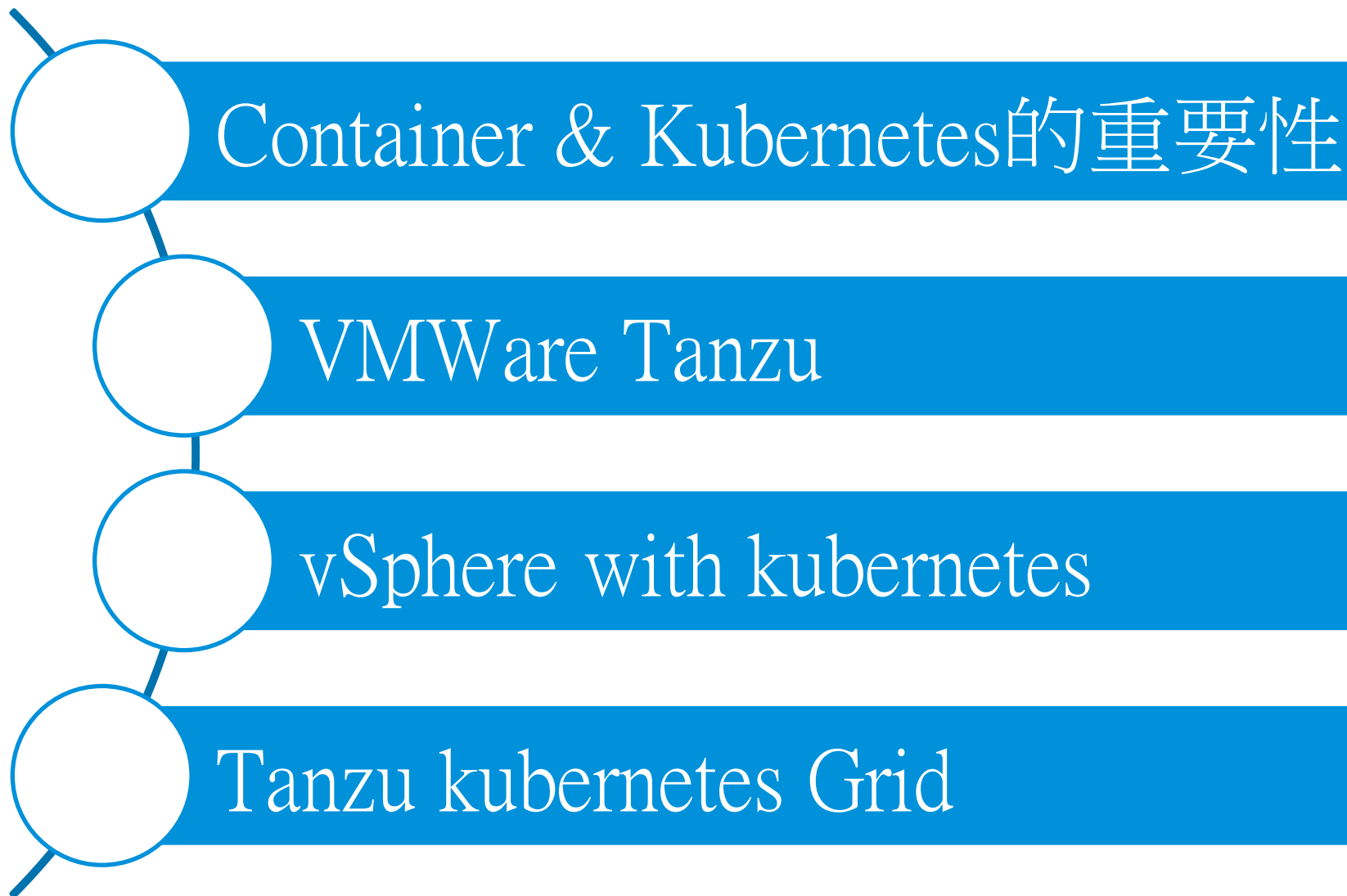


# VMware 透過 Kubernetes 重新架構 IT 世界 新一代容器架構平台

Resin Yan  
Zerone Engineer  
2020

## Agenda

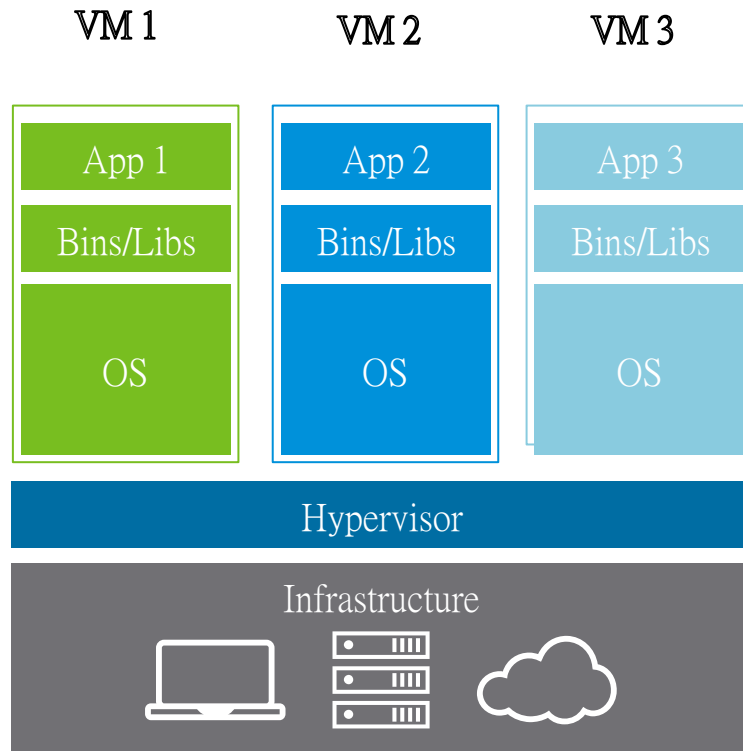


# Container & Kubernetes的重要性

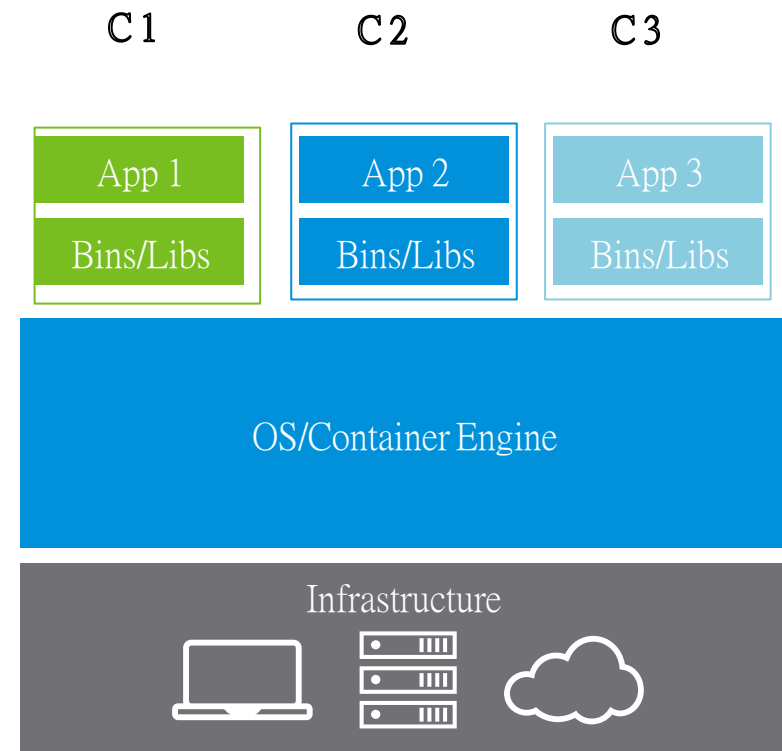
新型態平台架構

# 什麼是容器？

虛擬機 vs 容器



虛擬機



容器

# 虛擬機/容器

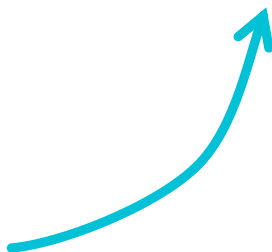


feature	虛擬機	容器
開機時間	分鐘	秒級
占用硬碟空間	通常幾GB	通常幾MB
運算效能	慢上許多	接近原生
支援上限	通常十到一百個	超過幾百個

# 導入容器方案的考量

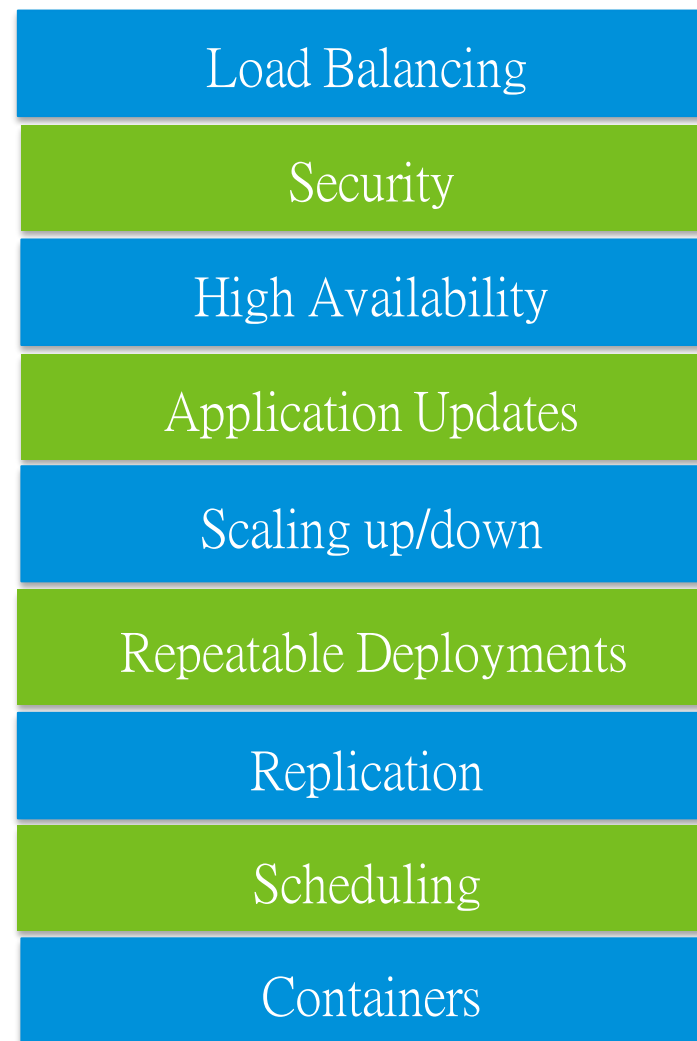
CONTAINERS IN  
DEVELOPMENT

學習 Gaps



Containers

CONTAINERS IN  
PRODUCTION



# Container 管控平台戰爭已經結束：贏家是Kubernetes



# What is Kubernetes (K8s)

Kubernetes, 是一個開源的容器調度平台，提供在分散式叢集環境中進行容器自動化部署、調度、擴展縮容、健康檢查等工作。

## 功能:

- 快速部署應用，維持應用狀態
- 自動擴展縮容
- 滾動式升級
- 資源調度

## 定位:

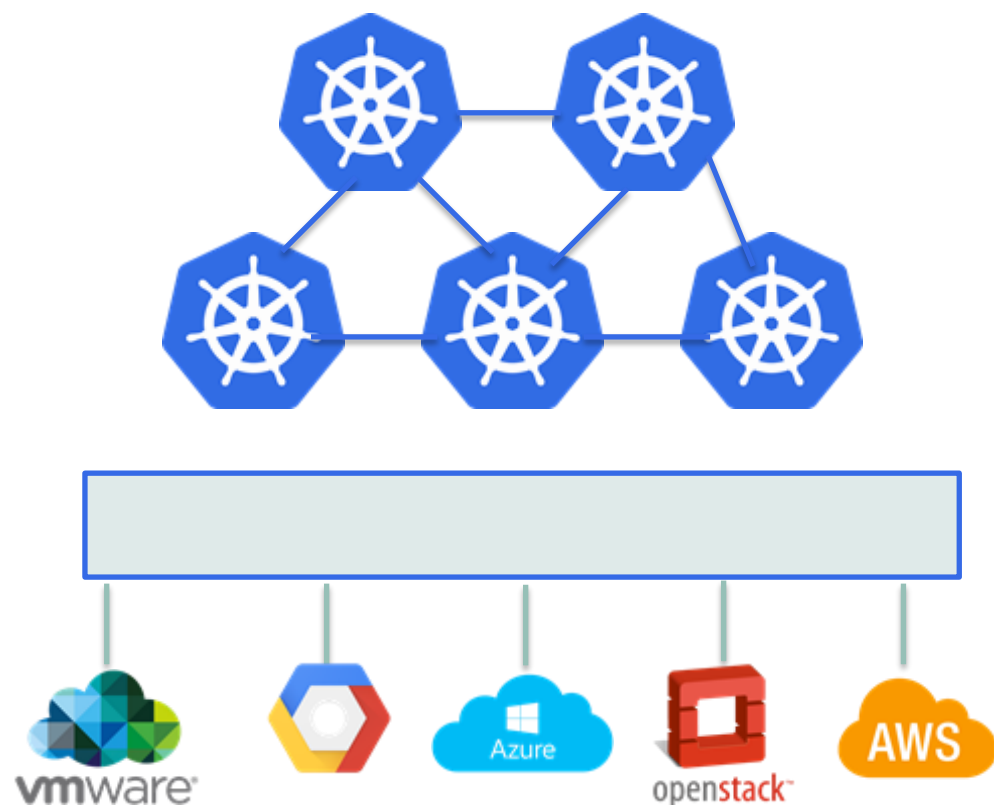
- 容器調度、CaaS



