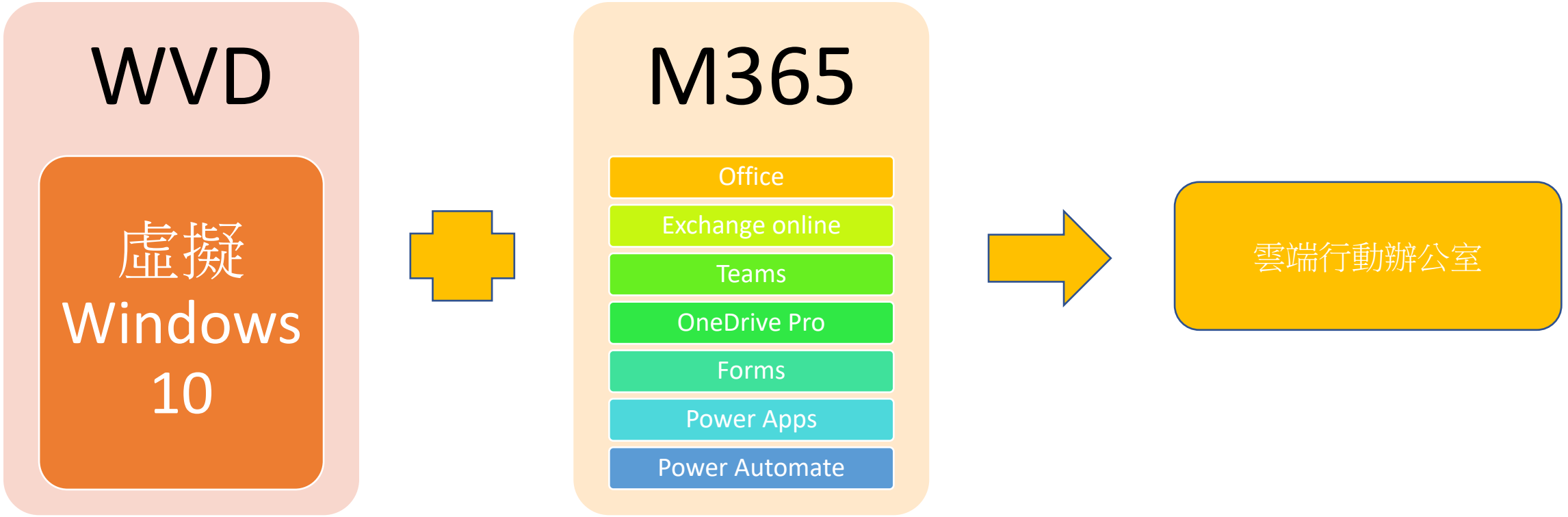
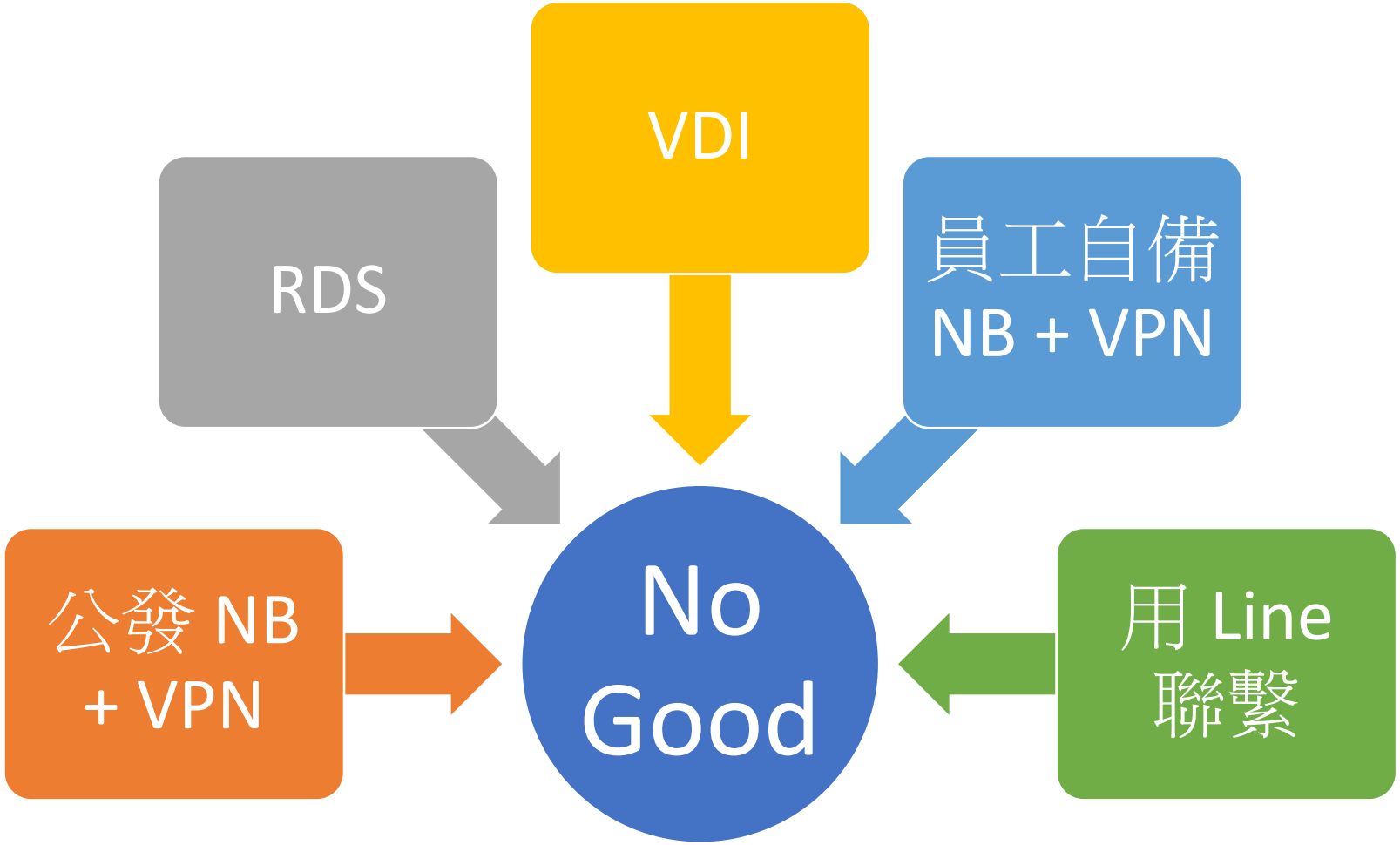
WVD (Azure 雲端虛擬桌面) + M365 雲端行動辦公室解決方案

