

CREATING THE LOAD BALANCER

A load balancer accepts incoming traffic from clients and routes requests to EC2 instances (Targets).

The load balancer also monitors the health of its registered targets and ensures that it routes traffic only to healthy targets.

When the load balancer detects an unhealthy target, it stops routing traffic to that target. It then resumes routing traffic to that target when it detects that the target is healthy again.

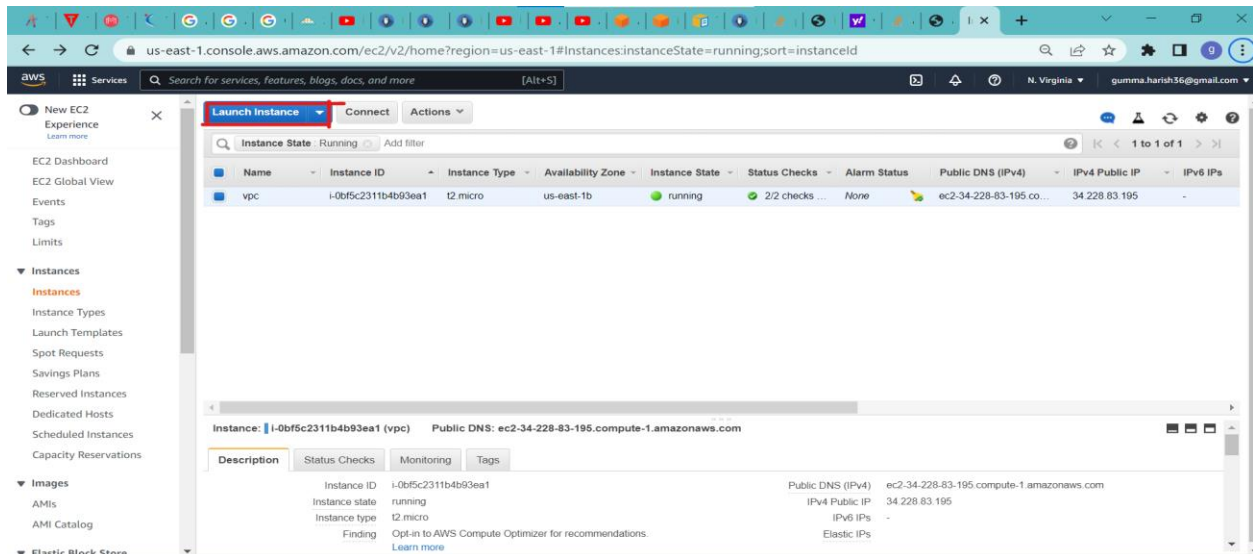
Step-1 Create Linux Machine

Launch instance --- Amazon Linux -- No of instances - 1 --- Name Tag- Lin-1 --- Security Group - LinSG09

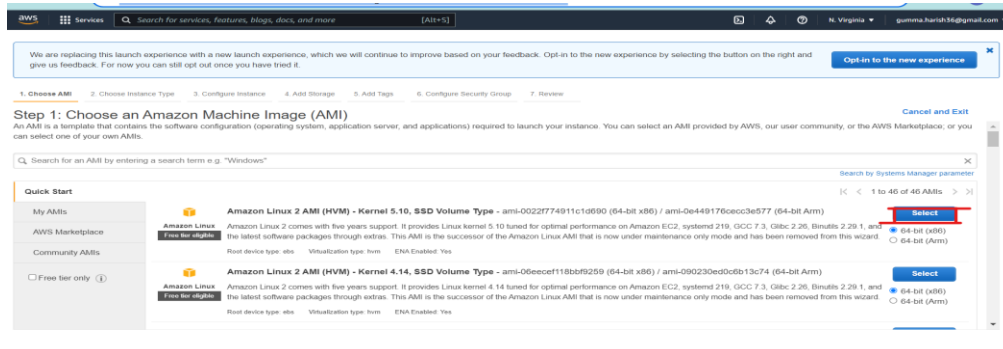
Description – LinSG

Add Rule

HTTP



Choose machine image



Choose an instance type

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.micro (1 ECUs, 1 vCPUs, 2.5 GHz, ~, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 GigaBit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Configure instance details

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances 1 Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network vpc-09f7ad00b450f1906 (default) Create new VPC

Subnet No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP Use subnet setting (Enable)

Hostname type Use subnet setting (IP name)

DNS Hostname ☒ Enable IP name (A record) DNS requests ☒ Enable resource-based IP-v4 (A record) DNS requests ☐ Enable resource-based IP-v6 (AAAA record) DNS requests

Placement group ☐ Add instance to placement group

Capacity Reservation Open

Domain join directory No directory Create new directory

IAM role None Create new IAM role

Cancel Previous Review and Launch Next: Add Storage

Add storage

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MiB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-08cbb15f1c8eb5387	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GiB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

Add file system

Cancel Previous Review and Launch Next: Add Tags

No need to add the tags

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces
This resource currently has no tags.				
Choose the Add tag button or click to add a new tag.				
Make sure your IAM policy includes permissions to create tags.				

