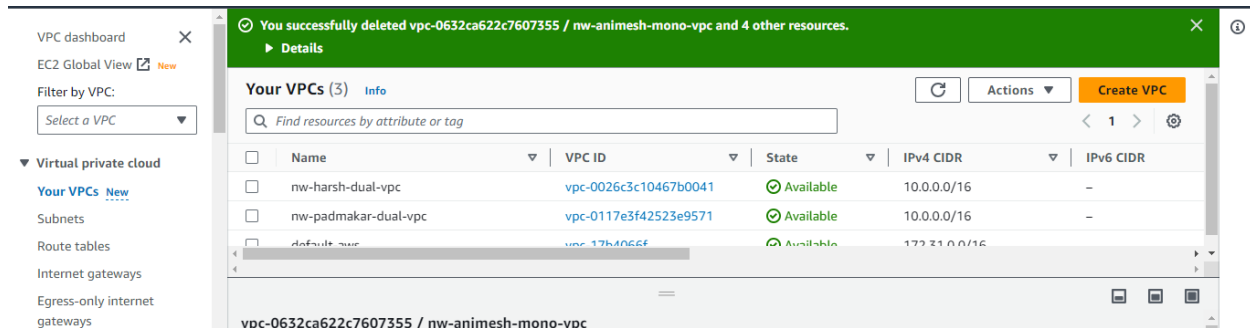
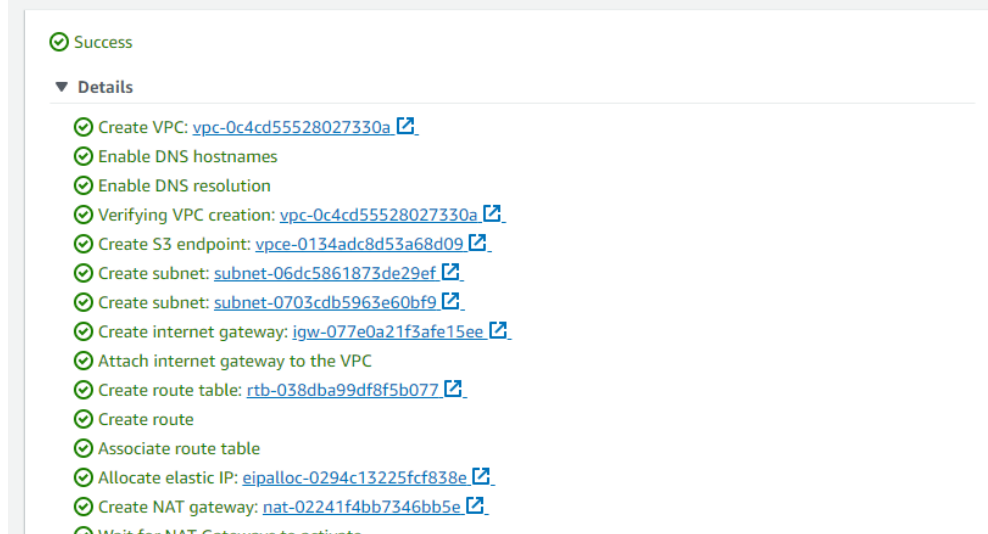


