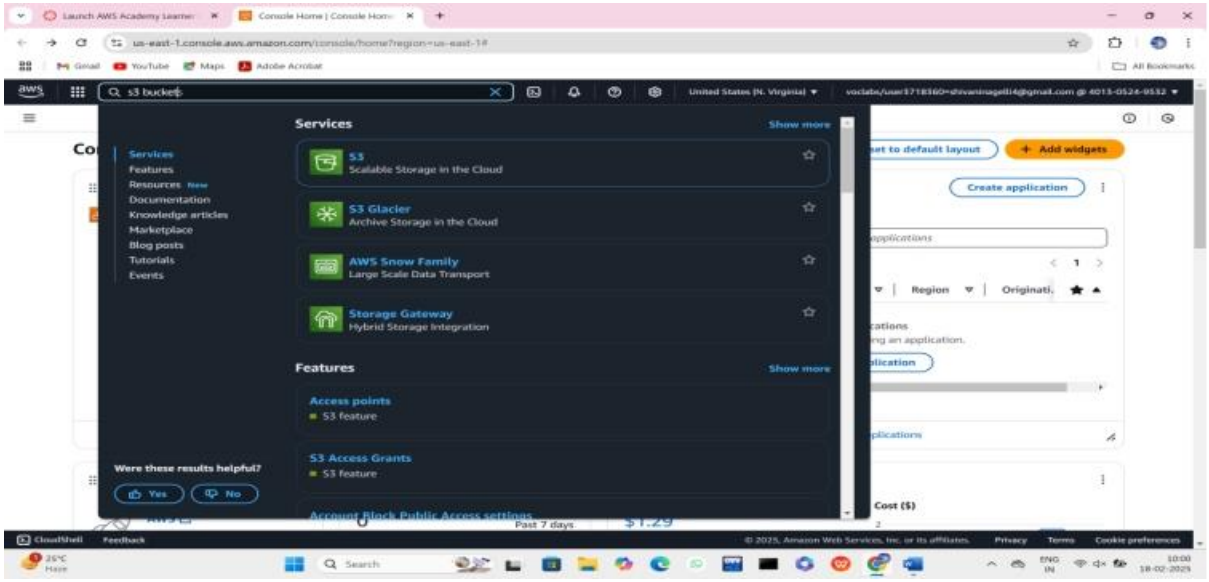
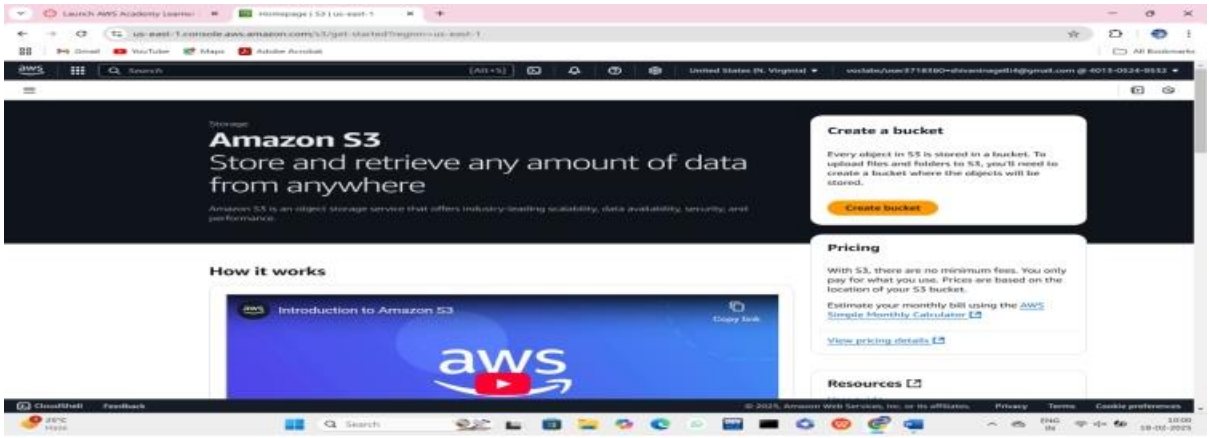
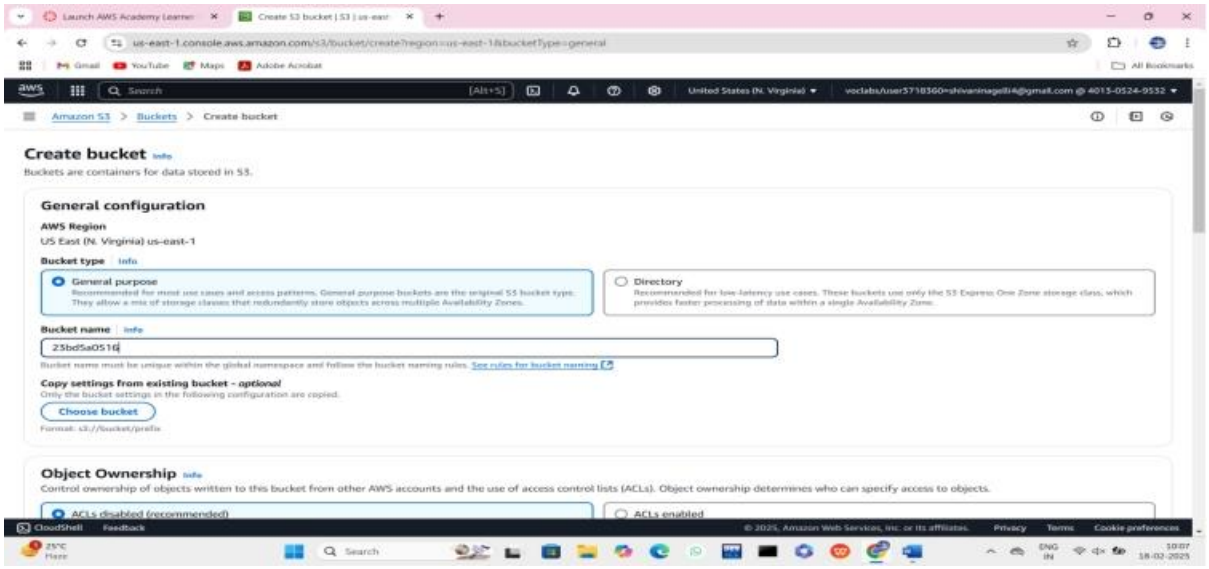
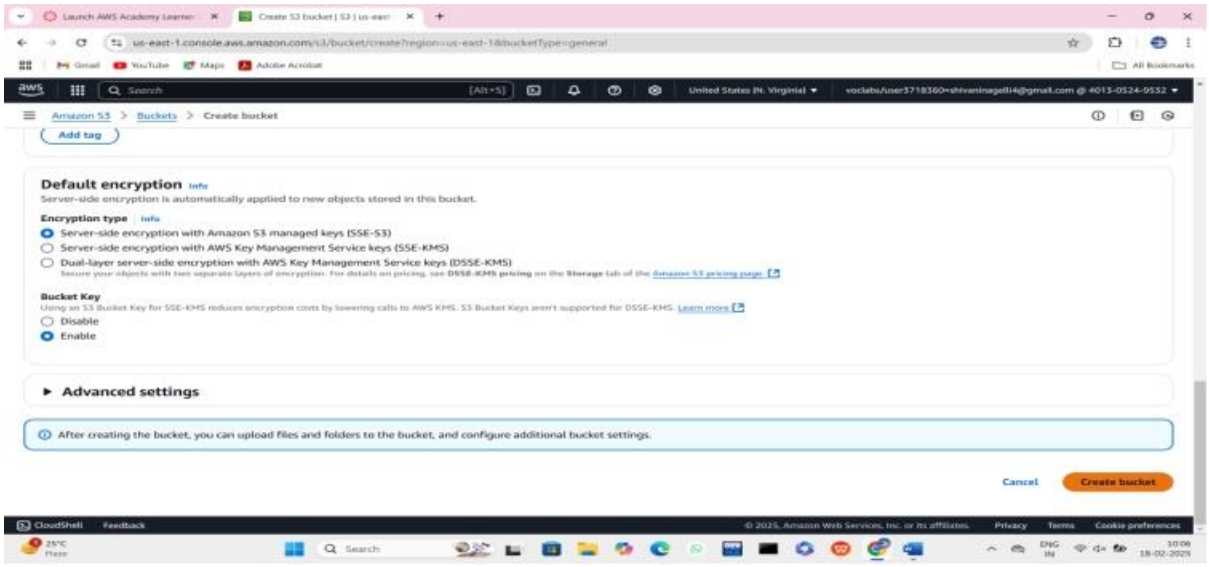
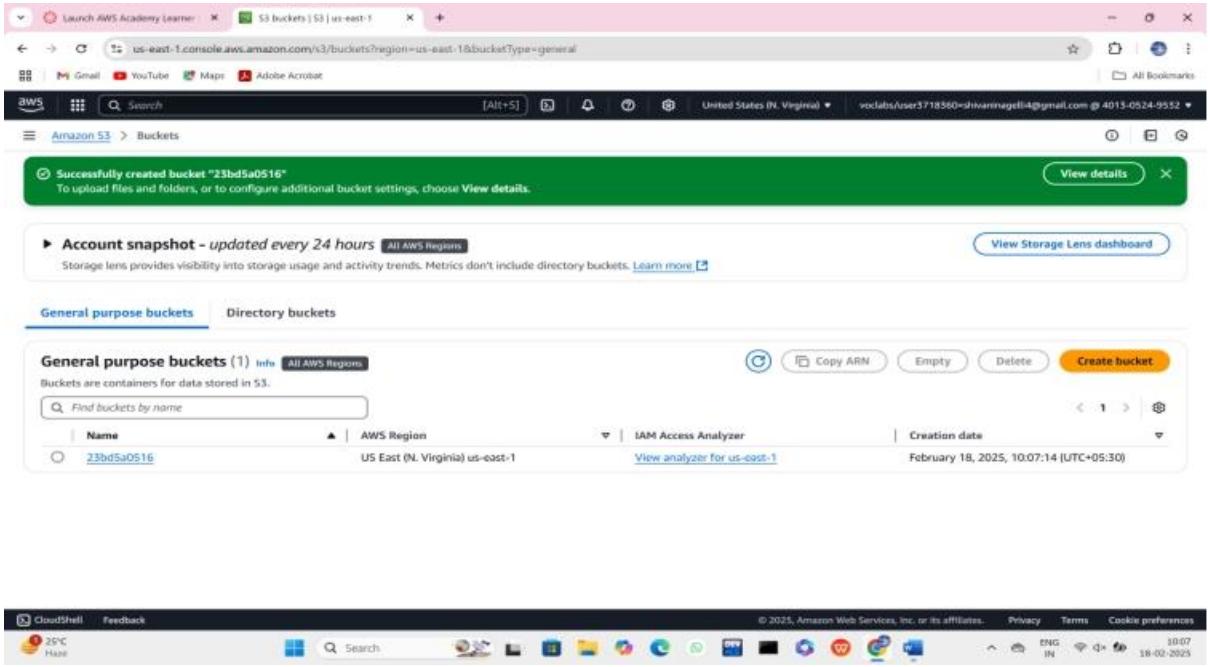
CREATION OF S3 BUCKET:

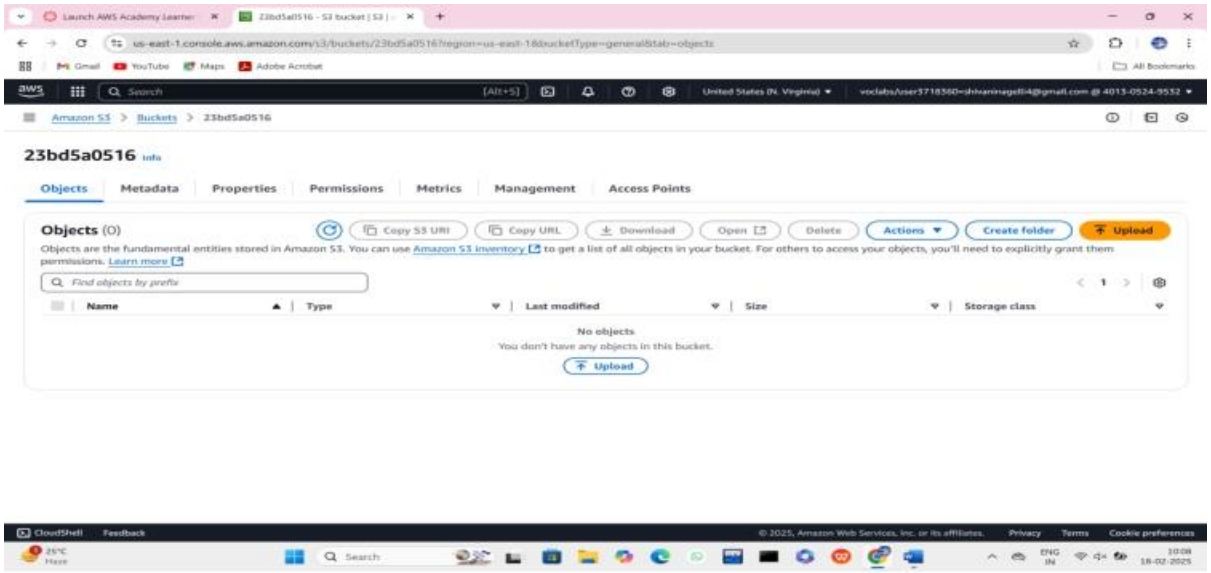


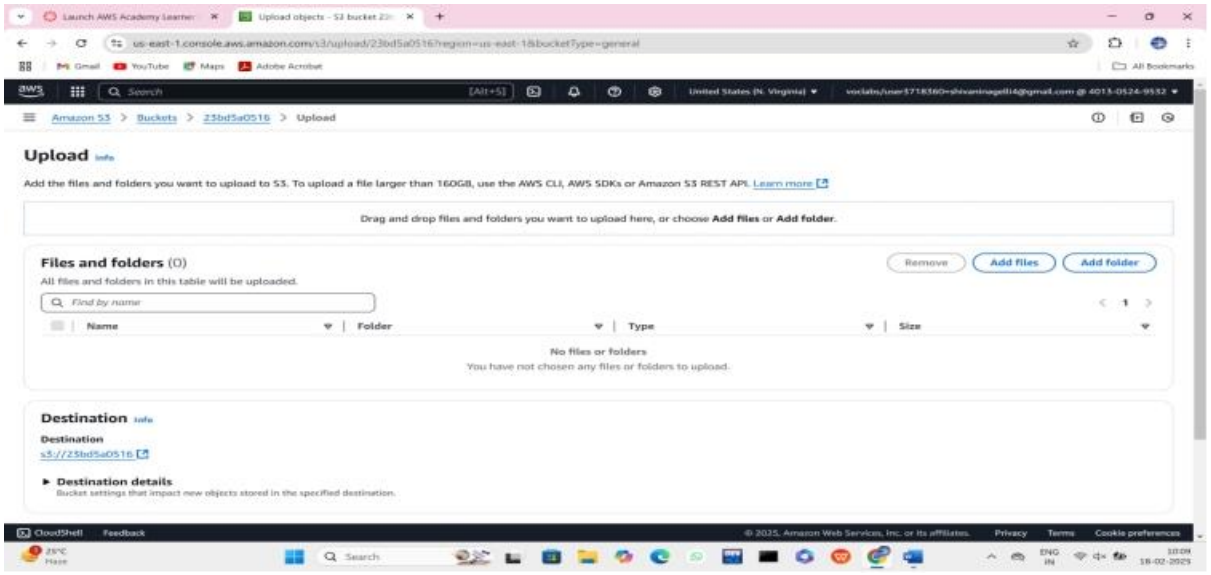


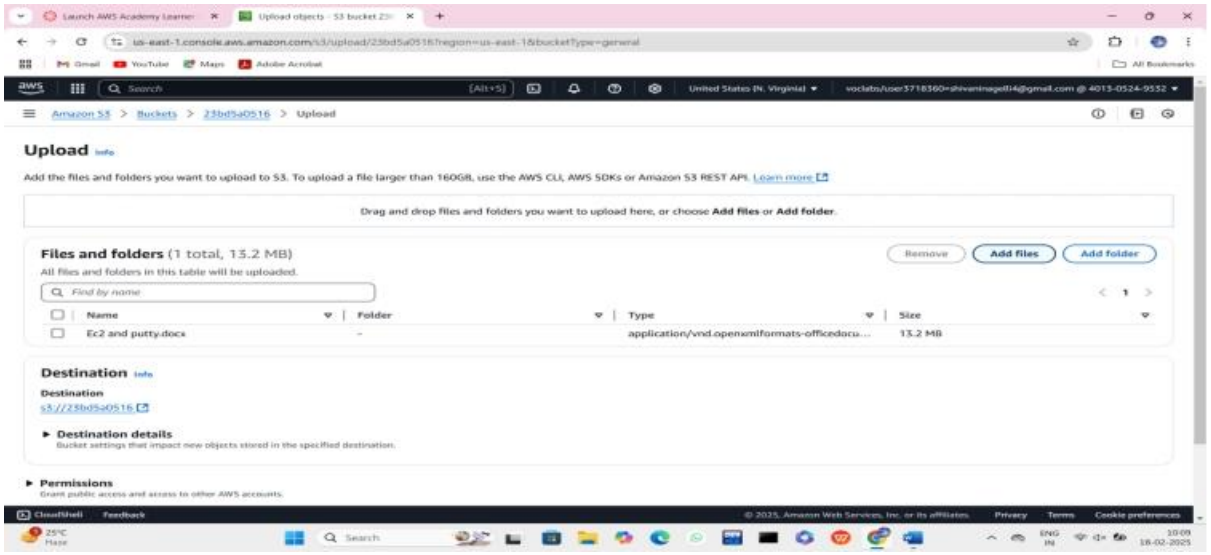


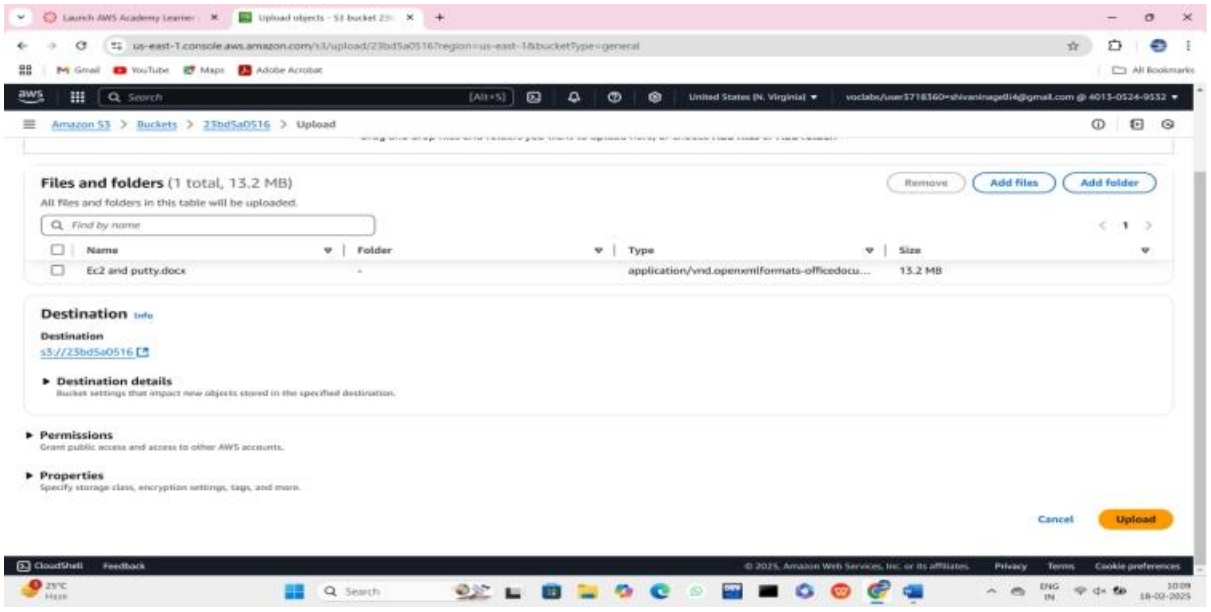

Amazon S3 > Buckets > Create bucket
Add tag
Default encryption Info
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Bucket Key
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

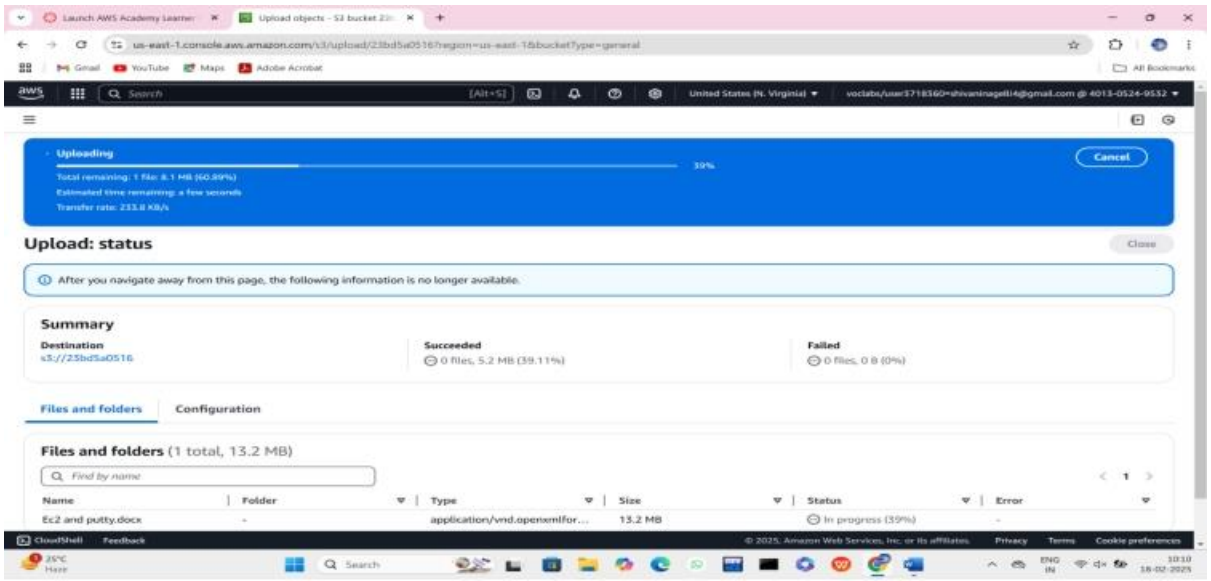

Amazon S3 > Buckets
Successfully created bucket "23bd5a0516"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Metrics 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
23bd5a0516
US East (N. Virginia) us-east-1
View analyzer for us-east-1
February 18, 2025, 10:07:14 (UTC+05:30)

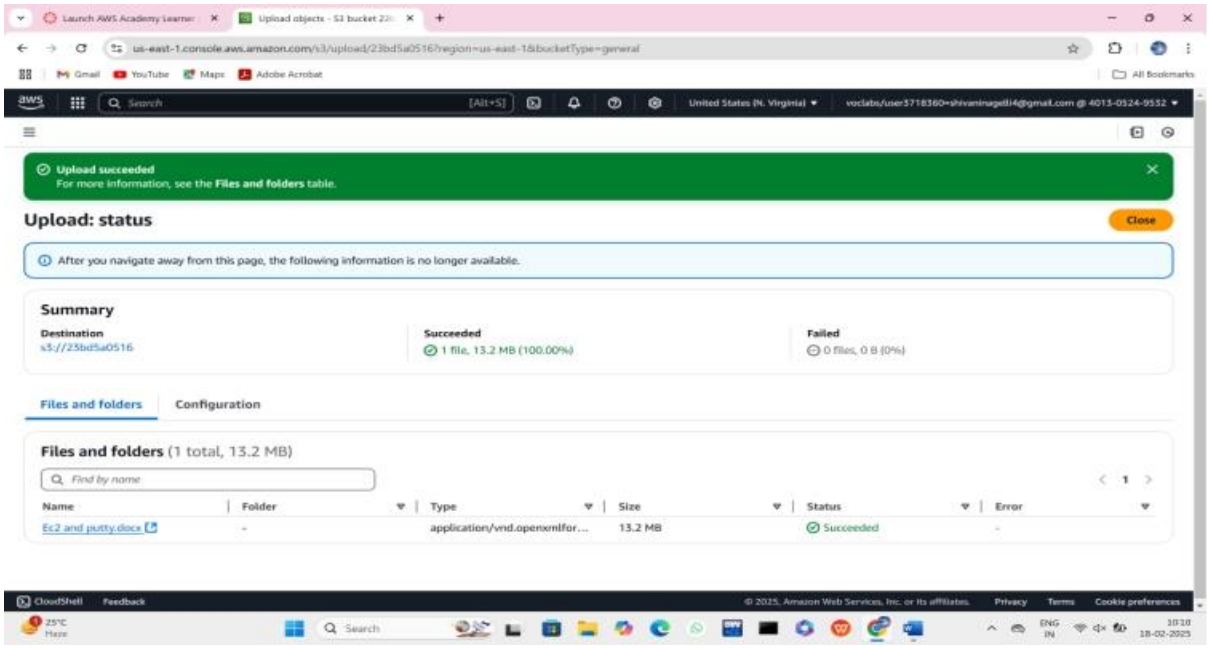

Launch AWS Academy Learner
23bd5a0516 - S3 bucket | S3
us-east-1.console.aws.amazon.com/s3/buckets/23bd5a0516?region=us-east-1&bucketType=general&tab=objects
Gmail
YouTube
Maps
Adobe Acrobat
All Bookmarks
Search
[Alt+S]
United States (N. Virginia)
Amazon S3 > Buckets > 23bd5a0516
23bd5a0516 Info
Objects
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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search

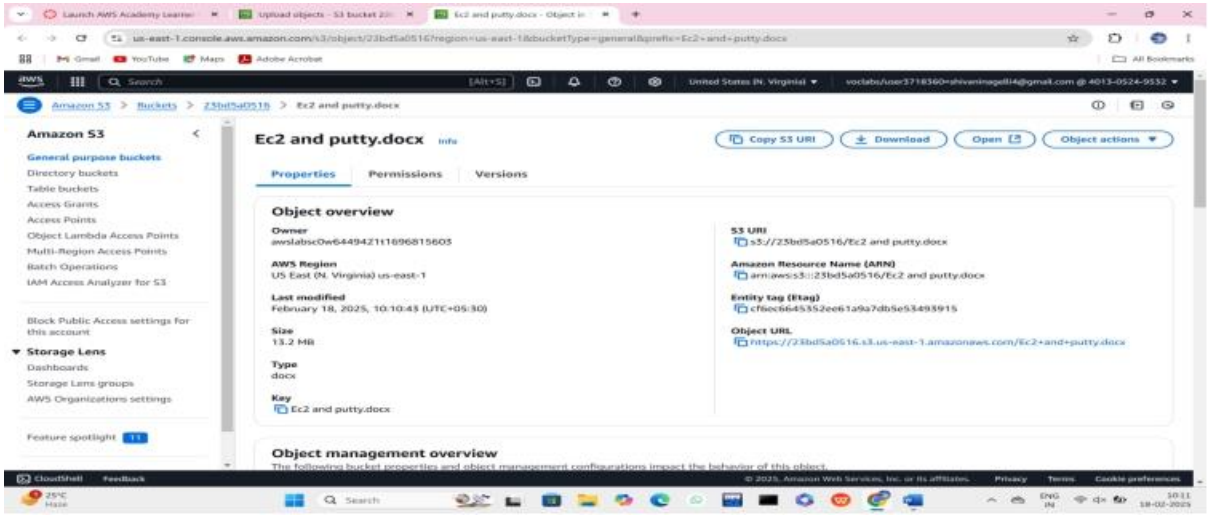

Launch AWS Academy Learner
Upload objects - S3 bucket 23b
us-east-1.console.aws.amazon.com/s3/upload/23bd5a0516?region=us-east-1&bucketType=general
Gmail
YouTube
Maps
Adobe Acrobat
All Bookmarks
Search
[Alt+S]
United States (N. Virginia)
Amazon S3 > Buckets > 23bd5a0516 > Upload
Upload Info
Add the files 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 (0)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
Name
Folder
Type
Size
No files or folders
You have not chosen any files or folders to upload.
Destination Info
Destination
s3://23bd5a0516
Destination details
Bucket settings that impact new objects stored in the specified destination.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search


Upload
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, 13.2 MB)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
Name
Folder
Type
Size
Ec2 and putty.docx
application/vnd.openxmlformats-officedocu...
13.2 MB
Destination
Destination
s3://23bd5a0516
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.

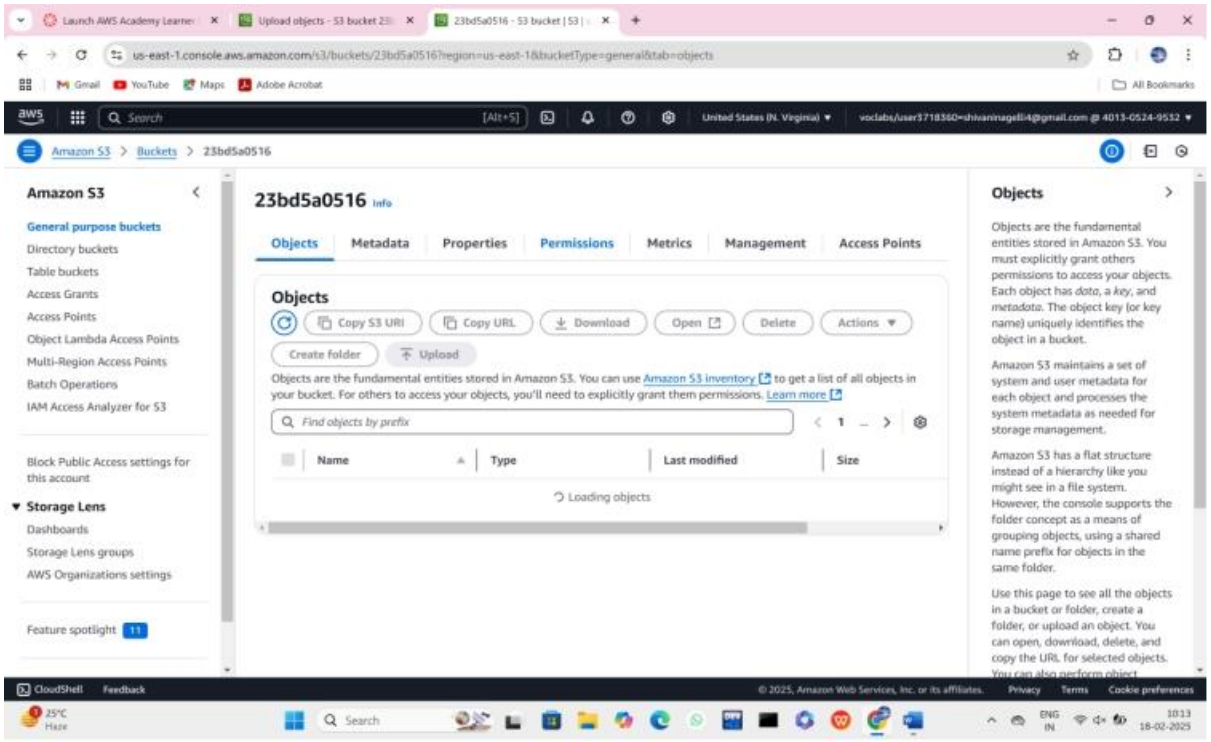

Files and folders (1 total, 13.2 MB)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
Name
Folder
Type
Size
Ec2 and putty.docx
application/vnd.openxmlformats-officedocu...
13.2 MB
Destination
Destination
s3://23bd5a0516
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Properties
Specify storage class, encryption settings, tags, and more.
Cancel
Upload

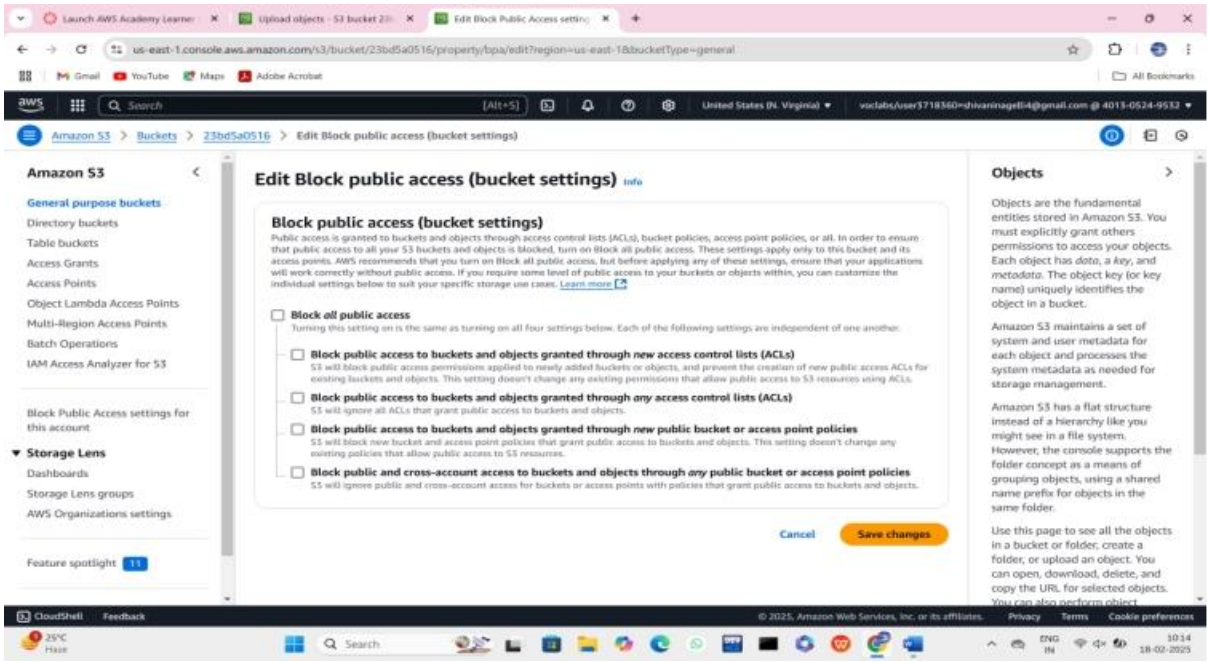

Uploading
Total remaining: 1 file: 8.1 MB (60.89%)
Estimated time remaining: a few seconds
Transfer rate: 233.8 KB/s
39%
Cancel
Upload: status
Close
After you navigate away from this page, the following information is no longer available.
Summary
Destination
s3://23bd5a0516
Succeeded
0 files, 5.2 MB (39.11%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 total, 13.2 MB)
Find by name
Name
Folder
Type
Size
Status
Error
Ec2 and putty.docx
application/vnd.openxmlfor...
13.2 MB
In progress (39%)

