

Line Balancing :

Create 2 Instances (select Linux as OS)

aws

Services

Resource Groups

nikigear

Mumbai

Support

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Add Tags

6. Configure Security Group

7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

Search by Systems Manager parameter

Quick Start

1 to 40 of 40 AMIs

My AMIs

AWS Marketplace

Community AMIs

☐ Free tier only

Amazon Linux

Free tier eligible

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0ebc1ac48dfd14136 (64-bit x86) / ami-0d17d97232c08403e (64-bit Arm)

64-bit (x86)

64-bit (Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 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.

Root device type: ebs

Virtualization type: hvm

ENA Enabled: Yes

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 types

Current generation

Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

Services

Resource Groups

★

nikigeared

Mumbai

Support

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

2

Launch into Auto Scaling Group

You may want to consider launching these instances into an Auto Scaling Group to help you maintain application availability and for easy scaling in the future. [Learn how Auto Scaling can help your application stay healthy and cost effective.](#)

Purchasing option

☐ Request Spot instances

Network

vpc-6cba5d07 (default)

Create new VPC

Subnet

No preference (default subnet in any Availability Zone)

Create new subnet

Auto-assign Public IP

Enable

Placement group

☐ Add instance to placement group

Capacity Reservation

Open

IAM role

None

Create new IAM role

Shutdown behavior

Stop

Stop - Hibernate behavior

☐ Enable hibernation as an additional stop behavior

Enable termination protection

☐ Protect against accidental termination

Monitoring

☐ Enable CloudWatch detailed monitoring

Additional charges apply.

Tenancy

Shared - Run a shared hardware instance

Additional charges will apply for dedicated tenancy

Services

Resource Groups

★

nikigeared

Mumbai

Support

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 (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-08d68946ad0e25c23	30	General Purpose S	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypt

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.

aws

Services ▾Resource Groups ▾🔖

🔔nikigeared ▾Mumbai ▾Support ▾

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. 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 name:

Description:

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ	
<div>All traffic ▾</div>	<div>All</div>	<div>0 - 65535</div>	<div>Anywhere ▾</div>	<div>0.0.0.0/0, ::/0</div>	<div>e.g. SSH for Admin Desktop</div>

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.

Create Load Balancer

Actions ▾

🔍 Filter by tags and attributes or search by keyword

☐

Name

▲

DNS name

▼ Load Balancing

Load Balancers

Target Groups New

Select load balancer type

Elastic Load Balancing supports three types of load balancers: Application Load Balancers, Network Load Balancers (new), and Classic Load Balancers. Choose the load balancer type that meets your needs. [Learn more about which load balancer is right for you](#)

Application Load Balancer

HTTP
HTTPS

Create

Choose an Application Load Balancer when you need a flexible feature set for your web applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

[Learn more >](#)

Network Load Balancer

TCP
TLS
UDP

Create

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

[Learn more >](#)

Classic Load Balancer

PREVIOUS GENERATION
for HTTP, HTTPS, and TCP

Create

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

[Learn more >](#)

1. Configure Load Balancer

2. Configure Security Settings

3. Configure Security Groups

4. Configure Routing

5. Register Targets

6. Review

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network.

Name ⓘ

niklb-2020

⚠ Load balancer names must contain only alphanumeric characters or hyphens, and must not start or end with a hyphen.

Scheme ⓘ

☒ Internet-facing
☐ Internal

IP address type ⓘ

ipv4

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
HTTP	80

Add listener

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You must specify at least two Availability Zones for your load balancer.

VPC ⓘ

vpc-6cba5d07 (172.31.0.0/16) (default)

Availability Zones

☒ ap-south-1a

subnet-f929f91

IPv4 address ⓘ

Assigned by AWS

☒ ap-south-1b

subnet-f7b5c7bb

IPv4 address ⓘ

Assigned by AWS

☐ ap-south-1c

subnet-53961228

aws

Services

Resource Groups

nikigeared

Mu

1. Configure Load Balancer

2. Configure Security Settings

3. Configure Security Groups

4. Configure Routing

5. Register Targets

Step 3: Configure Security Groups

A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to your load balancer. First, decide whether to create a new security group or select an existing one.

