

# LOAD BALANCER

Step 1:- create two identical instances in same region & configuration

--- creating instance

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

**Name and tags**

Name: ec2\_load balancer

**Application and OS Images (Amazon Machine Image)**

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

Recents: Quick Start

Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, Debian

**Summary**

Number of instances: 2

Software Image (AMI): Canonical, Ubuntu, 24.04, amd64

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Launch instance

----creating new security grp alltraffic

**Network settings**

VPC - required: vpc-0077c0b100707fd7e (default)

Subnet: No preference

Auto-assign public IP: Enable

**Firewall (security group)**

Create security group (selected) | Select existing security group

Security group name - required: alltraffic

Description - required

**Summary**

Number of instances: 2

Software Image (AMI): Canonical, Ubuntu, 24.04, amd64

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Launch instance

## -----writing script so instances install nginx while launching

**User data - optional** | Info  
Upload a file with your user data or enter it in the field.

[Choose file](#)

```
#! /bin/bash
sudo apt update -y
sudo apt install nginx -y

systemctl start nginx
systemctl enable nginx
```

☐ User data has already been base64 encoded

**Summary**

**Number of instances** | Info  
2  
When launching more than 1 instance, [consider EC2 Auto Scaling](#)

**Software image (AMI)**  
Canonical, Ubuntu, 24.04, amd64...[read more](#)  
ami-0e35ddab05955cf57

**Virtual server type (instance type)**  
t2.micro

**Firewall (security group)**  
New security group

**Storage (volumes)**  
1 volume(s) - 8 GiB

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

## Step 2:- Creating load balancer

**Load balancers**

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

[Filter load balancers](#)

Name	DNS name	State	VPC ID	Availability Zones	Type	Date crea
No load balancers You don't have any load balancers in ap-south-1						

[Create load balancer](#)

**0 load balancers selected**

Select a load balancer above.

----select required load balancer as shown

aws Search [Alt+S]

EC2 VPC S3 IAM Support

EC2 > Load balancers > Compare and select load balancer type

### Compare and select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

#### 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](#)

► Classic Load Balancer - previous generation

-----Selecting all AZ's

aws Search [Alt+S]

EC2 VPC S3 IAM Support

EC2 > Load balancers > Create Application Load Balancer

### Network mapping

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

**VPC** Info  
The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#). For a new VPC, [create a VPC](#).

vpc-0077c08100707167e  
IPv4 VPC CIDR: 172.31.0.0/16

**IP pools - new** Info  
You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view Pools in [Amazon VPC IP Address Manager console](#).

☐ Use IPAM pool for public IPv4 addresses  
The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

**Availability Zones and subnets** Info  
Select a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

ap-south-1a (aps1-az1)

ap-south-1b (aps1-az3)

ap-south-1c (aps1-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

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## -----selecting the security group we created

The screenshot shows the AWS Management Console interface for creating an Application Load Balancer. The page is titled "Create Application Load Balancer" and is located under the "Load balancers" section. The "Subnet" dropdown is set to "subnet-022b390090e2a32de". The "Security groups" section is highlighted with a black box, showing a dropdown menu with "alltraffic" selected. The "Listeners and routing" section shows a listener for HTTP:80 with a default action of "Forward to".

**Subnet**  
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.  
subnet-022b390090e2a32de  
IPv4 subnet CIDR: 172.31.16.0/20

