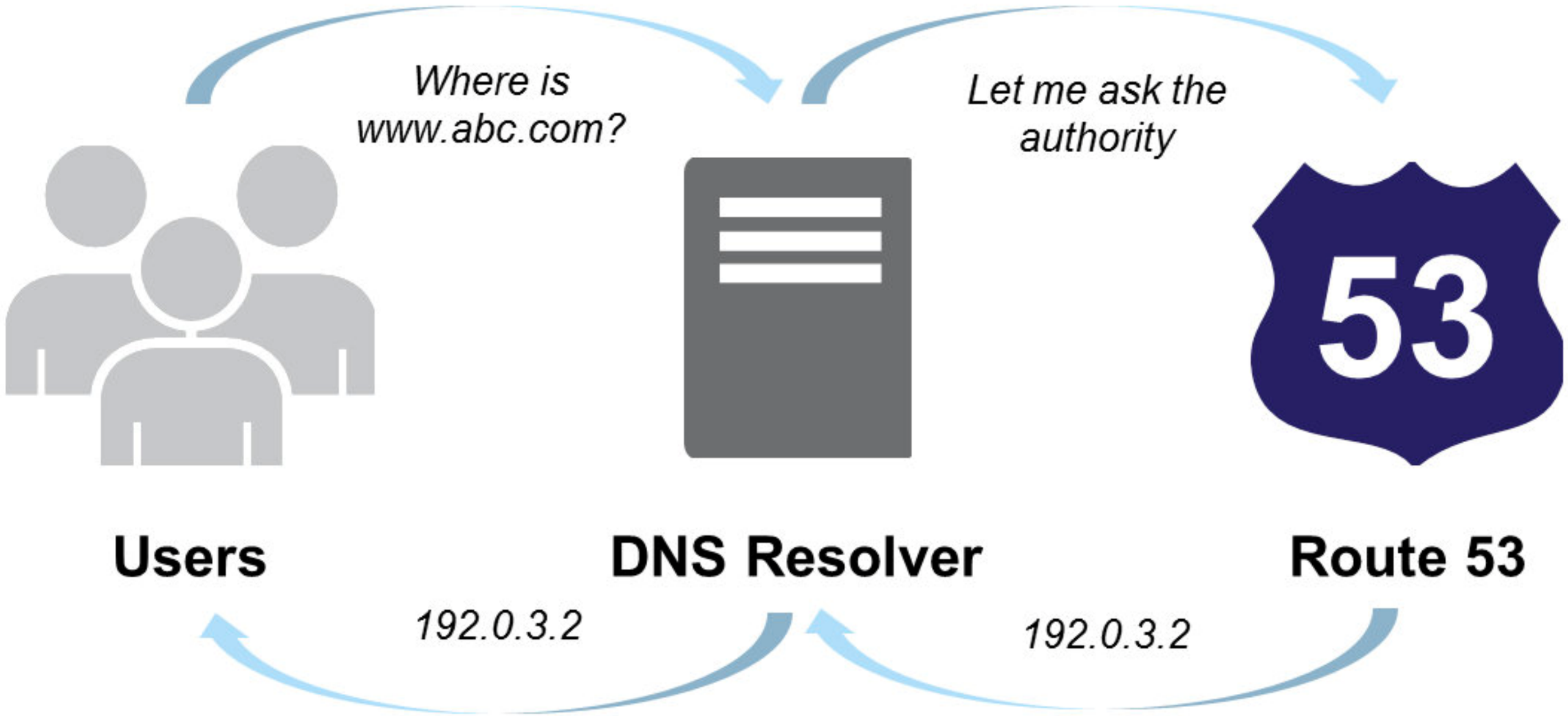
AWS Solutions Architect Associate

Session 1101

Networking and CDN: Route53 and Cloudfront. Sec, Id & Mgmt: Certificate Manager

August/2024

DNS Query



Source : AWS

Route 53 is an authorative DNS.

DNS Explained

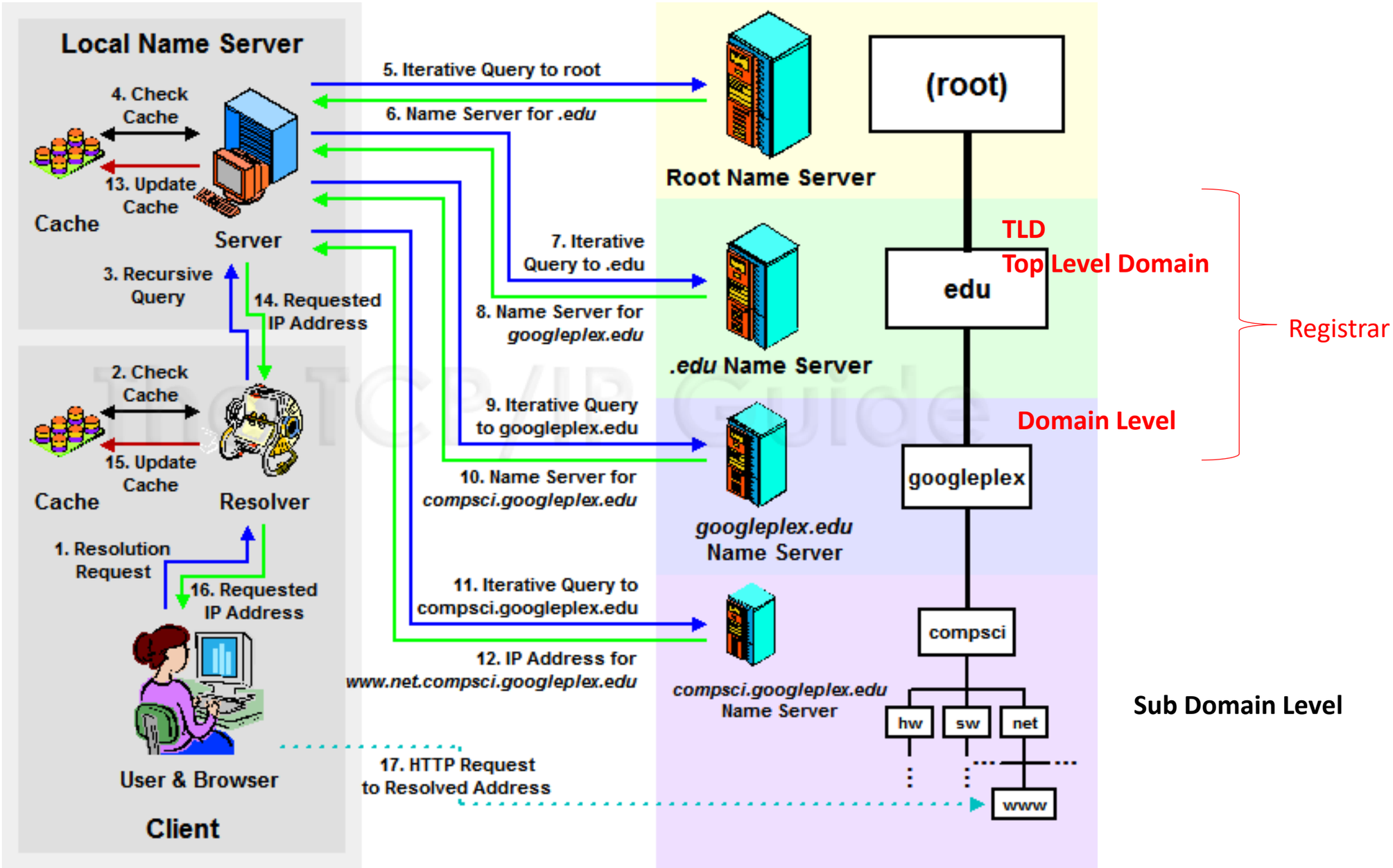
Domain Name System = Domain Name Resolution.
Many Levels, Many Actors, Many Concepts.

ISP DNS Server
Recursive Query

Windows
ipconfig /displaydns
ipconfig /flushdns

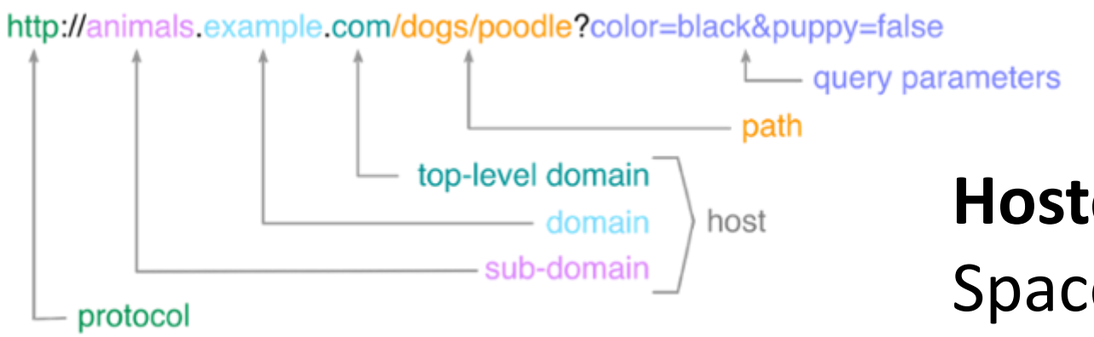
Local Resolver
C:\Windows\System32\drivers\etc\hosts

MacOS/Linux
See Reference



Taken from https://foxutech.com/what-is-dns-and-how-it-works/how-dns-works/ and Reference; https://help.dreamhost.com/hc/en-us/articles/214981288-Flushing-your-DNS-cache-in-Mac-OS-X-and-Linux (20/07/2024)

Hosted Zones and Record Types



Hosted Zone (AWS) = DNS Zone
Space where Records and hierarchy to manage a domain.

Important records and precedence

Common DNS Record Types	
Record	**Description**
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record
SOA	Start of Authority record
SRV	Service Location record
TXT	Text record

SOA: Administrative Information
NS: Name Server, replying as Authorative DNS Servers.
A: Return an IP Adress when get a subdomain on the Hosted Zone.
CNAME: Return a complete URL or Alias from the requested resource.

