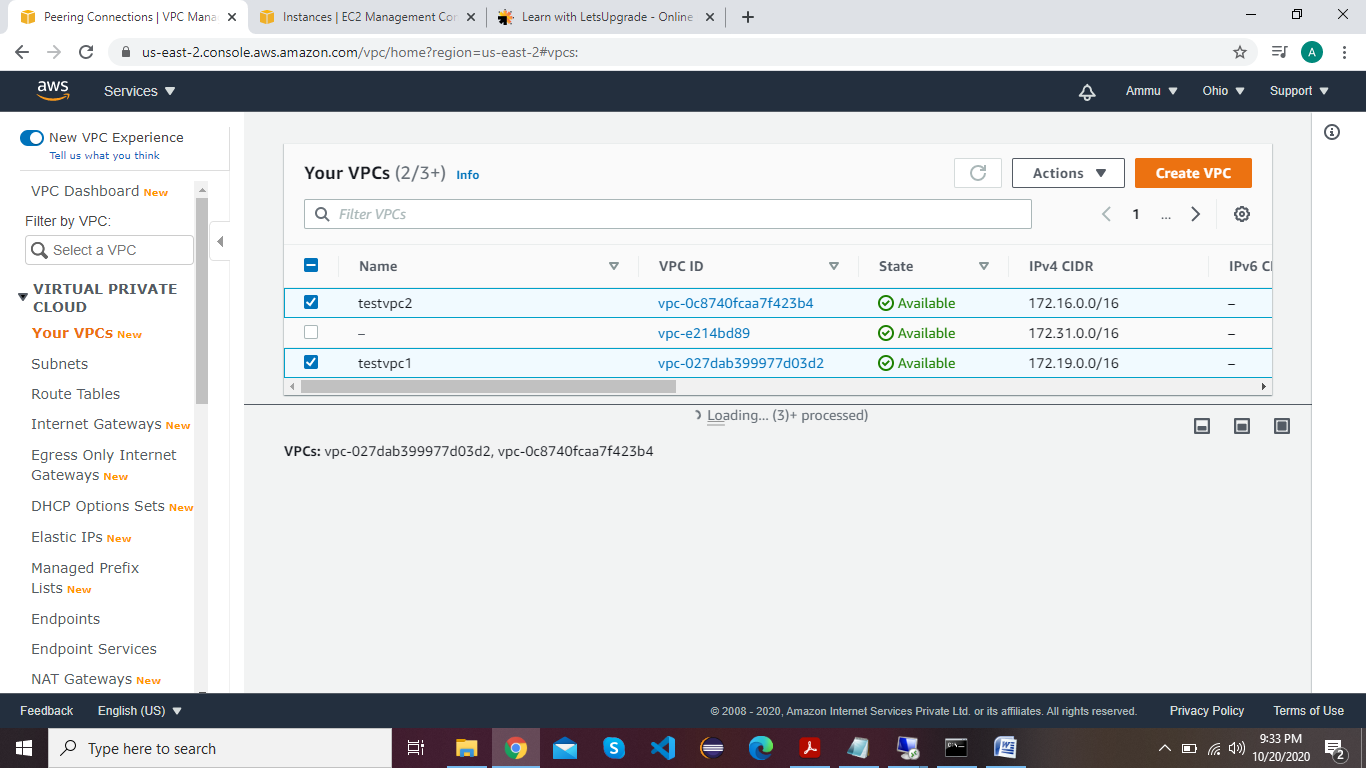
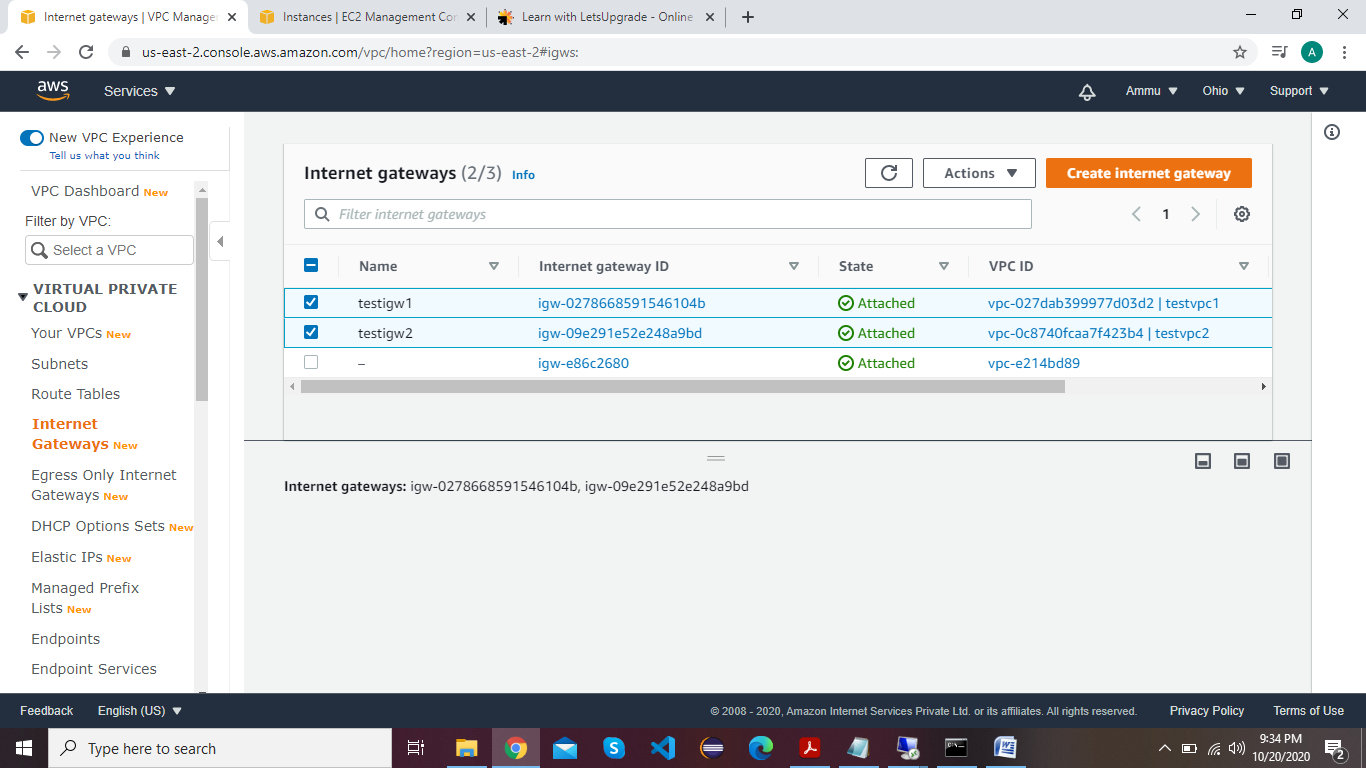
**PROJECT 1:VPC peering**

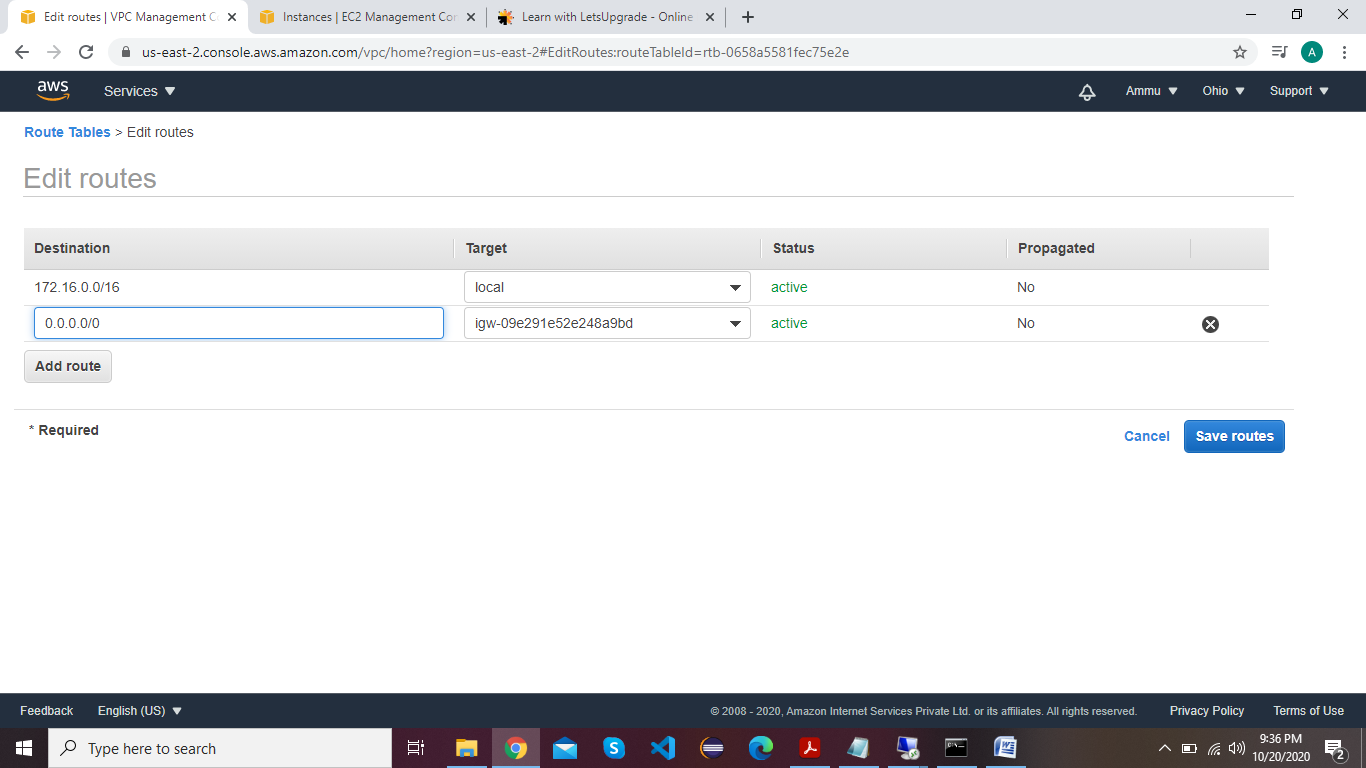
VPC’s List:



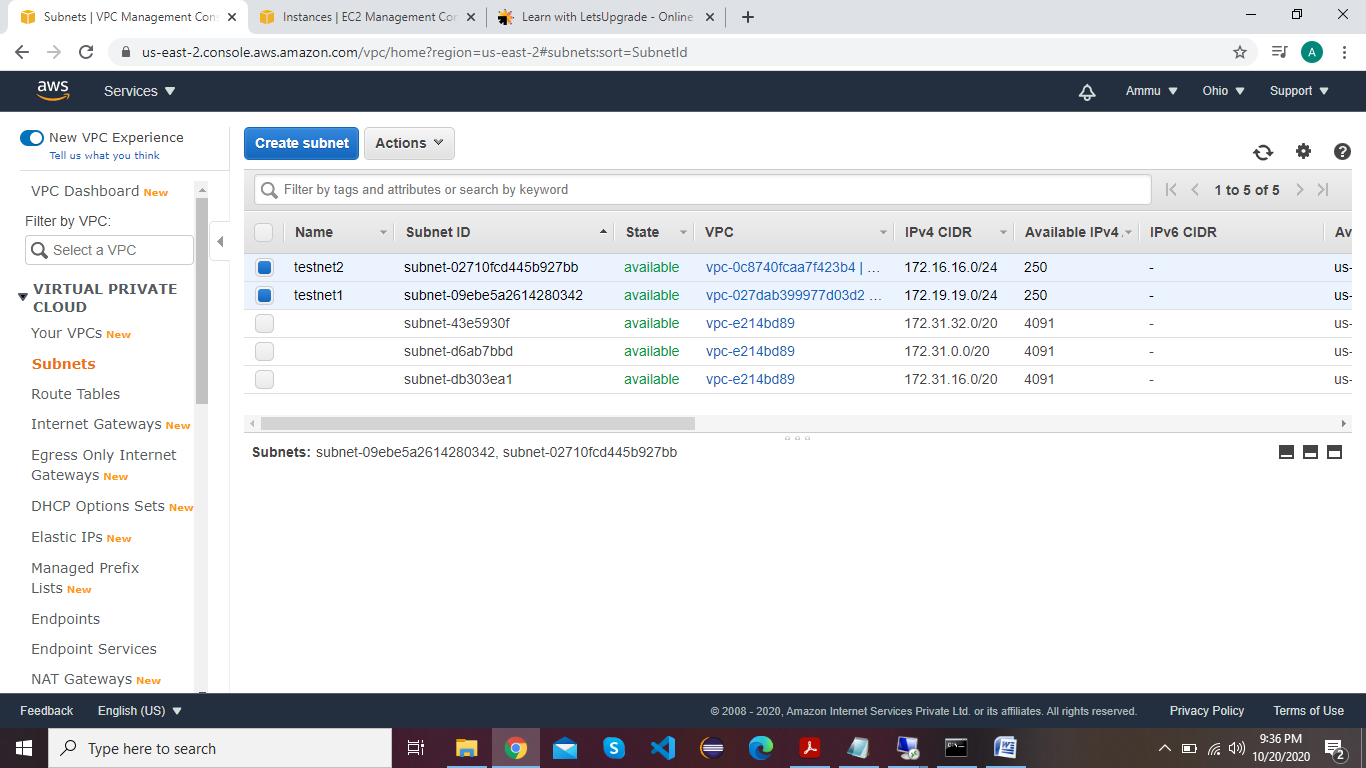
Internet Gateway’s and attached to VPC’s:



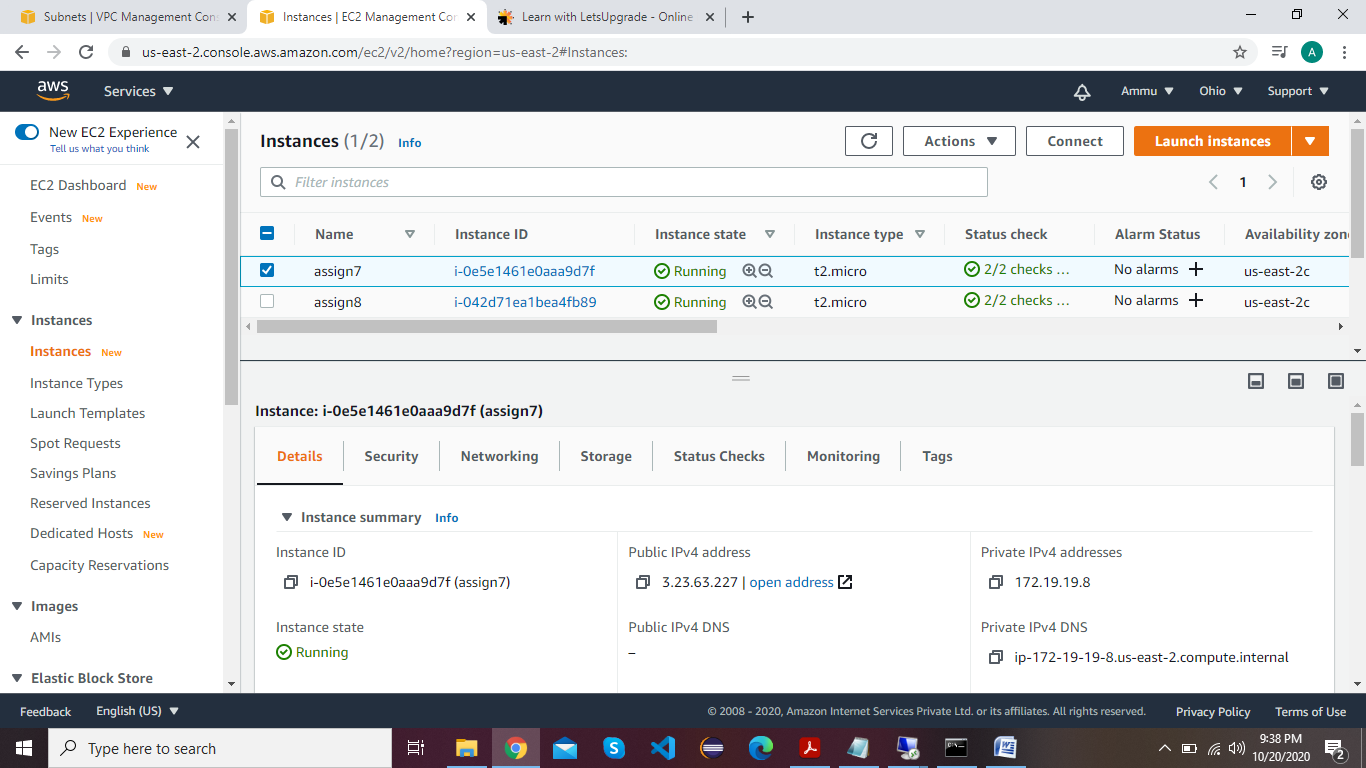
Route Tables List:



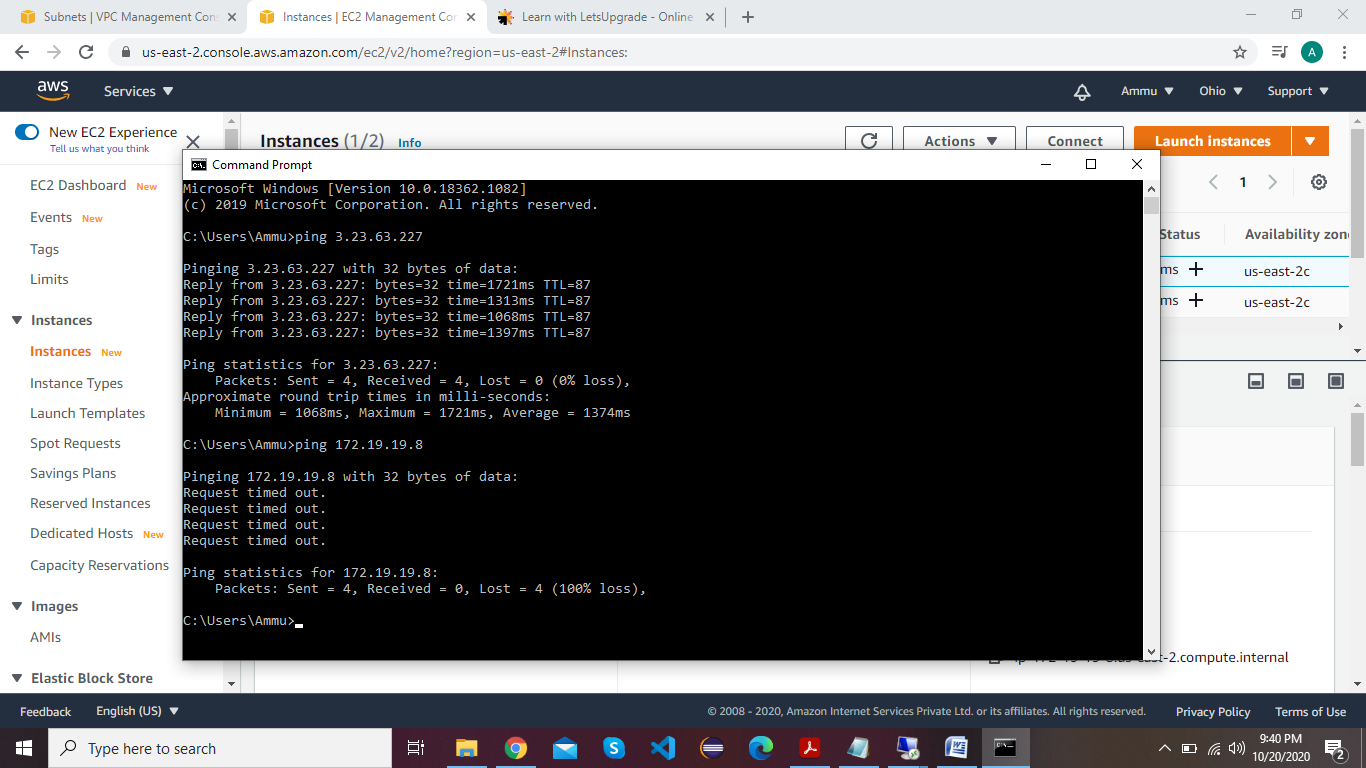
Subnets List:



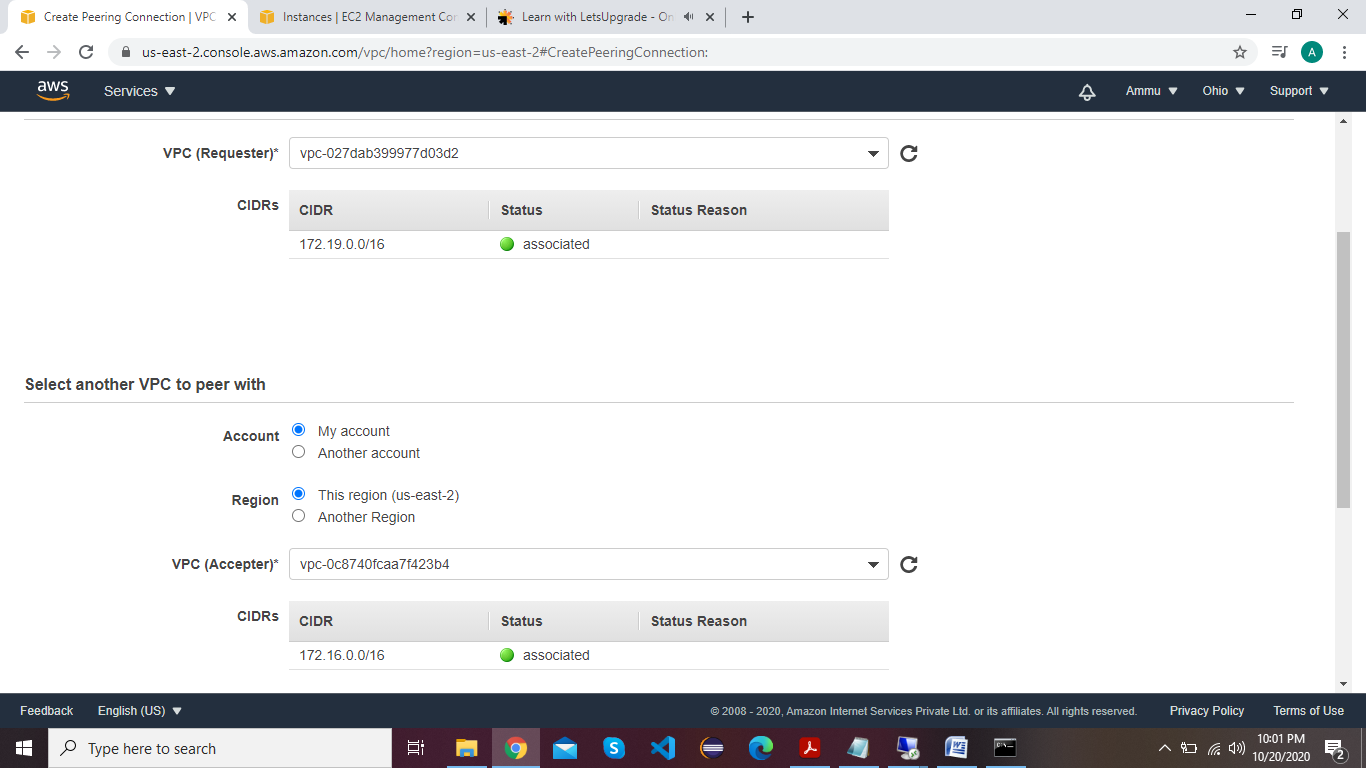
Instance Details :



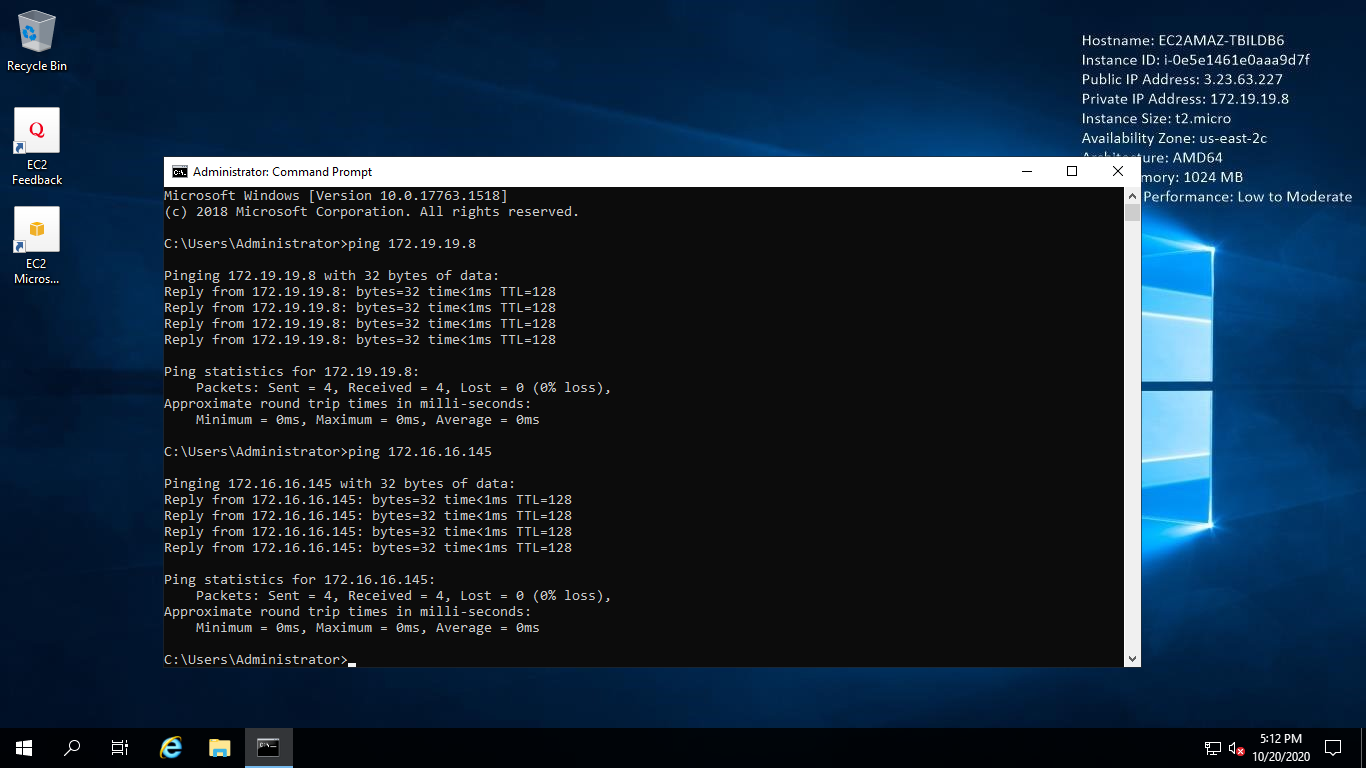
Public ip Success and Private ip Request time out:



Peer Connection with Requestor & Acceptor:

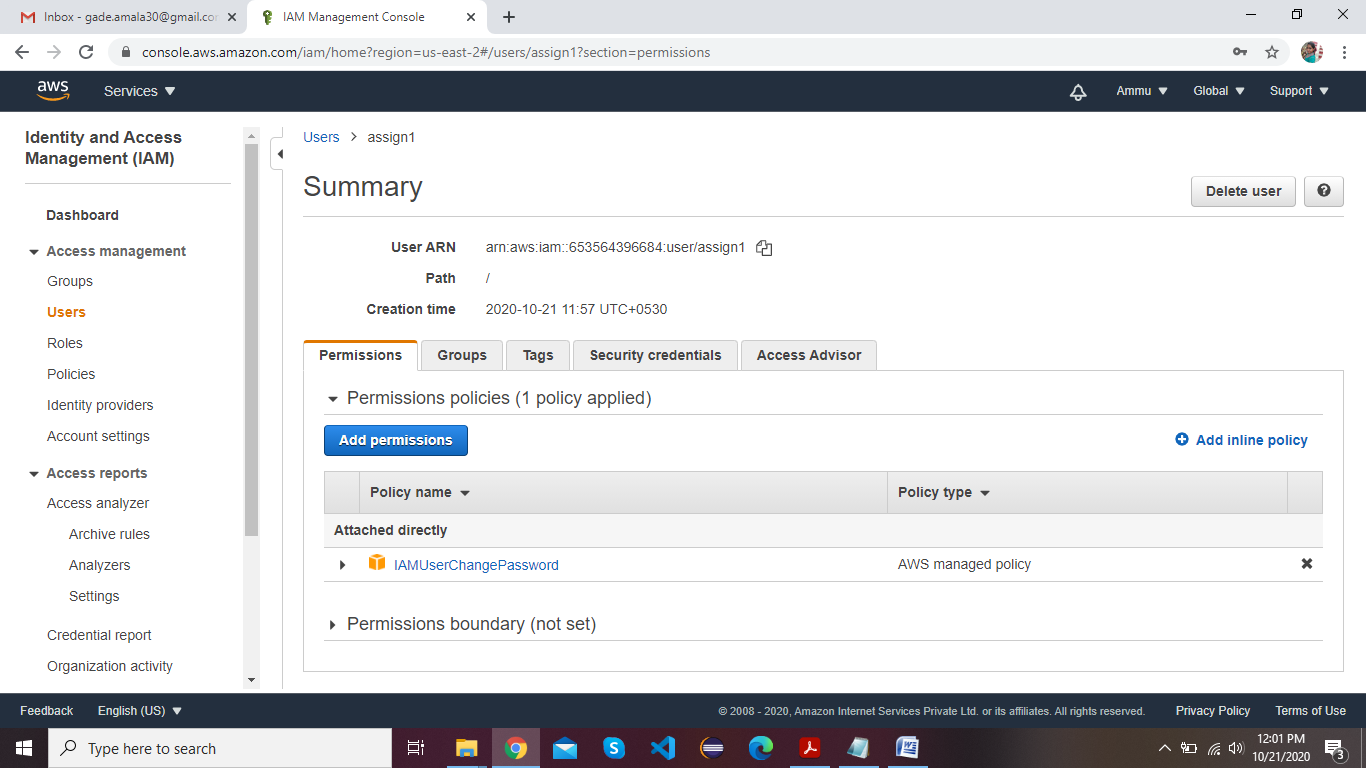


Success Private list:

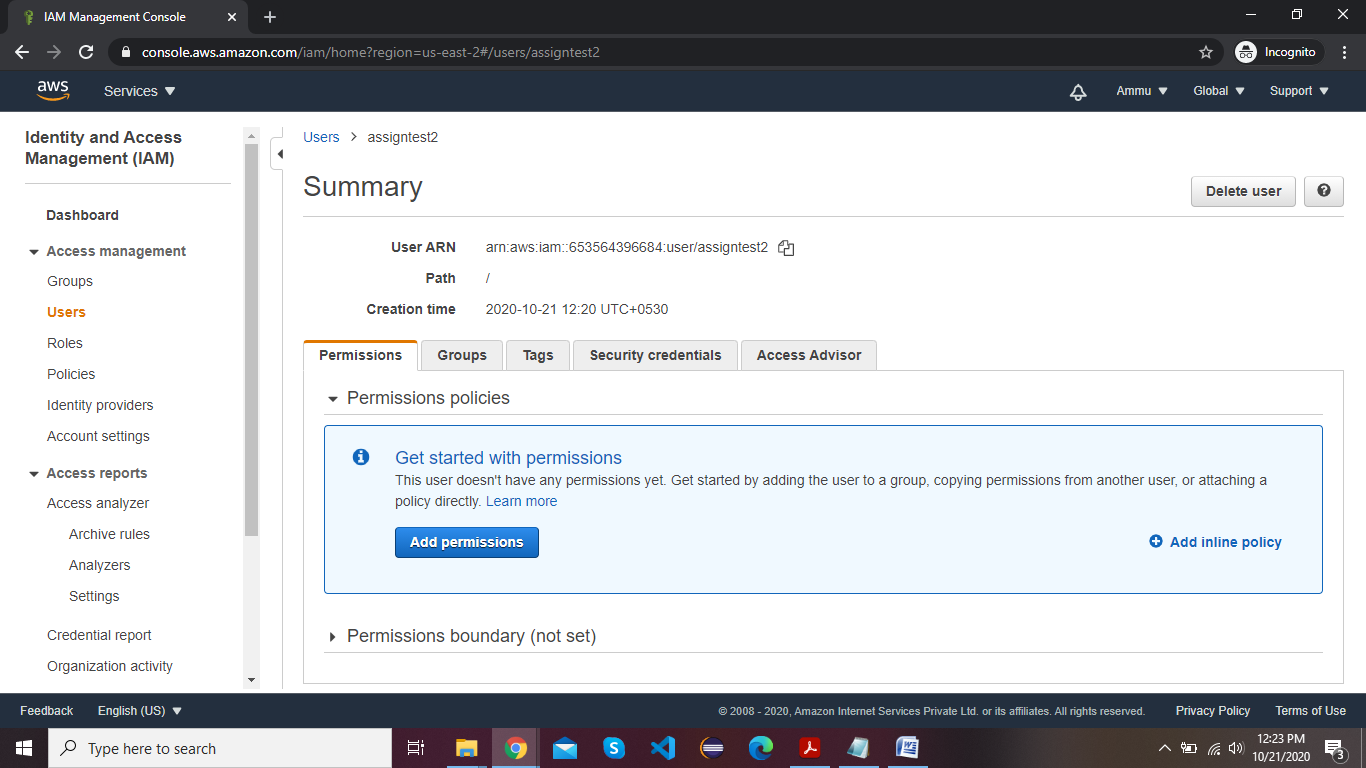


**Project 2 : IAM**

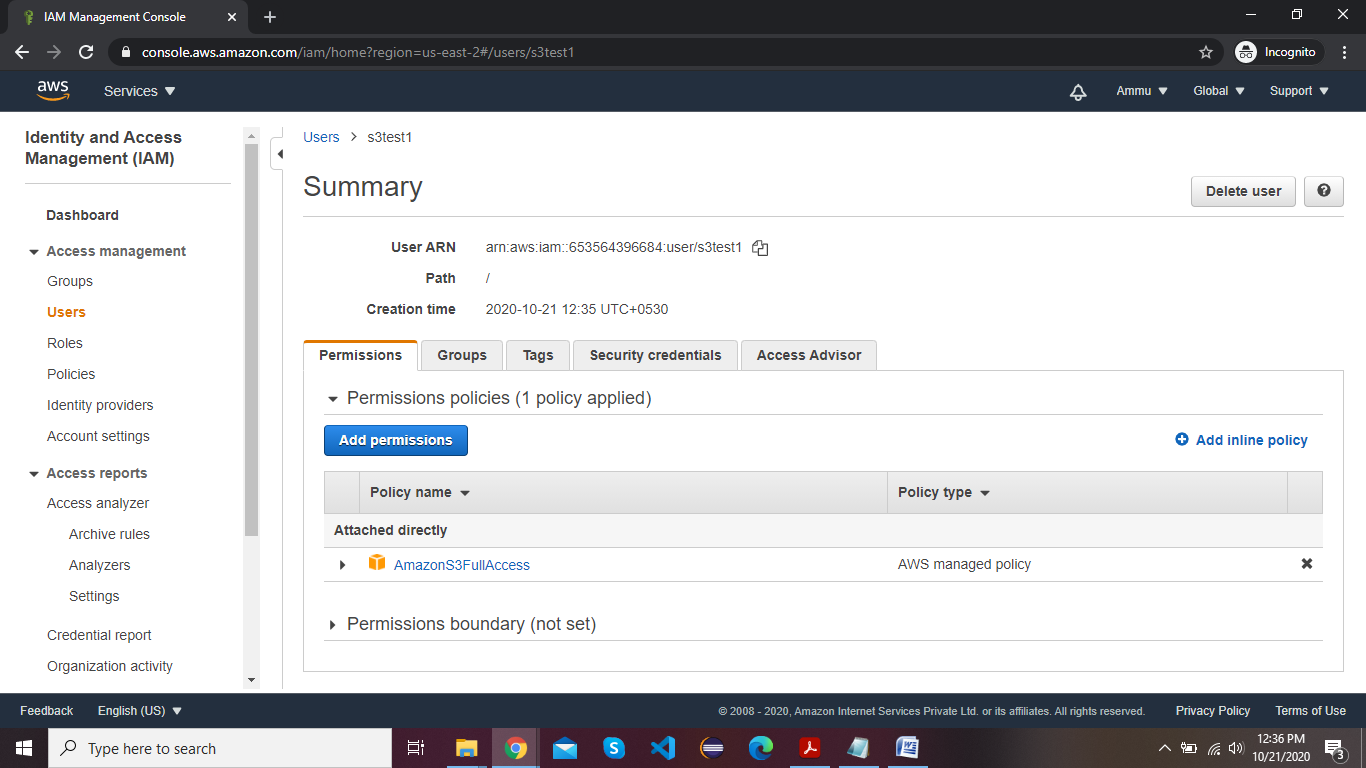
**Task 1:Creating users without permissions-IAM password policy check:**

****

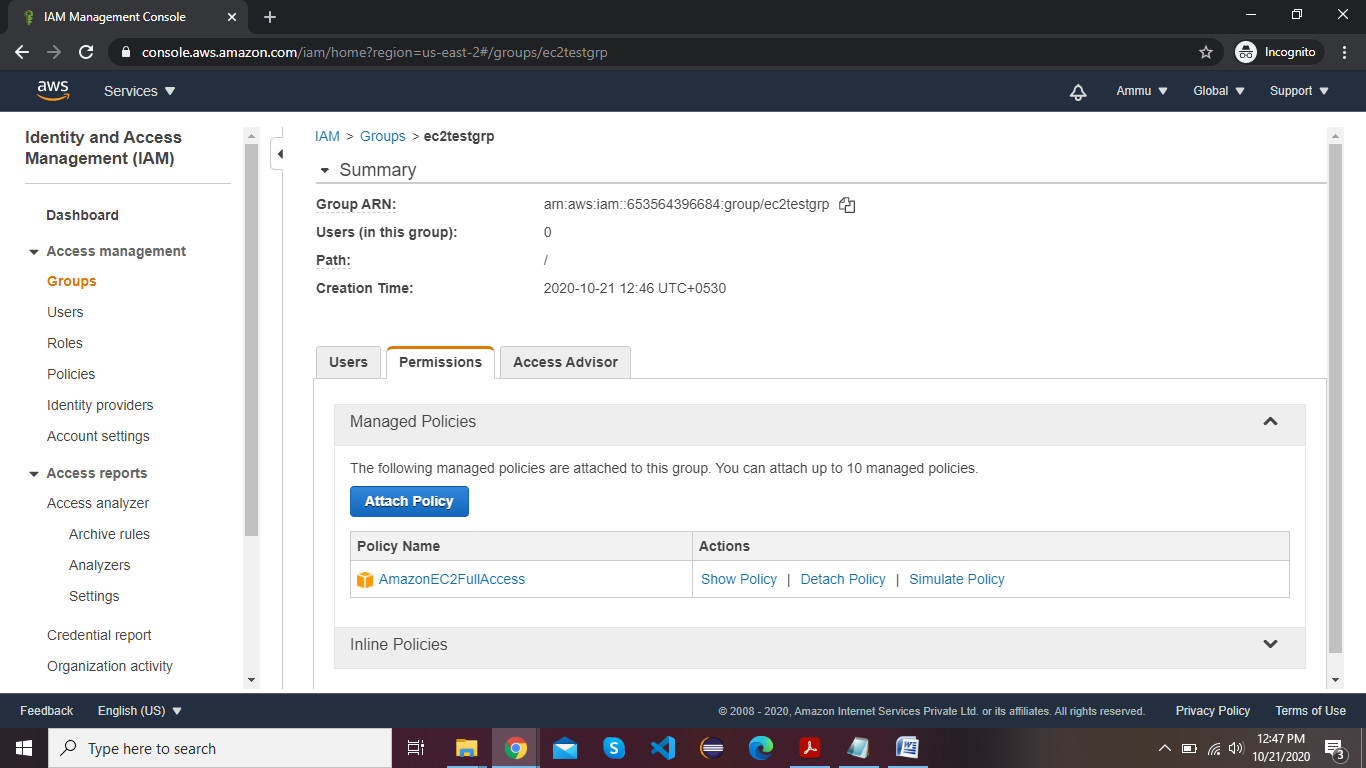
**Task 2:Creating users without the IAM password policy:**

