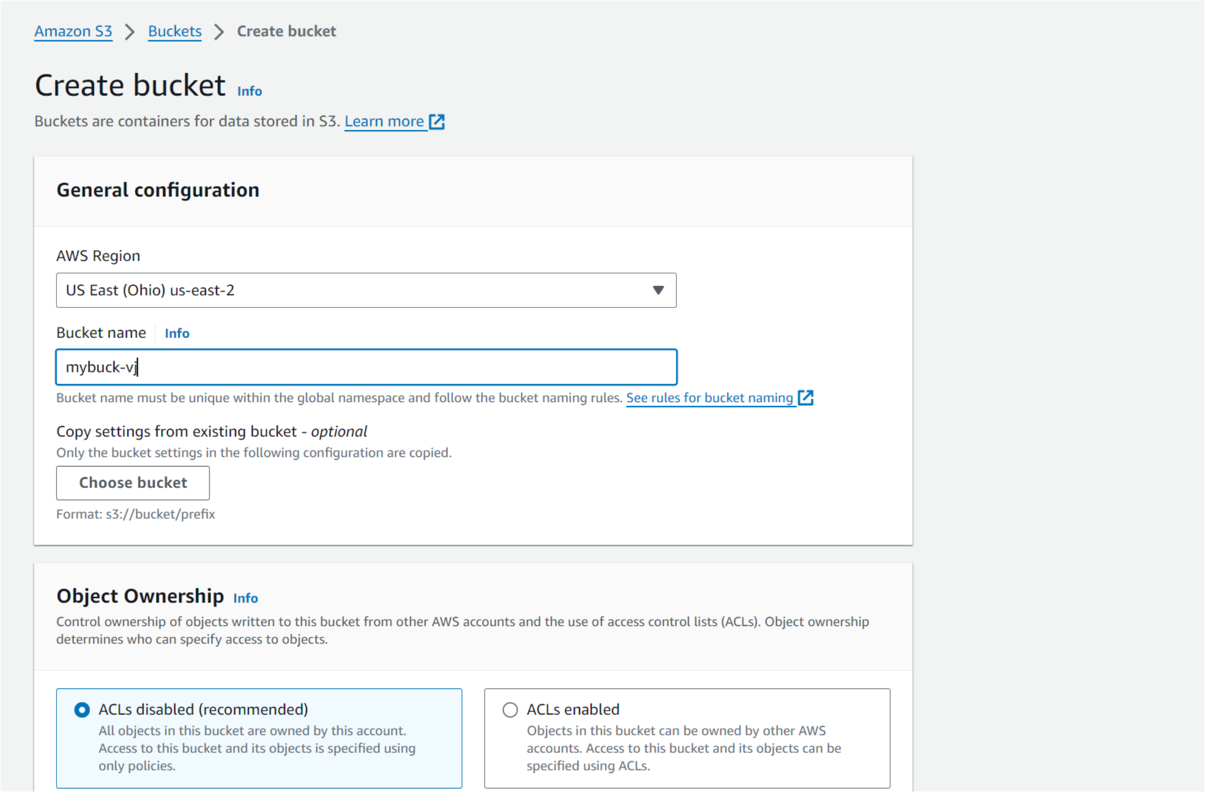
Step1:



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

AWS Region

US East (Ohio) us-east-2

Bucket name Info

mybuck-vj

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.

Format: s3://bucket/prefix

Object Ownership Info

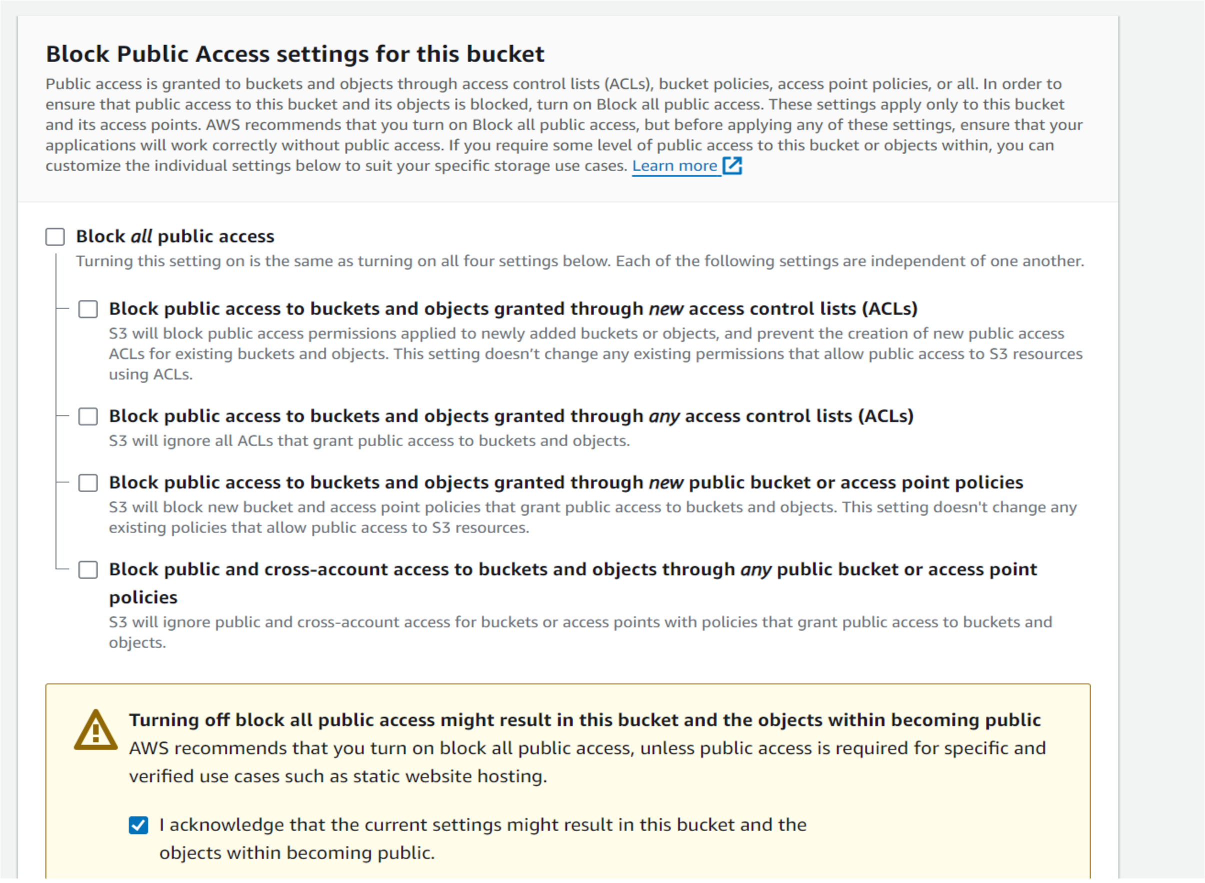
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● 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.

