微軟支援軟體極致套件包

Windows Server 2019終極指南

充分利用Windows Server 2019的本地投資。了解如何使用Windows Server 2019的高級混合功能將本地環境擴展到雲中。並且，了解在連接到雲時如何加其他安全層以及更新應用程序和基礎結構。

- 使用最新的操作系統更新本地服務器和存儲基礎結構，以確保安全性和最佳的性能價格。
- 支持創建雲原生應用程序，並使用容器和微服務更新傳統應用程序。
- 使用Windows Admin Center（一個免費的，基於瀏覽器的新應用程序）管理服務器，群集和超融合基礎架構。
- 將本地服務器擴展到Azure，以提供包括備份，災難恢復以及按需計算和存儲資源在內的服務。

一般

Windows Admin Center

Windows Admin Center 是以瀏覽器為基礎在本機部署的應用程式，用於管理伺服器、叢集、超融合式基礎結構以及 Windows 10 電腦。 除了 Windows 本身以外，不需另付費用，而且可以立即使用於生產環境中。

您可以在 Windows Server 2019、Windows 10 和舊版 Windows 及 Windows Server 上安裝 Windows Admin Center，並用它來管理執行 Windows Server 2008 R2 和更新版本的伺服器及叢集。

如需詳細資訊，請參閱 Windows Admin Center。

桌面體驗

因為 Windows Server 2019 是長期維護通道 (LTSC) 發行，所以包含**桌面體驗**。 (半年通道 (SAC) 版本預設不包含桌面體驗；這些版本只是 Server Core 和 Nano Server 容器映像版本。) 和 Windows Server 2016 一樣，在安裝作業系統期間，您可以選擇核心安裝或含桌面體驗的伺服器安裝。

安全性

Windows Defender 進階威脅防護 (ATP)

ATP 的深度平台感應器和回應動作會公開記憶體和核心層級攻擊，並透過隱藏惡意檔案和終止惡意處理程序來因應。

- 如需有關 Windows Defender ATP 的詳細資訊，請參閱 Windows Defender ATP 功能概觀 (英文)。
- 如需上架伺服器的詳細資訊，請參閱將伺服器上架到 Windows Defender ATP 服務。

Windows Defender ATP 惡意探索防護是一組新的主機入侵預防功能。 Windows Defender 惡意探索防護的四個元件專門設計來鎖定裝置以抵禦各種攻擊方式，並封鎖惡意程式碼攻擊中常用的行為，同時讓您平衡安全性風險和生產力需求。

- 降低攻擊面 (ASR) 是一組控制項，可透過封鎖可疑的惡意檔案 (例如 Office 檔案)、指令碼、橫向移動、勒索軟體行為以及電子郵件型威脅，讓企業防止惡意軟體進入機器。
- 網路保護透過 Windows Defender SmartScreen 阻止裝置上任何傳向不受信任主機/IP 位址的輸出程序，保護端點免受到 Web 型威脅。
- 受控資料夾存取權會阻止不受信任的處理程序存取受保護的資料夾，進而保護敏感性資料免受勒索軟體侵害。