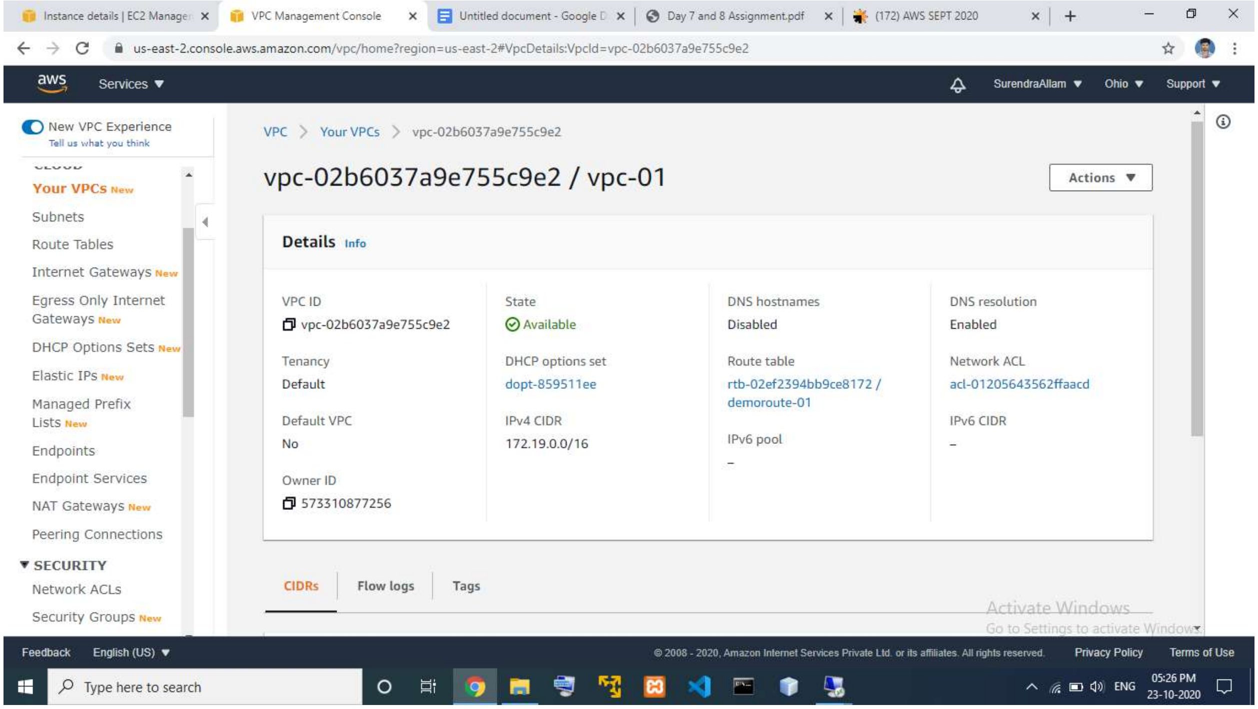
Advance AWS | Assignment Day 7 and 8

PROJECT 1:

VPC peering

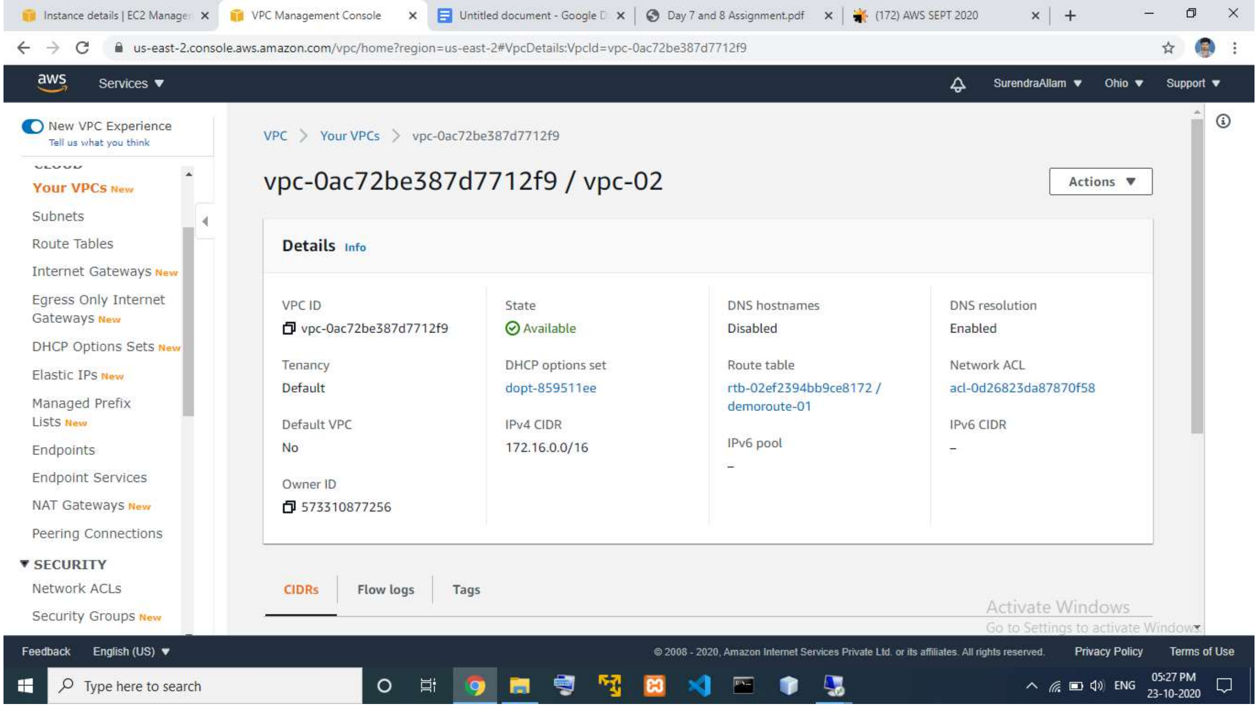
Ss1: VPCs list



vpc-02b6037a9e755c9e2 / vpc-01

Details Info

VPC ID: vpc-02b6037a9e755c9e2
State: Available
DNS hostnames: Disabled
DNS resolution: Enabled
Tenancy: Default
DHCP options set: dopt-859511ee
Route table: rtb-02ef2394bb9ce8172 / demoroute-01
Network ACL: acl-01205643562ffaacd
Default VPC: No
IPv4 CIDR: 172.19.0.0/16
IPv6 pool: –
IPv6 CIDR: –
Owner ID: 573310877256

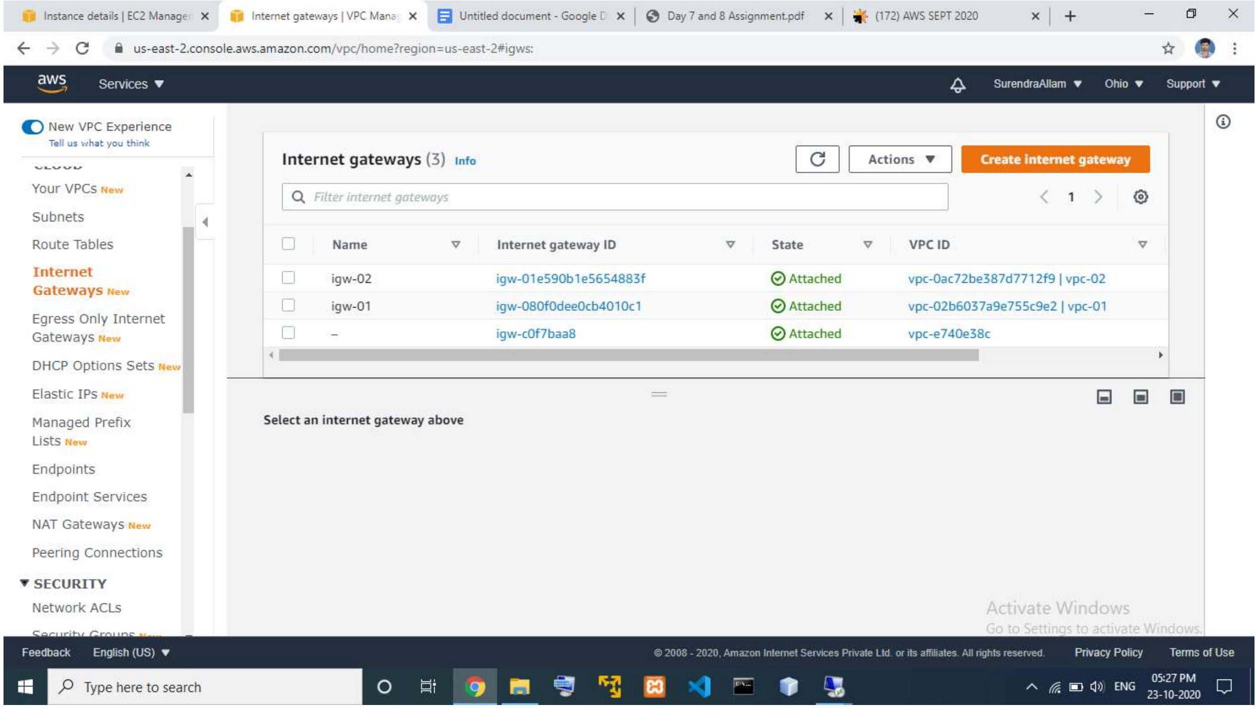


vpc-0ac72be387d7712f9 / vpc-02

Details Info

VPC ID: vpc-0ac72be387d7712f9
State: Available
DNS hostnames: Disabled
DNS resolution: Enabled
Tenancy: Default
DHCP options set: dopt-859511ee
Route table: rtb-02ef2394bb9ce8172 / demoroute-01
Network ACL: acl-0d26823da87870f58
Default VPC: No
IPv4 CIDR: 172.16.0.0/16
IPv6 pool: –
IPv6 CIDR: –
Owner ID: 573310877256

Ss2: IGW list



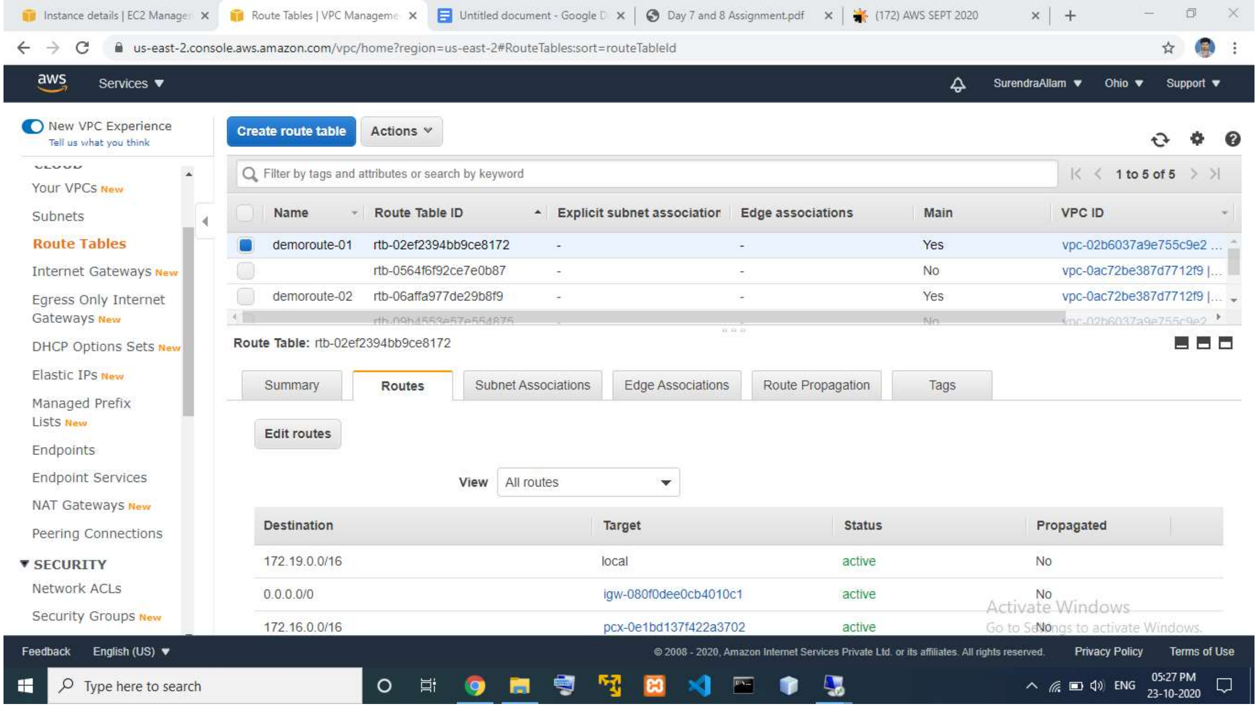
Internet gateways (3) Info

Name	Internet gateway ID	State	VPC ID
igw-02	igw-01e590b1e5654883f	Attached	vpc-0ac72be387d7712f9 | vpc-02
igw-01	igw-080f0dee0cb4010c1	Attached	vpc-02b6037a9e755c9e2 | vpc-01
–	igw-c0f7baa8	Attached	vpc-e740e38c

Select an internet gateway above

Ss3: Edit route list

Route1:



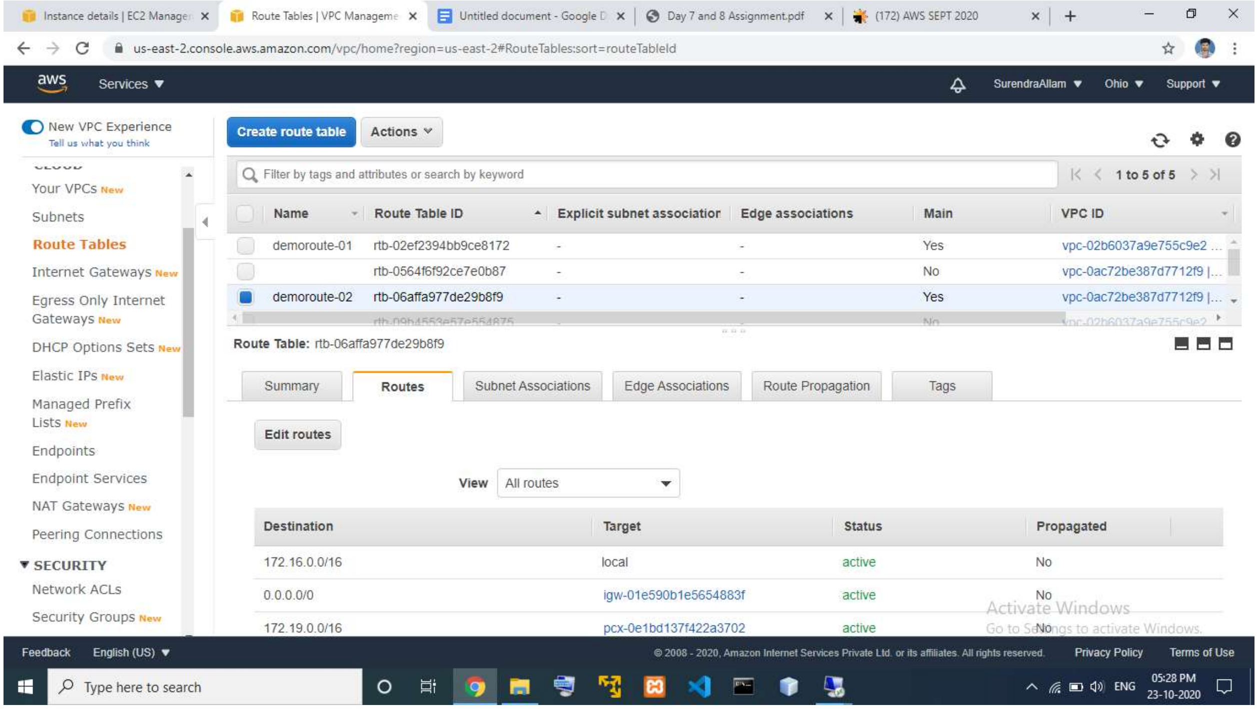
	Name	Route Table ID	Explicit subnet associatior	Edge associations	Main	VPC ID
☑	demoroute-01	rtb-02ef2394bb9ce8172	-	-	Yes	vpc-02b6037a9e755c9e2 ...
□		rtb-0564f6f92ce7e0b87	-	-	No	vpc-0ac72be387d7712f9 |...
□	demoroute-02	rtb-06affa977de29b8f9	-	-	Yes	vpc-0ac72be387d7712f9 |...
		rtb-09b4553e57e554875	-		No	vpc-02b6037a9e755c9e2

