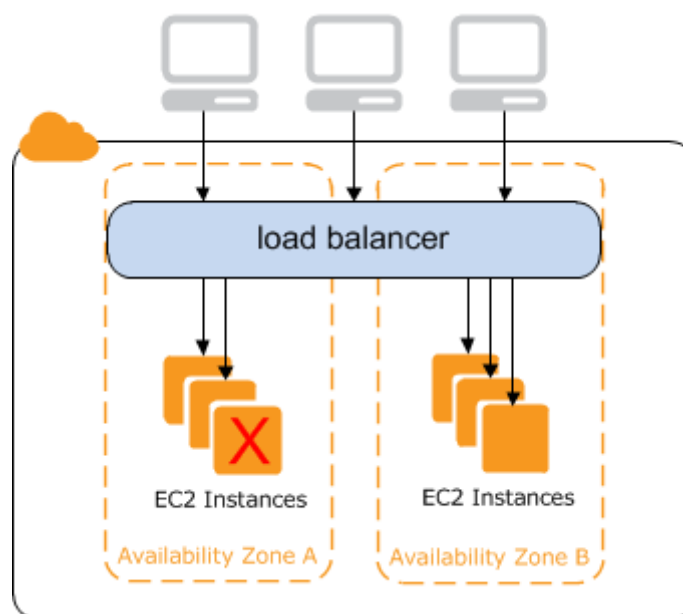


ELASTIC LOAD BALANCER:

Elastic Load Balancing automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in one or more Availability Zones.

It monitors the health of its registered targets, and routes traffic only to the healthy targets.



4 types of elastic load balancer:

- Classic load balancer
- Application load balancer
- Network load balancer
- Gateway load balancer

Classic load balancer:

Monolithic application support classic load balancer

Steps to create elastic load balancer:

Step1: launch linux instance----->(no of instance selec-->2)

Name and tags [Info](#)

Name: elb1 [Add additional tags](#)

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search: Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux, macOS, Ubuntu, Windows, Red Hat, S, Browse more AMIs

Number of instances [Info](#): 2

When launching more than 1 instance, consider EC2 Auto Scaling.

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...[read more](#) (ami-0cca134ec43cf708f)

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. [Cancel](#) [Launch instance](#)

Step2: create key pair --->add security group2(http)

Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type [Info](#): ssh

Protocol [Info](#): TCP

Port range [Info](#): 22

Source type [Info](#): Anywhere

Source [Info](#): Add CIDR, prefix list or security group (0.0.0.0/0 X)

Description - optional [Info](#): e.g. SSH for admin desktop

Security group rule 2 (TCP, 80, 0.0.0.0/0) [Remove](#)

Type [Info](#): HTTP

Protocol [Info](#): TCP

Port range [Info](#): 80

Source type [Info](#): Custom

Source [Info](#): Add CIDR, prefix list or security group (0.0.0.0/0 X)

Description - optional [Info](#): e.g. SSH for admin desktop

Step3: advanced details---->user data(any bash script type)

Create 2 EC2 insatnces with 2 diffrent AZ

add the below details under user data

#!/bin/bash

yum update -y

yum install httpd -y

service httpd start

echo "Hi you are hitting linux1 instance" > /var/www/html/index.html

User data [Info](#)

```
#!/bin/bash
yum update -y
yum install httpd -y
service httpd start
echo "Hi you are hitting linux1 instance" > /var/www/html/index.html
```

☐ User data has already been base64 encoded

When launching more than 1 instance, consider [EC2 Auto Scaling](#).

[Software Image \(AMI\)](#)
Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-0cca134ec43cf708f

