技能解封中間章程-庇護所疫軍之亂(Azure Anti-malware)

前言

<https://ithelp.ithome.com.tw/articles/10214088>

成本評估

**Azure Anti-malware 依下列定價面向計費：**

Azure 資訊安全中心透過其免費層與標準層保護所有 Azure 和特定內部部署資源。

在您升級至 Azure 資訊安全中心的標準層時，我們將自動註冊並開始保護您的所有資源，除非您明確決定退出。針對資訊安全中心保護的所有資源，我們將依照以下定價模式向您收費。

目前可透過 Azure 入口網站在訂用帳戶層級啟用 Azure 資訊安全中心。

標準層的前 30 天免費。30 天以後的使用量都依以下定價方案自動收費。

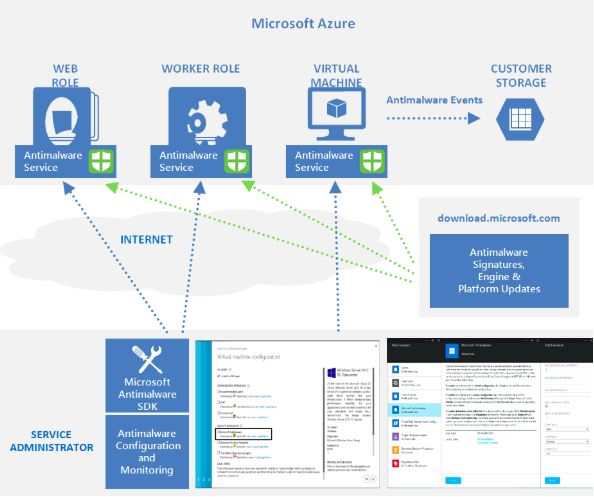
| 資源類型 | 免費層 | 標準層次 |
| --- | --- | --- |
| 虛擬機器 | 免費 | ~NT$438.792/伺服器/月 內含資料 – 500 MB/天 |
| 應用程式服務 | 免費 | ~NT$438.792/App Service/月 |
| SQL Database | 無法使用 | ~NT$438.792/伺服器/月 |
| MySQL (預覽) | 無法使用 | 免費 |
| PostgreSQL (預覽) | 無法使用 | 免費 |
| 儲存體 – 保護訂用帳戶內的所有儲存體帳戶 | 無法使用 | NT$0.602/10,000 筆交易 |
| 儲存體 – 保護訂用帳戶內的選擇性儲存體帳戶 | 無法使用 | NT$1.203/10,000 筆交易 |
| IoT 裝置 – 依裝置 | 無法使用 | NT$0.0301/月 |
| IoT 裝置 – 依訊息 | 無法使用 | NT$6.011/25,000 筆交易 |

一張含有 桌 的圖片

自動產生的描述

服務架構

1. 透過 Azure Portal or PowerShell將 Antimalware 延伸安裝檔推送至 Azure 中一個固定預設位置。
2. Azure VM 的 Agent 會啟動反惡意程式，將其組態設定套用。讓你如果沒有做任何自訂時就以預設組態來啟動其反惡意程式碼服務。
3. 執行過程中 Antimalware 會透過 Internet 下載最新保護定義載入到 Azure。
4. Antimalware 會將紀錄事件寫至 OS 事件記錄中。內容涵蓋反惡意程式碼用戶健康狀態、保護狀態、組態設定更新等定義的資訊。
5. 透過 Powershell 開啟 VM 反惡意程式碼監視，以便在此事件記錄中產生到你的 Azure Storage 一併寫入。



簡易實測環境

圖1. 在 VM中刀鋒視窗中有個延伸模組，可以從這裡做安裝

一張含有 文字 的圖片

自動產生的描述

圖2. 這裡有目前Azure都有支援微軟自家或是第三方(有授權問題請自行斟酌)

