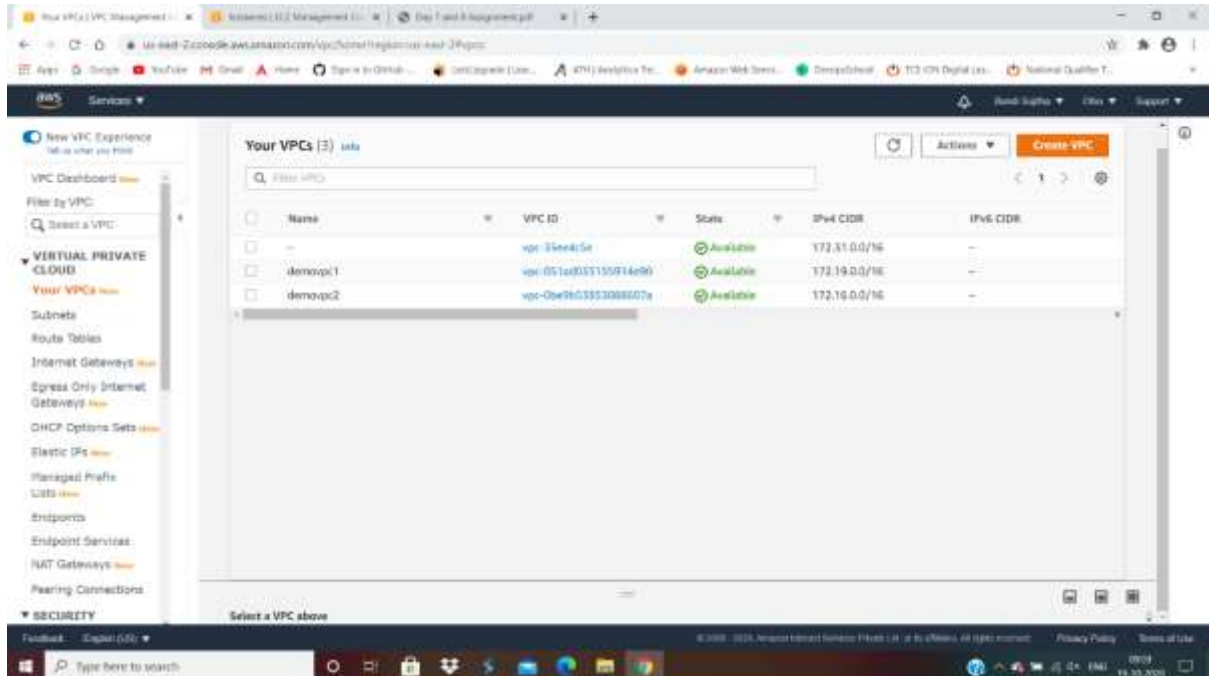


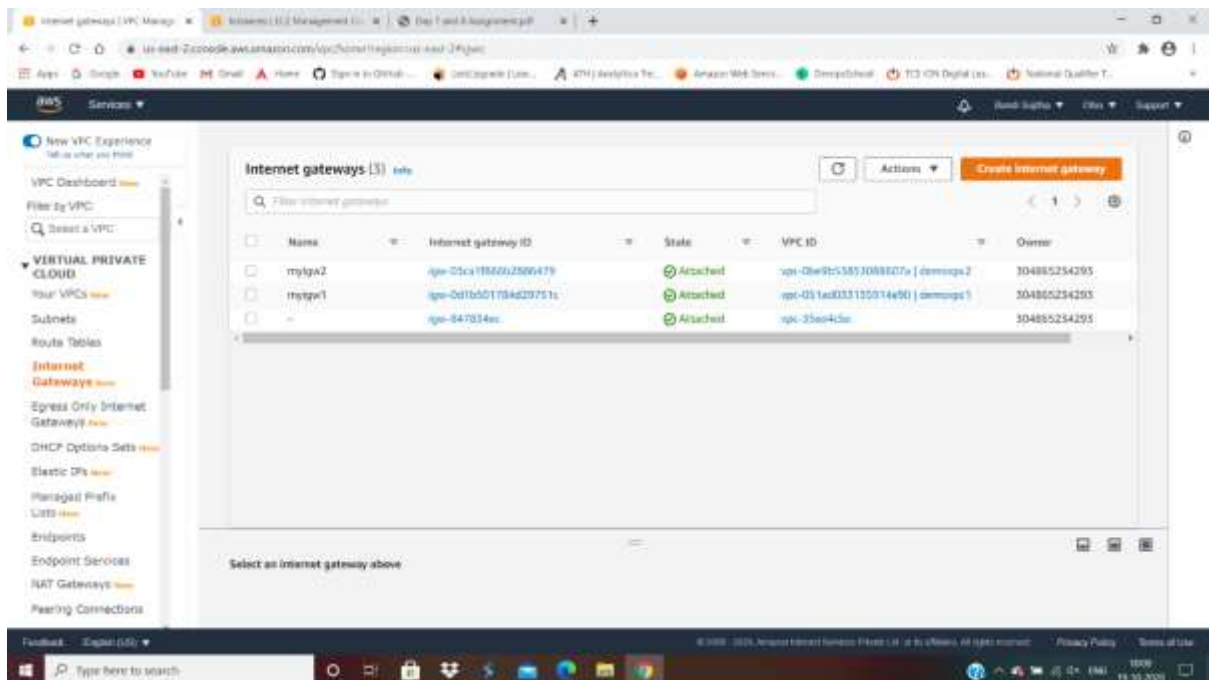
# Advance AWS Project

## Project 1: VPC peering

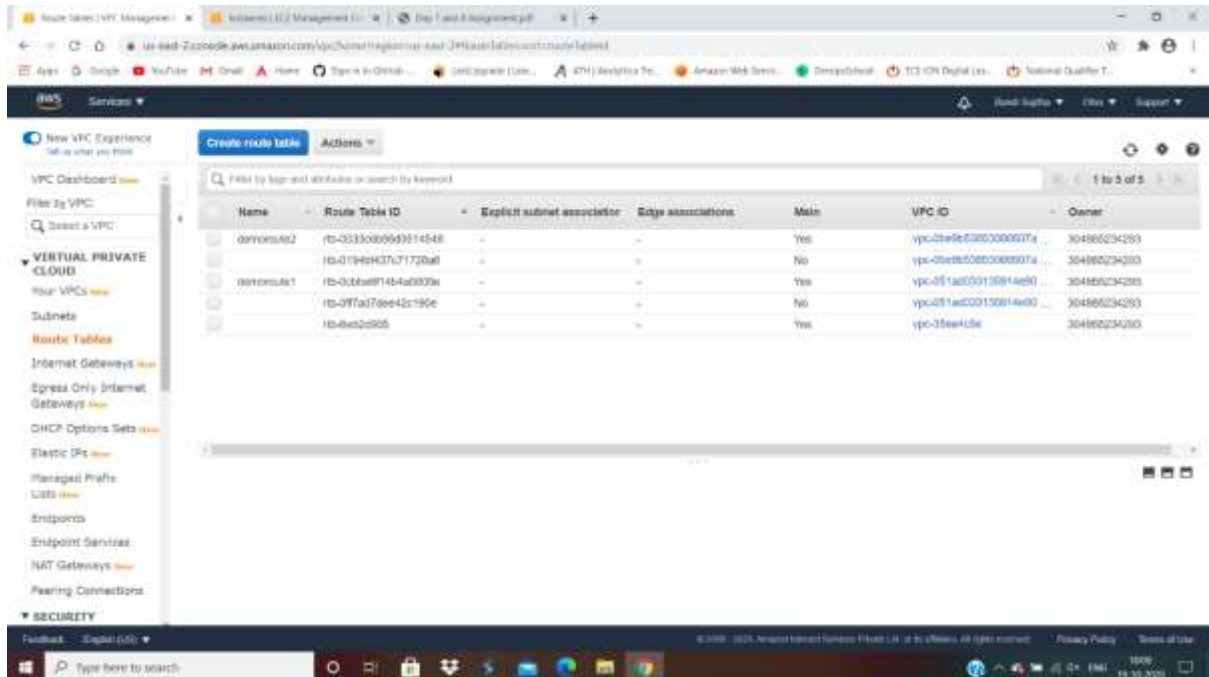
### SS1: VPCs list



### SS2: igw list

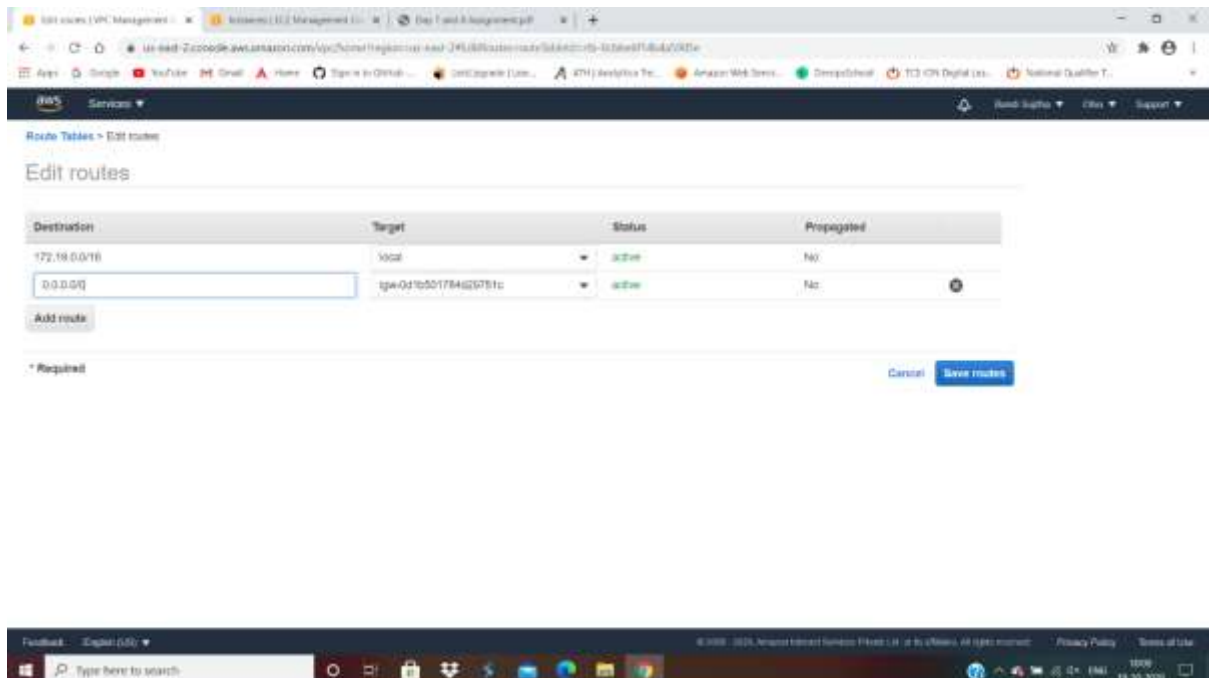


## SS3: edit route list



The screenshot shows the AWS Management Console interface for the 'Route Tables' section. The 'Create route table' button is highlighted in blue. Below the navigation pane, a table lists existing route tables. The table has the following columns: Name, Route Table ID, Explicit subnet association, Edge associations, Main, VPC ID, and Owner.

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
default-rt	rt-03330099d314548	--	--	Yes	vpc-0b9e0580000007a	304865234293