**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](#).

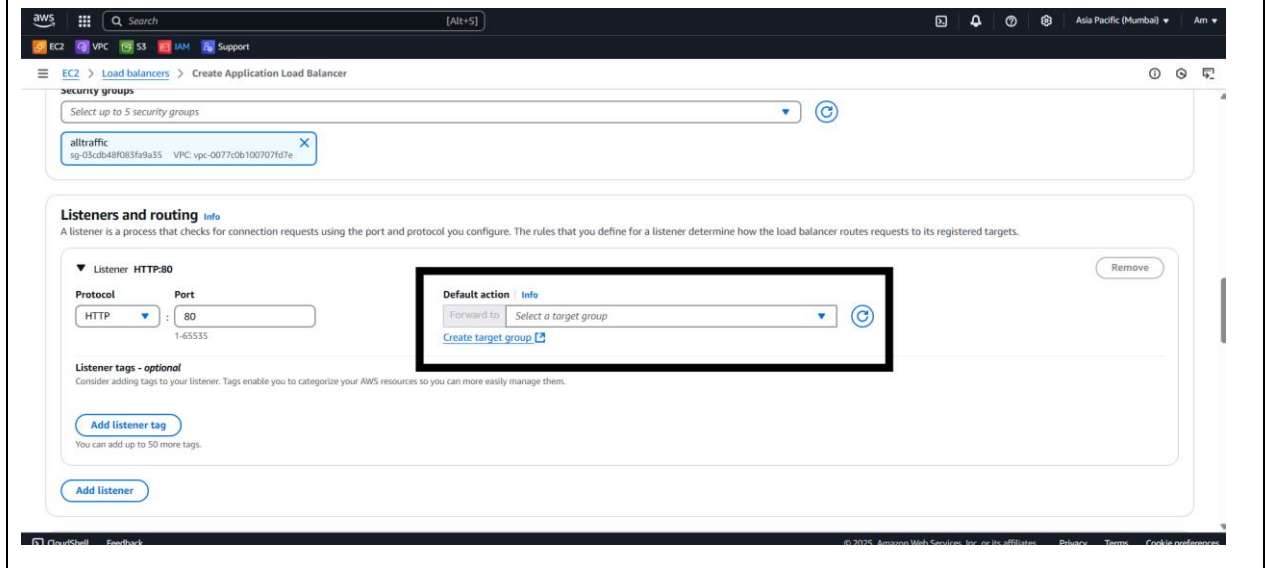
**Security groups**  
Select up to 5 security groups  
alltraffic  
sg-03cbb48f083fa9a35 VPC: vpc-0077c0b10070767e

**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.

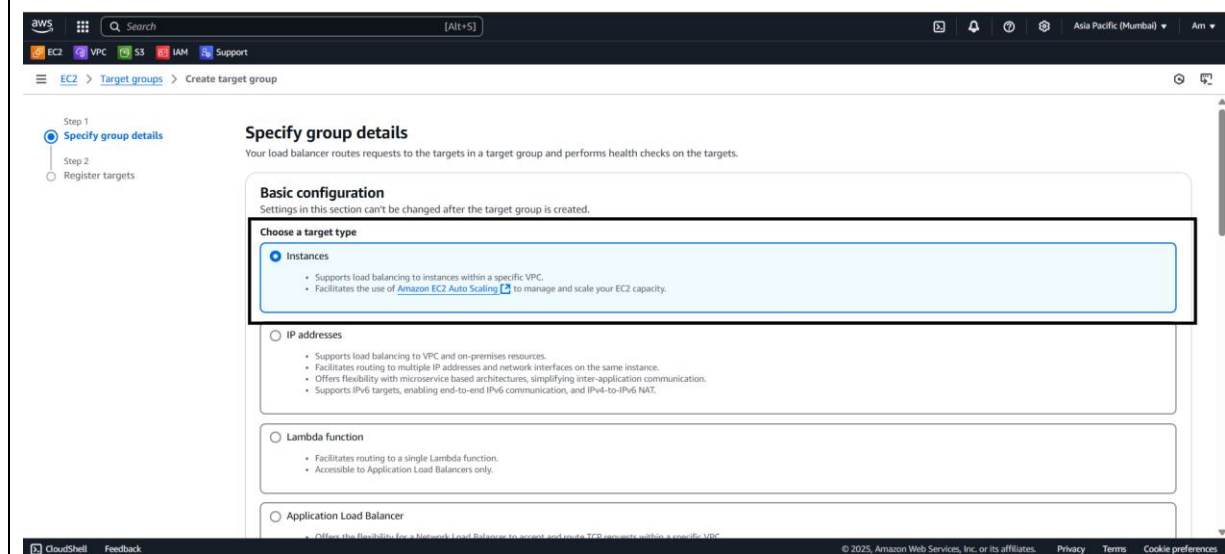
**Listener HTTP:80** [Remove](#)  
Protocol: HTTP Port: 80  
Default action: [Info](#)  
Forward to: Select a target group  
[Create target group](#)

Listener tags - optional

## -----create target group(use if already exist)



## ---as we are creating with instance select instance



## ---name it and select http port

**Target group name**  
my-TG  
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

**Protocol : Port**  
Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation.  
HTTP 80  
1-65535

**IP address type**  
Only targets with the indicated IP address type can be registered to this target group.  
☒ IPv4  
Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.  
☐ IPv6  
Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

**VPC**  
Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.  
vpc-0077c0b100707fd7e  
IPv4 VPC CIDR: 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.

