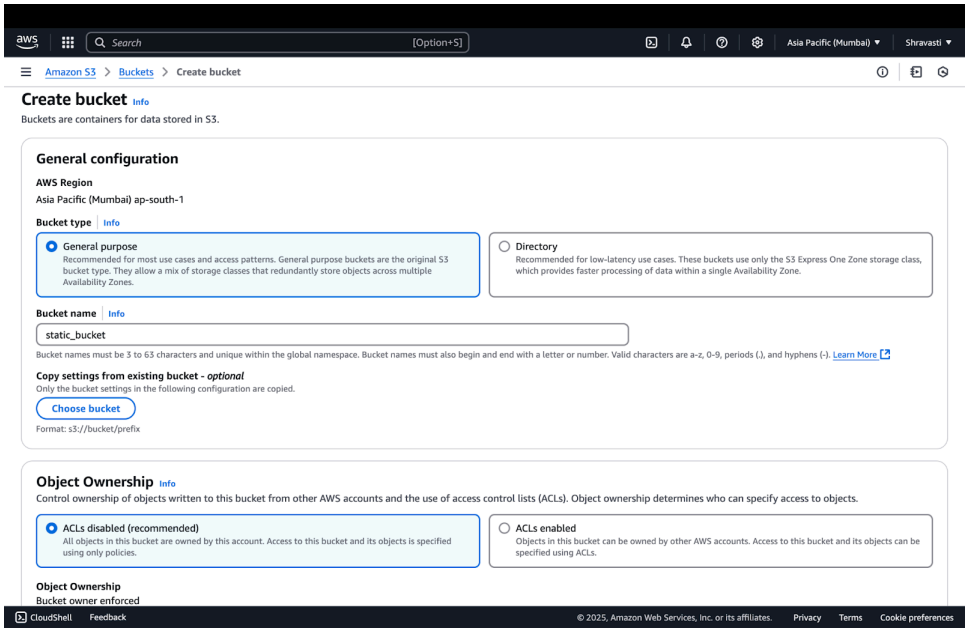
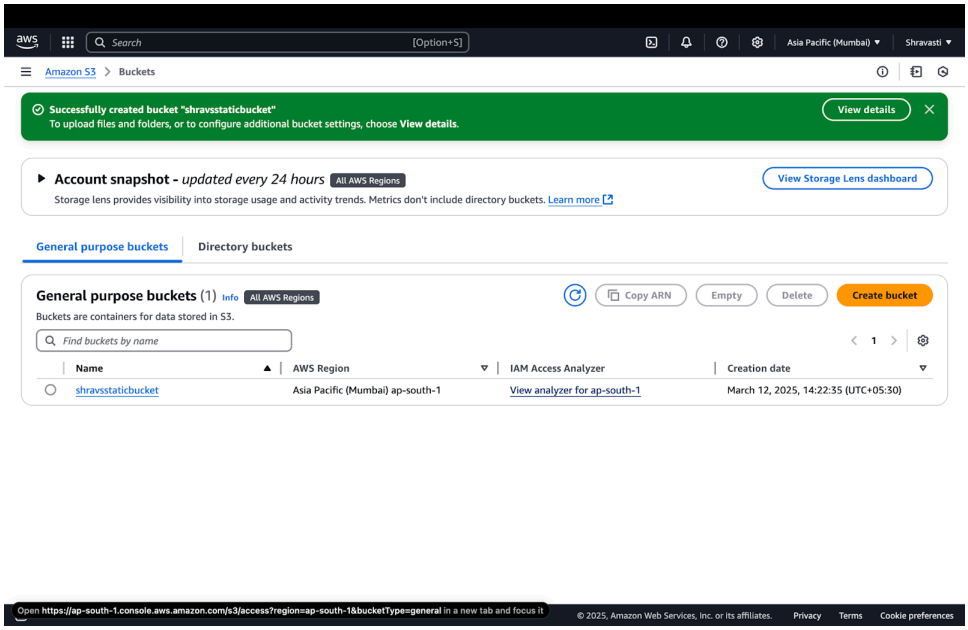
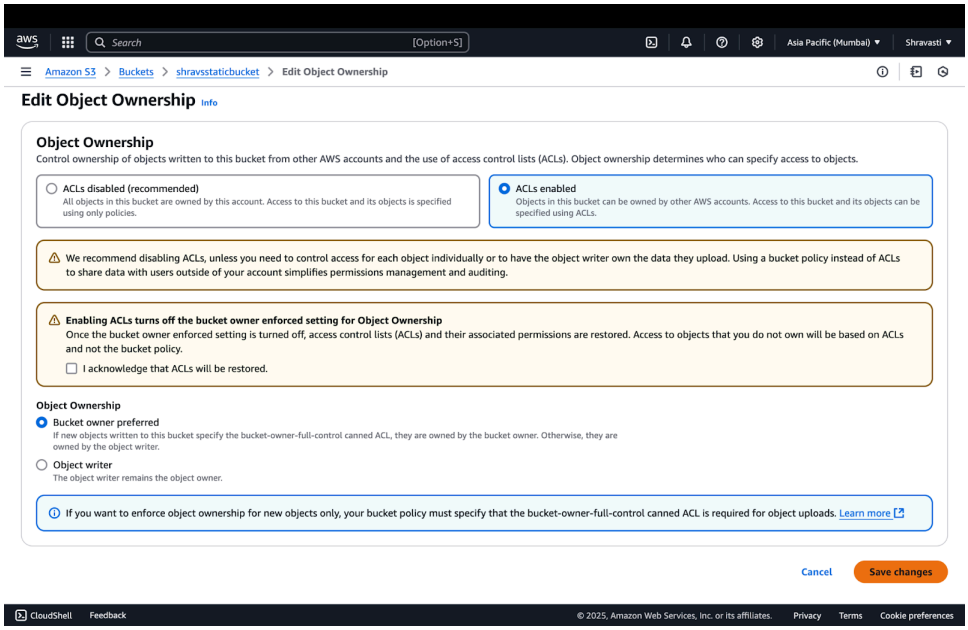
lab 8 : static website hosting using AWS S3

1. Create an S3 bucket

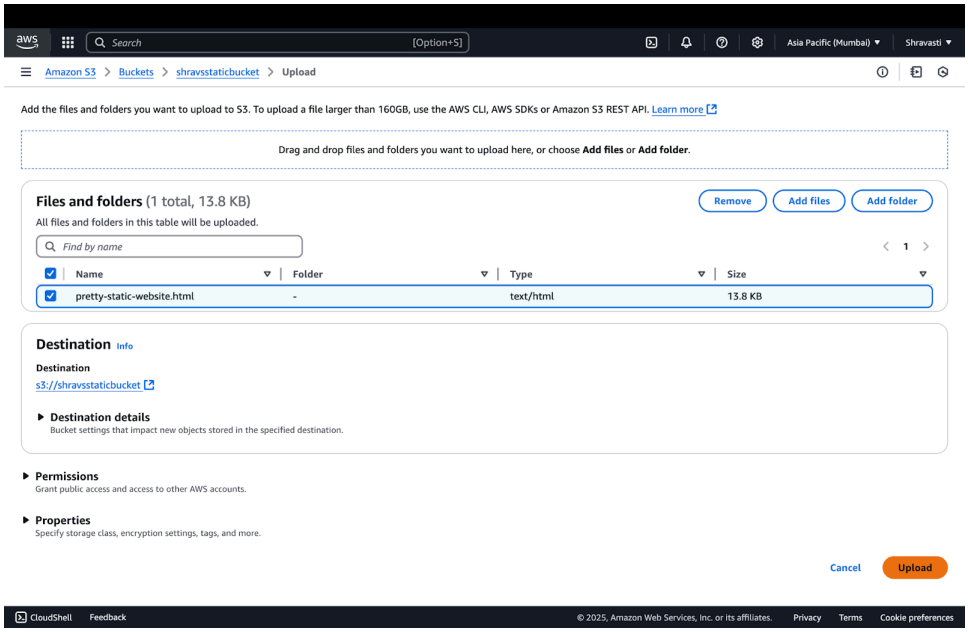


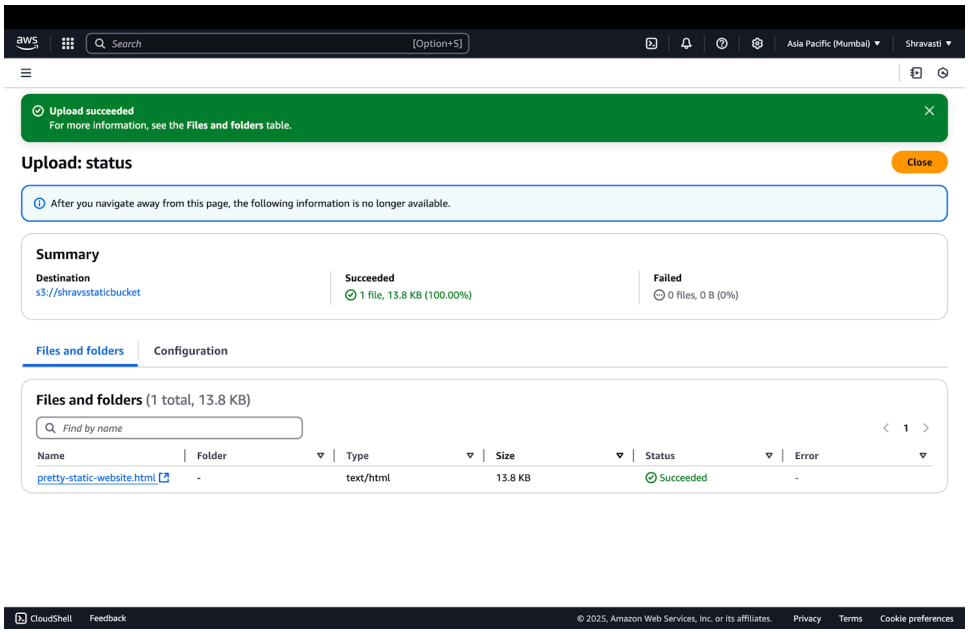


2. Edit Object Ownership to enable Access Control Lists (ACLs)

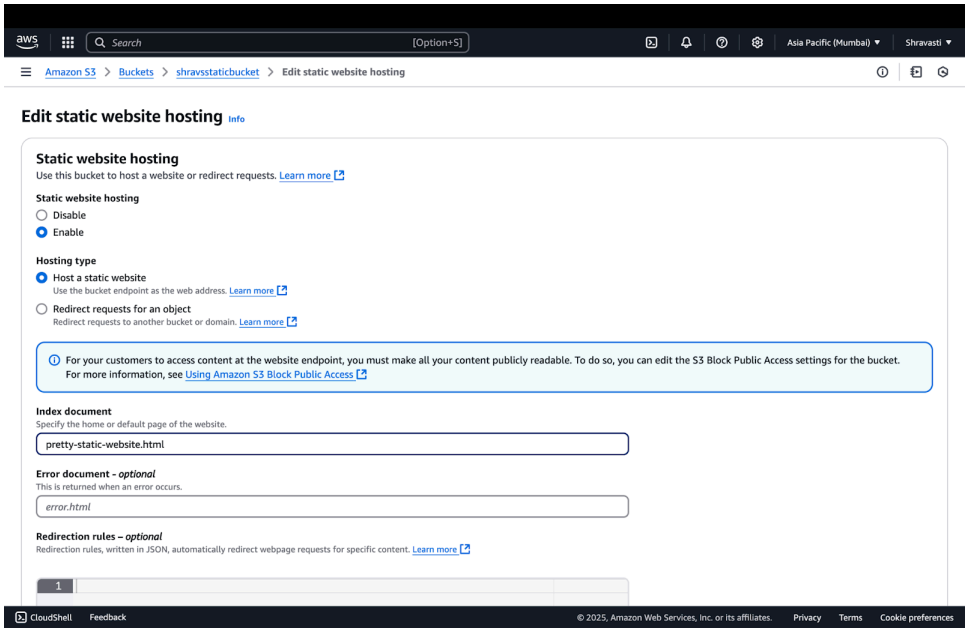


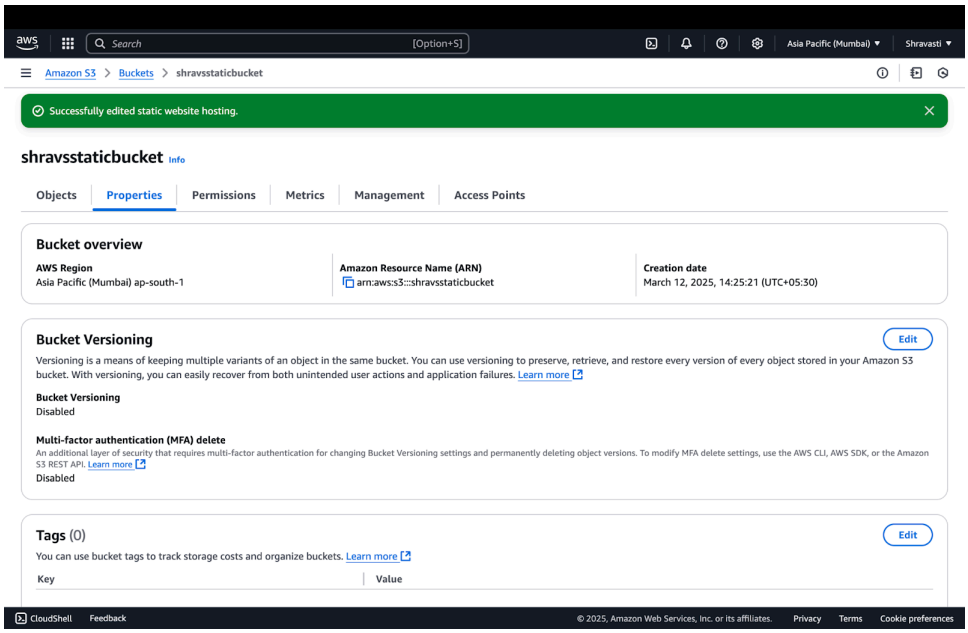
3. Upload an HTML file to the bucket



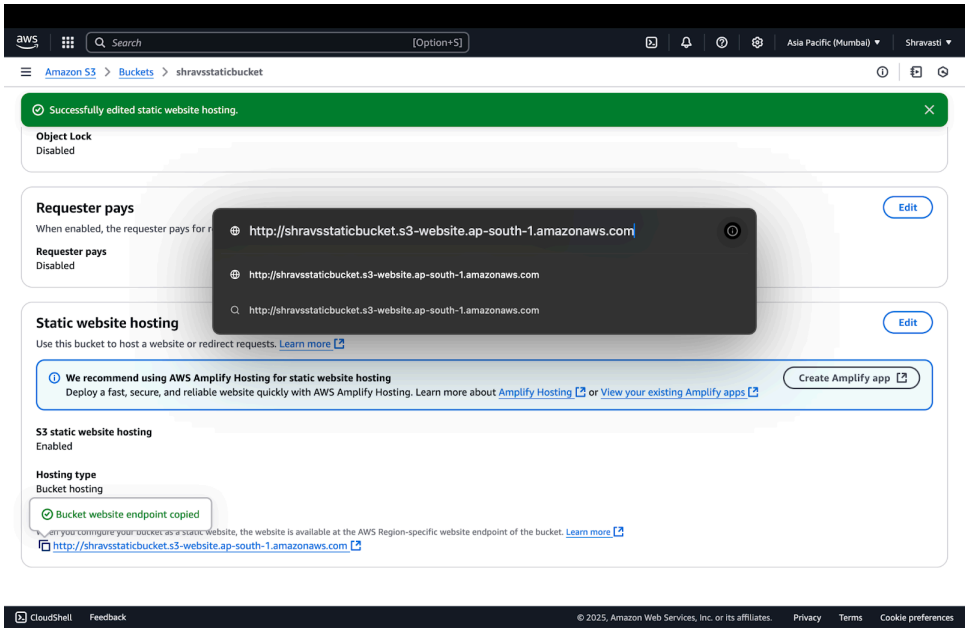


4. Navigate to bucket properties → static website hosting

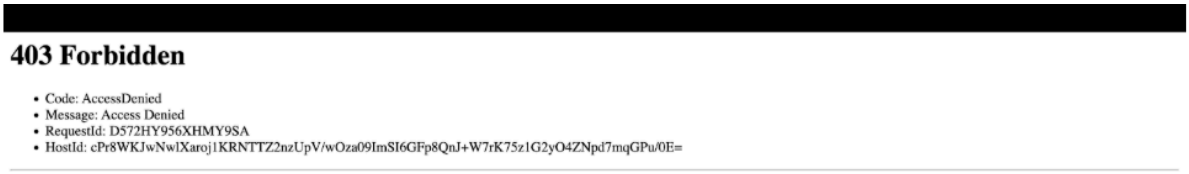




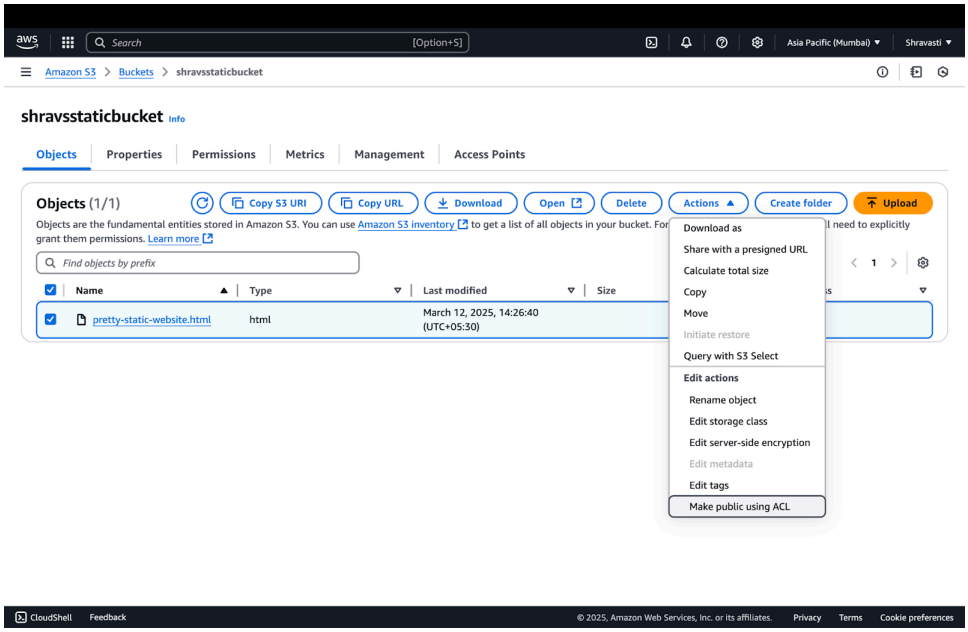
5. Paste the bucket website endpoint link in a browser

