HACKATHON-2K24

Team

CONQUERORS

Project Title :

Multi Region Bucket Accessing Using Peering Connections

Submitted by :

A. Kalyan - 21W91A0402

I. Rachana – 21W91A0441

A. Ashok Reddy – 21W91A0406

D. Sai Venkata Sai – 21W91A0426

E. John Mosses – 22W95A0405

Under the Esteemed Guidance of

Mr. AASHU DEV

AWS Academy Accreditation

AWS Academy Educator

AWS Solution Architect 2X Certified

AWS Re-Start Accreditation

TSS – Tech Sign Solutions

ABSTRACT

This project presents a robust and efficient method for accessing S3 buckets across multiple regions using Amazon Web Services (AWS). The architecture leverages key AWS services such as Multi-Region Access Points, AWS PrivateLink, VPC Peering, and S3 Cross-Region Replication (CRR). The Multi-Region Access Points route Amazon S3 data request traffic from multiple sources without the need for complex networking configurations. AWS PrivateLink provides a private connection for routing S3 requests into AWS or across multiple AWS Regions. VPC Peering is used to connect separate VPCs in different regions. S3 CRR is used to synchronize data among buckets in those Regions. The proposed architecture allows for the building of multi-region applications with the same architecture that's used in a single Region, and then run those applications anywhere in the world. This setup provides built-in network resilience with acceleration of internet-based requests to Amazon S3, thereby improving data availability and redundancy.

INTRODUCTION

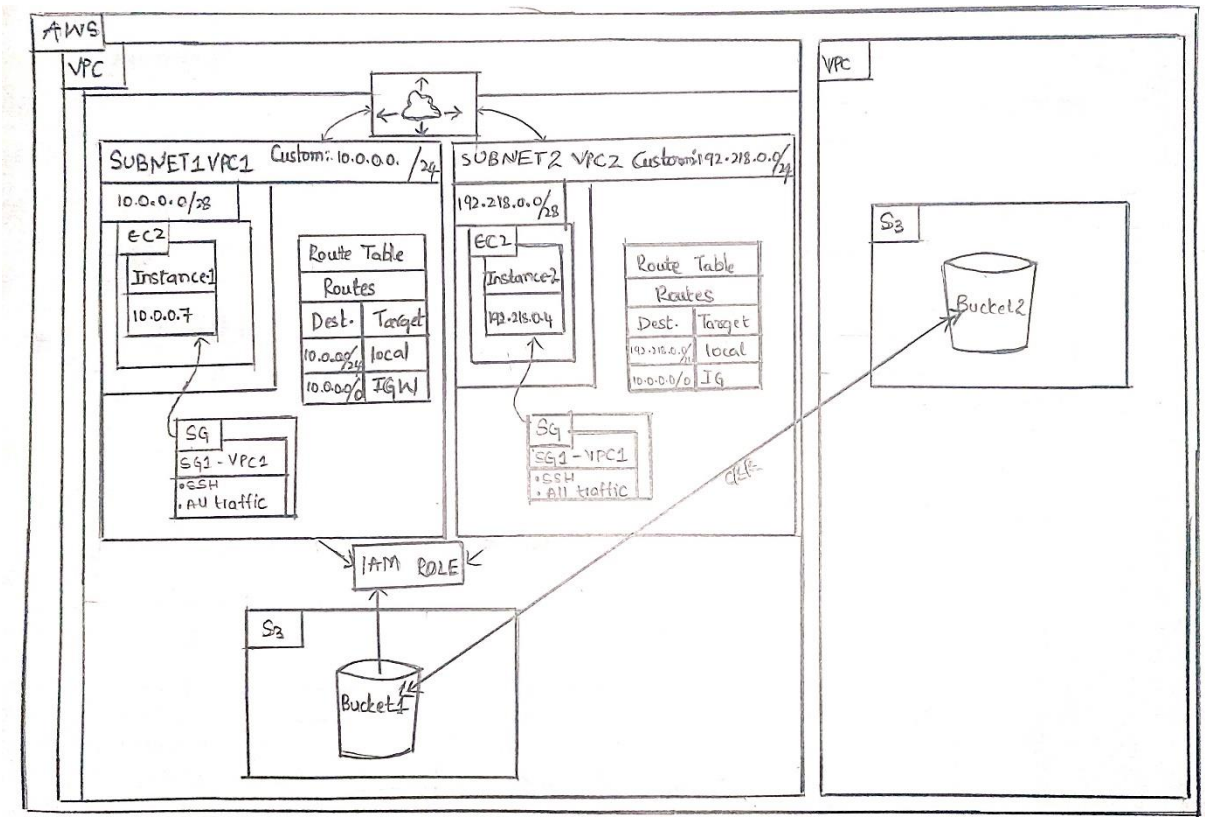
In the era of cloud computing, data accessibility and redundancy are of paramount importance. This project, titled “Multi-Region Bucket Accessing using Peering Connections in AWS”, aims to address these needs by leveraging the power and flexibility of Amazon Web Services (AWS).

The project focuses on the implementation of a robust system that allows for efficient access to S3 buckets across multiple regions. This is achieved through the use of several key AWS services, including Multi-Region Access Points, AWS PrivateLink, VPC Peering, and S3 Cross-Region Replication (CRR).

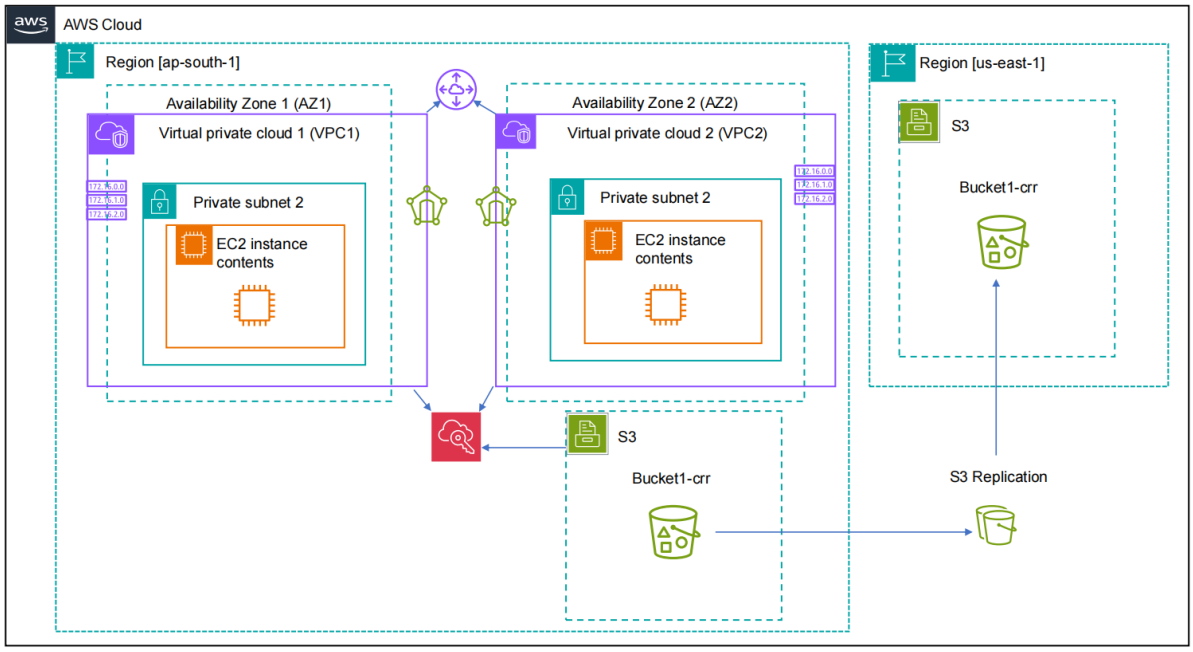
The architecture designed in this project not only ensures high availability and redundancy of data but also provides a resilient network with accelerated internet-based requests to Amazon S3. This system allows for the development and deployment of multi-region applications with the same architecture used in a single region, thereby offering a scalable and efficient solution for global data accessibility.

Stay tuned as we delve deeper into the intricacies of this project, exploring each component in detail and understanding how they all come together to form a comprehensive solution for multi-region data access in AWS.

Rough Architecture of Aws

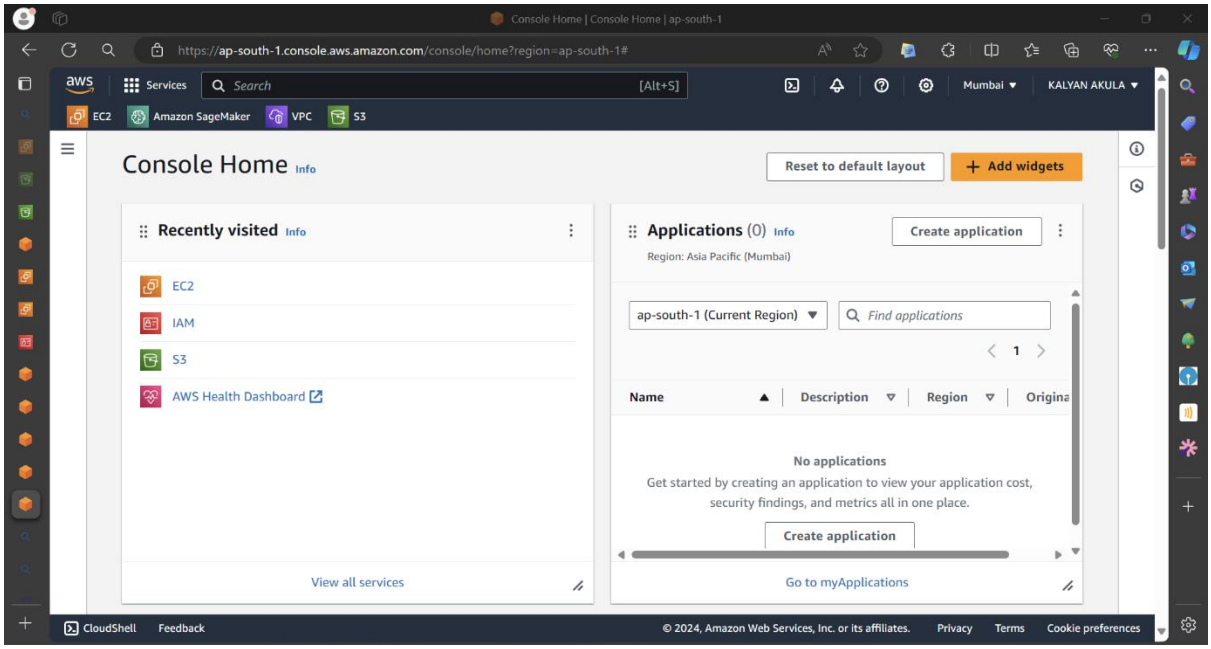


Real Time Architecture of AWS

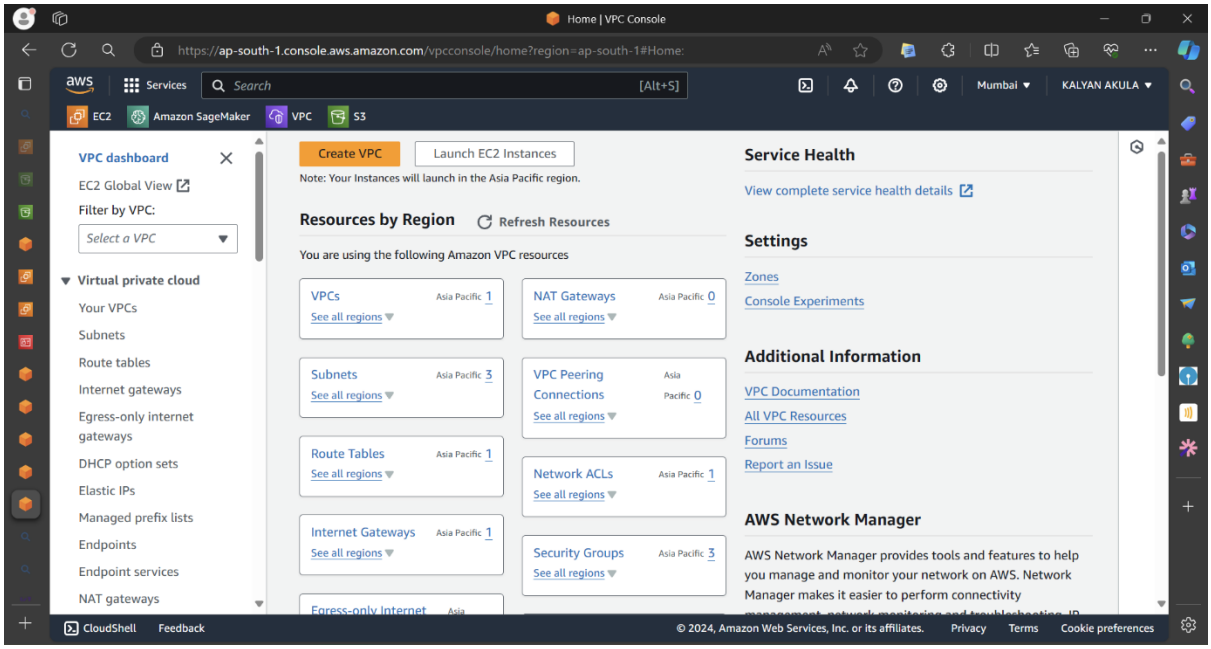


Creating 2 VPC’s in Mumbai region

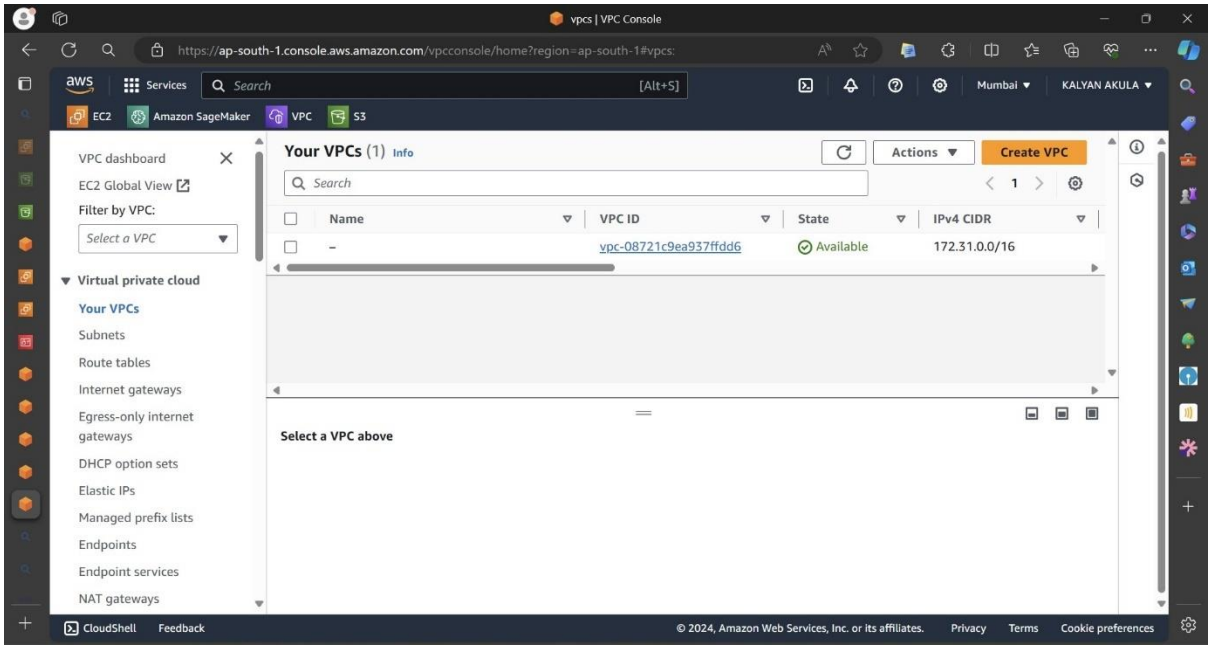
Step1 : open AWS



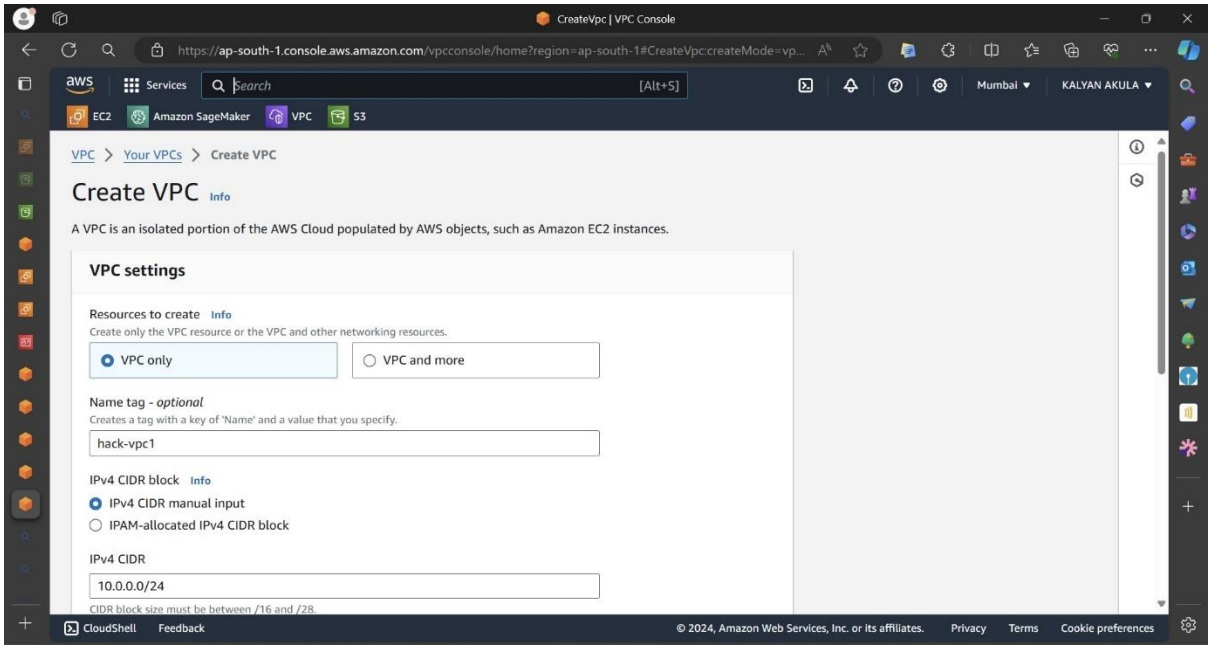
Step2 : Open VPC

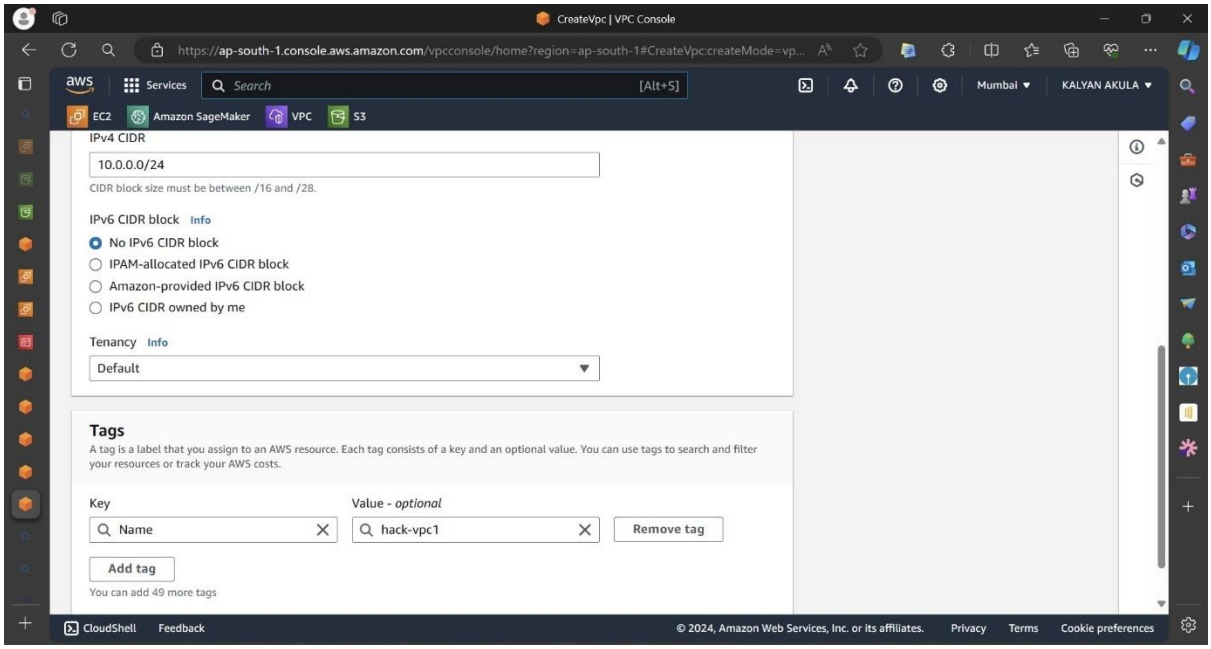


Step3 : Click on VPC & ‘Create VPC’

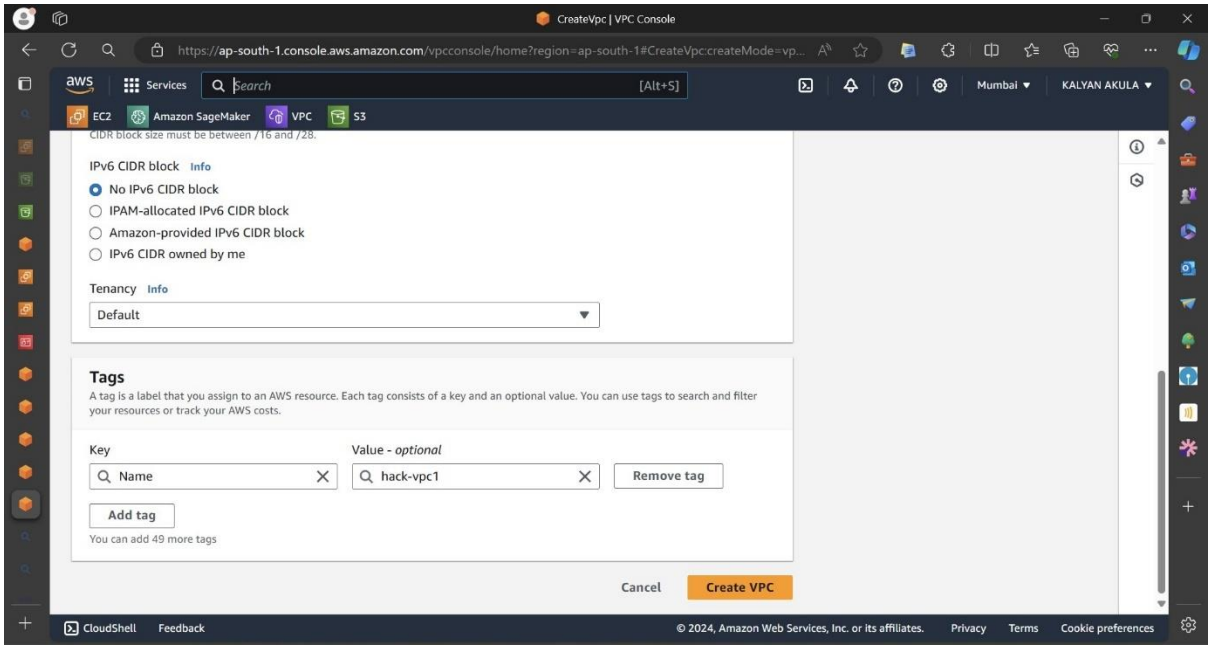


Step 4 : Enter the details as follows

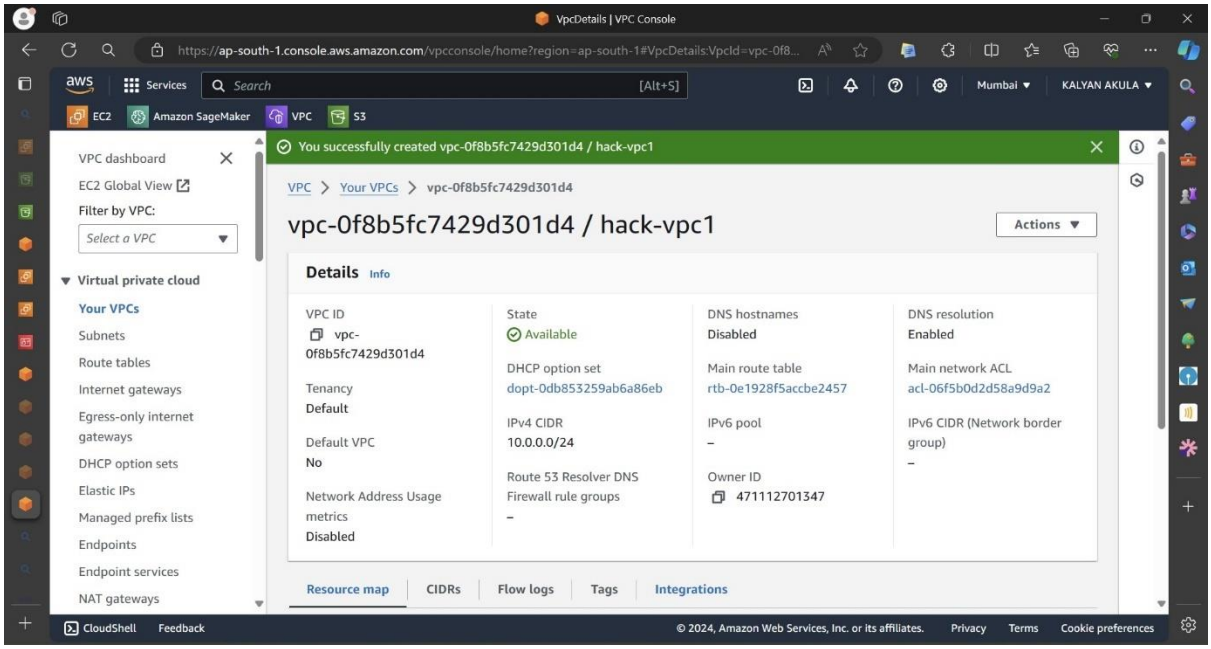




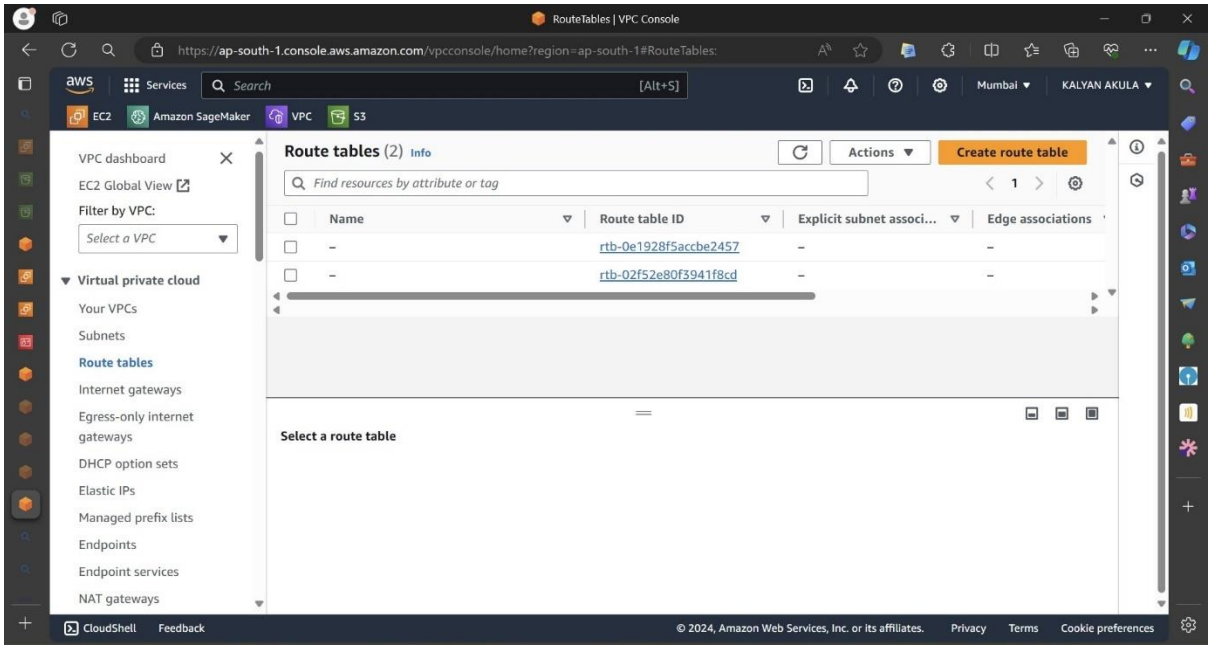
Step 5 : Click on ‘Create VPC’



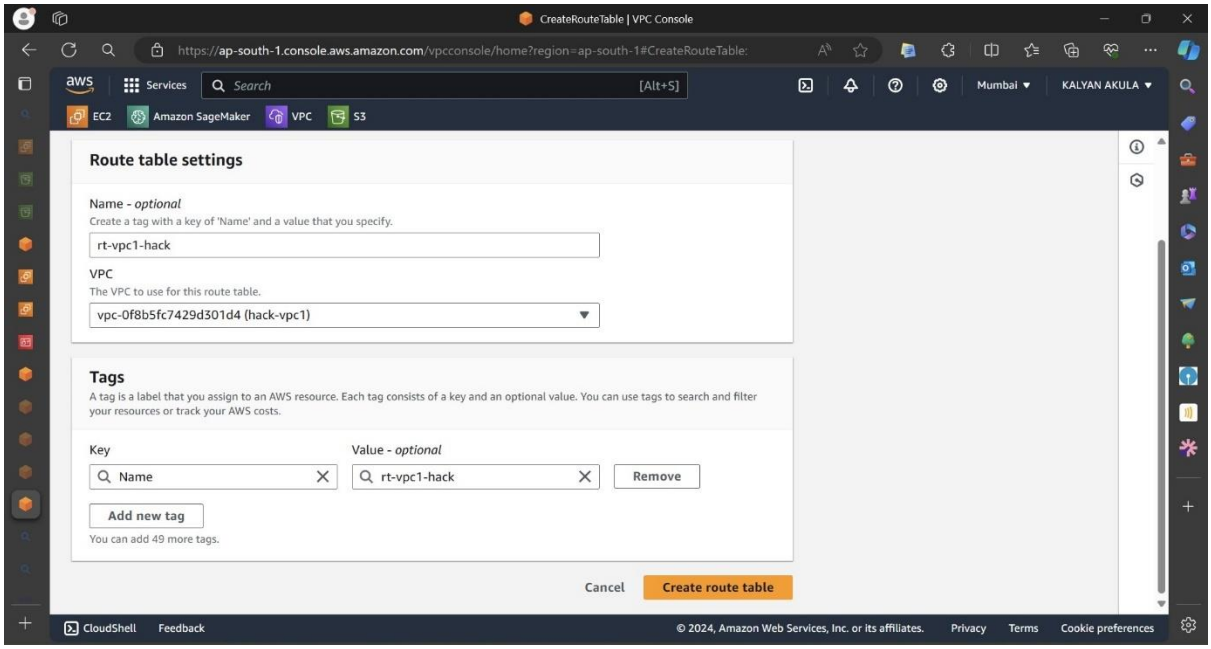
Step 6 : Click on ‘Route tables’ at left side to the window



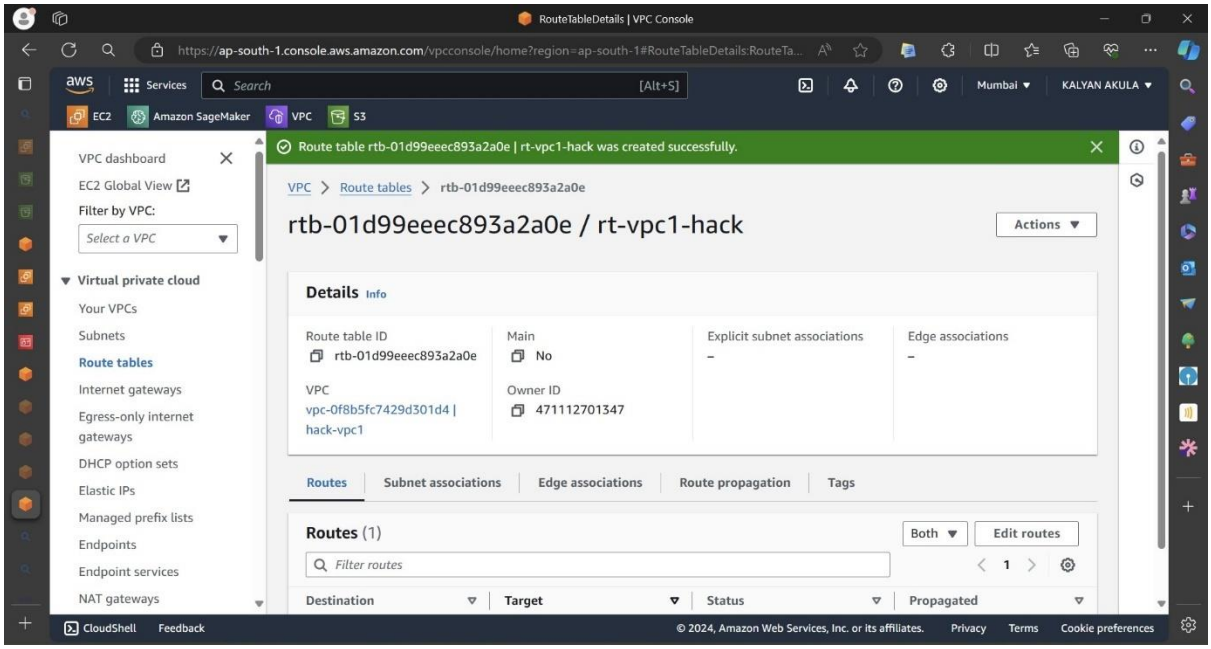
Step 7: Click on ‘Create Route Table’