rt-01940437c71720a0	rt-01940437c71720a0	--	--	No	vpc-0b9e0580000007a	304865234293
default-rt	rt-03330099d314548	--	--	Yes	vpc-0b9e0580000007a	304865234293
rt-077a70ee43c195e	rt-077a70ee43c195e	--	--	No	vpc-0b9e0580000007a	304865234293
rt-0a0c0905	rt-0a0c0905	--	--	Yes	vpc-0b9e0580000007a	304865234293

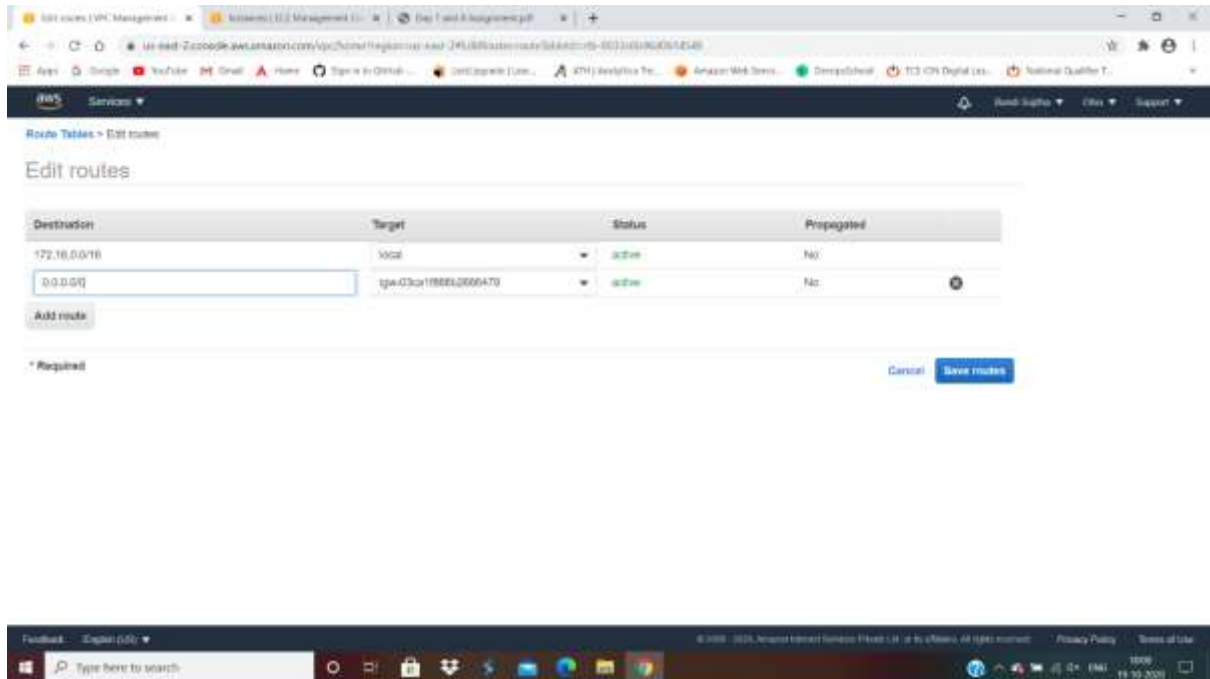


The screenshot shows the 'Edit routes' page in the AWS Management Console. The 'Destination' column shows '172.16.0.0/16' and '0.0.0.0/0'. The 'Target' column shows 'Vpc' and 'tgw-0d7b00178462751c'. The 'Status' column shows 'active' for both. The 'Propagated' column shows 'No' for both.

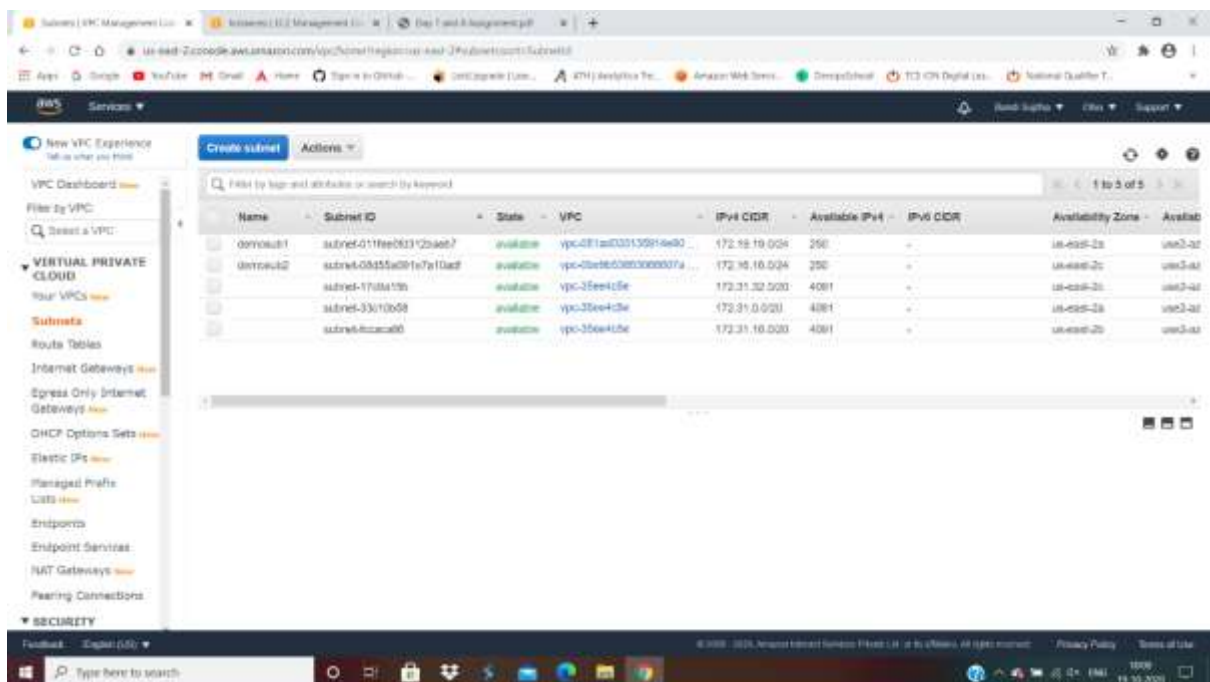
Destination	Target	Status	Propagated
172.16.0.0/16	Vpc	active	No
0.0.0.0/0	tgw-0d7b00178462751c	active	No