WVD 與 M365 的完美結合



COVID 19 來襲，現在與未來如何辦公



傳統 VDI 的缺點

- 硬體
- 軟體
- 建置

入門成本高

- 軟硬體採購與到貨
- 導入經驗

導入時間長

- 人員增加
- 硬體效能需提升

架構規模不易調整

- 備份
- 容錯
- 硬碟毀損
- 資安

維護不易

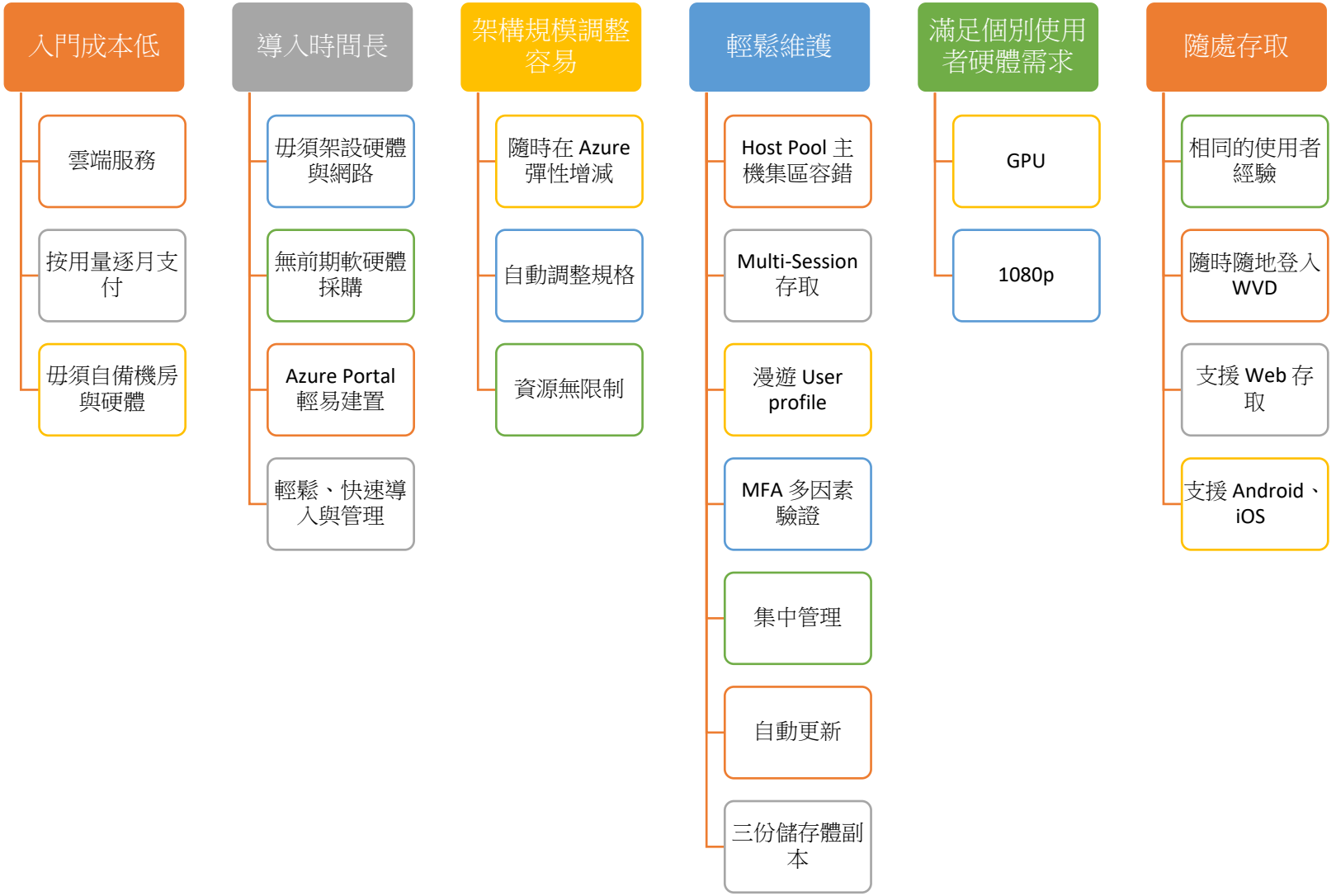
- GPU
- 1080p

無法滿足個別使用者需求

- 居家上班
- 行動工作者
- 手機無法存取

難以實現隨處存取

WVD (Azure 雲端虛擬桌面) 的優勢



WVD 的安全性


• 透過 Azure AD 輕鬆配置複雜的安全服務（例如 MFA）
Azure AD 安全服務
• 反向連接技術無需向虛擬機器開放輸入通訊埠
減少攻擊面
獨立的使用者工作階段
• 在單一和多重工作階段環境中隔離使用者的工作階段環境
細緻的存取控制
• 可以為多個管理員分配基於角色的存取控制

