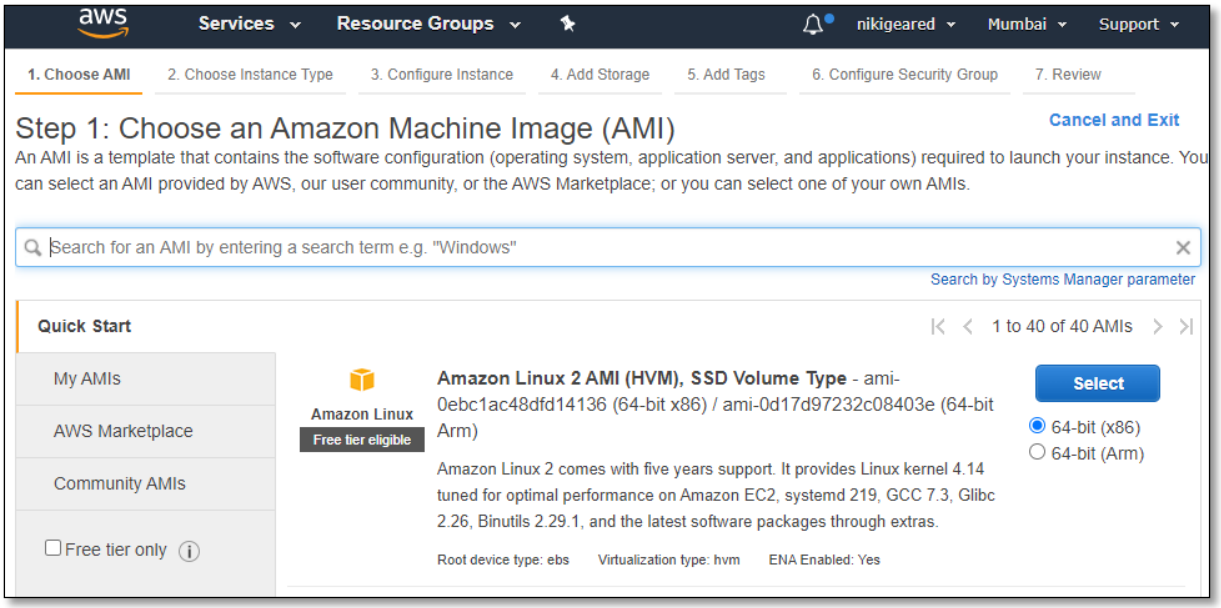
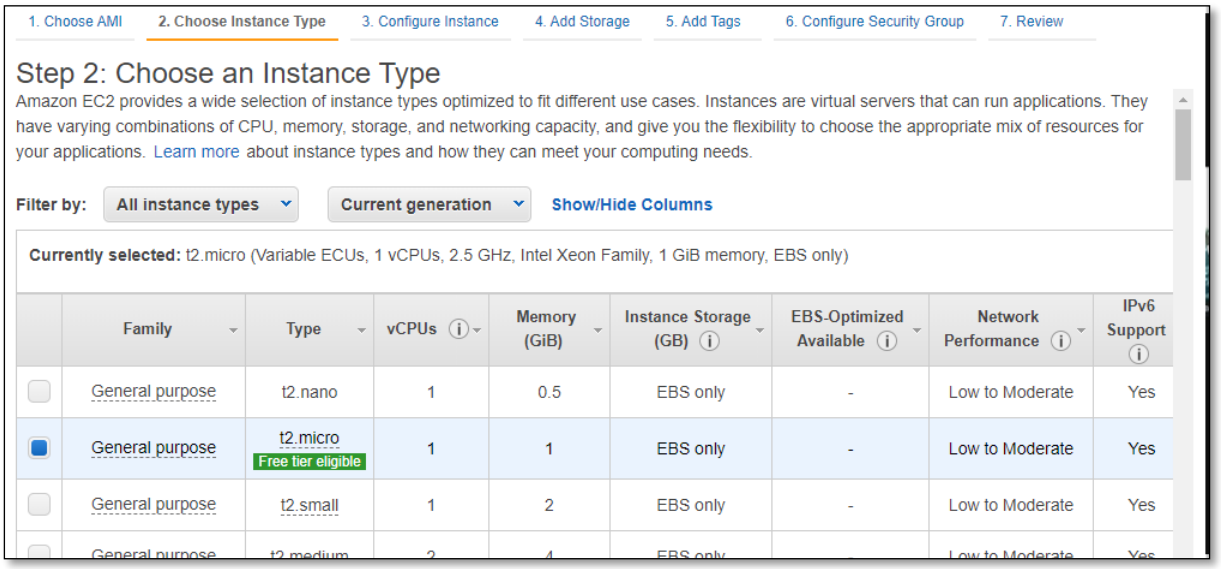
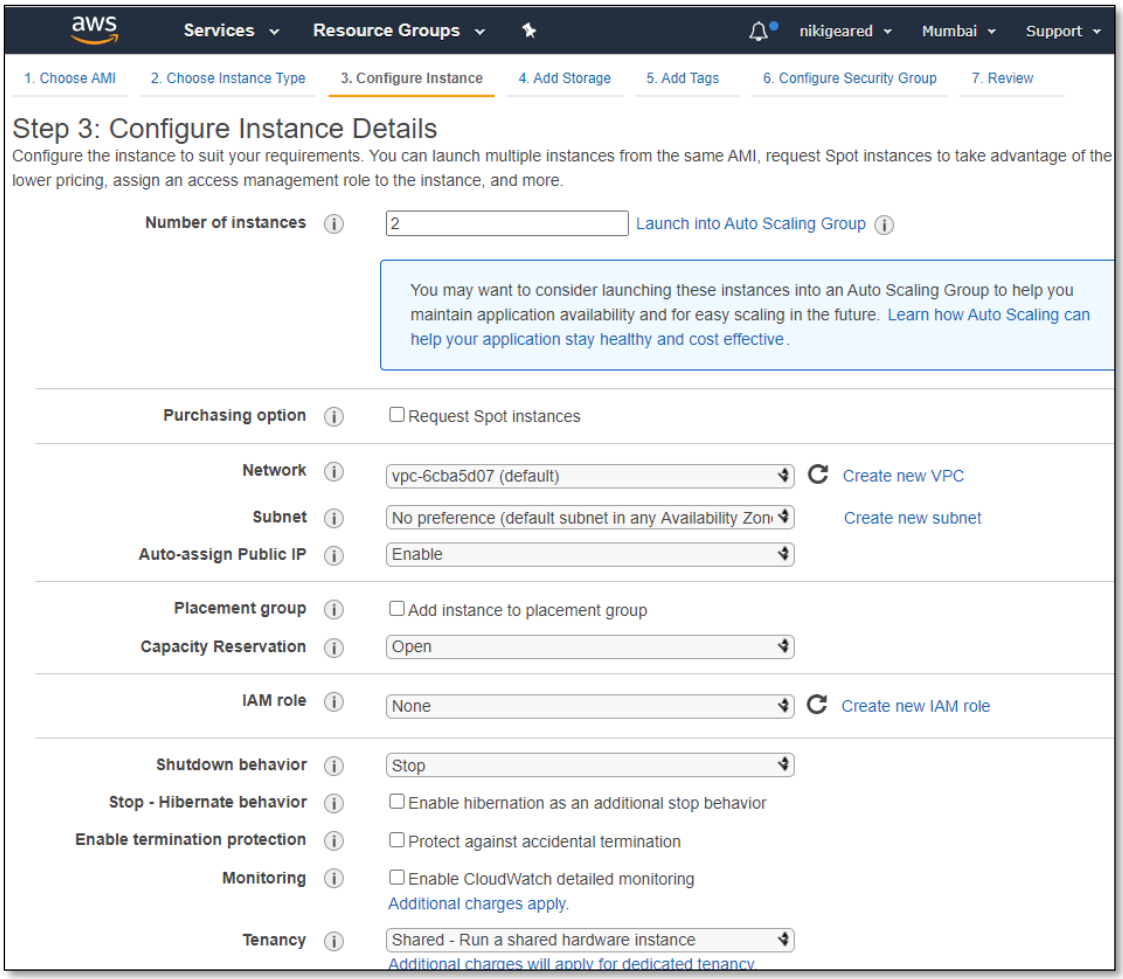
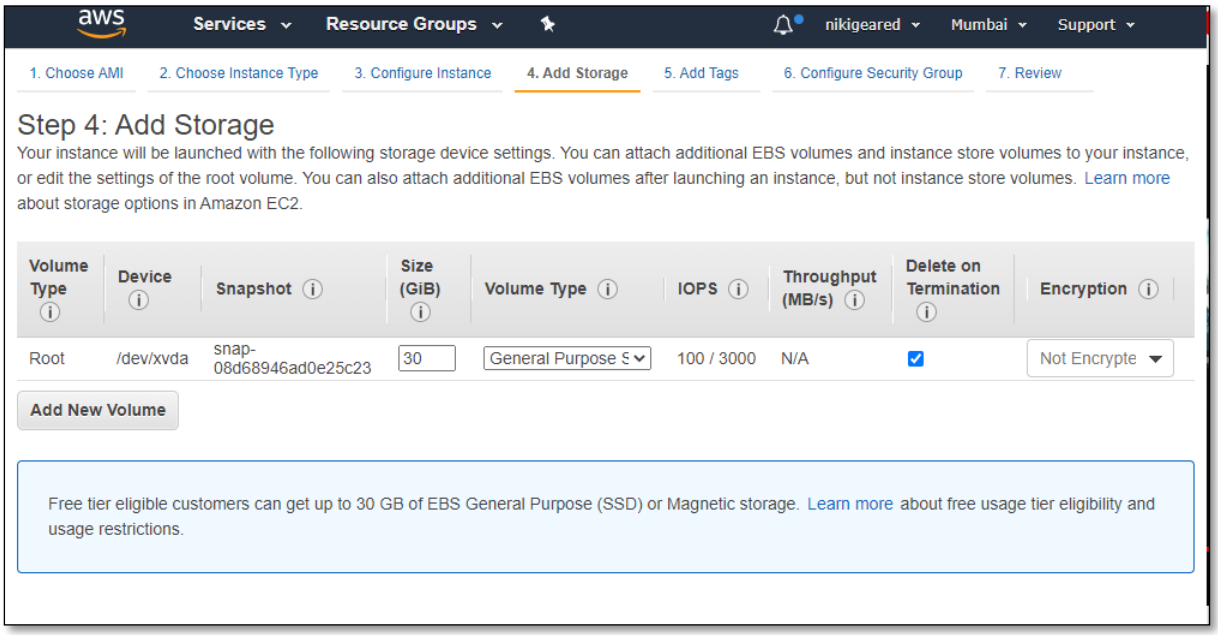
Line Balancing :

