SUSE

19TH OCTOBER 2022

後疫情時代數位轉型 – 提升敏捷力打造企業競爭力

陳瑞文 (Wales Chen)

SUSE 台灣區解決方案暨產品經理

企業競爭力？

企業競爭力？

1

在競爭性市場條件下，企業通過培育自身資源和能力，獲取外部可定址資源，並綜合加以利用，在為顧客創造價值的基礎上，實現自身價值的綜合性能力

2

是指在競爭性的市場中，一個企業所具有的能夠**比其他企業更有效地向市場提供產品和服務**，並獲得贏利和自身發展的綜合素質

敏捷力

應用服務容器化並透過完善且安全的資源配置機制
讓企業營運更加靈活並即時回應需求

敏捷力

應用服務 容器平台 並透過 容器安全 的 Kubernetes 機制
讓企業營運更加靈活並即時回應需求

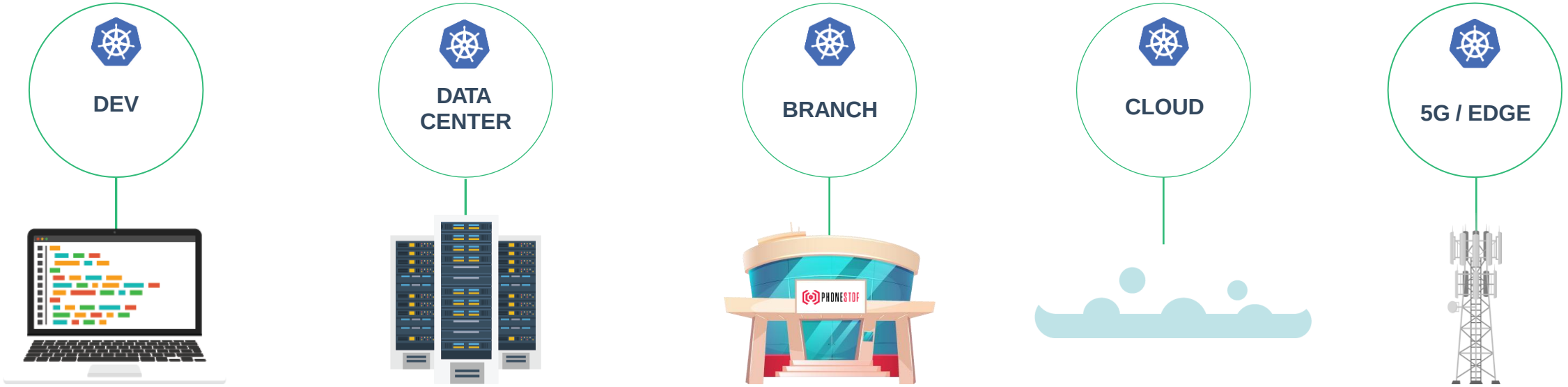
敏捷力

應用服務 RKE 並透過 NeuVector 的 Rancher 機制
讓企業營運更加靈活並即時回應需求

- RKE – Rancher Kubernetes Engine (K8S 平台)
- NeuVector – 容器安全平台
- Rancher – 多雲多叢集 K8S 管理平台

Kubernetes 叢集無所不在...

Kubernetes 與容器化應用已從雲端擴展至邊緣

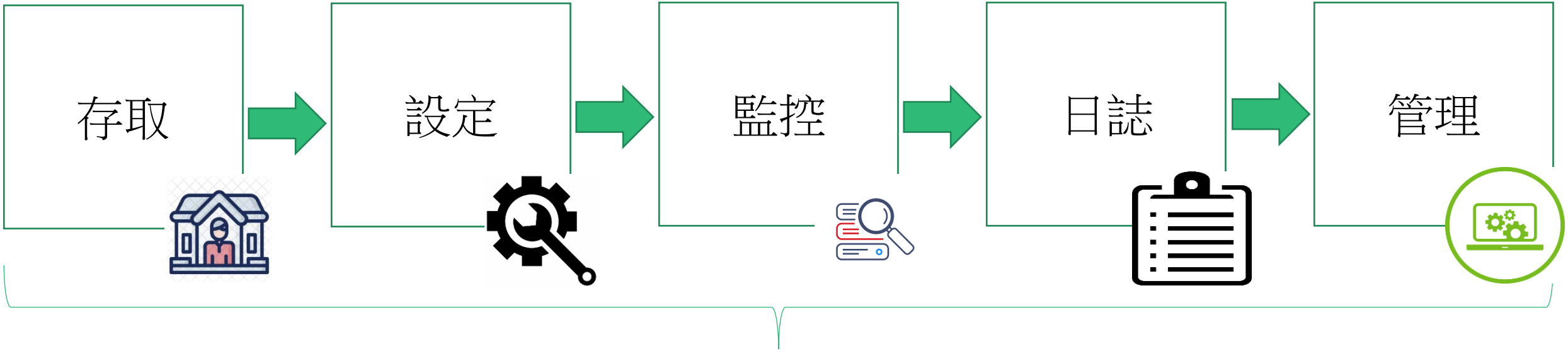


Kubernetes 叢集無所不在...

Kubernetes 與容器化應用已從雲端擴展至邊緣

該如何做到 Kubernetes 多雲多叢集管理 ?