遠端桌面服務

- 虛擬工作空間策略的平台

隨處存取Windows桌面和應用程式

允許使用者從任何設備和任何位置存取Windows應用程式和桌面

靈活部署

內部部署,
雲端部署, 或
混和部署

降低成本

整合基礎架構提高效率

安全可擴充的平台

保護敏感的企業資料
建立自訂化解決方案

Windows Virtual Desktop

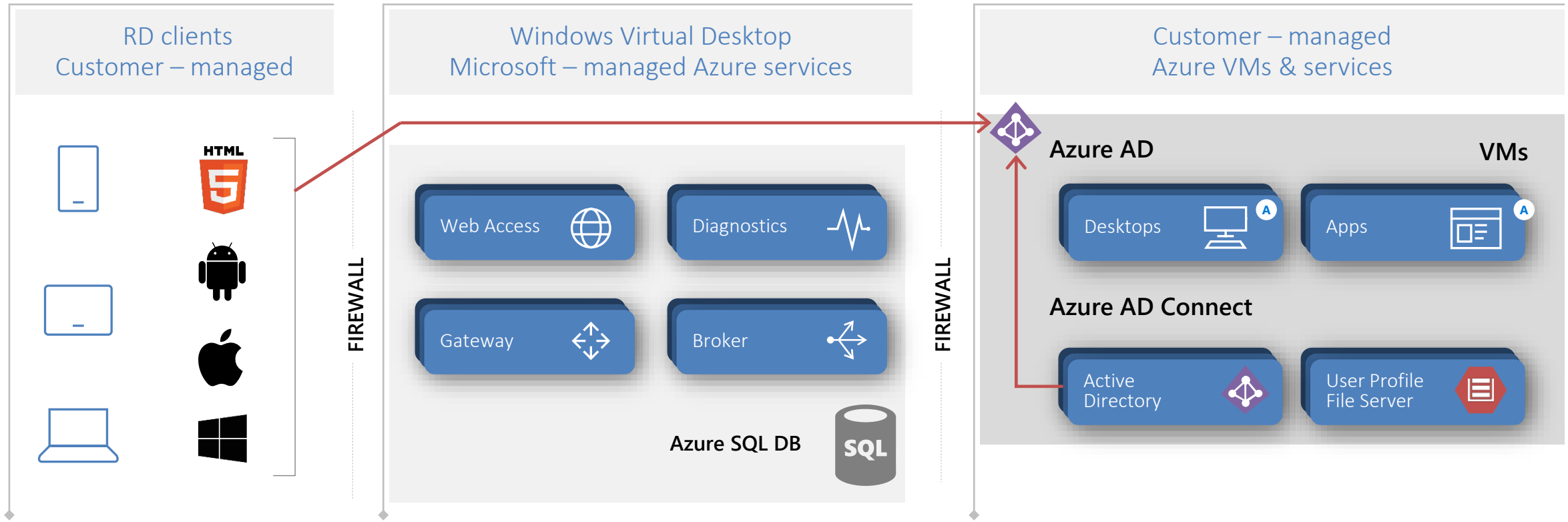
由 Azure 傳遞的最佳虛擬桌面體驗

- 提供唯一的多重工作階段 **Windows 10** 體驗
- 為 **Office 365 ProPlus** 提供最佳化
- 最靈活的服務允許您虛擬化桌面和應用程式
- 在幾分鐘內部署和擴展
- **Azure** 角色型存取控制**(Azure RBAC)**
- **Microsoft Teams**的**A / V**重新導向
- 與 **Microsoft 365** 的安全性和管理整合

