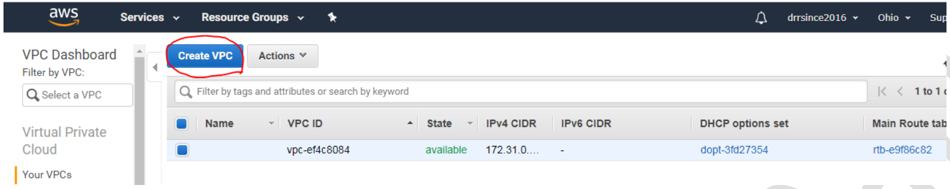
# Amazon Virtual Private Cloud

https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

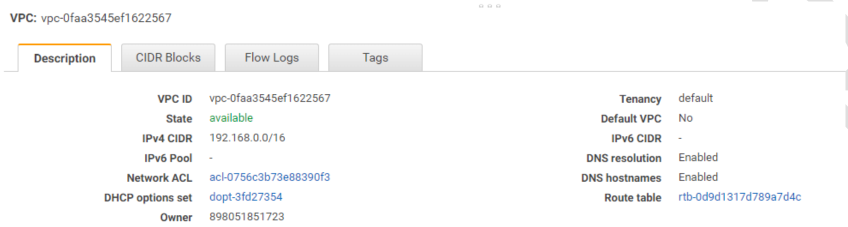
Amazon Virtual Private Cloud (Amazon VPC) enables you to define a virtual network in your own logically isolated area within the AWS cloud, known as a virtual private cloud (VPC). You can launch your Amazon EC2 resources, such as instances, into the subnets of your VPC. Your VPC closely resembles a traditional network that you might operate in your own data center, with the benefits of using scalable infrastructure from AWS. You can configure your VPC; you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings. You can connect instances in your VPC to the internet or to your own data center.

Step1:-Create new VPC

@Click Create VPC → enter the name tag and ip range with subnets → click on Create.

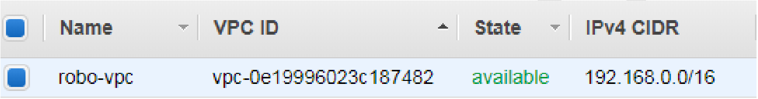


| Name | VPC ID | State | IPv4 CIDR | IPv6 CIDR | DHCP options set | Main Route tab |
|---|---|---|---|---|---|---|
| | vpc-ef4c8084 | available | 172.31.0.... | - | dopt-3fd27354 | rtb-e9f86c82 |



VPC: vpc-0faa3545ef1622567

| | | | |
|---|---|---|---|
| VPC ID | vpc-0faa3545ef1622567 | Tenancy | default |
| State | available | Default VPC | No |
| IPv4 CIDR | 192.168.0.0/16 | IPv6 CIDR | - |
| IPv6 Pool | - | DNS resolution | Enabled |
| Network ACL | acl-0756c3b73e88390f3 | DNS hostnames | Enabled |
| DHCP options set | dopt-3fd27354 | Route table | rtb-0d9d1317d789a7d4c |
| Owner | 898051851723 | | |

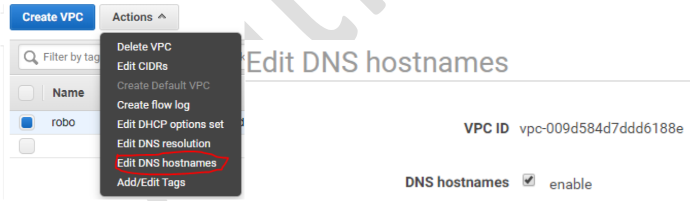


| Name | VPC ID | State | IPv4 CIDR |
|---|---|---|---|
| robo-vpc | vpc-0e19996023c187482 | available | 192.168.0.0/16 |

**Step1.1:- Using DNS with Your VPC**

Domain Name System (DNS) is a standard by which names used on the Internet are resolved to their corresponding IP addresses. A DNS hostname is a name that uniquely and absolutely names a computer; it's composed of a host name and a domain name. DNS servers resolve DNS hostnames to their corresponding IP addresses.

@Click on Actions → Edit DNS hostnames →select the enable →save



Edit DNS hostnames

VPC ID vpc-009d584d7ddd6188e

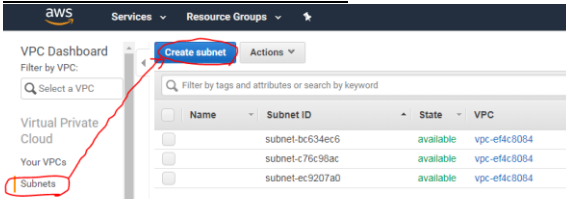
DNS hostnames ☑ enable

**Step2:-Create two subnets for public and private.**

Public :- If a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet.

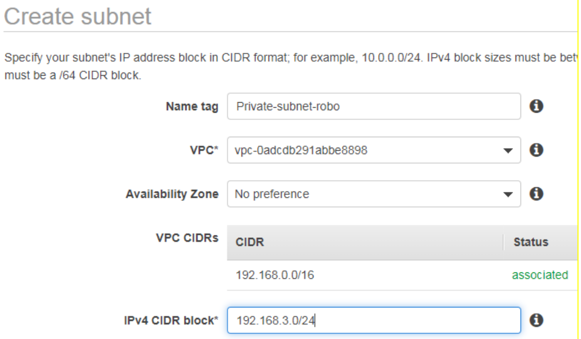
Private:- If a subnet doesn't have a route to the internet gateway, the subnet is known as a private subnet.

:-Click on Subnets → Create subnet



| Name | Subnet ID | State | VPC |
|---|---|---|---|
| | subnet-bc634ec6 | available | vpc-ef4c8084 |
| | subnet-c76c98ac | available | vpc-ef4c8084 |
| | subnet-ec9207a0 | available | vpc-ef4c8084 |

@Enter Name tag→ Select zone →enter CIDR block



Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be bet must be a /64 CIDR block.

