AWS CloudFront (CDN)

What is CloudFront ?

- CloudFront is a webservice provided by AWS to distribute contents securely with low latency and high speed from a nearest location for the users originated from.
- Its integrated and connected with AWS global infrastructure
- It can distribute static and dynamic contents
- For dynamic contents it doesn't cached the contents and send the traffic to origin server by reducing latency using amazon backbone network
- Static contents are get cached on the edge locations and served to the user directly from there
- It's a global service
- CloudFront route the user traffic to the nearest edge location from where the contents can be servers with lowest latency
- Its integrated with AWS Shield which prevent from DDoS attack
- Integrated with AWS WAF which prevents your web application from common web attacks like SQL injection
- If you are using origin as S3 and ELB then there is no additional cost for data transferred between origin and CloudFront
-

Edge Location :

- Currently it amazon has 200+ edge location across the countries/regions
- It has cache memory and cached all static contents requested by the users from the origin server
- It has 216 point of presence (POP), 11 regional edge cached, 200+ edge locations in 84 cities across 42 countries

Regional Edge Cache :

- It is similar to edge location, but work as an alternative of origin to reduce the load and increase performance of the origin
- When you delete the data from edge location those data are stored on the regional edge cache for a longer time and when needed edge location can get the data from regional cache rather reaching to the origin.
- This also helps to reduce the latency
- When data becomes infrequent access it started delete them and loads new data

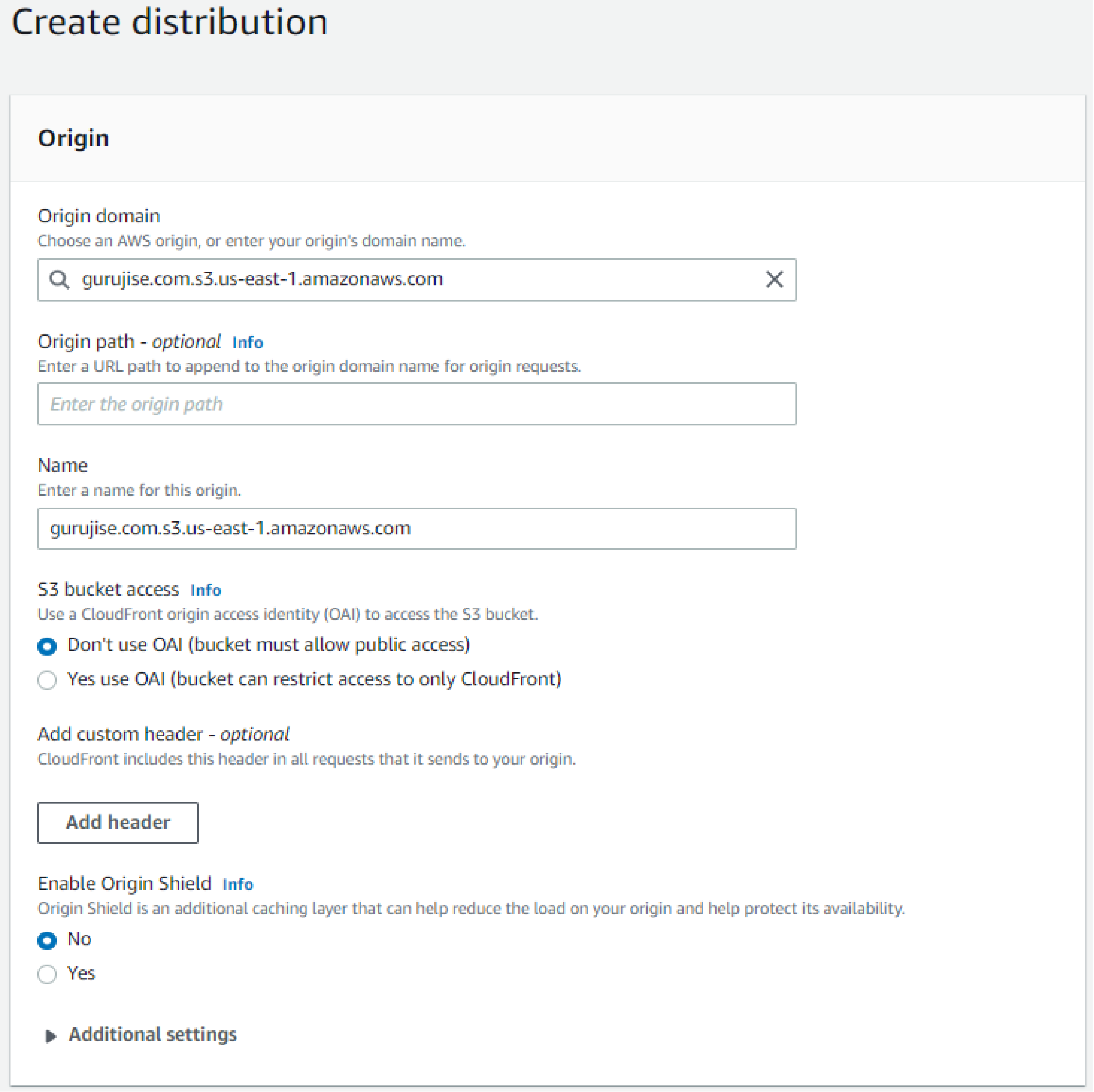
Important Points :

- **Invalidation Request :**
  - It removes the objects from both edge caches and regional edge caches before they actually expires
  - It required when you did new feature deployment or made any changes on your website
- **Origin Access Identity (OAI)**

    - It helps you to serve your private contents securely by restricting access to the object only from CloudFront instead of making public
    - Restrict bucket access
- When you use proxy method using PUT/POST/PATCH/OPTIONS/DELETE the request goes directly to the origin from edge locations and it never goes to the regional edge cache
- Requests related to dynamic contents always forwarded directly to the origin from edge location and never forwarded to regional edge cache
- Default cache age is 24 hours and maximum is 1 year

Integrating With Route-53 : (Using Custom Domain)

- When you create CloudFront distribution by default it provides a domain name for example “d111111abcdef8.cloudfront.net”
- However, if you do not want to use default domain and wants to use your own custom domain for example “gurujise.com”, you have to add an alternate domain name to your distribution
- Then you can create a record on Route-53 with your custom DomainName and map to CloudFront domain name.
- NOTE : Adding alternative domain required custom SSL certificate. So before you proceed with this setup you must have requested a custom certificate for your custom domain using ACM.



Create distribution

Origin

Origin domain

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

gurujise.com.s3.us-east-1.amazonaws.com

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.

gurujise.com.s3.us-east-1.amazonaws.com

S3 bucket access Info

Use a CloudFront origin access identity (OAI) to access the S3 bucket.

