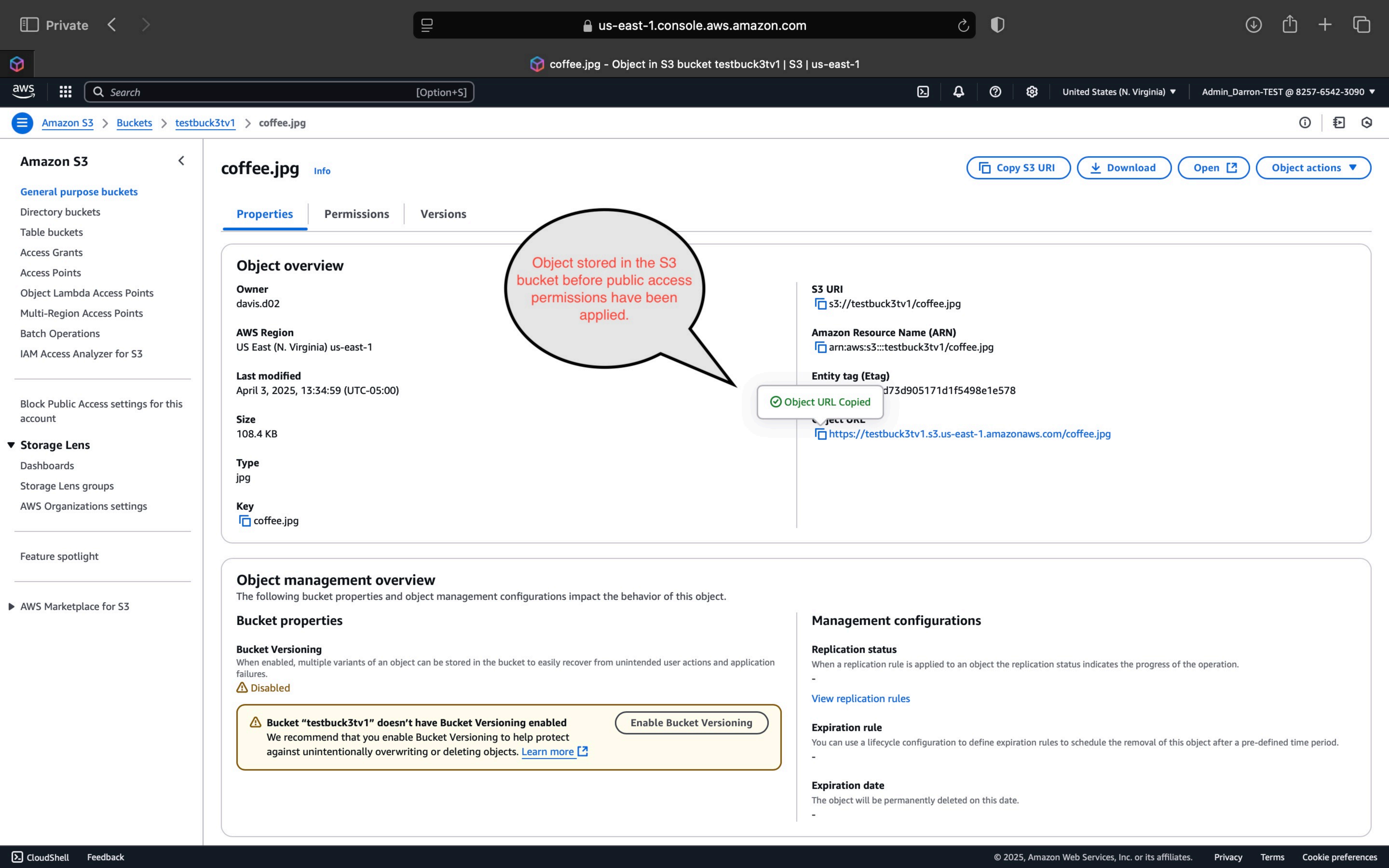


Private
us-east-1.console.aws.amazon.com
coffee.jpg - Object in S3 bucket testbuck3tv1 | S3 | us-east-1
aws
Search
[Option+S]
United States (N. Virginia) ▼
Admin_Darron-TEST @ 8257-6542-3090 ▼
Amazon S3 > Buckets > testbuck3tv1 > coffee.jpg
Amazon S3
General purpose buckets
Directory buckets
Table buckets
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
▶ AWS Marketplace for S3
Copy S3 URI
Download
Open
Object actions ▼
Properties
Permissions
Versions

coffee.jpg Info

Object stored in the S3 bucket before public access permissions have been applied.