****

**Task 3:Create a user with S3 full access:**

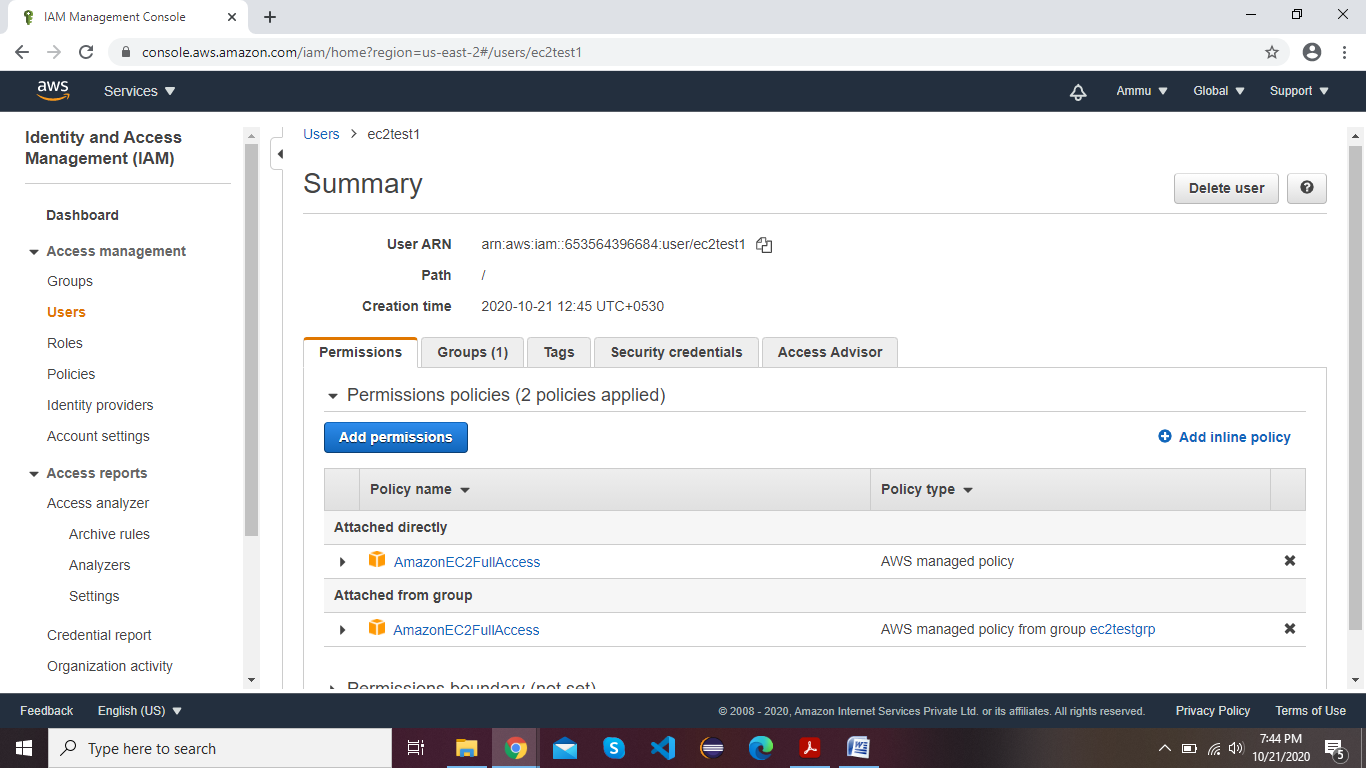
****

**Task4: Create a group with ec2 full access:**

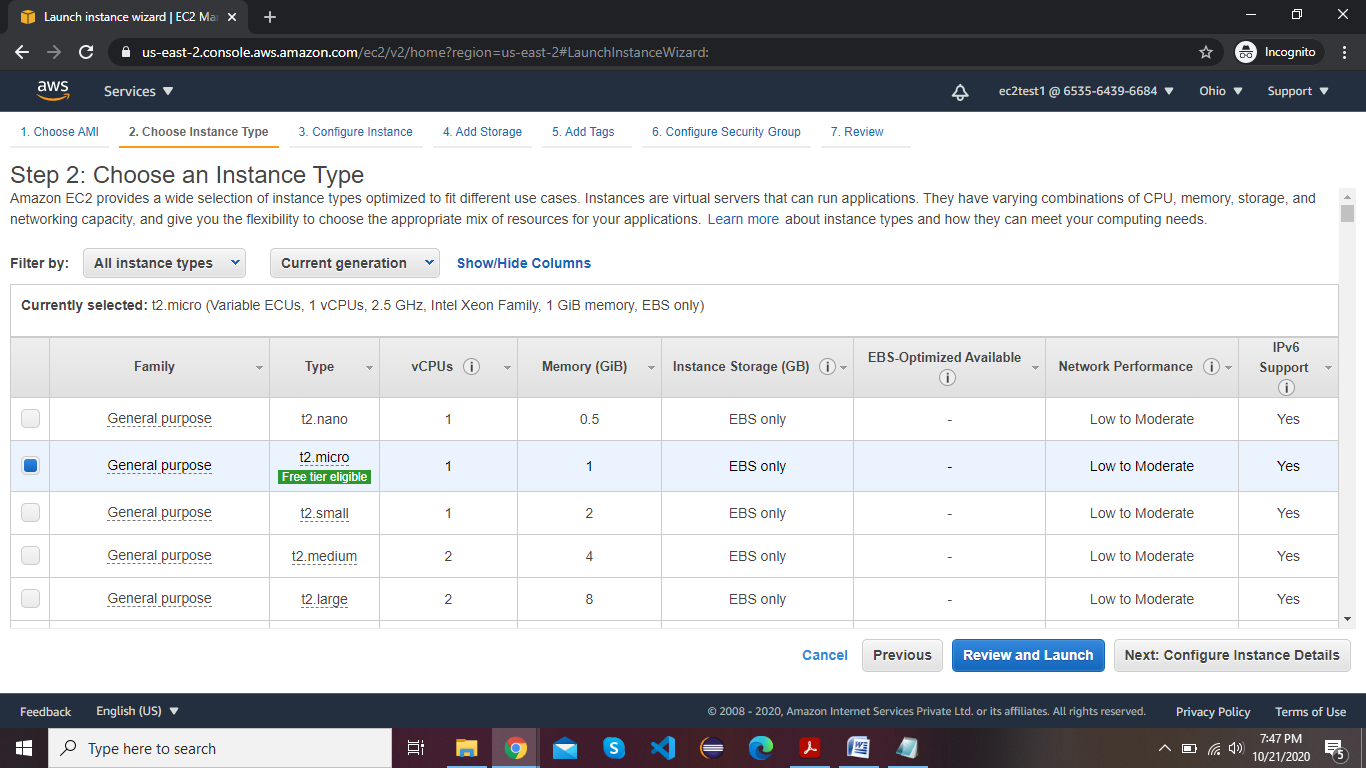
****

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

(a)User Summary with permission

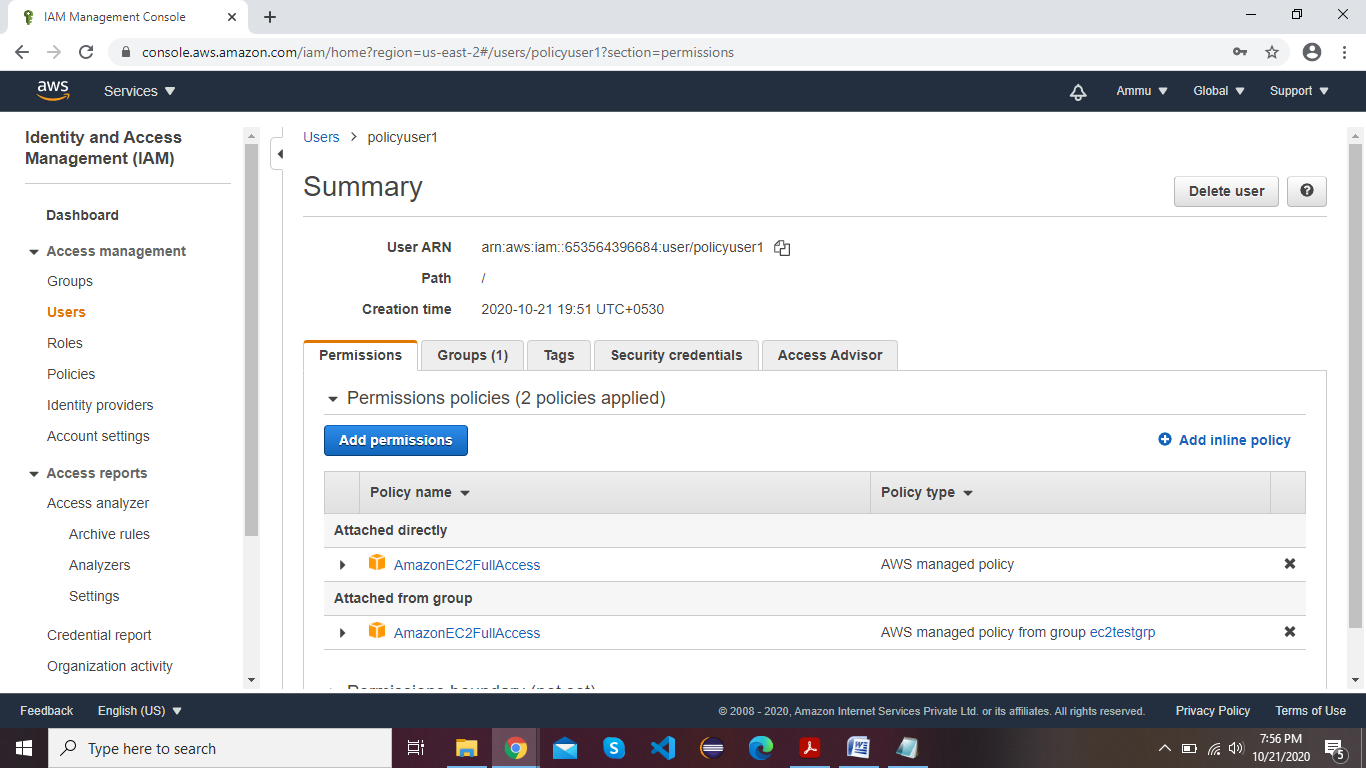