Name tag: Private-subnet-robo

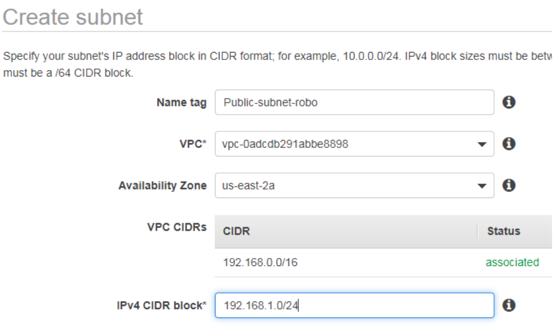
VPC*: vpc-0adcdb291abbe8898

Availability Zone: No preference

VPC CIDRs

| CIDR | Status |
|---|---|
| 192.168.0.0/16 | associated |

IPv4 CIDR block*: 192.168.3.0/24



Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be betw must be a /64 CIDR block.

Name tag: Public-subnet-robo

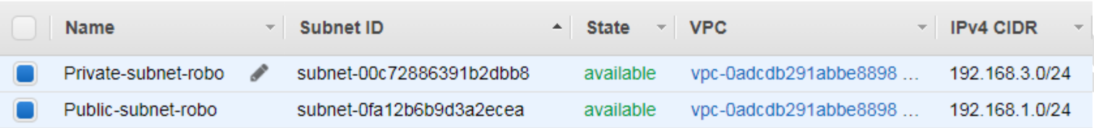
VPC*: vpc-0adcdb291abbe8898

Availability Zone: us-east-2a

VPC CIDRs

| CIDR | Status |
|---|---|
| 192.168.0.0/16 | associated |

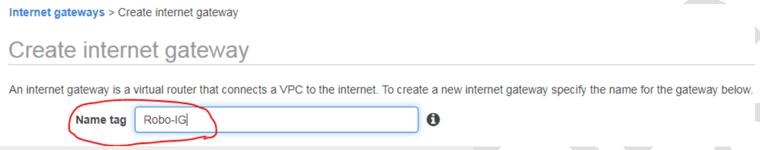
IPv4 CIDR block*: 192.168.1.0/24



| Name | Subnet ID | State | VPC | IPv4 CIDR |
|---|---|---|---|---|
| Private-subnet-robo | subnet-00c72886391b2dbb8 | available | vpc-0adcdb291abbe8898 ... | 192.168.3.0/24 |
| Public-subnet-robo | subnet-0fa12b6b9d3a2ecea | available | vpc-0adcdb291abbe8898 ... | 192.168.1.0/24 |

**Step3:- Create an internet gateway and attach the same to VPC**

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. An internet gateway supports IPv4 and IPv6 traffic.

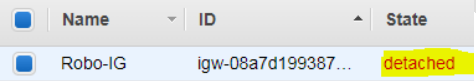


Internet gateways > Create internet gateway

Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

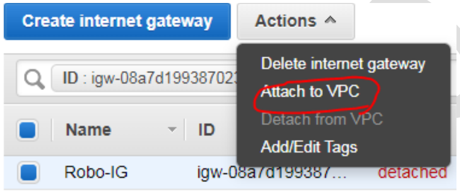
Name tag: Robo-IG



| Name | ID | State |
|---|---|---|
| Robo-IG | igw-08a7d199387... | detached |

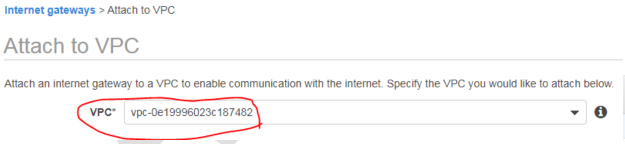
:-Now its in detached mode, after attach with VPC, it become attached mode.

@Click on Actions → Select Attach to VPC → Click Attach



ID : igw-08a7d19938702

| Name | ID | |
|---|---|---|
| Robo-IG | igw-08a7d199387... | detached |

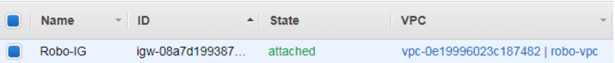


Internet gateways > Attach to VPC

Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

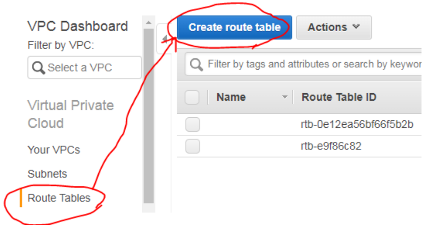
VPC*: vpc-0e19996023c187482



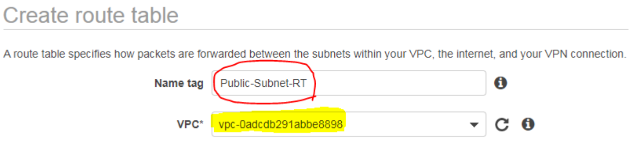
| Name | ID | State | VPC |
|---|---|---|---|
| Robo-IG | igw-08a7d199387... | attached | vpc-0e19996023c187482 \| robo-vpc |

Step4:-Create a route table Public and Private subnets with name standard.(Public-Subnet-RT | Private-Subnet-RT) and select the created VPC.

A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed.



