Tanzu for Kubernetes Operations

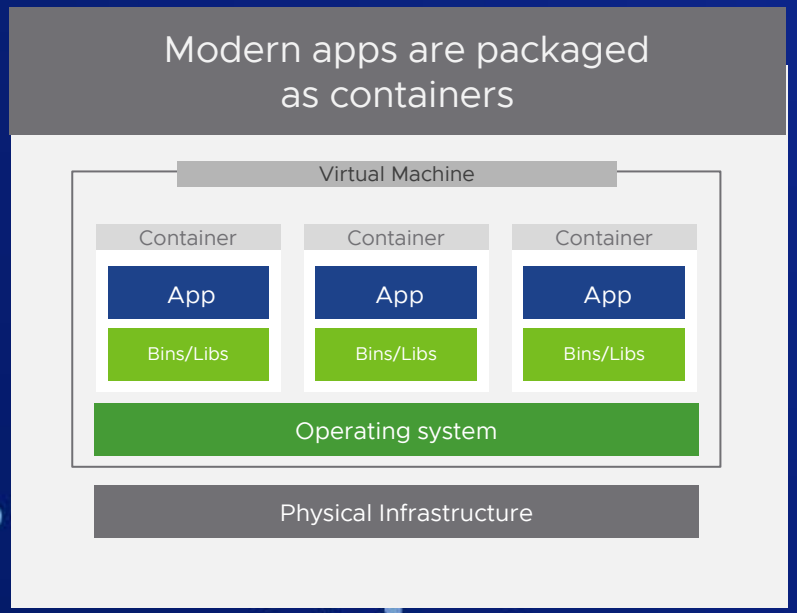
輕鬆掌控混合雲及多雲的管理、資安及監控

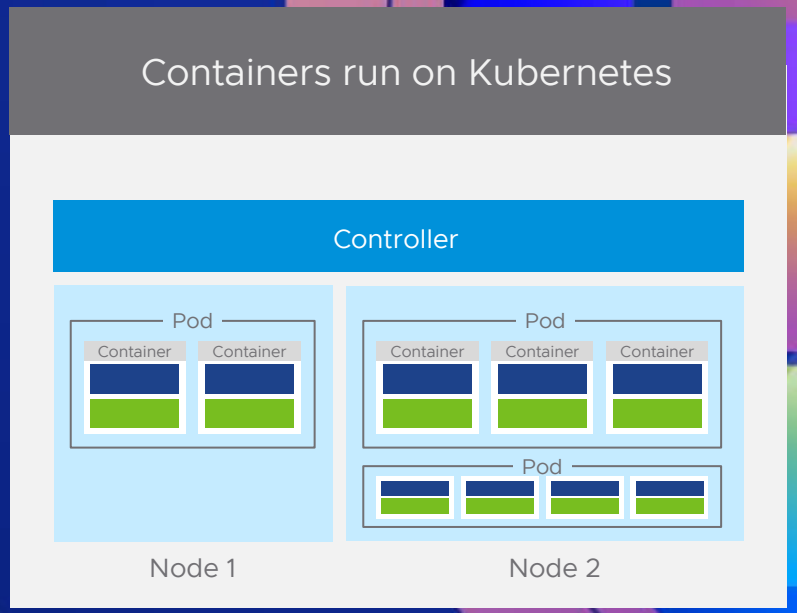
William Tzeng 曾英宸

MetaAge Product Director

2022/10/18

Kubernetes是多雲上現代應用的基礎





67% 的組織正在增加對容器的投資，以提高敏捷性1

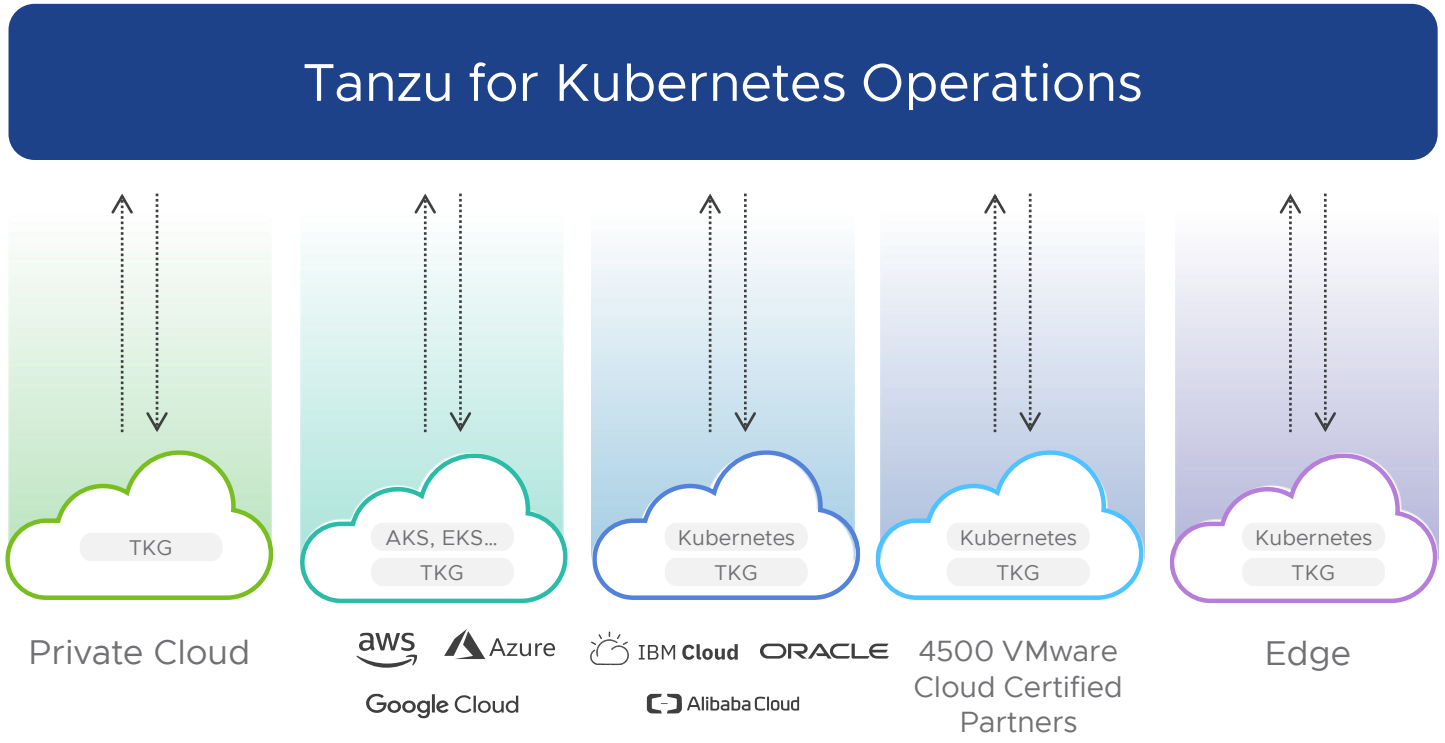
65% 的受訪者在生產環境中運行 Kubernetes，具有前三大優勢：

- 改進的資源利用率
- 更輕鬆的應用升級
- 更快的開發週期2

1- 多雲世界中的應用現代化，2020 年 VMware 市場洞察報告
2- 2021 年庫伯內特斯現狀，由 VMware 提供

VMware Tanzu for Kubernetes Operations

現代化的多雲容器基礎架構管理



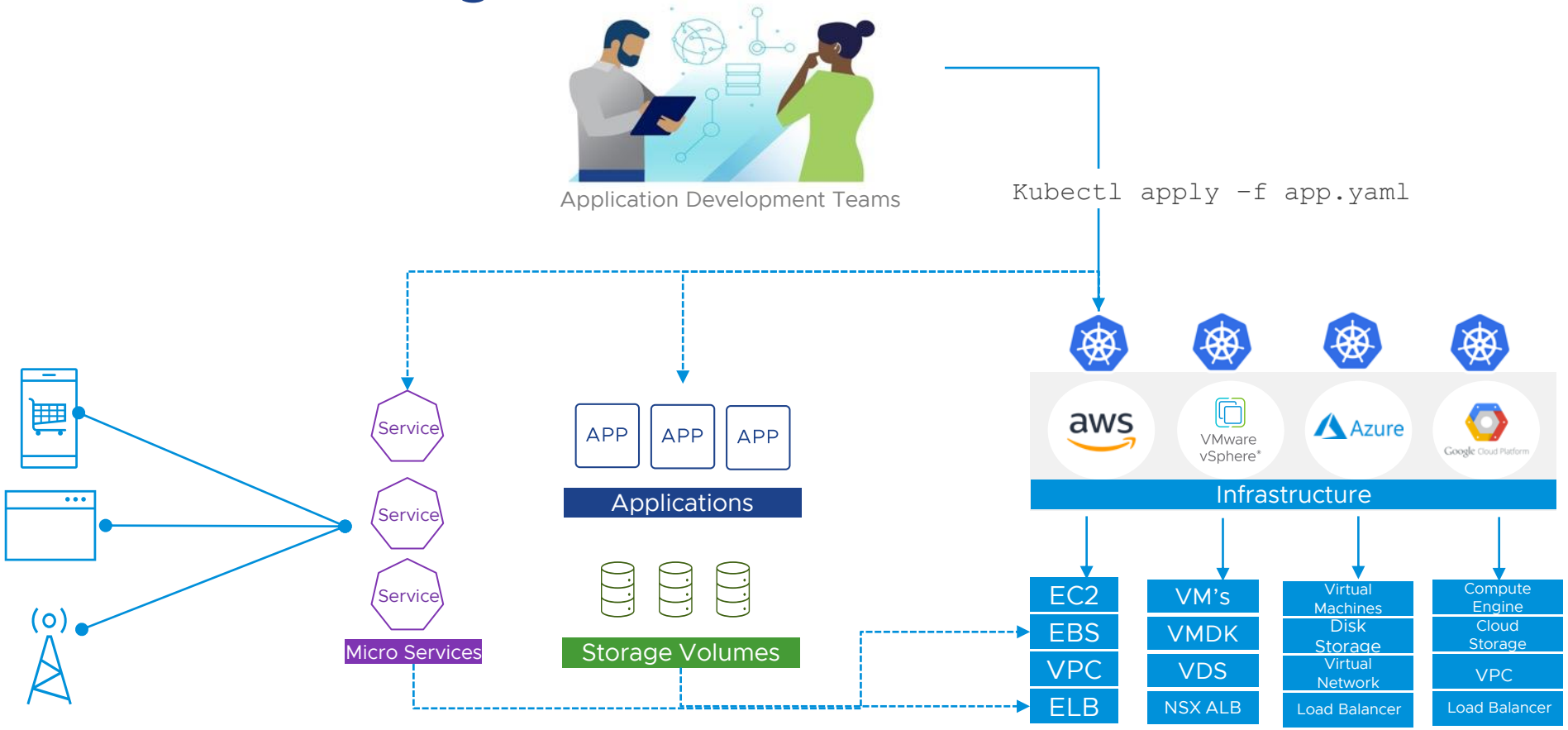
跨集群和雲應用自動化、策略驅動的管理和安全性

快速啟動並運行Kubernetes環境

連接和保護整個Kubernetes斯資產中的應用和數據

觀察並統一數據驅動的見解，以確保可靠的性能

Kubernetes as the Singular Infrastructure API



