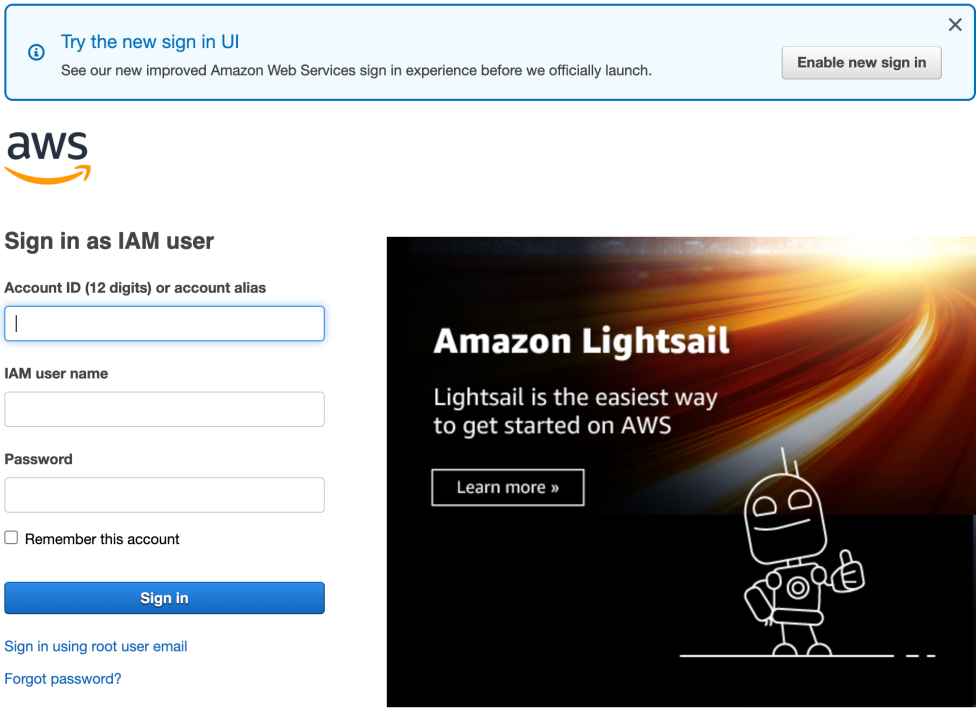
Practical 2: Storage as a Service Using AWS

Name : Khushi
Roll No. : A073

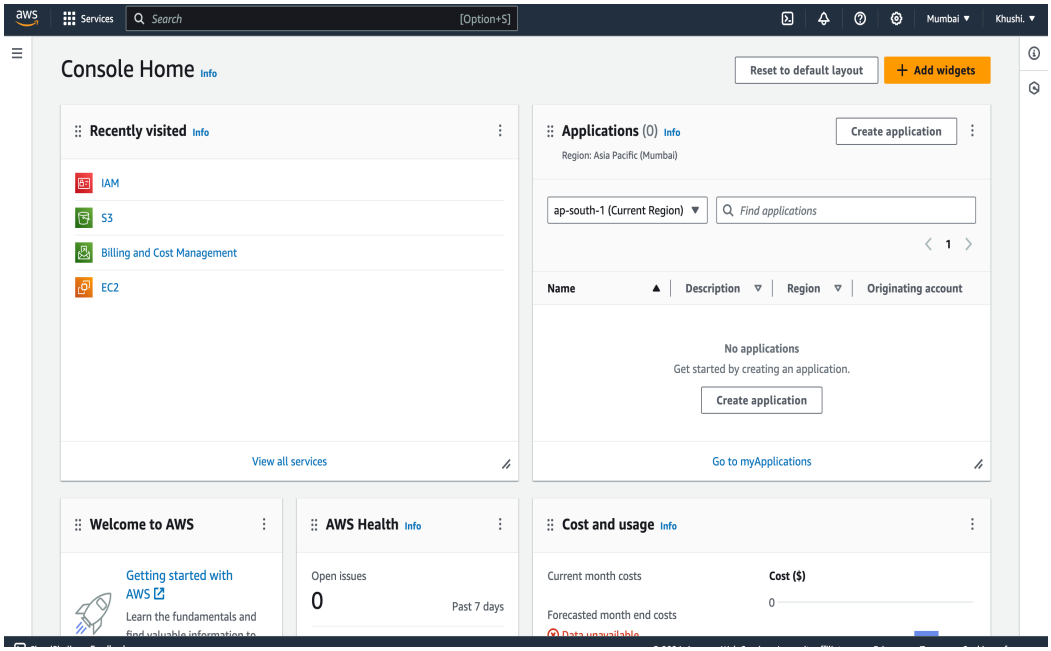
1. **Log in to AWS Management Console:**

   - Go to AWS Management Console.
   - Sign in with your credentials.

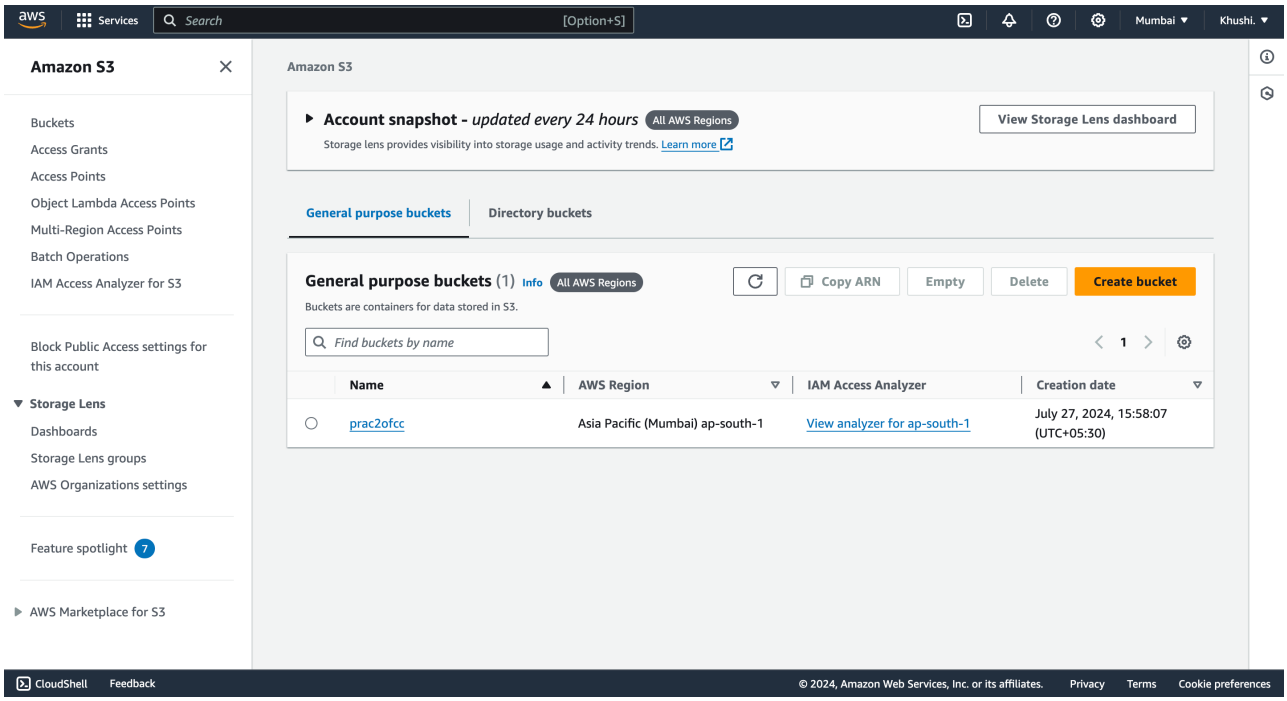


2. **Navigate to S3:**

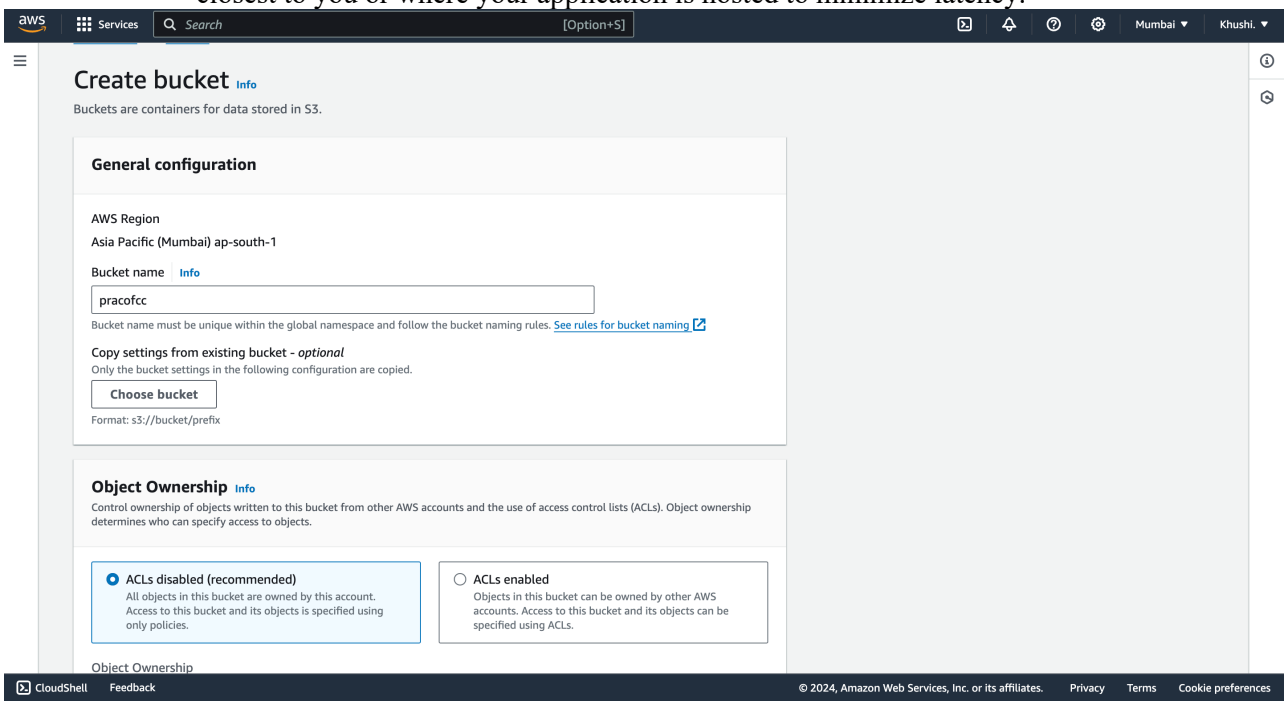
   - In the AWS Management Console, search for "S3."
   - Click on "S3" to open the Amazon S3 dashboard.