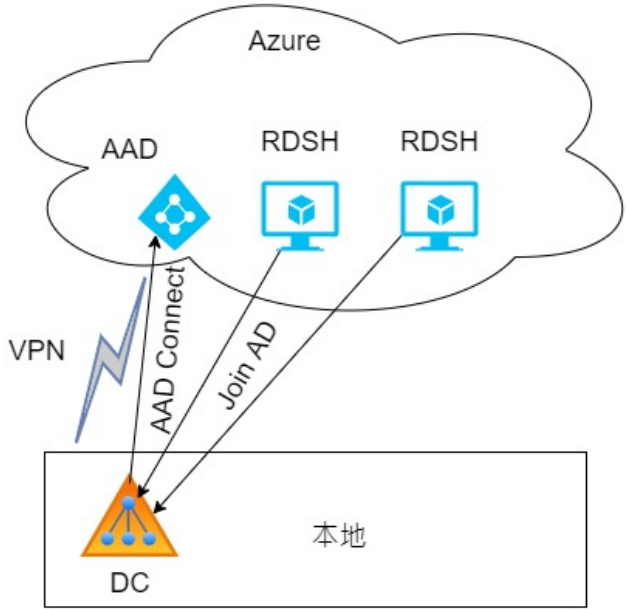
Windows Virtual Desktop
架構及部署

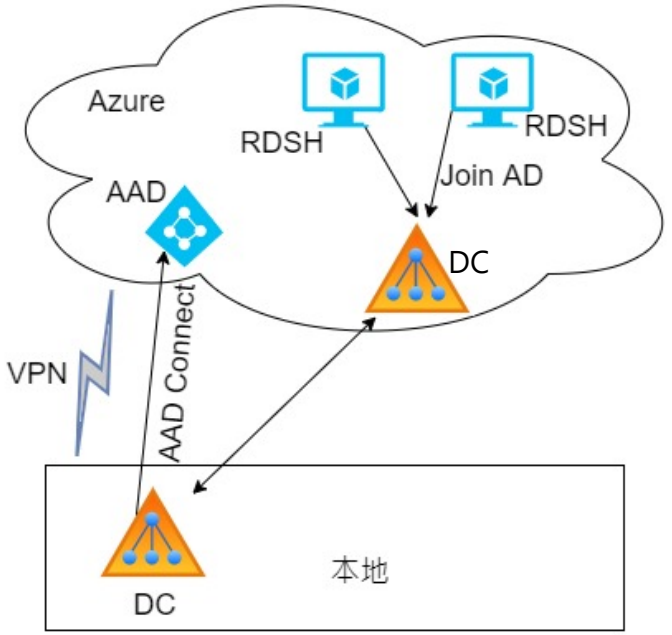
Azure AD 認證

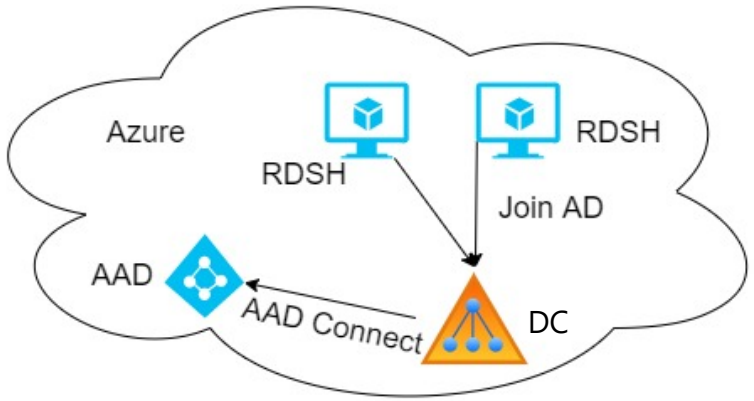
- 用戶端使用 Azure Active Directory (Azure AD) 身份進行驗證
- Azure AD 允許使用條件式存取和多因素身份驗證
- Windows VM 需要加入AD，以獲得最佳的應用程式相容性

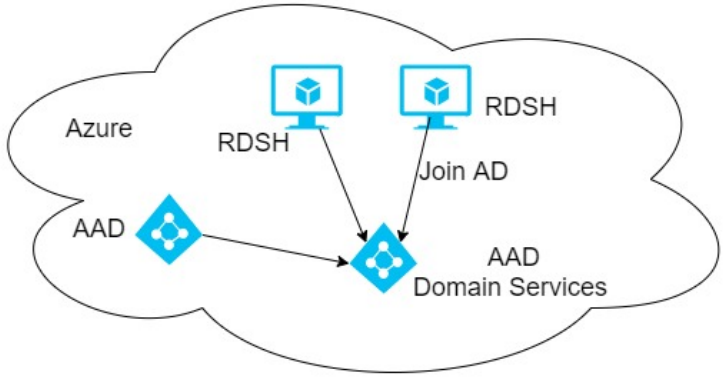


幾種架構


Azure
AAD
RDSH
RDSH
VPN
AAD Connect
Join AD
本地
DC


Azure
RDSH
RDSH
Join AD
AAD
DC
VPN
AAD Connect
本地
DC


Azure
RDSH
RDSH
Join AD
AAD
AAD Connect
DC


Azure
RDSH
RDSH
Join AD
AAD
AAD
Domain Services

先決條件

要求

Azure 訂閱

Azure Active Directory

- 完整的管理權限
- Azure AD Connect
- ADFS (optional for SSO)

決定您的身份識別策略(AD, ADDS)

