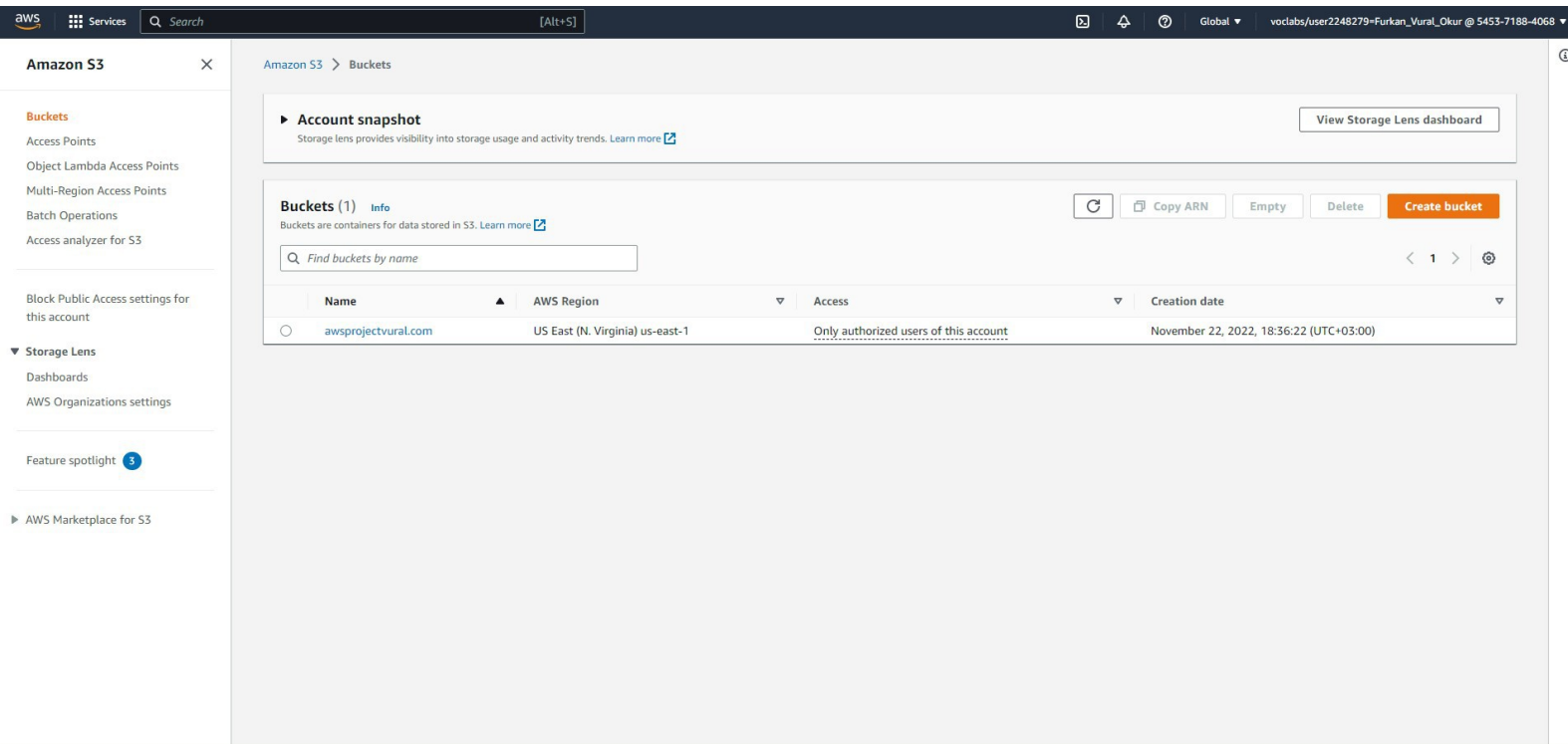


URL of the website: <http://awsprojectvural.com.s3-website-us-east-1.amazonaws.com>
AWS Account ID: 545371884068

CREATE BUCKET AND UPLOAD HTML FILES:

Type S3 in Search and enter S3 service. Click on create bucket on the next screen.



Amazon S3 > Buckets

Account snapshot
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

Buckets (1) [Info](#)
Buckets are containers for data stored in S3. [Learn more](#)

Name	AWS Region	Access	Creation date
awsprojectvural.com	US East (N. Virginia) us-east-1	Only authorized users of this account	November 22, 2022, 18:36:22 (UTC+03:00)

[View Storage Lens dashboard](#)

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Choose name and region.

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Click create bucket without changing anything.

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

Enter the bucket you created and drag and drop the HTML files you created before to the screen or upload them from the upload button.

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Follow security best practices for S3.

Amazon S3 > Buckets > awsprojectvural.com

awsprojectvural.com

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

Show versions

	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	awsprojectvuralerror.html	html	November 22, 2022, 18:50:35 (UTC+03:00)	38.0 B	Standard
<input type="checkbox"/>	awsprojectvuralindex.html	html	November 22, 2022, 18:50:36 (UTC+03:00)	197.0 B	Standard

Feedback

Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Click upload without changing anything.

aws

Services

Search

[Alt+S]

Upload

Info

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 folders**.

Files and folders (2 Total, 235.0 B)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	awsprojectvuralerror.ht ml	-	text/html	38.0 B
<input type="checkbox"/>	awsprojectvuralindex.ht ml	-	text/html	197.0 B

Destination

Destination

s3://awsprojectvural.com

► 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

Go to properties in your bucket. Click the edit button to the right of the static website hosting section at the bottom of the page.

Feature spotlight

► AWS Marketplace for S3

Static website hosting

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

Edit

Static website hosting

Enabled

Hosting type

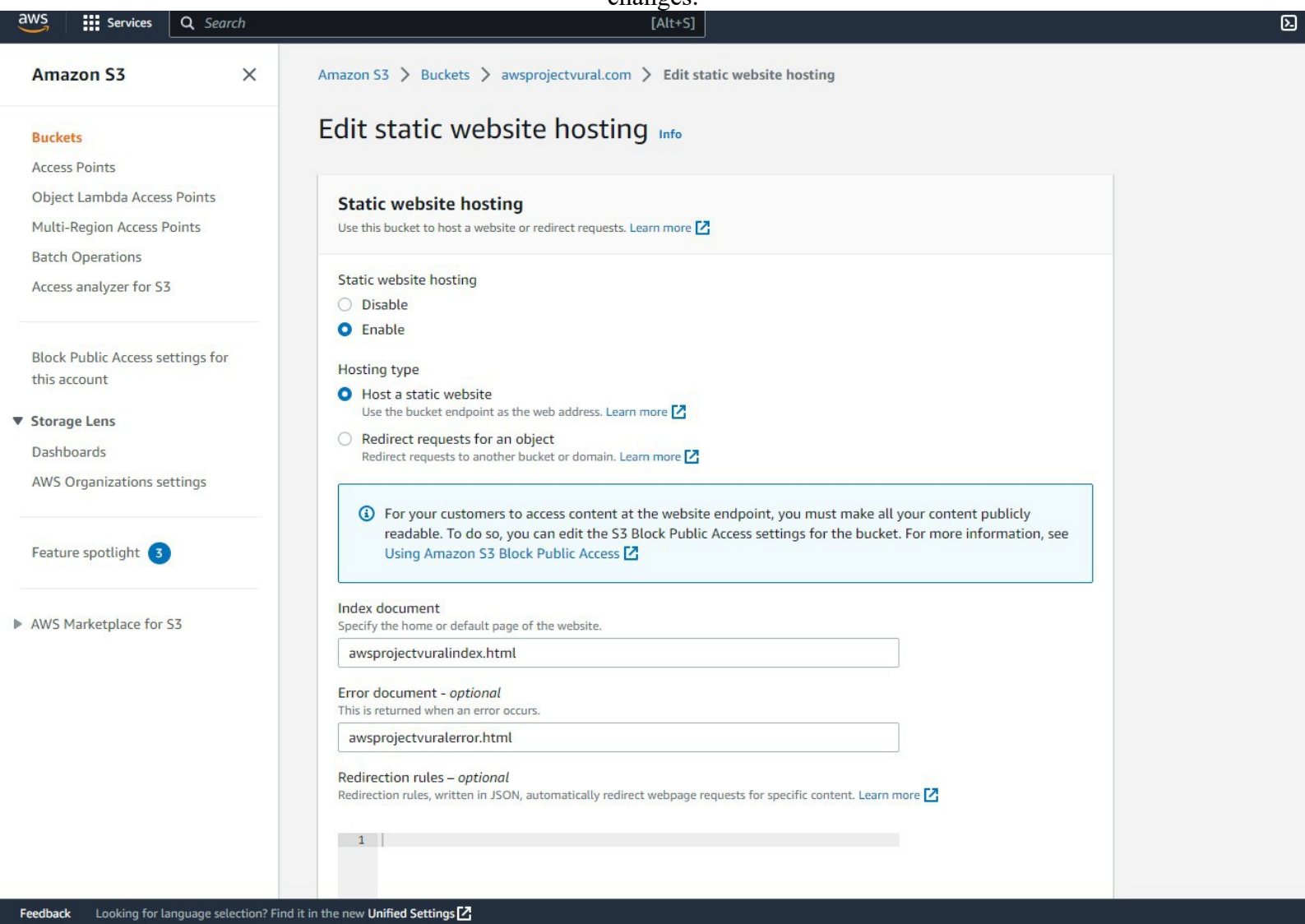
Bucket hosting

Bucket website endpoint

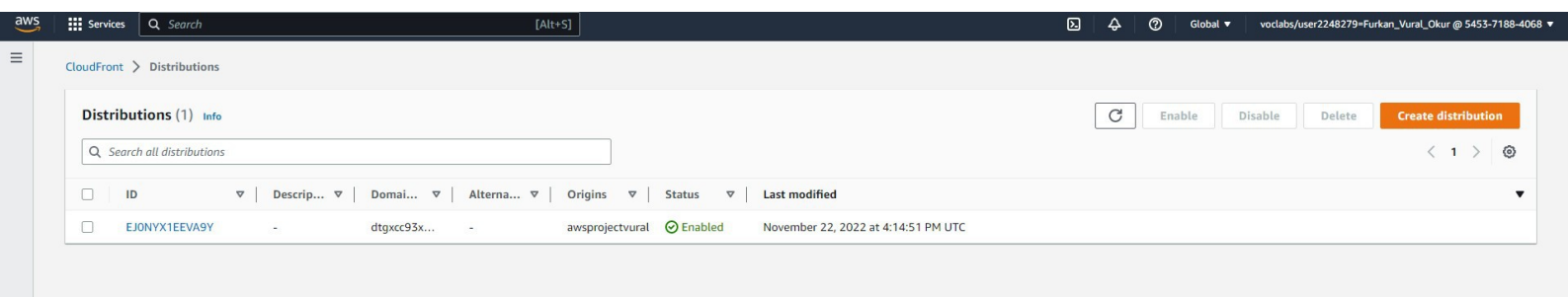
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

<http://awsprojectvural.com.s3-website-us-east-1.amazonaws.com>

Then enter the names of the HTML files you have uploaded to your bucket in the index document section and click save changes.



Then go to cloudfront service by typing cloudfront in the search field and click create distribution.



On the create distribution screen, select your origin domain.



Services

Search

[Alt+S]

CloudFront > Distributions > create

Create distribution

Origin

Origin domain

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

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

Origin path - optional

[Info](#)

Enter a URL path to append to the origin domain name for origin requests.

Enter the origin path

Name

Enter a name for this origin.

awsprojectvural.com.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.

Add custom header - optional

CloudFront includes this header in all requests that it sends to your origin.

Add header

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

Then write the name of your HTML file in the default root object section at the bottom of the page and click the create distribution button.

aws Services Search [Alt+S]

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

Add item

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).

Choose certificate

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.

awsprojectvuralindex.html

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

☒ Off
☐ On

IPv6

☐ Off
☒ On

Description - optional

Cancel Create distribution

Feedback Looking for language selection? Find it in the new [Unified Settings](#)

You have uploaded your static web content to S3 bucket and served static web content using CloudFront. That's it.

URL of the repository:

<https://github.com/FurkanVural/awsprojectvural.com.git>

Readme files on repository:

awsprojectvural.com

github URL:

<https://github.com/FurkanVural/awsprojectvural.com.git>

AWS Account ID: 545371884068

CHANGING S3 BUCKET TO BE NOT PUBLIC ACCECIBLE:

Go to the bucket you created and go to the permission section.

Click on edit under the block public access text.

Amazon S3 Buckets awsprojectvural.com

awsprojectvural.com Info

Publicly accessible

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access

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](#)

Edit

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](#)

Edit Delete

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

Copy

On the next screen, click on block all public access.

Amazon S3 Buckets awsprojectvural.com Edit 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.

Cancel Save changes

On the next screen, click on block all public access.

Amazon S3 > Buckets > awsprojectvural.com > Edit 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.

Cancel

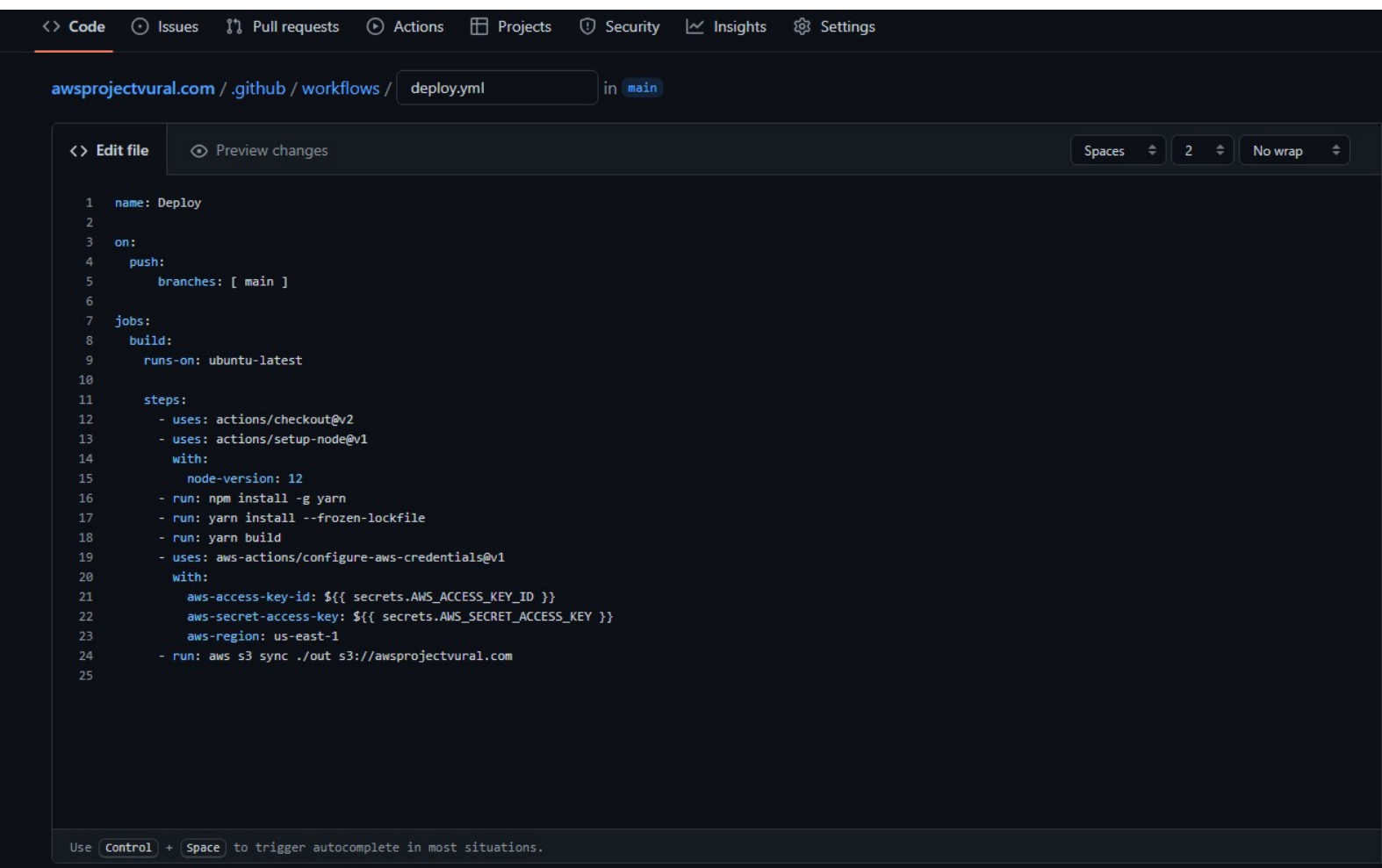
Save changes

Then save the changes with the save changes button.

The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, 'Services', a search bar, and the user's account information. The left sidebar shows the 'Amazon S3' service selected, with a list of S3 features like 'Buckets', 'Access Points', and 'Storage Lens'. The main content area is titled 'Amazon S3 > Buckets' and displays the 'Account snapshot' section. Below this, the 'Buckets (1)' section shows a table with one bucket, 'awsprojectvural.com', located in 'US East (N. Virginia) us-east-1' with 'Only authorized users of this account' access. The table has columns for Name, AWS Region, Access, and Creation date. At the bottom of the console, there is a 'Feature spotlight' section and a link to 'AWS Marketplace for S3'.

Name	AWS Region	Access	Creation date
awsprojectvural.com	US East (N. Virginia) us-east-1	Only authorized users of this account	November 22, 2022, 18:36:22 (UTC+03:00)

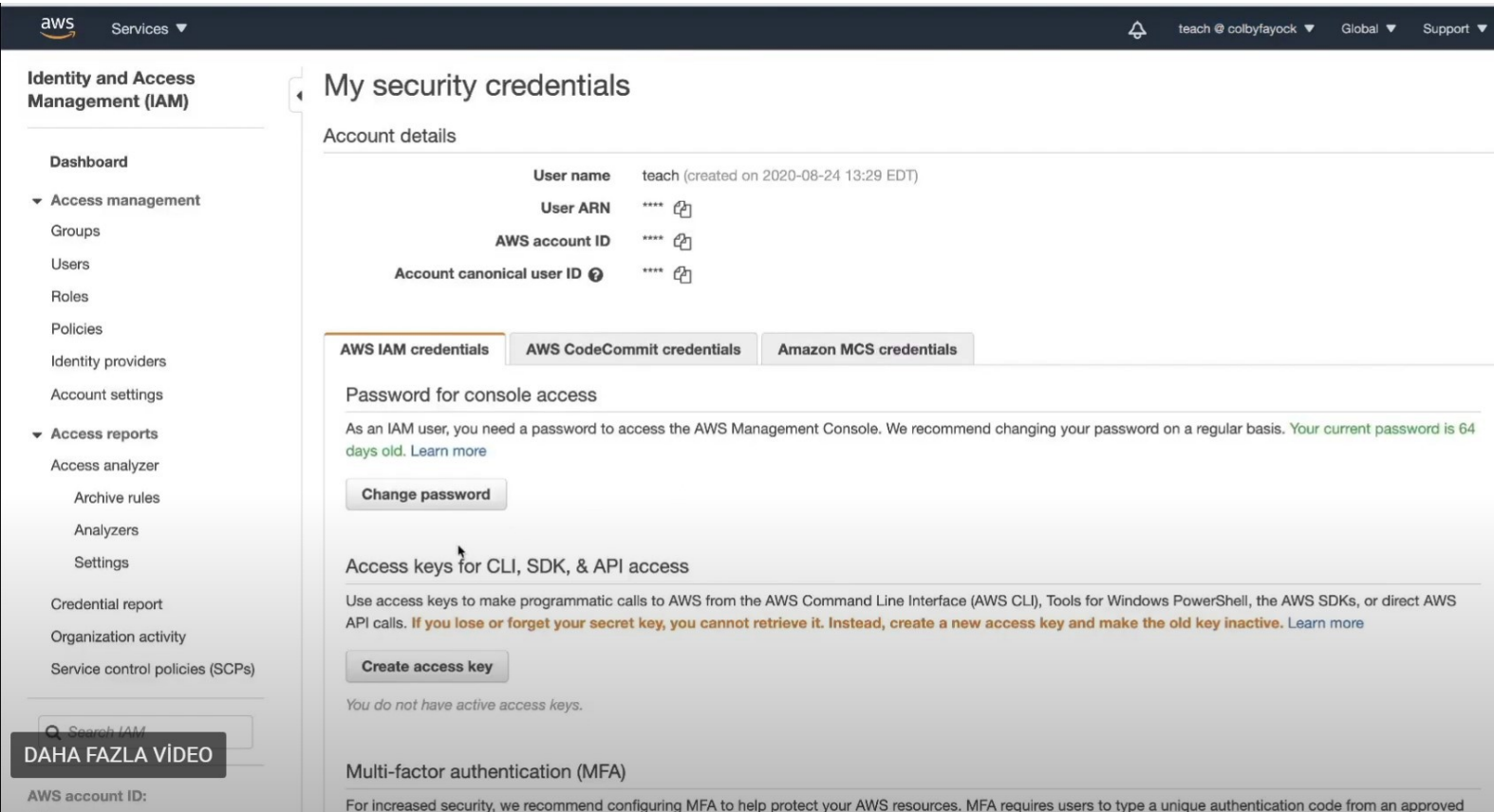
Github workflow to send static web content to S3 bucket



```
1 name: Deploy
2
3 on:
4   push:
5     branches: [ main ]
6
7 jobs:
8   build:
9     runs-on: ubuntu-latest
10
11     steps:
12       - uses: actions/checkout@v2
13       - uses: actions/setup-node@v1
14         with:
15           node-version: 12
16       - run: npm install -g yarn
17       - run: yarn install --frozen-lockfile
18       - run: yarn build
19       - uses: aws-actions/configure-aws-credentials@v1
20         with:
21           aws-access-key-id: ${ secrets.AWS_ACCESS_KEY_ID }
22           aws-secret-access-key: ${ secrets.AWS_SECRET_ACCESS_KEY }
23           aws-region: us-east-1
24       - run: aws s3 sync ./out s3://awsprojectvural.com
25
```

Use **Control** + **Space** to trigger autocomplete in most situations.

In AWS, go to my security credentials and click the create access key button.



The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with sections for 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Credential report'. The main content area is titled 'My security credentials' and shows account details for a user named 'teach'. Below the details, there are tabs for 'AWS IAM credentials', 'AWS CodeCommit credentials', and 'Amazon MCS credentials'. The 'AWS IAM credentials' tab is active, showing a 'Password for console access' section with a 'Change password' button. Below that is an 'Access keys for CLI, SDK, & API access' section with a 'Create access key' button. At the bottom, there is a 'Multi-factor authentication (MFA)' section.

My security credentials

Account details

User name	teach (created on 2020-08-24 13:29 EDT)
User ARN	****
AWS account ID	****
Account canonical user ID	****

AWS IAM credentials | AWS CodeCommit credentials | Amazon MCS credentials

Password for console access

As an IAM user, you need a password to access the AWS Management Console. We recommend changing your password on a regular basis. Your current password is 64 days old. [Learn more](#)

Change password

Access keys for CLI, SDK, & API access

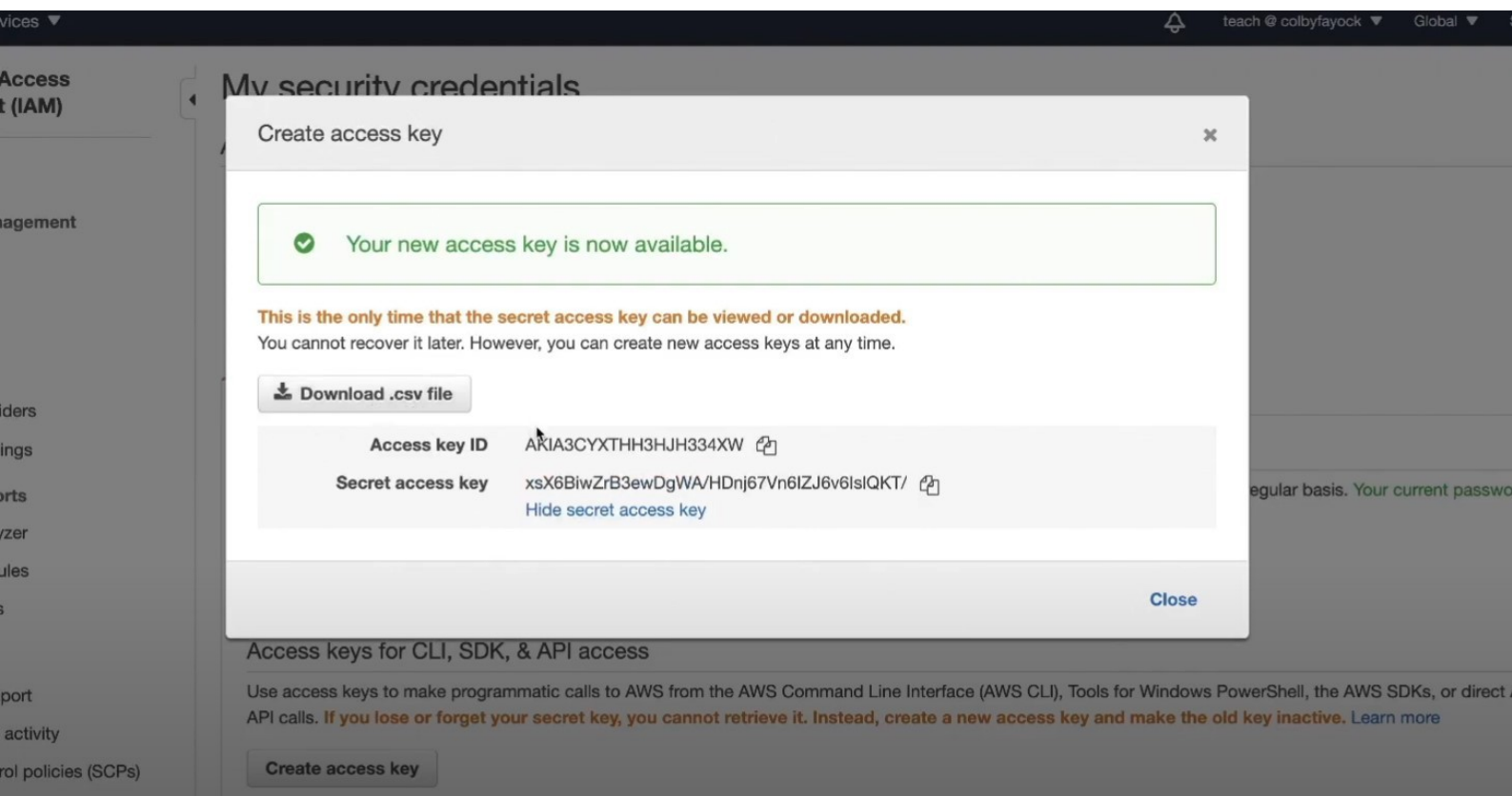
Use access keys to make programmatic calls to AWS from the AWS Command Line Interface (AWS CLI), Tools for Windows PowerShell, the AWS SDKs, or direct AWS API calls. **If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.** [Learn more](#)

Create access key

You do not have active access keys.

Multi-factor authentication (MFA)

For increased security, we recommend configuring MFA to help protect your AWS resources. MFA requires users to type a unique authentication code from an approved



Then create 2 secrets with these keys from the settings section in the bucket section.

