Microsoft Azure 雲的萬物論研討會

IT 轉型的反重力浪潮

掌握 Azure IaaS 精髓 並開始您的雲端旅程

曹祖聖

台灣微軟資深講師

jimycao@syset.com

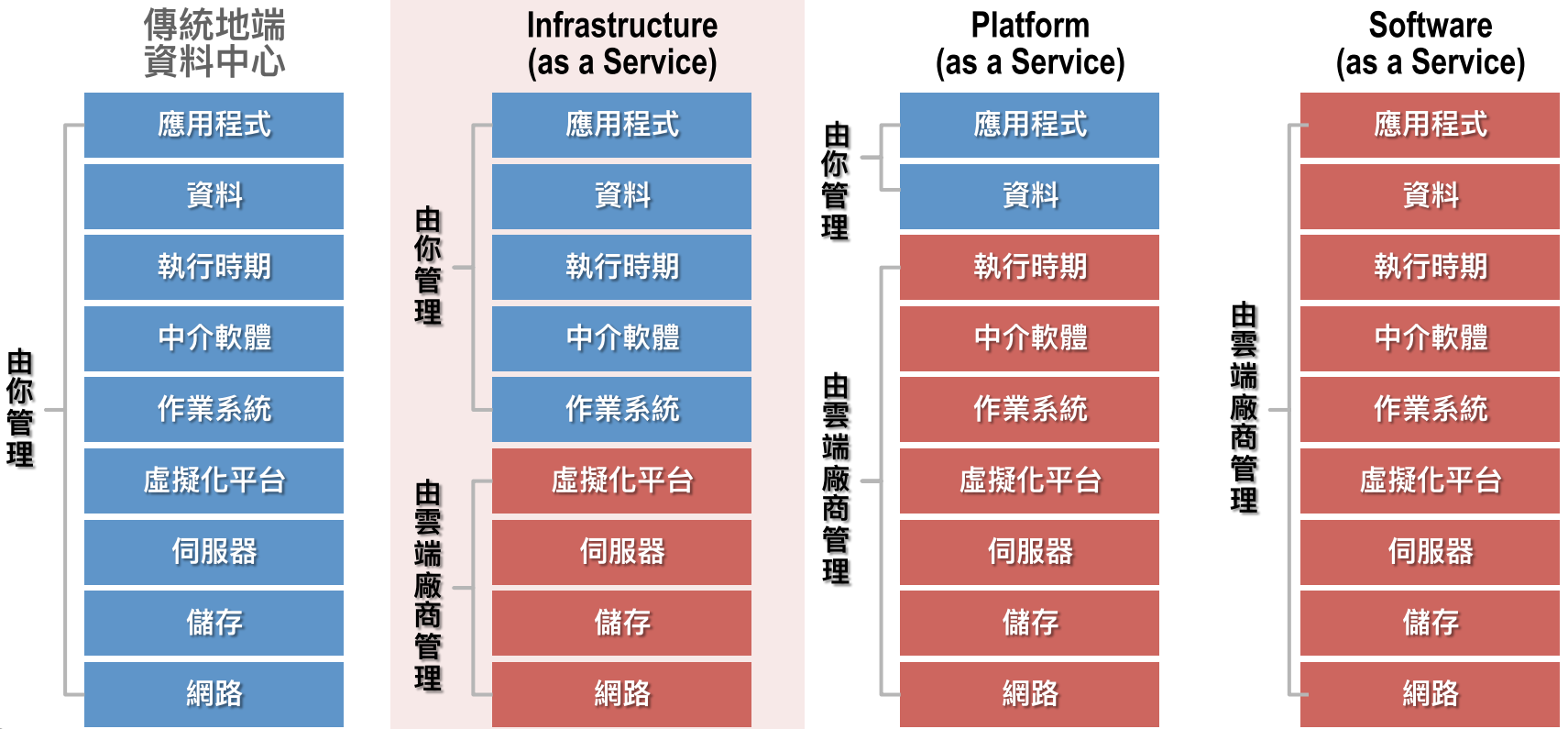
http://teacher.syset.com

MCP, MCP+I, MCSA, MCSE, MCDBA, MCAD, MCSD, MCTS, MCITP, MCPD, MCT, MVP

大綱

1. Azure IaaS 概觀
2. Azure IaaS 核心服務
   - → Azure 運算 – 虛擬機器
   - → Azure 儲存體
   - → Azure 網路
   - → Azure 管理與安全
   - → 移轉地端系統到 Azure IaaS – Azure Migrate

