D Y PATIL
INTERNATIONAL
UNIVERSITY
AKURDI PUNE

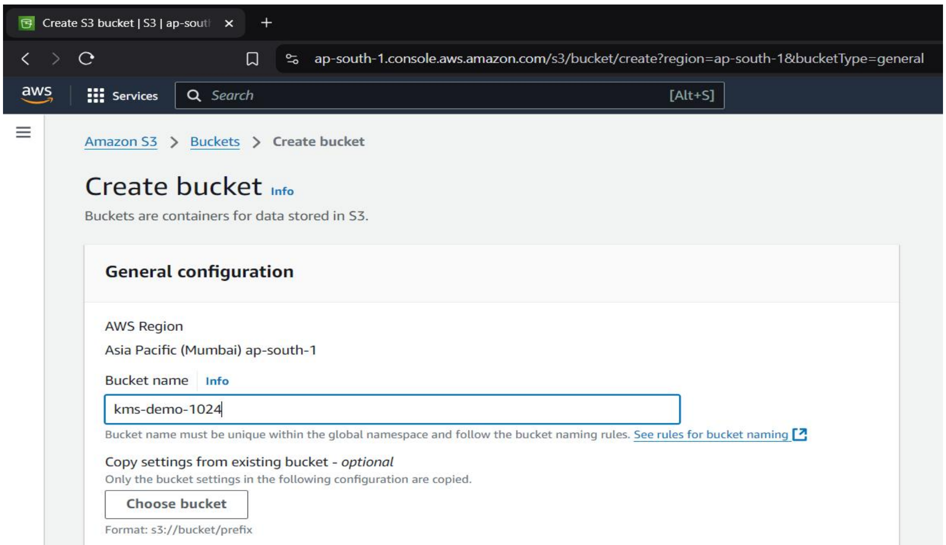
School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (SCSEA)
Subject: Advance Cloud Computing(ACC)

Name of the Student: **Shrushti Krishna Shrivastav** **PRN: 20220801024**

Title of Practicle : Encrypt an S3 bucket using AWS KMS

STEP1: Create bucket

Go to S3 service and create one bucket



Create S3 bucket | S3 | ap-south
ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
aws
Services
Search
[Alt+S]
Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

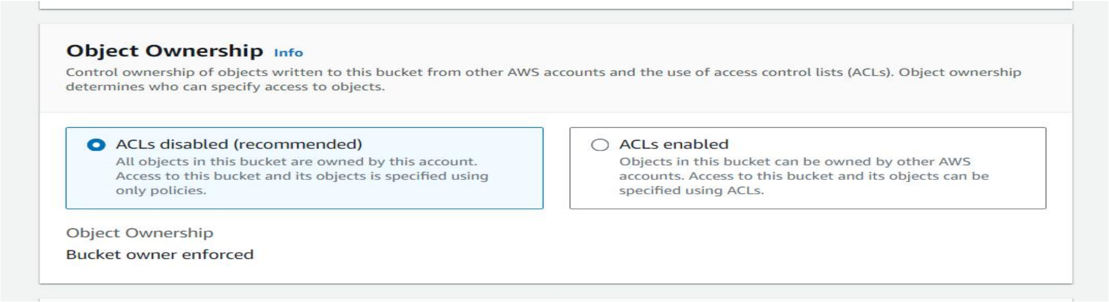
AWS Region
Asia Pacific (Mumbai) ap-south-1

Bucket name Info
kms-demo-1024

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.

Format: s3://bucket/prefix



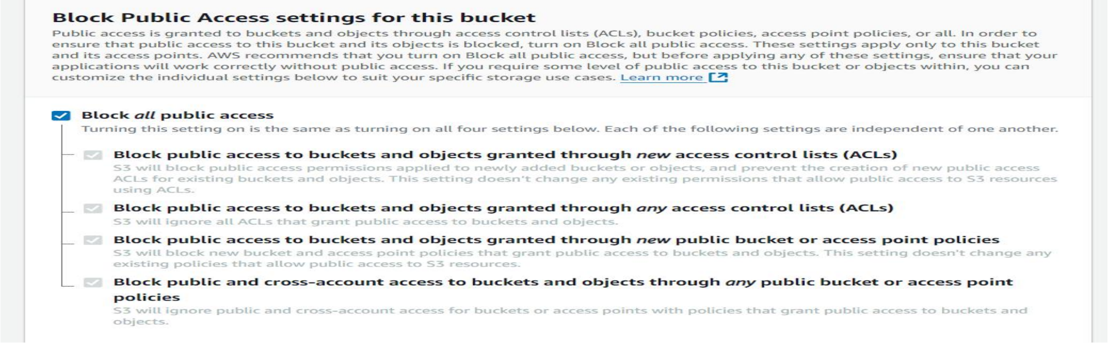
Object Ownership Info

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

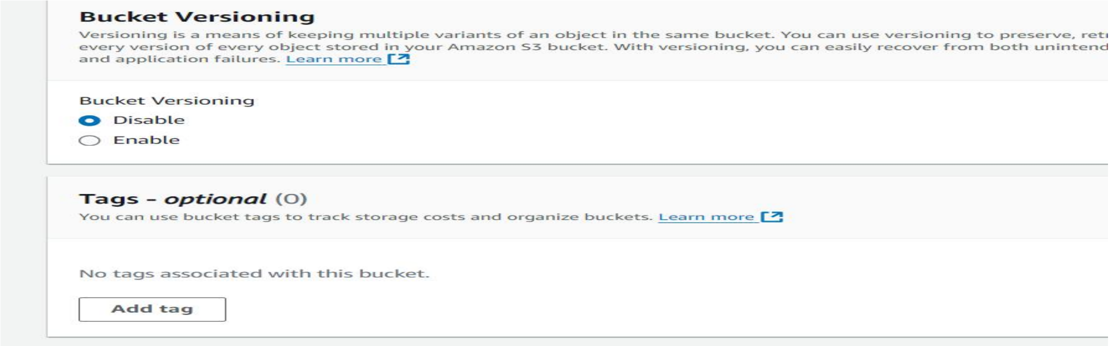


Block Public Access settings for this bucket

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 *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.



Bucket Versioning

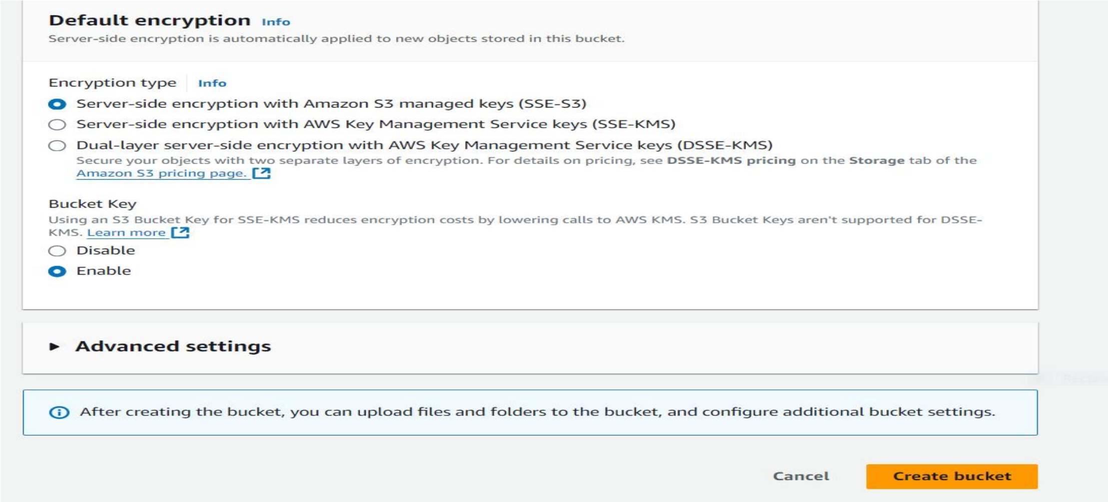
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, ret every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintend and application failures. Learn more

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.



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

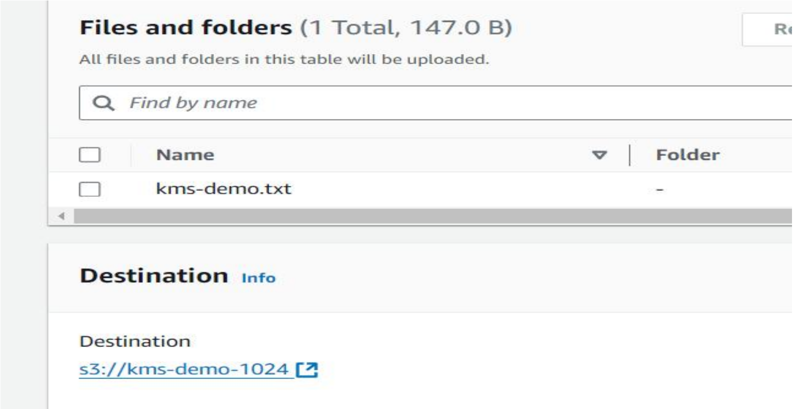
Encryption type Info
● Server-side encryption with Amazon S3 managed keys (SSE-S3)
○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
○ Disable
● Enable

▸ **Advanced settings**

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Also upload some files in this bucket



Files and folders (1 Total, 147.0 B)

All files and folders in this table will be uploaded.

□	Name	Folder
□	kms-demo.txt	-

Destination Info

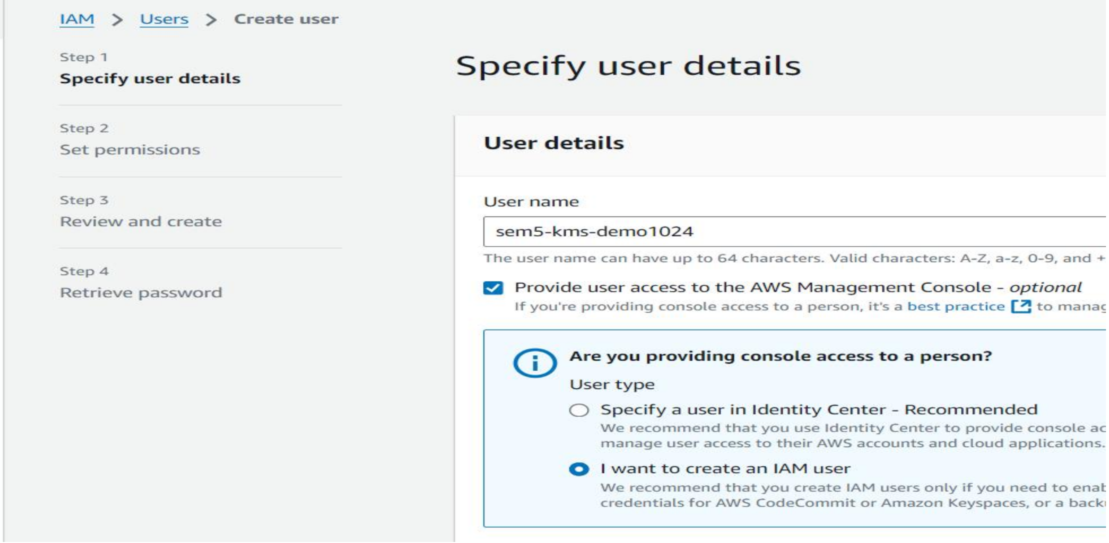
Destination
s3://kms-demo-1024

open the created bucket and check its properties and permission

(default encryption is selected for the object stored in this bucket.)