Route Table: rtb-02ef2394bb9ce8172

View: All routes

Destination	Target	Status	Propagated
172.19.0.0/16	local	active	No
0.0.0.0/0	igw-080f0dee0cb4010c1	active	No
172.16.0.0/16	pcx-0e1bd137f422a3702	active	No

Route2:



	Name	Route Table ID	Explicit subnet associatior	Edge associations	Main	VPC ID
□	demoroute-01	rtb-02ef2394bb9ce8172	-	-	Yes	vpc-02b6037a9e755c9e2 ...
□		rtb-0564f6f92ce7e0b87	-	-	No	vpc-0ac72be387d7712f9 |...
☑	demoroute-02	rtb-06affa977de29b8f9	-	-	Yes	vpc-0ac72be387d7712f9 |...
		rtb-09b4553e57e554875	-	-	No	vpc-02b6037a9e755c9e2

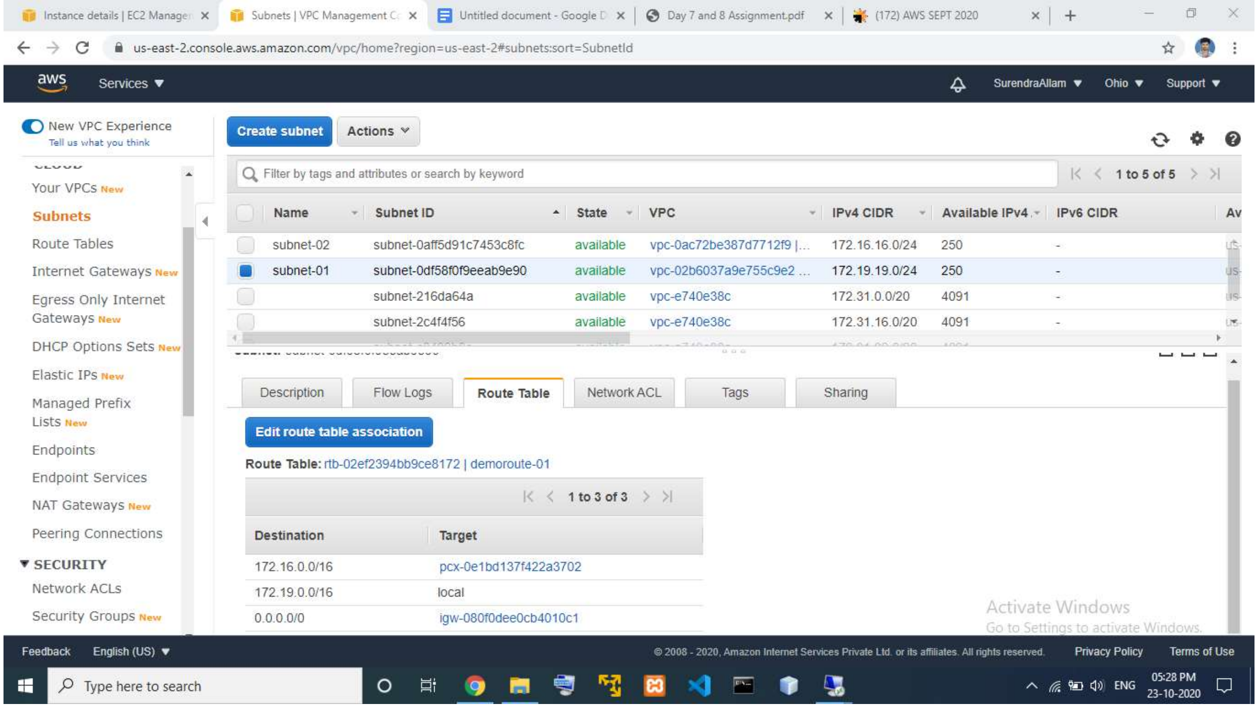
Route Table: rtb-06affa977de29b8f9

View: All routes

Destination	Target	Status	Propagated
172.16.0.0/16	local	active	No
0.0.0.0/0	igw-01e590b1e5654883f	active	No
172.19.0.0/16	pcx-0e1bd137f422a3702	active	No

Ss4: Subnet list

Subnet1:

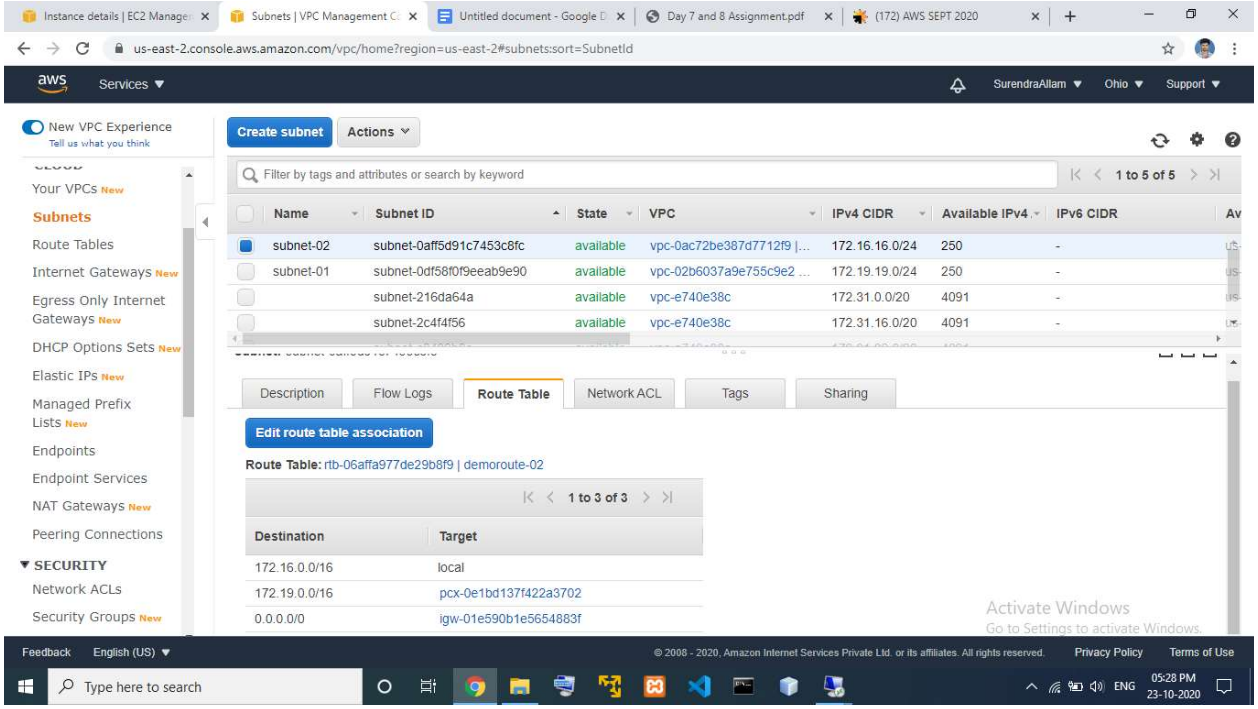


	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
□	subnet-02	subnet-0aff5d91c7453c8fc	available	vpc-0ac72be387d7712f9 |...	172.16.16.0/24	250	-
☑	subnet-01	subnet-0df58f0f9eeab9e90	available	vpc-02b6037a9e755c9e2 ...	172.19.19.0/24	250	-
□		subnet-216da64a	available	vpc-e740e38c	172.31.0.0/20	4091	-
□		subnet-2c4f4f56	available	vpc-e740e38c	172.31.16.0/20	4091	-

Route Table: rtb-02ef2394bb9ce8172 | demoroute-01

Destination	Target
172.16.0.0/16	pcx-0e1bd137f422a3702
172.19.0.0/16	local
0.0.0.0/0	igw-080f0dee0cb4010c1

Subnet2:



Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
subnet-02	subnet-0aff5d91c7453c8fc	available	vpc-0ac72be387d7712f9 |...	172.16.16.0/24	250	-
subnet-01	subnet-0df58f0f9eeab9e90	available	vpc-02b6037a9e755c9e2 ...	172.19.19.0/24	250	-
	subnet-216da64a	available	vpc-e740e38c	172.31.0.0/20	4091	-
	subnet-2c4f4f56	available	vpc-e740e38c	172.31.16.0/20	4091	-

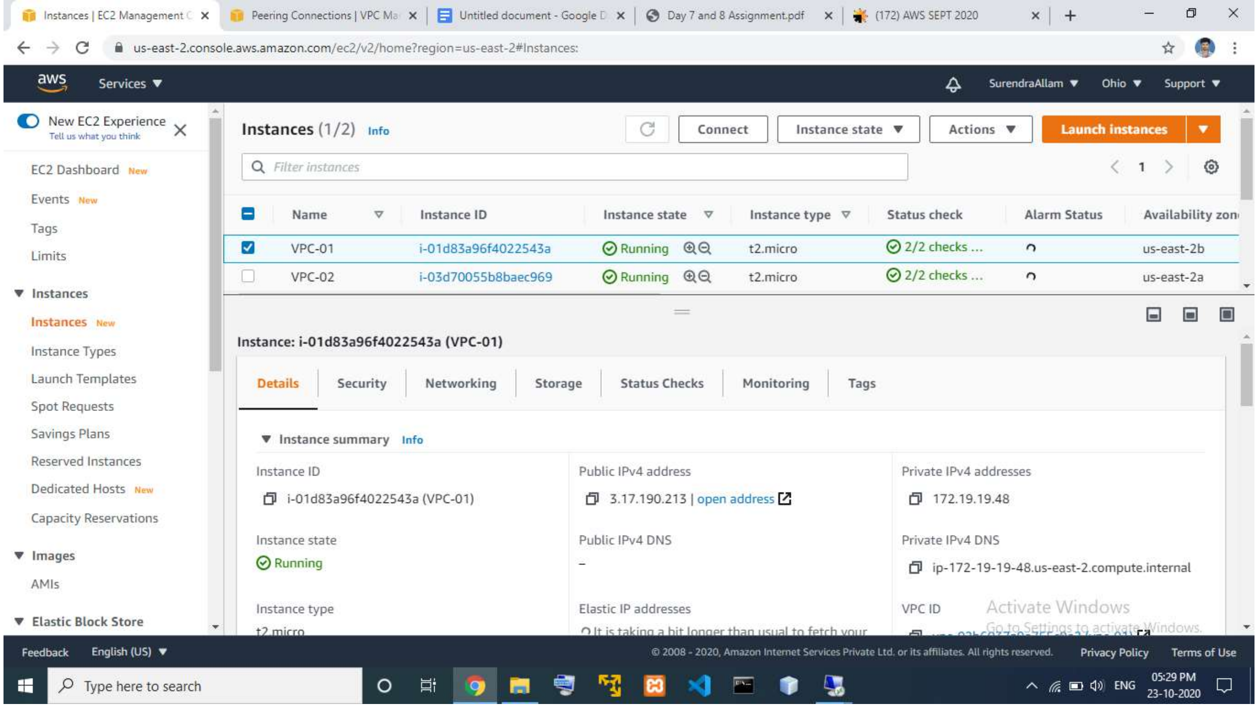
Route Table: rtb-06affa977de29b8f9 | demoroute-02

1 to 3 of 3

Destination	Target
172.16.0.0/16	local
172.19.0.0/16	pcx-0e1bd137f422a3702
0.0.0.0/0	igw-01e590b1e5654883f

Ss5: Instance details

Instance01:



Instances (1/2) Info

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zone
☑	VPC-01	i-01d83a96f4022543a	Running	t2.micro	2/2 checks ...		us-east-2b
☐	VPC-02	i-03d70055b8baec969	Running	t2.micro	2/2 checks ...		us-east-2a

Instance: i-01d83a96f4022543a (VPC-01)

Instance summary Info

Instance ID: i-01d83a96f4022543a (VPC-01)