Object overview

Owner
davis.d02

AWS Region
US East (N. Virginia) us-east-1

Last modified
April 3, 2025, 13:34:59 (UTC-05:00)

Size
108.4 KB

Type
jpg

Key
coffee.jpg

S3 URI
s3://testbuck3tv1/coffee.jpg

Amazon Resource Name (ARN)
arn:aws:s3:::testbuck3tv1/coffee.jpg

Entity tag (Etag)
d73d905171d1f5498e1e578

Object URL Copied

ject URL
https://testbuck3tv1.s3.us-east-1.amazonaws.com/coffee.jpg

Object management overview

The following bucket properties and object management configurations impact the behavior of this object.

Bucket properties

Bucket Versioning
When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures.
⚠ Disabled

⚠ **Bucket “testbuck3tv1” doesn’t have Bucket Versioning enabled**
We recommend that you enable Bucket Versioning to help protect against unintentionally overwriting or deleting objects. Learn more

Enable Bucket Versioning

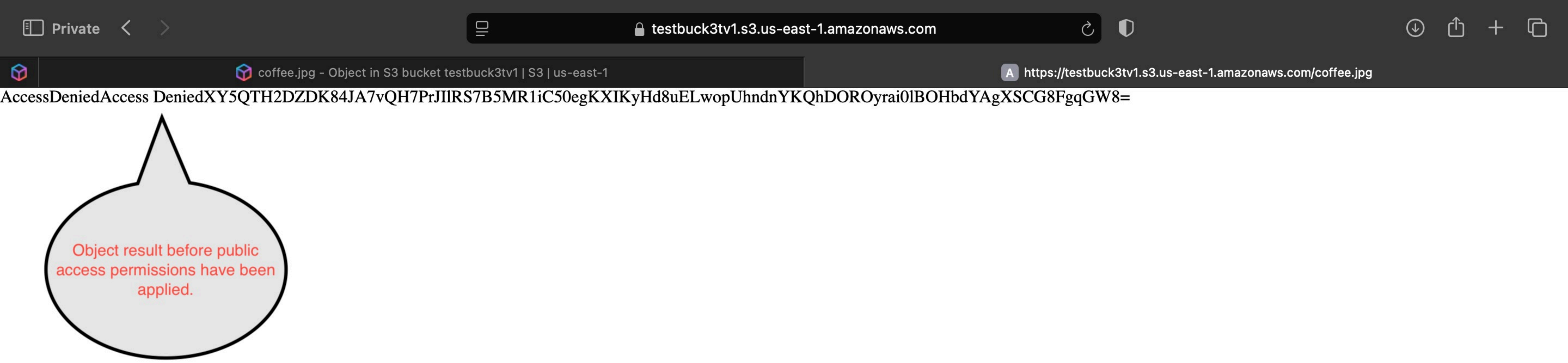
Management configurations

Replication status
When a replication rule is applied to an object the replication status indicates the progress of the operation.
-

View replication rules

Expiration rule
You can use a lifecycle configuration to define expiration rules to schedule the removal of this object after a pre-defined time period.
-

