

# Experiment : 9

## Title : Configure Failover Routing with Amazon Route 53

Date: 09/11/2022

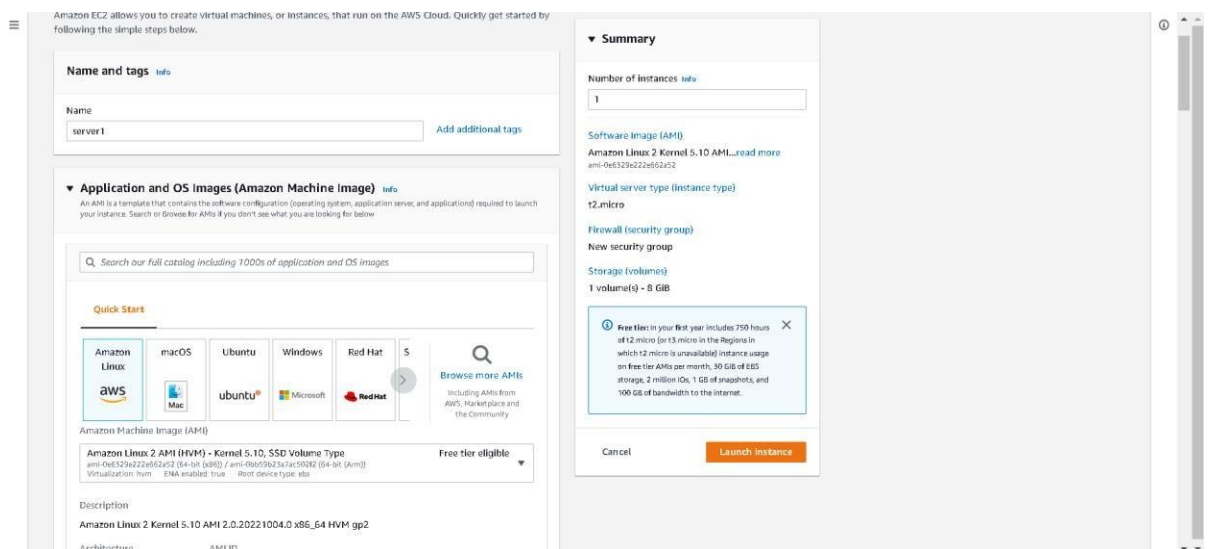
**Aim :** Configure DNS failover routing policy for Webservers across AWS Regions.

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

## Procedure :

Steps:

1. Create a Public webserver in region 1.



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)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

ad1543

Create new key pair

Network settings

VPC - required

vpc-0f5e6ca3b5f734813  
172.31.0.0/16

(default)

Subnet

subnet-0d6668b6a68d53e15  
VPC: vpc-0f5e6ca3b5f734813 Owner: 579394519347 Availability Zone: ap-south-1b  
IP addresses available: 4091 CIDR: 172.31.0.0/20

Create new subnet

Auto-assign public IP

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

Number of instances

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...  
ami-0e6329e22e662e52

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 On, 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.

22°C Cloudy

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

ENG IN 14:40 08-11-2022

AWSServices AWS Management Console Launch an Instance | EC2 Manager

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

aws Services Search [Alt+S]

