實戰指南

平台工程師的雲原生實戰指南

了解 Nutanix 如何協助平台團隊簡化基礎架構管理、加速應用程式交付，以及擴展 Kubernetes 環境



NUTANIX

目錄

第 1 章： 從自行建置邁向 IDP 模式 03
第 2 章： 大規模叢集機群管理 05
第 3 章： 在邊緣環境運行 Kubernetes 06
第 4 章： 安全性與合規性 07
第 5 章： 資料保護與管理 08
第 6 章： 實體隔離環境部署 09
第 7 章： 混合雲 Kubernetes 10
第 8 章： 加速開發人員交付效率 11

第 1 章
從自行建置邁向 IDP 模式

Kubernetes® 容器管理只是建立企業級雲原生平台的其中一環。隨著平台工程的演進，團隊正在重新思考如何打造兼具可擴展性、安全性，且開發人員友善的環境，同時評估自行建置是否仍是合適的路徑。

平台工程師為何紛紛擺脫自行建置 Kubernetes 的模式？

Kubernetes 是現代基礎架構的基石，但它本身並不足夠。生產就緒的平台也需要網路、儲存、可觀測性和安全性等能力。它還需要處理安全性、基於角色的存取控制 (RBAC)，以及 GitOps、政策管理和服務網格等其他功能。許多團隊一開始會採用自行建置的平台，針對這些需求拼接開放原始碼工具。一開始是可行的，但隨著叢集的增加，整合的挑戰也隨之增加。

平台工程師很快就會發現他們不只需要管理基礎架構，還需要管理開發人員體驗：佈建叢集、執行政策、疑難排解管道，以及不斷處理組態偏移。這種負擔會降低速度並增加風險。

許多團隊不想建立平台 - 而是想使用平台。這就是轉向內部開發人員平台 (IDP) 的原因：將複雜性抽象化，為開發人員提供通往生產的黃金之路。透過選擇平台方式，團隊可以將工作重心轉移到高影響力的貢獻上，例如促成對 AI 模型的存取、改善資料管道，以及加速創新。這反映出平台工程的演進，從提供基礎架構到提升開發人員的速度，以及驅動業務影響力。

常見挑戰

- **平衡速度與穩定性：**開發人員需要快速存取環境，而作業團隊必須保護正常運作時間和管理。
- **分散式系統的故障排除：**故障和日誌的數量在節點和叢集之間成倍增加，統一的可視性有限。
- **一致的安全性與合規性：**政策執行必須跨環境擴充，而不是臨時應用。
- **CNCF 生態系統的複雜性：**隨著數百個專案的快速發展，為了持續維持各項整合的最新狀態，往往會導致環境日益複雜且分散，並加重團隊的維運負擔與疲憊感。
- **跨供應商擴充：**混合與多雲端部署需要一致性，單靠 vanilla Kubernetes 無法達成。

自行建置雖能提供靈活性，但隨著規模擴大，往往會造成技術堆疊日益分散，並增加團隊的認知負擔。

Nutanix 價值：生產就緒的 IDP

Nutanix Kubernetes Platform (NKP)解決方案以完整、開放的企業級平台取代自行建置的無序擴張，為雲原生應用程式提供韌性、安全防護，以及持續營運所需的管理能力。無論叢集在何處執行，都能以標準化方式統一管理大規模叢集機群。

