

在 Azure 上搭建服务器

在 Microsoft Azure 上搭建服务器并配置开放特定端口对于各种应用程序至关重要，包括托管服务、代理等。本文将引导您完成创建 Azure 虚拟机 (VM) 以及配置防火墙以开放 1080 端口的过程。

目录

1. 前提条件
2. 创建 Azure 虚拟机
3. 配置防火墙以开放 1080 端口
4. 测试配置
5. 结论

前提条件

在开始之前，请确保您具备以下条件：

- 一个活跃的 Microsoft Azure 账户。
- 使用 Azure 门户的基本知识。
- SSH 客户端（如 macOS/Linux 上的终端或 Windows 上的 PuTTY）用于访问虚拟机。

创建 Azure 虚拟机

1. 登录 Azure 门户：打开 Azure 门户，并使用您的凭据登录。
2. 创建新的虚拟机：
 - 点击左上角的“创建资源”。
 - 从可用资源列表中选择“虚拟机”。
3. 配置虚拟机基本信息：
 - 订阅：选择您的 Azure 订阅。
 - 资源组：创建一个新的资源组或选择现有资源组。
 - 虚拟机名称：输入您的虚拟机名称（例如，AzureServer）。
 - 区域：选择最接近您的目标受众的区域。
 - 镜像：选择操作系统镜像（例如，Ubuntu 22.04 LTS）。
 - 大小：根据您的性能需求选择虚拟机大小。
 - 身份验证：选择 SSH 公钥以实现安全访问。上传您的公共 SSH 密钥。
4. 配置网络：
 - 确保虚拟机位于适当的虚拟网络和子网中。

- 保持公共 IP 启用以允许外部访问。

5. 审查并创建：

- 审查您的配置。
- 点击“创建”部署虚拟机。部署可能需要几分钟时间。

配置防火墙以开放 1080 端口

虚拟机启动并运行后，您需要配置 Azure 的网络安全组 (NSG) 以允许 1080 端口的流量。

1. 导航到虚拟机的网络设置：

- 在 Azure 门户中，转到“虚拟机”。
- 选择您的虚拟机 (AzureServer)。
- 点击左侧边栏的“网络”。

2. 识别网络安全组 (NSG)：

- 在“网络接口”下，找到相关的 NSG。
- 点击 NSG 以管理其规则。

3. 添加入站安全规则：

- 在 NSG 设置中，转到“入站安全规则”。
- 点击“添加”创建新规则。

4. 配置规则：

- 来源：任何（或指定范围以增强安全性）。
- 来源端口范围：*
- 目标：任何
- 目标端口范围：1080
- 协议：TCP
- 操作：允许
- 优先级：1000（确保不与现有规则冲突）。
- 名称：Allow-1080-TCP

5. 保存规则：

- 点击“添加”应用新规则。

测试配置

配置防火墙后，验证 1080 端口是否已开放并可访问至关重要。

1. 使用 Telnet 验证端口可访问性：从本地计算机运行：

```
telnet <YOUR_VM_IP> 1080
```

- 将 <YOUR_VM_IP> 替换为您的虚拟机公网 IP 地址。

- 如果连接成功，表示端口已开放且可访问。

2. 替代的端口检查工具：

- Netcat (nc)：

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

- 在线端口检查工具：使用像 canyouseeme.org 这样的在线服务检查 1080 端口是否开放。

3. 故障排除：

- 连接问题：验证 NSG 规则是否正确设置，并且虚拟机上的本地防火墙已配置允许 1080 端口的流量。
- IP 地址错误：确保您使用的是虚拟机的正确公网 IP 地址。

结论

通过本指南，您已成功在 Azure 上搭建了虚拟机并配置防火墙开放了 1080 端口。此设置为部署需要特定端口访问的各种应用程序或服务奠定了基础。

欲了解更多配置，例如在 1080 端口上设置代理服务或其他应用程序，请参阅我们专门的 [V2Ray 代理设置](#) 和 [生成自定义 vmess URL](#) 文章。