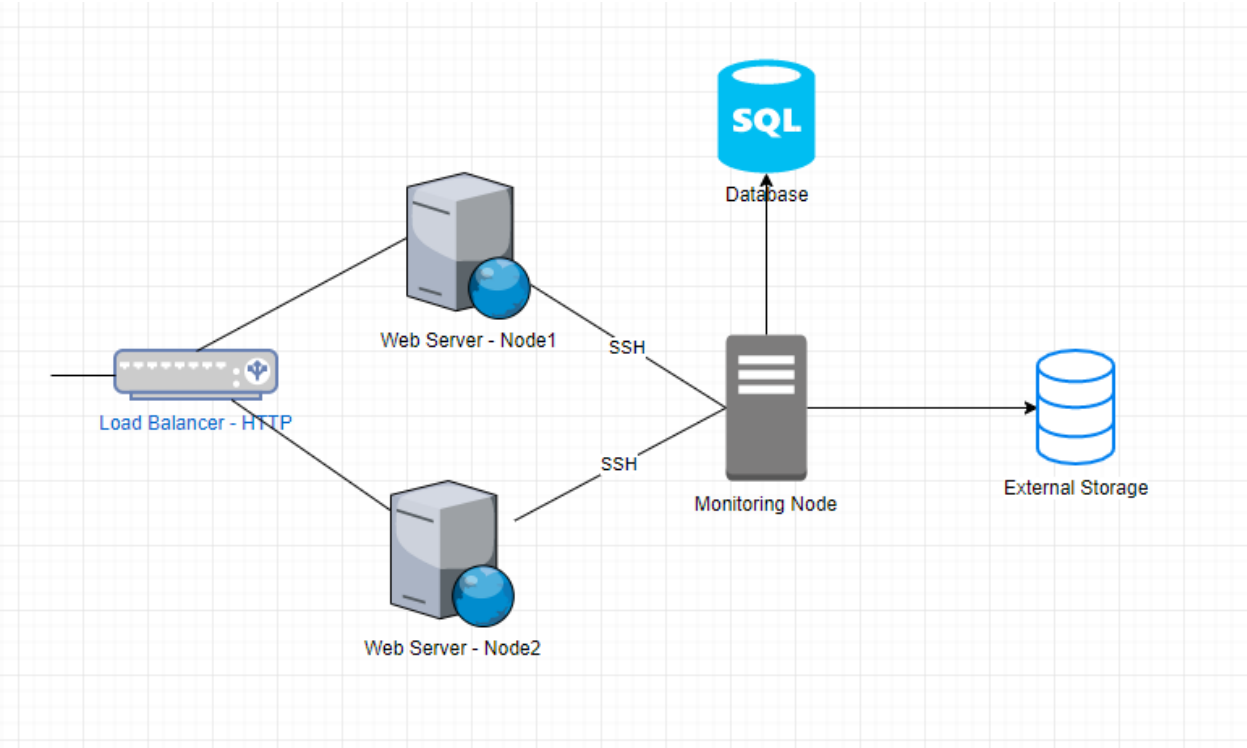
Assignment
London Stock Exchange Group

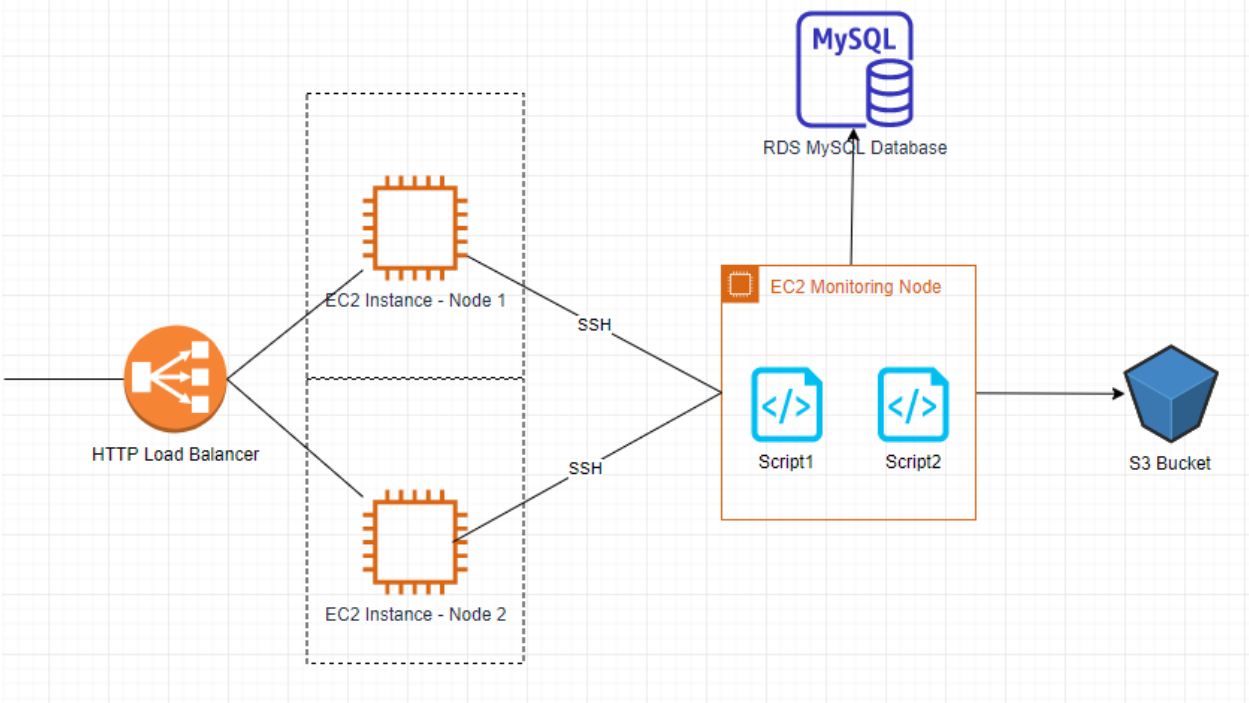
Lahiru Malavige

Table of Contents

High Level Architecture Diagram

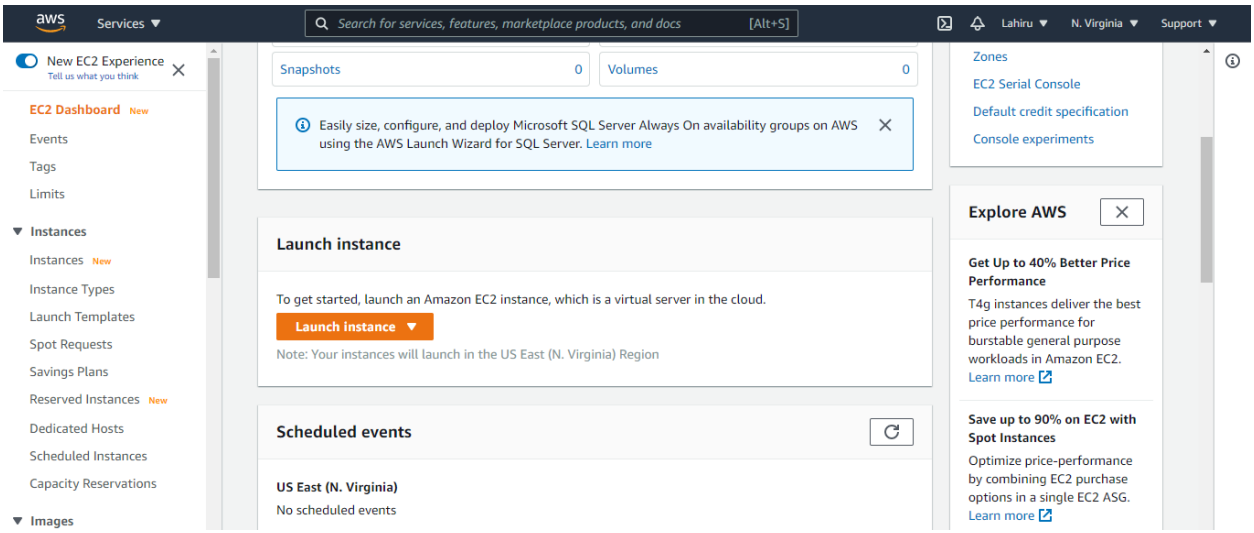


AWS based solution diagram

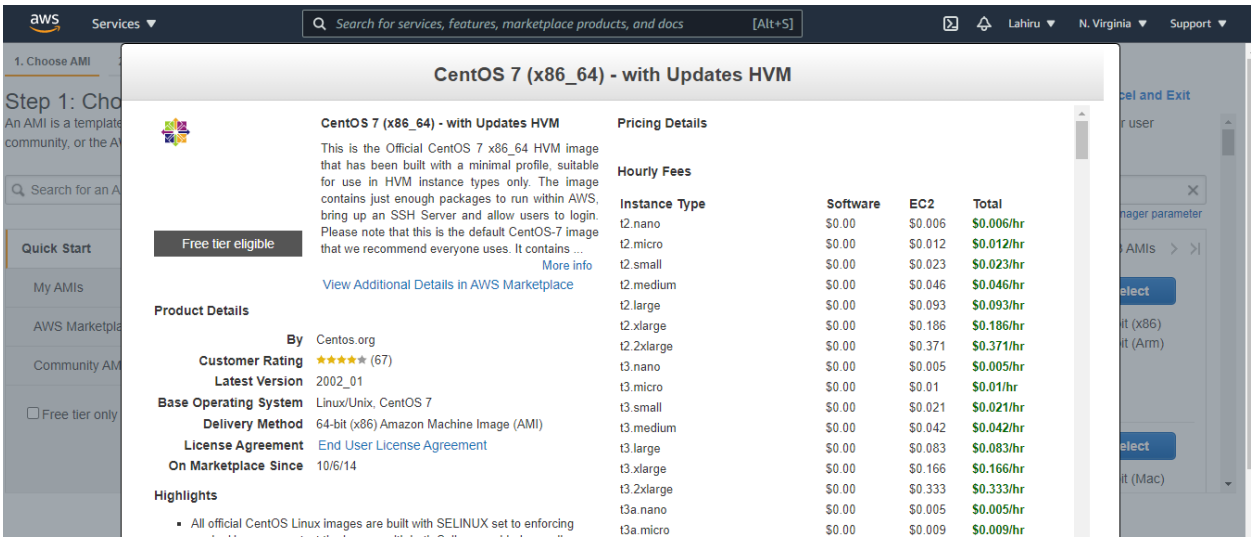


AMI creation

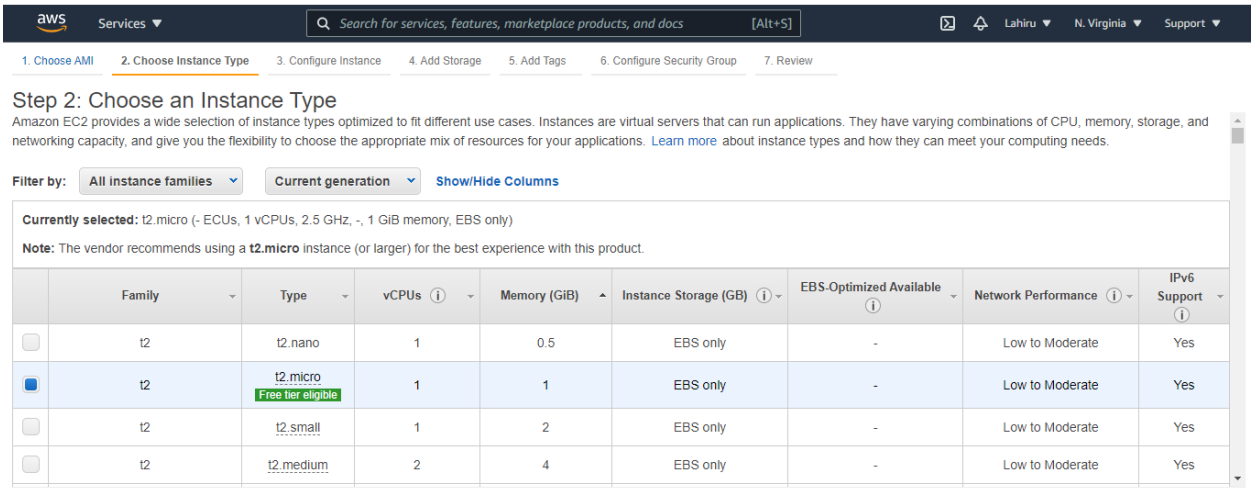
Amazon Machine Image makes it easier to deploy EC2 instances in AWS as it keeps the basic OS configurations of an instance and we can deploy multiple instances using a single AMI in the AWS environment as well. AWS has built in AMIs and also we can make an Amazon Machine