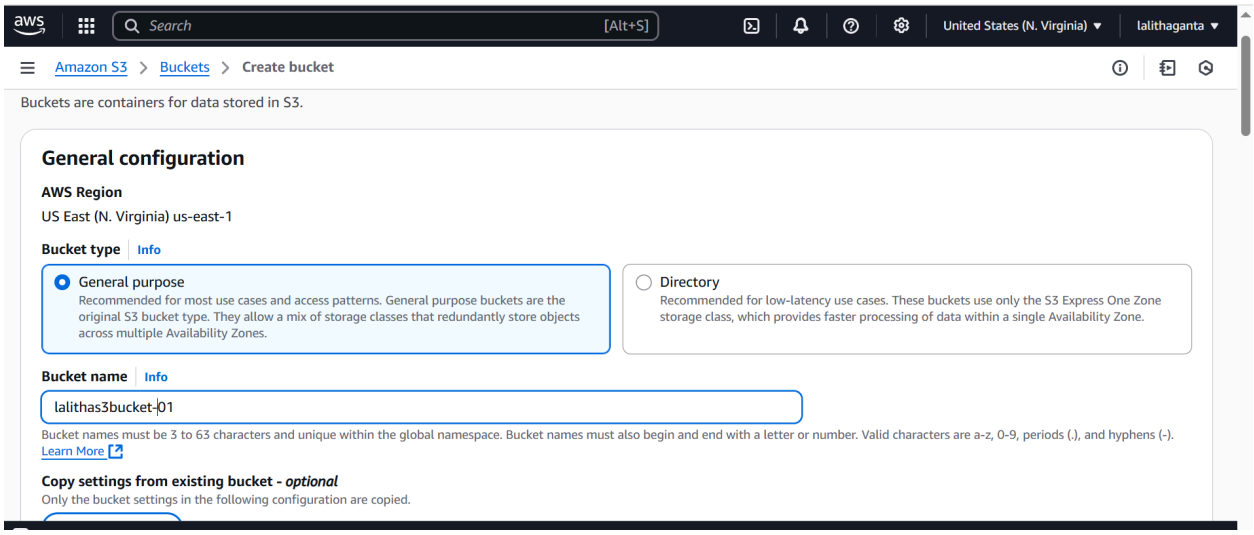
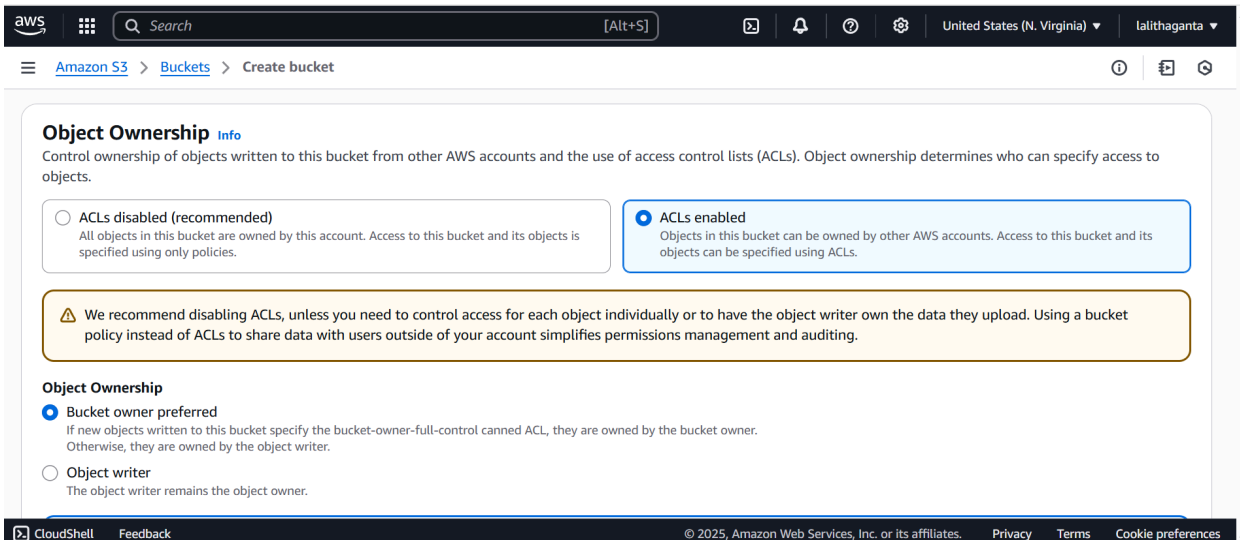
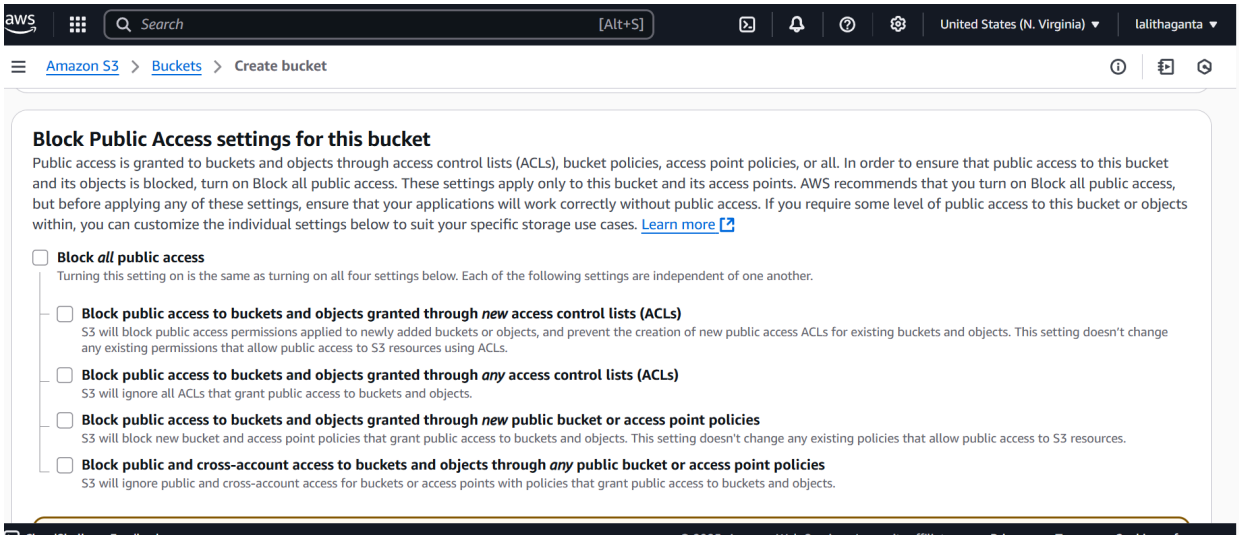
S3 Bucket Tasks

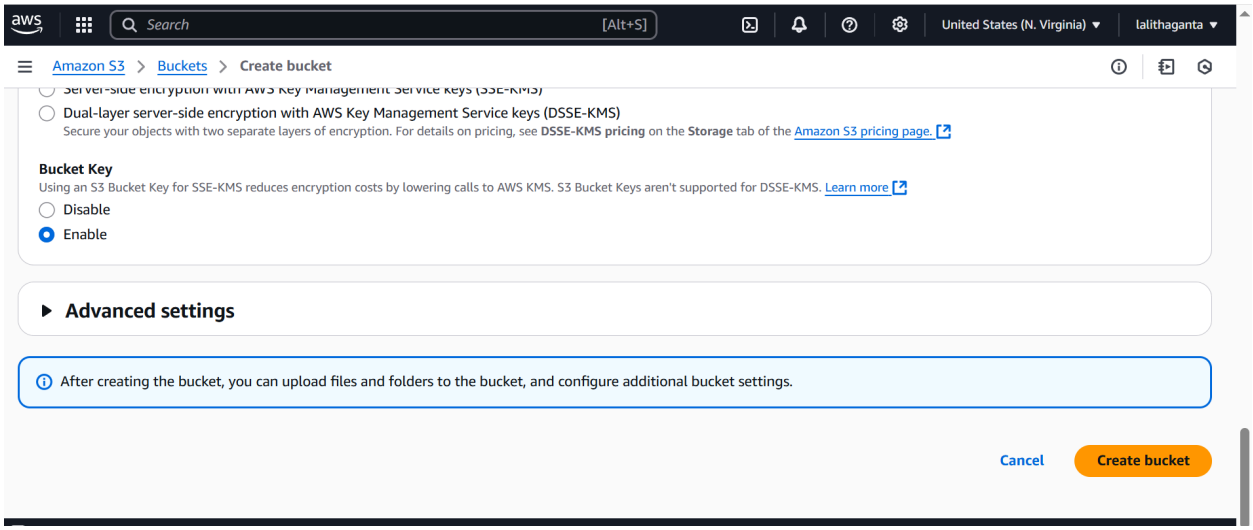
`1) Create s3 bucket and upload some objects to s3.`

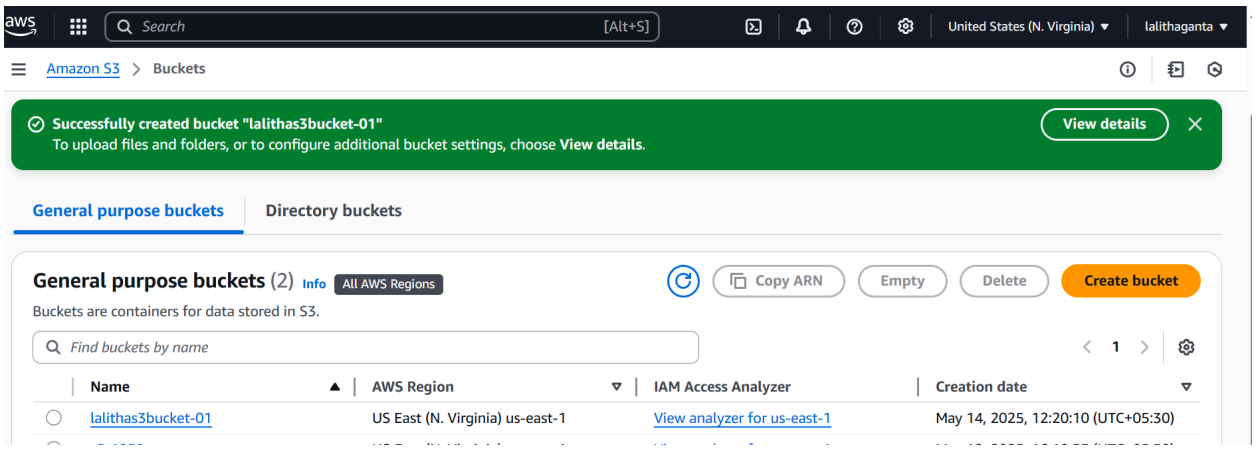
Create an S3 Bucket:
Sign in to the AWS Management Console
.Click "Create bucket"
.Bucket name Must be globally unique
Region Choose a region close to you
Click "Create bucket"
Upload Objects: Open the bucket by clicking its name.
Click "Upload"
Choose files from your computer Click "Upload"

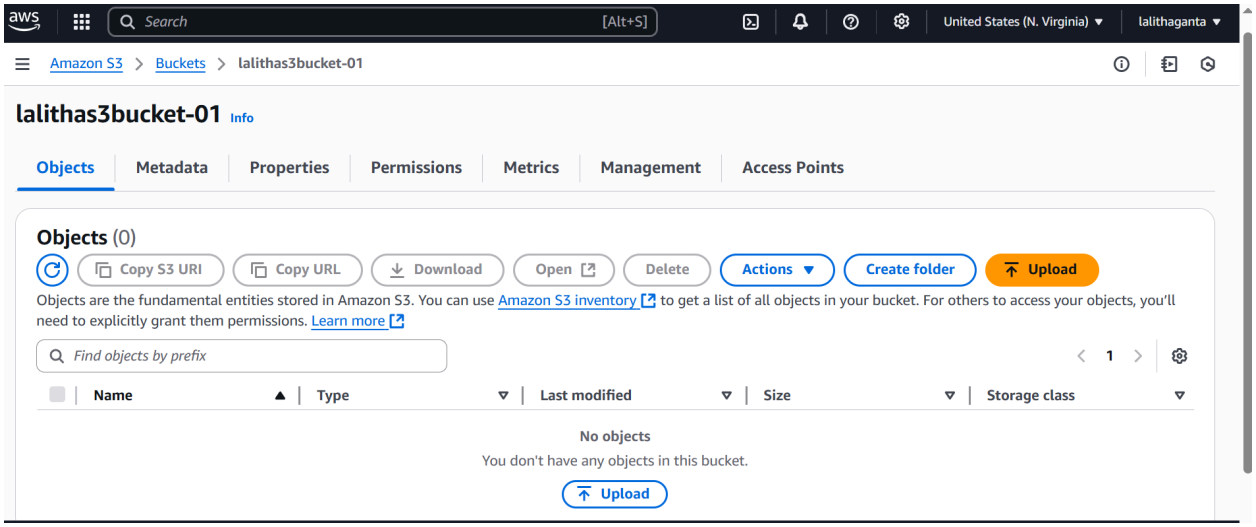


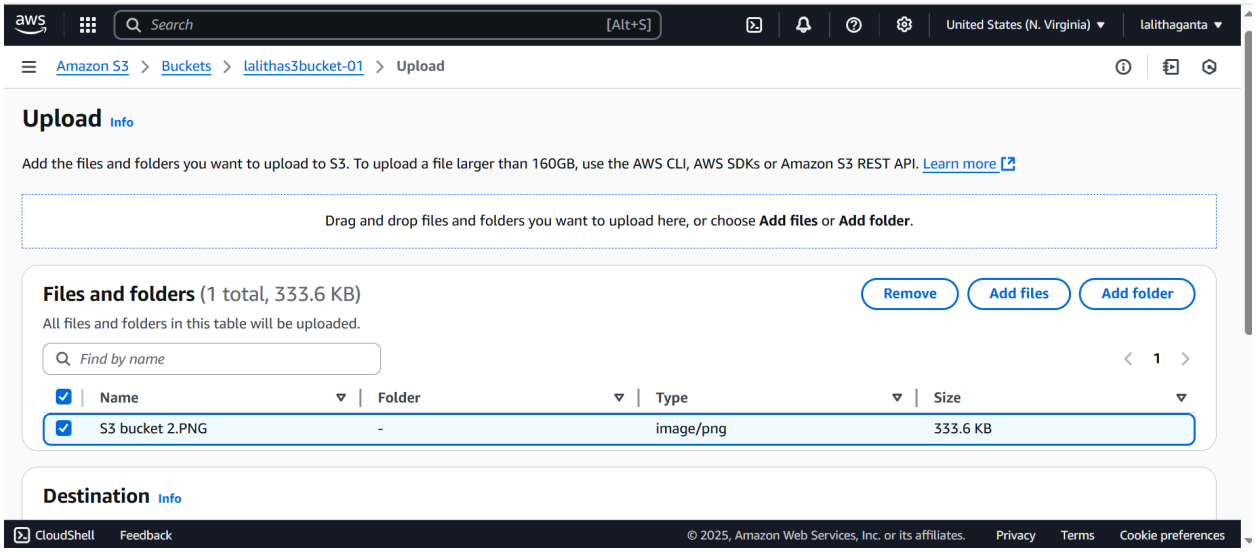

aws
Search
[Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > Create bucket
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
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.
We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.
Object Ownership
Bucket owner preferred
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.
Object writer
The object writer remains the object owner.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