Taken from https://raventools.com/marketing-glossary/top-level-domain/ (30/07/2024)

Route 53

Amazon Route 53

Hosted zone

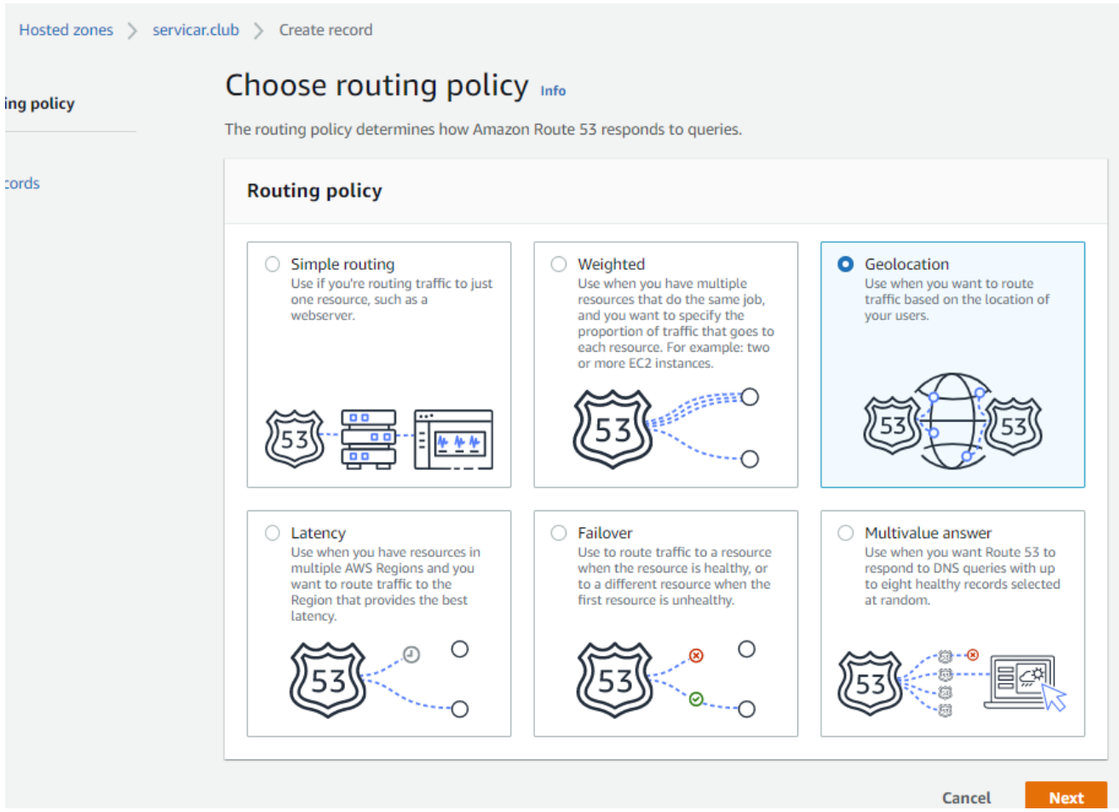
DNS (Domain Name Service) managed by AWS. It scalable and HA. It's called by Port Number of DNS: 53.

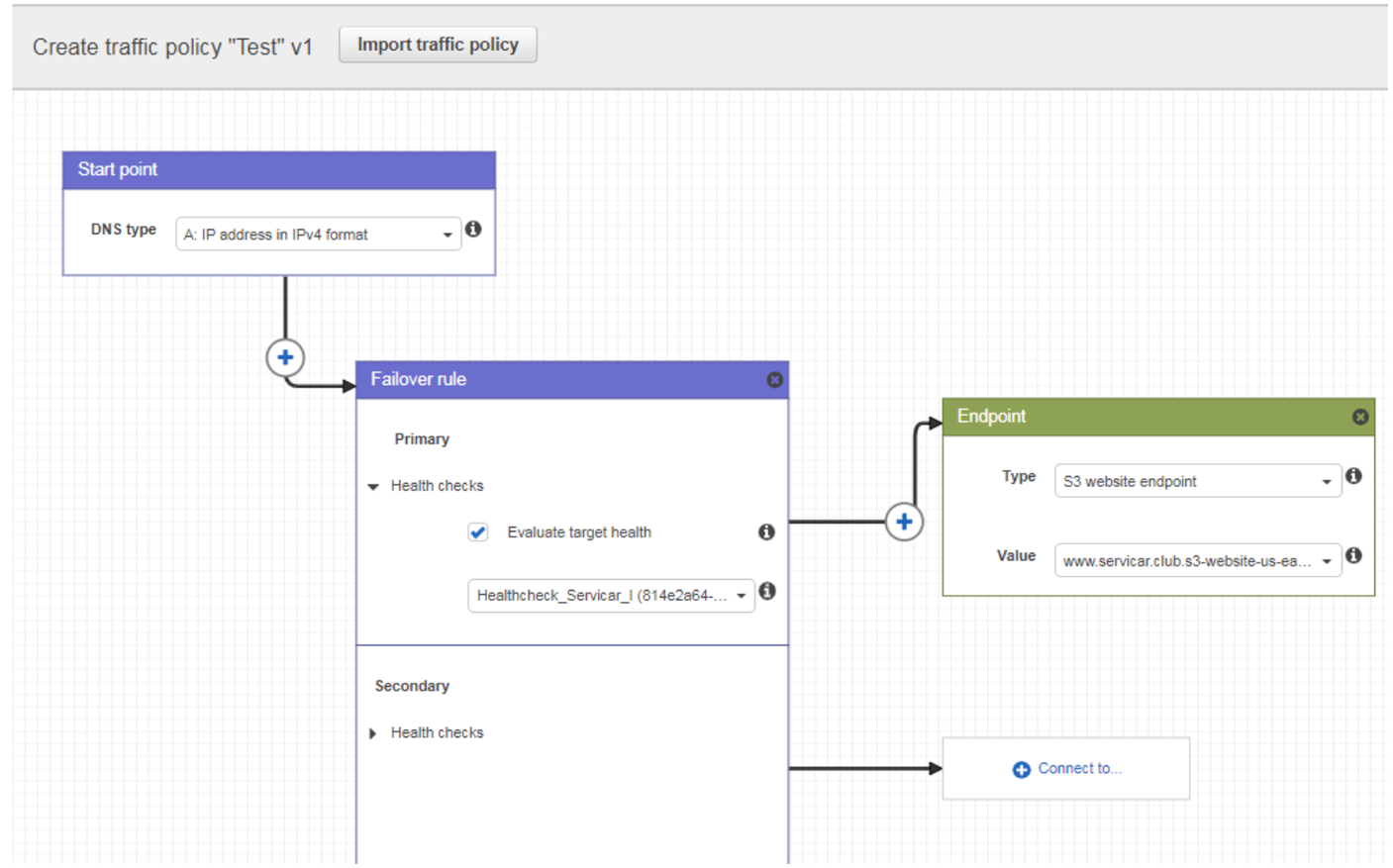
Provide different offers:

- Domain Registration and Transfer.
- Resolver (AWS VPC or On Premises), Private DNS*.
- Routing Policies on Hosted Zones.
- Traffic Flow (Policies: Latency, GeoDNS, Weighted, etc.). U$50/Month.
- DNS Failover using Health Check and Monitoring.
- Apex Support for CDN, S3.
- Alias target for: ELB, CDN, Beanstalk and S3.

* Prereqs: DNS Hostname and DNS Resolution.

