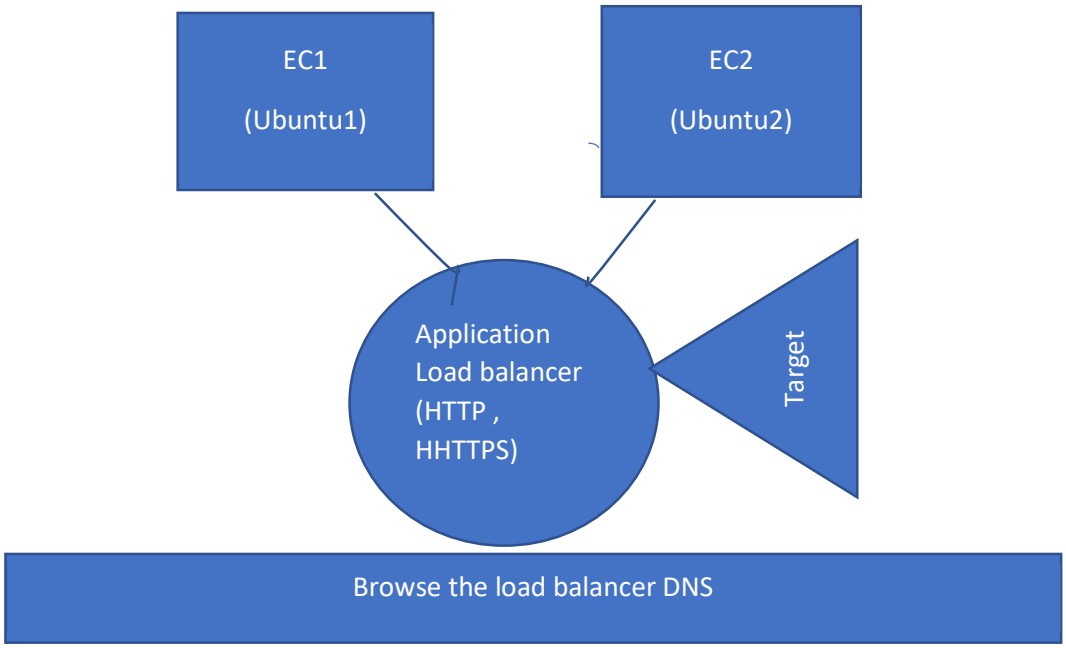
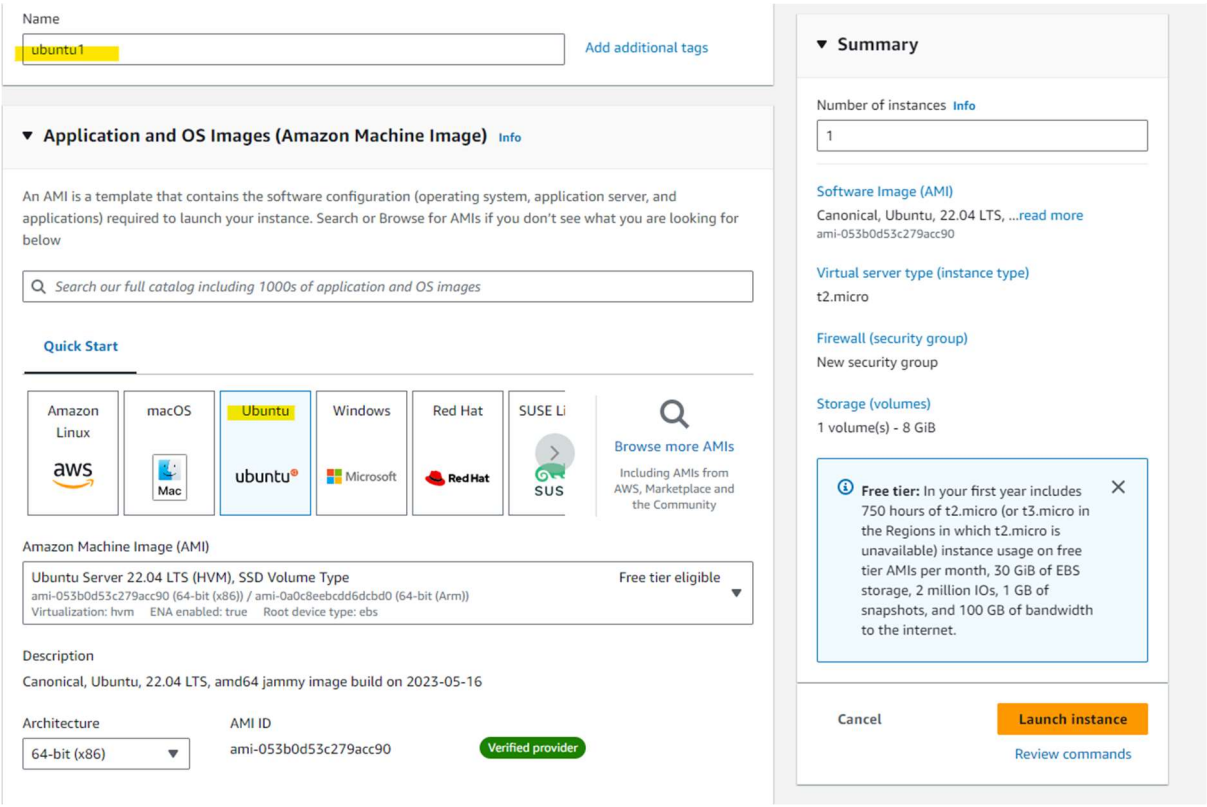
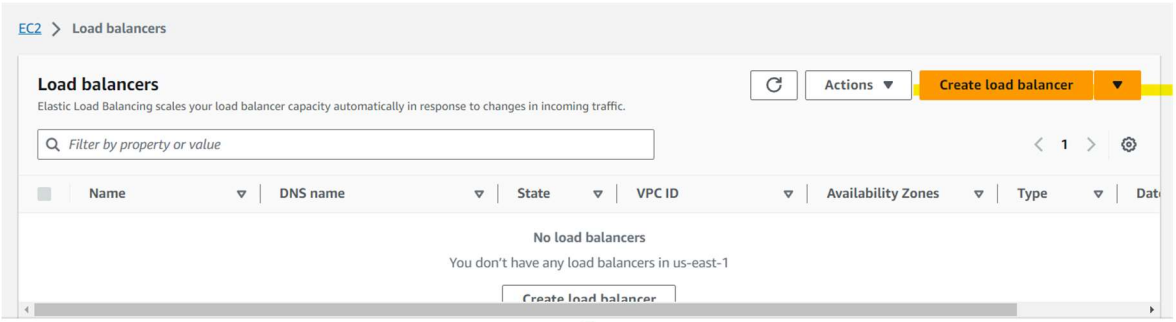
Load Balancer: Application load balancer



