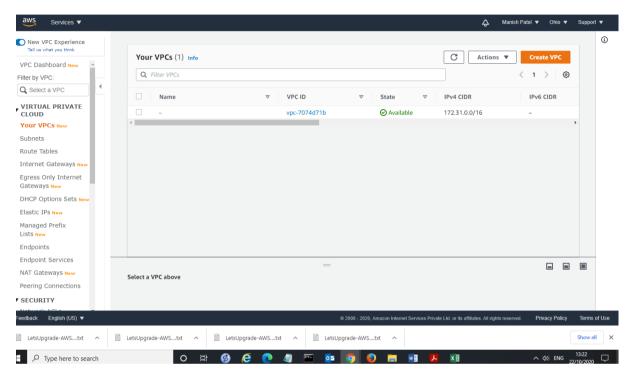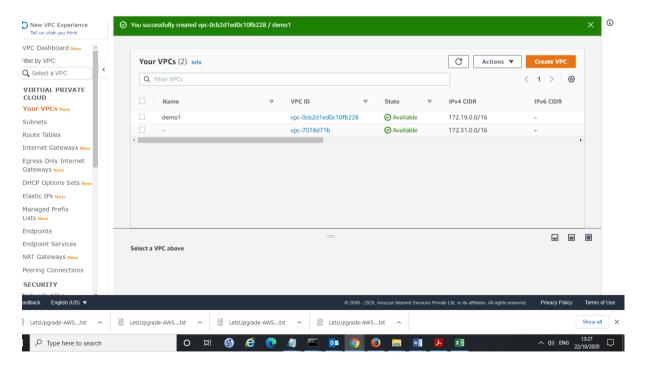# Assignment Day 7 and 8 | 18th October 2020

