**Linux Project: Michele Novack Abugosh**

**November 2019**

**Installed Software:**

**Ubuntu 16.04**

**PostgreSQL**

**Git**

**Apache2**

**mod\_wsgi**

**Python**

**Python Flask App**

**NTP**

**Lightsail AWS** 821479889842

**Project Description**

|  |
| --- |
| Taking a baseline installation of a Linux distribution on a virtual machine and prepare it to host your web applications, to include installing updates, securing it from a number of attack vectors and installing/configuring web and database servers. |

|  |  |
| --- | --- |
| **Name** | **Value** |
| **IP Address** | 3.84.147.247 |
| **SSH Port** | **2200** |
| **Username** | **grader** |
| **URL of Applicaiton** |  |

ec2-3-84-147-247.compute-1.amazonaws.com (3.84.147.247)

**Getting Connected to the Instance:**

1. **Launch an AWS Lightsail Instance and connect via SSH**
2. Using your browser, go to the account page for your AWS LightSail account.
   1. You will find your SSH key there.
   2. There is an option to download the default private key. The file name will be
      * LightsailDefaultKey-us-east-2.pem
   3. You need to change permission of the downloaded lightsail private key.
   4. Save the Key to home directory
   5. To do so, please run this command at your PC terminal: CD into Home Directory
      * chmod 600 Udacity.pem
   6. Change the name of the key to lightsail\_key.rsa. (The command is
   7. 'mv Udacity.pem Lightsail\_key.rsa').
   8. Time to connect to the remote server (AWS Lightsail instance). First, you need the IP address.
   9. Run this command (again, we are running this locally -- not on the instance):
   10. ssh -i Lightsail\_key.rsa ubuntu@ 3.84.147.247

**Check for updates**

Update all currently installed packages by typing:

1. sudo apt-get update
2. sudo apt-get upgrade
3. sudo apt-get dist-upgrade

**Launch Virtual Machine:**

1. Open Terminal : ssh -i Lightsail\_key.rsa ubuntu@ 3.84.140.171

**Create a New User:**

1. sudo adduser grader
2. Give Name Udacity Grader – say yes
3. Give Access: sudo nano /etc/sudoers.d/grader
4. Type: grader ALL=(ALL:ALL) ALL in nano editor, CTRL X and save
5. Check access: cat /etc/passwd
   1. Add Directory : **Temporarily log into the grader user: sudo -su grader**
      1. **Mkdir .ssh**
      2. **Change directory cd /home/grader**
      3. **touch .ssh/authorized\_keys**
      4. **nano .ssh/authorized\_keys**
      5. **copy the public key generated on your local machine to this file and save**
6. **chmod 700 .ssh**
7. **chmod 644 .ssh/authorized\_keys**
8. **Reload SSH sudo service ssh restart**
9. **Change owner from ubuntu to grader: sudo chown -R grader:grader /home/grader/.ssh**

**CHANGE THE SSH PORT FROM 22 to 2200. Make sure to configure the Lightsail firewall to allow it.**

1. **Remove root login, and force users to use key authentication by modifying the ssdh config** 
   1. **sudo nano /etc/ssh/sshd\_config**
2. **Enable server and set rules to outgoing ports and incoming ports:**

**Change the following line:**

# What ports, IPs and protocols we listen for

Port 2200

1. **Remove Root login:**

**Change the following line**

# Authentication:

PermitRootLogin no

1. **Force SSH login:**

**Change the following line**

# Change to no to disable tunnelled clear text passwords

PasswordAuthentication no

In AWS Lightsail Security Group, add 2200 as the inbound custom TCP Rule port

1. **Restart SSH service: run command sudo service ssh restart**
2. **Install NTP :** sudo apt-get install ntp.