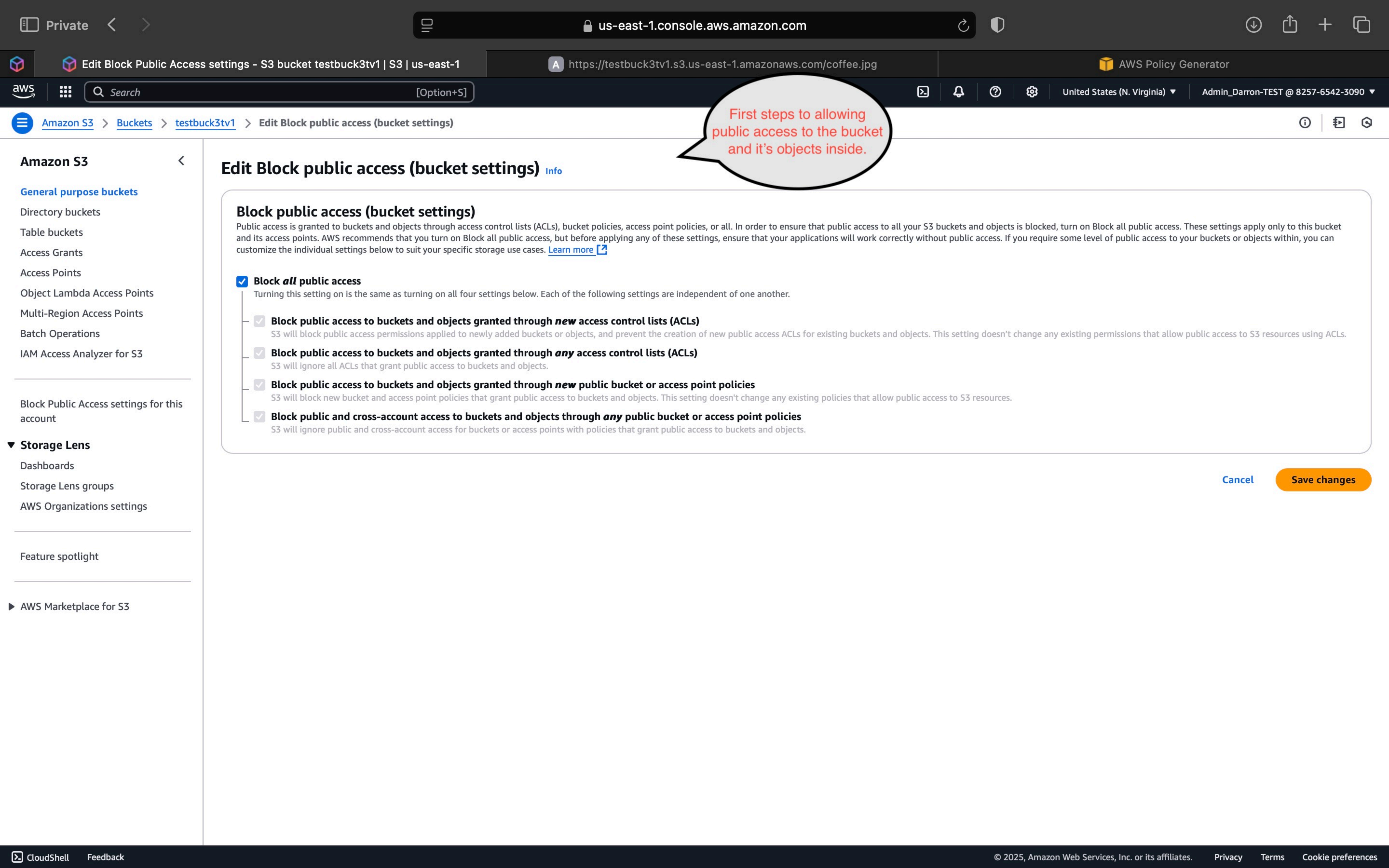
Expiration date
The object will be permanently deleted on this date.
-



Private
testbuck3tv1.s3.us-east-1.amazonaws.com
coffee.jpg - Object in S3 bucket testbuck3tv1 | S3 | us-east-1
https://testbuck3tv1.s3.us-east-1.amazonaws.com/coffee.jpg

```
AccessDeniedAccess DeniedXY5QTH2DZDK84JA7vQH7PrJIlRS7B5MR1iC50egKXIKyHd8uELwopUhndnYKQhDOROyrai0lBOHbdYAgXSCG8FgqGW8=
```

Object result before public access permissions have been applied.



Private
us-east-1.console.aws.amazon.com
Edit Block Public Access settings - S3 bucket testbuck3tv1 | S3 | us-east-1
https://testbuck3tv1.s3.us-east-1.amazonaws.com/coffee.jpg
AWS Policy Generator
Search
[Option+S]
United States (N. Virginia) ▼
Admin_Darron-TEST @ 8257-6542-3090 ▼
Amazon S3 > Buckets > testbuck3tv1 > Edit Block public access (bucket settings)
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
AWS Marketplace for S3

First steps to allowing public access to the bucket and it's objects inside.