Step2:

Uncheck the block public access



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

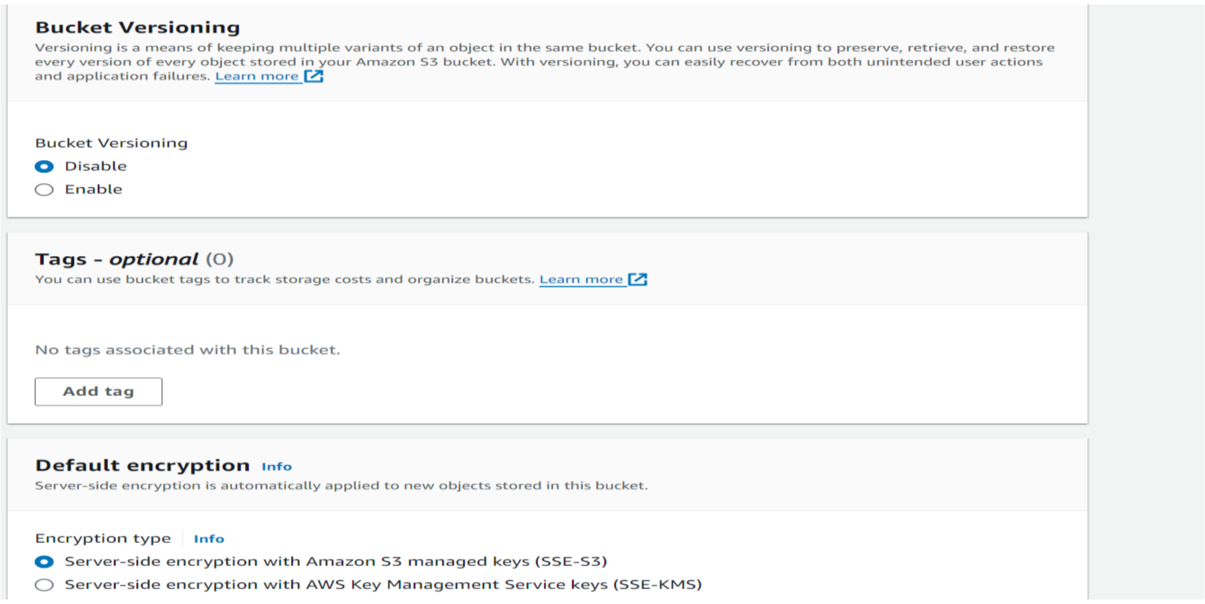
☐ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **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.

Ste3:



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

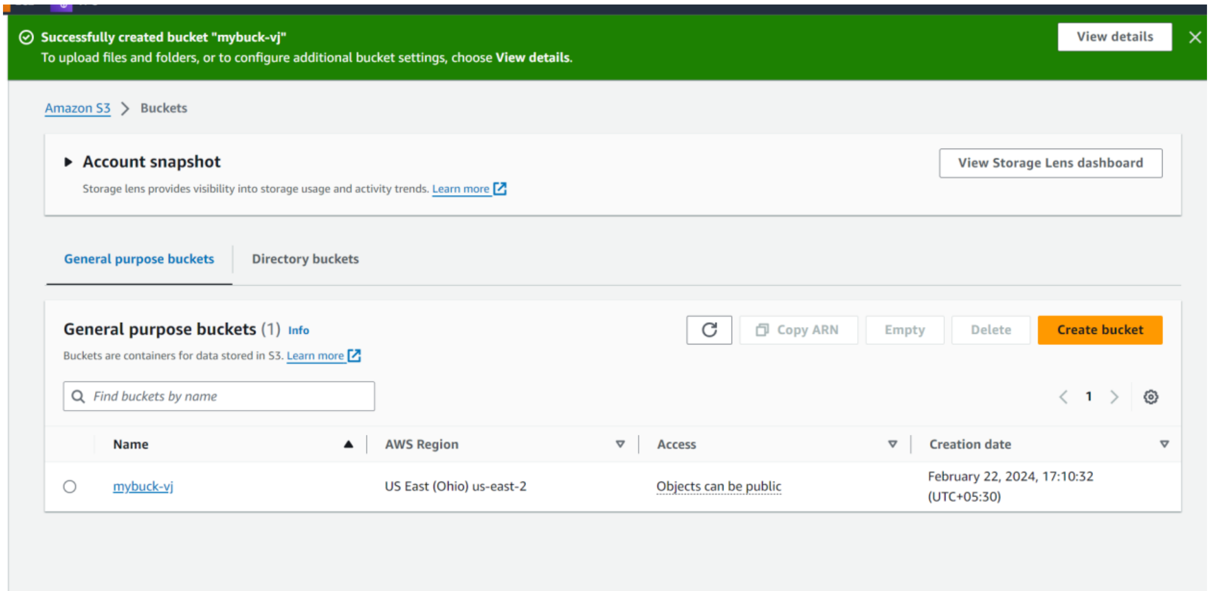
No tags associated with this bucket.

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)

Step4:



Successfully created bucket "mybuck-vj"

To upload files and folders, or to configure additional bucket settings, choose **View details**.

Amazon S3 > Buckets

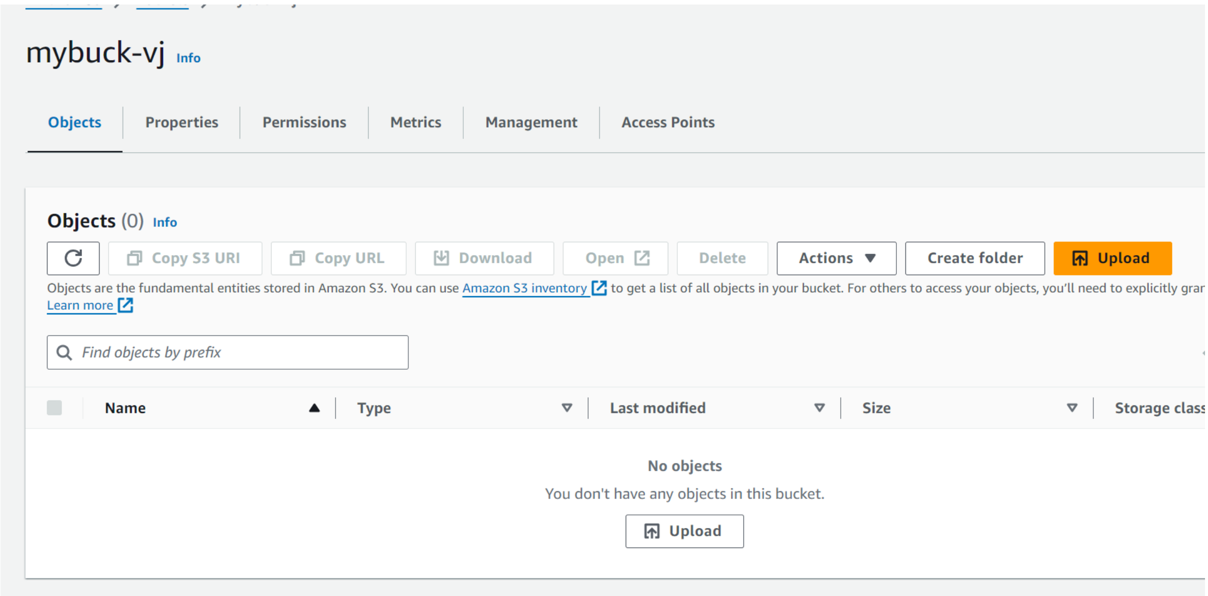
Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info

Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date
○ mybuck-vj	US East (Ohio) us-east-2	Objects can be public	February 22, 2024, 17:10:32 (UTC+05:30)