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Configure security group

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

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

Security group name:
Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

[Add Rule](#)

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review and Launch](#)

Add the HTTP port

Review instance launch

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, LinSG17, is open to the world.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.

You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details [Edit AMI](#)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-0022f77491c1d690

Free tier eligible: Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is n...
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security group name	Description
LinSG17	LinSG09

[Cancel](#) [Previous](#) [Launch](#)

First create a new key pair and download the key pair .after downloading the key pair than we need to launch the instance

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more](#) about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair type: ☒ RSA ☐ ED25519


[Download Key Pair](#)

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

[Cancel](#) [Launch Instances](#)

Launch status

Launch Status

 **Get notified of estimated charges**
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

▼ Here are some helpful resources to get you started

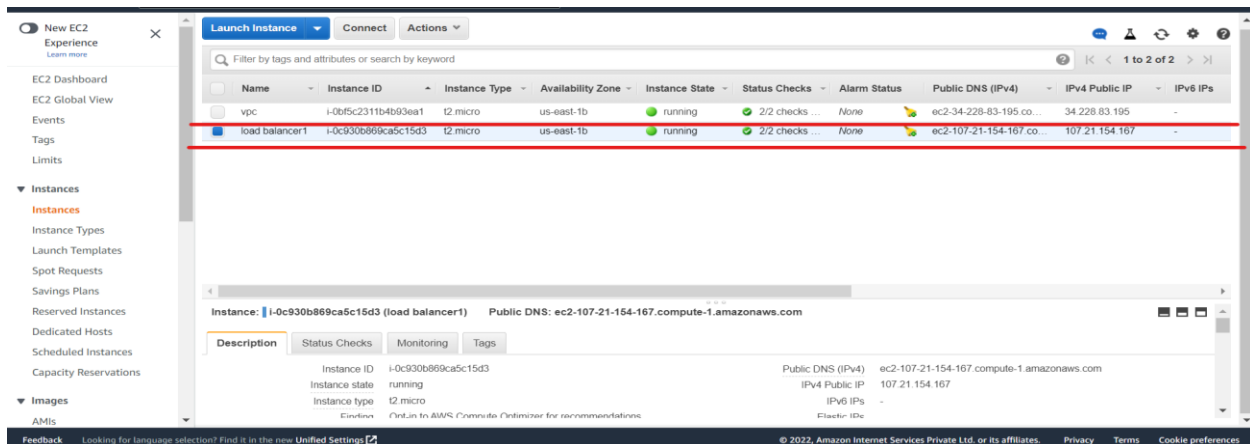
- [How to connect to your Linux instance](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: User Guide](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

View instances

Now new instance had launched (with the name of load balancer1)



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
vpc	i-0b5c2311b4b93ea1	t2.micro	us-east-1b	running	2/2 checks ...	None	ec2-34-228-83-195.co...	34.228.83.195	-
load balancer1	i-0c930b869ca5c15d3	t2.micro	us-east-1b	running	2/2 checks ...	None	ec2-107-21-154-167.co...	107.21.154.167	-

Instance: **i-0c930b869ca5c15d3 (load balancer1)** Public DNS: **ec2-107-21-154-167.compute-1.amazonaws.com**

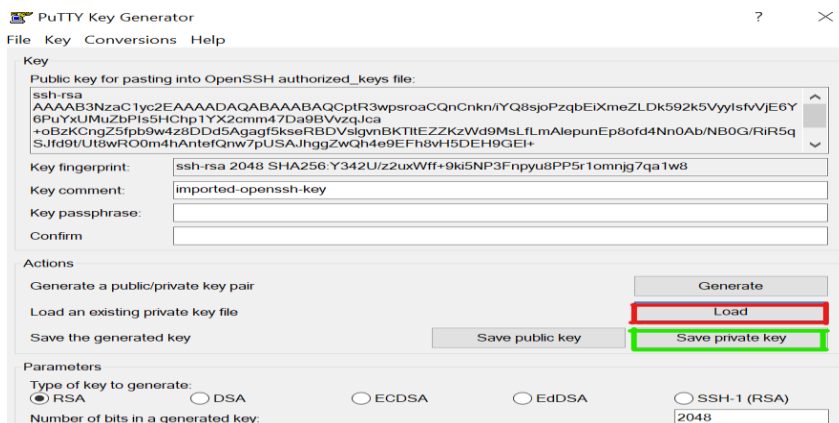
Description	Status Checks	Monitoring	Tags
Instance ID	i-0c930b869ca5c15d3		
Instance state	running		
Instance type	t2.micro		
Elavtion			
OnLin In AWS			
Consume Onlinizer for recommendations			
Public DNS (IPv4)	ec2-107-21-154-167.compute-1.amazonaws.com		
IPv4 Public IP	107.21.154.167		
IPv6 IPs	-		
Elastic IPs			

Step-2

Convert pem into ppk file

Using the puttygen we can convert the pem file into ppk file

- First load the pem file into the putty gen
- After loading the file we need to save the ppk file



