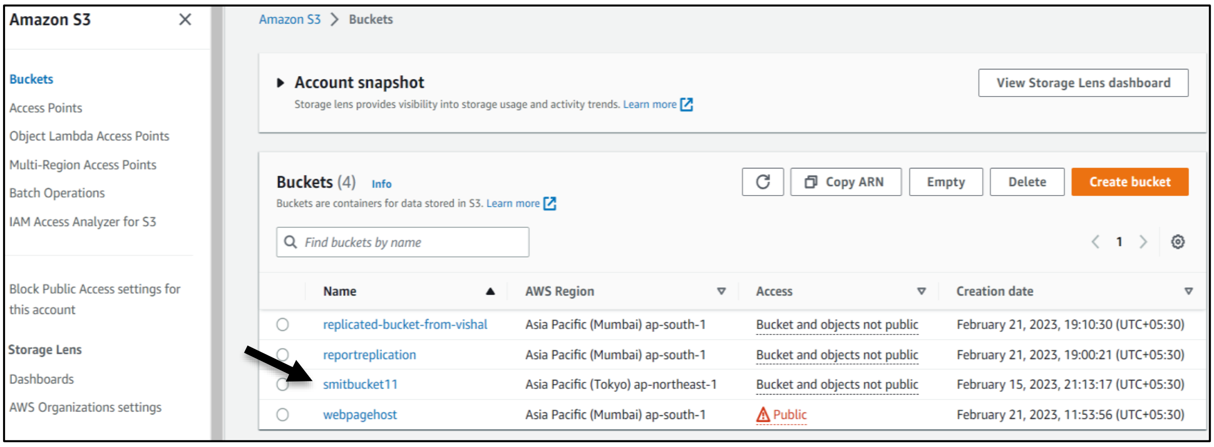
Host Static Website from S3 Bucket

- Login to your S3 console
- In the left navigation panel choose **Buckets**.


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Amazon S3 > Buckets
View Storage Lens dashboard
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1

Account snapshot

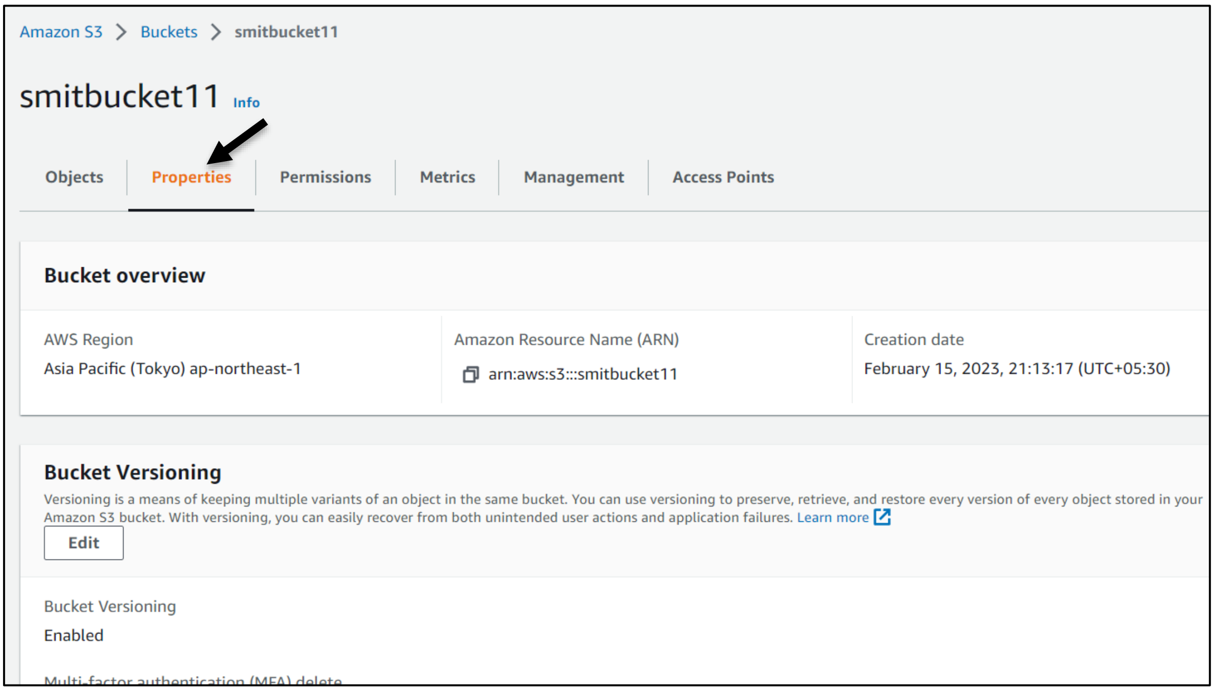
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (4) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	replicated-bucket-from-vishal	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 21, 2023, 19:10:30 (UTC+05:30)
○	reportreplication	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 21, 2023, 19:00:21 (UTC+05:30)
○	smitbucket11	Asia Pacific (Tokyo) ap-northeast-1	Bucket and objects not public	February 15, 2023, 21:13:17 (UTC+05:30)
○	webpagehost	Asia Pacific (Mumbai) ap-south-1	⚠ Public	February 21, 2023, 11:53:56 (UTC+05:30)

- Download the CSS template, extract it and then add the contents to the **"smitbucket11"** bucket.
- Click on bucket **'smitbucket11'**
- Open **properties** option



Bucket overview

AWS Region
Asia Pacific (Tokyo) ap-northeast-1

Amazon Resource Name (ARN)
arn:aws:s3:::smitbucket11

Creation date
February 15, 2023, 21:13:17 (UTC+05:30)

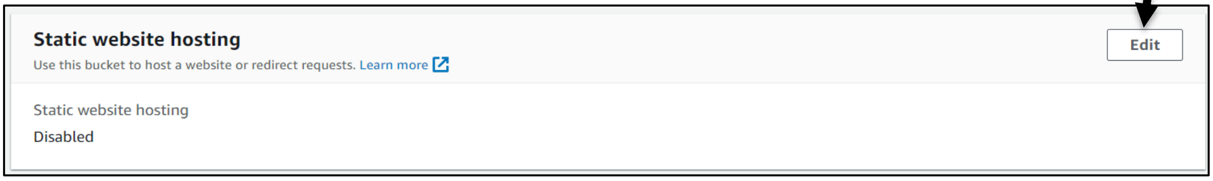
Bucket Versioning

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

- Scroll down to **Static Website Hosting** and click on Edit

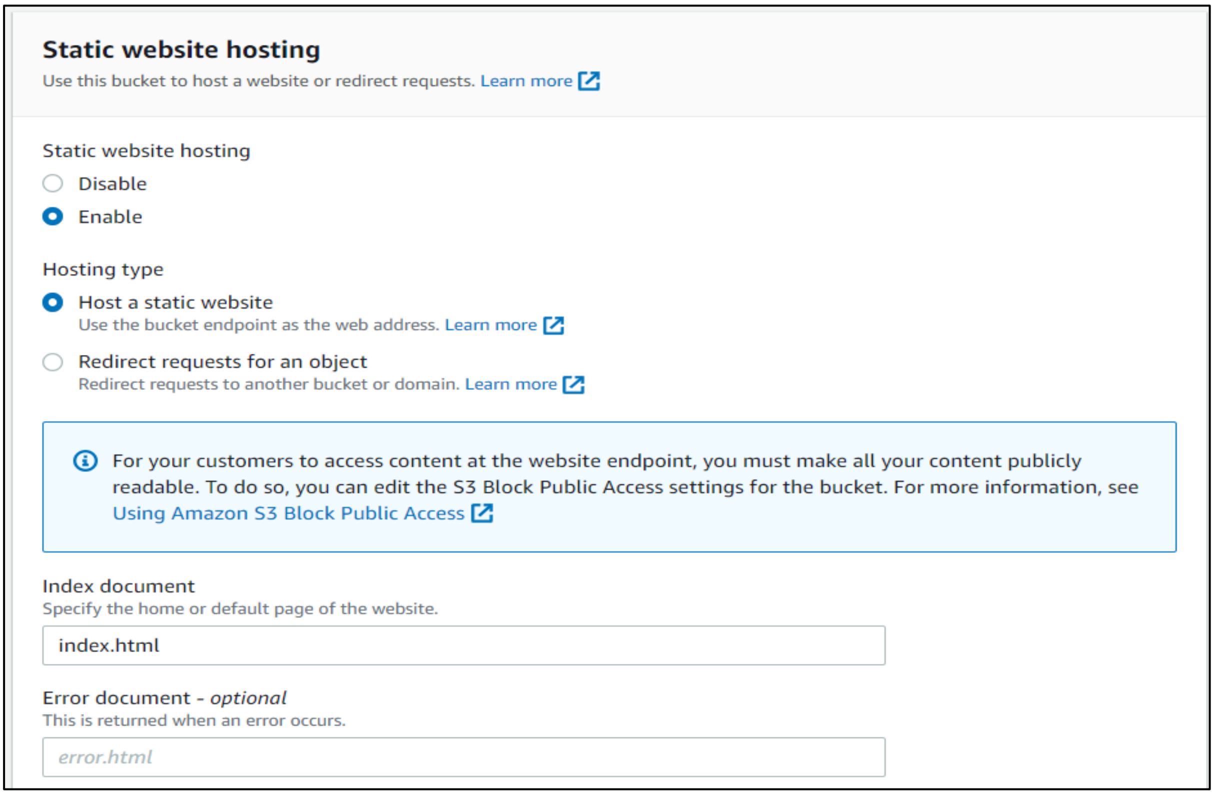


Static website hosting

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

Static website hosting
Disabled

- Enable **Static website hosting**
- Hosting type – select **Host a static website**
- Write **index.html** in Index document box



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

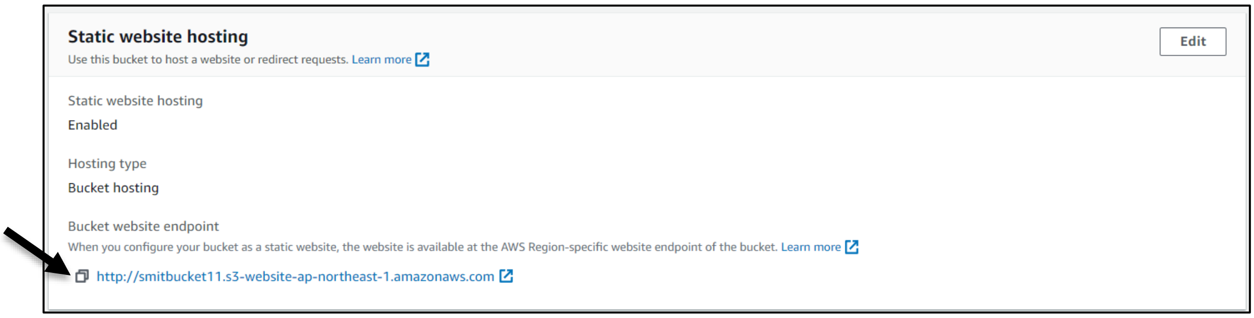
Index document
Specify the home or default page of the website.

index.html

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

error.html

- Click on **Save changes**



Static website hosting

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

Static website hosting
Enabled

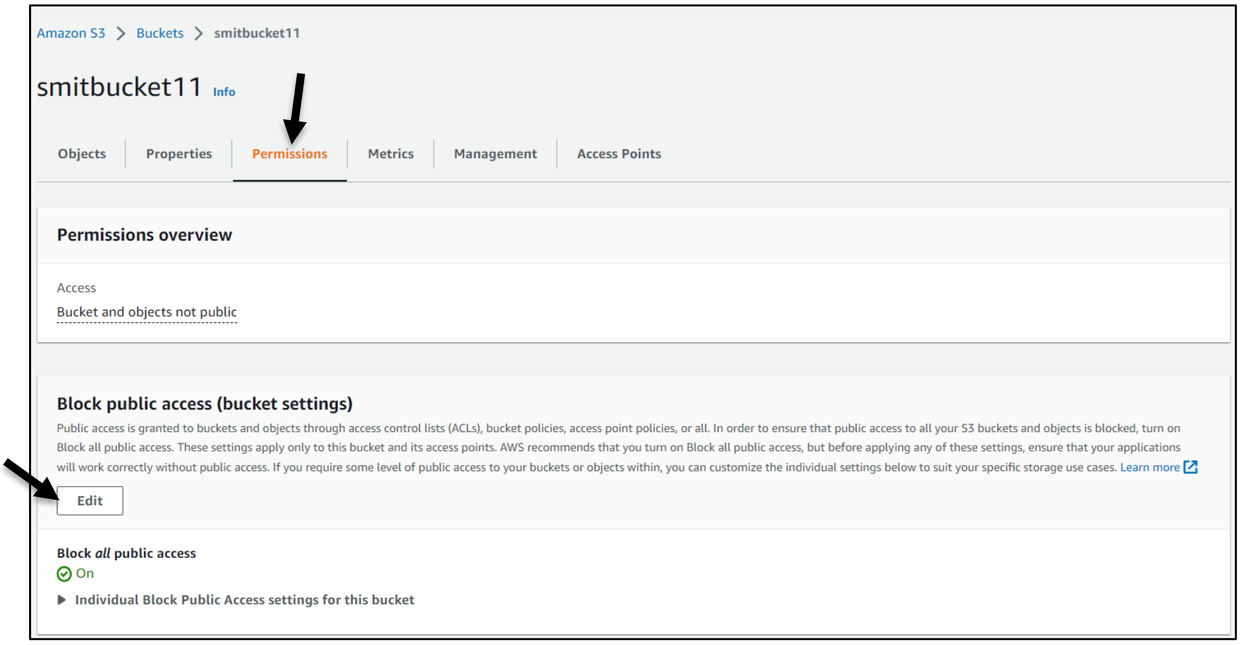
Hosting type
Bucket hosting

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://smitbucket11.s3-website-ap-northeast-1.amazonaws.com

- By following the above steps, we obtain a **URL for static website hosting**.

- Open **properties** option



Amazon S3 > Buckets > smitbucket11

smitbucket11 Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Permissions overview

Access

Bucket and objects not public

Block public access (bucket settings)

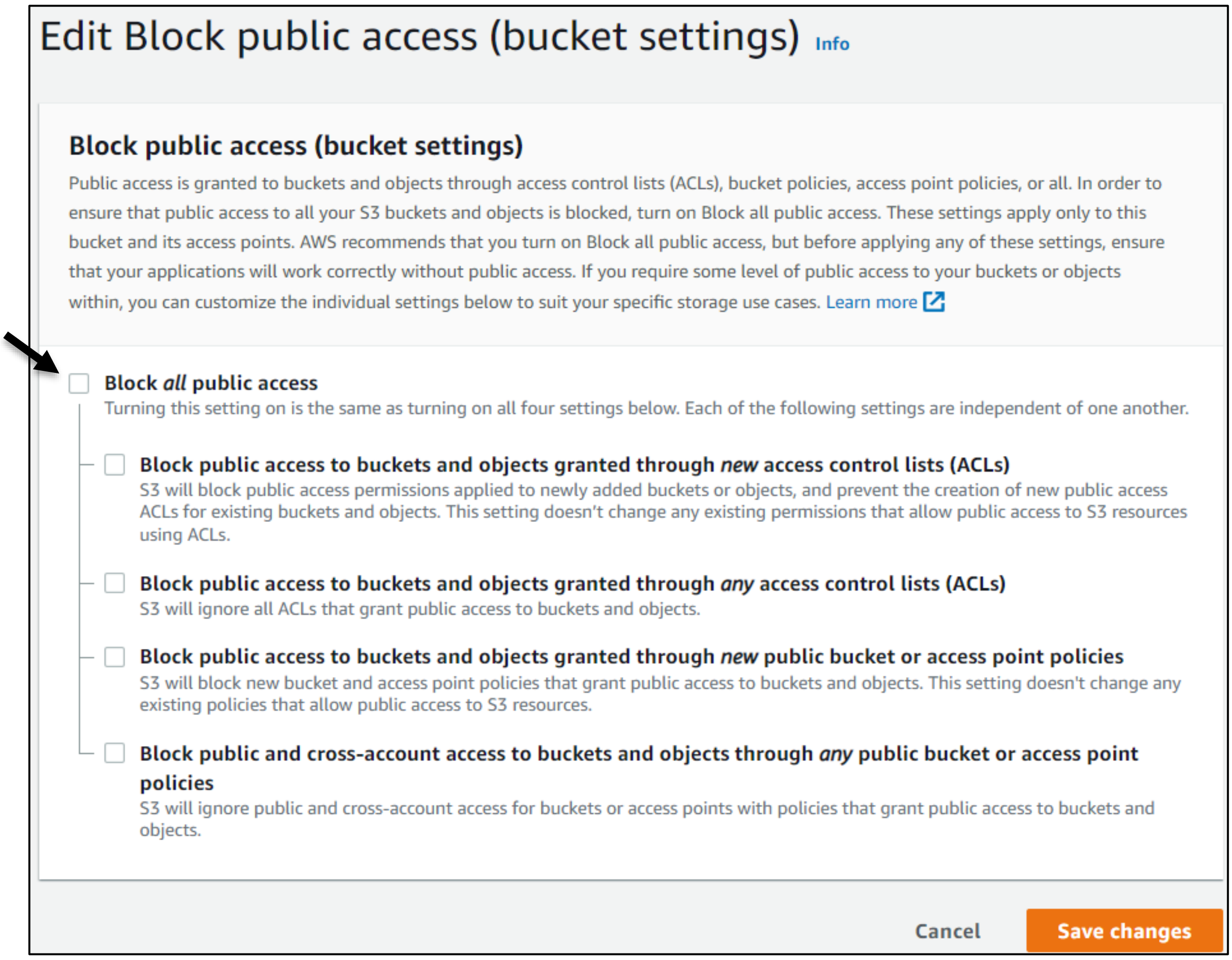
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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

▶ **Individual Block Public Access settings for this bucket**

- Click on Edit box of **Block public access (bucket settings)**



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.

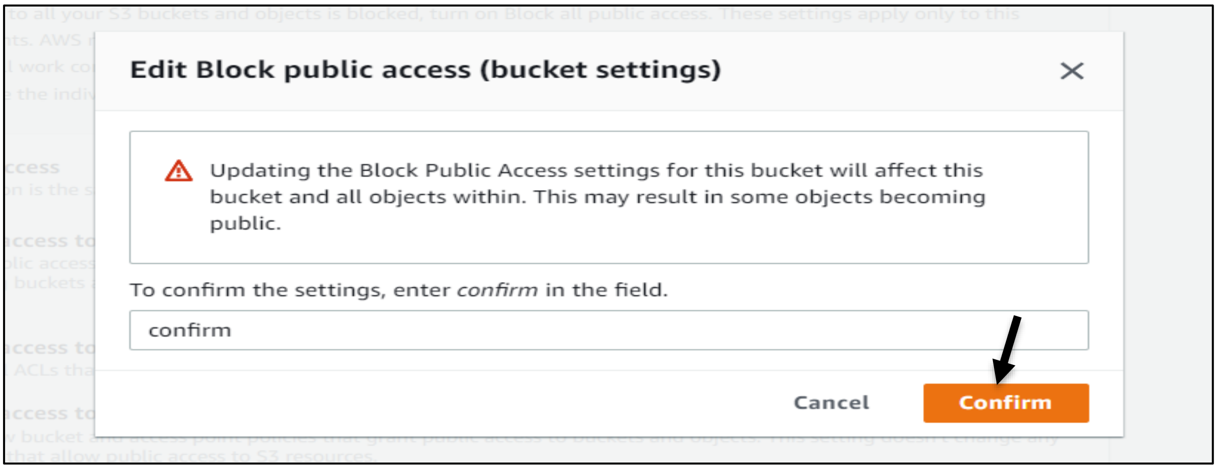
□ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing 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.

- Deselect **Block all public access** to give public access to the bucket.



Edit Block public access (bucket settings)

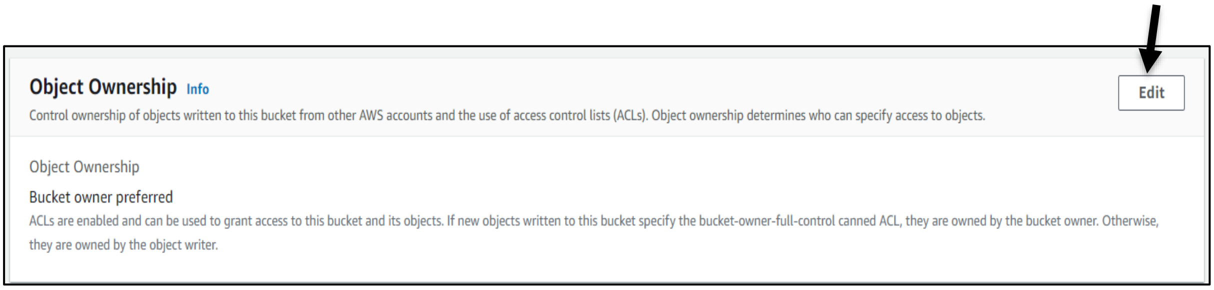
⚠ Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

confirm

- Write **confirm in box** and click on **confirm**

- In Permission option, **edit Object Ownership**



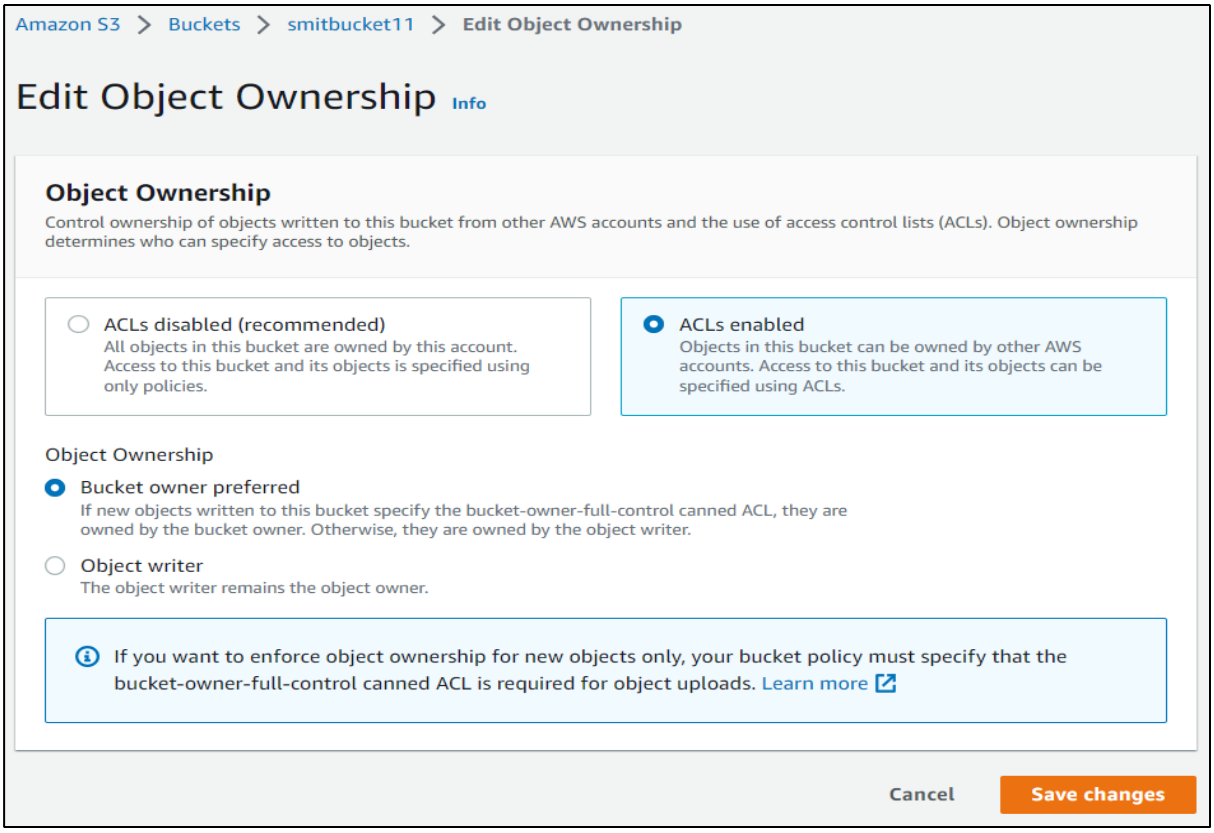
Object Ownership Info

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.

Object Ownership

Bucket owner preferred

ACLs are enabled and can be used to grant access to this bucket and its objects. 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.



Amazon S3 > Buckets > smitbucket11 > 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.

○ 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.

Object Ownership

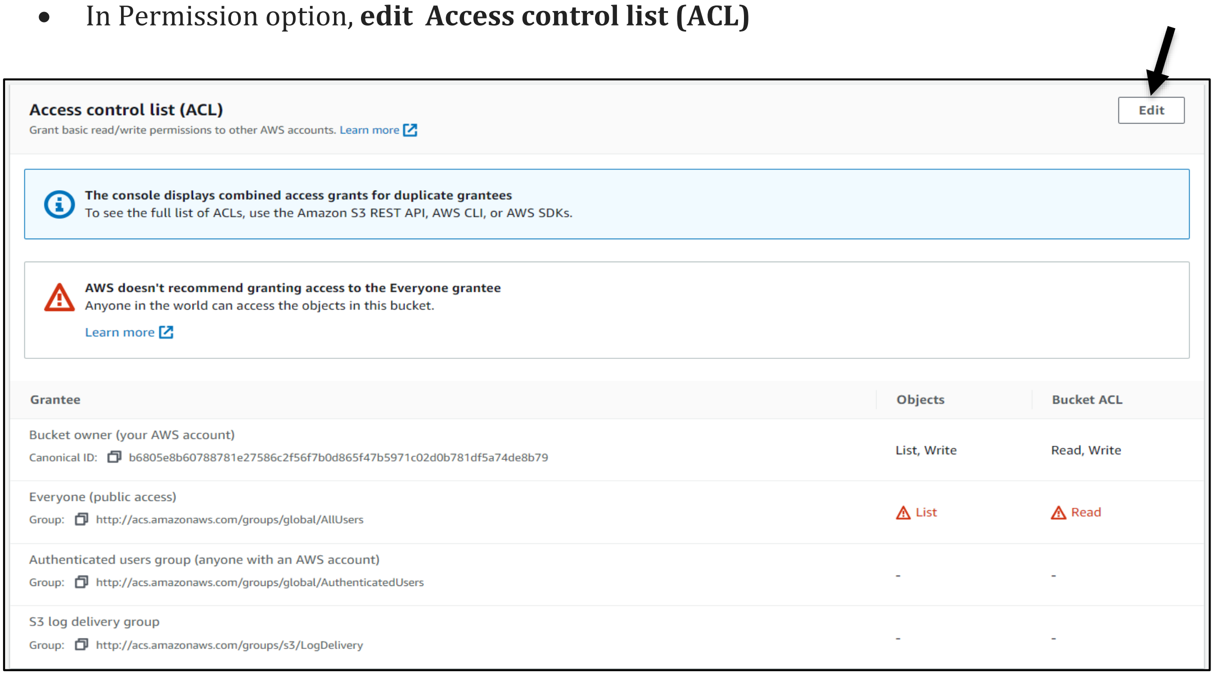
● Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

○ Object writer
The object writer remains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

- Select **ACLs enabled** in Object Ownership
- And Select **Bucket owner preferred**
- Click on **Save changes**

- In Permission option, **edit Access control list (ACL)**



Access control list (ACL)

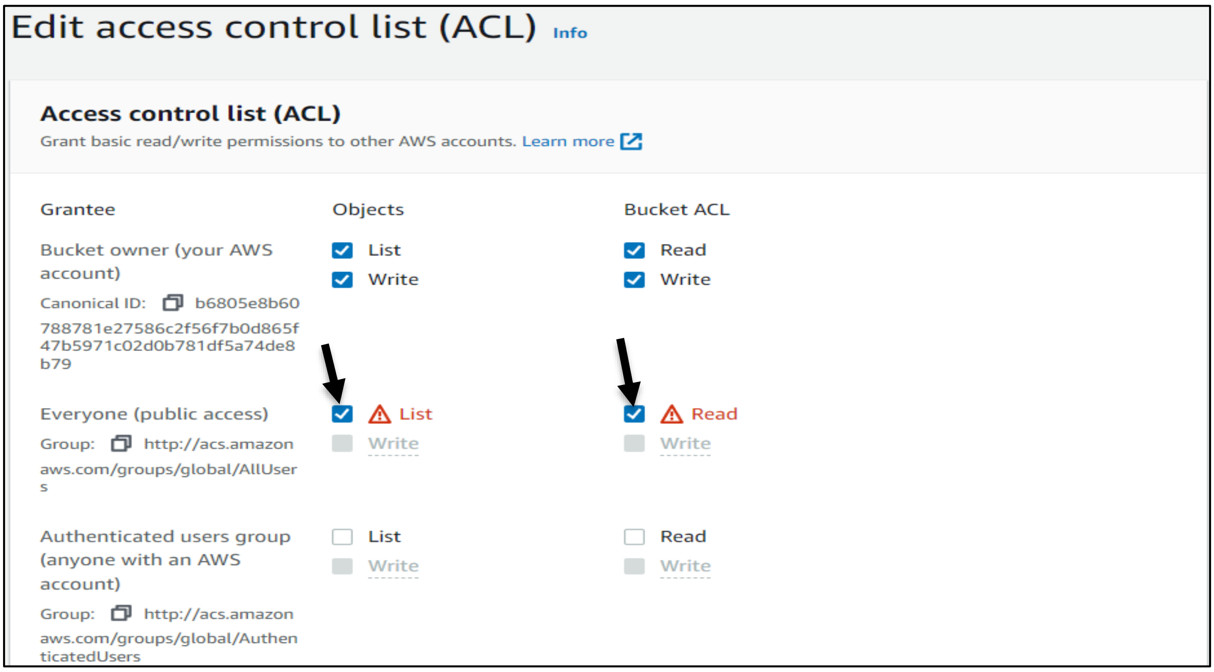
Grant basic read/write permissions to other AWS accounts. Learn more

The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

AWS doesn't recommend granting access to the Everyone grantee
Anyone in the world can access the objects in this bucket.

Learn more

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: b6805e8b60788781e27586c2f56f7b0d865f47b5971c02d0b781df5a74de8b79	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	⚠ List	⚠ Read
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-



Edit access control list (ACL)

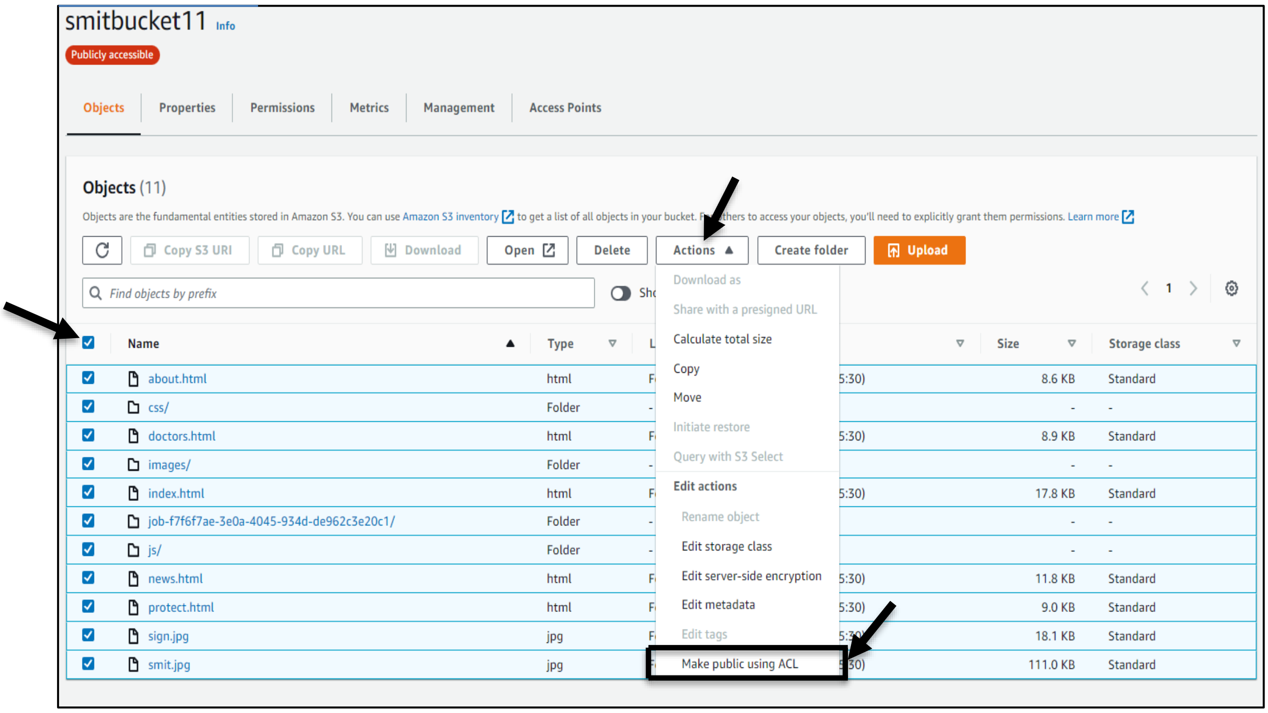
Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: b6805e8b60788781e27586c2f56f7b0d865f47b5971c02d0b781df5a74de8b79	☑ List ☑ Write	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	☑ ⚠ List □ Write	☑ ⚠ Read □ Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	□ List □ Write	□ Read □ Write

- In Everyone (public access), select **List** and **Read**
- Select box [ ] **I understand the effects of these changes on my objects and buckets.**
- Click on **Save changes**

- Go to bucket **‘smitbucket11’** and select all the objects



smitbucket11 Info

Publicly accessible

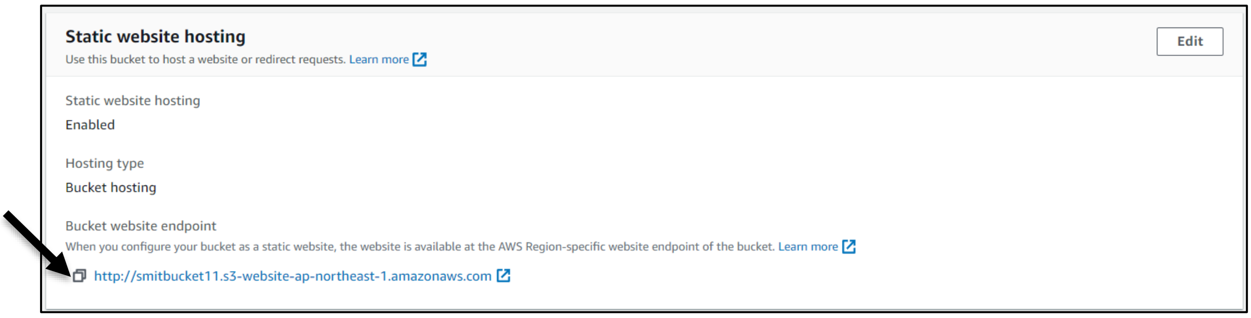
Objects (11)

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. F... thers to access your objects, you'll need to explicitly grant them permissions. Learn more

☑	Name	Type	L		Size	Storage class
☑	about.html	html	F	5:30)	8.6 KB	Standard
☑	css/	Folder	-		-	-
☑	doctors.html	html	F	5:30)	8.9 KB	Standard
☑	images/	Folder	-		-	-
☑	index.html	html	F	5:30)	17.8 KB	Standard
☑	job-f7f6f7ae-3e0a-4045-934d-de962c3e20c1/	Folder	-		-	-
☑	js/	Folder	-		-	-
☑	news.html	html	F	5:30)	11.8 KB	Standard
☑	protect.html	html	F	5:30)	9.0 KB	Standard
☑	sign.jpg	jpg	F	5:30)	18.1 KB	Standard
☑	smit.jpg	jpg	F	5:30)	111.0 KB	Standard

- After selecting all objects in bucket, click on **Actions** button and in that click on **Make public using ACL** and Make it Public.

- Now click on **bucket**, after that scroll down in **properties** to **Static Website Hosting**



Static website hosting

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

Static website hosting
Enabled

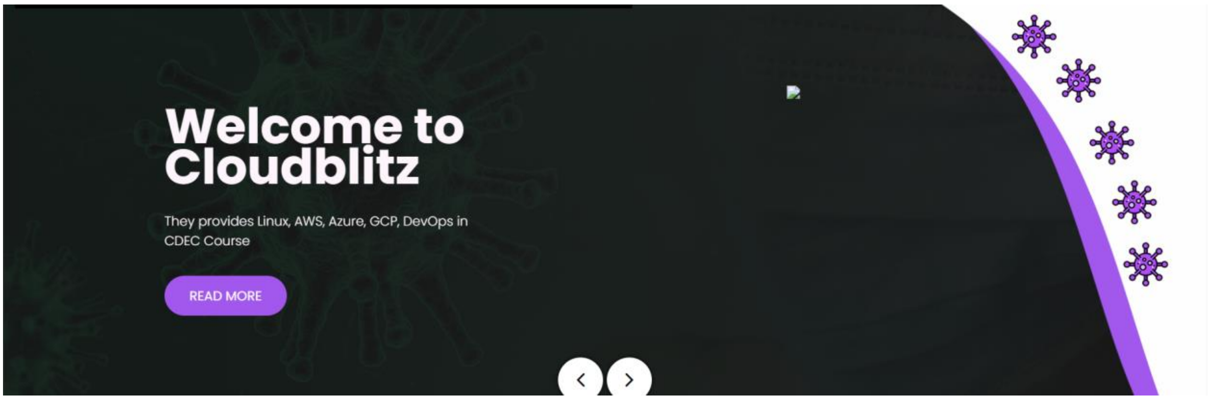
Hosting type
Bucket hosting

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://smitbucket11.s3-website-ap-northeast-1.amazonaws.com

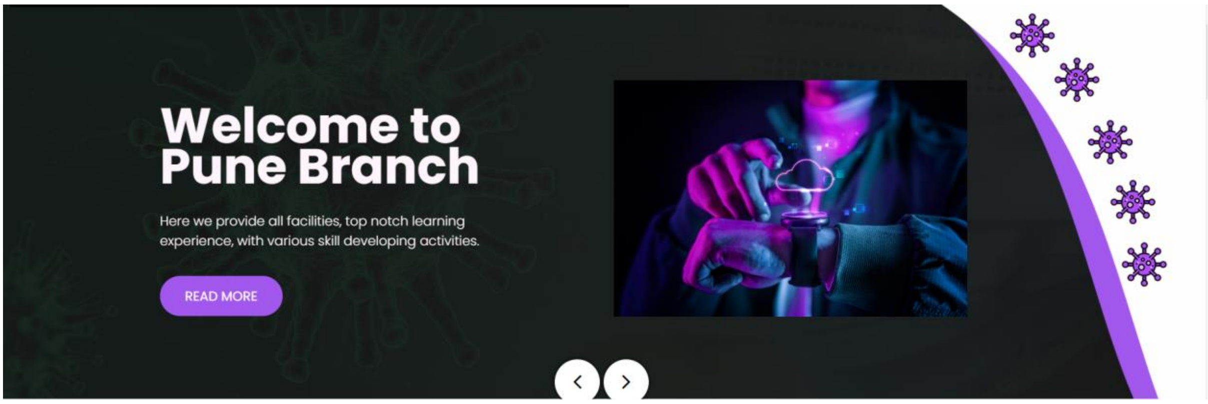
- Copy that link and paste to New Tab in Browser and hit the website. http://smitbucket11.s3-website-ap-northeast-1.amazonaws.com

- **So you can see now hosted Webpage below.**



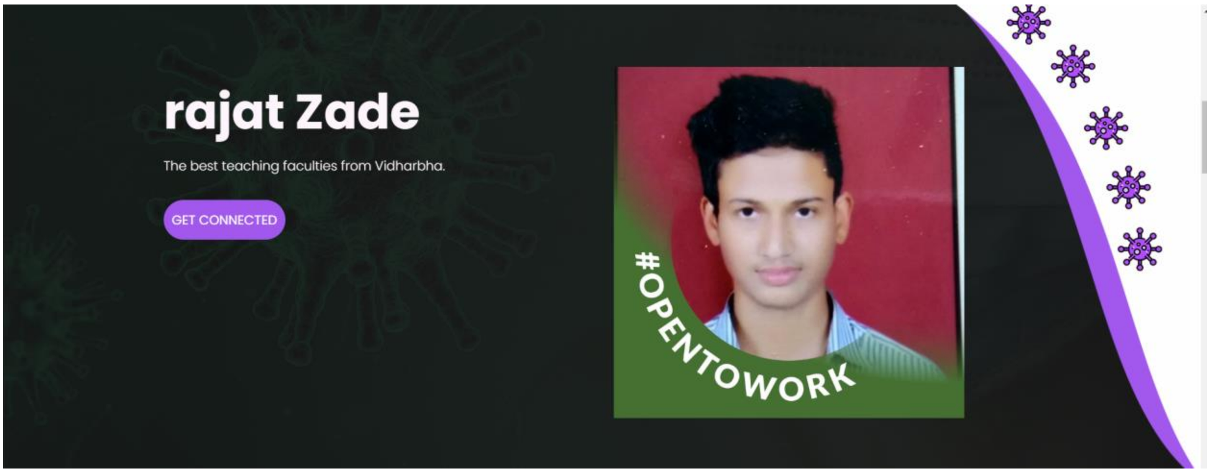
Welcome to Cloudblitz

They provides Linux, AWS, Azure, GCP, DevOps in CDEC Course



Welcome to Pune Branch

Here we provide all facilities, top notch learning experience, with various skill developing activities.



rajat Zade

The best teaching faculties from Vidharbha.