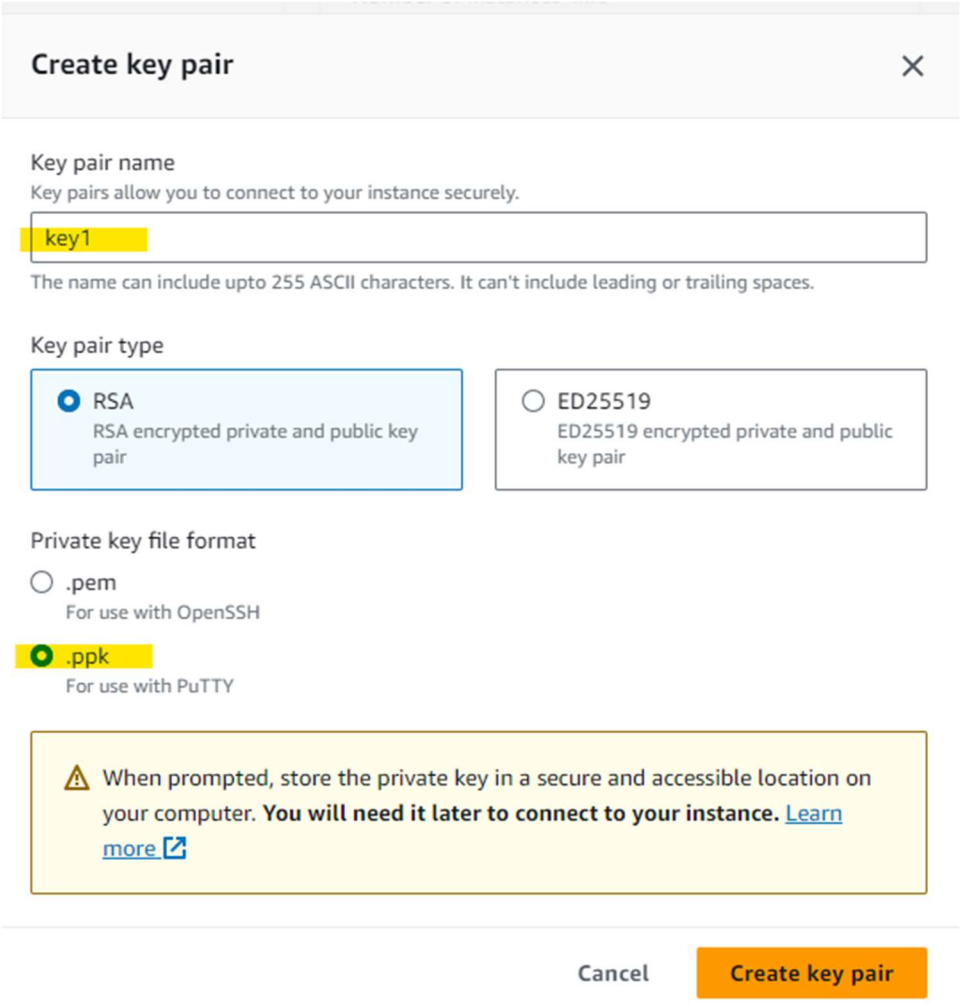
Create two EC2 (Ubuntu1 | Ubuntu2)

