Hosting a static website using Amazon s3

1. Create a S3 bucket in Amazon S3 service.

a. Logon to the https://console.aws.amazon.com with your root account.

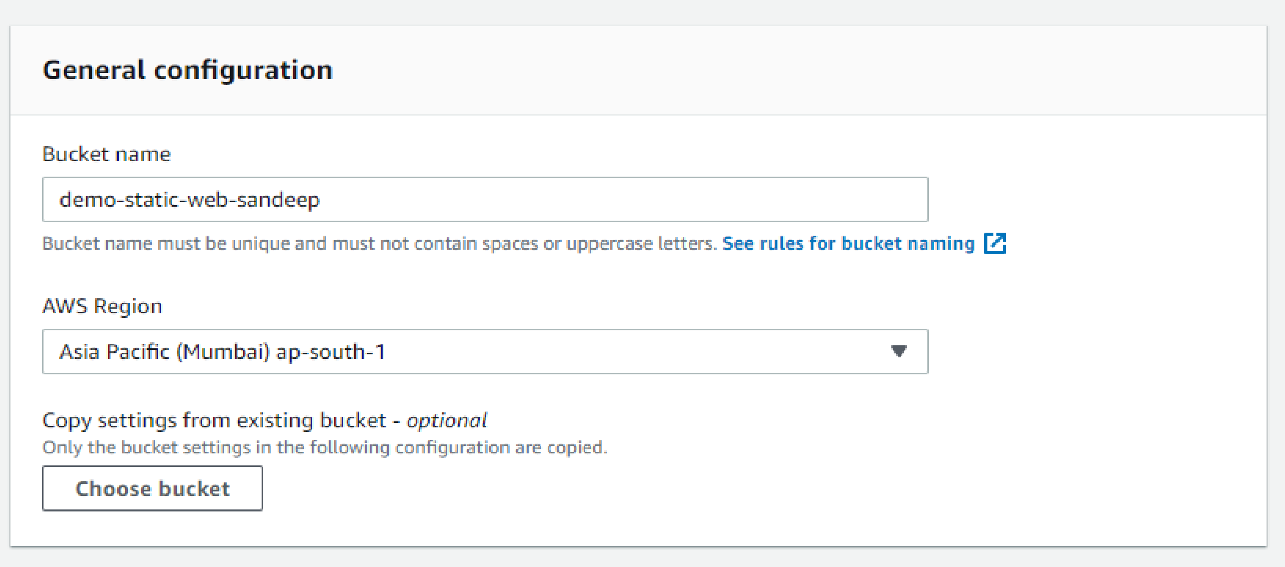
b. After login In the search bar type S3.

c. In the search result click the first option S3.

d. It will open the Amazon S3 service console.

e. In the S3 console, click **Create Bucket** button.

f. On the create bucket page, type a name for the bucket and select the required region (For this demo check if it's Mumbai)



General configuration

Bucket name: demo-static-web-sandeep

Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

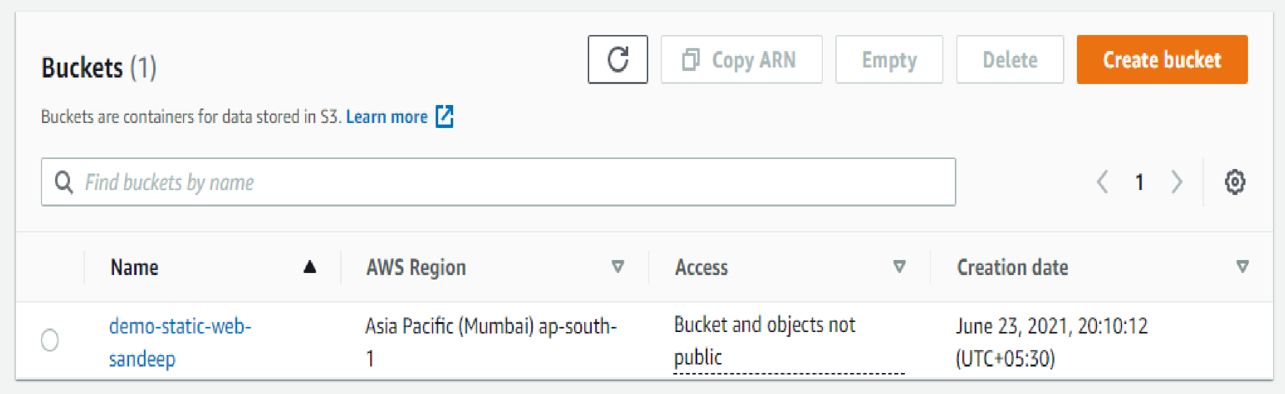
AWS Region: Asia Pacific (Mumbai) ap-south-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

g. Keep all other options as it is and click **Create Bucket** button at the end of the page.

h. The bucket is created.



