



## **Azure Virtual Machine and Database Basic Protection**

# Azure Virtual Machine and Database Basic Protection

- ▶ 將地端應用程式系統遷移至 Azure 雲端的過程中，最常見的遷移方法便是使用與地端一致的架構 → PaaS，也就是透過使用 Azure Virtual Machine 雲端服務來取代既有地端的應用程式伺服器，Azure Virtual Machine 上將具備應用程式服務與資料庫服務，企業能體驗 Azure Virtual Machine 服務的 SLA、三份儲存體副本與基本的網路安全防護。然而，陸續發生 Virtual Machine 遭受勒索軟體的攻擊，不僅蒙受金錢與營運的損失，也危及服務商的商譽。
- ▶ 我們推出了 Azure VM and Database Basic Protection 服務，在最節省經費的狀況下，為您做好虛擬機器與資料庫的保護。

# 我們將為您完成

## Azure Virtual Machine 保護

- ▶ Azure Virtual Machine 安裝反惡意程式碼軟體
- ▶ Azure Backup for Azure Virtual Machine
- ▶ Azure 磁碟快照
- ▶ 更新管理 → 快速評估所有代理程式機器上可用更新的狀態，並管理為伺服器安裝必要更新的程序
- ▶ 自動化腳本服務中的 Runbook 負責安裝更新
- ▶ 部署 Log Analytics 代理程式進行合規性掃描
- ▶ 限制管理埠 (RDP、SSH) 來源 IP，可搭配即時 (JIT) VM 存取
- ▶ 更換預設 port

## SQL 資料庫保護

- ▶ Azure Backup for SQL Server
- ▶ SQL Server 備份至 URL
- ▶ 還原測試

# Azure VM 安全保護

---

- ▶ 安裝防毒軟體
- ▶ 系統安全更新
- ▶ 網路安全性
- ▶ .....

