Creating a honeypot with AWS + T-pot

horizontal line

# 

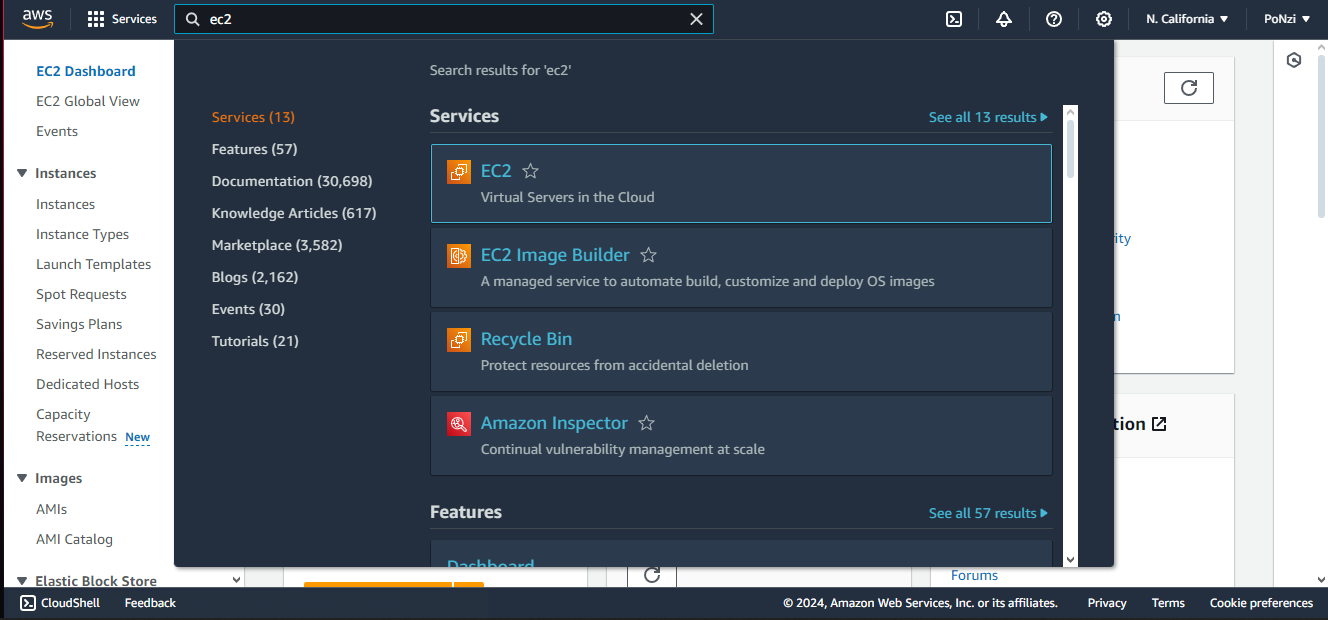
# Introduction

A honeypot is a cybersecurity mechanism designed to attract and detect unauthorized or malicious activity on a network. It acts as a decoy, deliberately mimicking a legitimate part of an information system, such as a server or database, to lure potential attackers. By engaging with the honeypot, attackers reveal their presence, methods, and intentions, allowing cybersecurity professionals to analyze the threats and enhance the security measures of the actual systems. Honeypots are valuable for gathering intelligence on new attack strategies, training security personnel, and reducing the risk to real assets. For this Project, we will be setting up T-pot using AWS so it eventually be linked to a SIEM to track, and plot, the attacks that will be coming in.