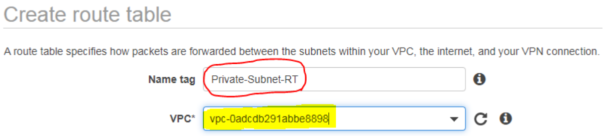
| Name | Route Table ID |
|---|---|
| | rtb-0e12ea56bf66f5b2b |
| | rtb-e9f86c82 |



Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

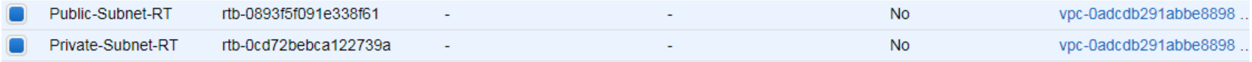
| | |
|---|---|
| Name tag | Public-Subnet-RT |
| VPC* | vpc-0adcdb291abbe8898 |



Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

| | |
|---|---|
| Name tag | Private-Subnet-RT |
| VPC* | vpc-0adcdb291abbe8898 |



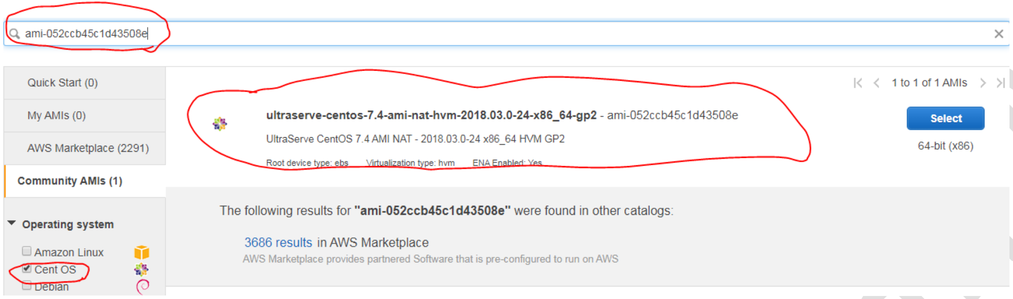
| | | | | | | |
|---|---|---|---|---|---|---|
| ■ | Public-Subnet-RT | rtb-0893f5f091e338f61 | - | - | No | vpc-0adcdb291abbe8898 .. |
| ■ | Private-Subnet-RT | rtb-0cd72bebca122739a | - | - | No | vpc-0adcdb291abbe8898 .. |

Step5:-Now create three instances (NAT instance | Public-subnet instance | Private-subnet instance)

Launch the EC2 instance with help of (AWS Launch-EC2instance.pdf)

@@5.1NAT instance

@Search for (ami-052ccb45c1d43508e) and click on Select



ami-052ccb45c1d43508e

**ultraserve-centos-7.4-ami-nat-hvm-2018.03.0-24-x86_64-gp2** - ami-052ccb45c1d43508e

UltraServe CentOS 7.4 AMI NAT - 2018.03.0-24 x86_64 HVM GP2

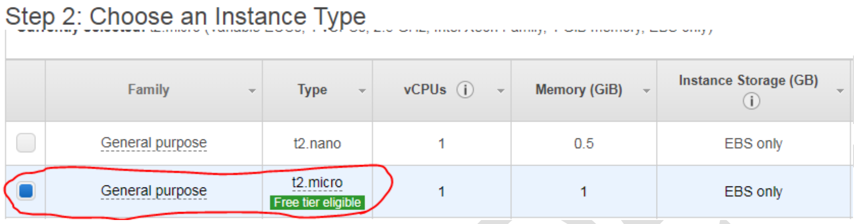
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86)

The following results for **"ami-052ccb45c1d43508e"** were found in other catalogs:

3686 results in AWS Marketplace

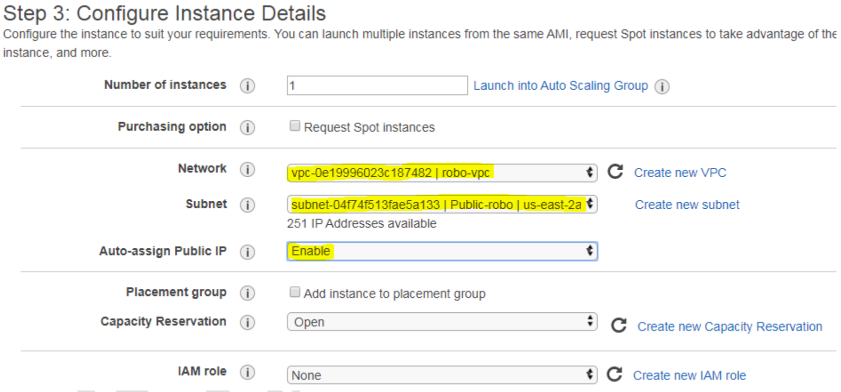
AWS Marketplace provides partnered Software that is pre-configured to run on AWS



Step 2: Choose an Instance Type

| | Family | Type | vCPUs | Memory (GiB) | Instance Storage (GB) |
|---|---|---|---|---|---|
| □ | General purpose | t2.nano | 1 | 0.5 | EBS only |
| ■ | General purpose | t2.micro<br>Free tier eligible | 1 | 1 | EBS only |

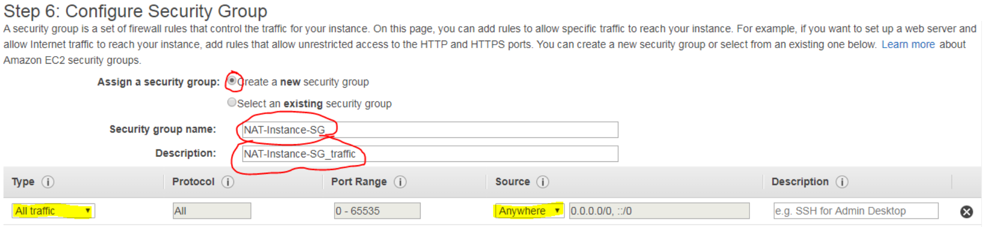
@Select Network VPC → then select Subnet → click on Enable for auto-assign-publicip



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 instance, and more.

| | |
|---|---|
| Number of instances | 1 — Launch into Auto Scaling Group |
| Purchasing option | □ Request Spot instances |
| Network | vpc-0e19996023c187482 \| robo-vpc — Create new VPC |
| Subnet | subnet-04f74f513fae5a133 \| Public-robo \| us-east-2a — Create new subnet<br>251 IP Addresses available |
| Auto-assign Public IP | Enable |
| Placement group | □ Add instance to placement group |
| Capacity Reservation | Open — Create new Capacity Reservation |
| IAM role | None — Create new IAM role |



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.