Buckets (1)

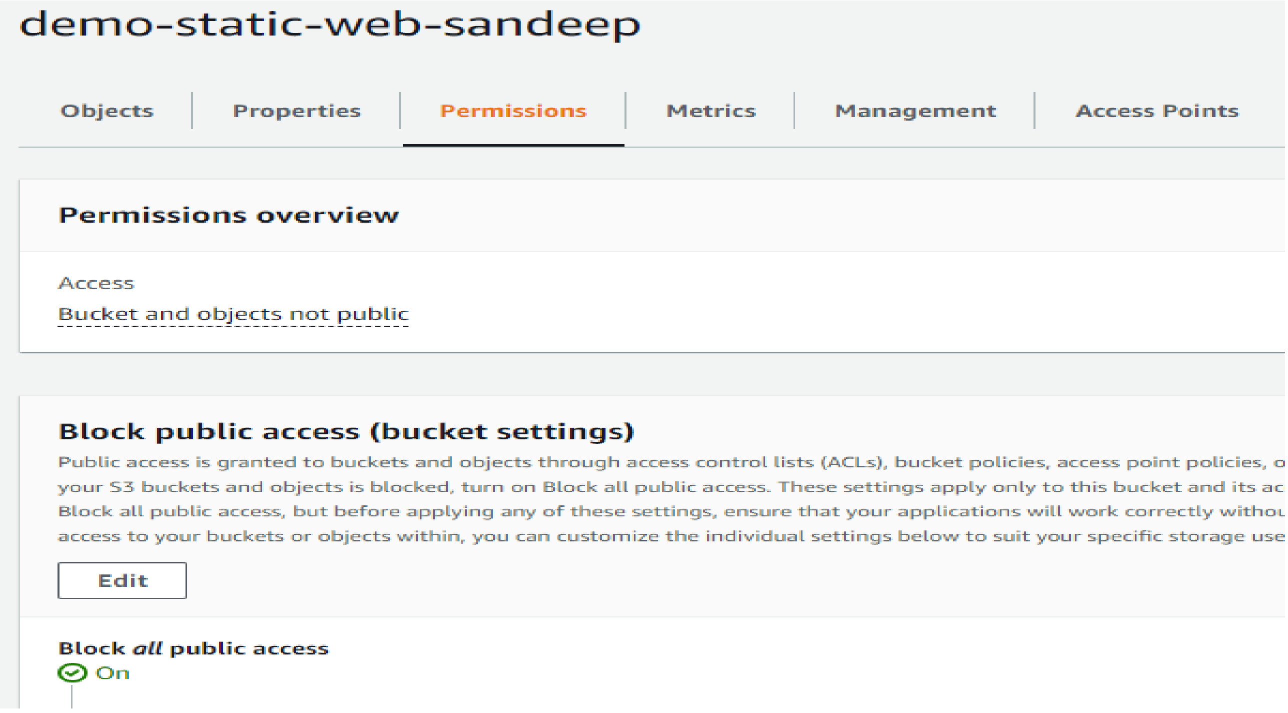
Buckets are containers for data stored in S3. Learn more

	Name ▲	AWS Region	Access	Creation date
○	demo-static-web-sandeep	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	June 23, 2021, 20:10:12 (UTC+05:30)

2. Make the above bucket public.

By default any S3 bucket created block any type of public access. As this bucket will be used for hosting web pages for any user, we need to open this bucket and its contents for public access.

a. Once the bucket is created, click on the name of the bucket. On the new page click the permissions tab, as shown below.



