iKala Cloud

從封閉到開放 -
實踐 API 經濟的最佳選擇：Apigee Hybrid

目錄

全面執行 API-first 商業策略：Apigee Hybrid

越來越多的企業採用 API 優先方法連結部署在混雲和多雲環境中的服務來驅動商業模式創新和資訊系統現代化。為了滿足混合雲環境下管理 API 的需求，我們推出 Apigee Hybrid 讓您彈性地部署您的 API 運行平台，同時還可以使用以雲端為基礎的開發人員入口網站、API 監控服務、API 分析服務。Apigee Hybrid 可以部署在 Anthos 環境中，藉此享有 Google Cloud 對自動化和安全控管的支援。

Apigee Hybrid 解決 Gap Inc. 以往部署系統時必須在雲端和地端環境二擇一的兩難問題。

Gap Inc. 使用 Apigee 發佈、保護、分析 API，並迅速地讓應用服務開發團隊開始使用這些 API。Apigee Hybrid 幫助 Gap Inc. 解決以往部署系統時必須在地端和雲端兩者環境擇一的兩難問題，提供了兩全其美的解決方案。

「當需要改善延遲或配合機敏資料管理辦法時，通常我們會將運行平台部署在地端，Apigee Hybrid 讓我們可以輕鬆地管理這些運行在地端的運行平台。於此同時，我們還能繼續享有所有的 Apigee 優勢，像是開發人員入口網站和豐富的 API 生命週期管理工具。」Gap Inc. 企業架構師 Patrick McMichael。

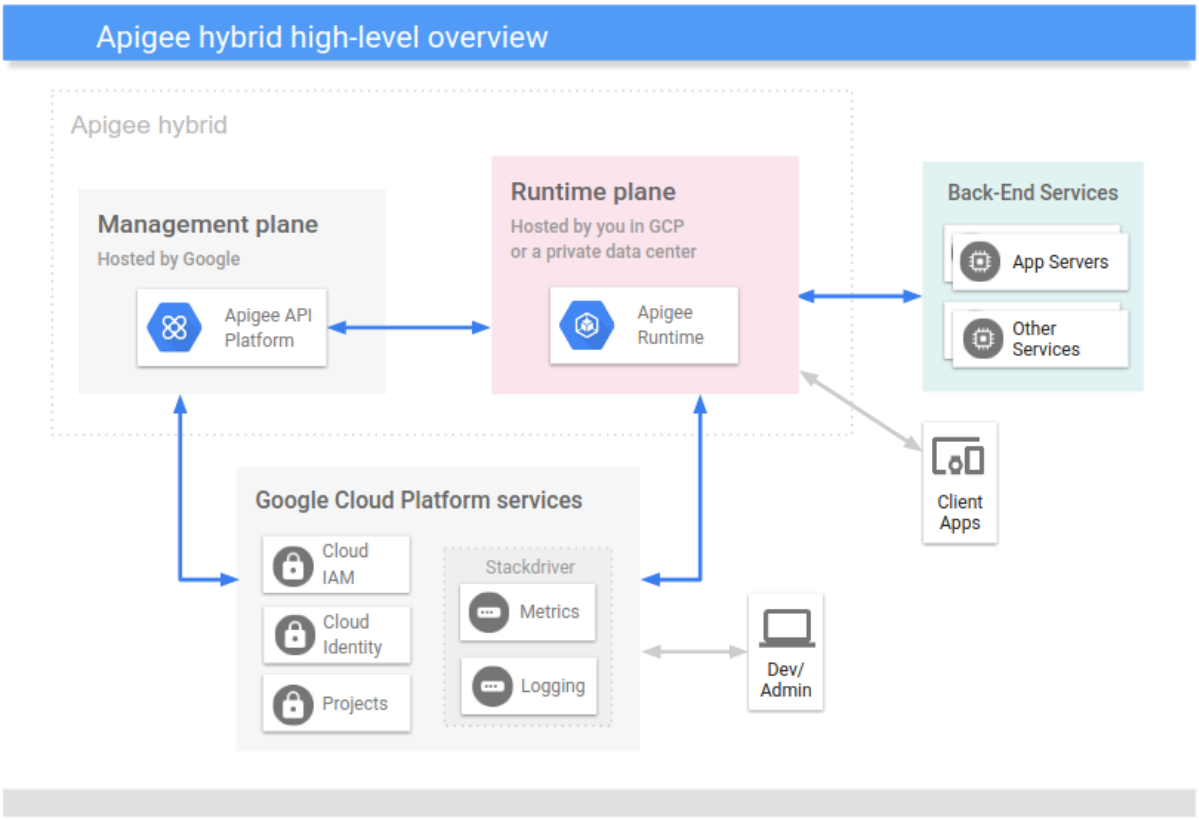
什麼是 Apigee hybrid?