(b) login as the IAM user show that this policy is in effect

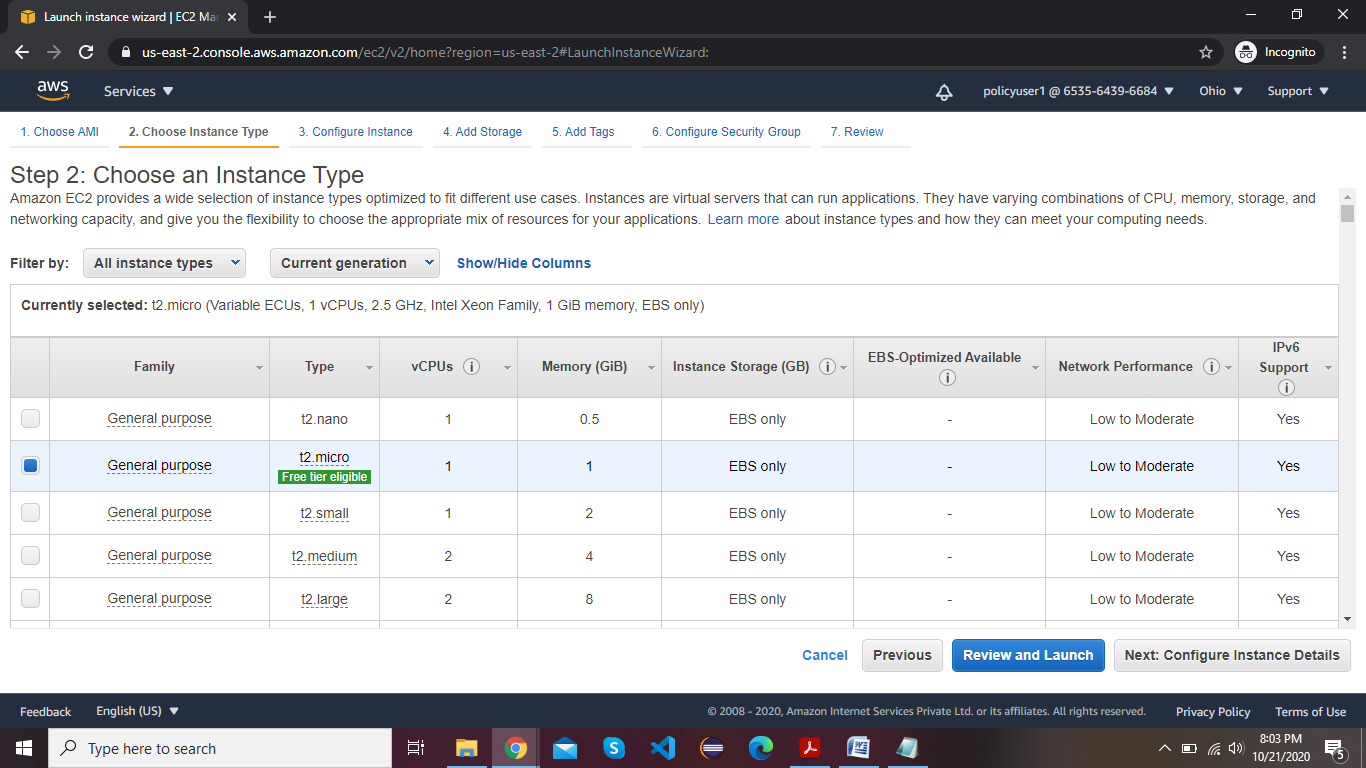


**Task 6:Copy policies from the existing user:**

1. attach user summary of the user from which you create a new user

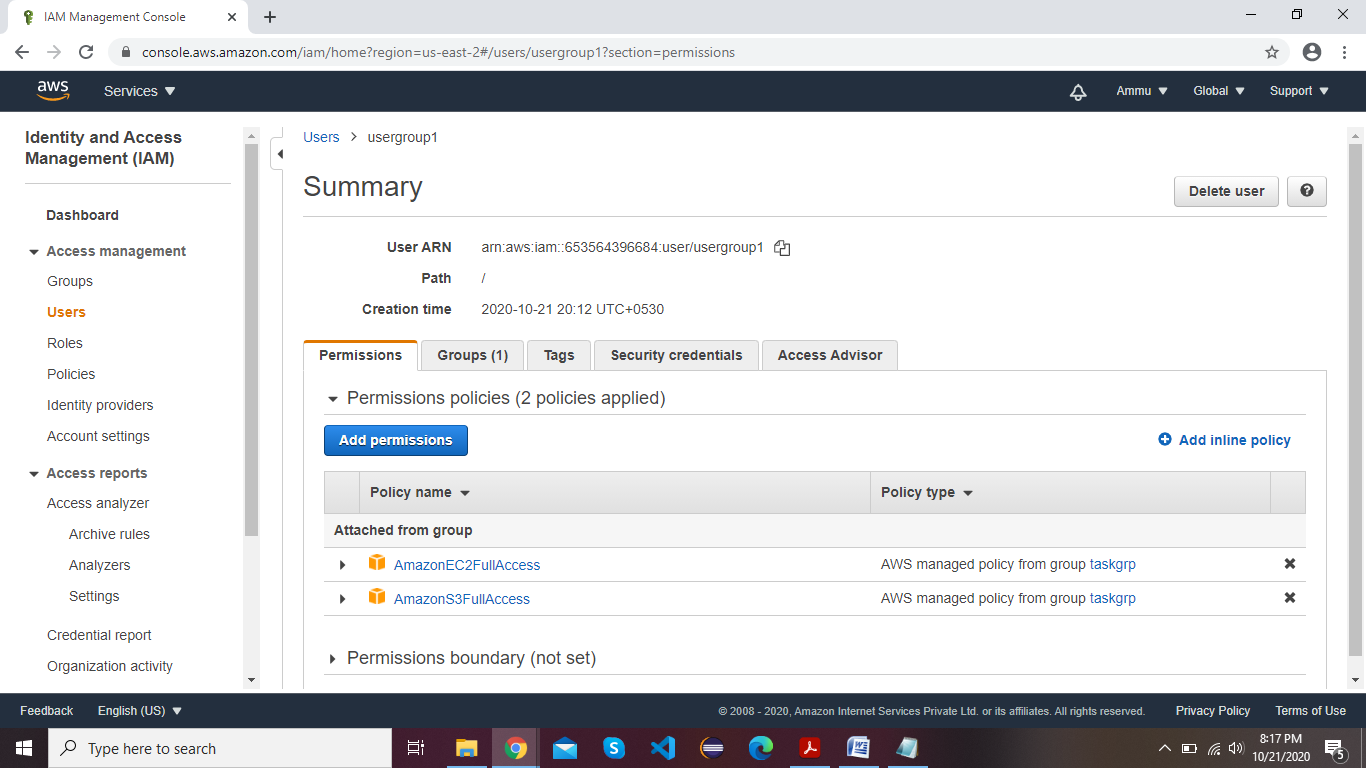
****

1. login as the IAM user show that this policy is in effect

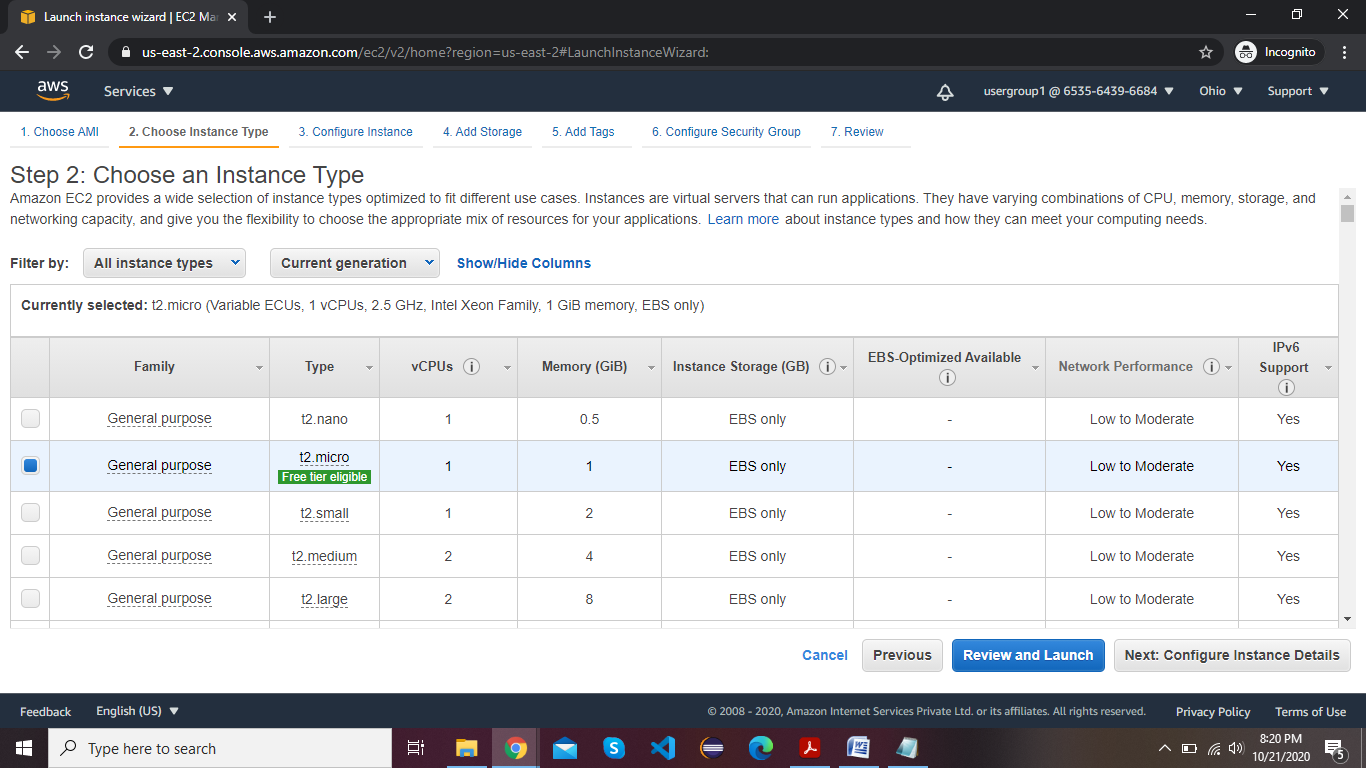