## 

## 

# Setting up T-pot

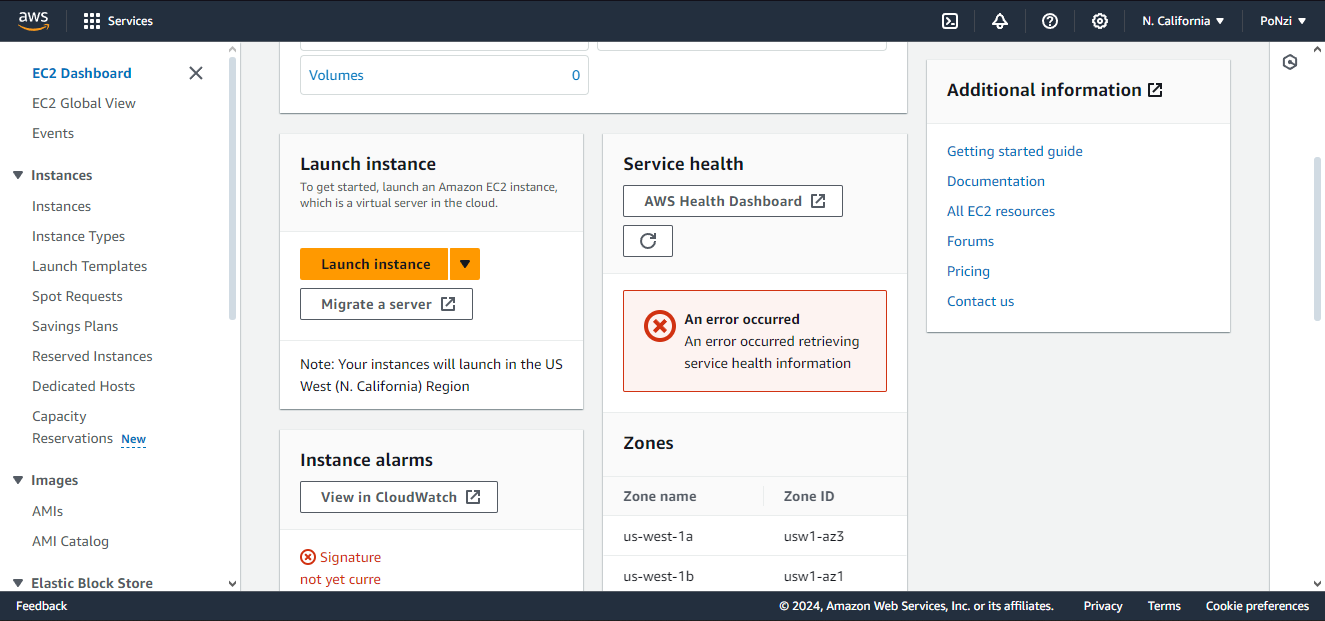


Once Logged in on AWS Click ‘Services’ (at the top of the screen) and click ‘EC2’, or alternatively search for ‘EC2’ using the search bar This will bring you to a screen where you’ll choose your instance to deploy T-Pot.

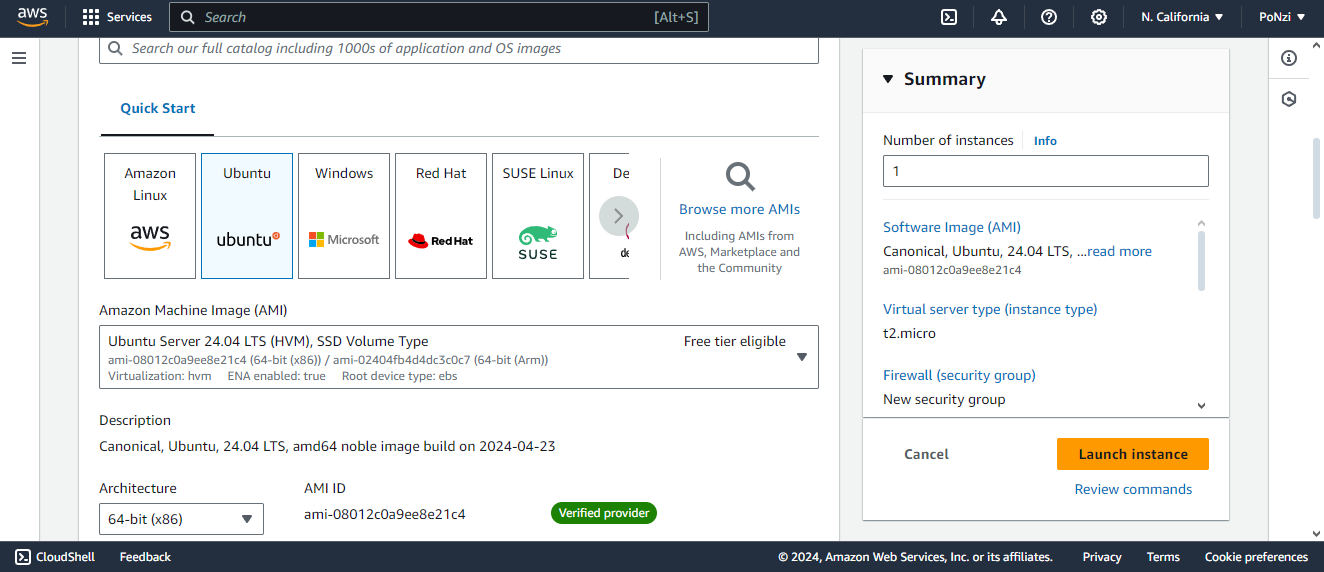
On the screen shown above you will have options to administrate your EC2 Instance. While on this screen, change the region that will be hosting your virtual machine. Doing this is that there will be reduced latency when you choose a region closer to you. If you choose to change the default region, Click the region name in the upper right hand corner of the screen and choose the region closest to you.

