

CloudFront



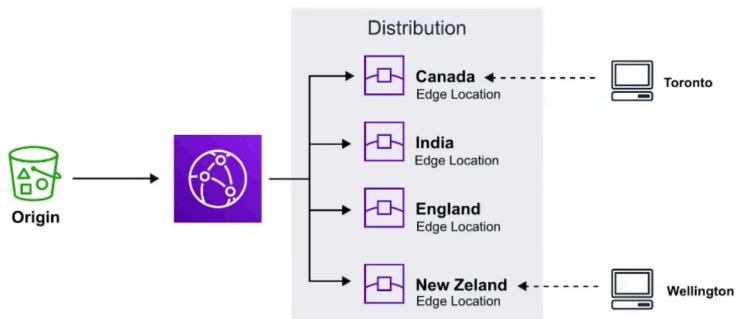
Content Distribution Network (CDN)
Creates cached copies of your website at various
Edge Locations around the world



Introduction to CloudFront

Content Delivery Network (CDN)

A CDN is a distributed network of servers which delivers web pages and content to users based on their **geographical location**, the **origin of the webpage**, and a **content delivery server**.



Can be used to **deliver an entire website** including static, dynamic and streaming

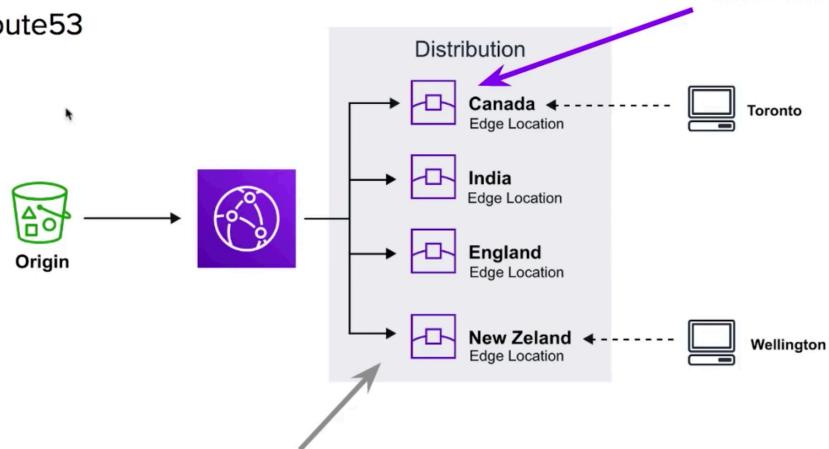
Requests for content are served from the nearest Edge Location for the best possible performance.



CloudFront - Core Components

Origin The location where all of original files are located. For example an S3 Bucket, EC2 Instance, ELB, or Route53

Edge Location The location where web content will be cached. This is different than an AWS Region or AZ



Distribution A collection of Edge locations which defines how cached content should behave



CloudFront – Distributions

A Distribution is a collection of Edge Locations.
You specific the Origin eg. S3, EC2, ELB, Route53

It replicates copies based on your **Price Class**

The screenshot shows the 'Distribution Settings' section of the CloudFront console. A dropdown menu for 'Price Class' is open, displaying three options: 'Use All Edge Locations (Best Performance)', 'Use Only U.S., Canada and Europe', and 'Use U.S., Canada, Europe, Asia, Middle East and Africa'. The first option is currently selected.

There are 2 types  of Distributions

1. Web (for websites)
2. RTMP (for streaming media)

Behaviours

Redirect to HTTPS, Restrict HTTP Methods, Restrict Viewer Access, Set TTLs

Invalidations

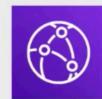
You can manually invalidate cache on specific files via Invalidations

Error Pages

You can serve up custom error pages .eg 404

Restrictions

You can use **Geo Restriction** to blacklist or whitelist specific countries

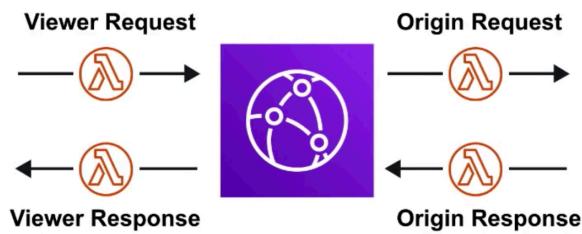


CloudFront - Lamdba@Edge

We use Lambda@Edge functions to **override the behaviour** of request and responses

The 4 Available Lambda@Edge Functions

1. **Viewer request** When CloudFront receives a request from a viewer
2. **Origin request** Before CloudFront forwards a request to the origin
3. **Origin response** When CloudFront receives a response from the origin
4. **Viewer response** Before CloudFront returns the response to the viewer

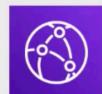


Lambda Function Associations

CloudFront Event	Lambda Function ARN	Include Body
Origin Request	arn:aws:lambda:us-east-1:65560434652	<input type="checkbox"/> X
Viewer Response	arn:aws:lambda:us-east-1:65560434652	<input type="checkbox"/> X
Viewer Request	arn:aws:lambda:us-east-1:65560434652	<input type="checkbox"/> +

Learn More





CloudFront – Protection

By Default a Distribution **allows everyone to have access.**

Original Identity Access (OAI)

A virtual user identity that will be used to give your CloudFront Distribution permission to fetch a private object

Restrict Viewer Access
(Use Signed URLs or
Signed Cookies)

Yes

No

If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content. For more information, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

In order to use Signed URLs or Signed Cookies you need to have an **OAI**

Signed URLs (Not the same thing as S3 Presigned URL)

A url with provides temporary access to cached objects

Signed Cookies

A cookie which is passed along with the request to CloudFront. The advantage of using a Cookie is you want to provide access to multiple restricted files. eg. Video streaming



CloudFront *CheatSheet*

- CloudFront is a CDN (Content Distribution Network). It makes website load fast by serving cached content that is nearby
- CloudFront distributes cached copy at **Edge Locations**
- Edge Locations aren't just not read-only, you can write to them eg. PUT objects
- **TTL** (Time to live) defines how long until the cache expires (refreshes cache)
- When you invalidate your cache, you are forcing it to immediately expire (refreshes cached data)
- Refreshing the cache **costs money because of transfer costs** to update Edge Locations
- **Origin** is the address of where the original copies of your files reside eg. S3, EC2, ELB, Route53
- **Distribution** defines a collection of Edge Locations and behaviour on how it should handle your cached content
- **Distributions** has 2 Types: **Web Distribution** (static website content) **RTMP** (streaming media)
- **Origin Identity Access (OAI)** is used access private S3 buckets
- Access to cached content can be protected via **SignedUrls** or **Signed Cookies**
- **Lambda@Edge** allows you to pass each request through a Lambda to change the behaviour of the response.