Microsoft

Reactor

MS Learn 學堂
Azure Kubernetes Service 學習

Friday 11th March | 3:30 PM HK

Kinfey Lo

Cloud Advocate | Microsoft

Hello , All !

Kinfey Lo – (盧建暉)

Microsoft Cloud Advocate

Former Microsoft MVP , Xamarin MVP and Microsoft RD, with more than 10 years of experience in cloud native, artificial intelligence, and mobile applications, providing application solutions for education, finance, and healthcare. Microsoft Iginte, Teched conference lecturer, Microsoft AI hackathon coach, currently at Microsoft, preaching technology and related application scenarios for technicians and different industries.

I love programming (Python , C# , TypeScript , Swift , Rust , Go)

Focus on artificial intelligence, mobile applications, cloud native

Github : https://github.com/lokinfey **Open Source Project :** https://github.com/SciSharp/TensorFlow.NET

Email : kinfeylo@microsoft.com **Blog :** https://blog.csdn.net/kinfey

Twitter : @Ljh8304

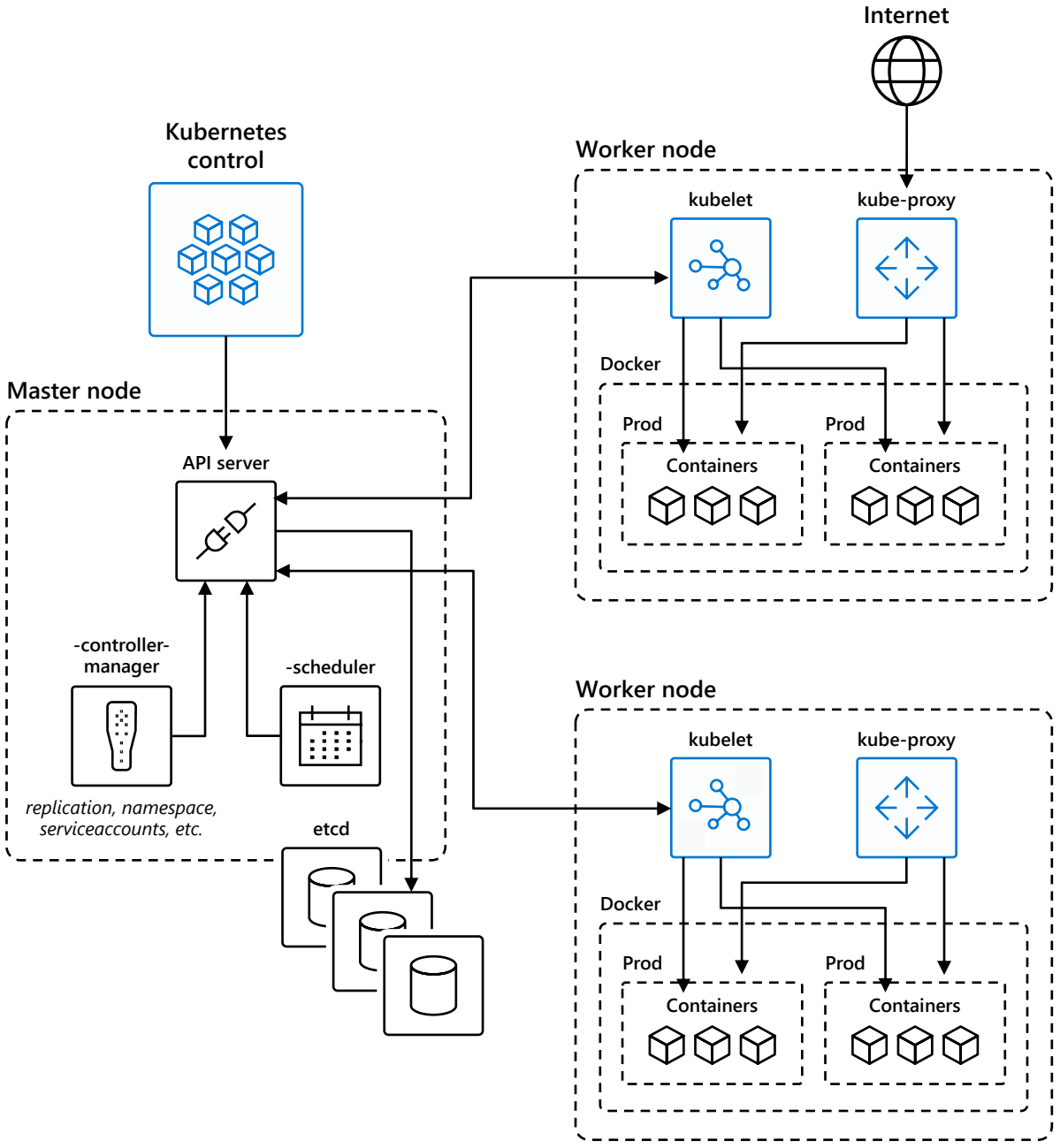
Azure 資源索取

Free Azure Plan https://azure.com/free

Free Azure Student Plan https://aka.ms/StudentGetAzure

Kubernetes

1. Kubernetes 用戶與 API 服務器通信並應用所需狀態
2. 主節點主動在工作節點上強制執行所需狀態
3. 工作節點支持容器之間的通信
4. 工作節點支持來自 Internet 的通信



Containers in Azure

App Service

Deploy web apps or APIs using containers in a PaaS environment

Service Fabric

Modernize .NET applications to microservices using Windows Server containers

Kubernetes Service

Scale and orchestrate Linux containers using Kubernetes

Container Instance

Elastically burst from your Azure Kubernetes Service (AKS) cluster

Functions

Run code on-demand without having to explicitly provision or manage infrastructure

Batch

Run large-scale parallel and high-performance computing (HPC) applications efficiently in the cloud