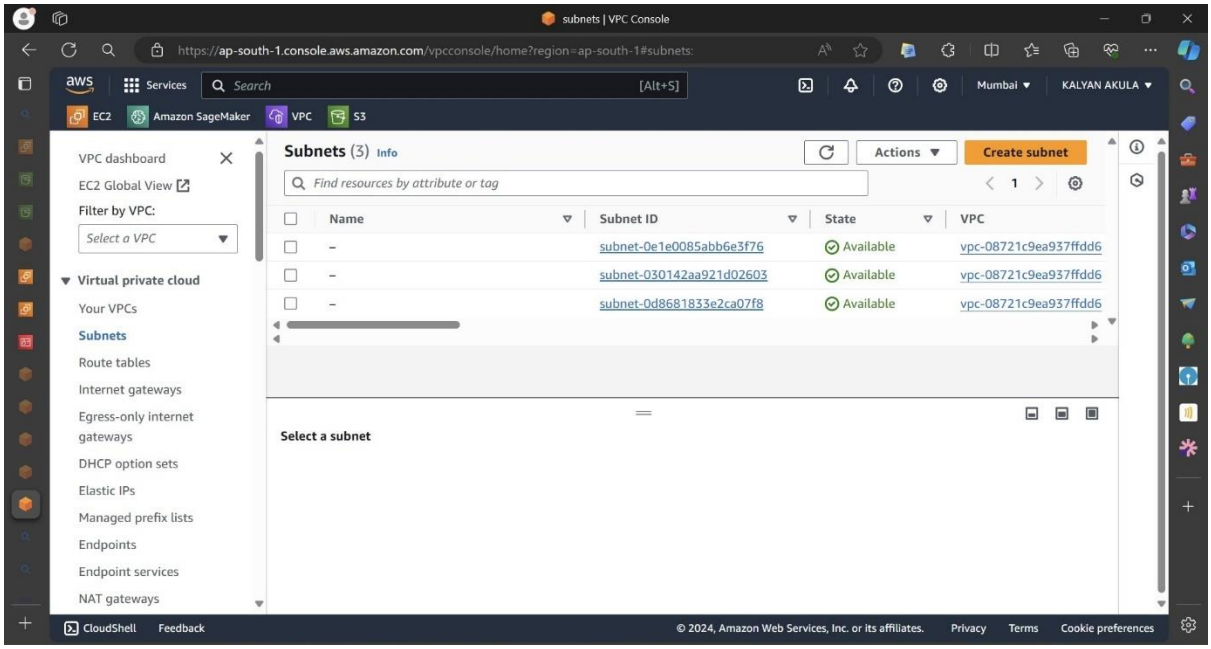
Step 8 : Fill the details as follows & click on ‘Create Table’



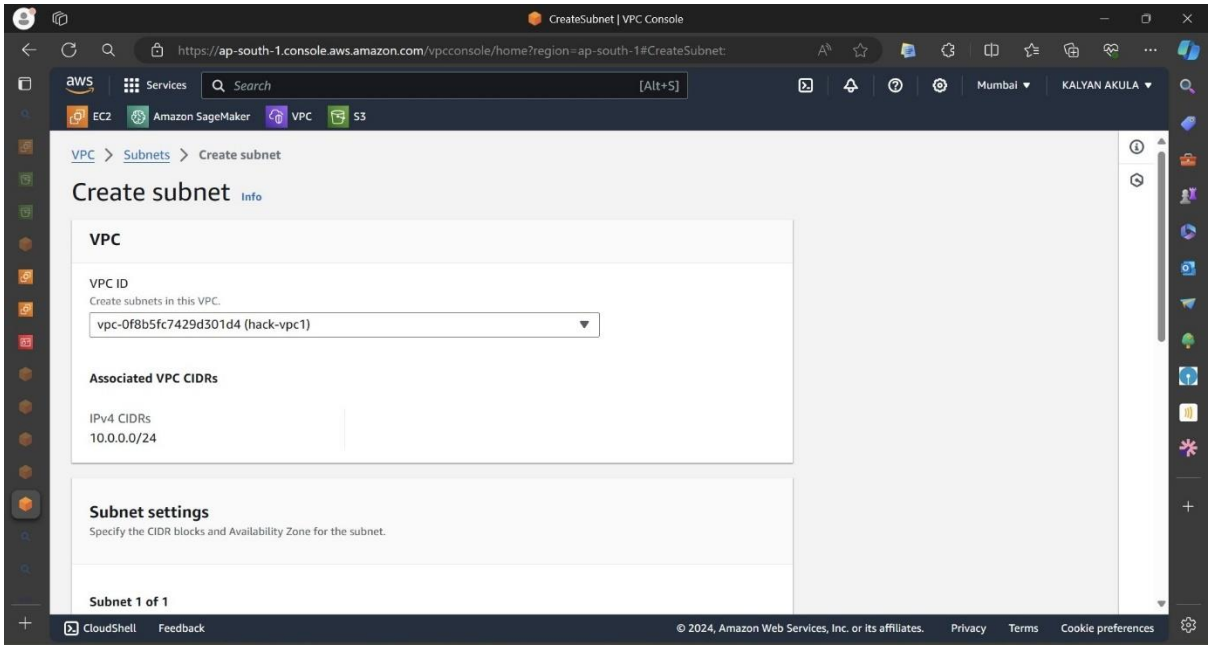
Step 9: Click on Subnet at left of window

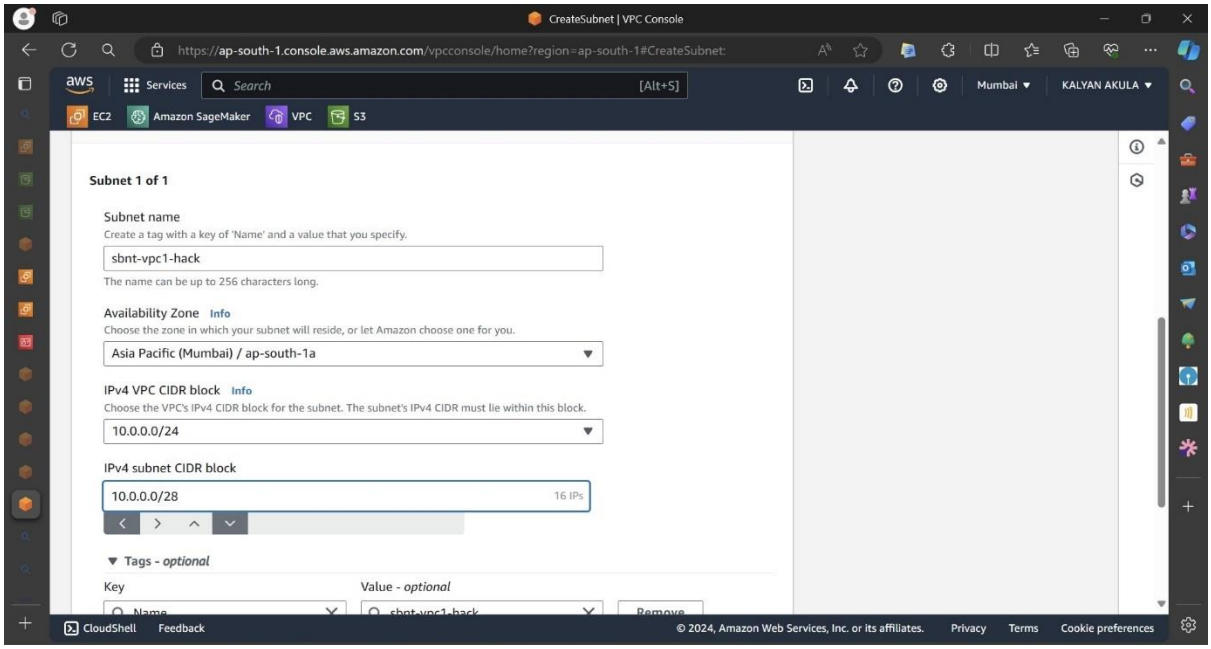


Step 10 : Click on create ‘Subnet’

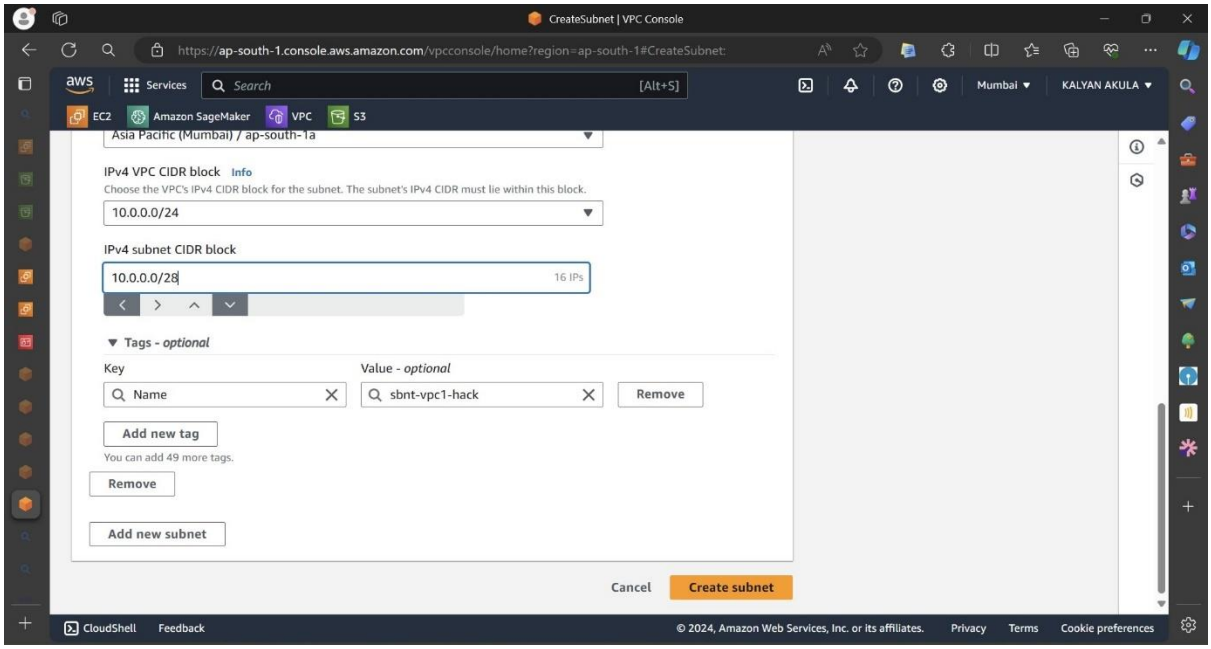


Step 11 : Fill the following Details

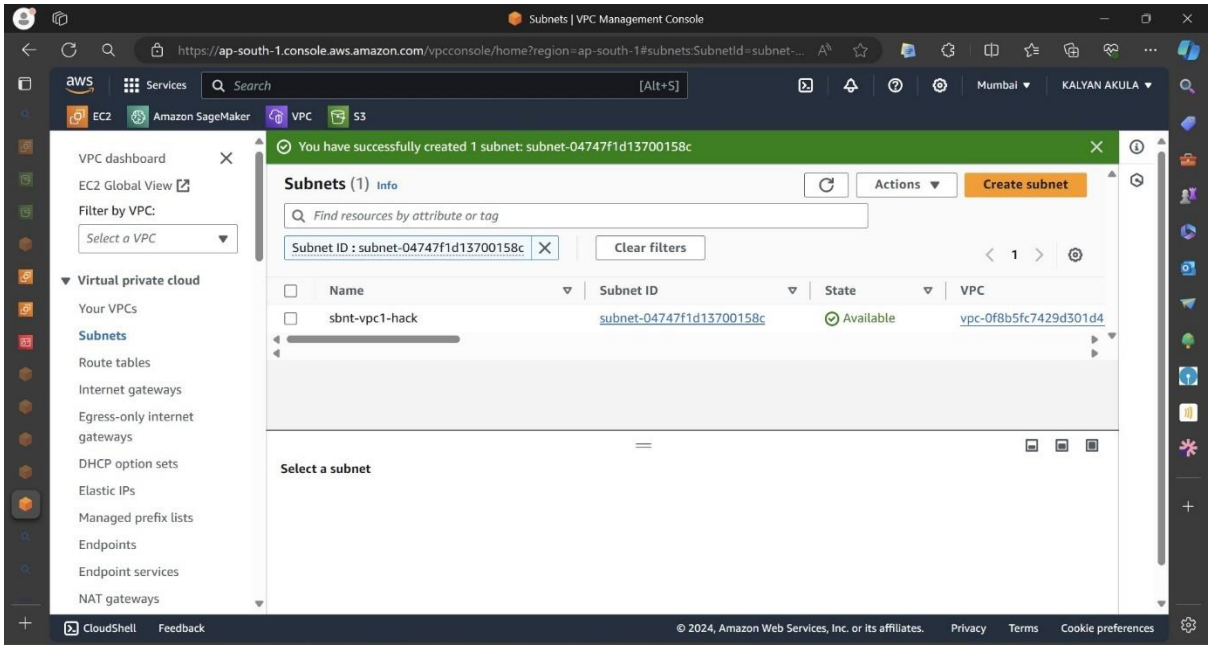




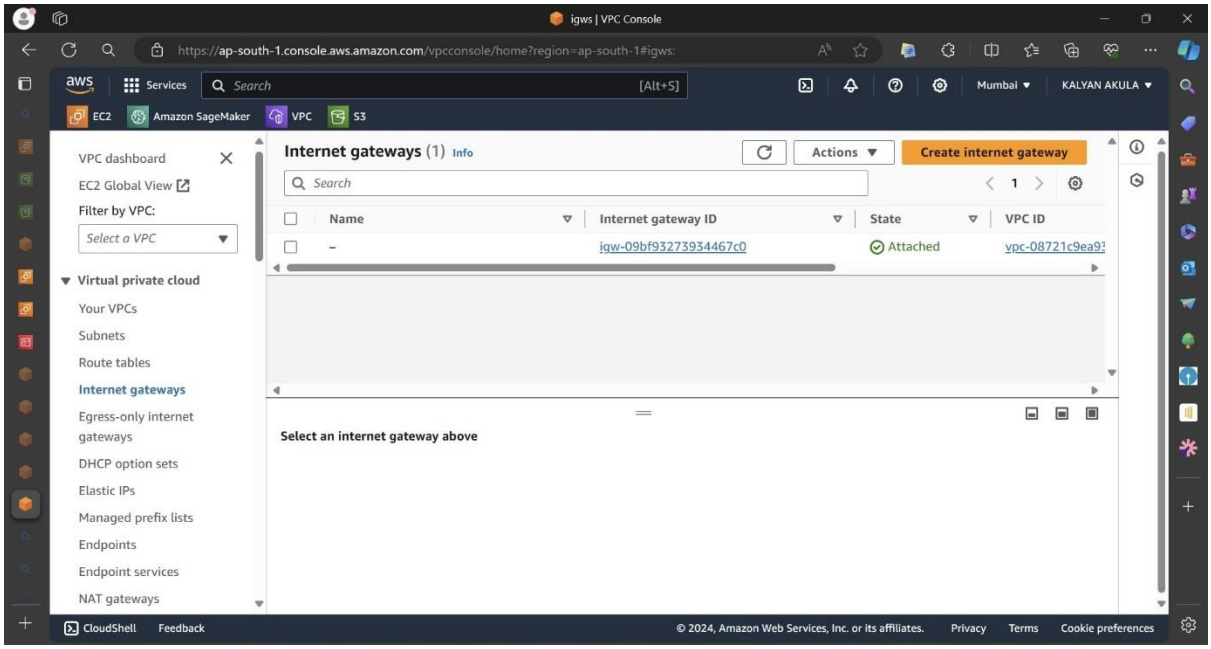
Step 12 : Click on 'Create Subnet'



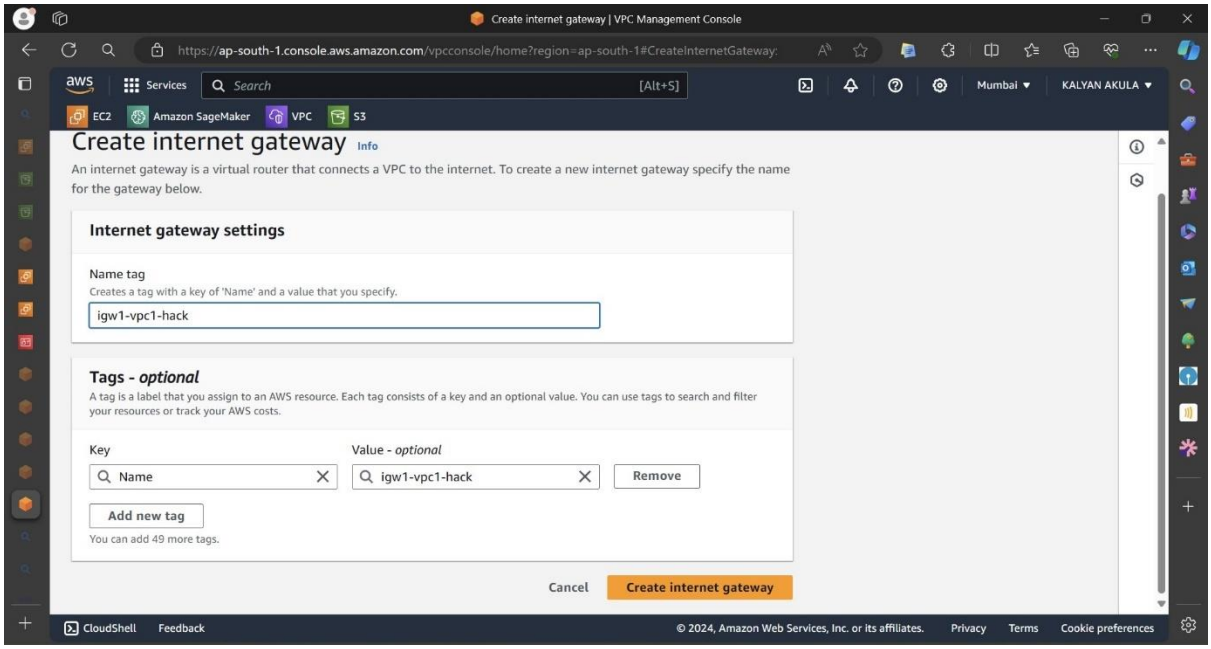
Step 13 : click on 'Internet Gateway'



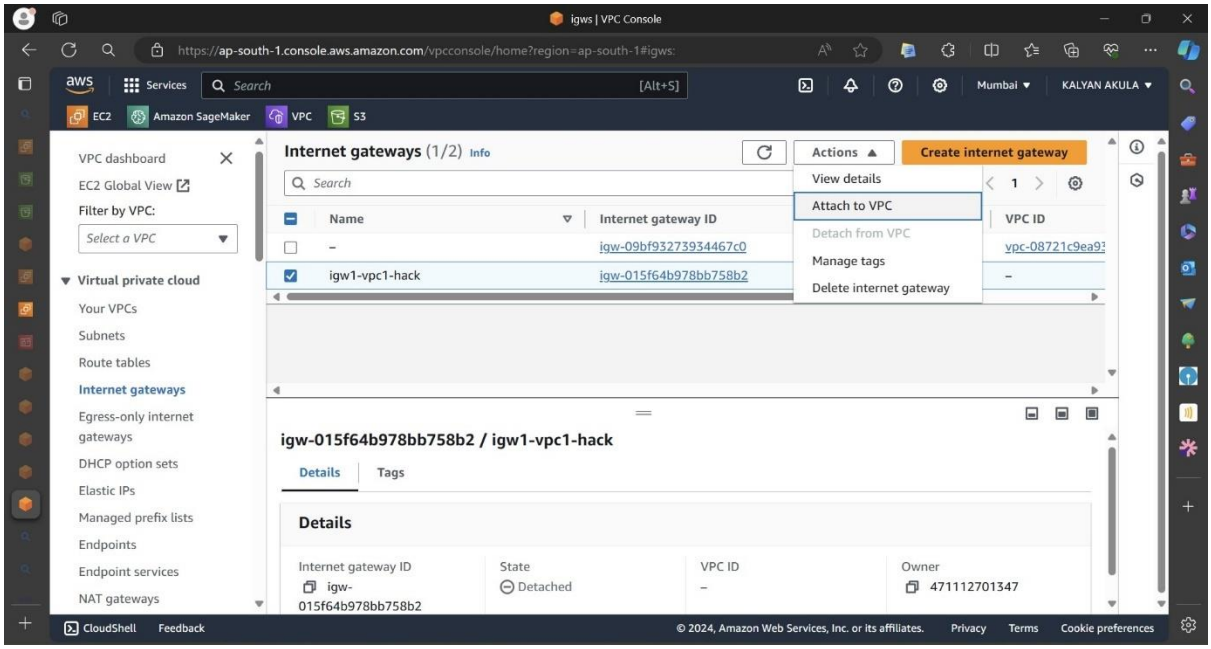
Step 15 : Click on ‘Create internet gateway’



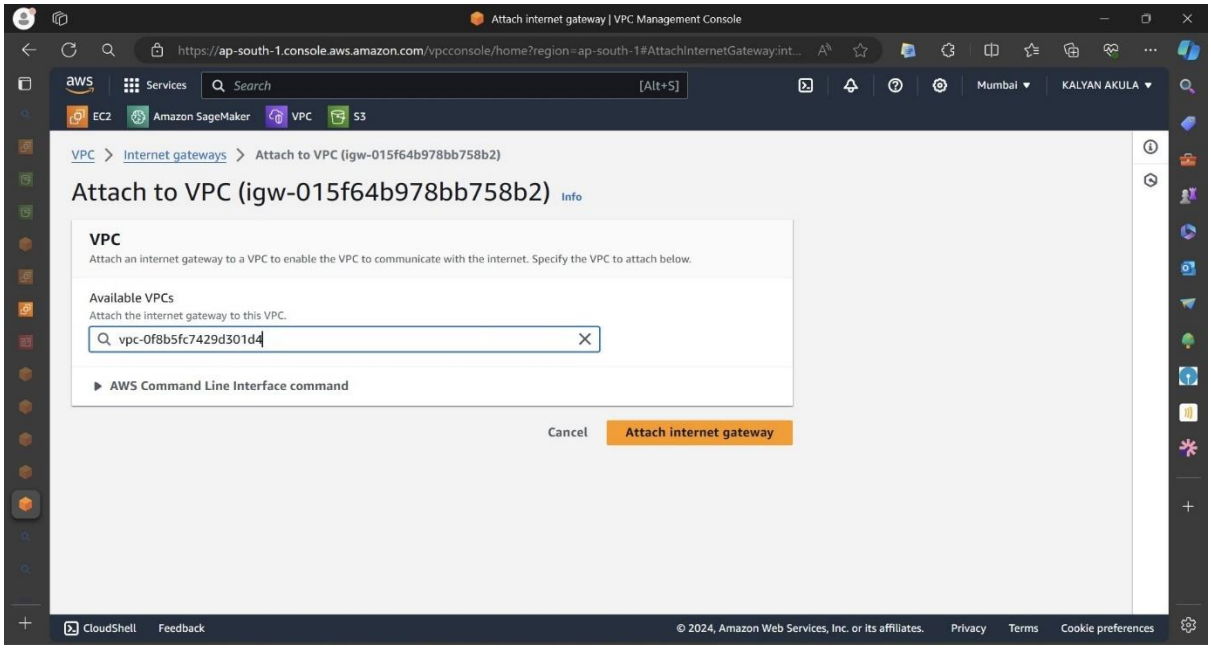
Step 16 : fill the following details & click on ‘Create internet gateway’



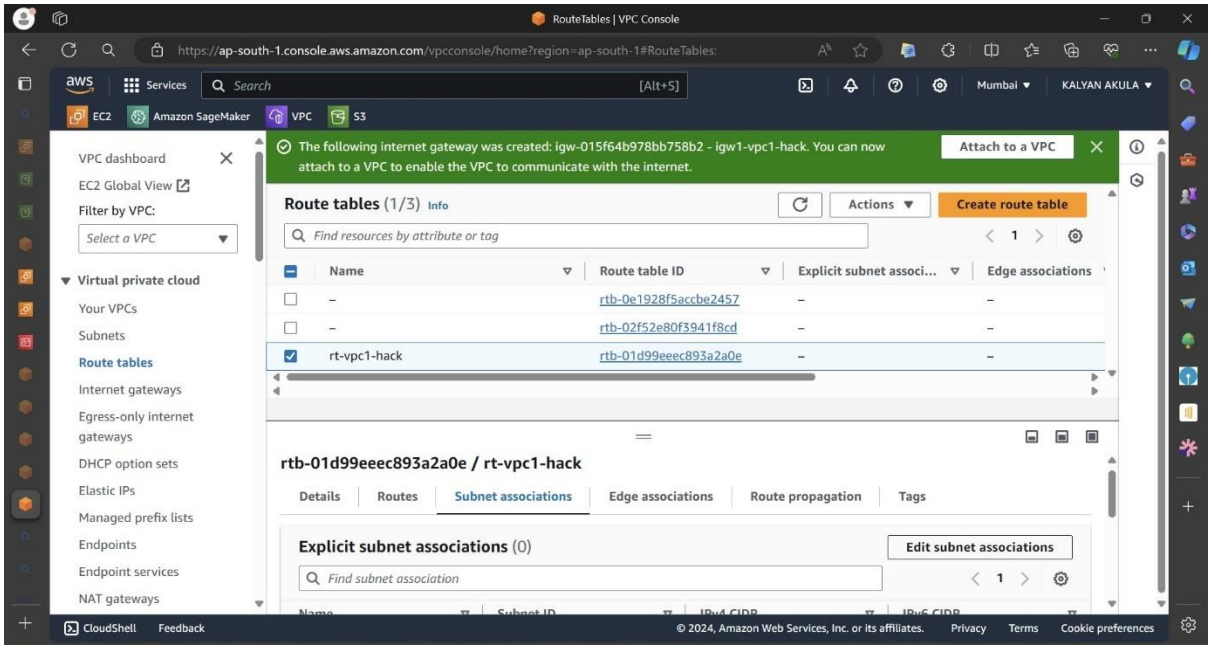
Step 17 : Select the Internet gateway , Click on ‘Actions’ & ‘Attach to VPC’



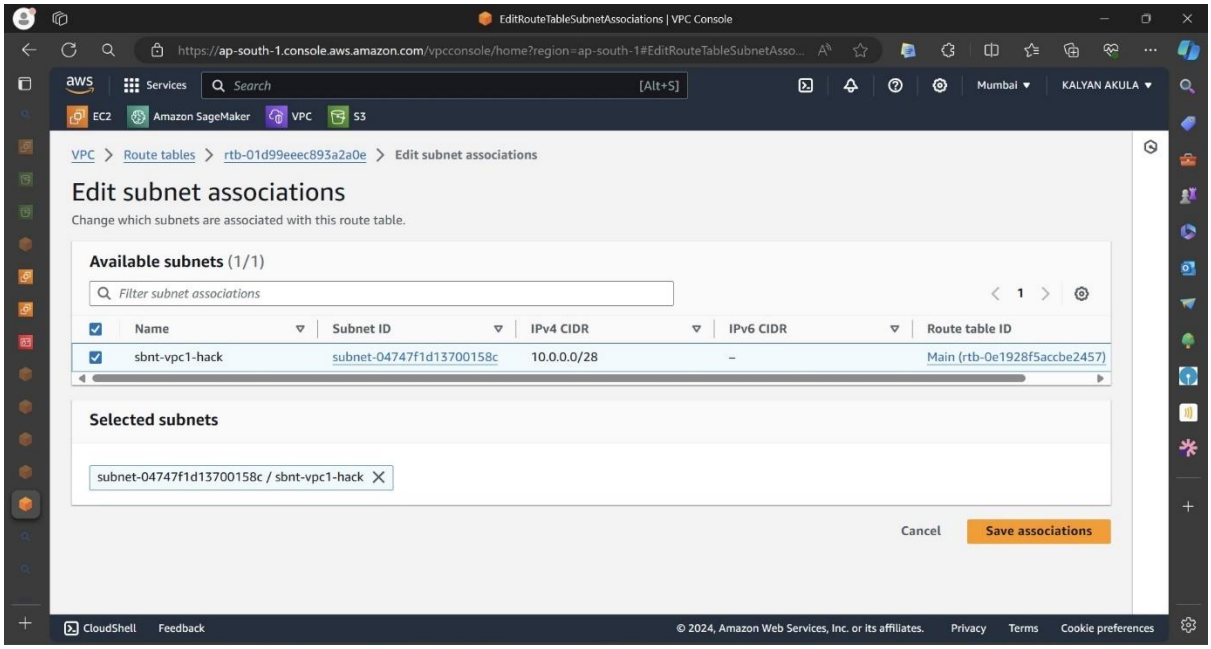
Step 18 : Fill the details & Click ‘Attach internet gateway’



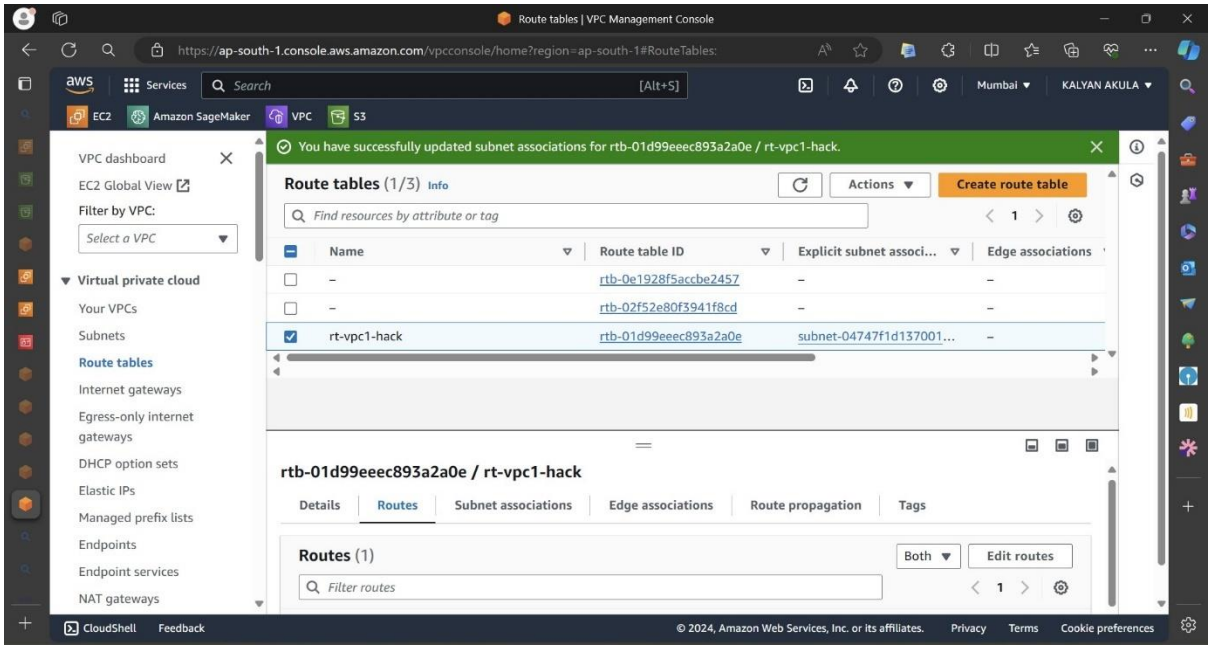
Step19 : Click on ‘Route table’ , ‘Subnet associations’ & ‘edit subnet associations’