RP on: Records of Hosted Zones vs Traffic Policies





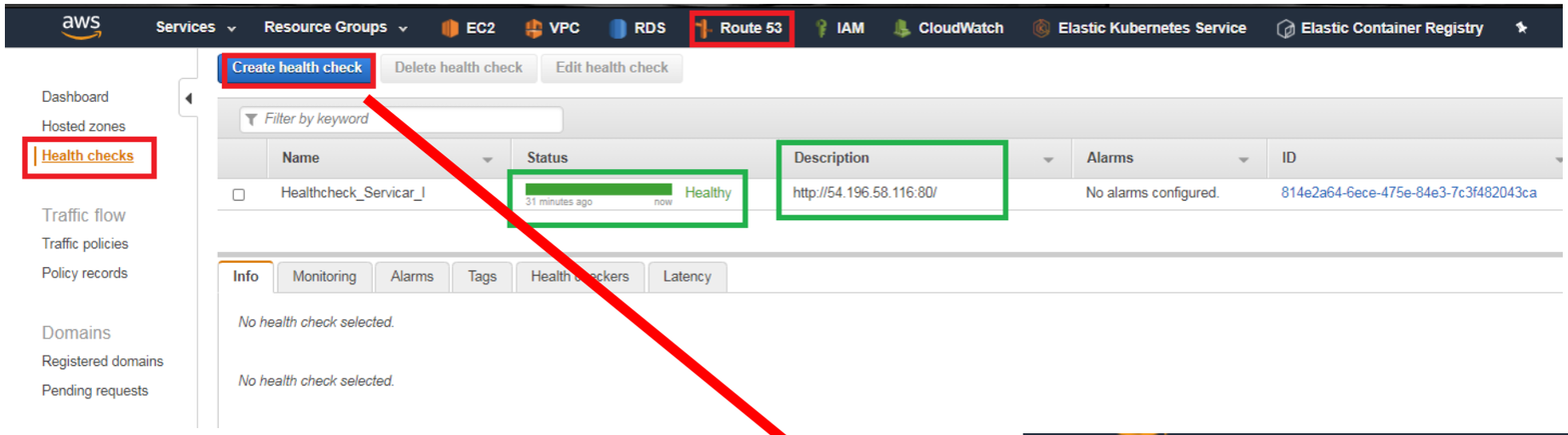
*** Records for Hosted Zones.**

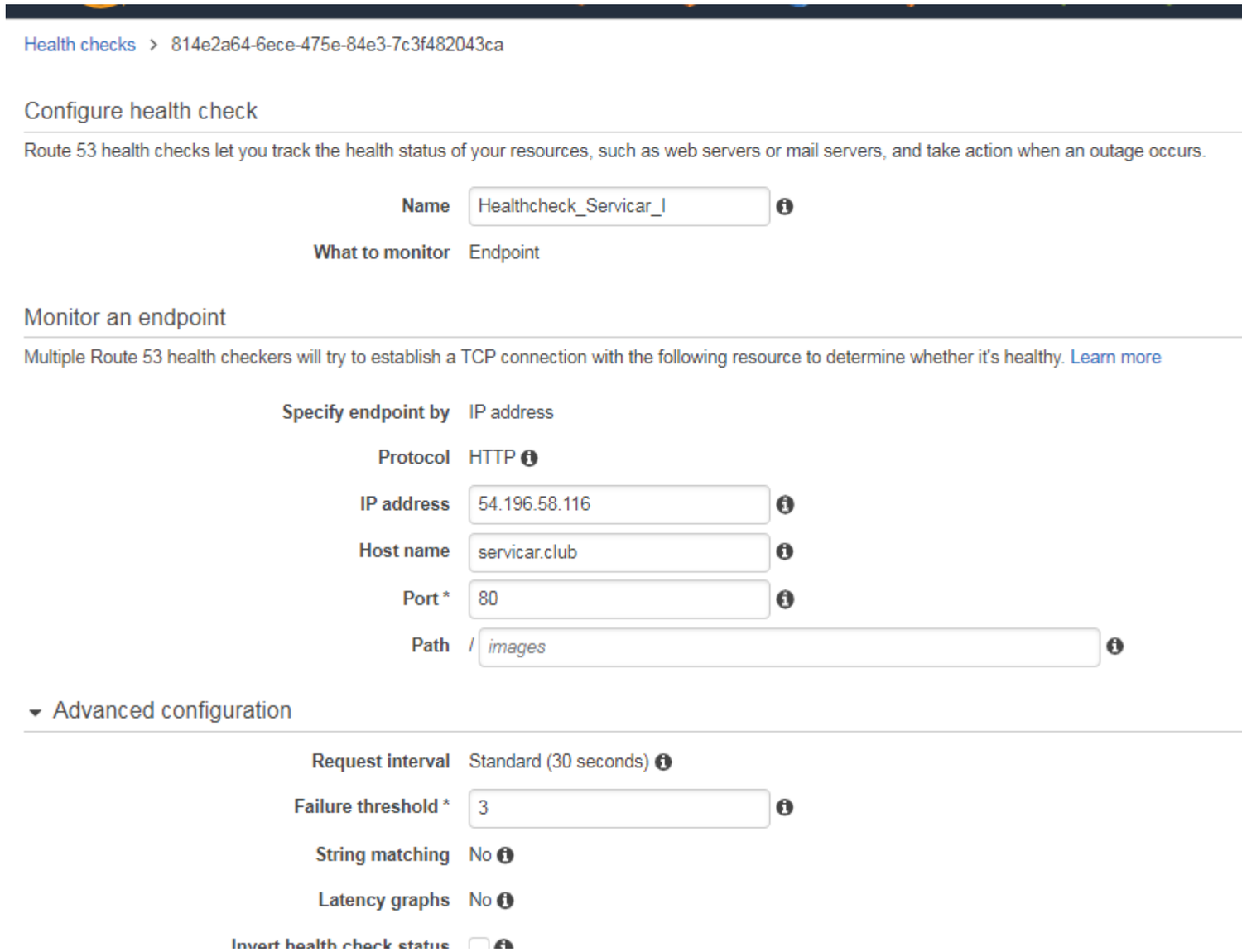
Simple, Weigthed, Failover, GeoLocation, Latency, Multivalue Answer.

*** Policies for Traffic Flow**

Weigthed, Failover, GeoLocation, Latency, Multivalue Answer, Geoproximity (Based on location of AWS DNS Resources then it choose your VPC Resources).

Route 53 – Health Check





Through healthcheck, you can check the target destination of your routing policy.

First step is to make Health check to define, the target is replying constantly.

Route 53 – Traffic Policy

- In addition to check resources at Hosted Zones, the flow applied policies to route traffic based on:
- **Simple route policy** (rp): i.e. web server.
- **Failover rp:** active-passive failover for region not service, otherwise simple rp.
- **Latency rp:** Best region based on its response time.
- **Multivalue answer rp:** Up to 8 healthy records.

Route 53 – Traffic Policy

- **Weighted rp:** New applications or Green projects. ie: Canary Releases.
- **Geolocation rp:** based on user location (country or continent).
- **Geoproximity rp.:** based on AWS resources location. Its only on Traffic Policy.

Routing Policies

Failover Policy

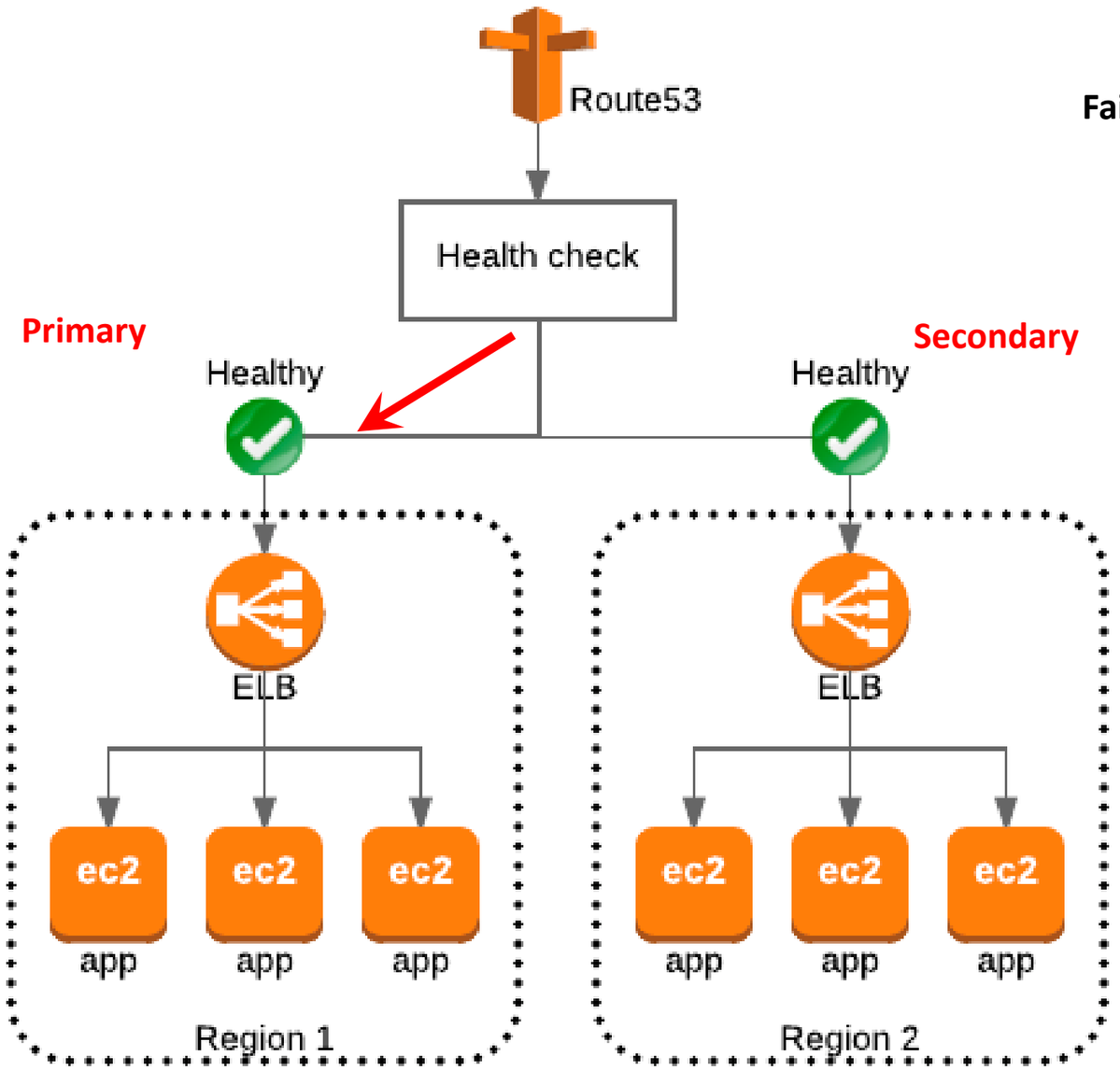


Figure 1 - Both regions operating normally

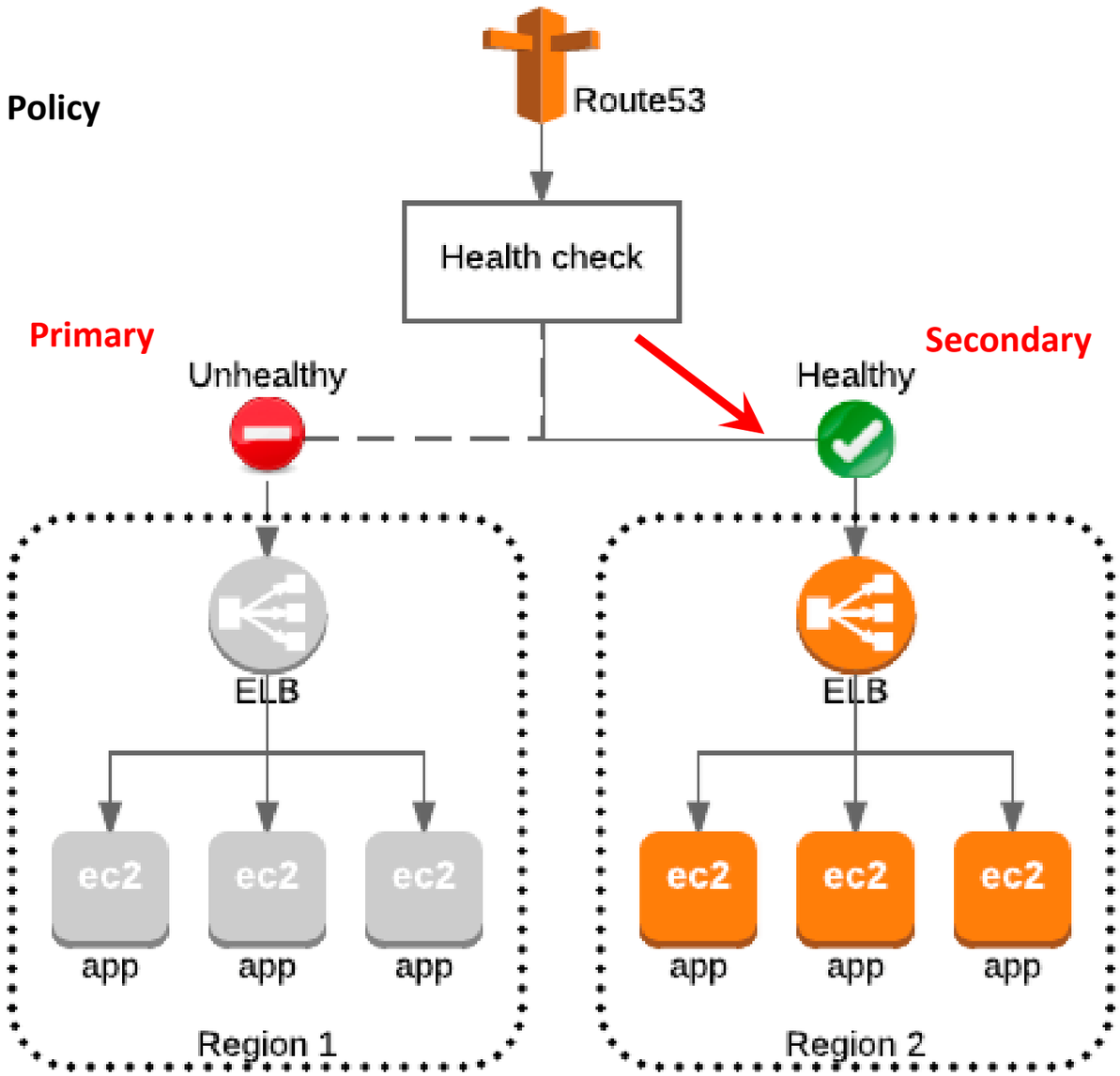
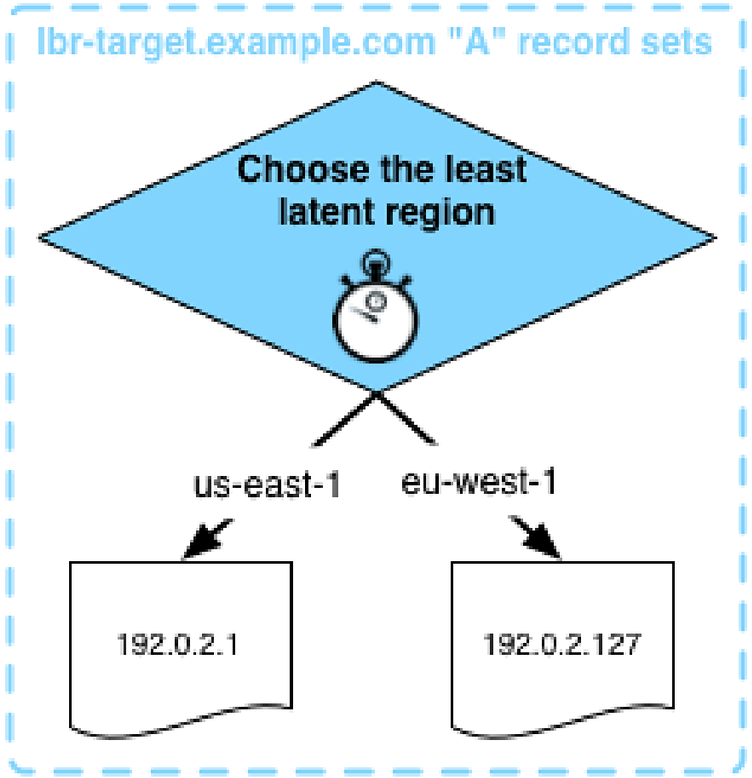
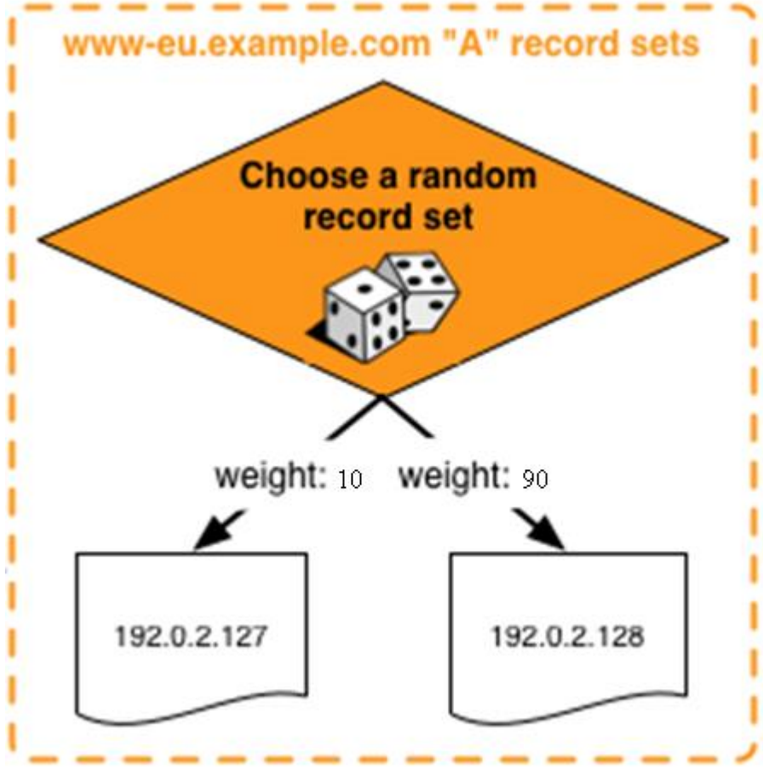