!!! Access to Kubernetes API = Access to your Infrastructure!!!

Kubernetes Infrastructure Ecosystem Providers

Plugins for various Vendors

Cloud Provider

vmware vSphere

aws

Google Cloud

openstack.

Azure

Network Provider

cisco ACI

apstra

cilium

flannel

ANTREA

vmware NSX

Contiv

PROJECT CALICO

Storage Provider

AWS EBS

Azure Disk

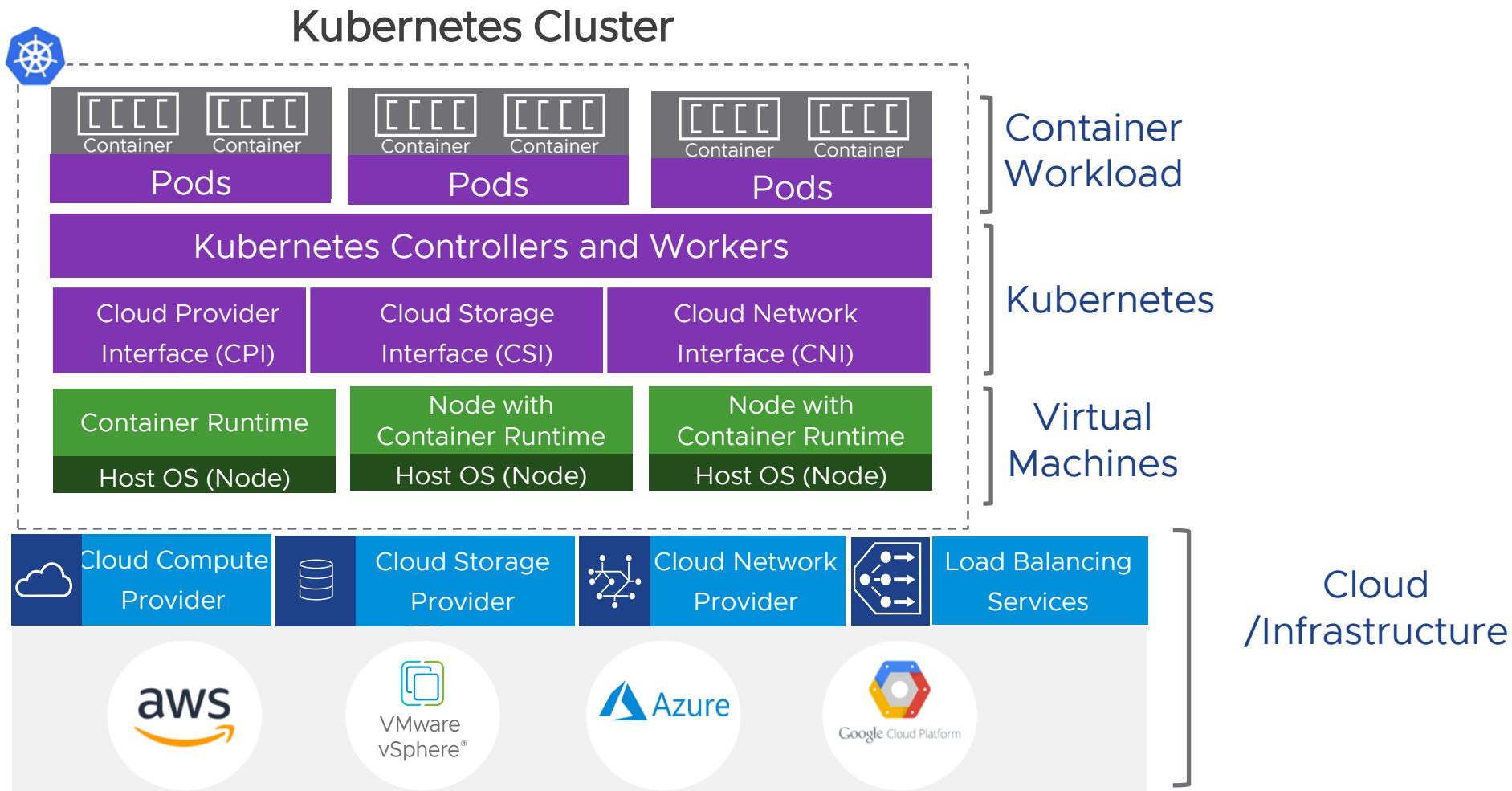
CSI

ceph

vmware vSphere Volume

GCP Drive

Kubernetes Abstractions and Layers



Challenges faced by the Ops Team

Challenges Managing Containerized Platforms

Application Development Teams

Kubectl apply -f app.yaml

Day 1

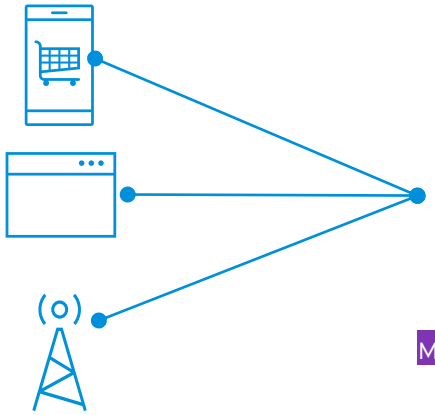
- Right level of access to the K8s API
- Self Service access to API