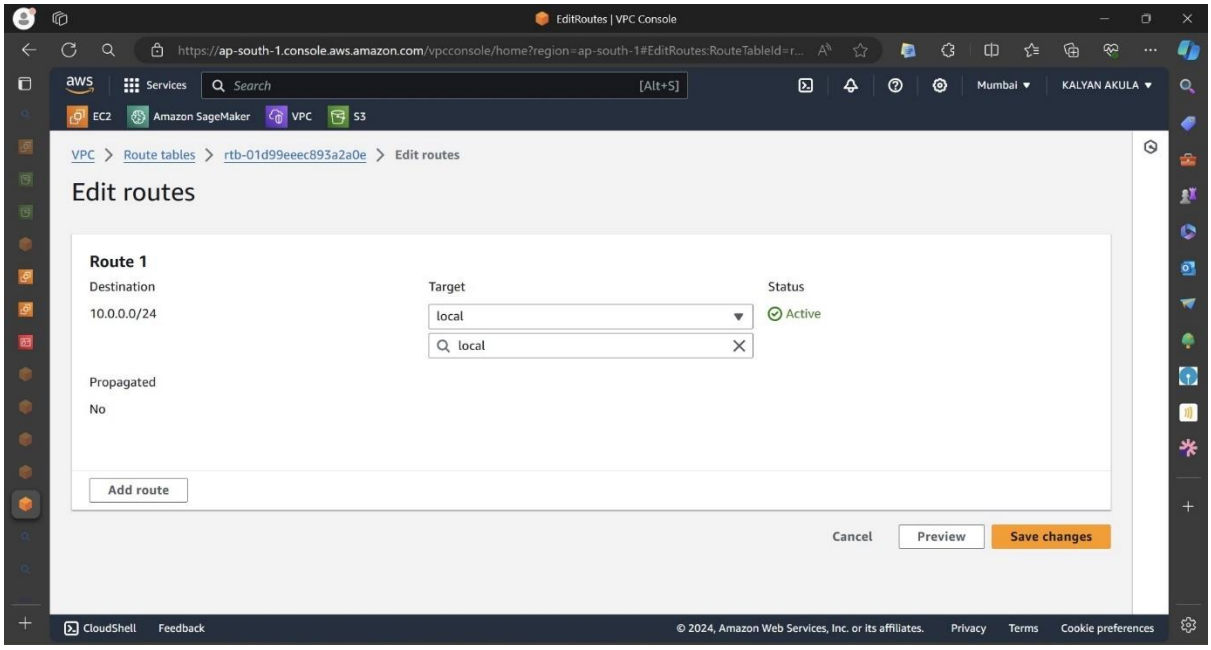
Step 20 : Select the subnet & click on Save Submissions

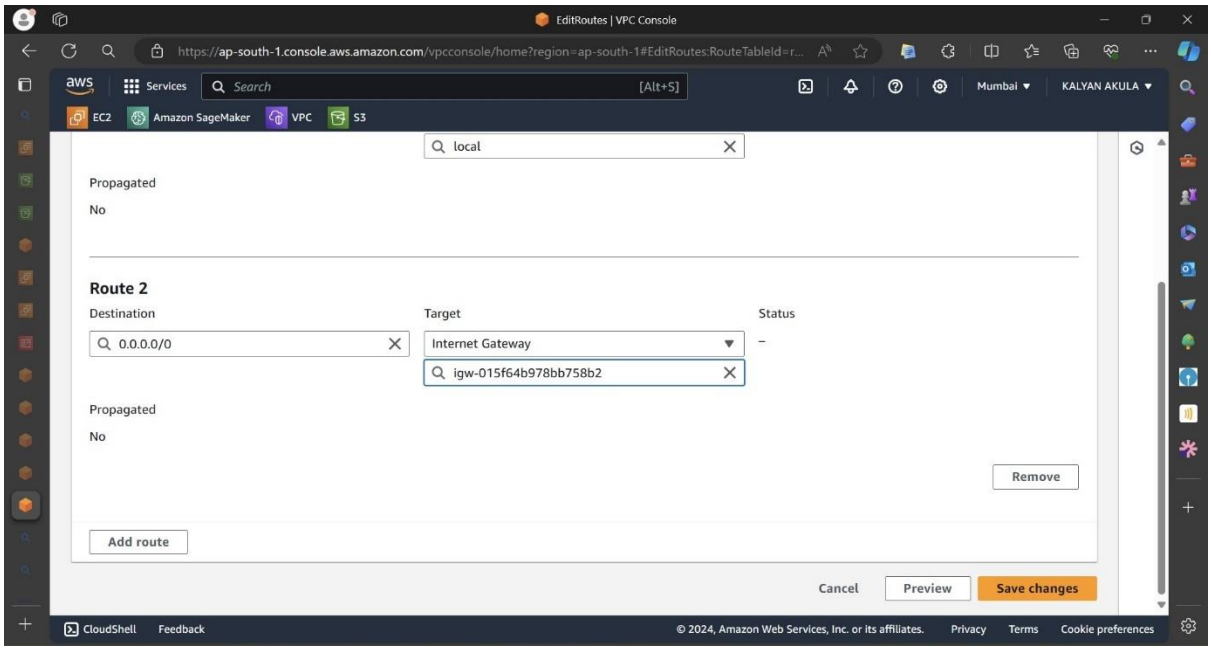


Step 21 : Now click on ‘Route tables’ , select the route , click on ‘Routes’ & Edit routes’

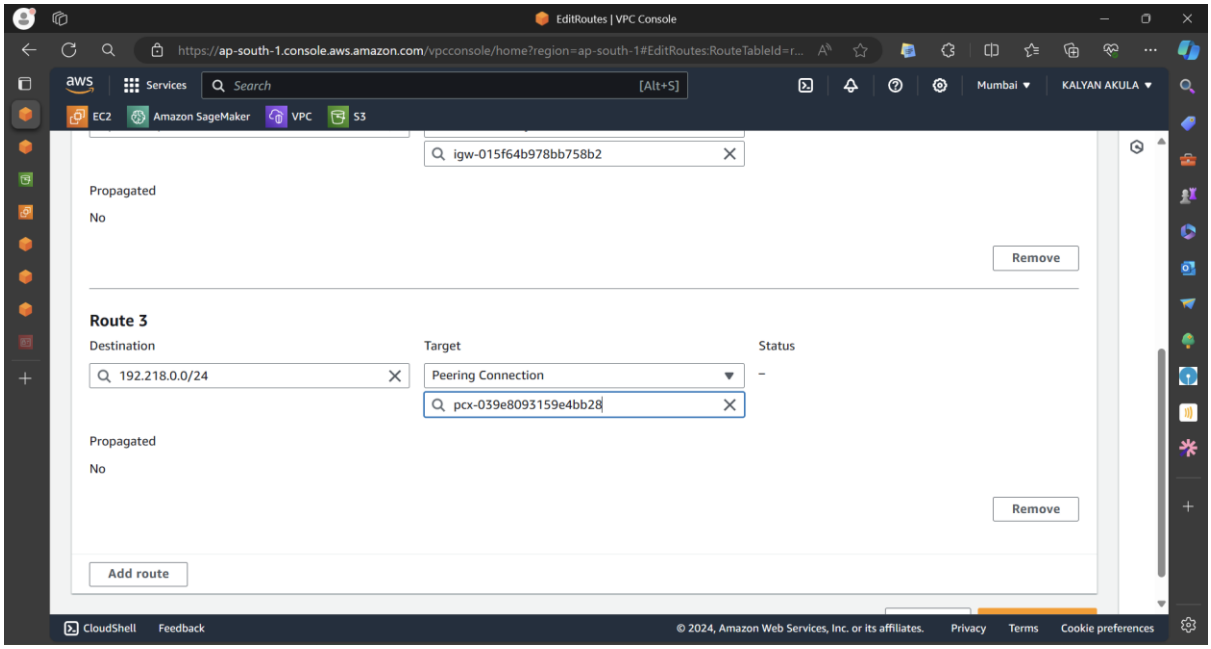


Step 22 : Fill the details in the following by adding a route & save the route

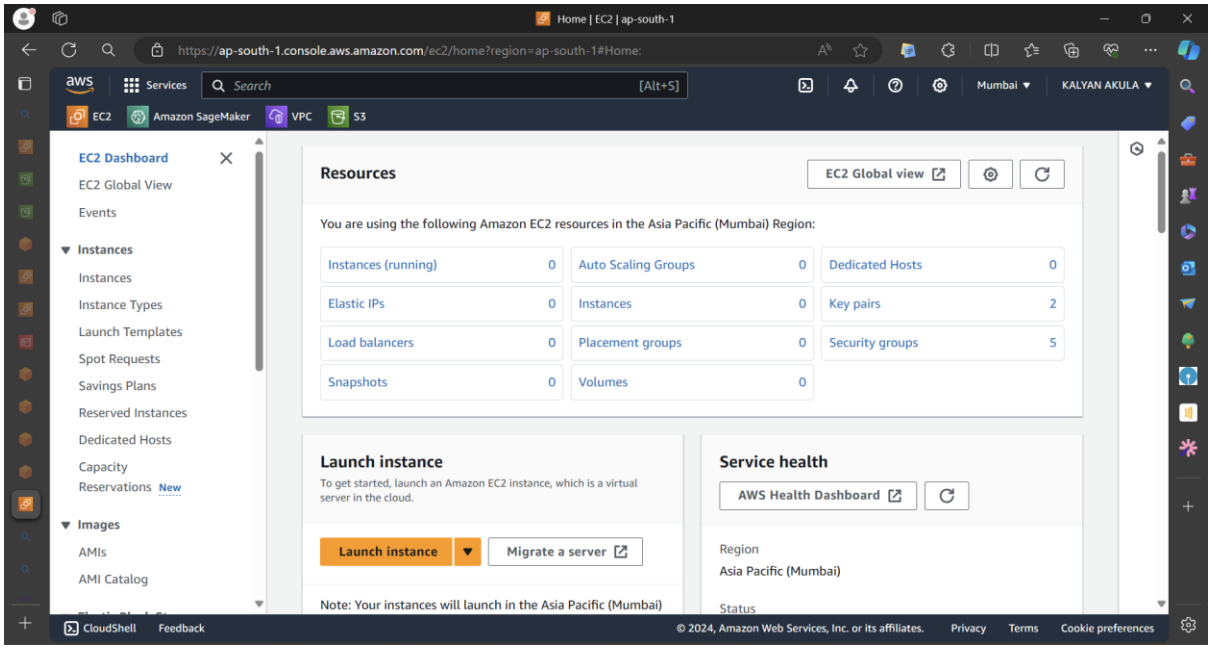




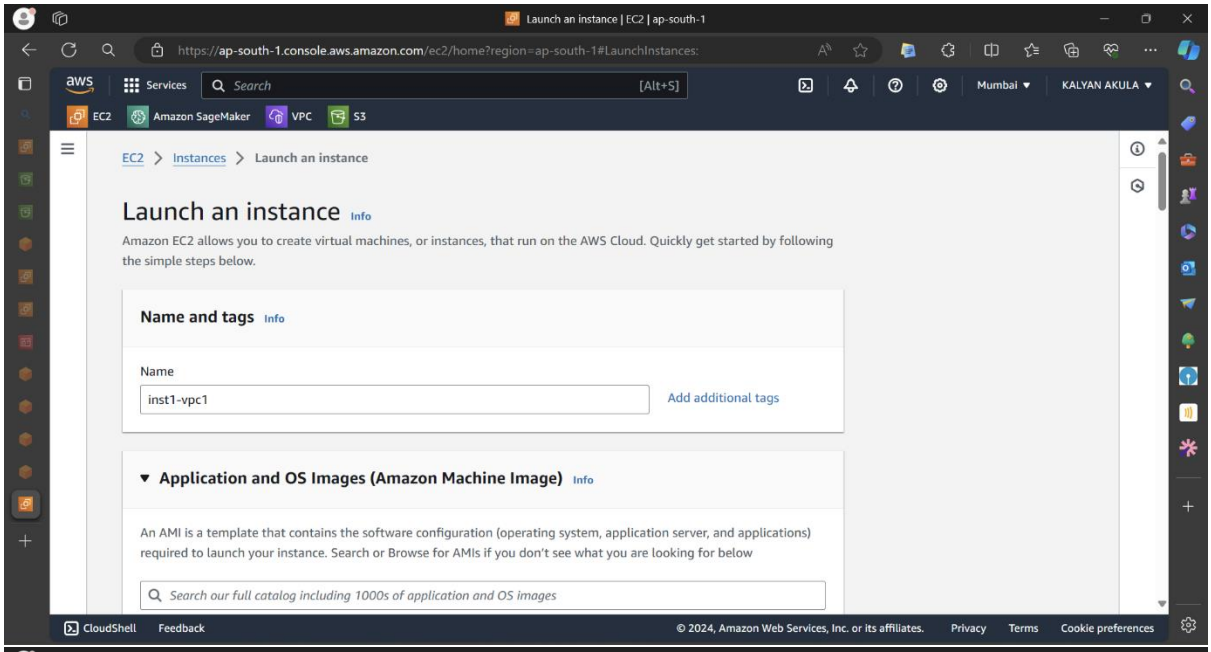
Step 23 : Now we need to add another route [destination & source route]

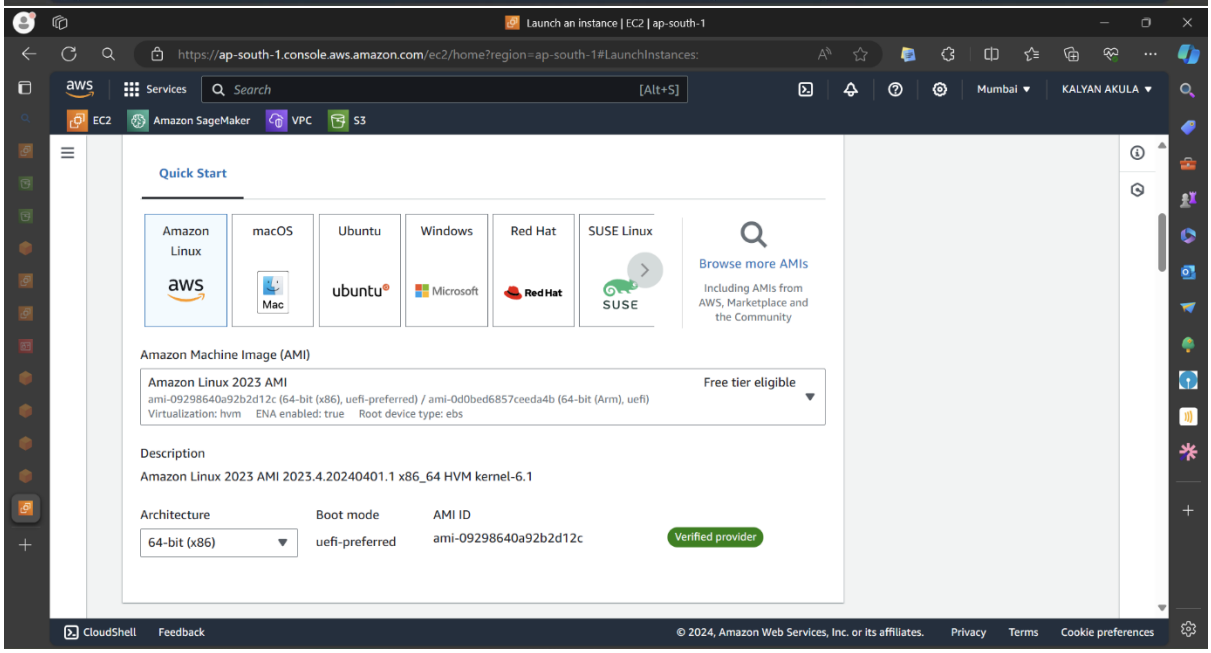


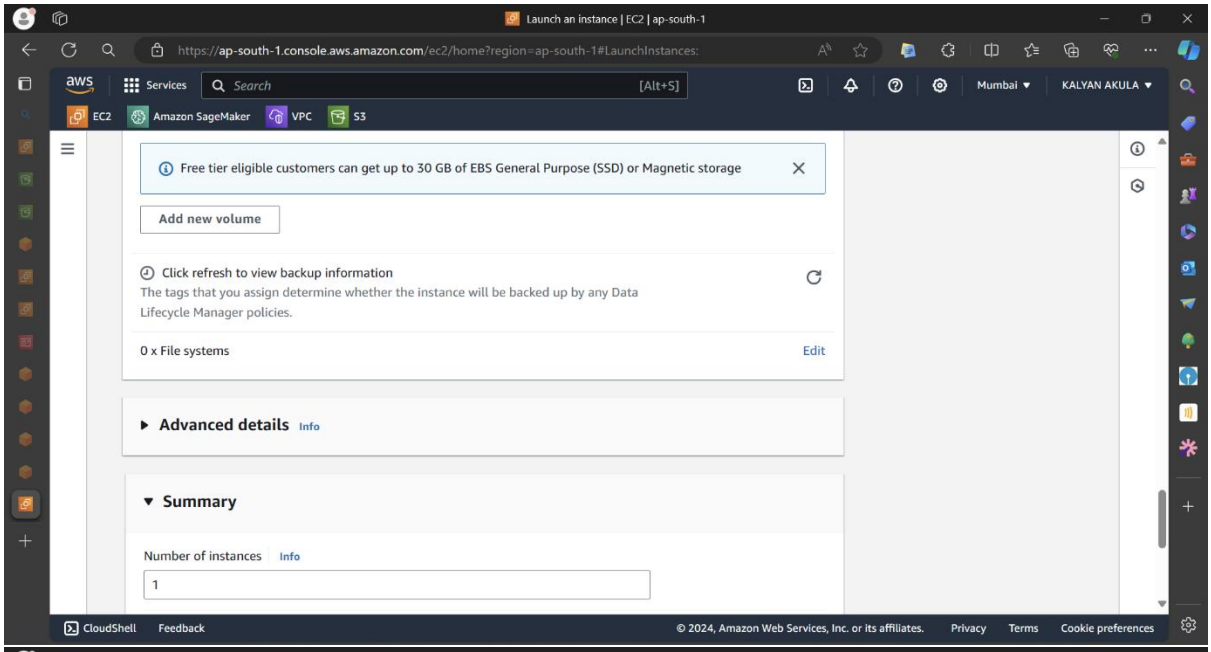
Step 24 : Now open EC2 in a new window

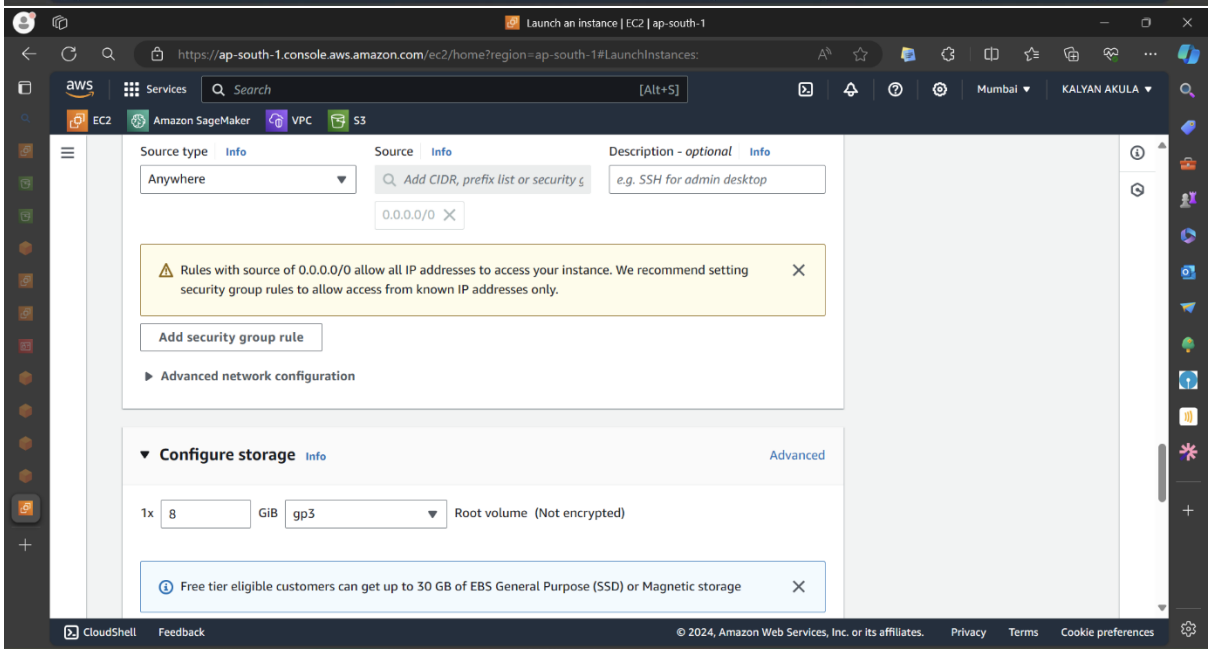


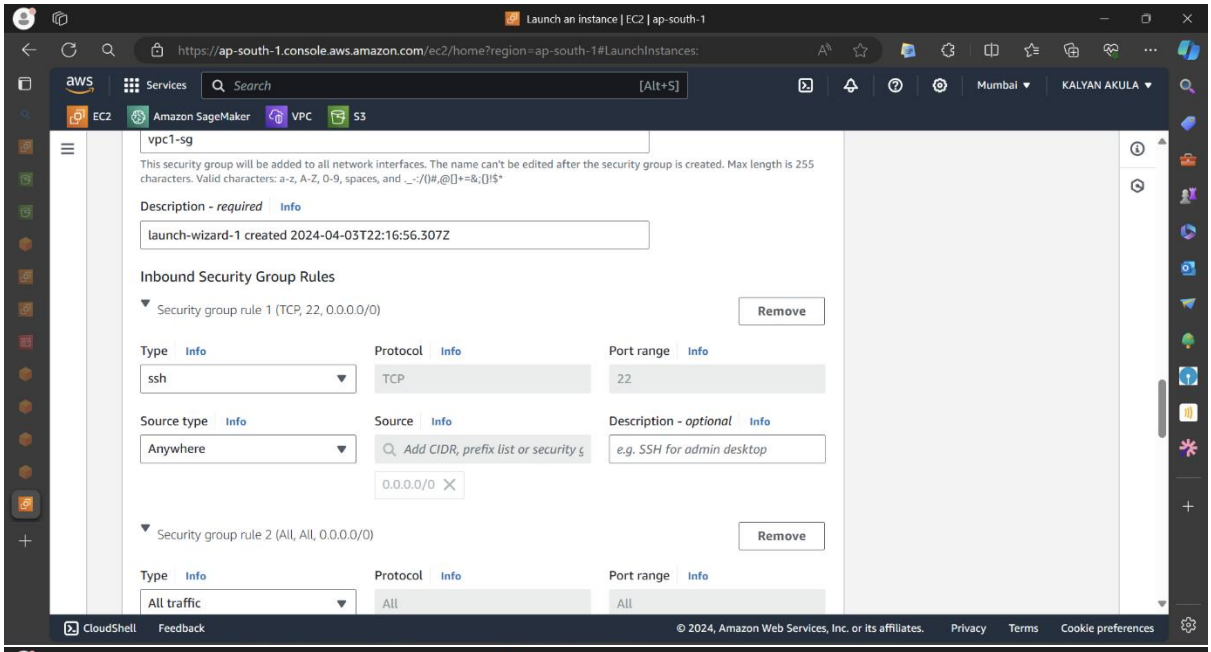
Step 25 : Now Create a Instance with the Following Details

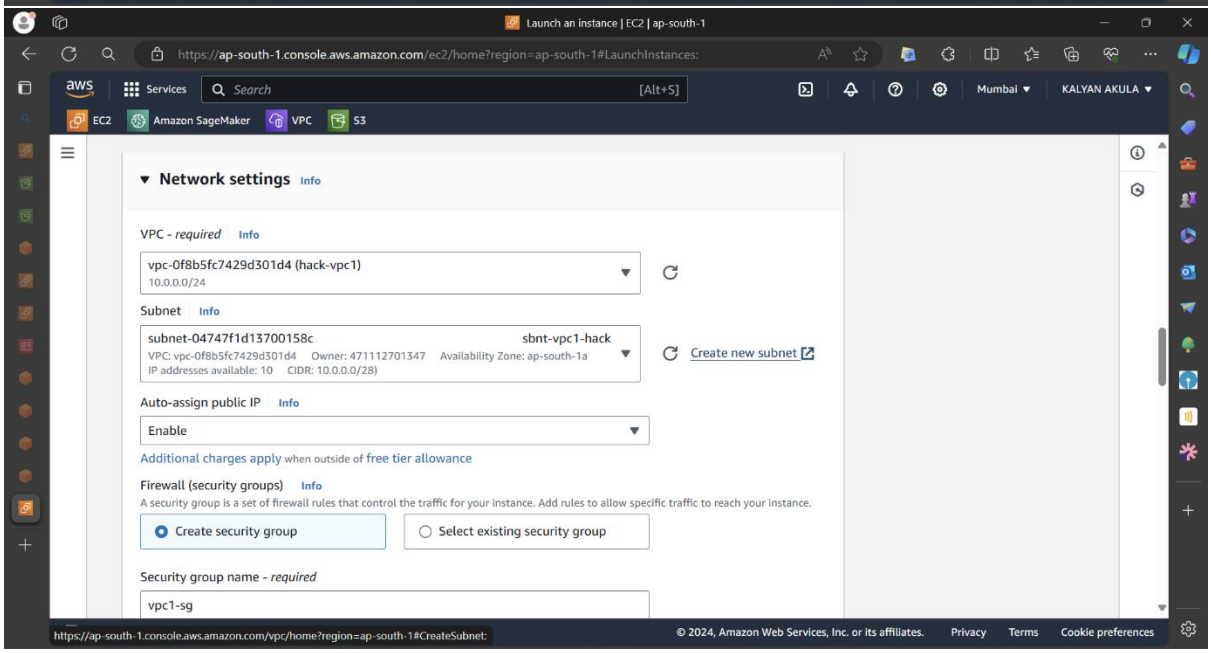

Launch an instance | EC2 | ap-south-1
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
inst1-vpc1
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

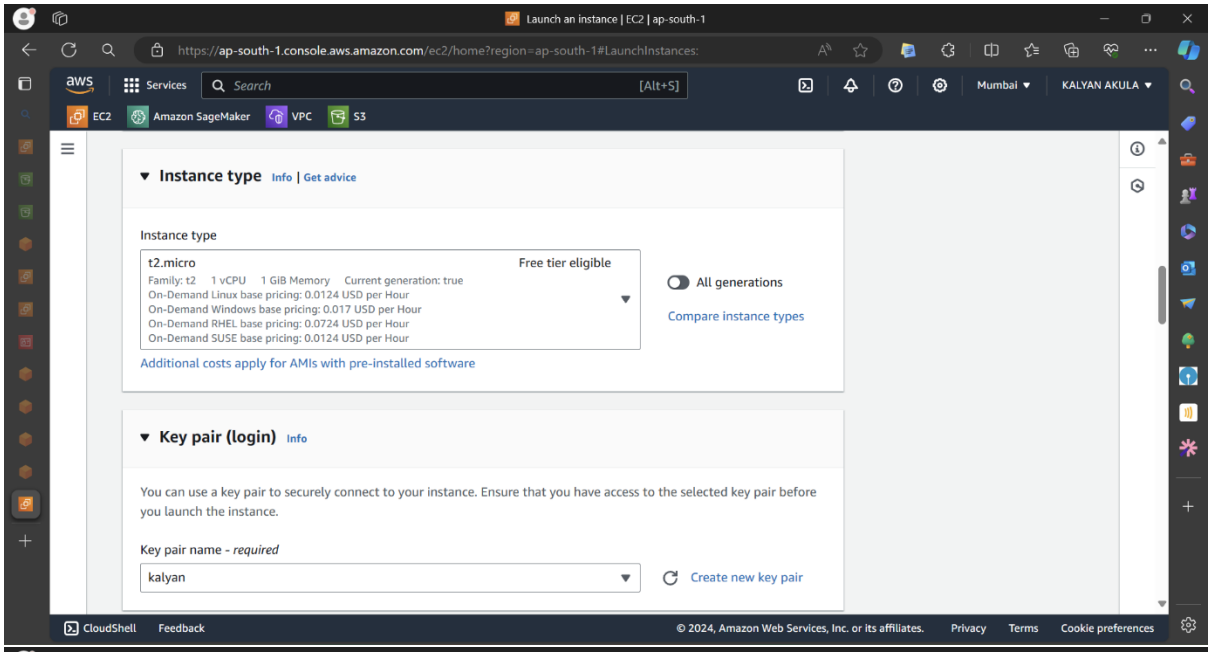

Launch an instance | EC2 | ap-south-1
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Amazon Linux 2023 AMI
ami-09298640a92b2d12c (64-bit (x86), uefi-preferred) / ami-0d0bed6857ceeda4b (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs
Free tier eligible
Description
Amazon Linux 2023 AMI 2023.4.20240401.1 x86_64 HVM kernel-6.1
Architecture
64-bit (x86)
Boot mode
uefi-preferred
AMI ID
ami-09298640a92b2d12c
Verified provider
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

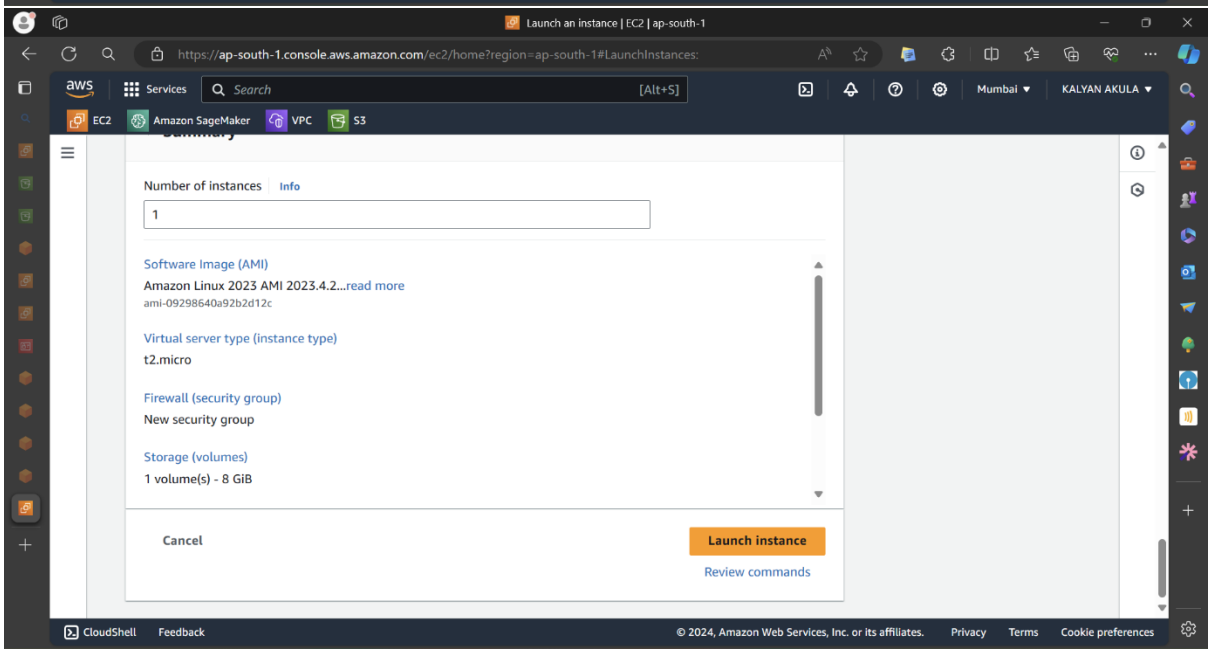

Launch an instance | EC2 | ap-south-1
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
aws
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
Add new volume
Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.
0 x File systems
Edit
Advanced details Info
Summary
Number of instances Info
1
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Launch an instance | EC2 | ap-south-1
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
aws
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security g
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Add security group rule
Advanced network configuration
Configure storage Info
Advanced
1x
8
GiB
gp3
Root volume (Not encrypted)
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Launch an instance | EC2 | ap-south-1
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
vpc1-sg
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required
Info
launch-wizard-1 created 2024-04-03T22:16:56.307Z
Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type
Info
ssh
Protocol
Info
TCP
Port range
Info
22
Source type
Info
Anywhere
Source
Info
Add CIDR, prefix list or security
Description - optional
Info
e.g. SSH for admin desktop
0.0.0.0/0
Security group rule 2 (All, All, 0.0.0.0/0)
Remove
Type
Info
All traffic
Protocol
Info
All
Port range
Info
All
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Launch an instance | EC2 | ap-south-1
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Network settings
Info
VPC - required
Info
vpc-0f8b5fc7429d301d4 (hack-vpc1)
10.0.0.0/24
Subnet
Info
subnet-04747f1d13700158c
sbnt-vpc1-hack
VPC: vpc-0f8b5fc7429d301d4 Owner: 471112701347 Availability Zone: ap-south-1a
IP addresses available: 10 CIDR: 10.0.0.0/28)
Create new subnet
Auto-assign public IP
Info
Enable
Additional charges apply when outside of free tier allowance
Firewall (security groups)
Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
vpc1-sg
https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#CreateSubnet:
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