Figure 2 - region 1 experiencing issues

Routing Policies



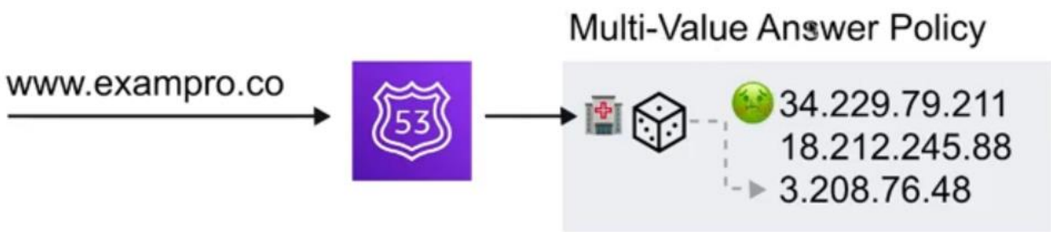
Latency Routing Policy: Based on source-destination latency and its latency table.



Weighted Routing Policy

Multi-value Answer Policy

Similar to Simple Routing, however with an added health check for your record set resources.

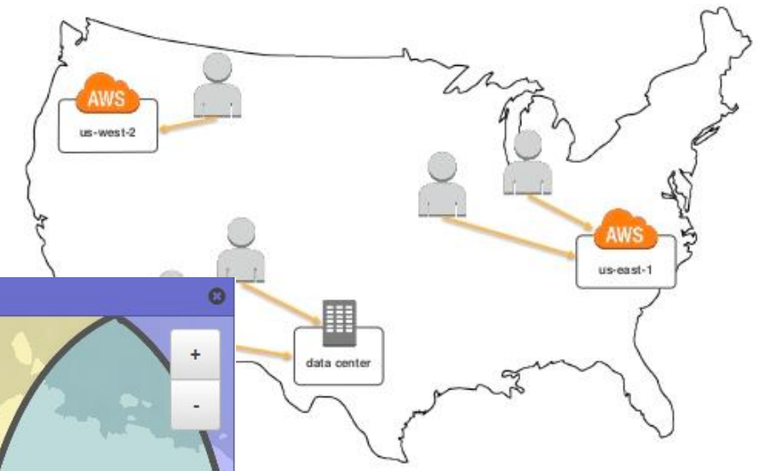


You can use simple routing with multiple values (one record with multiples IPs) however it doesn't check healthcheck, Route 53 only return ALL values to client who determine response or not.
With Multianswer policy, DNS return upto 8 random healthy records, and you create ALL records with the same DNS record type.

Taken from https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/ (15/05

Traffic Policy

GeoProximity Routing Policy: Used bias to increase georange to calculate the distance between source and AWS region. It choose the smallest distance.

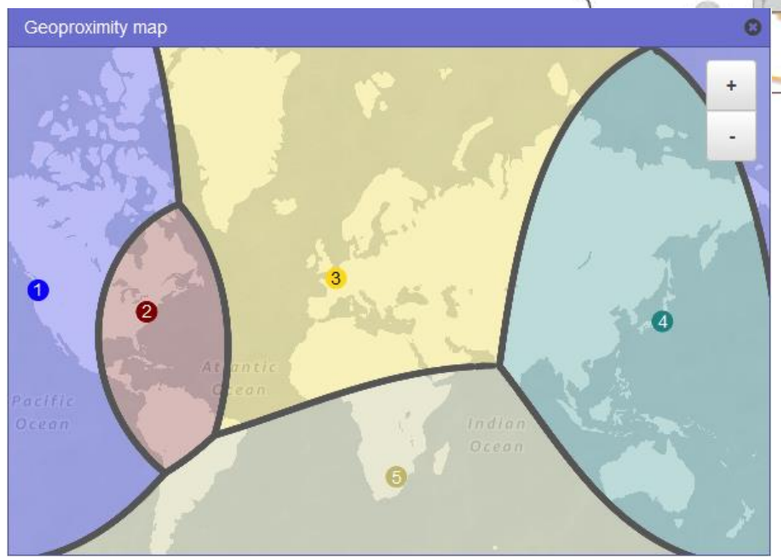


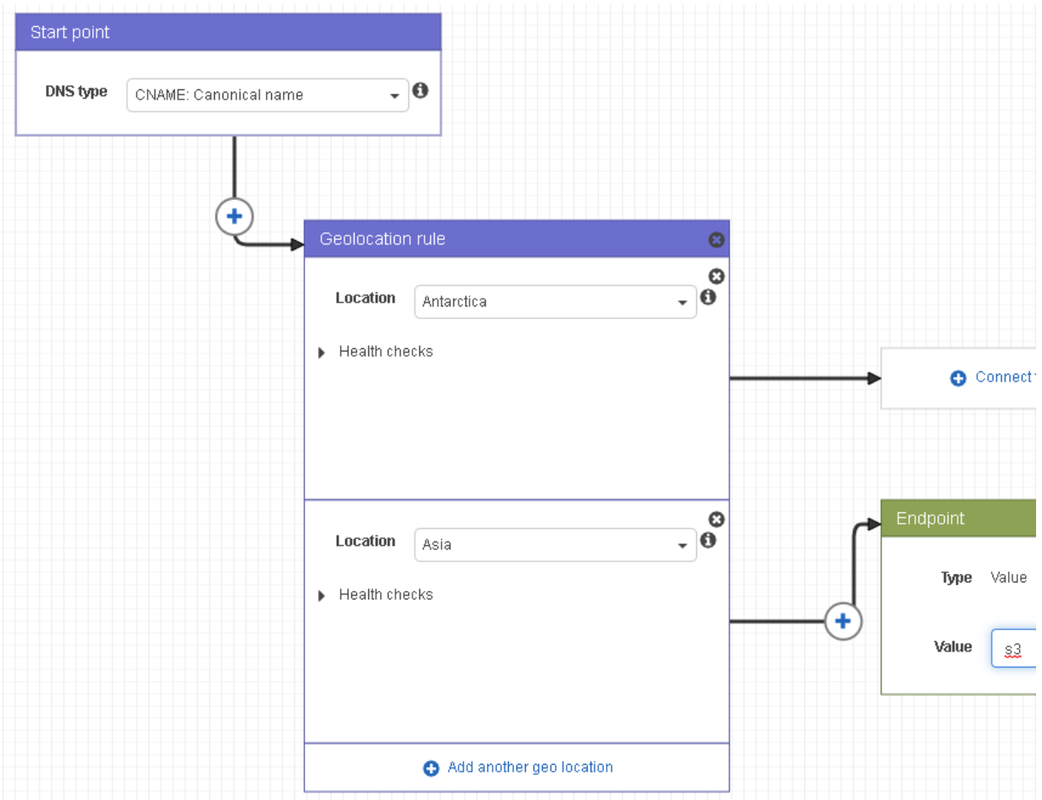
Positive bias

```
Biased distance = actual distance * [1 - (bias/100)]
```

Negative bias

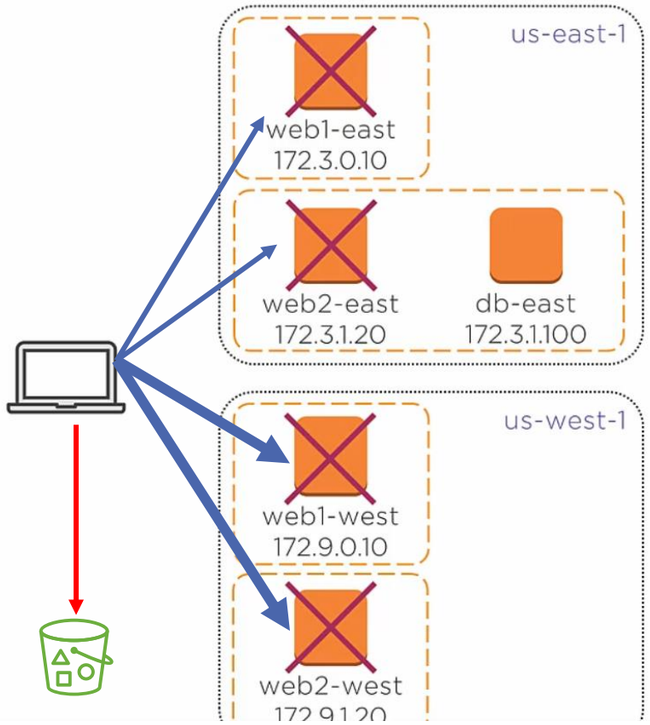
```
Biased distance = actual distance / [1 + (bias/100)]
```





GeoLocation Routing Policy: Routing based on Users location. Use case: Multinational Company with country portal (laws) or Netflix.