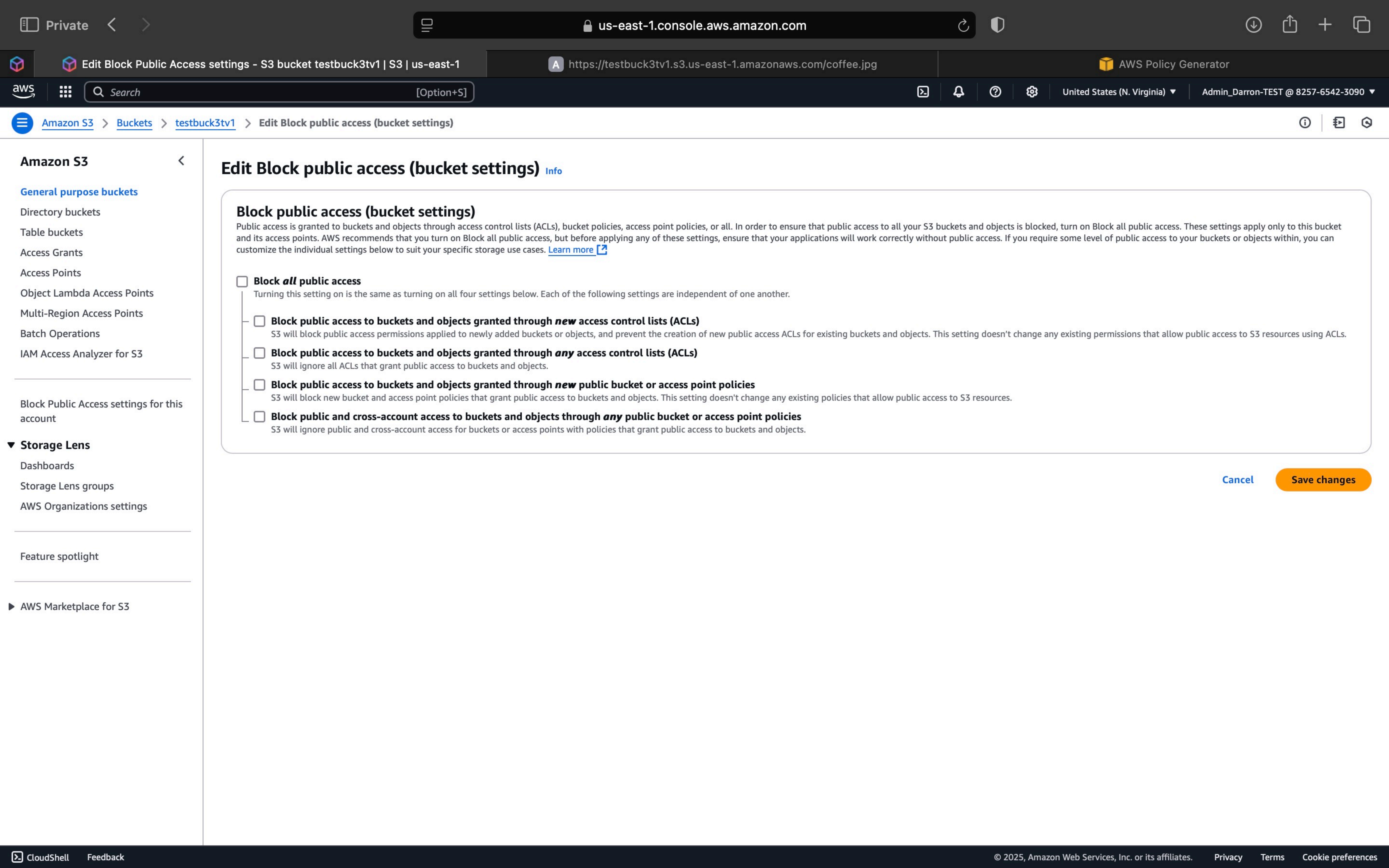
Edit Block public access (bucket settings) Info

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.


Private
us-east-1.console.aws.amazon.com
Edit Block Public Access settings - S3 bucket testbuck3tv1 | S3 | us-east-1
https://testbuck3tv1.s3.us-east-1.amazonaws.com/coffee.jpg
AWS Policy Generator
Search
[Option+S]
United States (N. Virginia)
Admin_Darron-TEST @ 8257-6542-3090
Amazon S3 > Buckets > testbuck3tv1 > Edit Block public access (bucket settings)
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
AWS Marketplace for S3

