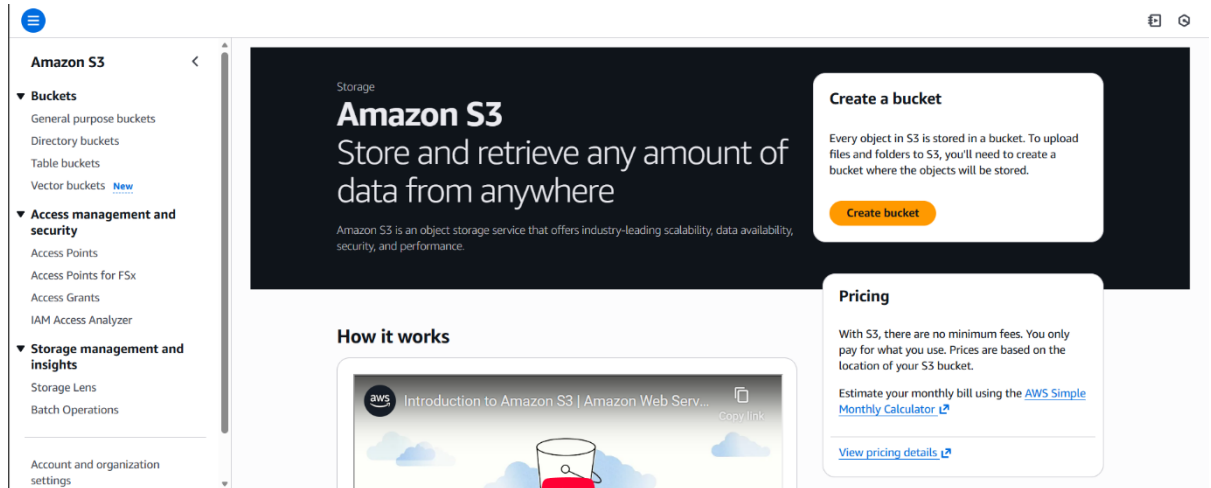


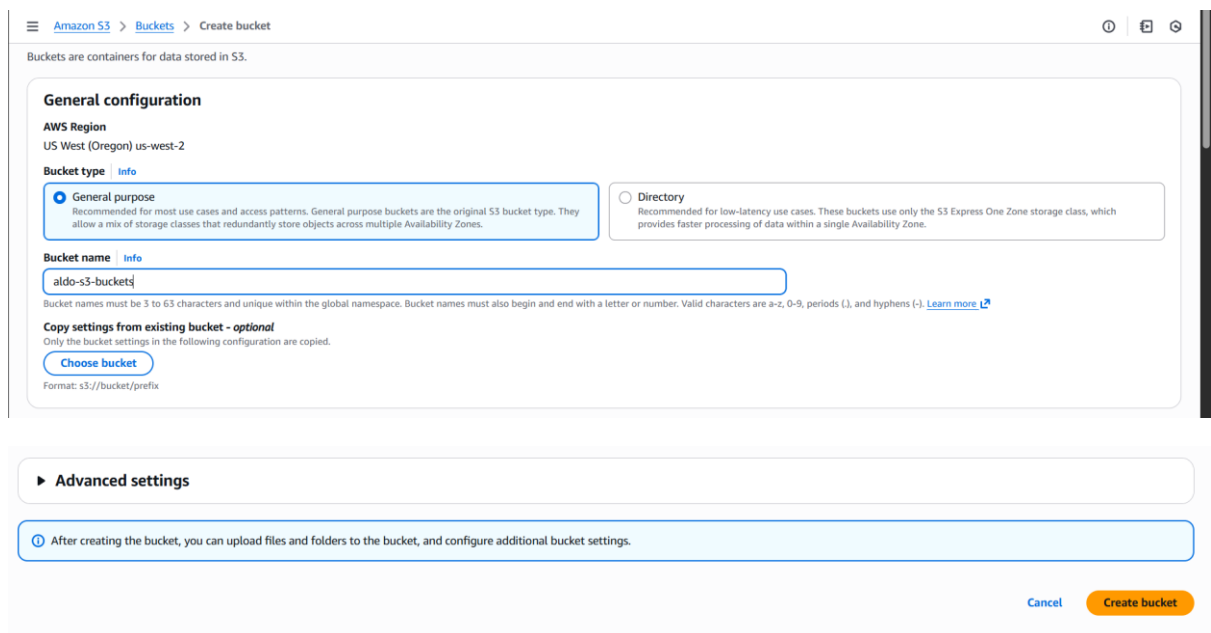
# Deploy Simple Website Using S3

## 1. In S3 console click Create Bucket



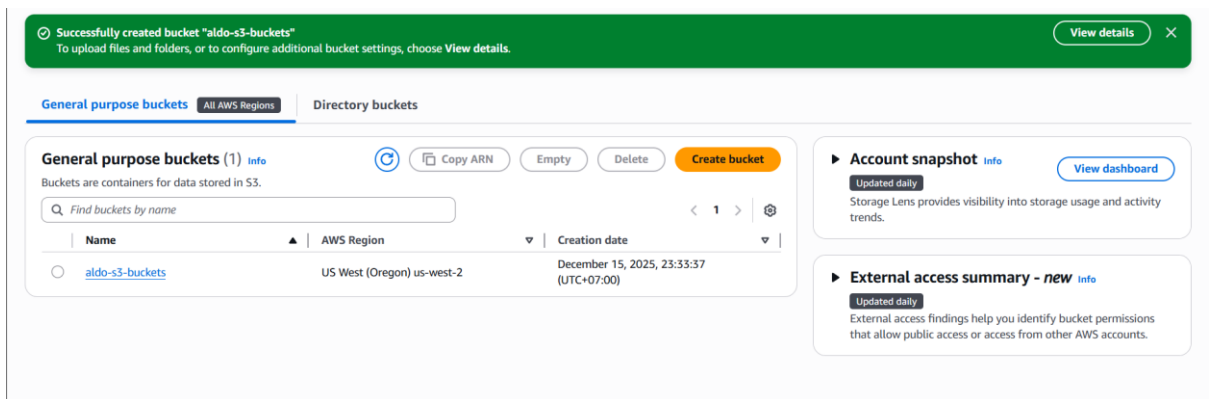
## 2. In page Create Bucket

1. Create your Bucket Name (must be unique)
2. Leave all default
3. Scroll until bottom and then click create bucket



## 3. Then you will see your bucket already successfully create

#### 4. Click your bucket name for upload file and configure bucket

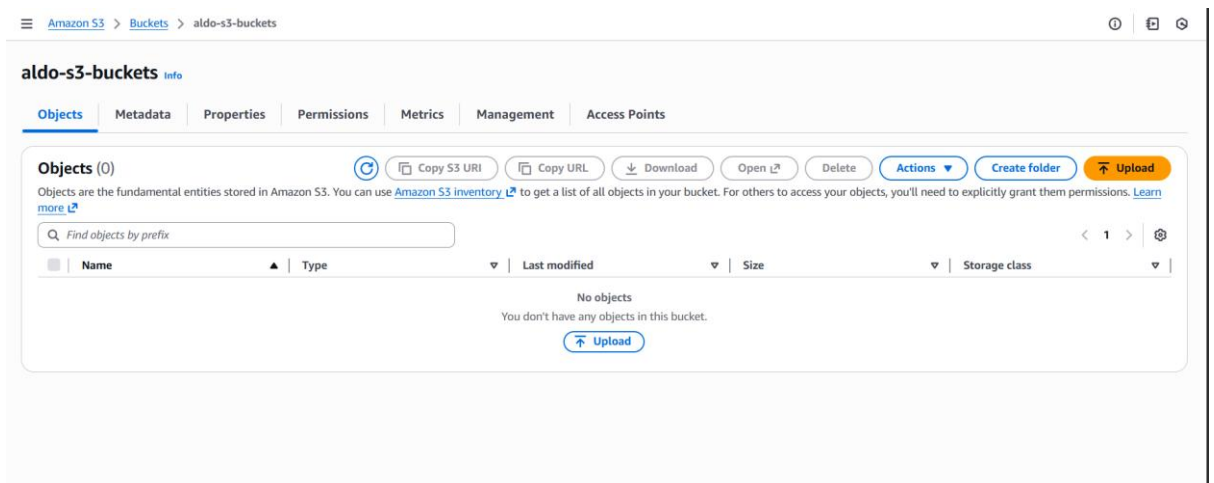


#### 5. Inside page bucket you will see a few configure

#### 6. First we have to upload your simple website

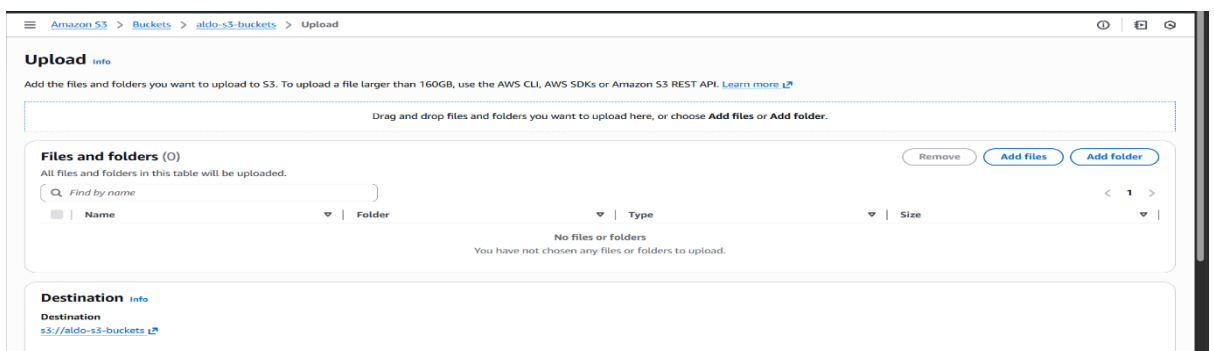
(in here I already make a simple website using HTML)

