技能解封中間章程-城池風險維安御林軍(Azure Security Center)

前言

<https://ithelp.ithome.com.tw/articles/10214085>

成本評估

**Azure Security Center 依下列定價面向計費：**

* 可透過 Azure Portal 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 1 |
| PostgreSQL (預覽) | 無法使用 | 免費 1 |
| 儲存體 – 保護訂用帳戶內的所有儲存體帳戶 3 | 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 3 | 無法使用 | NT$1.203/10,000 筆交易 2 |
| IoT 裝置 – 依裝置 | 無法使用 | NT$0.0301/月 4 |
| IoT 裝置 – 依訊息 | 無法使用 | NT$6.011/25,000 筆交易 4 |

1 顯示的定價為預覽價格。價格會在 GA 時變更。如需依資源分類的 ASC 功能詳細資料，請參閱資源專屬文件

2 選擇性儲存體帳戶的安全性變更將於 2020 年 1 月 1 日開始

3 Azure 資訊安全中心目前會保護 Azure Blob

4 (僅限預覽期間) 安全性訊息會根據客戶的 IoT 中樞配額來計算。

Azure Security Center Q&A

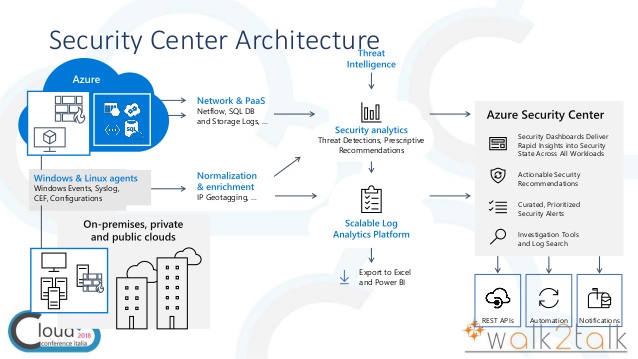
異常偵測器 API 的交易組成要素是什麼？

* 交易是 API 呼叫，其中在時間序列包含最大 1,000 個資料點的要求承載大小。
* 每累積 1,000 個資料點將計算為其他交易。舉例要求承載大小為 2050 個資料點的 API 呼叫會有 3 筆交易。要求承載大小的上限是 8,640 個資料點。時間序列中的每個資料點都是一組時間戳記/數值配對。

服務架構

* 原生就隸屬在 Azure 中的服務並不需要特別安裝 Agent，如像是 Azure PaaS 類型服務 SQL Database，Storage，WebApps等..都是由資訊安全中心做監視保護。
* 在 Windows 和 Linux 主機中則需要安裝 Microsoft Monitoring Agent，才可以啟動保護在雲端上或非 Azure 雲端中的企業內部實體或虛擬機器。Azure VM 則透過啟用連接就可以自動佈署讓資訊安全中心來做監視保護。

引用如下



簡易實測環境

圖1. 資訊安全中心總覽

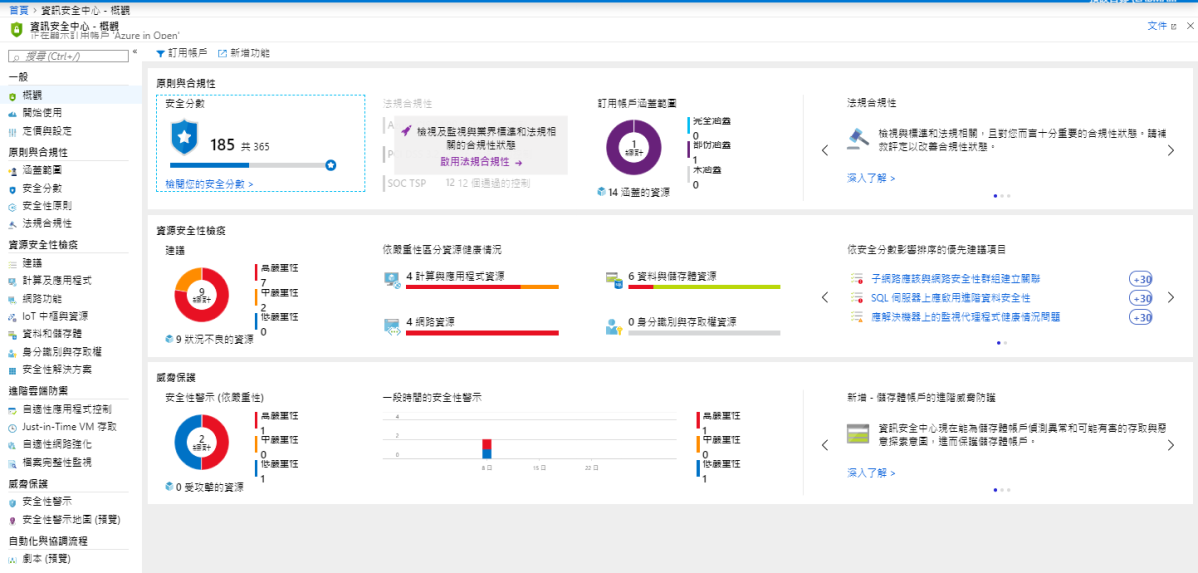


圖2. 法規層面功能是鎖住的(需要標準版)

