

S.KARTHEEK

RA2011028010068

## Experiment : 9

### Title : Configure Failover Routing with Amazon Route 53

Date: 09/11/2022

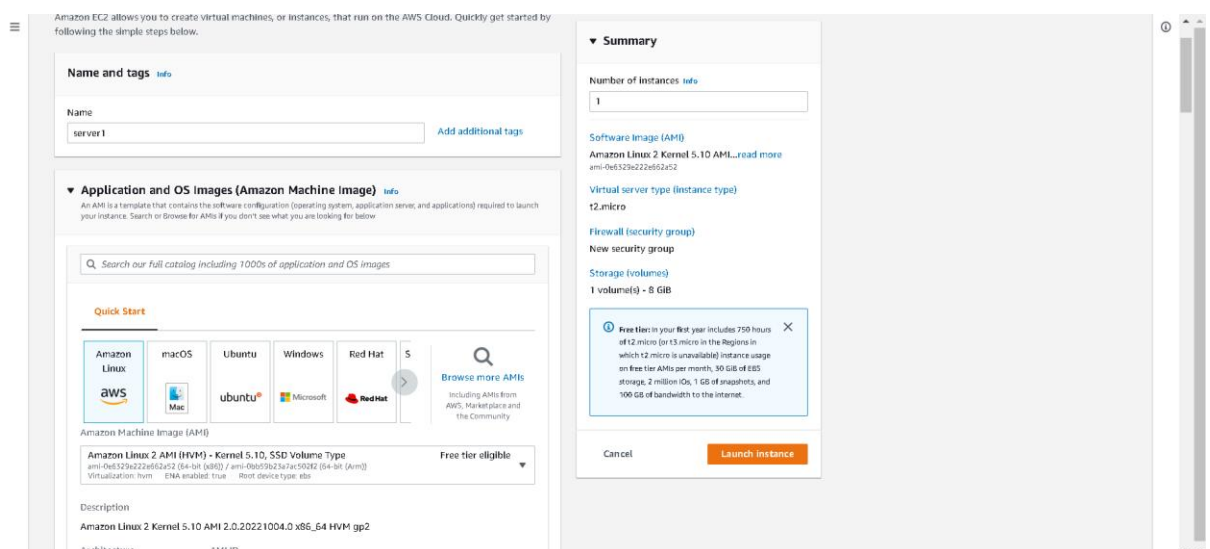
**Aim :** Configure DNS failover routing policy for Webservers across AWS Regions.

**Pre-requisites :** AWS Console, Amazon Route 53, Amazon EC2.

## Procedure :

Steps:

1. Create a Public webserver in region 1.



S.KARTHEEK

RA2011028010068

Instance type

t2.micro  
Family: t2, 1 vCPU, 1 GiB Memory  
On-Demand Linux pricing: 0.0124 USD per Hour  
On-Demand Windows pricing: 0.017 USD per Hour  
Free tier eligible  
[Compare instance types](#)

Key pair (login)

Key pair name - required

ad1543  
[Create new key pair](#)

Network settings

VPC - required

vpc-0f5e6ca3b5f734013 (default)  
172.31.0.0/16  
[Create new VPC](#)

Subnet

subnet-0d666856a68d53e15  
VPC: vpc-0f5e6ca3b5f734013 Owner: 979354539947 Availability Zone: ap-south-1b  
IP addresses available: 4091 CIDR: 172.31.0.0/20  
[Create new subnet](#)

Auto-assign public IP

Enable  
[Create new public IP](#)

Firewall (security groups)

Create security group

Select existing security group

Summary

Number of instances 1  
[Add](#)

Software Image (AMI)  
Amazon Linux 2 Kernel 5.10 AMI...  
[Read more](#)  
ami-0e6129e222e6b2e12

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 8 GiB

Free tier in your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet.

Cancel Launch instance

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Internet Services Private Ltd. or its affiliates

Privacy Terms Cookie preferences

27°C Cloudy

Windows taskbar

Services Search [Alt+S]

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#launchinstances

Launch an instance | EC2 Manag

Enable

Firewall (security groups)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Security group name - required

webserv

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_ (not at the beginning or end).

Description - required

launch-wizard-7 created 2022-11-08T09:04:56.116Z

Inbound security group rules

Security group rule 1 (TCP, 22, 14.96.13.220/32)

Remove

Type ssh Protocol TCP Port range 22

Source type My IP Name 14.96.13.220/32 Description - optional e.g. SSH for admin desktop

Security group rule 2 (TCP, 80, 0.0.0.0/0)

Remove

Type HTTP Protocol TCP Port range 80

Source type Custom Source 0.0.0.0/0 Description - optional e.g. SSH for admin desktop

Summary

Number of instances 1  
[Add](#)

Software Image (AMI)  
Amazon Linux 2 Kernel 5.10 AMI...  
[Read more](#)  
ami-0e6129e222e6b2e12