Kubernetes 多雲多叢集管理應該包括？



Rancher Multi-Cluster Management
（多雲多叢集管理）

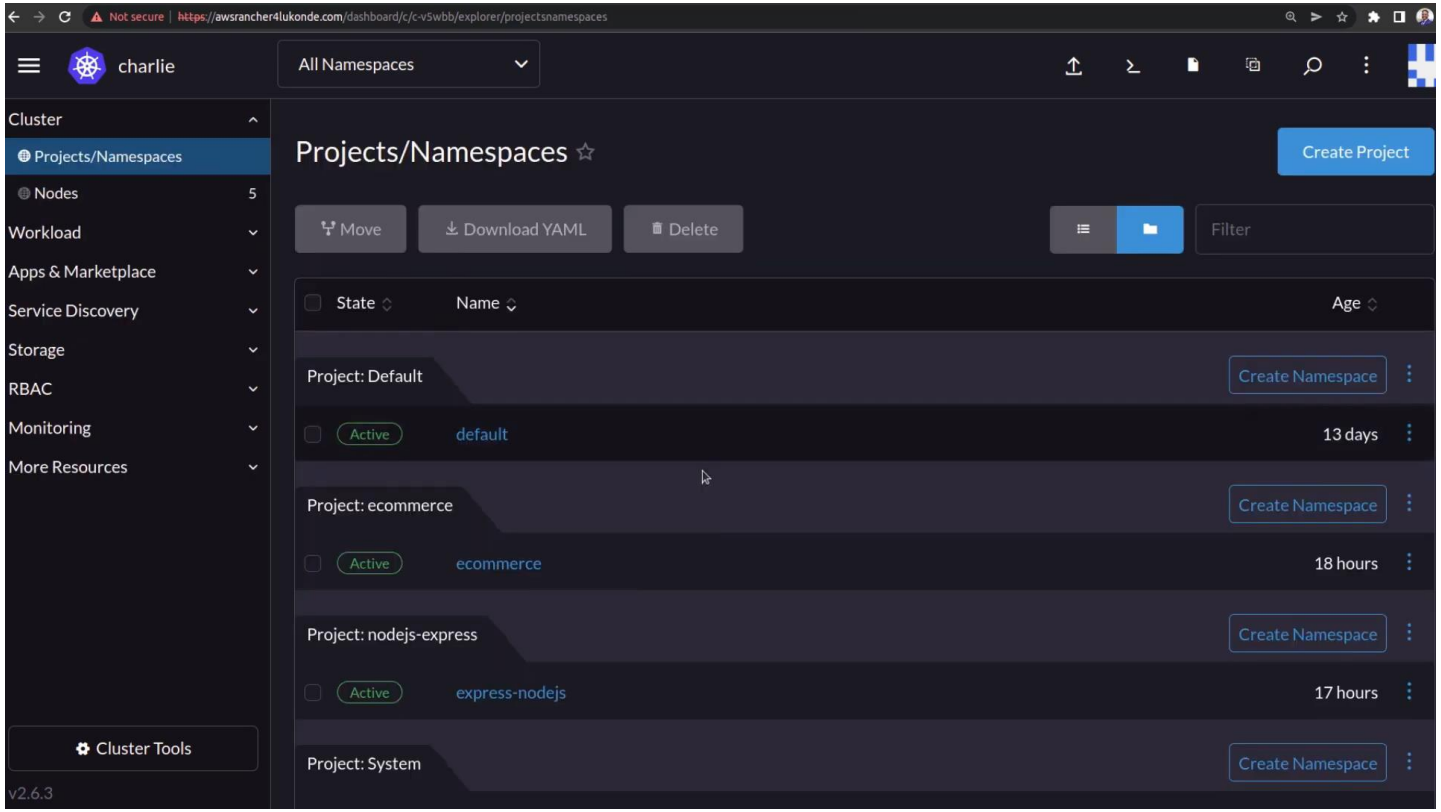
Kubernetes 多雲多叢集管理應該包括？

存取

針對操作與開發人員提供有管控的資源存取

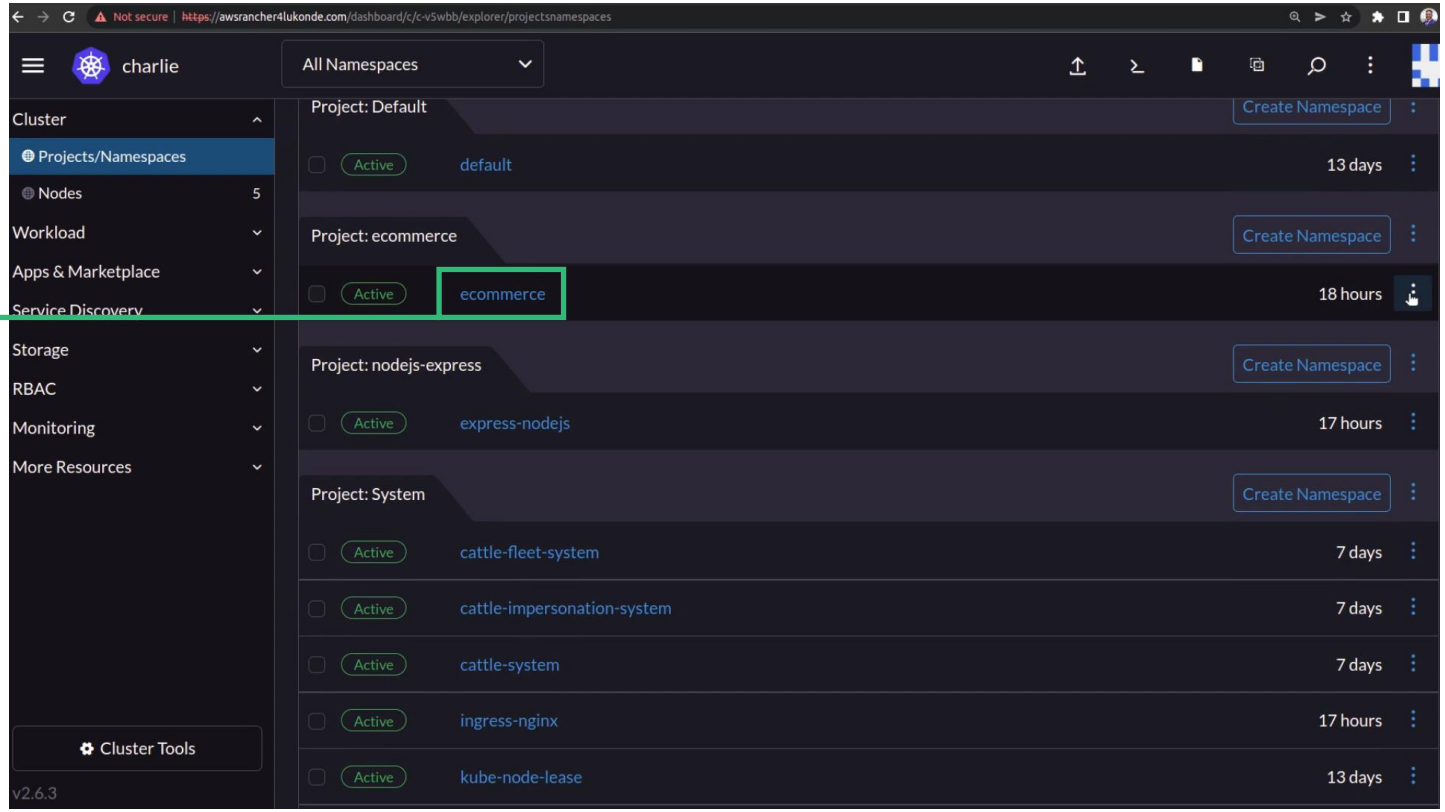
多租戶支援 (multi-tenancy) 及租戶隔離 (isolation)

- 支持各租戶獨享叢集
- 支援多租戶共用叢集並實現工作負載隔離、資源 配額管理
- 獨享叢集、共用叢集下實現嚴格管控同時支持用戶的靈活訪問和設置



多租戶支援 (multi-tenancy) 及租戶隔離 (isolation)

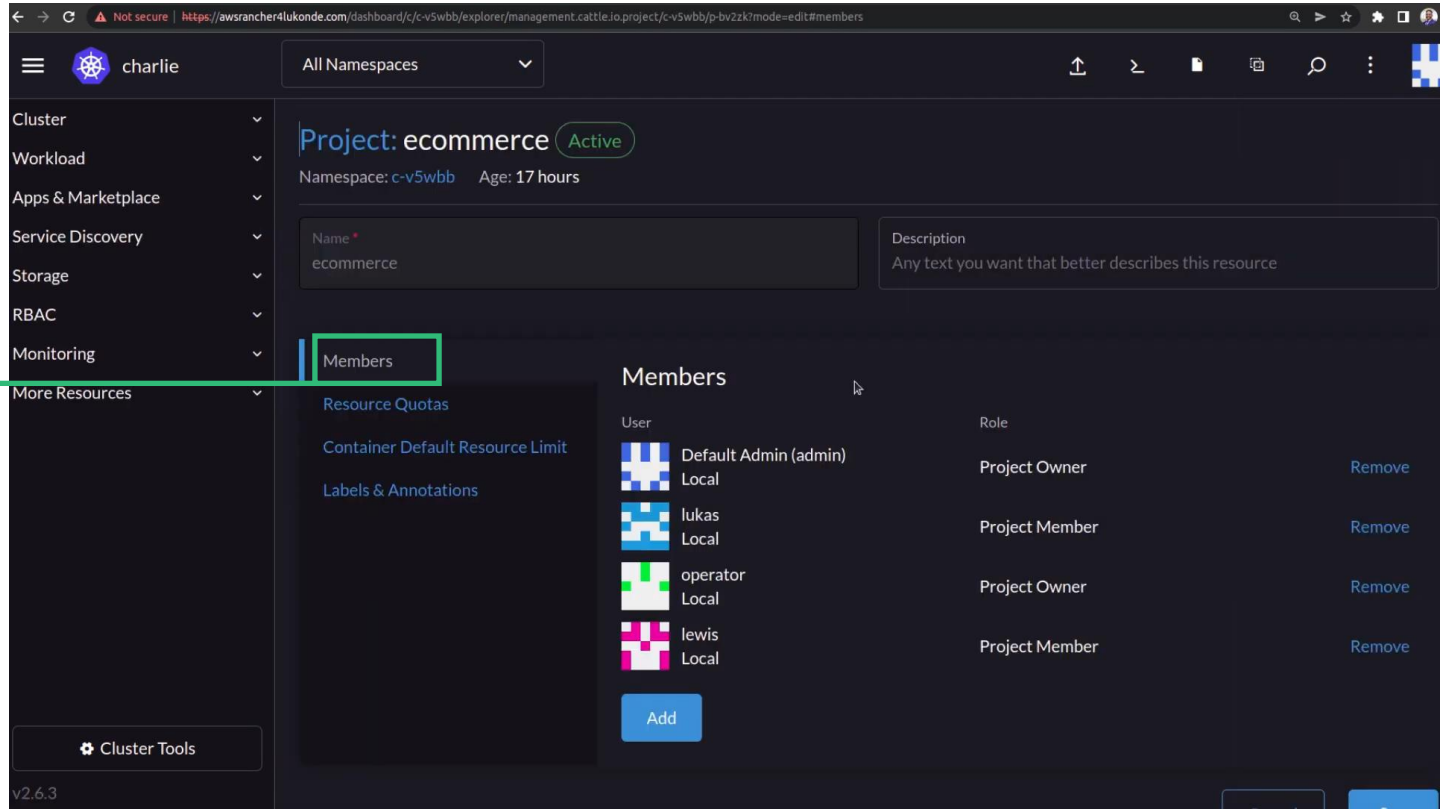
- 支持各租戶獨享叢集
- 支援多租戶共用叢集並實現工作負載隔離、資源 配額管理
- 獨享叢集、共用叢集下實現嚴格管控同時支持用戶的靈活訪問和設置



以 ecommerce project 為例

多租戶支援 (multi-tenancy) 及租戶隔離 (isolation)

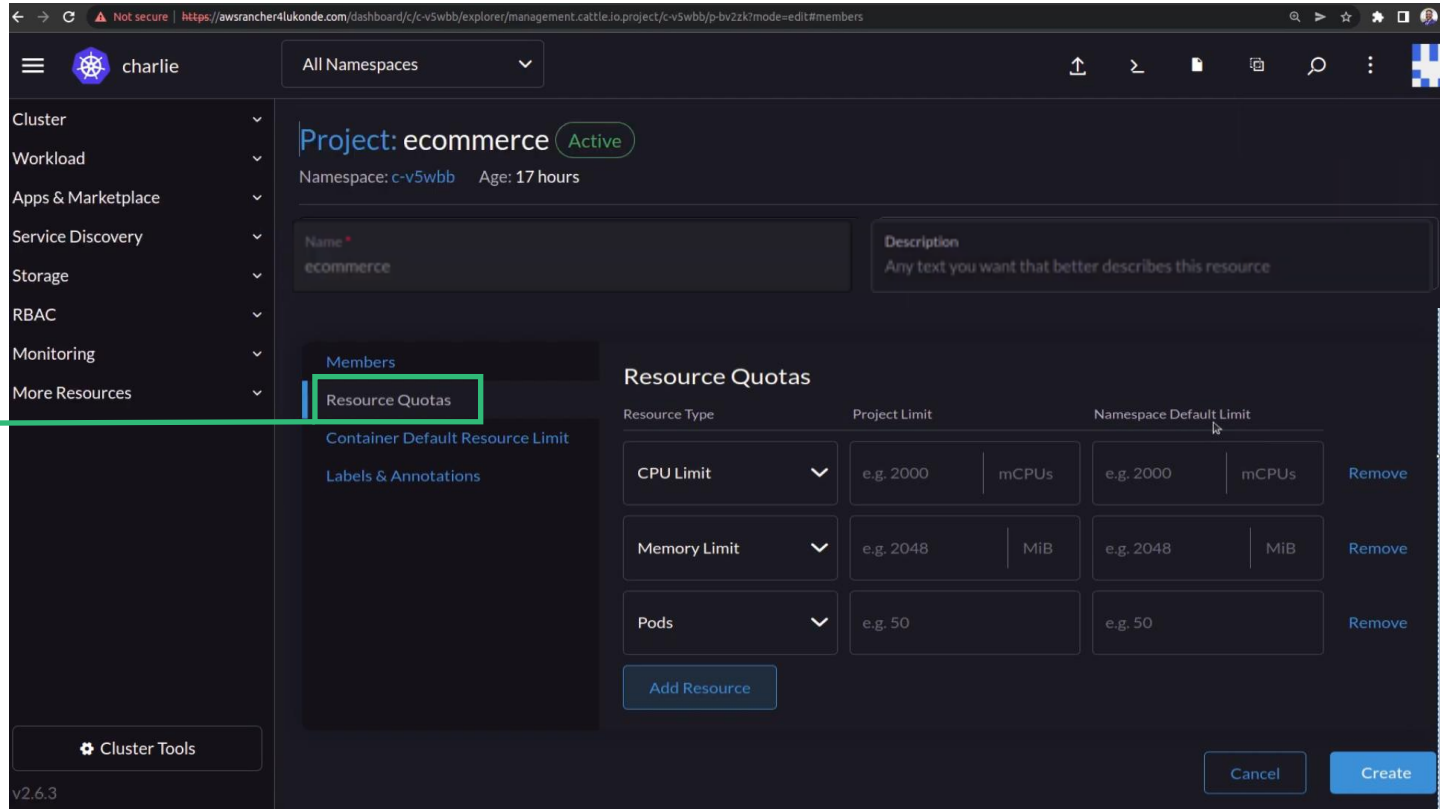
- 支持各租戶獨享叢集
- 支援多租戶共用叢集並實現工作負載隔離、資源 配額管理
- 獨享叢集、共用叢集下實現嚴格管控同時支持用戶的靈活訪問和設置