一張含有 文字 的圖片

自動產生的描述

圖3. 選擇升級為標準版，有30天試用

一張含有 文字 的圖片

自動產生的描述

圖4. 監視過程還是需要有安裝Agent，同意安裝繼續

一張含有 文字 的圖片

自動產生的描述

圖5. 安裝完成訊息通知

一張含有 文字 的圖片

自動產生的描述

圖6. 法規合規性涵蓋四類目前均已解鎖此功能



圖7. 其中包含評定的結果狀況並都有相對應的建議做法

一張含有 文字 的圖片

自動產生的描述

圖8. 以下為建議作法步驟的展示

一張含有 文字 的圖片

自動產生的描述

圖9. 此為展示成功的畫面

一張含有 文字 的圖片

自動產生的描述

圖10. 可以針對這四種合規類型分別下載報告

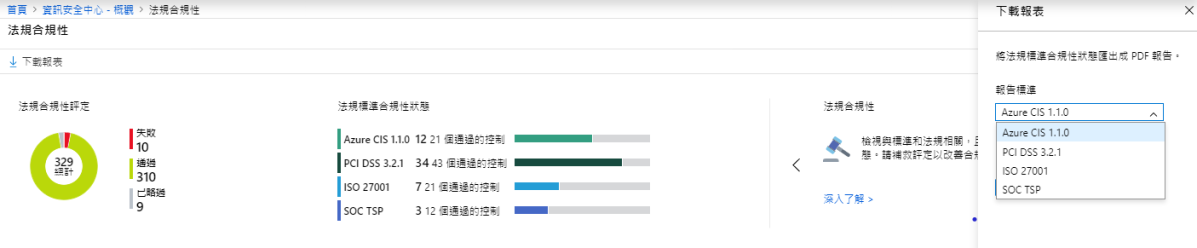


圖11. 報告形式如我所下載的範例

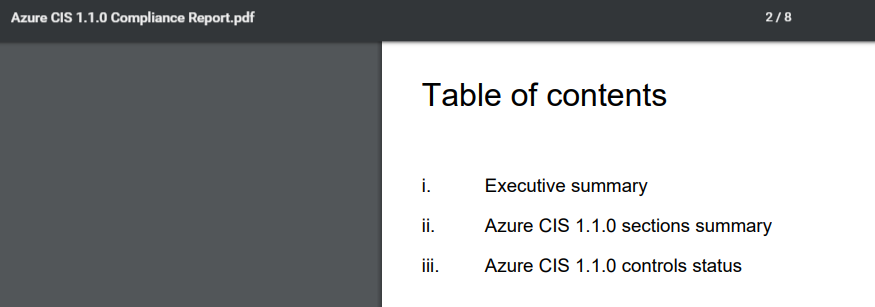


圖12. 裡面都有個別的完成狀態，可以夾帶給上級長官報告之用

一張含有 桌 的圖片

自動產生的描述

圖13. 以為示範除了建議外有些服務的建議是會直接帶的解決設置介面上(SQL為例)

一張含有 文字 的圖片

自動產生的描述

圖14. 設置SQL帳戶擁有AAD來做控管

一張含有 文字 的圖片

自動產生的描述

圖15. 設置完成(後續此項目就會是通過)

一張含有 文字 的圖片

自動產生的描述

圖16. 展示目前所有服務間的安全狀況一一列出(解決做法都如上述方式都有其引導)