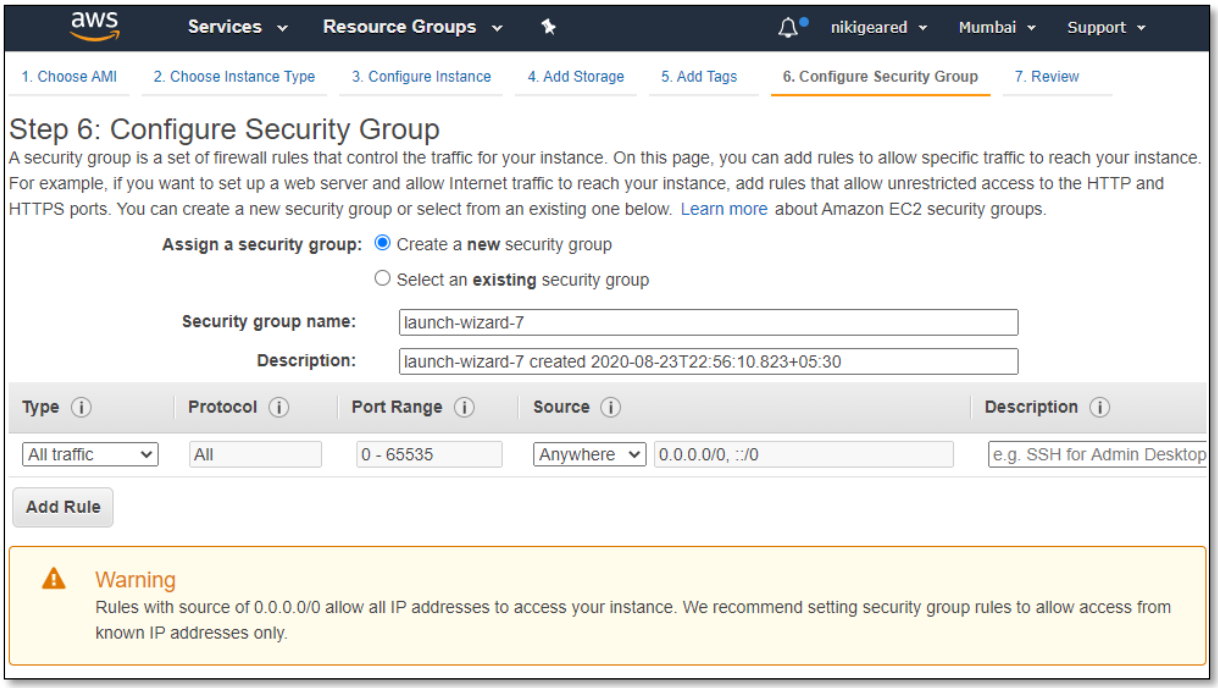
Create 2 Instances (select Linux as OS)

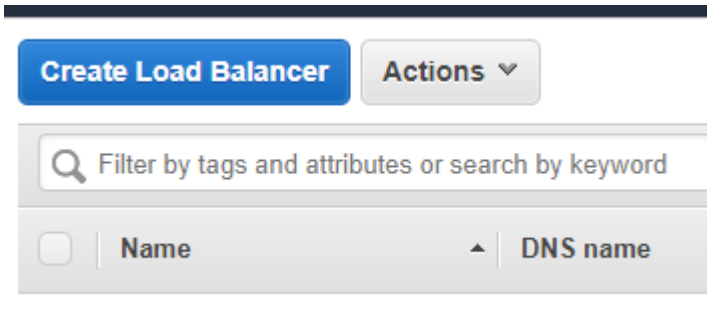


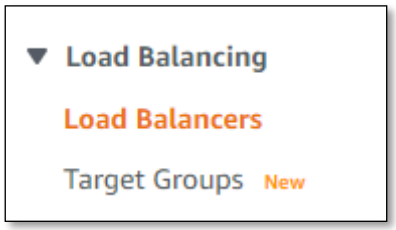


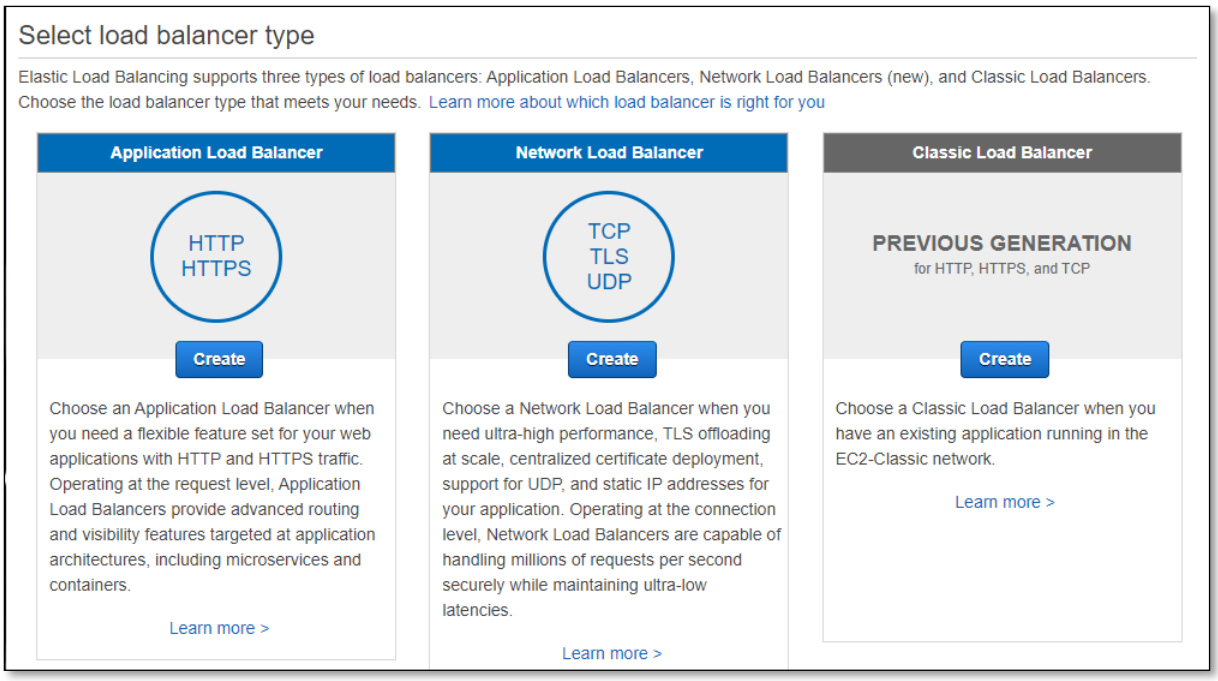

aws
Services
Resource Groups
nikigeared
Mumbai
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from 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 Zon
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.