# 安裝防毒軟體(Windows)

您應安裝反惡意程式碼軟體，以協助識別及移除病毒、間諜軟體和其他惡意軟體

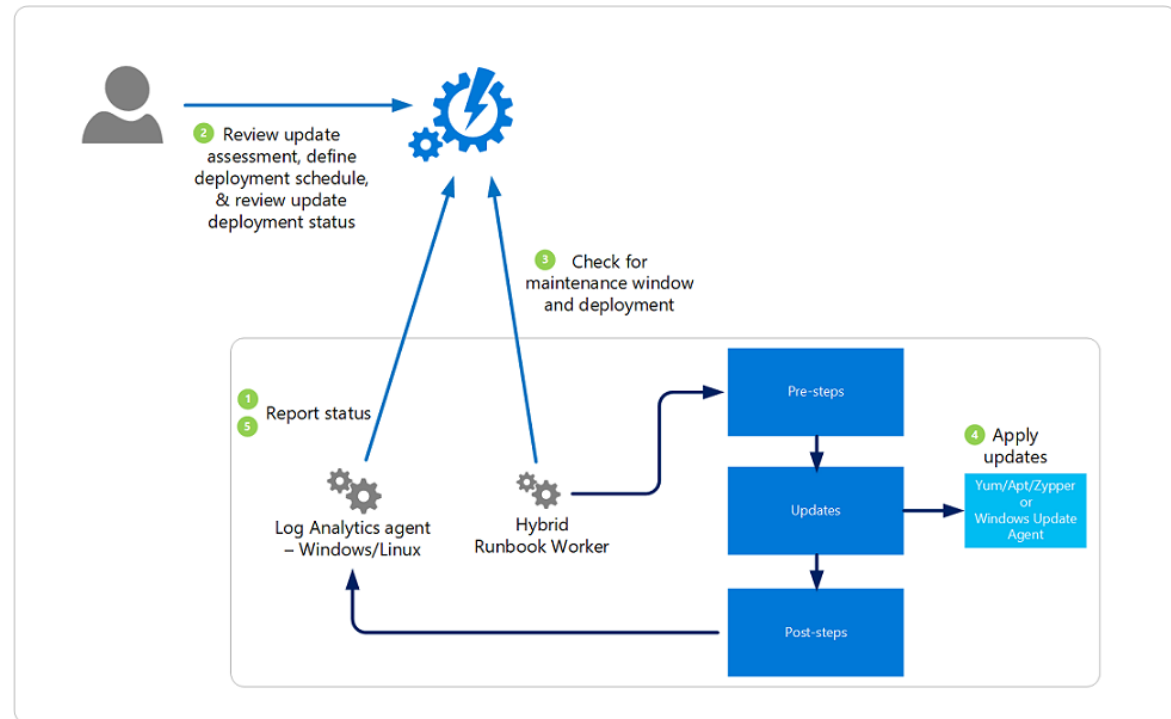
Microsoft AntiMalware



# 更新設定

快速評估所有代理程式機器上可用更新的狀態，並管理為伺服器安裝必要更新的程序。

部署Log Analytics 代理程式進行合規性掃描。  
自動化腳本服務中的Runbook 負責安裝更新。  
您無法檢視這些 Runbook 而其也不需要任何設定



# 網路安全性

攻擊者會針對開放管理埠持續掃描公用雲端 IP 範圍，並嘗試「簡單」的攻擊，例如常見密碼和已知未修補的弱點

限制管理埠 (RDP、SSH) 來源 IP，可搭配即時 (JIT) VM 存取(收費服務)

更換預設port

.....

sqlvm952

IP 設定 ①  
ipconfig1 (主要)

網路介面: sqlvm952 有效安全性規則 Troubleshoot VM connection issues 拓撲  
虛擬網路/子網路: sql-group-vnet/default NIC 公用 IP: 207.46.145.136 NIC 私人 IP: 10.0.1.4 加速的網路: 已停用

輸入連接埠規則 輸出連接埠規則 應用程式安全性組 負載平衡

網路安全性群組 SQLVM-nsg (連結到網路介面: sqlvm952)  
影響 0 個子網路, 1 個網路介面

優先順序	名稱	連接埠	通訊協定	來源	目的地
1300	RDP	3389	TCP	1.171.6.220	任何
310	Port_80	80	TCP	任何	任何
65000	AllowVnetInBound	任何	任何	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	任何	任何	AzureLoadBalancer	任何
65500	DenyAllInBound	任何	任何	任何	任何

首頁 > SQLVM

SQLVM | 執行命令 ...

SQLVM 虛擬機器

搜尋 (Ctrl+/)

屬性 鎖定 作業

塗墨 自動關機 備份 嚴重損壞修復 客體 + 主機更新 清查 變更追蹤 設定管理 (預覽) 原則 監視

執行命令指令碼

SetRDPPort

詳細資料  
Sets the default or user specific RDP port for the VM.

指令碼

參數

名稱: RDPPORT \* ①  
輸入值

執行

RunPowerShellS  
DisableNLA  
DisableWindows  
EnableAdminAc  
EnableEMS  
EnableRemoteP  
EnableWindows  
IPConfig  
RDPSettings  
ResetRDP  
SetRDPPort