[Virtual server type \(instance type\)](#)
t2.micro

[Firewall \(security group\)](#)
New security group

[Storage \(volumes\)](#)
1 volume(s) - 8 GiB

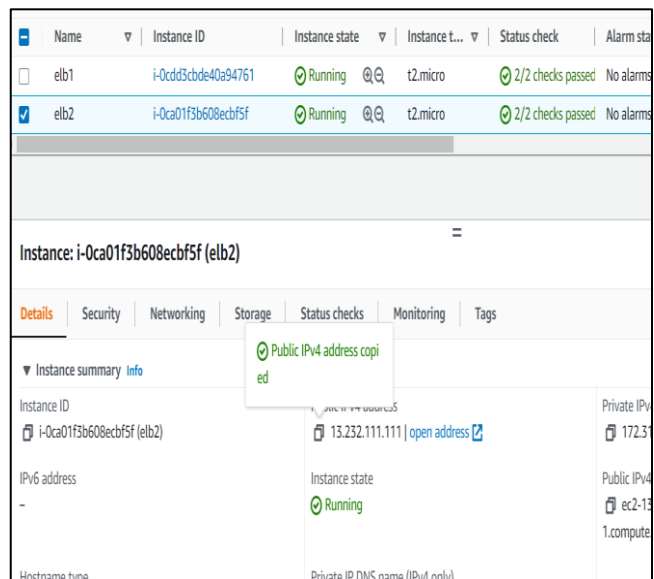
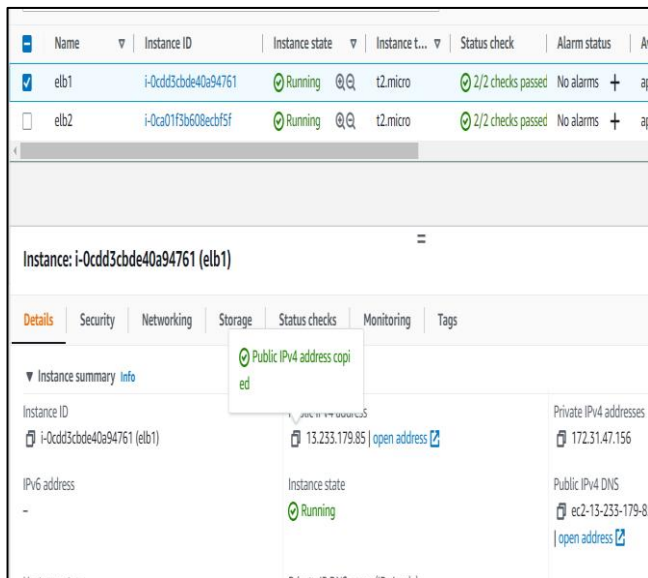
[Cancel](#) [Launch instance](#)

2 instance launch completed

Instances (2) Info								
Find instance by attribute or tag (case-sensitive)								
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance t...	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input type="checkbox"/>	elb1	i-0cdd3cbde40a94761	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	ec2-13-233-179-8
<input type="checkbox"/>	elb2	i-0ca01f3b608ecbf5f	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	ec2-13-232-111-7

Step4: elb1---->public ip copy--->put chrome page

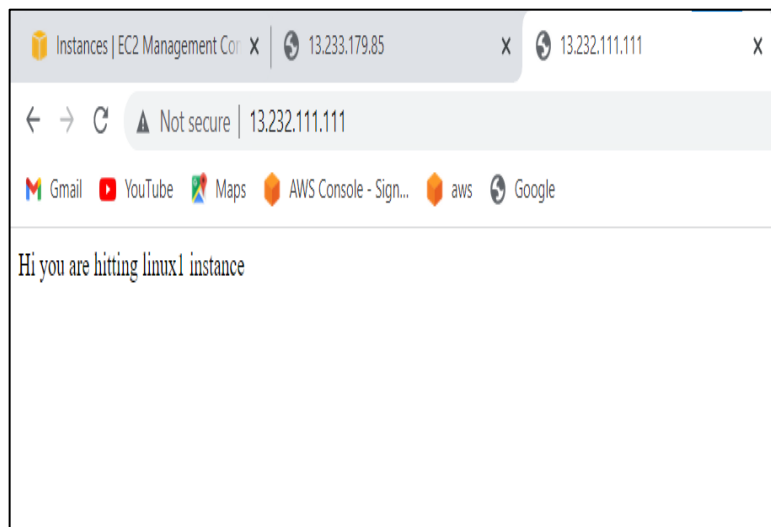
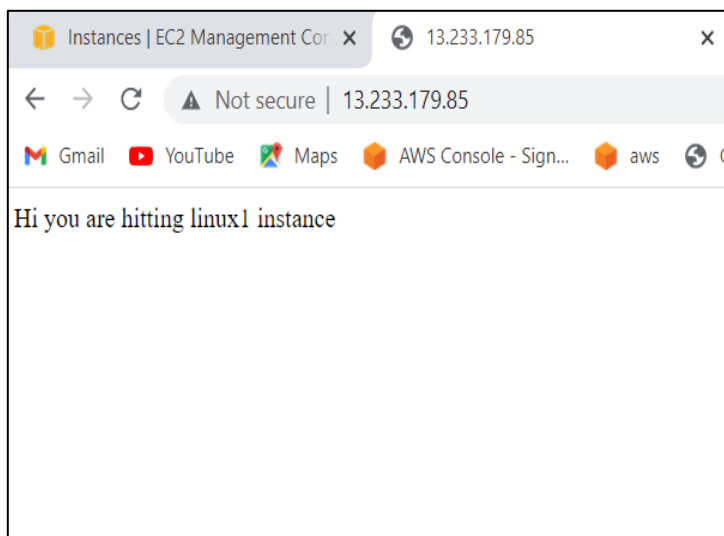
elb2--->public ip copy --->put chrome page



