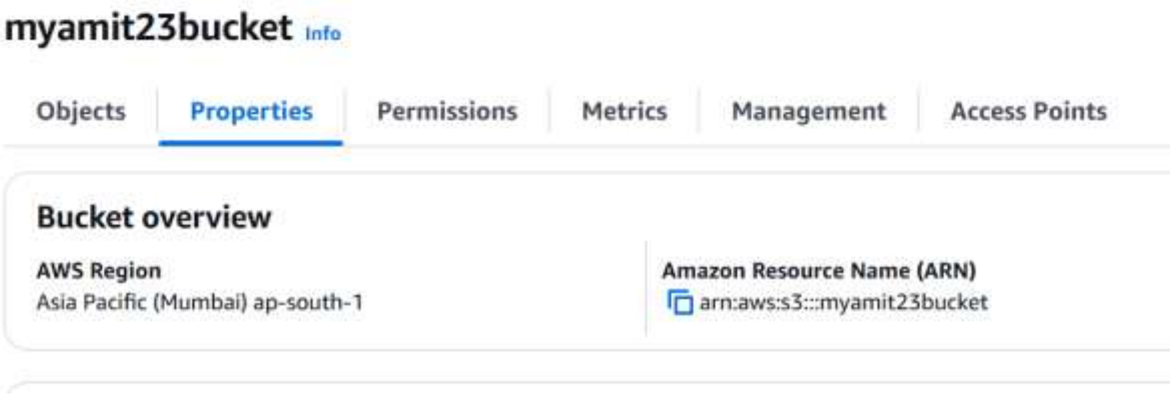
S3: Static website hosting

- Trainer will provide the static website page

https://github.com/amitopenwriteup/static-website-example.git

- Download and upload all the website of static website
-
- In bucket, go to properties section of bucket



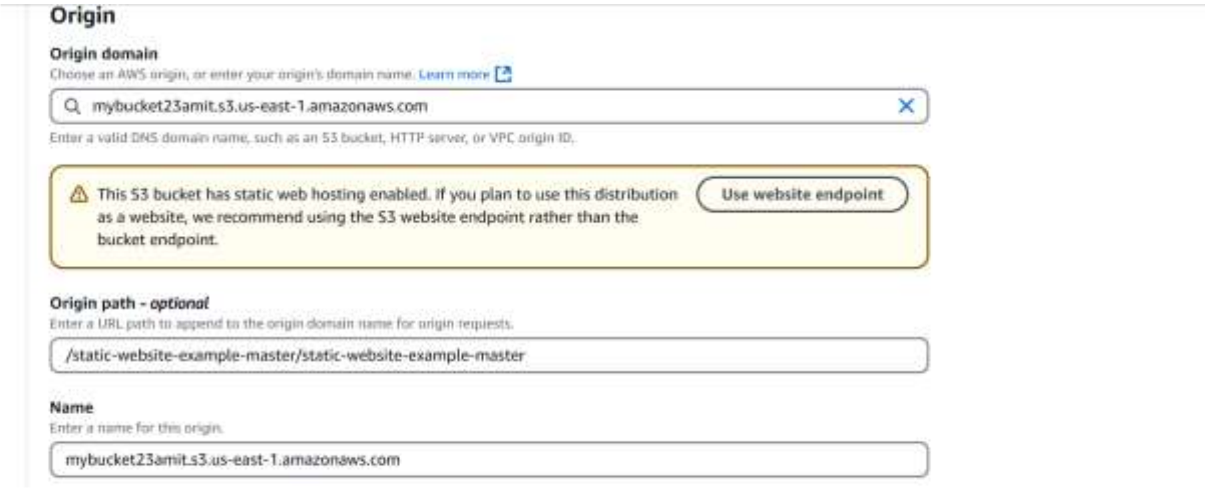
myamit23bucket Info

Bucket overview

AWS Region
Asia Pacific (Mumbai) ap-south-1

Amazon Resource Name (ARN)
arn:aws:s3:::myamit23bucket

Provide the source info



Origin

Origin domain
Choose an AWS origin, or enter your origin's domain name. Learn more

mybucket23amit.s3.us-east-1.amazonaws.com

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint.