IoT Edge

Move cloud analytics and custom business logic to devices

Ecosystem

Bring your Partner solutions that run great on Azure

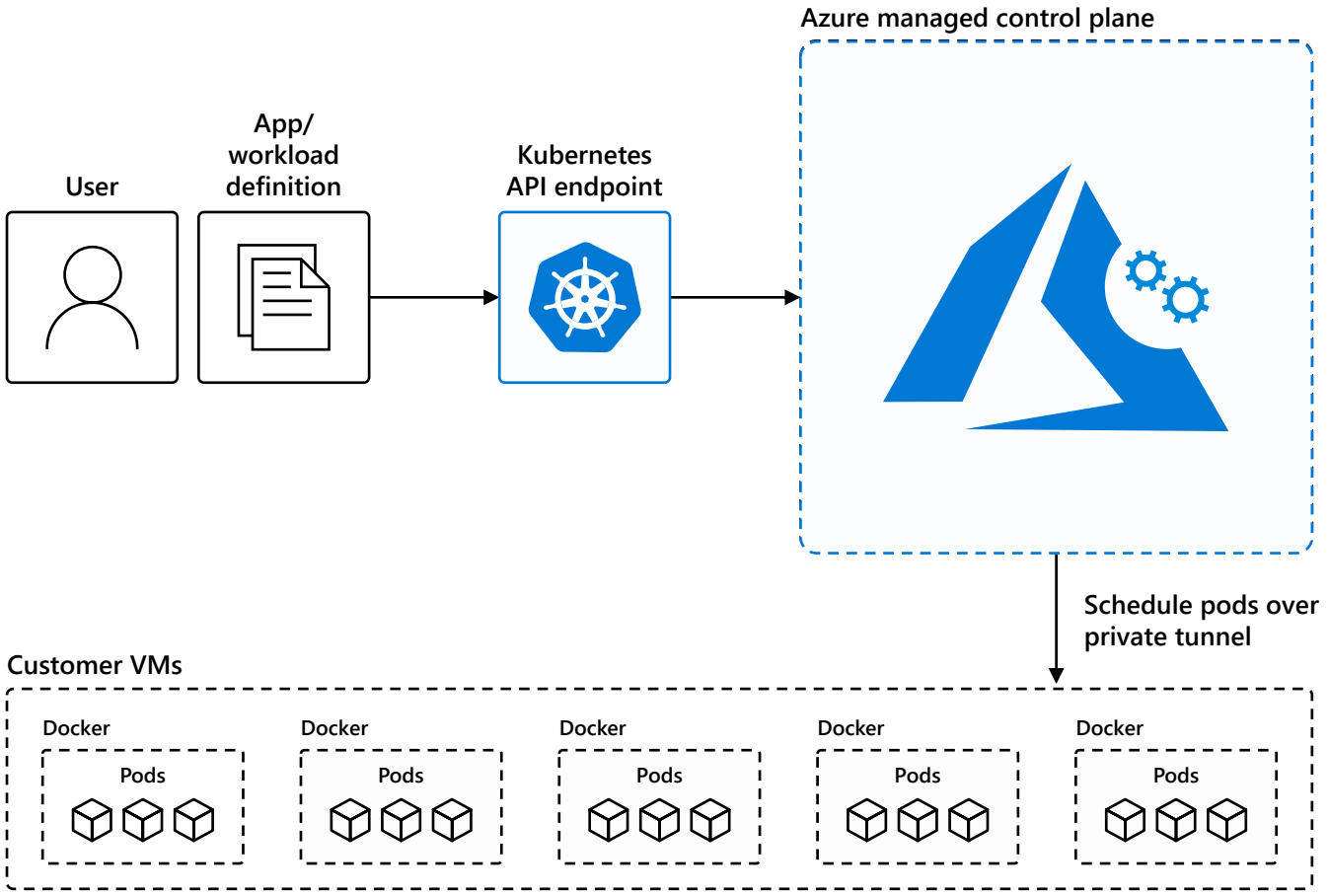
Azure Container Registry

Docker Hub

Choice of developer tools and clients

Managed Kubernetes on Azure

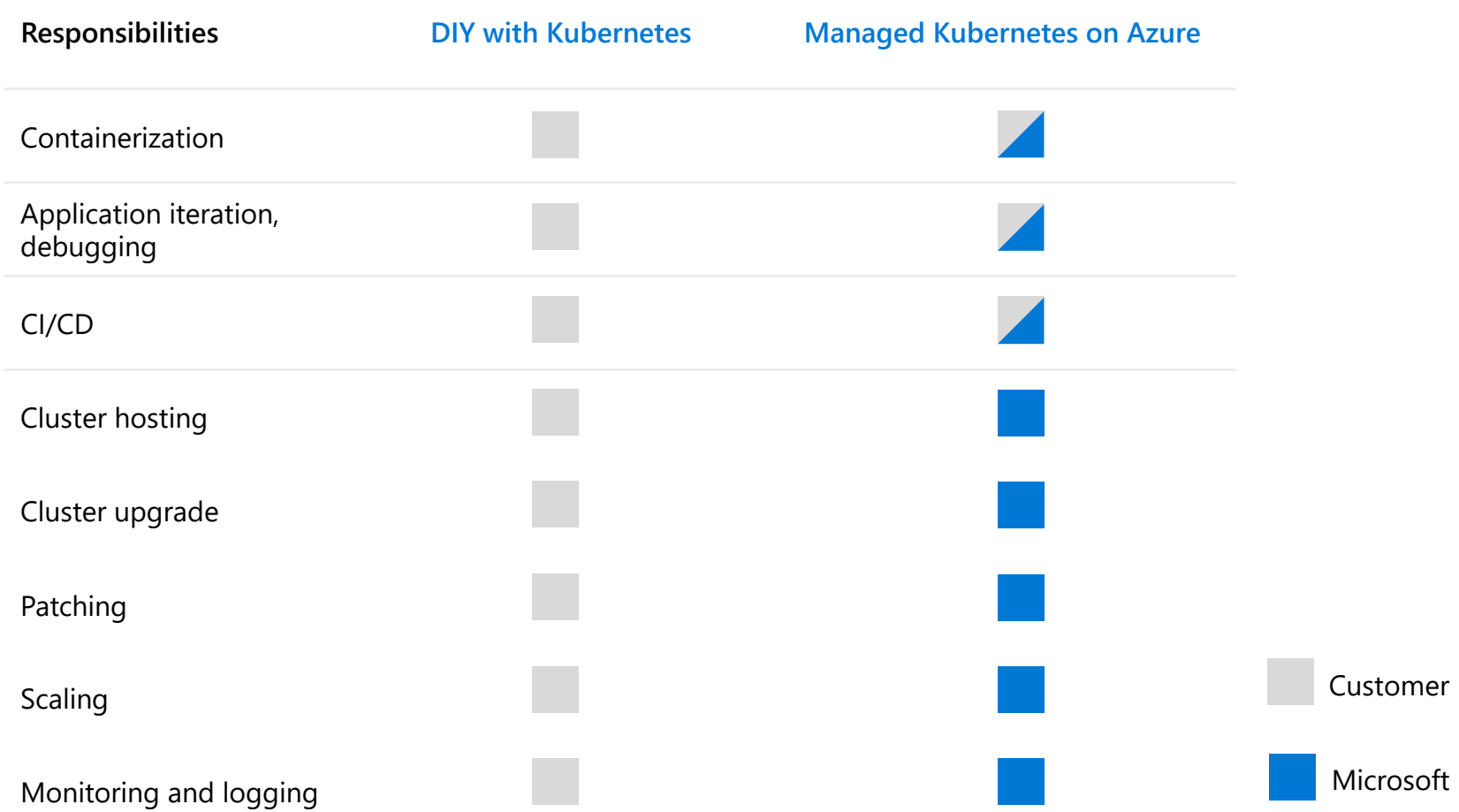
- 自動升級、補丁
- 高可靠性、可用性
- 簡單、安全的集群擴展
- 自我修復
- API 服務器監控
- 不收費



From infrastructure to **innovation**

Managed Kubernetes empowers you to do more

Focus on your containers and code, not the plumbing of them



Work how you want with opensource tools and APIs

	Development	DevOps	Monitoring	Networking	Storage	Security
Take advantage of services and tools in the Kubernetes ecosystem	HELM	Jenkins Terraform BRIGADE JFrog CODESHIP HASHICORP	Prometheus fluentd Grafana OPENTRACING DATADOG JAEGER	CNI Networking TIGERA	MAPR portworx	Twistlock aqua heptio RBAC
…or… Leverage growing Azure support	VS Code	Azure DevOps ARM	Azure Monitor	Azure VNET	Azure Storage	Azure Container Registry AAD Key Vault Security Center