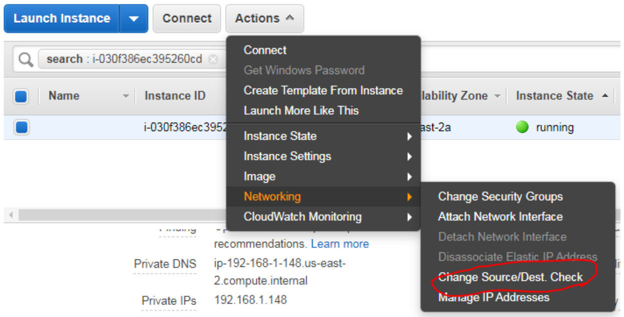
Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: NAT-Instance-SG

Description: NAT-Instance-SG_traffic

| Type | Protocol | Port Range | Source | | Description |
|---|---|---|---|---|---|
| All traffic | All | 0 - 65535 | Anywhere | 0.0.0.0/0, ::/0 | e.g. SSH for Admin Desktop |

@Once instance created, you have to disable the source and destination check.( By default its enabled)



Launch Instance | Connect | Actions

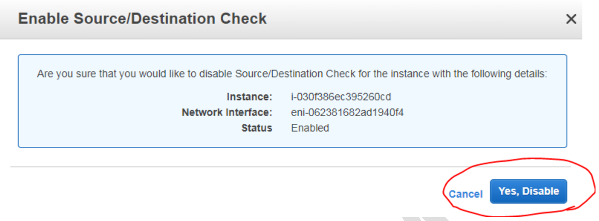
search : i-030f386ec395260cd

| Name | Instance ID | lability Zone | Instance State |
|---|---|---|---|
| | i-030f386ec3952 | ast-2a | running |

recommendations. Learn more

Private DNS ip-192-168-1-148.us-east-2.compute.internal

Private IPs 192.168.1.148

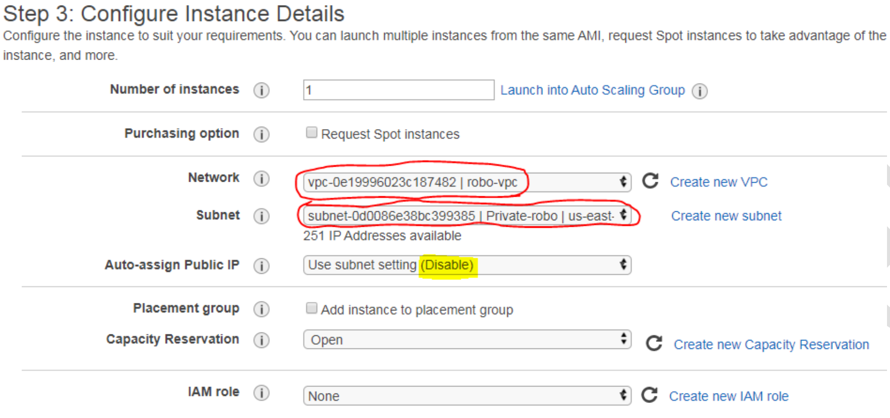


Enable Source/Destination Check ×

Are you sure that you would like to disable Source/Destination Check for the instance with the following details:

**Instance:** i-030f386ec395260cd
**Network Interface:** eni-062381682ad1940f4
**Status** Enabled

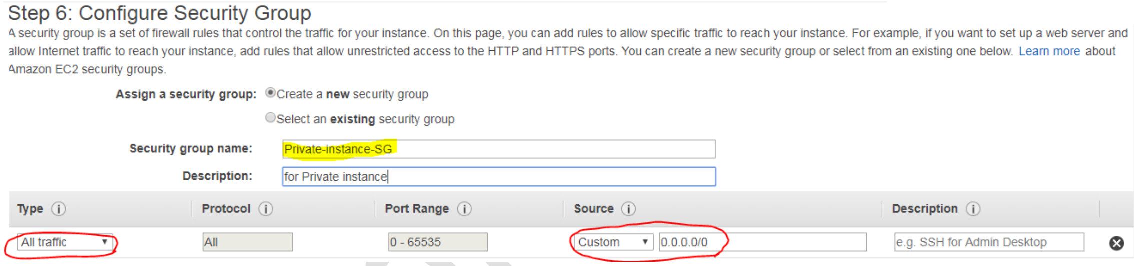
## Step5.2 Create normal centos EC2 private instance



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 instance, and more.

| | |
|---|---|
| **Number of instances** | 1 Launch into Auto Scaling Group |
| **Purchasing option** | □ Request Spot instances |
| **Network** | vpc-0e19996023c187482 \| robo-vpc — Create new VPC |
| **Subnet** | subnet-0d0086e38bc399385 \| Private-robo \| us-east- — Create new subnet<br>251 IP Addresses available |
| **Auto-assign Public IP** | Use subnet setting (Disable) |
| **Placement group** | □ Add instance to placement group |
| **Capacity Reservation** | Open — Create new Capacity Reservation |
| **IAM role** | None — Create new IAM role |



Step 6: Configure Security Group

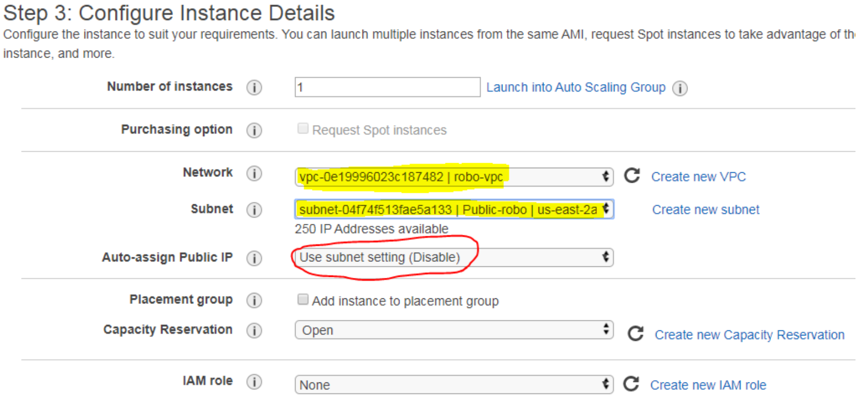
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted 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:** Private-instance-SG
**Description:** for Private instance

| Type | Protocol | Port Range | Source | Description |
|---|---|---|---|---|
| All traffic | All | 0 - 65535 | Custom 0.0.0.0/0 | e.g. SSH for Admin Desktop |