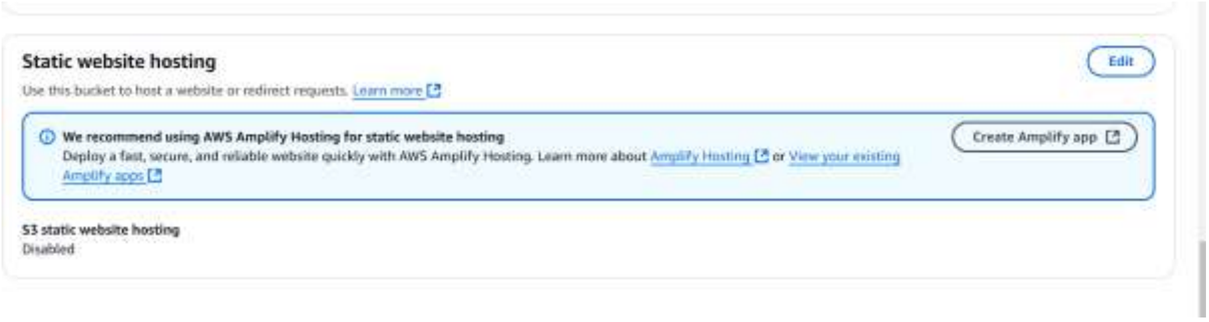
Origin path - *optional*
Enter a URL path to append to the origin domain name for origin requests.

/static-website-example-master/static-website-example-master

Name
Enter a name for this origin.

mybucket23amit.s3.us-east-1.amazonaws.com

- End of the page you will find, Static website hosting tab



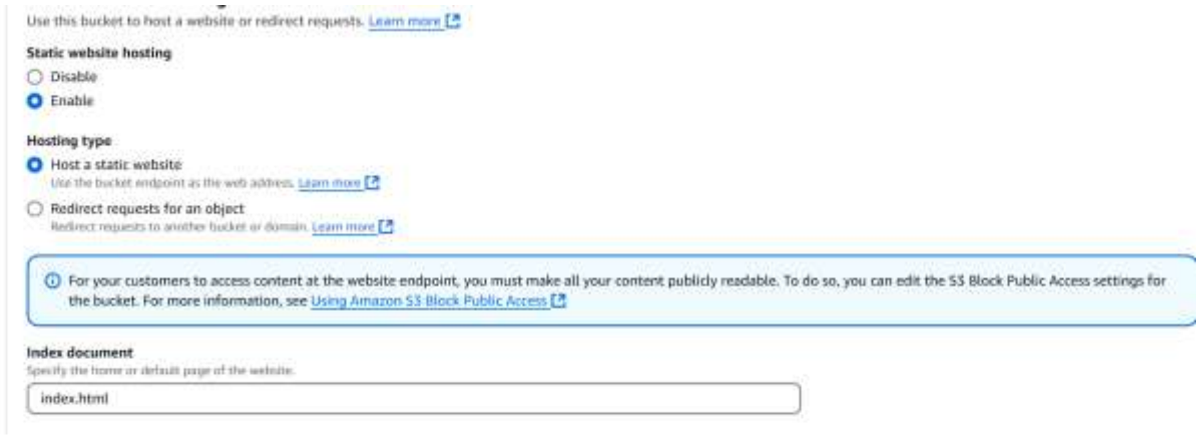
Static website hosting

Use this bucket to host a website or redirect requests. Learn more

We recommend using AWS Amplify Hosting for static website hosting
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about Amplify Hosting or View your existing Amplify apps

