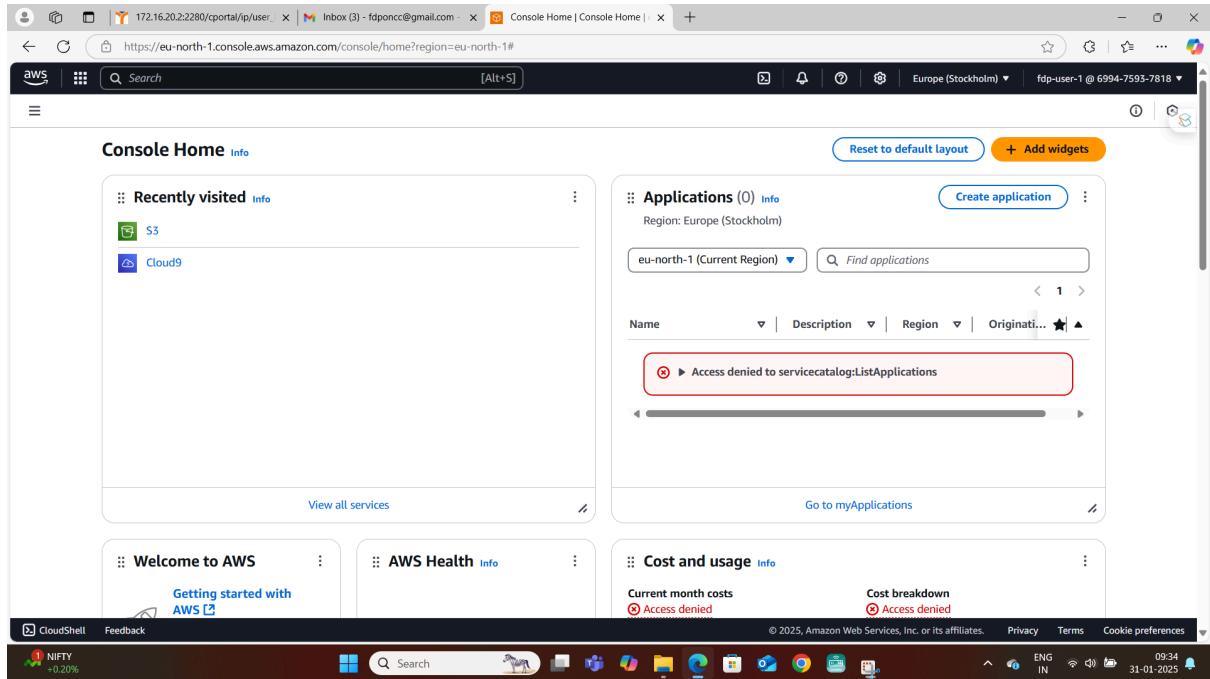
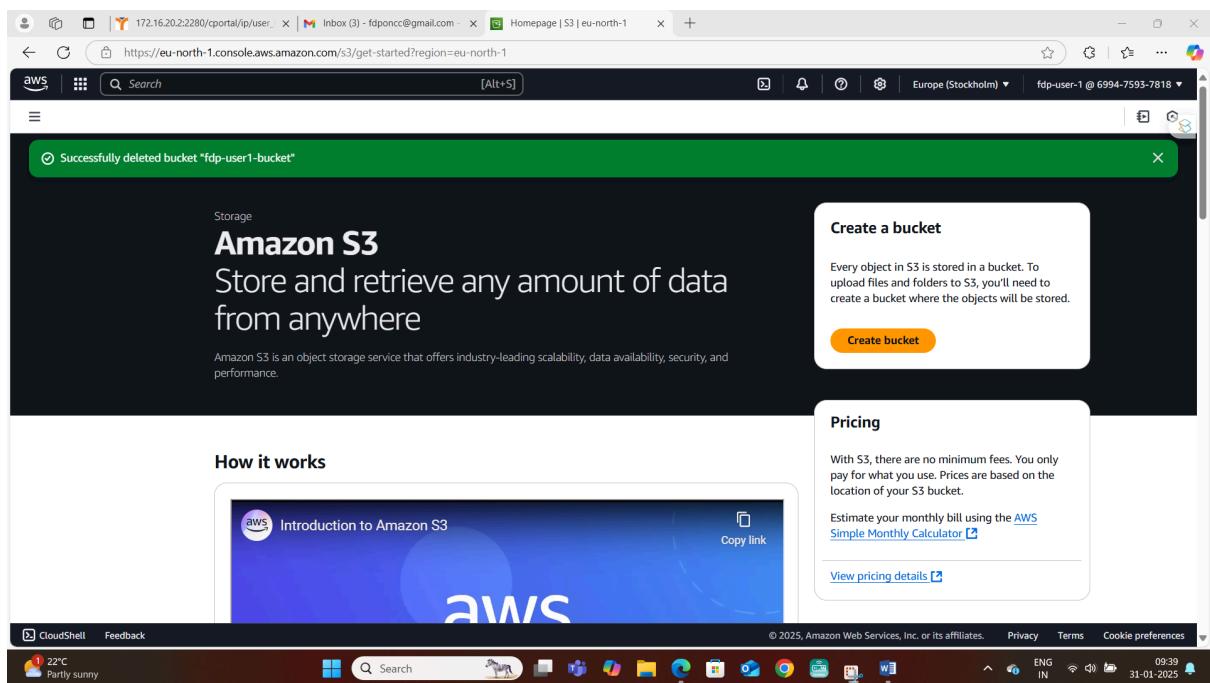