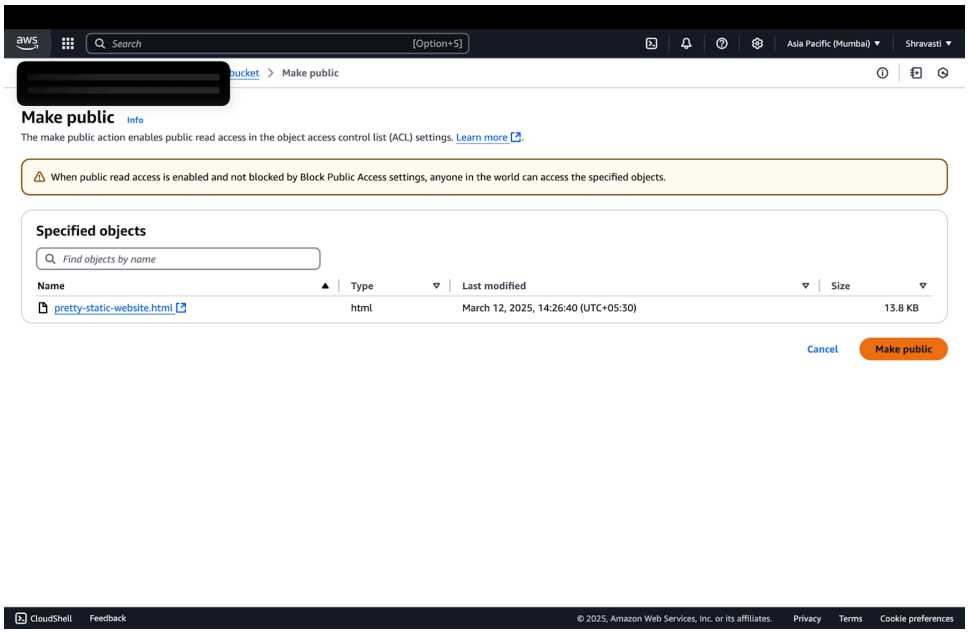


6. Access is denied to the website, since no access policy is written for it

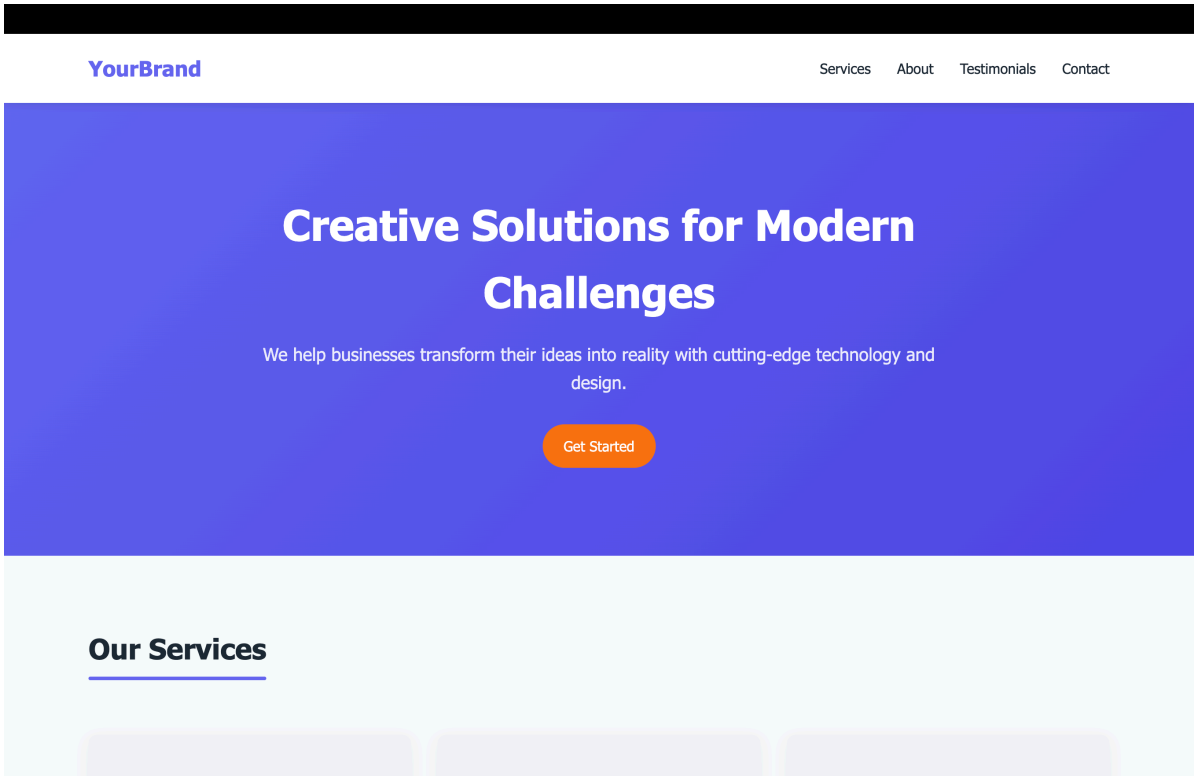


7. Make bucket objects public using ACL

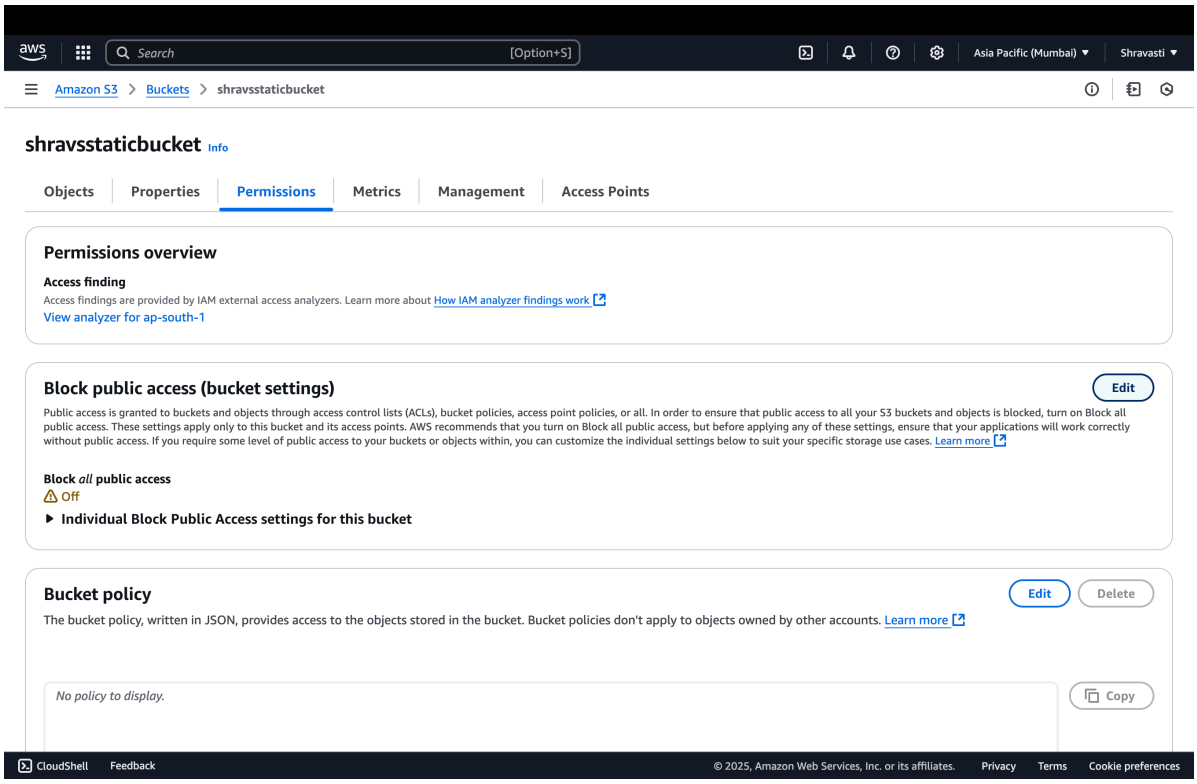


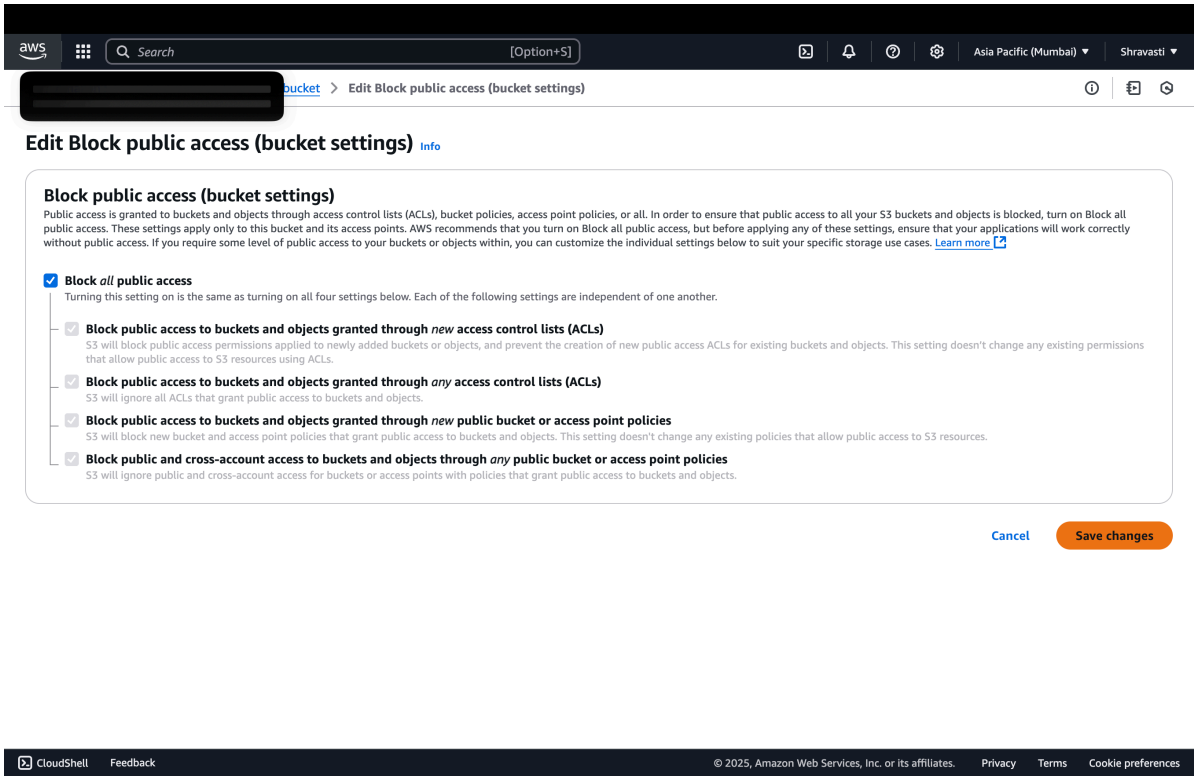


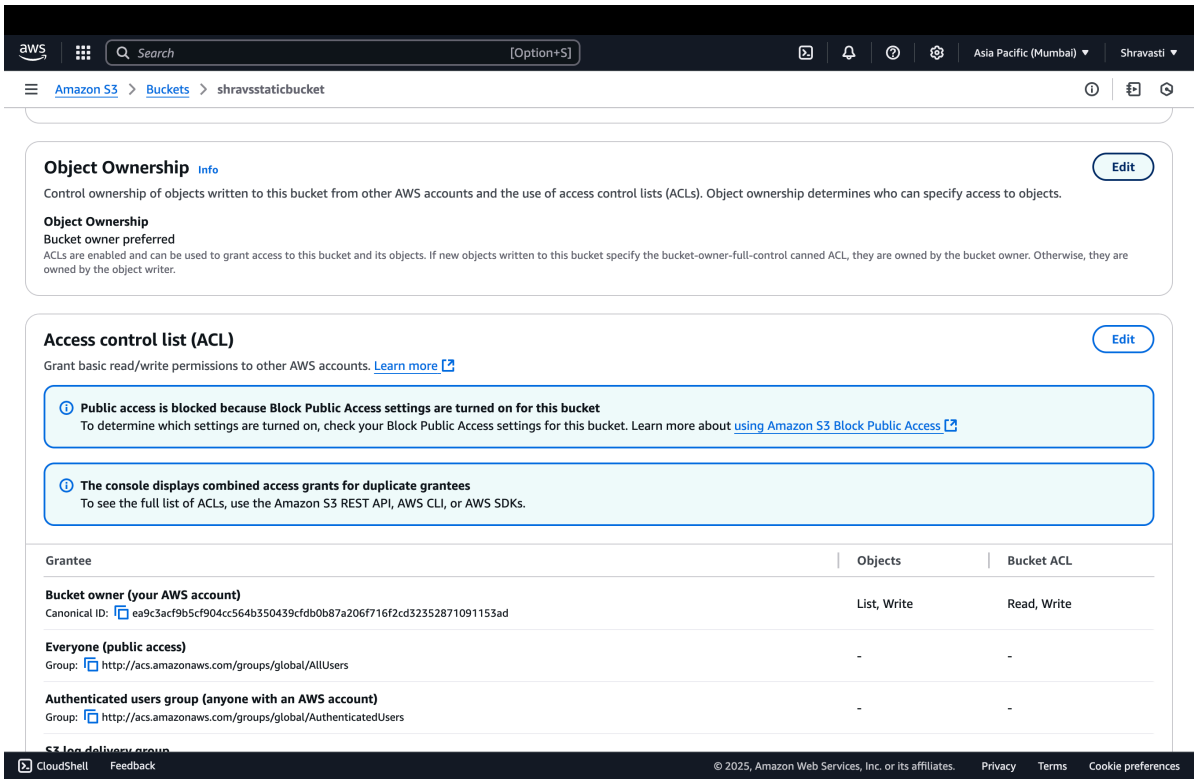
8. Refresh the page and the website will now be visible

