# AWS – ROUTE53

BY

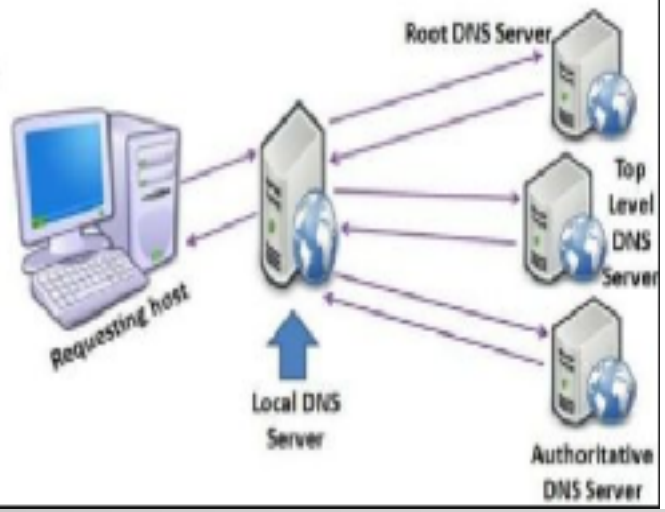
KESHAV KUMMARI

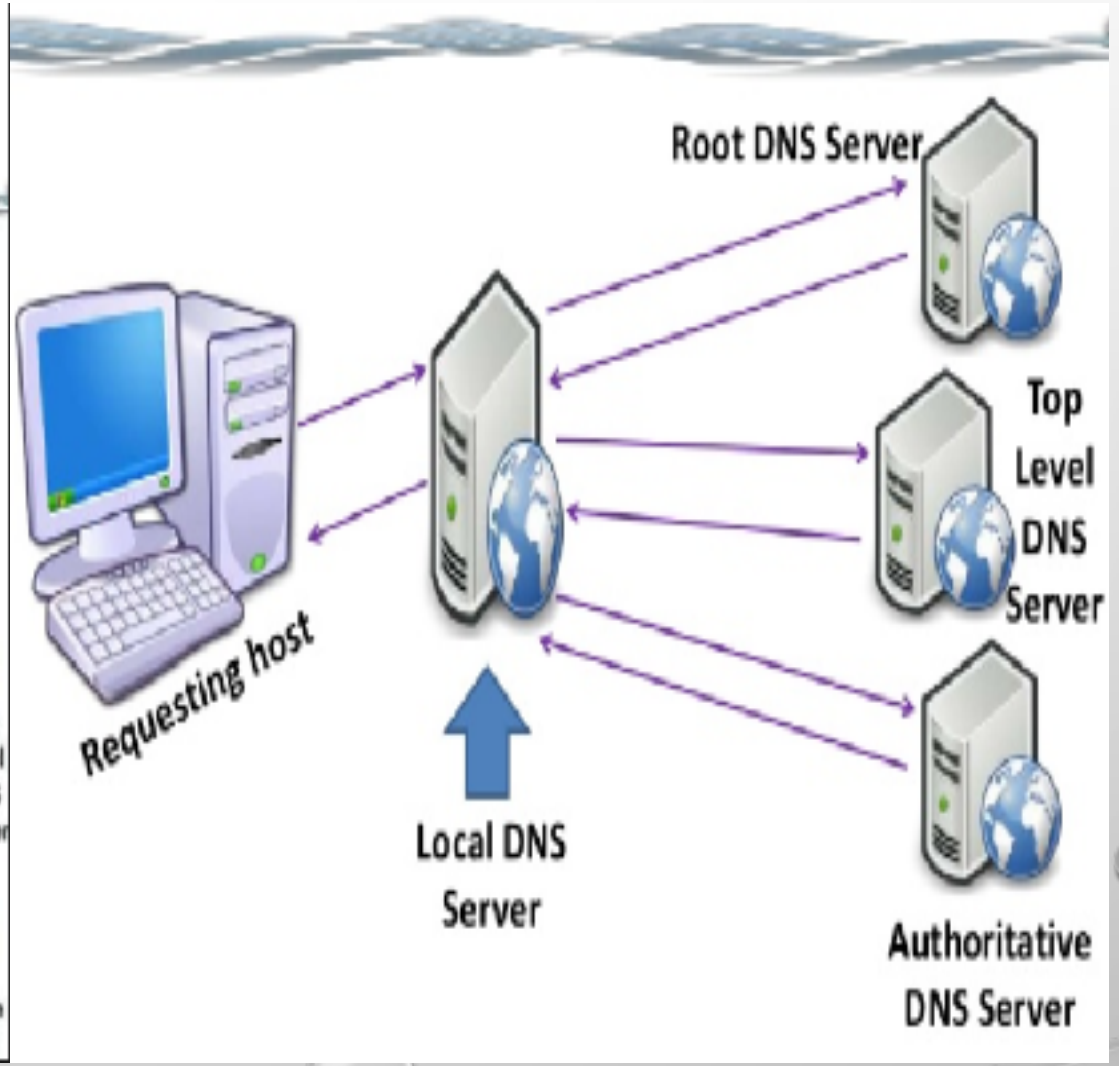
# DNS INDEX

# 1. DNS

## What is DNS?

- DNS stands for Domain Name System
- DNS is a hierarchical naming system for domain services, or any resource connected with internet or private network.
- The DNS translates Internet domain and host names to IP addresses.



# IPV4 VS IPV6

| | Internet Protocol version 4 (IPv4) | Internet Protocol version 6 (IPv6) |
|---|---|---|
| Deployed | 1981 | 1999 |
| Address Size | 32-bit number | 128-bit number |
| Address Format | Dotted Decimal Notation: 192.149.252.76 | Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD |
| Prefix Notation | 192.149.0.0/24 | 3FFE:F200:0234::/48 |
| Number of Addresses | $2^{32}$ = ~4,294,967,296 | $2^{128}$ = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456 |

IP CLASSES ADDRESS RANGE

| USES | CLASSES | IP RANGE | SUBNET MASK | PREFIX MASK | HOST PER SUBNET |
|---|---|---|---|---|---|
| PUBLIC IP DISTRIBUTION ADDRESS | CLASS-A | 0-126 | 255.0.0.0 | /8 | 16777216 |
| | CLASS-B | 128-191 | 255.255.0.0 | /16 | 65535 |
| | CLASS-C | 192-223 | 255.255.255.0 | /24 | 256 |
| MULTICAST IP | CLASS-D | 224-239 | | /4-/32 | |
| RESEARCH PURPOSE | CLASS-E | 240-255 | | /4-/32 | |
| | | | | | |
| NOTE- | | | | | |
| PRIVATE IP ADDRESS RANGE | | | | | |
| | CLASS-A | 10.0.0.0-10.255.255.255 | | | |
| | CLASS-B | 172.16.0.0-172.31.255.255 | | | |
| | CLASS-C | 192.168.0.0-192.168.0.255 | | | |
| | | | | | |
| Universal loopback Address | 127.0.0.1 | | | | |
| Automatic Private IP Addressing | 169.254.0.0 to 169.254.255.255 | | | | |

# TOP LEVEL DOMAINS



## IP Address Assignments

- Every network interface adapter on a network must have
  - The same network identifier as the others on the network
  - A unique host identifier
- The Internet Assigned Numbers Authority (IANA) assigns network identifiers, but you typically obtain network addresses from an Internet service provider (ISP).
- Network administrators assign host identifiers.

# DOMAIN REGISTRERS

Because all of the names in a given domain name have to be unique there needs to be a way to organize this all so that domain names aren't duplicated. This is where domain registrars come in. A registrar is an authority that can assign domain names directly under one or more top-level domains. These domains are registered with InterNIC, a service of ICANN, which enforces uniqueness of domain names across the Internet. Each domain name becomes registered in a central database known as the WhoIS database.

Popular domain registrars include GoDaddy.com, 123-reg.co.uk etc.

# SOA RECORDS

The SOA record stores information about;

- The name of the server that supplied the data for the zone.
- The administrator of the zone.
- The current version of the data file.
- The number of seconds a secondary name server should wait before checking for updates.
- The number of seconds a secondary name server should wait before retrying a failed zone transfer.
- The maximum number of seconds that a secondary name server can use data before it must either be refreshed or expire.
- The default number of seconds for the time-to-live file on resource records.

# NS RECORDS & A RECORDS

- NS STANDS FOR NAME SERVER RECORDS AND ARE USED BY TOP LEVEL DOMAIN SERVERS TO DIRECT TRAFIC TO THE CONTENT DNS SERVER WHICH CONTAINS THE AUTHORITATIVE DNS RECORDS.

- A RECORDS :
  - AN “A” RECORD IS THE FUNDAMENTAL TYPE OF DNS RECORD AND THE “A” IN A RECORD STANDS FOR “ADDRESS”.
  - THE “A” RECORD IS USED BY A COMPUTE TO TRANSLATE THE NAME OF THE DOMAIN TO THE IP ADDRESS.
  - FOR EXAMPLE HTTP://WWW.KESHAVKUMMARI.COM MIGHT POINT TO HTTP://13.126.193.140

# TTL & CNAMES

- **TTL:**
- THE LENGTH THAT A DNS RECORD IS CACHED ON EITHER THE RESOLVING SERVER OR THE USERS OWN LOCAL PC IS EQUAL TO THE VALUE OF THE “TIME TO LIVE”(TTL) IN SECONDS.
- THE LOWER THE TIME TO LIVE, THE FASTER CHANGES TO DNS RECORDS TAKE TO PROPAGATE THROUGHOUT THE INTERNET.

- **CNAMES :**
  - A CANONICAL NAME(CNAME) CAN BE USED TO RESOLVE ONE DOMAIN NAME TO ANOTHER.
  - FOR EXAMPLE, YOU MAY HAVE A MOBILE WEBSITE WITH THE DOMAIN NAME HTTP://M.KESHAVKUMMARI.COM THAT IS USED FOR FOR WHEN USERS BROWSE YOUR DOMAIN NAME ON THEIR MOBILE DEVICES.
  - YOU MAY ALSO WANT THE NAME HTTP://MOBILE.KESHAVKUMMARI.COM TO RESOLVE TO THIS SAME ADDRESS.

# ALIAS RECORDS

- ALIAS RECORDS ARE USED TO MAP RESOURCE RECORD SETS IN YOUR HOSTED ZONE TO **ELASTIC LOAD BALANCERS**, **CLOUDFRONT DISTRIBUTIONS**, OR **S3 BUCKETS** THAT ARE CONFIGURED AS WEBSITES.
- ALIAS RECORDS WORK LIKE A CNAME RECORD IN THAT YOU CAN MAP ONE DNS NAME(WWW.EXAMPLE.COM) TO ANOTHER "TARGET"DNS NAME(ELB1234.ELB.AMAZONAWS.COM).
- KEY DIFFERENCE – A CNAME CAN NOT BE USED FOR NAKED DOMAIN NAMES(ZONE APEX).
- YOU CAN NOT HAVE A CNAME FOR HTTP://CKK.COM , IT MUST BE EITHER AN A RECORD OR AN ALIAS.

# ALIAS RECORDS

- ALIAS RESOURCE RECORD SETS CAN SAVE YOU TIME BECAUSE AMAZON ROUTE 53 AUTOMATICALLY RECOGNIZES CHANGES IN THE RECORD SETS THAT THE ALIAS RESOURCE RECORD SET REFERS TO.

- FOR EXAMPLE, SUPPOSE AN ALIAS RESOURCE RECORD SET FOR EXAMPLE.COM POINTS TO AN ELB LOAD BALANCER AT LB1-123.AP-SOUTH-1.ELB.AMAZONAWS.COM.

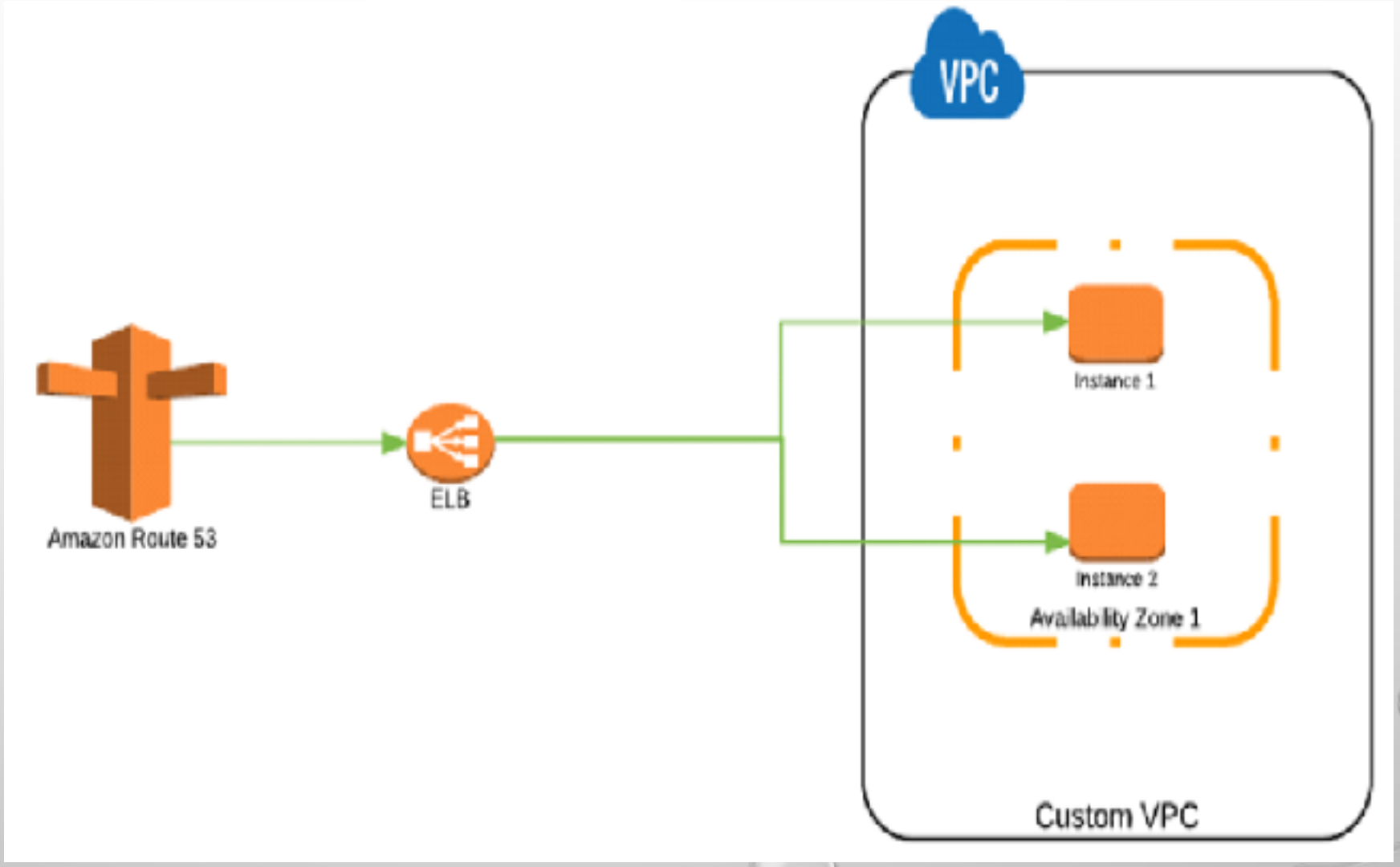
- IF THE IP ADDRESS OF THE LOAD BALANCER CHANGES, AMAZON ROUTE 53 WILL AUTOMATICALLY REFLECT THOSE CHANGES IN DNS ANSERS FOR EXAMPLE.COM WIHTOUT ANY CHANGES TO THE HOSTED ZONE THAT CONTAINS RESOURCE RECORD SETS FOR EXAMPLE.COM

# REGISTER A DOMAIN

- FROM GODADDY OR AWS OR VARIOUS OTHER VENDORS.

