



微軟for 大專院校 Serverless 規劃服務

包嵩豪 Gavin Pao.

Customer Success Account Manager

Microsoft Services / Microsoft CSU





微軟 Serverless 校園解決方案



Serverless Campus

三大服務面向

網路系統

計算機中心基礎維運



1. 軟、硬體設備購買與維護
2. 網路管理與校內資訊系統服務
3. 資訊安全管理 (防火牆、WAF...等)
4. 資訊系統備份/還原，身分驗證平台管理

行政教學

各單位支援與研究教授



1. 電腦教室應用 (雲端/虛擬桌面連線服務)
2. 提供HPC, Data and AI
3. 支援短期課程暨研習營

軟體應用

前瞻計畫



1. 人才培育 - FUTURE READY SKILLS
2. AI 體驗中心
3. 新學門/跨院所/通識領域之知識科技類課程

Computer Center 面對的難題 & 可能解決方案

- 自建系統但員工卻已經離職
- 難以使用的舊系統又更新不了
- 開發與系統管理脫鉤難以維護

網站、各系統
盤點至Azure
導入DevOp

1

- 遊走在安規邊緣的備份備援機制
- 全校大當機 不知該先修哪一機
- 來不及的還原

1.異地備援
2.災難還原與演
練
3.捨棄遠端機房

4

- 總是不夠分的GPU只好一直加購
- 永遠會過時的高階機種被迫重複投資
- 計畫型專案預算卻短暫的大量計算
- 不足的管理人力又要節省人力成本

1.計算資源類型
2.基礎硬體建設
3.移轉至Azure

2

3

雲端教室LabS
虛擬桌面WVD
服務至雲端

- 每年繳交高額保護費
- Citrix vs VMware (on Azure)
- 無法控制的系統版本更新與落差
- 硬體+授權+顯卡 = 鉅額投資

機房上雲的考量項目

On Premise

Compute & Licenses



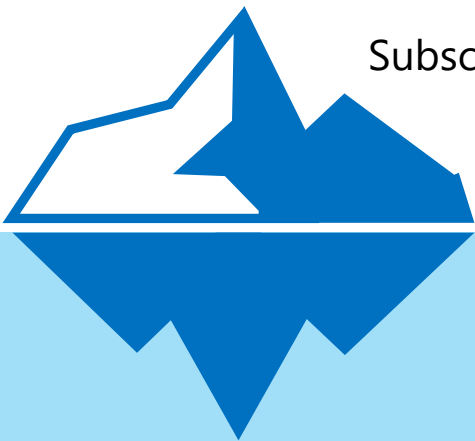
Compliance	- 法規
Security	- 資安
Risk over/under	- 風險
Insurance	- 保險
Training	- 培訓
IT Staff	- 人力

Consumables	
Software & License	- 授權
Maintenance (HW+SW)	- 維護
External contractors	- 外包

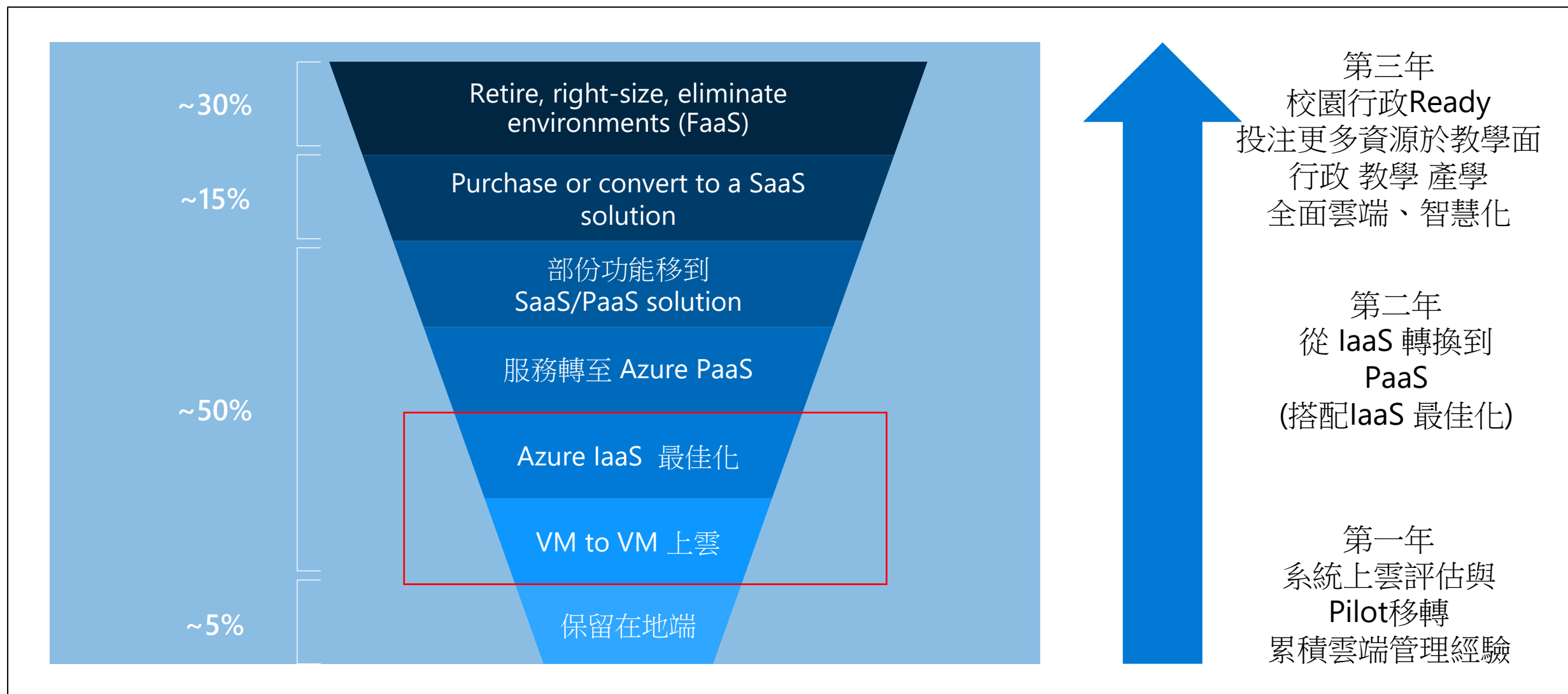
Cost of capex	- 資本支出
Cost of automation	- 自動化
Disaster Recovery	- 災害復原
Data center (space, electricity, cooling)	- 基礎建設