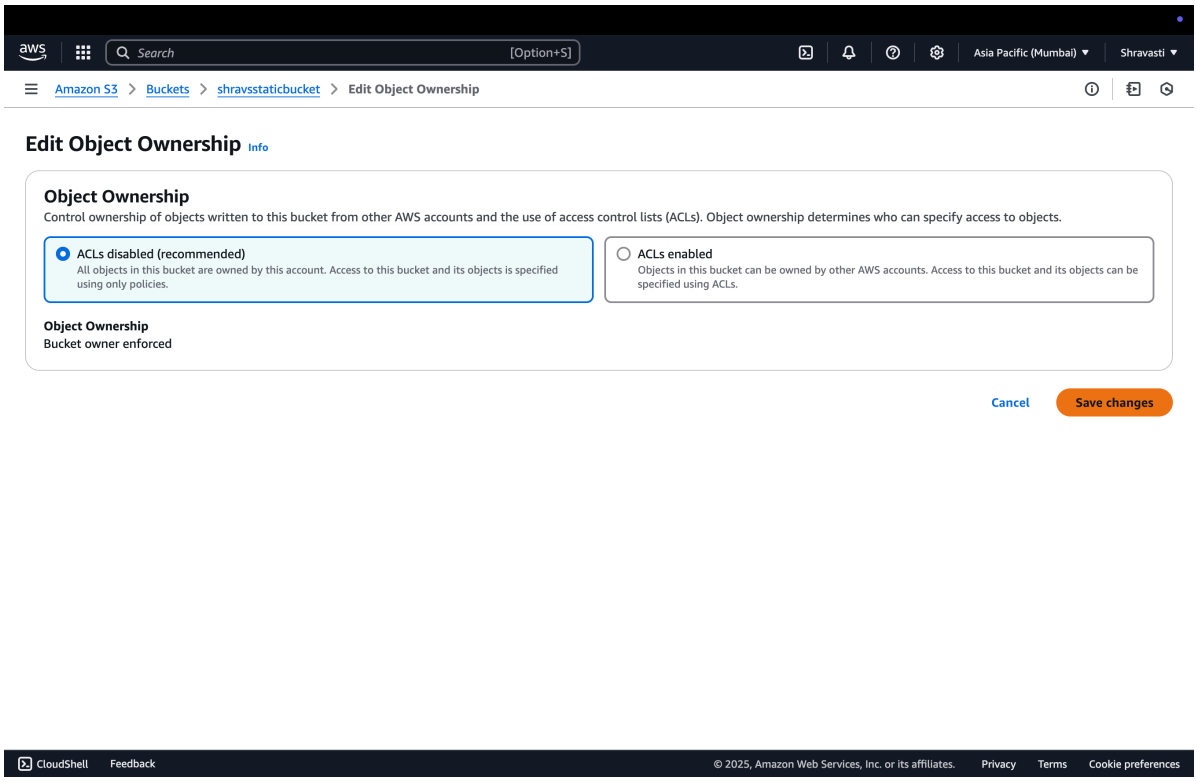


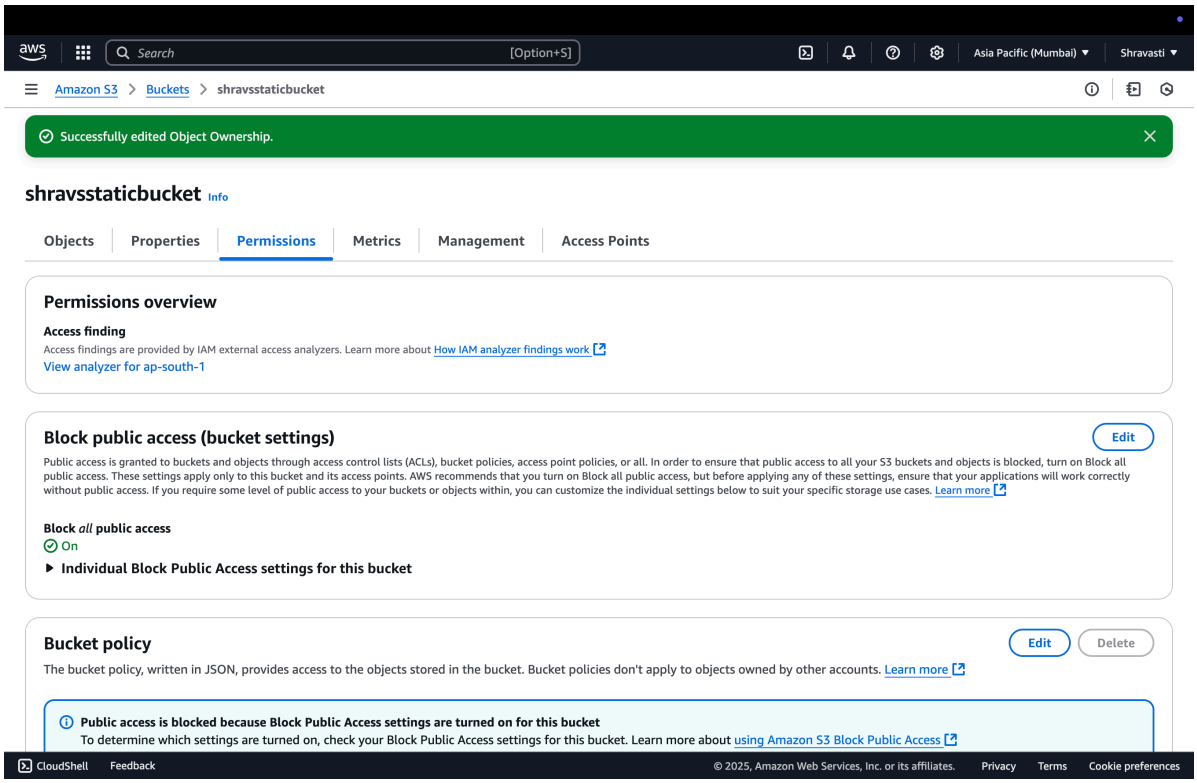
9. Revert ownership and public access settings



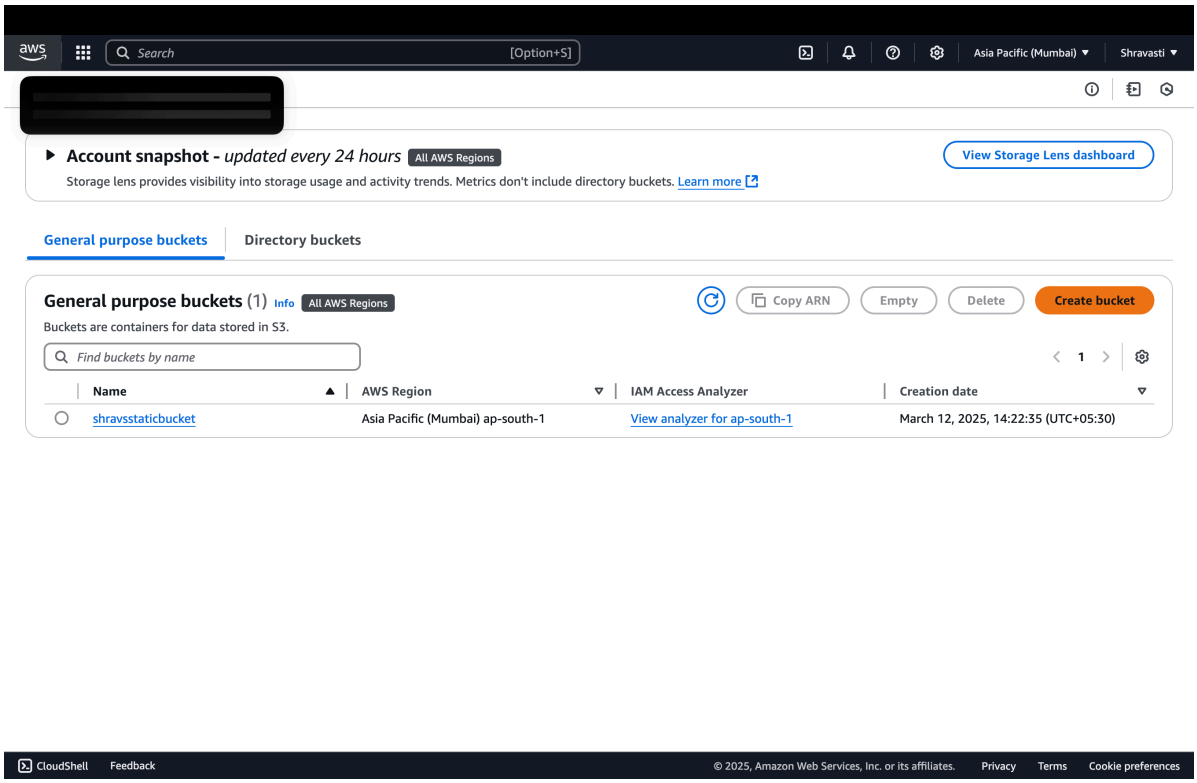


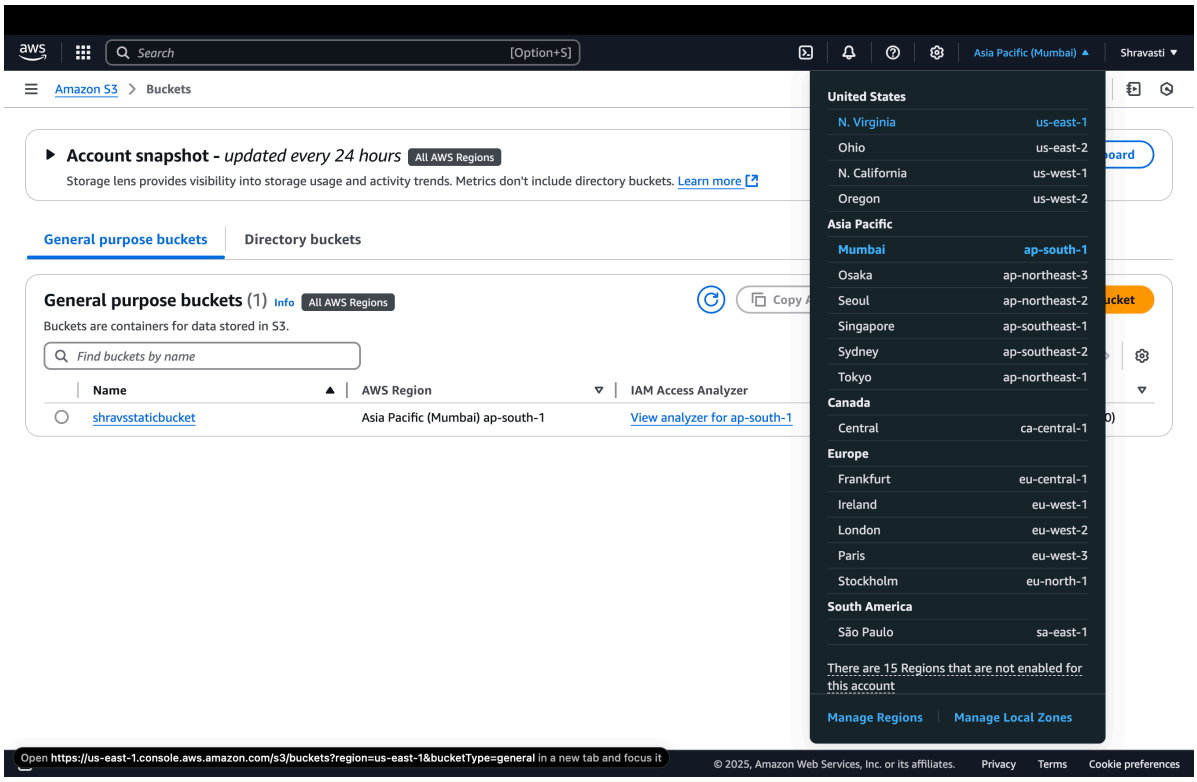

Search
[Option+S]
Asia Pacific (Mumbai)
Shravasti
Amazon S3 > Buckets > shravsstaticbucket
Object Ownership Info
Edit
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
Object Ownership
Bucket owner preferred
ACLs are enabled and can be used to grant access to this bucket and its objects. If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
Access control list (ACL)
Edit
Grant basic read/write permissions to other AWS accounts. Learn more
Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access
The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
Canonical ID: ea9c3acf9b5cf904cc564b350439cfdb0b87a206f716f2cd32352871091153ad
List, Write
Read, Write
Everyone (public access)
Group: http://acs.amazonaws.com/groups/global/AllUsers
-
-
Authenticated users group (anyone with an AWS account)
Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers
-
-
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

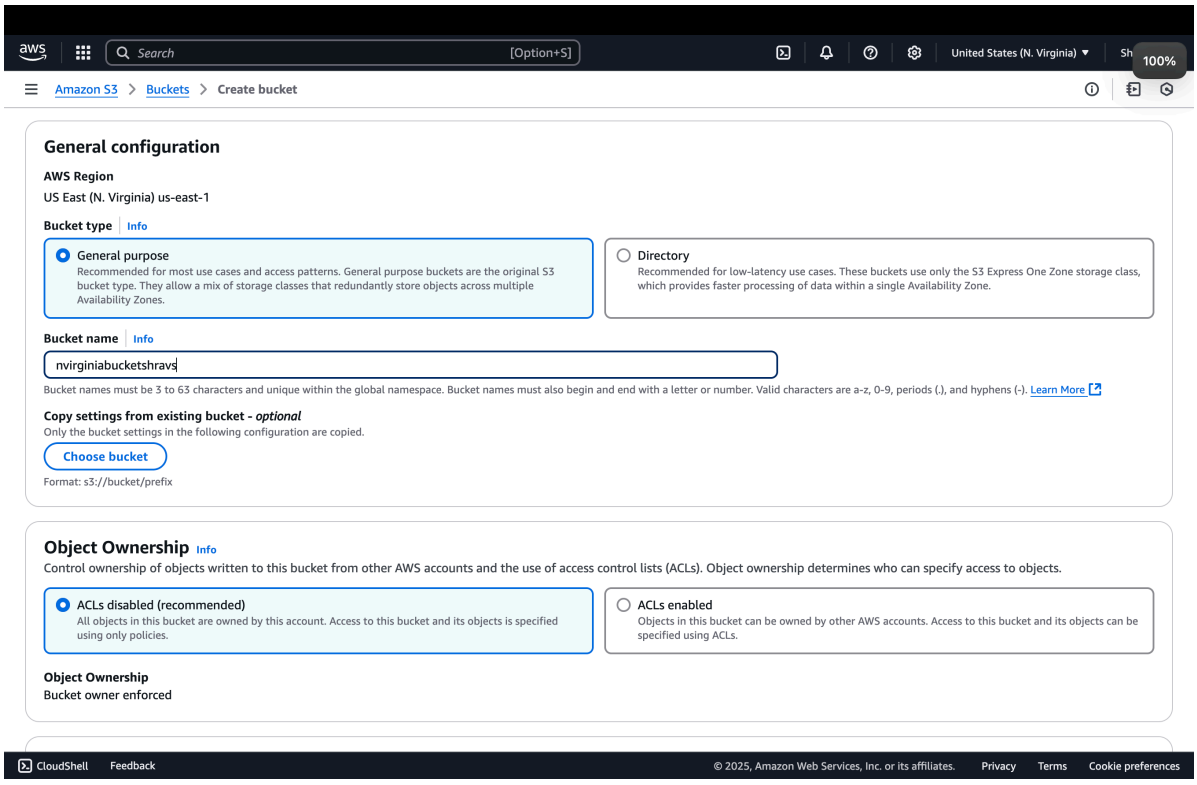

Search
[Option+S]
Asia Pacific (Mumbai)
Shravasti
Amazon S3 > Buckets > shravsstaticbucket > Edit Object Ownership
Edit Object Ownership Info
Object Ownership
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines 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
Cancel
Save changes
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

