AMAZON CLOUDFRONT

MẠNG PHÂN PHỐI NỘI DUNG (CDN)

Giải pháp CDN toàn cầu để tăng tốc phân phối nội dung web đến người dùng toàn thế giới

Hơn 600+ Edge Locations

Bảo mật tích hợp

Tăng tốc độ tải lên đến 80%

25 tháng 10, 2025

CloudFront Overview

Định nghĩa

Amazon CloudFront là CDN (Content Delivery Network) của AWS, được thiết kế để tăng tốc phân phối nội dung web, cả tĩnh và động, đến người dùng toàn cầu.

Ưu điểm chính

Tăng tốc độ

Cache nội dung tại Edge Locations, giảm thiểu độ trễ

Phạm vi toàn cầu

Hơn 600+ Edge Locations across 50+ countries

Bảo mật

DDoS protection, AWS WAF integration, SSL/TLS encryption

Khả năng mở rộng

Tự động thích ứng với lưu lượng truy cập toàn cầu

Ví dụ thực tế

Tình huống: Website thương mại điện tử toàn cầu với khách hàng ở Việt Nam, Nhật, và Mỹ.

Không dùng CloudFront

Tất cả request về region Singapore

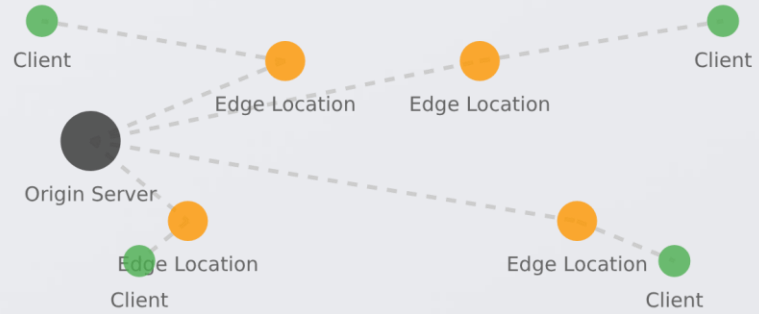
Latency cao, tốc độ chậm

→

Dùng CloudFront

Request được hướng đến Edge Location gần nhất

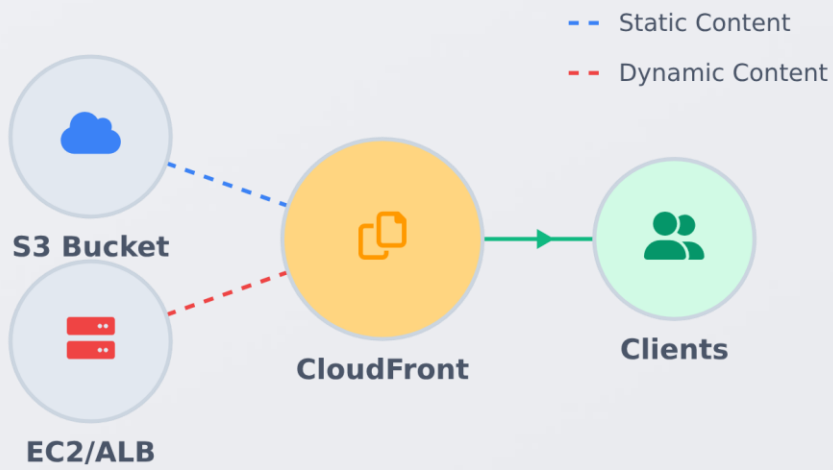
Nhanh hơn ~80% so với không dùng



CloudFront Origins

Định nghĩa

Origin trong CloudFront là nơi CloudFront retrieves (lấy) bản gốc của nội dung. Đây có thể là Amazon S3 bucket, HTTP server, hoặc các dịch vụ AWS khác.



Các loại Origin

S3 Bucket

Dùng để lưu trữ nội dung tĩnh như hình ảnh, video, HTML, CSS, JS

ALB / EC2 Instance

Dùng cho nội dung động cần xử lý bởi web server hoặc application

Custom HTTP Origin

Bất kỳ HTTP server nào ở ngoài AWS hoặc dịch vụ AWS khác exposing HTTP endpoint

Ví dụ thực tế

Dự án: Một website thương mại điện tử lưu trữ hình ảnh sản phẩm trong S3 và API backend chạy trên EC2.