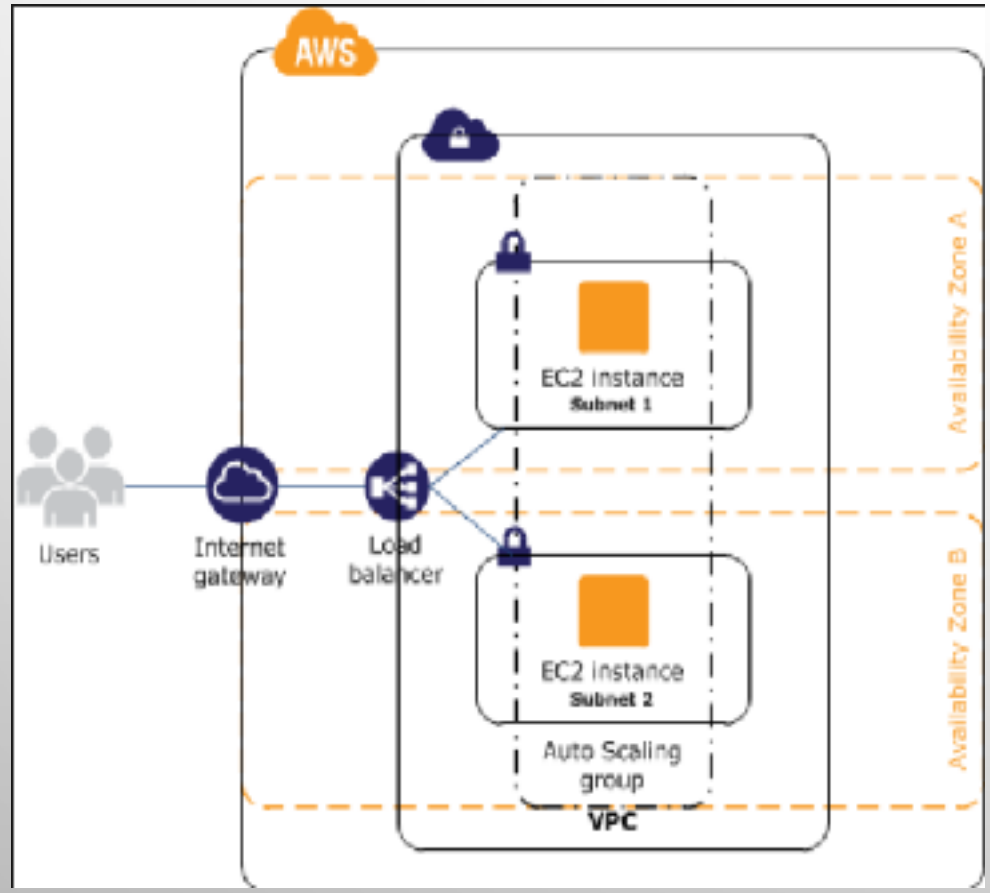
# SIMPLE ROUTING POLICY LAB

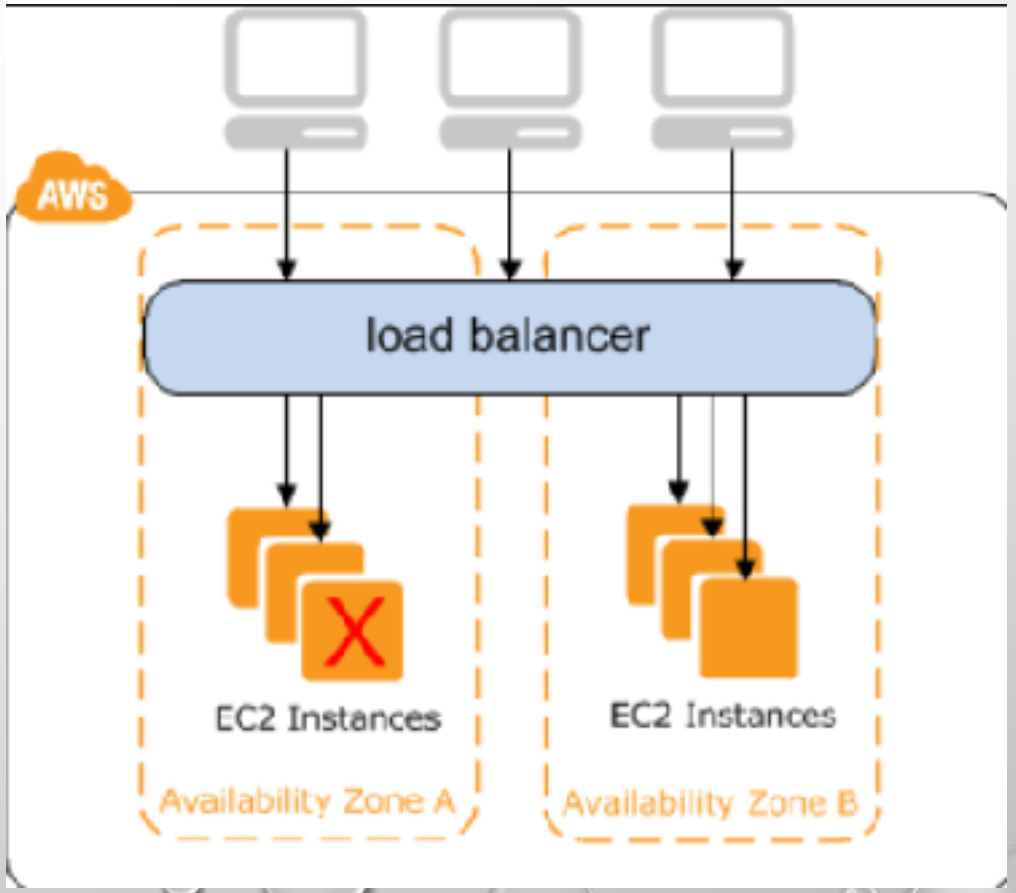
- SIMPLE
- WEIGHTED
- LATENCY
- FAILOVER
- GEOLOCATION



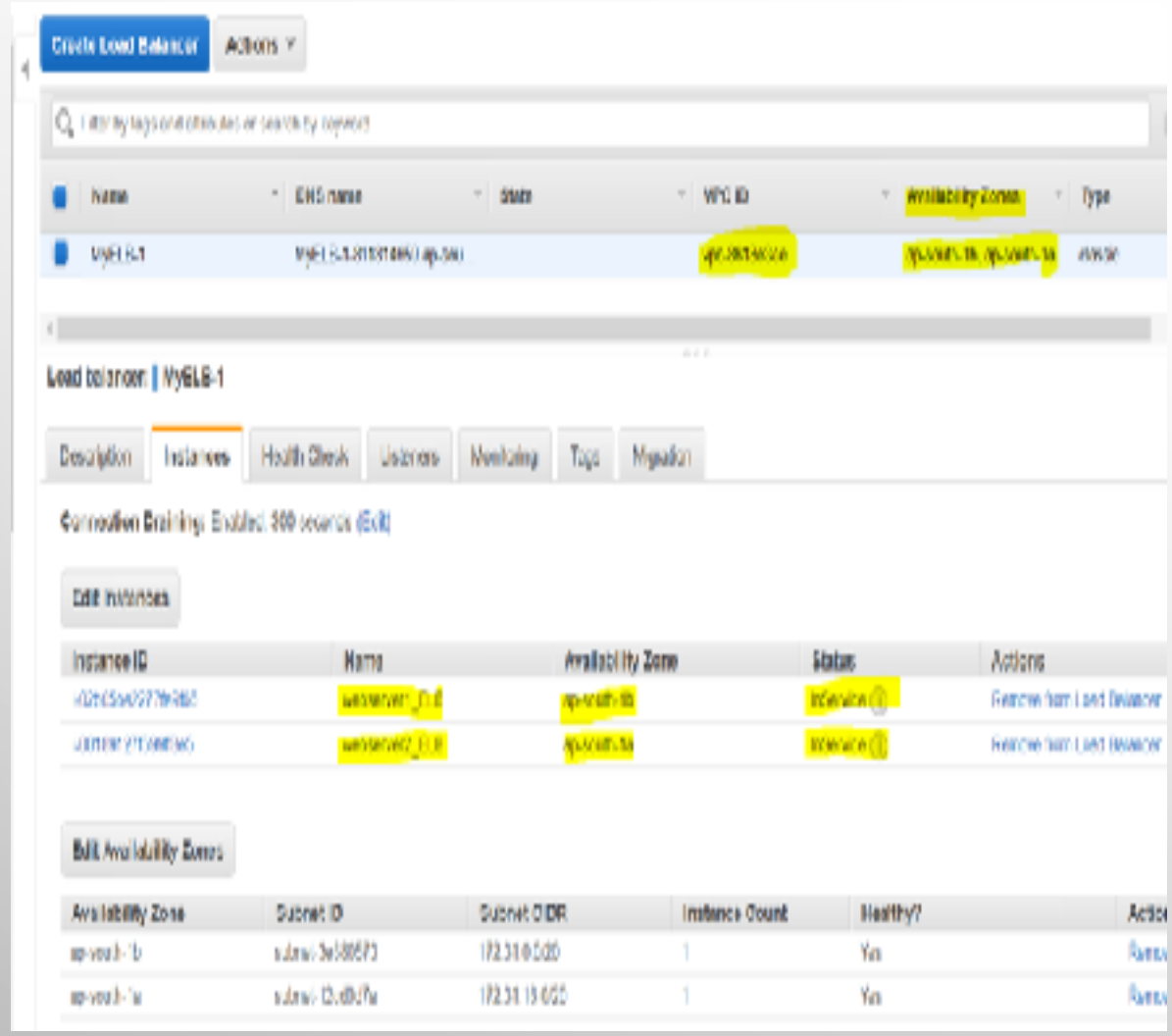
# LAB – SETUP ELB & EC2 INSTANCES

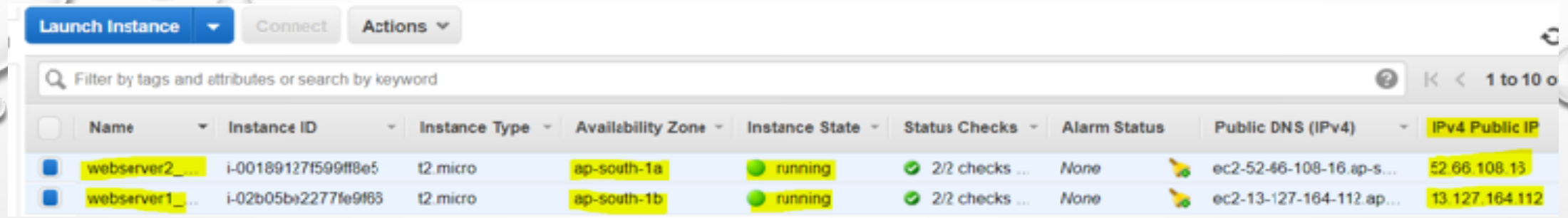
- CREATE A ELB-1 & ELB-2 ON TWO DIFFERENT AVAILABILITY ZONES AND CREATE 3 EC2 INSTANCES AND ADD 2 INSTANCES IN ONE ELB-1 AND ONE IN ELB-2.