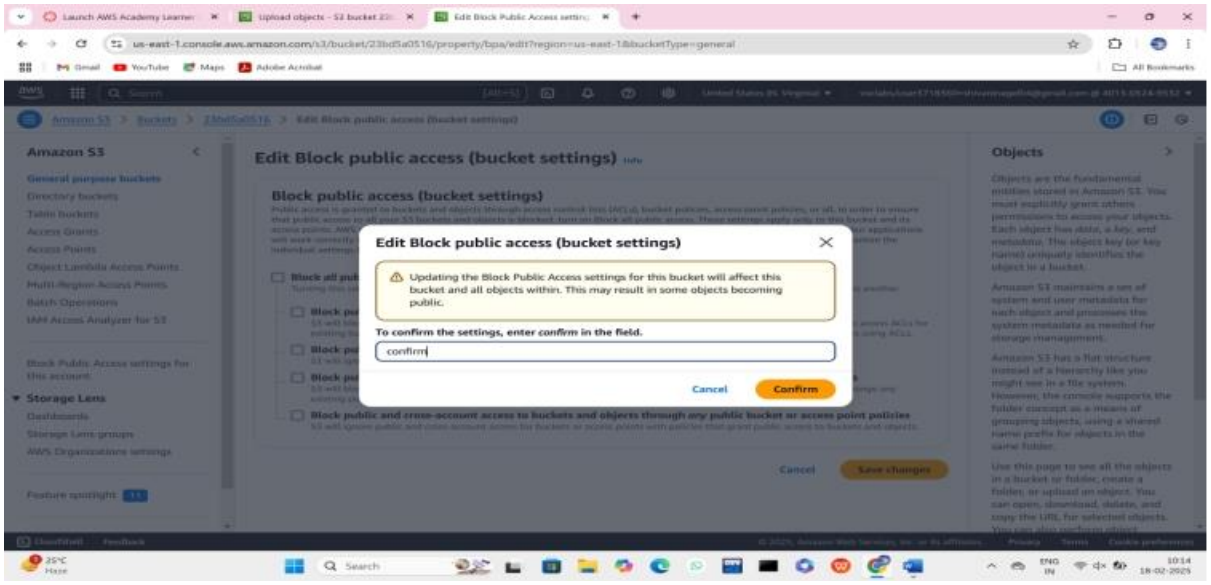

Upload succeeded
For more information, see the Files and folders table.
Upload: status
Close
After you navigate away from this page, the following information is no longer available.
Summary
Destination
s3://23bd5a0516
Succeeded
1 file, 13.2 MB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 total, 13.2 MB)
Find by name
Name
Folder
Type
Size
Status
Error
Ec2 and putty.docx
application/vnd.openxmlfor...
13.2 MB
Succeeded

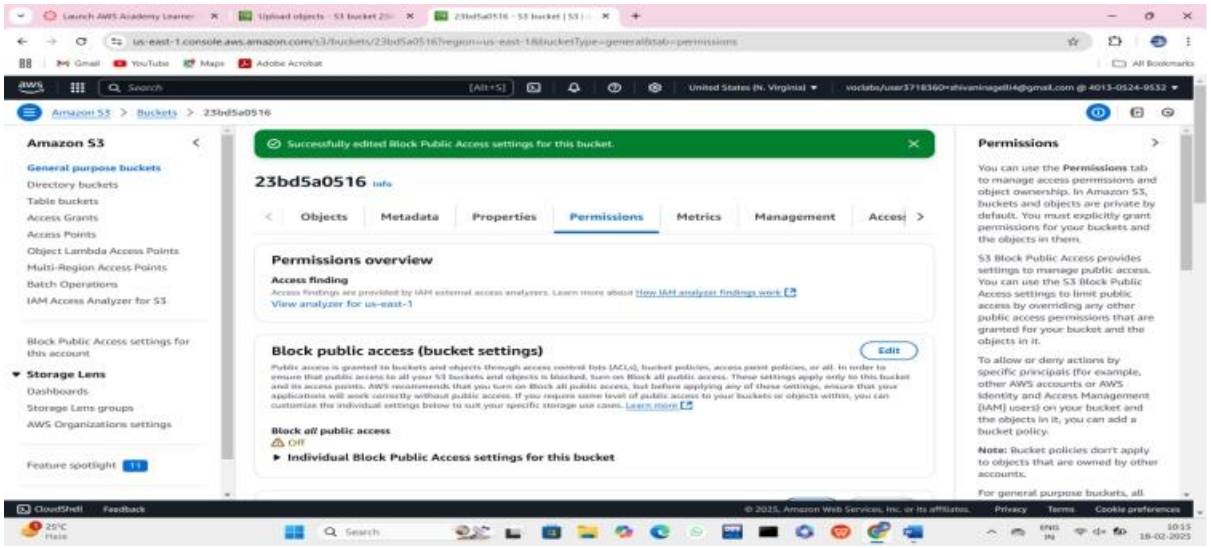

Amazon S3
Buckets
23bd5a0516
Ec2 and putty.docx
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
Ec2 and putty.docx
Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
awslabscOw6449421t1696815603
AWS Region
US East (N. Virginia) us-east-1
Last modified
February 18, 2025, 10:10:43 (UTC+05:30)
Size
13.2 MB
Type
docx
Key
Ec2 and putty.docx
S3 URI
s3://23bd5a0516/Ec2 and putty.docx
Amazon Resource Name (ARN)
arn:aws:s3:::23bd5a0516/Ec2 and putty.docx
Entity tag (Etag)
cf6ec6645352ee61a9a7db5e53493915
Object URL
https://23bd5a0516.s3.us-east-1.amazonaws.com/Ec2+and+putty.docx
Object management overview

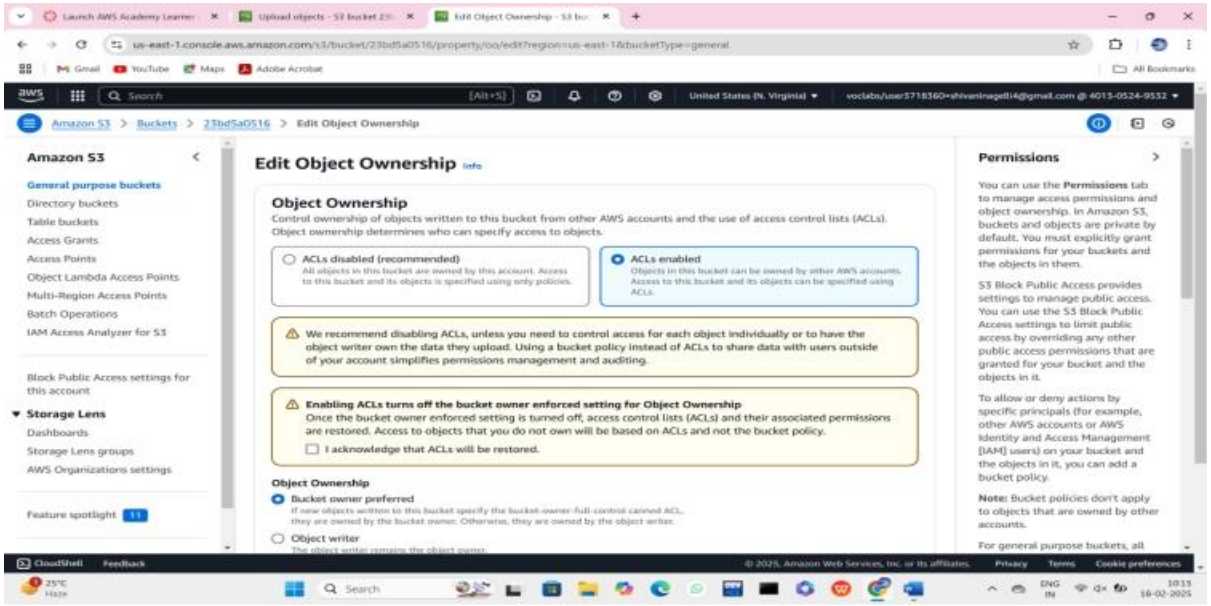

23bd5a0516.s3.us-east-1.amazonaws.com/Ec2+and+putty.docx
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>CBMK3MXNNRRV7X7MM</RequestId>
<HostId>uuBYwznZUC/XroOD7EuZeTL2DFozpqP+wp/K1wKKoXBjxkPoRtB9YZX4mA7CLgEl1P8LElq38Q=</HostId>
</Error>

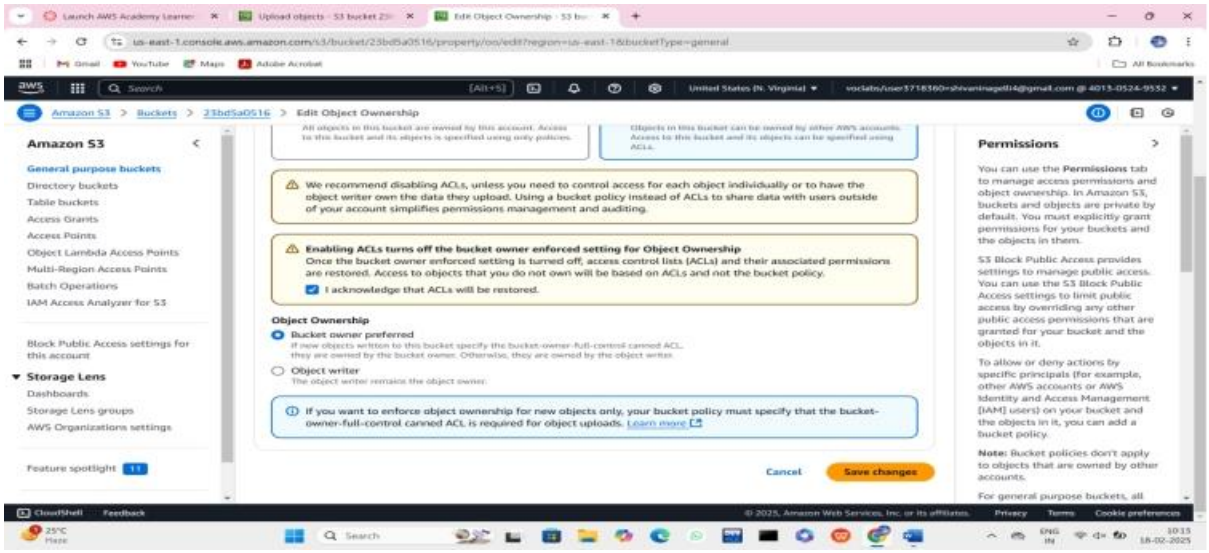

Launch AWS Academy Learner
Upload objects - S3 bucket 23
23bd5a0516 - S3 bucket | S3 |
us-east-1.console.aws.amazon.com/s3/buckets/23bd5a0516?region=us-east-1&bucketType=general&tab=objects
Gmail
YouTube
Maps
Adobe Acrobat
All Bookmarks
Search
[Alt+S]
United States (N. Virginia)
Amazon S3 > Buckets > 23bd5a0516
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
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 11
23bd5a0516 Info
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Objects
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
Loading objects
Objects are the fundamental entities stored in Amazon S3. You must explicitly grant others permissions to access your objects. Each object has data, a key, and metadata. The object key (or key name) uniquely identifies the object in a bucket.
Amazon S3 maintains a set of system and user metadata for each object and processes the system metadata as needed for storage management.
Amazon S3 has a flat structure instead of a hierarchy like you might see in a file system. However, the console supports the folder concept as a means of grouping objects, using a shared name prefix for objects in the same folder.
Use this page to see all the objects in a bucket or folder, create a folder, or upload an object. You can open, download, delete, and copy the URL for selected objects.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
10:13
18-02-2025

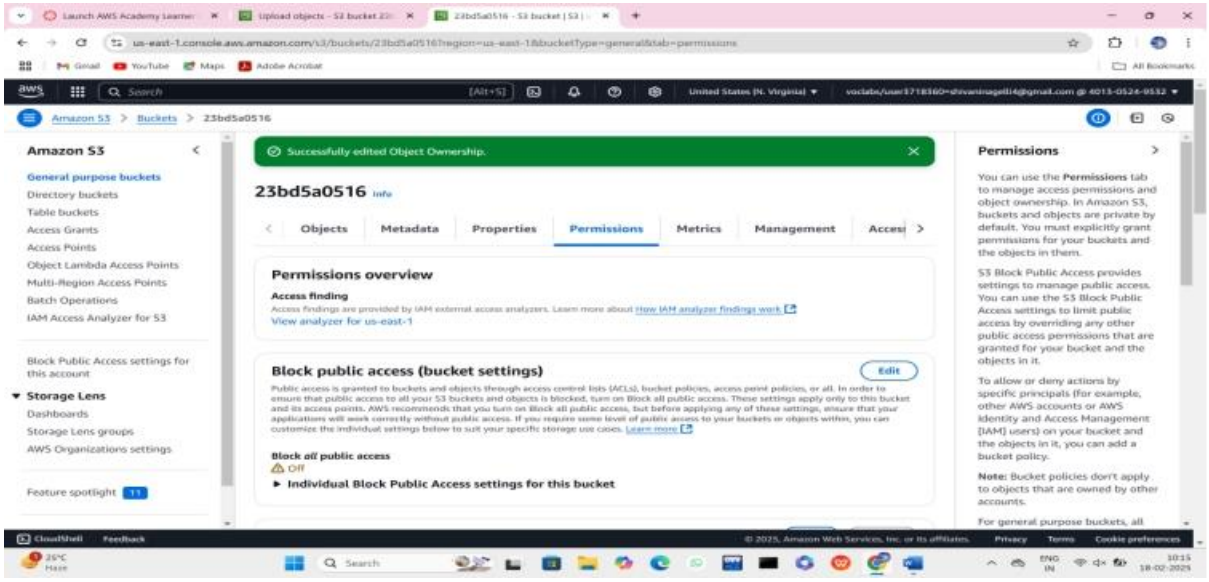

Launch AWS Academy Learner
Upload objects - S3 bucket 23
Edit Block Public Access settings
us-east-1.console.aws.amazon.com/s3/bucket/23bd5a0516/property/bpa/edit?region=us-east-1&bucketType=general
Amazon S3 > Buckets > 23bd5a0516 > Edit Block public access (bucket settings)
Edit Block public access (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
Objects are the fundamental entities stored in Amazon S3. You must explicitly grant others permissions to access your objects. Each object has data, a key, and metadata. The object key (or key name) uniquely identifies the object in a bucket.
Amazon S3 maintains a set of system and user metadata for each object and processes the system metadata as needed for storage management.
Amazon S3 has a flat structure instead of a hierarchy like you might see in a file system. However, the console supports the folder concept as a means of grouping objects, using a shared name prefix for objects in the same folder.
Use this page to see all the objects in a bucket or folder, create a folder, or upload an object. You can open, download, delete, and copy the URL for selected objects.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
ENG
IN
10:14
18-02-2025

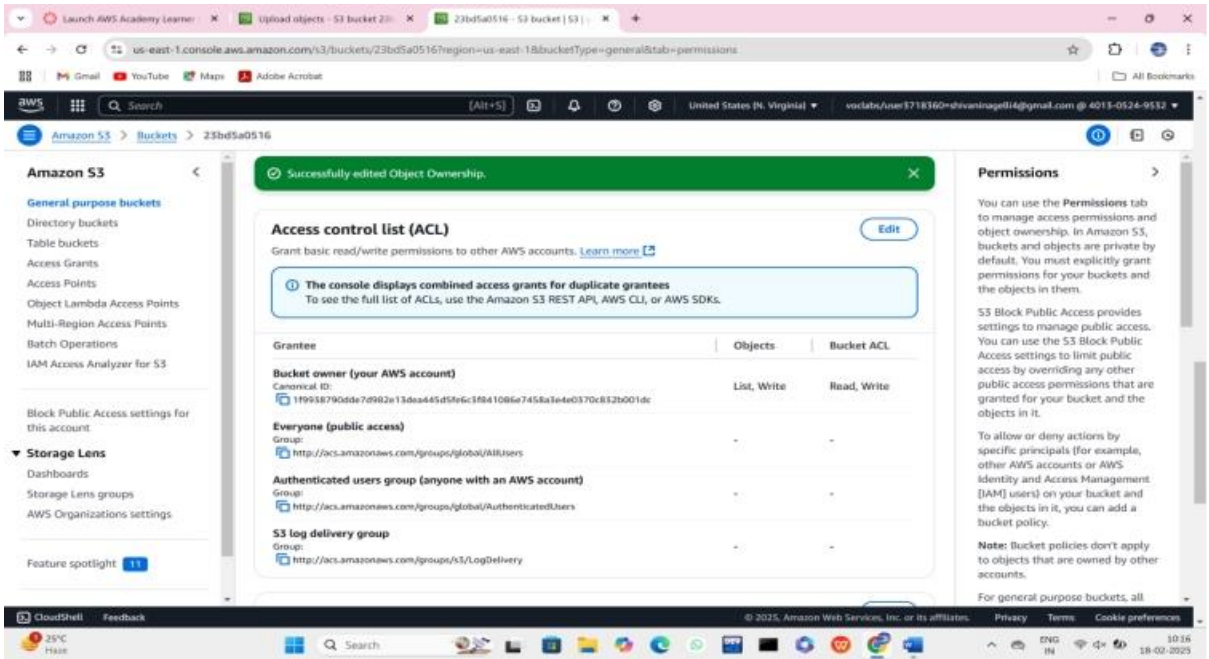

Edit Block public access (bucket settings)
Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.
To confirm the settings, enter confirm in the field.
confirm
Cancel
Confirm