Step5: elb1---->public ip copy--->put chrome page--->hitting linux1

elb2--->public ip copy --->put chrome page--->hitting linux1

} Same content shown



Step6:elb2 ---->change linux1 to linux2

1.Putty open ---->login:ec2-user

2.Change root user---->sudo -i

3.change disk ---->#cd /var/www/html

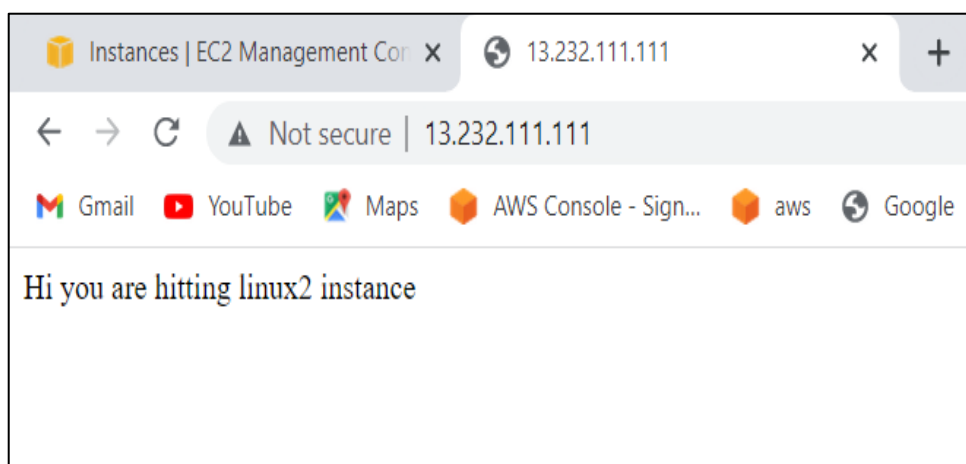
4.list----->ls (we give before bash script file will shown)---->index.html

5.now edit ---->vi index.html ---->linux1(change linux2) --->wq!

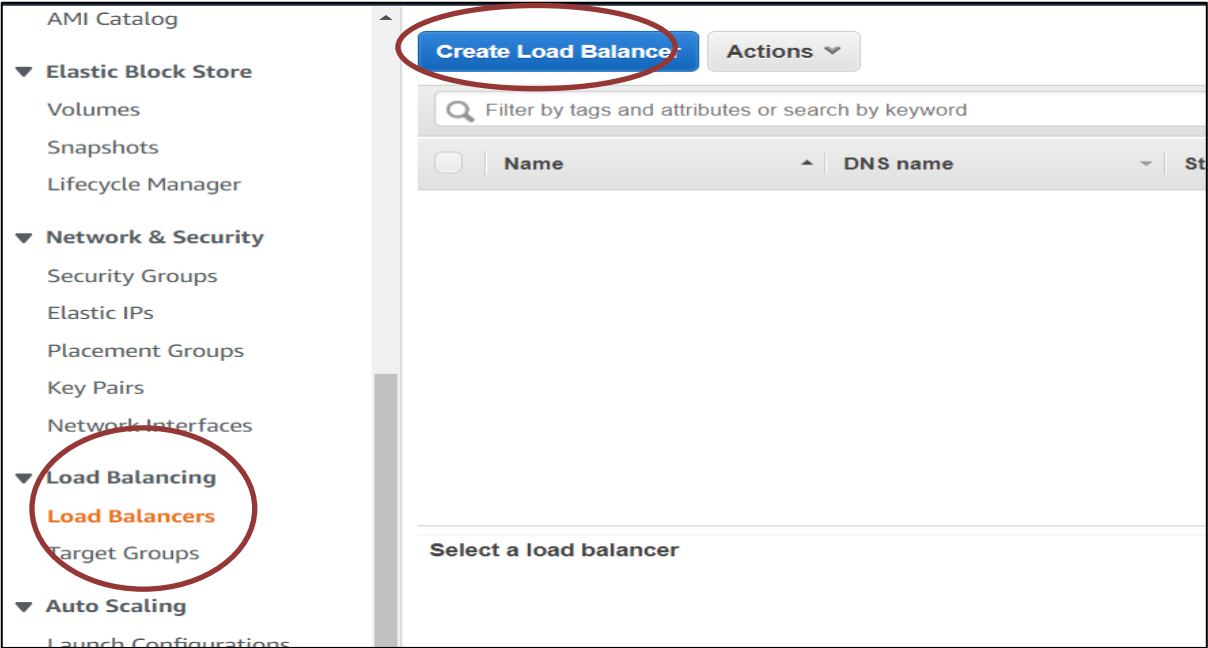
```
ec2-user@ip-172-31-46-201:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
  
  _ |  _ | _ )  
 _ | ( _ | /  Amazon Linux 2 AMI  
 _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-172-31-46-201 ~]$ sudo -i  
[root@ip-172-31-46-201 ~]# cd /var/www/html  
[root@ip-172-31-46-201 html]# ls  
index.html  
[root@ip-172-31-46-201 html]# vi index.html  
[root@ip-172-31-46-201 html]#
```

```
root@ip-172-31-46-201:/var/www/html  
Hi you are hitting linux2 instance  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~
```

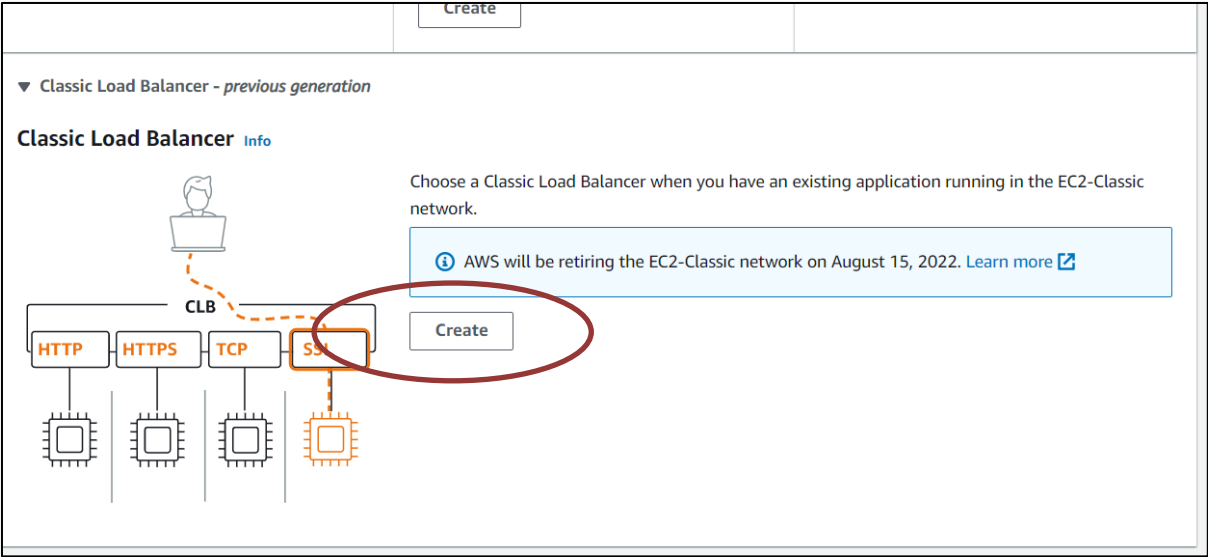
Now check elb2 public ip --->chrome--->it will change(linux2)