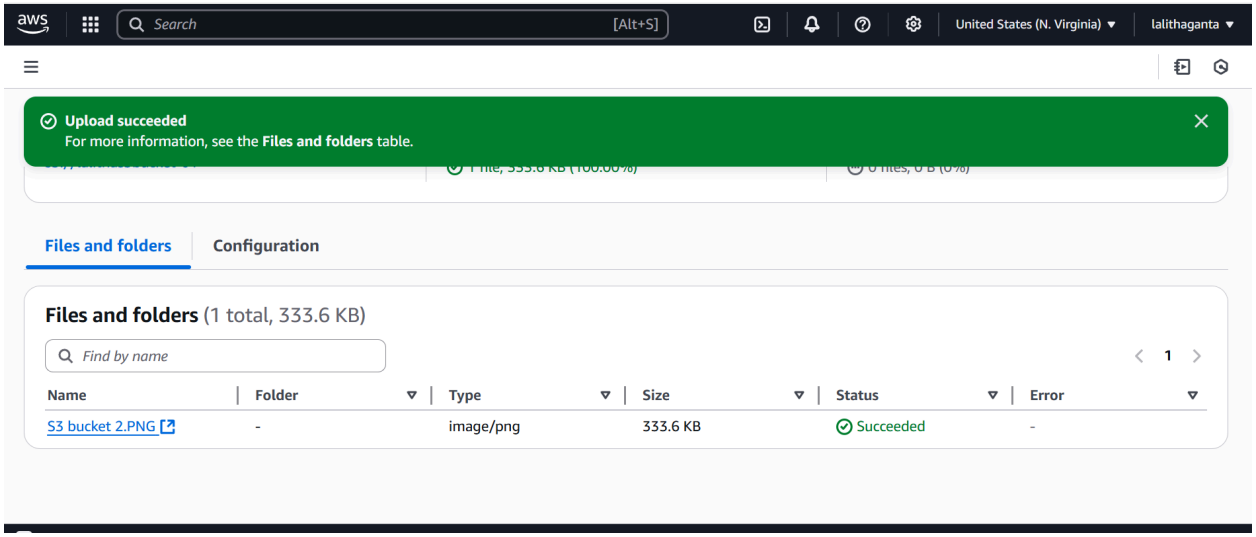

aws
Search
[Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > Create bucket
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public 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.

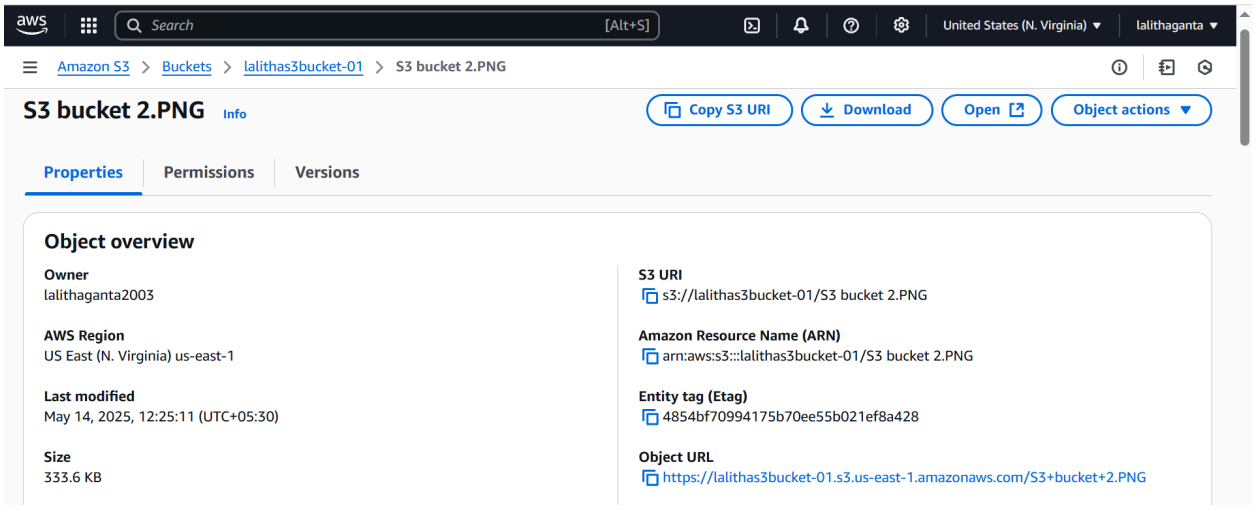

Search [Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > Create bucket
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of 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

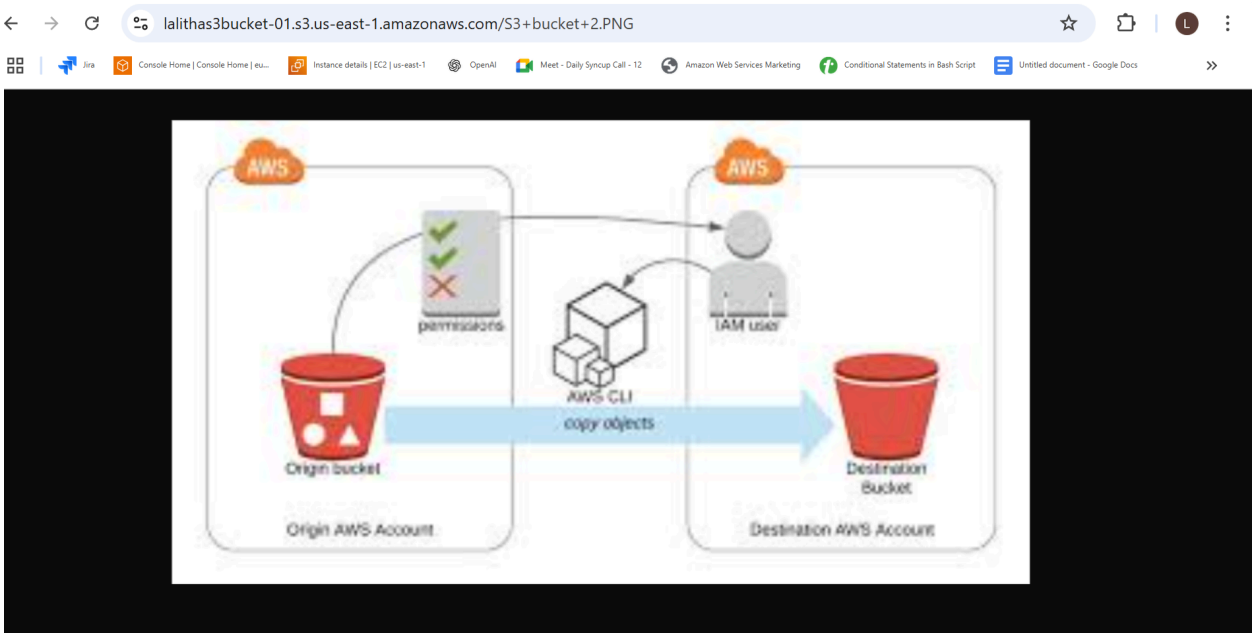

Search [Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets
Successfully created bucket "lalithas3bucket-01"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
General purpose buckets
Directory buckets
General purpose buckets (2) Info All AWS Regions
Copy ARN
Empty
Delete
Create bucket
Buckets are containers for data stored in S3.
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
lalithas3bucket-01
US East (N. Virginia) us-east-1
View analyzer for us-east-1
May 14, 2025, 12:20:10 (UTC+05:30)


Search [Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > lalithas3bucket-01
lalithas3bucket-01 Info
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Objects (0)
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
Name
Type
Last modified
Size
Storage class
No objects
You don't have any objects in this bucket.
Upload


Search [Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > lalithas3bucket-01 > 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, 333.6 KB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
1
Name
Folder
Type
Size
S3 bucket 2.PNG
-
image/png
333.6 KB
Destination Info
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
United States (N. Virginia)
lalithaganta
Upload succeeded
For more information, see the Files and folders table.
Files and folders
Configuration
Files and folders (1 total, 333.6 KB)
Find by name
1
Name
Folder
Type
Size
Status
Error
S3 bucket 2.PNG
-
image/png
333.6 KB
Succeeded
-


Search [Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > lalithas3bucket-01 > S3 bucket 2.PNG
S3 bucket 2.PNG Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
lalithaganta2003
AWS Region
US East (N. Virginia) us-east-1
Last modified
May 14, 2025, 12:25:11 (UTC+05:30)
Size
333.6 KB
S3 URI
s3://lalithas3bucket-01/S3 bucket 2.PNG
Amazon Resource Name (ARN)
arn:aws:s3:::lalithas3bucket-01/S3 bucket 2.PNG
Entity tag (Etag)
4854bf70994175b70ee55b021ef8a428
Object URL
https://lalithas3bucket-01.s3.us-east-1.amazonaws.com/S3+bucket+2.PNG



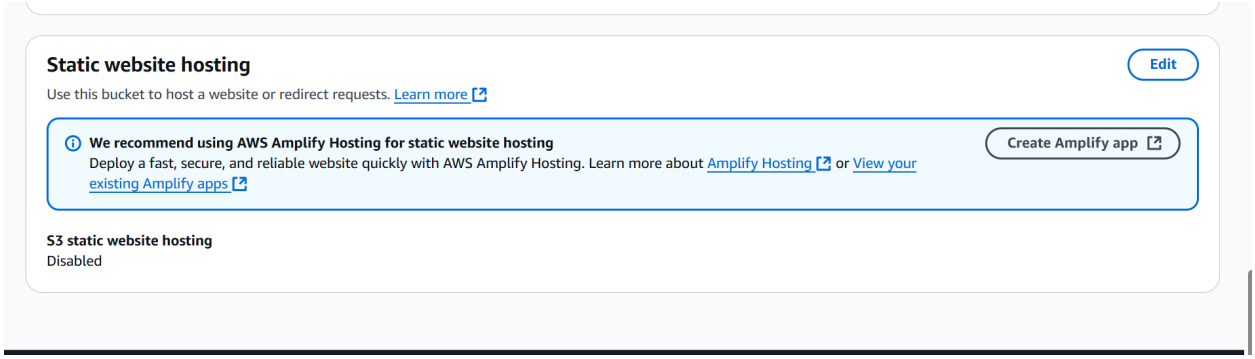
2) Deploy static website in s3 bucket.

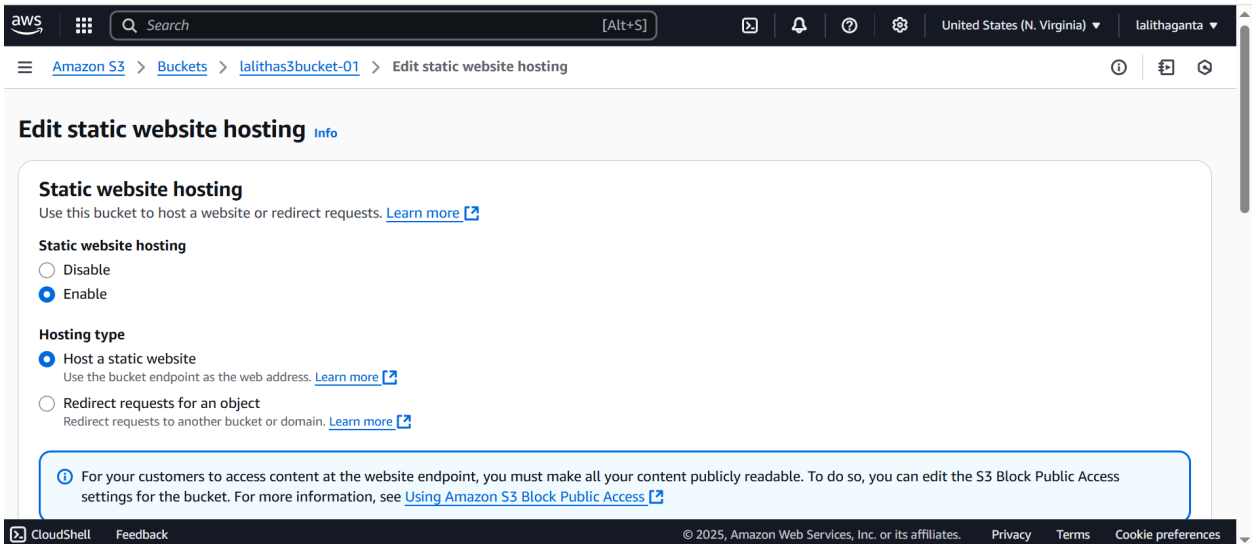
Click on the existing bucket and Upload Website Files
Index.html (homepage)
Error.html (custom error page)
Upload Files: Open the bucket.
Click "Upload" > Add files
.Enable Static Website Hosting Go to the "Properties" tab of your bucket.
Scroll to “Static website hosting”
Click Edit then: Choose Enable
Set Index document =index.html
Set Error document = error.html
Make Files Public:
Go to Bucket Policy - Go to the Permissions tab.
Click Bucket policy
Paste this JSON (replace your-bucket-name):
{