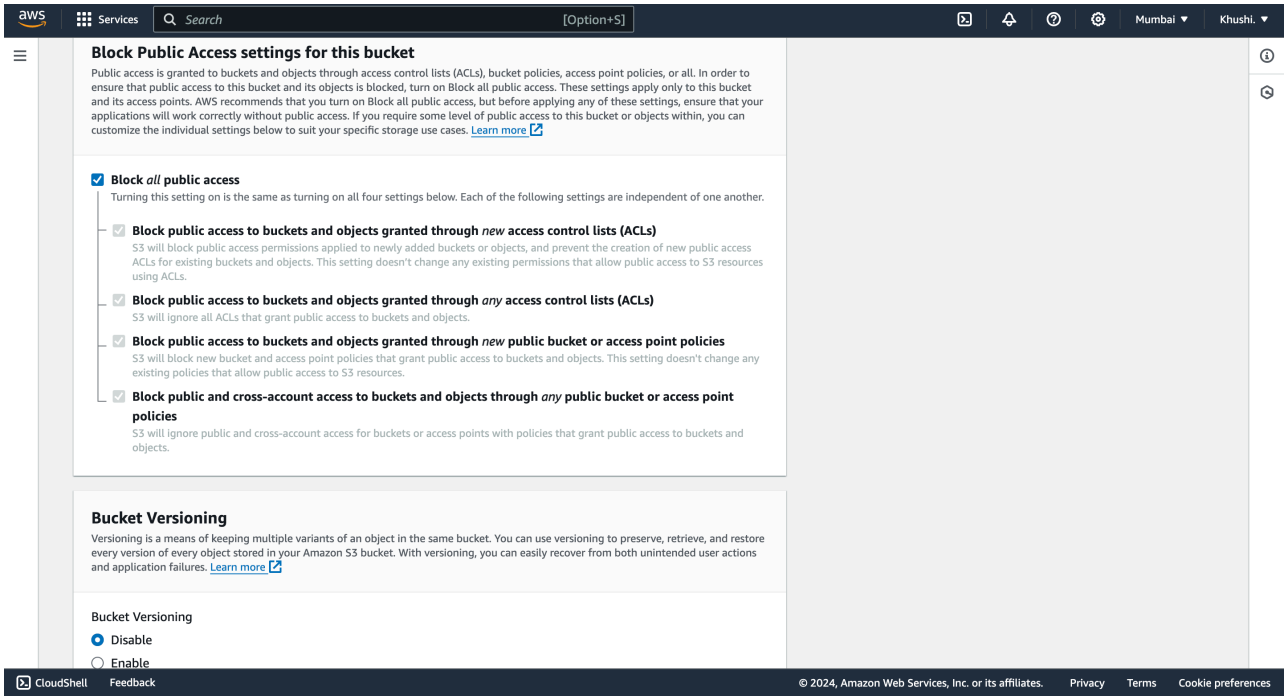
3. **Create a Bucket:**
   - Click on the “Create bucket” button.

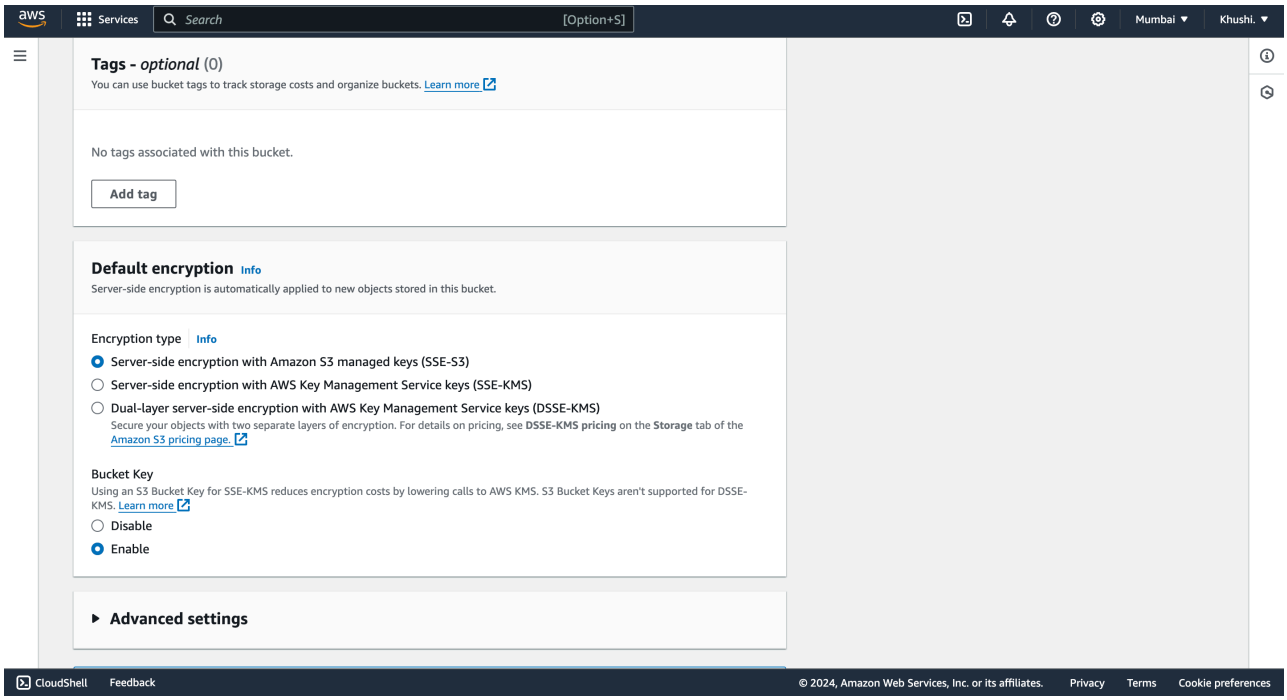


4. **Configure Bucket Settings:**
   - **Bucket Name:** Enter a unique name for your bucket (bucket names must be globally unique across all AWS users).
   - **Region:** Choose the AWS region where you want to create the bucket. Select the region closest to you or where your application is hosted to minimize latency.

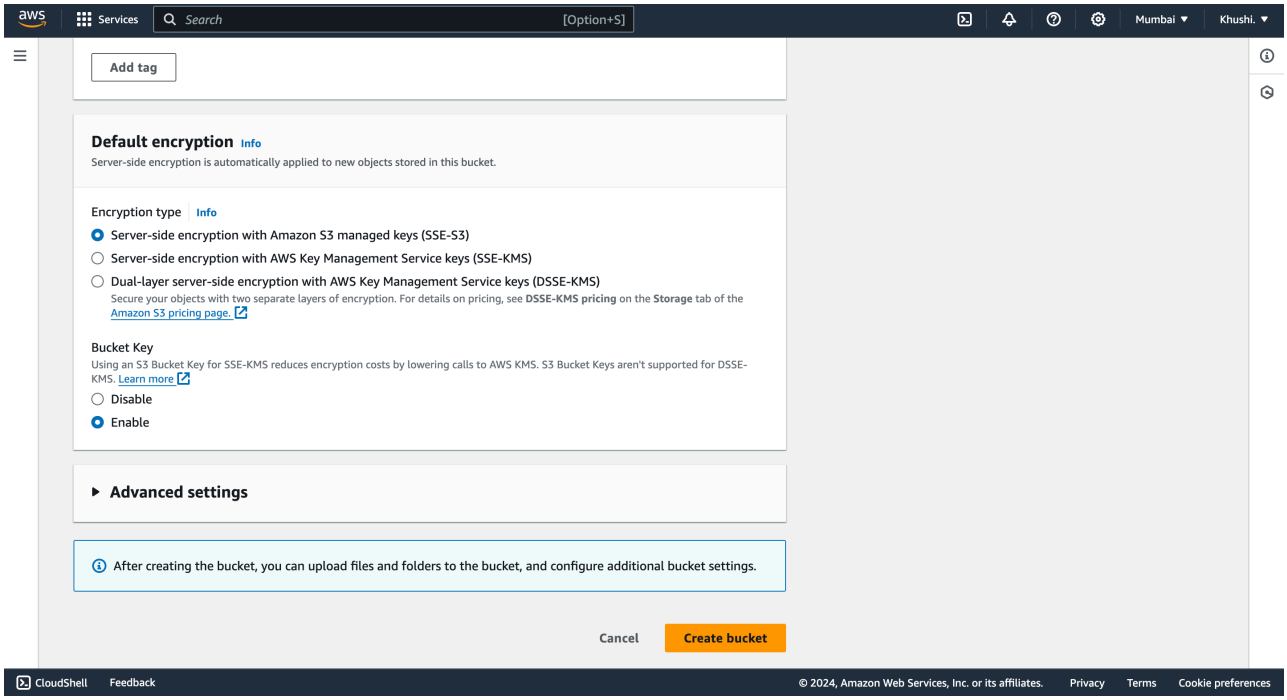


5. **Configure Bucket Options:**
   - **Block Public Access:** By default, block all public access to keep your data private. You can modify this later if needed.
   - **Versioning:** Enable versioning if you want to keep multiple versions of objects in the bucket.
   - **Tags:** Add any tags to categorize and manage your bucket.
   - **Object Lock:** Enable if you need to prevent objects from being deleted or overwritten (often used for regulatory compliance).