Image from a currently running EC2 instance as well. The intention of launching such EC2 instance is to come up with a customized AMI that can be later used in cloudformation in this setup. Two separate AMIs will be created for web nodes and the monitoring node.



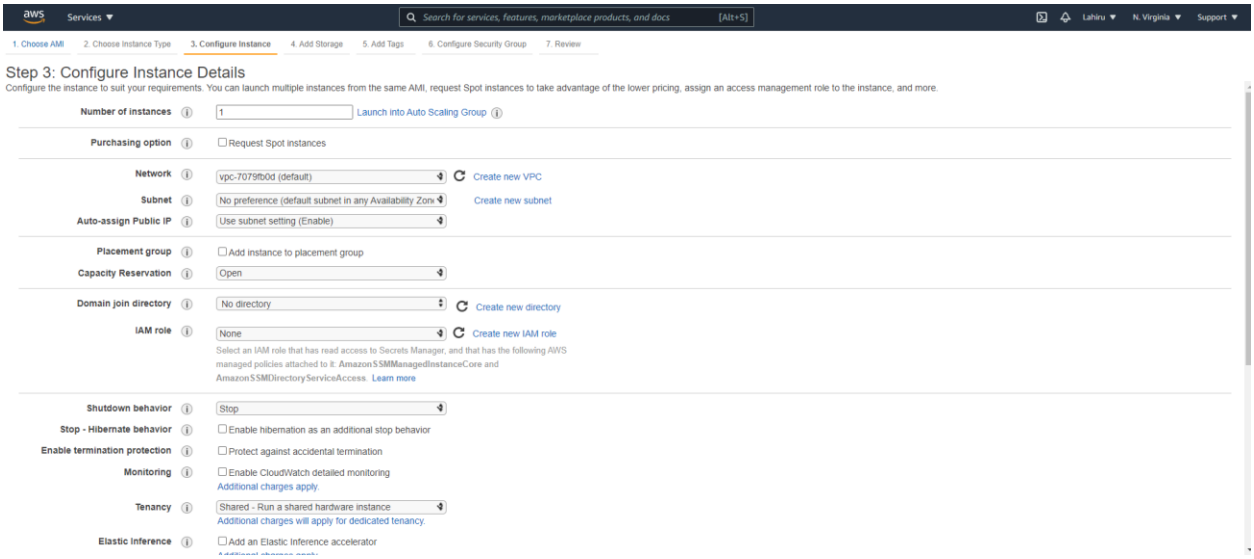
-



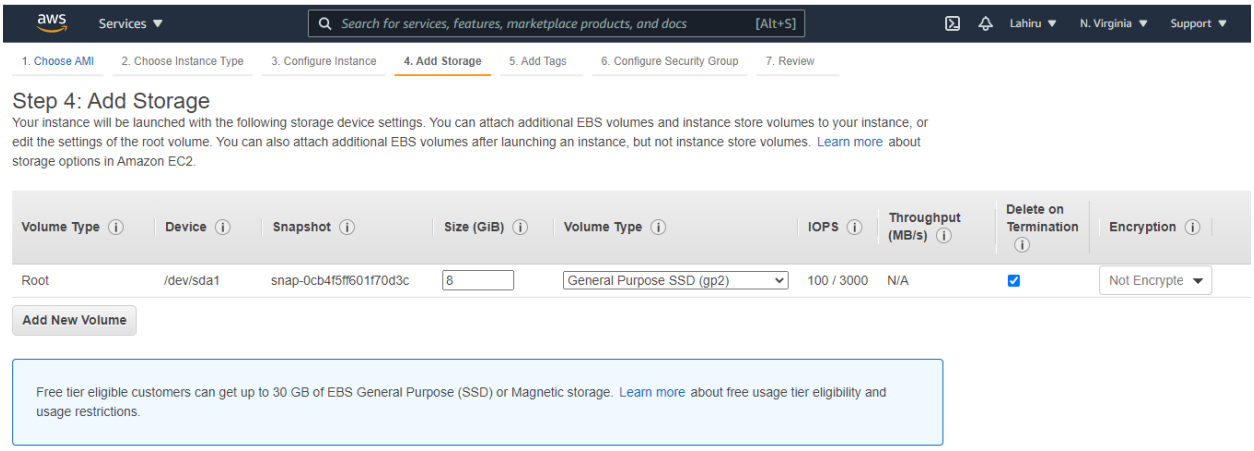
- Centos 7 was chosen as the AMI to setup the EC2 instances for this setup.



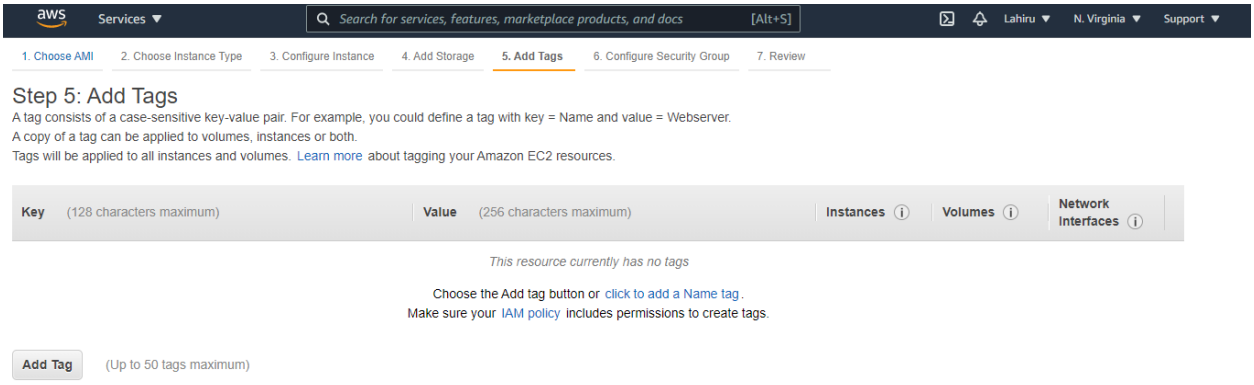
- The instance type must be chosen to cater the requirement. More computing power and memory, better network performances are more expensive as well.



