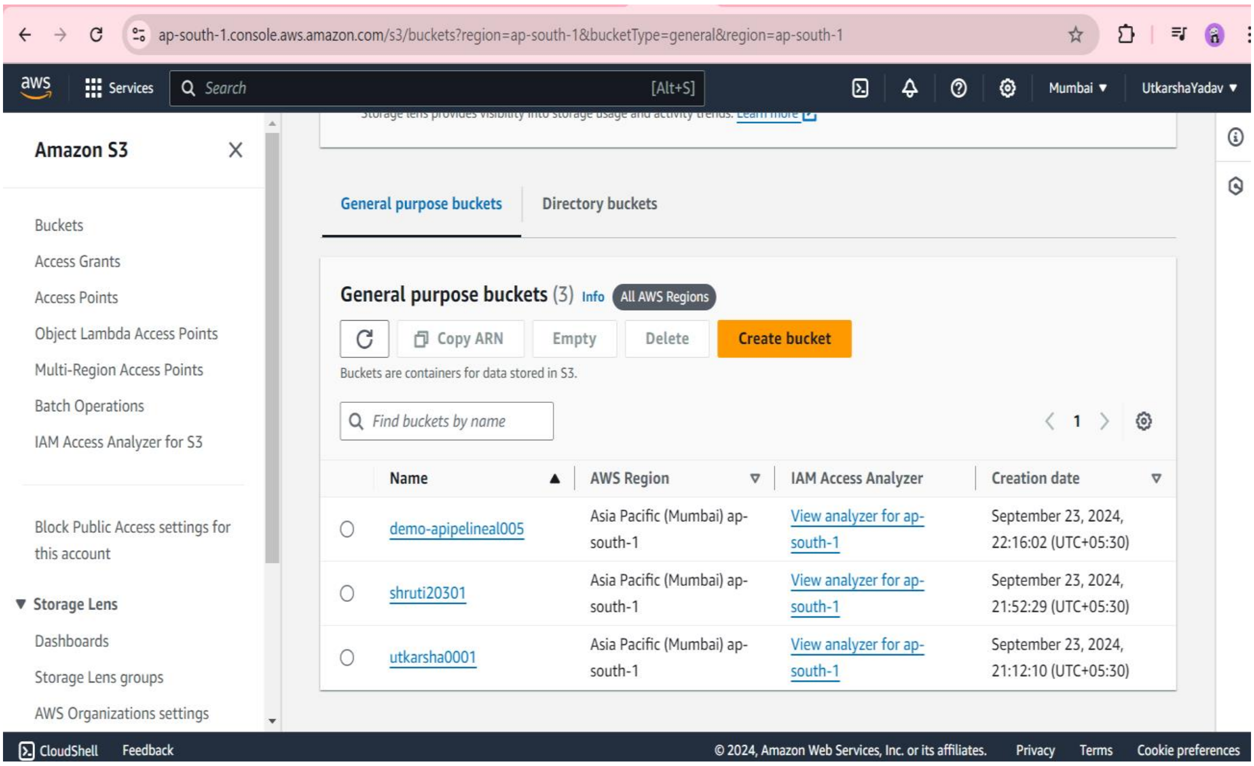
Assignment 4 Topic S3 Public bucket and private bucket

Create a private bucket and add a object.