mybuck-vj Info

Objects (0) Info

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 grar

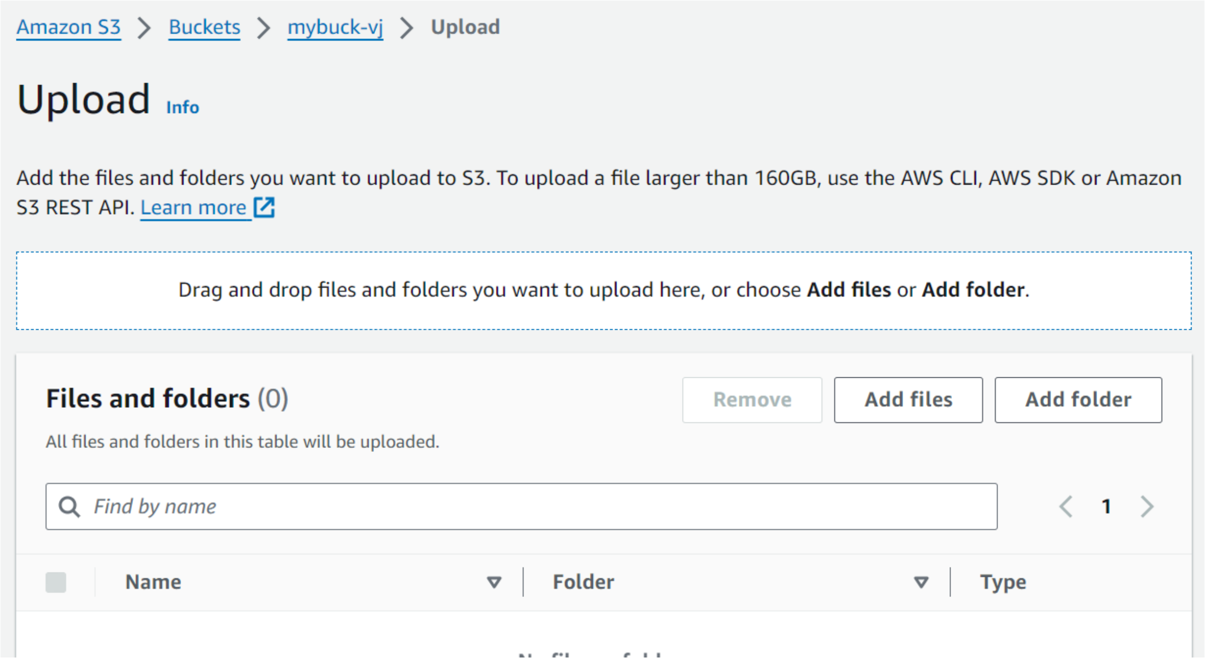
Learn more

Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

Step 5: upload files & folders



Amazon S3 > Buckets > mybuck-vj > Upload

Upload Info

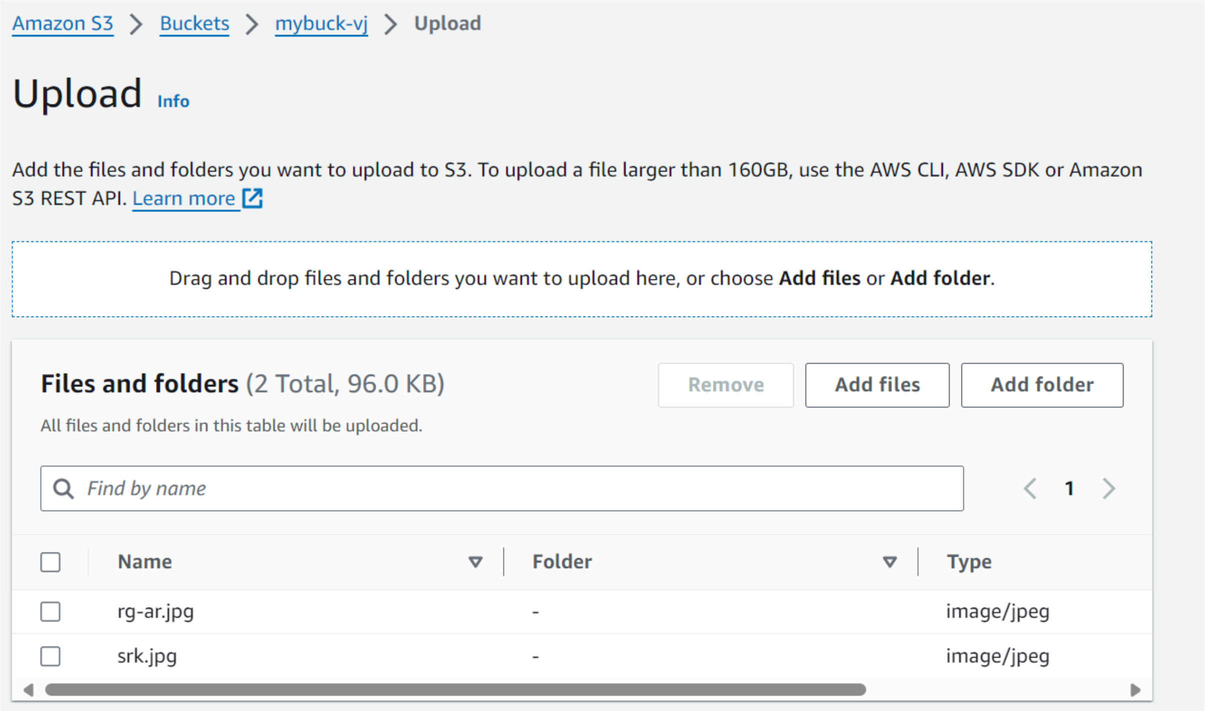
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

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.

□	Name	Folder	Type



Amazon S3 > Buckets > mybuck-vj > Upload

Upload Info

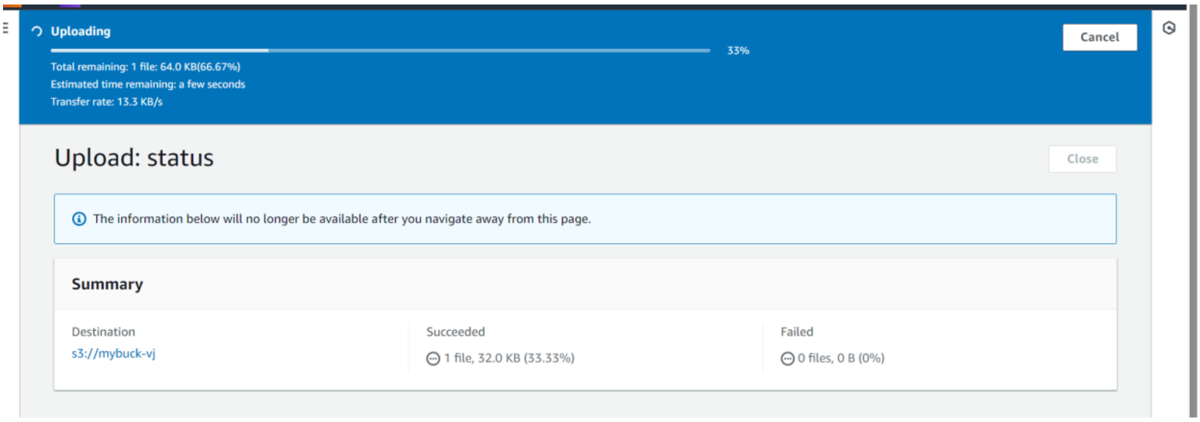
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (2 Total, 96.0 KB)

All files and folders in this table will be uploaded.

□	Name	Folder	Type
□	rg-ar.jpg	-	image/jpeg
□	srk.jpg	-	image/jpeg



Uploading

33%

Total remaining: 1 file: 64.0 KB(66.67%)
Estimated time remaining: a few seconds
Transfer rate: 13.3 KB/s