S3 ORCHASTRING SERVERLESS FUNCTIONS



CLICK S3 ----► CREATE BUCKET



SELECT THE BELOW OPTIONS

The screenshot shows the AWS S3 Buckets page. A green banner at the top indicates 'Successfully created bucket "fdp-user1-bucket"'. Below this, there's an 'Account snapshot' section with a link to 'View details'. Under 'General purpose buckets', there is one entry: 'fdp-user1-bucket' (Europe (Stockholm) eu-north-1). The table includes columns for Name, AWS Region, IAM Access Analyzer, and Creation date. Action buttons for Copy ARN, Delete, and Create bucket are available for each row.

CLICK ON YOUR BUCKET TO UPLOAD FILES

The screenshot shows the AWS S3 Upload status page. A green banner at the top says 'Upload succeeded'. The 'Upload: status' section shows 'Succeeded' (1 file, 0 B (0%)) and 'Failed' (0 files, 0 B (0%)). The 'Files and folders' section lists 'NUMBERS.txt' (text/plain, 0 B, Succeeded). The Windows taskbar at the bottom shows the upload was completed successfully.

IF YOU MODIFY A FILE AND REUPLOAD IT AGAIN THE VERSIONS CAN BE SEEN

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with navigation links like 'Amazon S3', 'General purpose buckets', 'Storage Lens', and 'Feature spotlight'. The main content area displays the 'NUMBERS.txt' object from the 'fdp-user1-bucket'. It shows two versions of the file:

Version ID	Type	Last modified	Size	Storage class
OU4E3OSO7zWoFH_W...	txt	January 31, 2025, 09:48:16 ...	0 B	Standard
m5_jtBt0_bSzZmvoF...	txt	January 31, 2025, 09:46:38 ...	0 B	Standard

At the bottom, there are standard browser controls for search, refresh, and navigation.

BUCKET POLICY, PERMISSIONS AND PROPERTIES FOR STATIC WEBSITE HOSTING

The screenshot shows the 'get-started' page for Amazon S3. The left sidebar is identical to the previous screenshot. The main content area has a dark background with white text. It features a large 'Create a bucket' button and a 'How it works' section with a video thumbnail titled 'Introduction to Amazon S3'.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket

Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the [AWS Simple Monthly Calculator](#).

[View pricing details](#)

Resources

Activate Windows
Go to Settings to activate Windows.

CloudShell Feedback

aws | Search [Alt+S] | Europe (Stockholm) | fdp-user-1 @ 6994-7593-7818 |

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region: Europe (Stockholm) eu-north-1

Bucket type: [Info](#)

- General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
- Directory

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name: [Info](#)

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.

[Choose bucket](#)

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.

[CloudShell](#) [Feedback](#)

[ACL enabled](#)

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Object Ownership: Bucket owner enforced

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.

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.

[Add tag](#)

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)
- Dual-layer server-side encryption with AWS Key Management Service keys (DSS-E-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- Disable
- Enable

Advanced settings

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

- Disable
- Enable

Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

ⓘ Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.