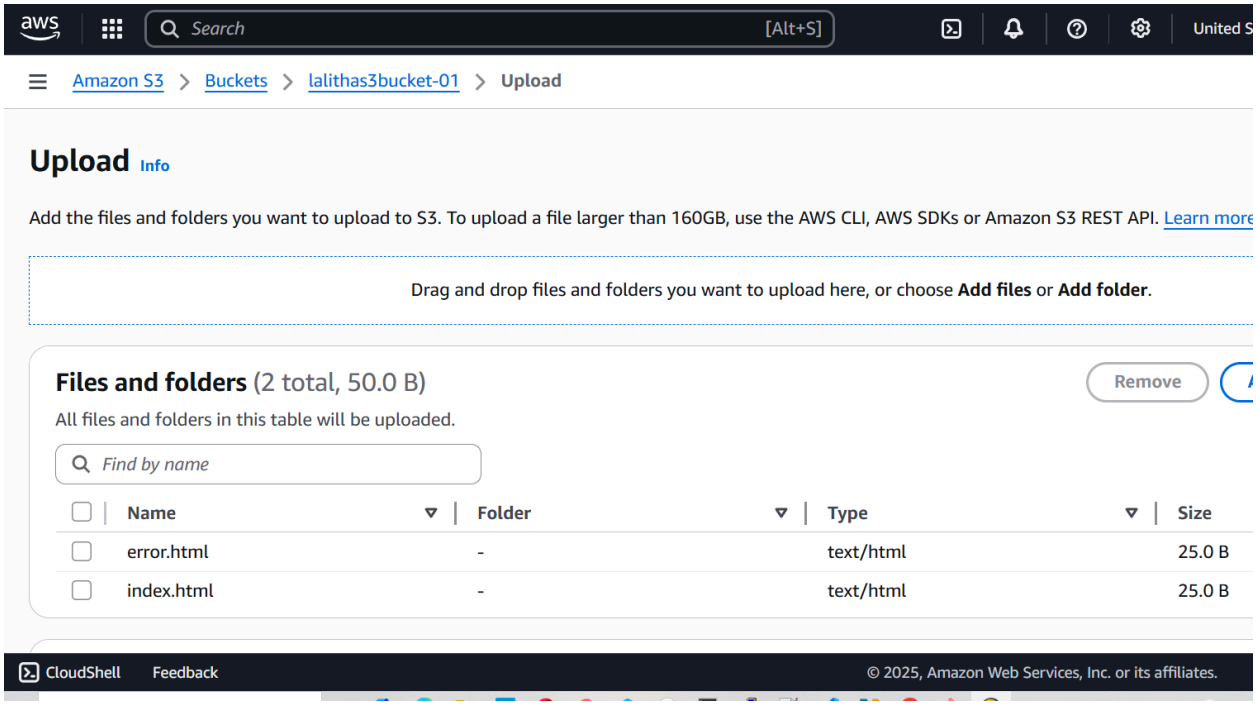
```
 "Version": "2012-10-17",
 "Statement": [
 {
     "Sid": "PublicReadGetObject",
       "Effect": "Allow",
         "Principal": "*",
       "Action": "s3:GetObject",
       "Resource": "arn:aws:s3:::bucket-name/*"
}
 ]

}
```

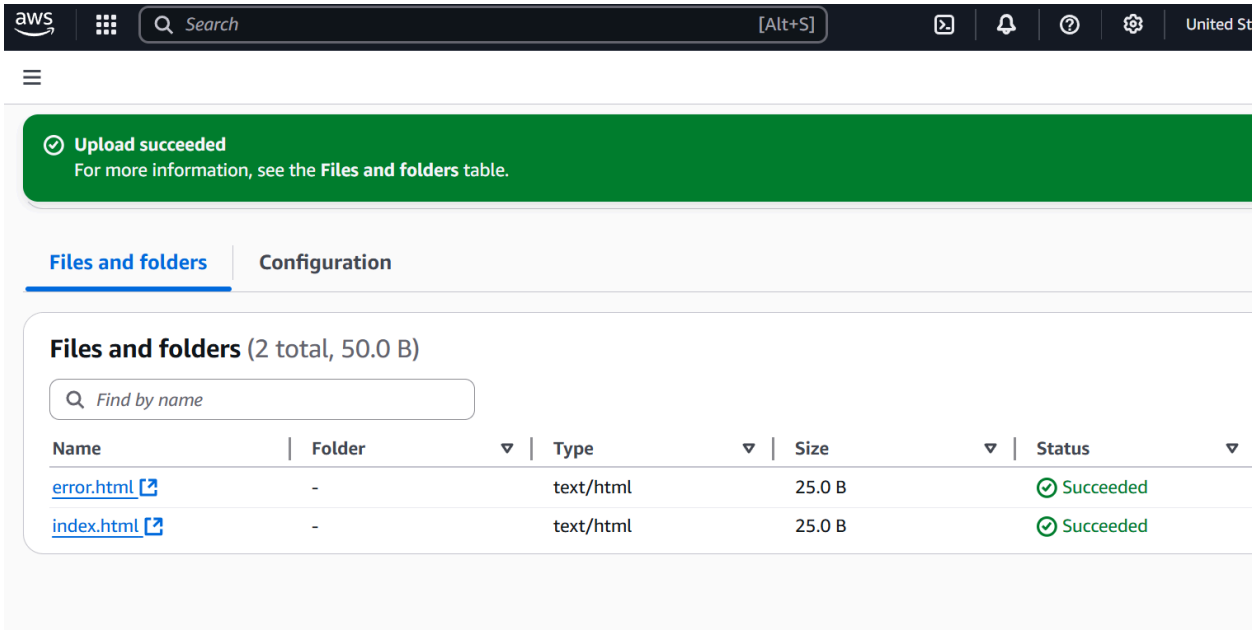
MINGW64:/c/Users/HP

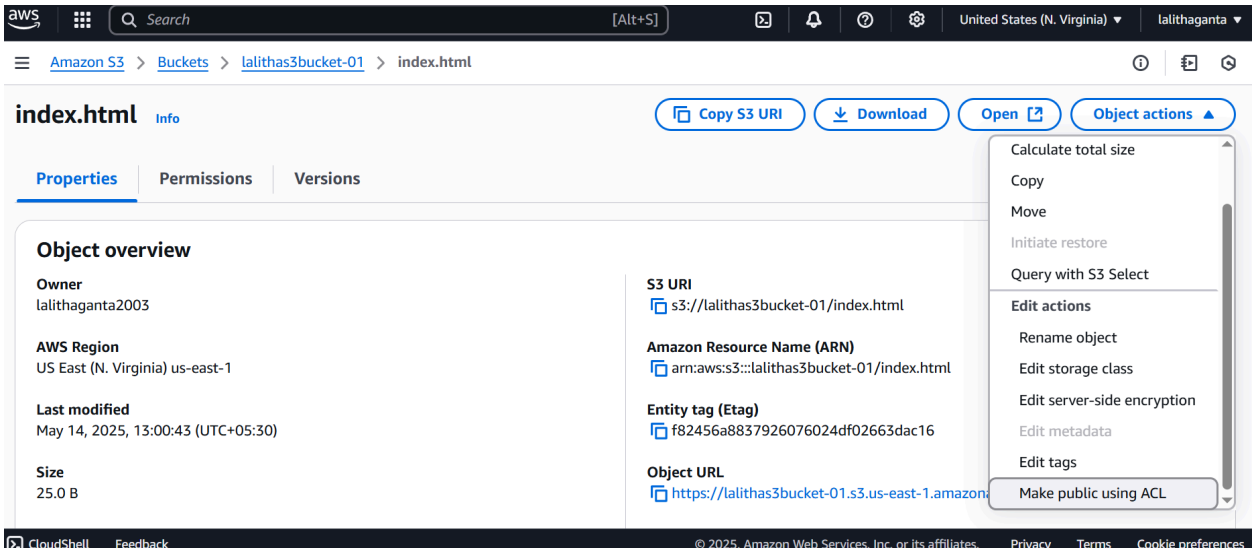
```
HP@LAPTOP-LPTR344H MINGW64 ~ (main)
$ vi index.html

HP@LAPTOP-LPTR344H MINGW64 ~ (main)
$ vi error.html

HP@LAPTOP-LPTR344H MINGW64 ~ (main)
$ cat index.html
Hi!
Welcome to S3 bucket.

HP@LAPTOP-LPTR344H MINGW64 ~ (main)
$ cat error.html
wait!
Under maintainence.

HP@LAPTOP-LPTR344H MINGW64 ~ (main)
$
```

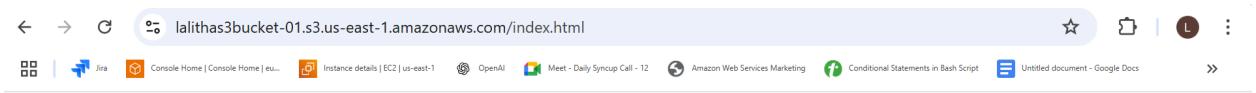


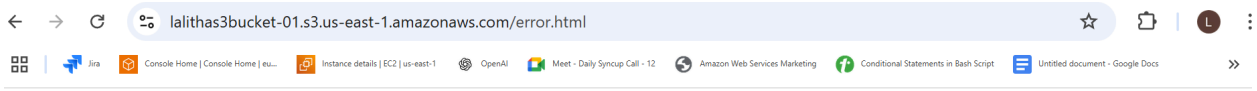

Search
[Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > lalithas3bucket-01 > Edit static website hosting
Edit static website hosting Info
Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Static website hosting
Disable
Enable
Hosting type
Host a static website
Use the bucket endpoint as the web address. Learn more
Redirect requests for an object
Redirect requests to another bucket or domain. Learn more
For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
Amazon S3 > Buckets > lalithas3bucket-01 > 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 (2 total, 50.0 B)
Remove
All files and folders in this table will be uploaded.
Find by name
Name
Folder
Type
Size
error.html
-
text/html
25.0 B
index.html
-
text/html
25.0 B
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.


Search
[Alt+S]
United St
Upload succeeded
For more information, see the Files and folders table.
Files and folders
Configuration
Files and folders (2 total, 50.0 B)
Find by name
Name
Folder
Type
Size
Status
error.html
-
text/html
25.0 B
Succeeded
index.html
-
text/html
25.0 B
Succeeded


Search
[Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3
Buckets
lalithas3bucket-01
index.html
index.html
Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
lalithaganta2003
AWS Region
US East (N. Virginia) us-east-1
Last modified
May 14, 2025, 13:00:43 (UTC+05:30)
Size
25.0 B
S3 URI
s3://lalithas3bucket-01/index.html
Amazon Resource Name (ARN)
arn:aws:s3:::lalithas3bucket-01/index.html
Entity tag (Etag)
f82456a8837926076024df02663dac16
Object URL
https://lalithas3bucket-01.s3.us-east-1.amazon
Calculate total size
Copy
Move
Initiate restore
Query with S3 Select
Edit actions
Rename object
Edit storage class
Edit server-side encryption
Edit metadata
Edit tags
Make public using ACL
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences





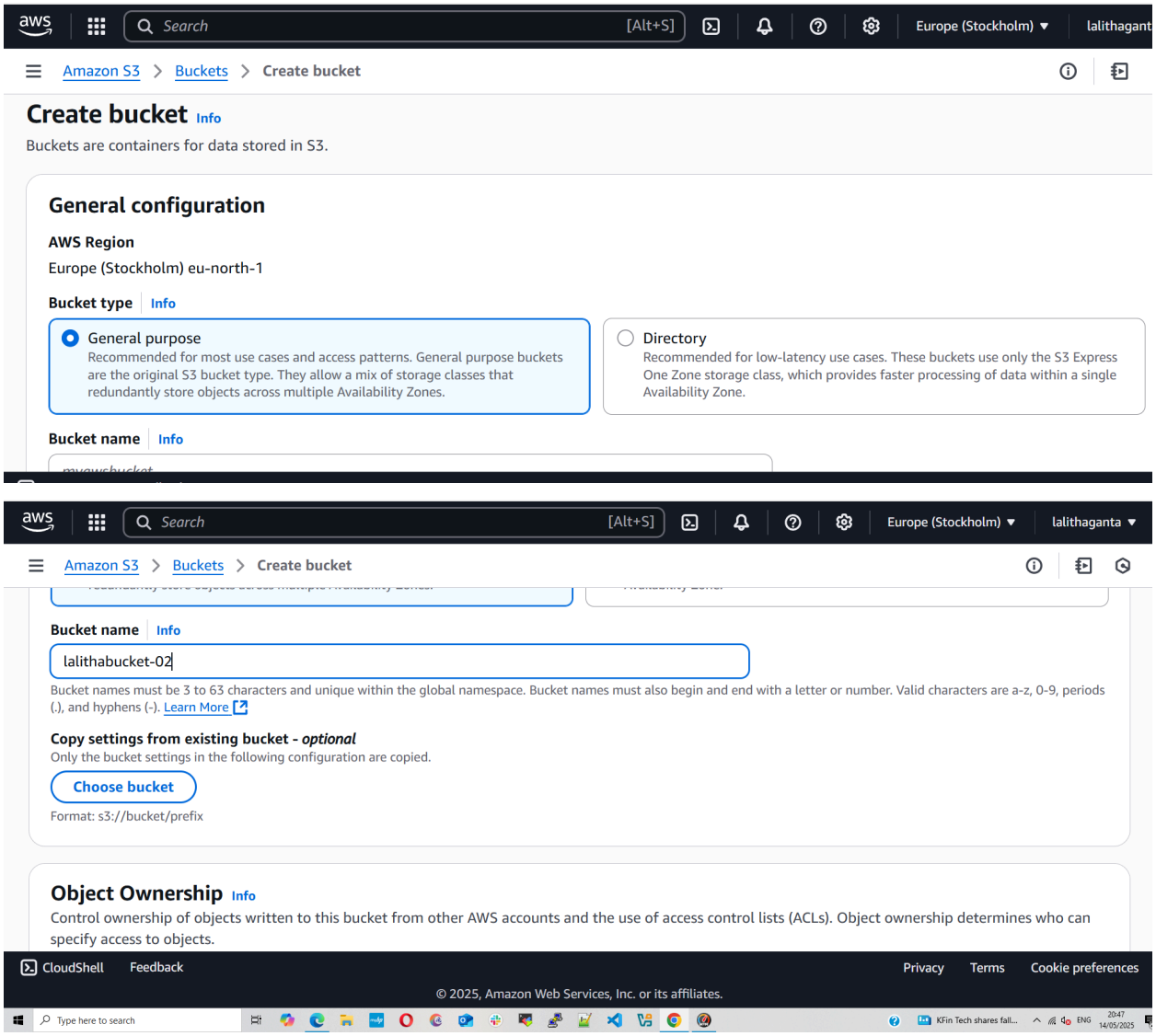
3) Enable cross region replication on s3 buckets.

