

**AWS – Amazon Cloud Foundations Labs 1-3**

Brendon Ahn | Advanced Cisco | 2022-2023



**Purpose**

To learn about and work with AWS by doing the Amazon Cloud Foundation labs, this includes learning how to set up AWS services and cloud applications.

**Background**

Amazon made AWS and this Cloud Foundations course was a way to teach people how to work with AWS and do things with their cloud services. These were made with beginners in minds; however, they do feel a lot like a massive ad for the company which is quite annoying. The labs themselves were quite straight forward and easy.

What was taught in Lab 1 was the AWS Management console. The Management console of AWS involves creating an account and it can be used to set up security settings. As this is just a foundations course, this lab was not really intensive and is just the basics. A good portion of the first lab was to show users how to find their ways around the Management Console. The Management Console does things like “provisioning resources, launching instances, setting up load balancers and creating or managing Amazon Simple Storage Service (S3) bucket.”

In lab 2 we saw the Amazon Simple Storage Service, or more commonly referred to as S3. We are shown how to create an S3 bucket, set up access policies, and work with objects. The benefits of S3 in AWS that the cloud foundations preach is its scalability and security, meaning that its very reliable and is recommended for companies that are constantly expanding.

With Lab 3 we saw Amazon Elastic Compute Cloud, or EC2. With this we kind of see the abbreviation convention, if it has a number after a letter there are that many words in a row that start with the before letter. It is a AWS service that has a scalable capacity in the cloud. We work with EC2 instances and one useful feature for companies is that it can be accesses using SSH. This means we can access cloud services remotely which is beneficial for employees as they can work from home amongst many other benefits for companies.

**Summary**

We worked with the Management Console, EC2, and S3 of AWS Amazon Cloud Foundations Labs and learned how to configure instances and access them remotely. We furthered our knowledge of Amazon Web Services.

**Lab Procedures**

**Lab 1**

1. Click Open AWS Management Console (If it doesn’t work allow pop-ups)

A screenshot of a web page

Description automatically generated with medium confidence

1. Go to Services and click IAMA screenshot of a computer

   Description automatically generated with medium confidence
2. Choose Users
3. Click user 1 and go to Permissions

A screenshot of a computer

Description automatically generated with medium confidence

1. Click on the GroupsA screenshot of a computer

   Description automatically generated with medium confidence
2. Click on the Security Credentials
3. Click User Groups and go to EC2-Support group and go to Permissions

A screenshot of a computer

Description automatically generated with low confidence

1. Click the + then -
2. Click User Groups then select S3-Support group

A screenshot of a computer screen

Description automatically generated with low confidence

1. Click + then –
2. Choose User Groups then select EC2-Admin group
3. Click the + then –

**Lab 2**

1. Open AWS Management Console
2. Go to Services and click VPC

A screenshot of a computer

Description automatically generated

1. Click on Launch VPC Wizard.
2. Select VPC with Public and Private Subnets
3. Choose Select and configure according to the instructions and click create VPC, then OK when its ready
4. Select Subnets and create a subnet with configurations according to the instructions and click create

A screenshot of a computer

Description automatically generated with medium confidence

1. Repeat step 6 with the other instructed configurations
2. Select Route Tables

A screenshot of a computer

Description automatically generated

1. Select the route table with Main = Yes and VPC = Lab VPC
2. In the Name column click the pencil and type Private Route Table and save
3. Select Routes then select Subnet Associations

A screenshot of a computer

Description automatically generated

1. Click Edit Subnet and select both Private Subnet 1 and 2 and save associations
2. Select the route table with Main = No and VPC = Lab VPC
3. In the Name column click on the pencil icon and type Public Route Table and click save
4. Repeat 8-12 with Public
5. Select Security Groups and click Create Security Group and enable settings as the instructions say

