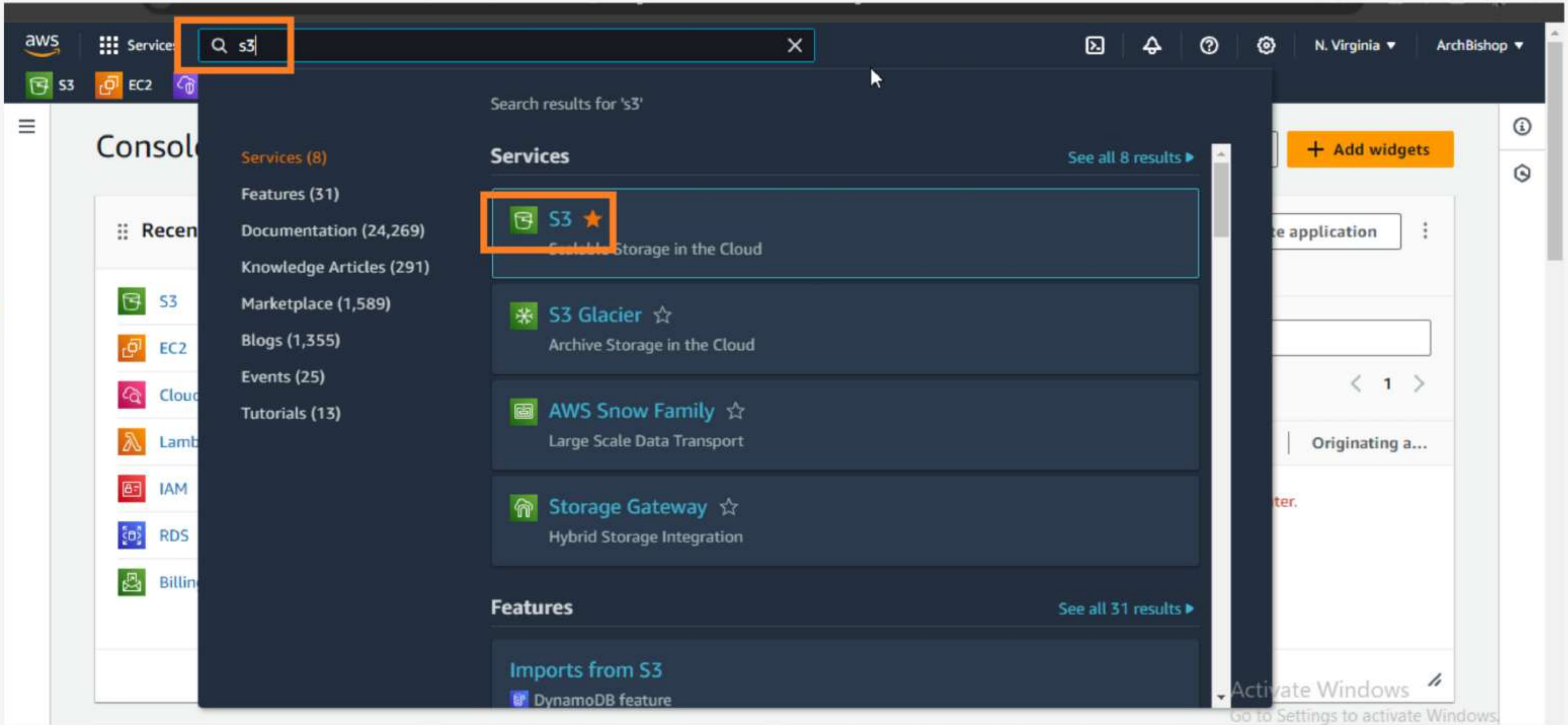
How to Host A Static Website with Amazon S3

Serving this Content through Cloudfront to Reduce Latency and Cost

By : Ayomide Ogunsanya @TheCloudLord

Log on to your AWS Console and on the Search Bar, Type in S3 and Click on the first Option.

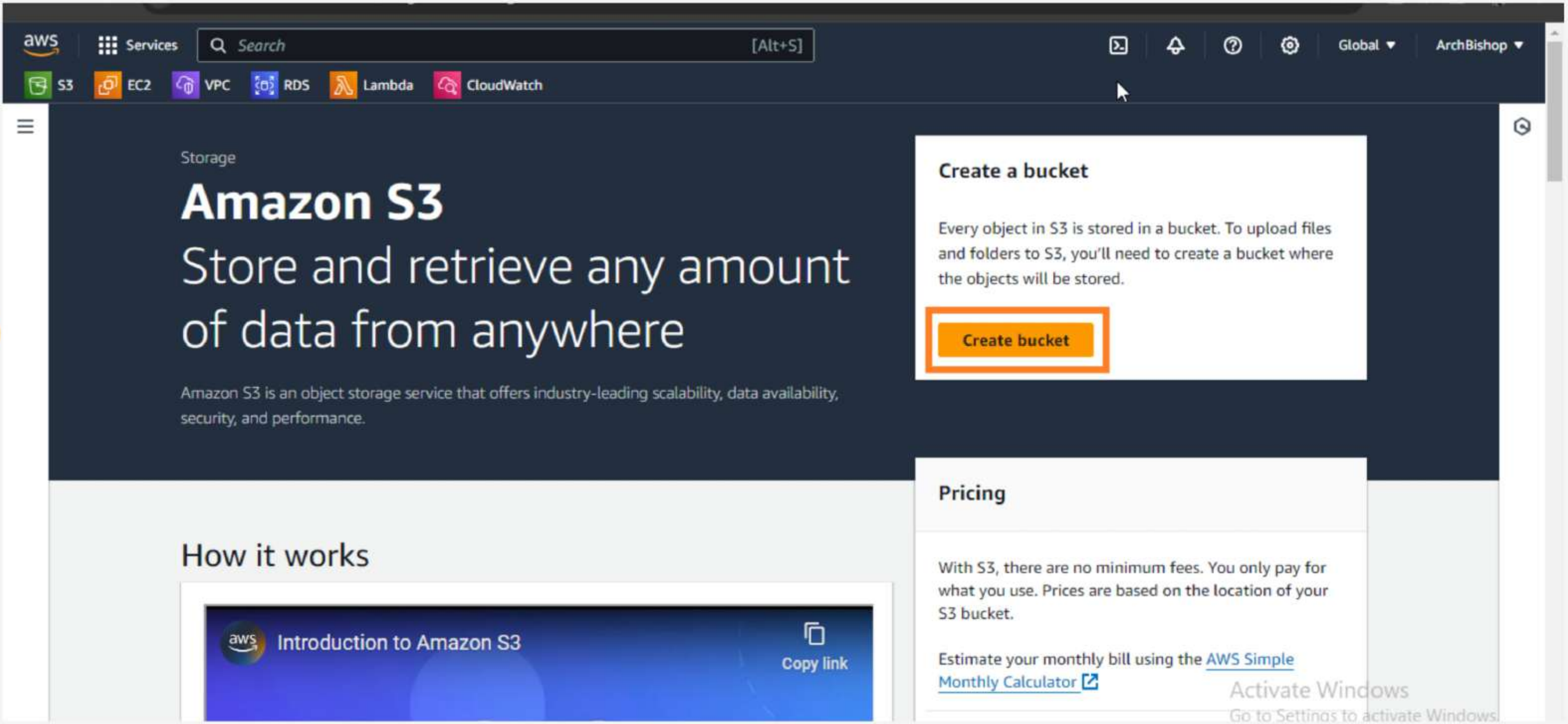
1.



BY AYOMIDE OGUNSANYA (THECLOUDLORD

Click on the "Create Bucket" Button.

2.



Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

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

How it works

Introduction to Amazon S3

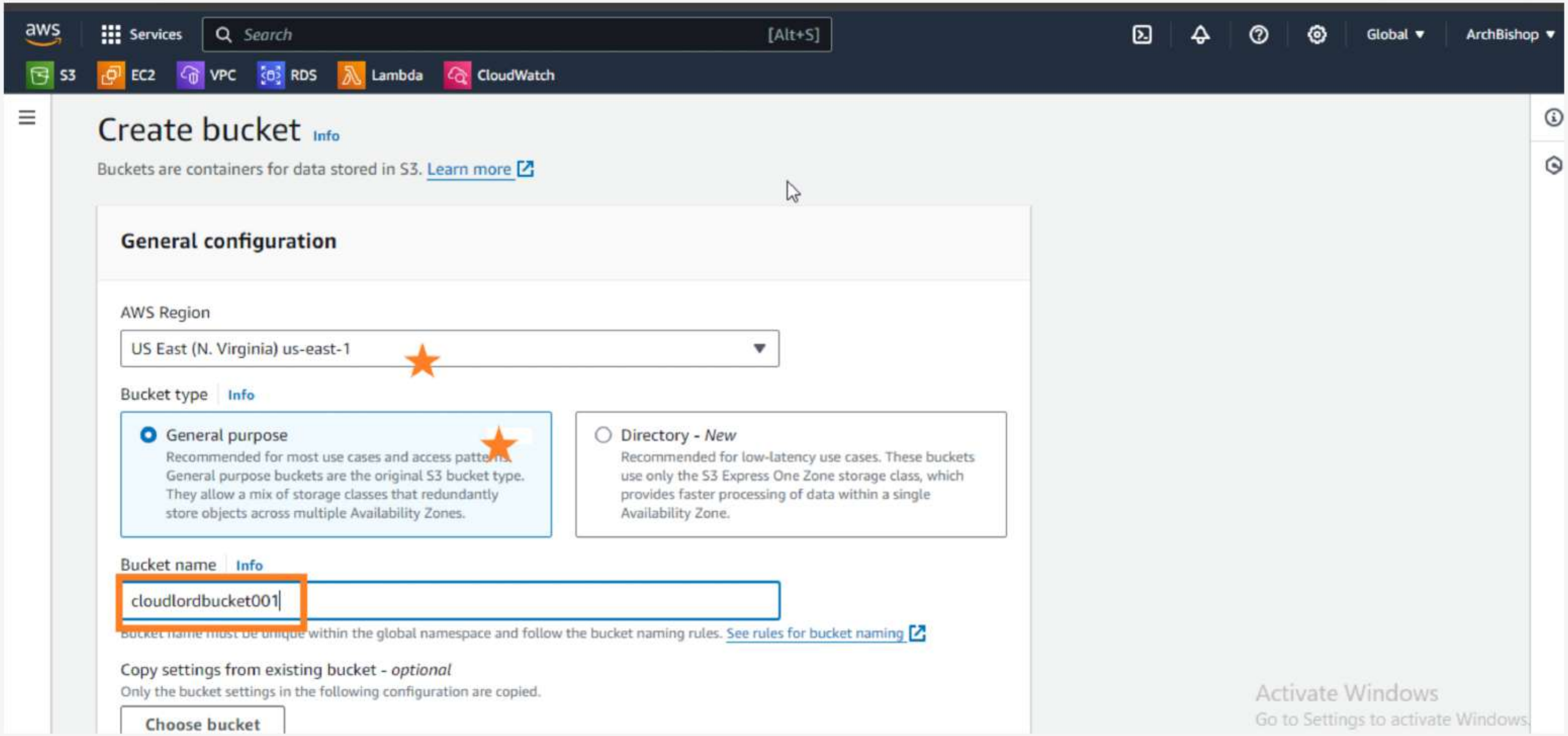
Copy link

Activate Windows
Go to Settings to activate Windows.

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Now, Create a Unique Bucket Name.

3.



Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

AWS Region

US East (N. Virginia) us-east-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 - *New*
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

cloudlordbucket001

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

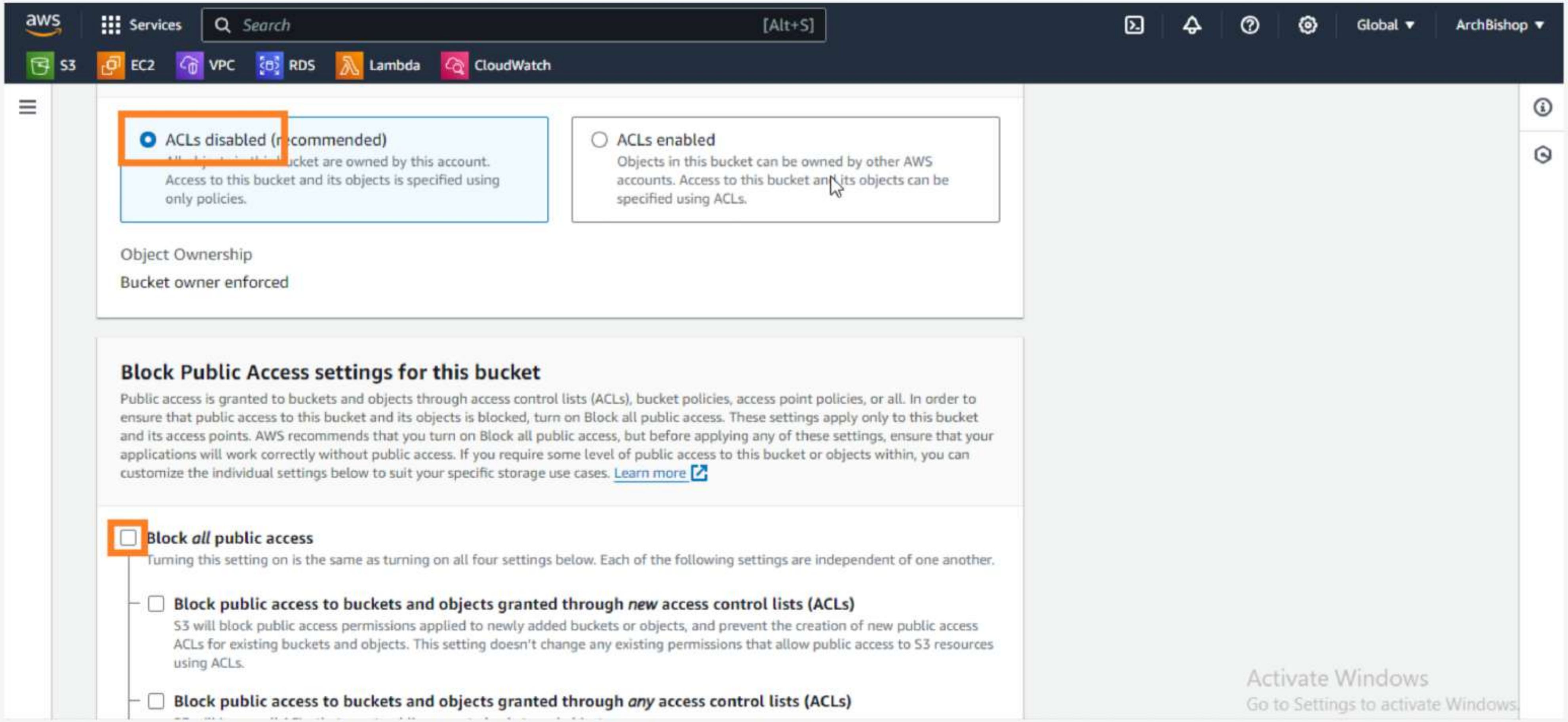
Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

Choose bucket

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Leave ACLs disabled and Uncheck "Block all Public access" to enable Public access.

4.



