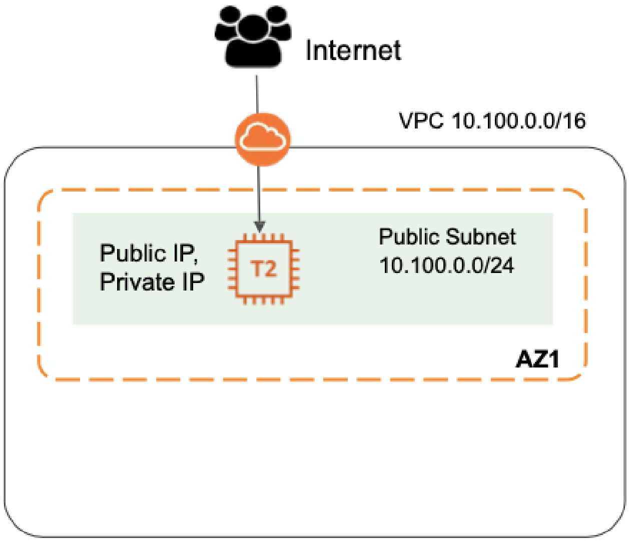
# LAB-VPC-1

## VPC with Single Public Subnet



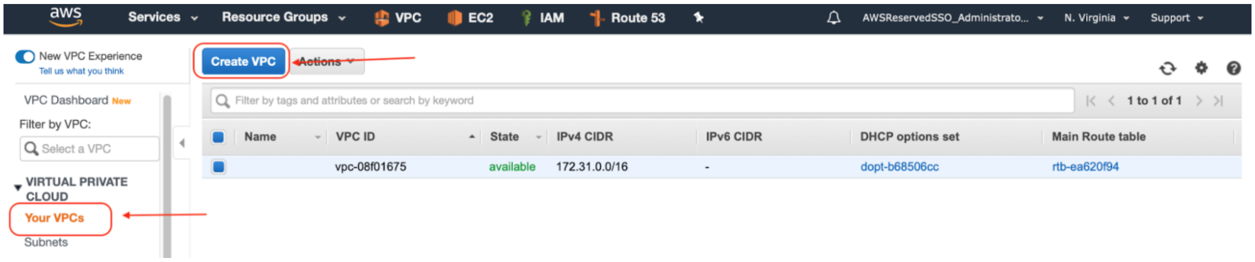
Public Subnet Route Table

| Destination | Target |
|---|---|
| 10.100.0.0/16 | local |
| 0.0.0.0/0 | igw-xxx |

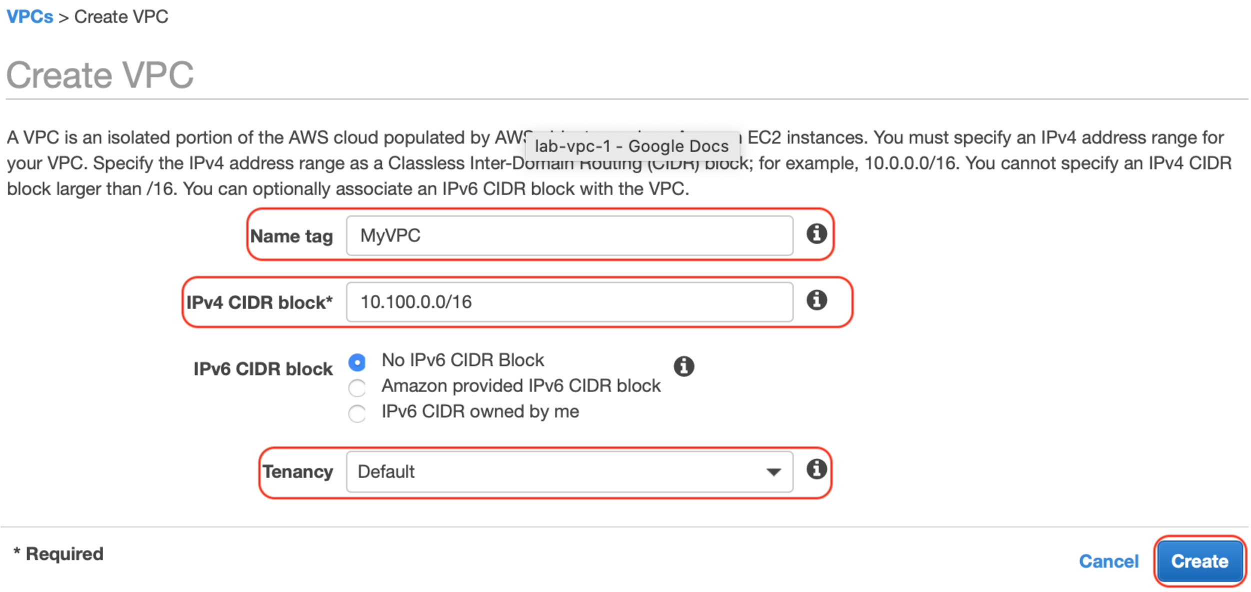
# Resolution

1 Create VPC

Go to VPC service -> Your VPCs -> Create VPC (Name: MyVPC, CIDR: 10.100.0.0/16) -> Create



| Name | VPC ID | State | IPv4 CIDR | IPv6 CIDR | DHCP options set | Main Route table |
|---|---|---|---|---|---|---|
| | vpc-08f01675 | available | 172.31.0.0/16 | - | dopt-b68506cc | rtb-ea620f94 |



VPCs > Create VPC

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS lab-vpc-1 - Google Docs EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an IPv6 CIDR block with the VPC.

Name tag: MyVPC

IPv4 CIDR block*: 10.100.0.0/16

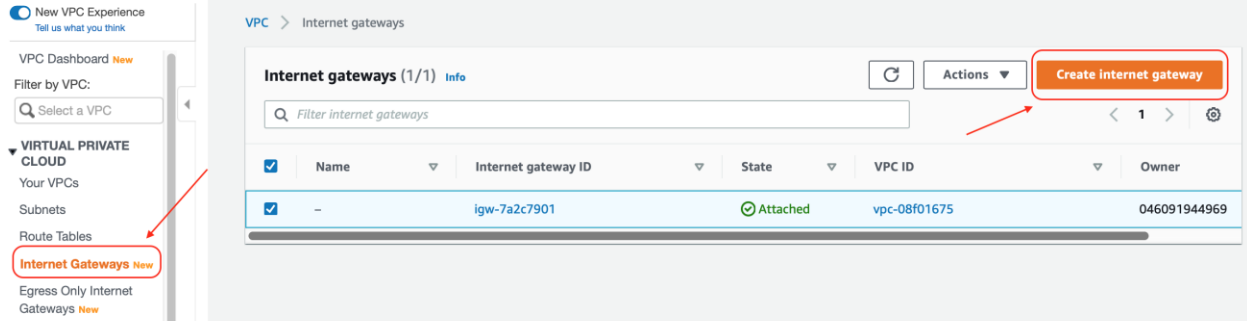
IPv6 CIDR block:
● No IPv6 CIDR Block
○ Amazon provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy: Default

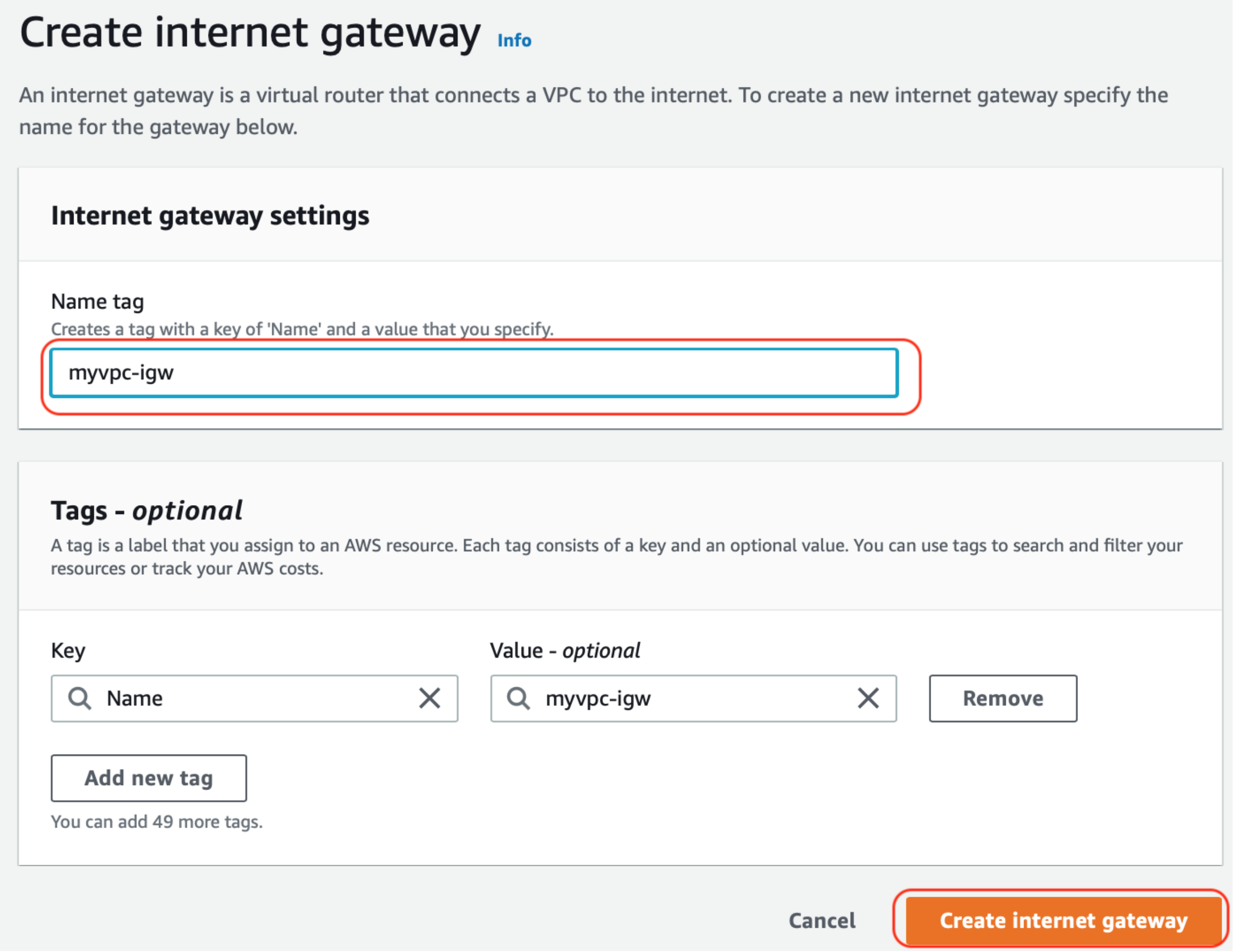
* Required

## Create Internet Gateway

Go to Internet Gateways -> Create internet gateway



| ☑ | Name | Internet gateway ID | State | VPC ID | Owner |
|---|---|---|---|---|---|
| ☑ | – | igw-7a2c7901 | ✓ Attached | vpc-08f01675 | 046091944969 |



# Create internet gateway Info

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.

### Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
myvpc-igw

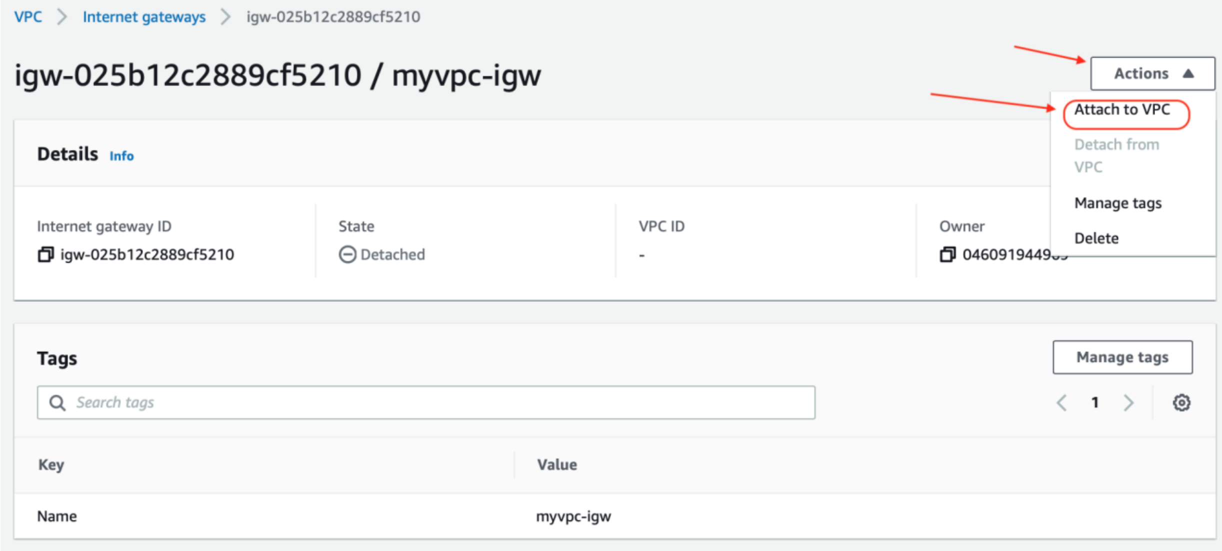
### Tags - *optional*

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.

| Key | Value - *optional* |
|---|---|
| Name | myvpc-igw |

You can add 49 more tags.

Attach Internet Gateway to VPC
Select Internet gateway -> Actions -> Attach to VPC -> Select your VPC



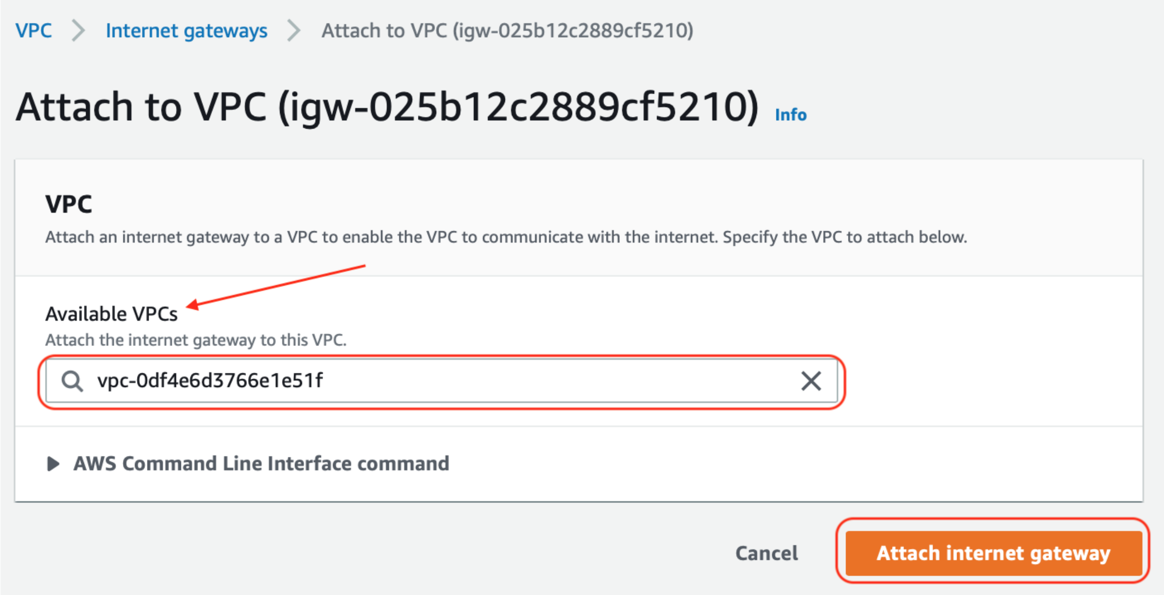
igw-025b12c2889cf5210 / myvpc-igw

Details Info

| Internet gateway ID | State | VPC ID | Owner |
|---|---|---|---|
| igw-025b12c2889cf5210 | Detached | - | 0460919449 |

Tags

| Key | Value |
|---|---|
| Name | myvpc-igw |


VPC > Internet gateways > Attach to VPC (igw-025b12c2889cf5210)
AWS Command Line Interface command
Cancel
Attach internet gateway

Attach to VPC (igw-025b12c2889cf5210) Info

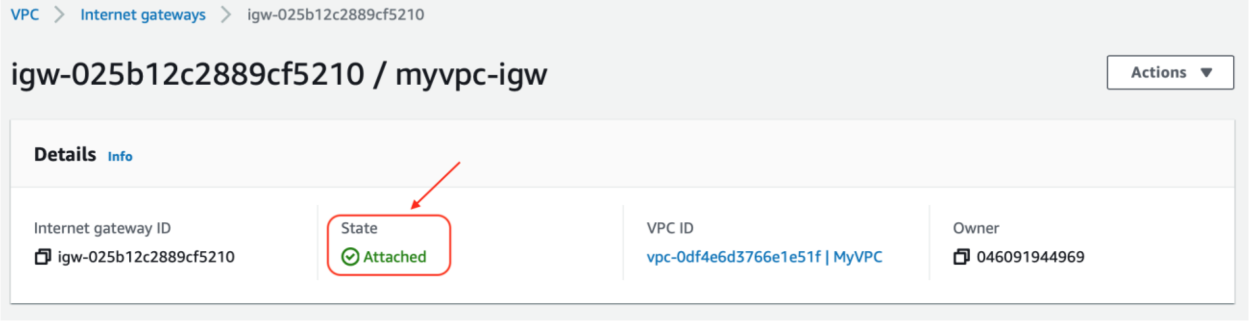
VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

vpc-0df4e6d3766e1e51f



VPC > Internet gateways > igw-025b12c2889cf5210

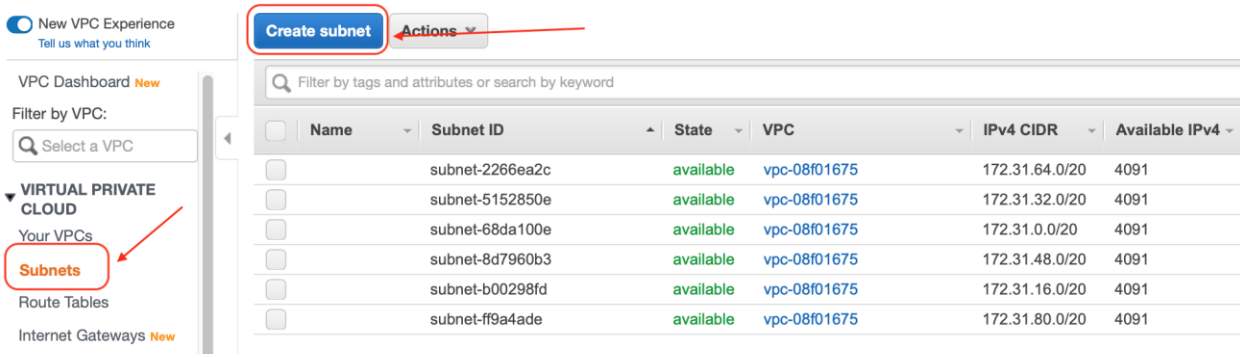
igw-025b12c2889cf5210 / myvpc-igw

Details Info

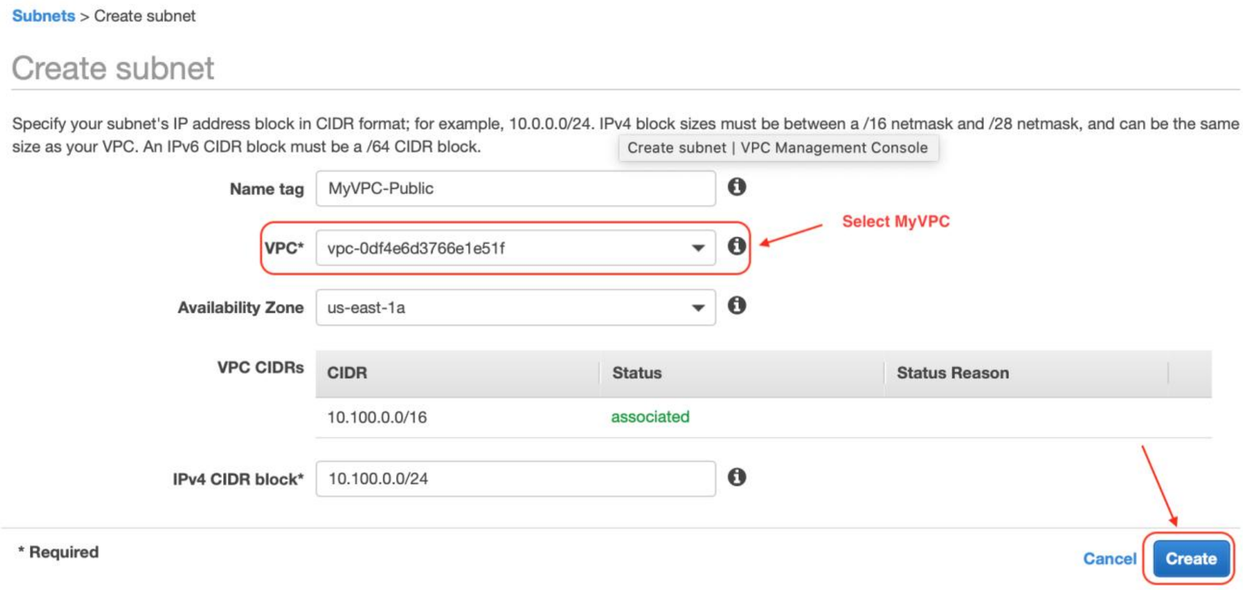
| Internet gateway ID | State | VPC ID | Owner |
|---|---|---|---|
| igw-025b12c2889cf5210 | Attached | vpc-0df4e6d3766e1e51f \| MyVPC | 046091944969 |

Create Subnet

Subnets -> Create subnet (Name: MyVPC-Public, VPC: MyVPC, AZ: Select first az - us-east-1a, CIDR: 10.100.0.0/24)



| Name | Subnet ID | State | VPC | IPv4 CIDR | Available IPv4 |
|---|---|---|---|---|---|
| | subnet-2266ea2c | available | vpc-08f01675 | 172.31.64.0/20 | 4091 |
| | subnet-5152850e | available | vpc-08f01675 | 172.31.32.0/20 | 4091 |
| | subnet-68da100e | available | vpc-08f01675 | 172.31.0.0/20 | 4091 |
| | subnet-8d7960b3 | available | vpc-08f01675 | 172.31.48.0/20 | 4091 |
| | subnet-b00298fd | available | vpc-08f01675 | 172.31.16.0/20 | 4091 |
| | subnet-ff9a4ade | available | vpc-08f01675 | 172.31.80.0/20 | 4091 |



Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: MyVPC-Public

VPC*: vpc-0df4e6d3766e1e51f

Select MyVPC

Availability Zone: us-east-1a

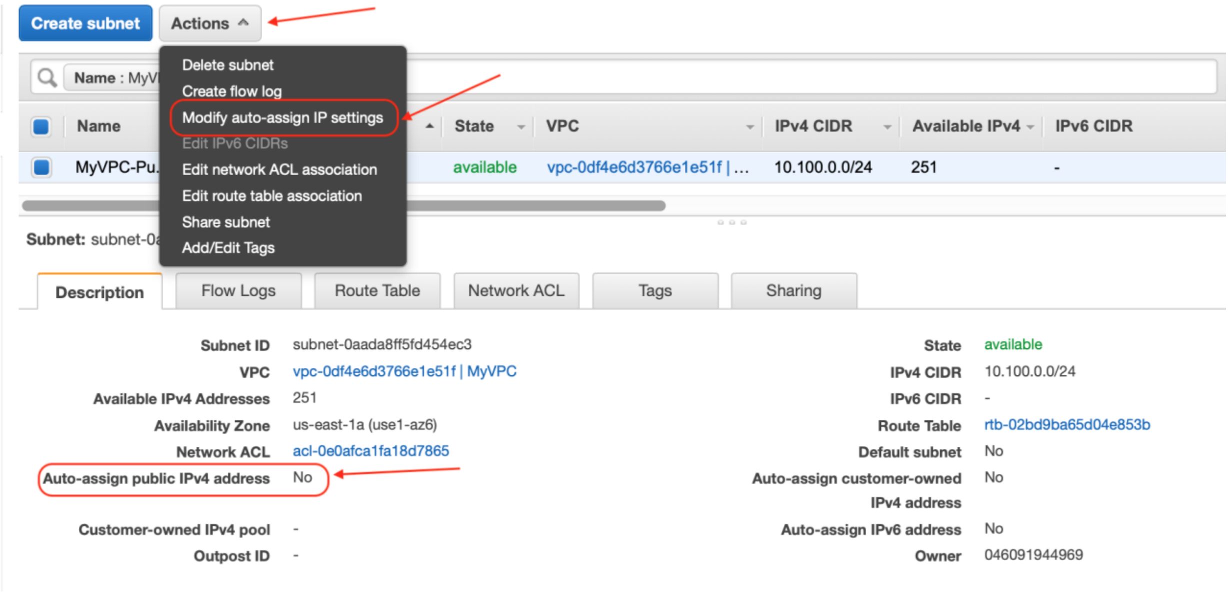
VPC CIDRs

| CIDR | Status | Status Reason |
|---|---|---|
| 10.100.0.0/16 | associated | |

IPv4 CIDR block*: 10.100.0.0/24

* Required

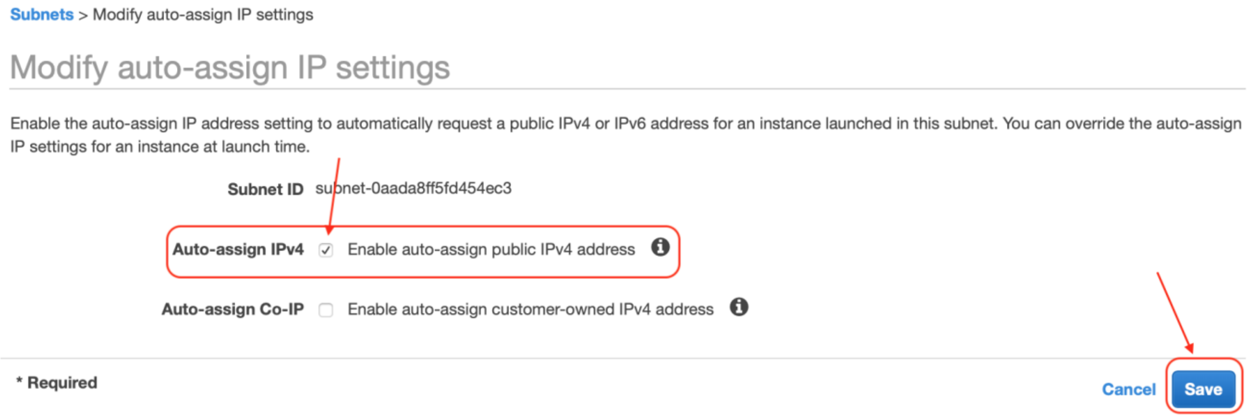
## Select Subnet -> Action -> Modify Auto Assign Public IP -> Enable -> Save



| Name | State | VPC | IPv4 CIDR | Available IPv4 | IPv6 CIDR |
|---|---|---|---|---|---|
| MyVPC-Pu... | available | vpc-0df4e6d3766e1e51f \| ... | 10.100.0.0/24 | 251 | - |

**Subnet:** subnet-0a

| | | | |
|---|---|---|---|
| **Subnet ID** | subnet-0aada8ff5fd454ec3 | **State** | available |
| **VPC** | vpc-0df4e6d3766e1e51f \| MyVPC | **IPv4 CIDR** | 10.100.0.0/24 |
| **Available IPv4 Addresses** | 251 | **IPv6 CIDR** | - |
| **Availability Zone** | us-east-1a (use1-az6) | **Route Table** | rtb-02bd9ba65d04e853b |
| **Network ACL** | acl-0e0afca1fa18d7865 | **Default subnet** | No |
| **Auto-assign public IPv4 address** | No | **Auto-assign customer-owned IPv4 address** | No |
| **Customer-owned IPv4 pool** | - | **Auto-assign IPv6 address** | No |
| **Outpost ID** | - | **Owner** | 046091944969 |


**Subnets** > Modify auto-assign IP settings

### Modify auto-assign IP settings

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for an instance launched in this subnet. You can override the auto-assign IP settings for an instance at launch time.

**Subnet ID** subnet-0aada8ff5fd454ec3

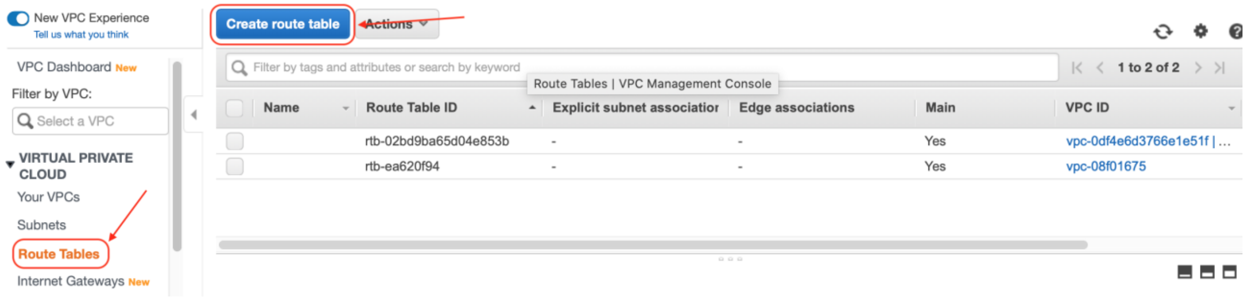
**Auto-assign IPv4** ☑ Enable auto-assign public IPv4 address

**Auto-assign Co-IP** □ Enable auto-assign customer-owned IPv4 address

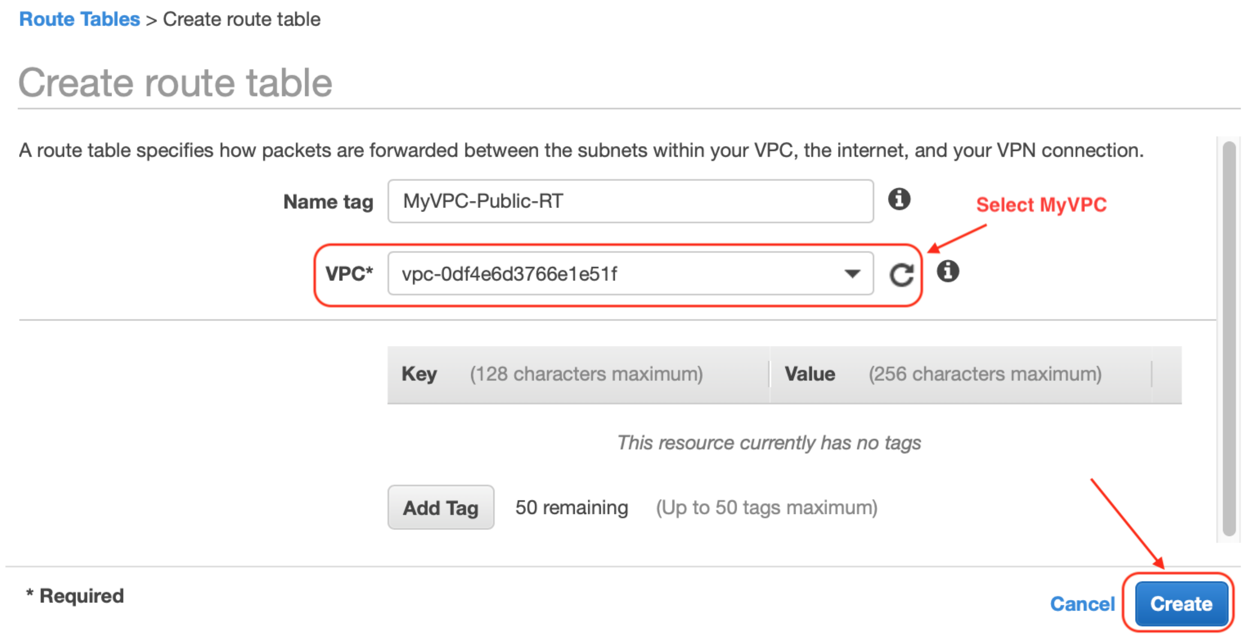
* Required

### Create Route Table

Route Tables -> Create Route Table (Name: MyVPC-Public, VPC: MyVPC)



| | Name | Route Table ID | Explicit subnet associatior | Edge associations | Main | VPC ID |
|---|---|---|---|---|---|---|
| □ | | rtb-02bd9ba65d04e853b | - | - | Yes | vpc-0df4e6d3766e1e51f \| ... |
| □ | | rtb-ea620f94 | - | - | Yes | vpc-08f01675 |



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

Name tag: MyVPC-Public-RT

VPC*: vpc-0df4e6d3766e1e51f

| Key (128 characters maximum) | Value (256 characters maximum) |
|---|---|

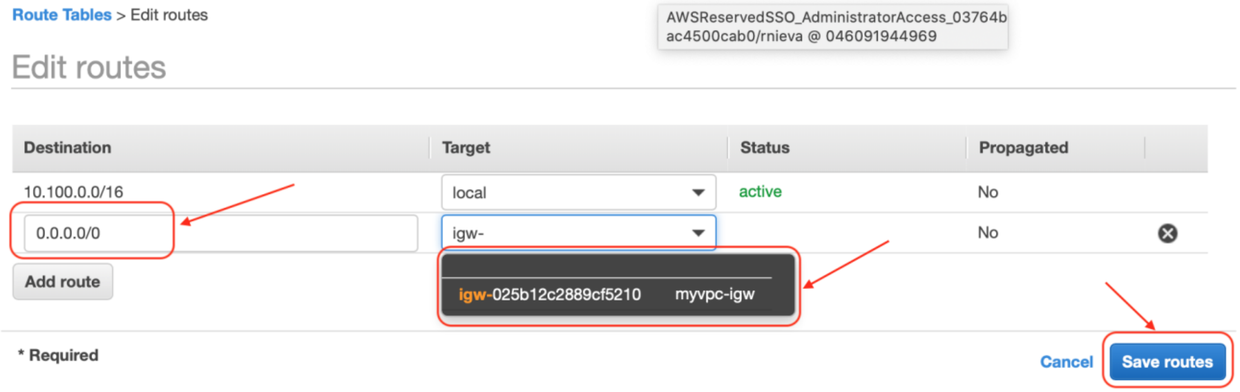
*This resource currently has no tags*

50 remaining (Up to 50 tags maximum)

* Required

### Add route to send all traffic that is not local to Internet Gateway

Select Route table -> Routes -> Edit -> Add another route (Destination: 0.0.0.0/0, Target: Internet gateway ->igw-xxx) -> Save