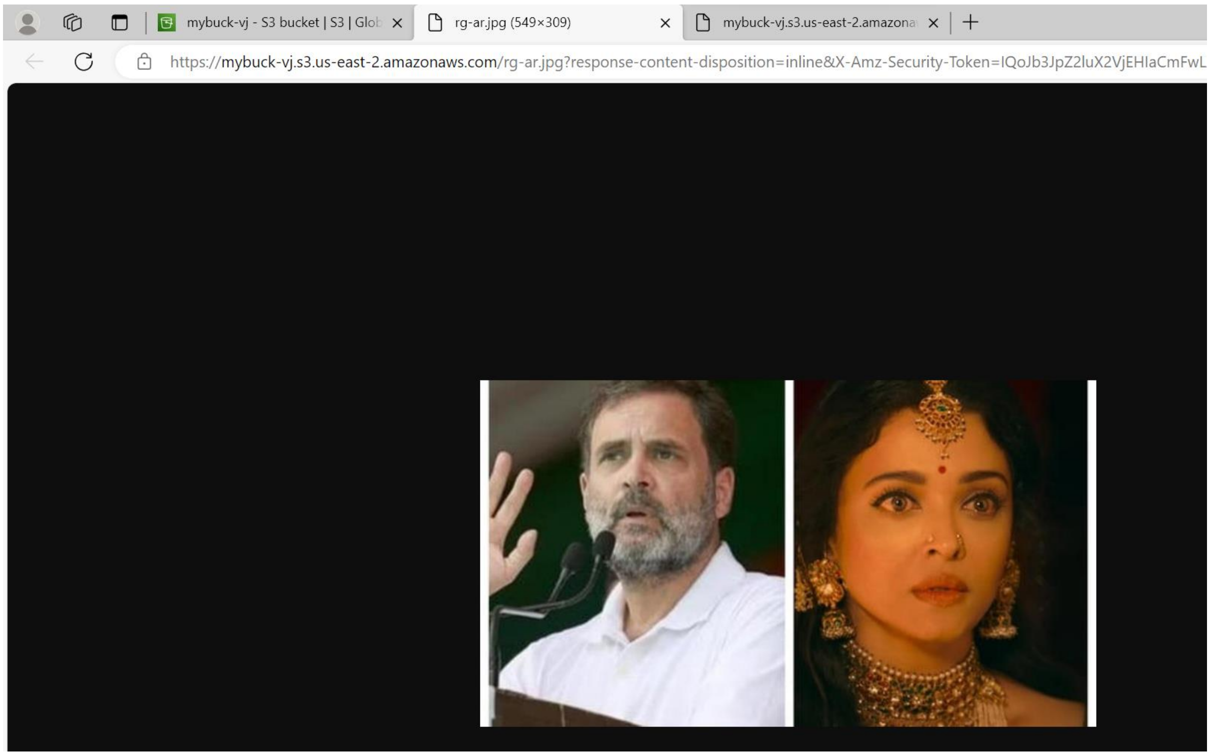
Upload: status

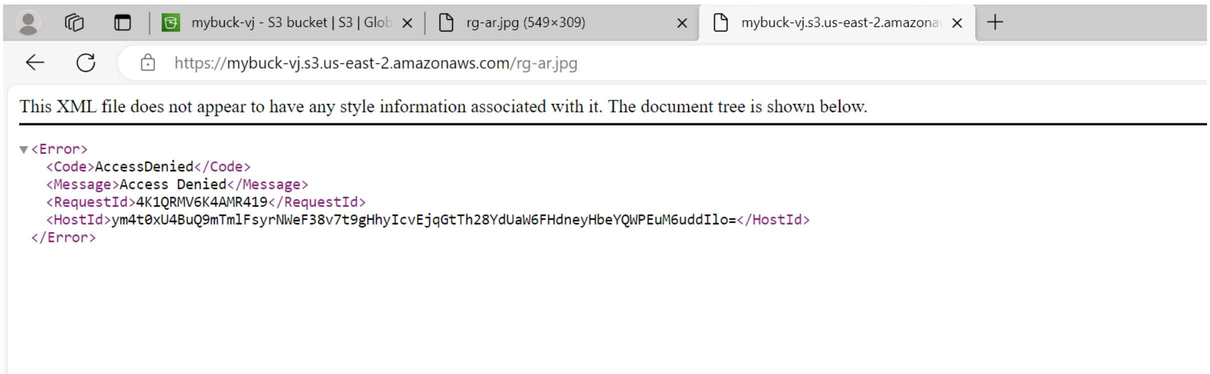
The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://mybuck-vj	1 file, 32.0 KB (33.33%)	0 files, 0 B (0%)

Step 6: now direct **OPEN** the image , it opens but try to copy the ARN nn give it in new tab ..it show error ...

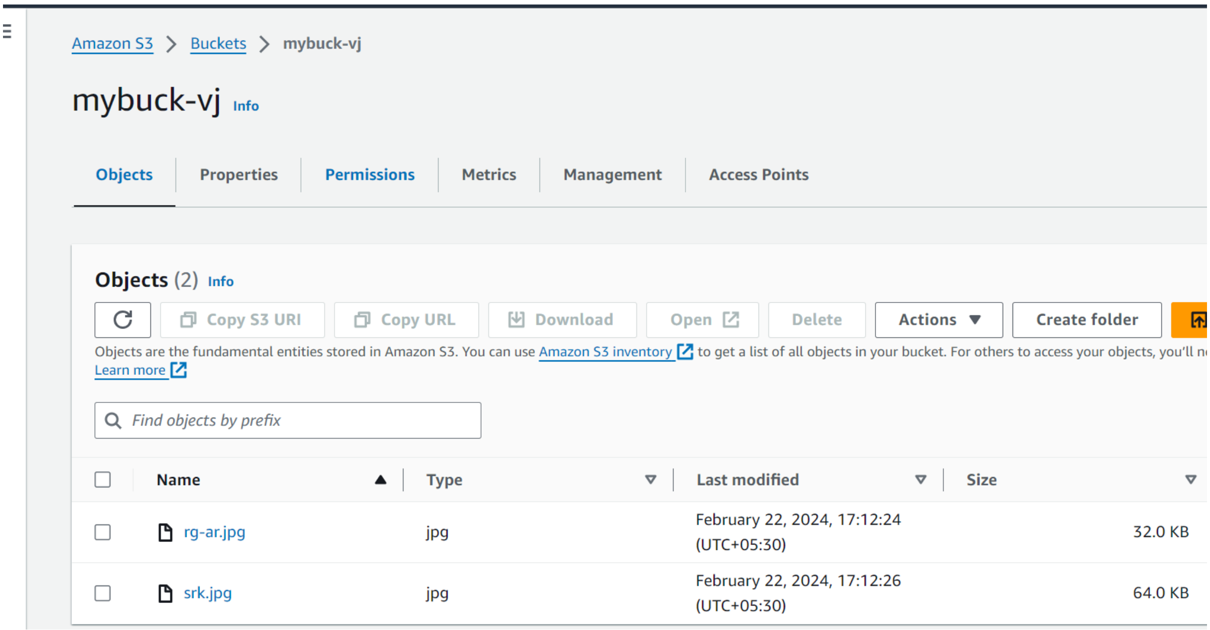

mybuck-vj - S3 bucket | S3 | Glob
rg-ar.jpg (549×309)
mybuck-vj.s3.us-east-2.amazona
https://mybuck-vj.s3.us-east-2.amazonaws.com/rg-ar.jpg?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEHIaCmFwL


mybuck-vj - S3 bucket | S3 | Glob
rg-ar.jpg (549×309)
mybuck-vj.s3.us-east-2.amazona
https://mybuck-vj.s3.us-east-2.amazonaws.com/rg-ar.jpg