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCApIR3wpsroaCQnCkn/iYQ8sjoPzqbEIXmeZLDk592k5VyyIsfVJ/E6Y6PUYXUMuZbPisSHChp1YX2cmmp47Da9BVzqJca+oBzKCngZ5fpb9w4z8DDd5Agagf5kseRBDVslgynBKTITEZZKzWd9MsLflmAlepunEp8ofd4Nn0Ab/NB0G/RIR5qS.Jfd9t/Ul8wROm4hAntefQnw7pUSA.JhggZwQh4e9EFh8vH5DEH9GEI+
```

Key comment: imported-openssh-key

Actions

Generate a public/private key pair **Generate**

Load an existing private key file **Load**

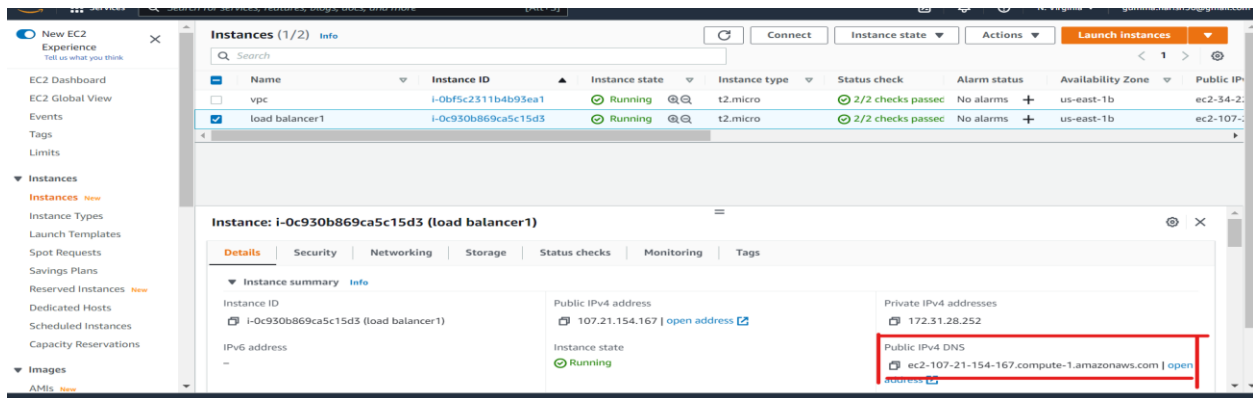
Save the generated key **Save private key**

Parameters

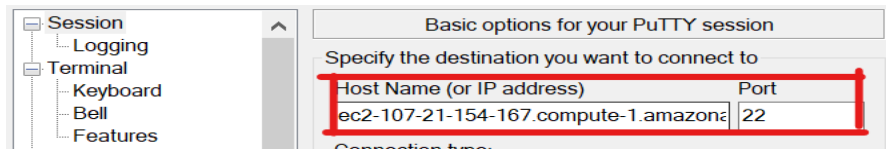
Type of key to generate: ☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

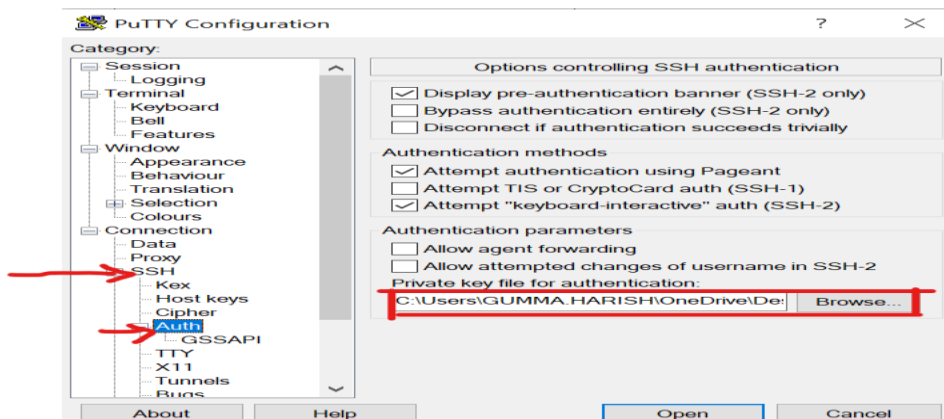
Now access the machine



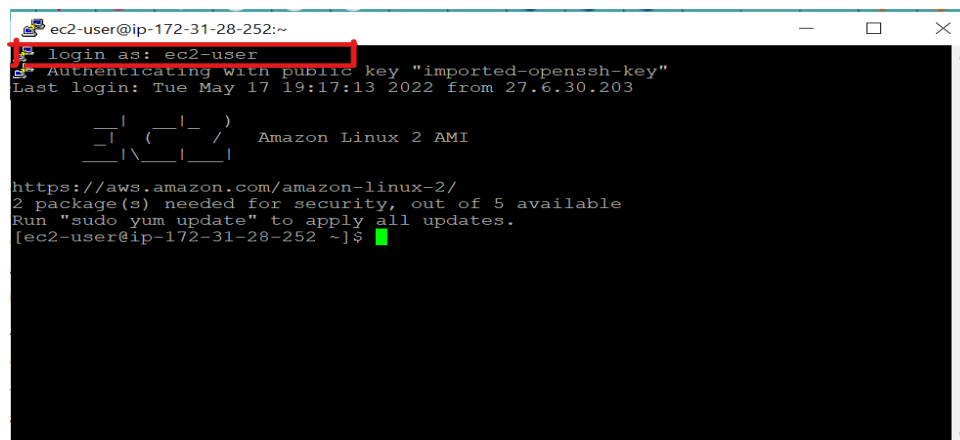
- Take the public DNS and paste into putty
- Open the putty under hostname we need add the public DNS of the instance



Now SSH under auth and browse for the ppk file (putty need the ppk file)



After open putty we will get the ec2 terminal . we need to login with the ec2-user



Step 4: Run the commands to install web package