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

webserver

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 \_/!@#%^&\*()~`

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

Name

0.0.0.0/0

Description - optional

e.g. SSH for admin desktop

Summary

Number of instances

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...  
ami-0e6329e22e662e52

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

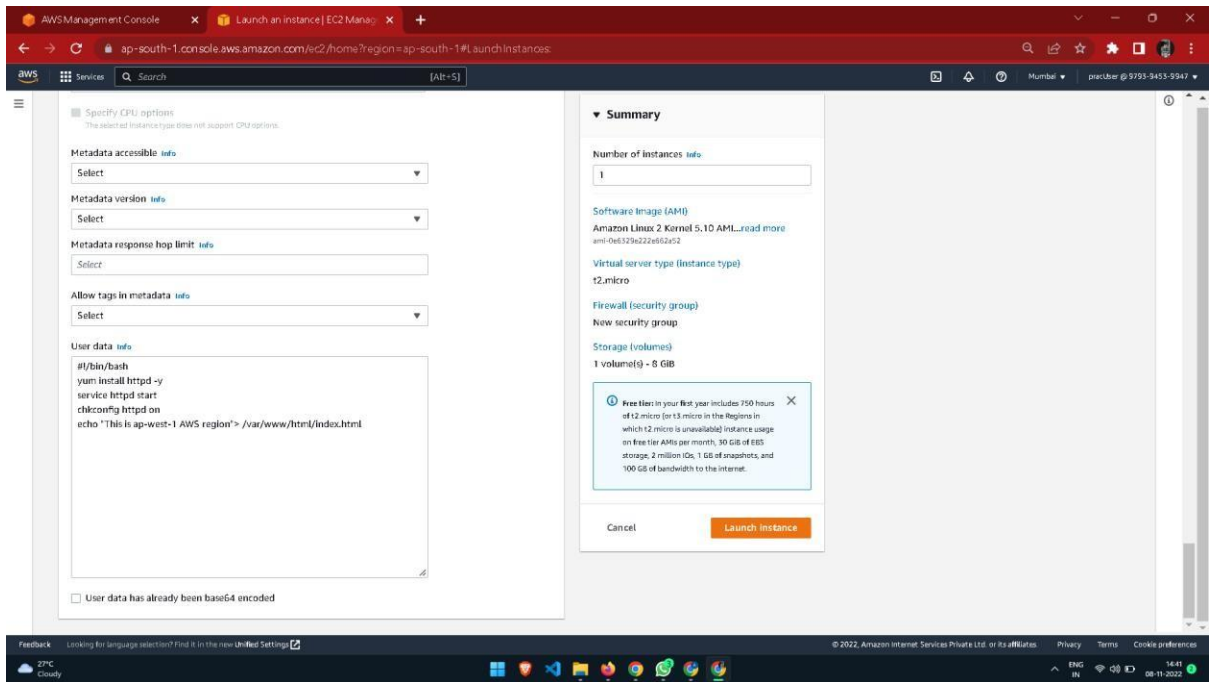
Storage (volumes)

1 volume(s) - 8 GiB

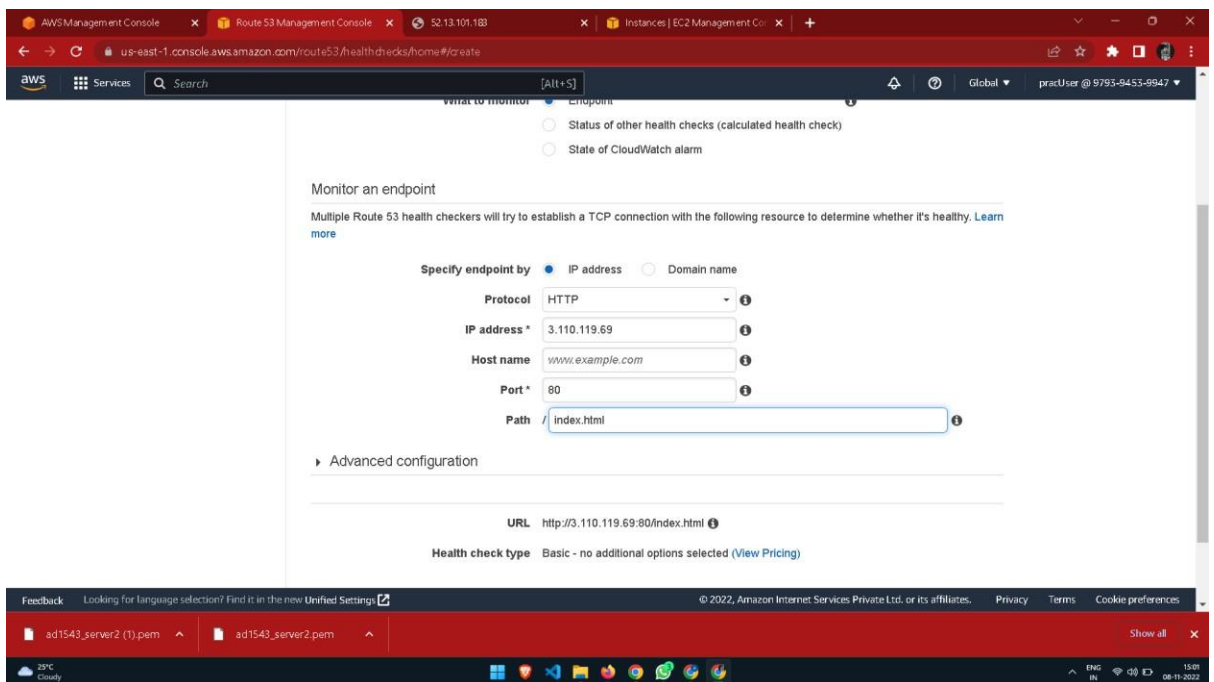
Free tier in your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million On, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet.