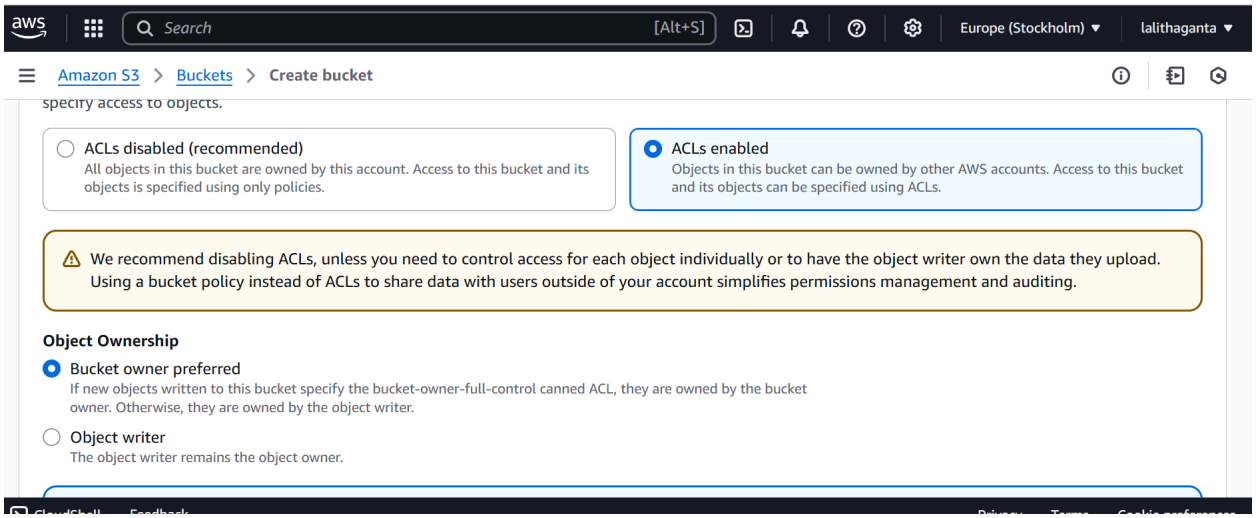
Create Source and Destination Buckets
Go to the S3 Console

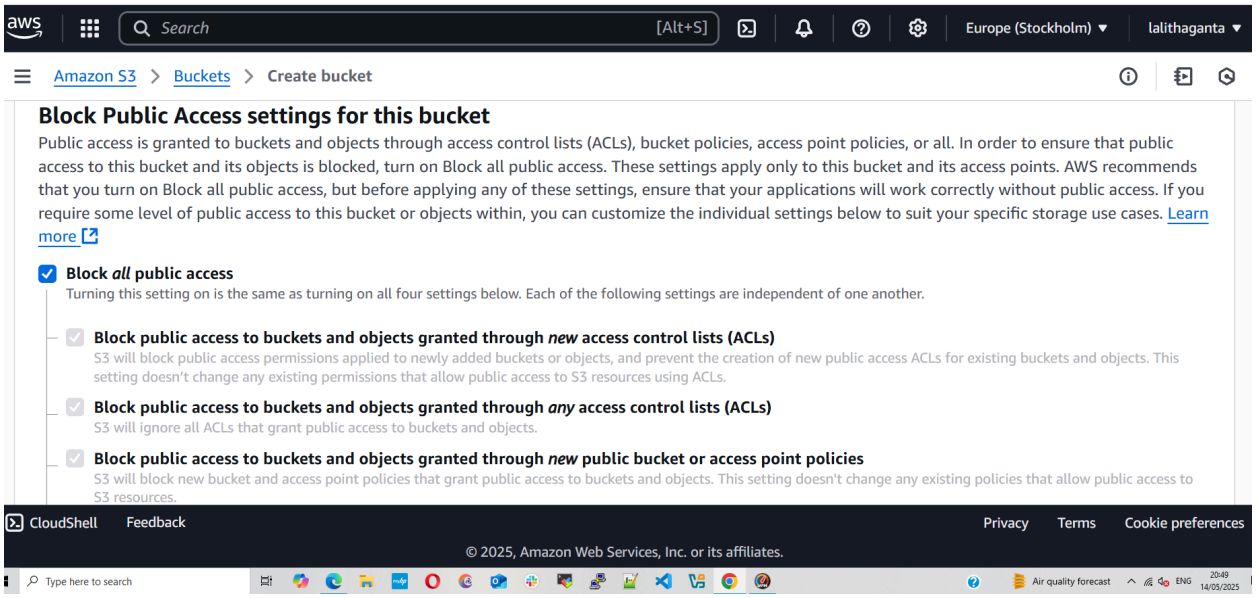
Create a source bucket and enable versioning

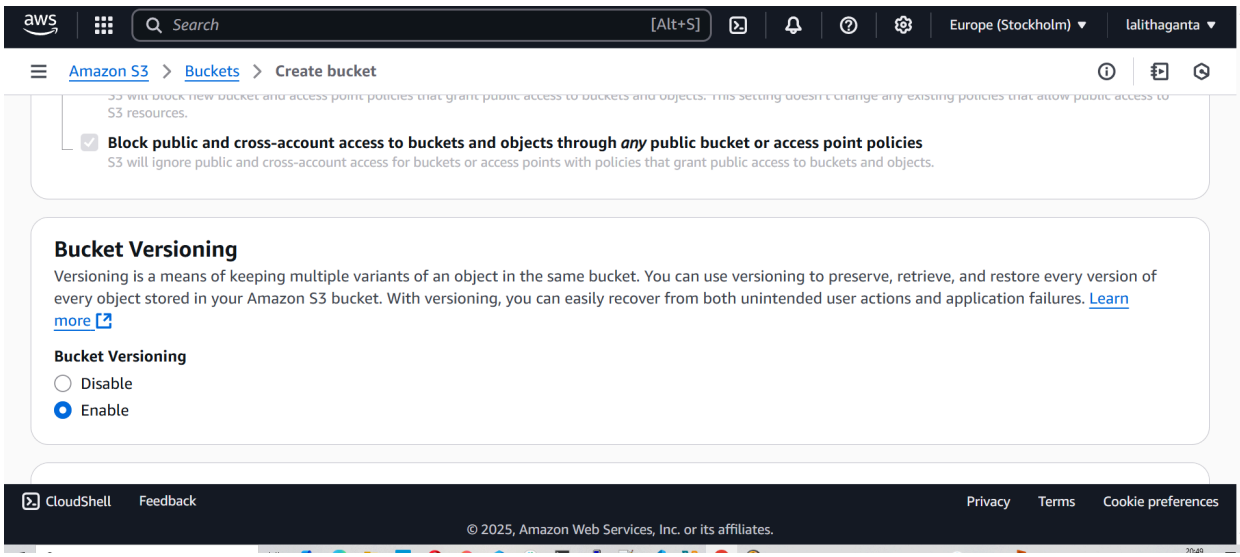
Create a destination bucket

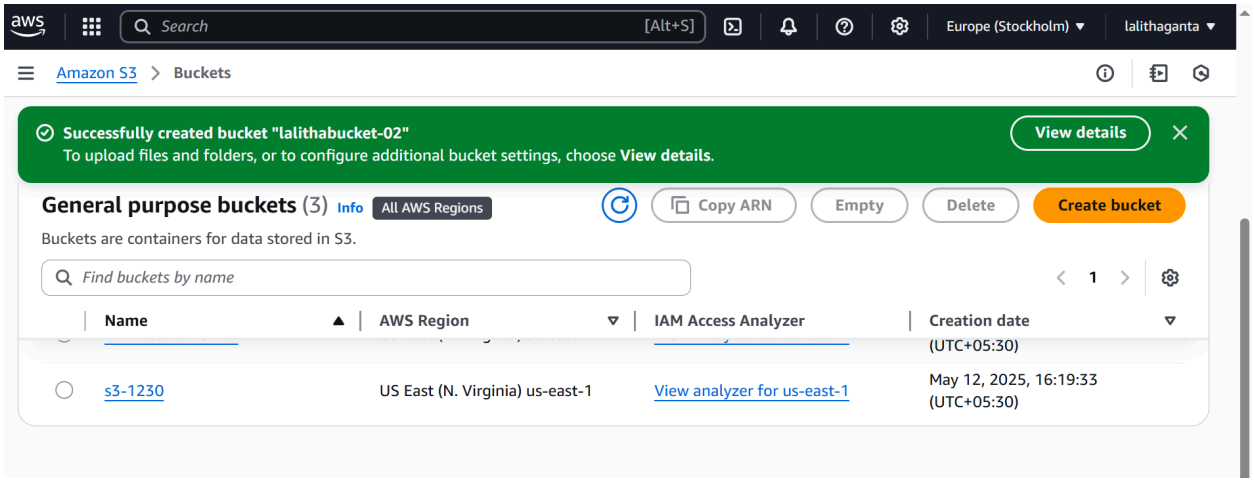
Enable Replication on Source Bucket
Open the source bucket
Go to the “Management” tab.
Scroll to “Replication rules” and click “Create replication rule”
Configure the Rule Rule name Any name (e.g., replicate-to-mumbai)
Status Keep it as enabled
Choose “This rule applies to all objects in the bucket”

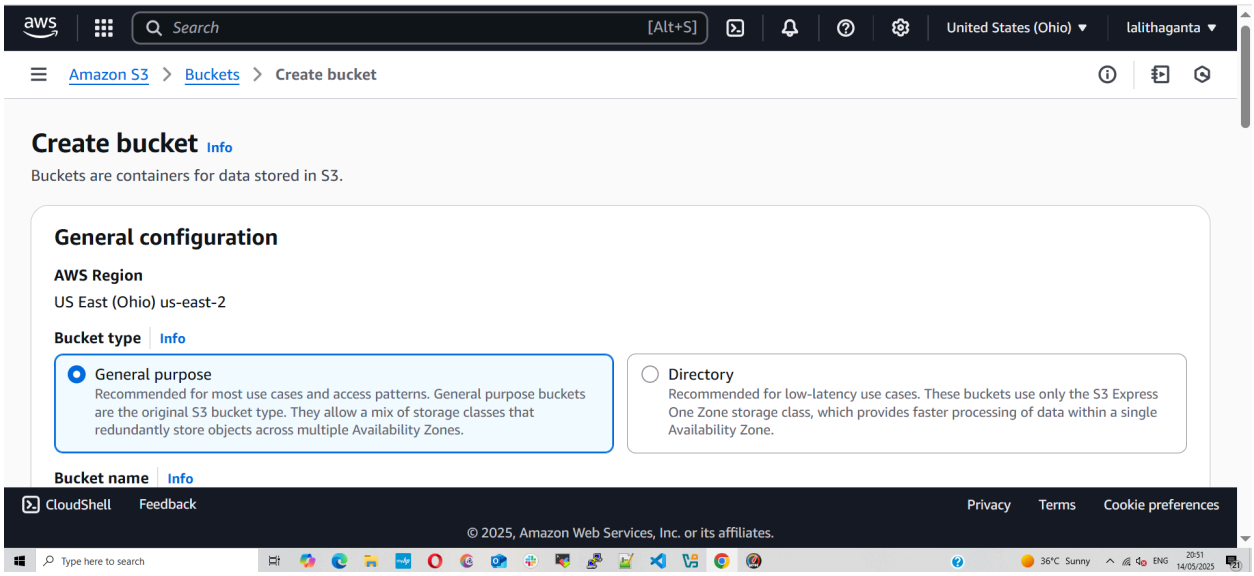


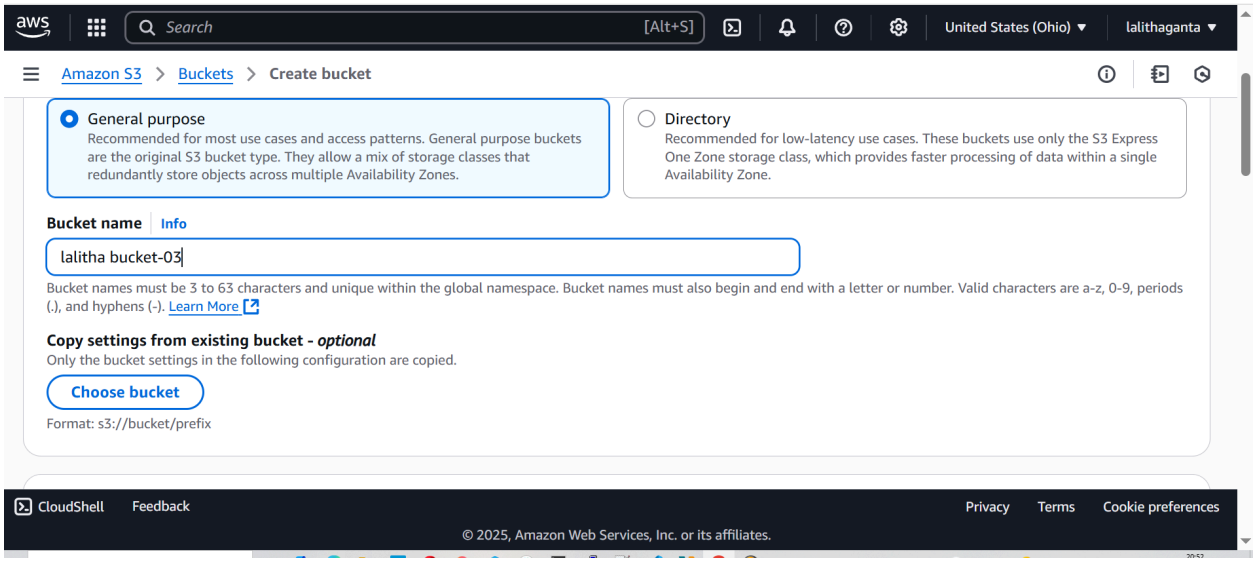

aws
Search
[Alt+S]
Europe (Stockholm)
lalithaganta
Amazon S3 > Buckets > Create bucket
specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.
Object Ownership
Bucket owner preferred
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.
Object writer
The object writer remains the object owner.

