**Section 10 ) Cloudfront ( is for caching globally)**

**Amazon CloudFront is a content delivery network offered by Amazon Web Services. Content delivery networks provide a globally-distributed network of proxy servers which cache content, such as web videos or other bulky media, more locally to consumers, thus improving access speed for downloading the content**

Note : if some user from usa want to access s3 in australia then cloudfront will cache data locally in usa and it will increase performance

Machine generated alternative text:
AWS CloudFront 
• Content Delivery Network (CDN) 
• Improves read performance, content 
is cached at the edge 
• 2 1 6 Point of Presence globally ( ge 
locations) 
• DDoS protection, integration w 
Shield, AWS Web Application 
Firewall 
• Can expose external H IT PS and 
Source: https://aws.amazon.com/cloudfront/features/?nc:sn&loc:2 
can talk to internal HIT PS backends 

Machine generated alternative text:
CloudFront — Origins 
• S3 bucket 
• For distributing files and caching them at the edge 
• Enhanced security with CloudFront Origin Access Identity (OAI) 
• CloudFront can be used as an i 
s (to load files to S3) 
• Custom Origin (HITP) 
• Application Load Balancer 
• EC2 instance 
• S3 website (must first enable the bucket as a static S3 website) 
• Any HTTP backend you want 

Machine generated alternative text:
CloudFront at a high level 
GET HTTP/I.I 
User-Agent: Mozilla/4.O (compatible; MSlE5.01; Windows NT) 
Host: www.example.com 
Accept-Encoding: gzip, deflate 
Origin 
or 
Client 
Fo rd Request 
to 'ur Origin 
Includes Query Strings 
Edge Location And Request Headers 
CACHE 
Local Cache 

Machine generated alternative text:
CloudFront — S3 
as an 
Private AWS 
Origin 
Private AWS 
private AWS 
eag 
Edge 
Mumbai 
Edge 
Melbour e 
Public www 
Public www 
eag 
AWS Cloud 
Edge 
Los Angeles 
Private AWS 
Edge 
Säo Paulo 
in (S3 buc 
Origin Access Identity 
+ S3 bucket policy 

Machine generated alternative text:
CloudFront 
Edge Location 
ALB or EC2 as an origin 
Security group 
Allow Public IP of Edge Locations 
EC2 Instances 
Must be Public 
Security group 
Allow Security Group 
of Load Balancer 
EC2 Instances 
Can be Private 
Security 
Allow Public IP of 
Edge Locations 
Edge Location 
Public IPS 
Application Load Balancer 
Must be Public 

Machine generated alternative text:
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 

**Cloudfront hands on**

|  |
| --- |
|  |
| Machine generated alternative text: AWS CloudFront Hands On  • We'll create an S3 bucket  • We'll create a CloudFront distribution  • We'll create an Origin Access I  • We'll limit the S3 bucket to b a -••-sed  nly using this identity      Step1:) **create a bucket and add files**  **Step 2) go to cloudfront**    **create distribution**    A distribution allows you to distribute content using a worldwide network of edge locations that provide low latency and high data transfer speeds    Machine generated alternative text: Create Distribution  Origin Settings  Origin Domain Name  Origin Path  Origin ID  Restrict Bucket Access  Origin Access Identity  Comment  Grant Read Permissions on  Bucket  S3-my-content-through-cloudfront-demo  @ Yes  o  No  @ Create a New Identity  o  Use an Existing Identity  access-identity-demo  @ Yes, Update Bucket Policy  o  No, I Will Update Permissions  O  O  O  O  0  Enter a description for the origin. This value lets you  distinguish multiple origins in the same distribution from  one another. The description for each origin must be  unique within the distribution.  If you want to require that users always access your  Amazon S3 content using CloudFront URLs, not  Amazon S3 URLs, click Yes. This is useful when you are  using signed URLs or signed cookies to restrict access  to your content. In the Help, see "Serving Private  Content through CloudFront".  Enter a comment that you can use to identify the new  origin access identity later, for example, "Static content  for example.com".    Machine generated alternative text: Viewer Protocol Policy  Allowed HTTP Methods  Field-level Encryption Config  Cached HTTP Methods  Cache and origin request  settings  Cache Policy  Origin Request Policy  o  HTTP and HTTPS  @ Redirect HTTP to HTTPS  o  HTTPS only  @ GET,  HEAD  o  GET, HEAD, OPTIONS  o  GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE  GET, HEAD (Cached by default)  @ Use a cache policy and origin request policy  o  Use legacy cache settings  Managed-CachingOptimized  View policy details  Learn More  View policy details  Learn More  O  O  O  O  O  Create a new policy  Create a new policy  O  O    **NOTE: it will take time to create may be it can take 10 minutes**  Note: while creating distribution we will select bucket name and tick bucket policy the it will create automatically    **Important**    An **Origin Access Identity** (OAI) is used for sharing private content via CloudFront. The OAI is a virtual user **identity** that will be used to give your CF distribution permission to fetch a private object from your **origin** server (e.g. S3 bucket).    **Note**    **Once cloudfront will create(distribution) then OAI (origin access identity will create automatically)**    Machine generated alternative text: Origin Access Identity  Delete  ENC21CSQBZ  Amazon S3 Canonical User ID  aa7f3da5e71 cce86834b3ddc27  Viewing 1 to 1 of 1 Items  Viewing 1 to 1 of 1 Items  Create Origin Access Identity  Comment  access-identity-demo  Edit    Bucket policy    Machine generated alternative text: lø  14  "Version'  "2ee8-1ø-17" ,  "policyForC10udFrontprivateContent"  " Statement "  "Sid" :  'Effect" :  "Allow" ,  "principal" .  "Action" :  "Resource" .  " s3 :GetObject" ,  arn:aws:s3  'arn: aws : lam: : cloudfront: user/CloudFront Origin Access Identity ENC21CSQB3MN9"  : : : my- content- through -cloudfront- demo/ * "    **Means anything that is coming from this user will allow:**    **AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity ENC2ICSQB3MN9"**    **Enter domain name now in url will be able to access it**    Machine generated alternative text: CloudFront Distributions  Delete  Enable  Disable  Comment  Create Distribution  Distribution Settings  Any State  Viewing: Any Delivery Method v  Origin  my-cont  Viewing 1 to 1 of 1 Items  Status State  Last Mod  Deploye Enable 2020-10-0  Viewing 1 to 1 of 1 Items  Domain Name  lc3cm1j14m96y.clou  CNAMEs  Delivery Method  e Web  E3191V940LWlBD      Cloudfront url : ----------------<https://d1c3cm1j14m96y.cloudfront.net/beach.jpg>      Cloudfront caching and caching invalidation hands on    Machine generated alternative text: CloudFront Caching  • Cache based on  • Headers  • Session Cookies  • Query String Parameters  • The cache lives at each CloudF  Edge  Location  • You want to maximize the cache h'  to minimize requests on the origiQ..  • Control the IT L (0 seconds to I  be set by the orign using the Cack-  Control header, Expires header...  • You can invalidate part of the cache using  the Createlnvalidation API  Client  Request  Origin  forwards  Edge Location  Check / Update cache  Based on Headers / Cookies  CACHE  Expire based on TTL  n    Note:  Cloudfront separate static and dynamic request    Machine generated alternative text: CloudFront — Maximize cache hits by  separating static and dynamic distributions  CDN Layer  CloudFront  ' Cacha•g—• correct  der•pnd cookie  Dynamic  Static content  Static requests  No headers / session caching rules  Required for maximizing cache hits  Dynamic Content (REST, HTTP server):  ALB + EC2      Hands on:    To see ttl setting :---- Click distribution/beahiour/edit    Machine generated alternative text: awS  Edit Behavior  cached HTTP Methods  Cache on Selected  R Headers  Minin-,um TTL  Maximum TTL  Default TTL  Forward Cookies  Query String ForwMdü•g and  Cach  Smooth  Restrict Viewer Access  (Uge URLS  Co m pre ss Objects Automatically  Resource  GET. HEAD (Cached by defa,tt)  86400  Nom v  Yes  Yes  O  O  O  O  O    NOTE:    Even though we will update file in s3 from cloudfront we will get same due to ttl time    **Solution : we need to do invalidate**    Machine generated alternative text: CloudFront Distributions E3191V940LWlBD  Cancel  obft  Invalidate  General  u  Origins  Create Invalidation  Distribution ID  Object Paths  Invalidating objects removes  or directory names. For mor  Create Invalidation  Invalidation ID  E3191V940LWlBD    Machine generated alternative text: CloudFront Distributions E3191V940LWlBD  Behaviors  Error Pages  Restrictions  Invalidations  Tags  General  Origins and Origin Groups  Invalidating objects removes them from CloudFront edge caches. A faster and less expensive method is to use versioned object  or directory names. For more information, see Invalidating Objects in the Amazon CloudFront Developer Guide.  Create Invalidation  Invalidation ID  Details  Copy  Status  O In Progress  Viewing 1 to 1  Date  2020-10-06 12:10 UTC+5:30  13KKNUQK46UIPX    **Now after invalidation anything updated in s3 bucket will update here also** |
| Cloudfront security    Machine generated alternative text: CloudFront Geo Restriction  • You can restrict who can access your distribution  • Whitelist: Allow your users to access your content only if they're in one of the  countries on a list of approved countries.  • Blacklist: Prevent your users from accessing your content if they're in one of the  countries on a blacklist of banned countries.  • The "country" is determined using a 3rd party Geo-IP database  • Use case: Copyright Laws to control access to content    Machine generated alternative text: CloudFront and I-ITTPS  • Viewer Protocol Policy:  • Redirect HTTP to HTTPS  • Or use HITPS only  • Origin Protocol Policy (HTTP  . only  • Or Match Viewer  H-rrp & H-rrps  • Note:  • S3 bucket "websites" dont support H VPS  Client  Viewer Protocol Policy  Edge Location  Origin Protocol Policy  Origin    NOTE:  **Security 1)**  For security we use OAI(origin access identity) and this is used to access to s3 bucket  **Security 2)**  **Beahviour/edit**  **Viewer protocol policy**  Machine generated alternative text: Default Cache Behavior Settings  O  O  O  O  Path Pattern  Origin or Origin Group  Viewer Protocol Polic  Allowed HTTP Methods  Default (*)  S3-my-content-through-cloudfront-demo  and HTTPS  @ Redirect HTTP to HTTP  o  HTTPS only  o  GET, HEAD, OPTIONS  o  GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE  **Security 3)**  **We can refer here whitelist or blacklist of country**  Machine generated alternative text: Edit Geo-Restrictions  O  O  O  Add  Remove  Cancel  Yes, Edit  Geo-Restriction Settings  Enable Geo-Restriction  Restriction Type  Countries  @Yes  ON0  itelist  O Blacklist  AF AFGHANISTAN  AX  - ALAND ISLANDS  AL ALBANIA  DZ ALGERIA  AS AMERICAN SAMOA  AD ANDORRA  **Whatever will add only allow people of that country to access s3 bucket by cloudfront**    **Cloudfront signed URL cookies**  **Requirement :**  **Want to give cloudfront access to premium people for this we need to use signed URL**  Machine generated alternative text: CloudFront Signed URL / Signed Cookies  • You want to distribute paid shared content to premium users over the world  • We can use CloudFront Signed URL / Cookie.VVe attach a policy with:  • Includes URL expiration  • Includes IP ranges to access the data m  • Trusted signers (which AWS acco ts  • How long should the URL be v id  signed URLs)  • Shared content (movie, music): make it ort few minutes)  • Private content (private to the it last for years  • Signed URL z: access to individual files (one signed URL per file)  • Signed Cookies access to multiple files (one signed cookie for many files)    Machine generated alternative text: CloudFront Signed URL Diagram  Amazon CloudFront  6)  Signed URL  Client  Amazon S3  O  Object  Authentication  + Authorization  Return  Signed URL  Use AWS SDK  Generate Signed URL  Application    Machine generated alternative text: CloudFront Signed URL vs  S3 Pre-Signed URL  • CloudFront Signed URL'  • Allow access to a path, no matter  the origin  • Account wide key-pair, only the root  can manage it  • Can filter by IR path, date, expiration  • Can leverage caching features  Origin  Client  Edge location  • S3 Pre-Signed URL'  • Issue a request as the person who  pre-signed the URL  • Uses the IAM key of the signing  IAM principal  • Limited lifetime  Client    CloudFront Signed URL are commonly used to distribute paid content through dynamic CloudFront Signed URL generation.    S3 CRR ( cross region replication) allows you to replicate the data from one bucket in a region to another bucket in another region |