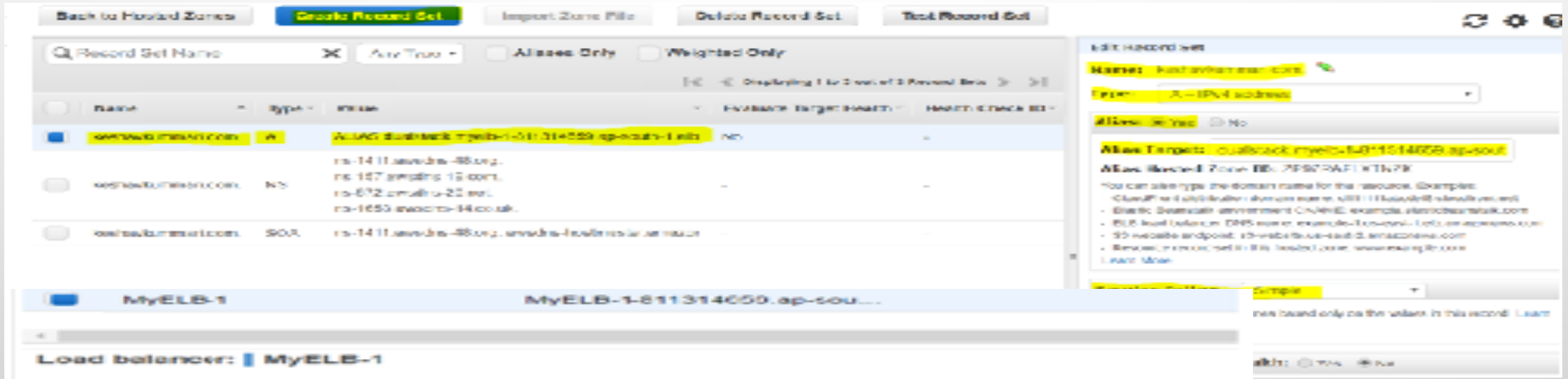


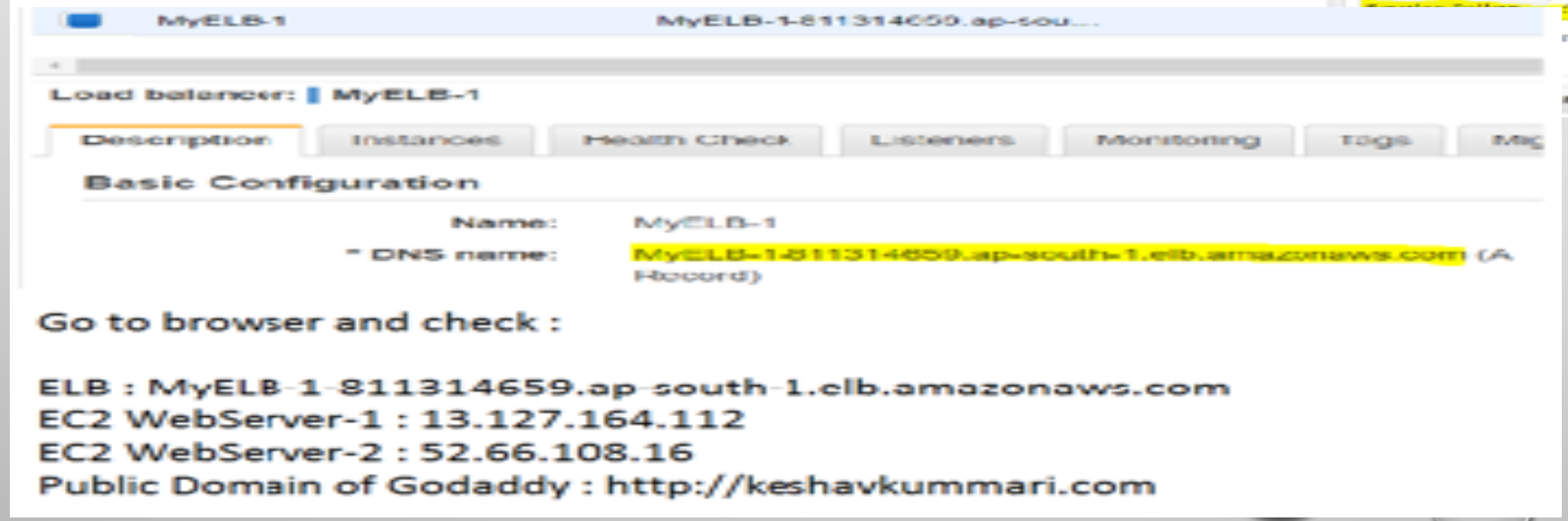



# LAB : CREATE TWO EC2 INSTANCE AND ONE ELB, USE THE EC2 INSTANCE SECURITY GROUP TO ELB AND ADD TWO EC2 INSTANCE TO ELB.





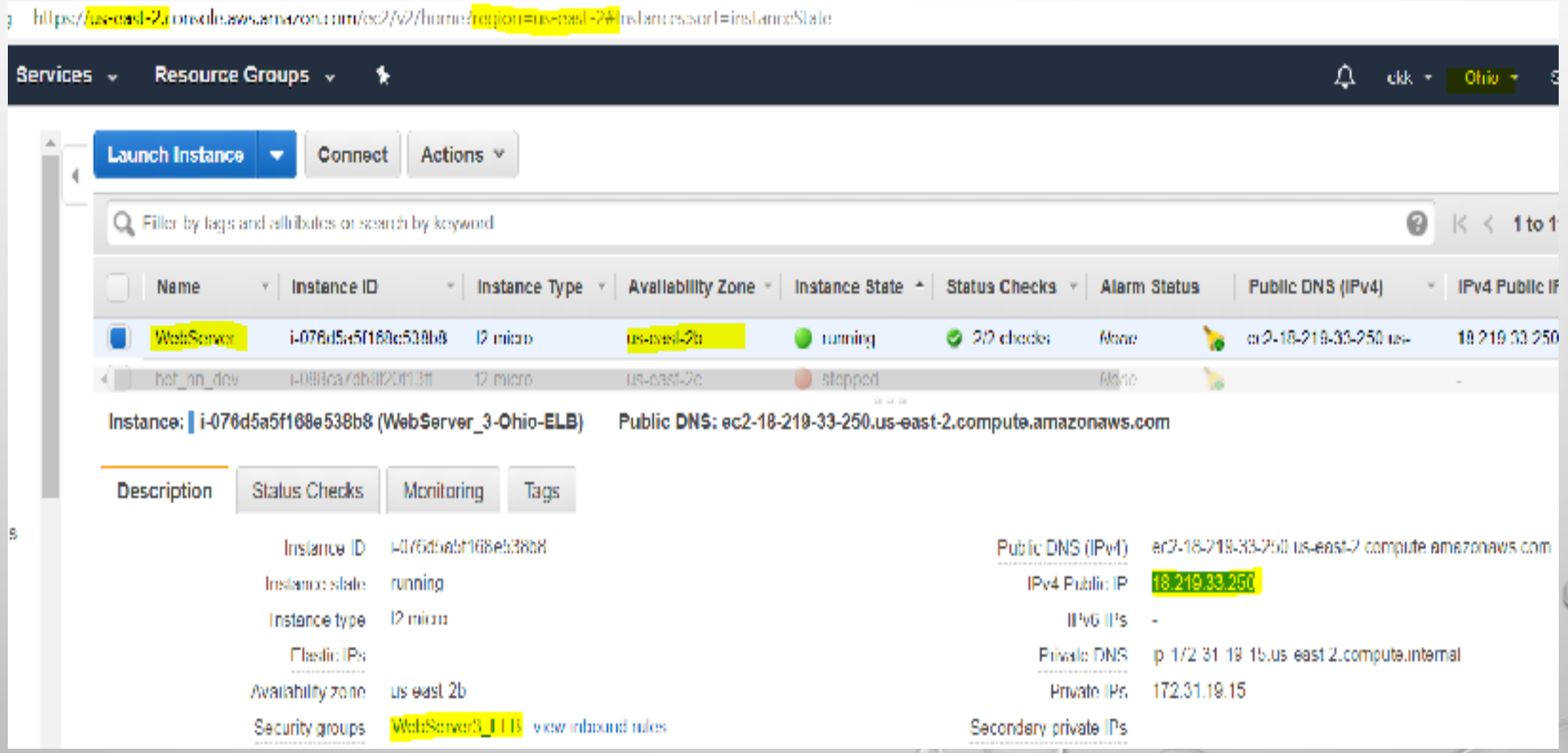



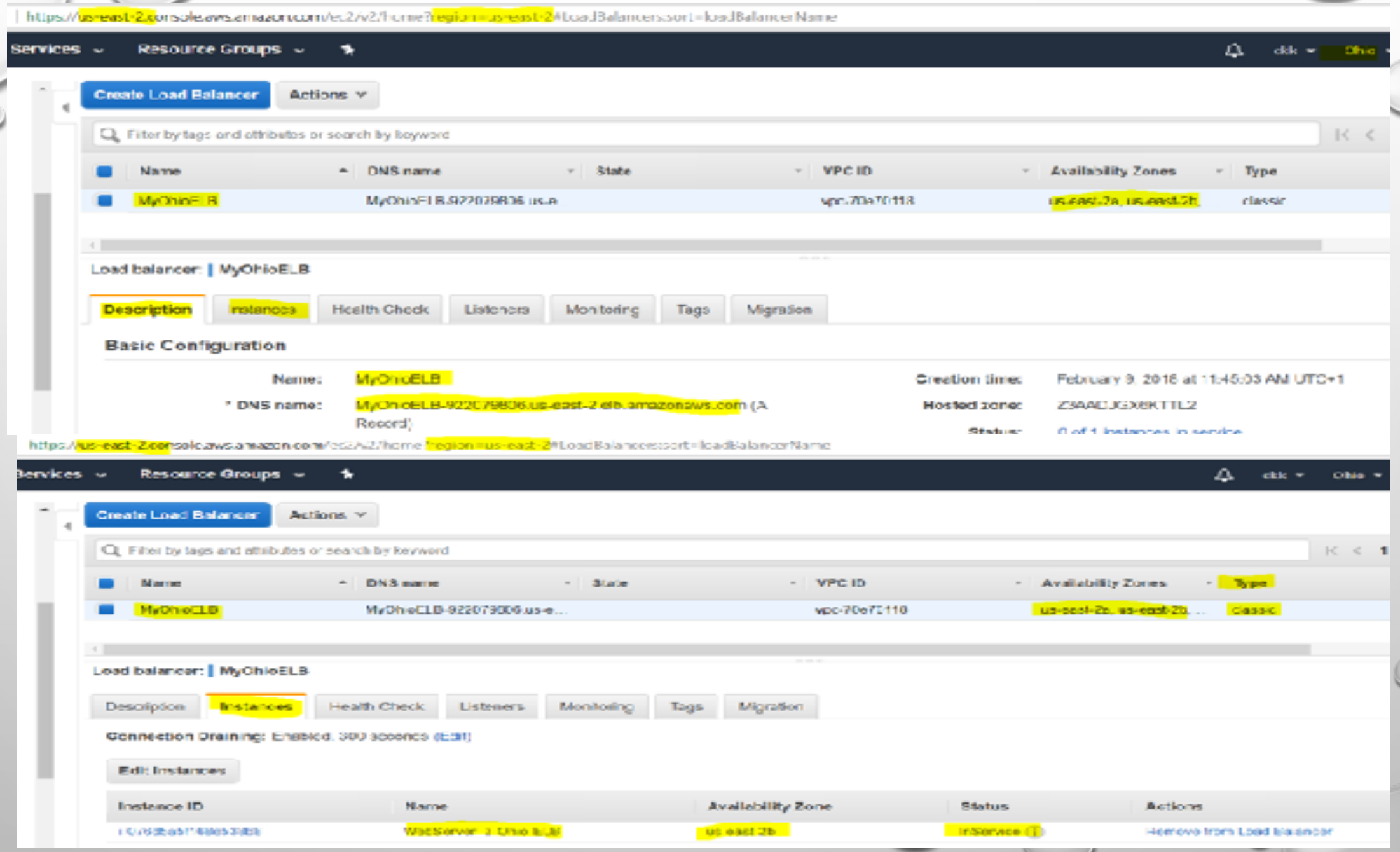



Go to browser and check :

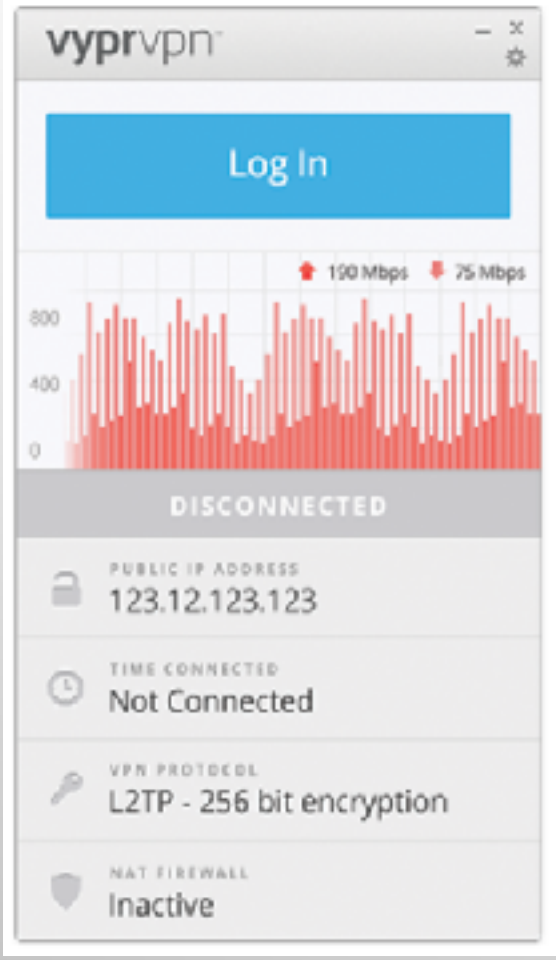
ELB : MyELB-1-811314659.ap-south-1.elb.amazonaws.com
EC2 WebServer-1 : 13.127.164.112
EC2 WebServer-2 : 52.66.108.16
Public Domain of Godaddy : http://keshavkummari.com

# CREATE A ONE MORE EC2 INSTANCE IN OTHER AZ AND CREATE A ONE MORE ELB AND ADD THIS EC2 INSTANCE TO IT.




Services
Resource Groups
Create Load Balancer
Actions
Filter by tags and attributes or search by keyword
Name
DNS name
State
VPC ID
Availability Zones
Type
MyOhioELB
classic
Load balancer: MyOhioELB
Description
Instances
Health Check
Listeners
Monitoring
Tags
Migration
Basic Configuration
Name: MyOhioELB
* DNS name: MyOhioELB-922073006.us-east-2.elb.amazonaws.com (A Record)
Creation time: February 9, 2016 at 11:45:03 AM UTC+1
Hosted zone: Z3AADJGX6KTTL2
Status: 0 of 1 instances in service
Connection Draining: Enabled, 300 seconds
Edit Instances
Instance ID
Name
Availability Zone
Status
Actions
WebServer-2
us-east-2b
InService
Remove from Load Balancer

# DOWNLOAD VPN AND TEST THE CONNECTION

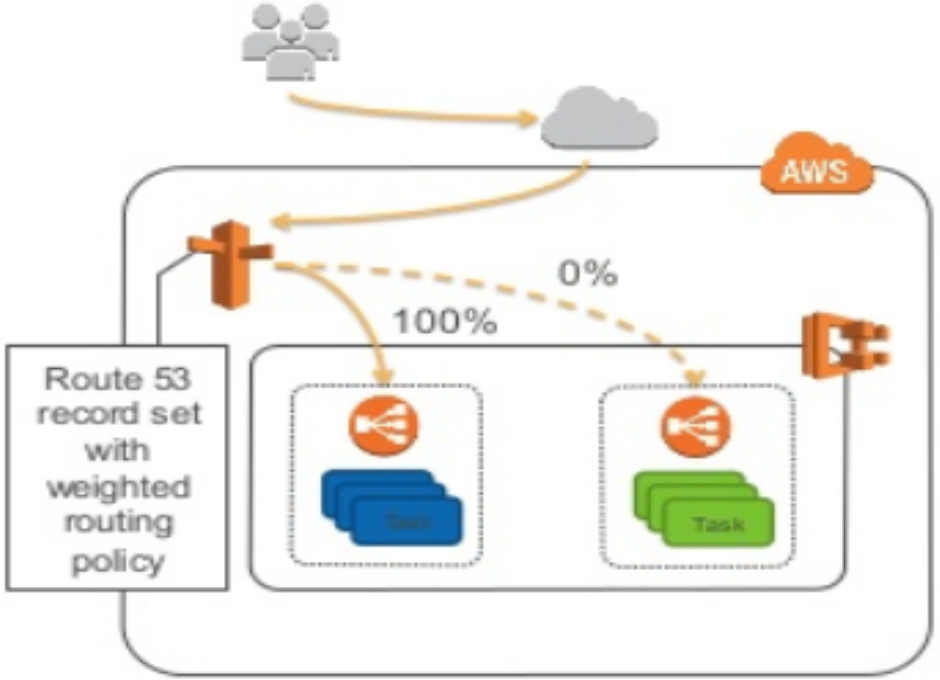


# 2. WEIGHTED

## Scheduling Containers: Long-Running App

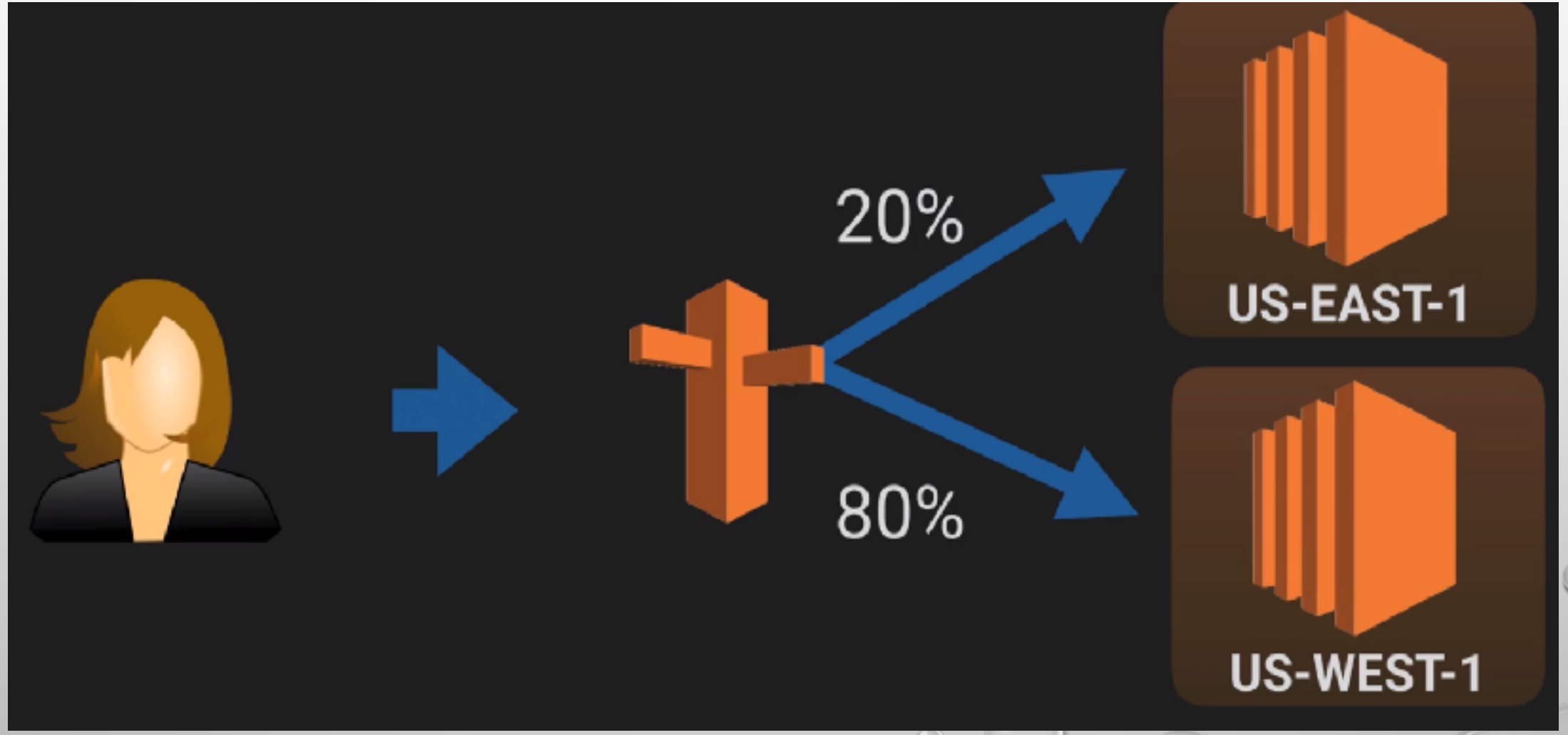
### Blue-Green Deployments

- Define two ECS services
- Each service is associated w/ ELB
- Both ELBs in Route 53 record set with weighted routing policy, 100% primary, 0% secondary
- Deploy to blue or green service and switch weights