****

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

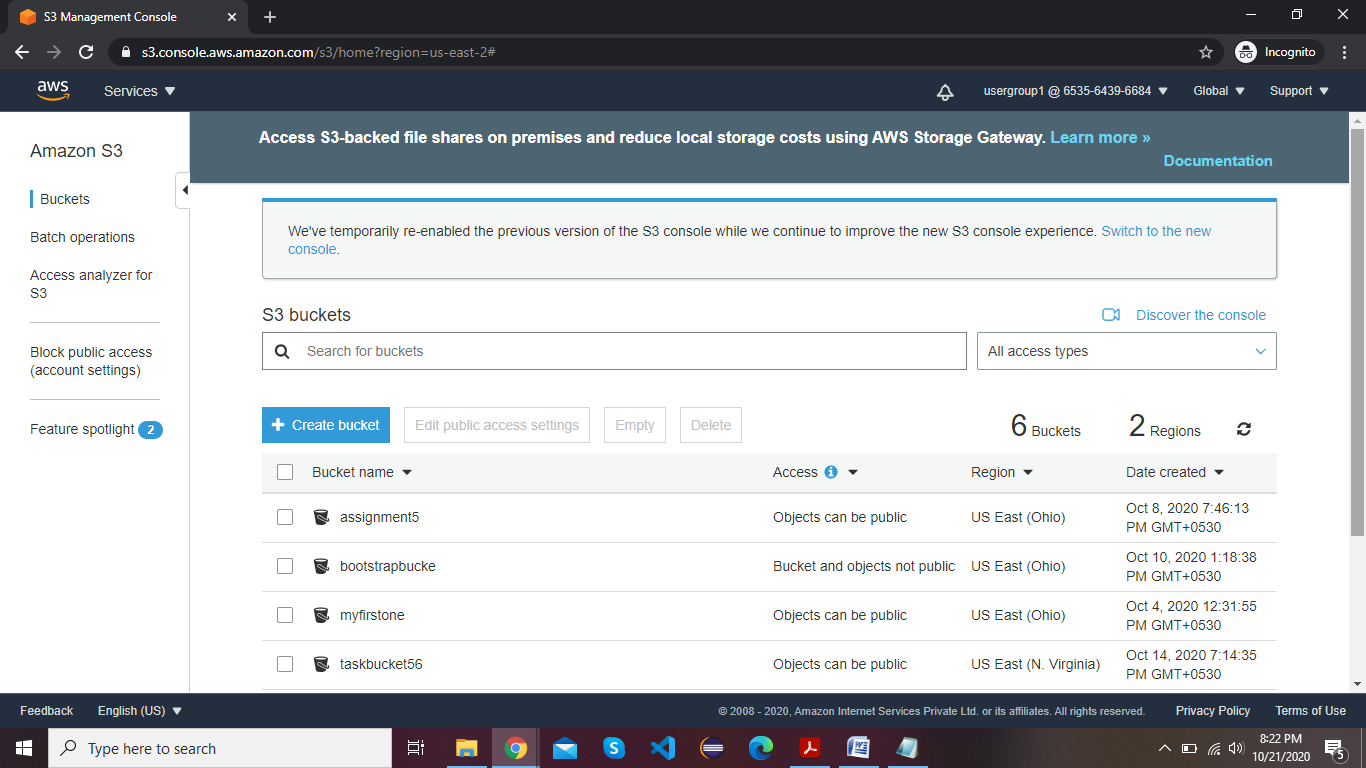
(a)Created group while creating user

****

(b)Reflecting policies for Created IAM User For ec2

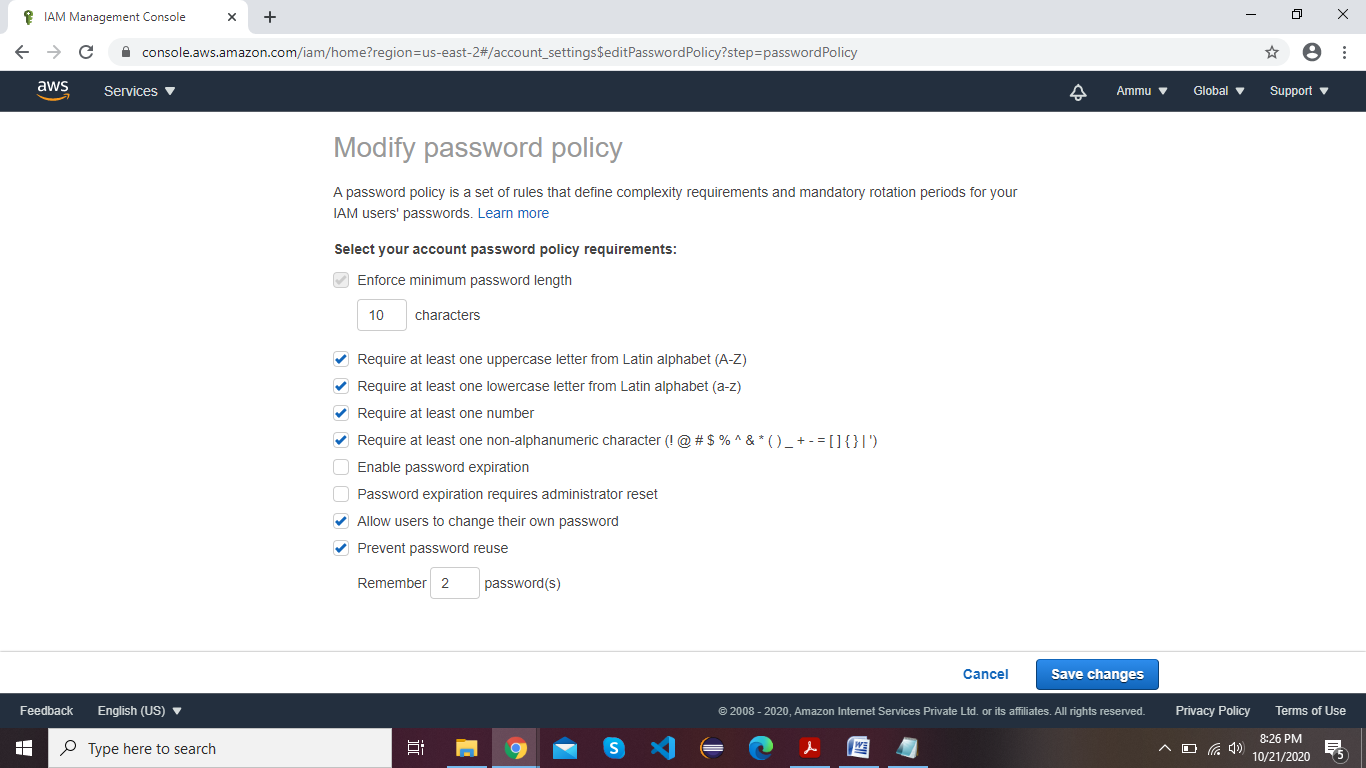


(c)Reflecting policies for Created IAM User For S3

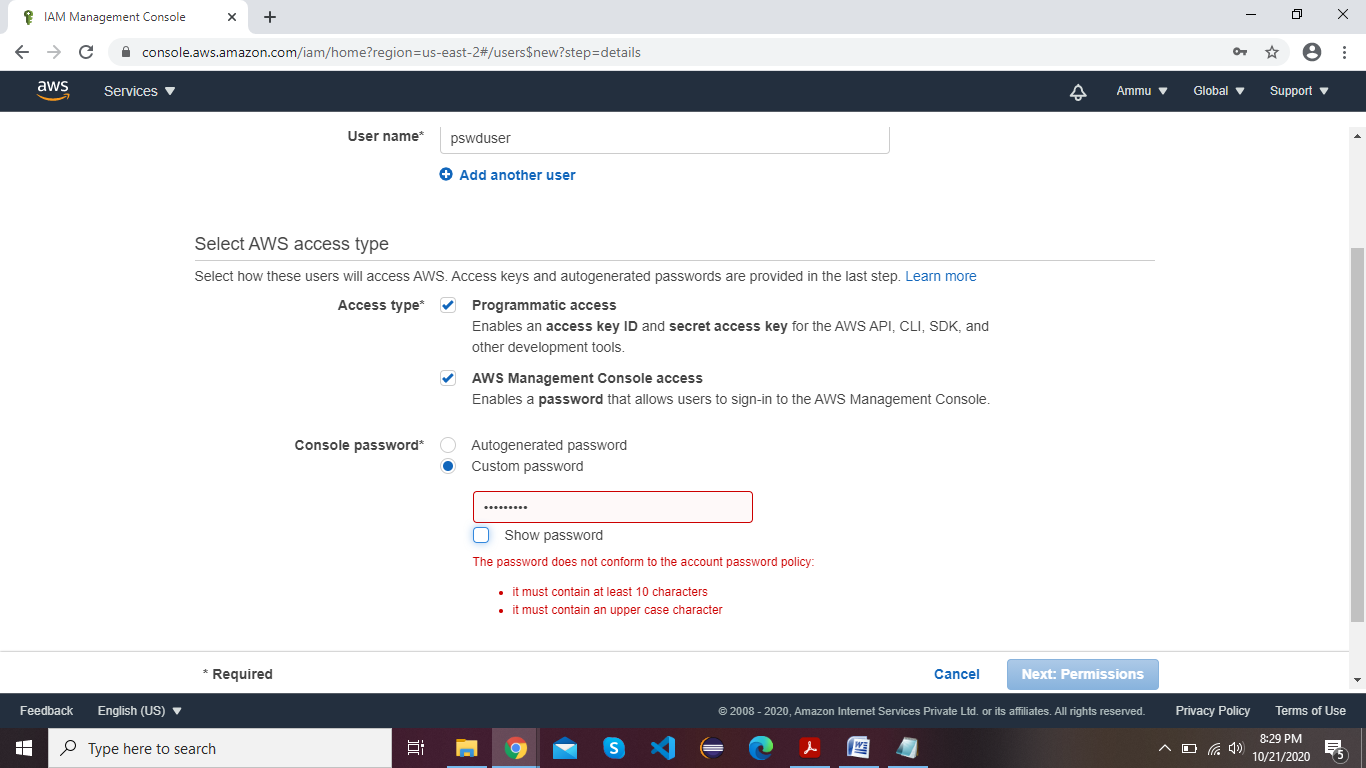