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>4K1QRMV6K4AMR419</RequestId>
   <HostId>ym4t0xU4BuQ9mTmlFsyrNWeF38v7t9gHhyIcvEjqGtTh28YdUaW6FHdneyHbeYQWPEuM6uddIlo=</HostId>
 </Error>
```

*** Step 7:**POLICY GENERATOR**



mybuck-vj

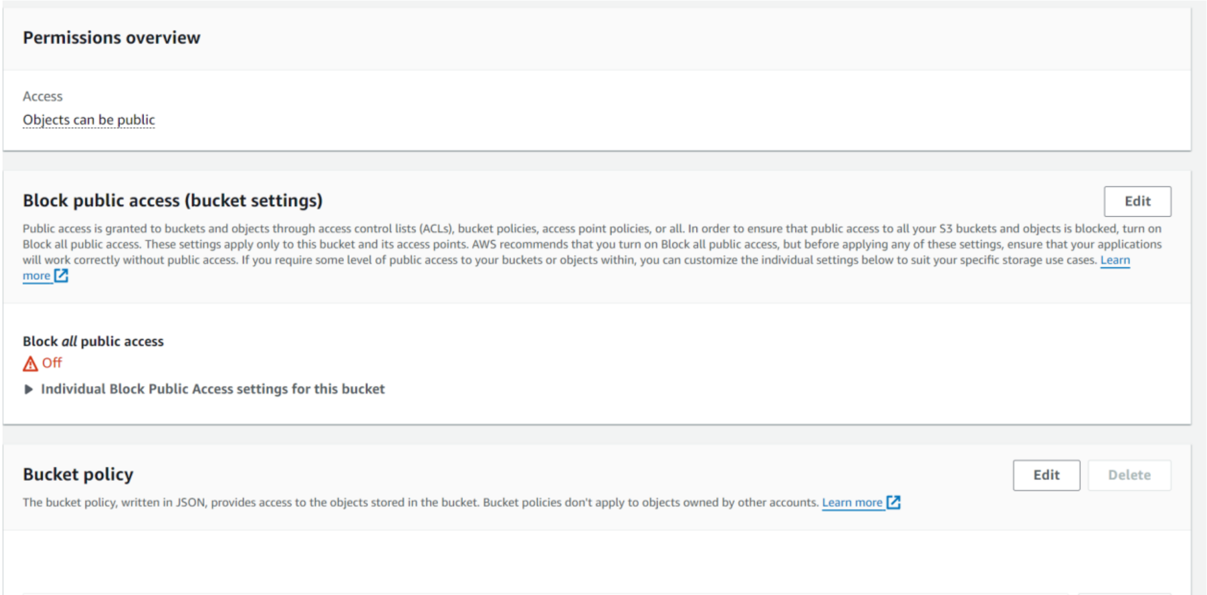
Objects (2)

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 n
Learn more

Find objects by prefix

□	Name ▲	Type	Last modified	Size
□	rg-ar.jpg	jpg	February 22, 2024, 17:12:24 (UTC+05:30)	32.0 KB
□	srk.jpg	jpg	February 22, 2024, 17:12:26 (UTC+05:30)	64.0 KB

Goto permissions



Permissions overview

Access
Objects can be public

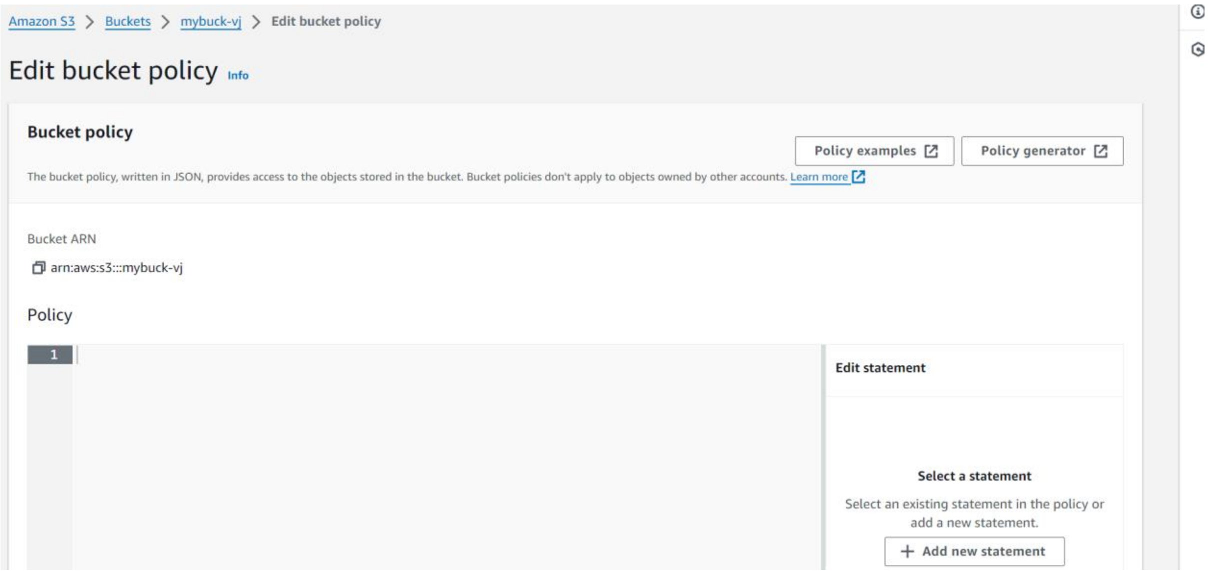
Block public access (bucket settings)

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
⚠ Off
▶ Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more



Amazon S3 > Buckets > mybuck-vj > Edit bucket policy

Edit bucket policy Info

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Bucket ARN

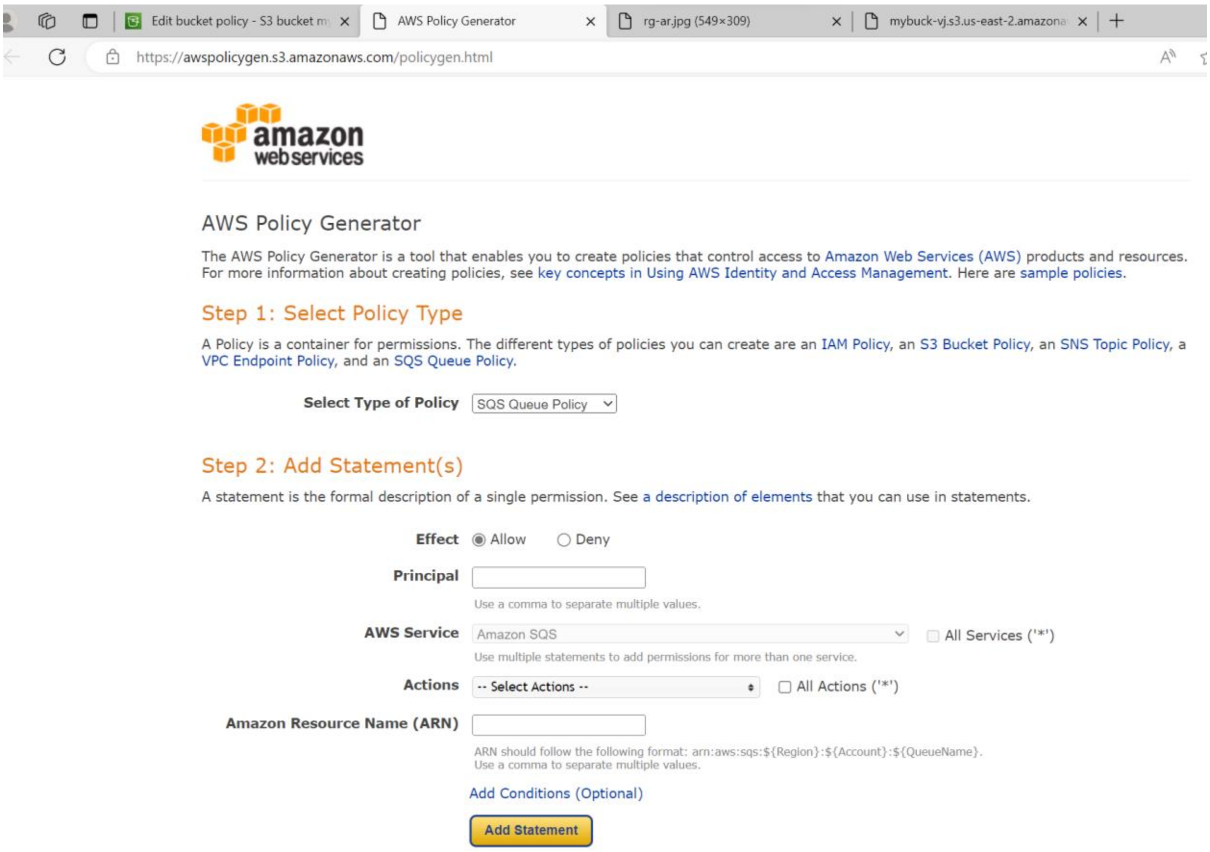
arn:aws:s3:::mybuck-vj

Policy

Edit statement

Select a statement

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



https://awspolicygen.s3.amazonaws.com/policygen.html

Edit bucket policy - S3 bucket m
AWS Policy Generator
rg-ar.jpg (549×309)
mybuck-vj.s3.us-east-2.amazona
amazon webservices

AWS Policy Generator

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