#### 7. Click upload



#### 8. In page upload , you click add file (chosed your website coding using HTML)

#### 9. The upload the file (if you using website using a image you have to upload the image )



#### 10. After upload you files you will see your file name

11. Then Scroll to bottom and click upload

12. You will see upload successfully in page , click X and then click close

**Files and folders** (1 total, 855.0 B)  
All files and folders in this table will be uploaded.

Remove Add files Add folder

Find by name

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	aldo-portfolio.html	-	text/html	855.0 B

**Destination** Info

**Destination**  
[s3://aldo-s3-buckets](#)

► **Destination details**  
Bucket settings that impact new objects stored in the specified destination.

► **Permissions**  
Grant public access and access to other AWS accounts.

► **Properties**  
Specify storage class, encryption settings, tags, and more.

Cancel Upload

Upload succeeded  
For more information, see the Files and folders table.

After you navigate away from this page, the following information is no longer available.

**Summary**

<b>Destination</b> <a href="#">s3://aldo-s3-buckets</a>	<b>Succeeded</b> 1 file, 855.0 B (100.00%)	<b>Failed</b> 0 files, 0 B (0%)
--	---	------------------------------------

Files and folders Configuration

**Files and folders** (1 total, 855.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
<a href="#">aldo-portfolio.html</a>	-	text/html	855.0 B	Succeeded	-

**Upload: status** Close

After you navigate away from this page, the following information is no longer available.

**Summary**

<b>Destination</b> <a href="#">s3://aldo-s3-buckets</a>	<b>Succeeded</b> 1 file, 855.0 B (100.00%)	<b>Failed</b> 0 files, 0 B (0%)
--	---	------------------------------------

Files and folders Configuration

13. You will back to configure page

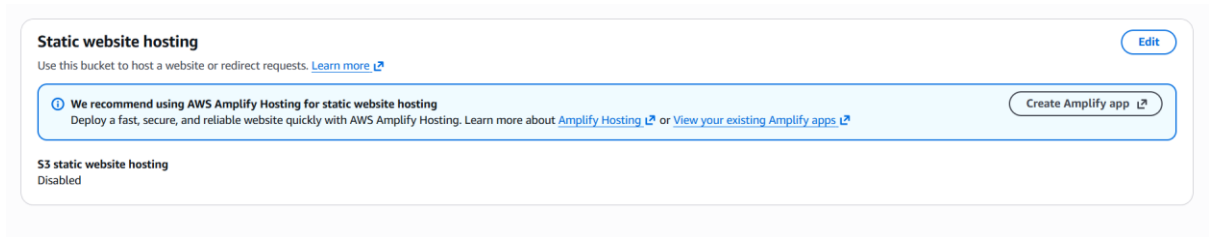
14. Click page Properties

15. Then just scroll until bottom and you will see “Static Website Hosting” click edit

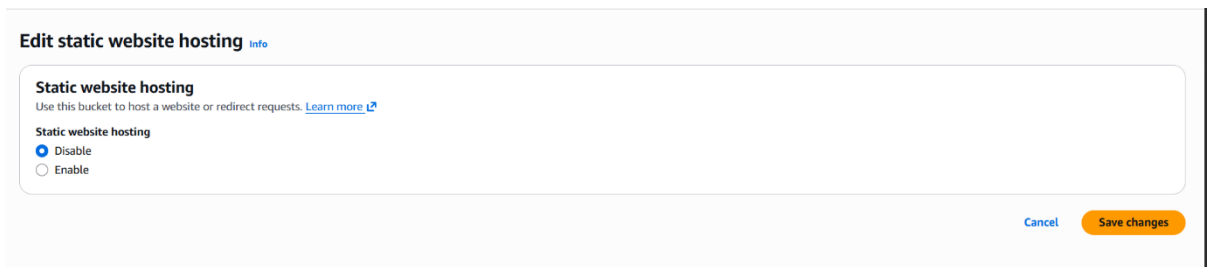
Amazon S3 > Buckets > aldo-s3-buckets

**aldo-s3-buckets** Info

Objects Metadata **Properties** Permissions Metrics Management Access Points



16. In page edit static website hosting click enable



17. After that you will see column index document and error document

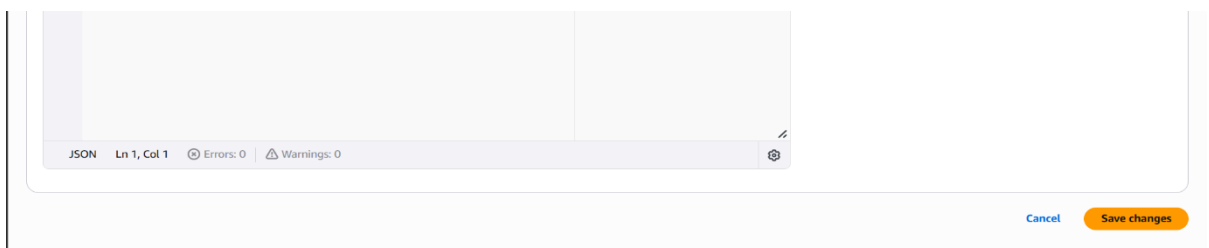
18. In the column index document fill with the name of the HTML file you uploaded at the beginning

19. In error document just leave blank

**Index document**  
Specify the home or default page of the website.

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

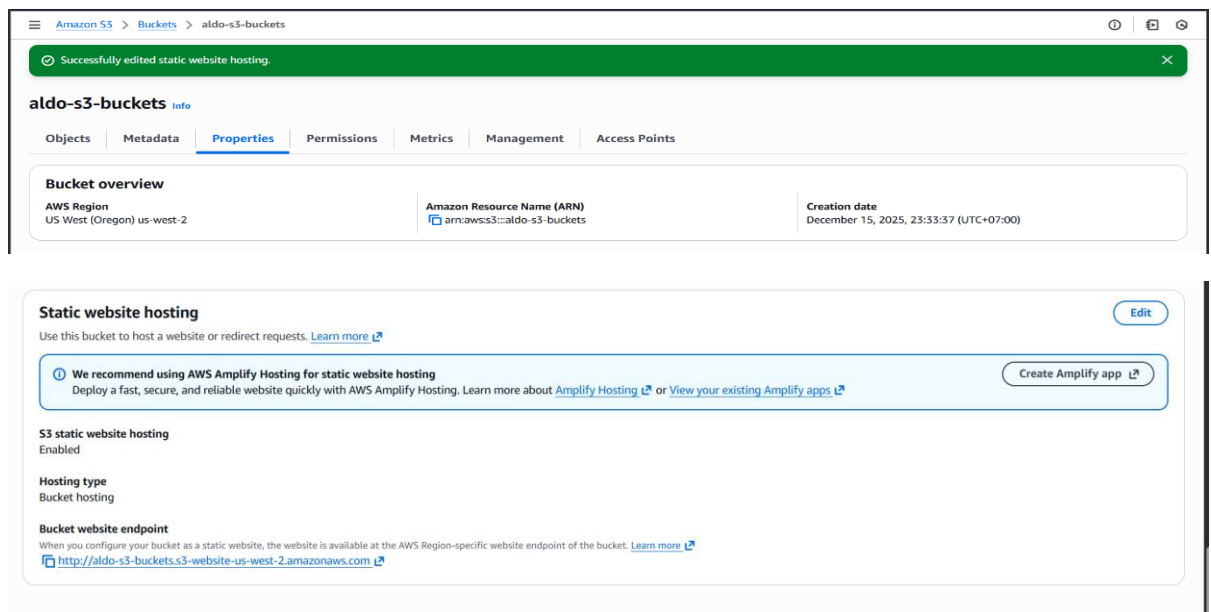
20. Then Scroll until bottom and click save changes



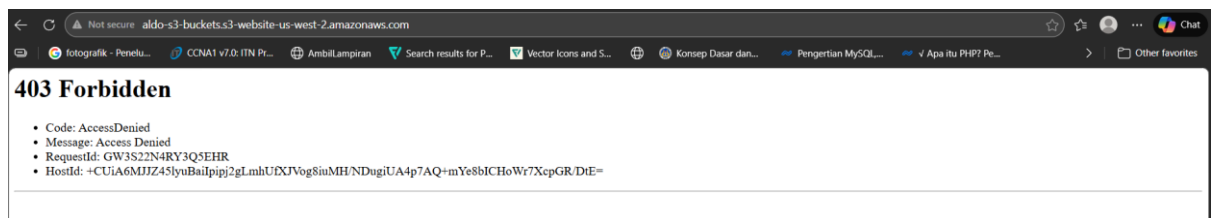
21. You will back to bucket console properties

22. Scroll to bottom and will see a link website in static website hosting page

23. Copy the link and open in new tab

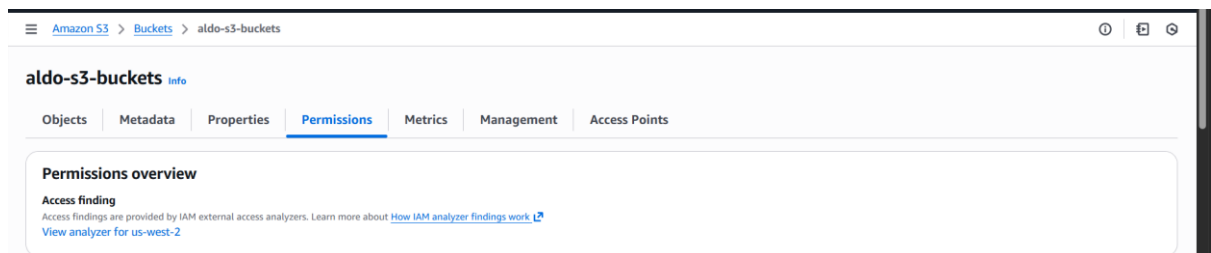


24. In the link that you copied, you will see a website cannot be accessed



25. Back to AWS console (don't close the website)

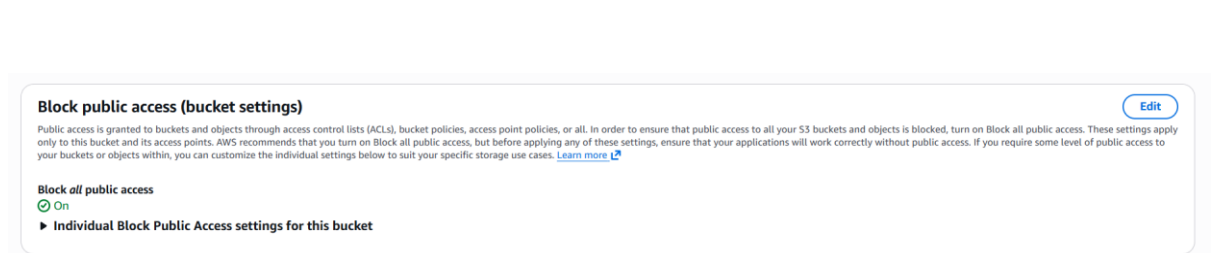
26. Go to page permissions



27. Inside page permissions click edit in column block public access

28. Uncheck Block all public access

29. Click save changes and confirm



**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.

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

**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.

[Cancel](#) [Confirm](#)

30. Then find column Object Ownership

31. Click edit

32. Inside page Object Ownership chose ACLs enabled

33. An check box I Acknowledge the ACLs will be restored

34. Scroll to bottom and click save changes

**Object Ownership** [Edit](#)

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.

**Object Ownership**  
Bucket owner enforced

ACLs are disabled. All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

Amazon S3 > Buckets > aldo-s3-buckets > Edit Object Ownership

### Edit Object Ownership info

**Object Ownership**  
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.

**Object Ownership**

☐ 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.

**⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.**

**⚠️ Enabling ACLs turns off the bucket owner enforced setting for Object Ownership**  
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

☐ I acknowledge that ACLs will be restored.

**Object Ownership**

☒ Bucket owner preferred  
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

35. Then You have to edit bucket policy

36. Click edit

37. Click + Add new statement

### 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](#)

[Edit](#) [Delete](#)

No policy to display.

[Copy](#)

**Bucket ARN**  
arn:aws:s3:::aldo-s3-buckets

**Policy**

1	Edit statement
	<p><b>Select a statement</b></p> <p>Select an existing statement in the policy or add a new statement.</p> <p><a href="#">+ Add new statement</a></p>

[+ Add new statement](#)

38. you have fill the statement

1. “sid” : “PublicReadGetObject”
2. “effect” : “Allow”
3. “Principal” : “ \* “
4. “Action” : “s3:GetObject”
5. “Resource” : “arn:aws:s3:::aldo-s3-buckets/\*”

39. Click save changes

arn:aws:s3:::aldo-s3-buckets

#### Policy

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

+ Add new statement

40. Then go back to page configure

41. Click Objects

42. Check box your html file

43. Click Action and click make publick using ACL

Amazon S3 > Buckets > aldo-s3-buckets

**aldos3-buckets** info

Objects (1/1)

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 object permissions. [Learn more](#)

Find objects by prefix

Name	Type	Last modified	Size
<input checked="" type="checkbox"/> aldo-portfolio.html	html	December 15, 2025, 23:35:24 (UTC+07:00)	

Actions menu:

- Download as
- Share with a presigned URL
- Calculate total size
- Copy
- Move
- Initiate restore
- Query with S3 Select
- Edit actions
  - Rename object
  - Edit storage class
  - Edit server-side encryption
  - Edit tags
- Make public using ACL



44. Click make public
45. Then back to your website and click refresh
46. Now you will see the website