\* Required

Cancel Save routes



## SS4: subnet list



## SS5: instance details

The screenshot shows the AWS Management Console interface. The left sidebar contains navigation options like EC2 Dashboard, Events, Tags, Limits, INSTANCES, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, AMIs, ELASTIC BLOCK STORAGE, Volumes, Snapshots, Lifecycle Manager, and NETWORK & CONTENT DELIVERY. The main content area displays a table of EC2 instances. The first instance, 'demo1', is selected, and its details are shown below the table. The instance is of type 't2.micro' in the 'us-east-2a' availability zone, with a public IP of 3.137.188.166. The details panel includes tabs for Description, Status Checks, Monitoring, and Tags. The Description tab is active, showing fields like Instance ID, Instance State, Instance Type, Ending, Private DNS, Private IP, Secondary private IPs, VPC ID, Platform, and Platform details. The Status Checks tab shows two checks, both in a 'Passing' state. The Monitoring tab shows the instance is part of a 'default' monitoring group. The Tags tab shows a single tag with the key 'Name' and value 'demo1'.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6
demo1	i-0b8c2888b7f53528	t2.micro	us-east-2a	running	2/2 checks	None	3.137.188.166	3.137.188.166	-
demo2	i-0c019d2af77764bc	t2.micro	us-east-2c	running	2/2 checks	None	18.220.65.143	18.220.65.143	-

**Instance: i-0b8c2888b7f53528 (demo1) Public IP: 3.137.188.166**

**Description**

Field	Value
Instance ID	i-0b8c2888b7f53528
Instance State	running
Instance Type	t2.micro
Ending	Opt-in to AWS Compute Optimizer for recommendations. <a href="#">Learn more</a>
Private DNS	ip-172-16-18-26.us-east-2.compute.internal
Private IP	172.16.18.26
Secondary private IPs	-
VPC ID	vpc-01a83315914a8d (default)
Platform	Windows
Platform details	Windows

**Status Checks**

Check	Status
System Status	Passing
Instance Status	Passing

**Monitoring**

Monitoring Group	Monitoring
default	Monitoring

**Tags**

Key	Value
Name	demo1

The screenshot shows the AWS Management Console interface. The left sidebar contains navigation options like EC2 Dashboard, Events, Tags, Limits, INSTANCES, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, AMIs, ELASTIC BLOCK STORAGE, Volumes, Snapshots, Lifecycle Manager, and NETWORK & CONTENT DELIVERY. The main content area displays a table of EC2 instances. The second instance, 'demo2', is selected, and its details are shown below the table. The instance is of type 't2.micro' in the 'us-east-2c' availability zone, with a public IP of 18.220.65.143. The details panel includes tabs for Description, Status Checks, Monitoring, and Tags. The Description tab is active, showing fields like Instance ID, Instance State, Instance Type, Ending, Private DNS, Private IP, Secondary private IPs, VPC ID, Platform, and Platform details. The Status Checks tab shows two checks, both in a 'Passing' state. The Monitoring tab shows the instance is part of a 'default' monitoring group. The Tags tab shows a single tag with the key 'Name' and value 'demo2'.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6
demo1	i-0b8c2888b7f53528	t2.micro	us-east-2a	running	2/2 checks	None	3.137.188.166	3.137.188.166	-
demo2	i-0c019d2af77764bc	t2.micro	us-east-2c	running	2/2 checks	None	18.220.65.143	18.220.65.143	-

**Instance: i-0c019d2af77764bc (demo2) Public IP: 18.220.65.143**

**Description**

Field	Value
Instance ID	i-0c019d2af77764bc
Instance State	running
Instance Type	t2.micro
Ending	Opt-in to AWS Compute Optimizer for recommendations. <a href="#">Learn more</a>
Private DNS	ip-172-16-18-237.us-east-2.compute.internal
Private IP	172.16.18.237
Secondary private IPs	-
VPC ID	vpc-01a83315914a8d (default)
Platform	Windows
Platform details	Windows

**Status Checks**

Check	Status
System Status	Passing
Instance Status	Passing

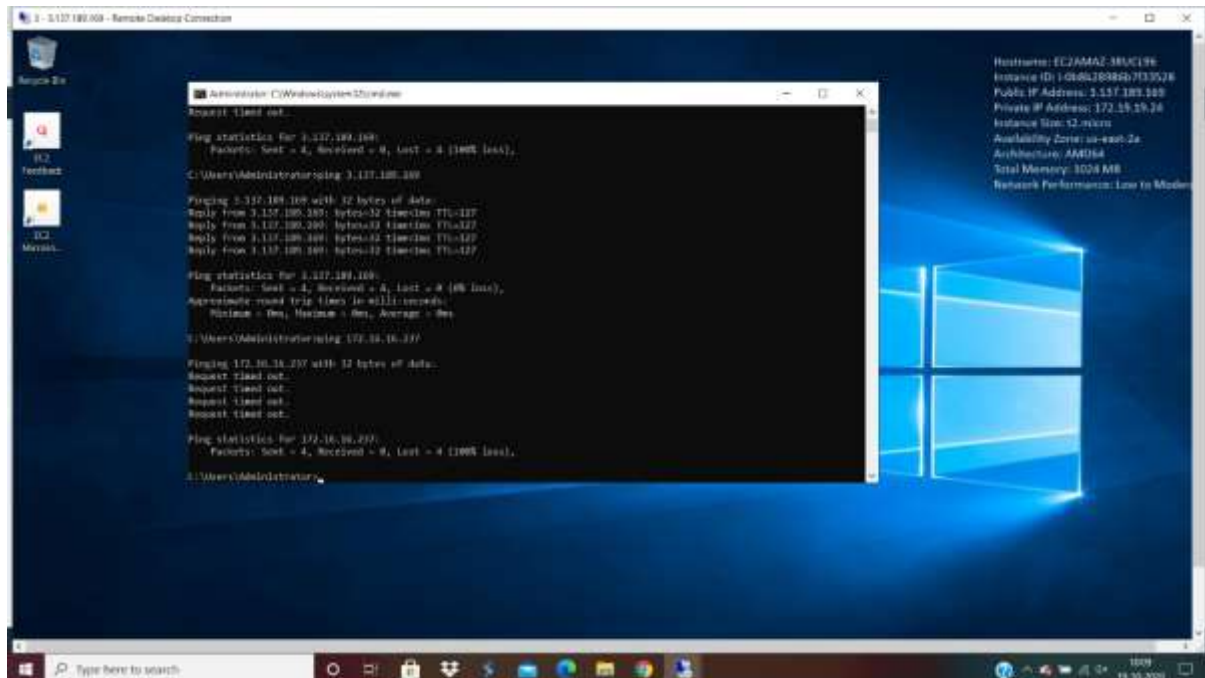
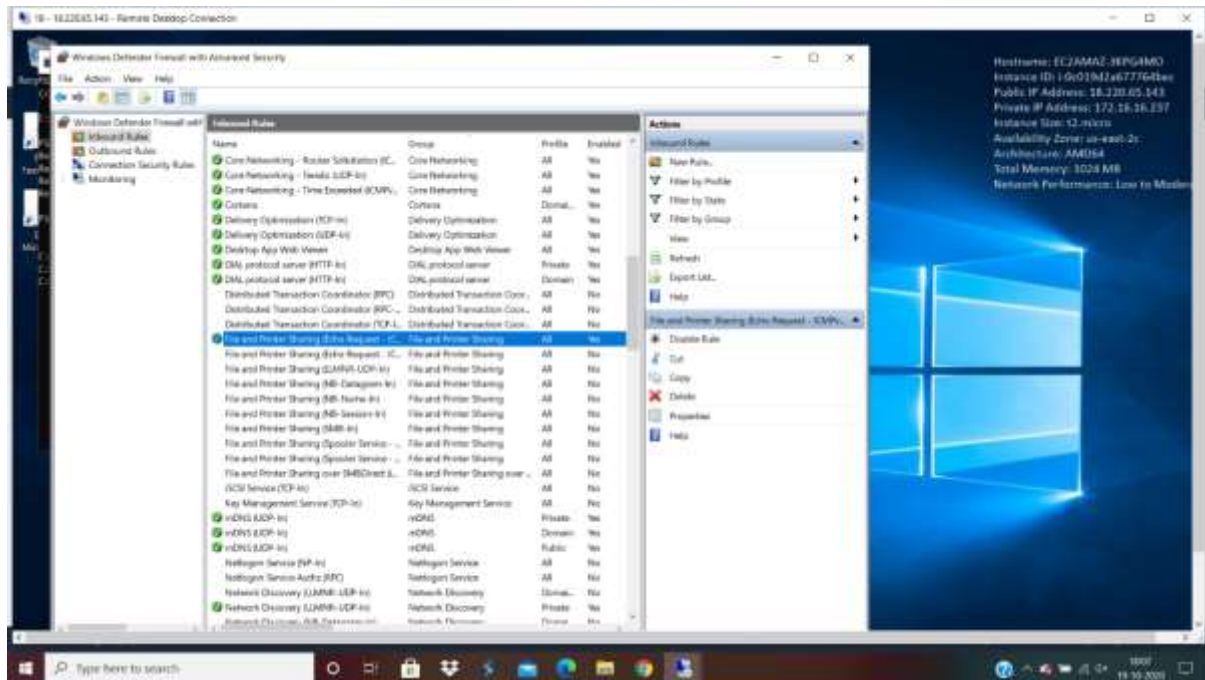
**Monitoring**