Step 1: Select Policy Type

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

Select Type of Policy: SQS Queue Policy

Step 2: Add Statement(s)

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

Effect ● Allow ○ Deny

Principal

Use a comma to separate multiple values.

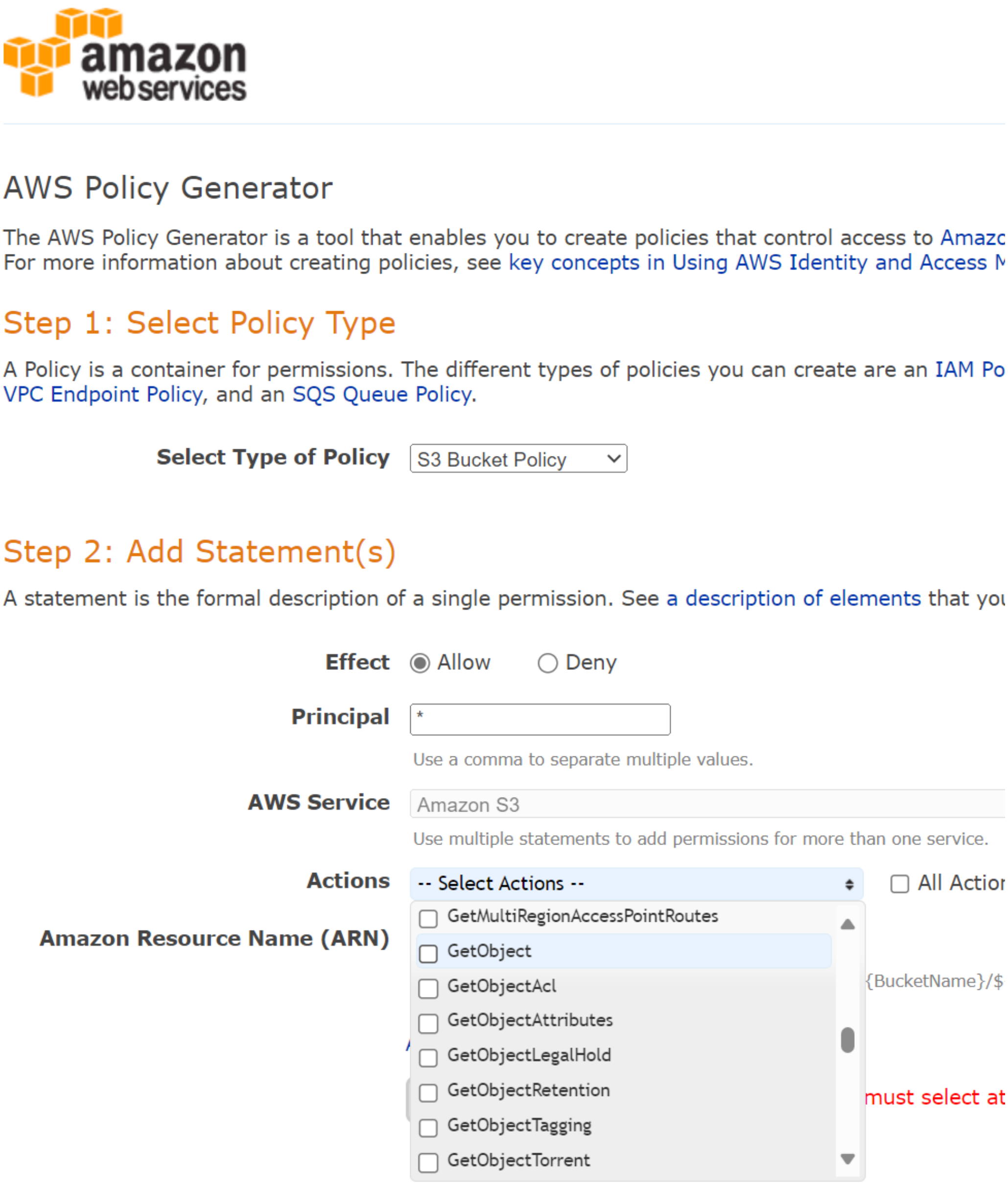
AWS Service: Amazon SQS □ All Services ('*')

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

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

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:sqs:${Region}:${Account}:${QueueName}. Use a comma to separate multiple values.



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazc
For more information about creating policies, see key concepts in Using AWS Identity and Access M

Step 1: Select Policy Type

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

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you

Effect ● Allow ○ Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3

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

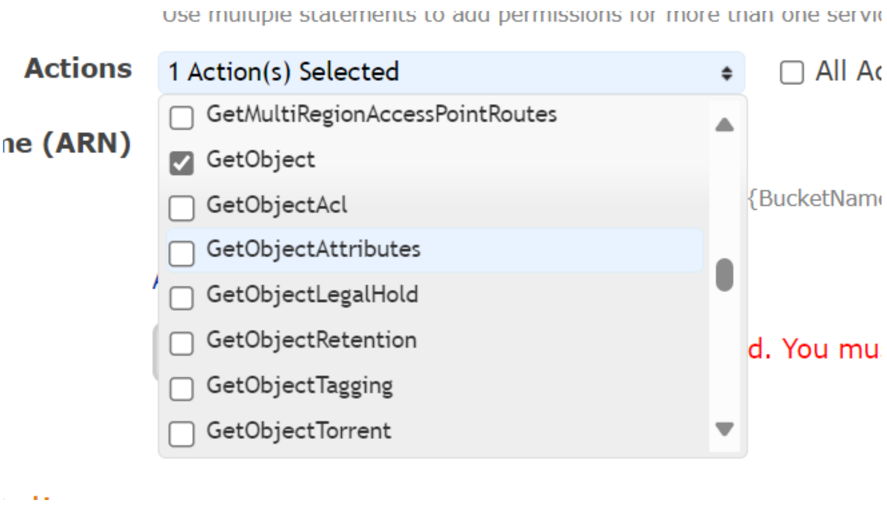
Actions -- Select Actions -- □ All Action

Amazon Resource Name (ARN)

□ GetMultiRegionAccessPointRoutes
□ GetObject
□ GetObjectAcl
□ GetObjectAttributes
□ GetObjectLegalHold
□ GetObjectRetention
□ GetObjectTagging
□ GetObjectTorrent

{BucketName}/$

must select at