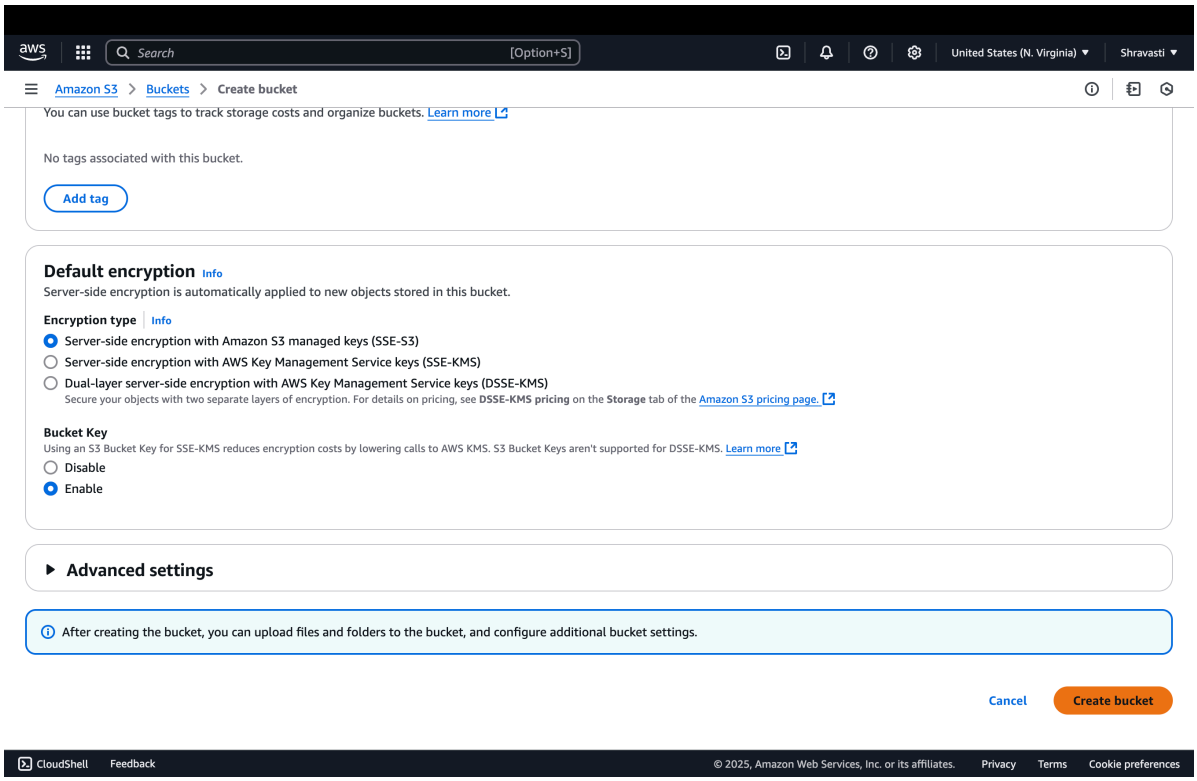


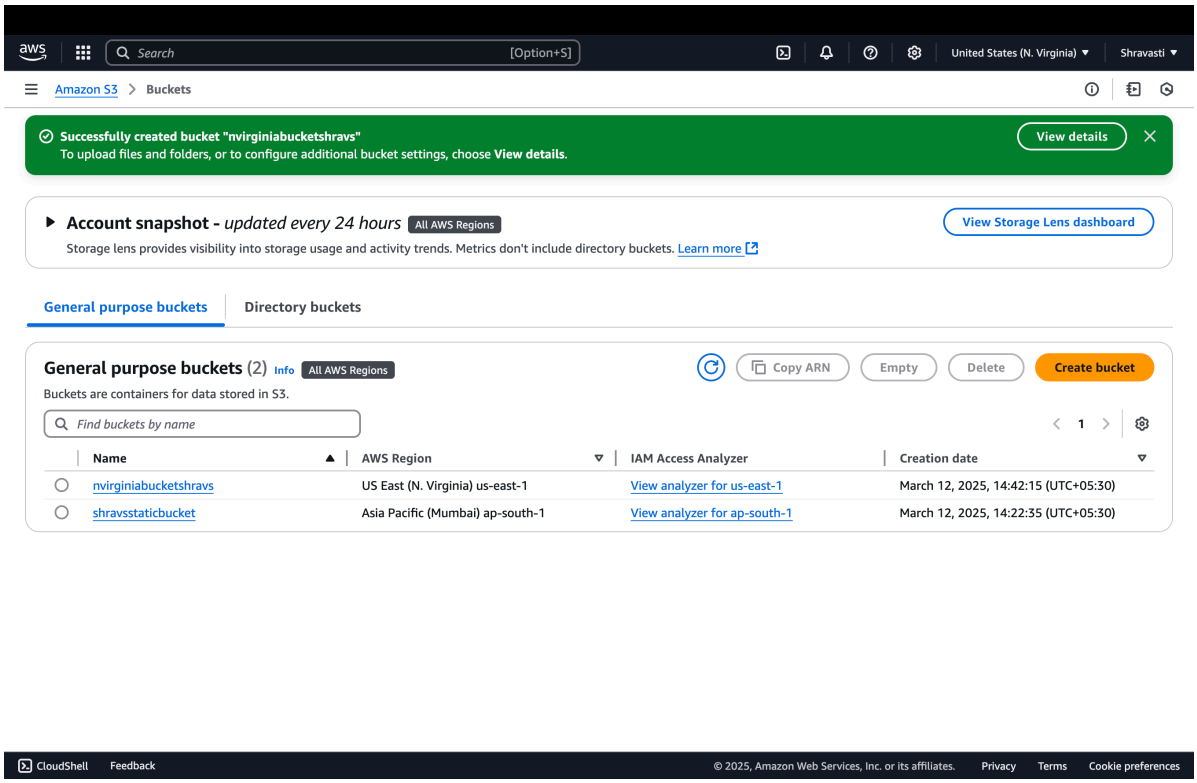
10. Create another bucket in a different region


Search
[Option+S]
Asia Pacific (Mumbai)
Shravasti
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
shravsstaticbucket
Asia Pacific (Mumbai) ap-south-1
View analyzer for ap-south-1
March 12, 2025, 14:22:35 (UTC+05:30)
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

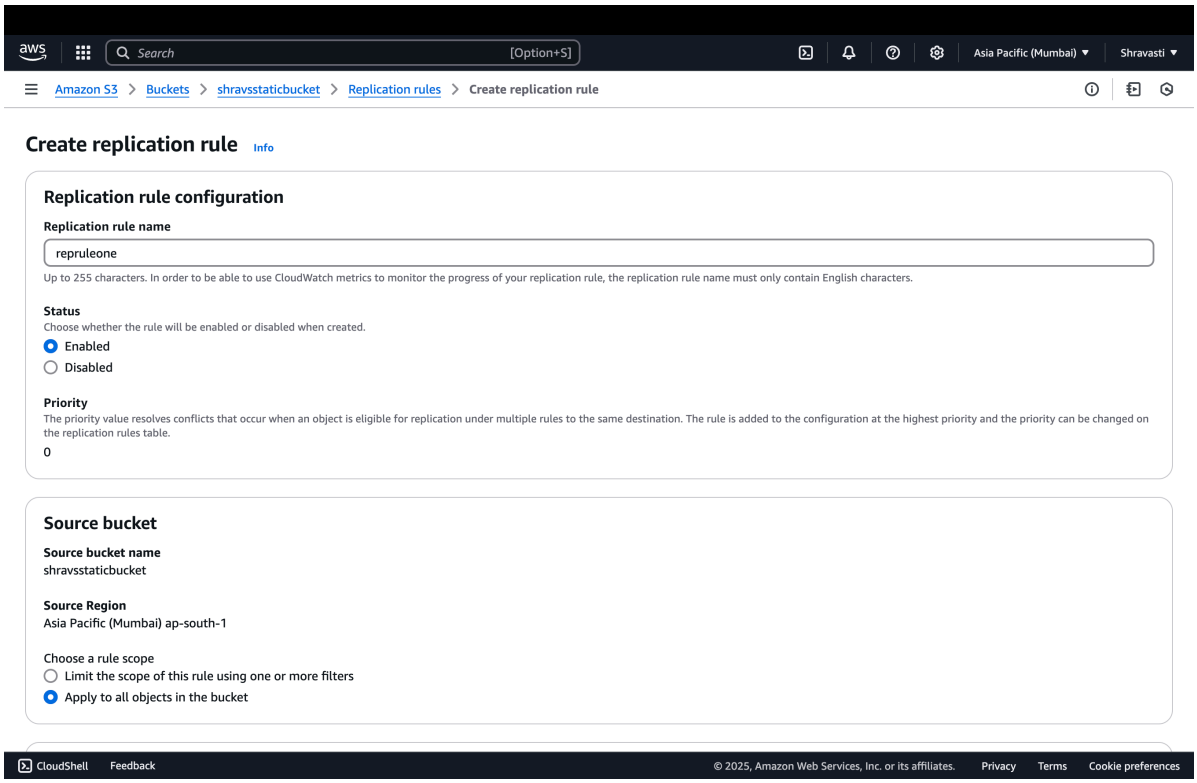

Search
[Option+S]
Asia Pacific (Mumbai)
Shravasti
Amazon S3
Buckets
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Buckets are containers for data stored in S3.
Find buckets by name
Name
AWS Region
IAM Access Analyzer
shravsstaticbucket
Asia Pacific (Mumbai) ap-south-1
View analyzer for ap-south-1
United States
N. Virginia us-east-1
Ohio us-east-2
N. California us-west-1
Oregon us-west-2
Asia Pacific
Mumbai ap-south-1
Osaka ap-northeast-3
Seoul ap-northeast-2
Singapore ap-southeast-1
Sydney ap-southeast-2
Tokyo ap-northeast-1
Canada
Central ca-central-1
Europe
Frankfurt eu-central-1
Ireland eu-west-1
London eu-west-2
Paris eu-west-3
Stockholm eu-north-1
South America
São Paulo sa-east-1
There are 15 Regions that are not enabled for this account
Manage Regions
Manage Local Zones
Open https://us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general in a new tab and focus it
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

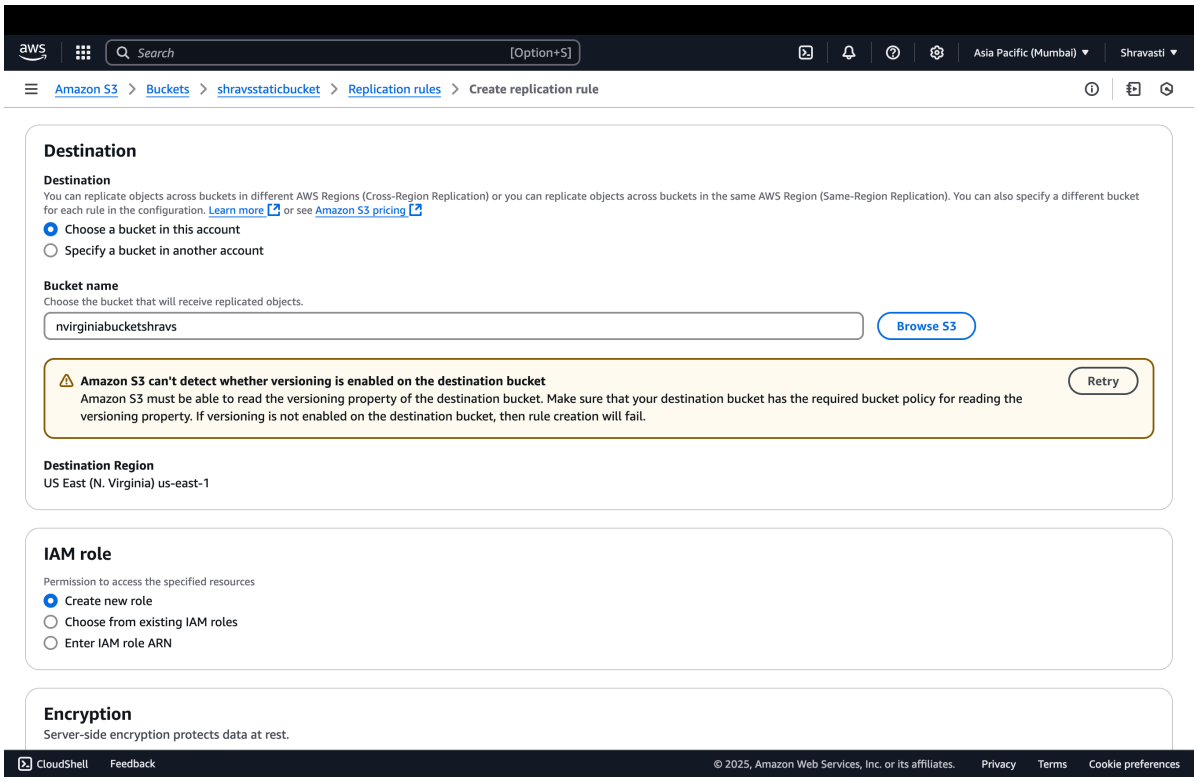

Search [Option+S]
United States (N. Virginia)
100%
Amazon S3 > Buckets > Create bucket
General configuration
AWS Region
US East (N. Virginia) us-east-1
Bucket type Info
General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
Directory
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
nvirginiabucketshravs
Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn More
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
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

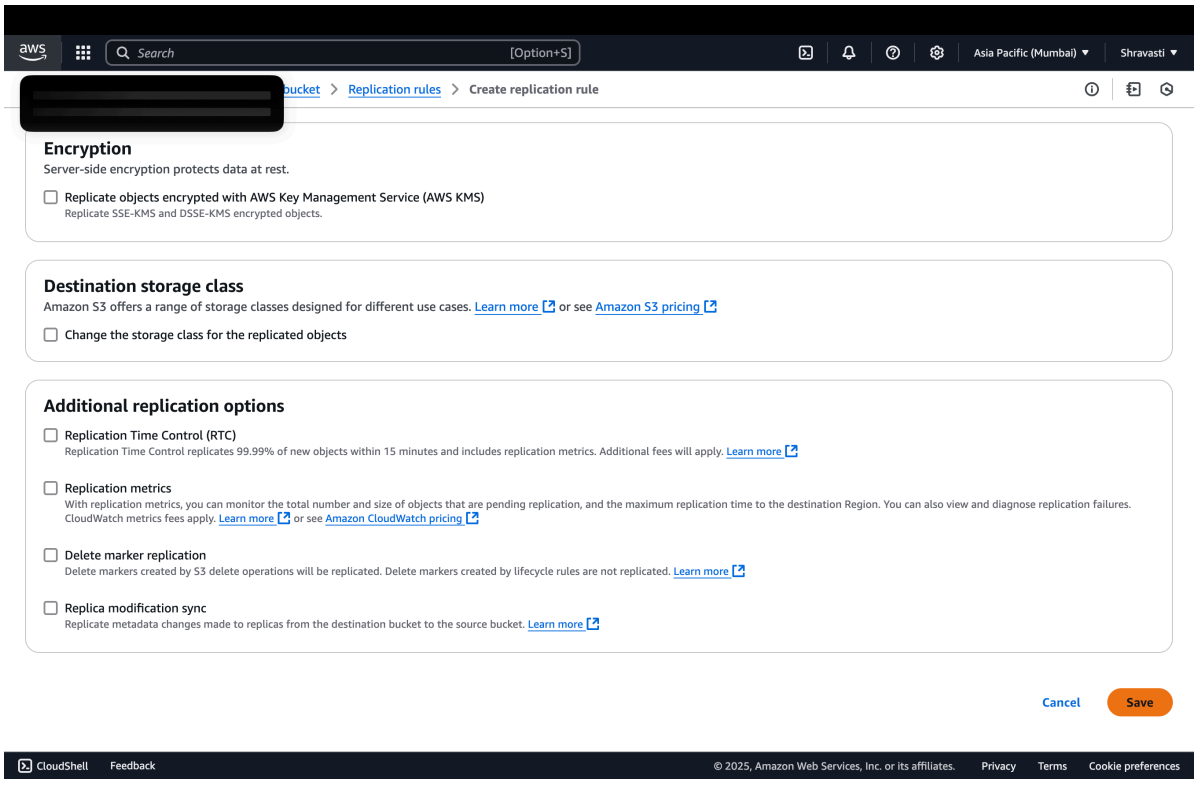

Search [Option+S]
United States (N. Virginia)
Shravasti
Amazon S3 > Buckets > Create bucket
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add tag
Default encryption Info
Server-side encryption is automatically applied to new objects 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.
Cancel
Create bucket
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

