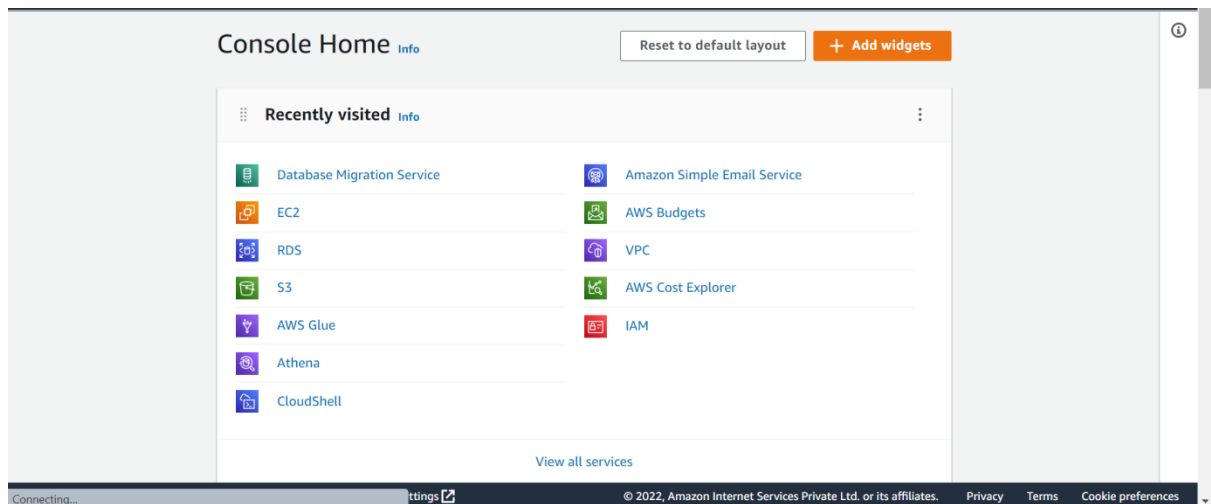


Experiment 8—Configure Failover Routing with Amazon Route 53

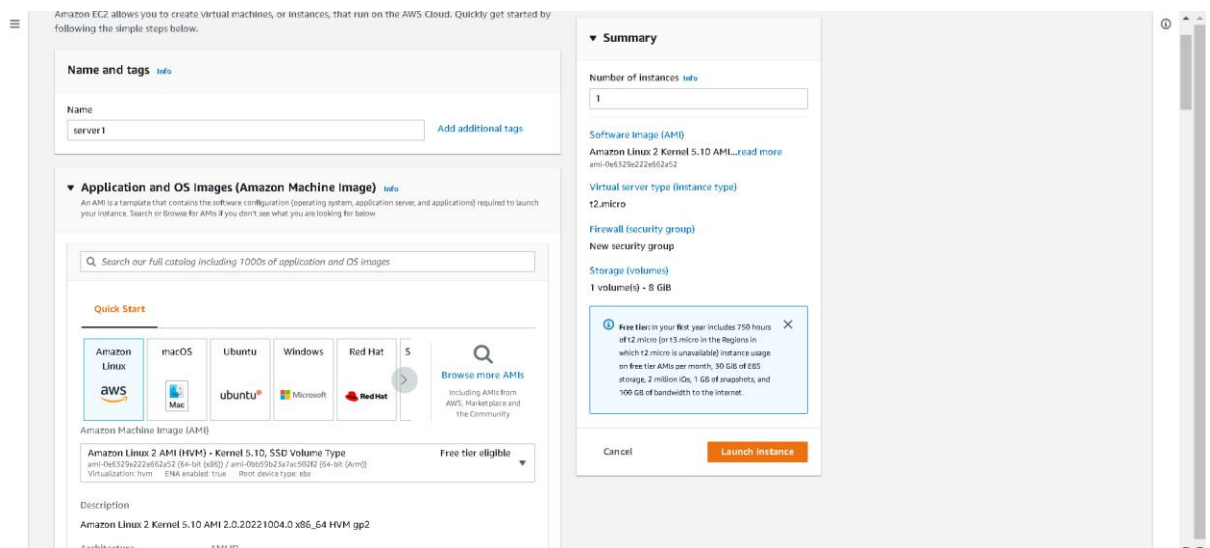
AIM: To configure failover routing with Amazon Route 53.

PROCEDURE:

1. Firstly, open the AWS console homepage on browser (<https://aws.amazon.com/console/>).



1. Create a Public webserver in region 1.



Services

Search

[Alt+S]

Mumbai

prachar @ 9793-9453-9947

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0124 USD per Hour

On-Demand Windows pricing: 0.0173 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

(default)

Subnet

subnet-0d666856a68d53e15

VPC: vpc-0f5e6ca3b5f734813 Owner: 979394539947 Availability Zone: ap-south-1b

IP addresses available: 4091 CIDR: 172.31.0.0/16

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

Summary

Number of instances

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AML...read more

ami-0e6329e222e62a52

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 IOPS, 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

Services

Search

[Alt+S]

Mumbai

prachar @ 9793-9453-9947

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

webservers

Description - required

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

Inbound security groups 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

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AML...read more

ami-0e6329e222e62a52

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 IOPS, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet.

Cancel

Launch instance

Feedback

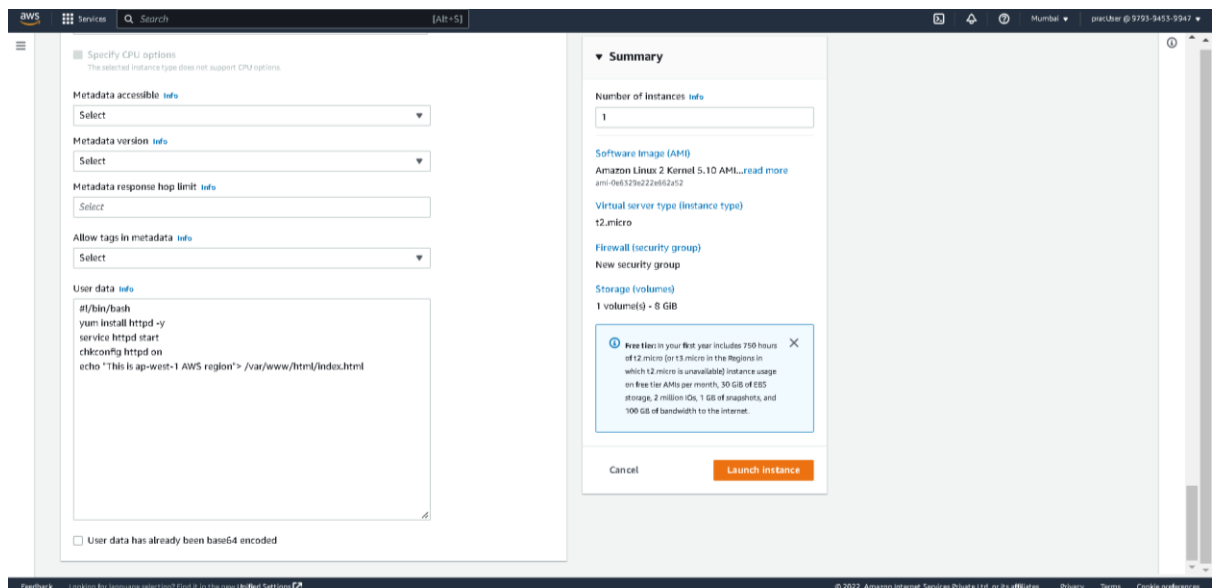
Looking for language selection? Find it in the new Unified Settings

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

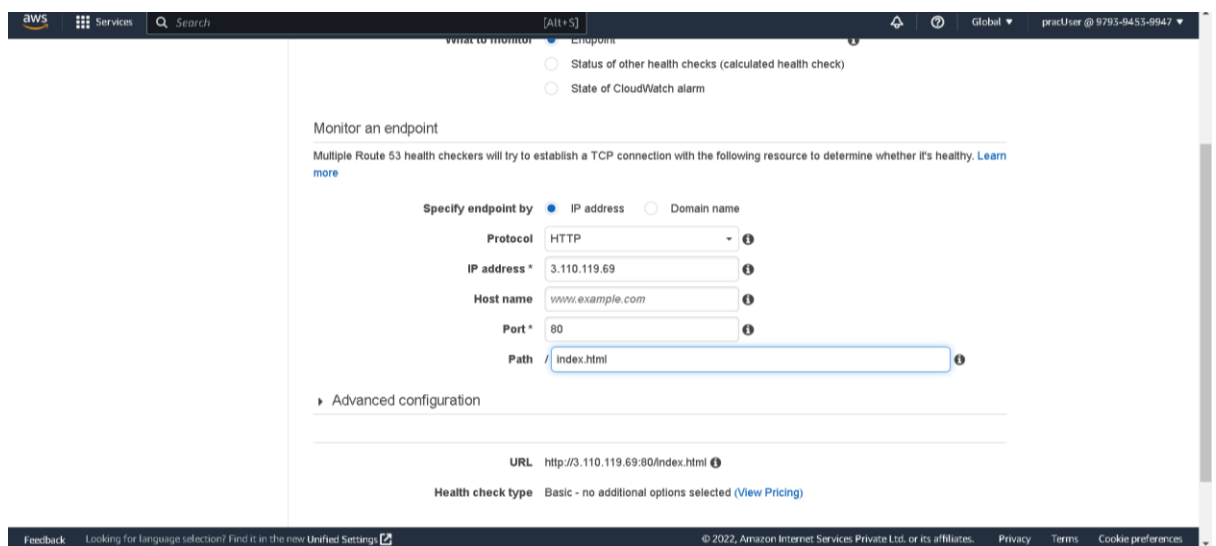
Privacy

Terms

Cookie preferences



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

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

IP address *

Host name

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

Health check with id 5567d956-467c-4c91-8751-560c96756133 has been created successfully

[Create health check](#) [Delete health check](#) [Edit health check](#)

Filter by keyword

Name	Status	Description	Alarms	ID
<input type="checkbox"/> webserver-us-west-2	Unknown	http://52.13.101.183:80/index.html	No alarms configured.	5567d956-467c-4c91
<input type="checkbox"/> webserver-ap-south-1	Healthy 15 minutes ago	http://3.110.119.69:80/index.html	No alarms configured.	adf1d20d-8363-4516

Info Monitoring Alarms Tags Health checkers Latency

No health check selected.

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

Hosted zone configuration
A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain name [Info](#)
This is the name of the domain that you want to route traffic for.

Domain name is empty.
Valid characters: a-z, 0-9, ! * # \$ % & ' () * + , - / : ; < = > ? @ [\] ^ _ ` { | } . ~

Description - optional [Info](#)
This value lets you distinguish hosted zones that have the same name.

The description can have up to 256 characters. 0/256

Type [Info](#)
The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

☒ **Public hosted zone**
A public hosted zone determines how traffic is routed on the internet.

☐ **Private hosted zone**
A private hosted zone determines how traffic is routed within an Amazon VPC.

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:

A failover routing with Amazon Route 53 was configured successfully.