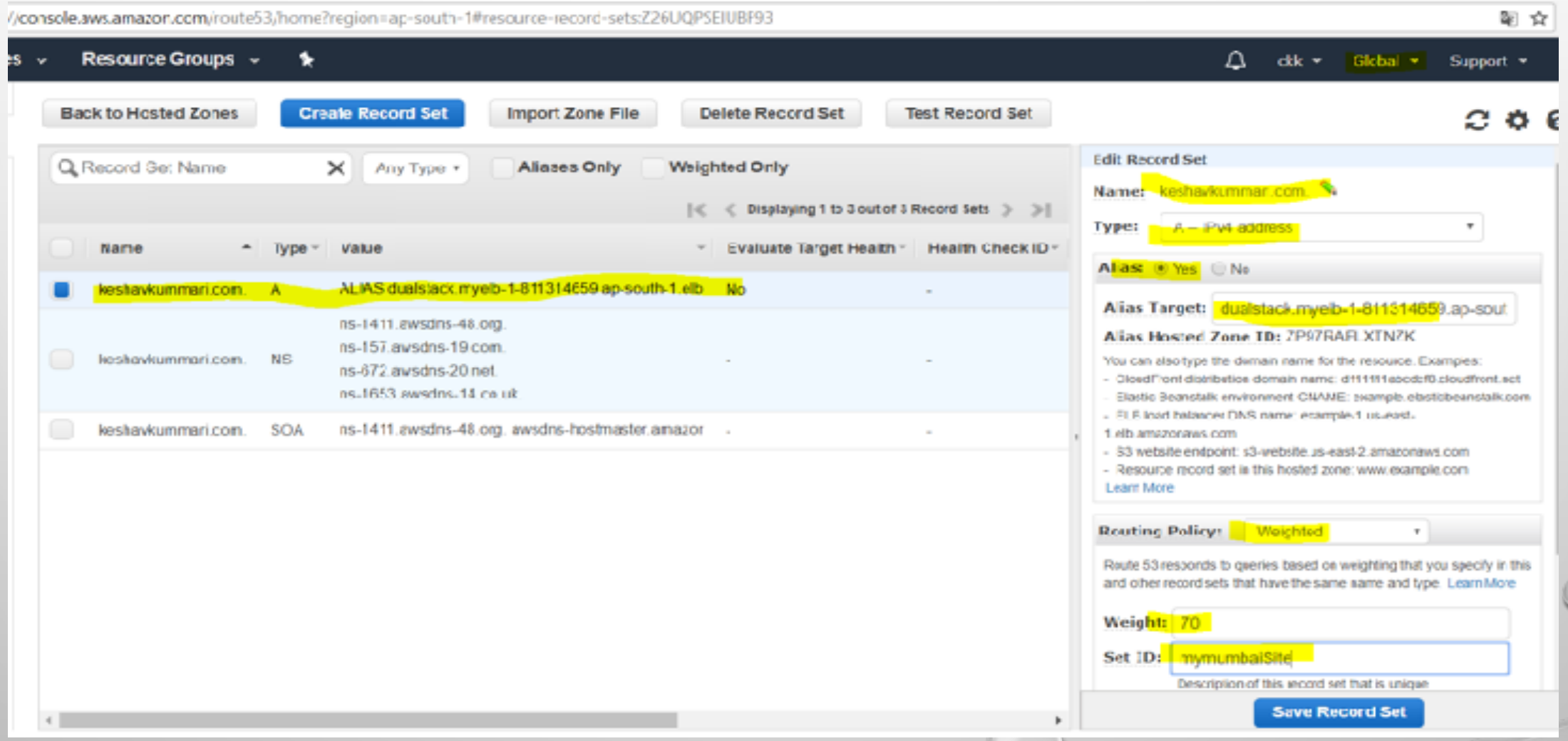



amazon web services

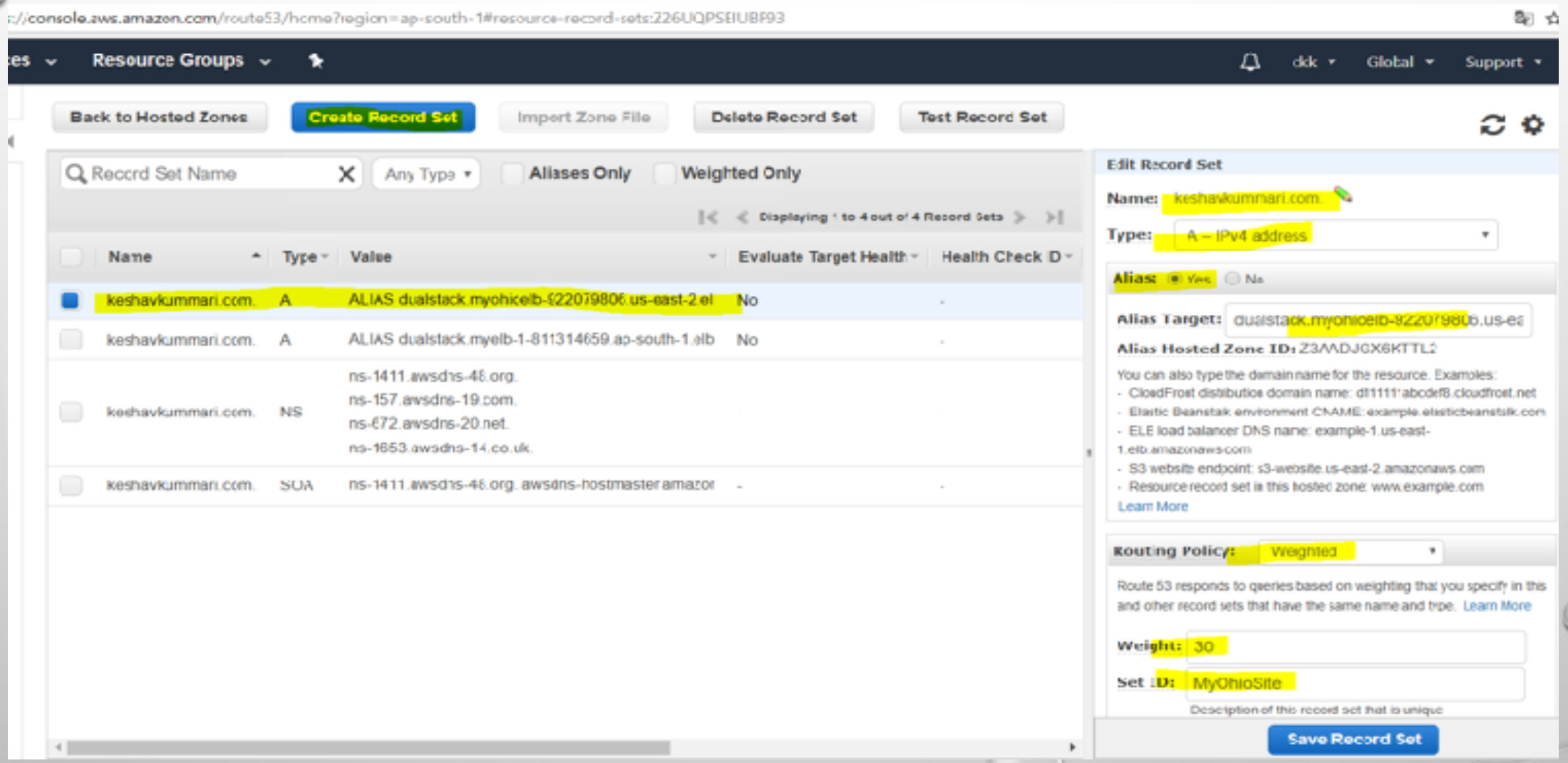
# WEIGHTED ROUTING POLICIES



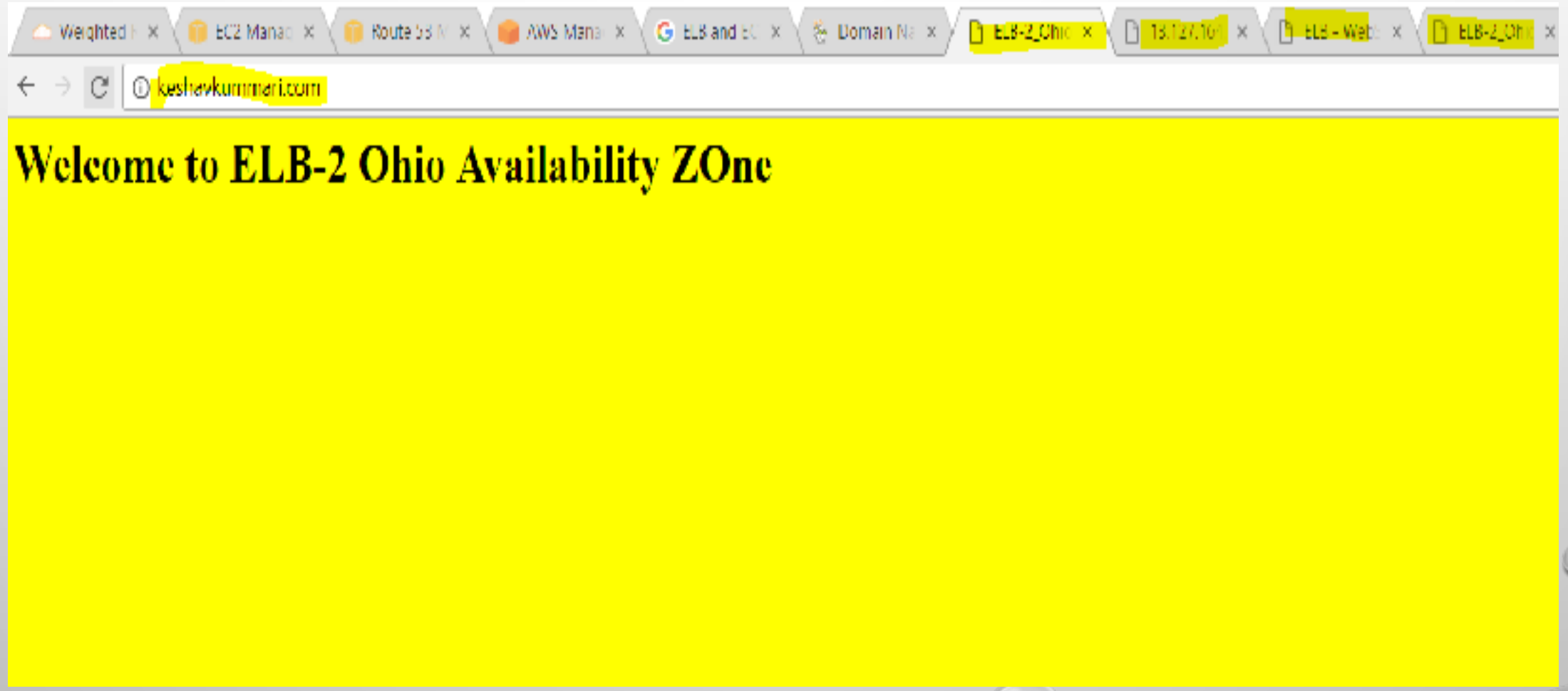
# WEIGHTED ROUTING POLICIES – CONFIGURED 70%



# CONFIGURING ROUTING POLICY ON ELB-2



# NOW TRAFIC IS ROUTING TO TWO DIFFERENT ELB'S & AZ AS WELL

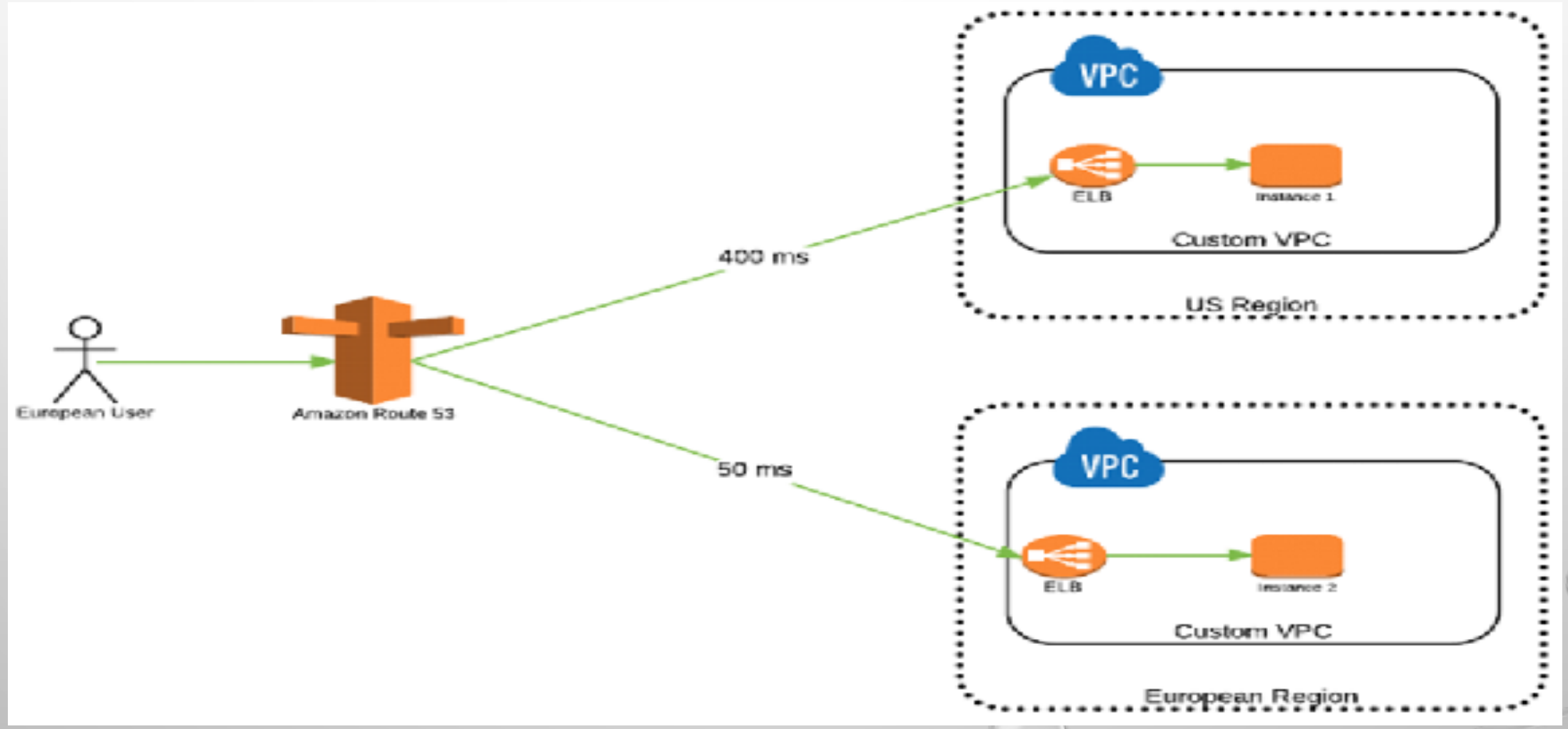


# 3. LATENCY

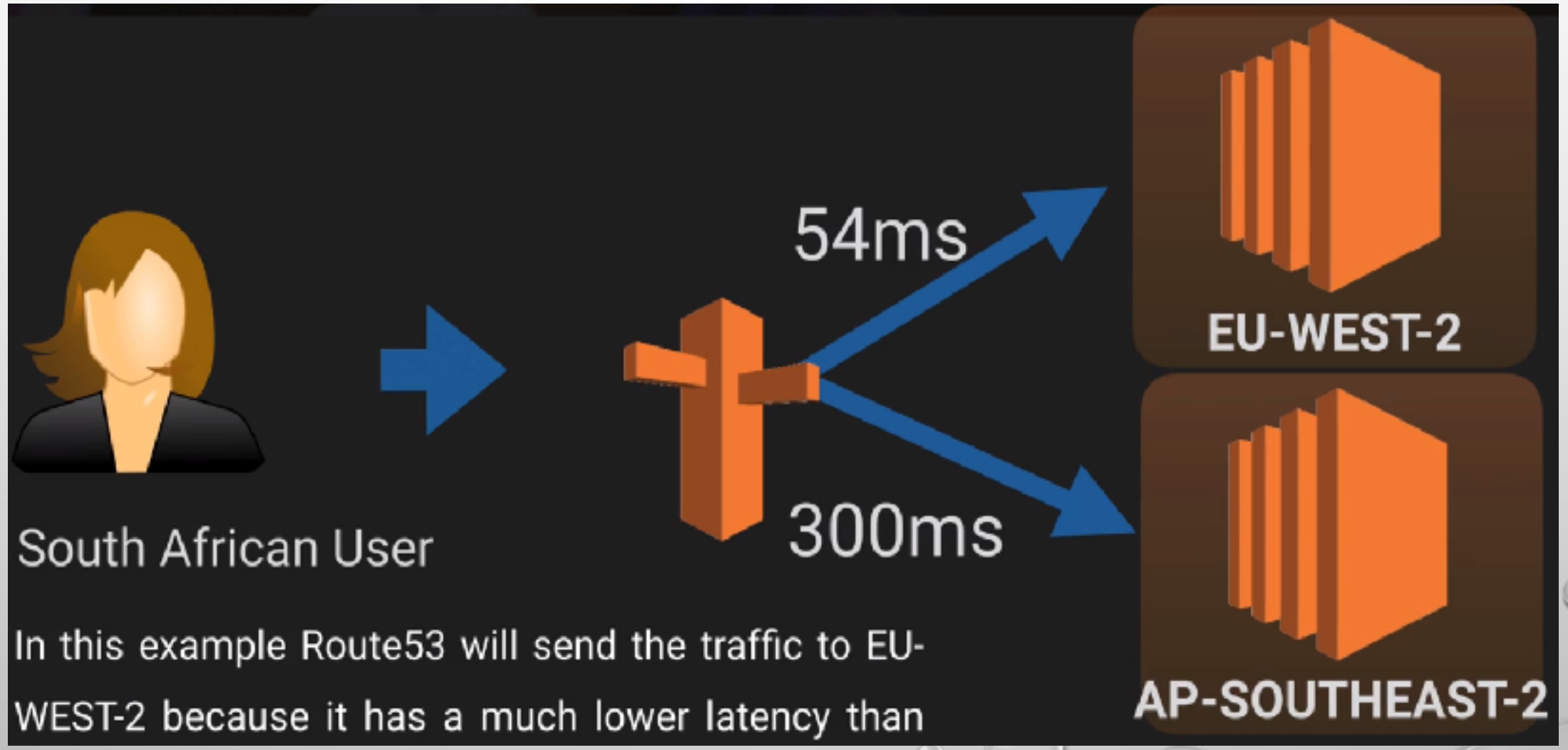
Latency based routing allows you to route your traffic based on the lowest network latency for your end user (ie which region will give them the fastest response time).

