Aws CloudFront

CloudFront

- Content Delivery Network (CDN)
- Improves read performance, content is cached at the edge
- Improves users experience
- 216 Point of Presence globally (edge locations)
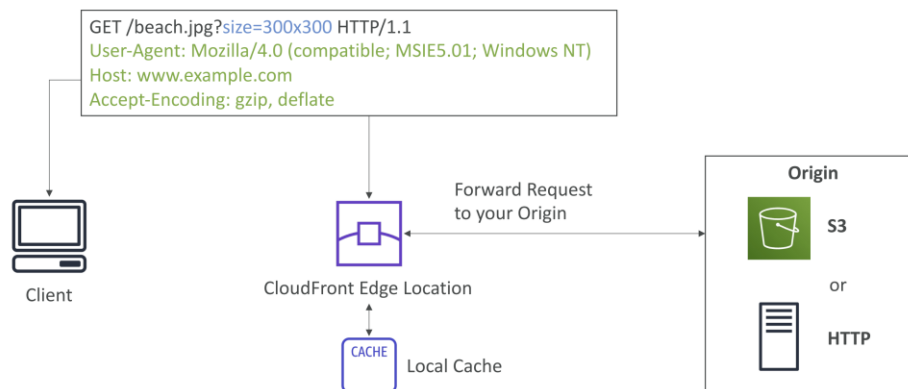- DDoS protection (because worldwide), integration with Shield, AWS Web Application Firewall
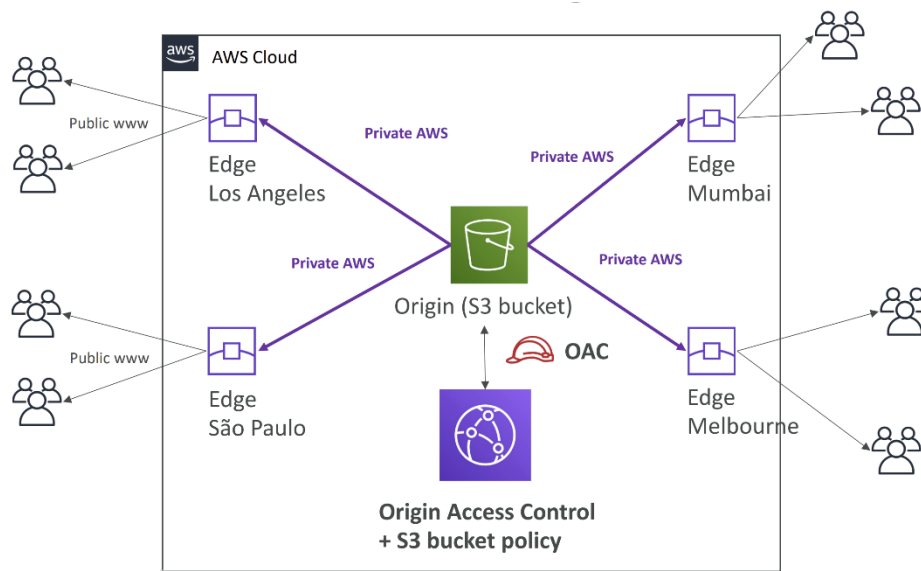
Source: https://aws.amazon.com/cloudfront/features/?nc=sn&loc=2

CloudFront – Origins

- **S3 bucket**
  - For distributing files and caching them at the edge
  - Enhanced security with CloudFront **Origin Access Control (OAC)**
  - OAC is replacing Origin Access Identity (OAI)
  - CloudFront can be used as an ingress (to upload files to S3)

- **Custom Origin (HTTP)**
  - Application Load Balancer
  - EC2 instance
  - S3 website (must first enable the bucket as a static S3 website)
  - Any HTTP backend you want

CloudFront at a high level

GET /beach.jpg?size=300x300 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE5.01; Windows NT)
Host: www.example.com
Accept-Encoding: gzip, deflate

Client

CloudFront Edge Location

CACHE Local Cache

Forward Request to your Origin

Origin

S3

or

HTTP

CloudFront – S3 as an Origin

CloudFront vs S3 Cross Region Replication

- CloudFront:
  - Global Edge network
  - Files are cached for a TTL (maybe a day)
  - Great for static content that must be available everywhere

- S3 Cross Region Replication:
  - Must be setup for each region you want replication to happen
  - Files are updated in near real-time
  - Read only
  - Great for dynamic content that needs to be available at low-latency in few regions
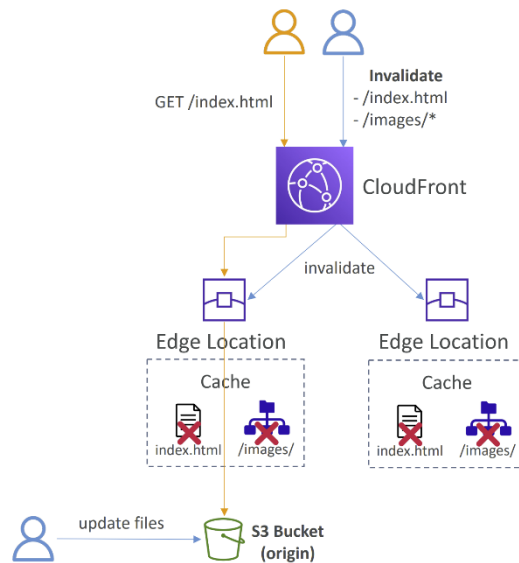
Lab: show how the CloudFront work