# Azure VM 資料安全

## Azure OS 備份

- ▶ Azure Backup for Azure VM
- ▶ Azure Disk快照
- ▶ 第三方備份軟體

## Azure 資料備份

- ▶ Azure Backup for SQL server
- ▶ SQL Server 備份至 URL
- ▶ 第三方備份軟體

RTO/RPO

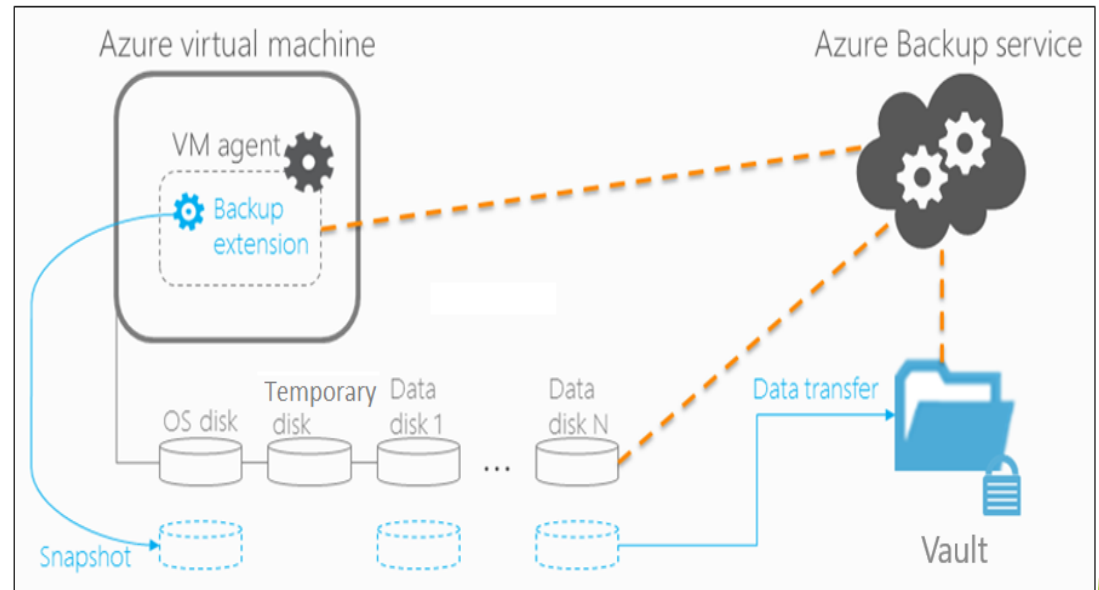


# Azure Backup for Azure VM

Azure 備份提供獨立、隔離的備份，以防止您的 VM 上發生非預期的資料損毀。備份會儲存在復原服務保存庫中，其具有內建的復原點管理功能

資料一致性，操作便利

按執行個體數目收取服務費用+存放資料的儲存費用



# Azure Backup for Azure VM計費

### Azure 備份

區域:  類型:

---

受保護的執行個體計算

VM ×  GB = \$300.54

---

備份原則

備份每日備份:  天  
備份每週備份:  週  
備份每月備份:  月  
備份每年備份:  年

備份立即響應恢復:  天

---

備份儲存體資料特性

平均每日資料量:  備種:

---

儲存體費用計算

平均每月備份資料	189 GB	= \$255.82
平均每月快照集使用量資料	3 GB	= \$13.07

如需詳細的年度和月份估計 (包括趨勢), 請參閱 <https://aka.ms/AzureBackupDetailedEstimates>

預付費用	\$0.00
每個月的成本	\$569.44

# Azure Disk快照

快照集是完整的虛擬硬碟 (VHD) 唯讀複本,建議您完全關閉 VM 後再建立快照集，以清除所有進行中的處理序。

雖然您可以隨時擷取快照集，但如果 VM 正在執行，仍然會有資料串流處理到磁碟。快照集所包含的部分作業可能在進行傳輸。此外，如果涉及多個磁碟，則可能在不同時間發生不同磁碟的快照集。這些案例可能會導致快照集未經協調。這種缺乏協調的狀況對於等量磁碟區而言會特別有問題，如果在備份期間發生變更，其中所包含的檔案可能會損毀。

## 省錢

資料可能不完整，排程處理目前為預覽階段

# Azure Disk快照計費

受控磁碟的快照收費按照磁碟等級、LRS還是ZRS選項收費，按照磁碟中實際的資料大小收取

例如：如果您創建了一個受控磁碟的快照，該快照具有128GB的容量和10GB的實際使用數據大小，那麼只會為10GB的使用數據大小快照。

如果建立增量快照集，按照實際增加的資料收費儲存費用。

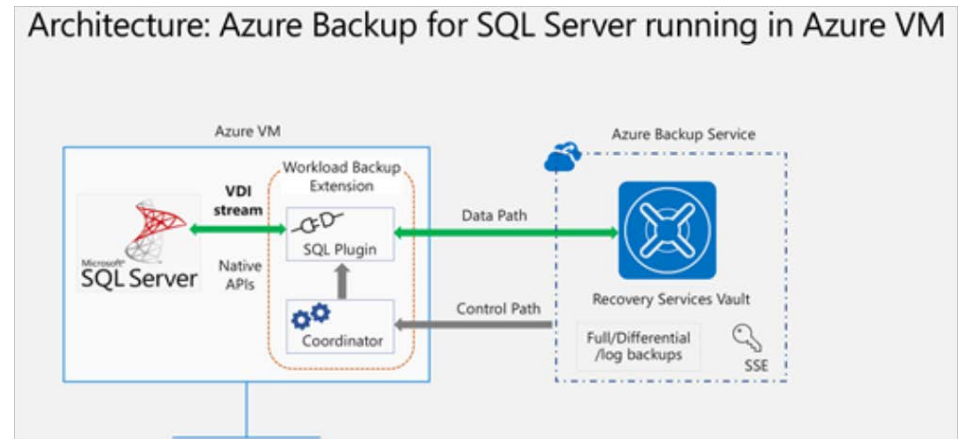
例如：您所用的磁碟的佈建大小為128 GB，並使用了100 GB。第一個增量快照收集只會收取已使用大小100 GB的費用。在您建立第二個快照集之前，磁碟上增加了20 GB的資料。第二個增量快照集只會收回20 GB的費用。