To use latency-based routing you create a latency resource record set for the Amazon EC2 (or ELB) resource in each region that hosts your website. When Amazon Route 53 receives a query for your site, it selects the latency resource record set for the region that gives the user the lowest latency. Route 53 then responds with the value associated with that resource record set.

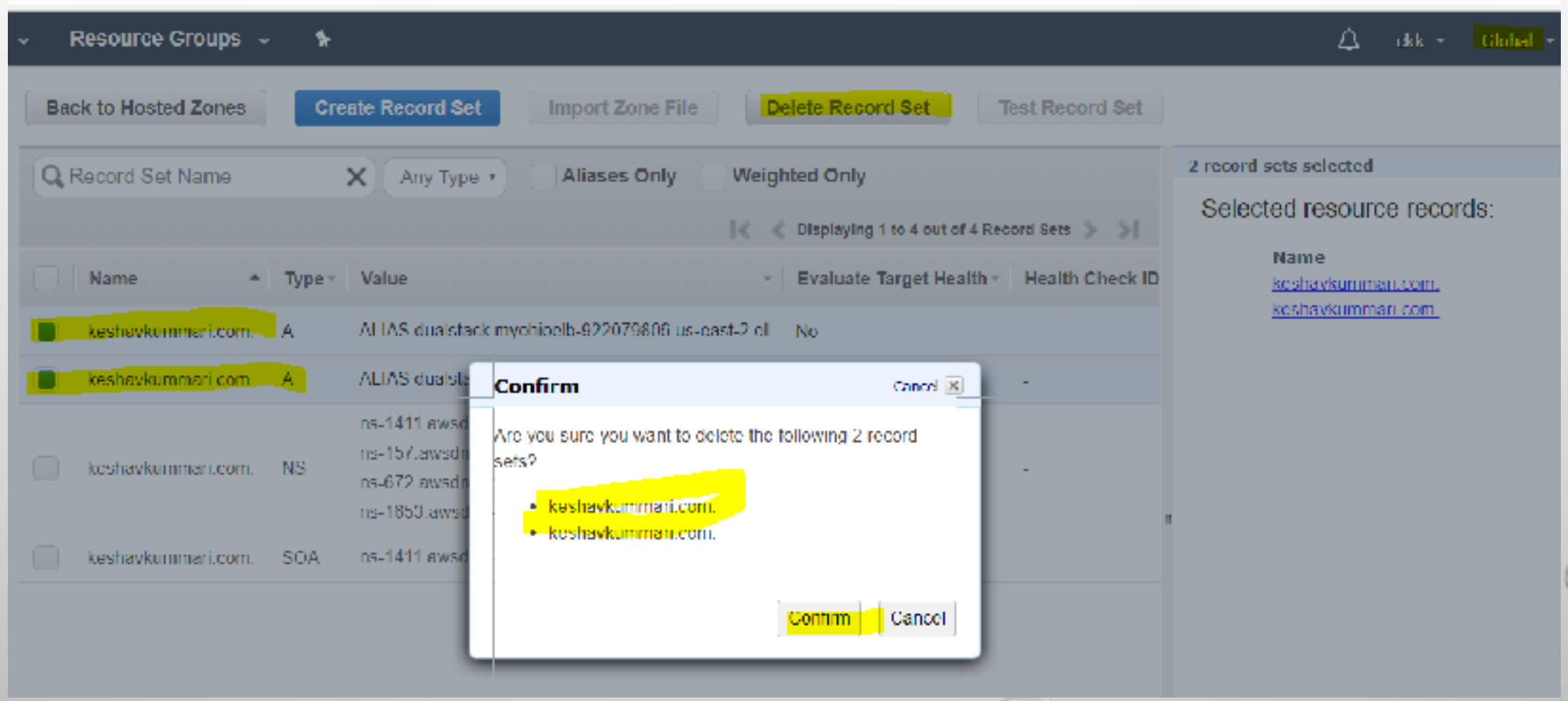
# LATENCY


European User
Amazon Route 53
400 ms
50 ms
VPC
ELB
Instance 1
Custom VPC
US Region
VPC
ELB
Instance 2
Custom VPC
European Region

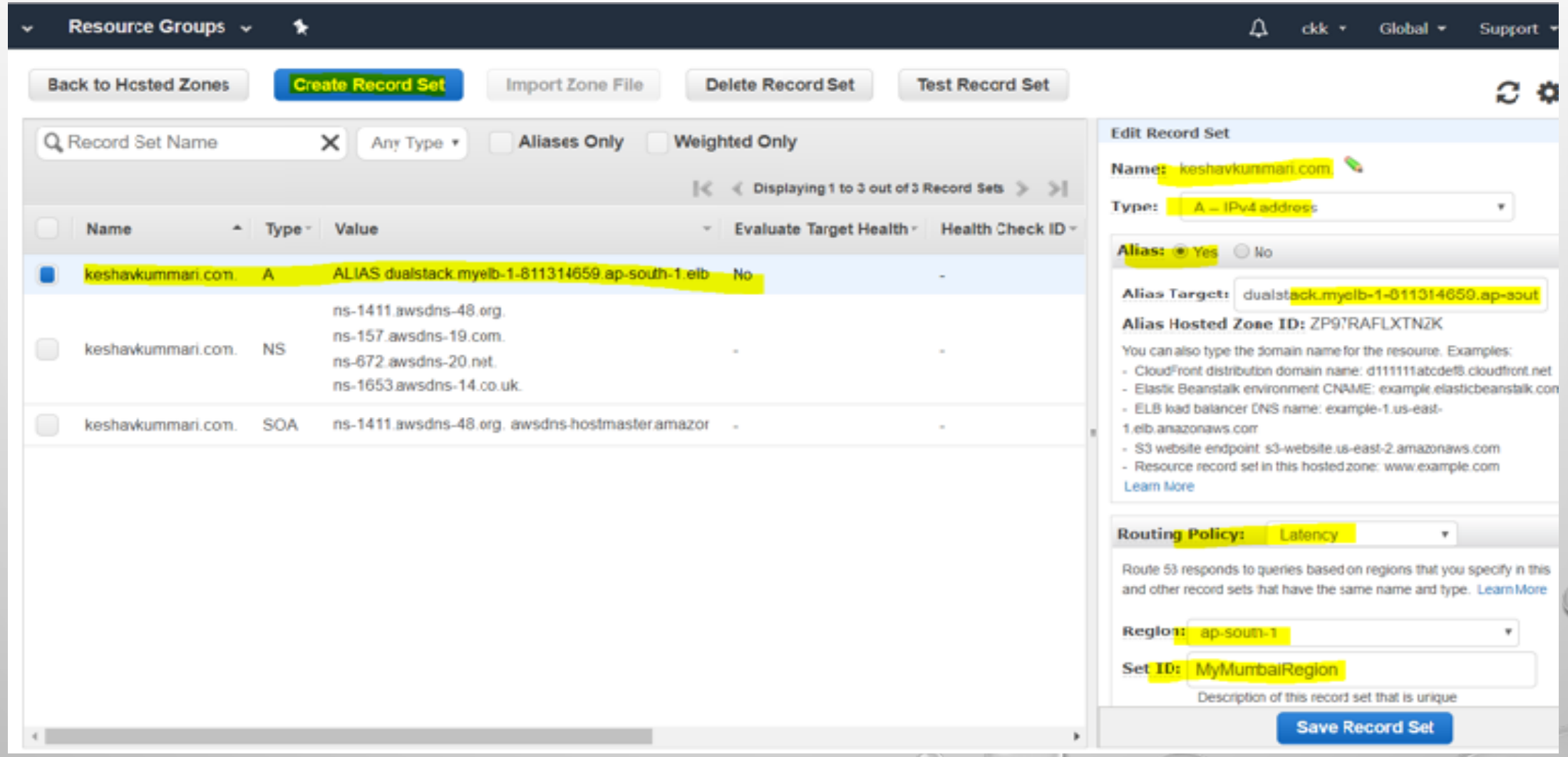
# EXAMPLE - LATENCY



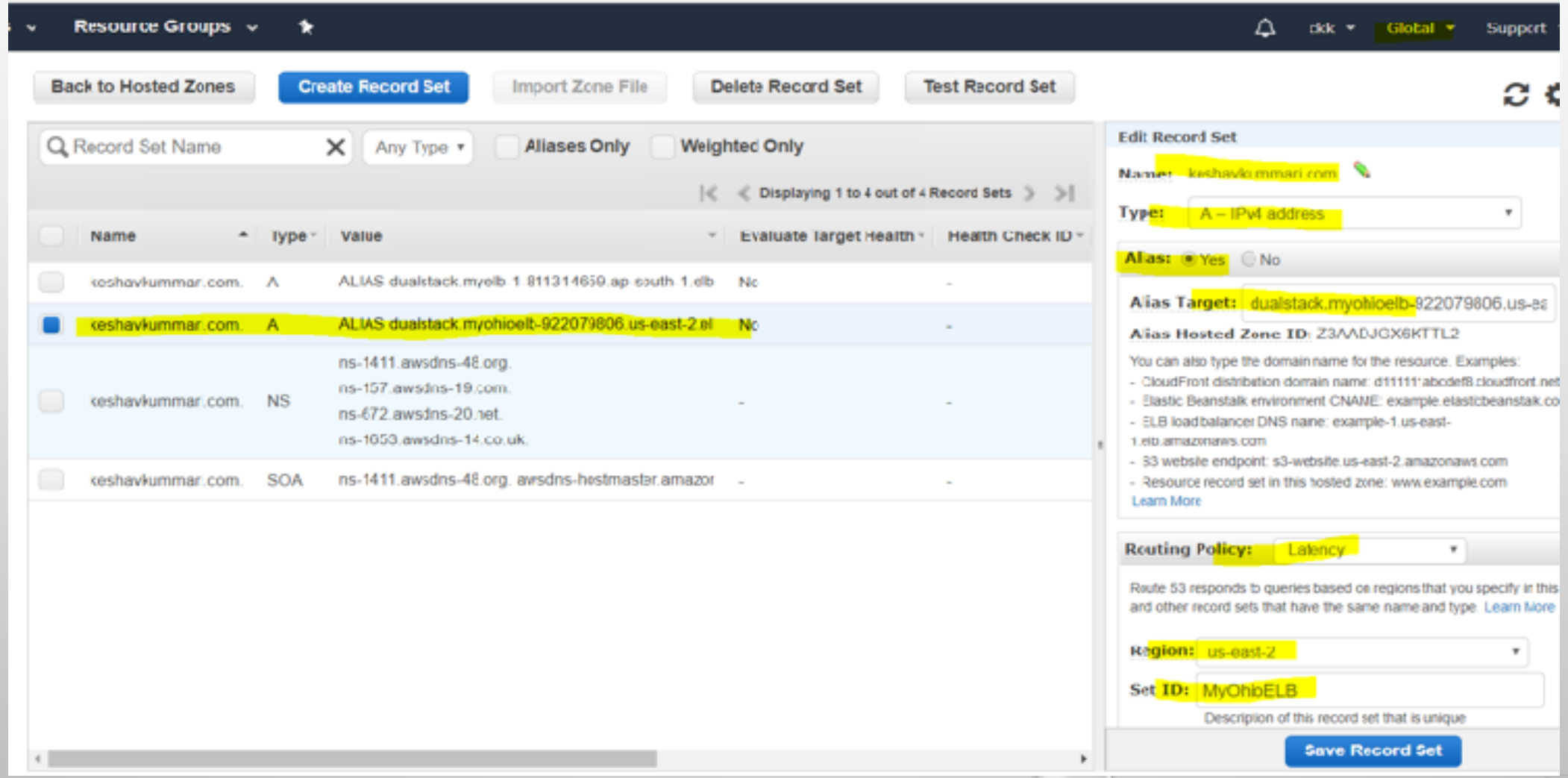
# BEFORE CONTINUING THE LATENCY TRY TO DELETE EXISTING A RECORDS



# CREATE A RECORD SET IN ROUTE53 FOR ELB-1



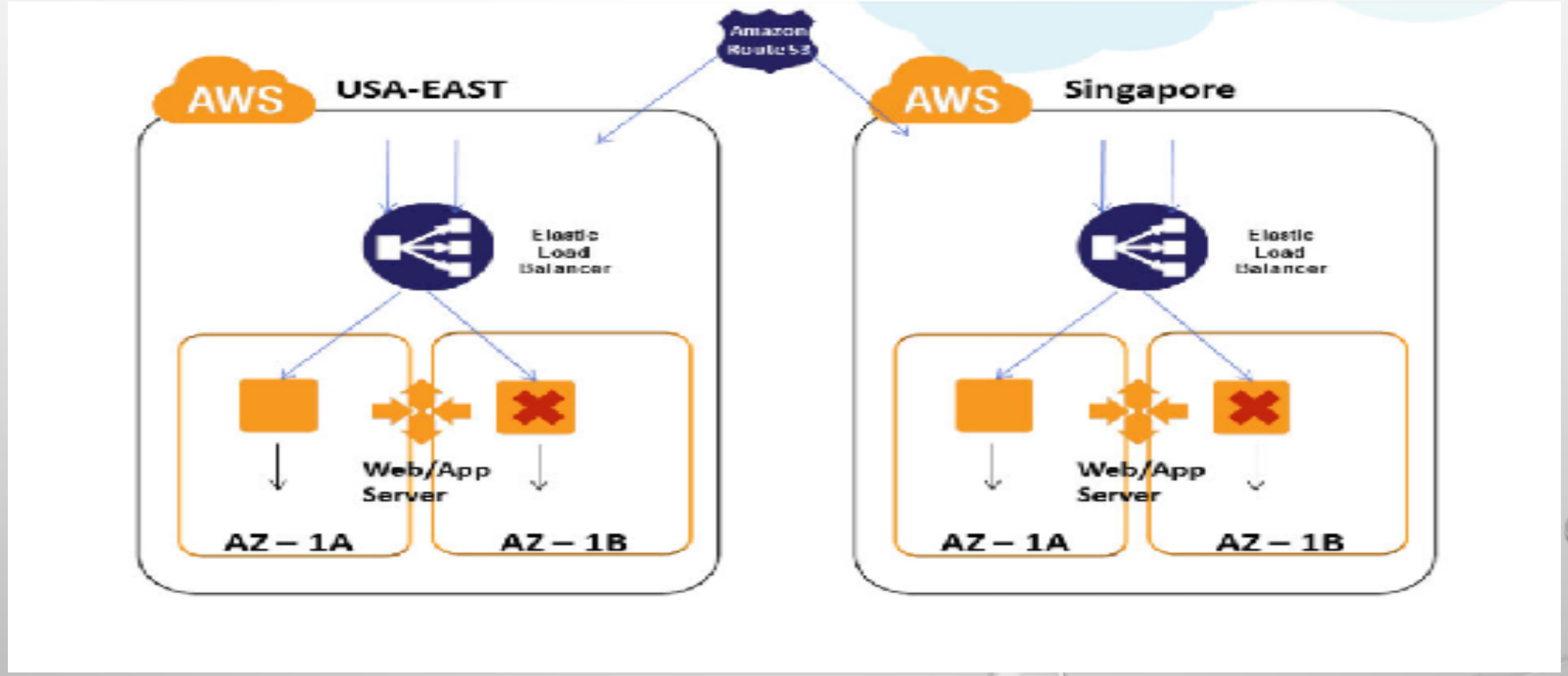
# CREATE A RECORD SET IN ROUTE53 FOR ELB-2