關鍵能力：

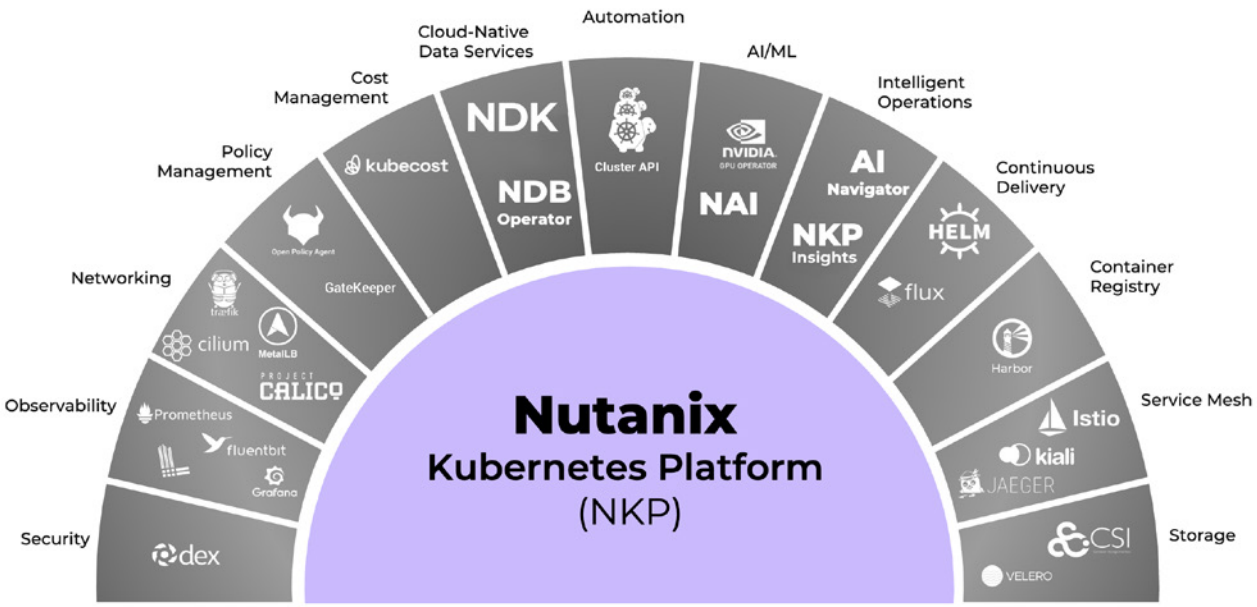
- **開放且完整：**全堆疊平台提供在生產中部署和運行容器化應用程式所需的所有元件，還可存取經過驗證的 CNCF 專案的完整目錄，讓你能夠整合符合需求的工具。
- **自動化部署：**在任何環境中自動化 Kubernetes 部署、擴充與升級。
- **統一的可觀察性：**利用整合式記錄、監控和警示功能快速排除故障。
- **可行的洞察力：**透過 NKP Insights 和 AI Navigator 獲得最佳化建議、疑難排解提示和最佳實作指導。透過提供即時指導、具根源分析功能的異常偵測，以及對話式疑難排解介面，為管理員帶來專家級支援，縮小技術差距。
- **無縫擴充：**使用 Kubernetes Cluster API 進行宣告式擴充與生命週期管理。
- **純正上游 Kubernetes：**不採用可能導致供應商綁定的專有 API。
- **跨環境的可攜性：**維持一致的作業，隨時隨地執行工作負載。

擺脫自行建置和維護客製化工具的複雜性。Nutanix 平台採用純正上游 Kubernetes，不使用額外封裝，也不會造成供應商綁定。你可直接導入最新的雲原生創新技術，並快速提供價值，讓你的團隊可以專注於創新，而非整合。

了解更多資訊：

The New Stack：要打造正式環境就緒的平台，光有 Kubernetes 還不夠

使用 NKP 在正式環境中執行 Kubernetes | Nutanix University



第 2 章
大規模叢集機群管理

隨著組織在團隊、站點和雲端間擴充 Kubernetes，叢集會成倍增加 - 每個叢集都有自己的生命週期、工作負載和政策。這種分散性會導致組態偏移、安全性不一致以及作業開銷增加，因此，採用一致的生命週期管理、工作負載配置、政策執行，以及可觀察性至關重要。

常見挑戰

- **叢集間的漂移：**由於變更的套用方式不一致，組態會出現偏差。
- **自動化缺口：**腳本和管道在規模擴大時失敗，導致叢集不同步。
- **頻寬和連線問題：**遠端和邊緣網站會中斷升級和政策鋪陳。
- **營運開銷：**手動升級、監控和修補功能會在不同環境中倍增。
- **混合基礎架構：**不同的供應商在 API、網路和安全控制方面各有不同。