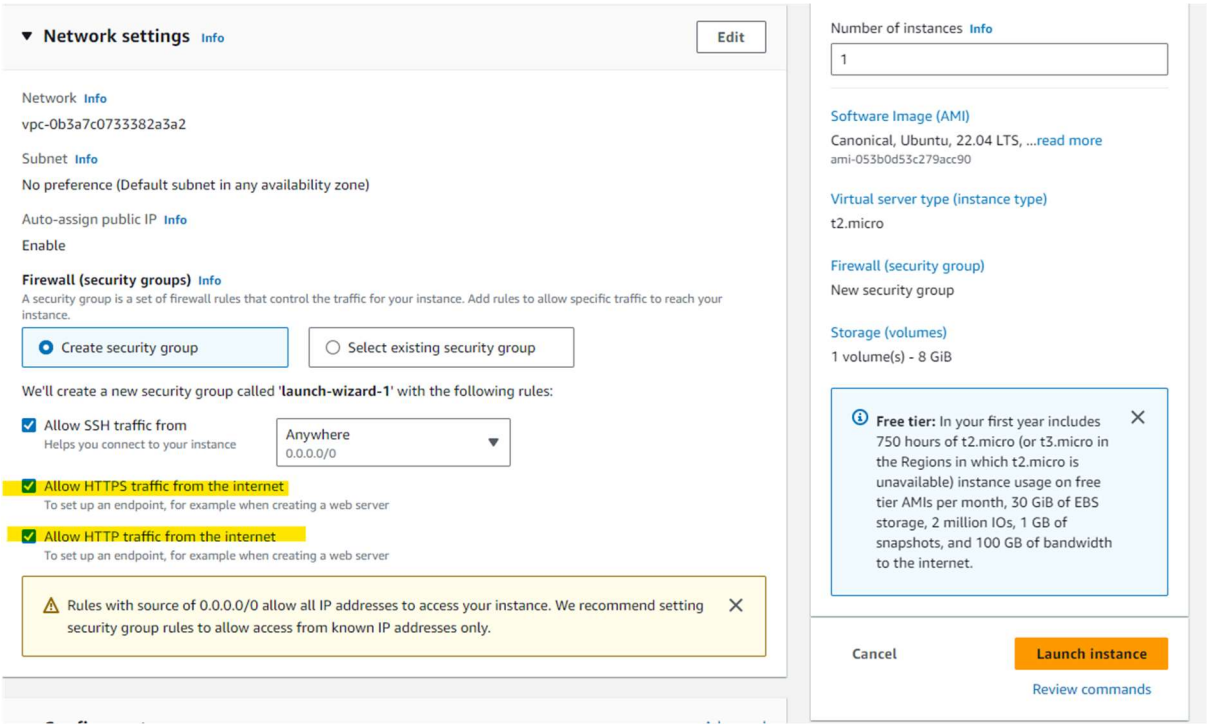


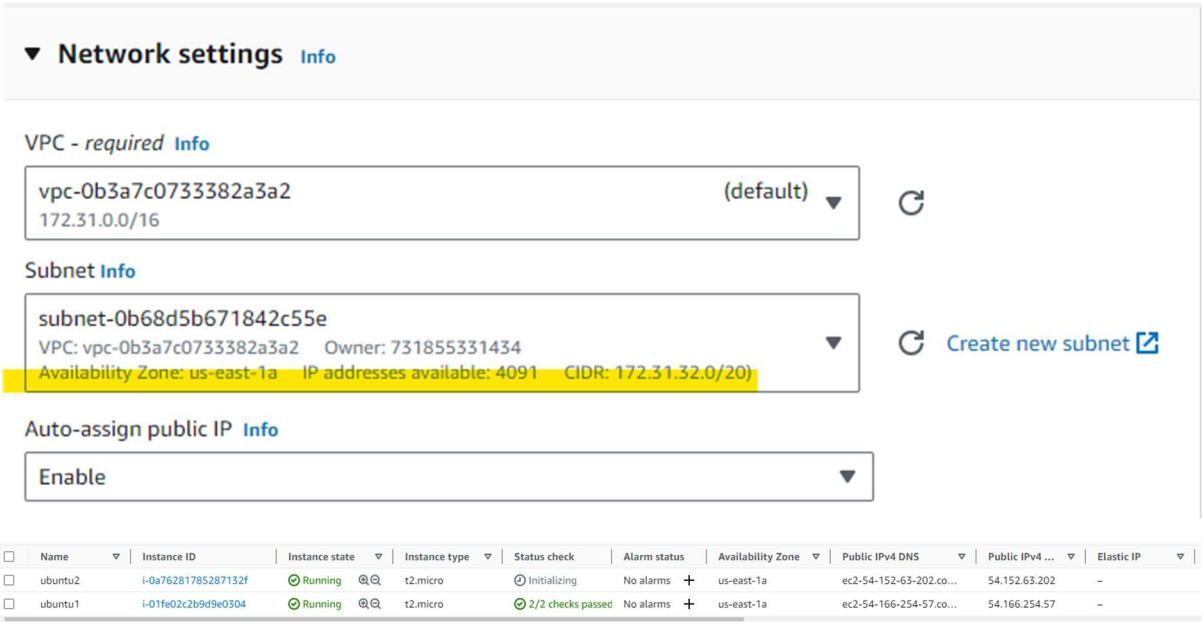
Create Load balancer



=







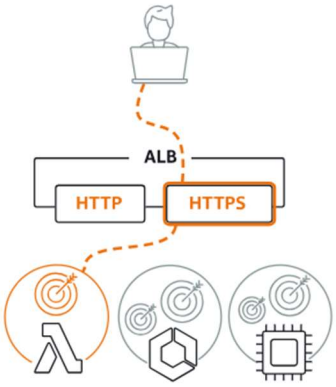
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
ubuntu2	i-0a76281785287132f	Running	t2.micro	Initializing	No alarms	us-east-1a	ec2-54-152-63-202.co...	54.152.63.202	–
ubuntu1	i-01fe02c2b9d9e0304	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-54-166-254-57.co...	54.166.254.57	–