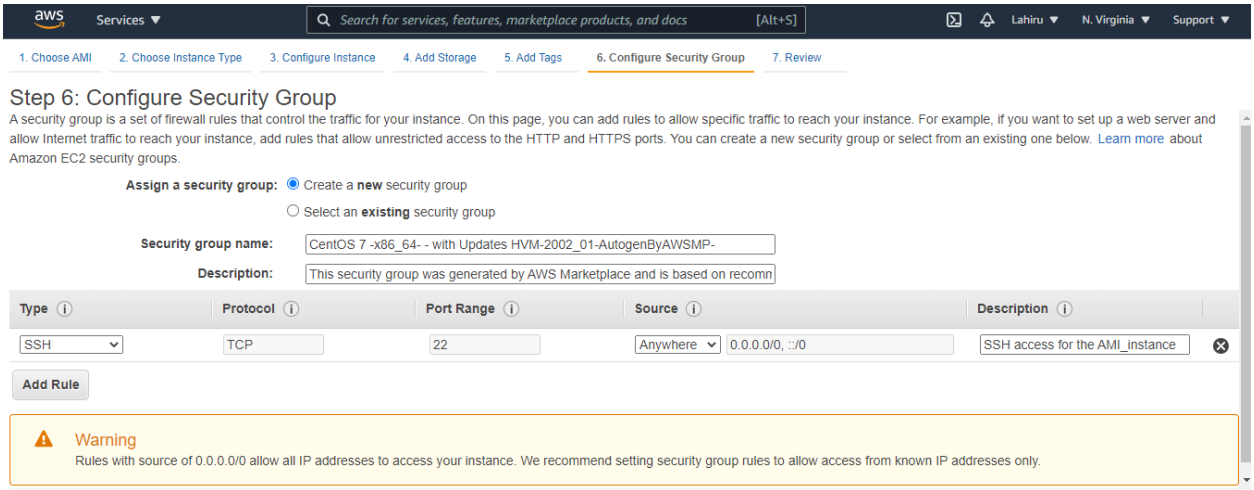
- An EC2 instance is always deployed in a virtual private cloud. There are options to define the subnet. Identity and Access Management plays a major role in security in EC2 instances. If there are already created IAM roles they can be applied. If not, those configurations can be applied later on.



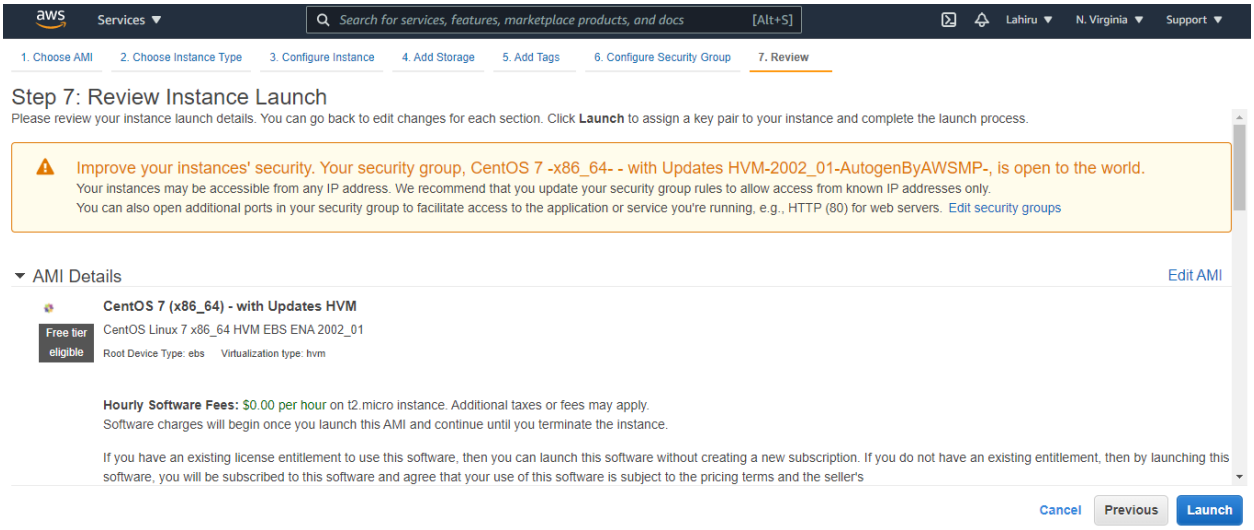
- Size of the storage device in EC2 instance must be declared and the different volume types like SSD, HDD and magnetic disks are given as options. IOPS will also differ according to the volume type and faster storages will require more cost.



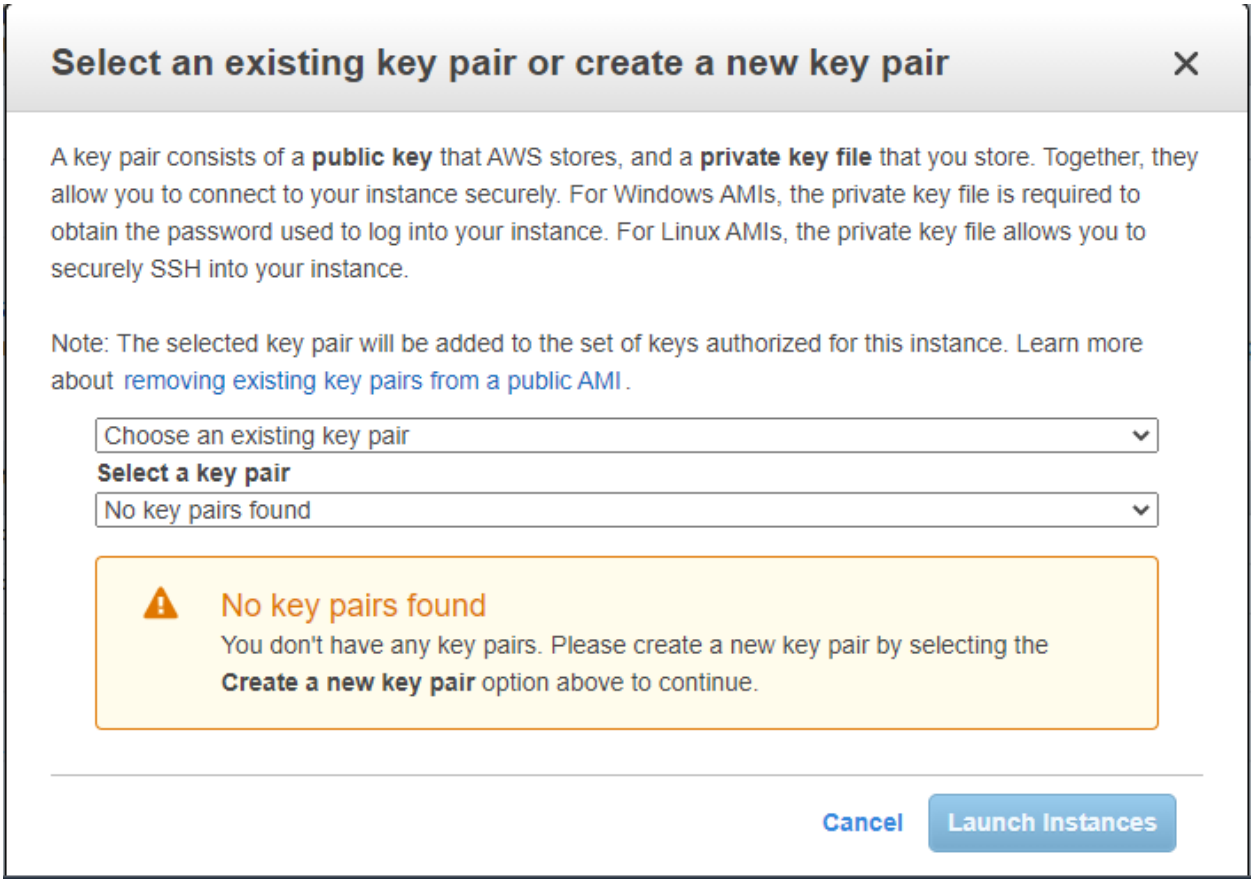
- Tags are very useful in configuration management.



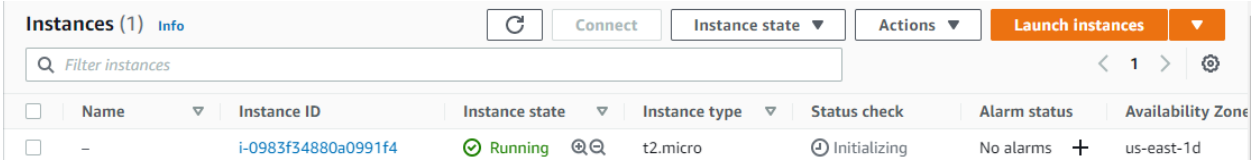
- Security group will act as the firewall daemon or iptables in a linux server. It gives the option to allow certain ports and IP addresses both inbound and outbound traffic.



- After reviewing the selected options, the EC2 instance can be launched.

