Amazon CloudFront

Accelerate your application using CloudFront

Accelerate your content using CloudFront

Whole site delivery

API acceleration

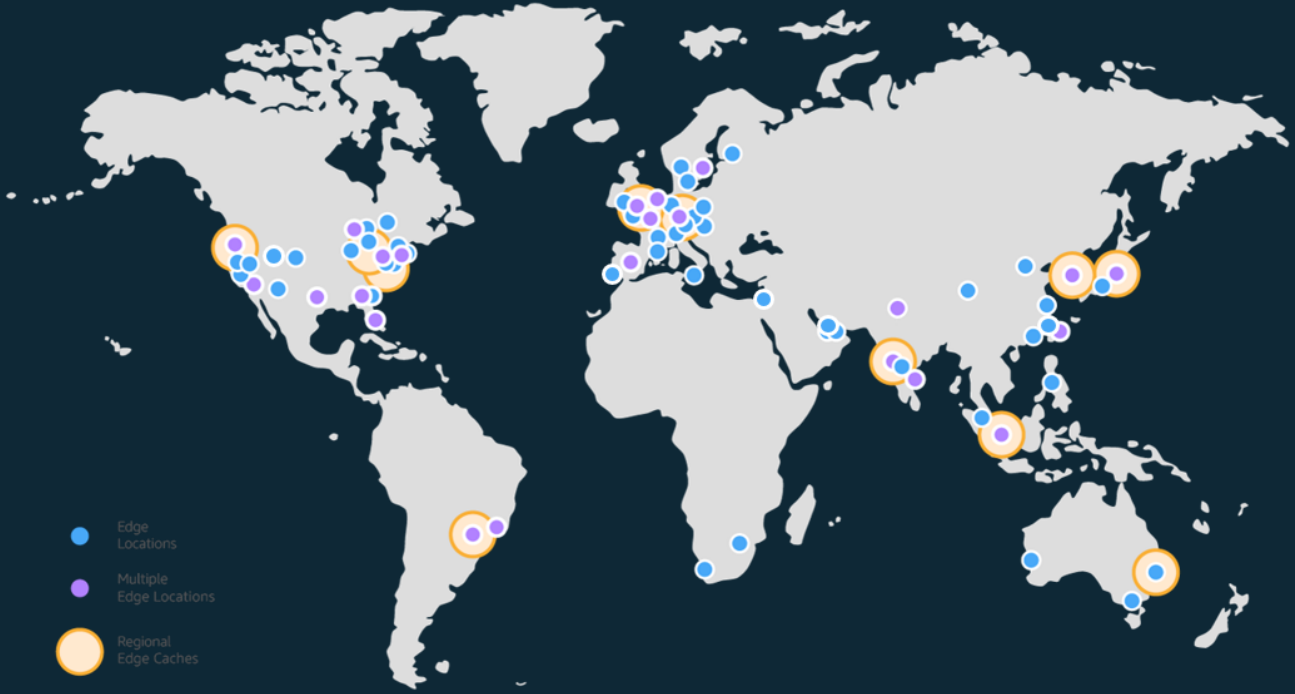
Custom content using Lambda@Edge

Static object delivery

Video streaming

Large file downloads

Amazon CloudFront’s Extensive Global Reach

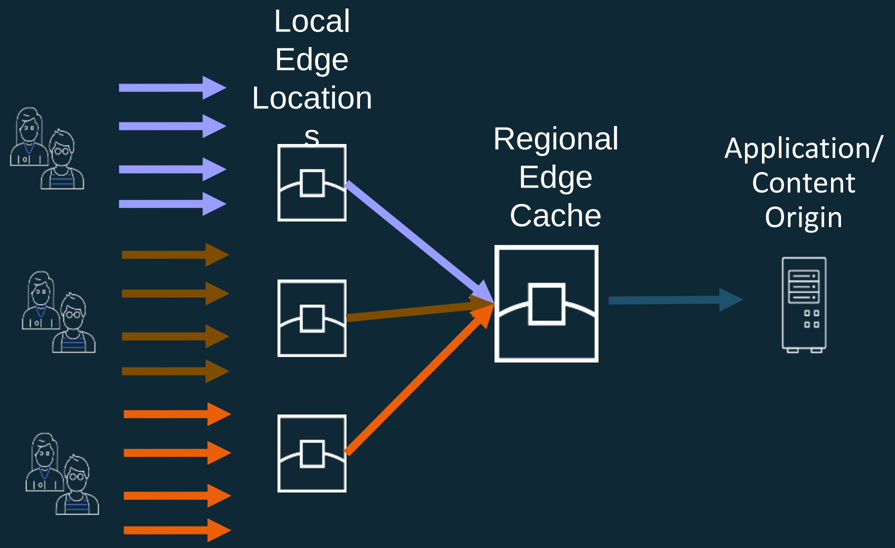


CloudFront now covers:

- **191+ POPs**
- **11 Regional Edge Caches (REC)**
- **33+ Countries**
- **73+ Cities**

Benefits of CDN

- Massive Scale (many 10s of Tbps and millions of requests/sec)
- Requests routed to “best” edge location based on multiple performance metrics
- Built-in security & dDoS protection
- Localized and optimized connections (reduce RTTs, latency, reuse connections, etc)
- Uses dedicated AWS backbone for excellent performance, reliability & security.
- Hierarchical architecture for origin protection and offload
- Reduced Costs vs Regional Data Transfer Out.