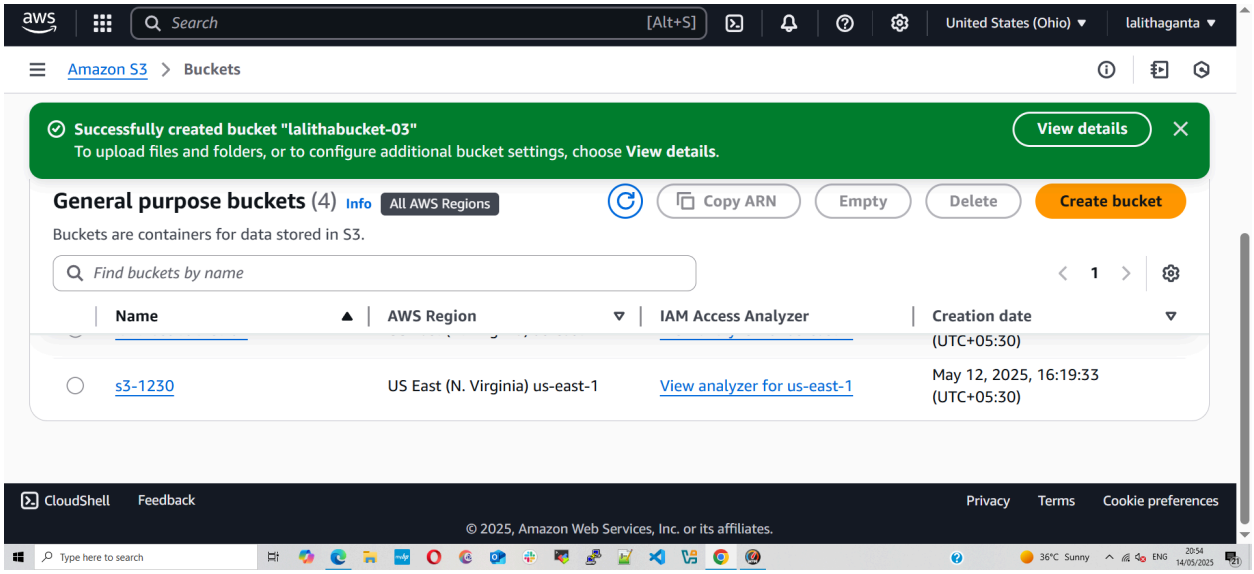

aws
Search
[Alt+S]
Europe (Stockholm)
lalithaganta
Amazon S3 > Buckets > Create bucket
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access 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.
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.

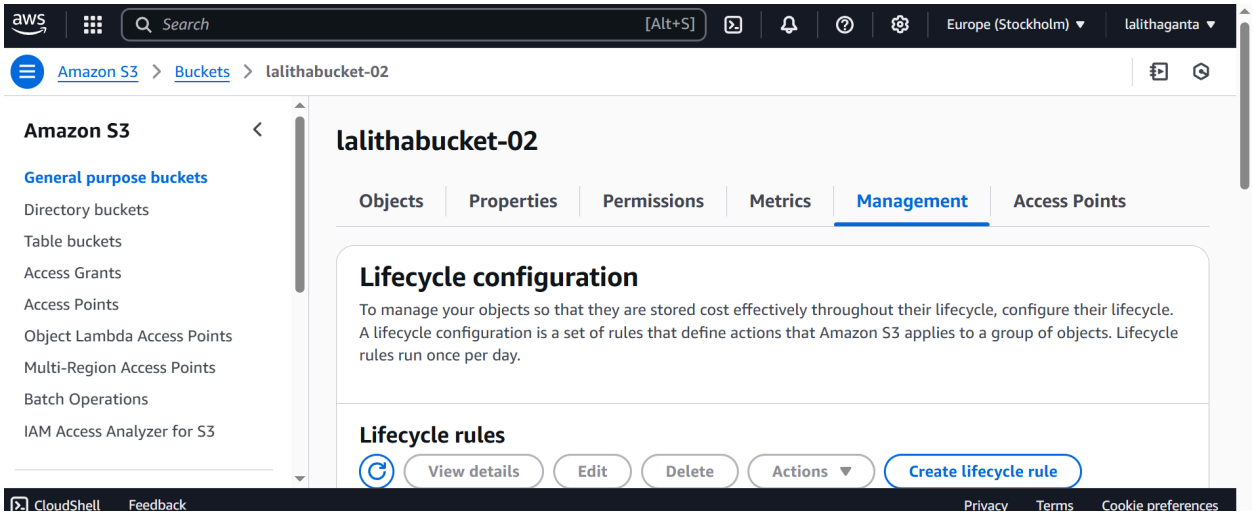

aws
Search
[Alt+S]
Europe (Stockholm)
lalithaganta
Amazon S3 > Buckets > Create bucket
S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies 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, 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
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.

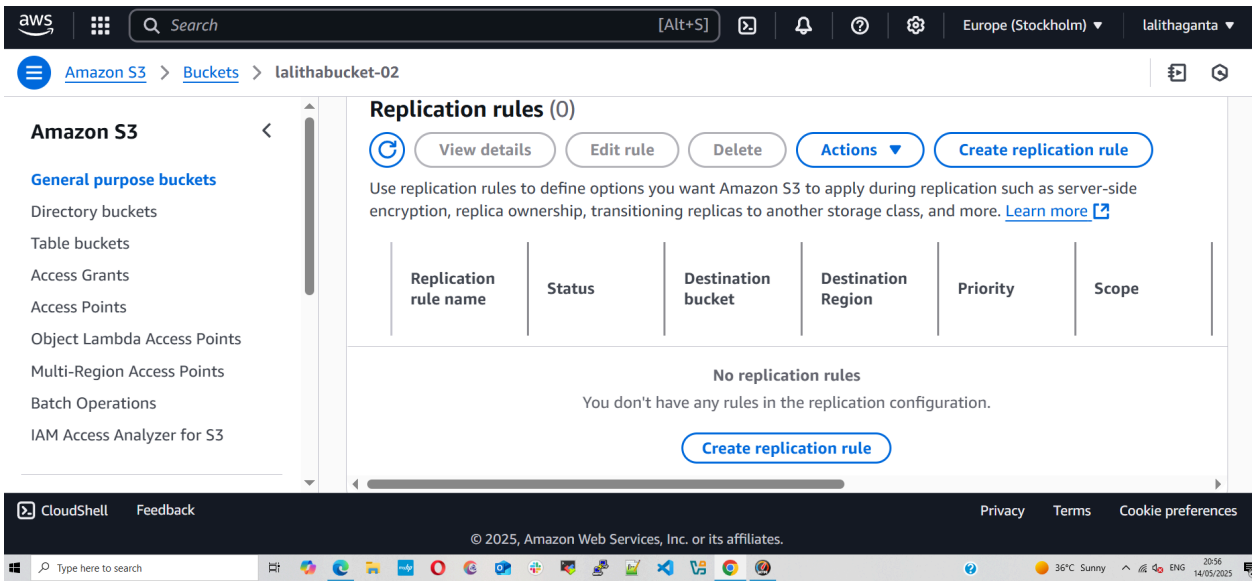

Search [Alt+S]
Europe (Stockholm)
lalithaganta
Amazon S3 > Buckets
Successfully created bucket "lalithabucket-02"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
General purpose buckets (3) Info
All AWS Regions
Copy ARN
Empty
Delete
Create bucket
Buckets are containers for data stored in S3.
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
(UTC+05:30)
s3-1230
US East (N. Virginia) us-east-1
View analyzer for us-east-1
May 12, 2025, 16:19:33 (UTC+05:30)

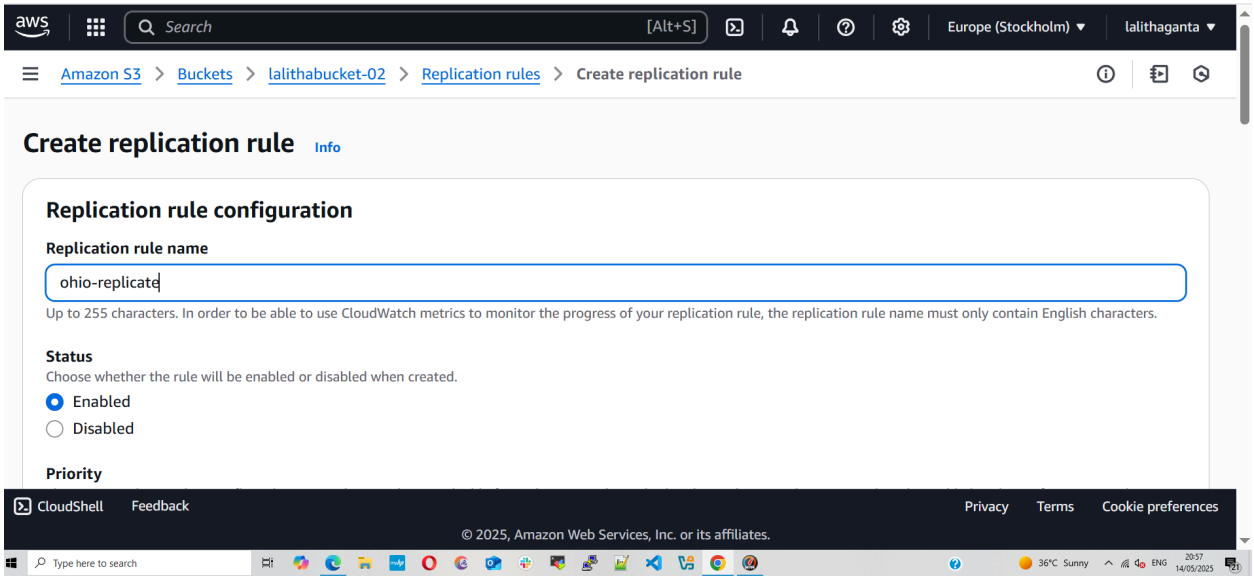

Search [Alt+S]
United States (Ohio)
lalithaganta
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
US East (Ohio) us-east-2
Bucket type Info
General purpose
Recommended for most use cases and access patterns. General 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
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.

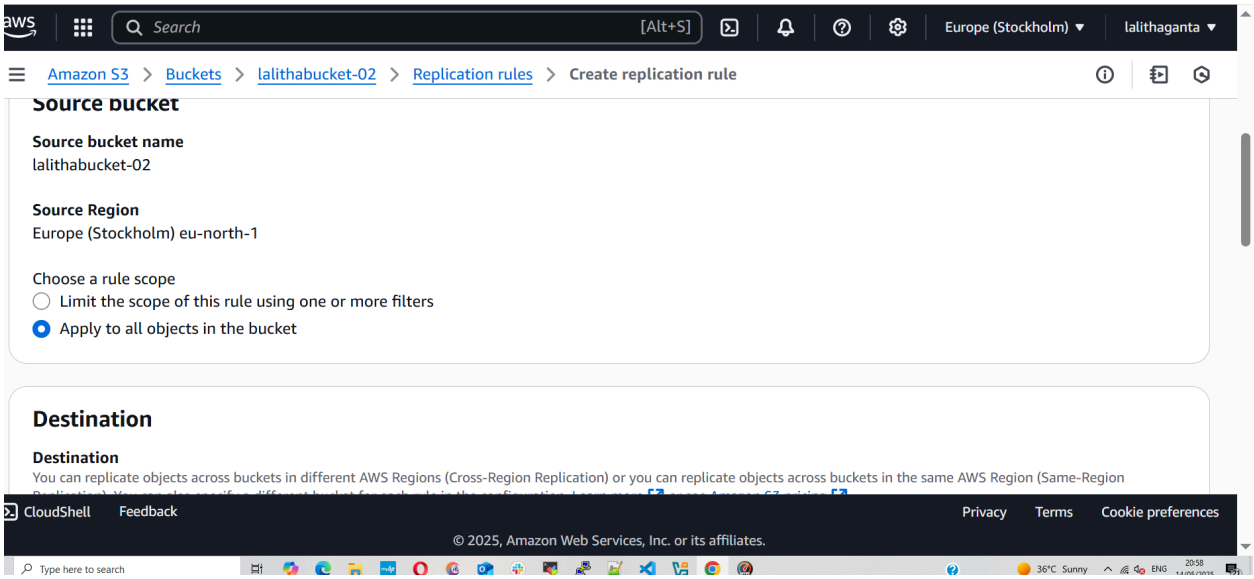

Search [Alt+S]
United States (Ohio)
lalithaganta
Amazon S3 > Buckets > Create bucket
General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability 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
lalitha bucket-03
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
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.