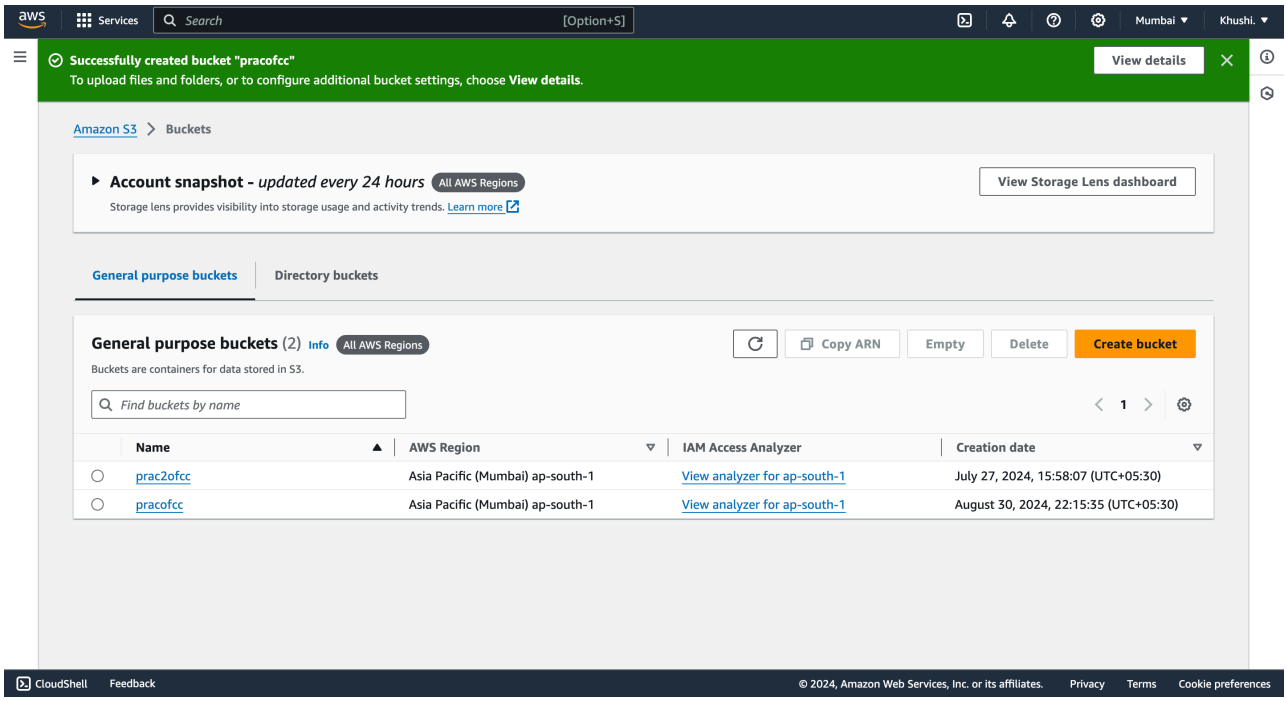




6. **Review and Create:**
   - Review your settings to ensure everything is configured as needed.
   - Click on the “Create bucket” button to finalize the creation.



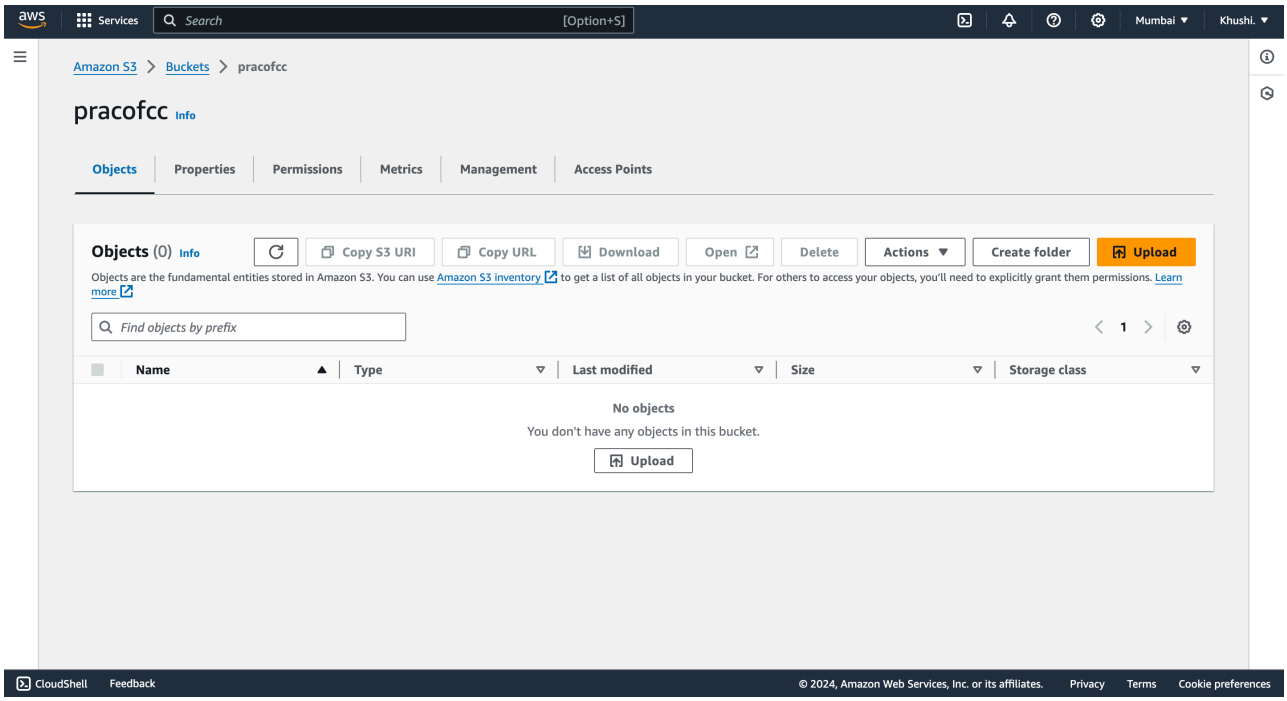
7. **Bucket Created:**
    - Your S3 bucket is now created and ready to use. You'll be redirected to the bucket's overview page.