Route Tables > Edit routes

AWSReservedSSO_AdministratorAccess_03764bac4500cab0/rnieva @ 046091944969

Edit routes

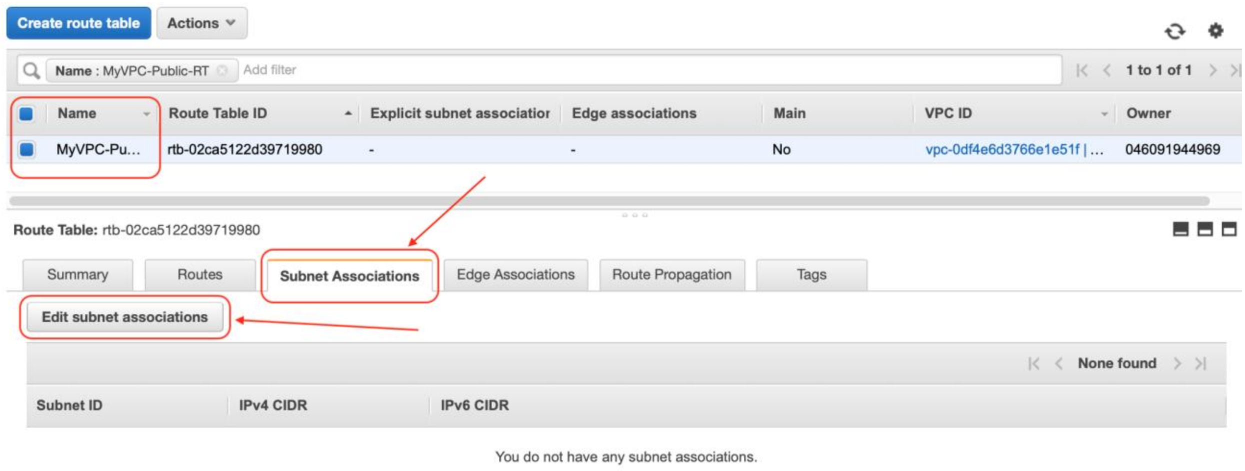
| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.100.0.0/16 | local | active | No |
| 0.0.0.0/0 | igw- | | No |

igw-025b12c2889cf5210 myvpc-igw

* Required

### Associate Route table with Subnet to make it Public Subnet

Select Route table -> Subnet Associations -> Edit -> Check the MyVPC-Public subnet -> Save



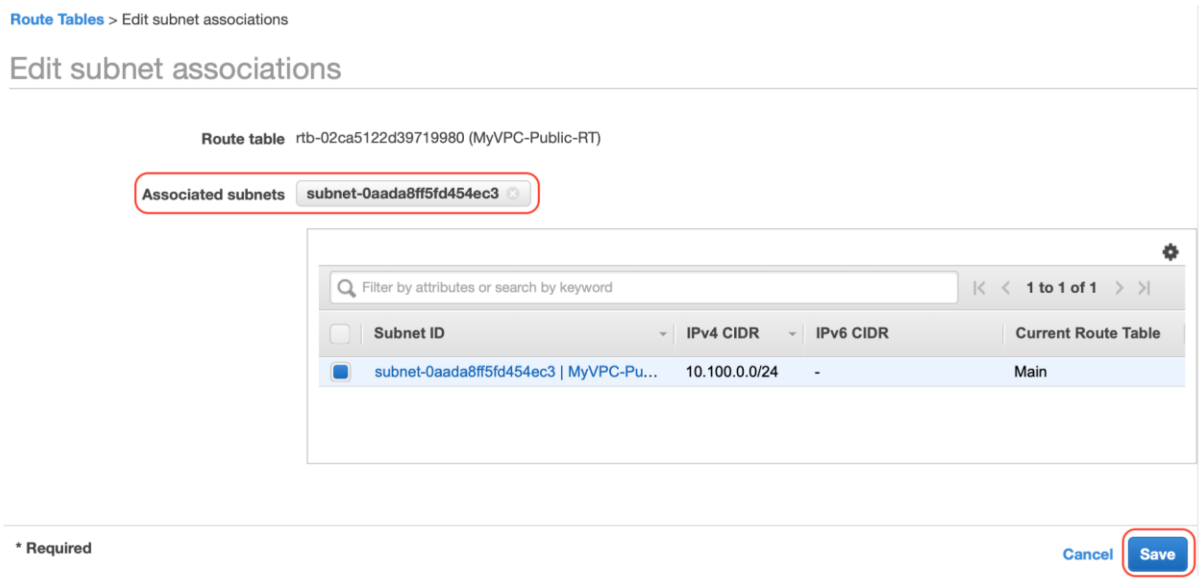
Name : MyVPC-Public-RT

| ☑ Name | Route Table ID | Explicit subnet associatior | Edge associations | Main | VPC ID | Owner |
|---|---|---|---|---|---|---|
| ☑ MyVPC-Pu... | rtb-02ca5122d39719980 | - | - | No | vpc-0df4e6d3766e1e51f \| ... | 046091944969 |

Route Table: rtb-02ca5122d39719980

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

You do not have any subnet associations.



Route Tables > Edit subnet associations

Edit subnet associations

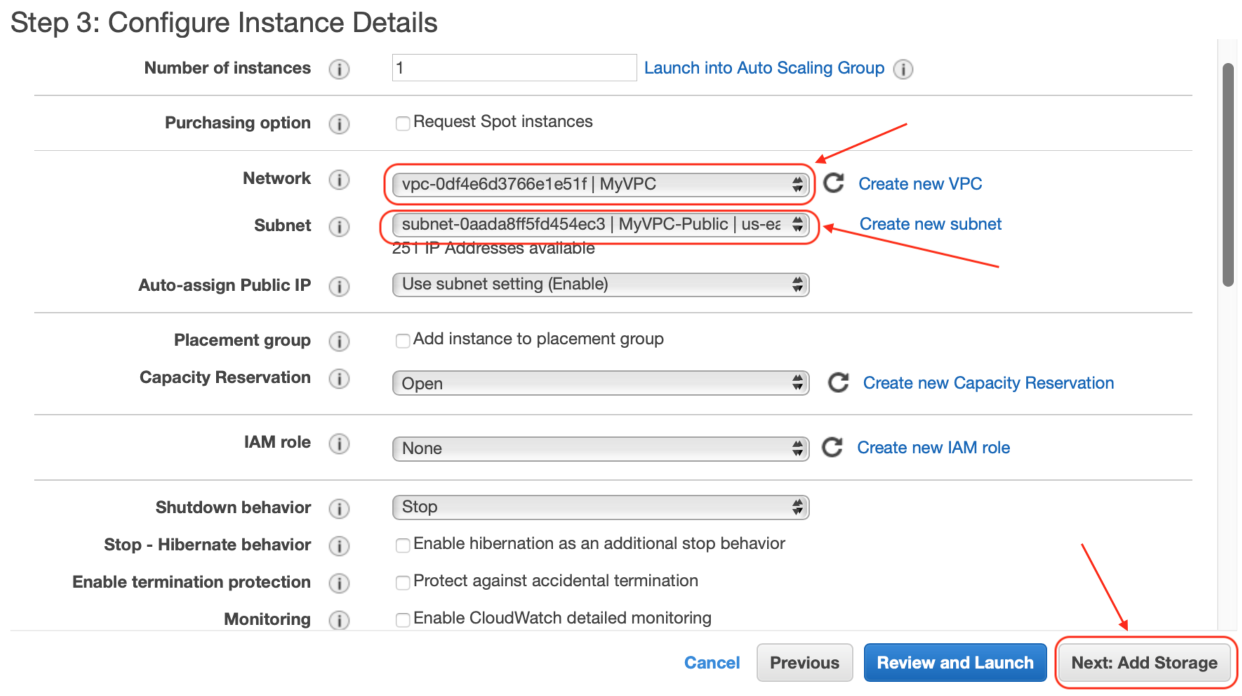
Route table rtb-02ca5122d39719980 (MyVPC-Public-RT)

Associated subnets subnet-0aada8ff5fd454ec3

| ☐ | Subnet ID | IPv4 CIDR | IPv6 CIDR | Current Route Table |
|---|---|---|---|---|
| ■ | subnet-0aada8ff5fd454ec3 \| MyVPC-Pu... | 10.100.0.0/24 | - | Main |

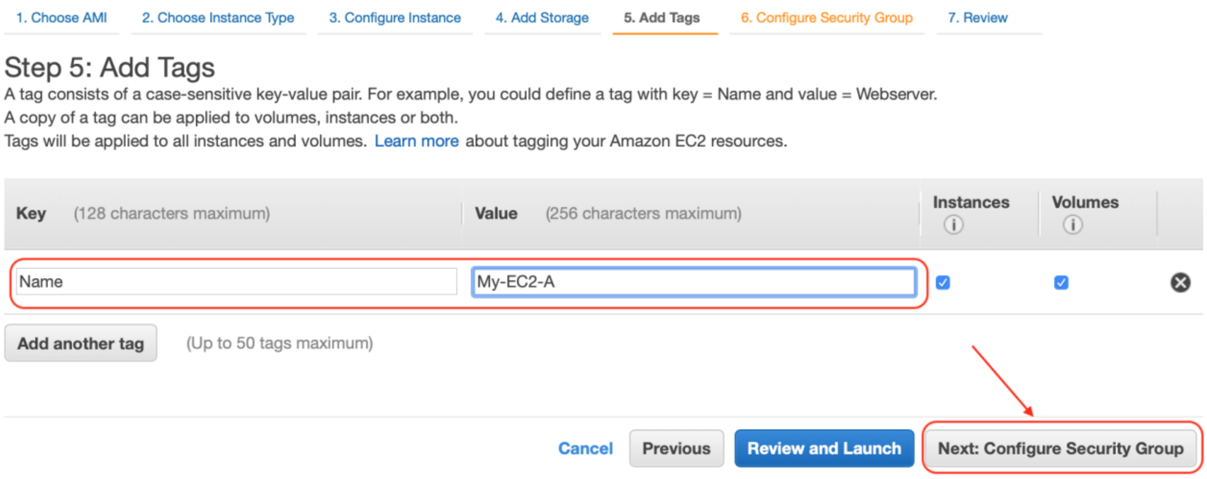
* Required

## Launch EC2 instance in newly created Public Subnet



Step 3: Configure Instance Details

| | |
|---|---|
| Number of instances | 1 Launch into Auto Scaling Group |
| Purchasing option | □ Request Spot instances |
| Network | vpc-0df4e6d3766e51f \| MyVPC Create new VPC |
| Subnet | subnet-0aada8ff5fd454ec3 \| MyVPC-Public \| us-ea Create new subnet<br>251 IP Addresses available |
| Auto-assign Public IP | Use subnet setting (Enable) |
| Placement group | □ Add instance to placement group |
| Capacity Reservation | Open Create new Capacity Reservation |
| 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 |

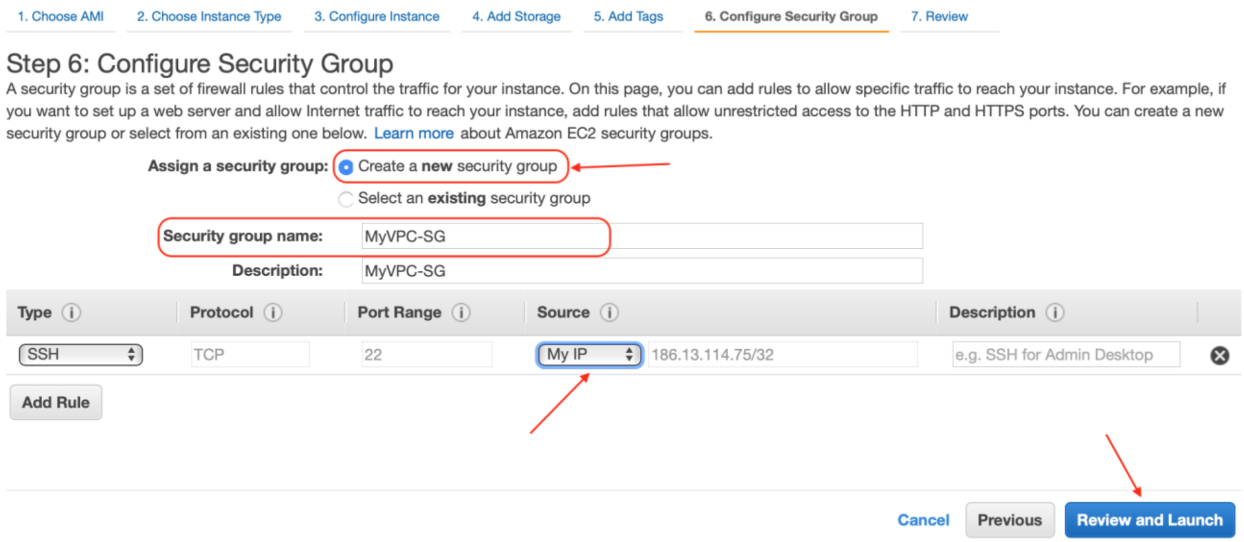


### Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

| Key (128 characters maximum) | Value (256 characters maximum) | Instances | Volumes |
|---|---|---|---|
| Name | My-EC2-A | ☑ | ☑ |

