AWS Marketplace: Private Network Connector Deployment Prerequisites

Before deploying a Windows EC2 instance and Entra Private Network Connector, ensure that you meet the pre-requisites listed below. These steps are crucial for the Connector VM's functionality and the deployment's success within the AWS environment.

Start with securing an offline Entra Access token and TenantID. Instructions provided below under **Prerequisites (Entra Configuration).** Access tokens are required for connector registration, especially if MFA is enabled on your Entra Tenant. Also retrieve your TenantID from the Entra Admin Center's "Identity" tab under "Overview".

In addition, you need to configure your EC2 environment to ensure that connector has outbound connectivity needed for its operation, under **Prerequisites (Network and EC2 Configuration)**. No inbound connectivity is necessary. You can either use existing VPC and Subnet or create a new one. **Instructions for creating a new VPC and Subnet are provided below if needed**. You can skip these instructions if you are using existing VPC and Subnet. In either case, please Ensure the Connector VM has outbound internet connectivity.

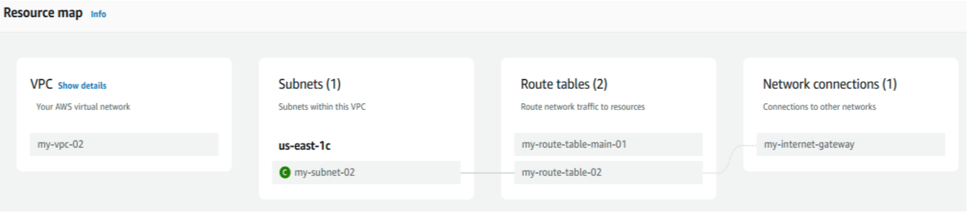
Prerequisites (Entra Configuration)

1. Entra TenantID:
   - Locate your TenantID in the Entra Admin Center.
   - Go to the "Identity" tab and click on "Overview".
   - Copy and securely store the TenantID for use during deployment.
   - These steps will ensure you have the required credentials ready for the connector deployment.

2. Access Token:
   - Obtain an offline access token to register the connector.
   - Use the sample PowerShell script at the Get-Token documentation link (https://learn.microsoft.com/entra/global-secure-access/powershell-samples).
   - Save the script as "Get-Token.ps1" on your local machine.
   - Run the script in an elevated PowerShell window on a Windows machine without a prior installation of the Private Network Connector.
   - The script will generate a Token for you to input during registration. Follow the prompts on the PowerShell Window for Token Details.
   - If your Entra Tenant has MFA enabled, the access token is necessary for registration.

Prerequisites (Network and EC2 Configuration)

1. Existing VPC and Subnet: The deployment requires an existing Virtual Private Cloud (VPC) and a designated Subnet within the AWS infrastructure.
    a. Create a VPC; For VPC Settings:
        i. Resources to created: VPC only
        ii. IPv4 CIDR block: IPv4 CIDR manual input
        iii. IPv4 CIDR: 10.0.0.0/24
        iv. IPv6 CIDR block: No IPv6 CIDR block
    b. Create a subnet; Subnet Settings:
        i. VPC ID: Assign the VPC just created
        ii. Availability Zone: Chose the availability zone
        iii. IPv4 VPC CIDR block: 10.0.0.0/24
        iv. IPv4 subnet CIDR block: 10.0.0.0/28 (minimum /28 recommended)
        v. Click "Create Subnet"
    c. Modify Subnet's IP addressing behavior
        i. Select your subnet and choose Actions, Edit subnet settings.
        ii. Check the **Enable auto-assign public IPv4 address** check box, and then choose Save.
2. Create a new Internet Gateway
    a. An Internet Gateway (IGW) is a component that allows communication between instances in your VPC and the internet. It serves as a target for traffic destined for the internet.
3. Attach Internet Gateway to the VPC
    a. Next assign the internet gateway to the VPC so it can route the internet traffic appropriately.
4. Create a Route Table
5. Create a Route in Route Table
    a. *Add a route in the route table above that points to the Internet Gateway created above. This route effectively tells the VPC how to route traffic destined for the internet—any traffic matching this route will be sent out through the Internet Gateway. E.g., parameters below.*
        i. **Destination**: `0.0.0.0/0` (this matches all IP addresses)
        ii. **Target**: [Internet Gateway ID]
    b. Select the Route table ID-> click the route table-> click "edit routes"-> click "add route"-> Destination: "::/0" -> Target: "Internet Gateway" -> Type in the ID of the Internet Gateway you created (i.e. "igw-xxxxxxxxxxxxxxxxx")-> click "Save changes"

6. Assocaite Route Table with Subnet
    a. Go back to your Subnets, click on the subnet you created
    b. Go to route table tab-> click on “edit route table association”-> “Route table ID”: click the route table you just created-> select “Save”
7. Click your VPC and your resource map should look like below. Note that your resource names could be different than what is in picture below.
    a. 
Resource map Info
VPC Show details
Your AWS virtual network
my-vpc-02
Subnets (1)
Subnets within this VPC
us-east-1c
my-subnet-02
Route tables (2)
Route network traffic to resources
my-route-table-main-01
my-route-table-02
Network connections (1)
Connections to other networks
my-internet-gateway