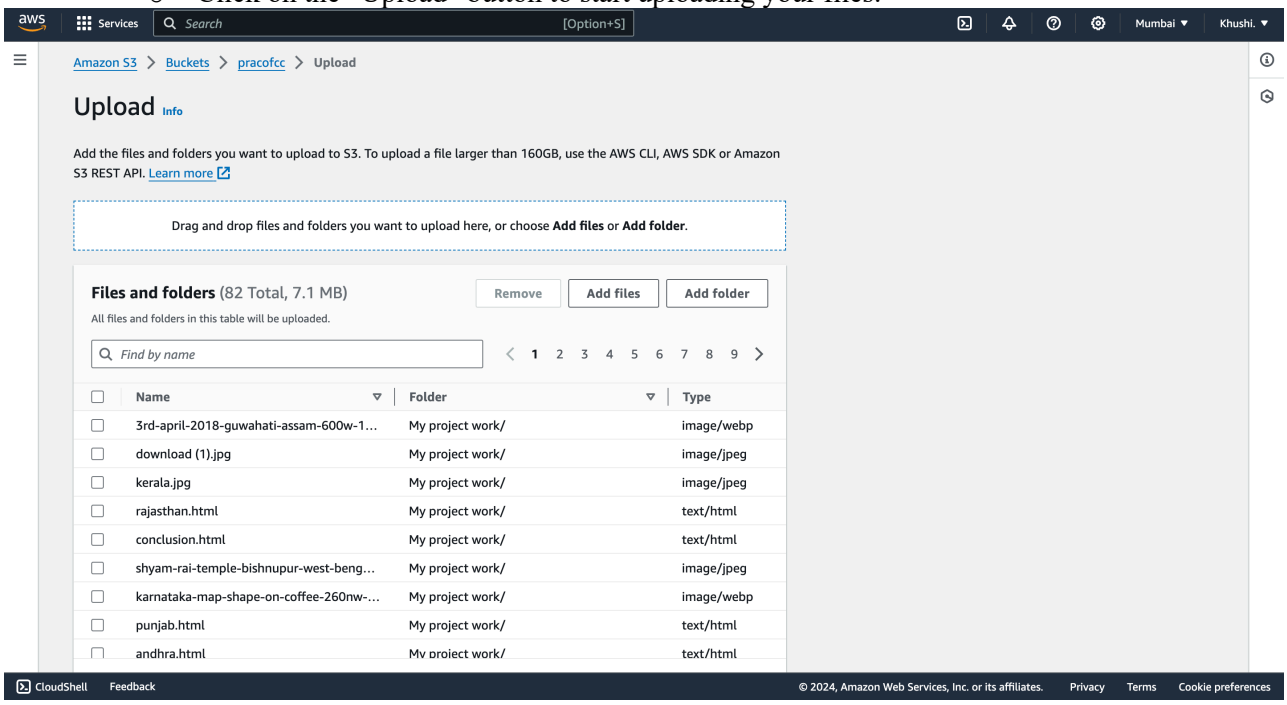
Uploading Files to Your S3 Bucket

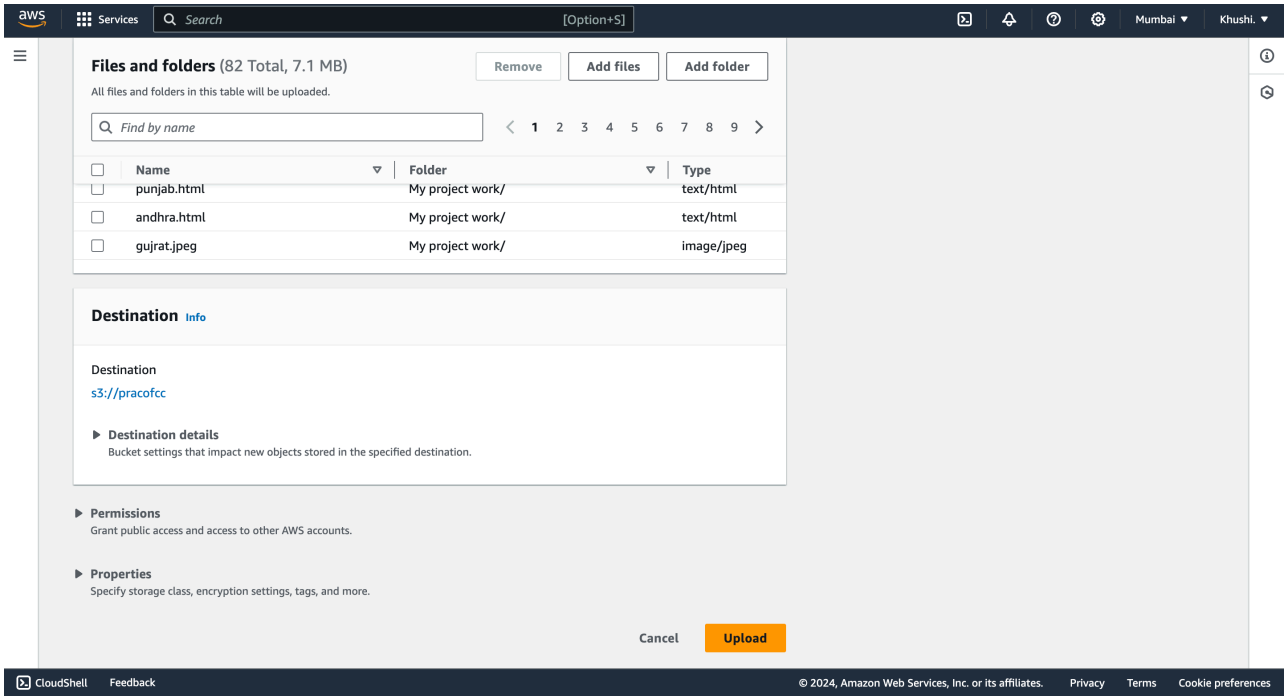
1. **Open Your Bucket:**
    - Click on your newly created bucket in the S3 dashboard.

2. **Upload Files:**
    - Click on the "Upload" button.
    - Drag and drop files into the console or click "Add files" to browse your computer.
    - Optionally, click "Add folder" to upload entire folders.

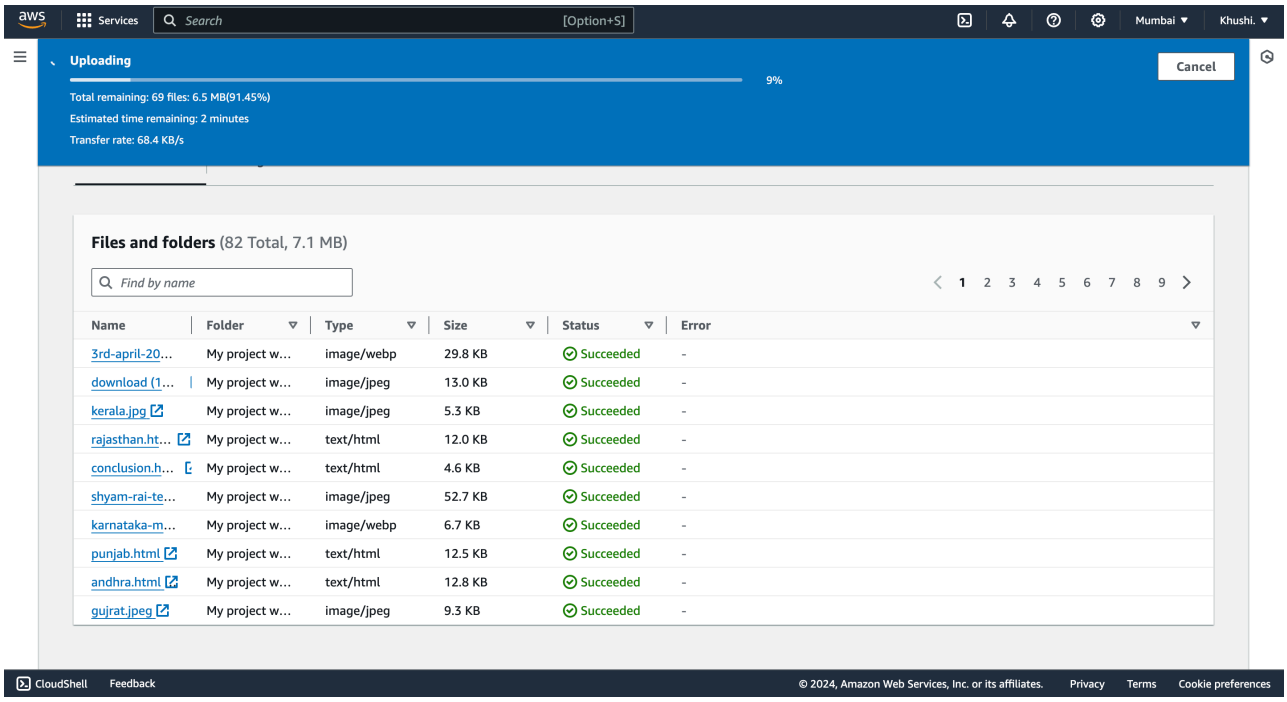


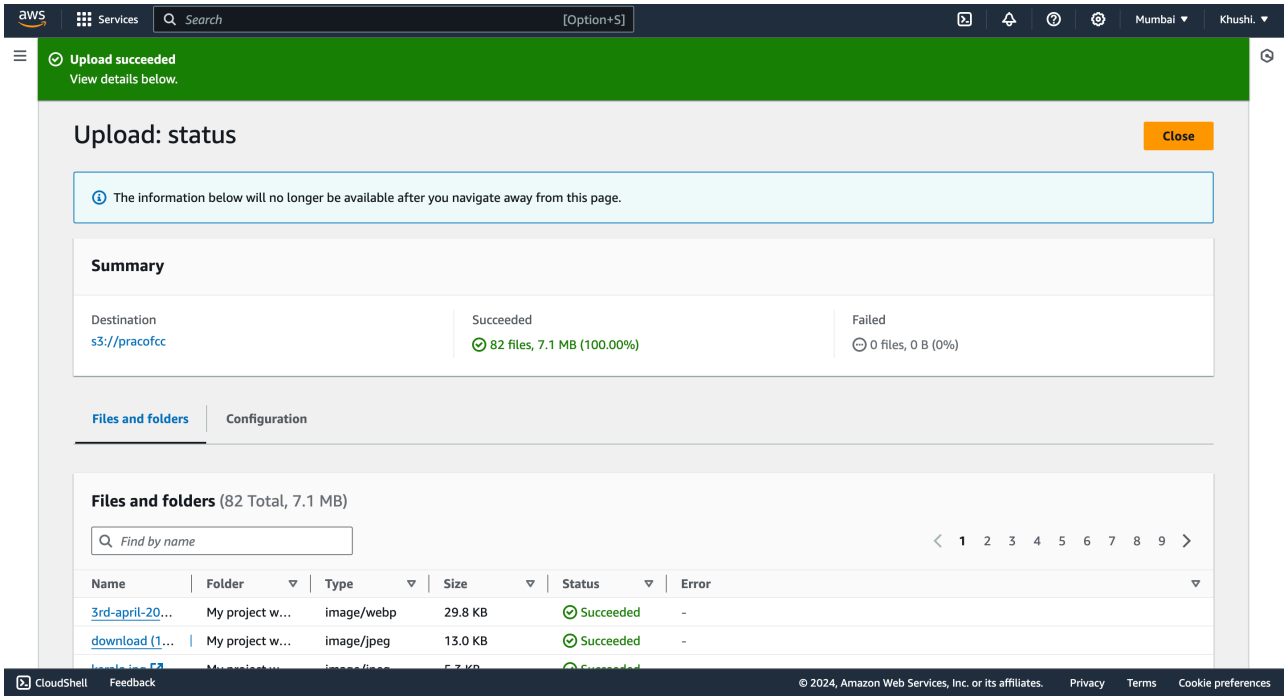
3. **Set Permissions (Optional):**
    - By default, files are private. You can modify permissions during the upload process if you want to make them public or restrict access.
4. **Upload:**
    - Click on the “Upload” button to start uploading your files.

