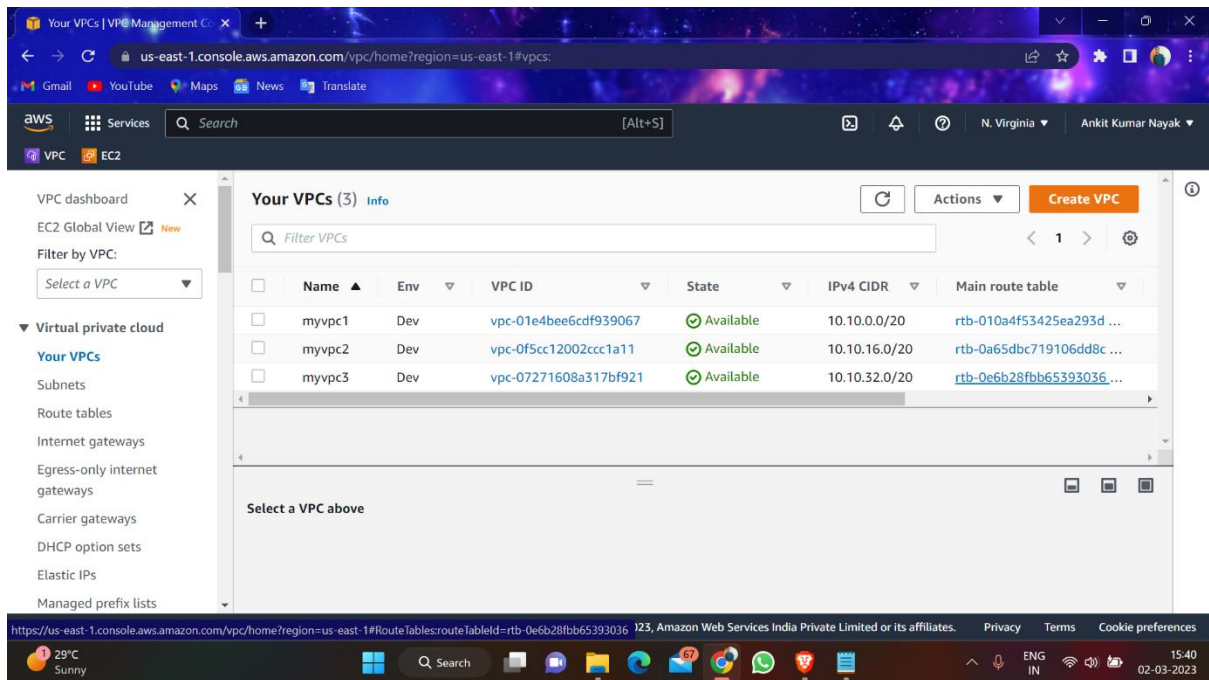
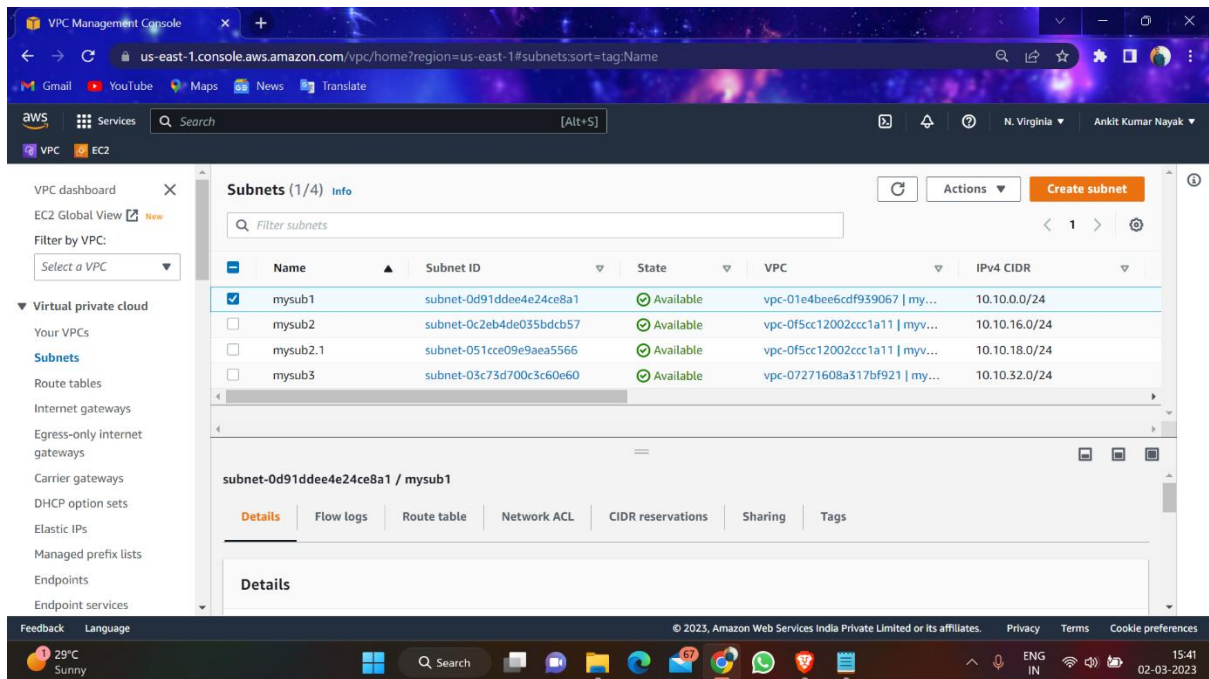