Azure 雲端服務模型



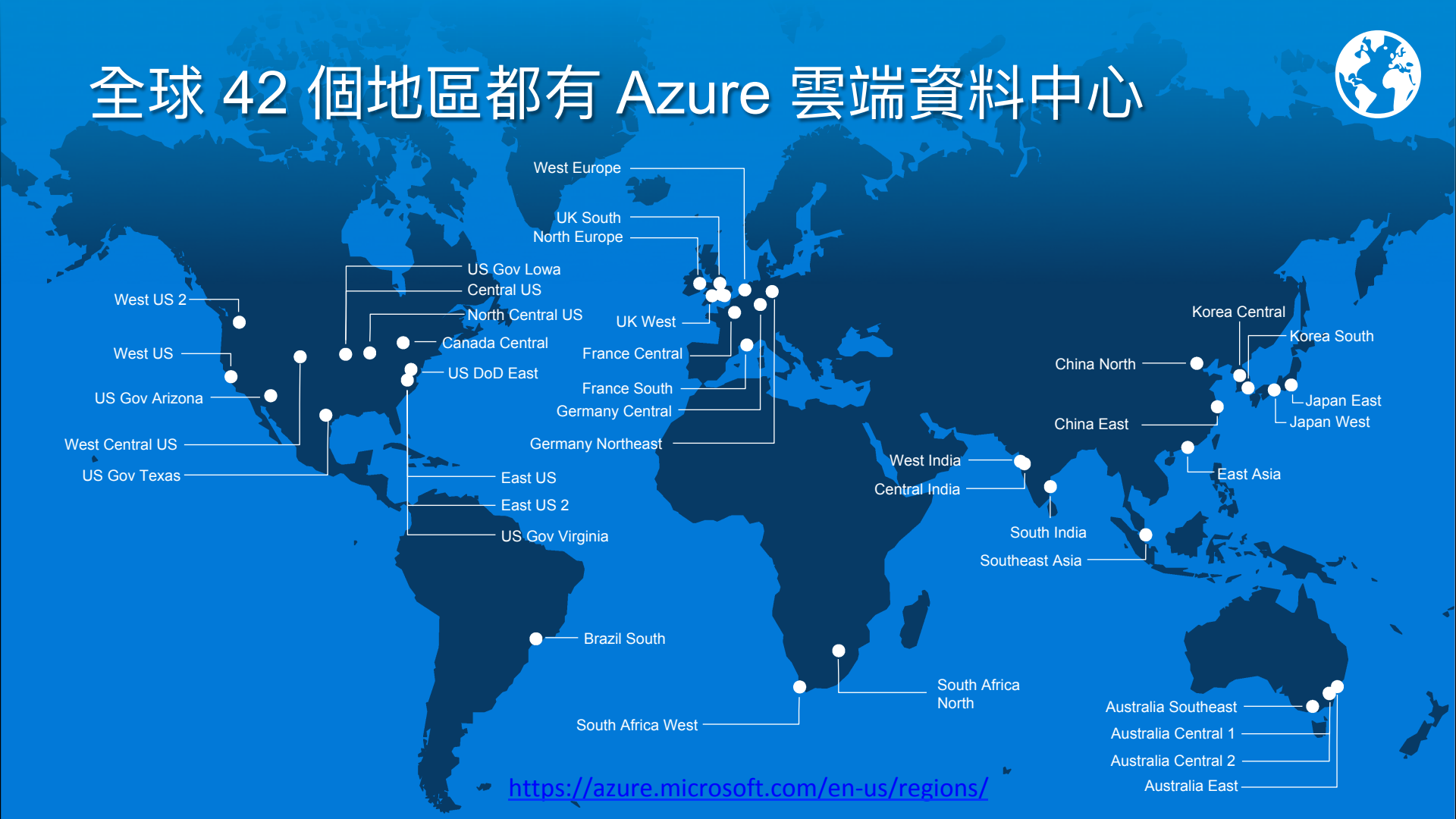
Azure IaaS 的特點

全球化

值得信任

混合與開放

全球 42 個地區都有 Azure 雲端資料中心



https://azure.microsoft.com/en-us/regions/

Azure 通過多項業界標準規範

GLOBAL

- ISO 27001
- ISO 27018
- ISO 27017
- ISO 22301
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CSA STAR Self-Assessment
- CSA STAR Certification
- CSA STAR Attestation

US GOV

- Moderate JAB P-ATO
- High JAB P-ATO
- DoD DISA SRG Level 2
- DoD DISA SRG Level 4
- SP 800-171
- FIPS 140-2
- Section 508 VPAT
- ITAR
- CJIS
- IRS 1075

INDUSTRY

- PCI DSS Level 1
- CDSA
- MPAA
- FACT UK
- Shared Assessments
- FISC Japan
- HIPAA / HITECH Act
- HITRUST
- GxP 21 CFR Part 11
- MARS-E
- IG Toolkit UK
- FERPA
- GLBA
- FFIEC

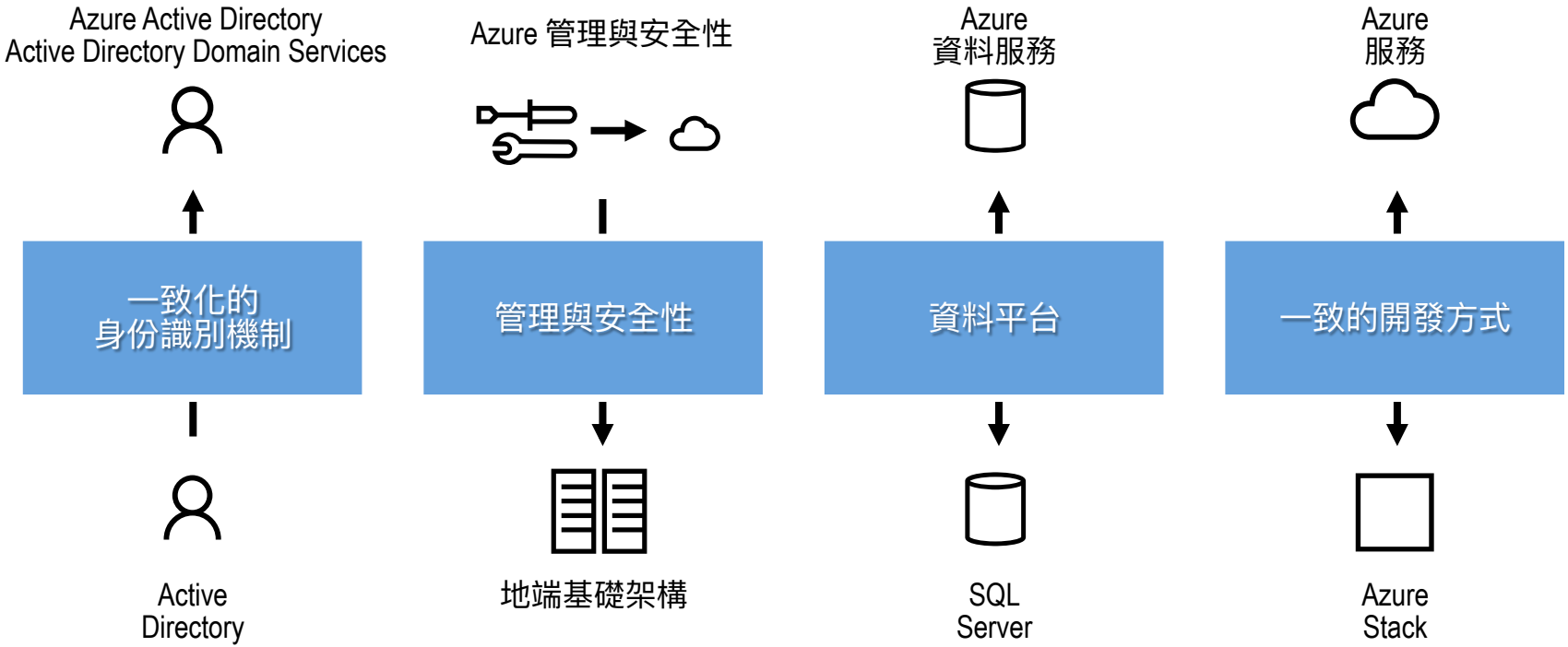
REGIONAL

- Argentina PDPA
- EU Model Clauses
- UK G-Cloud
- China DJCP
- China GB 18030
- China TRUCS
- Singapore MTCS
- Australia IRAP/CCSL
- New Zealand GCIO
- Japan My Number Act
- ENISA IAF
- Japan CS Mark Gold
- Spain ENS
- Spain DPA
- India MeitY
- Canada Privacy Laws
- Privacy Shield
- Germany IT Grundschutz workbook