## Configure Security Group



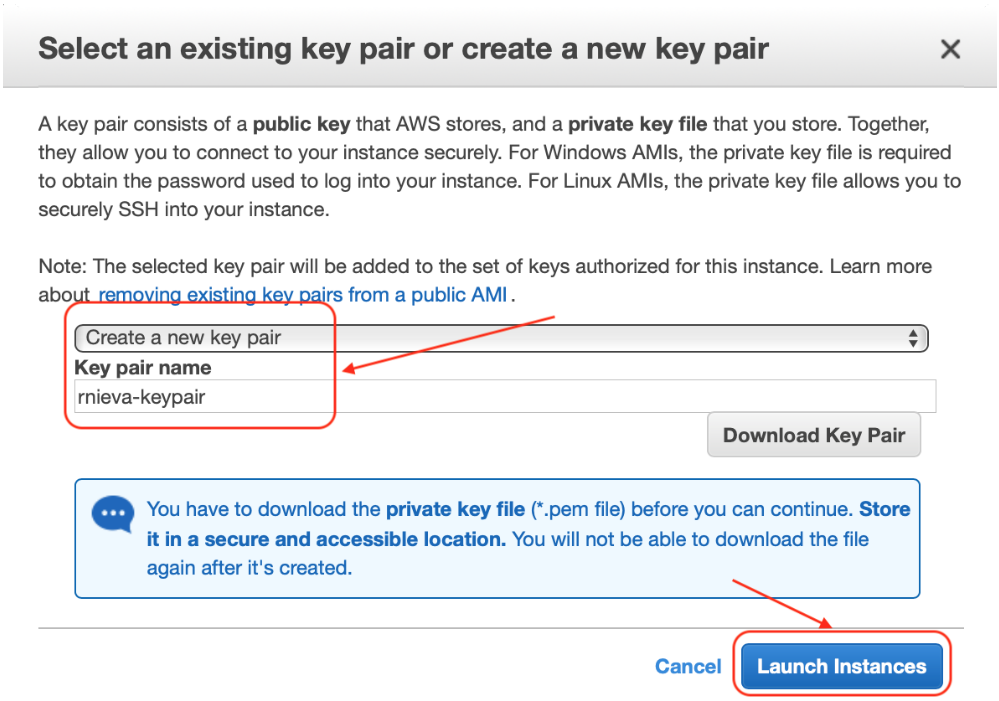
### Step 6: Configure Security Group

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: MyVPC-SG
Description: MyVPC-SG

| Type | Protocol | Port Range | Source | Description |
|---|---|---|---|---|
| SSH | TCP | 22 | My IP 186.13.114.75/32 | e.g. SSH for Admin Desktop |



## Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

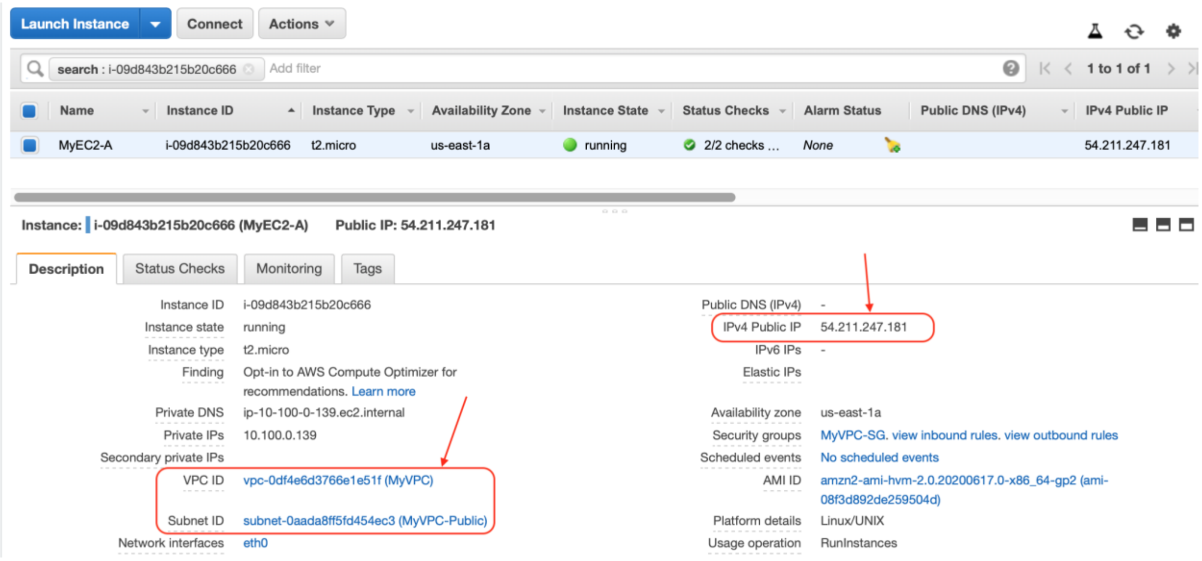
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair

**Key pair name**

rnieva-keypair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.



search : i-09d843b215b20c666

1 to 1 of 1

| Name | Instance ID | Instance Type | Availability Zone | Instance State | Status Checks | Alarm Status | Public DNS (IPv4) | IPv4 Public IP |
|---|---|---|---|---|---|---|---|---|
| MyEC2-A | i-09d843b215b20c666 | t2.micro | us-east-1a | running | 2/2 checks ... | None | | 54.211.247.181 |

Instance: i-09d843b215b20c666 (MyEC2-A) Public IP: 54.211.247.181

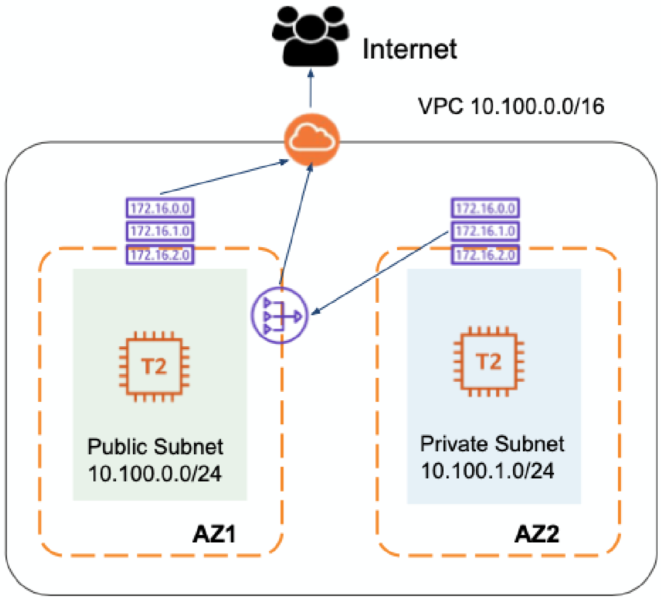
| | | | |
|---|---|---|---|
| Instance ID | i-09d843b215b20c666 | Public DNS (IPv4) | - |
| Instance state | running | IPv4 Public IP | 54.211.247.181 |
| Instance type | t2.micro | IPv6 IPs | - |
| Finding | Opt-in to AWS Compute Optimizer for recommendations. Learn more | Elastic IPs | |
| Private DNS | ip-10-100-0-139.ec2.internal | Availability zone | us-east-1a |
| Private IPs | 10.100.0.139 | Security groups | MyVPC-SG. view inbound rules. view outbound rules |
| Secondary private IPs | | Scheduled events | No scheduled events |
| VPC ID | vpc-0df4e6d3766e1e51f (MyVPC) | AMI ID | amzn2-ami-hvm-2.0.20200617.0-x86_64-gp2 (ami-08f3d892de259504d) |
| Subnet ID | subnet-0aada8ff5fd454ec3 (MyVPC-Public) | Platform details | Linux/UNIX |
| Network interfaces | eth0 | Usage operation | RunInstances |

### Connect to EC2 instance using the public IP from your laptop using linux terminal (ec2-user)

```
$ chmod 600 rnieva-keypair.pem

$ ls -l rnieva-keypair.pem
-rw-------@ 1 rnieva  staff  1692 Jul 24 16:56 rnieva-keypair.pem

$ ssh -irnieva-keypair.pem ec2-user@54.211.247.181
The authenticity of host '54.211.247.181 (54.211.247.181)' can't be
established.
ECDSA key fingerprint is
SHA256:gPaH78Hue2C+uPgXbB0+wdrx/q5UqQZ6MWZR78qDvLo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '54.211.247.181' (ECDSA) to the list of known
hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
14 package(s) needed for security, out of 31 available
Run "sudo yum update" to apply all updates.
-bash: warning: setlocale: LC_CTYPE: cannot change locale (UTF-8): No such
file or directory

[ec2-user@ip-10-100-0-139 ~]$ uptime
 20:07:48 up 10 min,  1 user,  load average: 0.00, 0.01, 0.00
```

# LAB-VPC-1

## VPC with Public and Private Subnet



Public Subnet Route Table

| Destination | Target |
|---|---|
| 10.100.0.0/16 | local |
| 0.0.0.0/0 | igw-xxx |

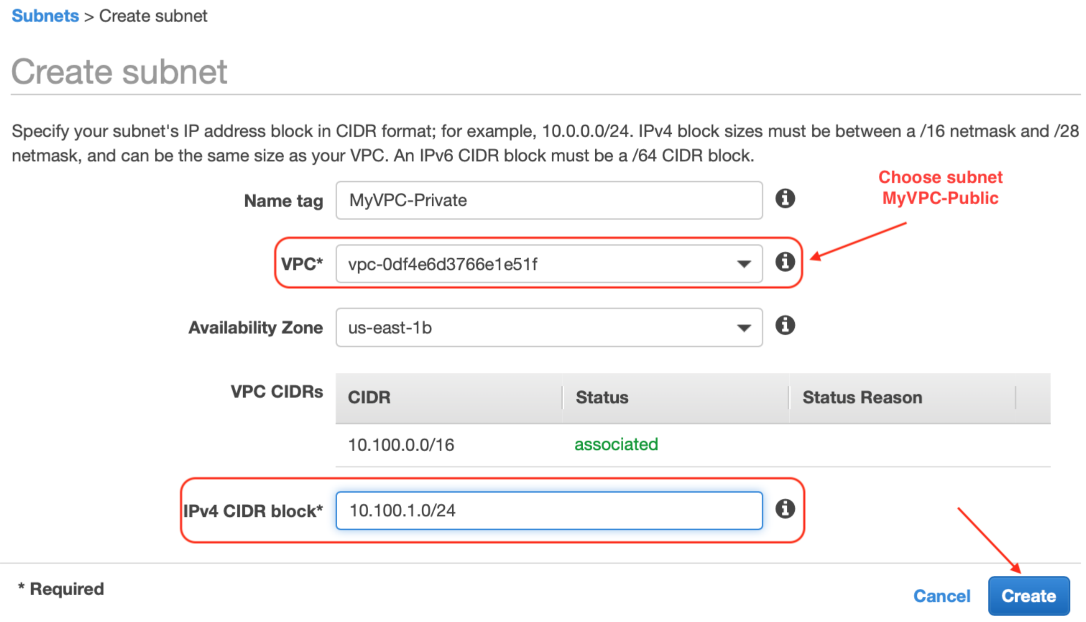
Private Subnet Route Table

| Destination | Target |
|---|---|
| 10.100.0.0/16 | local |

# Solution:

## Create a Private Subnet

Create subnet (Name: MyVPC-Private, VPC: MyVPC, AZ: Select different az (us-east-1b), CIDR: 10.100.1.0/24) 2. Create Private route table