### 

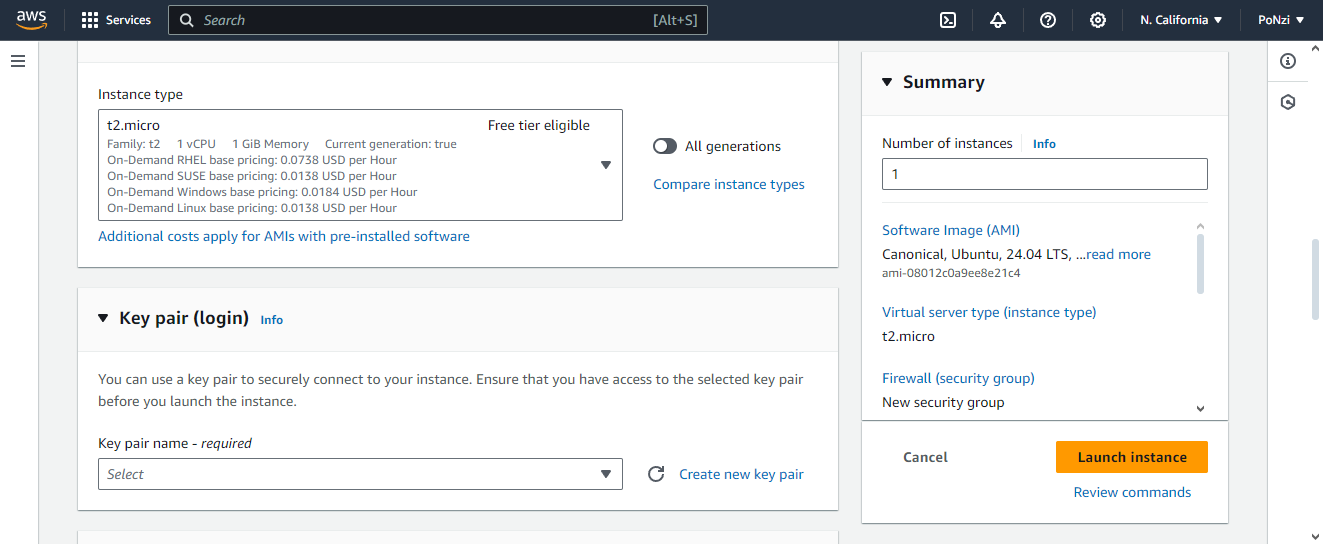
### Setting up your Virtual Machine



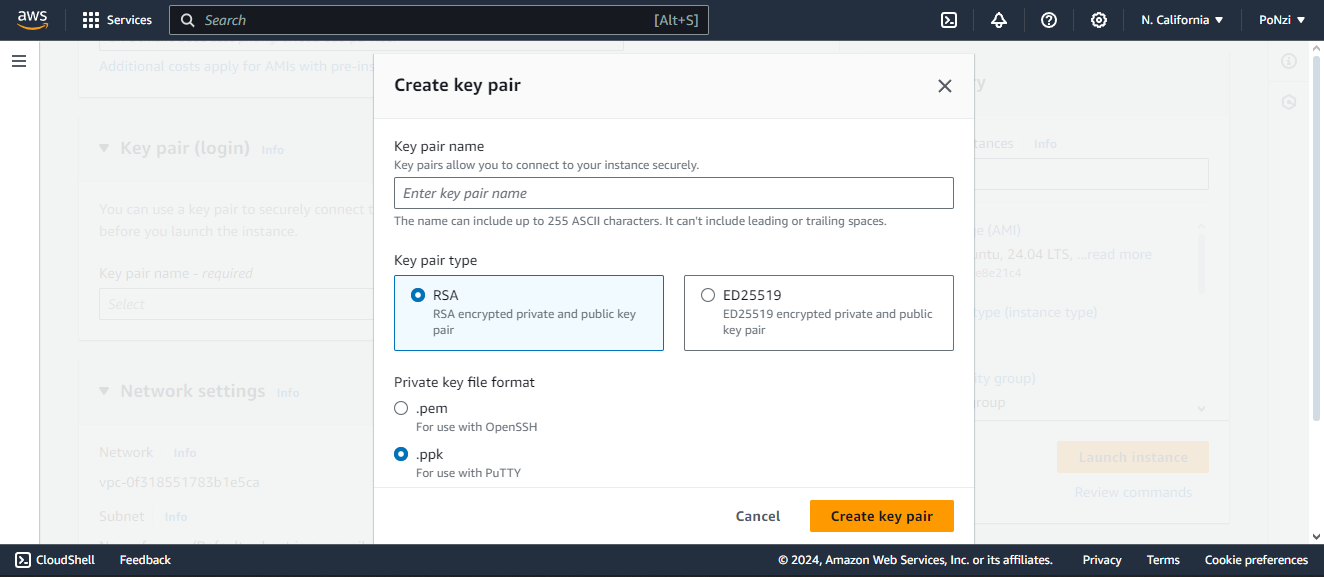
Now that you have selected your region, click on the orange ‘Launch Instance’ button. To get T-pot started, we will need to select Ubuntu Server 24.04 LTS. This should automatically be selected after selecting Ubuntu (shown below).