一張含有 文字 的圖片

自動產生的描述

圖3. 其中有預設是否有排除不做安全掃描的項目可以依照需求設置，另外也排程掃描

一張含有 文字 的圖片

自動產生的描述

圖4. 此示範透過資訊安全中心提示建議未安裝 Endpoint

一張含有 文字 的圖片

自動產生的描述

圖5. 對此機器勾選安裝

一張含有 文字 的圖片

自動產生的描述

圖6. 我們看到預設就是微軟的Antimalware (此沒的選，就是唯一支持)

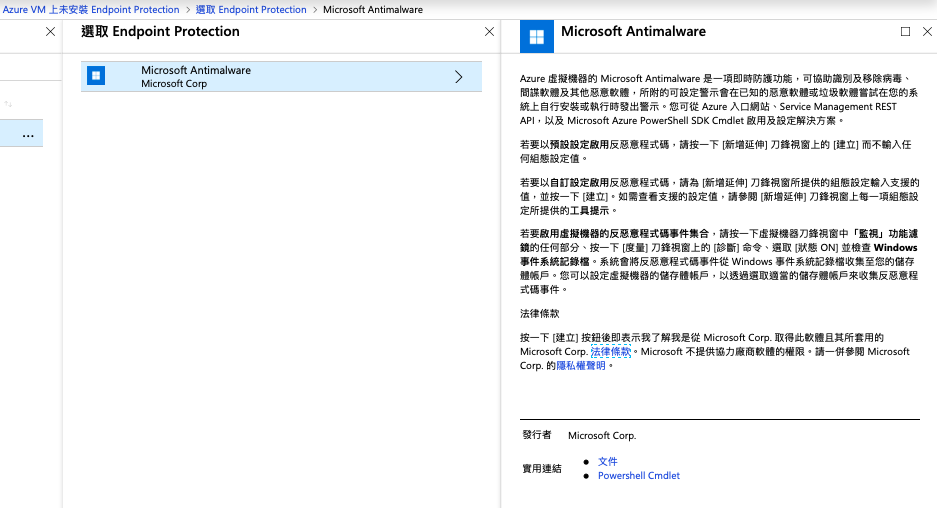


圖7. 其中有預設是否有排除不做安全掃描的項目可以依照需求設置，另外也排程掃描

一張含有 文字 的圖片

自動產生的描述

圖8. 安裝完成的狀態已顯示以解決

一張含有 文字 的圖片

自動產生的描述

圖9. 你從回到剛剛VM的延伸模組就看到此已經安裝上去

一張含有 文字 的圖片

自動產生的描述

圖10. 補充一下監視上需要還需要搭配系統診斷，請啟用Guest Diag

一張含有 文字 的圖片

自動產生的描述

圖11. 透過在資訊安全中心對於資料收集上工作區選擇以及自動佈署Agent已收集未來的長期發展

一張含有 文字 的圖片

自動產生的描述

圖12. 設置診斷的通知

一張含有 文字 的圖片

自動產生的描述

圖13. 對於VM上從效能到事件都做收集來為後續事件來做請命

一張含有 文字 的圖片

自動產生的描述

圖14. 針對診斷事件紀錄每個細項調整是否需要

一張含有 文字 的圖片

自動產生的描述

**如何透過 Antimalware 延伸模組開啟監視**

* 如需實際監視主機資安狀態則要透過 Antimalware PowerShell 來啟用診斷讓 VM 中 Antimalware Event 聚集。
* 透過設定 Azure 診斷延伸模組，從事件記錄檔來源 Microsoft Antimalware 擷取事件至 Azure Storage。其中包含錯誤，警告或詳細資訊等反惡意事件類型。  
  以下是 PowerShell 針對 VM 的範例：  
  PS C:> Add-AzureAccount  
  PS C:> Select-AzureSubscription -SubscriptionName “"  
  PS C:> $StorageContext = New-AzureStorageContext -StorageAccountName “" -StorageAccountKey (Get-AzureStorageKey -StorageAccountName “").Primary  
  PS C:> Set-AzureServiceAntimalwareExtension -ServiceName “" -Monitoring ON -StorageContext $StorageContext