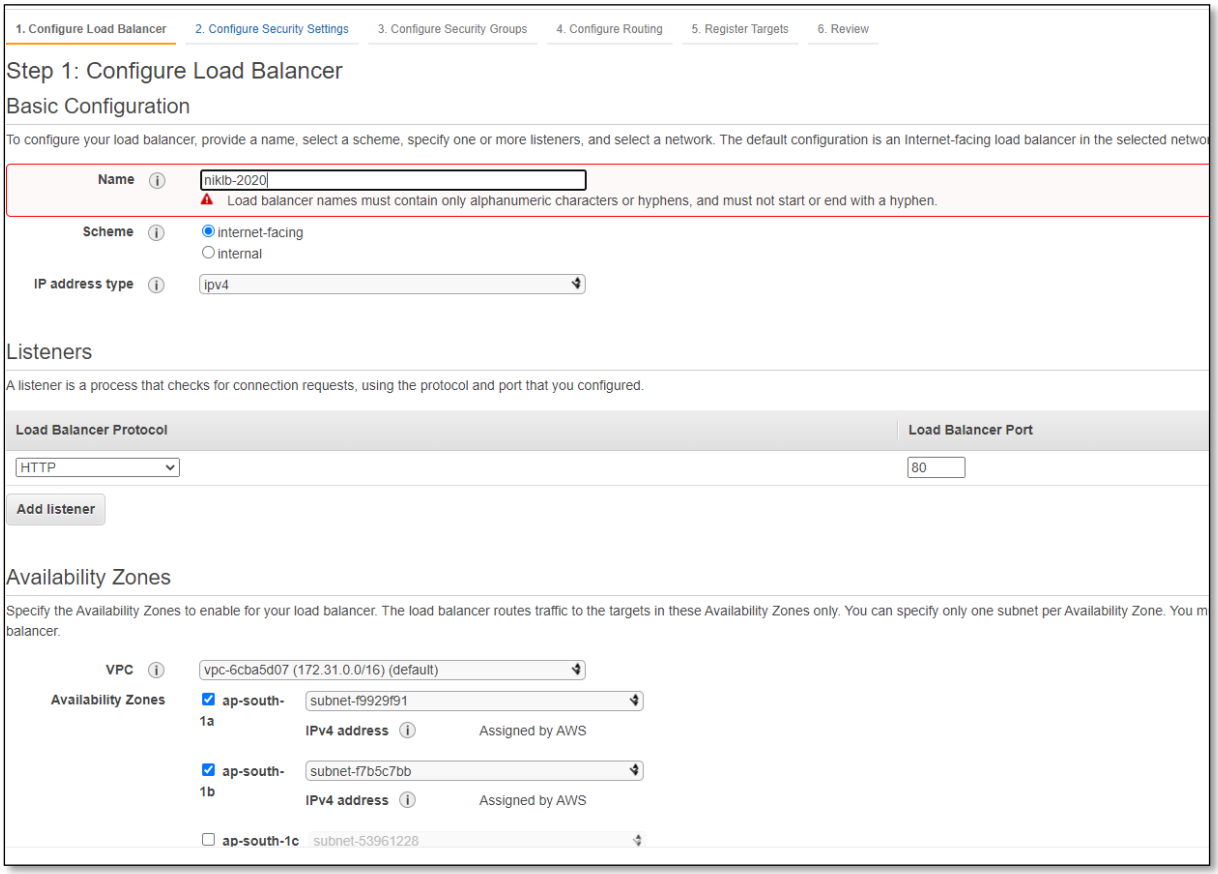

aws
Services
Resource Groups
nikigeared
Mumbai
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional 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
Not Encrypte
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.

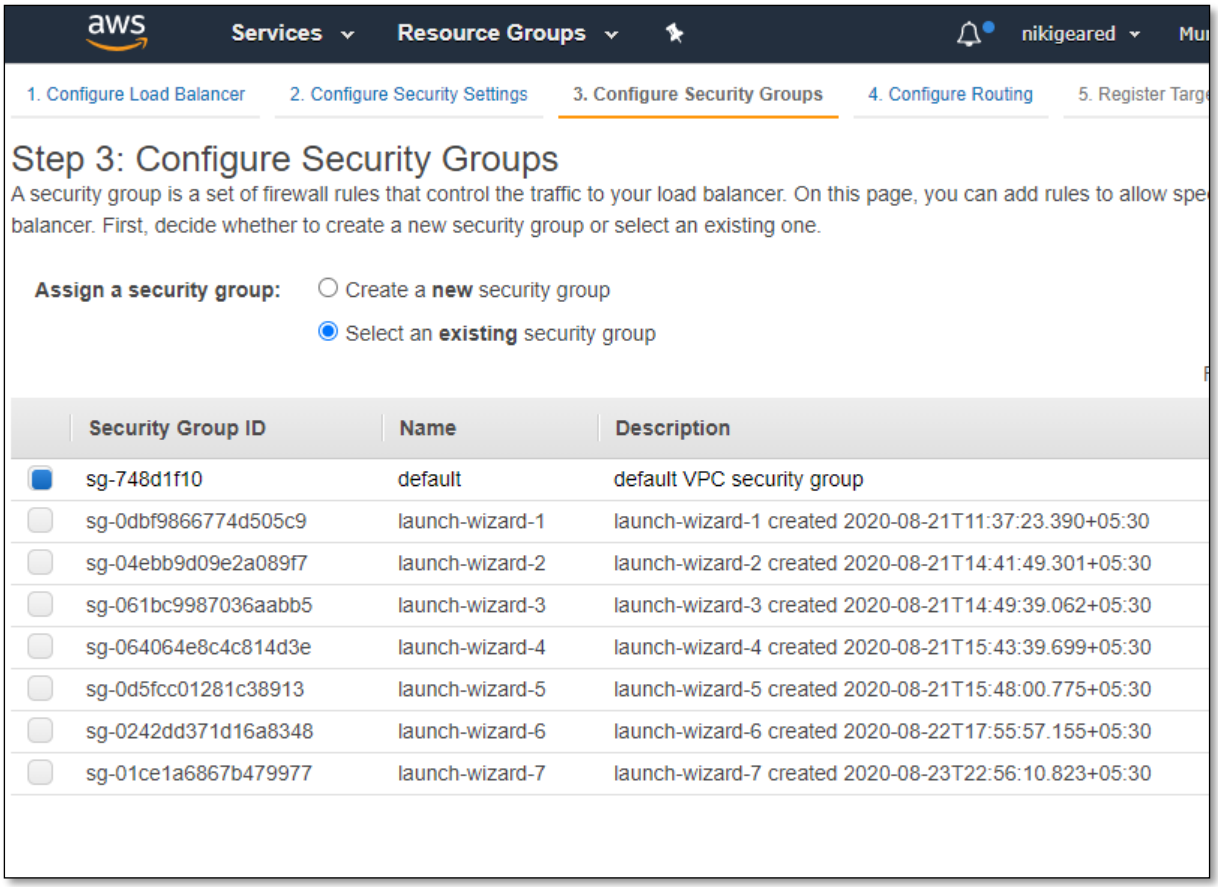

aws
Services
Resource Groups
nikigeared
Mumbai
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. 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 name: launch-wizard-7
Description: launch-wizard-7 created 2020-08-23T22:56:10.823+05:30
Type
Protocol
Port Range
Source
Description
All traffic
All
0 - 65535
Anywhere
0.0.0.0/0, ::/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.

