

Einrichten eines Azure-Servers

Das Einrichten eines Servers auf Microsoft Azure und die Konfiguration, um bestimmte Ports zu öffnen, ist für verschiedene Anwendungen unerlässlich, einschließlich Hosting-Diensten, Proxys und mehr. Diese Anleitung führt Sie durch den Prozess der Erstellung einer Azure Virtual Machine (VM) und der Konfiguration der Firewall, um Port 1080 zu öffnen.

Inhaltsverzeichnis

1. Voraussetzungen
2. Erstellen einer Azure Virtual Machine
3. Konfigurieren der Firewall, um Port 1080 zu öffnen
4. Testen der Konfiguration
5. Fazit

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie Folgendes haben:

- Ein aktives Microsoft Azure-Konto.
- Grundkenntnisse in der Verwendung des Azure-Portals.
- Ein SSH-Client (wie Terminal auf macOS/Linux oder PuTTY auf Windows) für den Zugriff auf die VM.

Erstellen einer Azure Virtual Machine

1. Melden Sie sich beim Azure-Portal an: Navigieren Sie zum Azure-Portal und melden Sie sich mit Ihren Anmeldedaten an.
2. Erstellen Sie eine neue virtuelle Maschine:
 - Klicken Sie in der oberen linken Ecke auf „Ressource erstellen“.
 - Wählen Sie „Virtuelle Maschine“ aus der Liste der verfügbaren Ressourcen aus.
3. Konfigurieren Sie die grundlegenden Einstellungen der VM:
 - Abonnement: Wählen Sie Ihr Azure-Abonnement aus.

- Ressourcengruppe: Erstellen Sie eine neue Ressourcengruppe oder wählen Sie eine bestehende aus.
- Name der virtuellen Maschine: Geben Sie einen Namen für Ihre VM ein (z. B. AzureServer).
- Region: Wählen Sie die Region aus, die Ihrem Zielpublikum am nächsten liegt.
- Image: Wählen Sie ein Betriebssystem-Image aus (z. B. Ubuntu 22.04 LTS).
- Größe: Wählen Sie eine VM-Größe basierend auf Ihren Leistungsanforderungen aus.
- Authentifizierung: Wählen Sie den SSH-Public-Key für einen sicheren Zugriff. Laden Sie Ihren öffentlichen SSH-Schlüssel hoch.

4. Netzwerkkonfiguration:

- Stellen Sie sicher, dass die VM in das richtige virtuelle Netzwerk und Subnetz platziert wird.
- Lassen Sie die öffentliche IP-Adresse aktiviert, um externen Zugriff zu ermöglichen.

5. Überprüfen und Erstellen:

- Überprüfen Sie Ihre Konfigurationen.
- Klicken Sie auf "Erstellen", um die VM bereitzustellen. Die Bereitstellung kann einige Minuten dauern.

Konfiguration der Firewall zur Freigabe von Port 1080

Sobald Ihre VM betriebsbereit ist, müssen Sie die Netzwerksicherheitsgruppe (NSG) von Azure konfigurieren, um Datenverkehr auf Port 1080 zuzulassen.

1. Navigieren Sie zu den Netzwerkeinstellungen Ihrer VM:

- Gehen Sie im Azure-Portal zu "Virtuelle Maschinen".
- Wählen Sie Ihre VM (AzureServer) aus.
- Klicken Sie in der linken Seitenleiste auf "Netzwerk".

2. Identifizieren Sie die Netzwerksicherheitsgruppe (NSG):

- Unter "Netzwerkschnittstelle" finden Sie die zugehörige NSG.
- Klicken Sie auf die NSG, um ihre Regeln zu verwalten.

3. Fügen Sie eine eingehende Sicherheitsregel hinzu:

- Gehen Sie in den NSG-Einstellungen zu "Eingehende Sicherheitsregeln".

- Klicken Sie auf “Hinzufügen”, um eine neue Regel zu erstellen.

4. Regel konfigurieren:

- Quelle: Beliebig (oder geben Sie einen Bereich für erhöhte Sicherheit an).
- Quellportbereiche: *
- Ziel: Beliebig
- Zielportbereiche: 1080
- Protokoll: TCP
- Aktion: Zulassen
- Priorität: 1000 (stellen Sie sicher, dass sie nicht mit bestehenden Regeln in Konflikt steht).
- Name: Allow-1080-TCP

5. Regel speichern:

- Klicken Sie auf “Hinzufügen”, um die neue Regel anzuwenden.

Testen der Konfiguration

Nach der Konfiguration der Firewall ist es wichtig, zu überprüfen, ob Port 1080 geöffnet und zugänglich ist.

1. Verwenden Sie Telnet, um die Port-Erreichbarkeit zu überprüfen: Führen Sie auf Ihrem lokalen Rechner den folgenden Befehl aus:

```
telnet <Ihre_VM_IP> 1080
```

- Ersetzen Sie <YOUR_VM_IP> durch die öffentliche IP-Adresse Ihrer VM.
- Wenn die Verbindung erfolgreich ist, ist der Port offen und erreichbar.

2. Alternative Port-Checking-Tools:

- Netcat (nc):

```
nc -zv <YOUR_VM_IP> 1080
```

- Online-Port-Checker: Verwenden Sie Online-Dienste wie canyouseeme.org, um zu überprüfen, ob Port 1080 geöffnet ist.

3. Fehlerbehebung:

- Verbindungsprobleme: Überprüfen Sie, ob die NSG-Regeln korrekt eingerichtet sind und dass alle lokalen Firewalls auf der VM so konfiguriert sind, dass sie Datenverkehr auf Port 1080 zulassen.
- Falsche IP: Stellen Sie sicher, dass Sie die korrekte öffentliche IP-Adresse Ihrer VM verwenden.

Fazit

Indem Sie dieser Anleitung gefolgt sind, haben Sie erfolgreich eine Azure Virtual Machine eingerichtet und die Firewall so konfiguriert, dass Port 1080 geöffnet ist. Diese Einrichtung bildet die Grundlage für die Bereitstellung verschiedener Anwendungen oder Dienste, die einen spezifischen Portzugriff erfordern.

Für weitere Konfigurationen, wie das Einrichten von Proxy-Diensten oder anderen Anwendungen auf Port 1080, lesen Sie unsere speziellen Beiträge zu V2Ray-Proxy-Einrichtung und Erstellen einer benutzerdefinierten vmess-URL.