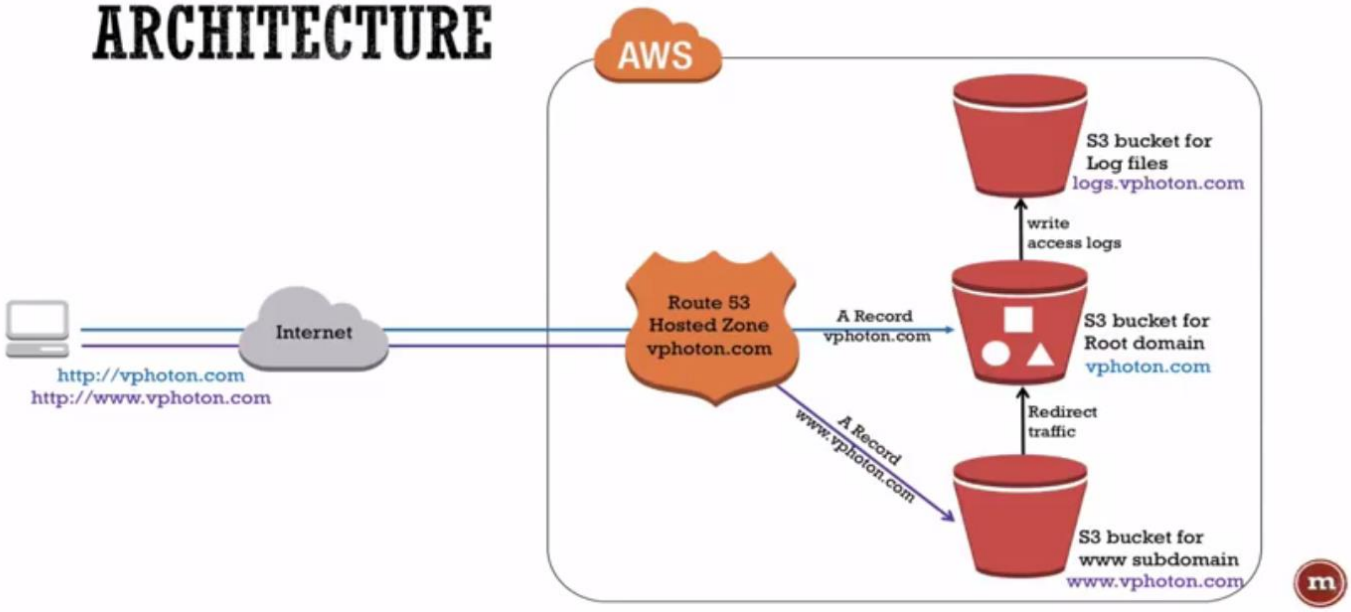
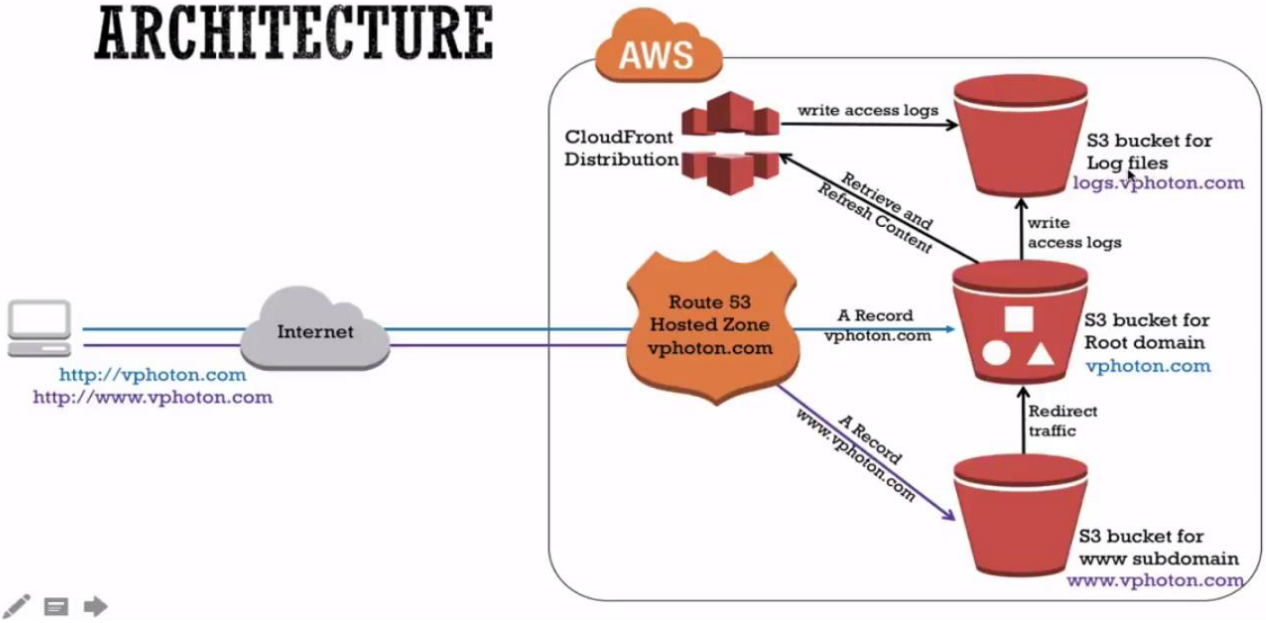
AWS – HOW TO CONFIGURE CLOUDFRONT FOR S3 BUCKET