STEP2: Create IAM-USER

Go to IAM service and create one User



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

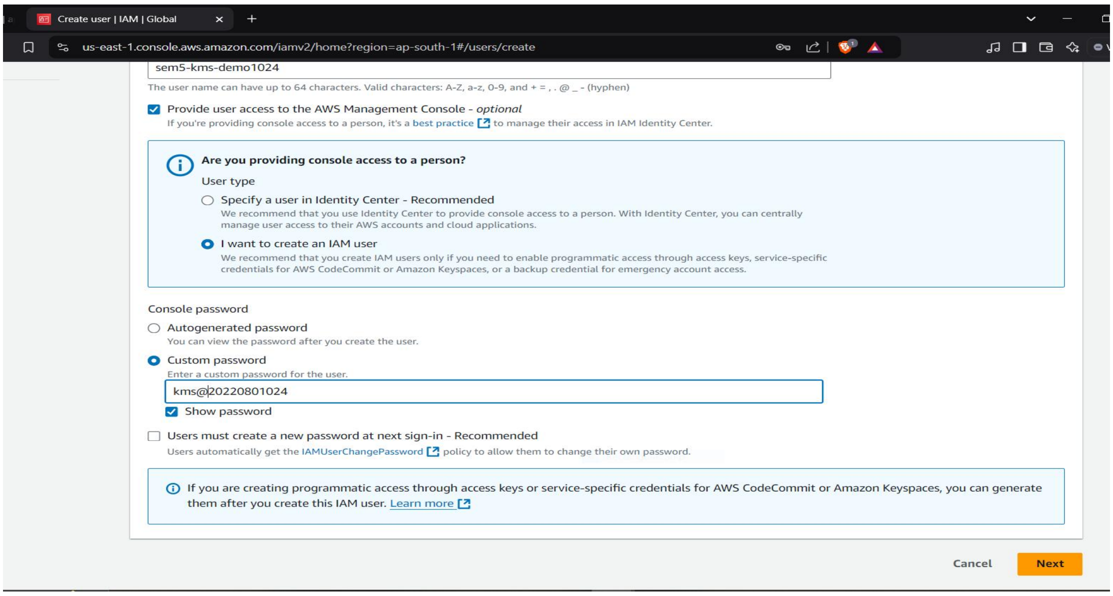
Specify user details

User details

User name
sem5-kms-demo1024
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +

☑ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a best practice to manag

Are you providing console access to a person?
User type
○ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console ac
manage user access to their AWS accounts and cloud applications.
● I want to create an IAM user
We recommend that you create IAM users only if you need to enab
credentials for AWS CodeCommit or Amazon Keyspaces, or a back



Create user | IAM | Global

us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/create

sem5-kms-demo1024
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?
User type
○ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
● I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password
○ Autogenerated password
You can view the password after you create the user.
● Custom password
Enter a custom password for the user.
kms@20220801024
☑ Show password

□ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

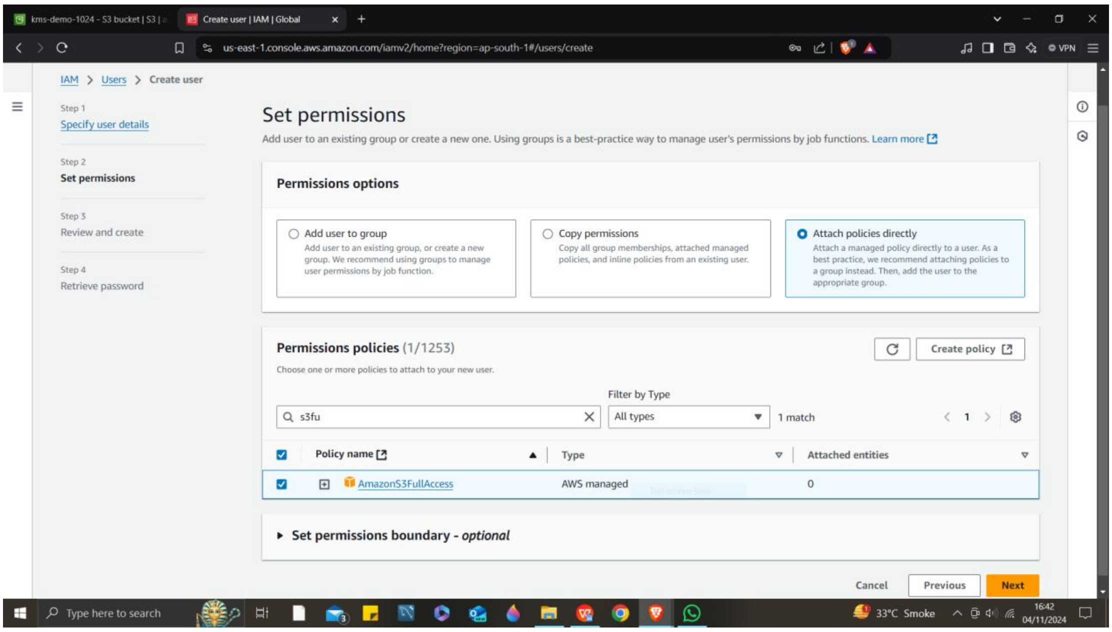
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

D Y PATIL
INTERNATIONAL
UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (SCSEA)
Subject: Advance Cloud Computing(ACC)

Name of the Student: **Shrushti Krishna Shrivastav** **PRN: 20220801024**

Title of Practicle : Encrypt an S3 bucket using AWS KMS



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1253)

Choose one or more policies to attach to your new user.

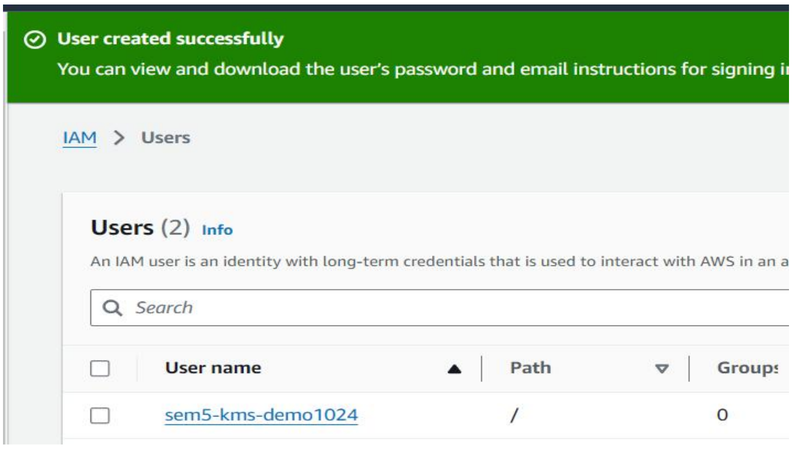
Search: s3fu
Filter by Type: All types
1 match

☑	Policy name	Type	Attached entities
☑	AmazonS3FullAccess	AWS managed	0

▸ Set permissions boundary - *optional*

kms-demo-1024 - S3 bucket | S3 |
Create user | IAM | Global
us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/create
VPN
Create policy
Cancel
Previous
Next
Type here to search
33°C Smoke
16:42
04/11/2024

Remember your username and password or download the csv file in step4



User created successfully

You can view and download the user's password and email instructions for signing i

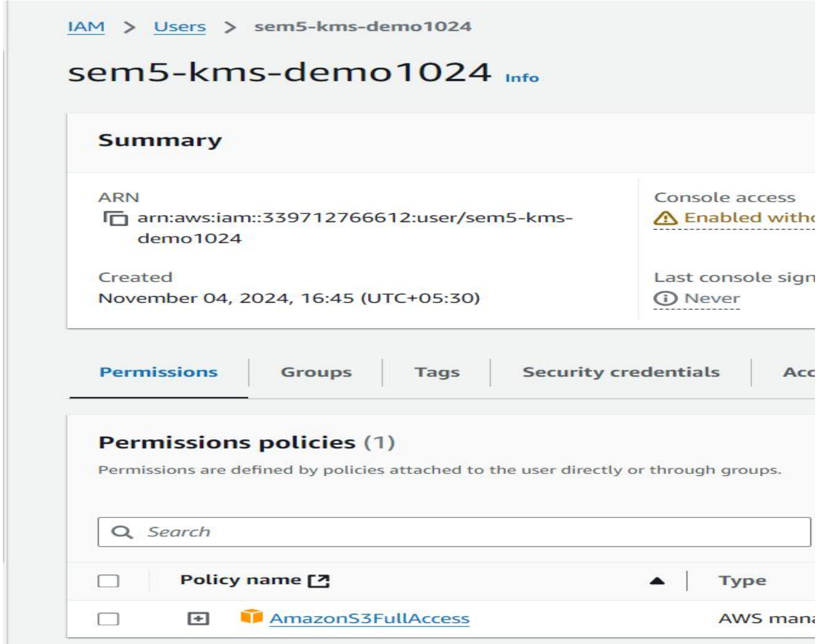
IAM > Users

Users (2) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an a

Search

□	User name	Path	Group:
□	sem5-kms-demo1024	/	0



IAM > Users > sem5-kms-demo1024

sem5-kms-demo1024 Info

Summary

ARN
arn:aws:iam::339712766612:user/sem5-kms-demo1024

Created
November 04, 2024, 16:45 (UTC+05:30)

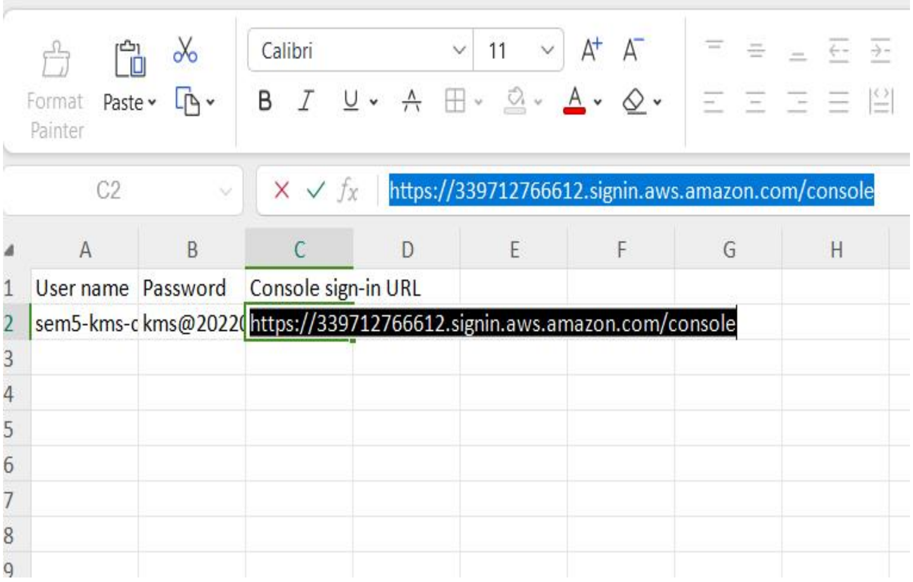
Console access
Enabled witho

Last console sign
Never

Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.

