Configuring and Connecting to the EC2 Instance

Option 1: Configure Mac Terminal

This is a **one-time** step.

To connect to your EC2 instance using a Mac Terminal, you will first need to install the AWS CLI and then configure it. Below are the steps to do this:

Step 1: Install AWS CLI on Mac

1. **Open Terminal:**
   - On your Mac, open the Terminal application. This should be located in the Applications directory.
2. **Install Homebrew (if not already installed):**
   - Homebrew is a package manager for macOS that simplifies the installation of software. If you don't have Homebrew installed, run the following command in Terminal:
     `/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/`
   - Follow the on-screen instructions to complete the installation.
3. **Install AWS CLI using Homebrew:**
   - Once Homebrew is installed, you can easily install the AWS CLI by running the following command:
     `brew install awscli`
   - This will download and install the AWS CLI on your Mac.
4. **Verify Installation:**
   - After installation, verify that the AWS CLI is installed correctly by typing:
     `aws --version`
   - You should see output showing the installed version of the AWS CLI.

Step 2: Configure the AWS CLI

1. **Run the AWS CLI Configuration Command:**
   - In Terminal, configure the AWS CLI by running:
     `aws configure`
2. **Enter Your AWS Credentials:**
   - The CLI will prompt you to enter the following information:
     - AWS Access Key ID: Enter your AWS Access Key ID (see below).
     - AWS Secret Access Key: Enter your AWS Secret Access Key (see below).
     - Default region name: Enter your preferred region (for example, us-east-1).
     - Default output format: Enter None.

How to Obtain Your AWS Access Key ID and AWS Secret Access Key:

For New Users:

1. Sign in to the AWS Management Console and navigate to the IAM (Identity and Access Management) Console.
2. Create a New IAM User:
   - In the IAM Dashboard, click on "Users" in the left-hand menu.
   - Click "Add user".
   - Provide a username and check the "Programmatic access" checkbox to generate an access key.
   - Click "Next: Permissions" to assign appropriate permissions, either directly or by attaching a policy (e.g., AmazonS3FullAccess if you need S3 access).
   - Follow the remaining prompts and then click "Create user".
3. Download or View the Access Key:
   - After creating the user, you'll see a page with the Access Key ID and Secret Access Key. You can download these credentials as a .csv file or view them directly on the page.
   - Important: This is the only time you'll be able to view the Secret Access Key, so make sure to store it securely.

For Existing Users:

1. Sign in to the AWS Management Console and navigate to the IAM Console.
2. Access Your Existing IAM User:
   - In the IAM Dashboard, click on "Users" in the left-hand menu.
   - Click on your username to access the details.
3. Create a New Access Key (if none exists or if you need a new one):
   - Go to the "Security credentials" tab.
   - Scroll down to the "Access keys" section.
   - Click on "Create access key". AWS will generate a new Access Key ID and Secret Access Key for you.
4. Download or View the Access Key:
   - As with new users, you'll have the option to download the key or view it once. Ensure it is stored securely.
5. **Verify Configuration:**
   - You can verify your configuration by listing the S3 buckets or EC2 instances:
     `aws s3 ls`
     or
     `aws ec2 describe-instances`
   - If configured correctly, this should return a list of your S3 buckets or EC2 instances.

Option 2: Configure Windows Terminal

This is a **one-time** step.

To configure the AWS CLI on a Windows machine and connect to an EC2 instance, follow these steps:

Step 1: Install AWS CLI on Windows

1. **Open PowerShell or Command Prompt:**
   - On your Windows machine, open PowerShell or Command Prompt by searching for it in the Start menu.
2. **Download the AWS CLI Installer:**
   - Download the AWS CLI installer for Windows from the AWS CLI official website. You can download the .msi installer directly by clicking here.
3. **Run the Installer:**
   - Once downloaded, run the .msi installer. Follow the on-screen instructions to complete the installation. The installer will automatically install the AWS CLI to your system.
4. **Verify Installation:**
   - After installation, verify that the AWS CLI is installed correctly by typing the following command in PowerShell or Command Prompt:
     `aws --version`
   - You should see output showing the installed version of the AWS CLI, confirming that it is ready to use.

Step 2: Configure the AWS CLI

1. **Run the AWS CLI Configuration Command:**
   - In PowerShell or Command Prompt, configure the AWS CLI by running:
     `aws configure`
2. **Enter Your AWS Credentials:**
   - The CLI will prompt you to enter the following information:
     - AWS Access Key ID: Enter your AWS Access Key ID (see below).
     - AWS Secret Access Key: Enter your AWS Secret Access Key (see below).
     - Default region name: Enter your preferred region (for example, us-east-1).
     - Default output format: Enter None.

How to Obtain Your AWS Access Key ID and AWS Secret Access Key:

For New Users:

1. Sign in to the AWS Management Console and navigate to the IAM (Identity and Access Management) Console.
2. Create a New IAM User:
   - In the IAM Dashboard, click on "Users" in the left-hand menu.
   - Click "Add user".
   - Provide a username and check the "Programmatic access" checkbox to generate an access key.
   - Click "Next: Permissions" to assign appropriate permissions, either directly or by attaching a policy (e.g., AmazonS3FullAccess if you need S3 access).
   - Follow the remaining prompts and then click "Create user".
3. Download or View the Access Key:
   - After creating the user, you'll see a page with the Access Key ID and Secret Access Key. You can download these credentials as a .csv file or view them directly on the page.
   - Important: This is the only time you'll be able to view the Secret Access Key, so make sure to store it securely.