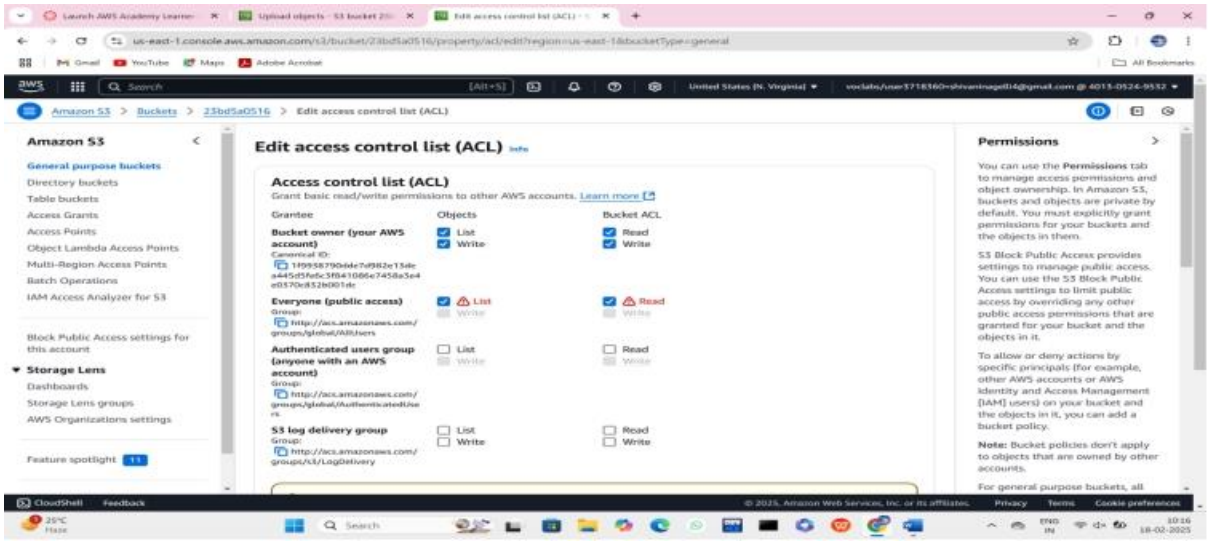

Successfully edited Block Public Access settings for this bucket.
23bd5a0516
Objects
Metadata
Properties
Permissions
Metrics
Management
Permissions overview
Block public access (bucket settings)
Edit
Block all public access
Off
Individual Block Public Access settings for this bucket

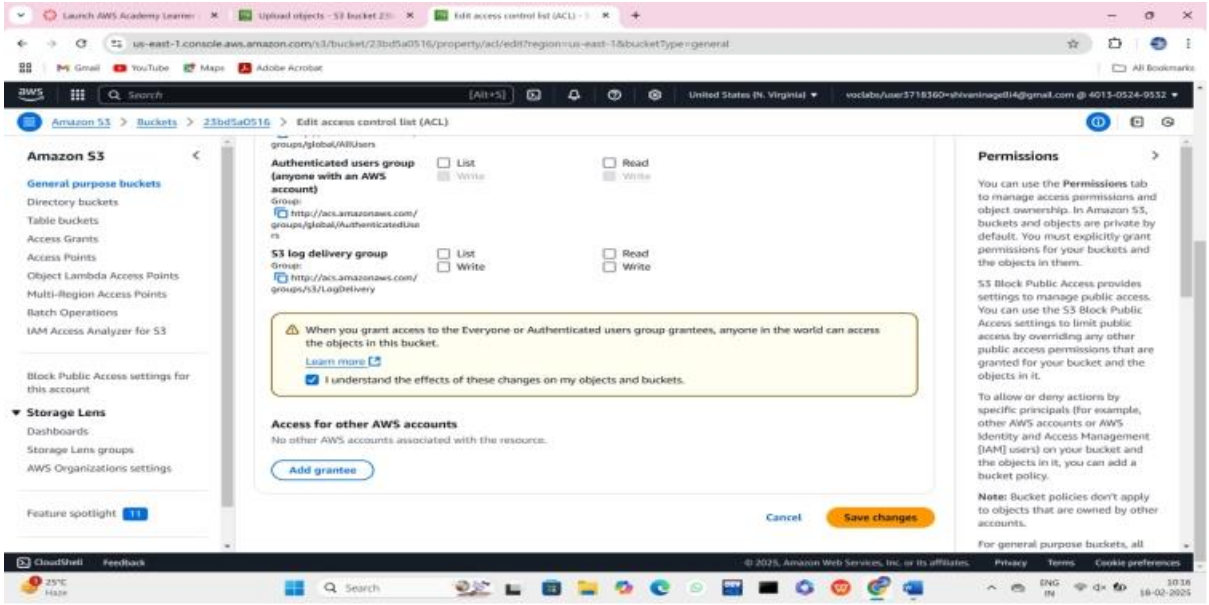

Edit Object Ownership
Object Ownership
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. 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.
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.
Enabling ACLs turns off the bucket owner enforced setting for Object Ownership
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.
I acknowledge that ACLs will be restored.
Object Ownership
Bucket owner preferred
Object writer

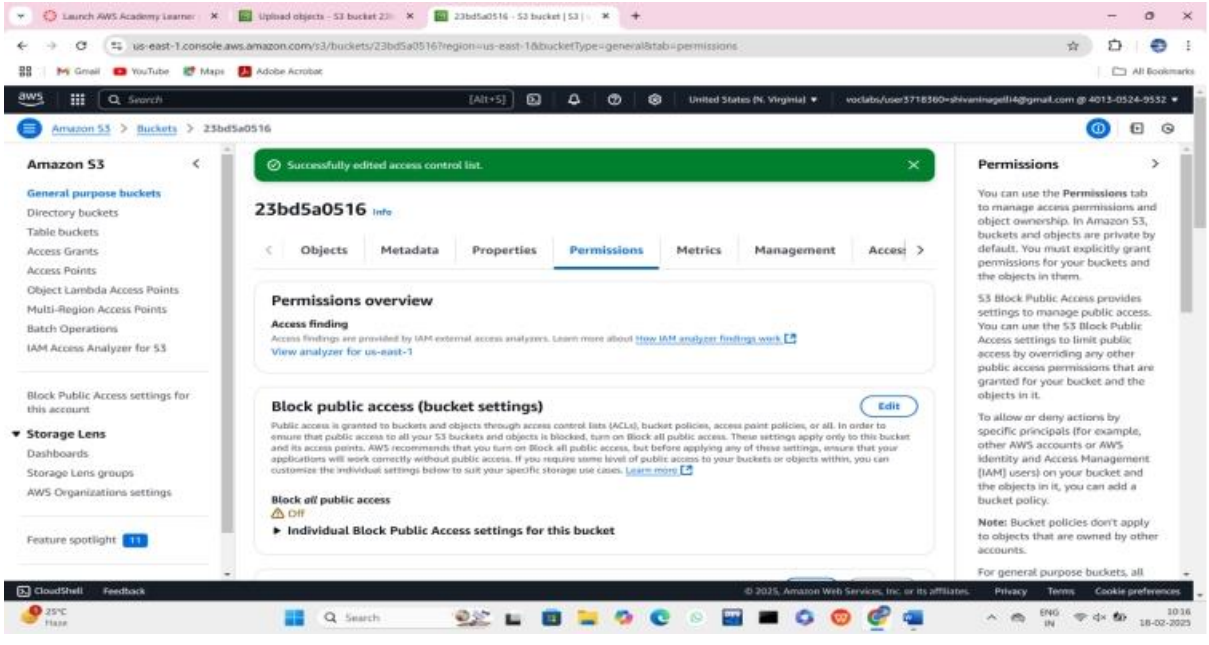

Amazon S3 > Buckets > 23bd5a0516 > Edit Object Ownership
We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.
Enabling ACLs turns off the bucket owner enforced setting for Object Ownership
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.
I acknowledge that ACLs will be restored.
Object Ownership
Bucket owner preferred
Object writer
If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more
Cancel
Save changes
Permissions

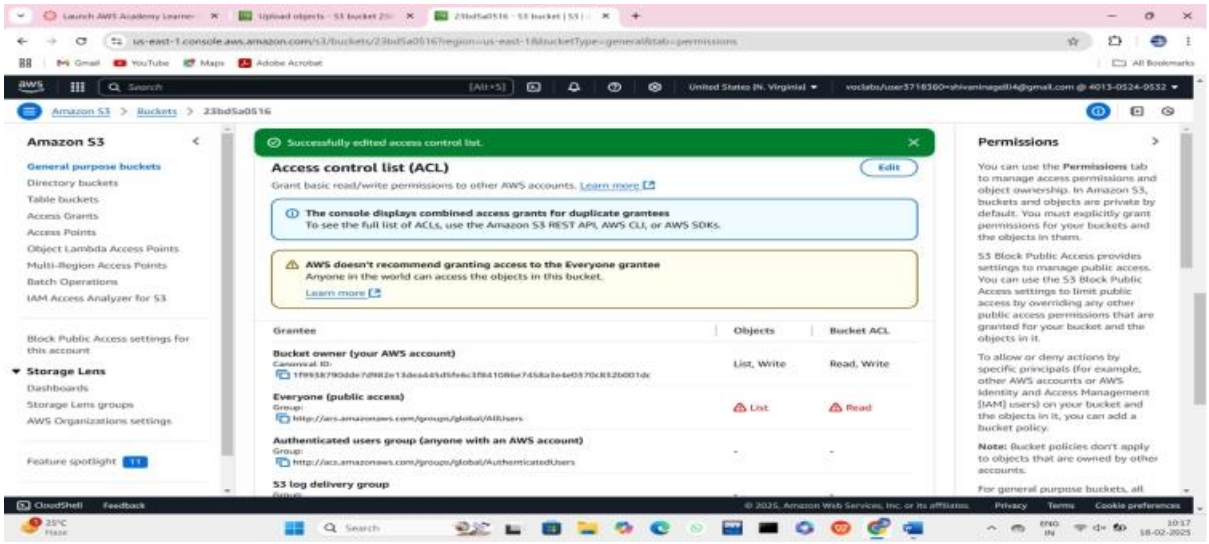

Successfully edited Object Ownership.
23bd5a0516 info
Objects
Metadata
Properties
Permissions
Metrics
Management
Permissions overview
Access finding
View analyzer for us-east-1
Block public access (bucket settings)
Edit
Block all public access
Off
Individual Block Public Access settings for this bucket
Permissions

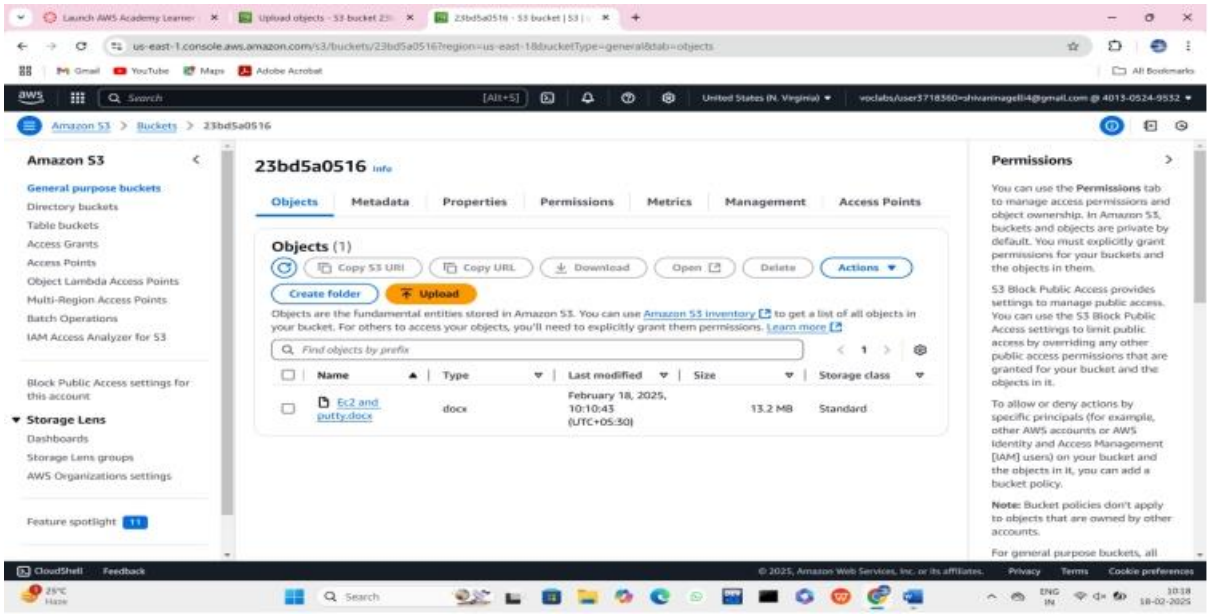

Successfully edited Object Ownership.
Access control list (ACL)
Edit
Grant basic read/write permissions to other AWS accounts. Learn more
The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
Canonical ID:
19958790dde7d982e13dea445d5fe6c3f841086e7458a3e4e0370c832b001dc
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
S3 log delivery group
Group:
http://acs.amazonaws.com/groups/s3/LogDelivery
Permissions

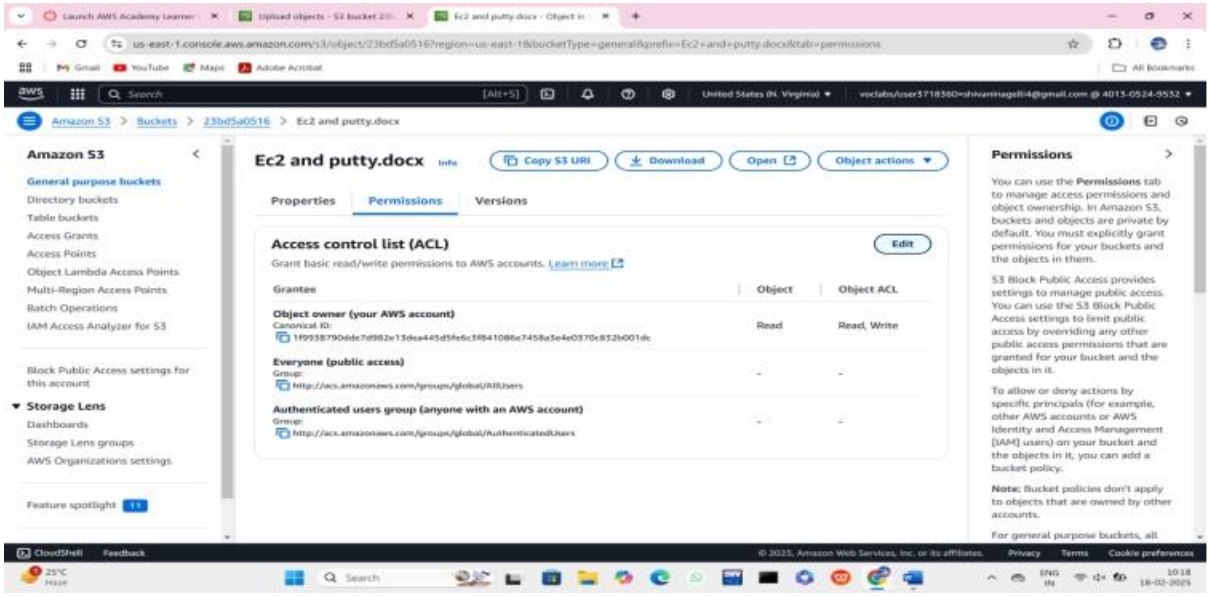

Amazon S3 > Buckets > 23bd5a0516 > Edit access control list (ACL)
Edit access control list (ACL)
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
Everyone (public access)
Authenticated users group (anyone with an AWS account)
S3 log delivery group
Permissions
You can use the Permissions tab to manage access permissions and object ownership. In Amazon S3, buckets and objects are private by default. You must explicitly grant permissions for your buckets and the objects in them.
S3 Block Public Access provides settings to manage public access. You can use the S3 Block Public Access settings to limit public access by overriding any other public access permissions that are granted for your bucket and the objects in it.
To allow or deny actions by specific principals (for example, other AWS accounts or AWS Identity and Access Management [IAM] users) on your bucket and the objects in it, you can add a bucket policy.
Note: Bucket policies don't apply to objects that are owned by other accounts.