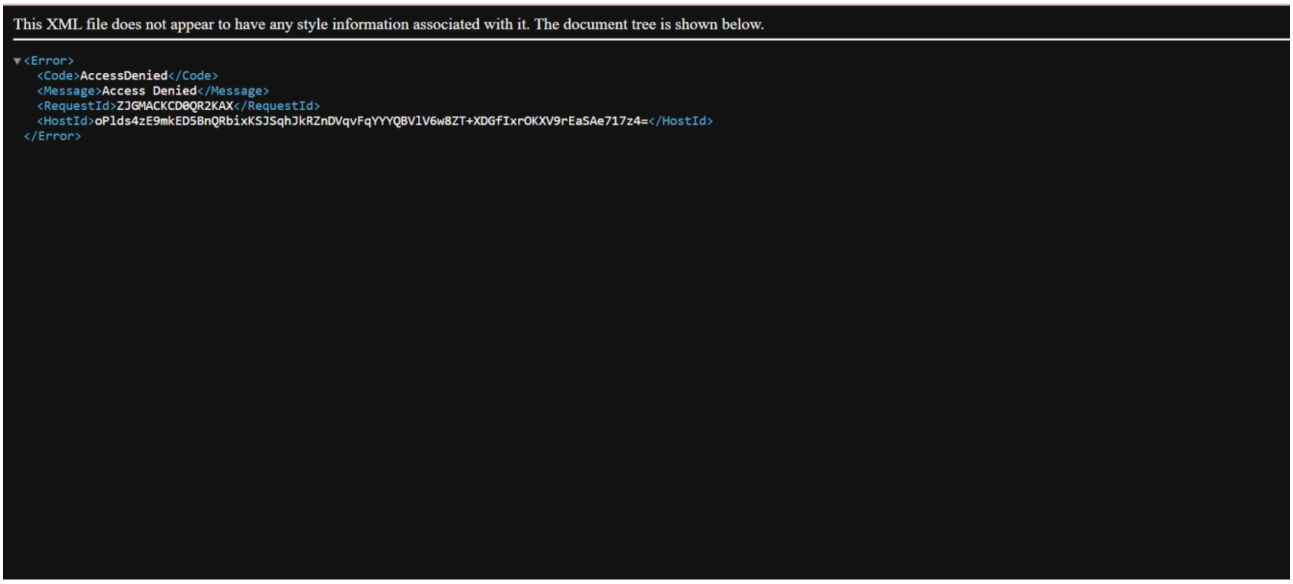


General purpose buckets (3)

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	demo-apipelineal005	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	September 23, 2024, 22:16:02 (UTC+05:30)
○	shruti20301	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	September 23, 2024, 21:52:29 (UTC+05:30)
○	utkarsha0001	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	September 23, 2024, 21:12:10 (UTC+05:30)

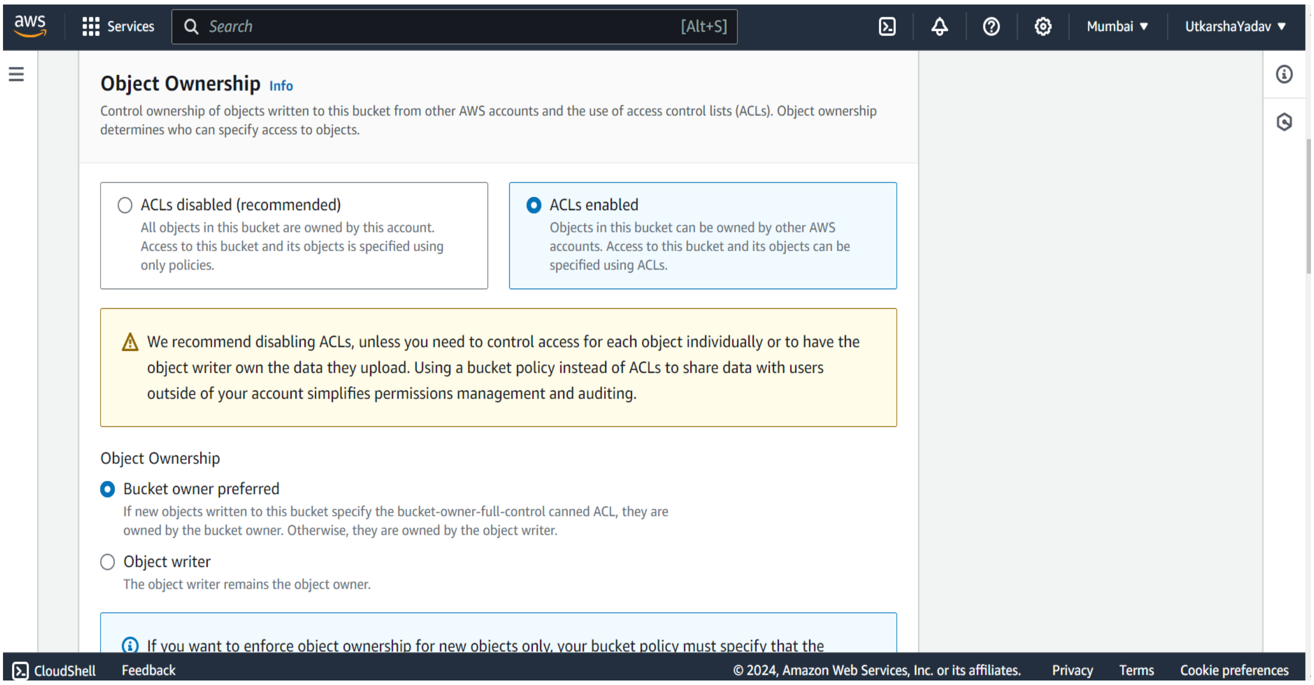
Object is not access-able, we need to provide permission to make private object public.