Monitoring Group	Monitoring
default	Monitoring

**Tags**

Key	Value
Name	demo2

SS6: success public, rto private IP





## SS7: peering with req and acceptor

**Create Peering Connection** | VPC | Subnets | VPC Management | VPC Peering Connections

Select a local VPC to peer with

VPC (Requester): vpc-081aa033135214e90

CIDR	Status	Status Reason
172.16.0.0/16	associated	

Select another VPC to peer with

Account: ☒ My account ☐ Another account

Region: ☒ This region (us-east-2) ☐ Another Region

VPC (Accepter): vpc-0ba0b5335305802fa

CIDR	Status	Status Reason
172.16.0.0/16	associated	

Feedback | English (US)

© 2020 Amazon Web Services. All rights reserved. Privacy Policy | Terms of Use

**Edit routes**

Destination	Target	Status	Propagated
172.16.0.0/16	vpc	active	No
0.0.0.0/0	igw-0d1b501784625781c	active	No
172.16.0.0/16	pcr-065ea42a019a07c2d	active	No

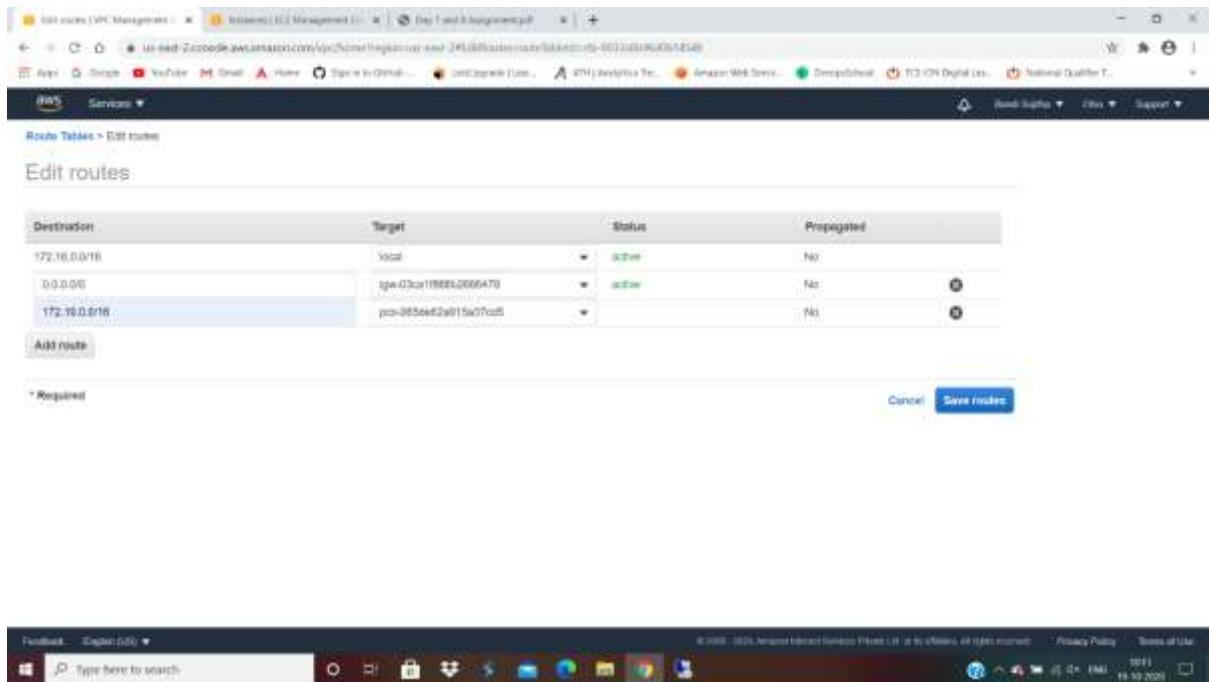
[Add route](#)

\* Required

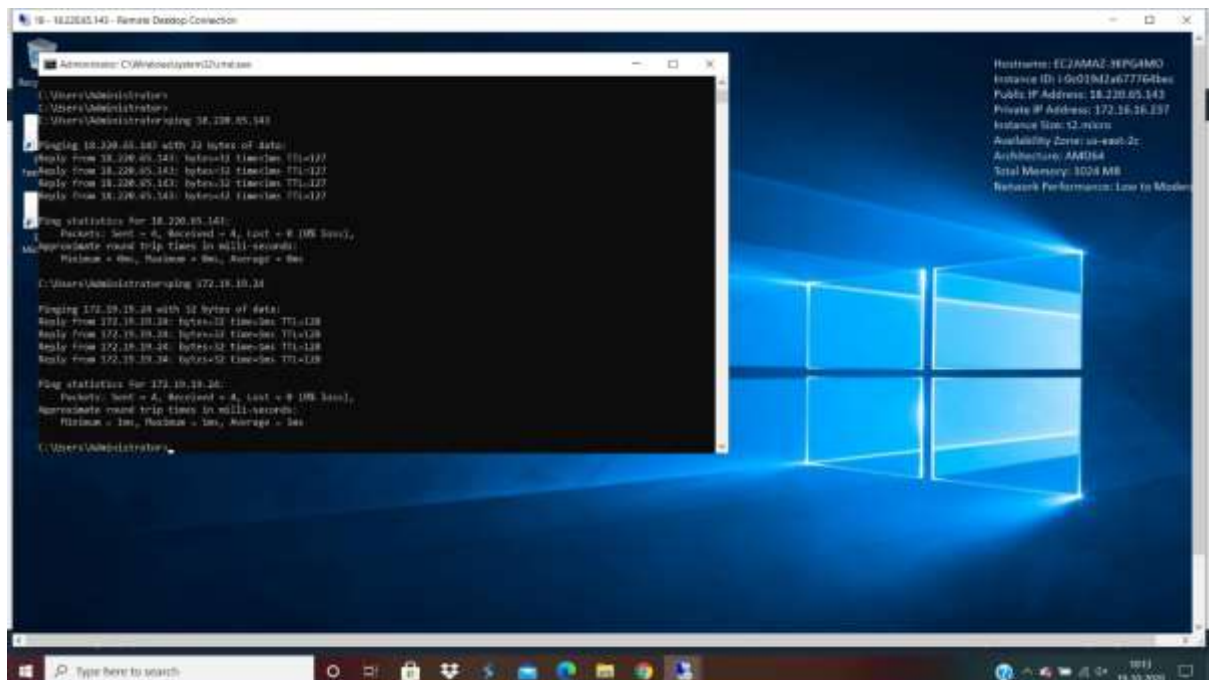
[Cancel](#) [Save routes](#)

Feedback | English (US)

