CloudFront

Content Delivery Network

Chandra Lingam

Cloud Wave LLC

Motivation

- Global Audience
- Performance

App

Data | Video | Image | API

Content

Option 1 – Keep your app in several regions

- Route traffic to appropriate region
- Complex setup

App Region 1 | App Region 2 | App Region 3 | App Region 4 | App Region 5

App in major regions

Option 2 – CloudFront CDN

- Edge Caching – Globally distributed
- Securely deliver to customers globally
- Low Latency

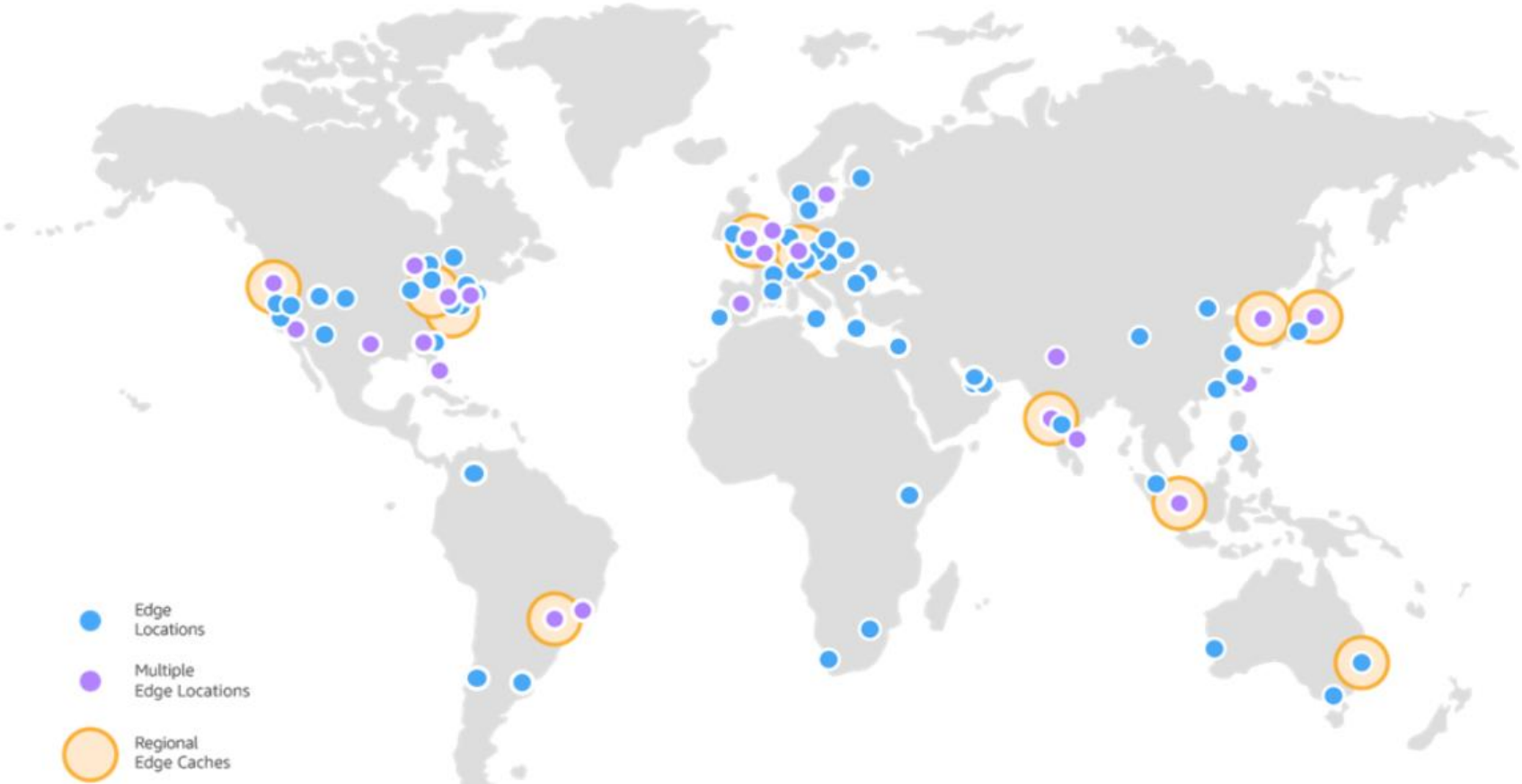
CloudFront

App

Origin

Source: https://aws.amazon.com/cloudfront/features/

Locations and 11 Regional Edge Caches) in 84 cities across 42 countries. Amazon CloudFront Edge locations are located in:



Types of Content

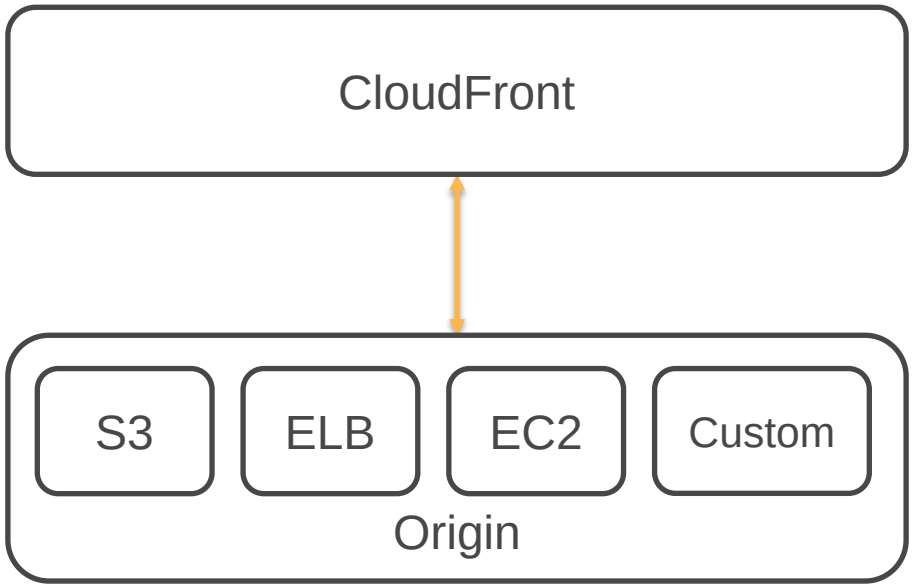
- Static – videos, images, JavaScript
- Dynamic – weather data
- User specific – user photo, health report
- Not-Cacheable – OTP (one-time password), payment card details

HTTP Cache Control Headers – cache or not to cache, how long to cache, public or private cache and so forth

CloudFront Performance

- Cache copies of content close to your users
- CloudFront routes request to nearest edge location
- For content not available at edge and regional edge cache:
    - Request is sent to the origin
    - CloudFront keeps persistent connection to Origin – minimizes connection establishment overhead
- Data transfer over AWS backbone network (for origin hosted in AWS)

Origin



- Dynamic and Static Content
- Streaming, Video on demand, Live streaming
- Restrict access - Signed URLs, Signed Cookies
- Geo Restriction
- Configurable Caching, Invalidation Option
- Personalized – Query String Parameters, HTTP Cookies
- Backup Origin (primary not healthy)