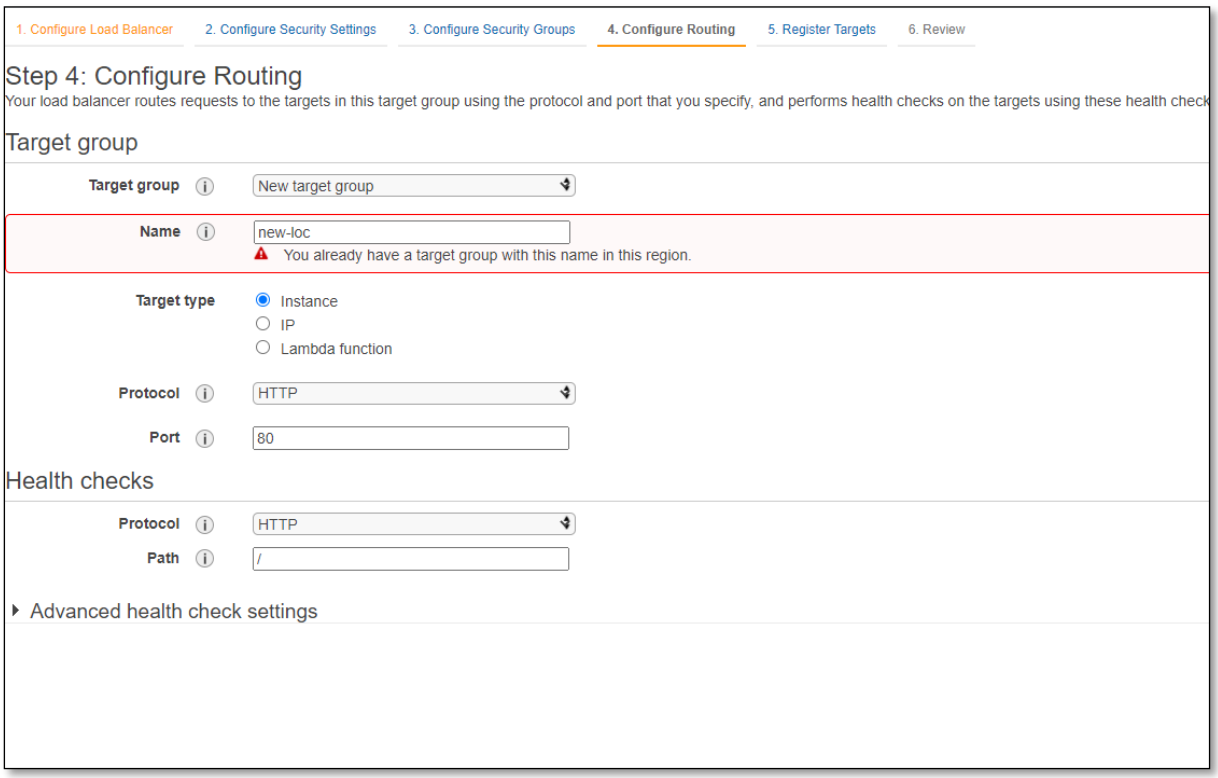

Create Load Balancer
Actions
Filter by tags and attributes or search by keyword
Name
DNS name

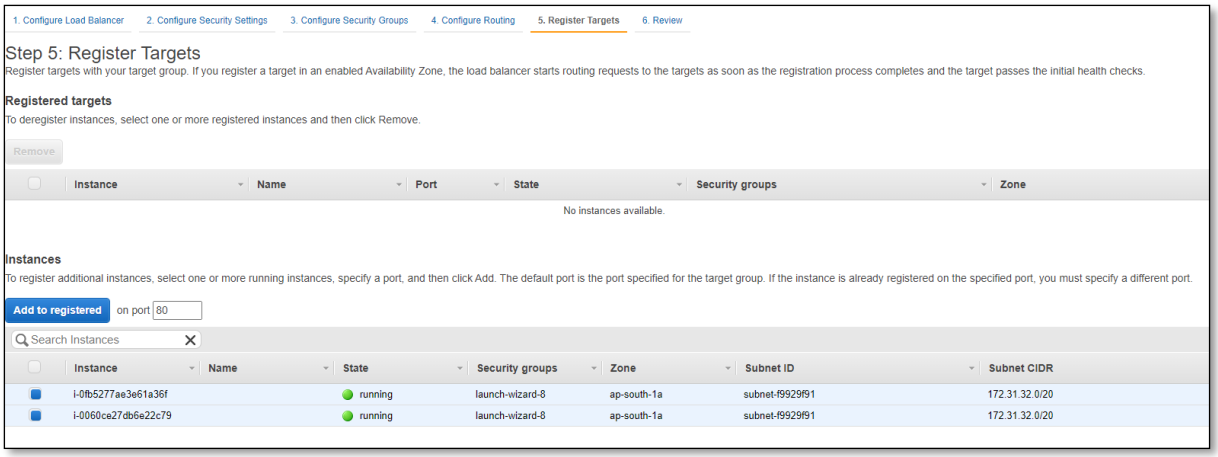

Load Balancing
Load Balancers
Target Groups
New

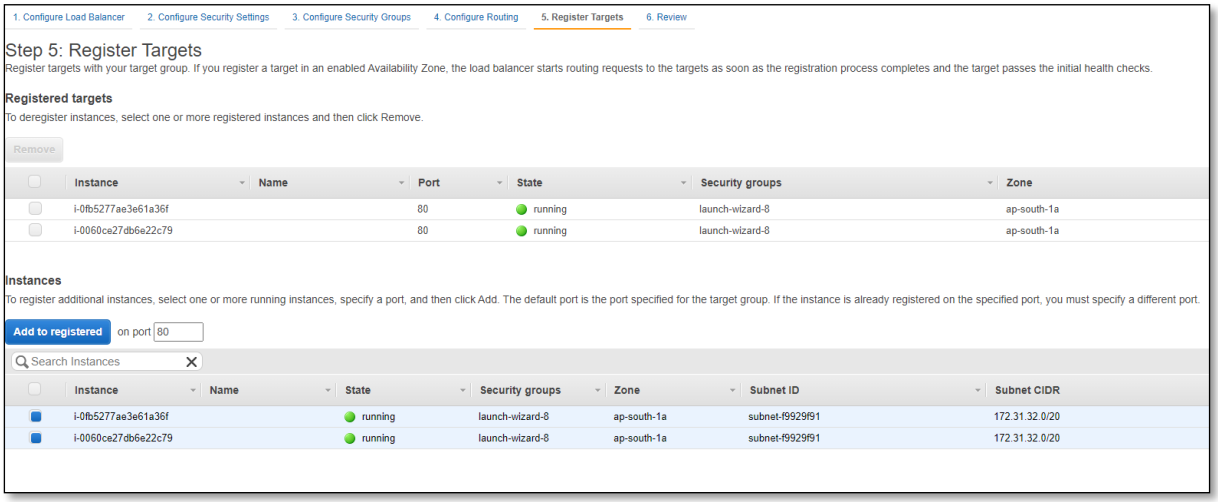

Select load balancer type
Elastic Load Balancing supports three types of load balancers: Application Load Balancers, Network Load Balancers (new), and Classic Load Balancers.
Choose the load balancer type that meets your needs. Learn more about which load balancer is right for you
Application Load Balancer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