Apigee Hybrid 是個可以讓您同時管理部署在地端 (on-prem) 和雲端 (GCP) 的 API：

在一個地方管理所有的 API	Apigee Hybrid 幫助您在 Google Cloud Platform 上同時管理內部和外部的 API。透過統一管理，您可以提供一致的 API 使用體驗，無論是開放 API 給您的開發人員、合作夥伴、 或是客戶。
滿足安全性和合規性的需求	如果出自於安全性和合規性的考量，必須將您的應用程式部署在地端 (on-prem) 環境中，搭配企業級混合雲 API 閘道 (API Gateway)，您可以部署和管理 Apigee 運行平台在您的地端環境中。您可以使用現有合規又安全的的設施來管理和控制運行平台。
幫助您實現多雲策略	同時考量到成本和效能的時候，您可能會考慮採用多雲策略來取得一個平衡。無論您正在評估不同的雲服務供應商，或是已經採用多雲策略，您的 API 管理平台都應該讓您有彈性可以滿足需求。Apigee Hybrid 可以部署和管理企業級的混合雲 API 閘道 (API Gateway) 在您的資料中心、Google Cloud Platform、或是同時兩者。

混合雲環境下的 API 管理解決方案

Apigee Hybrid 包含兩個部分，一個是由 Google 維護的管理平台，一個是由您安裝的運行平台，運行平台可以安裝在地端的 Kubernetes，也可以安裝在雲端 (GCP) 的 Kubernetes (GKE)。兩個平台都有使用到 Google Cloud Platform 上的服務，如下圖所示：



您可以看到，Apigee hybrid 主要由以下幾個部分組成：

- Apigee-run management plane: 管理平台運行在雲端，由 Google 負責維護。管理平台提供網頁 UI、管理用的 API (management API)、和 API 使用分析服務。
- Customer-managed runtime plane: 運行平台被部署在您所控管的 Kubernetes 叢集中，所有的 API 流量都會通過運行平台，並在運行平台內被處理。透過 Kubernetes 管理容器化的運行平台，例如階段式的版本更新、自動擴展，幫助您更敏捷地維運運行平台。
- Google Cloud Platform: Google管理的雲端服務。

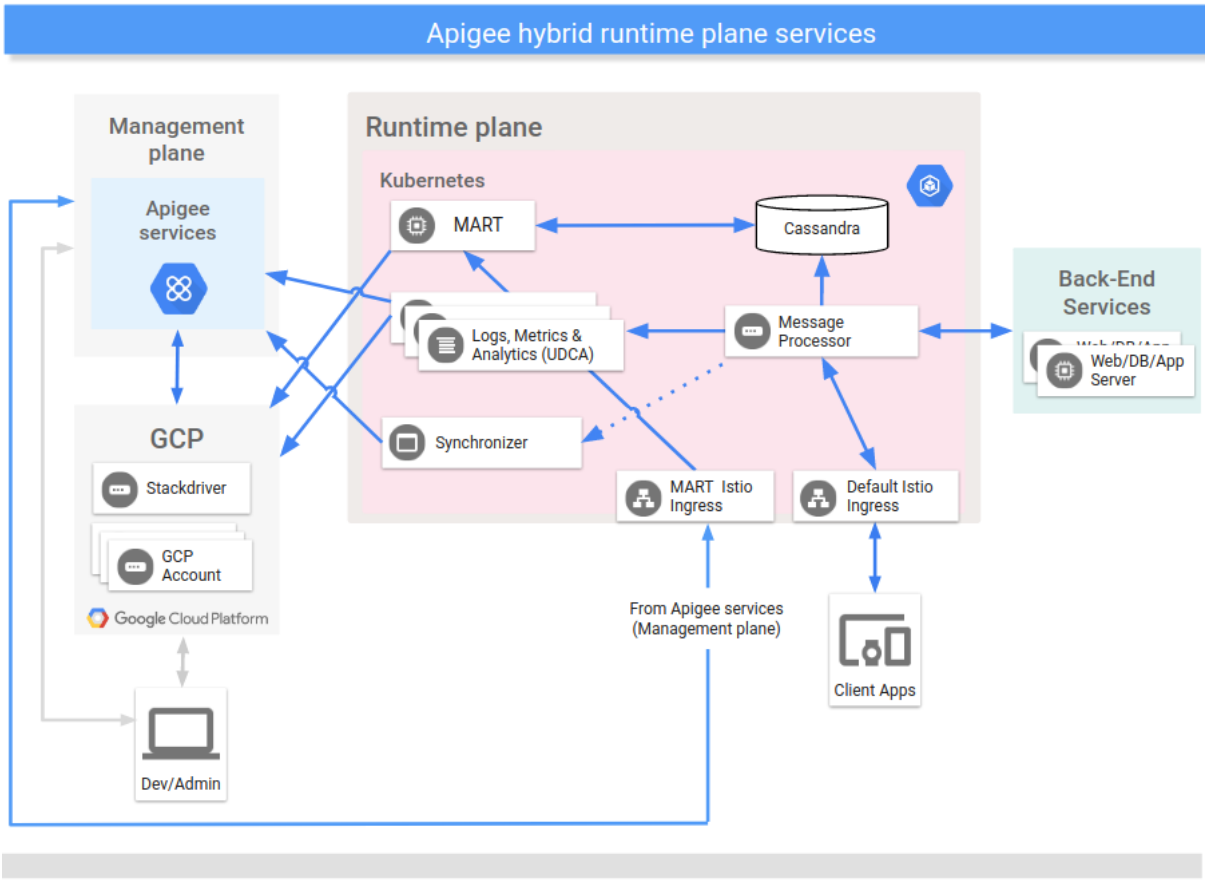
Apigee Hybrid 有一點很重要的概念是 所有的 API 流量只會在您所管控的網路內被處理，只有管理平台像是網頁 UI、API 使用分析服務才會運行在雲端由 Google 所維護。