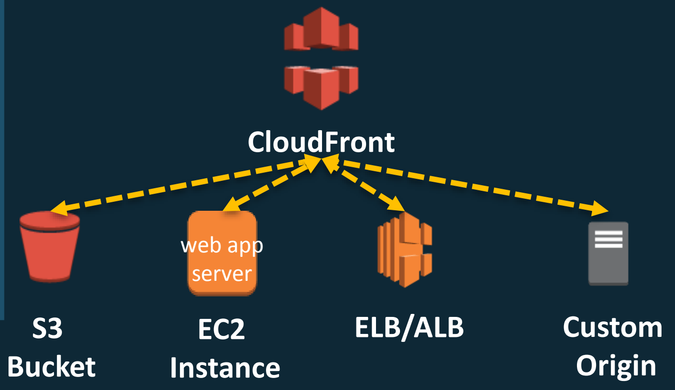
Building Blocks of a CloudFront Configuration

Distributions

- Unique CloudFront.net domain name to reference objects (abc123.cloudfront.net)
- Custom domains
- Custom TLS configuration
- Enable H2, IPV6 & logging to S3
- Associate to WAF ACL

Origins

- Any HTTP(s) endpoint
- TCP ports & timeouts
- TLS configuration



CloudFront

web app server

S3 Bucket

EC2 Instance

ELB/ALB

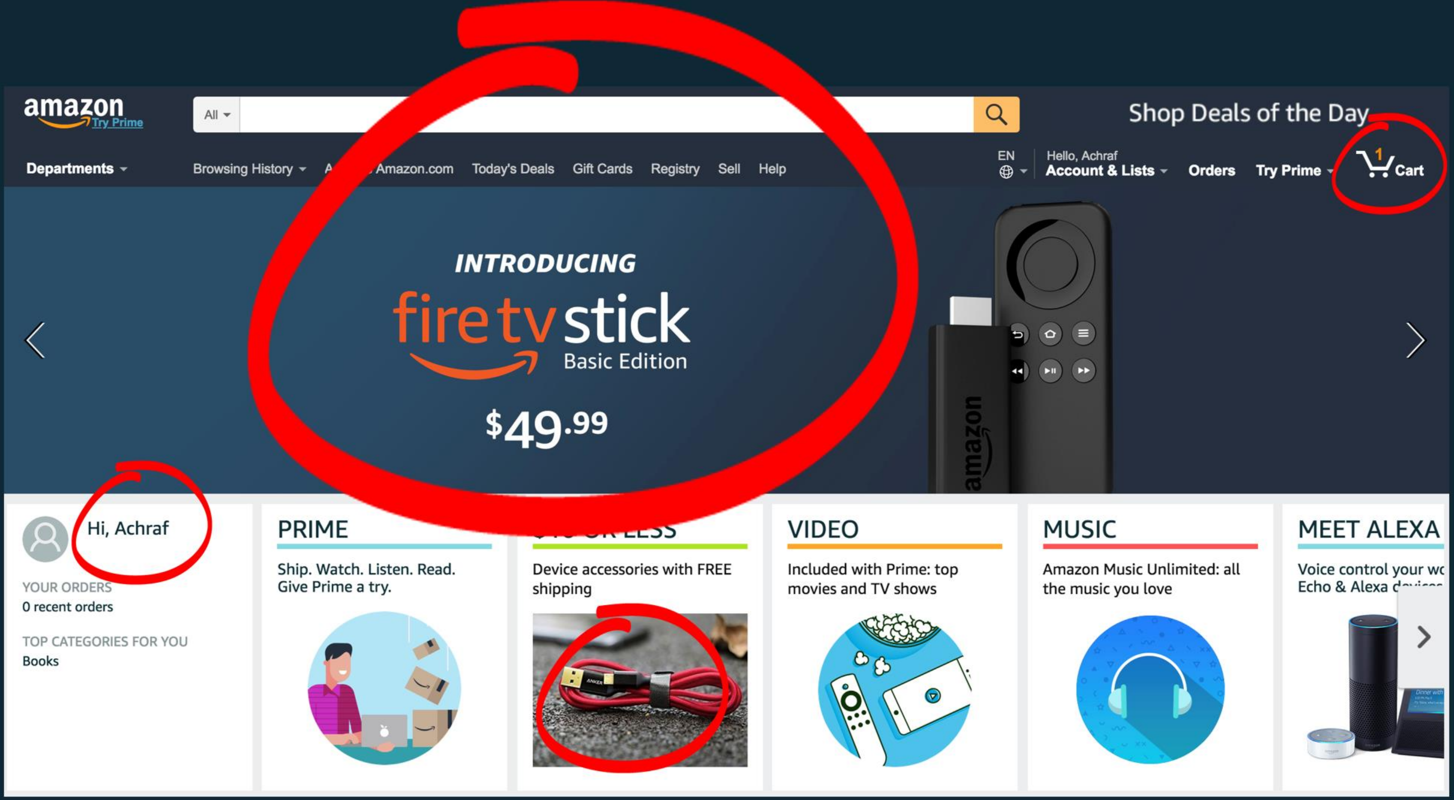
Custom Origin

Behaviors

- Path condition
- Select origin
- HTTP Methods
- Caching and forwarding policy
- Enable Object compression
- Configure features (Lambda@Edge triggers, Field Level Encryption, Signed URLs)

CloudFront caching best practices

Cache as much as possible



Hi, Achraf

YOUR ORDERS
0 recent orders

TOP CATEGORIES FOR YOU
Books

Ship. Watch. Listen. Read. Give Prime a try.

