Sử dụng Amazon CloudFront để tăng tốc việc phân phối các web tĩnh được lưu trữ trong Amazon S3 cho người dùng cuối. CloudFront có thể lưu trữ nội dung tại các vị trí cạnh gần hơn với người xem của bạn, mang lại cho họ hiệu suất cao hơn, phạm vi tiếp cận toàn cầu tức thì và tính khả dụng của nền tảng cao hơn. Đối với Amazon EC2 phục vụ nội dung động và tĩnh, cũng nên cân nhắc sử dụng CloudFront vì nó cung cấp một số lợi ích bổ sung. Nâng cao hiệu suất, bảo mật và chi phí bạn nhận khi sử dụng CloudFront để chạy các web động hoặc tĩnh từ Amazon EC2.

Performance

Cacheable Content

Mặc dù hầu hết các ứng dụng phục vụ nội dung tĩnh từ Amazon S3, các content từ Amazon EC2 sử dụng CloudFront edge Location và Region edge cache sẽ được cache trên CloudFront. Các ứng dụng có thể giảm workload và băng thông trong khi đưa content đến gần hơi với người dùng, giảm độ trễ khi service sử dụng nội dung tĩnh.

Global Reach

Mạng toàn cầu CloudFront, bao gồm hơn 100 điểm, giảm thời gian thiết lập các kết nối hướng tới người xem vì khoảng cách vật lý đến người xem được rút ngắn. Điều này làm giảm độ trễ tổng thể để phục vụ cả nội dung tĩnh và động.

Persistent Connections

Kết nối liên tục : CloudFront duy trì một nhóm các kết nối liên tục đến điểm gốc (LB-> EC2), do đó giảm thời gian thiết lập các kết nối mới với điểm gốc. Qua các kết nối này, lưu lượng giữa nguồn gốc CloudFront và AWS được định tuyến qua mạng đường trục riêng để đảm bảo độ tin cậy và hiệu suất. Điều này làm giảm độ trễ tổng thể để phục vụ cả nội dung tĩnh và động.

Collapsed Forwarding

Trong khi lưu lượng truy cập tăng cao, CloudFront tổng hợp các request đồng thời cho các lỗi bộ nhớ cache, không tìm thấy cache trước khi chuyển tiếp yêu cầu đến phía dưới để giảm tải cho hệ thống .

Security

Dịch vị chống DDOS phân tán

Cũng như các dịch vụ AWS khác, AWS Shield Standard được bao gồm miễn phí khi bạn sử dụng CloudFront. CloudFront cung cấp cơ chế chống lại các cuộc tấn công DDOS bằng cách phân phối lưu lượng truy cập trên nhiều điểm (POP - points of presence) và các yêu cầu lọc để đảm bảo rằng chỉ các yêu cầu HTTP (S) hợp lệ mới được chuyển tiếp đến các máy chủ. Với tính năng hạn chế địa lý của CloudFront, còn được gọi là khóa địa lý, bạn có thể sử dụng CloudFront để cách ly các cuộc tấn công có nguồn gốc từ một vị trí địa lý cụ thể.

Encryption in Transit

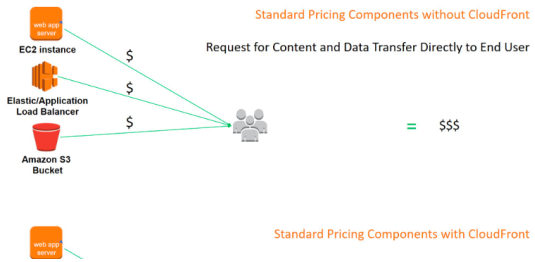
Có thể định cấu hình CloudFront để thực thi nghiêm ngặt các giao thức SSL. CloudFront tích hợp với Trình quản lý chứng chỉ AWS (ACM), nơi bạn có thể yêu cầu, tải lên và quản lý chứng chỉ của mình mà không mất thêm chi phí. CloudFront hỗ trợ cả Chỉ định tên máy chủ (SNI) và chứng chỉ địa chỉ IP chuyên dụng tùy chỉnh. Mặc dù các request HTTPS được tính thêm một phần phí cho mỗi request nhưng không có phí bổ sung cho việc sử dụng chứng chỉ SNI.

