School of Information Studies

Syracuse University

IST 615 – Cloud Management

Lab #2
Virtual Machines in AWS

IMPORTANT INSTRUCTIONS[1]:

i) Read this document in its entirety BEFORE starting the lab.
ii) You will need to access your AWS Academy account to access the AWS Cloud resources needed to complete this lab
iii) Some screenshots may not appear "exactly" as depicted in this document. They are intended as a guide and you should adapt to your own local situation/environment.
iv) Download the user_data.txt file that is associated with this lab
v) You will need to provide screen captures that indicate your progress with the steps required in this lab. There will be notices for you to capture screenshots during some of the steps in this lab. Make sure each capture has been correctly completed in your system.

Contents

1 Introduction 2
2 Lab objectives 2
3 Launch and configure an Amazon EC2 instance 2
4 Test your web server 4
5 Update your security group 4
6 Cost effectiveness 5
7 Resize your instance 6
8 Connect to your AWS EC2 instance via SSH 7
8.1 SSH into your Amazon EC2 web server from a Windows system 7
8.2 SSH into your Amazon EC2 web server from a Mac or Linux system 8
9 Clean up your environment 9
10 Lab report 9

[1] School of Information Studies, Syracuse University
Lab created by Carlos E. Caicedo
Last updated on February/2024 by Carlos Caicedo

1 Introduction

You have been hired by a company to provision a proof of concept (POC) webserver for testing their new web-based application. The webserver must run on a Linux machine. It must be configured as an Apache HTTP server, be cost effective and publicly accessible.

For the webserver you will need to create and launch a t2.micro Amazon Elastic Compute Cloud (Amazon EC2) instance using a free tier Linux Amazon Machine Image (AMI). An AMI is a template used to create a virtual machine within Amazon EC2.

An Amazon EC2 instance provides scalable computing capacity in the Amazon Web Services (AWS) Cloud. When you launch an Amazon EC2 instance, you are creating a virtual server. This means you are securing space on a physical server located in an AWS data center for your use. The allocated space consists of the compute, storage, and network resources you need to run your webserver workload.

2 Lab objectives

In this lab you will:

- Launch and configure an Amazon EC2 instance
- Troubleshoot your Amazon EC2 instance
- Update a security group
- Create and test a security group rule
- Resize an instance
- Connect to your AWS EC2 instance via SSH

3 Launch and configure an Amazon EC2 instance

(Note: When you create your AWS account, AWS creates a default Amazon Virtual Private Cloud (Amazon VPC) for you in each region. Your default Amazon VPC contains a default subnet.)

The first requirement is that the product team would like a Linux webserver that has Apache installed on it. They would also like for it to be publicly accessible, so let’s work on it:

1. In the **AWS Management Console**, expand the “Services" drop down menu and select the **Compute** service and afterwards, select **EC2.** (Then select **EC2 Dashboard** if you are not already in that window).
2. From the Amazon **EC2 dashboard**, click Launch Instance (Big orange button) and then click on the “Launch Instance” option
3. Once you are in the “Launch an instance” window, proceed to give a Name to the EC2 instance that you will create (e.g. Lab02vm)

4. Notice the variety of AMIs located below "Quick Start" section. These are templates for different types of configurations. Select the **Amazon Linux 2023 AMI** (Free tier eligible)**.** Please note it might already have been selected by default.
5. In the **Instance type** section. Select the **t2.micro** instance.
6. In the **Key pair (login)** section click on **Create new key pair,** in the window that appears, name your key pair ***awskey01*** and make sure that the Key pair type is RSA and the Private key file format is .pem. Then click **Create Key Pair.** Save the private key to your desktop. You will need this key later. **(Please note you only have one chance to save the key, don't cancel this operation and remember where you saved the key!!)**
7. In the **Network settings** section, click on **Edit**, change the ***Security group name*** field to *WebserverSG*. Change the ***Description*** field to *SG for lab 2*