Day 0

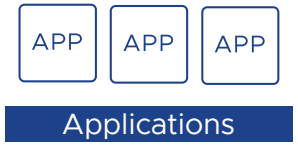
- Ability to Provision Clusters on demand
- Right Drivers, Base OS image, Secure

Day n

- Full Stack Monitoring
- Backup & Restore

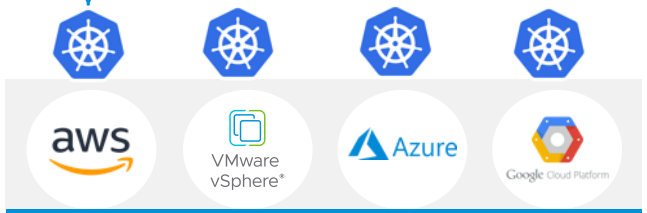


Micro Services



Applications

Storage Volumes



Infrastructure

EC2	VM's	Virtual Machines	Compute Engine
EBS	VMDK	Disk Storage	Cloud Storage
VPC	VDS	Virtual Network	VPC
ELB	NSX ALB	Load Balancer	Load Balancer

Day 2

- Service are Encrypted?
- Secure Communications
- Monitoring

Day 2

- What workloads are being Provisioned
- What services are being exposed?
- How much Infra is being Provisioned?

Tanzu for Kubernetes Operations

Challenges faced by the Ops Team

Tanzu for Kubernetes Operations

Application Development Teams

Kubectl apply –f app.yaml

Day 1

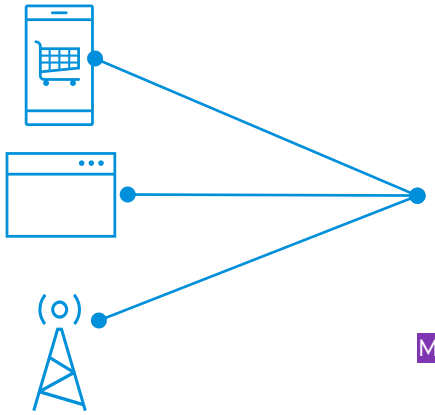
- -Provide Central Identity to the K8s API
- -Self –Service Access

Tanzu Mission Control

Tanzu Kubernetes Grid

Day 0

- Deploy Secure K8s clusters in minutes on any Cloud/Infra



Micro Services

Applications

Storage Volumes

Infrastructure

EC2	VM's	Virtual Machines	Compute Engine
EBS	VMDK	Disk Storage	Cloud Storage
VPC	VDS	Virtual Network	VPC
ELB	NSX ALB	Load Balancer	Load Balancer

Day n

- Full Stack Monitoring
- Backup & Restore

Tanzu Observability

Day 2

- Cross-Cloud Service Mesh
- mTLS by default

Tanzu Service Mesh

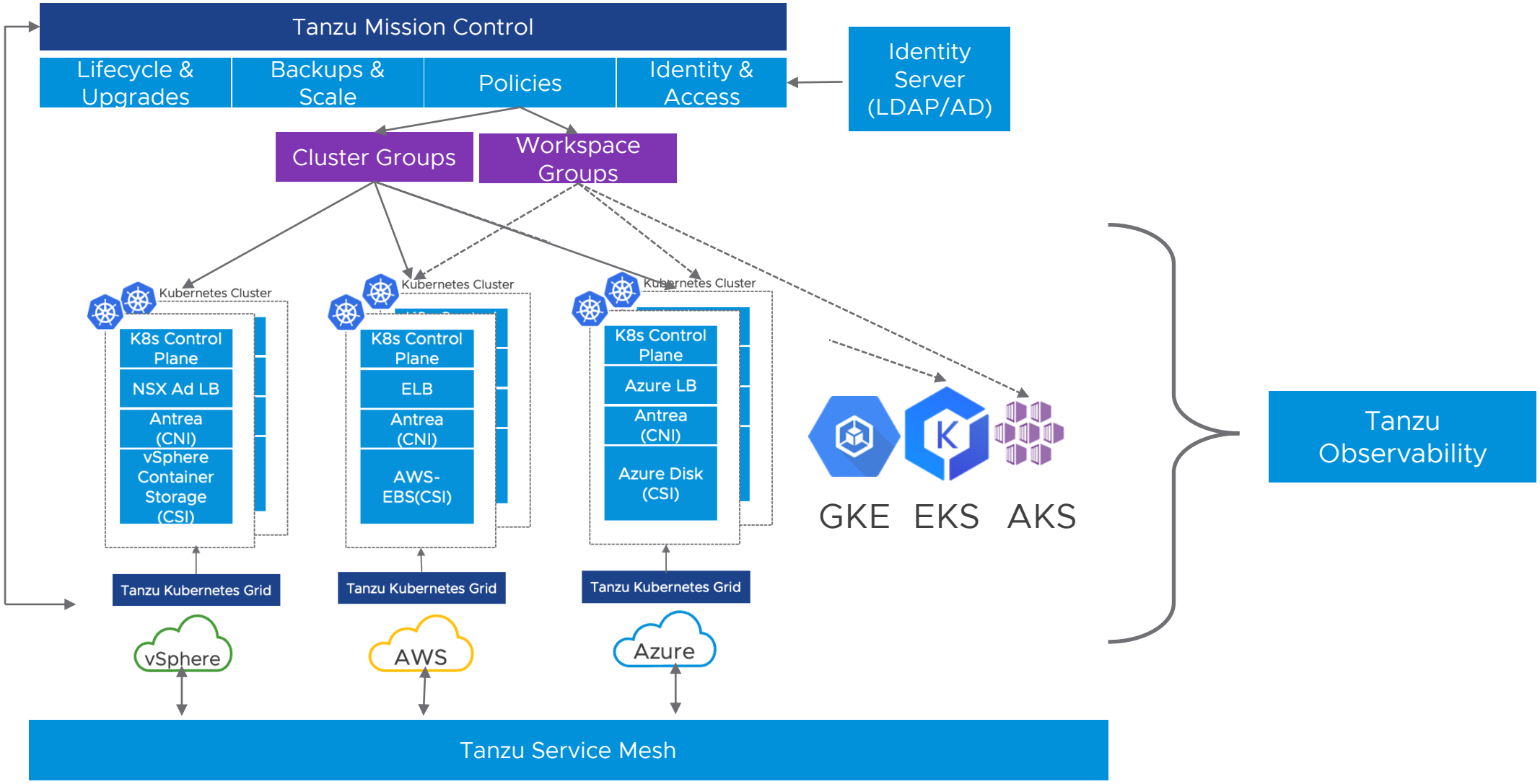
Day 2

- Establish Enterprise-wide Guardrails
- Implement Network , Image, Custom Policies
- Implement fleet wide

Tanzu Mission Control

Tanzu for Kubernetes Operations

Architecture



Kubernetes 多叢集如何管理?