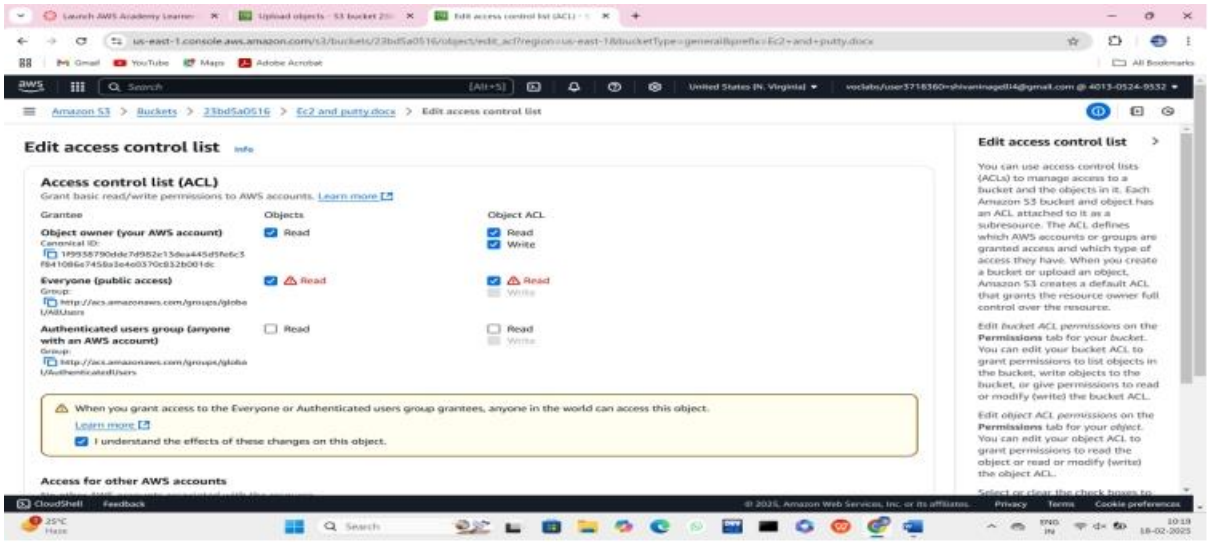

When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.
Learn more
I understand the effects of these changes on my objects and buckets.
Access for other AWS accounts
No other AWS accounts associated with the resource.
Add grantee
Cancel
Save changes

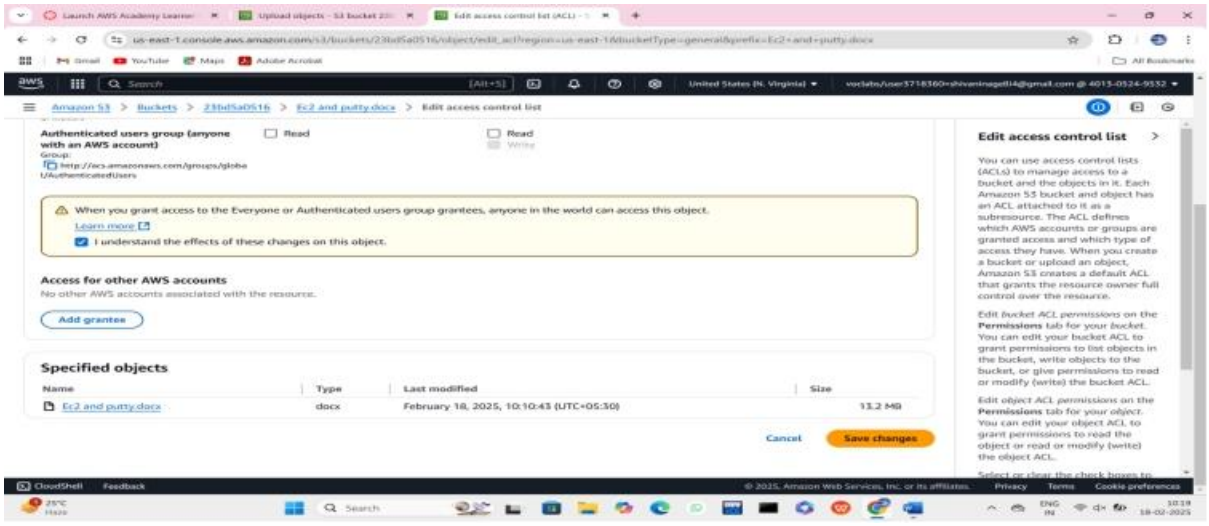

Successfully edited access control list.
23bd5a0516
Objects
Metadata
Properties
Permissions
Metrics
Management
Permissions overview
Access finding
View analyzer for us-east-1
Block public access (bucket settings)
Edit
Block all public access
Off
Individual Block Public Access settings for this bucket

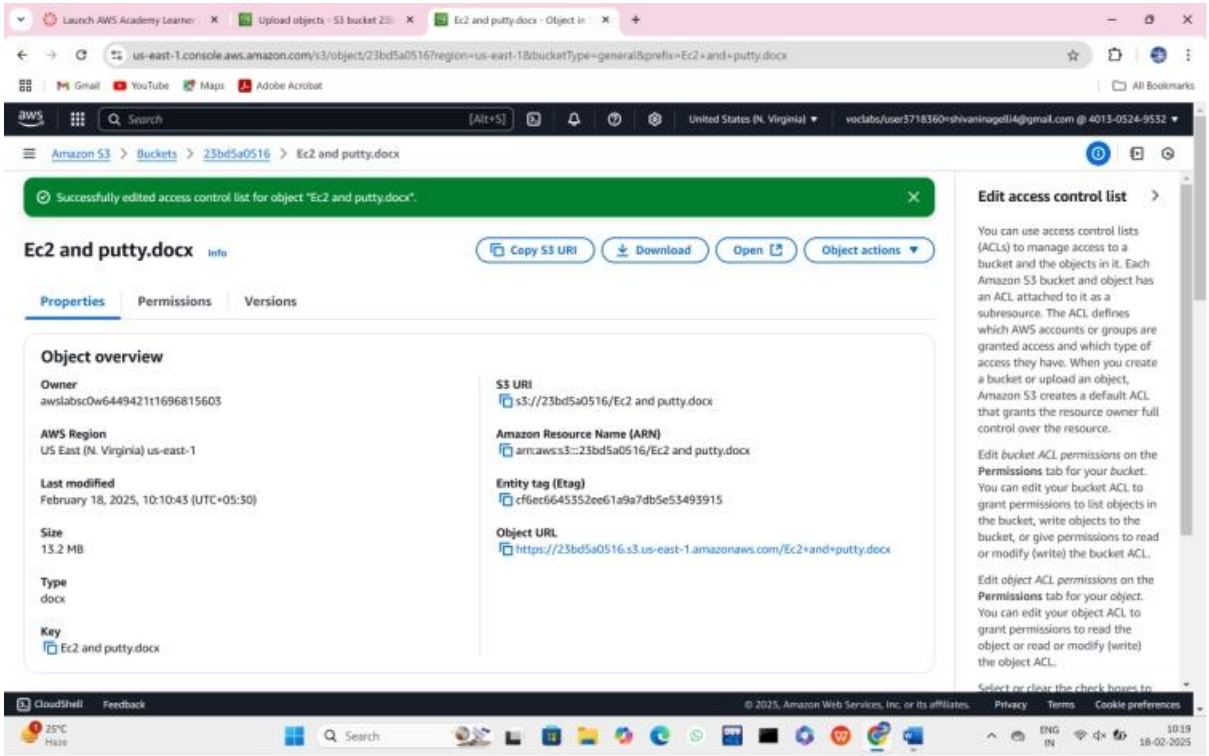

Amazon S3
Buckets
23bd5a0516
Successfully edited access control list.
Access control list (ACL)
Edit
Grant basic read/write permissions to other AWS accounts. Learn more
The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.
AWS doesn't recommend granting access to the Everyone grantee
Anyone in the world can access the objects in this bucket.
Learn more
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
List, Write
Read, Write
Everyone (public access)
List
Read
Authenticated users group (anyone with an AWS account)
S3 log delivery group
Permissions
You can use the Permissions tab to manage access permissions and object ownership. In Amazon S3, buckets and objects are private by default. You must explicitly grant permissions for your buckets and the objects in them.
S3 Block Public Access provides settings to manage public access. You can use the S3 Block Public Access settings to limit public access by overriding any other public access permissions that are granted for your bucket and the objects in it.
To allow or deny actions by specific principals (for example, other AWS accounts or AWS Identity and Access Management [IAM] users) on your bucket and the objects in it, you can add a bucket policy.
Note: Bucket policies don't apply to objects that are owned by other accounts.
For general purpose buckets, all
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
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
CloudShell
Feedback

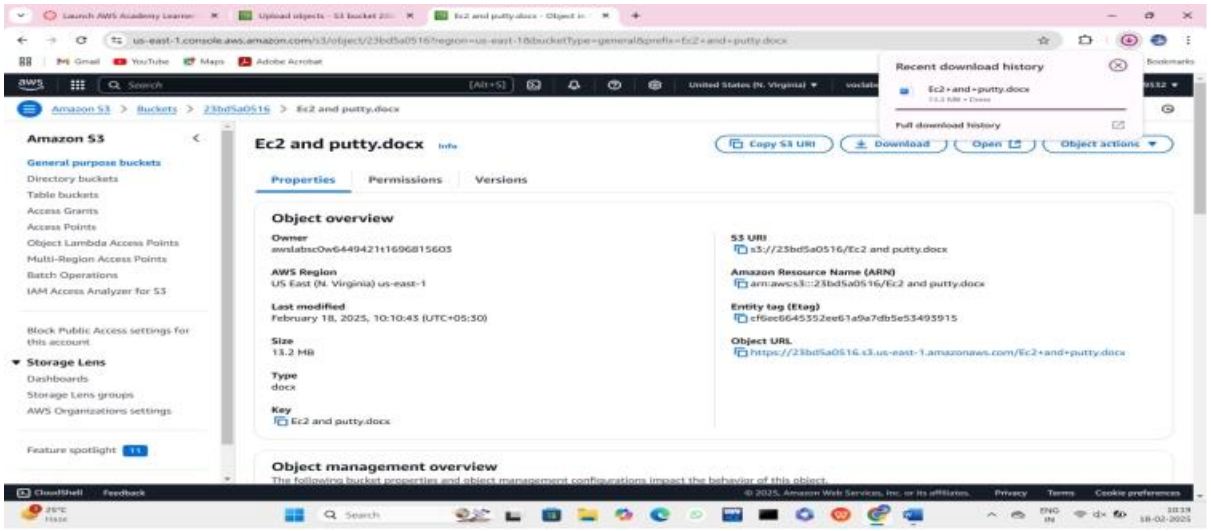

Amazon S3
Buckets
23bd5a0516
23bd5a0516 Info
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Objects (1)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list 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
Ec2 and putty.docx
docx
February 18, 2025, 10:10:43 (UTC+05:30)
13.2 MB
Standard
Permissions
You can use the Permissions tab to manage access permissions and object ownership. In Amazon S3, buckets and objects are private by default. You must explicitly grant permissions for your buckets and the objects in them.
S3 Block Public Access provides settings to manage public access. You can use the S3 Block Public Access settings to limit public access by overriding any other public access permissions that are granted for your bucket and the objects in it.
To allow or deny actions by specific principals (for example, other AWS accounts or AWS Identity and Access Management [IAM] users) on your bucket and the objects in it, you can add a bucket policy.
Note: Bucket policies don't apply to objects that are owned by other accounts.
For general purpose buckets, all
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
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
CloudShell
Feedback

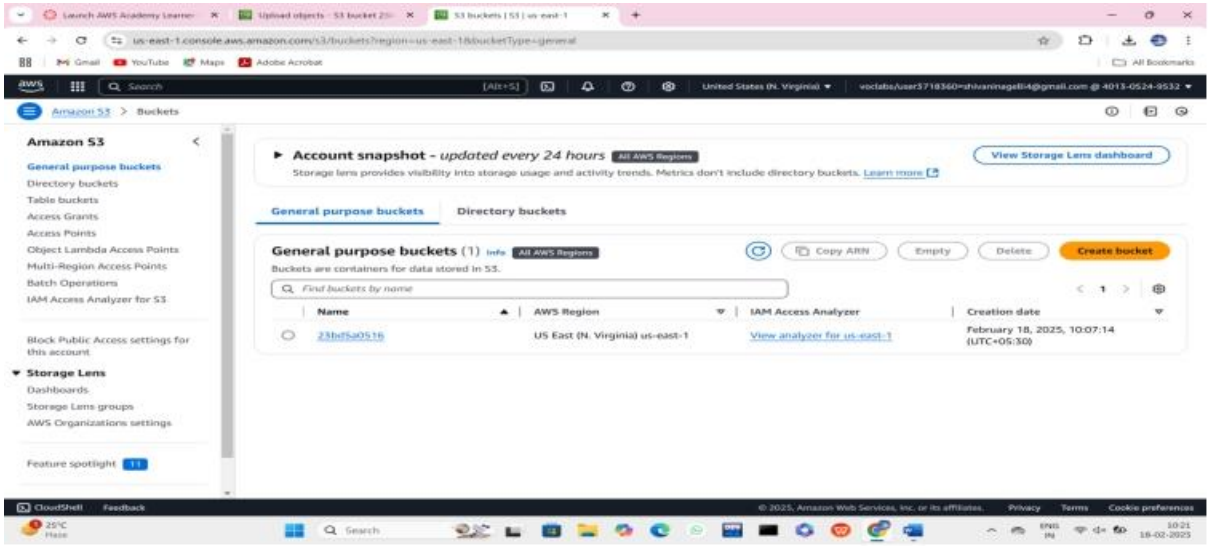

Amazon S3
Buckets
23bd5a0516
Ec2 and putty.docx
Ec2 and putty.docx Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Access control list (ACL)
Edit
Grant basic read/write permissions to AWS accounts. Learn more
Grantee
Object
Object ACL
Object owner (your AWS account)
Read
Read, Write
Everyone (public access)
Authenticated users group (anyone with an AWS account)
Permissions
You can use the Permissions tab to manage access permissions and object ownership. In Amazon S3, buckets and objects are private by default. You must explicitly grant permissions for your buckets and the objects in them.
S3 Block Public Access provides settings to manage public access. You can use the S3 Block Public Access settings to limit public access by overriding any other public access permissions that are granted for your bucket and the objects in it.
To allow or deny actions by specific principals (for example, other AWS accounts or AWS Identity and Access Management [IAM] users) on your bucket and the objects in it, you can add a bucket policy.
Note: Bucket policies don't apply to objects that are owned by other accounts.
For general purpose buckets, all
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
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
CloudShell
Feedback

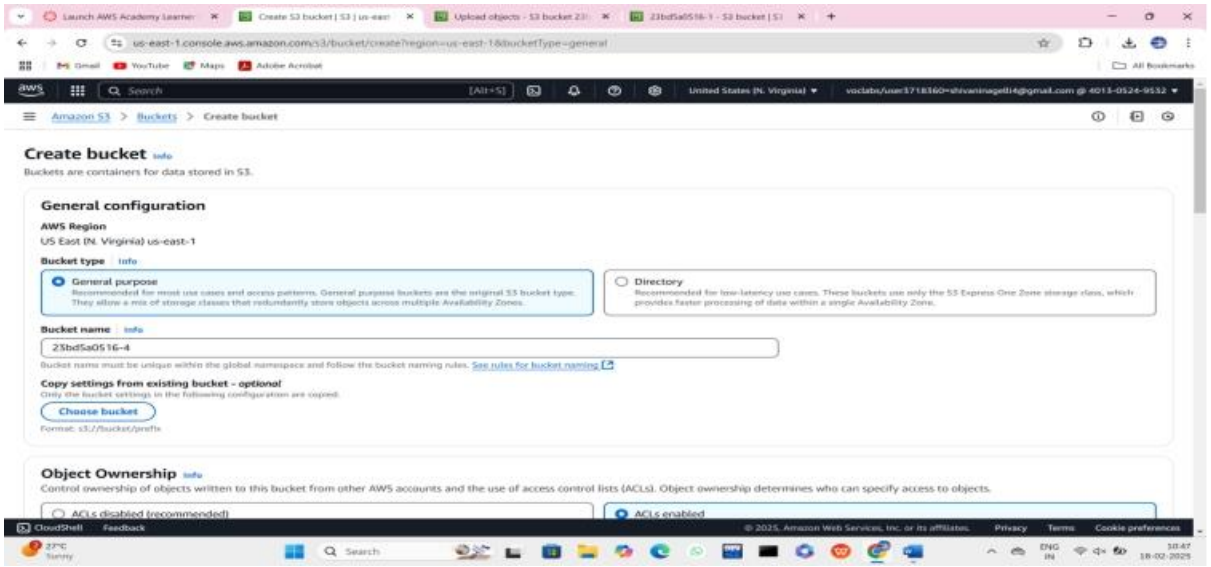

Edit access control list
Access control list (ACL)
Grant basic read/write permissions to AWS accounts. Learn more
Grantee
Objects
Object ACL
Object owner (your AWS account)
Read
Read
Write
Everyone (public access)
Read
Read
Authenticated users group (anyone with an AWS account)
Read
Read
When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.
Learn more
I understand the effects of these changes on this object.
Access for other AWS accounts
Edit access control list
You can use access control lists (ACLs) to manage access to a bucket and the objects in it. Each Amazon S3 bucket and object has an ACL attached to it as a subresource. The ACL defines which AWS accounts or groups are granted access and which type of access they have. When you create a bucket or upload an object, Amazon S3 creates a default ACL that grants the resource owner full control over the resource.
Edit bucket ACL permissions on the Permissions tab for your bucket. You can edit your bucket ACL to grant permissions to list objects in the bucket, write objects to the bucket, or give permissions to read or modify (write) the bucket ACL.
Edit object ACL permissions on the Permissions tab for your object. You can edit your object ACL to grant permissions to read the object or read or modify (write) the object ACL.