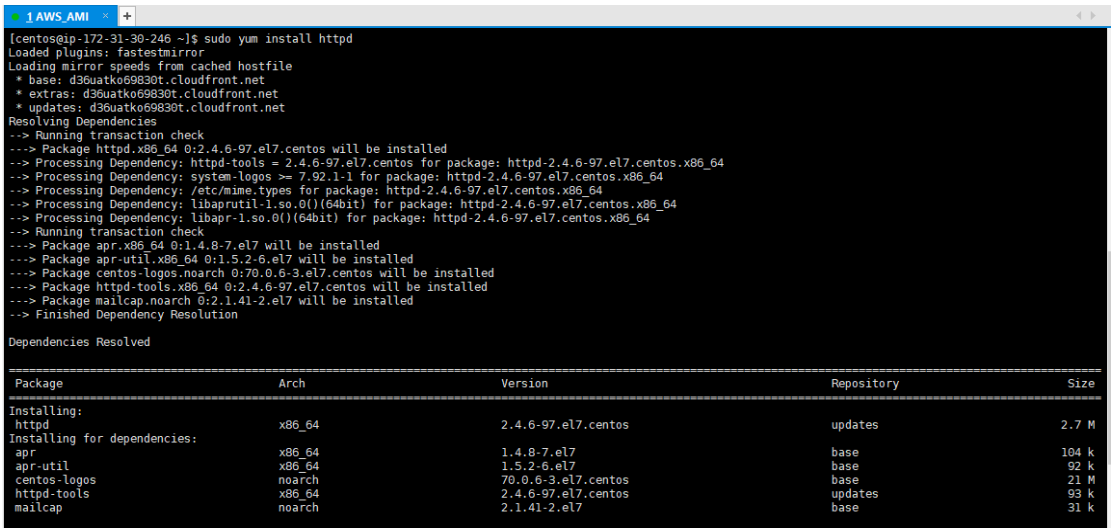


- SSH key pair must be created in order to access the newly created EC2 instance. If there is an already created key pair(.pem) available, that can be used reused for any instance that we deploy through AWS.

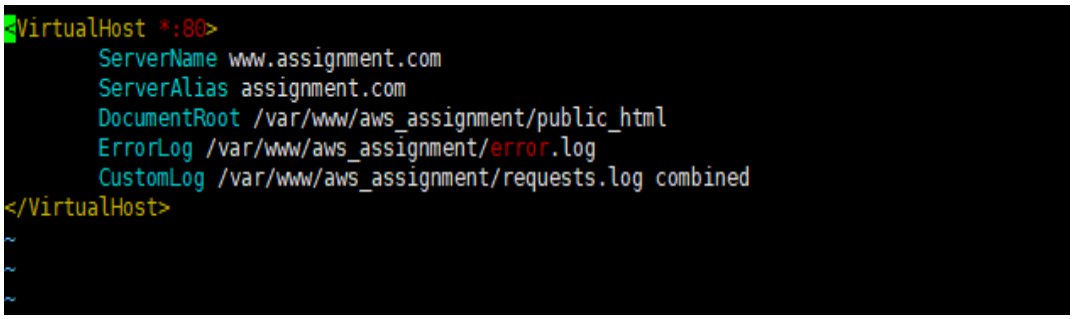


- Instance is ready and up and running as shown in the dashboard.

Preparing the EC2 instances to create the customized AMI templates

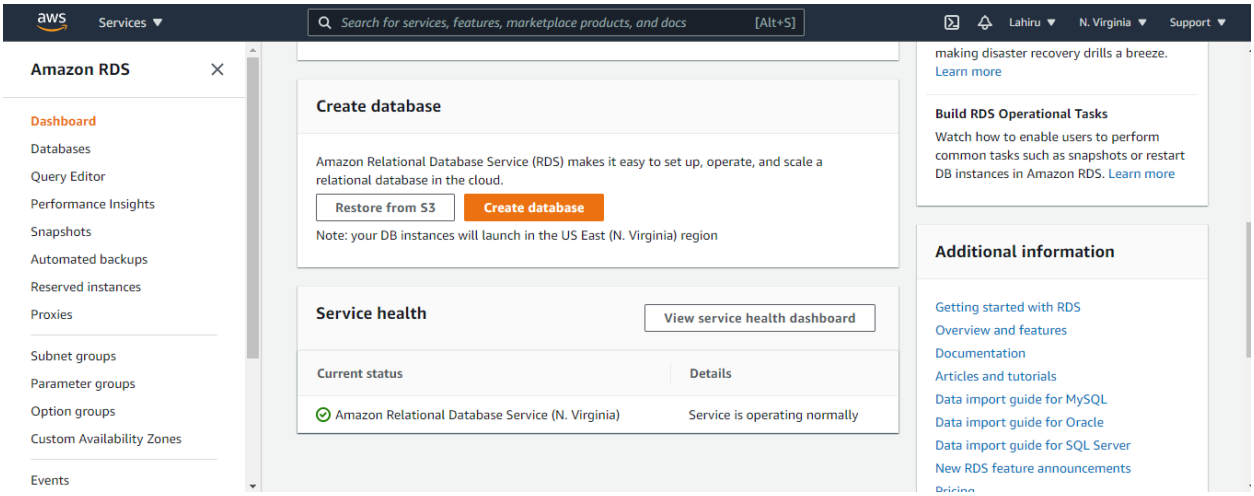


- Installing httpd (apache) web service in order to setup the web service.

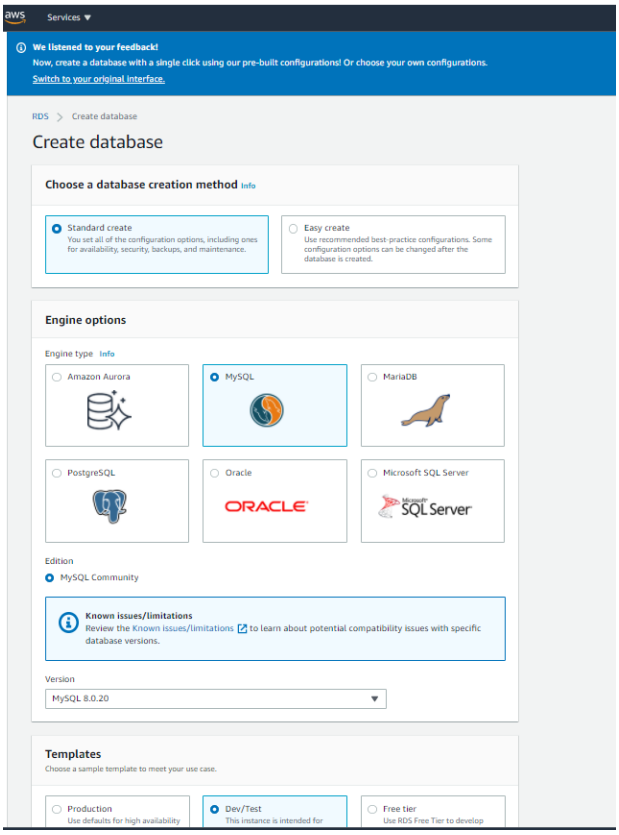


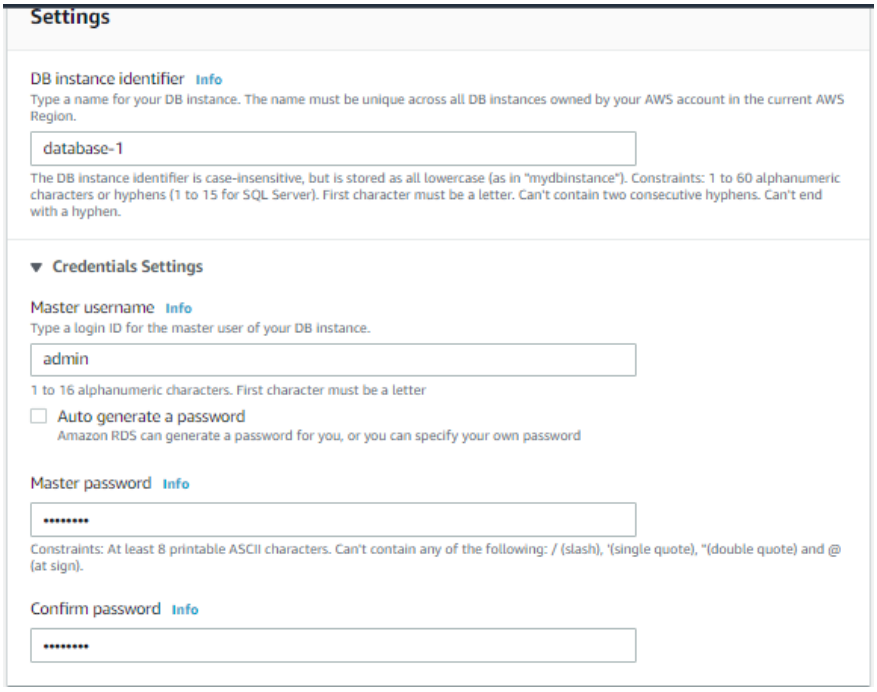
- Virtual host is created (/etc/httpd/conf.d/assignment.com.conf) in order to serve the web page which is placed in the document root. Virtual hosting allows multiple web applications to be served in one server. It is recommended rather than using the default web root with default config file.