技術選項多、部署有彈性

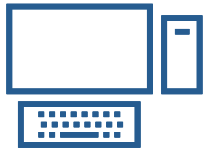
DevOps	Nagios	VAGRANT		GRUNT				Xamarin		
管理	CHEF	puppet labs	ANSIBLE	SALTSTACK			mist.io	libcloud		SCALR CLOUD MANAGEMENT
應用程式		Joomla!	Drupal		APPRENDA					
應用程式 平台與工具	php	nodeJS		JS	Ruby	IJ	eclipse			
資料庫與 中介軟體		redis	CLEARDB	cloudera	MySQL	mongoDB.		Couchbase		
基礎架構			redhat	SUSE		bitnami	ORACLE LINUX	FreeBSD	docker	

一致性的身份識別、應用程式、資料與管理



IaaS 核心服務

Azure IaaS 的核心服務



計算

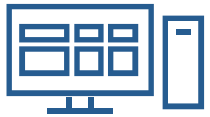
虛擬機器
可用性設定組
虛擬機器擴展集

儲存

磁碟
Blob 儲存
檔案
Azure File、Azure File Sync

網路

虛擬網路、VPN、
ExpressRoute、負載平衡器、
DNS、Traffic Manager



安全與管理

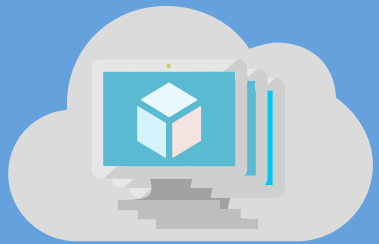
記錄檔分析、備份、
站台復原、安全中心

[redacted]

虛擬機器、虛擬機器擴展集

虛擬機器

使用現有的虛擬化技術、最小化學習曲線
可以執行絕大部份的 Windows 或 Linux 工作負載
移轉到雲端最簡單的一種選擇
彈性的機器規格選擇 – 選擇最適合工作負載的 VM 規格
進階的網路與儲存能力

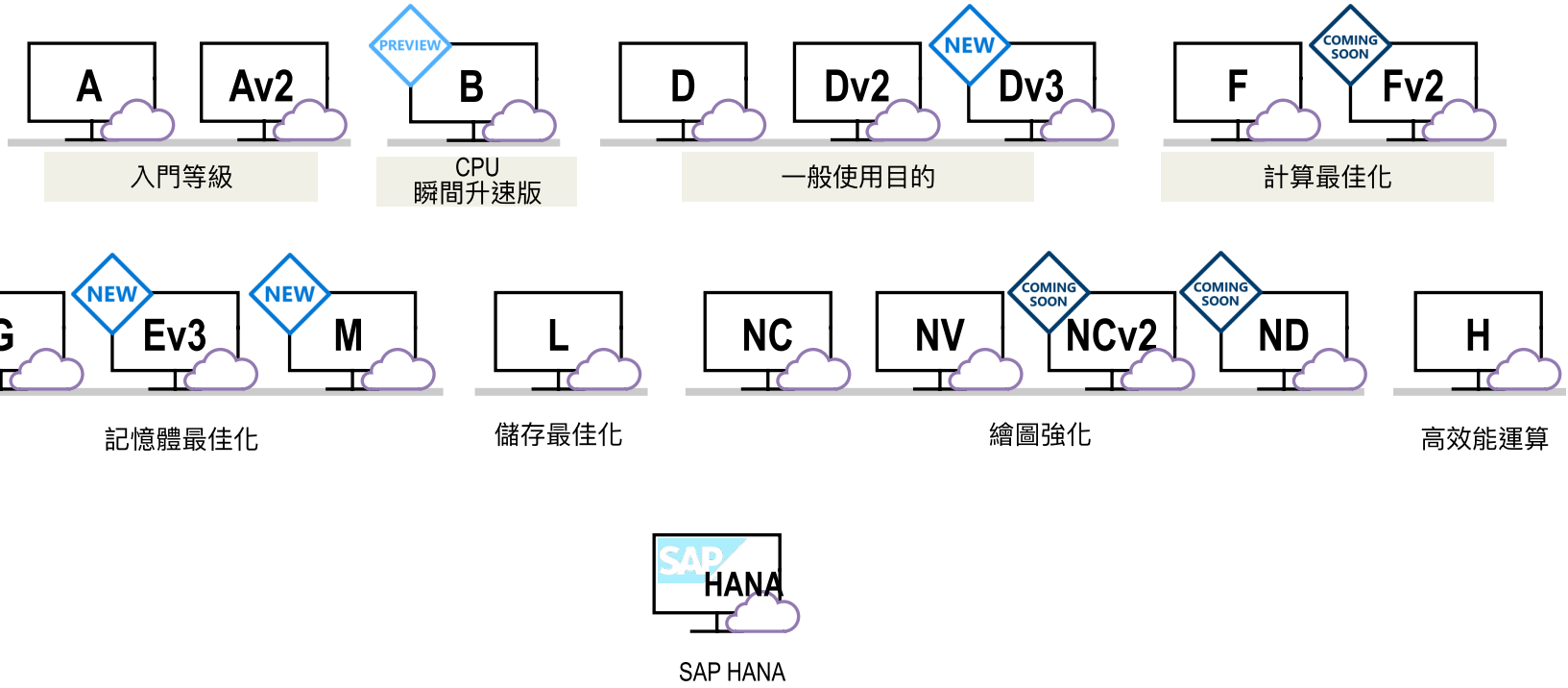


虛擬機器擴展集

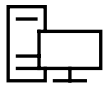
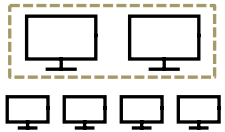
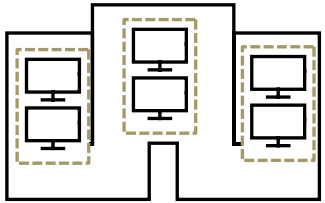
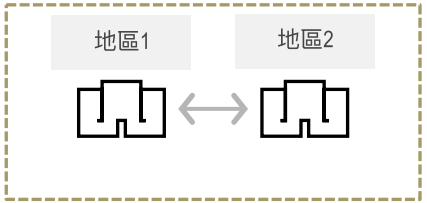
完全釋放虛擬機器的彈性與能力
設計用來處理高負載的應用
全自動調整規模 (增加或減少)、最高到 1000 個執行個體

計算 儲存 網路 管理

適合各類型系統的虛擬主機規格選項



可用性選項

VM SLA 99.9% (使用高級儲存)	VM SLA 99.95%	VM SLA 99.99%	多區域災難復原
			
單一虛擬機器 容易提升與移轉	可用性設定組 Availability Sets 同一個資料中心中的 VM 失敗保護	可用性區域 Availability Zones 整個資料中心的失敗保護	配對的地區 Paired Regions 提供地區 (Region) 保護