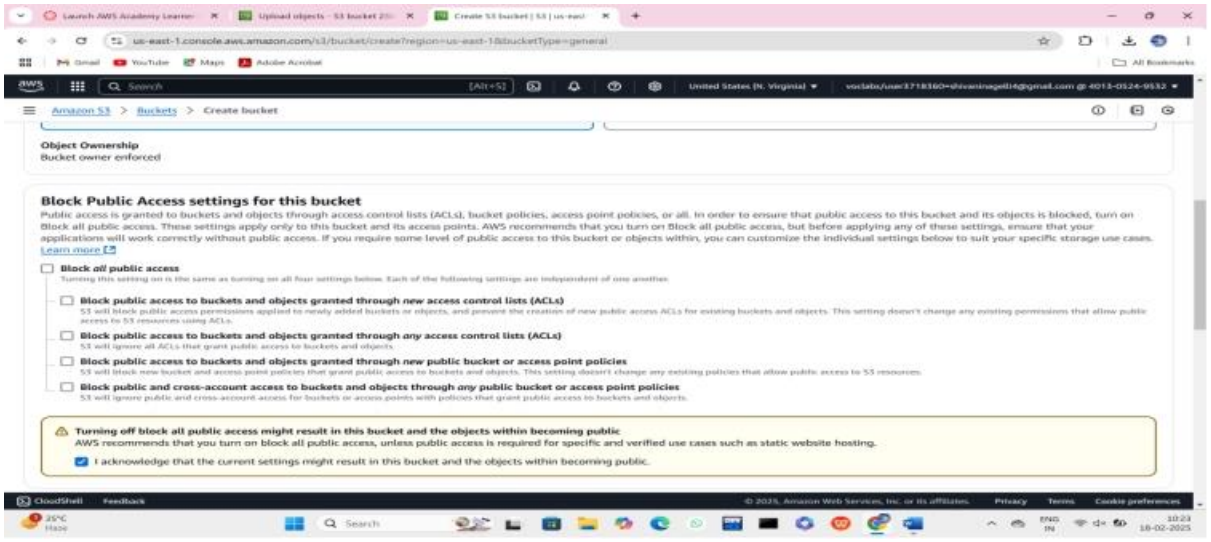

Authenticated users group (anyone with an AWS account)
Read
Read
When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.
Learn more
I understand the effects of these changes on this object.
Access for other AWS accounts
No other AWS accounts associated with the resource.
Add grantee
Specified objects
Name
Type
Last modified
Size
Ec2 and putty.docx
docx
February 18, 2025, 10:10:43 (UTC+05:30)
13.2 MB
Cancel
Save changes
Edit access control list

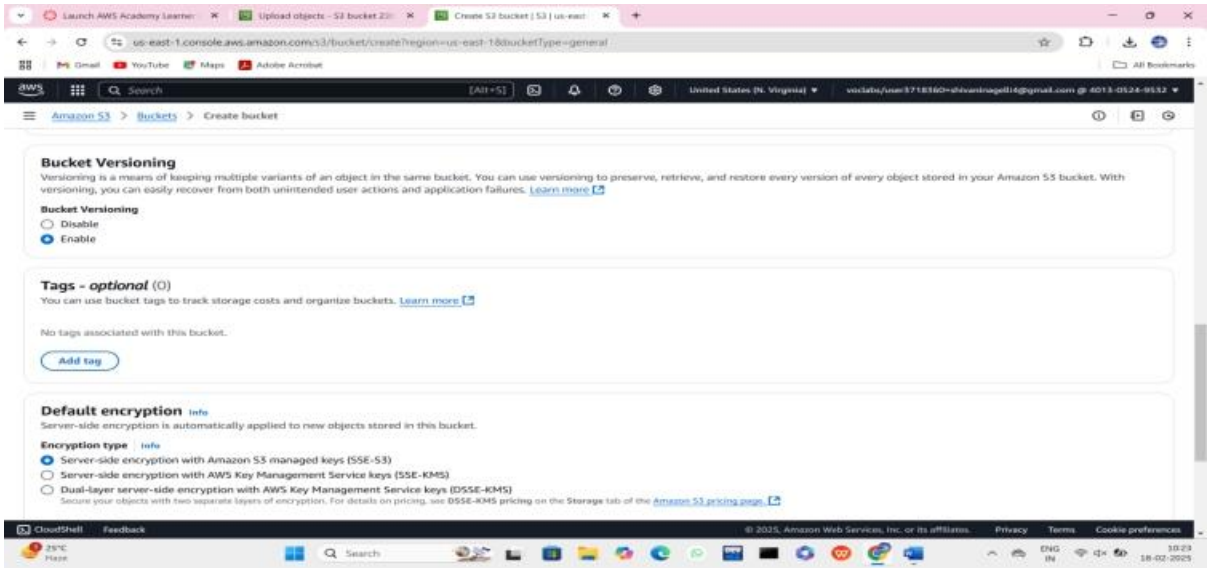

Successfully edited access control list for object "Ec2 and putty.docx".
Ec2 and putty.docx
Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
awslabsc0w6449421t1696815603
AWS Region
US East (N. Virginia) us-east-1
Last modified
February 18, 2025, 10:10:43 (UTC+05:30)
Size
13.2 MB
Type
docx
Key
Ec2 and putty.docx
S3 URI
s3://23bd5a0516/Ec2 and putty.docx
Amazon Resource Name (ARN)
arn:aws:s3:::23bd5a0516/Ec2 and putty.docx
Entity tag (Etag)
cf6ec6645352ee61a9a7db5e53493915
Object URL
https://23bd5a0516.s3.us-east-1.amazonaws.com/Ec2+and+putty.docx
Edit access control list

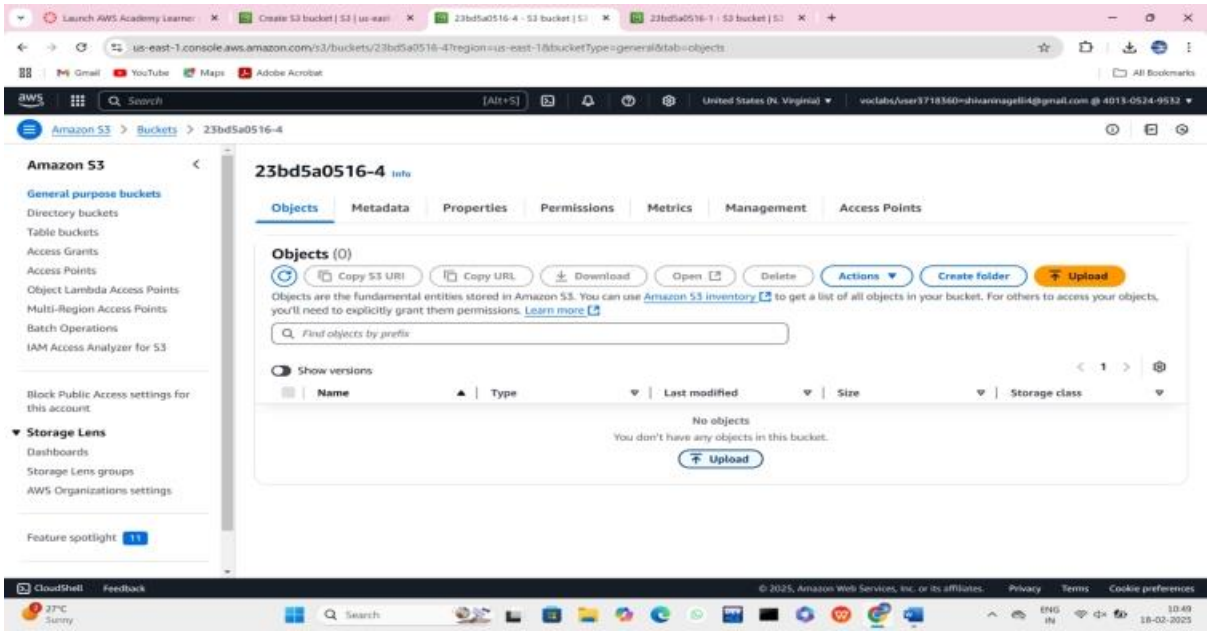

Recent download history
Ec2+and+putty.docx
Full download history
Amazon S3 > Buckets > 23bd5a0516 > Ec2 and putty.docx
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
Ec2 and putty.docx
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
awslabscOw6449421t1696815603
AWS Region
US East (N. Virginia) us-east-1
Last modified
February 18, 2025, 10:10:43 (UTC+05:30)
Size
13.2 MB
Type
docx
Key
Ec2 and putty.docx
S3 URI
s3://23bd5a0516/Ec2 and putty.docx
Amazon Resource Name (ARN)
arn:aws:s3:::23bd5a0516/Ec2 and putty.docx
Entity tag (Etag)
cf6ec6645552ee61a9a7db5e53493915
Object URL
https://23bd5a0516.s3.us-east-1.amazonaws.com/Ec2+and+putty.docx
Object management overview
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

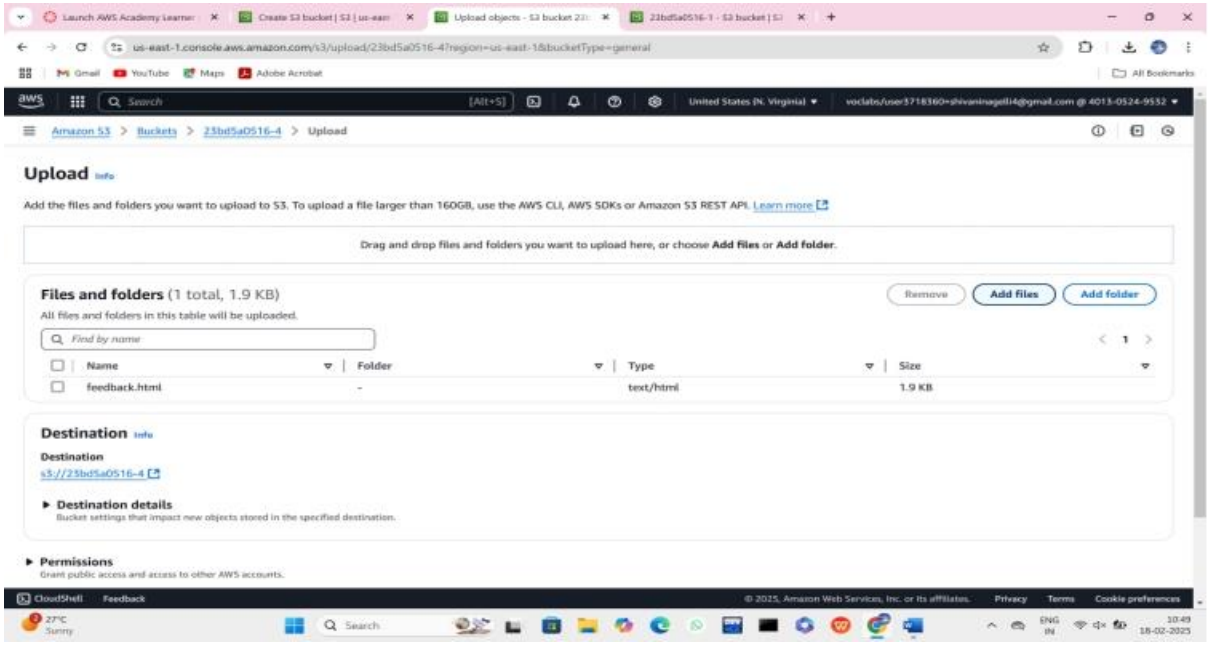

Amazon S3 > Buckets
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
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
23bd5a0516
US East (N. Virginia) us-east-1
View analyzer for us-east-1
February 18, 2025, 10:07:14 (UTC+05:30)
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

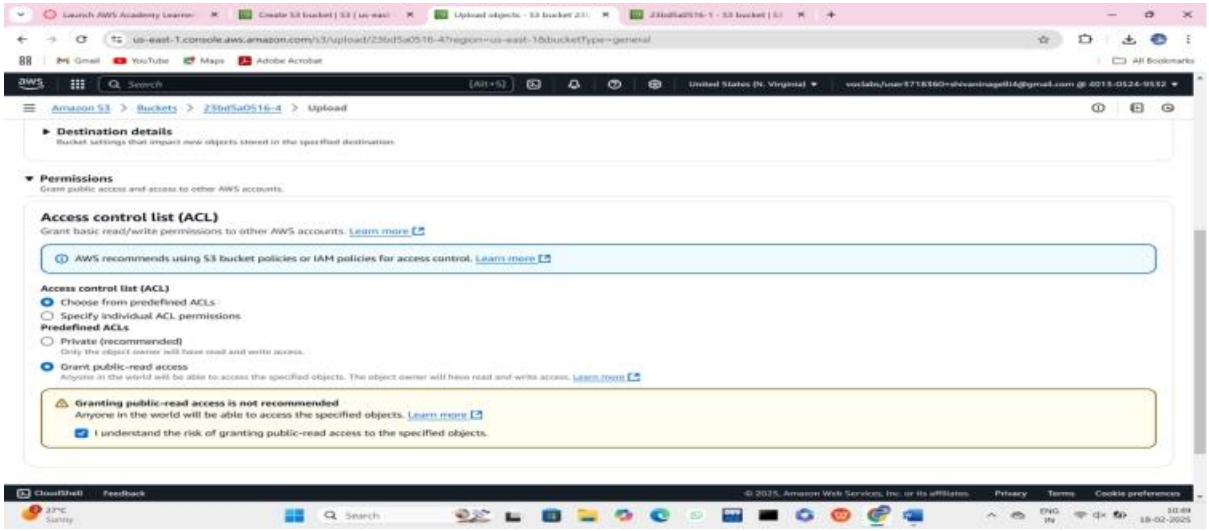

Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
US East (N. Virginia) us-east-1
Bucket type Info
General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
Directory
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
23bd5a0516-4
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
ACLs enabled
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

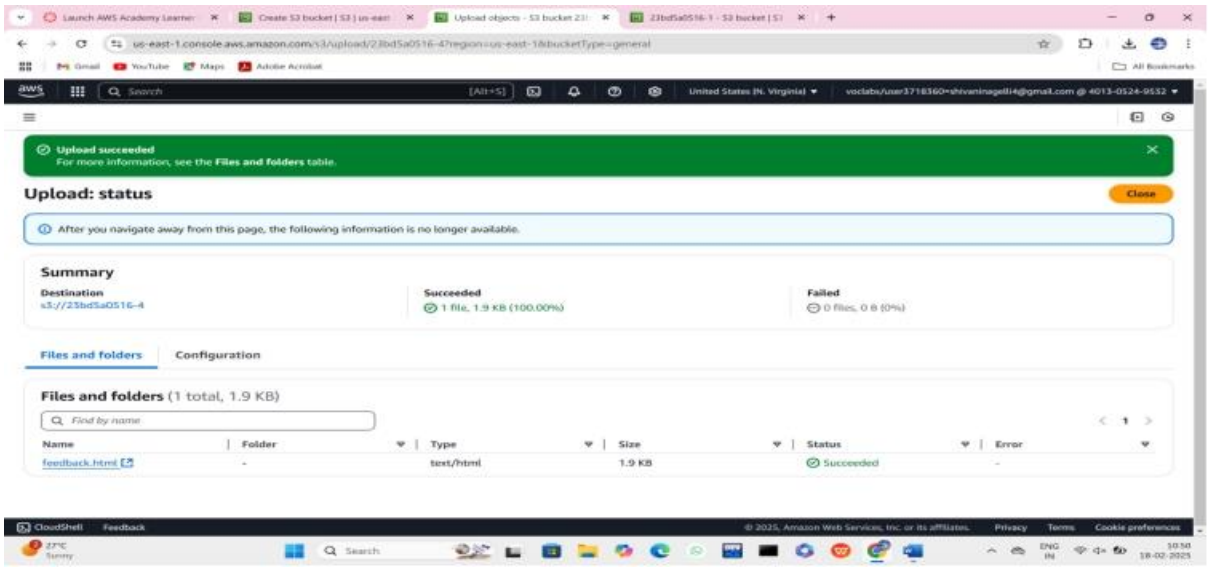

Amazon S3 > Buckets > Create bucket
Object Ownership
Bucket owner enforced
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases.
Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
I acknowledge that the current settings might result in this bucket and the objects within becoming public.

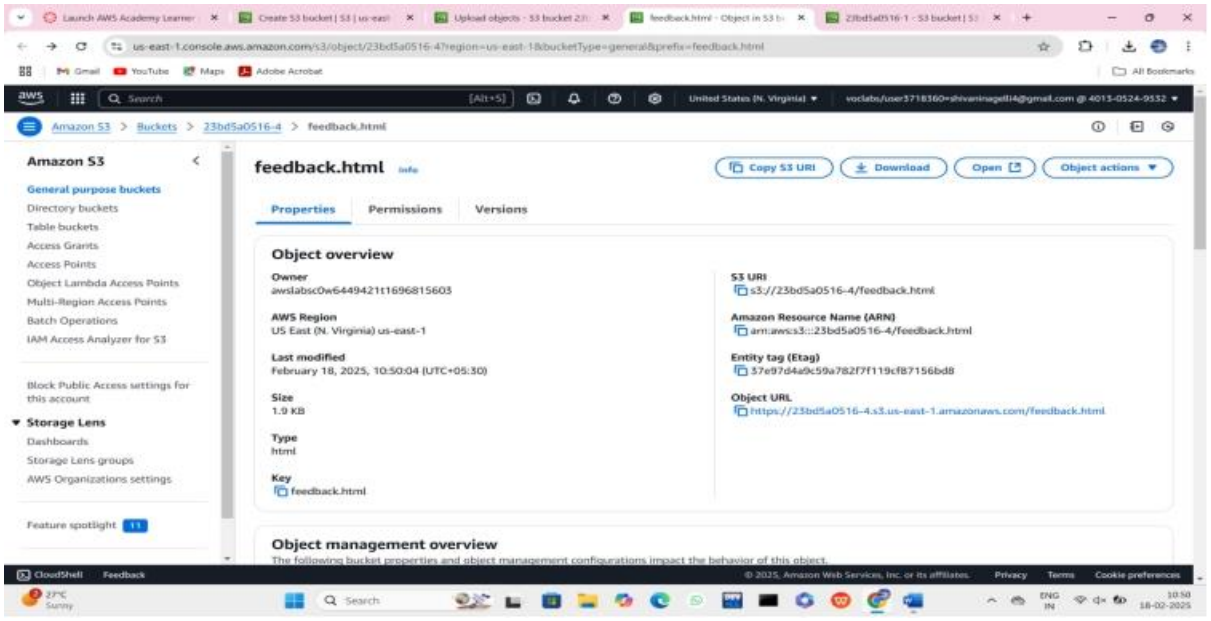

Amazon S3 > Buckets > Create bucket
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disable
Enable
Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add tag
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.