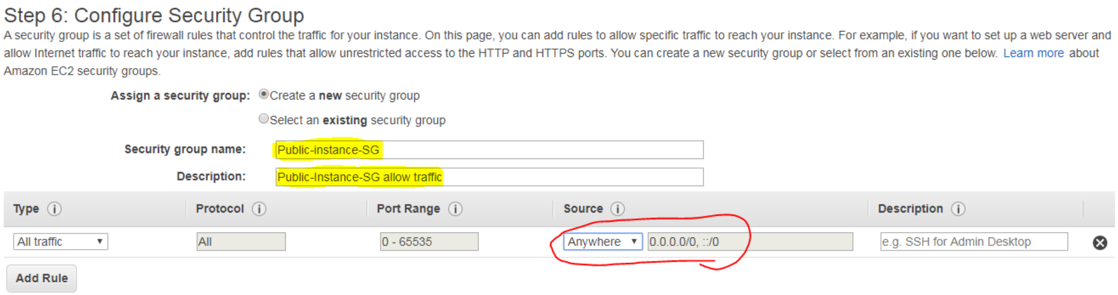
## Step5.3 Create normal centos EC2 public instance.



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 th instance, and more.

| | |
|---|---|
| **Number of instances** | 1 Launch into Auto Scaling Group |
| **Purchasing option** | □ Request Spot instances |
| **Network** | vpc-0e19996023c187482 \| robo-vpc — Create new VPC |
| **Subnet** | subnet-04f74f513fae5a133 \| Public-robo \| us-east-2a — Create new subnet<br>250 IP Addresses available |
| **Auto-assign Public IP** | Use subnet setting (Disable) |
| **Placement group** | □ Add instance to placement group |
| **Capacity Reservation** | Open — Create new Capacity Reservation |
| **IAM role** | None — Create new IAM role |



Step 6: Configure Security Group

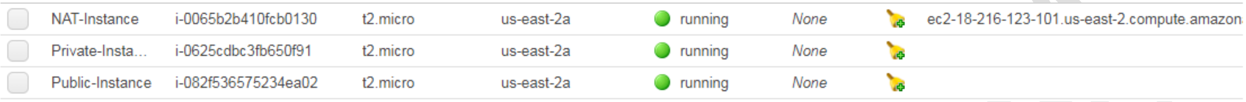
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted 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:** Public-instance-SG
**Description:** Public-Instance-SG allow traffic

| Type | Protocol | Port Range | Source | Description |
|---|---|---|---|---|
| All traffic | All | 0 - 65535 | Anywhere 0.0.0.0/0, ::/0 | e.g. SSH for Admin Desktop |

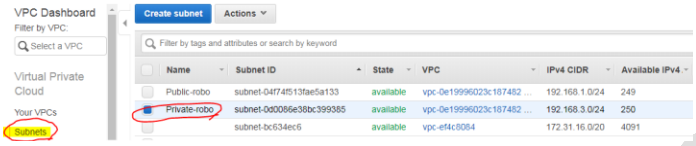
## @All three instances are created.



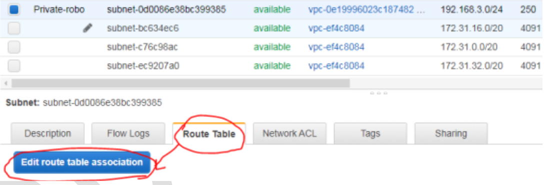
| | | | | | | |
|---|---|---|---|---|---|---|
| NAT-Instance | i-0065b2b410fcb0130 | t2.micro | us-east-2a | running | None | ec2-18-216-123-101.us-east-2.compute.amazon |
| Private-Insta... | i-0625cdbc3fb650f91 | t2.micro | us-east-2a | running | None | |
| Public-Instance | i-082f536575234ea02 | t2.micro | us-east-2a | running | None | |

## Step6:-Now associate the route tables(private to NAT instance and public to IGW)

## Click on VPC → click Subnet → then select Private-robo → select Route Table→ click on Edit

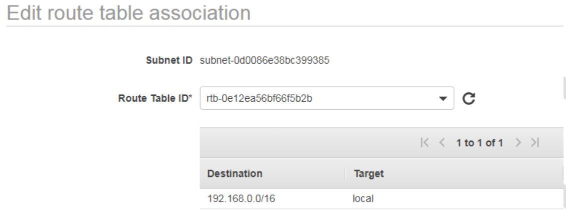


| Name | Subnet ID | State | VPC | IPv4 CIDR | Available IPv4 |
|---|---|---|---|---|---|
| Public-robo | subnet-04f74f513fae5a133 | available | vpc-0e19996023c187482 ... | 192.168.1.0/24 | 249 |
| Private-robo | subnet-0d0086e38bc399385 | available | vpc-0e19996023c187482 ... | 192.168.3.0/24 | 250 |
| | subnet-bc634ec6 | available | vpc-ef4c8084 | 172.31.16.0/20 | 4091 |



| | | | | | |
|---|---|---|---|---|---|
| Private-robo | subnet-0d0086e38bc399385 | available | vpc-0e19996023c187482 ... | 192.168.3.0/24 | 250 |
| | subnet-bc634ec6 | available | vpc-ef4c8084 | 172.31.16.0/20 | 4091 |
| | subnet-c76c98ac | available | vpc-ef4c8084 | 172.31.0.0/20 | 4091 |
| | subnet-ec9207a0 | available | vpc-ef4c8084 | 172.31.32.0/20 | 4091 |