CloudFront Caching

- The cache lives at each CloudFront **Edge Location**
- CloudFront identifies each object in the cache using the **Cache Key**
- You want to maximize the Cache Hit ratio to minimize requests to the origin
- You can invalidate part of the cache using the **CreateInvalidation** API
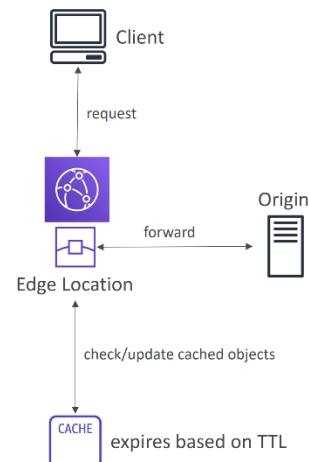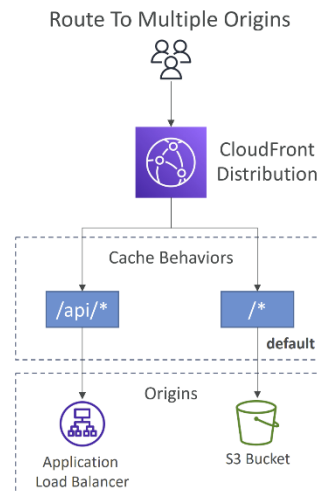
CloudFront – Cache Invalidations

- In case you update the back-end origin, CloudFront doesn't know about it and will only get the refreshed content after the TTL has expired
- However, you can force an entire or partial cache refresh (thus bypassing the TTL) by performing a **CloudFront Invalidation**
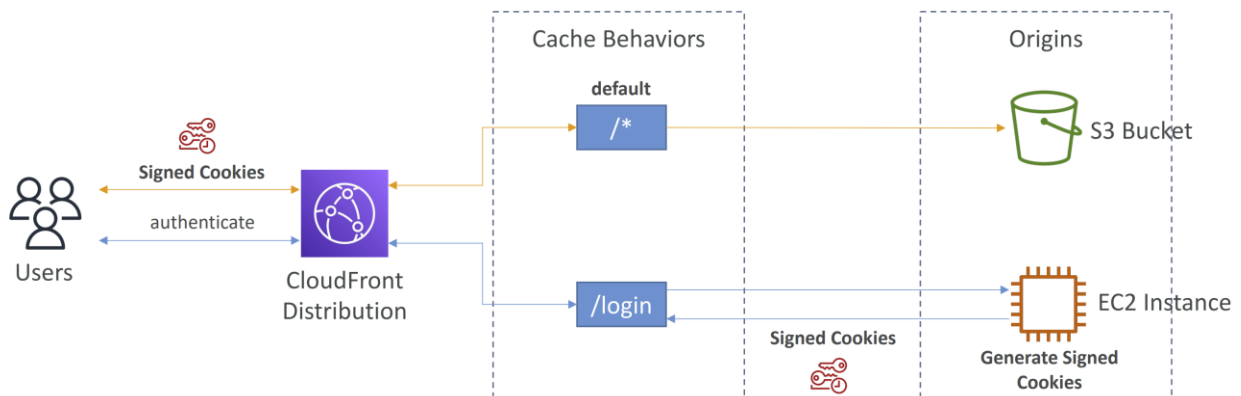- You can invalidate all files (*) or a special path (/images/*)

GET /index.html

Invalidate
- /index.html
- /images/*

CloudFront

invalidate

Edge Location

Edge Location

Cache

Cache

index.html /images/

index.html /images/

update files

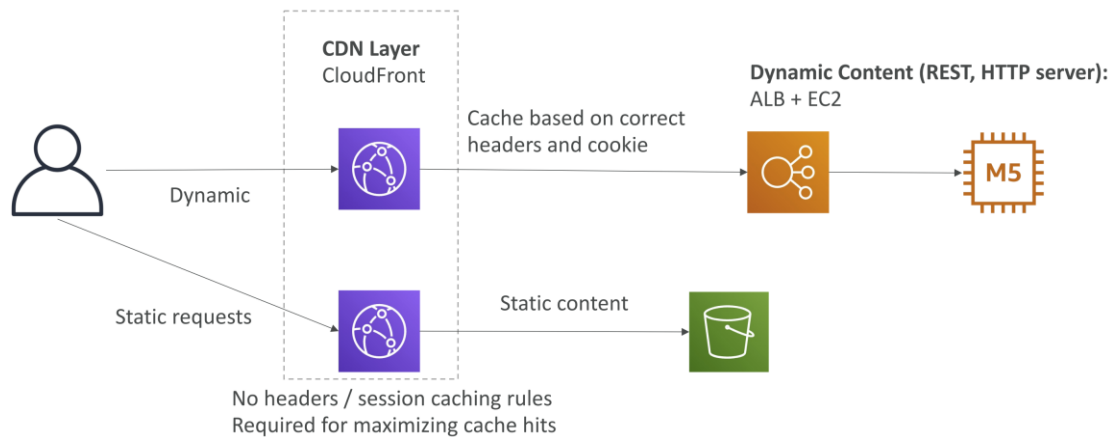**S3 Bucket (origin)**

CloudFront – Cache Behavior

- Configure different settings for a given URL path pattern
- Example: one specific cache behavior to **images/*.jpg** files on your origin web server
- Route to different kind of origins/origin groups based on the content type or path pattern
  - /images/*
  - /api/*
  - /* (default cache behavior)
- When adding additional Cache Behaviors, the Default Cache Behavior is always the last to be processed **and is always /***

Route To Multiple Origins

CloudFront Distribution

Cache Behaviors

/api/*   /*

default

Origins

Application Load Balancer

S3 Bucket

CloudFront – Cache Behaviors – Sign in Page

Cache Behaviors

Origins

default

/*

S3 Bucket

Signed Cookies

authenticate

Users

CloudFront Distribution

/login

EC2 Instance

Signed Cookies
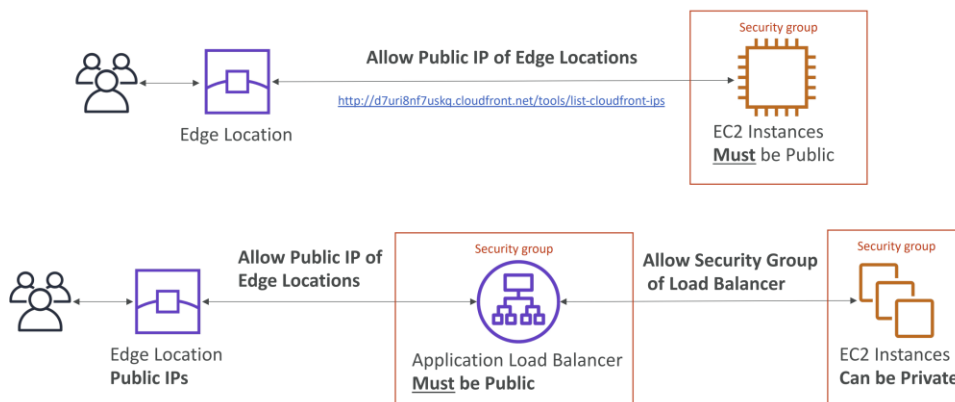
Generate Signed Cookies

CloudFront – Maximize cache hits by separating static and dynamic distributions.

Lab: show how invalidation work in CloudFront

CloudFront – ALB or EC2 as an origin

IP need to permit to for accessing the edge location
http://d7uri8nf7uskq.cloudfront.net/tools/list-cloudfront-ips

CloudFront Geo Restriction

- You can restrict who can access your distribution
  - Allowlist: Allow your users to access your content only if they're in one of the countries on a list of approved countries.
  - Blocklist: Prevent your users from accessing your content if they're in one of the countries on a list of banned countries.

- The "country" is determined using a 3rd party Geo-IP database
- Use case: Copyright Laws to control access to content

In geo set only access the website from Bangladesh now check the website from usa and we can see the page is not showing

CloudFront – Pricing

• CloudFront Edge locations are all around the world
• The cost of data out per edge location varies

Per Month	United States, Mexico, & Canada	Europe & Israel	South Africa, Kenya, & Middle East	South America	Japan	Australia & New Zealand	Hong Kong, Philippines, Singapore, South Korea, Taiwan, & Thailand	India
First 10TB	$0.085	$0.085	$0.110	$0.110	$0.114	$0.114	$0.140	$0.170
Next 40TB	$0.080	$0.080	$0.105	$0.105	$0.089	$0.098	$0.135	$0.130
Next 100TB	$0.060	$0.060	$0.090	$0.090	$0.086	$0.094	$0.120	$0.110
Next 350TB	$0.040	$0.040	$0.080	$0.080	$0.084	$0.092	$0.100	$0.100
Next 524TB	$0.030	$0.030	$0.060	$0.060	$0.080	$0.090	$0.080	$0.100
Next 4PB	$0.025	$0.025	$0.050	$0.050	$0.070	$0.085	$0.070	$0.100
Over 5PB	$0.020	$0.020	$0.040	$0.040	$0.060	$0.080	$0.060	$0.100

lower ————————————————————→ higher