Use multiple statements to add permissions for more than one servi

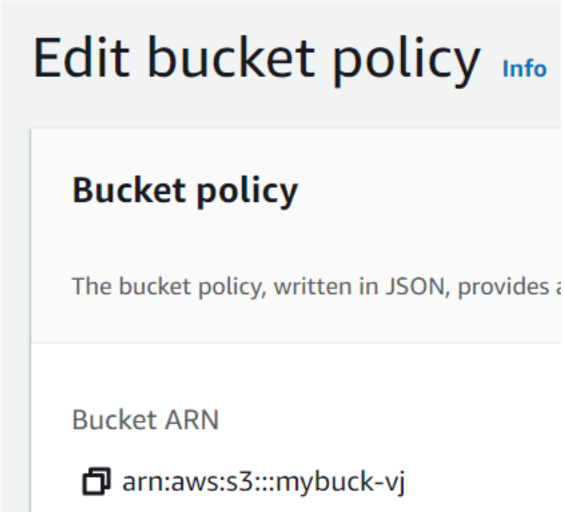
Actions 1 Action(s) Selected □ All Ac

ne (ARN)

□ GetMultiRegionAccessPointRoutes
☑ GetObject
□ GetObjectAcl
□ GetObjectAttributes
□ GetObjectLegalHold
□ GetObjectRetention
□ GetObjectTagging
□ GetObjectTorrent

{BucketNam

d. You mu



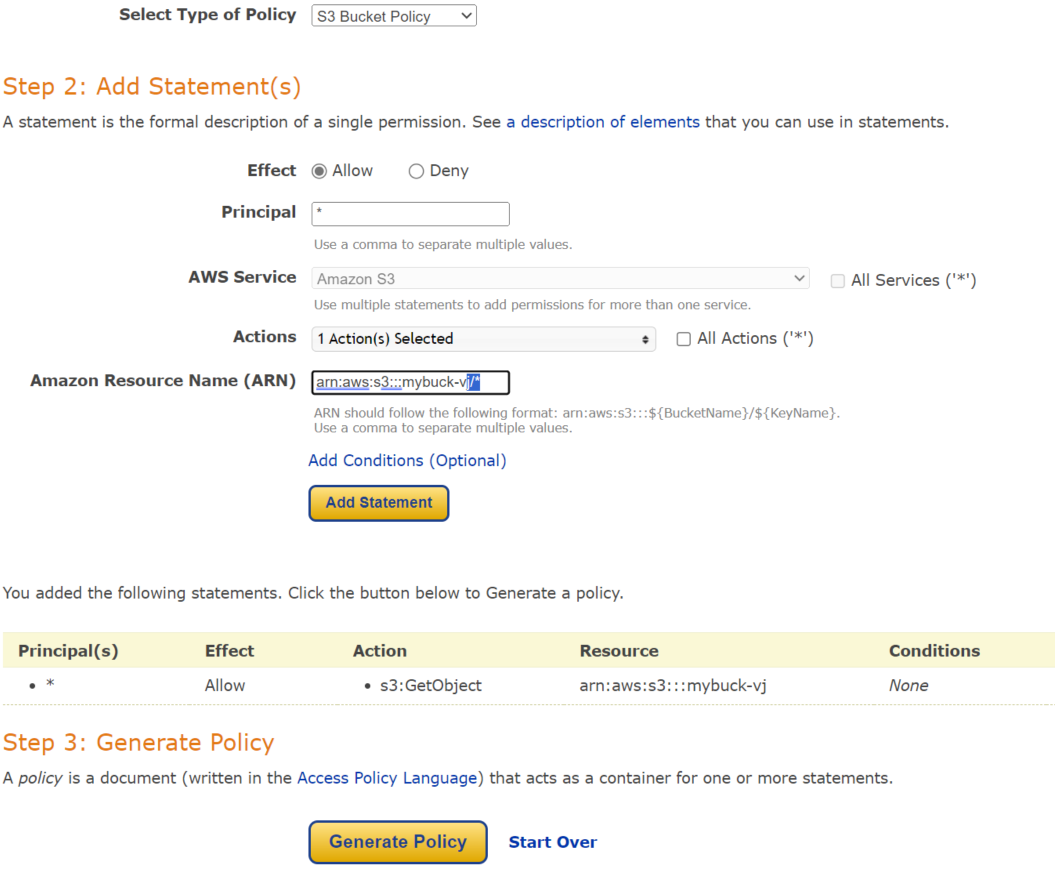
Edit bucket policy Info

Bucket policy

The bucket policy, written in JSON, provides a

Bucket ARN

arn:aws:s3:::mybuck-vj



Select Type of Policy: S3 Bucket Policy

Step 2: Add Statement(s)

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

Effect: ● Allow ○ Deny

Principal: *

Use a comma to separate multiple values.

AWS Service: Amazon S3 □ All Services ('*')

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

Actions: 1 Action(s) Selected □ All Actions ('*')

Amazon Resource Name (ARN): arn:aws:s3:::mybuck-vj/*

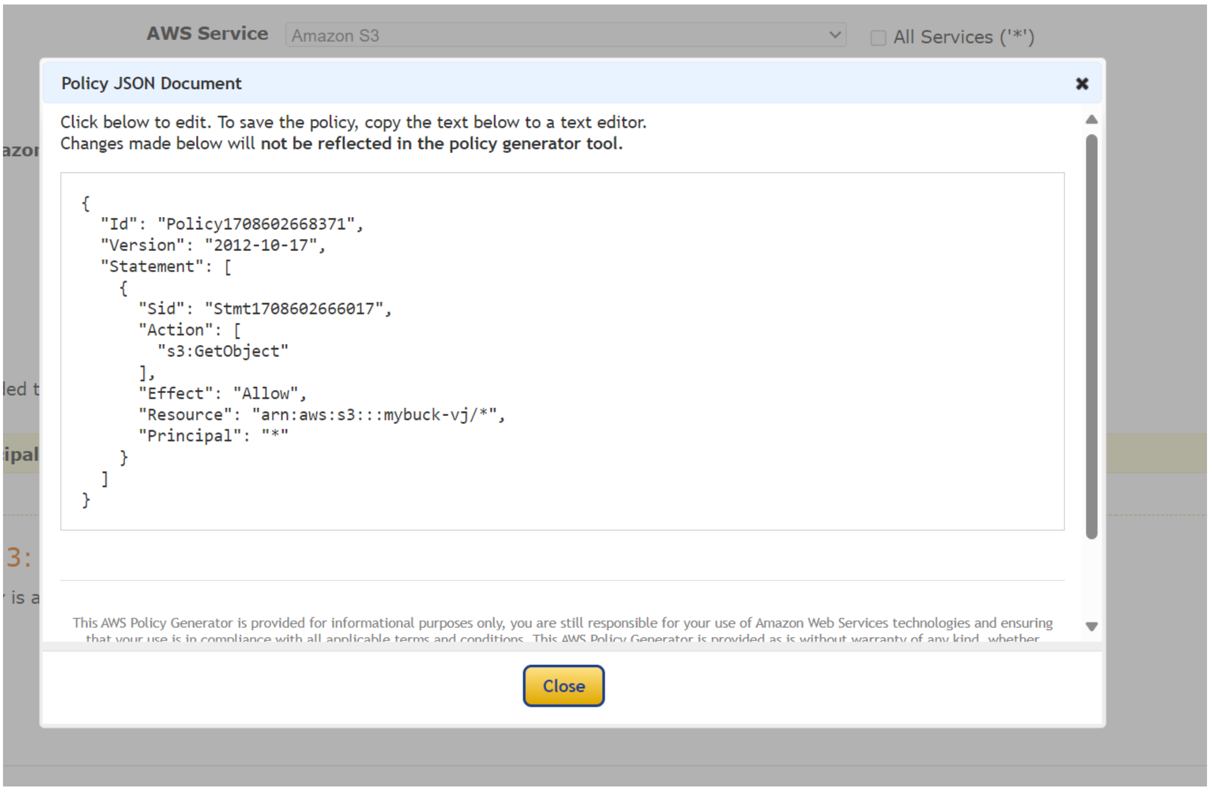
ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

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

Principal(s)	Effect	Action	Resource	Conditions
- *	Allow	- s3:GetObject	arn:aws:s3:::mybuck-vj	*None*

Step 3: Generate Policy

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

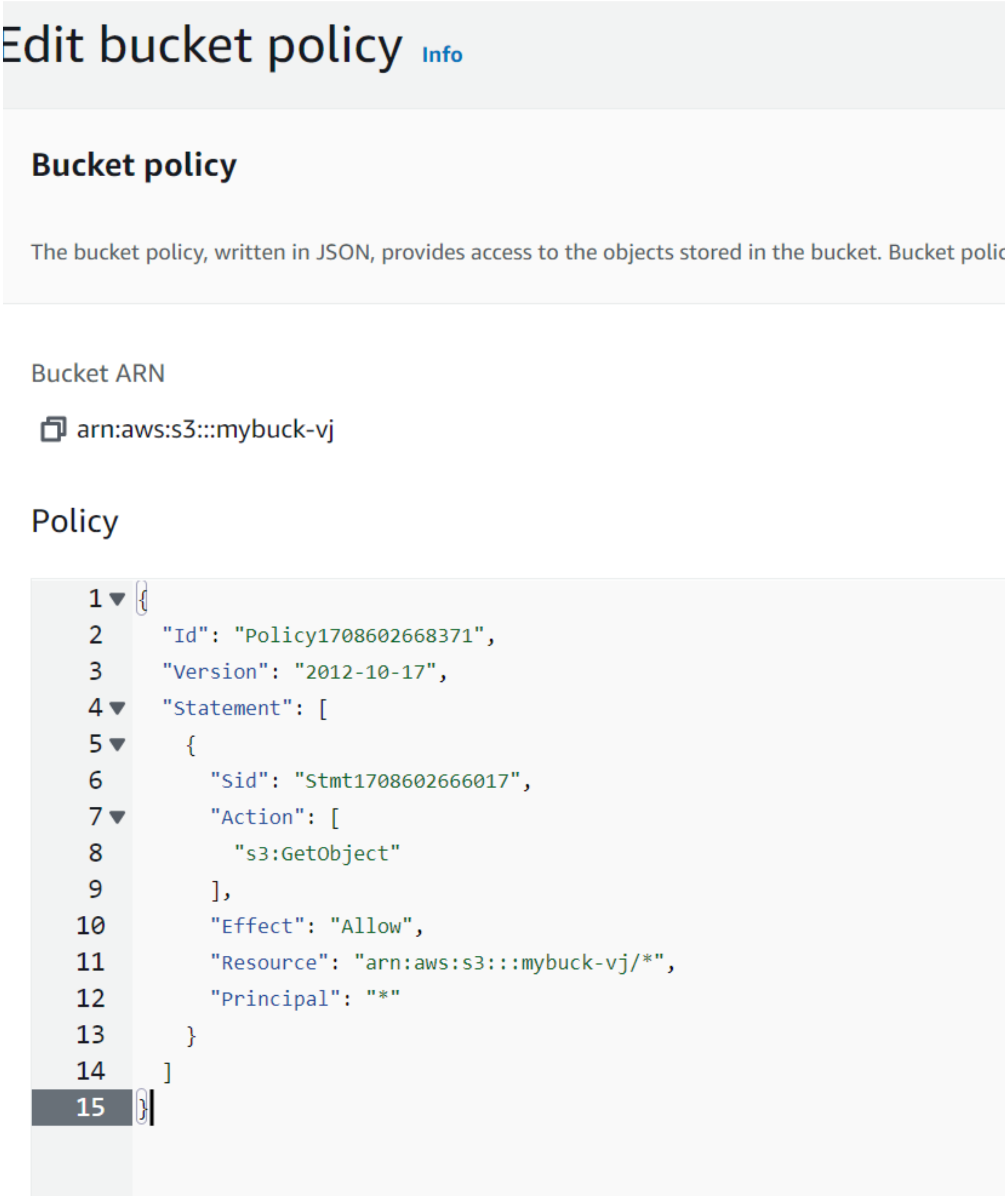


Policy JSON Document

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

