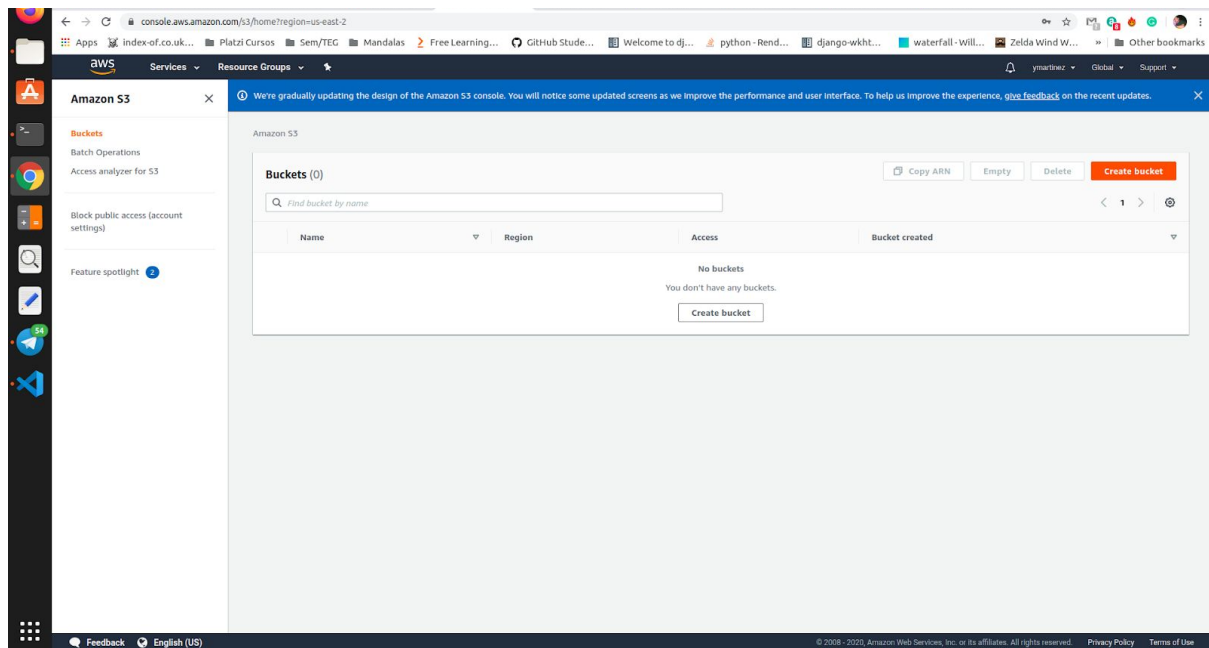
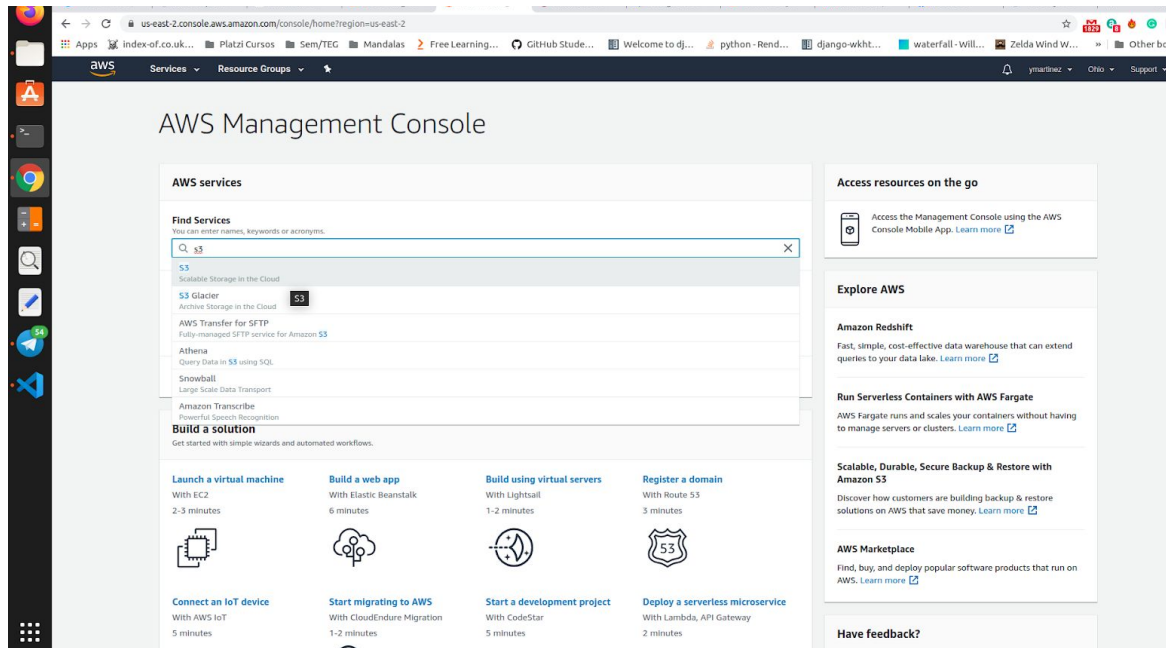


Deploy Static Website on AWS by Ybrahim Martinez

Website Files

Creating the S3 bucket



Amazon S3

Buckets

Batch Operations

Access analyzer for S3

Block public access (account settings)

Feature spotlight

Amazon S3

Create bucket

Create bucket

General configuration

Bucket name

udacity-static-web-page

Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

Region

US East (Ohio) us-east-2

Bucket settings for Block Public Access

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 enabling 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)

It 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.

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.

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

Advanced settings

Cancel

Create bucket

Feedback

English (US)

© 2008 - 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

Amazon S3

Buckets

Batch Operations

Access analyzer for S3

Block public access (account settings)

Feature spotlight

Amazon S3

Successfully created bucket udacity-static-web-page

To upload files and folders, or to configure additional bucket settings such as Bucket Versioning, tags, and default encryption, choose Go to bucket details.

Go to bucket details

Buckets (1)

Copy ARN

Empty

Delete

Create bucket

Find bucket by name

Name	Region	Access	Bucket created
udacity-static-web-page	US East (Ohio) us-east-2	Objects can be public	2020-04-16T17:37:17.000Z

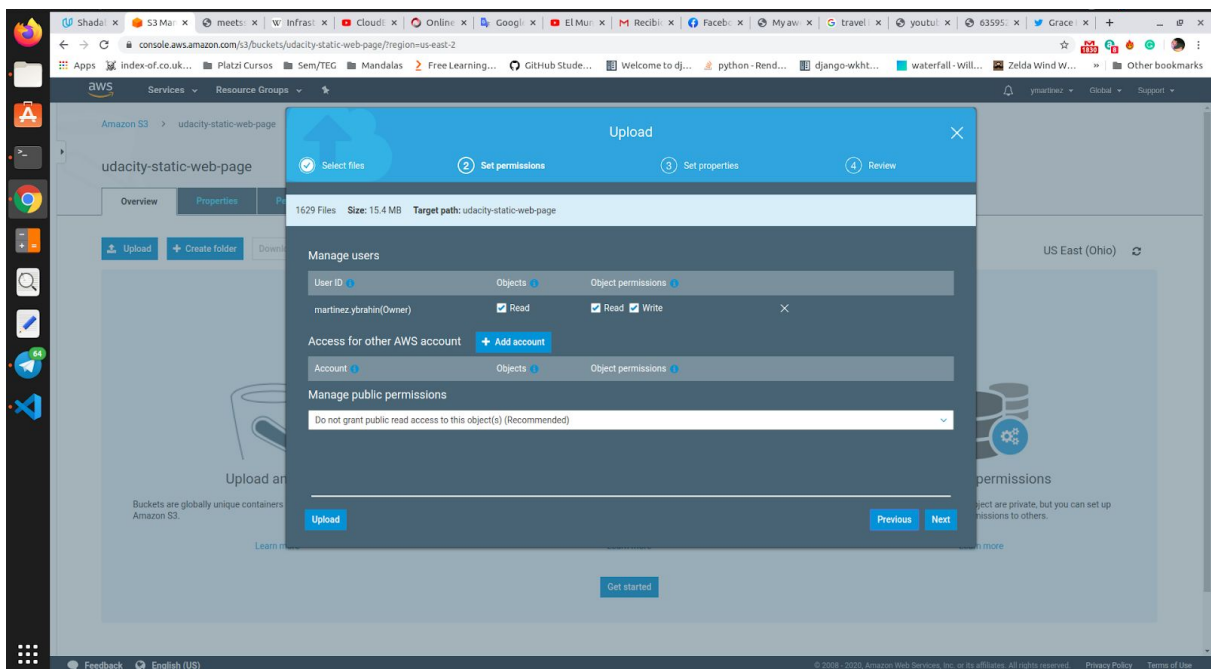
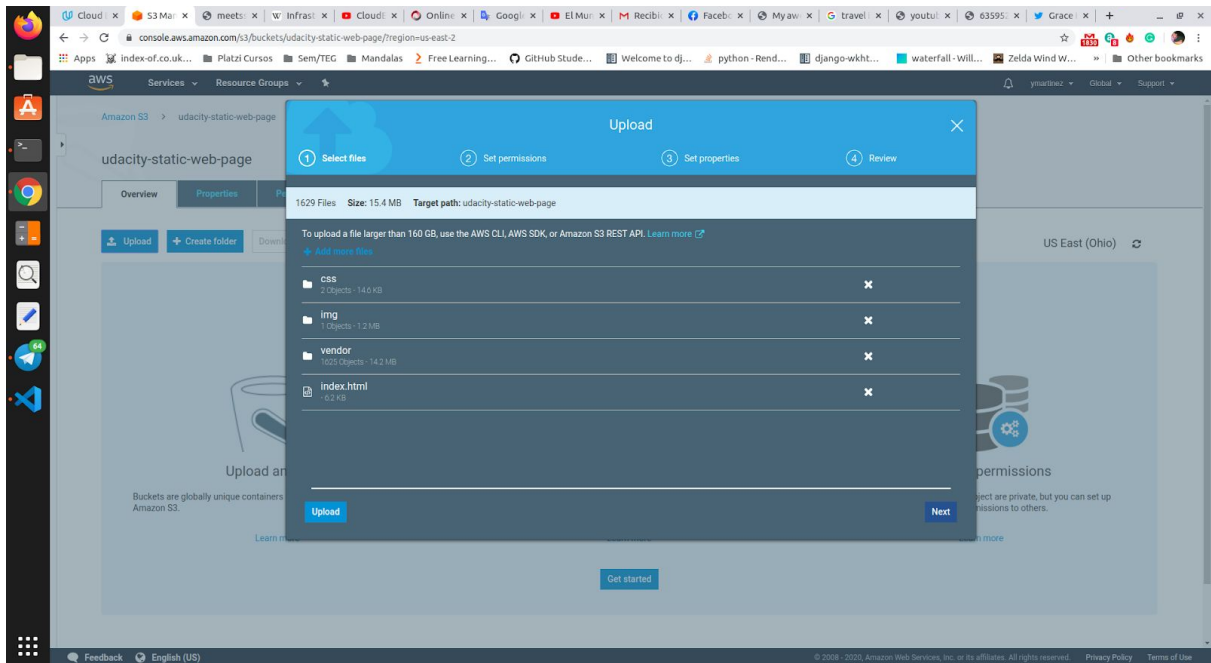
https://console.aws.amazon.com/s3/buckets/udacity-static-web-page/region-us-east-2

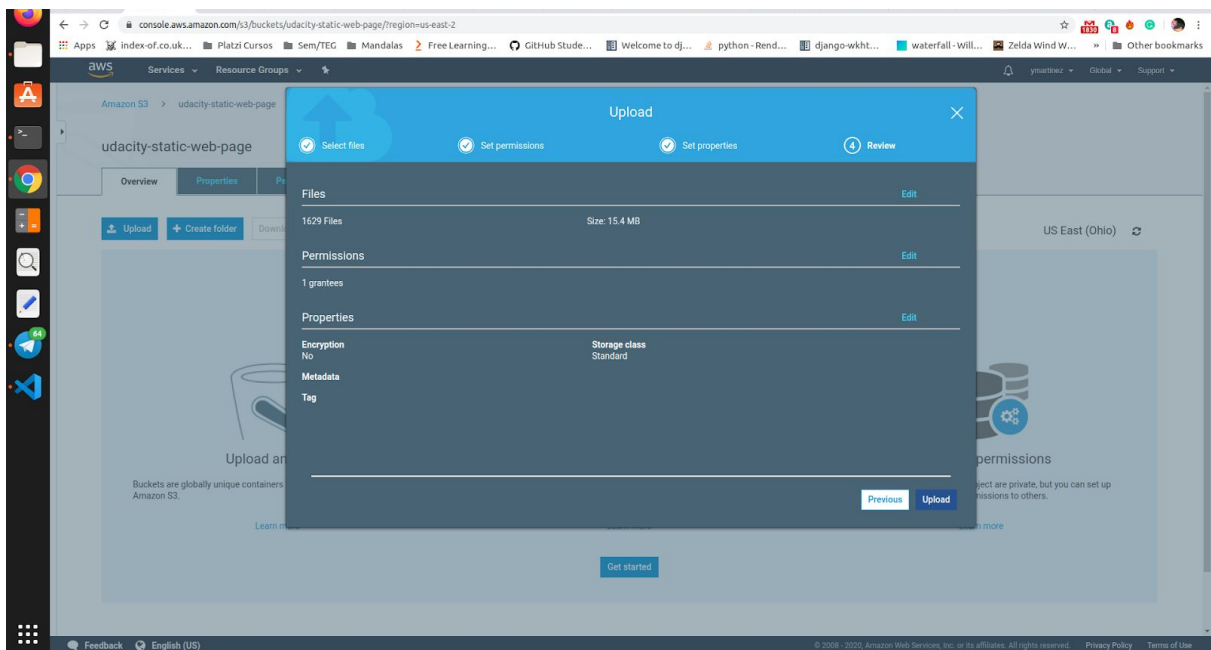
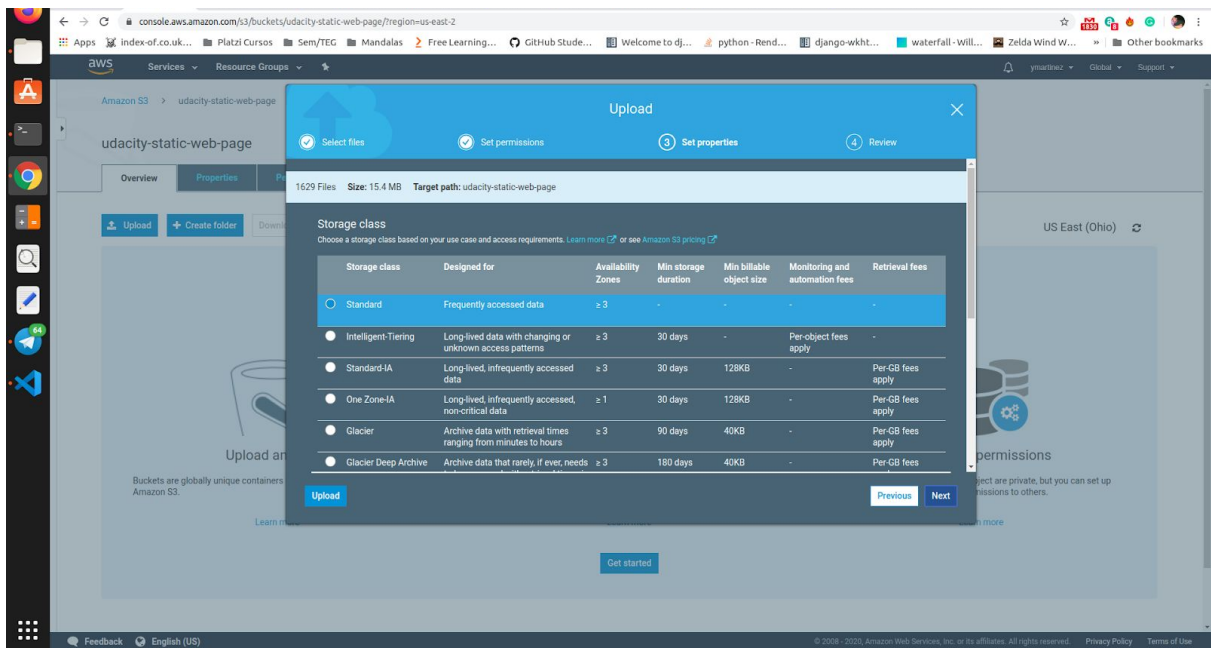
© 2008 - 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

Uploading the files



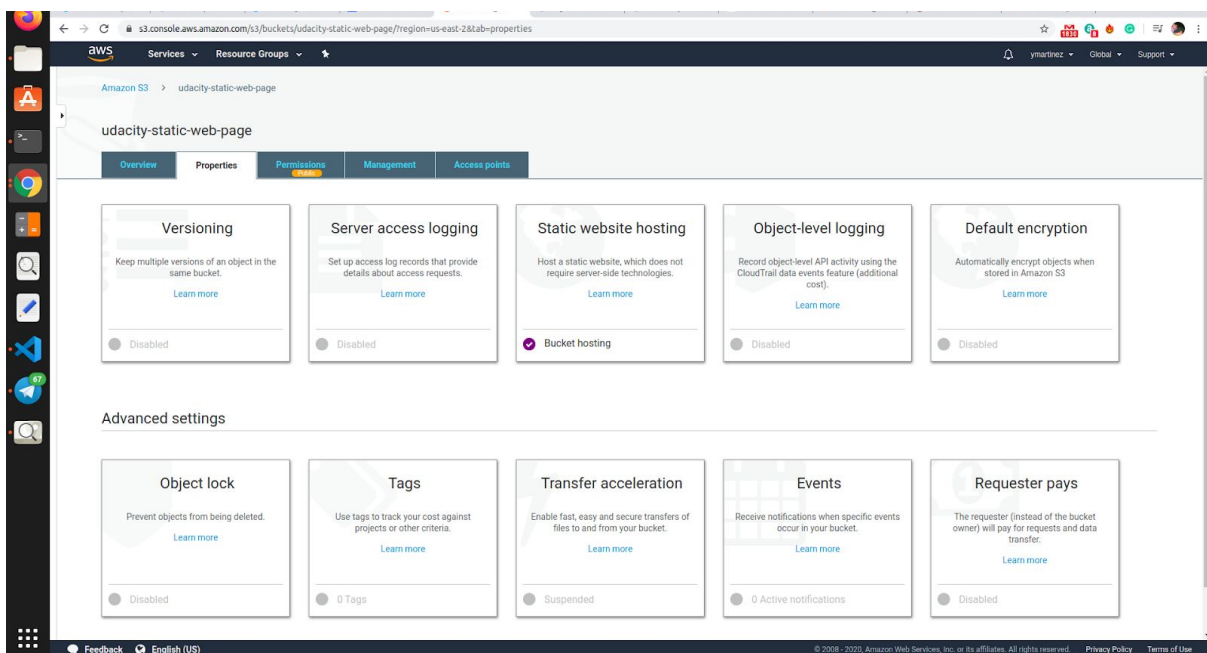
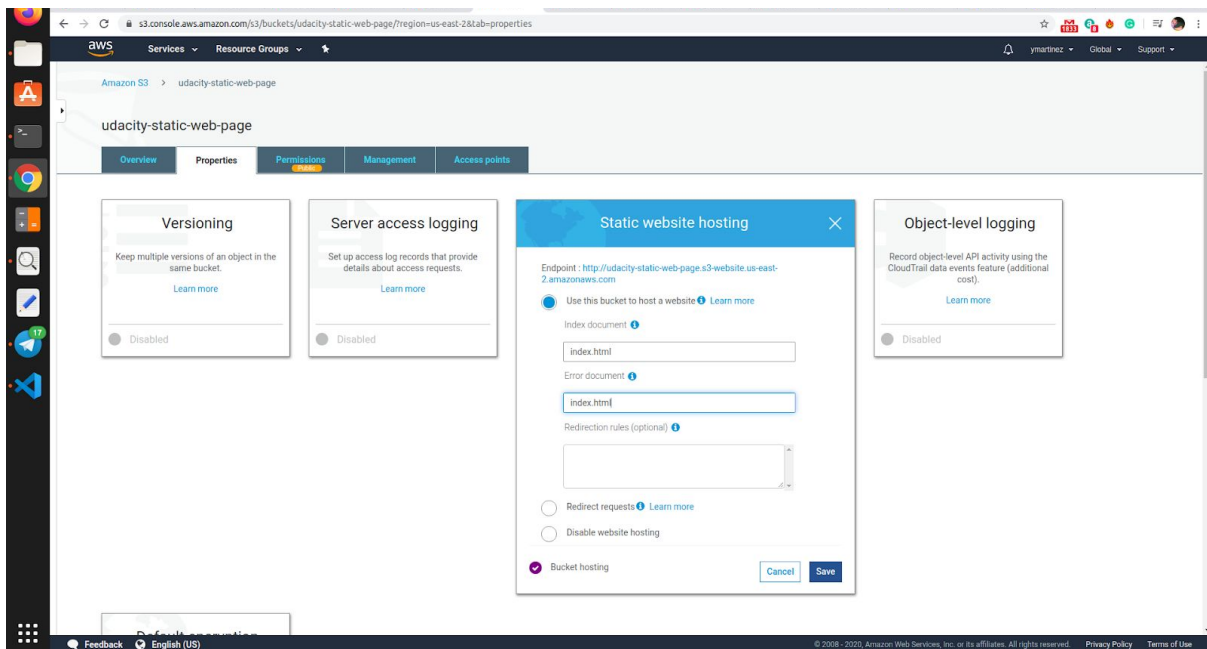


Securing the S3 bucket with an IAM policy

The screenshot shows the AWS Management Console interface for the 'udacity-static-web-page' bucket. The 'Permissions' tab is selected, and the 'Bucket Policy' button is highlighted. The 'Block public access' button is also visible. The 'Bucket policy editor' section shows a JSON policy that is currently empty. The console includes a sidebar with navigation options like 'Buckets', 'Batch operations', and 'Access analyzer for S3'. The top navigation bar shows the user's profile and various service links.

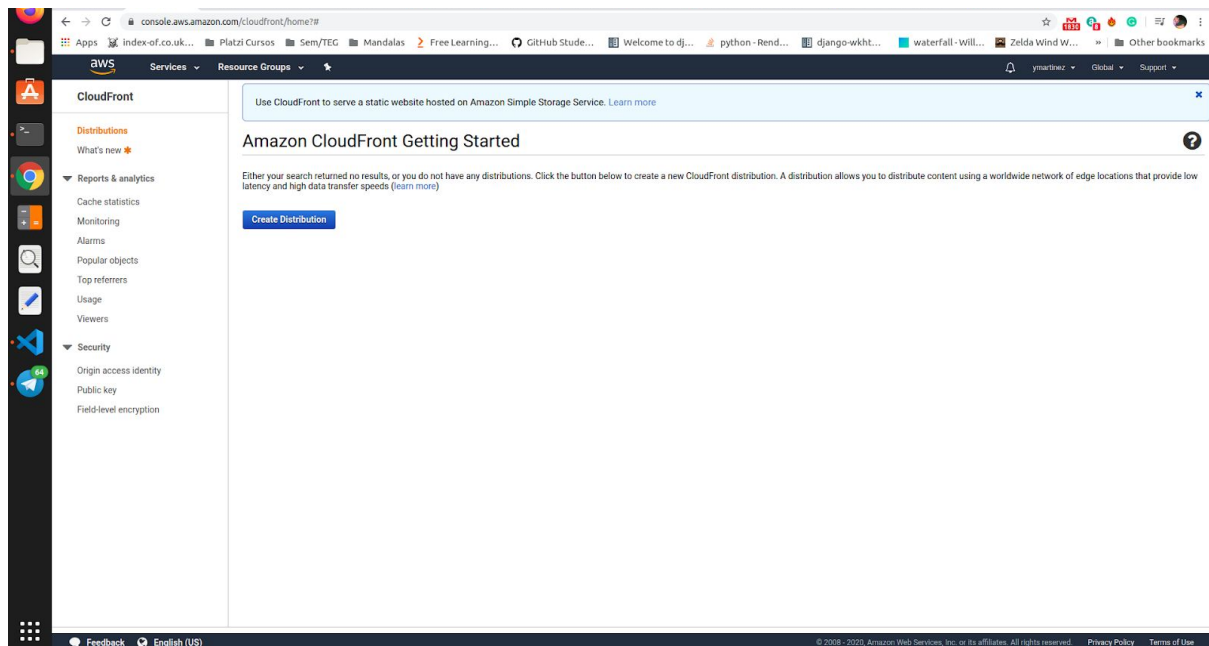
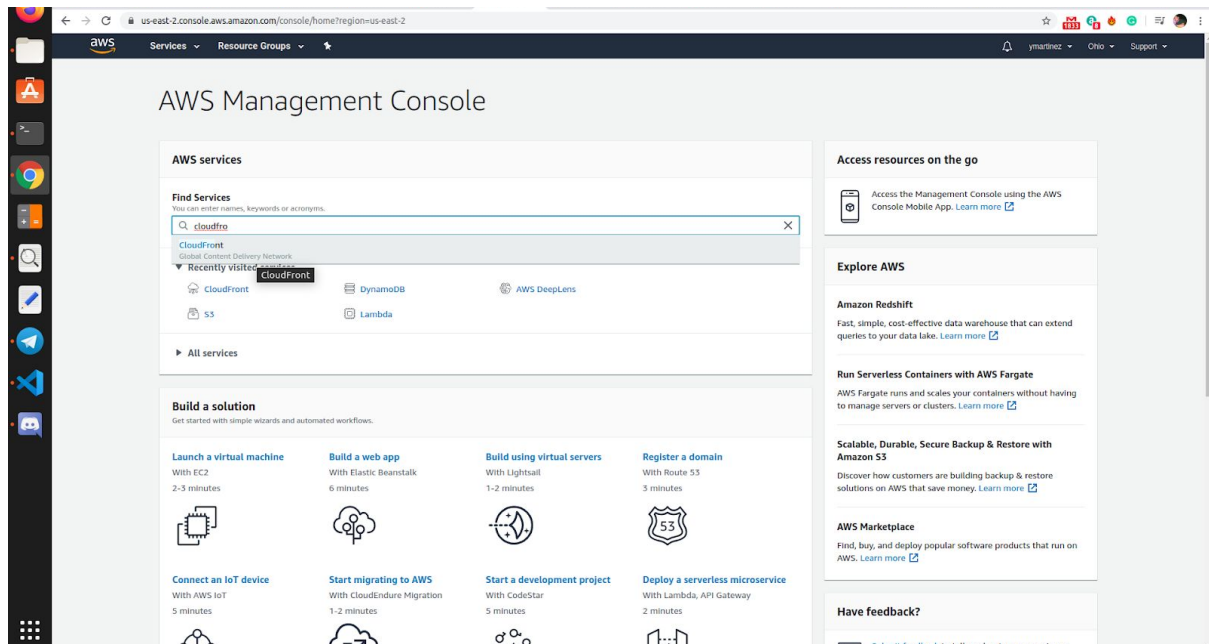
The screenshot shows the AWS Management Console interface for the 'udacity-static-web-page' bucket. A warning message is displayed: 'This bucket has public access. You have provided public access to this bucket. We highly recommend that you never grant any kind of public access to your S3 bucket.' The 'Bucket Policy' button is highlighted, and the 'Block public access' button is also visible. The 'Bucket policy editor' section shows a JSON policy that is updated to allow public access. The console includes a sidebar with navigation options like 'Buckets', 'Batch operations', and 'Access analyzer for S3'. The top navigation bar shows the user's profile and various service links.

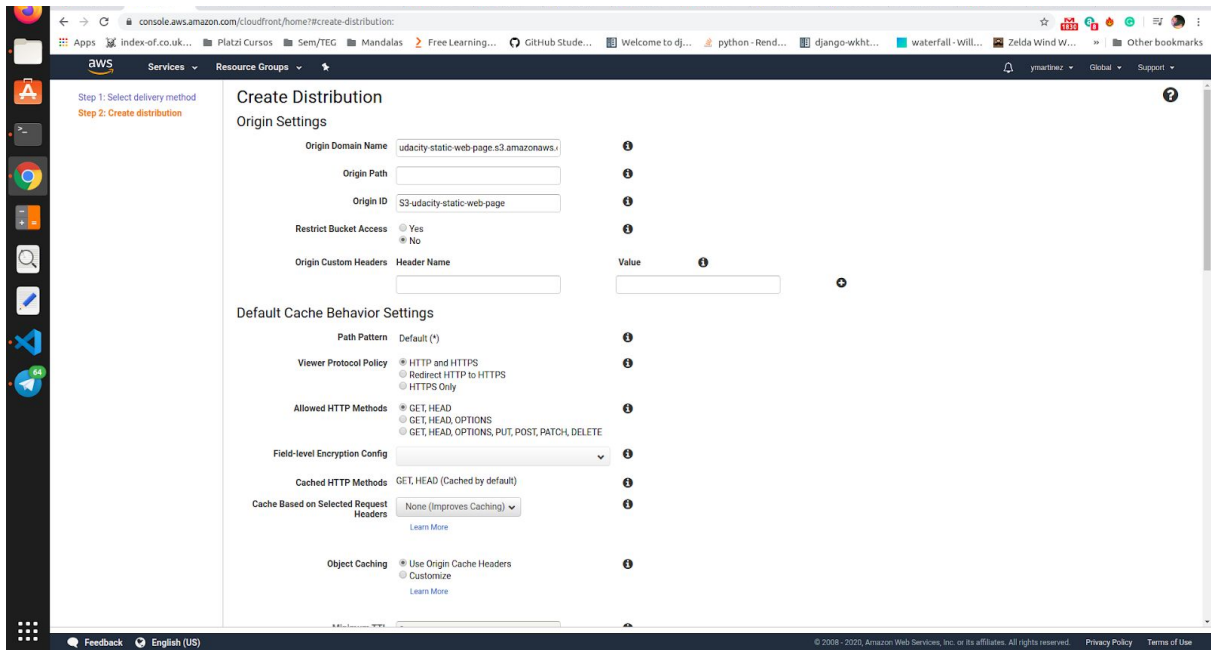
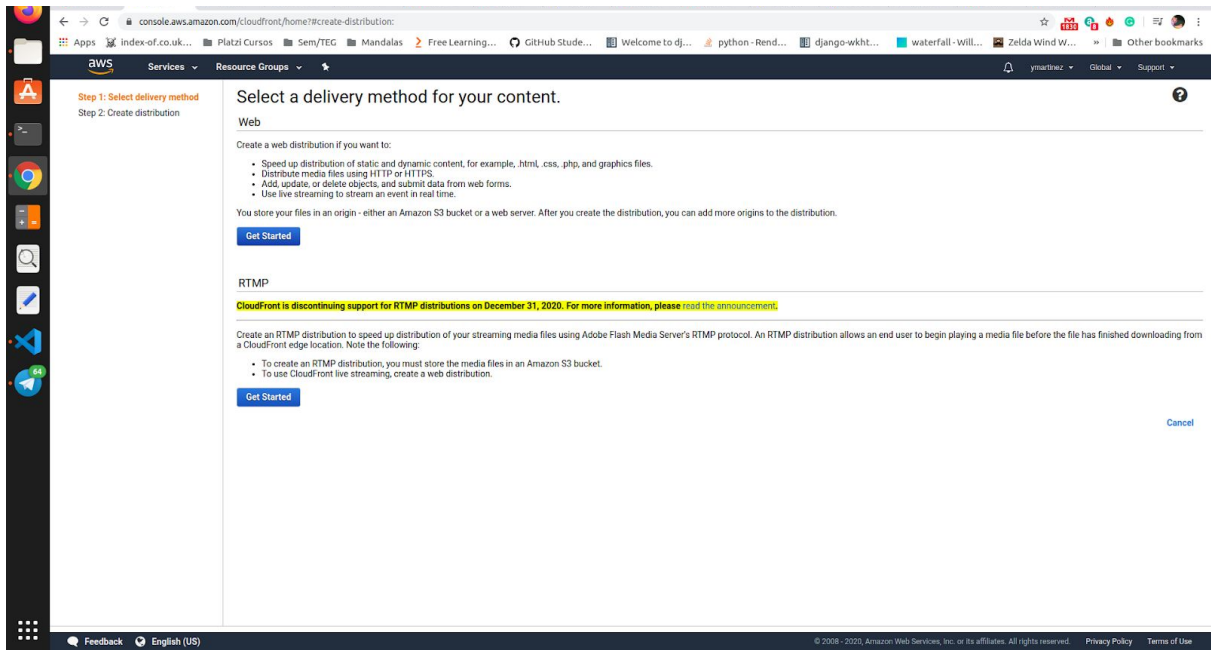
Configuring the S3 bucket to support static website hosting

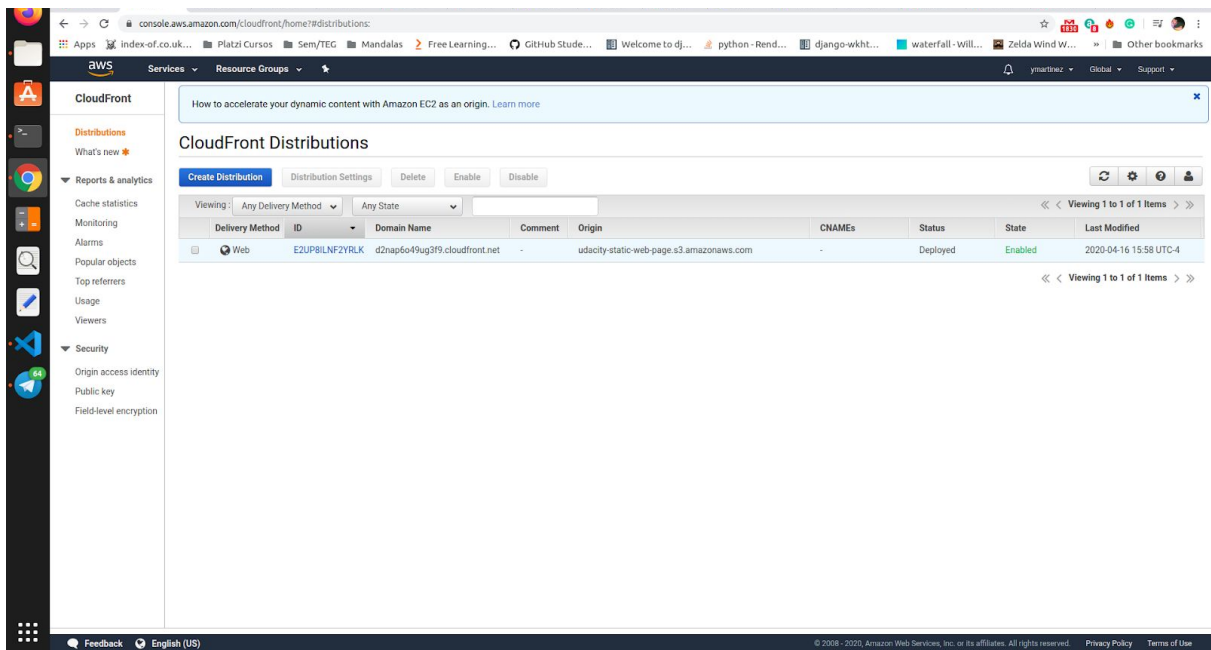


Website distribution

Configuring the Cloudfront service on the S3 bucket







Web browser access

Accessing to the website