Public IPv4 address: 3.17.190.213 | open address

Private IPv4 addresses: 172.19.19.48

Instance state: Running

Public IPv4 DNS: –

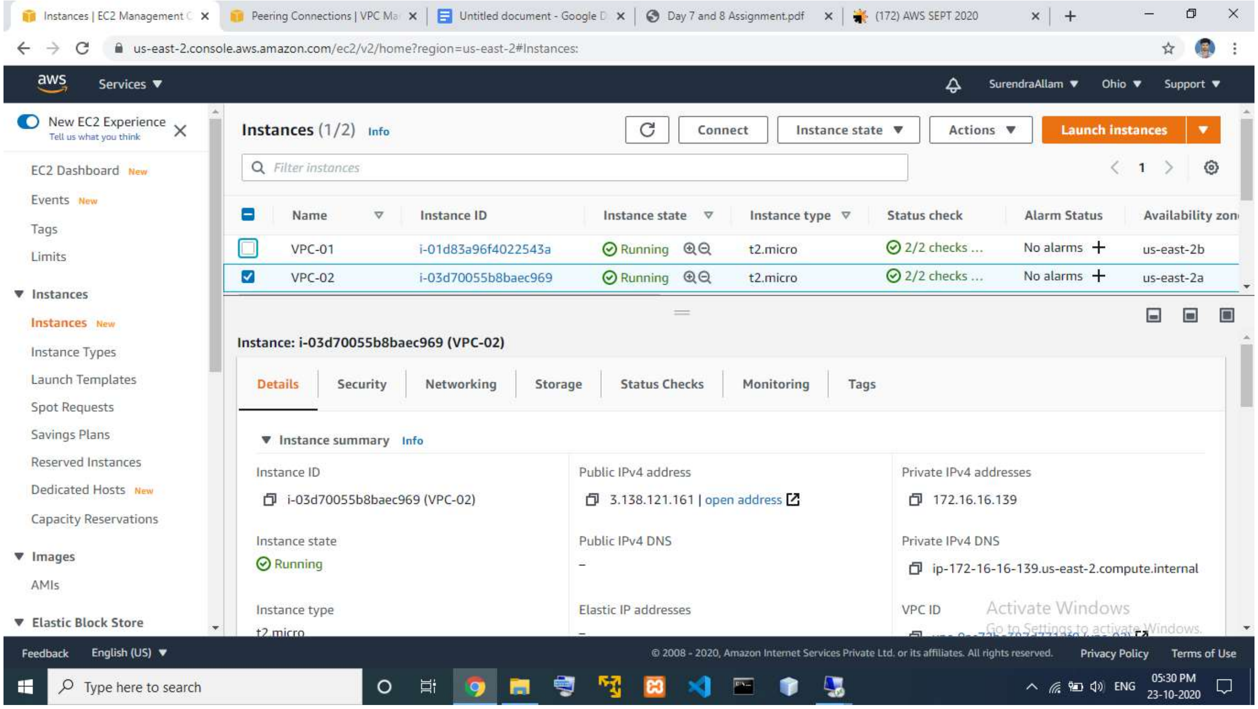
Private IPv4 DNS: ip-172-19-19-48.us-east-2.compute.internal

Instance type: t2.micro

Elastic IP addresses: It is taking a bit longer than usual to fetch your

VPC ID

Instance02:



Instances (1/2)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zone
□	VPC-01	i-01d83a96f4022543a	Running	t2.micro	2/2 checks ...	No alarms	us-east-2b
☑	VPC-02	i-03d70055b8baec969	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a

Instance: i-03d70055b8baec969 (VPC-02)

Instance summary

Instance ID: i-03d70055b8baec969 (VPC-02)

Public IPv4 address: 3.138.121.161 | open address

Private IPv4 addresses: 172.16.16.139

Instance state: Running

Public IPv4 DNS: –

Private IPv4 DNS: ip-172-16-16-139.us-east-2.compute.internal

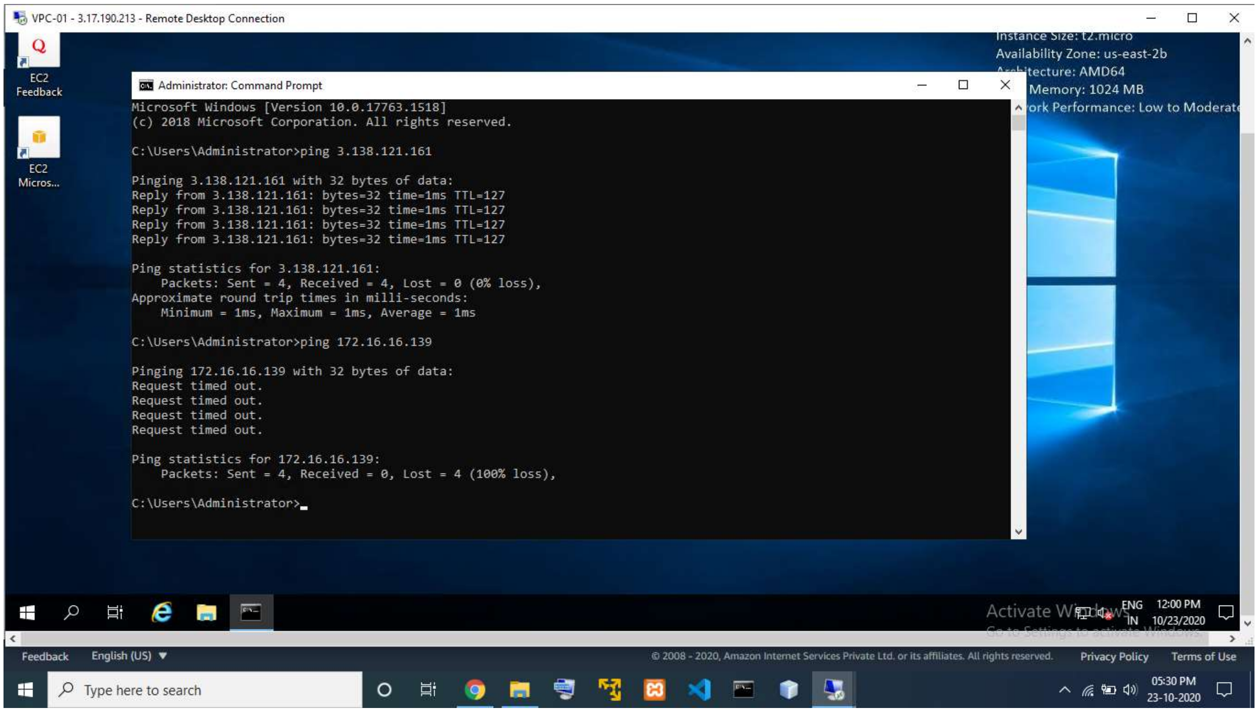
Instance type: t2.micro

Elastic IP addresses: –

VPC ID

Ss6: success public, rto private IP

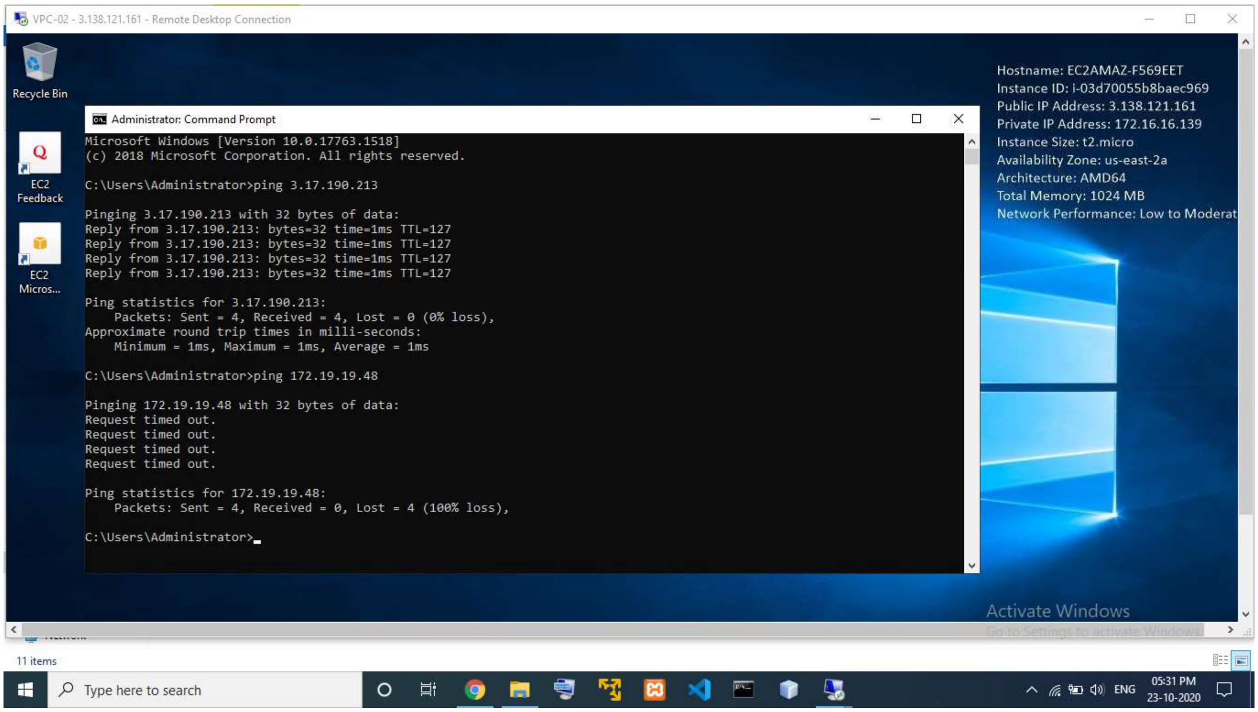
Output-1:(Instance01)



```
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 3.138.121.161

Pinging 3.138.121.161 with 32 bytes of data:
Reply from 3.138.121.161: bytes=32 time=1ms TTL=127
Reply from 3.138.121.161: bytes=32 time=1ms TTL=127
Reply from 3.138.121.161: bytes=32 time=1ms TTL=127
Reply from 3.138.121.161: bytes=32 time=1ms TTL=127

Ping statistics for 3.138.121.161:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>ping 172.16.16.139

Pinging 172.16.16.139 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.16.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>_
```

VPC-01 - 3.17.190.213 - Remote Desktop Connection
Administrator: Command Prompt
EC2 Feedback
EC2 Micros...
Instance Size: t2.micro
Availability Zone: us-east-2b
Architecture: AMD64
Memory: 1024 MB
ork Performance: Low to Moderate
Activate Windows
Go to Settings to activate Windows.
ENG IN
12:00 PM
10/23/2020
Feedback
English (US)
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
ENG
05:30 PM
23-10-2020

Output02(Instance02):

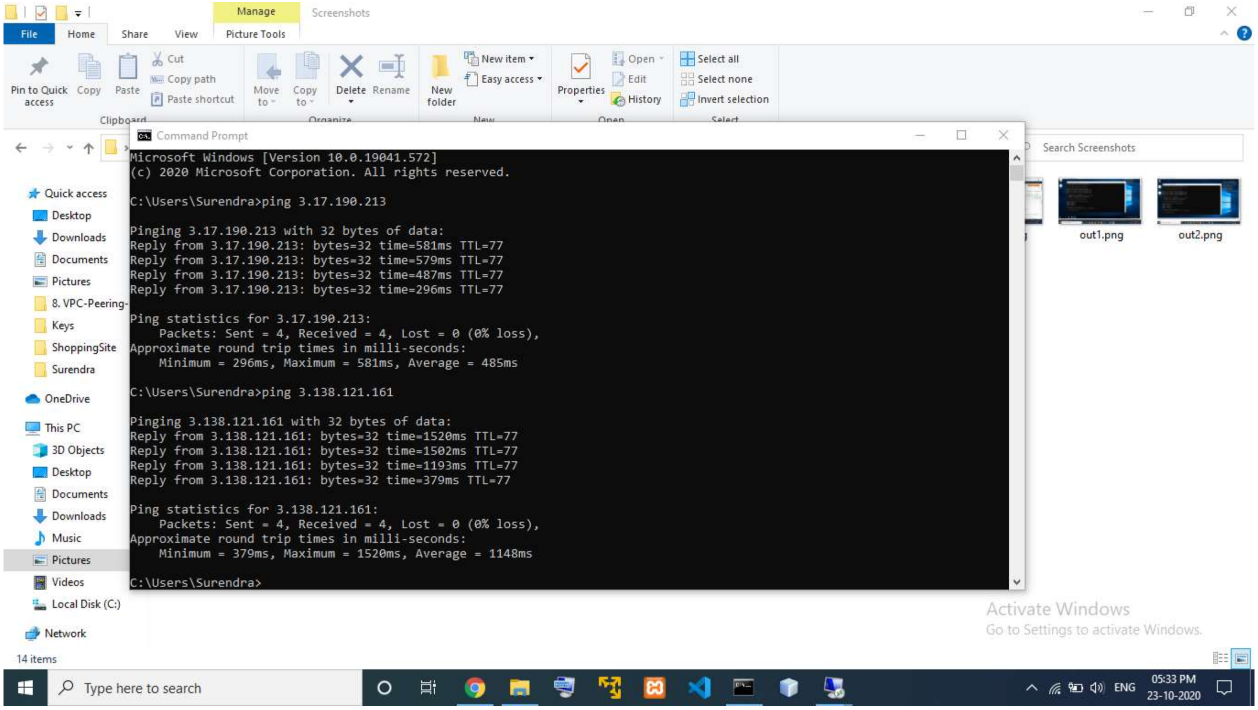


VPC-02 - 3.138.121.161 - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Micros...
Administrator: Command Prompt
Activate Windows
Go to Settings to activate Windows.
11 items
Type here to search
ENG
05:31 PM
23-10-2020

Hostname: EC2AMAZ-F569EET
Instance ID: i-03d70055b8baec969
Public IP Address: 3.138.121.161
Private IP Address: 172.16.16.139
Instance Size: t2.micro
Availability Zone: us-east-2a
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to Moderat

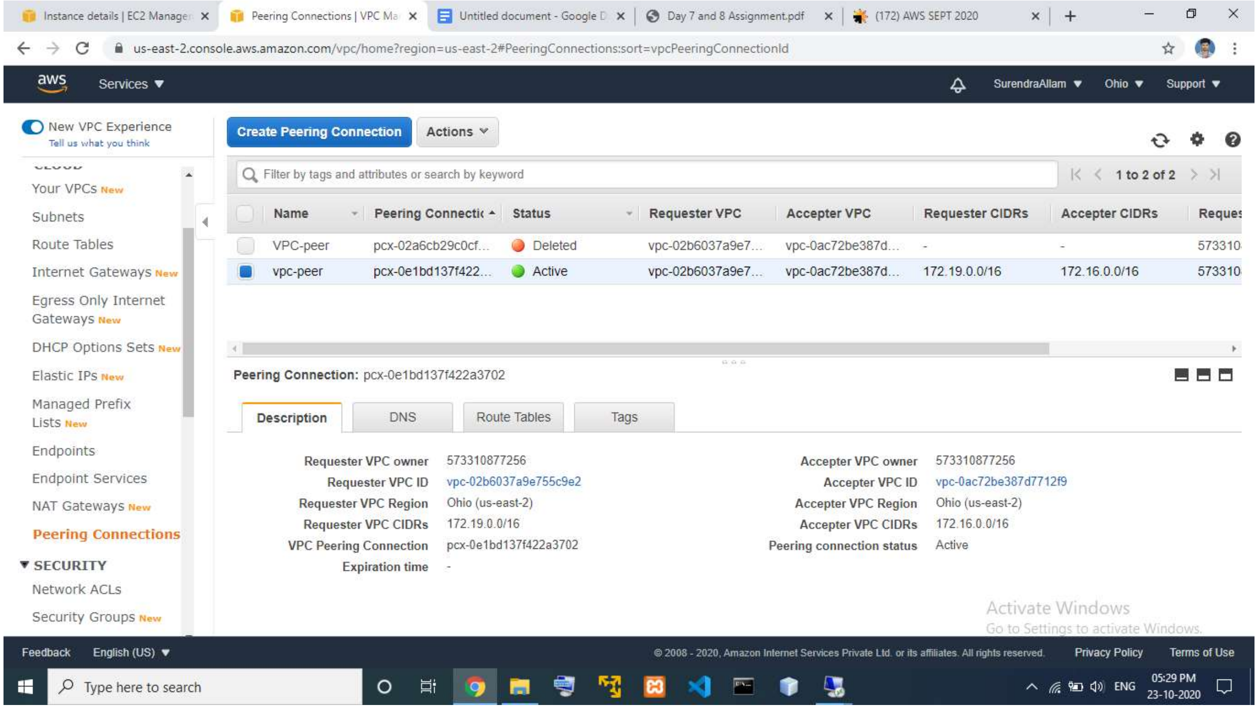
```
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 3.17.190.213

Pinging 3.17.190.213 with 32 bytes of data:
Reply from 3.17.190.213: bytes=32 time=1ms TTL=127
Reply from 3.17.190.213: bytes=32 time=1ms TTL=127
Reply from 3.17.190.213: bytes=32 time=1ms TTL=127
Reply from 3.17.190.213: bytes=32 time=1ms TTL=127

Ping statistics for 3.17.190.213:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>ping 172.19.19.48

Pinging 172.19.19.48 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.19.19.48:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>_
```