# kubernetes



# Kubernetes 在正式環境中維運的不足



**高可用性.** 叢集節點本身不具備開箱即用的可用性，(Masters, Workers and etcd nodes)。

**伸展性.** Kubernetes叢集處理節點上的pod / 服務，但沒有提供擴展的機制給Workers, Masters 和 etcd 虛擬機。

**網路安全.** Kubernetes有自己的網路設定，但是其功能薄弱，無法符合企業需求。

**健康檢查和治愈.** Kubernetes叢集只對運行在節點上的工作負載的健康進行常規的健康檢查。

**升級.** 在大型叢集上進行滾動升級是很困難的。誰管理它運行的系統？

# VMware Tanzu

VMWare Kubernetes 平台

隆重介紹

# VMware Tanzu

建置新一代應用平台

執行完整的 Kubernetes 平台

為開發人員與 IT 管理 Kubernetes



# VMware Tanzu

開發

新一代應用平台

Bitnami | Pivotal

執行

企業級 Kubernetes

vSphere with kubernetes | Tanzu Kubernetes grid

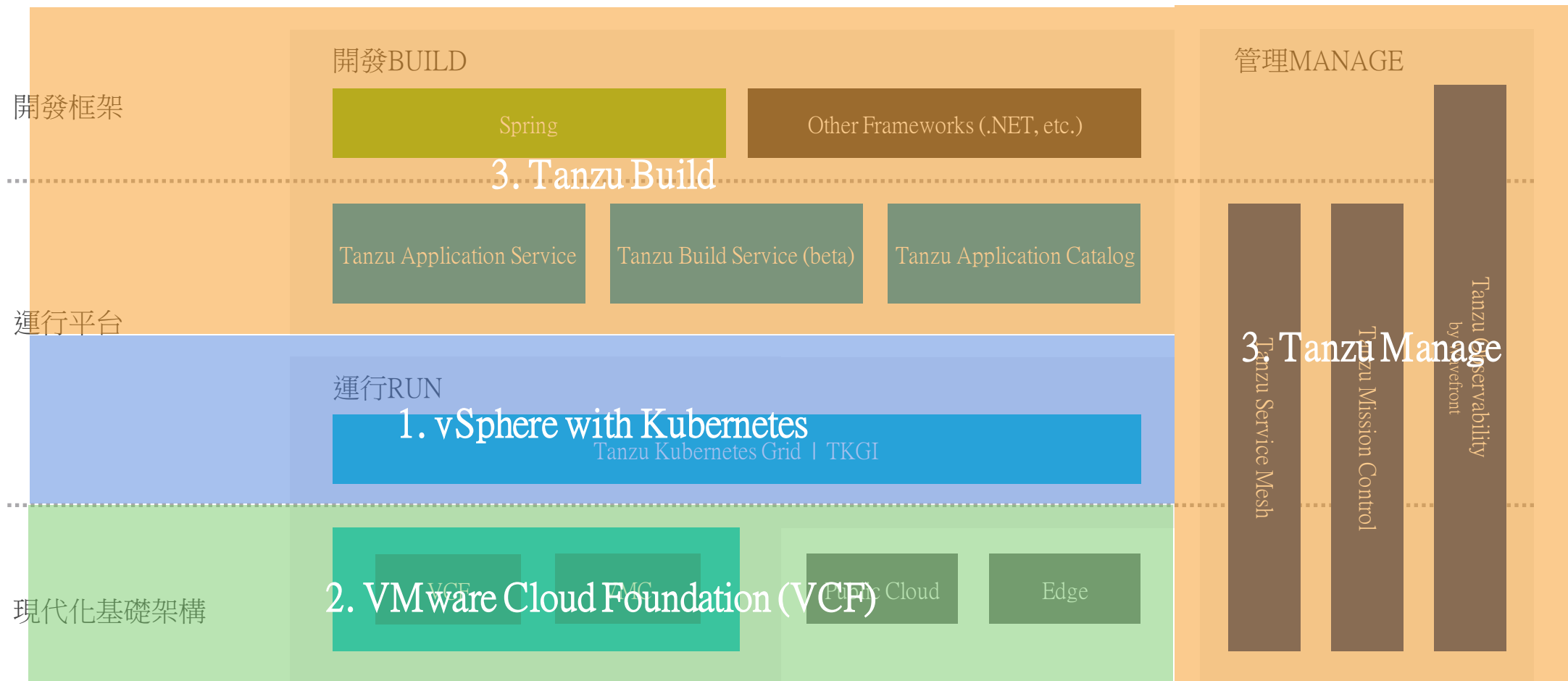
管理

單一控制點

多雲  
多叢集  
多團隊

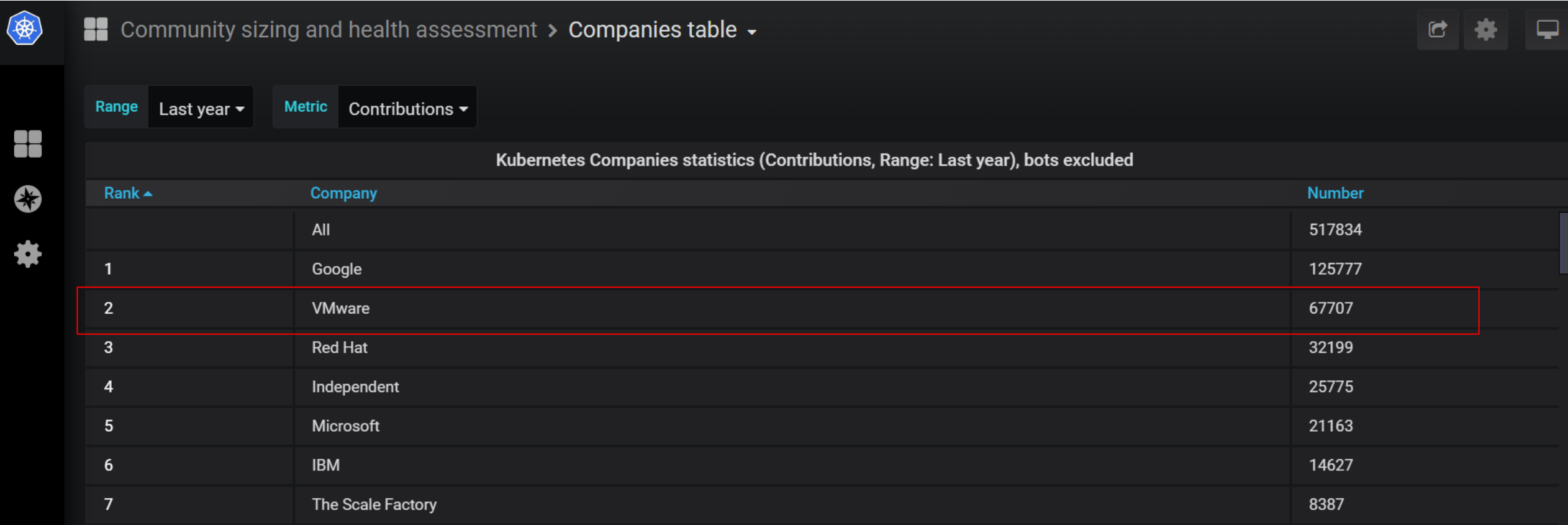
# 完整的容器堆疊架構平台

VMware Tanzu



# Kubernetes 貢獻度

VMware Tanzu



Community sizing and health assessment > Companies table ▾

Range: Last year ▾ Metric: Contributions ▾

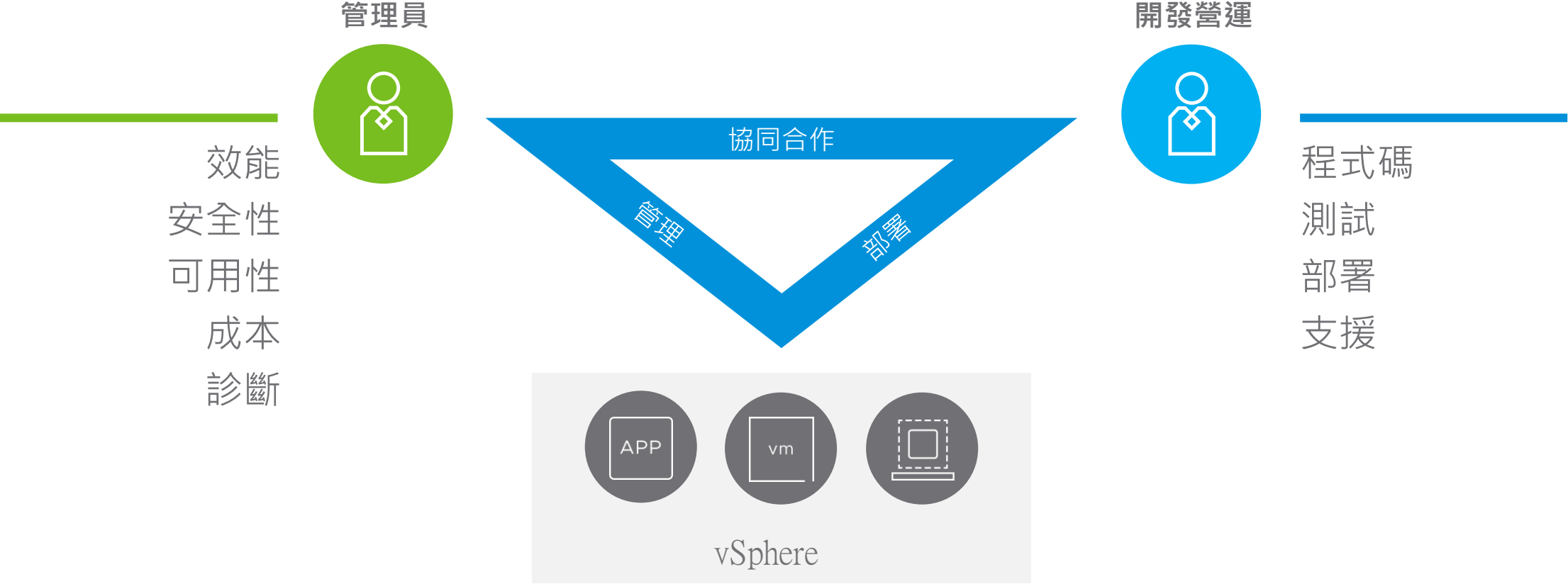
Kubernetes Companies statistics (Contributions, Range: Last year), bots excluded