Tanzu Mission Control

Tanzu Mission Control 管理持續成長的 K8s 平台

取得混合雲和多雲部署的掌控權和能見度

營運

Tanzu Mission Control

交付一致且統一的多雲 Kubernetes 式平台

開發

生命週期管理和設定

安全性、合規和稽核

可觀察性和診斷

連線能力和流量管理

身分識別和存取權

資料保護

應用程式和服務管理

隨處使用任何 Kubernetes 叢集

地端

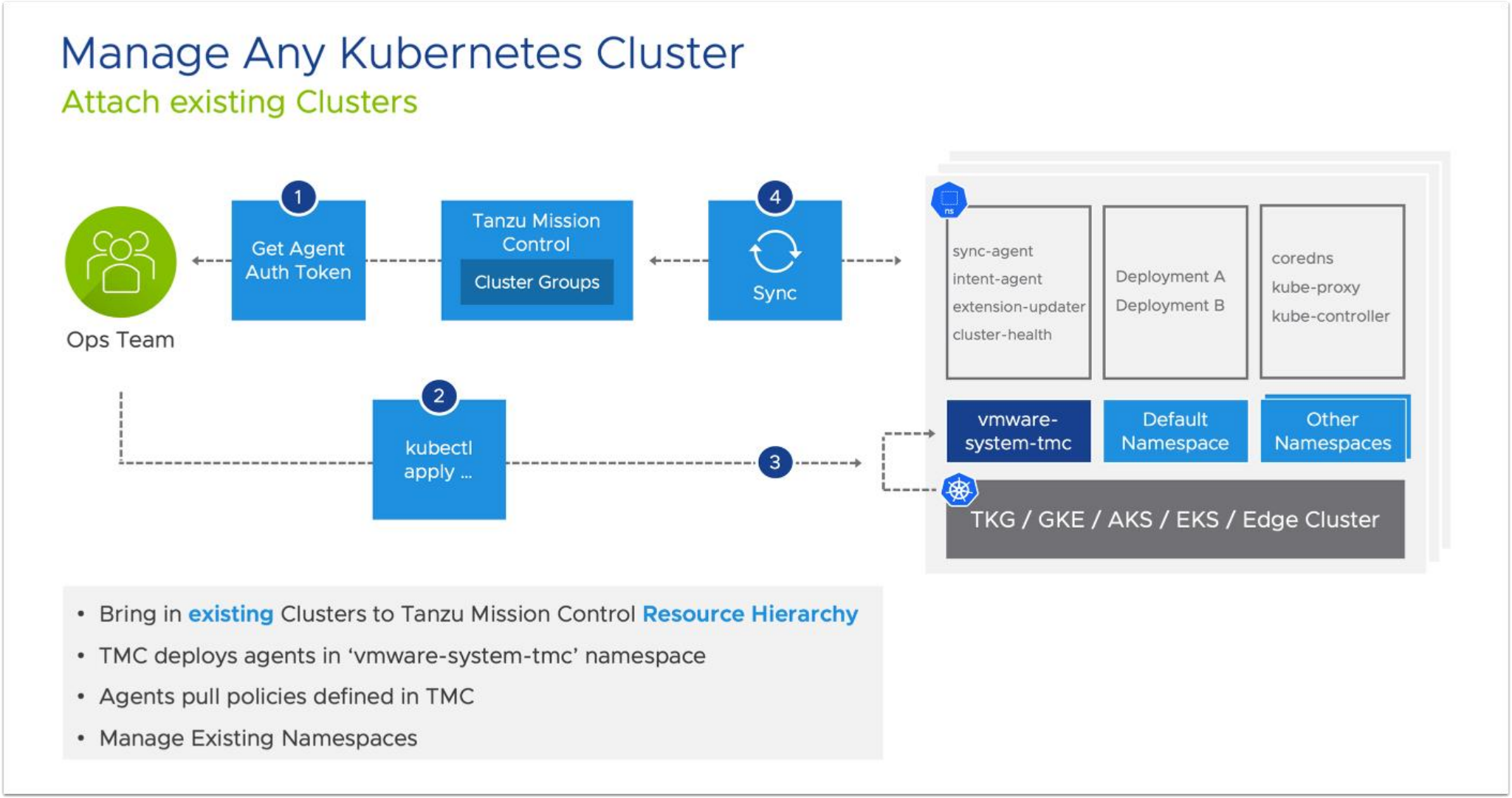
公有雲

邊緣

*藍圖

Tanzu Mission Control 管理任何 Kubernetes Cluster

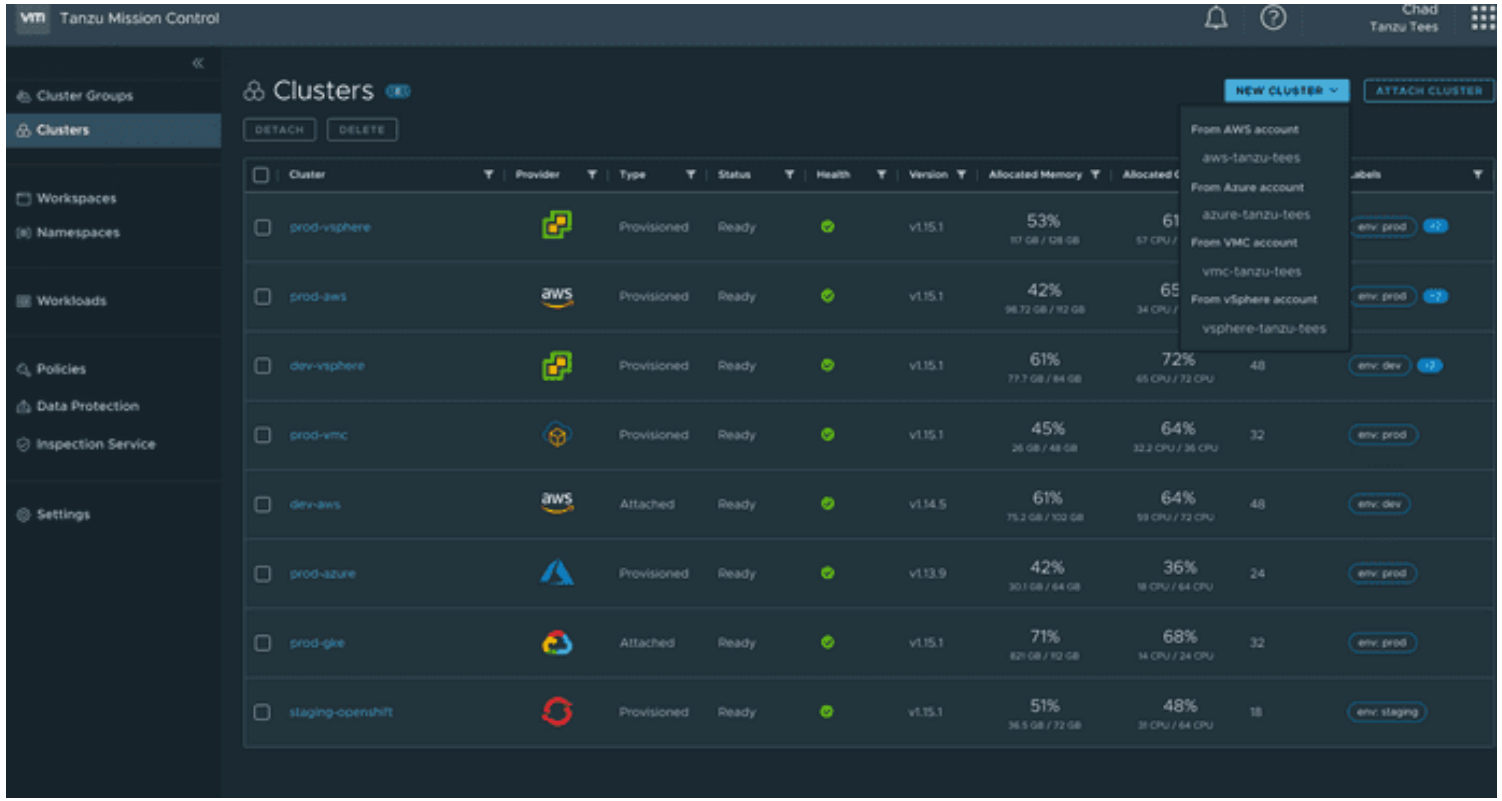
基於標準 Kubernetes API 的管理



多叢集生命週期管理 Cluster Lifecycle Management

Provision / Attach / Scale / Upgrade / Delete

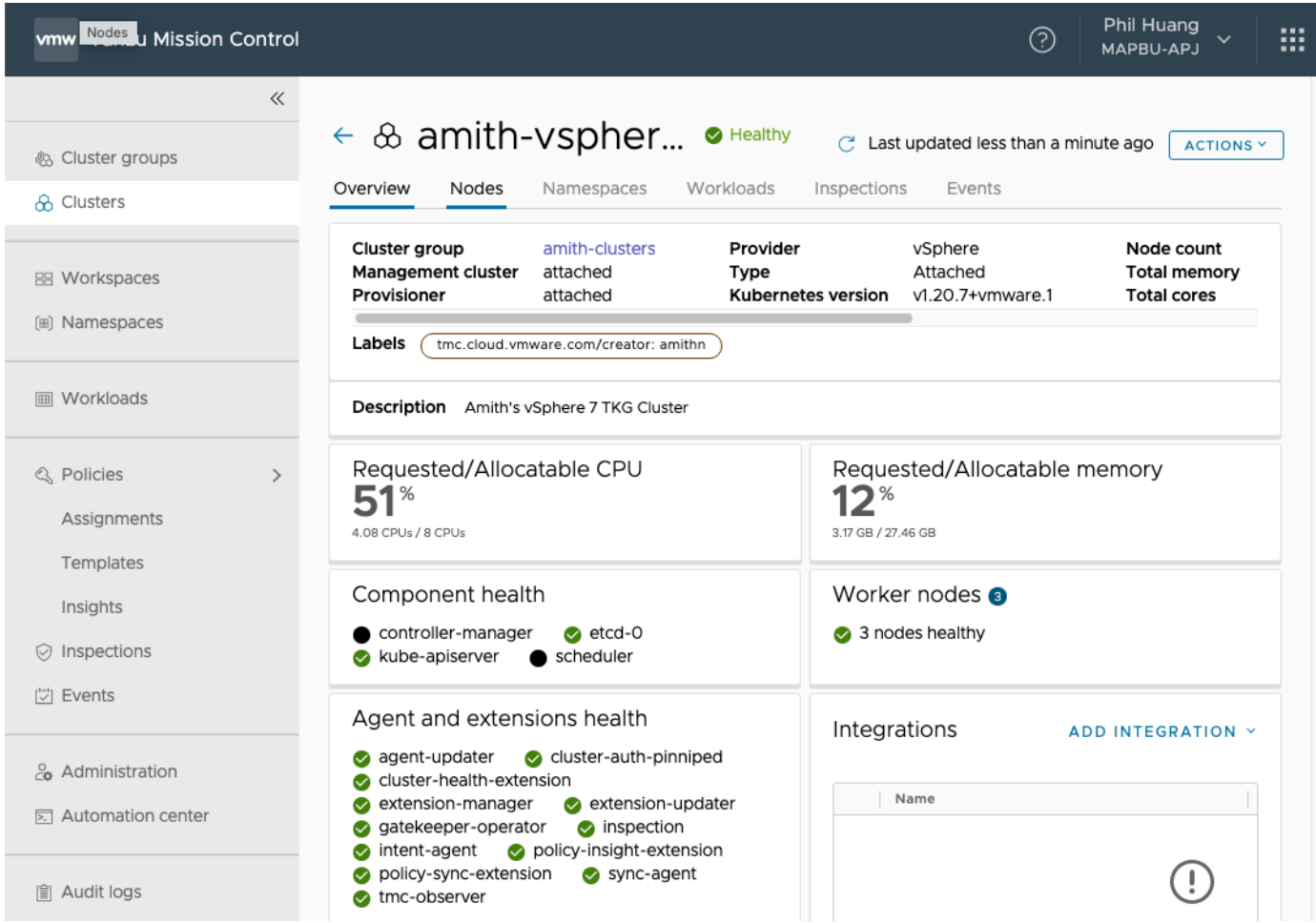
- 部署新的 Tanzu Kubernetes Grid 叢集
  - vSphere
  - AWS
  - Azure
- 管理既有已符合標準 Kubernetes API 的叢集
  - Tanzu Kubernetes Grid