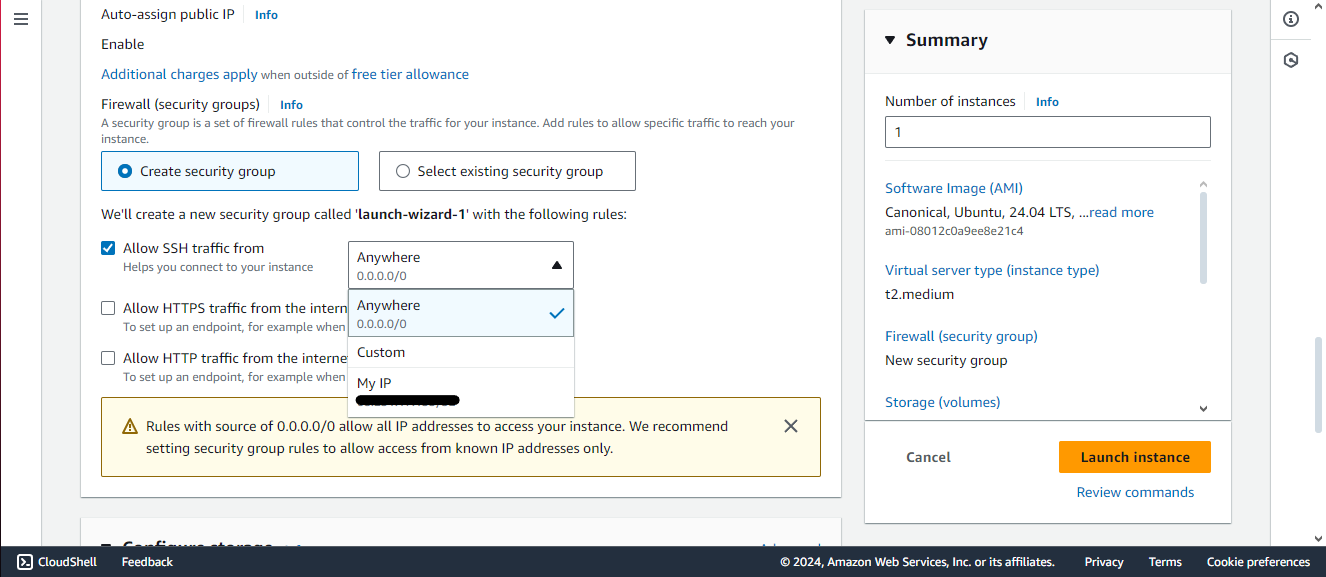
Next we need to choose our Instance Type. If you want to stay in the Free Tier, choose the t2.micro instance, this comes with 1 vCPU and 1GB of memory. The T-Pot system requirements document says you need to have at least 4GB of memory to run T-Pot, but you can get away with a t2.micro though it may be slow. If you are wanting to leave the honeypot up and running so that you can use them for personal or professional purposes, I would recommend a t2.medium or t2.large, but this will have a cost associated with it (about $2.76 per day as of writing this).