Database creation

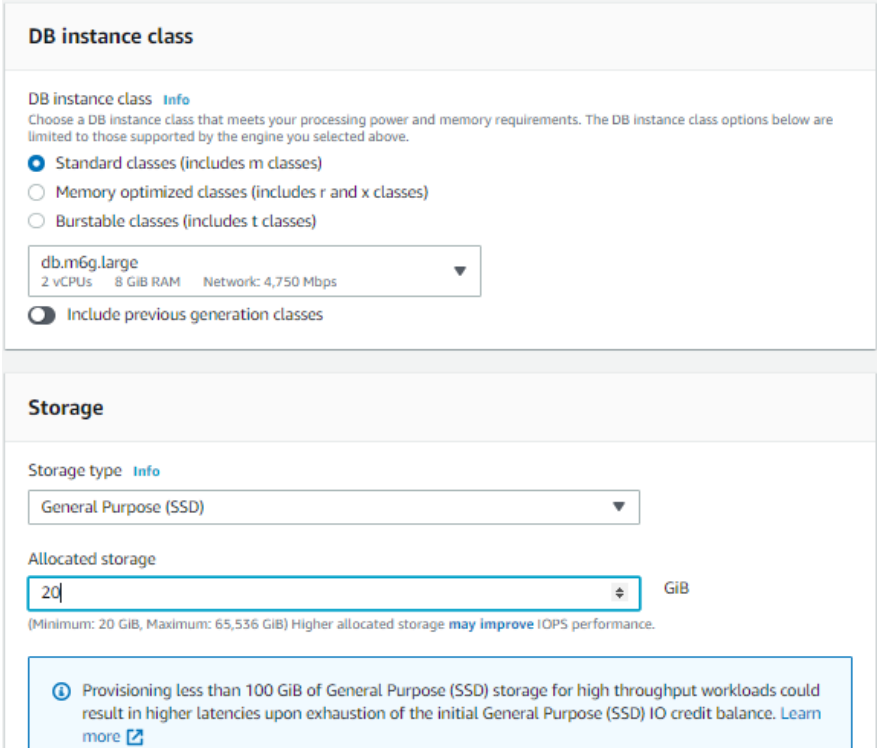


- AWS provide various database solutions like Relational Database Solution (RDS), Aurora, DynamoDB. A simple RDS solution like mysql can be used for this solution since we need to just store the timestamp and the status in the database only.





- DB identifier, master username and password must be provided.



- Database can be chosen from the given options to cater the requirement of the solution. The high performance database solutions will cost more.

Connectivity

Virtual private cloud (VPC) Info
VPC that defines the virtual networking environment for this DB instance.

Default VPC (vpc-7079fb0d)

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change the VPC selection.

Subnet group Info
DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

default

Public access Info

- Yes
  Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.
- No
  RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group
Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

- Choose existing
  Choose existing VPC security groups
- Create new
  Create new VPC security group

New VPC security group name

AWS_Assignment_RDS

Availability Zone Info

No preference

Additional configuration

Database port Info
TCP/IP port that the database will use for application connections.

3306

- Database is also created under the same virtual private cloud and the default port is chosen as 3306.

Database authentication

Database authentication options Info

- (●) Password authentication
  Authenticates using database passwords.
- ( ) Password and IAM database authentication
  Authenticates using the database password and user credentials through AWS IAM users and roles.
- ( ) Password and Kerberos authentication (not available for this version)
  Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

▸ Additional configuration

Database options, encryption enabled, backup enabled, backtrack disabled, Performance Insights enabled, Enhanced Monitoring enabled, maintenance, CloudWatch Logs, delete protection disabled

Estimated monthly costs

DB instance	110.96 USD
Storage	2.30 USD
Total	**113.26 USD**

This billing estimate is based on on-demand usage as described in Amazon RDS Pricing. Estimate does not include costs for backup storage, IOs (if applicable), or data transfer.

Estimate your monthly costs for the DB Instance using the AWS Simple Monthly Calculator.

You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

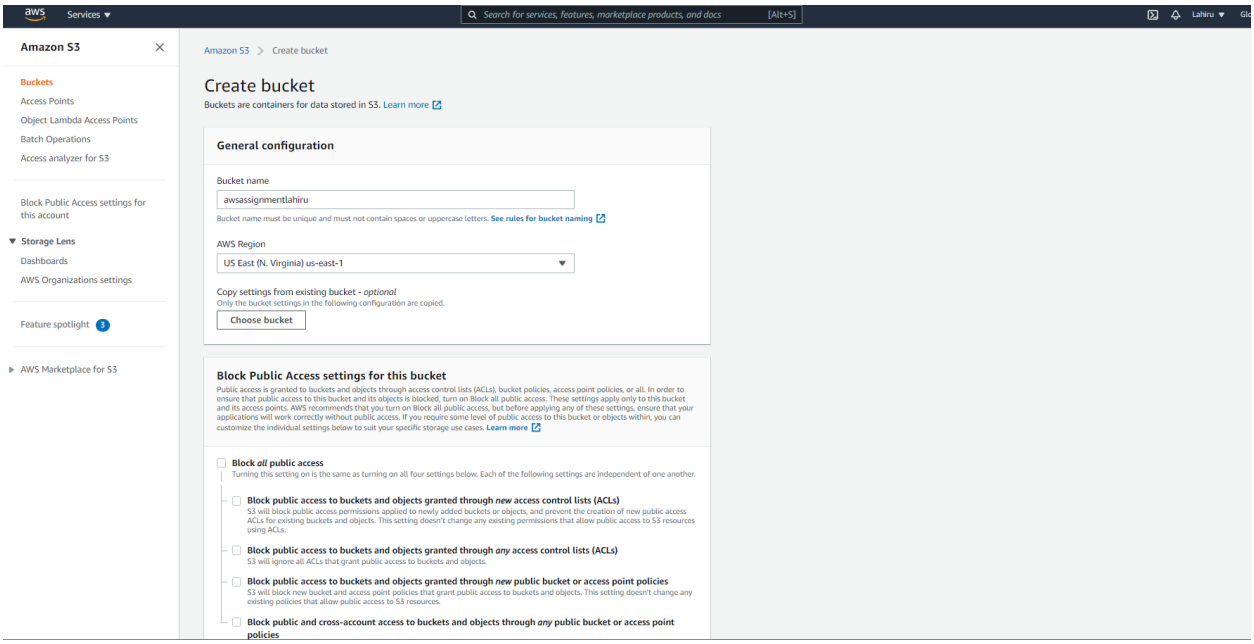
Cancel | Create database

- Different authentication modes can be chosen for the database. IAM based authentication requires IAM roles to be created and applied. The password authentication is the classic way of accessing the DBMS. This username and password will be used by the monitoring instance to connect to the DBMS.

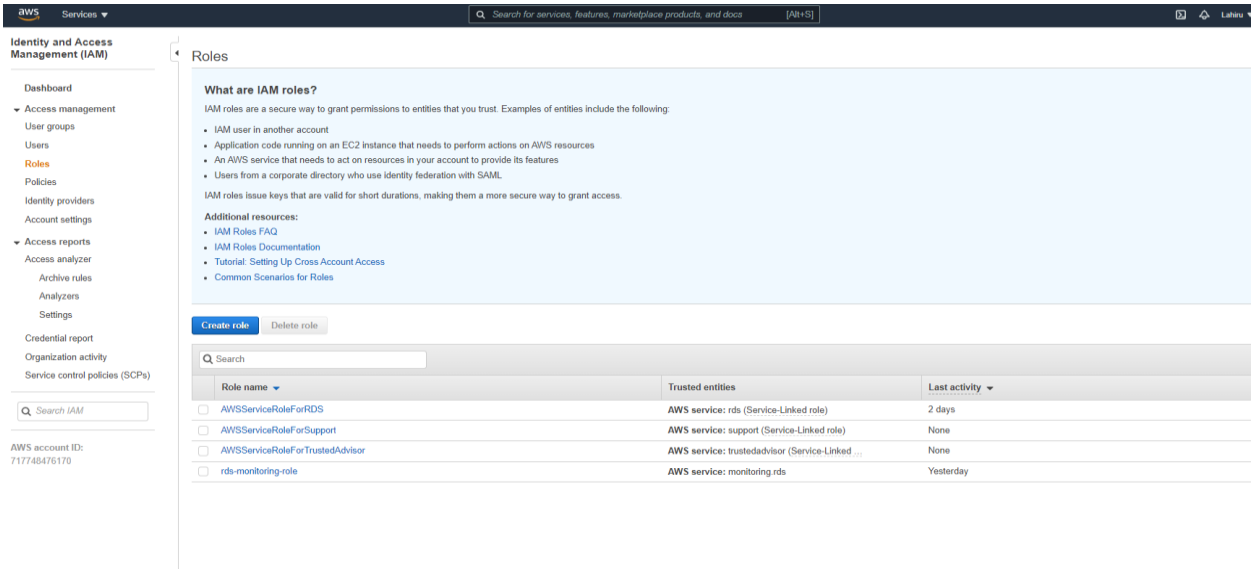
```
[root@ip-172-31-30-246 ~]# mysql -h database-1.crdxxeqjw7mf.us-east-1.rds.amazonaws.com -u admin -P 3306 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 87
Server version: 8.0.20 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> create database web_page_status;
Query OK, 1 row affected (0.00 sec)

MySQL [(none)]> use web_page_status;
Database changed
MySQL [web_page_status]> create table status(status VARCHAR(50) NOT NULL, timestamp DATE NOT NULL);
Query OK, 0 rows affected (0.02 sec)

MySQL [web_page_status]> show tables;
+--------------------------+
| Tables_in_web_page_status |
+--------------------------+
| status                   |
+--------------------------+
1 row in set (0.00 sec)

MySQL [web_page_status]> exit
Bye
```

- Logged in to the RDS through mysql client and created the database and table. Values will be inserted in to the table during the execution of the script1. Password is stored in the .my.cnf file and read/write permission changed only to the owner.