S3 static website hosting
Disabled

Enable the static website



Use this bucket to host a website or redirect requests. Learn more

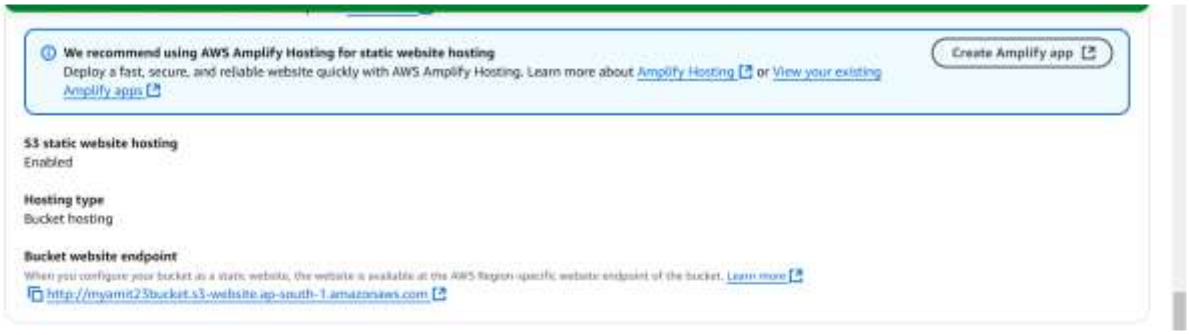
Static website hosting
○ Disable
● Enable

Hosting type
● Host a static website
Use the bucket endpoint as the web address. Learn more
○ Redirect requests for an object
Redirect requests to another bucket or domain. Learn more

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access

Index document
Specify the home or default page of the website.
index.html

Check the link and you will find the website



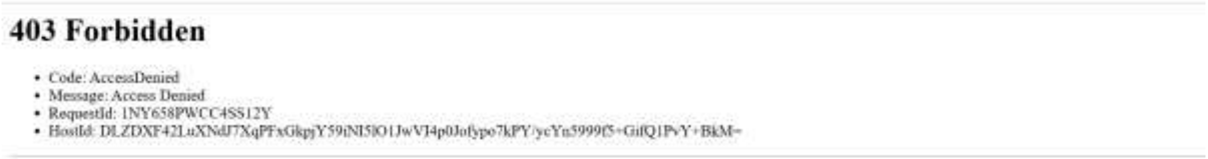
We recommend using AWS Amplify Hosting for static website hosting
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about Amplify Hosting or View your existing Amplify apps

S3 static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more
http://myamit23bucket.s3-website.ap-south-1.amazonaws.com

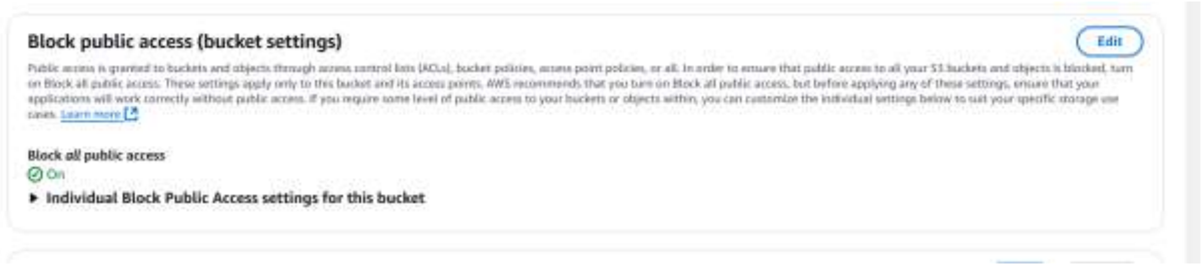
IF you click on bucket website endpoint, it will give the error message



403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 1NY658PWCC4SS12Y
- HostId: DLZDXF42LuXNdJ7XqPFxGkpjY59iNI5lO1JwVI4p0Jofypo7kPY/ycYn5999f5+GifQ1PvY+BkM=