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>ZJGMACKCD0QR2KAX</RequestId>
   <HostId>oPlds4zE9mkED5BnQRbixKSJSqhJkRZnDVqvFqYYYQBVlV6w8ZT+XDGfIxrOKXV9rEaSAe717z4=</HostId>
 </Error>
```

Create new bucket and change permissions to make it public



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.

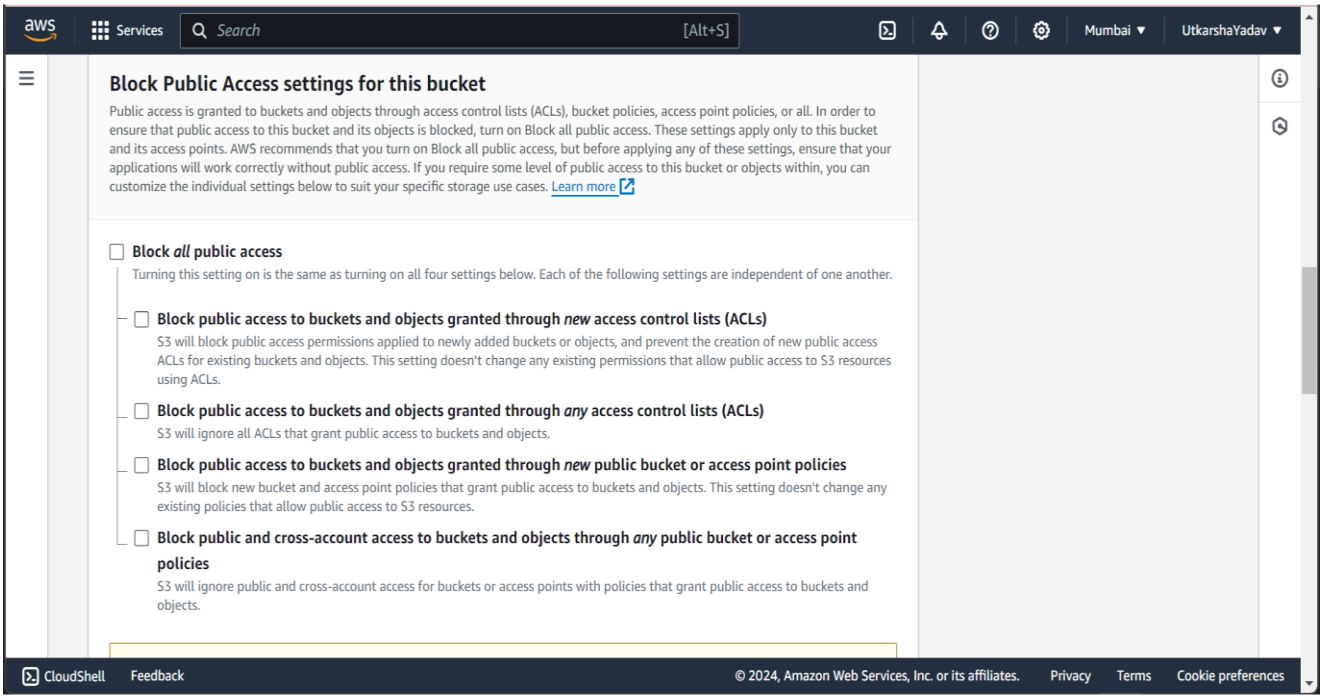
Object Ownership

● 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.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the

Unchecked all- Block all public access and create bucket