ⓘ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

PRESS CREATE BUCKET -> U WILL GET THE FOLLOWING PAGE

The screenshot shows the AWS S3 buckets page. At the top, a green banner says "Successfully created bucket 'fdp-user2-bucket'". Below it, there's an "Account snapshot" section and a table of general purpose buckets.

Name	AWS Region	IAM Access Analyzer	Creation date
fdp-user1-bucket	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	January 31, 2025, 09:42:31 (UTC+05:30)
fdp-user2-bucket	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	January 31, 2025, 14:33:03 (UTC+05:30)

GO TO UR BUCKET -> UPLOAD A HTML FILE

The screenshot shows the AWS S3 upload status page. It displays a summary of the upload and a detailed view of the uploaded file.

Summary

Destination	Succeeded	Failed
s3://fdp-user2-bucket	1 file, 296.0 B (100.00%)	0 files, 0 B (0%)

Files and folders

Name	Folder	Type	Size	Status	Error
second.html	-	text/html	296.0 B	Succeeded	-

CLICK ON HTML FILE

Screenshot of the AWS S3 Object Details page for 'second.html' in the 'fdp-user2-bucket'.

Object Overview:

- Owner:** b94c702ea25b7f7d0e775384fc0db2c6e1191470fc7b65b7bba4c7fba40ea89d
- AWS Region:** Europe (Stockholm) eu-north-1
- Last modified:** January 31, 2025, 14:35:52 (UTC+05:30)
- Size:** 296.0 B
- Type:** html
- Key:** second.html

Object URI: s3://fdp-user2-bucket/second.html

Amazon Resource Name (ARN): arn:aws:s3:::fdp-user2-bucket/second.html

Entity tag (Etag): de49fc0dc16015fdd740523f88656991

Object URL: https://fdp-user2-bucket.s3.eu-north-1.amazonaws.com/second.html

Object Management Overview:

- 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. Enabled.
- 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 made noncurrent and generate a delete marker on this date.

Storage class: Standard

Server-side encryption settings:

- Encryption type:** SSE-S3

Checksums:

- Checksum function:** CRC64NVME
- Checksum value:** tCAQuNPhnuo=

Tags (0):

Metadata (1):

Type	Key	Value
System defined	Content-Type	text/html

Object Lock:

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

Object Lock: Disabled

Amazon S3 currently does not support enabling Object Lock after a bucket has been created. To enable Object Lock for this bucket, contact [Customer Support](#).

**TO HOST WEBSITE ---- GO TO UR BUCKET ---- PROPERTIES ->Static website hosting ->
EDIT ->**

Screenshot of the AWS S3 Bucket Overview page for 'fdp-user2-bucket'.

Bucket overview

AWS Region: Europe (Stockholm) eu-north-1
Amazon Resource Name (ARN): arn:aws:s3:::fdp-user2-bucket
Creation date: January 31, 2025, 14:33:05 (UTC+05:30)

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: Enabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

MFA Delete: Disabled

Tags (0)
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key: cloudShell Value: Feedback

No tags associated with this resource.

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

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)

Bucket Key: When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

Enabled

Intelligent-Tiering Archive configurations (0)
Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. [Learn more](#)

[Find Intelligent-Tiering Archive configurations](#)

Name	Status	Scope	Days until transition to Archive Access tier	Days until transition to Deep Archive Access tier
No archive configurations	No configurations to display.			

[Create configuration](#)

Server access logging [Info](#)
Log requests for access to your bucket. Use [CloudWatch](#) to check the health of your server access logging. [Learn more](#)

Server access logging: Disabled

AWS CloudTrail data events [Info](#)
Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. [Learn more](#)

Name: [Access](#)

You don't have permission to get AWS CloudTrail data events details
You or your AWS administrator must update your IAM permissions to allow `cloudtrail:DescribeTrails`. After you obtain the necessary permission, choose Refresh. Learn more about [Identity and access management in Amazon S3](#)

API response

Event notifications (0)
Send a notification when specific events occur in your bucket. [Learn more](#)

Name	Event types	Filters	Destination type	Destination
No event notifications	Choose Create event notification to be notified when a specific event occurs.			