● Don't use OAI (bucket must allow public access)

○ Yes use OAI (bucket can restrict access to only CloudFront)

Add custom header - *optional*

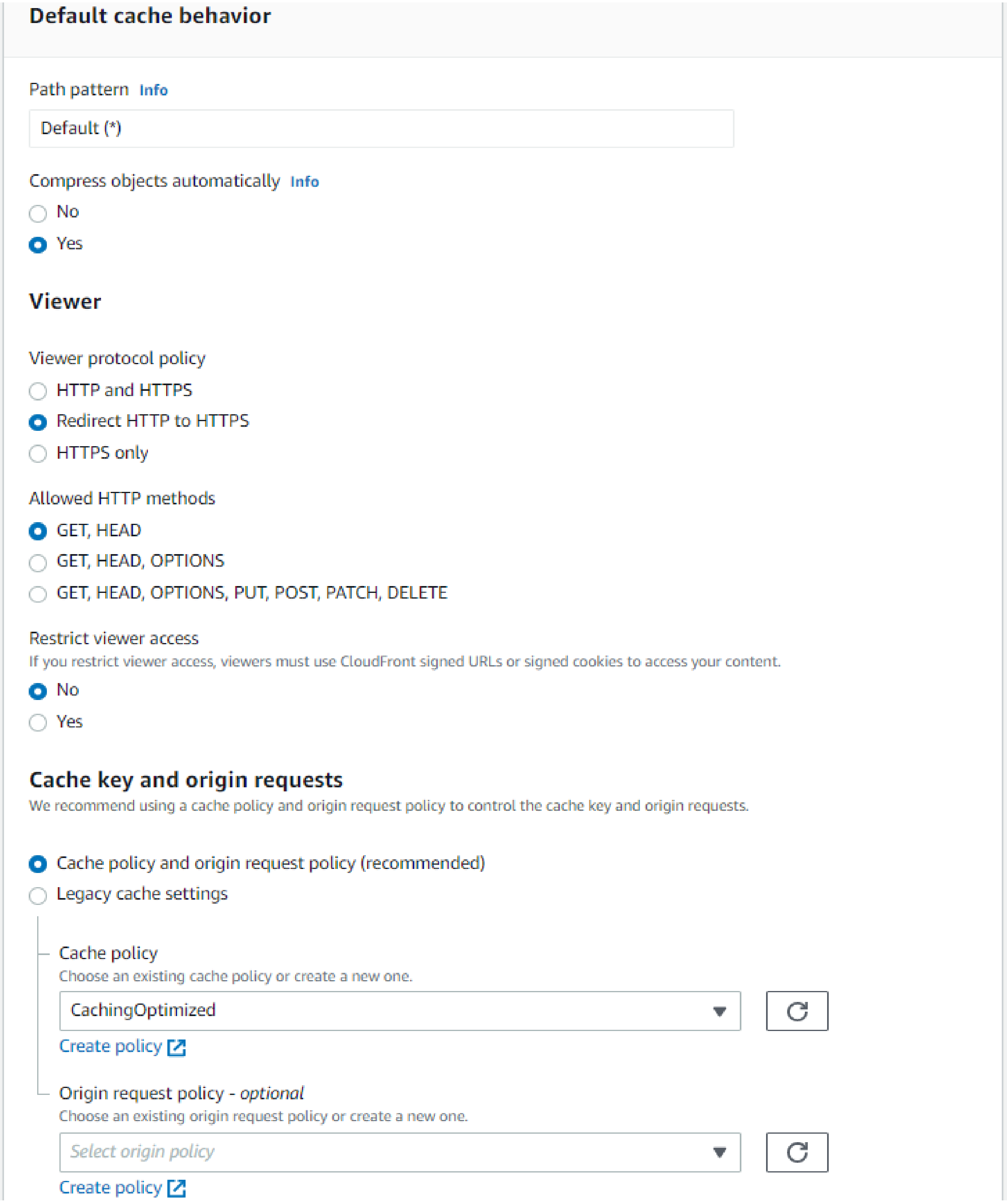
CloudFront includes this header in all requests that it sends to your origin.

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



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 ▼

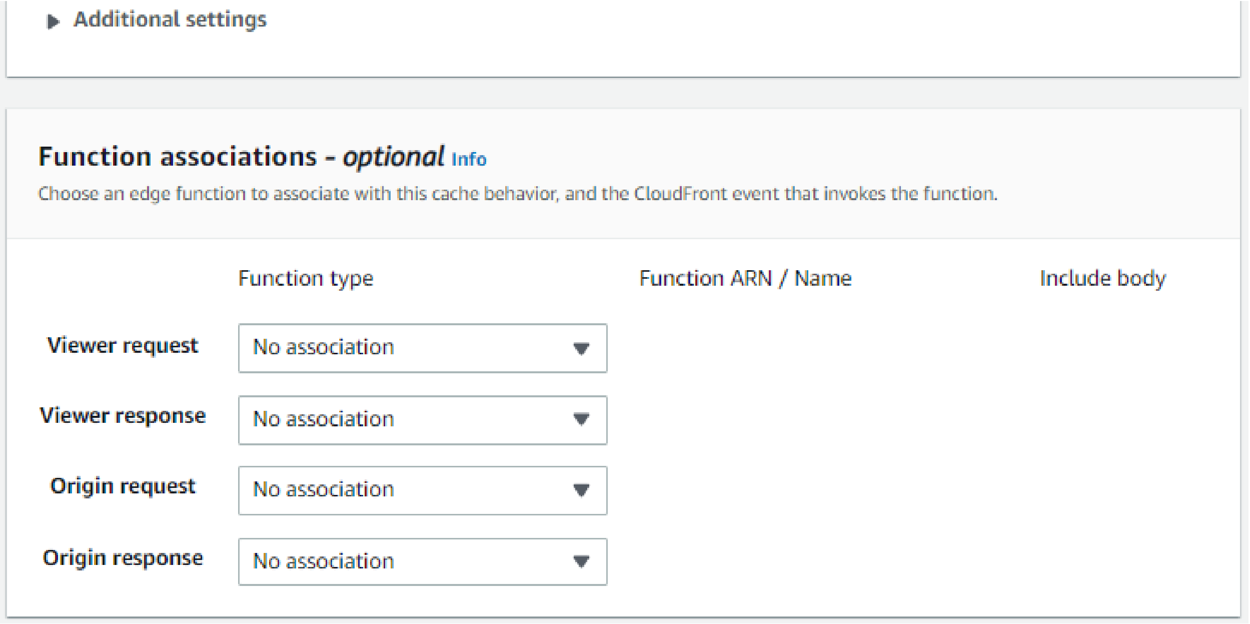
Create policy

Origin request policy - *optional*

Choose an existing origin request policy or create a new one.