Output(Base Machine):



```
Microsoft Windows [Version 10.0.19041.572]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Surendra>ping 3.17.190.213

Pinging 3.17.190.213 with 32 bytes of data:
Reply from 3.17.190.213: bytes=32 time=581ms TTL=77
Reply from 3.17.190.213: bytes=32 time=579ms TTL=77
Reply from 3.17.190.213: bytes=32 time=487ms TTL=77
Reply from 3.17.190.213: bytes=32 time=296ms TTL=77

Ping statistics for 3.17.190.213:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 296ms, Maximum = 581ms, Average = 485ms

C:\Users\Surendra>ping 3.138.121.161

Pinging 3.138.121.161 with 32 bytes of data:
Reply from 3.138.121.161: bytes=32 time=1520ms TTL=77
Reply from 3.138.121.161: bytes=32 time=1502ms TTL=77
Reply from 3.138.121.161: bytes=32 time=1193ms TTL=77
Reply from 3.138.121.161: bytes=32 time=379ms TTL=77

Ping statistics for 3.138.121.161:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 379ms, Maximum = 1520ms, Average = 1148ms

C:\Users\Surendra>
```

Ss7: peering with req and acceptor



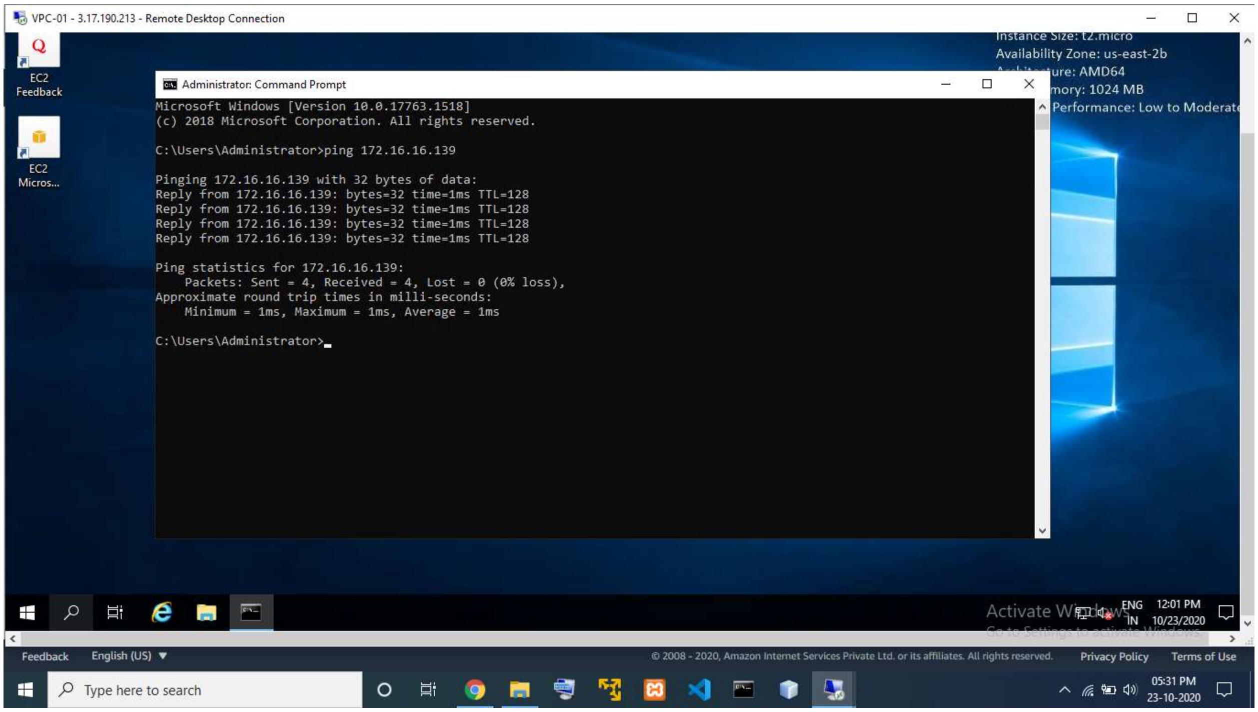
us-east-2.console.amazon.com/vpc/home?region=us-east-2#PeeringConnections:sort=vpcPeeringConnectionId

Name	Peering Connectic	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Reques
VPC-peer	pcx-02a6cb29c0cf...	Deleted	vpc-02b6037a9e7...	vpc-0ac72be387d...	-	-	573310
vpc-peer	pcx-0e1bd137f422...	Active	vpc-02b6037a9e7...	vpc-0ac72be387d...	172.19.0.0/16	172.16.0.0/16	573310

Peering Connection: pcx-0e1bd137f422a3702

Requester VPC owner	573310877256	Accepter VPC owner	573310877256
Requester VPC ID	vpc-02b6037a9e755c9e2	Accepter VPC ID	vpc-0ac72be387d7712f9
Requester VPC Region	Ohio (us-east-2)	Accepter VPC Region	Ohio (us-east-2)
Requester VPC CIDRs	172.19.0.0/16	Accepter VPC CIDRs	172.16.0.0/16
VPC Peering Connection	pcx-0e1bd137f422a3702	Peering connection status	Active
Expiration time	-		

Ss8: success for private Instance01_Output(Private IP success):



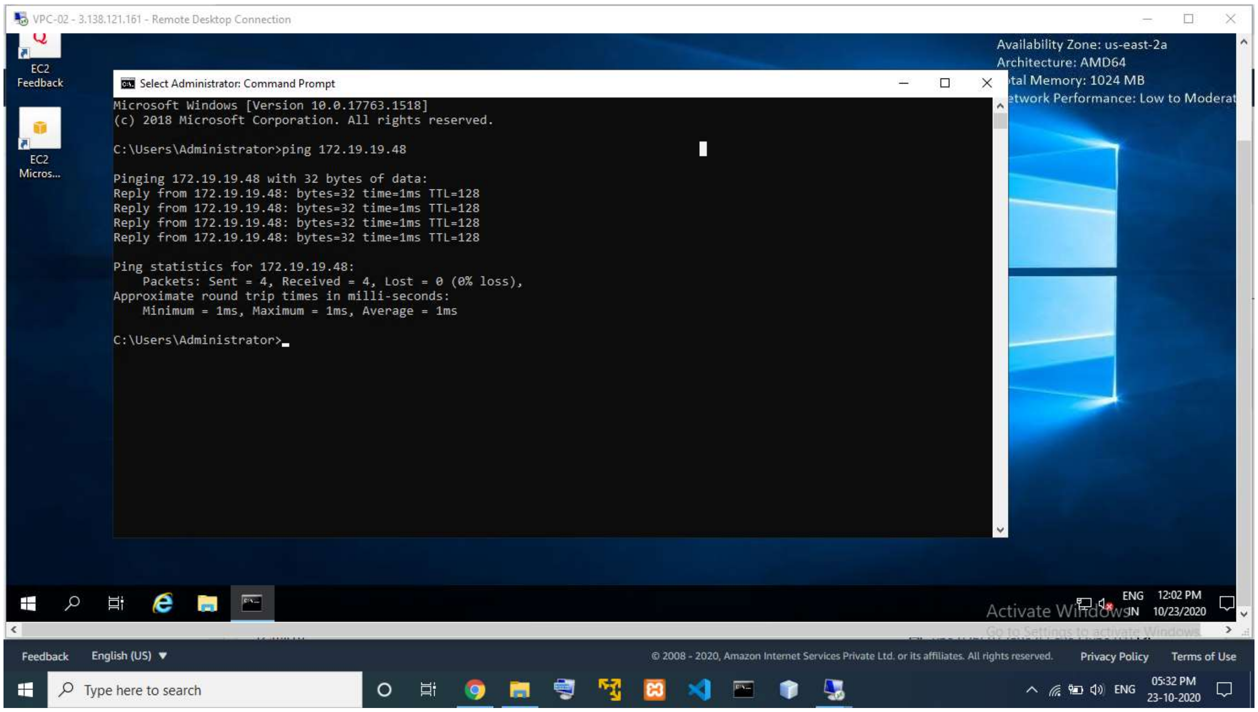
VPC-01 - 3.17.190.213 - Remote Desktop Connection

Instance Size: t2.micro
Availability Zone: us-east-2b
Architecture: AMD64
Memory: 1024 MB
Performance: Low to Moderate

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 172.16.16.139

Pinging 172.16.16.139 with 32 bytes of data:
Reply from 172.16.16.139: bytes=32 time=1ms TTL=128
Reply from 172.16.16.139: bytes=32 time=1ms TTL=128
Reply from 172.16.16.139: bytes=32 time=1ms TTL=128
Reply from 172.16.16.139: bytes=32 time=1ms TTL=128

Ping statistics for 172.16.16.139:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>_
```

Instance02_Output(Private IP success):


VPC-02 - 3.138.121.161 - Remote Desktop Connection
EC2 Feedback
EC2 Micros...
Select Administrator: Command Prompt
Availability Zone: us-east-2a
Architecture: AMD64
tal Memory: 1024 MB
etwork Performance: Low to Moderat
Activate Windows
Go to Settings to activate Windows.
ENG IN
12:02 PM
10/23/2020
Feedback
English (US)
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
ENG
05:32 PM
23-10-2020

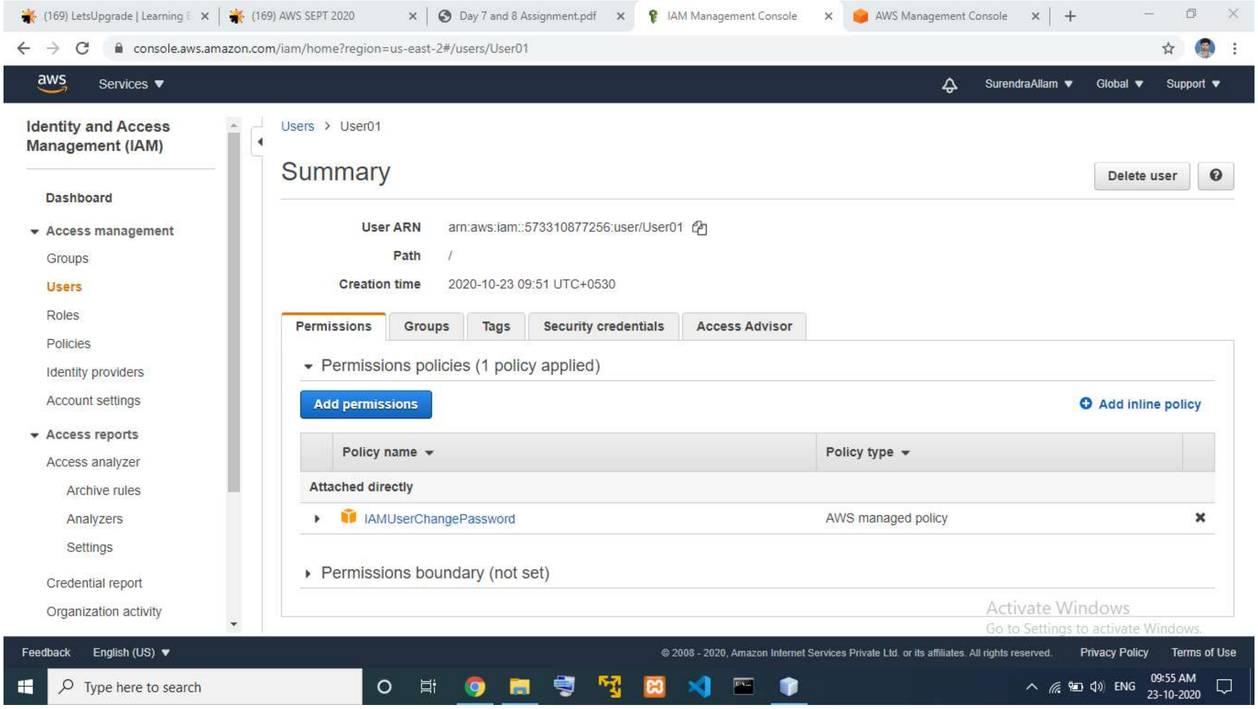
```
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 172.19.19.48

Pinging 172.19.19.48 with 32 bytes of data:
Reply from 172.19.19.48: bytes=32 time=1ms TTL=128
Reply from 172.19.19.48: bytes=32 time=1ms TTL=128
Reply from 172.19.19.48: bytes=32 time=1ms TTL=128
Reply from 172.19.19.48: bytes=32 time=1ms TTL=128