**Subnet:** subnet-0d0086e38bc399385



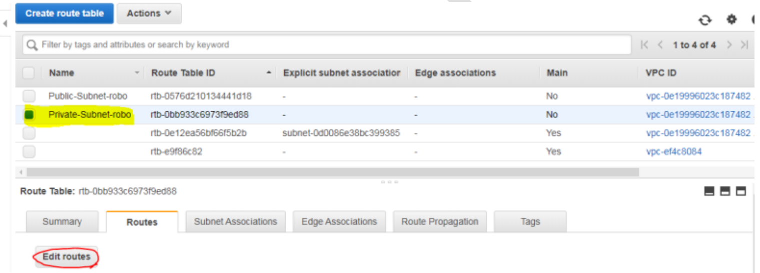
Edit route table association

**Subnet ID** subnet-0d0086e38bc399385

**Route Table ID*** rtb-0e12ea56bf66f5b2b

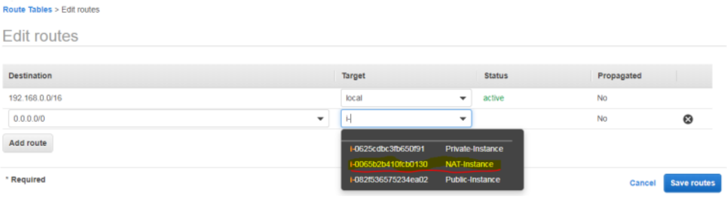
| Destination | Target |
|---|---|
| 192.168.0.0/16 | local |

## Step6.1Click on Route Tables → Select Routes → select Edit routes→ add rules → then select NAT instance Target



| Name | Route Table ID | Explicit subnet associatior | Edge associations | Main | VPC ID |
|---|---|---|---|---|---|
| Public-Subnet-robo | rtb-0576d210134441d18 | - | - | No | vpc-0e19996023c187482 |
| Private-Subnet-robo | rtb-0bb933c6973f9ed88 | - | - | No | vpc-0e19996023c187482 |
| | rtb-0e12ea56bf66f5b2b | subnet-0d0086e38bc399385 | - | Yes | vpc-0e19996023c187482 |
| | rtb-e9f86c82 | - | - | Yes | vpc-ef4c8084 |

**Route Table:** rtb-0bb933c6973f9ed88

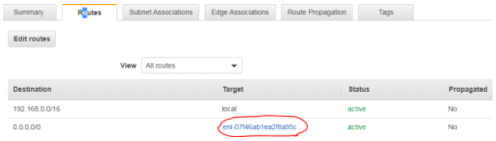


Route Tables > Edit routes

Edit routes

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 192.168.0.0/16 | local | active | No |
| 0.0.0.0/0 | i- | | No |

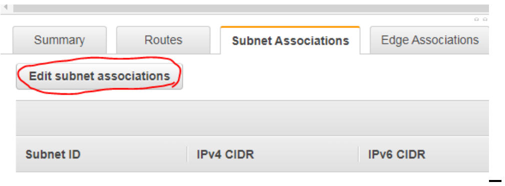
| | |
|---|---|
| i-0625cdbc3fb650f91 | Private-Instance |
| i-0065b2b410fcb0130 | NAT-Instance |
| i-082f536575234ea02 | Public-Instance |



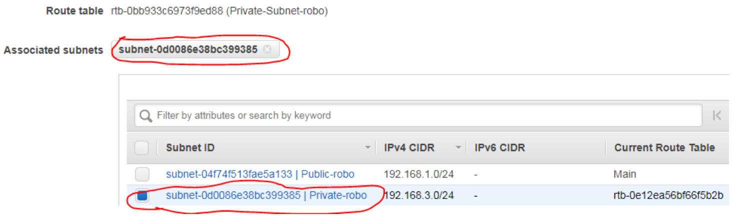
View All routes

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 192.168.0.0/16 | local | active | No |
| 0.0.0.0/0 | eni-07f46ab1ea2f8a95c | active | No |

## Step6.2 go to next tab (Subnet Association and select Private subnet.



| Subnet ID | IPv4 CIDR | IPv6 CIDR |
|---|---|---|

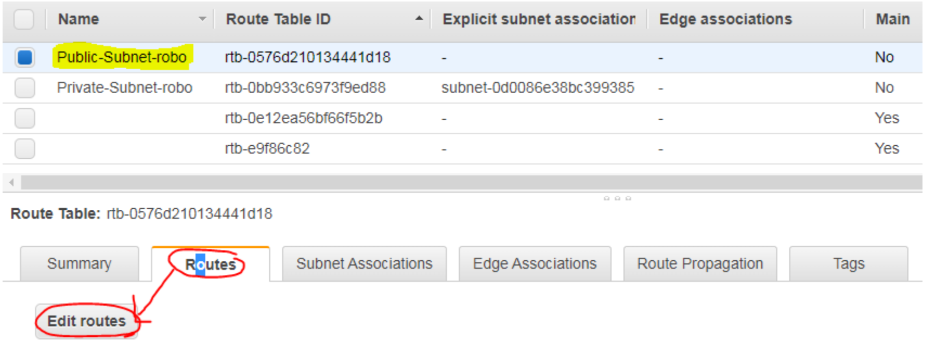


**Route table** rtb-0bb933c6973f9ed88 (Private-Subnet-robo)

**Associated subnets** subnet-0d0086e38bc399385

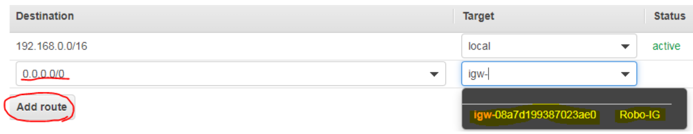
| Subnet ID | IPv4 CIDR | IPv6 CIDR | Current Route Table |
|---|---|---|---|
| subnet-04f74f513fae5a133 \| Public-robo | 192.168.1.0/24 | - | Main |
| subnet-0d0086e38bc399385 \| Private-robo | 192.168.3.0/24 | - | rtb-0e12ea56bf66f5b2b |