# DOWNLOAD VPN AND TEST THE CONNECTION

- CHECK THE CONNECTION LATENCY

# 4. FAILOVER


Amazon Route 53
AWS
USA-EAST
Elastic Load Balancer
Web/App Server
AZ – 1A
AZ – 1B
AWS
Singapore
Elastic Load Balancer
Web/App Server
AZ – 1A
AZ – 1B

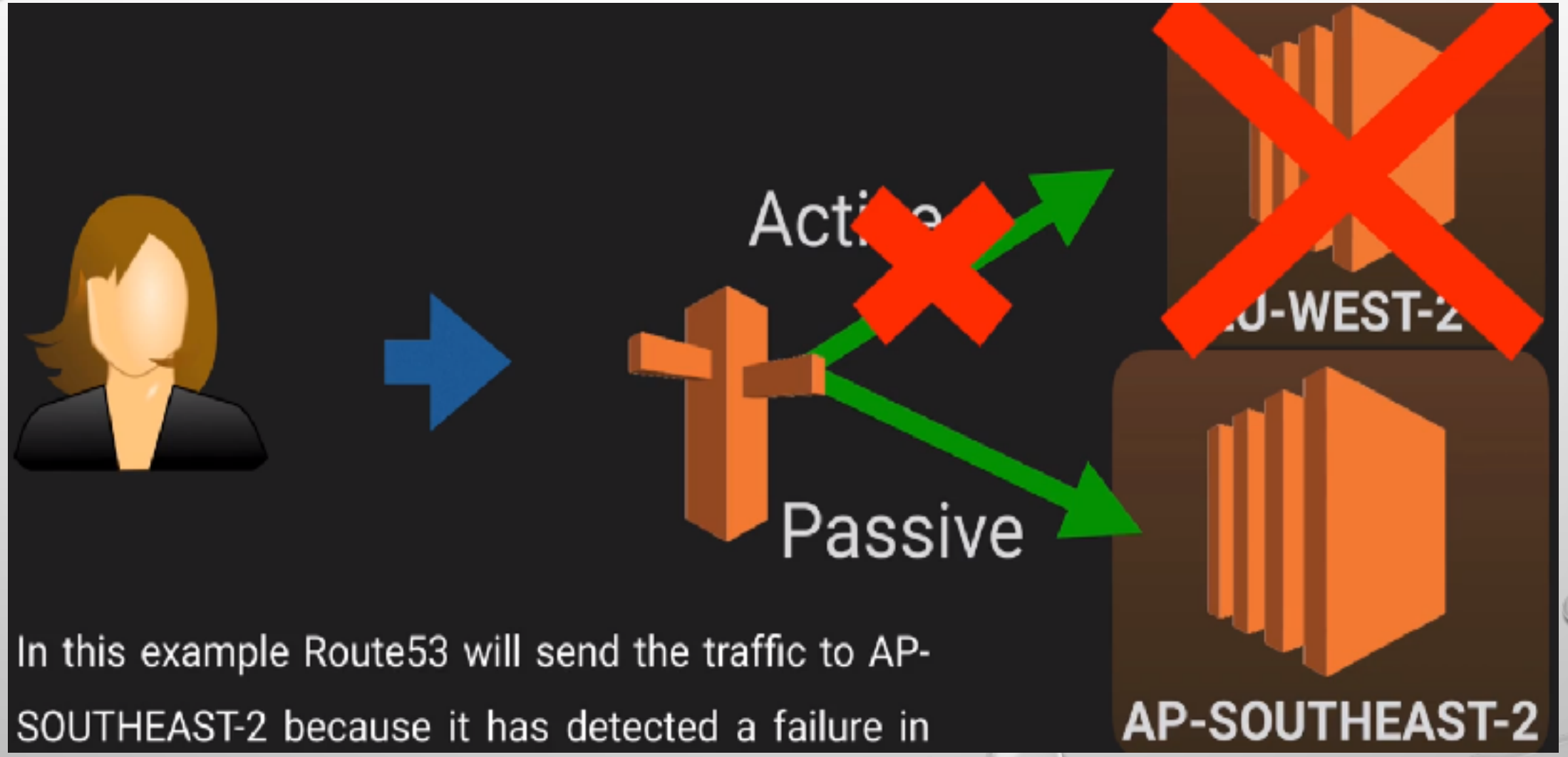
# FAILOVER ROUTING POLICIES

Failover routing policies are used when you want to create an active/passive set up. For example you may want your primary site to be in EU-WEST-2 and your secondary DR Site in AP-SOUTHEAST-2.

Route53 will monitor the health of your primary site using a health check.

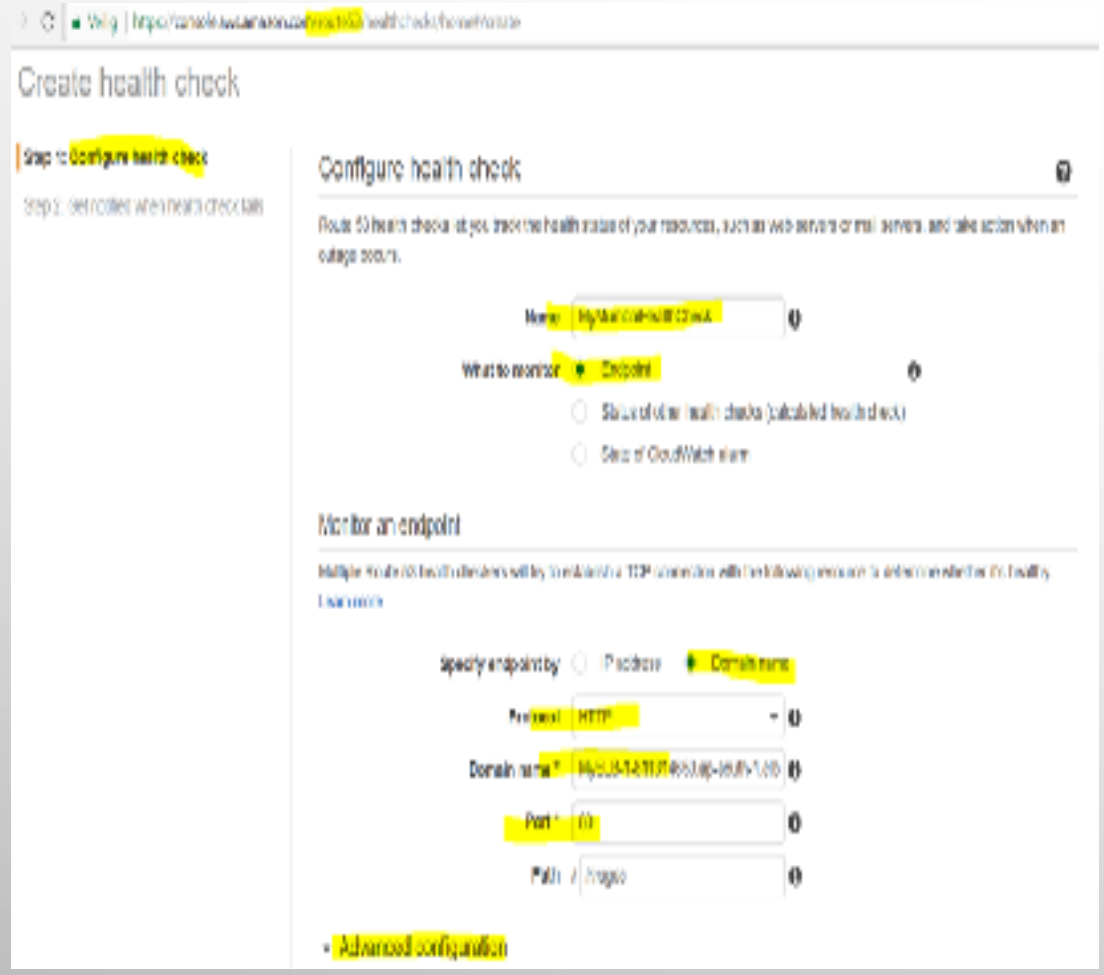
A health check monitors the health of your end points.

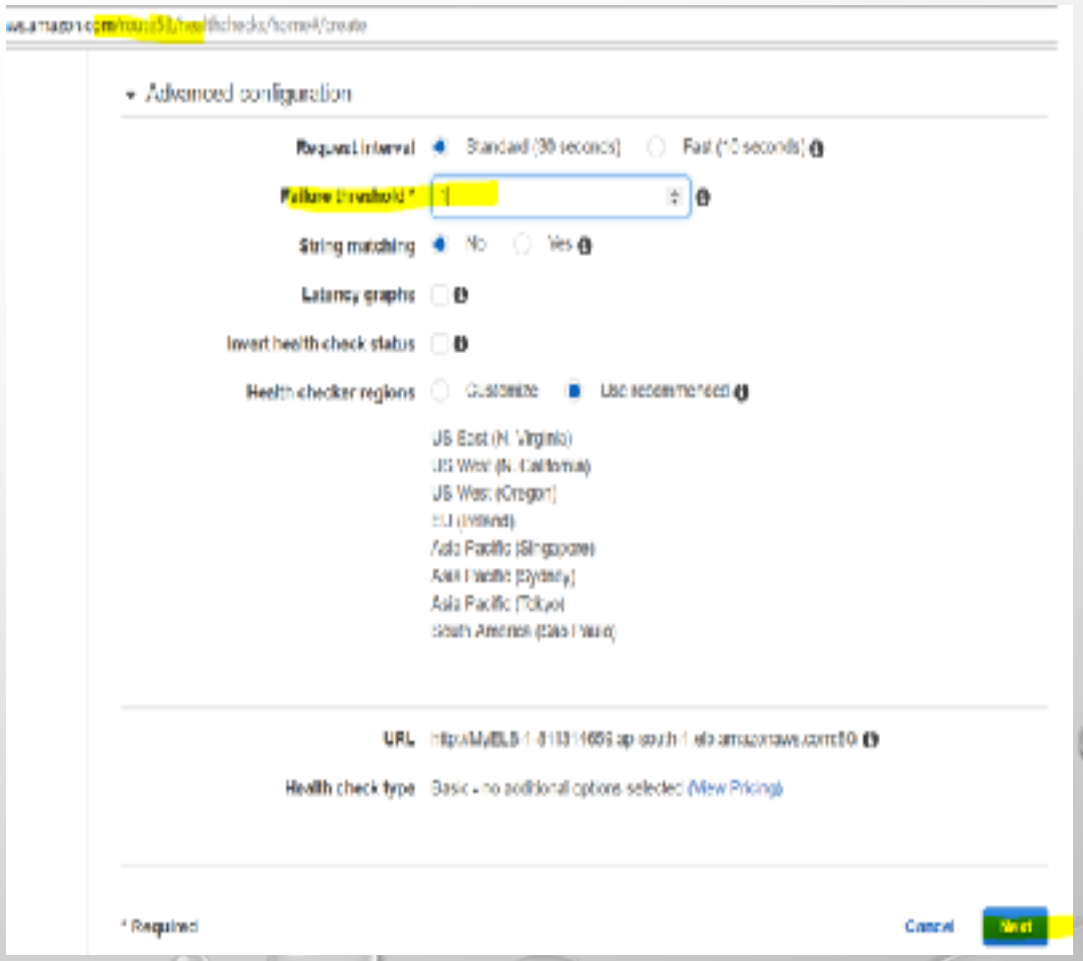
# EXAMPLE

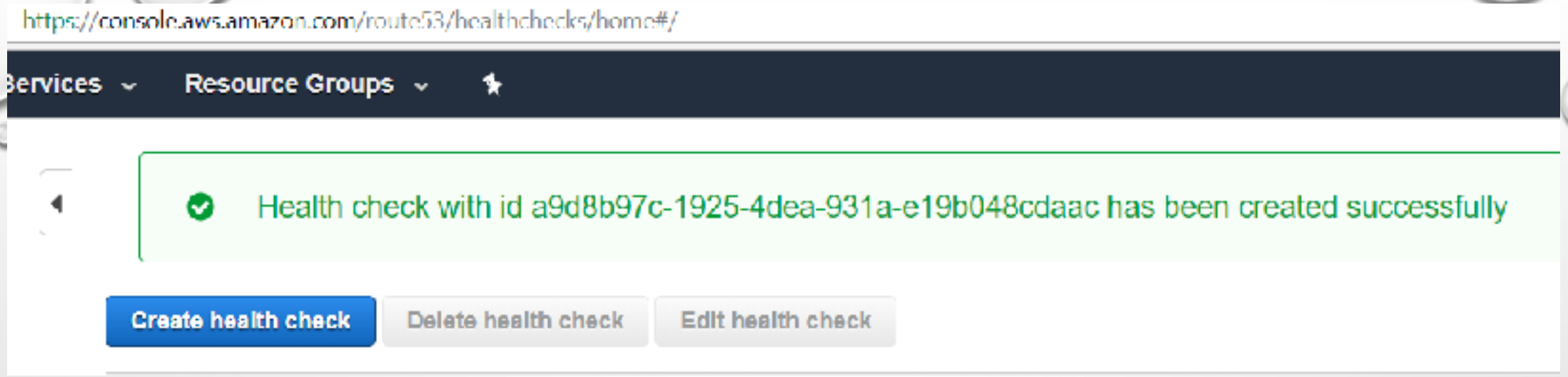

Passive
AP-SOUTHEAST-2
In this example Route53 will send the traffic to AP-
SOUTHEAST-2 because it has detected a failure in

# BEFORE WE SETUP FAILOVER, FIRST WE SHOULD SET UP HEALTH CHECK

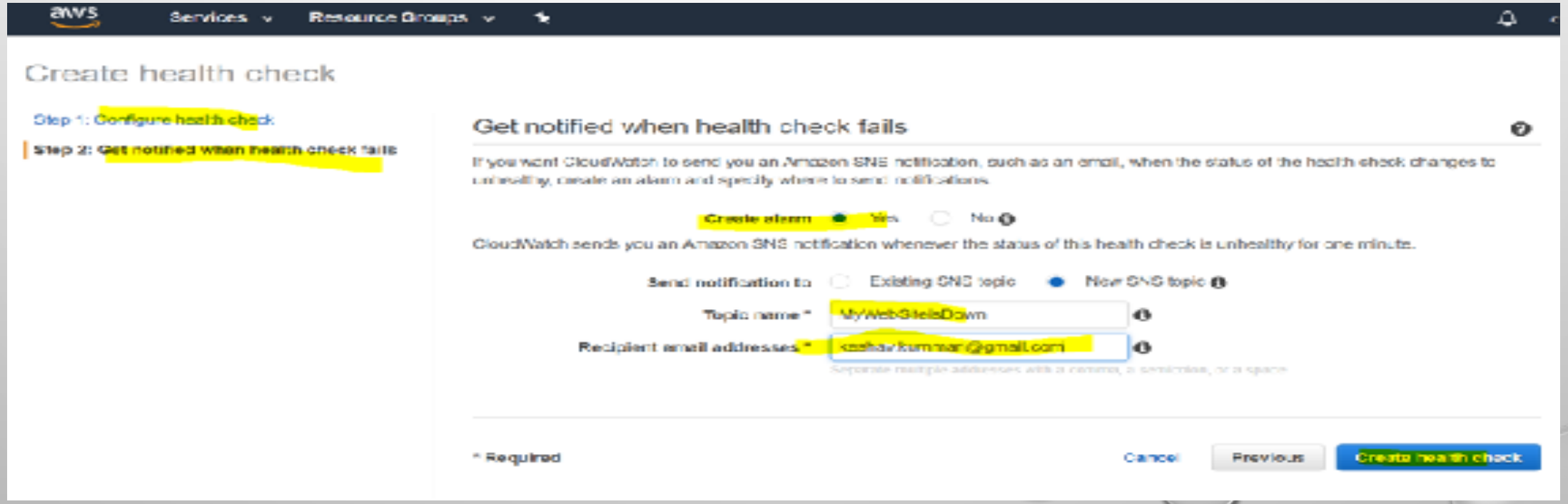
- GO TO ELB-1 AND COPY THE DNS(I.E. **MYELB-1-811314659.AP-SOUTH-1.ELB.AMAZONAWS.COM**)



