技能解封初始篇章-堡壘前線 (Bastion)

**前言**

原本在非戰區中孤獨生活的主機(俗稱跳板機或Jumpbox)仍舊還是有SLA的高風險需要投入人力做管理。

Azure Bastion 的誕生，完全受控 PaaS 服務，可讓你直接透過 Azure Portal，對虛擬機器支援安全RDP 和 SSH 安全存取連線。

Azure Bastion 會直接佈建您的虛擬網路(VNet)中，並支援使用 SSL 的所有虛擬機器，而沒有任何透過公用 IP 位址的暴露風險。

經強化的單一存取點，存取虛擬網路內的所有虛擬機器。防禦主機作為主要公開存取，有助降低在網際網路流竄暴露的風險，並限制連接埠掃描及其他以虛擬機器為目標的惡意程式碼威脅等。

預覽階段能實測的地區

小弟就選擇的美東地區，不為什麼就只是成本相對低廉前兩名。

一張含有 文字 的圖片

自動產生的描述

成本評估

| 美東為例 | | 價格 | |
| --- | --- | --- | --- |
| Azure Bastion | | 每小時 NT$2.856 | |
| 輸出資料傳輸 | 區域 11 | | 區域 21 |
| 前 5 GB/月 | 免費 | | 免費 |
| 5 GB – 10 TB2/月 | 每 GB NT$1.3074 | | 每 GB NT$1.8033 |
| 之後的 40 TB (10 TB – 50 TB)/月 | 每 GB NT$1.2473 | | 每 GB NT$1.2774 |
| 之後的 100 TB (50 TB – 150 TB)/月 | 每 GB NT$1.0519 | | 每 GB NT$1.2323 |
| 之後的 350 TB (150 TB – 500 TB)/月 | 每 GB NT$0.7514 | | 每 GB NT$1.2022 |
| 超過 500 TB/月 | [與我們連絡](https://azure.microsoft.com/zh-tw/overview/sales-number/) | | [與我們連絡](https://azure.microsoft.com/zh-tw/overview/sales-number/) |

區域 1 和區域 2 分別是對應到哪些地區？

子地區是您選擇部署應用程式和相關資料的最低層級地理位置。資料傳輸 (CDN 除外)「區域 1」和「區域 2」對應的地區如下：

* **區域 1** – 西歐，美國東部，美國中南部，美國西部
* **區域 2** – 澳洲東部，日本東部

簡易環境示範

圖1. 預覽期間尚未正式能透過Azure Portal能夠找到，則需要透過此URL Preview連結

<https://aka.ms/BastionHost>

一張含有 文字 的圖片

自動產生的描述

圖2. 在新增Marketplace服務搜尋"Bastion"

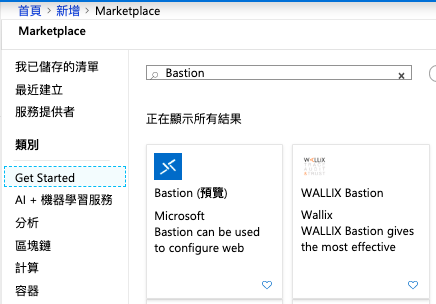


圖3. 選擇建立

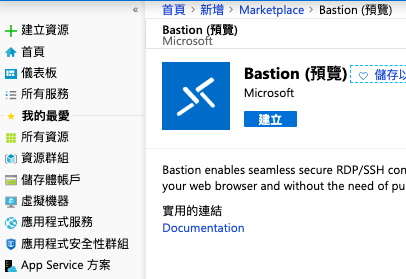


圖4. 建立前有個重點是子網路請用以下固定名稱AzureBastionSubnet，其他包含地區與公用IP指定好即可

一張含有 文字 的圖片

自動產生的描述

圖5. 建立完成後 Bastion 介面樣貌(包含到所顯示對外的 DNS FQDN)

一張含有 文字 的圖片

自動產生的描述

圖6. 接下來把我們熟悉的 VM 對外公用 IP 直接關閉

一張含有 文字 的圖片

自動產生的描述

圖7. 點選連線原來的 RDP 所能連線只剩下 Private IP 並無法從網際網路連線

一張含有 文字 的圖片

自動產生的描述

圖8. 我們看到了一個特別的字眼 “Bastion" 並打上您原本設置的 VM 登入本機帳密

一張含有 文字 的圖片

自動產生的描述

圖9. 就透過瀏覽器分頁 HTML 5 技術遠端桌面連線中，並且旁邊有個可以從地端的檔案文字複製到此Clipboard(看起來是暫存之用)

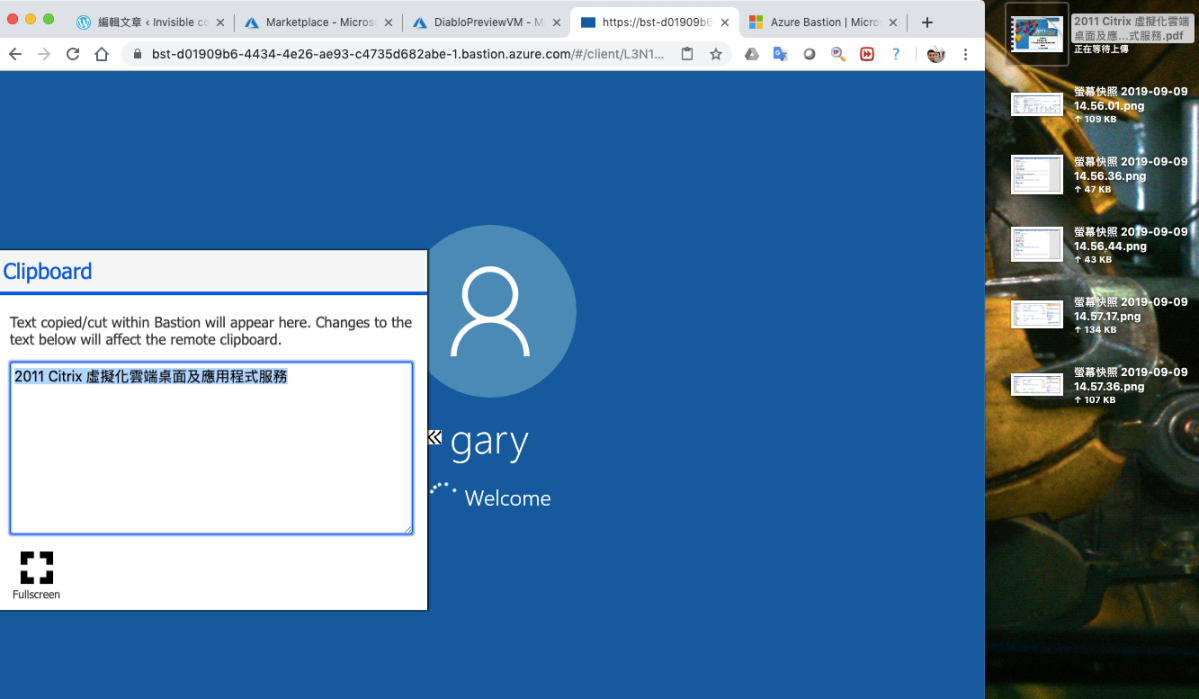


圖10. 已經正常登入進去沒有問題，另外補充上述剪貼簿這件事的確直接從地端複製文字到雲端ＶＭ主機內的文字檔案是不行的，透過剛剛以暫存的剪貼簿上內文則是沒有問題(忘記截圖所以只能口述一下．．．．．)

一張含有 文字, 螢幕擷取畫面, 監視器, 螢幕 的圖片

自動產生的描述