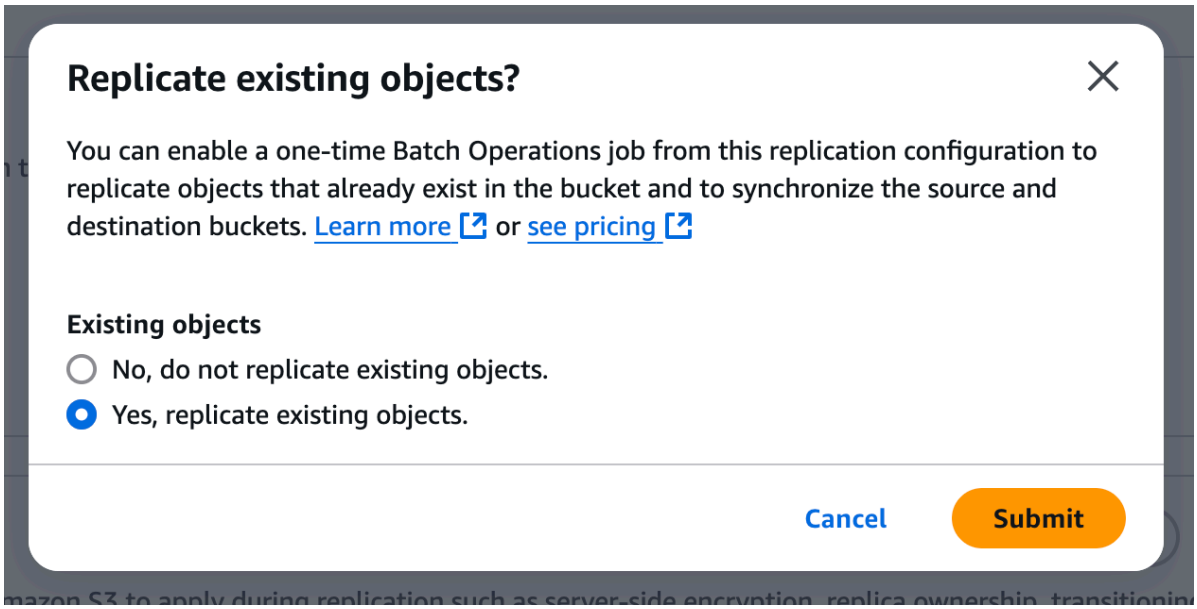


11. Select the bucket created in Mumbai region → navigate to Management tab → Create replication rule

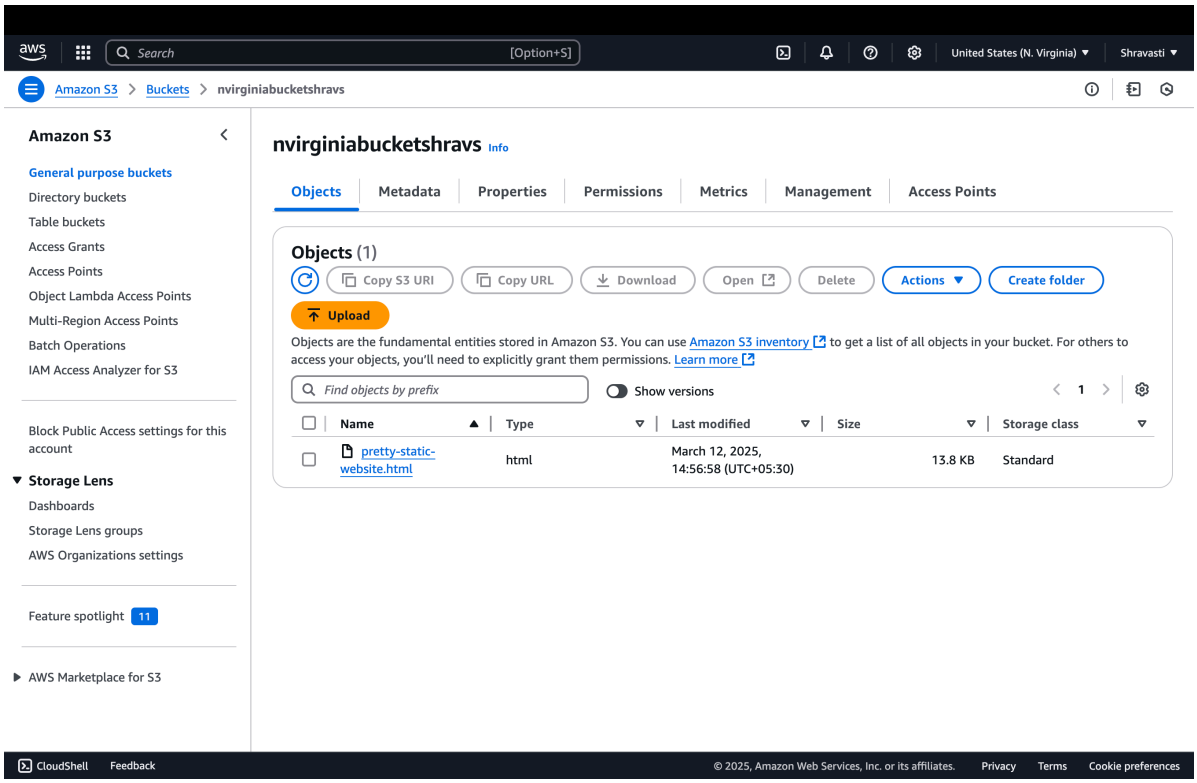

Search
[Option+S]
Asia Pacific (Mumbai)
Shravasti
Amazon S3 > Buckets > shravsstaticbucket > Replication rules > Create replication rule
Create replication rule
Info
Replication rule configuration
Replication rule name
repruleone
Up to 255 characters. In order to be able to use CloudWatch metrics to 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.
0
Source bucket
Source bucket name
shravsstaticbucket
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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Option+S]
Asia Pacific (Mumbai)
Shravasti
Amazon S3 > Buckets > shravsstaticbucket > Replication rules > Create replication rule
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.
nvirginiabucketshravs
Browse S3
Amazon S3 can't detect whether versioning is enabled on the destination bucket
Amazon S3 must be able to read the versioning property of the destination bucket. Make sure that your destination bucket has the required bucket policy for reading the versioning property. If versioning is not enabled on the destination bucket, then rule creation will fail.
Retry
Destination Region
US East (N. Virginia) us-east-1
IAM role
Permission to access the specified resources
Create new role
Choose from existing IAM roles
Enter IAM role ARN
Encryption
Server-side encryption protects data at rest.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

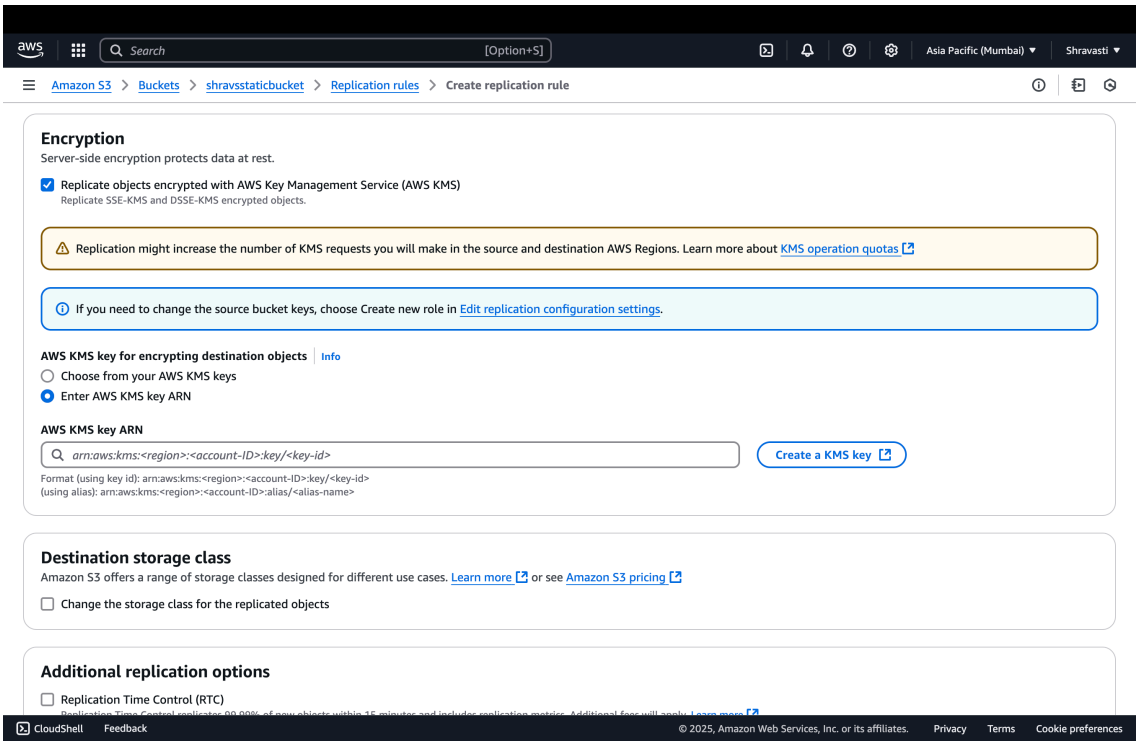




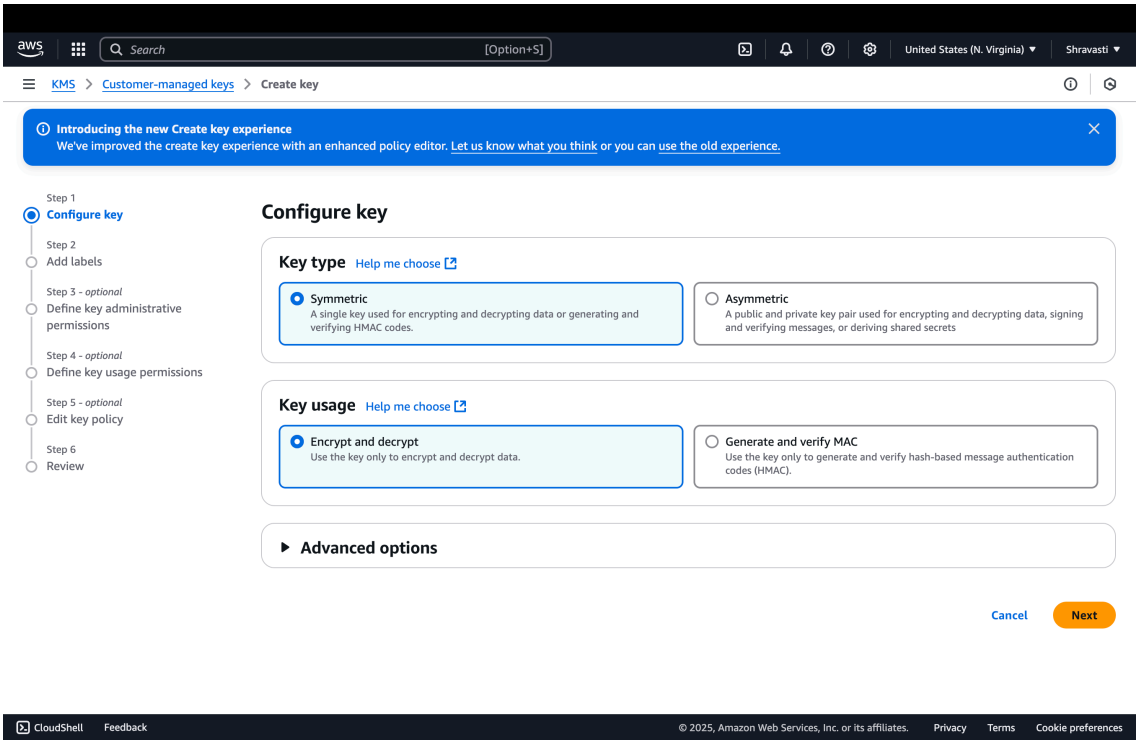
Objects will be replicated in the destination bucket



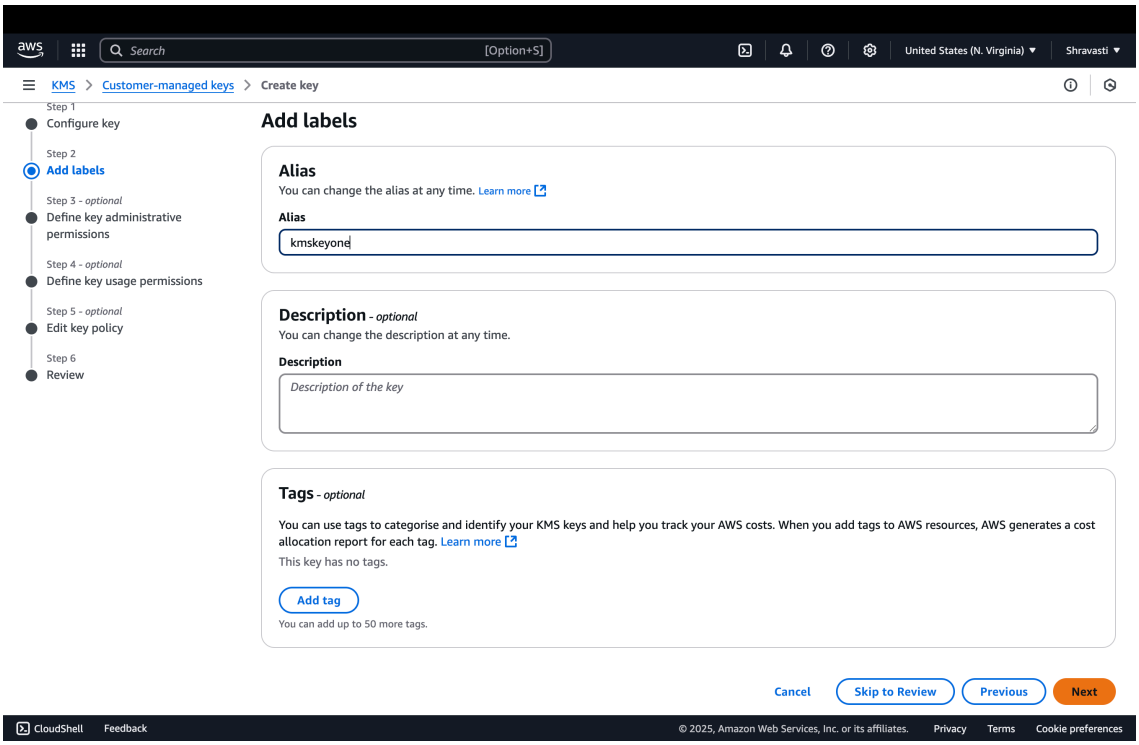
12. KMS
    a. Navigate to Properties → Encryption



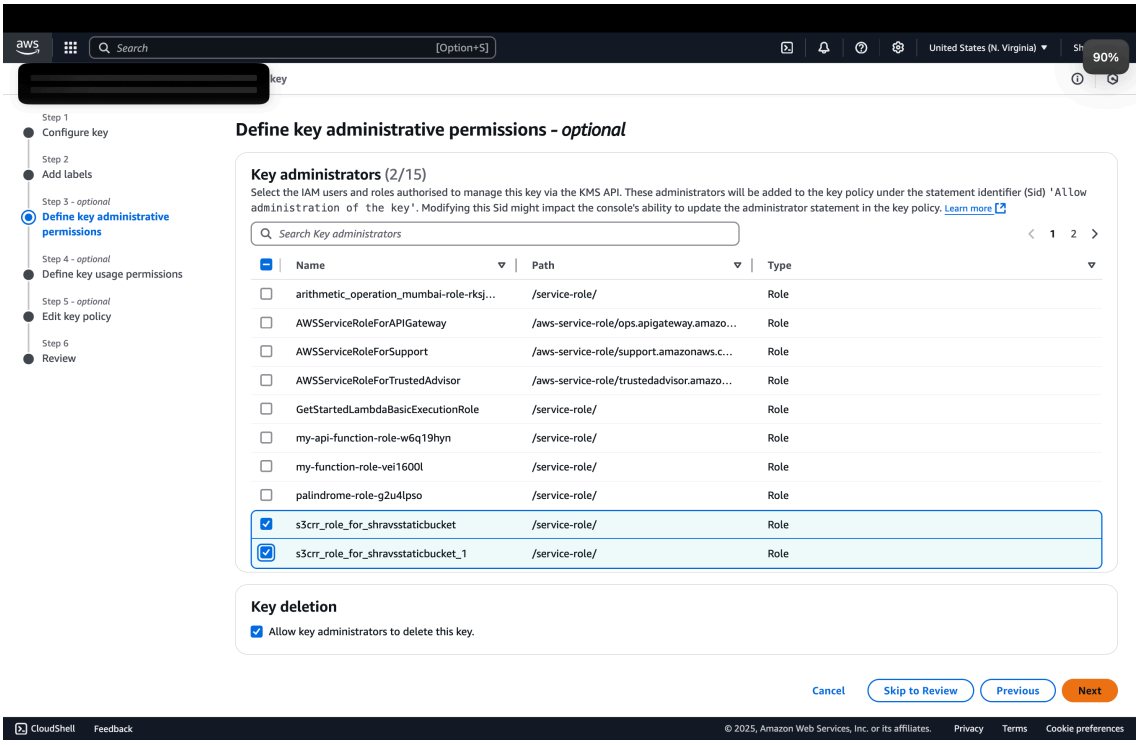
b. Key type - Symmetric; Key usage - encrypt and decrypt