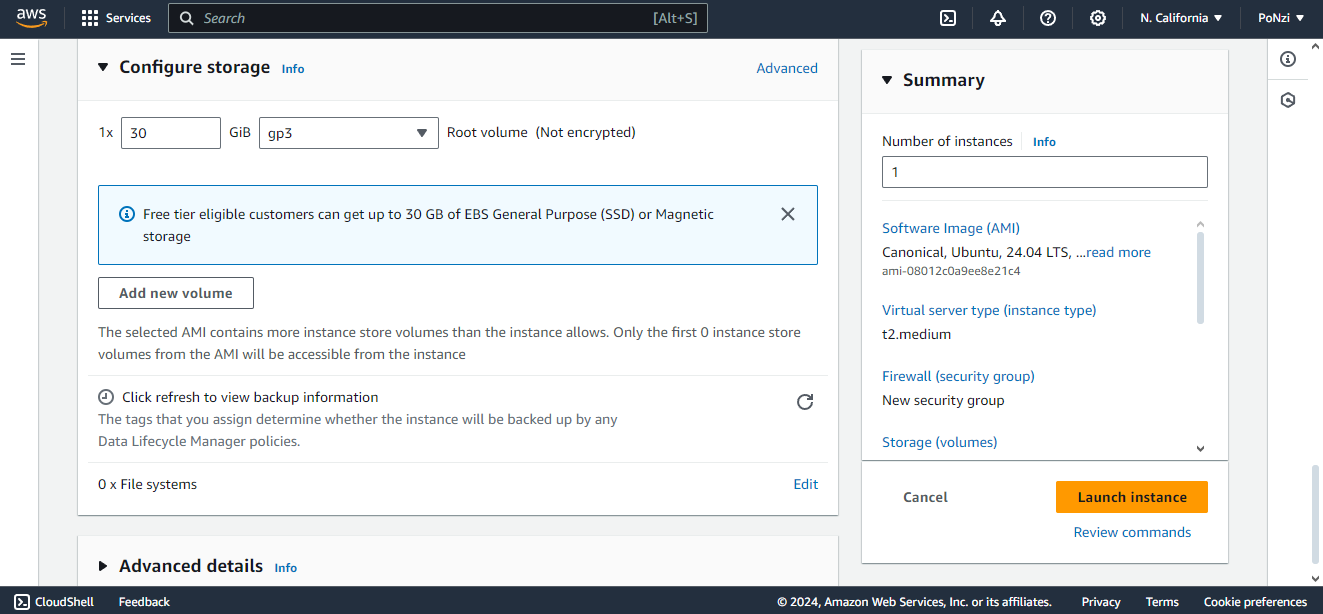


Once your Instance type is chosen, we will need to create a Key pair, this will be used to SSH into your machine. For this example, I will be using the setting shown below, as I will be using PuTTY for this example. This will download a .ppk file that will be used later.



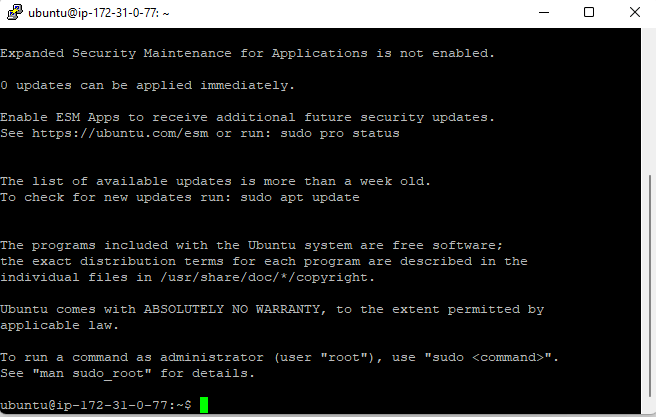
This next part is important and it’s something we’ll be revisiting again after installing and setting up T-Pot. The Security Groups will be what controls internal and external access to your EC2 instance. The default setting allows inbound SSH connections from an undefined IP range. Do **NOT** use this, as it would allow anyone to connect your EC2 instance.To fix this, Click the button that says ‘anywhere’ and choose ‘My IP’ so that your EC2 instance only accepts incoming SSH connections from your computer. This will be changed once T-pot is configured, as it has a built in SSH Honeypot.



Lastly, we will need to set up the storage for this. Free-tier includes 30 GiB of gp3, so we will be using that for this machine.****

Now that we are done, we can select ‘Launch Instance’. This will initiate the launch of your virtual machine, and may take a few minutes to complete. Once complete, click on the name of the machine to see if it has been launched, if so, refer to this guide to connect to your machine using PuTTy: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html#putty-private-key>

Now you should see that you have successfully connected and you will be presented with a command prompt, like so



# Configuring your honeypot

From here, we can start setting up Ubuntu with T-Pot. As Ubuntu does not come with a default root password (you will need to remember this password). Use the following command to change the root password, you will not be able to see the characters you are typing, so be sure to type correctly and keep track of it.