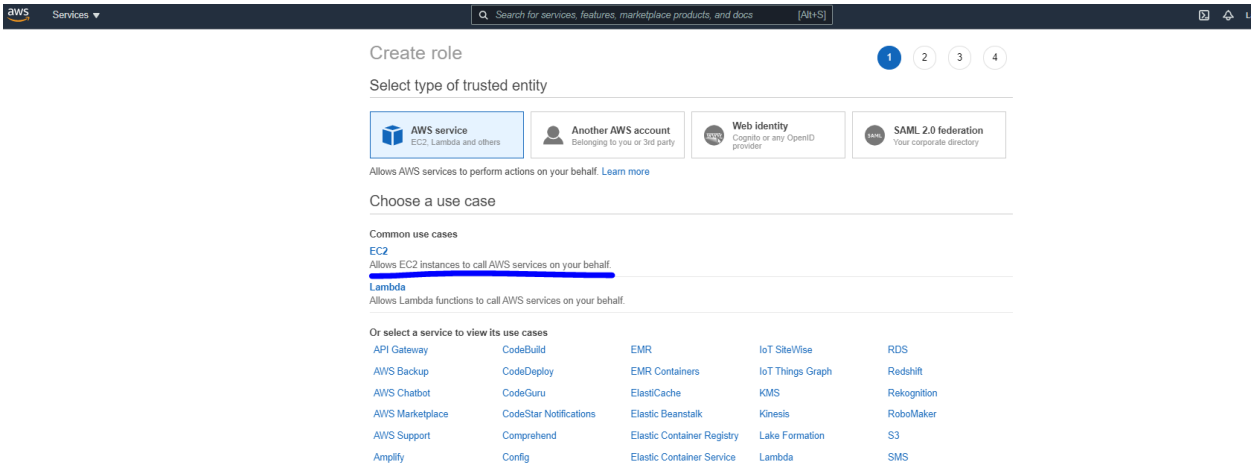
S3 bucket creation with IAM role access for EC2



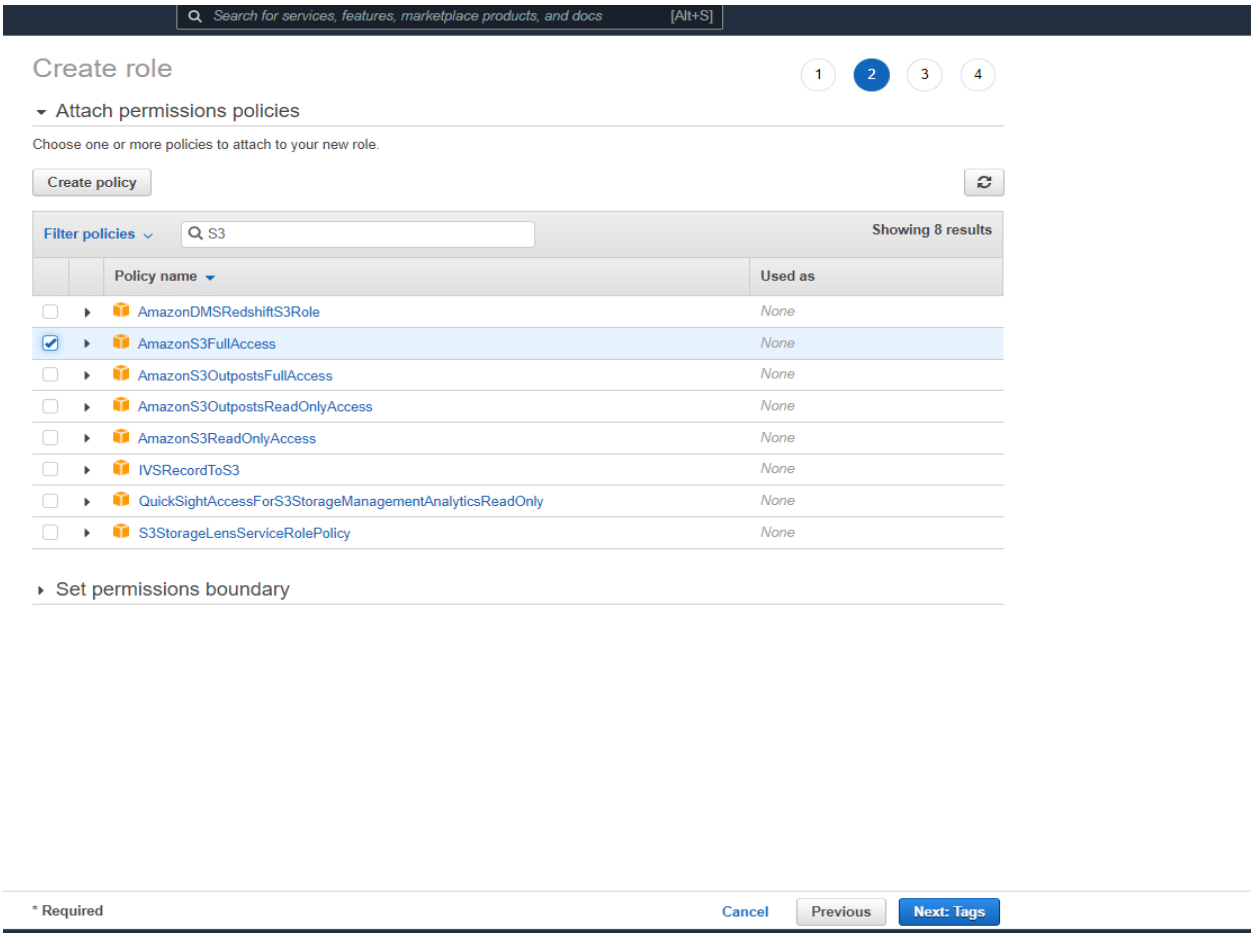
- AWS provides a wide range of storage solutions like Amazon S3, Cloudfront, EFS, EBS, glacier and storage gateway. All these solutions serve different purposes and has different costing architectures. Therefore, simple object-based storage solution which is known as S3 bucket is ideal for this solutions to store the logs. It operates independent and can be easily accessed through IAM roles.



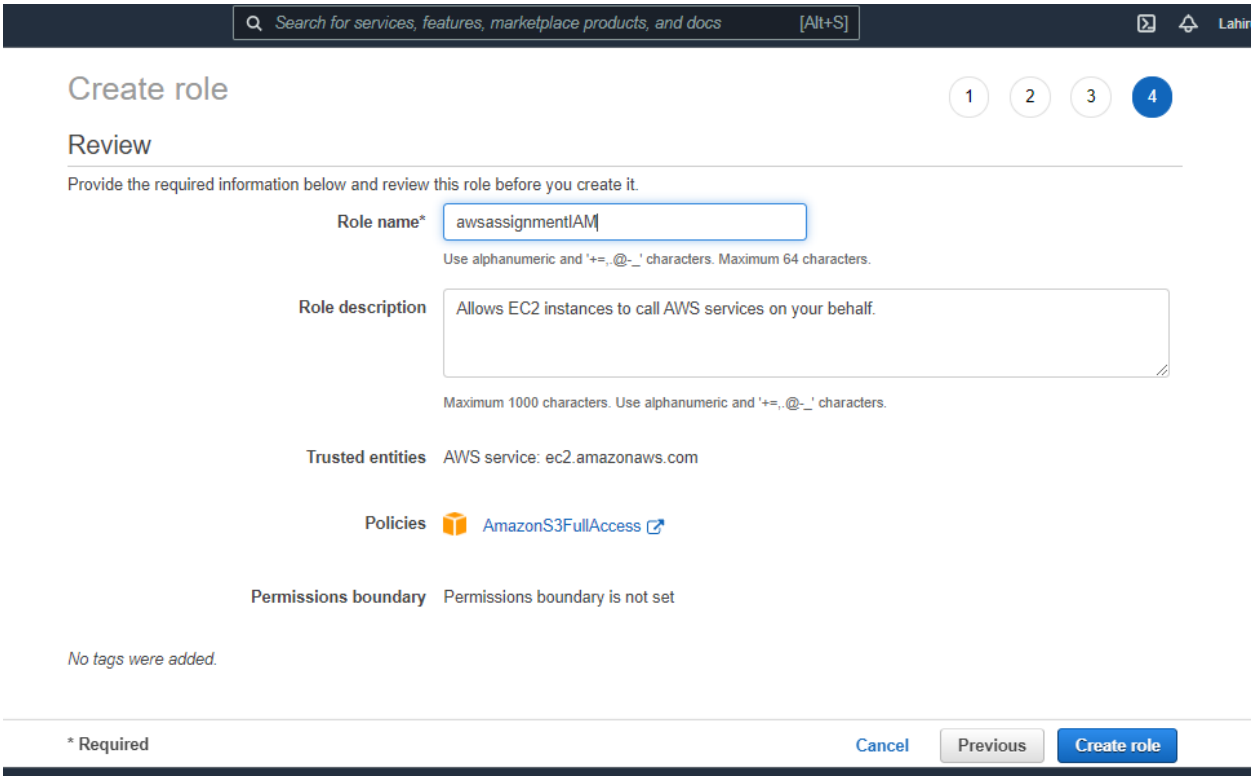
- Access can be granted to the S3 bucket by assigning the IAM role to the instance or users.