制定可存取的租戶 (members)

多租戶支援 (multi-tenancy) 及租戶隔離 (isolation)

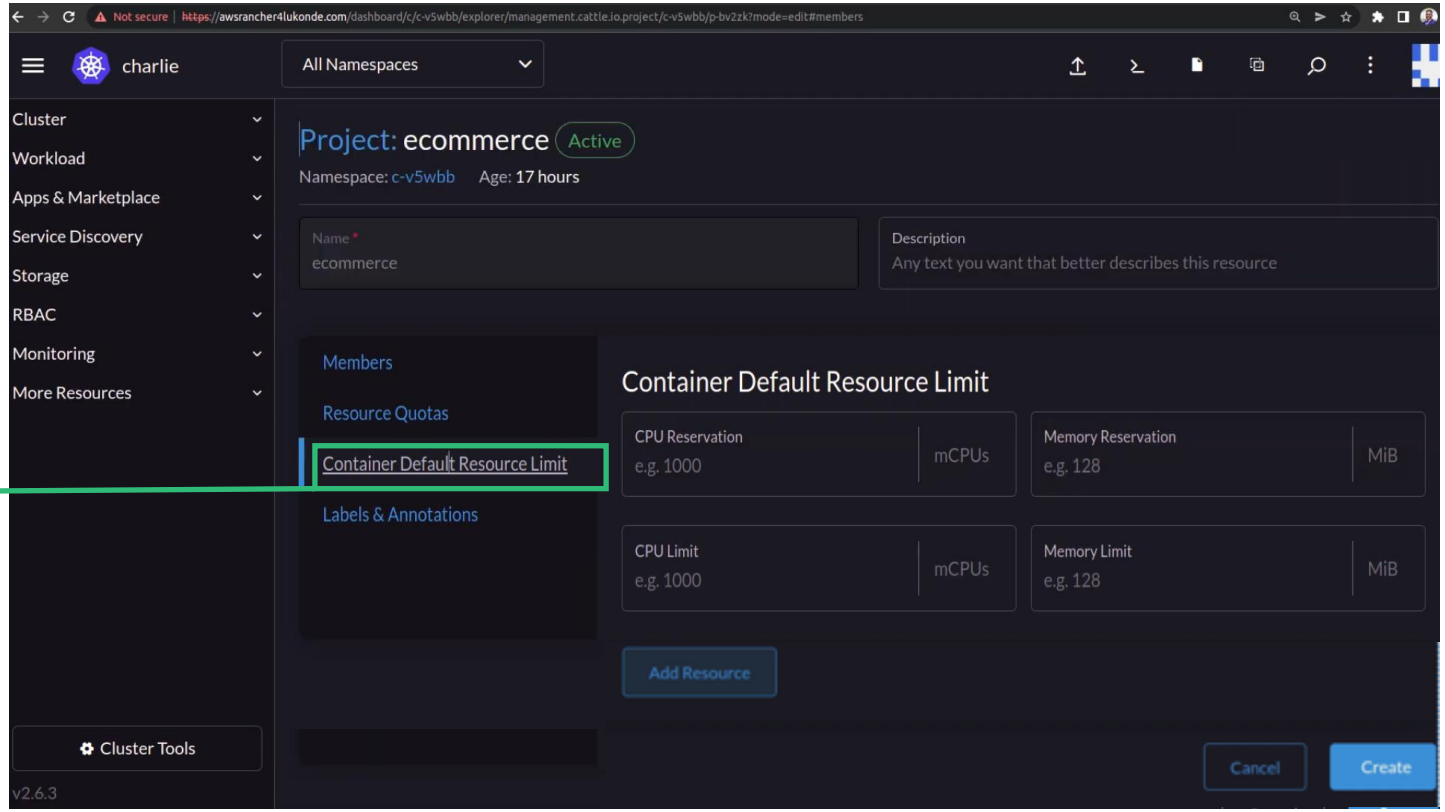
- 支持各租戶獨享叢集
- 支援多租戶共用叢集並實現工作負載隔離、資源 配額管理
- 獨享叢集、共用叢集下實現嚴格管控同時支持用戶的靈活訪問和設置



設定可使用的資源 (resource quota)

多租戶支援 (multi-tenancy) 及租戶隔離 (isolation)

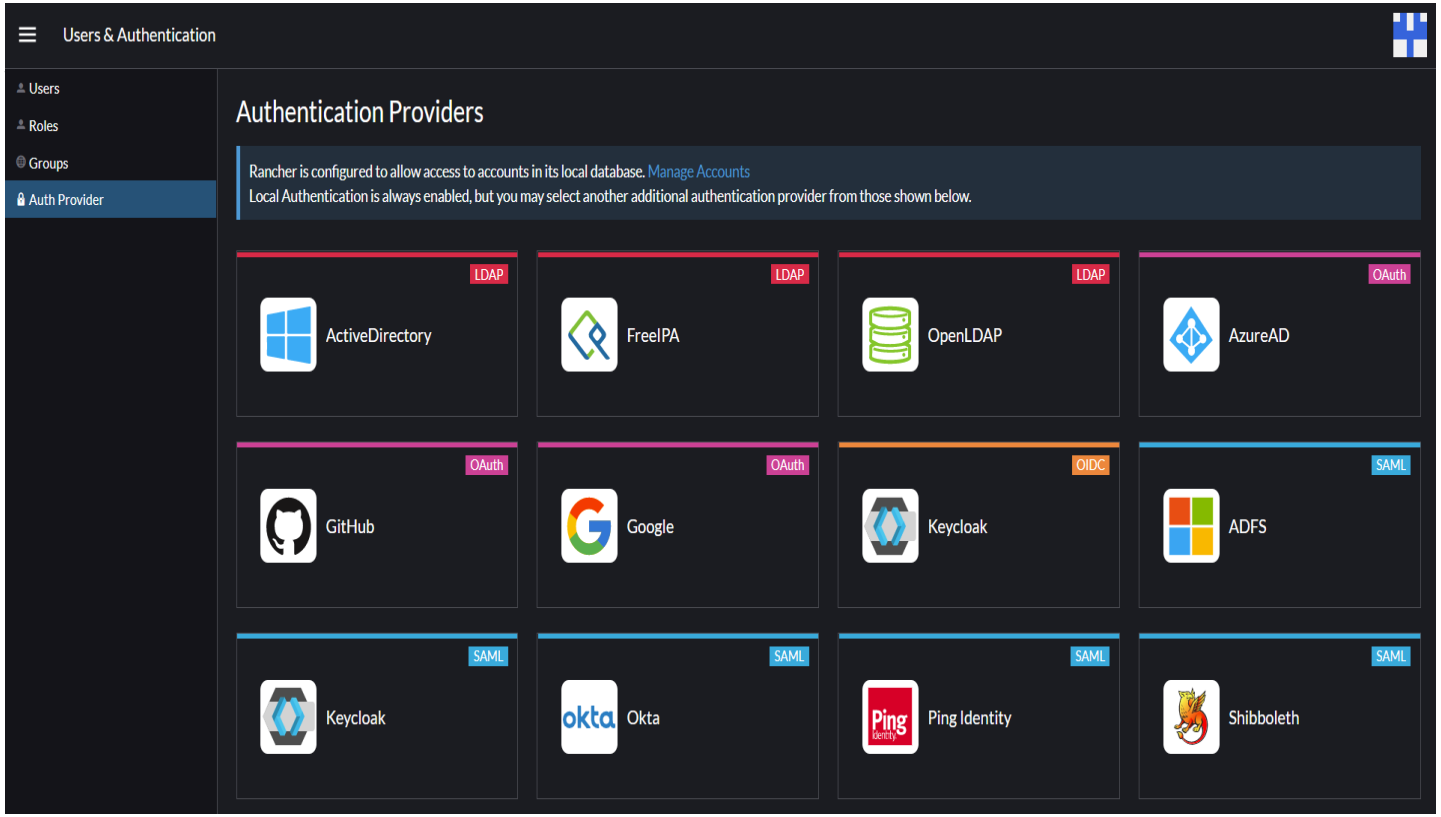
- 支持各租戶獨享叢集
- 支援多租戶共用叢集並實現工作負載隔離、資源 配額管理
- 獨享叢集、共用叢集下實現嚴格管控同時支持用戶的靈活訪問和設置



設定容器內的預設資源上限 (limits)

多租戶機制整合集中式用戶管理

- 多種認證方式整合 (AD, Azure LDAP, Github, SAML, etc.)
- 全域、叢集、專案等多層級的用戶角色定義和控制
- 支援 RBAC 自訂角色管理



Kubernetes 多雲多叢集管理應該包括？

設定

透過**單一設定**機制讓部署與運作簡單化

設定管理的必要性

- 方式一致降低風險
- 靈活且有效率
- 可信賴

常見且 **SUSE** 支援的設定管理工具

- Ansible
- SaltStack
- Etc...

