

# Configuring a Static Website With S3 And CloudFront

This type of site is called a static website and is used to display content that does not change frequently

- During this hands-on, I will host a static website using the Amazon Simple Storage S3 To do that, I'll store a website files on Amazon S3 and also use S3 to deliver the content to visitors to the website.
- After setting up the static website on S3, I will use Amazon CloudFront to create a content delivery network (CDN). A CDN makes the website content available from data centers around the world, called edge locations. Using edge locations improves the speed of the website by reducing latency. Doing so is especially important for the website displays large media files such as high-resolution images, audio, or video.

## **Hands-on steps:**

- Creating an Amazon S3 Bucket for a Static Website
- Uploading a Static Site to an Amazon S3 Bucket
- Creating an Amazon CloudFront Distribution for the Static Website

### *Creating an Amazon S3 Bucket for a Static Website*

1. In the AWS Management Console search bar, enter S3, and click the S3 result under Services
2. To start creating a new Amazon S3 bucket, in the top-right, click Create bucket
3. Under General configuration, enter the following:
4. Region: Ensure US West (Oregon) us-west-2 is selected
5. Bucket name: calabs-bucket-333
6. Make sure to select ACLs Enabled
7. In the Block Public Access section, un-check the Block all public access check box
8. To finish creating your Amazon S3 bucket, scroll to the bottom of the form and click Create bucket
9. In the list, click the name of your bucket
10. In the row of tabs under Bucket overview, click Properties
11. Scroll to the bottom of the Properties page and in the Static website hosting section, on the right, click Edit
12. In the Static website hosting field, select Enable
13. Enter the following, leaving all other fields at their defaults:
- 14.
15. Index document: Enter index.html
16. Error document: Enter error/index.html
17. To finish enabling static website hosting, scroll to the bottom, and click Save changes

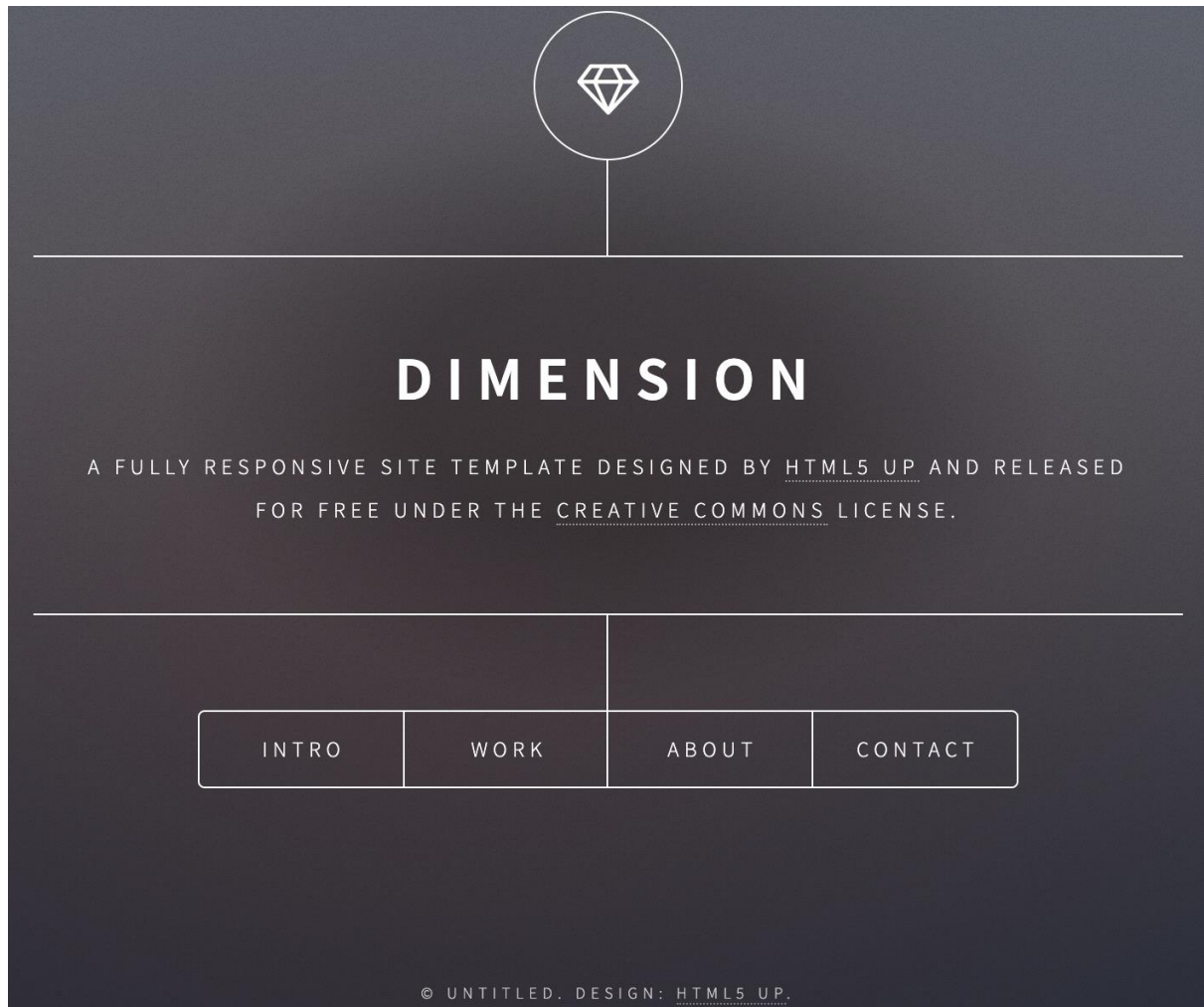
- *Uploading a Static Site to an Amazon S3 Bucket:*

1. In the Amazon S3 console, in the row of tabs, click Permissions
2. Scroll down to the Bucket policy section, and on the right, click Edit.
3. In the Policy editor, copy and paste the following

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddPerm",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::calabs-bucket-333/*"  
    }  
  ]  
}
```

- This policy will allow public access to all objects in your S3 bucket
  - Next, you will download a basic website from a public GitHub repository and load it into your S3 bucket, This is an example website
4. In the row of tabs, click Objects.
  5. To begin uploading the website to your Amazon S3 bucket, scroll down and click Upload
  6. In the Files and folders section, click Add files

7. To retrieve the endpoint for your bucket, click the Properties tab, scroll to the bottom, and click the copy icon next to the Bucket website endpoint



## *Creating an Amazon CloudFront Distribution for the Static Website*

In this step, I will set up an Amazon CloudFront distribution for my static site hosted in your Amazon S3 bucket, update the bucket policy to allow access to the CloudFront distribution, and update permissions to block public access to the S3 bucket

1. In the AWS Management Console search bar, enter CloudFront, and click the CloudFront result under Services
2. To start creating a distribution, click Create a CloudFront Distribution
3. Under Origin, in the Origin Domain text-box, enter the Amazon S3 static website hosting endpoint that I created earlier
4. Under Origin, in the Origin access, select Origin access control settings and click Create control setting
5. Under Create control setting, enter the following values:

Name: Enter calabs-s3cf-`<UniqueNumber>` (Append a unique number to the end of calabs-s3cf-)

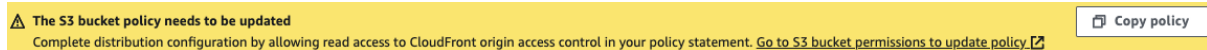
Signing behavior: Ensure Sign requests is selected

5. Select Do not enable security protections under Web Application Firewall (WAF)
6. Scroll down to Settings, and in the Price class selection, select Use only North America and Europe
7. In the Default root object field, enter index.html

8. To finish configuring your distribution, at the bottom of the page, click Create distribution

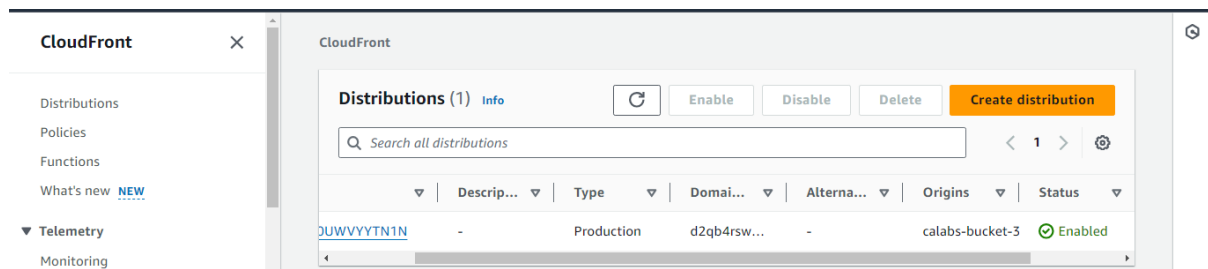
CloudFront automatically assigns an ID (top of the page) and a Distribution domain name to the distribution and starts updating the edge locations to serve your content

9. Click Copy policy at the top of the page

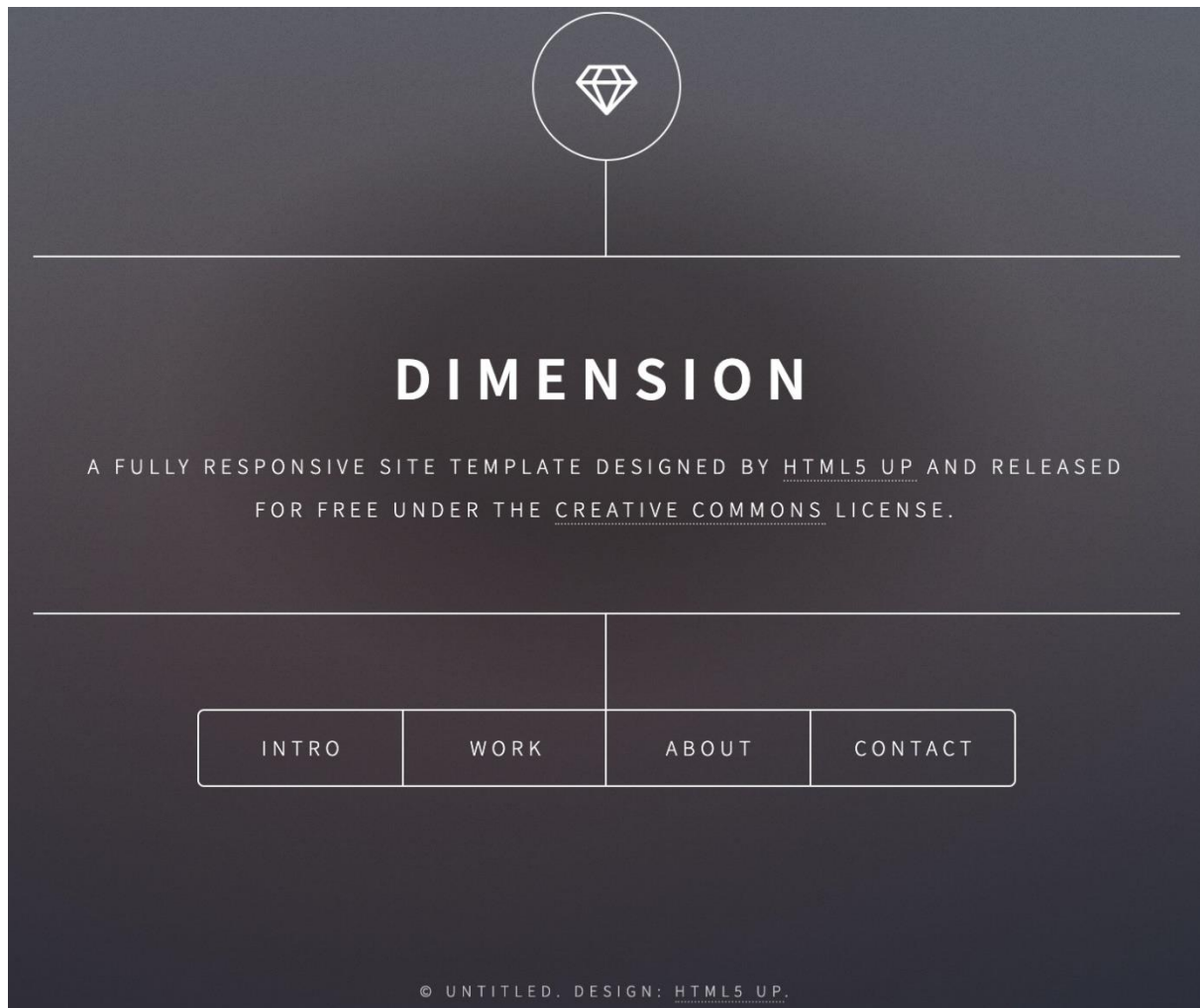


This policy provides a new bucket policy that provides the s3:GetObject permission to the distribution. This allows for blocking all public access to the S3 bucket while maintaining access to the website via the distribution.

10. To implement the policy, return to the bucket you created, click the Permissions tab, scroll down to the Bucket policy section, click Edit, paste the policy you copied, and click Save changes
11. Under the Block public access (bucket settings) section click Edit, select the Block all public access box, click Save changes, enter confirm into the field, and click Confirm
12. Return to the CloudFront Distributions table
13. Copy the value of the Distribution Domain Name field



14. Paste the domain name into the address bar of a new browser tab.



### Summary:

In this hands-on I created an Amazon S3 bucket and used it to host a static website. I created an Amazon CloudFront distribution and configured it to use your S3 bucket as an origin. I tested that I could access the static website directly through Amazon S3, and through your Amazon CloudFront distribution. I updated the S3 bucket policy to restrict access to only the CloudFront distribution and blocked all public access to the S3 bucket