IaaS Computing

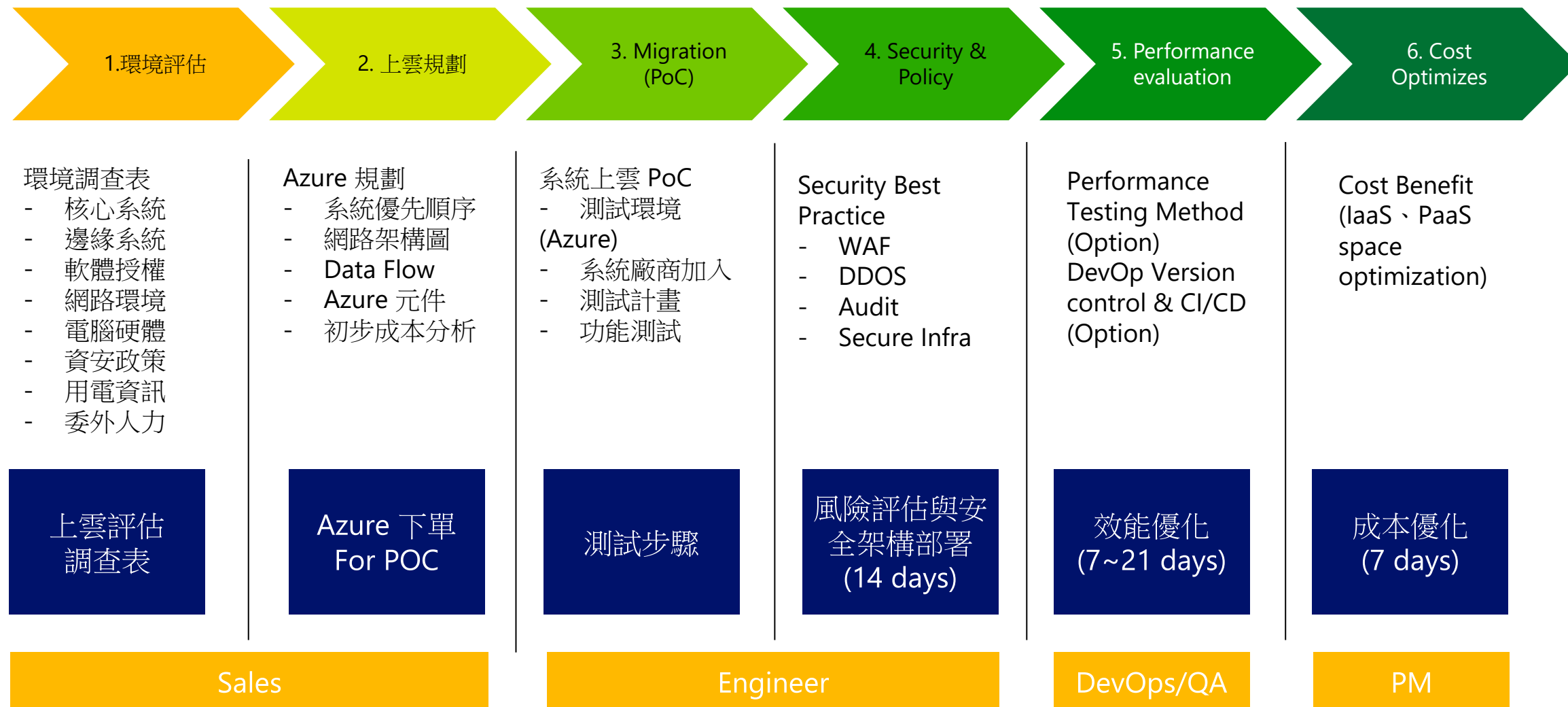
Subscription Fee



Serverless 服務上雲的考量及規劃順序



上雲服務評估步驟

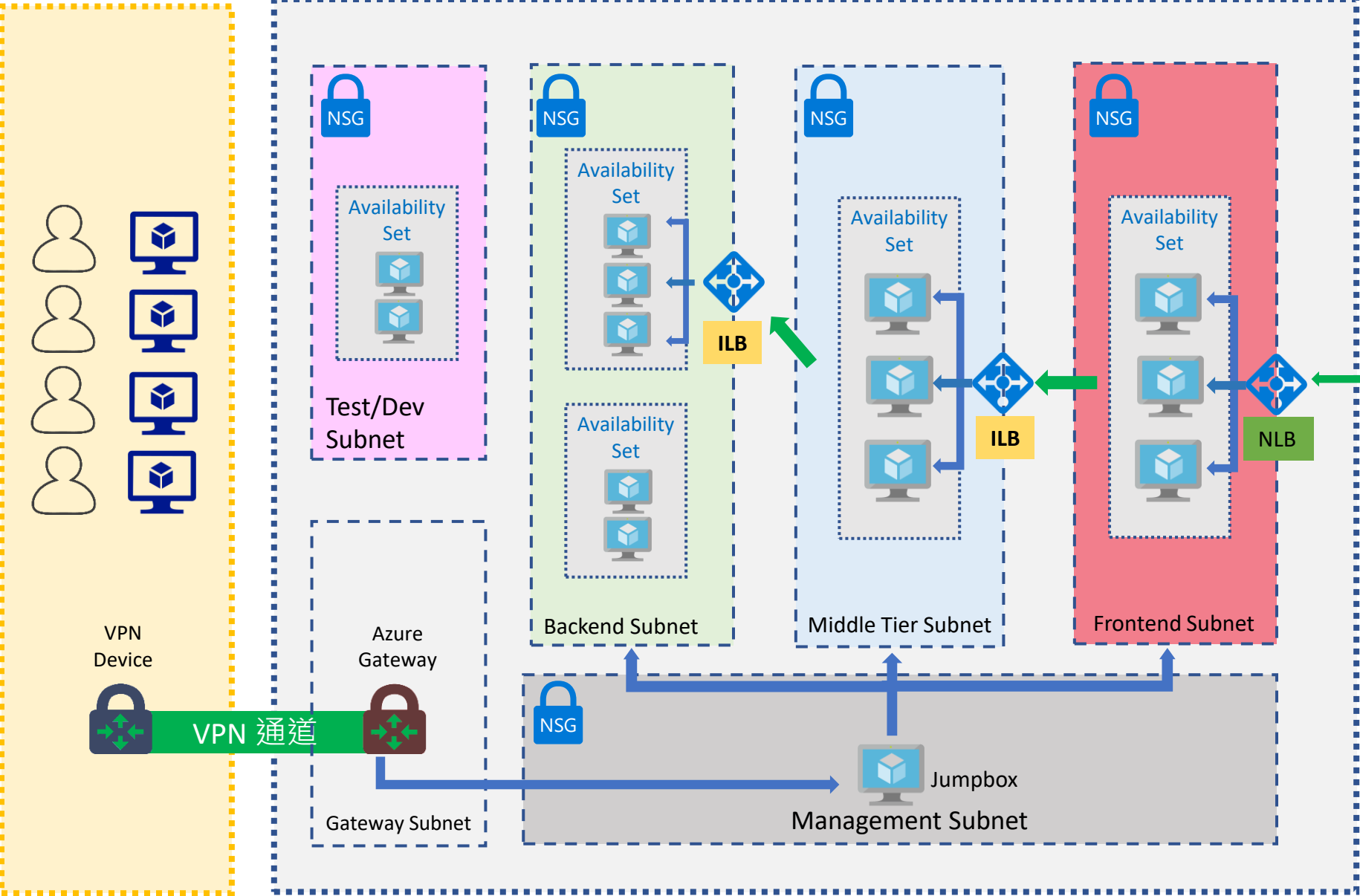


上雲評估項目建議

現有資訊環境上雲評估項目：

- 現有主要系統的 **Server / Storage** 規格及維護成本
- **Firewall** 對外流量 (各系統), **Firewall VPN** 廠牌
- 學校既有 **Windows Server / SQL Server (DB) License**
- 各應用系統對外網路需求
- 備份週期及備份量

建議未來學校的Azure IaaS 網路架構示意圖



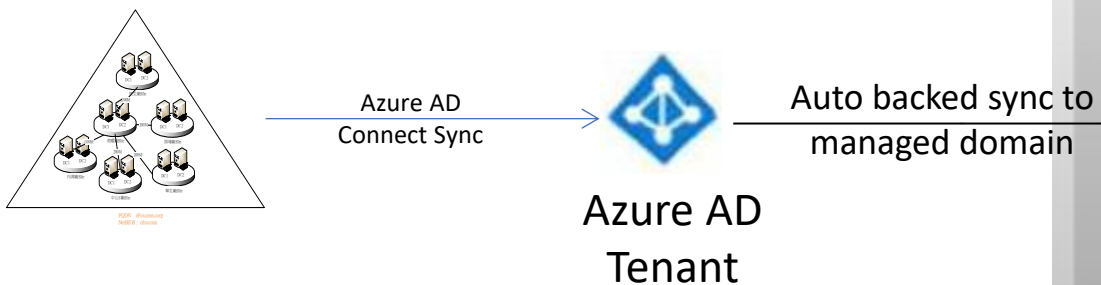
- 規劃透過 Jumpbox 管理其他 VM (引入PAW機制-安全終端機)
- 比照或優於地端的網路安全架構規劃，設定DMZ等各種應用子網段。
- 搭配客製化的 PowerShell，在各Subnet的VM建立後即套用對應的安全設定，確保各Subnet間的連線是在事先規劃的架構下運作，提高雲端網路架構的安全性。
- 為達到 Azure IaaS 集中管理的目的，可以考慮在 Backend Subnet 部署AADDs(Managed domain)，所有的IaaS VM都必須加入該AD集中進行管理 (比照地端的VM組態、安全管理標準)，並且為VM規劃另一個雲端AD帳號進行管理。(AADDs 使用者帳號可以來自AAD，以提供SSO的驗證需要，提升應用系統的SSO帳號安全性)

地端

Azure 虛擬網路

透過AAD DS 支援 RDS / WVD 的SSO應用架構

AAD DS (Managed Domain) 為學校提供一個由微軟提供維護又更加安全的AD服務，用來支援 RDS / WVD應用，提供一個與地端AD相同的使用者帳號資訊，但是卻是完全獨立、全新的雲端受管理的AD，更安全又不需要自行管理DC的高可用性AD雲端服務。





Service for Serverless 三年上雲計劃



Benefit after migration

Training

– 培訓

IT Staff

(Serverless skill ready)

Skill Up

– 人力

Cost of capex

– 資本支出

Cost of automation

- 自動化支出

Disaster Recovery

– 災害復原

Data center (space, electricity, cooling)

Cost Optimize

Compliance

– 法規

Security

– 資安

Risk over/under

– 風險

Insurance

– 保險

Risk transfer

Consumables

– 視需要調整用量

Software & License

– 授權

Maintenance (HW+SW)

– 維護

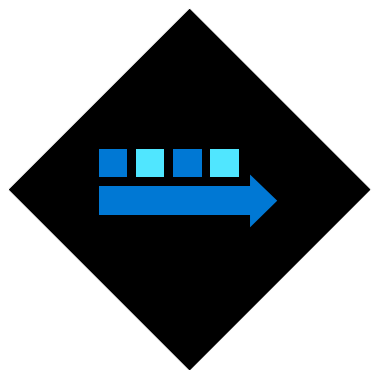
External contractors

– 外包

Scalable / Urgent resource

第一年: 系統上雲評估與Pilot移轉累積雲端管理經驗

進行應用系統 Migration，打造Serverless Campus 第一步



Azure Migrate



主要任務

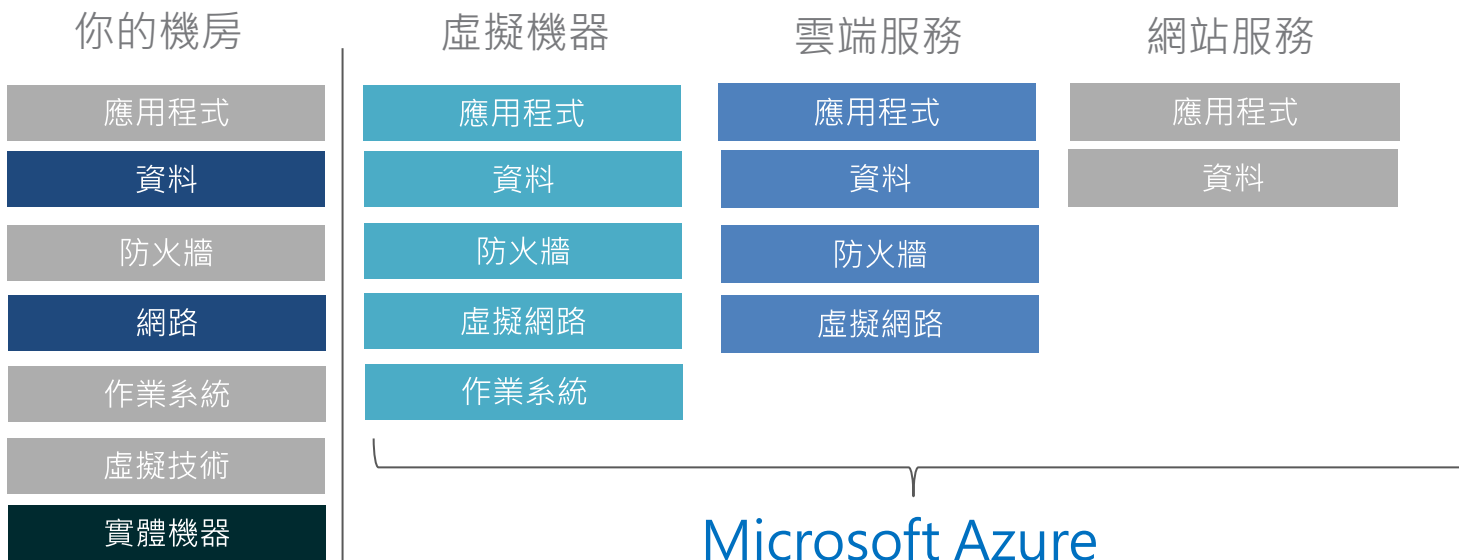
如學校首頁網站、網路課程系統整合CDN/WAF應用、Web應用移轉IaaS/PaaS Pilot驗證 與 雲端Infra 核心架構導入(Azure mini landing zone)