# Transit GW, S3 , IAM role

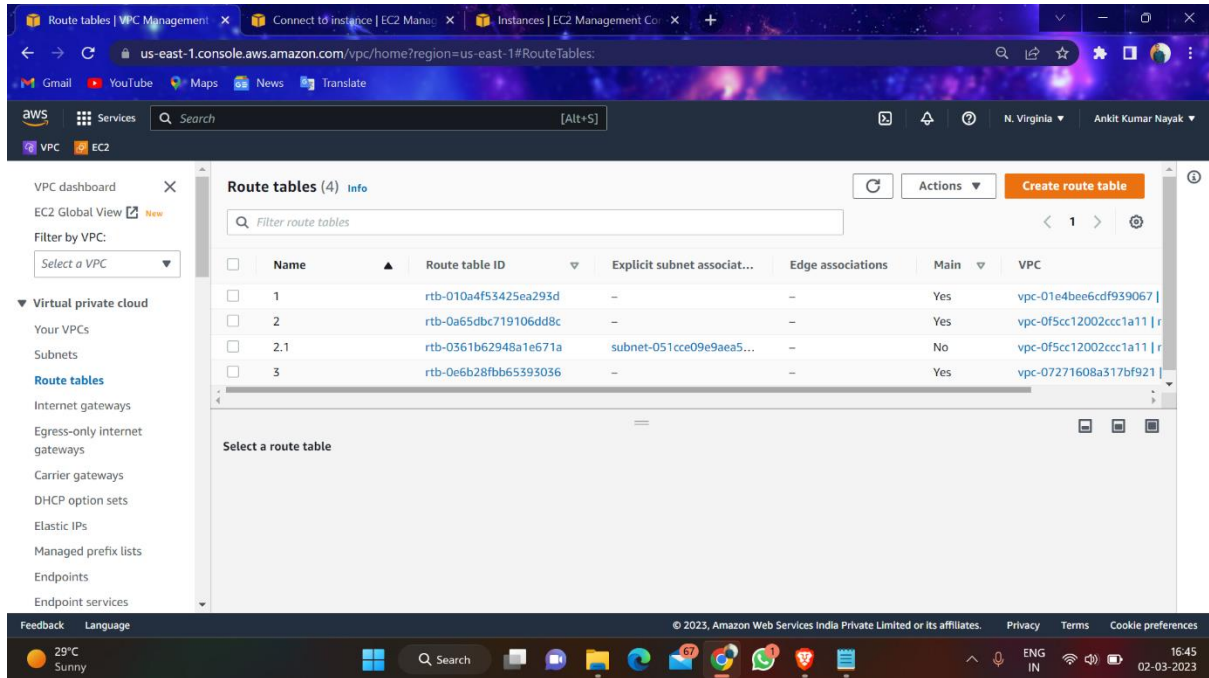
## 1-Creating VPC



## 2-Creating Subnet



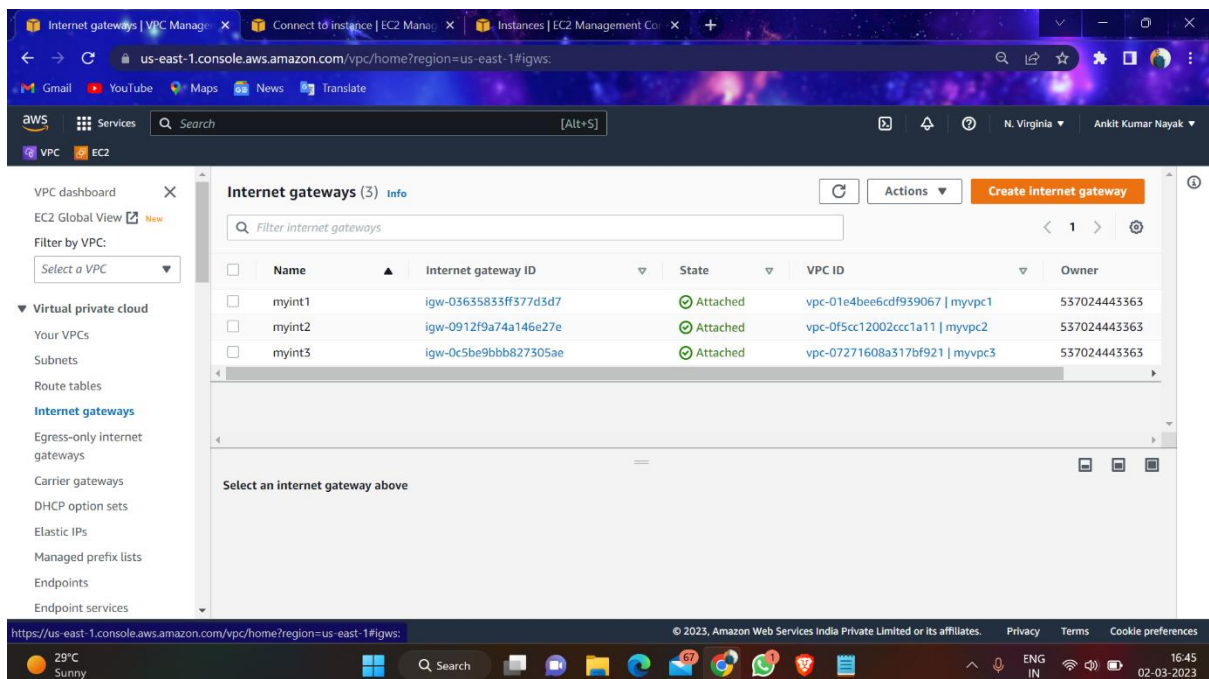
### 3-Creating route tables



The screenshot shows the AWS Management Console for the 'us-east-1' region. The 'Route tables' page is active, displaying a list of four route tables. The table has columns for Name, Route table ID, Explicit subnet associations, Edge associations, Main status, and VPC. The first three route tables are associated with the main VPC, while the fourth is associated with a different VPC.

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
1	rtb-010a4f53425ea293d	-	-	Yes	vpc-01e4bee6cdf939067
2	rtb-0a65dbc719106dd8c	-	-	Yes	vpc-0f5cc12002ccc1a11
2.1	rtb-0361b62948a1e671a	subnet-051cce09e9aea5...	-	No	vpc-0f5cc12002ccc1a11
3	rtb-0e6b28fbb65393036	-	-	Yes	vpc-07271608a317bf921

### 4-Creating Internet gateway and attach to vpc



The screenshot shows the AWS Management Console for the 'us-east-1' region. The 'Internet gateways' page is active, displaying a list of three internet gateways. The table has columns for Name, Internet gateway ID, State, VPC ID, and Owner. All three internet gateways are in the 'Attached' state.

Name	Internet gateway ID	State	VPC ID	Owner
myint1	igw-03635833ff377d3d7	Attached	vpc-01e4bee6cdf939067   myvpc1	537024443363
myint2	igw-0912f9a74a146e27e	Attached	vpc-0f5cc12002ccc1a11   myvpc2	537024443363
myint3	igw-0c5be9bbb827305ae	Attached	vpc-07271608a317bf921   myvpc3	537024443363

## 5-Creating transit gateways

The screenshot shows the AWS Management Console for the 'us-east-1' region. The 'Transit gateways' page is active, displaying a list of transit gateways. The table below shows the details of the 'newtrans' transit gateway.

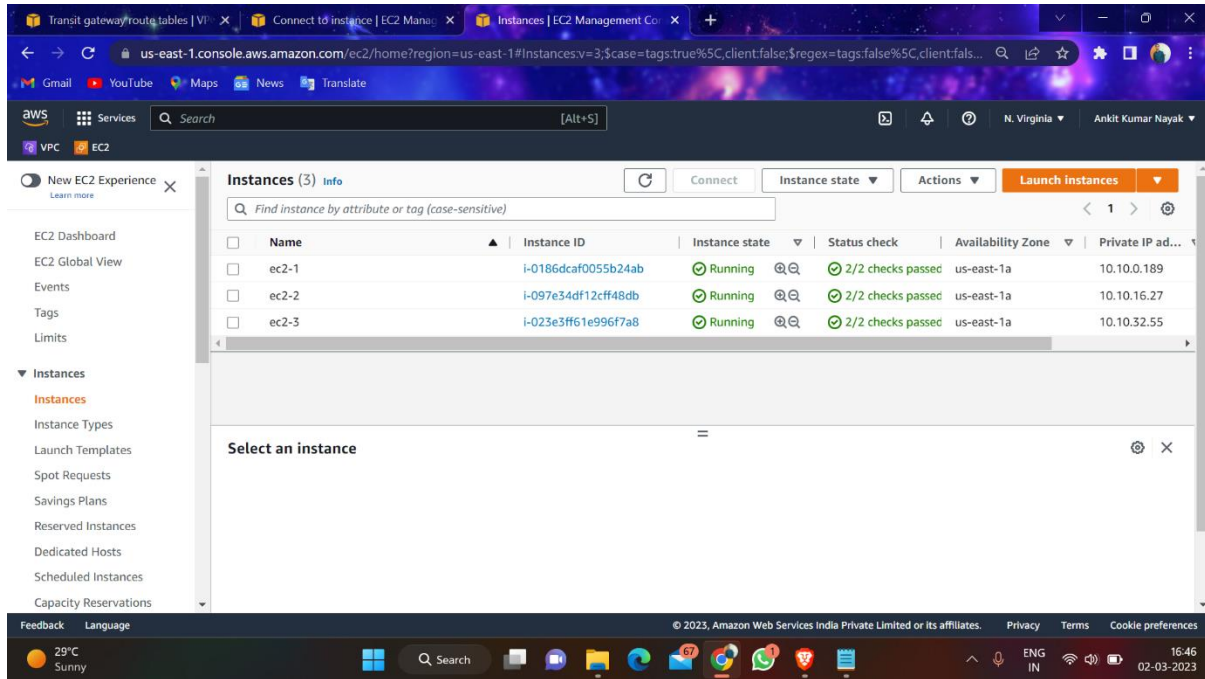
Name	Transit gateway ID	Owner ID	State
newtrans	tgw-0fb2a115d1f54eb4b	537024443363	Available