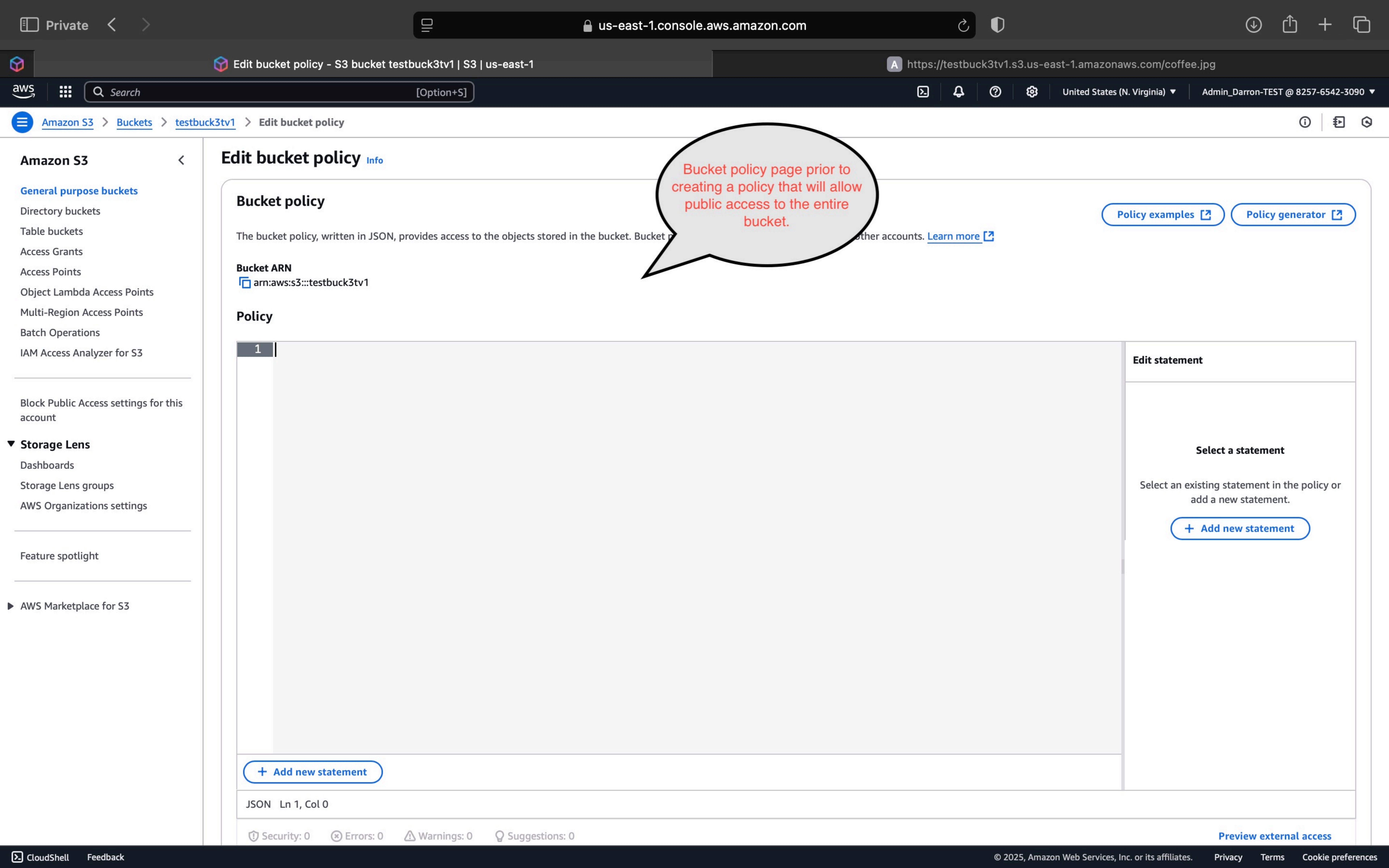
Edit Block public access (bucket settings) Info

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.



Bucket policy page prior to creating a policy that will allow public access to the entire bucket.

Edit bucket policy

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket p other accounts. Learn more