S3 Bucket
Hình ảnh sản phẩm

→

CloudFront
Phân phối nội dung

→

EC2/ALB
API backend

CloudFront vs S3 Cross Region Replication

Tiêu chí	CloudFront	S3 Cross-Region Replication
Phân phối	Global Edge Network (PoPs)	Region-to-Region
Cập nhật	Cache theo TTL	Gần như real-time
Dùng cho	Nội dung tĩnh	Sao lưu / đồng bộ dữ liệu

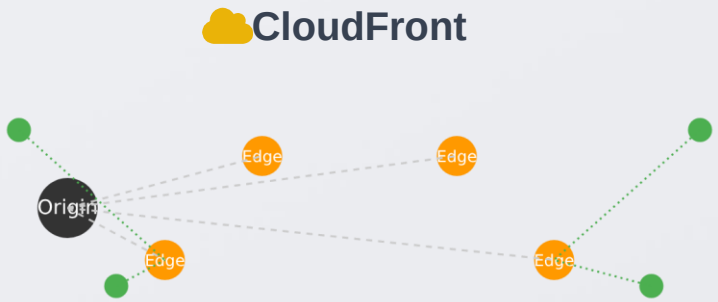
Ví dụ thực tế

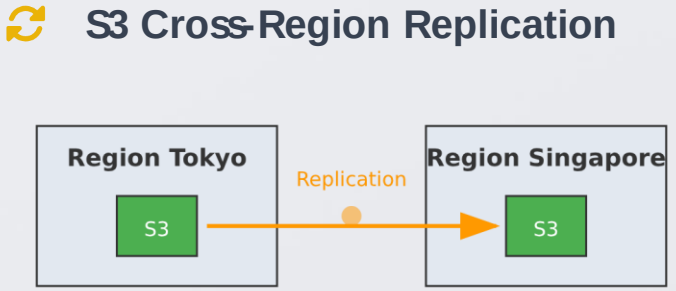
Trang Blog

Một trang blog chỉ cần cache nội dung HTML vài giờ (CloudFront) để tăng tốc độ tải cho người đọc toàn cầu.

Dữ liệu người dùng

Dữ liệu người dùng thì cần đồng bộ liên tục giữa Tokyo và Singapore (S3 CRR) để đảm bảo tính nhất quán.





CloudFront Caching

Cơ chế Cache

CloudFront cache tồn tại tại Edge Locations, giúp tăng tốc độ phân phối nội dung bằng cách lưu trữ bản sao của nội dung gần người dùng.

Mục tiêu chính:

Tăng Cache Hit Ratio

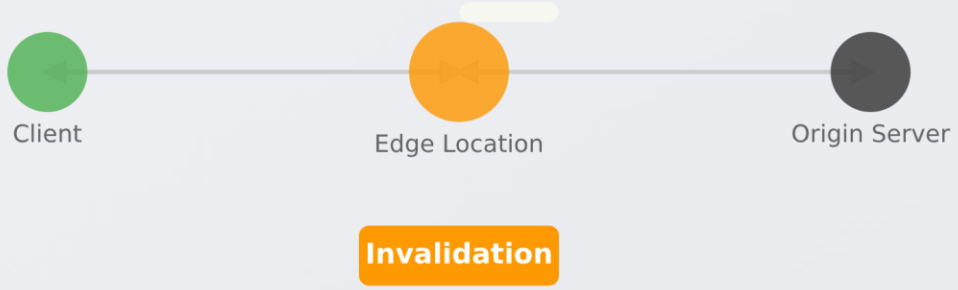
Tỷ lệ phần trăm request được phục vụ trực tiếp từ cache thay vì phải fetch từ origin server.

Cache Invalidation

Khi nào cần dùng: Khi nội dung gốc đã thay đổi và bạn muốn cập nhật cache ngay lập tức.

Lưu ý: Content cached tại Edge Locations sẽ remain trong một thời gian định trước (Time-to-Live), cần invalidation nếu muốn cập nhật sớm.

```
# Ví dụ lệnh AWS CLI để invalidation cache
aws cloudfront create-invalidation    --paths "/logo.png"
```



Time-to-Live (TTL)

Thời gian cache tồn tại trước khi hết hạn, có thể cấu hình theo từng cache behavior.