```
sudo su
```

```
yum update -y
```

```
yum install httpd -y
```

```
cd /var/www/html
```

```
echo "MyGoogle-1" > index.html
```

```
ls
```

```
service httpd start
```

```
chkconfig httpd on
```

1.sudo -i

```
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-172-31-28-252 ~]$ sudo su  
[root@ip-172-31-28-252 ec2-user]# sudo -i  
[root@ip-172-31-28-252 ~]#
```

2.yum update -y

```
Installed:  
kernel.x86_64 0:5.10.112-108.499.amzn2  
  
Updated:  
curl.x86_64 0:7.79.1-2.amzn2.0.1  
iproute.x86_64 0:5.10.0-2.amzn2.0.2  
kernel-tools.x86_64 0:5.10.112-108.499.amzn2  
libcurl.x86_64 0:7.79.1-2.amzn2.0.1
```

3. yum install httpd -y

Output

```
Installed:  
httpd.x86_64 0:2.4.53-1.amzn2  
  
Dependency Installed:  
apr.x86_64 0:1.7.0-9.amzn2  
apr-util.x86_64 0:1.6.1-5.amzn2.0.2  
apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2  
generic-logos-httpd.noarch 0:18.0.0-4.amzn2  
httpd-filesystem.noarch 0:2.4.53-1.amzn2  
httpd-tools.x86_64 0:2.4.53-1.amzn2  
mailcap.noarch 0:2.1.41-2.amzn2  
mod_http2.x86_64 0:1.15.19-1.amzn2.0.1
```

4.cd /var/www/html

```
[root@ip-172-31-28-252 ~]# cd /var/www/html  
[root@ip-172-31-28-252 html]#
```

5. echo "MyGoogle-1" > index.html

```
[root@ip-172-31-28-252 html]# echo "MYGOOGLE-1" > index.html
```

6.ls

```
[root@ip-172-31-28-252 html]#  
[root@ip-172-31-28-252 html]# ls  
index.html  
[root@ip-172-31-28-252 html]#  
[root@ip-172-31-28-252 html]#  
[root@ip-172-31-28-252 html]# cat index.html  
MYGOOGLE-1  
[root@ip-172-31-28-252 html]#
```

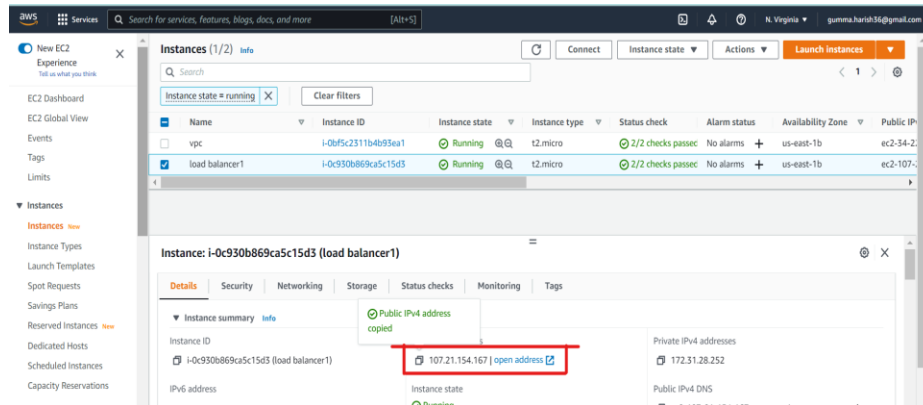
7. service httpd start

8. chkconfig httpd on