配對的地區：https://docs.microsoft.com/zh-tw/azure/best-practices-availability-paired-regions

Azure 儲存

IaaS

儲存　虛擬機器　網路

磁碟 Disks
保存 Azure IaaS 虛擬機器的磁碟

進階儲存體磁碟
Premium Storage Disks SSD、高 IOPS、低延遲

檔案 Files
雲端上被完整管理的檔案共用

支援 SMB 與 REST 存取

舊應用程式無痛移轉

可以跟地端檔案伺服器同步 (Azure File Sync)

Blobs
高規模擴展能力、支援 REST 存取的雲端物件儲存體

Block Blobs: 循序檔案 I/O 支援熱、冷和封存層
Page Blobs: 隨機讀寫
Append Blobs

表格 Tables
自動整規模的大量 NoSQL 儲存

跟據負載自動調整規模

可以擴展到 PB 等級

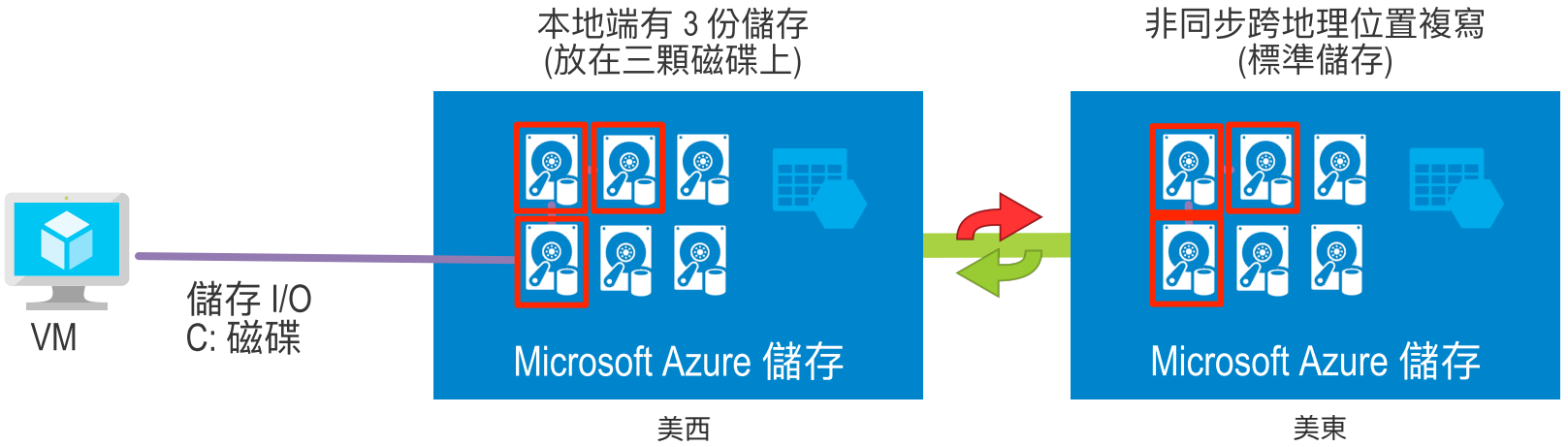
快速的 key/value 查詢

佇列 Queues
提供雲端服務之間非同步通訊用

支援佇列訊息可視性逾時機制，以保護不穩定的應用程式取用佇列訊息

建置在統一的分散式儲存系統
高耐用性、靜態加密、高度一致的複寫、容錯、自動負載平衡

虛擬機器儲存


本地端有 3 份儲存
(放在三顆磁碟上)
非同步跨地理位置複寫
(標準儲存)
VM
儲存 I/O
C: 磁碟
Microsoft Azure 儲存
Microsoft Azure 儲存
美西
美東

虛擬機器儲存

進階儲存體

SSD、高 IOPS、低延遲

最高 64 TB、80000 IOPs

適合需要高 IPOs 的應用，例如資料庫、檔案伺服器、高 I/O 的應用程式...