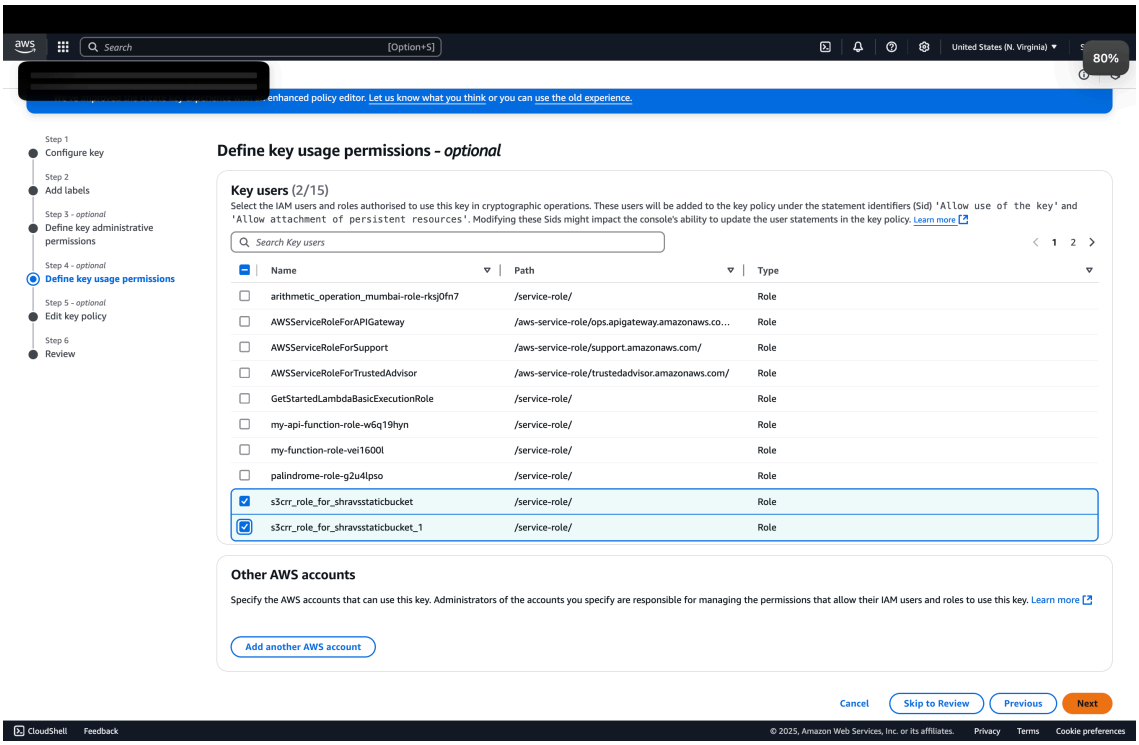
c. Add a name for the key



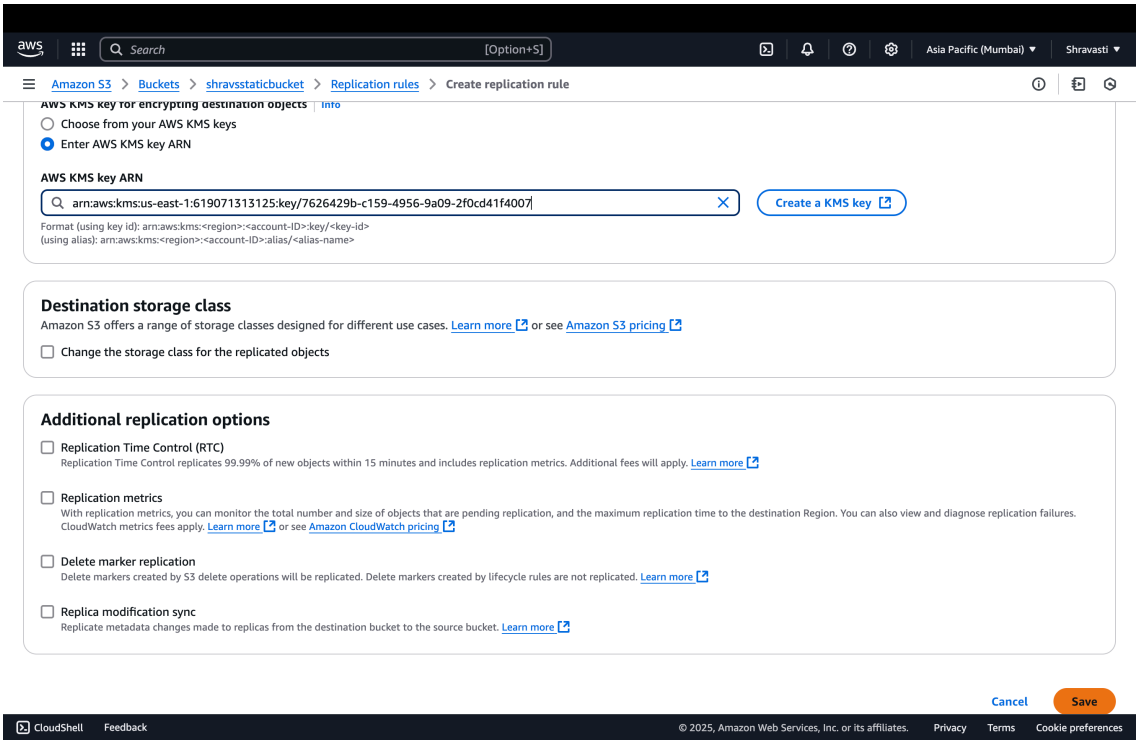
d. Add bucket IAM roles as key administrators



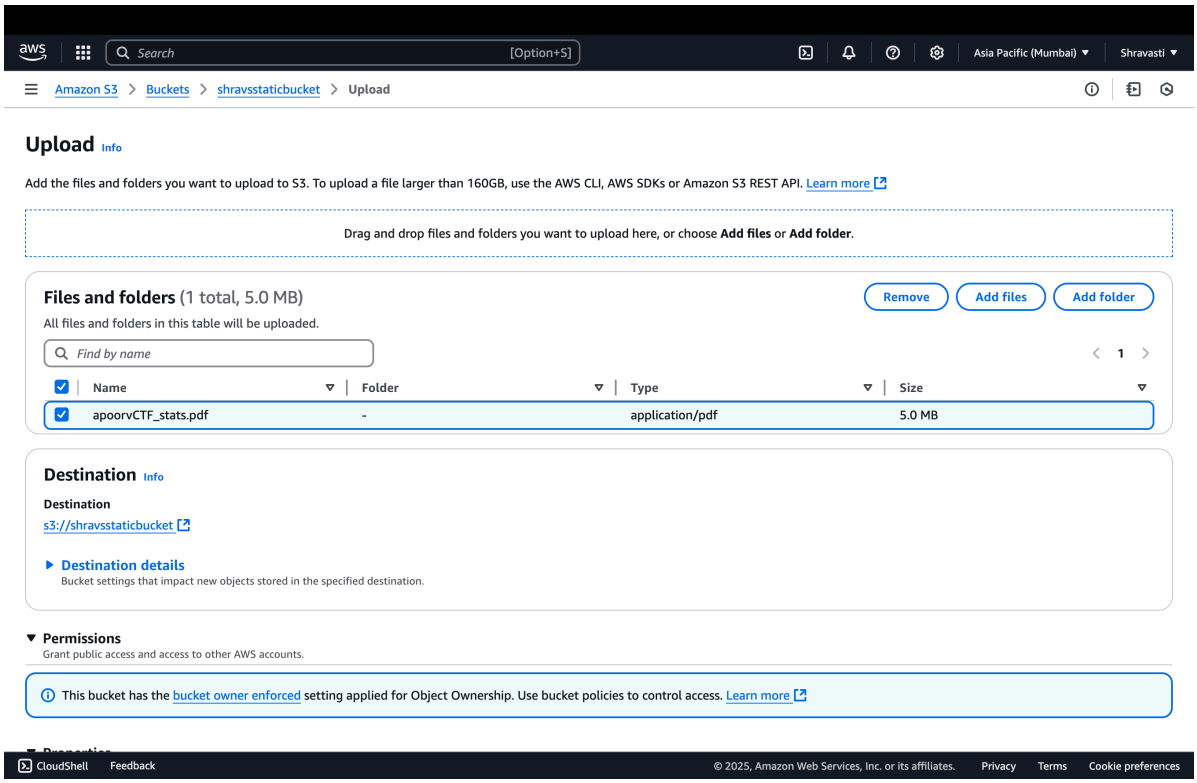
e. Add bucket IAM users as key users

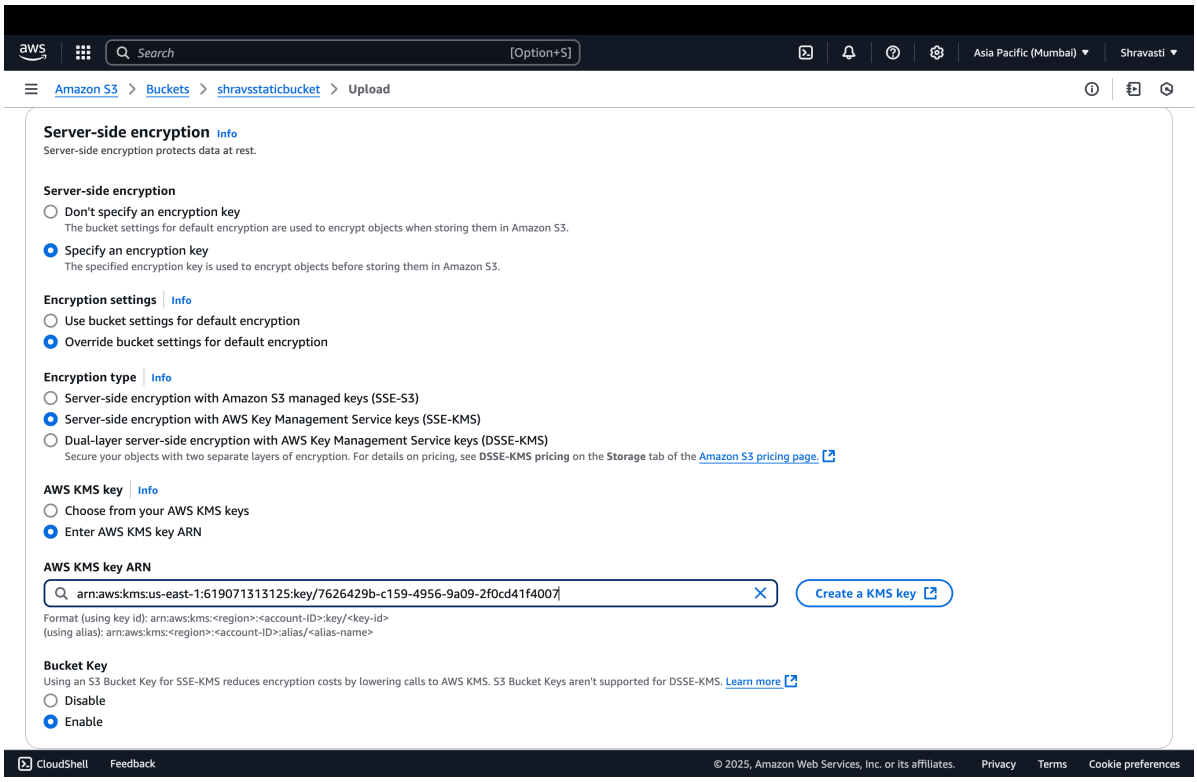


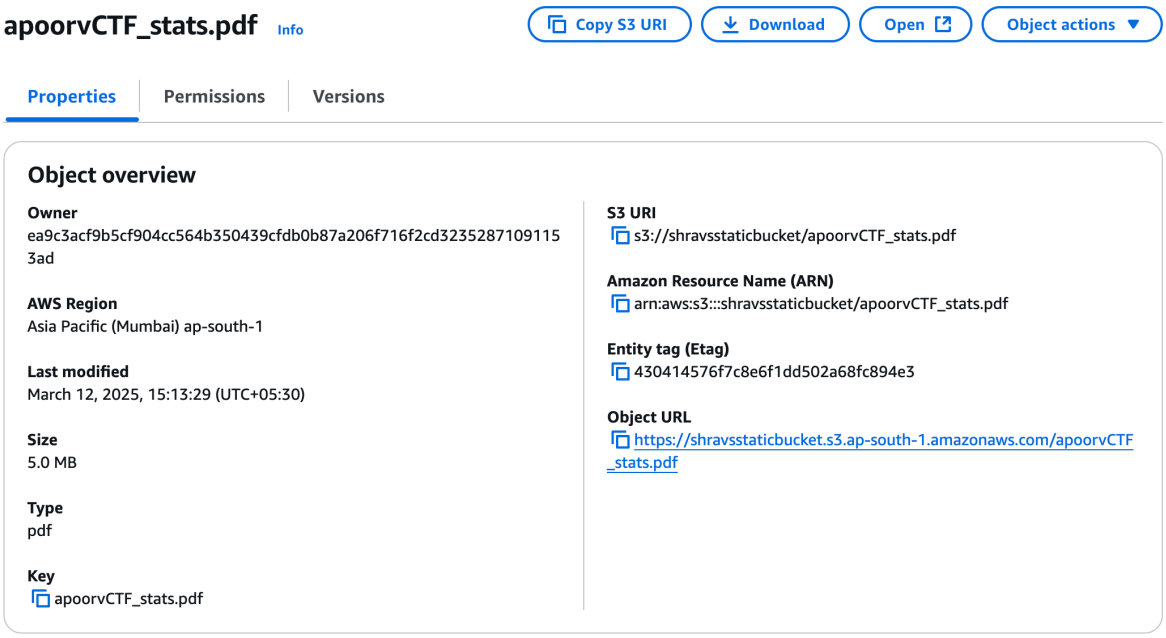
f. Copy paste key ARN



13. Upload a new file to the source bucket i.e. bucket in Mumbai region


Search [Option+S]
Asia Pacific (Mumbai)
Shravasti
Amazon S3 > Buckets > shravsstaticbucket > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 total, 5.0 MB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
1
Name
Folder
Type
Size
apoorvCTF_stats.pdf
-
application/pdf
5.0 MB
Destination Info
Destination
s3://shravsstaticbucket
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
This bucket has the bucket owner enforced setting applied for Object Ownership. Use bucket policies to control access. Learn more
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

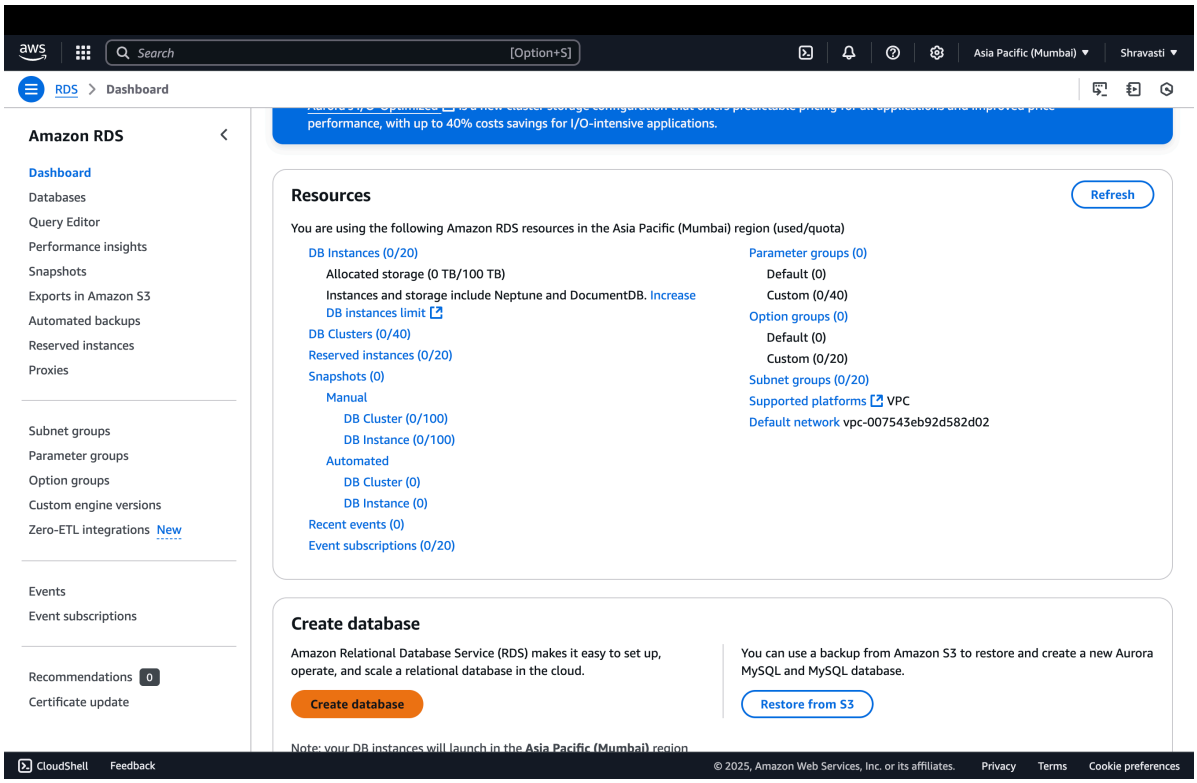

Search [Option+S]
Asia Pacific (Mumbai)
Shravasti
Amazon S3 > Buckets > shravsstaticbucket > Upload
Server-side encryption Info
Server-side encryption protects data at rest.
Server-side encryption
Don't specify an encryption key
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.
Specify an encryption key
The specified encryption key is used to encrypt objects before storing them in Amazon S3.
Encryption settings Info
Use bucket settings for default encryption
Override bucket settings for default encryption
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:us-east-1:619071313125:key/7626429b-c159-4956-9a09-2f0cd41f4007
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>
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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