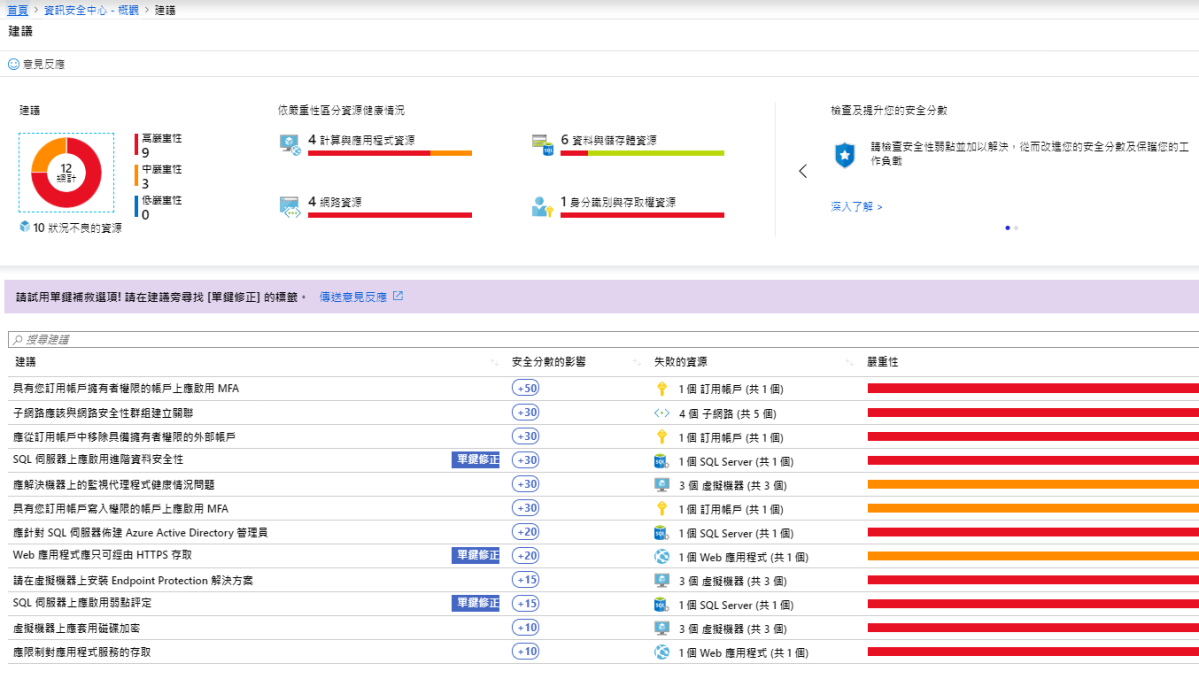


圖17. 另外在安全原則上也需要從免費設置成標準(威脅防護才會啟動)

一張含有 文字 的圖片

自動產生的描述

圖18. 檢視套用的訂閱以及Log分析上述的功能都已經為標準層

一張含有 文字 的圖片

自動產生的描述

圖19. 檢視網路狀態也有相對應的環形圖統計以及提醒的功能缺失建議改善



圖20. SQL 健康狀態亦同

一張含有 文字 的圖片

自動產生的描述

圖21. 此安全解決方案就可以綜觀透過以下功能來做更多監視的強化尤其如非Azure的機器也是能享有其保護監視權力



圖22. 透過原來Log分析的工作區新增一台地端主機試試

一張含有 文字 的圖片

自動產生的描述

圖23. 安裝Agent到所需的地端主機(版本自行確認)