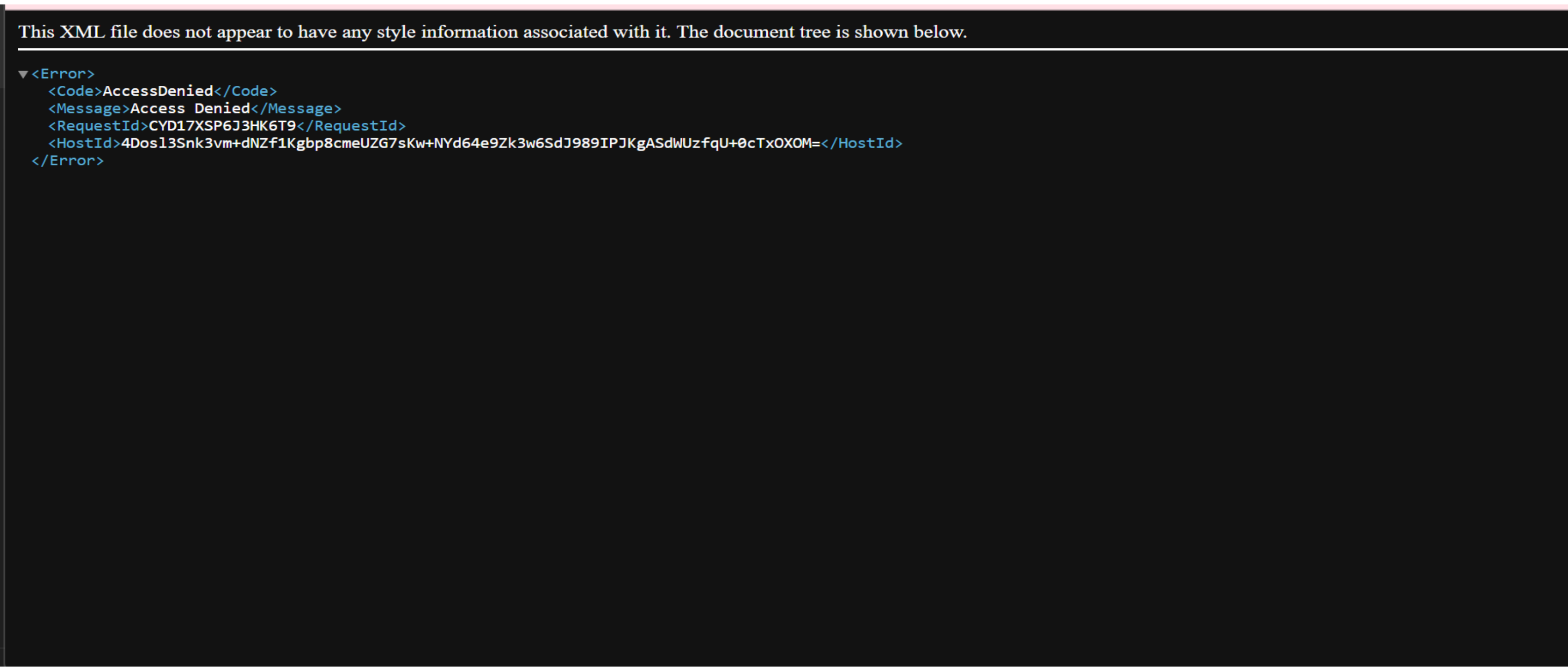
Block Public Access settings for this bucket

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.

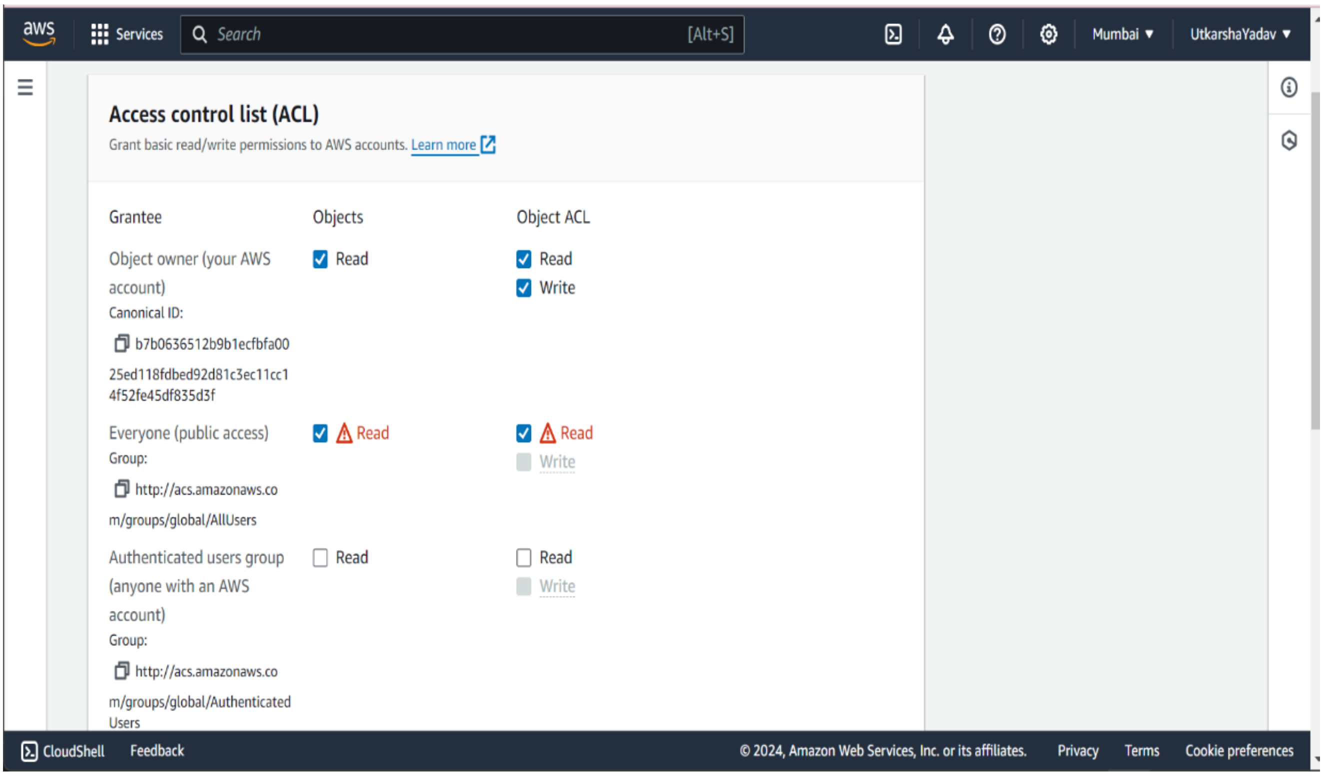
Add object to bucket and check the url of object it is still not access able, so to make object public we need give permissions to object.



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>CYD17XSP6J3HK6T9</RequestId>
   <HostId>4Dosl3Snk3vm+dNZf1Kgbp8cmeUZG7sKw+NYd64e9Zk3w6SdJ989IPJKgASdWUzfqU+0cTxOXOM=</HostId>
 </Error>
```