Basic networking

使用 kubenet 網絡插件並具有以下功能

節點和 Pod 位於不同的 IP 子網上

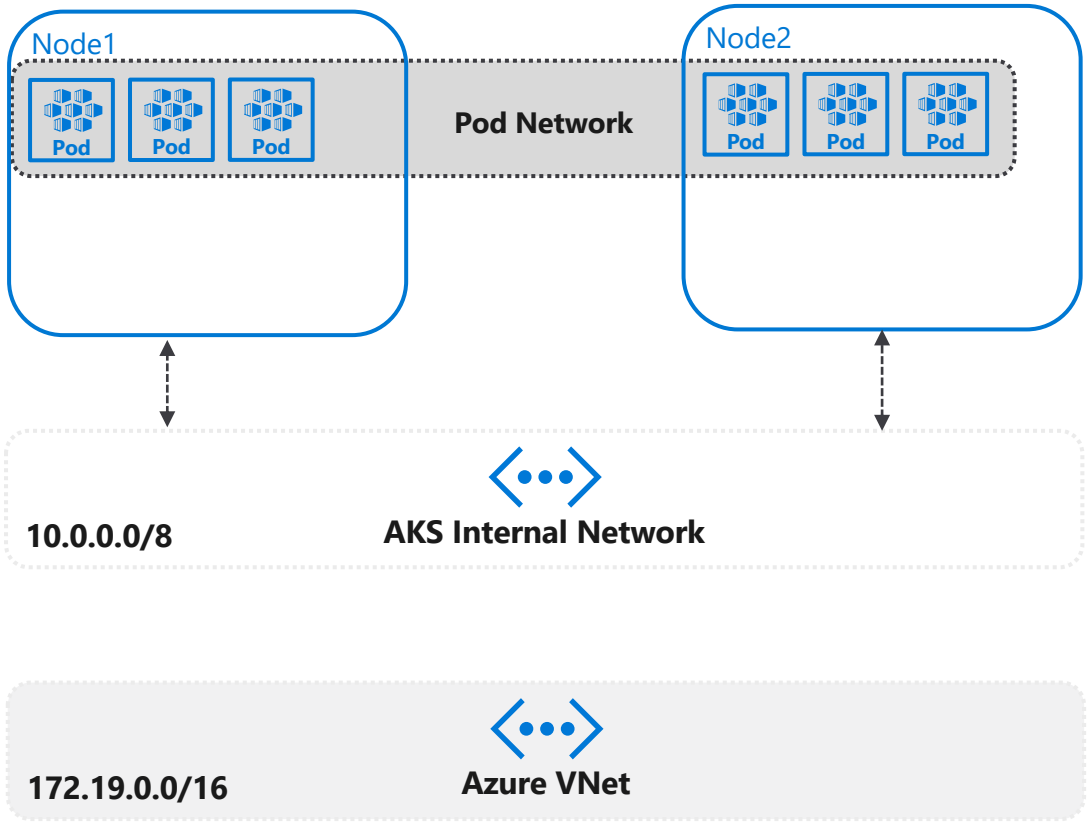
用戶定義的路由和 IP 轉髮用於跨節點的 Pod 之間的連接。

缺點

2 個不同的 IP CIDR 進行管理

性能影響

對等或本地連接很難實現



Advanced networking

使用 Azure CNI（容器網絡接口）

CNI 是一種供應商中立協議，容器運行時使用它向網絡提供商發出請求

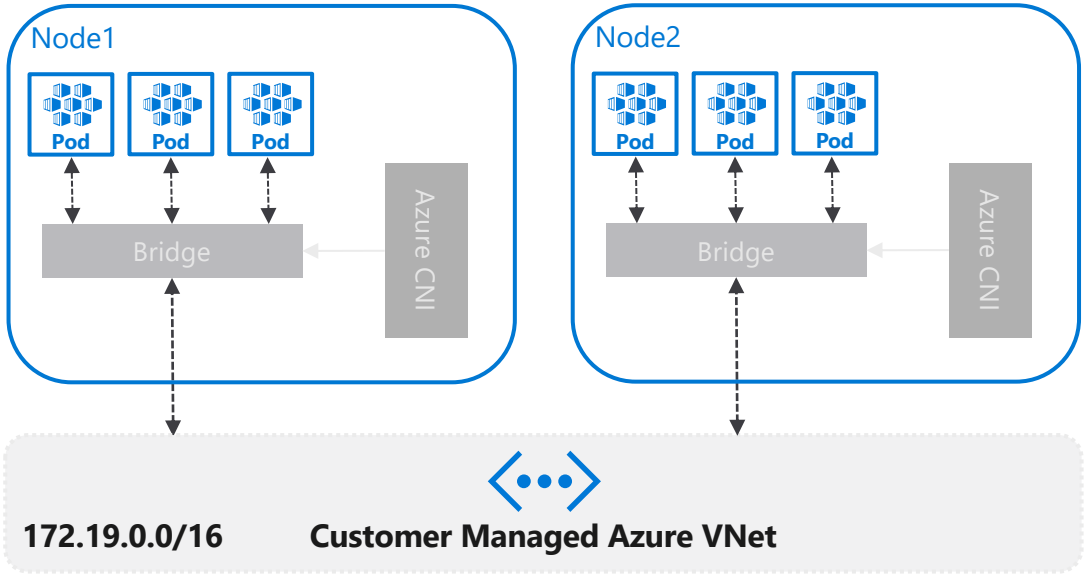
Azure CNI 是一種允許您將 Kubernetes 與您的 VNET 集成的實現