demo-static-web-sandeep

Permissions overview

Access
Bucket and objects not public

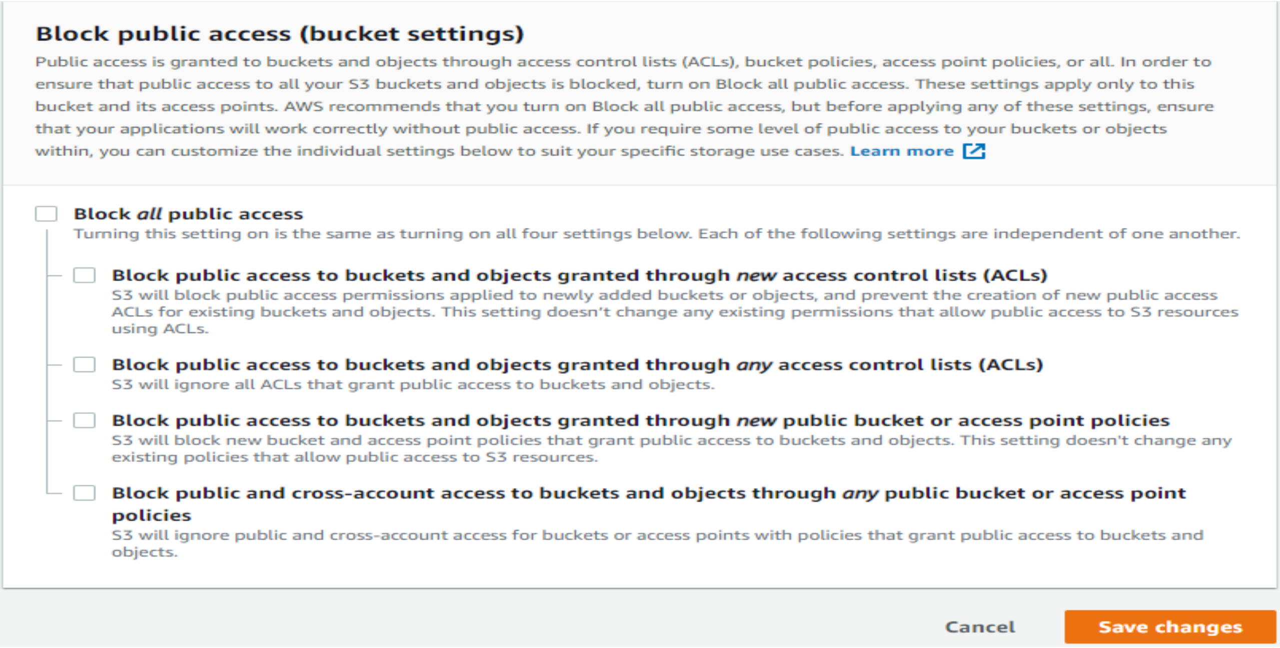
Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, o
your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its ac
Block all public access, but before applying any of these settings, ensure that your applications will work correctly withou
access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use

Block *all* public access
✓ On

b. Now click on the Edit button below the Block public access (bucket settings) option.

c. On the page that opens, uncheck the **Block all public access** check box. Click **Save changes** button.



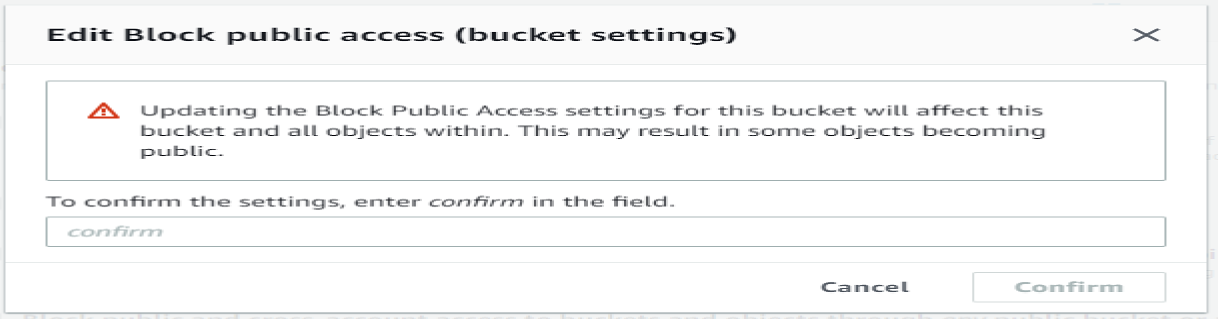
Block public access (bucket settings)

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.

d. A warning window will be displayed. Type confirm and click Confirm button.