Rank ▲	Company	Number
	All	517834
1	Google	125777
2	VMware	67707
3	Red Hat	32199
4	Independent	25775
5	Microsoft	21163
6	IBM	14627
7	The Scale Factory	8387

# vSphere 7 with Kubernetes

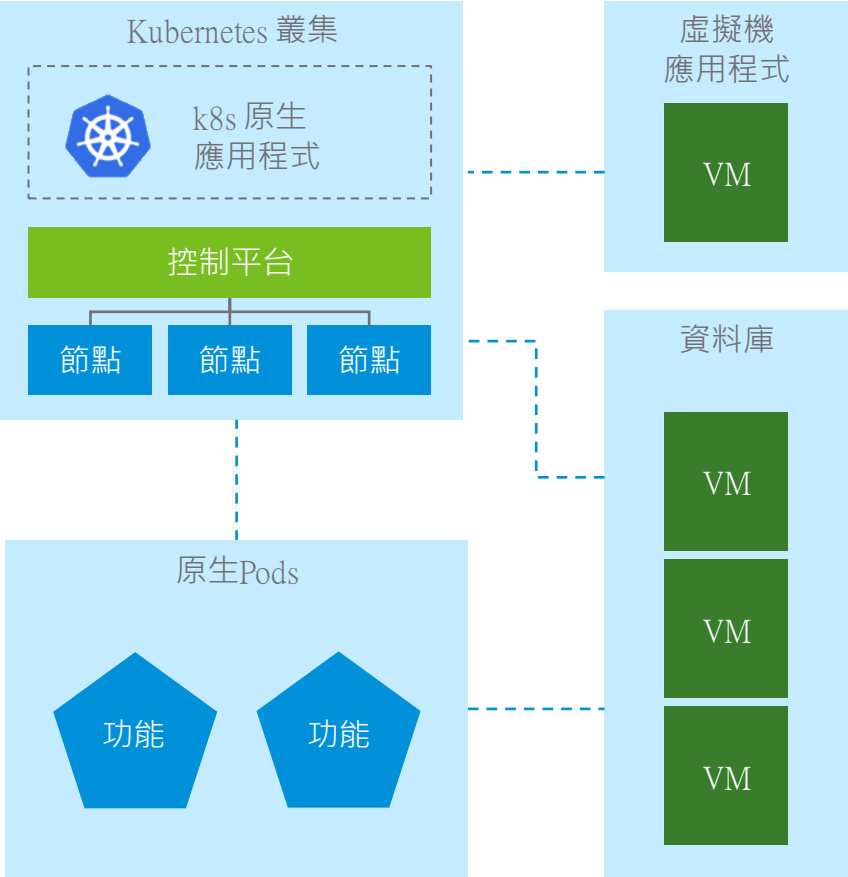
## 工作負載管理

# 使用 VMware 做為連接開發團隊與管理員的平台

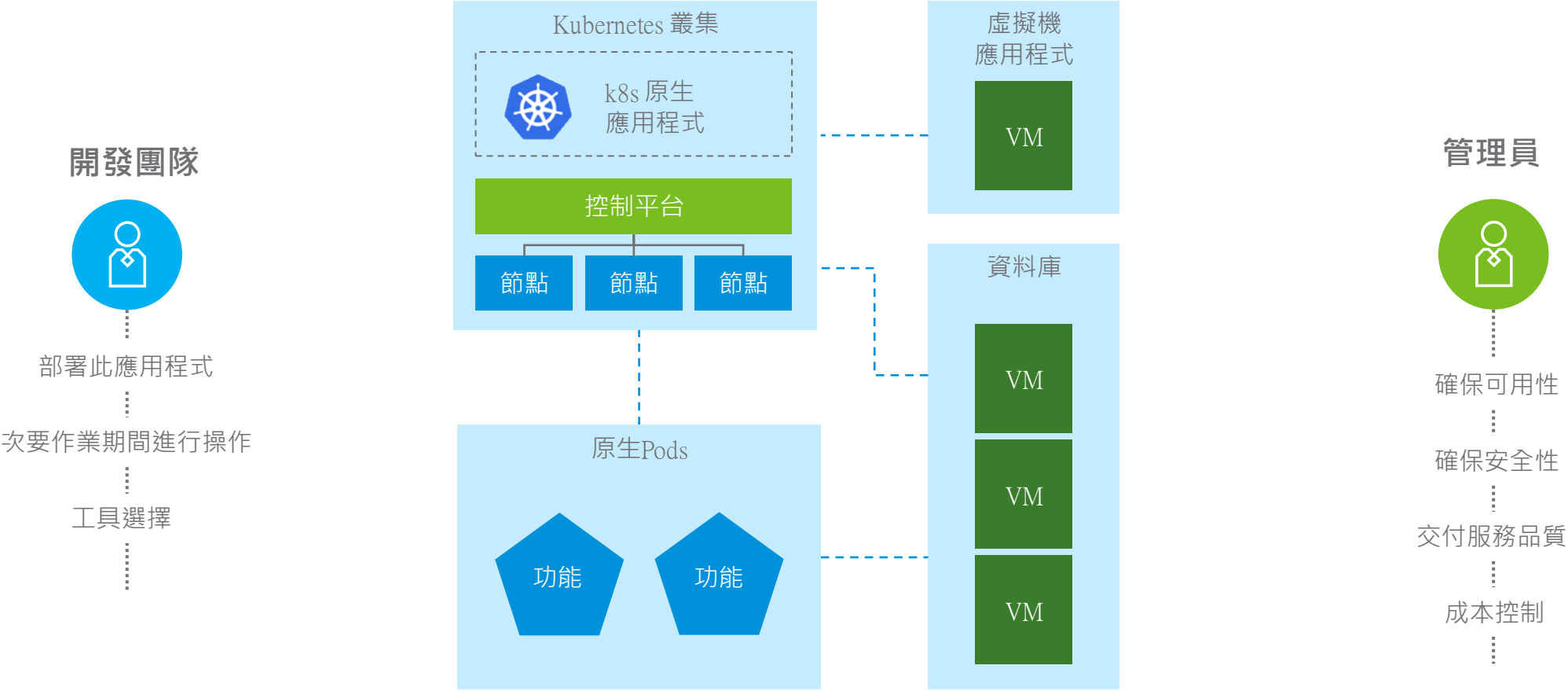




# 什麼是工作負載？



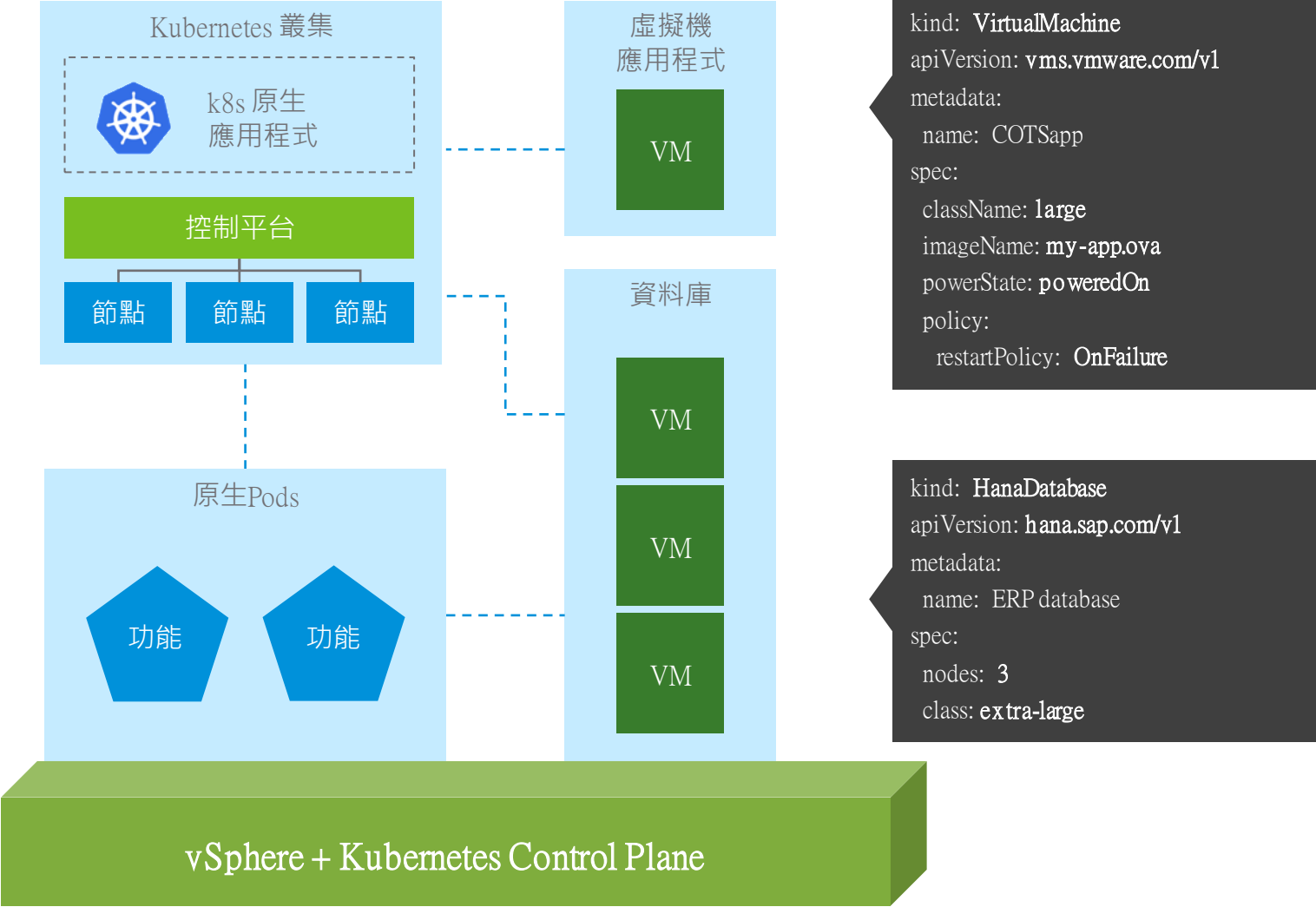
# 挑戰



# 使用 Kubernetes 管理工作負載！

```
kind: KubernetesCluster
apiVersion: vks.vmware.com/v1
metadata:
  name: My Application
spec:
  topology:
    workers:
      count: 3
      class: small
      distribution: v1.16.8
```