Device accessories with FREE shipping

Included with Prime: top movies and TV shows

Amazon Music Unlimited: all the music you love

Voice control your wo
Echo & Alexa d

Use the right settings

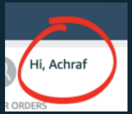
Static Content

- Use Cache Control directives either in per-object response headers or CloudFront config
- Partition resources of like characteristics
- Check metadata forwarding rules to reduce unintended variants
- Resource Versioning using URL Parameters, eTag, or TTLs

Dynamic Content

- Use 0 sec TTL to leverage “revalidation”
- Or mark as non-cacheable:
  - Cache-Control: private, no-store
  - In Cache Behavior, pick ‘All’ for ‘Cache based on Selected Headers’

/api/name

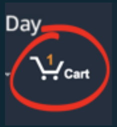


Private long-lived content

```
Cache-Control: private, max-age=2592000
ETag: “fsd435fsd3dfgkjhgff”
```

Disable caching on CloudFront (Forward all headers)

/api/cart



Private dynamic content

```
Cache-Control: no-store
```

Disable caching on CloudFront (Forward all headers)

/image.jpg

Shared static content

```
Cache-Control: max-age=31536000
ETag: “fsd435fsd3dfgkjhgff”
```

URL versioning

/images/hero.jpg

Shared mutable content

```
Cache-Control: no-cache
ETag: “fsd435fsd3dfgkjhgff”
```

Set MinTTL on distribution

Optimize Metadata Forwarding and Content Variants

- Whitelist only what changes the response (Cookies, Headers, Query String)
- Pay attention to case sensitivity and order
- Reduce variability of forwarded headers
  - Use CloudFront provided headers (country, device type, etc…)
  - Use Lambda@Edge to extract relevant data
  - Use CloudFront native capabilities (Logs, Geo/URL Signing access control)
- Leverage responsive web design & minify heavy assets like images for the platform they are viewed on.

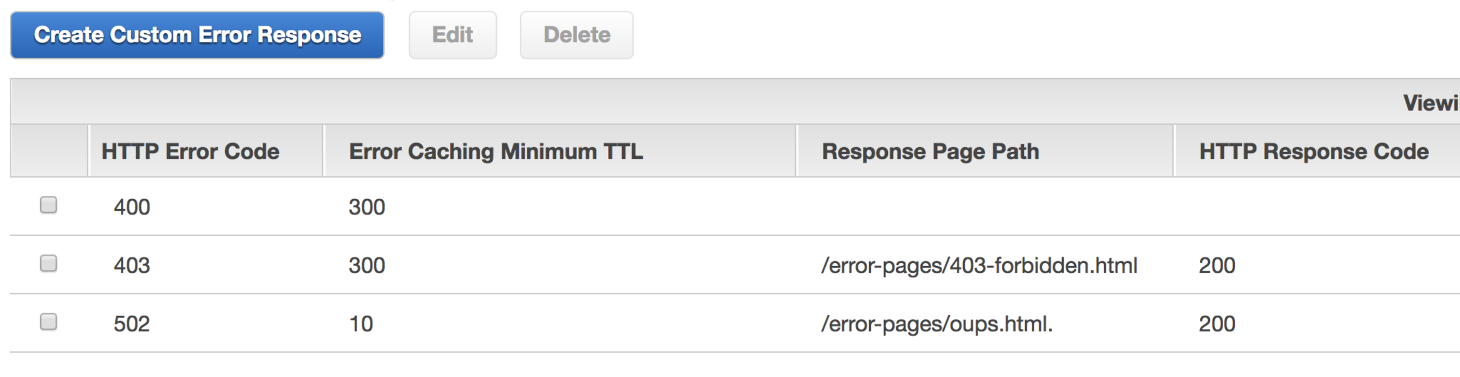
Start Building on AWS Today

Start Building on AWS Today

Start Building on AWS Today

Use Custom Error Pages

- Increase origin availability by caching 4xx & 5xx error responses
- Serve stale content when origin is not available
- Customize and normalize error pages for better user experience
- Hide error codes from potential attackers

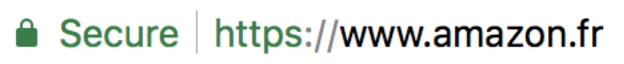


				Viewi
	HTTP Error Code	Error Caching Minimum TTL	Response Page Path	HTTP Response Code
□	400	300		
□	403	300	/error-pages/403-forbidden.html	200
□	502	10	/error-pages/oups.html.	200