關於運行平台

運行平台是一組容器化服務，可以設置在您所使用的 Kubernetes 叢集環境。所有的 API 流量都會通過運行平台，並在運行平台內被處理。運行平台包括以下幾個部分組成：

- Message Processors
- Synchronizer
- Cassandra
- MART
- UDCA

運行平台在您所管理的 Kubernetes 叢集中運作。下圖顯示了運行平台內的主要服務：



關於運行平台內的元件服務，請參閱以下說明。此外，也可以參閱運行平台元件服務設定文件。以下各節將更詳盡的介紹運行平台服務。

訊息處理器

部署在運行平台內的 Hybrid Message Processors (MPs) 元件是負責處理 API 請求和執行對應的 API 處理規則。MPs 是從本地儲存空間載入所有已部署的物件資訊，包含 API Proxies、資源、目標伺服器、憑證、和金鑰。您可以部署一個 Istio Ingress 控制器將 MPs 開放對外來處理來自外部的 API 請求。

同步器

同步器從管理平台獲取 API 環境 (environment) 的組態設定，並將它傳送到運行平台。這份設定稱為契約 (contract)。同步器會定期檢查管理伺服器 (Management Server)，並在偵測到更新時下載新的組態設定。下載後的組態設定是以 JSON 檔案格式儲存在本地儲存空間提供給 MPs 讀取。儲存在本地端的組態設定讓運行平台可以正常運作而不依賴管理平台。契約可以讓運行平台上的 MPs 使用儲存在本地端的資料作為組態設定。如果管理平台和運行平台之間的網路連線中斷，運行平台上的功能仍然可以正常運作。

同步器下載的組態設定內容包含：

- API 代理伺服器設定 (proxy bundles) 和 共享的流程部署 (shared flow deployments)
- 流程掛鉤 (flow hooks)
- 環境資訊 (environment information)
- 共享的 API 資源 (shared API resources)
- 目標伺服器設定 (target server definition)
- TLS 設定
- 環境快取 (environment caches)
- Key Value Map (KVM) 名稱
- 資料屏蔽 (data masks)

Cassandra 資料庫

Apache Cassandra 是運行平台的資料庫，在運行平台中提供資料持久服務 (Core Persistence Services, CPS)。Cassandra 是分散式的資料系統，可為運行平台上的資料提供持久性。Cassandra 資料庫是以 Kubernetes StatefulSet 形式部署在您的 Kubernetes 叢集中的資料節點群組 (data node pool)。 將資料儲存服務和運行平台中負責邏輯處理的服務部署在鄰近的位置有助於滿足安全性和高擴展性的系統需求。