My Blog: http://myvirtualbytes.com

ARCHITECTURE

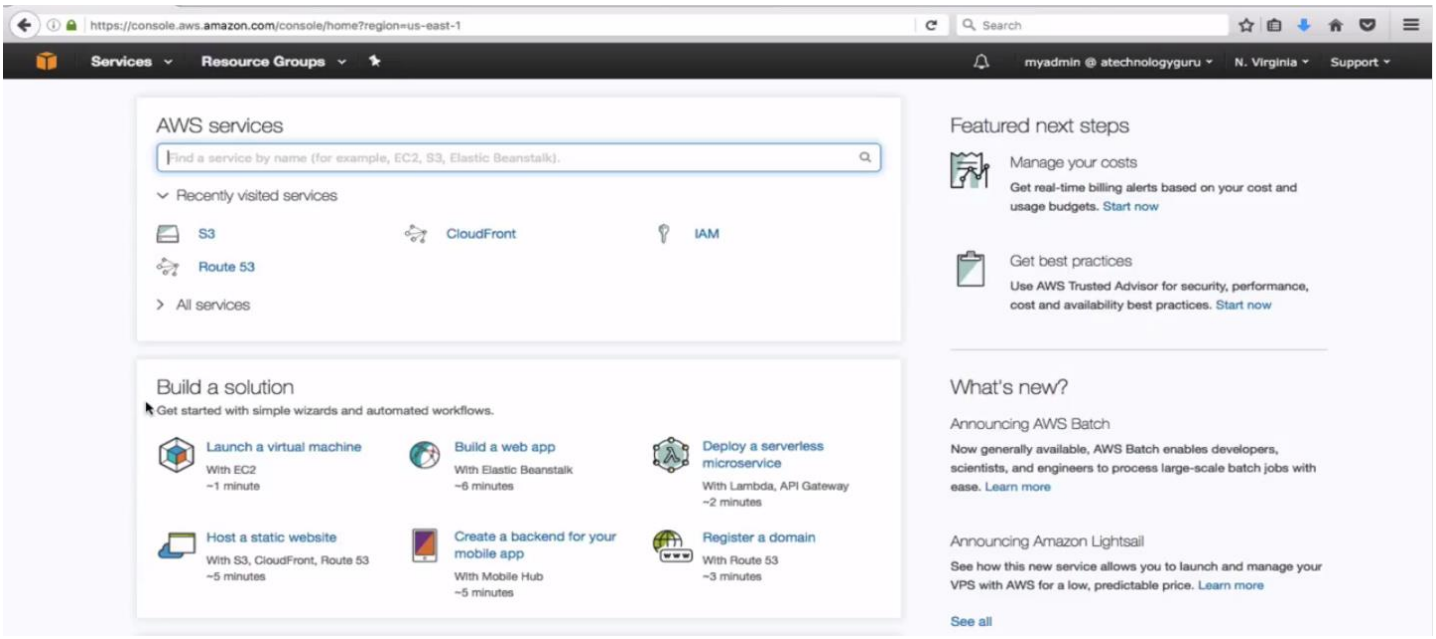


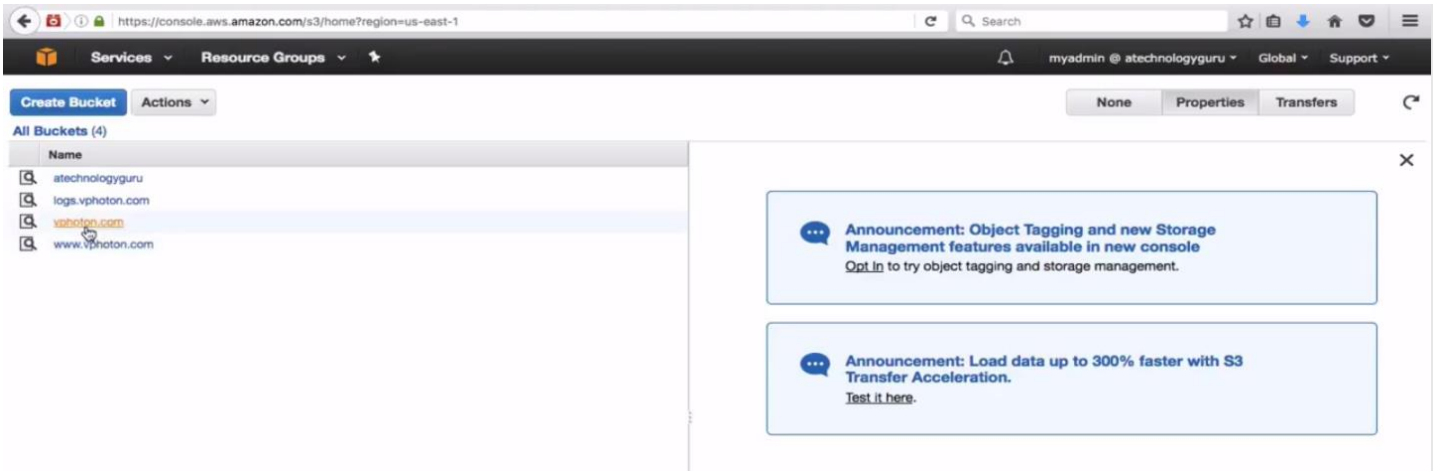
ARCHITECTURE

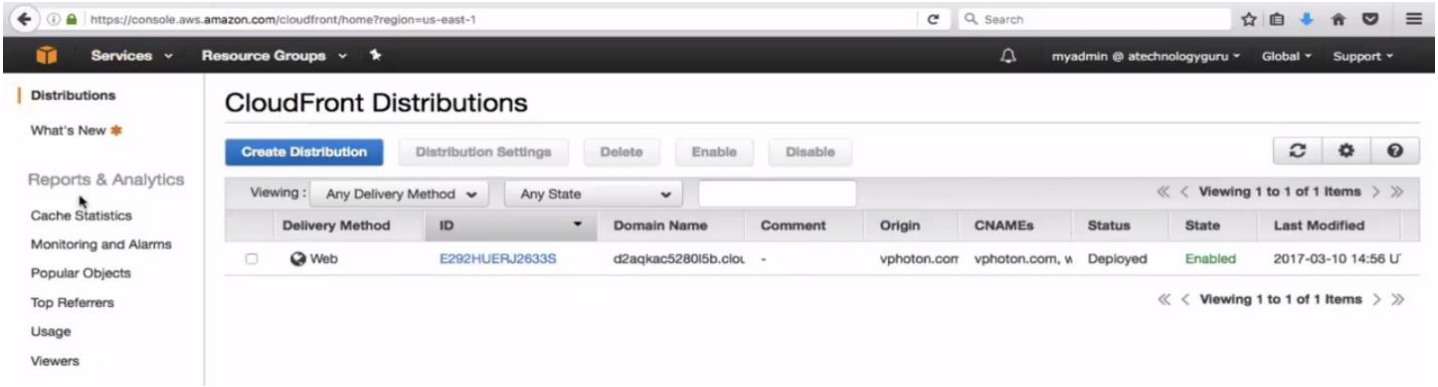


CLOUDFRONT SETUP

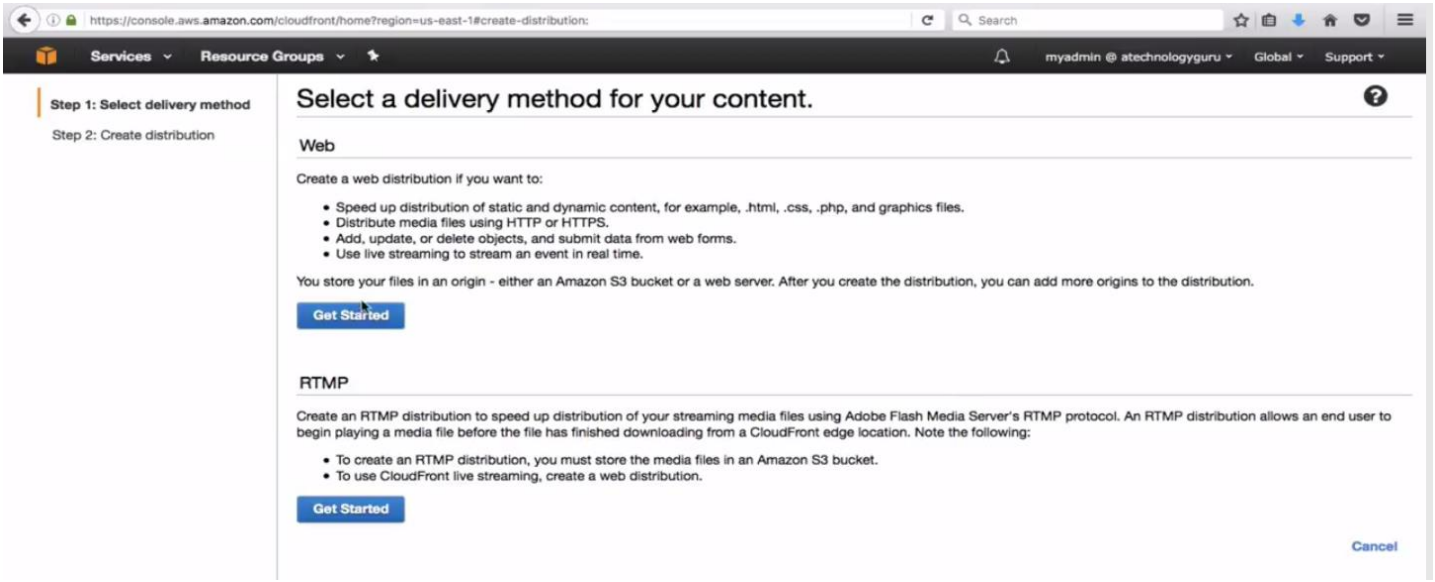
- Delivery Method = Web
- Origin Domain = S3 bucket → vphoton.com.s3.amazonaws.com
- Restrict Bucket Access = Yes
- Origin Access Identity = New
- Grant Read Permissions on Bucket = Yes, update
- Viewer Protocol Policy = HTTPS
- Restrict Viewer Access (Use Signed URLs or Signed Cookies) = No
- Alternate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