Nutanix 的價值：實現全叢集機群一致性

Nutanix為 Kubernetes 叢集機群提供單一管理平面，實現叢集、供應商和環境的一致性。

關鍵能力：

- **一鍵式應用程式與組態部署：**無需手動步驟，即可將驗證的變更推出至每個叢集。
- **持續調節的 GitOps：**NKP 以 Flux CD 為基礎，即使在低連線性或邊緣環境中，也能確保配置的一致性。
- **不可變更的基礎架構：**NKP 中的 Cluster API 不會變更即時基礎架構，而是會取代資源以強制執行所需狀態，從而消除漂移並提高可靠性。在資料中心、邊緣和雲端的每個叢集上推出經過驗證的變更，無需手動進行。
- **完全整合的 CNCF 工具：**包含生產就緒的可觀察性、政策與安全專案。
- **內建實體隔離支援：**叢集機群可在受限或斷網環境中安全執行，並提供完整的生命週期管理。

Nutanix 為 Kubernetes 叢集機群提供單一管理平台，讓團隊能夠輕鬆部署經過驗證的變更、執行政策，並全面掌握不同供應商環境的運作狀況。藉此打造一個具備韌性的平台，在資料中心、邊緣與雲端環境中維持一致的營運管理，並提供無縫的使用體驗。

了解更多：
使用 NKP 進行叢集機群管理 | Nutanix University

第 3 章
在邊緣環境運行 Kubernetes

傳統的 IoT 模型是針對遙測和集中式分析而建立，但在現今的邊緣環境中卻有不足。在製造業、零售業及遠端作業等產業中，企業需要管理數百或數千個分散式站台，而這些站台的連線通常並不可靠。這些地點需要輕量、自主且能在資料產生的地方處理資料的基礎架構。

常見挑戰

- **傳統的 IoT 堆疊：**專為資料收集而建立，而非即時處理或人工智慧工作負載。
- **不可靠的連線：**偏遠地點通常在網際網路存取有限或無網際網路存取的情況下運作。
- **營運開銷：**管理多個地點的基礎結構會增加複雜性。
- **資源限制：**邊緣站點的運算、儲存和電力有限。
- **安全性與法規遵循：**分散式環境擴大了攻擊面。

Nutanix 的價值：全堆疊平台

Nutanix 為邊緣環境提供完整的解決方案，將基礎架構、Kubernetes 協調和應用程式生命週期管理整合在單一平台中。

關鍵能力：

- **彈性邊緣基礎架構：**精巧、為邊緣環境最佳化的叢集，可部署於裸機或虛擬化環境中運行。
- **斷線作業：**NKP 專為間歇性或無網路連線的情境而設計，並在隔離環境中提供完整的生命週期管理支援。
- **集中式機群管理：**使用工作區和專案等內建 NKP 功能，從單一控制平面管理所有邊緣叢集。
- **基於 GitOps 的應用程式交付：**使用專案直接從 Git 套件庫部署應用程式，確保不同網站的一致性。
- **彈性的叢集配置：**自訂控制平面和工作站節點大小，以符合網站限制 (1、3 或 5 節點控制平面)。
- **精簡應用程式堆疊：**內建可觀察性、政策及生命週期工具，針對邊緣使用個案進行最佳化。

Nutanix 為 Kubernetes 叢集機群提供單一管理平台，讓團隊能夠輕鬆部署經過驗證的變更、執行政策，並全面掌握不同供應商環境的運作狀況。藉此打造一個具備韌性的平台，在資料中心、邊緣與雲端環境中維持一致的營運管理，並提供無縫的使用體驗。

第 4 章
安全性與合規性

隨著 Kubernetes 環境在叢集與團隊之間擴展，強制執行一致的安全性與合規性變得非常重要。企業必須管理多租用權、隔離工作負載，並確保影像傳輸的安全性，尤其是在受管制的產業和分散式環境中。