優點

單一 IP CIDR 進行管理

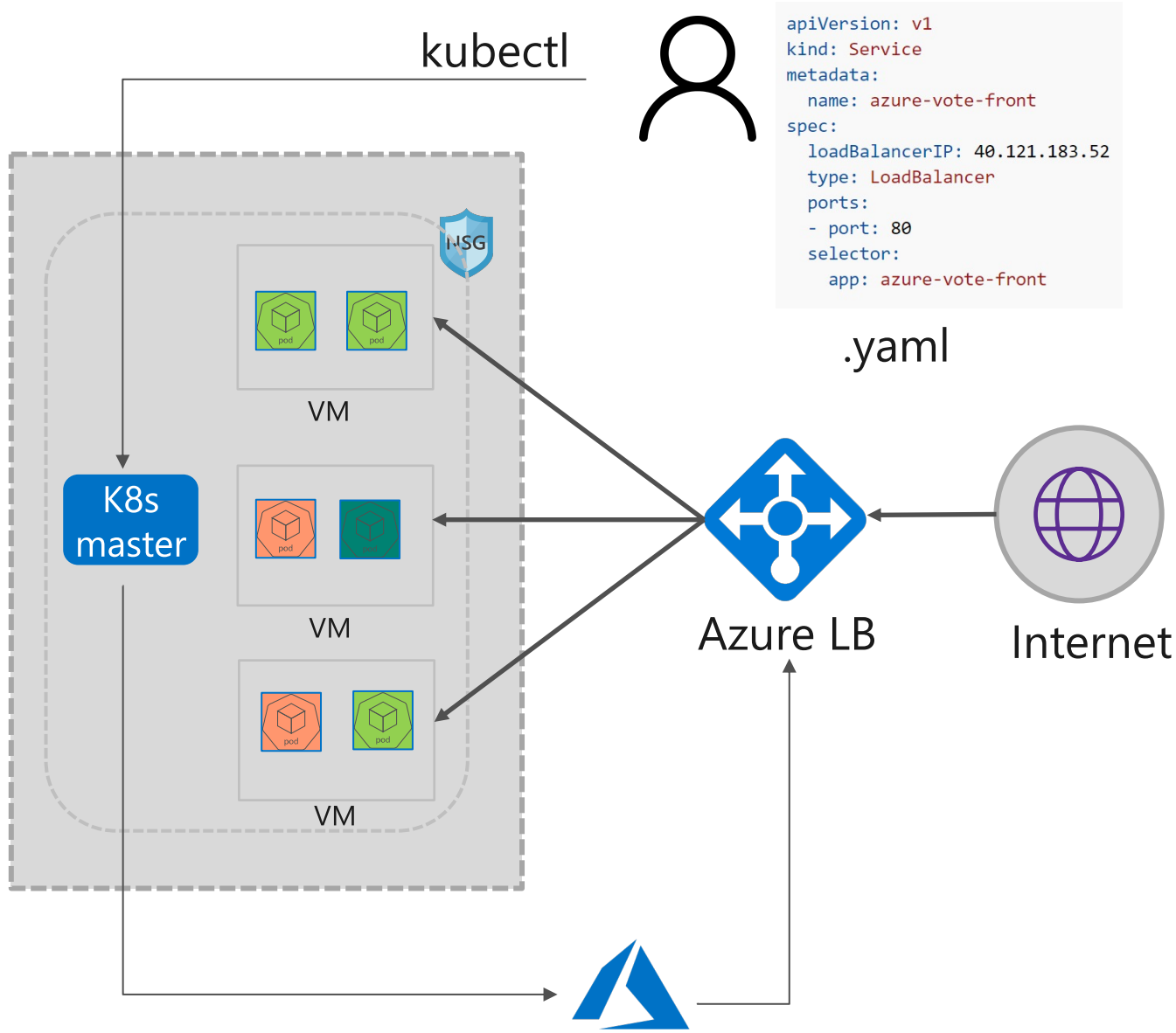
更好的性能

對等互連和本地連接是開箱即用的



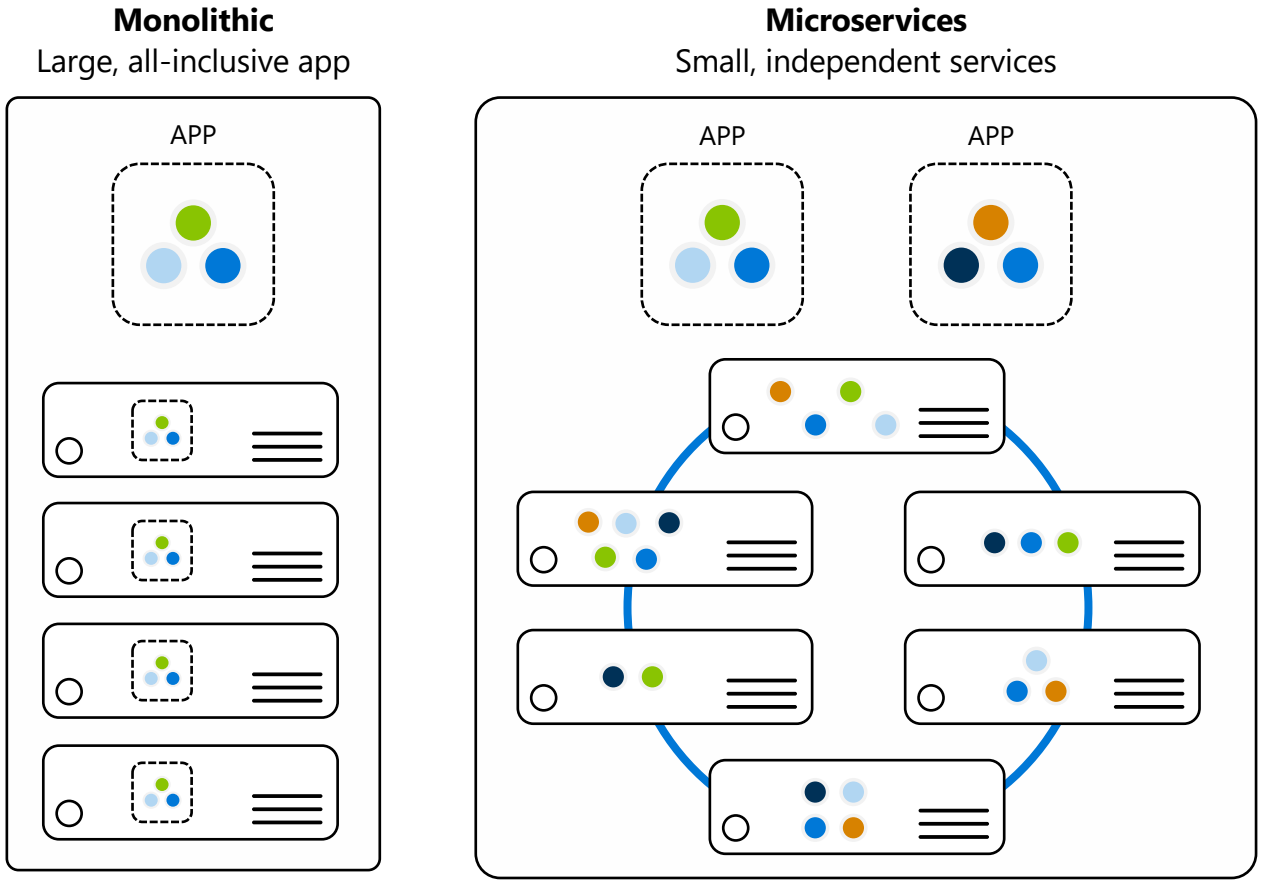
Network Load Balancing: Azure LB

- 使用 Azure 負載均衡器對 Pod 進行 TCP/UDP 負載均衡
- 與 Kubectl 集成，輕鬆一鍵部署
- 流量負載均衡並分發到虛擬機
- 每個 VM 的運行狀況探測
- KubeProxy 轉發到特定的 pod
- ExternalTrafficPolicy：本地，保留的客戶端源 IP
- ExternalTrafficPolicy：集群實現均衡分佈