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

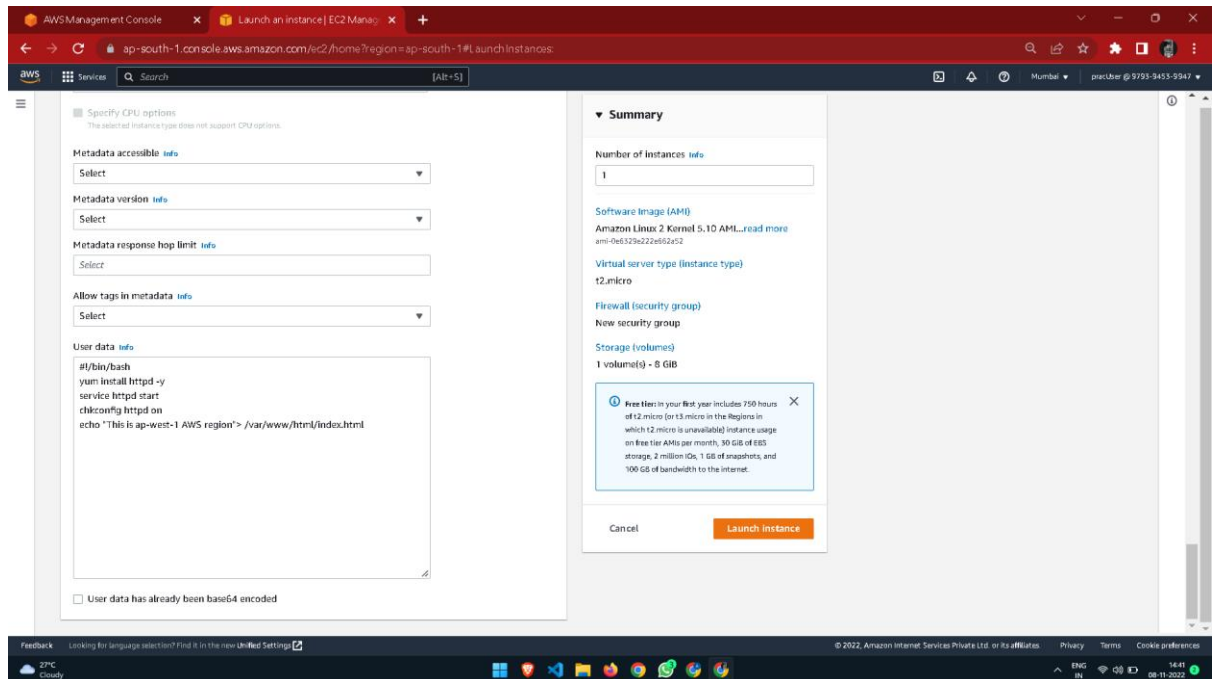
Storage (volumes)  
1 volume(s) - 8 GiB

Free tier in your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet.

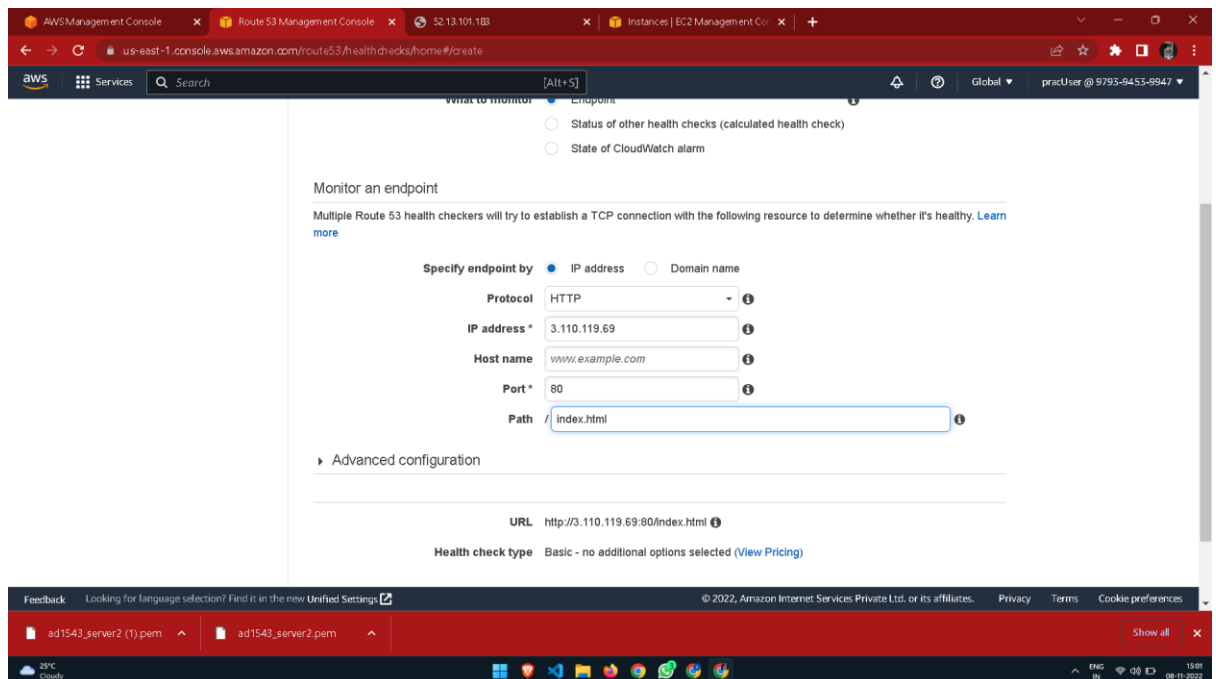
Cancel Launch instance

S.KARTHEEK

RA2011028010068



2. Create a public webserver in region 2.
3. Create a Route53 public hosted zone (e.g: Yourdomain.com).
4. Create 2 health checks for both the webserver.