Go to Bucket Permission tab

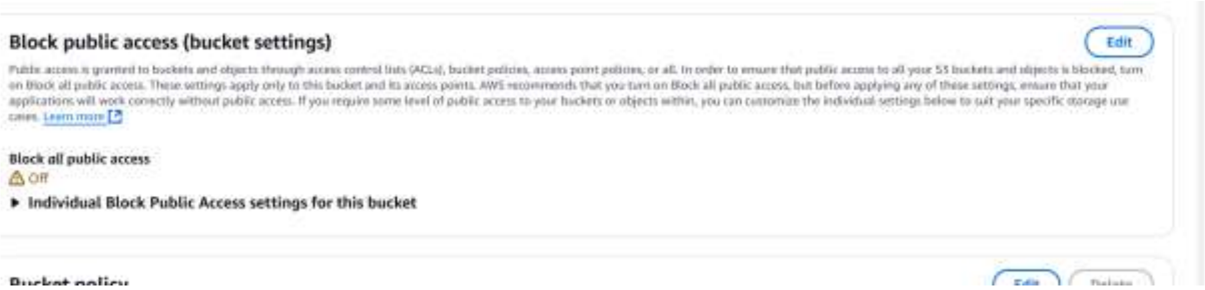


Block public access (bucket settings)

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
✓ On

Click on edit and off the public access

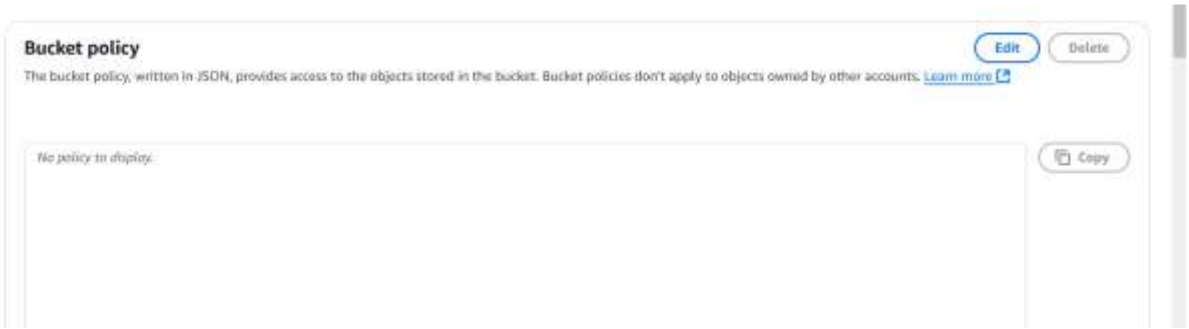


Block public access (bucket settings)

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

If you check the website endpoint, still it will not accessible since we have not created the policy

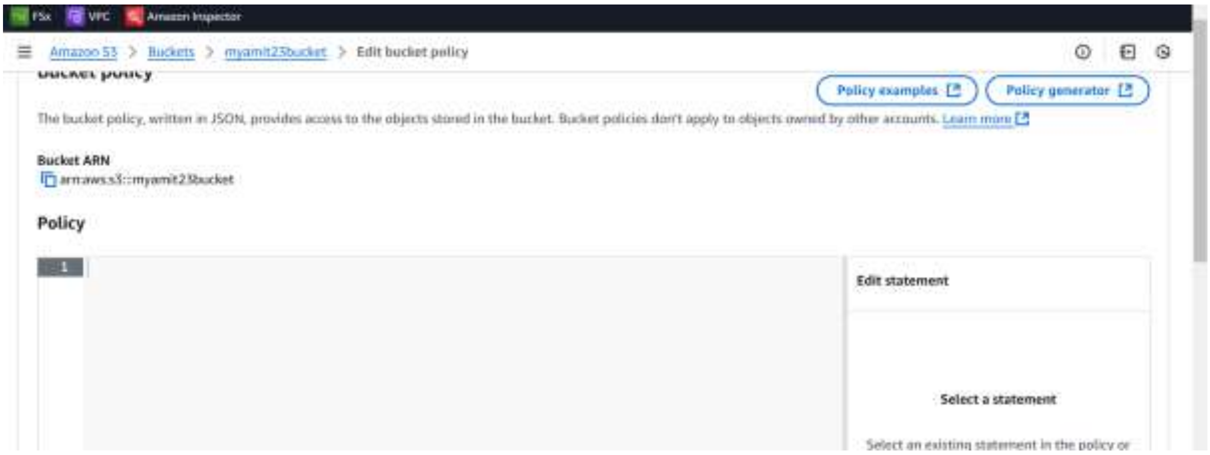


Bucket policy

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

No policy to display.