Chaining Routing Policies



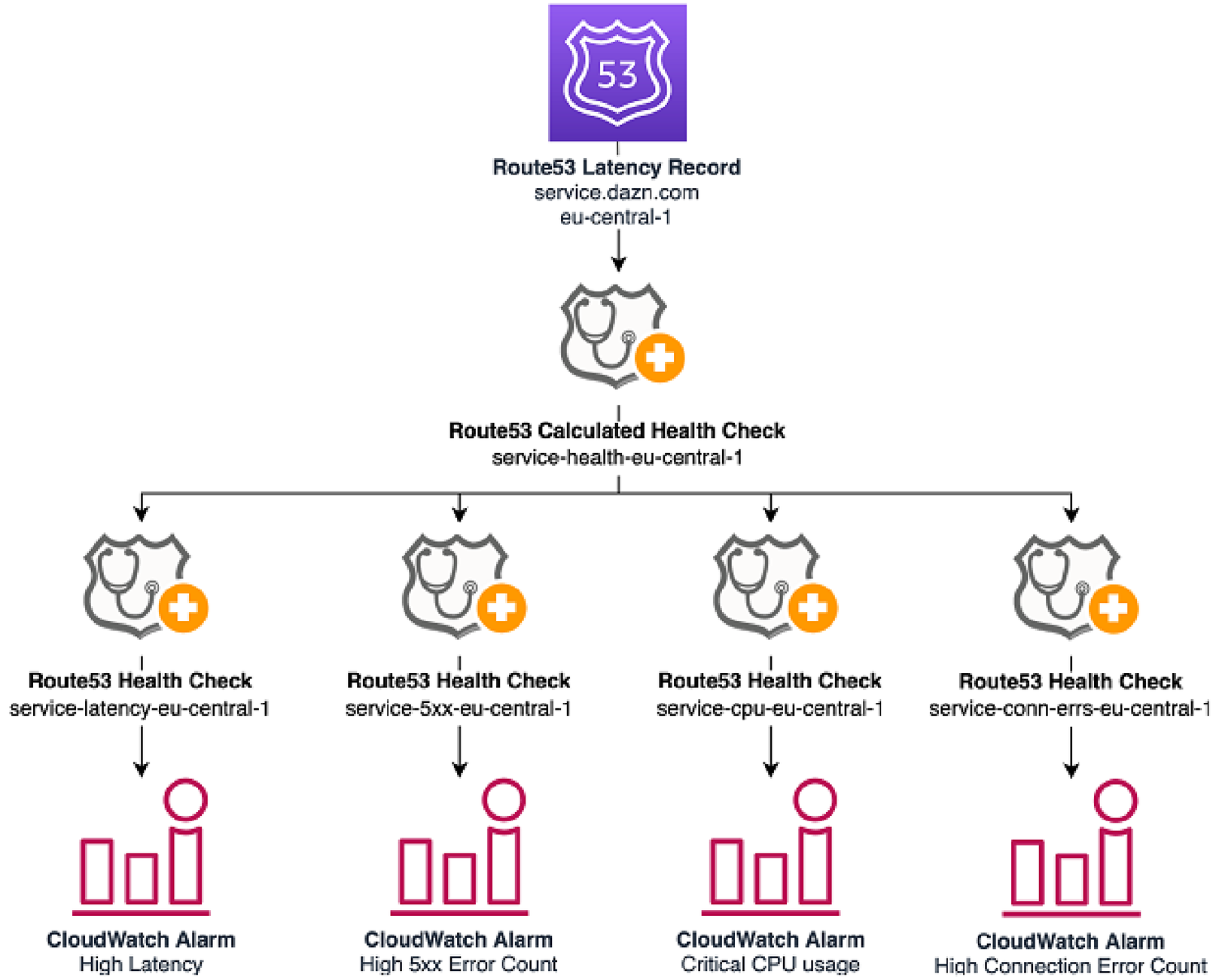
benpiper.host		Public
Name	Policy	Target
www	Failover (primary)	weighted
www	Failover (secondary)	S3 bucket
weighted	Weighted (10)	web1-east
weighted	Weighted (10)	web2-east
weighted	Weighted (20)	web1-west
weighted	Weighted (20)	web2-west
web1-east	Simple	52.206.88.55
web2-east	Simple	18.208.90.217
web1-west	Simple	54.219.0.218
web2-west	Simple	54.177.105.227

First a Failover Policy, then a Weighted Policy which rerouting to Simple Policy (subdomain).

Taken from https://app.pluralsight.com/player?course=aws-networking-deep-dive-route-53-dns (15/05/2020)

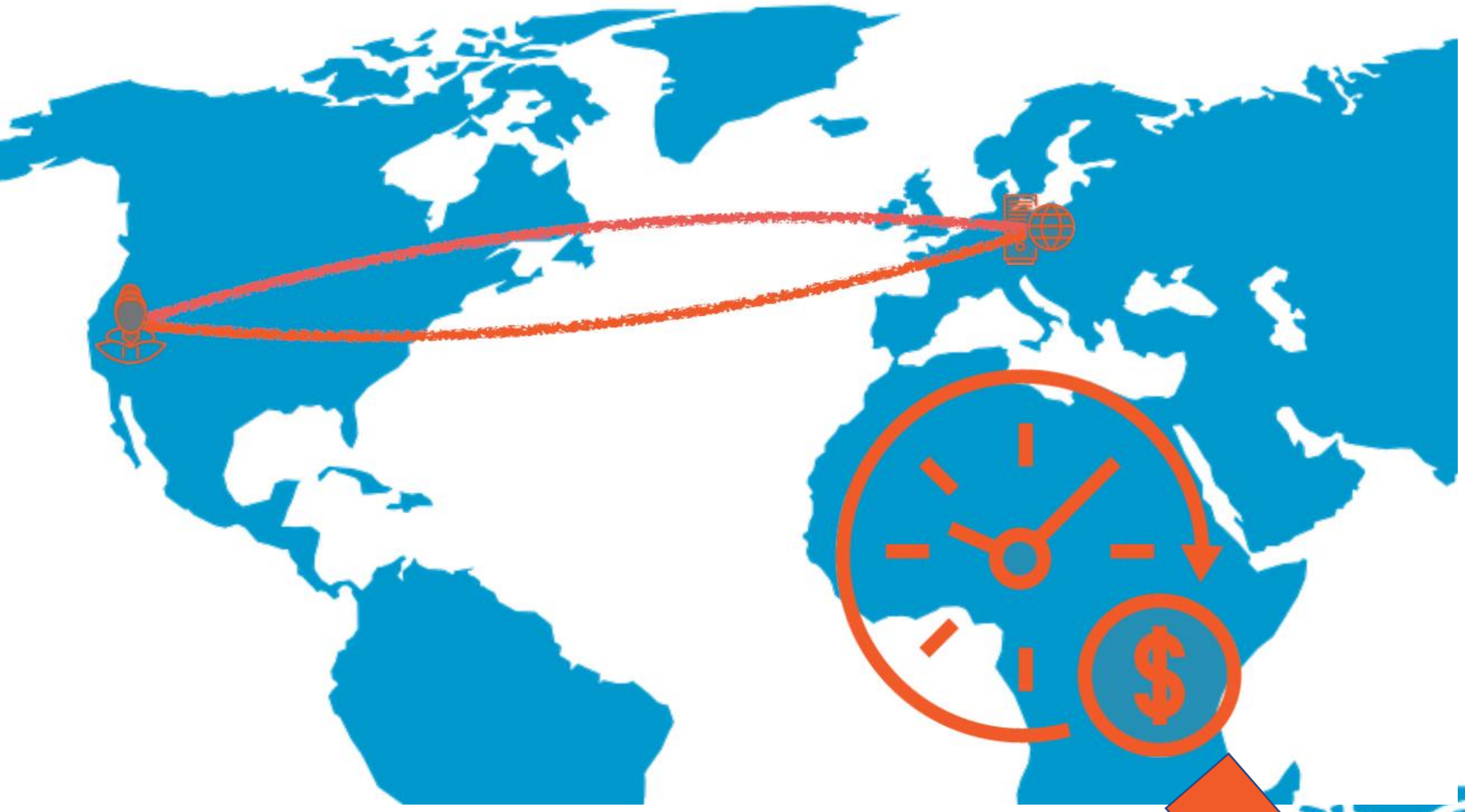
Additional Probes

Anticipated bad behavior on regions using CloudWatch and integrated with Route 53



Taken from https://medium.com/dazn-tech/how-to-implement-the-perfect-failover-strategy-using-amazon-route53-1cc4b19fa9c7 (18/07/2024)

Content Delivery Network - CDN



Key Points:

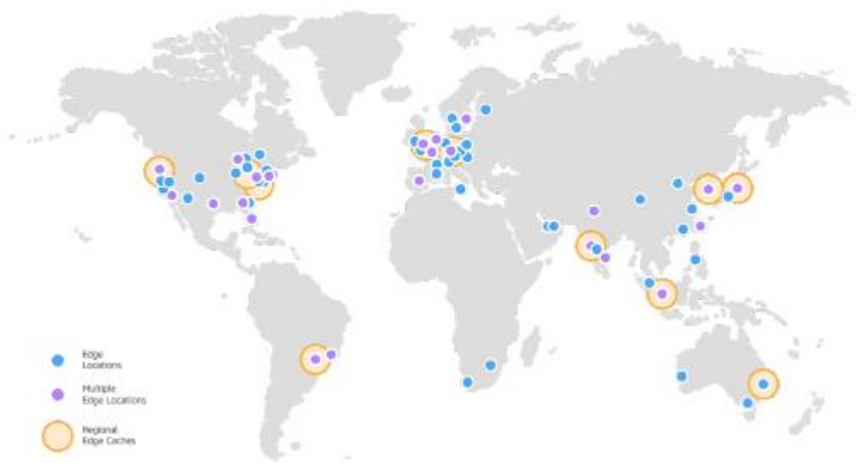
- Geographically Distributed Network
- Cached Static Content (Cfront use dynamic TOO!)
- Reduce distance between visitors
- Reduce response time

Taken from https://app.pluralsight.com/library/courses/cloudfront-aws-delivering-content (25/06/2021)

Cloudfront

Benefits:

Improving website load times (Reduce distance, reduce file sizes, optimizing certificate negotiation)
Reducing bandwidth costs (Reduced origin requests lower bandwidth costs)
Increasing content availability and redundancy (Load balancing, Intelligent failover)
Improving website security (Hosting TLS/SSL certificates, Preventing DDOS attacks, Enabling web application firewalls)

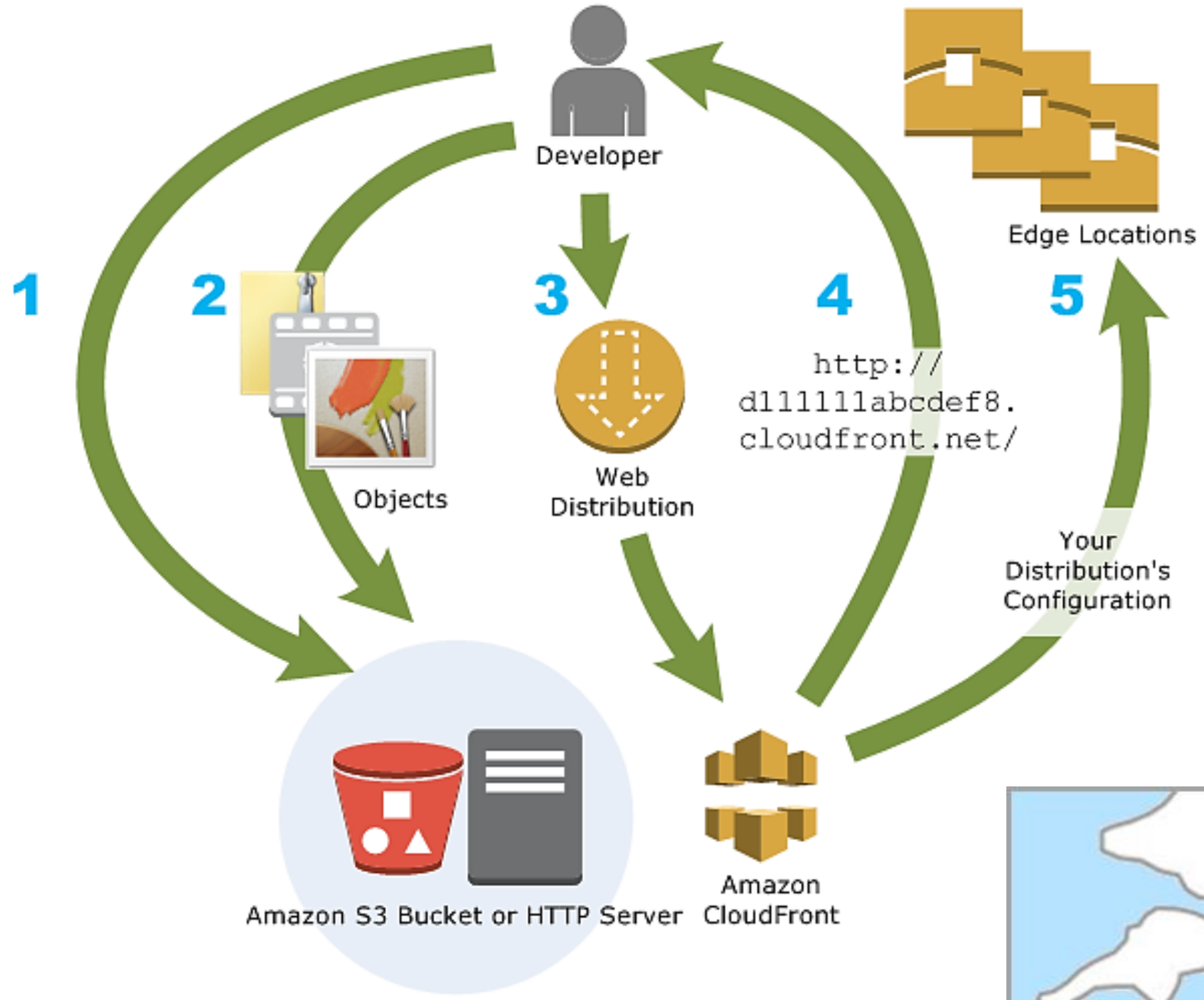


Taken from https://medium.com/dazn-tech/how-to-implement-the-perfect-failover-strategy-using-amazon-route53-1cc4b19fa9c7 (18/07/2024)

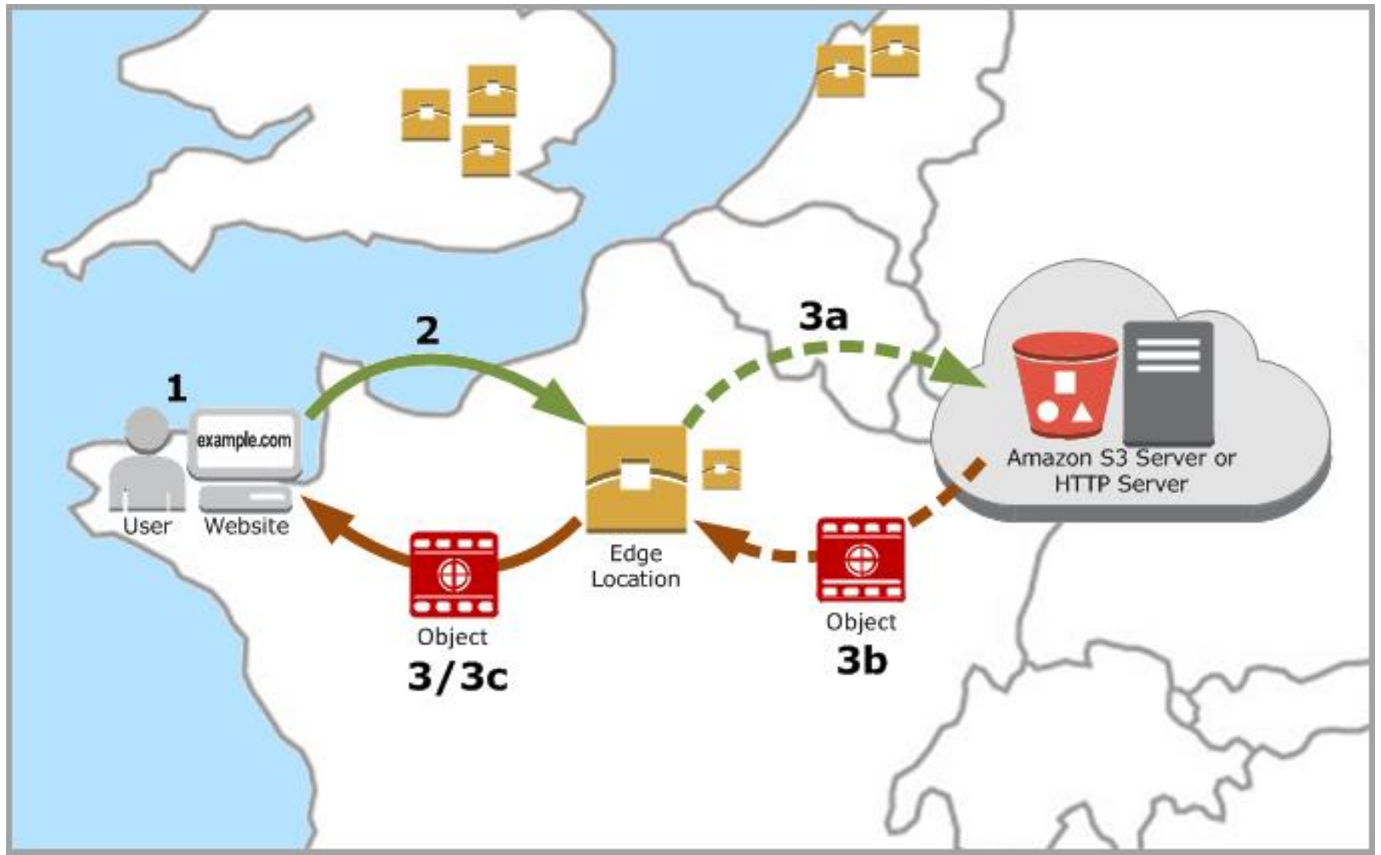
PERFORMANCE
Network optimizations for optimal performance
Dynamic or static content (HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS and PATCH)
Cache Retention
COST
Pay-as-you-go
Free data transfer
Reduced traffic to origin
AVAILABILITY
Increase application availability
Enabling redundancy for origins
SECURITY
AWS Shield & WAF
SSL/TLS Encryptions and HTTPS
Access Control
PROGRAMMABLE
Full-featured APIs
Edge behaviors
Lambda@Edge

Note: On Regional Edge Cache, works with GET Method only.

How to work



Taken from https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html and https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/HowCloudFrontWorks.html (30/07/2024)



Key Terms

CloudFront Distribution

The collection of an ORIGIN and all the associated caching and traffic handling rules

CloudFront Origin

An Origin is where you direct CloudFront to sends requests for your content.