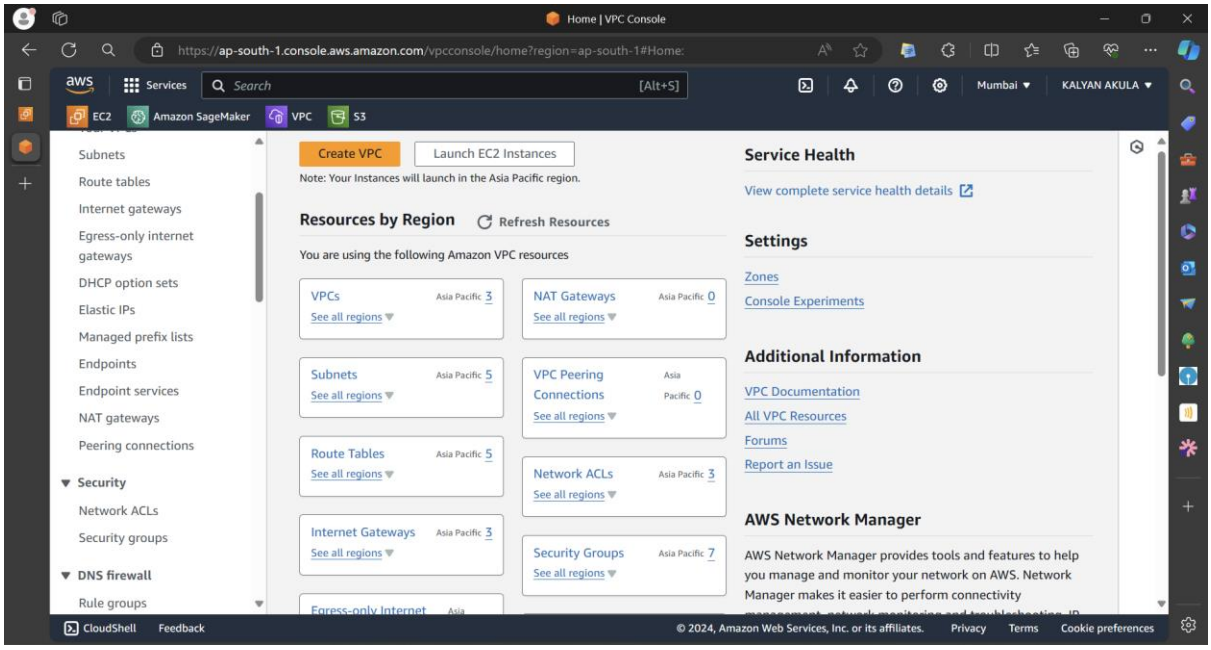




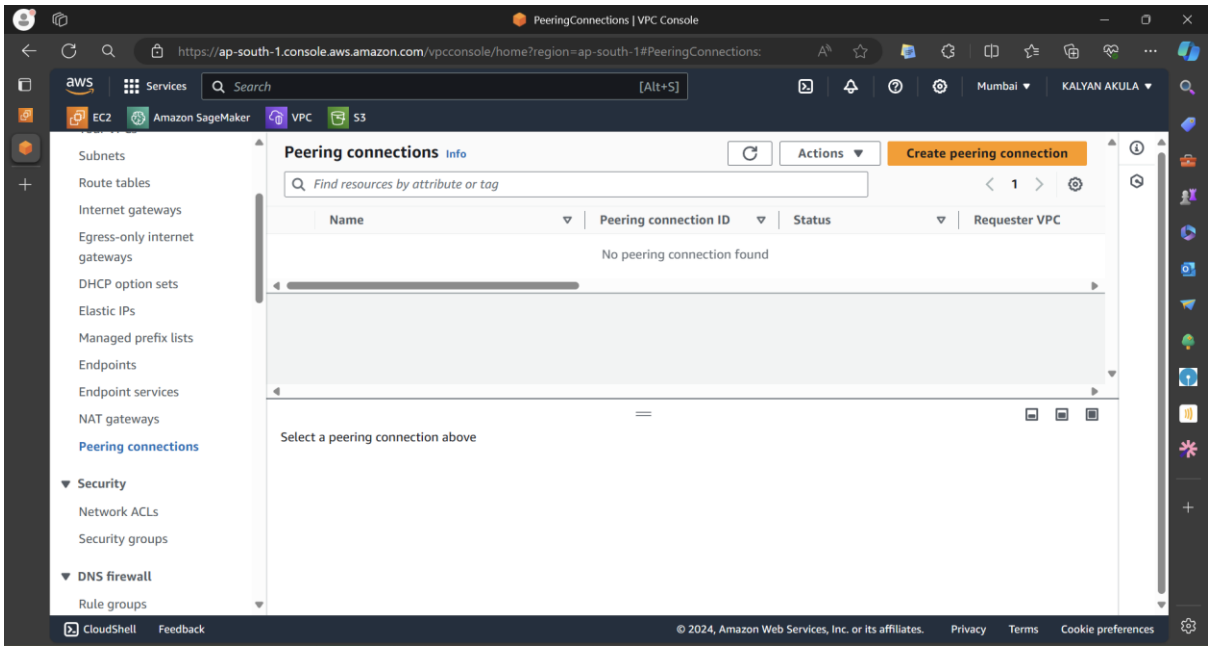
Step 26 : Now follow from Step 2 – Step 26 , for creating another VPC

Peering connection between VPC1&VPC2

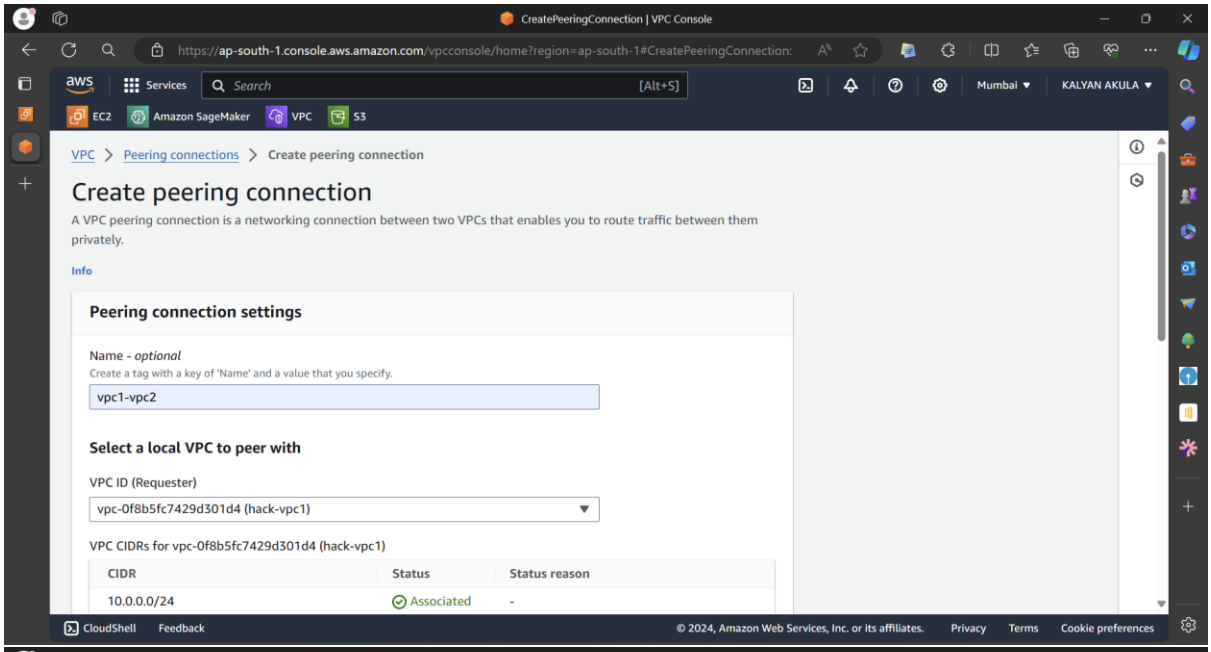
Step 1 : Go to VPC Dashboard & open Peering Connections

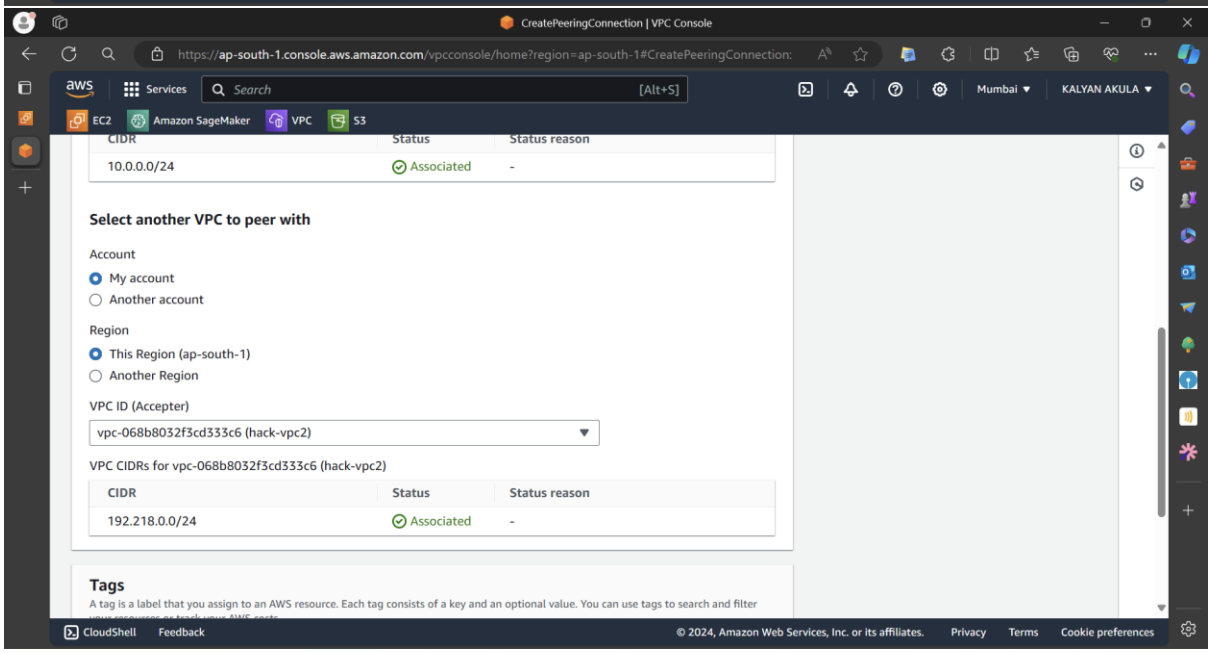


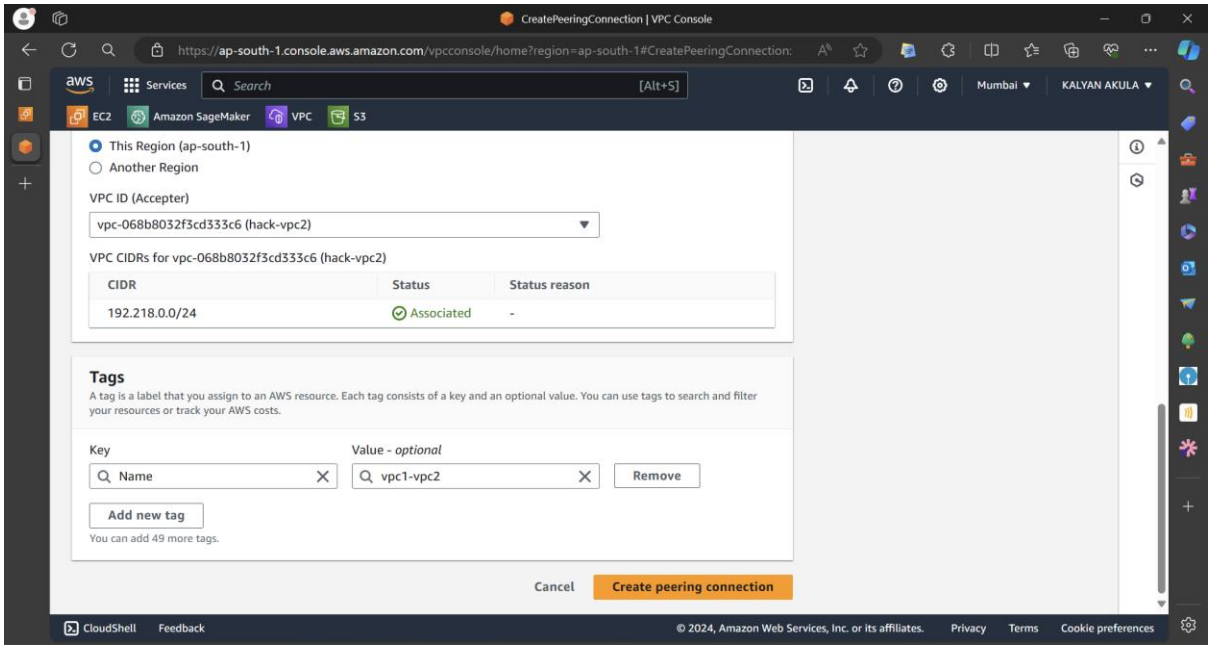
Step 2 : Click on ‘Create Peering Connection’



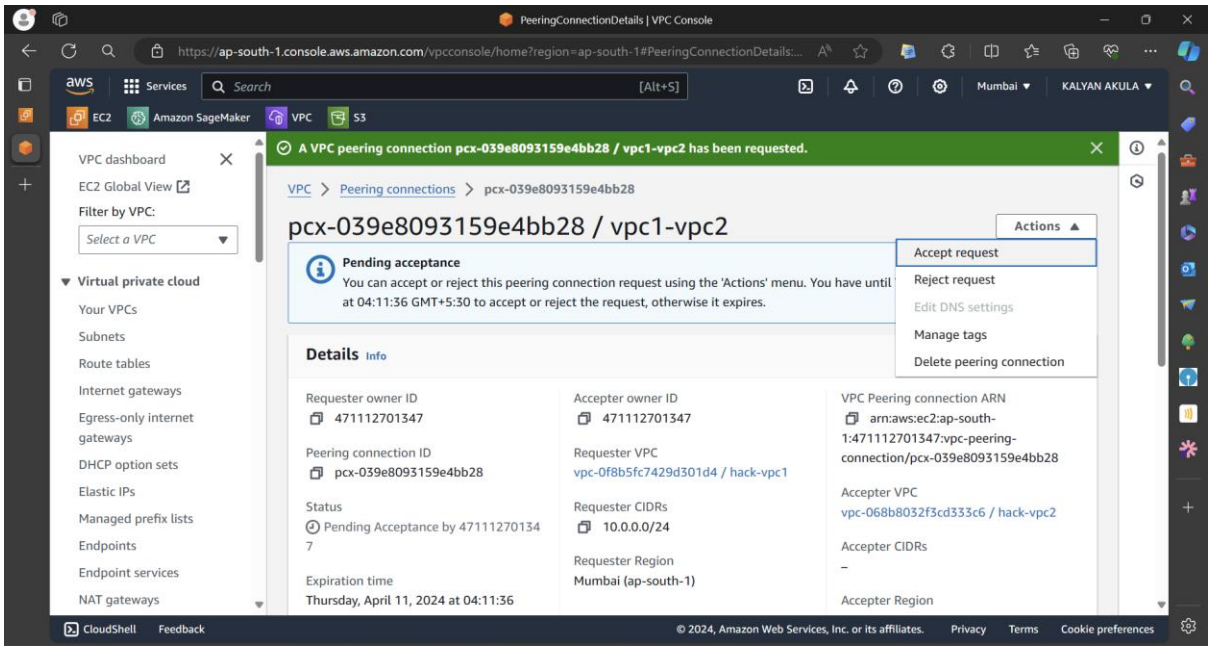
Step 3: Fill the following details & click on ‘Create peering connection’


CreatePeeringConnection | VPC Console
https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreatePeeringConnection:
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
VPC > Peering connections > Create peering connection
Create peering connection
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately.
Info
Peering connection settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
vpc1-vpc2
Select a local VPC to peer with
VPC ID (Requester)
vpc-0f8b5fc7429d301d4 (hack-vpc1)
VPC CIDRs for vpc-0f8b5fc7429d301d4 (hack-vpc1)
CIDR
Status
Status reason
10.0.0.0/24
Associated
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


CreatePeeringConnection | VPC Console
https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreatePeeringConnection:
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
CIDR
Status
Status reason
10.0.0.0/24
Associated
-
Select another VPC to peer with
Account
My account
Another account
Region
This Region (ap-south-1)
Another Region
VPC ID (Accepter)
vpc-068b8032f3cd333c6 (hack-vpc2)
VPC CIDRs for vpc-068b8032f3cd333c6 (hack-vpc2)
CIDR
Status
Status reason
192.218.0.0/24
Associated
-
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

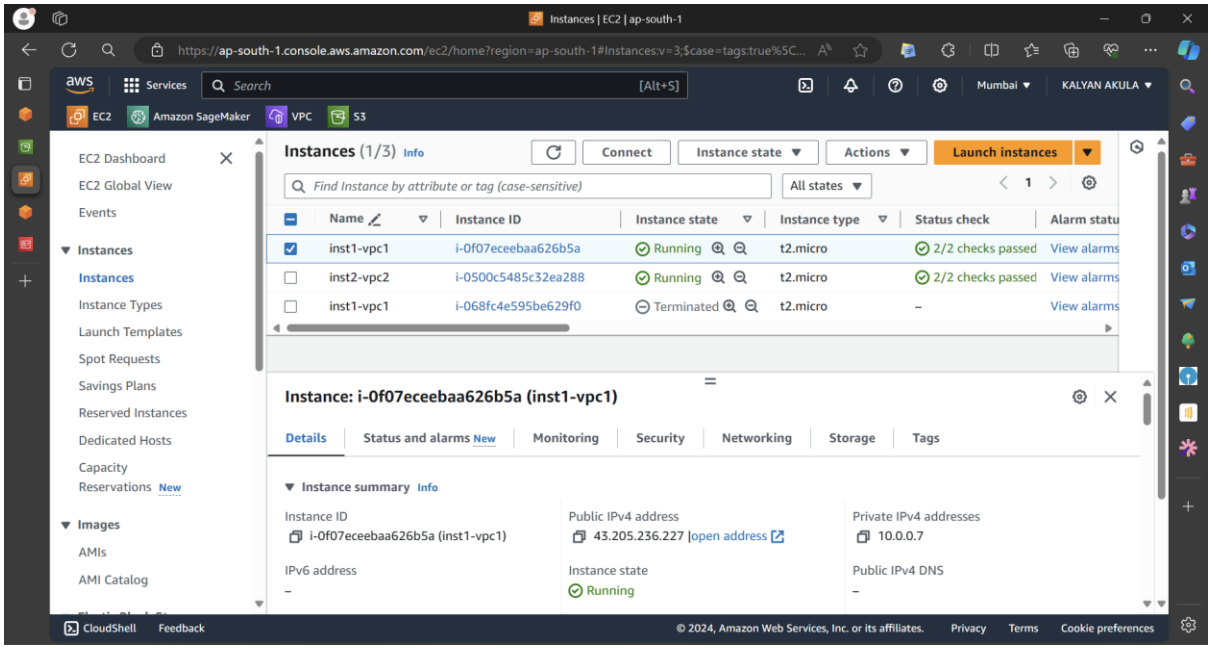


Step 4 : Now click on ‘Actions’ & ‘Accept request’

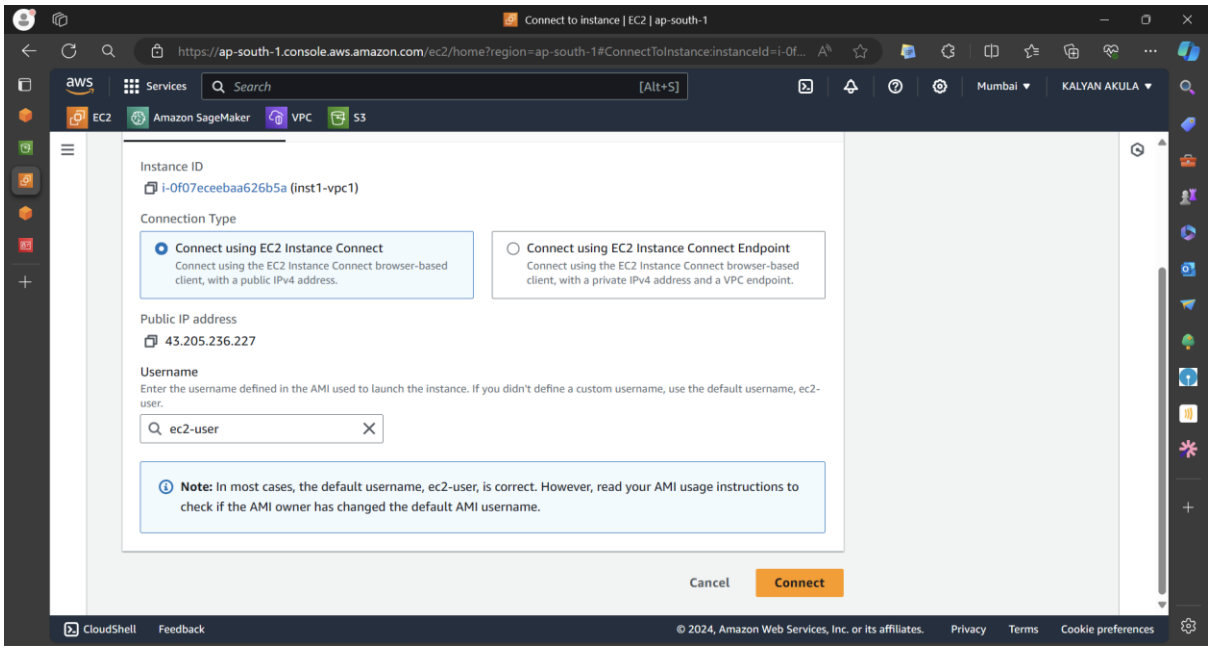


Step 5 : Go to EC2 Dashboard

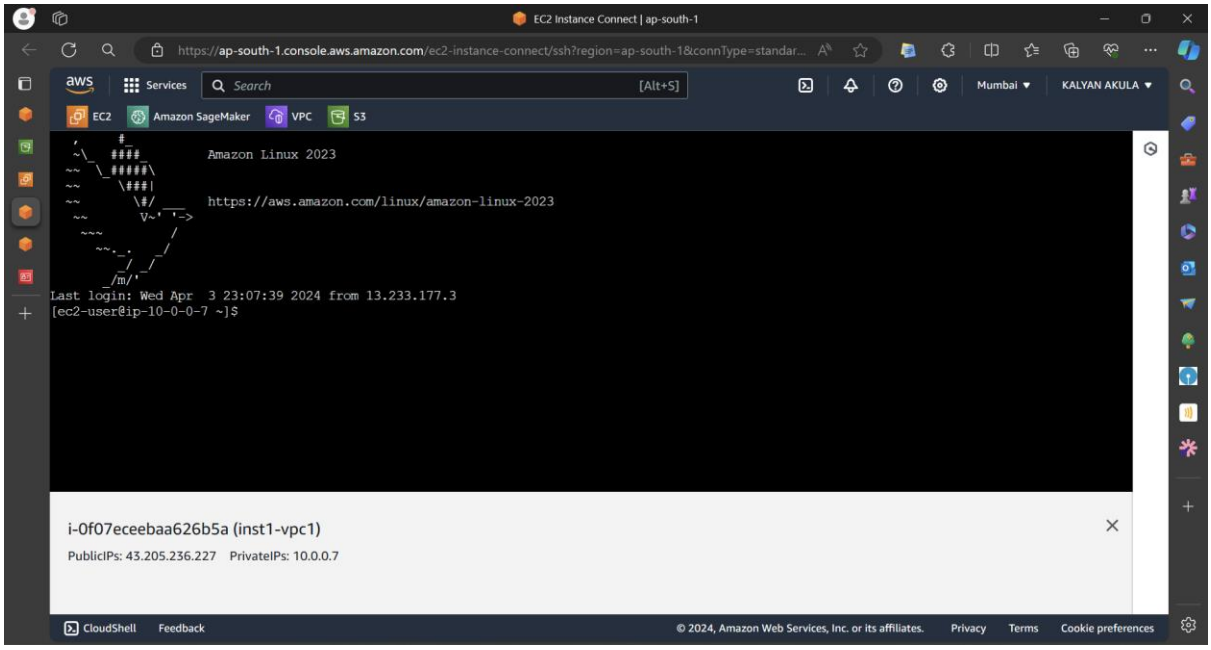
Step 6 : Select Inst1-vpc1 & click on connect



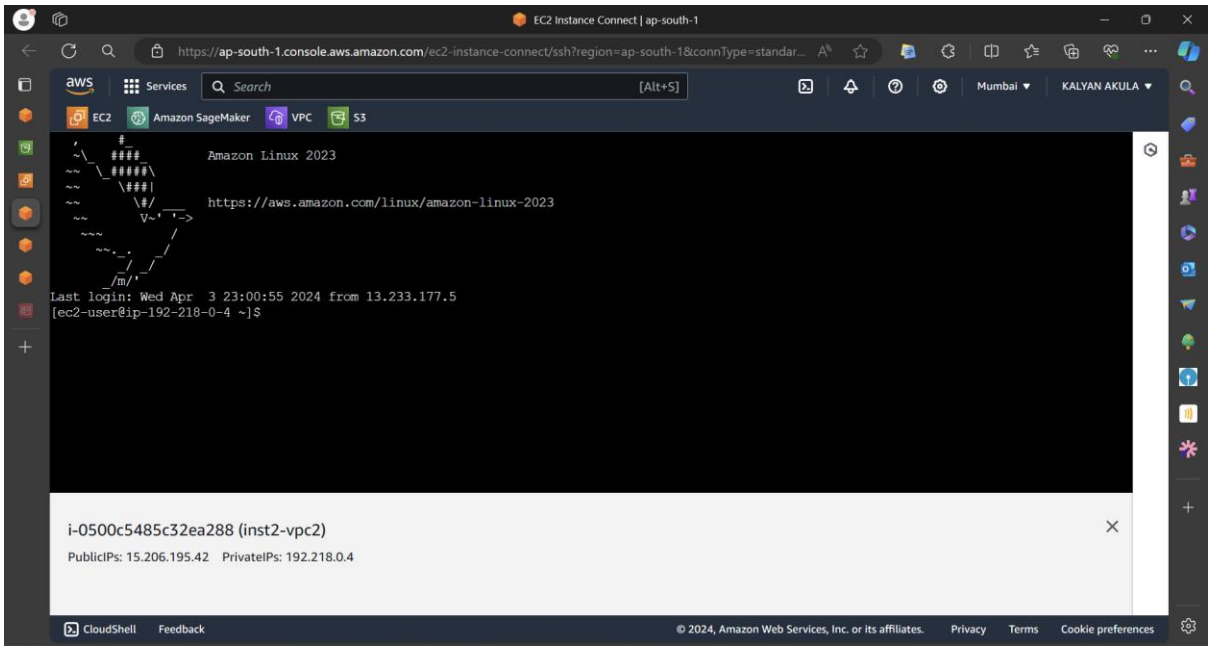
Step 7 : Click on connect



- Linux interface Opens

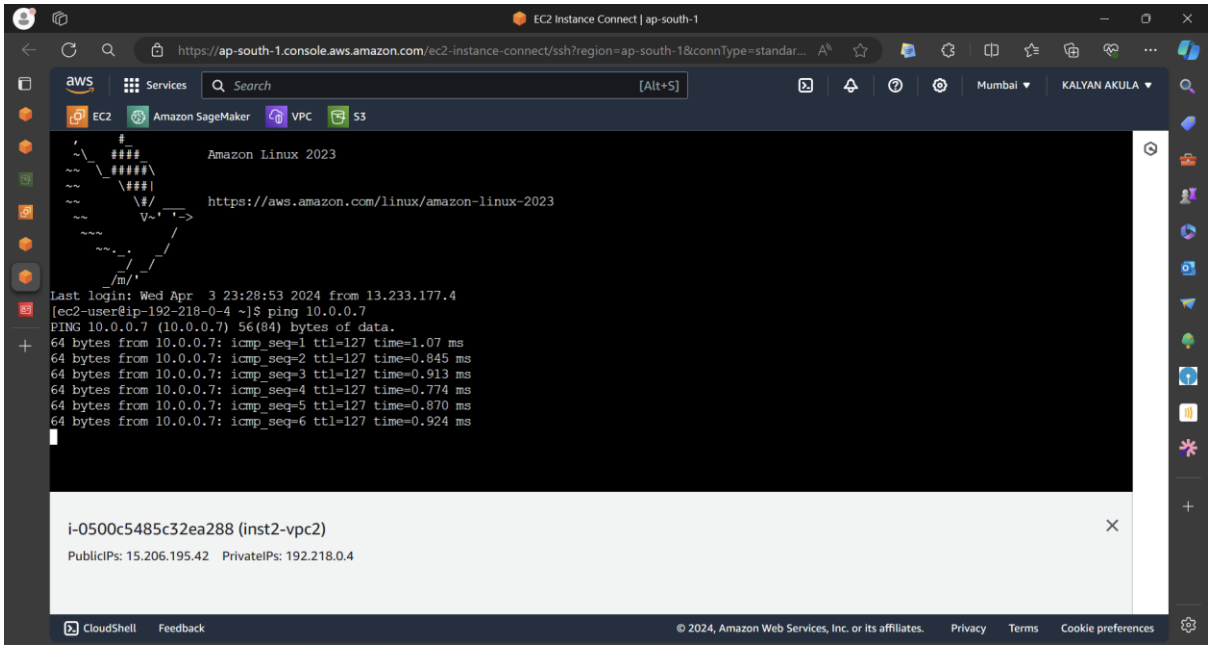


Step 8 : In the same way we need to connect inst2-vpc2 & open Linux interface

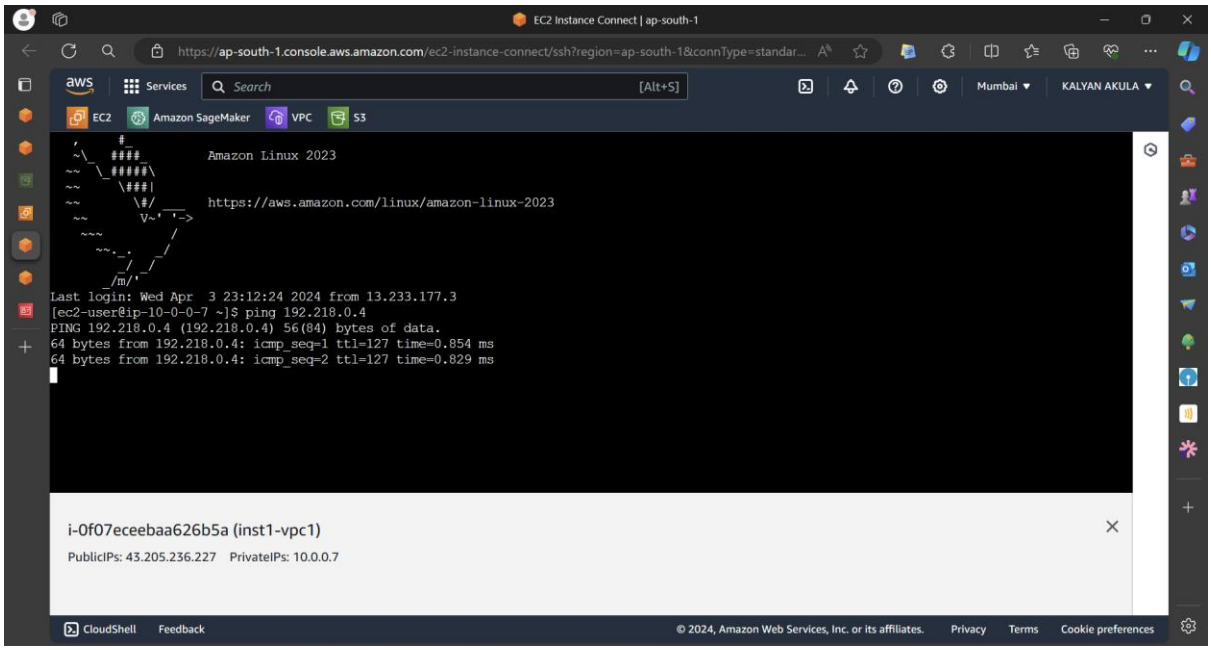


Step 9 : In the linux interface , we need to enter command

- pin [ip of another instance]
    - if it runs successfully , the peering connection is established.