## 6-Creating transit gateway attachment

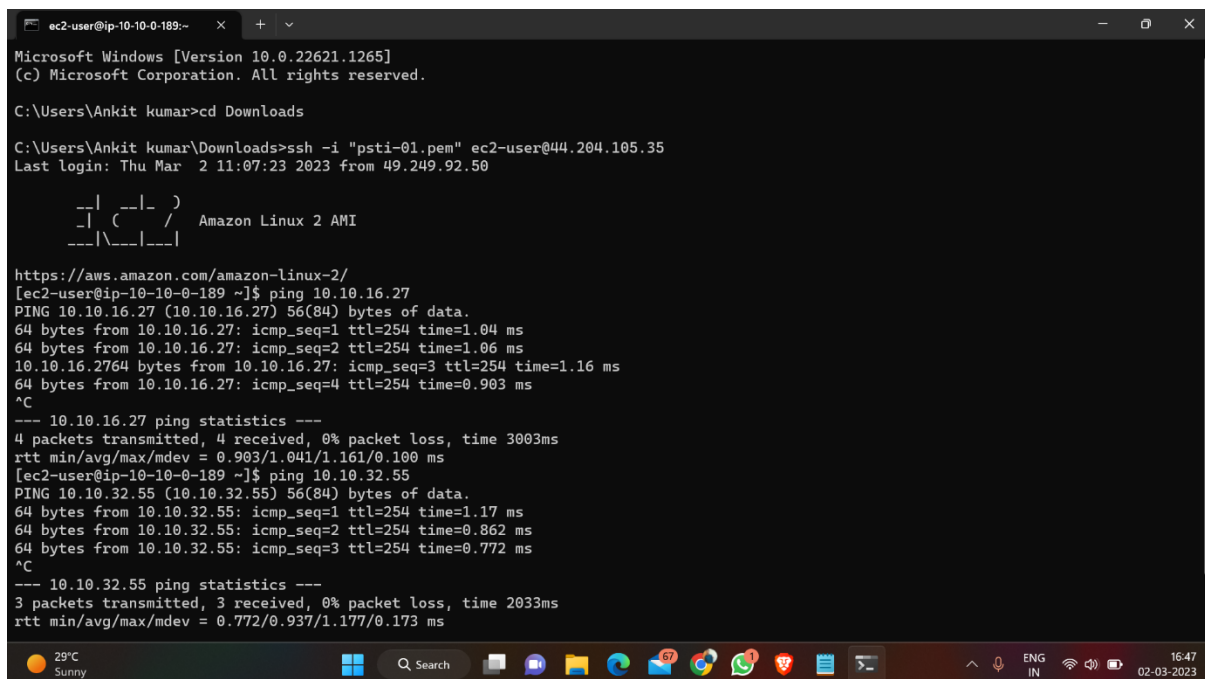
The screenshot shows the AWS Management Console for the 'us-east-1' region. The 'Transit gateway attachments' page is active, displaying a list of transit gateway attachments. The table below shows the details of the three attachments.

Name	Transit gateway attachment ID	Transit gateway ID	Resource type	Resource ID
newtrans1	tgw-attach-017d437c5d4fa3011	tgw-0fb2a115d1f54eb4b	VPC	vpc-01e4bee6cdf939067
newtrans2	tgw-attach-0dbe6cb5bb4cf0baa	tgw-0fb2a115d1f54eb4b	VPC	vpc-0f5cc12002ccc1a11
newtrans3	tgw-attach-089cef0cea5fbd715	tgw-0fb2a115d1f54eb4b	VPC	vpc-07271608a317bf921

# 7-Creating Instance

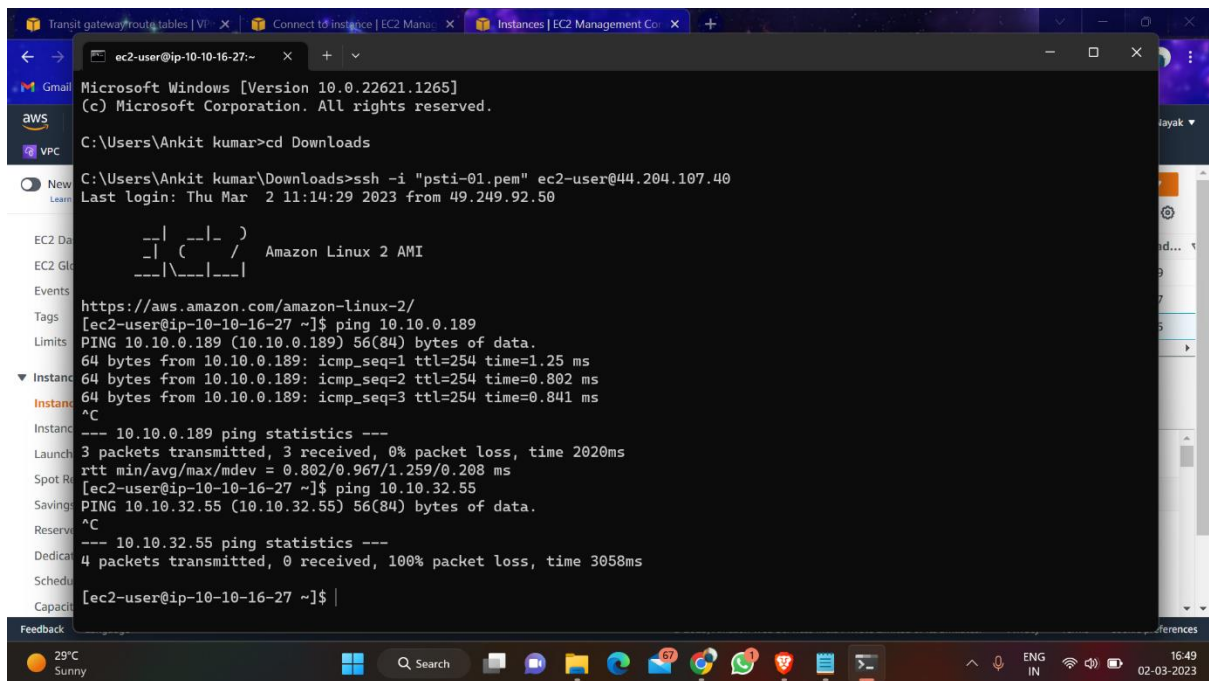


8- Machine 1 should ping with machine 2,  
and machine 1 should ping with machine 3  
Machine 1—Machine 2