**Subnets** > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: MyVPC-Private

VPC*: vpc-0df4e6d3766e1e51f

Availability Zone: us-east-1b

VPC CIDRs

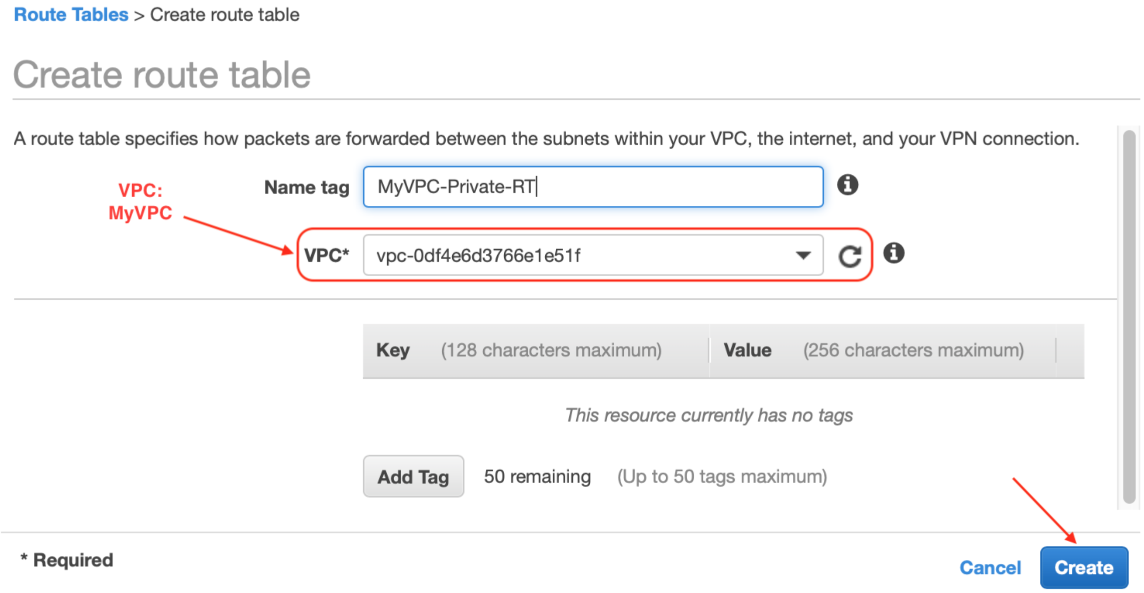
| CIDR | Status | Status Reason |
|---|---|---|
| 10.100.0.0/16 | associated | |

IPv4 CIDR block*: 10.100.1.0/24

* Required

Choose subnet MyVPC-Public

Create Private route table
Route Tables -> Create Route Table (Name: MyVPC-Private, VPC: MyVPC)



**Route Tables** > Create route table

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: MyVPC-Private-RT

VPC*: vpc-0df4e6d3766e1e51f

| Key (128 characters maximum) | Value (256 characters maximum) |
|---|---|

*This resource currently has no tags*

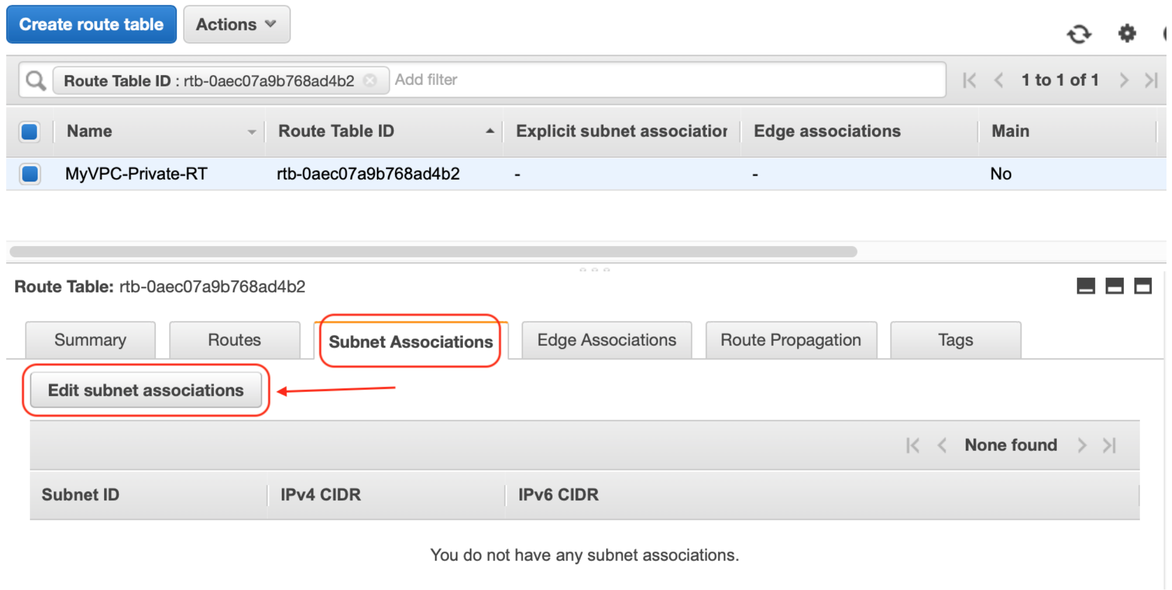
50 remaining (Up to 50 tags maximum)

* Required

VPC: MyVPC

mundosE
PEOPLE & BUSINESS SCHOOL

Associate Route table with Subnet to make it Private subnet
Select Route table -> Subnet Associations -> Edit -> Check the MyVPC-Private subnet -> Save



Route Table ID : rtb-0aec07a9b768ad4b2 Add filter 1 to 1 of 1

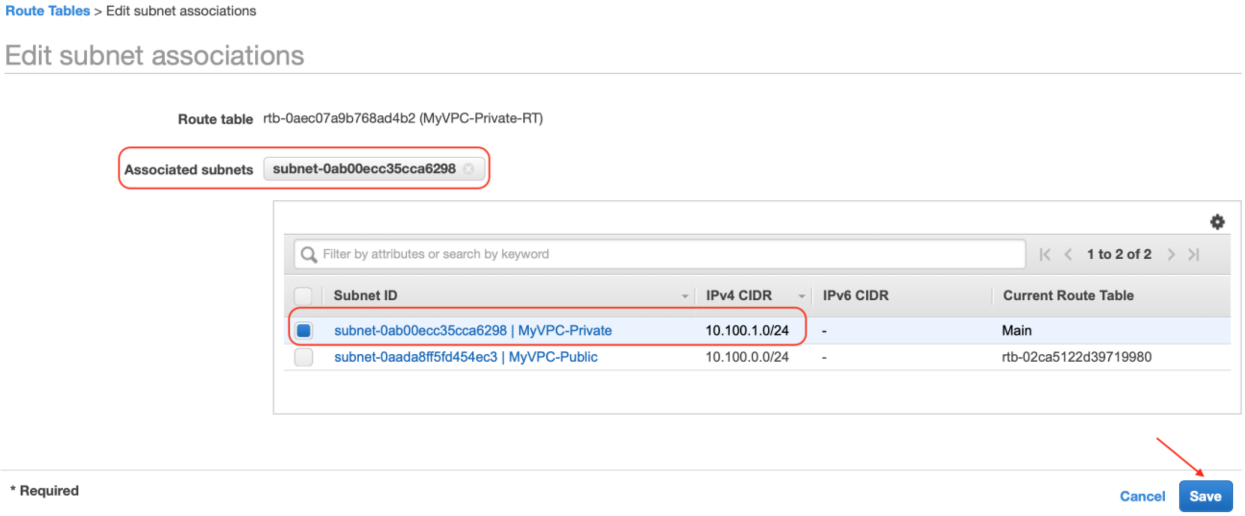
| ☑ | Name | Route Table ID | Explicit subnet associatior | Edge associations | Main |
|---|---|---|---|---|---|
| ☑ | MyVPC-Private-RT | rtb-0aec07a9b768ad4b2 | - | - | No |

**Route Table:** rtb-0aec07a9b768ad4b2

None found

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

You do not have any subnet associations.



Route Tables > Edit subnet associations

Edit subnet associations

**Route table** rtb-0aec07a9b768ad4b2 (MyVPC-Private-RT)

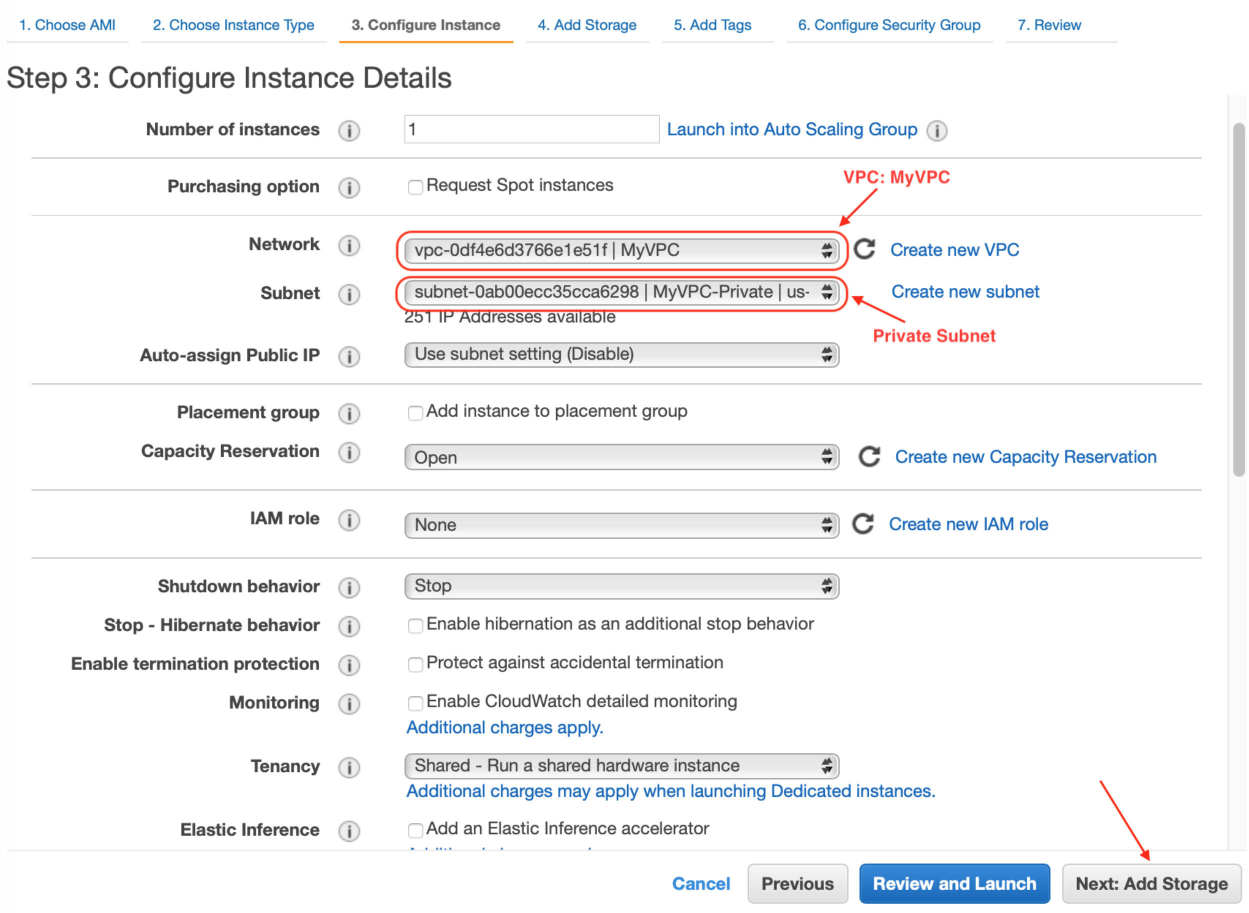
**Associated subnets** subnet-0ab00ecc35cca6298