Origin Server

Nơi CloudFront retrieves nội dung gốc, có thể là S3, EC2, ALB hoặc custom HTTP origin.

Edge Locations

Network of strategically located servers cache content closer to end-users.

Cache Invalidation API

API để remove object khỏi cache across all Edge Locations, force fetch mới từ origin.

CloudFront Cache Key

Định nghĩa

Cache Key là định danh duy nhất mà CloudFront sử dụng để xác định xem object đã yêu cầu có đang có trong cache tại Edge Location hay không.

Thành phần mặc định

Hostname

Tên miền của request

URL Path

Đường dẫn của file yêu cầu

Cấu hình

Cache Policy

Cấu hình thông qua Cache Policy để bao gồm thêm Query String, Header, Cookie

Ví dụ

```
aws cloudfront create-cache-policy --cache-policy-config
file://policy.json
```

Ví dụ: Xử lý đa ngôn ngữ

Tình huống: Website có hai phiên bản ngôn ngữ:

https://www.example.com/page

https://www.example.com/page?lang=vi

Không bao gồm query string

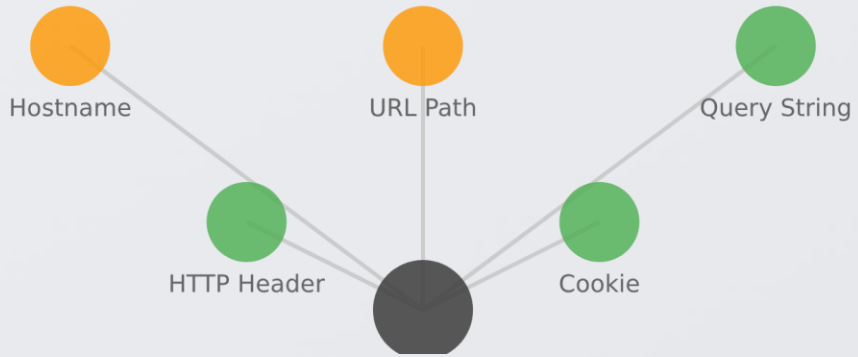
CloudFront sẽ coi hai URL là giống nhau

→ Có thể trả về sai ngôn ngữ

Bao gồm lang trong Cache Key

CloudFront tạo cache riêng cho mỗi ngôn ngữ

→ Đúng ngôn ngữ cho từng user



Cache Invalidation

Định nghĩa

Cache Invalidation là quá trình xóa một hoặc toàn bộ cache trước khi hết hạn TTL (Time-to-Live), đảm bảo người dùng nhận được nội dung mới nhất từ origin server.

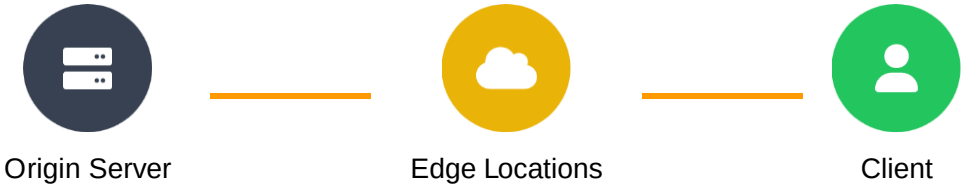
Khi nào cần sử dụng

- Khi nội dung gốc trên origin server đã thay đổi
- Để cập nhật nhanh chóng nội dung mới mà không chờ TTL hết hạn
- Đối với file quan trọng như index.html, logo.png, config.js...

Lệnh AWS CLI

```
# Xóa cache file logo.png
aws cloudfront create-invalidation     --paths
"/logo.png"
```

Quy trình invalidation



1. Upload file mới lên S3
logo.png v2

2. Create Invalidation
Xóa cache tại Edge

3. Next request
Fetch mới từ Origin

Ví dụ thực tế

Trường hợp không sử dụng Invalidation

- Upload logo mới lên S3
- Người dùng tiếp tục thấy logo cũ cho đến khi TTL hết hạn

Trường hợp sử dụng Invalidation

- Upload logo mới lên S3
- aws cloudfront create-invalidation --paths "/logo.png"
- Người dùng nhận ngay logo mới mà không cần chờ TTL

Cache Behaviors

Định nghĩa

Cache Behaviors cho phép bạn định nghĩa chính sách cache khác nhau cho từng loại nội dung hoặc đường dẫn cụ thể trong một CloudFront Distribution.