標準儲存體

HDD、最高到 500 IOPs

適合不需要高 IOPs 磁碟的應用，例如 Web 應用程式

檔案

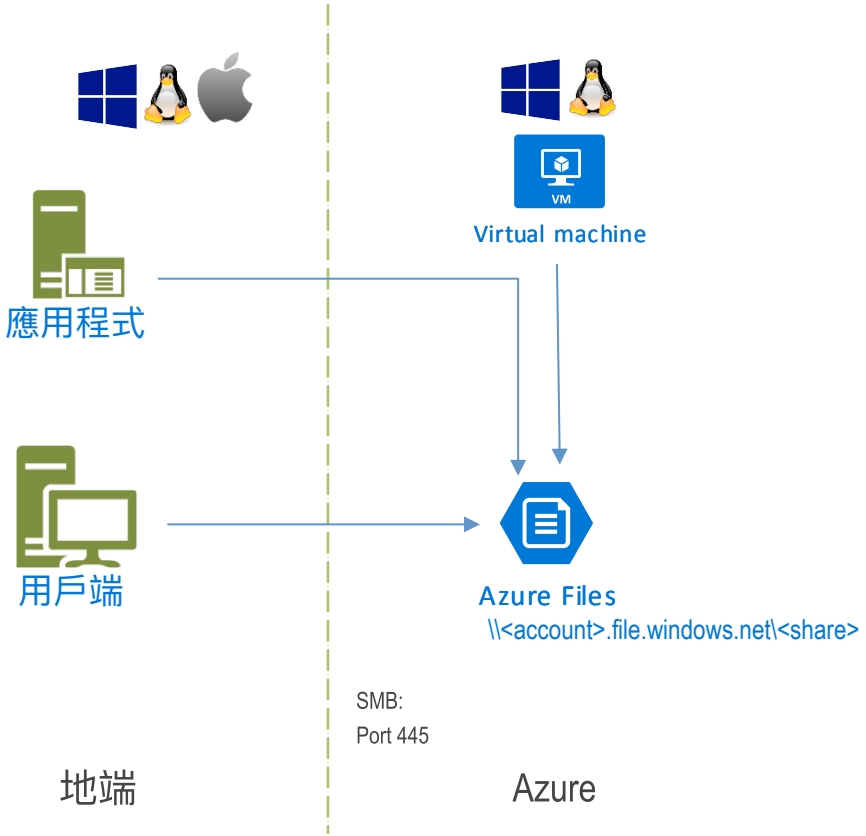
SMB 共用資料夾

SMB 3.0

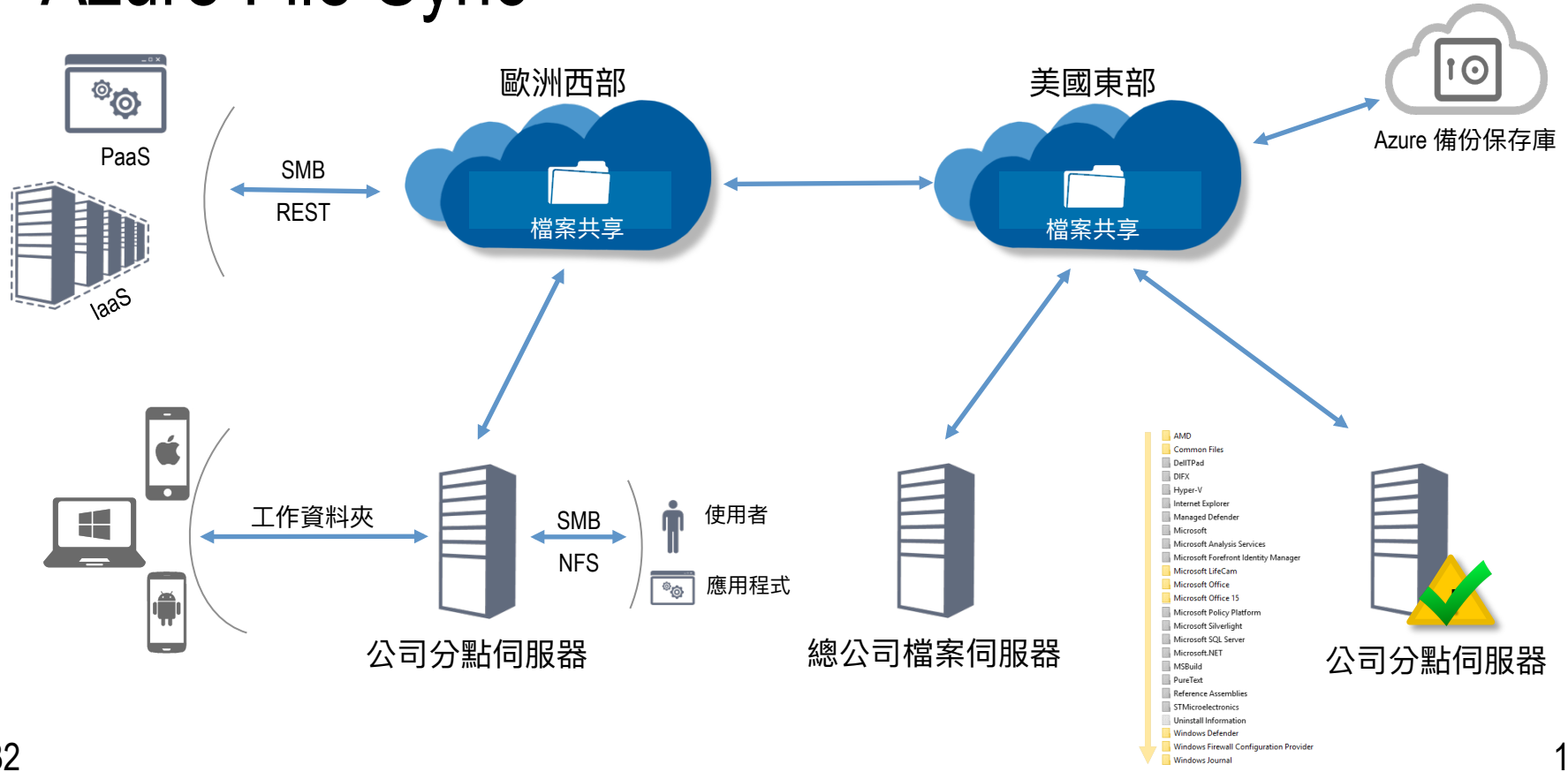
共用儲存 (供多部虛擬機器同時進行讀寫)、取代檔案伺服器、支援舊有的應用程式、...

Azure File

- ✓直接可以使用
- ✓支援多種用戶端與通訊協定
  - SMB 2.1, 3.0, REST
  - Windows, Linux, Mac OS
  - Azure 與地端存取
- ✓安全
  - 資料靜態加密
  - 透過 SMB 的安全連接
- ✓同步 (Azure File Sync)
  - 跨站台存取
  - 雲端多階層儲存



Azure File Sync



虛擬機器網路

支援 IPv4 與 IPv6

支援多張虛擬網卡 (路由器、防火牆)

私有 IP 或/與 公有 IP (靜態或動態)