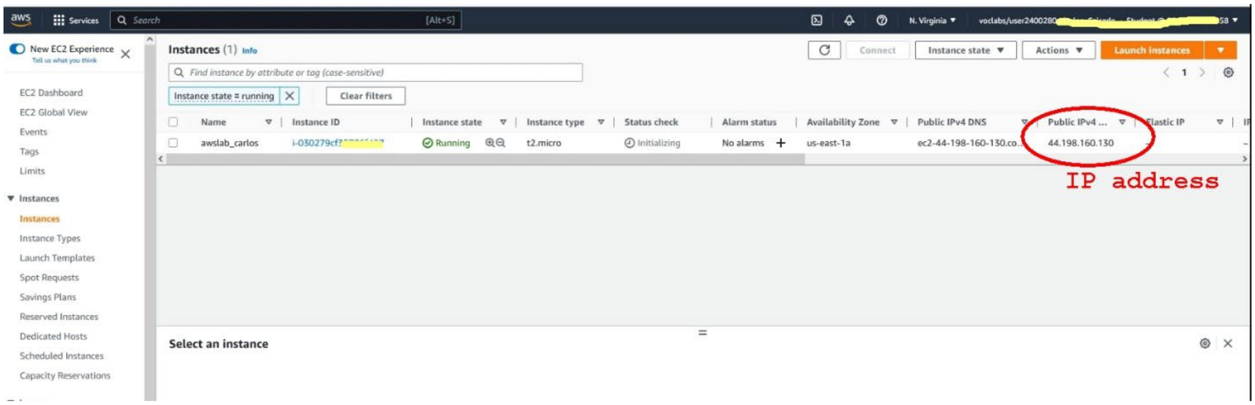
   Don't change any other Network related setting at this moment, we are going to use our default Amazon VPC and launch our Amazon EC2 instance into the default public subnet where AWS will automatically assign our virtual machine a public IP address.
8. Scroll down until you find the **Advanced details** section, expand it, and scroll down all the way to the ***User data*** section
   a. Open the **user_data.txt** file provided to you by the instructor on a basic text editor like Notepad or VSCode. The text editor must be one that DOES NOT introduce new line breaks or formatting to the text in the file!!
   b. **IMPORTANT !!!:** Replace the *netid* text in the last command line of file's text content **with your own netid.** *Do not change any other text.*
   c. Copy the content of your updated **user_data.txt** file and paste it into the ***User data*** section. We are providing code that runs the first time that the virtual machine starts up. The code will complete the configuration of this virtual machine. This process is called *bootstrapping*. Make sure your netid is in the last line of the text that you copied in the *User data* section.
   d. The user_data.txt file contains Bash commands that configure your EC2 instance into a Web server by executing the following tasks (See if you can identify which actions each line of script performs) :
      1. Installs, enables, and starts the Apache Web Server software (httpd).
      2. Creates an index.html page with a message that mentions your netid.
9. Click on the **Launch Instance** button. Your EC2 instance (your Virtual machine, your web server) will take a while to create.
10. Once the EC2 instance is created, scroll to the bottom of the page and click **View all instances**. You'll be taken to the Instances page. Alternatively, you can access the AWS menu (with the hamburger icon) and click on the "Instances" option.

FOR YOUR REPORT

- SCS01 - CAPTURE A SCREENSHOT OF YOUR BROWSER THAT SHOWS THAT THE NEW EC2 INSTANCE IS NOW IN YOUR DASHBOARD

4 Test your web server

1. In the **Instances** page, select your webserver instance and copy the Public IPv4 address to your clipboard (The IP v4 address will have the structure A.B.C.D where A, B, C, and D are numbers – see the figure below. Your IP address will have a different set of numbers than the shown in the figure)
2. Paste the public IP address into a new browser window and observe the results.
    a. The format of the webpage request that uses your public IP address should be: http://A.B.C.D (where A.B.C.D is your server's Public IP address)
3. Did the webpage load properly? If not, what may be the issue?



	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
□	awslab_carlos	i-030279cf[redacted]	Running	t2.micro	Initializing	No alarms +	us-east-1a	ec2-44-198-160-130.co...	44.198.160.130	–

You have successfully launched your webserver but when you tried to access the Public IP address, there is an error of the form: *This site cannot be reached or connection timeout.*

The company's product team won't be able to access their application if they can't reach the webserver. It is our job to figure out how to fix this issue.

Look back at the previous steps and read about security groups. Are you allowing normal web traffic (traffic to Port 80) to access your webserver?

5 Update your security group

1. Keep the web browser open and go back to the Amazon **EC2 Dashboard**
2. In the left navigation pane (you can open it with the hamburger icon), under **Network & Security,** click **Security Groups.** You might need to click the refresh button of the dashboard to see a complete list of security groups.
3. Select the **WebserverSG** security group
4. Find the **Inbound rules** tab. Notice the security group currently has no rules that allow HTTP traffic.