## Creating Vpc's



After configuration


## Create VPC workflow




## Edit subnet settings [Info](#)

### Subnet

Subnet ID

 subnet-06dc5861873de29ef

Name

 nw-animesh-dual-subnet-public1-us-west-2a

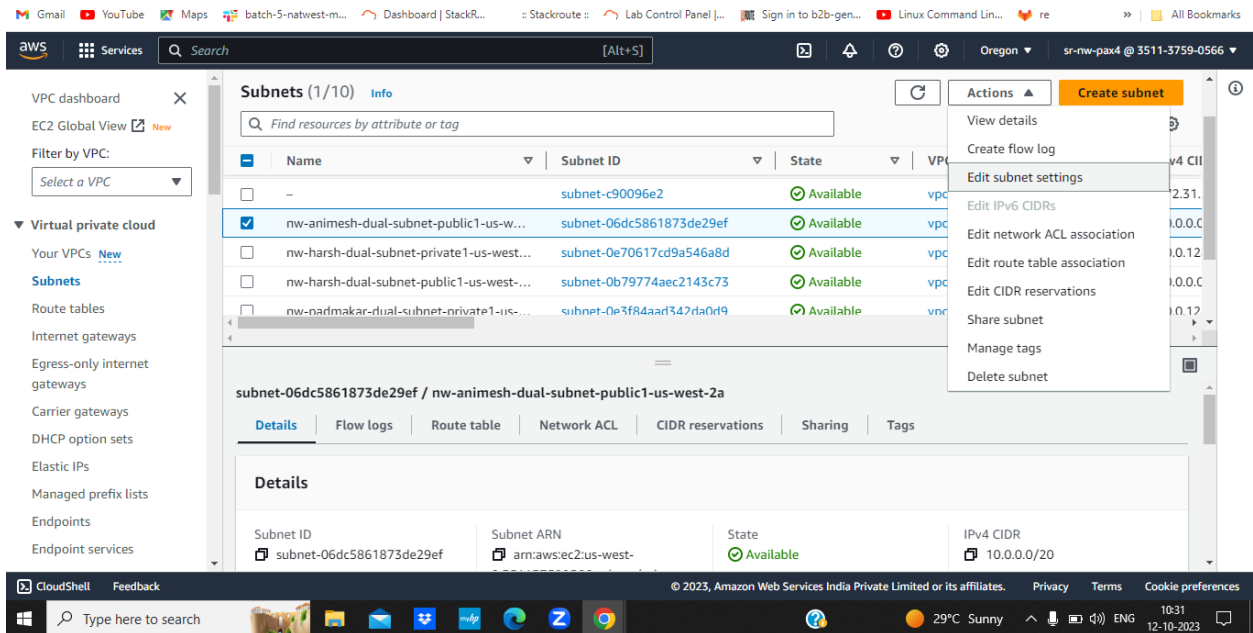
### Auto-assign IP settings [Info](#)

Enable the auto-assign IP settings to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

☒ Enable auto-assign public IPv4 address [Info](#)

☐ Enable auto-assign customer-owned IPv4 address [Info](#)  
Option disabled because no customer owned pools found.

## Edit subnet



The screenshot shows the AWS Management Console interface. The left sidebar displays the 'Virtual private cloud' section with 'Subnets' selected. The main content area shows a list of subnets. The subnet 'nw-animesh-dual-subnet-public1-us-west-2a' (ID: subnet-06dc5861873de29ef) is selected. The 'Actions' menu is open, showing options like 'View details', 'Create flow log', 'Edit subnet settings', etc. The 'Edit subnet settings' option is highlighted. Below the menu, the details for the selected subnet are shown, including its ID, ARN, state (Available), and IPv4 CIDR (10.0.0.0/20).

Name	Subnet ID	State	VPC
-	subnet-c90096e2	Available	vpc-
nw-animesh-dual-subnet-public1-us-west-2a	subnet-06dc5861873de29ef	Available	vpc-
nw-harsh-dual-subnet-private1-us-west-2a	subnet-0e70617cd9a546a8d	Available	vpc-
nw-harsh-dual-subnet-public1-us-west-2a	subnet-0b79774aec2143c73	Available	vpc-
nw-narlmakar-dual-subnet-private1-us-west-2a	subnet-0e3f84aad347da0d9	Available	vpc-

subnet-06dc5861873de29ef / nw-animesh-dual-subnet-public1-us-west-2a

Details

Subnet ID	Subnet ARN	State	IPv4 CIDR
subnet-06dc5861873de29ef	arn:aws:ec2:us-west-2:3511-3759-0566:subnet/subnet-06dc5861873de29ef	Available	10.0.0.0/20

## Save the setting

### DNS64 settings

Enable DNS64 to allow IPv6-only services in Amazon VPC to communicate with IPv4-only services and networks.