常見且適用於 IT 基礎架構的設定與管理

SUSE Manager 支援 Ansible 與 Salt 腳本, 執行伺服器的 package 與 patch 更新等等

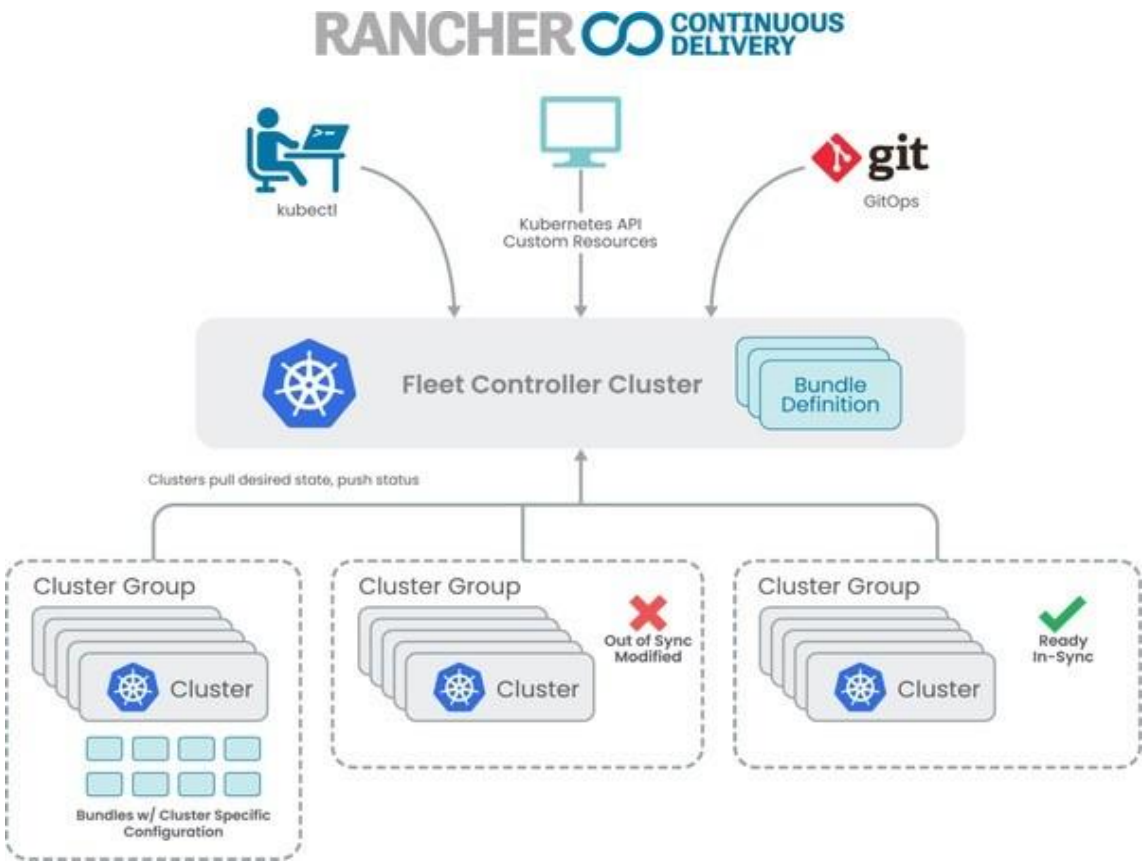
但這些好像不太適用於 K8S 應用服務 ???

針對 Kubernetes 常見的 GitOps 工具

- Argo CD —— SUSE Rancher 整合
- Fleet —— SUSE Rancher 內建
- Etc...

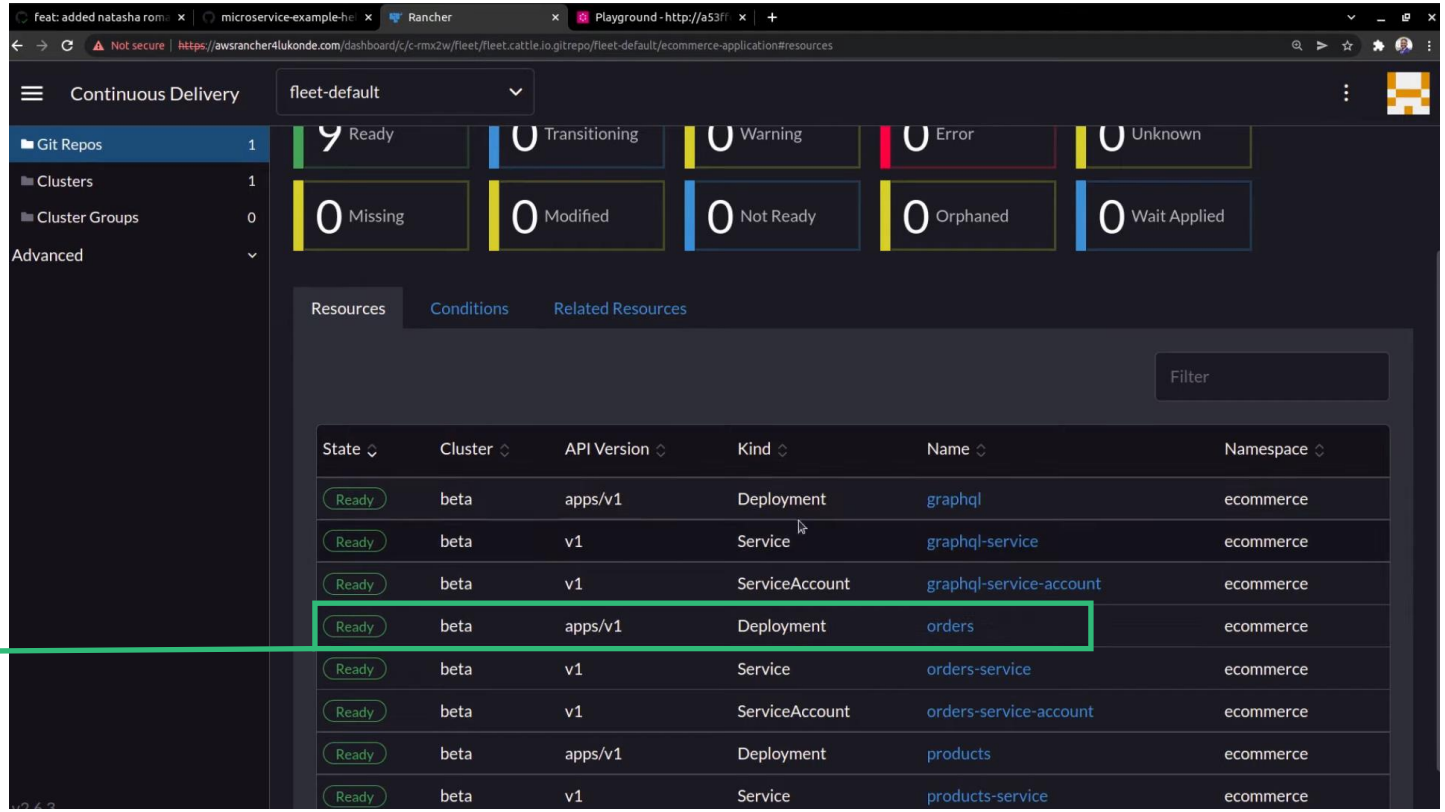
Fleet – SUSE Rancher 內建並提供商業支援的 GitOps 工具

- Fleet Manager (gitjob 組件 polling) 從 git pull 代碼
- Fleet Manager 運行 “fleet apply”通過 k8s resource 檔生成
- bundles 資源對象
- 為每個下游叢集生成 bundleDeployment 資源對象
- 下游 agent 從 Fleet Manager 中 pull bundleDeployment 資源對象
- 生成 Helm charts & 運行 Helm 部署
- 更新狀態資訊



Fleet – SUSE Rancher 內建並提供商業支援的 GitOps 工具

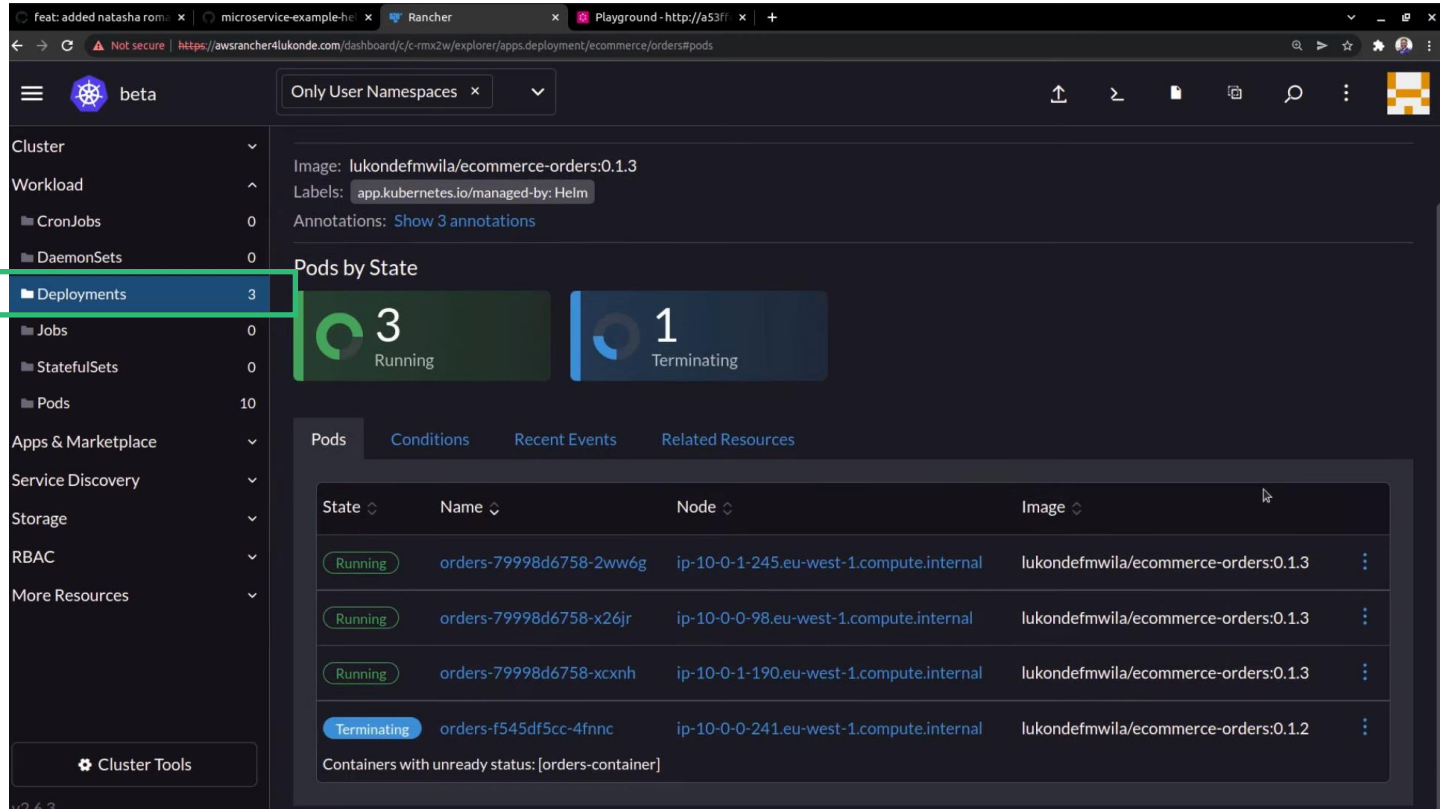
- 支援多叢集
- 支援多租戶
- 透過 CRD 定義設定



名稱為 orders 的 deployment, 點擊它...