所有相關的Azure資源(影像、虛擬網路、儲存體)等都必須在同一個資料中心

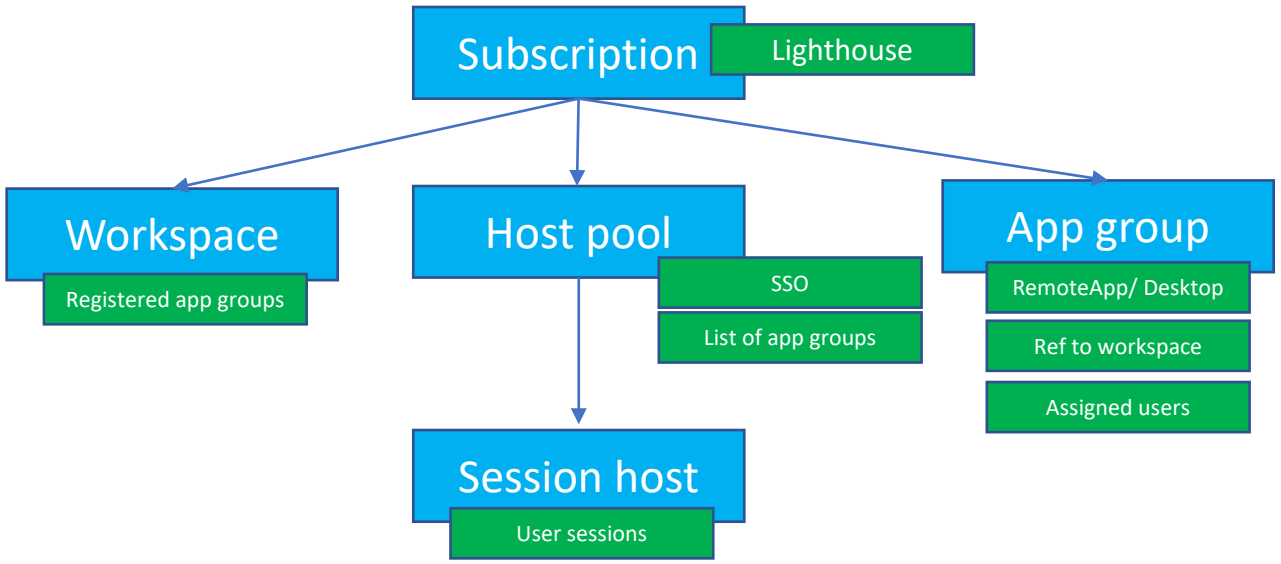
選用：網路/內部部署連接 — Express route，VPN

必要的認證(Azure AD, Service Principle, etc…)