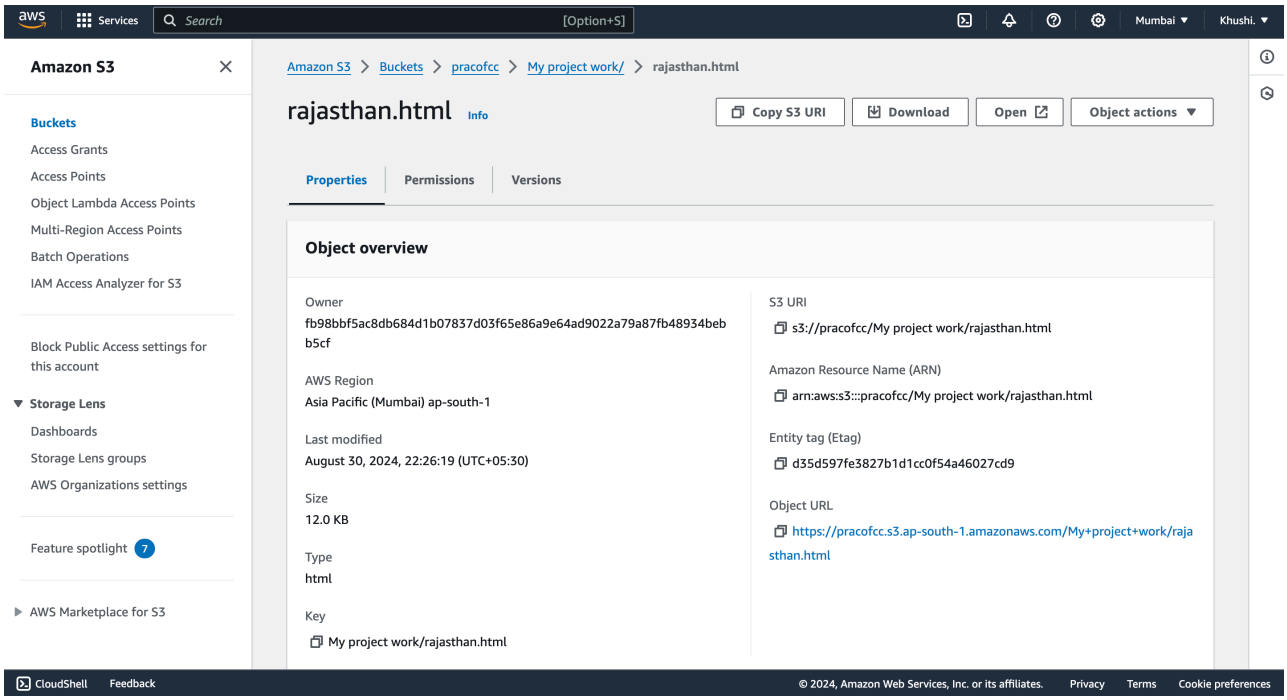


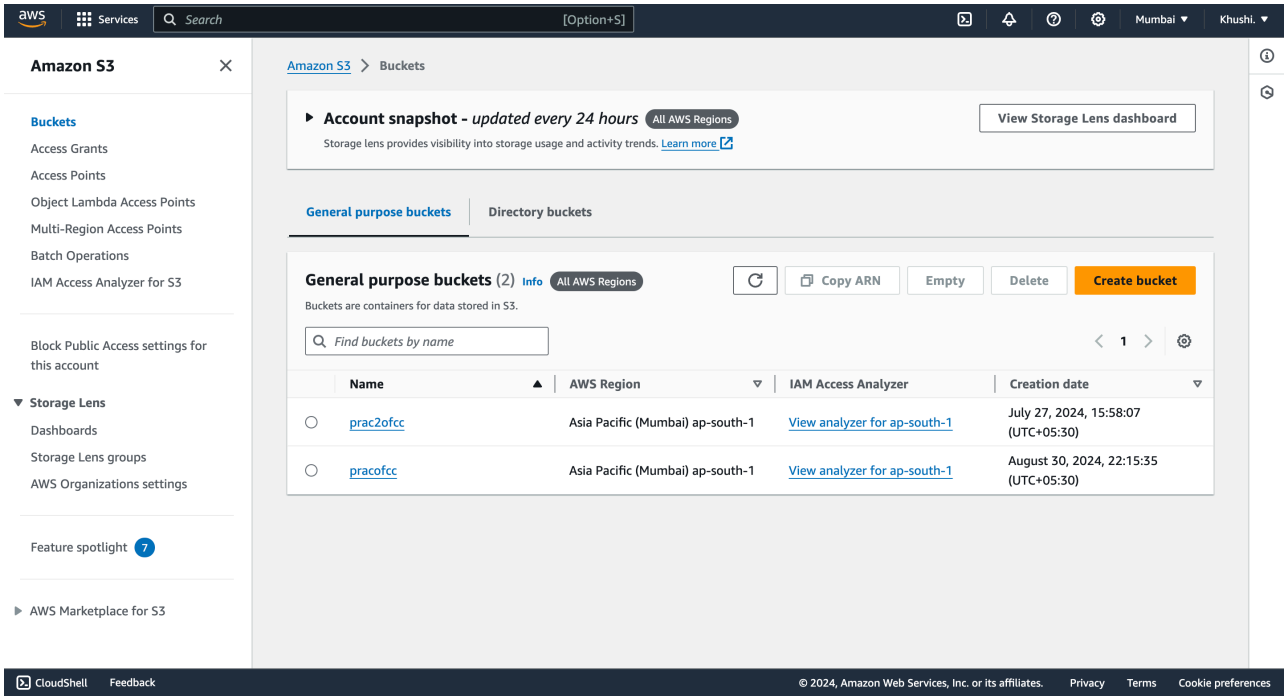


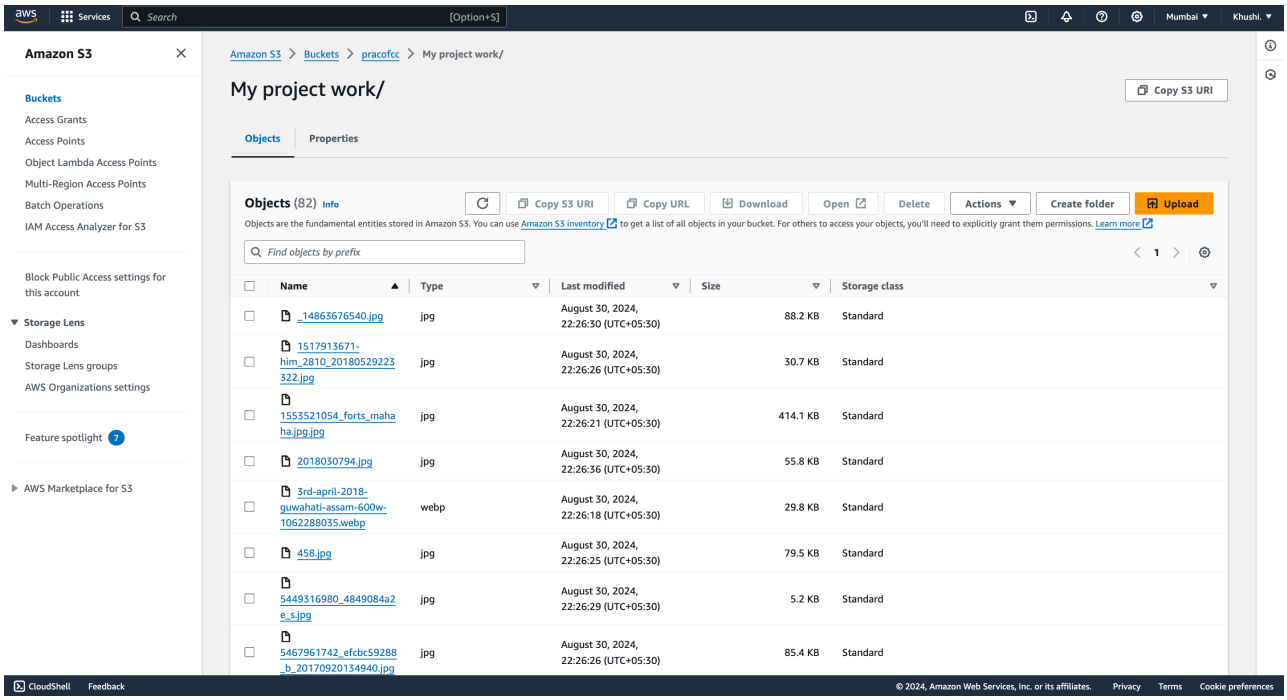
5. Wait for some time to upload the files.