Manish Patel
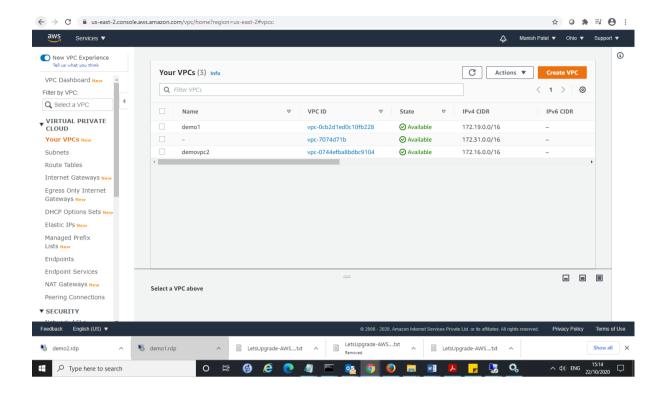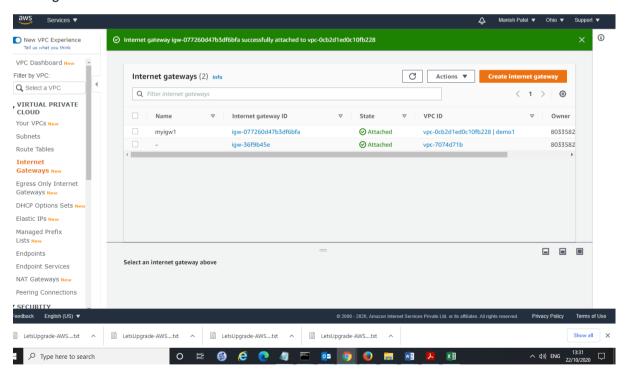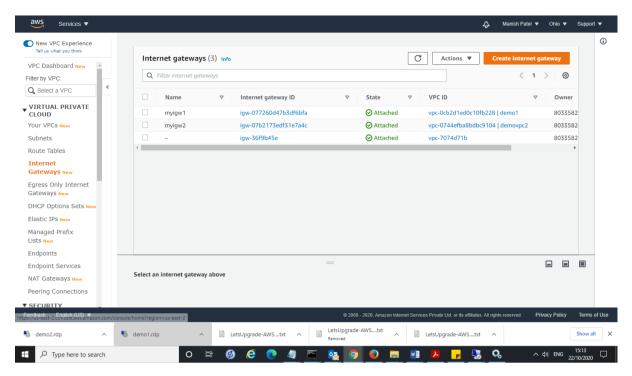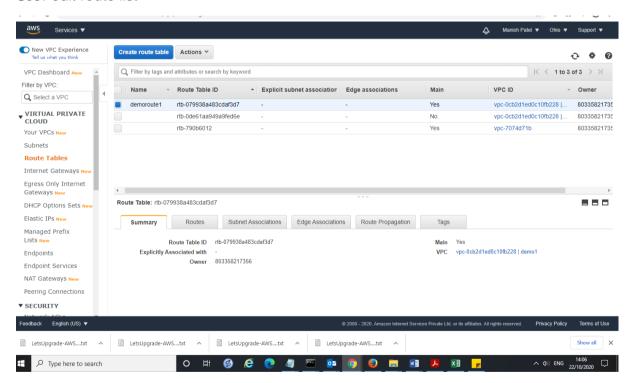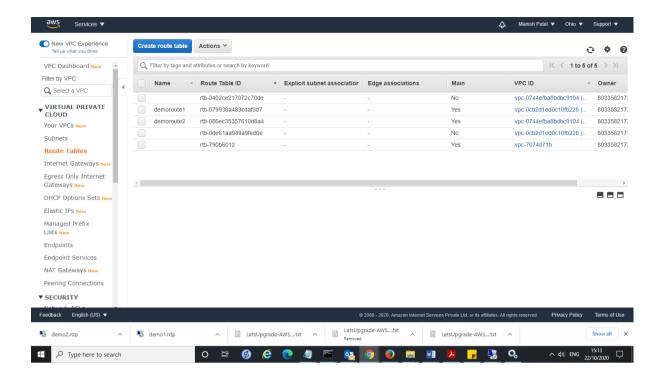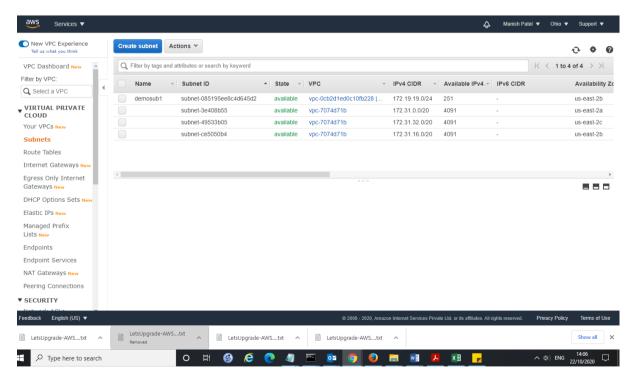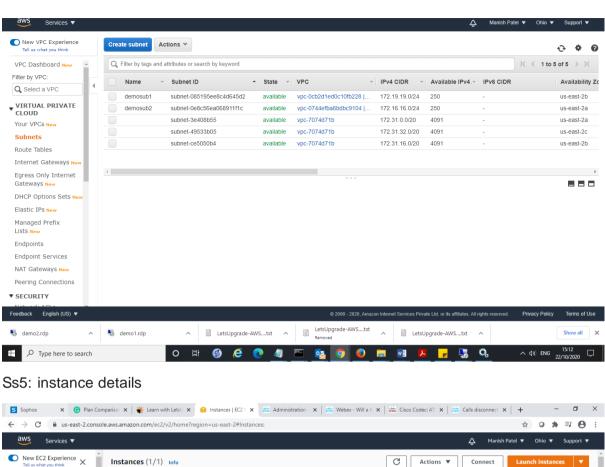
PROJECT 1:
VPC peering

Ss1: VPCs list

Demo1 created

Ss2: igw list

Ss3: edit route list

Ss4: subnet list

Ss5: instance details

SS

Ss6: success public, rto private IP

```
C:\Users\Manish_patel>ping 52.15.220.58

Pinging 52.15.220.58 with 32 bytes of data:
Reply from 52.15.220.58: bytes=32 time=216ms TTL=100
Reply from 52.15.220.58: bytes=32 time=217ms TTL=100
Reply from 52.15.220.58: bytes=32 time=216ms TTL=100
Reply from 52.15.220.58: bytes=32 time=216ms TTL=100

Ping statistics for 52.15.220.58:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 216ms, Maximum = 217ms, Average = 216ms

C:\Users\Manish_patel>ping 172.19.19.36

Pinging 172.19.19.36 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.19.19.36:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Manish_patel>
```

Ss7: peering with req and acceptor

Ss8: success for private

Project 2:
IAM

Task 1:Creating users without permissions-IAM password policy check.
Ss1: user summary with all tab information

Task 2:Creating users without the IAM password policy.
Ss2: user summary with all tab information

Task 3:Create a user with S3 full access
Ss3: User summary

Task4: Create a group with ec2 full access
Ss4: group summary

Task 5: Add user to a group and check if user policy and the group policy is reflecting on the user