Ping statistics for 172.19.19.48:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>
```

Project 2:

IAM

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

Ss1: user summary with all tab information



Summary

User ARN arn:aws:iam::573310877256:user/User01

Path /

Creation time 2020-10-23 09:51 UTC+0530

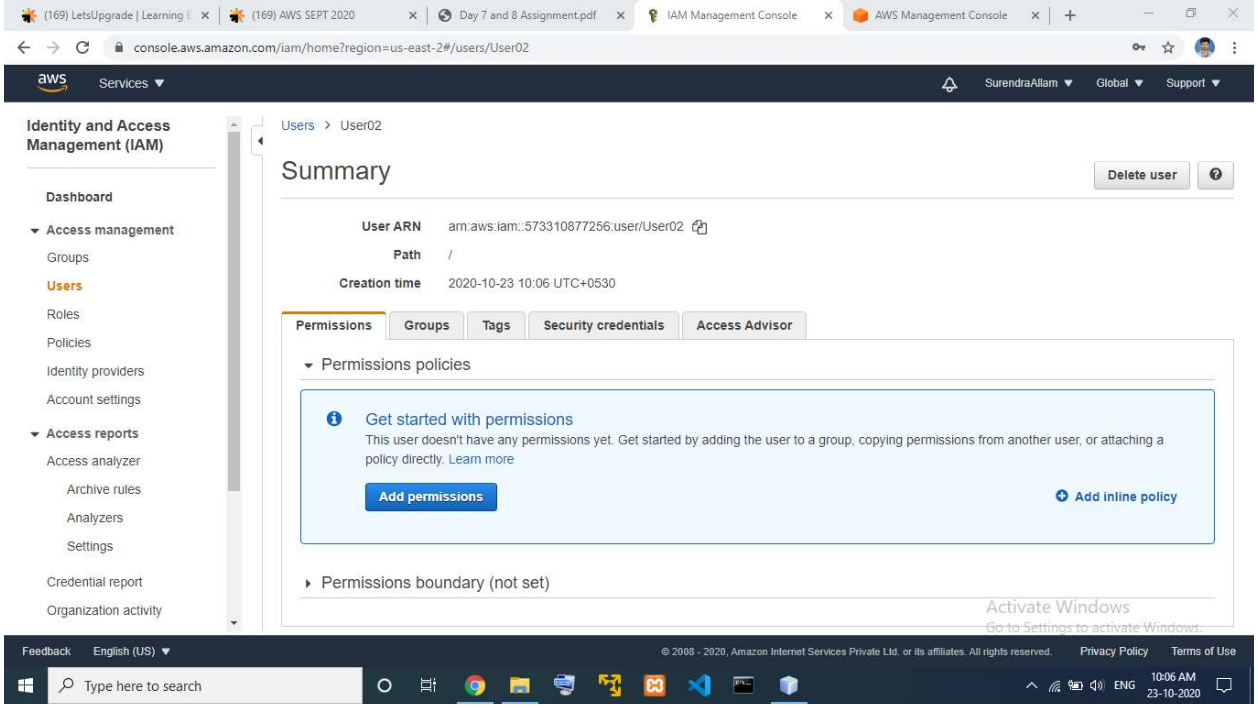
Permissions policies (1 policy applied)

Policy name	Policy type
Attached directly	
IAMUserChangePassword	AWS managed policy

Permissions boundary (not set)

Task 2:Creating users without the IAM password policy.

Ss2: user summary with all tab information



Summary

User ARN arn:aws:iam::573310877256:user/User02

Path /

Creation time 2020-10-23 10:06 UTC+0530

Permissions policies

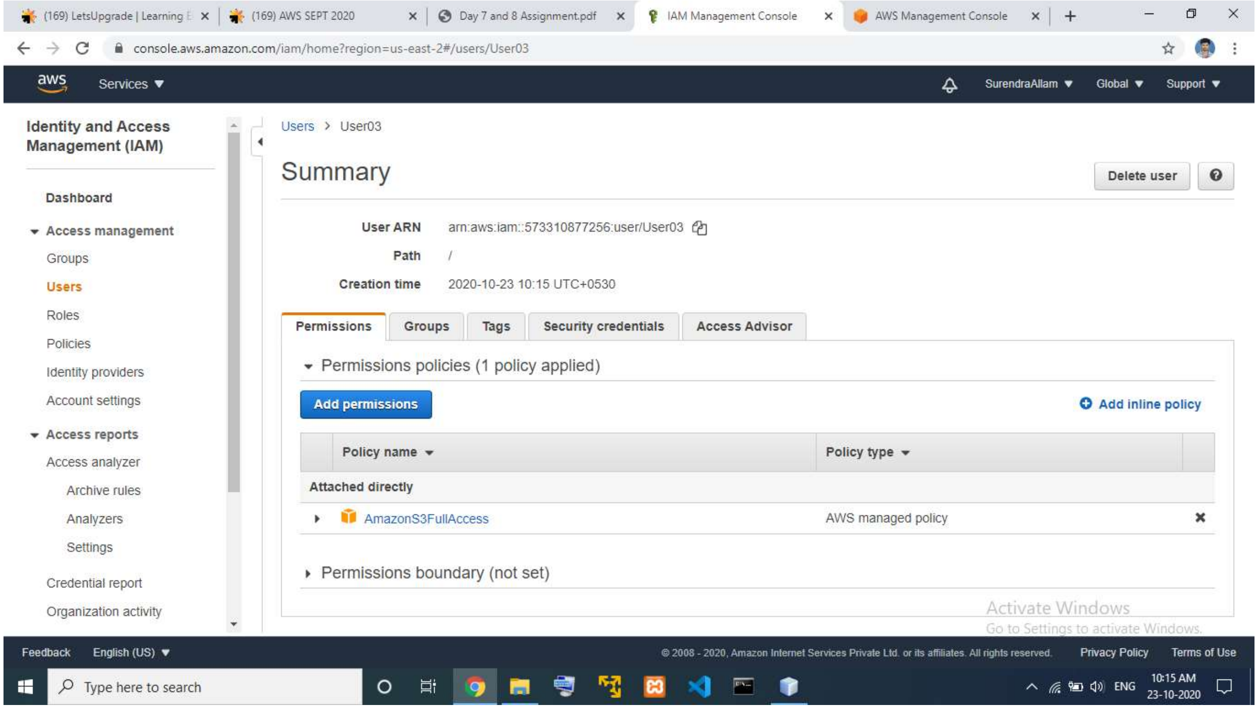
Get started with permissions

This user doesn't have any permissions yet. Get started by adding the user to a group, copying permissions from another user, or attaching a policy directly. Learn more

Permissions boundary (not set)

Task 3:Create a user with S3 full access

Ss3: User summary



Summary

User ARN	arn:aws:iam::573310877256:user/User03
Path	/
Creation time	2020-10-23 10:15 UTC+0530

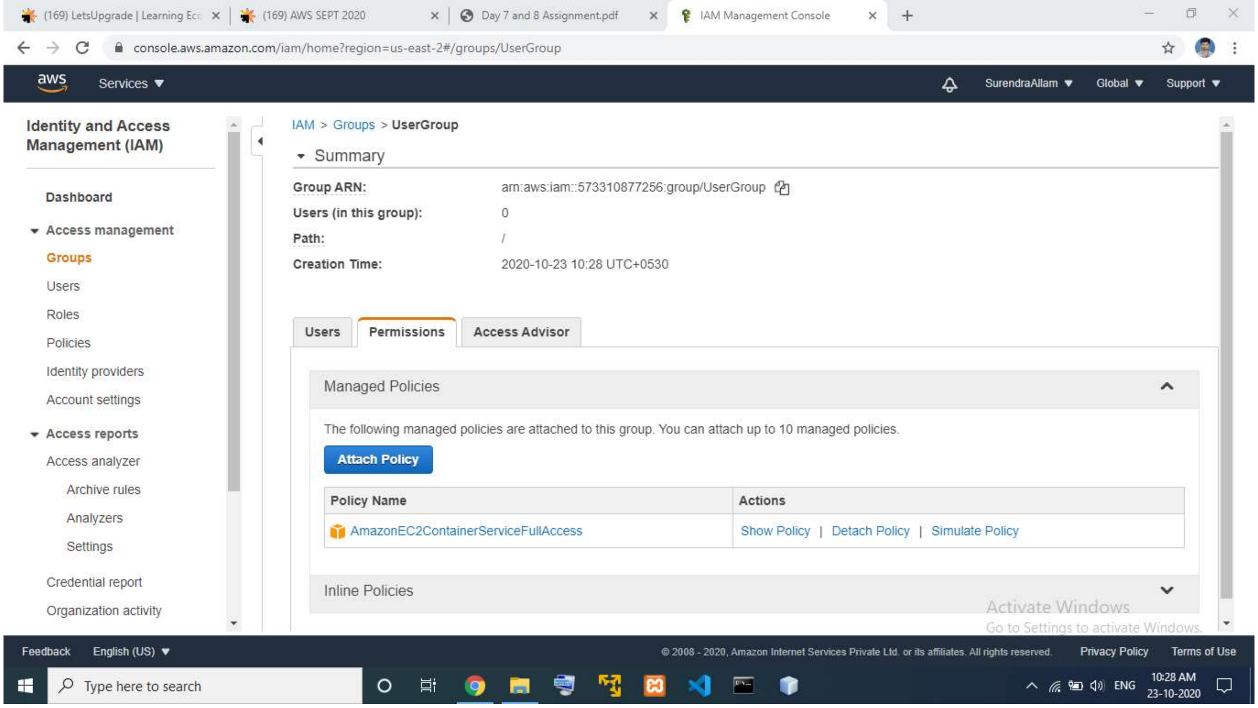
Permissions policies (1 policy applied)

Policy name	Policy type
Attached directly	
AmazonS3FullAccess	AWS managed policy

Permissions boundary (not set)

Task4: Create a group with ec2 full access

Ss4: group summary



Summary

Group ARN:	arn:aws:iam::573310877256:group/UserGroup
Users (in this group):	0
Path:	/
Creation Time:	2020-10-23 10:28 UTC+0530

Managed Policies

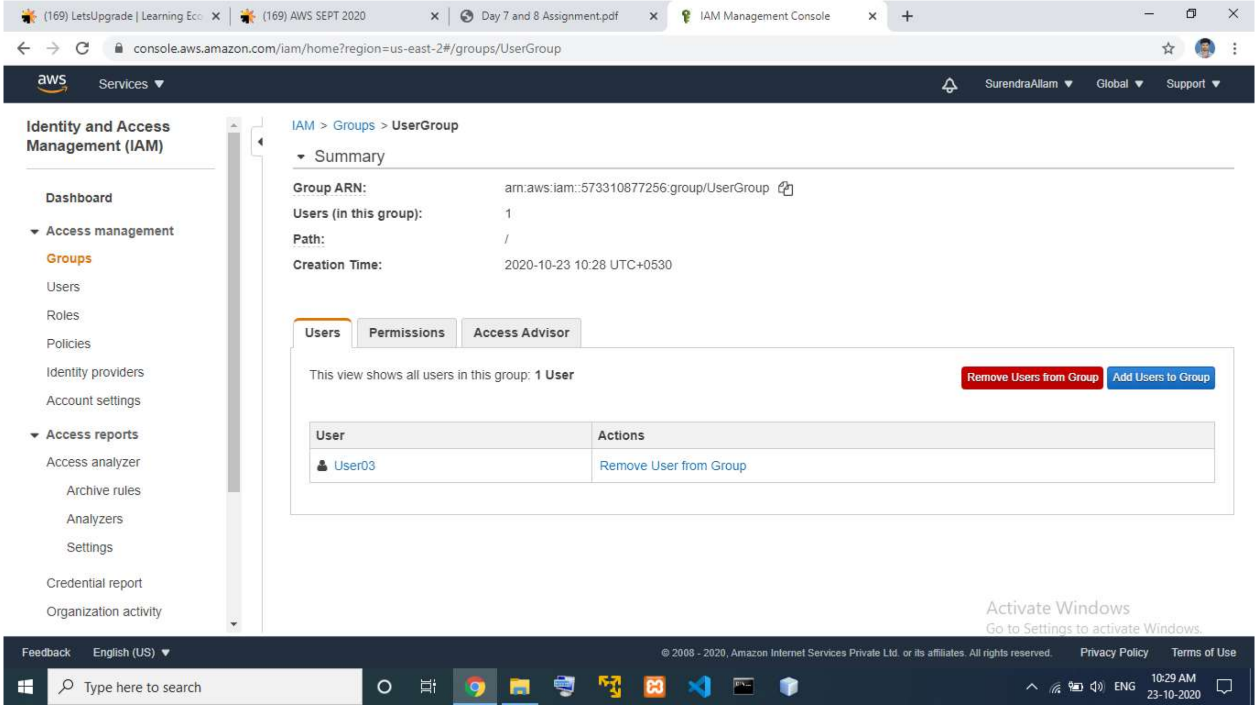
The following managed policies are attached to this group. You can attach up to 10 managed policies.

Policy Name	Actions
AmazonEC2ContainerServiceFullAccess	Show Policy | Detach Policy | Simulate Policy

Inline Policies

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



IAM > Groups > UserGroup

Summary

Group ARN: arn:aws:iam::573310877256:group/UserGroup

Users (in this group): 1

Path: /

Creation Time: 2020-10-23 10:28 UTC+0530

Users | Permissions | Access Advisor

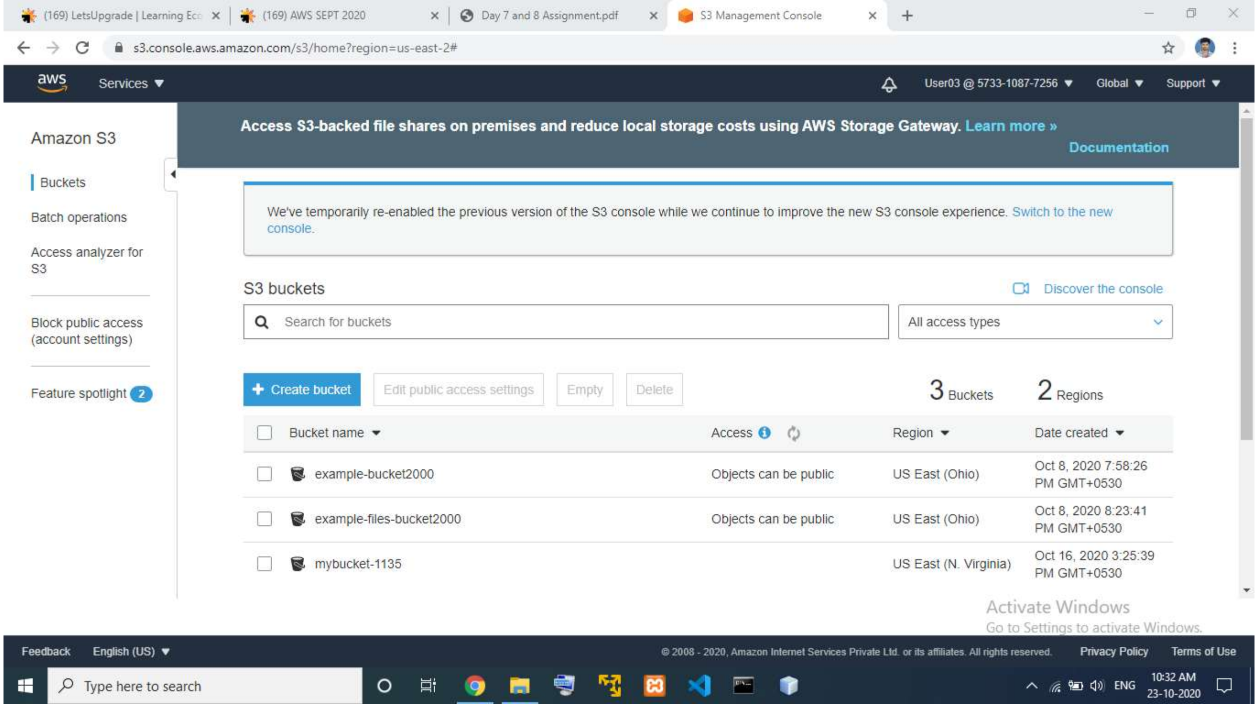
This view shows all users in this group: **1 User**

Remove Users from Group | Add Users to Group

User	Actions
User03	Remove User from Group

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

User Policy(S3_Full_Access) Reflecting:


(169) LetsUpgrade | Learning Eco
(169) AWS SEPT 2020
Day 7 and 8 Assignment.pdf
S3 Management Console
s3.console.aws.amazon.com/s3/home?region=us-east-2#
aws
Services
User03 @ 5733-1087-7256
Global
Support
Amazon S3
Buckets
Batch operations
Access analyzer for S3
Block public access (account settings)
Feature spotlight 2
Activate Windows
Go to Settings to activate Windows.
Feedback
English (US)
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
ENG
10:32 AM
23-10-2020

Access S3-backed file shares on premises and reduce local storage costs using AWS Storage Gateway. Learn more »

Documentation

We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. Switch to the new console.

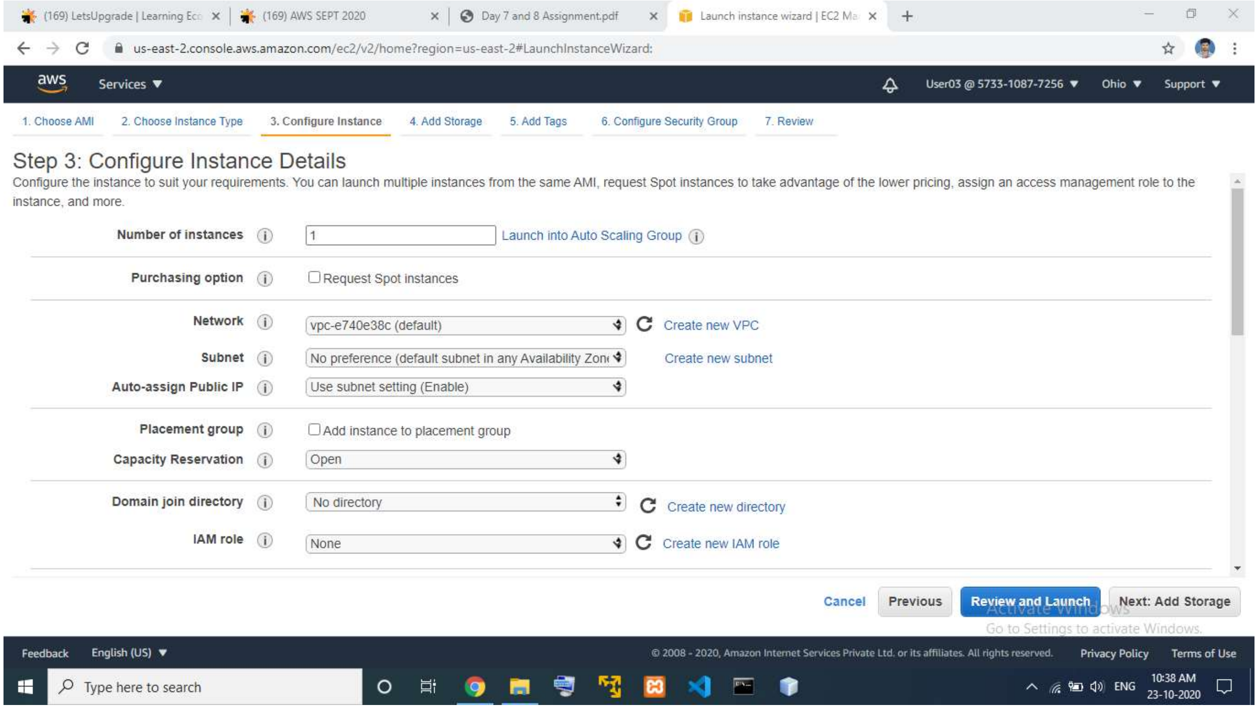
S3 buckets — Discover the console

Search for buckets — All access types

+ Create bucket | Edit public access settings | Empty | Delete — 3 Buckets — 2 Regions

Bucket name	Access	Region	Date created
example-bucket2000	Objects can be public	US East (Ohio)	Oct 8, 2020 7:58:26 PM GMT+0530
example-files-bucket2000	Objects can be public	US East (Ohio)	Oct 8, 2020 8:23:41 PM GMT+0530
mybucket-1135		US East (N. Virginia)	Oct 16, 2020 3:25:39 PM GMT+0530

Group Policy(EC02_Full_Access) Reflecting:


(169) LetsUpgrade | Learning Eco
(169) AWS SEPT 2020
Day 7 and 8 Assignment.pdf
Launch instance wizard | EC2 Ma
us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:
aws
Services ▼
User03 @ 5733-1087-7256 ▼
Ohio ▼
Support ▼
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-e740e38c (default) — Create new VPC

Subnet: No preference (default subnet in any Availability Zone) — Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

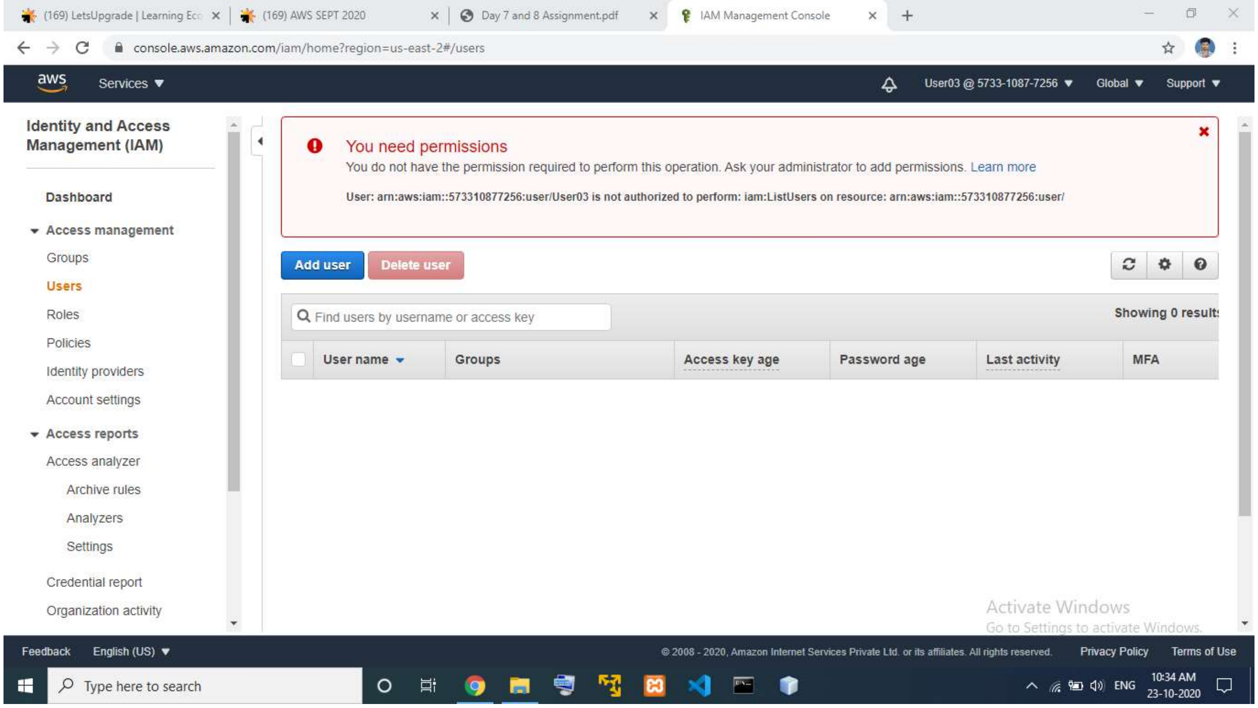
Placement group: □ Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory — Create new directory

IAM role: None — Create new IAM role

Other Policy(S3_Full_Access) Not Reflecting:



You need permissions

You do not have the permission required to perform this operation. Ask your administrator to add permissions. Learn more

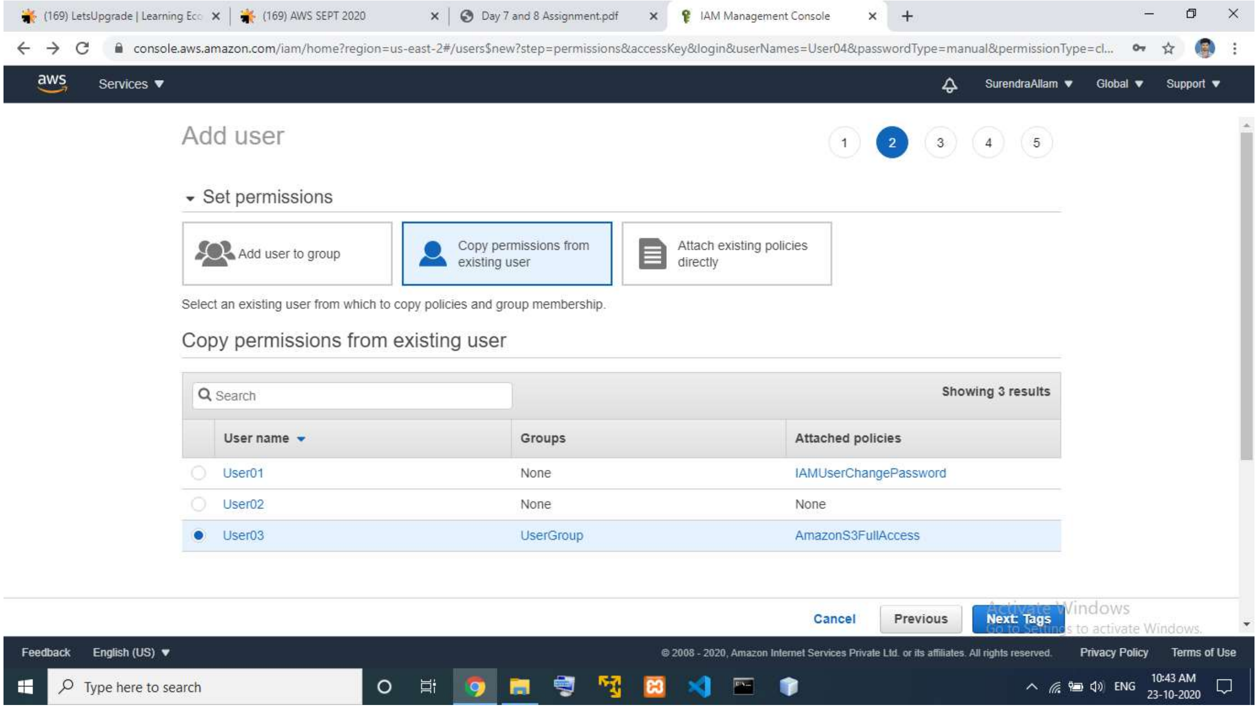
User: arn:aws:iam::573310877256:user/User03 is not authorized to perform: iam:ListUsers on resource: arn:aws:iam::573310877256:user/

□	User name ▼	Groups	Access key age	Password age	Last activity	MFA

Activate Windows
Go to Settings to activate Windows.
Feedback
English (US) ▼
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
ENG
10:34 AM
23-10-2020

Task 6:Copy policies from the existing user

Ss7: attach user summary of the user from which you create a new user


(169) LetsUpgrade | Learning Ecc
(169) AWS SEPT 2020
Day 7 and 8 Assignment.pdf
IAM Management Console
console.aws.amazon.com/iam/home?region=us-east-2#/users$new?step=permissions&accessKey&login&userNames=User04&passwordType=manual&permissionType=cl...
aws
Services
SurendraAllam
Global
Support
1
2
3
4
5
Feedback
English (US)
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
ENG
10:43 AM
23-10-2020
Activate Windows
Go to Settings to activate Windows.

Add user

Set permissions

Add user to group | Copy permissions from existing user | Attach existing policies directly

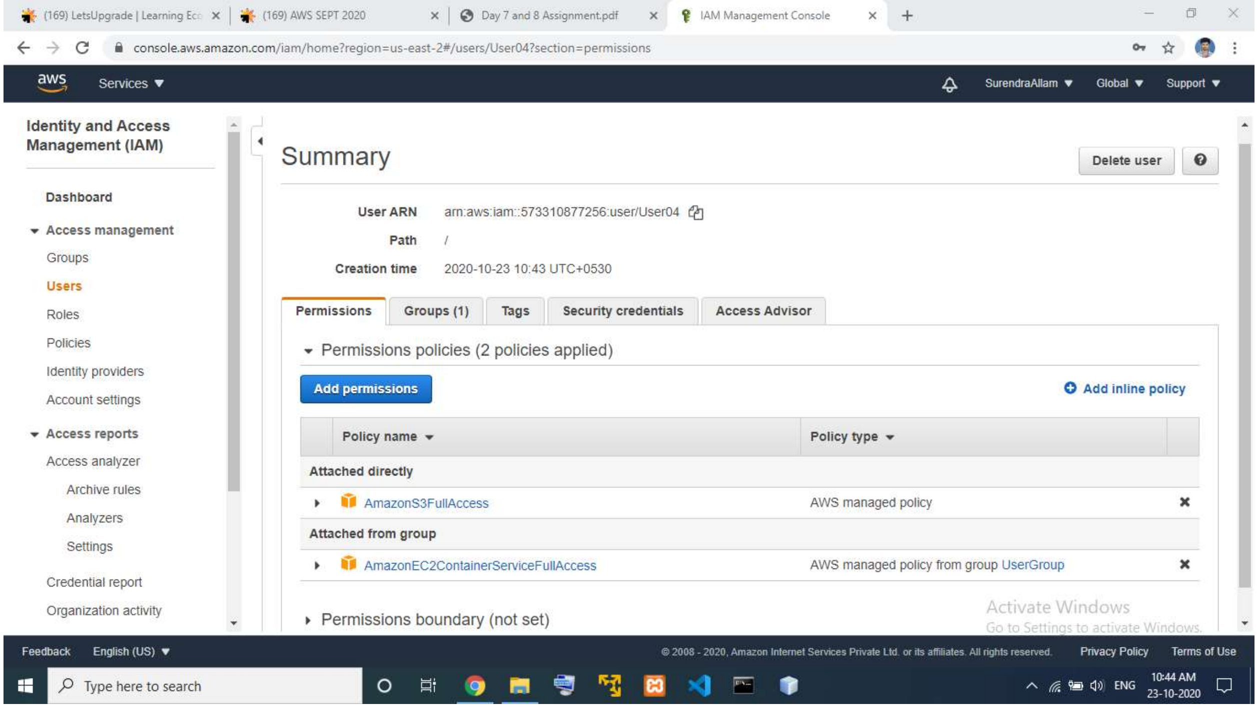
Select an existing user from which to copy policies and group membership.

Copy permissions from existing user

Search — Showing 3 results

	User name	Groups	Attached policies
○	User01	None	IAMUserChangePassword
○	User02	None	None
●	User03	UserGroup	AmazonS3FullAccess

Cancel · Previous · Next: Tags



Summary

User ARN arn:aws:iam::573310877256:user/User04

Path /

Creation time 2020-10-23 10:43 UTC+0530

Permissions | Groups (1) | Tags | Security credentials | Access Advisor

Permissions policies (2 policies applied)

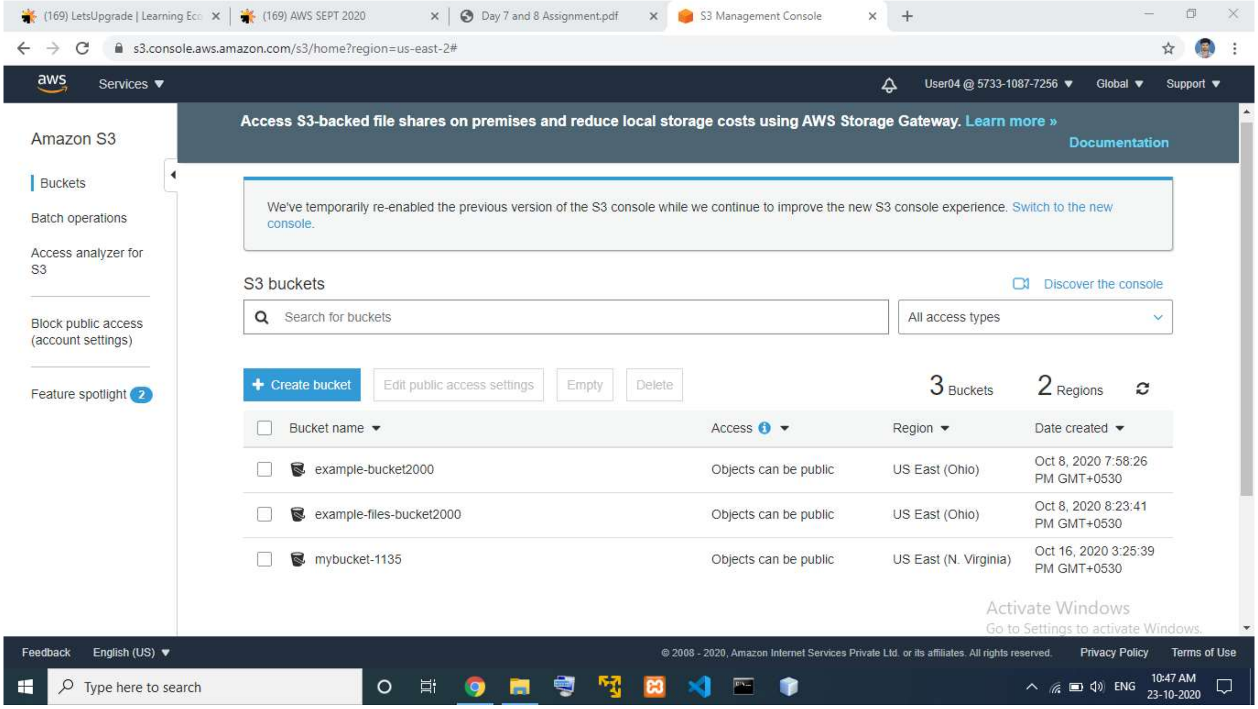
Add permissions · Add inline policy

Policy name	Policy type
Attached directly	
AmazonS3FullAccess	AWS managed policy
Attached from group	
AmazonEC2ContainerServiceFullAccess	AWS managed policy from group UserGroup

Permissions boundary (not set)

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

S3 Full Access reflecting:



(169) LetsUpgrade | Learning Eco
(169) AWS SEPT 2020
Day 7 and 8 Assignment.pdf
S3 Management Console
s3.console.aws.amazon.com/s3/home?region=us-east-2#
aws
Services
User04 @ 5733-1087-7256
Global
Support

Amazon S3

- Buckets
- Batch operations
- Access analyzer for S3
- Block public access (account settings)
- Feature spotlight 2

Access S3-backed file shares on premises and reduce local storage costs using AWS Storage Gateway. Learn more »