Create a rule

Let's create a rule in the **Inbound rules** tab

5. Click **Edit inbound rules**
6. Click **Add Rule** and then configure the following settings:

   Under the drop down box for **Type**, select **HTTP**

   (*Note: you may have to scroll down in the dropdown menu to find HTTP)*

   Source: Anywhere-IPv4 (This option will be in a dropdown menu)

   Click **Save rules**

The new Inbound HTTP rule will create an entry for IPV4 source IP address (0.0.0.0/0). If everything was done correctly you should see TWO Inbound rules listed and the following test should be successful.

***Note**: Make sure you that the inbound rule that allows SSH traffic still exists, otherwise you won't be able to perform some of the upcoming tasks in this lab*

FOR YOUR REPORT

- SCS02 - CAPTURE A SCREENSHOT OF YOUR BROWSER THAT SHOWS THAT YOU HAVE TWO INBOUND RULES

Test your rule

7. Return to the web browser tab you previously opened, the one with the webserver public IP address, and refresh the browser page
8. You should see the message:

```
Hello, welcome to the IST 615 AWS lab instance created by
<your_netid>.
```

Congratulations! You successfully launched a webserver**,** and your product team is very pleased to have a server for the POC of their application.

FOR YOUR REPORT

- SCS03 - CAPTURE A SCREENSHOT OF YOUR BROWSER WITH THE MESSAGE THAT SHOWS YOUR NETID

6 Cost effectiveness

You used a t2.micro instance but what are some other ways that we can save on cost for your company? Cloud computing services use a **utility-based pricing** model. Basically, if you leave your light on, there is an associated cost that will show up in your electricity bill. If our product team only works on Mondays through Fridays between the hours of 8:00 AM and 6:00 PM, can we minimize cost by turning off the server when it is not being used?

Stop your Amazon EC2 instance

1. Go to the “Instances” section in the left hand navigation menu and click “Instances”.
2. Select your running instance and then at the top of the screen click **Instance State > Stop instance**.
3. Your instance will do a normal shutdown and then will stop running

7 Resize your instance

The product team has noticed that the virtual machine running the webserver is underpowered. Their software requires a little bit more horsepower, and they’ve asked for your help

1. Select your Web Server instance and then go to the **Actions** menu, select **Instance settings > Change Instance Type**

   (Note: you can only do this if the "Instance state" is "Stopped". You might need to refresh your environment or move in an out of the "Instances" panel to see the updated state).
2. Then configure the following:
   a. **Instance Type:** t2.small
   b. Click **Change**

Start the resized instance

3. In the left navigation panel, click **Instances**.
4. Select your server and in the *Actions* menu, select **Instance State > Start instance**
5. SCS04 - **FOR YOUR REPORT: CAPTURE A SCREENSHOT OF THE RE-SIZED EC2 INSTANCE. The screenshot should display the configuration information related to the new Instance type of the EC2 instance.**
6. Copy and take note of the **new** public IPv4 address assigned to your EC2 Amazon instance
7. Open up a browser tab and enter the new IP address of your EC2 instance. Verify that your web page still works

After you have setup the web server and verified it works, you can proceed to connect to your AWS EC2 instance via SSH.

8 Connect to your AWS EC2 instance via SSH

Now that you have successfully launched an Amazon EC2 with a bootstrap script, configured the security group correctly to allow traffic in the SSH / HTTP ports, and tested Port 80 HTTP, check to make sure you can SSH into the EC2 instance.

1. Navigate to the EC2 Dashboard and click on **Running Instances**.
2. Click and highlight the EC2 instance you created previously (in the first activity).
3. Write down the IPv4 Public IP address. You will need this address later.

*Now let's use SSH to remotely connect (login) to the EC2 instance. To do so, you can use **select one of the following options depending on the operating system of the client machine** that you will use to remotely connect to your webserver (i.e. the client machine could be your laptop)*

8.1 SSH into your Amazon EC2 web server from a Windows system

This section tells you how to use Secure Shell (SSH) on a Windows PC/laptop to connect to your EC2 web server instance. If you are using Mac OS (by Apple Inc.) or Linux, please refer to the instructions in section 8.2

Follow the instructions mentioned in the video titled "Setting SSH key permissions on Windows" (available in Blackboard) to configure the awskey01.pem *file that you downloaded in a previous step so that it can be used to connect via ssh to your EC2 instance. At the end of the video the command structure to activate the ssh connection is mentioned but you can only execute it after completing the initial steps mentioned in the video.*