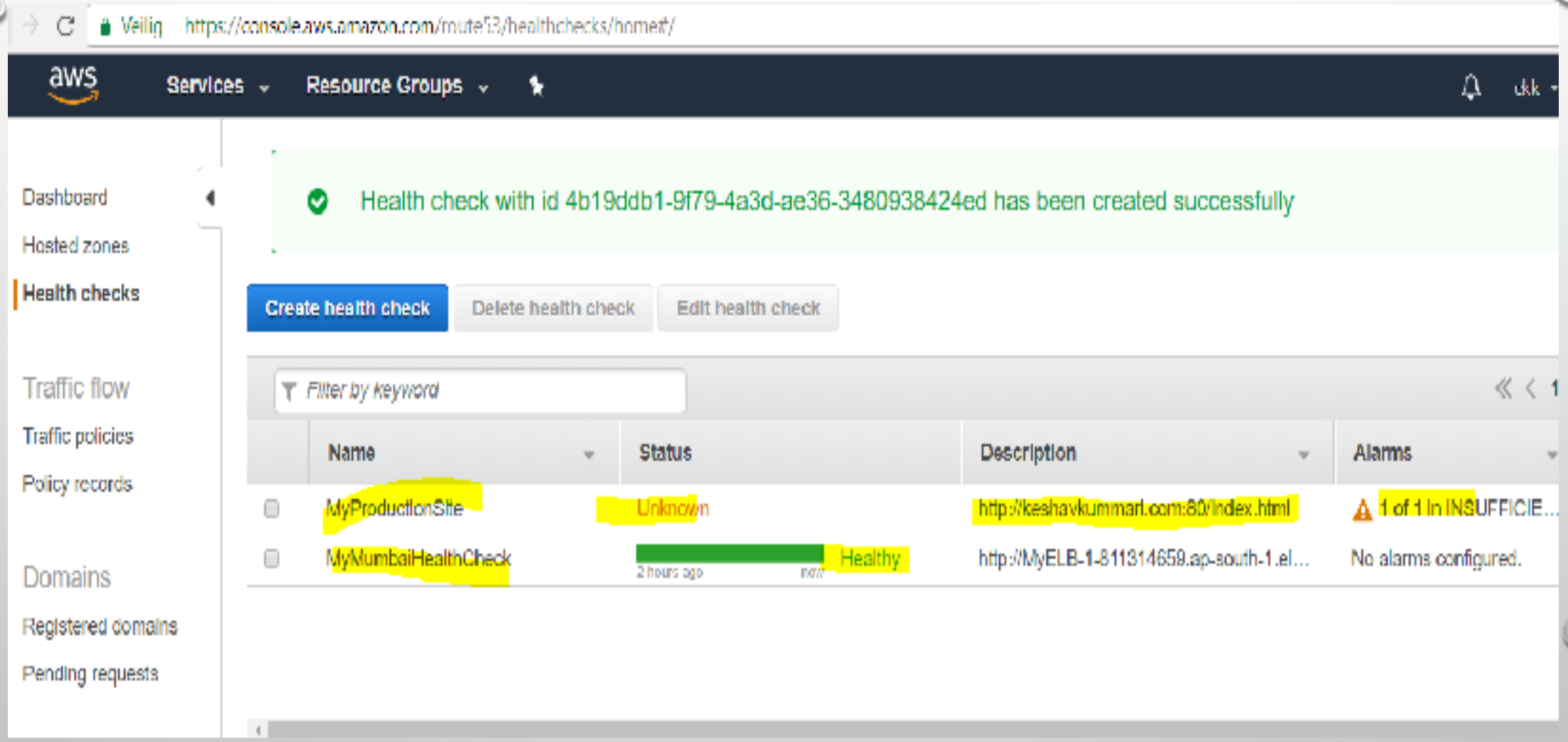





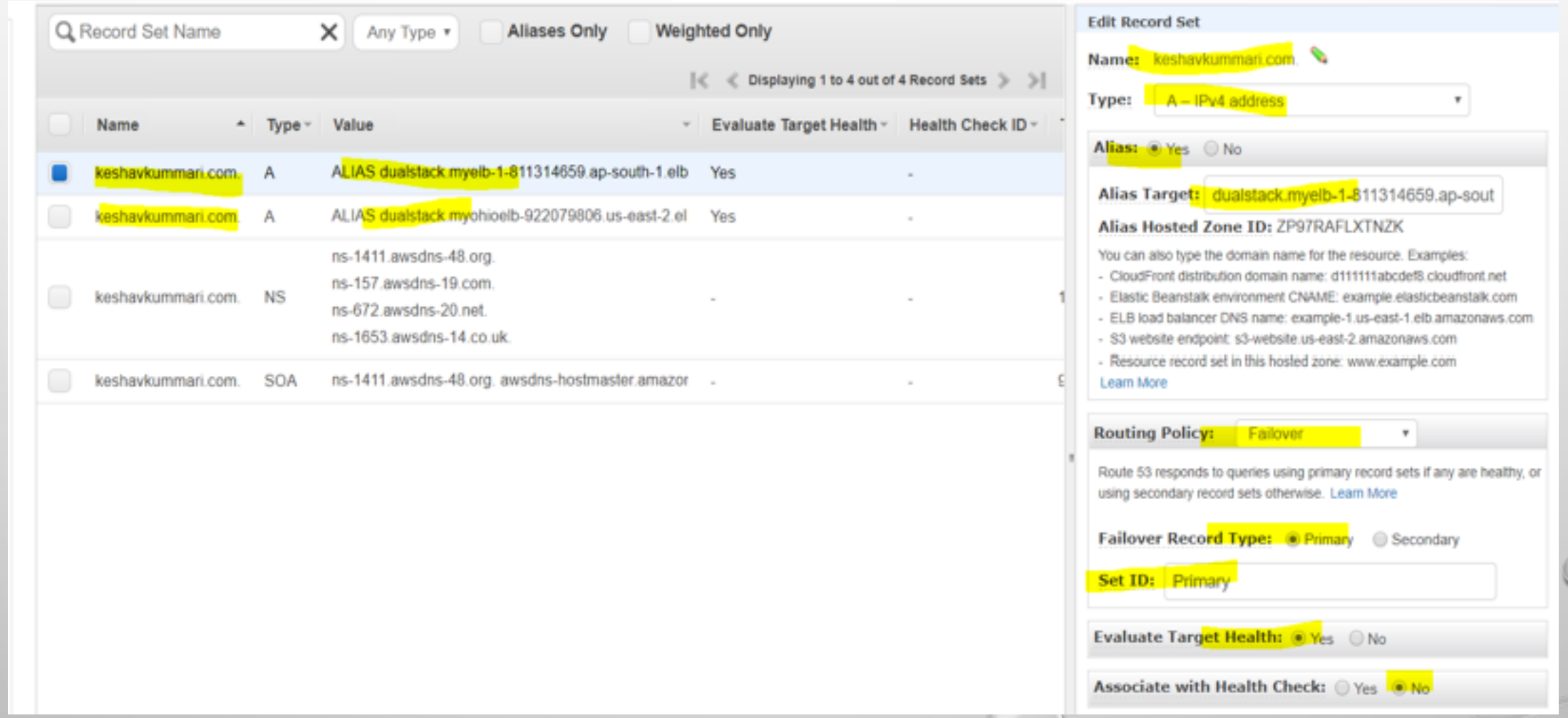

## CREATE A HEALTH CHECK ON ENTIRE WEBSITE



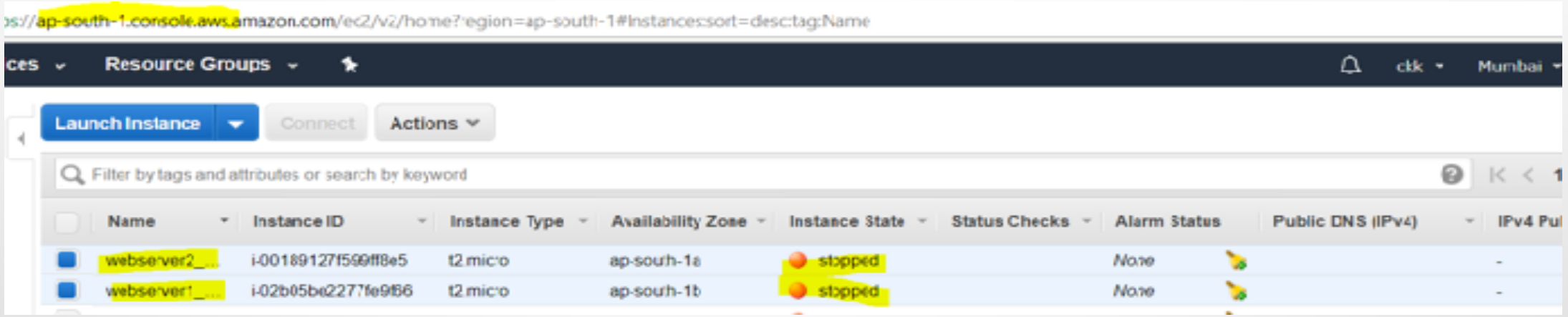
# ALERT


Veilig https://console.aws.amazon.com/route53/healthchecks/home#/
aws
Services
Resource Groups
ckk
Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Health check with id 4b19ddb1-9f79-4a3d-ae36-3480938424ed has been created successfully
Create health check
Delete health check
Edit health check
Filter by keyword
Name
Status
Description
Alarms
MyProductionSite
Unknown
http://keshavkummari.com:80/index.html
1 of 1 In INSUFFICIE...
MyMumbaiHealthCheck
2 hours ago
now
Healthy
http://MyELB-1-811314659.ap-south-1.el...
No alarms configured.

