Project: Deploy Static Website on AWS

Hello, my name: Aya Rabih

 working! Dev-ops engineering in multinational lovely company and today we will learn Deploy Static Website on AWS. This project it is so critical to lean it and get more info for cloud and AWS.

So, in this documentation you will find all steps you need it to create it with deep details.

AWS

CloudFront Distribution

S3 Bucket
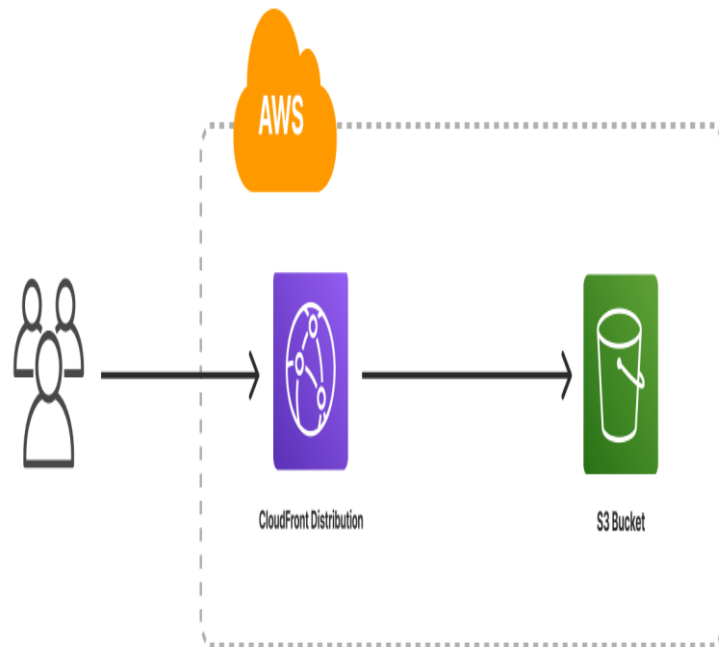
Create by Aya Rabih

Linked in   GitHub

PROJECT OVERVIEW

The cloud is perfect for hosting static websites that only include HTML, CSS, and JavaScript files that require no server-side processing. The whole project has two major intentions to implement:

Hosting a static website on S3 and

Accessing the cached website pages using Cloud Front content delivery network (CDN) service. Recall that Cloud Front offers low latency and high transfer speeds during website rendering.

Note that Static website hosting essentially requires a public bucket, whereas the Cloud Front can work with public and private buckets.

- ➢ In this project, you will deploy a static website to AWS by performing the following steps:
1. You will create a public S3 bucket and upload the website files to your bucket.
2. You will configure the bucket for website hosting and secure it using IAM policies.
3. You will speed up content delivery using AWS's content distribution network service, Cloud Front.
4. You will access your website in a browser using the unique Cloud Front endpoint.

1) <u>You will create a public S3 bucket and upload the website files to your bucket.</u>

➢ Click create bucket
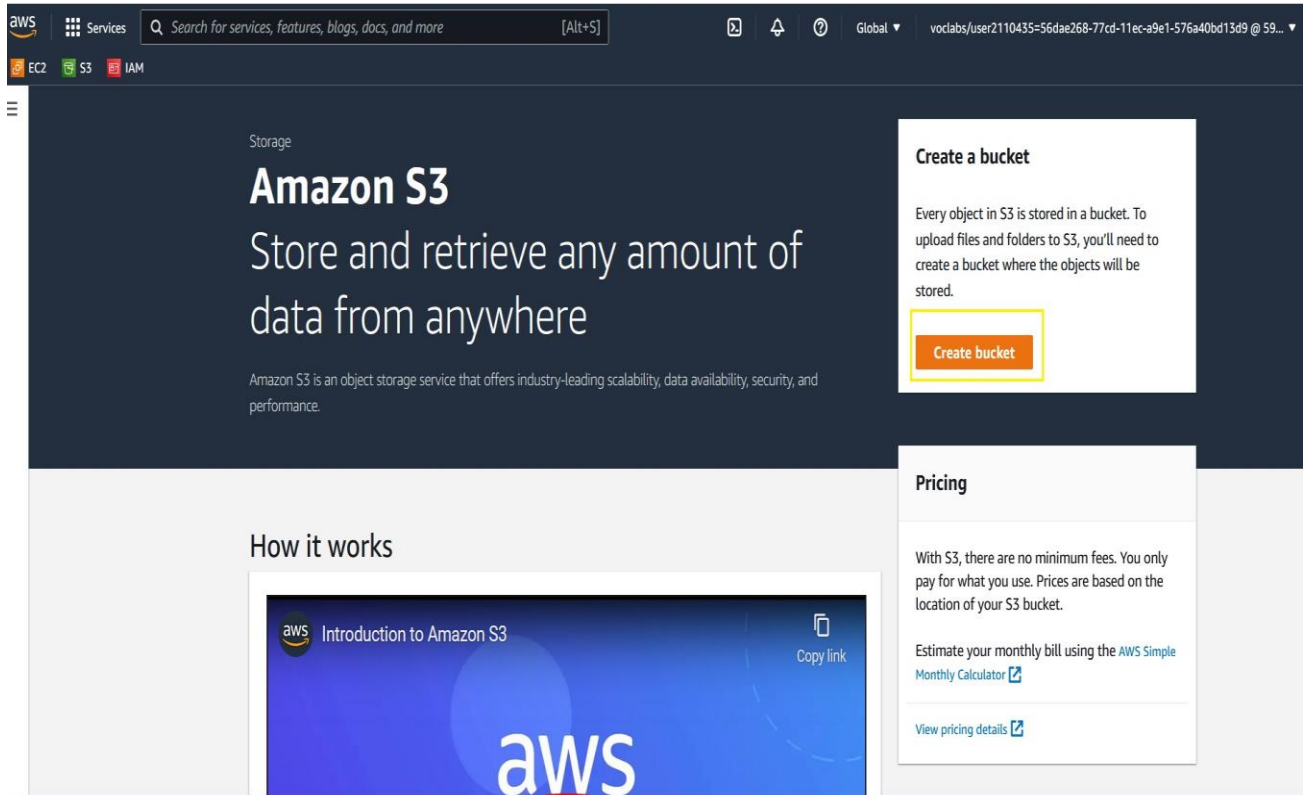
➢ Click create bucket name
➢ Click create Region you will create your bucket there
➢ Click create Acls disabled

Create bucket Info

Buckets are containers for data stored in S3. Learn more 🔗

General configuration

Bucket name

```
my-598824656916 bucket
```

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

AWS Region

```
US East (Ohio) us-east-2                              ▼
```

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

Choose bucket

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.

○ 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

➢ Click to remove block all public access

➢ Click to sure that you want be public

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)**
      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.

➢ Click 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*

Track storage cost or other criteria by tagging your bucket. 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

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Learn more

○ Disable

○ Enable
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

ⓘ Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.

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

Cancel   **Create bucket**

➢ Now we create bucket

⊘ **Successfully created bucket "my-598824656916-bucket"**
To upload files and folders, or to configure additional bucket settings choose **View details**.

View details   X

ⓘ Follow security best practices for S3.   Learn more   X

Amazon S3 > Buckets

▶ **Account snapshot**   View Storage Lens dashboard

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

Buckets (1)   Info   ⟳   🗇 Copy ARN   Empty   Delete   **Create bucket**

Buckets are containers for data stored in S3. Learn more 🔗

Q Find buckets by name   ⟨ 1 ⟩ ⚙

	Name ▲	AWS Region ▽	Access ▽	Creation date ▽
○	my-598824656916-bucket	US East (Ohio) us-east-2	Objects can be public	September 6, 2022, 01:42:44 (UTC+02:00)

2. You will configure the bucket for website hosting and secure it using IAM policies

➢ Upload files to S3 Bucket

Amazon S3 > Buckets > my-598824656916-bucket

my-598824656916-bucket   Info

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

Objects (0)

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**

Q Find objects by prefix   ⟨ 1 ⟩ ⚙

☐	Name ▲	Type ▽	Last modified ▽	Size ▽	Storage class ▽

No objects

You don't have any objects in this bucket.

🔼 Upload

➢ Click "Add files" to upload the index.html file, and click "Add folder" to upload the css, img, and vendor folders.

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 (0)   Remove   **Add files**   **Add folder**
All files and folders in this table will be uploaded.

🔍 Find by name   ‹ 1 ›

☐	Name ▲	Folder ▽	Type ▽	Size ▽

No files or folders

You have not chosen any files or folders to upload.

حجم الملف	تاريخ آخر تعديل	الاسم	
KB 342	-	MACOSX__	📁
KB 15	-	css	📁
KB 418	-	img	📁
MB 14	-	vendor	📁
KB 6	2019/05/18	index.html	📄
382 بايت	2019/05/18	README.txt	📄

➢ Now update files to S3 Bucket

➢ Now complete update files to S3 Bucket

1. Click on the "Permissions" tab.

2. The "Bucket Policy" section shows it is empty. Click on the Edit button.

```
{
"Version":"2012-10-17",
"Statement":[
 {
    "Sid":"AddPerm",
    "Effect":"Allow",
    "Principal": "*",
    "Action":["s3:GetObject"],
    "Resource":["arn:aws:s3::: my-598824656916-bucket/*"]
 }
]
}
```

3- Enter the following bucket policy replacing my-598824656916-bucketwith the name of your bucket and click "Save".

CONFIGURE S3 BUCKET

1. Go to the Properties tab and then scroll down to edit the Static website hosting section
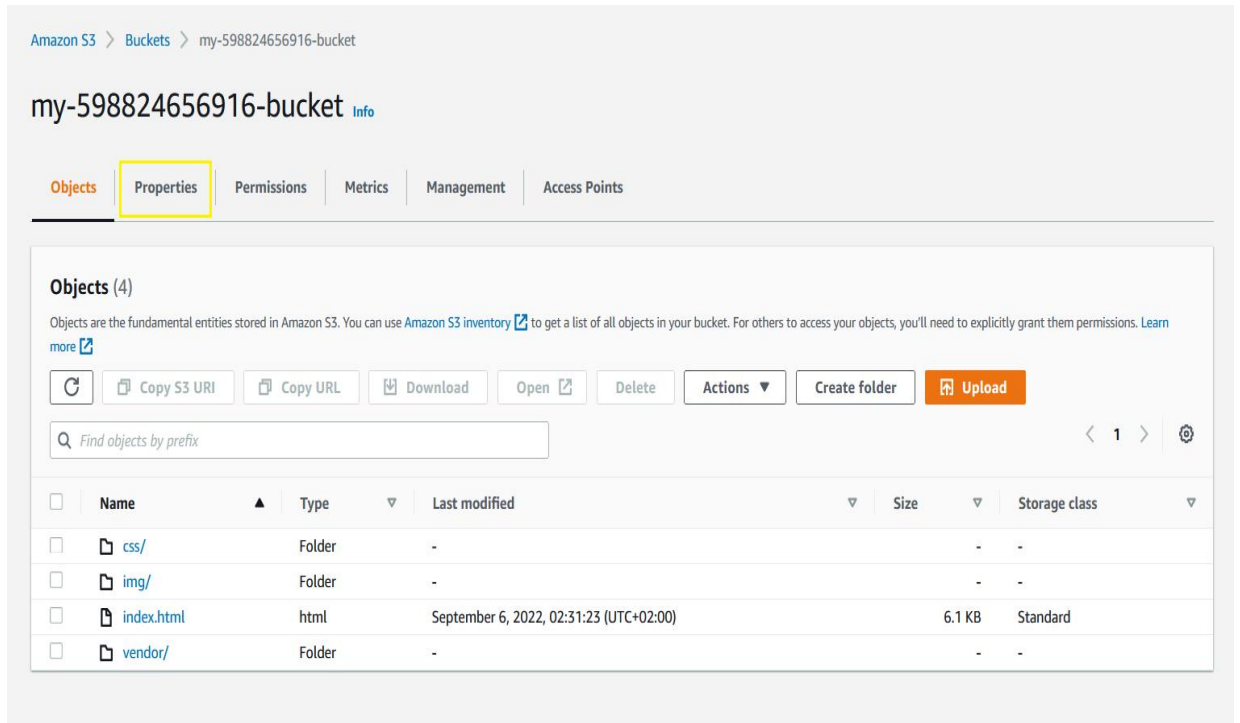
2. Click on the "Edit" button to see the Edit static website hosting screen.
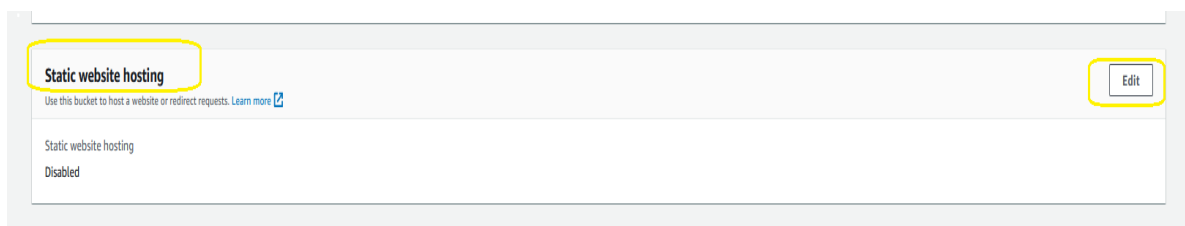
3. Now, enable the Static website hosting, and provide the default home page and error page for your website.

4. Check the **Static website hosting** section again under the **Properties** tab. You must now be able to view the website endpoint as shown below:
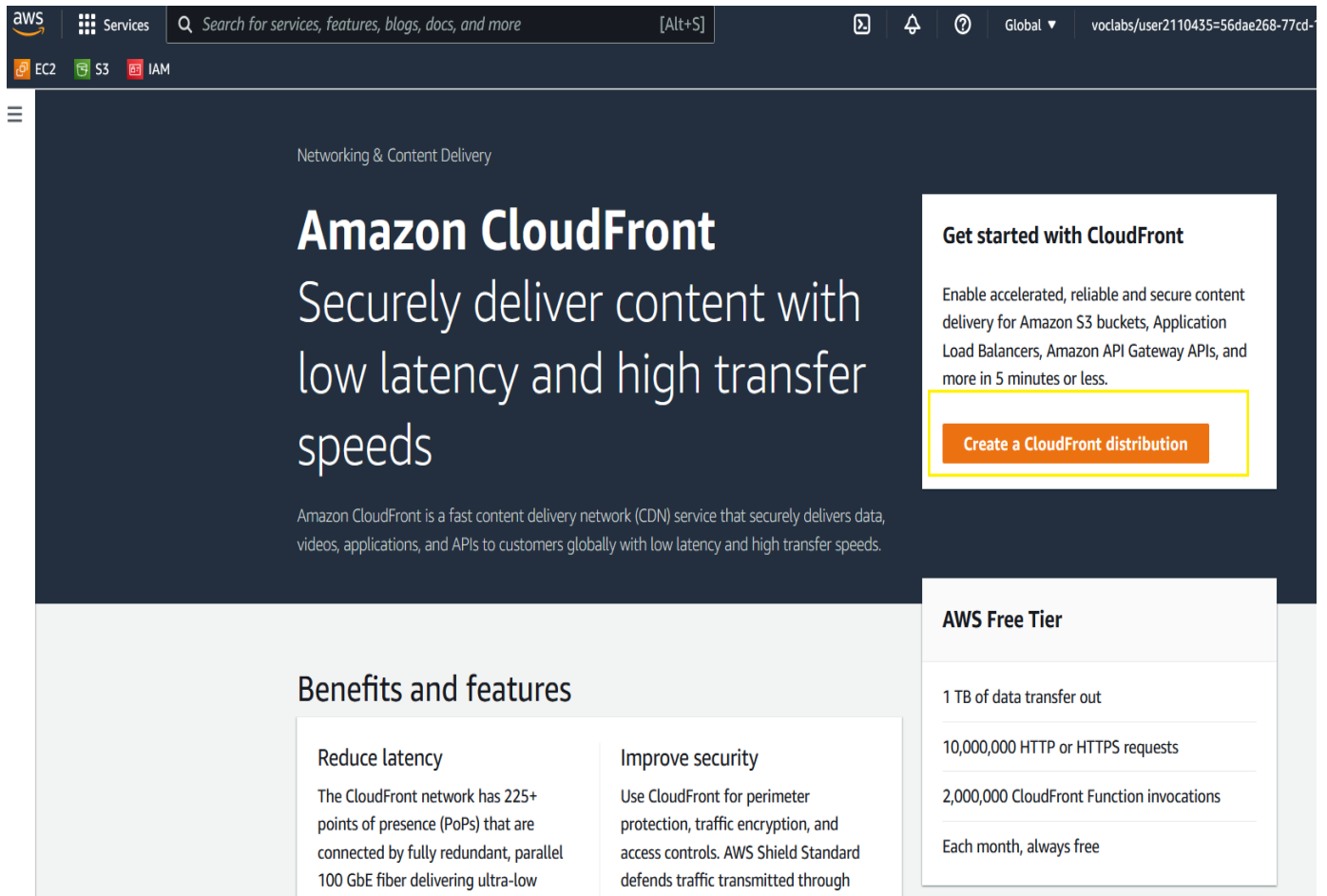

5. Copy the website endpoint for future use (WE GIT IT)

Udacity's School of Cloud Computing   HOME   ABOUT   POST   CONTACT

Travel Blog

Search destinations and book your hotel

The Most Popular Destinations for Solo Travelers

Here are the spots where you're most likely to meet other people who are traveling alone.

Posted by Jane Doe on September 24, 2019
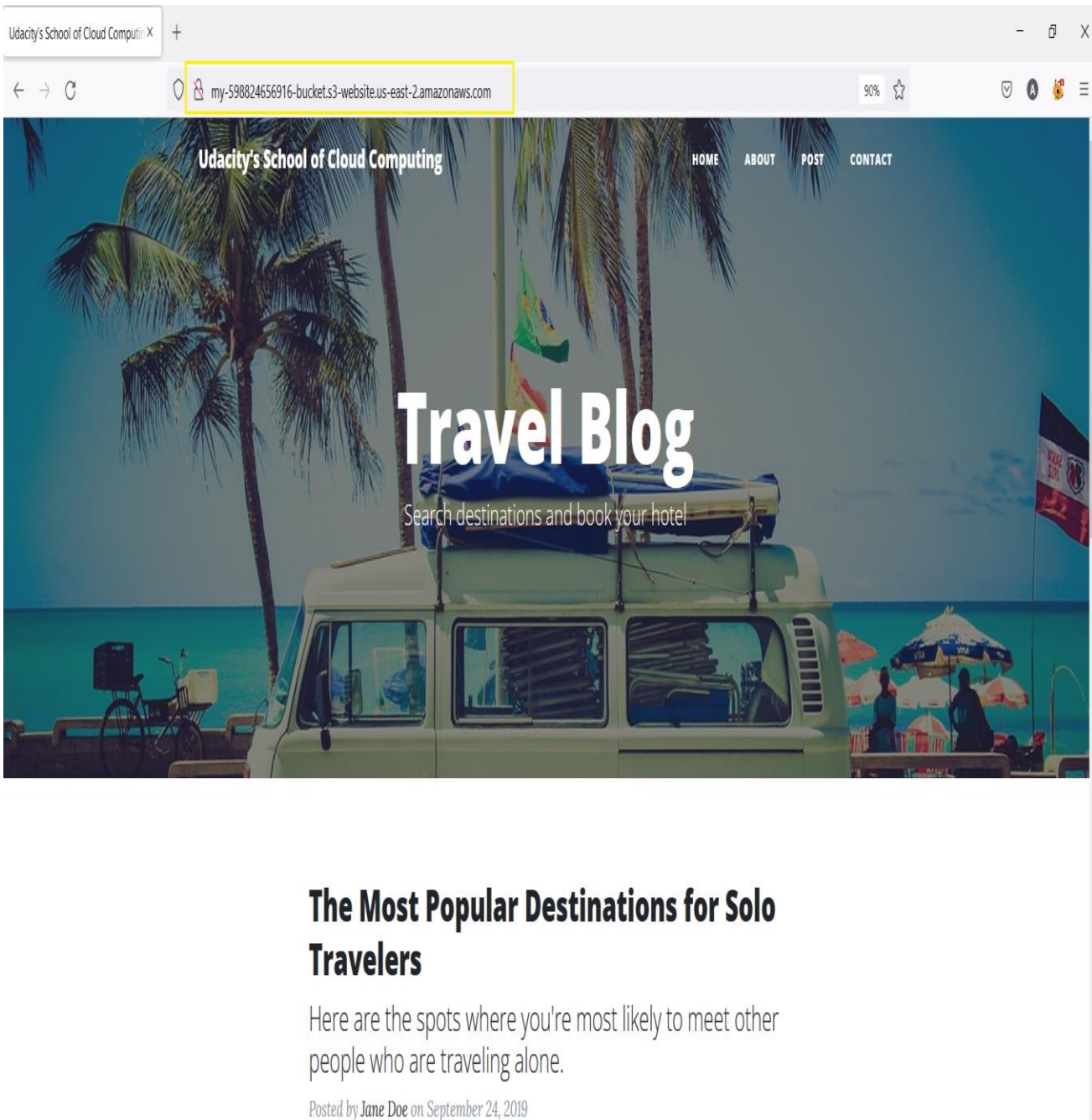
Distribute Website via CloudFront

1. Select "cloud front"

2. Click "Create Distribution".

3. Configure distribution

Create distribution

Origin

Don't select the bucket from the dropdown list. Paste the Static website hosting endpoint of the form http://my-598824656916-bucket.s3-website.us-east-2.amazonaws.com/

Origin domain

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

```
Q   my-598824656916-bucket.s3-website.us-east-2.amazonaws.com        X
```

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.

```
my-598824656916-bucket.s3-website.us-east-2.amazonaws.com
```

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

▶ Additional settings

Default cache behavior

Path pattern | Info

Default (*)

Compress objects automatically | Info

○ No
● Yes

Viewer

Viewer protocol policy

○ HTTP and HTTPS
● Redirect HTTP to HTTPS
○ HTTPS only

Allowed HTTP methods

● GET, HEAD
○ GET, HEAD, OPTIONS
○ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Restrict viewer access

If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content.

● No
○ 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

┌─ Cache policy
│   Choose an existing cache policy or create a new one.
│
│   ┌──┐ ┌──────┐
│   │ CachingOptimized   ▼ │ │ ⟳   │
│   │ Default policy when CF compression is enabled   │ └──────┘
│   └──┘
│
│   Create policy 🗗   View policy 🗗
│
└─ Origin request policy - *optional*
    Choose an existing origin request policy or create a new one.

5. Click distribution

Settings

Price class | Info
Choose the price class associated with the maximum price that you want to pay.

- ● Use all edge locations (best performance)
- ○ Use only North America and Europe
- ○ Use North America, Europe, Asia, Middle East, and Africa

AWS WAF web ACL - optional
Choose the web ACL in AWS WAF to associate with this distribution.

Choose web ACL ▼

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.

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

- ● Off
- ○ On

IPv6

- ○ Off
- ● On

Description - optional

Cancel   [**Create distribution**]

6. now all things is perfect distribution
7. get link cope and past in new tap

✓ NOW task DONE