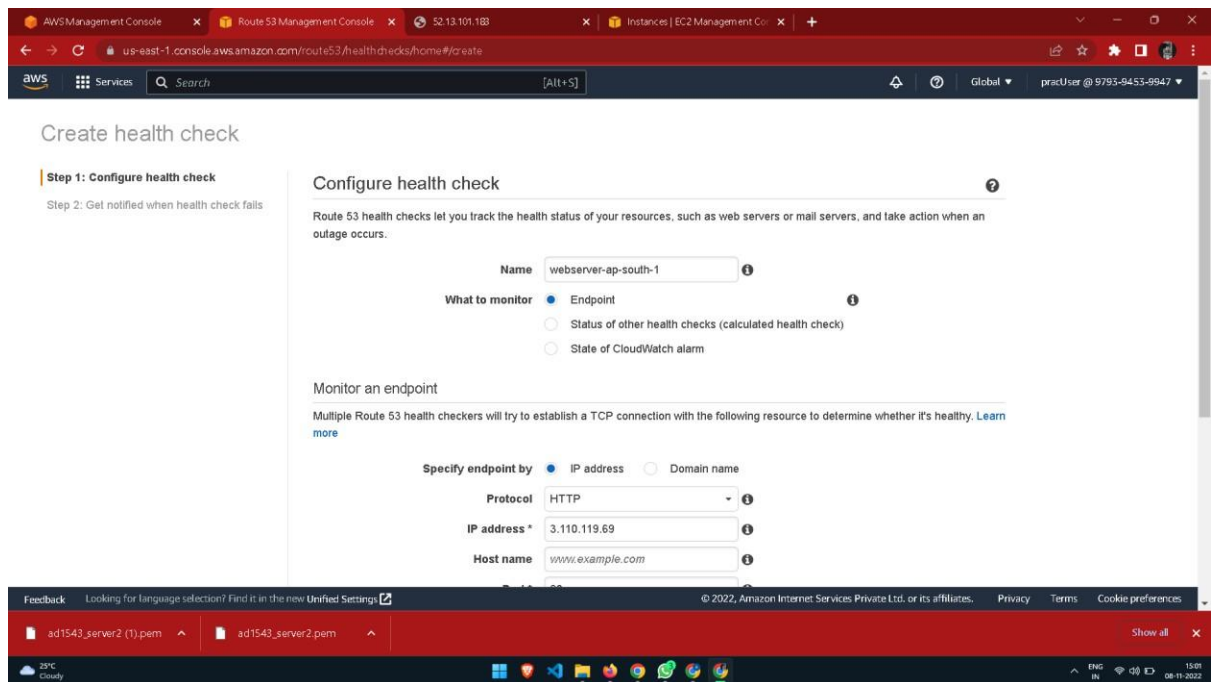
Cancel

Launch instance

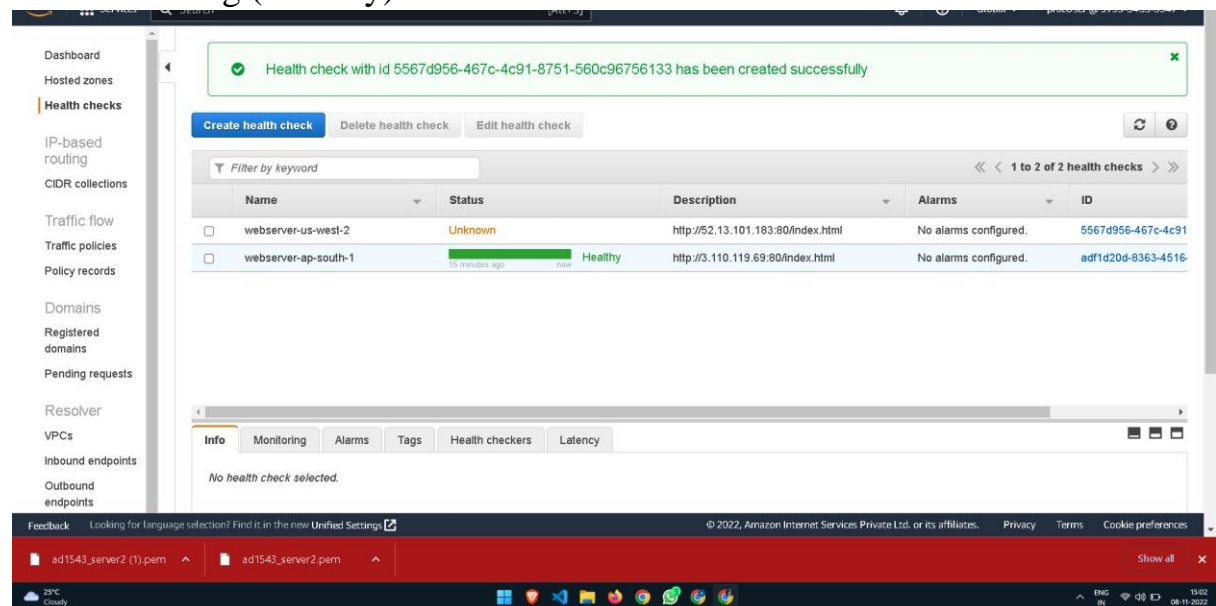


2. Create a public webserver in region 2.
3. Create a Route53 public hosted zone (e.g: Yourdomain.com).