Create Load balancer

Select application load balancer

Load balancer types

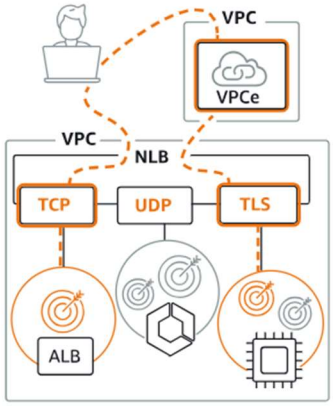
Application Load Balancer Info



Choose an Application Load Balancer when you need a flexible feature set for your 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.

Create

Network Load Balancer Info



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 applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Create

Gateway Load Balancer Info

Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create

Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

▶ How Elastic Load Balancing works

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

Pria

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme Info

Scheme can't be changed after the load balancer is created.

- (●) Internet-facing
  An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more
- ( ) Internal
  An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type Info

Select the type of IP addresses that your subnets use.

- (●) IPv4
  Recommended for internal load balancers.
- ( ) Dualstack
  Includes IPv4 and IPv6 addresses.

Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC Info

Select the virtual private cloud (VPC) for your targets or you can create a new VPC. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups.

-
vpc-0b3a7c0733382a3a2
IPv4: 172.31.0.0/16

Mappings Info

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

us-east-1a (use1-az6)

Subnet

subnet-0b68d5b671842c55e

IPv4 address

Assigned by AWS

us-east-1b (use1-az1)

Subnet

subnet-02b47ec2ae9a2fc01

IPv4 address

Assigned by AWS

us-east-1c (use1-az2)

Security groups Info

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

Select up to 5 security groups

launch-wizard-1
sg-0776f767cef793bbf VPC: vpc-0b3a7c0733382a3a2

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Listener **HTTP:80** Remove

Protocol: HTTP

Port: 80

1-65535

Default action Info

Forward to *Select a target group*

Create target group

Listener tags - *optional*

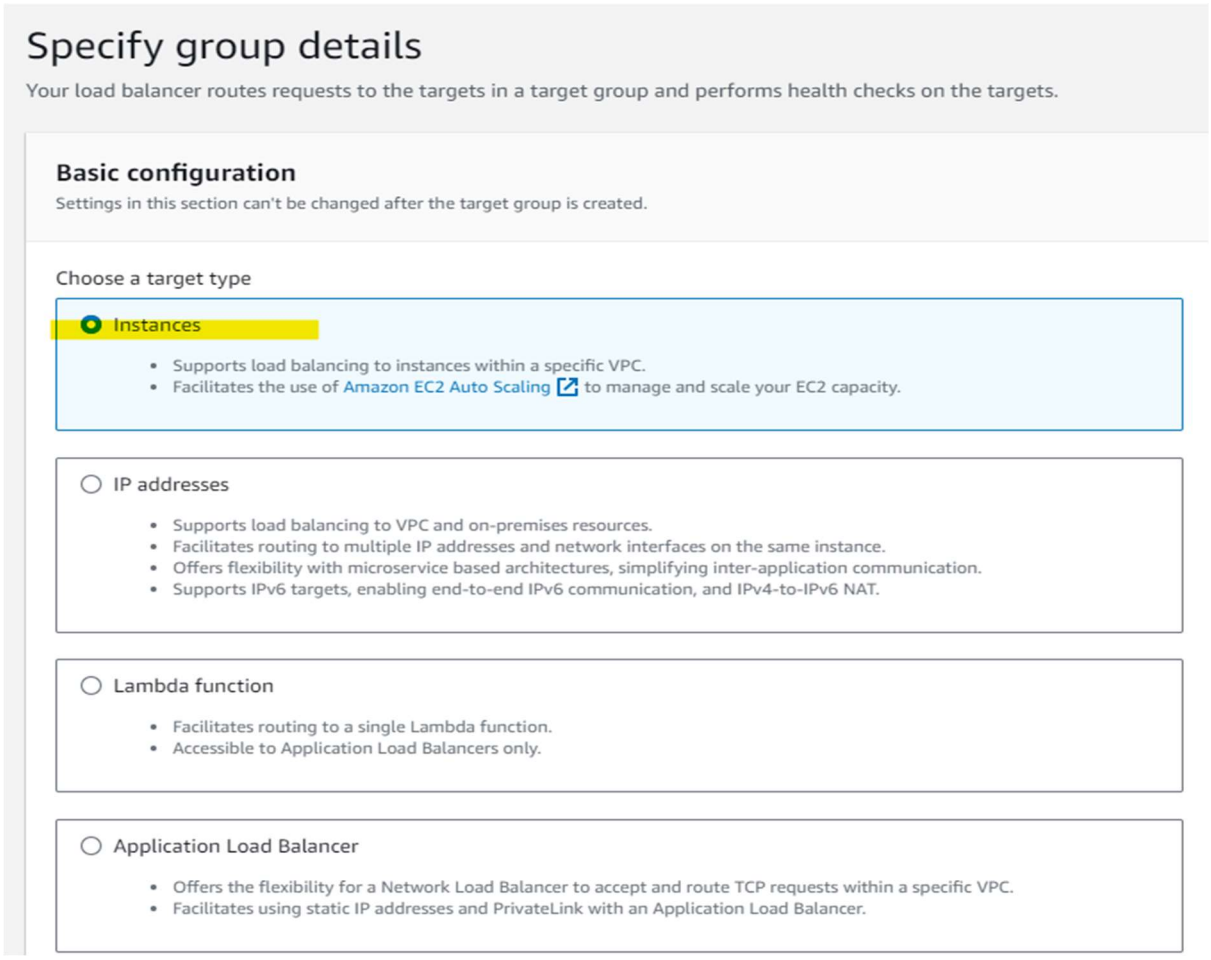
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