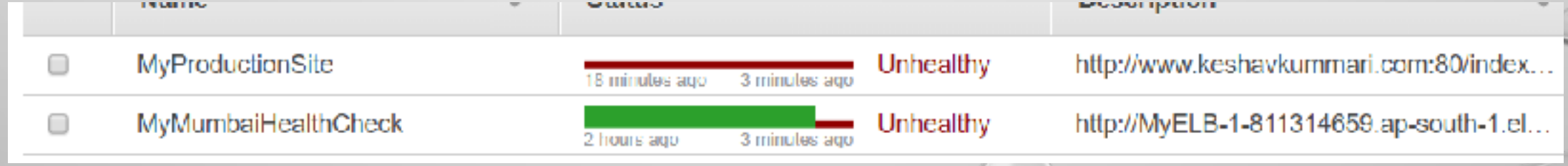
# GO TO ROUTE53 AND CONFIGURE ELB-1



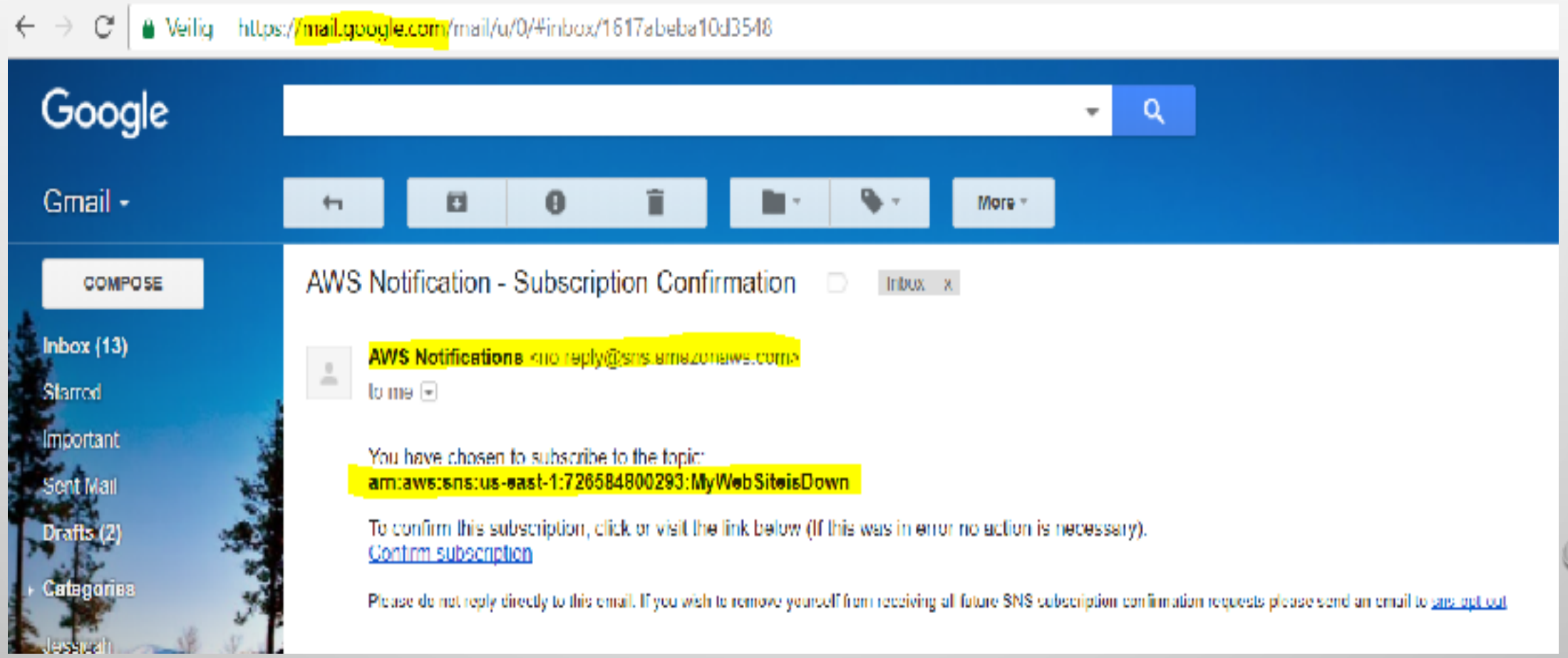
# STOP 2 EC2 INSTANCE FROM ELB-1 AND CROSS CHECK THE ALERT AND WEBSITE



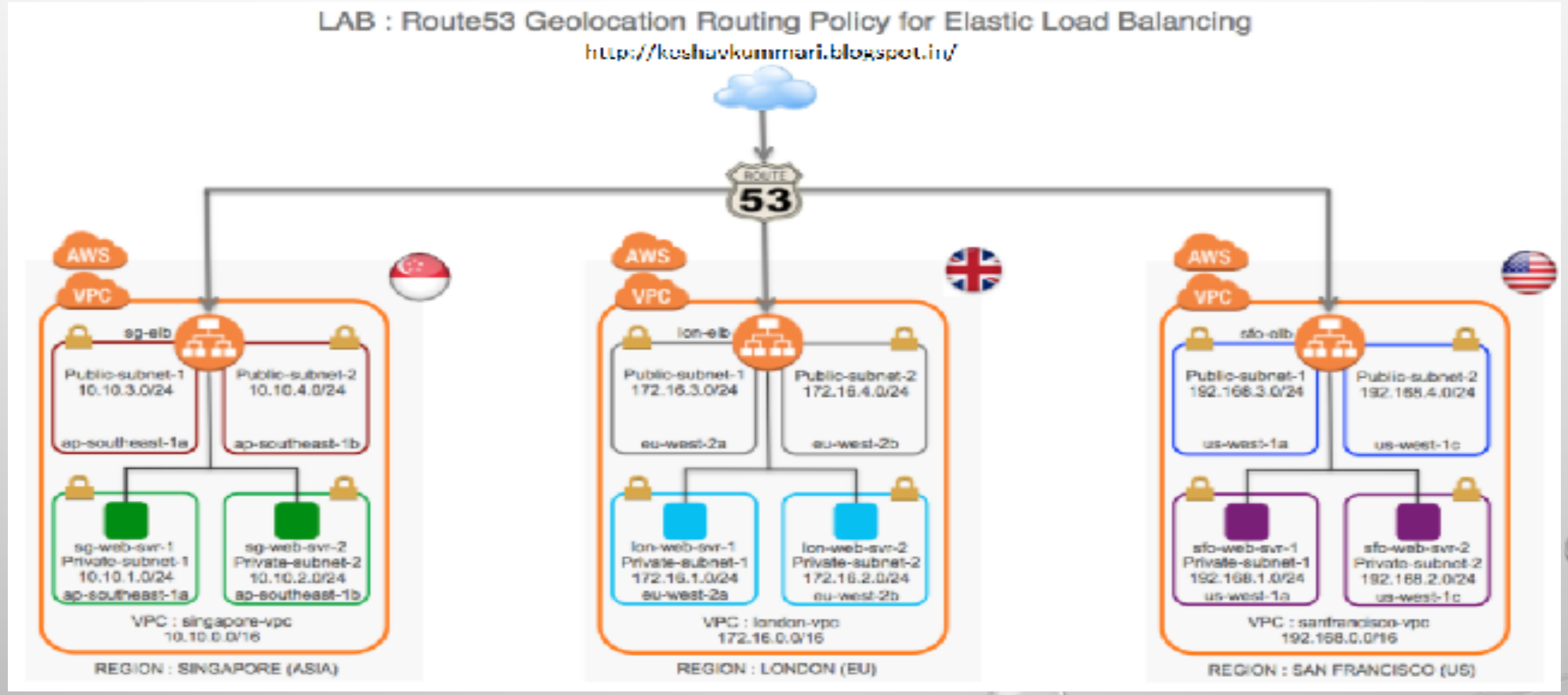




# GO TO YOUR MAIL BOX AND CROSS CHECK THE MAIL ALERT



# 5. GEOLOCATION

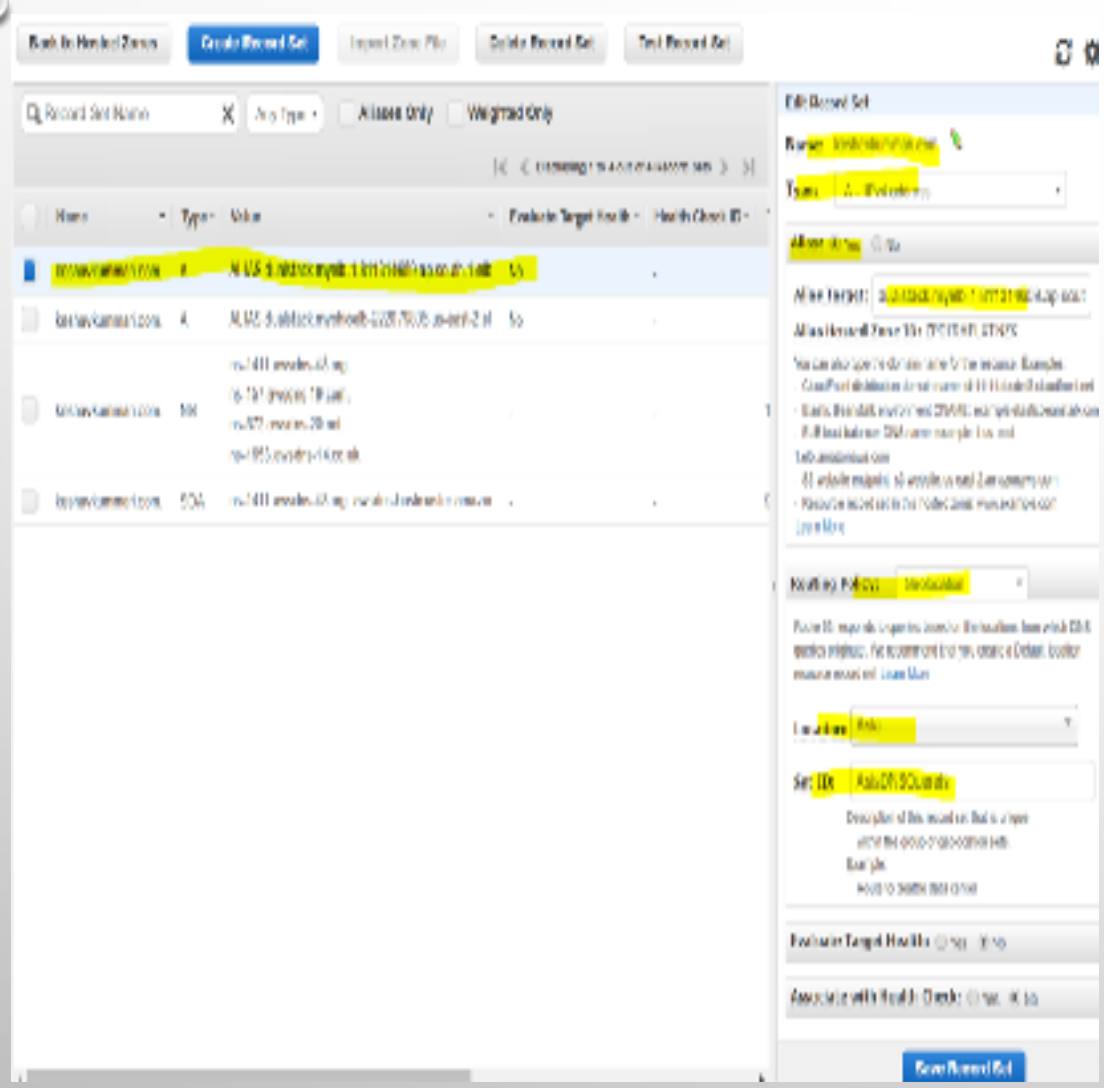


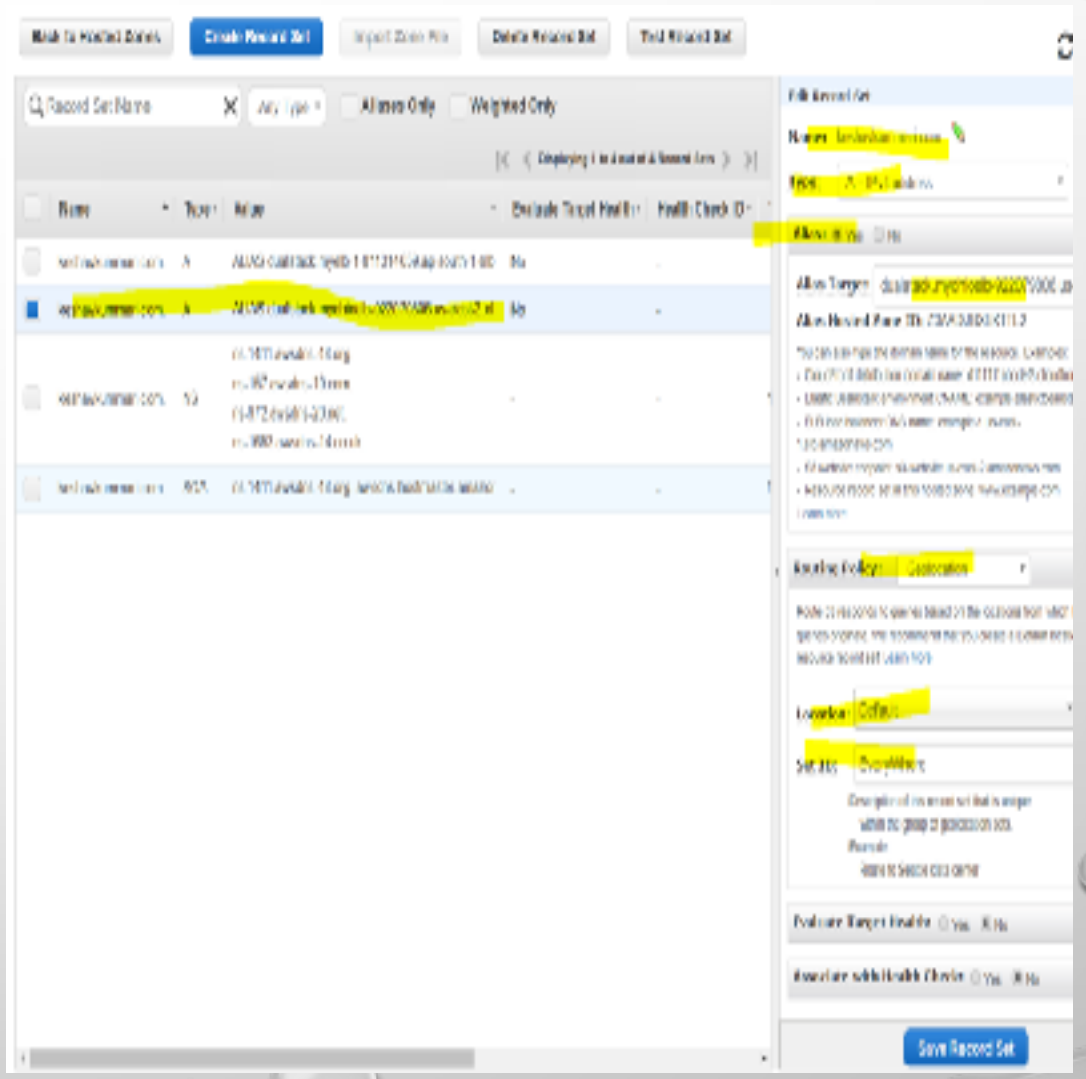
# GEOLOCATION

Geolocation routing lets you choose where your traffic will be sent based on the geographic location of your users (ie the location from which DNS queries originate). For example, you might want all queries from Europe to be routed to a fleet of EC2 instances that are specifically configured for your European customers. These servers may have the local language of your European customers and all prices are displayed in Euros.

# GEOLOCATION

# GO TO ROUTE53





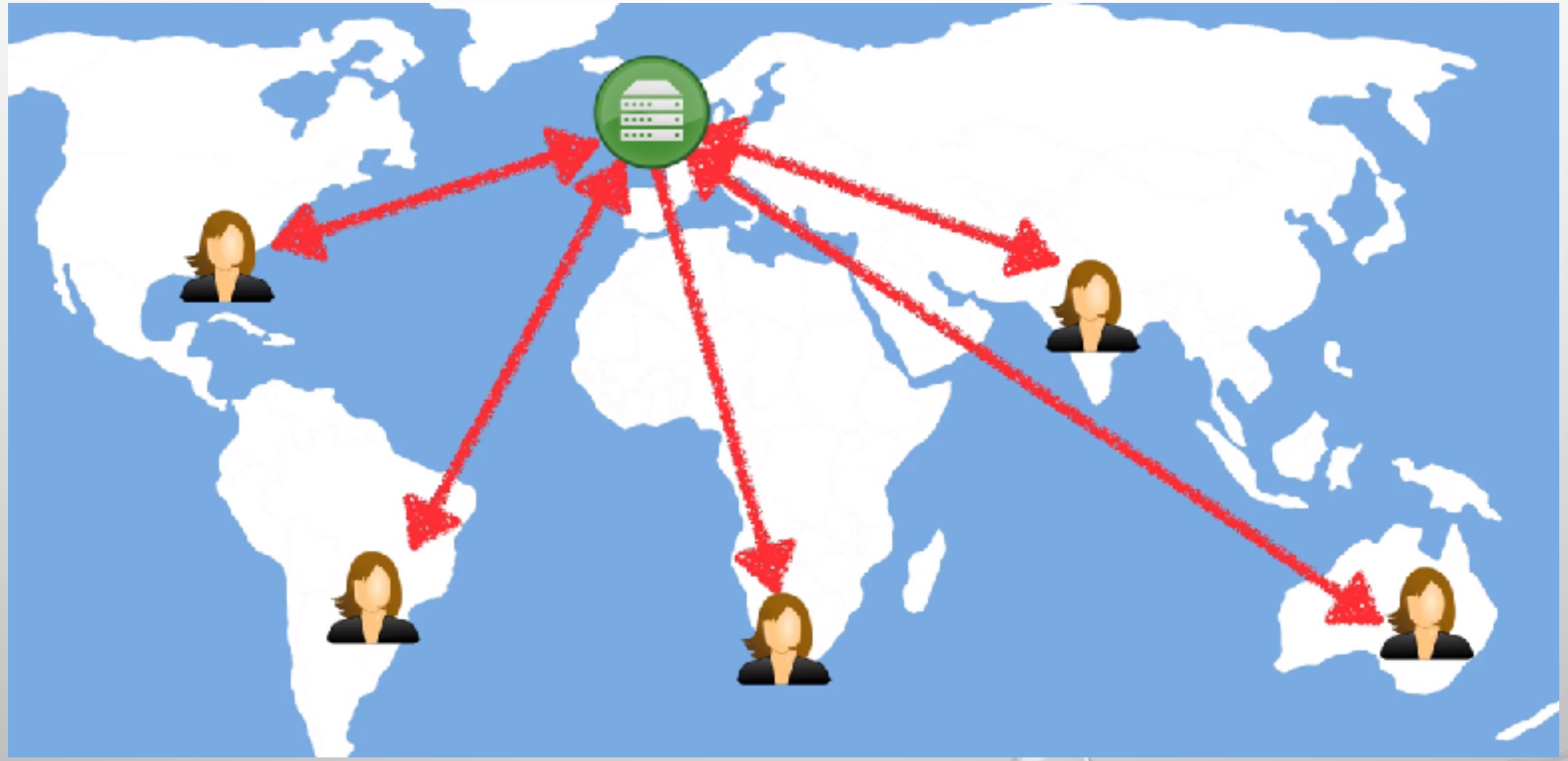
# DOWNLOAD VPN AND TEST THE CONNECTION

- CHECK THE CONNECTION FROM DIFFERENT COUNTRY:

# WHAT IS A CDN?

A content delivery network (CDN) is a system of distributed servers (network) that deliver webpages and other web content to a user based on the geographic locations of the user, the origin of the webpage and a content delivery server.

# CDN EXAMPLE



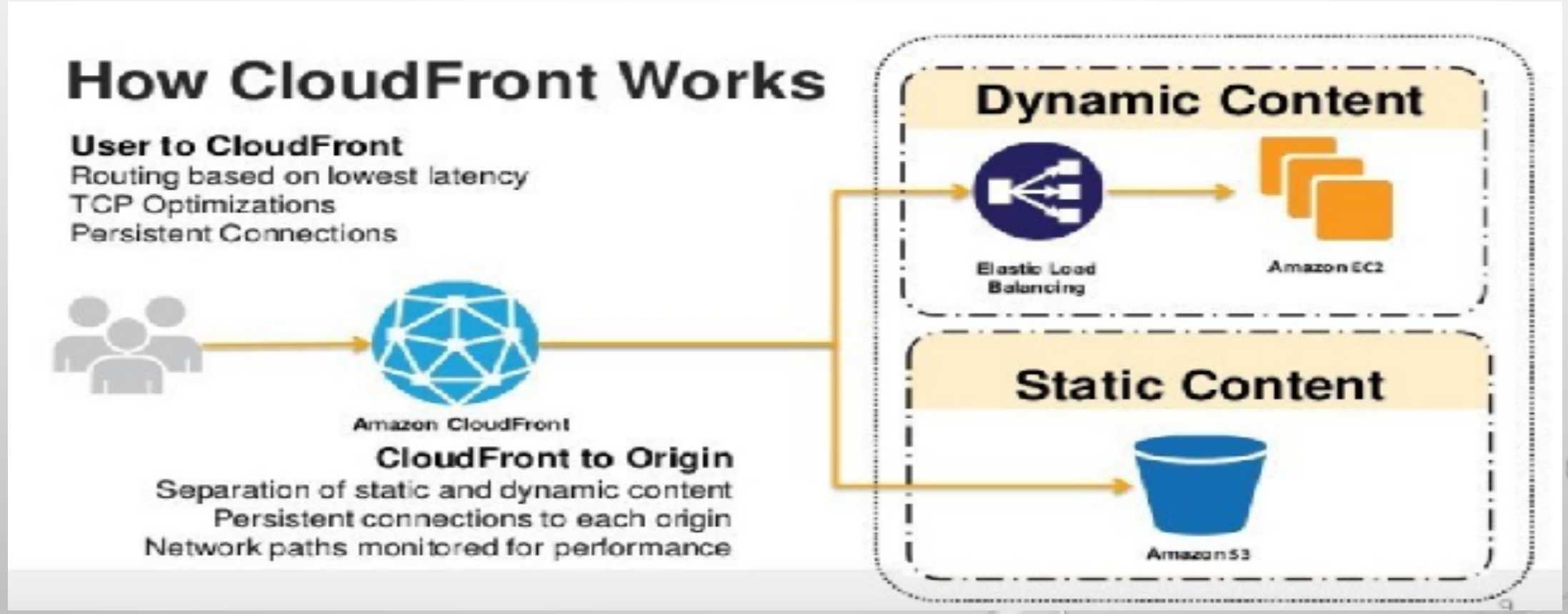
# WHAT IS CLOUDFRONT?

Amazon CloudFront can be used to deliver your entire website, including dynamic, static, streaming, and interactive content using a global network of edge locations. Requests for your content are automatically routed to the nearest edge location, so content is delivered with the best possible performance.

Amazon CloudFront is optimized to work with other Amazon Web Services, like Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Load Balancing, and Amazon Route 53. Amazon CloudFront also works seamlessly with any non-AWS origin server, which stores the original, definitive versions of your files.

# CLOUDFRONT KEY TERMINOLOGY

- WEB DISTRIBUTION - TYPICALLY USED FOR WEBSITES.
- RTMP - USED FOR MEDIA STREAMING



- Edge Location - This is the location where content will be cached. This is separate to an AWS Region/AZ
- Origin - This is the origin of all the files that the CDN will distribute. This can be either an S3 Bucket, an EC2 Instance, an Elastic Load Balancer or Route53.
- Distribution - This is the name given the CDN which consists of a collection of Edge Locations.

# CDN EXAMPLE-2