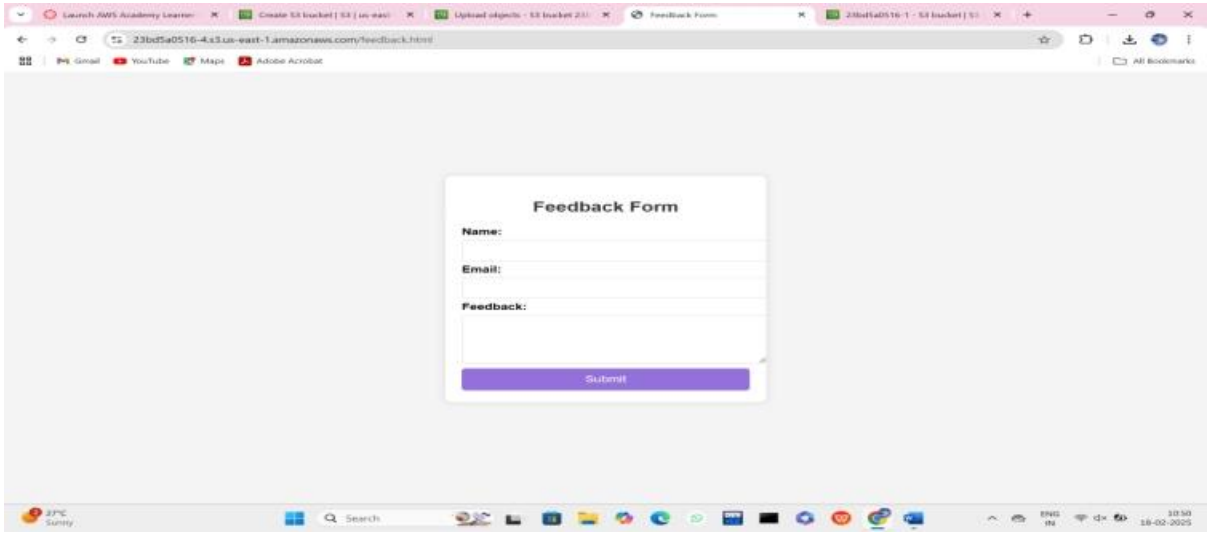

Amazon S3 > Buckets > 23bd5a0516-4
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 11
23bd5a0516-4 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
Show versions
Name
Type
Last modified
Size
Storage class
No objects
You don't have any objects in this bucket.
Upload

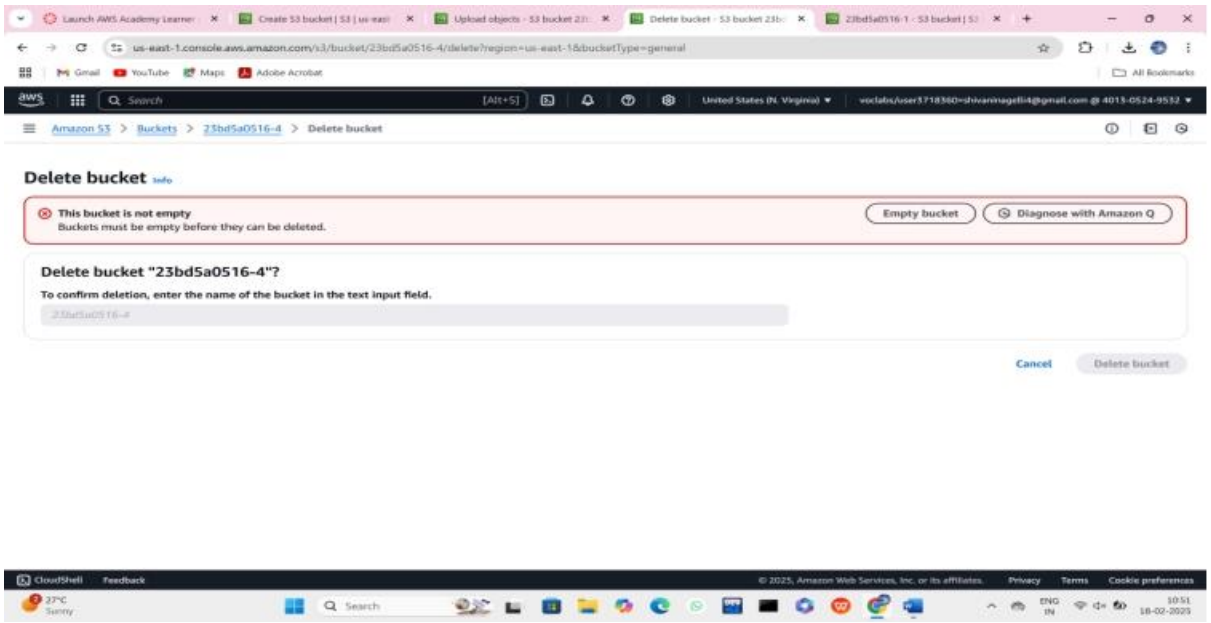

Amazon S3 > Buckets > 23bd5a0516-4 > Upload
Upload
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 total, 1.9 KB)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
Name
Folder
Type
Size
feedback.html
-
text/html
1.9 KB
Destination
Destination
s3://23bd5a0516-4
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.

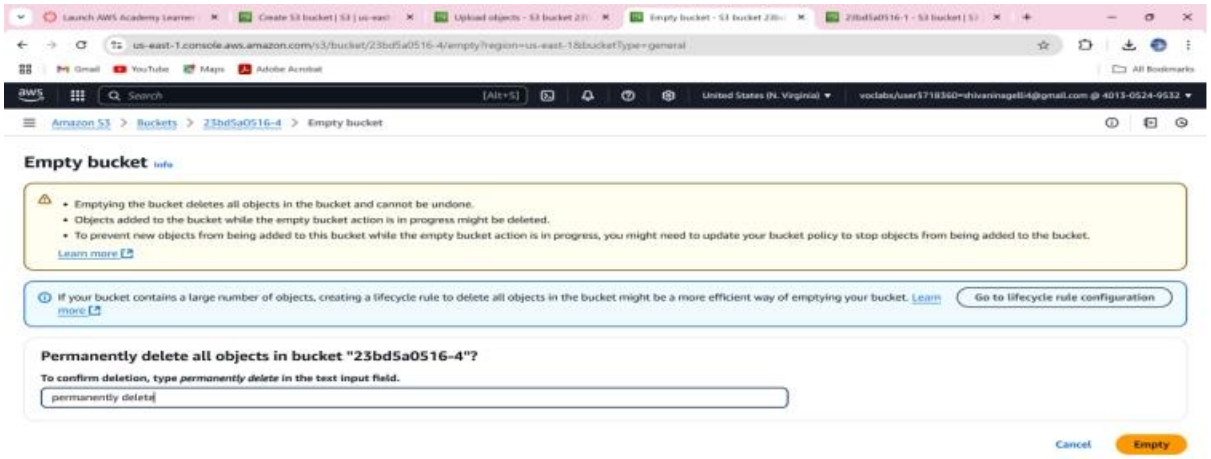

Amazon S3 > Buckets > 23bd5a0516-4 > Upload
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more
AWS recommends using S3 bucket policies or IAM policies for access control. Learn more
Access control list (ACL)
Choose from predefined ACLs
Specify individual ACL permissions
Predefined ACLs
Private (recommended)
Only the object owner will have read and write access.
Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. Learn more
Granting public-read access is not recommended
Anyone in the world will be able to access the specified objects. Learn more
I understand the risk of granting public-read access to the specified objects.

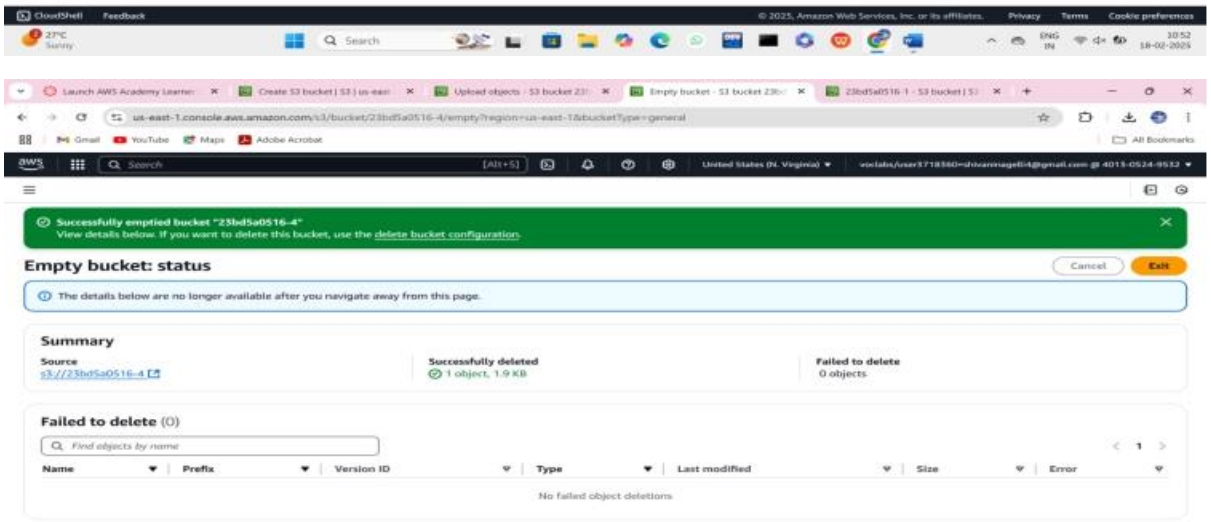

Upload succeeded
For more information, see the Files and folders table.
Upload: status
Close
After you navigate away from this page, the following information is no longer available.
Summary
Destination
s3://23bd5a0516-4
Succeeded
1 file, 1.9 KB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 total, 1.9 KB)
Find by name
Name
Folder
Type
Size
Status
Error
feedback.html
-
text/html
1.9 KB
Succeeded

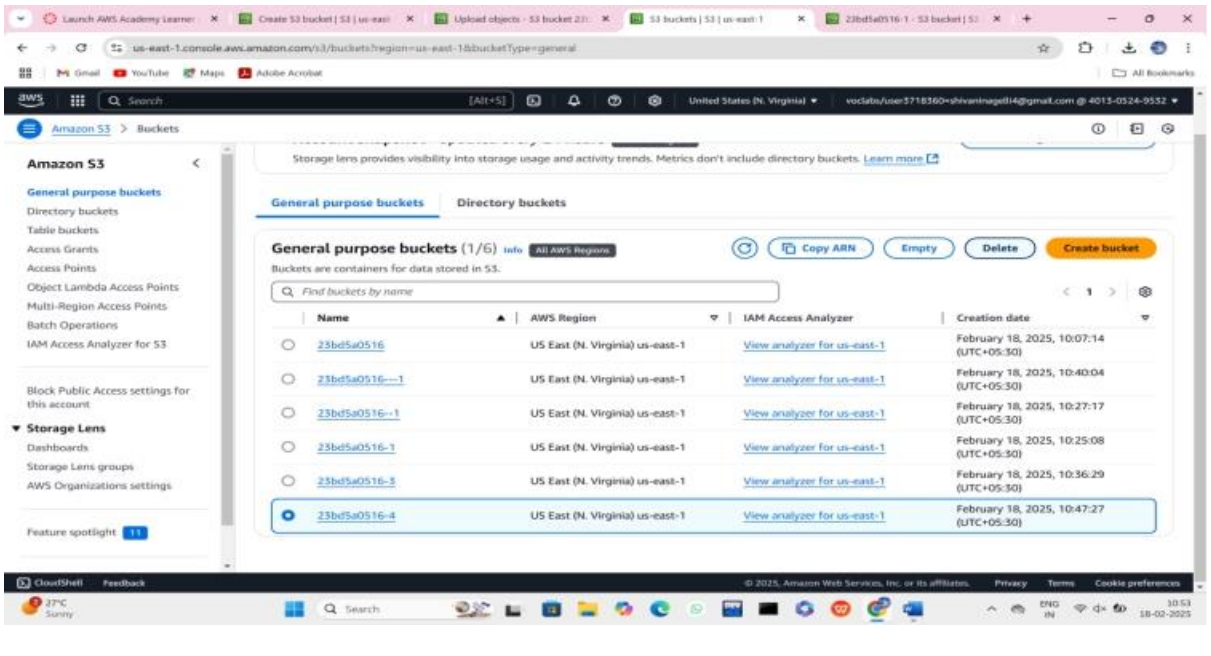

Amazon S3
feedback.html
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
awslabsc0w6449421t1696815603
AWS Region
US East (N. Virginia) us-east-1
Last modified
February 18, 2025, 10:50:04 (UTC+05:30)
Size
1.9 KB
Type
html
Key
feedback.html
S3 URI
s3://23bd5a0516-4/feedback.html
Amazon Resource Name (ARN)
arn:aws:s3:::23bd5a0516-4/feedback.html
Entity tag (Etag)
37e97d4a9c59a782f7f119cf87156bd8
Object URL
https://23bd5a0516-4.s3.us-east-1.amazonaws.com/feedback.html
Object management overview

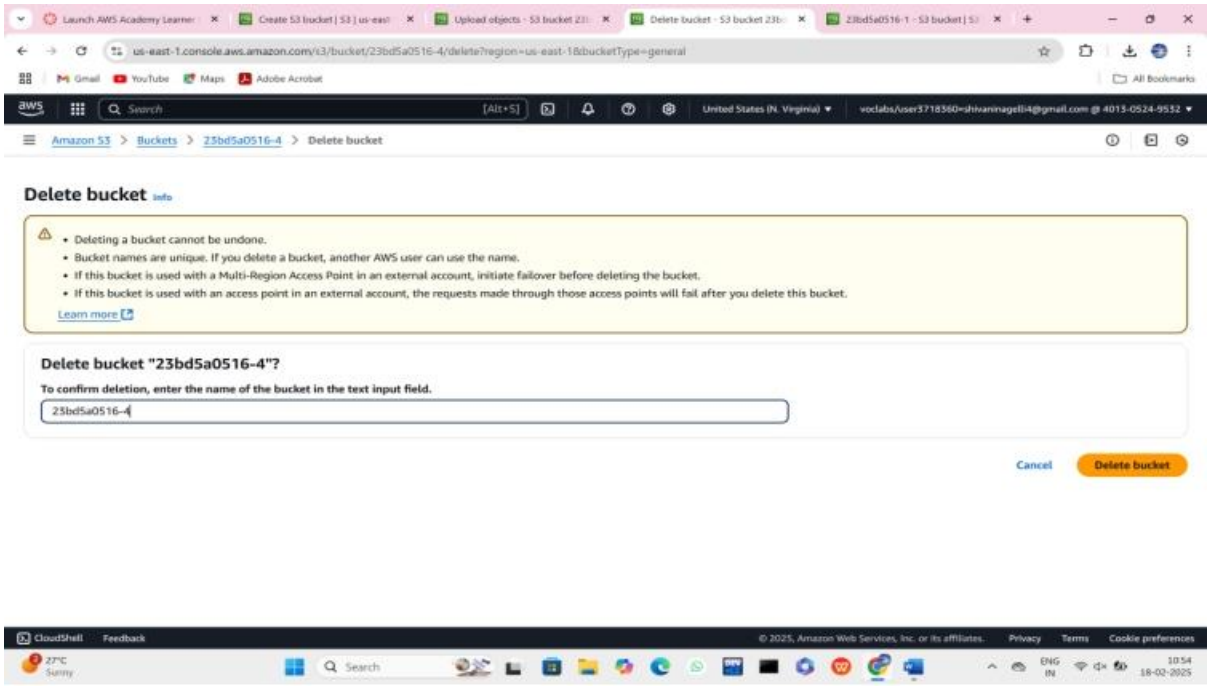

Feedback Form
Name:
Email:
Feedback:
Submit

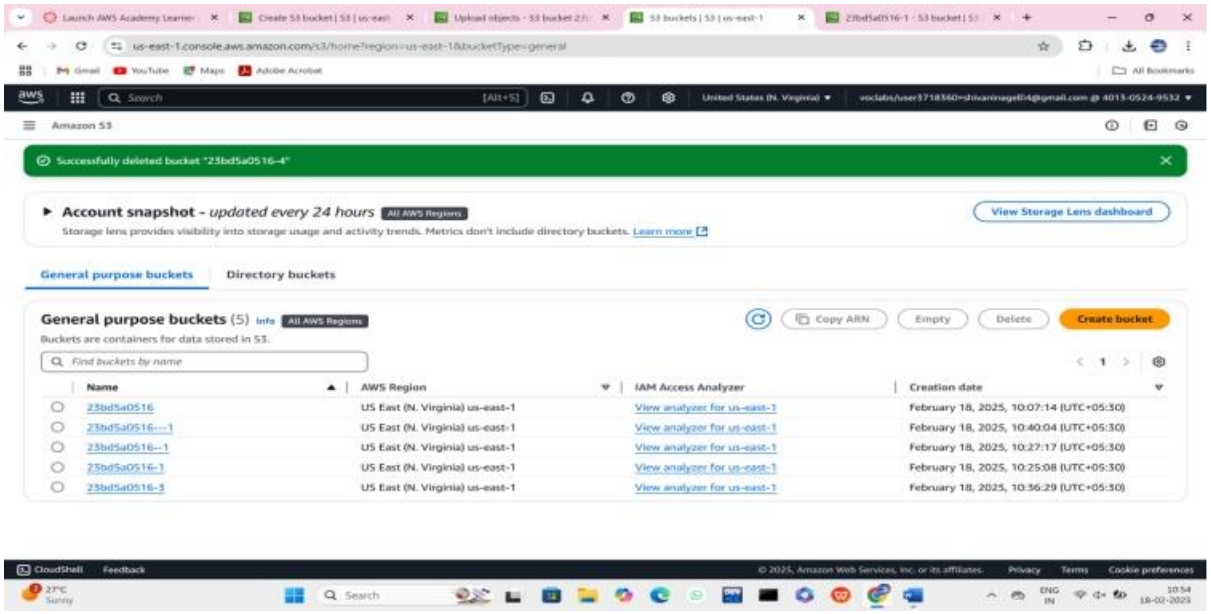

Delete bucket
This bucket is not empty
Buckets must be empty before they can be deleted.
Empty bucket
Diagnose with Amazon Q
Delete bucket "23bd5a0516-4"?
To confirm deletion, enter the name of the bucket in the text input field.
Cancel
Delete bucket