CloudFront security controls

HTTPS secure delivery

- Single platform for HTTP and HTTPS delivery
- Redirect HTTP to HTTPS on the edge
- Control TLS policy
- TLS features: session resumption, OSCP stapling & Perfect Forward Secrecy



Secure | https://www.amazon.fr

TLS/SSL options through CloudFront

Default CloudFront SSL

- CloudFront certificate shared across customers

Use case

- *dxxx.cloudfront.net*

SNI custom SSL

- Bring your own SSL certificate
- Relies on the SNI extension of the Transport Layer Security protocol

Use case

- *www.example.com*
- Some older browsers/OS do not support SNI extension

Dedicated IP custom SSL

- Bring your own SSL certificate
- CloudFront allocates dedicated IP addresses for your SSL content

Use case

- *www.example.com*
- Supported by all browsers/OS

Free SSL certificates for ACM-integrated services like CloudFront

Restricting external access to your content

Signed URLs

- Add signature to the URL query string
- Your URL changes

Use case

- Restrict access to individual files
- Users are using a client that doesn't support cookies

Signed cookies

- Add signature to a cookie
- Your URL does **NOT** change

Use case

- Restrict access to multiple files
- You don’t want to change URLs

Geo Restriction

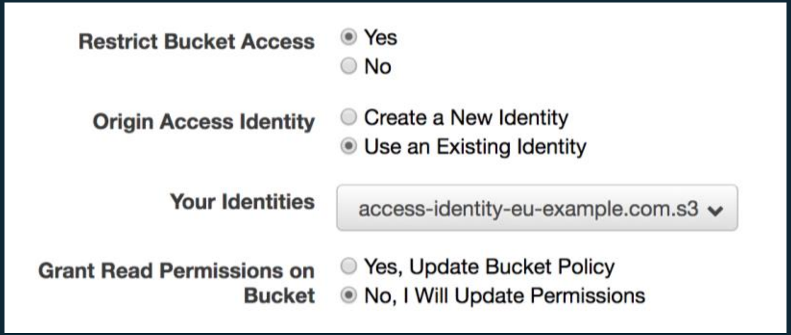
- Country based whitelist or blacklist

Use case

- Broad restriction based on geographical mapping of client IP

Origin Protection & Access Control

- Forward custom headers for custom origin
- Use VPC security groups to allow only CloudFront Ips
- Use integrated Origin Access Identity to allow only CloudFront to access S3 bucket and set permissions



Restrict Bucket Access	● Yes ○ No
Origin Access Identity	○ Create a New Identity ● Use an Existing Identity
Your Identities	access-identity-eu-example.com.s3
Grant Read Permissions on Bucket	○ Yes, Update Bucket Policy ● No, I Will Update Permissions

Security Capabilities

Built-in / Included

AWS Shield

- Comprehensive defense against all known network and transport layer DDoS attacks
- Protection against SSL abuse, malformed HTTP requests.
- Compliance: PCI DSS Level 1, FedRAMP (Agency ATO), SOC, ISO 9001, 27001, 27017, 27018, GDPR