Microservices: for faster app development

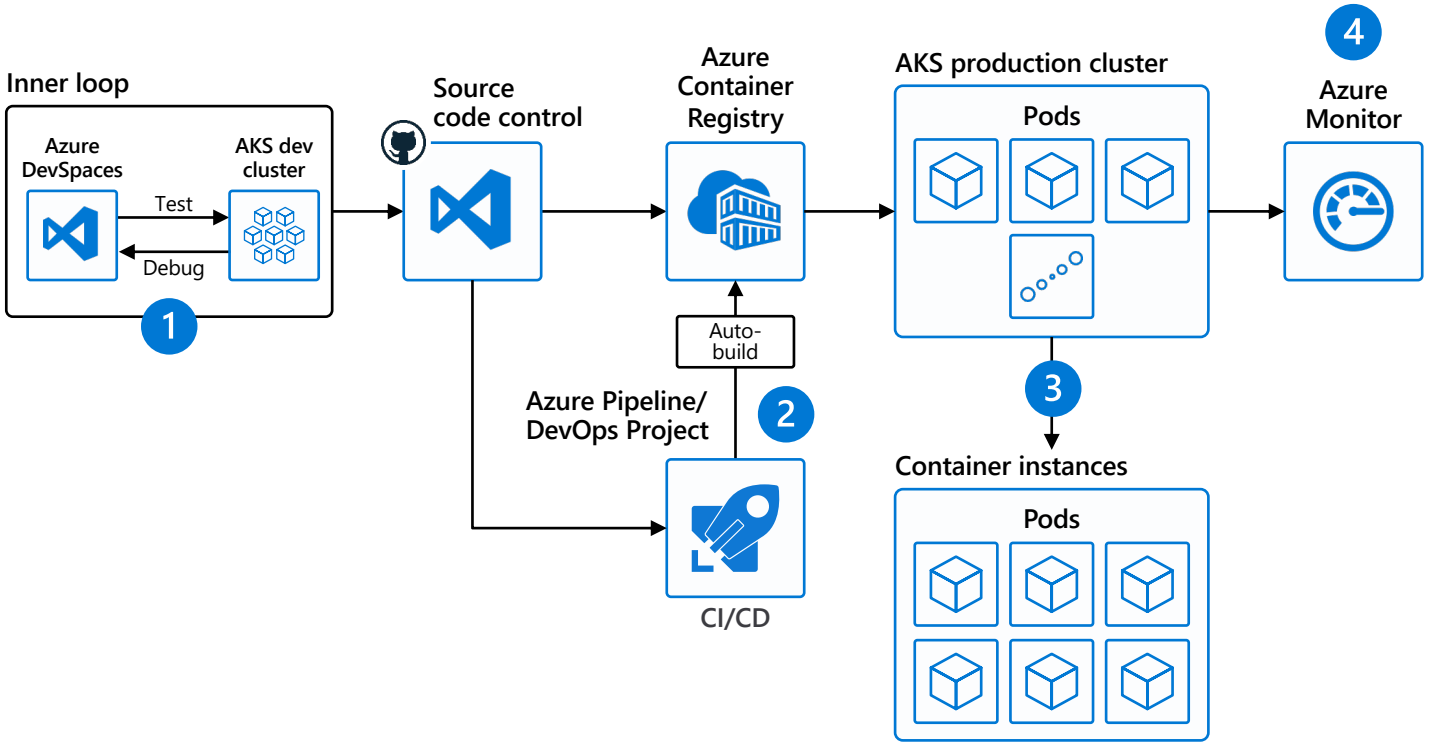
- 獨立部署
- 提高每項服務的規模和資源利用率
- 更小、更專注的團隊



Microservices: for faster app development

Capabilities

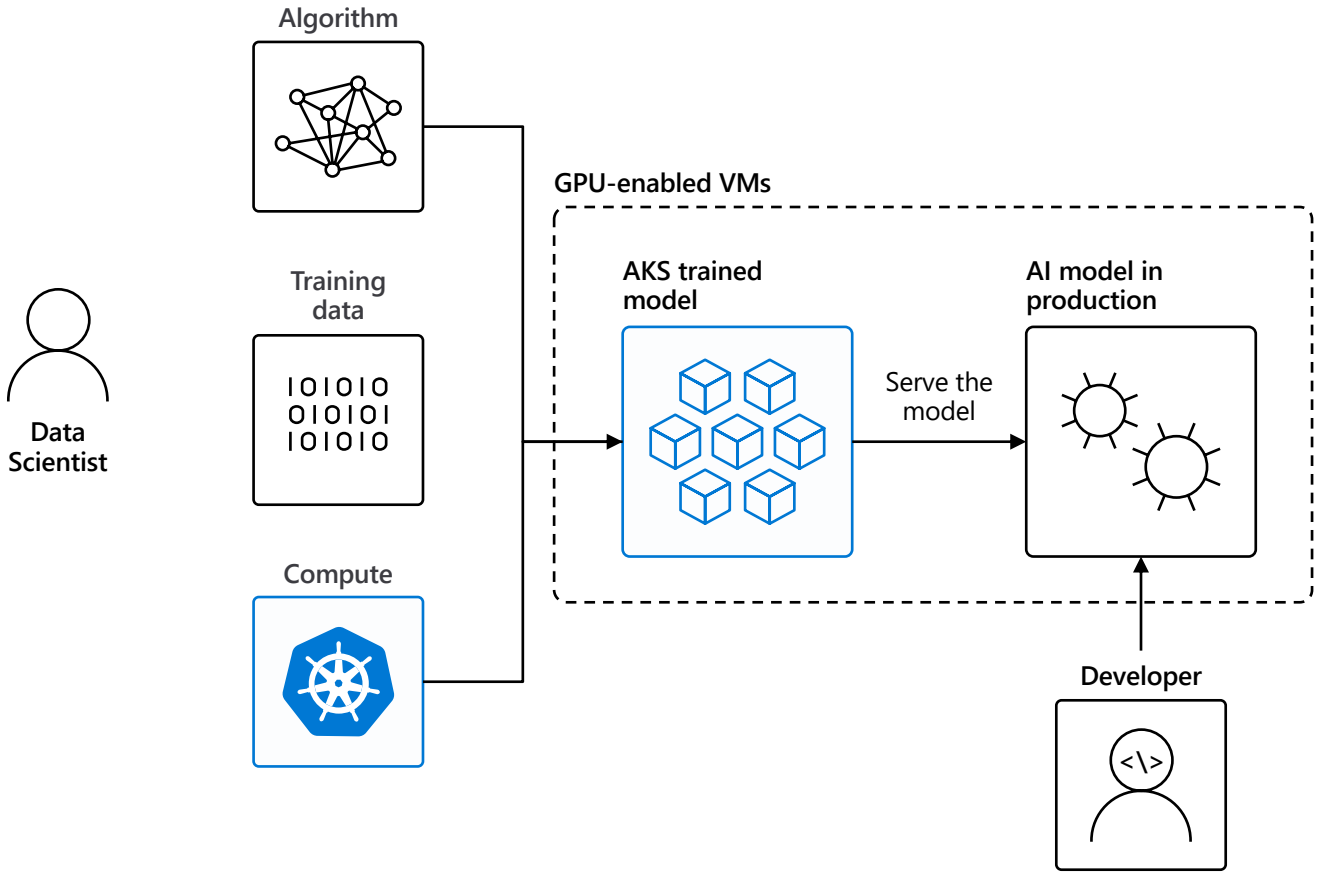
1. 使用 Azure Dev Spaces 以迭代方式開發、測試和調試針對 AKS 群集的微服務。
2. Azure DevOps 與 Helm 進行原生集成，有助於簡化持續集成/持續交付 (CI/CD)
3. 虛擬節點——一種虛擬 Kubelet 實現——允許快速擴展服務以應對不可預測的流量。
4. Azure Monitor 提供單一管理平台，用於監控應用遙測、集群到容器級別的健康分析。