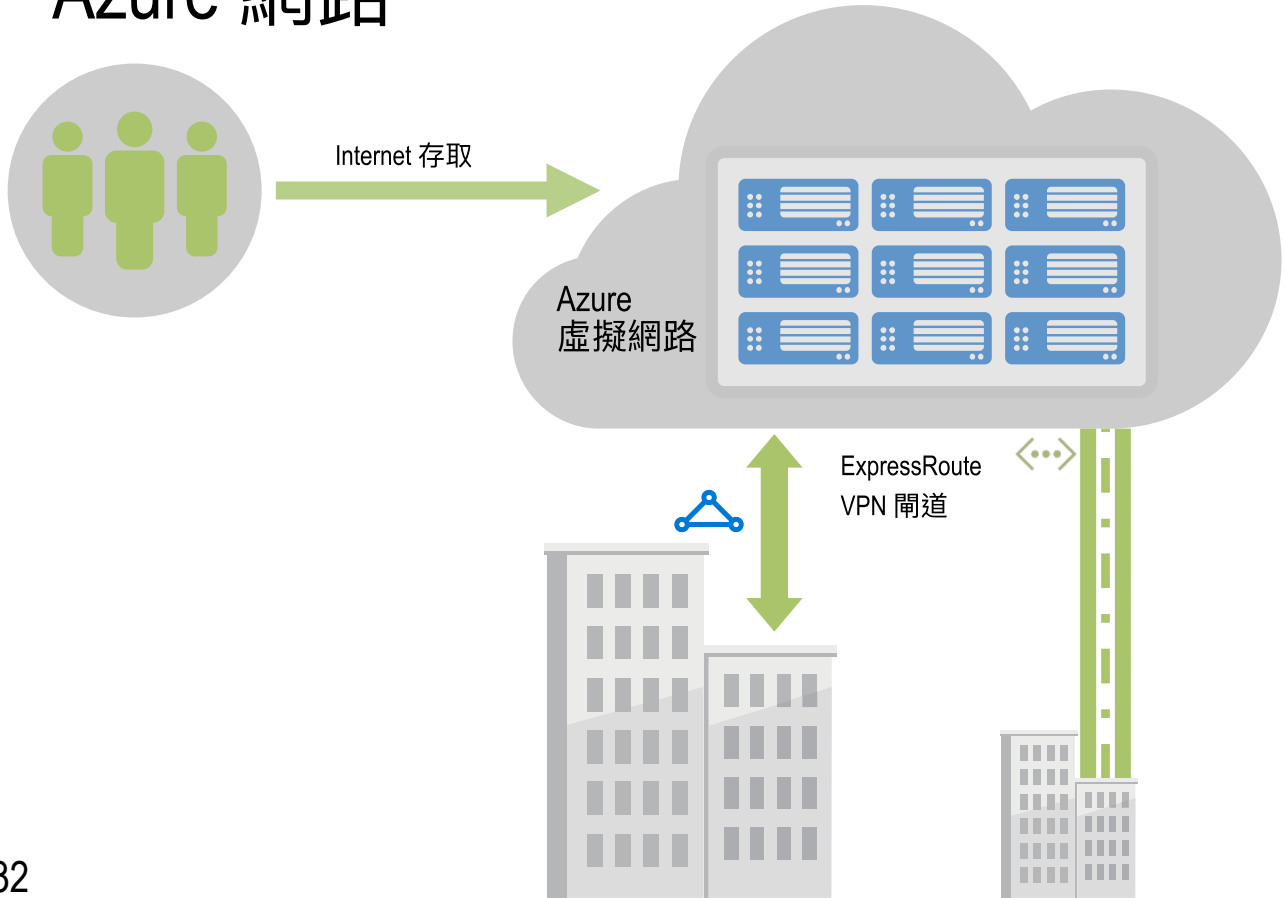
使用網路安全群組 (NSG) 來隔離網路

透過虛擬網路指派 DNS，或者直接使用 Azure DNS

加速網路 （SRI-OV，25Gbps)

固定 MAC 位址

Azure 網路



虛擬網路

- 私有 IP 位置、網路層級隔離
- 使用網段與安全群組進行網路分割
- 使用使用者自訂路由來控制網路傳輸

混合雲連線

- 點到站 VPN (開發/測試)
- VPN 閘道: 站對站 VPN
- ExpressRoute: 企業等級私有連線
- 將 AD 網域範圍擴展到 Azure

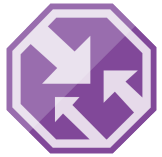
負載平衡

負載平衡器

OSI 第 4 層

應用程式閘道
(含 Web 應用程式防火牆 WAF)

OSI 第 7 層



流量管理員 (Traffic Manager)

DNS

Azure 市集上第三方廠商提供的方案

實作混合雲 – 連接 Azure

點對站台 VPN	• 小規模部署 • 隨處可以連接 Azure
站台對站台 VPN	• 從地端或其它 Auzre 地區連線到 Azure
虛擬網路對等互連 Vnet Peering	• 在同一個地區 (region) 內的兩個虛擬網路互連 • 提供 VM 對 VM 的直接連接能力 • 設定 Azure 路由表 (UDR)
ExpressRoute 私有線路	• 地端資料中心與 Azure 之間的專線

https://docs.microsoft.com/zh-tw/azure/vpn-gateway/vpn-gateway-about-vpngateways

管理與安全

Azure Active Directory
雲端的目錄與身份管理

Azure 資源管理員
組織、部署與控制 Azure 上的資源

Azure 安全中心
避免、偵測與回應威脅

Azure Advisor
針對高可用性、安全性、效能與成本提供建議

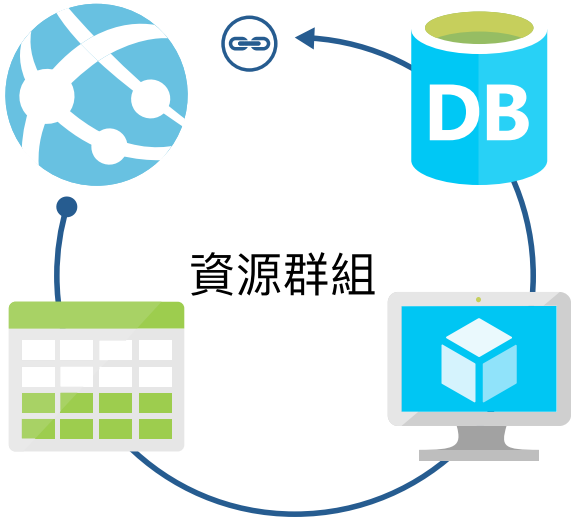
Azure Log Analytics
收集、分析與搜尋本地端與雲端記錄資料，並以視覺化呈現

Azure Key Vault
安全儲存密碼與金鑰

Azure Backup
備份虛擬機器、資料、... 到 Azure

Azure Site Recovery
提供跨站台災難復原機制

Azure 資源管理員 (ARM)