**Configure the Uncomplicated Firewall (UFW)**

Configure the Uncomplicated Firewall (UFW) to only allow incoming connections for SSH (port 2200), HTTP (port 80), and NTP (port 123)

Sudo ufw status # this will check to see if active(should stated inactive)sudo

Sudo ufw default deny incoming

Sudo ufw default allow outgoing

sudo ufw allow 2200/tcp

sudo ufw allow 80/tcp

sudo ufw allow 123/udp

sudo ufw enable

Add 3 rules above as Security Group inbound rules of AWS Lightsail instance

INSTALL THE FOLLOWING:

**Configure the local timezone to UTC**

1. Configure the time zone

**$** sudo dpkg-reconfigure tzdata

1. It is already set to UTC.

### **Configure firewall to monitor for repeated unsuccessful login attempts and ban attackers**

1. Sudo apt-get update
2. Sudo apt-get install fail2ban
3. Install the sendmail package to send the alers to the admin user : sudo apt-get install sendmail
4. Create a file to safely customize the fail2ban functionality : sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
5. Adjust fail2ban configurations: sudo nano /etc/fail2ban/jail.local
   1. Set the destmail: admin user’s email
   2. Set all the bantime: bantime = 1800
   3. Set the action: action = %(action\_mwl)s

Sources: [DigitalOcean](https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-ubuntu-14-04), [Reddit](https://www.reddit.com/r/linuxadmin/comments/2lravs/fail2ban_does_not_detect_my_ssh_privatekey/).

**Install and configure Apache to serve a Python mod\_wsgi application**

1. Install Apache sudo apt-get install apache2
2. Install sudo apt-get install libapache2-mod-wsgi-py3
3. Install mod\_wsgi\_wsgi : sudo apt-get install python-setuptools libapache2-mod-wsgi
4. Sudo apt-get update
5. Restart Apache sudo service apache2 restart

#### **Install Flask using the pip tool (which also needs to be installed).**

**$** sudo apt-get install python-pip

**$** sudo pip install flask

**Create a Directory for the Flask App**

We'll create a directory in our home directory to work in, and link to it from the site-root defined in apache's configuration (/var/www/html by defualt, see /etc/apache2/sites-enabled/000-default.conf for the current value).

**$** mkdir ~/flaskapp

**$** sudo ln -sT ~/flaskapp /var/www/html/flaskapp

**Install and Configure PostgreSQL**

<https://tecadmin.net/install-postgresql-server-on-ubuntu/>

Start with the import of the GPG key for PostgreSQL packages.

sudo apt-get install wget ca-certificates

wget --quiet -O - https://www.postgresql.org/media/keys/ACCC4CF8.asc | sudo apt-key add -

Now add the repository to your system.

sudo sh -c 'echo "deb http://apt.postgresql.org/pub/repos/apt/ `lsb\_release -cs`-pgdg main" >> /etc/apt/sources.list.d/pgdg.list'

**Install and Configure PostgreSQL on ubuntu**

sudo apt-get update

sudo apt-get install postgresql postgresql-contrib

## Connect to PostgreSQL

sudo su - postgres

psql

disconnect from PostgreSQL database postgres-# \q

**Create a New Database name Catalog**

**Create a New User name Grader in postgreSQL shell**

**$** postgres=# CREATE DATABASE catalog;

**$** postgres=# CREATE USER grader;

SET A PASSWORD FOR A USER GRADER “ GRADER “

**$ postgres=# ALTER ROLE grader WITH PASSWORD ‘grader’;**

**GIVE USER “Grader” permission to Catalog application database**

**$ postgres=# GRANT ALL PRIVELEGES ON DATABASE catalog to grader;**

**QUIT POSTGRESQL**

**$ postgres=#/q**

**EXIT ;postgres: exit**

**INSTALL GIT:**

**$** sudo apt-get install git

1. Change directory cd/var/www to the var/www/directory
2. Create Application Directory
3. **$** sudo mkdir FlaskA

The contents of this repository are covered under the [MIT License](https://devhub.io/repos/LICENSE).