Bucket ARN

arn:aws:s3:::testbuck3tv1

Policy

```
1
```

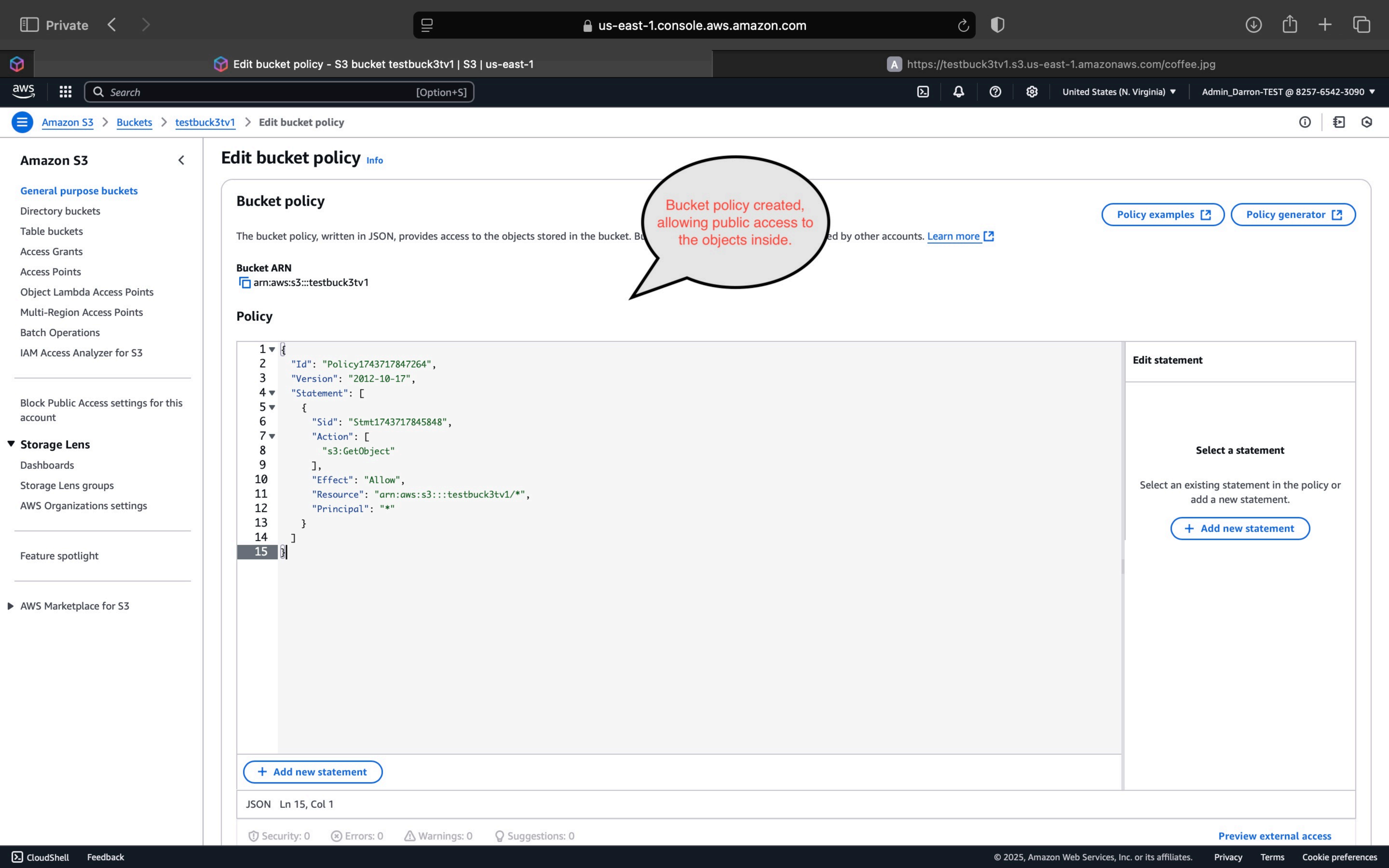
JSON Ln 1, Col 0

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

Private
us-east-1.console.aws.amazon.com
Edit bucket policy - S3 bucket testbuck3tv1 | S3 | us-east-1
https://testbuck3tv1.s3.us-east-1.amazonaws.com/coffee.jpg
aws
Search
[Option+S]
United States (N. Virginia)
Admin_Darron-TEST @ 8257-6542-3090
Amazon S3 > Buckets > testbuck3tv1 > 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
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Info
Policy examples
Policy generator
+ Add new statement
+ Add new statement
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Preview external access
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Private
us-east-1.console.aws.amazon.com
Edit bucket policy - S3 bucket testbuck3tv1 | S3 | us-east-1
https://testbuck3tv1.s3.us-east-1.amazonaws.com/coffee.jpg
Search
[Option+S]
United States (N. Virginia)
Admin_Darron-TEST @ 8257-6542-3090
Amazon S3 > Buckets > testbuck3tv1 > 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
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Policy examples
Policy generator
Edit statement
Add new statement
Add new statement
Preview external access
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Bucket policy created, allowing public access to the objects inside.