台灣微軟
微軟Partner

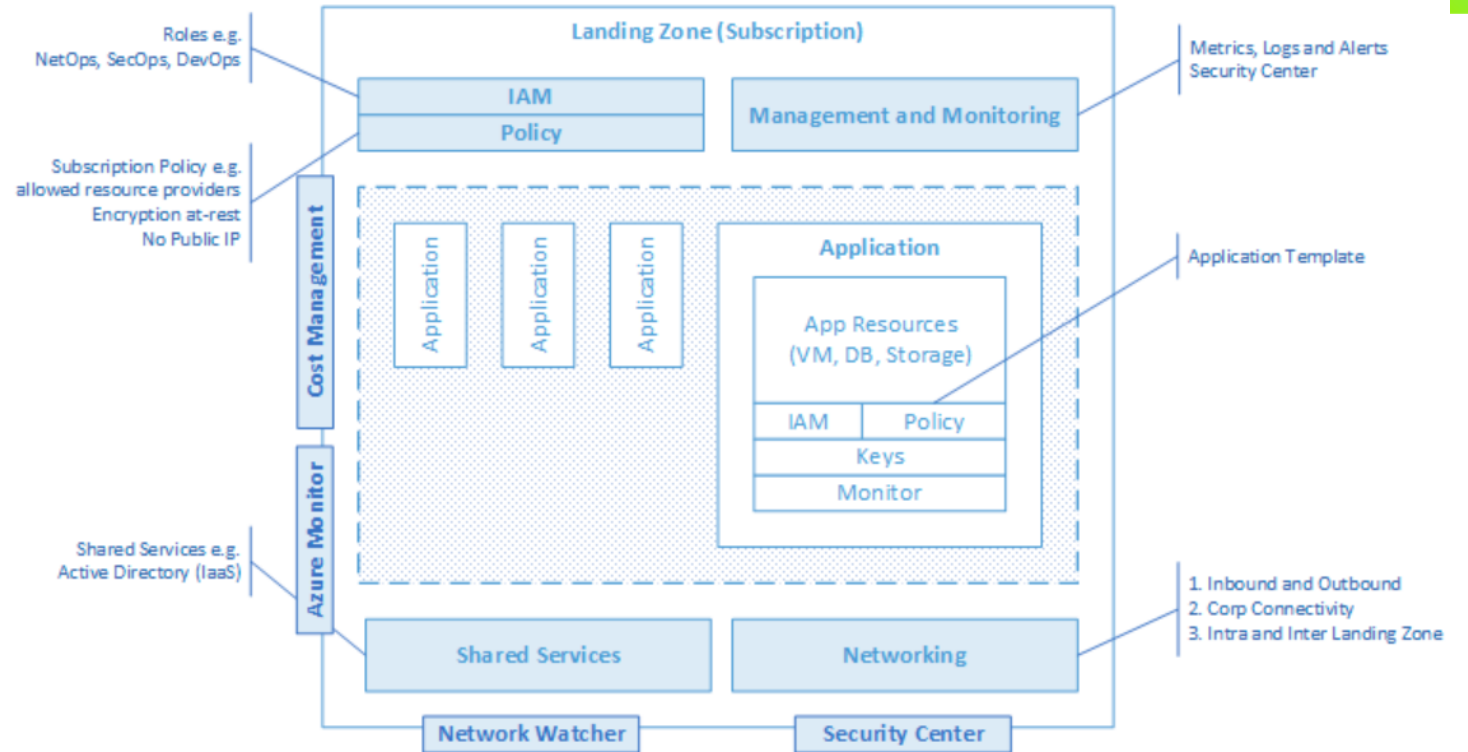
微軟專業團隊專家諮詢服務、雲端開發教育訓練
協助學校建置與雲端管理自動化機制導入、提升IT人員雲端管理技術

雲端費用	\$3,000,000
系統/調效/優化/改寫	\$4,000,000
整體維運服務	\$1,200,000



Landing Zones

The principle purpose of the “Landing Zone” is therefore to ensure that when an application landing on Azure, the required “plumbing” is already in place, providing greater agility and compliance with enterprise security and governance requirements.



重要規劃區域

 Subscription Organization & Governance	 Identity & Access Management	 Network	 BCDR
 Security	 Archetypes & Landing Zones	 Platform Monitoring & Management	 DevOps & Automation

Azure Mini-Landing Zone Workstreams

Azure Mini-Landing Zone contains multiple workstreams to deliver an enterprise grade, secure by design, Azure environment

Workstream



Archetypes & Landing Zones

Enable Customers on the journey to Azure, to plan, design and implement Azure to fit their requirements and needs.

Define and build the initial design to enable the foundation in Azure.



Identity Access & Management

Integrate between on-premises Active Directory Domain Services and Azure Active Directory. Design and implement premium Azure Active Directory capabilities: Conditional access and Multi-Factor Authentication.



Azure Security Insights

Secure Azure resources by activating Azure Security Center with security policy & compliance, resource security hygiene and threat protection capabilities.



Azure Administration & Governance

Guide IT teams to understand how to apply governance principles in your Azure environment with Enrollment and Subscription model, Identity and Access control (RBAC), Naming Convention, Azure Resource Management (Tags) and Azure Policy.



Azure Monitor & Management

Establish monitoring and management functionality using Azure Monitor, Alerts, and Log Analytics. Resources backup and ensure high availability with Azure Backup and Site Recovery Services. Accelerate cloud deployment align with DevOps practices.

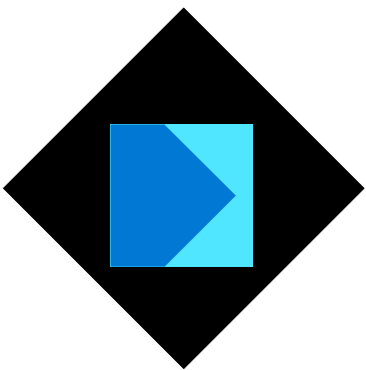
Outcome

Azure Mini-Landing Zone Workstreams & Timeline

Workstream		Capabilities	Duration
Archetypes & Landing Zones		Architecture Service: Azure Infrastructure	9 days
		Activate Hybrid Cloud	7 days
Identity Access & Management		Architectural Service - Azure Active Directory - Designing a Secure Cloud Identity	3 days
		Azure AD Conditional Access and MFA	5 days
Azure Security Insights		Azure Security Center Fundamentals	4 days
Azure Administration & Governance		Activate Azure with Administration and Governance	4 days
Azure Monitor & Management		Activate Azure Monitor	3 days
		Activate Azure with Recovery Services	4 days
		Activate Azure with Automated Deployments	2 days

第二年:從 IaaS 轉換到 PaaS (搭配IaaS 最佳化)