**Create health check**

**Step 1: Configure health check**  
Step 2: Get notified when health check fails

### Configure health check

Route 53 health checks let you track the health status of your resources, such as web servers or mail servers, and take action when an outage occurs.

**Name** webserver-ap-south-1

**What to monitor**

- ☒ Endpoint
- ☐ Status of other health checks (calculated health check)
- ☐ State of CloudWatch alarm

**Monitor an endpoint**

Multiple Route 53 health checkers will try to establish a TCP connection with the following resource to determine whether it's healthy. [Learn more](#)

**Specify endpoint by** ☒ IP address ☐ Domain name

**Protocol** HTTP

**IP address \*** 3.110.119.69

**Host name** www.example.com

5. Create a subdomain A record test.yourdomain.com and configure it as failover routing (Primary).

**Health checks**

Create health check Delete health check Edit health check

Filter by keyword

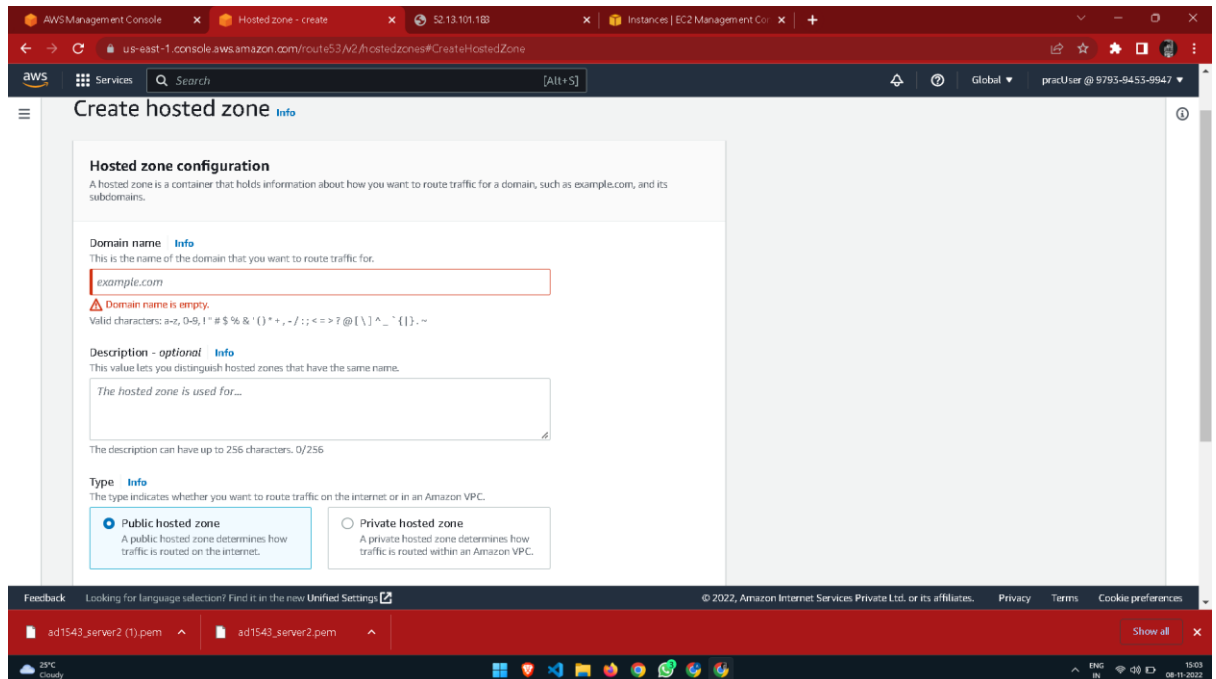
Name	Status	Description	Alarms	ID
webserver-us-west-2	Unknown	http://52.13.101.183:80/index.html	No alarms configured.	5567d956-467c-4c91
webserver-ap-south-1	Healthy	http://3.110.119.69:80/index.html	No alarms configured.	adf1d20d-8363-4516

1 to 2 of 2 health checks

Info Monitoring Alarms Tags Health checkers Latency

No health check selected.

6. Create another same subdomain A record test.yourdomain.com and configure it as failover routing (secondary).



7. Test the connection by hitting `http://test.yourdomain.com`.
8. Login to primary webserver in region 1 and stop `httpd` service.
9. Wait for TTL to expire and see If you get redirected to another web server in region 2.

## Result:

Hence, we have successfully configure DNS failover routing policy for Webserver across AWS Regions.