```
MYGOOGLE-I
[root@ip-172-31-28-252 html]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-28-252 html]# chkconfig httpd on
Note: Forwarding request to 'systemctl enable httpd.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@ip-172-31-28-252 html]#
```

Step-5 Now take the public ip and paste into the browser

Access the webserver by using public_ip

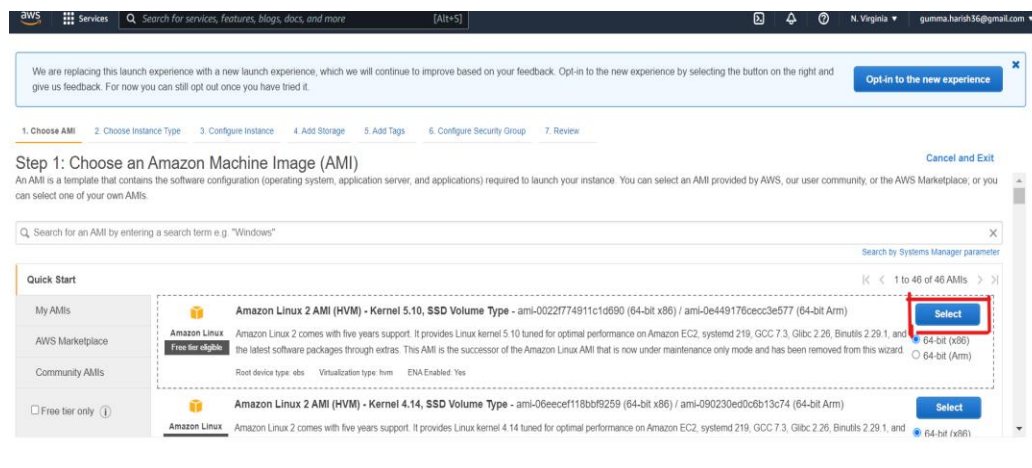


Output and final result



Steps-6

Create a one more instance



Choose an instance type

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All Instance families Current generation Show/Hide Columns

Currently selected: t2.micro (1 ECUs, 1 vCPU, 2.5 GHz, ~1 GB memory, EBS only)

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
t2	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Configure instance details

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: ☐ Request Spot instances

Network: vpc-09f7ab90b450f1906 (default) Create new VPC

Subnet: No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP: ☐ Use subnet setting (Enable)

Hostname type: Use subnet setting (IP name)

DNS Hostname: ☐ Enable IP name (A record) DNS requests
☒ Enable resource-based IPv4 (A record) DNS requests
☐ Enable resource-based IPv6 (AAAA record) DNS requests

Placement group: ☐ Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory Create new directory

IAM role: None Create new IAM role

Cancel Previous Review and Launch Next: Add Storage

Add storage

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MiB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-0f1cbb15f1cbb5387	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

Add file system

Cancel Previous Review and Launch Next: Add Tags

No need to add the tags

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces
This resource currently has no tags.				
Choose the Add tag button or click to add a Name tag.				
Make sure your IAM policy includes permissions to create tags.				

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Configure security Group

We need to select the existing security group (use the previous security group what we used for the above instance)

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

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

Security Group ID	Name	Description	Actions
sg-0340cb7878da701a7	default	default VPC security group	Copy to new
sg-0dccb7ba2fc95535b	launch-wizard-1	launch-wizard-1 created 2022-05-04T17:42:41.699+05:30	Copy to new
sg-0f5ce591137f0131	launch-wizard-10	launch-wizard-10 created 2022-05-07T23:32:06.480+05:30	Copy to new
sg-04046baf0bee0ddfe	launch-wizard-11	launch-wizard-11 created 2022-05-07T23:33:00.224+05:30	Copy to new
sg-00945fd1b3df523ef	launch-wizard-12	launch-wizard-12 created 2022-05-08T18:06:46.543+05:30	Copy to new

Inbound rules for sg-0783ce93f3841a5fd

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	:::0	
SSH	TCP	22	0.0.0.0/0	

[Cancel](#) [Previous](#) [Review and Launch](#)

Review instance launch

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, LinSG17, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details [Edit AMI](#)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-0022f774911c1d690
Free tier eligible
Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.
This AMI is the successor of the Amazon Linux AMI that is n...
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security group name	Description
LinSG17	LinSG17

[Cancel](#) [Previous](#) [Launch](#)

Now select the existing key pair and launch the instance

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

Choose an existing key pair

Select a key pair

good | RSA

☒ I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

[Cancel](#) [Launch Instances](#)

Launch status

Launch Status



Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

Here are some helpful resources to get you started

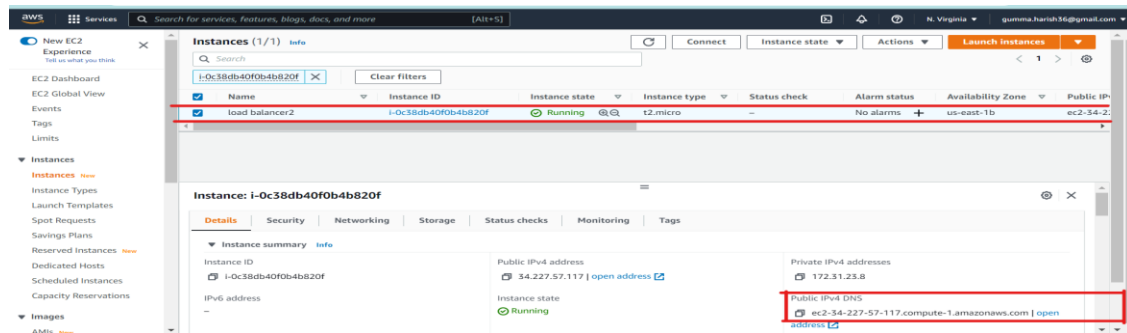
- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

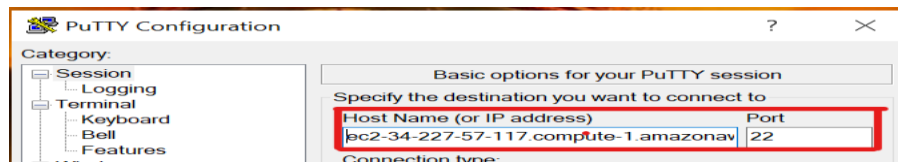
- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

[View instances](#)

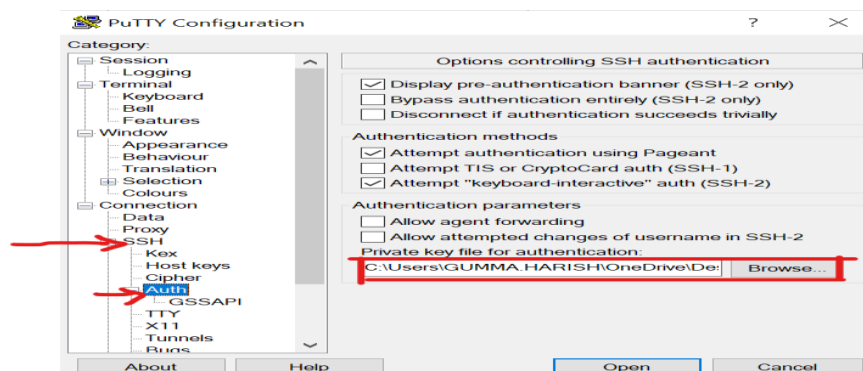
Now new instance had launched (with the name of load balancer2)



- Take the public DNS and paste into putty
- Open the putty under hostname we need add the public DNS of the instance



Now SSH under auth and browse for the pkc file (putty need the pkc file)



After open putty we will get the ec2 terminal . we need to login with the **ec2-user**