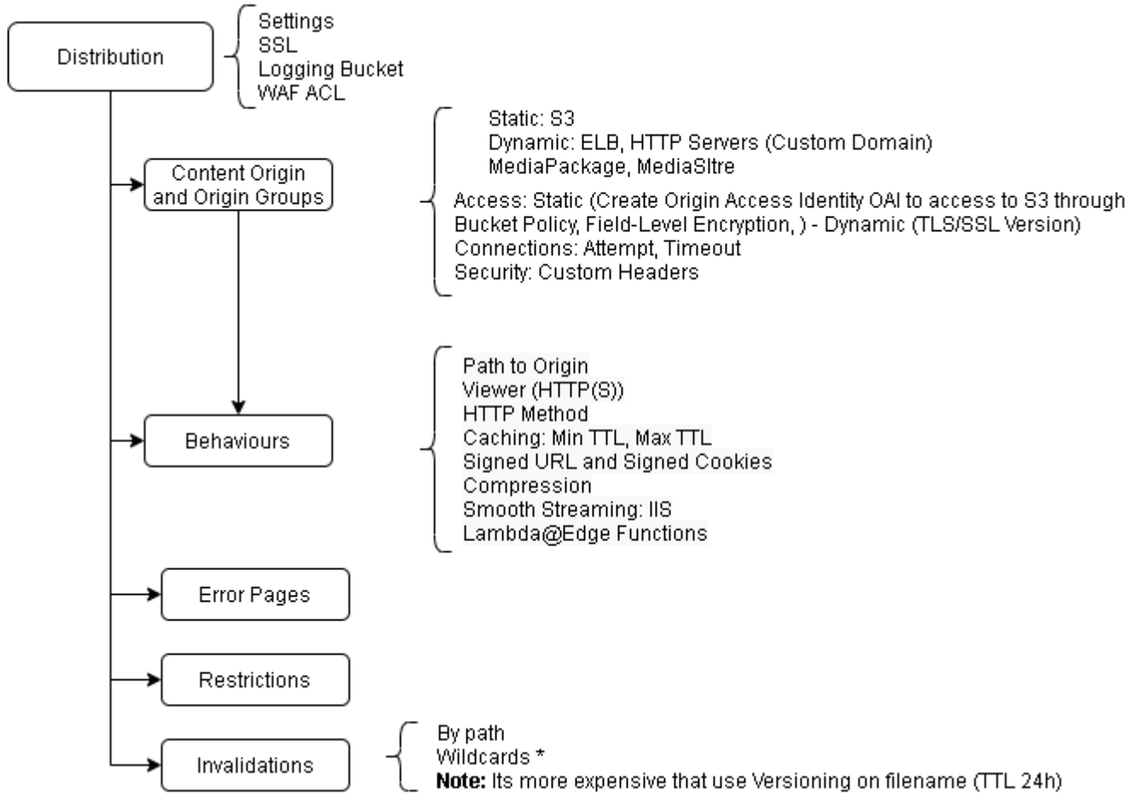
Caching Behavior

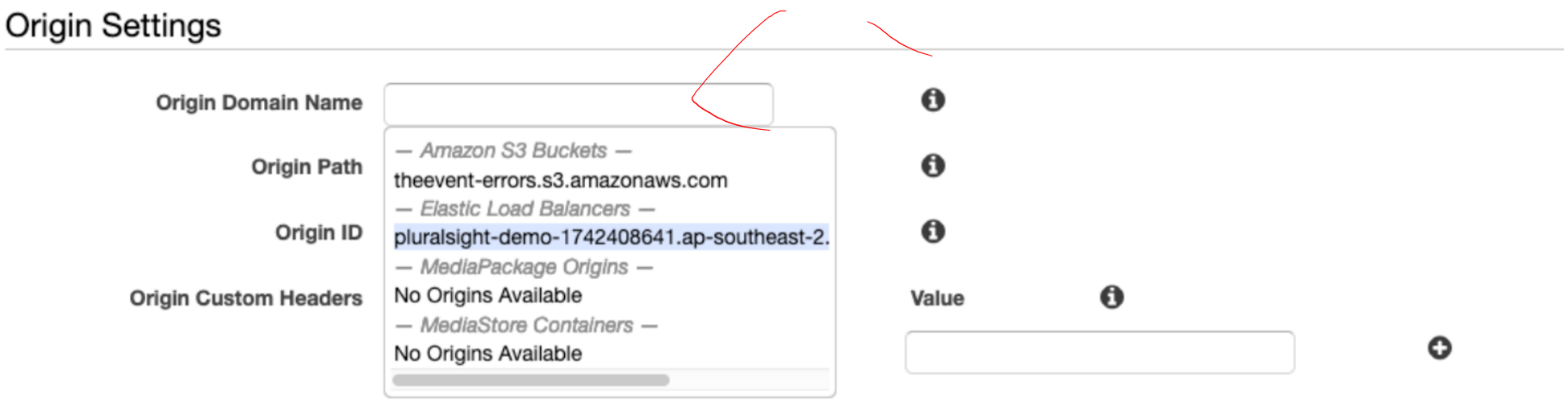
Rules which define how CloudFront handles and processes incoming requests.

Contains: Origin Definition, Cache Duration, Forwarding, Request Headers, Compression Encryption

CloudFront Invalidation

Method to notify CloudFront to retrieve a refreshed file from your Origin.





Taken from https://app.pluralsight.com/library/courses/cloudfront-aws-delivering-content (25/06/2021)

Distribution Settings

Price Class: Use All Edge Locations (Best Performance)

AWS WAF Web ACL: None

Alternate Domain Names (CNAMEs):

SSL Certificate:
- Default CloudFront Certificate (*.cloudfront.net)
- Custom SSL Certificate (example.com):

Request or Import a Certificate with ACM

Supported HTTP Versions:
- HTTP/2, HTTP/1.1, HTTP/1.0
- HTTP/1.1, HTTP/1.0

Default Root Object:

Logging:
- On
- Off

Bucket for Logs:

Log Prefix:

Cookie Logging:
- On
- Off

Enable IPv6: ☑

Learn more

Comment:

Distribution State:
- Enabled
- Disabled

Make a certificate using ACM
and DNS Record using Alias to this Distribution

Taken from https://app.pluralsight.com/library/courses/cloudfront-aws-delivering-content (25/06/2021)

Default Behavior

Path Pattern Default (*)

Viewer Protocol Policy
- (●) HTTP and HTTPS
- ( ) Redirect HTTP to HTTPS
- ( ) HTTPS Only

Allowed HTTP Methods
- (●) GET, HEAD
- ( ) GET, HEAD, OPTIONS
- ( ) GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Field-level Encryption Config [ ]

Cached HTTP Methods GET, HEAD (Cached by default)

Cache Based on Selected Request Headers None (Improves Caching)

Learn More

Object Caching
- (●) Use Origin Cache Headers
- ( ) Customize

Learn More

Minimum TTL 0

Maximum TTL 31536000

Default TTL 86400

Forward Cookies None (Improves Caching)

Query String Forwarding and Caching None (Improves Caching)

Smooth Streaming
- ( ) Yes
- (●) No

Restrict Viewer Access (Use Signed URLs or Signed Cookies)
- ( ) Yes
- (●) No

Compress Objects Automatically
- ( ) Yes
- (●) No

Learn More

Lambda Function Associations

CloudFront Event	Lambda Function ARN
Select Event Type	

Learn More

Taken from https://app.pluralsight.com/library/courses/cloudfront-aws-delivering-content (25/06/2021)

Pricing

Free Tier

Included in Always Free Tier

- 1 TB of data transfer out to the internet per month
- 10,000,000 HTTP or HTTPS Requests per month
- 2,000,000 CloudFront Function invocations per month
- 2,000,000 CloudFront KeyValueStore reads per month
- Free SSL certificates
- No limitations, all features available

On-demand

Amazon CloudFront charges traffic served based on the following dimensions:

Data Transfer Out (Internet/Origin)

HTTP/HTTPS Requests

Other optional features are priced as shown below

Discounted Pricing

Custom Pricing

For customers who are willing to make certain minimum traffic commits (typically 10 TB/month or higher).
Contact Us

CloudFront Security Savings Bundle

Self-service pricing plan that combines CloudFront with benefits for AWS WAF to provide significant savings in exchange for a monthly spend commitment for a 1 year term.

On-demand Pricing

Regional Data Transfer Out to Internet (per GB)

Per Month	United States, Mexico, & Canada	Europe & Israel	South Africa, Kenya, & Middle East	South America	Japan	Australia & New Zealand	Hong Kong, Indonesia, Philippines, Singapore, South Korea, Taiwan, & Thailand	India
First 10TB	$0.085	$0.085	$0.110	$0.110	$0.114	$0.114	$0.120	$0.109
Next 40TB	$0.080	$0.080	$0.105	$0.105	$0.089	$0.098	$0.100	$0.085
Next 100TB	$0.060	$0.060	$0.090	$0.090	$0.086	$0.094	$0.095	$0.082
Next 350TB	$0.040	$0.040	$0.080	$0.080	$0.084	$0.092	$0.090	$0.080
Next 524TB	$0.030	$0.030	$0.060	$0.060	$0.080	$0.090	$0.080	$0.078
Next 4PB	$0.025	$0.025	$0.050	$0.050	$0.070	$0.085	$0.070	$0.075
Over 5PB	$0.020	$0.020	$0.040	$0.040	$0.060	$0.080	$0.060	$0.072

Customers willing to make minimum traffic commits of typically 10 TB/month or higher are eligible for discounted pricing. Contact us

Taken from https://aws.amazon.com/cloudfront/pricing/ (18/07/2024)

Pricing examples

Pricing Example 2: Dynamic e-commerce application

You use CloudFront real-time logs to get information about requests made to a distribution in real time. You also need to invalidate objects from CloudFront Cache when there is an update to your website content.

For Mexico, the data transfer out to internet is charged at $0.085 per GB after the first TB. HTTPS requests are charged at $0.01 per 10,000 requests after the first 20,000,000. Real-time logs are charged based on the number of log lines that are generated. You pay $0.01 for every 1,000,000 log lines that CloudFront publishes to your log destination; every request generates 1 log line. Finally, let's assume you make a total of 2,000 invalidation requests per month for all your distributions. The first 1,000 invalidation paths that you submit per month are free. Thereafter, you will be charged $0.005 per path requested for invalidation.

1 TB data transfer ou

10,000,000 HTTPS requ

10,000,000 log lines

First 1,000 invalidation p

Remaining 1,000 invalidatic

Pricing Example 3: Media streaming application

When streaming video, you use a Lambda@Edge origin response trigger for response customization. You also use Origin Shield to reduce load on your origins by providing just-in-time packaging for live streams and on-the-fly image processing.

For USA, the data transfer out to internet is charged at $0.085 per GB after the first TB. HTTPS requests are charged at $0.01 per 10,000 requests after the first 20,000,000. Let's assume your Lambda@Edge function executed 60 million times in one month, and it ran for 10ms each time. L@E charges are calculated based on compute and requests. Monthly compute price is $0.00000625125 per 128 MB-second, and the monthly request price is $0.60 per 1 million requests. Origin Shield request pricing for origins configured in USA is $0.0075 per 10,000 HTTPS requests. Let's assume the total number of dynamic requests going to Origin Shield is 10 percent of all your HTTPS requests: 10% x 200M = 20M.