常見挑戰

- **不一致的安全政策：**叢集間不同的組態會導致執行缺口。
- **手動憑證管理：**靜態機密和憑證增加了作業開銷和風險。
- **多租用的複雜性：**很難在不同環境中安全地隔離工作負載和使用者。
- **安全的影像傳送：**確保可信來源和弱點掃描通常需要手動進行。
- **合規要求：**在不同環境中符合 FIPS 140-2 等標準需要整合工具。

Nutanix 的價值：全堆疊平台

Nutanix 提供全面的安全功能，可確保不同叢集、使用者與工作負載之間維持一致的安全政策，同時簡化合規性和存取管理。

關鍵能力：

- **端對端安全性：**基於角色的存取控制 (RBAC)、加密、FIPS 140-2 支援，以及整合式法規遵循工具，為 Kubernetes 工作負載提供安全的環境。
- **集中式驗證：**開箱即用的整合式 SSO，針對所有 NKP 管理和連接的叢集提供聯合驗證。
- **靈活的身分整合：**將現有的企業識別供應商與 NKP 無縫連接。
- **無憑證存取：**直接在瀏覽器中顯示 kubectl 登入資訊 - 省去手動憑證處理。
- **雲原生網路：**由 CNCF 專案 Cilium 和 Calico 所提供的高度可擴充與安全的網路。
- **Pod 層級防火牆：**使用 Kubernetes 網路政策來控制哪些 Pod 和服務可以彼此存取。

Nutanix 可確保各個 Kubernetes 叢集維持一致的安全性與合規性，並簡化從邊緣、核心到雲端環境的存取控制、工作負載隔離，以及法規遵循。

了解更多：

使用 NKP 網路政策保護容器化應用程式 | Nutanix University

Nutanix Kubernetes Platform 安全秘訣：Gatekeeper 政策 | Nutanix University

第 5 章
資料保護與管理

隨著 Kubernetes 的應用範圍擴大到具狀態工作負載，資料成為平台策略的核心。具狀態工作負載帶來新的複雜性，例如：需要持久性儲存、合規性和災難復原。雖然 Container Storage Interface (CSI) 驅動程式可標準化儲存的配置方式，但卻無法解決企業級資料保護、行動性或治理的問題。平台工程師現在面臨的挑戰是如何在混合與多雲環境中管理資料，並將其視為首要考量。

常見挑戰

- **有限的 CSI 範圍：**CSI 可處理儲存配置，但缺乏內建的資料保護和 DR 功能。
- **零散的工具：**將備份、DR 和遷移的多個解決方案拼接在一起會增加複雜性。
- **合規壓力：**法規要求資料零遺失，並嚴格控制資料儲存的地點與方式。
- **多叢集環境：**跨叢集和雲端管理資料需要一致的政策和工具。
- **開發人員的摩擦：**複雜的資料工作流程會減慢自助服務和平台工程的速度。

Nutanix 價值：Kubernetes 企業級資料服務

Nutanix 利用企業級資料保護和管理功能擴展 CSI，在叢集和雲端提供以應用程式為中心、政策驅動的服務。就像 Kubernetes 一樣，所有的資料服務都被設計為分散式且能毫不費力地擴充。

關鍵能力：

- **適用於 Kubernetes 的企業級儲存：**Nutanix Unified Storage 為具狀態應用程式提供整合式持久性儲存，包括支援區塊、檔案和物件儲存。其擴充架構與 Kubernetes 應用程式的建立與執行方式一致，可確保在叢集間進行簡化的擴充。
- **分層資料服務：**使用 Nutanix Data Services (NDK)，支援同步及非同步複寫、備份及還原，並提供彈性的 RPO/RTO 選項。
- **以應用程式為中心的管理：**使用政策式複寫和快照工具，保護整個應用程式命名空間及其相關資料和 Kubernetes 物件。
- **自助服務工具：**宣告式 CRD 驅動介面可讓開發人員無需承受過多認知負擔，即可輕鬆管理資料工作流程。
- **合規政策：**跨邊緣、雲端和內部環境強制執行儲存和保護政策。
- **多角色支援：**IT 管理員和平台工程師使用 Prism Central 和 kubectl 等熟悉的工具來管理基礎架構和資料。
- **工作負載移動性：**在不同叢集與供應商環境之間遷移具狀態應用程式，以處理升級、重新平衡或雲端轉型需求。
- **同級產品中最佳的整合：**使用 Velero 等 CNCF 專案進行備份與還原，並支援物件儲存與混合雲目標。
- **適用於 Kubernetes 的資料庫管理：**Nutanix Database Services (NDB)可為 Kubernetes 環境中執行的資料庫自動進行佈建、修補和保護。

Nutanix 為 Kubernetes 提供可靠、可擴展的資料保護與管理，透過以應用程式為中心的統一方法，弭平 CSI 與企業需求之間的落差。

了解更多：

Kubernetes 應用程式層級資料服務

使用 Nutanix 與 NDK 實現 Kubernetes 災難復原 | Nutanix University

第 6 章
實體隔離環境部署

Kubernetes 原本是為雲原生環境而設計，但許多企業和政府組織都是在斷線、受限或高度安全的網路中運作。這類實體隔離環境常見於國防、製造和遠端作業，因此需要能夠獨立於網際網路運作，同時維持安全性、一致性和作業效率的平台。

常見挑戰

- **有限的網路：**頻寬限制、高延遲和封包遺失會破壞作業。
- **隔離網路：**無法存取網際網路，需要堡壘主機或 DMZ 進行更新。
- **受限制的網路：**嚴格的安全政策、目的地過濾和代理要求。
- **雲原生預設：**大多數容器工具的設計，都以能夠持續連線至公有容器登錄庫為前提。
- **營運開銷：**手動設定和分散的工具造成風險和複雜性。

Nutanix 的價值：實體隔離優先架構

Nutanix Kubernetes 平台專為在斷網環境中安全且自主運作而打造，提供完整的 Kubernetes 技術堆疊，並整合安全防護、容器登錄庫與生命週期管理工具。

關鍵能力：

- **實體隔離優先設計：**從安裝到生命週期管理，都可以離線完成。
- **Uber Bundle：**單一離線捆綁，包含容器影像和圖表，以佈建叢集。
- **內建容器登錄庫支援：**透過應用程式目錄部署 Harbor 容器登錄庫，以便在本機託管和管理容器映像檔。
- **代理和離線支援：**使用現有的代理伺服器，或使用離線套件直接從本機容器登錄庫進行安裝。
- **軍事級 DevSecOps：**
  - 預先掃描的版本和安裝套件，可進行安全、有效的部署
  - SSO 和集中式 RBAC 可提供統一的存取控制
  - 多租用支援可安全隔離工作負載
  - VPC 整合與網路政策可提供精細的流量控制
  - 加密通訊以保護傳輸中的資料
  - 政策強制執行與異常偵測，可主動提供安全性與合規性

NKP 透過結構化套件、內建容器登錄庫，以及嚴謹的實體隔離環境測試，即使在最嚴苛的環境中，也能快速且順利完成部署。藉助自動化與清楚明確的操作指引，即使是複雜的環境設定也能可靠部署，讓 Kubernetes 能夠在任何需要的環境中安全執行，並靈活擴展規模。

第 7 章
混合雲 Kubernetes

隨著企業在多種環境中採用 Kubernetes，許多企業發現他們在 AWS (EKS)、Azure (AKS) 和 Google Cloud (GKE) 等不同的公有雲中管理叢集。雖然這些管理服務功能強大，但它們的設計是在各自的生態系統中運作，因此難以維持跨平台運作的一致性、可見性和治理。

常見挑戰

- **零散的工具：**每個雲端供應商都有自己的主控台、API 和運作模式。
- **不一致的安全性與政策：**不同環境的管理方式各異，增加風險。
- **營運開銷：**管理多個堆疊會增加複雜性和成本。
- **能見度有限：**難以追蹤雲端的使用量、效能與成本。
- **孤立的團隊：**不同的環境通常會導致工作重複和工作流程不一致。