☐ Enable DNS64 [Info](#)

Cancel

Save

You have successfully changed subnet settings:

- Enable auto-assign public IPv4 address

Subnets (10) [Info](#)

Find resources by attribute or tag

Actions

Create subnet

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	nw-animesh-dual-subnet-public1-us-w...	subnet-06dc5861873de29ef	Available	vpc-0c4cd55528027330a   nw-...	10.0.0.0/24
<input type="checkbox"/>	nw-harsh-dual-subnet-private1-us-west...	subnet-0e70617cd9a546a8d	Available	vpc-0026c3c10467b0041   nw-...	10.0.128.0/24

Click on security groups

## ▼ Security

Network ACLs

Security groups

aws

Services

Search

[Alt+S]

Oregon

sr-nw-pax4 @ 3511-3759-0566

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

▼ Security

Network ACLs

Security groups

▼ DNS firewall

Rule groups

Domain lists

▼ Network Firewall

Firewalls

Firewall policies

Security Groups (9) [Info](#)

Filter security groups

Actions

Export security groups to CSV

Create security group

<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description
<input type="checkbox"/>	-	sg-0a1ef4a5d3841a637	launch-wizard-2	vpc-17b4066f	launch-wizard-2 create...
<input type="checkbox"/>	-	sg-0e63c6e5ec54051b	default	vpc-0117e3f42523e9571	default VPC security gr...
<input type="checkbox"/>	-	sg-01f136997c14fda75	default	vpc-0026c3c10467b0041	default VPC security gr...
<input type="checkbox"/>	-	sg-0e991eac05504c482	nw-padmaakar-custo...	vpc-0117e3f42523e9571	Allow access
<input type="checkbox"/>	-	sg-0170d5f3ph3e28rce	launch-wizard-1	vpc-17b4066f	launch-wizard-1 create...

[VPC](#) > [Security Groups](#) > Create security group

## Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group

### Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

## Giving name

### Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

#### Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)



Checking inbound rule

Inbound rules Info

Type Info

Protocol Info

Port range Info

Source Info

Description - optional Info

All traffic ▼

All

All

Cus... ▼

Q

sg-0a2346b1118016a99 X

Delete

SSH ▼

TCP

22

My IP ▼

Q

112.79.109.177/32 X

Delete

Add rule

Click on create security

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags

Cancel Create security group

Inbound rules

Inbound rules (2)

Q Filter security group rules

< 1 > ⚙

<input type="checkbox"/>	Name ▼	Security group rule... ▼	IP version ▼	Type ▼	Protocol ▼
<input type="checkbox"/>	-	sgr-0b908f01725b364...	-	All traffic	All
<input type="checkbox"/>	-	sgr-0f5ba6b2a71718624	IPv4	SSH	TCP

Virtual private cloud

Virtual private cloud

Your VPCs [New](#)

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

VPC > Security Groups > sg-0b3aa68850b94adfa - nw-animesh-custom-sg

sg-0b3aa68850b94adfa - nw-animesh-custom-sg

Actions

Details

Security group name	Security group ID	Description	VPC ID
nw-animesh-custom-sg	sg-0b3aa68850b94adfa	custom sg	vpc-0c4cd55528027330a
Owner	Inbound rules count	Outbound rules count	
351137590566	2 Permission entries	1 Permission entry	

Inbound rules Outbound rules Tags

Inbound rules (2)

Filter security group rules

Manage tags Edit inbound rules

## Doing network setting for public sg

Network settings

VPC - required

vpc-0c4cd55528027330a (nw-animesh-dual-vpc)

10.0.0.0/16

Subnet

subnet-06dc5861873de29ef nw-animesh-dual-subnet-public1-us-west-2a

VPC: vpc-0c4cd55528027330a Owner: 351137590566

Availability Zone: us-west-2a IP addresses available: 4090 CIDR: 10.0.0.0/20

Auto-assign public IP

Enable

Firewall (security groups)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

## Select security groups

Auto-assign public IP [Info](#)

Enable

**Firewall (security groups)** [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group


☒ Select existing security group

Common security groups [Info](#)

Select security groups

nw-animesh-custom-sg sg-0b3aa68850b94adfa ✕  
VPC: vpc-0c4cd55528027330a

default sg-0a2346b1118016a99 ✕  
VPC: vpc-0c4cd55528027330a


 [Compare security group rules](#)

 [Hide all selected](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

## Launch an instance

[EC2](#) > [Instances](#) > Launch an instance

 **Success**  
Successfully initiated launch of instance ([i-092c4636477154b92](#))

▶ Launch log

Next Steps

< 1 2 3 4 5 6 >

Create billing and free tier usage alerts  
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.  
[Create billing alerts](#)

Connect to your instance  
Once your instance is running, log into it from your local computer.  
[Connect to instance](#)  
[Learn more](#)

Connect an RDS database  
Configure the connection between an EC2 instance and a database to allow traffic flow between them.  
[Connect an RDS database](#)  
[Create a new RDS database](#)

Create EBS snapshot policy  
Create a policy that automates the creation, retention, and deletion of EBS snapshots.  
[Create EBS snapshot policy](#)

[EC2](#) > [Instances](#) > Launch an instance

## Launch an instance [Info](#)

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 [Info](#)

Name

*e.g. My Web Server*

[Add additional tags](#)

## Private 1

VPC - required [Info](#)

vpc-0c4cd55528027330a (nw-animesh-dual-vpc)  
10.0.0.0/16



Subnet [Info](#)

subnet-0703cdb5963e60bf9 nw-animesh-dual-subnet-private1-us-west-2a  
VPC: vpc-0c4cd55528027330a Owner: 351137590566  
Availability Zone: us-west-2a IP addresses available: 4091 CIDR: 10.0.128.0/20



[Create new subnet](#)

Auto-assign public IP [Info](#)

Disable



Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group

☒ Select existing security group

Common security groups [Info](#)

Select security groups



default sg-0a2346b1118016a99 X  
VPC: vpc-0c4cd55528027330a



[Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.



[EC2](#) > [Instances](#) > Launch an instance

## Launch an instance [Info](#)

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 [Info](#)

Name

*e.g. My Web Server*

[Add additional tags](#)

### VPC - required [Info](#)

vpc-0c4cd55528027330a (nw-animesh-dual-vpc)  
10.0.0.0/16



### Subnet [Info](#)

subnet-0703cdb5963e60bf9 nw-animesh-dual-subnet-private1-us-west-2a  
VPC: vpc-0c4cd55528027330a Owner: 351137590566  
Availability Zone: us-west-2a IP addresses available: 4091 CIDR: 10.0.128.0/20



[Create new subnet](#)

### Auto-assign public IP [Info](#)

Disable



### Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group

☒ Select existing security group

### Common security groups [Info](#)

Select security groups



default sg-0a2346b1118016a99 X  
VPC: vpc-0c4cd55528027330a

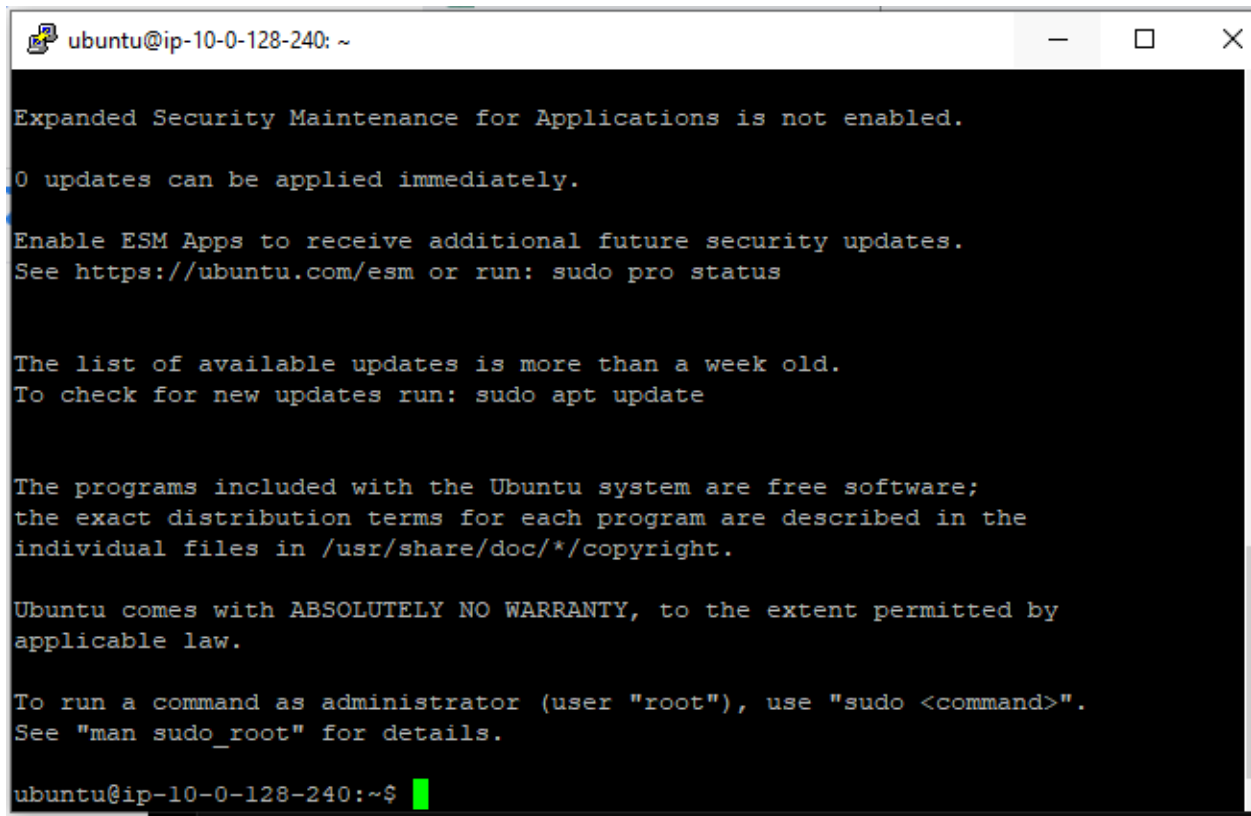


[Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

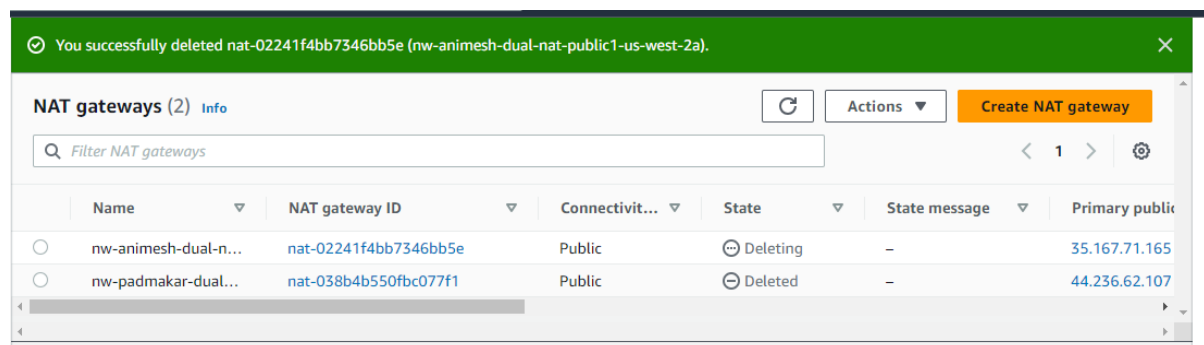
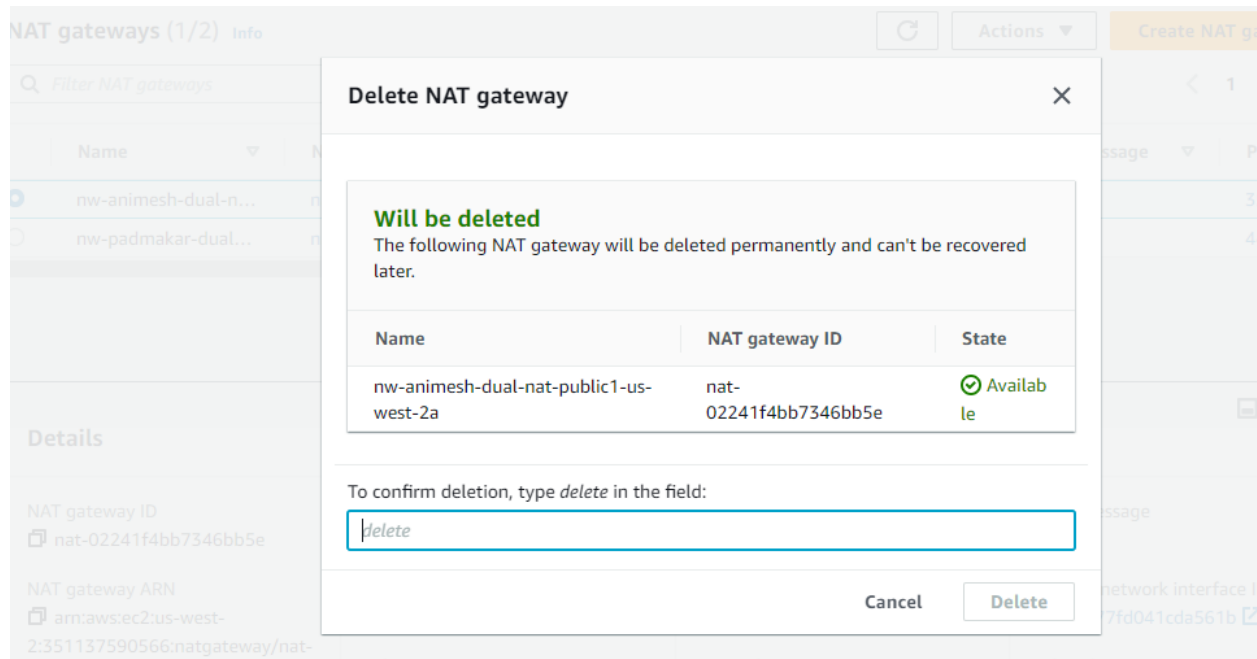
Connecting with localhost

Able to connect with one network other

A terminal window titled 'ubuntu@ip-10-0-128-240: ~' with standard window controls. The terminal displays several system messages in a monospaced font. The messages include information about security updates, ESM (Expanded Security Maintenance) status, update availability, software licensing, warranty, and the use of sudo. The prompt 'ubuntu@ip-10-0-128-240:~\$' is visible at the bottom with a green cursor.

```
ubuntu@ip-10-0-128-240: ~  
  
Expanded Security Maintenance for Applications is not enabled.  
  
0 updates can be applied immediately.  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
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-10-0-128-240:~$
```

After deleting it we cannot connect



Will show below error message

```
ubuntu@workspace: ~  
--- google.com ping statistics ---  
5 packets transmitted, 0 received, 100% packet loss, time 4090ms  
  
ubuntu@ip-10-0-128-240:~$ ls  
ubuntu@ip-10-0-128-240:~$ exit  
logout  
Connection to 10.0.128.240 closed.  
ubuntu@workspace:~$ ping -c 5 google.com  
PING google.com (142.251.33.110) 56(84) bytes of data.  
64 bytes from sea30s10-in-fl4.1e100.net (142.251.33.110): icmp_seq=1 ttl=96 time  
=6.93 ms  
64 bytes from sea30s10-in-fl4.1e100.net (142.251.33.110): icmp_seq=2 ttl=96 time  
=7.03 ms  
64 bytes from sea30s10-in-fl4.1e100.net (142.251.33.110): icmp_seq=3 ttl=96 time  
=7.01 ms  
64 bytes from sea30s10-in-fl4.1e100.net (142.251.33.110): icmp_seq=4 ttl=96 time  
=7.01 ms  
64 bytes from sea30s10-in-fl4.1e100.net (142.251.33.110): icmp_seq=5 ttl=96 time  
=7.01 ms  
  
--- google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 6.934/6.998/7.027/0.032 ms  
ubuntu@workspace:~$
```

```
ubuntu@workspace: ~  
--- google.com ping statistics ---  
5 packets transmitted, 0 received, 100% packet loss, time 4090ms  
  
ubuntu@ip-10-0-128-240:~$ ls  
ubuntu@ip-10-0-128-240:~$ exit  
logout  
Connection to 10.0.128.240 closed.  
ubuntu@workspace:~$ ping -c 5 google.com  
PING google.com (142.251.33.110) 56(84) bytes of data.  
64 bytes from sea30s10-in-fl4.1e100.net (142.251.33.110): icmp_seq=1 ttl=96 time  
=6.93 ms  
64 bytes from sea30s10-in-fl4.1e100.net (142.251.33.110): icmp_seq=2 ttl=96 time  
=7.03 ms  
64 bytes from sea30s10-in-fl4.1e100.net (142.251.33.110): icmp_seq=3 ttl=96 time  
=7.01 ms  
64 bytes from sea30s10-in-fl4.1e100.net (142.251.33.110): icmp_seq=4 ttl=96 time  
=7.01 ms  
64 bytes from sea30s10-in-fl4.1e100.net (142.251.33.110): icmp_seq=5 ttl=96 time  
=7.01 ms  
  
--- google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 6.934/6.998/7.027/0.032 ms  
ubuntu@workspace:~$
```

## Deleting elastic ip

aws Services Search [Alt+S] Oregon sr-nw-pax4 @ 3511-3759-0566

▼ Images  
AMIs  
AMI Catalog

▼ Elastic Block Store  
Volumes  
Snapshots  
Lifecycle Manager

▼ Network & Security  
Security Groups  
**Elastic IPs**  
Placement Groups  
Key Pairs  
Network Interfaces

▼ Load Balancing  
Load Balancers  
Target Groups

### Elastic IP addresses (1/1)

Filter Elastic IP addresses

<input checked="" type="checkbox"/>	Name	Allocated IPv4 add...	Type	Allocation ID	Reverse DN
<input checked="" type="checkbox"/>	nw-animesh-dual-eip-us-west-2a	35.167.71.165	Public IP	eipalloc-0294c13225fcf838e	-

Association ID  
-

Scope  
VPC

Associated instance ID  
-

Private IP address  
-

Network interface ID  
-

Network interface owner account ID  
-

Public DNS  
-

NAT Gateway ID  
-

Address pool  
Amazon

Network Border Group  
us-west-2

Filter by VPC:  
Select a VPC

▼ Virtual private cloud  
Your VPCs New  
Subnets  
Route tables  
Internet gateways  
Egress-only Internet gateways  
DHCP option sets  
**Elastic IPs**  
Managed prefix lists

### Elastic IP addresses (2)

Filter Elastic IP addresses

<input type="checkbox"/>	Name	Allocated IPv4 add...	Type
<input type="checkbox"/>	nw-moni-dual-eip-us-east-2a	3.130.144.125	Public IP
<input type="checkbox"/>	nw-mayank-dual-eip-us-east-2a	3.135.91.181	Public IP

View details

Release Elastic IP addresses

Associate Elastic IP address

Disassociate Elastic IP address

Update reverse DNS

Enable transfers

Disable transfers

Accept transfers

2fa716373fbf  
f986316fe90d