

# Tutorial: S3 + CloudFront + CI/CD Pipeline

## Objective:

- Host a static website on **AWS S3**.
- Serve the website globally using **CloudFront CDN**.
- Automate deployment with **GitHub Actions** to sync updates from the repository to S3.
- Ensure the live site always displays the latest changes by automatically invalidating the **CloudFront cache** after each update.

## Create a basic s3 bucket

The screenshot shows the AWS S3 Bucket Properties page for 'my-lab-site-karim'. The top navigation bar includes 'Amazon S3 > Buckets > my-lab-site-karim'. The main tabs are 'Objects', 'Metadata', 'Properties' (which is selected), 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Properties' tab has several sections: 'Bucket overview' (AWS Region: US East (N. Virginia) us-east-1, ARN: arn:aws:s3:::my-lab-site-karim, Creation date: August 30, 2025, 07:21:02 (UTC+05:45)), 'Bucket Versioning' (disabled), 'Multi-factor authentication (MFA) delete' (disabled), and 'Tags (0)' (no tags associated with this resource).

## Enable Static Hosting

## 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](#) 

 For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can 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](#) 

Upload a basic index.html

## 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 SDKs 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**.

### Files and folders (1 total, 233.0 B)

All files and folders in this table will be uploaded.

Find by name				
Name	Folder	Type	Size	Re
index.html	-	text/html	233 B	

## Destination Info

### Destination

[s3://my-lab-site-karim](#)

#### ► Destination details

Bucket settings that impact new objects stored in the specified destination.

#### ► Permissions

Grant public access and access to other AWS accounts.

# Create a CloudFront Distribution

ⓘ We've streamlined the process of creating a CloudFront distribution. Continue here and [let us know what you think](#). Or go to the previous [Create Distribution page](#).

- Step 1 **Get started**
- Step 2 **Specify origin**
- Step 3  Enable security
- Step 4  Review and create

## Get started

Connect your websites, apps, files, video streams, and other content to CloudFront. We optimize the performance, reliability, and security for you.

### Distribution options Info

#### Distribution name

Name will be stored as a tag on the resource. You can add a name, or more tags, later.

karim-site-dist

#### Description - optional

(Optional) Enter a description for this distribution.

#### Distribution type

Single website or app

Choose if each website or application will have a unique configuration.

Multi-tenant architecture - New

Choose when you have multiple domains that need to share configurations. This is a common architecture for SaaS providers.

### Custom domain Info

#### Domain - optional

Use your own custom domain with free HTTPS to provide a secure, friendly URL for your app. You can add a custom domain later if you do not have a Route 53 domain.

[Check domain](#)

CloudFront > Distributions > Create distribution

We've streamlined the process of creating a CloudFront distribution. Continue here and let us know what you think. Or go to the previous [Create Distribution page](#).

**Specify origin**

**Origin type**

Your origin is where your content (such as a website or app) lives. CloudFront works with AWS-based origins and origins hosted on other cloud providers.

- Amazon S3** Deliver static assets like files and images, statically generated websites or single page applications (SPA).
- Elastic Load Balancer** Deliver applications hosted behind ELB such as dynamic websites, web services, and APIs.
- API Gateway** Deliver API endpoints for REST APIs hosted on API Gateway.
- Elemental MediaPackage** Deliver end-to-end live events or video on demand (VOD).
- VPC origin** Deliver applications and content hosted within private VPCs, such as EC2 Instances and Application Load Balancers.
- Other** Refer to any AWS or non-AWS origin through its publicly resolvable URL.

**Origin**

**S3 origin**  
Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

[Browse S3](#)

**Warning:** This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint. [Use website endpoint](#)

Do not enable security as of now.

CloudFront > Distributions > Create distribution

We've streamlined the process of creating a CloudFront distribution. Continue here and let us know what you think. Or go to the previous [Create Distribution page](#).

**Enable security**

**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.

[Cancel](#) [Previous](#) [Next](#)

CloudFront > Distributions > EEOBIIDO36LPL

Successfully created new distribution.

**karim-site-dist** Standard [View metrics](#)

[General](#) [Security](#) [Origins](#) [Behaviors](#) [Error pages](#) [Invalidations](#) [Tags](#) [Logging](#)

**Details**

Name karim-site-dist <a href="#">Edit</a>	Distribution domain name <a href="#">d44czrag1q862.cloudfront.net</a>	ARN <a href="#">arn:aws:cloudfront::729286129486:distribution/EEOBIIDO36LPL</a>	Last modified <a href="#">Deploying</a>
--	--	--	--

**Settings**

Description -	Alternate domain names <a href="#">Add domain</a>	Standard logging <a href="#">Off</a>
Price class Use all edge locations (best performance)		Cookie logging <a href="#">Off</a>
Supported HTTP versions HTTP/2, HTTP/1.1, HTTP/1.0		Default root object -

**Continuous deployment** [Info](#)

[Create staging distribution](#)

Edit the dist to add the root object (index.html)

The screenshot shows the 'Edit settings' page for a CloudFront distribution. The navigation bar at the top includes 'CloudFront' > 'Distributions' > 'E29NYDYBNLKM1E' > 'Edit settings'. The main section is titled 'Edit settings' and contains several configuration sections:

- Settings**
  - Anycast static IP list**: A note states 'Deliver traffic from a small set of IP addresses'. Below it says 'There are no Anycast static IP lists available' and a link to 'Create an Anycast static IP list'.
  - Price class** (radio buttons):
    - Use all edge locations (best performance)
    - Use only North America and Europe
    - Use North America, Europe, Asia, Middle East, and Africa
  - Alternate domain name (CNAME) - optional**: A note says 'Add the custom domain names that you use in URLs for the files served by this distribution.' A blue 'Add item' button is present.
  - Custom SSL certificate - optional**: A note says 'Associate a certificate from AWS Certificate Manager. The certificate must be in the US East (N. Virginia) Region (us-east-1).'
    - 'Choose certificate' dropdown.
    - 'Request certificate' button.
  - Supported HTTP versions**: A note says '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**: A note says 'The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.' The input field contains 'index.html'.
  - IPv6**: Radio buttons
    - Off
    - On
  - Description - optional**: A text input field.

Make sure that S3 has the correct policies to allows CDN to use the bucket.

The screenshot shows the 'Permissions' tab selected in the top navigation bar of the S3 bucket details page. Below it, the 'Permissions overview' section is visible, containing information about access findings and a link to learn more about IAM analyzer findings. The 'Block public access (bucket settings)' section is expanded, showing that 'Block all public access' is turned 'On'. A note indicates that public access is blocked because Block Public Access settings are turned on for this bucket. The 'Bucket policy' section displays a JSON policy document that grants CloudFront service principal permission to get objects from the bucket. The policy includes a condition that restricts access to objects where the CloudFront distribution's ARN matches the source ARN.

Amazon S3 > Buckets > my-lab-site-karim

**Amazon S3**

General purpose buckets

- Directory buckets
- Table buckets
- Vector buckets
- Access Grants
- Access Points (General Purpose Buckets, FSx file systems)
- Access Points (Directory Buckets)
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboard

**my-lab-site-karim** Info

Objects | Metadata | Properties | **Permissions** | Metrics | Management | Access

**Permissions overview**

**Access finding**

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)

[View analyzer for us-east-1](#)

**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 objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**

On

► 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](#)

**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](#)

```
{ "Version": "2008-10-17", "Id": "PolicyForCloudFrontPrivateContent", "Statement": [ { "Sid": "AllowCloudFrontServicePrincipal", "Effect": "Allow", "Principal": { "Service": "cloudfront.amazonaws.com" }, "Action": "s3:GetObject", "Resource": "arn:aws:s3:::my-lab-site-karim/*", "Condition": { "ArnLike": { "AWS:SourceArn": "arn:aws:cloudfront::729286129486:distribution/E29NYDYBNLKM1E" } } } ] }
```

**Edit** **Delete** **Copy**

If s3 doesn't have correct policies, we can copy the policies from CloudFront → Distributions → <DistributionName> → Edit origin

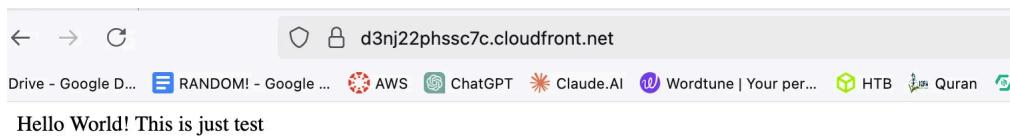
The screenshot shows the 'Edit origin' configuration page for a CloudFront distribution. The left sidebar lists navigation options: CloudFront, Distributions (selected), Policies, Functions, Static IPs, VPC origins, What's new, SaaS (Multi-tenant distributions, Distribution tenants), Telemetry (Monitoring, Alarms, Logs), and Reports & analytics (Cache statistics). The main content area is titled 'Edit origin' and contains several sections:

- Settings**:
  - Origin domain**: A search bar containing 'my-lab-site-karim.s3.us-east-1.amazonaws.com' with a clear button (X) and a note below it: "Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID."
  - A warning message: "⚠️ This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint." with a "Use website endpoint" button.
- Origin path - optional**: A text input field with placeholder text "Enter the origin path".
- Name**: A text input field containing "my-lab-site-karim.s3.us-east-1.amazonaws.com-mexlmnh3iuq".
- 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**: A dropdown menu showing "oac-my-lab-site-karim.s3.us-east-1.amazonaws.com-mexln3q1zc3" with a "Create new OAC" button.
- Policy statement**: A note: " ⓘ You must allow access to CloudFront using this policy statement. Learn more about giving CloudFront permission to access the S3 bucket." with a "Copy policy" button and a link to "Go to S3 bucket permissions".
- Add custom header - optional**: A note: "CloudFront includes this header in all requests that it sends to your origin." with a "Add header" button.
- Enable Origin Shield**: A button.

Copy the policy and paste it in s3 permissions.

Website is ready.

Using the Distribution domain name, we can access the website hosted on s3



## Using github actions to deploy a website from github repo diestctl to s3 bucket.

Create AWS\_ACCESS\_KEY\_ID and AWS\_SECRET\_ACCESS\_KEY using the aws provided accesskey and secretkey

The screenshot shows the GitHub repository settings for 'my-s3-lab'. The 'Actions secrets and variables' section is open. On the left sidebar, under 'Secrets and variables', the 'Actions' tab is selected. In the main area, there are two environment secrets listed:

Name	Last updated
AWS_ACCESS_KEY_ID	now
AWS_SECRET_ACCESS_KEY	now

## Create github actions workflow

The screenshot shows a GitHub repository named 'my-s3-lab'. The 'Code' tab is selected, displaying the contents of the 'main.yml' file under the '.github/workflows' directory. The code in the file is a GitHub Actions workflow for deploying a static website to AWS S3.

```

name: Deploy to AWS S3
on:
  push:
    branches:
      - main
jobs:
  deploy:
    runs-on: ubuntu-latest
    steps:
      - name: Checkout
        uses: actions/checkout@v3
      - name: Configure AWS Credentials
        uses: aws-actions/configure-aws-credentials@v2
        with:
          aws-access-key-id: ${{ secrets.AWS_ACCESS_KEY_ID }}
          aws-secret-access-key: ${{ secrets.AWS_SECRET_ACCESS_KEY }}
          aws-region: us-east-1
      - name: Deploy static site to S3 bucket
        run: |
          aws s3 sync ./public/my-lab-site-karim --recursive --exclude "*" --include ".git/*"
          aws s3 rm s3://my-lab-site-karim --recursive --exclude "*" --include ".github/*"
          aws s3 rm s3://my-lab-site-karim --recursive --exclude "*" --include ".DS_Store"
      - name: Invalidate CloudFront cache
        run: |
          aws cloudfront create-invalidation \
            --distribution-id E29WVYDYNLNUKME \
            --paths "/a"

```

**name:** Deploy to AWS S3

**on:**

**push:**

**branches:**

- main

**jobs:**

**deploy:**

**runs-on:** ubuntu-latest

**steps:**

- name: Checkout

uses: actions/checkout@v3

- name: Configure AWS Credentials

uses: aws-actions/configure-aws-credentials@v2

**with:**

- aws-access-key-id: \${{ secrets.AWS\_ACCESS\_KEY\_ID }}

- aws-secret-access-key: \${{ secrets.AWS\_SECRET\_ACCESS\_KEY }}

- aws-region: us-east-1

```

# --- One-time cleanup step ---
- name: Clean up old junk files in S3
  run: |
    aws s3 rm s3://my-lab-site-karim --recursive --exclude "*" --include ".git/*"
    aws s3 rm s3://my-lab-site-karim --recursive --exclude "*" --include ".github/*"
    aws s3 rm s3://my-lab-site-karim --recursive --exclude "*" --include ".DS_Store"

- name: Deploy static site to S3 bucket
  run: |
    aws s3 sync ./ s3://my-lab-site-karim --delete \
    --exclude ".git/*" \
    --exclude ".github/*" \
    --exclude ".DS_Store"

- name: Invalidate CloudFront cache
  run: |
    aws cloudfront create-invalidation \
    --distribution-id E29NYDYBNLKM1E \
    --paths "/*"

```

This workflow automatically deploys your static website to AWS S3 whenever you push to the `main` branch. It first checks out your GitHub repository and configures AWS credentials so it can access your S3 bucket and CloudFront distribution. Then it performs a one-time cleanup to remove old unnecessary files like `.git`, `.github`, and `.DS_Store` from the S3 bucket. After that, it syncs your local website files to S3, making sure only the actual site files are uploaded and any removed files are deleted from the bucket. Finally, it invalidates the CloudFront cache so that visitors immediately see the updated content.

Workflow has been completed.

The screenshot shows the GitHub Actions interface. In the top navigation bar, there are links for Code, Issues, Pull requests, Actions (which is highlighted), Projects, Wiki, Security, Insights, and Settings. The main area is titled "Actions" and has a sub-section "Deploy to AWS S3". On the right, there's a search bar for "Workflow runs" and a filter for "main.yml". Below this, it says "1 workflow run" and lists a single run: "Create main.yml" (status: green, event: Deploy to AWS S3 #1, commit: 76f69f6 pushed by KarimShahid, branch: main, timestamp: 5 minutes ago, duration: 13s). There are dropdown menus for Event, Status, Branch, and Actor.

New Site is ready.

The website for "Café Al Karim" is displayed. The header features the cafe's name in a large, stylized font. Below the header are two images: one showing a variety of pastries like croissants and swirl buns, and another showing a display case filled with various cakes and tarts. A descriptive paragraph below the images reads: "The Café offers an assortment of delicious and delectable pastries and coffees that will put a smile on your face. From cookies to croissants, tarts and cakes, each treat is specially prepared to excite your tastebuds and brighten your day!" At the bottom, there are three callout boxes: one for "Frank bakes a rich variety of cookies. Try them all!" showing several types of cookies; one for "Tea Coffee Latte Hot Chocolate Yes, we" showing a cup of coffee with chocolate sauce; and one for "Our tarts are always a customer favorite!" showing several small tarts topped with strawberries and berries.