```

  _ | ( _ | _ )
  _ | ( _ | _ /
  _ | \ _ | _ |
                                     Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 5 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-23-8 ~]$
```

Step 7: Run the commands to install web package

```
sudo su
```

```
yum update -y
```

```
yum install httpd -y
```

```
cd /var/www/html
```

```
echo "MyGoogle-2" > index.html
```

Is

```
service httpd start
```

```
chkconfig httpd on
```

1.sudo su

2. yum update -y

```

https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 5 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-23-8 ~]$ sudo su
[root@ip-172-31-23-8 ec2-user]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core

```

```

Installed:
  kernel.x86_64 0:5.10.112-108.499.amzn2

Updated:
  curl.x86_64 0:7.79.1-2.amzn2.0.1      iproute.x86_64 0:5.10.0-2.amzn2.0.2      kernel-tools.x86_64 0:5.10.112-108.499.amzn2      libcurl.x86_64 0:7.79.1-2.amzn2.0.1

Complete!
  
```

3.yum install httpd -y

```
[root@ip-172-31-23-8 ec2-user]# yum install httpd -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
Resolving Dependencies
--> Running transaction check
--> Package httpd.x86_64 0:2.4.53-1.amzn2 will be installed
--> Processing Dependency: httpd-tools = 2.4.53-1.amzn2 for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: httpd-filesystem = 2.4.53-1.amzn2 for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: system-logos-httpd for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: mod_http2 for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: httpd-filesystem for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: /etc/mime.types for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: libaprutil-1.so.0()(64bit) for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: libapr-1.so.0()(64bit) for package: httpd-2.4.53-1.amzn2.x86_64
--> Running transaction check
--> Package apr.x86_64 0:1.7.0-9.amzn2 will be installed
--> Package apr-util.x86_64 0:1.6.1-5.amzn2.0.2 will be installed
```

```
4.cd /var/www/html
```

```
[root@ip-172-31-23-8 ~]#  
[root@ip-172-31-23-8 ~]# cd /var/www/html  
[root@ip-172-31-23-8 html]#
```

5. echo "MyGoogle-2" > index.html