Optional Services

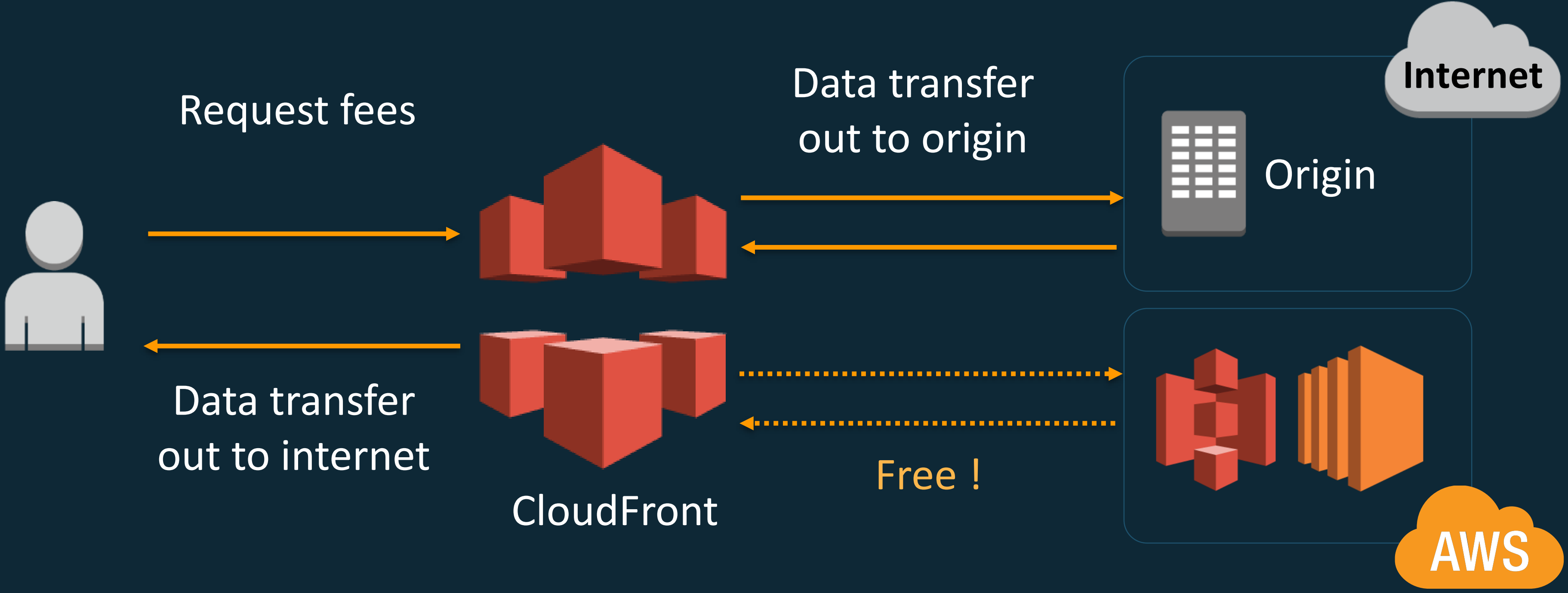
AWS WAF

- SQLi
- XSS
- rate limiting
- geoblocking rules
- string/regex matching
- ip rules

Shield Advanced

- AWS DDoS Response Team assistance
- Advanced protections including WAF
- Attack visibility, cost protection

Pricing components



Request fees

Data transfer out to origin

Data transfer out to internet

Free !

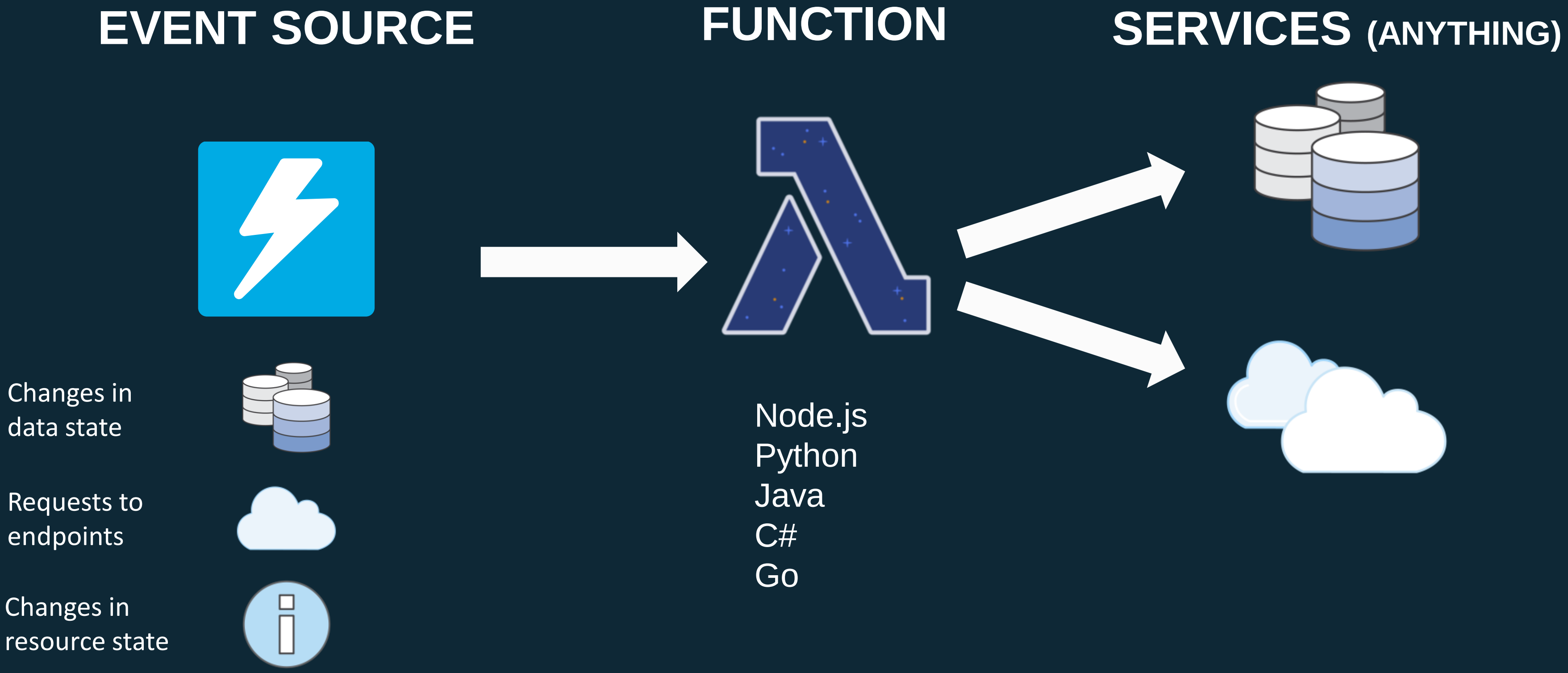
Lambda@Edge

AWS Lambda: Why Serverless?