□	Policy name	Type
□	AmazonS3FullAccess	AWS man

Now open the csv file and copy the url (for iam user sign in)



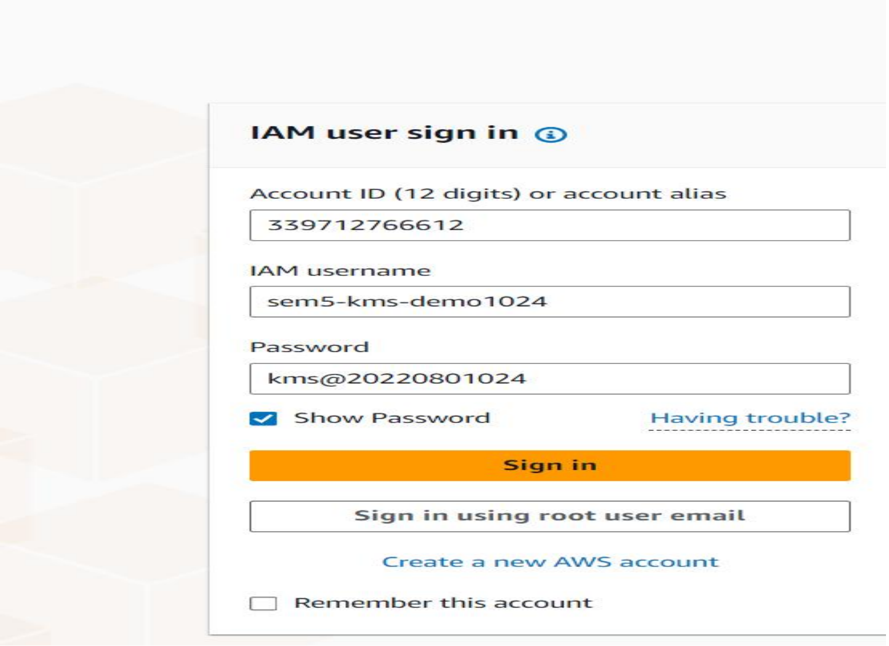
https://339712766612.signin.aws.amazon.com/console

	A	B	C
1	User name	Password	Console sign-in URL
2	sem5-kms-c	kms@2022(	https://339712766612.signin.aws.amazon.com/console

Name of the Student: **Shrushti Krishna Shrivastav** **PRN: 20220801024**

Title of Practicle : Encrypt an S3 bucket using AWS KMS

Open private window or different browser and paste the url--



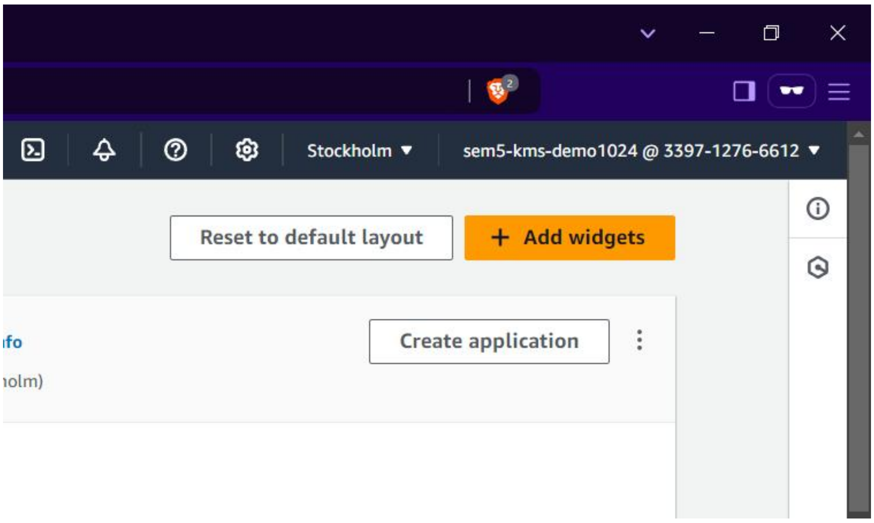
IAM user sign in

Account ID (12 digits) or account alias
339712766612

IAM username
sem5-kms-demo1024

Password
kms@20220801024

☑ Show Password



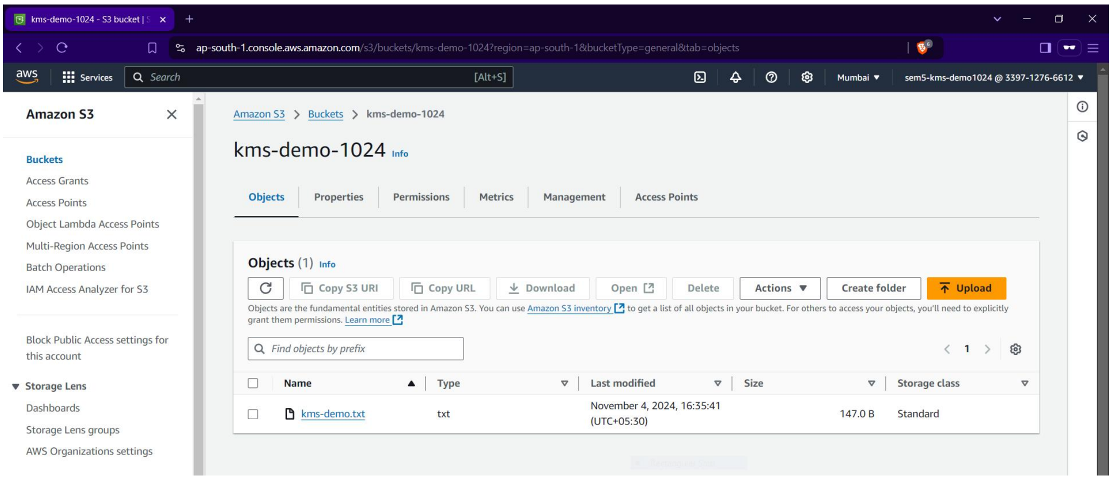
Stockholm ▼ sem5-kms-demo1024 @ 3397-1276-6612 ▼

Select your region and and here with this user you only have access for s3

Name of the Student: Shrushti Krishna Shrivastav **PRN:** 20220801024

Title of Practicle : Encrypt an S3 bucket using AWS KMS

Go to s3 and try to access the object that was uploaded by root user

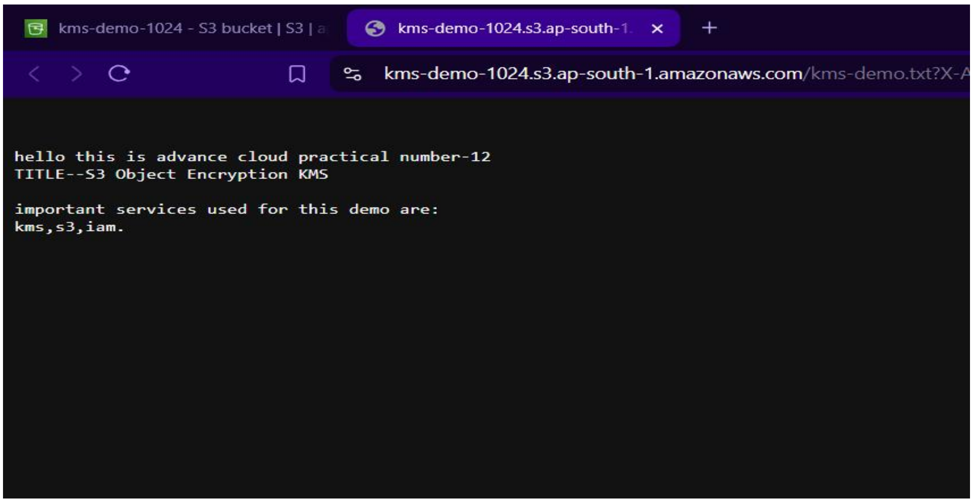


kms-demo-1024 - S3 bucket
ap-south-1.console.aws.amazon.com/s3/buckets/kms-demo-1024?region=ap-south-1&bucketType=general&tab=objects
Services
Search
[Alt+S]
Mumbai
sem5-kms-demo1024 @ 3397-1276-6612
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
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 > kms-demo-1024
kms-demo-1024 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix

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

Name	Type	Last modified	Size	Storage class
kms-demo.txt	txt	November 4, 2024, 16:35:41 (UTC+05:30)	147.0 B	Standard

We are able to access our object through iam user as it has full access of s3, when the encryption type is: SSE-S3