考量所有的應用系統在雲端應用架構的最佳整合方案



PaaS or IaaS+PaaS

雲端費用	\$3,600,000
系統/調效/優化/改寫	\$6,000,000
整體維運服務	\$1,000,000



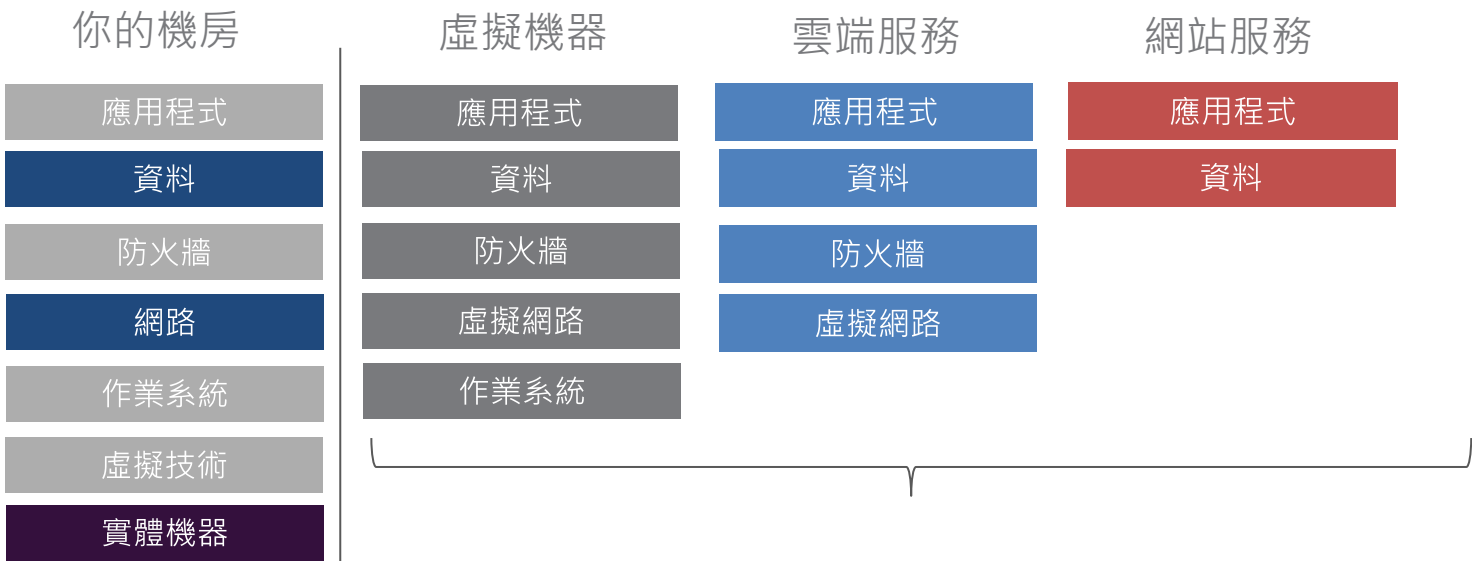
主要任務

檢視系統在Azure上架構及成本，評估效益並視情況協助學校評估調整架構轉為 純PaaS服務 或 IaaS+ PaaS服務



台灣微軟
微軟Partner

微軟專業團隊專家協助評估現有架構，並協助調整、移轉PaaS架構導入DevOps開發教育訓練，提升資訊人員雲端架構的技術與管理能力



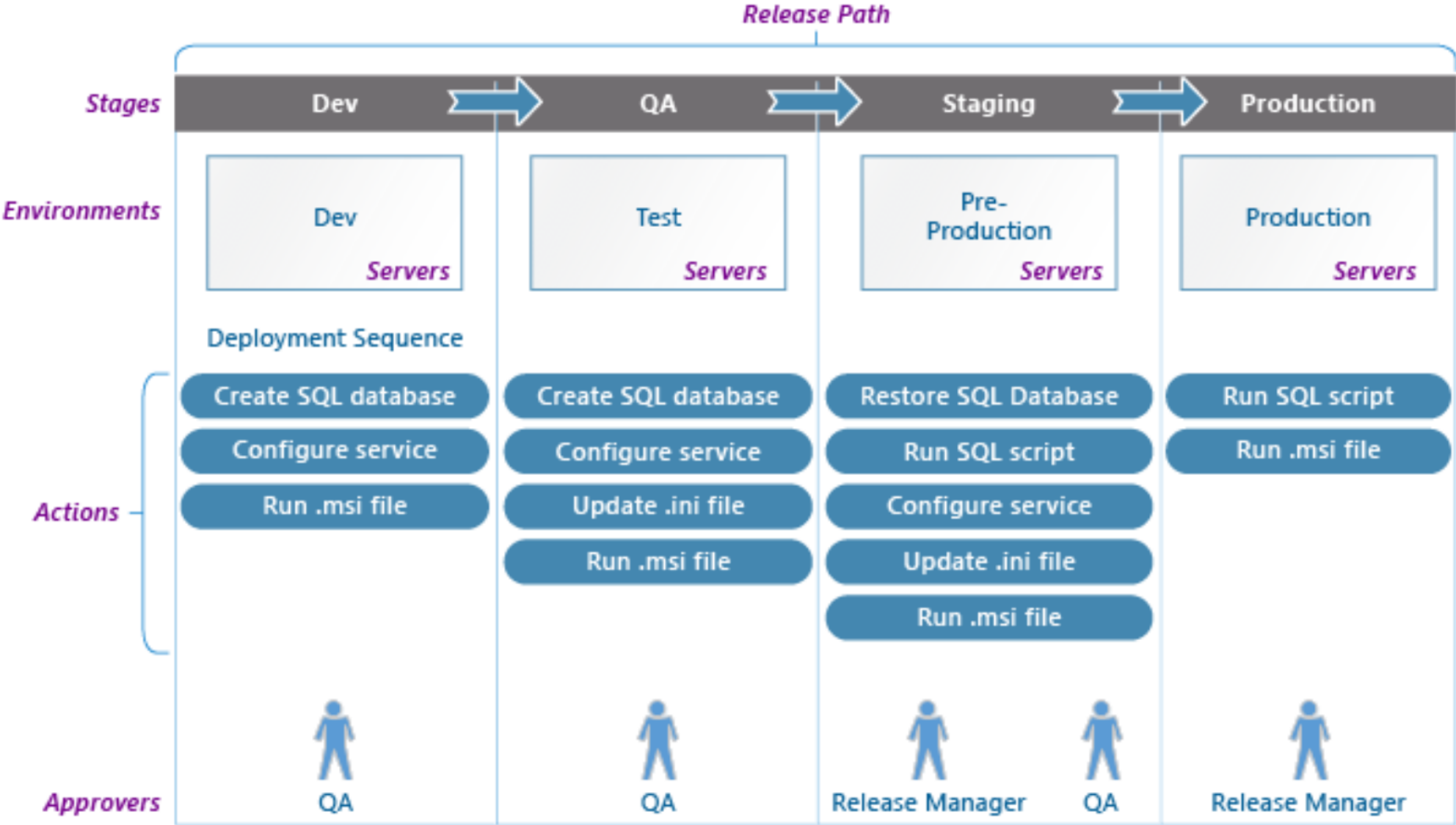
Azure DevOps 之自動部署與發行管理導入支援服務

服務項目	服務內容	預估時程	備註
軟體生命週期(ALM)之自動部署與發行管理導入支援服務 ----- Goal: 高效率的應用系統開發平台 Value: 彈性支援企業資訊應用需求	Azure DevOps Server 軟體生命週期(ALM)之自動部署與發行管理導入支援服務 此服務執行內容根據以下需求規劃如下: 1.需求：整合既有的Git至新建的Azure DevOps Server 服務提供與時數天數預估: A.建置 Azure DevOps Server Update 1.1 以上版本 (2 Web , SQL Cluster- DB , 1 Backup) (4 Day) B. 建置步驟流程撰寫 (1 Day) C. 協助將現有的Git整合到 Azure DevOps Update 1.1 (1 Day) D.將現有的Git整合Azure DevOps Server 過程截圖撰寫。(1 Day) 2.需求：透過 Azure DevOps Server 進行版控與自動部署ASP.Net網站標準程序 服務提供與時數天數預估: A.到場協助 Azure DevOps Server 發行管理功能安裝與設定。(1 Day) B.Release management 安裝與設定手冊(1 day) C.以Azure DevOps Server 發行管理平台協助實作以下作業：(3 Days, 以下作業將以一個 ASP.Net網站為例) 發行階段規劃 部署流程設計 與 Azure DevOps Server 2019 Azure Pipelines (Team Build、CI / CD) 整合 發行簽核與驗證 D.整理此次Pilot ASP.Net 網站應用系統發行管理階段規劃、部署 SOP、發行簽核與驗證程序(4 day)	預估至少16天 On-site Service	