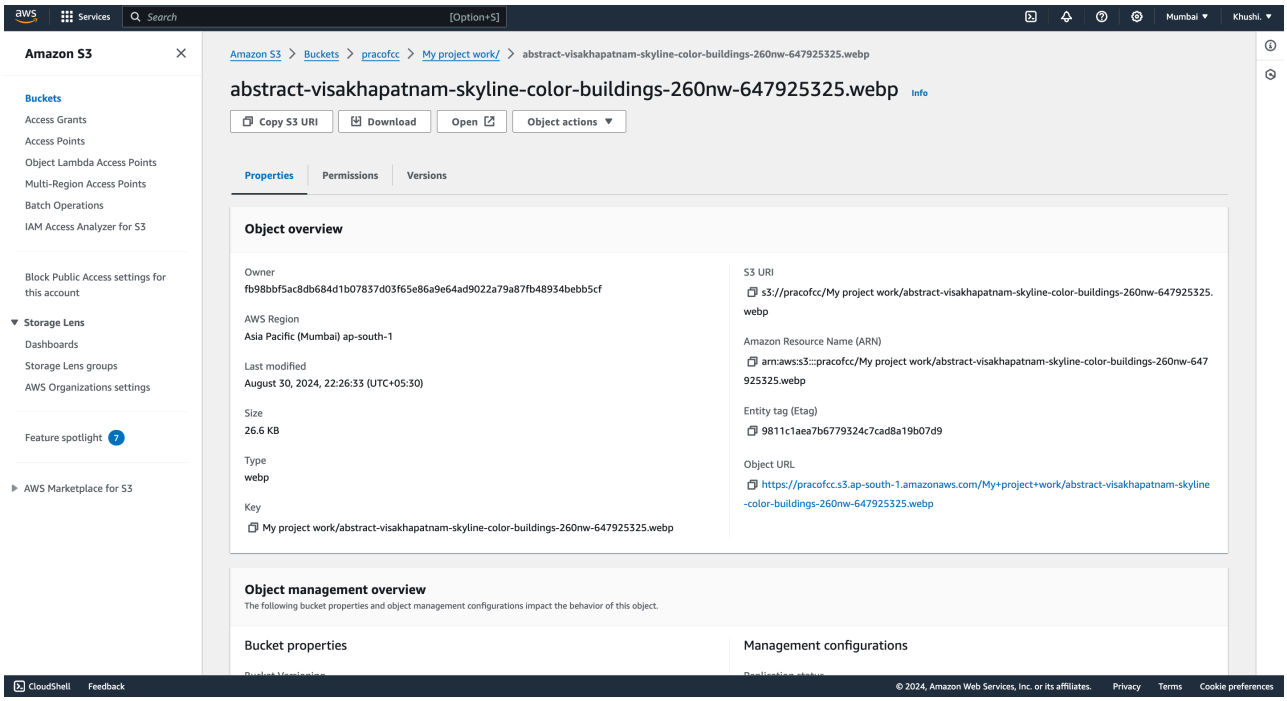



Services
Search
[Option+S]
Mumbai
Khushi.
Upload succeeded
View details below.
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://pracofcc
Succeeded
82 files, 7.1 MB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (82 Total, 7.1 MB)
Find by name
1 2 3 4 5 6 7 8 9
Name
Folder
Type
Size
Status
Error
3rd-april-20...
My project w...
image/webp
29.8 KB
Succeeded
-
download (1...
My project w...
image/jpeg
13.0 KB
Succeeded
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Option+S]
Mumbai
Khushi.
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
AWS Marketplace for S3
Amazon S3 > Buckets > pracofcc > My project work/ > rajasthan.html
rajasthan.html
Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
fb98bbf5ac8db684d1b07837d03f65e86a9e64ad9022a79a87fb48934bebb5cf
AWS Region
Asia Pacific (Mumbai) ap-south-1
Last modified
August 30, 2024, 22:26:19 (UTC+05:30)
Size
12.0 KB
Type
html
Key
My project work/rajasthan.html
S3 URI
s3://pracofcc/My project work/rajasthan.html
Amazon Resource Name (ARN)
arn:aws:s3:::pracofcc/My project work/rajasthan.html
Entity tag (Etag)
d35d597fe3827b1d1cc0f54a46027cd9
Object URL
https://pracofcc.s3.ap-south-1.amazonaws.com/My+project+work/rajasthan.html
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

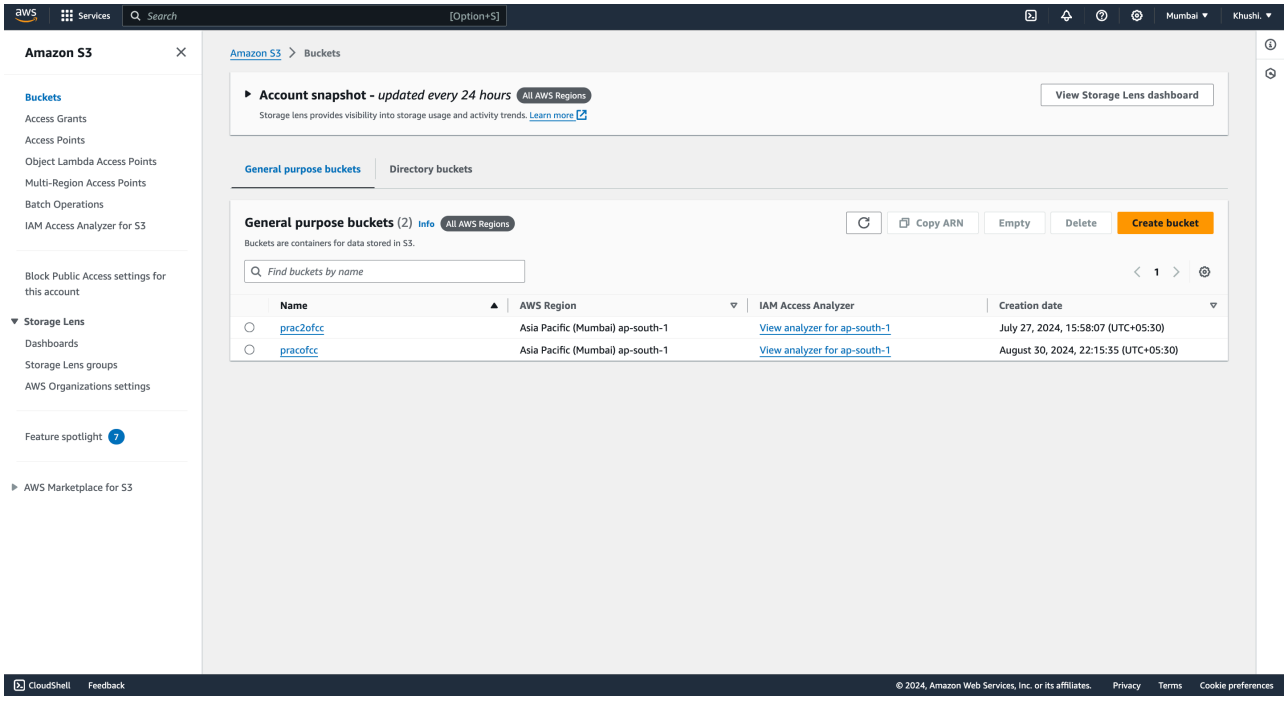

aws
Services
Search
[Option+S]
Mumbai
Khushi.
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (2) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1
Name
AWS Region
IAM Access Analyzer
Creation date
prac2ofcc
Asia Pacific (Mumbai) ap-south-1
View analyzer for ap-south-1
July 27, 2024, 15:58:07 (UTC+05:30)
pracofcc
Asia Pacific (Mumbai) ap-south-1
View analyzer for ap-south-1
August 30, 2024, 22:15:35 (UTC+05:30)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