© 2020 Amazon Web Services. All rights reserved. Privacy Policy | Terms of Use

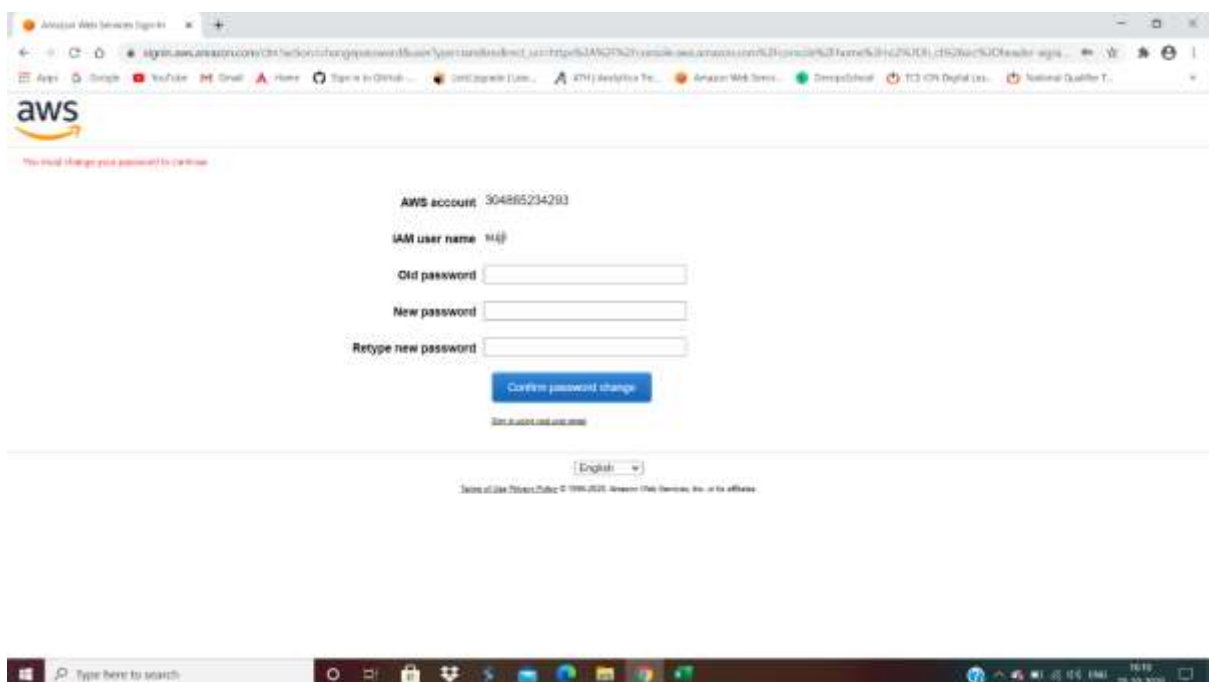
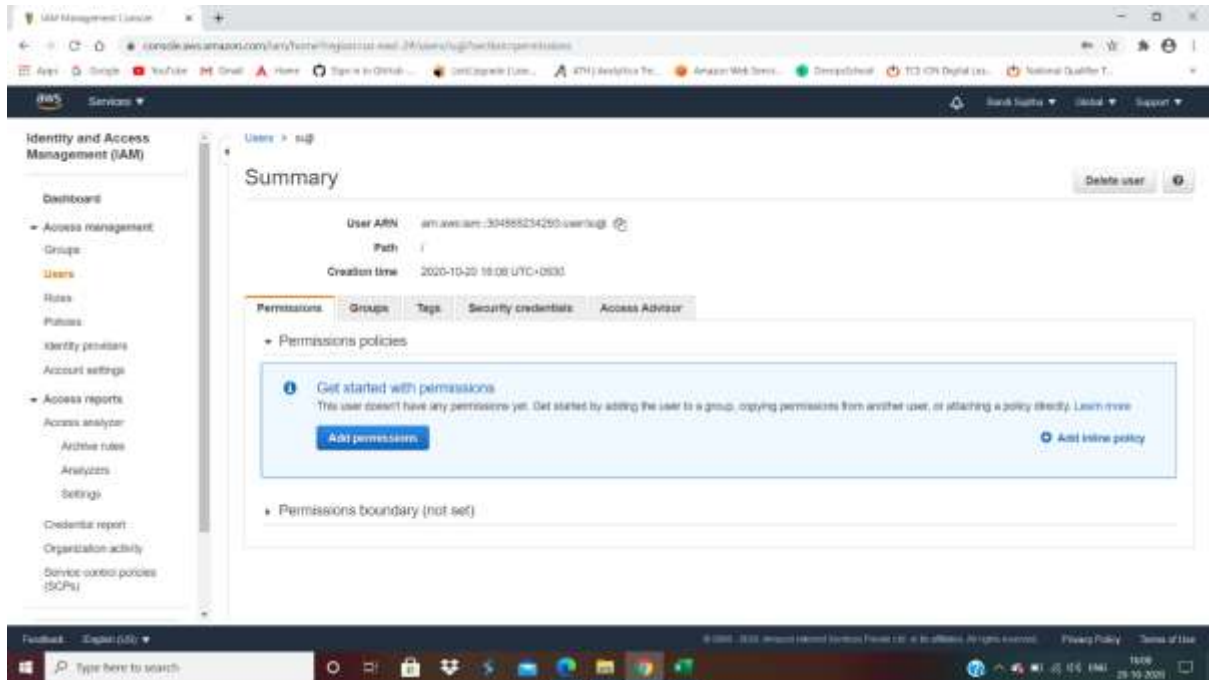