Nutanix 的價值：跨雲端統一 Kubernetes

Nutanix Kubernetes 平台在雲原生服務與企業需求之間架起了一座橋樑，為地端、公有雲和邊緣環境提供一致的 Kubernetes 體驗。

關鍵能力：

- **集中化管理：**從單一主控台跨雲端部署、升級及監控叢集。
- **雲原生相容性：**與 AWS、Azure 及 GCP 的服務整合，讓團隊可以在已使用的服務上進行建置。
- **統一工具：**一套工具和工作流程橫跨所有環境，減少學習曲線和重複。
- **成本與資源可見性：**深入了解應用程式層級的成本，並全面掌握基礎結構的使用情況。
- **政策一致性：**在不同環境中統一執行管理與自動化。
- **營運效率：**簡化生命週期管理並降低人工成本。
- **適用於地端部署的全堆疊基礎架構：**透過單一平台統一管理 Kubernetes、虛擬機、儲存、網路、安全性與協同編排，簡化環境建置，並降低持續營運階段的複雜性。

Nutanix 可在各種環境中實現一致、政策驅動的 Kubernetes 體驗。透過集中化控制、整合式工具以及成本與效能的可視性，無論工作負載在何處執行，團隊都能簡化作業、降低風險並加速交付。

了解更多：
一致的混合多雲 Kubernetes 體驗 | Nutanix University

第 8 章
加速開發人員交付效率

開發人員的生產力是企業成功的關鍵驅動力，但在許多組織中，開發人員花在基礎架構上的時間可能多於編寫程式碼的時間。從佈建環境到管理相依性，開發與作業之間的摩擦會降低交付速度。平台工程旨在消除這些障礙，為開發人員提供簡化的自助服務體驗，讓程式碼能夠快速、可靠地從開發環境推進至 QA，再部署至正式環境。

常見挑戰

- **交接緩慢：**開發、品保與正式環境之間的手動流程會延誤版本發布。
- **工具過多：**開發人員必須跨環境學習和維護多種工具。
- **缺乏自動化：**基礎結構的佈建與更新通常需要提交服務請求單，或使用客製化指令碼。
- **不一致的環境：**階段之間的差異會導致錯誤和重工。
- **合規負擔：**安全與政策執行往往採取被動因應的方式，且仰賴手動作業。

Nutanix 價值：透過平台工程加速開發效率

Nutanix 提供全堆疊 Kubernetes 平台，可簡化基礎設施、整合現有的 CI/CD 管道，並賦予開發人員自助服務功能。

關鍵能力：

- **CI/CD 整合：**NKP 可與現有管道搭配使用，因此團隊無需為了配合專有 API 而重新建置工作流程。
- **開發人員自助服務：**Workspaces 與 Projects 可讓開發人員獨立部署和管理應用程式。
- **全堆疊平台：**提供企業應用程式所需的一切，包括基礎架構、資料服務、網路及業務連續性。
- **內建保護機制：**OPA Gatekeeper 政策可確保合規性，同時不影響工作流程效率。
- **可觀察性與自動化：**整合式記錄、監控和警示功能可簡化故障排除和版本驗證。

Nutanix 透過提供安全的 Kubernetes 自助服務體驗，協助平台團隊提升開發人員的交付效率。藉助自動化、一致性與全堆疊整合，開發人員可專注於建置應用程式，而無需耗費心力管理基礎架構；同時，營運團隊仍能在不同環境中維持完善的控制與可靠性。

準備了解更多？

探索雲原生技術資源中心提供的技術部落格文章、操作教學影片，以及經驗證的設計方案。

NUTANIX

info@nutanix.com | www.nutanix.com | @nutanix

©2026 Nutanix, Inc.保留所有權利。Nutanix、Nutanix 標誌和本文件所提及的所有 Nutanix 產品及服務名稱，均屬於 Nutanix 公司在美國和其他國家的註冊商標或商標。
Kubernetes® 是 Linux Foundation 在美國和其他國家的註冊商標。本文提及的所有其他品牌名稱均僅供識別參考，並且可能為其各自擁有者所屬商標。

ACloudNativePlaybookForPlatformEngineers-v2-zh-TW-101526