AWS CloudFront

Cloud Front

- Amazon CloudFront is a content delivery web service.

- It integrates with other Amazon Web Services products to give developers and businesses an easy way to distribute content to end users with low latency, high data transfer speeds, and no minimum usage commitments.

- In Amazon CloudFront, your content is organized into distributions.

- A distribution specifies the location or locations of the original version of your files.

- A distribution has a unique CloudFront.net domain name (e.g. abc123.cloudfront.net) that you can use to reference your objects through the global network of edge locations.

- If you wish, you can also map your own domain name (e.g. www.example.com) to your distribution.

- You can create distributions to either download your content using the HTTP or HTTPS protocols, or stream your content using the RTMP protocol.

Cloud Front

Map courtesy of the University of Texas Libraries, The University of Texas at Austin

Cloud Front Process

- Store the original versions of your files on one or more origin servers.

- An origin server is the location of the definitive version of an object.

- Origin servers could be other Amazon Web Services – an Amazon S3 bucket, an Amazon EC2 instance, or an Elastic Load Balancer – or your own origin server.

- Create a distribution to register your origin servers with Amazon CloudFront through a simple API call or the AWS Management Console.

- When configuring more than one origin server, use URL pattern matches to specify which origin has what content. You can assign one of the origins as the default origin.

Cloud Front Process

- Use your distribution's domain name in your web pages, media player, or application.

- When end users request an object using this domain name, they are automatically routed to the nearest edge location for high performance delivery of your content.

- Pay only for the data transfer and requests that you actually use.

- Amazon CloudFront's availability is backed with the Amazon CloudFront Service Level Agreement.

The Amazon CloudFront Global Edge Network

- To deliver content to end users with lower latency, Amazon CloudFront uses a global network of edge locations for content delivery.

- Amazon CloudFront edge locations:
  - 14 in US
  - 10 in Europe
  - 9 in Asia
  - 2 in Australia
  - 2 in South America

Amazon Cloud Front Distributions

- To deliver content through Amazon CloudFront, you create a distribution.

- There are two types of distributions you can create
  - web distributions for HTTP/HTTPS
  - TMP Distributions for RTMP and its variants.

- Each distribution has a unique domain name that you can use in your web application.

- An example of an Amazon CloudFront domain name is abc123.cloudfront.net.

Web Distributions for HTTP Delivery

- An Amazon CloudFront web distribution can be used as a content delivery network to deliver your content using the HTTP or HTTPS protocols.

- Amazon CloudFront identifies the origin servers that hold the original version of your content by using URL matching rules you configure for each distribution (e.g., all requests that match /images/* could use your Amazon S3 as the origin, all requests matching *.php could use your Amazon EC2 instance as the origin, etc.).
  - To work with web distribution
  - You place the original version of your objects in your origin servers.
  - You call the Create Distribution API, which will return your distribution's domain name.
  - You create links to your objects in your web site or web application using the domain name.

Web Distributions for HTTP Delivery

- When a viewer requests a web page or content using that domain name, Amazon CloudFront determines the best edge location to serve your content.

- If an edge location doesn't have a copy of the file requested by the viewer, Amazon CloudFront will pull a copy from the origin server and hold it at the edge location so it's available for future requests.

- Content can be delivered using either the HTTP or HTTPS protocol.

- By default, your distribution will accept requests on either protocol.

- However, if you want your content delivered only over an HTTPS connection, you can configure your distributions to only accept requests that come over HTTPS.

- When Amazon CloudFront needs to get a file from the origin server, it will use the same protocol that was used for the end user request.