Click on Edit of bucket policy, and click on policy generator



Amazon S3 > Buckets > myamit23bucket > Edit 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:::myamit23bucket

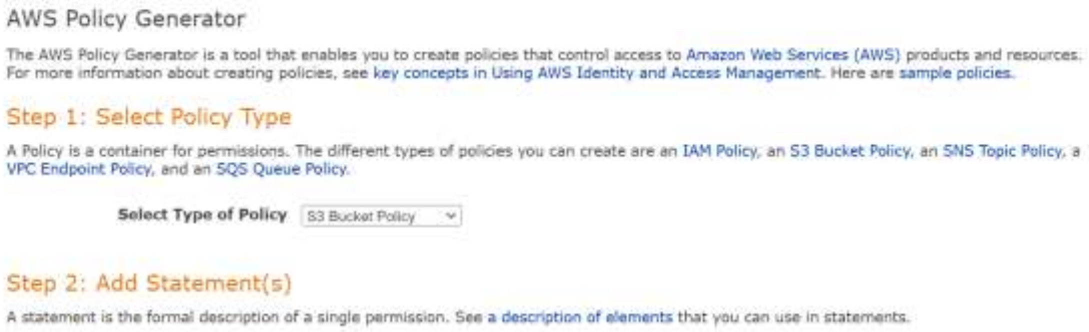
Policy

Edit statement

Select a statement

Select an existing statement in the policy or

Select the policy type: S3bucket policy



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

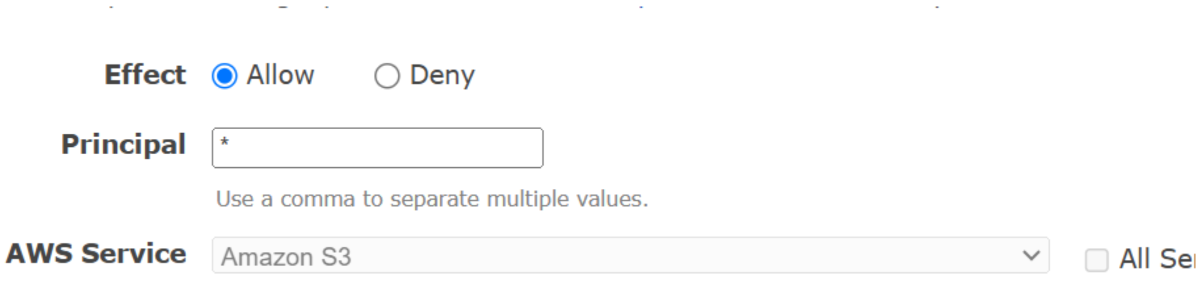
A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy: 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.