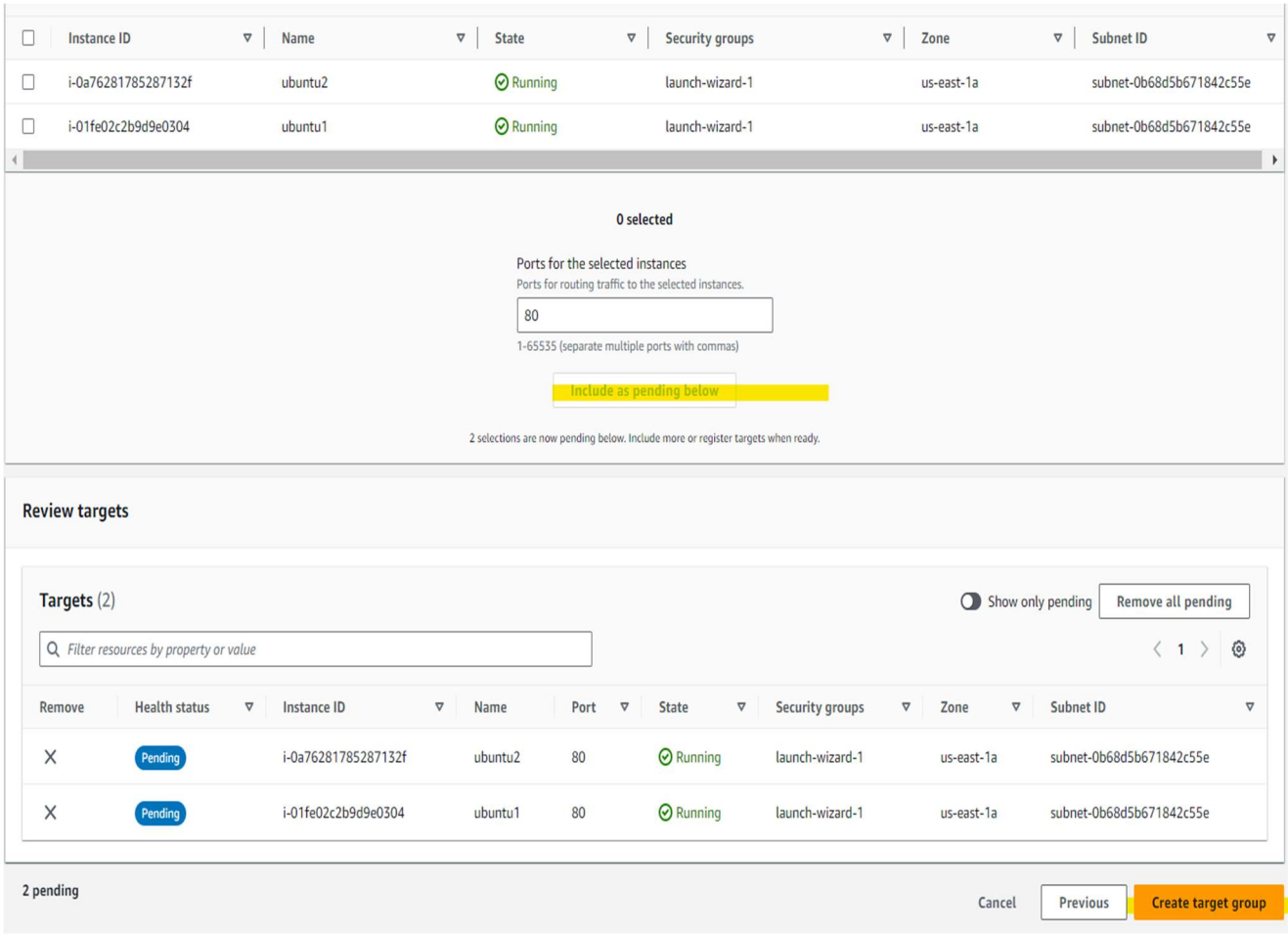
Add listener tag

You can add up to 50 more tags.

Add listener

To create target group





Review targets

Targets (2)

Show only pending | Remove all pending

Filter resources by property or value

1

Remove	Health status	Instance ID	Name	Port	State	Security groups	Zone	Subnet ID
X	Pending	i-0a76281785287132f	ubuntu2	80	Running	launch-wizard-1	us-east-1a	subnet-0b68d5b671842c55e
X	Pending	i-01fe02c2b9d9e0304	ubuntu1	80	Running	launch-wizard-1	us-east-1a	subnet-0b68d5b671842c55e

2 pending

Cancel | Previous | Create target group

Target group name

target1

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol

HTTP

Port

80

1-65535

VPC

Select the VPC with the instances that you want to include in the target group.