A screenshot of a computer

Description automatically generated with medium confidence

1. In Inbound rules click Add Rule and configure as per the instructions then click Create Security Group
2. Go to Services and click EC2
3. Click Launch Instance then select Amazon Linux 2 AMI (HVM), SSD Volume Type
4. Click t2.micro and Next: Configure Instance Details and configure as described
5. Click Next: Add storage and then Next: Add tags
6. Click Add Tag and set the key to Name and the value to Web Server 1
7. Click Next: Configure Security Group then select Select An Existing Security Group and click Web Security Group and then Review and Launch
8. Select Proceed Without a Key Pair and then Launch Instances
9. Select View Instances until it passes
10. Select the Instance you just launched and click Connect
11. Select EC2 Instance Connect(Browser-Based SSH Connection) and click Connect
12. Open a browser and go to a public IP of your instance

**Lab 3**

1. Open the EC2 console and select an Amazon Machine Image (AMI)
2. Go to Choose an AMI and select the Amazon Linux 2 AMI
3. Choose the t2.micro instance type
4. Configure Network and select Lab VPC

A screenshot of a computer

Description automatically generated

1. Enable Termination Protection Check the box Protect Against Accidental Termination
2. Expand Advanced Details and click Advanced Details
3. Add User Data Copy and paste the following commands into the User Data Field: #!/bin/bash yum -y install httpd systemctl enable httpd systemctl start httpd echo '<html><h1>Hello From Your Web Server!</h1></html>' > /var/www/html/index.html
4. Select Next: Add Storage
5. Add a tag with Key: Name and Value: Web Server
6. Configure a Security Group named Web Server Security Group with a description
7. Delete Existing SSH Command, Delete the existing SSH command in the security group inbound rules.
8. Click Review and Launch then Launch
9. Select or Create Key Pair
10. Acknowledge and Launch
11. Click View Instances
12. Click on the Instance then select Status Checks then Monitoring
13. Go to Actions dropdown and select Monitor And Troubleshoot and then Get System Log
14. Click Cancel
15. Go to your browser and open a new tab
16. Paste the IPv4 Public IP of your instance
17. Keep the browser open and return to the EC2 Management Console.
18. Select Security Groups
19. Choose the Web Server Security Group
20. Select the Inbound Rules
21. Edit Inbound Rules and configure

A screenshot of a computer

Description automatically generated

1. Return to the web server tab
2. In EC2 select Instances
3. Stop the Instance
4. Go to Actions and Instance Setting then Change Instance Type and select t2.small and apply
5. Select Volumes then go to Actions and click Modify Volume
6. Select the Instance again and go to Action then Instance Settings
7. Select Change Instance Type then select t2.small and apply

A screenshot of a computer

Description automatically generated with medium confidence

1. Go to Volumes then select Root EBS Volume then go to Actions and Modify Volume

A screenshot of a computer

Description automatically generated

1. Increase the volume size to 10 GB then click Modify and confirm
2. Select Instances and go to Actions then Start Instance
3. Select Limits then Running Instances
4. Select Instances and choose the Instance you ran
5. Go to Actions then Instance Setting and select Change Termination Protection



1. Unselect Enable and save
2. Go to Instances and select the instance
3. Go to Actions then Terminate Instance then Confirm

A screenshot of a computer

Description automatically generated

**Problems**

Finding everything and understanding all the instructions were a bit of an issue for me. There was a lot of wait time in these labs and I would over click which created some lag. I also had the problem of typos with IPs when trying to connect remotely. I also had to go back sometime to reconfigure some steps as I messed up a bit at times and that created issues when trying to access an Instance. There was a lot I had to go back and redo in order to move on to next steps. With going back there was a lot of additional navigation I had to do. I also had to go back after I was done with all the labs to do the steps which was the worst and most time-consuming part, at least that’s what it felt like.

**Conclusion**

In conclusion Amazon Cloud Foundations is an Ad for AWS as well as an introduction for beginners. It taught me how to navigate the Management Console, work with S3 and EC2 Instances and gain a better understanding of various AWS services pertaining to cloud.