Amazon S3 > Buckets > 23bd5a0516-4 > Empty bucket
Empty bucket
Emptying the bucket deletes all objects in the bucket and cannot be undone.
Objects added to the bucket while the empty bucket action is in progress might be deleted.
To prevent new objects from being added to this bucket while the empty bucket action is in progress, you might need to update your bucket policy to stop objects from being added to the bucket.
Learn more
If your bucket contains a large number of objects, creating a lifecycle rule to delete all objects in the bucket might be a more efficient way of emptying your bucket. Learn more
Go to lifecycle rule configuration
Permanently delete all objects in bucket "23bd5a0516-4"?
To confirm deletion, type permanently delete in the text input field.
permanently delete
Cancel
Empty

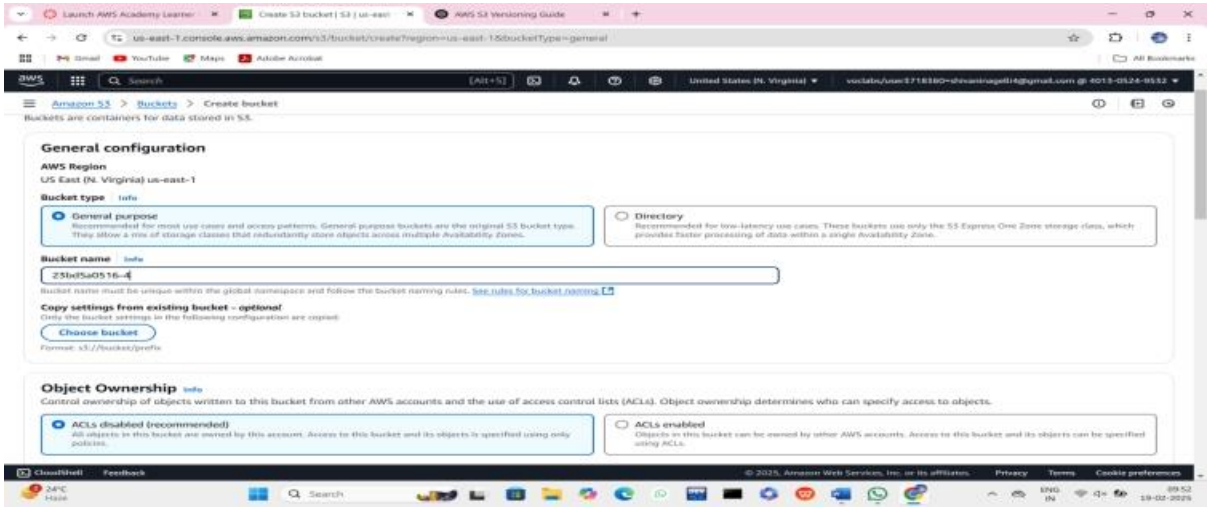

Successfully emptied bucket "23bd5a0516-4"
View details below. If you want to delete this bucket, use the delete bucket configuration.
Empty bucket: status
Cancel
Exit
The details below are no longer available after you navigate away from this page.
Summary
Source
s3://23bd5a0516-4
Successfully deleted
1 object, 1.9 KB
Failed to delete
0 objects
Failed to delete (0)
Find objects by name
Name
Prefix
Version ID
Type
Last modified
Size
Error
No failed object deletions

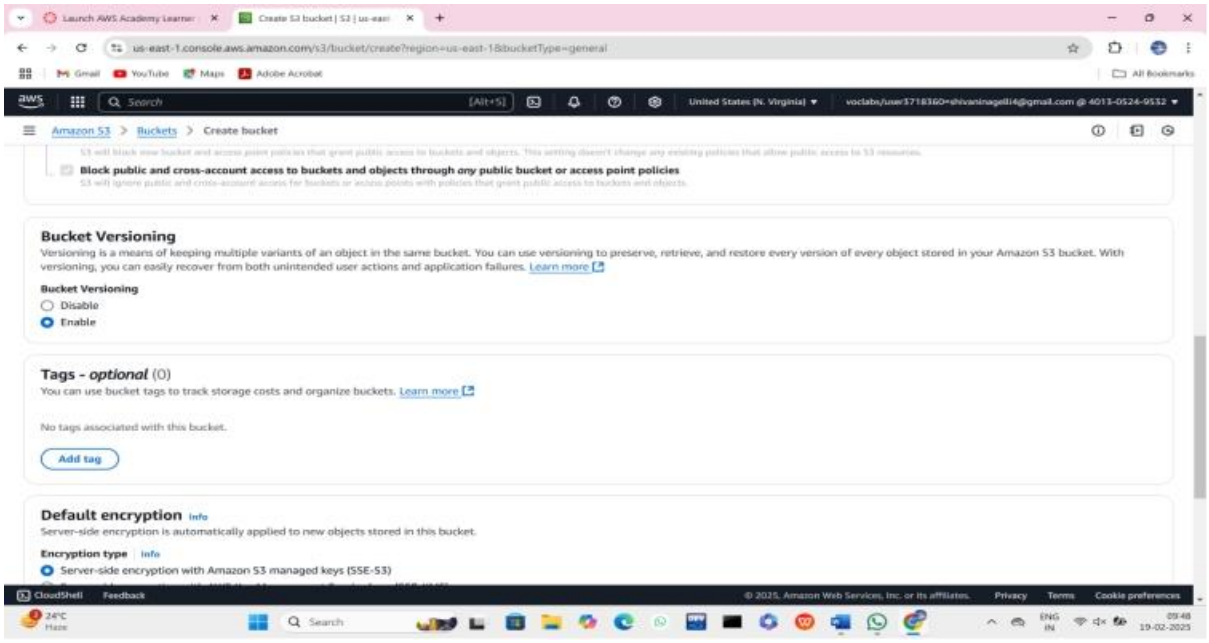

Amazon S3 > Buckets
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
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 (1/6)
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
23bd5a0516
US East (N. Virginia) us-east-1
View analyzer for us-east-1
February 18, 2025, 10:07:14 (UTC+05:30)
23bd5a0516---1
US East (N. Virginia) us-east-1
View analyzer for us-east-1
February 18, 2025, 10:40:04 (UTC+05:30)
23bd5a0516--1
US East (N. Virginia) us-east-1
View analyzer for us-east-1
February 18, 2025, 10:27:17 (UTC+05:30)
23bd5a0516-1
US East (N. Virginia) us-east-1
View analyzer for us-east-1
February 18, 2025, 10:25:08 (UTC+05:30)
23bd5a0516-3
US East (N. Virginia) us-east-1
View analyzer for us-east-1
February 18, 2025, 10:36:29 (UTC+05:30)
23bd5a0516-4
US East (N. Virginia) us-east-1
View analyzer for us-east-1
February 18, 2025, 10:47:27 (UTC+05:30)

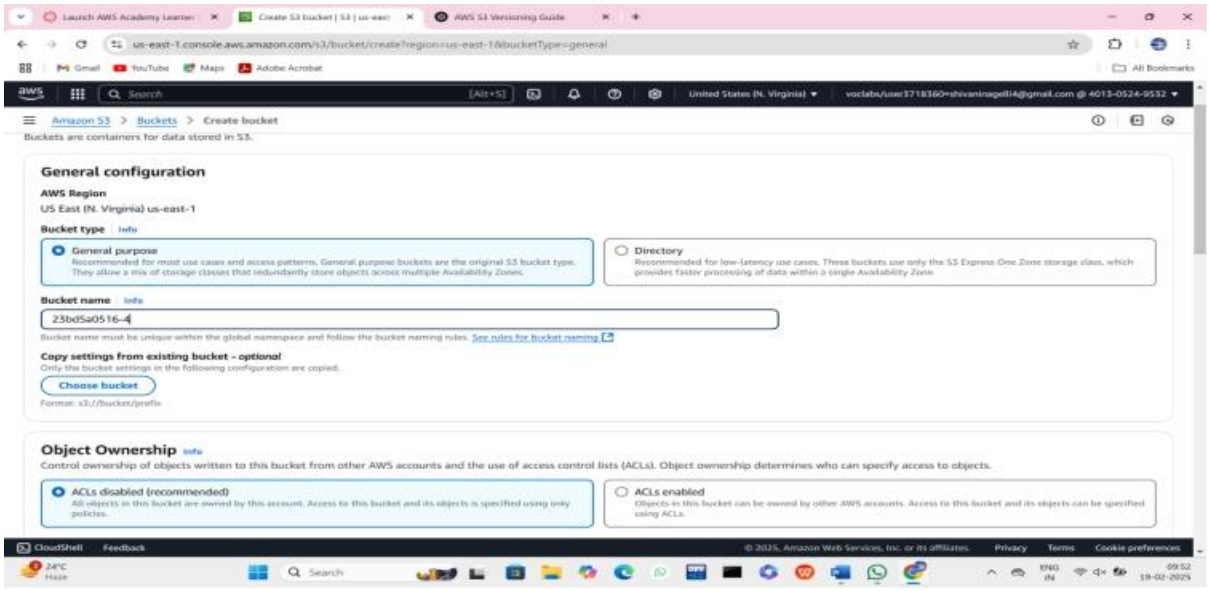

Amazon S3 > Buckets > 23bd5a0516-4 > Delete bucket
Delete bucket
• Deleting a bucket cannot be undone.
• Bucket names are unique. If you delete a bucket, another AWS user can use the name.
• If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
• If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.
Learn more
Delete bucket "23bd5a0516-4"?
To confirm deletion, enter the name of the bucket in the text input field.
23bd5a0516-4
Cancel
Delete bucket

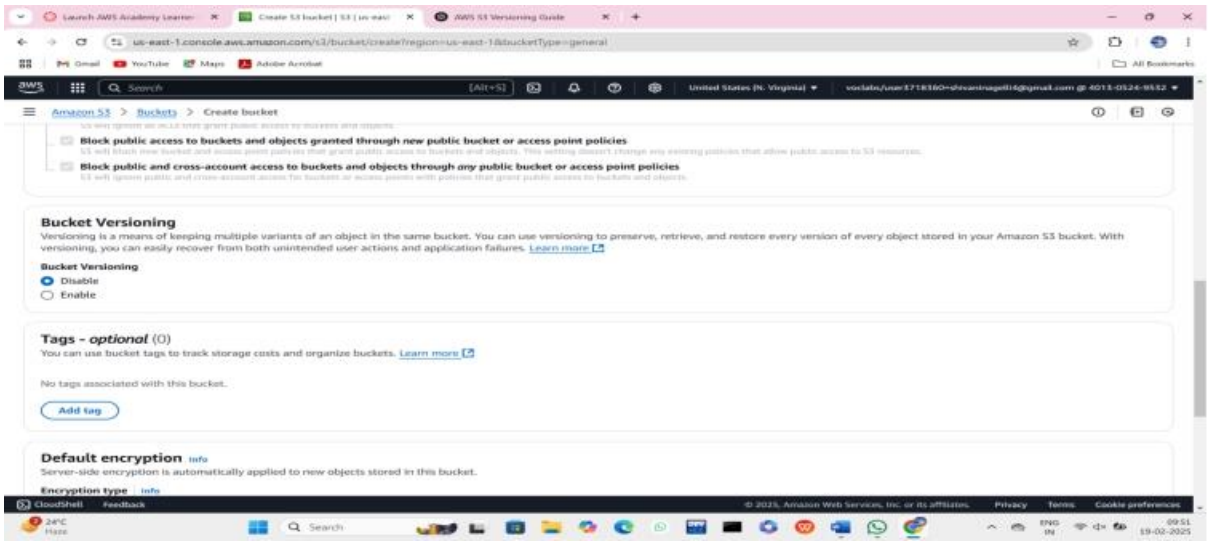

Amazon S3
Successfully deleted bucket "23bd5a0516-4"
Account snapshot - updated every 24 hours
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (5)
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
23bd5a0516
US East (N. Virginia) us-east-1
View analyzer for us-east-1
Febuary 18, 2025, 10:07:14 (UTC+05:30)
23bd5a0516---1
US East (N. Virginia) us-east-1
View analyzer for us-east-1
Febuary 18, 2025, 10:40:04 (UTC+05:30)
23bd5a0516--1
US East (N. Virginia) us-east-1
View analyzer for us-east-1
Febuary 18, 2025, 10:27:17 (UTC+05:30)
23bd5a0516-1
US East (N. Virginia) us-east-1
View analyzer for us-east-1
Febuary 18, 2025, 10:25:08 (UTC+05:30)
23bd5a0516-3
US East (N. Virginia) us-east-1
View analyzer for us-east-1
Febuary 18, 2025, 10:36:29 (UTC+05:30)

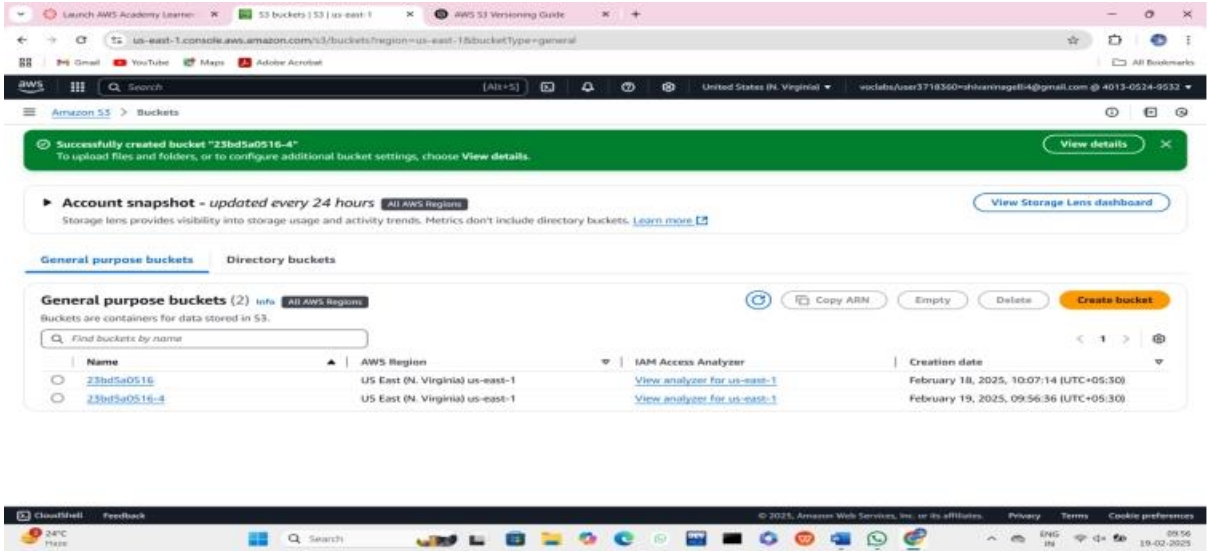
Bucket versioning:






Amazon S3 > Buckets > Create bucket
Buckets are containers for data stored in S3.
General configuration
AWS Region
US East (N. Virginia) us-east-1
Bucket type Info
General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
Directory
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
23bd5a0516-4
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Block public access to buckets and objects granted through new public bucket or access point policies
Block public and cross-account access to buckets and objects through any public bucket or access point policies
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disable
Enable
Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add tag
Default encryption Info
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Amazon S3 > Buckets
Successfully created bucket "23bd5a0516-4"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
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 (2) 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
23bd5a0516
US East (N. Virginia) us-east-1
View analyzer for us-east-1
February 18, 2025, 10:07:14 (UTC+05:30)
23bd5a0516-4
US East (N. Virginia) us-east-1
View analyzer for us-east-1
February 19, 2025, 09:56:36 (UTC+05:30)
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences