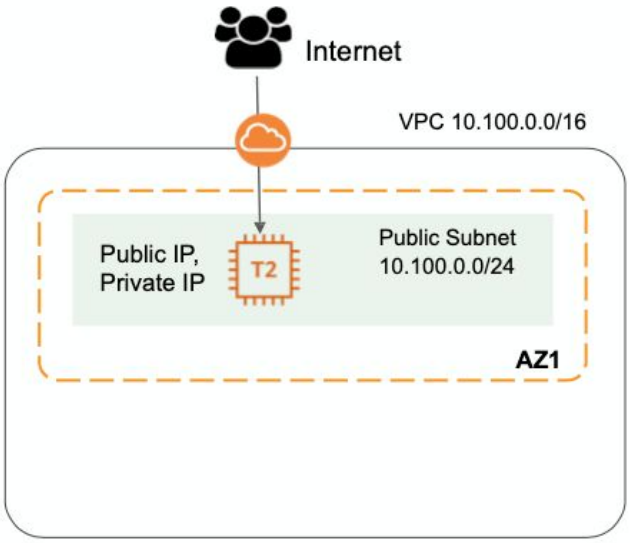

DevOps
CERTIFICACIÓN
Universitaria
UNC
FCEFyN
mE

LAB-VPC-1

VPC with Single Public Subnet



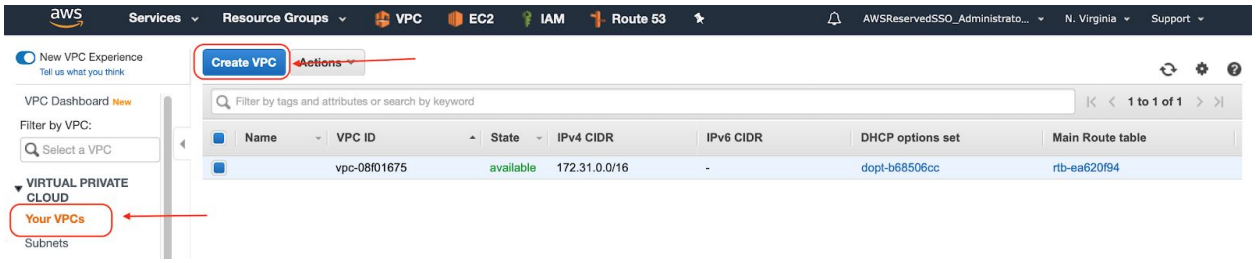
Public Subnet Route Table

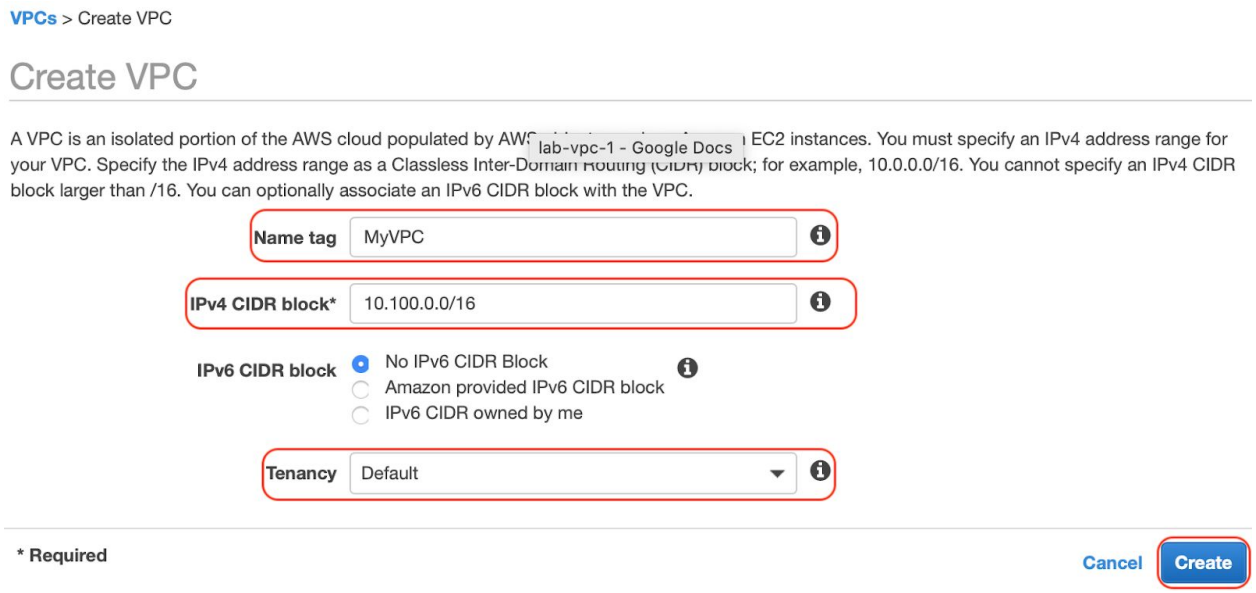
Destination	Target
10.100.0.0/16	local
0.0.0.0/0	igw-xxx

Resolution

Create VPC

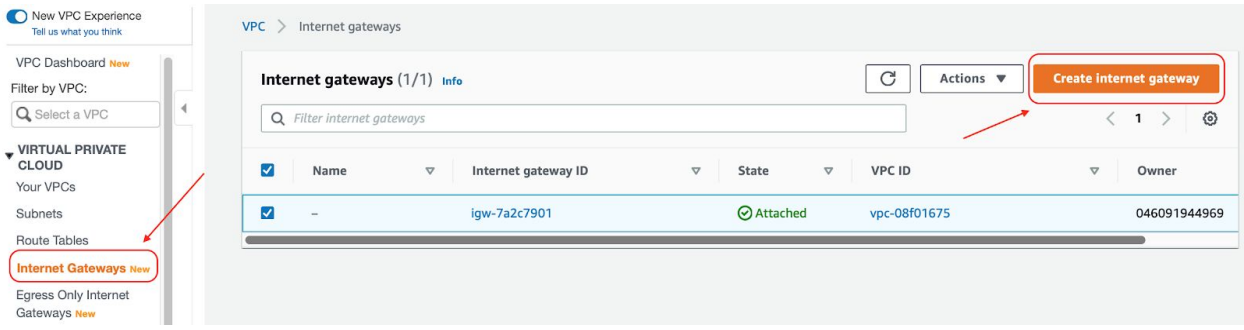
Go to VPC service -> Your VPCs -> Create VPC (Name: MyVPC, CIDR: 10.100.0.0/16) -> Create

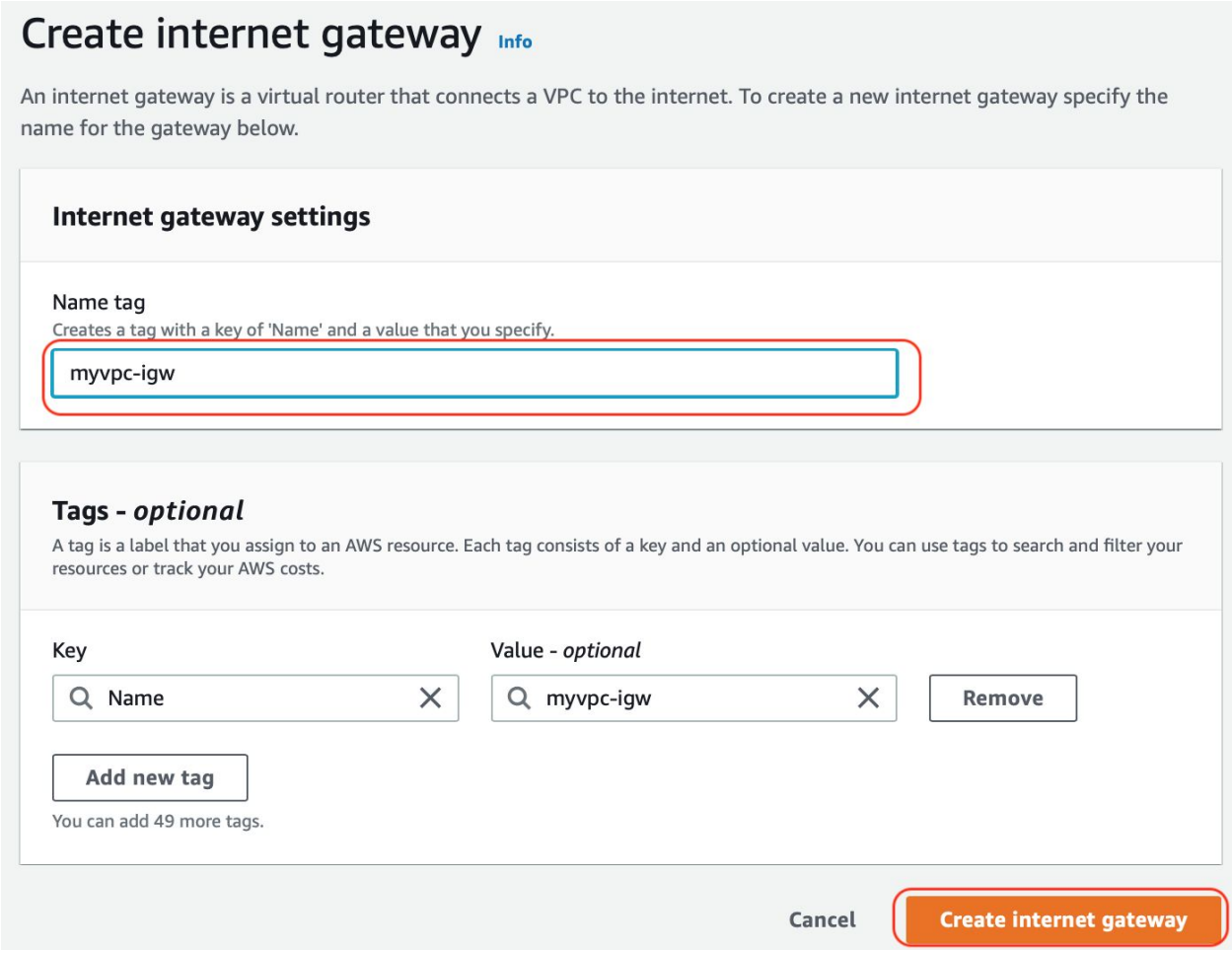




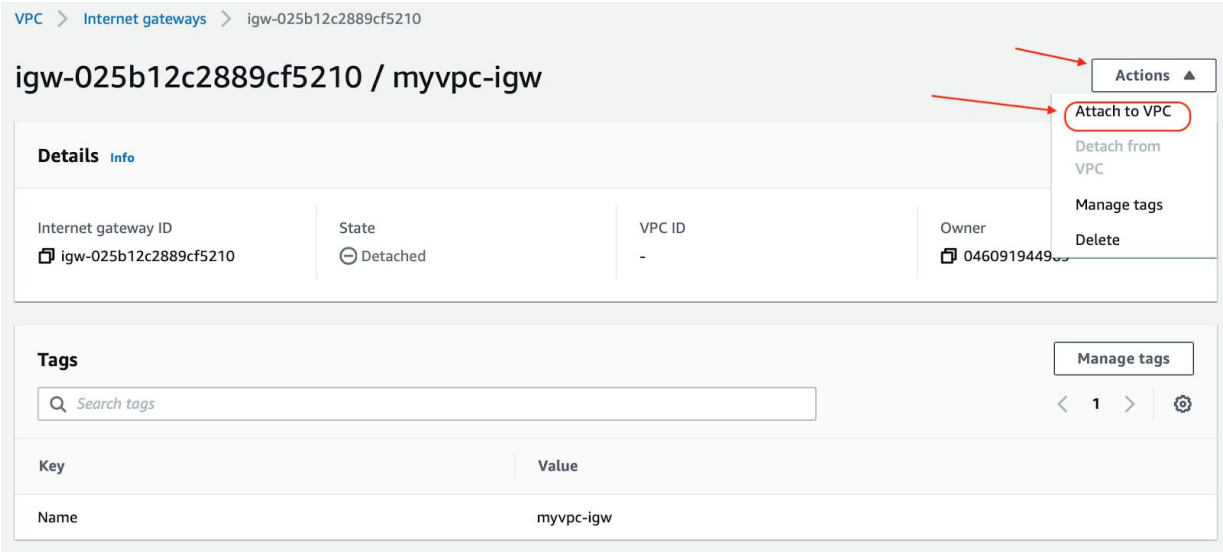
Create Internet Gateway

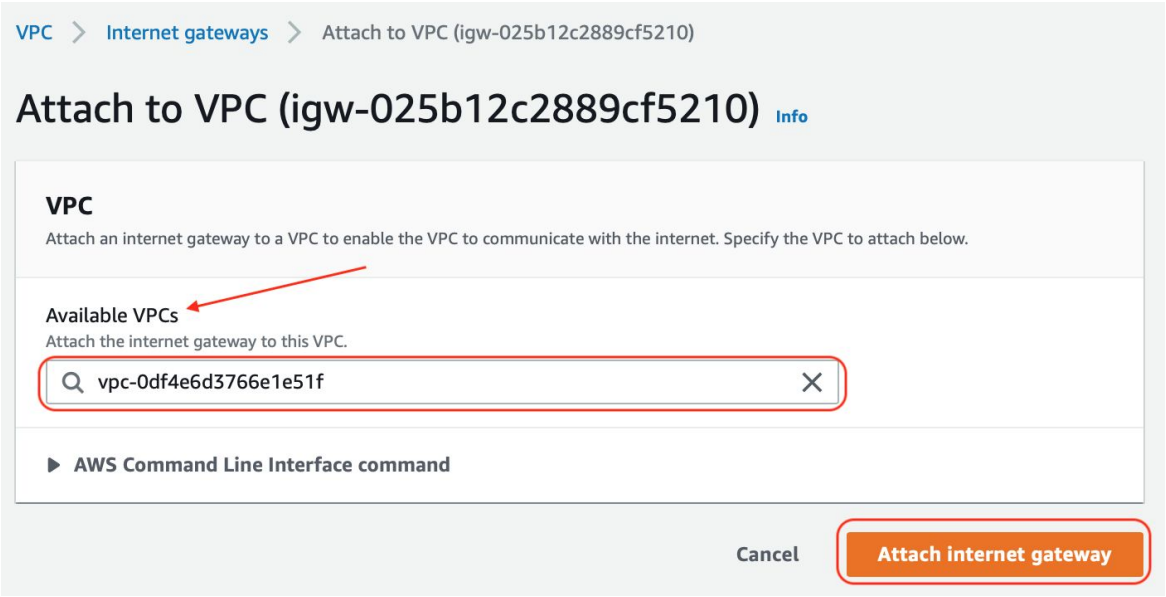
Go to Internet Gateways -> Create internet gateway





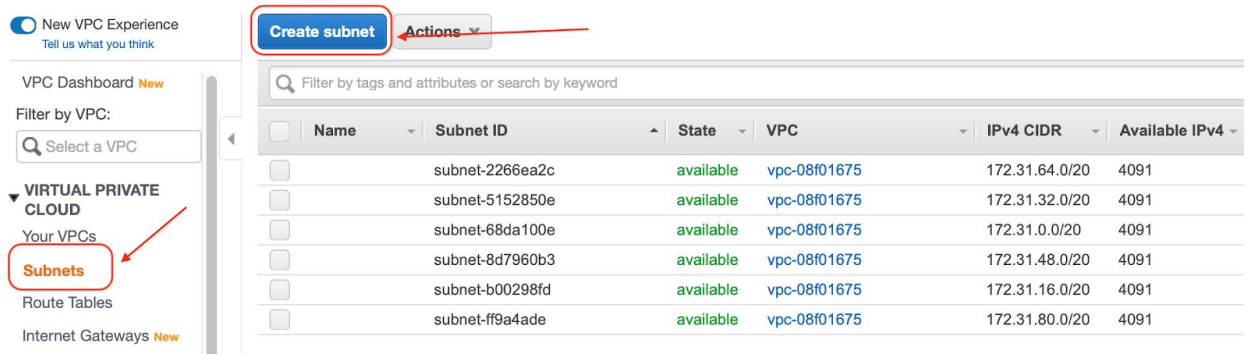
Attach Internet Gateway to VPC
Select Internet gateway -> Actions -> Attach to VPC -> Select your VPC

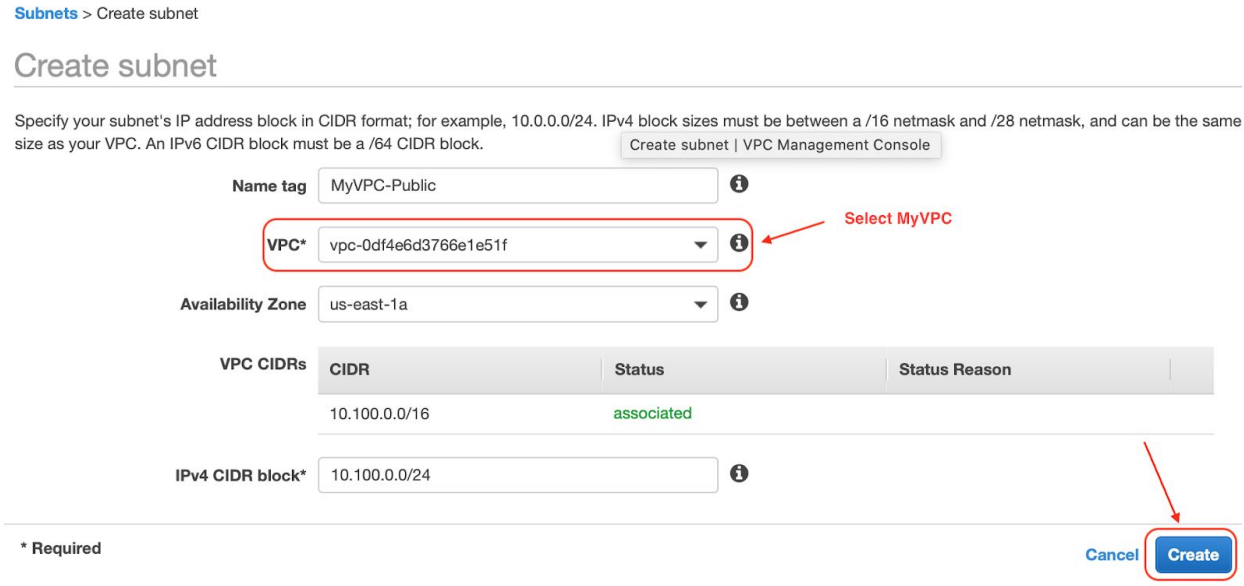




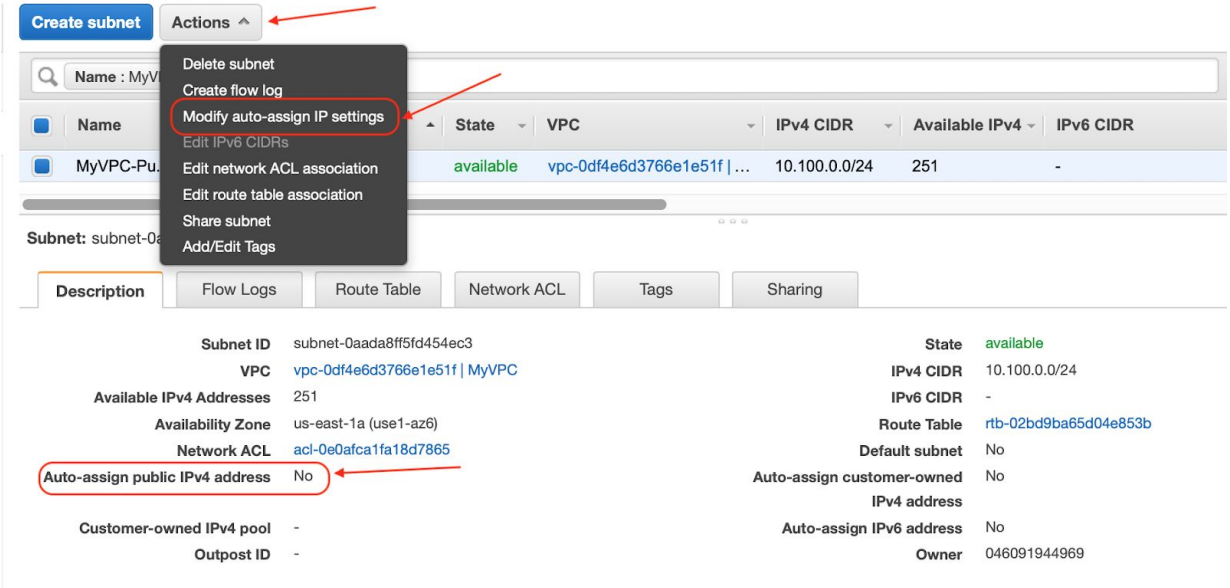
Create Subnet

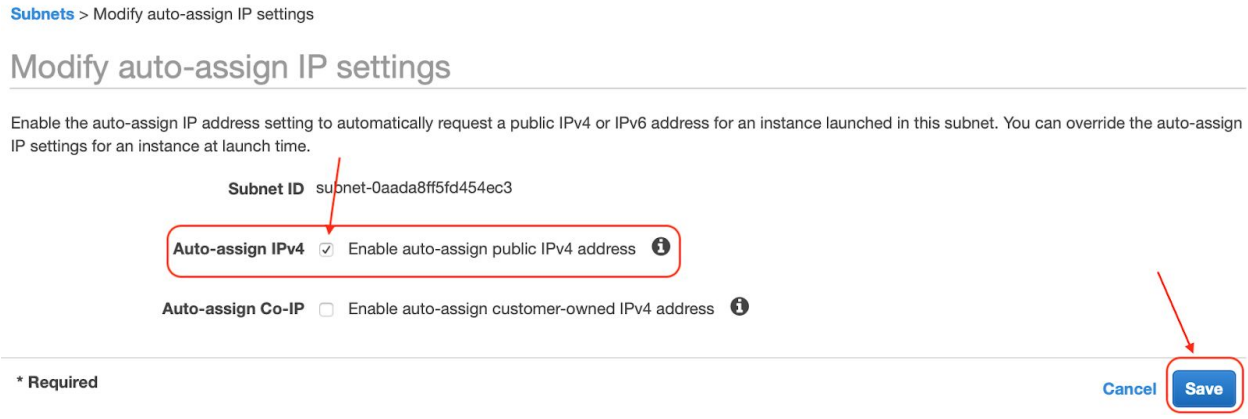
Subnets -> Create subnet (Name: MyVPC-Public, VPC: MyVPC, AZ: Select first az - us-east-1a, CIDR: 10.100.0.0/24)





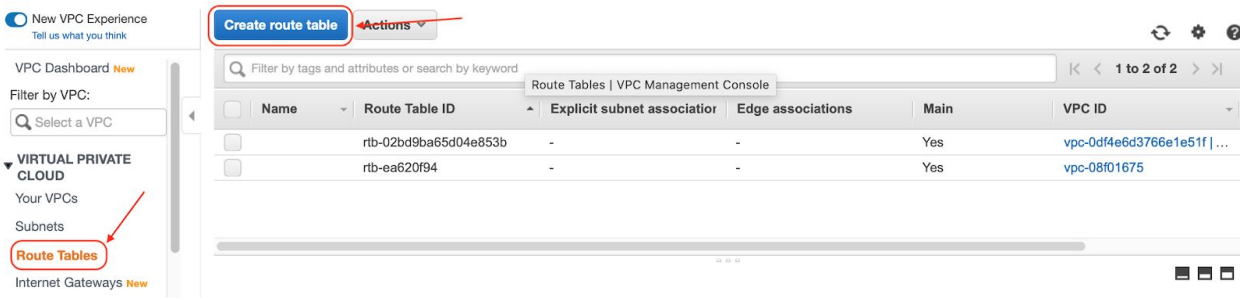
Select Subnet -> Action -> Modify Auto Assign Public IP -> Enable -> Save

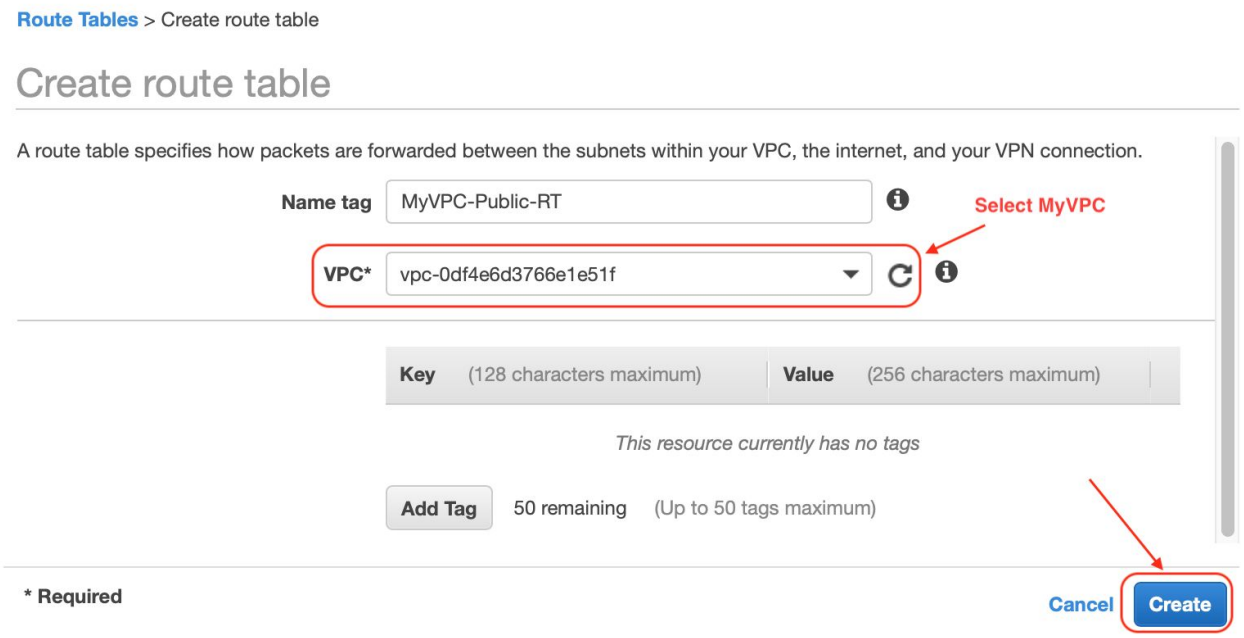




Create Route Table

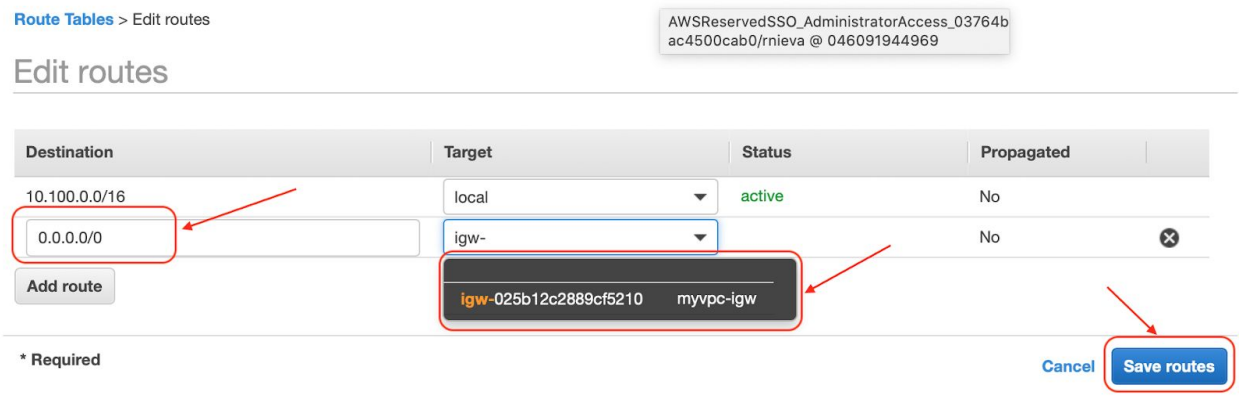
Route Tables -> Create Route Table (Name: MyVPC-Public, VPC: MyVPC)





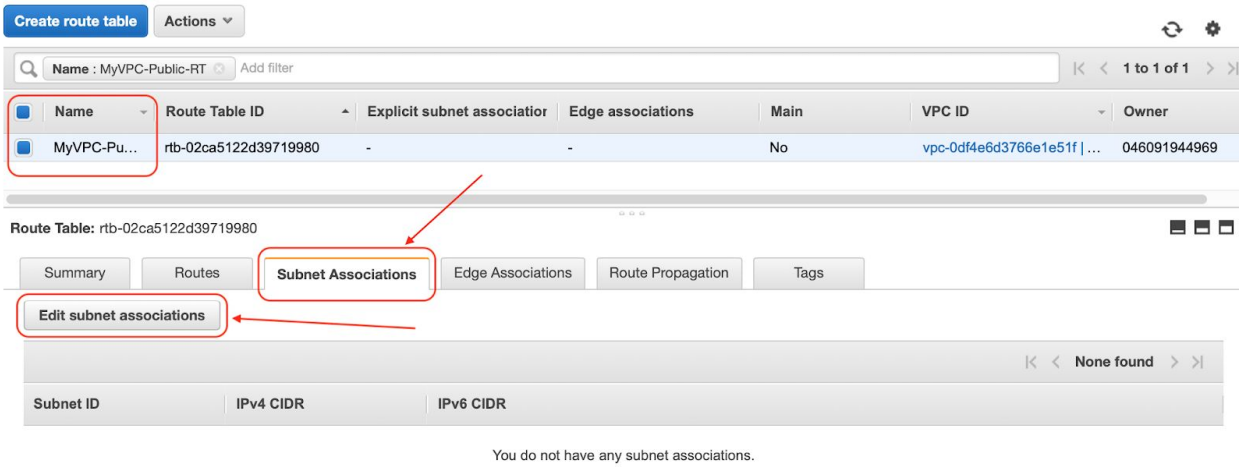
Add route to send all traffic that is not local to Internet Gateway

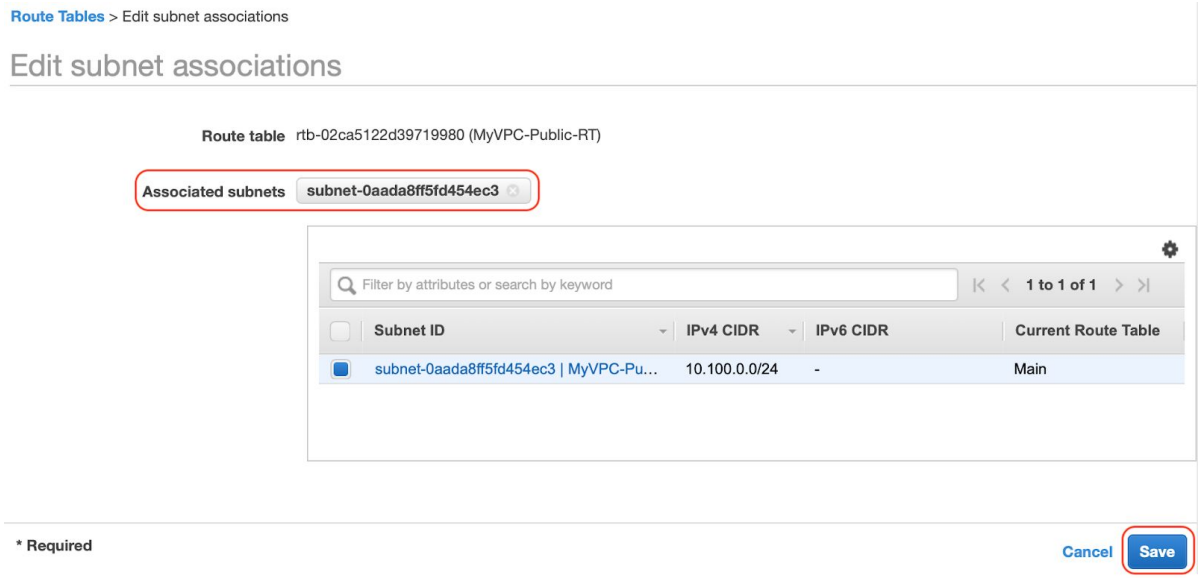
Select Route table -> Routes -> Edit -> Add another route (Destination: 0.0.0.0/0, Target: Internet gateway -> igw-xxx) -> Save



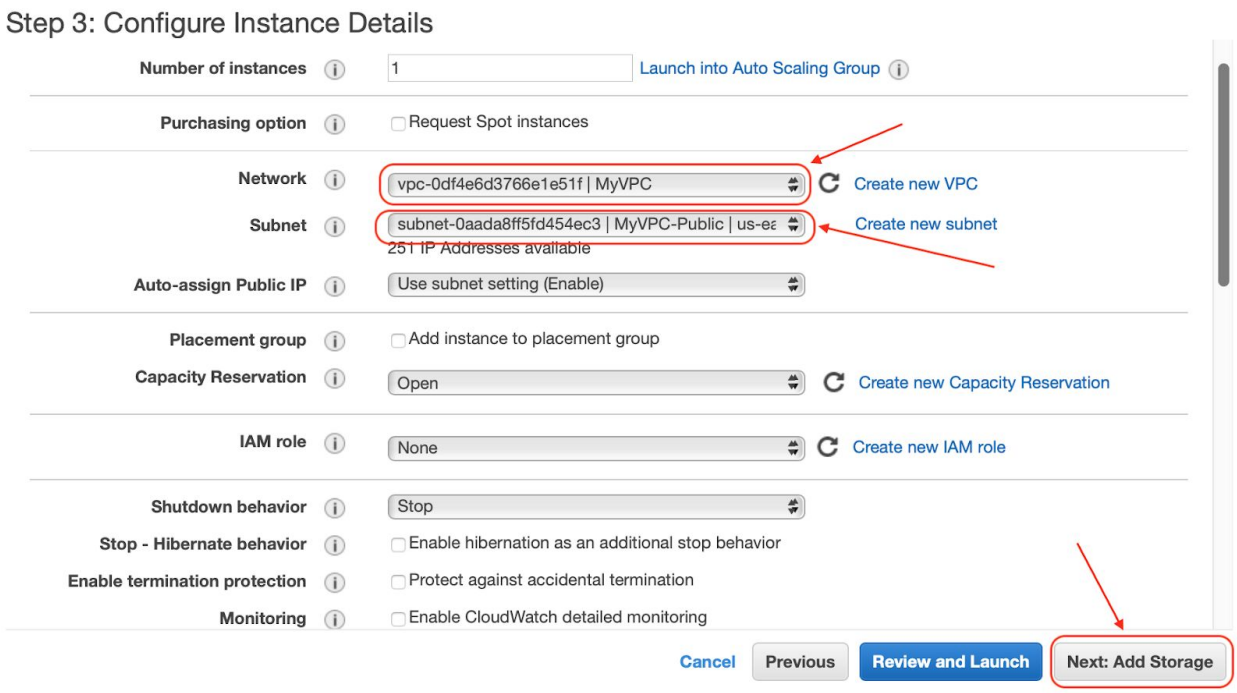
Associate Route table with Subnet to make it Public Subnet

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





Launch EC2 instance in newly created Public Subnet



1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | 4. Add Storage | 5. Add Tags | 6. Configure Security Group | 7. Review

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	☑	☑

Add another tag (Up to 50 tags maximum)

Cancel | Previous | Review and Launch | Next: Configure Security Group

Configure Security Group

1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | 4. Add Storage | 5. Add Tags | 6. Configure Security Group | 7. Review

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

Add Rule

Cancel | Previous | Review and Launch

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

Download Key Pair

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.

Cancel | Launch Instances

Launch Instance | Connect | Actions

search : i-09d843b215b20c666 | Add filter | 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**

Description | Status Checks | Monitoring | Tags

Instance ID	i-09d843b215b20c666
Instance state	running
Instance type	t2.micro
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Private DNS	ip-10-100-0-139.ec2.internal
Private IPs	10.100.0.139
Secondary private IPs	
VPC ID	vpc-0df4e6d3766e1e51f (MyVPC)
Subnet ID	subnet-0aada8ff5fd454ec3 (MyVPC-Public)
Network interfaces	eth0

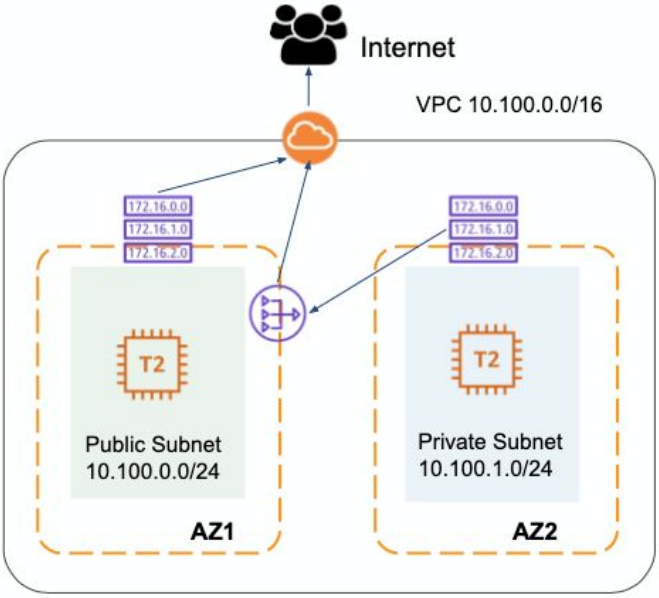
Public DNS (IPv4)	-
IPv4 Public IP	54.211.247.181
IPv6 IPs	-
Elastic IPs	
Availability zone	us-east-1a
Security groups	MyVPC-SG. view inbound rules. view outbound rules
Scheduled events	No scheduled events
AMI ID	amzn2-ami-hvm-2.0.20200617.0-x86_64-gp2 (ami-08f3d892de259504d)
Platform details	Linux/UNIX
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 -i rnieva-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

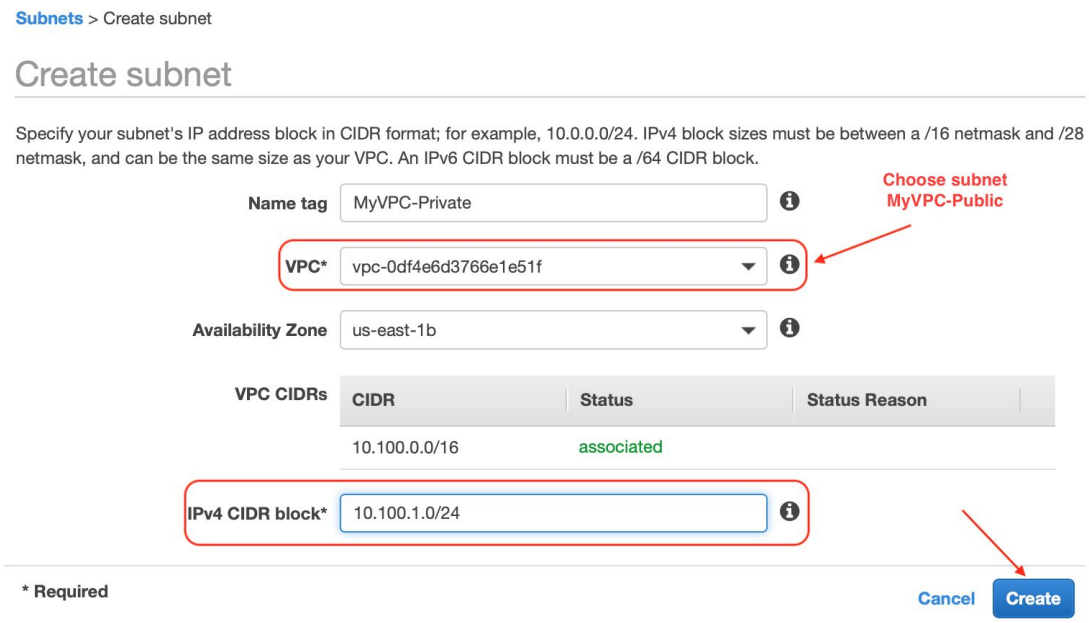
Private Subnet Route Table

Destination	Target
10.100.0.0/16	local

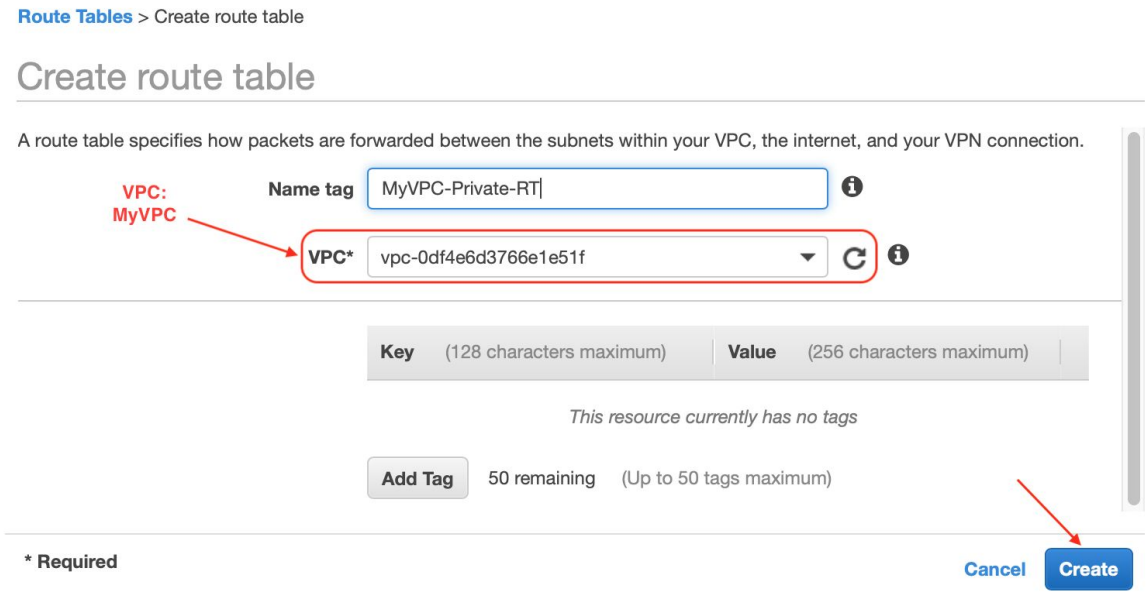
Solution:

Create a Private Subnet

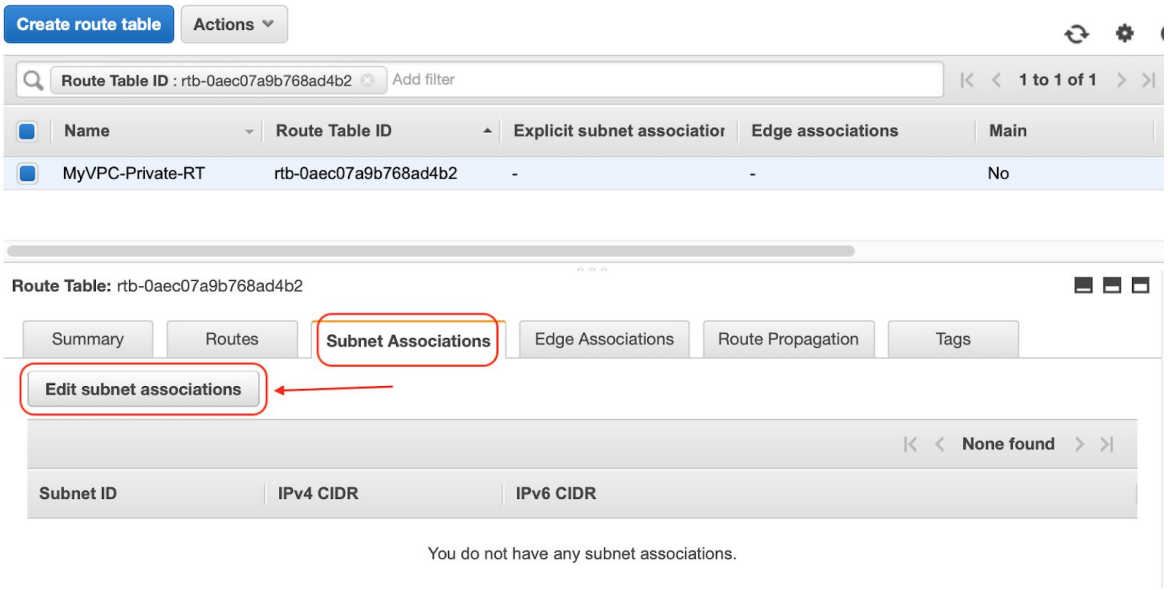
Create subnet (Name: MyVPC-Private, VPC: MyVPC, AZ: Select different az (us-east-1b), CIDR: 10.100.1.0/24) 2. Create Private route table

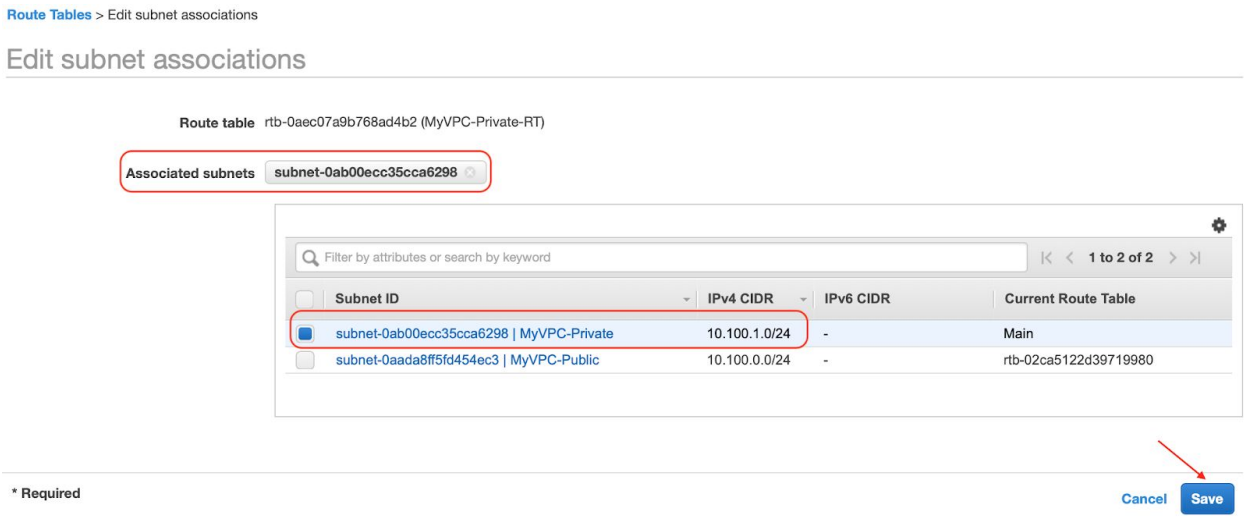


Create Private route table
Route Tables -> Create Route Table (Name: MyVPC-Private, VPC: MyVPC)

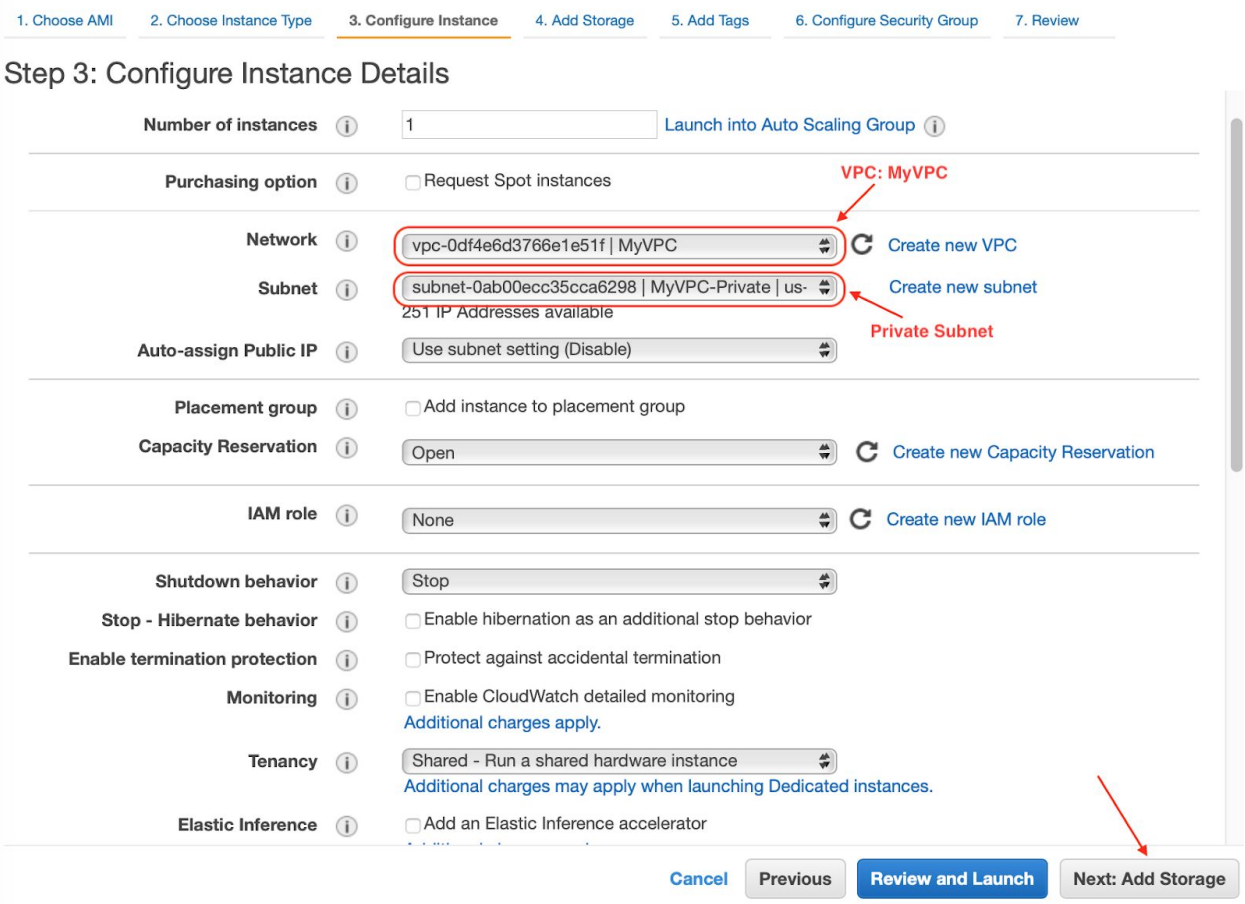


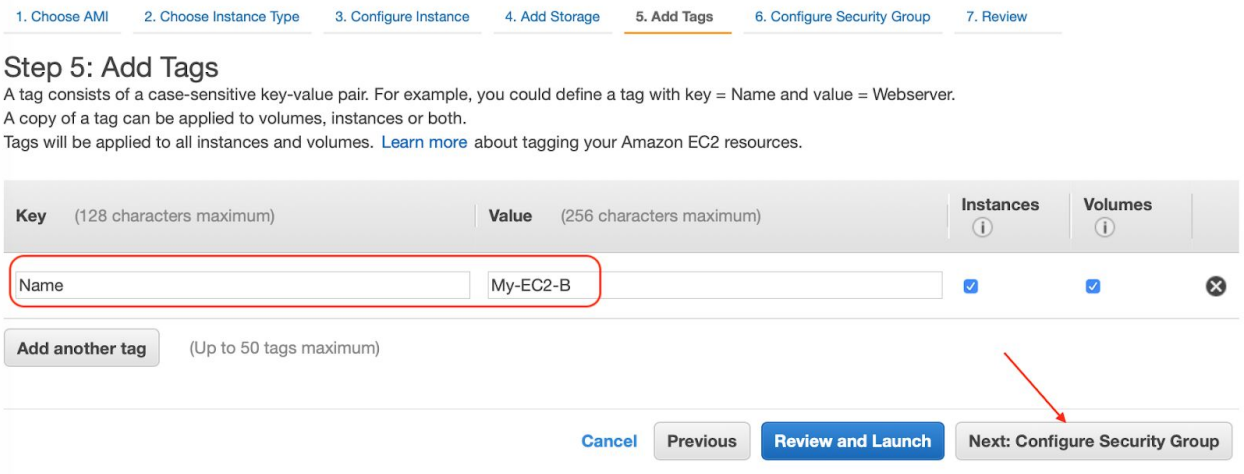
Associate Route table with Subnet to make it Private subnet
Select Route table -> Subnet Associations -> Edit -> Check the MyVPC-Private subnet -> Save





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





1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | 4. Add Storage | 5. Add Tags | 6. Configure Security Group | 7. Review

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

Add Rule

Cancel | Previous | Review and Launch

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

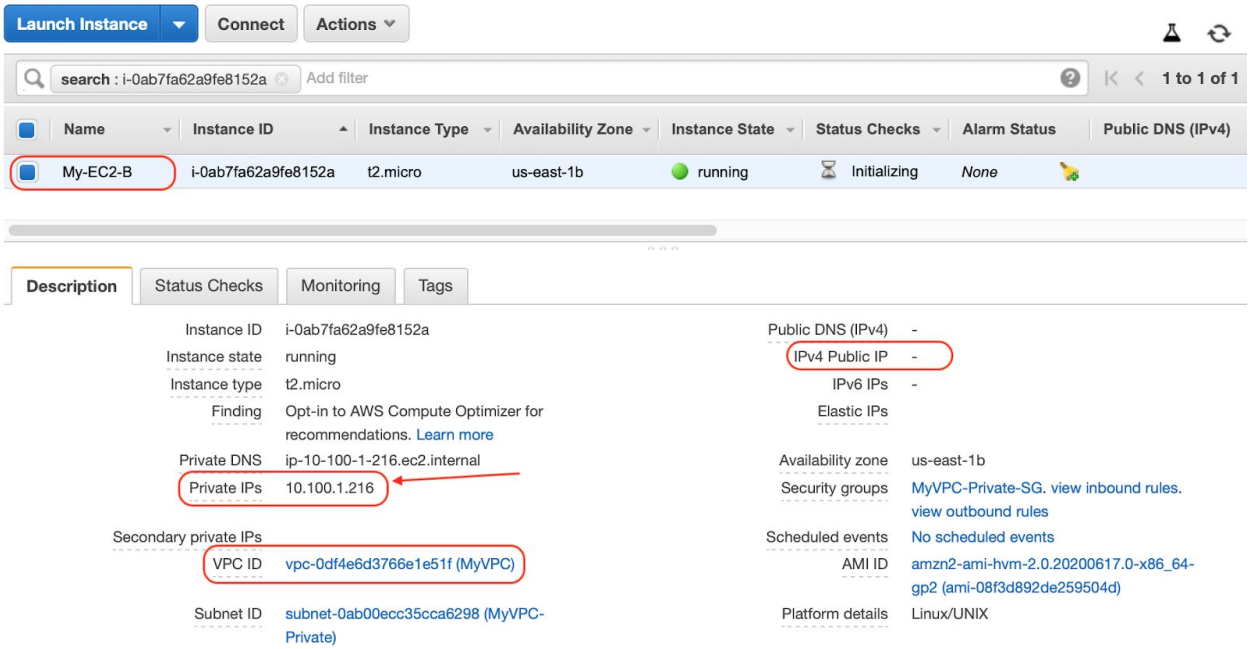
Select a key pair

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.

Cancel | Launch Instances

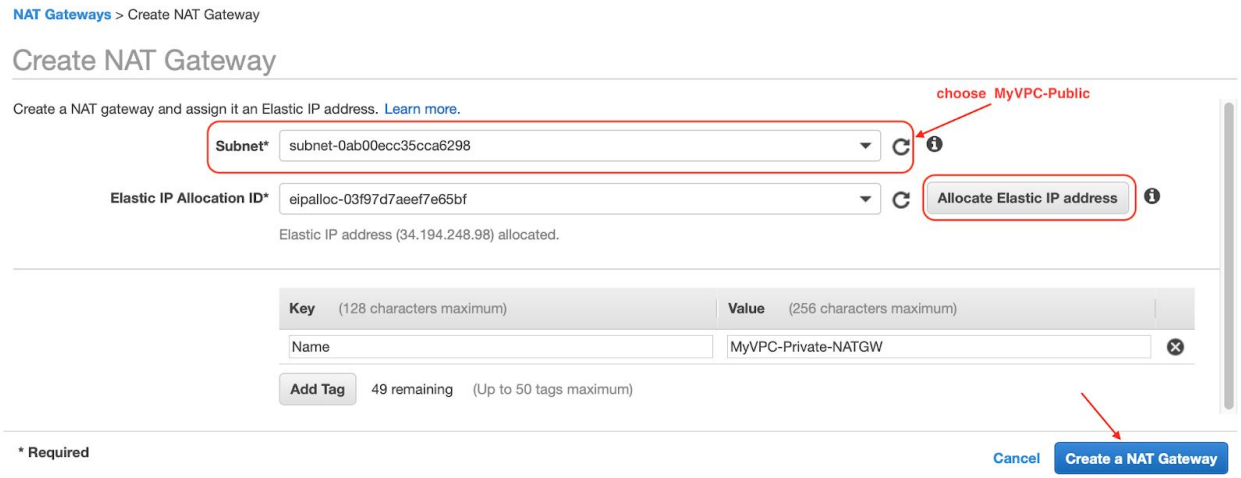
Note down the My-EC2-B private IP address.



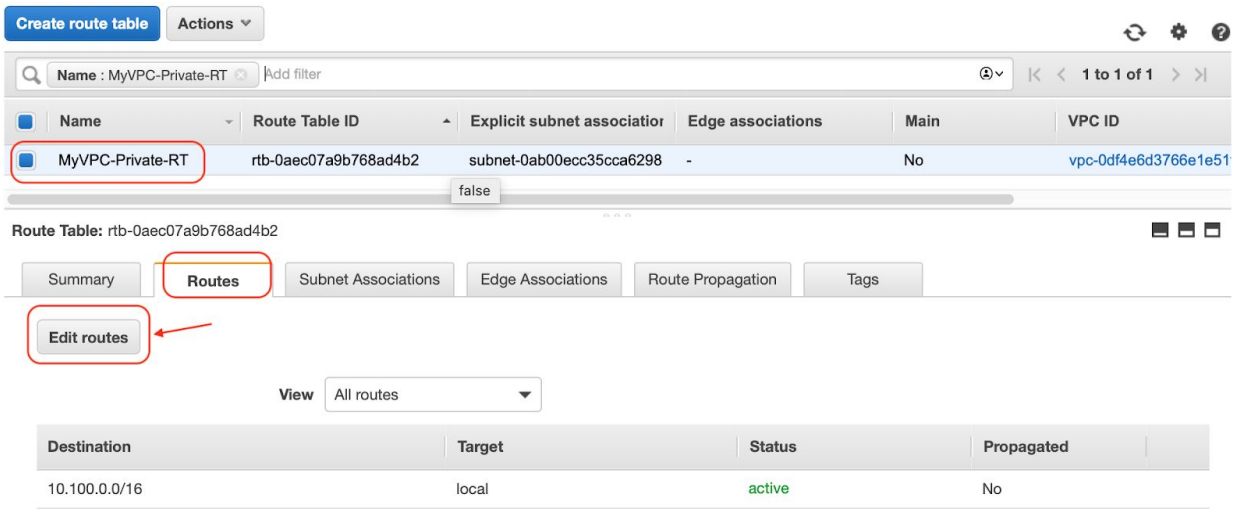
Try to ping EC2-B private IP from EC2-A instance

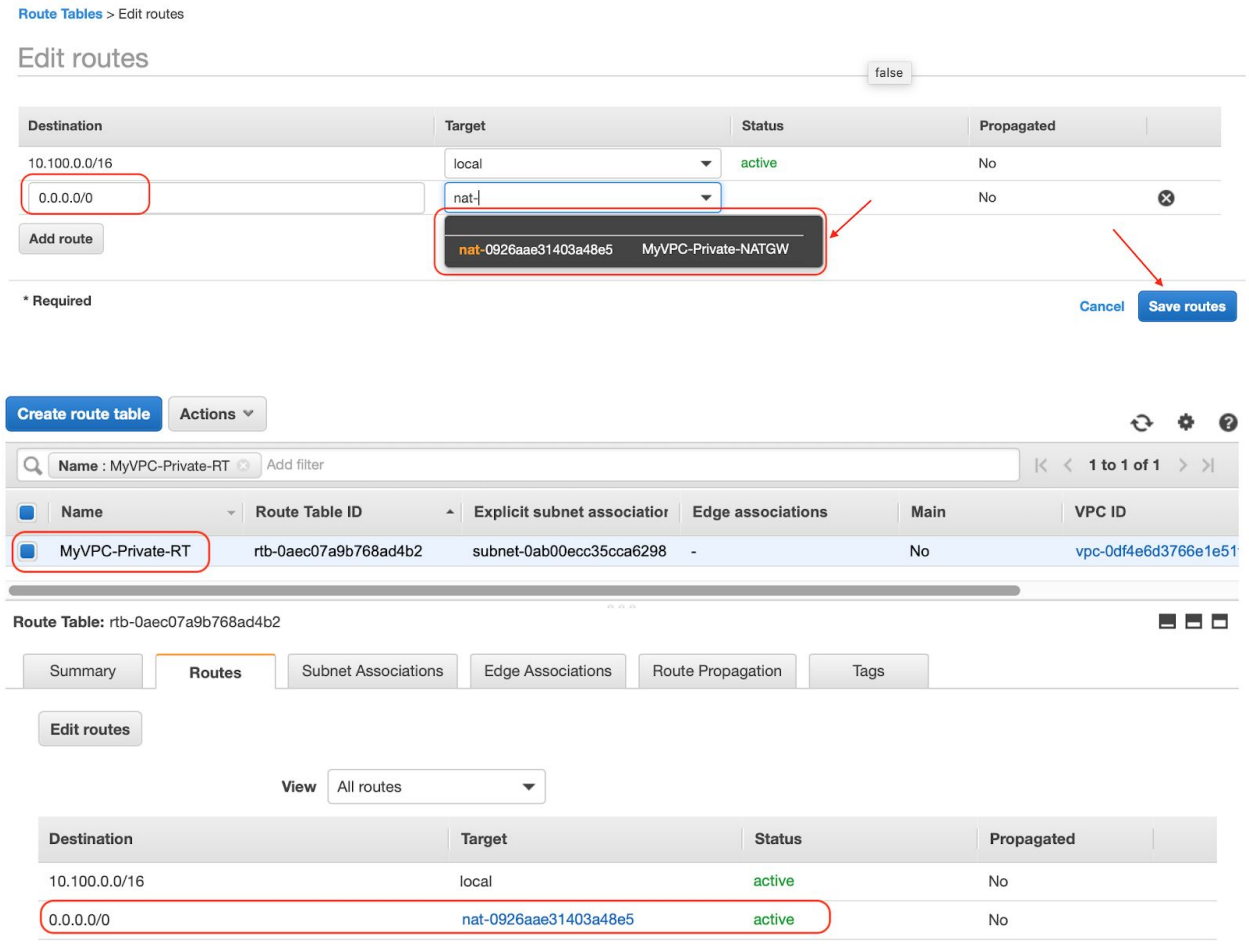
```
[ec2-user@ip-10-100-0-139 ~]$ ping -c 5 10.100.1.216
PING 10.100.1.216 (10.100.1.216) 56(84) bytes of data.
64 bytes from 10.100.1.216: icmp_seq=1 ttl=255 time=1.22 ms
64 bytes from 10.100.1.216: icmp_seq=2 ttl=255 time=0.868 ms
64 bytes from 10.100.1.216: icmp_seq=3 ttl=255 time=0.701 ms
64 bytes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



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





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 -i rnieva-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
```