https://github.com/Microsoft/SmartHotel360-AKS-DevSpaces-Demo

Data scientist in a box

- 快速部署和高可用性
- 低延遲數據處理
- 跨測試、控制和生產的一致環境

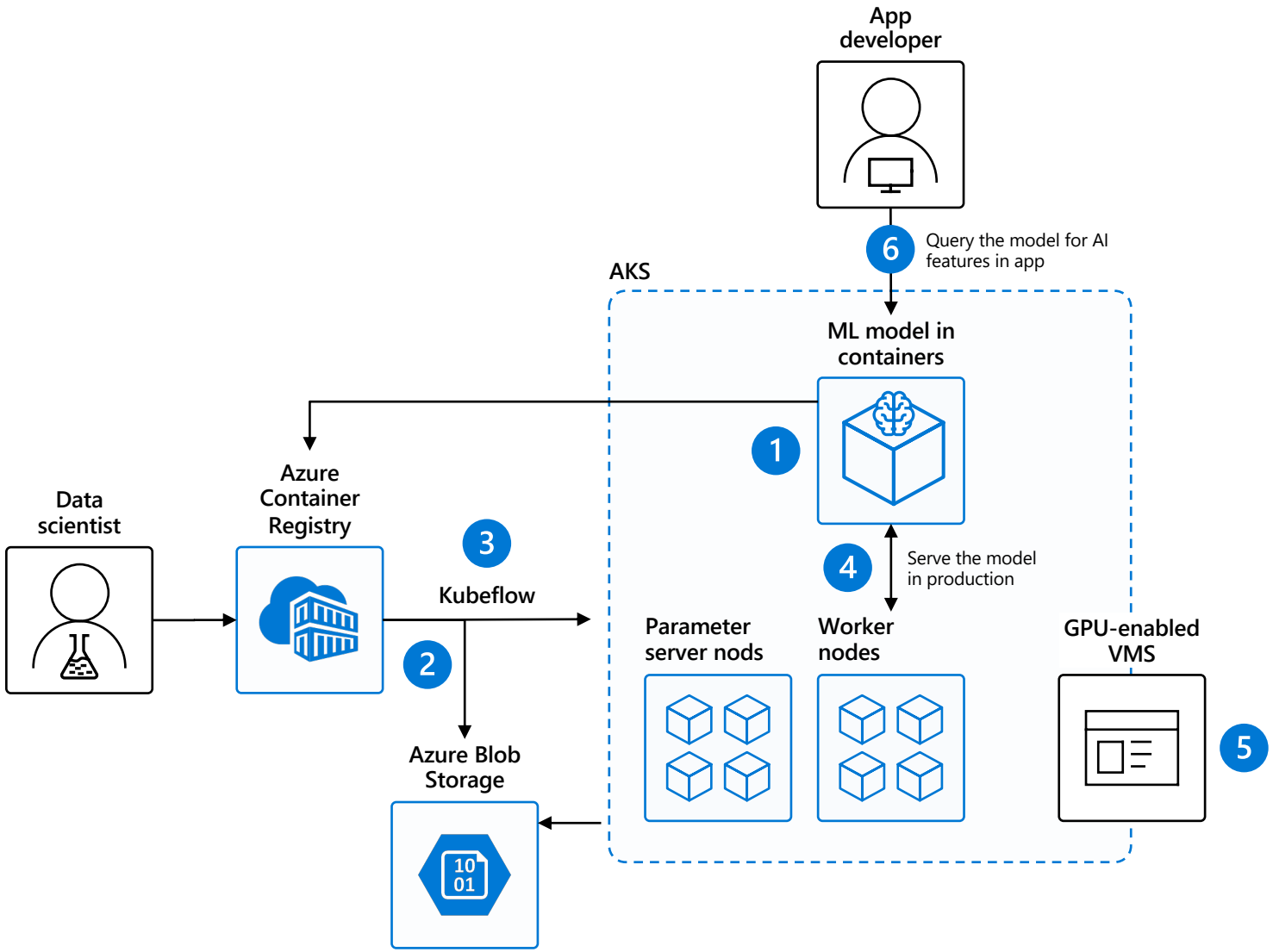


https://github.com/Azure/kubeflow-labs

Data scientist in a box

Capabilities

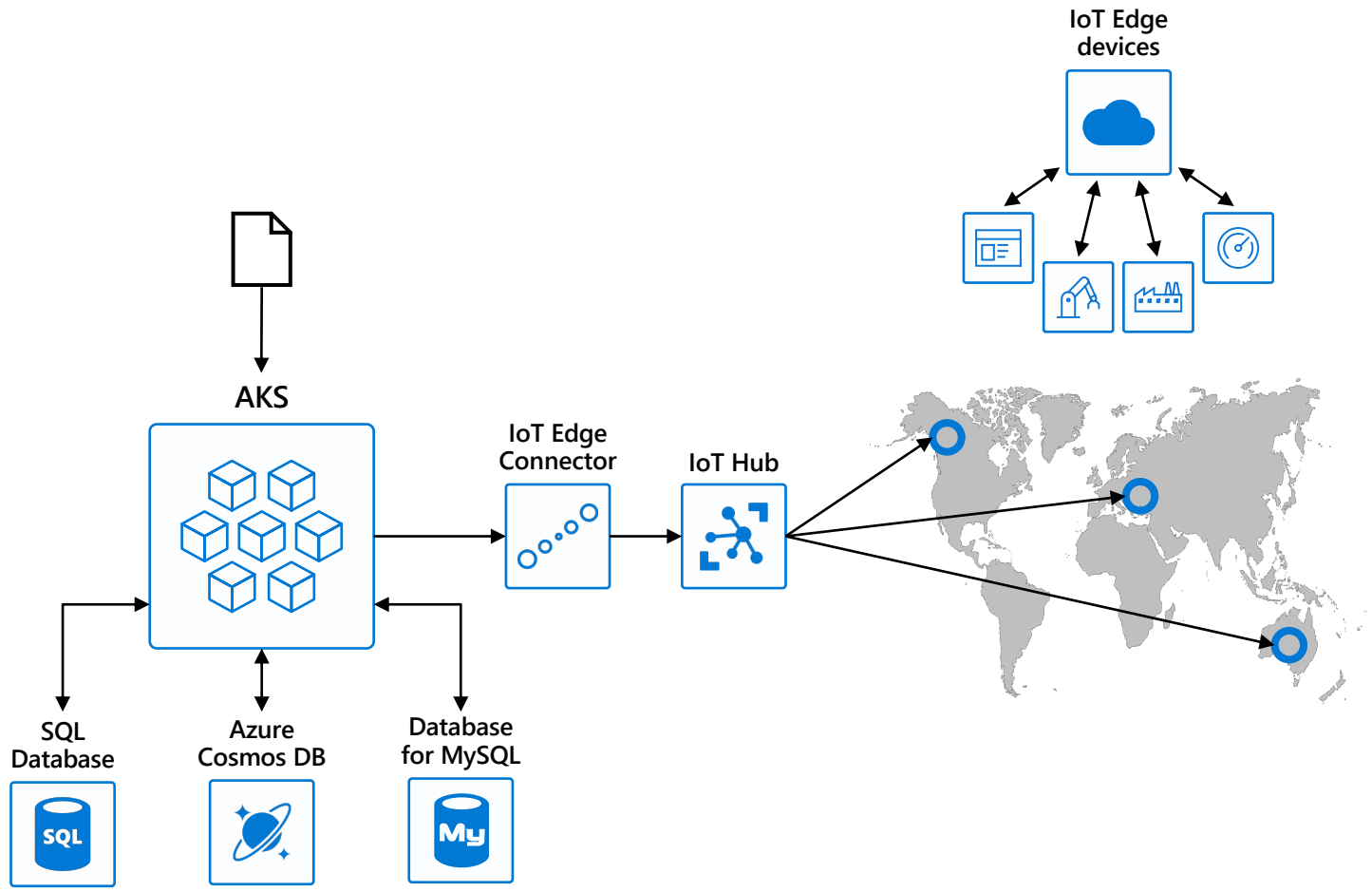
1. 將 ML 模型打包到容器中並發佈到 Azure Container Registry
2. Azure Blob 存儲託管訓練數據集和訓練模型
3. 使用 Kubeflow 將訓練作業部署到 AKS，分佈式訓練作業到 AKS 包括參數服務器和 Worker 節點
4. 使用 Kubeflow 服務生產模型，促進跨測試、控制和生產的一致環境
5. AKS 支持啟用 GPU 的 VM
6. 開發人員可以構建功能來查詢在 AKS 集群中運行的模型