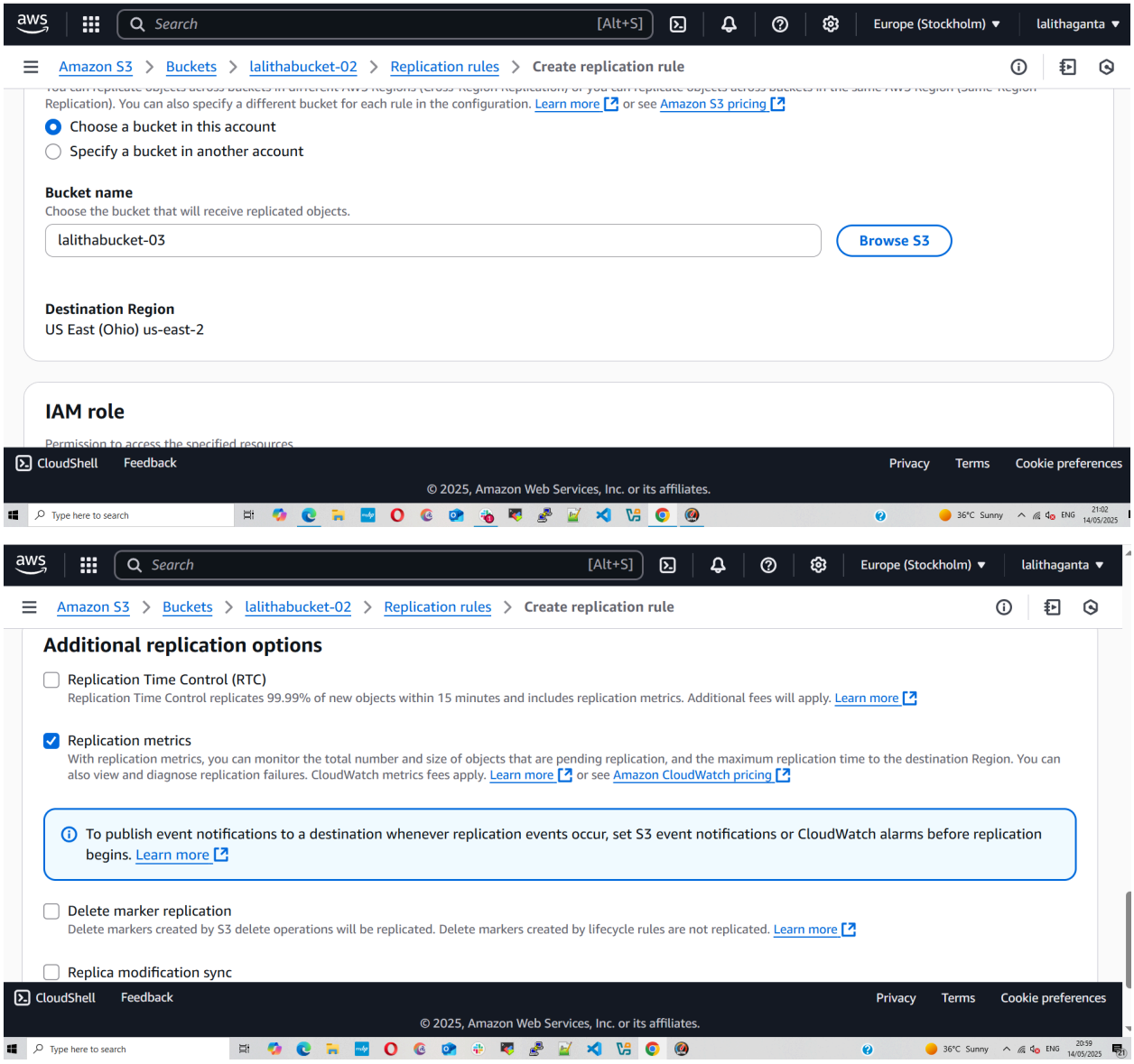

Search [Alt+S]
United States (Ohio)
lalithaganta
Amazon S3 > Buckets
Successfully created bucket "lalithabucket-03"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
General purpose buckets (4) Info All AWS Regions
Copy ARN
Empty
Delete
Create bucket
Buckets are containers for data stored in S3.
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
s3-1230
US East (N. Virginia) us-east-1
View analyzer for us-east-1
May 12, 2025, 16:19:33 (UTC+05:30)
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.


Search [Alt+S]
Europe (Stockholm)
lalithaganta
Amazon S3 > Buckets > lalithabucket-02
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
lalithabucket-02
Objects
Properties
Permissions
Metrics
Management
Access Points
Lifecycle configuration
To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.
Lifecycle rules
View details
Edit
Delete
Actions
Create lifecycle rule
CloudShell
Feedback
Privacy
Terms
Cookie preferences

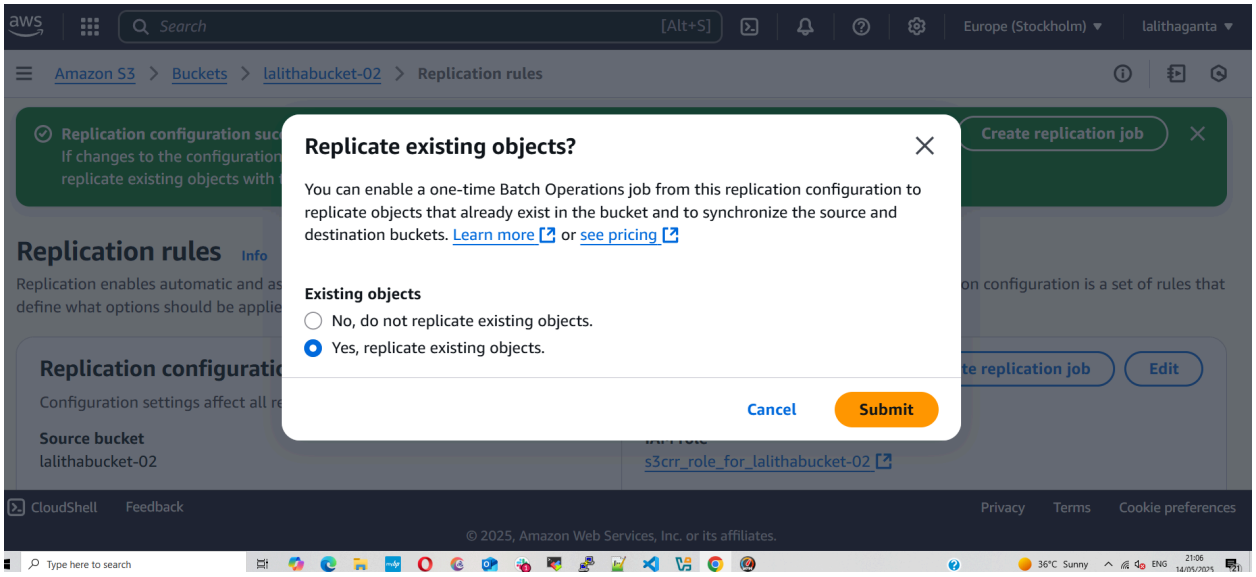

Search [Alt+S]
Europe (Stockholm)
lalithaganta
Amazon S3 > Buckets > lalithabucket-02
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Replication rules (0)
View details
Edit rule
Delete
Actions
Create replication rule
Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. Learn more
Replication rule name
Status
Destination bucket
Destination Region
Priority
Scope
No replication rules
You don't have any rules in the replication configuration.
Create replication rule
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.

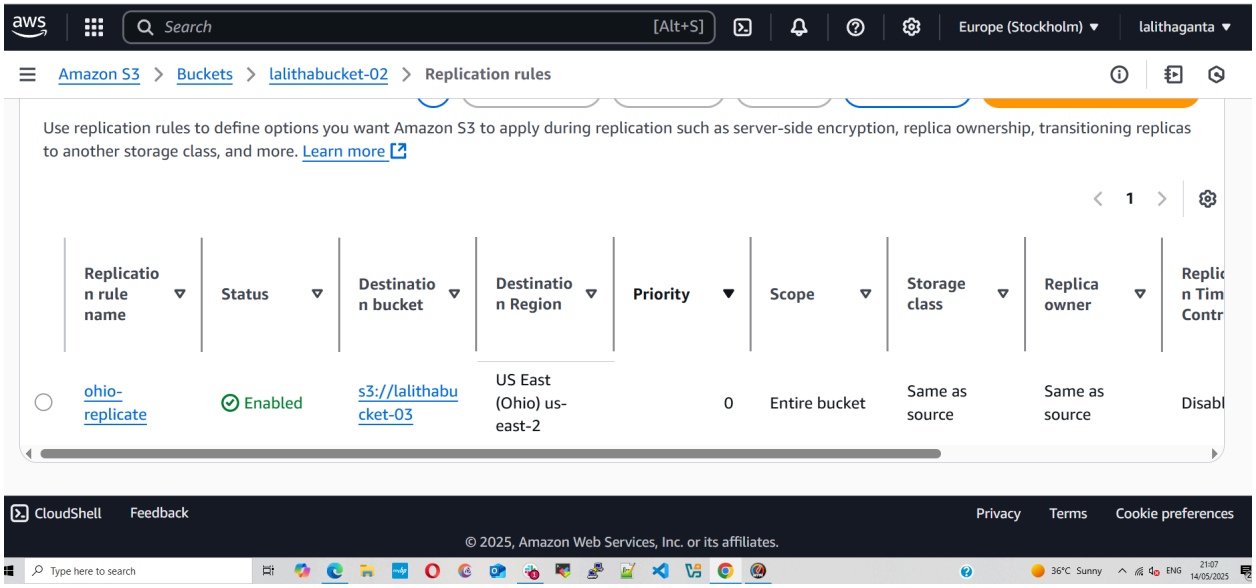

Search [Alt+S]
Europe (Stockholm)
lalithaganta
Amazon S3 > Buckets > lalithabucket-02 > Replication rules > Create replication rule
Create replication rule Info
Replication rule configuration
Replication rule name
ohio-replicate
Up to 255 characters. In order to be able to use CloudWatch metrics to monitor 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
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.
Type here to search
36°C Sunny
ENG
20:57
14/05/2025


Search [Alt+S]
Europe (Stockholm)
lalithaganta
Amazon S3 > Buckets > lalithabucket-02 > Replication rules > Create replication rule
Source bucket
Source bucket name
lalithabucket-02
Source Region
Europe (Stockholm) eu-north-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
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.
Type here to search
36°C Sunny
ENG
20:58

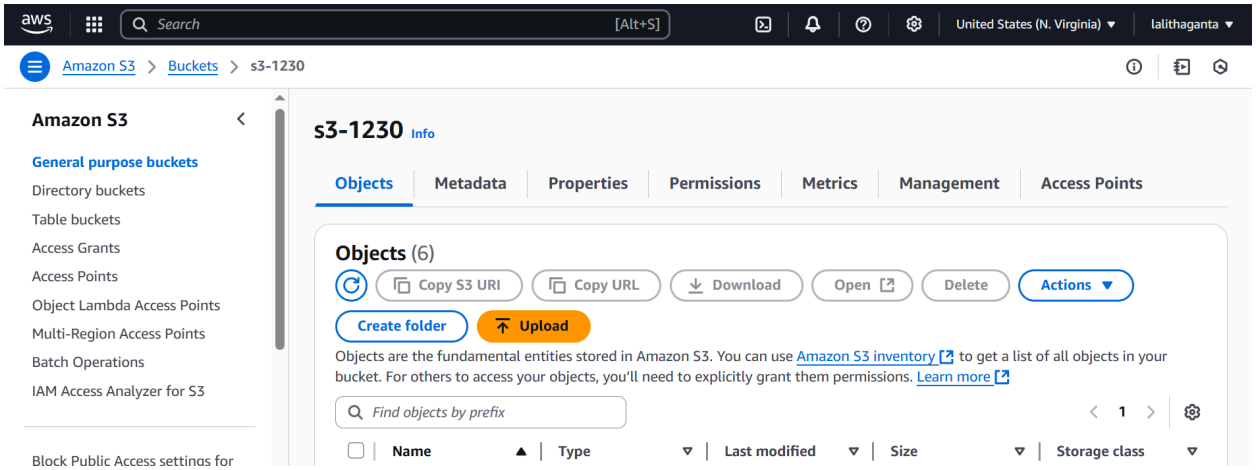

aws
Search
[Alt+S]
Europe (Stockholm)
lalithaganta
Amazon S3 > Buckets > lalithabucket-02 > Replication rules > Create replication rule
Replication). You can also specify a different bucket for each rule in the configuration. Learn more or see Amazon S3 pricing
Choose a bucket in this account
Specify a bucket in another account
Bucket name
Choose the bucket that will receive replicated objects.
lalithabucket-03
Browse S3
Destination Region
US East (Ohio) us-east-2
IAM role
Permission to access the specified resources
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.
Type here to search
36°C Sunny
ENG
21:02
14/05/2025

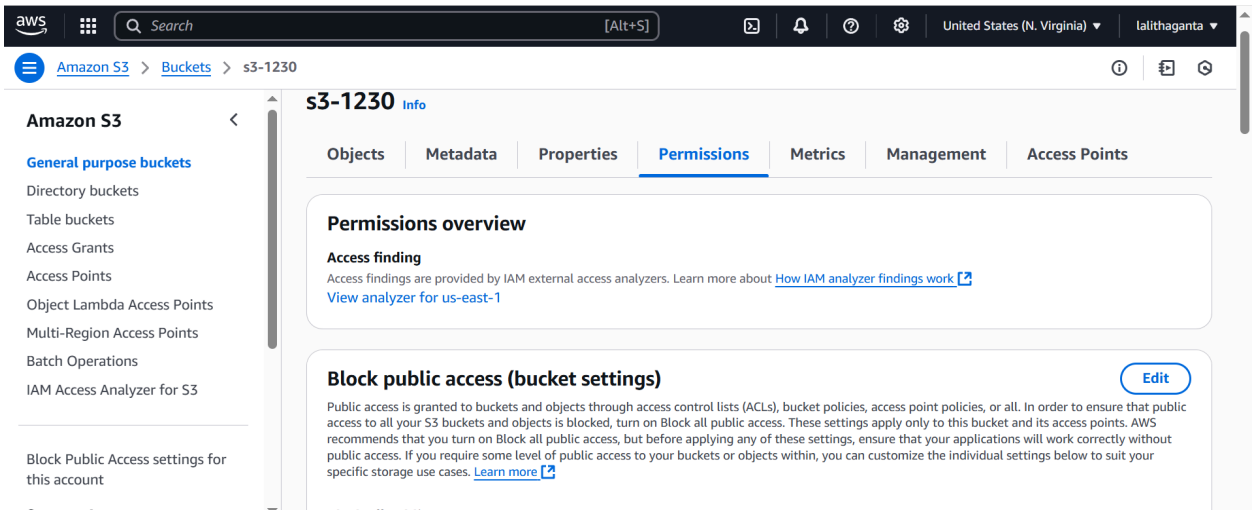
aws
Search
[Alt+S]
Europe (Stockholm)
lalithaganta
Amazon S3 > Buckets > lalithabucket-02 > Replication rules > Create replication rule
Additional replication options
Replication Time Control (RTC)
Replication Time Control replicates 99.99% of new objects within 15 minutes and includes replication metrics. Additional fees will apply. Learn more
Replication metrics
With replication metrics, you can monitor the total number and size of objects that are pending replication, and the maximum replication time to the destination Region. You can also view and diagnose replication failures. CloudWatch metrics fees apply. Learn more or see Amazon CloudWatch pricing
To publish event notifications to a destination whenever replication events occur, set S3 event notifications or CloudWatch alarms before replication begins. Learn more
Delete marker replication
Delete markers created by S3 delete operations will be replicated. Delete markers created by lifecycle rules are not replicated. Learn more
Replica modification sync
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.
Type here to search
36°C Sunny
ENG
20:59
14/05/2025