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

Security Group ID	Name	Description
<input checked="" type="checkbox"/> sg-748d1f10	default	default VPC security group
<input type="checkbox"/> sg-0dbf9866774d505c9	launch-wizard-1	launch-wizard-1 created 2020-08-21T11:37:23.390+05:30
<input type="checkbox"/> sg-04ebb9d09e2a089f7	launch-wizard-2	launch-wizard-2 created 2020-08-21T14:41:49.301+05:30
<input type="checkbox"/> sg-061bc9987036aabb5	launch-wizard-3	launch-wizard-3 created 2020-08-21T14:49:39.062+05:30
<input type="checkbox"/> sg-064064e8c4c814d3e	launch-wizard-4	launch-wizard-4 created 2020-08-21T15:43:39.699+05:30
<input type="checkbox"/> sg-0d5fcc01281c38913	launch-wizard-5	launch-wizard-5 created 2020-08-21T15:48:00.775+05:30
<input type="checkbox"/> sg-0242dd371d16a8348	launch-wizard-6	launch-wizard-6 created 2020-08-22T17:55:57.155+05:30
<input type="checkbox"/> sg-01ce1a6867b479977	launch-wizard-7	launch-wizard-7 created 2020-08-23T22:56:10.823+05:30

1. Configure Load Balancer

2. Configure Security Settings

3. Configure Security Groups

4. Configure Routing

5. Register Targets

6. Review

Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health checks.

Target group

Target group ⓘ

New target group

Name ⓘ

new-loc

⚠ You already have a target group with this name in this region.

Target type

☒ Instance
☐ IP
☐ Lambda function

Protocol ⓘ

HTTP

Port ⓘ

80

Health checks

Protocol ⓘ

HTTP

Path ⓘ

/

▶ Advanced health check settings

1. Configure Load Balancer2. Configure Security Settings3. Configure Security Groups4. Configure Routing5. Register Targets6. Review

Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

To deregister instances, select one or more registered instances and then click Remove.

Remove

<input type="checkbox"/>	Instance	Name	Port	State	Security groups	Zone
No instances available.						

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered

 on port

Q Search Instances

X

<input type="checkbox"/>	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-0fb5277ae3e61a36f		running	launch-wizard-8	ap-south-1a	subnet-f9929f91	172.31.32.0/20
<input checked="" type="checkbox"/>	i-0060ce27db6e22c79		running	launch-wizard-8	ap-south-1a	subnet-f9929f91	172.31.32.0/20

1. Configure Load Balancer2. Configure Security Settings3. Configure Security Groups4. Configure Routing5. Register Targets6. Review

Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

To deregister instances, select one or more registered instances and then click Remove.

Remove

<input type="checkbox"/>	Instance	Name	Port	State	Security groups	Zone
<input type="checkbox"/>	i-0fb5277ae3e61a36f		80	running	launch-wizard-8	ap-south-1a
<input type="checkbox"/>	i-0060ce27db6e22c79		80	running	launch-wizard-8	ap-south-1a

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered

 on port

Q Search Instances

X

<input type="checkbox"/>	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-0fb5277ae3e61a36f		running	launch-wizard-8	ap-south-1a	subnet-f9929f91	172.31.32.0/20
<input checked="" type="checkbox"/>	i-0060ce27db6e22c79		running	launch-wizard-8	ap-south-1a	subnet-f9929f91	172.31.32.0/20

1. Configure Load Balancer2. Configure Security Settings3. Configure Security Groups4. Configure Routing5. Register Targets6. Review

Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

To deregister instances, select one or more registered instances and then click Remove.

Remove

<input type="checkbox"/>	Instance	Name	Port	State	Security groups	Zone
<input type="checkbox"/>	i-03ed461cad1f80b01	linux1	80	running	launch-wizard-7	ap-south-1a
<input type="checkbox"/>	i-0512f10ba2f6d9362	linux2	80	running	launch-wizard-7	ap-south-1a

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered on port 80

Search Instances

<input type="checkbox"/>	Instance	Name	State	Security	Zone	Subnet ID	Subnet CIDR
<input type="checkbox"/>	i-03ed461ca...	linux1	running	launch-wizar...	ap-south-1a	subnet-f9929f91	172.31.32.0/20
<input type="checkbox"/>	i-0512f10ba...	linux2	running	launch-wizar...	ap-south-1a	subnet-f9929f91	172.31.32.0/20