  - vSphere with Tanzu
  - GKE / AKS / EKS / OCP



全叢集狀態可視化 Global Visibility and Diagnostics

基於標準 Kubernetes API 獲取叢集資訊

- 針對特定叢集提供下列 6 點 Kubernetes 檢視能力
  1. Overview
  2. Nodes
  3. Namespace
  4. Workload
  5. Inspection
  6. Events
- 透過以上能力可快速了解特定叢集內資源利用狀態、工作負載狀態、叢集持續合規性檢查

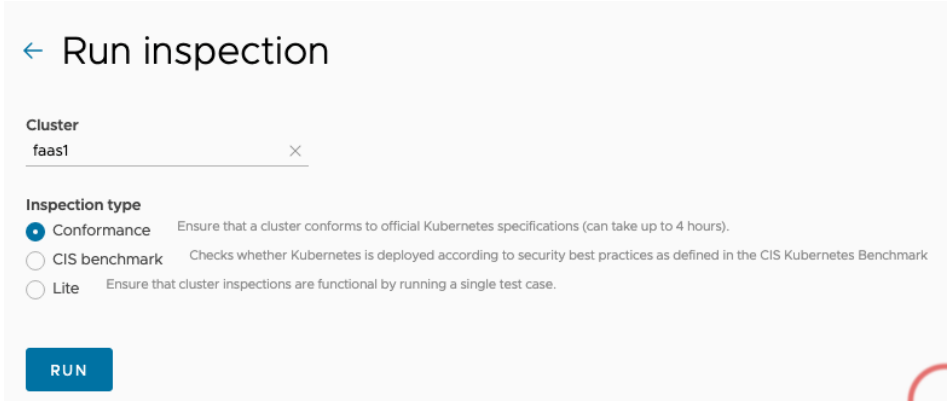


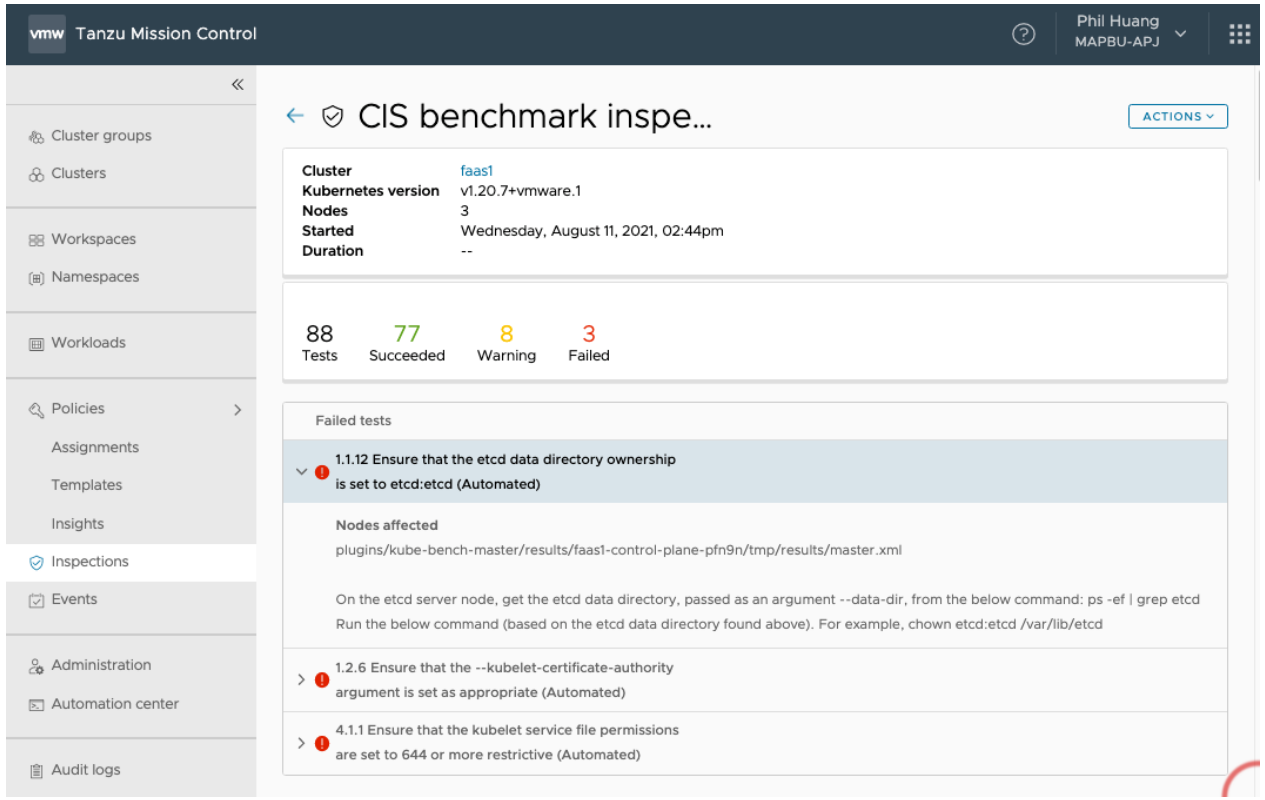
Ref: VMware Tanzu Mission Control – About Getting Started with VMware Tanzu Mission Control

叢集合規檢查機制 Cluster Inspection

內建 Project Sonobuoy 提供多叢集環境一致性檢查

- 可針對特定叢集運行 3 種 Inspection 檢查
  1. Conformance：基於 K8s 驗證標準測試
  2. CIS Benchmark：基於 CIS 公布之基準評估叢集合規性
  3. Lite：進行簡單 Pod 新增移除測試
- 可於網頁上直接觀察檢查及確認測驗報告



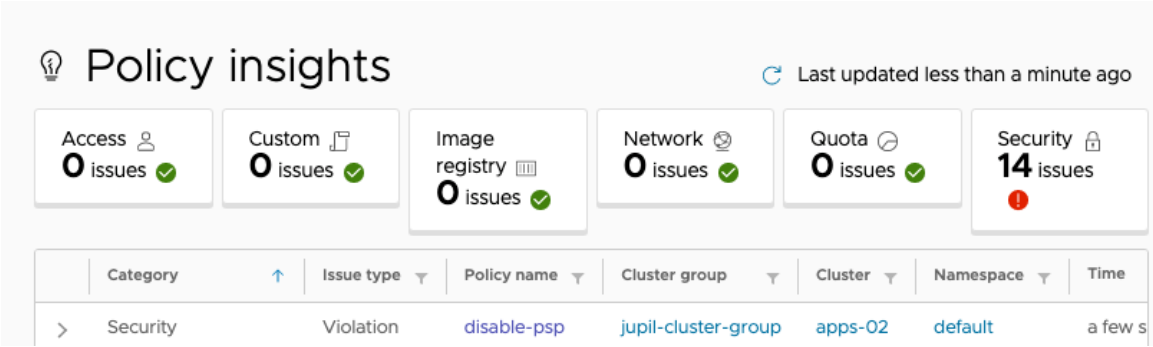


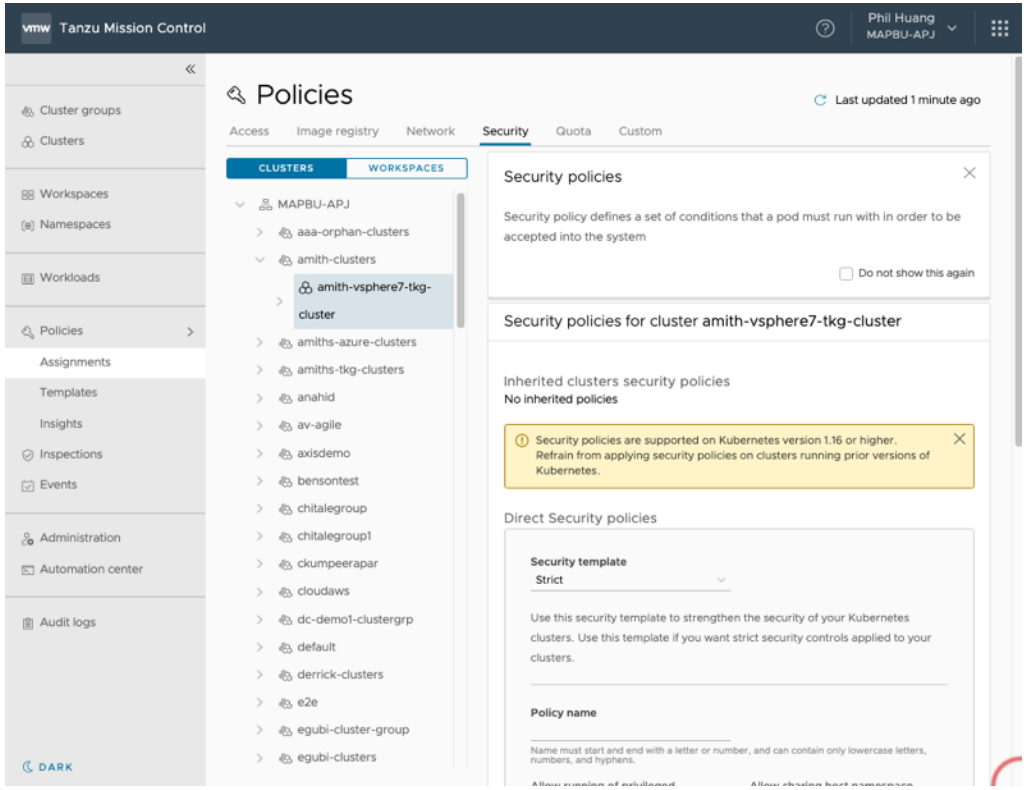
Ref: VMware Tanzu Mission Control – Cluster Inspection

集中式策略管理 Centralized Policy Management

內建 Open Policy Agent 管理多叢集策略

- 針對多叢集管理提供 Policy 管控機制，包含 5 大面向
  1. Access
  2. Image Registry
  3. Network
  4. Security
  5. Quota
- 透過 Policy Insight 可快速識別所有叢集所遭遇的 Policy 管理衝突，進行修復
- 透過 Policy Template 可確保每一個叢集初始匯入的 Policy 皆保持一致



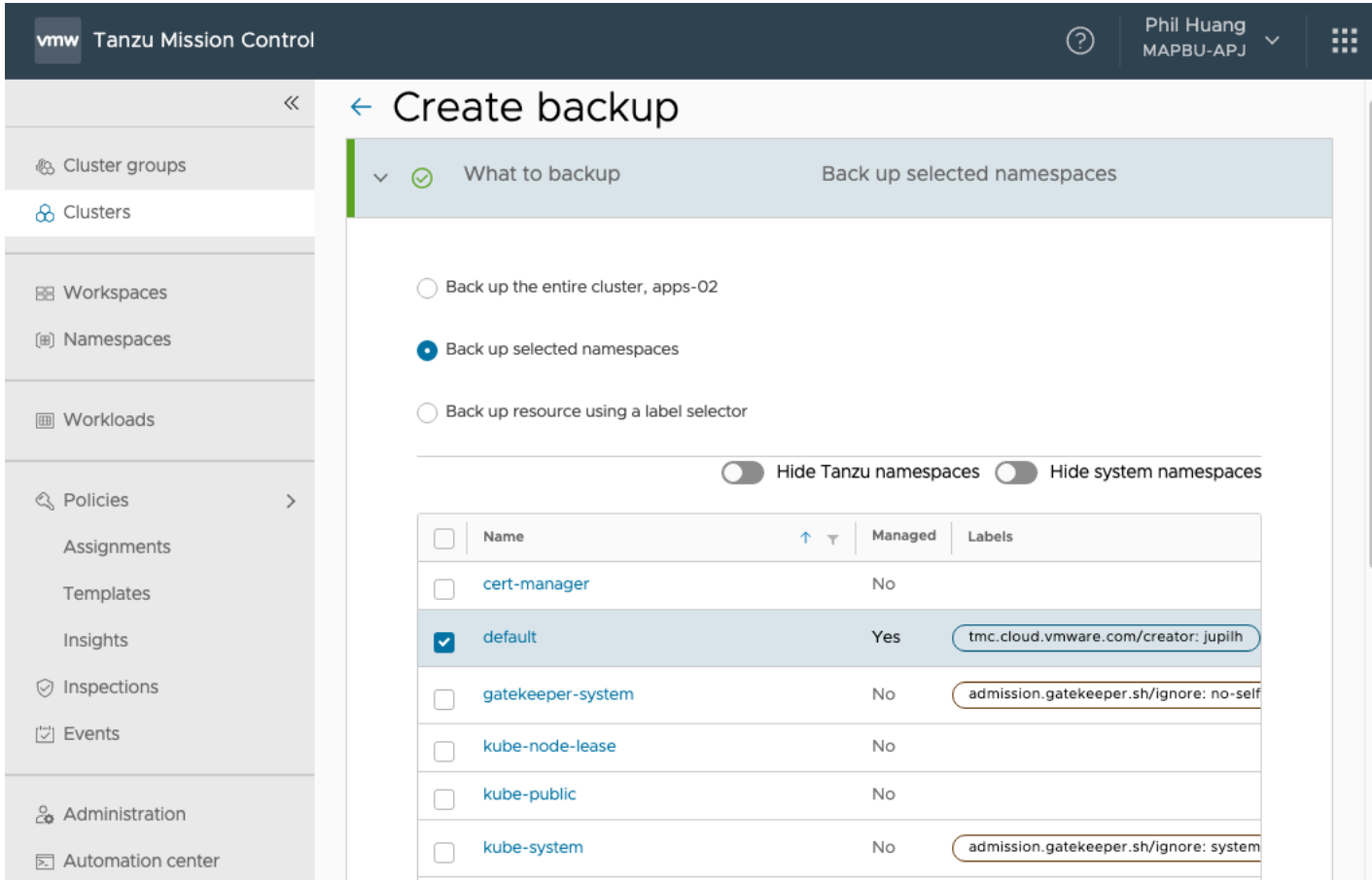


Ref: VMware Tanzu Mission Control – Policy-Driven Cluster Management

資料保護 Data Protection

內建 Velero 及 Restic 進行雲原生備份還原能力

- 針對特定叢集可進行以下 3 種備份操作
  1. 特定叢集全備份
  2. 特定叢集之特定 Namespace 備份
  3. 特定叢集之特定 Label 備份



Ref: VMware Tanzu Mission Control – Data Protection

Tanzu Mission Control

集中式 Kubernetes 管理平台所提供 3 大優勢

VMware Tanzu™
Mission Control™

雲原生可觀測性的實踐

Tanzu Observability

管理現在多雲應用服務的挑戰

Digital Enterprise – innovation, customer satisfaction and competitiveness are at stake!

