Guide for spinning up an EC2 instance on AWS

DATABREW
July 2019

This is a basic guide for setting up an EC2 instance on AWS. The purpose/context of this guide is getting OpenHDS running on a remote server.

Basic confiuguration

- Log into the AWS console: aws.amazon.com
- Click the "Launch a virtual machine" option under "Build a solution"
- Select "Ubuntu Server 18.04 LTS (HVM)"
- To the far right select 64-bit (x86)
- Click "select"
- Choose the default instance type (General purpose, t2.micro, etc.)
- Click "Review and launch"
- Click "Edit security groups"
- Ensure that there is an SSH tyupe rule with source set to 0.0.0.0/0 to allow any address to SSH in.
- Click "launch" in the bottom right
- A modal will show up saying "Select an existing key pair or create a new key pair"
- Select "Create a new key pair"
- Name it "openhd key"
- Download the .pem file into your /home/<username>/.ssh/id_rsa directory
- If that directory does not exist, run the steps in the next section ("Setting up SSH keys")
- Run the following to change permissions on your key: chmod 400 ~/.ssh/openhdskey.pem
- Click "Launch instances"
- Wait a few minutes for the system to launch (check the "launch log" if you're impatient)
- Click on the name of the instance (once launched)
- This will bring you to the instances menu, where you can see things (in the "Description" tab below) like public IP address, etc.

Setting up SSH keys

- If you don't have an SSH key on your system yet, run the following:
    - ssh-keygen -t rsa -b 4096 -C "youremail@host.com"
    - Select defaults (ie, press enter when it asks you the location, password, etc.)

- You will now have a file at /home/<username>/.ssh/id_rsa
- To verify, type: ls ~/.ssh/id_* (this will show your key)
- To change permissions to be slightly safer, run the following: chmod 400 ~/.ssh/id_rsa

Connect to the server

- In the "Instances" menu, click on "Connect" in the upper left
- This will give instructions for connecting via an SSH client
- It will be something very similar to the below:
- `ssh -i "/home/joebrew/.ssh/openhdskey.pem" ubuntu@ec2-3-17-72-248.us-east-2.compute.amazonaws.com`
- Congratulations! You are now able to run linux commands on your new ubuntu server

Managing users (ie, creating ssh keypairs for other users)

- Having ssh'ed into the server, run the following: sudo adduser <username_of_new_user>
    - Type a password
    - Press "enter" for all other options
- To create a user with no password, run the following: sudo adduser <username_of_new_user> --disabled-password. For example:
    - sudo adduser benmbrew --disabled-password
- Switch to that user: sudo su - benmbrew
- Create a .ssh directory for the new user and change permissions:
    - mkdir .ssh; chmod 700 .ssh
- Create a file named "authorized_+keys" in the .ssh dir and change permissions
- `	touch .ssh/authorized_keys; chmod 600 .ssh/authorized_keys
- Open whatever public key is going to be associated with this user (the .pub file) and paste the content into the authorized_keys file (ie, open authorized_keys in nano first and then copy-paste from your local machine)
- Grant sudo access to the new users: sudo usermod -a -G sudo benmbrew