Select origin policy ▼

Create policy

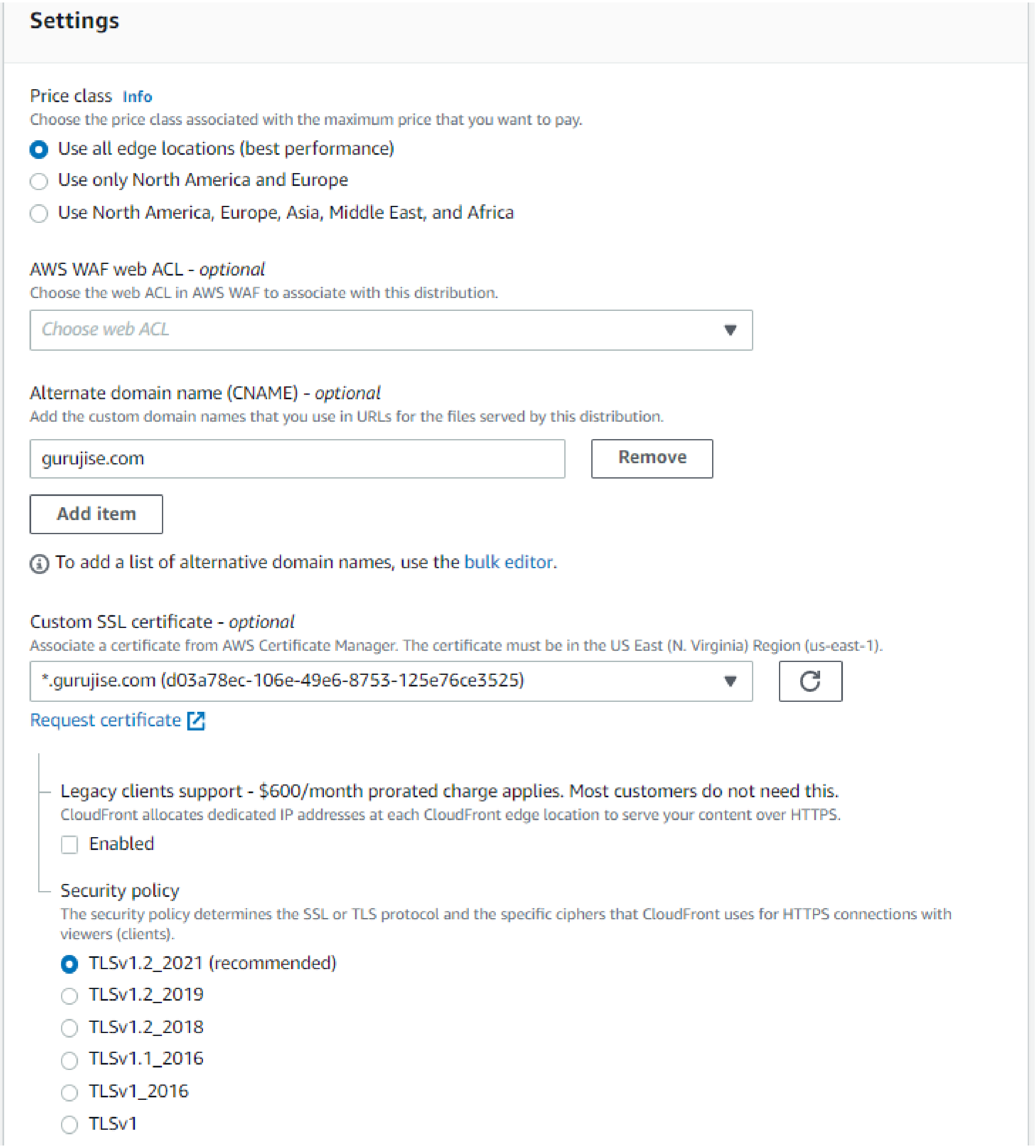


▶ Additional settings

Function associations - *optional* Info

Choose an edge function to associate with this cache behavior, and the CloudFront event that invokes the function.

	Function type	Function ARN / Name	Include body
Viewer request	No association ▼		
Viewer response	No association ▼		
Origin request	No association ▼		
Origin response	No association ▼		



Settings

Price class

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.

gurujise.com

ⓘ 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).

*.gurujise.com (d03a78ec-106e-49e6-8753-125e76ce3525) ▼

Legacy clients support - $600/month prorated charge applies. Most customers do not need this.

CloudFront allocates dedicated IP addresses at each CloudFront edge location to serve your content over HTTPS.

□ Enabled

Security policy

The security policy determines the SSL or TLS protocol and the specific ciphers that CloudFront uses for HTTPS connections with viewers (clients).

● TLSv1.2_2021 (recommended)

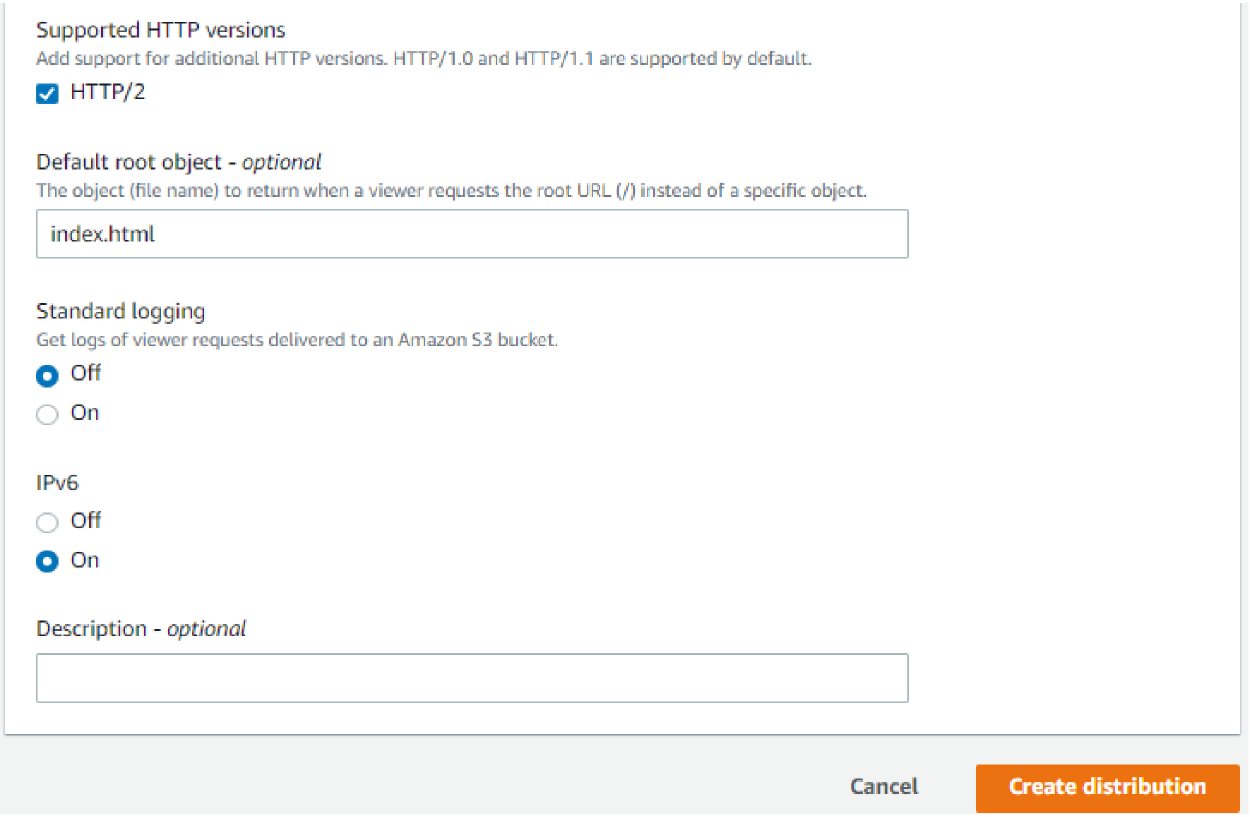
○ TLSv1.2_2019

○ TLSv1.2_2018

○ TLSv1.1_2016

○ TLSv1_2016

○ TLSv1



Supported HTTP versions

Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default.

☑ HTTP/2

Default root object - *optional*

The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.

index.html

Standard logging

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

● Off

○ On

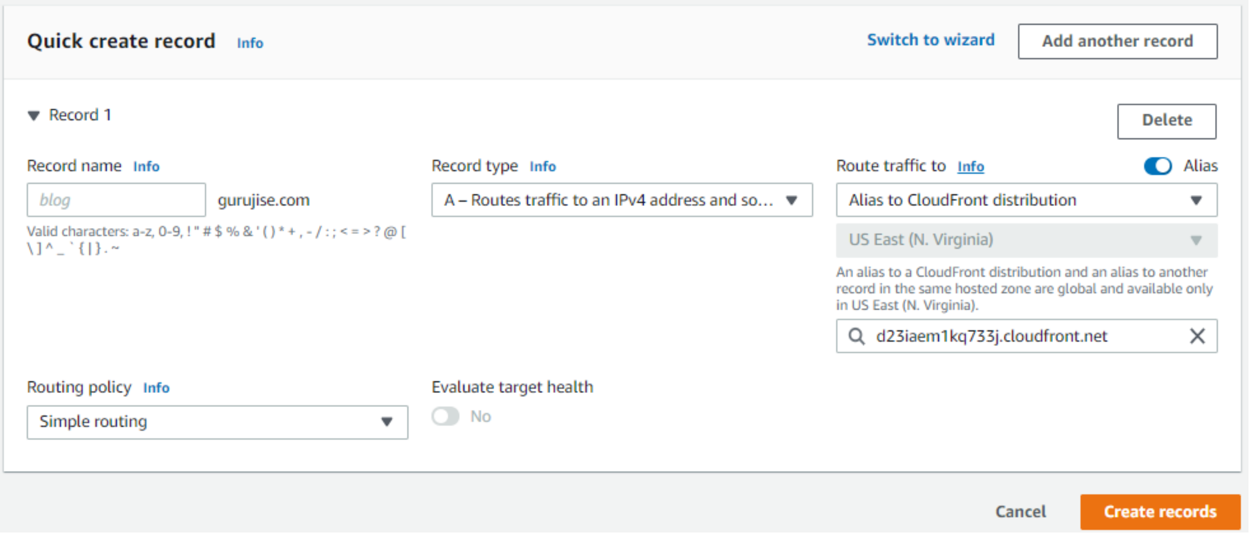
IPv6

○ Off

● On

Description - *optional*

- Then create a record on Route-53 as per the below setting



Quick create record Info

Record 1

Record name: blog gurujise.com

Valid characters: a-z, 0-9, ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } . ~

Record type: A – Routes traffic to an IPv4 address and so...

Route traffic to: Alias — Alias to CloudFront distribution

US East (N. Virginia)

An alias to a CloudFront distribution and an alias to another record in the same hosted zone are global and available only in US East (N. Virginia).

d23iaem1kq733j.cloudfront.net

Routing policy: Simple routing

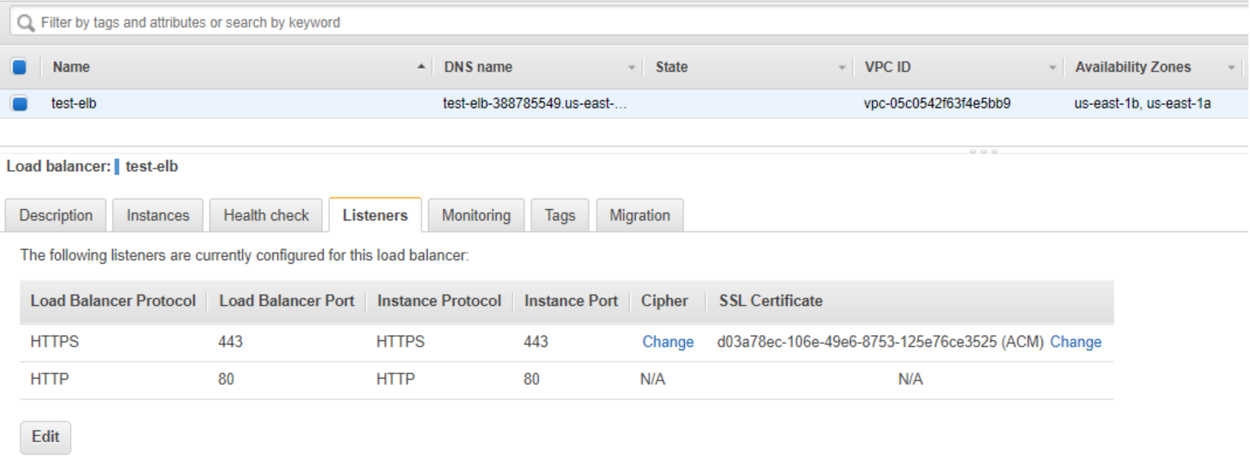
Evaluate target health: No

- Then you can test by accessing the Custom DNS name “gurujise.com”. it should be accessible. In case of any issue try to access by changing the protocols (http/https) for the first time.

Configure With Multiple Origins :

1. Launch an EC2 instance and configure a sample application which will be accessible from Internet and put the EC2 instance under Load Balancer
2. Make sure, you configured with the same custom SSL certificate on the ELB which is used on the CloudFront

3. Allow port 443(HTTPS) on both the security group at ELB and EC2 level



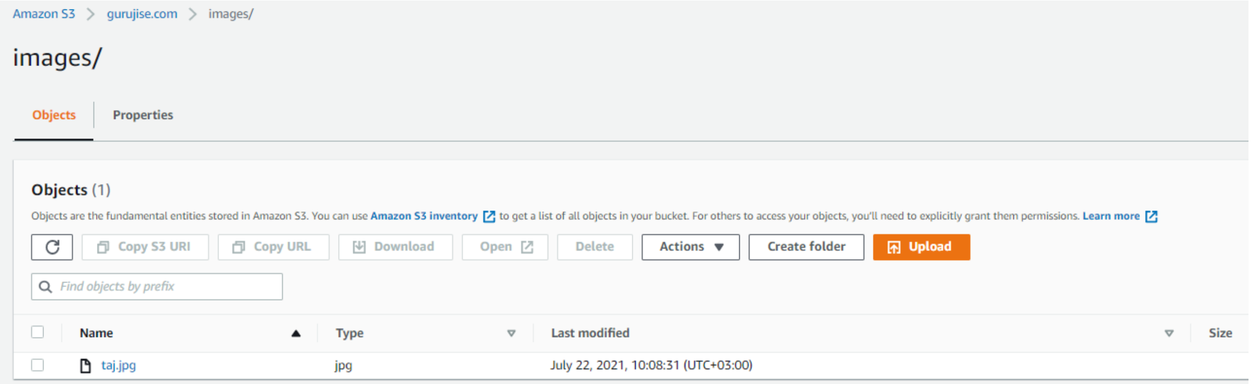
Name	DNS name	State	VPC ID	Availability Zones
test-elb	test-elb-388785549.us-east-…		vpc-05c0542f63f4e5bb9	us-east-1b, us-east-1a

Load balancer: test-elb

The following listeners are currently configured for this load balancer:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port	Cipher	SSL Certificate
HTTPS	443	HTTPS	443	Change	d03a78ec-106e-49e6-8753-125e76ce3525 (ACM) Change
HTTP	80	HTTP	80	N/A	N/A

4. Create a folder inside the same S3 bucket you used previously and put an image what you can access later to verify



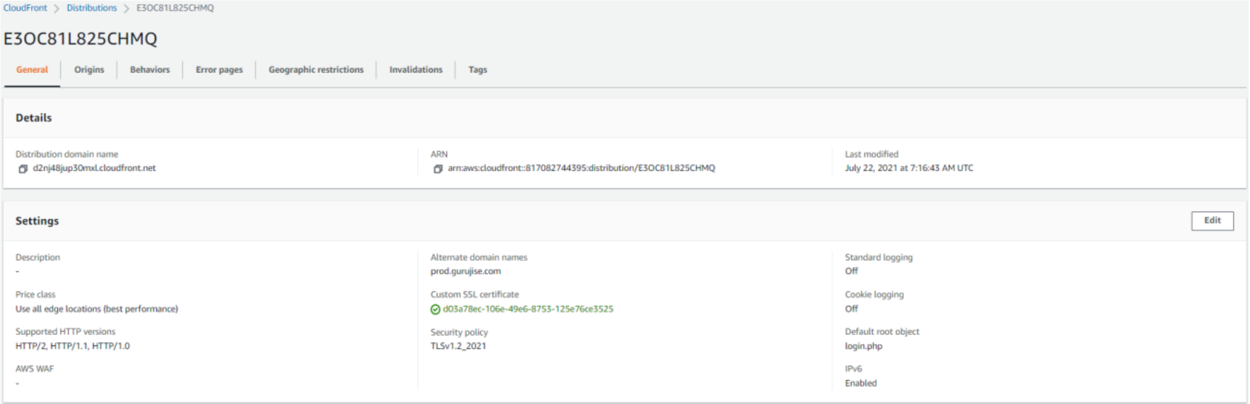
images/

Objects (1)

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

Name	Type	Last modified	Size
taj.jpg	jpg	July 22, 2021, 10:08:31 (UTC+03:00)	

5. Create the CloudFront distribution details



E3OC81L825CHMQ

Details

Distribution domain name
d2nj48jup30mxl.cloudfront.net

ARN
arn:aws:cloudfront::817082744395:distribution/E3OC81L825CHMQ

Last modified
July 22, 2021 at 7:16:43 AM UTC

Settings

Description
-

Price class
Use all edge locations (best performance)

Supported HTTP versions
HTTP/2, HTTP/1.1, HTTP/1.0

AWS WAF
-

Alternate domain names
prod.gurujise.com

Custom SSL certificate
d03a78ec-106e-49e6-8753-125e76ce3525

Security policy
TLSv1.2_2021

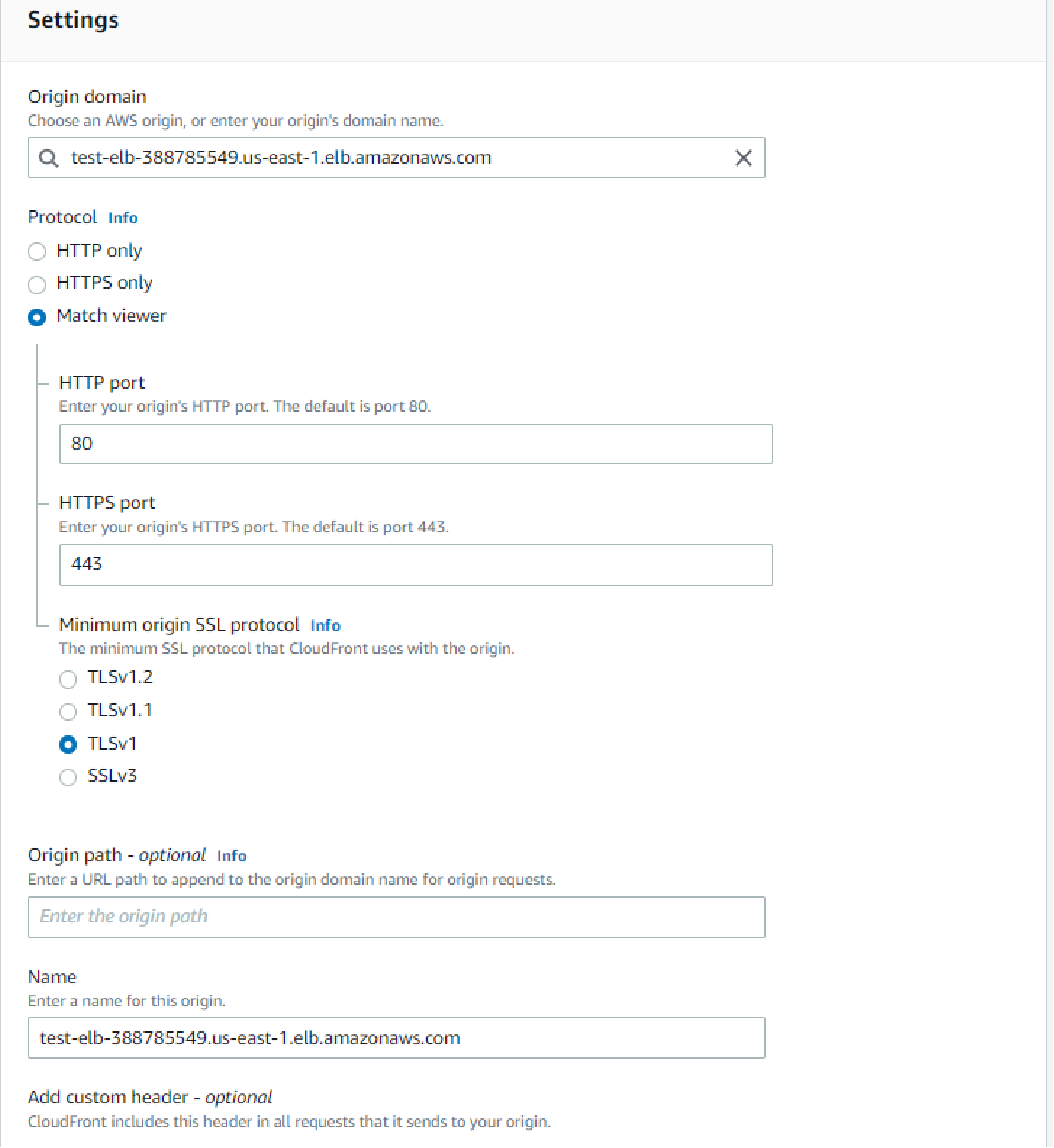
Standard logging
Off

Cookie logging
Off

Default root object
login.php

IPv6
Enabled

6. Create another Origin on the same CloudFront distribution for another application deployed on the EC2 and ELB



Settings

Origin domain
Choose an AWS origin, or enter your origin's domain name.
test-elb-388785549.us-east-1.elb.amazonaws.com

Protocol Info
○ HTTP only
○ HTTPS only
● Match viewer

HTTP port
Enter your origin's HTTP port. The default is port 80.
80

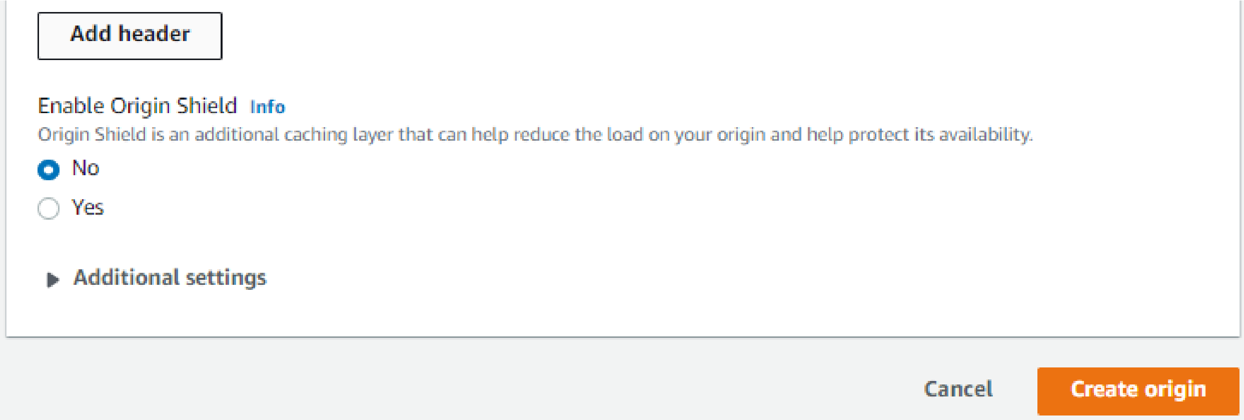
HTTPS port
Enter your origin's HTTPS port. The default is port 443.
443

Minimum origin SSL protocol Info
The minimum SSL protocol that CloudFront uses with the origin.
○ TLSv1.2
○ TLSv1.1
● TLSv1
○ SSLv3

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.
test-elb-388785549.us-east-1.elb.amazonaws.com

Add custom header - *optional*
CloudFront includes this header in all requests that it sends to your origin.

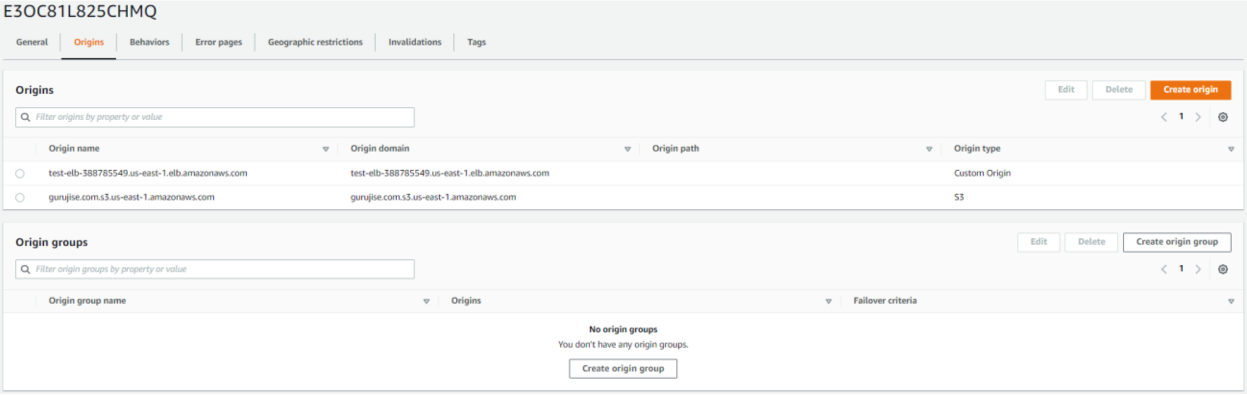


Enable Origin Shield Info

Origin Shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.

● No

○ Yes



E3OC81L825CHMQ

Origins

	Origin name	Origin domain	Origin path	Origin type
○	test-elb-388785549.us-east-1.elb.amazonaws.com	test-elb-388785549.us-east-1.elb.amazonaws.com		Custom Origin
○	gurujise.com.s3.us-east-1.amazonaws.com	gurujise.com.s3.us-east-1.amazonaws.com		S3

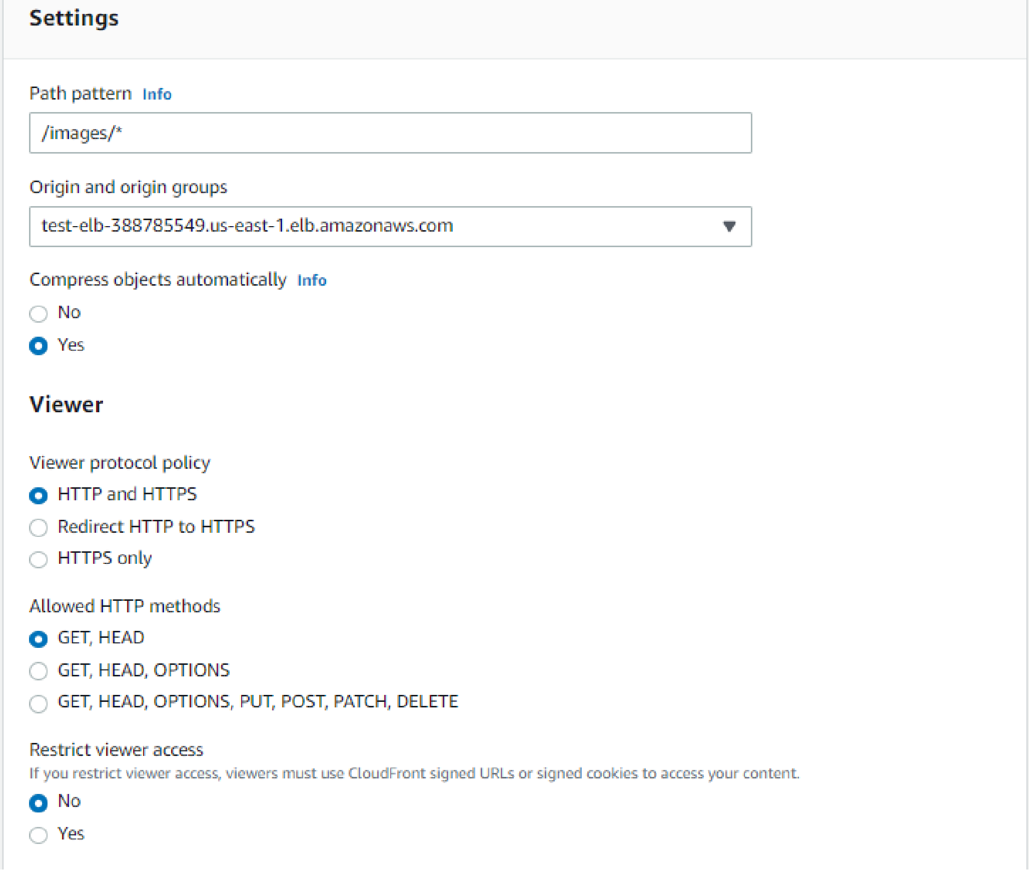
Origin groups

Origin group name	Origins	Failover criteria

No origin groups

You don't have any origin groups.

7. Then create a behaviors for the 2nd Origin as per the below mentioned settings



Settings

Path pattern Info

/images/*

Origin and origin groups

test-elb-388785549.us-east-1.elb.amazonaws.com

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

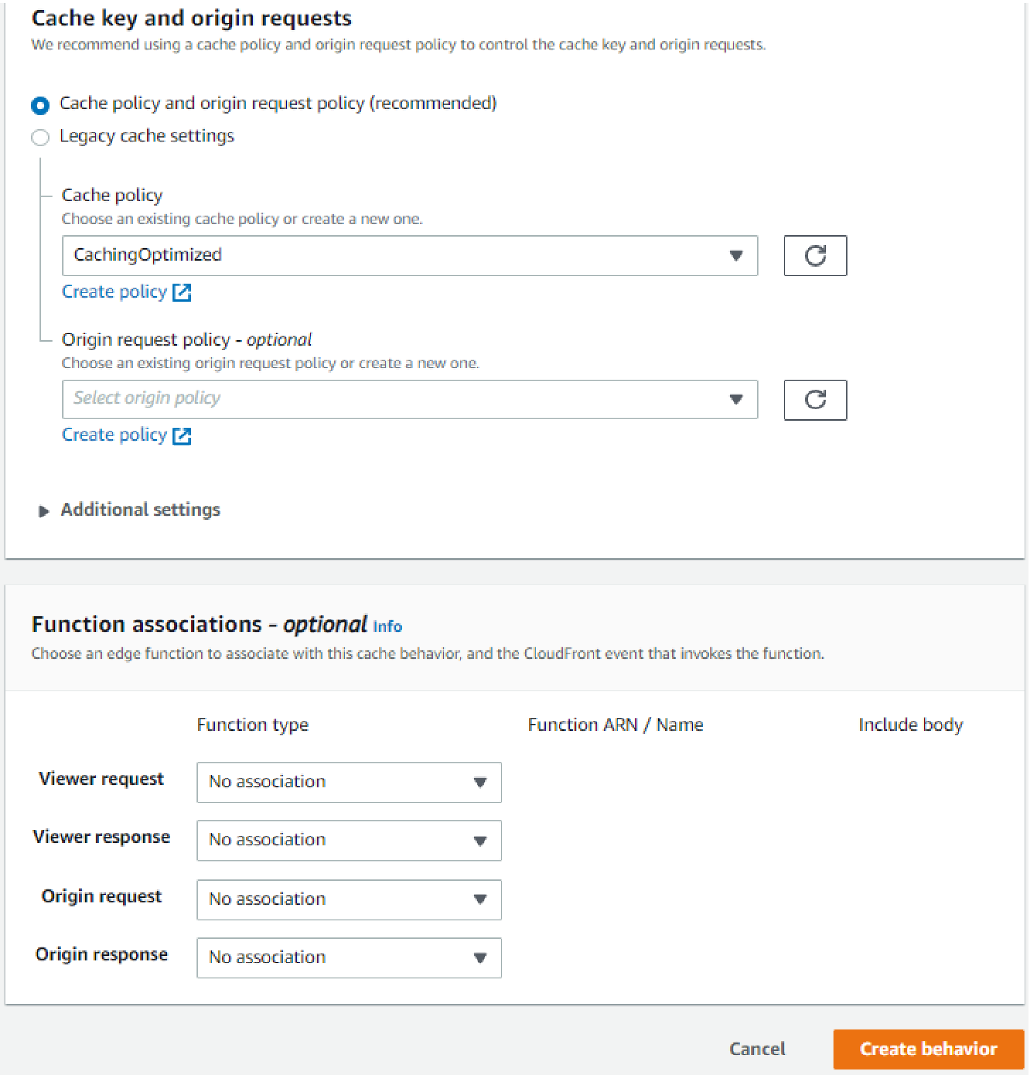
○ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

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 ▼

Create policy

Origin request policy - *optional*

Choose an existing origin request policy or create a new one.

Select origin policy ▼

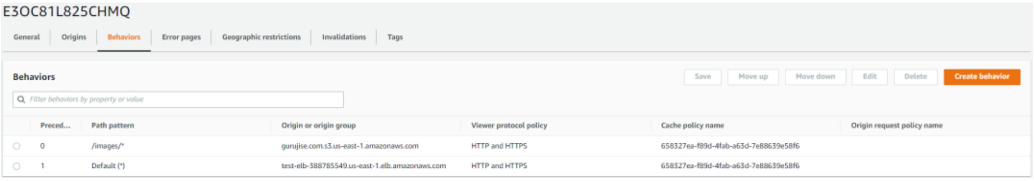
Create policy

▶ Additional settings

Function associations - *optional* Info

Choose an edge function to associate with this cache behavior, and the CloudFront event that invokes the function.

	Function type	Function ARN / Name	Include body
Viewer request	No association ▼		
Viewer response	No association ▼		
Origin request	No association ▼		
Origin response	No association ▼		

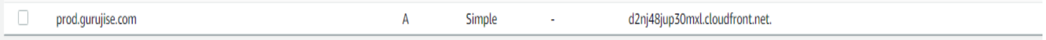


E3OC81L825CHMQ

Behaviors

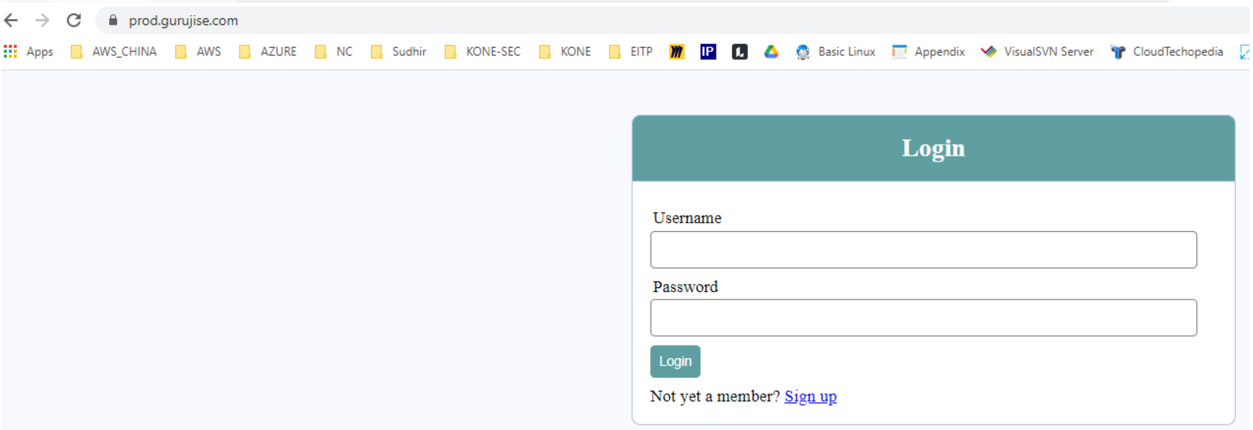
	Preced...	Path pattern	Origin or origin group	Viewer protocol policy	Cache policy name	Origin request policy name
○	0	/images/*	gurujise.com.s3.us-east-1.amazonaws.com	HTTP and HTTPS	658327ea-f89d-4fab-a63d-7e88639e58f6	
○	1	Default (*)	test-elb-388785549.us-east-1.elb.amazonaws.com	HTTP and HTTPS	658327ea-f89d-4fab-a63d-7e88639e58f6	

8. Make sure you have the below records created on Route-53 like below pointing to the CloudFront distribution

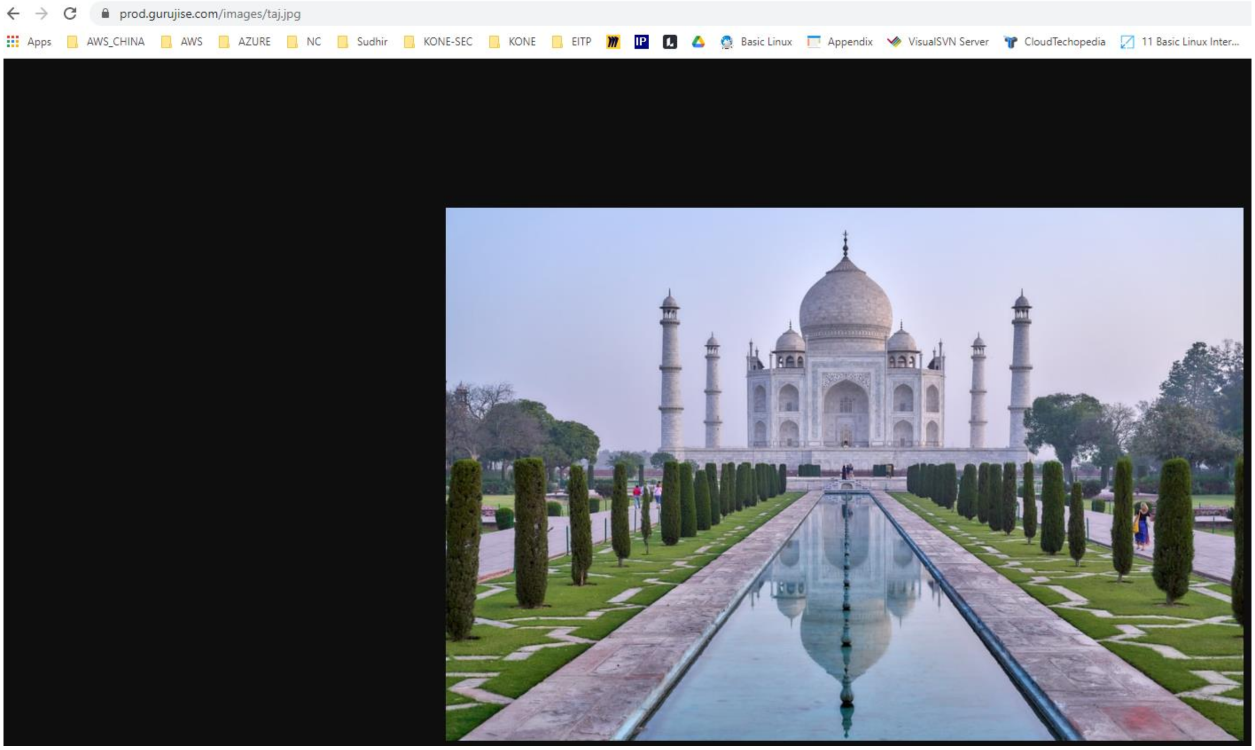


□	prod.gurujise.com	A	Simple	-	d2nj48jup30mxl.cloudfront.net.

9. Now you can test by accessing your custom DNS name "prod.gurujise.com" you it should route the traffic to EC2 instance as per the behaviors configuration



10. Now you can define the s3 images folder path along with the object name and try to access so that it will forward the traffic to S3 and server the image "prod.gurujise.com/images/taj.jpg"

11. 

Clean-up :

- After all above activities do not forget to clean-up all created resources to stop your unnecessary billings.

Pricing :

- https://aws.amazon.com/cloudfront/pricing/