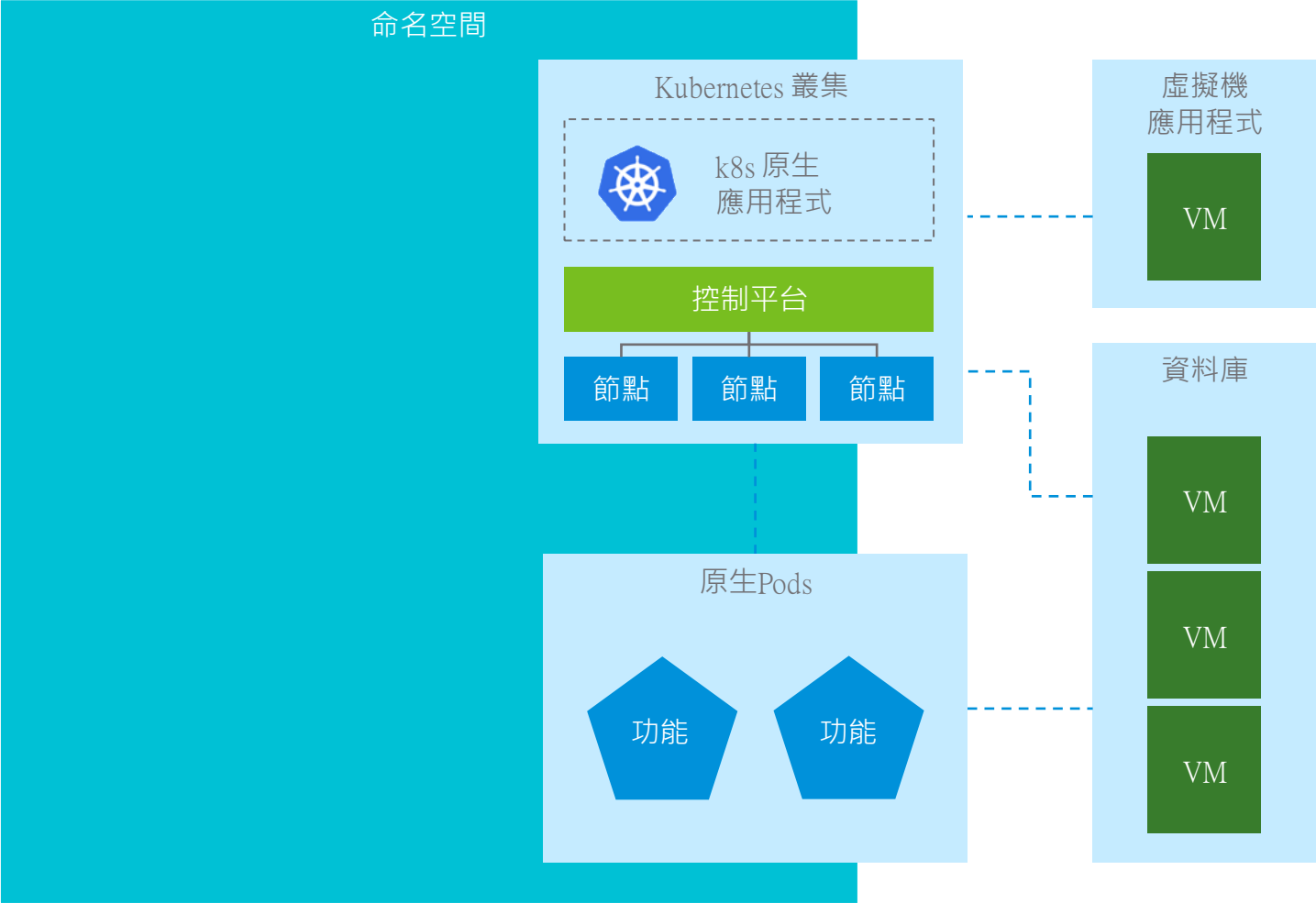
```
kind: Pod
apiVersion: v1
metadata:
  name: Function 1
spec:
  containers:
    - name: func1
      image: func1
      ports:
        - containerPort: 80
```



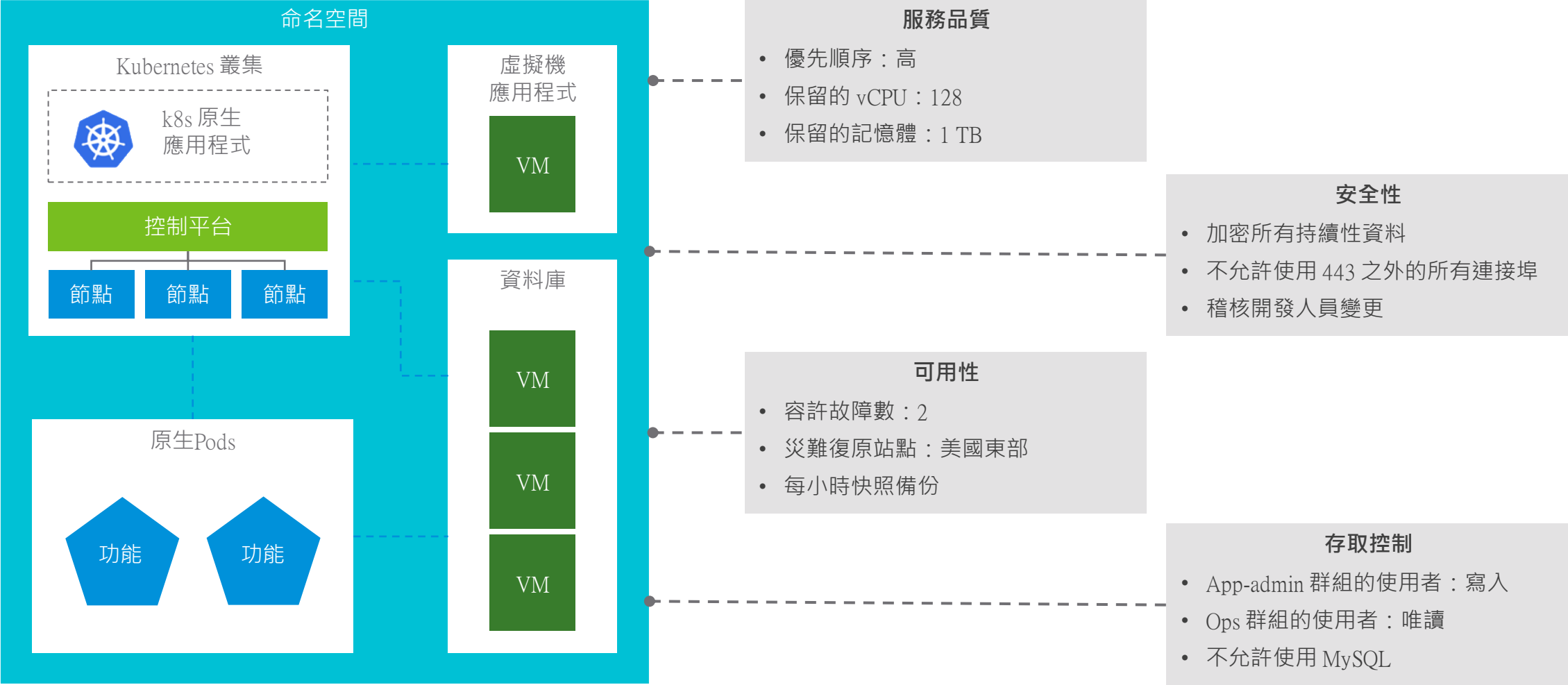
```
kind: VirtualMachine
apiVersion: vms.vmware.com/v1
metadata:
  name: COTSapp
spec:
  className: large
  imageName: my-app.ova
  powerState: poweredOn
  policy:
    restartPolicy: OnFailure
```

```
kind: HanaDatabase
apiVersion: hana.sap.com/v1
metadata:
  name: ERP database
spec:
  nodes: 3
  class: extra-large
```