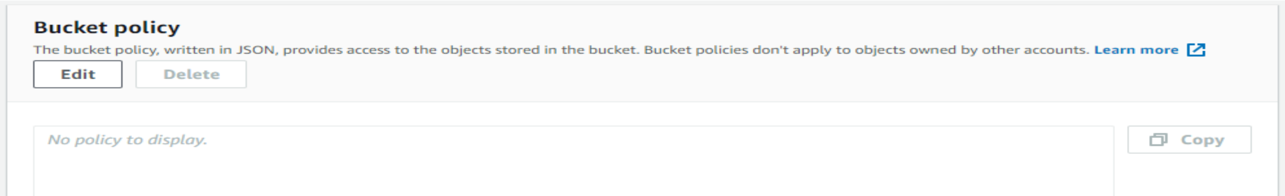
Edit Block public access (bucket settings)

⚠ 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

e. Once your back to the bucket properties page, scroll down and click Edit in the **Bucket policy** section.

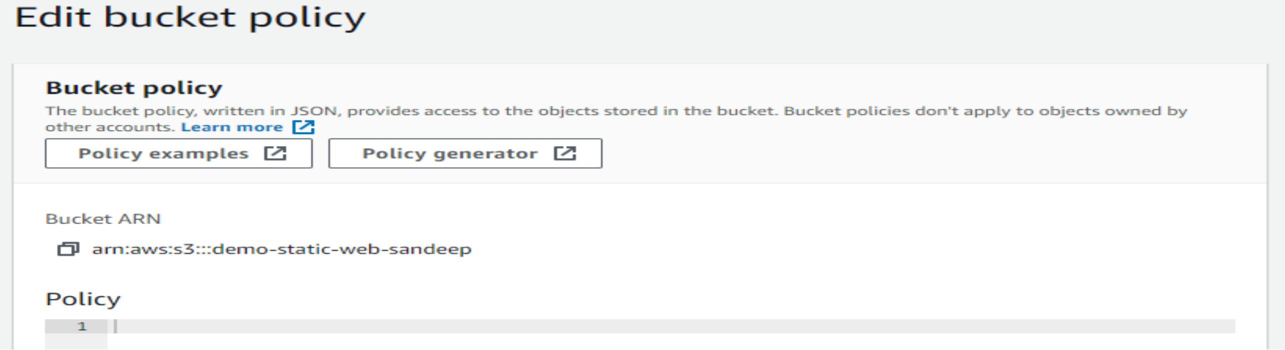


Bucket policy

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.

f. Now click on the **Policy generator** button.



Edit bucket policy

Bucket policy

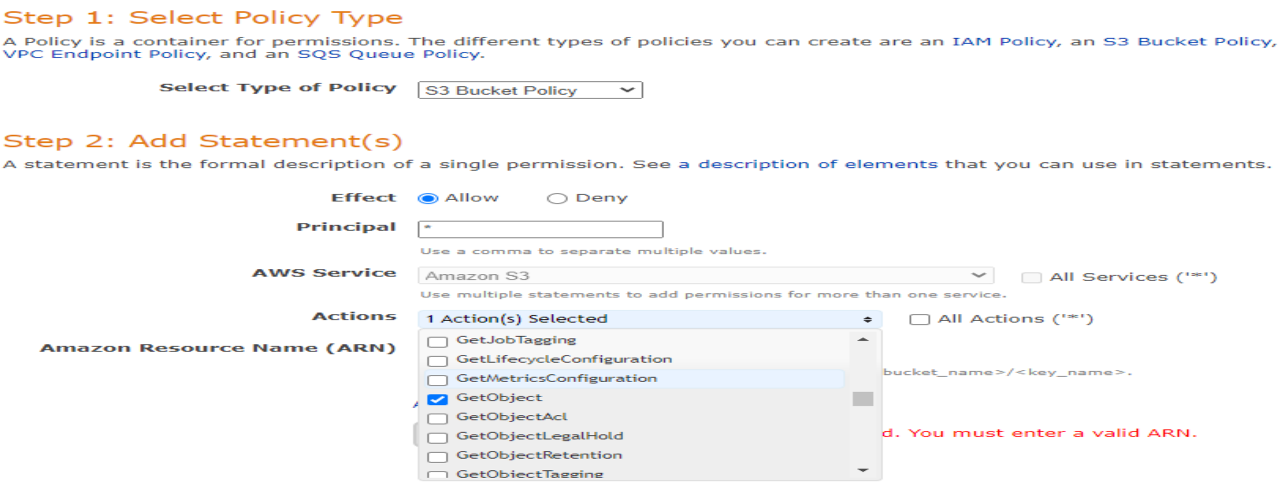
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Bucket ARN

arn:aws:s3:::demo-static-web-sandeep

Policy

g. On the Policy generator page that opens in a new tab, first select the **type of the policy** as the **S3 bucket policy**. In the **Principal** field type *****. In the **Actions** field, click the drop down menu and select the check box of the **GetObject** option only as shown below.