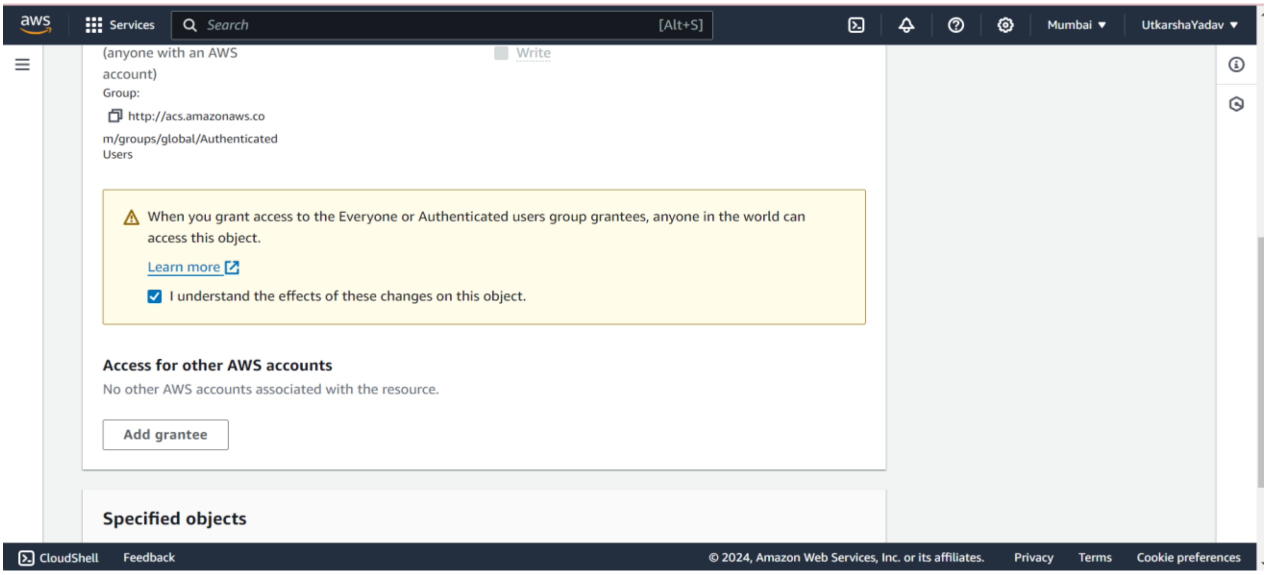
Give permission to Object by check read (everyone(public)) access