預期影響

過長的 MTTR
存有判斷盲區

難以整合不同數據
定位問題

較慢的應用服務
交付和創新

賺錢速度變慢
提升維運難度

新挑戰

對於各類基礎建設、服務及應用程式
有爆炸性成長

技術所造成穀倉效應, 警告風暴
難以端到端，輔以數據佐證，聚焦問題

新世界

APP

多樣化的現代化應用服務於多雲上

vmware CLOUD™ aws Azure Google Cloud

MTTR: Mean Time To Recovery，平均修復時間，將系統還原至正常狀態所需時間長度的平均值

可觀察性 Observability vs. 監控 Monitoring

可觀察性是能夠基於有效數據，回溯資訊、分析以及預測當前服務之行為

捕獲/顯示
可見的**外部**訊號

醫生看診

橫跨外部和詳細的內部指標之間關聯性分析

自動化數據統計分析

身體健康指標監測

Gartner

“現代應用程式和服務，其本身既有的複雜性，以及 DevOps 等新技術實踐的興起，讓取多組織對傳統的監控工具和技術感到沮喪”

“可觀察性工具減少了服務中斷的次數和其影響和嚴重性”

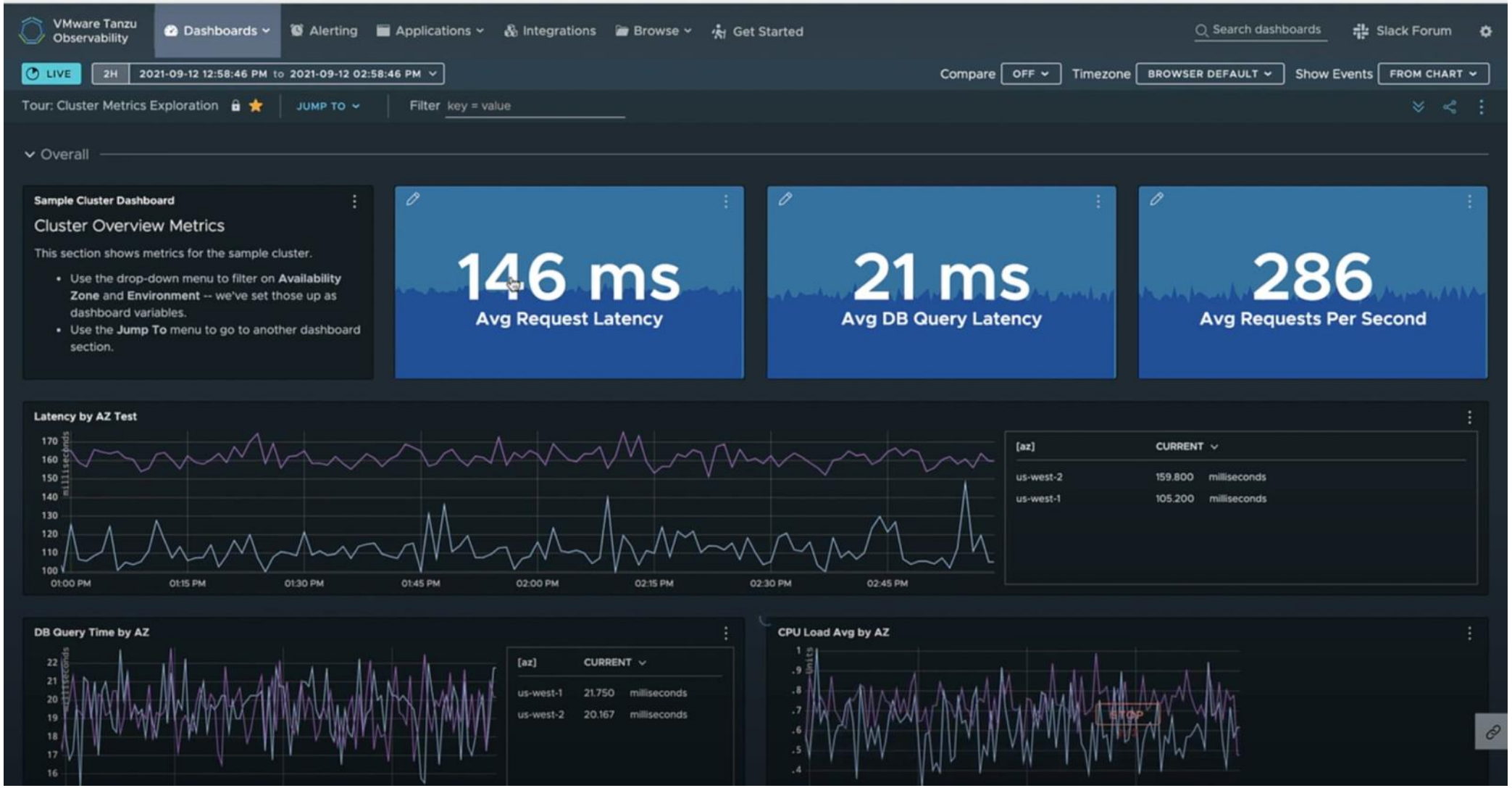
Gartner, Hype Cycle for IT Performance Analysis, 30 July, 2019

Tanzu Observability 確保完整堆疊的平台可觀察性

讓組織內的所有相關人員能運用單一資料來源

資料視覺化圖表：美觀、優良、正確

Tanzu Observability - Dashboard



具體 Tanzu Observability 是收集什麼資料?