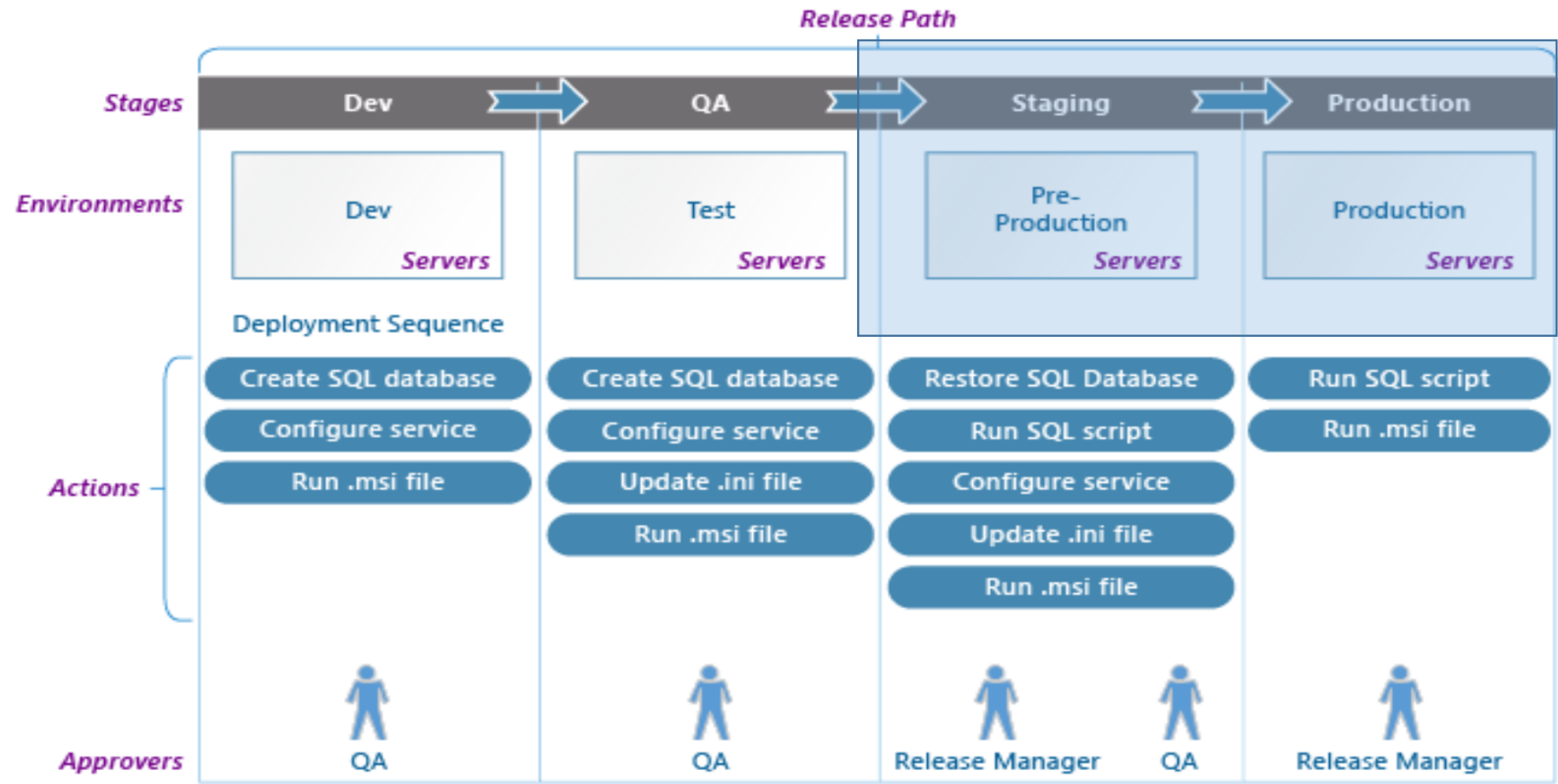
Azure DevOps之自動部署與發行管理導入支援服務

服務項目	服務內容	預估時程	備註
軟體生命週期(ALM)之自動部署與發行管理導入支援服務 ----- Goal: 高效率的應用系統開發平台 Value: 彈性支援企業資訊應用需求	3.需求 :希望進行.Net版本控制(Default is Git) 並 針對此次Pilot ASP.Net 網站應用系統發行管理驗證過程進行教育訓練 服務提供與天數預估: A.到場提供Azure DevOps管理 與 Git 教育訓練 (4 Days, 包含Hands-On Lab) --上課 – 1Day (Git 4hr ~ 5 hr , DevOp系統管理 1~2 hr) --準備 – 1Day (Slide與Demo 環境準備) B.到場提供Azure DevOps管理 與 Git 教育訓練 (包含 Hand's on Lab 版本) (3 day) --上課 – 1Day (Git 6hr ~ 8 hr , DevOp系統管理 1~2 hr) --準備 – 2 Day (Slide 、 LAB 與Demo 環境準備) C.到場提供 CI / CD (Azure Pipelines) 教育訓練: (2 Days, 包含Hands-On Lab) --上課 – 1Day --準備 – 1 Day (Slide與Demo 環境準備) ----- 課程大綱 (1 Day, 2場) Session 1: Azure DevOps Server Build (9:00AM~12:00PM) 持續整合基礎介紹 Agent 介紹 Agent 與 Azure DevOps 底層運作 Agent Queue Agent Pool 持續整合與設定 (ASP.NET Web Application 或是 ASP.NET Core 為主) Session 2 : Azure DevOps Server Release (1:30PM~5:00PM) 持續部署基礎介紹 Release Management Flow Release Approvals Phase & Task Deployment Group Deployment Pool 持續部署與設定 (IIS 站台為主)	預估至少11天 On-site Service	

Software Release Management Best Practices (Sample)



此服務將著重的階段：Version control & Release to Production phase



為何需要自動部署與發行管理機制

- 使得網站上線程序更加可預測和可靠 (Predictable and Reliable)

傳統的手動人工部署來進行發行管理是很辛苦的，除了程式本身可能的問題，其他還可能包含組態檔案、Script 版本、權限相關等等的常見風險都時常出現在日常上線發行管理過程。透過導入正式的發行管理機制，可消除並降低手動部署相關風險與節省許多手動開銷。此案將導入 **Azure DevOp Server**，可以進行網站上線部署自動化程序設計，並進行既有上線程序的驗證整合，從而使網站的發行管理更加可預測和可靠。

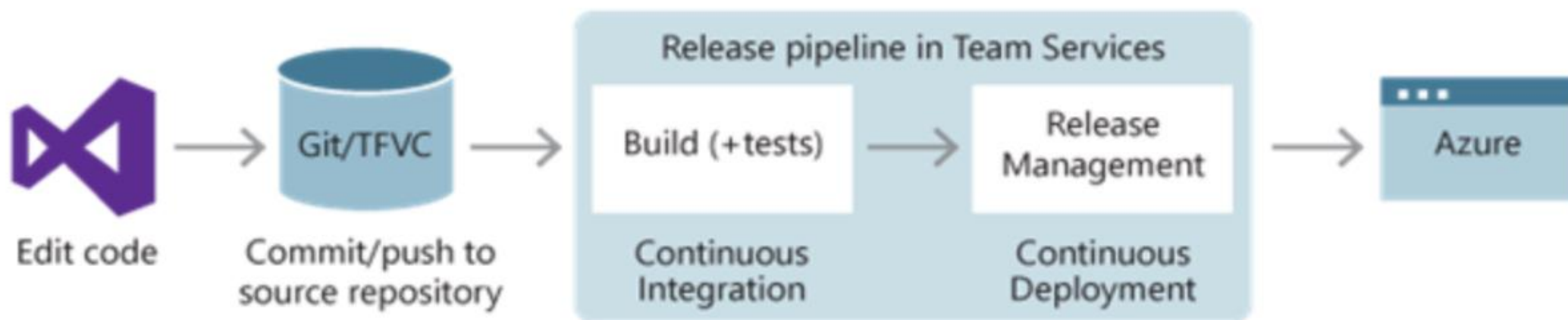
- 落實網站組態管理

考慮一下要部署ASP.NET網站的過程中，可能需要在web.config文件（連接字符串等）中具有特定於環境的應用程序進行設置。因此每次進行發行版本時，這些組態需求都需要進行更改。過去，當我們透過發佈路徑進行網站推播部署時，都要手動進行此類配置更改，因此提高了上線組態管理的人為風險。此案將導入 **Azure DevOp Server (Azure Pipelines)**自動部署機制，將可降低這類的風險，並且可以在網站發佈時，通過參數化配置值來滿足網站組態管理需要。

- 將專注於更重要的事情

發行管理機制將允許每個功能專注於重要的工作，即開發人員可以編寫代碼，測試分析師可以執行和編寫自動化測試計劃。**Azure DevOp Server (Azure Pipelines)** 發行管理機制，將為開發團隊提供近乎即時的循環測試回饋，如果該變更已經破壞了某些重要的內容，則可以設置通知相關開發人員，並且讓測試分析師可以在正式發佈網站功能變更之前發現錯誤。

可與微軟的Azure 應用整合 (IaaS / PaaS) 做為內、外部開發應用管理平台



人員更專注於教學資源，整合行政 教學 產學，朝向全面雲端、智慧化，全面轉型、成就學生

人員更專注於教學資源，整合行政 教學 產學，朝向全面雲端、智慧化，全面轉型、成就學生



行政全面雲端平台化，專注於教學資源，全面導入雲端實驗室、提供研究人員HPC資源、AI工具等，學校評鑑加分

微軟專業團隊專家顧問 24x7 持續支援雲端服務管理
 微軟教育團隊全力協助學校導入最新技術以及教學開發
 微軟Partner 成為最主要的後盾、持續協助學校轉型

移轉所有行政服務於此

你的機房	虛擬機器	雲端服務	網站服務
應用程式	應用程式	應用程式	應用程式
資料	資料	資料	資料
防火牆	防火牆	防火牆	
網路	虛擬網路	虛擬網路	
作業系統	作業系統		
虛擬技術			
實體機器			

Microsoft Azure

Microsoft Azure



客戶成功案例



快速實現雲: 學院只花六個月就實現 IT 轉型

Products and Services

[Azure](#)
[Azure Active Directory](#)
[Azure SQL Database](#)
[Azure Virtual Machines](#)
[FastTrack for Azure](#)
[FastTrack for Office 365](#)
[Power BI](#)
[SQL Server](#)

Industry

[Higher Education](#)

Organization Size

[Medium \(50 - 999 employees\)](#)

Country

[United States](#)



LeFaive 和他的團隊決定開始探索雲端的解決方案,他們將 Web Server 遷移到 Azure。然後發生了一些意想不到的事情。LeFaive 指出:「最初將伺服器移動到 Azure 只是一個方便的選擇。但是,當團隊看到轉換的易用性以及雲端可用的功能時,他們開始勇於嘗試。從這一點開始,事情進展得非常快。」

借助 Azure, SJVC 可以快速將現有軟體和工作負載移動到雲中,同時探索其他功能。該學院使用各種雲服務,包括 Azure 虛擬機器、Azure SQL 資料庫和 Azure AD。為了進行報告, SJVC 還在 Azure 虛擬機器上運行 SQL Server 資料庫,並使用 Microsoft Power BI 來可視化數據。IT 團隊也開始使用最新的平臺即服務 (PaaS) 產品。LeFaive 說:「最初,我們的策略是簡單地將本地環境『提升並轉移』到 Azure。但我們意識到,我們並沒有充分利用 Azure 的潛力,我的目標是擁有一個無伺服器計算環境。將來,我非常興奮地看到我的開發人員將如何使用 Azure 服務結構和 Azure 函數。」

通過最大化 **Azure** 服務 將更多時間轉為專注於學生

Products and Services

[Azure Active Directory](#)

[Azure App Service](#)

[Azure Backup](#)

[Azure Cloud Services](#)

[Azure DevOps](#)

[Azure Site Recovery](#)

[Office 365](#)

Industry

[Higher Education](#)

Organization Size

[Corporate \(10,000+ employees\)](#)

Country

[United States](#)