Build and run applications without managing servers

- No servers to manage
- Run at scale
- Respond quickly to events
- Only pay for compute time that you use
- Developer productivity

Serverless applications



EVENT SOURCE

Changes in data state

Requests to endpoints

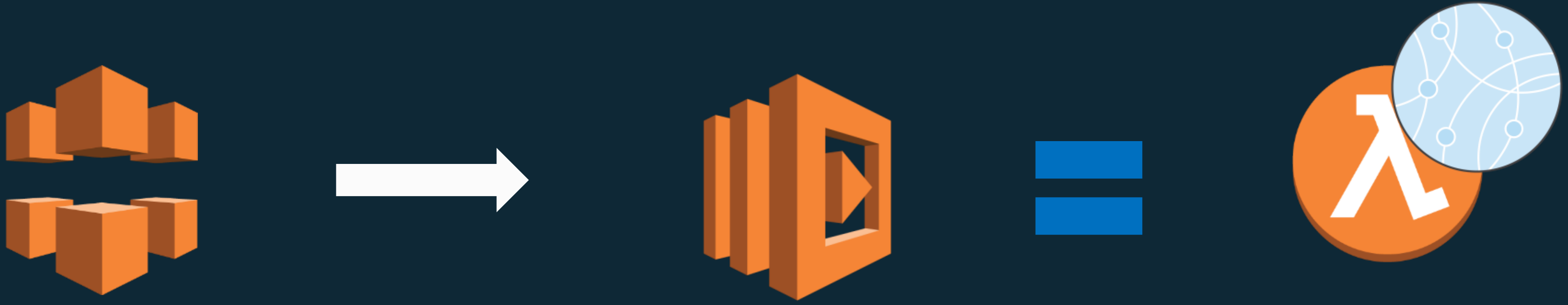
Changes in resource state

FUNCTION

Node.js
Python
Java
C#
Go

SERVICES (ANYTHING)

AWS Lambda@Edge



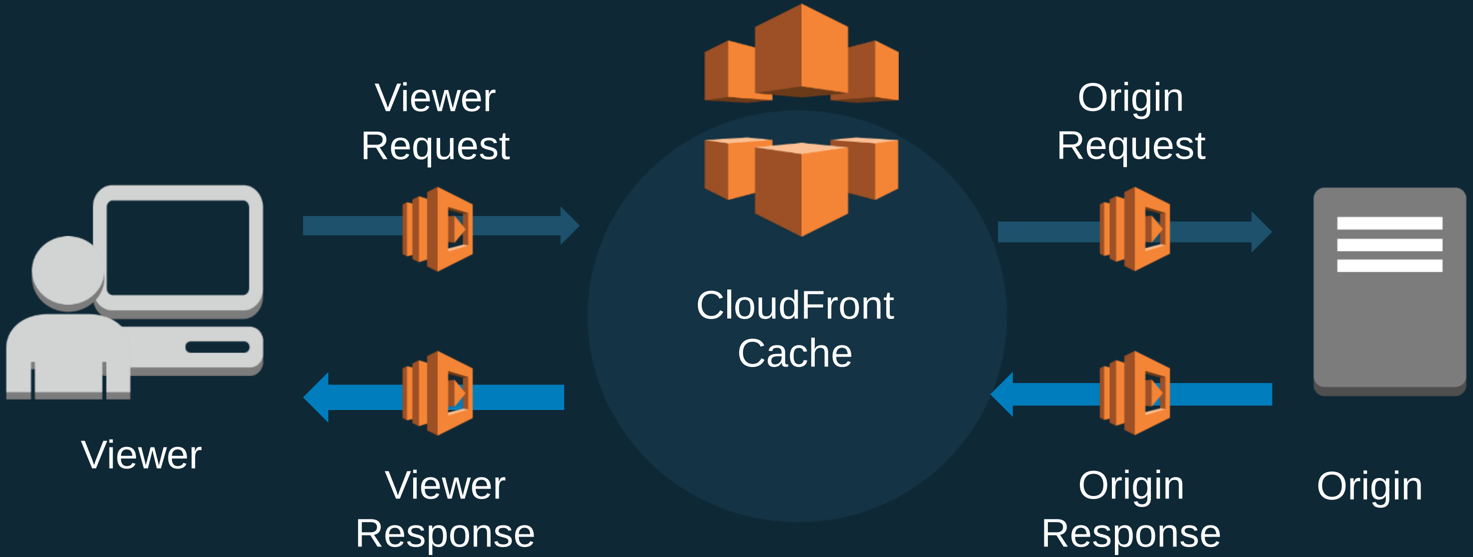
Amazon CloudFront
(Event Source)

AWS Lambda

Lambda@Edge

Global Serverless:
Run Lambda Functions Across AWS Locations

CloudFront and Lambda@Edge



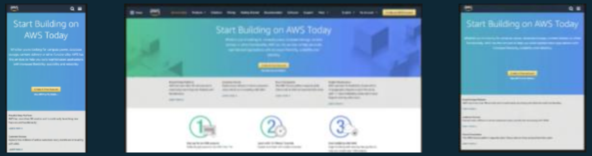
Lambda@Edge use cases

Simple HTTP manipulations	Dynamic content generation	Origin independence
User-Agent header normalization	Redirections/Rewrites	Pretty URLs
Adding HSTS security/CORS headers	Render pages	API wrapper
Enforcing Cache-Control headers	SEO optimization	Authorization
A/B testing	Personalize error responses	Bot mitigation