Once you have started the ssh session on the EC2 instance using the *ec2-user* username, perform the following steps:

1. At the command prompt, type **pwd** and enter.
2. You should see that you're in the **/home/ec2-user** directory**.**
3. At the command prompt, type **cat /var/www/html/index.html** and then press Enter.
4. You should see the content of the file that displayed the welcome message for your website and which includes your netid as part of the text.
5. SCS05 - **FOR YOUR REPORT: CAPTURE A SCREENSHOT OF THE SSH SESSION TO YOUR EC2 INSTANCE. The screenshot should display the output of the commands executed in steps 1 and 4**

If you have completed the previous steps, Congratulations! You have successfully connected to your Web server via the command line. You can proceed to the end of this document write your lab report and clean up your environment.

8.2 SSH into your Amazon EC2 web server from a Mac or Linux system

This section tells you how to use Secure Shell (SSH) on a Mac or Linux based system to connect to your EC2 web server instance. If you are using Windows, please skip go to section 8.1

You will need to open a SSH client on your computer. Mac computers have a Terminal app that can is used for SSH. Open the Terminal app to complete the steps to connect to you web server.

Remember the .pem file you downloaded when you are launching your EC2 instance? Put it on your MAC's desktop.

Before you can connect to your webserver, you will need to set the permissions of your private key file so that only you can read it. Do not skip this step, otherwise you will not be able to connect to your EC2 instance. Use the following command in the Terminal command prompt:

```
chmod 400 Desktop/awskey01.pem
```

Now, you are ready to connect to your instance. In the terminal window, enter the following command in the Terminal command prompt:

```
ssh -i Desktop/awskey01.pem ec2-user@xxx.xxx.xxx.xxx
```

Where xxx.xxx.xxx.xxx is the IPv4 public IP address of your EC2 instance.

You will see a message asking if you want to proceed with the connection. Answer **yes** to continue with the connection process.

After you have successfully connected to your EC2 instance perform the following tasks:

1. At the command prompt, type **pwd** and enter.
2. You should see that you're in the **/home/ec2-user directory.**
3. At the command prompt, type **cat /var/www/html/index.html** and then press Enter.
4. You should see the content of the file that displayed the welcome message for your website and which includes your netid as part of the text.
5. SCS05 - **FOR YOUR REPORT: CAPTURE A SCREENSHOT OF THE SSH SESSION TO YOUR EC2 INSTANCE. The screeshot should display the output of the commands executed in steps 1 and 4**

If you have completed the previous steps, Congratulations! You have successfully connected to your Web server via the command line. You can proceed to the end of this document write your lab report and clean up your environment.

9 Clean up your environment

Note: Execute these steps ONLY after you have completed the submission of your lab report.

The company's product team has fully deployed their software into a production setting. You are requested to get rid of the POC testing machine you created.

Steps

1. Find and select your **WebServer instance**
2. Select **Instance State > Terminate**
3. Delete your Webserver SG security group by navigating to the **Security Groups** option in the left-hand navigation panel within the **Network & Security** category. Ensure there is a check mark in the box next to your Security Group. Click on the **Actions** drop down menu and select **Delete security group**
4. You may also want to delete your awskey01 key by navigating to the **Key Pairs** option in the left hand navigation panel within the **Network & Security** category. Ensure there is a checkmark in the box next to your Key Pair Name click the **Actions** dropdown box, click **Delete** confirm deletion by typing *Delete* in the field - click Delete.

10 Lab report

For your report, please include the following items:

(Remember to include a title page)

Part 1 (70 points):

Include all the screenshots required throughout the lab guide. Provide a small description of what is being shown in each screenshot

Part 2 (30 points):

You launched and configured an Amazon EC2 instance, resized it, and changed the security group. Use that experience (and some additional research), to answer the following questions.

1. What is the purpose/use of the Amazon EC2 service?
2. What is an Amazon Machine Image (AMI)?
3. What is the purpose of user data when creating an EC2 instance?
4. What do you use to control what types of traffic can access your Amazon EC2 instances?
5. Why would you want to resize an Amazon EC2 instance?
6. A security group works like a firewall because it contains a set of rules that filter traffic coming into and out of an Amazon EC2 instance. By default, all non-local traffic is ______. (Choose from the following options: Allowed, blocked, or neither)