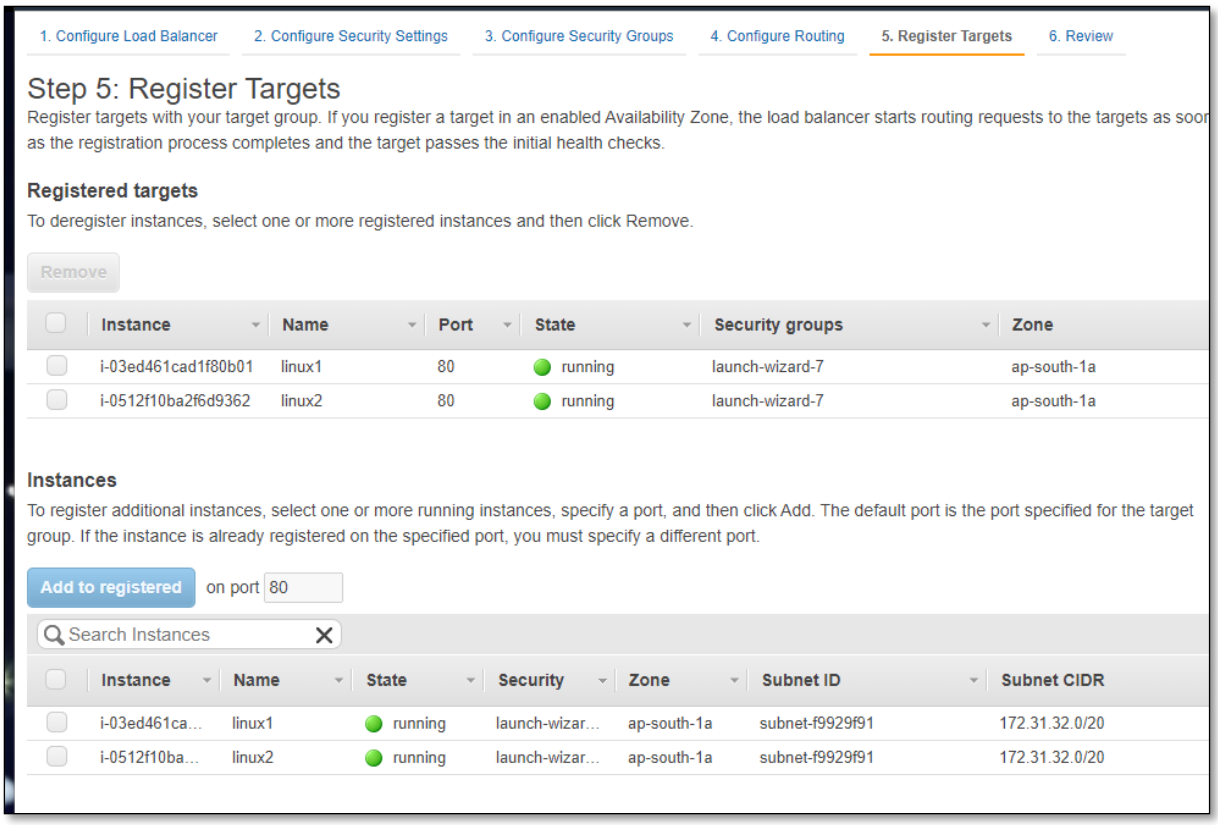

1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review
Step 1: Configure Load Balancer
Basic Configuration
To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected netwo
Name
nlklb-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 m
balancer.
VPC
vpc-6cba5d07 (172.31.0.0/16) (default)
Availability Zones
ap-south-1a
subnet-f9929f91
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
1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targ
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 spe
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
sg-748d1f10
default
default VPC security group
sg-0dbf9866774d505c9
launch-wizard-1
launch-wizard-1 created 2020-08-21T11:37:23.390+05:30
sg-04ebb9d09e2a089f7
launch-wizard-2
launch-wizard-2 created 2020-08-21T14:41:49.301+05:30
sg-061bc9987036aabb5
launch-wizard-3
launch-wizard-3 created 2020-08-21T14:49:39.062+05:30
sg-064064e8c4c814d3e
launch-wizard-4
launch-wizard-4 created 2020-08-21T15:43:39.699+05:30
sg-0d5fcc01281c38913
launch-wizard-5
launch-wizard-5 created 2020-08-21T15:48:00.775+05:30
sg-0242dd371d16a8348
launch-wizard-6
launch-wizard-6 created 2020-08-22T17:55:57.155+05:30
sg-01ce1a6867b479977
launch-wizard-7
launch-wizard-7 created 2020-08-23T22:56:10.823+05:30

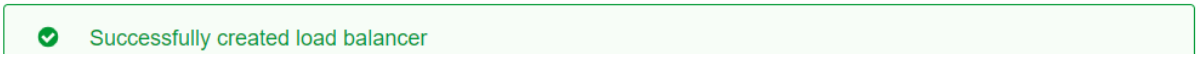

1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review
Step 4: Configure Routing
Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check
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

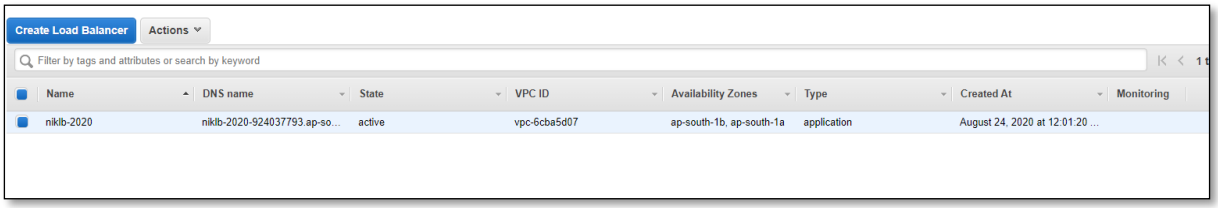

1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review
Step 5: Register Targets
Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests 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
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 80
Search Instances
Instance
Name
State
Security groups
Zone
Subnet ID
Subnet CIDR
i-0fb5277ae3e61a36f
running
launch-wizard-8
ap-south-1a
subnet-f9929f91
172.31.32.0/20
i-0060ce27db6e22c79
running
launch-wizard-8
ap-south-1a
subnet-f9929f91
172.31.32.0/20


1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. 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
Instance
Name
Port
State
Security groups
Zone
i-0fb5277ae3e61a36f
80
running
launch-wizard-8
ap-south-1a
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 80
Search Instances
Instance
Name
State
Security groups
Zone
Subnet ID
Subnet CIDR
i-0fb5277ae3e61a36f
running
launch-wizard-8
ap-south-1a
subnet-f9929f91
172.31.32.0/20
i-0060ce27db6e22c79
running
launch-wizard-8
ap-south-1a
subnet-f9929f91
172.31.32.0/20