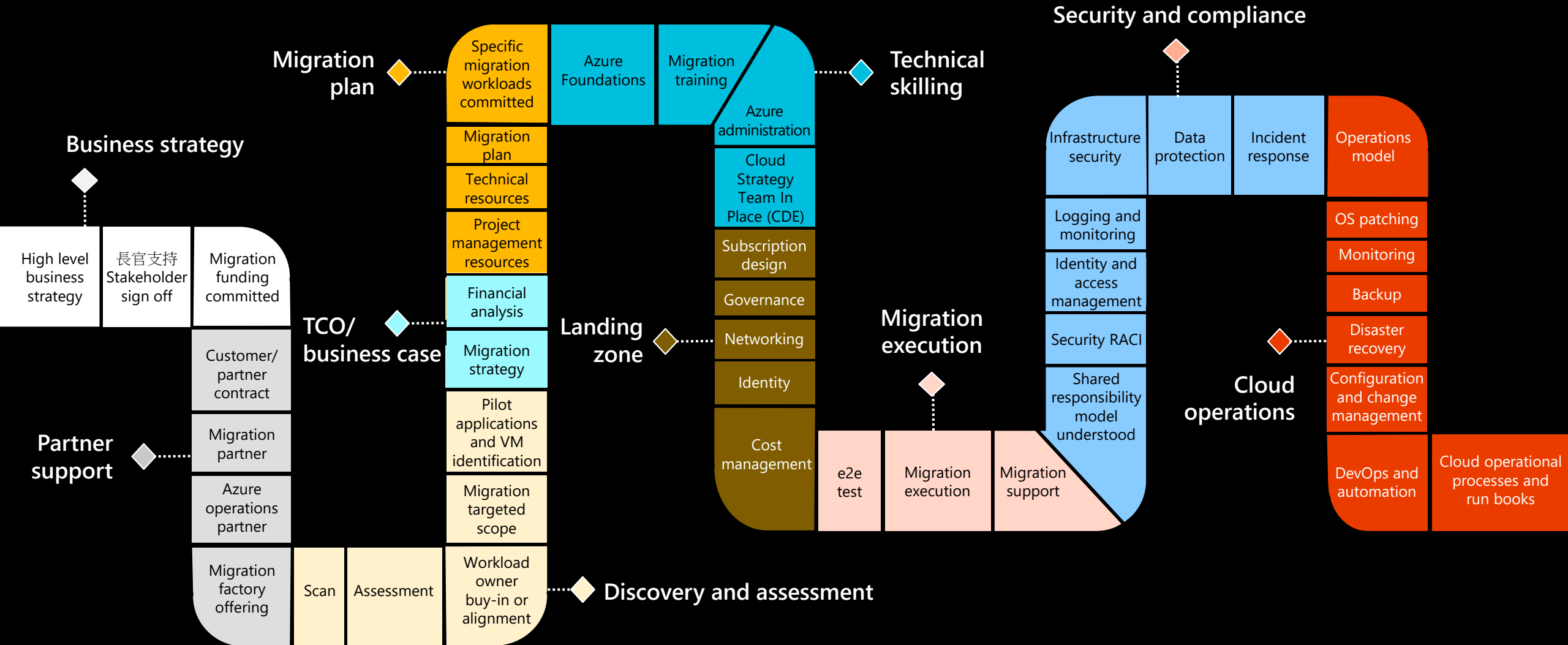
SAN DIEGO STATE
UNIVERSITY

「隨著我們從本地雲轉向公有雲,我們花費更少的時間操作存儲備份和計算基礎架構,並花更多的時間專注於更重要的業務需求。」

Tom Voss

IT Operations Manager
San Diego State University

No migration is ever linear or simple....



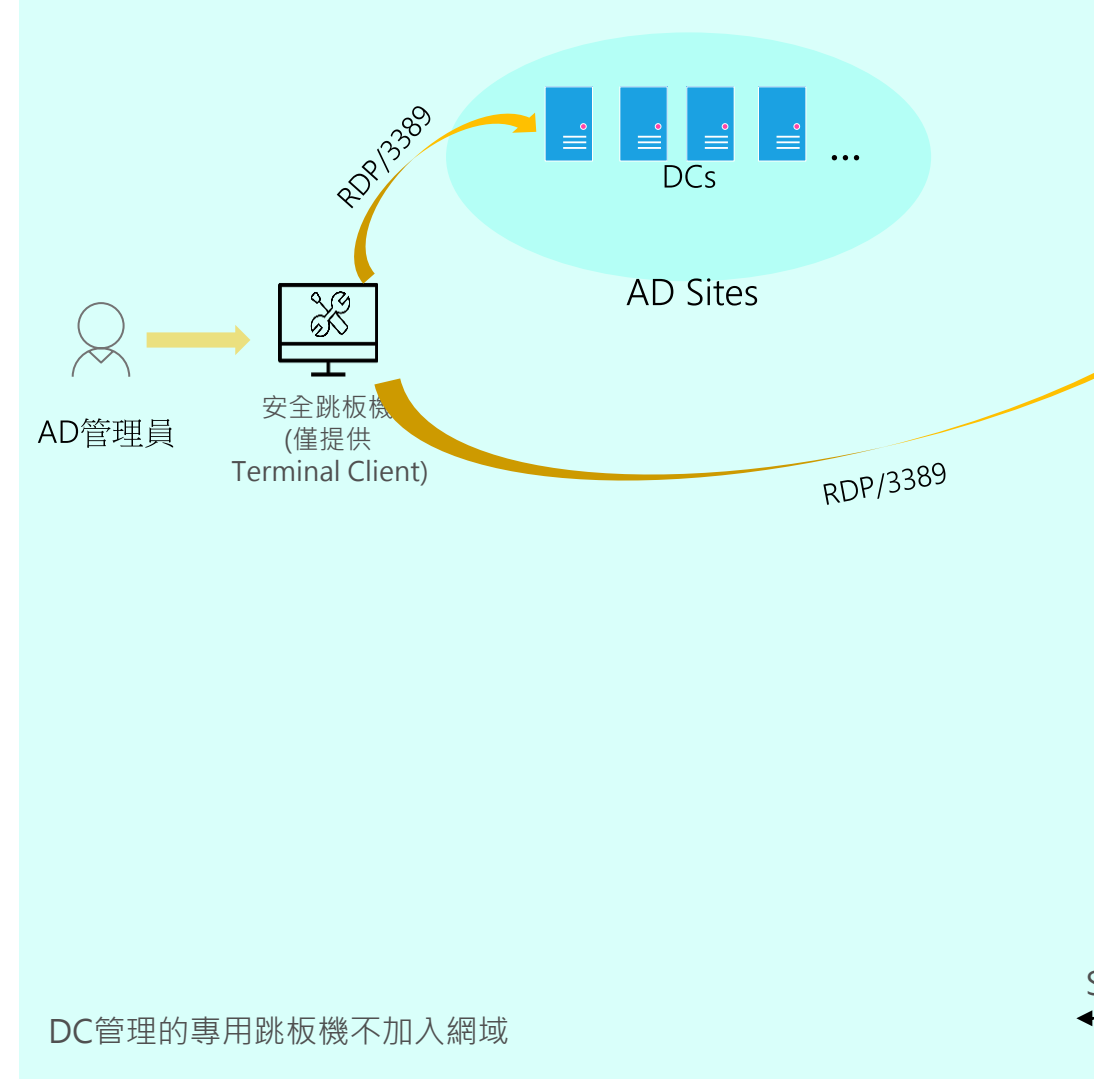


Azure IaaS 安全跳板機 (PAW)解決方案 補充資訊

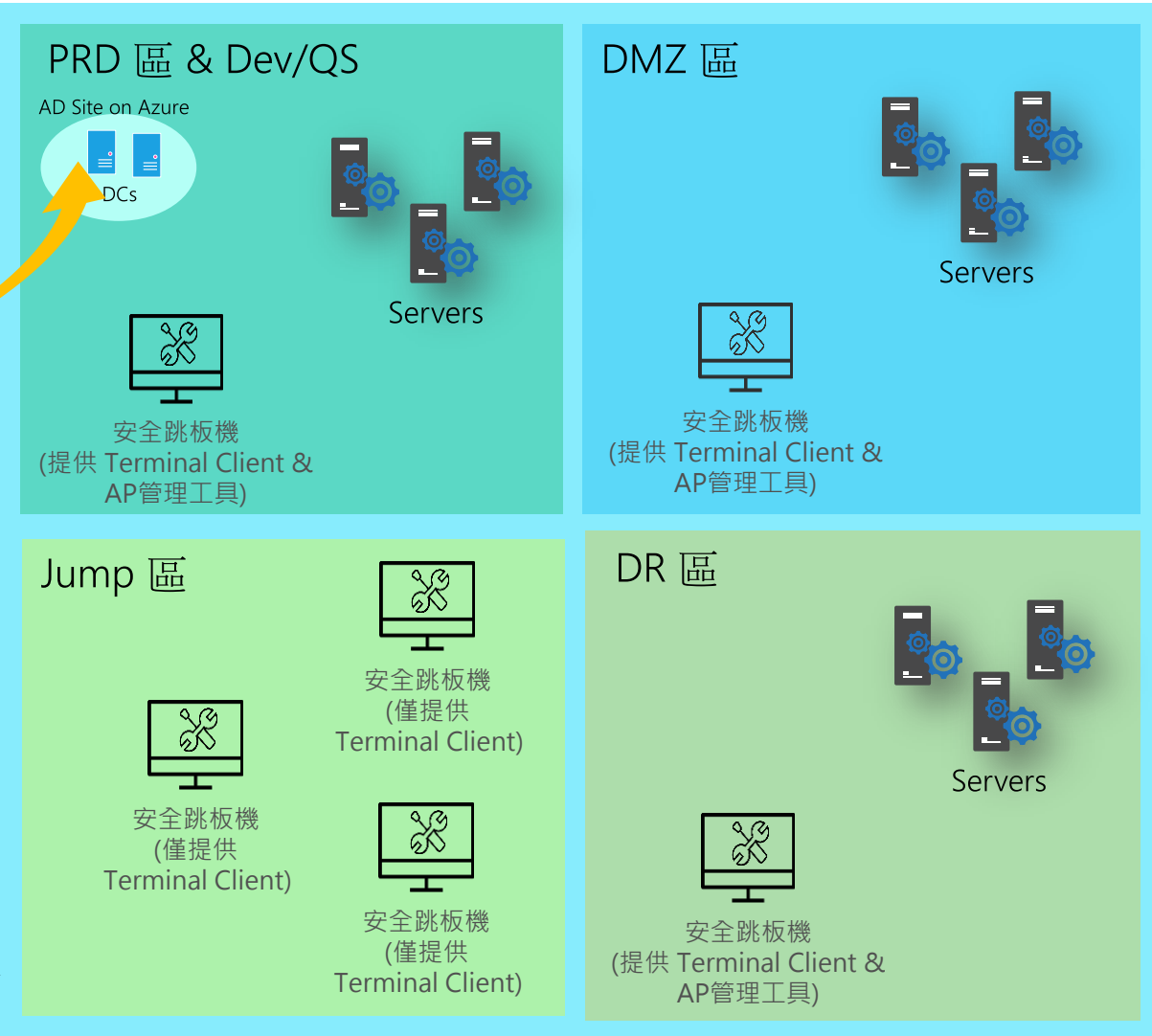


跳板機架構規劃示意圖 (For DC管理)