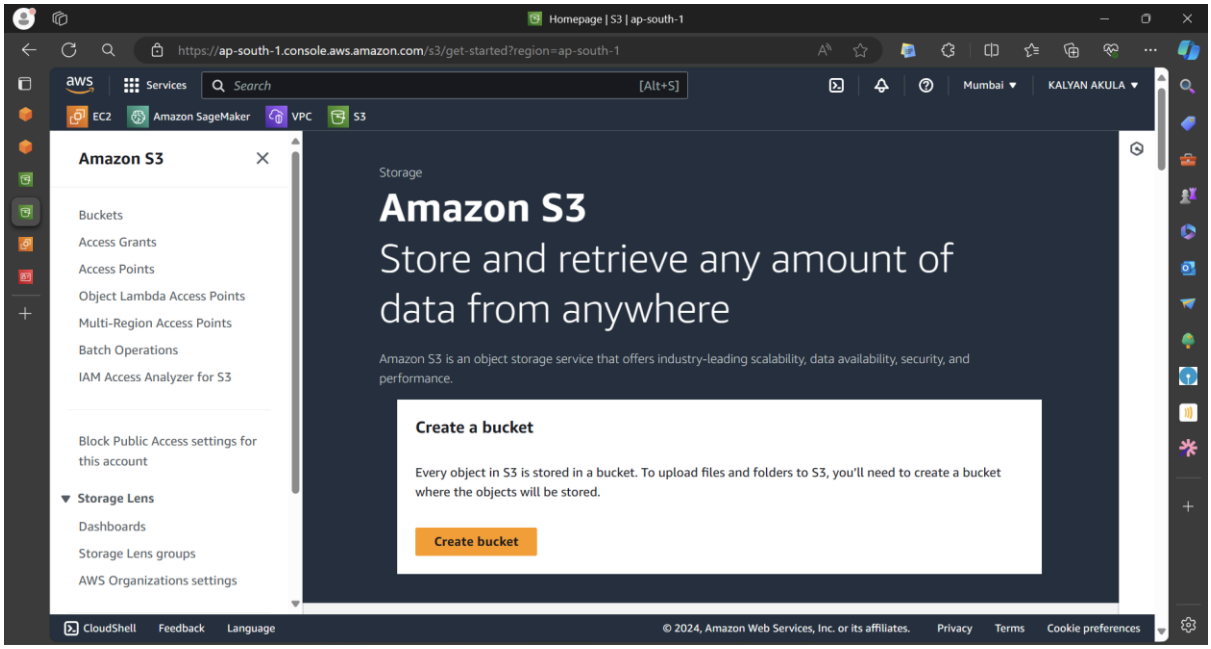


Step 10 : Check same for inst2-vpc2

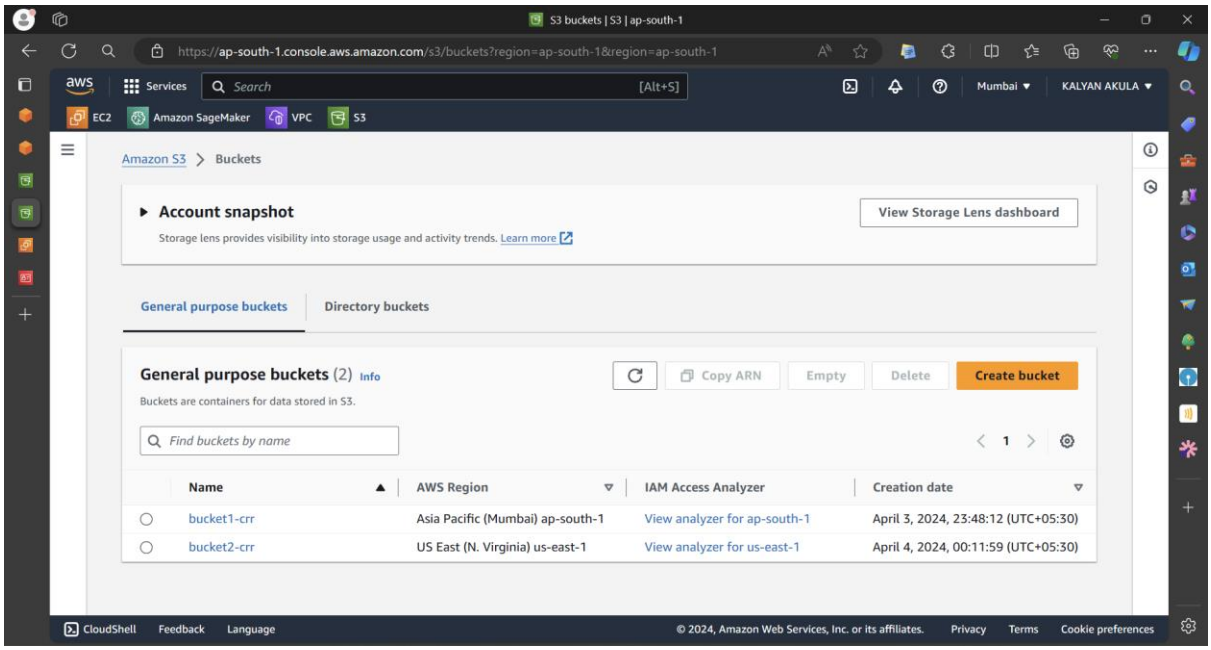


Creating S3 Buckets in 2 different regions & establishing a Cross Region Replication

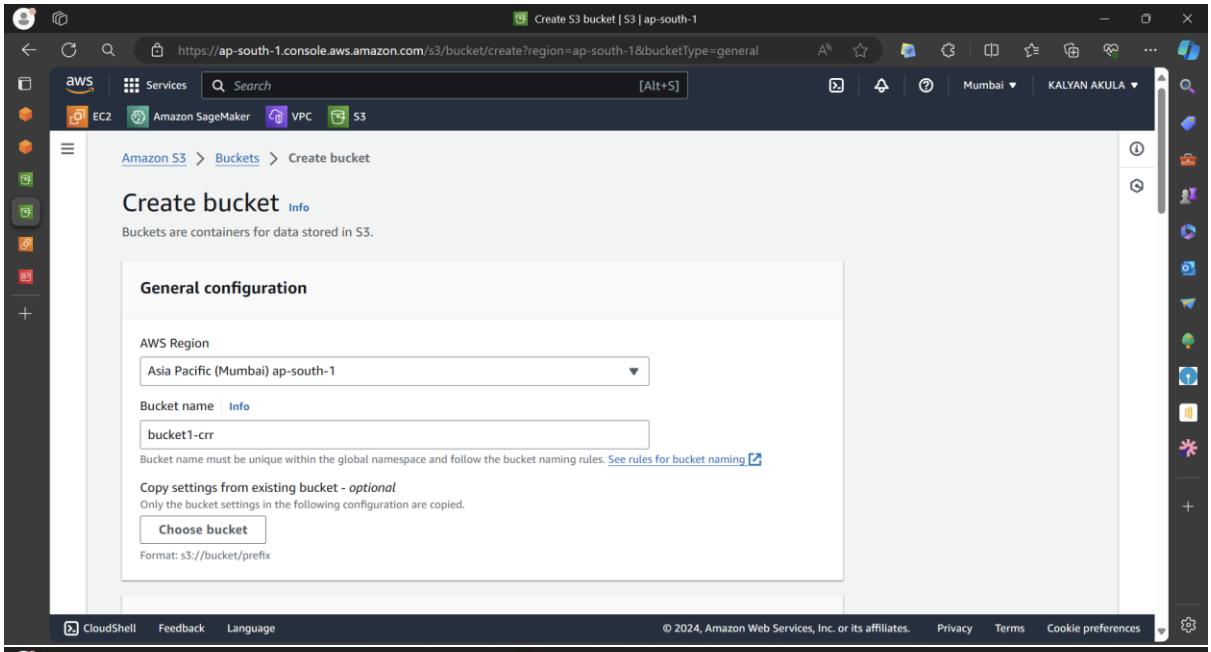
Step 1 : open S3 & click on Buckets

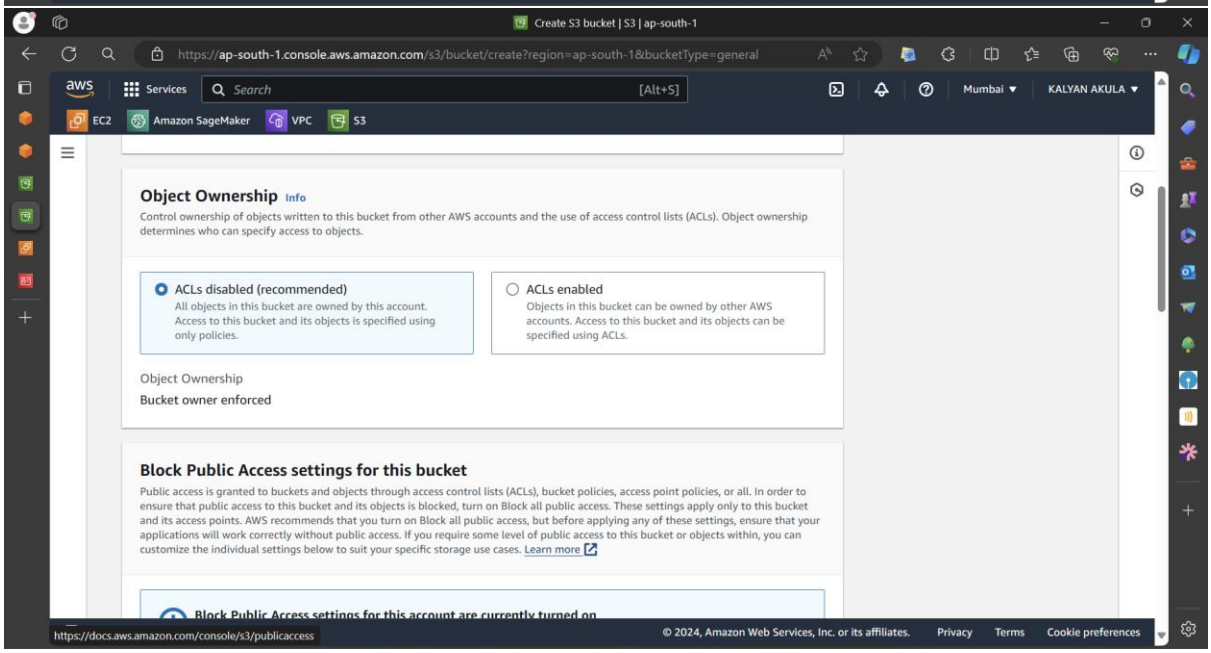


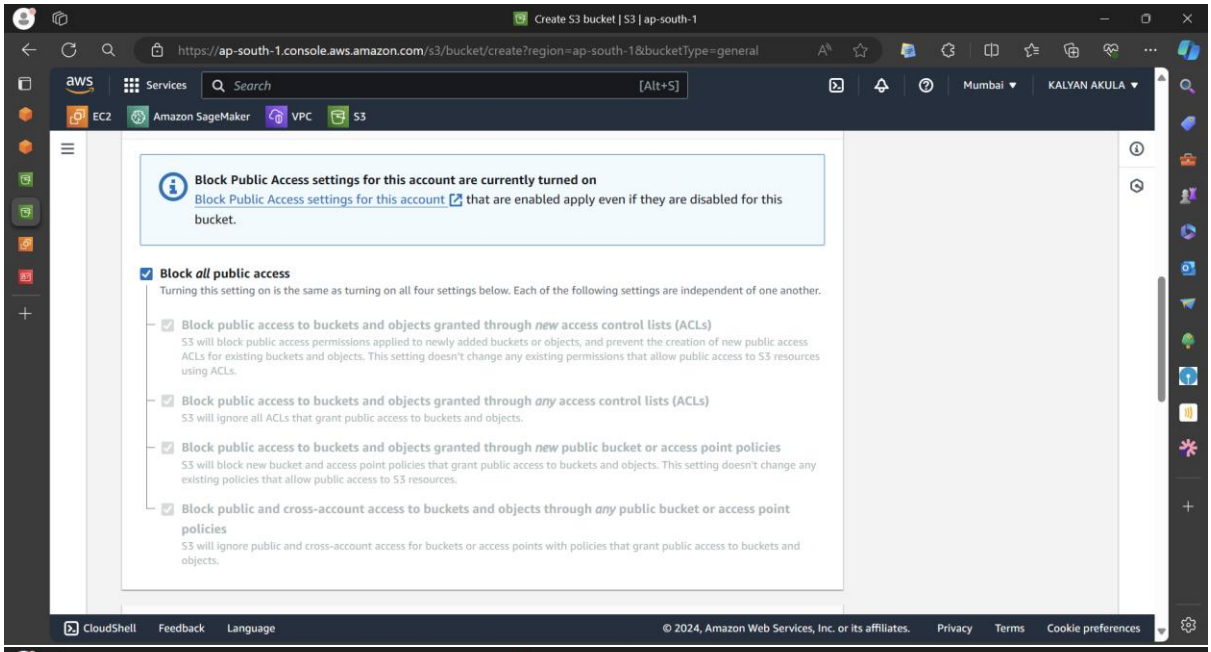
Step 2 : Create a Bucket

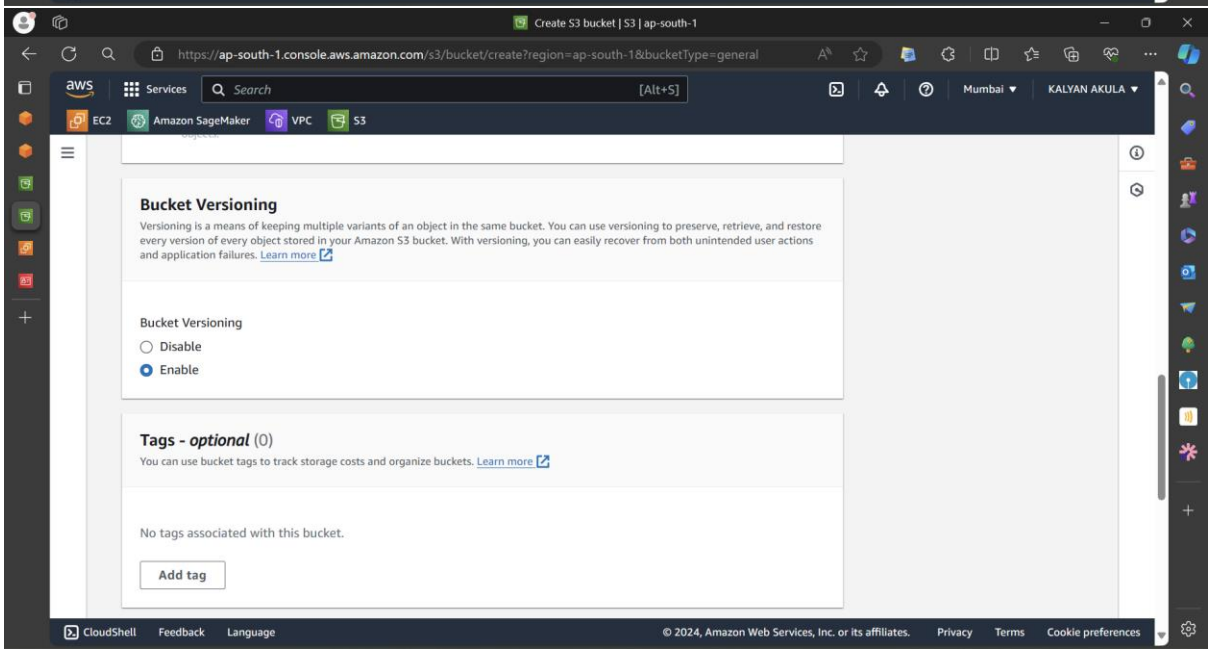


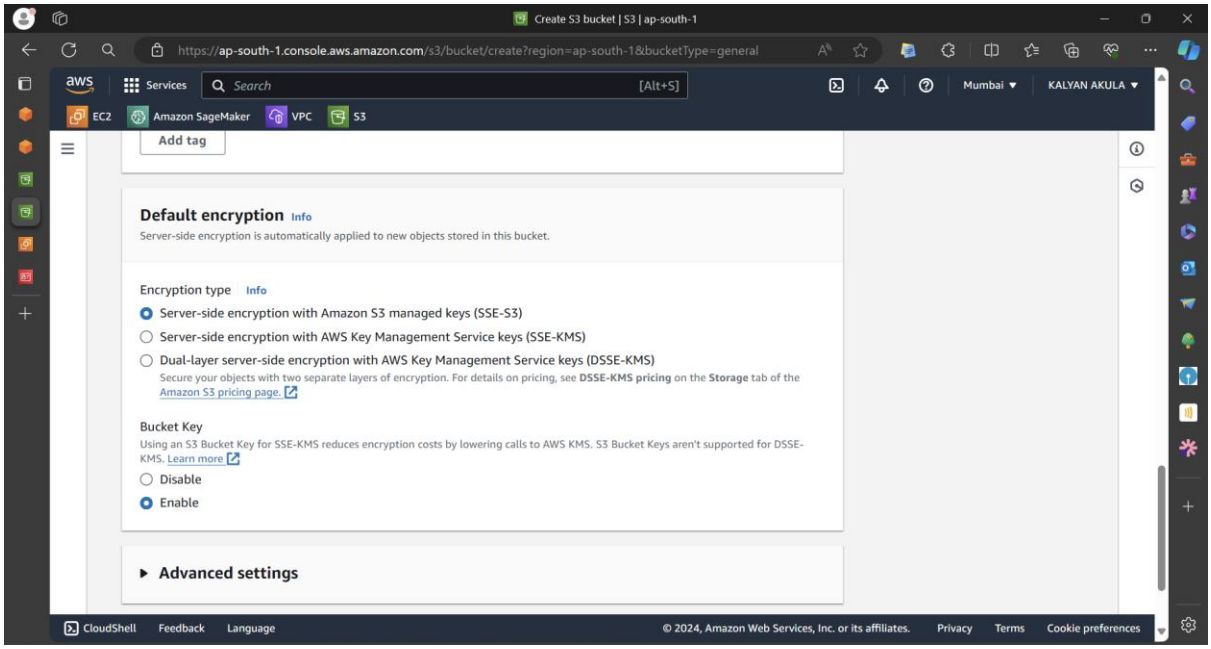
Step 3 : Fill the details as follows


Create S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
Asia Pacific (Mumbai) ap-south-1
Bucket name Info
bucket1-crr
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

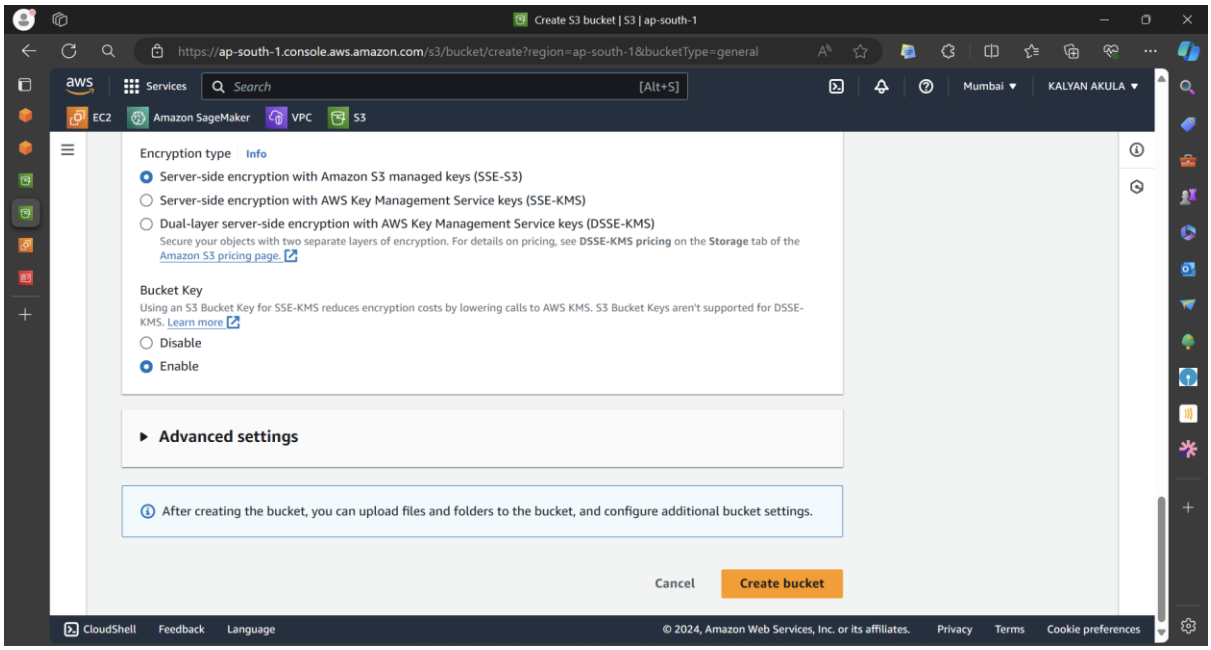

Create S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Bucket owner enforced
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block Public Access settings for this account are currently turned on
https://docs.aws.amazon.com/console/s3/publicaccess
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Create S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Block Public Access settings for this account are currently turned on
Block Public Access settings for this account that are enabled apply even if they are disabled for this bucket.
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

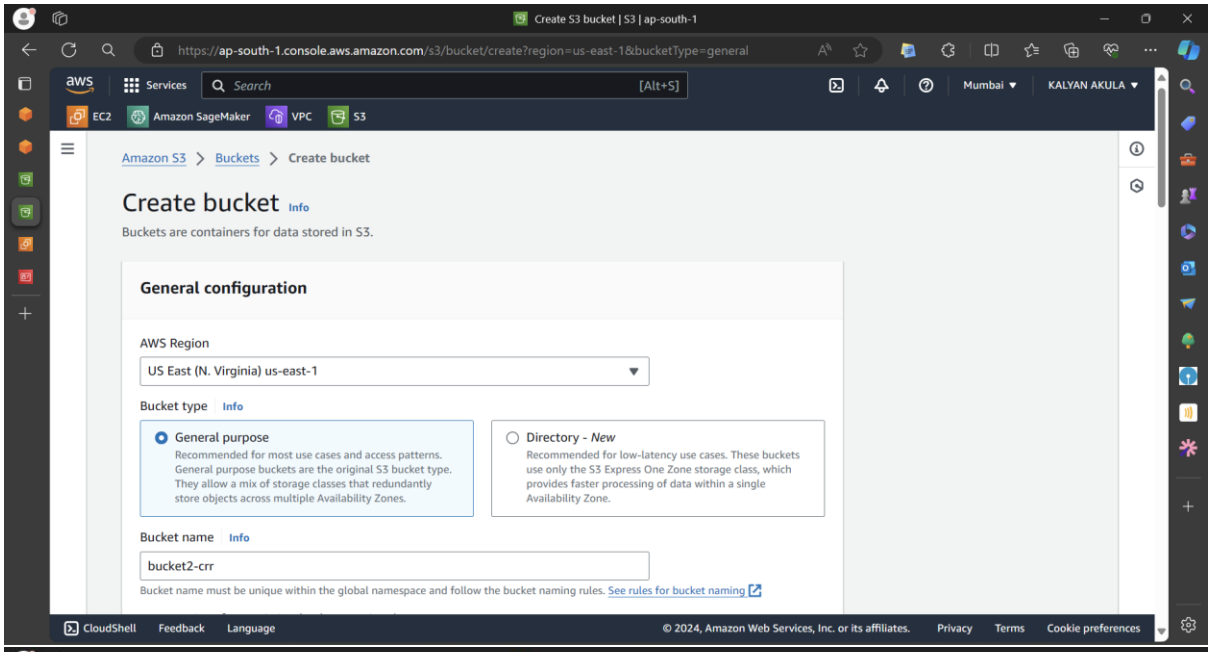

Create S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disable
Enable
Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add tag
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

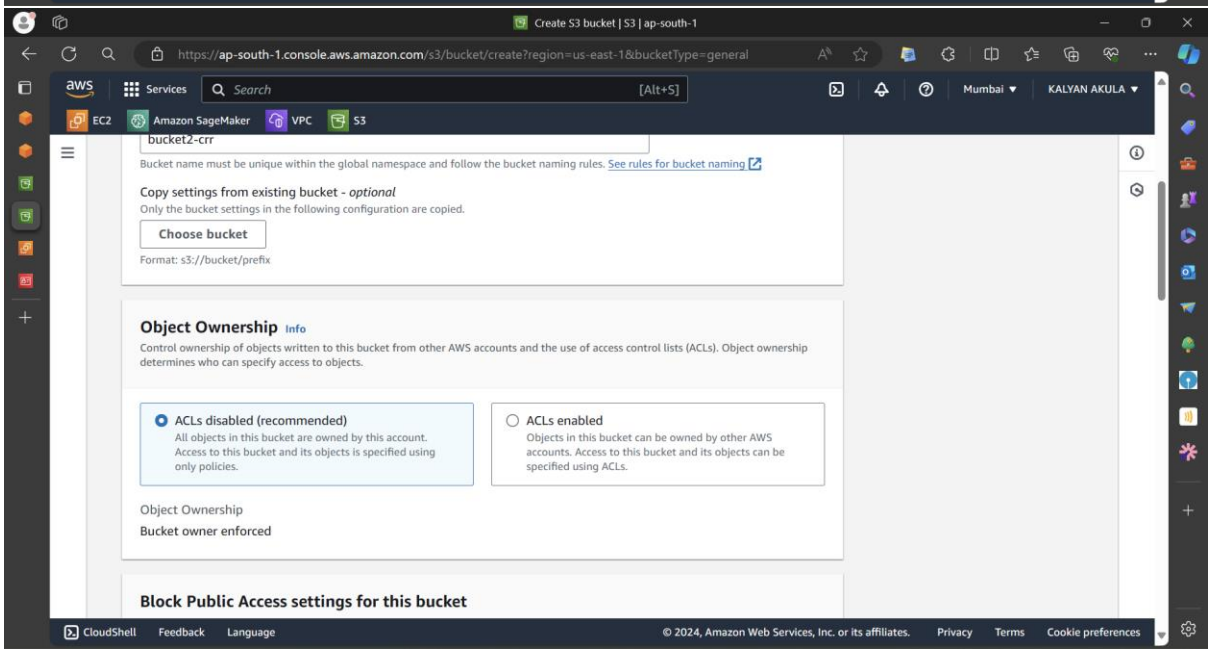


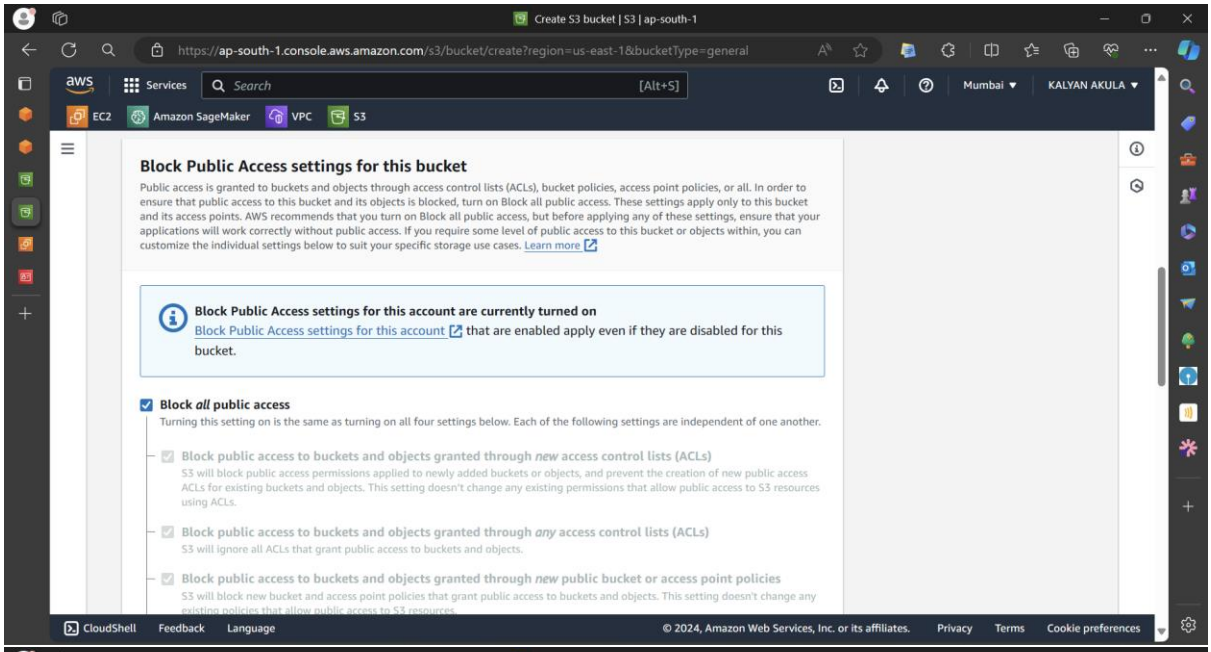
Step 4 : Click on Create Bucket

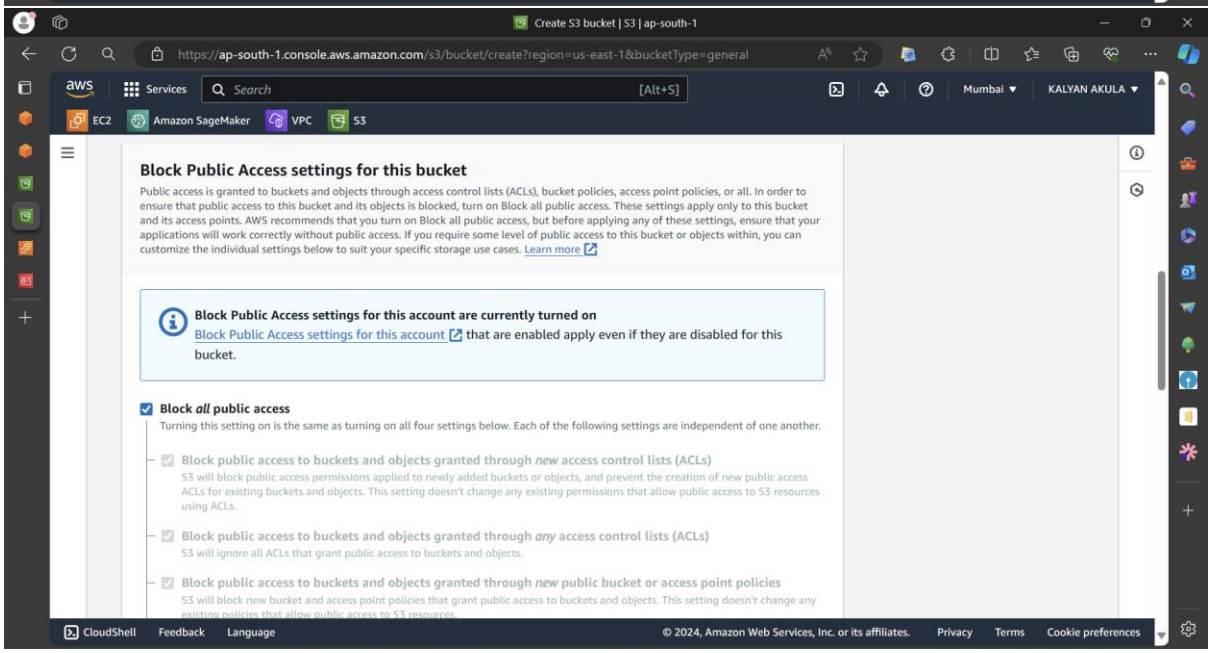


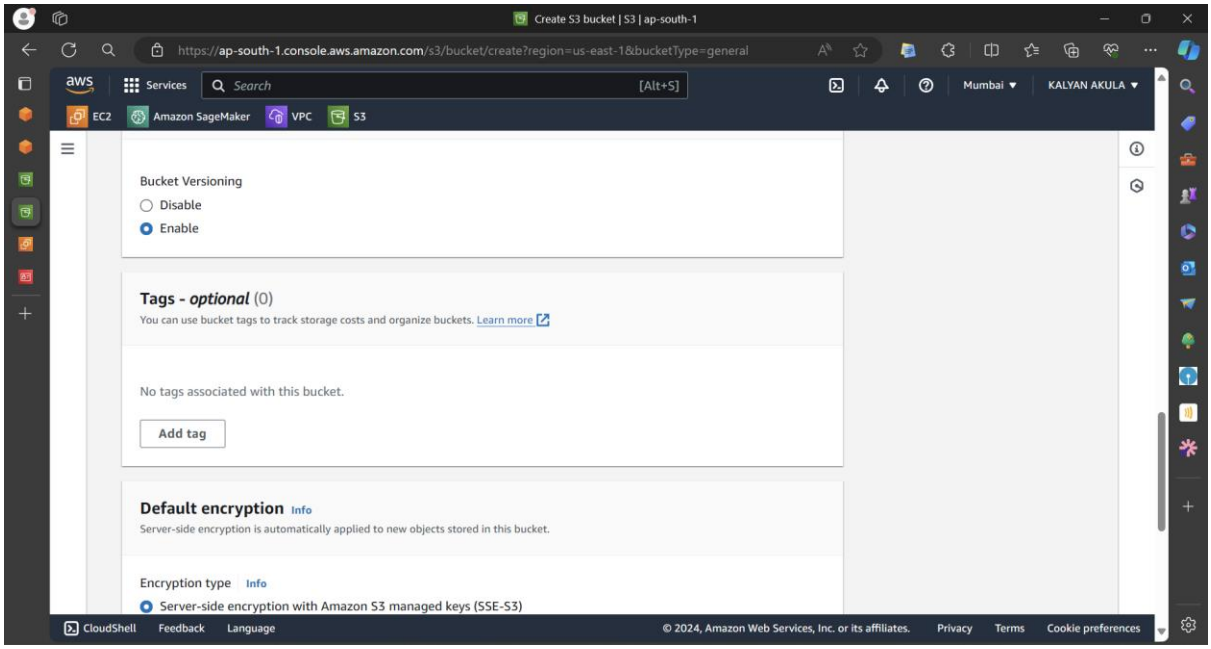
Step 5 : Again create a Bucket with the following details


Create S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
US East (N. Virginia) us-east-1
Bucket type Info
General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
Directory - New
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.
Bucket name Info
bucket2-crr
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

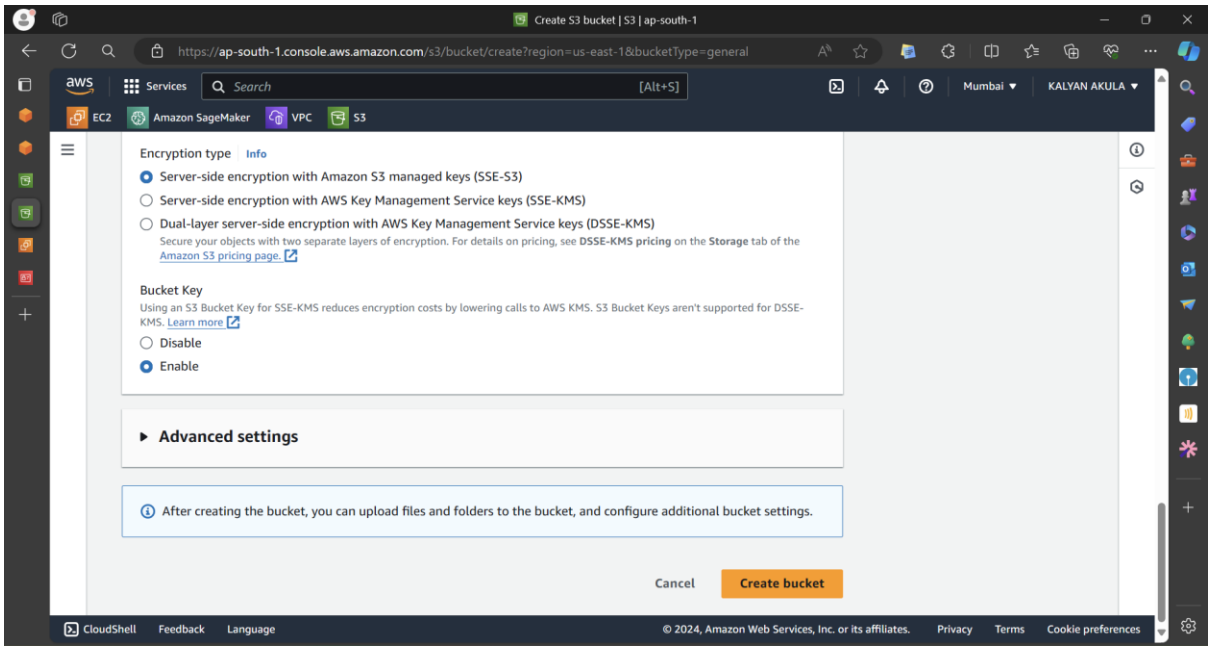

Create S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
bucket2-crr
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Bucket owner enforced
Block Public Access settings for this bucket
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Create S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block Public Access settings for this account are currently turned on
Block Public Access settings for this account that are enabled apply even if they are disabled for this bucket.
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