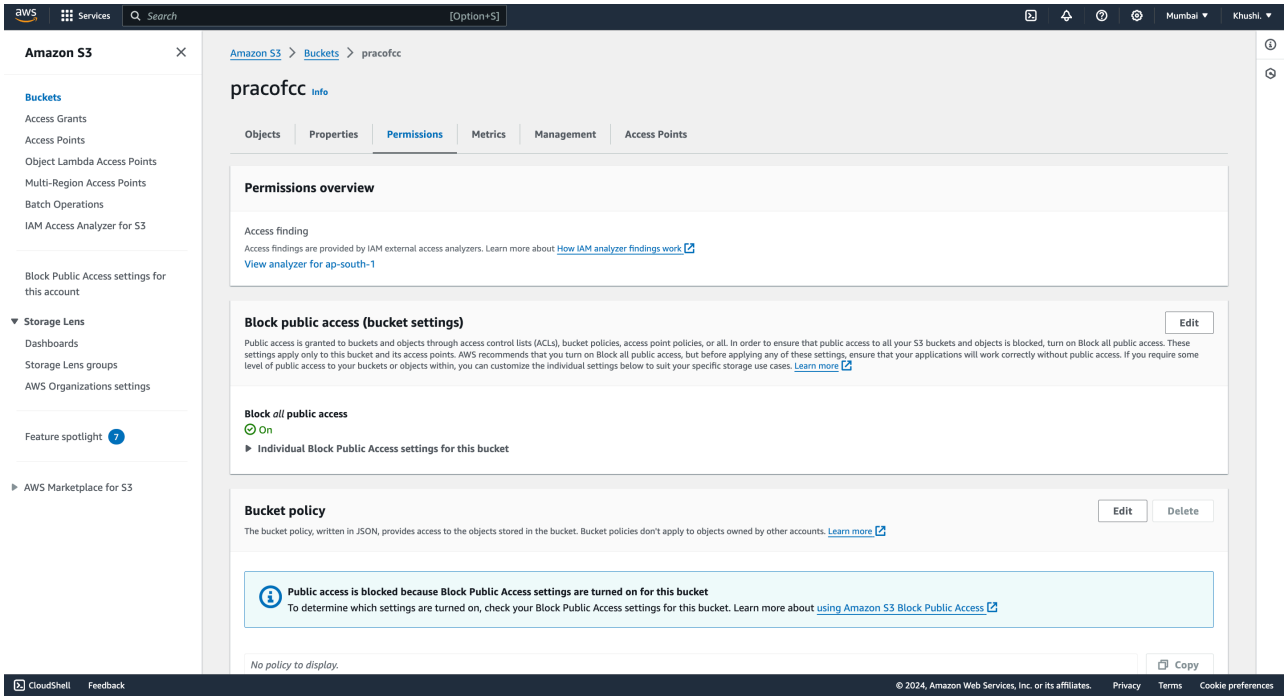

aws
Services
Search
[Option+S]
Mumbai
Khushi.
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
Amazon S3 > Buckets > pracofcc > My project work/
My project work/
Copy S3 URI
Objects
Properties
Objects (82) 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
1
Name
Type
Last modified
Size
Storage class
_14863676540.jpg
jpg
August 30, 2024, 22:26:30 (UTC+05:30)
88.2 KB
Standard
1517913671-him_2810_20180529223322.jpg
jpg
August 30, 2024, 22:26:26 (UTC+05:30)
30.7 KB
Standard
1553521054_forts_mahaha.jpg.jpg
jpg
August 30, 2024, 22:26:21 (UTC+05:30)
414.1 KB
Standard
2018030794.jpg
jpg
August 30, 2024, 22:26:36 (UTC+05:30)
55.8 KB
Standard
3rd-april-2018-guwahati-assam-600w-1062288035.webp
webp
August 30, 2024, 22:26:18 (UTC+05:30)
29.8 KB
Standard
458.jpg
jpg
August 30, 2024, 22:26:25 (UTC+05:30)
79.5 KB
Standard
5449316980_4849084a2e_s.jpg
jpg
August 30, 2024, 22:26:29 (UTC+05:30)
5.2 KB
Standard
5467961742_efcbc59288_b_20170920134940.jpg
jpg
August 30, 2024, 22:26:26 (UTC+05:30)
85.4 KB
Standard
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