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, 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.

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 ('*')

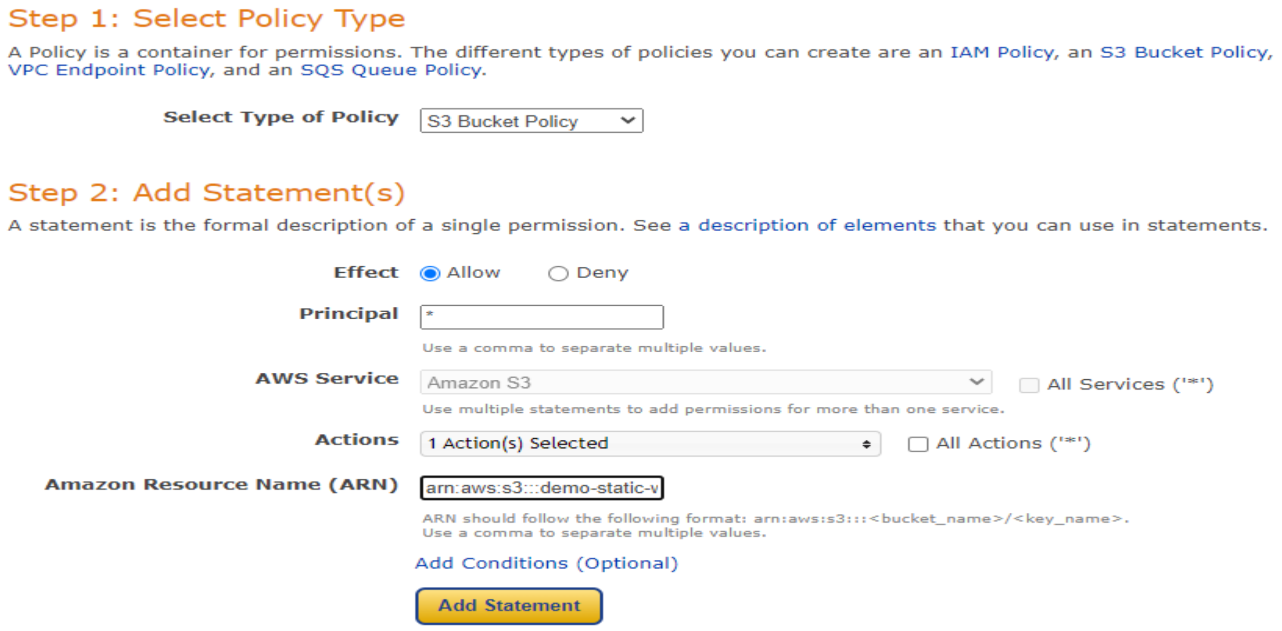
□ GetJobTagging
□ GetLifecycleConfiguration
□ GetMetricsConfiguration
☑ GetObject
□ GetObjectAcl
□ GetObjectLegalHold
□ GetObjectRetention
□ GetObjectTagging

Amazon Resource Name (ARN)

bucket_name>/<key_name>.

d. You must enter a valid ARN.

In the Amazon Resource Name (ARN) field, you need to enter the S3 bucket ARN. Go to your Amazon S3 tab. There just below the Policy generator button, you will find the Bucket ARN. Copy that ARN and then come to policy generator page and paste the value in the ARN field. Then just scroll and at the end of the ARN add **.** *It should be like* ***arn:aws:s3:::demo-static-web-sandeep***/*
The final values will look as shown below.



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, 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.

Effect: ● Allow ○ Deny

Principal: *

Use a comma to separate multiple values.