允許 Azure 的應用程式管理

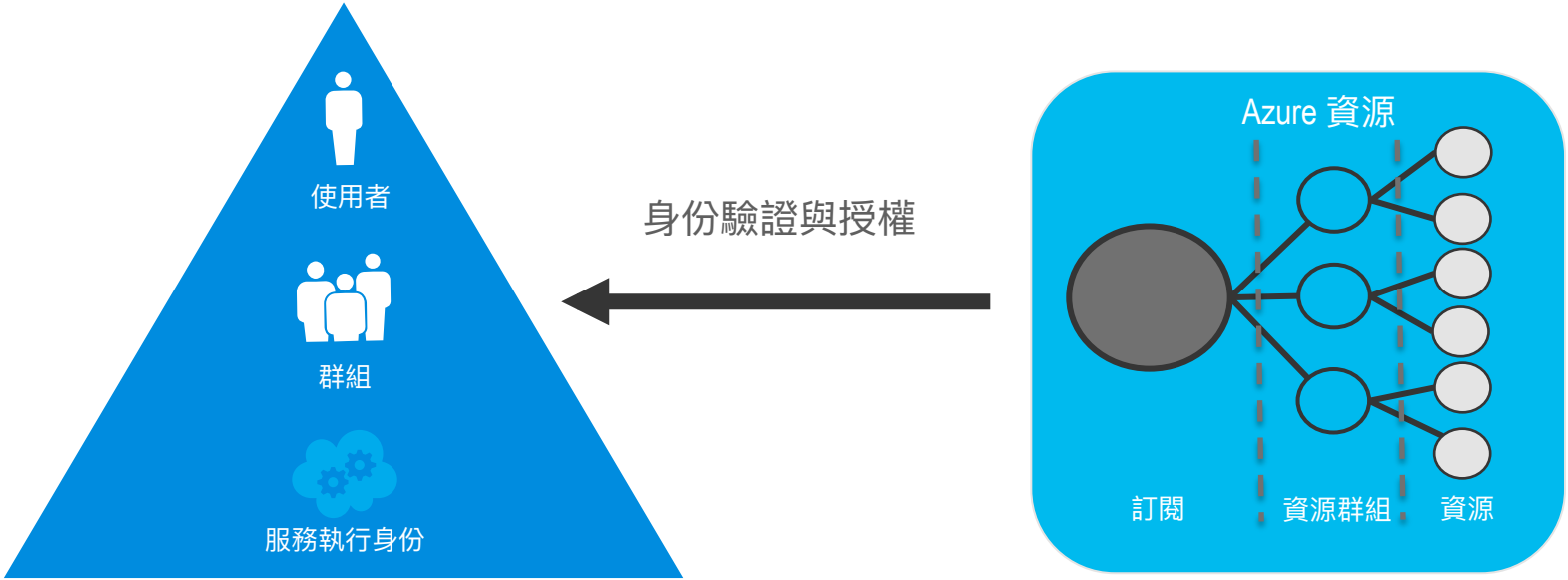
資源群組 (RG) 是可以容納多 IaaS 或 PaaS 資源的容器

對應應用程式部署與組態設定，支援 DevOps

管控方式: 以角色為基礎的存取控制 (RBAC)、原則、資源鎖定

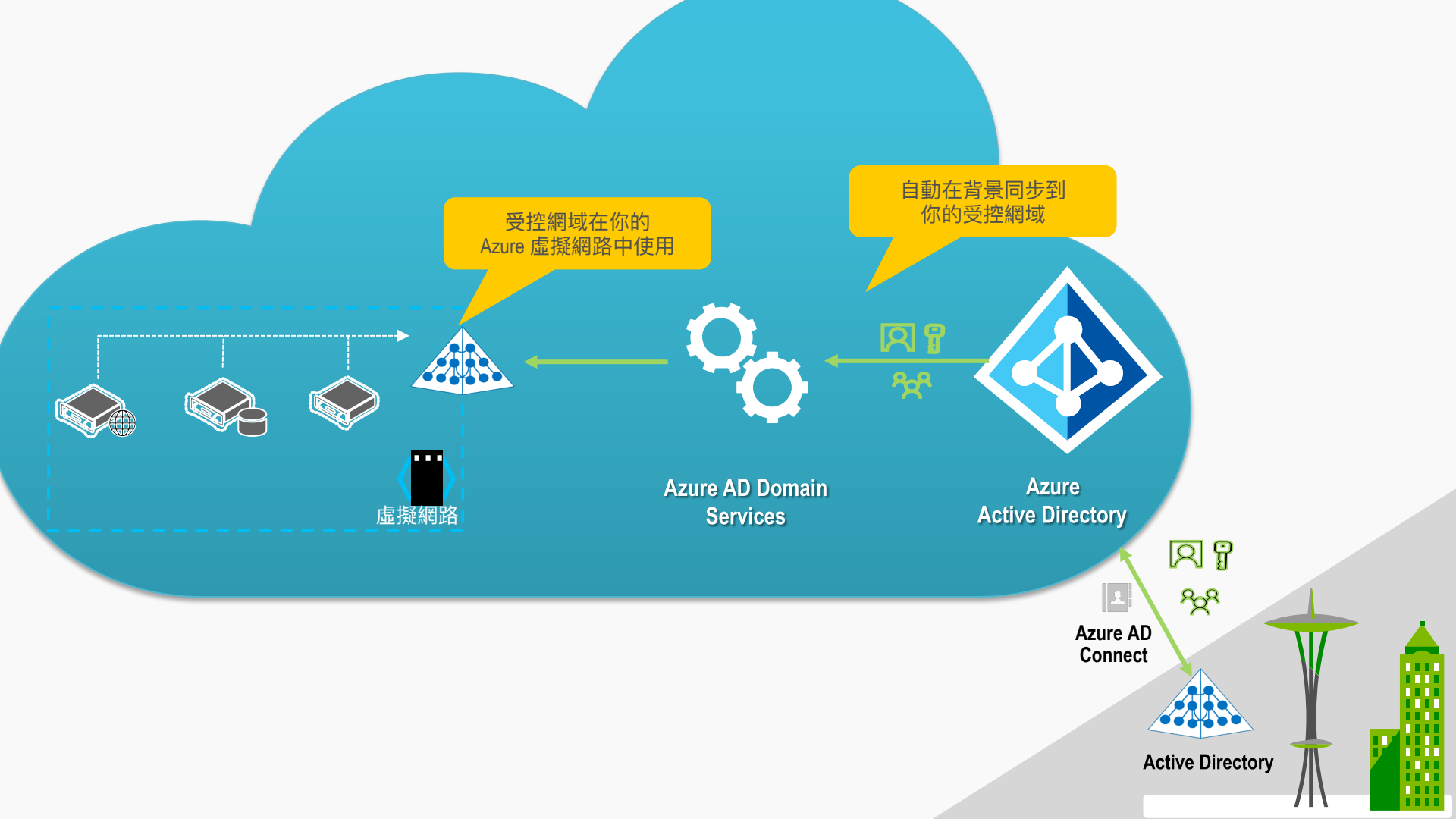
支援範本部署

Azure Active Directory



Azure Active Directory

Azure 訂閱


受控網域在你的
Azure 虛擬網路中使用
自動在背景同步到
你的受控網域
虛擬網路
Azure AD Domain
Services
Azure
Active Directory
Azure AD
Connect
Active Directory

Microsoft

Azure for IT Pro 三堂課 3

邁向身分驗證達人之路

駕馭 Azure AD, Azure Domain Service 以及多重驗證 (MFA)

日期：2018 年 4 月 20 日 (五) 14:00 – 17: 30

地點：台北市忠孝東路五段 68 號 19 樓 (台灣微軟 19 F MPR 123)

講師：曹祖聖

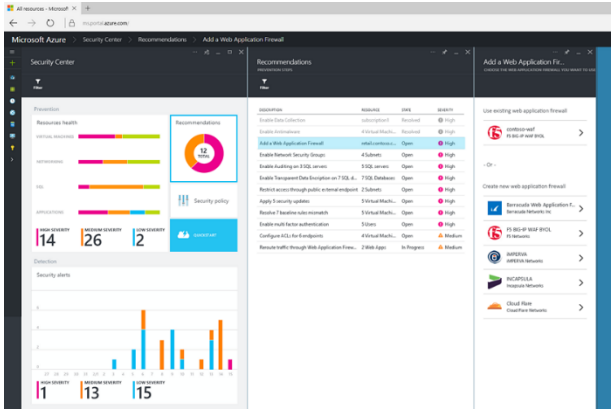
Azure 安全中心

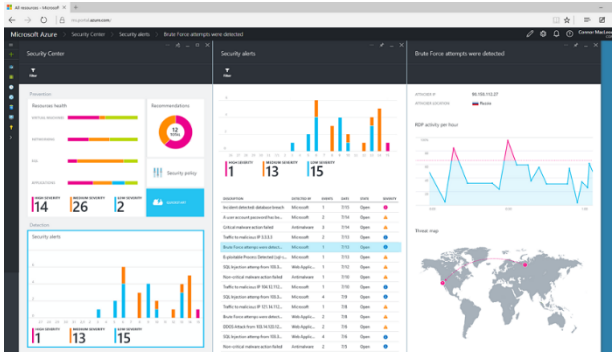
了解你的雲端安全狀態

透過安全性原則定義，讓 Azure 資源所有者了解到必須做那些安全控制

可以整合來自微軟或第三方伙伴提供的安全解決方案

結合微軟全球威脅專家與人工智慧分析，深入分析各項事件，協助你及早偵測並減少可能的威脅。





Azure 記錄分析 (Log Analytics)