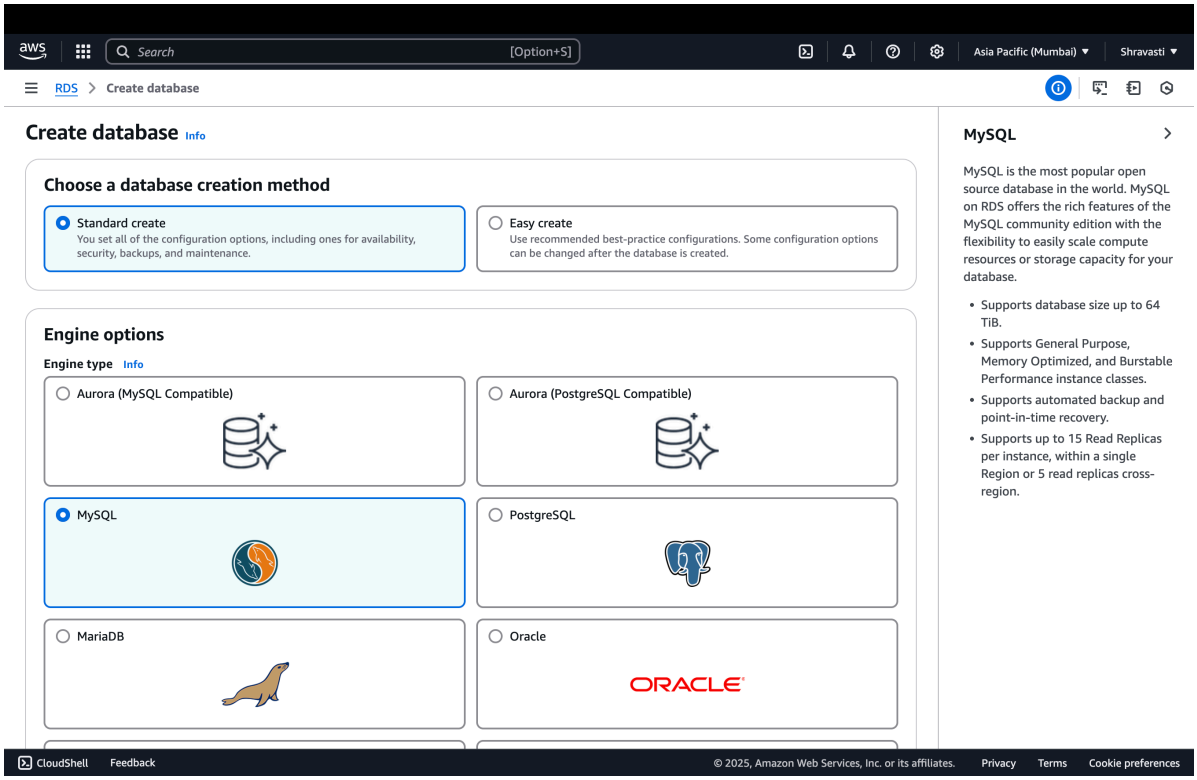
RDS Database

1. Create an RDS database

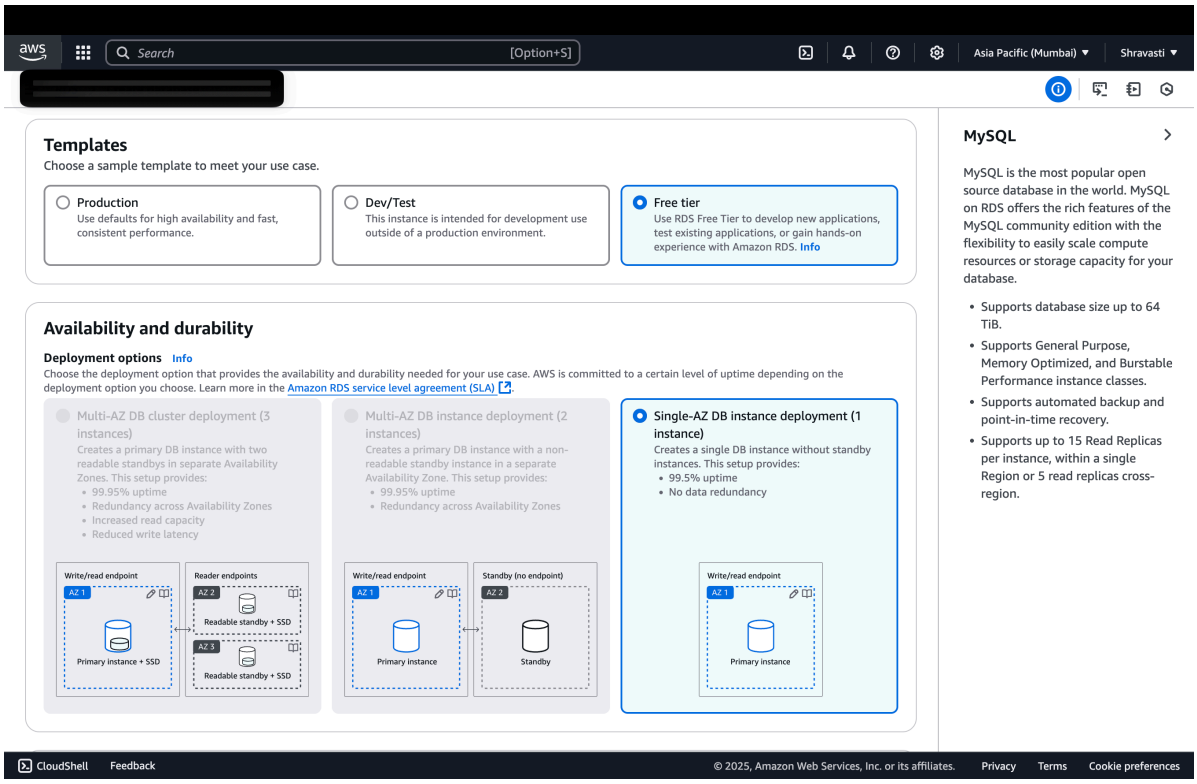
   click on create database



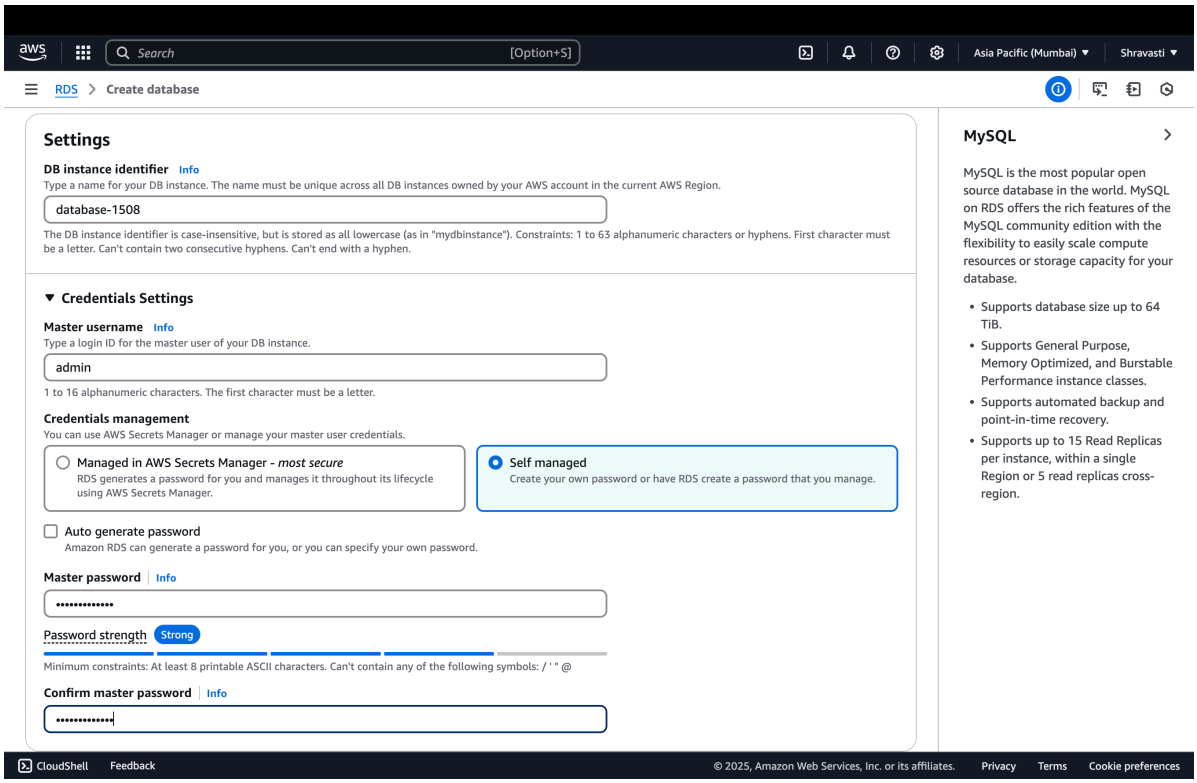
choose standard creation → MySQL as engine



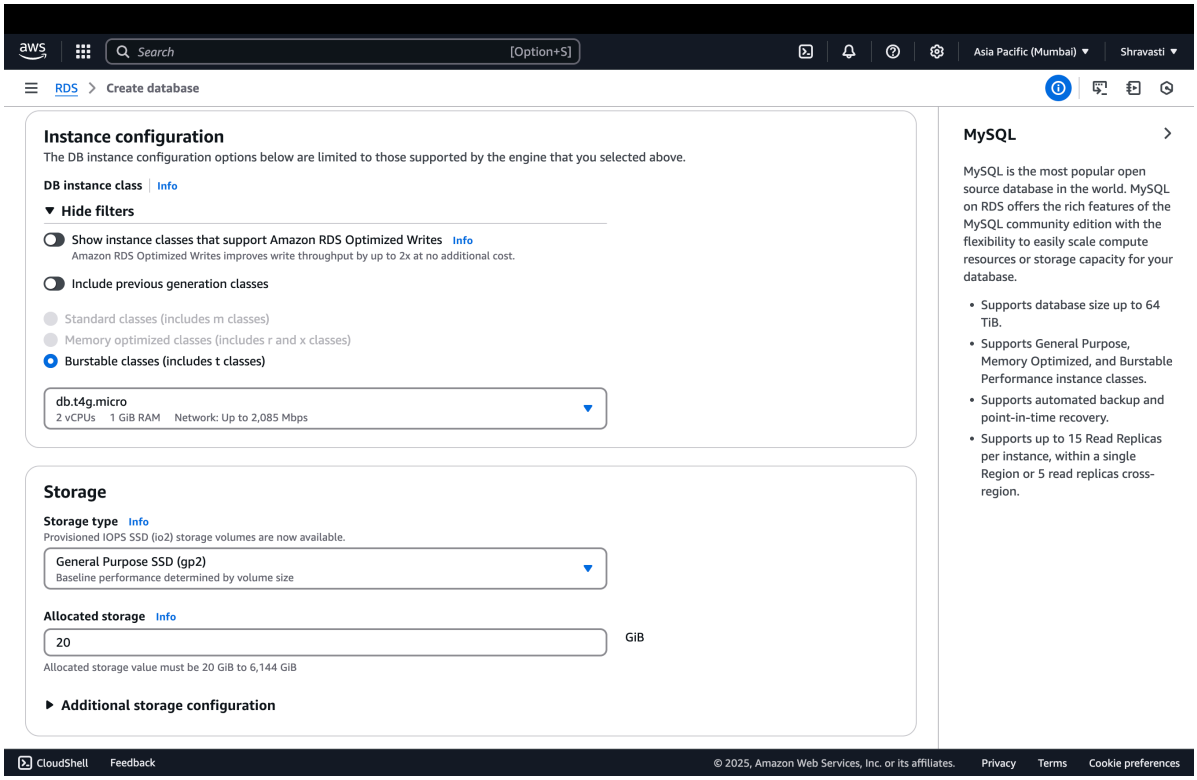
choose free tier template

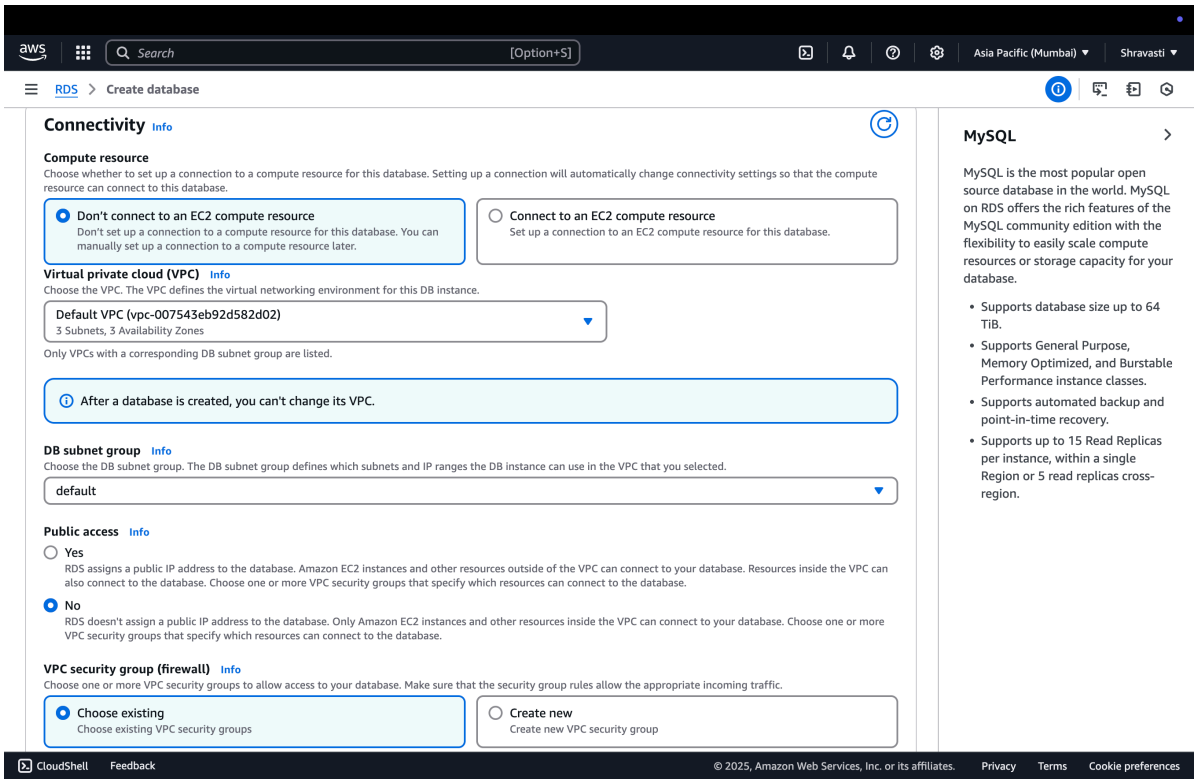


add a name for the database instance → use self-managed credentials → add master password