## Machine 1—Machine 3



The screenshot shows a Windows terminal window with the following content:

```
Transit gateway/route tables | VI... x Connect to instance | EC2 Manu... x Instances | EC2 Management Co... x +
ec2-user@ip-10-10-16-27:~$
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Ankit kumar>cd Downloads

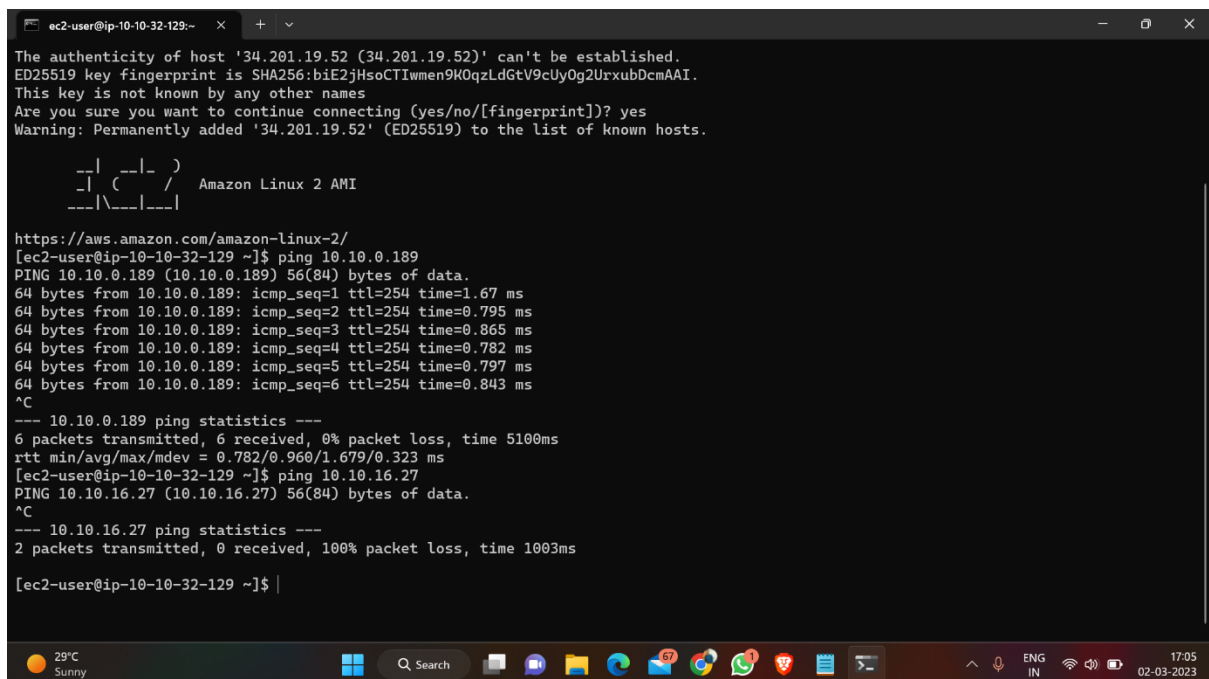
C:\Users\Ankit kumar\Downloads>ssh -i "psti-01.pem" ec2-user@44.204.107.40
Last login: Thu Mar  2 11:14:29 2023 from 49.249.92.50

  _ _ | _ _ | _ )
  _ | ( _ _ | /   Amazon Linux 2 AMI
  _ _ | _ _ | _ _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-10-16-27 ~]$ ping 10.10.0.189
PING 10.10.0.189 (10.10.0.189) 56(84) bytes of data.
64 bytes from 10.10.0.189: icmp_seq=1 ttl=254 time=1.25 ms
64 bytes from 10.10.0.189: icmp_seq=2 ttl=254 time=0.802 ms
64 bytes from 10.10.0.189: icmp_seq=3 ttl=254 time=0.841 ms
^C
--- 10.10.0.189 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.802/0.967/1.259/0.208 ms
[ec2-user@ip-10-10-16-27 ~]$ ping 10.10.32.55
PING 10.10.32.55 (10.10.32.55) 56(84) bytes of data.
^C
--- 10.10.32.55 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3058ms

[ec2-user@ip-10-10-16-27 ~]$ |
```

## Machine 2—Machine 3 nothing pinging



The screenshot shows a Windows terminal window with the following content:

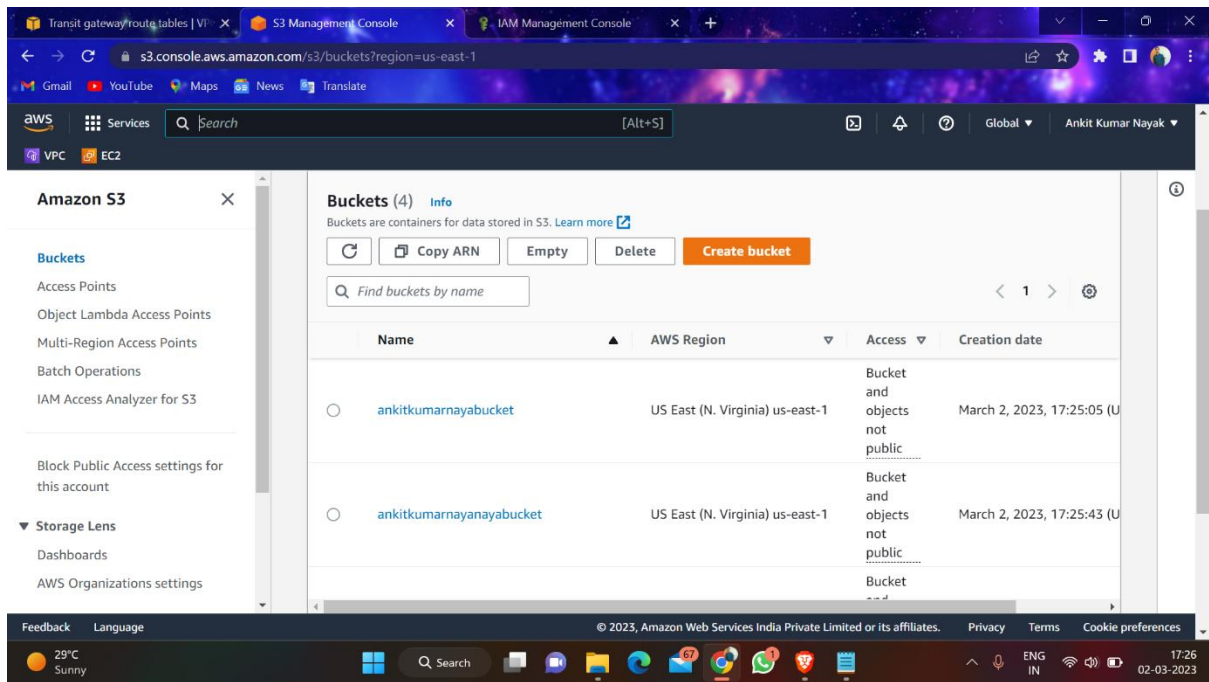
```
ec2-user@ip-10-10-32-129:~$
The authenticity of host '34.201.19.52 (34.201.19.52)' can't be established.
ED25519 key fingerprint is SHA256:biE2jHsoCTIwmn9K0qzLdGtV9cUyOg2UrxubDcmAAI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '34.201.19.52' (ED25519) to the list of known hosts.

  _ _ | _ _ | _ )
  _ | ( _ _ | /   Amazon Linux 2 AMI
  _ _ | _ _ | _ _ |

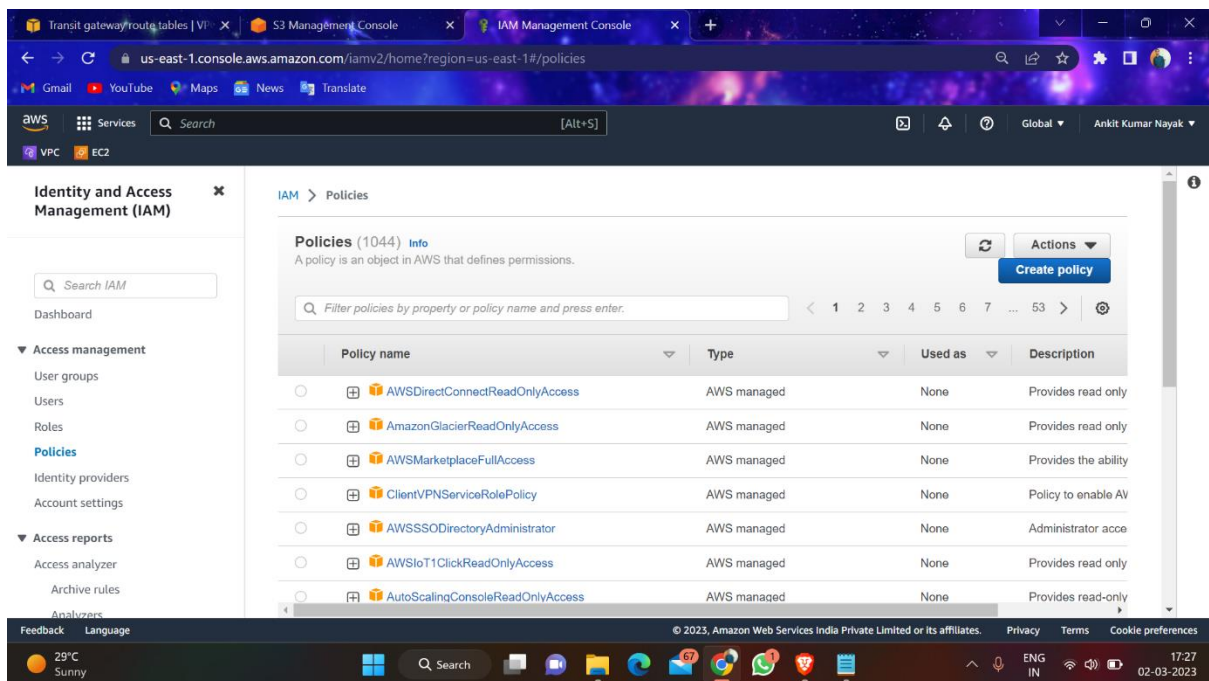
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-10-32-129 ~]$ ping 10.10.0.189
PING 10.10.0.189 (10.10.0.189) 56(84) bytes of data.
64 bytes from 10.10.0.189: icmp_seq=1 ttl=254 time=1.67 ms
64 bytes from 10.10.0.189: icmp_seq=2 ttl=254 time=0.795 ms
64 bytes from 10.10.0.189: icmp_seq=3 ttl=254 time=0.865 ms
64 bytes from 10.10.0.189: icmp_seq=4 ttl=254 time=0.782 ms
64 bytes from 10.10.0.189: icmp_seq=5 ttl=254 time=0.797 ms
64 bytes from 10.10.0.189: icmp_seq=6 ttl=254 time=0.843 ms
^C
--- 10.10.0.189 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5100ms
rtt min/avg/max/mdev = 0.782/0.960/1.679/0.323 ms
[ec2-user@ip-10-10-32-129 ~]$ ping 10.10.16.27
PING 10.10.16.27 (10.10.16.27) 56(84) bytes of data.
^C
--- 10.10.16.27 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1003ms

[ec2-user@ip-10-10-32-129 ~]$ |
```