# Azure Backup for SQL Server

支援所有備份類型的工作負載  
感知備份-完整、差異和  
記錄

15分鐘 RPO (復原點目標)  
頻繁的記錄備份

時間點復原，最多可達一秒  
個別資料庫層級的備份與還原



# Azure Backup for SQL Server計費

### Azure 備份

區域:  選擇:

---

#### 受保護的執行個體計算

×  GB

= \$1,164.60

---

#### 備份原則

Azure 備份提供 Azure VM 上的 SQL Server 的完整、差異和記錄備份功能。基於備份儲存體預估的目的，我們會根據您的保留需求選擇最佳的原則類型。如需詳細的估計，請參閱 <https://aka.ms/AzureBackupDetailedEstimates>

保留每日備份:  天  
保留每週備份:  週  
保留每月備份:  月  
保留每年備份:  年  
保留記錄備份:  天

---

#### 備份儲存體資料特性

平均每日資料更換:  備運:

---

#### 儲存體費用計算

平均每月備份資料  GB = \$500.20

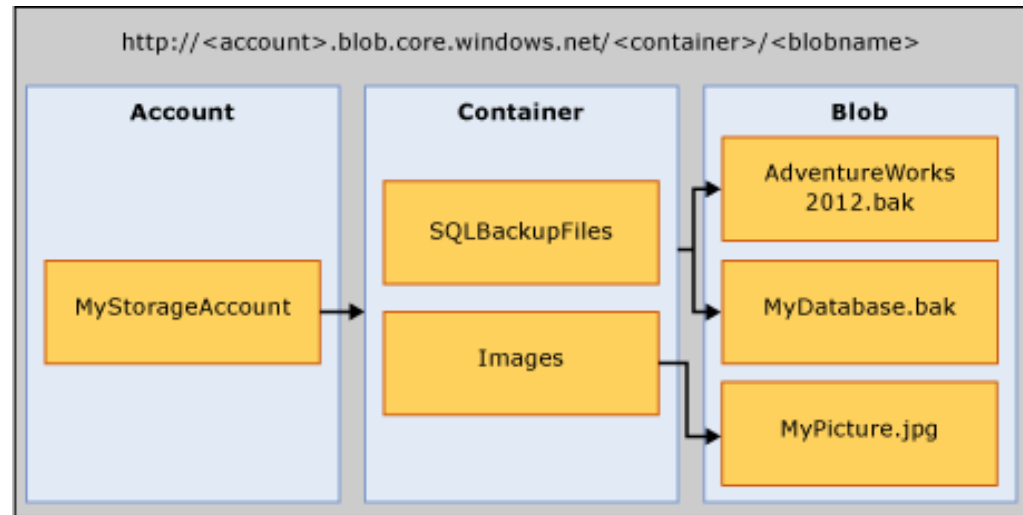
如需詳細的年度和月份估計 (包括趨勢)，請參閱 <https://aka.ms/AzureBackupDetailedEstimates>

預付費用	\$0.00
每個月的成本	\$1,664.80

# SQL Server 備份至 URL

認證中使用儲存體金鑰，則會使用分頁 Blob 存放，僅能在 SQL Server 2014 或更新版本中使用。

如果使用共用存取簽章，就會使用區塊 Blob，僅能在 SQL Server 2016 或更新版本中使用。



# SQL Server 備份至 URL 計費

SQL Server 備份至 URL 只是將 Azure 儲存體當做一個存放空間，收費按照儲存體的定價收取

<https://azure.microsoft.com/zh-tw/pricing/details/storage/page-blobs/>

<https://azure.microsoft.com/zh-tw/pricing/details/storage/blobs/>