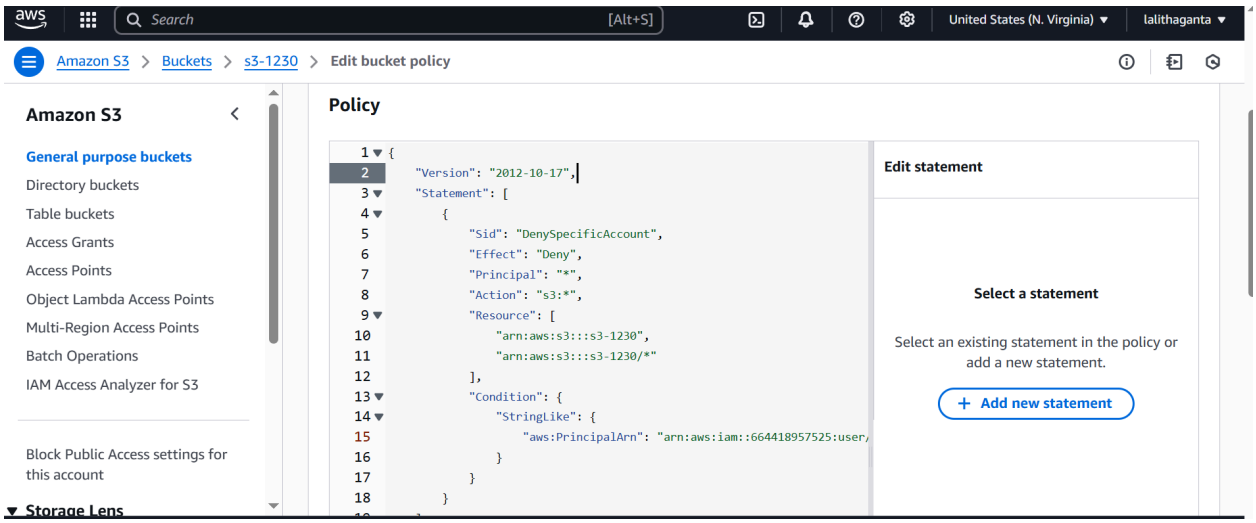


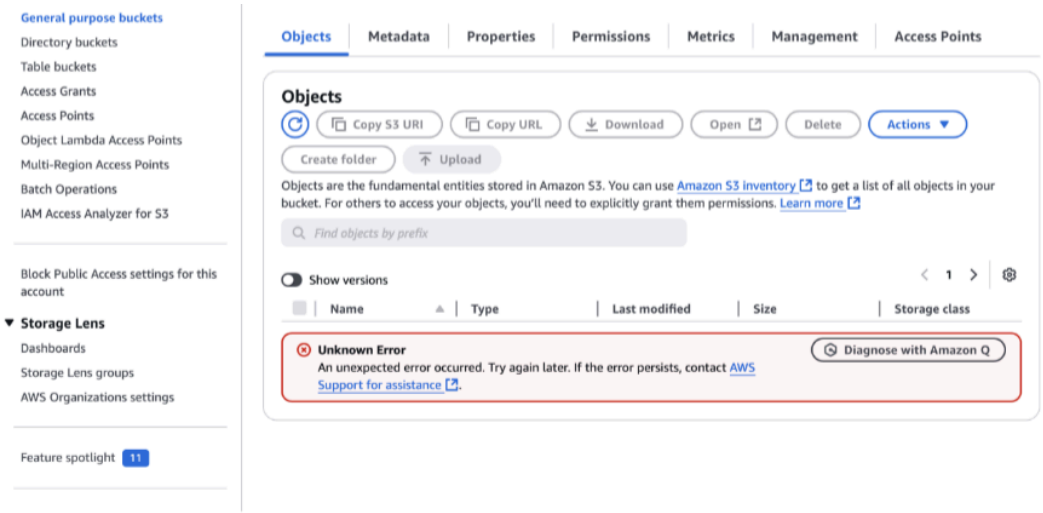


4) Configure bucket policy,only Admin user can see the objects of s3 bucket.


aws
Search
[Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > s3-1230
Amazon S3
General purpose buckets
Directory buckets
Table 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
s3-1230 Info
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Objects (6)
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

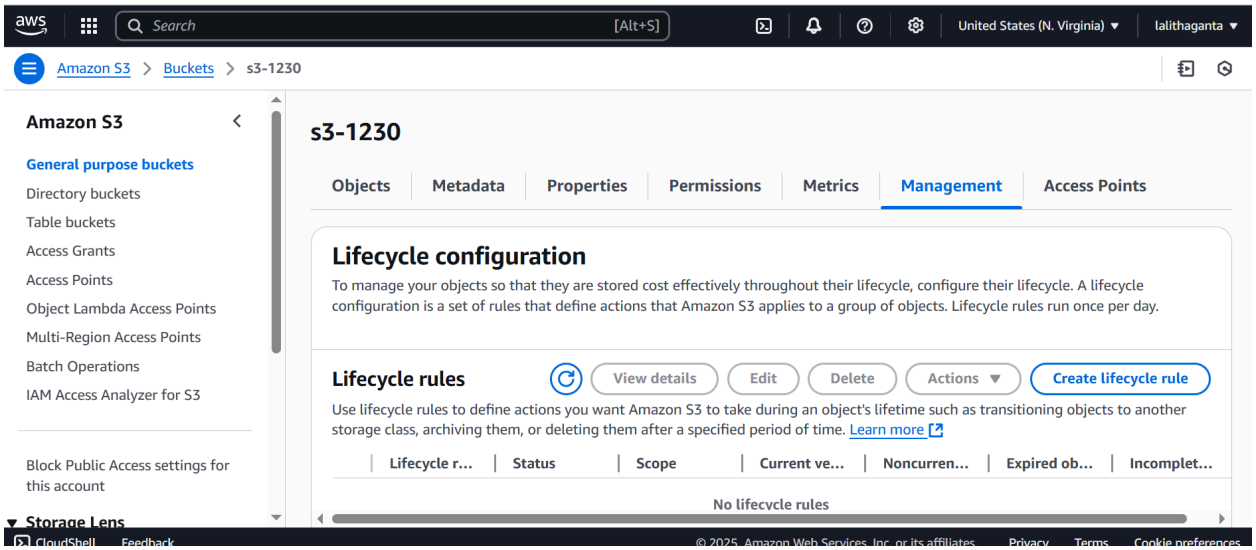

aws
Search
[Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > s3-1230
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
s3-1230 Info
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access finding
Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work
View analyzer for us-east-1
Block public access (bucket settings)
Edit
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

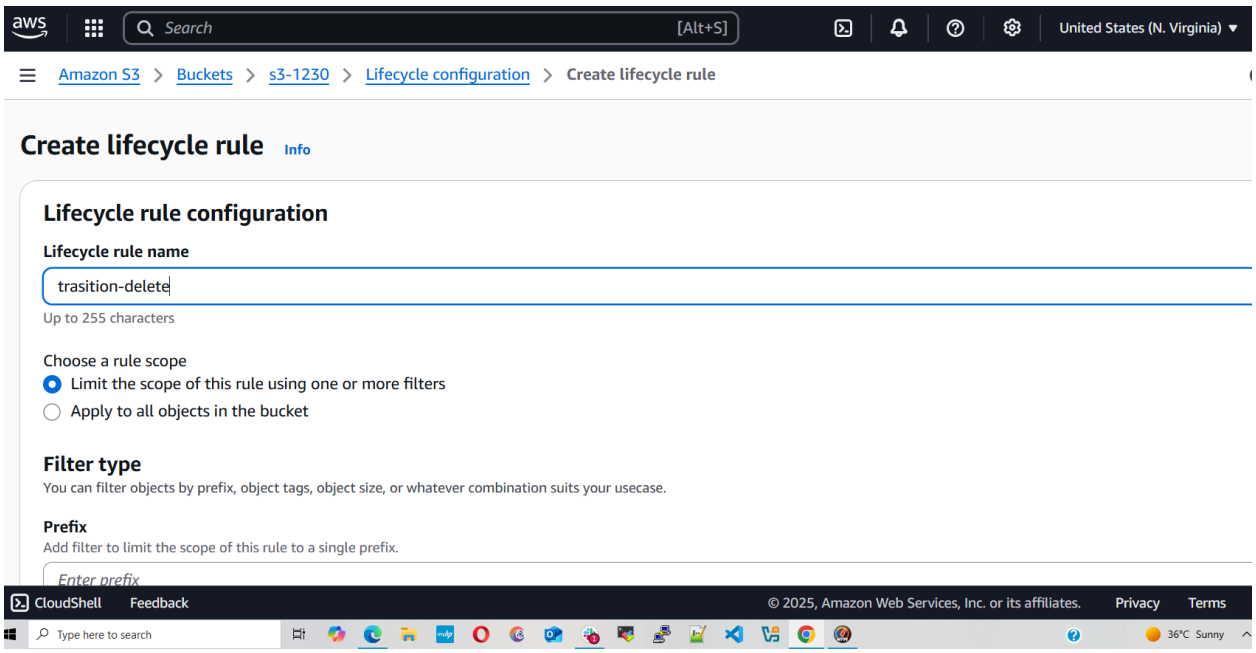

aws
Search
[Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > s3-1230 > Edit bucket policy
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Policy
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "DenySpecificAccount",
"Effect": "Deny",
"Principal": "*",
"Action": "s3:*",
"Resource": [
"arn:aws:s3:::s3-1230",
"arn:aws:s3:::s3-1230/*"
],
"Condition": {
"StringLike": {
"aws:PrincipalArn": "arn:aws:iam::664418957525:user/
}
}
}
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement

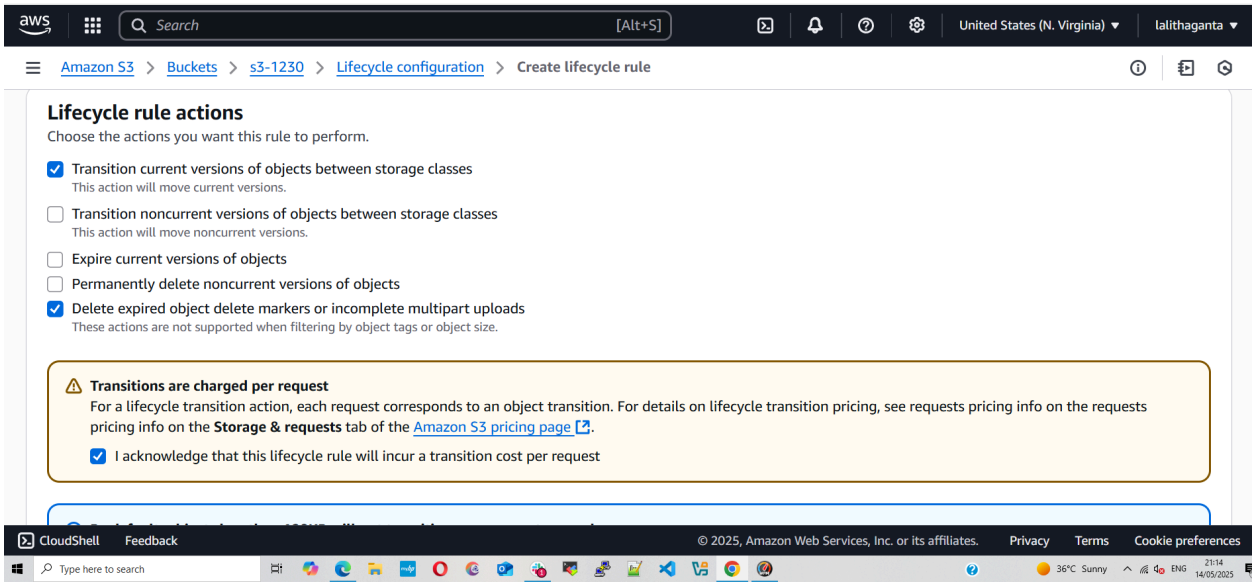


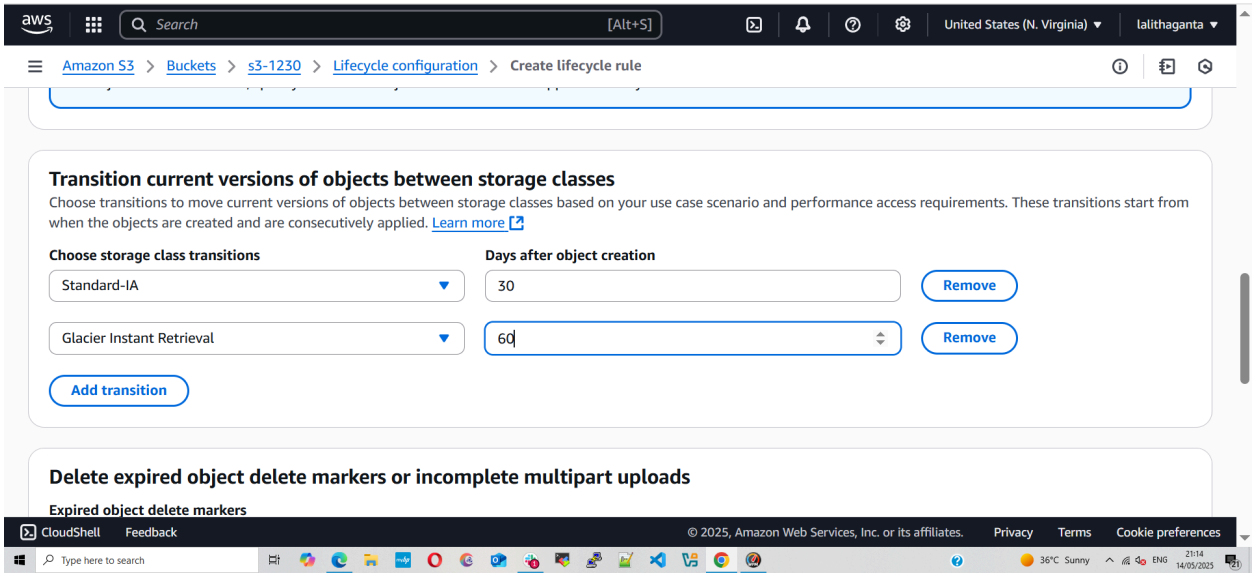
5) Setup lifecycle policies to automatically transition or delete objects based on specific criteria.

