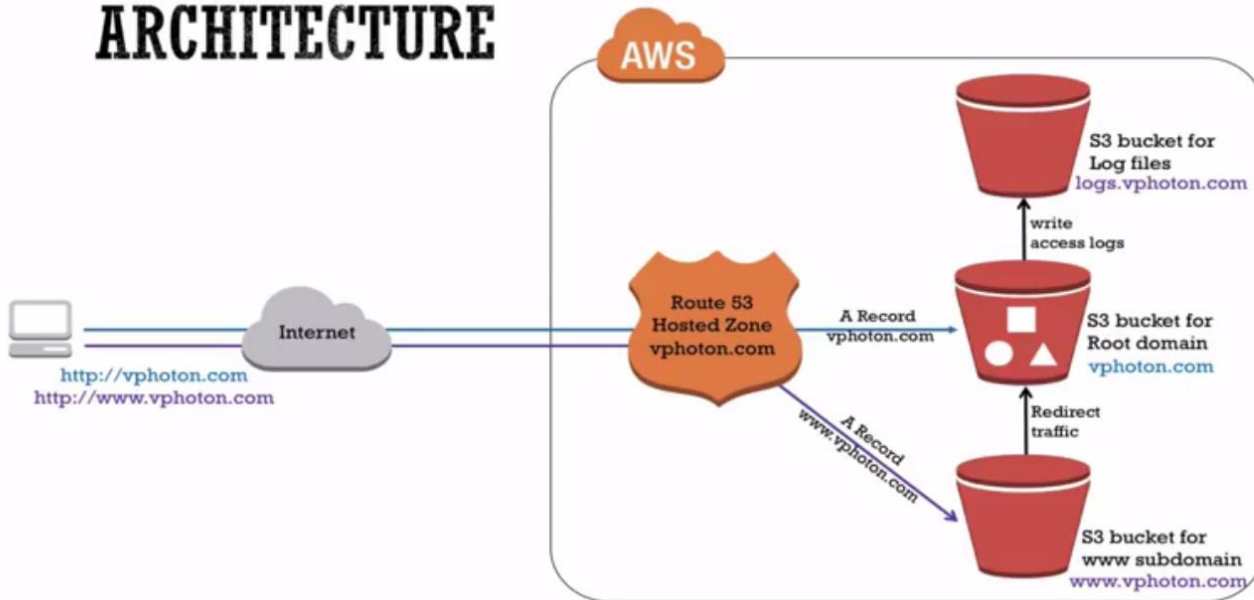


AWS — HOW TO CONFIGURE CLOUDFRONT FOR S3 BUCKET

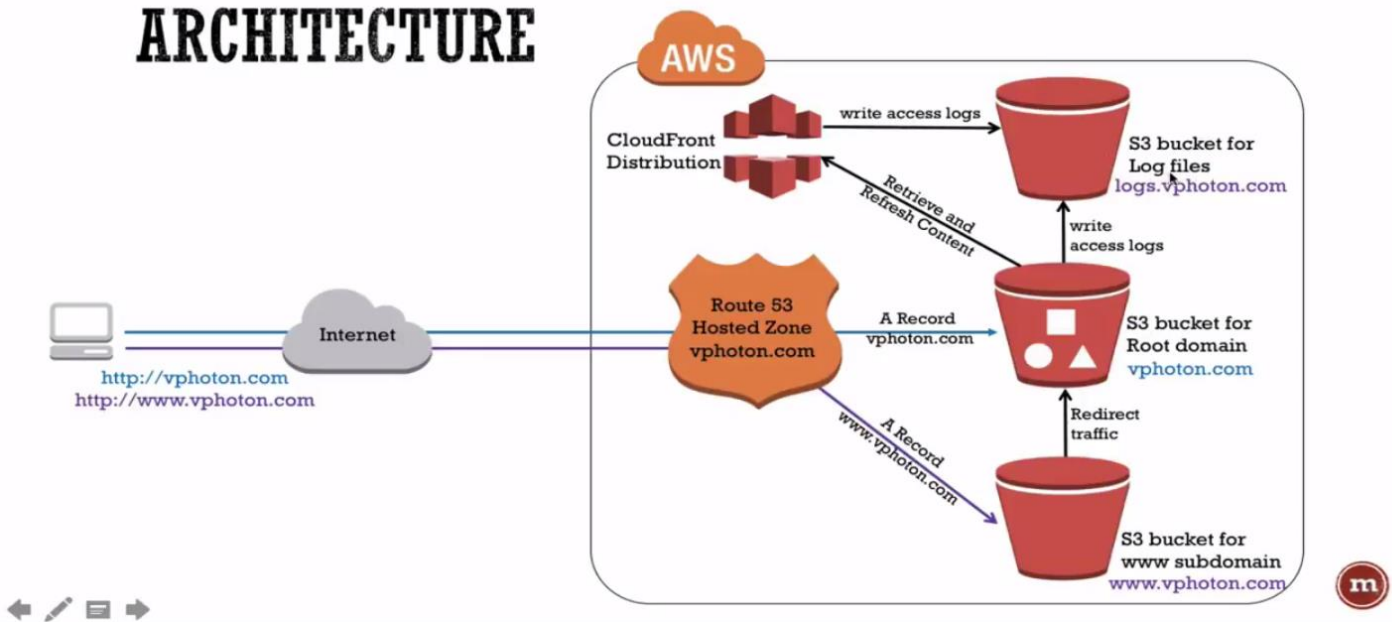


My Blog: <http://myvirtualbytes.com>

ARCHITECTURE



ARCHITECTURE



CLOUDFRONT SETUP

- Delivery Method = **Web**
- Origin Domain = **S3 bucket** → `vphoton.com.s3.amazonaws.com`
- Restrict Bucket Access = **Yes**
- Origin Access Identity = **New**
- Grant Read Permissions on Bucket = **Yes, update**
- Viewer Protocol Policy = **HTTPS**
- Restrict Viewer Access (Use Signed URLs or Signed Cookies) = **No**
- Alternate Domain Names (CNAMEs) = `www.vphoton.com`, `vphoton.com`
- Default Root Object = `index.html`
- Logging = **Yes**
- Bucket for Logs = `logs.vphoton.com` ; Log Prefix = `cdn/`



https://console.aws.amazon.com/console/home?region=us-east-1

Services Resource Groups

myadmin @ atechologyguru N. Virginia Support

AWS services

Find a service by name (for example, EC2, S3, Elastic Beanstalk).

Recently visited services

- S3
- CloudFront
- IAM
- Route 53

All services

Build a solution

Get started with simple wizards and automated workflows.

- Launch a virtual machine
With EC2
~1 minute
- Build a web app
With Elastic Beanstalk
~6 minutes
- Deploy a serverless microservice
With Lambda, API Gateway
~2 minutes
- Host a static website
With S3, CloudFront, Route 53
~5 minutes
- Create a backend for your mobile app
With Mobile Hub
~5 minutes
- Register a domain
With Route 53
~3 minutes

Featured next steps

- Manage your costs
Get real-time billing alerts based on your cost and usage budgets. [Start now](#)
- Get best practices
Use AWS Trusted Advisor for security, performance, cost and availability best practices. [Start now](#)

What's new?

Announcing AWS Batch
Now generally available, AWS Batch enables developers, scientists, and engineers to process large-scale batch jobs with ease. [Learn more](#)

Announcing Amazon Lightsail
See how this new service allows you to launch and manage your VPS with AWS for a low, predictable price. [Learn more](#)

[See all](#)

https://console.aws.amazon.com/s3/home?region=us-east-1

Services Resource Groups

myadmin @ atechologyguru Global Support

Create Bucket Actions

All Buckets (4)

Name
atechnologyguru
logs.vphoton.com
vphoton.com
www.vphoton.com

None Properties Transfers

Announcement: Object Tagging and new Storage Management features available in new console. [Opt in](#) to try object tagging and storage management.

Announcement: Load data up to 300% faster with S3 Transfer Acceleration. [Test it here](#).

https://console.aws.amazon.com/cloudfront/home?region=us-east-1

Services Resource Groups

myadmin @ atechologyguru Global Support

CloudFront Distributions

Create Distribution Distribution Settings Delete Enable Disable

Viewing: Any Delivery Method Any State

Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
Web	E292HUERJ2633S	d2a9kac5280l5b.clo	-	vphoton.com	vphoton.com, v	Deployed	Enabled	2017-03-10 14:56 U

What's New

Reports & Analytics

- Cache Statistics
- Monitoring and Alarms
- Popular Objects
- Top Referrers
- Usage
- Viewers

We already have a distribution called Web that is already deployed. Let us create a new one again

Step 1: Select delivery method

Step 2: Create distribution

Select a delivery method for your content.

Web

Create a web distribution if you want to:

- Speed up distribution of static and dynamic content, for example, .html, .css, .php, and graphics files.
- Distribute media files using HTTP or HTTPS.
- Add, update, or delete objects, and submit data from web forms.
- Use live streaming to stream an event in real time.

You store your files in an origin - either an Amazon S3 bucket or a web server. After you create the distribution, you can add more origins to the distribution.

Get Started

RTMP

Create an RTMP distribution to speed up distribution of your streaming media files using Adobe Flash Media Server's RTMP protocol. An RTMP distribution allows an end user to begin playing a media file before the file has finished downloading from a CloudFront edge location. Note the following:

- To create an RTMP distribution, you must store the media files in an Amazon S3 bucket.
- To use CloudFront live streaming, create a web distribution.

Get Started

Cancel

Step 1: Select delivery method

Step 2: Create distribution

Create Distribution

Origin Settings

Origin Domain Name

vphoton.com.s3.amazonaws.com

Origin Path

Origin ID

S3-vphoton.com

Restrict Bucket Access

Yes

No

Origin Access Identity

Create a New Identity

Use an Existing Identity

Comment

access-identity-vphoton.com.s3.amazor

Grant Read Permissions on Bucket

Yes, Update Bucket Policy

No, I Will Update Permissions

Origin Custom Headers

Header Name

Value

Default Cache Behavior Settings

Path Pattern

Default (*)

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

docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

Search

English

Sign In to the Console

Menu

amazon web services

Working with Distributions

Working with Web Distributions

Using CloudFront with Lambda@Edge

Working with RTMP Distributions

Working with Objects

Request and Response Behavior

Serving Private Content through CloudFront

Task List: Serving Private Content

Using an Origin Access Identity to Restrict Access to Your Amazon S3 Content

Specifying the AWS Accounts That Can Create Signed URLs and Signed Cookies (Trusted Signers)

Choosing Between Signed URLs and Signed Cookies

Using Signed URLs

Note

To create origin access identities, you must use the CloudFront console or CloudFront API version 2009-09-09 or later.

To ensure that your users access your objects using only CloudFront URLs, regardless of whether the URLs are signed, perform the following tasks:

1. Create an origin access identity, which is a special CloudFront user, and associate the origin access identity with your distribution. (For web distributions, you associate the origin access identity with origins, so you can secure all or just some of your Amazon S3 content.) You can also create an origin access identity and add it to your distribution when you create the distribution. For more information, see [Creating a CloudFront Origin Access Identity and Adding it to Your Distribution](#).

2. Change the permissions either on your Amazon S3 bucket or on the objects in your bucket so only the origin access identity has read permission (or read and download permission). When your users access your Amazon S3 objects through CloudFront, the CloudFront origin access identity gets the objects on your users' behalf. If your users request objects directly by using Amazon S3 URLs, they're denied access. The origin access identity has permission to access objects in your Amazon S3 bucket, but users don't. For more information, see [Granting the Origin Access Identity Permission to Read Objects in Your Amazon S3 Bucket](#).

PDF | Kindle

On this page:

Creating a CloudFront Origin Access Identity and Adding it to Your Distribution

Granting the Origin Access Identity Permission to Read Objects in Your Amazon S3 Bucket

Using an Origin Access Identity in Amazon S3 Regions that Support Only Signature Version 4 Authentication

https://console.aws.amazon.com/cloudfront/home?region=us-east-1#create-distribution:

Search

myadmin @ atechologyguru

Global

Support

Services

Resource Groups

Step 1: Select delivery method

Step 2: Create distribution

Grant Read Permissions on Bucket

☒ Yes, Update Bucket Policy

☐ No, I Will Update Permissions

Origin Custom Headers

Header Name

Value

Default Cache Behavior Settings

Path Pattern

Default (*)

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

Cached HTTP Methods

GET, HEAD (Cached by default)

Forward Headers

None (Improves Caching)

Object Caching

☒ Use Origin Cache Headers

☐ Customize

[Learn More](#)

Minimum TTL

0

Maximum TTL

31536000

Default TTL

86400

Forward Cookies

None (Improves Caching)

Query String Forwarding and

None (Improves Caching)

← ⓘ

https://console.aws.amazon.com/cloudfront/home?region=us-east-1#create-distribution:

☆ ⬇ 🏠 🔍

Services ▾ Resource Groups ▾ ⭐

myadmin @ atechologyguru ▾ Global ▾ Support ▾

Learn More

Step 1: Select delivery method

Step 2: Create distribution

Lambda Function Associations

Event Type

Lambda Function ARN

Distribution Settings

Price Class

Use All Edge Locations (Best Performance) ▾

ⓘ

AWS WAF Web ACL

None ▾

ⓘ

Alternate Domain Names (CNAMEs)

www.yphoton.com
yphoton.com

ⓘ

SSL Certificate

☒ Default CloudFront Certificate (*.cloudfront.net)

Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d1111111abcdcf8.cloudfront.net/logo.jpg).
Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

☐ Custom SSL Certificate (example.com):

Choose this option if you want your users to access your content by using an alternate domain name, such as https://www.example.com/logo.jpg.
You can use a certificate stored in AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.

No certificates available ▾

🔄

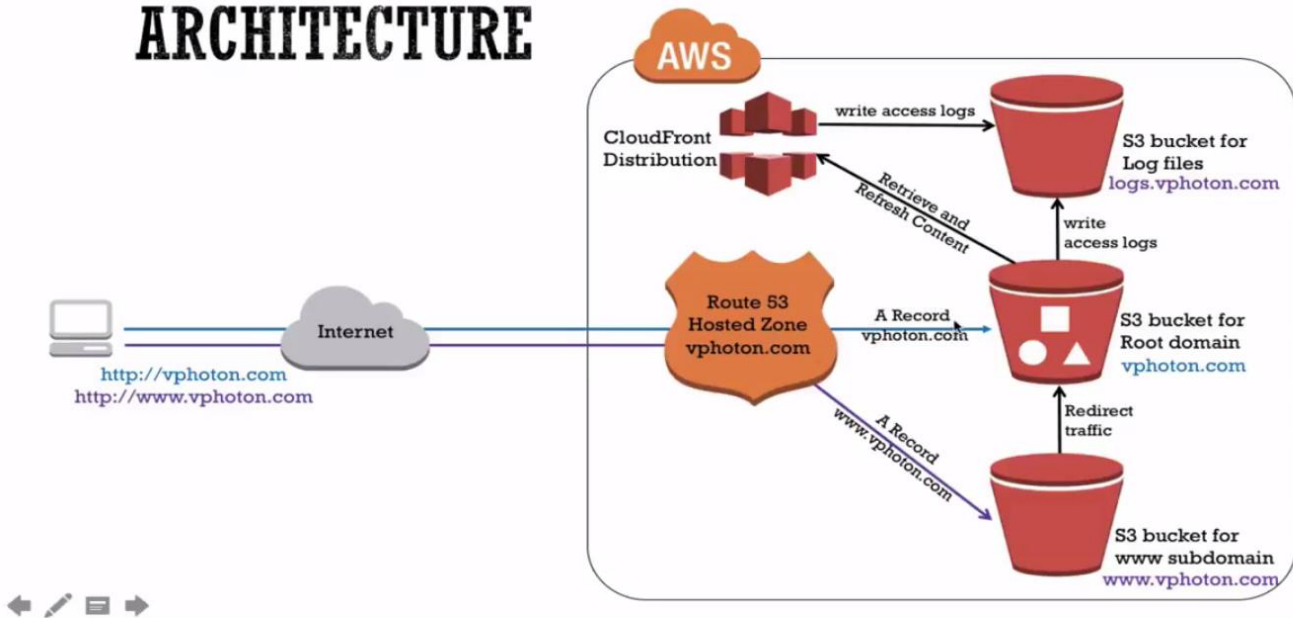
Request or Import a Certificate with ACM

[Learn more](#) about using custom SSL/TLS certificates with CloudFront.

[Learn more](#) about using ACM.

This will create that distribution for you, it will take about 15 – 20 minutes to create your distribution

ARCHITECTURE

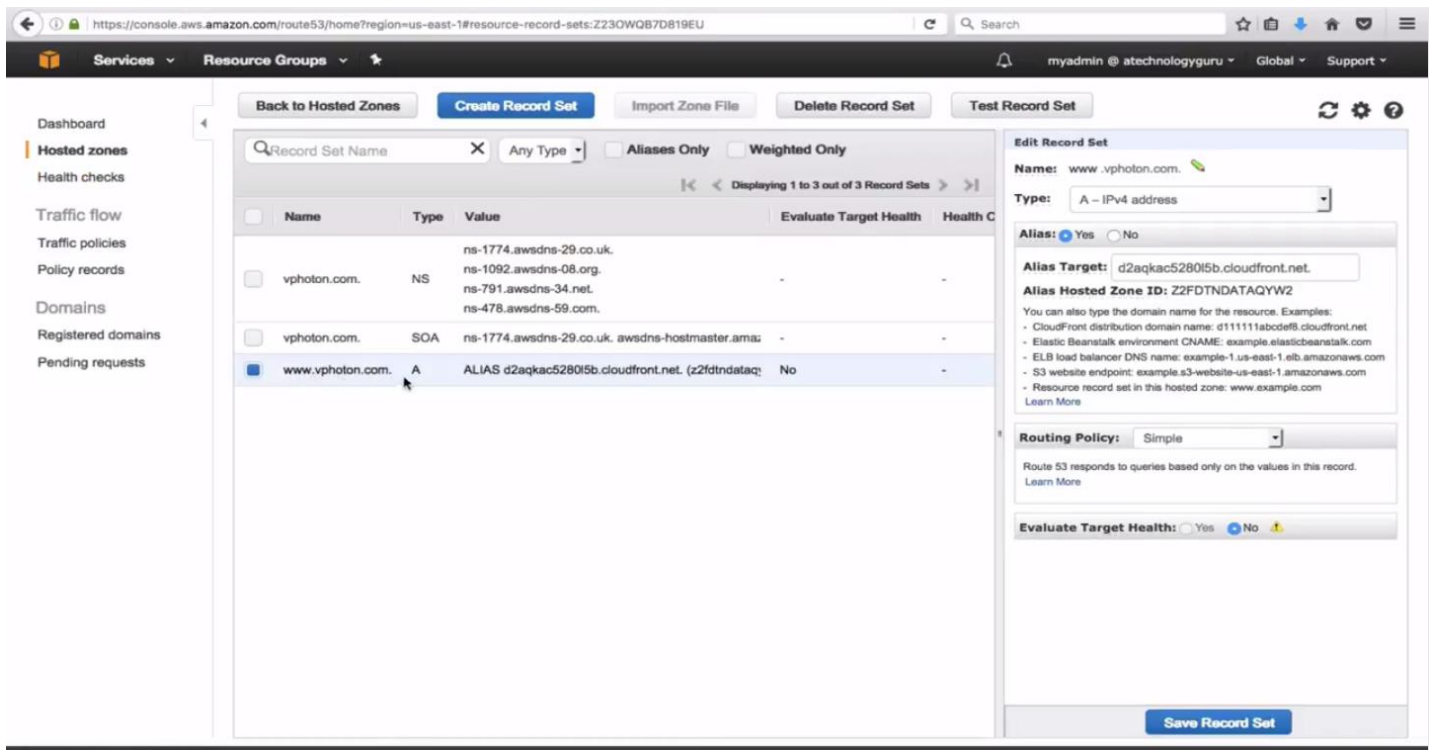


You now need to point your hosted zone to the CloudFront distribution instead of to your S3 bucket

The screenshot shows the AWS Route 53 console. The left sidebar includes links to Dashboard, Hosted zones, Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The main content area is titled 'DNS management' and shows '1 Hosted zones'. Below this, there is a 'Register domain' section with a text input for 'Type a domain name', a dropdown for '.com - \$12.00', and a 'Check' button. To the right, there are sections for 'Traffic management', 'Availability monitoring', and 'Domain registration'. At the bottom right, there is a 'Service health' section showing 'Amazon Route 53 Service is operating normally.'

The screenshot shows the 'Create Hosted Zone' page in the AWS Route 53 console. The left sidebar is the same as the previous screenshot. The main content area has buttons for 'Create Hosted Zone', 'Go to Record Sets', and 'Delete Hosted Zone'. Below these is a search bar and a table listing the hosted zones. The table has columns for 'Domain Name', 'Type', 'Record Set Count', 'Comment', and 'Hosted Zone ID'. There is one entry for 'vphoton.com.' with a 'Public' type and 3 record sets.

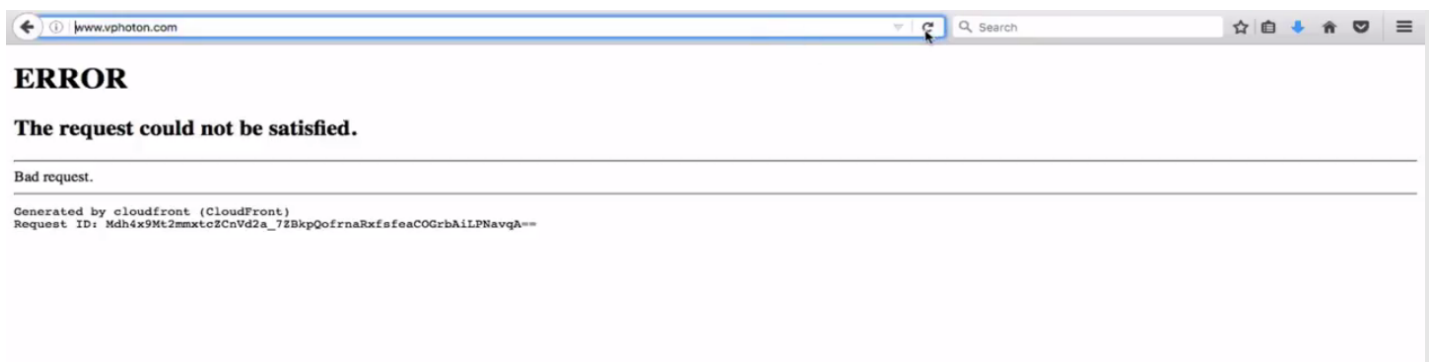
Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
vphoton.com.	Public	3		Z23OWQB7D819EU



The A Record for your site should now be pointing to that CloudFront distribution endpoint as above.



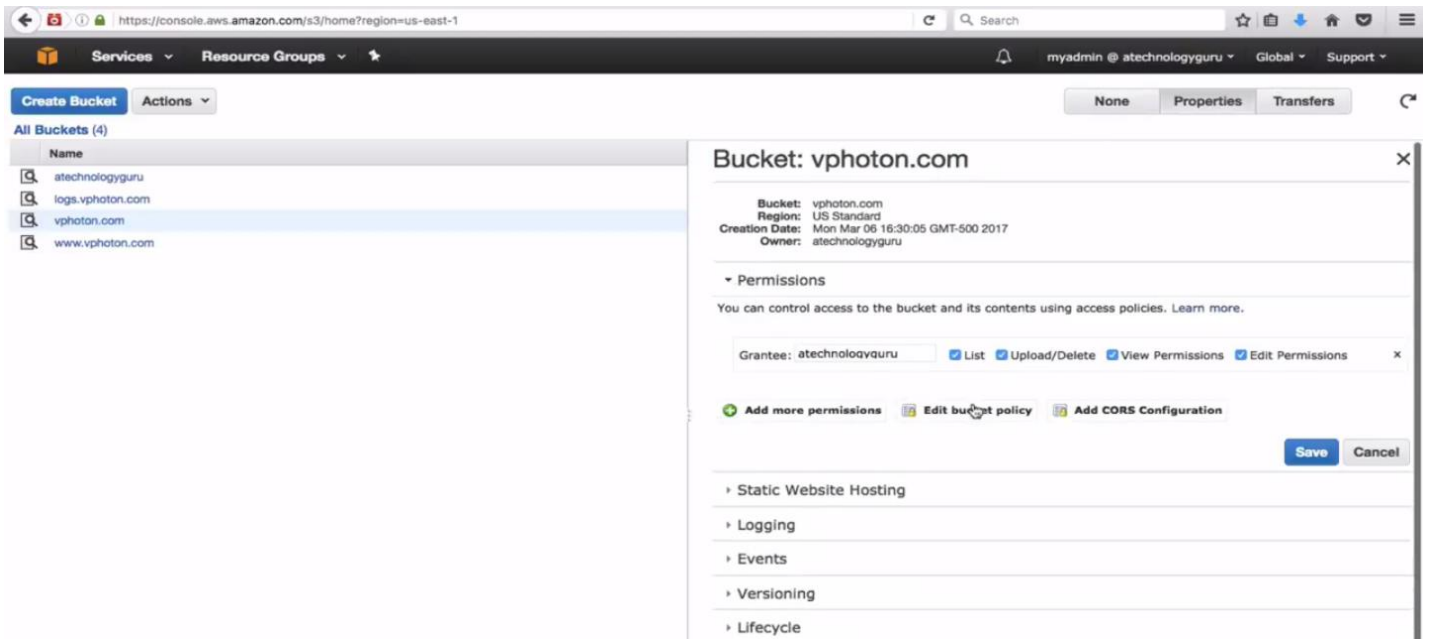
You can no longer go directly to your S3 bucket anymore

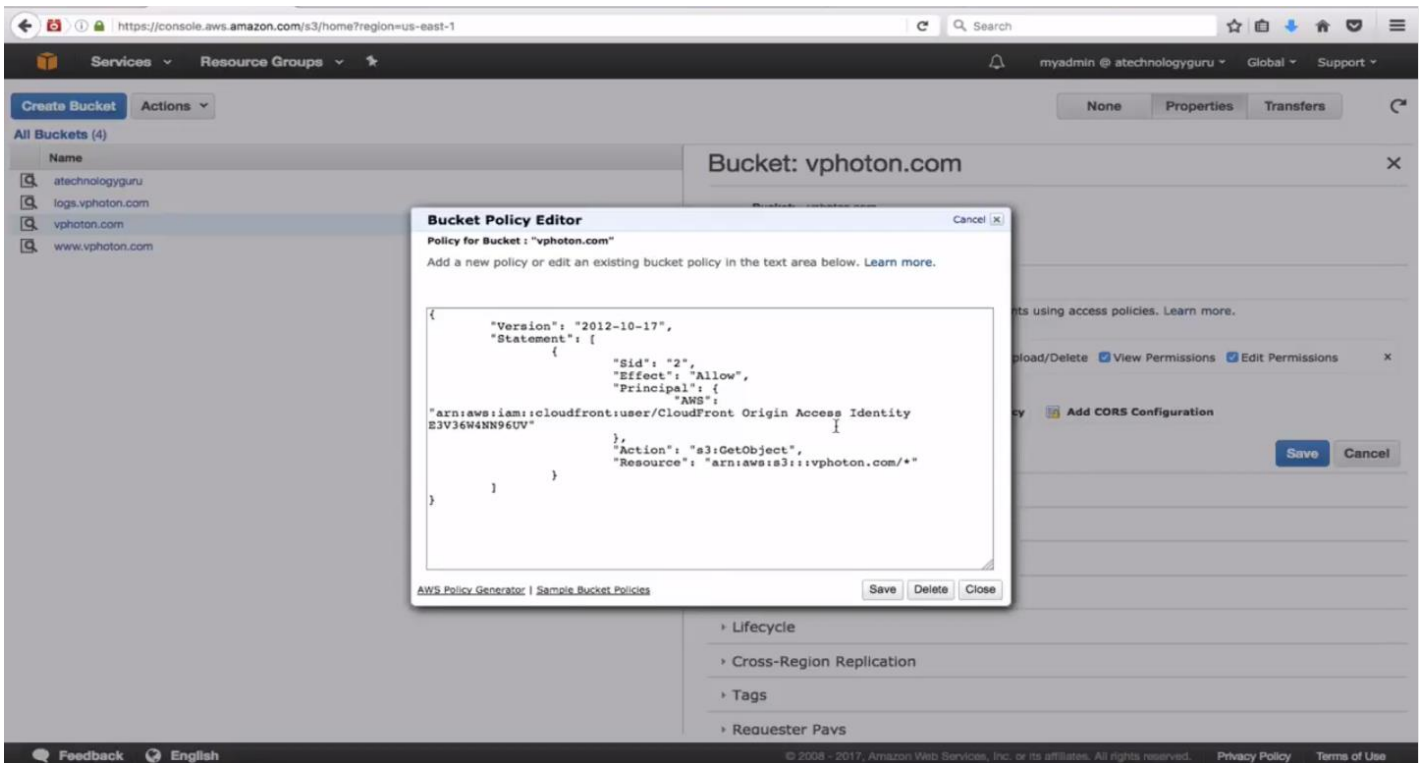


The HTTP protocol is not working anymore as above

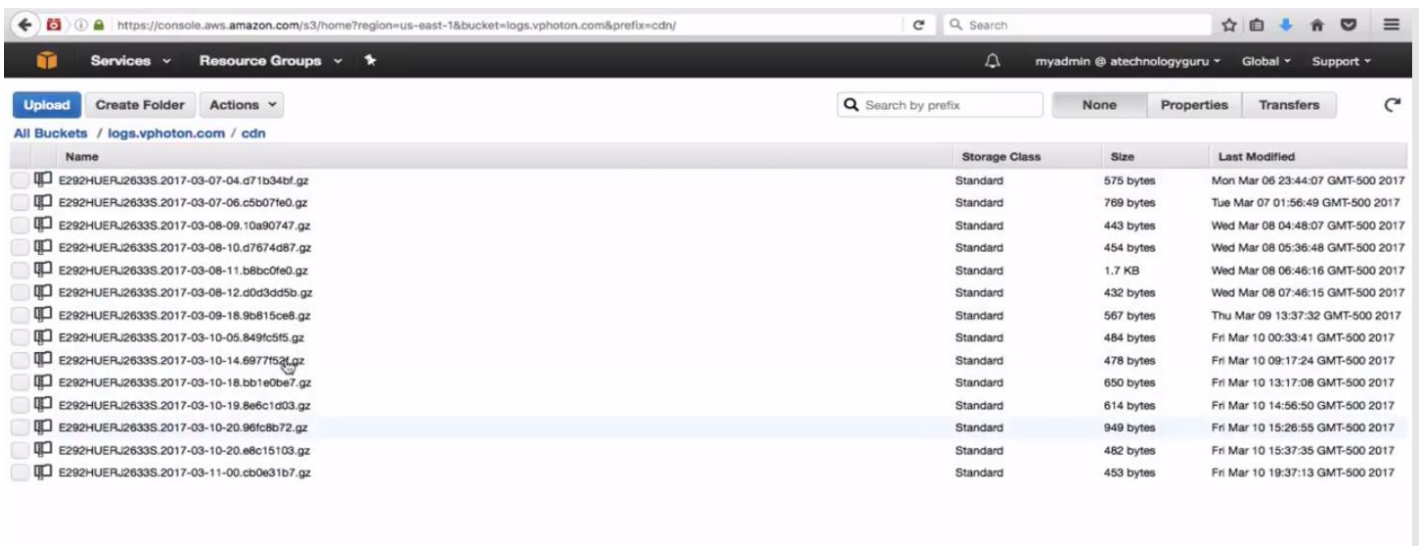


The HTTPS now works fine and we can see our site show up





This is the bucket policy created for us by the special CloudFront user



Here is the logs S3 bucket