SS8: success for private



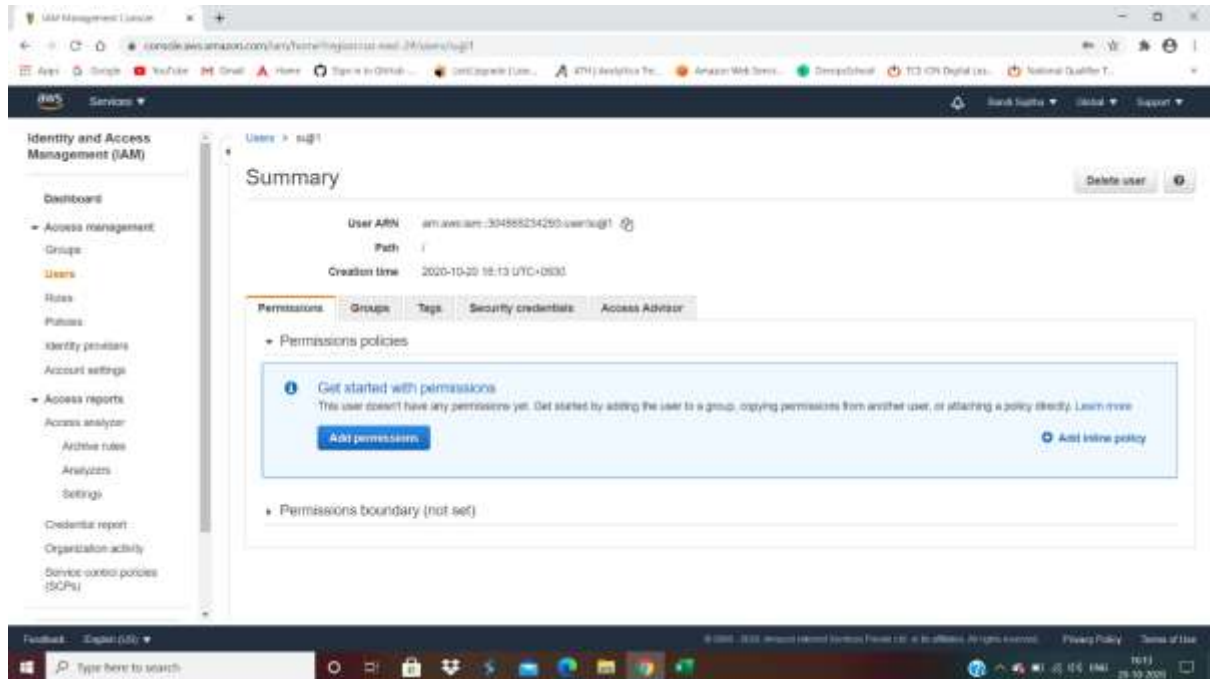
## Project 2: IAM

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

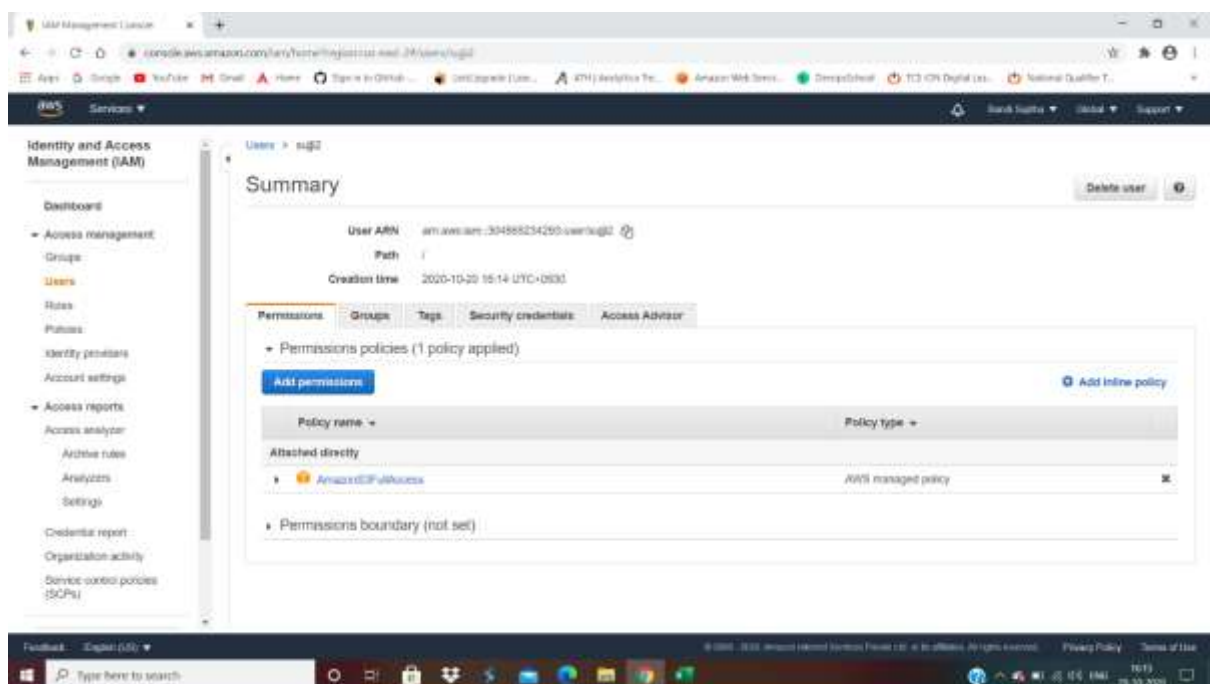




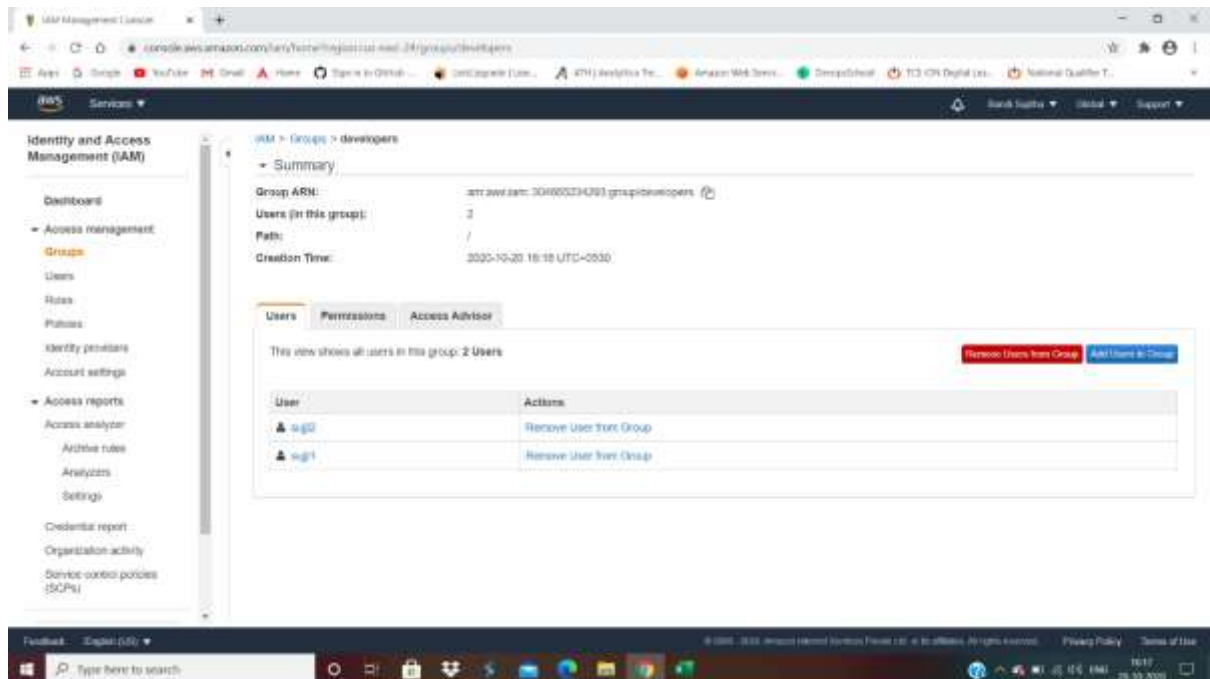
## Task 2: Creating users without the IAM password policy.



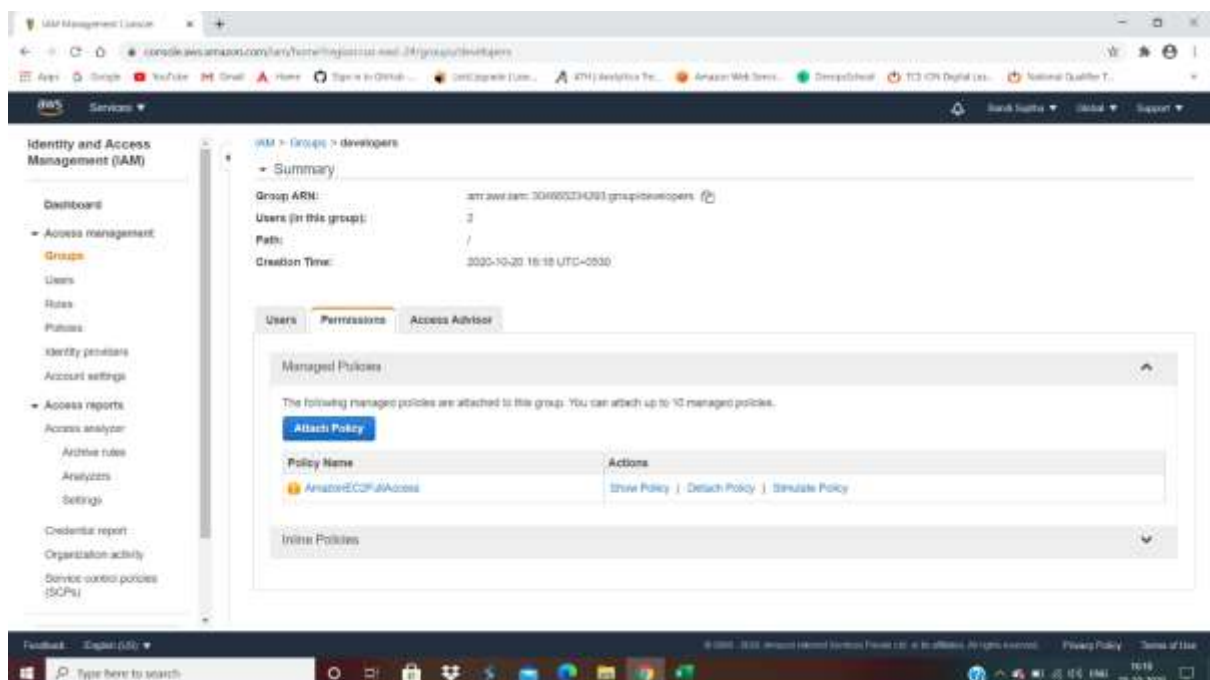
## Task 3: Create a user with S3 full access