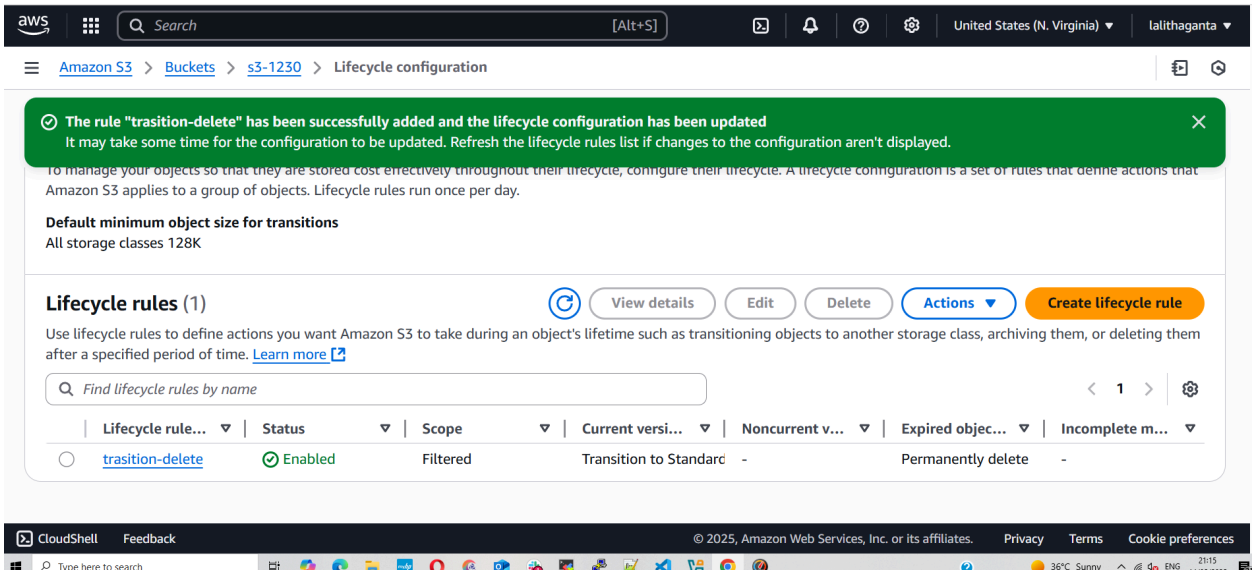
Go to Your S3 Bucket
Open the AWS Management Console
Navigate to S3 and select the bucket where you want to set the lifecycle
Policy. Go to the Management Tab
Click on the “Management” tab.
Scroll to “Lifecycle rules”
Click “Create lifecycle rule”
Configure Rule Name and Scope
Name your rule (e.g. archive-older-than-30-days).
choose whether this rule applies to:


Search [Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > s3-1230
Amazon S3
General purpose buckets
Directory buckets
Table 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
s3-1230
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Lifecycle configuration
To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.
Lifecycle rules
View details
Edit
Delete
Actions
Create lifecycle rule
Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. Learn more
Lifecycle r...
Status
Scope
Current ve...
Noncurren...
Expired ob...
Incomplet...
No lifecycle rules
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
United States (N. Virginia)
Amazon S3 > Buckets > s3-1230 > Lifecycle configuration > Create lifecycle rule
Create lifecycle rule Info
Lifecycle rule configuration
Lifecycle rule name
trasition-delete
Up to 255 characters
Choose a rule scope
Limit the scope of this rule using one or more filters
Apply to all objects in the bucket
Filter type
You can filter objects by prefix, object tags, object size, or whatever combination suits your usecase.
Prefix
Add filter to limit the scope of this rule to a single prefix.
Enter prefix
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Type here to search
36°C Sunny


aws
Search
[Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > s3-1230 > Lifecycle configuration > Create lifecycle rule
Lifecycle rule actions
Choose the actions you want this rule to perform.
Transition current versions of objects between storage classes
This action will move current versions.
Transition noncurrent versions of objects between storage classes
This action will move noncurrent versions.
Expire current versions of objects
Permanently delete noncurrent versions of objects
Delete expired object delete markers or incomplete multipart uploads
These actions are not supported when filtering by object tags or object size.
Transitions are charged per request
For a lifecycle transition action, each request corresponds to an object transition. For details on lifecycle transition pricing, see requests pricing info on the requests pricing info on the Storage & requests tab of the Amazon S3 pricing page.
I acknowledge that this lifecycle rule will incur a transition cost per request
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
36°C Sunny
ENG
21:14
14/05/2025


aws
Search
[Alt+S]
United States (N. Virginia)
lalithaganta
Amazon S3 > Buckets > s3-1230 > Lifecycle configuration > Create lifecycle rule
Transition current versions of objects between storage classes
Choose transitions to move current versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects are created and are consecutively applied. Learn more
Choose storage class transitions
Days after object creation
Standard-IA
30
Remove
Glacier Instant Retrieval
60
Remove
Add transition
Delete expired object delete markers or incomplete multipart uploads
Expired object delete markers
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
36°C Sunny
ENG
21:14
14/05/2025

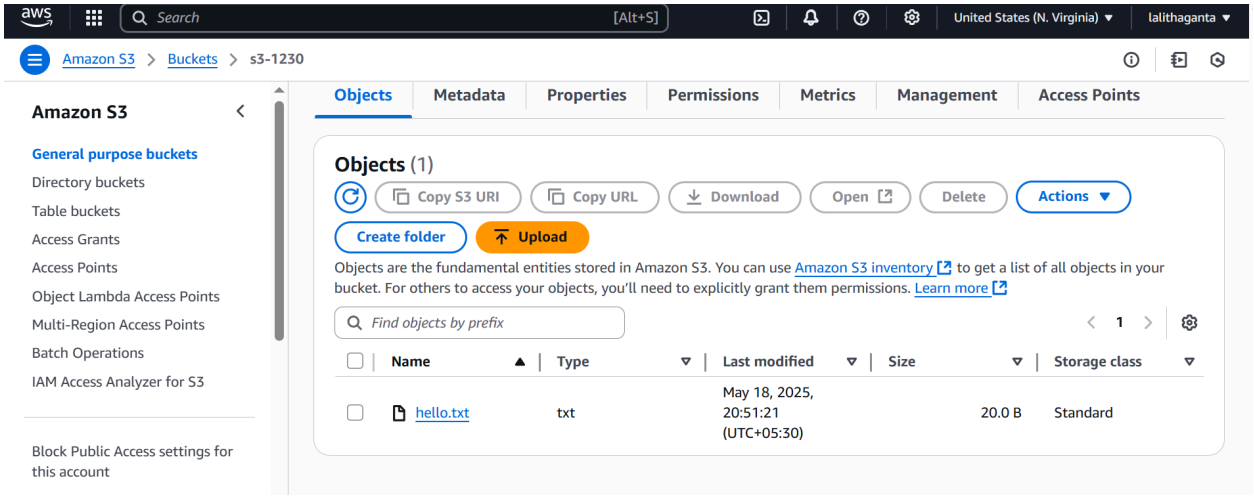


6) Push some objects in s3 using AWS CLI.

Create a sample file
Bash CopyEdit
echo
"Hello from lalitha" > hello.txt
Upload the file to your S3 bucket:
aws s3 cp testfile.txt s3://s3-1230/
Upload a folder recursively:
aws s3 cp ./samplefolder/ s3-1230 --recursive

```
HP@LAPTOP-LPTR344H MINGW64 ~ (main)
$ aws --version
aws-cli/1.40.12 Python/3.12.6 Windows/10 botocore/1.38.13

HP@LAPTOP-LPTR344H MINGW64 ~ (main)
$ aws configure
AWS Access Key ID [****************Q2NV]: AKIAZVMTUXDKTNHZ3COU
AWS Secret Access Key [****************f1tA]: 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
Default region name [eu-north-1]: eu-north-1
Default output format [json]: json

HP@LAPTOP-LPTR344H MINGW64 ~ (main)
$
```

```
HP@LAPTOP-LPTR344H MINGW64 ~/Downloads (master)
$ pwd
/c/Users/HP/Downloads

HP@LAPTOP-LPTR344H MINGW64 ~/Downloads (master)
$ echo "Hello from lalitha!" > hello.txt

HP@LAPTOP-LPTR344H MINGW64 ~/Downloads (master)
$ aws s3 cp hello.txt s3://s3-1230/
upload: .\hello.txt to s3://s3-1230/hello.txt

HP@LAPTOP-LPTR344H MINGW64 ~/Downloads (master)
$
```



7) Write a bash script to create s3 bucket.

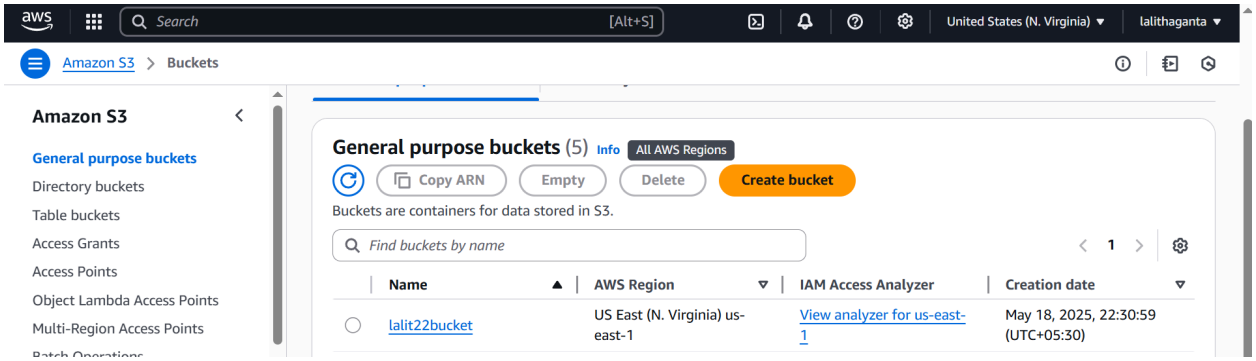
Save the code as create_s3_bucket.sh
Give permissions : chmod +x create_s3_bucket.sh
Run as ./create_s3_bucket.sh

```
#!/bin/bash
# Check if bucket name is provided
if [ -z "$1" ]; then
  echo "Usage: $0 <bucket-name>"
  exit 1
fi
BUCKET_NAME=$1
REGION="us-east-1"
# Create the S3 bucket
echo "Creating S3 bucket: $BUCKET_NAME in region $REGION"
aws s3api create-bucket --bucket "$BUCKET_NAME" --region "$REGION"
--create-bucket-configuration LocationConstraint="$REGION"
# Check exit status
if [ $? -eq 0 ]; then
  echo " S3 bucket \"$BUCKET_NAME\" created successfully."
else
  echo " Failed to create S3 bucket \"$BUCKET_NAME\"."
  exit 1
fi
```

MINGW64:/c/Users/HP/OneDrive/Desktop

```
#!/bin/bash

# Set the bucket name and region
BUCKET_NAME="lalit22bucket"
REGION="us-east-1"

# Step 1: Show what we're doing
echo "Creating bucket: $BUCKET_NAME in region: $REGION"

# Step 2: Confirm action
read -p "Proceed? (y/n): " CONFIRM
if [[ "$CONFIRM" != "y" ]]; then
  echo "Operation cancelled."
  exit 1
fi

# Step 3: Create the bucket
if [ "$REGION" == "us-east-1" ]; then
  aws s3api create-bucket \
    --bucket "$BUCKET_NAME" \
    --region "$REGION"
else
  aws s3api create-bucket \
    --bucket "$BUCKET_NAME" \
    --region "$REGION" \
    --create-bucket-configuration LocationConstraint="$REGION"
fi

# Step 4: Check if bucket creation succeeded
if [ $? -eq 0 ]; then
  echo "✅ Bucket '$BUCKET_NAME' created successfully."
else
  echo "❌ Failed to create bucket '$BUCKET_NAME'. Check your permissions or try a different name."
fi
~
~
```

```
MINGW64:/c/Users/HP/OneDrive/Desktop
HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop (main)
$ aws --version
aws-cli/1.40.12 Python/3.12.6 Windows/10 botocore/1.38.13

HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop (main)
$ aws configure
AWS Access Key ID [****************JSUL]: AKIAZVMTUXDK44BKJSUL

AWS Secret Access Key [****************DBDO]:
Default region name [eu-north-1]:
Default output format [json]:


HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop (main)
$

HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop (main)
$

HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop (main)
$ vi create_s3_bucket.sh

HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop (main)
$ chmod +x create_s3_bucket.sh

HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop (main)
$ ./create_s3_bucket.sh
Creating bucket: lalit22bucket in region: us-east-1
Proceed? (y/n): y
{
    "Location": "/lalit22bucket"
}
✅ Bucket 'lalit22bucket' created successfully.
```



8) Upload one 1 gb of file to s3 using cli.

```
HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop/Devops (main)
$ aws s3 cp test s3://s3-1230/ --recursive
upload: test\02-Client-server-Architecture (1) - Copy.mp4 to s3://s3-1230/02-Client-server-Architecture (1) - Copy.mp4
upload: test\01-Devops_Introduction (1).mp4 to s3://s3-1230/01-Devops_Introduction (1).mp4
upload: test\04-Linux-basics (1).mp4 to s3://s3-1230/04-Linux-basics (1).mp4
upload: test\03-Linux-basics (1).mp4 to s3://s3-1230/03-Linux-basics (1).mp4
upload: test\05-Linux-basics (1).mp4 to s3://s3-1230/05-Linux-basics (1).mp4

HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop/Devops (main)
$
```