## -----register targets and click on include as pending below

**Register targets**  
This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

**Available instances (2/2)**  
Filter instances

<input checked="" type="checkbox"/>	Instance ID	Name	State	Security groups	Zone	Private IPv4
<input checked="" type="checkbox"/>	i-07c111218203e9849	ec2_load balancer	Running	alltraffic	ap-south-1b	172.31.8.17
<input checked="" type="checkbox"/>	i-0eb6d9cb65d7746fb	ec2_load balancer	Running	alltraffic	ap-south-1b	172.31.0.12

2 selected

Ports for the selected instances  
Ports for routing traffic to the selected instances.  
80  
1-65535 (separate multiple ports with commas)  
[Include as pending below](#)

## ----click on create target group

**Review targets**

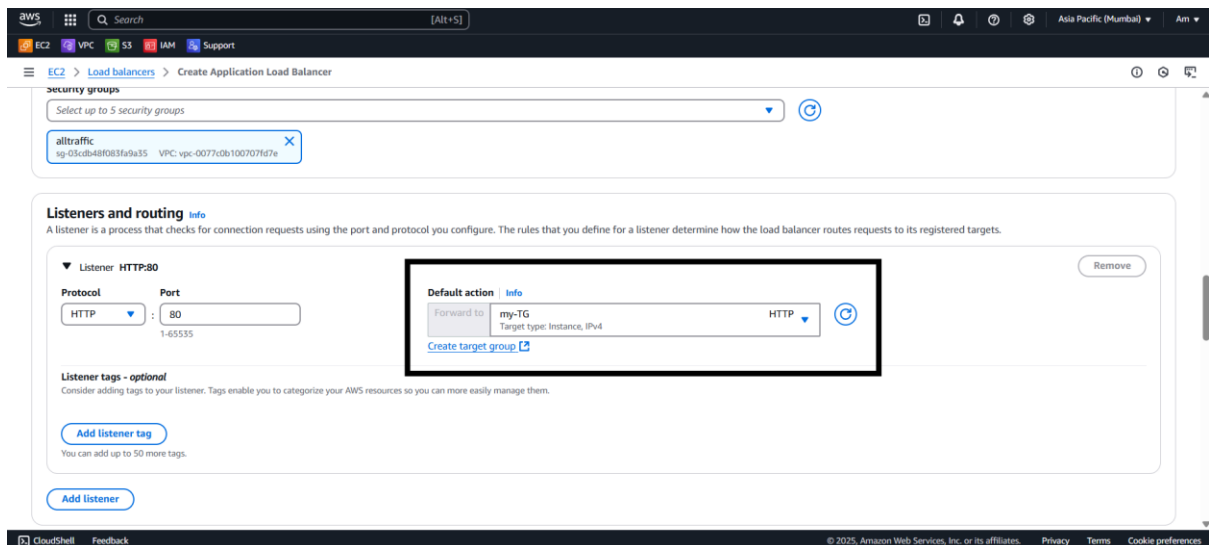
**Targets (2)**  
Filter targets Show only pending Remove all pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-07c111218203e9849	ec2_load balancer	80	Running	alltraffic	ap-south-1b	172.31.8.173	subnet-057311227b8b41e9b	April 5, 202
i-0eb6d9cb65d7746fb	ec2_load balancer	80	Running	alltraffic	ap-south-1b	172.31.0.128	subnet-057311227b8b41e9b	April 5, 202

2 pending

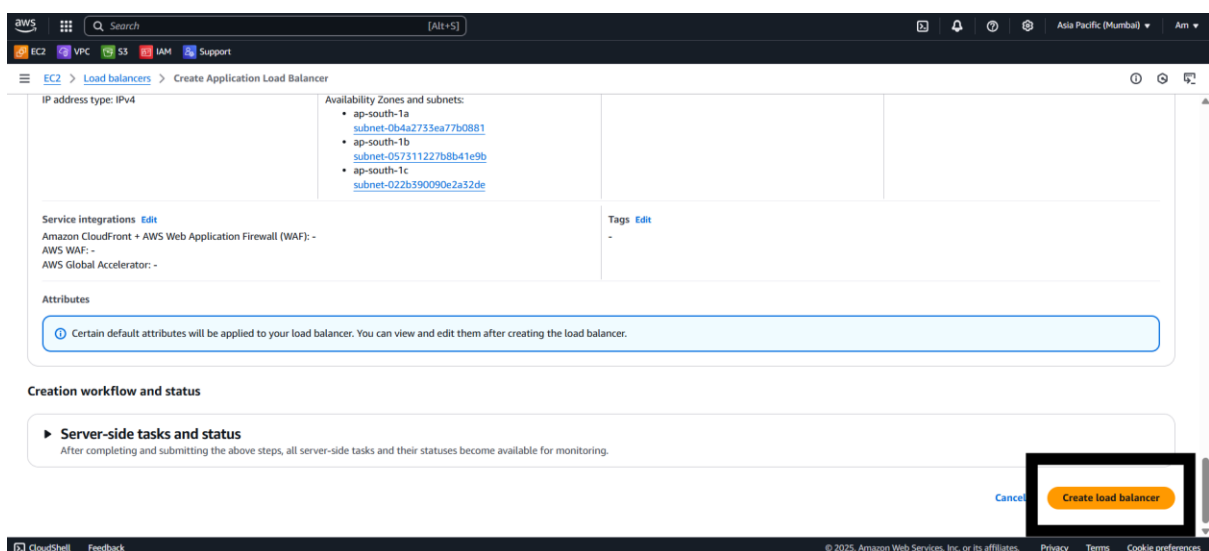
[Cancel](#) [Previous](#) [Create target group](#)

## ----select target group in load balancer screen now



The screenshot shows the AWS Management Console interface for creating an Application Load Balancer. The 'Listeners and routing' section is active, showing a listener named 'Listener HTTP:80' with protocol 'HTTP' and port '80'. The 'Default action' dropdown menu is highlighted with a red box, showing the selected target group 'my-TG' and the option to 'Create target group'. The 'Listener tags - optional' section is also visible, with an 'Add listener tag' button.

## ----create load balance now



The screenshot shows the 'Creation workflow and status' section of the 'Create Application Load Balancer' page. The 'Server-side tasks and status' section is expanded, showing the progress of the load balancer creation. The 'Create load balancer' button is highlighted with a red box, indicating the final step in the process.

# ---connect ssh to git

aws [Search] [Alt+S]

EC2 VPC S3 IAM Support

EC2 > Instances > i-07c111218203e9849 > Connect to instance

### Connect to instance Info

Connect to your instance i-07c111218203e9849 (ec2\_load balancer) using any of these options

EC2 Instance Connect Session Manager **SSH client** EC2 serial console

Instance ID  
i-07c111218203e9849 (ec2\_load balancer)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is Mumbai\_keypair.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.  
chmod 400 "Mumbai\_keypair.pem"
4. Connect to your instance using its Public DNS:  
ec2-13-203-76-120.ap-south-1.compute.amazonaws.com

Example:  
ssh -i "Mumbai\_keypair.pem" ubuntu@ec2-13-203-76-120.ap-south-1.compute.amazonaws.com

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel

```
ubuntu@ip-172-31-8-173: ~
* Documentation: https://help.ubuntu.com
* Management:   https://landscape.canonical.com
* Support:       https://ubuntu.com/pro

System information as of Sat Apr  5 13:05:04 UTC 2025

System load:  0.0          Processes:    106
Usage of /:   28.5% of 6.71GB Users logged in:  0
Memory usage: 22%          IPv4 address for enx0: 172.31.8.173
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

60 updates can be applied immediately.
34 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-8-173:~$ |
```