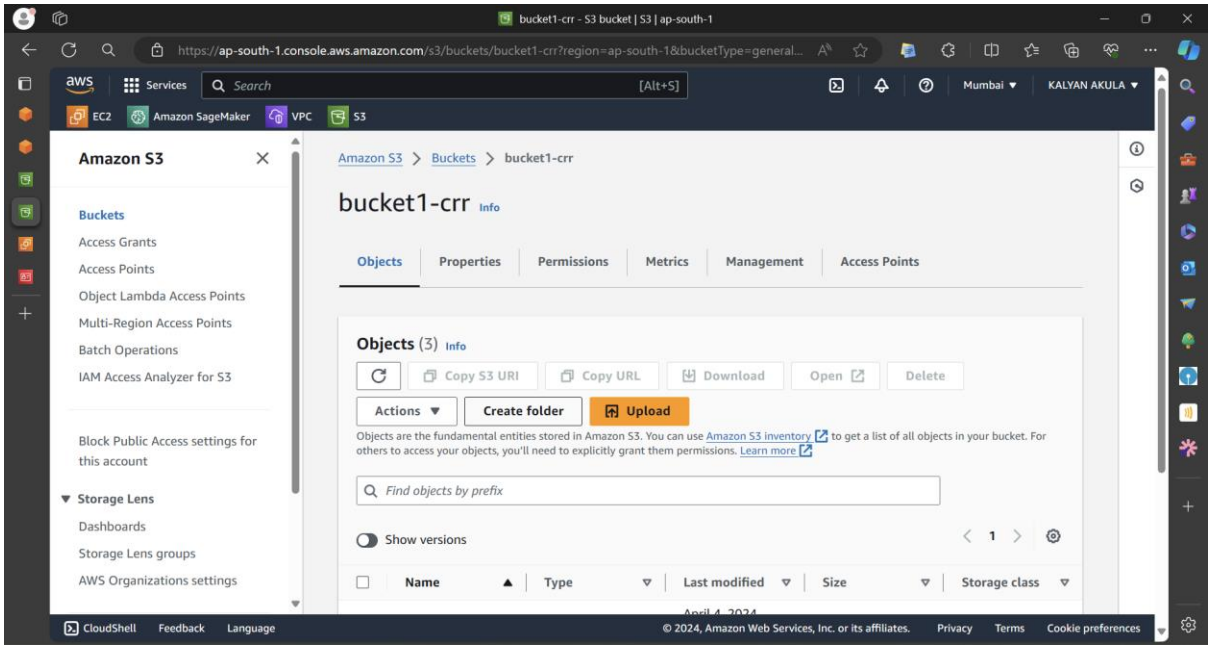

Create S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block Public Access settings for this account are currently turned on
Block Public Access settings for this account that are enabled apply even if they are disabled for this bucket.
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



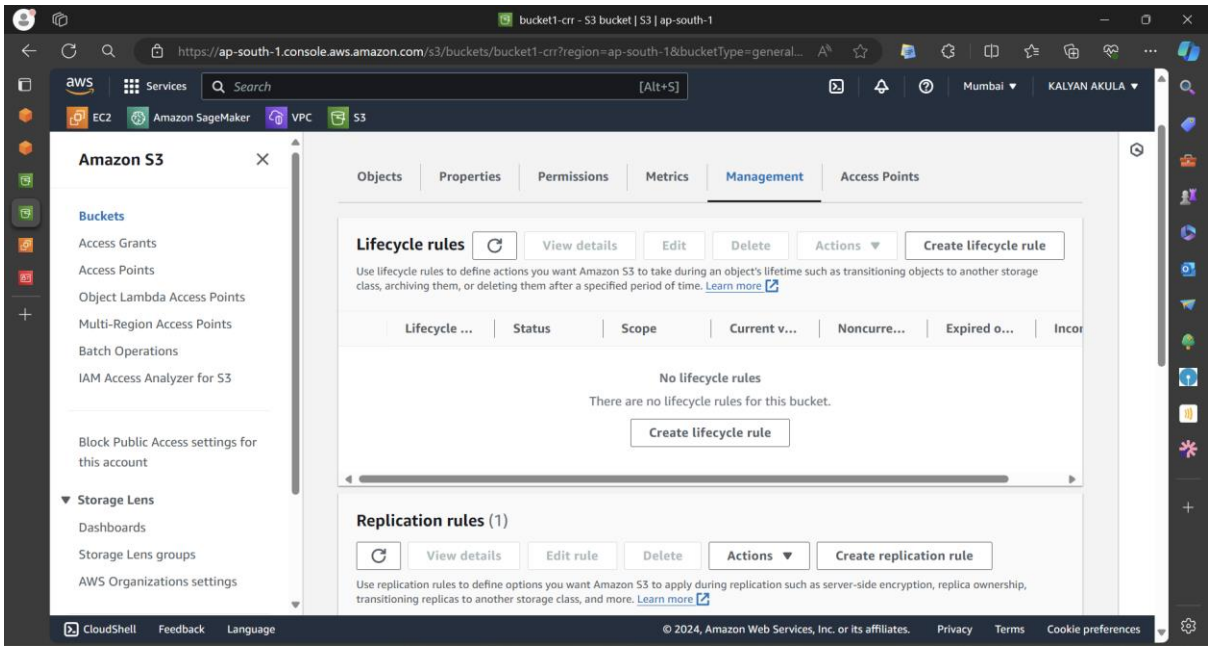
Step 6 : Click on Create Bucket



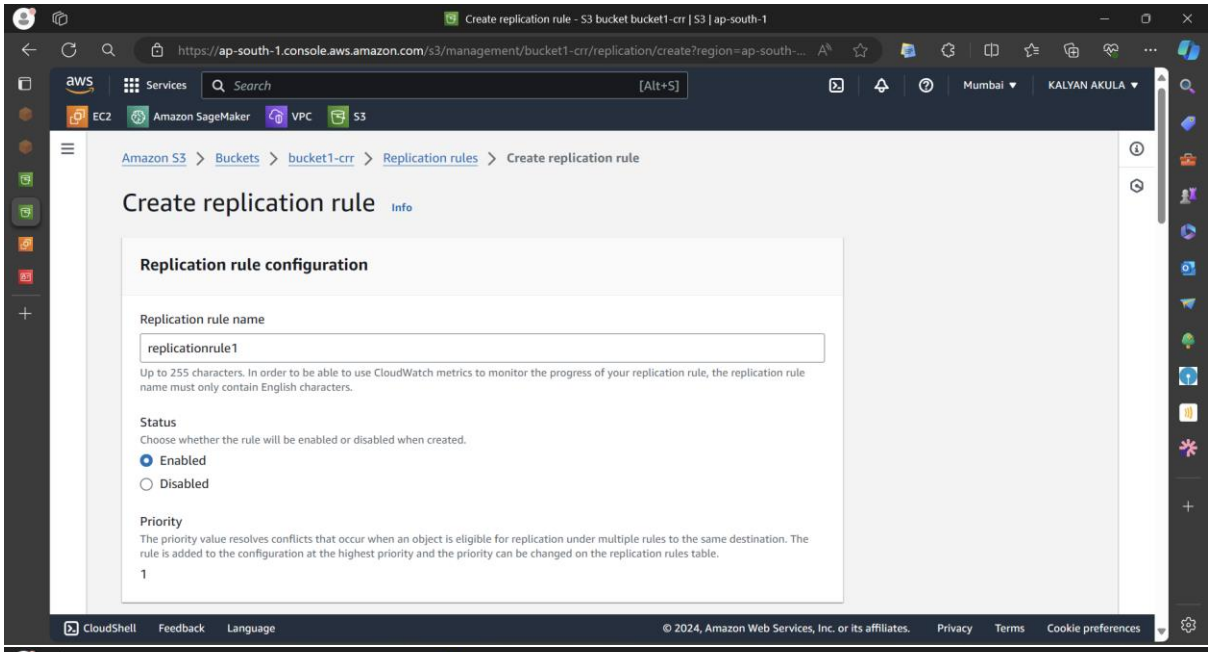
Step 7 : Click on Bucket1-crr

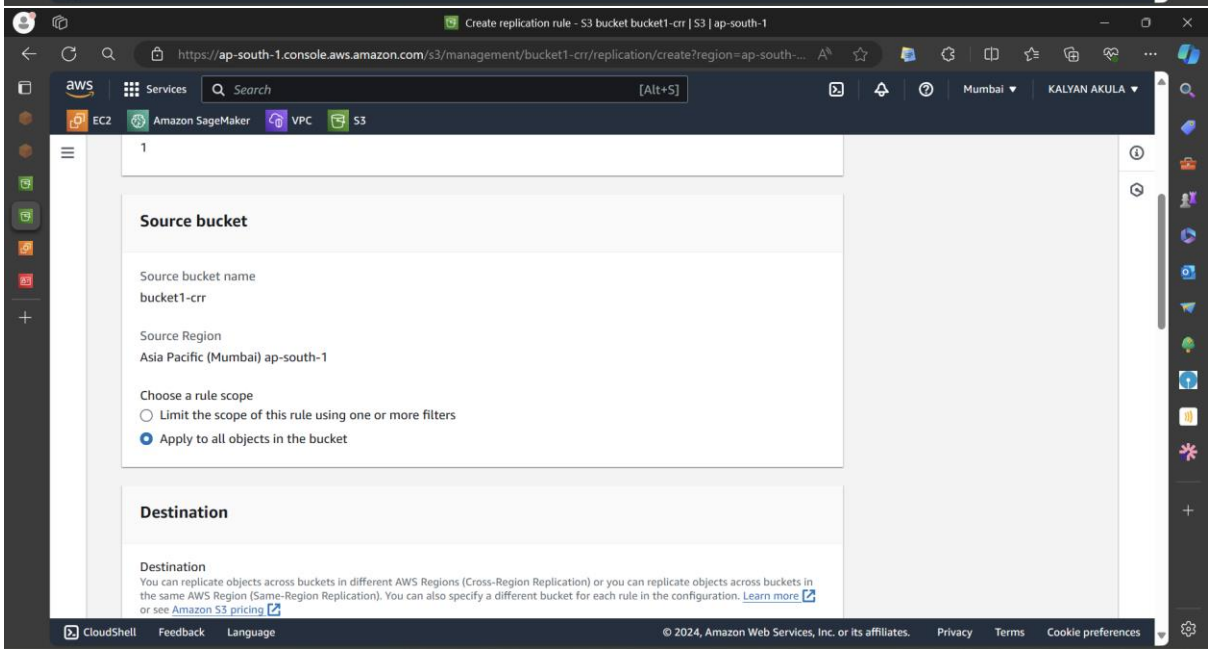


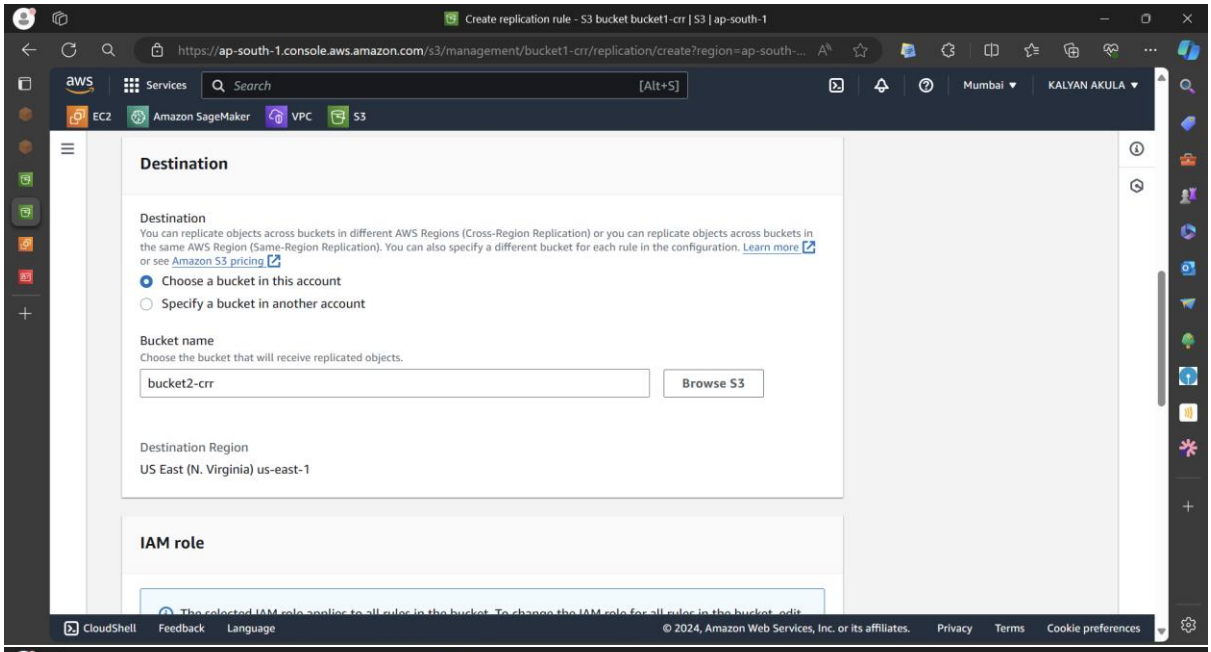
Step 8 : Click on Management , in Replication rules Click on Create replication rule

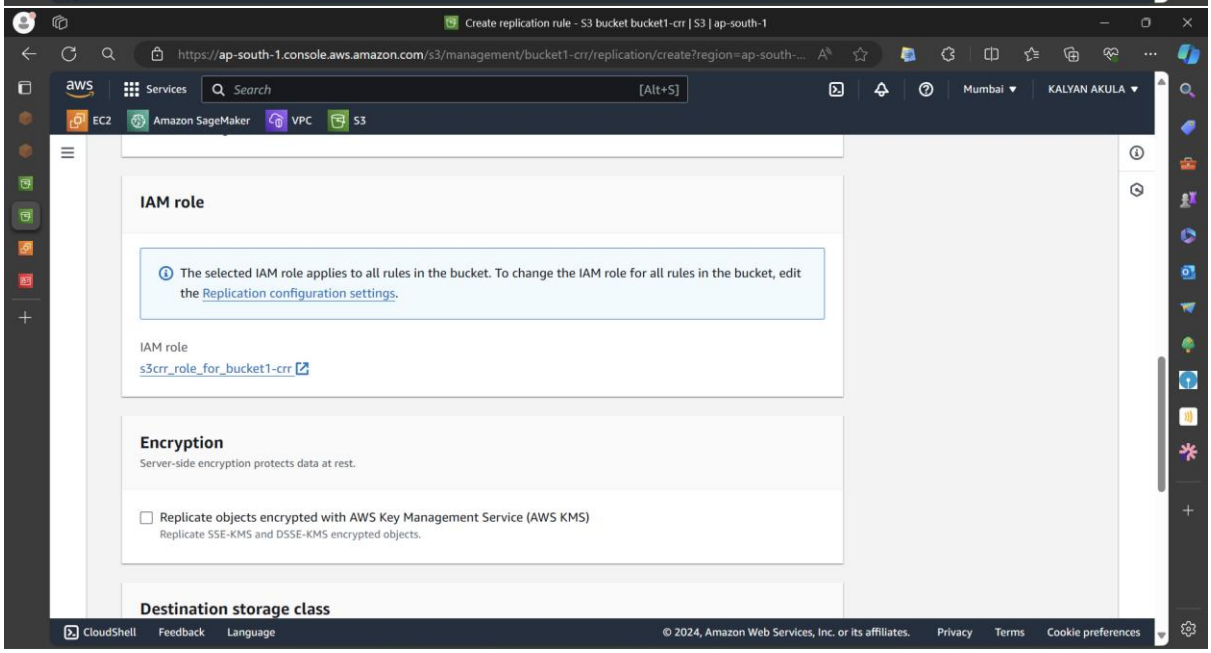


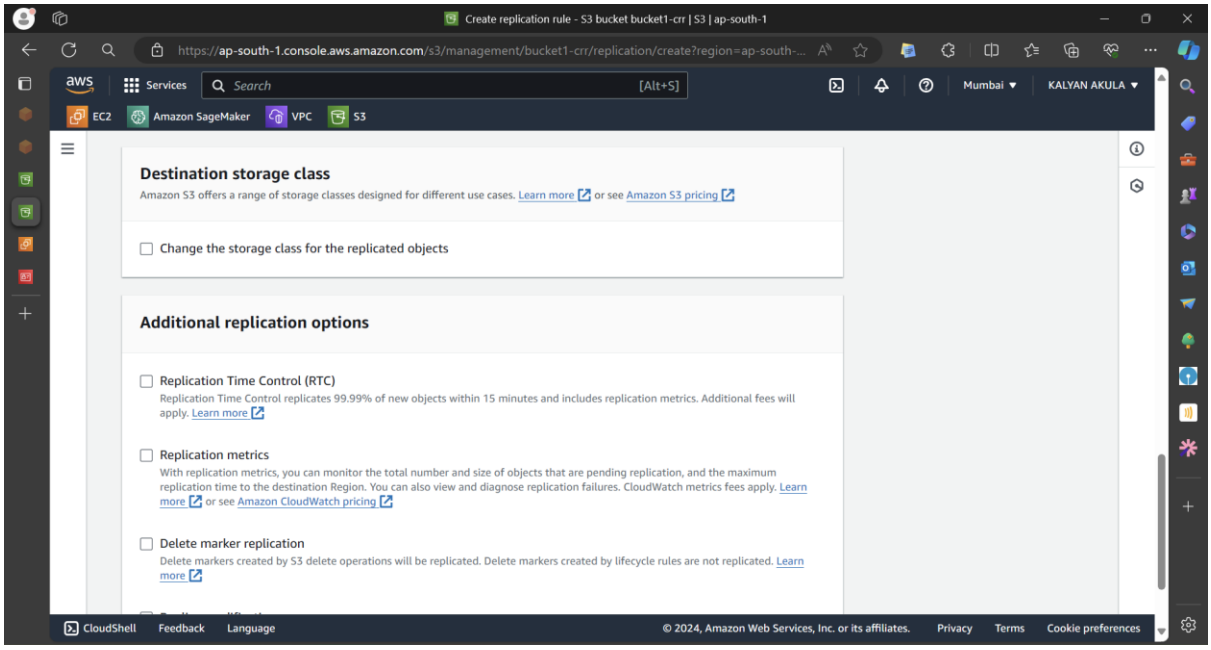
Step 9 : Fill the data as follows


Create replication rule - S3 bucket bucket1-crr | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/management/bucket1-crr/replication/create?region=ap-south-...
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Amazon S3 > Buckets > bucket1-crr > Replication rules > Create replication rule
Create replication rule Info
Replication rule configuration
Replication rule name
replicationrule1
Up to 255 characters. In order to be able to use CloudWatch metrics to monitor the progress of your replication rule, the replication rule name must only contain English characters.
Status
Choose whether the rule will be enabled or disabled when created.
Enabled
Disabled
Priority
The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.
1
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

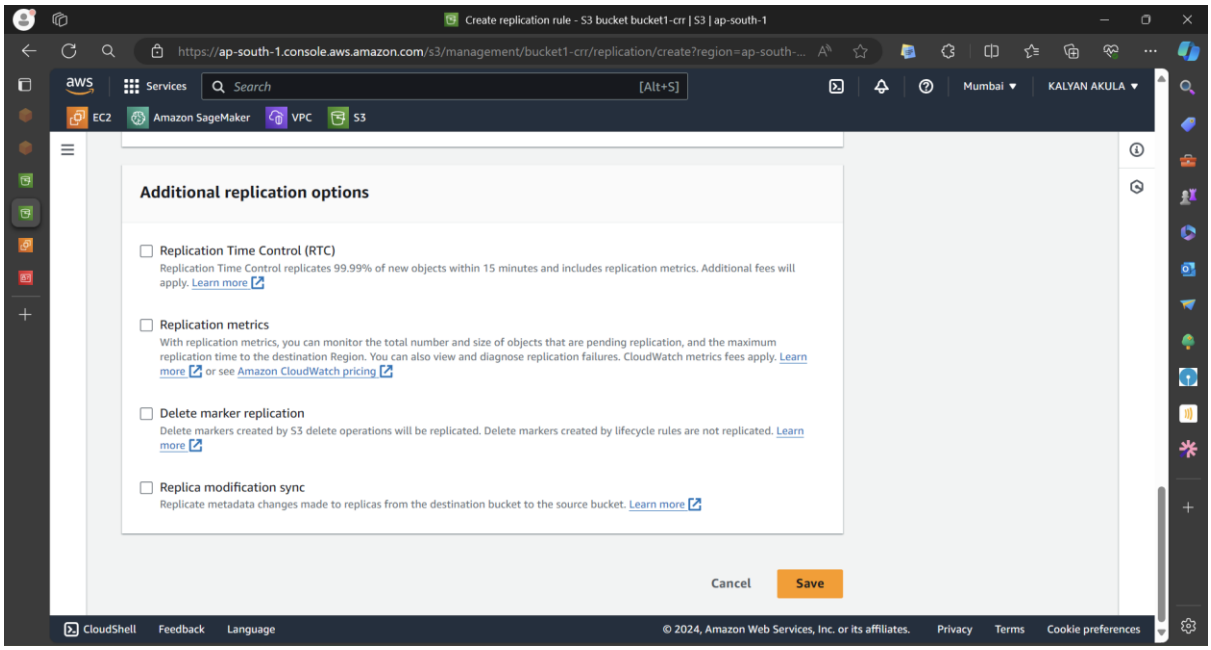

Create replication rule - S3 bucket bucket1-crr | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/management/bucket1-crr/replication/create?region=ap-south-...
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
1
Source bucket
Source bucket name
bucket1-crr
Source Region
Asia Pacific (Mumbai) ap-south-1
Choose a rule scope
Limit the scope of this rule using one or more filters
Apply to all objects in the bucket
Destination
Destination
You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. Learn more
or see Amazon S3 pricing
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Create replication rule - S3 bucket bucket1-crr | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/management/bucket1-crr/replication/create?region=ap-south-...
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Destination
Destination
You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. Learn more or see Amazon S3 pricing
Choose a bucket in this account
Specify a bucket in another account
Bucket name
Choose the bucket that will receive replicated objects.
bucket2-crr
Browse S3
Destination Region
US East (N. Virginia) us-east-1
IAM role
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Create replication rule - S3 bucket bucket1-crr | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/management/bucket1-crr/replication/create?region=ap-south-...
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
IAM role
The selected IAM role applies to all rules in the bucket. To change the IAM role for all rules in the bucket, edit the Replication configuration settings.
IAM role
s3crr_role_for_bucket1-crr
Encryption
Server-side encryption protects data at rest.
Replicate objects encrypted with AWS Key Management Service (AWS KMS)
Replicate SSE-KMS and DSSE-KMS encrypted objects.
Destination storage class
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

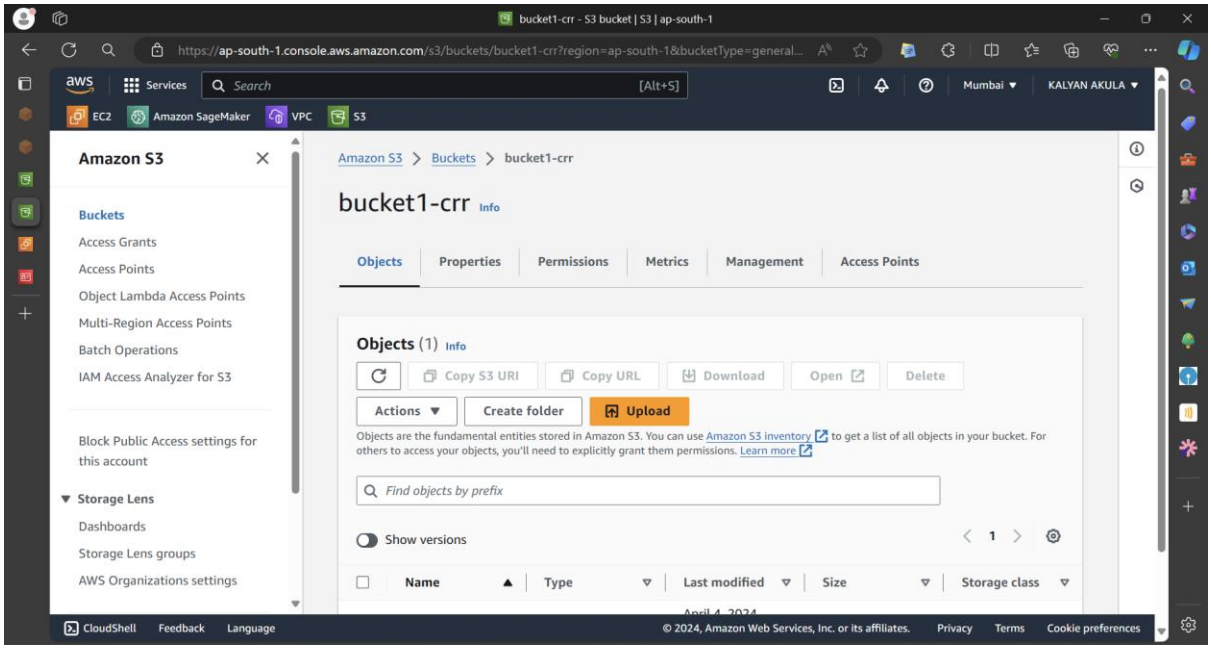


Step 9 : Click on Save



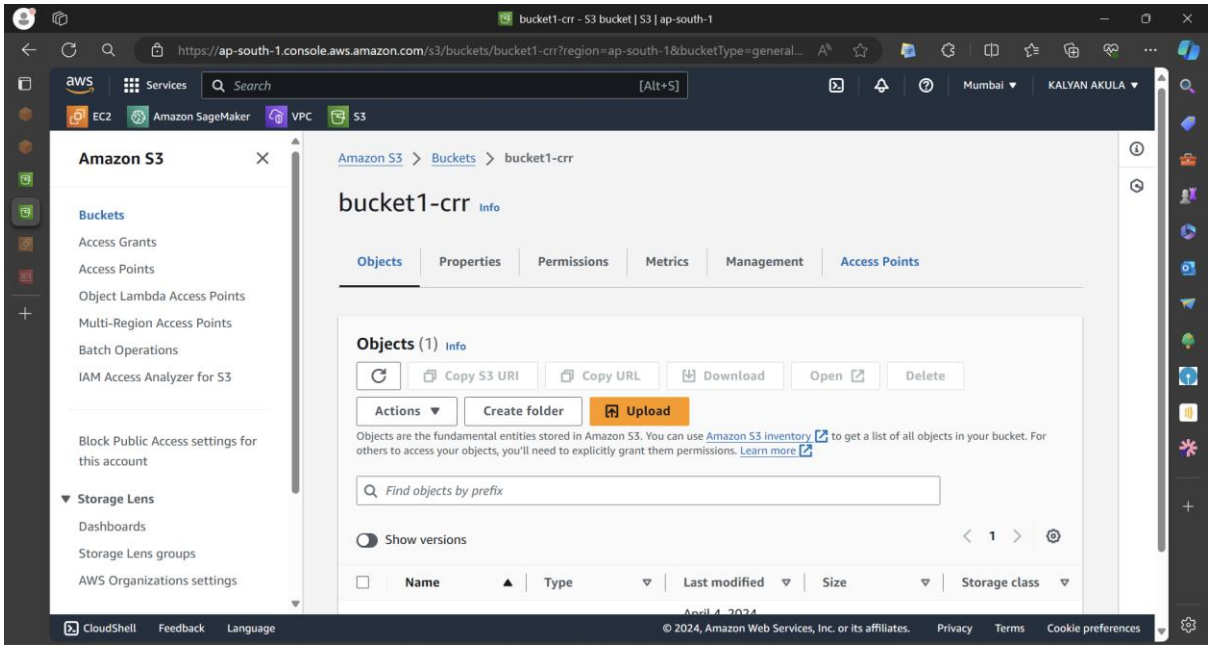
- To check whether the CRR is established or not

Step 10 : open bucket1-crr

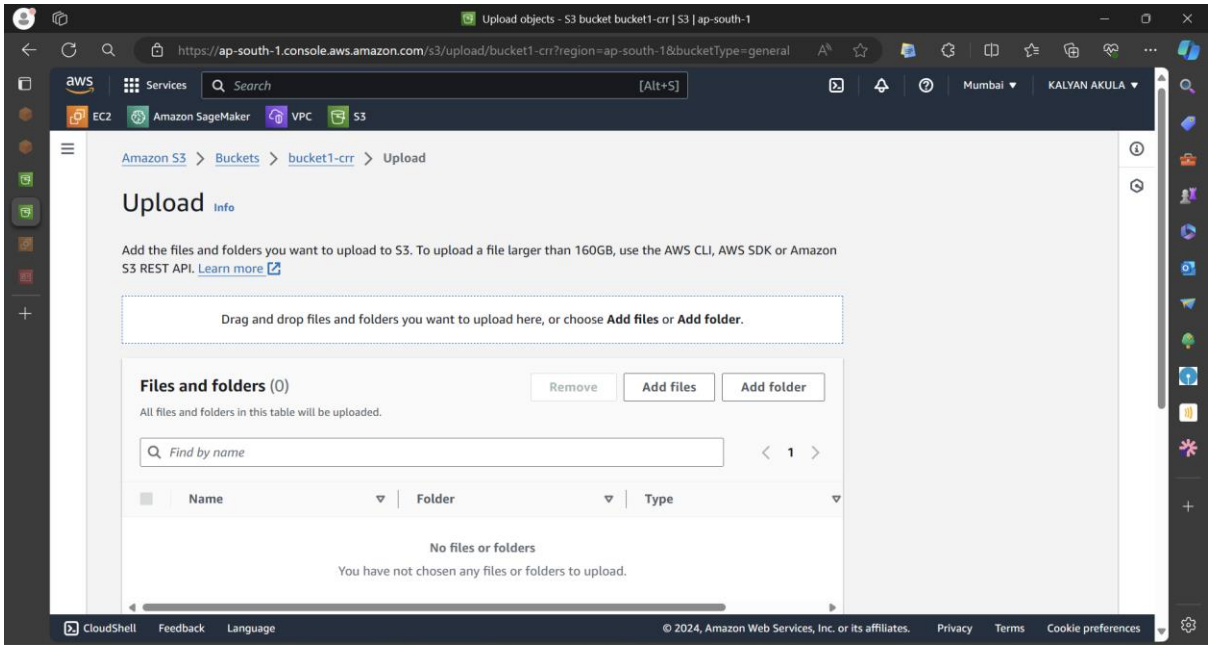


Step 11: Now we need to upload a file in Bucket1-crr & it has to be reflect in Bucket2-crr