Provide principal: Whom to provide the access



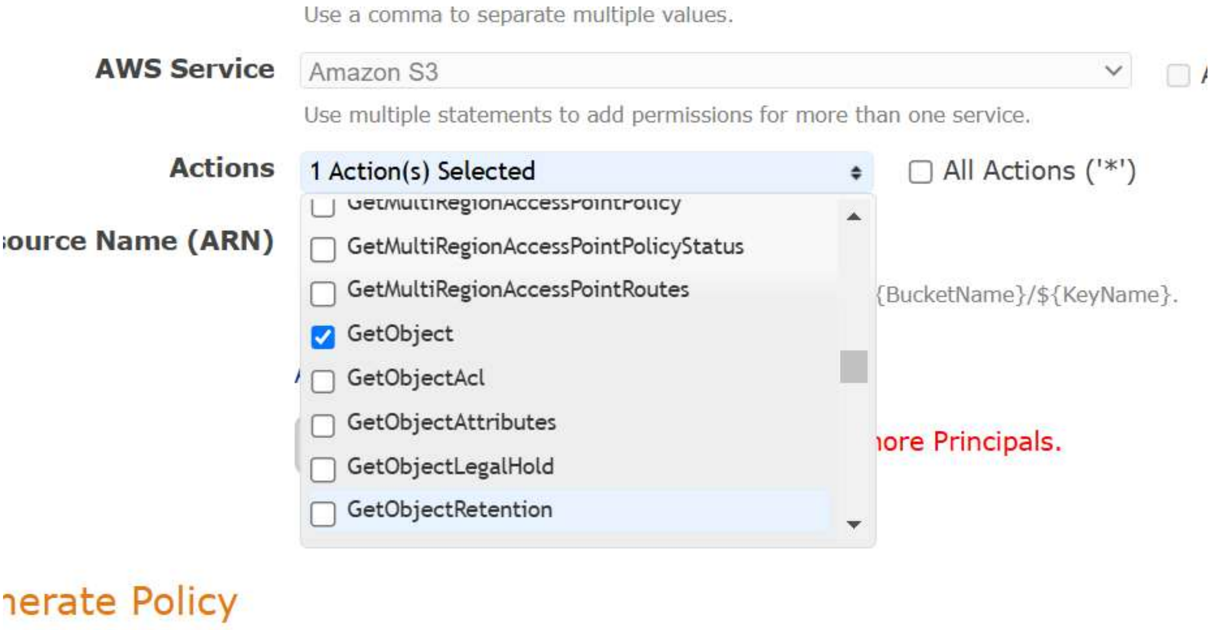
Effect ● Allow ○ Deny

Principal: *

Use a comma to separate multiple values.

AWS Service: Amazon S3 □ All Se

In Action field, select get object



Use a comma to separate multiple values.

AWS Service: Amazon S3 □ /

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

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

□ GetMultiRegionAccessPointPolicy
□ GetMultiRegionAccessPointPolicyStatus
□ GetMultiRegionAccessPointRoutes
☑ GetObject
□ GetObjectAcl
□ GetObjectAttributes
□ GetObjectLegalHold
□ GetObjectRetention

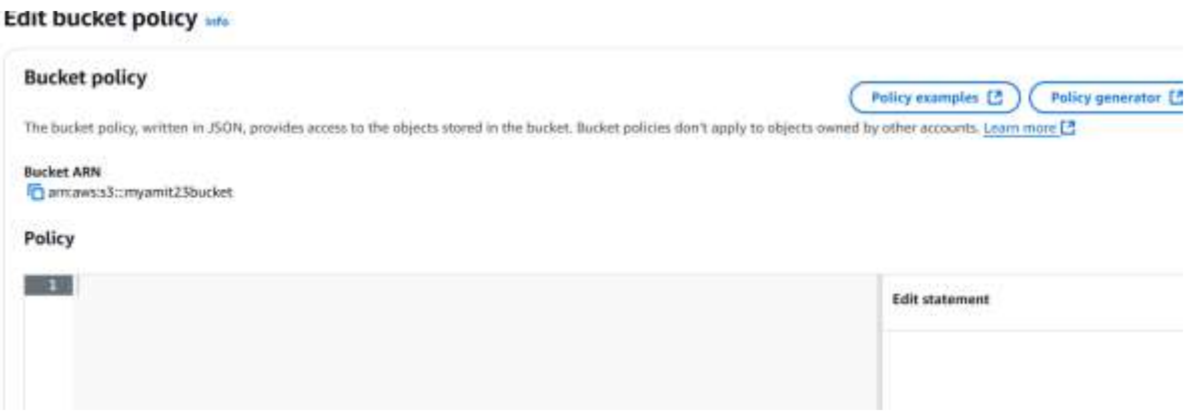
ource Name (ARN)

{BucketName}/${KeyName}.

nore Principals.