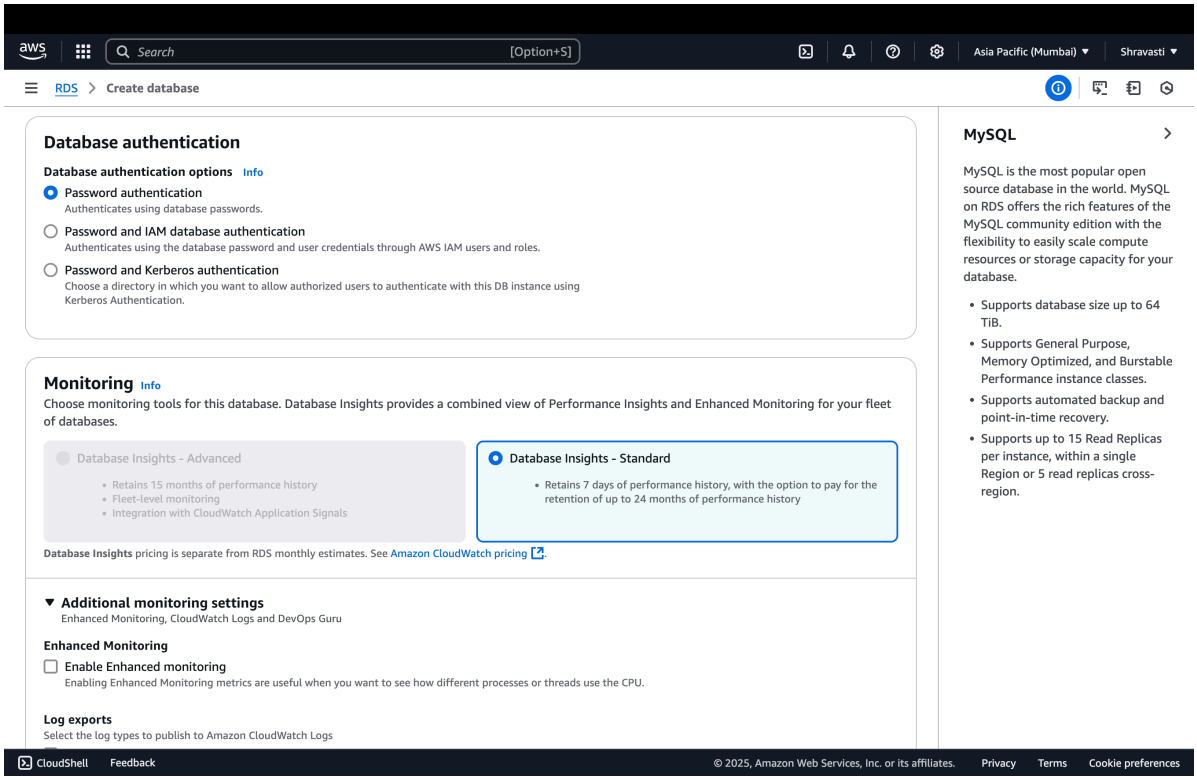


let the other configurations be default

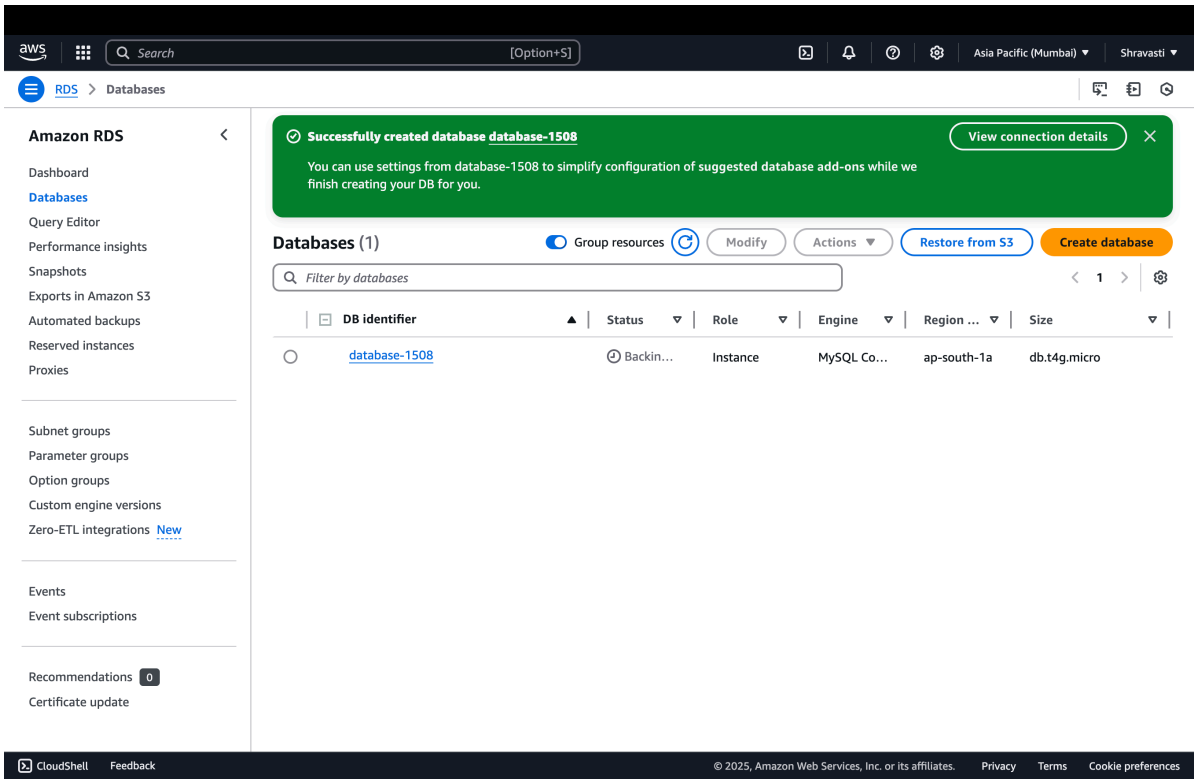




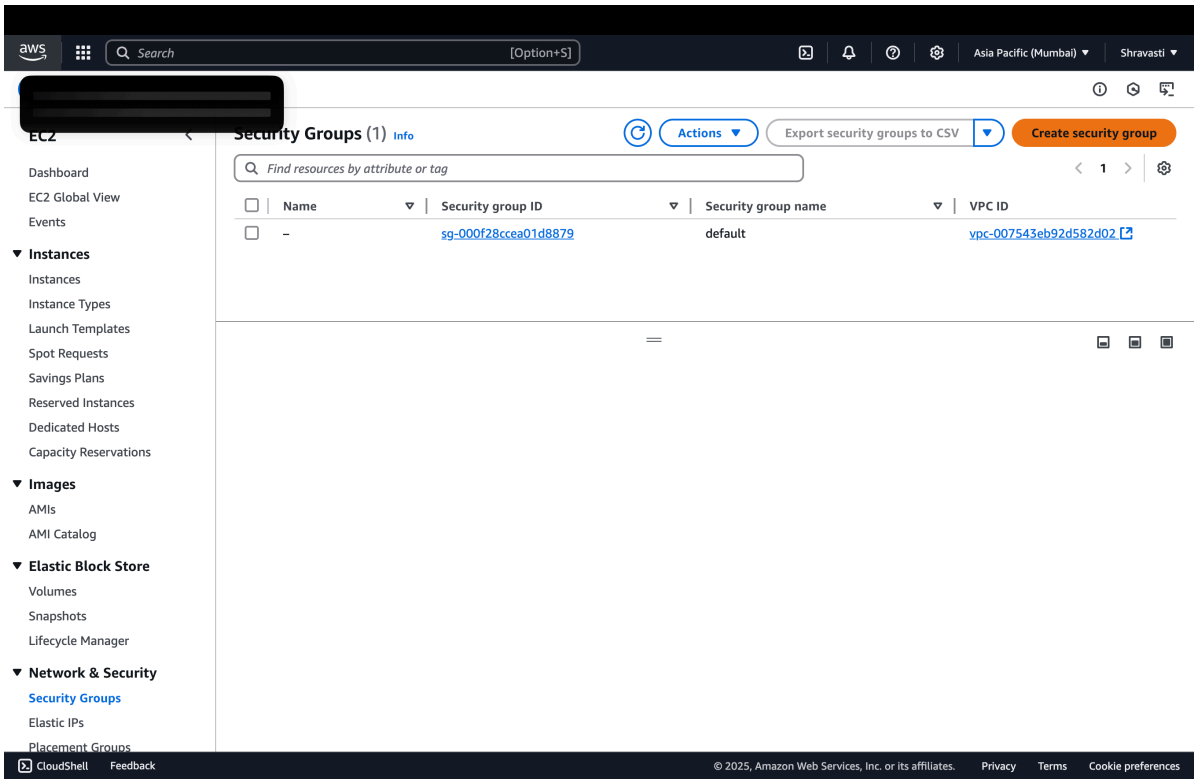
database authentication method → password authentication



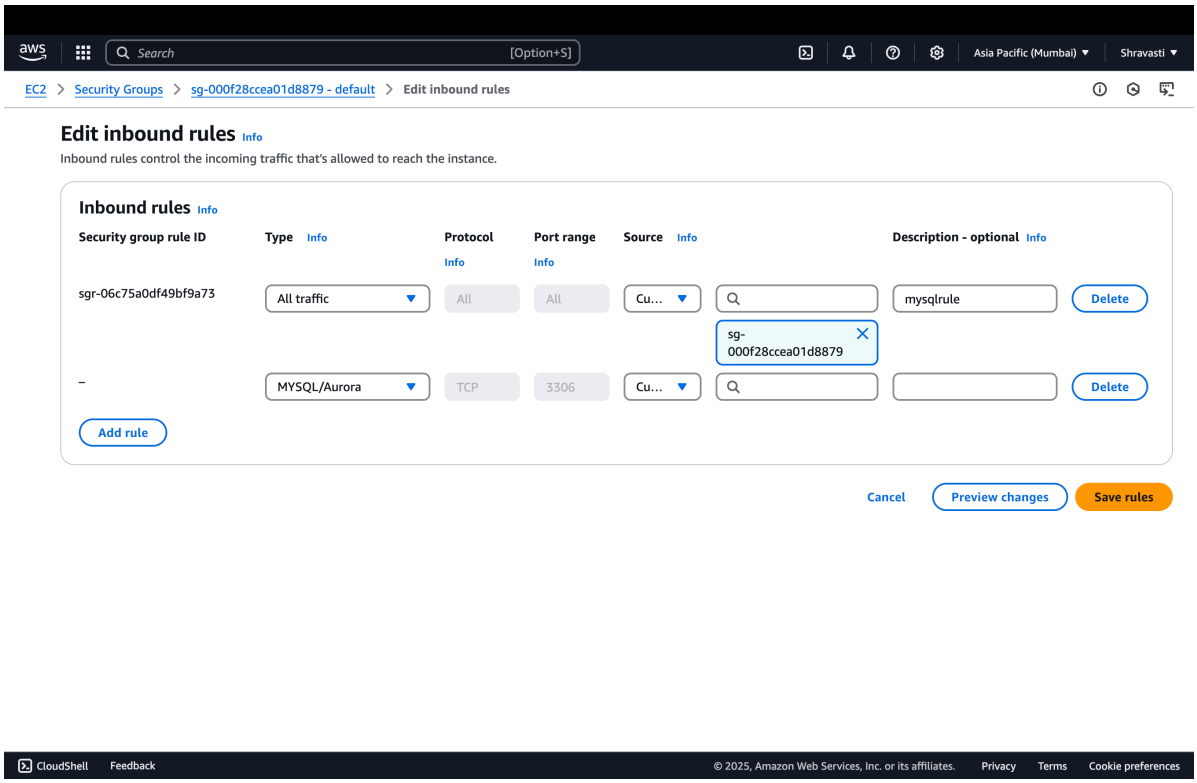
database will be created successfully



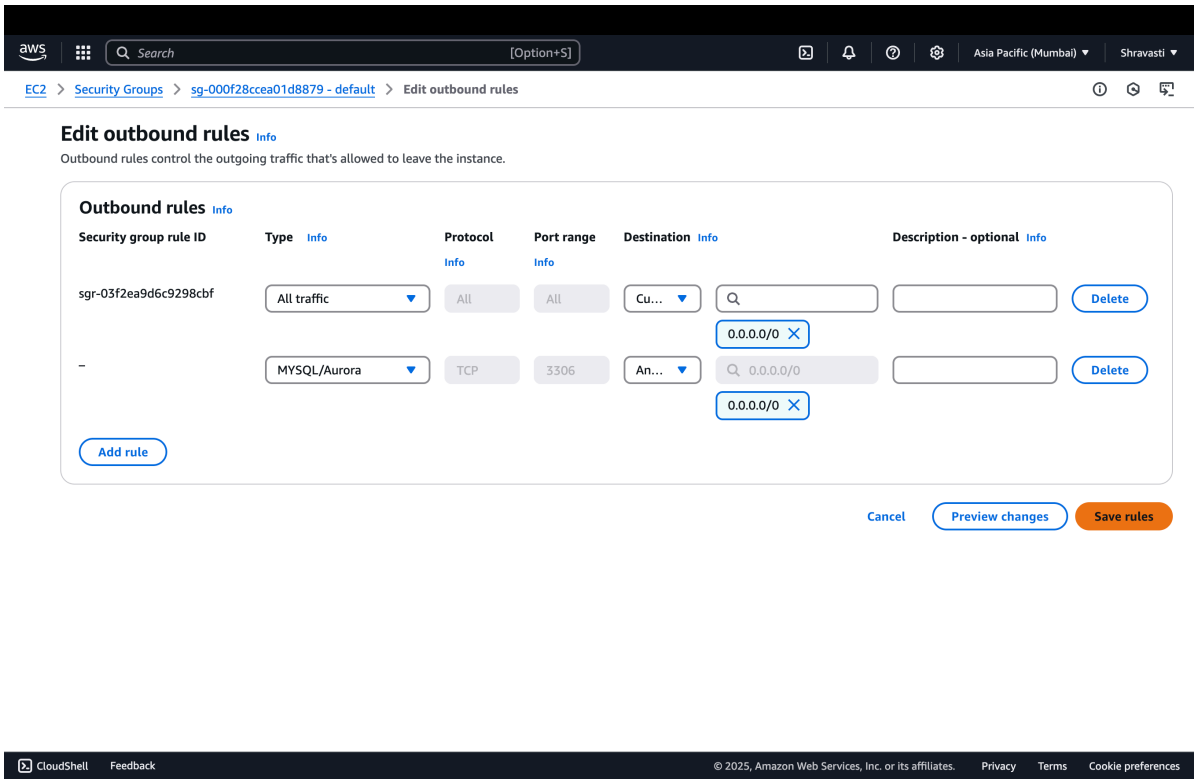
2. Navigate to the search bar and search for security group



3. inbound rules



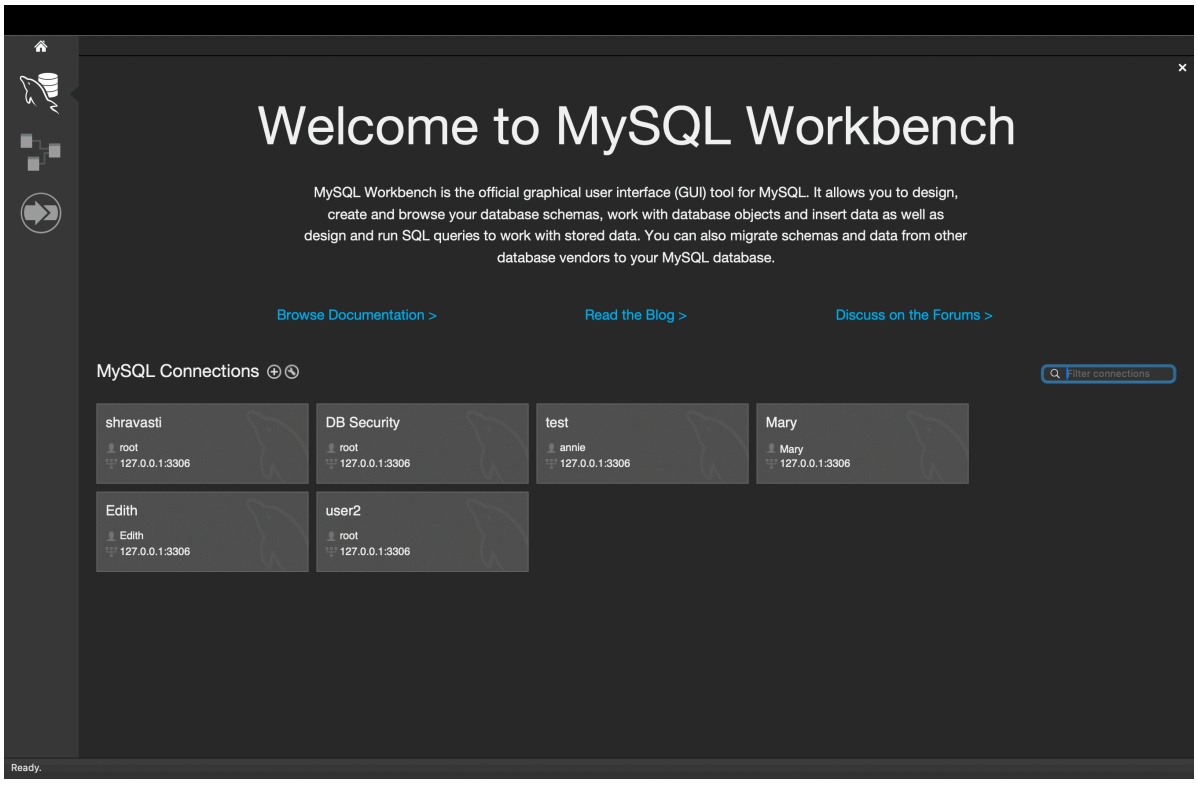
4. outbound rule



5. Navigate to the connectivity and security tab in RDS service → copy the endpoint link given there

   database-1508.cpwi88a8e8aa.ap-south-1.rds.amazonaws.com

6. Open MySQL Workbench


Welcome to MySQL Workbench
MySQL Workbench is the official graphical user interface (GUI) tool for MySQL. It allows you to design, create and browse your database schemas, work with database objects and insert data as well as design and run SQL queries to work with stored data. You can also migrate schemas and data from other database vendors to your MySQL database.
Browse Documentation >
Read the Blog >
Discuss on the Forums >
MySQL Connections
Filter connections
shravasti
root
127.0.0.1:3306
DB Security
root
127.0.0.1:3306
test
annie
127.0.0.1:3306
Mary
Mary
127.0.0.1:3306
Edith
Edith
127.0.0.1:3306
user2
root
127.0.0.1:3306
Ready.