CloudFront and AWS Global Accelerator

Uday Manchanda

September 19, 2021

1 CloudFront

- CDN (Content Delivery Network)
- Improves read performance, content is cached at the edge
- 216 edge locations
- DDos Protection, integration with AWS Shield, AWS WAF
- Expose external HTTPS and can talk to internal HTTPS backends
- Origins
  - S3 bucket - for distributing files and caching them at the edge
  - enhanced security with CF Origin Access Identity (OAI) - allows communication from CF and nowhere else
  - Custom origin (HTTP) - ALB, EC2, S3 website, any HTTP backend
- Edge location are connected to the origin we defined
- Client access CF distribution, client sends HTTP request to CF, edge location forwards request to your origin
- Edge location caches the request

1.1 CF - S3 as an origin

- edge location will fetch data from s3 location
- edge location will use an OAI to access s3 bucket, which is an IAM role for your CF origin

1.2 ALB or EC2 as an origin

- Ec2 instances must be public
- ege location will access ec2 instance, must allow public IP of edge location
- for alb it also must be public
- alb must allow public ip of edge location, alb then allows SG of of LB

1.3 Geo Restriction

- you can restrict who can access your distribution
- via: whitelist, blacklist
- Country is determined via third party geo ip database
- CF vs s3 CRR
  - Cf - great for static content that must be available everywhere
  - s3 crr - great for dynamic content that needs to be available at low-latency in a few regions

1.4 CloudFront Signed URL/Cookies

- lets say you want to distribute paid shared content to premium users all over the world
- attach a policy with: url expiration, IP ranges, trusted signers
- Signed URL = access to individual files (one signed URL per file)
- Signed cookies = access to multiple files
- CF signed url vs S3 signed URL
  - CF - allows access to a path, no matter the origin, account wide, leverge all caching features
  - s3 - issue a request as the person who pre signed the URL, uses IAM key of the signing IAM principal, limited lifetime

1.5 Advanced Concepts

- the more data transferred out of CF the lower the cost
- ccan reduce the number of edge locations for cost reduction
- three price classes
  - Price class all

  - Price class 200
  - Price class 100
- Multiple Origin - route to different kinds of origins based on the content type based on path pattern
- Origin Groups - increase HA and do failover. Have one primary and one secondary
- can set up replication if primary and secondary buckets are in different regions
- Field level encryption - protect sensitive information thru application stack
- sensitive info encrypted at the edge location close to the user
- Uses assyemtric encryption

2 Global Accelerator

- The problem
  - Deployed a global application and have global users who want to access it
  - they go over the public internet which can add a lot of latency due to hops
  - we wish to go as fast as possible thru aws newtork to minimize latency
- uses anycast IP to send traffic directly to edge locations, edge locations send traffic to your application
- leverages the aws internal network to route your application
- works with: elastic IP, ec2, ALb, NLB, public or private
- Consistent Performance - intelligent routing, no issues with caching, internal network
- Health checks
- only 2 ips need to be whitelisted and DDoS protection

2.1 Global Accelerator vs CloudFront

- both use the aws global network and its edge locations around the world
- both integrate with aws shield for DDoS protection
- CloudFront
  - improves performance for both cacheable content and dynamic content
  - content is served at the edge

- Global Accelerator
  - improves performance for a wide range of applications over TCP or UDP
  - Proxying packets at the edge to applications running in one or more AWS regions
  - Good fit for non HTTP use cases
  - or for HTTP use cases that require static IP addresses or fast failover