Điểm chính

- Mỗi behavior có thể được cấu hình với cài đặt riêng cho caching, bảo mật, và routing
- Có thể chỉ định origin khác nhau cho từng behavior
- Các behavior cụ thể sẽ được ưu tiên trước behavior mặc định

Lợi ích của Cache Behaviors:

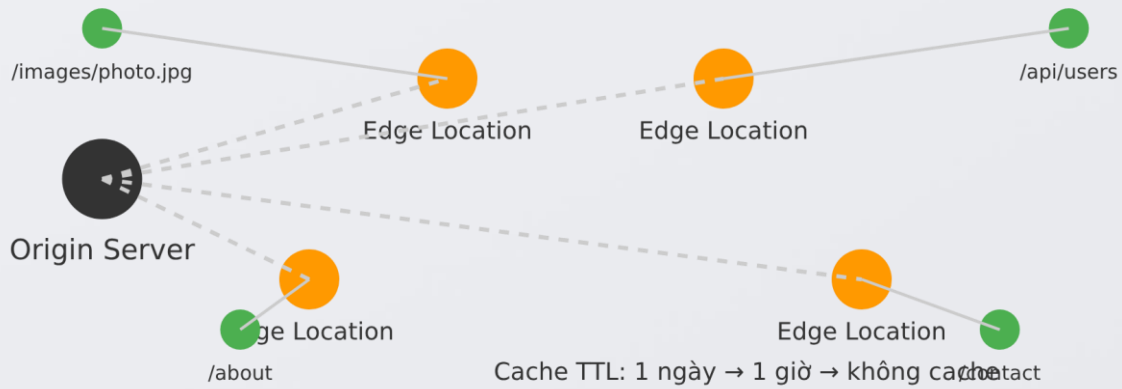
- Tối ưu hóa hiệu năng cho từng loại nội dung
- Đảm bảo nội dung động luôn cập nhật
- Giảm chi phí bằng cách cache hiệu quả

Ví dụ cấu hình

/images/*
- TTL cache: 1 ngày
- Cache toàn cầu

/api/*
- Không cache
- Luôn forward to origin

/*
- TTL cache: 1 giờ
- Default behavior



Geo Restriction

Định nghĩa

Geo Restriction (geo-blocking) là tính năng cho phép kiểm soát truy cập nội dung dựa trên vị trí địa lý của người dùng thông qua địa chỉ IP.

Tính năng chính

Allowlist

Chỉ cho phép truy cập từ các quốc gia cụ thể

Blocklist

Chặn truy cập từ các quốc gia cụ thể

Bảo mật nội dung

Ngăn chặn việc phân phối nội dung trái phép

Ví dụ: Phim bản quyền

Tình huống: Một dịch vụ streaming có hợp đồng bản quyền chỉ cho phép phát một bộ phim nhất định tại Việt Nam.

Cấu hình đúng

- Enable Geo Restriction
- Chọn Allowlist
- Thêm "VN" vào danh sách cho phép

Kết quả

- Người dùng Việt Nam: Truy cập thành công
- Người dùng Mỹ: Nhận lỗi 403 Forbidden

Signed URL / Signed Cookies

Signed URL

URL được ký để cấp quyền truy cập tạm thời đến một file riêng tư.

- Cấp quyền cho một file duy nhất
- Có thể thiết lập thời hạn sử dụng
- Được sử dụng cho các nội dung cần bảo mật cao

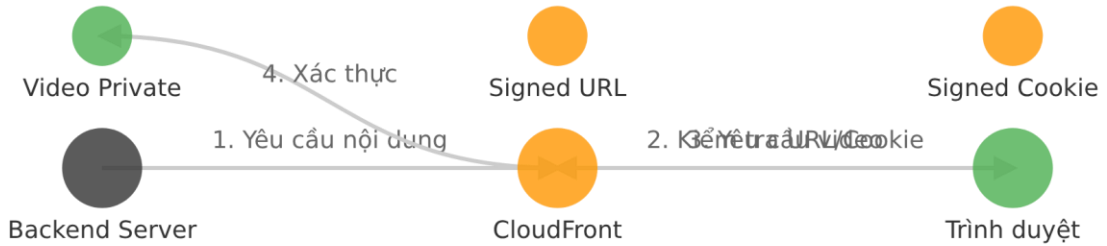
Signed Cookie

Cookie được ký để cấp quyền truy cập tạm thời đến nhiều file riêng tư.