For Existing Users:

1. Sign in to the AWS Management Console and navigate to the IAM Console.
2. Access Your Existing IAM User:
   - In the IAM Dashboard, click on "Users" in the left-hand menu.
   - Click on your username to access the details.
3. Create a New Access Key (if none exists or if you need a new one):
   - Go to the "Security credentials" tab.
   - Scroll down to the "Access keys" section.
   - Click on "Create access key". AWS will generate a new Access Key ID and Secret Access Key for you.
4. Download or View the Access Key:
   - As with new users, you'll have the option to download the key or view it once. Ensure it is stored securely.
5. **Verify Configuration:**
   - You can verify your configuration by listing the S3 buckets or EC2 instances. Run one of the following commands:
     `aws s3 ls`
     or
     `aws ec2 describe-instances`
   - If configured correctly, this should return a list of your S3 buckets or EC2 instances.

Additional Steps (if required):

- **Set Environment Variables (Optional):**
  - If you want to make sure the AWS CLI is accessible from any directory, ensure that the installation path is included in your system's

environment variables. This is typically done automatically by the installer.

- **Connect to EC2 Instance Using SSH (Optional):**
  - To connect to your EC2 instance using SSH from Windows, you can use PuTTY or the Windows Subsystem for Linux (WSL) with an SSH client. Ensure that you have your .pem key file and that it is converted to .ppk if using PuTTY.

Connect to Sniffles on EC2

You can now access the Sniffles instance that is running on AWS EC2.

Connect to Your EC2 Instance

1. **Locate Your PEM File:**
   - Ensure you have the .pem key pair file that was created when you launched your EC2 instance.
2. **Set Permissions for the PEM File:**
   - Run the following command to set the correct permissions for the key pair file:
     `chmod 400 /path/to/your-keypair.pem`
   - Replace `/path/to/your-keypair.pem` with the actual path to your .pem file.
3. **Connect to the EC2 Instance:**
   - Use the SSH command to connect to your EC2 instance. Run the following command in Terminal:
     `ssh -i /path/to/your-keypair.pem ubuntu@your-instance-public-dns`
   - Replace `/path/to/your-keypair.pem` with the path to your .pem file and `your-instance-public-dns` with the Public DNS address of your EC2 instance. You can find the Public DNS in the AWS Management Console under the "Instances" section.
4. **Access Your EC2 Instance:**
   - Once connected, you will have shell access to your EC2 instance, allowing you to manage it as needed.

Additional Tips:

- **Using SSH Config File:** If you frequently connect to the same instance, consider setting up an SSH config file to simplify the connection command.
- **Security Considerations:** Ensure your .pem file is kept secure, as it provides access to your EC2 instance.

Configure AWS Credentials

This is a one-time step.

After logging into the EC2 instance, you must configure your AWS credentials by following these steps:

Step 1: Connect to the EC2 Instance

- Ensure you are logged into the EC2 instance using SSH as previously explained.

Step 2: Configure AWS CLI with Your Credentials

1. **Run the AWS CLI Configuration Command:**
   - On your EC2 instance, configure the AWS CLI by running:
     `aws configure`
2. **Enter Your AWS Credentials:**
   - The CLI will prompt you to enter the following information:
     - AWS Access Key ID: Enter your AWS Access Key ID (see below).
     - AWS Secret Access Key: Enter your AWS Secret Access Key (see below).
     - Default region name: Enter the region where your S3 bucket is located (e.g., us-east-1).
     - Default output format: Enter None.

How to Obtain Your AWS Access Key ID and AWS Secret Access Key:

For New Users:

1. Sign in to the AWS Management Console and navigate to the IAM (Identity and Access Management) Console.
2. Create a New IAM User:
   - In the IAM Dashboard, click on "Users" in the left-hand menu.
   - Click "Add user".
   - Provide a username and check the "Programmatic access" checkbox to generate an access key.
   - Click "Next: Permissions" to assign appropriate permissions, either directly or by attaching a policy (e.g., AmazonS3FullAccess if you need S3 access).
   - Follow the remaining prompts and then click "Create user".
3. Download or View the Access Key:
   - After creating the user, you'll see a page with the Access Key ID and Secret Access Key. You can download these credentials as a .csv file or view them directly on the page.
   - Important: This is the only time you'll be able to view the Secret Access Key, so make sure to store it securely.

For Existing Users:

1. Sign in to the AWS Management Console and navigate to the IAM Console.
2. Access Your Existing IAM User:
    - In the IAM Dashboard, click on "Users" in the left-hand menu.
    - Click on your username to access the details.
3. Create a New Access Key (if none exists or if you need a new one):
    - Go to the "Security credentials" tab.
    - Scroll down to the "Access keys" section.
    - Click on "Create access key". AWS will generate a new Access Key ID and Secret Access Key for you.
4. Download or View the Access Key:
    - As with new users, you'll have the option to download the key or view it once. Ensure it is stored securely.
5. **Verify Configuration:**
    - To verify that the credentials are configured correctly, you can try listing the contents of your S3 bucket.
      `aws s3 ls s3://your-bucket-name`
    - Replace `your-bucket-name` with the actual name of your S3 bucket.

Important Note: By configuring your AWS credentials directly on the EC2 instance, you enable the instance to interact with S3 buckets. This is essential for performing operations like uploading or downloading files from an S3 bucket.