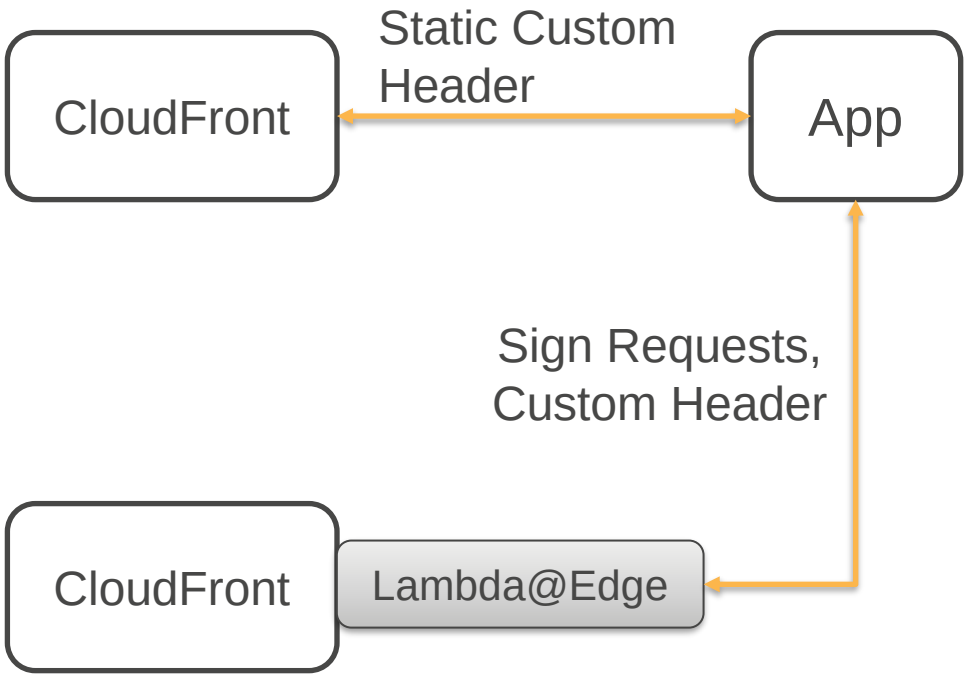
Security, Lambda@Edge

Securing S3 Origin

Origin Access Identity – Limit access to S3 bucket only from CloudFront Identity

When configured, CloudFront uses OAI credentials to sign S3 requests

Securing App Origin



- Static Custom Header – To validate requests from CloudFront
- Lambda@Edge
  - Custom Header
  - Sign Requests
- SSL/TLS
- Field Level Encryption (example: credit card number)
- Customize – HTTP Cookies, Query String Parameters

Security at the Edge

CloudFront

AWS Shield

Web Application Firewall

CloudFront – Front door for your application. Shield your critical content and infrastructure

AWS Shield

- Protection against DDoS Attacks. Standard features (no cost) – protects against layer 3 and layer 4 attacks
- Advanced (paid) – protection against larger and more sophisticated attacks (ELB, CloudFront, Route53), billing protection

WAF

- Control access to content (allow, deny, count requests based on criteria)
- SQL Injection, Cross-site scripting Protection

Lambda@Edge

Lambda functions at edge locations

Customize application behavior – without touching origin systems

Run application logic close to your end users

Improve responsiveness

Configure to run in-response to request lifecycle:

- Viewer Request/Response
- Origin Request/Response

Verify Authentication Credentials at Edge - JWT (JSON Web Tokens)

Bot detection

Lambda@Edge Usage

- Resize images, Render pages
- A/B Testing
- Redirect requests for outdated resource to updated resource
- Modify cache control headers
- Route to different origins based on content of the request
- Sign requests to custom origin
- Add Custom HTTP Headers
- Custom Load Balancing

Reference:

https://aws.amazon.com/blogs/networking-and-content-delivery/lambdaedge-design-best-practices/

Compliance

PCI DSS (Payment Card Industry)

HIPAA (Health Information Privacy)

SOC (System and Organization Control)

Lab – CloudFront Distribution

- S3 Origin
- Cache Duration
- Content Invalidation
- Origin Access Identity - Secure S3 Bucket

This lab is a modified version of AWS Getting Started Example:
https://aws.amazon.com/getting-started/tutorials/deliver-content-faster/

- Modified to incorporate Origin Access Identity, Invalidation, Cache Control

Cache Control

- Origin
- Override with Lambda@Edge
- CloudFront Distribution Configuration

Large Cache Duration => Stale Data
Small Cache Duration => Frequent reads from source
Pick a right cache duration based on application data refresh requirements

S3 Cache Control

CloudFront caches S3 objects for 24 hours (default)

Let’s add custom cache instructions using the S3 Console

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html

https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serving-outdated-content-s3/

Chandra Lingam

50,000+ Students

Up-to-date Content