● 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 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

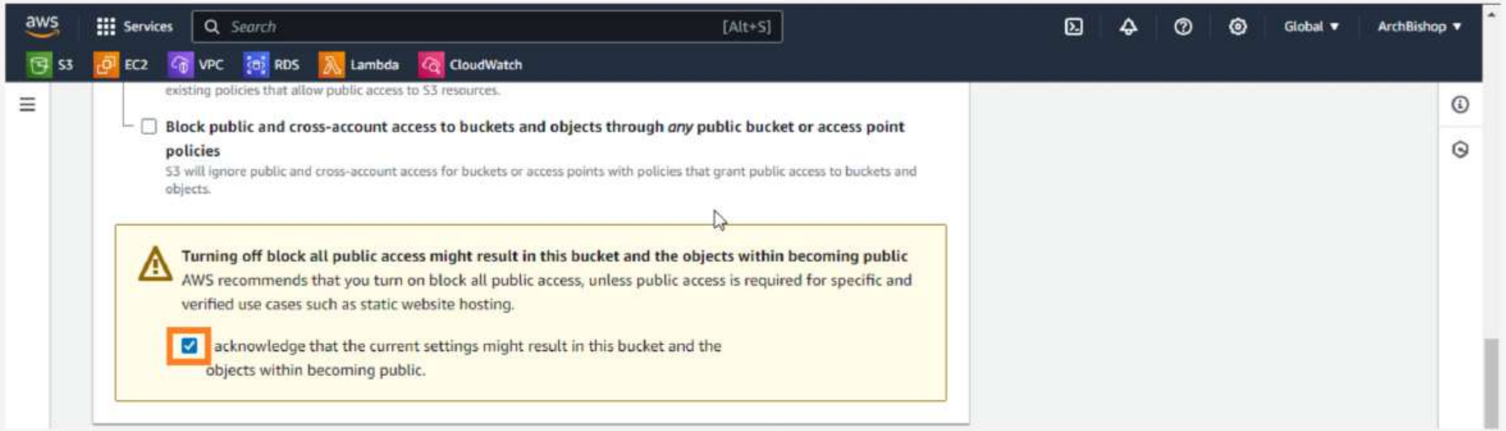
□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **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)**

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Click on the "Acknowledge" CheckBox, Leave all other settings the way it is, scroll down and click on "Create Bucket" Button

5.

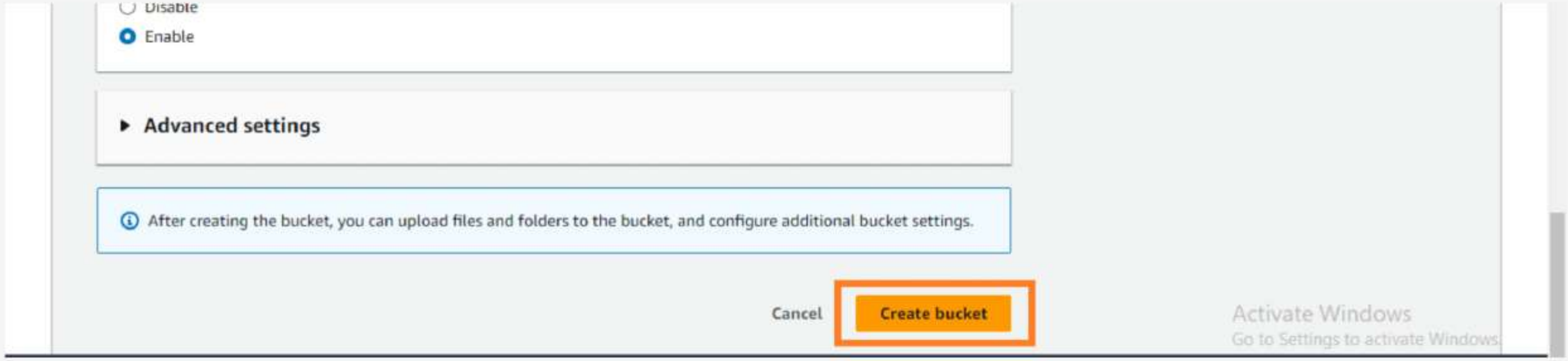


existing policies that allow public access to S3 resources.

□ **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.

☑ acknowledge that the current settings might result in this bucket and the objects within becoming public.



○ Disable
● Enable

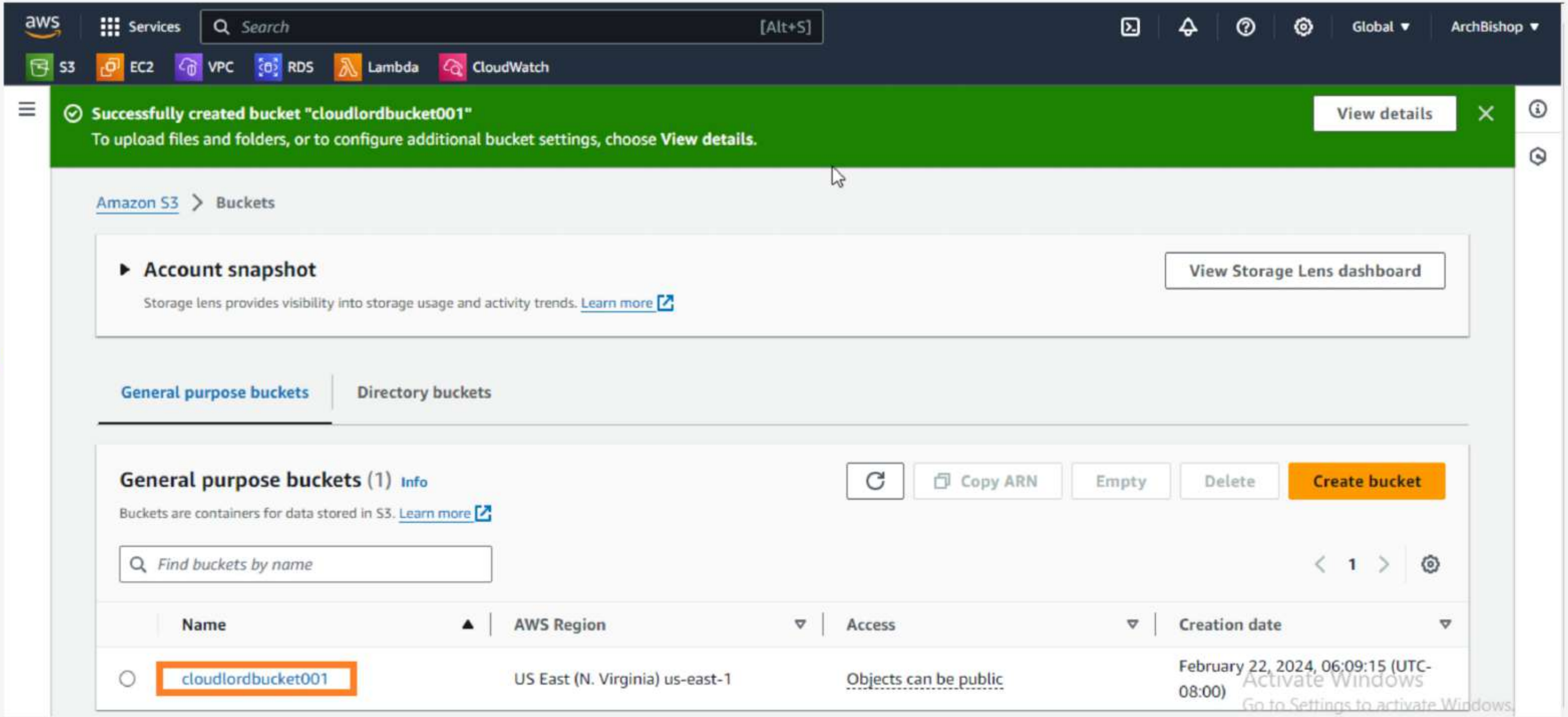
▸ **Advanced settings**

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

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Now, Click on the Bucket Name.

6.



Successfully created bucket "cloudlordbucket001"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

▸ **Account snapshot**

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

General purpose buckets (1)

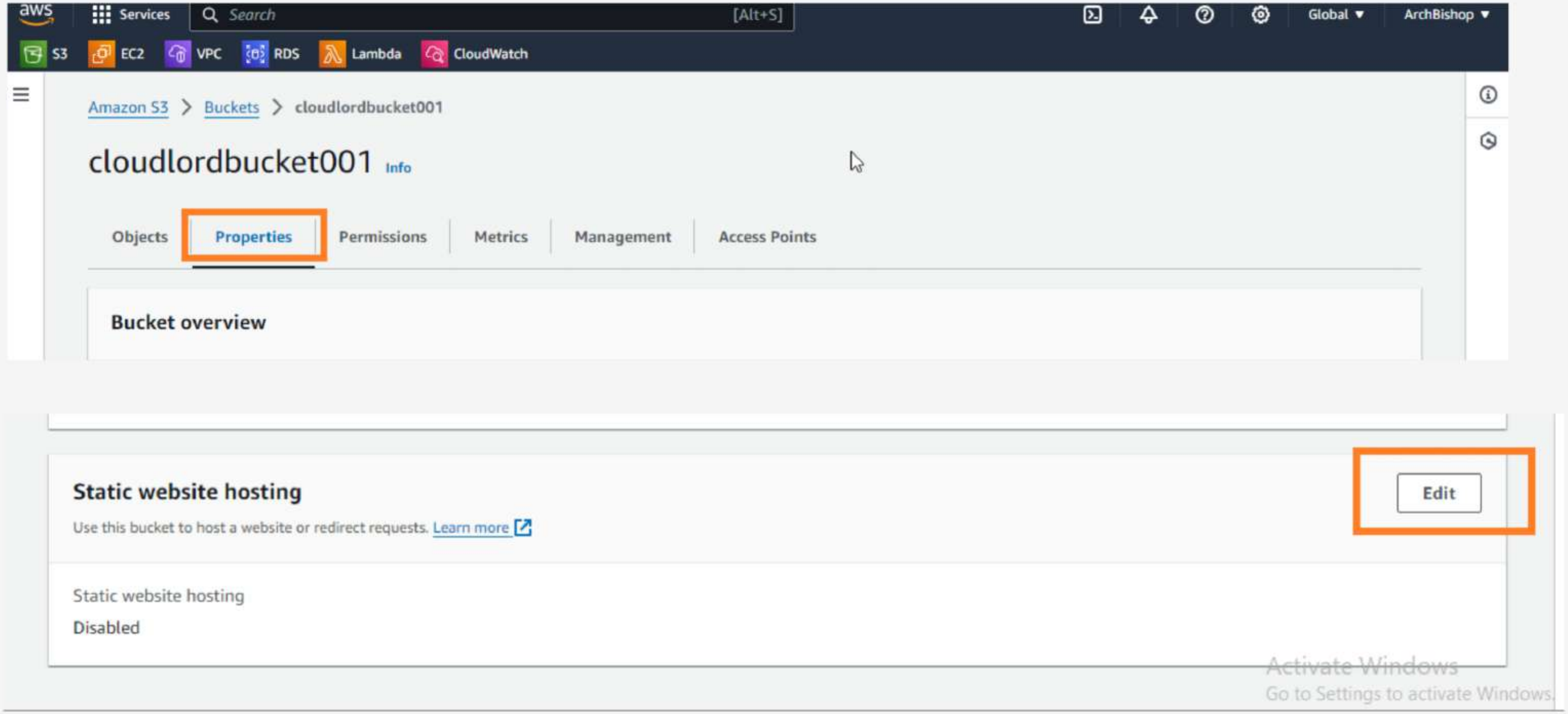
Buckets are containers for data stored in S3. Learn more

	Name ▲	AWS Region	Access	Creation date
○	cloudlordbucket001	US East (N. Virginia) us-east-1	Objects can be public	February 22, 2024, 06:09:15 (UTC-08:00)

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Now, Click on the "Properties" Option, Scroll Down and Click on the Edit Button for "Static Website Hosting"

7.



Static website hosting

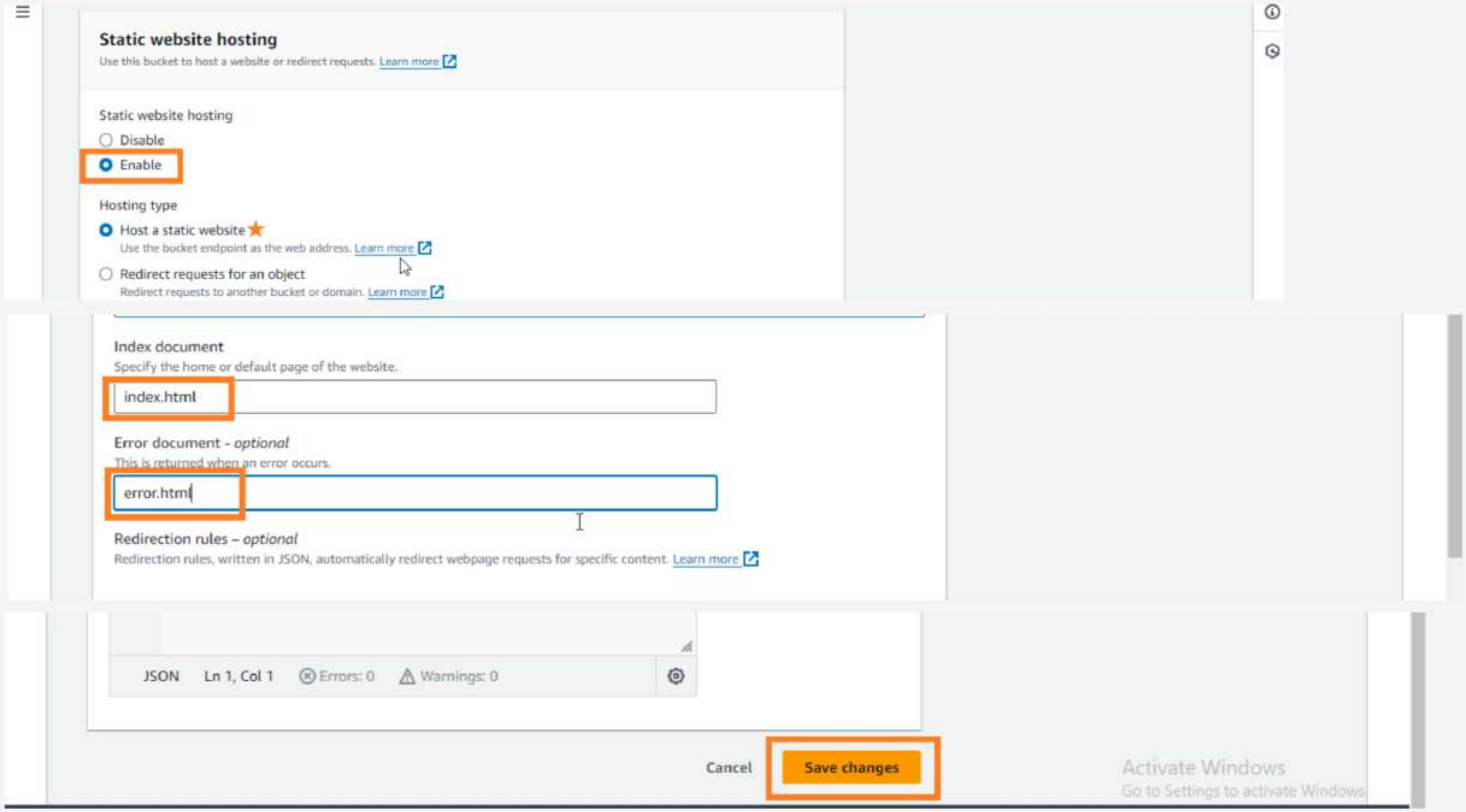
Use this bucket to host a website or redirect requests.

Static website hosting
Disabled

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Click Enable Static Website Hosting and Type in a Name for your index.html eg "Index.html" as used by me and (error.html name which is optional)
Scroll Down and Click on the "Save Changes" Button

8.



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

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

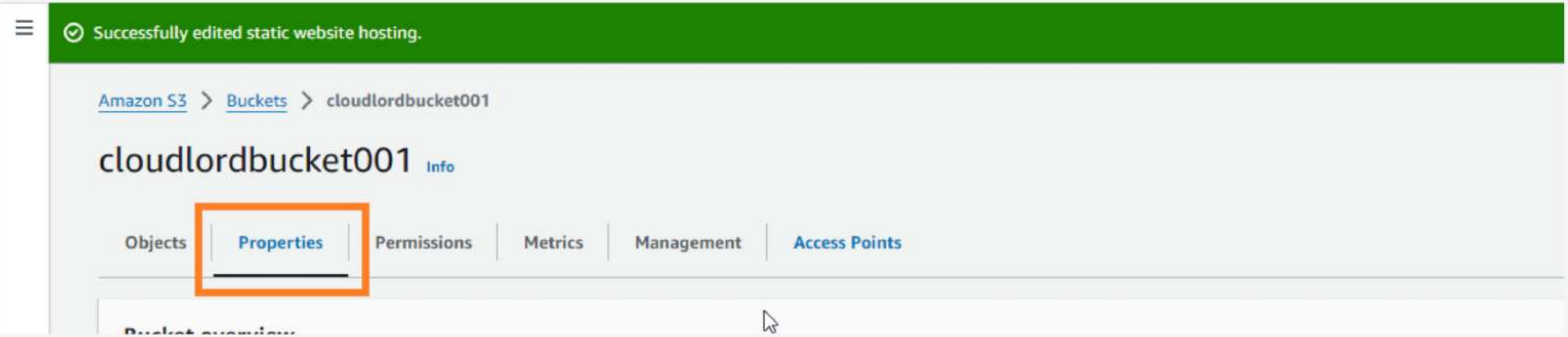
Redirection rules – *optional*

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Still on the "Properties" Tab, Scroll down to "Static Website Hosting" Option and click on the Generated URL

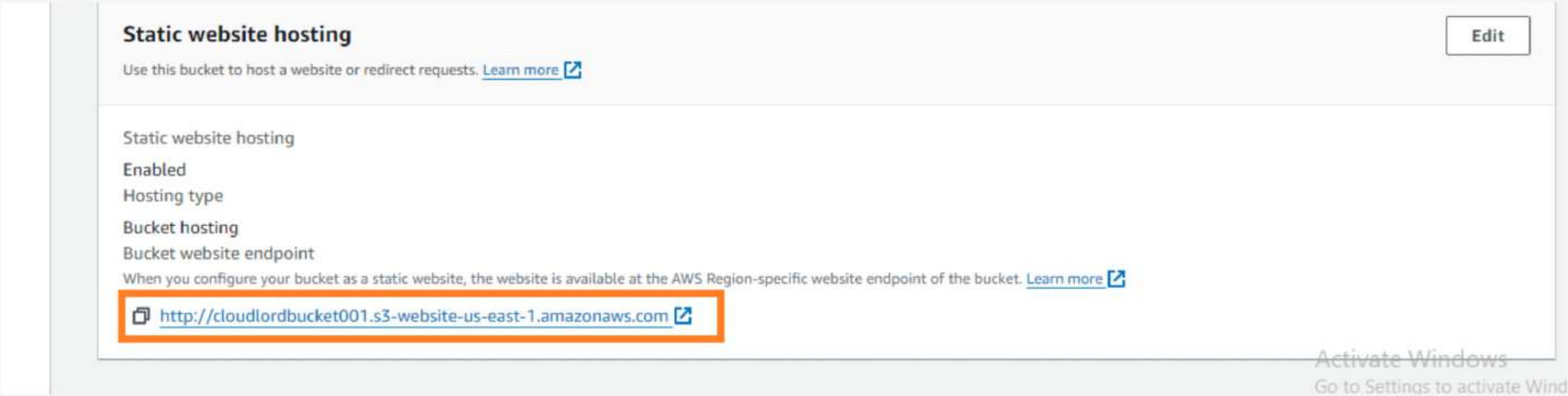
9.



Successfully edited static website hosting.

Amazon S3 > Buckets > cloudlordbucket001

cloudlordbucket001 Info



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

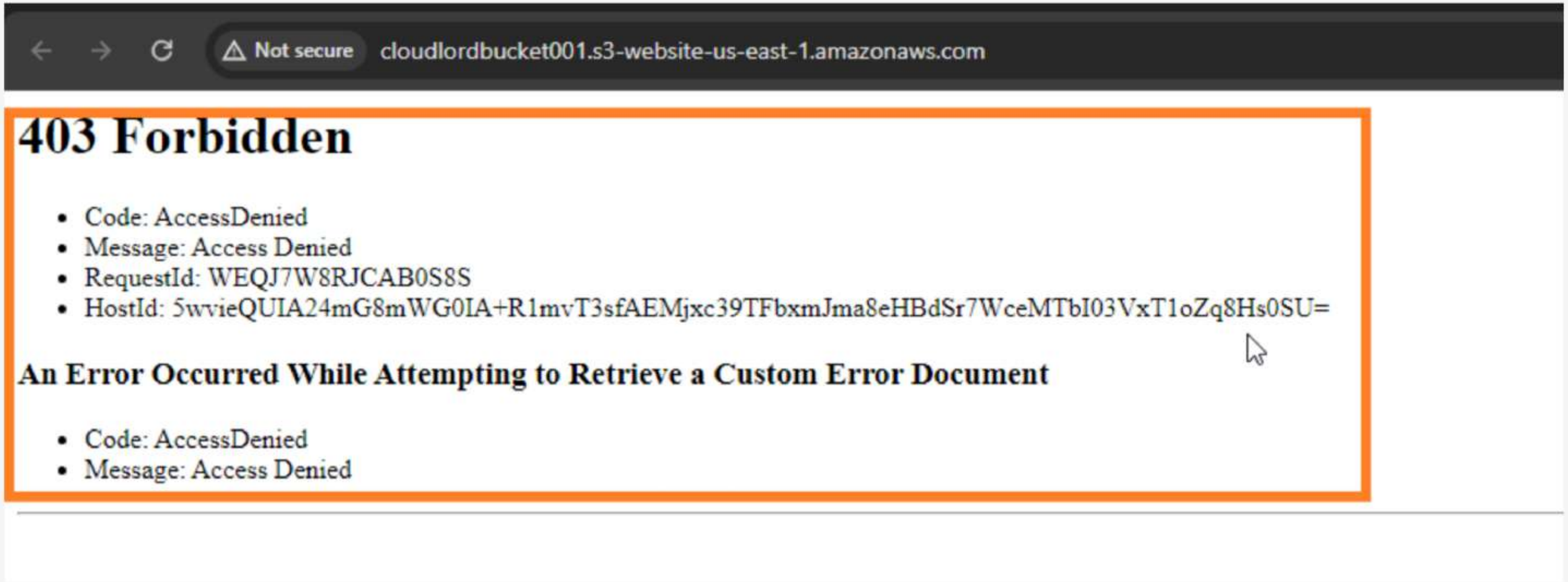
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more

http://cloudlordbucket001.s3-website-us-east-1.amazonaws.com

BY AYOMIDE OGUNSANYA (THECLOUDLORD

It shows a "403 forbidden Access Denied" message and that's because we haven't configured the Bucket Policy to Allow Public Access (Think of the Bucket Policy like Doors with Specific keys)

10.



403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: WEQJ7W8RJCAB0S8S
- HostId: 5wvieQUIA24mG8mWG0IA+R1mvT3sfAEMjxc39TFbxmJma8eHBdSr7WceMTbI03VxT1oZq8Hs0SU=

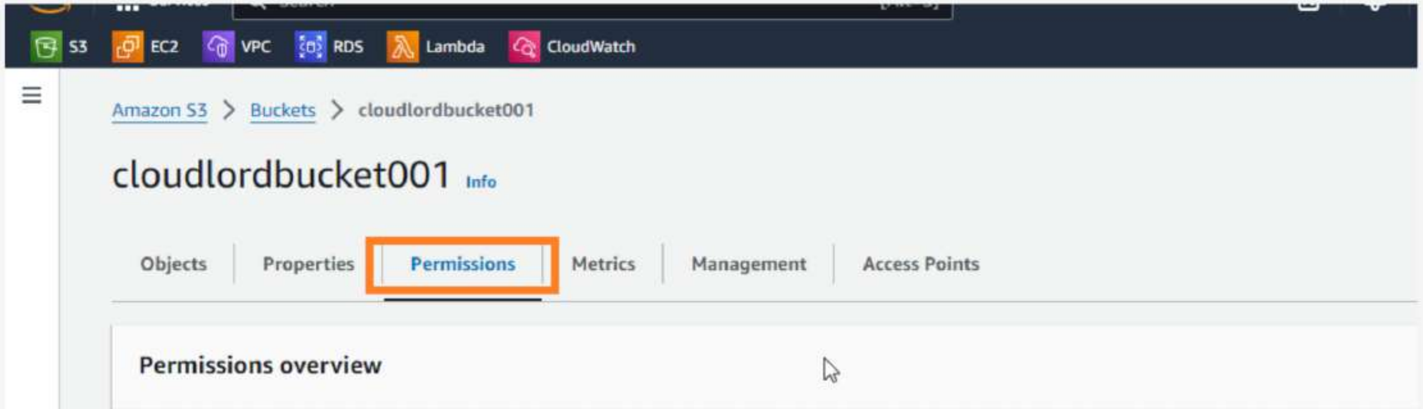
An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied

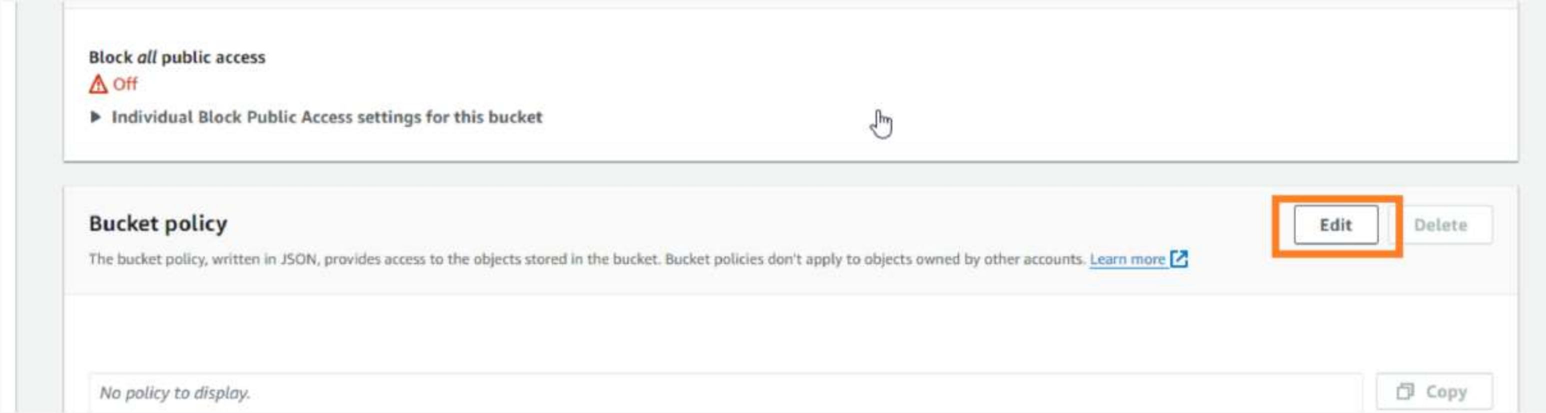
BY AYOMIDE OGUNSANYA (THECLOUDLORD

Now, Return to your AWS Console.
To Configure Our Bucket Policy to allow Public Access, Go to the "Permissions" Tab, Scroll down to "Bucket Policy" Option and Clik on the "Edit" button

11.



Permissions overview


Block *all* public access

⚠ Off

▶ Individual Block Public Access settings for this bucket

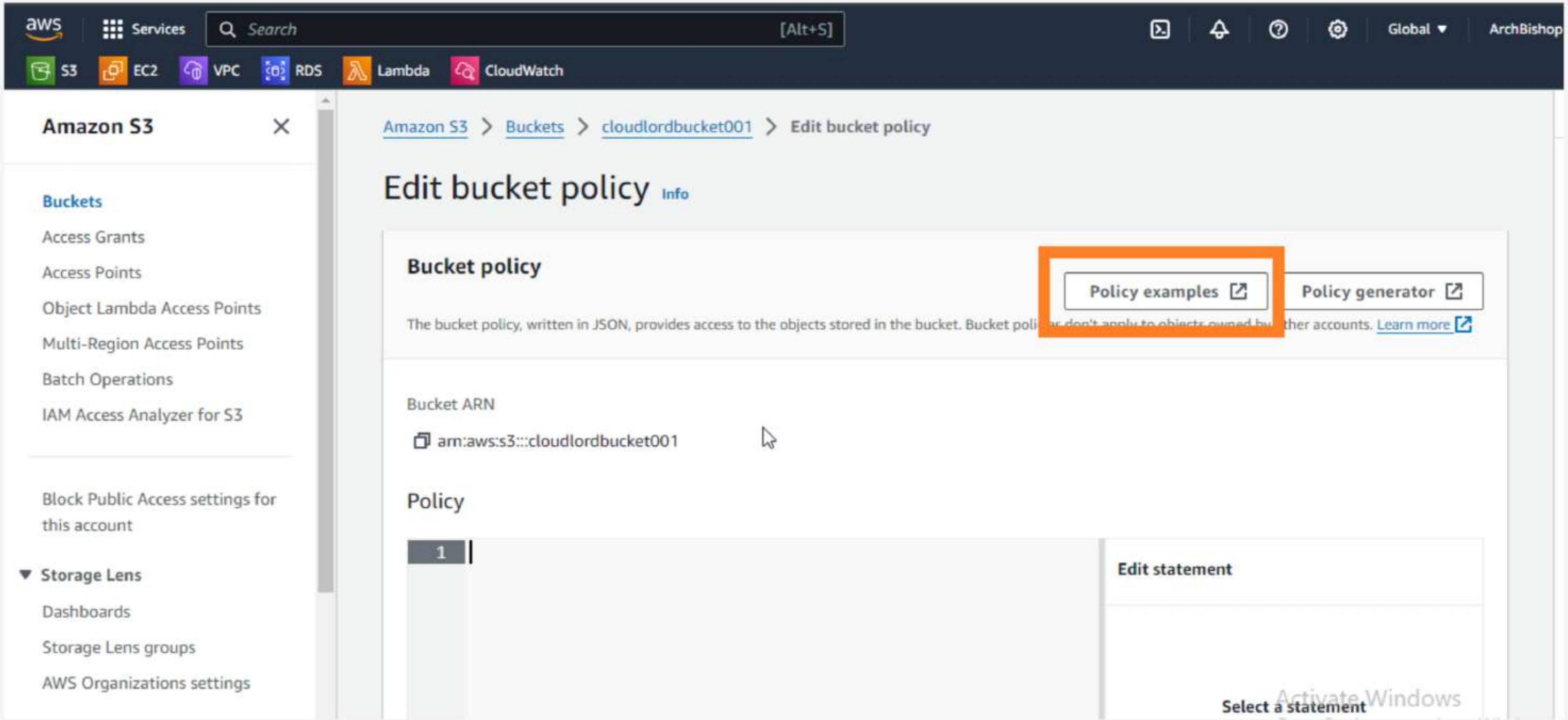
Bucket policy

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.

12.

Click on the "Policy examples" button which takes you to the AWS documentation page.



Amazon S3 > Buckets > cloudlordbucket001 > Edit bucket policy

Edit bucket policy Info

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket poli… …ther accounts. Learn more

Bucket ARN

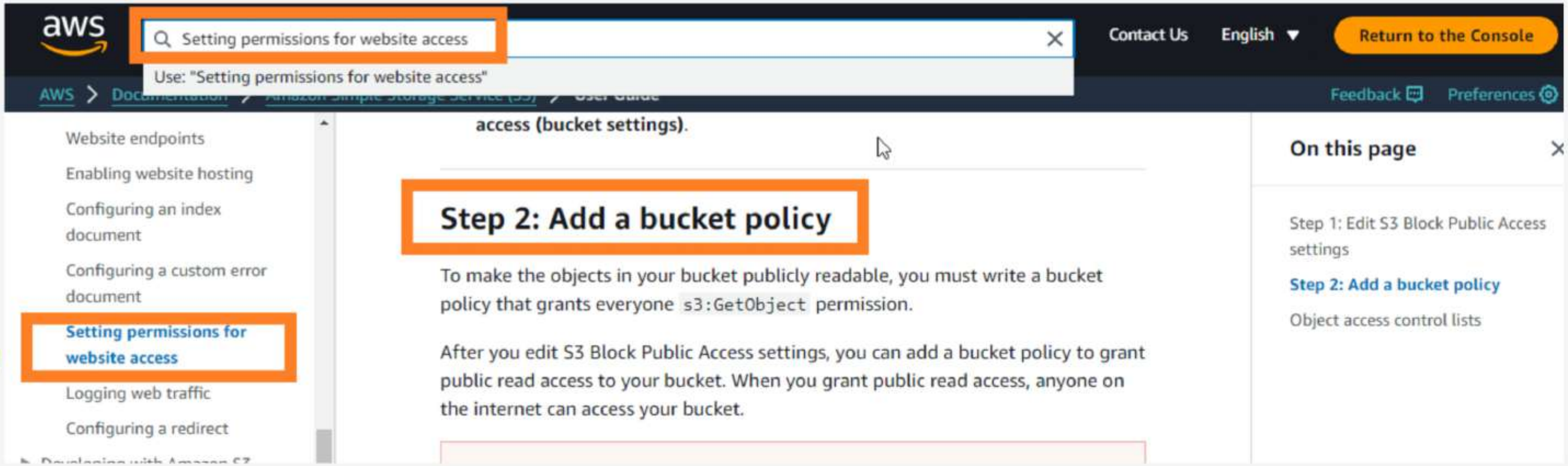
arn:aws:s3:::cloudlordbucket001

Policy

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Search for "Setting Permissions for Website access" Scroll down to Step 2 and copy the Bucket policy

13.

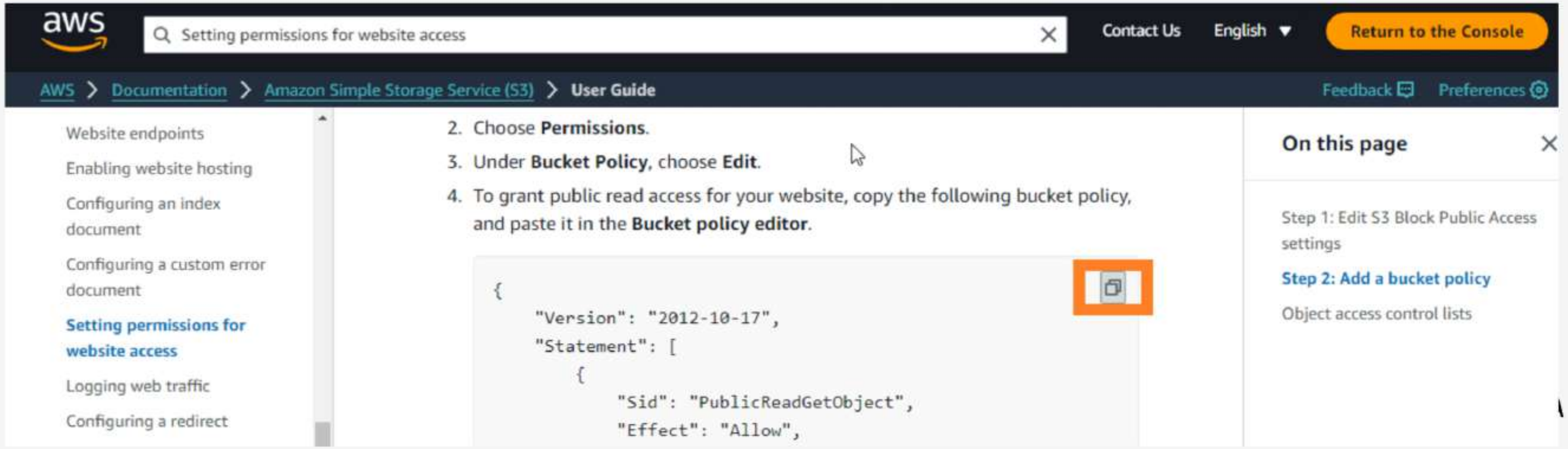

aws
Setting permissions for website access
Use: "Setting permissions for website access"
Contact Us
English
Return to the Console
AWS
Feedback
Preferences
Website endpoints
Enabling website hosting
Configuring an index document
Configuring a custom error document
Setting permissions for website access
Logging web traffic
Configuring a redirect
On this page
Step 1: Edit S3 Block Public Access settings
Step 2: Add a bucket policy
Object access control lists

access (bucket settings).

Step 2: Add a bucket policy

To make the objects in your bucket publicly readable, you must write a bucket policy that grants everyone `s3:GetObject` permission.

After you edit S3 Block Public Access settings, you can add a bucket policy to grant public read access to your bucket. When you grant public read access, anyone on the internet can access your bucket.


aws
Setting permissions for website access
Contact Us
English
Return to the Console
AWS > Documentation > Amazon Simple Storage Service (S3) > User Guide
Feedback
Preferences
Website endpoints
Enabling website hosting
Configuring an index document
Configuring a custom error document
Setting permissions for website access
Logging web traffic
Configuring a redirect
On this page
Step 1: Edit S3 Block Public Access settings
Step 2: Add a bucket policy
Object access control lists

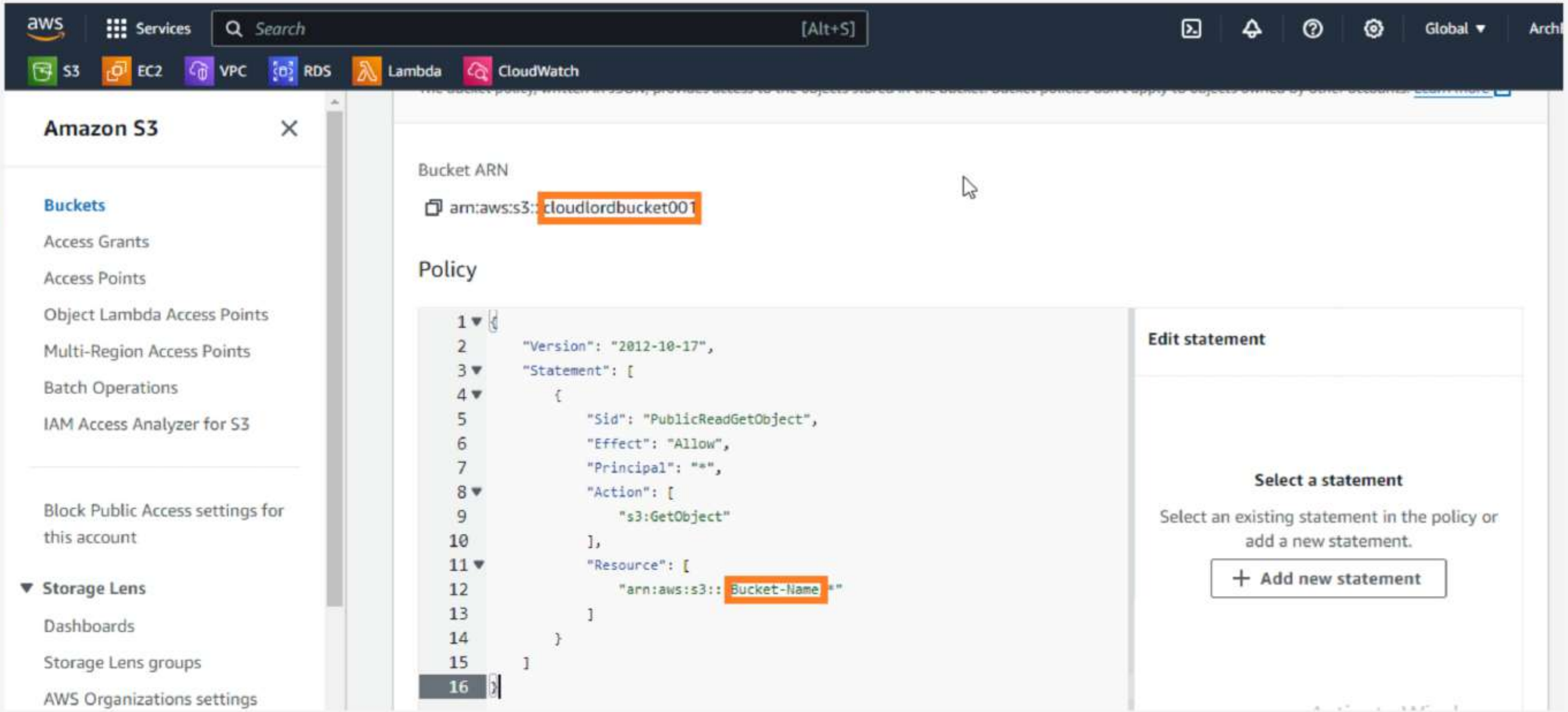
2. Choose **Permissions**.
3. Under **Bucket Policy**, choose **Edit**.
4. To grant public read access for your website, copy the following bucket policy, and paste it in the **Bucket policy editor**.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
```

(THECLOUDLORD

Go back to the AWS Console and Paste the Policy. Now, Replace the word "Bucket-name" on the bucket policy with your Bucket arn name which on my case is "Cloudlordbucket001" , this can be done by copy and paste.

14.


aws
Services
Search
[Alt+S]
Global
Archi
S3
EC2
VPC
RDS
Lambda
CloudWatch
Amazon S3
Buckets
Access Grants
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
Storage Lens groups
AWS Organizations settings
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement

Bucket ARN

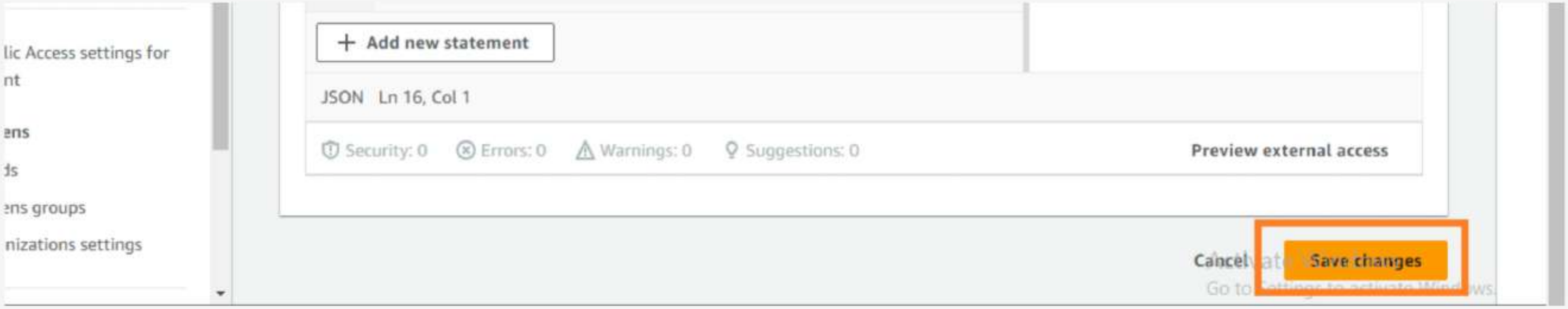
arn:aws:s3:::cloudlordbucket001

Policy

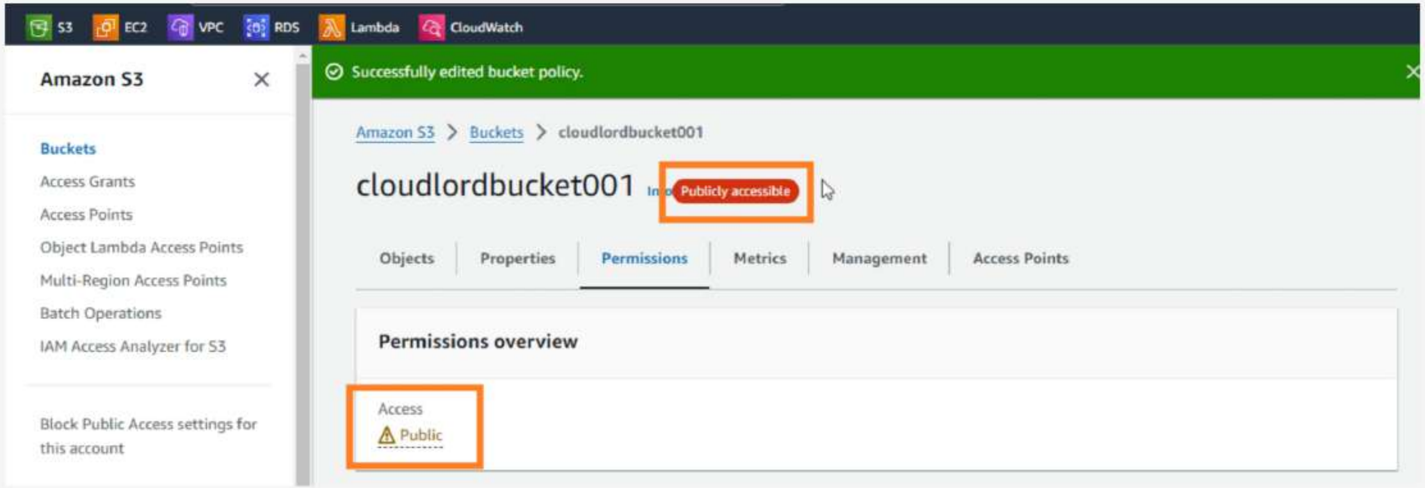
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"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

Click on the "Save changes" button
Now your S3 Bucket is Accessible Publicly!

15.



JSON Ln 16, Col 1



S3
EC2
VPC
RDS
Lambda
CloudWatch
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Amazon S3 > Buckets > cloudlordbucket001
Info
Objects
Properties
Permissions
Metrics
Management
Access Points

Successfully edited bucket policy.

cloudlordbucket001 Publicly accessible

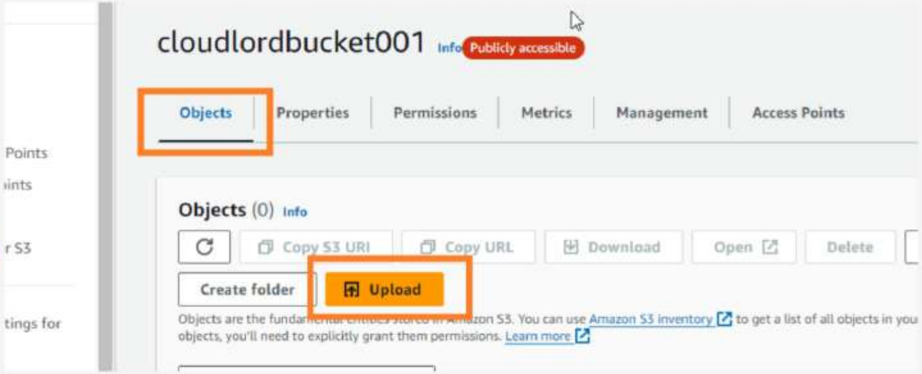
Permissions overview

Access
⚠ Public

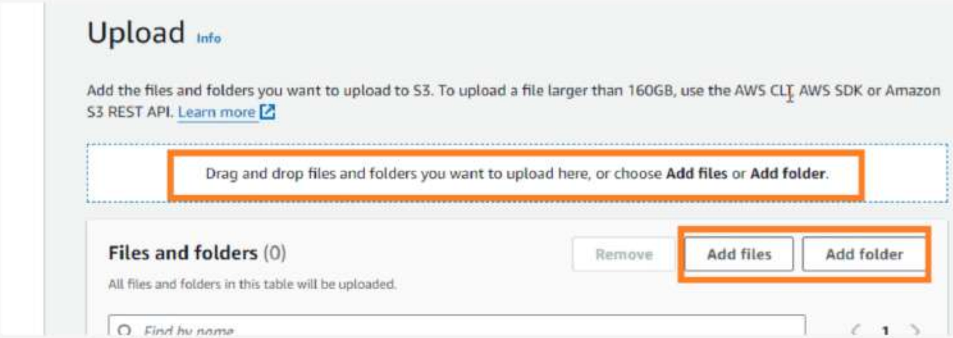
BY AYOMIDE OGUNSANYA (THECLOUDLORD

16.

Now, Click on the "Object" tab Click on the "Upload" button to drag and drop or add files manually. On my case, I'm uploading an html file. Scroll down and click on the "Upload" button when done.



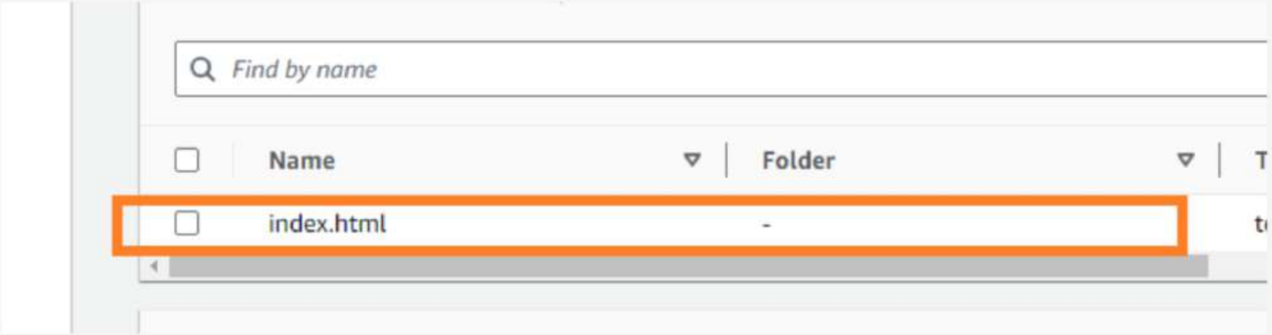
Objects are the fundar… …azon S3. You can use Amazon S3 inventory to get a list of all objects in you… objects, you'll need to explicitly grant them permissions. Learn more



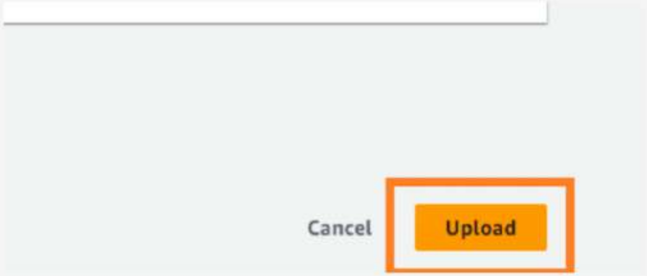
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

All files and folders in this table will be uploaded.



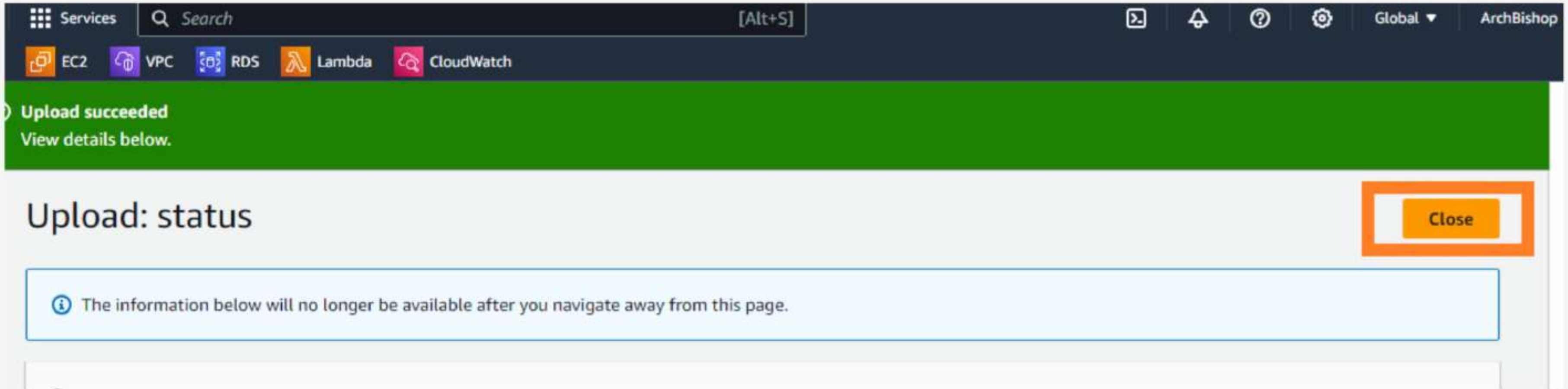
	Name	Folder
□	index.html	-



BY AYOMIDE OGUNSANYA (THECLOUDLORD

Click the "Close" button after upload is done.
To comfirm public accessibility, Click on the "Properties" tab and Scroll down to "Static website hosting" option, Click on the URL

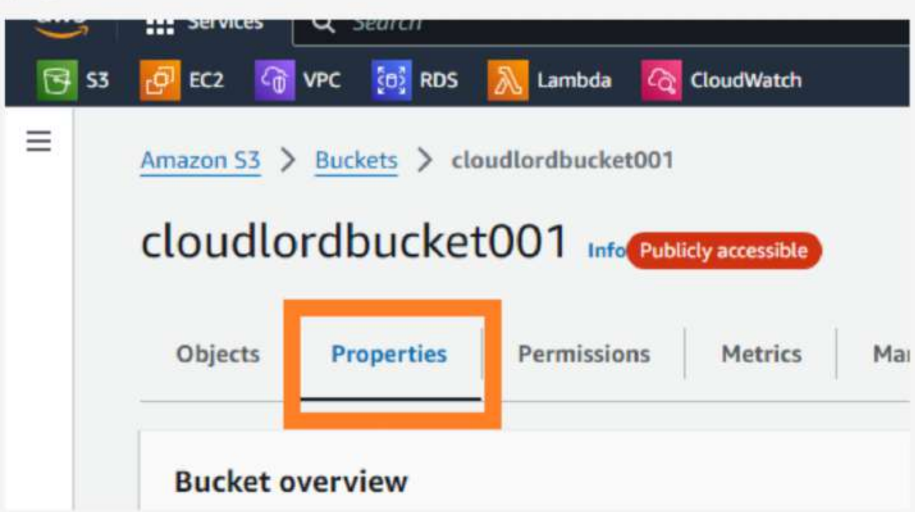
17.



Upload succeeded
View details below.

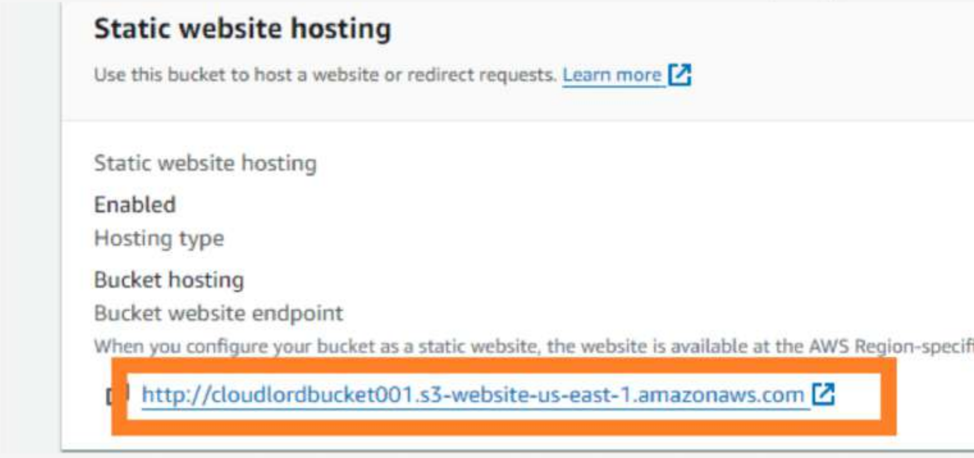
Upload: status

ⓘ The information below will no longer be available after you navigate away from this page.



cloudlordbucket001

Bucket overview



Static website hosting

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

Static website hosting
Enabled

Hosting type
Bucket hosting

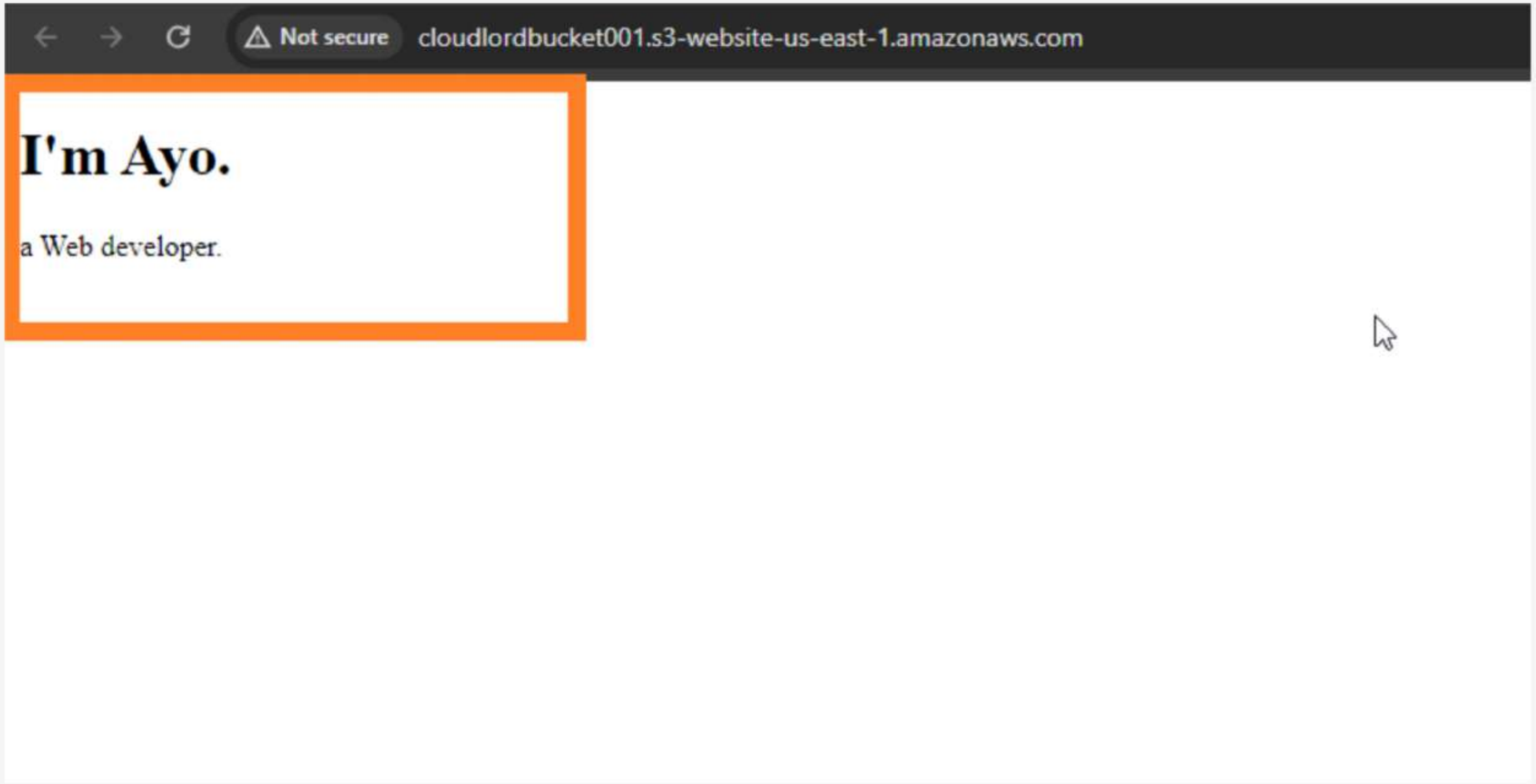
Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specif

http://cloudlordbucket001.s3-website-us-east-1.amazonaws.com

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Now our Static Website is Publicly Accessible. (Congratulations on completing this Milestone so far)
Now, Let's Map this Site to a Cloudfront distribution, this is done to take advantage of the Cache use of Cloudfront, Reduce Latency and Continous Cost to the S3 Bucket

18.



cloudlordbucket001.s3-website-us-east-1.amazonaws.com

I'm Ayo.

a Web developer.

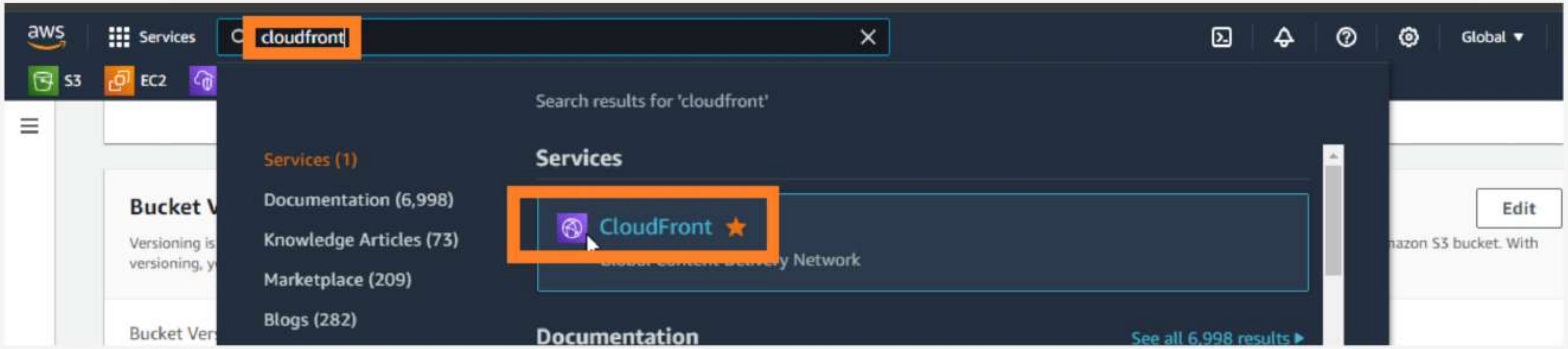
BY AYOMIDE OGUNSANYA (THECLOUDLORD

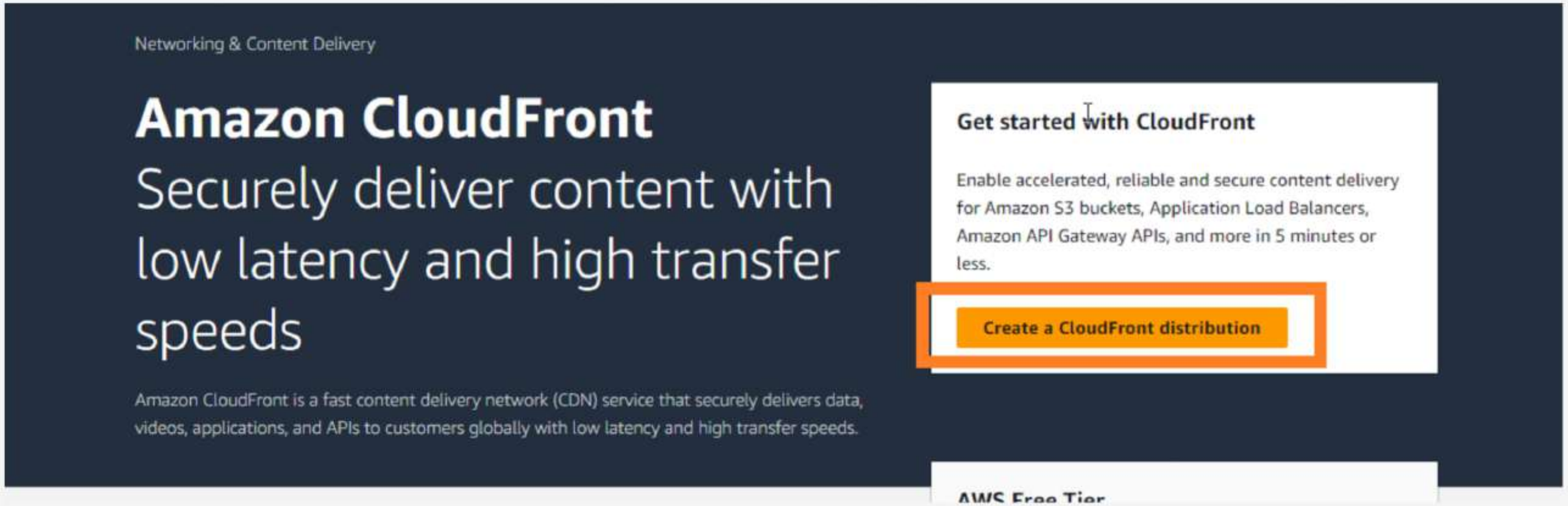
Applying Cloud front

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Go back to your AWS Console and Search for "Cloudfront" and Click. Now, Click on "Create Cloudfront Distribution"

19.




Networking & Content Delivery

Amazon CloudFront

Securely deliver content with low latency and high transfer speeds

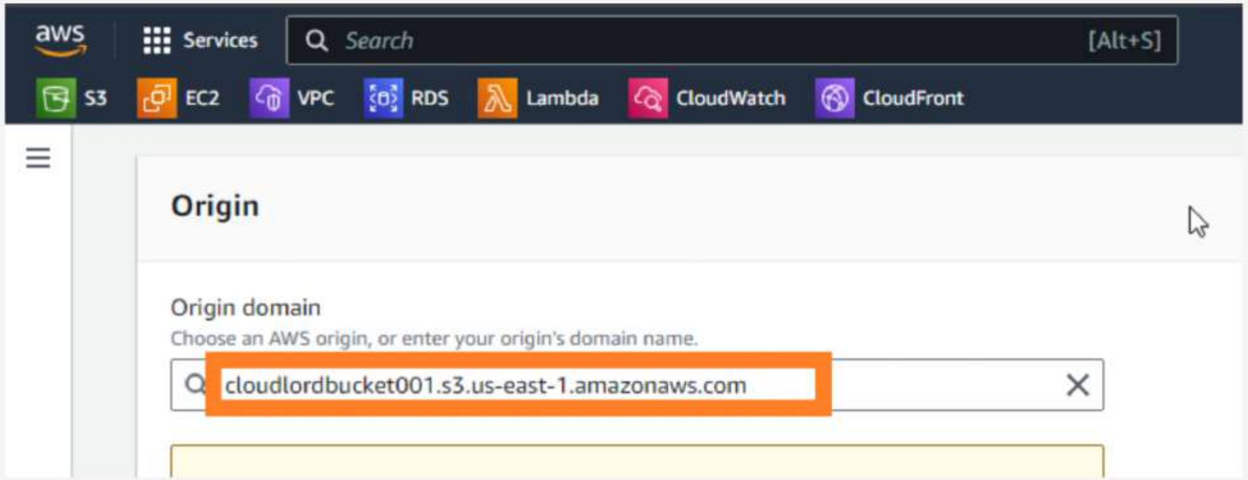
Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

Get started with CloudFront

Enable accelerated, reliable and secure content delivery for Amazon S3 buckets, Application Load Balancers, Amazon API Gateway APIs, and more in 5 minutes or less.

Click on the "Origin Domain", select the your domain listed.
Scroll down to "Origin Access", Click on "Origin access control settings (recommended)"
then click on the "Create new OAC" button

20.

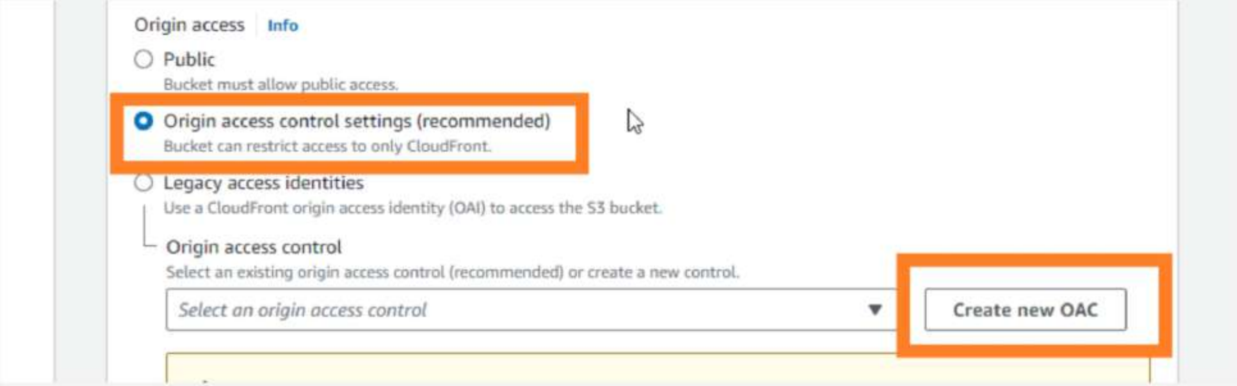


Origin

Origin domain

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

cloudlordbucket001.s3.us-east-1.amazonaws.com



Origin access Info

○ Public
Bucket must allow public access.

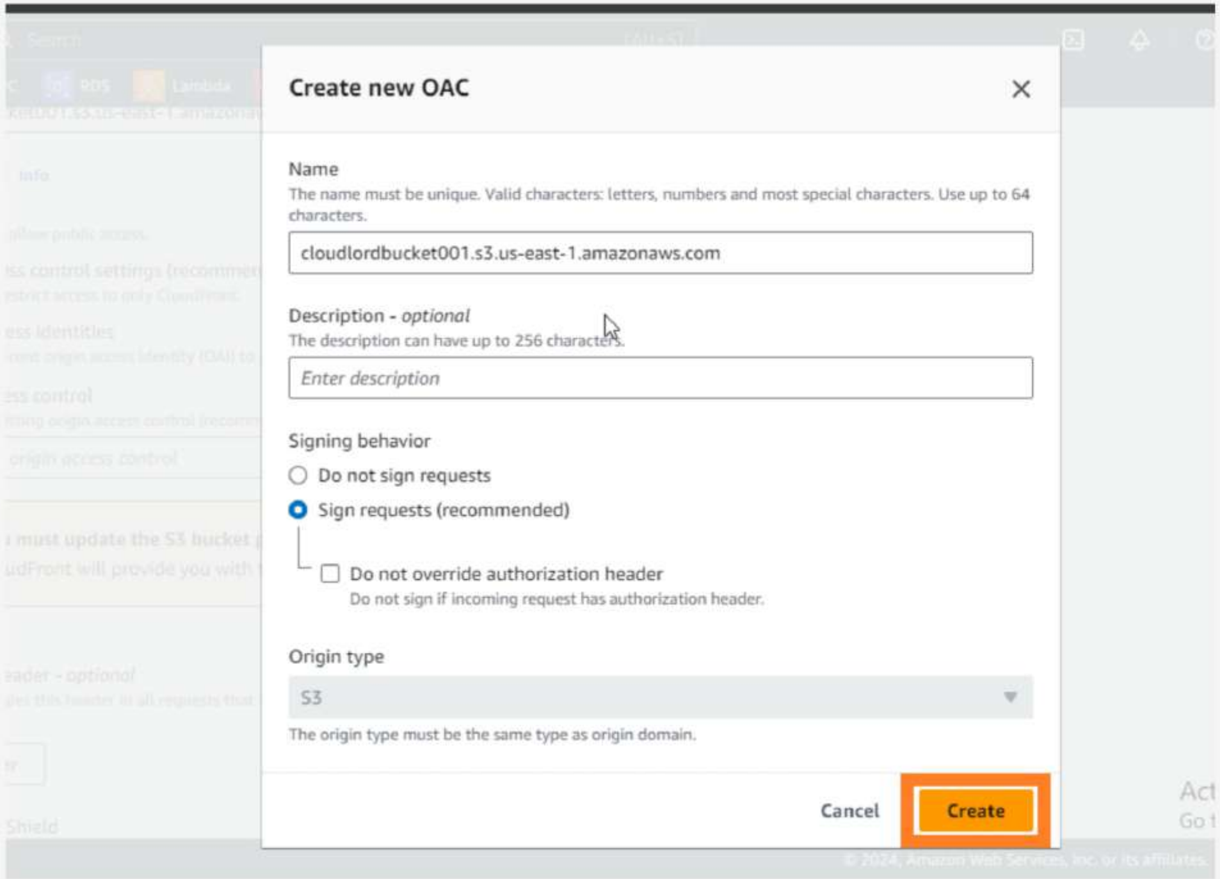
● Origin access control settings (recommended)
Bucket can restrict access to only CloudFront.

○ Legacy access identities
Use a CloudFront origin access identity (OAI) to access the S3 bucket.

Origin access control
Select an existing origin access control (recommended) or create a new control.

Leave the OAC settings as it is and Click "Create"

21.



Create new OAC

Name

The name must be unique. Valid characters: letters, numbers and most special characters. Use up to 64 characters.

cloudlordbucket001.s3.us-east-1.amazonaws.com

Description - *optional*

The description can have up to 256 characters.

Enter description

Signing behavior

○ Do not sign requests

● Sign requests (recommended)

□ Do not override authorization header

Do not sign if incoming request has authorization header.

Origin type

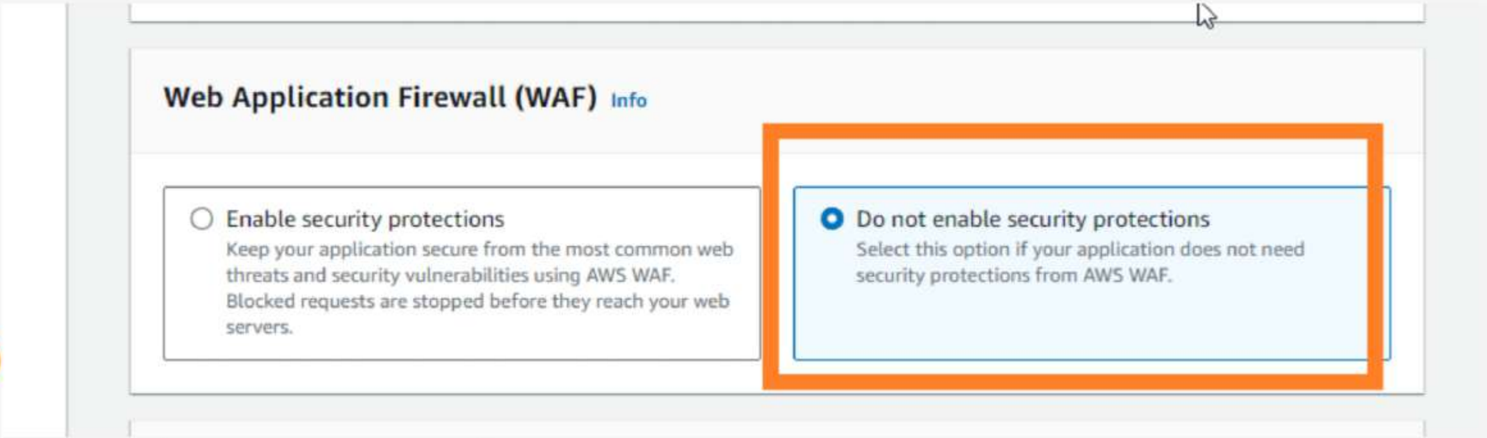
S3

The origin type must be the same type as origin domain.

BY AYOMIDE OGUNSANYA (THECLOUDLORD

22.

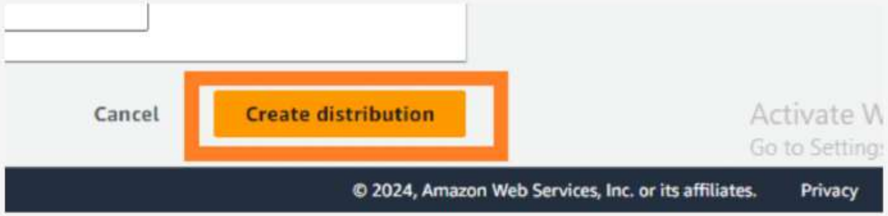
Scroll to Web Application Firewall (WAF) option, click on "do not enable security protection".
Scroll down and Click "Create Distribution"
Copy the New Generated CloudFront policy.

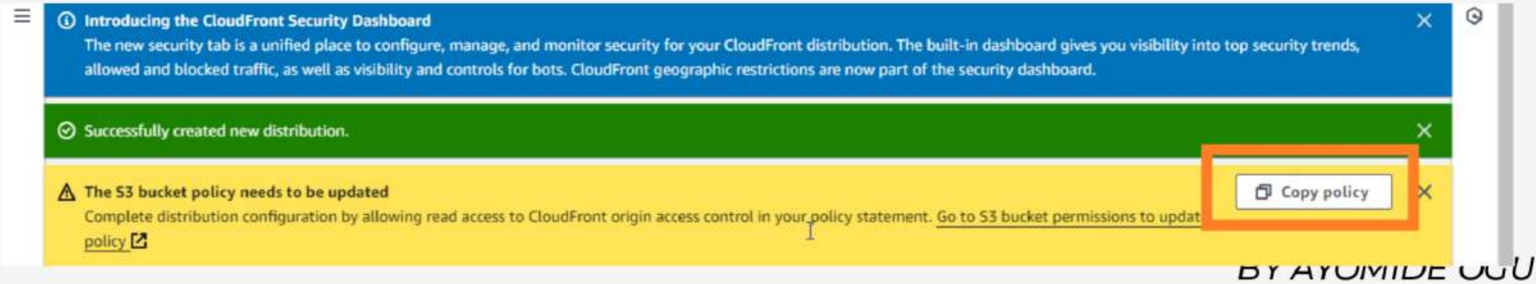


Web Application Firewall (WAF) Info

○ Enable security protections
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

● Do not enable security protections
Select this option if your application does not need security protections from AWS WAF.





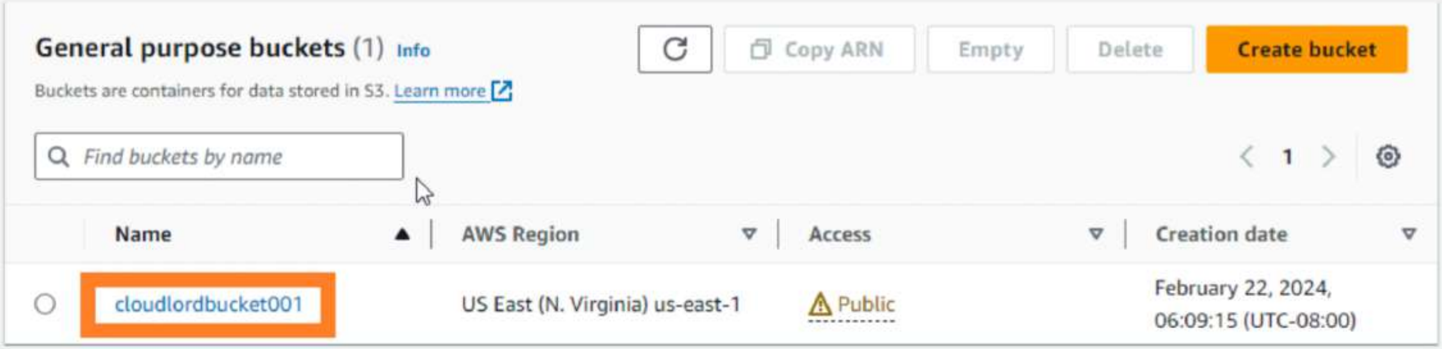
ⓘ Introducing the CloudFront Security Dashboard
The new security tab is a unified place to configure, manage, and monitor security for your CloudFront distribution. The built-in dashboard gives you visibility into top security trends, allowed and blocked traffic, as well as visibility and controls for bots. CloudFront geographic restrictions are now part of the security dashboard.

✓ Successfully created new distribution.

⚠ The S3 bucket policy needs to be updated
Complete distribution configuration by allowing read access to CloudFront origin access control in your policy statement. Go to S3 bucket permissions to updat policy

Now Return to your S3 Bucket
Click on your Bucket name
Click on "Permissions" tab
And Click on "Edit" for Block public access option

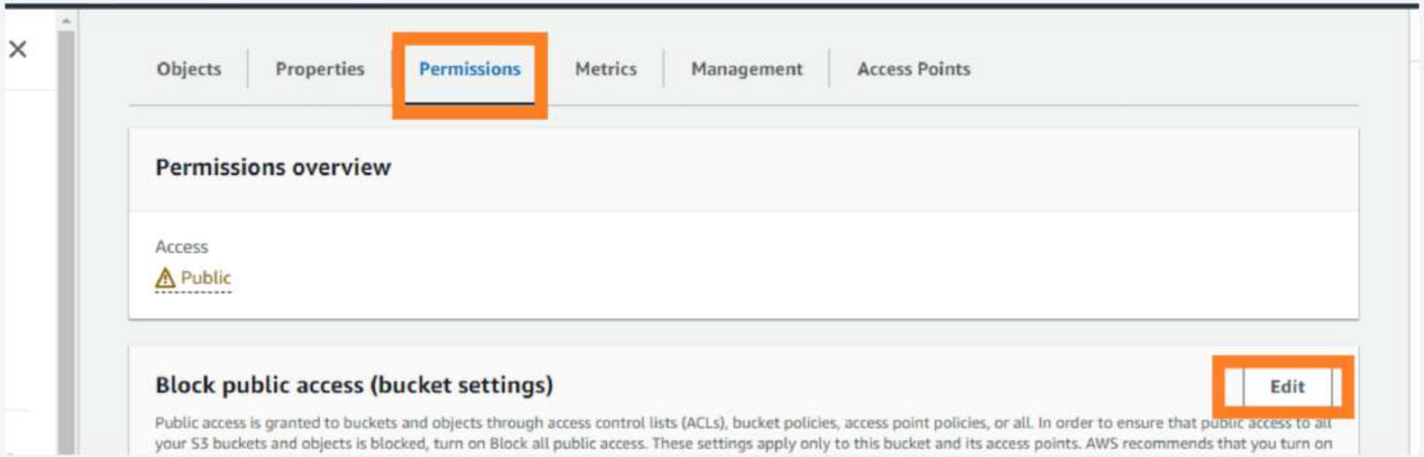
23.



General purpose buckets (1) Info

Buckets are containers for data stored in S3. Learn more

	Name ▲	AWS Region ▽	Access ▽	Creation date ▽
○	cloudlordbucket001	US East (N. Virginia) us-east-1	⚠ Public	February 22, 2024, 06:09:15 (UTC-08:00)



Permissions overview

Access
⚠ Public

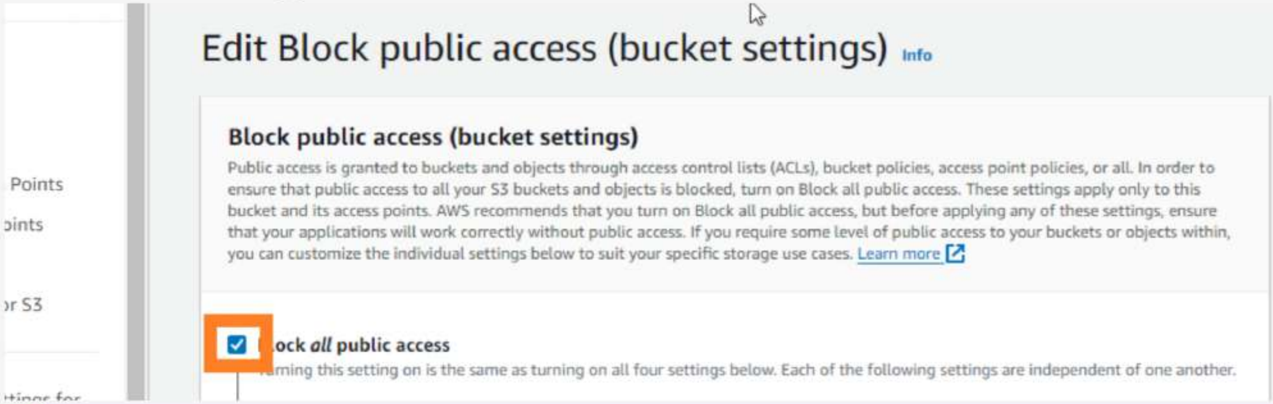
Block public access (bucket settings)

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

BY AYOMIDE OGUNSANYA (THECLOUDLORD

24.

Click on Block Public Access Checkbox and Save changes.
Now, Edit the Bucket policy and Paste the New Bucket Policy Gotten from Cloudfront.
Save changes.



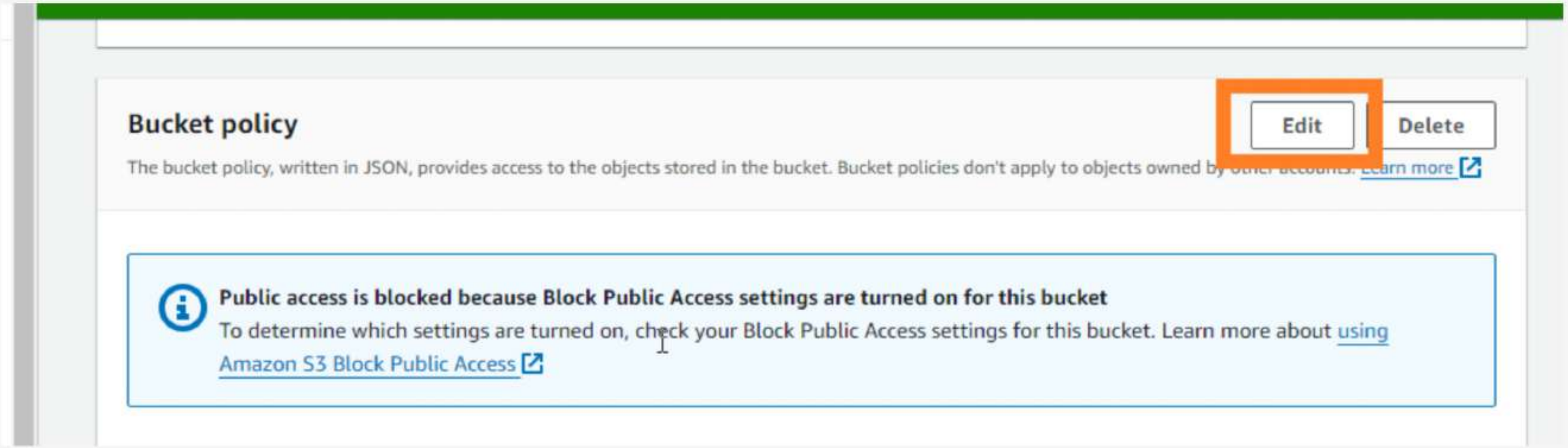
Edit Block public access (bucket settings) Info

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.



Bucket policy

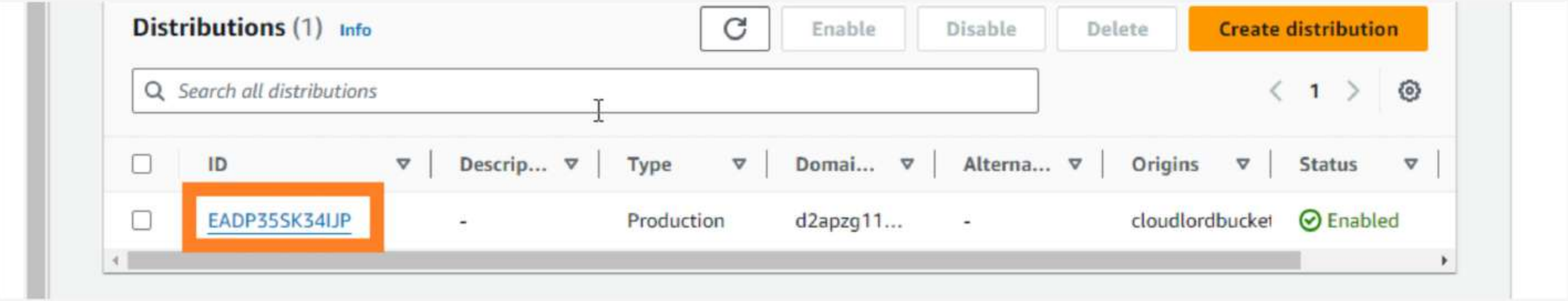
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Public access is blocked because Block Public Access settings are turned on for this bucket

To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

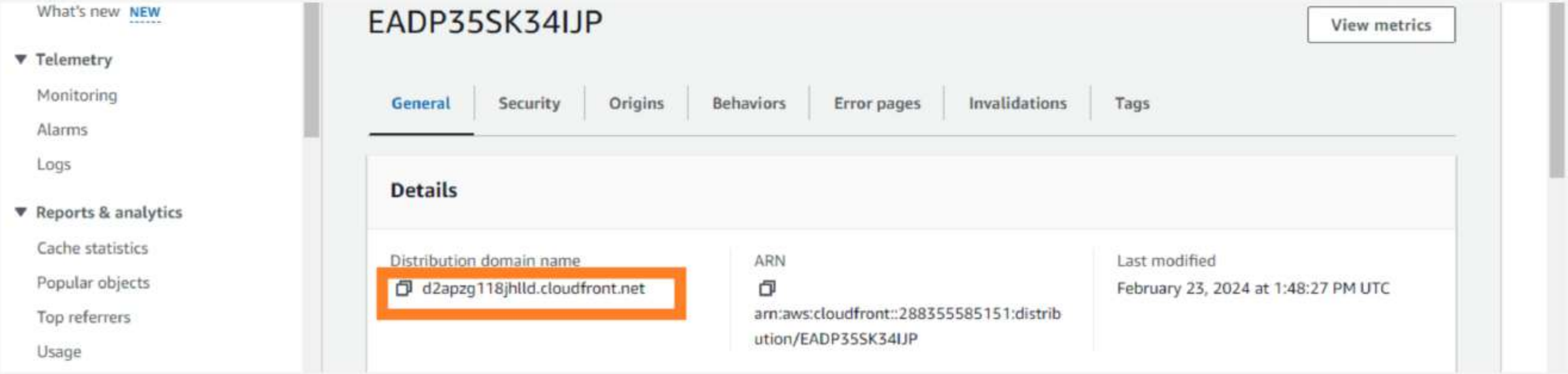
Now, Go to Cloudfront, Click on your Cloudfront "ID". Copy the "Distribution Domain Name" and paste in a new tab on your Browser

25.



Distributions (1) Info

□	ID	Descrip...	Type	Domai...	Alterna...	Origins	Status
□	EADP35SK34IJP	-	Production	d2apzg11...	-	cloudlordbucket	✓ Enabled



EADP35SK34IJP

Details

Distribution domain name
d2apzg118jhlld.cloudfront.net

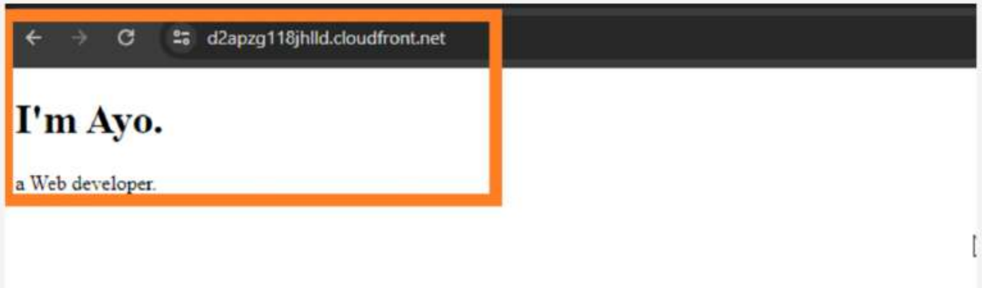
ARN
arn:aws:cloudfront::288355585151:distribution/EADP35SK34IJP

Last modified
February 23, 2024 at 1:48:27 PM UTC

BY AYOMIDE OGUNSANYA (THECLOUDLORD

The Site Opens Successfully. WELDONE!
Now, Let's add a TTL (Time to Live lets you specify how long you want your site loading from Cloudfront before Reloading from s3 bucket) to our Cloudfront Distribution.
Click on Behavior Tab, Click on the check icon, Click on Edit

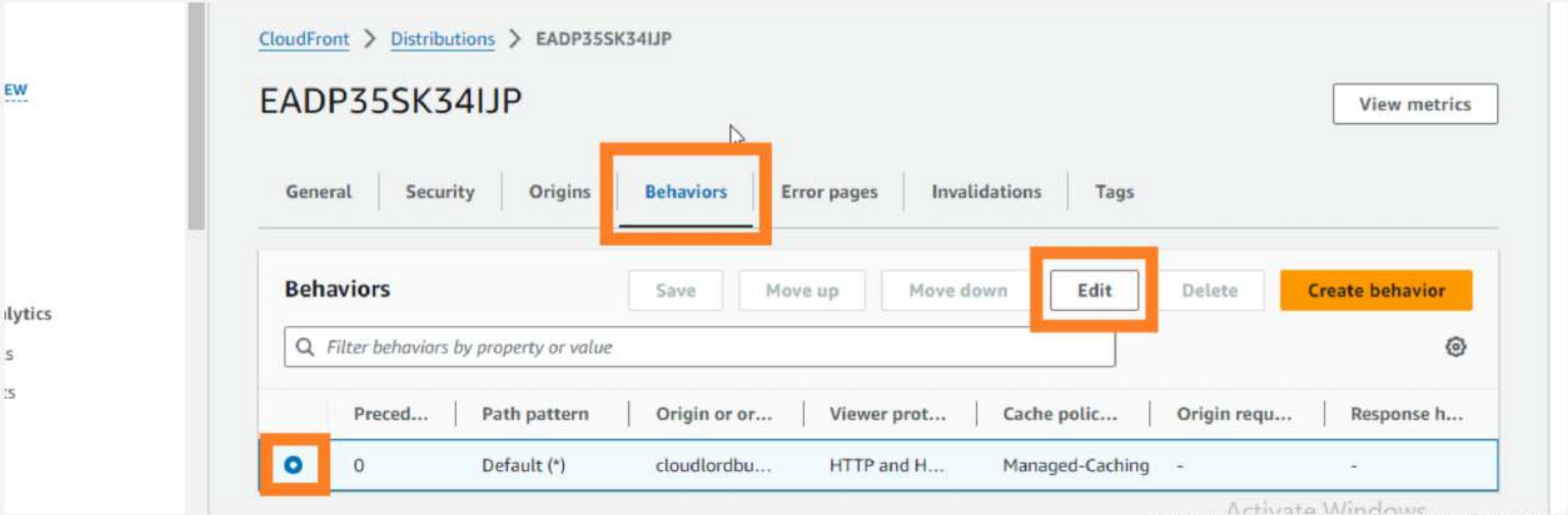
26.



d2apzg118jhlld.cloudfront.net

I'm Ayo.

a Web developer.



CloudFront > Distributions > EADP35SK34IJP

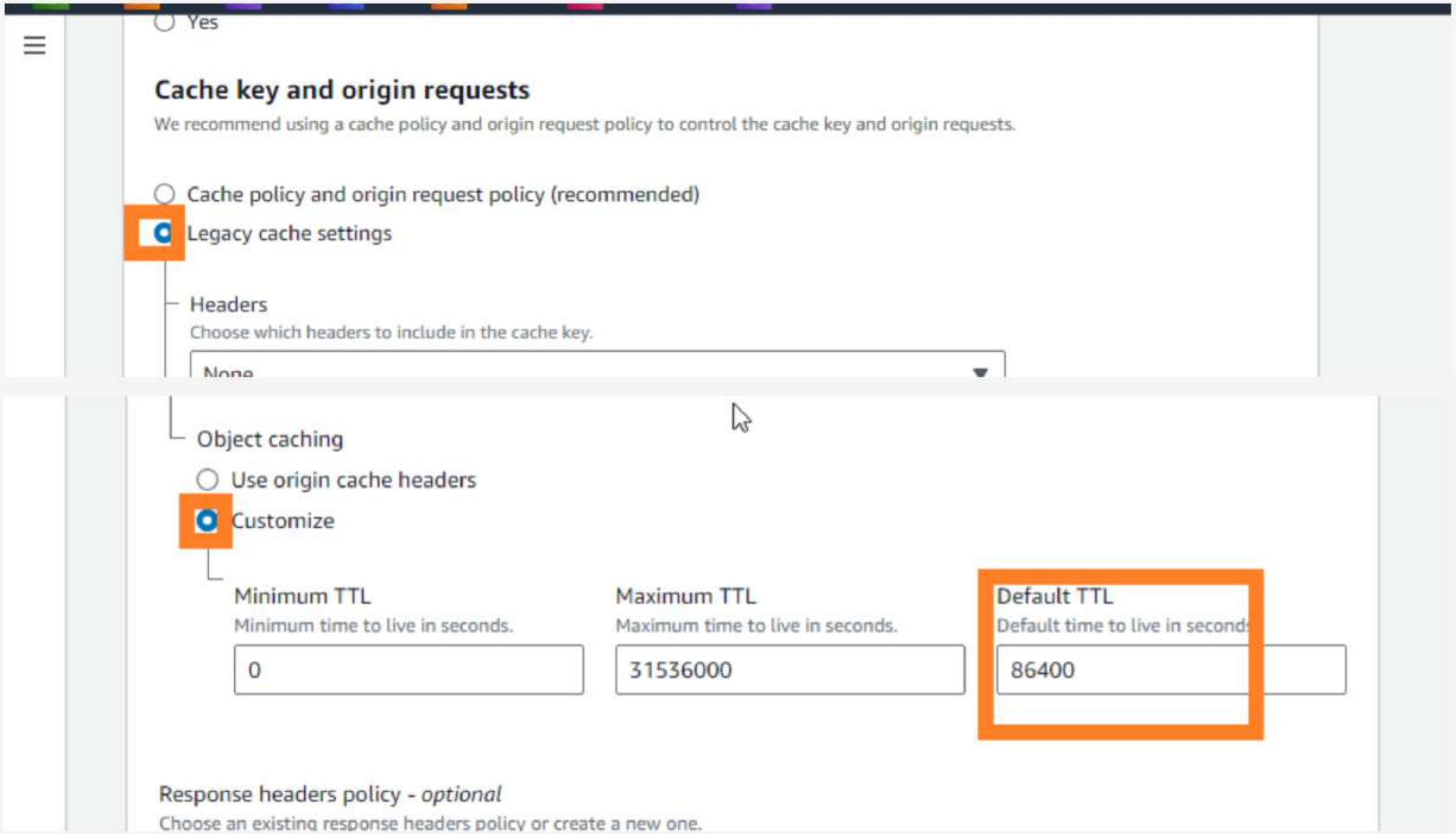
EADP35SK34IJP

	Preced...	Path pattern	Origin or or...	Viewer prot...	Cache polic...	Origin requ...	Response h...
●	0	Default (*)	cloudlordbu...	HTTP and H...	Managed-Caching	-	-

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Scroll to "Cache key and Origin Request", Click "Legacy cache settings" , now under "Object Caching" Click "Customize". Now you can Set the "Default TTL" to the Amount of seconds you want.
Save when done. GoodLuck

27.



○ Yes

Cache key and origin requests

We recommend using a cache policy and origin request policy to control the cache key and origin requests.

○ Cache policy and origin request policy (recommended)
● Legacy cache settings

Headers
Choose which headers to include in the cache key.
None

Object caching
○ Use origin cache headers
● Customize

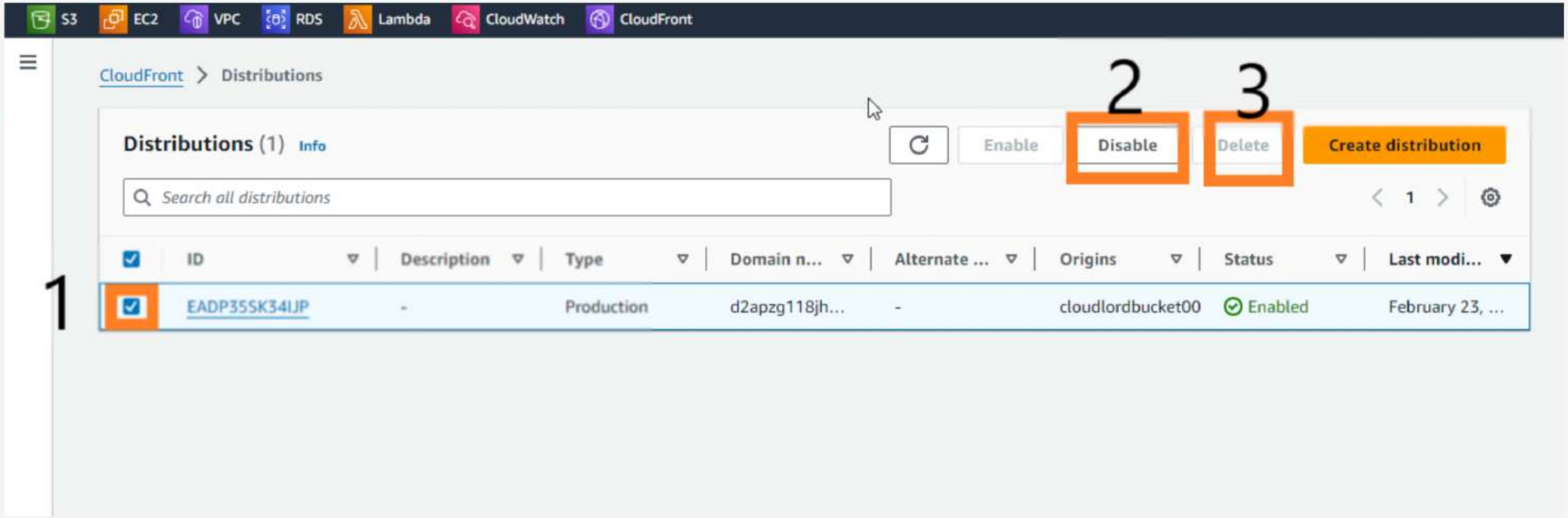
Minimum TTL	Maximum TTL	Default TTL
Minimum time to live in seconds.	Maximum time to live in seconds.	Default time to live in seconds
0	31536000	86400

Response headers policy - *optional*
Choose an existing response headers policy or create a new one.

BY AYOMIDE OGUNSANYA (THECLOUDLORD

Warning! Make Sure You Disable and Delete your Cloudfront Distribution if not in use to Avoid Billing on your account. Follow the Steps as indicated below the same applies to your S3 bucket on the next page.

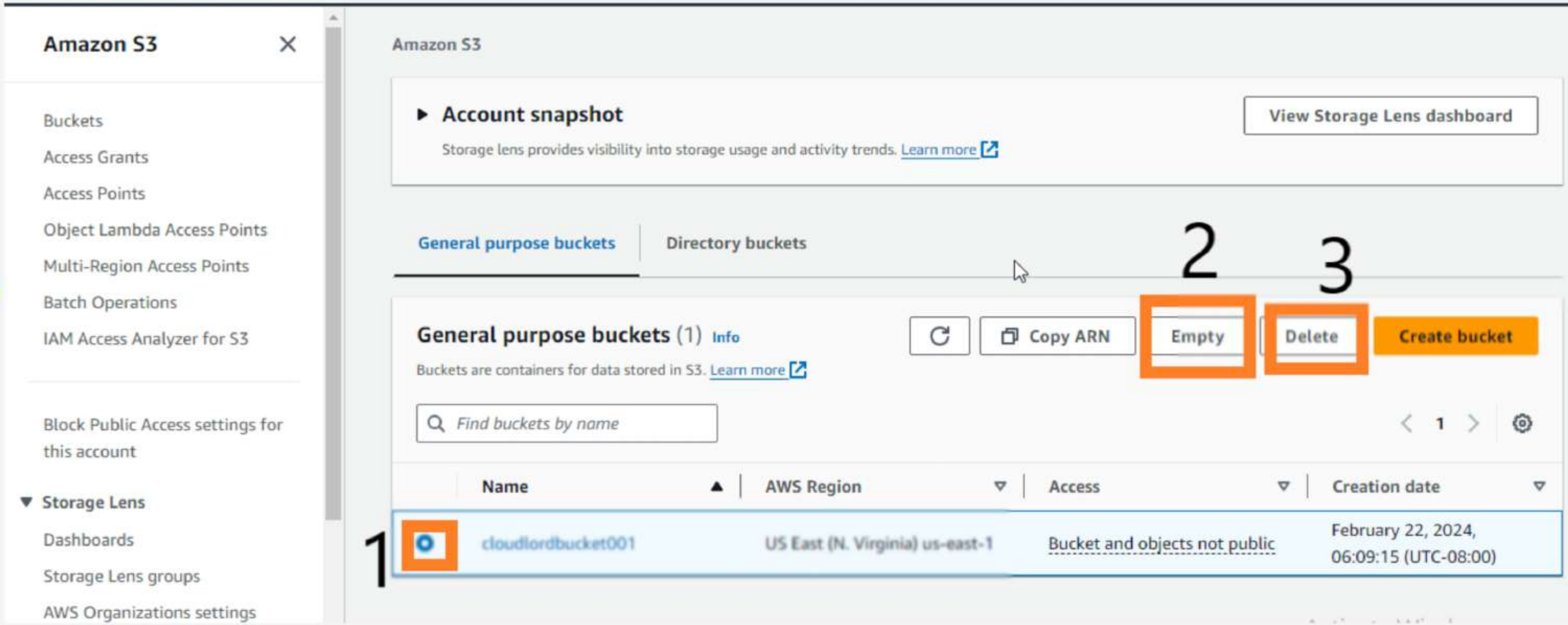
28.



☑	ID	Description	Type	Domain n...	Alternate ...	Origins	Status	Last modi...
☑	EADP35SK34IJP	-	Production	d2apzg118jh...	-	cloudlordbucket00	✓ Enabled	February 23, ...

BY AYOMIDE OGUNSANYA (THECLOUDLORD

29.



Amazon S3

- Buckets
- Access Grants
- 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
  - Storage Lens groups
  - AWS Organizations settings

Amazon S3

▶ Account snapshot

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

General purpose buckets (1) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
●	cloudlordbucket001	US East (N. Virginia) us-east-1	Bucket and objects not public	February 22, 2024, 06:09:15 (UTC-08:00)

BY AYOMIDE OGUNSANYA (THECLOUDLORD)

30. Thank You

@TheCloudLord

@TheCloudLord_

Ayomide Ogunsanya