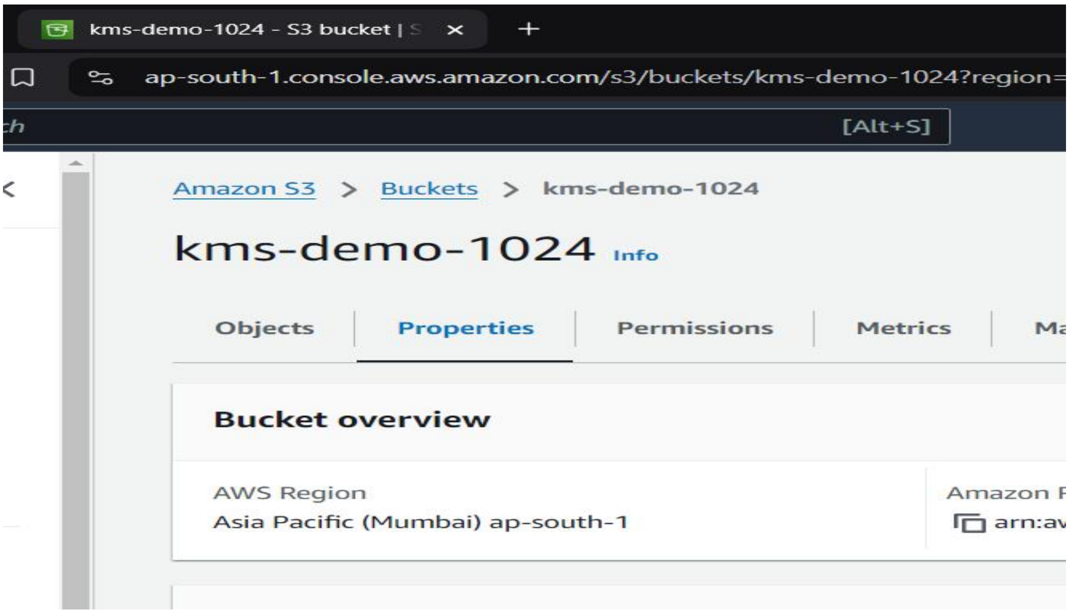
kms-demo-1024 - S3 bucket | S3 | a
kms-demo-1024.s3.ap-south-1.
kms-demo-1024.s3.ap-south-1.amazonaws.com/kms-demo.txt?X-A

```
hello this is advance cloud practical number-12
TITLE--S3 Object Encryption KMS

important services used for this demo are:
kms,s3,iam.
```

STEP3: Changes in encryption of bucket(root user)

Go to root user, S3 service, go to your object's properties


kms-demo-1024 - S3 bucket | S

ap-south-1.console.aws.amazon.com/s3/buckets/kms-demo-1024?region=

Amazon S3 > Buckets > kms-demo-1024

kms-demo-1024 Info

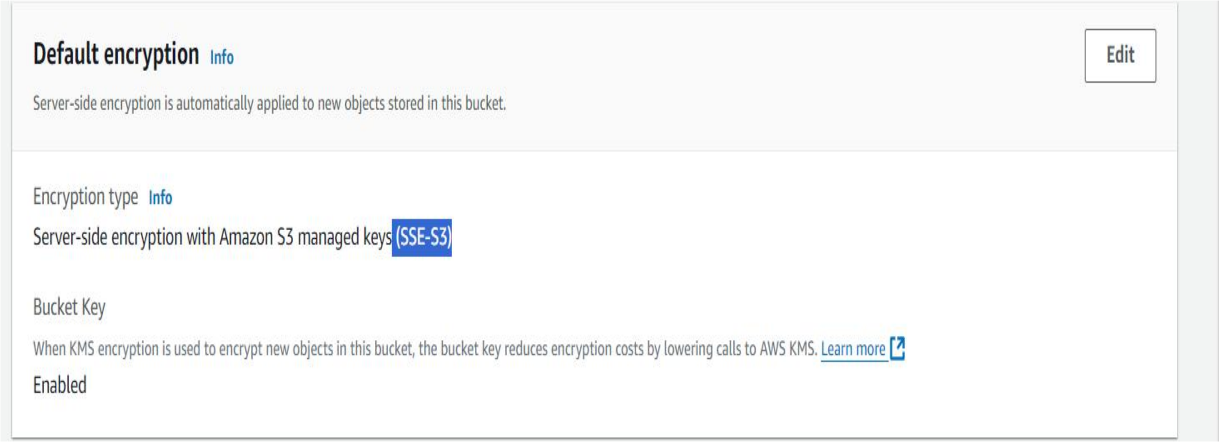
Bucket overview

AWS Region
Asia Pacific (Mumbai) ap-south-1

Amazon R
arn:av

Scroll a bit and you'll find encryption -- edit .

Edit the encryption type: change to kms


Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

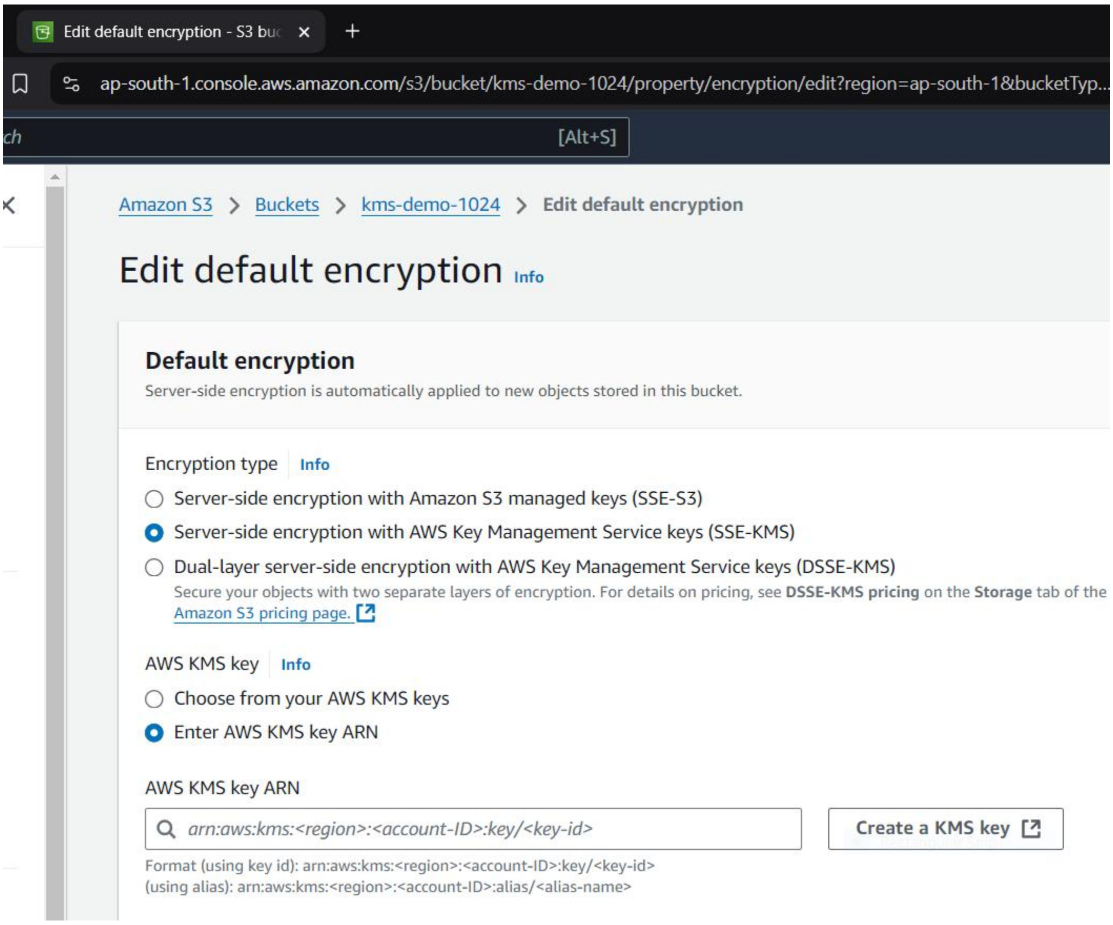
Server-side encryption with Amazon S3 managed keys (SSE-S3)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more

Enabled

SSE-KMS



Edit default encryption - S3 buc

ap-south-1.console.aws.amazon.com/s3/bucket/kms-demo-1024/property/encryption/edit?region=ap-south-1&bucketTyp...

Amazon S3 > Buckets > kms-demo-1024 > Edit default encryption

Edit default encryption Info

Default encryption

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

○ Server-side encryption with Amazon S3 managed keys (SSE-S3)

● Server-side encryption with AWS Key Management Service keys (SSE-KMS)

○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

AWS KMS key Info

○ Choose from your AWS KMS keys

● Enter AWS KMS key ARN

AWS KMS key ARN

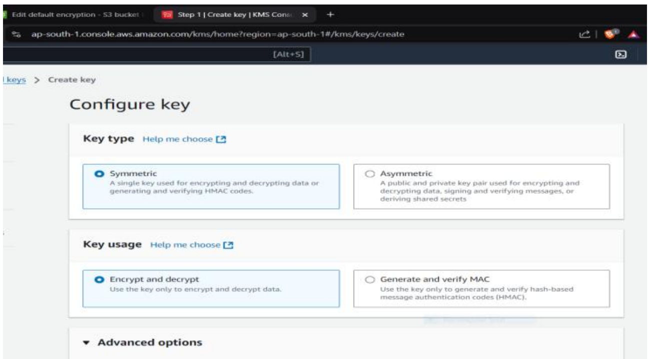
arn:aws:kms:<region>:<account-ID>:key/<key-id>

Create a KMS key

Format (using key id): arn:aws:kms:<region>:<account-ID>:key/<key-id>
(using alias): arn:aws:kms:<region>:<account-ID>:alias/<alias-name>

Here we need ARN of the KMS key we want to attach

For that create a kms key--- default setting for step1



Edit default encryption - S3 bucket | Step 1 | Create key | KMS Cons

ap-south-1.console.aws.amazon.com/kms/home?region=ap-south-1#/kms/keys/create

keys > Create key

Configure key

Key type Help me choose

● Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes.

○ Asymmetric
A public and private key pair used for encrypting and decrypting data, signing and verifying messages, or deriving shared secrets

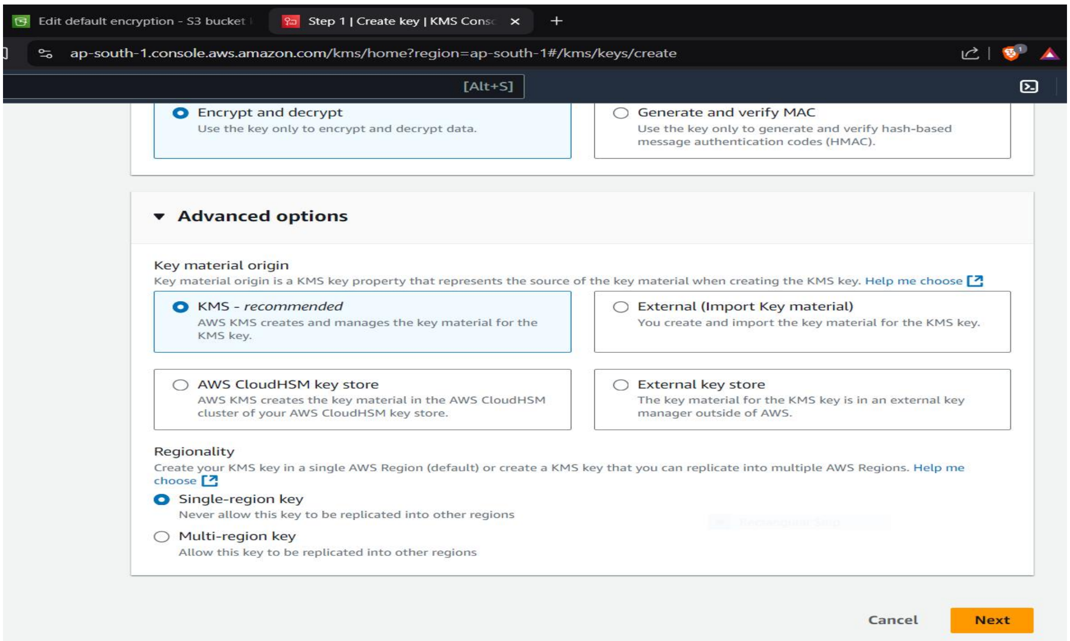
Key usage Help me choose

● Encrypt and decrypt
Use the key only to encrypt and decrypt data.

○ Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

▾ Advanced options

Continue step1



Edit default encryption - S3 bucket
Step 1 | Create key | KMS Conso
[Alt+S]

ap-south-1.console.aws.amazon.com/kms/home?region=ap-south-1#/kms/keys/create

● Encrypt and decrypt
Use the key only to encrypt and decrypt data.

○ Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

▼ Advanced options

Key material origin
Key material origin is a KMS key property that represents the source of the key material when creating the KMS key. Help me choose

● KMS - *recommended*
AWS KMS creates and manages the key material for the KMS key.

○ External (Import Key material)
You create and import the key material for the KMS key.

○ AWS CloudHSM key store
AWS KMS creates the key material in the AWS CloudHSM cluster of your AWS CloudHSM key store.

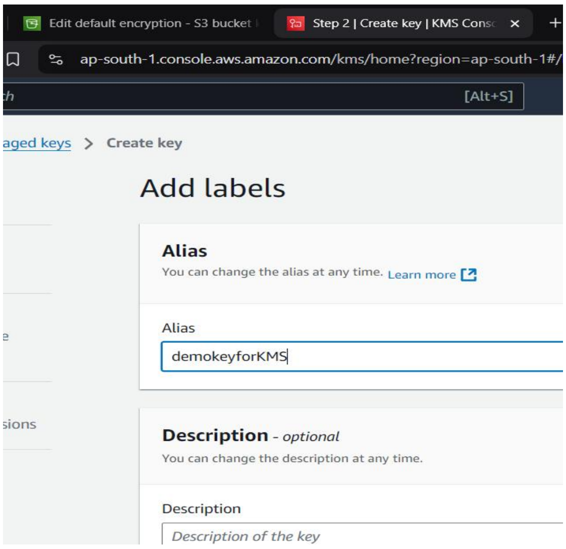
○ External key store
The key material for the KMS key is in an external key manager outside of AWS.

Regionality
Create your KMS key in a single AWS Region (default) or create a KMS key that you can replicate into multiple AWS Regions. Help me choose

● Single-region key
Never allow this key to be replicated into other regions

○ Multi-region key
Allow this key to be replicated into other regions

Step2--



Edit default encryption - S3 bucket
Step 2 | Create key | KMS Conso
[Alt+S]
aged keys > Create key

ap-south-1.console.aws.amazon.com/kms/home?region=ap-south-1#/

Add labels

Alias
You can change the alias at any time. Learn more

Alias
demokeyforKMS

Description - *optional*
You can change the description at any time.

Description
Description of the key

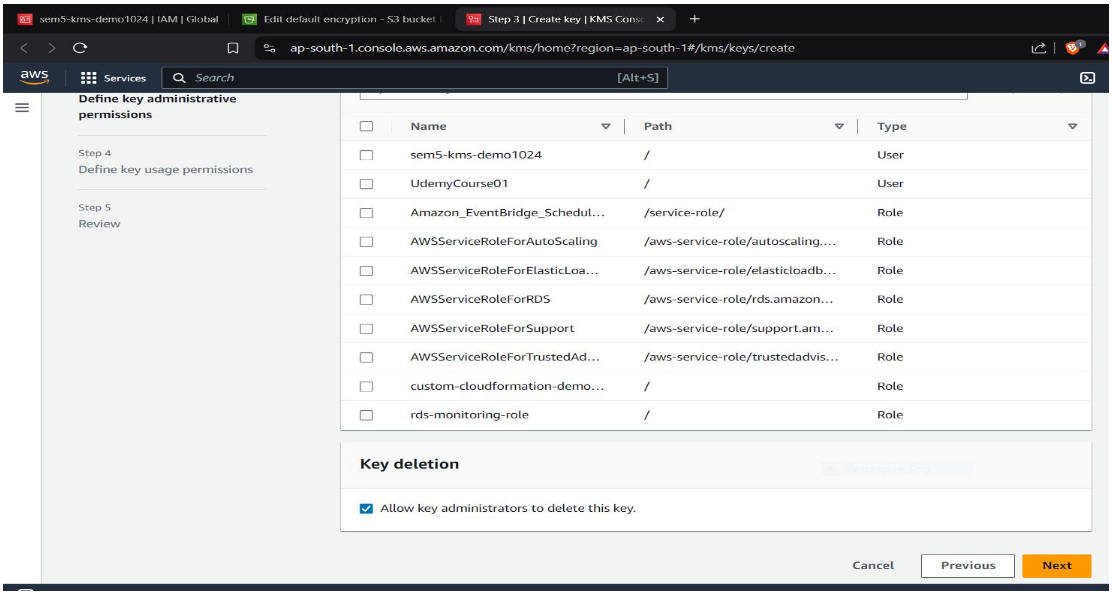
D Y PATIL
INTERNATIONAL
UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (SCSEA)
Subject: Advance Cloud Computing(ACC)

Name of the Student: **Shrushti Krishna Shrivastav** **PRN: 20220801024**

Title of Practicle : Encrypt an S3 bucket using AWS KMS

Step3--(default)



sem5-kms-demo1024 | IAM | Global
Edit default encryption - S3 bucket
Step 3 | Create key | KMS Conso
ap-south-1.console.aws.amazon.com/kms/home?region=ap-south-1#/kms/keys/create
aws
Services
Search
[Alt+S]

Define key administrative permissions

Step 4
Define key usage permissions

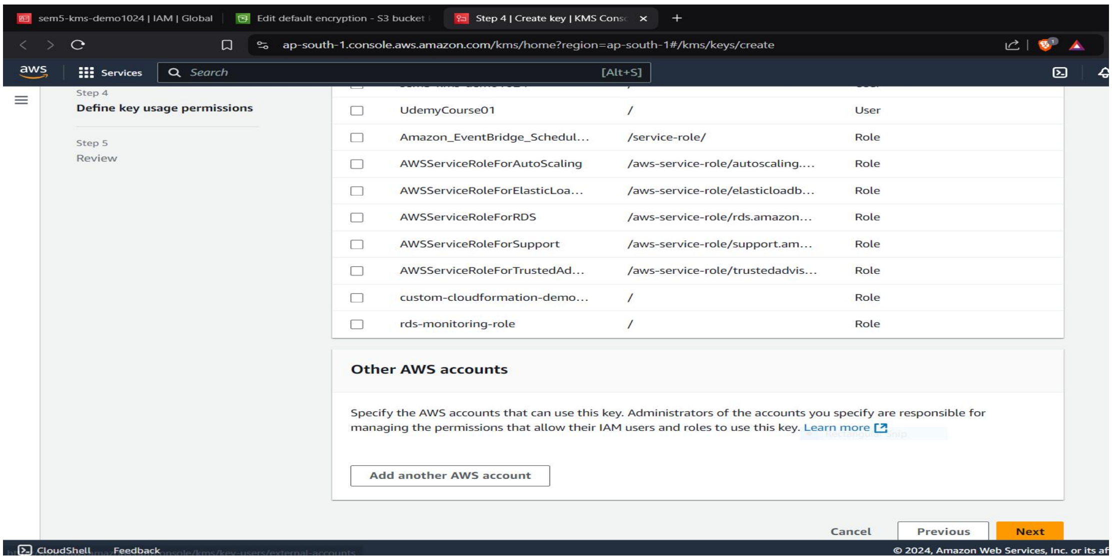
Step 5
Review

□	Name	Path	Type
□	sem5-kms-demo1024	/	User
□	UdemyCourse01	/	User
□	Amazon_EventBridge_Schedul...	/service-role/	Role
□	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling....	Role
□	AWSServiceRoleForElasticLoa...	/aws-service-role/elasticloadb...	Role
□	AWSServiceRoleForRDS	/aws-service-role/rds.amazon...	Role
□	AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
□	AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role
□	custom-cloudformation-demo...	/	Role
□	rds-monitoring-role	/	Role

Key deletion

☑ Allow key administrators to delete this key.

Step4--(default)



sem5-kms-demo1024 | IAM | Global
Edit default encryption - S3 bucket
Step 4 | Create key | KMS Conso
ap-south-1.console.aws.amazon.com/kms/home?region=ap-south-1#/kms/keys/create
aws
Services
Search
[Alt+S]

Step 4
Define key usage permissions

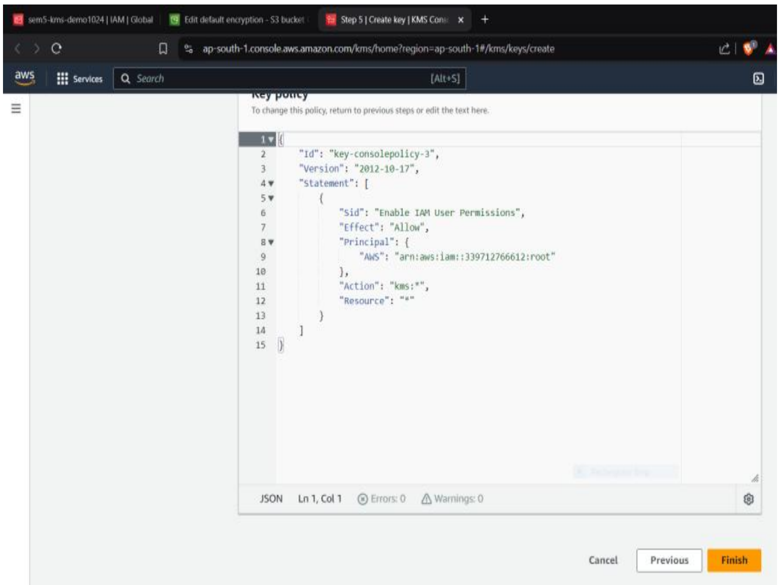
Step 5
Review

□	Name	Path	Type
□	UdemyCourse01	/	User
□	Amazon_EventBridge_Schedul...	/service-role/	Role
□	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling....	Role
□	AWSServiceRoleForElasticLoa...	/aws-service-role/elasticloadb...	Role
□	AWSServiceRoleForRDS	/aws-service-role/rds.amazon...	Role
□	AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
□	AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role
□	custom-cloudformation-demo...	/	Role
□	rds-monitoring-role	/	Role

Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. Learn more

Step5--



ap-south-1.console.aws.amazon.com/kms/home?region=ap-south-1#/kms/keys/create

Key policy

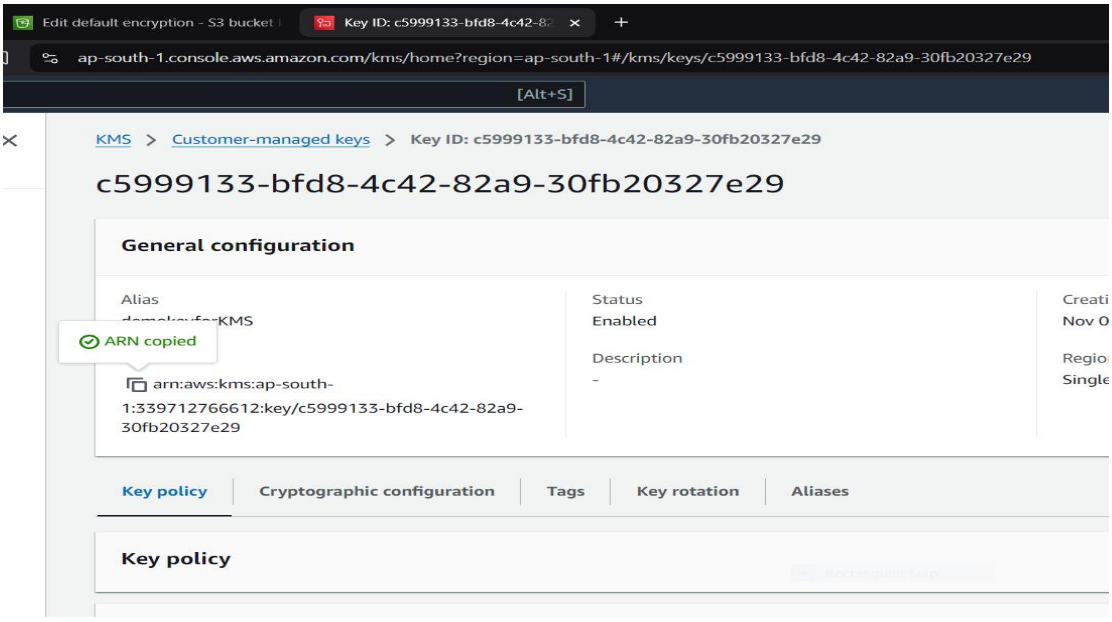
To change this policy, return to previous steps or edit the text here.

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::339712766612:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

JSON Ln 1, Col 1 Errors: 0 Warnings: 0

Create the key.

Once the status is enabled open the key and copy the ARN generated for the key



ap-south-1.console.aws.amazon.com/kms/home?region=ap-south-1#/kms/keys/c5999133-bfd8-4c42-82a9-30fb20327e29

KMS > Customer-managed keys > Key ID: c5999133-bfd8-4c42-82a9-30fb20327e29

c5999133-bfd8-4c42-82a9-30fb20327e29

General configuration

Alias
demokeyforKMS

ARN copied

arn:aws:kms:ap-south-1:339712766612:key/c5999133-bfd8-4c42-82a9-30fb20327e29

Status
Enabled

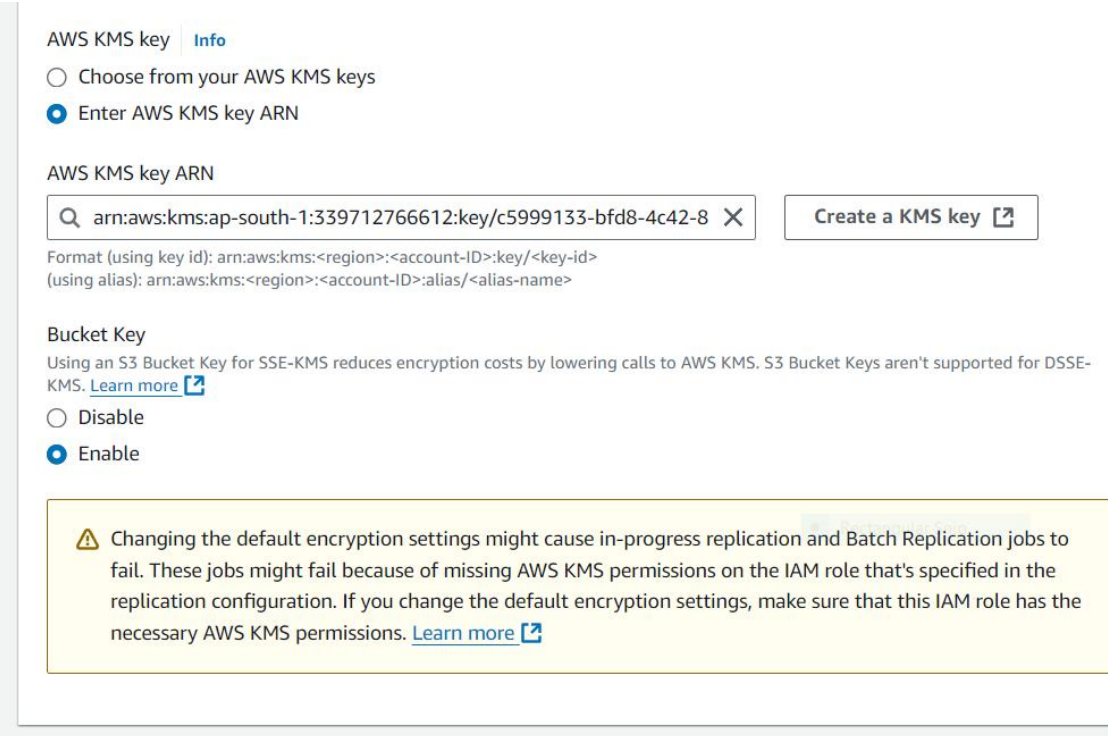
Description
-

Creati
Nov 0

Regio
Single

Key policy

Paste the ARN and save changes.



AWS KMS key Info

○ Choose from your AWS KMS keys

● Enter AWS KMS key ARN

AWS KMS key ARN

arn:aws:kms:ap-south-1:339712766612:key/c5999133-bfd8-4c42-8

Format (using key id): arn:aws:kms:<region>:<account-ID>:key/<key-id>
(using alias): arn:aws:kms:<region>:<account-ID>:alias/<alias-name>

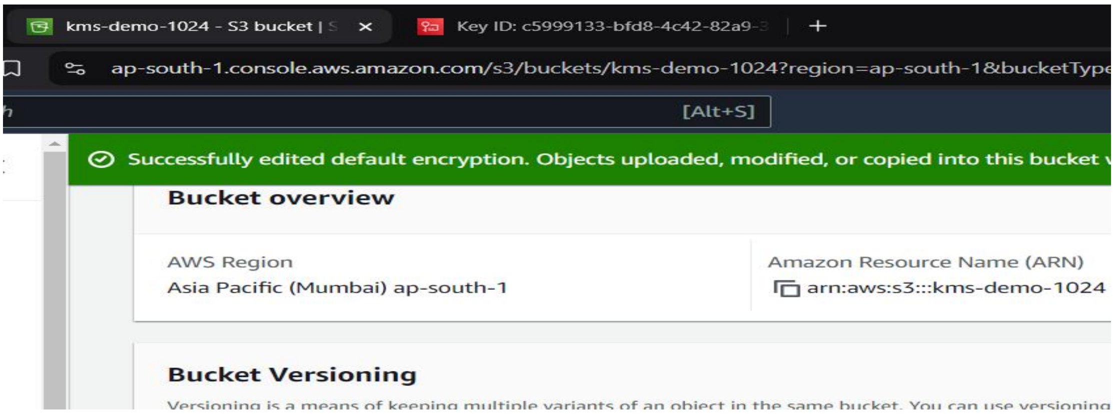
Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

○ Disable

● Enable

Changing the default encryption settings might cause in-progress replication and Batch Replication jobs to fail. These jobs might fail because of missing AWS KMS permissions on the IAM role that's specified in the replication configuration. If you change the default encryption settings, make sure that this IAM role has the necessary AWS KMS permissions. Learn more



kms-demo-1024 - S3 bucket | S
Key ID: c5999133-bfd8-4c42-82a9-
[Alt+S]

ap-south-1.console.aws.amazon.com/s3/buckets/kms-demo-1024?region=ap-south-1&bucketType

Successfully edited default encryption. Objects uploaded, modified, or copied into this bucket v

Bucket overview

AWS Region
Asia Pacific (Mumbai) ap-south-1

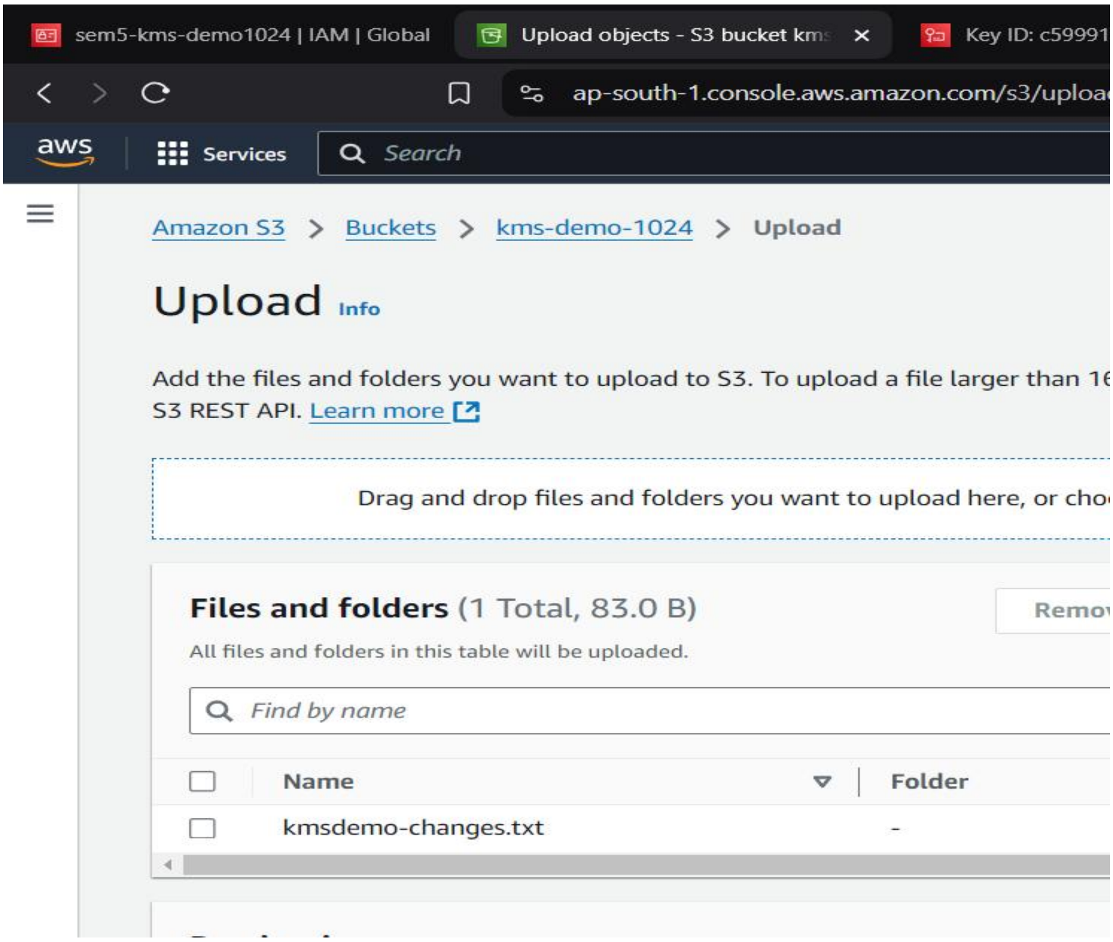
Amazon Resource Name (ARN)
arn:aws:s3:::kms-demo-1024