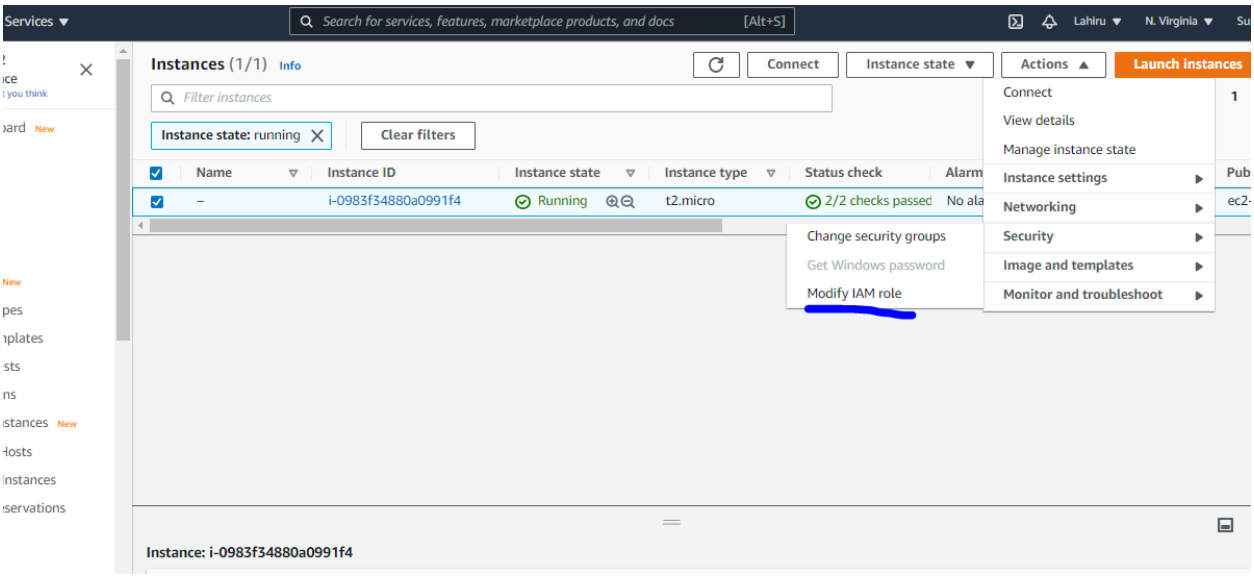
- Two use cases provided as the options to select to create the IAM role. Monitoring node needs access to the S3 bucket to push the log files. That requires the EC2 instance to access the S3 bucket using IAM role.

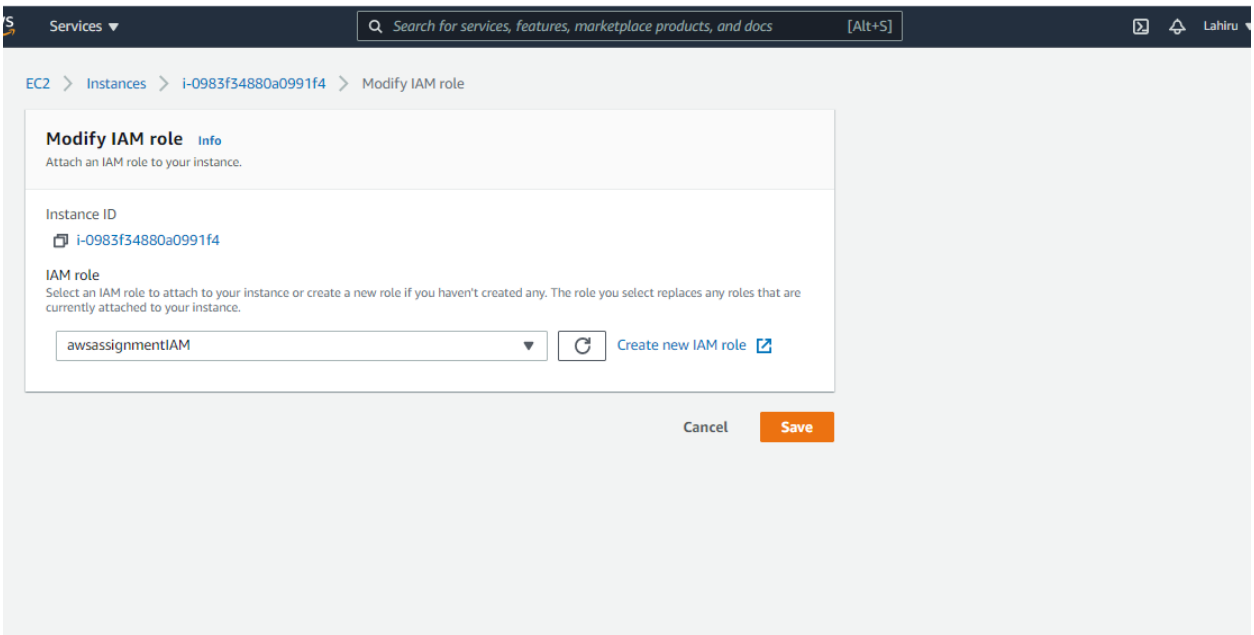


- Full access to S3 bucket is granted to the IAM role that is being created.



- An identifier must be provided for the IAM role.





- Final step is to apply the IAM role to the monitoring instance

Setting up the monitoring instance.

```
[centos@ip-172-31-37-229 ~]$ sudo yum install postfix
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: d36uatko69830t.cloudfront.net
 * extras: d36uatko69830t.cloudfront.net
 * updates: d36uatko69830t.cloudfront.net
Resolving Dependencies
--> Running transaction check
---> Package postfix.x86_64 2:2.10.1-9.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================================
 Package                    Arch                    Version                    Repository                    Size
================================================================================================================================
Installing:
 postfix                    x86_64                  2:2.10.1-9.el7             base                          2.4 M

Transaction Summary
================================================================================================================================
Install  1 Package

Total download size: 2.4 M
Installed size: 12 M
Is this ok [y/d/N]:
```

```
[centos@ip-172-31-37-229 ~]$ sudo yum install mailx
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: d36uatko69830t.cloudfront.net
 * extras: d36uatko69830t.cloudfront.net
 * updates: d36uatko69830t.cloudfront.net
Resolving Dependencies
--> Running transaction check
---> Package mailx.x86_64 0:12.5-19.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================================
 Package                    Arch                    Version                    Repository                    Size
================================================================================================================================
Installing:
 mailx                      x86_64                  12.5-19.el7                base                          245 k

Transaction Summary
================================================================================================================================
Install  1 Package

Total download size: 245 k
```

- The monitoring instance need to send emails to an external party (application support team). Therefore, the mailx and postfix packages installed in order to do the email configurations.

```
relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt
smtp_tls_security_level = encrypt
smtp_sasl_security_options = noanonymous
smtp_sasl_tls_security_options = noanonymous
inet_protocols = ipv4
~
~
~
~
~
~
~
```

- Main configurations for the postfix. SMTP relay is useful in forwarding the email rather than maintaining a mail server. Therefore, relayhost is given as smtp.gmail.com which is provided by the gmail. Credentials are saved in the /etc/postfix/sasl_passwd file.

```
[smtp.gmail.com]:587    alerts.aws.assignment@gmail.com:[redacted]
~
~
```

- Sender email address and the password is stored in the file

```
[centos@ip-172-31-30-246 ~]$ sudo postmap /etc/postfix/sasl_passwd
[centos@ip-172-31-30-246 ~]$ ll /etc/postfix/sasl_passwd.db
-rw-------. 1 root root 12288 Apr 29 18:07 /etc/postfix/sasl_passwd.db
[centos@ip-172-31-30-246 ~]$
```

- Run postmap /etc/postfix/sasl_passwd command and restart the postfix service

Setting up the environment - Instructions.