https://github.com/Azure/kubeflow-labs

可擴展的物聯網解決方案

- 可移植的代碼，在任何地方運行
- 彈性可擴展性和可管理性
- 快速部署和高可用性



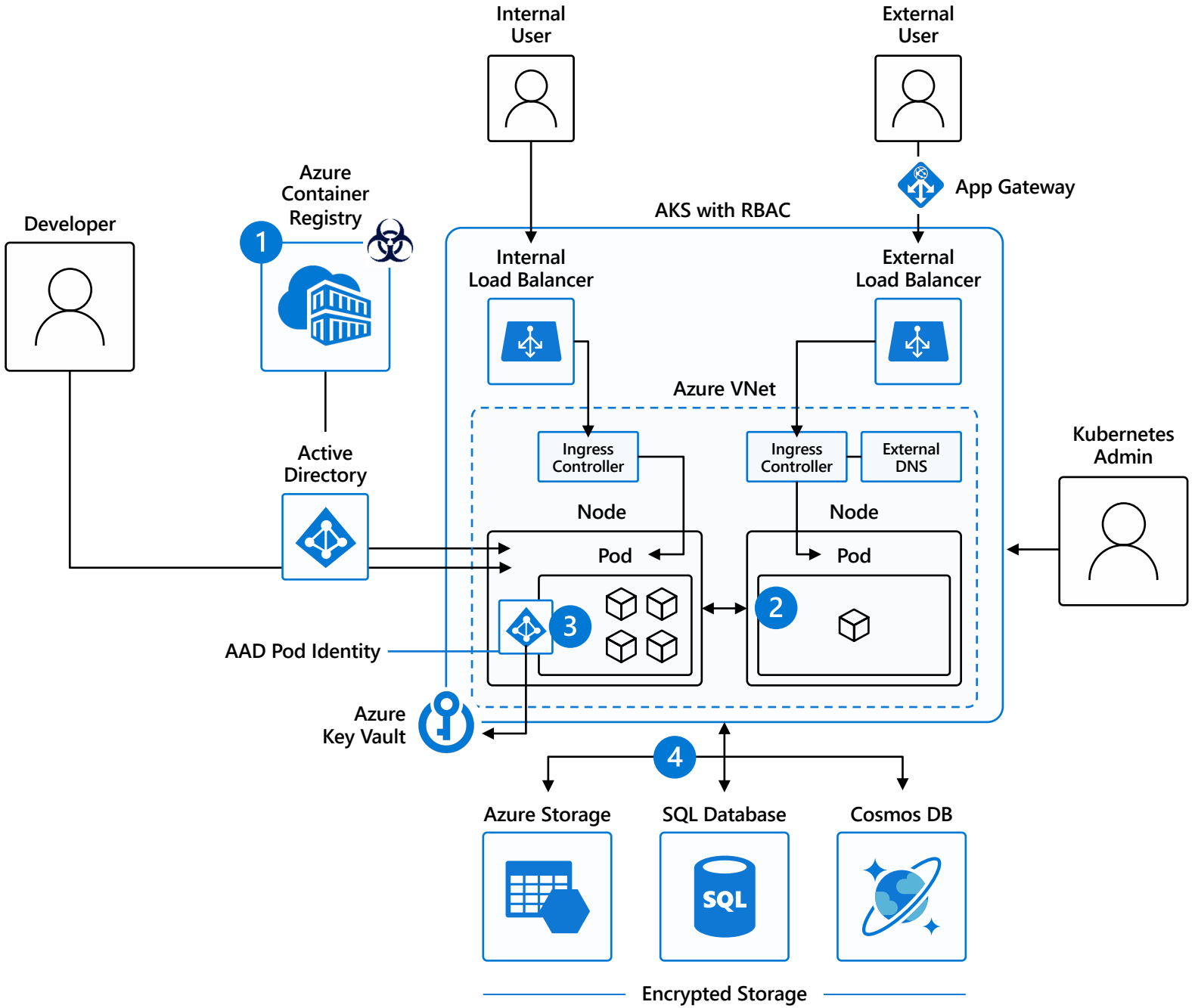
Security overview

1. **Image and container level security**
   - AAD 認證的容器註冊表訪問
   - 用於圖像驗證的 ACR 圖像掃描和內容信任

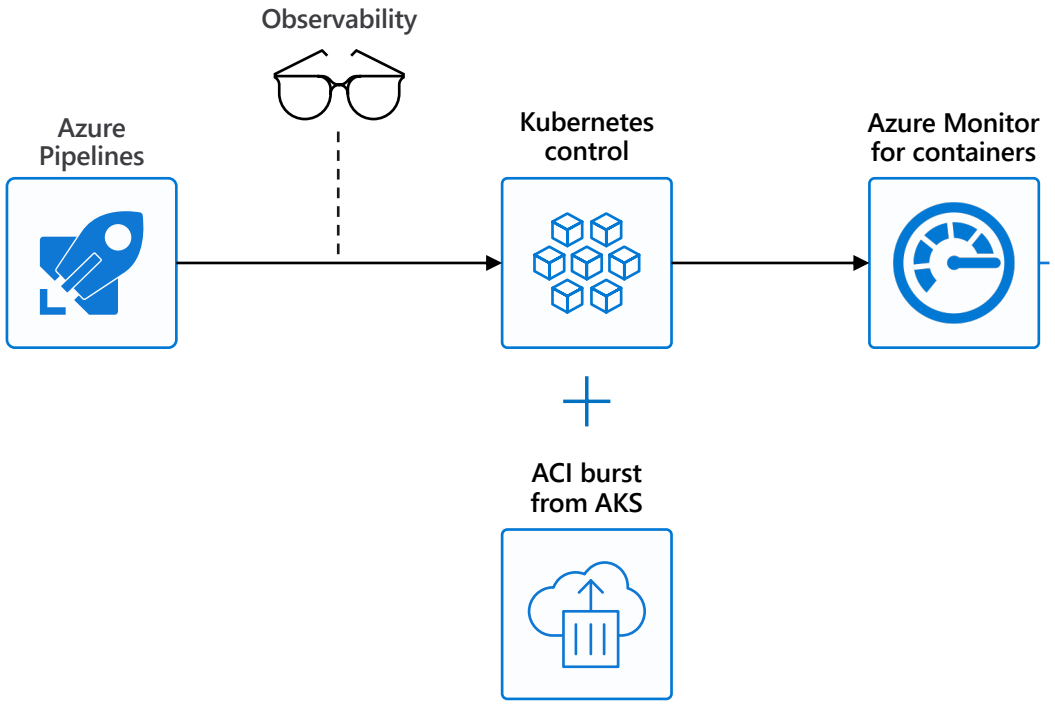
2. **Node and cluster level security**
   - 每晚自動安全修補
   - 部署在沒有公共地址的私有虛擬網絡子網中的節點
   - 保護命名空間（和節點）之間通信路徑的網絡策略
   - Pod 安全策略
   - 用於身份驗證的 K8s RBAC 和 AAD

3. **Pod level security**
   - 使用 AAD Pod Identity 控制 Pod 級別
   - Pod 安全上下文

4. **Workload level security**
   - Azure 基於角色的訪問控制 (RBAC) 和安全策略組
   - 通過 Pod Identity 安全訪問資源和服務（例如 Azure Key Vault）
   - 存儲加密
   - 帶有 WAF 的應用程序網關可防止威脅和入侵