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning

Now this bucket has encryption type: SSE-KMS(encryption and decryption both)

Go to bucket and upload new file.



sem5-kms-demo1024 | IAM | Global
Upload objects - S3 bucket kms
Key ID: c59991
ap-south-1.console.aws.amazon.com/s3/uploa
aws
Services
Search
Amazon S3 > Buckets > kms-demo-1024 > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 16
S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or cho

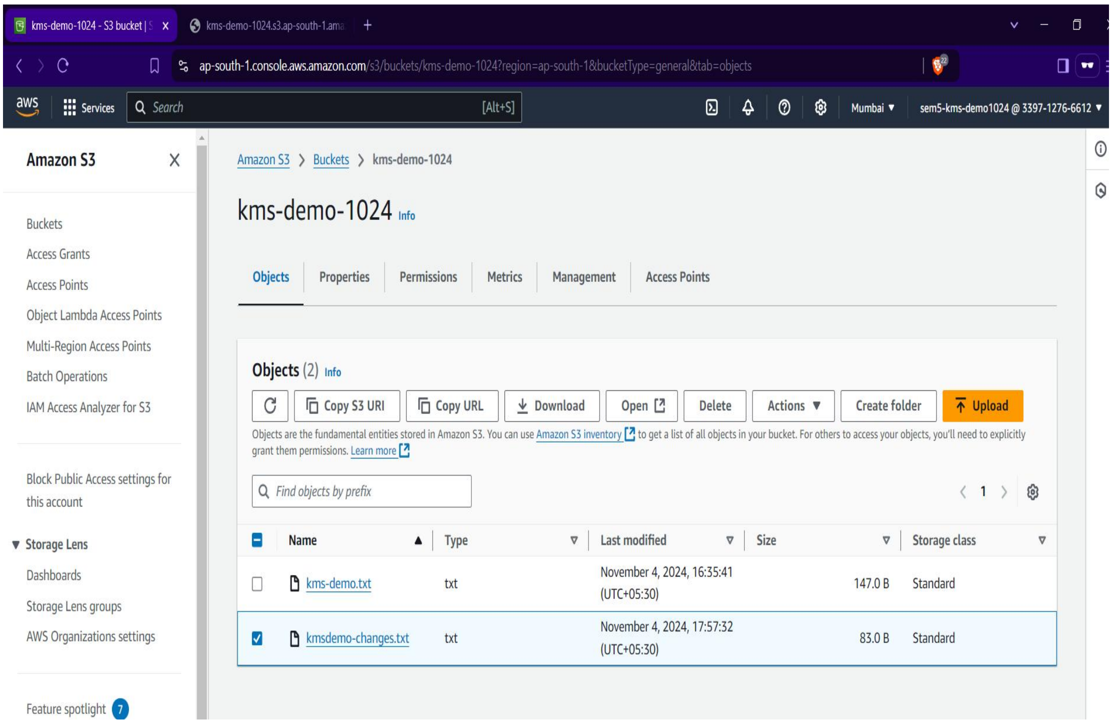
Files and folders (1 Total, 83.0 B)

All files and folders in this table will be uploaded.

	Name	Folder
□	kmsdemo-changes.txt	-

STEP4: Go to IAM-USER

Go to IAM user, S3 service, go to your object and try to access newly uploaded file.



ap-south-1.console.aws.amazon.com/s3/buckets/kms-demo-1024?region=ap-south-1&bucketType=general&tab=objects

Amazon S3 > Buckets > kms-demo-1024

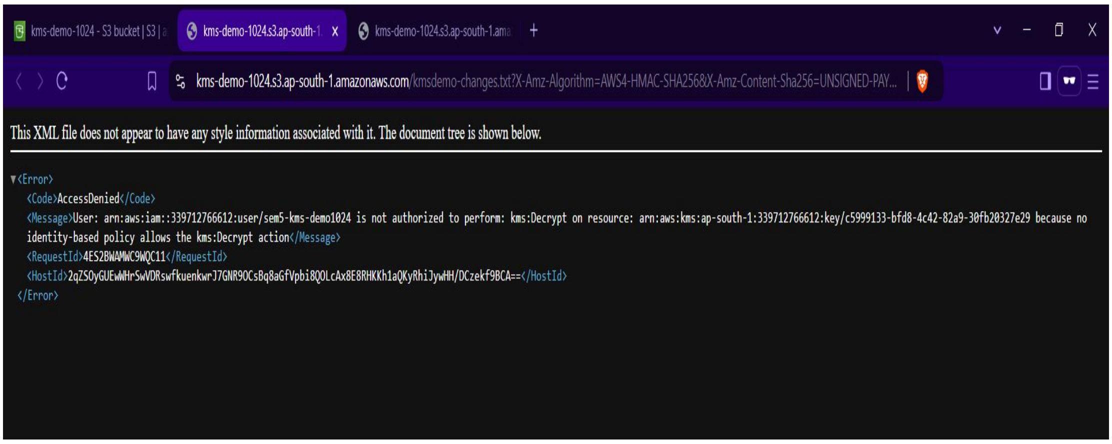
kms-demo-1024 Info

Objects (2) Info

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

	Name	Type	Last modified	Size	Storage class
□	kms-demo.txt	txt	November 4, 2024, 16:35:41 (UTC+05:30)	147.0 B	Standard
☑	kmsdemo-changes.txt	txt	November 4, 2024, 17:57:32 (UTC+05:30)	83.0 B	Standard

Access denied.



kms-demo-1024.s3.ap-south-1.amazonaws.com/kmsdemo-changes.txt?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAY...

This XML file does not appear to have any style information associated with it. The document tree is shown below.

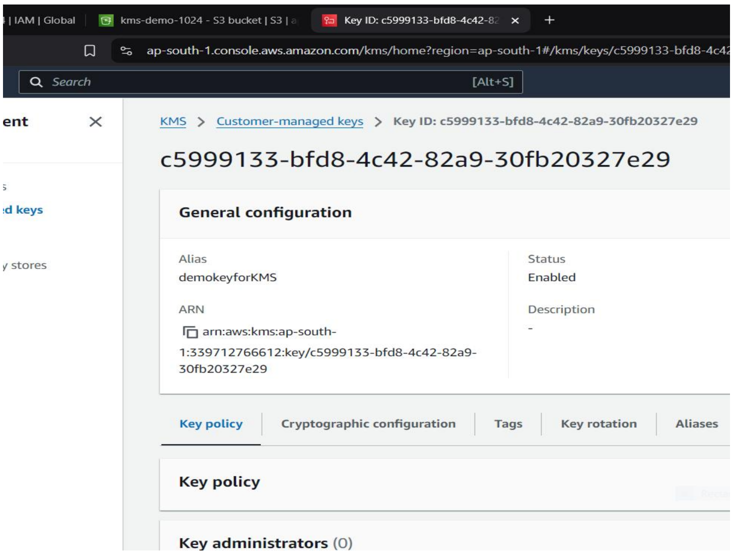
```
▼<Error>
  <Code>AccessDenied</Code>
  <Message>User: arn:aws:iam::339712766612:user/sem5-kms-demo1024 is not authorized to perform: kms:Decrypt on resource: arn:aws:kms:ap-south-1:339712766612:key/c5999133-bfd8-4c42-82a9-30fb20327e29 because no
  identity-based policy allows the kms:Decrypt action</Message>
  <RequestId>4ES2BWAMWC9WQC11</RequestId>
  <HostId>2qZSOyGUEwWHrSwVDRswfkuenkwrJ7GNR9OCsBq8aGfVpbi8QOLcAx8E8RHKKh1aQKyRhiJywHH/DCzekf9BCA==</HostId>
</Error>
```

kms-demo-1024 - S3 bucket | S3
kms-demo-1024.s3.ap-south-1
kms-demo-1024.s3.ap-south-1.ama

This is because Root-user have encrypted the object using KMS key and with that even if user has full access for the service it can't access the objects unless it has kms access too .For that,

STEP5: Go to ROOT-USER

Go to kms and select the key--



KMS > Customer-managed keys > Key ID: c5999133-bfd8-4c42-82a9-30fb20327e29

c5999133-bfd8-4c42-82a9-30fb20327e29

General configuration

Alias: demokeyforKMS

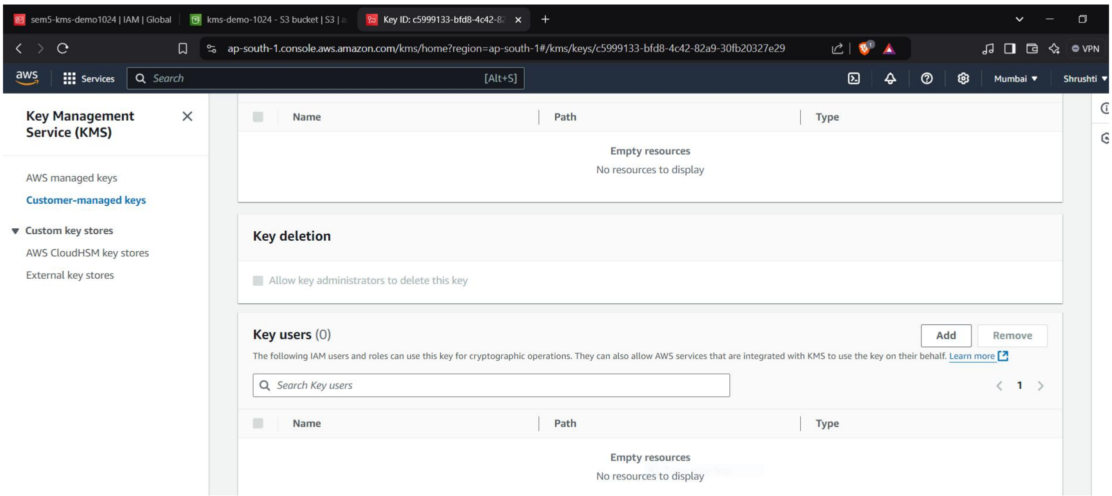
Status: Enabled

ARN: arn:aws:kms:ap-south-1:339712766612:key/c5999133-bfd8-4c42-82a9-30fb20327e29

