**Technical Report**

Sayuru Harith

January 29,2021

****

**Introduction**

This is a technical report that every step and action I carried out according to home assignment. This assessment contains two sections and I have to attempt both sections as well. The assignment based on Amazon web services.

**Set Up AWS**

Have to logging aws official web site and create an aws account. It will give 12-month free tier access to use aws services. After provide contact information have to provide payment information to the system. Until the verification of our aws account they will charging 2 USD from our credit card. After successful verification of the account, they will refund 2 USD as well.

There is another identity confirmation from aws account side. Aws automated system will contact you with an OTP code. It will send to your phone number via text message or voice mail.

Now you are successful logging to the aws console. But aws service may take up 24 hours to fully activate your aws account.

**Run a freely available web server**

When we are trying to run a freely available web server, first wen need to create virtual machine using Amazon Elastic compute cloud (EC2). That allows users to rent virtual computers on which to run their own computer applications.

Launch EC2 INSTANCE

Clicking aws services we have to launch EC2 instance, After that they will assign you, what kind of operating system we can freely access. “Amazon Linux operating system, RedHat Enterprise, Ubuntu Server” whatever you familiar with you can take any operating system as well.

Configure SECURITY GROUP

Then you to configure security group. In here you can create new security group using “SSH”,” HTTP”,” HTTPS” and whatever you need.

When you review and launch EC2 instance, you need to generate key pair. It will generate as .pem file. After that you can successfully load EC2 instance.

Connect Linux Instance using PUTTY

**Install PuTTY on your local computer**

Download and install PuTTY from the PUTTY download page. If you already have an older version of PuTTY installed, it’s better to download the latest version. Be sure to install the entire suite.

**Convert your private key using PuTTYgen**

Locate the private key (.pem file) for the key pair that you specified when you launched the instance. Convert the .pem file to a .ppk file for use with PuTTY.

PuTTY does not natively support the private key format for SSH keys. PuTTY provides a tool named PuTTYgen, which converts keys to the required format for PuTTY. You must convert your private key (.pem file) into this format (.ppk file) as follows in order to connect to your instance using PuTTY.

Then we can run freely available webserver. I installed apache web server using command ”sudo apt-get install apache2”.

**Deploy content to Web Server**

Using HTML script we can deploy simple static text content “Hello World”

<DOCTYPE html>

<html>

<head>

<title>page title</title>

</head>

<body>

<h1> Hello world </h1>

</body>

<script src = "https://shd123.s3.us-east-2.amazonaws.com/s3aws.html"></script>

</html>

**Enable SSH into EC2**

When you trying to enable SSH inti EC2, clicking your instance you can go to connect. In here you have to run this command if necessary, to ensure your key is not publicly viewable

chmod 400 AWSubuntu.pem

After that you have to connect your instance using its public DNS.

ssh -i "AWSubuntu.pem" ubuntu@ec2-18-222-208-207.us-east-2.compute.amazonaws.com

Then you can enable SSH into EC2.

**Periodically stop and start instance using Lambda function**

Create IAM role

First we need to go to the IAM role. In here we have to create IAM policy. When clicking create policy it will navigate to the Jason file. Then we have to write down Jason script to create policy.

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": [

"ec2:Start\*",

"ec2:Stop\*"

],

"Resource": "\*"

},

{

"Sid": "VisualEditor1",

"Effect": "Allow",

"Action": [

"logs:CreateLogStream",

"logs:CreateLogGroup",

"logs:PutLogEvents"

],

"Resource": "arn:aws:logs:\*:\*:\*"

}

]

}

After that need to go with the review policy and give it to the name and you can create policy.

Now we navigate to IAM role and go to create role, start it clicking lambda.

Then we have to choose a policy, what we are create earlier. After that give name to the IAM role and create role as well.

Create LAMBDA Function

Find an AWS lambda in AWS console. After clicking AWS lambda go to create function. Then create an lambda function to stop instance. When we go to the permission, choose existing AWS policy(IAM role) what we create earlier. Then create function.

Scroll down and you can find json file and write a Jason script code to stop instance.

import boto3

region = 'us-east-2b'

instances = ['i-0004badb41807d9f7']

ec2 = boto3.client('ec2', region\_name=region)

def lambda\_handler(event, context):

ec2.stop\_instances(InstanceIds=instances)

print('stopped your instances' + str(instances))

If this script execute properly. Ec2 instance will automatically stop. But in my case occur an error while I execute this script.

{  
  "errorMessage": "2021-01-28T03:34:36.476Z 31599400-2a49-4284-969e-ae91508c45d3 Task timed out after 3.00 seconds"  
}  
Summary  
Code SHA-256  
reXQxqT61GwsczbZPbjA3F4nn4WC/y4H8tQu/xJnsS8=  
Request ID  
31599400-2a49-4284-969e-ae91508c45d3  
Init duration  
376.36 ms 2021-01-28T03  
Duration  
3003.40 ms  
Billed duration  
3000 ms  
Resources configured  
128 MB  
Max memory used  
83 MB  
Log output  
The section below shows the logging calls in your code. Click here to view the corresponding CloudWatch log group.  
START RequestId: 31599400-2a49-4284-969e-ae91508c45d3 Version: $LATEST  
END RequestId: 31599400-2a49-4284-969e-ae91508c45d3  
REPORT RequestId: 31599400-2a49-4284-969e-ae91508c45d3 Duration: 3003.40 ms Billed Duration: 3000 ms Memory Size: 128 MB Max Memory Used: 83 MB Init Duration: 376.36 ms  
2021-01-28T03:34:36.476Z 31599400-2a49-4284-969e-ae91508c45d3 Task timed out after 3.00 seconds"

**Collect log files and upload to S3 bucket**

Create S3 bucket

Clicking services of AWS console you can find S3 storage and go to the S3 bucket create bucket with put unique name and region.

Then go to the bucket policy and update the bucket with policy using lambda function.

{

"Version": "2012-10-17",

"Id": "Policy1611848734379",

"Statement": [

{

"Sid": "Stmt1611848730196",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::698847319302:root"

},

"Action": "s3:PutObject",

"Resource": "arn:aws:s3:::shdlogfiles/mylogs/AWSlogs/698847319302/\""

}

]

}

Create IAM role policy

Clicking services of the AWS console go to the IAM role and create list bucket policy with using lambda function.

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"s3:ListBucket",

"s3:HeadBucket"

],

"Resource": "\*"

}

]

}

When we upload log files S3, have to log groups with some content. Let’s go head to the create lambda function again and create lambda function to CloudWatch logs export to S3.

**Issues**

* when I create my AWS account, it’s pop up an error while my phone number verification process. I'm waited 24 hours to fully activate my account but still not. And I chat with the system support, but they also notify my phone number is not verify by calling also. After that they continue this process while send an OTP code to my mail. They told me that 48 hours it will take to fully activate my AWS account.
* When create lambda function to Ec2 instance will automatically stop. It occurs an error while I execute the script.
* When create lambda function to CloudWatch logs export to S3, it also occurs an error while execute the function.