Lambda@Edge Best Practices

#1 Do you need Lambda@Edge? Consider the options

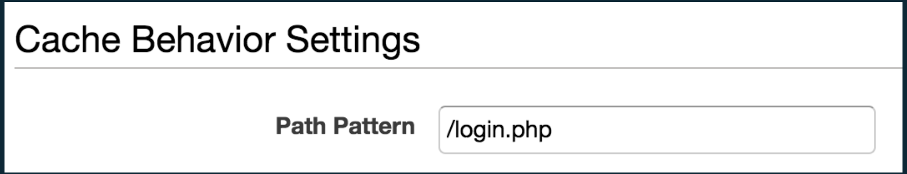
- CloudFront already provide native features:
  - Device identification: CloudFront-Is-Mobile-Viewer headers
  - Analytics: CloudFront Access Logs delivered to S3 & WAF logs
  - Access Control: CloudFront signed URLs/cookies, Geo-blocking, WAF
- Leverage responsive web design
- Some logic is better off on the origin!


Start Building on AWS Today
Start Building on AWS Today
Start Building on AWS Today

#2 Invoke Lambda@Edge only when you need it

- For every request or only on cache misses?

- Use the most specific CloudFront behavior:

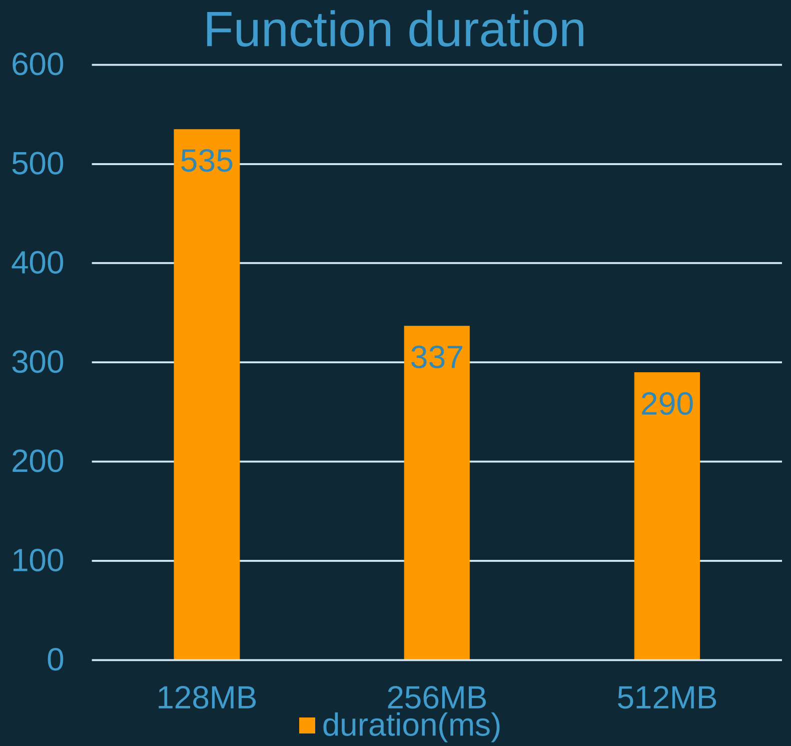


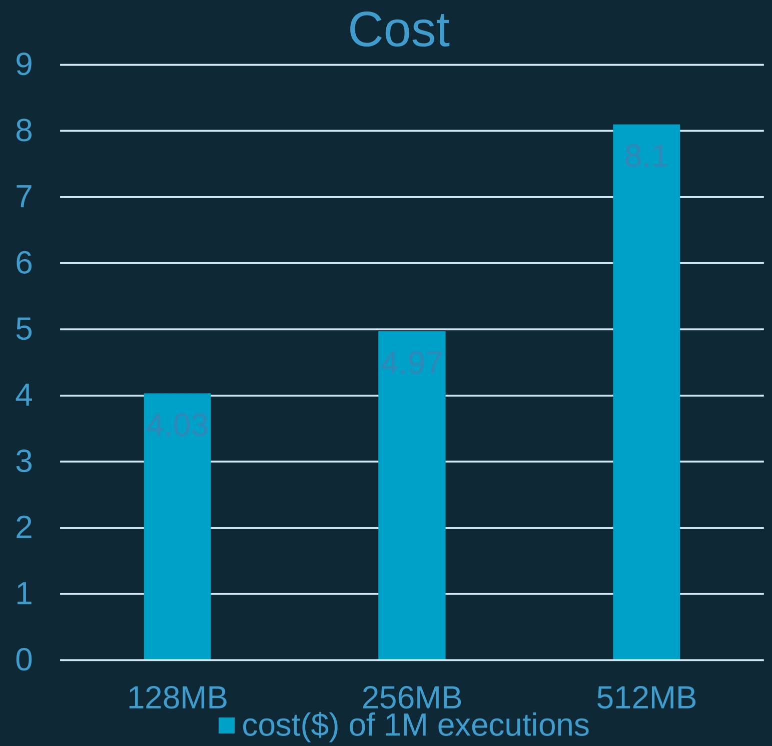
Cache Behavior Settings

Path Pattern: /login.php

- Remove it when it’s not used any more

#3 Choose the optimal memory configuration


Function duration


Cost

Lambda@Edge Security Best Practice

Lambda@Edge Security Best Practices

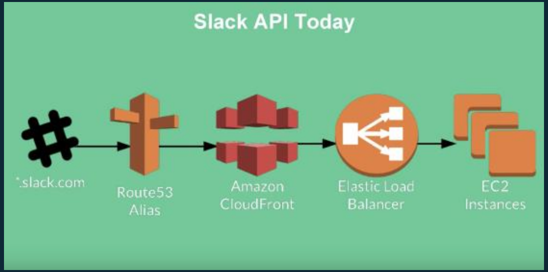
- Adopt the principle of least privilege
- Monitor and log functions and set alarms
- Deploy functions in minimal granularity
- Encrypt Data in transit (Use HTTPS or AWS SDK)
- Manage secrets in secure storage
- Follow secure application coding convention and use WAF
- Delete Lambda functions that you are no longer using

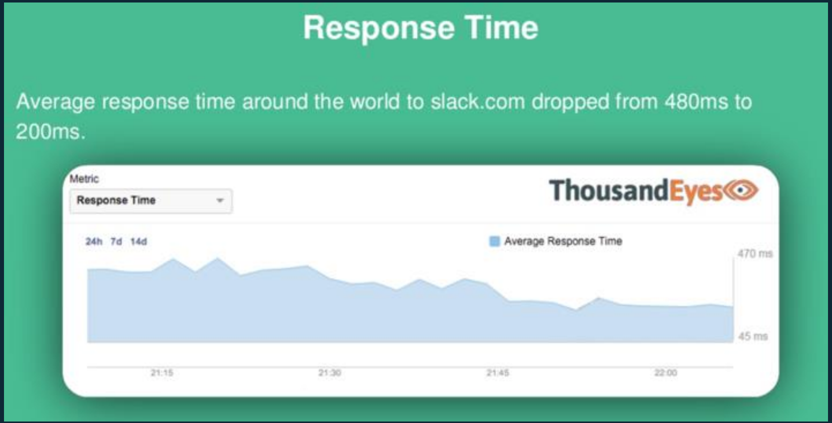
Appendixes

API Acceleration - Slack

- Slack host their API behind ALB for serving json files with 5B requests/week. They were looking for DDoS protection

- Slack selected CloudFront for its DDoS protection, performance and stability that outperformed other solutions.