地端環境



Azure IaaS環境



跳板機架構規劃示意圖 (For Azure 的AP Server 管理)

地端環境

地端AP管理員需要管理 Azure上的PRD & Dev/QS區的 AP Server情境

1. AP管理員從桌機(或地端指定裝置)透過RDP遠端桌面服務登入 Jump 區 for PRD & Dev/QS區專用的安全跳板機 (可以限定特定網域群組，甚至鎖定來源裝置IP)
2. 再從Jump區 for PRD & Dev/QS區專用的安全跳板機，透過RDP遠端桌面服務登入PRD & Dev/QS區的專用的安全跳板機(with AP管理工具，並透過APP Locker機制限定特定管理工具可以執行，其它未開放的程式或工具則不允許執行，並且並且已鎖定來自 Hub區 for PRD & Dev/QS區專用的安全跳板機IP (可以限定特定網域群組能登入此跳板機)
3. AP管理員原則上只能透過管理工具進行AP Server的管理 (如透過SSMS管理SQL Server)
4. 建議透過限定特定網域群組，如Server管理員或臨時除錯需要的AP管理員群組成員能登入相關AP Server進行管理)



AP管理員for PRD / Dev/QS

RDP/3389

S2SVPN

Azure IaaS環境

PRD & Dev/QS區

AD Site on Azure

DCs

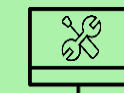
Server Admin
with RDP/3389

AP Admin
with Mgm Tools

Servers

安全跳板機
(提供 Terminal Client &
AP管理工具)

Jump 區



安全跳板機
(僅提供
Terminal Client)

安全跳板機
(僅提供
Terminal Client)

安全跳板機
(僅提供
Terminal Client)

DMZ 區



Servers



安全跳板機
(提供 Terminal Client &
AP管理工具)

DR 區



Servers



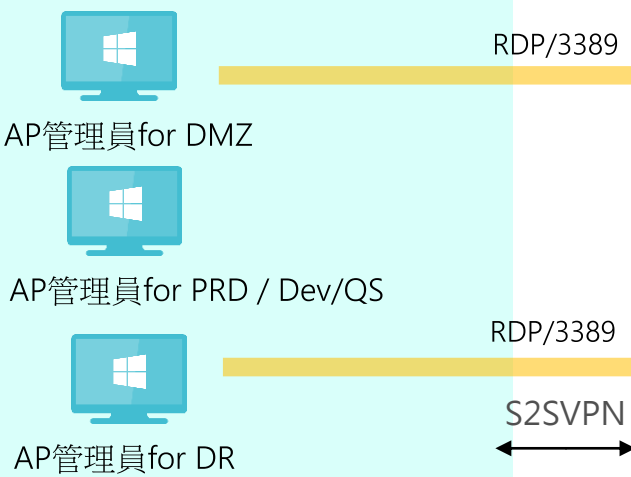
安全跳板機
(提供 Terminal Client &
AP管理工具)

跳板機架構規劃示意圖 (For Azure 的AP Server 管理)

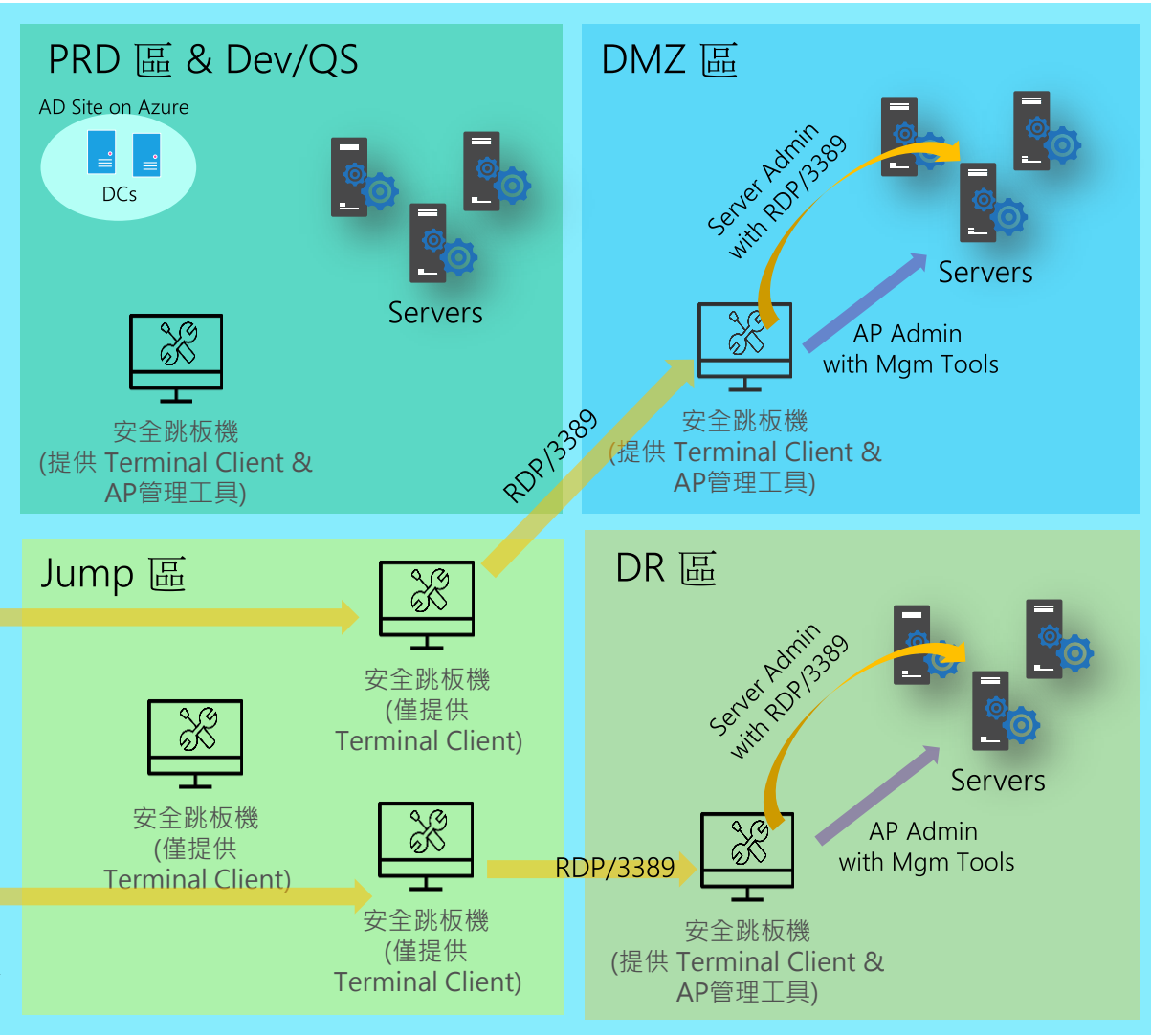
地端環境

地端AP管理員需要管理 Azure上的DMZ 或 DR 區的 AP Server情境

比照 for PRD & Dev/QS區的情境，DMZ 或 DR區都在HUB區有專用的安全跳板機，並且在 DMZ或 DR區 也配置了專屬的安全跳板機 with 相關AP管理工具。建議透過個別限定特定網域群組，進行相關RDP登入權限的設計，達成安全的AP與AP Server管理作業權限的委派效果。



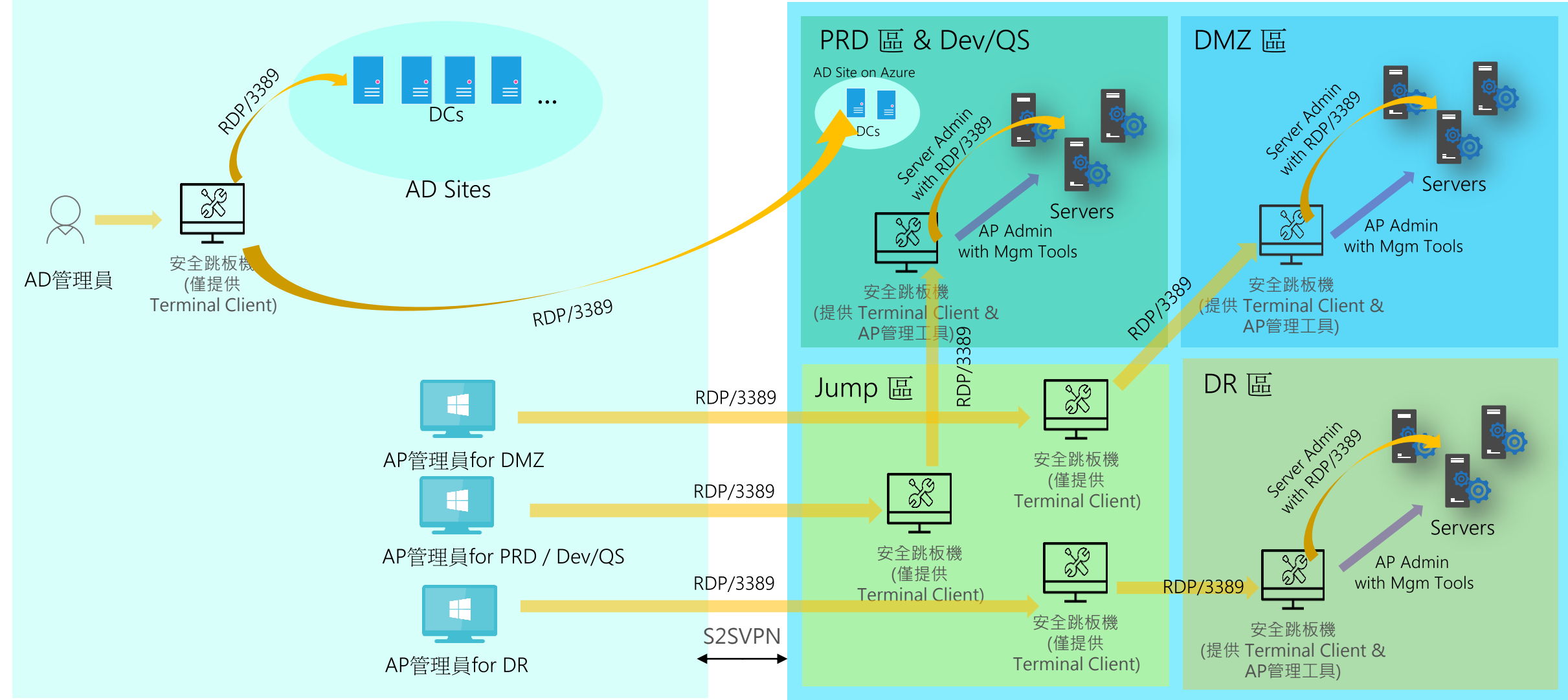
Azure IaaS環境



跳板機架構規劃示意圖 (Overview)