-
vpc-0b3a7c0733382a3a2
IPv4: 172.31.0.0/16

Protocol version

- (•) HTTP1
  Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
- ( ) HTTP2
  Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
- ( ) gRPC
  Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

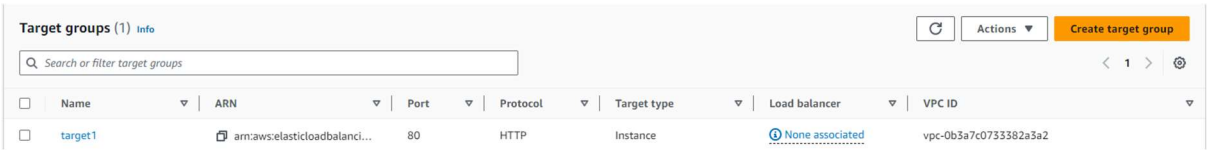
HTTP

Health check path

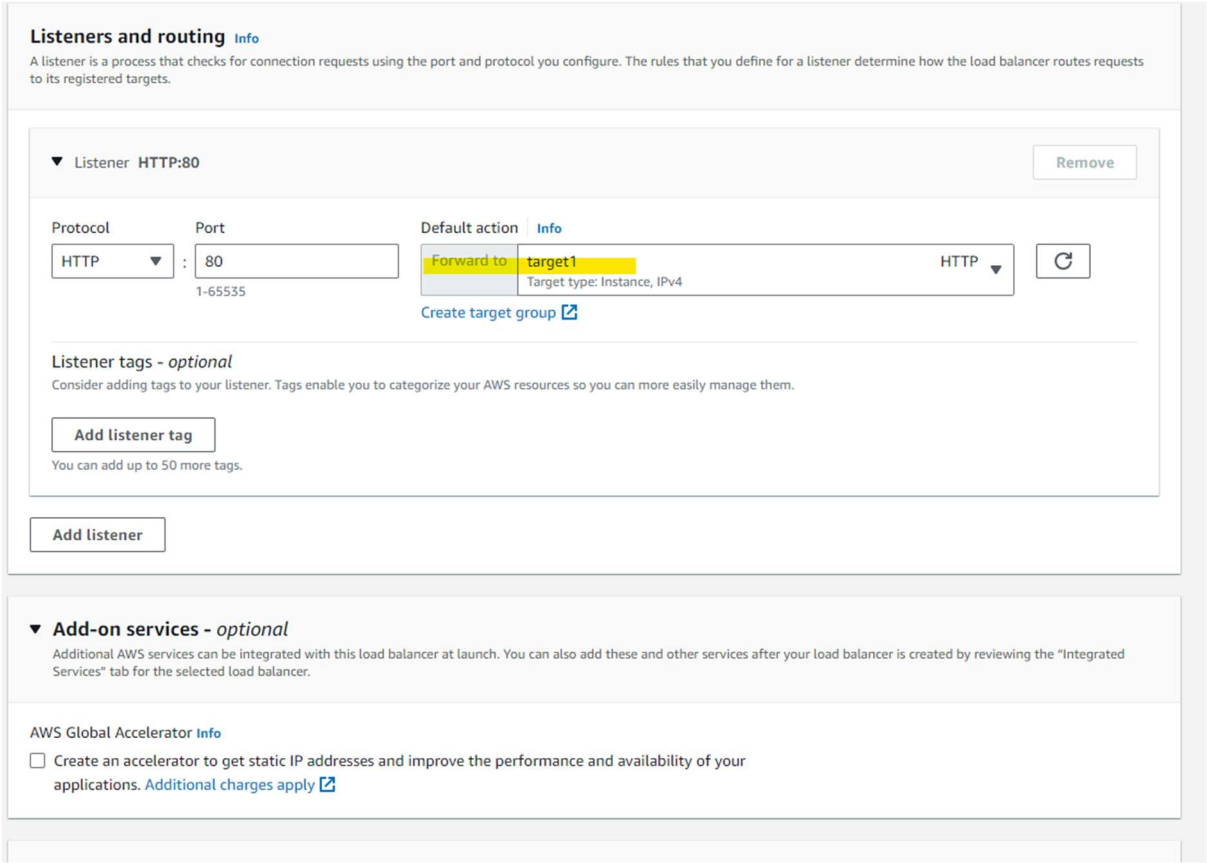
Use the default path of "/" to ping the root, or specify a custom path if preferred.

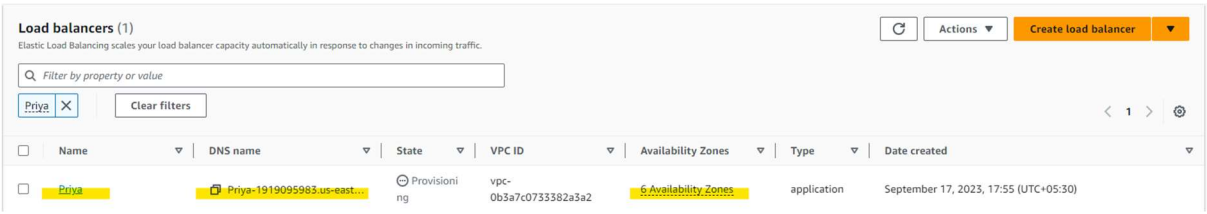
/index.html

Up to 1024 characters allowed.