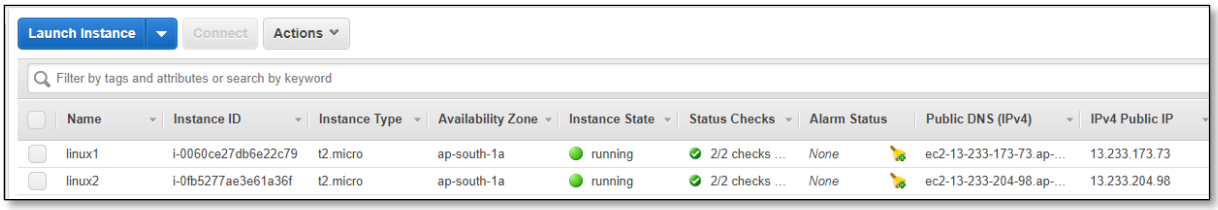


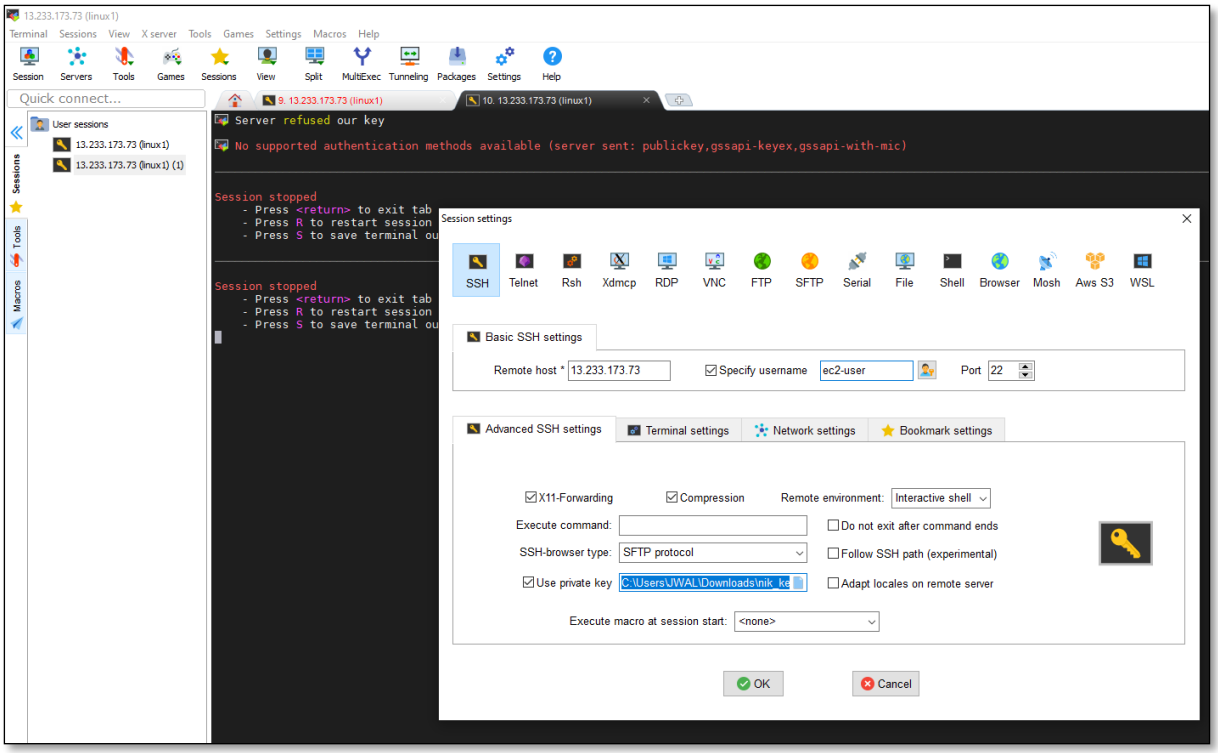
Load Balancer Creation Status

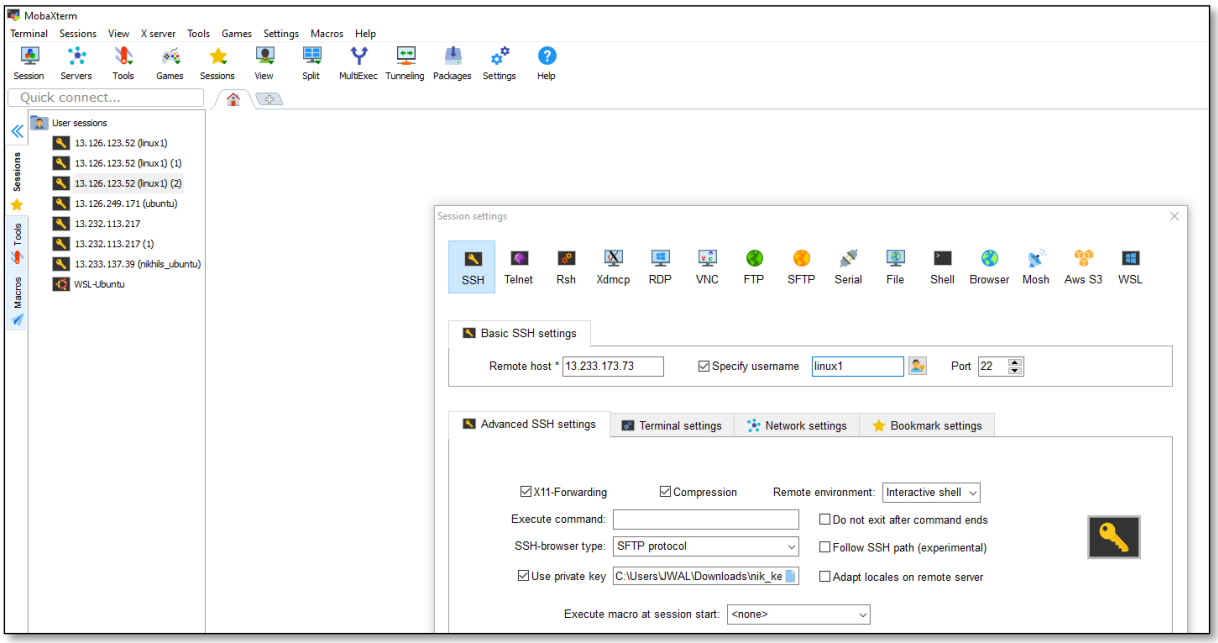


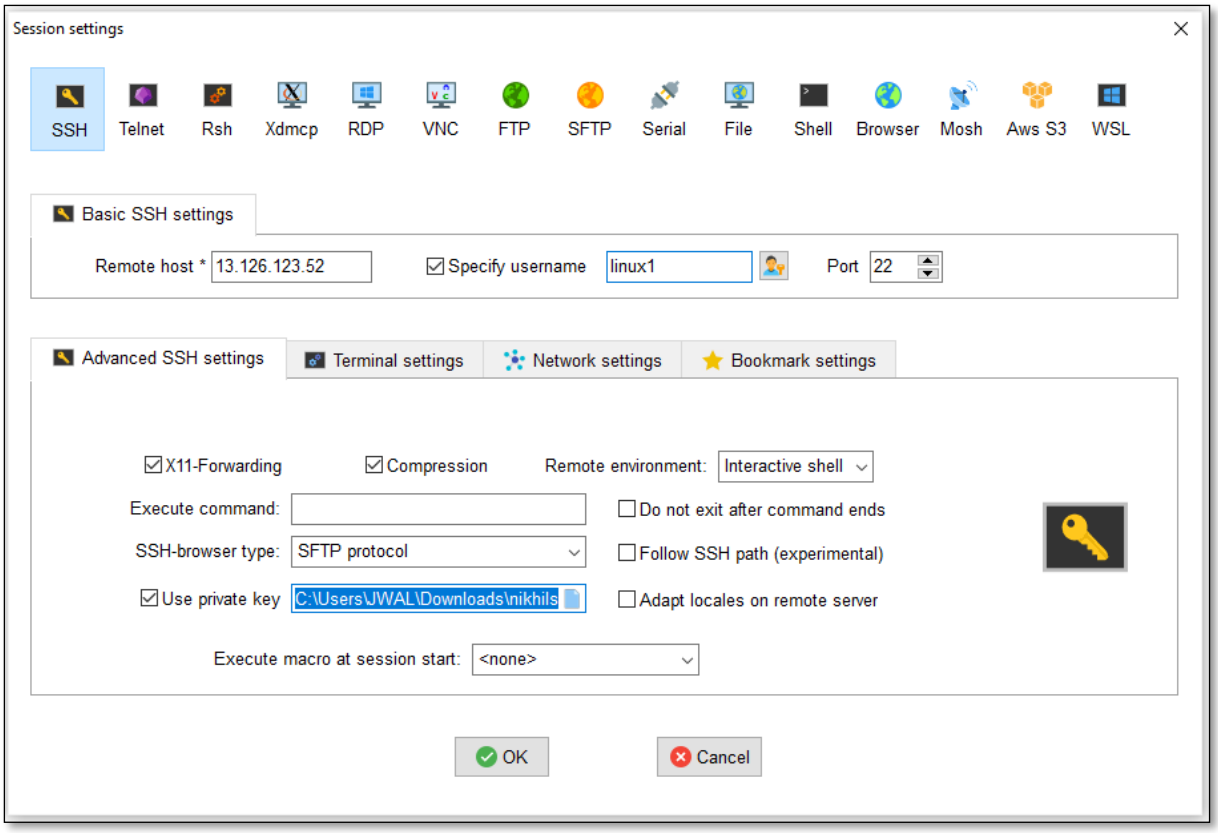


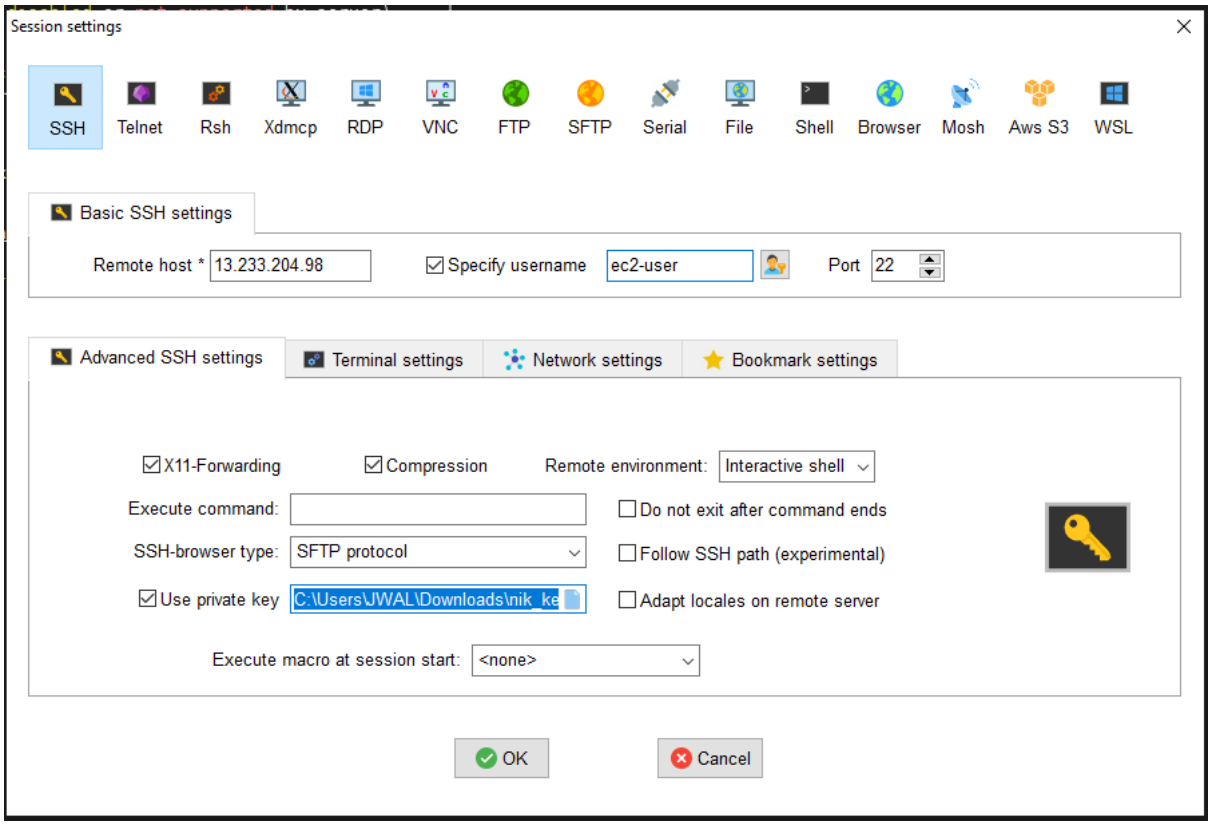
Configure the Instances:

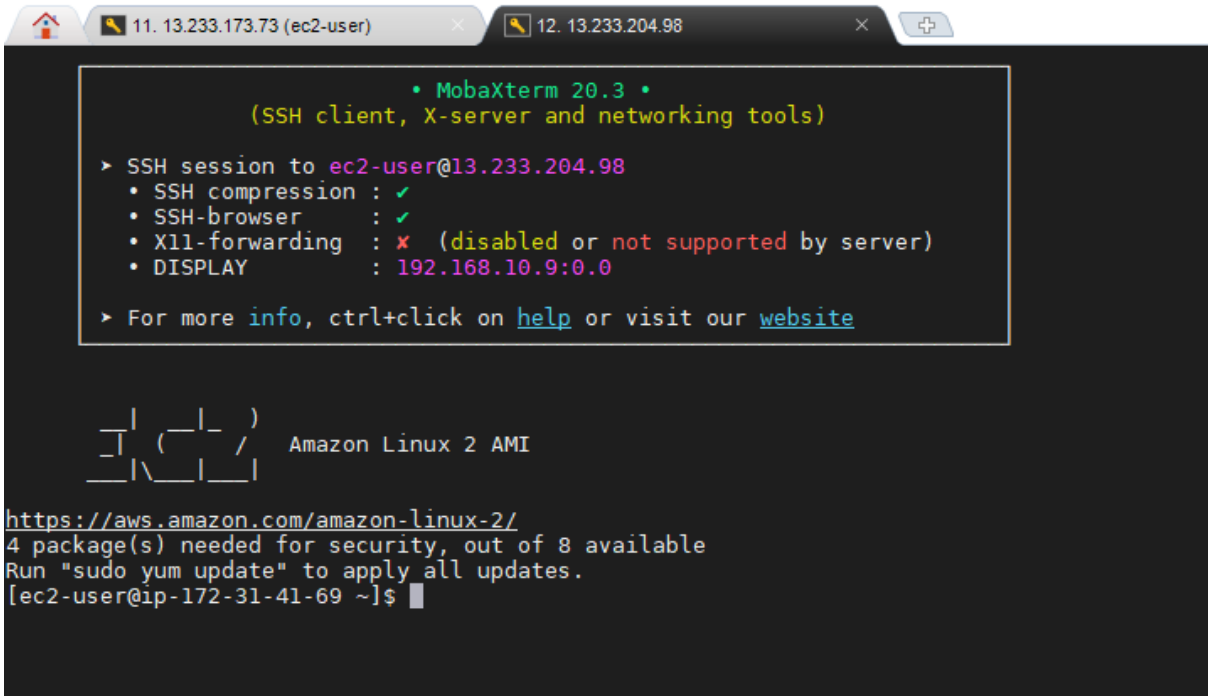



13.233.173.73 (linux1)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
User sessions
13.233.173.73 (linux1)
13.233.173.73 (linux1) (1)
Server refused our key
No supported authentication methods available (server sent: publickey,gssapi-keyex,gssapi-with-mic)
Session stopped
- Press <return> to exit tab
- Press R to restart session
- Press S to save terminal ou
Session settings
SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL
Basic SSH settings
Remote host * 13.233.173.73
Specify username ec2-user
Port 22
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
X11-Forwarding
Compression
Remote environment: Interactive shell
Execute command:
Do not exit after command ends
SSH-browser type: SFTP protocol
Follow SSH path (experimental)
Use private key C:\Users\JWAL\Downloads\nik_ke
Adapt locales on remote server
Execute macro at session start: <none>
OK
Cancel


MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
User sessions
13.126.123.52 (linux1)
13.126.123.52 (linux1) (1)
13.126.123.52 (linux1) (2)
13.126.249.171 (ubuntu)
13.232.113.217
13.232.113.217 (1)
13.233.137.39 (nikhils_ubuntu)
WSL-Ubuntu
Session settings
SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL
Basic SSH settings
Remote host * 13.233.173.73
Specify username linux1
Port 22
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
X11-Forwarding
Compression
Remote environment: Interactive shell
Execute command:
Do not exit after command ends
SSH-browser type: SFTP protocol
Follow SSH path (experimental)
Use private key C:\Users\JWAL\Downloads\nik_ke
Adapt locales on remote server
Execute macro at session start: <none>

