可觀測性 (Observability) 在 Kubernetes Day2 Operation的考量與實踐

E.W. Kuo @ iThome Kubernetes Summit 2022

二哥

- 緯創資通員工
- 社群的參與者
- 技術的佈道師
- 台灣資料工程協會會員
- Kafka 修煉之道講師

Techlearn
個人技術學習與收集

Wistron DX lab
緯創數位轉型技術實驗室

Agenda

Day2 Operation

Day2 運營

定義與說明

Challenge of Kubernetes Day 2 Operation

Kubernetes Day2

運營的挑戰

Tame operational complexity

馴服運營

複雜性

Observability

可觀測性

實踐與思維

Observability Demo

可觀測性

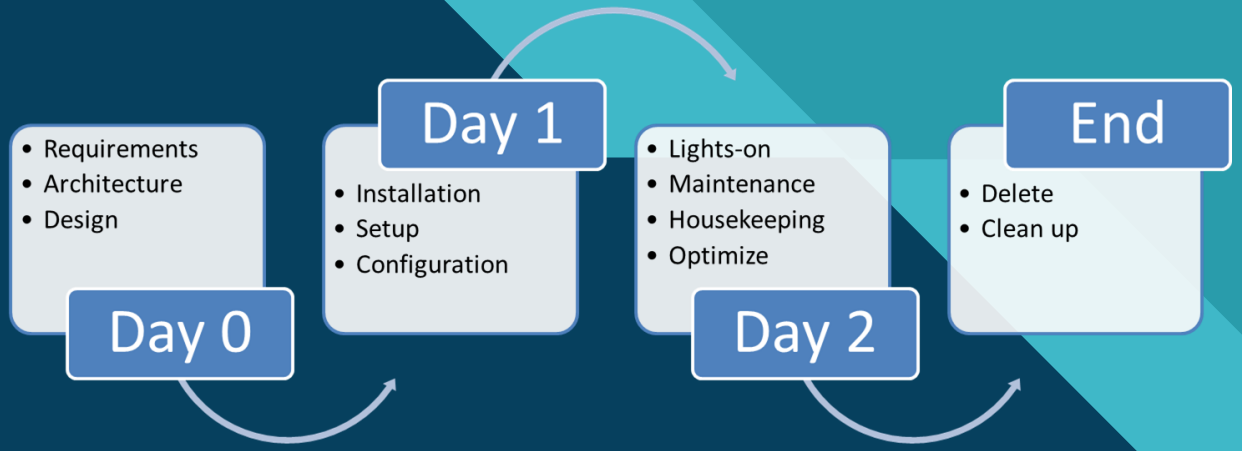
關聯演示

Day2 Operation

定義與說明

Day 2 Operation 的定義

- 一旦“**某物**”投入運營，Day 2 Operation 就是直到該“**某物**”被移除或被取代前所需要照料它的時間段。
- Day 2 Operation 是系統為組織生成結果與價值的地方。
- 組織需要在 Day 2 Operation 中不斷尋求改進，以最大限度地提高收益。

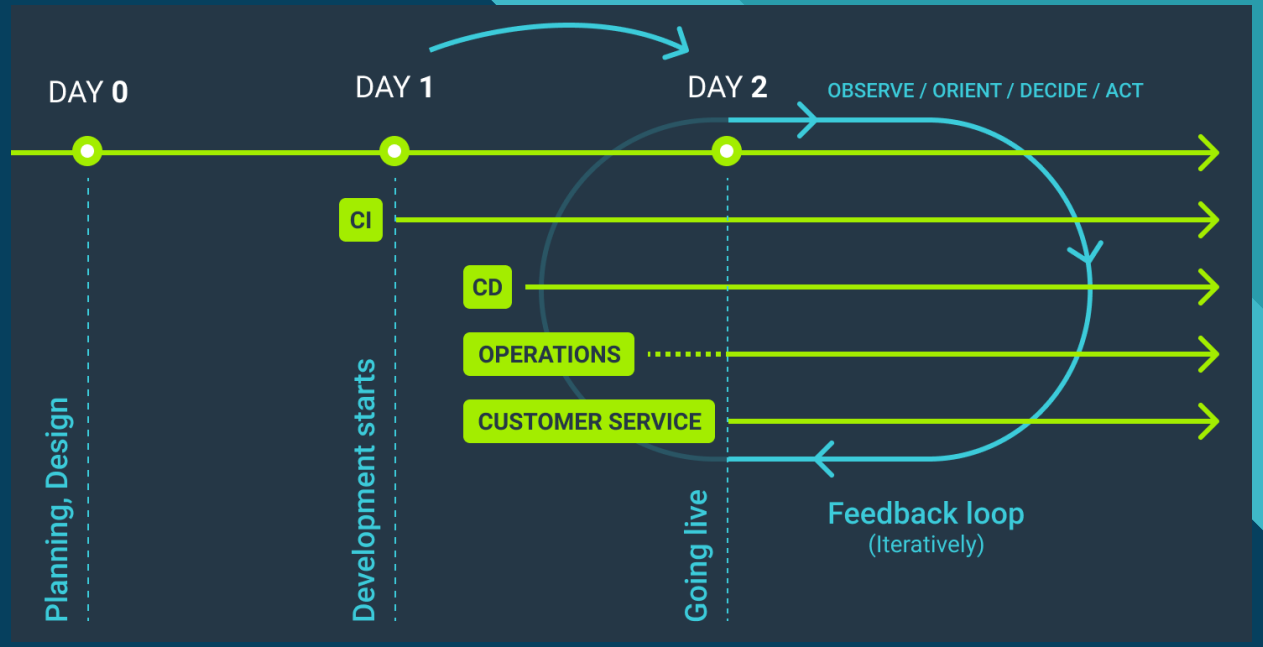


什麼是 Kubernetes Day 2

- 當組織遷移到 Kubernetes 時，最明顯、最緊迫的挑戰與 Day 0 和 Day 1 有關
- 推動 Kubernetes 的動力通常是：
  - 提高**開發人員**的**敏捷性**
  - 提高**開發人員**的**開發速度**
  - 通過讓**開發人員**訪問**自助服務**配置來**消除開發過程中的摩擦**

什麼是 Kubernetes Day 2

- 速度和敏捷性的顯著提高，從每月部署轉變為每日部署。
- 但是應用程序的生命週期不會在部署時結束。任何應用程序最長的生命週期階段是需要對其進行監控、升級和保護的生產階段。
- Kubernetes Day 2 Operation 對於 Kubernetes 的持續成功至關重要，但在急於部署時可能會被忽略。

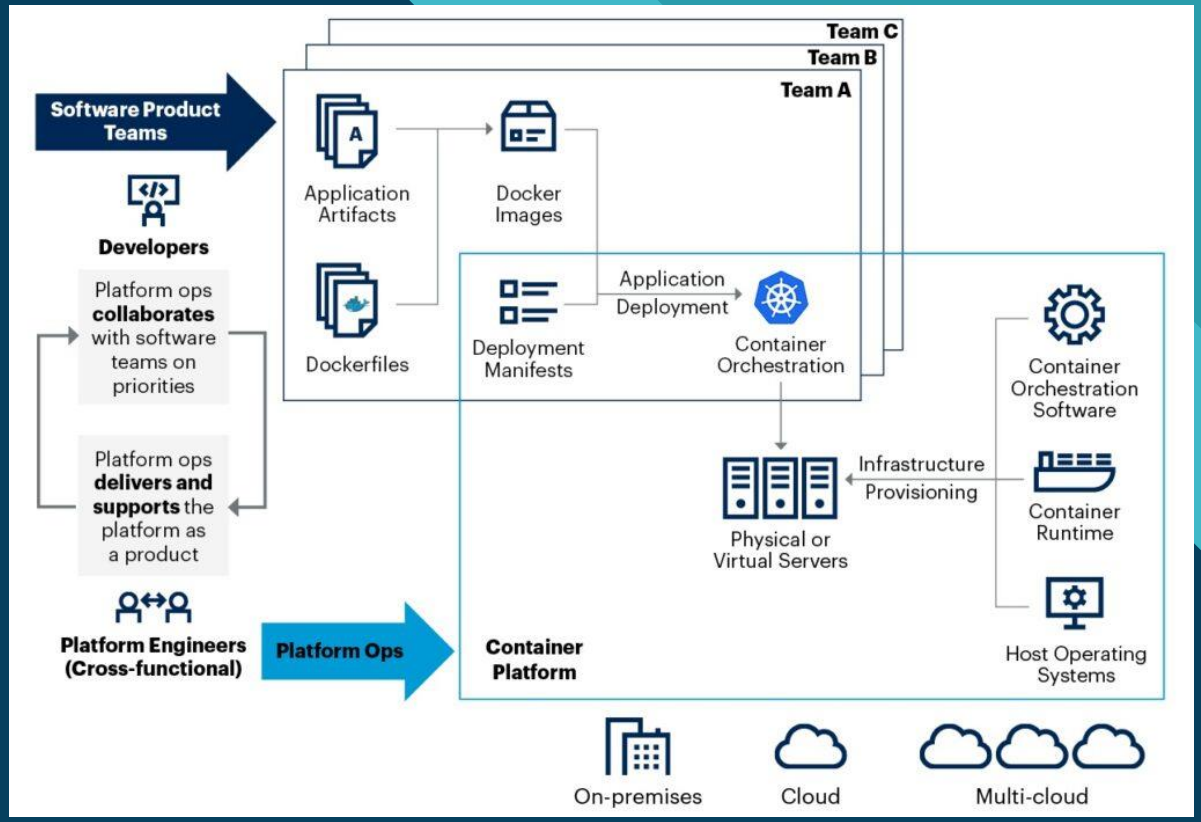


Challenge of Kubernetes Day 2 Operation

運營Kubernetes的挑戰

Kubernetes Day2 Ops 要作那些事?