**Task8: setting a password policy:**

1. Password Policy Screen

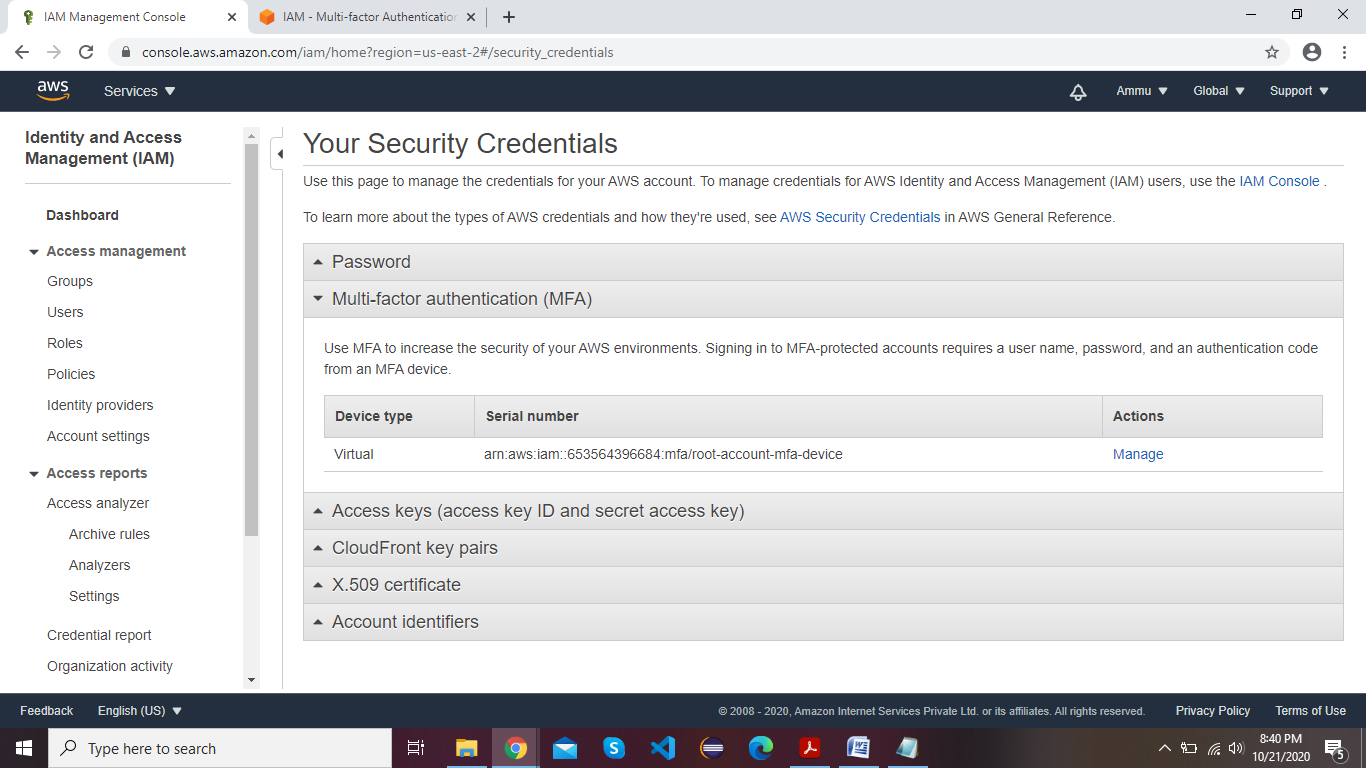


1. login as the user and show password incompatibility error

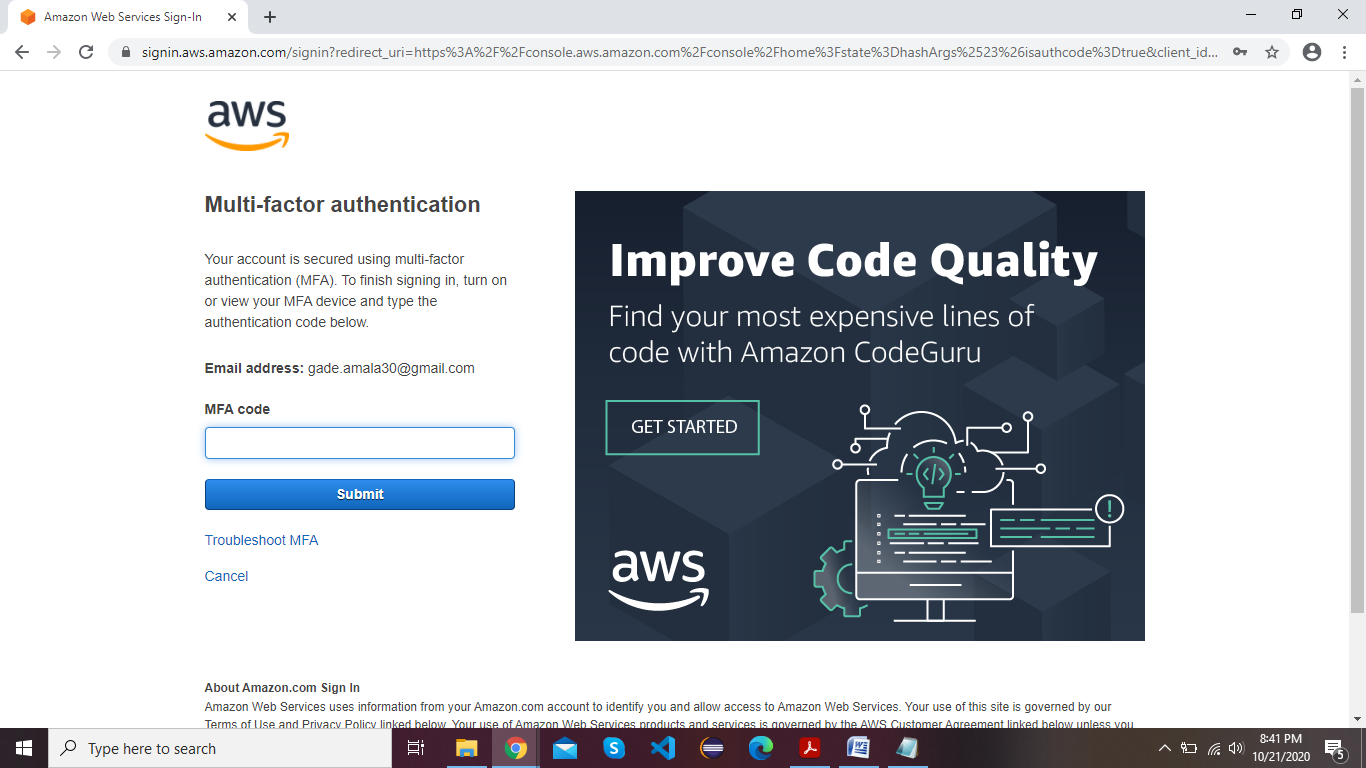
****

**Task 9:Enabling MFA and using an MFA device**

1. Enable MFA

****

**(b**)Login screen for MFA for root user

****