1. Run the cloudformation script in https://gitlab.com/lahirumal/aws_assignment
2. Since cloudformation script uses private AMIs and the AMI ID values in the environment.json file must be changed in order to execute under a different AWS account.
3. Install httpd in the web instances using 'yum install httpd'
4. Install postfix and mailx using 'yum install postfix' and 'yum install mailx' in monitoring instance.
5. Copy the configuration files as provided in the folder to the required locations as mentioned below.
    a. .my.cnf -> /home/centos/.my.cnf in Monitoring server (AMI)
    b. assignment.com.conf -> /etc/httpd/conf.d/assignment.com.conf in web instances (AMI)
    c. httpd.conf -> /etc/httpd/conf/httpd.conf in web instances (AMI)
    d. main.cf -> /etc/postfix/main.cf in Monitoring server (AMI)
    e. sasl_password -> /etc/postfix/sasl_passwd (Run postmap /etc/postfix/sasl_passwd) in Monitoring server (AMI)
    f. script1.sh -> /home/centos/script1.sh
    g. script2.sh -> /home/centos/script2.sh
6. Both the scripts are recommended to be copied to a home folder of the user (centos) that the scripts are being executed and the below contrab entries must be placed under the particular user in each server
    a. Web application nodes.
        i. 59 23 * * * sh /home/centos/log_rotate.sh > /dev/null 2>&1
        ii. 00 08 * * 1-5 sudo /bin/systemctl start httpd.service > /dev/null 2>&1
        iii. 00 16 * * 1-5 sudo /bin/systemctl stop httpd.service > /dev/null 2>&1
    b. Monitoring node (Based on the time interval to execute the periodic check and log extraction – every 30 minutes).
        i. */30 * * * * sh /home/centos/script1.sh > /dev/null 2>&1
        ii. 00 00 * * * sh /home/centos/script2.sh > /dev/null 2>&1
7. It is recommended to create two AMIs using the above steps and then pass the AMI IDs to the cloudformation script which will automate the process. Before executing the cloudformation script, an IAM role with the name 'awsassignmentIAM' needed to be created with the below policies.
    a. AutoScalingReadOnlyAccess
    b. AmazonS3FullAccess
    c. EC2InstanceConnect
8. SSH key pair needed to be created in the name "AWS_Assignment_AMI" in order to access the servers via ssh. Key will be applied to each instances via the cloudformation script.
9. Once everything is ready execute the below command to create the cloudformation stack using the cloudformation.yaml and environment.json file in the local PC.
    a. aws cloudformation create-stack --stack-name startmyinstance --template-body file://cloudformation.yaml --parameters file://environment.json

Limitations and Suggestions

- Public DNS is suggested to be used for the web application. Currently the end point of the load balancer is hard coded .
    - Eg - http://startmyin-loadbala-641fppoj4jun-781586019.us-east-1.elb.amazonaws.com
- SSL certificate can be installed at the load balancer level will provide more security to the web application.
- Private DNS can be used for the MySQL RDS to connect from the monitoring instance. Currently the end point is hard coded into the script.
    - Eg - lseg-rds.crdxxeqjw7mf.us-east-1.rds.amazonaws.com
- Resources with least costs were used in the solution and therefore the better performance, security and logging features provided by AWS are not used.

Output of the solution.

Hello World!!!

- Web page is loading from the web application.

```
[centos@ip-10-192-21-42 aws_assignment]$ ls
error.log  error.log_ip-10-192-21-42.ec2.internal_043021  public_html  requests.log  requests.log_ip-10-192-21-42.ec2.internal_043021
[centos@ip-10-192-21-42 aws_assignment]$
```

```
[centos@ip-10-192-20-85 aws_assignment]$ ls
error.log  error.log_ip-10-192-20-85.ec2.internal_043021  public_html  requests.log  requests.log_ip-10-192-20-85.ec2.internal_043021
[centos@ip-10-192-20-85 aws_assignment]$
```

- Logs are rotated in the web server instances.

```
[centos@ip-10-192-10-155 ~]$ ls
script1.log  script1.sh  script2.log  script2.sh
[centos@ip-10-192-10-155 ~]$ cat script1.log

04/30/21 03:00:11 Web service is up
04/30/21 03:00:11 Script_1 successfully executed
04/30/21 03:00:12 Web service is up
04/30/21 03:00:12 Script_1 successfully executed
[centos@ip-10-192-10-155 ~]$
```

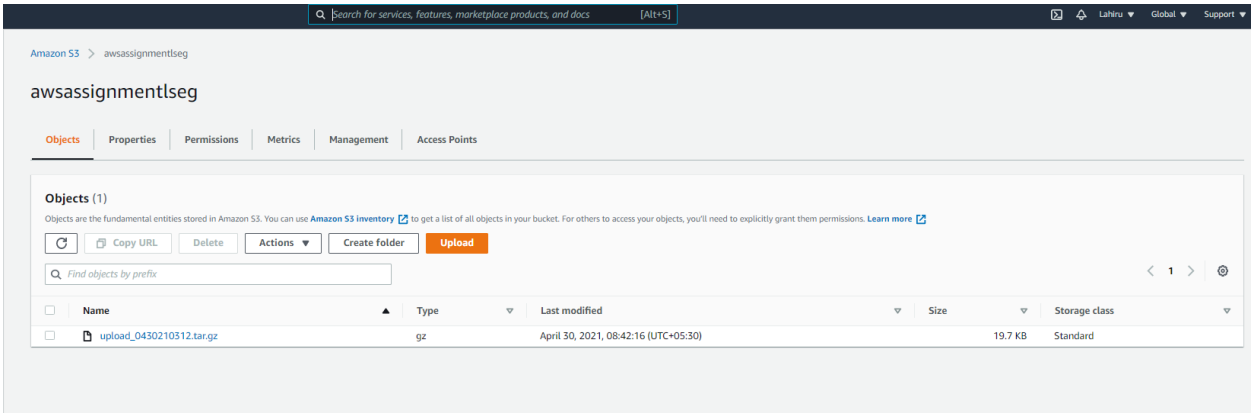
- Script 1 is getting successfully executed at both web instances.

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 217
Server version: 8.0.20 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> use web_page_status;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [web_page_status]> select * from status_log
    -> ;
+---------+-------------------+
| status  | timestamp         |
+---------+-------------------+
| success | 04/30/21 03:00:11 |
| success | 04/30/21 03:00:12 |
+---------+-------------------+
2 rows in set (0.01 sec)

MySQL [web_page_status]>
```

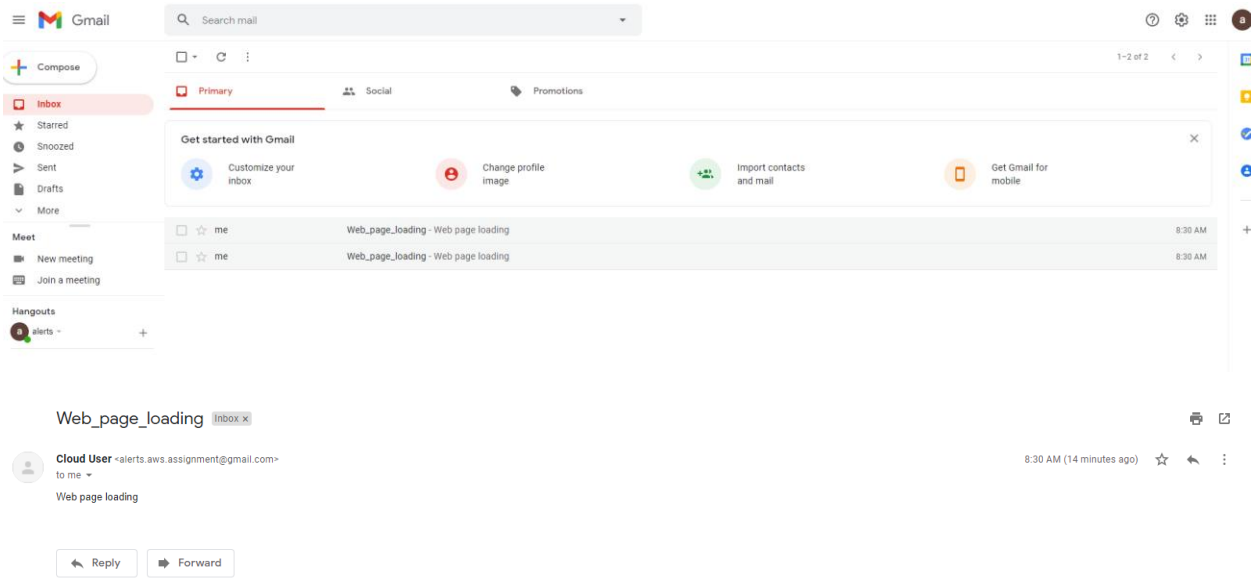
- Database is getting updated successfully.

```
[centos@ip-10-192-10-155 ~]$ ls
10.192.20.85_index.html  10.192.21.42_index.html  script12.log  script1.log  script1.sh  script2.log  script2.sh
[centos@ip-10-192-10-155 ~]$ ./script2.sh
EC2 Instance IPs
10.192.21.42 10.192.20.85
index.html                                                                                                  100%  124    91.3KB/s   00:00
error.log_ip-10-192-21-42.ec2.internal_043021                                                               100% 1638   738.1KB/s   00:00
requests.log_ip-10-192-21-42.ec2.internal_043021                                                            100% 1638   669.5KB/s   00:00
upload: ./upload_0430210312.tar.gz to s3://awsassignmentlseg/upload_0430210312.tar.gz
index.html                                                                                                  100%  124   166.5KB/s   00:00
error.log_ip-10-192-20-85.ec2.internal_043021                                                               100%  223KB  29.6MB/s   00:00
requests.log_ip-10-192-20-85.ec2.internal_043021                                                            100%  223KB  30.2MB/s   00:00
upload: ./upload_0430210312.tar.gz to s3://awsassignmentlseg/upload_0430210312.tar.gz
[centos@ip-10-192-10-155 ~]$ cat script2.log

04/30/21 03:12:12 Script_2 successfully executed
04/30/21 03:12:12 Script_2 successfully executed
[centos@ip-10-192-10-155 ~]$
```

- Script2 getting successfully executed.



- Compressed file is successfully uploaded in to the S3 bucket.



- Email notifications are sent to the alerts inbox for both web instances.

Scripts

Scripts are available at https://gitlab.com/lahirumal/aws_assignment as well.

1. Cloudformation.yaml
2. Environment.json
3. Script1.sh
4. Script2.sh