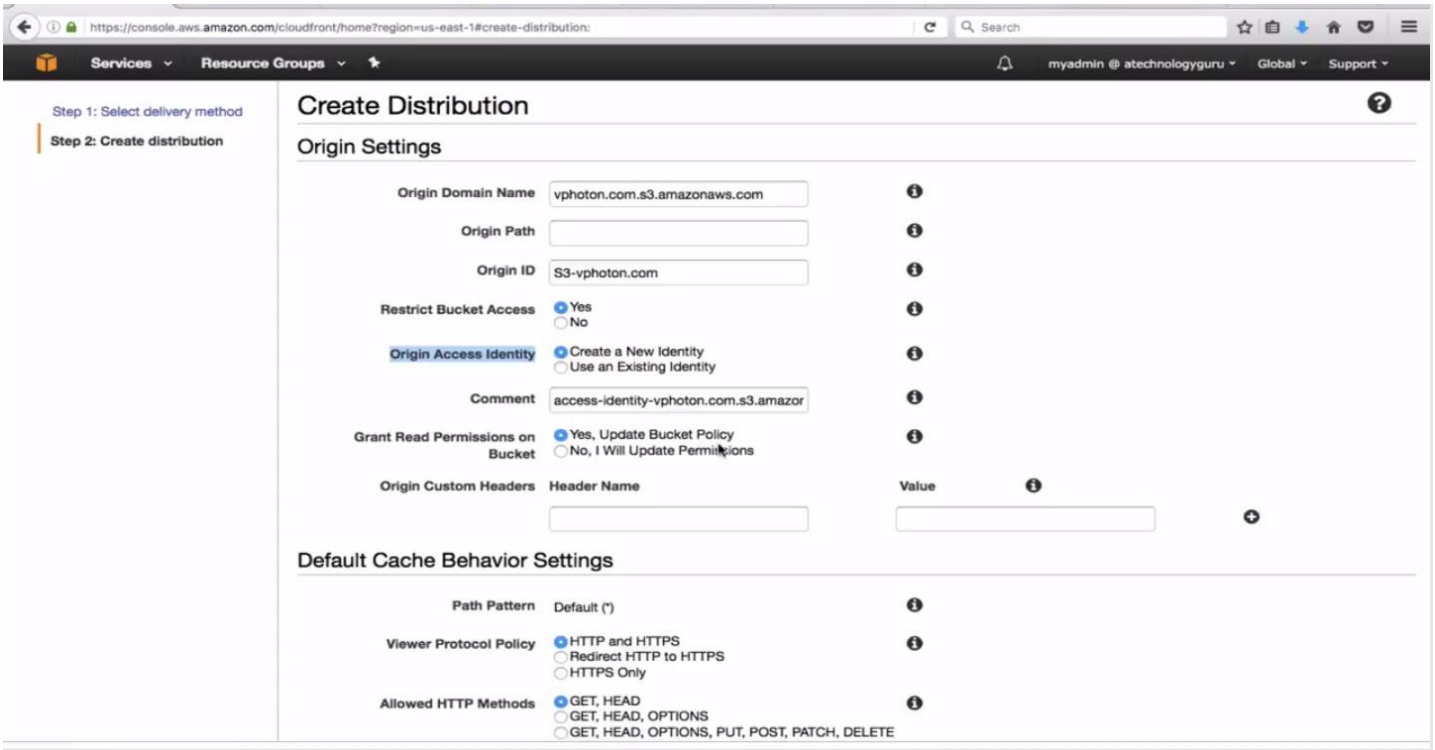


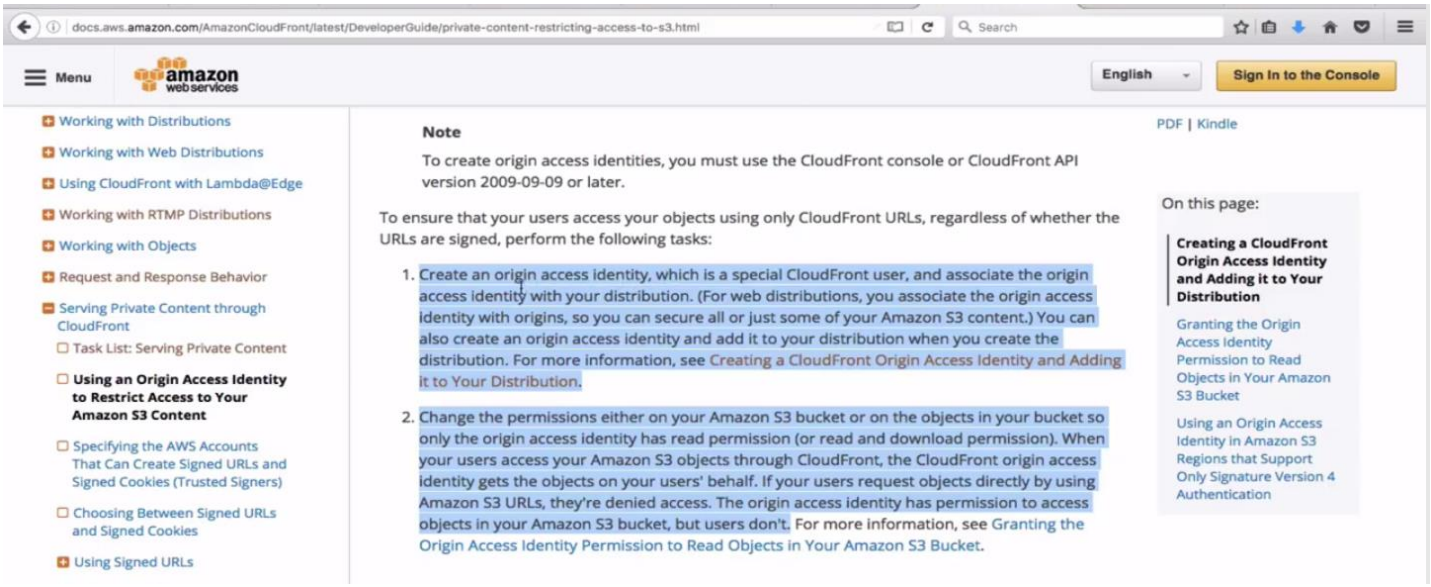


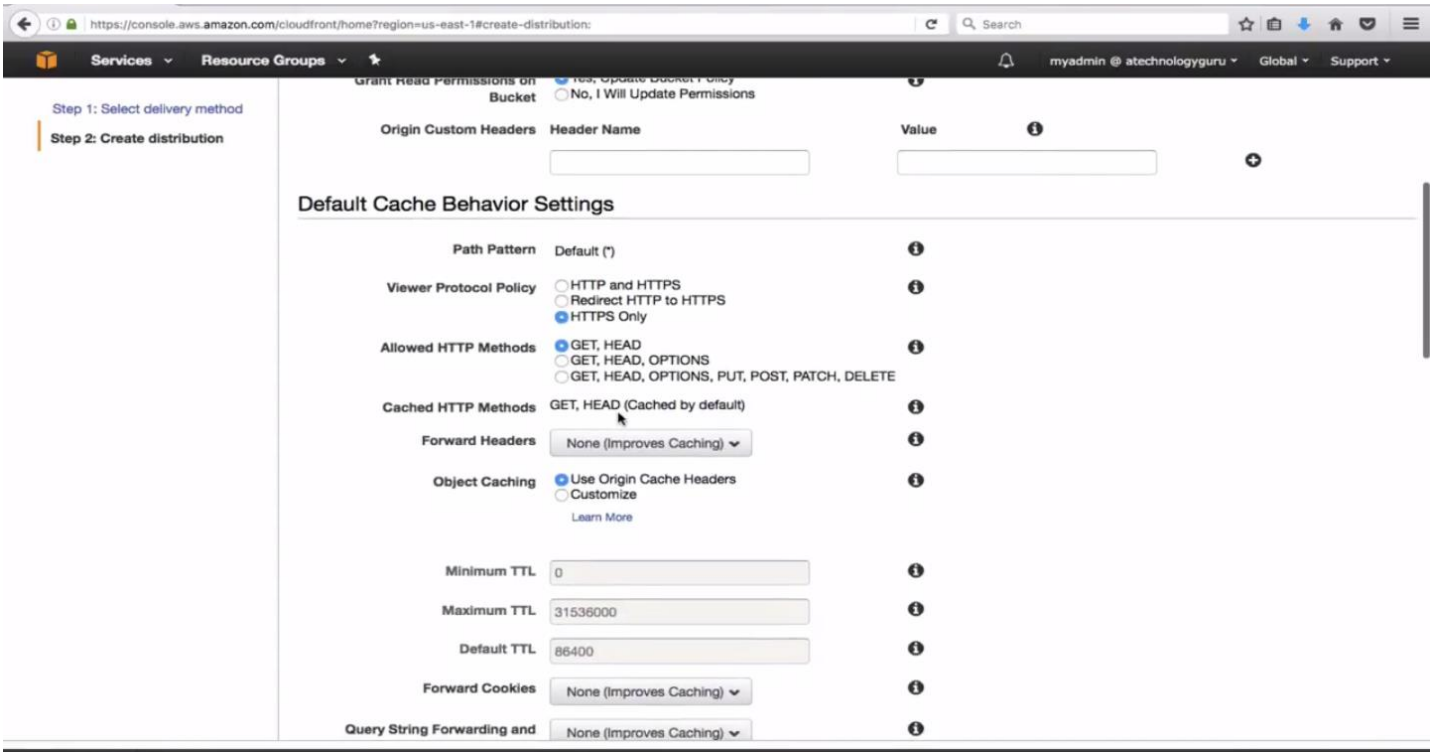


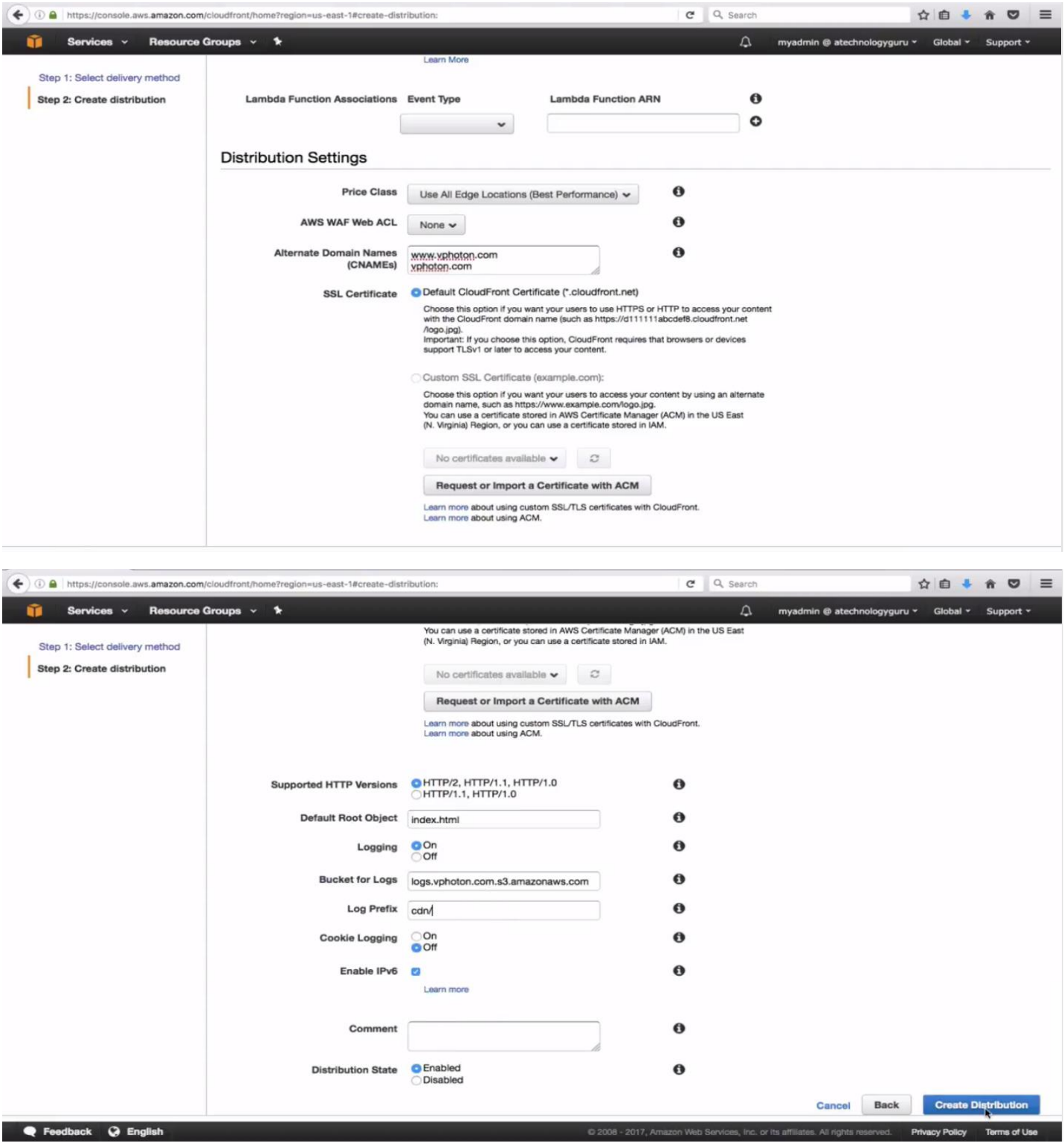
We already have a distribution called Web that is already deployed. Let us create a new one again


https://console.aws.amazon.com/cloudfront/home?region=us-east-1#create-distribution:
Search
Services
Resource Groups
myadmin @ atechnologyguru
Global
Support
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

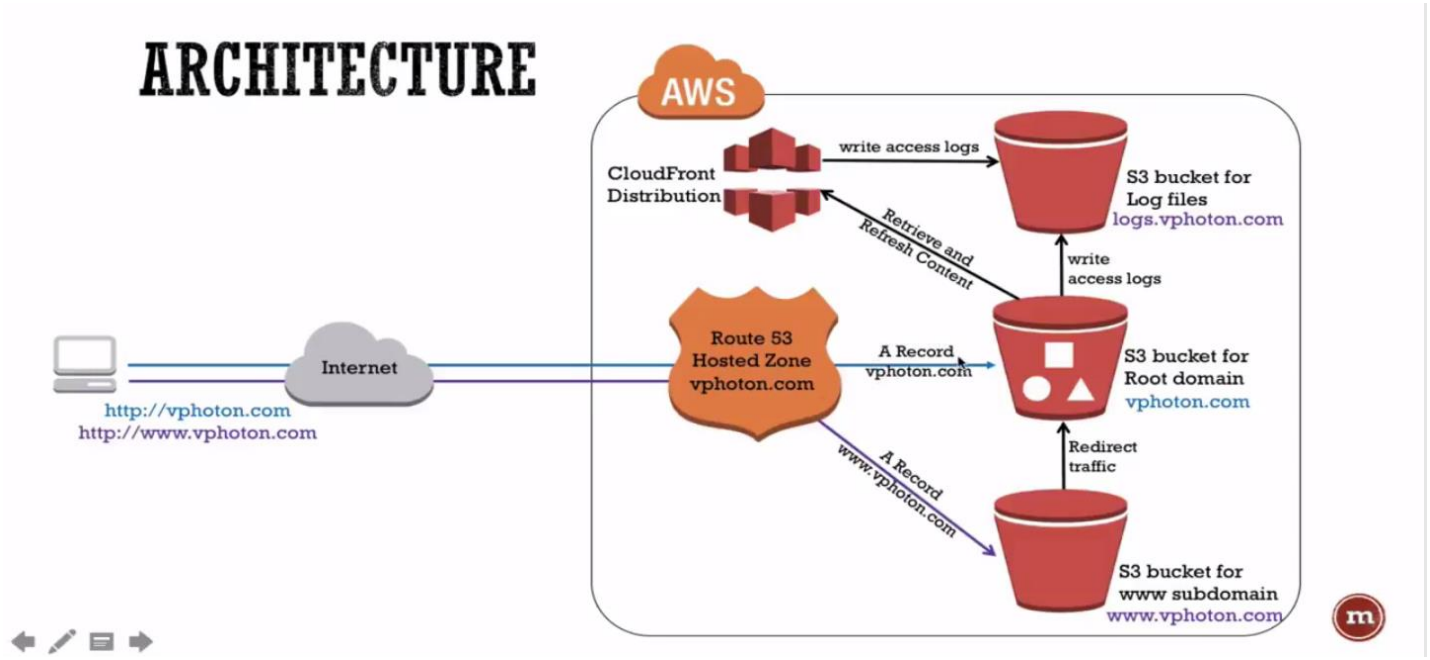

https://console.aws.amazon.com/cloudfront/home?region=us-east-1#create-distribution:
Search
Services
Resource Groups
myadmin @ atechnologyguru
Global
Support
Step 1: Select delivery method
Step 2: Create distribution
Create Distribution
Origin Settings
Origin Domain Name
vphoton.com.s3.amazonaws.com
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
Menu
amazon web services
English
Sign In to the Console
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

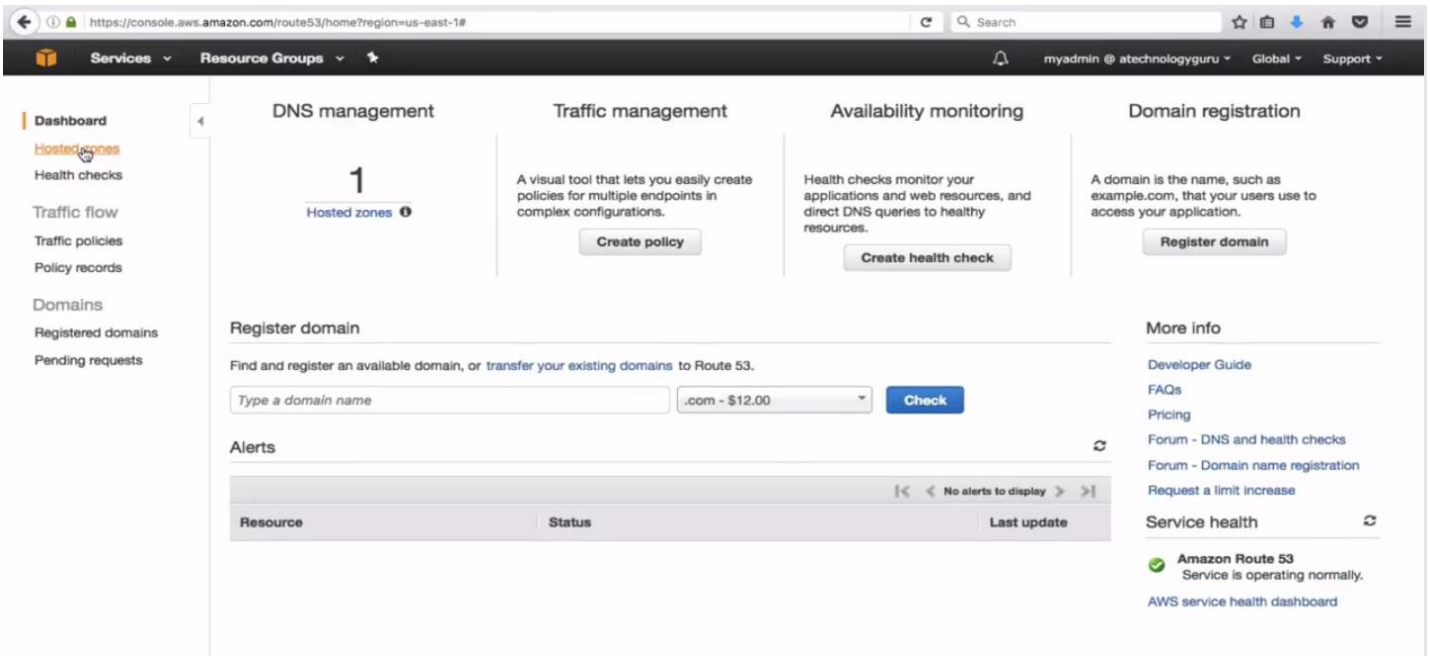

https://console.aws.amazon.com/cloudfront/home?region=us-east-1#create-distribution:
Search
Services
Resource Groups
myadmin @ atechnologyguru
Global
Support
Step 1: Select delivery method
Step 2: Create distribution
Grant Read Permissions on Bucket
No, I Will Update Permissions
Origin Custom Headers
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)

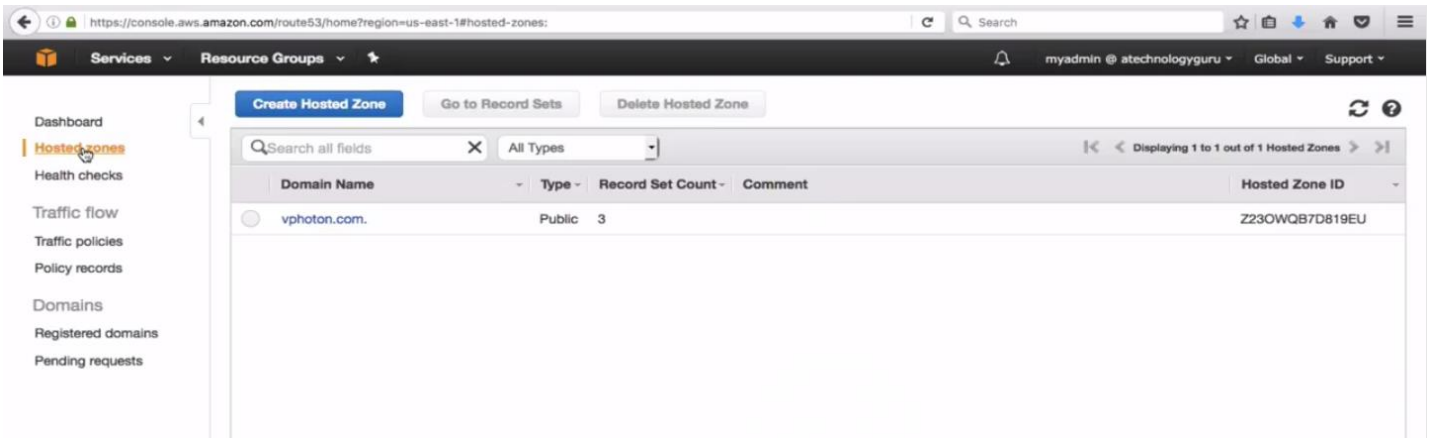


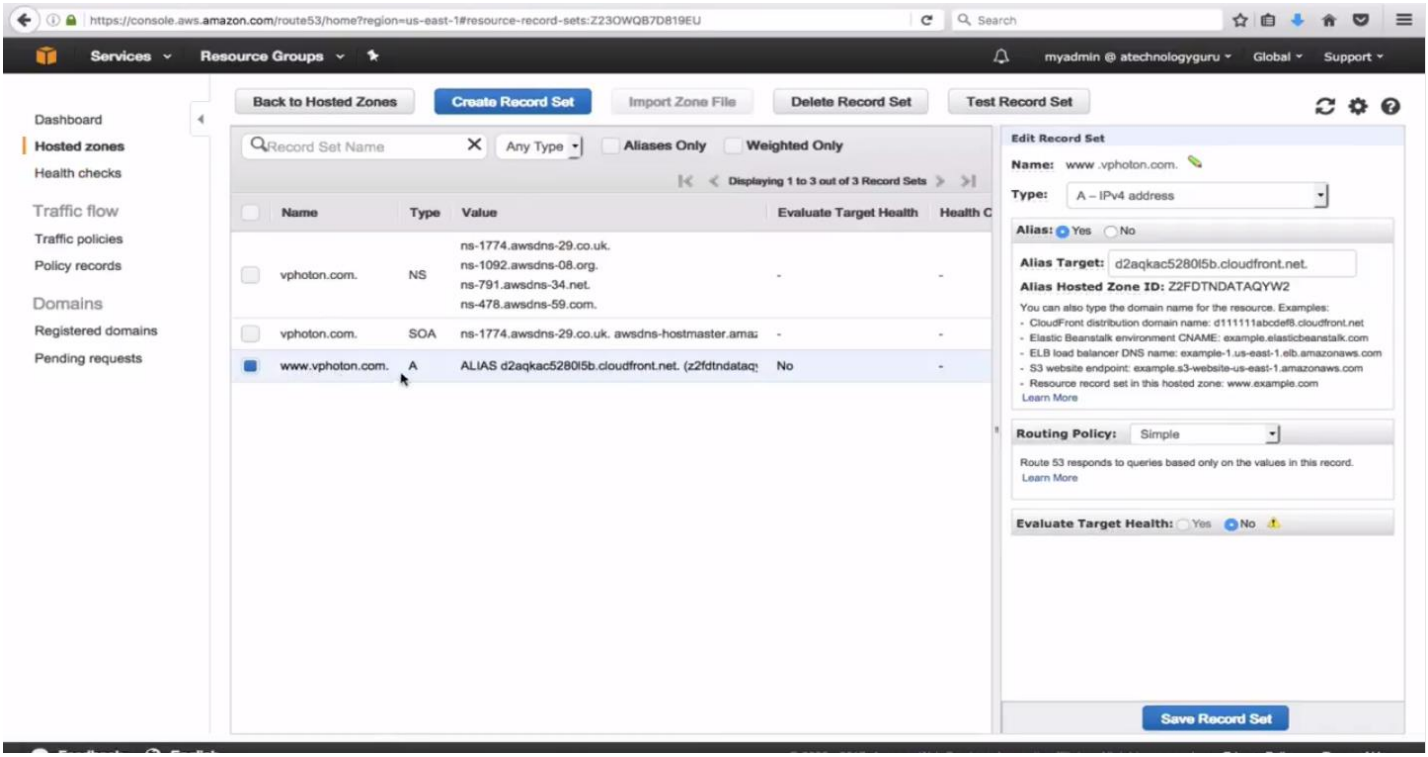
This will create that distribution for you, it will take about 15 – 20 minutes to create your distribution



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

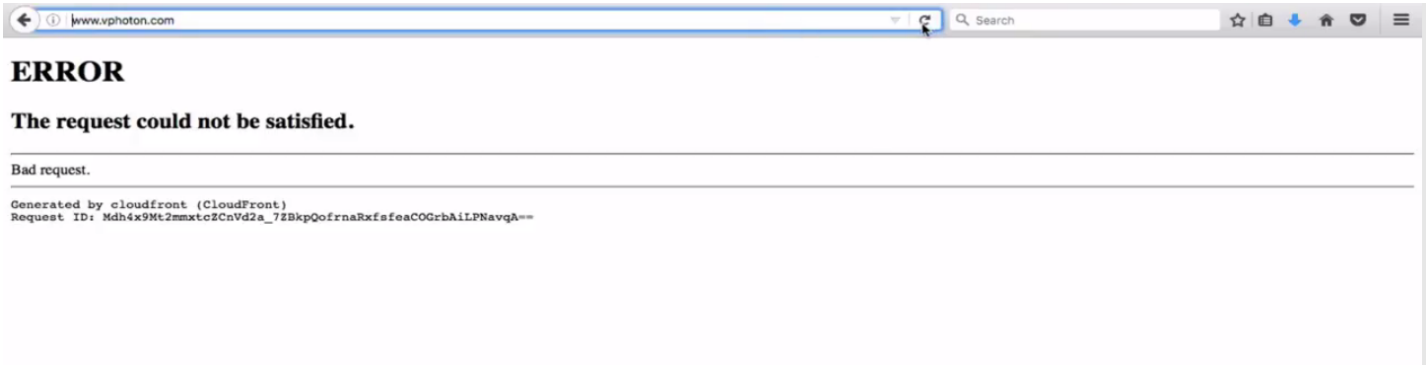




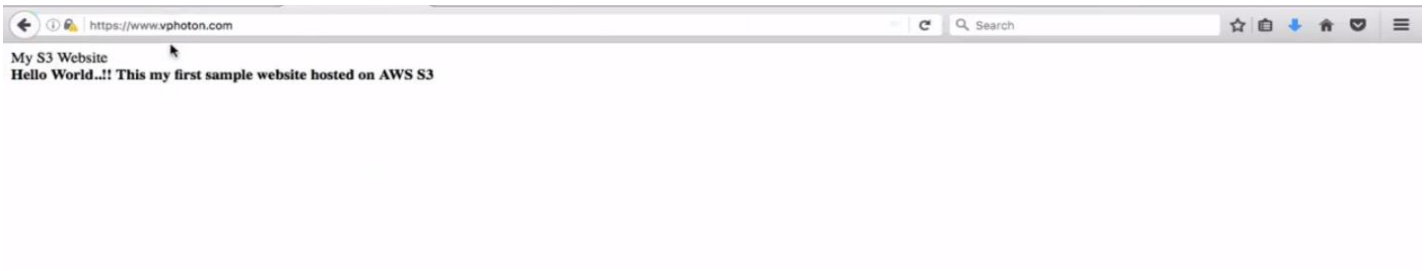


The A Record for your site should now be pointing to that CloudFront distribution endpoint as above.

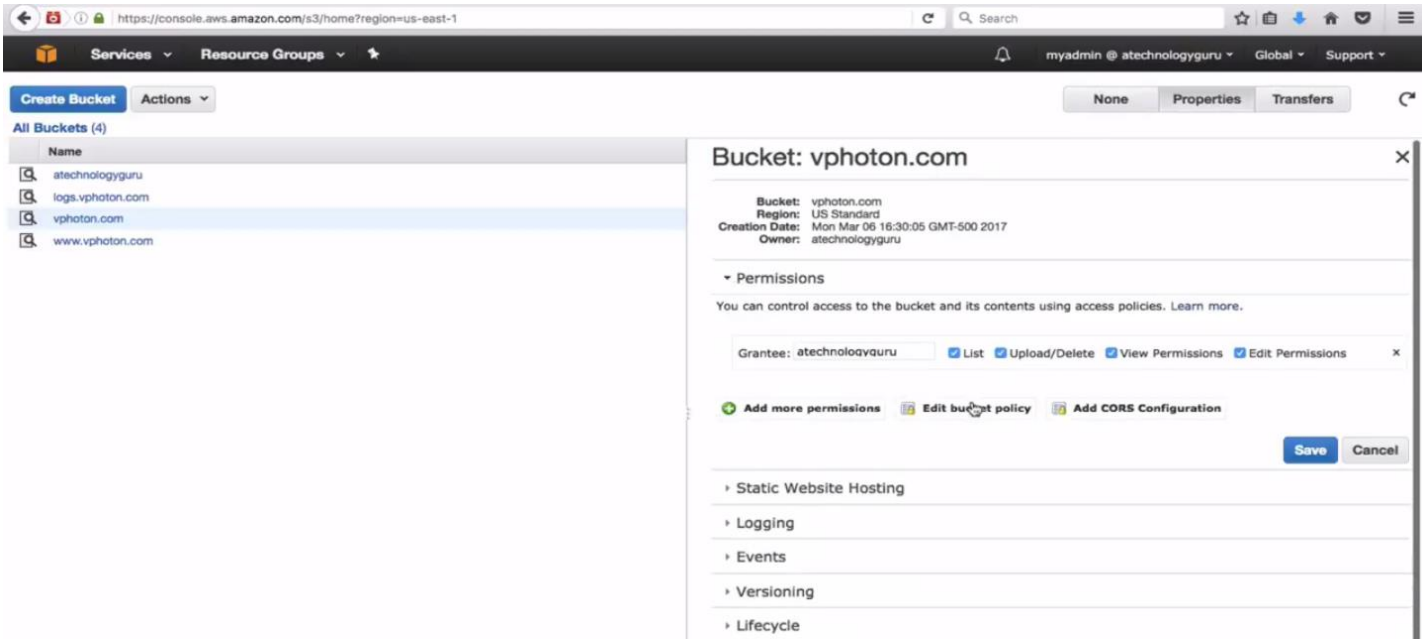
You can no longer go directly to your S3 bucket anymore

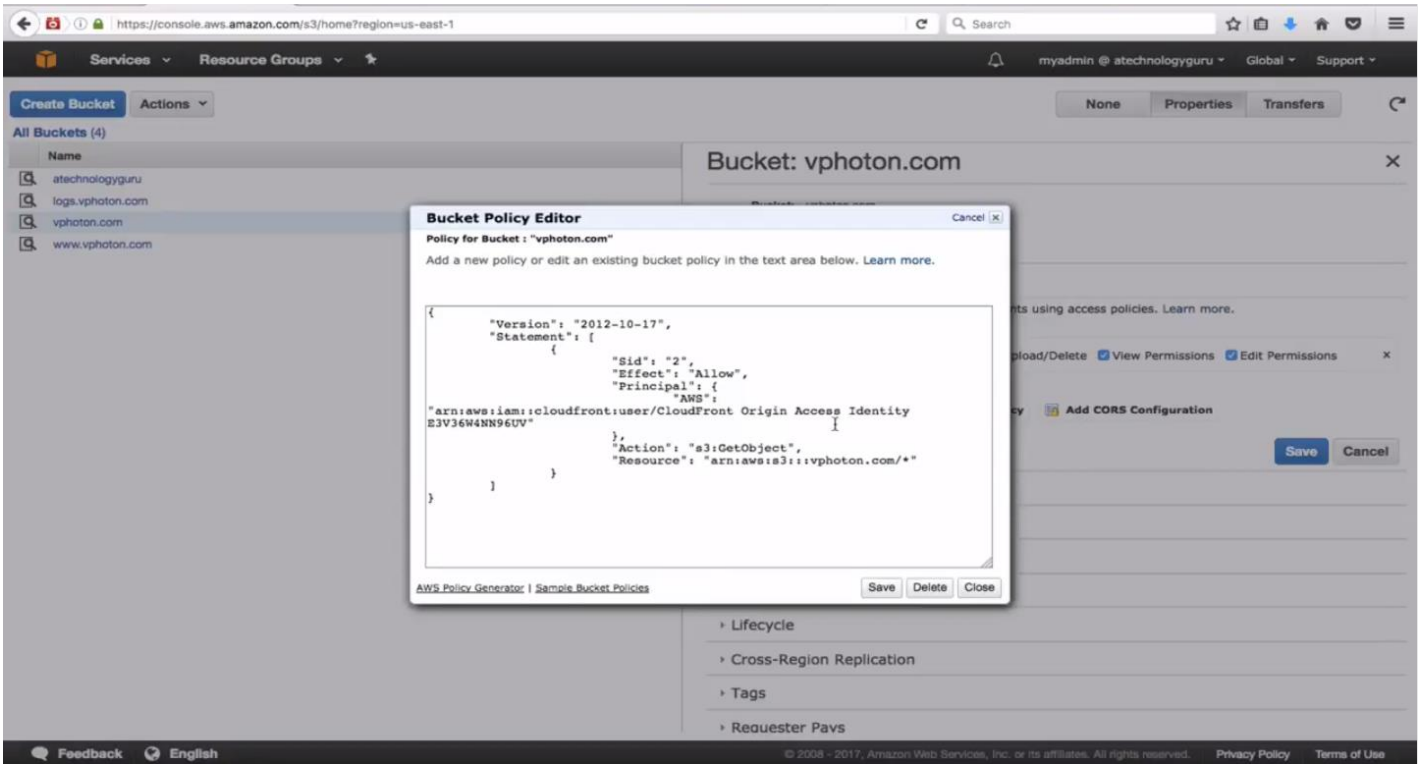


The HTTP protocol is not working anymore as above

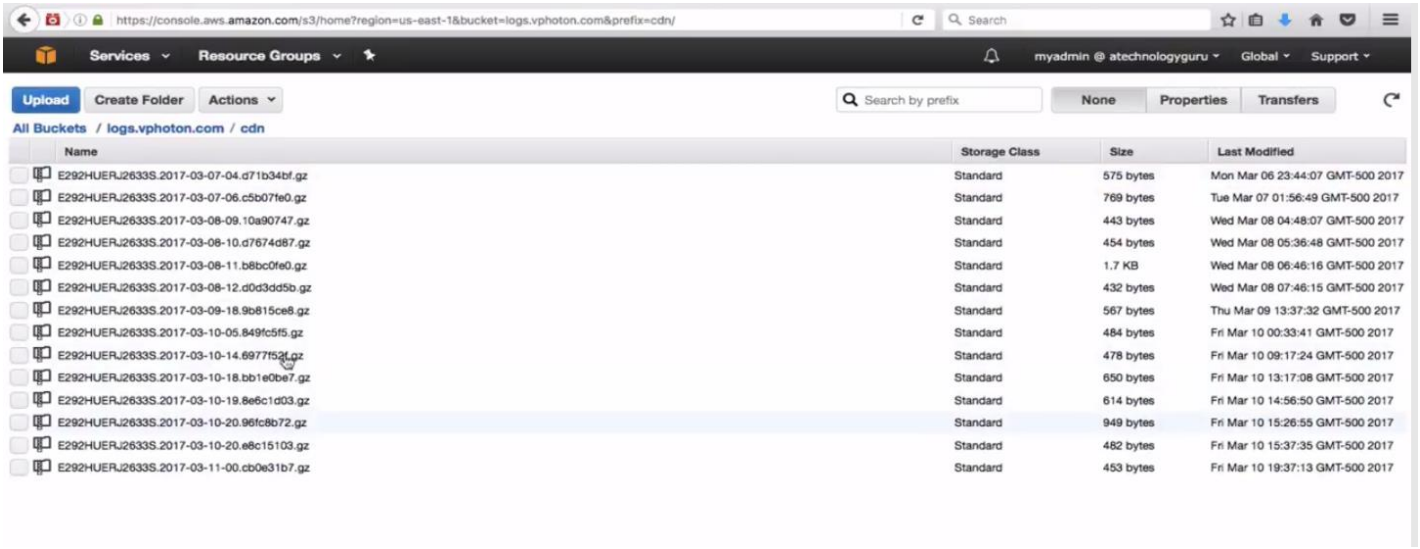


The HTTPS now works fine and we can see our site show up





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



Here is the logs S3 bucket