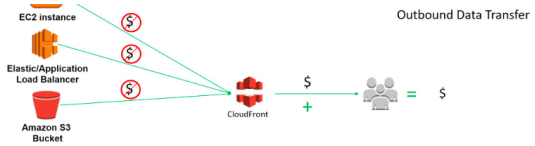
Web Application Firewall (WAF)

CloudFront tích hợp với AWS WAF, cho phép bạn định cấu hình các quy tắc để lọc các yêu cầu độc hại (chẳng hạn như SQL injection, cross-site script, v.v.) có thể gây hại cho dịch vụ của bạn. Yêu cầu được filter tại mỗi vị trí POP để giảm thiểu độ trễ từ các CF thuộc region đến edge location tránh các mối đe dọa khỏi cơ sở hạ tầng gốc.

Cost

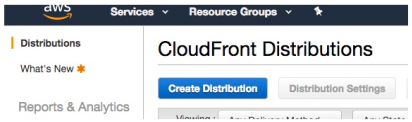
Phí chuyển dữ liệu đi từ các dịch vụ AWS sang CloudFront là $ 0 / GB. Chi phí phát sinh từ CloudFront thường thấp hơn cho mỗi GB truyền dữ liệu cho cùng một cấp và vùng. Điều này có nghĩa là bạn có thể tận dụng hiệu suất và tính năng bảo mật của CloudFront bằng cách đặt nó trước ứng dụng (ALB), AWS Elastic Beanstalk, Amazon S3 và các tài nguyên AWS khác cung cấp các đối tượng HTTP(S) mà không có chi phí bổ sung. CloudFront tính phí request cho mỗi đối tượng (object).



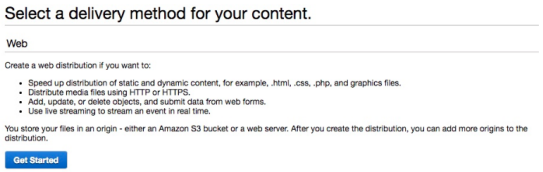


Config

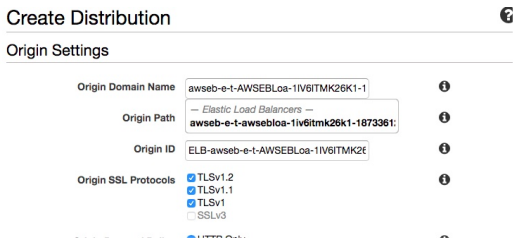
Tạo 1 distribution mới



Chọn web distribution



Ở Orgin setting chọn LB đã được tạo



Dưới **Default Cache Behaviors Settings**

- Viewer Protocol Policy: Redirect HTTP to HTTPS
- Allowed Methods: Get, Head, Options, Put, Post, Patch, Delete
- Compress Object Automatically: Yes
- Các giá trị còn lại để default

Chú ý : Mặc định sử dụng origins cache-control headers để xác định thời gian các object lưu lại trong bộ đệm của CloudFront. Nếu không có cache-control headers được trả về, trong trường hợp này, CloudFront sẽ mặc định Thời gian sống (TTL) là 24 giờ.

Dưới **Distribution Settings**

Logging: On
Bucket for Logs : Chọn bucket logs đã được tạo trên S3

Thêm một Cache Behavior cho nội dung động (không thể lưu trong bộ nhớ cache).

- Chọn distribution vừa tạo ở trện chọn tab Behavior --> create Behavior

- Setting

- Path pattern : admin, asset, ... (example.com/admin)

- Chọn LB đã tạo giống như step trên

- Redirect từ HTTP sang HTTPS

- Allowed Methods: Get, Head, Options, Put, Post, Patch, Delete

- Cached Based on Selected Request Headers: ALL

Lưu ý: Khi bạn định cấu hình cache behavior để chuyển tiếp tất cả các tiêu đề đến origin thì CloudFront coi nội dung là động, bỏ qua (bypass) tất cả các lớp bộ đệm của dịch vụ.

REF : https://aws.amazon.com/vi/blogs/networking-and-content-delivery/dynamic-whole-site-delivery-with-amazon-cloudfront/

https://aws.amazon.com/blogs/startups/how-to-accelerate-your-wordpress-site-with-amazon-cloudfront/