Access control list (ACL)

Grant basic read/write permissions to AWS accounts. Learn more

Grantee	Objects	Object ACL
Object owner (your AWS account) Canonical ID: b7b0636512b9b1ecfbfa0025ed118fdbed92d81c3ec11cc14f52fe45df835d3f	☑ Read	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	☑ ⚠ Read	☑ ⚠ Read □ Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	□ Read	□ Read □ Write



(anyone with an AWS account)
Group:
http://acs.amazonaws.com/groups/global/AuthenticatedUsers

□ Write

When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.

Learn more

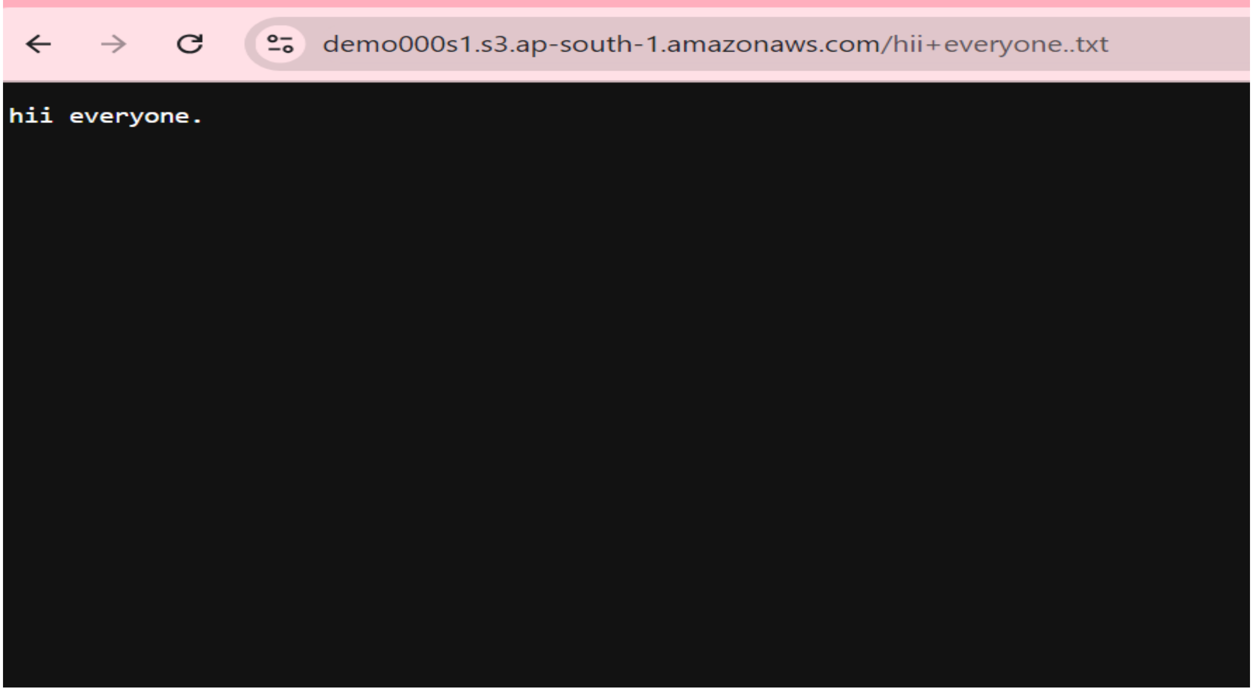
☑ I understand the effects of these changes on this object.

Access for other AWS accounts

No other AWS accounts associated with the resource.

Specified objects

Now object is public



demo000s1.s3.ap-south-1.amazonaws.com/hii+everyone..txt

```
hii everyone.
```