- 集群標準化和生命週期管理
- 安全訪問和環境隔離
- 維運可觀察性和流程透通性
- 治理與合規
- 持續第三方元件整合和維護



Ref. Use Platform Engineering to Implement DevOps Workflows with Kubernetes (Gartner)

Kubernetes Day2 Ops 的挑戰排行

遷移到 / 使用 Kubernetes 時，面臨的最大挑戰是什麼？

- **In-house skills / manpower**
- Company culture
- Tooling
- Security & Compliance

1240 out of 1279 people answered this question (with multiple choice)

48.0%	Lack of in-house skills/limited manpower	595 responses
37.7%	Company IT structure	468 responses
31.9%	Incompatibility with legacy systems	396 responses
29.3%	Difficulty training users	363 responses
24.8%	Security and compliance concerns not addressed adequately	307 responses
21.6%	Integrating cloud-native applications together	268 responses
16.8%	Poor or limited support from platform providers or partners	208 responses
16.5%	Networking requirements not addressed adequately	205 responses
16.4%	Cost overruns	203 responses
15.6%	Storage/Data requirements not addressed adequately	194 responses
14.9%	Observability / monitoring requirements not addressed	185 responses
13.4%	Inefficient day to day operations	166 responses
11.0%	Cloud platforms don't meet needs/expectations	137 responses
10.7%	Lack of flexibility when it comes to address workload	133 responses
0.6%	Other	7 responses

Canonical (Ubuntu) – K8S Operation Survey @2021/Nov, 1300 受訪者

Tame operational complexity

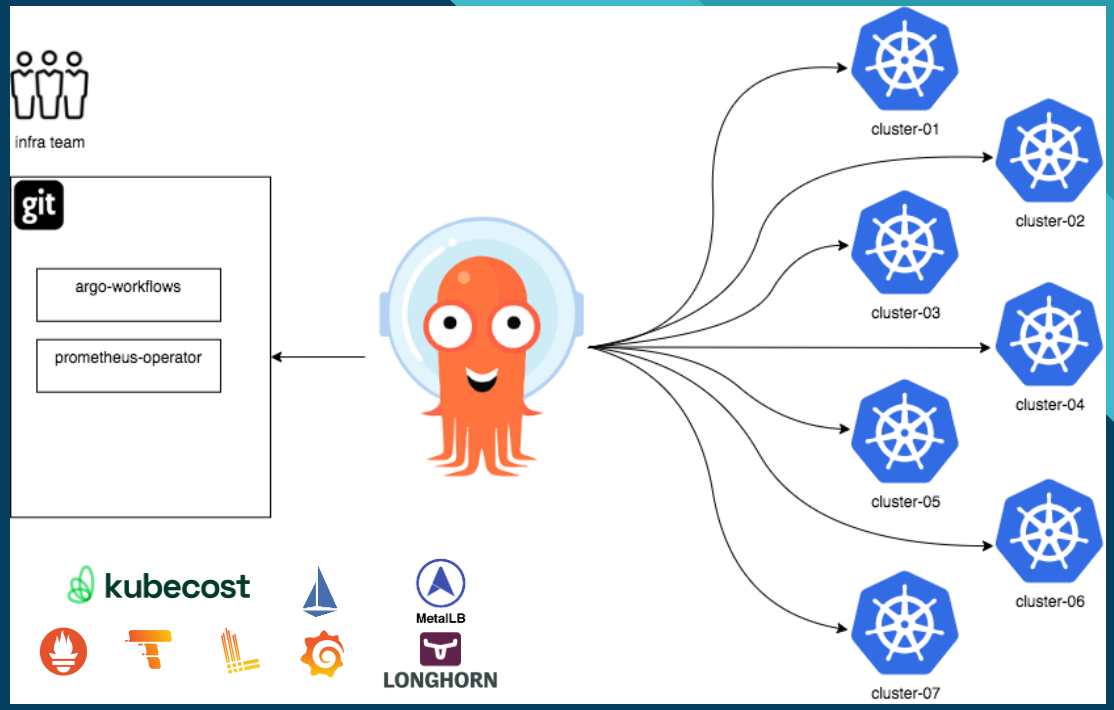
馴服運營的複雜性

馴服 Kubernetes Day2 Ops 複雜性

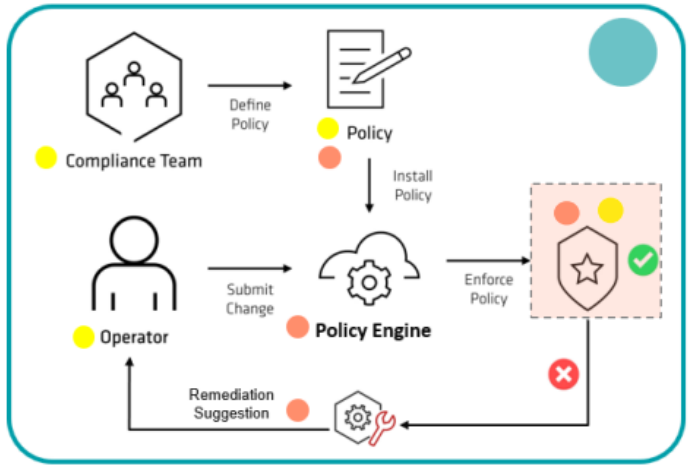
- **A single pane of glass platform**
  - 運營團隊需要能夠通過一個統一的儀表板在一個地方可視化整個系統。
- **Complete separation of concerns**
  - 應用程序開發人員應該能夠盡可能地自助服務，依靠一小群平台工程師來管理底層操作系統。
- **Centralized policy controls**
  - 運營團隊需要一種集中控制集群和工作負載策略的方法，以確保根據組織圍繞安全性、合規性和其他最佳實踐的策略配置 Kubernetes 和容器。
- **Kubernetes-native monitoring and logging for security and availability**
  - 中央管理面板必須包含強大的雲原生環境監控功能
- **Resource utilization tools**
  - Kubernetes Day2 管理運營必須包括幫助公司了解其成本、優化資源利用率並最終降低總體成本的工具。

GitOps 痛苦x甜密

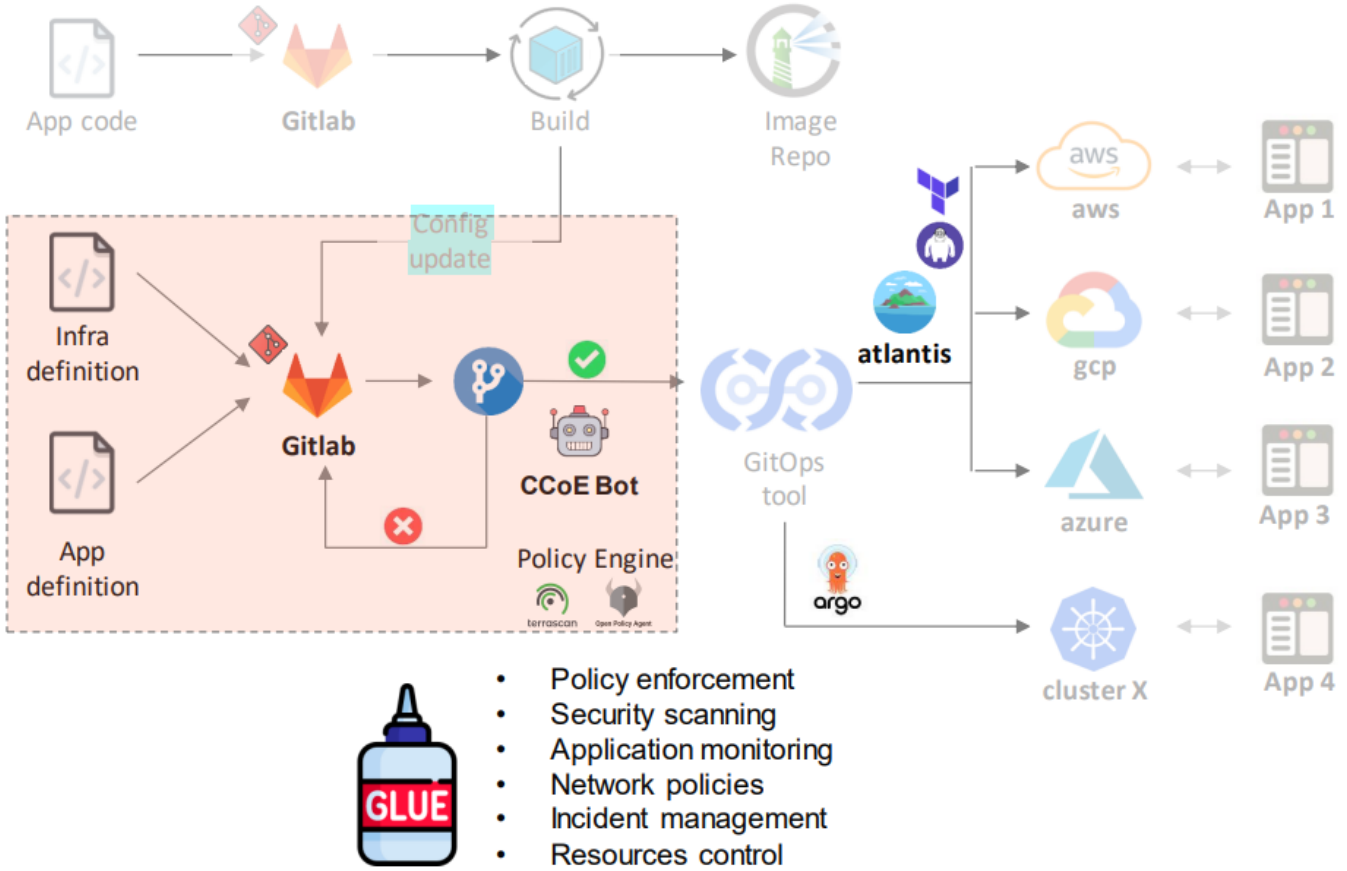
- 有能力記錄叢集環境上的一切變化
- 使用宣告式(Declarative)的文件格式來描述或是設定環境上要用到的所有資源
- 所有的環境變化都可支援審核機制，要通過審核才會往下運作
- 權限控管，控制誰有能力去對環境資源進行更改
- 有辦法針對期望的狀態與運行的狀態進行比對



GitOps 與資安合規守門員一拍即合



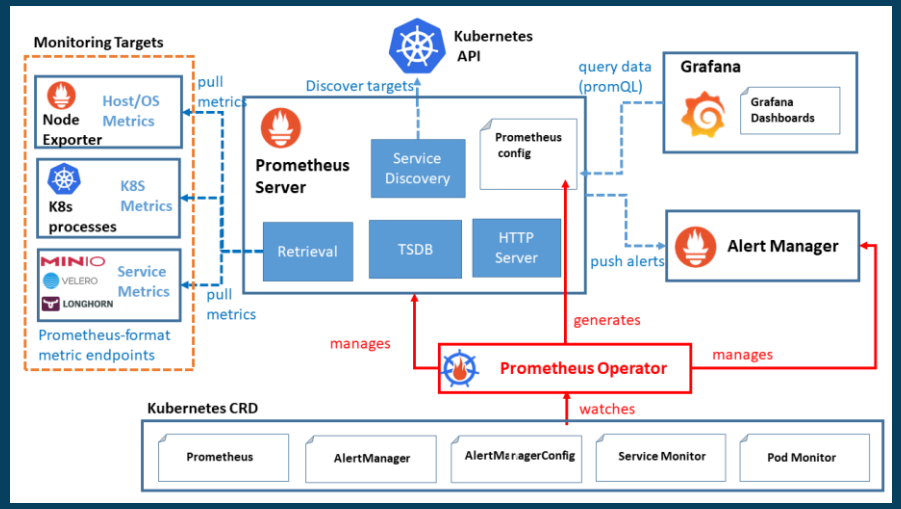
系統架構與整合



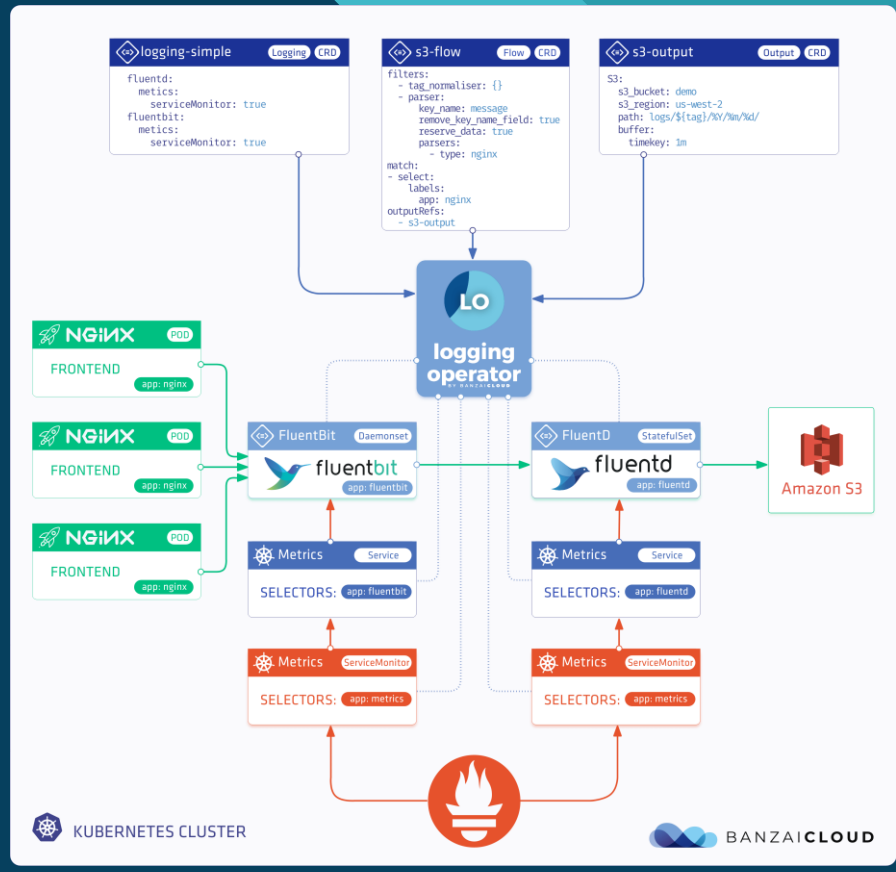
- Policy enforcement
- Security scanning
- Application monitoring
- Network policies
- Incident management
- Resources control

GitOps 的好朋友 - xxxOperator

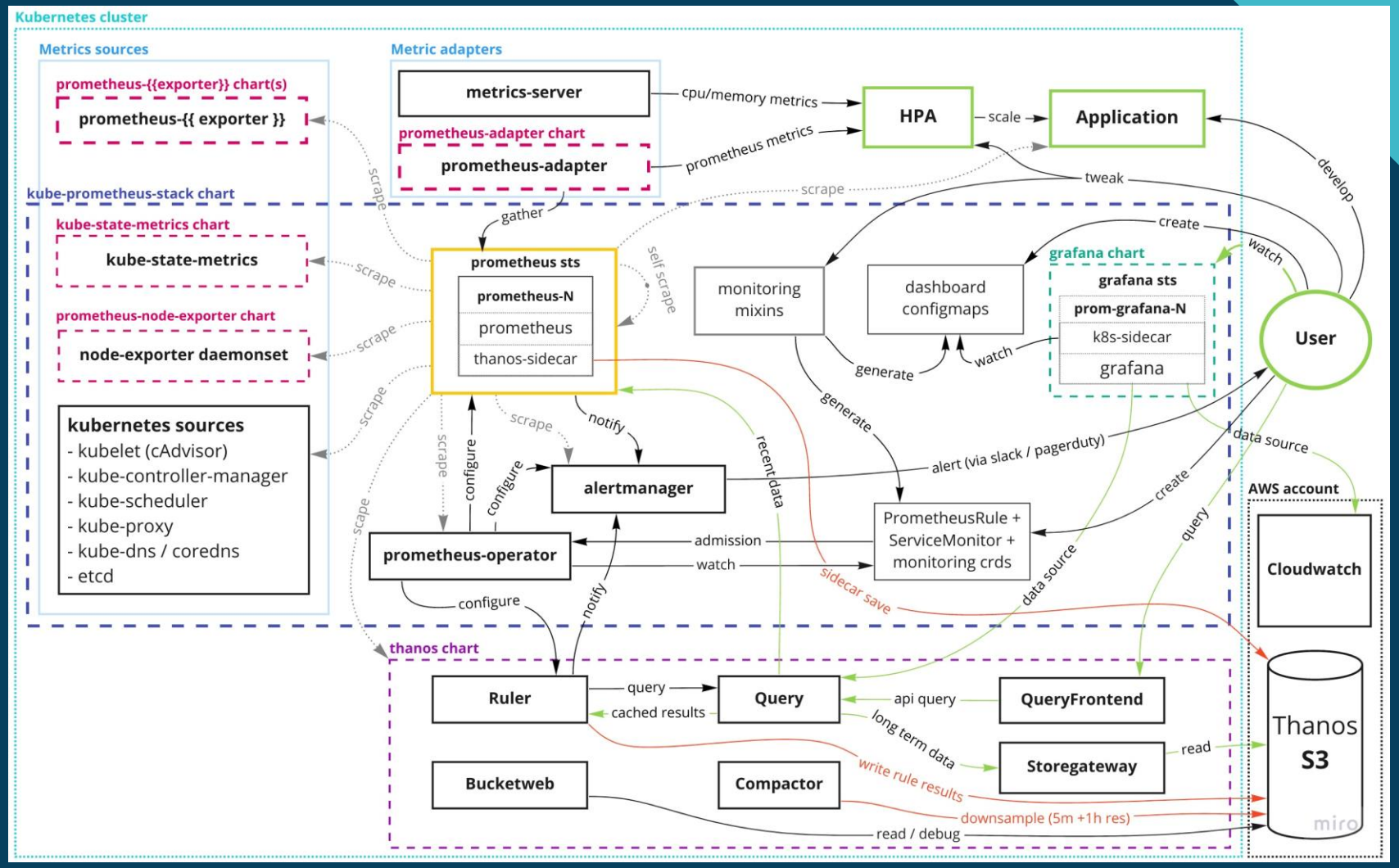
- Operator 的目標是將 operation 知識放入軟件中
- Operator 運行在 Kubernetes 集群內並根據宣告式 (Declarative) 的 CRD 文件來自動化常見的 Day 1和 Day2 的活動。

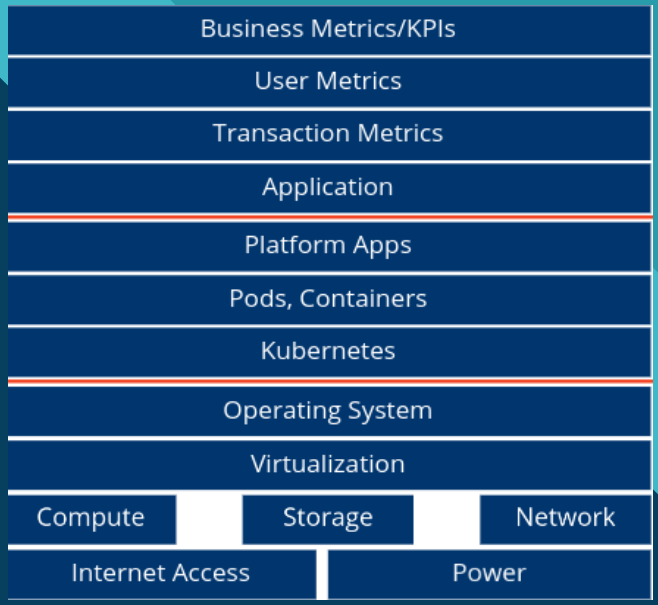


OPERATOR FRAMEWORK



Kube-Prometheus-stack 一站式可觀測性百寶箱



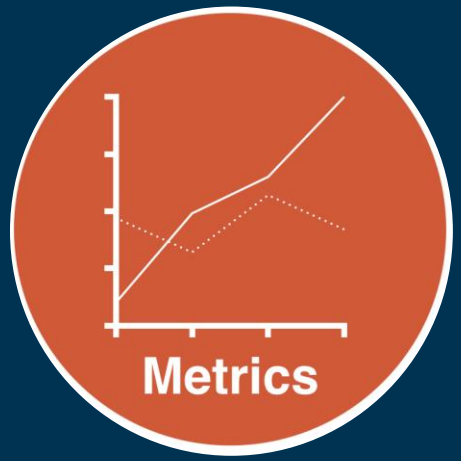


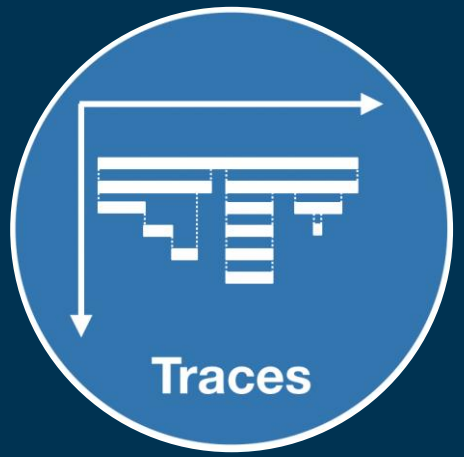
Ref. https://clux.dev/post/2022-01-11-prometheus-ecosystem/

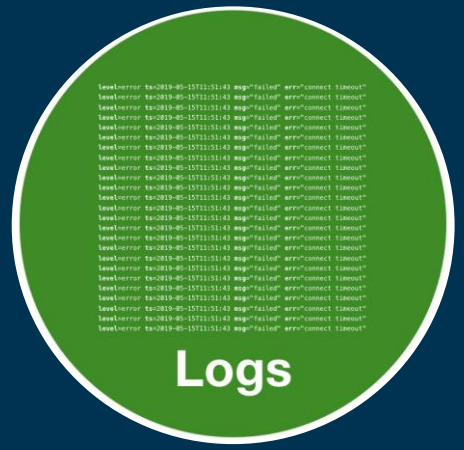
Observability

可觀測性的實踐與思維

可觀性三大支柱







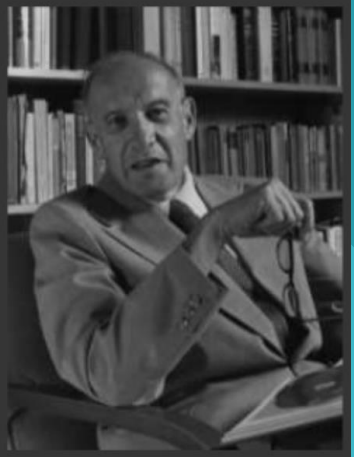
用**數據**來了解你的系統狀況！

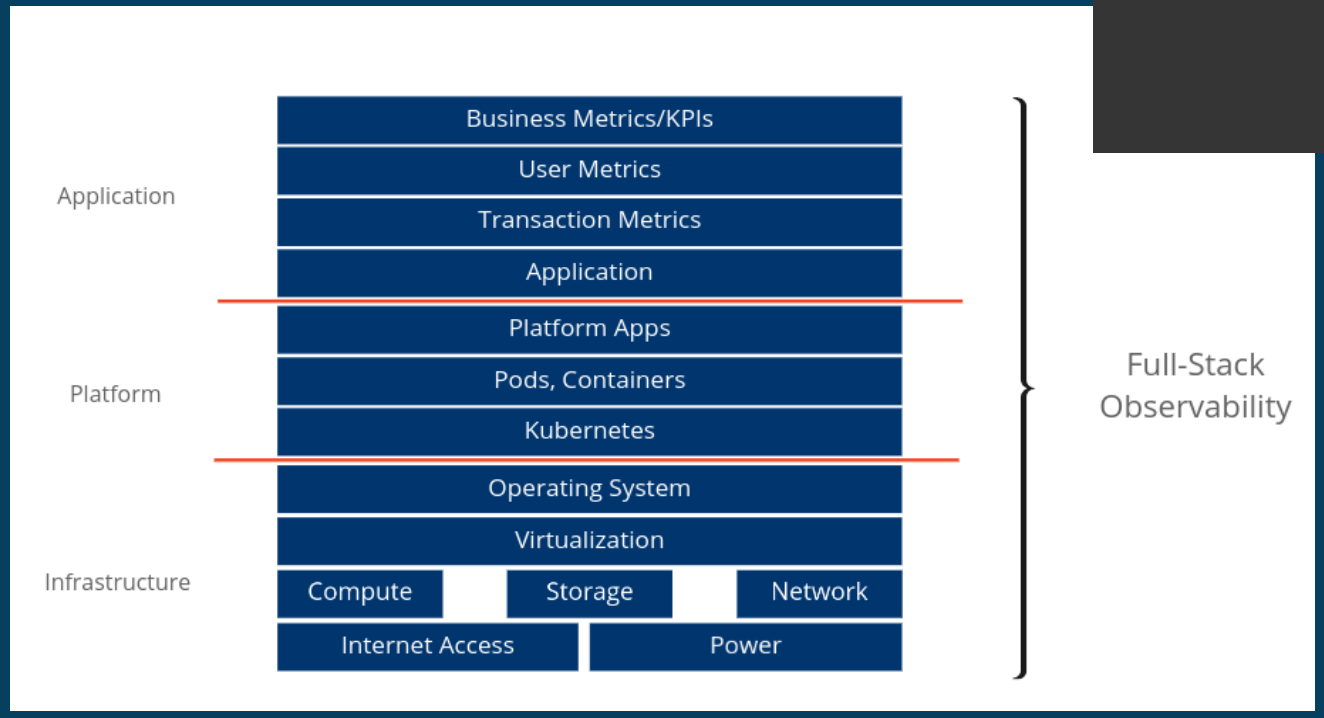
儀器化一切並收集遙測數據

« If you can't measure it, you can't improve it »

-Peter Drucker

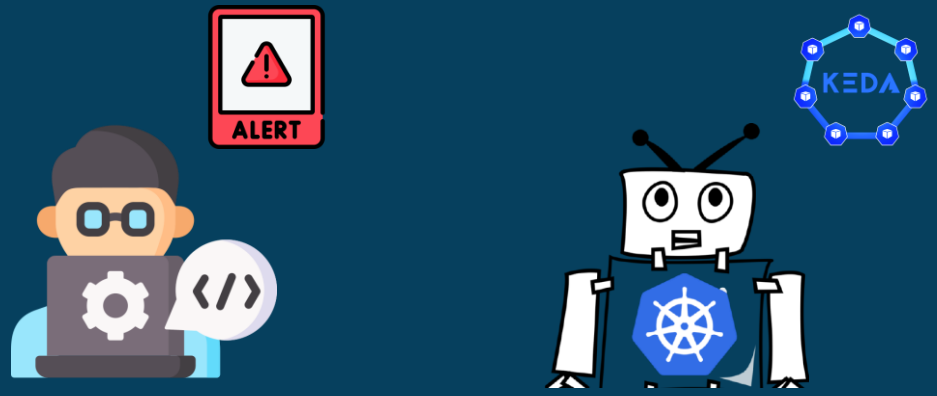
Management Guru

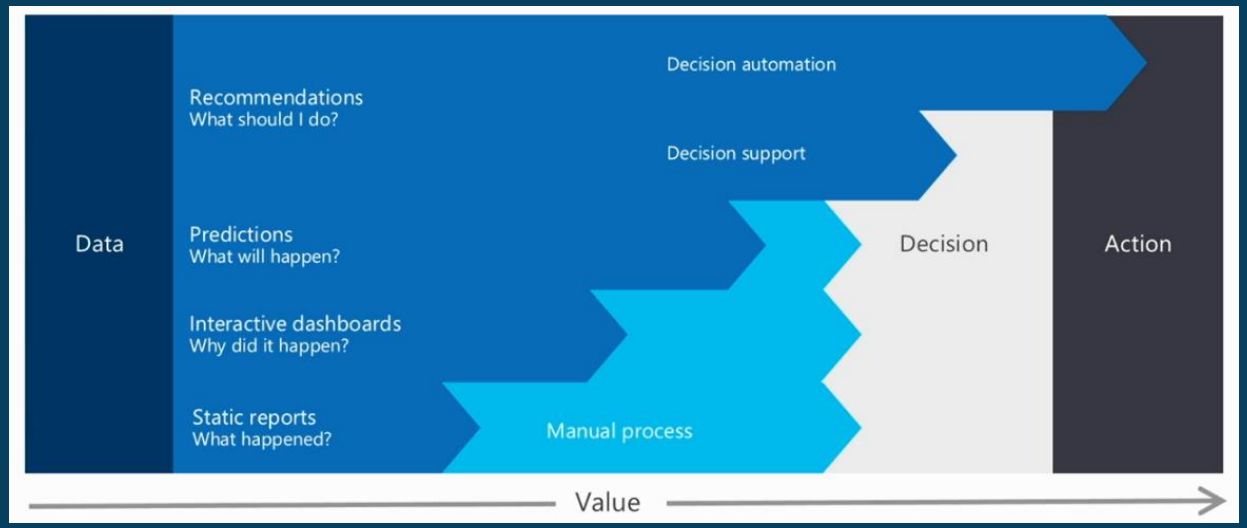


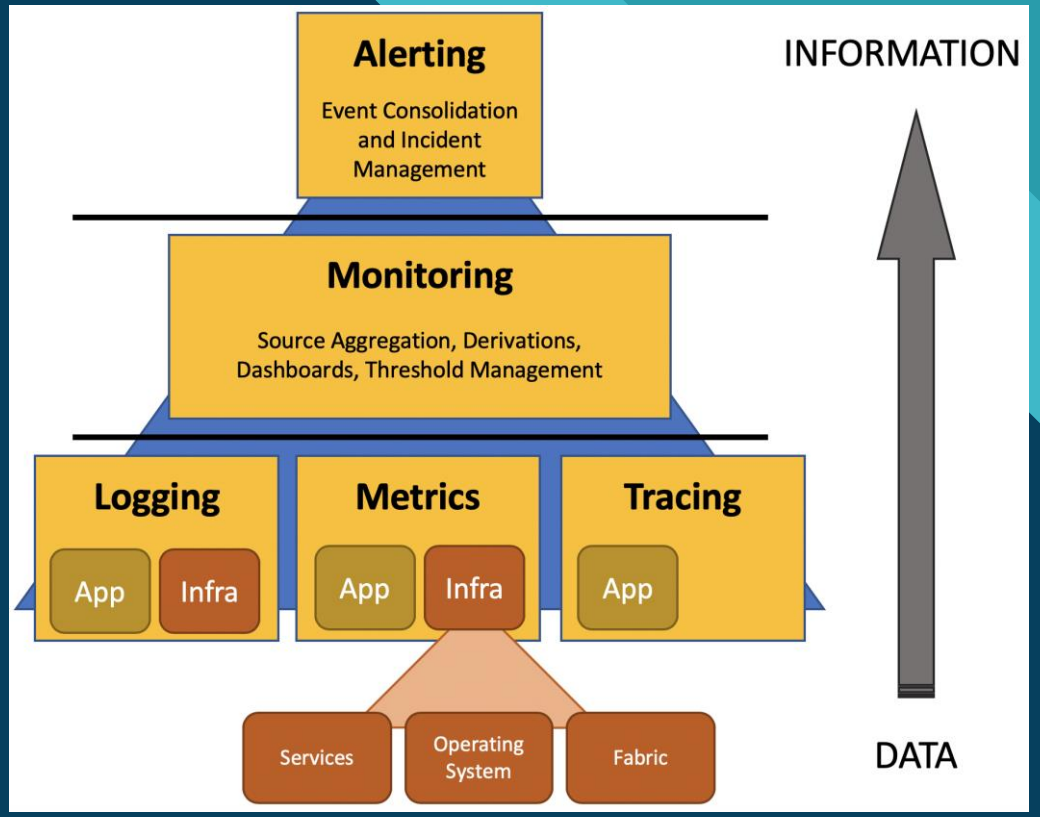


OpenTelemetry

如何將遙測數據轉化為 Actionable 的見解





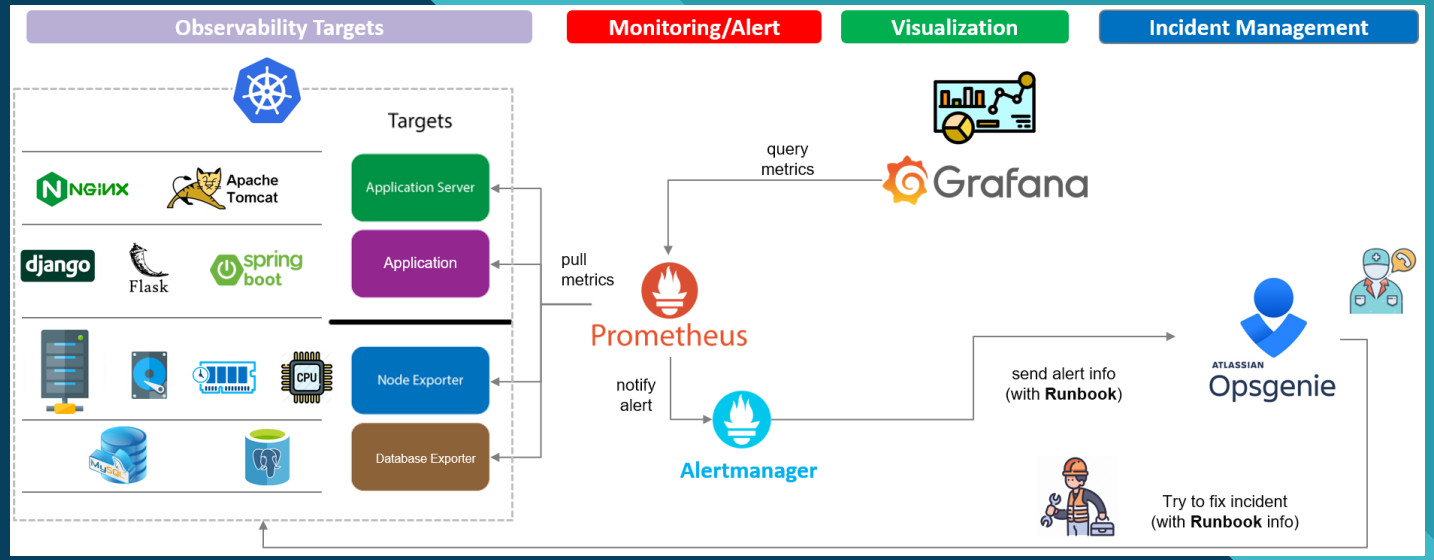


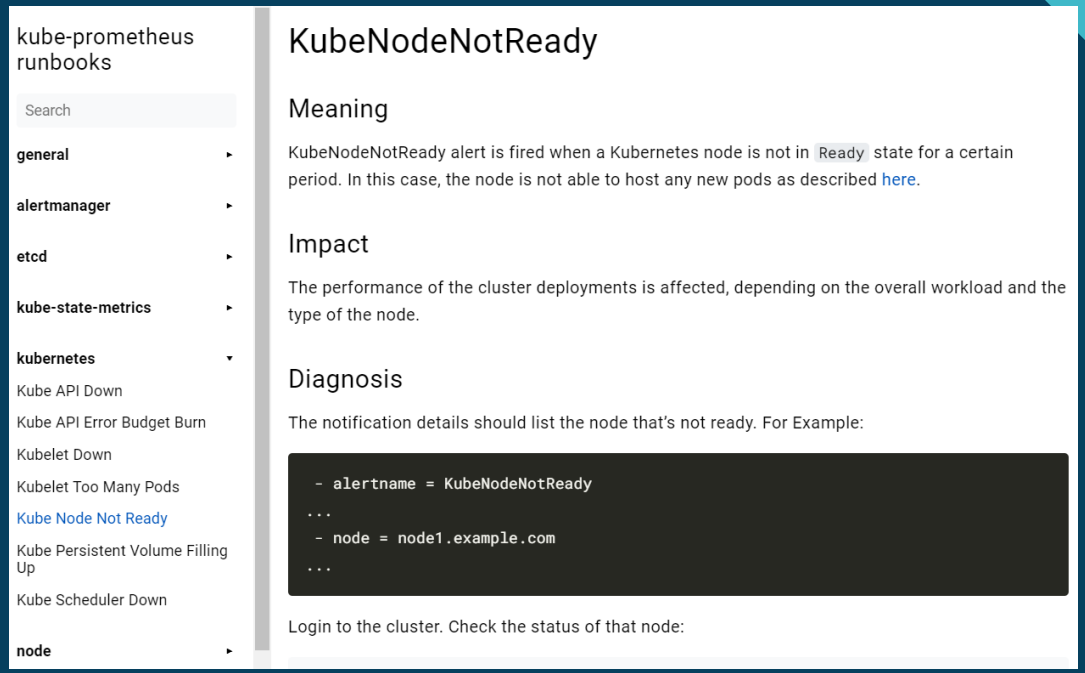
什麼是 Runbook?

- Runbook 是詳細的“how-to”指南，用於完成運營流程中經常重複的任務或程序。
- 創建 Runbook 的目的是為團隊中的每個人（無論是新人還是經驗豐富的人）提供快速準確地解決特定問題的知識和步驟。

每一個 alert 都應該要有一個 runbook！

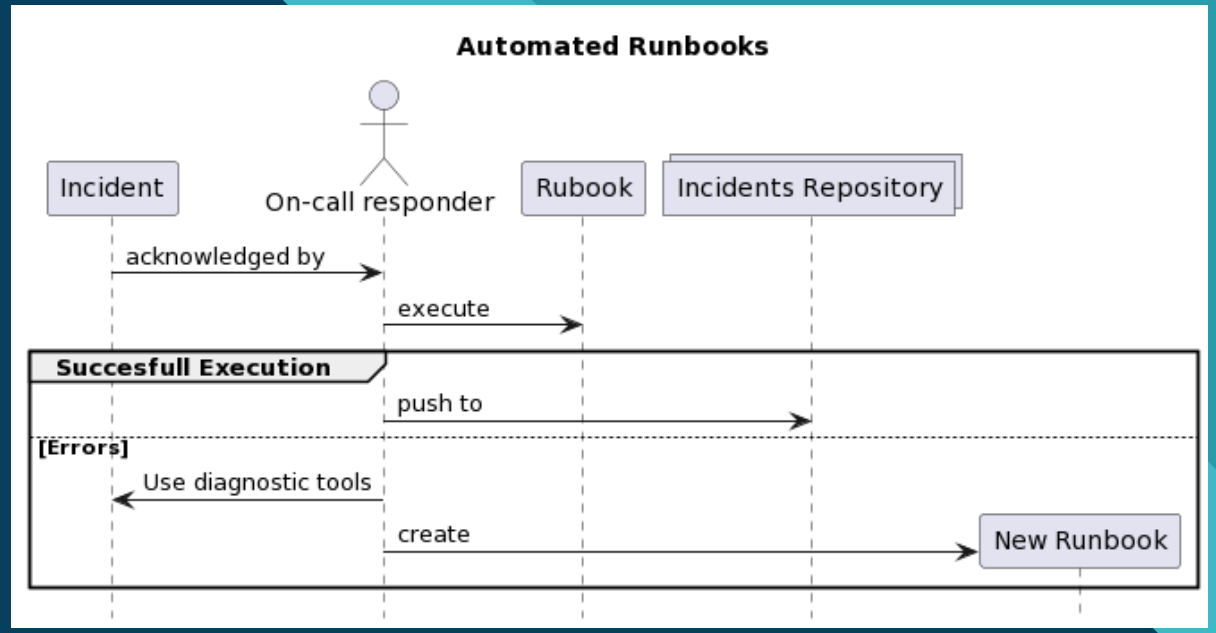
Ref. https://runbooks.prometheus-operator.dev/