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

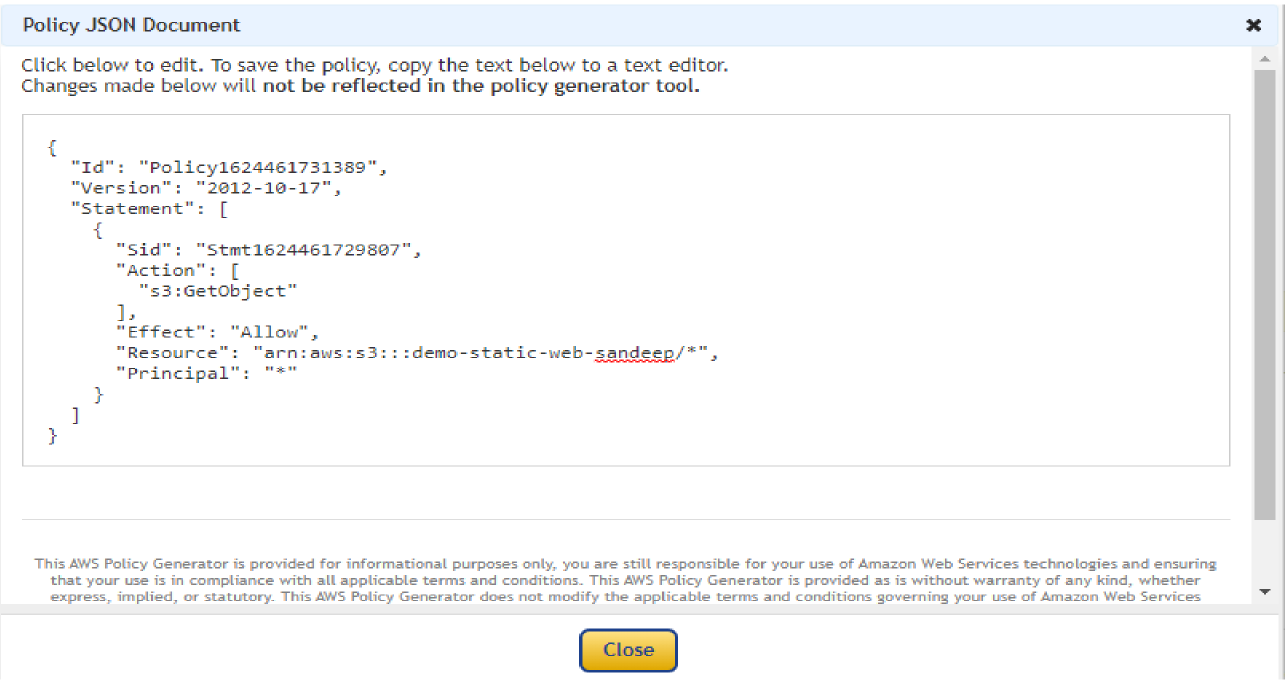
Use multiple statements to add permissions for more than one service.

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

Amazon Resource Name (ARN): arn:aws:s3:::demo-static-v

ARN should follow the following format: arn:aws:s3:::<bucket_name>/<key_name>.
Use a comma to separate multiple values.

Now click on the **Add Statement** button. A statement will appear below the Add Statement button. Now click **Generate Policy** button. A window will display the policy in the JASON format.



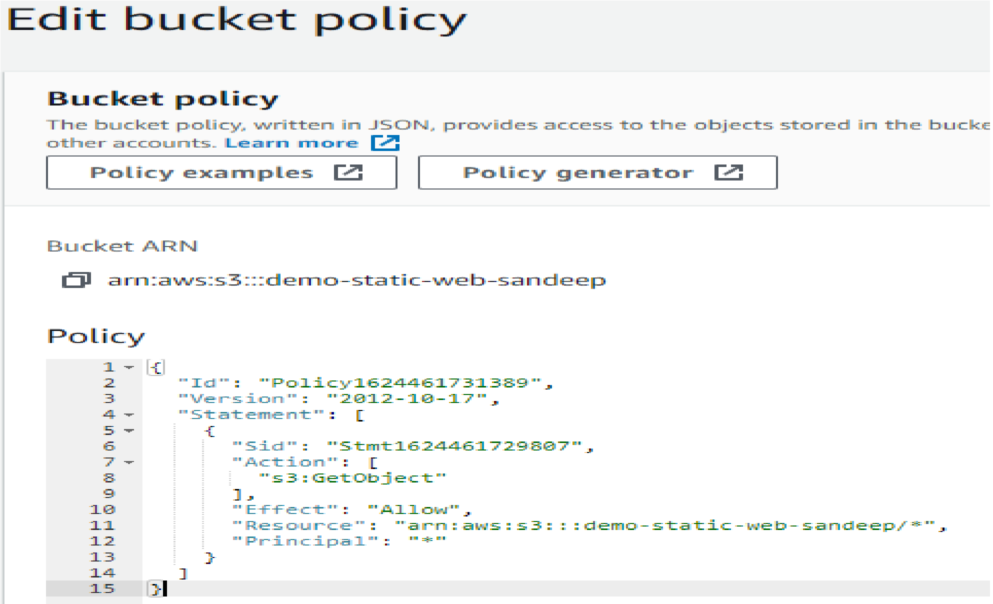
Policy JSON Document

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": "Policy1624461731389",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1624461729807",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::demo-static-web-sandeep/*",
      "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 express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services