4. Create 2 health checks for both the webserver.

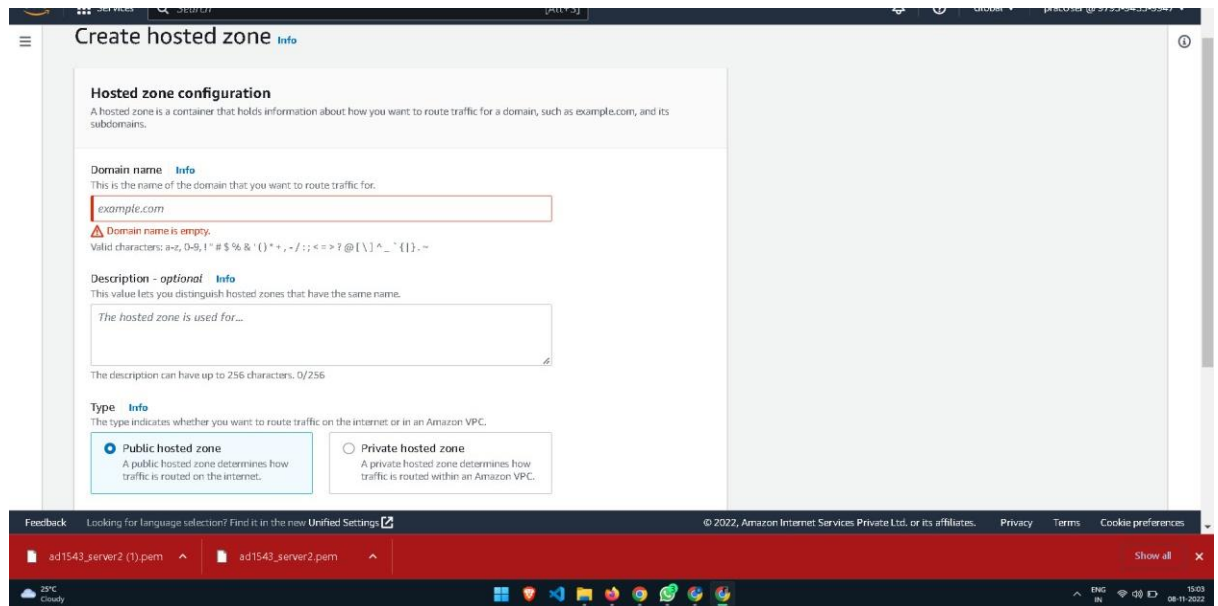




5. Create a subdomain A record test.yourdomain.com and configure it as failover routing (Primary).



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.