ubuntu@your-ip-address:~$ sudo passwd ubuntu

New password:

Retype new password:

passwd: password updated successfully

```

So let's update and upgrade our instance first (which you should do every time you use your instance) by using the following command:

sudo apt update && apt upgrade -y

```

Next, we will want to generate a keygen for this machine using the following command:

ssh-keygen

Press Enter again

Enter passphrase for keygen

```

Now that we’ve prepped Ubuntu for the honeypot install

, we can now quickly move through the install of T-Pot by using the following commands (If the git clone command does not work on the first try, you may need to install git. Walkthrough link for this provided here https://us.ovhcloud.com/community/tutorials/how-to-install-git-ubuntu/):

git clone https://github.com/dtag-dev-sec/t-pot-autoinstall.git

cd t-pot-autoinstall/

sudo su

./install.sh

```

This guide will walk you through the installation of T-Pot on your Ubuntu instance. The process involves providing a few key pieces of information during the installation.

The first prompt you will see is:

```

Which user do you usually work with?

This script is invoked by root, but what is your normal username?

Enter username: ubuntu

```

Next, you will be presented with the following options:

```

# How do you want to proceed? Enter your choice.

# Required: 4GB RAM, 64GB disk

# Recommended: 8GB RAM, 128GB SSD

# 1 — T-Pot’s STANDARD INSTALLATION # Standard Honeypots, Suricata & ELK #

# 2 — T-Pot’s HONEYPOTS ONLY # Honeypots only, w/o Suricata & ELK #

# 3 — T-Pot’s INDUSTRIAL EDITION # Conpot, eMobility, Suricata & ELK #

# 4 — T-Pot’s FULL INSTALLATION # Everything

```

I recommend selecting Option 4 if your EC2 instance can support the full installation. For those on the free tier, Option 1 is suitable as it requires fewer resources. If you plan to use this setup for learning and research, upgrading to a more robust instance and choosing Option 4 is advisable.

Make your selection and press Enter. The Ubuntu instance will then begin downloading and installing the necessary components for the chosen version. During the installation, you will be prompted to set a password for web access:

```

### Please enter a password for your user ubuntu for web access.

Password: myPassw0rd

```

For simplicity, you can use the default password, `myPassw0rd`. You will be asked to re-enter the password to confirm it. After this, the installation script will proceed and eventually display:

```

### Thanks for your patience. Now rebooting. Remember to login on SSH port 64295 next time or visit the dashboard on port 64297!

./install.sh: line 500: 9604 Terminated reboot

Connection to ec2–12–34–56–78.us-west-2.compute.amazonaws.com closed by remote host.

Connection to ec2–12–34–56–78.us-west-2.compute.amazonaws.com closed.

```

After the reboot, modify the Security Group settings on your EC2 instance to access your honeypots. By default, the SSH port (22) will be used as a honeypot, so you need to use port 64295 for SSH and port 64297 for web access.

To do this:

1. Go to the EC2 instance page on AWS.

2. Click `Services` at the top of the screen and select `EC2`.

3. Click `Running Instances` to see your instance details.

4. Under the `Description` tab, find `Security Groups` and click the `launch-wizard#` link.

5. Click the `Inbound` tab and then `Edit`.

6. Add a new rule for SSH:

- Type: `Custom TCP Rule`

- Port Range: `64295`

- Source: `My IP`

- Description: `SSH`

7. Add a new rule for web access:

- Type: `Custom TCP Rule`

- Port Range: `64297`

- Source: `My IP`

- Description: `Web Access`

8. Delete the original SSH rule (port 22).

9. Add rules to open your honeypots to all inbound traffic:

- For port range `0–64294` and source `Anywhere`.

- For port range `64298–65535` and source `Anywhere`.

After completing these steps, your Security Group settings should be properly configured.

To connect back to T-Pot, use the SSH command provided earlier. Additionally, you can now connect to the web portal to start visualizing attacks. Note that the IP address may change after the initial reboot, so ensure you use the updated public IP address from your AWS instance details page.

To access the web browser or SSH, use:

```

https://your.AWS.IP.address:64297

```

Enter the credentials used during setup:

```

Username: ubuntu

Password: yourpasswd

```

For SSH:

ssh -i “./FolderName/YourFileName.pem” ubuntu@ec2–12–34–56–78.us-west-2.compute.amazonaws.com

```

Connecting to the web interface should display the relevant dashboard, while connecting through SSH will show a similar message as during the initial connection to the Ubuntu instance.