nerate Policy

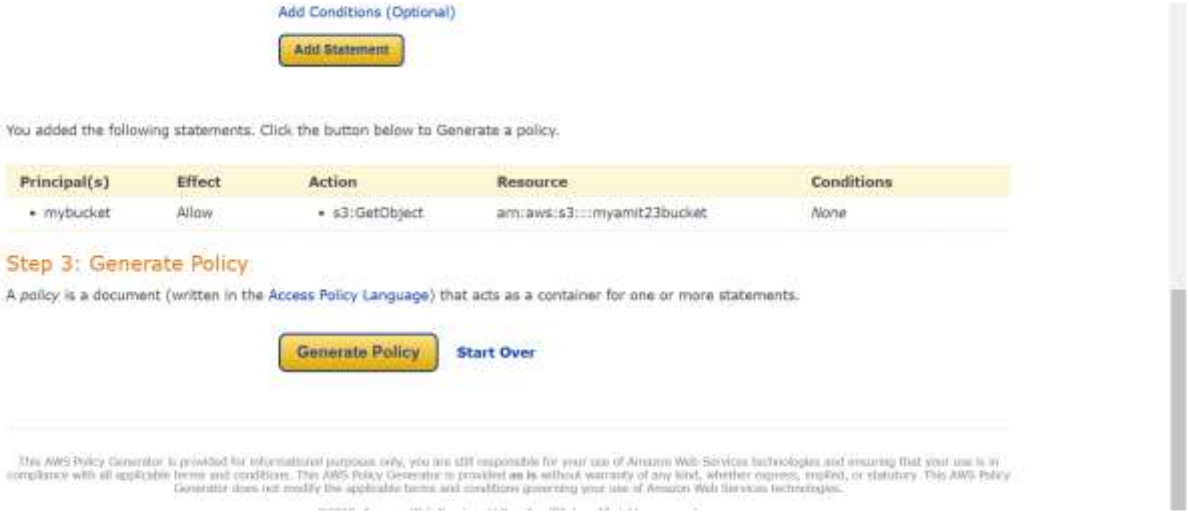
Bucket Arn, you will go to bucket tab



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:::myamit23bucket

Click on Add statement, and generate policy



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

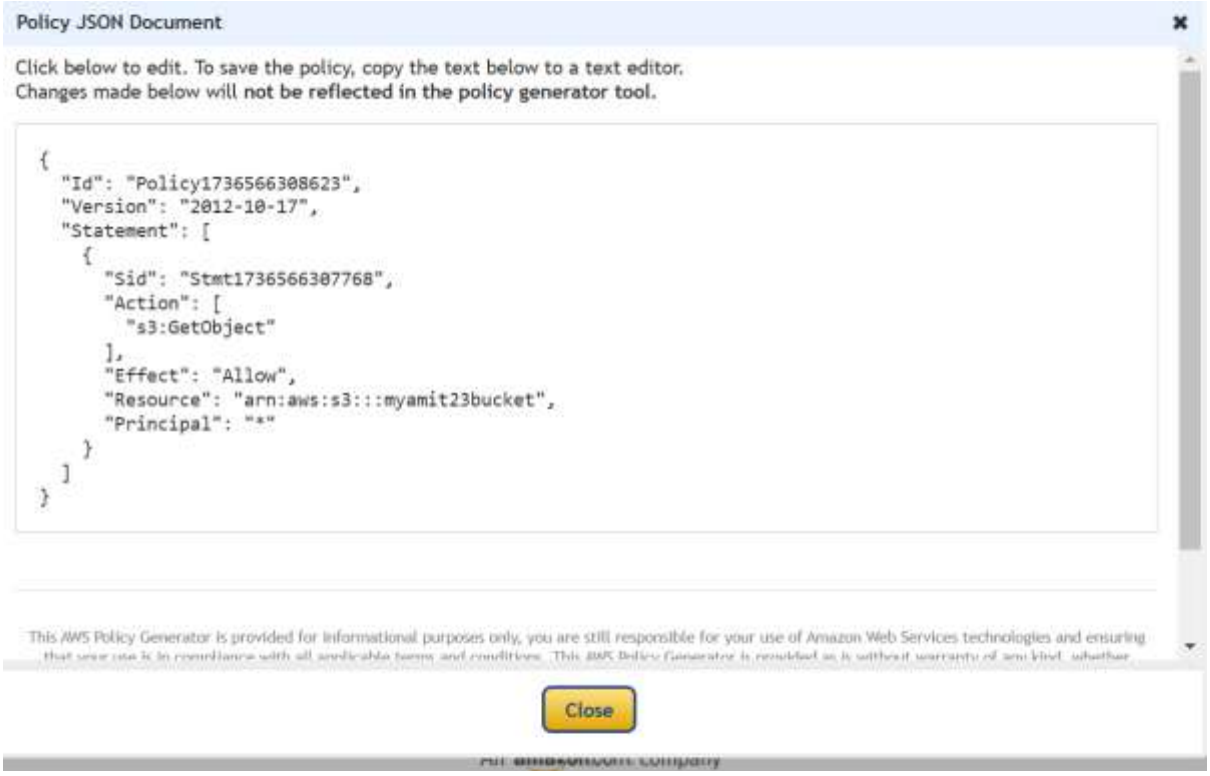
Principal(s)	Effect	Action	Resource	Conditions
• mybucket	Allow	• s3:GetObject	arn:aws:s3:::myamit23bucket	*None*