- For example, if an end user requests a file using HTTPS that is not already in an edge location, Amazon CloudFront will use HTTPS to get the file from the origin.
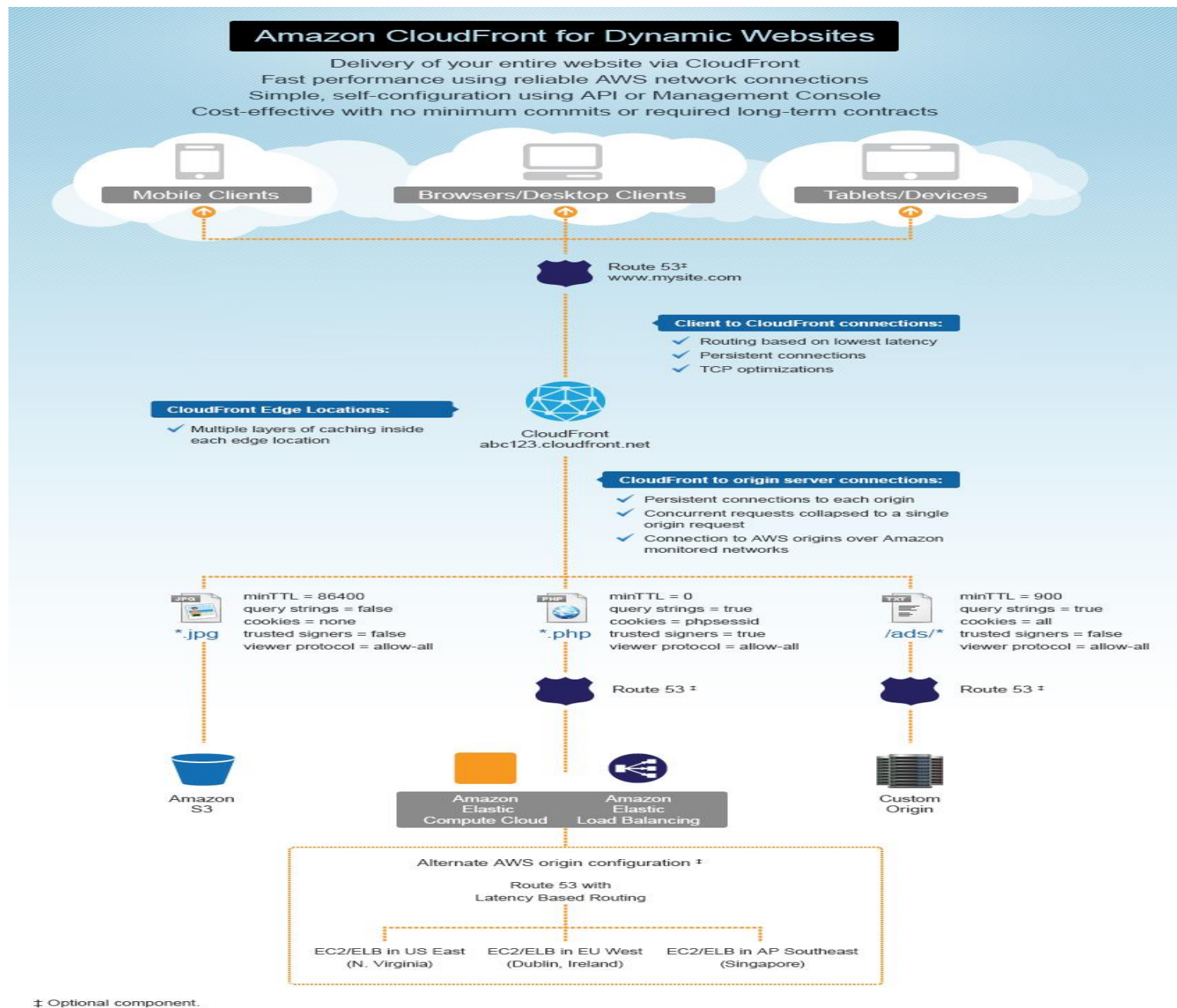
Web Distributions for HTTP Delivery

- Web distributions support the following HTTP methods: GET, HEAD, POST, PUT, DELETE, OPTIONS, and PATCH.

- By default, the response to GET and HEAD methods will be cached at CloudFront edge locations. You may choose to configure your Amazon CloudFront distribution to cache the response for the OPTIONS request.

- Other HTTP methods (POST, PUT, DELETE, and PATCH) are not cached and simply proxied to the origin by Amazon CloudFront edge locations.

Cache Behaviors

- A cache behavior is the set of rules you configure for a given URL pattern based on file extensions, file names, or any portion of a URL path on your website (e.g., *.jpg). You can configure multiple cache behaviors for your web distribution.

- Amazon CloudFront will match incoming viewer requests with your list of URL patterns, and if there is a match, the service will honor the cache behavior you configure for that URL pattern.

- Each cache behavior can include the following Amazon CloudFront configuration values: origin server name, viewer connection protocol, minimum expiration period, query string parameters, and trusted signers for private content.

Origin Servers

- You can configure one or more origin servers for your Amazon CloudFront web distribution.

- Origin servers can be an AWS resource, such as Amazon S3, Amazon EC2, Elastic Load Balancing, or a custom origin server outside of AWS.

- Amazon CloudFront will request content from each origin server by matching the URLs requested by the viewer with rules you configure for your distribution.

- This feature allows you the flexibility to use each AWS resource for what it's designed for – Amazon S3 for storage, Amazon EC2 for compute, etc. – without the need to create multiple distributions and manage multiple domain names on your website.

Amazon CloudFront for Dynamic Websites

Delivery of your entire website via CloudFront
Fast performance using reliable AWS network connections
Simple, self-configuration using API or Management Console
Cost-effective with no minimum commits or required long-term contracts

Mobile Clients

Browsers/Desktop Clients

Tablets/Devices

Route 53‡
www.mysite.com

Client to CloudFront connections:
- ✓ Routing based on lowest latency
- ✓ Persistent connections
- ✓ TCP optimizations

CloudFront Edge Locations:
- ✓ Multiple layers of caching inside each edge location

CloudFront
abc123.cloudfront.net

CloudFront to origin server connections:
- ✓ Persistent connections to each origin
- ✓ Concurrent requests collapsed to a single origin request
- ✓ Connection to AWS origins over Amazon monitored networks

*.jpg	*.php	/ads/*
minTTL = 86400	minTTL = 0	minTTL = 900
query strings = false	query strings = true	query strings = true
cookies = none	cookies = phpsessid	cookies = all
trusted signers = false	trusted signers = true	trusted signers = false
viewer protocol = allow-all	viewer protocol = allow-all	viewer protocol = allow-all

Route 53 ‡

Route 53 ‡

Amazon
S3

Amazon
Elastic
Compute Cloud

Amazon
Elastic
Load Balancing

Custom
Origin

Alternate AWS origin configuration ‡

Route 53 with
Latency Based Routing

EC2/ELB in US East
(N. Virginia)

EC2/ELB in EU West
(Dublin, Ireland)

EC2/ELB in AP Southeast
(Singapore)

‡ Optional component.

Private Content

- You can use Amazon CloudFront's private content feature to control who is able to access your content.

- This optional feature lets you use Amazon CloudFront to deliver valuable content that you prefer not to make publicly available by requiring your users to use a signed url or have a signed HTTP cookie when requesting your content.

Device Detection

- Amazon CloudFront can determine whether the end user request came from a Desktop, Tablet, Smart TV, or Mobile device and pass that information in the form of new HTTP Headers to your origin server - Amazon EC2, Elastic Load Balancing, or your custom origin server.

- Amazon CloudFront will also cache the different versions of the content at that edge location.

Geo Targeting

- Amazon CloudFront can also detect the country where the end users are accessing your content from.

- Amazon CloudFront can then pass the information about the country in a new HTTP header to your custom origin server.

- Your origin server can generate different versions of the content for users in different countries and cache these different versions at the edge location to serve subsequent users visiting your website from the same country.

Cross Origin Resource Sharing (CORS)

- Amazon CloudFront may be configured to forward the Origin header value so your origin server (Amazon S3 or a custom origin) can support cross-origin access via CORS (Cross-Origin Resource Sharing).

- CORS defines a way for client web applications that are loaded in one domain to interact with resources in a different domain.

Viewer Connection Protocol

- Content can be delivered to viewers using either the HTTP or HTTPS protocol.

- By default, your web distribution will accept requests on either protocol. However, if you want all your content or certain URLs delivered only over an HTTPS connection, you can configure your distribution to only accept requests that come over HTTPS for that content.

- You can configure this feature separately for each URL pattern in your web distribution as part of the cache behavior for that URL pattern.

Protocol Detection

- You can configure Amazon CloudFront to include the protocol (HTTP vs HTTPS) of your end user's request as part of the cache key to uniquely identify an object in cache.

- This allows you to customize your content based on the protocol your end users are using to access your content.

Custom SSL

- Custom SSL certificate support lets you deliver content over HTTPS using your own domain name and your own SSL certificate.

- This gives visitors to your website the security benefits of CloudFront over an SSL connection that uses your own domain name in addition to lower latency and higher reliability.

- You can also configure CloudFront to use HTTPS connections for origin fetches so that your data is encrypted end-to-end from your origin to your end users.

- Configuring Custom SSL certificate support is easy; you don't need to learn any proprietary code or hire any consultants to configure it for you.

Geo Restriction

- Geo Restriction or Geoblocking lets you choose the countries in which you want to restrict access to your content.

- By configuring either a whitelist or a blacklist of countries you can control delivery of your content through Amazon CloudFront only to countries where you have the license to distribute.

- Amazon CloudFront lets you configure a Minimum time-to-live (Min TTL), a Maximum TTL (Max TTL) and a Default TTL to specify how long CloudFront caches your objects in edge locations.

- Amazon CloudFront uses the expiration period that your origin sets on your files (through Cache-Control headers) to determine whether CloudFront needs to check the origin for an updated version of the file.

Query String Parameters

- Query string parameters are often used to return customized content generated by a script running on the origin server.

- By default, Amazon CloudFront does not forward query string parameters (e.g., "?x=1&y=2") to the origin

- In addition, the query string portion of the URL is ignored when identifying a unique object in the cache.

Gzip

- You can configure CloudFront to automatically apply GZIP compression when browsers and other clients request a compressed object with text and other compressible file formats.

- This means that if you are already using Amazon S3, CloudFront can transparently compress this type of content.

HTTP Cookie Support

- Amazon CloudFront supports delivery of dynamic content that is customized or personalized using HTTP cookies.

- To use this feature, you specify whether you want Amazon CloudFront to forward some or all of your cookies to your custom origin server.

Forward Headers to Origin

- You can use Amazon CloudFront to forward all (or a whitelist of) request headers to your origin server.

- These headers contain information such as the device used by your visitors or the country from which they accessed your content.

- For example, if you are hosting multiple websites on the same web server, you can configure Amazon CloudFront to forward the Host header to your origin.

- When your origin returns different versions of the same object based on the values in the Host header, Amazon CloudFront will cache the objects separately based on those values.

Add or Modify Request Headers Forwarded From CloudFront to Origin

- You can configure Amazon CloudFront to add custom headers, or override the value of existing headers, to requests forwarded to your origin.

- You can use these headers to help validate that requests made to your origin were sent from CloudFront; you can even configure your origin to only allow requests that contain the custom header values you specify.

Default Root Object

- You can specify a default file (e.g., index.html) that will be served for requests made for the root of your distribution without an object name specified – for instance, requests made to http://abc123.cloudfront.net/ alone, without a file name.

Object Versioning and Cache Invalidation

- You have two options to update your files cached at the Amazon CloudFront edge locations. You can use object versioning to manage changes to your content.

- To implement object versioning, you create a unique filename in your origin server for each version of your file and use the file name corresponding to the correct version in your web pages or applications.

- With this technique, Amazon CloudFront caches the version of the object that you want without needing to wait for an object to expire before you can serve a newer version.

Access Logs

- You can choose to receive more information about the traffic delivered or streamed by your Amazon CloudFront distribution by enabling access logs.

- Access logs are activity records that show you detailed information about each request made for your content.

- CloudFront access are automatically delivered multiple times per hour and the logs within those files will typically be available within an hour of your viewers requesting that object.

CloudFront Usage Charts

- Amazon CloudFront Usage Charts let you track trends in data transfer and requests (both HTTP and HTTPS) for each of your active CloudFront Web distributions.

- These charts show your usage from each CloudFront region at daily or hourly granularity, going back up to 60 days. They also include totals, average, and peak usage during the time interval selected.

CloudFront Monitoring & Alarming using Amazon CloudWatch

- You can monitor, alarm and receive notifications on the operational performance of your Amazon CloudFront distributions using Amazon CloudWatch, giving you more visibility into the overall health of your web application.

- CloudFront automatically publishes six operational metrics, each at 1-minute granularity, into Amazon CloudWatch.

- You can then use CloudWatch to set alarms on any abnormal patterns in your CloudFront traffic.

CloudFront Cache Statistics Reports

- loudFront Cache Statistics charts show you a variety of information about your CloudFront distributions including:

  - Total Requests: Shows the total number of requests for all HTTP status codes.

  - Percentage of Viewer Requests by Result Type: Shows hits, misses, and errors as a percentage of total viewer requests.

  - Bytes Transferred to Viewers: Shows the total number of bytes served to viewers and the bytes served just for cache misses.

  - HTTP Status Codes: Shows viewer requests by HTTP status code – 2xx, 3xx, 4xx, and 5xx.

  - Percentage of GET Requests that Didn't Finish Downloading: Shows the percentage of total requests that didn't finish downloading the requested object.

CloudFront Popular Objects Report

- he Popular Objects Report shows request count, cache hit and cache miss counts, as well as error rates for the 50 most popular objects during the specified period.

- This helps you understand which content is most popular among your viewers, or identify any issues (such as high error rates) with your most requested objects.

CloudFront Viewers Report

- The Viewers Report shows the countries where your end users are located as well as the browsers and operating systems they use. For all these reports you can also display the trend over time. The Viewer Reports include the following:

  - Locations: shows the top 50 countries where your end users are accessing the content that you are distributing using Amazon CloudFront. You can also use the report to see the states and territories for end users in the United States.
  - Browsers: shows the top 10 browsers that your end users are using to access your content. The report shows the top 10 browsers by name, or by name and version.

  - Operating system: shows the top 10 operating system that your end users are accessing your content from. The report shows the top 10 version by name, or by name and version.
  - Devices: shows you how many requests come from mobile, tablets, desktops, and smart TVs during a specified time period.

CloudFront Top Referrers Report

- The Top Referrers report shows you the top 25 domains that referred viewers to your website.

- These top referrers can be search engines, other websites that link directly to your objects, or your own website.

- You can display the Top Referrers report for any date range in the previous 60 days.

CloudTrail Logs

- You can get a history of all CloudFront API calls made on your account by enabling AWS CloudTrail from the AWS Management Console.

- AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you for security, operational or compliance auditing.

Zone Apex Support

- You can use CloudFront to deliver content from the root domain, or "zone apex" of your website.

- For example, you can configure both http://www.example.com and http://example.com to point at the same CloudFront distribution, without the performance penalty or availability risk of managing a redirect service.

Using Amazon CloudFront with AWS WAF to Protect Your Web Applications

- AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications.

- AWS WAF allows you to create rules based on IP addresses, HTTP headers, and custom URIs. Using these rules, AWS WAF can block, allow, or monitor (count) web requests for your web application.

RTMP Distributions for On-Demand Media Delivery

- Amazon CloudFront lets you create "RTMP distributions" to deliver your rich media content in a different way than other Amazon CloudFront distributions.

- RTMP distributions deliver content to end users in real time – the end-users watch the bytes as they are delivered. To do this, RTMP distributions use the Real Time Messaging Protocol (RTMP) and several of its variants, instead of the HTTP or HTTPS protocols used by other Amazon CloudFront distributions.

- Amazon CloudFront uses Adobe's Flash Media Server 3.5 to power its RTMP distributions.

Using Amazon CloudFront with Amazon Route 53

- Amazon Route 53 is AWS's reliable and cost-effective Domain Name System (DNS) web service.

- Similar to Amazon CloudFront, Route 53 is designed to be fast and answers DNS queries with low latency by using a global network of DNS servers.

- You can use Amazon Route 53 to map custom domain names (including the zone apex, i.e. example.com without the www) to your Amazon CloudFront distributions using a feature called Alias record. Route 53 doesn't charge for queries to Alias records that are mapped to a CloudFront distribution.

Using Amazon CloudFront with Amazon S3

- Amazon CloudFront is optimized to use Amazon S3 as its origin server to store the original versions of your static files.

- Amazon CloudFront works well for delivery of static objects that are frequently accessed – "popular" objects.

- With Amazon CloudFront, copies of your popular objects are cached in a network of edge locations around the world.

- Because these edge locations are close to your viewers, your objects can be served more quickly than if they were served from one of Amazon S3's central locations.

- This improves your viewers' experience for frequently accessed static content: they get lower latency and faster data transfer rates.

- Delivering your popular objects using an Amazon CloudFront edge location can also reduce your costs, as Amazon CloudFront's rates for data transfer are lower than Amazon S3's at higher usage tiers.

Using Amazon CloudFront with Amazon EC2 and Elastic Load Balancing

- Amazon EC2 provides compute capacity in the AWS cloud.

- When using Amazon EC2 as your Amazon CloudFront origin server, you get the benefit of working with the same set of tools to configure and manage the delivery of your entire web application.

- In addition, Amazon EC2 offers the same pay-as-you-go and pay-for-use pricing model as Amazon CloudFront does.

- Plus, the routes between Amazon CloudFront edge locations and Amazon EC2 data centers are constantly monitored and optimized for performance and availability.

- Any issues with these network routes are quickly detected and fixed or viewers are automatically routed to another Amazon monitored network route, minimizing impact to viewers of your applications.

Cloud Front Limits

- By default, your distributions support peak data transfer speeds of 10 gigabits per second

- peak request rates of 15,000 requests per second.