Select all and copy the above policy. Click Close. Now go to your Amazon S3 console and in the Policy field paste this policy.



Edit bucket policy

Bucket policy

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

Bucket ARN

arn:aws:s3:::demo-static-web-sandeep

Policy

```
{
    "Id": "Policy1624461731389",
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "Stmt1624461729807",
        "Action": [
          "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": "arn:aws:s3:::demo-static-web-sandeep/*",
        "Principal": "*"
      }
    ]
}
```

Scroll down and on the page click Save Changes.

3. Create an index,html file on your laptop and upload to S3 bucket.

a. Create a folder on C or D drive.
b. In that folder create a text document. Name it as index.html.
c. Now paste following html code or type your own code.

```
<html>
 <head> <title>My Website Home Page</title> </head>
<body> <h1>Welcome to my website</h1>
<p>Now hosted on Amazon S3!</p>
</body>
</html>
```

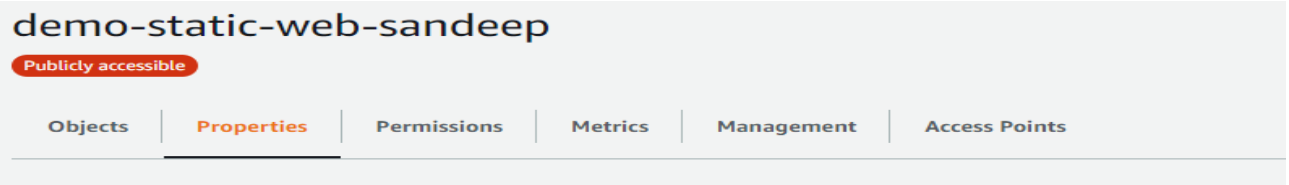
d. Save the file.

e. Now rename the file as Windows will add the .txt extension to the index.html file so it will be like index.html.txt. So Click on the view tab in the explorer window where the file is shown. In the view tab click the file name extensions check box. Then rename the file and remove .txt extension.

f. Now go to the Amazon S3 console and upload this index.html file to the above bucket.

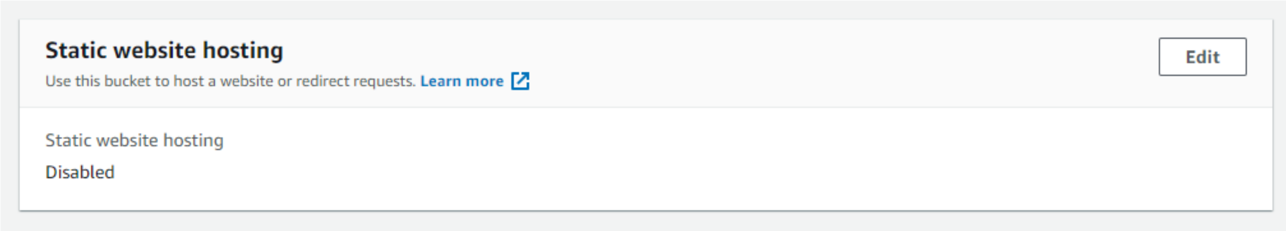
4. Enable Static Web Hosting for the S3 Bucket.

a. In the Amazon S3 console, click on the bucket name and then click the properties tab.



demo-static-web-sandeep

Scroll Down and go to the end of the page. There Static website hosting option is present.