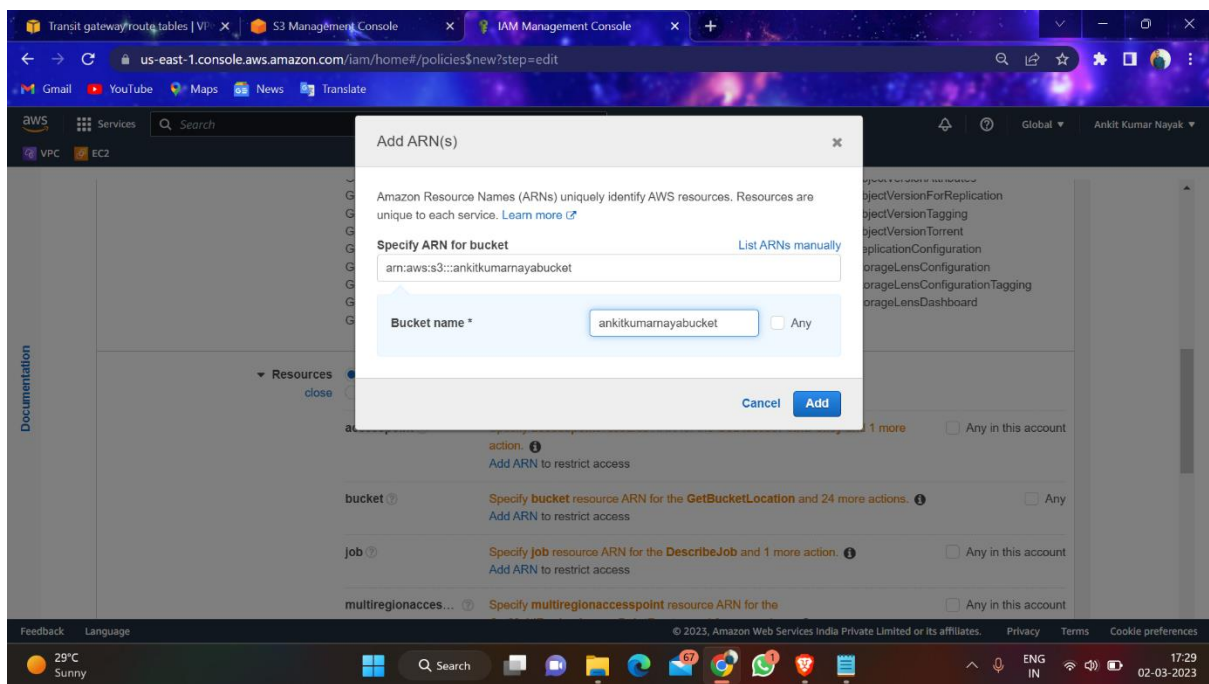
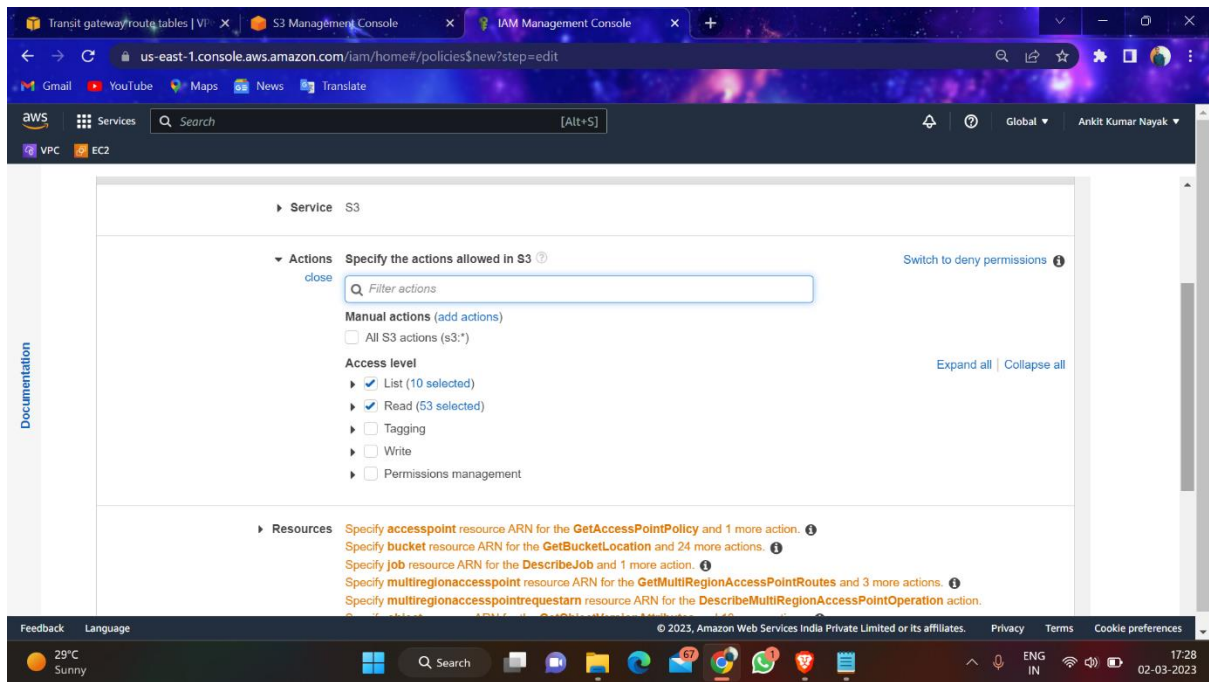
## 9- Create Buckets in same region