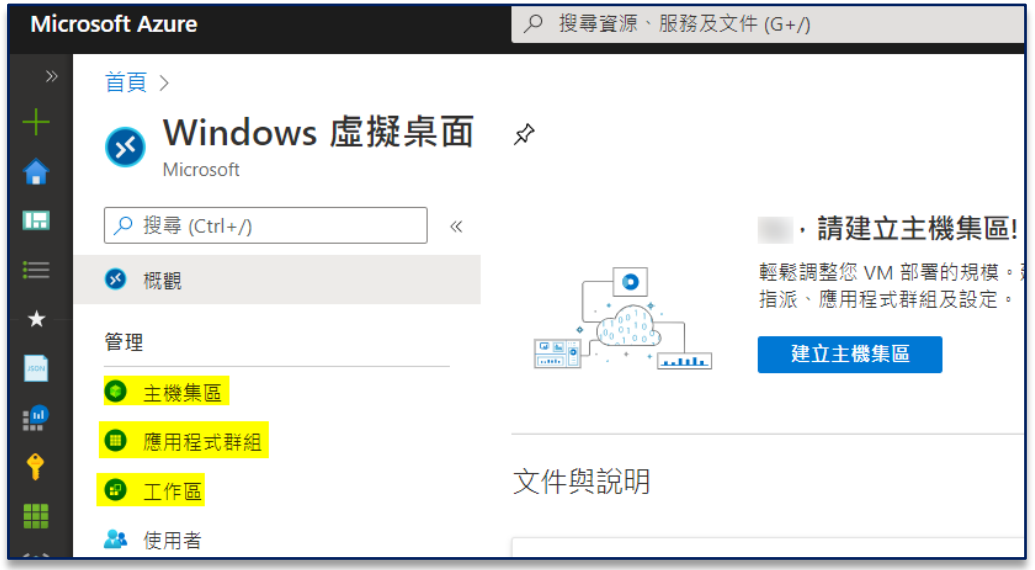
正確的授權

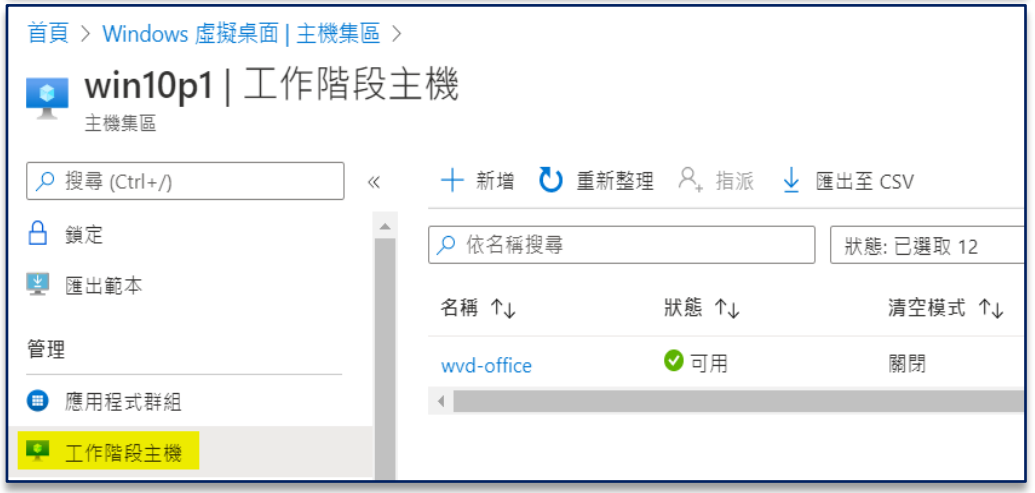
WVD 物件模型

2020春季更新版 物件模型



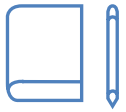
注意：所有資源都將具有與其關聯的資源群組和位置





效能指南

應將 VM 部署到具有 WVD 叢集的 Azure 區域



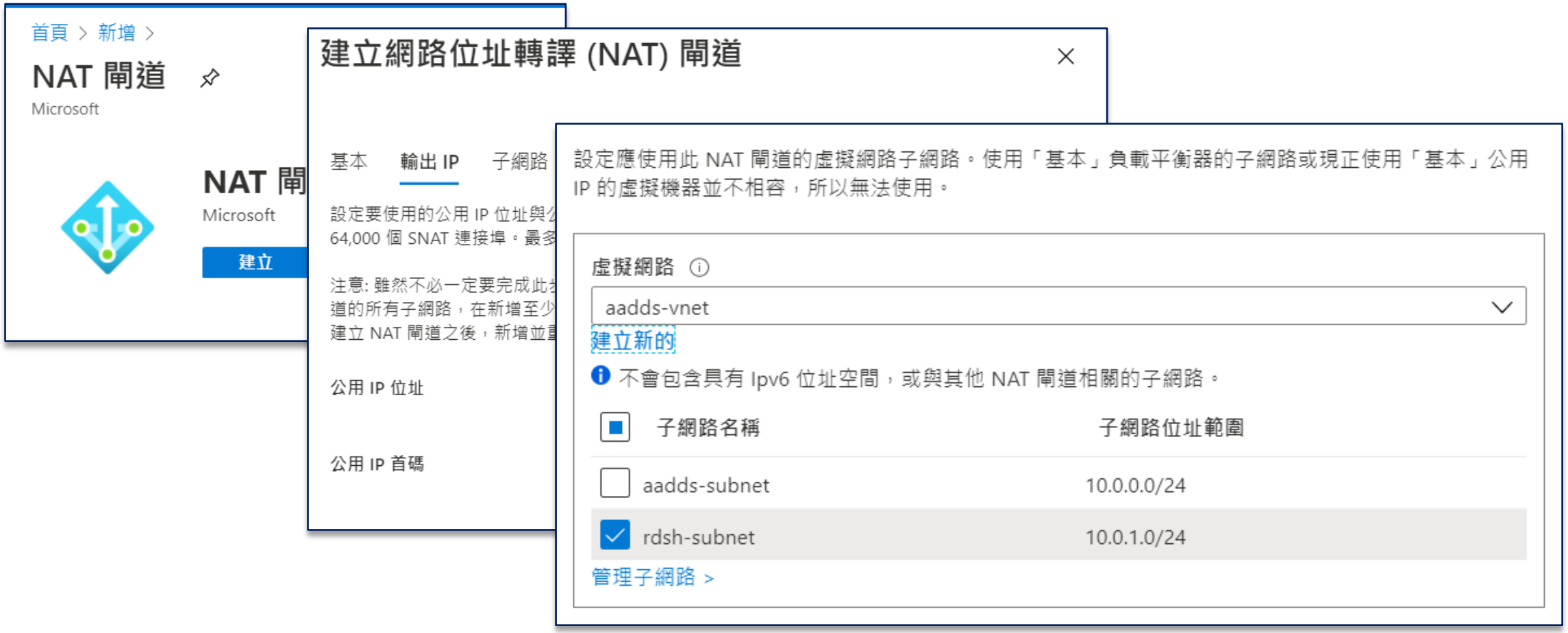
Active Directory 資料中心應該位於工作階段主機池所在的每個區域

建議混合使用廣度和深度縮放，以適應尖峰和離峰時間

利用多使用者密度來獲得最划算的選擇

虛擬機器配置應符合使用案例和主機池的需求