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.

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 express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

Copy the json format, from the site

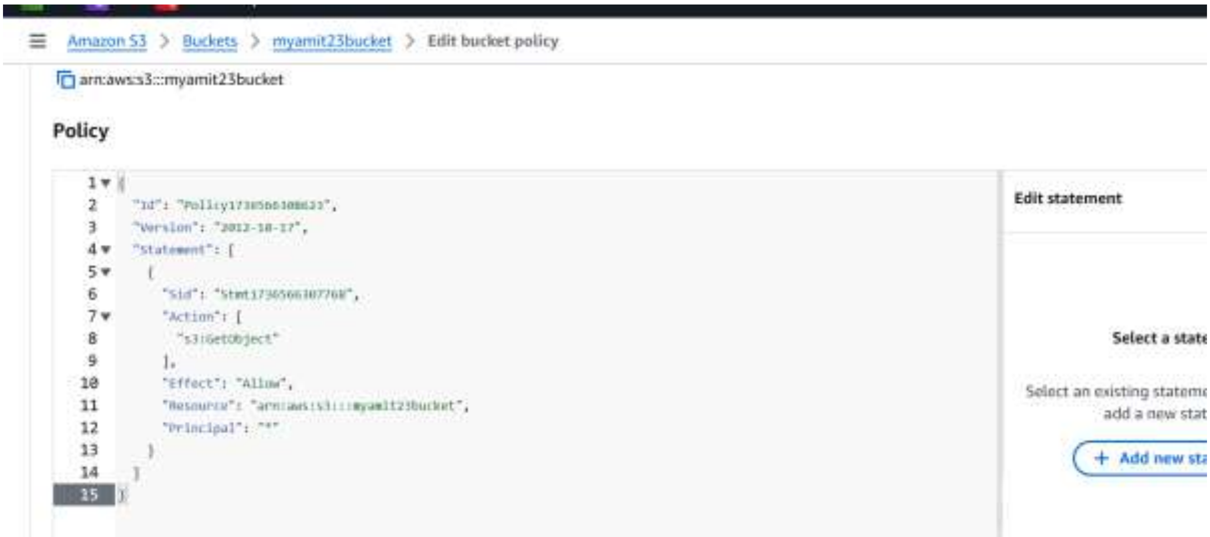


Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will not be reflected in the policy generator tool.

```
{
  "Id": "Policy1736566308623",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1736566307768",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::myamit23bucket",
      "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

Go to bucket add policy option copy this json , If try to change it will fail



Amazon S3 > Buckets > myamit23bucket > Edit bucket policy
arn:aws:s3:::myamit23bucket
Policy
Edit statement
Select a state
Select an existing stateme
add a new stat
+ Add new sta

```
{
  "Id": "Policy1736566308623",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1736566307768",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::myamit23bucket",
      "Principal": "*"
    }
  ]
}
```

Go to Resource, make this change

```
{
  "Version": "2012-10-17",
  "Id": "Policy1736566538815",
    "Statement": [
        {
            "Sid": "Stmt1736566307768",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::myamit23bucket/*"
        }
    ]
}
```

Now save the changes. Now try to access the bucket endpoint, it must work