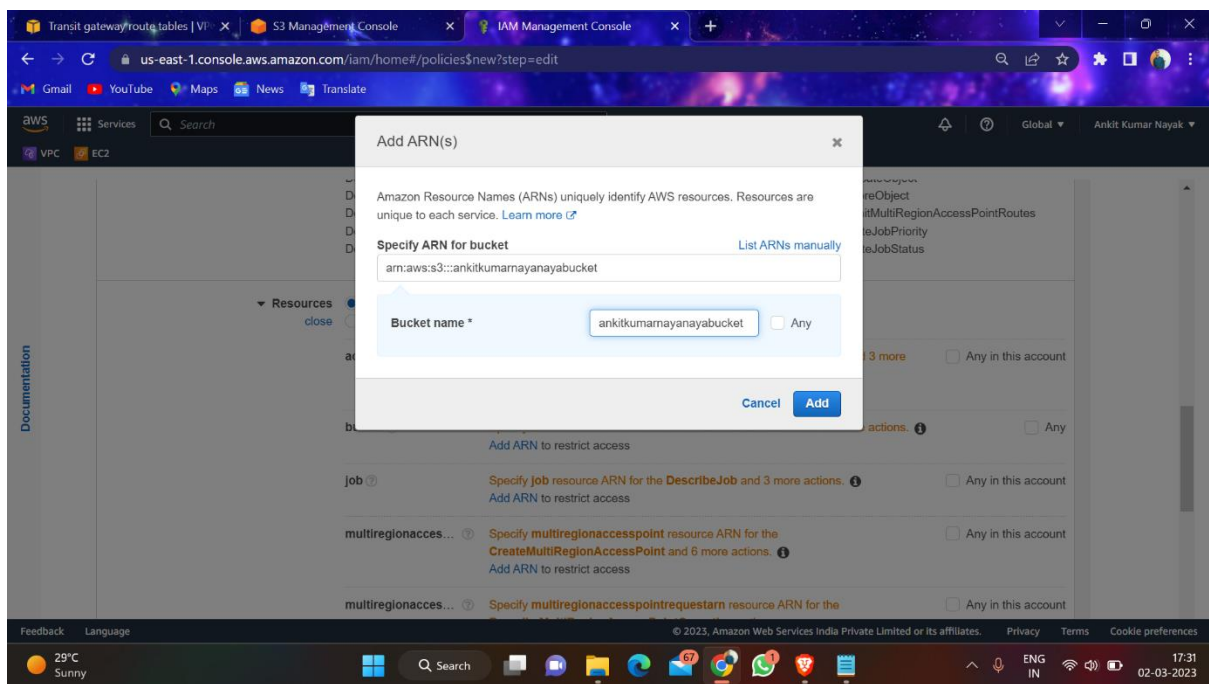
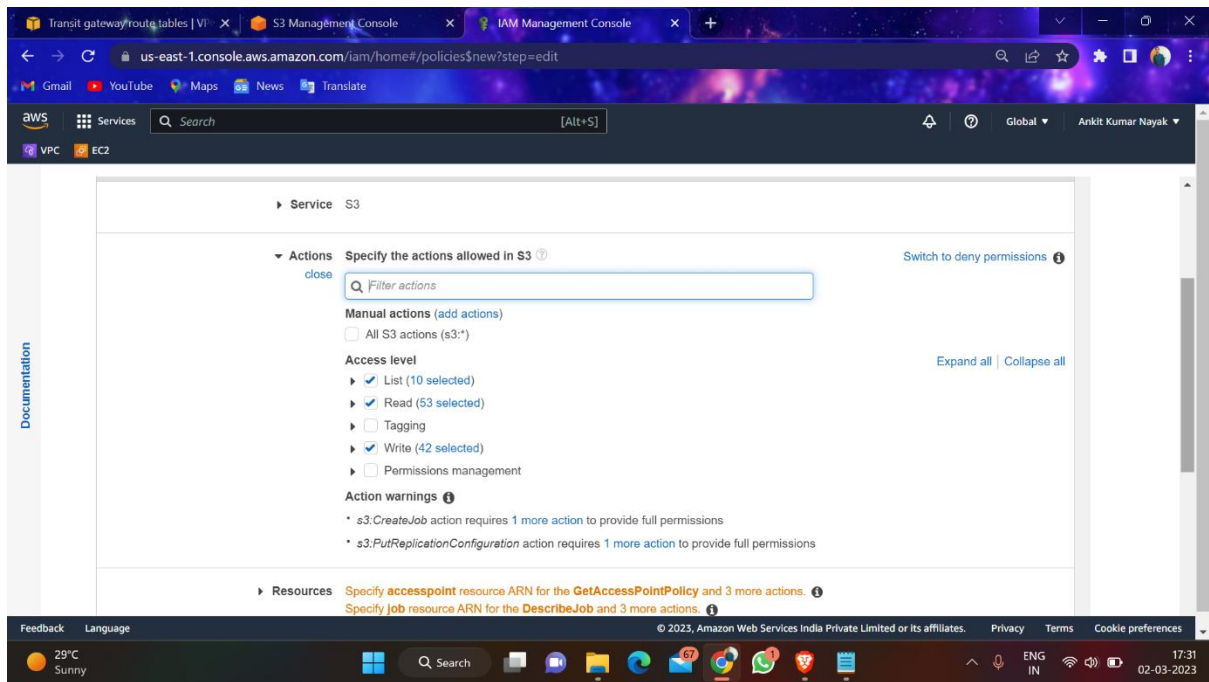
## 10- Create 2 policies with 2 buckets