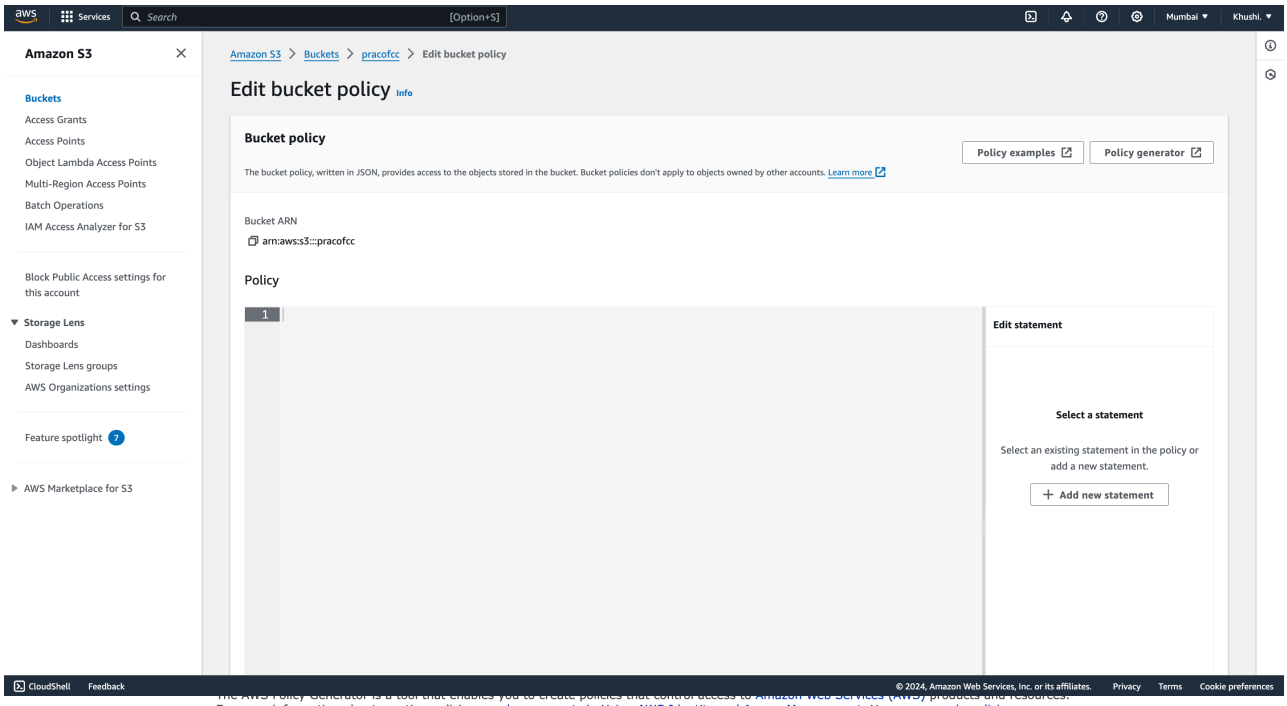


This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>117RC151K0S9BR4W</RequestId>
  <HostId>ORIVQt+9j/AjBW7gqbRGVBUNQSJ+sJjjF+FPUlisBiwxX8gBTKfodTuRPqPAQM9B0zLMXPFhssA=</HostId>
</Error>
```





The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources.
For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect Allow Deny

Principal *

Use a comma to separate multiple values.

AWS Service

Amazon S3

All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions 1 Action(s) Selected

All Actions ('*')

Amazon Resource Name (ARN)

GetMultiRegionAccessPointPolicy
GetMultiRegionAccessPointPolicyStatus
GetMultiRegionAccessPointRoutes
GetObject
GetObjectAcl
GetObjectAttributes
GetObjectLegalHold

:${BucketName}/${KeyName}.

alid. You must enter a valid ARN.

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect (•) Allow ( ) Deny

Principal [ ]

Use a comma to separate multiple values.

AWS Service

Amazon S3

[ ] All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- [ ] All Actions ('*')

Amazon Resource Name (ARN) [ ]

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3:::pracofcc	*None*

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

Generate Policy Start Over

AWS Service

Amazon S3

All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- All Actions ('*')

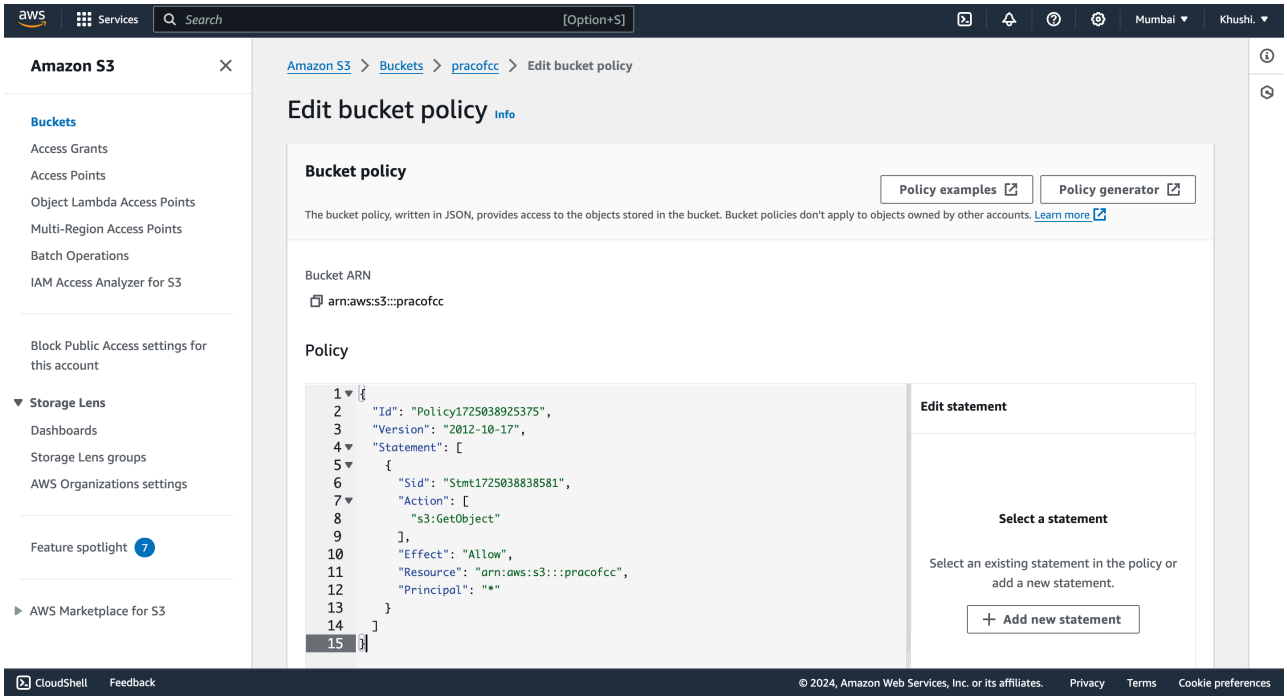
Policy JSON Document

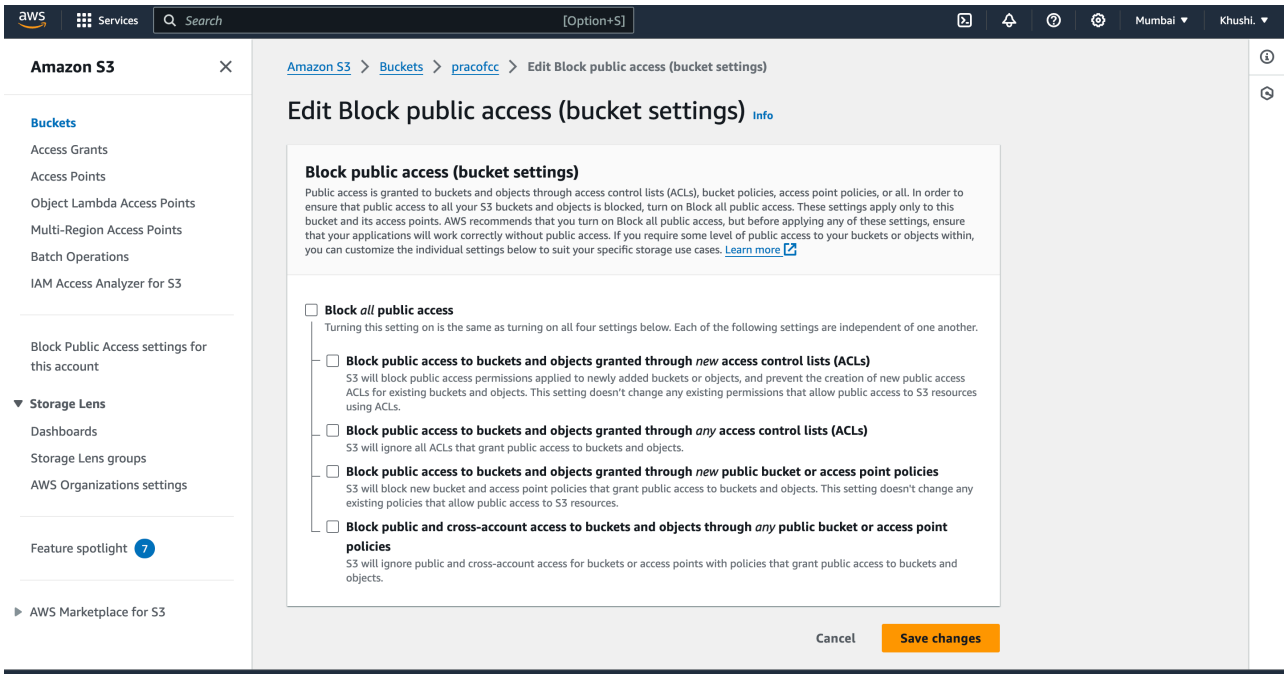
Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

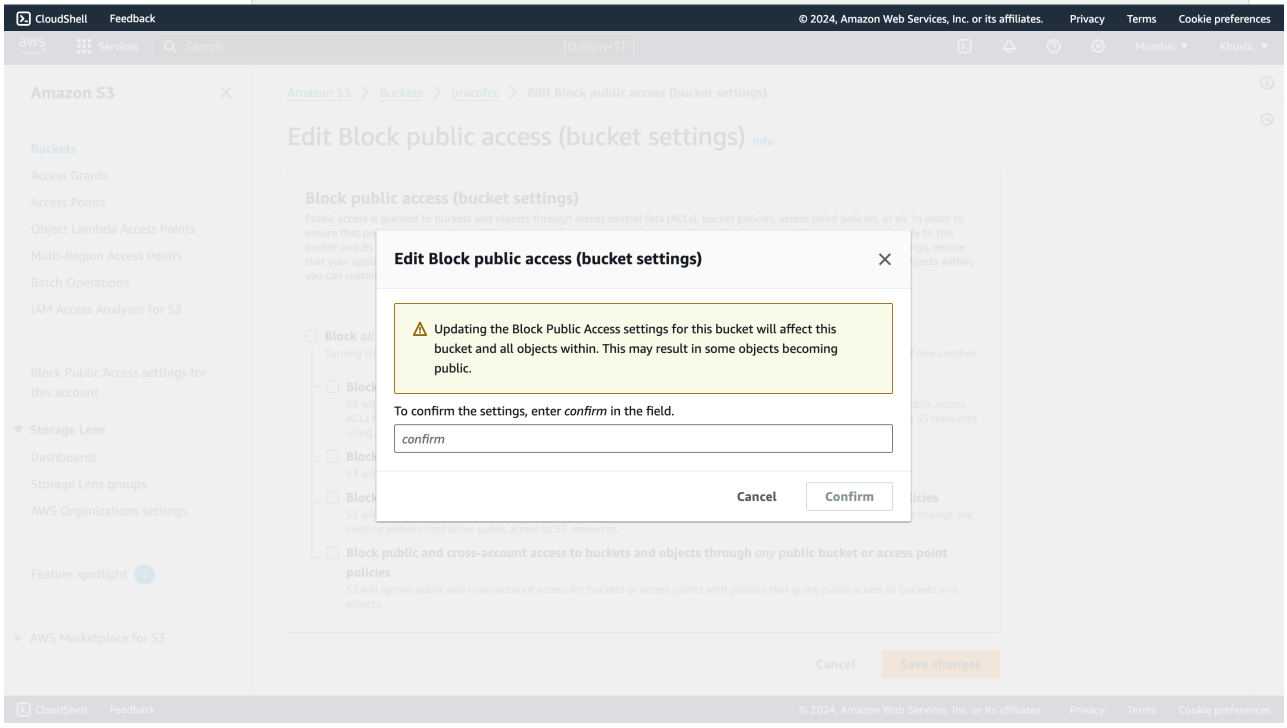

```
{
  "Id": "Policy1725038843326",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1725038838581",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::pracofcc",
      "Principal": "*"
    }
  ]
}
```

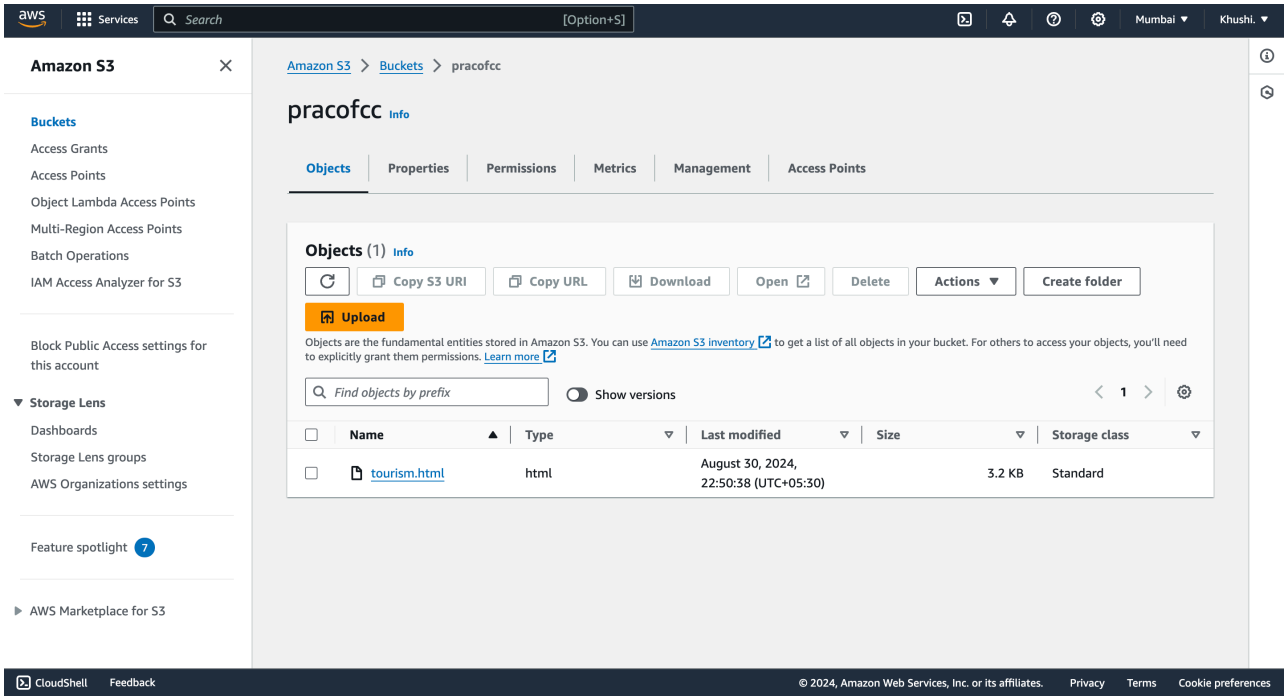

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that

Close


Services
Search
[Option+S]
Mumbai
Khushi.
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
AWS Marketplace for S3
Amazon S3 > Buckets > pracofcc > Edit bucket policy
Edit bucket policy Info
Bucket policy
Policy examples
Policy generator
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
Bucket ARN
arn:aws:s3:::pracofcc
Policy
{
"Id": "Policy1725038925375",
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Stmt1725038838581",
"Action": [
"s3:GetObject"
],
"Effect": "Allow",
"Resource": "arn:aws:s3:::pracofcc",
"Principal": "*"
}
]
}
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
Add new statement
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Option+S]
Mumbai
Khushi.
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
AWS Marketplace for S3
Amazon S3 > Buckets > pracofcc > Edit Block public access (bucket settings)
Edit Block public access (bucket settings) Info
Block public access (bucket settings)
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 all your S3 buckets and 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 your buckets 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.
Cancel
Save changes
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Edit Block public access (bucket settings)
Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.
To confirm the settings, enter confirm in the field.
confirm
Cancel
Confirm



You can see your file by copy paste it on the chrome