Filter by attributes or search by keyword 1 to 2 of 2

| □ | Subnet ID | IPv4 CIDR | IPv6 CIDR | Current Route Table |
|---|---|---|---|---|
| ☑ | subnet-0ab00ecc35cca6298 \| MyVPC-Private | 10.100.1.0/24 | - | Main |
| □ | subnet-0aada8ff5fd454ec3 \| MyVPC-Public | 10.100.0.0/24 | - | rtb-02ca5122d39719980 |

* Required

## Launch another EC2 instance in same VPC but in newly created Private subnet



### Step 3: Configure Instance Details

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

VPC: MyVPC

Network: vpc-0df4e6d3766e1e51f | MyVPC — Create new VPC

Subnet: subnet-0ab00ecc35cca6298 | MyVPC-Private | us- — Create new subnet

251 IP Addresses available

Private Subnet

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

Shutdown behavior: Stop

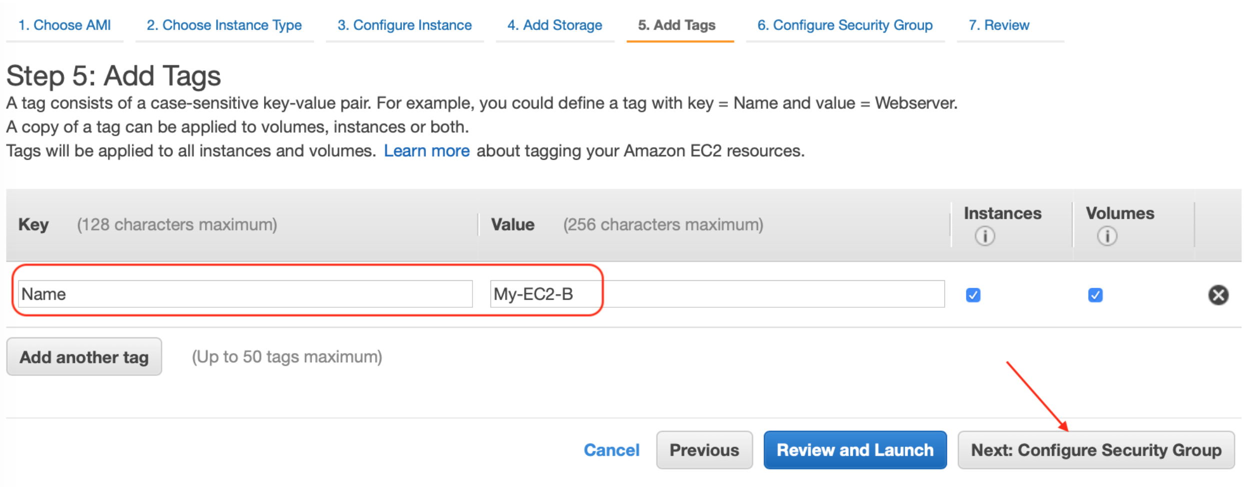
Stop - Hibernate behavior: □ Enable hibernation as an additional stop behavior

Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
Additional charges may apply when launching Dedicated instances.

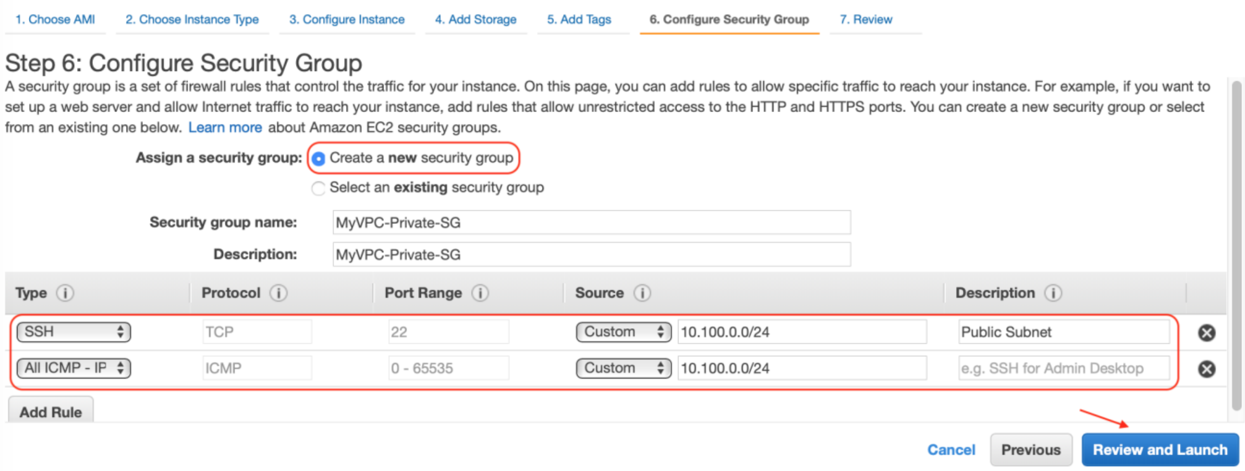
Elastic Inference: □ Add an Elastic Inference accelerator



### Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

| Key (128 characters maximum) | Value (256 characters maximum) | Instances | Volumes |
|---|---|---|---|
| Name | My-EC2-B | ☑ | ☑ |



Step 6: Configure Security Group

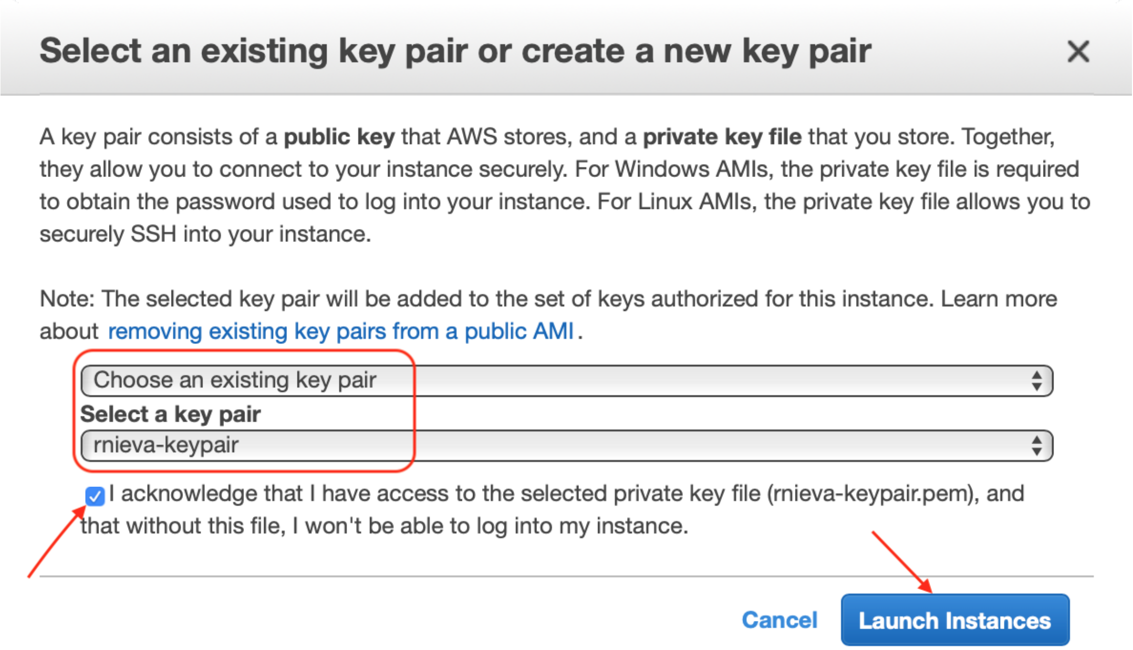
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted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

**Description:** MyVPC-Private-SG

| Type | Protocol | Port Range | Source | | Description |
|---|---|---|---|---|---|
| SSH | TCP | 22 | Custom | 10.100.0.0/24 | Public Subnet |
| All ICMP - IP | ICMP | 0 - 65535 | Custom | 10.100.0.0/24 | e.g. SSH for Admin Desktop |



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

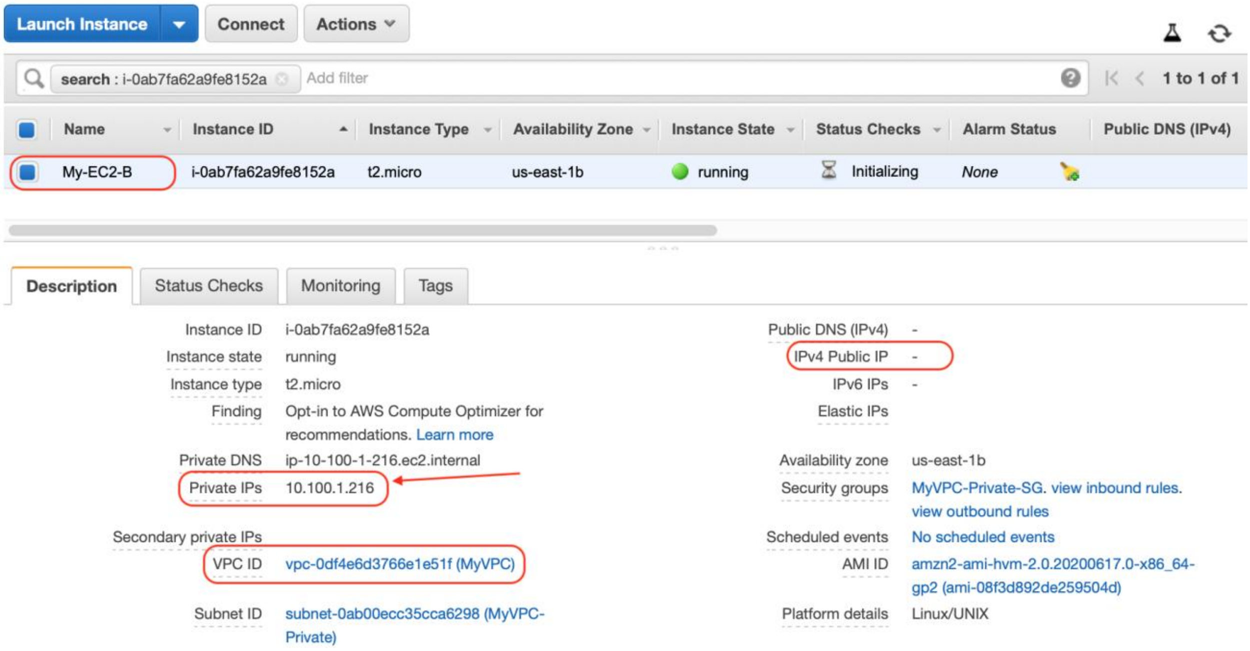
Choose an existing key pair

**Select a key pair**

rnieva-keypair

☑ I acknowledge that I have access to the selected private key file (rnieva-keypair.pem), and that without this file, I won't be able to log into my instance.