Description: -

| IAM | Global
kms-demo-1024 - S3 bucket | S3 | a
Key ID: c5999133-bfd8-4c42-82
ap-south-1.console.aws.amazon.com/kms/home?region=ap-south-1#/kms/keys/c5999133-bfd8-4c42
Search [Alt+S]
ent
d keys
y stores
Key policy
Cryptographic configuration
Tags
Key rotation
Aliases
Key policy
Key administrators (0)

Scroll up,



Key deletion

☐ Allow key administrators to delete this key

Key users (0)

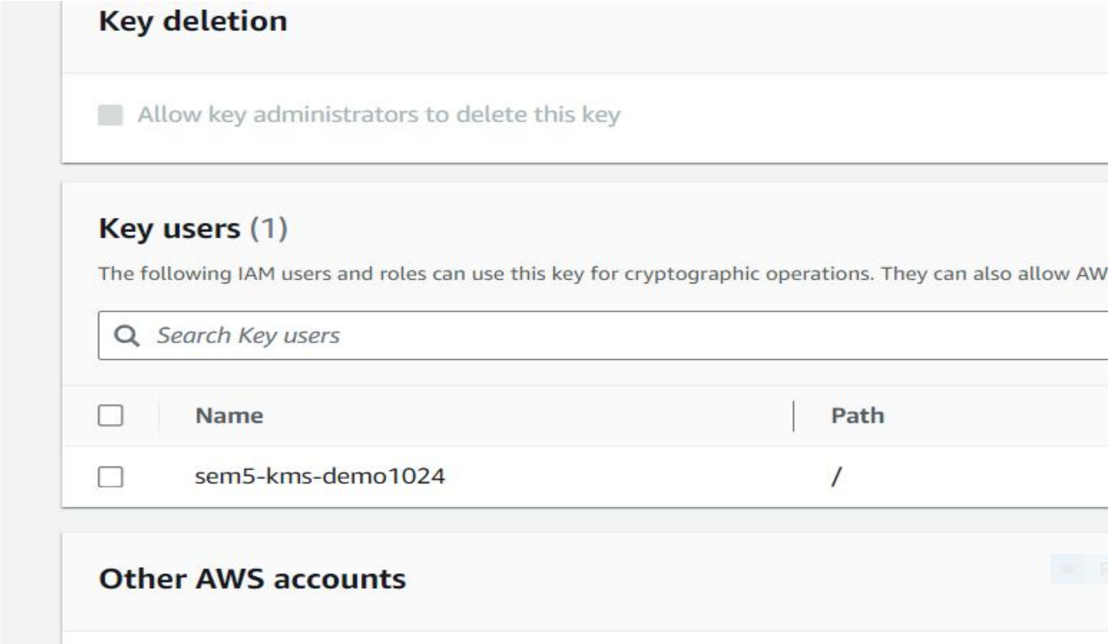
The following IAM users and roles can use this key for cryptographic operations. They can also allow AWS services that are integrated with KMS to use the key on their behalf. Learn more

Name	Path	Type

Empty resources
No resources to display

sem5-kms-demo1024 | IAM | Global
kms-demo-1024 - S3 bucket | S3 | a
Key ID: c5999133-bfd8-4c42-82
ap-south-1.console.aws.amazon.com/kms/home?region=ap-south-1#/kms/keys/c5999133-bfd8-4c42-82a9-30fb20327e29
VPN
aws
Services
Search [Alt+S]
Mumbai
Shrushti
Key Management Service (KMS)
AWS managed keys
Customer-managed keys
Custom key stores
AWS CloudHSM key stores
External key stores
Name
Path
Type
Empty resources
No resources to display
Add
Remove
Search Key users
1

Add user.



Key deletion

□ Allow key administrators to delete this key

Key users (1)

The following IAM users and roles can use this key for cryptographic operations. They can also allow AW

Search Key users

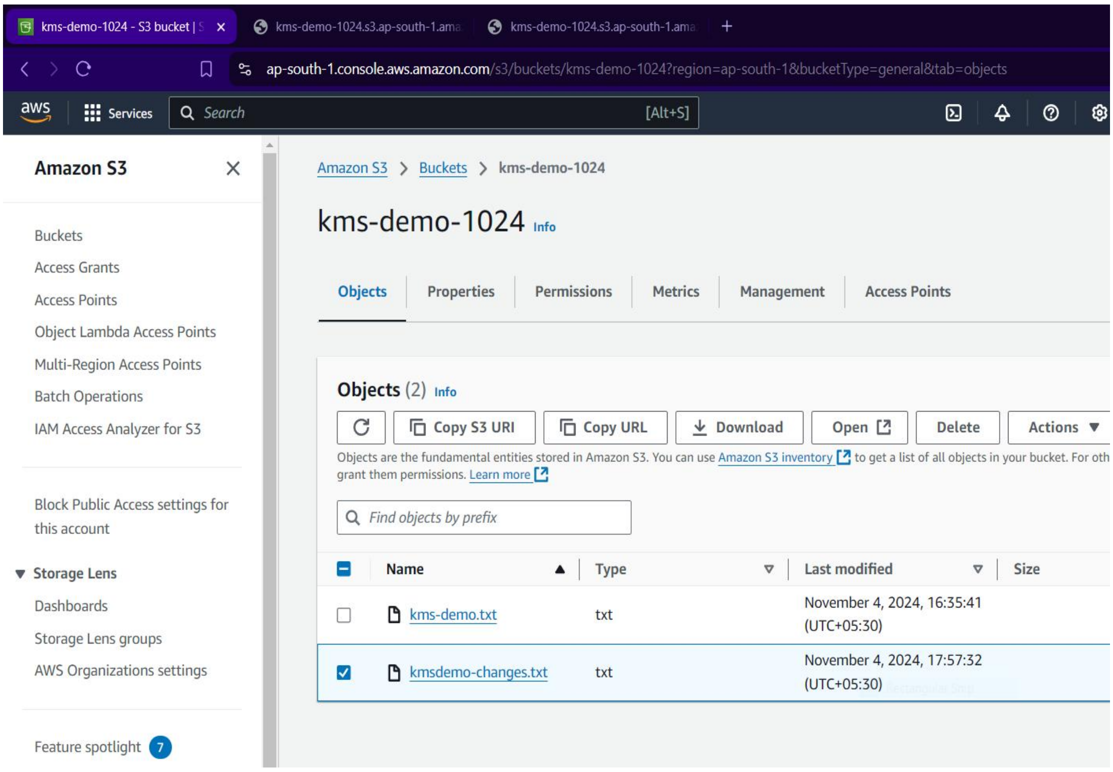
□	Name	Path
□	sem5-kms-demo1024	/

Other AWS accounts

This allow the specific user to do cryptographic operation(which means the user can encrypt and decrypt the file using this kms key)

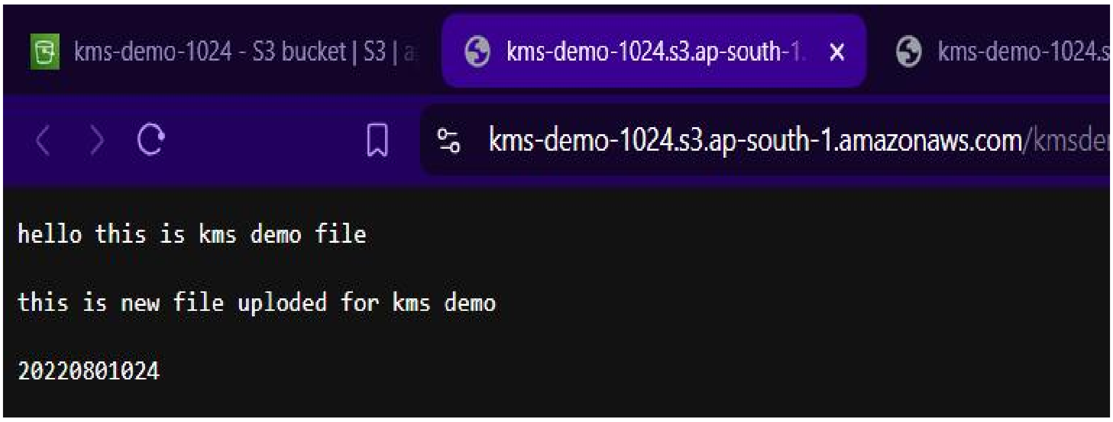
STEP6: Go to IAM-USER

Go to IAM user, and try to access the file again


kms-demo-1024 - S3 bucket | S
kms-demo-1024.s3.ap-south-1.ama
kms-demo-1024.s3.ap-south-1.ama
ap-south-1.console.aws.amazon.com/s3/buckets/kms-demo-1024?region=ap-south-1&bucketType=general&tab=objects
aws
Services
Search
[Alt+S]
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
Feature spotlight 7
Amazon S3 > Buckets > kms-demo-1024
kms-demo-1024 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (2) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions ▼
Find objects by prefix

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 oth grant them permissions. Learn more

	Name	Type	Last modified	Size
□	kms-demo.txt	txt	November 4, 2024, 16:35:41 (UTC+05:30)	
☑	kmsdemo-changes.txt	txt	November 4, 2024, 17:57:32 (UTC+05:30)	


kms-demo-1024 - S3 bucket | S3 | a
kms-demo-1024.s3.ap-south-1.
kms-demo-1024.s
kms-demo-1024.s3.ap-south-1.amazonaws.com/kmsde

```
hello this is kms demo file

this is new file uploded for kms demo

20220801024
```

IAM-USER IS NOW ABLE TO ACCESS THE FILE USING KMS ENCRYPTION.