	Cost Calculation	Total Cost
20,000GB Data transfer out	(1 TB x $0)+ (19,000 x $0.085 per GB)	$1615
200,000,000 HTTPS requests	(10,000,000 x $0) + (190,000,000 x $0.01 per 10,000 requests)	$190
60,000,000ms of Lambda@Edge compute costs	60,000,000ms x 0.01sec x $0.00000625125 per 128 MB-second	$3.78
60,000,000 Lambda@Edge requests	60,000,000 x $0.60 per 1,000,000 requests	$36
20,000,000 Origin Shield requests	20,000,000 x $0.0075 per 10,000 requests	$15
	Total Monthly Cost	**$1,859.78**

Taken from https://aws.amazon.com/cloudfront/pricing/ (18/07/2024)

AWS Certificate Manager


AWS Certificate Manager (ACM)


Elastic Load Balancing


Amazon CloudFront


AWS Elastic Beanstalk


AWS Nitro Enclaves


Amazon API Gateway


AWS CloudFormation

Old Steps: Generate CSR, send it to CA, and return & install certificate.
Service to issue Public or Private Certificates (Also import).
Options: SSL or TLS.
Auto Renovation, Multiple Domain Names, Wildcards, Algorithms.

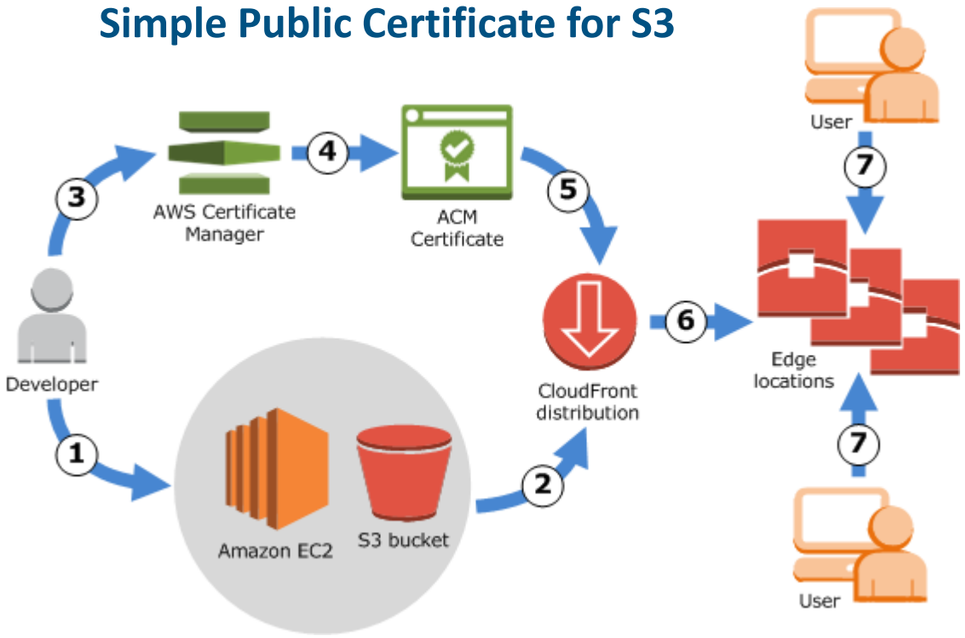
Pricing:
Free Public Certificates due to link to AWS Services.
Private Certificates: CA Authority U$400 Month, and after per # of certificates

Certificates from a general-purpose mode private CA

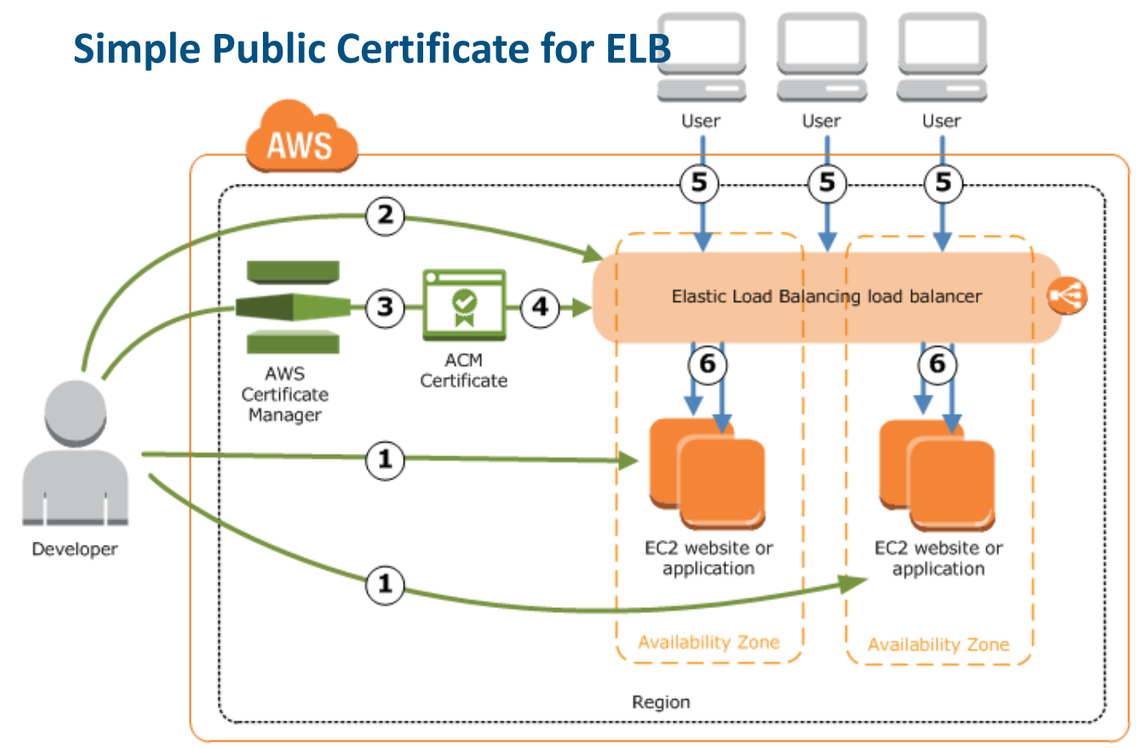
Number of certificates issued in the month / per Region	Price (per certificate)
1 - 1,000 certificates	$0.75
1,001 - 10,000 certificates	$0.35
10,001+ certificates	$0.001

More info at
https://docs.aws.amazon.com/acm/latest/userguide/acm-services.html and https://aws.amazon.com/certificate-manager/pricing/?nc=sn&loc=3 (30/07/2024)

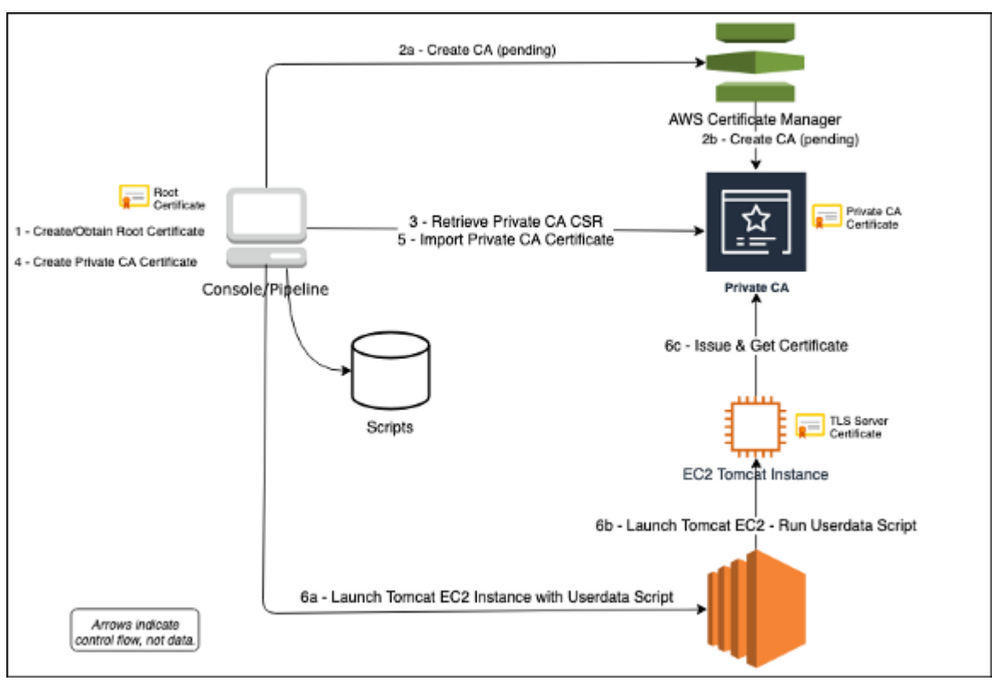
Simple Public Certificate for S3



Simple Public Certificate for ELB



Private Certificate for EC2 Instance (Old Way)



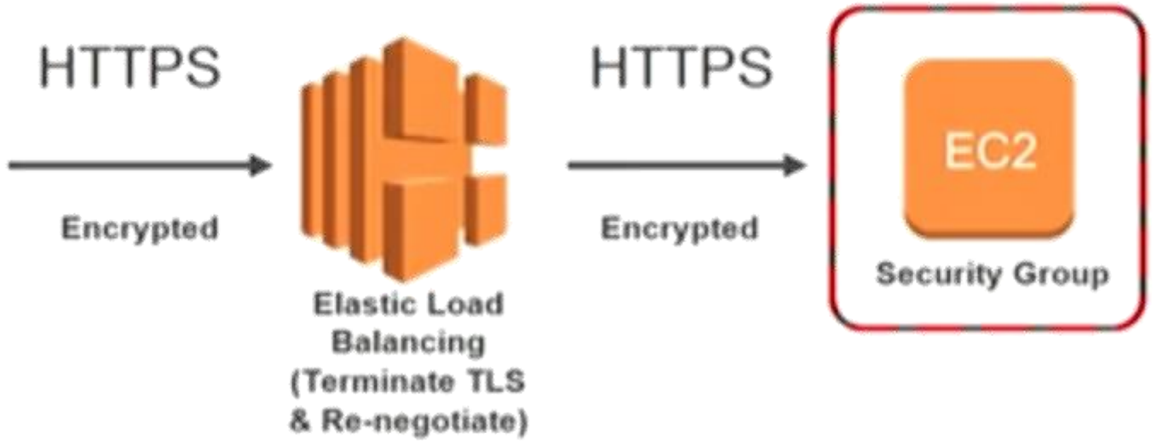
Taken from https://medium.com/@frederik.willaert/setting-up-a-private-certificate-authority-on-aws-b220154cf98 and https://stackoverflow.com/questions/43553181/aws-certificate-manager-for-elb-pointing-to-a-apache-server-running-on-ec2 (18/07/2024)

TLS Termination and Renegotiation

TLS Pass Through

TLS Termination

TLS Termination & Renegotiate



Taken from https://ashishrajan.medium.com/aws-security-best-practices-amazon-certificate-manager-aka-acm-cloudsecurity-b6e28ff1715d (30/07/2024)