

設置 Azure 同服器

在 Microsoft Azure 上設置服務器並配置其以打開特定端口對於各種應用程序（包括託管服務、代理等）至關重要。本指南將引導您完成創建 Azure 虛擬機（VM）並配置防火牆以打開端口 1080 的過程。

目錄

1. 先決條件
2. 創建 Azure 虛擬機
3. 配置防火牆以打開端口 1080
4. 測試配置
5. 結論

先決條件

在開始之前，請確保您具備以下條件：

- 一個有效的Microsoft Azure帳戶。
- 使用 Azure Portal 的基本知識。
- 用於訪問 VM 的 SSH 客戶端（如 macOS/Linux 上的 Terminal 或 Windows 上的 PuTTY）。

創建 Azure 虛擬機

1. 登錄 Azure Portal：導航至 Azure Portal 並使用您的憑據登錄。
2. 創建新的虛擬機：
 - 點擊左上角的“創建資源”。
 - 從可用資源列表中選擇“虛擬機”。
3. 配置 VM 基礎設置：
 - 訂閱：選擇您的 Azure 訂閱。
 - 資源組：創建新的資源組或選擇現有的資源組。
 - 虛擬機名稱：為您的 VM 輸入名稱（例如 AzureServer）。
 - 區域：選擇最接近目標受眾的區域。

- 映像：選擇操作系統映像（例如 Ubuntu 22.04 LTS）。
- 大小：根據您的性能需求選擇 VM 大小。
- 身份驗證：選擇 SSH 公鑰以進行安全訪問。上傳您的 SSH 公鑰。

4. 配置網絡：

- 確保 VM 放置在適當的虛擬網絡和子網中。
- 啟用公共 IP 以允許外部訪問。

5. 審查並創建：

- 審查您的配置。
- 點擊 “創建” 以部署 VM。部署可能需要幾分鐘。

配置防火牆以打開端口 1080

一旦您的 VM 啟動並運行，您需要配置 Azure 的網絡安全組（NSG）以允許端口 1080 上的流量。

1. 導航至您的 VM 的網絡設置：

- 在 Azure Portal 中，轉到 “虛擬機”。
- 選擇您的 VM（AzureServer）。
- 點擊左側邊欄中的 “網絡”。

2. 識別網絡安全組（NSG）：

- 在 “網絡接口” 下，找到相關的 NSG。
- 點擊 NSG 以管理其規則。

3. 添加入站安全規則：

- 在 NSG 設置中，轉到 “入站安全規則”。
- 點擊 “添加” 以創建新規則。

4. 配置規則：

- 源：任何（或指定範圍以增強安全性）。
- 源端口範圍：*
- 目標：任何
- 目標端口範圍：1080
- 協議：TCP
- 操作：允許
- 優先級：1000（確保它不與現有規則衝突）。

- 名稱：Allow-1080-TCP

5. 保存規則：

- 點擊 “添加” 以應用新規則。

測試配置

配置防火牆後，必須驗證端口 1080 是否打開並可訪問。

1. 使用 Telnet 驗證端口可訪問性：從本地機器運行：

```
telnet <您的 VM_IP> 1080
```

- 將 < 您的 VM_IP> 替換為您的 VM 的公共 IP 地址。
- 如果連接成功，則端口已打開並可訪問。

2. 替代端口檢查工具：

- Netcat (nc)：

```
nc -zv <您的 VM_IP> 1080
```

- 在線端口檢查器：使用在線服務如canyouseeme.org檢查端口 1080 是否打開。

3. 故障排除：

- 連接問題：驗證 NSG 規則是否正確設置，並且 VM 上的任何本地防火牆都配置為允許端口 1080 上的流量。
- 錯誤的 IP：確保您使用的是 VM 的正確公共 IP 地址。

結論

通過遵循本指南，您已成功設置了 Azure 虛擬機並配置了防火牆以打開端口 1080。此設置為部署需要特定端口訪問的各種應用程序或服務奠定了基礎。

如需進一步配置，例如在端口 1080 上設置代理服務或其他應用程序，請參閱我們關於 V2Ray 代理設置和生成自定義 vmess URL 的專用文章。