MLflow server setup in AWS

Here's a step-by-step guide to set up an MLflow server using an EC2 instance, an S3 bucket, and an IAM role. This guide includes all the necessary commands and configurations:

1. Create an IAM User for MLflow

- Log in to the AWS Management Console.
- Search for "IAM" and select it from the services list.
- Create a New IAM User:
    1. Click on **Users** on the left sidebar.
    2. Click **Add use**r.
    3. Enter a **User name** (e.g., `mlflow-user`).
    4. Select **"Programmatic access"** as the access type.
    5. Click **"Next: Permissions"**.
    6. **Attach policies**:
    7. Choose **"Attach existing policies directly"**.
    8. **AmazonS3FullAccess** (for S3 bucket access)
    9. **AmazonEC2FullAccess** (for EC2 access)
    10. **AmazonS3ReadOnlyAccess** (optional, for read access to S3 buckets)
    11. Click **"Next: Tags"** and then **"Next: Review".**
    12. Click **"Create user"**.
    13. Download the **Access key ID** and **Secret access key.**

2. Create an S3 Bucket

1. Go to the S3 Console:

- Search for **"S3"** in the AWS Management Console.

2. Create a Bucket:

- Click **"Create bucket".**
- Enter a **Bucket name** (e.g., `mlflow-s3-bucket`).
- Choose a region.
- Click **"Create bucket".**

MLflow server setup in AWS

3. Create an EC2 Instance

1**. Go to the EC2 Console:**

   - Search for **"EC2"** in the AWS Management Console.

2. **Launch an Instance:**

- Click **"Launch** Instance".
- Choose an **Amazon Machine Image (AMI)** (e.g., **Ubuntu Server).**
- Choose an **Instance Type** (e.g., **t2.micro** for the free tier).
- Configure **instance Details** (default settings are usually fine).
- Add **Storage** (default settings are usually fine).
- Configure **Security Group**:

  Add a rule to allow **TCP traffic on port 5000 from 0.0.0.0/0**(for accessing MLflow UI).

- **Review and Launch.**

  Create or choose an **existing key pair** for SSH access.

- Click **"Launch Instance".**

4. Connect to Your EC2 Instance

1. Access your EC2 instance:

- Go to the **Instances page** in the EC2 console.
- Select your instance and click **"Connect".**
- Follow the instructions to connect via SSH.

5. Setup MLflow on Your EC2 Instance

Once connected to your EC2 instance via SSH, run the following commands:

1. Update package list

sudo apt update

2.Install pip for Python 3

sudo apt install -y python3-pip

3.Install pipx for managing Python applications

sudo apt install -y pipx

 4.Ensure pipx path is added to environment

pipx ensurepath

5.Install pipenv for managing Python environments

pipx install pipenv

6.Temporarily add pipenv to the PATH

export PATH="$PATH:$HOME/.local/bin"

7. Permanently add pipenv to the PATH

echo 'export PATH="$PATH:$HOME/.local/bin"' >> ~/.bashrc

 8.Create a directory for MLflow

mkdir mlflow

cd mlflow

9.Create and activate a new Python environment using pipenv

pipenv shell

10.Install necessary packages

pipenv install setuptools

pipenv install mlflow

pipenv install awscli

pipenv install boto3

11.Configure AWS CLI

aws configure

- Enter the **Access Key ID**, **Secret Access Key**, and default **region** when prompted.

12.Start MLflow server

mlflow server --host 0.0.0.0 --default-artifact-root s3://mlflow-s3-bucket

6. Update Security Group Rules

1. Modify Inbound Rules:

  - Go to the **Security Groups** section in the EC2 console.

  - Select the security group associated with your EC2 instance.

MLflow server setup in AWS

  - Edit **Inbound Rule** to allow **TCP traffic on port 5000** from **0.0.0.0/0.**

7. Access MLflow UI

1. **Obtain the Public IP Address:**

  - Go to the **instances** page in the EC2 console.
  - Copy the **Public IP** or **Public DNS** of your instance.

2. **Access MLflow UI**:

  - Open your browser and navigate to `http://<Public_IP>:5000`.

8. Set Environment Variable for MLflow Tracking URI

In your local environment or code, set the `MLFLOW_TRACKING_URI` to point to your MLflow server:

export MLFLOW_TRACKING_URI=http://<Public_IP>:5000

Replace `<Public_IP>` with the actual public IP address or DNS of your EC2 instance.

Summary

1. **Create IAM user** with necessary policies.

2. **Create S3 bucket** for storing artifacts.

3. **Launch EC2 instance** and connect to it.

4. **Install and configure MLflow** on the EC2 instance.

5. **Update security group rules** to allow access.

6. **Access MLflow UI** and set up your tracking URI.

This setup allows you to run MLflow on an EC2 instance with S3 as the artifact store, and IAM for managing access.