Edit bucket policy Info

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bu ed by other accounts. Learn more

Bucket ARN

arn:aws:s3:::testbuck3tv1

Policy

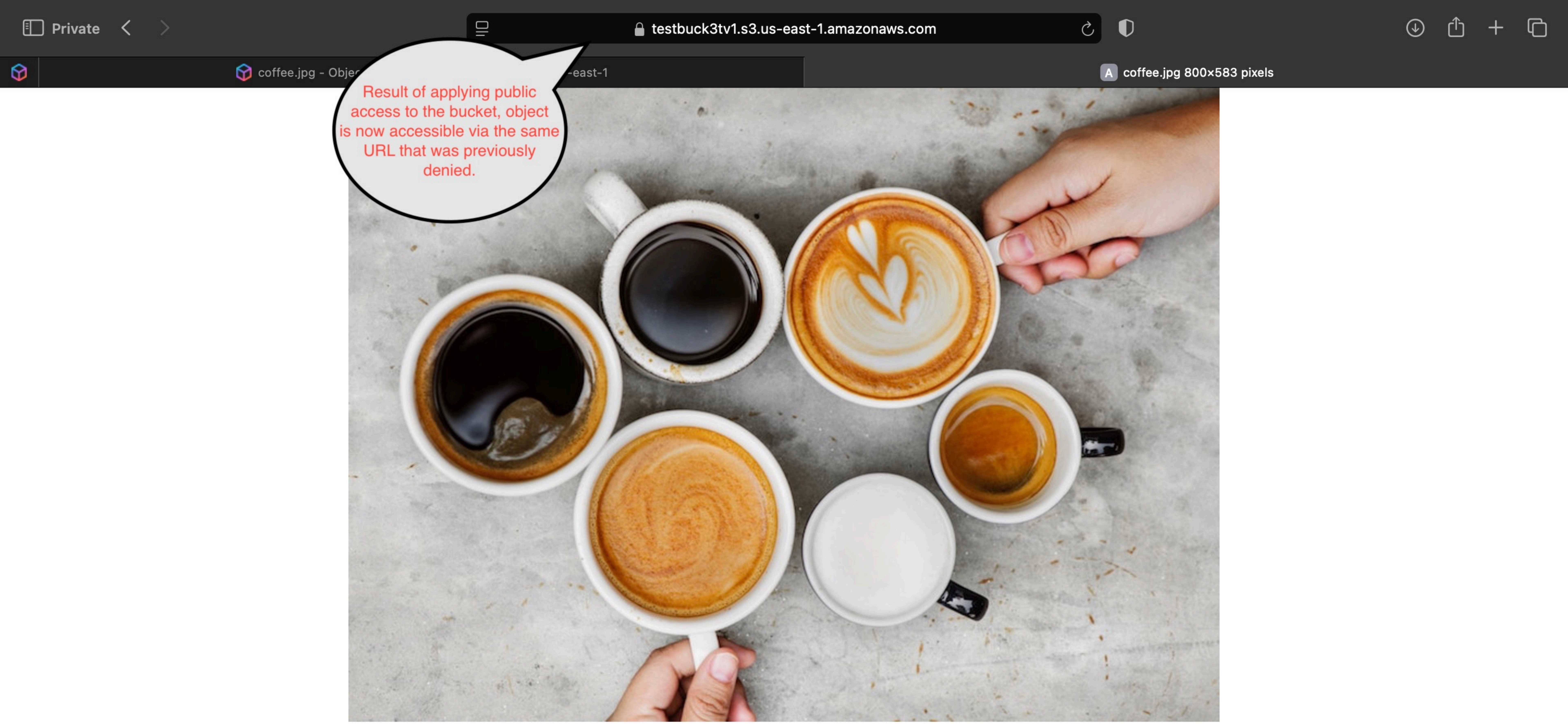
```
{
  "Id": "Policy1743717847264",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1743717845848",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::testbuck3tv1/*",
      "Principal": "*"
    }
  ]
}
```

Select a statement

Select an existing statement in the policy or add a new statement.

JSON Ln 15, Col 1

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0


Private
testbuck3tv1.s3.us-east-1.amazonaws.com
coffee.jpg - Objec
-east-1
coffee.jpg 800×583 pixels

Result of applying public access to the bucket, object is now accessible via the same URL that was previously denied.