Response Time

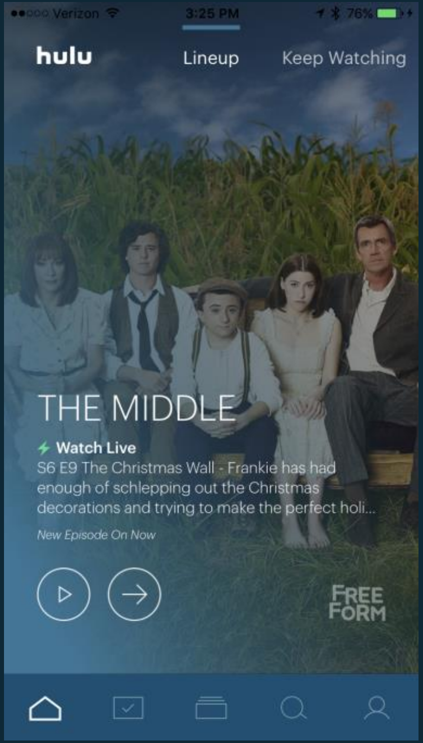
Average response time around the world to slack.com dropped from 480ms to 200ms.

Average response time improved from 480ms to 200ms

Live streaming - Hulu

- For its live service, Hulu put all content ingest, repackaging, DVR controls, and origin serving in the cloud. Hulu is serving 50 Live channels for 32 million subscribers

- Hulu selected CloudFront for its **scalability.**



THE MIDDLE

S6 E9 The Christmas Wall - Frankie has had enough of schlepping out the Christmas decorations and trying to make the perfect holi...

New Episode On Now

Video on Demand: Vevo

- Vevo brings a library of 140,000 HD music video to worldwide audience generating over 18 Bn views/month

- Vevo selected CloudFront to deliver web static assets and streaming HD ABR video, for its global footprint, available capacity and performances.

Bot Protection - DataDome

DataDome is a cybersecurity solution for web and mobile applications that analyzes non-human traffic in real time.

DataDome uses Lambda@Edge to make its bot-mitigation cybersecurity solution available in one click. Lambda@Edge eliminate server setup, simplifying the onboarding process to under 2 minutes.

Adding HSTS Headers – Macquarie Bank/DEFT

Macquarie Bank are owners of DEFT. DEFT is a payment and account receivable platform that processes millions of transactions per year.

DEFT uses Lambda@Edge to add HTTPS Strict Transport Security (HSTS) header on responses from Cloudfront to ensure users connect over HTTPS

Thank you!