Fleet – SUSE Rancher 內建並提供商業支援的 GitOps 工具

- 支援多叢集
- 支援多租戶
- 透過 CRD 定義設定



看到詳細資訊及允許進一步的操作

Kubernetes 多雲多叢集管理應該包括哪些？

監控

透過完整的**監控**機制即時**示警**並**通知**管理人員

整合 Prometheus & Grafana 與示警機制進行監控與通知

- 內建並透過 Prometheus 針對以下元件進行監控與示警
  - 叢集 node 的狀態與程序
  - Kubernetes 元件
  - 軟體部署
- 允許管理人員客製 Grafana 儀表板內容
- 啟動監控後, 透過 Notifiers 經由以下方式通知管理人員任示警事件
  - Slack, Email, PagerDuty, WeChat, 與 webhooks
- Alerts 則可針對 cluster 或 project 層級, 設定驅動 notification 的規則

Kubernetes 多雲多叢集管理應該包括哪些？

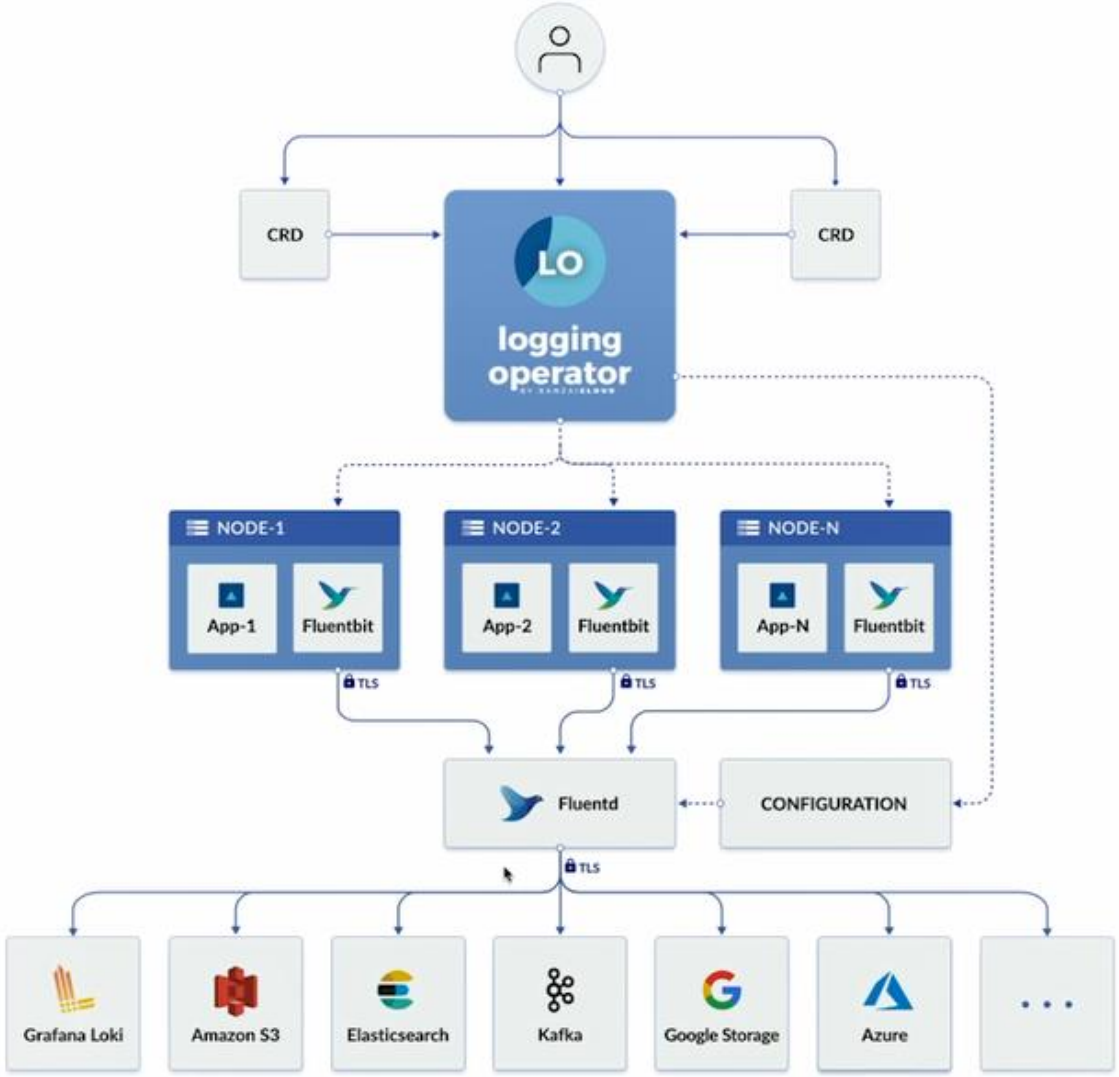
日誌

收集事件產生的日誌協助未來的問題分析

整合 Fluentbit 與 Fluentd 收集與管理日誌

- 支援 CustomResourceDefinitions

- 可制定日誌收集內容, 並透過 flows 機制將日誌 output 到指定的應用進行處理
  - Loki
  - Elasticsearch
  - Kafka
  - Etc...

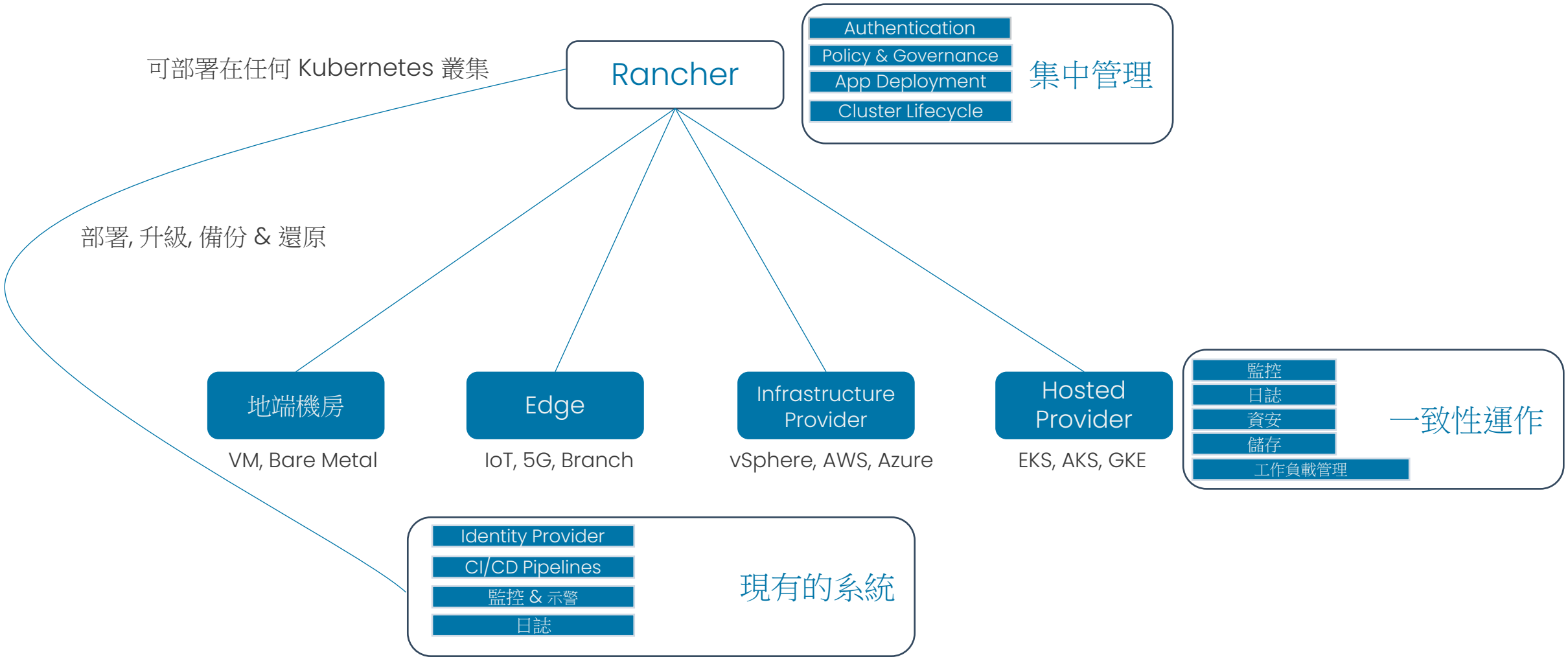


Kubernetes 多雲多叢集管理應該包括哪些？

管理

透過單一介面與機制管理 CNCF 認證的 K8S 叢集

透過 SUSE Rancher 集中管理符合 CNCF 認證的 K8S 叢集



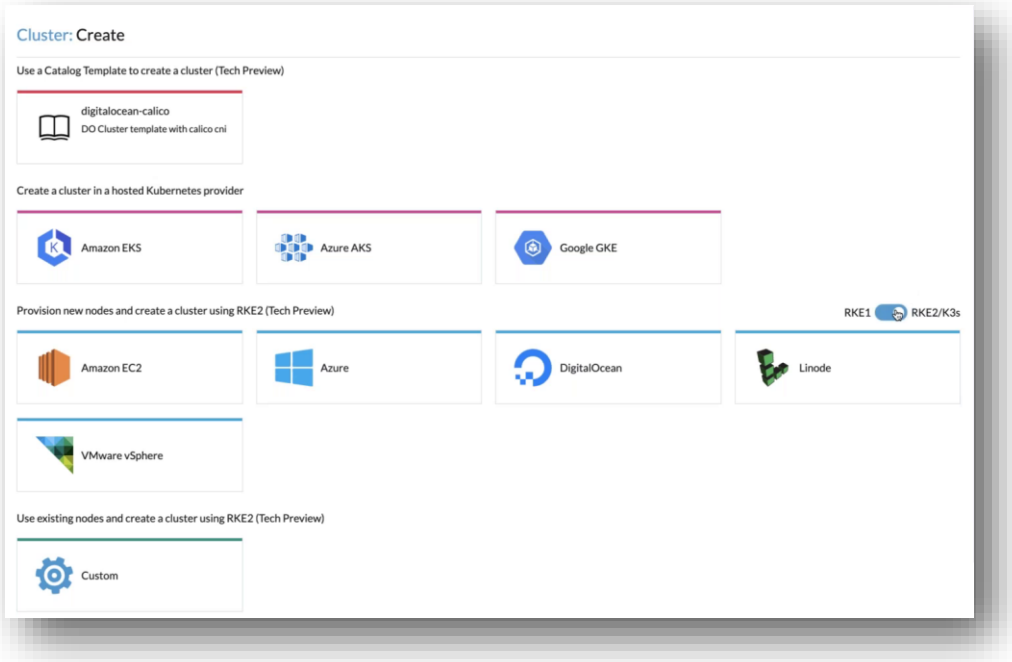
了解 Multi-Cloud 需求

- 為何 multi cloud?
  - 費用
  - 避免廠商 lock-in
  - 雲端特定功能 (IaaS/PaaS/DaaS/等等)
  - 應用服務 Agility
- 使用案例
  - 雲端炸裂
  - DR 災難備援
  - 職責切割 (Dev/Prod/Test)
- 為何 Kubernetes ?
  - 一致的 API
  - 標準的工具
- Rancher 如何讓這些變得更有利 ?

SUSE Rancher – 叢集的運作與管理

SUSE Rancher 大大降低初次部署與之後與 K8S 平台營運的上手難度

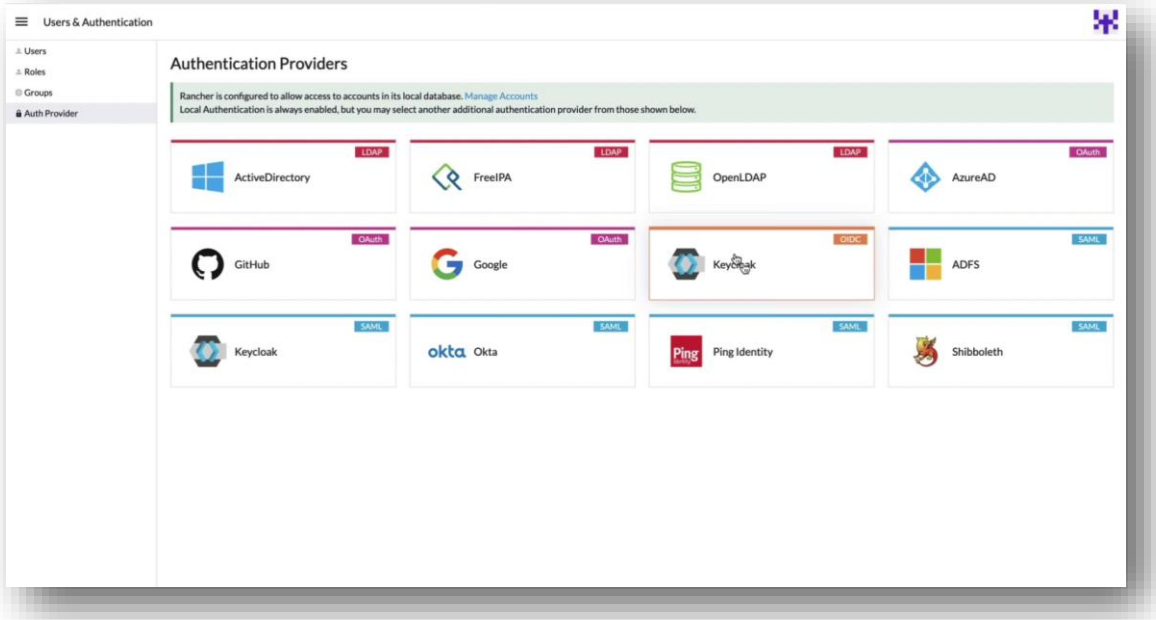
- 透過單一且一致的圖形介面與 API, 在任何基礎架構平台上部署 Kubernetes
- 管理完整的叢集生命週期, 包括升級, 擴充, 及災難備援
- 針對雲端代管的 Kubernetes 例如 AWS EKS, Azure AKS, 及 Google GKE 提供一流的支援
- 自動化與第三方服務整合的強化 API



SUSE Rancher – 整合的存取控管, 資安與政策管理

Rancher 支援集中身份驗證、訪問管理和一致的策略管理

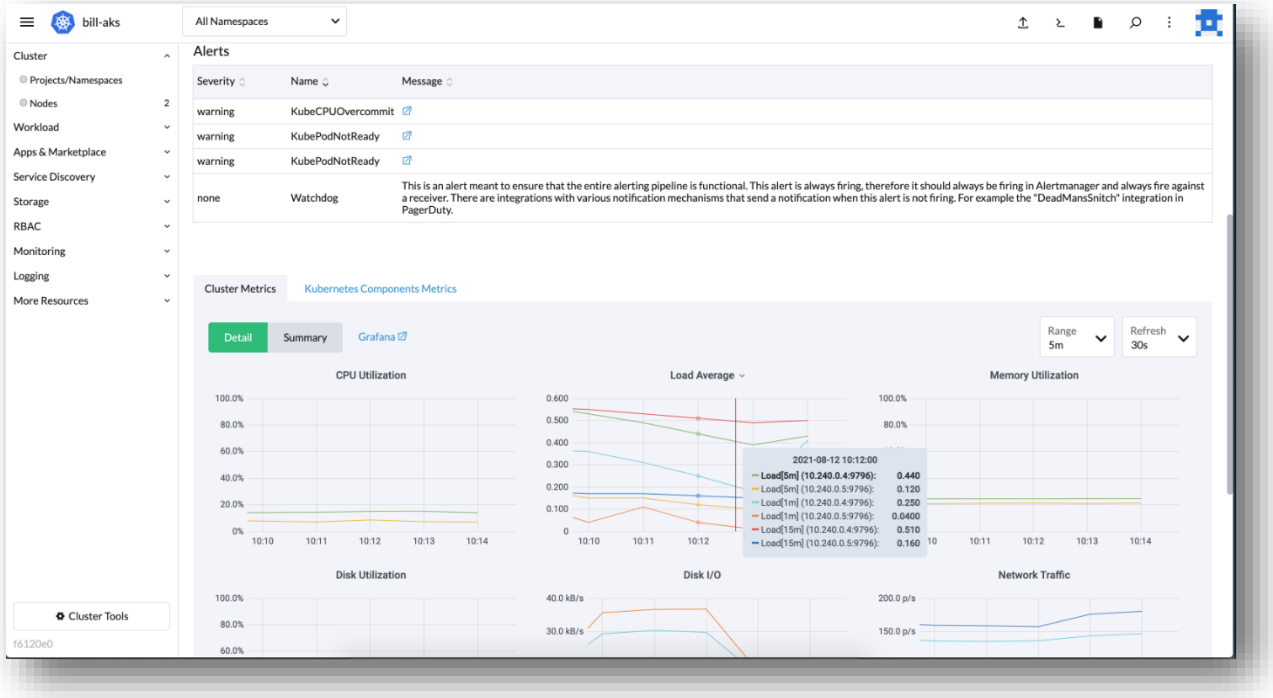
- 輕鬆將所有 Kubernetes 環境與現有的企業身份驗證提供程序（AD、LDAP、Keycloak 等）整合
- 有效率的集中存取控管之管理 (建構在 Kubernetes RBAC)
- 多租戶叢集的管理 (Rancher Projects)
- 資安與網路政策的集中管理
- 透過 CIS 叢集樣板, CIS Benchmark 合規掃描, 與 OPA 政策管理機制, 強化叢集運作



SUSE Rancher – 工作負載的管理

SUSE Rancher 針對工作負載管理與自助服務提供完善的 GUI 圖形操作介面

- 透過 GUI 圖形介面管理 Kubernetes 工作負載及資源
- 提供一個整合以 Helm 為基礎的應用市集
- 用於日誌傳送、監控、服務網格或持續交付的附加服務的 Turnkey Key 設定



Kubernetes 多雲多叢集管理應該包括哪些？

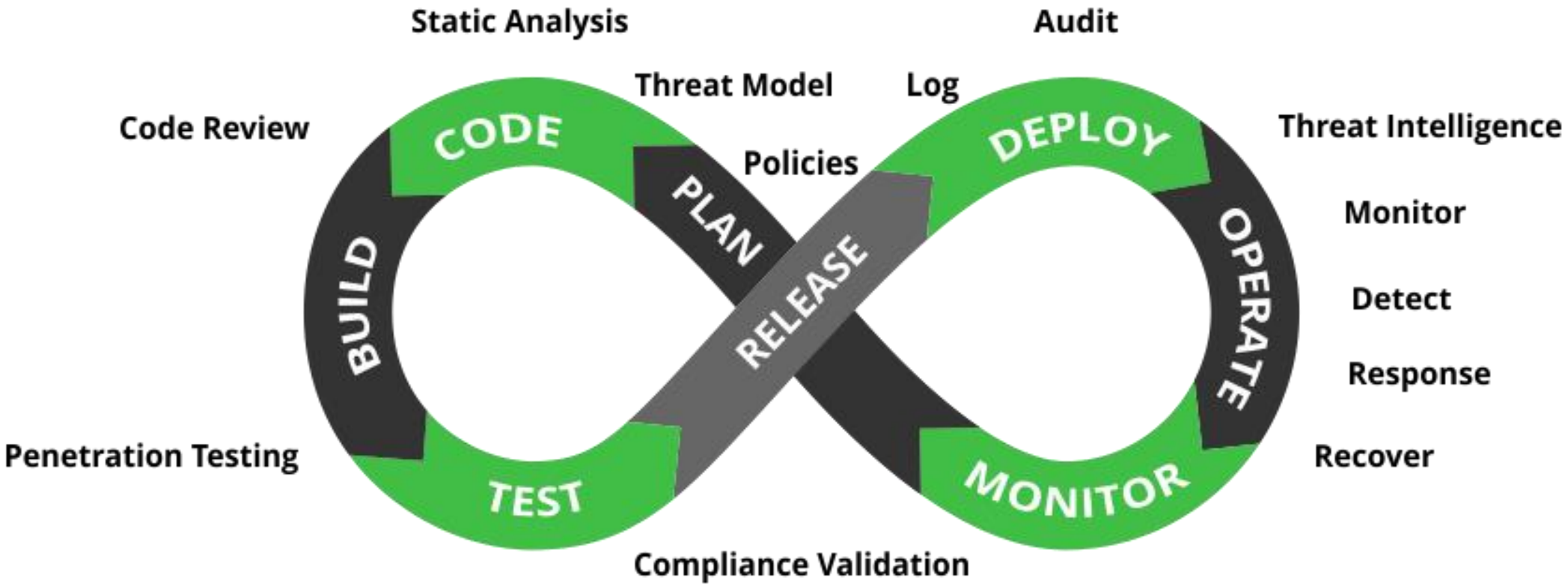
NeuVector 容器安全

存取 → 設定 → 監控 → 日誌 → 管理

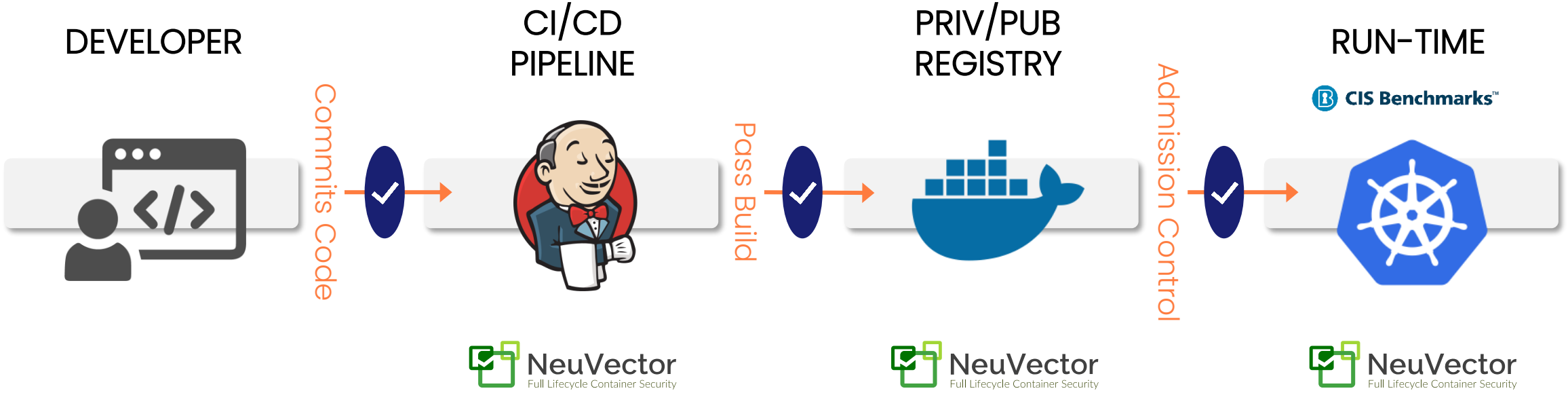




DevSecOps



NeuVector – 與 DevOps 流程 (CI/CD) 無縫對接



NeuVector – 涵蓋從開發到上線的完整容器資安保護

BUILD | TEST | STAGING | PRODUCTION

漏洞 & 合規管理

程式建置 掃描

映像倉庫 掃描

CIS 資安準則
& 客製化稽核

資安合規
PCI, GDPR, NIST

應用執行時掃描
容器, 主機, 平台

風險報告 & 修正

NeuVector – 涵蓋從開發到上線的完整容器資安保護

BUILD TEST STAGING PRODUCTION

漏洞 & 合規管理

程式建置 掃描

映像倉庫 掃描

CIS 資安準則
& 客製化稽核

資安合規
PCI, GDPR, NIST

應用執行時掃描
容器, 主機, 平台

應用執行時的保護

部署

精細管控

容器防火牆
整合深層封包分析/資料外洩防護的防護

容器工作負載資安
隔絕 程序 & 檔案系統

警示 & 鑑識

NeuVector – 涵蓋從開發到上線的完整容器資安保護

BUILD | TEST | STAGING | PRODUCTION

漏洞 & 合規管理

程式建置 掃描

映像倉庫 掃描

CIS 資安準則
& 客製化稽核

資安合規
PCI, GDPR, NIST

應用執行時掃描
容器, 主機, 平台

應用執行時的保護

資安政策即代碼

資安自動化
行為學習

部署

精細管控

容器防火牆
整合深層封包分析/資料外洩防護的防護

容器工作負載資安
隔絕 程序 & 檔案系統

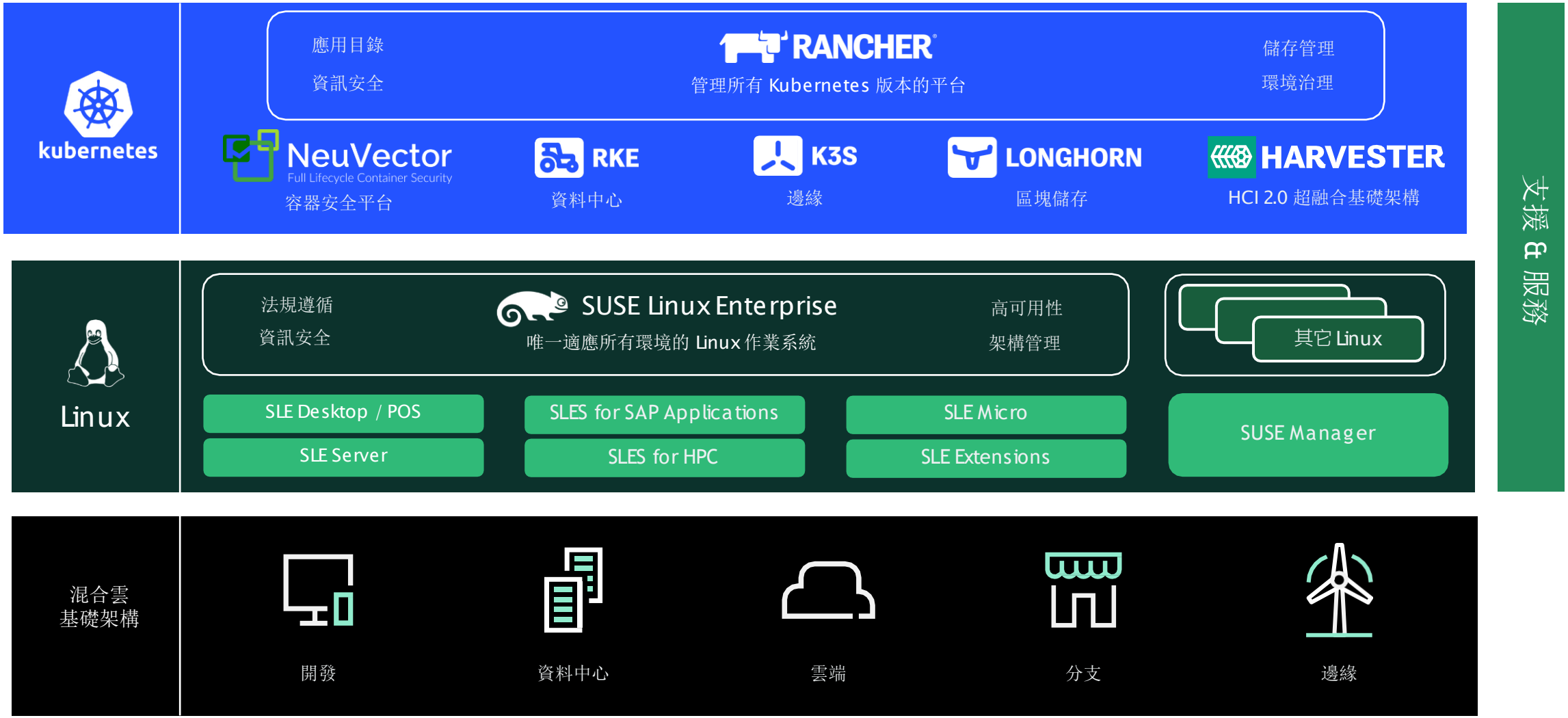
警示 & 鑑識

SUSE **成立於** 1992, **德國紐倫堡**

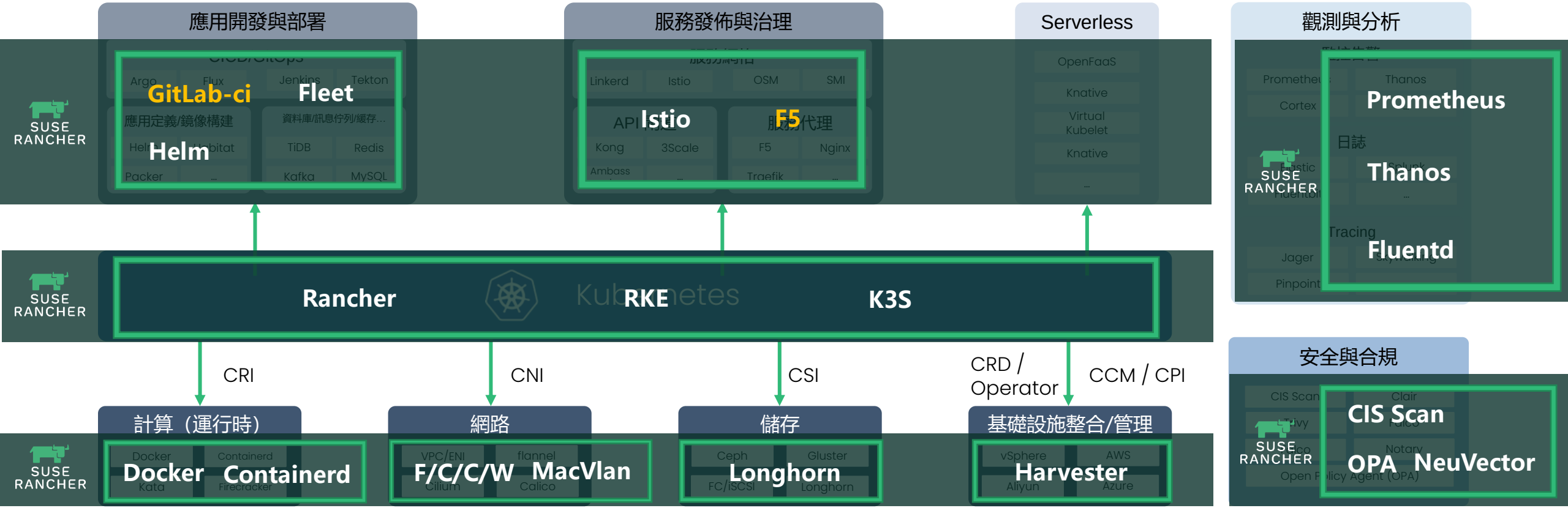
容器領域的創新者與領導者

2014 to 2017	2018	2019	2020至今
以Docker為核心	針對 Kubernetes 多雲管理	將 Kubernetes 擴展到邊緣	持續創新
• RancherOS 容器作業系統 • Longhorn 雲原生存儲 • Rancher 1.x 容器管理平台（業界唯一同時支援 Swarm / Kubernetes / Mesos 等多種編排引擎的統一管理平台）	• Rancher 2.0 容器管理平台（業界首創統一管理私有化叢集、公有雲託管容器服務及協力廠商 Kubernetes 叢集）	• K3s 羽量級 Kubernetes 引擎（業界首個針對開發環境、分支機構及邊緣場景的 Kubernetes 發行版本） • K3OS 針對邊緣場景內置 K3s 的羽量級作業系統 • Submariner 跨集群網路方案	• Harvester 是以 Kubernetes 為主的超融合平台 • Fleet 超大規模叢集管理 • Rancher Desktop
• Gartner 全球最酷雲基礎設施供應商 • OCI 開放容器委員會創始成員	• Forrester 企業容器平台領導者 • CNCF 雲原生基金會管理員委員會成員	• Gartner 技術成熟度報告代表廠商 • CDF 持續交付基金會創始成員 • Longhorn 成為 CNCF 社區開源項目	• Forrester 多雲容器平台領導者 • CNCF 雲原生基金會技術監督委員會成員 • K3s 成為 CNCF 社區開源項目

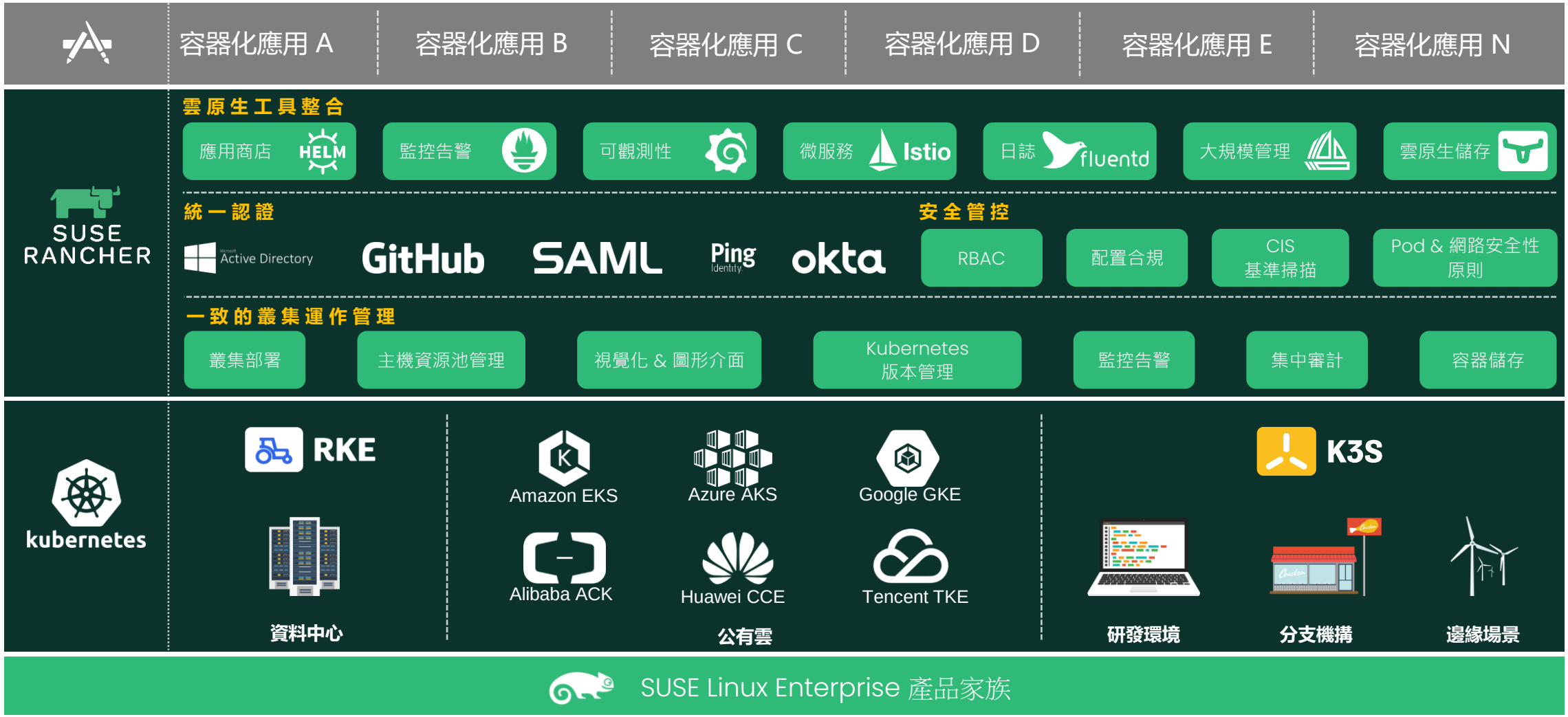
SUSE 提供開源軟體企業級支援



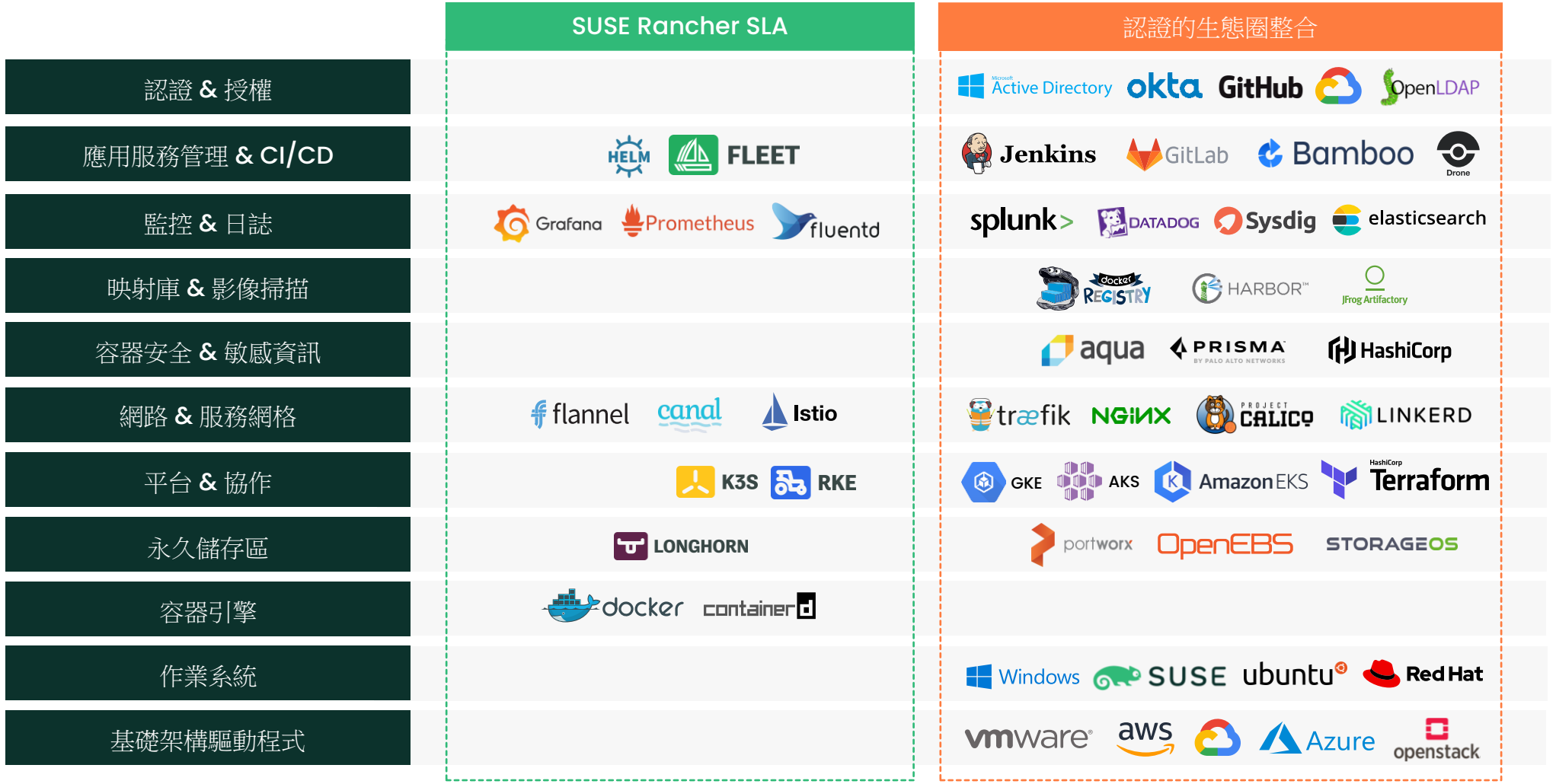
雲原生核心發展



Rancher 幫助用戶實現 Kubernetes 無處不在



SUSE Rancher 所支援的生態圈



SUSE 在開源的創新

完整專案列表可在此找到 **suse-projects.github.io**

KUBERNETES

RANCHER DESKTOP

Kubernetes 在你的筆電

HARVESTER

Open source hyperconverged infrastructure (HCI) software.

KUBEWARDEN

Kubernetes admission control using WebAssembly (WASM).

HYPPER

A dependency-aware package manager built on Helm.

EPINIO

An opinionated platform that runs on Kubernetes and takes you from code to URL in one step

OPNI

AI/ML-driven anomaly detection for Kubernetes.

LINUX

SLE BCI

Flexible developer environment tailored for modern containerized application development, CI/CD application containerization.

trento

A cloud-native web console aiming to improve the workday of SAP Applications admins

Aquarium

Easy to deploy, Ceph-based storage appliance. Its UX is centered around "declarative goals" – e.g. "Give me a 100 TB CephFS share, able to tolerate 2 device failures, optimized for density."

選擇 SUSE 解決方案所帶來的優勢

價格合理

高效能

提供
在地技術支援
& 教育訓練

Thank you

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

+49 (0)911-740 53-0 (Worldwide)

Maxfeldstrasse 5

90409 Nuremberg

www.suse.com