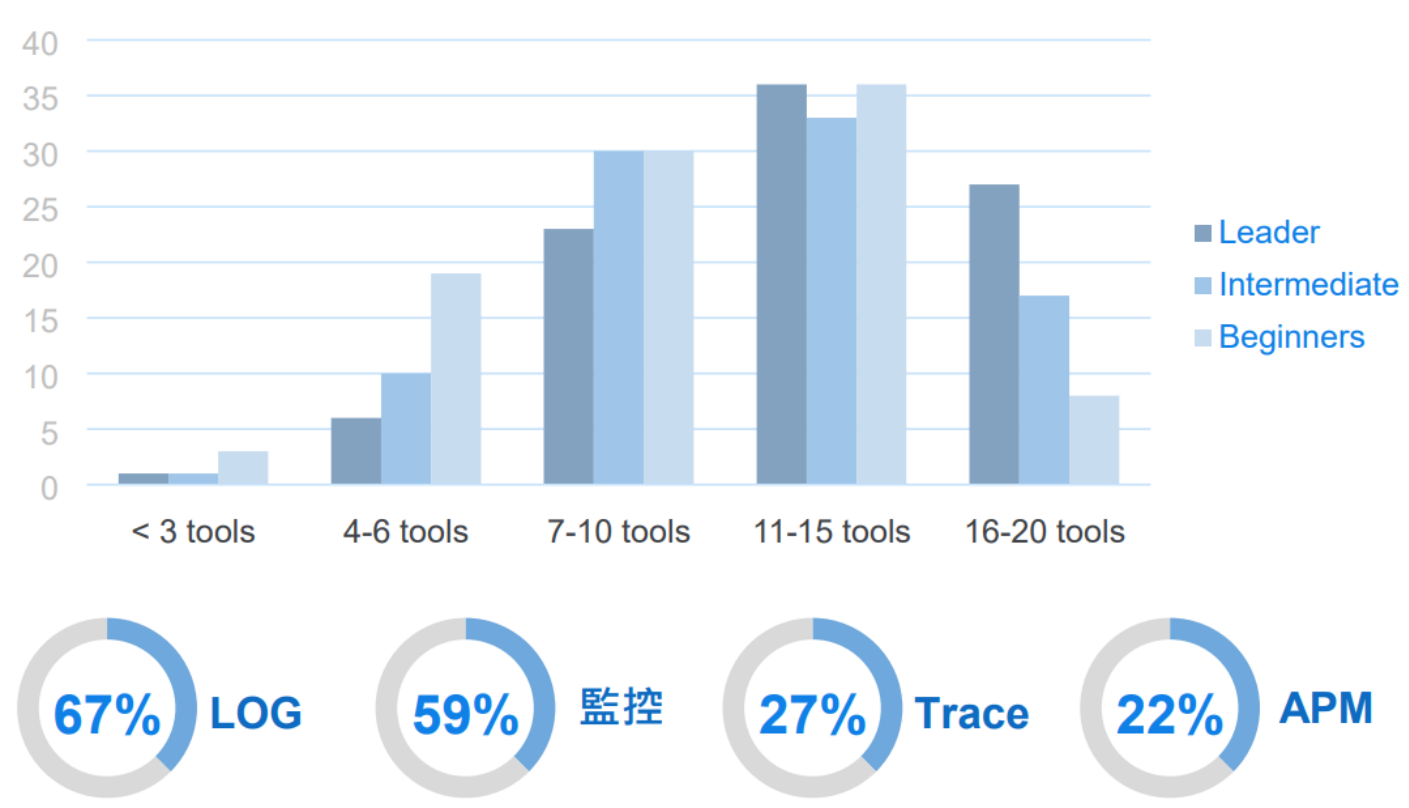
不同類型的 Runbook

- 手動
  - Step-by-step instructions followed by the operator
- 半自動
  - A combination of operator-followed steps with automated steps
- 全自動
  - All steps are automated and require no operator



如何有效查找根因的挑戰

- 工具未整合：10+ observability tools.