```
[root@ip-172-31-23-8 html]# echo "MYGoogle-2" >index.html
```

6.ls

```
[root@ip-172-31-23-8 html]# ls
index.html
```

7.service httpd start

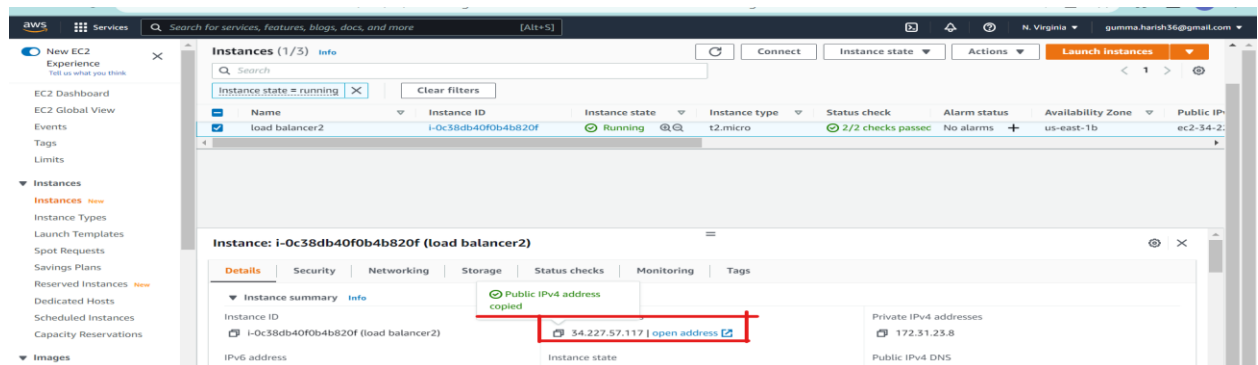
```
[root@ip-172-31-23-8 html]# service httpd start
Redirecting to /bin/systemctl start httpd.service
```

8.chkconfig httpd on

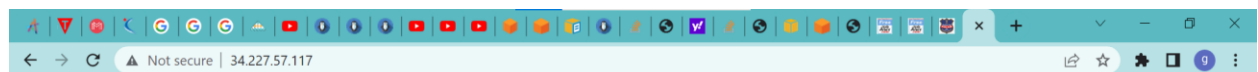
```
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-23-8 html]# chkconfig httpd on
Note: Forwarding request to 'systemctl enable httpd.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@ip-172-31-23-8 html]#
```

Step -9 Now take the public ip and paste into the browser

Access the webserver by using public_ip



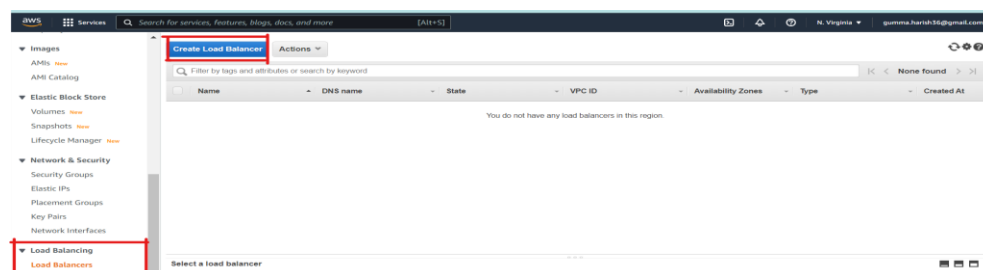
Final out put



MYGoogle-2

Step-10 : Create load balancers

Select classic load balancer



Select the classic load balancer

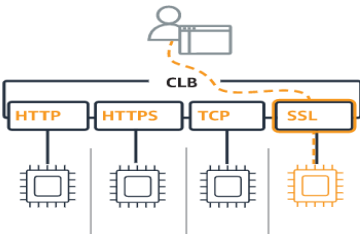
▼ Classic Load Balancer - previous generation

Classic Load Balancer [Info](#)

Choose a Classic Load Balancer when you have an existing application running in the EC2-Classic network.

ⓘ AWS will be retiring the EC2-Classic network on August 15, 2022. [Learn more](#)

Create



Step-11

Load Balancer Name - Myload--> Next ----> select existing security group ---> NEXT --

Define load balancer

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 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name:

Create LB inside:

Create an internal load balancer: ☐ (what's this?)

Enable advanced VPC configuration: ☐

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

Add

Cancel Next: Assign Security Groups

Assign security groups

(select the existing security group which we used for instances)

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 this load balancer. This can be changed at any time.

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

Security Group ID	Name	Description	Actions
sg-0340ba7878da701a7	default	default VPC security group	Copy to new
sg-0d0c07ba2b956358a	launch-vizcard-1	launch-vizcard-1 created 2022-05-04T17:42:41.699+05:30	Copy to new
sg-0f5ca5911379131	launch-vizcard-10	launch-vizcard-10 created 2022-05-07T23:32:08.400+05:30	Copy to new
sg-04040a0c5a0e0d9e	launch-vizcard-11	launch-vizcard-11 created 2022-05-07T23:32:08.224+05:30	Copy to new
sg-009450103d0523ef	launch-vizcard-12	launch-vizcard-12 created 2022-05-08T18:06:46.543+05:30	Copy to new
sg-0ba799f7110e6d9f	launch-vizcard-13	launch-vizcard-13 created 2022-05-08T18:07:45.405+05:30	Copy to new
sg-02c5a074309d3329a	launch-vizcard-14	launch-vizcard-14 created 2022-05-08T23:06:20.210+05:30	Copy to new
sg-09ca07d0eac2291f	launch-vizcard-15	launch-vizcard-15 created 2022-05-10T19:23:19.900+05:30	Copy to new
sg-0240503b0153a0577	launch-vizcard-16	launch-vizcard-16 created 2022-05-10T23:58:08.270+05:30	Copy to new
sg-008a6d087363a759	launch-vizcard-17	launch-vizcard-17 created 2022-05-11T23:47:36.825+05:30	Copy to new
sg-0004ee0510924c08	launch-vizcard-18	launch-vizcard-18 created 2022-05-11T23:54:13.910+05:30	Copy to new
sg-09a91a15a918d046a	launch-vizcard-19	launch-vizcard-19 created 2022-05-12T11:52:35.396+05:30	Copy to new
sg-074a5d0b01190d0c37	launch-vizcard-2	launch-vizcard-2 created 2022-05-04T20:29:30.229+05:30	Copy to new
sg-065d5420505a0ca0	launch-vizcard-3	launch-vizcard-3 created 2022-05-05T12:50:36.996+05:30	Copy to new
sg-02f024b01a55670f	launch-vizcard-4	launch-vizcard-4 created 2022-05-05T13:00:53.882+05:30	Copy to new
sg-0c30ba791a90a12	launch-vizcard-5	launch-vizcard-5 created 2022-05-05T22:29:45.573+05:30	Copy to new