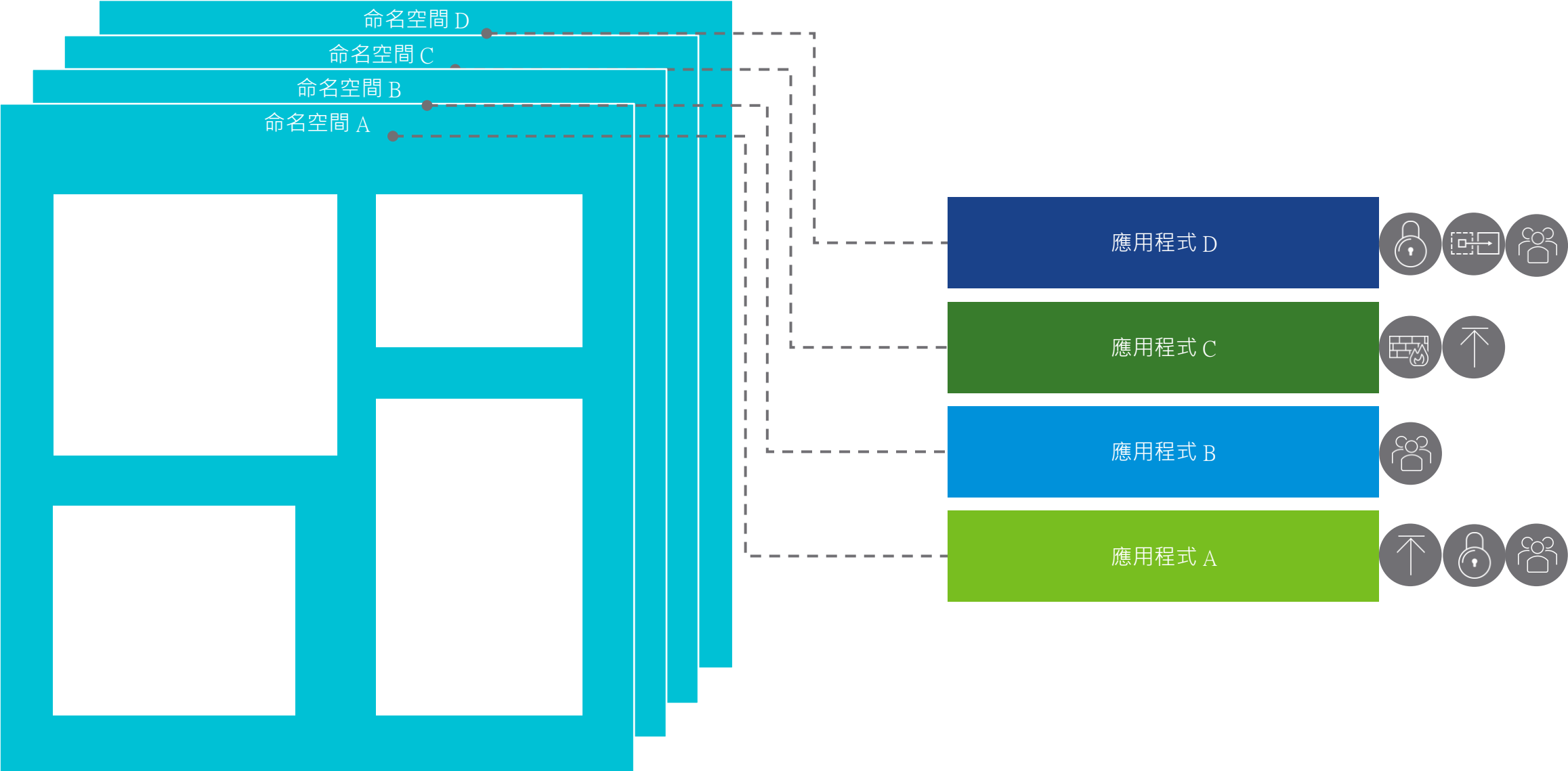
# 以命名空間當做管理單位



# 以命名空間當做管理單位

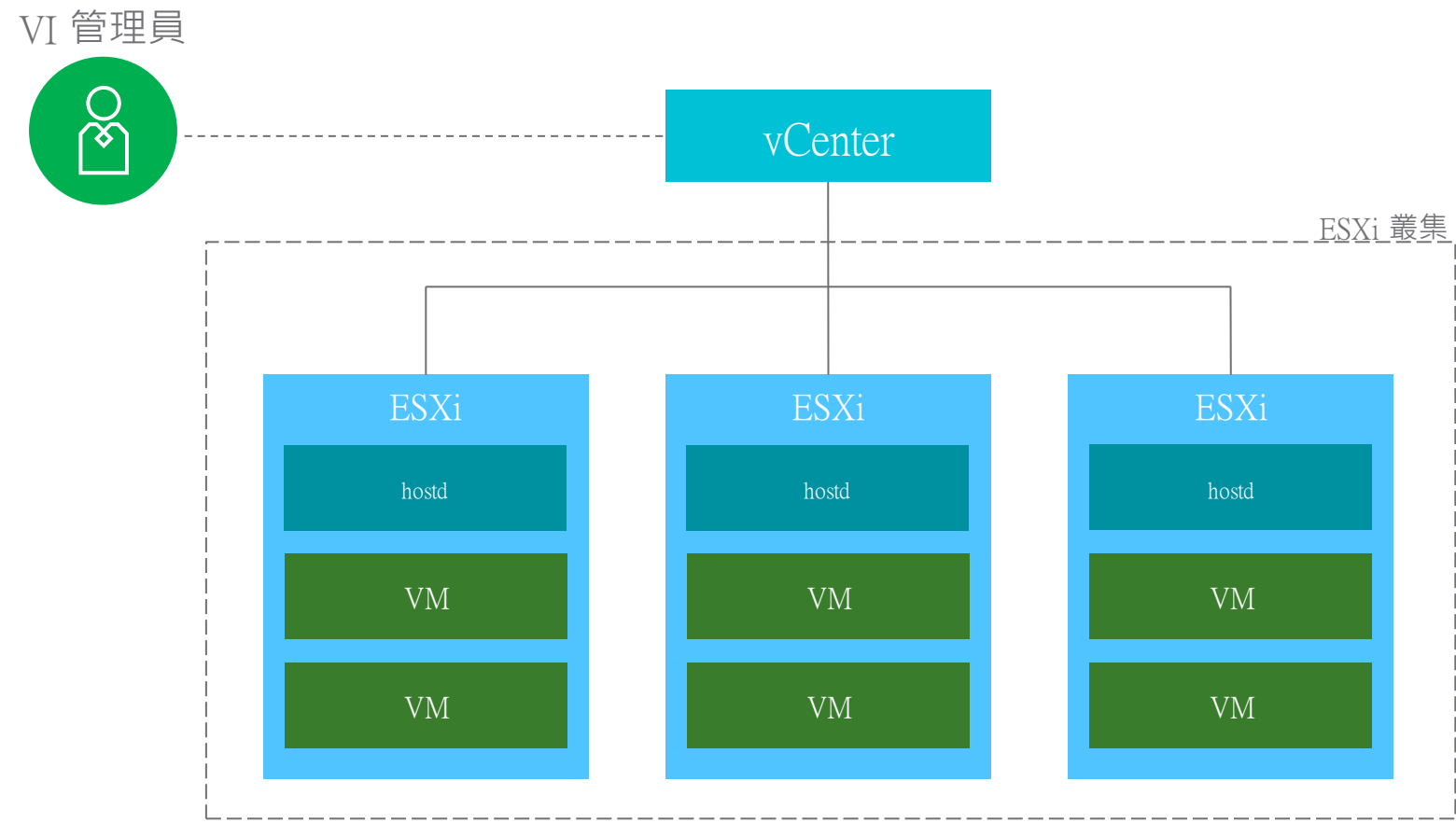


# 將命名空間對應至應用程式



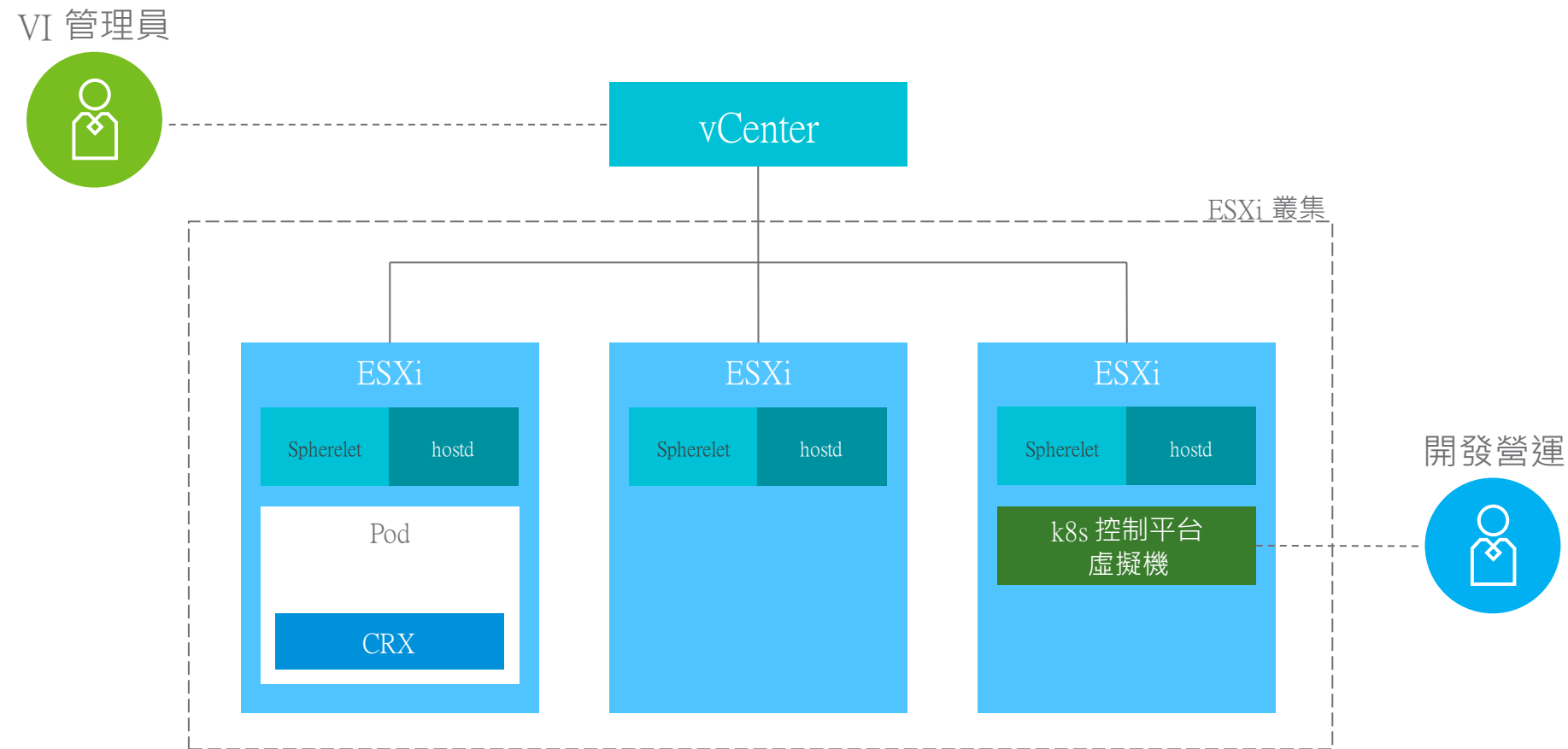
# 工作負載平台

# 在具有主管叢集的 vSphere 中啟用 Kubernetes





# 在具有主管叢集的 vSphere 中啟用 Kubernetes

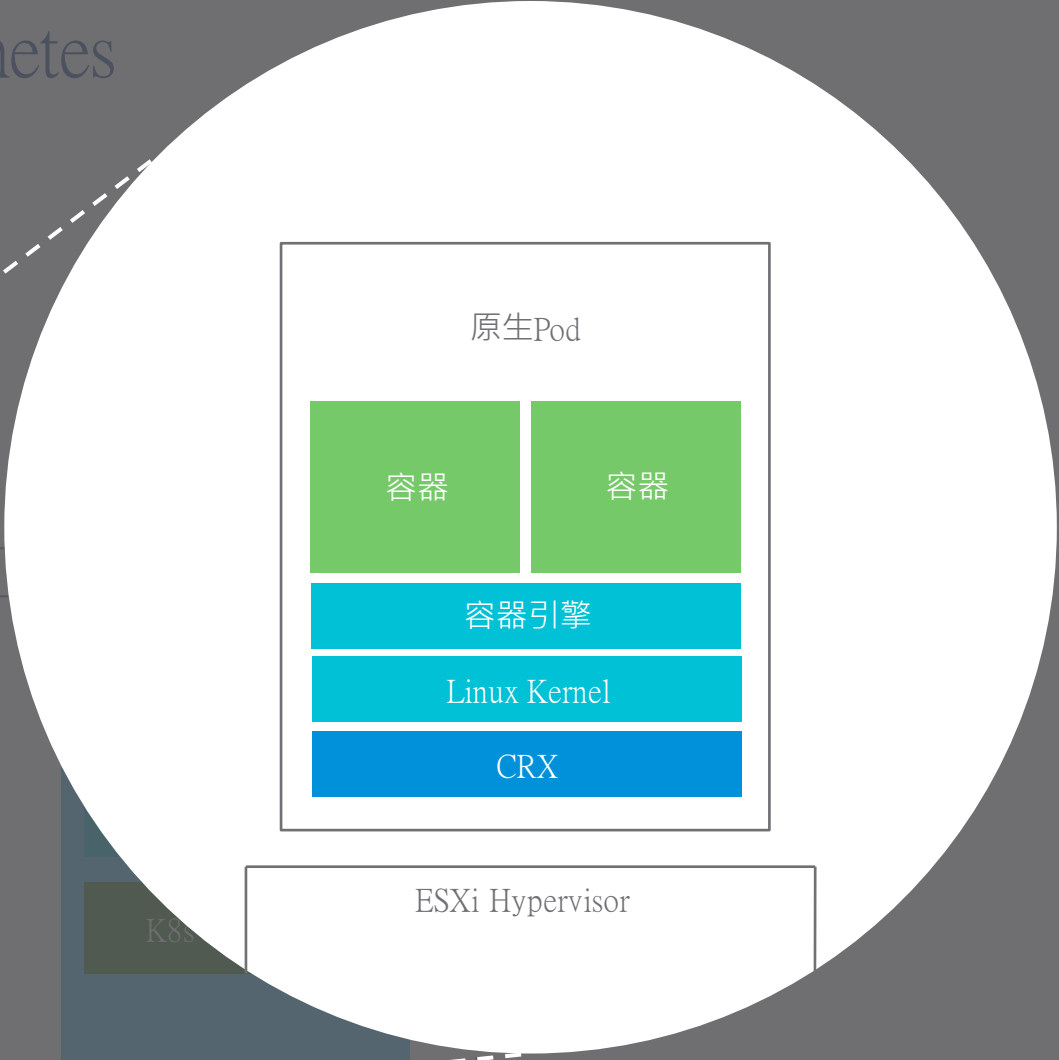


# 在具有主管叢集的 vSphere 中啟用 Kubernetes

VI 管理員