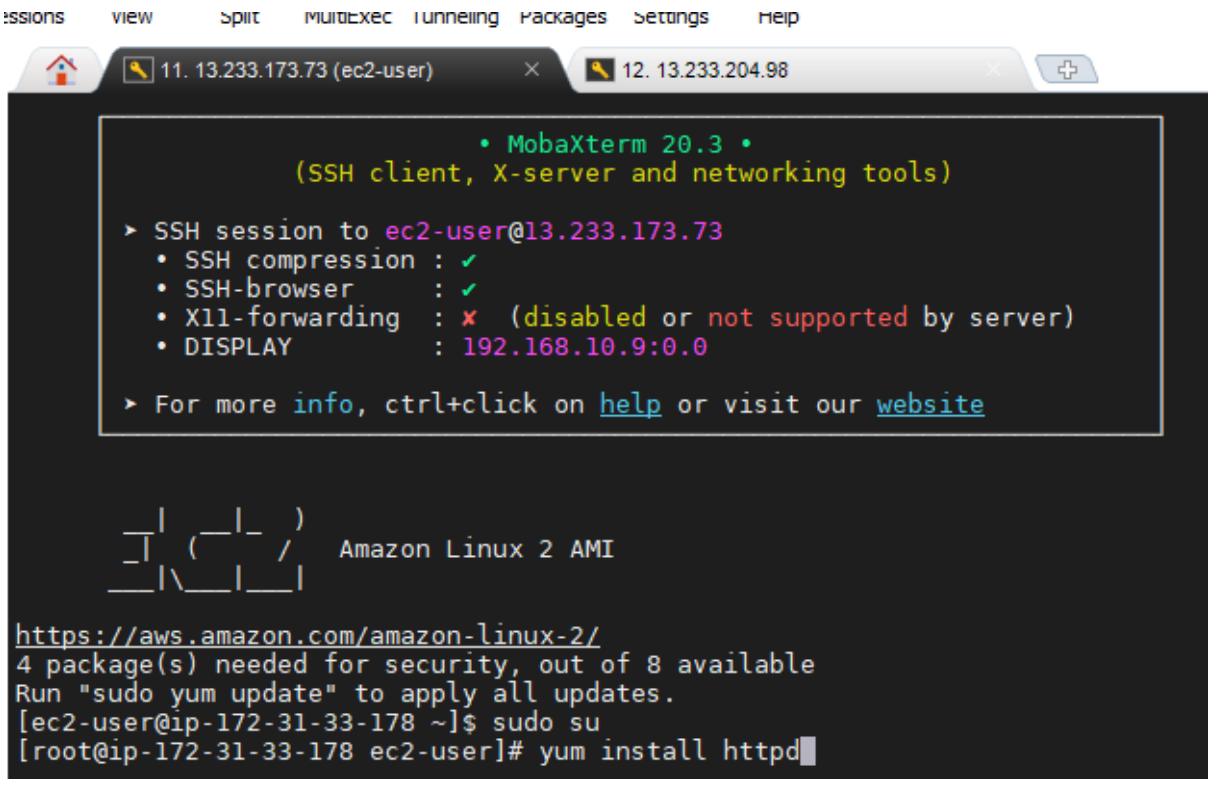

Session settings
SSH
Telnet
Rsh
Xdmcp
RDP
VNC
FTP
SFTP
Serial
File
Shell
Browser
Mosh
Aws S3
WSL
Basic SSH settings
Remote host * 13.126.123.52
Specify username
linux1
Port 22
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
X11-Forwarding
Compression
Remote environment: Interactive shell
Execute command:
Do not exit after command ends
SSH-browser type: SFTP protocol
Follow SSH path (experimental)
Use private key
C:\Users\JWAL\Downloads\nikhils
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 username
ec2-user
Port 22
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
X11-Forwarding
Compression
Remote environment: Interactive shell
Execute command:
Do not exit after command ends
SSH-browser type: SFTP protocol
Follow SSH path (experimental)
Use private key
C:\Users\JWAL\Downloads\nik_ke
Adapt locales on remote server
Execute macro at session start: <none>
OK
Cancel



Sudo su

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

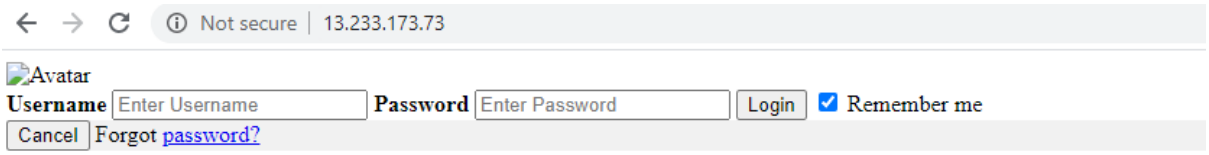
Press ‘i’ and this will be change into Insert Mode

Paste

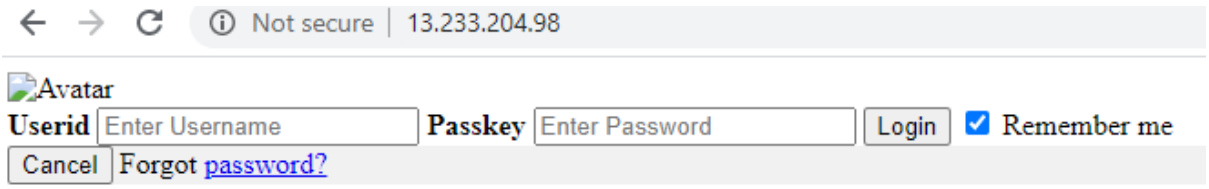
:wq

more index.html

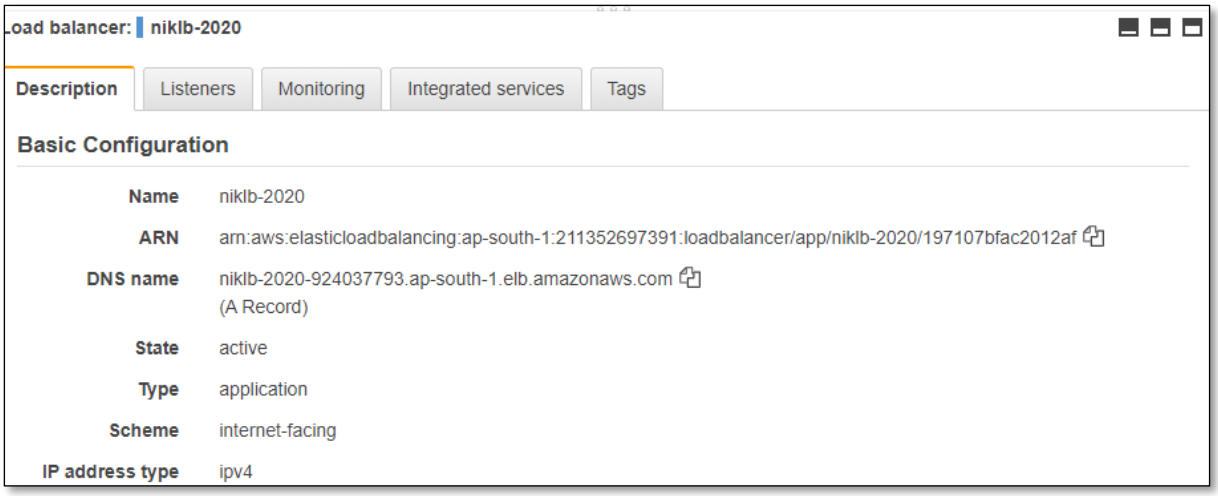
service httpd start

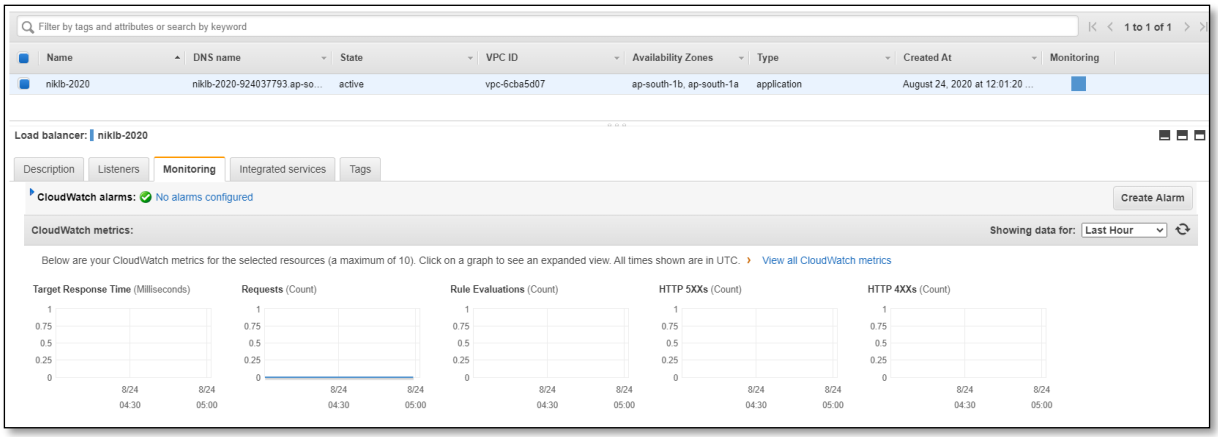


Similary do the Same for 2nd Machine and userid instead of user name and passkey instead of password



Load Balancers





Target Groups