\*read only policies



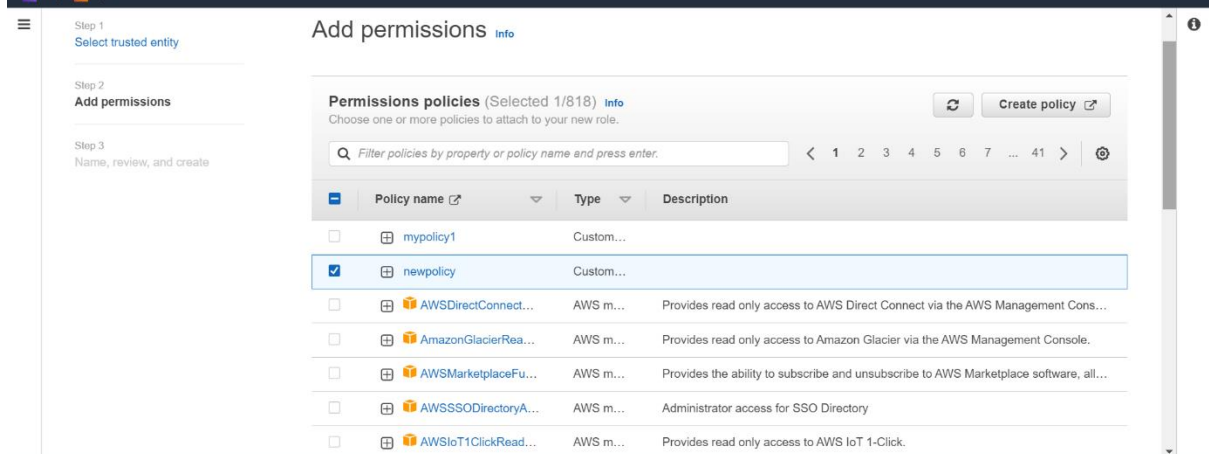
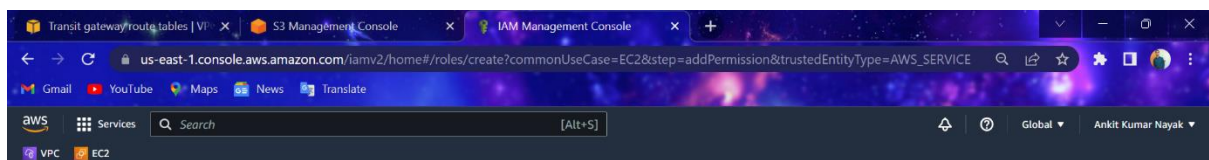
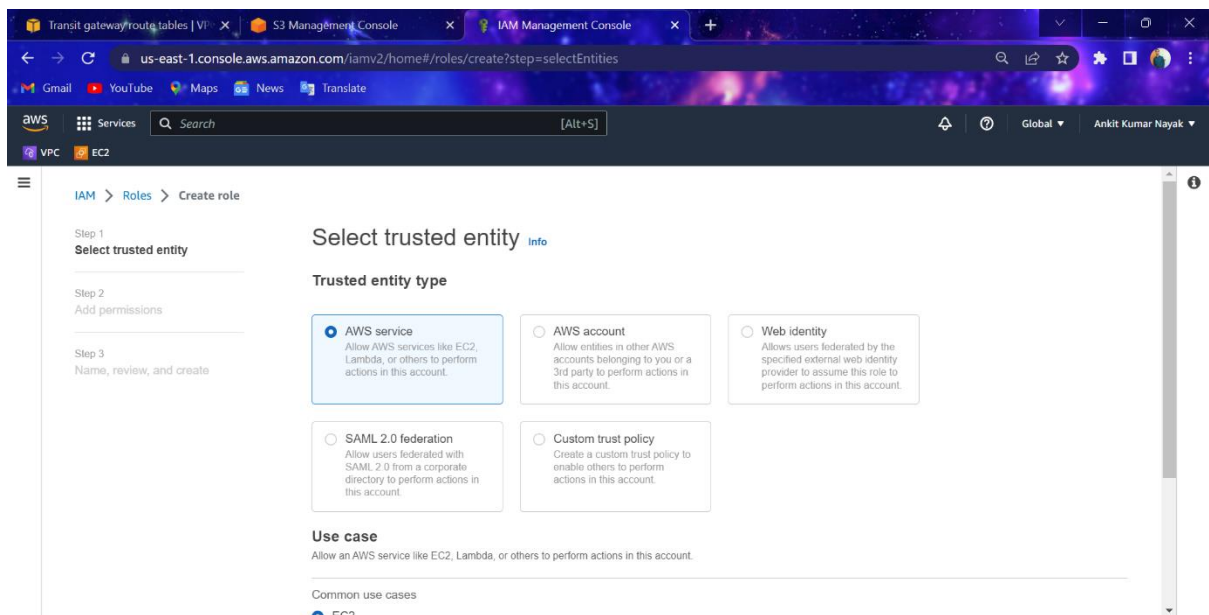
# \*read and write policies





# 11- Create 2 roles in IAM

For 1<sup>st</sup> bucket



For 2<sup>nd</sup> bucket

This screenshot shows the 'Select trusted entity' step in the AWS IAM console. The left sidebar indicates the current step is 'Step 1: Select trusted entity'. The main area is titled 'Select trusted entity' and 'Trusted entity type'. There are five radio button options: 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. Below these is a 'Use case' section with a text input field and a 'Common use cases' section with a dropdown menu showing 'EC2'. The bottom of the screen shows a Windows taskbar with various application icons and a system tray with the date and time.

Transit gateway/route tables | VI | X S3 Management Console X IAM Management Console X +

us-east-1.console.aws.amazon.com/iamv2/home#/roles/create?step=selectEntities

Gmail YouTube Maps News Translate

aws Services Search [Alt+S]

VPC EC2

Feedback Language

29°C Sunny

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

17:33 02-03-2023

This screenshot shows the 'Add permissions' step in the AWS IAM console. The left sidebar indicates the current step is 'Step 2: Add permissions'. The main area is titled 'Add permissions' and 'Permissions policies (Selected 1/818)'. There is a search bar and a table of policies. The table has columns for 'Policy name', 'Type', and 'Description'. The first policy, 'mypolicy1', is selected. The bottom of the screen shows a Windows taskbar with various application icons and a system tray with the date and time.

Transit gateway/route tables | VI | X S3 Management Console X IAM Management Console X +

us-east-1.console.aws.amazon.com/iamv2/home#/roles/create?commonUseCase=EC2&step=addPermission&trustedEntityType=AWS\_SERVICE

Gmail YouTube Maps News Translate

aws Services Search [Alt+S]

VPC EC2

Feedback Language

29°C Sunny

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

17:35 02-03-2023

12- When u try to logging into 1<sup>st</sup> machine and try to read the bucket we are able to but if we want to copy any file into it it will show error