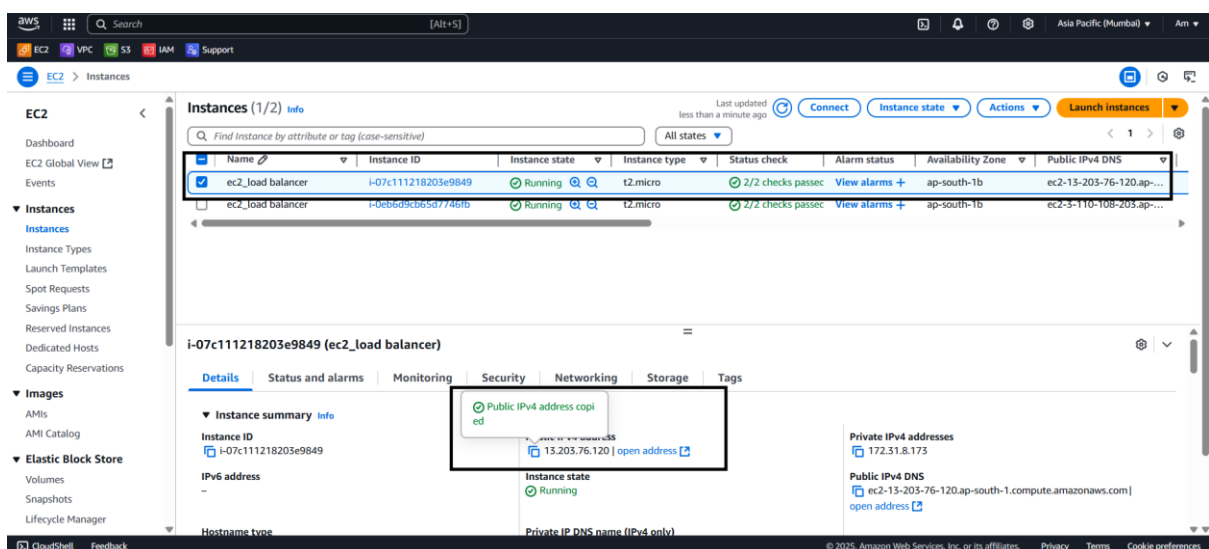
## --check nginx is working

```
root@ip-172-31-8-173: ~  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-172-31-8-173:~$ sudo -i  
root@ip-172-31-8-173:~# system status nginx  
Command 'system' not found, did you mean:  
  command 'systemd' from deb systemd (255.4-1ubuntu8.6)  
  command 'system3' from deb simh (3.8.1-6.1)  
Try: apt install <deb name>  
root@ip-172-31-8-173:~# systemctl status nginx  
● nginx.service - A high performance web server and a reverse proxy server  
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)  
   Active: active (running) since Sat 2025-04-05 12:36:19 UTC; 29min ago  
     Docs: man:nginx(8)  
  Main PID: 1534 (nginx)  
    Tasks: 2 (limit: 1129)  
   Memory: 1.8M (peak: 2.0M)  
      CPU: 16ms  
   CGroup: /system.slice/nginx.service  
           └─1534 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"  
             └─1535 "nginx: worker process"  
  
Apr 05 12:36:19 ip-172-31-8-173 systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy server:  
Apr 05 12:36:19 ip-172-31-8-173 systemd[1]: Started nginx.service - A high performance web server and a reverse proxy server:  
lines 1-14/14 (END)
```

## ---using command writing custom message for proxy server nginx

```
root@ip-172-31-8-173:~#  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-172-31-8-173:~$ sudo -i  
root@ip-172-31-8-173:~# system status nginx  
Command 'system' not found, did you mean:  
  command 'systemd' from deb systemd (255.4-1ubuntu8.6)  
  command 'system3' from deb simh (3.8.1-6.1)  
Try: apt install <deb name>  
root@ip-172-31-8-173:~# systemctl status nginx  
● nginx.service - A high performance web server and a reverse proxy server  
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)  
   Active: active (running) since Sat 2025-04-05 12:36:19 UTC; 29min ago  
     Docs: man:nginx(8)  
    Main PID: 1534 (nginx)  
      Tasks: 2 (limit: 1129)  
    Memory: 1.8M (peak: 2.0M)  
       CPU: 16ms  
    CGroup: /system.slice/nginx.service  
            └─1534 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"  
            └─1535 "nginx: worker process"  
  
Apr 05 12:36:19 ip-172-31-8-173 systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy server:  
Apr 05 12:36:19 ip-172-31-8-173 systemd[1]: Started nginx.service - A high performance web server and a reverse proxy server:  
  
root@ip-172-31-8-173:~#  
root@ip-172-31-8-173:~#  
root@ip-172-31-8-173:~# cat >> /var/www/html/nginx.services  
Hello world
```

## ---selecting one instance and trying to connect to proxy server nginx



----This page should open after accessing public IP for both instances



## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](https://nginx.org).  
Commercial support is available at [nginx.com](https://nginx.com).

*Thank you for using nginx.*