vCenter



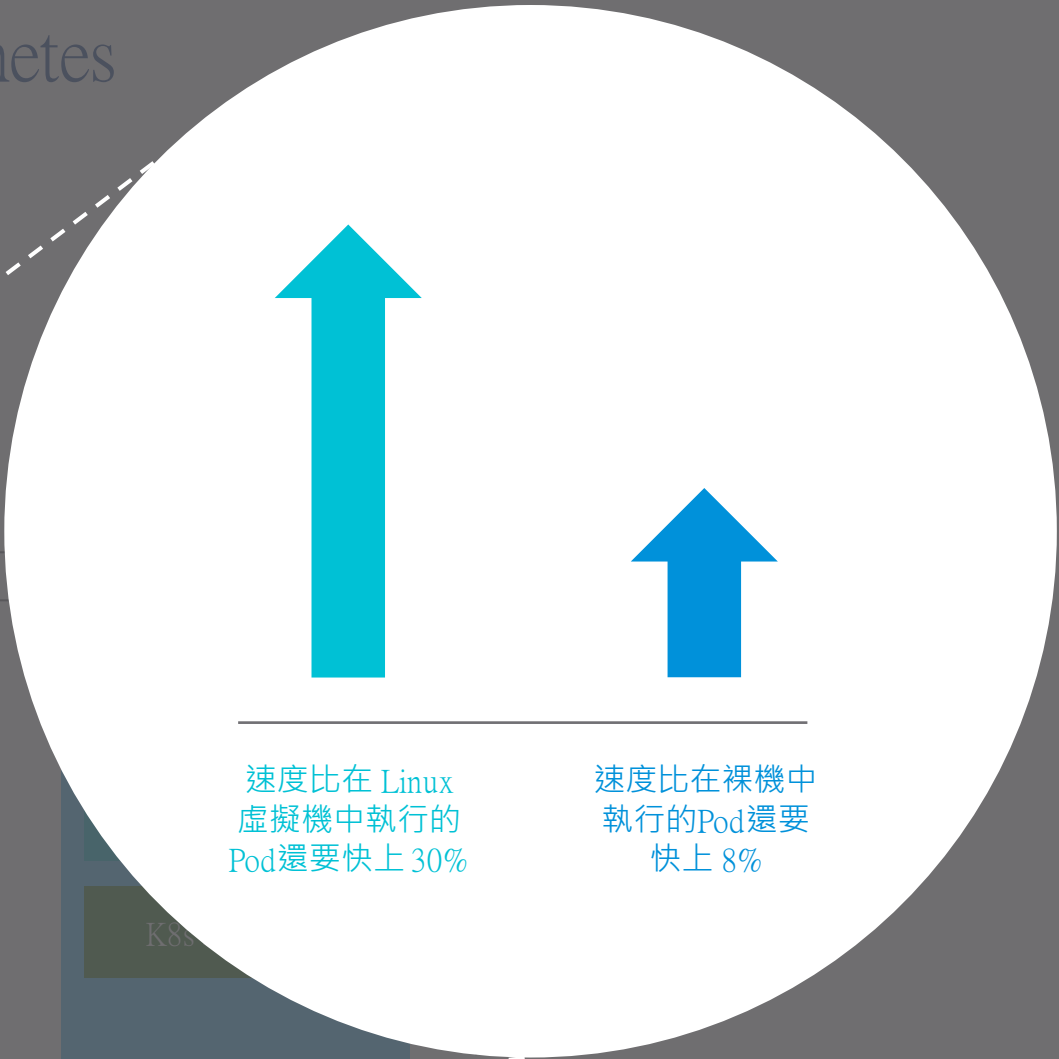
ESXi Hypervisor

# 在具有主管叢集的 vSphere 中啟用 Kubernetes

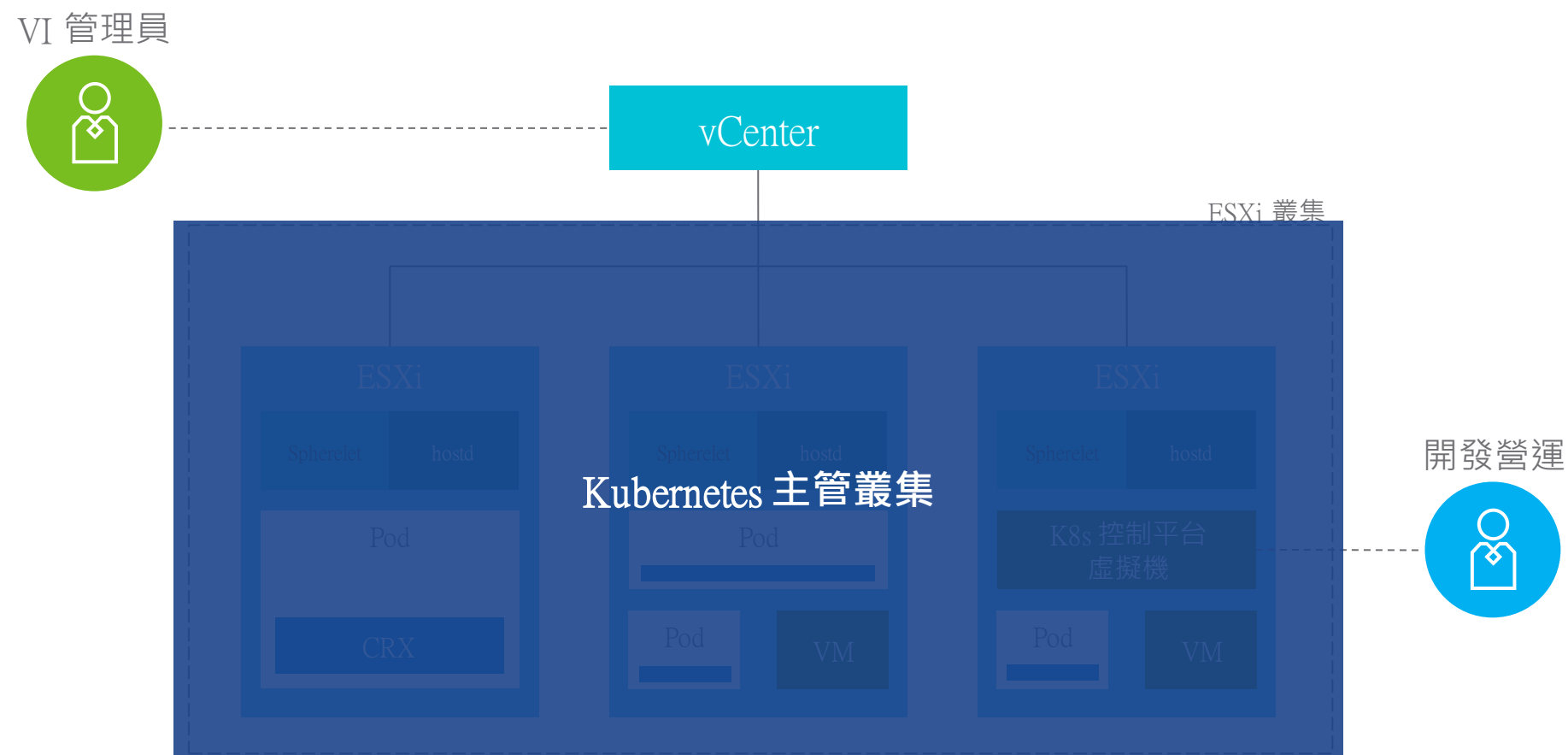
VI 管理員



vCenter

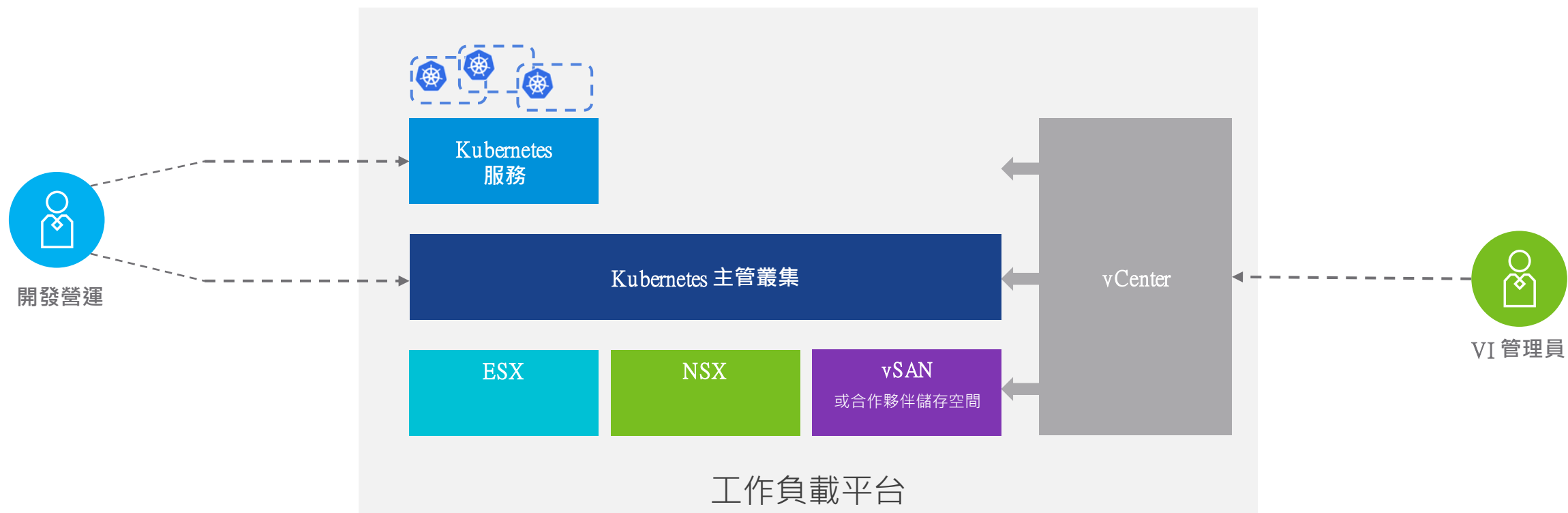


# 在具有主管叢集的 vSphere 中啟用 Kubernetes



# Kubernetes服務-客體叢集

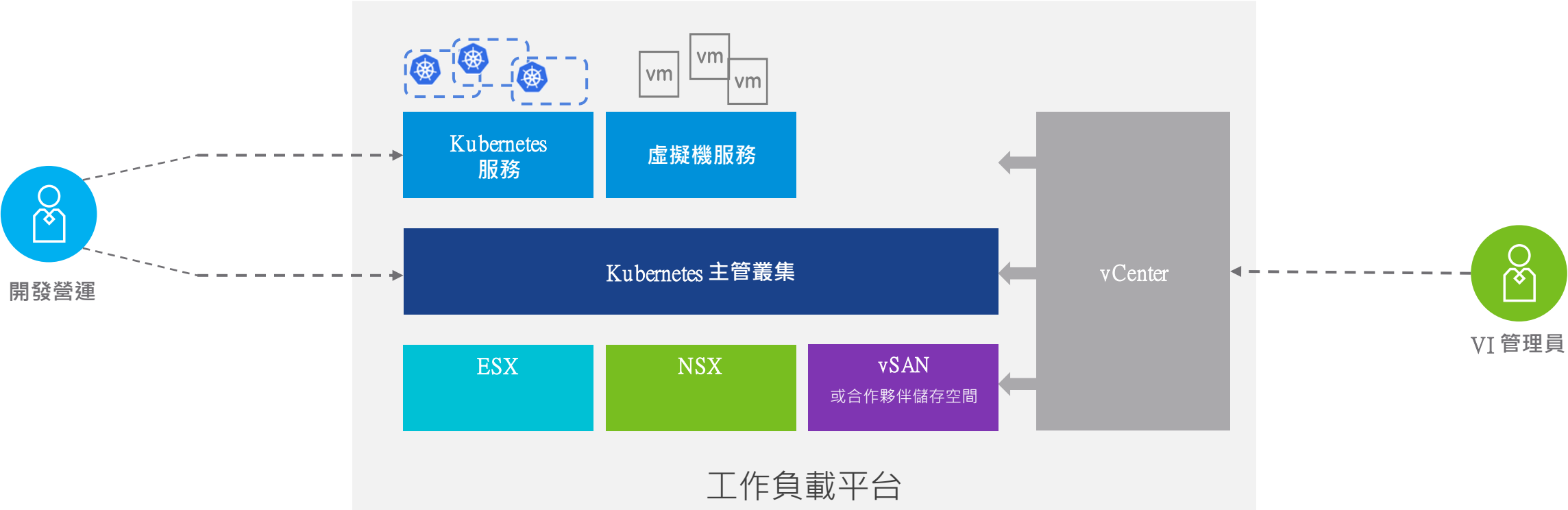
利用cluster API創造出的巢狀結構