1-To list the item in buckets

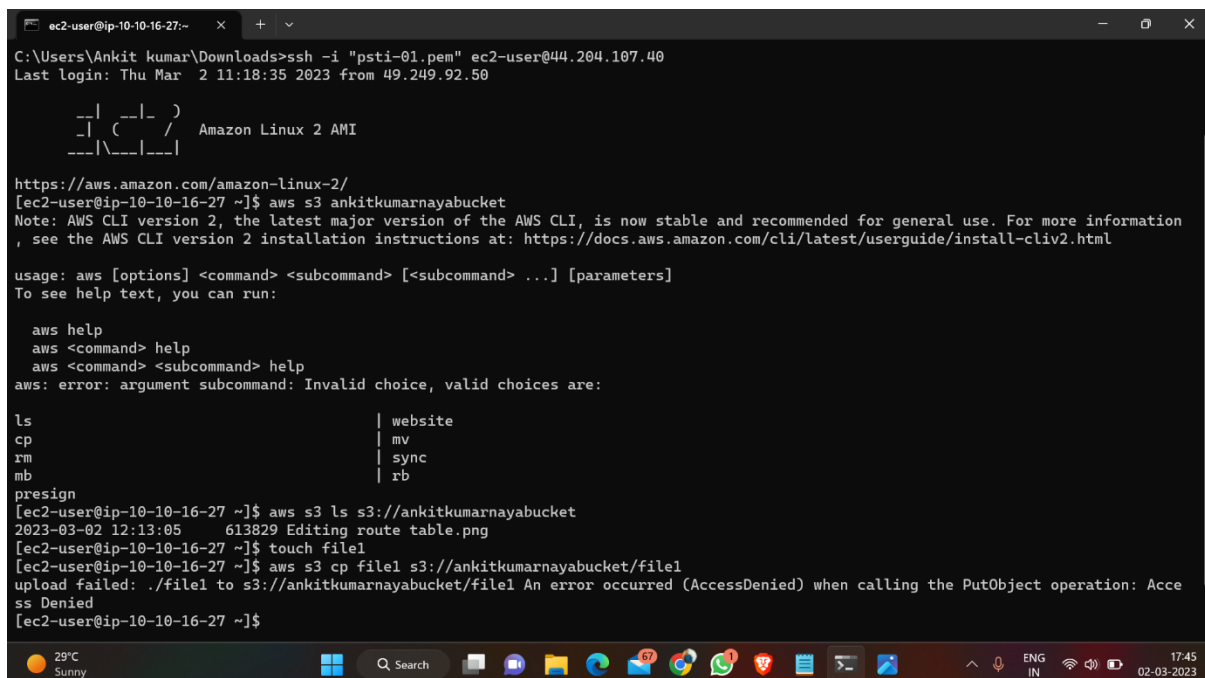
Aws s3 ls s3://bucketname

2-To create a file

Touch file1

3-To copy the file into bucket

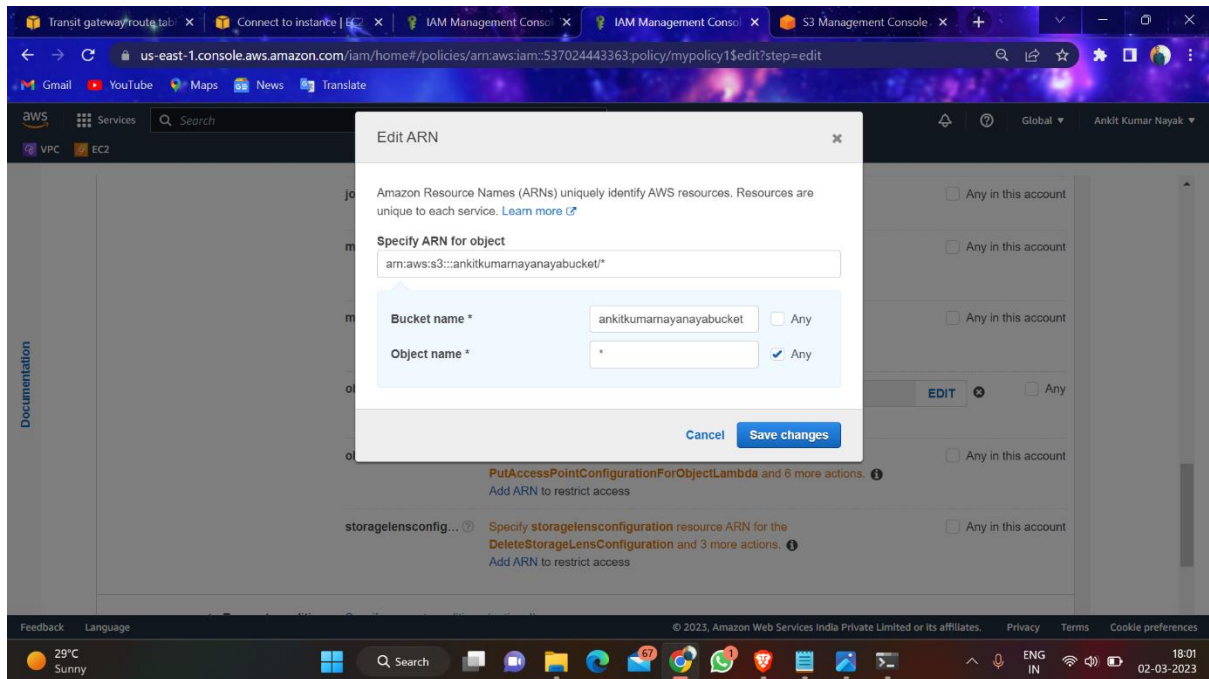
Aws s3 cp s3://bucketname/file1



```
ec2-user@ip-10-10-16-27:~  
C:\Users\Ankit kumar\Downloads>ssh -i "psti-01.pem" ec2-user@44.204.107.40  
Last login: Thu Mar  2 11:18:35 2023 from 49.249.92.50  
  
  _ _ | _ _ | _ )  
 _ | ( _ /  
 _ _ | _ _ | _ _ |  
Amazon Linux 2 AMI  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-10-16-27 ~]$ aws s3 ankitkumarnayabucket  
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information  
, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html  
  
usage: aws [options] <command> [<subcommand> [<subcommand> ...] [parameters]]  
To see help text, you can run:  
  
aws help  
aws <command> help  
aws <command> <subcommand> help  
aws: error: argument subcommand: Invalid choice, valid choices are:  
  
ls | website  
cp | mv  
rm | sync  
mb | rb  
presign  
[ec2-user@ip-10-10-16-27 ~]$ aws s3 ls s3://ankitkumarnayabucket  
2023-03-02 12:13:05 613829 Editing route table.png  
[ec2-user@ip-10-10-16-27 ~]$ touch file1  
[ec2-user@ip-10-10-16-27 ~]$ aws s3 cp file1 s3://ankitkumarnayabucket/file1  
upload failed: ./file1 to s3://ankitkumarnayabucket/file1 An error occurred (AccessDenied) when calling the PutObject operation: Access Denied  
[ec2-user@ip-10-10-16-27 ~]$
```

## 13- Goto your polices and edit polices

Resource→object, add your 2<sup>nd</sup> bucket name and give object as any.



14- When u try to logging into 2<sup>nd</sup> machine and try to read the bucket we are able to and if we want to copy any file into it it will copy and list it

1-To list the item in buckets

Aws s3 ls s3://bucketname

2-To create a file

Touch file1

3-To copy the file into bucket

Aws s3 cp s3://bucketname/file1



```
ec2-user@ip-10-10-32-129:~$ ssh -i "psti-01.pem" ec2-user@34.201.19.52
Last login: Thu Mar  2 12:16:49 2023 from 49.249.92.50

  __|  __|_  )
 _| (  /  Amazon Linux 2 AMI
---|\\_____|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-10-32-129 ~]$ touch file1
[ec2-user@ip-10-10-32-129 ~]$ aws s3 cp file1 s3://ankitkumarnayanayabucket/file1
upload: ./file1 to s3://ankitkumarnayanayabucket/file1
[ec2-user@ip-10-10-32-129 ~]$ aws s3 ls file1 s3://ankitkumarnayanayabucket

Unknown options: s3://ankitkumarnayanayabucket
[ec2-user@ip-10-10-32-129 ~]$ aws s3 ls s3://ankitkumarnayanayabucket
2023-03-02 12:16:07      696076 EC2 instance.png
2023-03-02 12:33:18           0 file1
[ec2-user@ip-10-10-32-129 ~]$ |
```

15- Now try to logging into 2<sup>nd</sup> machine and try to access the bucket of 3<sup>rd</sup> machine we will get error

```
ec2-user@ip-10-10-32-129:~$ ssh -i "psti-01.pem" ec2-user@34.201.19.52
Last login: Thu Mar  2 12:32:32 2023 from 49.249.92.50

  __|  __|_  )
 _| (  /  Amazon Linux 2 AMI
---|\\_____|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-10-32-129 ~]$ touch file4
[ec2-user@ip-10-10-32-129 ~]$ aws s3 cp file4 s3://ankitkumarnayanayabucket/file4
upload failed: ./file4 to s3://ankitkumarnayanayabucket/file4 An error occurred (AccessDenied) when calling the PutObject operation: Access Denied
[ec2-user@ip-10-10-32-129 ~]$
```