Cassandra 資料庫儲存的資料包含以下內容：

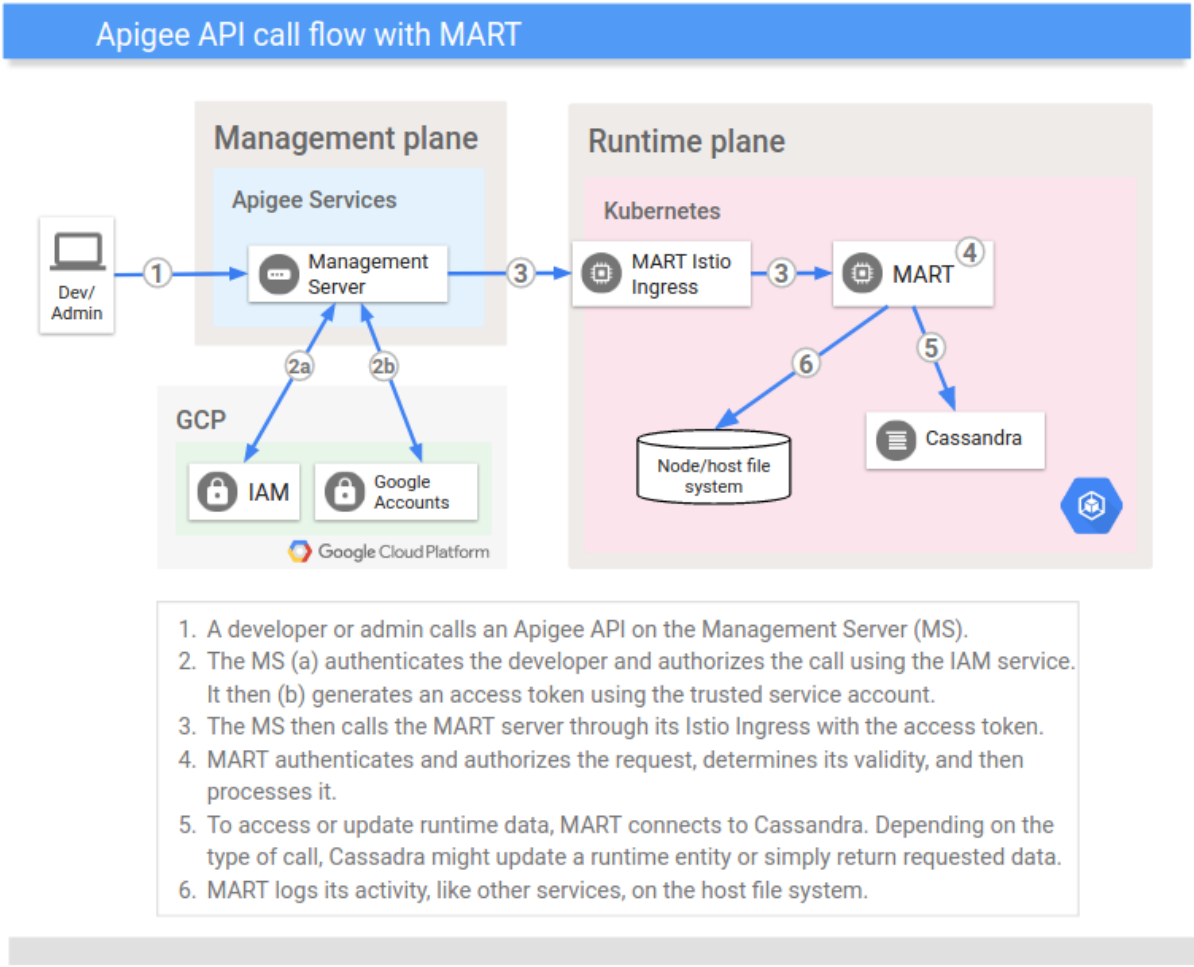
- 金鑰管理系統 (KMS)
- Key Value Map (KVM)
- 回應快取 (response cache)
- OAuth
- 配額 (quotas)

運行平台資料管理 API (MART)

在處理 API 請求時可以存取隸屬於您的組織 (organization) 的資料，這些資料像是應用程式組態設定資料、 KMS 資料、快取資料、KVM 資料，都儲存在運行平台內的 Cassandra。如果要存取或是更新這些資料，例如新增一筆 KVM 資料到您的環境 中，或刪除一筆 KVM 資料從您的環境中，您可以透過 Apigee Hybrid UI 或 使用 Apigee APIs。MART 負責處理這類存取運行平台資料庫的 API 請求。本章節將介紹Apigee APIs在訪問資料庫期間MART所扮演的角色。