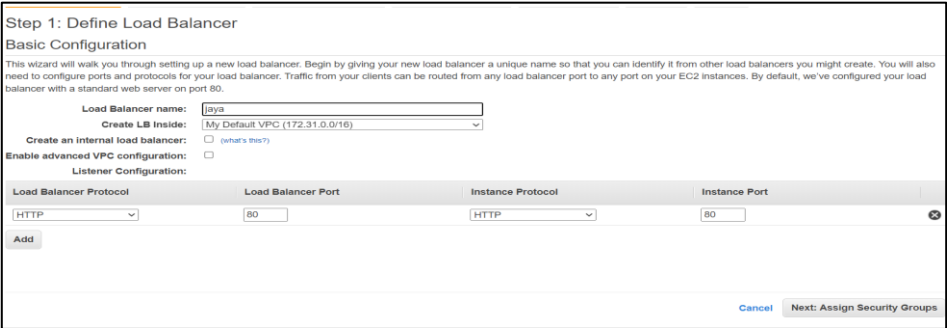
Step7:load balancing--->load balacer--->create load balacer



Step8:select load balancer type--->classic load balancer--->create



Step9:define load balancer--->any name(eg.java)--->next



Step10:assign security group--->select exiting security group(instance security

Instances (1/2) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type
elb1	i-0cdd3cbde40a94761	Running	t2.micro
elb2	i-0ca01f3b608ecbf5f	Running	t2.micro

Instance: i-0cdd3cbde40a94761 (elb1)

Details | **Security** | Networking | Storage | Status checks | Monitoring

Security details

IAM Role: -

Owner ID: 795071115491

Security groups

- sg-05b92fc560ff4fbdd (launch-wizard-5)

Inbound rules

Outbound rules

1. Define Load Balancer | 2. **Assign Security Groups** | 3. Configure Security Settings | 4. Configure Health Check | 5. Add EC2 Instances | 6. Add Tags | 7. Review

Step 2: Assign Security Groups

You have selected the option of having your Elastic Load Balancer inside of a VPC, which allows you to assign security groups to your load balancer. Please select the security groups to assign to the load balancer. This can be changed at any time.

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

Filter: VPC security groups

Security Group ID	Name	Description	Actions
sg-0180300400dbff0f4	AutoScaling-Security-Group-1	AutoScaling-Security-Group-1 (2022-12-23T06:17:55.995Z)	Copy to clipboard
sg-0181ee44ea24de8b9	default	default VPC security group	Copy to clipboard
sg-0c3a746939f51130f	launch-wizard-1	launch-wizard created 2022-12-23T04:06:08.894Z	Copy to clipboard
sg-0b7f737e6b4c2a133	launch-wizard-2	launch-wizard-2 created 2022-12-23T04:28:14.200Z	Copy to clipboard
sg-0cc8b9f4b07a91e1b	launch-wizard-3	launch-wizard created 2022-12-23T04:42:47.840Z	Copy to clipboard
sg-0f8a382c1a7b5c1d3	launch-wizard-4	launch-wizard created 2022-12-23T05:06:33.567Z	Copy to clipboard
sg-05b92fc560ff4fbdd	launch-wizard-5	launch-wizard-5 created 2022-12-23T06:56:51.962Z	Copy to clipboard

Instance security groups --->match same security group select -->next

1. Define Load Balancer | 2. Assign Security Groups | 3. **Configure Security Settings** | 4. Configure Health Check | 5. Add EC2 Instances | 6. Add Tags | 7. Review

Step 3: Configure Security Settings

⚠ Improve your load balancer's security. Your load balancer is not using any secure listeners. If your traffic to the load balancer needs to be secure, use either the HTTPS or the SSL protocol for your front-end connection. You can go back to the first step to add/configure secure listeners under **Basic Configuration** section. You can also continue with current settings.