Ref. 可觀測性(Observability)的實踐 – Marcus @ DevOps Days Taipei 2022

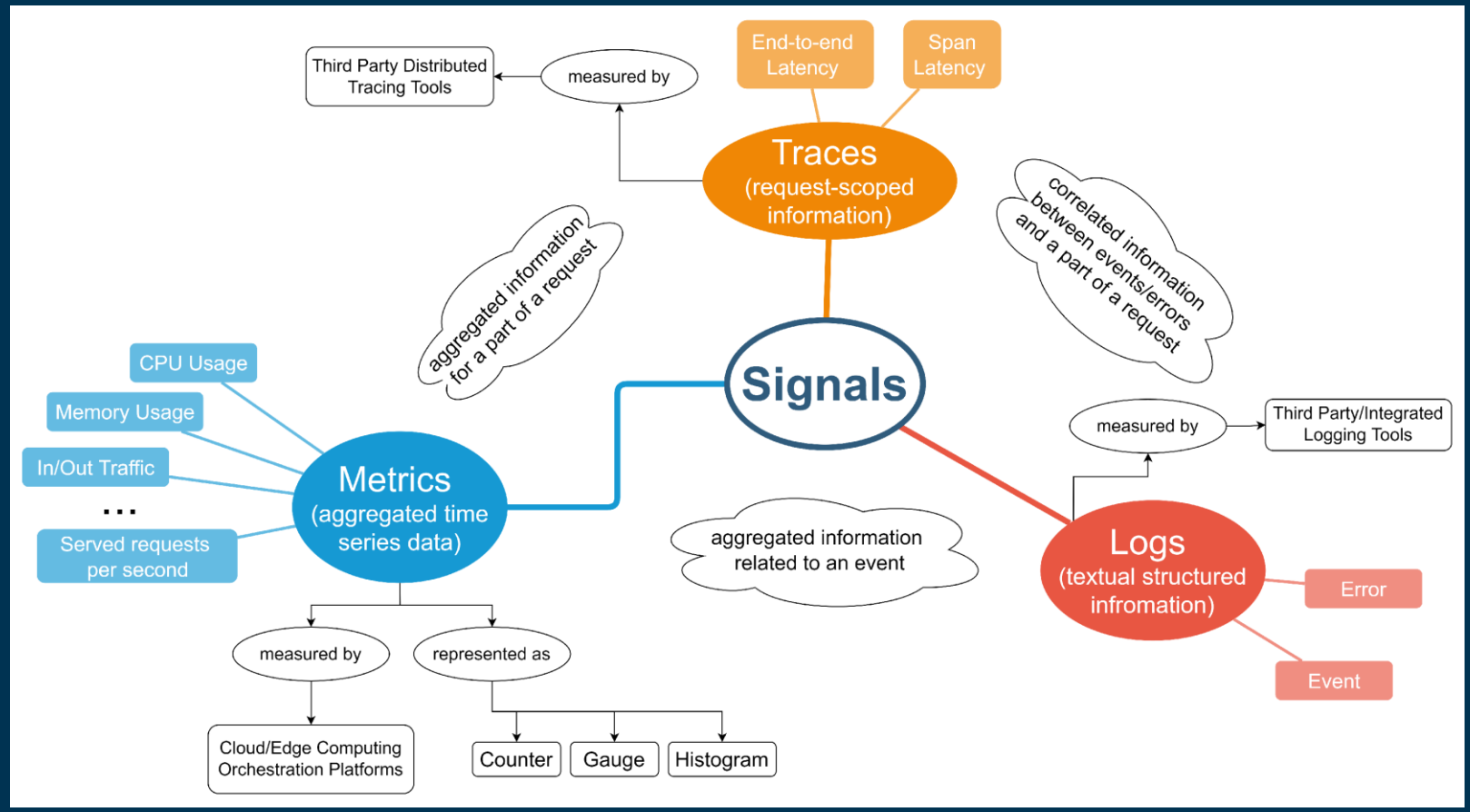
可組合的可觀察性平台

Metrics

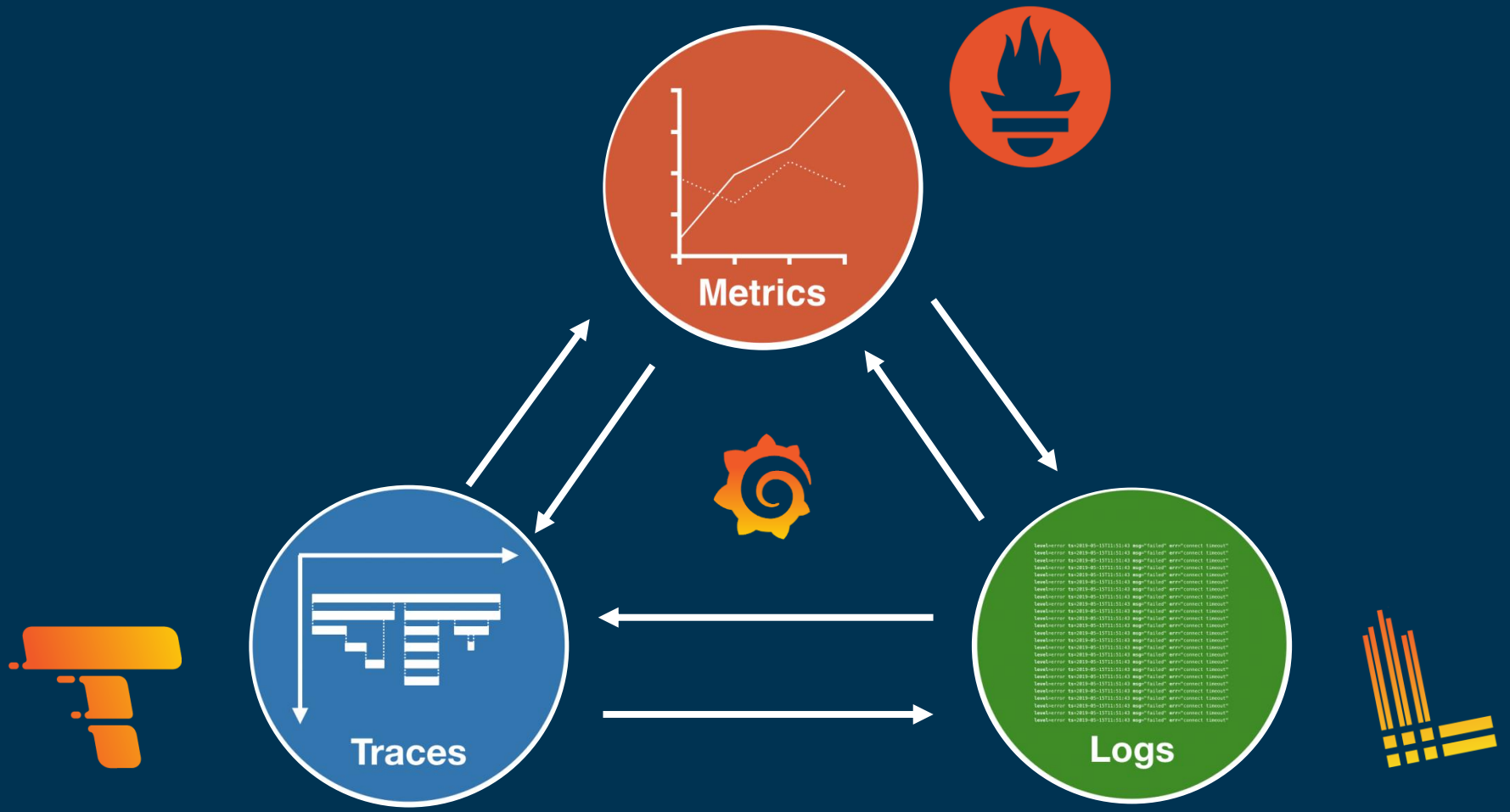
Logs

Traces

串連與關聯 (Correlated) 遙測數據



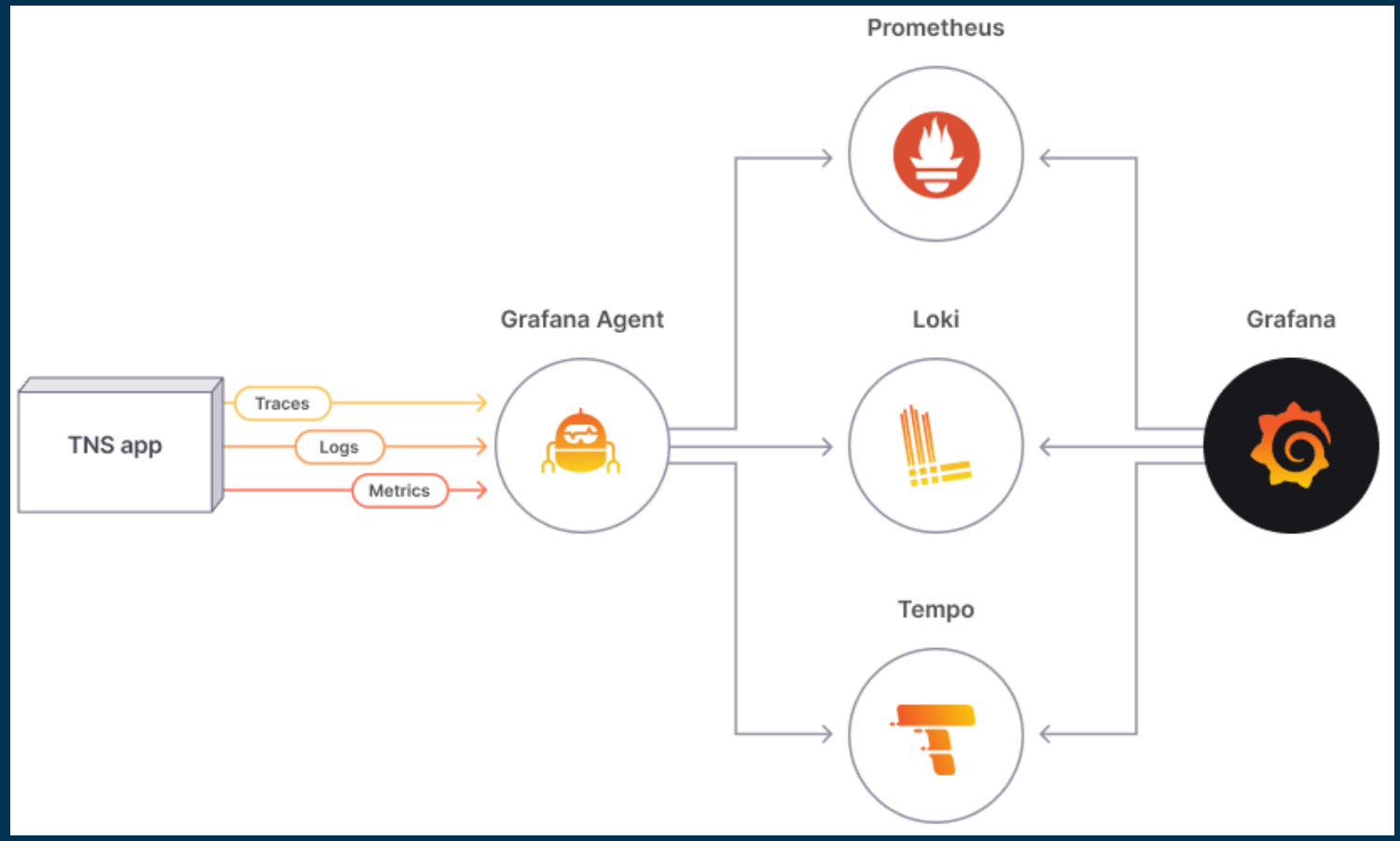
串連與關聯 (Correlated) 遙測數據



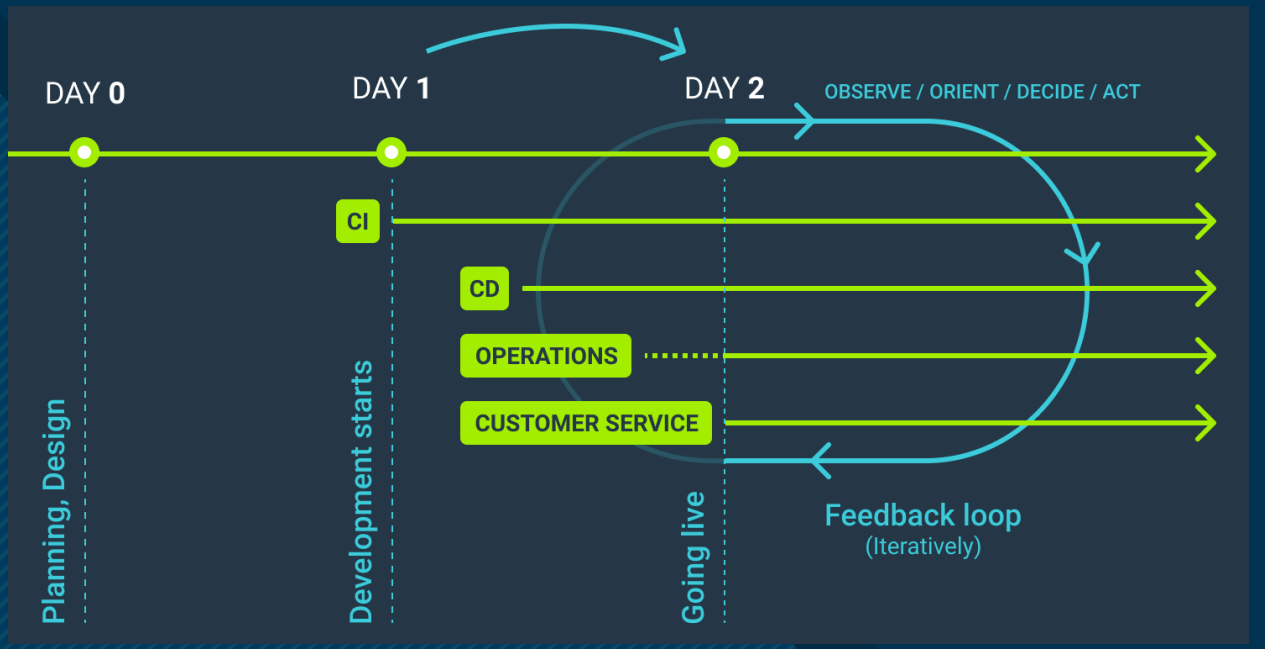
Observability Demo

可觀測性關聯演示

範例架構



Ref. https://github.com/grafana/tns



開始考慮 Day2 Operation 永遠不會太早。組織在設計和實施階段做出的選擇在 Day2 會產生巨大的影響。

監控工具和集中控制應在部署應用程序之前就該就位，而且為應用程序開發人員建立正確的流程可以減少開發摩擦同時還可以簡化未來的營運。

謝謝聆聽!!