Note down the My-EC2-B private IP address.



| Name | Instance ID | Instance Type | Availability Zone | Instance State | Status Checks | Alarm Status | Public DNS (IPv4) |
|---|---|---|---|---|---|---|---|
| My-EC2-B | i-0ab7fa62a9fe8152a | t2.micro | us-east-1b | ● running | Initializing | *None* | |

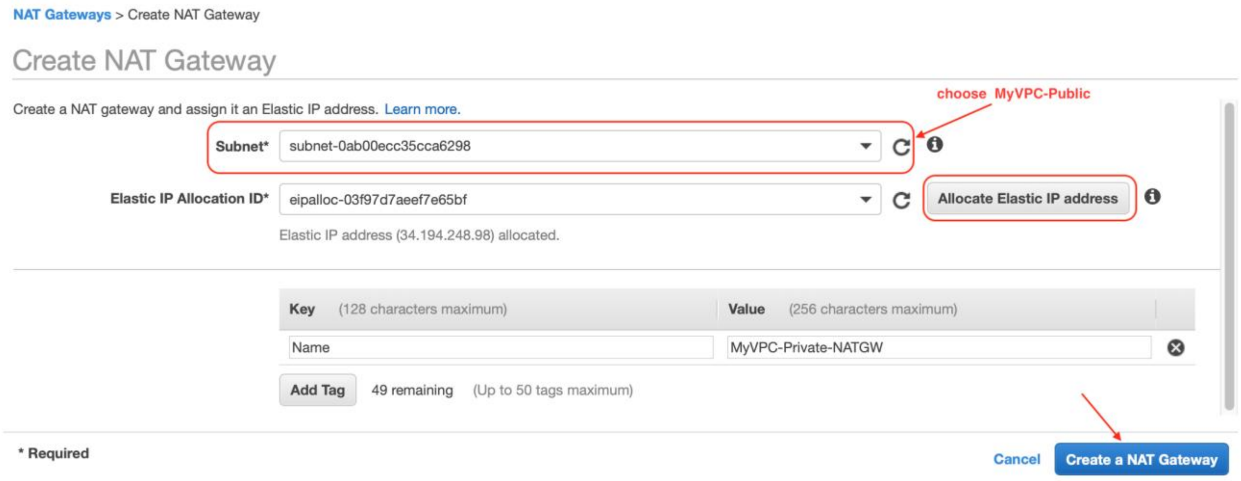
| | | | |
|---|---|---|---|
| Instance ID | i-0ab7fa62a9fe8152a | Public DNS (IPv4) | - |
| Instance state | running | IPv4 Public IP | - |
| Instance type | t2.micro | IPv6 IPs | - |
| Finding | Opt-in to AWS Compute Optimizer for recommendations. Learn more | Elastic IPs | |
| Private DNS | ip-10-100-1-216.ec2.internal | Availability zone | us-east-1b |
| Private IPs | 10.100.1.216 | Security groups | MyVPC-Private-SG. view inbound rules. view outbound rules |
| Secondary private IPs | | Scheduled events | No scheduled events |
| VPC ID | vpc-0df4e6d3766e1e51f (MyVPC) | AMI ID | amzn2-ami-hvm-2.0.20200617.0-x86_64-gp2 (ami-08f3d892de259504d) |
| Subnet ID | subnet-0ab00ecc35cca6298 (MyVPC-Private) | Platform details | Linux/UNIX |

## Try to ping EC2-B private IP from EC2-A instance

```
[ec2-user@ip-10-100-0-139 ~]$ ping -c 5 10.100.1.216
PING 10.100.1.216 (10.100.1.216) 56(84) bytes of data.
64 bytes from 10.100.1.216: icmp_seq=1 ttl=255 time=1.22 ms
64 bytes from 10.100.1.216: icmp_seq=2 ttl=255 time=0.868 ms
64 bytes from 10.100.1.216: icmp_seq=3 ttl=255 time=0.701 ms
64 bytes from 10.100.1.216: icmp_seq=4 ttl=255 time=0.725 ms
64 bytes from 10.100.1.216: icmp_seq=5 ttl=255 time=0.739 ms

--- 10.100.1.216 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4073ms
rtt min/avg/max/mdev = 0.701/0.850/1.221/0.197 ms
```

Create a NAT gateway in your VPC

VPC -> NAT Gateways -> Create NAT Gateway



NAT Gateways > Create NAT Gateway

Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. Learn more.

choose MyVPC-Public

Subnet*: subnet-0ab00ecc35cca6298

Elastic IP Allocation ID*: eipalloc-03f97d7aeef7e65bf

Elastic IP address (34.194.248.98) allocated.

| Key (128 characters maximum) | Value (256 characters maximum) |
|---|---|
| Name | MyVPC-Private-NATGW |

49 remaining (Up to 50 tags maximum)

* Required

**Add a route in Private subnet for internet traffic and route through NAT Gateway**

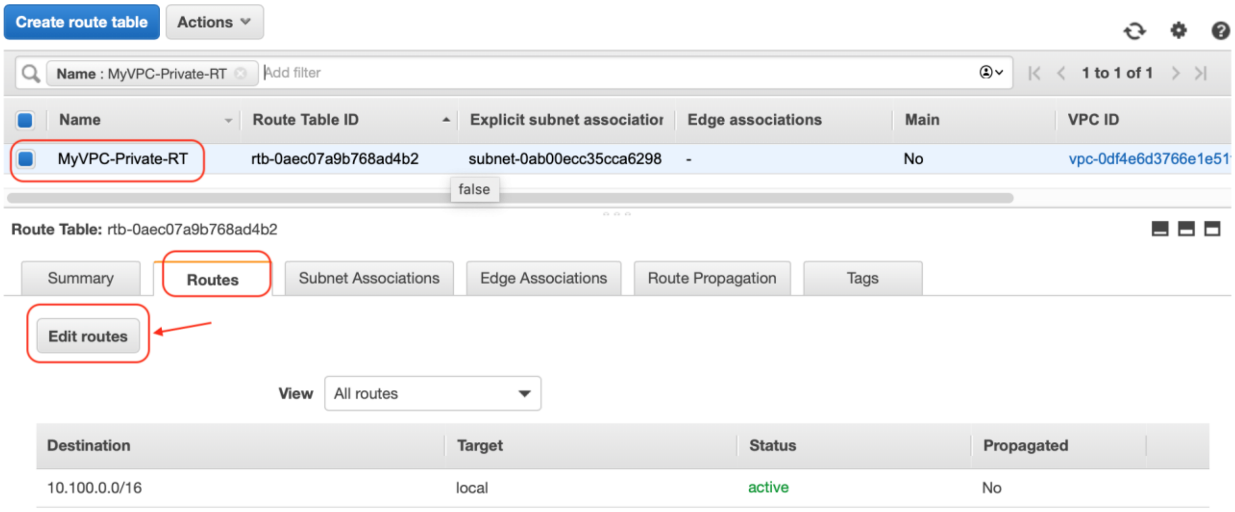
Route Tables -> Select MyVPC-Private route table

Routes -> Edit -> Add another route

Destination: 0.0.0.0/0

Target: nat-gateway

Save



Name : MyVPC-Private-RT

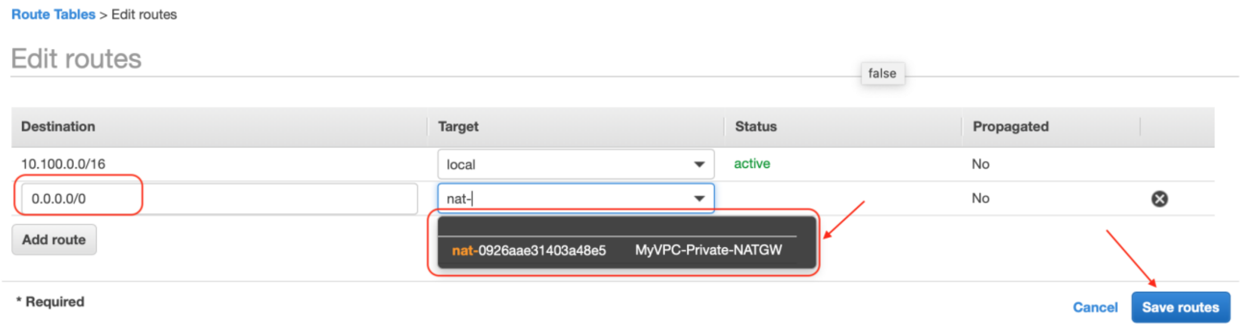
| Name | Route Table ID | Explicit subnet associatior | Edge associations | Main | VPC ID |
|---|---|---|---|---|---|
| MyVPC-Private-RT | rtb-0aec07a9b768ad4b2 | subnet-0ab00ecc35cca6298 | - | No | vpc-0df4e6d3766e1e51 |

false

Route Table: rtb-0aec07a9b768ad4b2

View: All routes

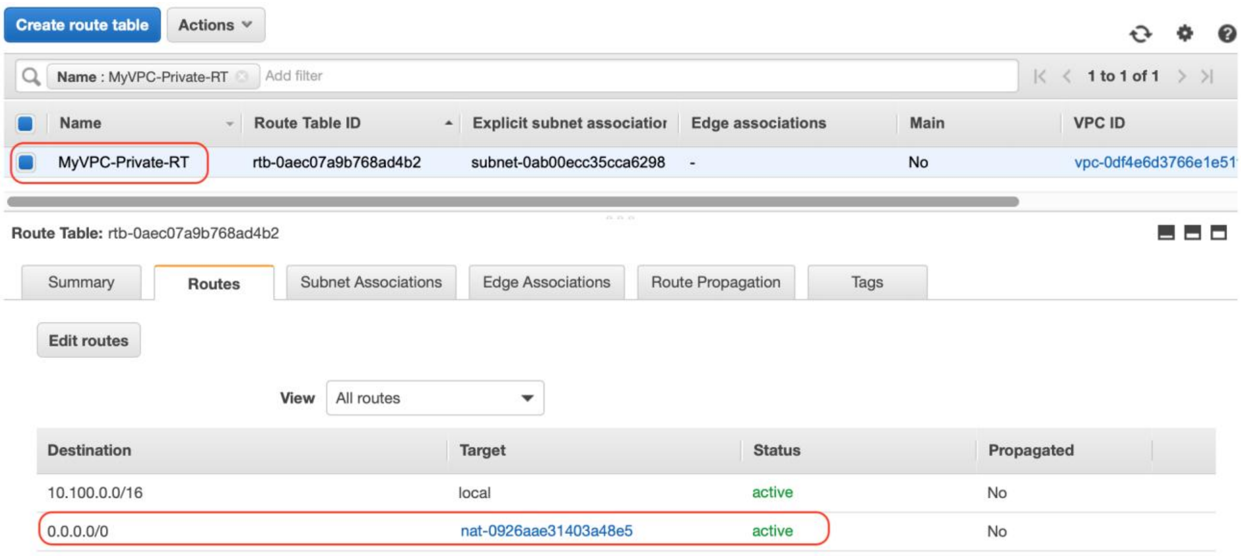
| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.100.0.0/16 | local | active | No |



Route Tables > Edit routes

Edit routes

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.100.0.0/16 | local | active | No |
| 0.0.0.0/0 | nat- | | No |



| Name | Route Table ID | Explicit subnet associatior | Edge associations | Main | VPC ID |
|---|---|---|---|---|---|
| MyVPC-Private-RT | rtb-0aec07a9b768ad4b2 | subnet-0ab00ecc35cca6298 | - | No | vpc-0df4e6d3766e1e51 |

Route Table: rtb-0aec07a9b768ad4b2

View: All routes

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.100.0.0/16 | local | active | No |
| 0.0.0.0/0 | nat-0926aae31403a48e5 | active | No |

## Try to connect to EC2-B instance from EC2-A

```
[ec2-user@ip-10-100-0-139 ~]$ touch rnieva-keypair.pem
[ec2-user@ip-10-100-0-139 ~]$ vi rnieva-keypair.pem
[ec2-user@ip-10-100-0-139 ~]$chmod 600 rnieva-keypair.pem
[ec2-user@ip-10-100-0-139 ~]$ssh -irnieva-keypair.pem ec2-user@10.100.1.216
The authenticity of host '10.100.1.216 (10.100.1.216)' can't be established.
ECDSA key fingerprint is SHA256:200tS7bQDvWk06Gr0mhornCZepZVwUMj0xfFTharR7U.
ECDSA key fingerprint is MD5:1c:2d:3f:43:40:ec:f1:4d:67:22:8b:31:3b:b0:04:d7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.100.1.216' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-100-1-216 ~]$ uptime
 21:40:06 up 19 min,  1 user,  load average: 0.00, 0.00, 0.00
```

## Try to ping google.com from MyEC2-B

```
[ec2-user@ip-10-100-1-216 ~]$ ping -c 3 google.com
PING google.com (172.217.8.14) 56(84) bytes of data.
64 bytes from iad23s59-in-f14.1e100.net (172.217.8.14): icmp_seq=1 ttl=113
time=2.43 ms
64 bytes from iad23s59-in-f14.1e100.net (172.217.8.14): icmp_seq=2 ttl=113
time=1.89 ms
64 bytes from iad23s59-in-f14.1e100.net (172.217.8.14): icmp_seq=3 ttl=113
time=1.85 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.852/2.061/2.437/0.268 ms
```