```
{
  "Id": "Policy1708602668371",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1708602666017",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mybuck-vj/*",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether



Edit bucket policy

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket polic

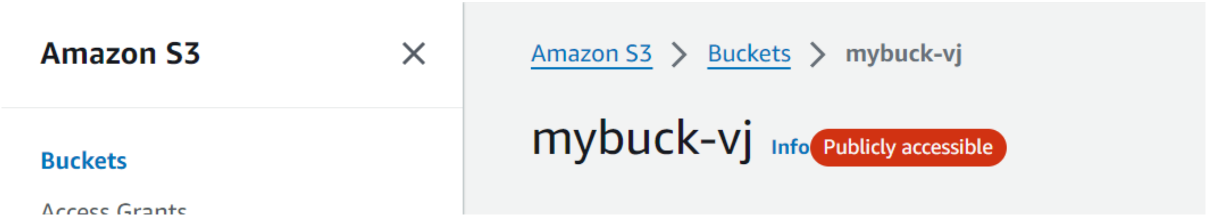
Bucket ARN

arn:aws:s3:::mybuck-vj

Policy

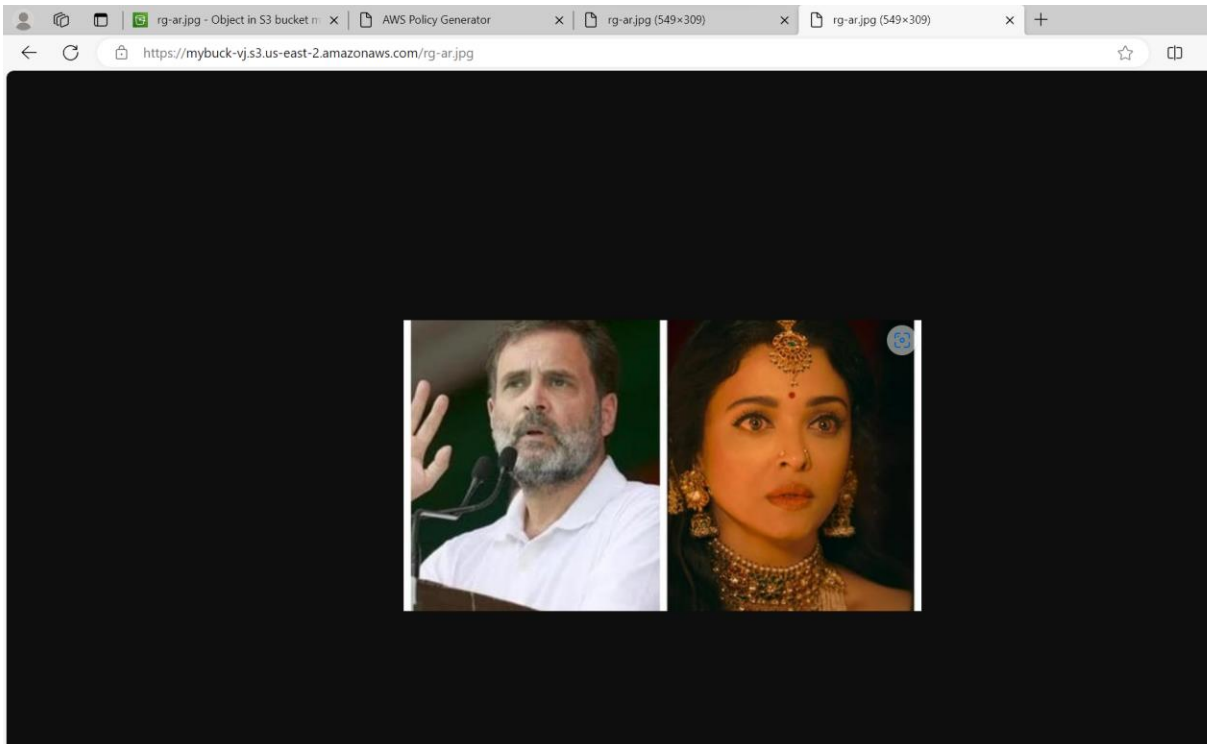
```
{
  "Id": "Policy1708602668371",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1708602666017",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mybuck-vj/*",
      "Principal": "*"
    }
  ]
}
```

Save changes -→ refresh the page



mybuck-vj Publicly accessible

Reload the page :


rg-ar.jpg - Object in S3 bucket m
AWS Policy Generator
rg-ar.jpg (549×309)
rg-ar.jpg (549×309)
https://mybuck-vj.s3.us-east-2.amazonaws.com/rg-ar.jpg