MART 是什麼？	呼叫 Apigee API 時，是先送身份驗證請求到管理平台上的管理主機 (Management Server, MS)。MS 驗證並授權該請求，然後轉送該請求到運行平台上的 MART。轉送請求時會附加一個代碼 (token)，這個代碼是由 MS 透過預先設定好的服務帳號所產生。 MART 接收到請求時，確認驗證和授權後再執行企業邏輯的驗證。（舉例來說，發出請求的應用程式如果是一個 API 產品的一部分，MART 會先確保該請求是合格有效的），確認請求是合格有效後，MART 才會處理該請求。 Cassandra 也儲存 MART 處理的資料。（畢竟它是運行平台的資料庫）MART 會根據請求的類型從 Cassandra 讀取或更新資料。
MART 不是什麼？	雖然 MART 有對外開放，您不會直接呼叫 MART。（MART 必須有對外開放的埠號 (port)，這樣才能接收來自 MS 的呼叫，呼叫授權是透過服務帳號 (service account) 的機制）。 除此之外，MART 不接受其他應用程式的 API 呼叫，這些來自其他應用程式的API 呼叫應該是透過 Istio Ingress Controller 被路由到您運行平台的 MPs 來處理。

MART 和 MPs 都可以訪問相同的運行平台的資料庫 (Cassandra)， KMS、KVMs、和快取等等這些資料透過這個方式可以在運行平台中共享。下圖顯示了 Apigee API 的呼叫流程：



通用資料收集代理程式 (UDCA)

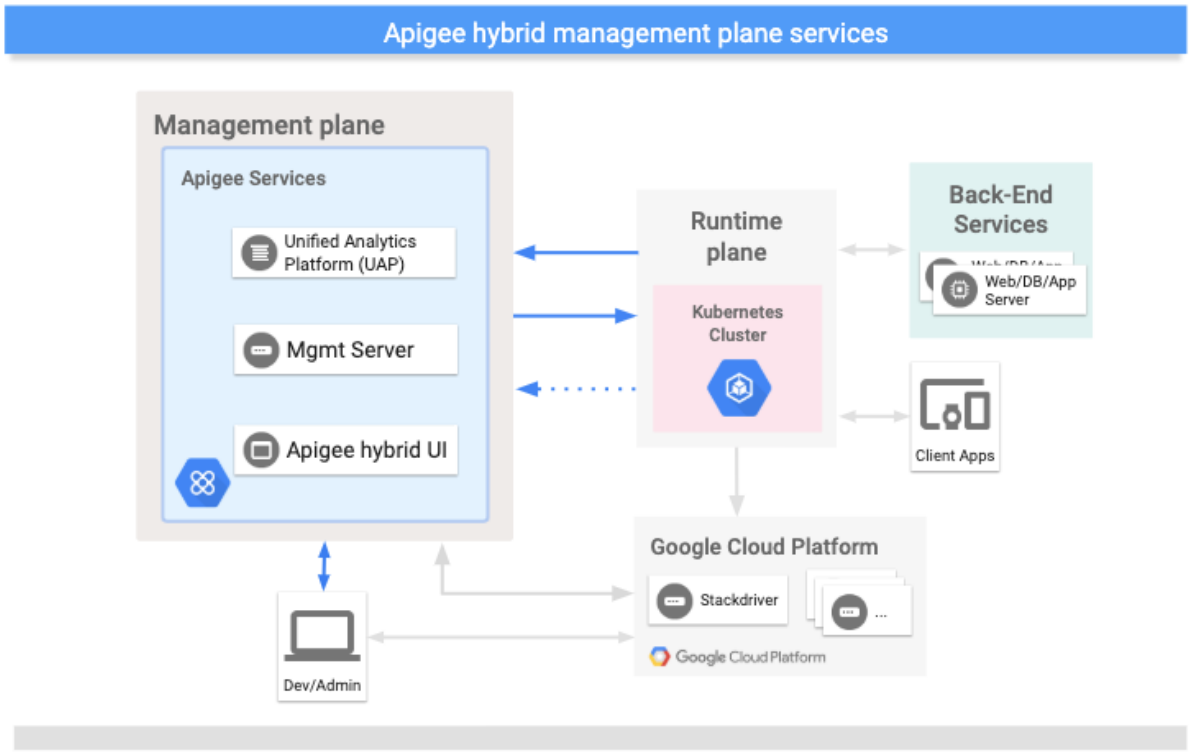
UDCA 在運行平台中扮演資料收集的角色、收集的資料類型包含追蹤 (trace)、分析 (analytics) 和部署狀態 (deployment status) 並將它們傳送到管理平台中的 UAP 服務。更多相關訊息，請參閱資料收集說明文件。