Step6.3:-Click on Route Tables → Select Routes → select Edit routes→ add rules → then select NAT instance Target

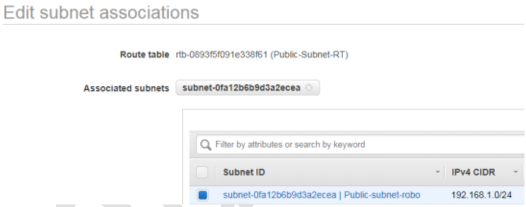


| | Name | Route Table ID | Explicit subnet associatior | Edge associations | Main |
|---|---|---|---|---|---|
| ☑ | Public-Subnet-robo | rtb-0576d210134441d18 | - | - | No |
| □ | Private-Subnet-robo | rtb-0bb933c6973f9ed88 | subnet-0d0086e38bc399385 | - | No |
| □ | | rtb-0e12ea56bf66f5b2b | - | - | Yes |
| □ | | rtb-e9f86c82 | - | - | Yes |

**Route Table:** rtb-0576d210134441d18



| Destination | Target | Status |
|---|---|---|
| 192.168.0.0/16 | local | active |
| 0.0.0.0/0 | igw-| | |



Edit subnet associations

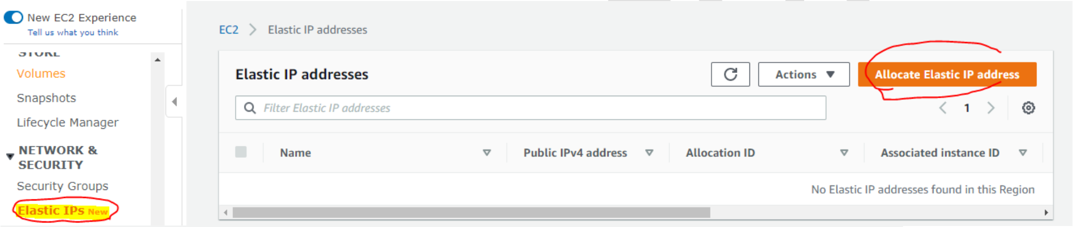
**Route table** rtb-0893f5f091e338f61 (Public-Subnet-RT)

**Associated subnets** subnet-0fa12b6b9d3a2ecea

| | Subnet ID | IPv4 CIDR |
|---|---|---|
| ☑ | subnet-0fa12b6b9d3a2ecea \| Public-subnet-robo | 192.168.1.0/24 |

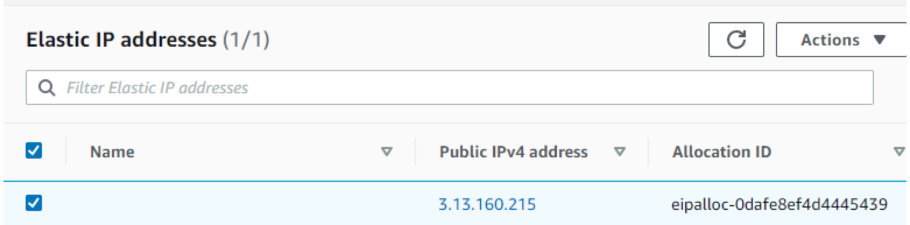
Step7:-Assign EIP to public instance.

Click on EC2 → Select Elastic IPS → Allocate Elastic IP address →



| □ | Name | Public IPv4 address | Allocation ID | Associated instance ID |
|---|---|---|---|---|

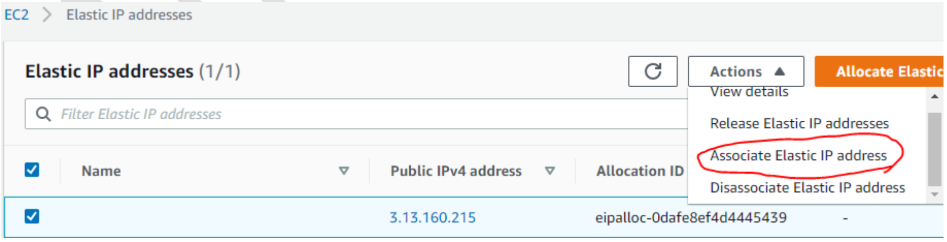
No Elastic IP addresses found in this Region



Elastic IP addresses (1/1)

| ☑ | Name | Public IPv4 address | Allocation ID |
|---|---|---|---|
| ☑ | | 3.13.160.215 | eipalloc-0dafe8ef4d4445439 |

Then Select EIP → click Associate Elastic IP address→

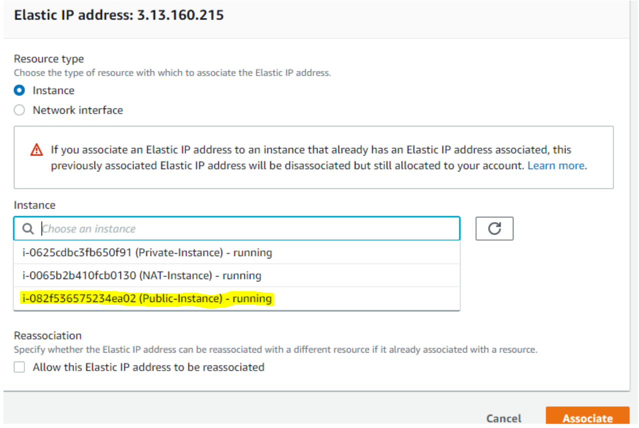


EC2 > Elastic IP addresses

Elastic IP addresses (1/1)

Actions
Allocate Elastic
Filter Elastic IP addresses
View details
Release Elastic IP addresses
Associate Elastic IP address
Disassociate Elastic IP address

| ☑ | Name | Public IPv4 address | Allocation ID | |
|---|---|---|---|---|
| ☑ | | 3.13.160.215 | eipalloc-0dafe8ef4d4445439 | - |



**Elastic IP address: 3.13.160.215**

Resource type

Choose the type of resource with which to associate the Elastic IP address.