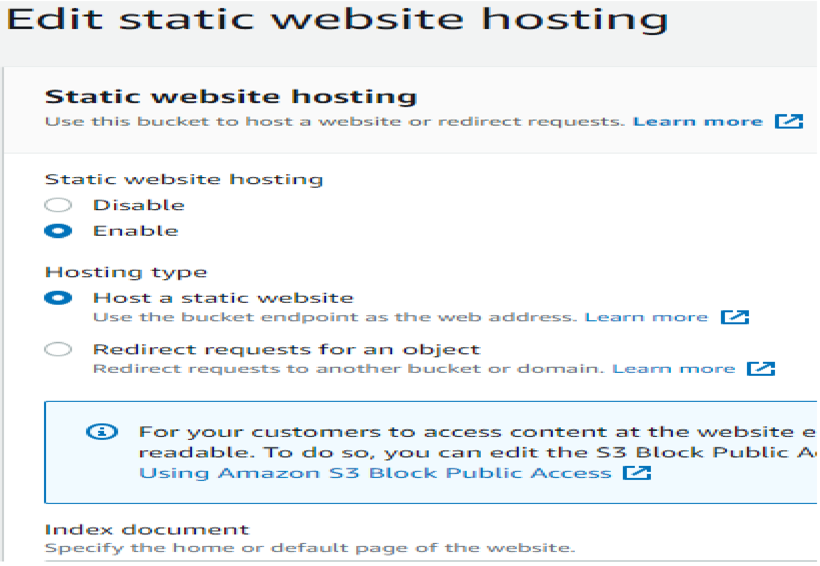
Static website hosting

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

Static website hosting

Disabled

Click Edit and Click Enable. In the Index document field type the file name as index.html.. Click Save Changes.



Edit static website hosting

Static website hosting

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

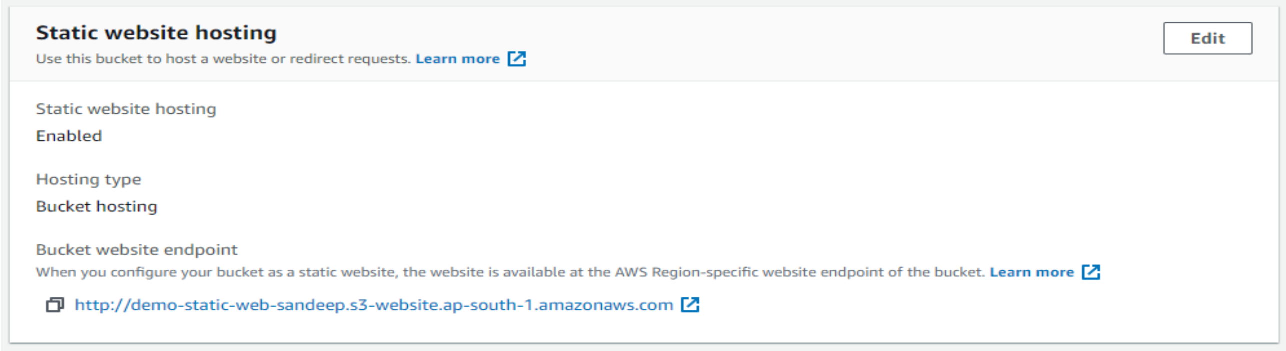
Redirect requests to another bucket or domain. Learn more

For your customers to access content at the website e
readable. To do so, you can edit the S3 Block Public A
Using Amazon S3 Block Public Access

Index document

Specify the home or default page of the website.

Now scroll down to the page to go to the static website hosting section.



Static website hosting

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

Static website hosting

Enabled

Hosting type

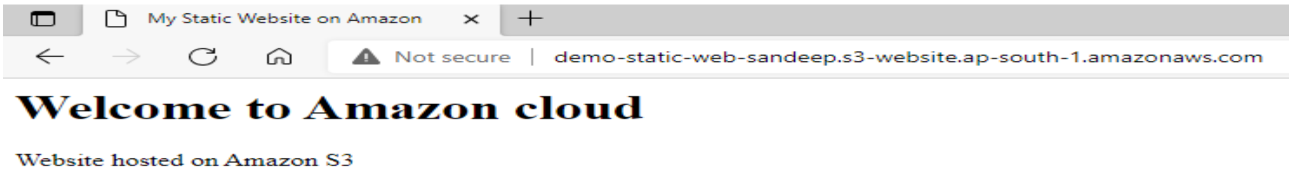
Bucket hosting

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://demo-static-web-sandeep.s3-website.ap-south-1.amazonaws.com

The URL for your website will be displayed. Copy that and paste it in the browser. Your website should be displayed now.



My Static Website on Amazon

Not secure | demo-static-web-sandeep.s3-website.ap-south-1.amazonaws.com

Welcome to Amazon cloud

Website hosted on Amazon S3