關於管理平台

管理平台在Google Cloud Platform上運作，其管理服務包含：

- Apigee hybrid UI：提拱使用介面 (UI) 給開發人員建立和部署 API 代理伺服設定 (API proxies)、設定 API 處理規則 (policies)、建立 API 產品 (products)、建立應用程式 (apps)。管理人員則可以透過這個使用介面 (Apigee Hybrid UI) 監控部署狀態。
- Apigee APIs：提供程式介面 (API) 用以管理組織資訊 (organization) 和環境資訊 (environments)。
- Unified Analytics Platform (UAP)：負責接收和處理來自運行平台上報的部署狀態 (deployment status) 資料。

下圖顯示了管理平台內的主要服務：



關於 Google Cloud 服務

以下表格說明 Apigee Hybrid 使用到的主要 GCP 服務內容：

GCP 服務	說明
身份認證	使用者身份驗證是透過 GCP 使用者帳號 (GCP user account) 驗證機制，系統服務授權是透過 GCP 服務帳號 (GCP service account)。
角色	存取權限管理是透過 GCP IAM 角色 (role) 機制，Apigee 預設角色已經整合在 GCP IAM 角色清單中。
資源階層結構	Apigee 資源隸屬於 GCP 專案 (概念上如同其他 GCP 資源)。(GCP 專案 (project) 物件與 Apigee 組織 (organization) 物件互相連結)。
Stackdriver	提供日誌和監控服務。

使用者類型

在 Apigee Hybrid 中有以下幾種主要的使用者類型：

角色	責任/任務	延伸閱讀
系統管理人員 / 維運人員	• 在 Apigee Hybrid 運行平台安裝、設定元件服務 • 設定 GCP、Apigee、服務帳號 • 建立 GCP 專案和啟用服務 • 管理 Kubernetes 叢集 • 維護上述資源 • 故障排除 API 代理伺服設定 (API proxies)	• 下載並安裝apigeectl • 設定 GCP 服務和 Apigee Hybrid UI • 安裝 Apigee hybrid • 管理 Apigee hybrid • Apigee hybrid 資料收集 • Apigee Hybrid 服務設定 • Kubernetes
開發人員	• 建立 API 代理伺服器 (API proxies) 透過 Apigee Hybrid UI 或 Apigee APIs • 部署 API 代理伺服器到運行平台 • 故障排除 API 代理伺服器 • 測試 API 代理伺服器	• 使用 Apigee Hybrid 建立和部署 API 代理伺服器 • Apigee hybrid 資料收集 • API 處理規則

優勢

Apigee hybrid 具有以下優勢：

降低持有成本

如果您是正在使用 Apigee Edge for Private Cloud 版本的客戶，Apigee Hybrid 讓您用更少的軟體管理您的地端 API。

提高敏捷性

由於 Apigee Hybrid 是在容器中運行，您可以發揮容器化系統的優勢，像是階段式的版本釋出、自動擴展等等。

降低延遲

所有和管理平台的溝通都是非同步的，而且處理 API 請求不依賴於管理平台的溝通。

增加 API 的採用

雖然使用 Apigee Edge Public Cloud 也可以管理您的內部 API，但是透過 Apigee Hybrid 可以進一步降低延遲。之所以能夠提升效率的原因在於您的 API 閘道 (gateway) 部署在地端運行，非常靠近您的後端服務。如果您是正在使用 Apigee Edge Public Cloud 版本的客戶，透過 Apigee Hybrid 您可以進一步增加 API 的採用，因為納入了內部 API。如果您正在使用 Edge Microgateway，透過 Apigee Hybrid 您也可以進一步增加 API 的採用，因為 Apigee Hybrid 克服了 Edge Microgateway 的限制。

更佳的控制方式

許多企業採取混合雲策略。管理部署在私有雲資料中心的 API 運行平台，對於大型企業來說是一個關鍵需求。Apigee Hybrid 運行平台可以部署在 GCP 或您的資料中心。

參考資料

[1] Don’t just move to the cloud, modernize with Google Cloud
[2] What is Apigee hybrid?