Documentation

We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. Switch to the new console.

S3 buckets

Discover the console

Search for buckets | All access types

Create bucket | Edit public access settings | Empty | Delete

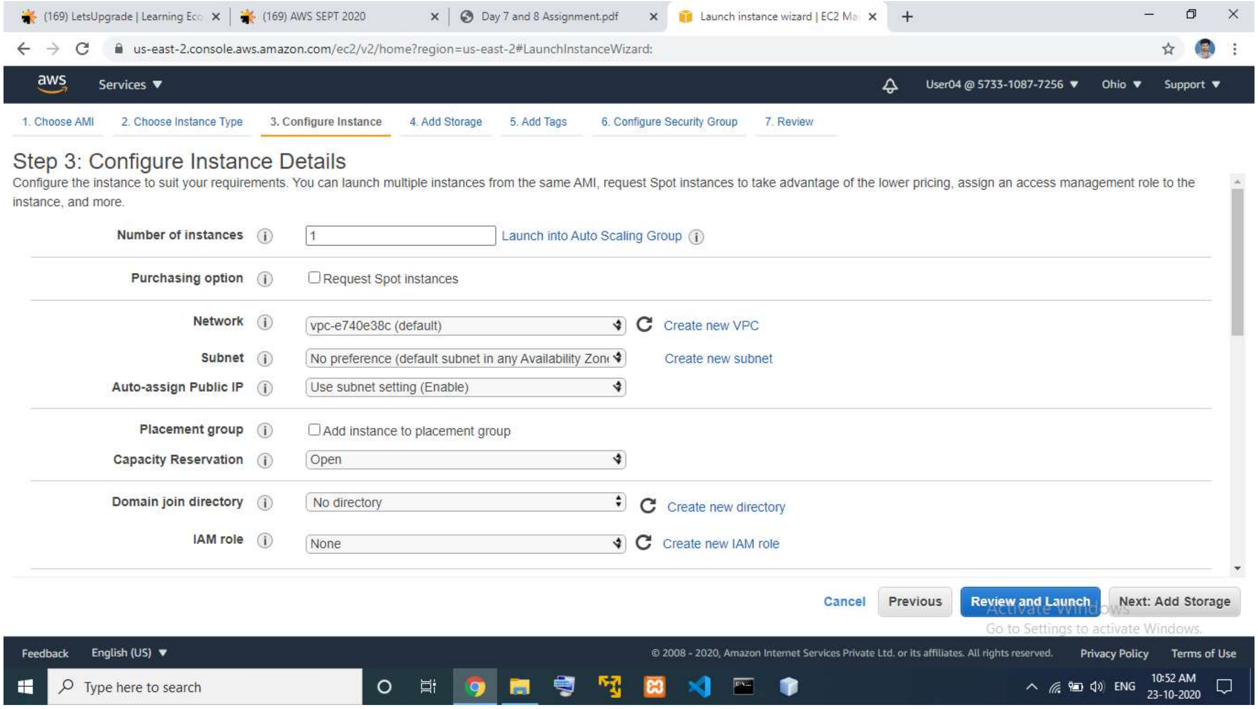
3 Buckets 2 Regions

	Bucket name	Access	Region	Date created
□	example-bucket2000	Objects can be public	US East (Ohio)	Oct 8, 2020 7:58:26 PM GMT+0530
□	example-files-bucket2000	Objects can be public	US East (Ohio)	Oct 8, 2020 8:23:41 PM GMT+0530
□	mybucket-1135	Objects can be public	US East (N. Virginia)	Oct 16, 2020 3:25:39 PM GMT+0530

Activate Windows
Go to Settings to activate Windows.

Feedback
English (US)
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
ENG
10:47 AM
23-10-2020

EC2 Full Access reflecting:



(169) LetsUpgrade | Learning Eco
(169) AWS SEPT 2020
Day 7 and 8 Assignment.pdf
Launch instance wizard | EC2 Ma
us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:
aws
Services
User04 @ 5733-1087-7256
Ohio
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

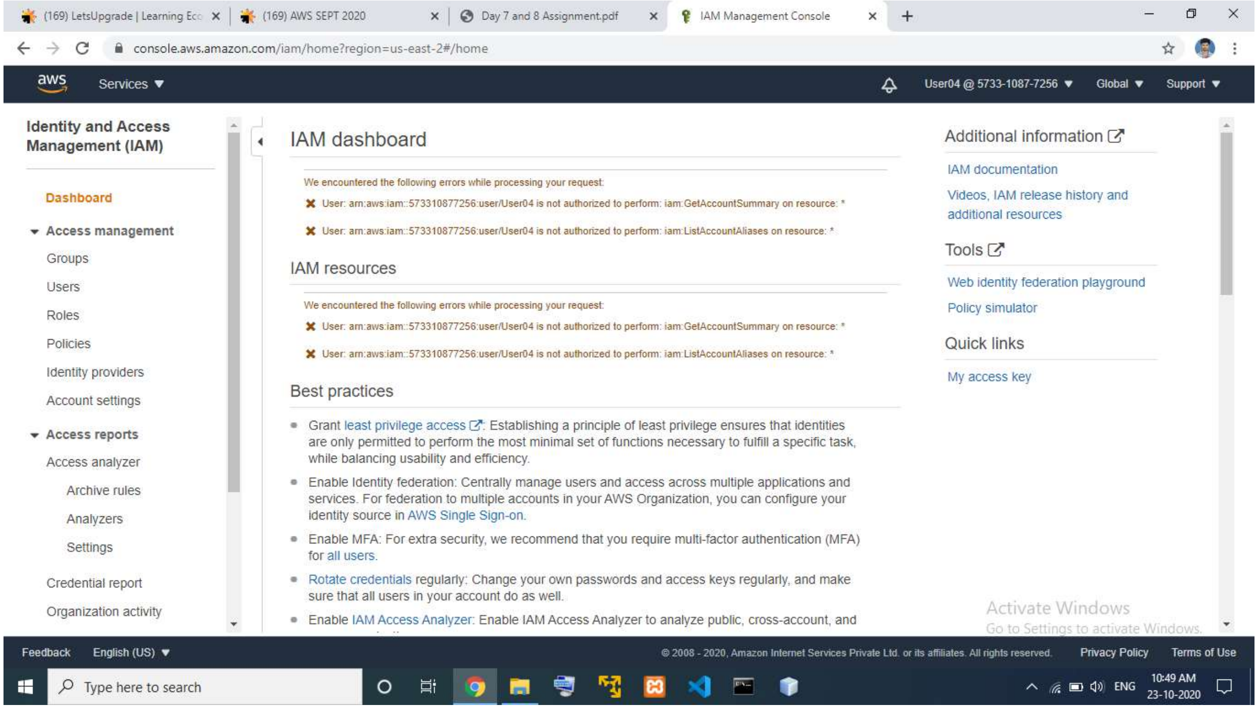
Number of instances	1	Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances	
Network	vpc-e740e38c (default)	Create new VPC
Subnet	No preference (default subnet in any Availability Zon	Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)	
Placement group	□ Add instance to placement group	
Capacity Reservation	Open	
Domain join directory	No directory	Create new directory
IAM role	None	Create new IAM role

Cancel | Previous | Review and Launch | Next: Add Storage

Activate Windows
Go to Settings to activate Windows.

Feedback
English (US)
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
ENG
10:52 AM
23-10-2020

Others not reflecting:



IAM dashboard

We encountered the following errors while processing your request:

- User: arn:aws:iam::573310877256:user/User04 is not authorized to perform: iam:GetAccountSummary on resource: *
- User: arn:aws:iam::573310877256:user/User04 is not authorized to perform: iam:ListAccountAliases on resource: *

IAM resources

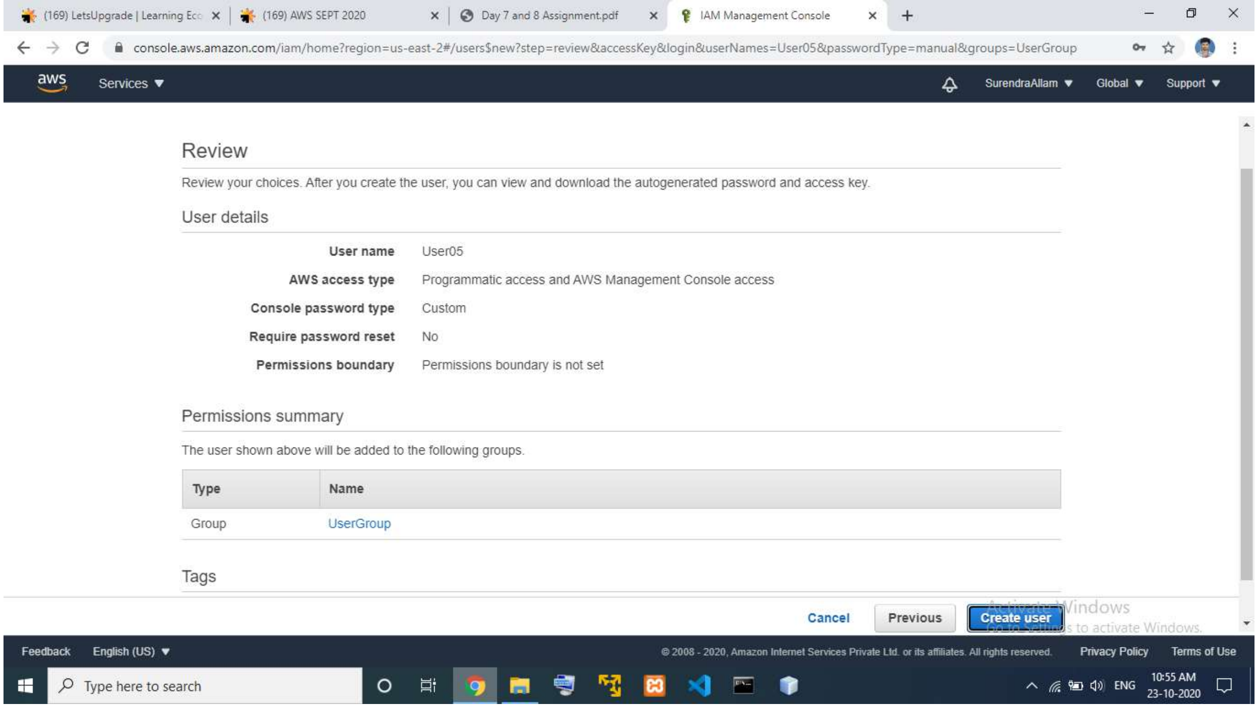
We encountered the following errors while processing your request:

- User: arn:aws:iam::573310877256:user/User04 is not authorized to perform: iam:GetAccountSummary on resource: *
- User: arn:aws:iam::573310877256:user/User04 is not authorized to perform: iam:ListAccountAliases on resource: *

Best practices

- Grant least privilege access: Establishing a principle of least privilege ensures that identities are only permitted to perform the most minimal set of functions necessary to fulfill a specific task, while balancing usability and efficiency.
- Enable Identity federation: Centrally manage users and access across multiple applications and services. For federation to multiple accounts in your AWS Organization, you can configure your identity source in AWS Single Sign-on.
- Enable MFA: For extra security, we recommend that you require multi-factor authentication (MFA) for all users.
- Rotate credentials regularly: Change your own passwords and access keys regularly, and make sure that all users in your account do as well.
- Enable IAM Access Analyzer: Enable IAM Access Analyzer to analyze public, cross-account, and

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


(169) LetsUpgrade | Learning Eco
(169) AWS SEPT 2020
Day 7 and 8 Assignment.pdf