sg-02a0a0f0b0ba0312	launch-vizcard-6	launch-vizcard-6 created 2022-05-07T22:50:03.943+05:30	Copy to new
sg-00508a0505a05a44	launch-vizcard-7	launch-vizcard-7 created 2022-05-07T22:56:25.405+05:30	Copy to new
sg-0e01aac0001603c0	launch-vizcard-8	launch-vizcard-8 created 2022-05-07T22:57:25.290+05:30	Copy to new
sg-0a000a000a000a00	launch-vizcard-9	launch-vizcard-9 created 2022-05-08T23:44:03.200+05:30	Copy to new
sg-0730a00700a1a08	LRSG17	LRSG09	Copy to new

Cancel Previous Next: Configure Security Settings

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: 2 seconds
Interval: 5 seconds
Unhealthy threshold: 2
Healthy threshold: 2

Cancel Previous **Next: Add EC2 Instances**

Response Timeout - 2 Seconds

Interval - 5 Seconds

Unhealthy threshold - 2

Healthy threshold - 2

Next -- Attach both the instances

Add EC2 instances (what we created)

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-09f7ab90b450f1906 (172.31.0.0/16)

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR	
<input type="checkbox"/>	i-0bf5c2311b4b93ea1	vpc	running	launch-wizard-19	us-east-1b	subnet-0a4d3f1...	172.31.16.0/20
<input checked="" type="checkbox"/>	i-0c930b869ca5c15d3	load balancer1	running	LinSG17	us-east-1b	subnet-0a4d3f1...	172.31.16.0/20
<input checked="" type="checkbox"/>	i-0c38db40f0b4b820f	load balancer2	running	LinSG17	us-east-1b	subnet-0a4d3f1...	172.31.16.0/20

Availability Zone Distribution
2 instances in us-east-1b

☒ Enable Cross-Zone Load Balancing
☒ Enable Connection Draining: 300 seconds

Cancel Previous **Next: Add Tags**

Review

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 7: Review

Please review the load balancer details before continuing

Define Load Balancer [Edit load balancer definition](#)

Load Balancer name: myload
Scheme: internet-facing
Port Configuration: 80 (HTTP) forwarding to 80 (HTTP)

Configure Health Check [Edit health check](#)

Ping Target: HTTP:80/index.html
Timeout: 2 seconds
Interval: 5 seconds
Unhealthy threshold: 2
Healthy threshold: 2

Add EC2 Instances [Edit instances](#)

Cross-zone load balancing: Enabled
Connection Draining: Enabled, 300 seconds
Instances: i-0c930b869ca5c15d3 (load balancer1), i-0c38db40f0b4b820f (load balancer2)

VPC Information [Edit subnets](#)

VPC: vpc-09f7ab90b450f1906
Subnets: subnet-0a4d3f17099ef2ed4, subnet-0934ce2b40d835c8d, subnet-0654ef8d2ee23b066, subnet-0a83c6bd19fc39979, subnet-09a0030b0cb7a28b8, subnet-026a0e52ce62d9548

Cancel Previous **Create**

Load Balancer Creation Status

Load Balancer Creation Status



Successfully created load balancer

Load balancer **myload** was successfully created.

Note: It may take a few minutes for your instances to become active in the new load balancer.

Close

Name	DNS name	State	VPC ID	Availability Zones	Type	Created At
myload	myload-2070105061.us-east-1.elb.amazonaws.com	Available	vpc-097ab90b450f1906	us-east-1f, us-east-1e, ...	classic	May 18, 2022 at 10:10 AM

Step-12

Access the load balance by using DNS

and experience the load balancer.

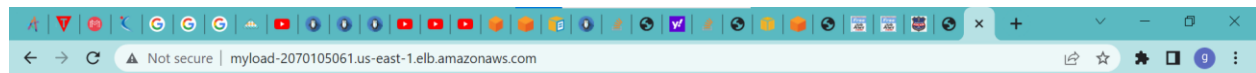
Take the DNS of load balancer

Using the load balancer DNS we are getting the content

The main aim of the load balancer If one server is down, it should redirect the traffic to another server.

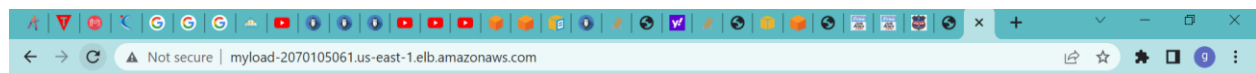
Now load balance will start sending the traffic

Load balancer will also monitor the health checks of ec2 instances



MYGOOGLE-1

Same DNS we are getting different content because load balancer will distribut the traffic .if one server goes download it automatically route the traffic to another server



MYGoogle-2