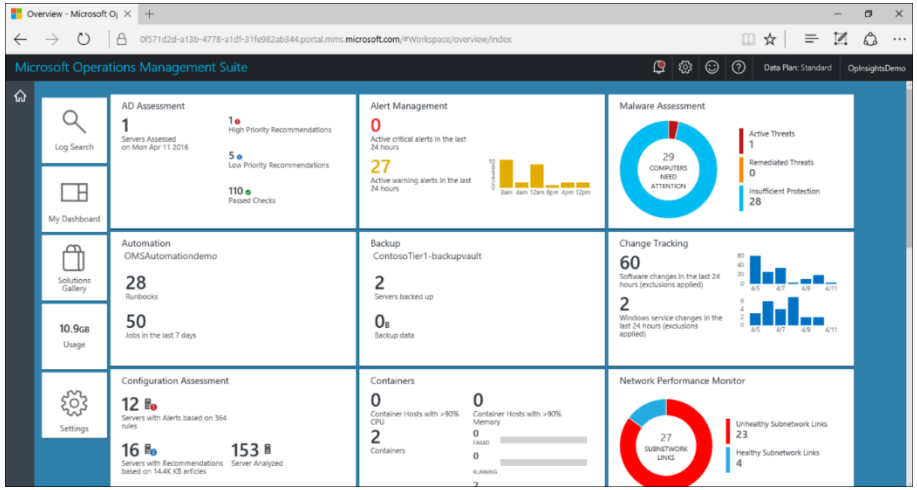
掌握你的混合雲環境的所有狀況

監控與收集資料的對象包含本地端資料中心與公有雲 (Azure、 AWS)

很容易收集、交叉對應、分析與視覺化你的機器資料

實體、虛擬、使用量、健康狀況、... IT 狀況一目瞭然

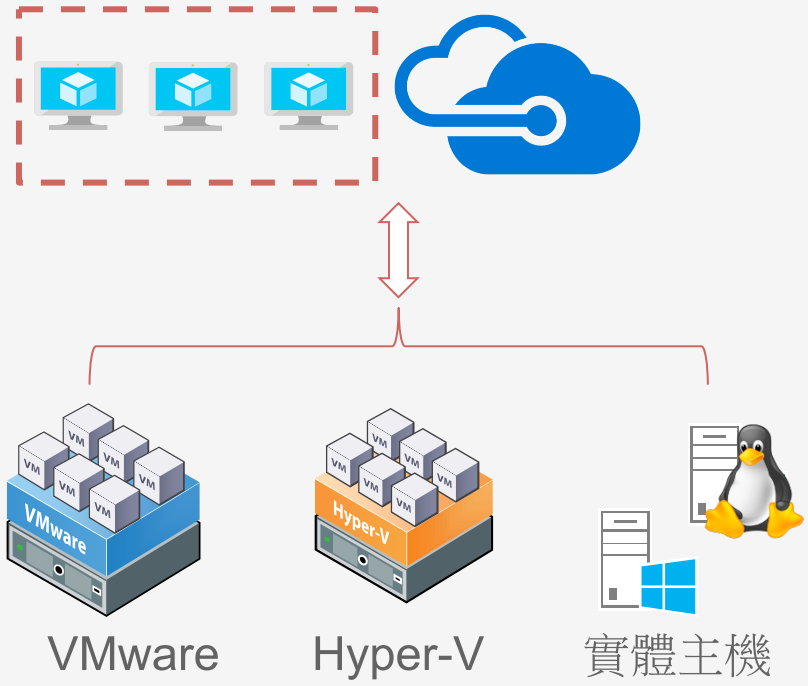
收集對象支援 Windows 與 Linux



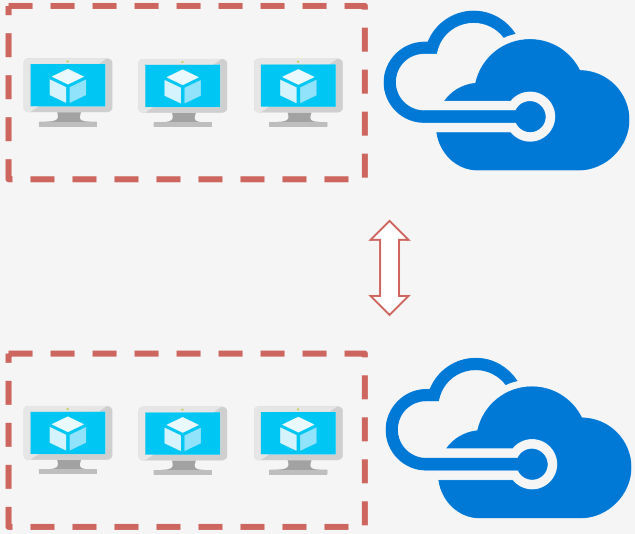
Azure Site Recovery

災難復原 + 移轉

計算 儲存 網路 管理



使用 Azure 做為本地端的備援



使用 Azure 做為 Azure 的備援

計算 儲存 網路 管理

Azure Migrate

	探索	移轉	最佳化
	Azure Migrate		
Microsoft	Database Migration Assistant	**Azure Site Recovery** Database Migration Service	Operations Management Suite CLOUDYN
Partners	Cloudamize, TSO Logic, CLOUDPHYSICS, BitTitan, RISC Networks CloudScape, MOVERE	CloudEndure, VELOSTRATA, Zerto, VEEAM, VISION SOLUTIONS, 5NINE SOFTWARE	docker, CloudAtlas

結論

- 將 Azure 當成你的另一個遠端機房
- 選擇適合的 Azure IaaS 服務
- 將你地端的資源部份或全部移轉到 Azure 上
- 整合 Azure 與地端的資源
- 善用 Azure 的管理與監控服務來改善 IT 資料中心的環境

課程資料

今天課程的簡報檔

4/20 身份驗證課程