aws

ServicesResource Groups

nikigearedMumbaiSupport

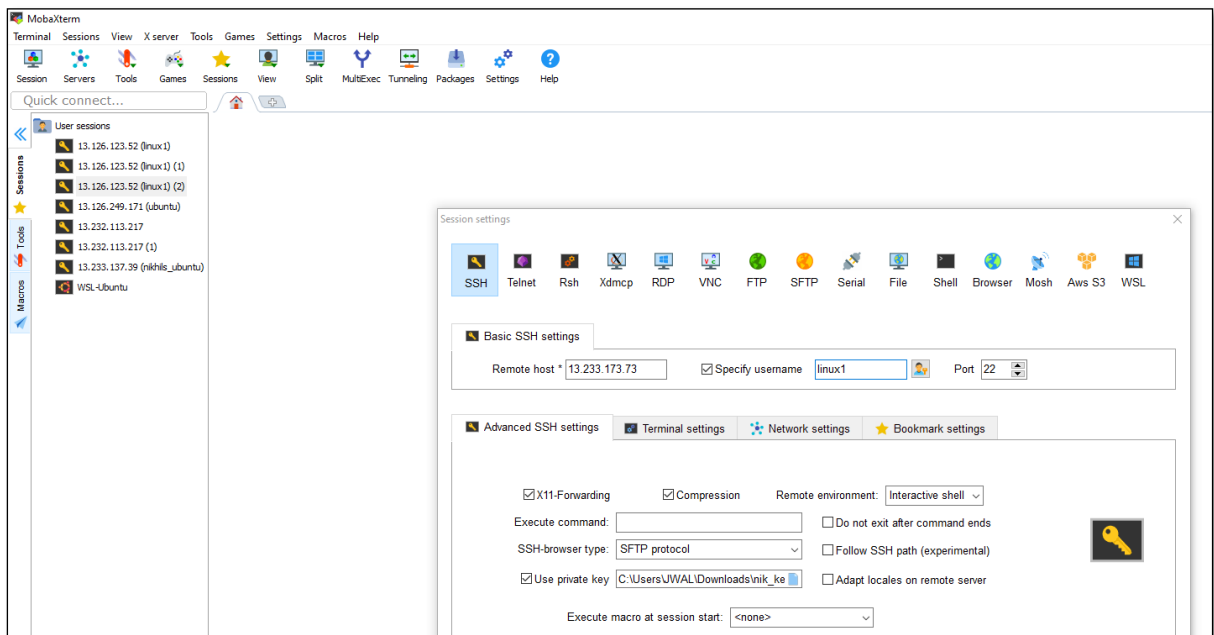
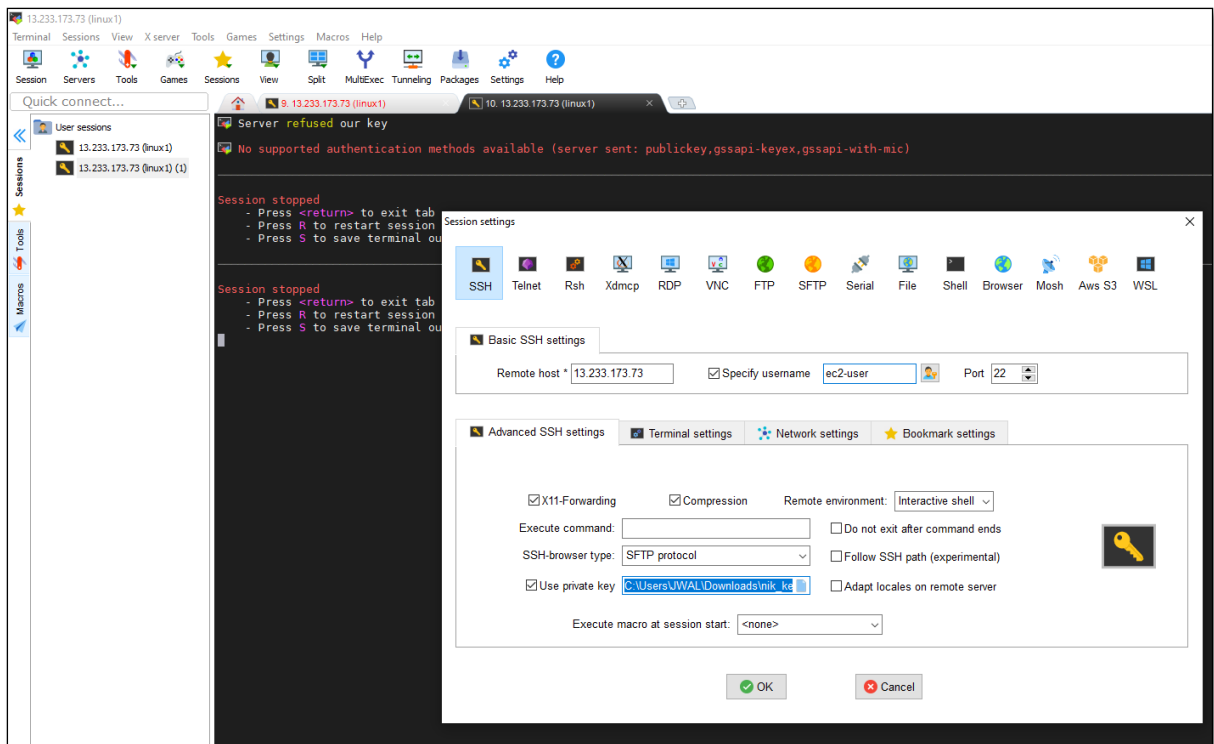
Load Balancer Creation Status