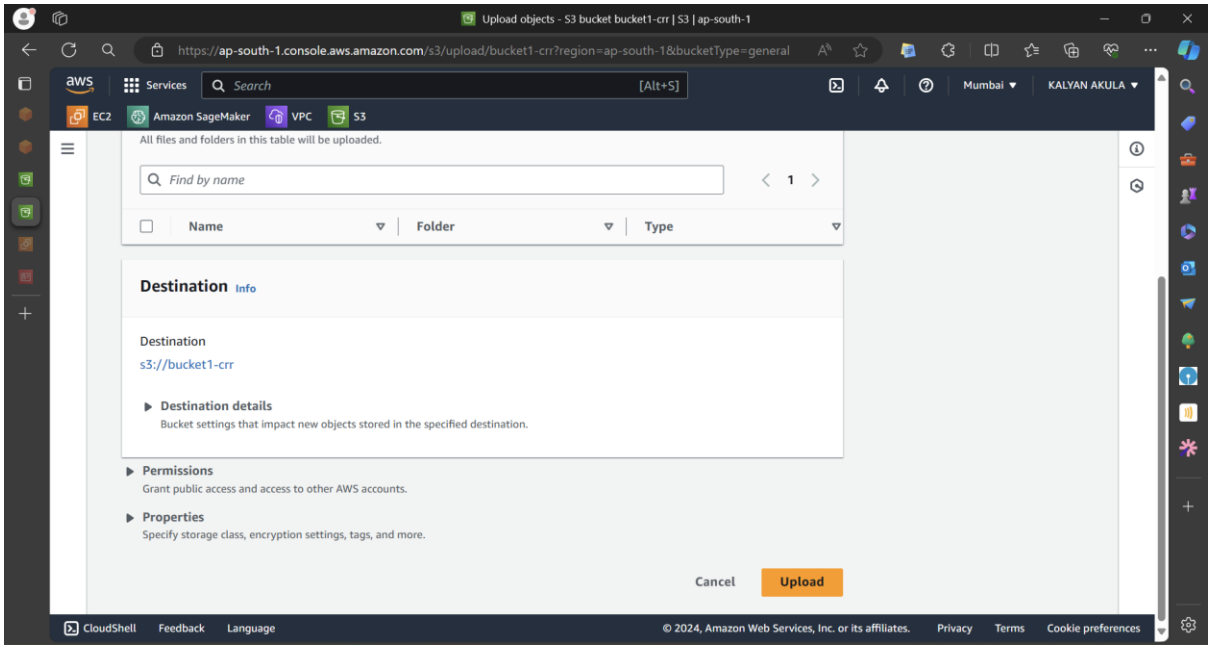
- Click on upload



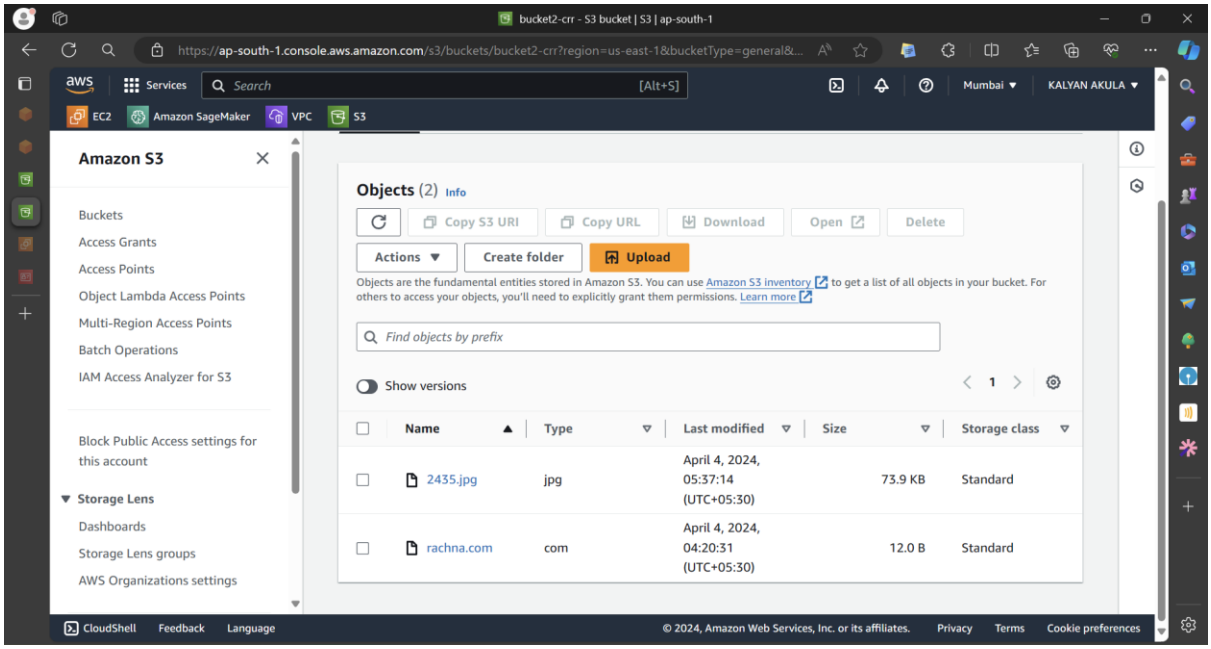
- Click on Add Files



- Add a file & Scroll down , then click on upload



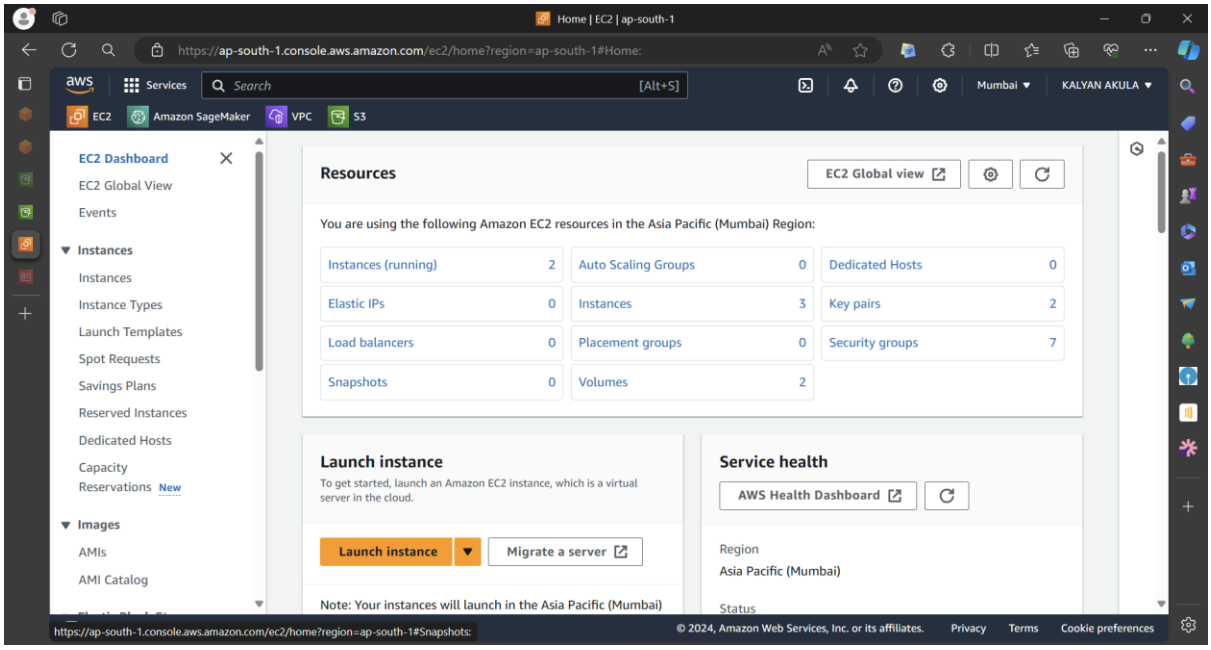
- Now it has to reflect in Bucket2-crr



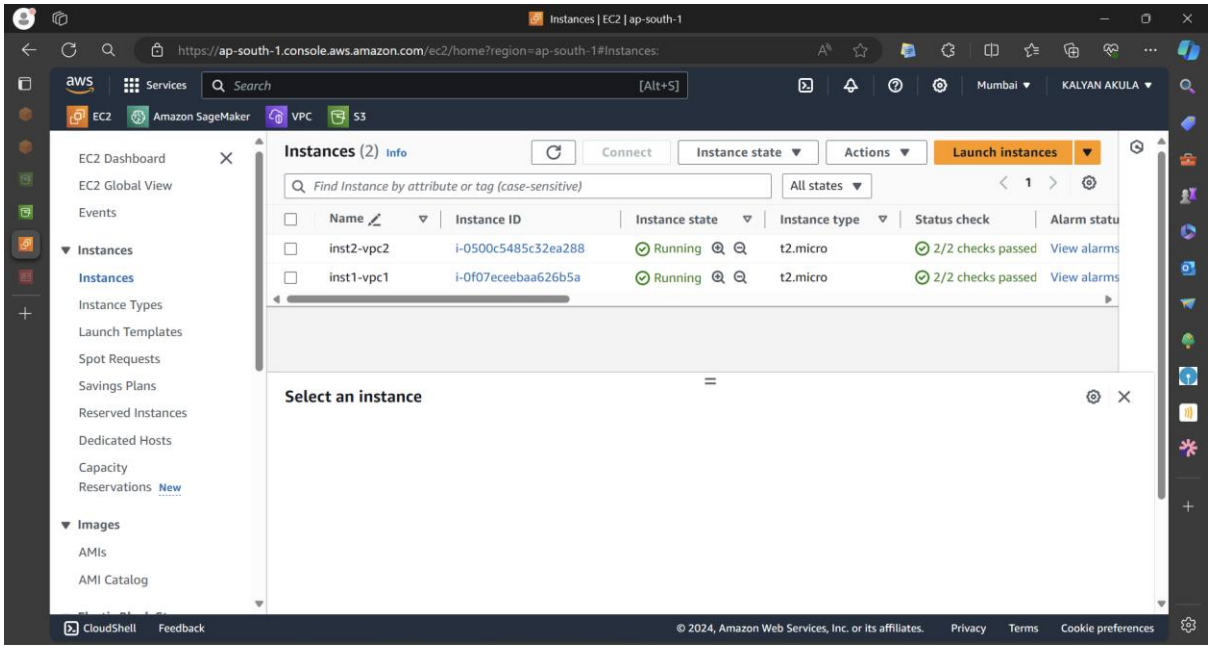
- Here the file gets uploaded . So, the CRR is established

Establishing Connection between VPC's & S3:Bucket1 in the same region

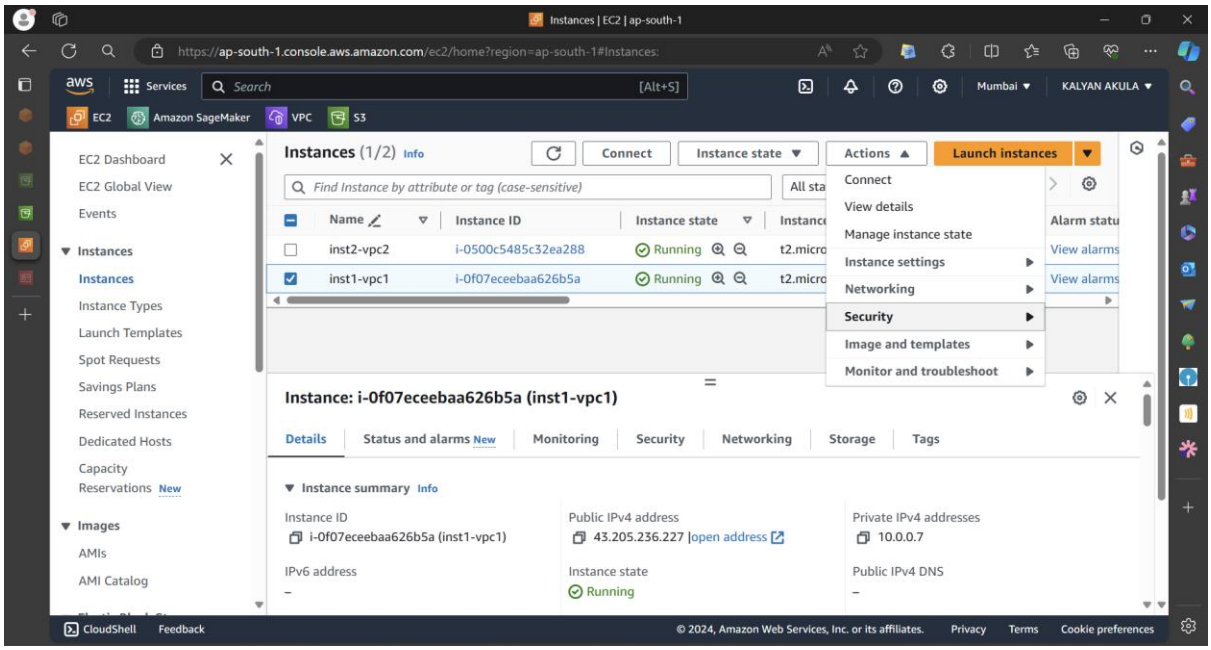
Step 1: Go to EC2 Instance dashboard



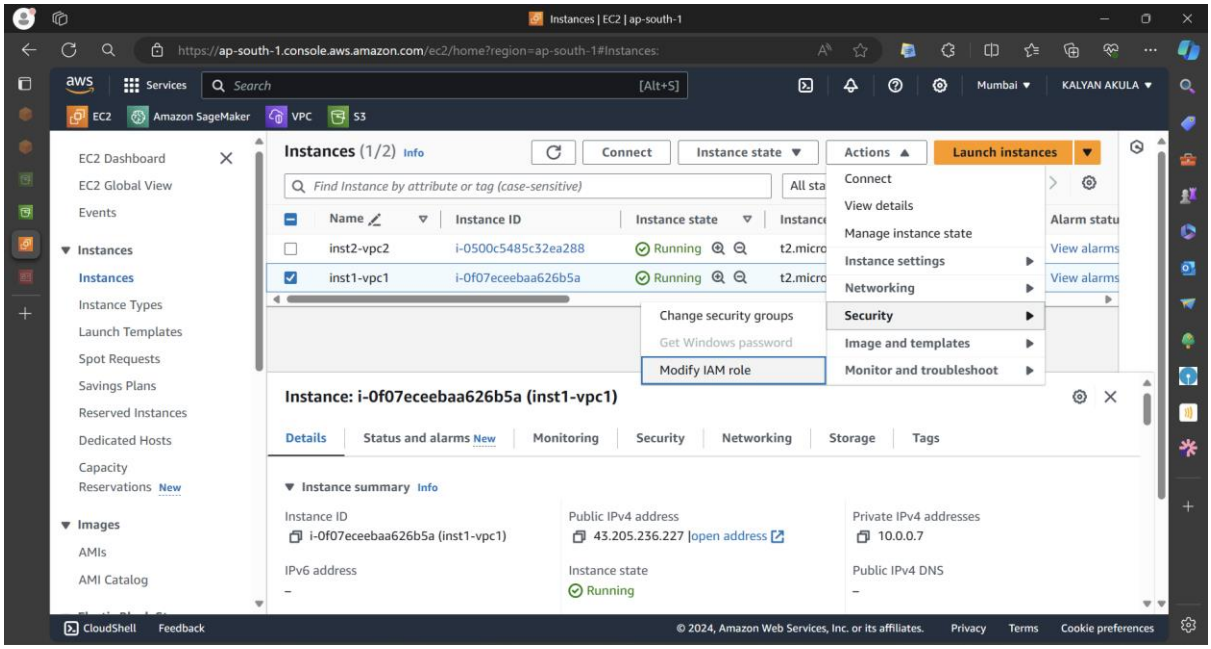
Step 2 : Go to Instances



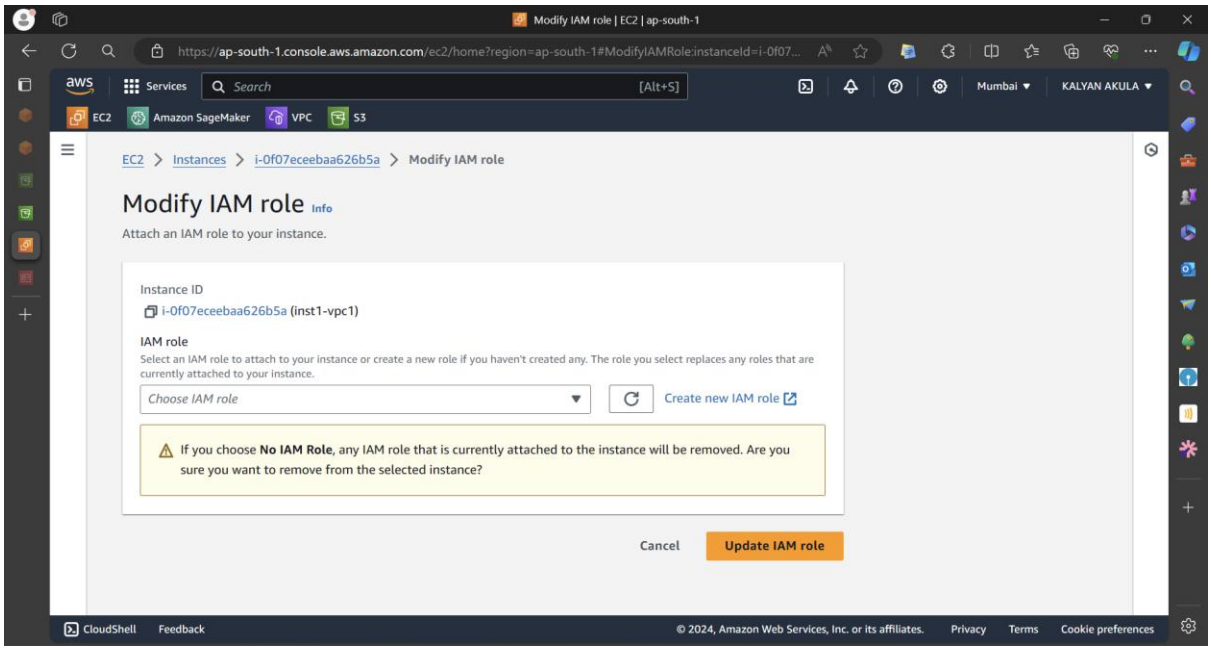
Step 3: Select an instance & Select Actions



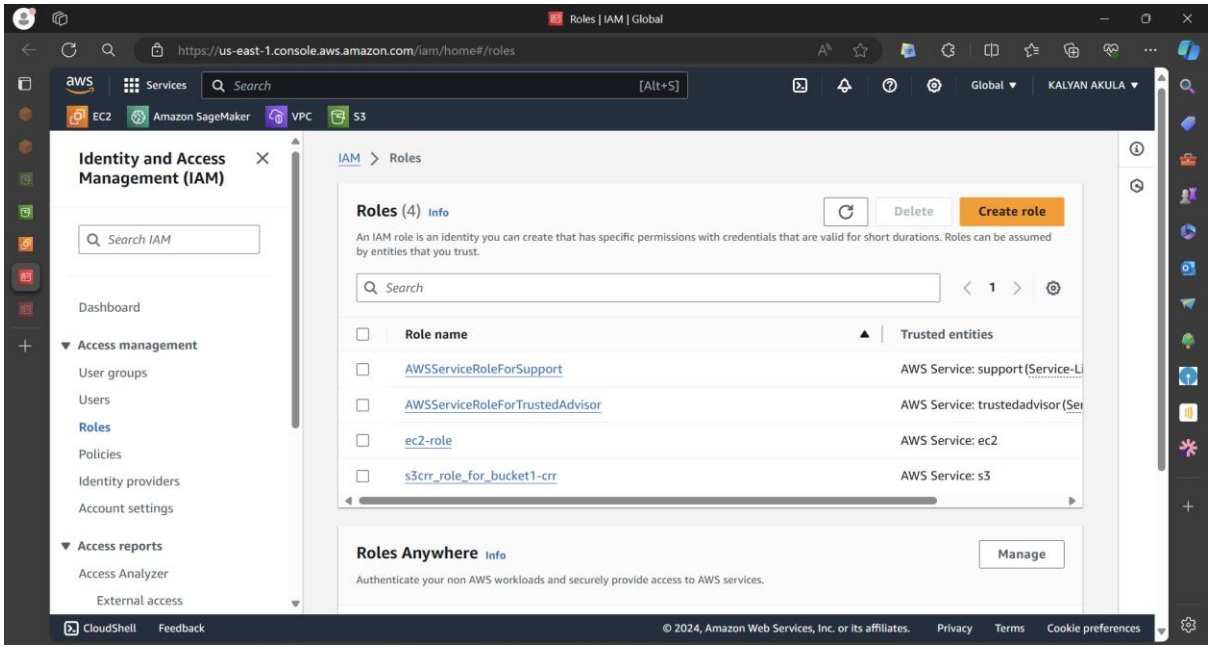
Step 4 : Click on Security & Modify IAM rule