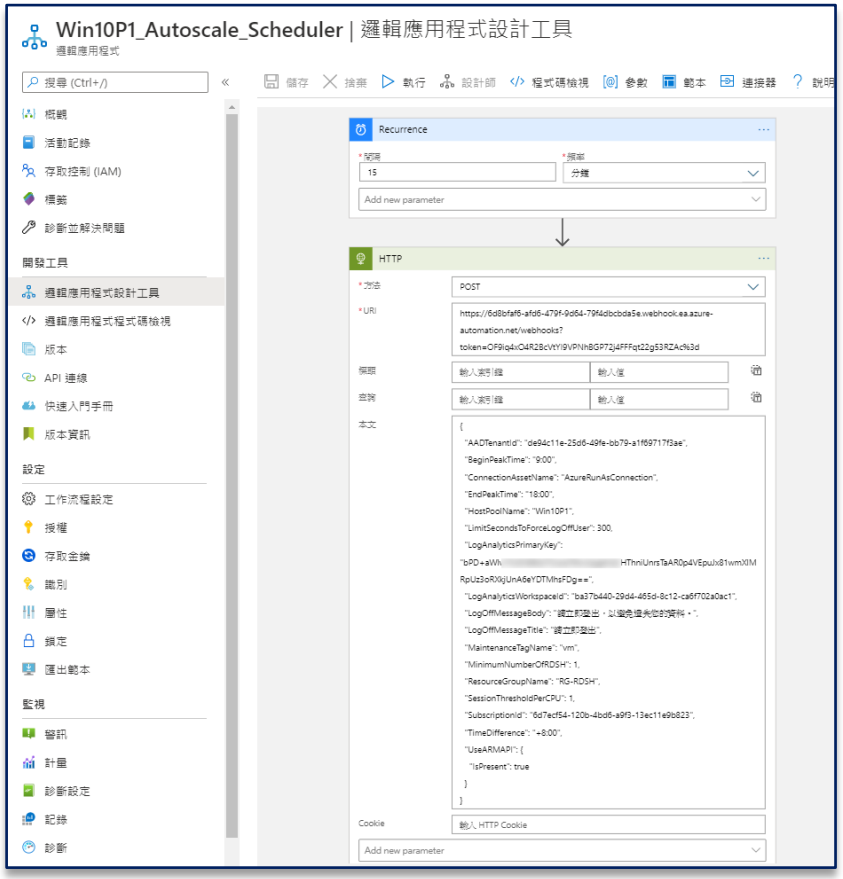
固定輸出IP

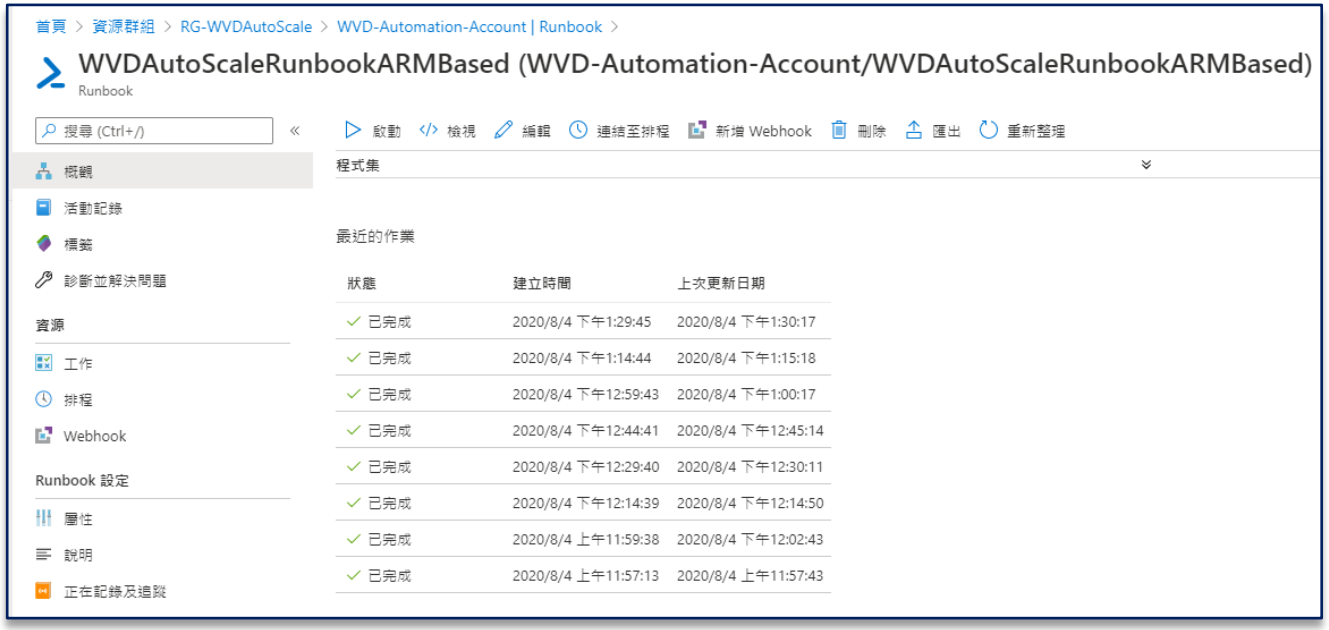


※ NAT閘道按照使用時間和流量收費

規模調整

使用Automation和Logic App搭配按照規則調整規模





https://docs.microsoft.com/zh-tw/azure/virtual-desktop/set-up-scaling-script

Windows Virtual Desktop
資訊安全及資料保護

什麼是多因素驗證

使用兩個或多個因素:

- 您知道的一些資訊，例如密碼或PIN
- 您擁有的東西，例如電話，信用卡或硬體權杖
- 可以實際識別您身份的東西，例如指紋，臉部辨識或其他生物特徵辨識

使用兩個不同的管道更安全，比使用一種身份驗證提供更多的保障.