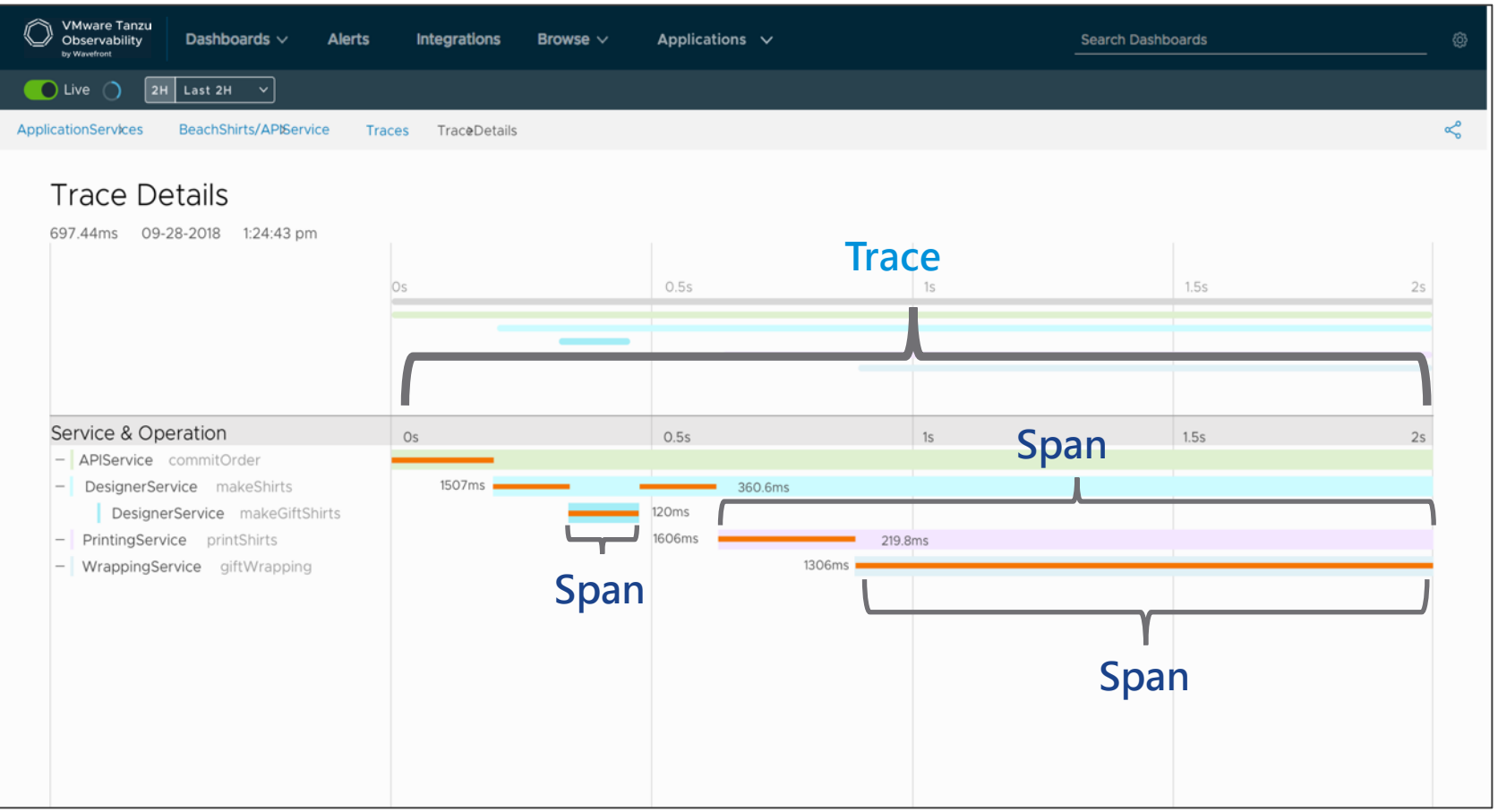
基於 Time Series 格式，採集 6 大指標類型

Metrics	Description	Use Cases	Remark
儀表 Gauge	顯示指標的即時變化，可增可減	CPU Load / Memory Usage / Network Connections	同 Prometheus Metrics Type
計數器 Counter	顯示指標值只增不減	機器啟動時間、HTTP 訪問量	同 Prometheus Metrics Type
直方圖 Histogram	顯示某個區間的數據分佈狀況	適用於非常高頻率的數據	同 Prometheus Metrics Type
Delta Counter	用於監控 Serverless 的突發流量	顯示 FaaS 功能執行或失敗次數	
跟蹤 Trace	基於應用程式中的單個工作流，顯示特定請求如何通過應用程序進行傳播	Distrubuted Tracing	基於 OpenTelemetry 標準
跨度 Span	Trace 中的最小單位。表示服務中的操作所花費時間	Distrubuted Tracing	基於 OpenTelemetry 標準

Ref: https://docs.wavefront.com/metric_types.html#summary-of-metric-types

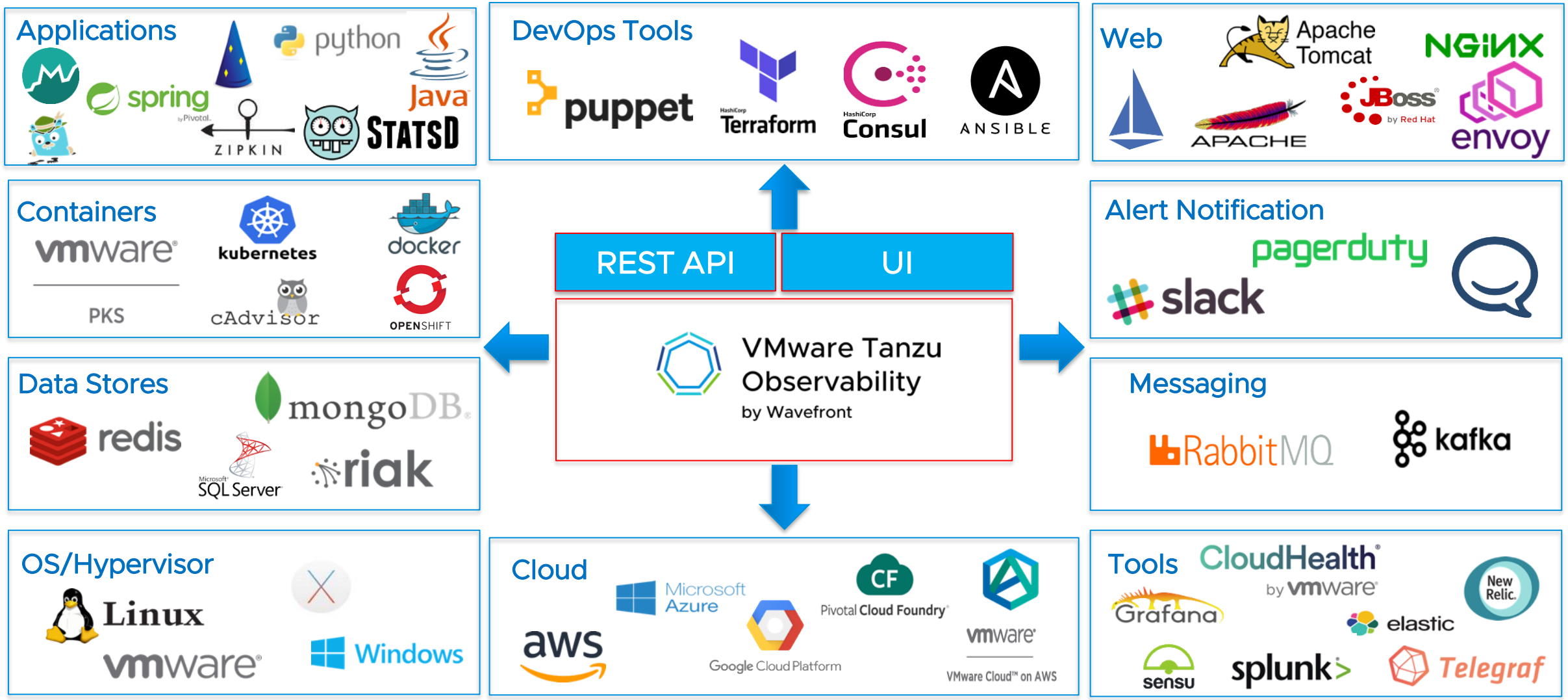
直觀分析呼叫順序、快速定位效能瓶頸

Tanzu Observability – 分散式追蹤 Distributed Tracing



- **更輕易地監控微服務：**相容於 OpenTelemetry 標準，可以新增自訂義 Metrics
- **更快速地定位瓶頸：** 更直觀地了解每一個 Trace 所呼叫的上下文順序 (SpanContext) 邏輯關係，進而迅速收斂可能問題點
- **更高效地優化程式：** 透過分析 Trace 內部的 Span 過程，更能迅速地定位 API / SDK 呼叫時的效能瓶頸

Tanzu Observability 提供 200+ 種應用程式的可見性



為何要採用 Tanzu Observability?

藉由 Tanzu Observability 導入實踐更快速的維運所需及開發所要之交付能力

負責系統監控者

- 針對不同平台維運所需之開箱即用儀表板
- AIOps 協助快速進行異常檢測 (Anomaly Detection)
- 長達 18 個月之資料儲存及分析
- 提供 200+ 以上應用程式整合及平台整合
- 客製化函數計算能力
- 採用單一計價方式

負責應用服務開發者

- 針對常見 App 提供開箱即用儀表板
- AIOps 協助快速進行異常檢測 (Anomaly Detection)
- 支援開放標準雲原生可遙測框架 OpenTelemetry
- 可使用 Trace / Span 進行端到端 Distributed Tracing
- 1s 圖表即時呈現能力

VMware Tanzu for Kubernetes Operations Hands on Lab

- (HOL-2234-02-MAP)

Title	Time
Introduction to Tanzu for Kubernetes Operations	15 min
Introduction to Tanzu Kubernetes Grid	45 min
VMware Tanzu Mission Control	30 min
Tanzu Observability Basics	15 min
Introduction to NSX Advanced Load Balancer (Avi)	15 min
Introduction to Tanzu Service Mesh	15 min
Introduction to Harbor	30 min

https://labs.hol.vmware.com/HOL/catalogs/lab/104

Thank You