✔ Successfully created load balancer

Create Load Balancer Actions									
Filter by tags and attributes or search by keyword									
<input checked="" type="checkbox"/>	Name	DNS name	State	VPC ID	Availability Zones	Type	Created At	Monitoring	
<input checked="" type="checkbox"/>	nikib-2020	nikib-2020-924037793.ap-so...	active	vpc-6cba5d07	ap-south-1b, ap-south-1a	application	August 24, 2020 at 12:01:20 ...		

Configure the Instances:

Launch Instance Connect Actions									
Filter by tags and attributes or search by keyword									
<input type="checkbox"/>	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
<input type="checkbox"/>	linux1	i-0060ce27db6e22c79	t2.micro	ap-south-1a	running	2/2 checks ...	None	ec2-13-233-173-73.ap-...	13.233.173.73
<input type="checkbox"/>	linux2	i-0fb5277ae3e61a36f	t2.micro	ap-south-1a	running	2/2 checks ...	None	ec2-13-233-204-98.ap-...	13.233.204.98



Session settings

SSH

Telnet

Rsh

Xdmcp

RDP

VNC

FTP

SFTP

Serial

File

Shell

Browser

Mosh

Aws S3

WSL

Basic SSH settings

Remote host *13.126.123.52

☒ Specify usernamelinux1

Port22

Advanced SSH settings

Terminal settings

Network settings

Bookmark settings

☒ X11-Forwarding☒ CompressionRemote environment:Interactive shell

Execute command:

SSH-browser type:SFTP protocol

☒ Use private keyC:\Users\JWAL\Downloads\nikhils

☐ Do not exit after command ends

☐ Follow SSH path (experimental)

☐ Adapt locales on remote server

Execute macro at session start:<none>

OK

Cancel

Session settings

SSH

Telnet

Rsh

Xdmcp

RDP

VNC

FTP

SFTP

Serial

File

Shell

Browser

Mosh

Aws S3

WSL

Basic SSH settings

Remote host *13.233.204.98

☒ Specify usernameec2-user

Port22

Advanced SSH settings

Terminal settings

Network settings

Bookmark settings

☒ X11-Forwarding☒ CompressionRemote environment:Interactive shell

Execute command:

SSH-browser type:SFTP protocol

☒ Use private keyC:\Users\JWAL\Downloads\nik_ke

☐ Do not exit after command ends

☐ Follow SSH path (experimental)

☐ Adapt locales on remote server

Execute macro at session start:<none>

OK

Cancel

The screenshot shows a MobaXterm window with two tabs. The active tab is titled '12. 13.233.204.98'. The terminal displays the MobaXterm 20.3 logo and a list of SSH session details for an 'ec2-user' on '13.233.204.98'. The details include SSH compression (checked), SSH-browser (checked), X11-forwarding (disabled), and DISPLAY (192.168.10.9:0.0). Below this, there is a link to the MobaXterm website. The terminal then shows the Amazon Linux 2 AMI logo and a message about security updates, followed by a prompt for the user 'ec2-user' at 'ip-172-31-41-69'.

```
• MobaXterm 20.3 •
(SSh client, X-server and networking tools)

> SSH session to ec2-user@13.233.204.98
  • SSH compression : ✓
  • SSH-browser      : ✓
  • X11-forwarding   : ✗ (disabled or not supported by server)
  • DISPLAY          : 192.168.10.9:0.0

> For more info, ctrl+click on help or visit our website

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

https://aws.amazon.com/amazon-linux-2/
4 package(s) needed for security, out of 8 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-41-69 ~]$
```

Sudo su

yum install httpd

The screenshot shows a MobaXterm window with two tabs. The active tab is titled '11. 13.233.173.73 (ec2-user)'. The terminal displays the MobaXterm 20.3 logo and a list of SSH session details for an 'ec2-user' on '13.233.173.73'. The details include SSH compression (checked), SSH-browser (checked), X11-forwarding (disabled), and DISPLAY (192.168.10.9:0.0). Below this, there is a link to the MobaXterm website. The terminal then shows the Amazon Linux 2 AMI logo and a message about security updates. The user 'ec2-user' at 'ip-172-31-33-178' runs 'sudo su' to become root, and then runs 'yum install httpd'.

```
• MobaXterm 20.3 •
(SSh client, X-server and networking tools)

> SSH session to ec2-user@13.233.173.73
  • SSH compression : ✓
  • SSH-browser      : ✓
  • X11-forwarding   : ✗ (disabled or not supported by server)
  • DISPLAY          : 192.168.10.9:0.0

> For more info, ctrl+click on help or visit our website

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

https://aws.amazon.com/amazon-linux-2/
4 package(s) needed for security, out of 8 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-33-178 ~]$ sudo su
[root@ip-172-31-33-178 ec2-user]# yum install httpd
```