內部部署 | 混合雲 | 公有雲

# 虛擬機服務

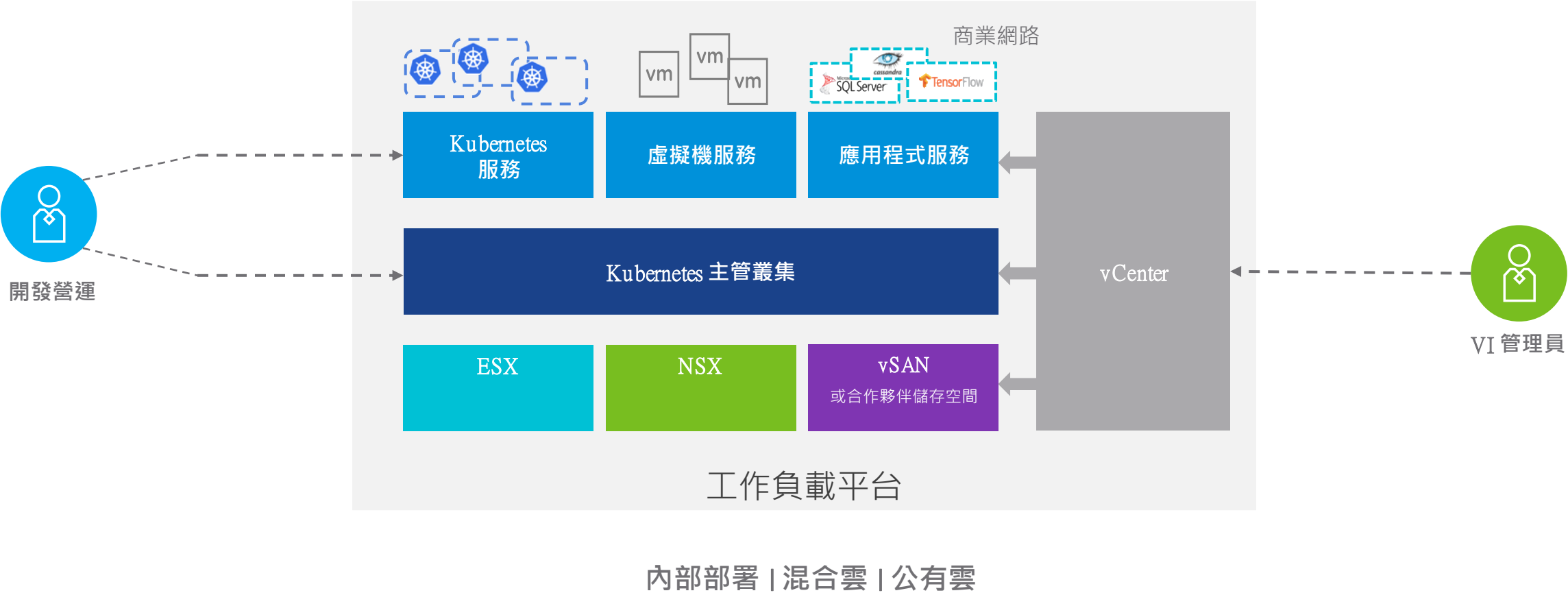
透過yaml檔案建立虛擬機



內部部署 | 混合雲 | 公有雲

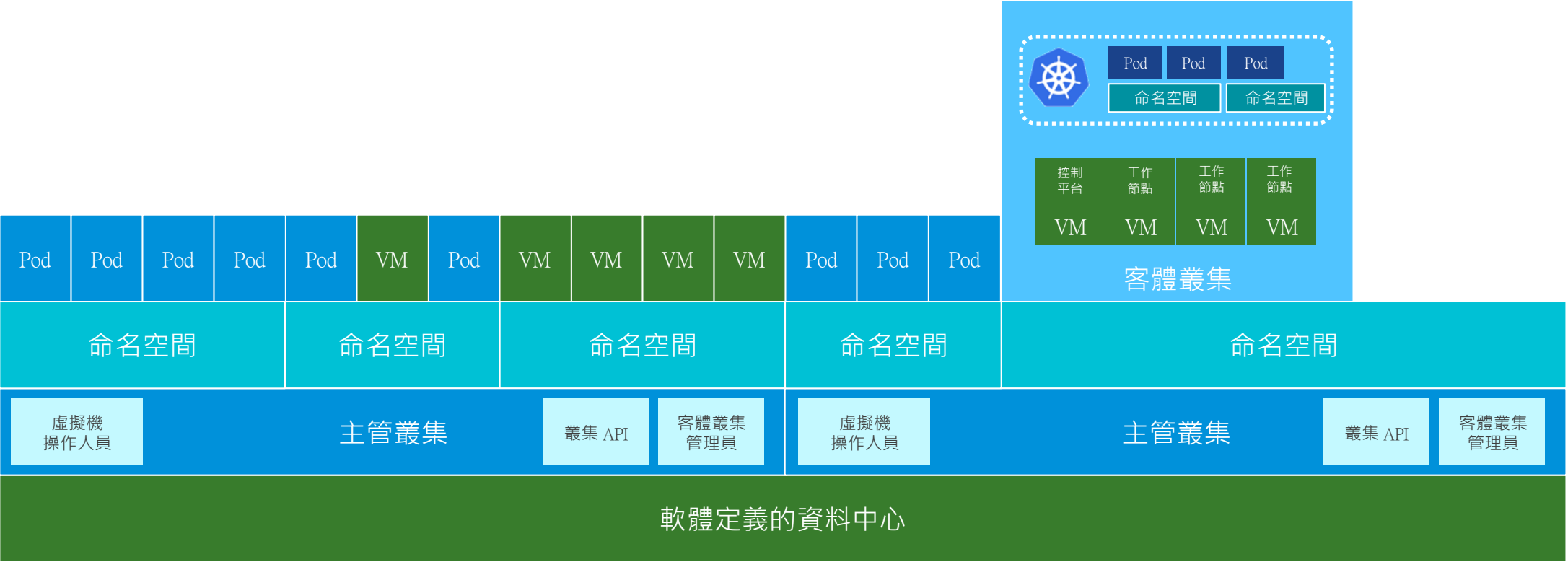
# 應用服務

透過pod VM來達到更強的效能已經更高的安全性



內部部署 | 混合雲 | 公有雲

# 工作負載平台架構





# 在主管叢集與客體叢集之間選擇



## 客體叢集：

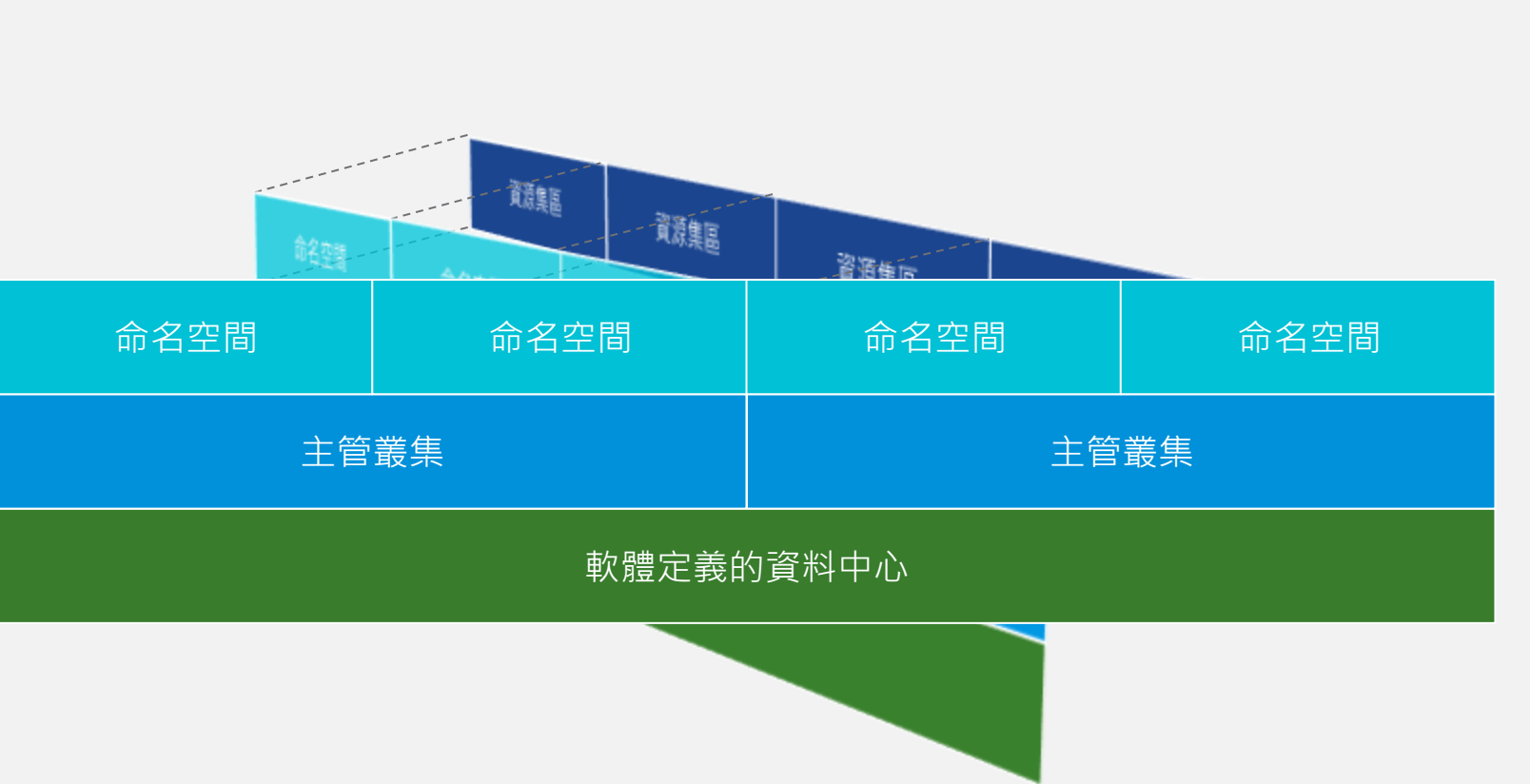
- 與上游 k8s 完全相容
- 可設定的 k8s 控制平台
- 彈性的生命週期，包括升級作業
- 可輕鬆安裝及自訂偏好工具