- Cấp quyền cho nhiều file cùng lúc
- Cookie được lưu trữ trong trình duyệt
- Phù hợp cho các trang web cần bảo mật nhiều nội dung

Ví dụ: Khóa học trực tuyến

Một khóa học online chỉ cho phép học viên truy cập video trong 2 giờ sau khi đăng ký.



Quy trình hoạt động:

- Backend tạo Signed URL hết hạn sau 2 tiếng
- Link được gửi cho học viên
- Hết hạn → người khác không thể tải video
- Ngăn chặn việc chia sẻ URL giữa các người dùng

Pricing & Price Classes

Giá cả

Giá CloudFront khác nhau theo vùng Edge Locations, phản ánh chi phí vận hành khác nhau.

- Tính theo dữ liệu truyền ra khỏi Edge Locations
- Số lượng yêu cầu HTTP/HTTPS
- Dữ liệu truyền giữa AWS origins và Edge Locations thường miễn phí

Ví dụ tối ưu chi phí

Website phục vụ khách hàng chủ yếu ở châu Á:

- Chọn Price Class 100
- Tiết kiệm đến **30-40%** chi phí so với Price Class All
- Vẫn đảm bảo tốc độ tốt nhờ Edge Locations gần khách hàng

Price Classes

Price Class All

Bao gồm tất cả Edge Locations toàn cầu

- Hiệu năng cao nhất
- Latency thấp nhất
- Phạm vi toàn cầu

Price Class 200

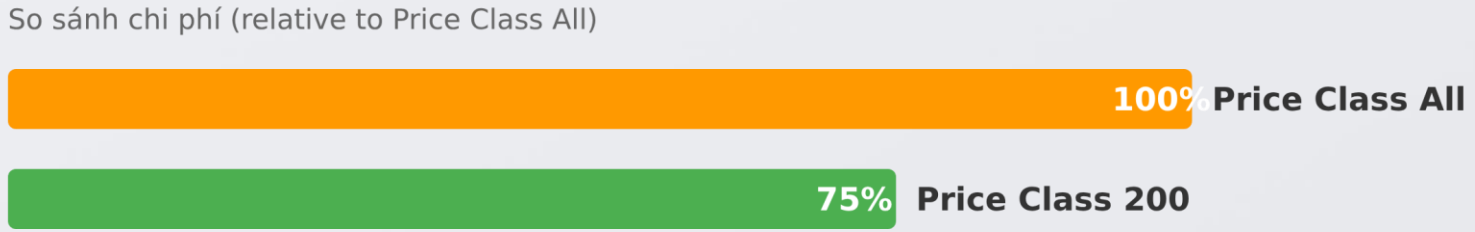
Loại trừ một số Edge Locations đắt đỏ

- Cân bằng giữa hiệu năng và chi phí
- Vùng thấp hơn về lưu lượng
- Vùng cao về chi phí vận hành

Price Class 100

Chỉ dùng Edge Locations rẻ nhất

- Chi phí thấp nhất
- Chỉ vùng có mật độ lưu lượng cao
- Vùng chi phí vận hành thấp



Tổng kết

Tính năng bảo mật

- Bảo vệ DDoS thông qua AWS Shield Standard
- Integration với AWS WAF cho bảo mật ứng dụng
- Hỗ trợ SSL/TLS encryption

Kỹ thuật cache

- Cache Key: định danh duy nhất cho object cache
- Cache Policy: cấu hình cách cache hoạt động
- Cache Invalidation: làm mới cache sớm hơn TTL

Bảo vệ nội dung

- Geo Restriction: kiểm soát truy cập theo quốc gia
- Signed URLs: cấp quyền truy cập tạm thời đến nội dung riêng tư
- Signed Cookies: bảo vệ nhiều file nội dung cùng lúc

Tối ưu chi phí

- Price Classes: lựa chọn Edge Locations dựa trên khu vực
- Tiết kiệm đến 40% chi phí với Price Class 100
- Free data transfer giữa AWS origins và Edge Locations

CloudFront là **CDN mạnh mẽ, bảo mật, giảm độ trễ toàn cầu**, giúp cải thiện trải nghiệm người dùng và tối ưu hóa chi phí triển khai.