Azure Monitor for containers



可視化

使用向下鑽取和過濾器可視化從集群到容器的整體運行狀況和性能

監測

通過多集群運行狀況匯總視圖提供見解

監控和分析

監控和分析 Kubernetes 和容器部署性能、事件、運行狀況和日誌

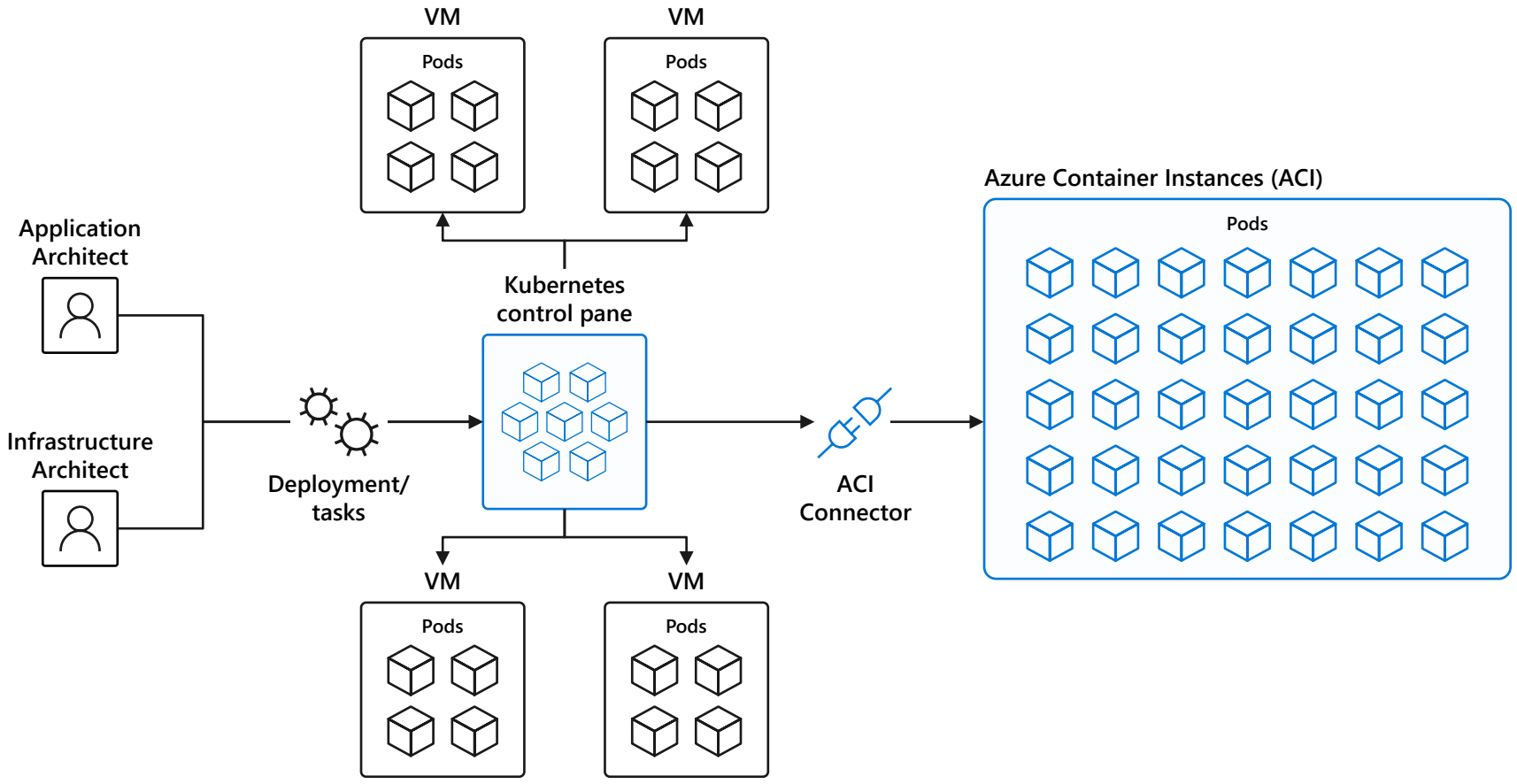
響應

與問題管理和 ITSM 工具集成的本機警報

可觀察性

觀察容器部署狀態的實時容器日誌

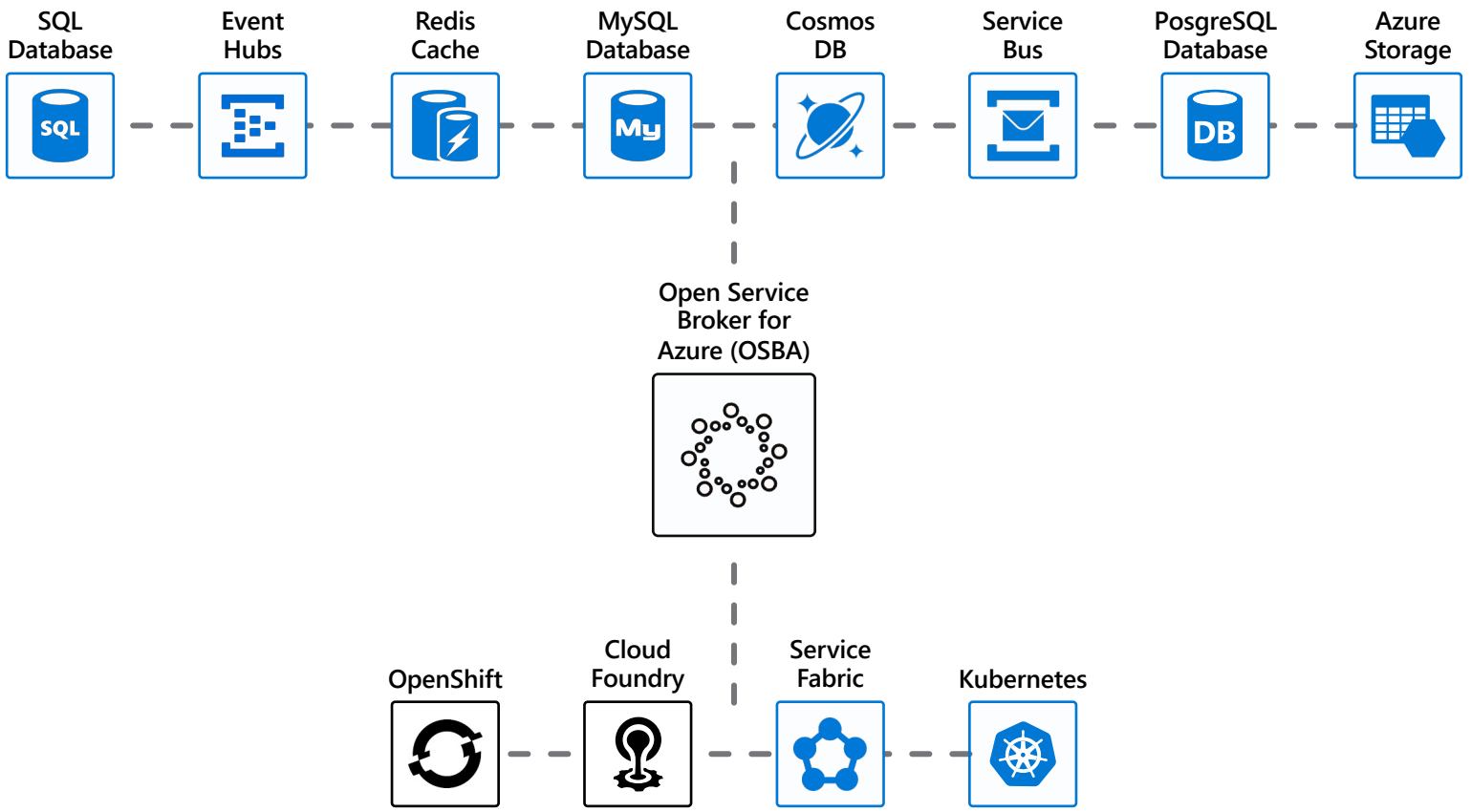
縮放


VM
VM
Pods
Pods
Application Architect
Infrastructure Architect
Kubernetes control pane
Deployment/ tasks
ACI Connector
Azure Container Instances (ACI)
Pods
VM
VM
Pods
Pods

Use Azure Managed Data Platform Services

Open Service Broker for Azure (OSBA)

Easily access to SLA-backed Azure Services such as Azure Database for MySQL



MS Learn Module 推薦

https://aka.ms/HKLearnAKS

Microsoft

Reactor

Thank You!

Q&A