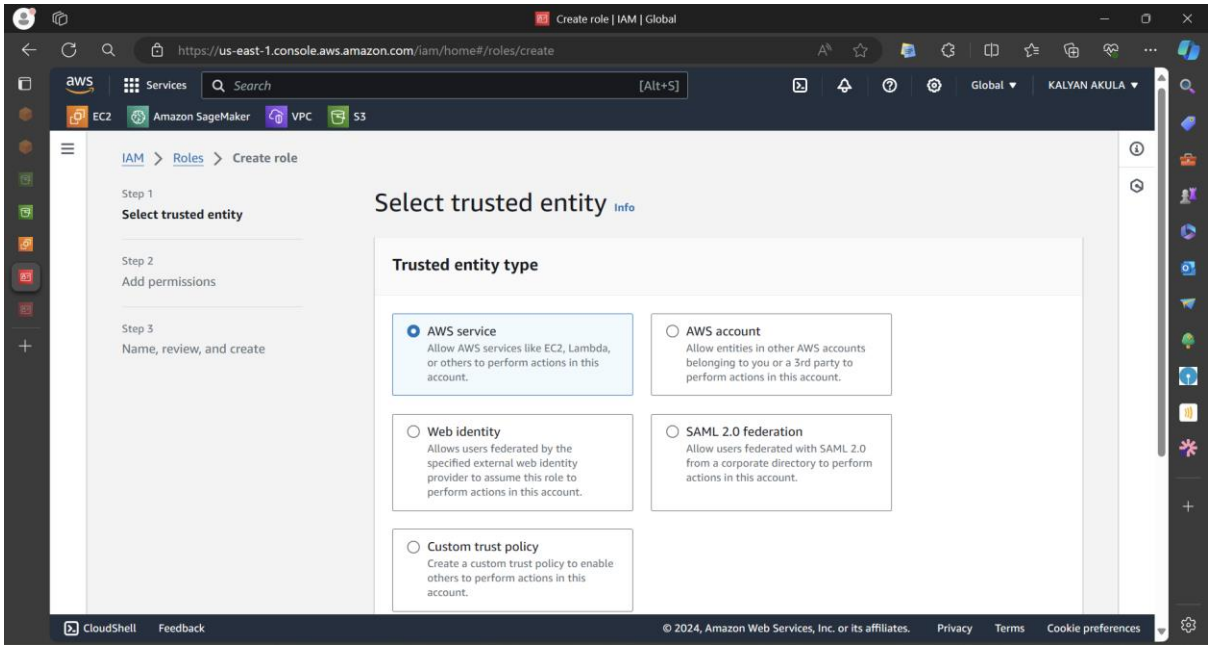
Step 5 : Click on Create new IAM role

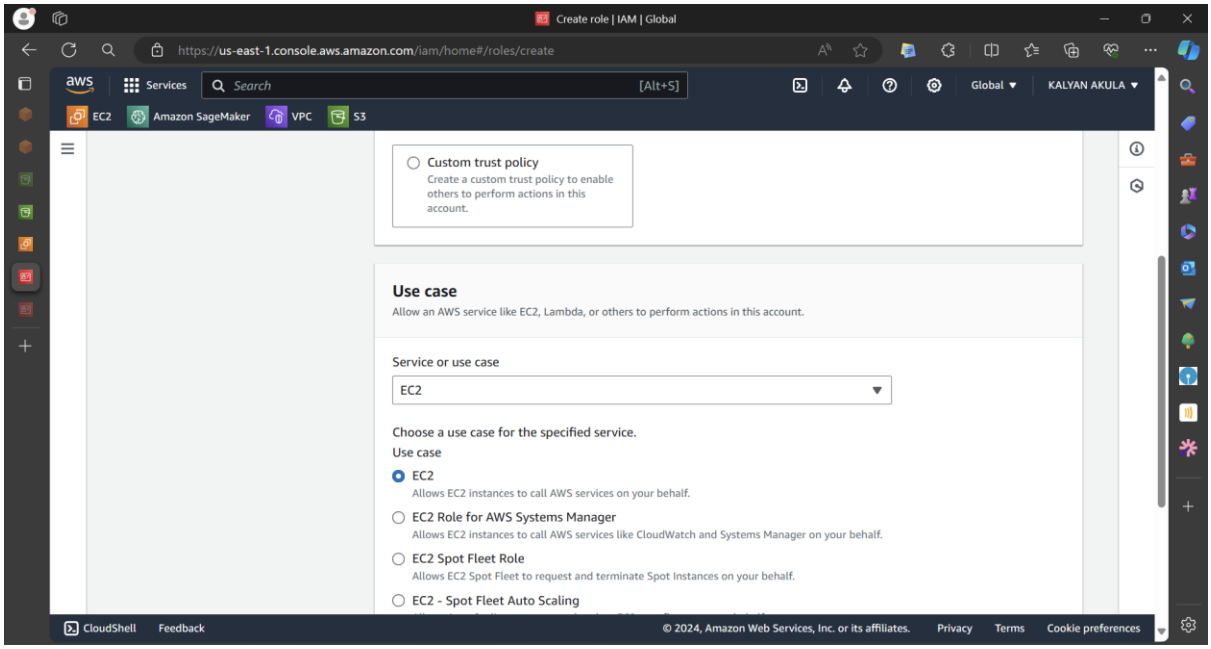


Step 6 : Click on Create Role

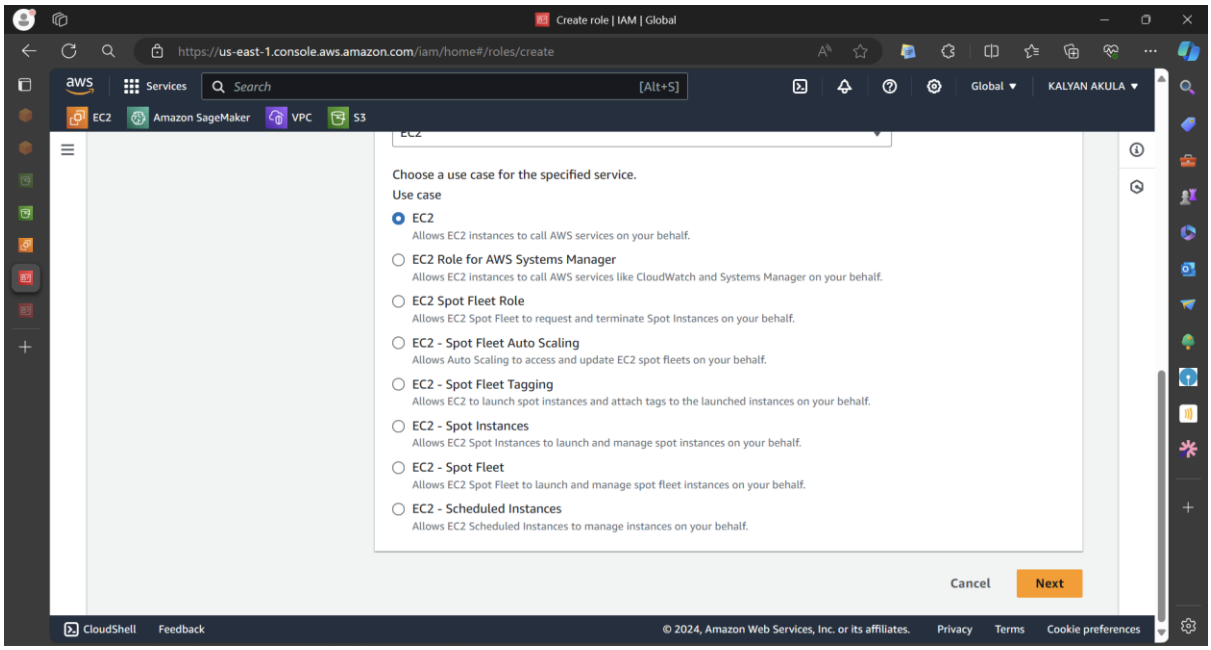


Step 7 : Fill details as follows

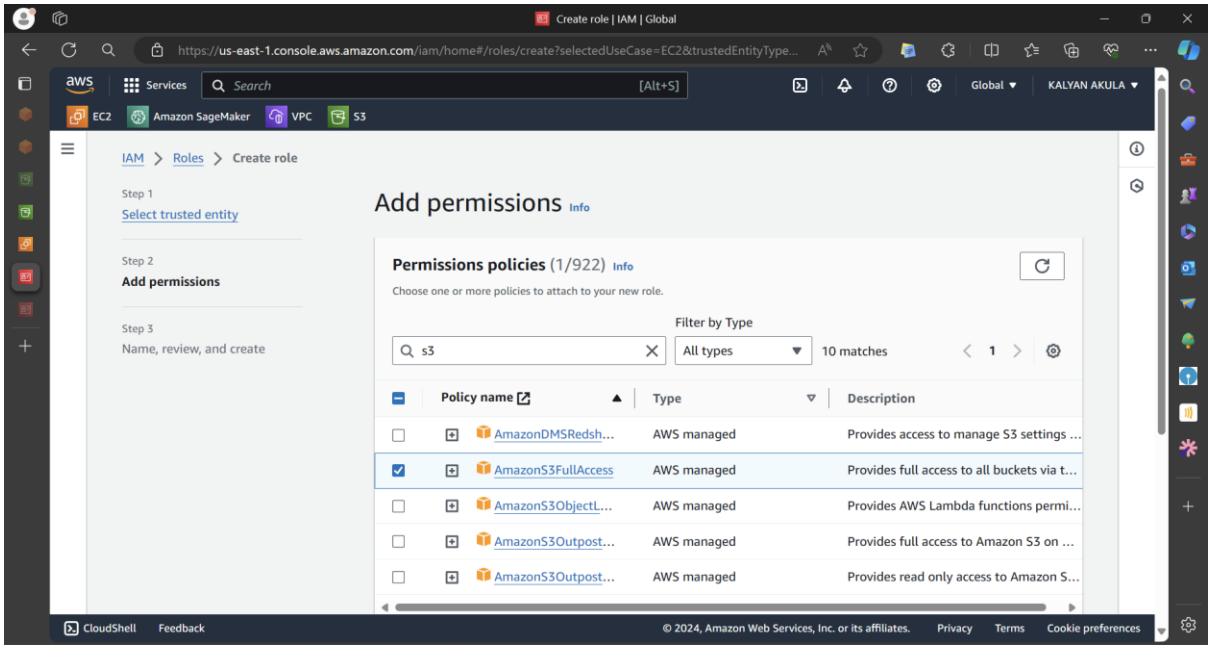




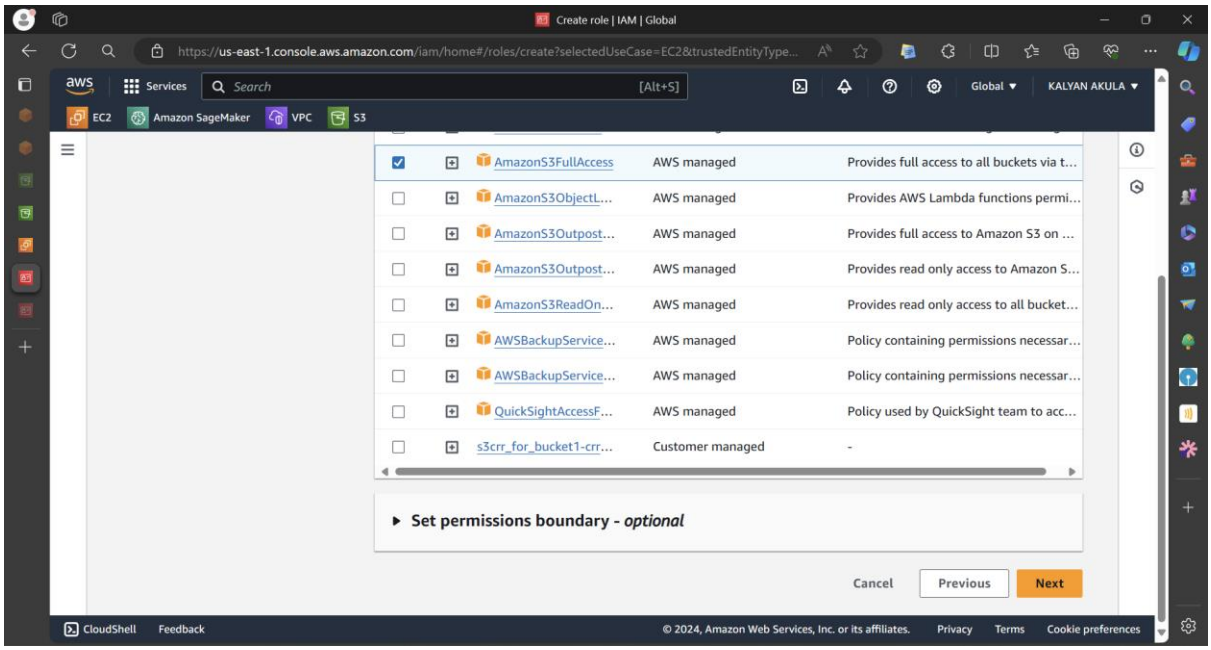
Step 8 : Click on next



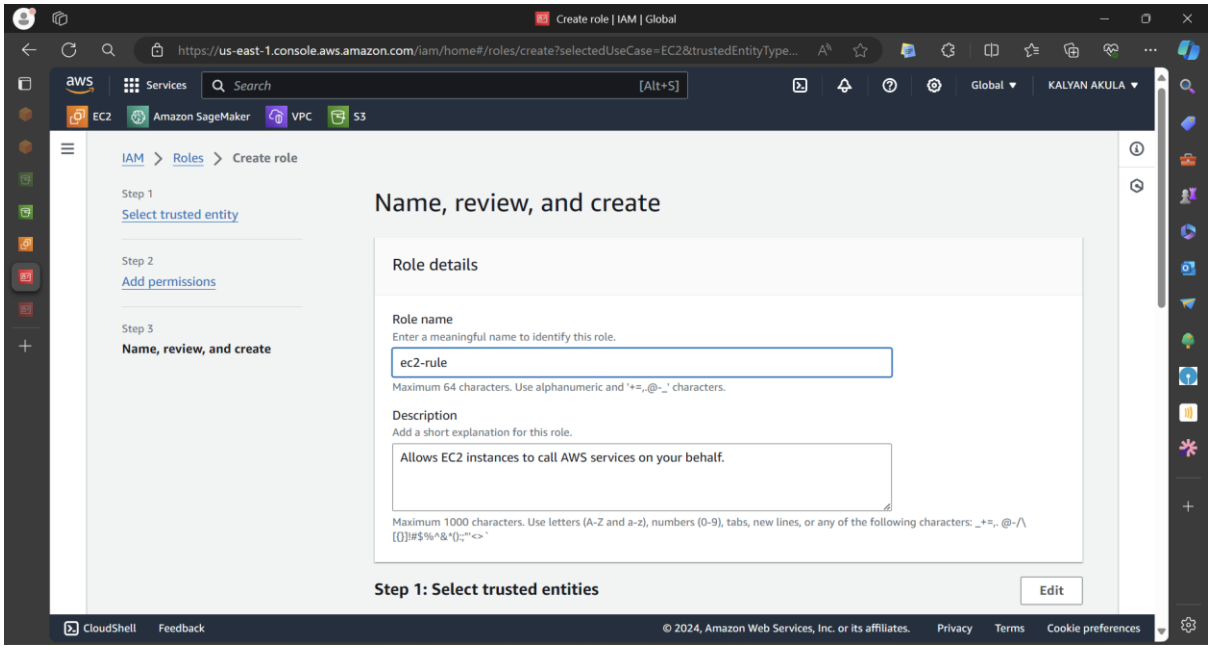
Step 9 : Select Amazons3fullaccess

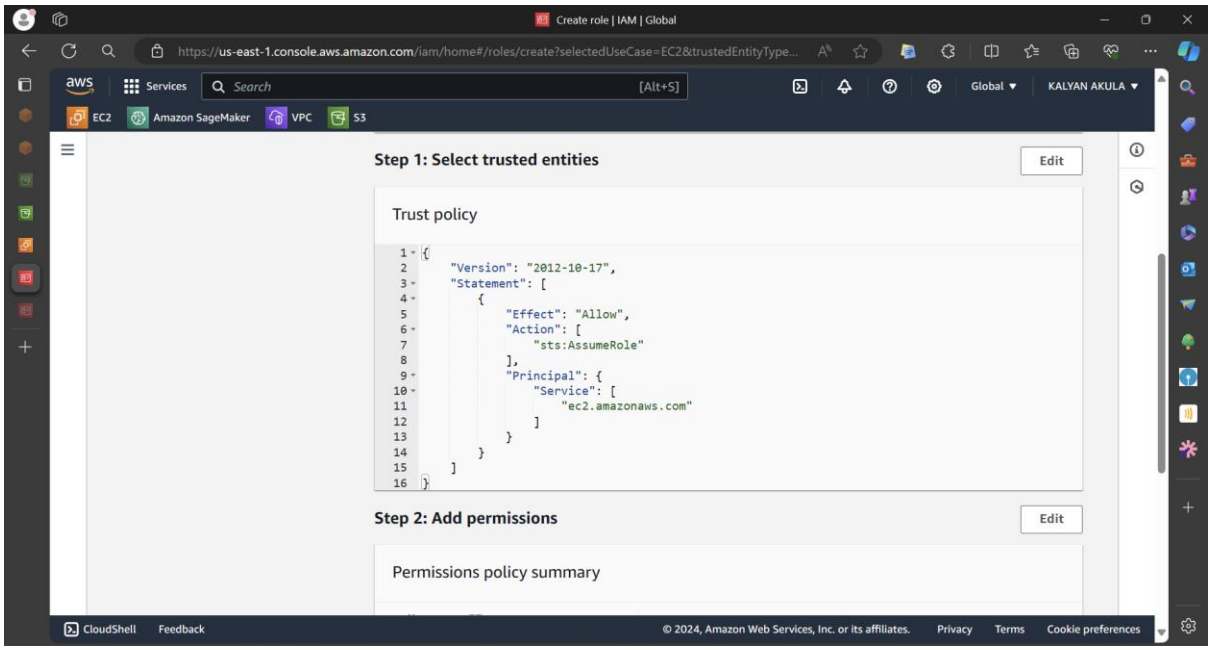


Step 10 : Click on Next

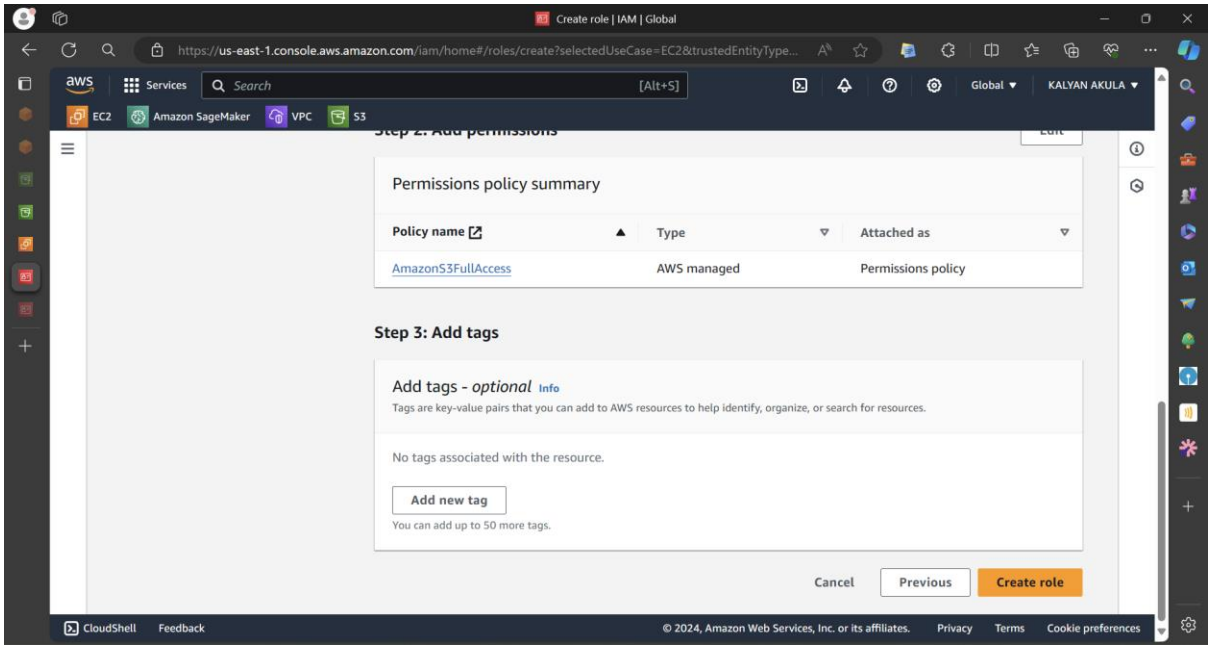


Step 11 : fill details as follows



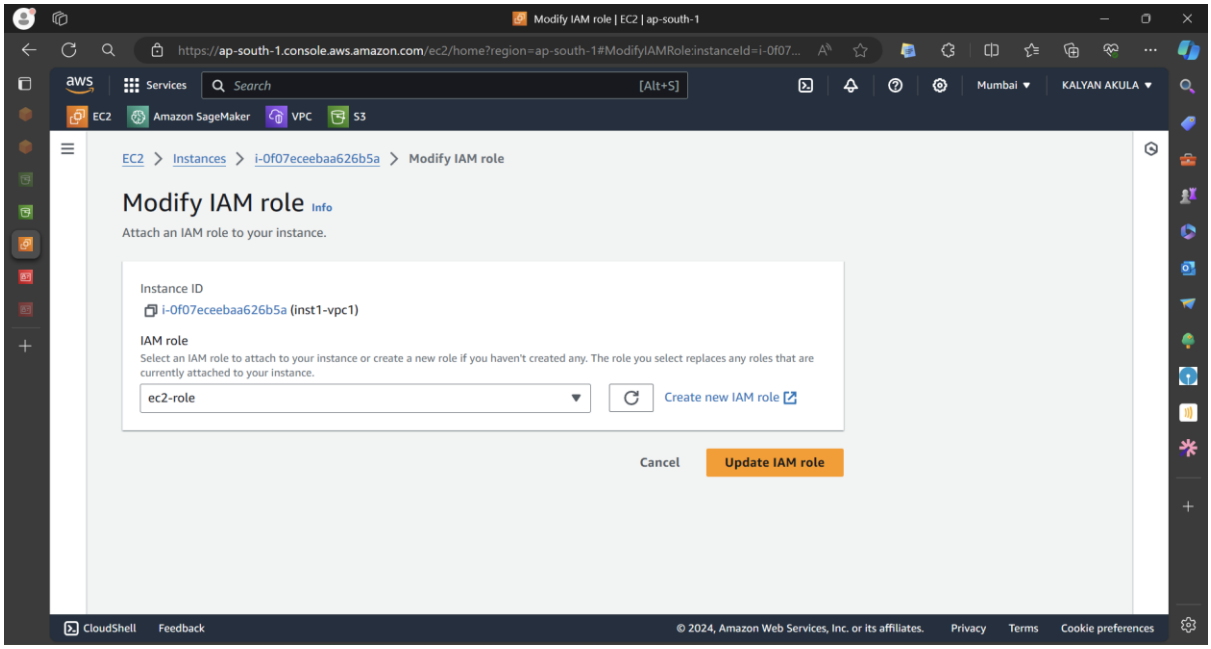


Step 12 : click on create roll



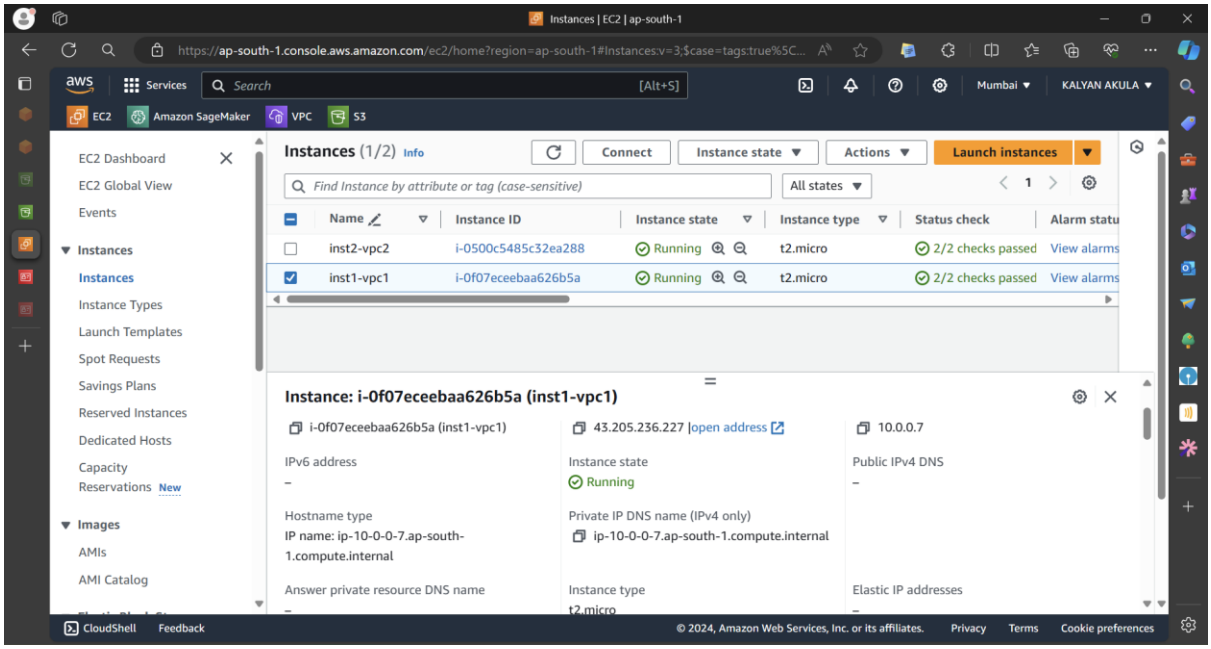
Step 13 : Now go back to Modify IAM role tab

Step 14 : Select ec2-rule

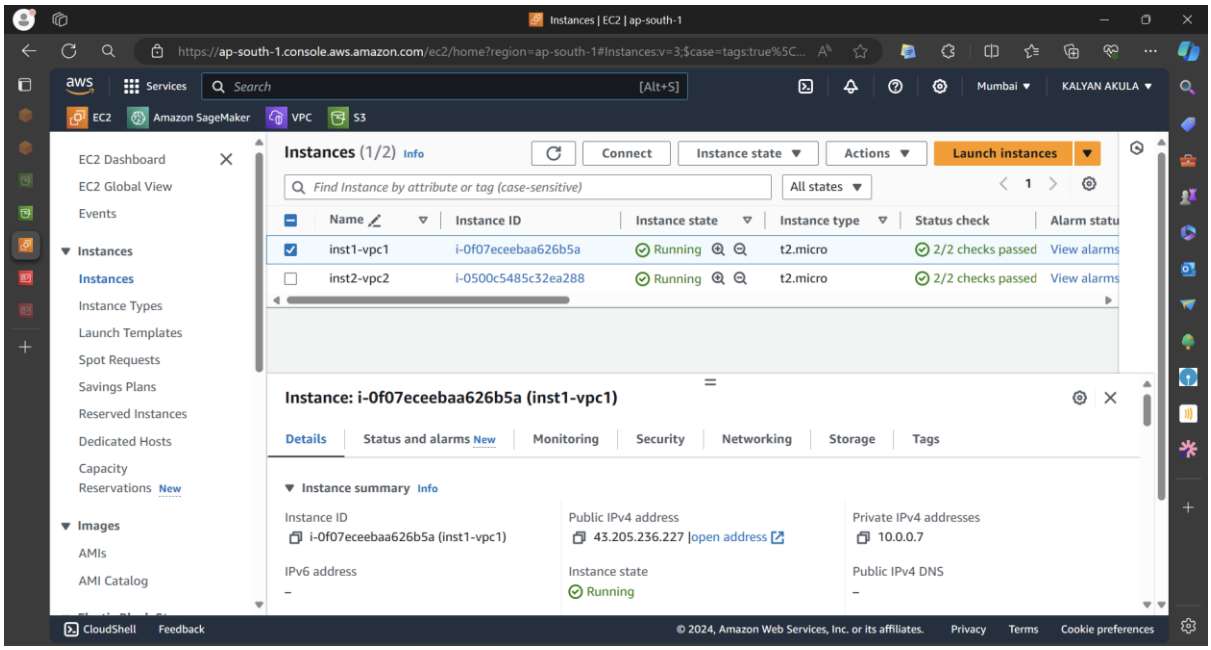


Step 15 : Click on Update IAM role

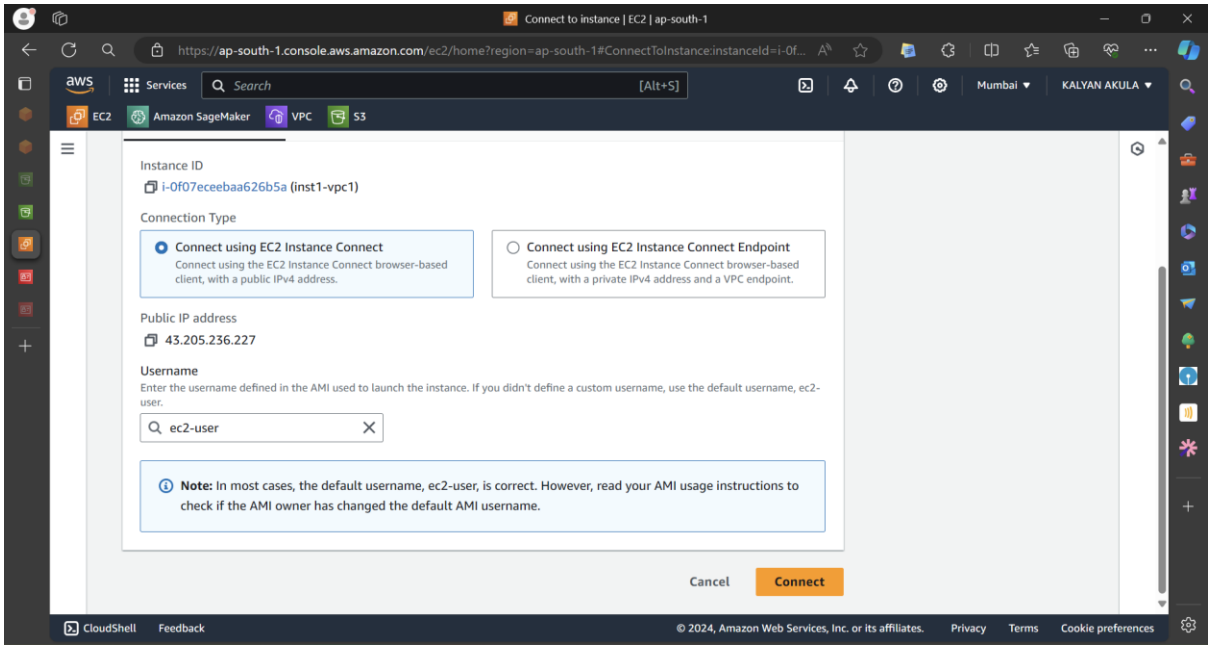
Step 16 : Now Go to instance tab



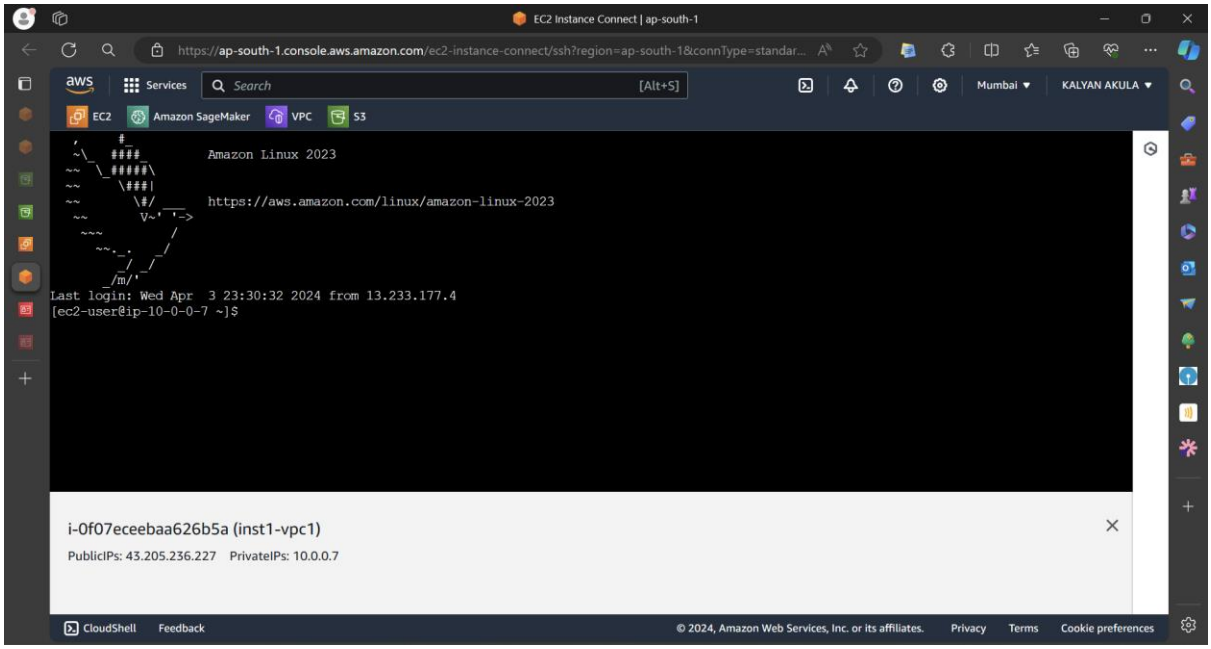
Step 17 : Select inst1-vpc1 & Click on Connect



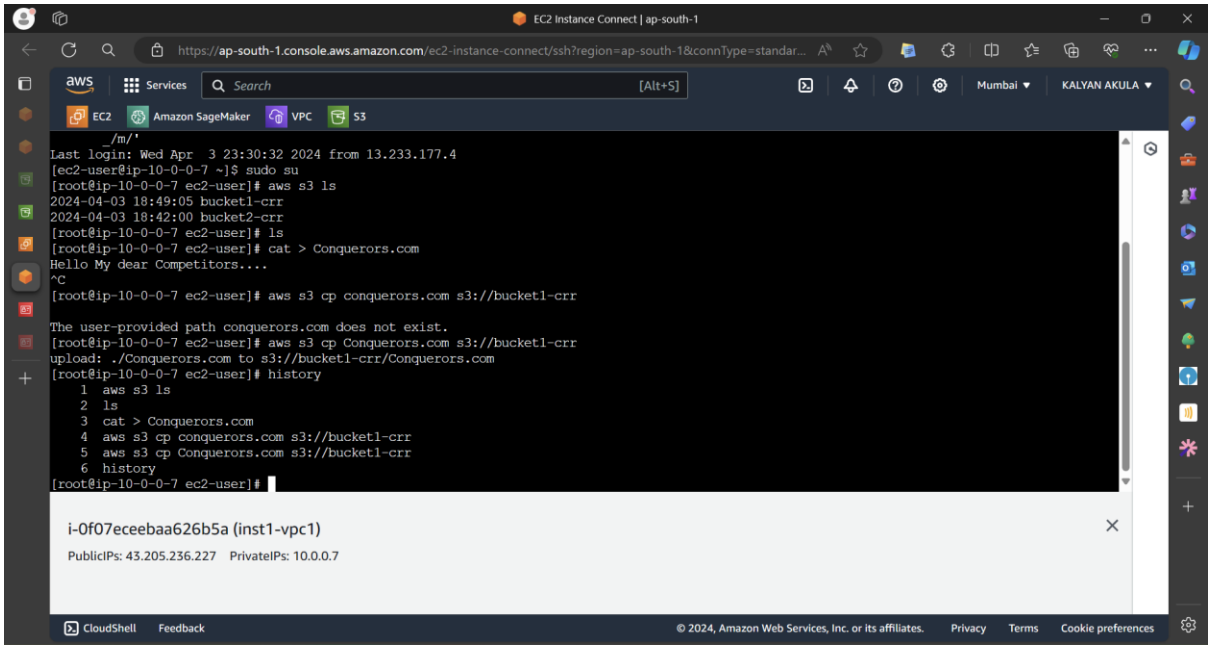
Step 18 : Click on Connect



- A linux interface will open



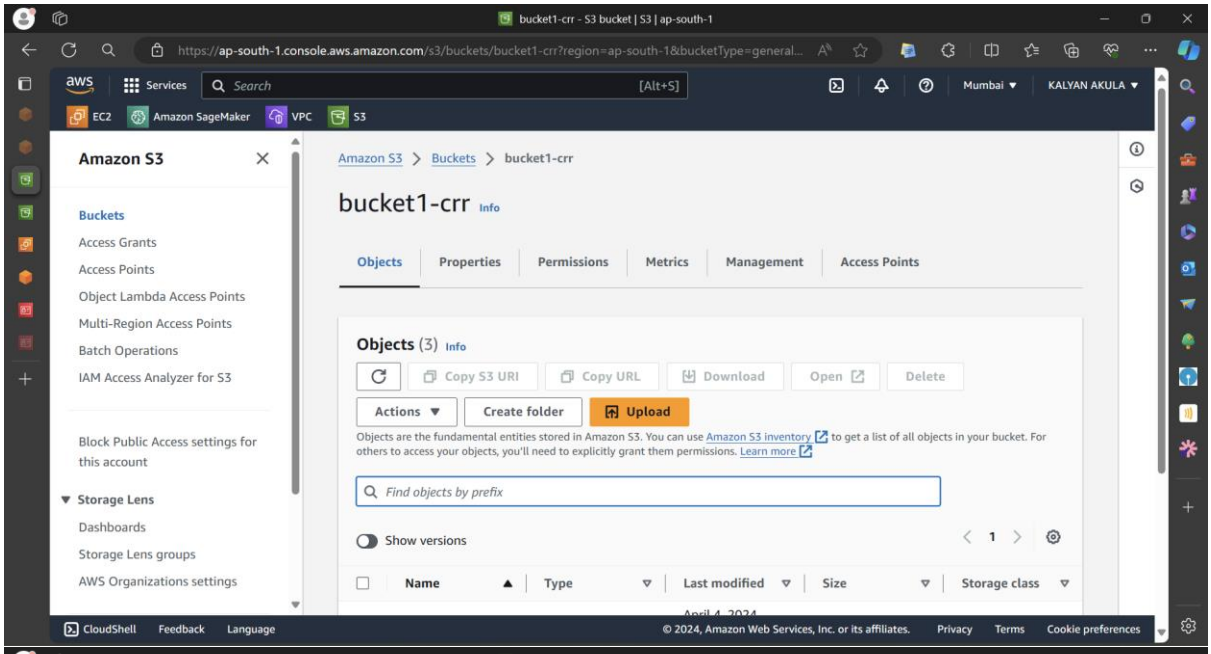
Step 19 : By entering the following commands , we can upload files in S3:Bucket1-crr

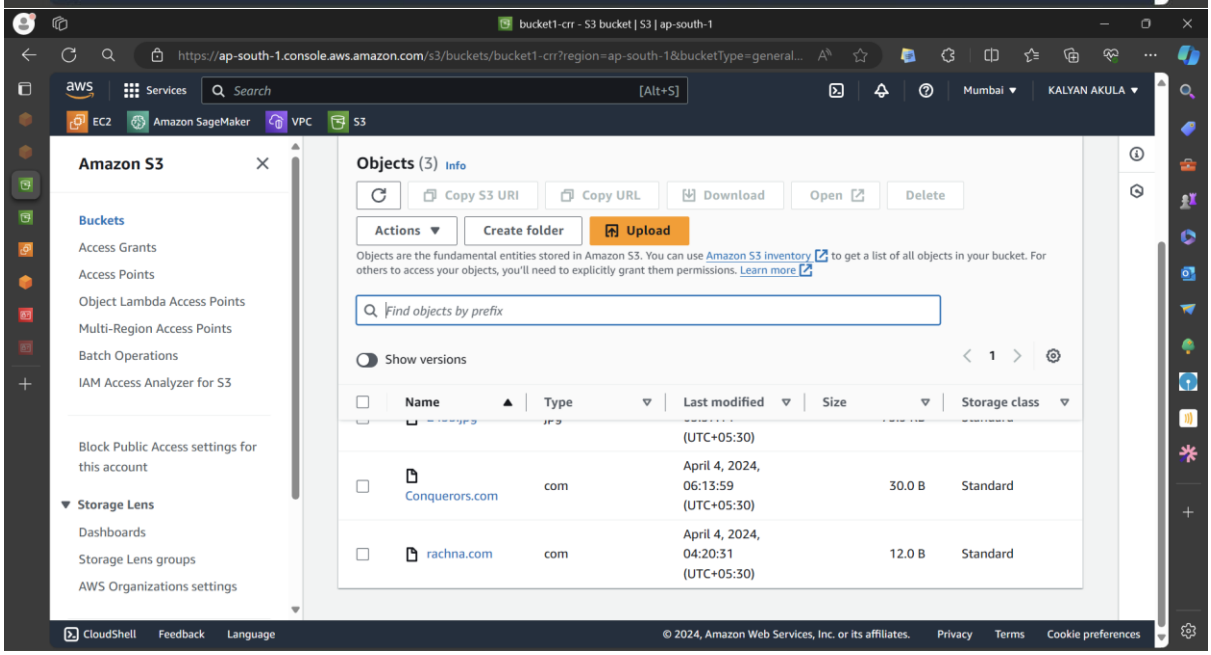


End Results

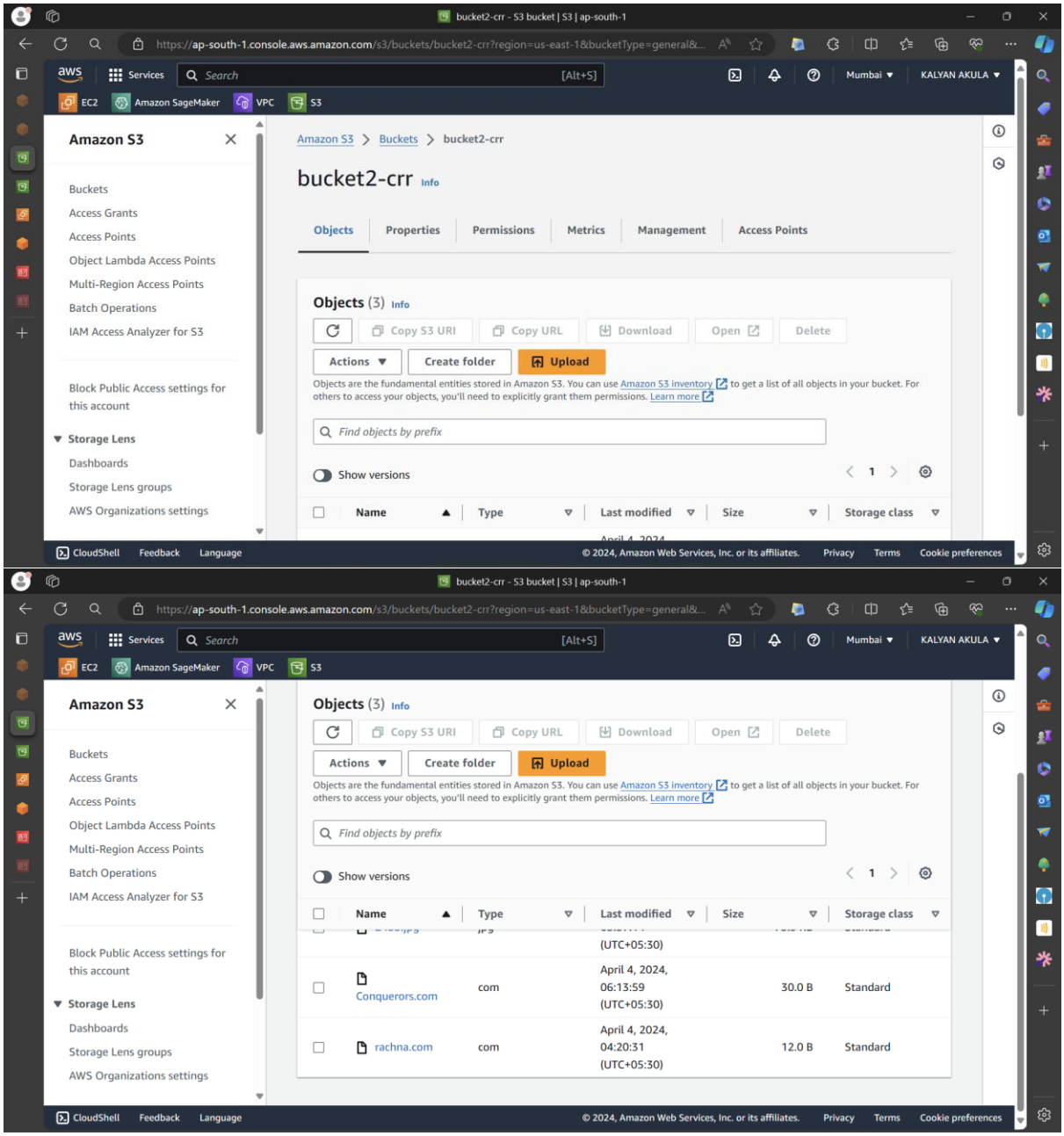
- **By using this commands , We can upload data files from EC2 instance to the Bucket1-crr in the same region.**
- We already established a CRR between Bucket1-crr & bucket2-crr , which are from different regions'
- So , if we upload files in Bucket1-crr through instance , it will also reflects in bucket2-crr

BUCKET1-CRR


bucket1-crr - S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/buckets/bucket1-crr?region=ap-south-1&bucketType=general...
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Amazon S3 > Buckets > bucket1-crr
bucket1-crr Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (3) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
Show versions
Name
Type
Last modified
Size
Storage class
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


bucket1-crr - S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/buckets/bucket1-crr?region=ap-south-1&bucketType=general...
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Objects (3) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
Show versions
Name
Type
Last modified
Size
Storage class
(UTC+05:30)
Conquerors.com
com
April 4, 2024, 06:13:59 (UTC+05:30)
30.0 B
Standard
rachna.com
com
April 4, 2024, 04:20:31 (UTC+05:30)
12.0 B
Standard
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

BUCKET2-CRR


bucket2-crr - S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/buckets/bucket2-crr?region=us-east-1&bucketType=general&...
aws
Services
Search
[Alt+S]
Mumbai
KALYAN AKULA
EC2
Amazon SageMaker
VPC
S3
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Amazon S3 > Buckets > bucket2-crr
bucket2-crr Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (3) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
Show versions
1
Name
Type
Last modified
Size
Storage class
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

bucket2-crr - S3 bucket | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/buckets/bucket2-crr?region=us-east-1&bucketType=general&...
Amazon S3
Objects (3) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
Show versions
1
Name
Type
Last modified
Size
Storage class
(UTC+05:30)
Conquerors.com
com
April 4, 2024, 06:13:59 (UTC+05:30)
30.0 B
Standard
rachna.com
com
April 4, 2024, 04:20:31 (UTC+05:30)
12.0 B
Standard
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences