

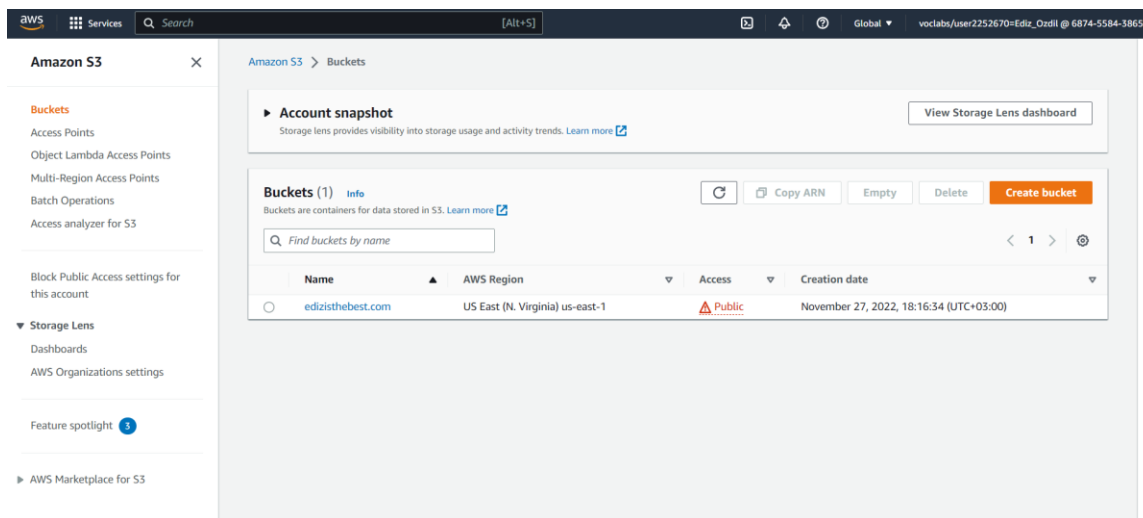
EDİZ ÖZDİL – 1906811

COP4493 PROJECT

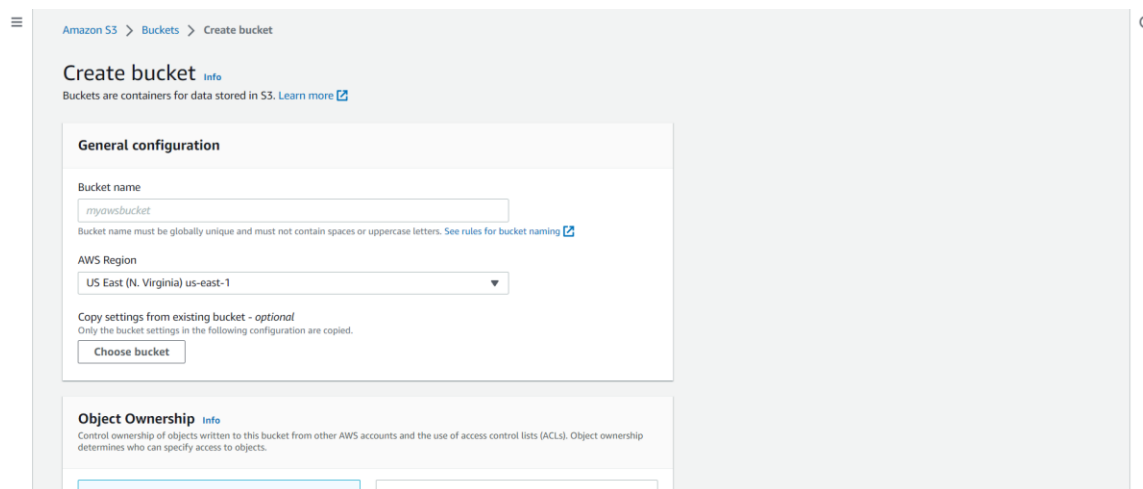
URL OF THE WEBSITE: <http://edizisthebest.com.s3-website-us-east-1.amazonaws.com/>

ACCOUNT ID: 687455843865

1. Create a bucket and click the create bucket



2. Enter bucket name and choose the region



3.Create Bucket

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 (0) - optional

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

No tags associated with this bucket.

Add tag

Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption

☒ Disable

☐ Enable

► Advanced settings

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

Cancel

Create bucket

4. Enable static website hosting. Assign index and error files and upload them to the objects.

edizisthebest.com

Publicly accessible

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (2)

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 objects, you'll need to explicitly grant them permissions. [Learn more](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

<

1

>

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	error.html	html	November 27, 2022, 19:18:44 (UTC+03:00)	0 B	Standard
<input type="checkbox"/>	index.html	html	November 27, 2022, 18:29:50 (UTC+03:00)	197.0 B	Standard

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](#)

i 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

Redirection rules - optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

```
< error.html  < index.html X
C: > Users > EdizOzdil > OneDrive - Cubedots > Desktop > < index.html > html
1  <html xmlns="http://www.w3.org/1999/xhtml" >
2  <head>
3  |   <title>My Website Home Page</title>
4  </head>
5  <body>
6  |   <h1>Welcome to my website</h1>
7  |   <p>Now hosted on Amazon S3!</p>
8  </body>
9  </html>
```

```
< error.html X  < index.html
C: > Users > EdizOzdil > OneDrive - Cubedots > Desktop > < error.html
1  
```

5. Edit block public access settings.To create a public, static website, you might also have to edit the Block Public Access settings for your account before adding a bucket policy. Clear Block all public access, and choose 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.

☐ **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](#)

© 2022 Amazon Web Services, Inc. or its affiliates

6. Add a bucket policy that makes my bucket content publicly available. To grant public read access to your website, copy the following bucket policy, and paste it into the Bucket policy editor.

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](#)

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

[Copy](#)

© 2022 Amazon Web Services, Inc. or its affiliates

7. Create a distribution screen, select the origin domain and write our index.html file to the default root object part and create our distribution.

Create distribution

Origin

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

Origin path - optional [Info](#)
Enter a URL path to append to the origin domain name for origin requests.

Name
Enter a name for this origin.

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.

Add custom header - optional
CloudFront includes this header in all requests that it sends to your origin.

Enable Origin Shield [Info](#)
Origin Shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.

☒ **No**

☐ **Yes**

Alternate domain name (CNAME) - optional
Add the custom domain names that you use in URLs for the files served by this distribution.

ⓘ To add a list of alternative domain names, use the [bulk editor](#).

Custom SSL certificate - optional
Associate a certificate from AWS Certificate Manager. The certificate must be in the US East (N. Virginia) Region (us-east-1).

[Request certificate](#)

Supported HTTP versions
Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default.

☒ **HTTP/2**

☐ **HTTP/3**

Default root object - optional
The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.

Standard logging
Get logs of viewer requests delivered to an Amazon S3 bucket.

☒ **Off**

☐ **On**

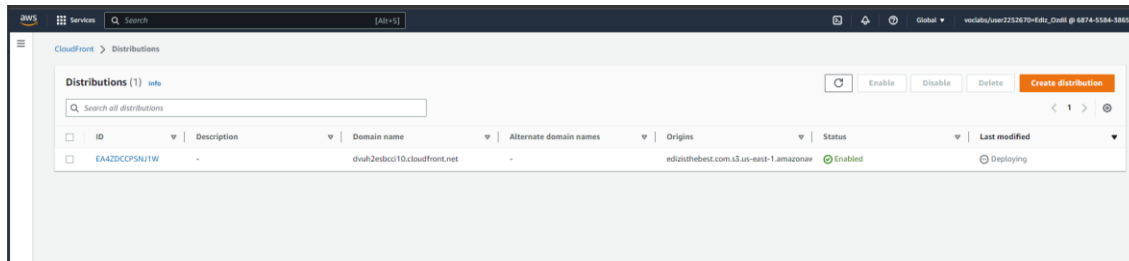
IPv6

☐ **Off**

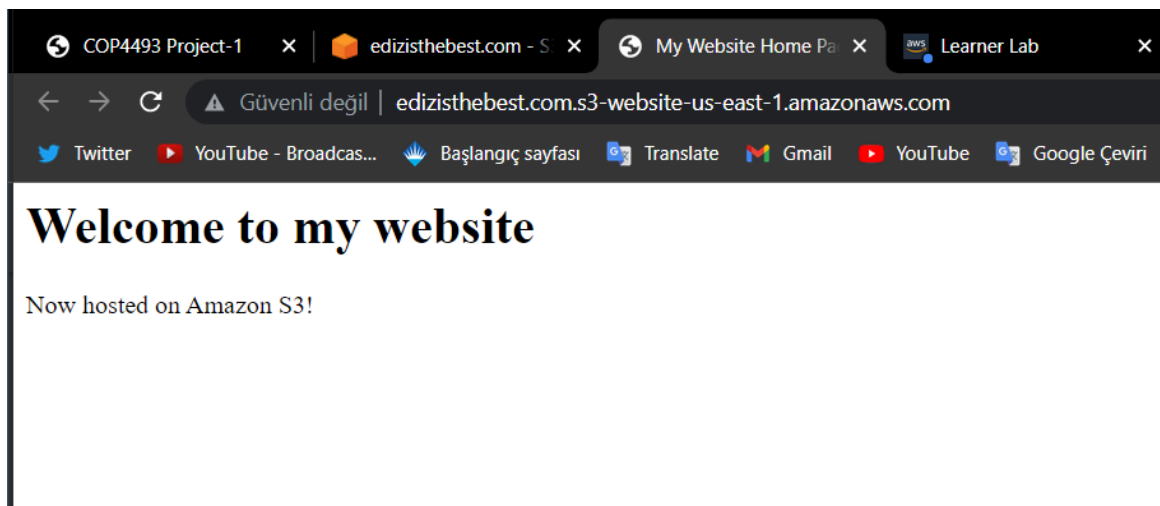
☒ **On**

Description - optional

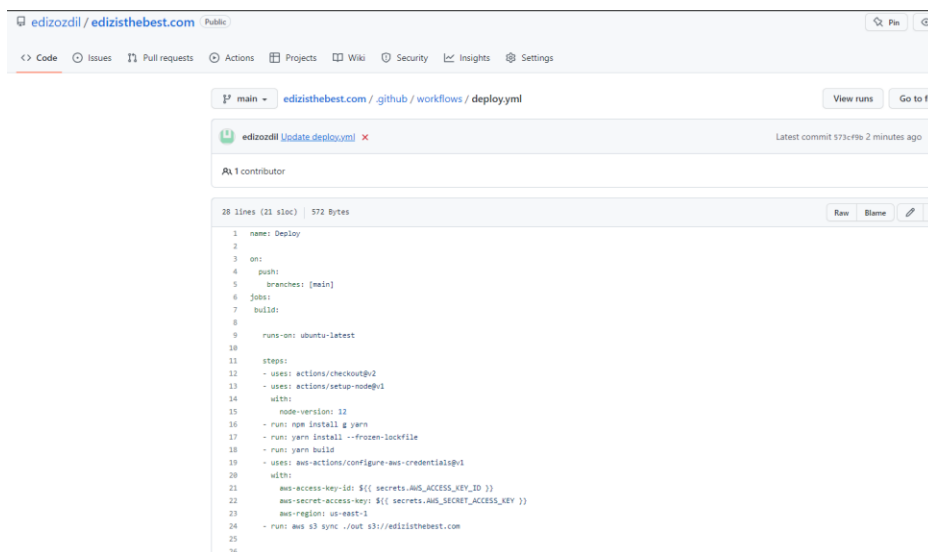
8. Our distribution is ready.



9. Also our project is ready too.



10. BONUS GITHUB PART





Unable to create user

AWS could not create the user you requested. [Learn more](#)

User: arn:aws:sts::687455843865:assumed-role/voclabs/user2252670=Ediz_Ozdil is not authorized to perform: iam:CreateUser on resource: arn:aws:iam::687455843865:user/ed because no identity-based policy allows the iam:CreateUser action

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	ed
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes

I don't have permission for adding users and see their access and secret access keys then Git project failed.

edizozdil / edizisthebest.com Public

<> Code Issues Pull requests Actions Projects Wiki Security Insights Settings

← Deploy

Update deploy.yml #8

Summary

Jobs

build

Run details

Usage

Workflow file

build

failed 3 minutes ago in 23s

- > Set up job
- > Run actions/checkout@v2
- > Run actions/setup-node@v1
- > Run npm install g yarn
- > Run yarn install --frozen-lockfile
- > Run yarn build
 - Run aws-actions/configure-aws-credentials@v1
 - Run aws s3 sync ./out s3://edizisthebest.com
- > Post Run actions/checkout@v2
- > Complete job