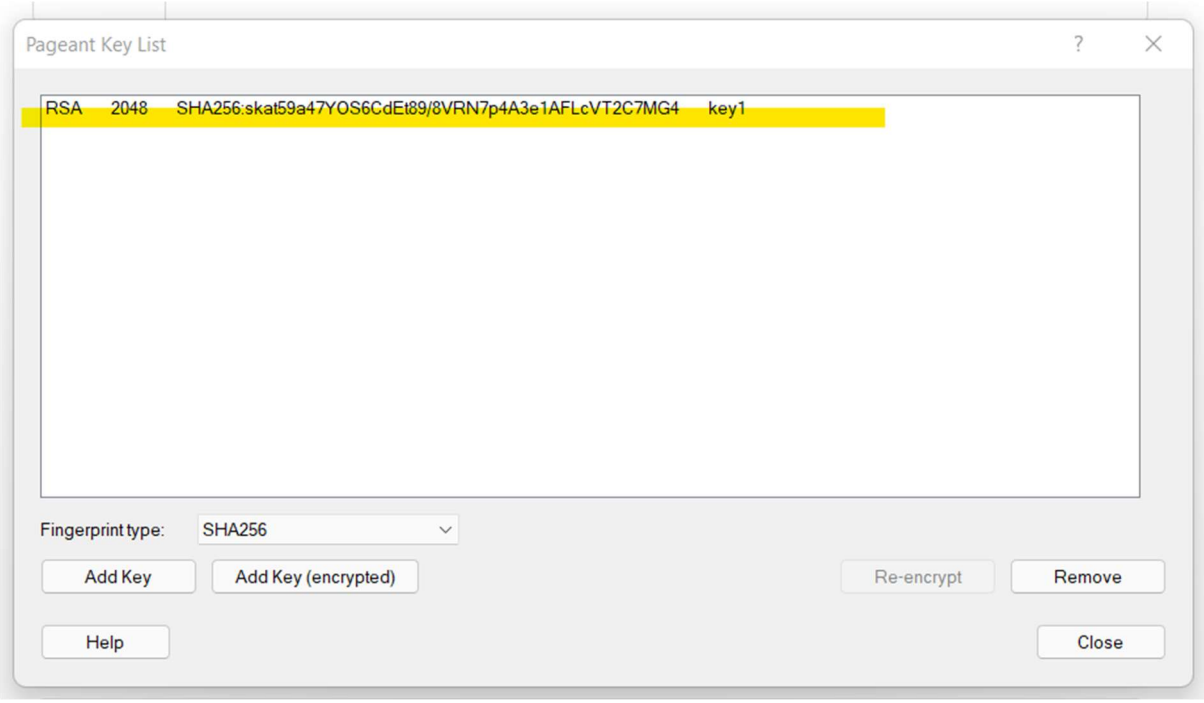


Now select target group

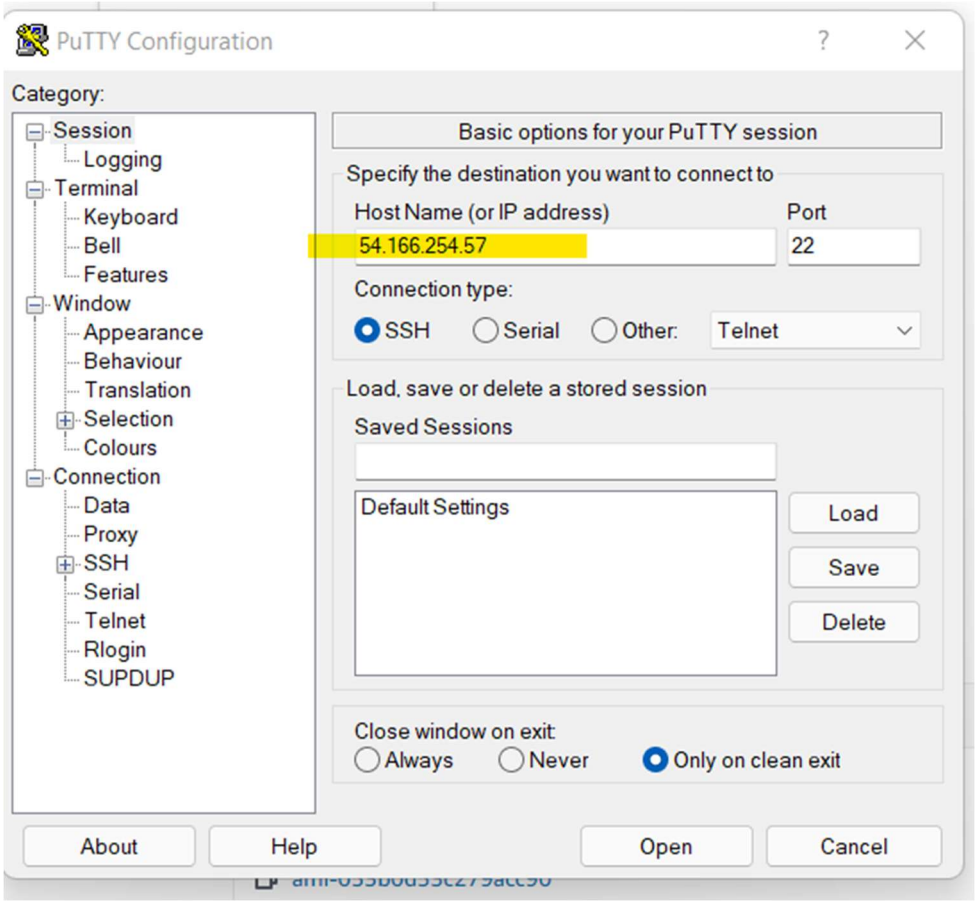


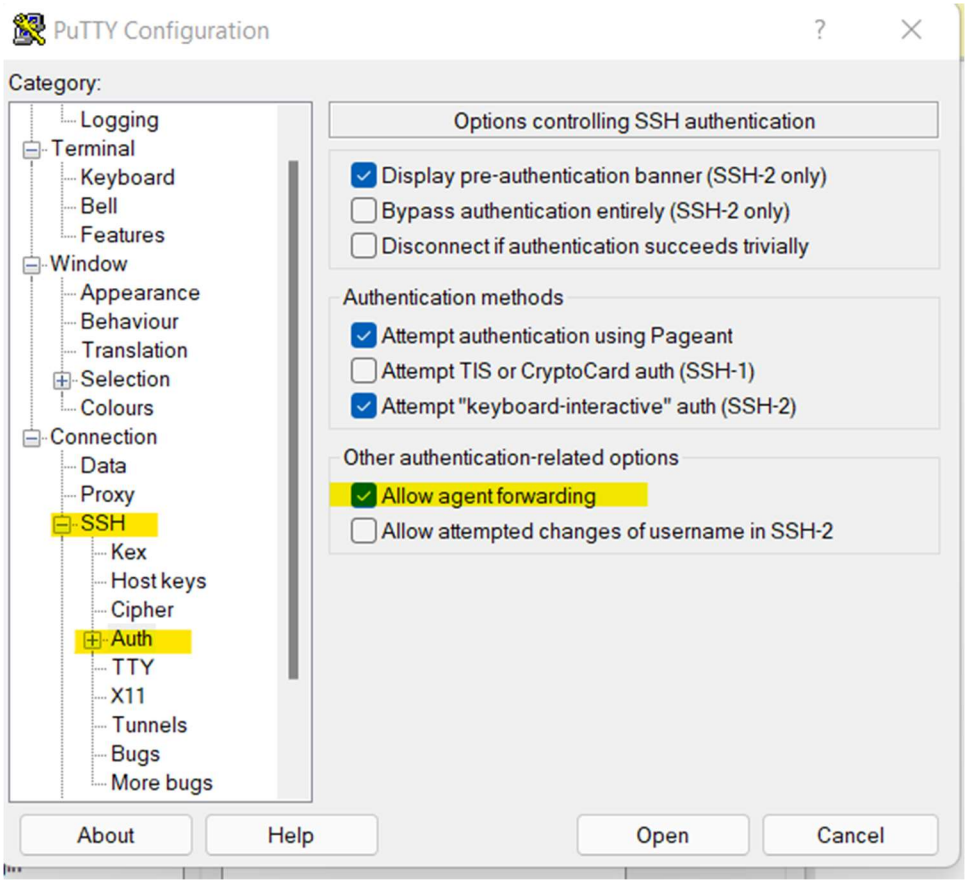


Add key to Putty Pageant



Connect through Putty





Once connected

Use below commands :-

apt update

apt install apache2

systemctl restart apache2

systemctl enable apache2

cd /var/www/html

nano index.html

To remove :- ri index.html

Vi index.html

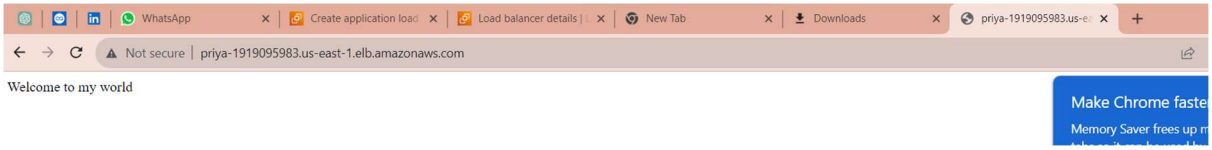
Enter note by clicking insert

To save : escape, shift : ,wq , enter

```
root@ip-172-31-44-103: /var/www/html
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36.1-4build1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ip-172-31-44-103:/home/ubuntu# systemctl apache2
Unknown command verb apache2.
root@ip-172-31-44-103:/home/ubuntu# systemctl restart apache2
root@ip-172-31-44-103:/home/ubuntu# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@ip-172-31-44-103:/home/ubuntu# cd /var/www/html
root@ip-172-31-44-103:/var/www/html# nano index.html
root@ip-172-31-44-103:/var/www/html# rm index.html
root@ip-172-31-44-103:/var/www/html# vi index.html
root@ip-172-31-44-103:/var/www/html#
```

Repeat same steps for ubuntu2

Copy load balancer DNS and paste in browser



Based on health check the page will be switched