IAM Management Console
console.aws.amazon.com/iam/home?region=us-east-2#/users$new?step=review&accessKey&login&userNames=User05&passwordType=manual&groups=UserGroup
aws
Services
SurendraAllam
Global
Support
Cancel
Previous
Create user
Activate Windows
Go to Settings to activate Windows.
Feedback
English (US)
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
ENG
10:55 AM
23-10-2020

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	User05
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

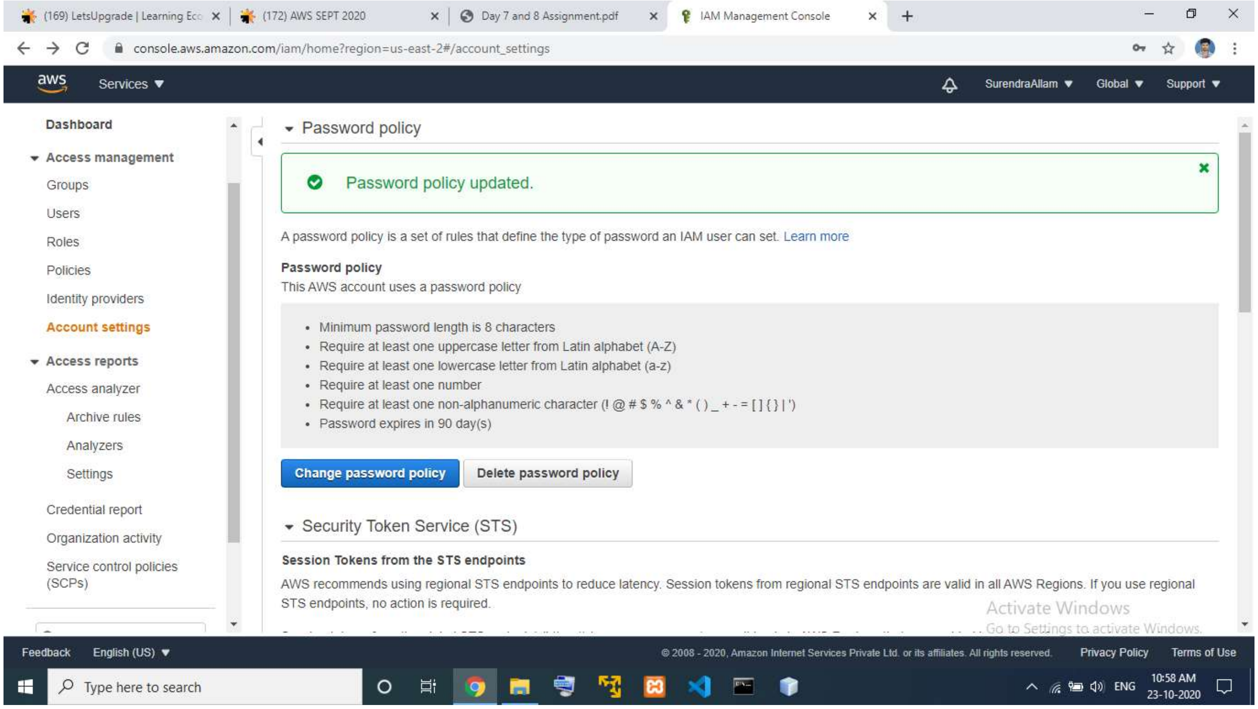
The user shown above will be added to the following groups.

Type	Name
Group	UserGroup

Tags

Task8: setting a password policy

Ss9: password policy screen



Password policy

Password policy updated.

A password policy is a set of rules that define the type of password an IAM user can set. Learn more

Password policy

This AWS account uses a password policy

- Minimum password length is 8 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 (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')
- Password expires in 90 day(s)

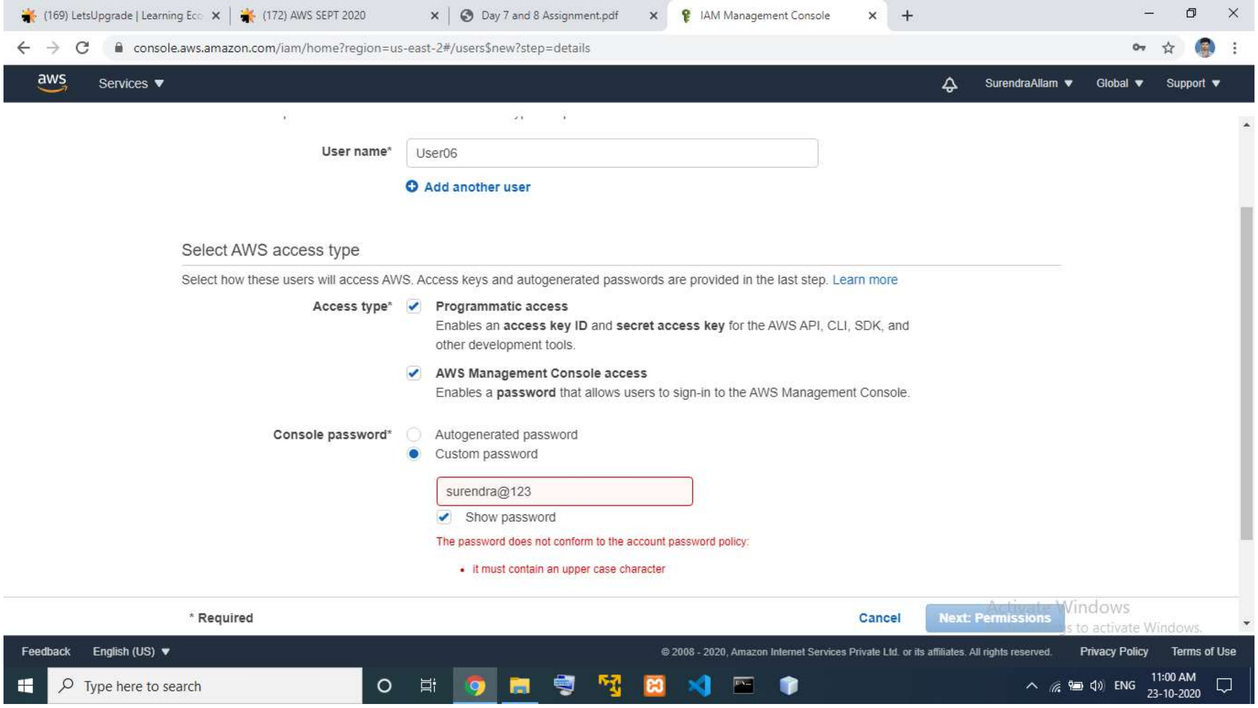
Change password policy | Delete password policy

Security Token Service (STS)

Session Tokens from the STS endpoints

AWS recommends using regional STS endpoints to reduce latency. Session tokens from regional STS endpoints are valid in all AWS Regions. If you use regional STS endpoints, no action is required.

Ss10: login as the user and show password incompatibility error


(169) LetsUpgrade | Learning Eco
(172) AWS SEPT 2020
Day 7 and 8 Assignment.pdf
IAM Management Console
console.aws.amazon.com/iam/home?region=us-east-2#/users$new?step=details
aws
Services
SurendraAllam
Global
Support
Feedback
English (US)
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
ENG
11:00 AM
23-10-2020

User name* User06

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

surendra@123

☑ Show password

The password does not conform to the account password policy:

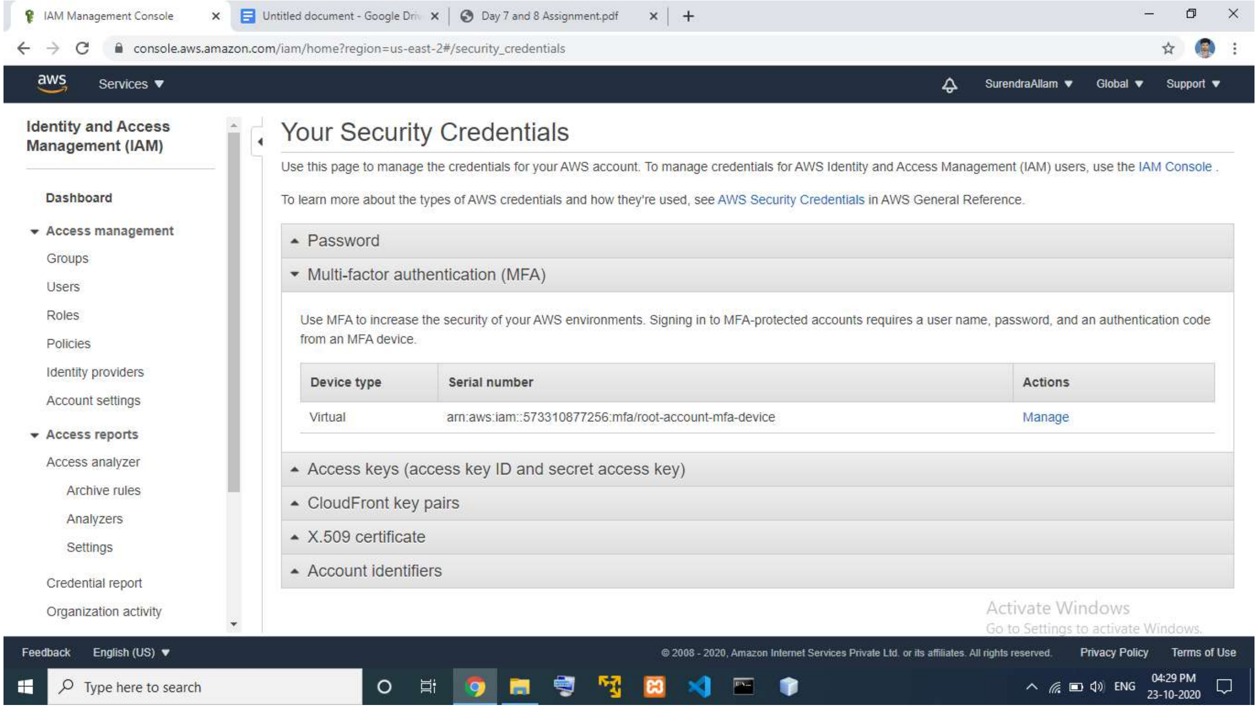
- it must contain an upper case character

* 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::573310877256:mfa/root-account-mfa-device	Manage

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

▲ CloudFront key pairs

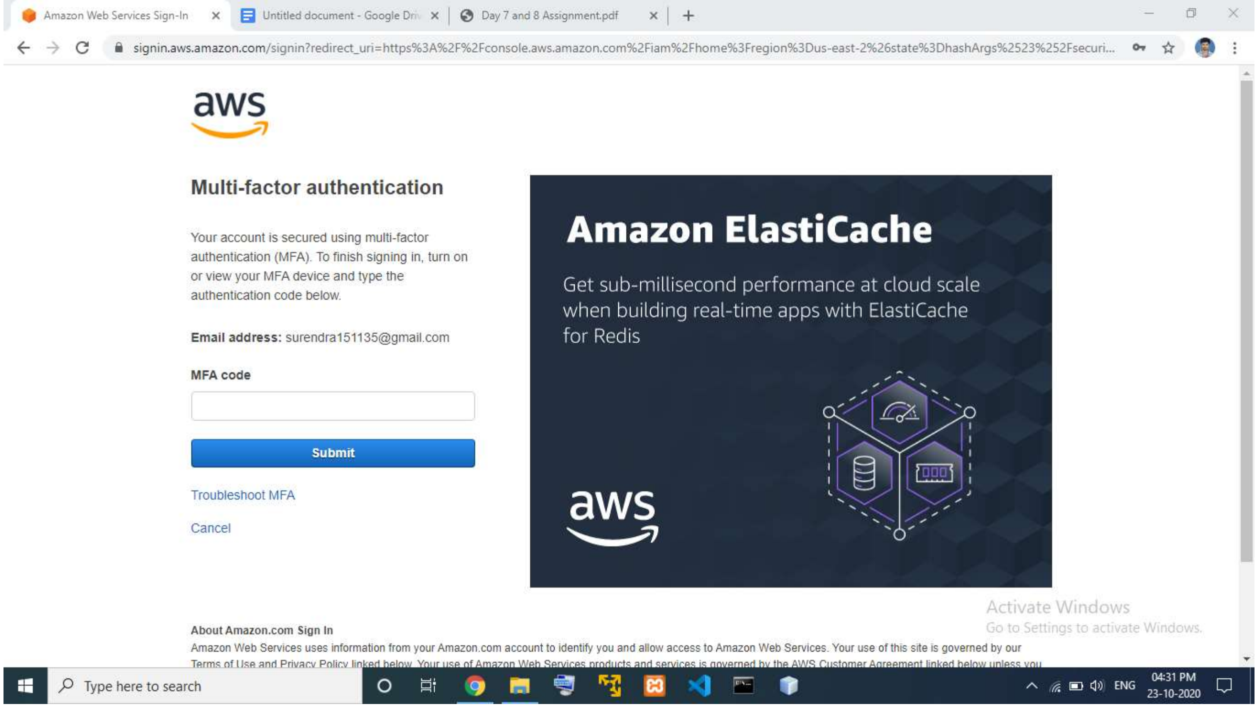
▲ X.509 certificate

▲ Account identifiers

Activate Windows
Go to Settings to activate Windows.

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Ss12: login screen for MFA



Amazon Web Services Sign-In
Untitled document - Google Driv
Day 7 and 8 Assignment.pdf
signin.aws.amazon.com/signin?redirect_uri=https%3A%2F%2Fconsole.aws.amazon.com%2Fiam%2Fhome%3Fregion%3Dus-east-2%26state%3DhashArgs%2523%252Fsecuri...
aws
Amazon ElastiCache
Get sub-millisecond performance at cloud scale when building real-time apps with ElastiCache for Redis
aws
Type here to search
ENG
04:31 PM
23-10-2020

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: surendra151135@gmail.com

MFA code

Submit

Troubleshoot MFA

Cancel

Activate Windows
Go to Settings to activate Windows.

About Amazon.com Sign In

Amazon Web Services uses information from your Amazon.com account to identify you and allow access to Amazon Web Services. Your use of this site is governed by our Terms of Use and Privacy Policy linked below. Your use of Amazon Web Services products and services is governed by the AWS Customer Agreement linked below unless you