Ss5: user summary with permissions

Ss6: login as this user show that this policy is in effect

Task 6:Copy policies from the existing user
Ss7: attach user summary of the user from which you create a new user

Ss8: login as this user show that this policy is in effect

Task 7:Add user to a group in the process of creating a user

Task8: setting a password policy
Ss9: password policy screen

Ss10: login as the user and show password incompatibility error

User name* rashmin

⊕ Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ Programmatic access
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ AWS Management Console access
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ○ Autogenerated password
● Custom password

pass@12345
☑ Show password
The password does not conform to the account password policy:
• it must contain an upper case character

Require password reset ☑ User must create a new password at next sign-in

* Required   Cancel   Next: Permissions

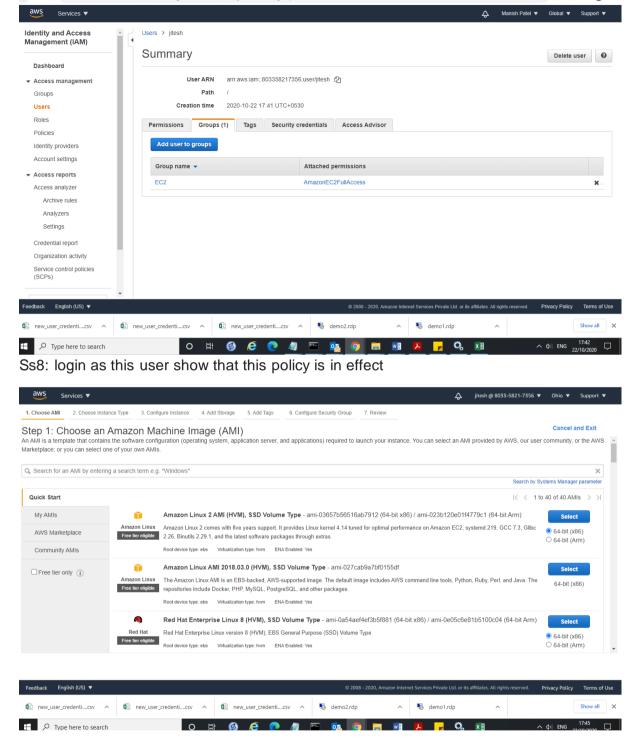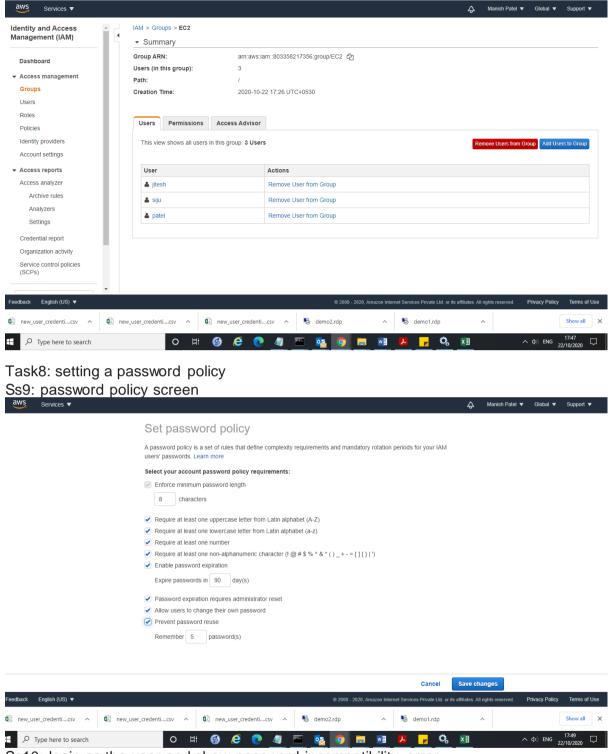## Task 9:Enabling MFA and using an MFA device
Ss11: enable MFA

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console.

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

▲ Password

▼ Multi-factor authentication (MFA)

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.

Device type	Serial number	Actions
Virtual	arn:aws:iam::803358217356:mfa/root-account-mfa-device	Manage

▲ Access keys (access key ID and secret access key)

▲ CloudFront key pairs

▲ X.509 certificate

▲ Account identifiers

Ss12: login screen for MFA

aws

Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: manishpatel.ecengg@gmail.com

MFA code

[   ]

[Submit]

Troubleshoot MFA

Cancel

**Amazon
Aurora Serverless**

Automatically starts, scales, and shuts down your database

aws