**AWS Systems Manager Session Manager Setup Guide**

**1. Prerequisites**

Ensure you have the following in place:

* A VPC with both public and private subnets.
* An EC2 instance in the private subnet.
* An EC2 instance in the public subnet.
* IAM roles with the necessary permissions.

**2. Create VPC with Public and Private Subnets**

* **VPC Creation:**
  + Create a new VPC or use an existing one with a CIDR block, e.g., 10.0.0.0/16.
* **Subnets:**
  + Public Subnet: Create a public subnet with a CIDR block, e.g., 10.0.1.0/24, and associate it with a route table that has an Internet gateway (IGW) route.
  + Private Subnet: Create a private subnet with a CIDR block, e.g., 10.0.2.0/24, and ensure the route table that has an NAT gateway (NAT) to the internet.

**3. Create EC2 Instance in Private Subnet**

* **Launch an EC2 Instance:**
  + Launch an EC2 instance in the private subnet using a supported AMI (Amazon Linux, Ubuntu etc.).
* **Assign IAM Role:**
  + Ensure that the IAM Role assigned to the EC2 instance has the following permissions to connect the other tools like s3:
    - **AmazonSSMManagedInstanceCore**: Enables SSM agent communication with Systems Manager.
    - **AdministratorAccess**: Grants full access to all AWS services.
    - **AmazonEC2FullAccess**: Specifically for managing EC2 instances.
    - **AmazonSSMFullAccess**: Grants full permissions to manage and use all AWS Systems Manager services.
    - **AmazonEC2RoleforSSM**: Grants necessary permissions to allow EC2 instances to communicate with SSM and perform necessary tasks.
* **Trust Relationship:**

**json**

**{**

**"Version": "2012-10-17",**

**"Statement": [**

**{**

**"Effect": "Allow",**

**"Principal": {**

**"Service": [**

**"backup.amazonaws.com",**

**"ssm.amazonaws.com",**

**"ec2.amazonaws.com"**

**]**

**},**

**"Action": "sts:AssumeRole"**

**}**

**]**

**}**

**4. Create SSM Endpoints for Private Subnet**

Since your EC2 instance is in a private subnet, it cannot directly access the public internet. To allow the instance to communicate with AWS Systems Manager and other services, configure VPC endpoints as follows:

* **Create SSM VPC Endpoint:**
  + Go to the VPC Console → Endpoints → Create Endpoint.
  + Select the com.amazonaws.<region>.ssm service name for Systems Manager.
  + Similarly, create an endpoint for com.amazonaws.<region>.ssm.messages.
  + Create an endpoint for com.amazonaws.<region>.ec2messages and associate it with the private subnet.

**5. Enable Systems Manager Session Manager**

* **Run Command to Install Agent:**
  + In SSM, go to **Run Command**.
  + Click on SSMAgent Update.
  + Select the instance name Manually.
  + Click on Run Command to automatically install the agent.
* **Manual Installation**:
  + $ curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu\_64bit/session-manager-plugin.deb" -o "session-manager-plugin.deb.
  + $ sudo dpkg -i session-manager-plugin.deb
  + $ sudo systemctl start snap.amazon-ssm-agent.amazon-ssm-agent.service
  + $ sudo systemctl stop snap.amazon-ssm-agent.amazon-ssm-agent.service
  + $ sudo systemctl status snap.amazon-ssm-agent.amazon-ssm-agent.service

**6. AWS CLI and Session Manager Setup**

* **Install AWS CLI:**
  + Install AWS CLI locally and configure it using aws configure.
  + Install the Session Manager plugin locally on Ubuntu(to install follow above commands).
* **Start Session:**
  + **$ aws ssm start-session --target <instance-id>**

**7. Testing Session Manager**

Once the setup is complete, test the Session Manager connection:

* Go to the AWS Systems Manager Console → Session Manager.
* Click on Start session.
* Choose the EC2 instance in your private subnet.
* Initiate the session. If successful, you will be connected to your EC2 instance without needing a public IP or SSH access.

**8. Troubleshooting**

* **SSM Agent installed instance Not Showing in Session Manager:**
* Ensure that the SSM agent is installed and running on the EC2 instance.
  + Check the status of session manager agent, If it fails reinstall or update ssm agent.
* **Verify VPC Endpoints:**
  + Check that the VPC endpoints for SSM, EC2Messages, and SSM Messages are correctly configured and attached to the correct subnets.
* **IAM Role Permissions**:
  + Ensure the IAM Role attached to the EC2 instance has appropriate permissions (**AmazonSSMManagedInstanceCore**).