## 主管叢集：

- 強大的安全性與資源隔離
- 效能優勢
- 無伺服器經驗

# 平台整合

# 具有主管叢集命名空間的多租戶



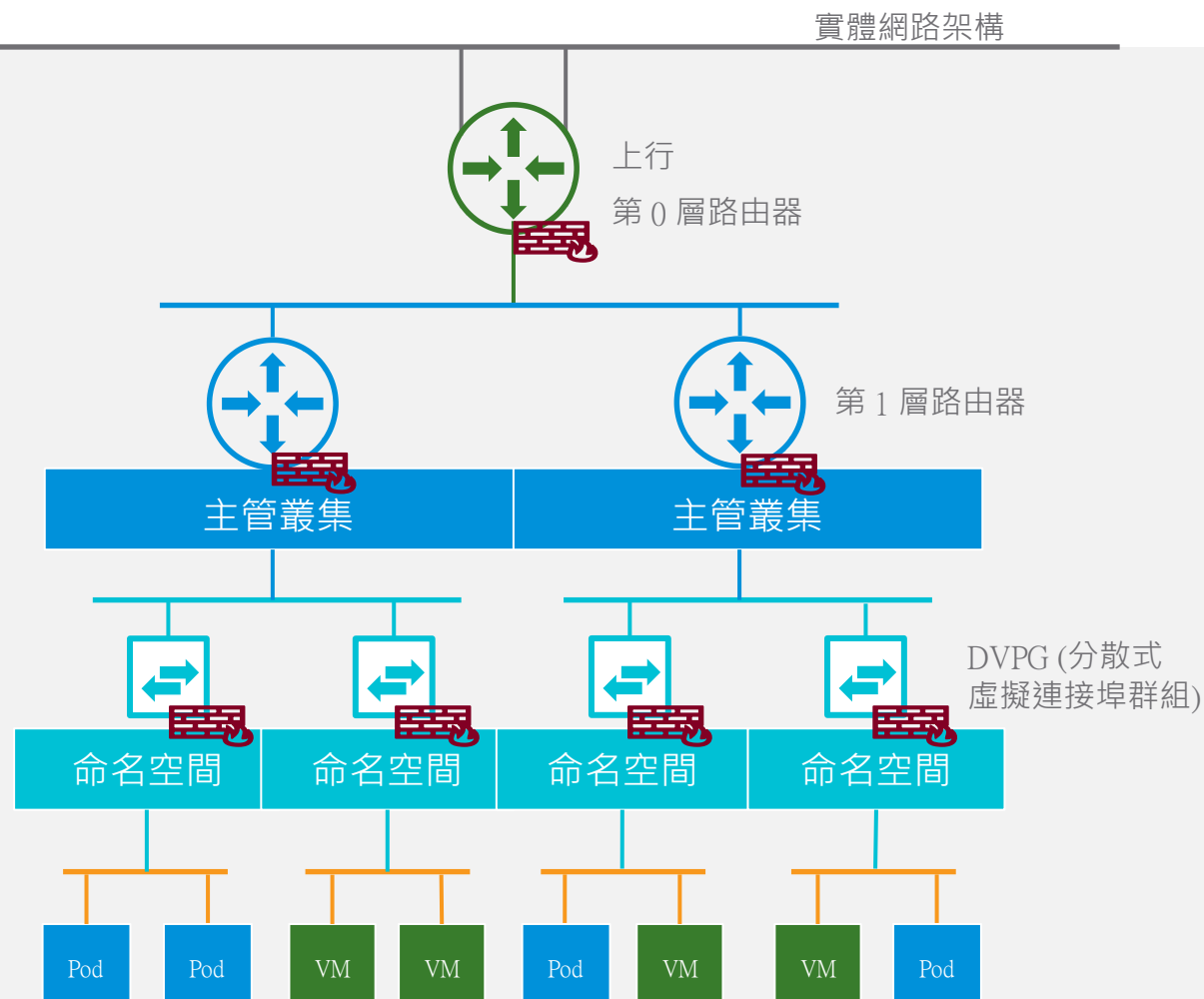
每個命名空間皆有專屬的資源集區

除了能隔離資源，還能針對CPU/記憶體/儲存空間進行配額控制

命名空間中的所有工作負載皆受到命名空間配額限制

- 客體叢集
- 原生Pod
- 虛擬機

# 主管叢集網路拓撲與隔離



WCP 會運用 NSX 網路功能

主管叢集與第1層路由器及分散式防火牆互相隔離

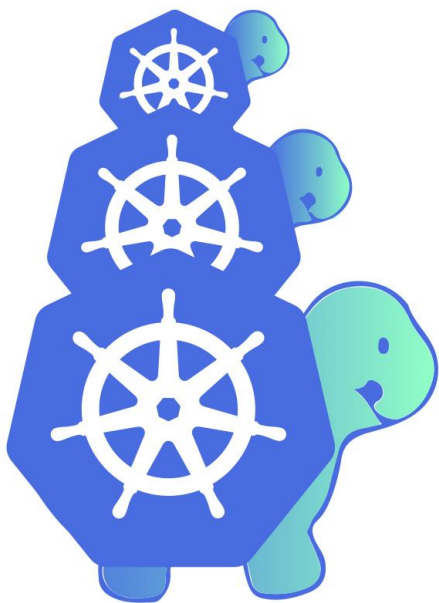
命名空間與 DVPG 及分散式防火牆互相隔離

輸入流量預設會遭到所有命名空間拒絕

客體叢集可使用您偏好的層疊網路  
(預設為 Calico)

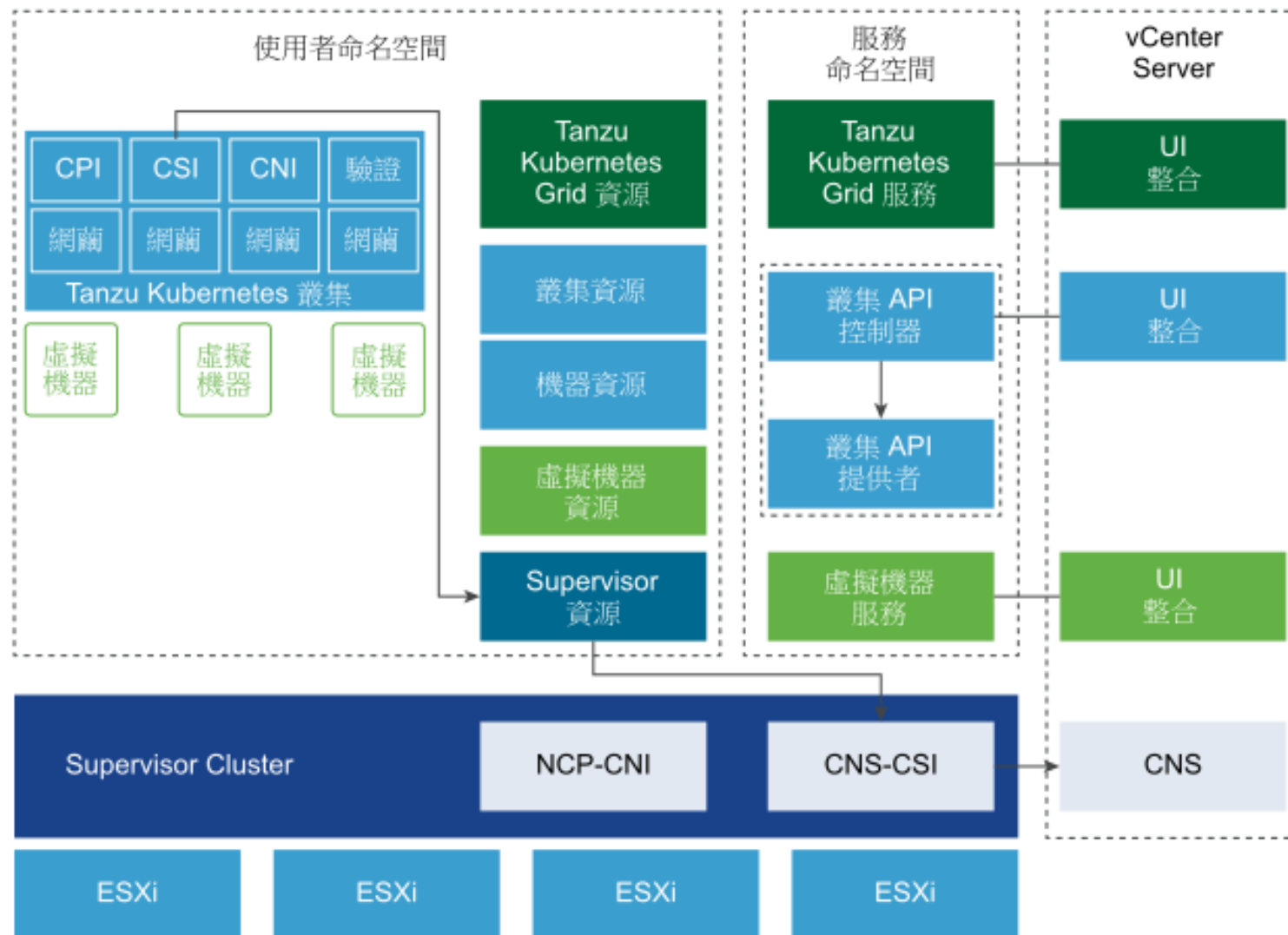
# Tanzu Kubernetes Grid

使用Cluster API建立巢狀結構



# Tanzu Kubernetes Grid(TKG)

輕量化的解決方案



# 感謝聆聽