Cancel Previous Next: Configure Health Check

1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | 4. **Configure Health Check** | 5. Add EC2 Instances | 6. Add Tags | 7. Review

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Ping Protocol: HTTP

Ping Port: 80

Ping Path: /index.html

Advanced Details

Response Timeout: 5 seconds

Interval: 30 seconds

Unhealthy threshold: 2

Healthy threshold: 10

Cancel Previous Next: Add EC2 Instances

Configure security setting

Configure health check

Two instance select--->next

1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | 4. Configure Health Check | 5. **Add EC2 Instances** | 6. Add Tags | 7. Review

Step 5: Add EC2 Instances

The table below lists all your running EC2 Instances. Check the boxes in the Select column to add those Instances to this load balancer.

VPC: vpc-0f0767193d3df8800 (172.31.0.0/16)

Select	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-0cdd3cbde40a94761	elb1	running	launch-wizard-5	ap-south-1a	subnet-0bf35d2...	172.31.32.0/20
<input checked="" type="checkbox"/>	i-0ca01f3b608ecbf5f	elb2	running	launch-wizard-5	ap-south-1a	subnet-0bf35d2...	172.31.32.0/20

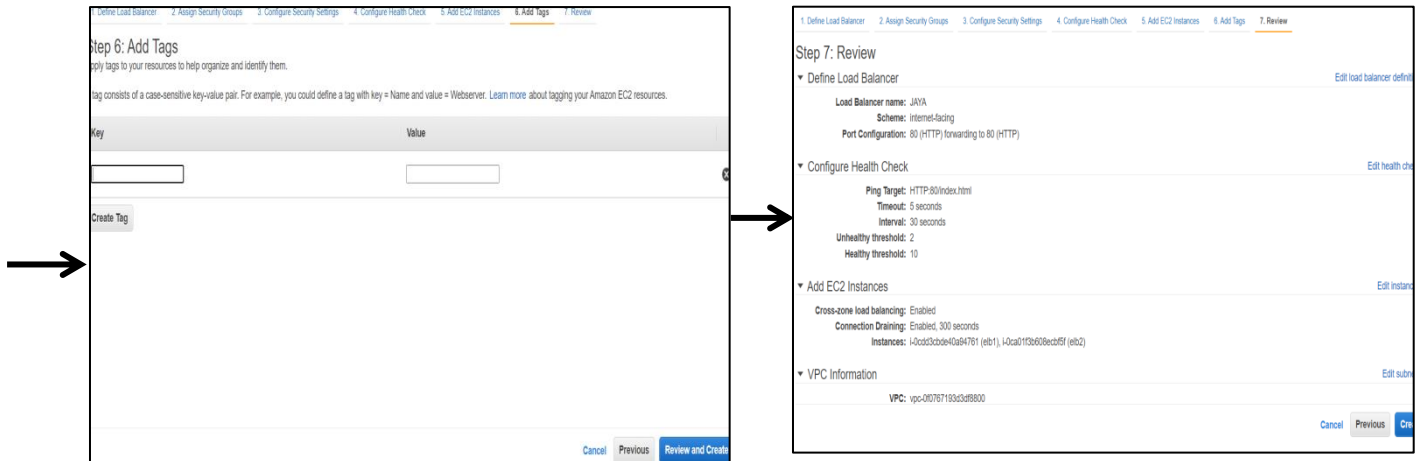
Availability Zone Distribution

2 Instances in ap-south-1a

☒ Enable Cross-Zone Load Balancing