● Instance

○ Network interface

⚠ If you associate an Elastic IP address to an instance that already has an Elastic IP address associated, this previously associated Elastic IP address will be disassociated but still allocated to your account. Learn more.

Instance

Choose an instance

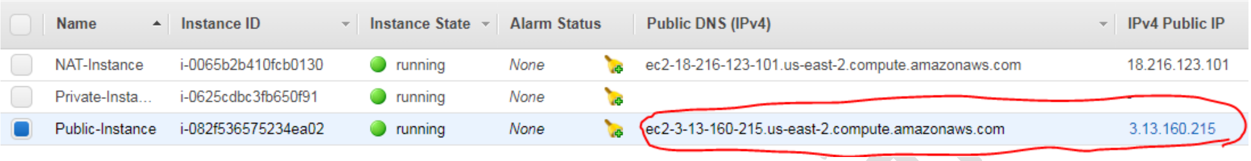
- i-0625cdbc3fb650f91 (Private-Instance) - running
- i-0065b2b410fcb0130 (NAT-Instance) - running
- i-082f536575234ea02 (Public-Instance) - running

Reassociation

Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

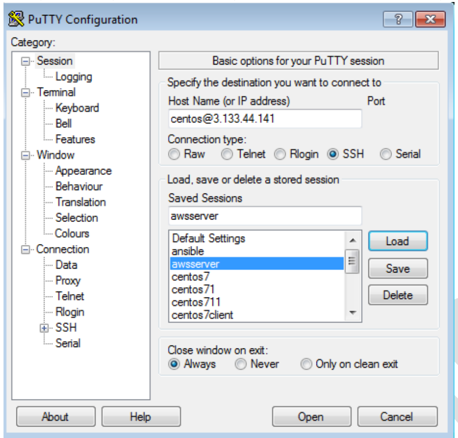
□ Allow this Elastic IP address to be reassociated

@Go to EC2 instances and you see the public DNS and IP.



| Name | Instance ID | Instance State | Alarm Status | Public DNS (IPv4) | IPv4 Public IP |
|---|---|---|---|---|---|
| NAT-Instance | i-0065b2b410fcb0130 | running | None | ec2-18-216-123-101.us-east-2.compute.amazonaws.com | 18.216.123.101 |
| Private-Insta... | i-0625cdbc3fb650f91 | running | None | | |
| Public-Instance | i-082f536575234ea02 | running | None | ec2-3-13-160-215.us-east-2.compute.amazonaws.com | 3.13.160.215 |

Step 8:-Try to access public instance via public IP.



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): centos@3.133.44.141

Port

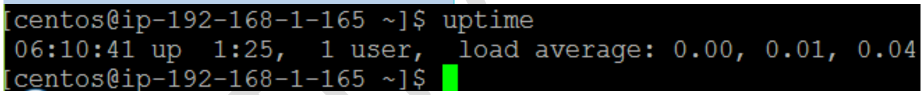
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: awsserver

- Default Settings
- ansible
- awsserver
- centos7
- centos71
- centos711
- centos7client

Close window on exit: ● Always ○ Never ○ Only on clean exit



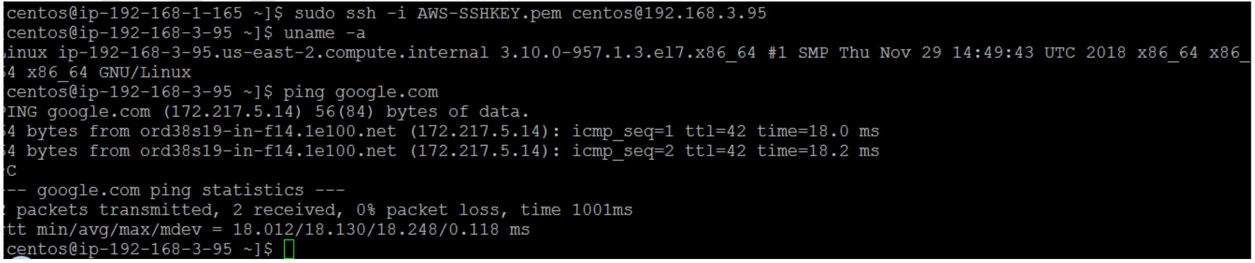
```
[centos@ip-192-168-1-165 ~]$ uptime
 06:10:41 up  1:25,  1 user,  load average: 0.00, 0.01, 0.04
[centos@ip-192-168-1-165 ~]$ 
```

@@Then login to private instance via public instance and verify the internet connectivity.

@Copy your aws .pem key to public instance by using winscp.

#ssh -I AWS-SSHKEY.pem centos@<private ip>

#ping google.com



```
[centos@ip-192-168-1-165 ~]$ sudo ssh -i AWS-SSHKEY.pem centos@192.168.3.95
[centos@ip-192-168-3-95 ~]$ uname -a
Linux ip-192-168-3-95.us-east-2.compute.internal 3.10.0-957.1.3.el7.x86_64 #1 SMP Thu Nov 29 14:49:43 UTC 2018 x86_64 x86_
64 x86_64 GNU/Linux
[centos@ip-192-168-3-95 ~]$ ping google.com
PING google.com (172.217.5.14) 56(84) bytes of data.
64 bytes from ord38s19-in-f14.1e100.net (172.217.5.14): icmp_seq=1 ttl=42 time=18.0 ms
64 bytes from ord38s19-in-f14.1e100.net (172.217.5.14): icmp_seq=2 ttl=42 time=18.2 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 18.012/18.130/18.248/0.118 ms
[centos@ip-192-168-3-95 ~]$ 
```

Note:- Here there is no direct internet connectivity to private instance, since NAT route rule has been selected on this instance, so all the traffic will go via NAT instances which will be act as router here.