[Create event notification](#)

Amazon EventBridge
For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. [Learn more](#) or see [EventBridge pricing](#)

Send notifications to Amazon EventBridge for all events in this bucket
Off

Transfer acceleration
Use an accelerated endpoint for faster data transfers. [Learn more](#)

Transfer acceleration is not available for this bucket
Amazon S3 Transfer acceleration is not available for your bucket because it is located in an unsupported Region. [Learn more](#)

Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

Object Lock: Disabled

Requester pays
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays: Disabled

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 -> GIVE FILE NAME -> SAVE

The screenshot shows the 'Edit static website hosting' configuration page for an S3 bucket named 'fdp-user2-bucket'. The 'Static website hosting' section is enabled. Under 'Hosting type', 'Host a static website' is selected. The 'Index document' field contains 'second.html'. The 'Error document' field contains 'error.html'. A note at the bottom states: '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.' At the bottom right are 'Cancel' and 'Save changes' buttons.

aws | Search [Alt+S] | Europe (Stockholm) | fdp-user-1 @ 6994-7593-7818 | ☰ | 🔍 | ⓘ | 🌐 | Edit static website hosting

☰ Amazon S3 > Buckets > fdp-user2-bucket > Edit static website hosting

Edit static website hosting [Info](#)

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 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.
second.html

Error document - optional
This is returned when an error occurs.
error.html

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

1

JSON Ln 1, Col 1 Errors: 0 Warnings: 0

Cancel Save changes

U WILL GET THIS PAGE -> CLICK THE URL TO RUN PROGRAM ->

Bucket overview

AWS Region: Europe (Stockholm) eu-north-1 | Amazon Resource Name (ARN): arn:aws:s3:::fdp-user2-bucket | Creation date: January 31, 2025, 14:33:03 (UTC+05:30)

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

Enabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Tags (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key	Value
No tags associated with this resource.	

Default encryption

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type

Server-side encryption with Amazon S3 managed keys (SSE-S3)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

Enabled

Intelligent-Tiering Archive configurations (0)

Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. [Learn more](#)

Server access logging

Log requests for access to your bucket. Use [CloudWatch](#) to check the health of your server access logging. [Learn more](#)

AWS CloudTrail data events

Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. [Learn more](#)

Event notifications (0)

Send a notification when specific events occur in your bucket. [Learn more](#)

Amazon EventBridge

For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. [Learn more](#) or see [EventBridge pricing](#)

Transfer acceleration

Use an accelerated endpoint for faster data transfers. [Learn more](#)

Object Lock

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays

Disabled

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

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://fdp-user2-bucket.s3-website.eu-north-1.amazonaws.com>

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 4GHC477H47C1D002
- HostId: EHe+wJm6tUsQ3qBX8FVgnr/l4knxgE1v40G5AiUd0M4kF9cXBpLpbEquYL+9oQbTF/Sgs1QL2N8Sxcmle8YDzbTFHm10ZUTs

CHANGE

>PERMISSIONS-> BUCKET POLICY -> WRITE THE BELOW CODE IN BUCKET POLICY->

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PublicReadGetObject",  
            "Effect": "Allow",  
            "Principal": "*",  
            "Action": [  
                "s3:GetObject"  
            ],  
            "Resource": [  
                "arn:aws:s3:::<Bucket-Name>/*"  
            ]  
        }  
    ]  
}
```

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
arnaws:s3:::fdp-user2-bucket

Policy

```
1▼ {  
2    "Version": "2012-10-17",  
3    "Statement": [  
4        {  
5            "Sid": "PublicReadGetObject",  
6            "Effect": "Allow",  
7            "Principal": "*",  
8            "Action": [  
9                "s3:GetObject"  
10            ],  
11            "Resource": [  
12        }  
13    ]  
14}
```

Edit statement
PublicReadGetObject [Remove](#)

Add actions
Choose a service Filter services

Included

Actions

JSON Ln 12, Col 17

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

[Preview external access](#)

You need permissions
User: arn:aws:iam::699475937818:user/fdp-user-1 is not authorized to perform: access-analyzer:ValidatePolicy on resource: arn:aws:access-analyzer:eu-north-1:699475937818:*

[Cancel](#) [Save changes](#)

THEN SAVE AND RUN THE URL AGAIN