☒ Enable Connection Draining 300 seconds

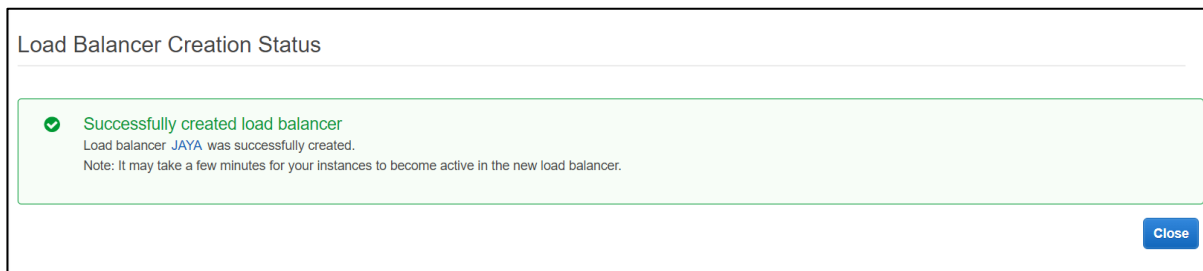
Cancel Previous Next: Add Tags



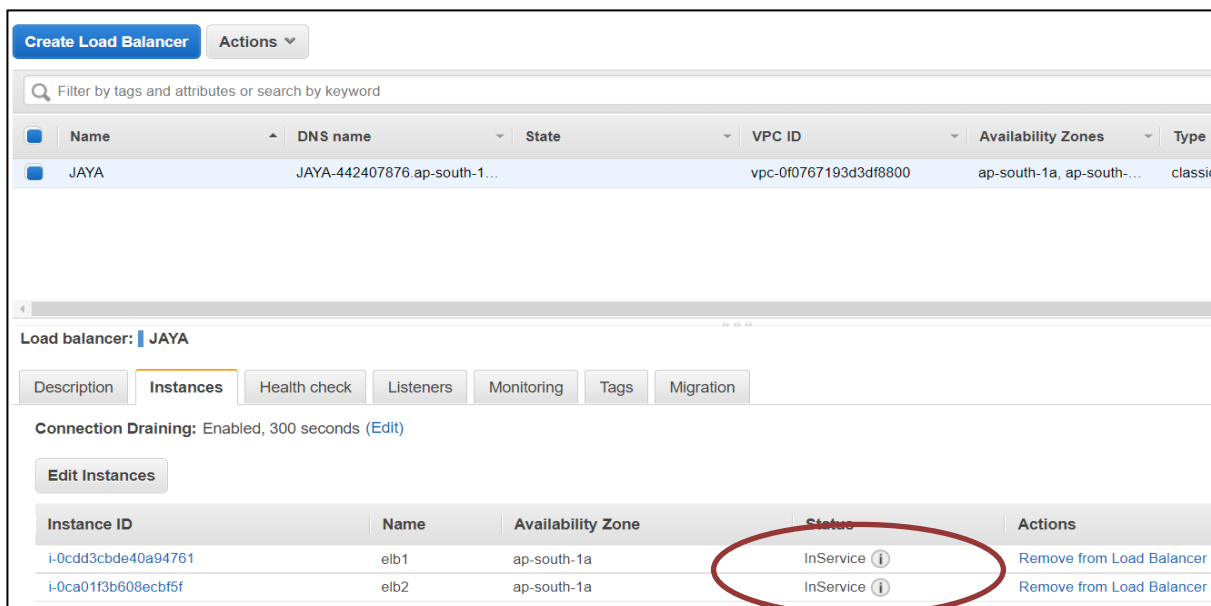
Review and create

create

Load balancer created



Step11:load balancer home-->instance-->instance id---->inservice(done)



Step12:load balacer home--->description--->DNS name(copy)

The screenshot shows the AWS Management Console interface for a Load Balancer named 'JAYA'. The 'Description' tab is selected, displaying the following configuration details:

Property	Value	Property	Value
Name	JAYA	Creation time	December 23, 2022 at 4:47:52 PM UTC+5:30
* DNS name	JAYA-442407876.ap-south-1.elb.amazonaws.com (A Record)	Hosted zone	ZP97RAFLXTNZK
Type	Classic (Migrate Now)	Status	2 of 2 instances in service
Scheme	internet-facing	VPC	vpc-0f0767193d3df8800

Step12:DNS name-->JAYA-442407876.ap-south-1.elb.amazonaws.com--->copy and put chrome text box

The screenshot shows a web browser window with the address bar displaying 'jaya-442407876.ap-south-1.elb.amazonaws.com'. The page content displays the message: 'Hi you are hitting linux1 instance'.

Refresh chrome---->shown linux2

The screenshot shows the same web browser window after a refresh. The page content now displays the message: 'Hi you are hitting linux2 instance'.

Finally elastic load balacer is work