cd /var/www/html #cd –Change directory

pwd- #Print Working Directory

```
Complete!
[root@ip-172-31-33-178 ec2-user]# cd /var/www/html
[root@ip-172-31-33-178 html]# pwd
/var/www/html
[root@ip-172-31-33-178 html]# vi index.html
```

Vi index.html

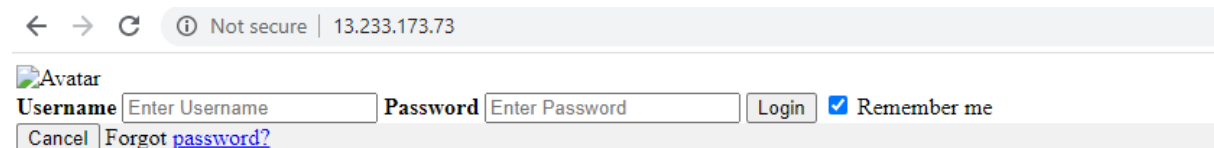
Press ‘i’ and this will be change into Insert Mode

Paste

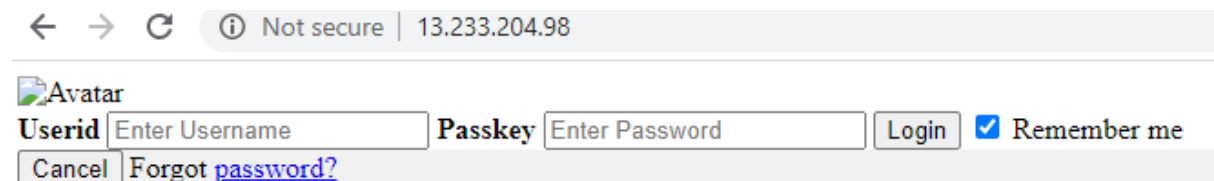
:wq

more index.html

service httpd start



Similarly do the Same for 2nd Machine and userid instead of user name and passkey instead of password



Load Balancers

Load balancer: **niklb-2020**

Description | Listeners | Monitoring | Integrated services | Tags

Basic Configuration

Name	niklb-2020
ARN	arn:aws:elasticloadbalancing:ap-south-1:211352697391:loadbalancer/app/niklb-2020/197107bfac2012af
DNS name	niklb-2020-924037793.ap-south-1.elb.amazonaws.com (A Record)
State	active
Type	application
Scheme	internet-facing
IP address type	ipv4

Filter by tags and attributes or search by keyword

1 to 1 of 1

Name	DNS name	State	VPC ID	Availability Zones	Type	Created At	Monitoring
niklb-2020	niklb-2020-924037793.ap-so...	active	vpc-6cba5d07	ap-south-1b, ap-south-1a	application	August 24, 2020 at 12:01:20 ...	

Load balancer: **niklb-2020**

Description | Listeners | Monitoring | Integrated services | Tags

CloudWatch alarms: No alarms configured [Create Alarm](#)

CloudWatch metrics: Showing data for: Last Hour

Below are your CloudWatch metrics for the selected resources (a maximum of 10). Click on a graph to see an expanded view. All times shown are in UTC. [View all CloudWatch metrics](#)

Target Response Time (Milliseconds)

Requests (Count)

Rule Evaluations (Count)

HTTP 5XXs (Count)

HTTP 4XXs (Count)

Target Groups

EC2 > Target groups > new-loc

new-loc [Delete](#)

arn:aws:elasticloadbalancing:ap-south-1:211352697391:targetgroup/new-loc/7cd0a5422afc6965

Basic configuration

Target type instance	Protocol : Port HTTP : 80	VPC vpc-6cba5d07	Load balancer niklb-2020
-------------------------	------------------------------	---------------------	-----------------------------

Group details | **Targets** | Monitoring | Tags

Registered targets (2)

[Deregister](#) [Register targets](#)

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Status	Status details
<input type="checkbox"/>	i-0060ce27db6e22c79	linux1	80	ap-south-1a	healthy	
<input type="checkbox"/>	i-0fb5277ae3e61a36f	linux2	80	ap-south-1a	healthy	