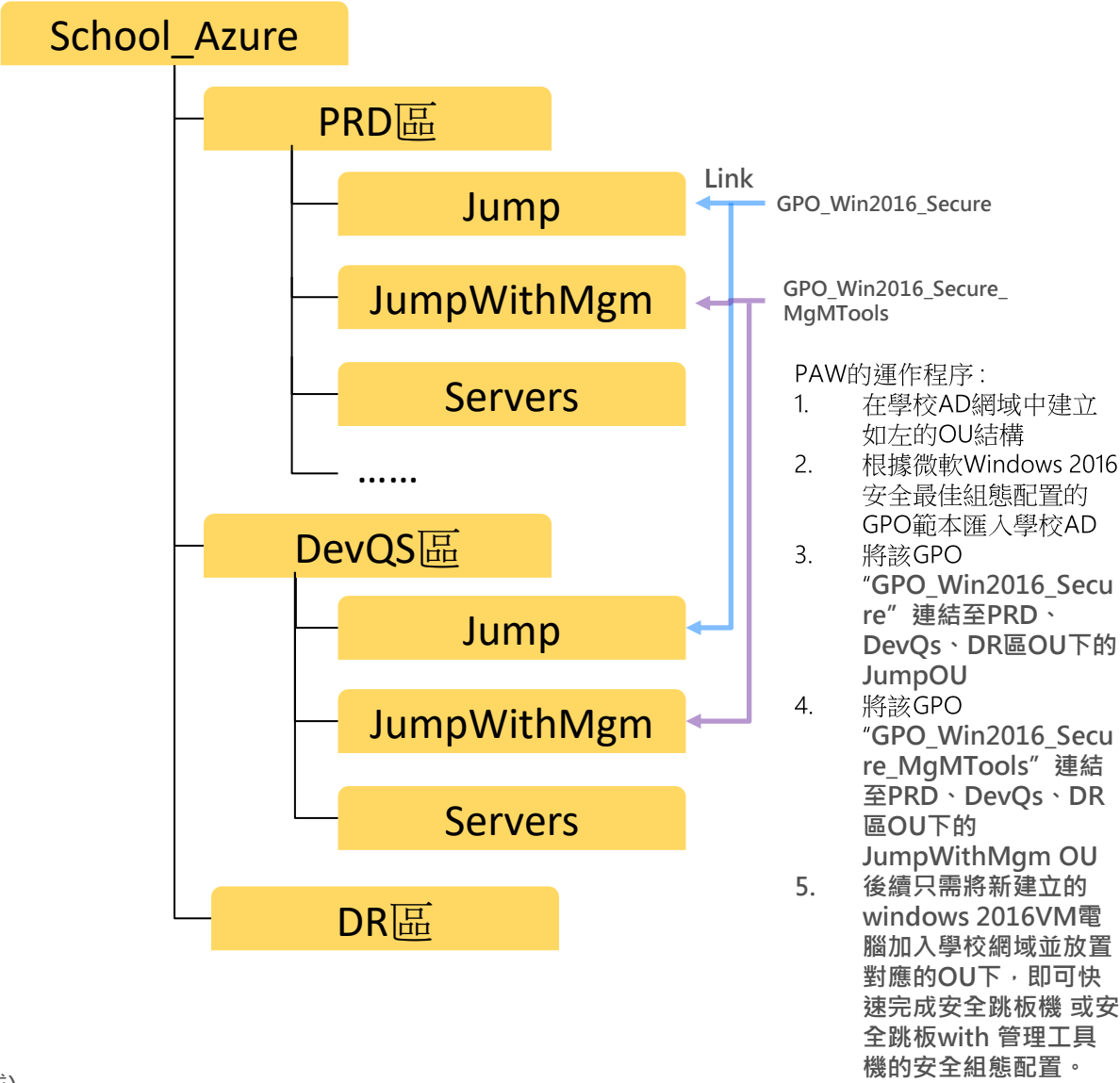
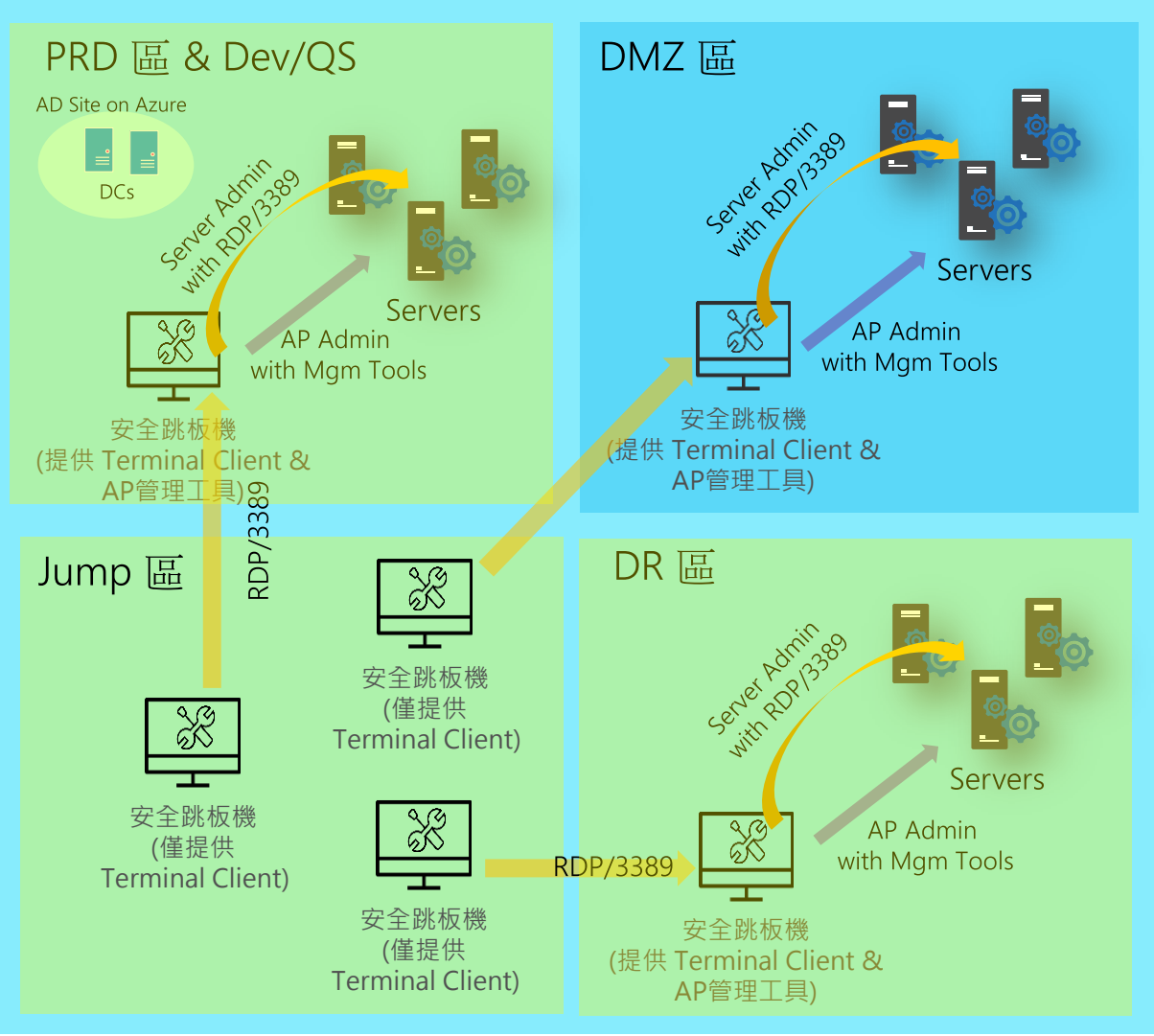
地端環境

Azure IaaS環境



PAW OU邏輯架構規劃for 跳板機管理 on Azure 示意圖

Azure IaaS環境



Azure的跳板機都會加入學校網域 (DMZ區的 AP管理工具安全跳板機應該加入DMZ網域)

A scenic photograph of a sunset over a mountain range. The sun is a bright, glowing orb on the right side of the frame, partially obscured by a long, horizontal band of dark, textured clouds. Sunbeams radiate from the sun, fanning out across the sky. The mountains in the foreground are dark and silhouetted against the warm, golden light of the setting sun. The sky transitions from a deep blue at the top to a warm orange and yellow near the horizon.

It's Time !!

Start Planning with Microsoft Azure for Serverless solution