一張含有 文字 的圖片

自動產生的描述

圖24. 開始安裝Agent

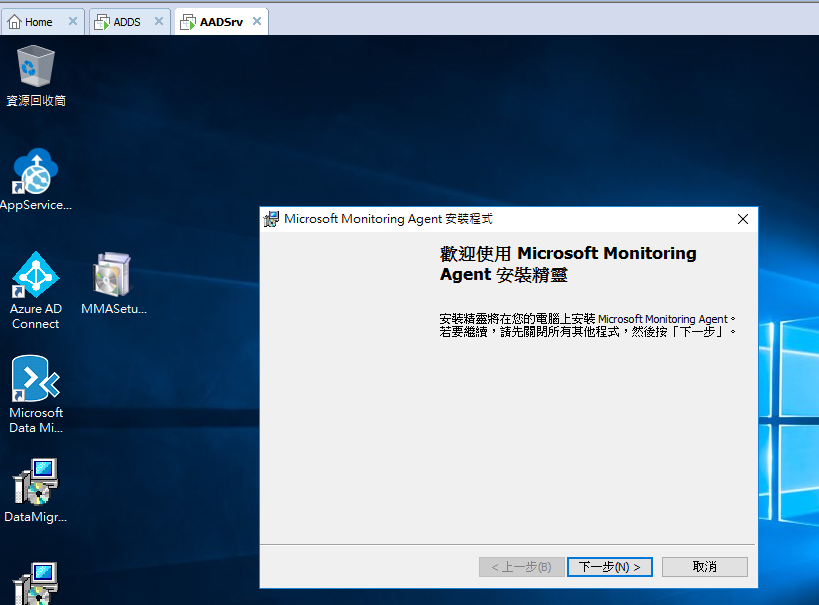


圖25. 安裝過程要把此主機資訊傳送至Azure Log 分析中

一張含有 文字, 監視器, 螢幕擷取畫面, 電子用品 的圖片

自動產生的描述

圖26. 包含工作區識別與金鑰

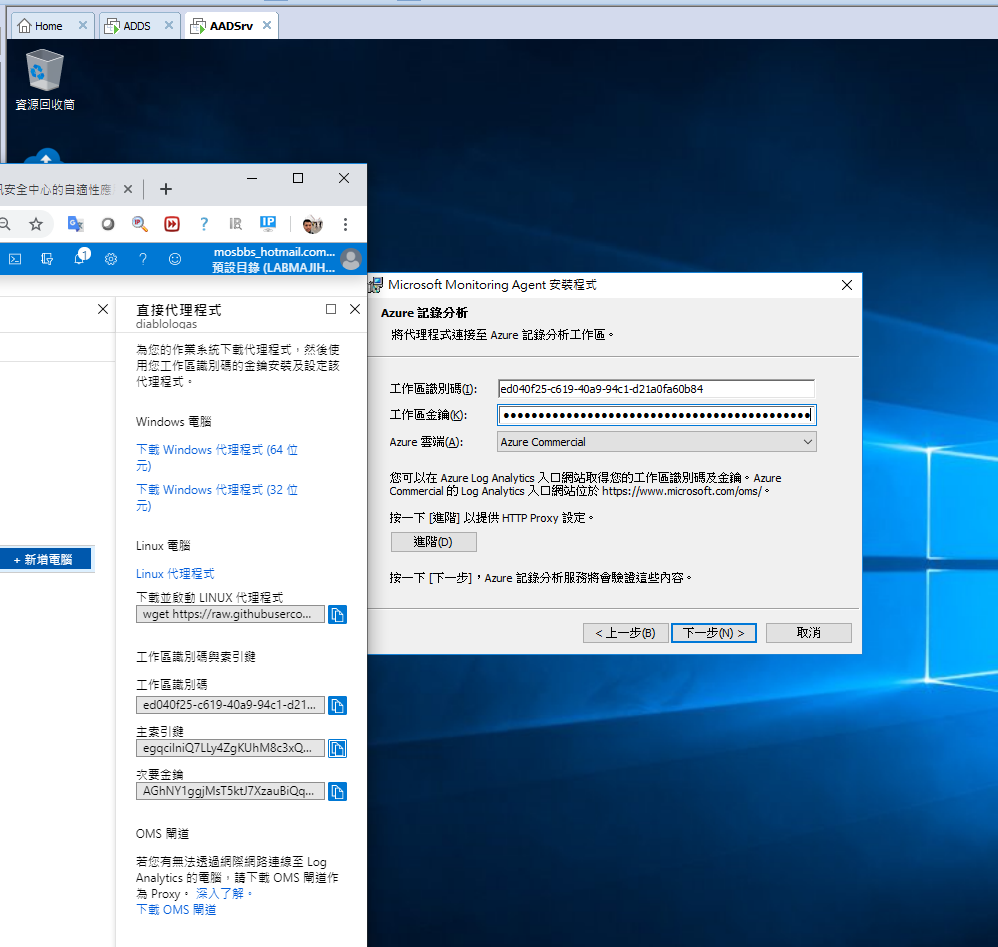


圖27. 上述通過後就可以開始安裝Agent

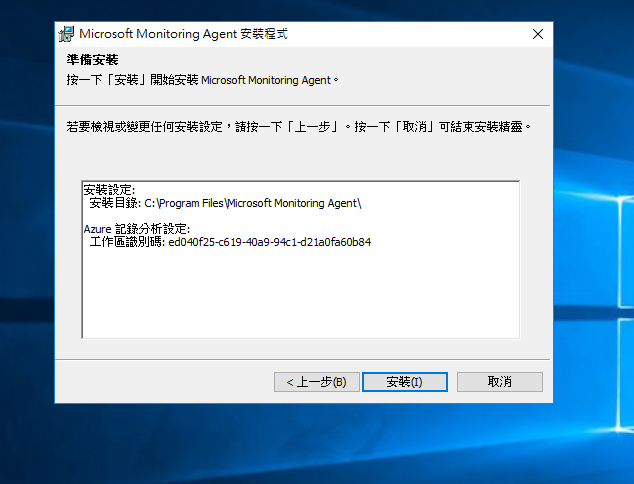


圖28. 安裝完成

一張含有 文字 的圖片

自動產生的描述

圖29. 以下就是安裝Agent後與安全中心註冊後的主機

一張含有 文字 的圖片

自動產生的描述

圖30. 一樣也有相關資訊狀態的建議(不過還是需要對照功能差異性，畢竟雲端支援的還是最完善)一張含有 文字 的圖片

自動產生的描述

圖31. JIT 也一直是指標功能

一張含有 文字 的圖片

自動產生的描述

圖32. 決定好你需要連線的Posts及連線時間後(從開啟那刻算)



圖33. 回到這台受到JIT保護的網路NSG的清單變化就很明顯看到以但時效過了就會用此Policy來阻擋

一張含有 桌 的圖片

自動產生的描述

圖34. 檔案完整可以包含機器本身的資料夾檔案路徑會是檔案本身受保護避免竄改

一張含有 文字 的圖片

自動產生的描述