什麼是條件式存取？

新式安全性的範圍現在已延伸到組織的網路之外，可包含使用者和裝置身分識別。 組織可以利用這些身分識別訊號作為其存取控制決策的一部分

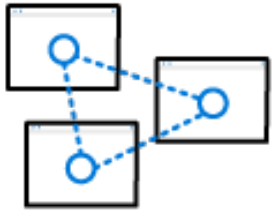
條件式存取是 Azure Active Directory 用來將訊號結合在一起、進行決策及強制執行組織原則的工具

基於使用者和位置的條件存取

透過使用基於位置的條件存取原則限制基於地區位置或IP地址的使用者存取來保持機敏資料的安全

基於裝置的條件存取

確保只有註冊和允許的設備才能使用基於設備的條件存取存取公司資料



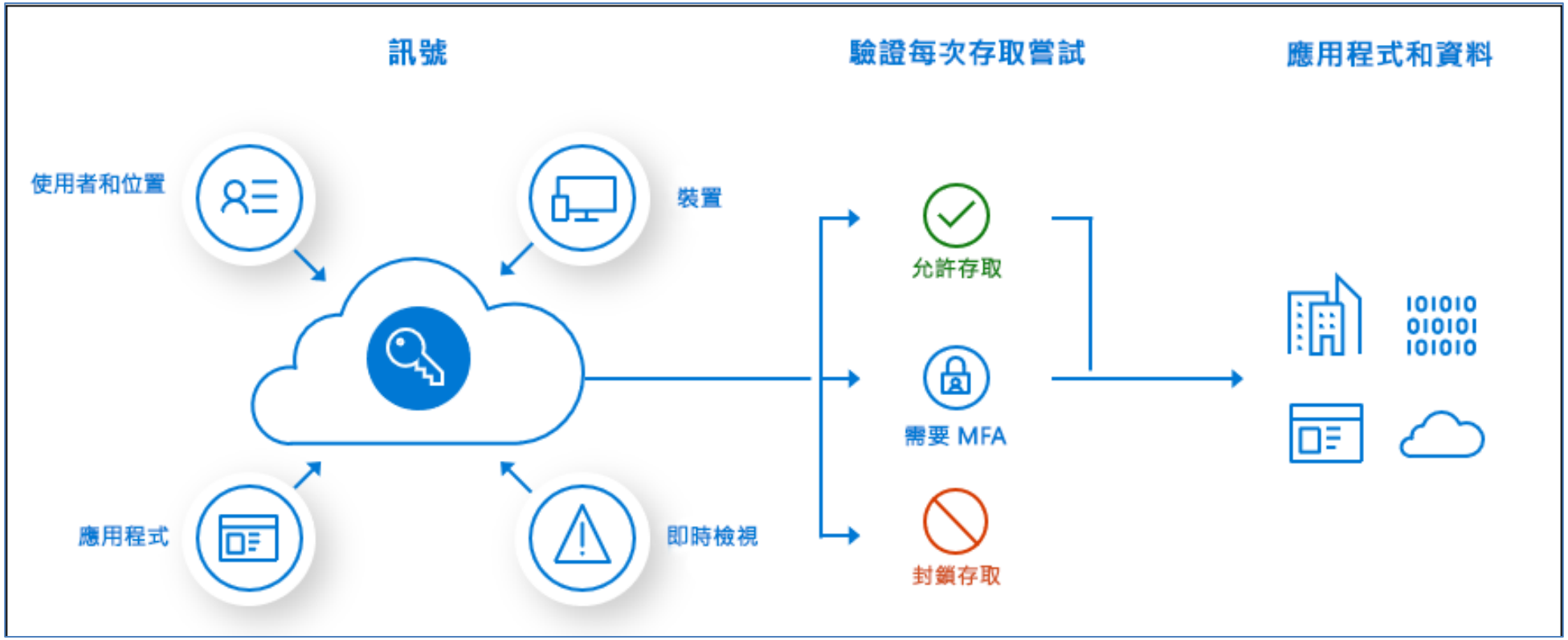
基於應用的條件存取

當使用者不在公司網路中時，工作不必停止。 安全存取公司雲端和本地應用程式，並通過條件存取來保持控制

基於風險的條件存取

基於風險的條件存取原則可以保護您的資料免受駭客攻擊，該原則可以應用於所有應用程式和所有用戶，無論是本地還是雲端帳號

條件式存取 – MFA 的現代使用方式



雲端行動辦公室的建置服務

行動辦公室解決方案 (企業純雲端一線工作人員 10 人版)
架構討論
Windows Virtual Desktop 建置與設定
服務開通、帳戶建立、授權指派
Office 雲端版
Exchange online 電子郵件服務設定 (2G)
Teams 視訊會議服務建立與使用說明
OneDrive pro 雲端硬碟設定與使用說明 (2G)
MFA 多因素驗證與使用說明
Power Apps 行動 App 簡易應用說明
Forms 簡易應用說明
Azure (儲存體、頻寬費、虛擬機器)

行動辦公室解決方案 (企業純雲端)
架構討論
Windows Virtual Desktop 建置與設定
服務開通、帳戶建立、授權指派
Office 應用程式佈署
Exchange online 電子郵件服務設定
Teams 視訊會議服務建立與使用說明
OneDrive pro 雲端硬碟設定與使用說明
MFA 多因素驗證與使用說明
Power Apps 行動 App 簡易應用說明
Forms 簡易應用說明
Azure (儲存體、頻寬費、虛擬機器)