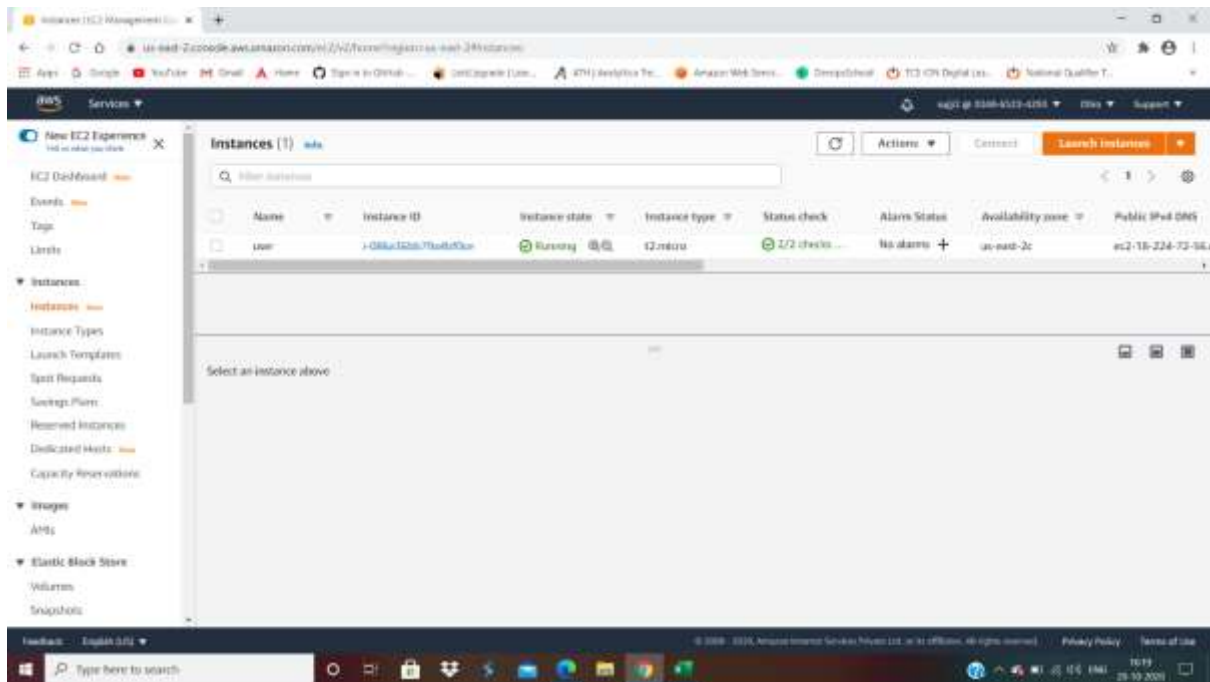


## Task4: Create a group with ec2 full access

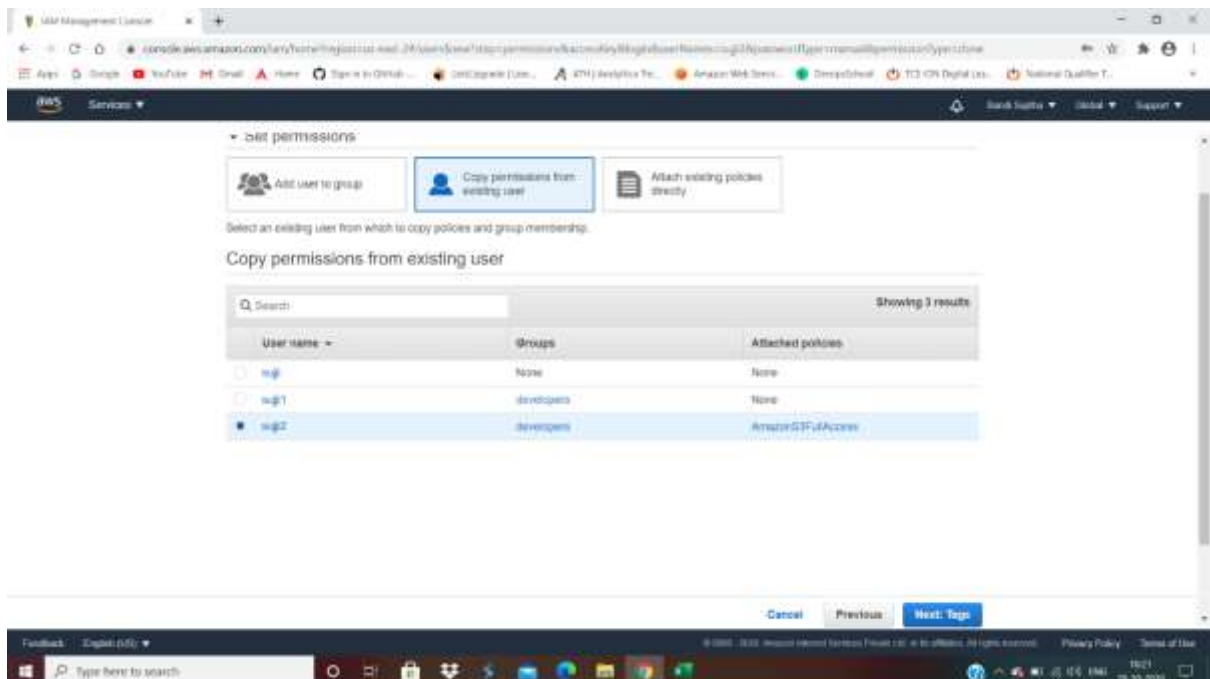


## Task 5: Add user to a group and check if user policy and the group policy is reflecting on the user





## Task 6: Copy policies from the existing user



Identity and Access Management (IAM)

Users > su@3

### Summary

[Delete user](#)

User ARN: [arn:aws:iam::304568234290:user:su@3](#)  
Path: /  
Creation time: 2020-10-20 18:21 UTC+0800

Permissions Groups (1) Tags Security credentials Access Advisor

Permissions policies (2 policies applied)

[Add permissions](#) [Add inline policy](#)

Policy name	Policy type
Attached directly	
<a href="#">AmazonEC2FullAccess</a>	AWS managed policy
Attached from group	
<a href="#">Show 1 more</a>	

Permissions boundary (not set)

Feedback Expand (55)

© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

19:03 29.10.2020

Identity and Access Management (IAM)

Users > su@3

### Summary

[Delete user](#)

User ARN: [arn:aws:iam::304568234290:user:su@3](#)  
Path: /  
Creation time: 2020-10-20 18:21 UTC+0800

Permissions Groups (1) Tags Security credentials Access Advisor

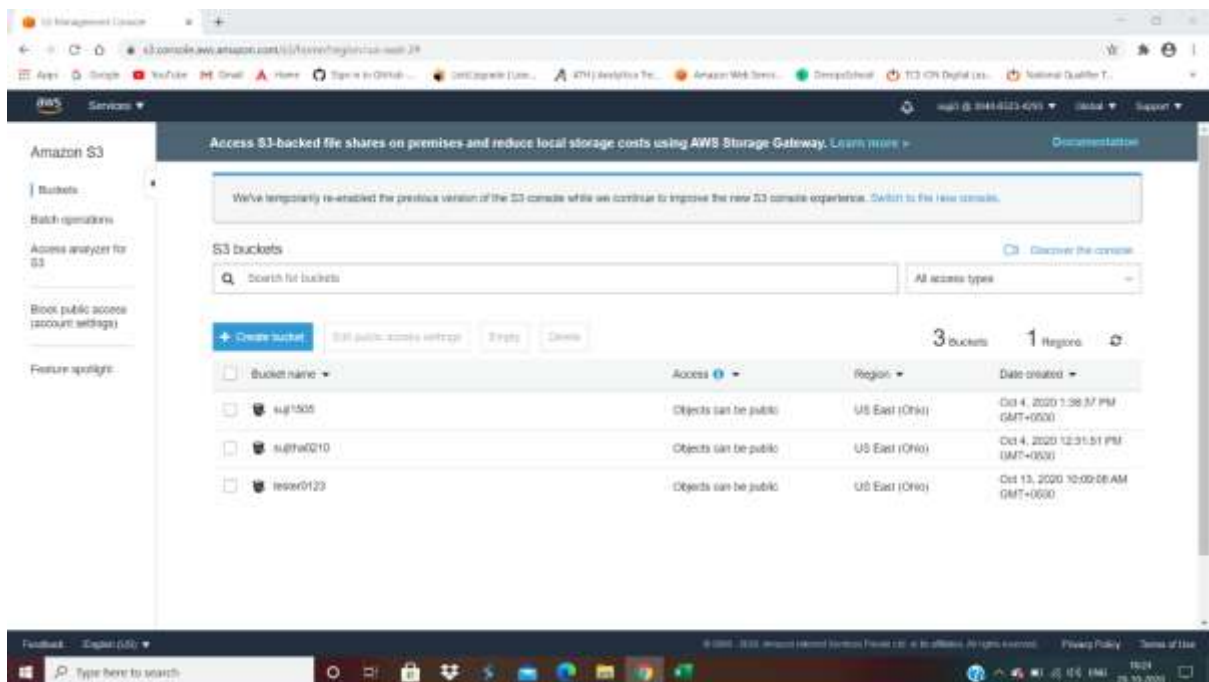
[Add user to groups](#)

Group name	Attached permissions
<a href="#">developers</a>	<a href="#">AmazonEC2FullAccess</a>

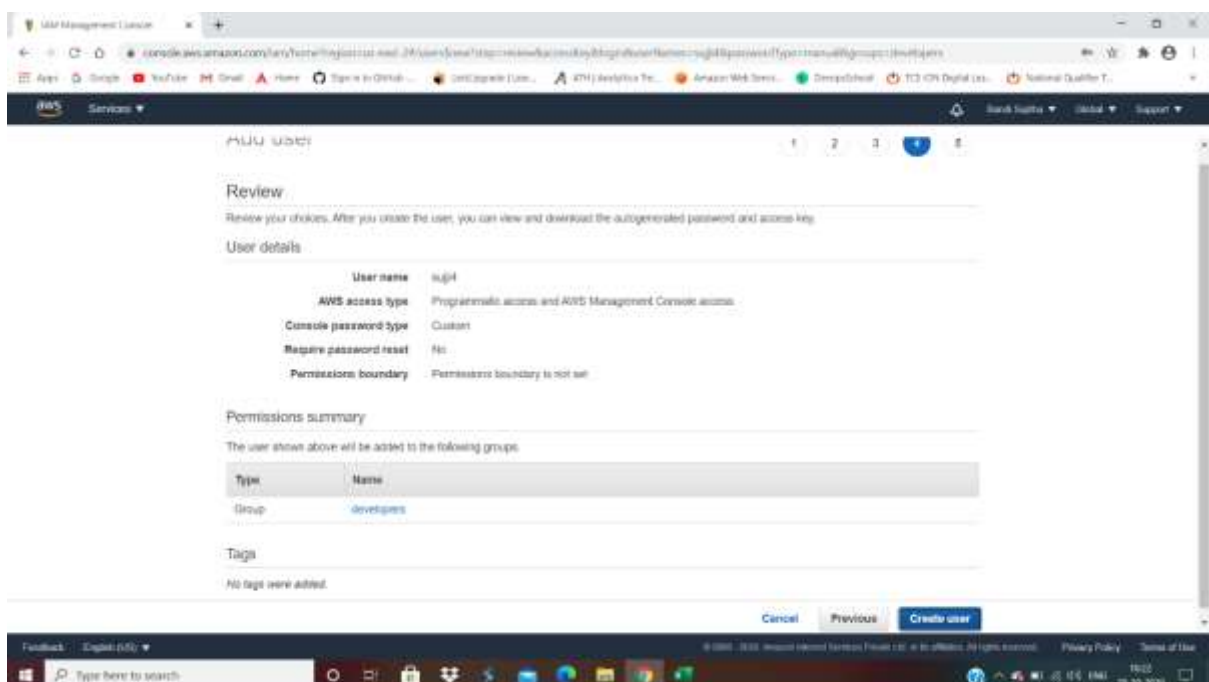
Feedback Expand (55)

© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

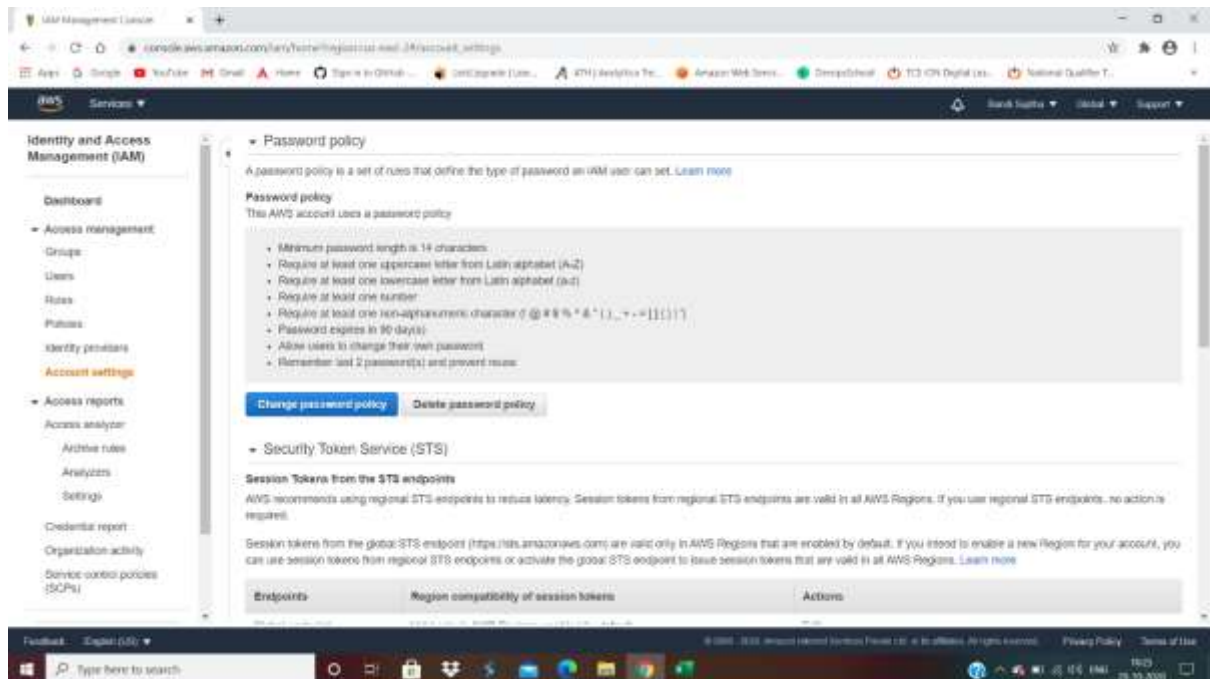
19:03 29.10.2020



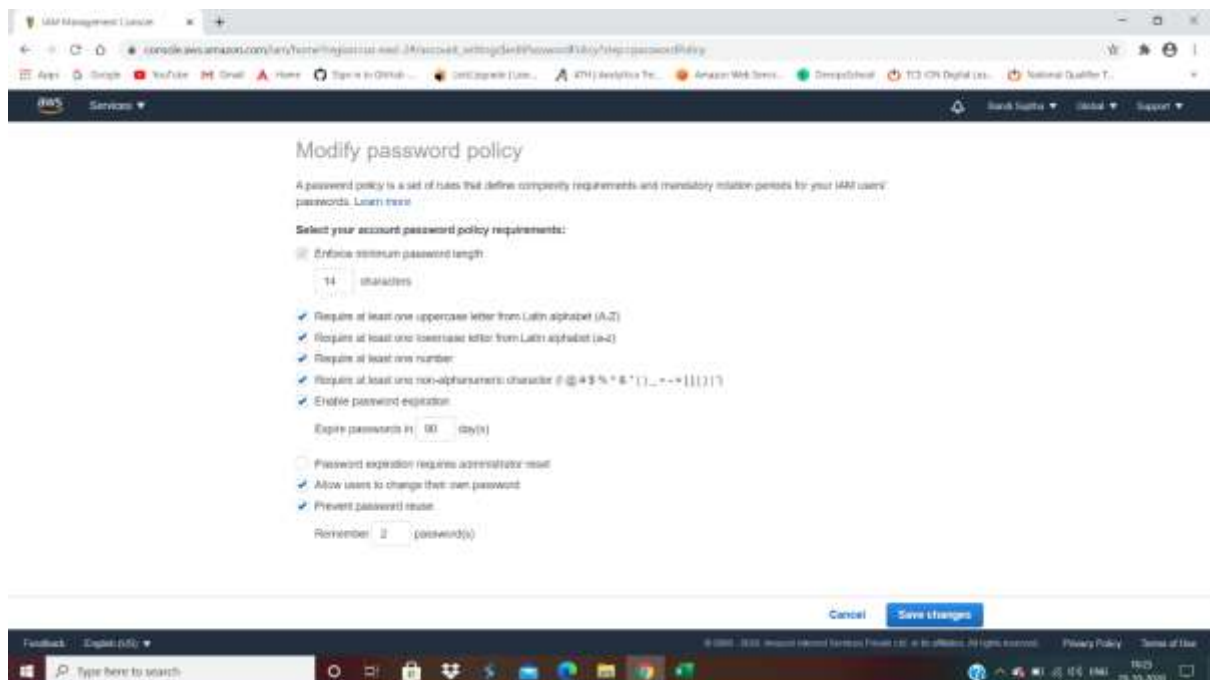
Task 7: Add user to a group in the process of creating a user



## Task8: setting a password policy



The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible with options like Dashboard, Access management, Groups, Users, Roles, Policies, Identity providers, Account settings (highlighted), Access reports, Access analyzer, Artifact rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled 'Password policy'. It explains that a password policy is a set of rules defining password types and includes a list of requirements for the AWS account's policy: Minimum password length is 14 characters, Require at least one uppercase letter from Latin alphabet (A-Z), Require at least one lowercase letter from Latin alphabet (a-z), Require at least one number, Require at least one non-alphanumeric character (characters: !@#\$%^&\*()\_+~`{|}[]), Password expires in 90 day(s), Allow users to change their own password, and Remember last 2 password(s) and prevent reuse. Below this list are buttons for 'Change password policy' and 'Delete password policy'. The 'Security Token Service (STS)' section follows, discussing session tokens from regional and global endpoints. At the bottom, there are tabs for 'Endpoints', 'Region compatibility of session tokens', and 'Actions'.



The screenshot shows the 'Modify password policy' page in the AWS IAM console. The title is 'Modify password policy'. Below the title, it states: 'A password policy is a set of rules that define complexity requirements and mandatory rotation periods for your IAM users' passwords. Learn more'. The 'Select your account password policy requirements:' section contains several options: 'Enforce minimum password length' (checked) with a value of '14' characters; 'Require at least one uppercase letter from Latin alphabet (A-Z)' (checked); 'Require at least one lowercase letter from Latin alphabet (a-z)' (checked); 'Require at least one number' (checked); 'Require at least one non-alphanumeric character (characters: !@#\$%^&\*()\_+~`{|}[])' (checked); 'Enable password expiration' (checked) with a value of '90' day(s); 'Password expiration requires administrator reset' (unchecked); 'Allow users to change their own password' (checked); 'Prevent password reuse' (checked) with a value of '2' password(s). At the bottom, there are 'Cancel' and 'Save changes' buttons.



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

