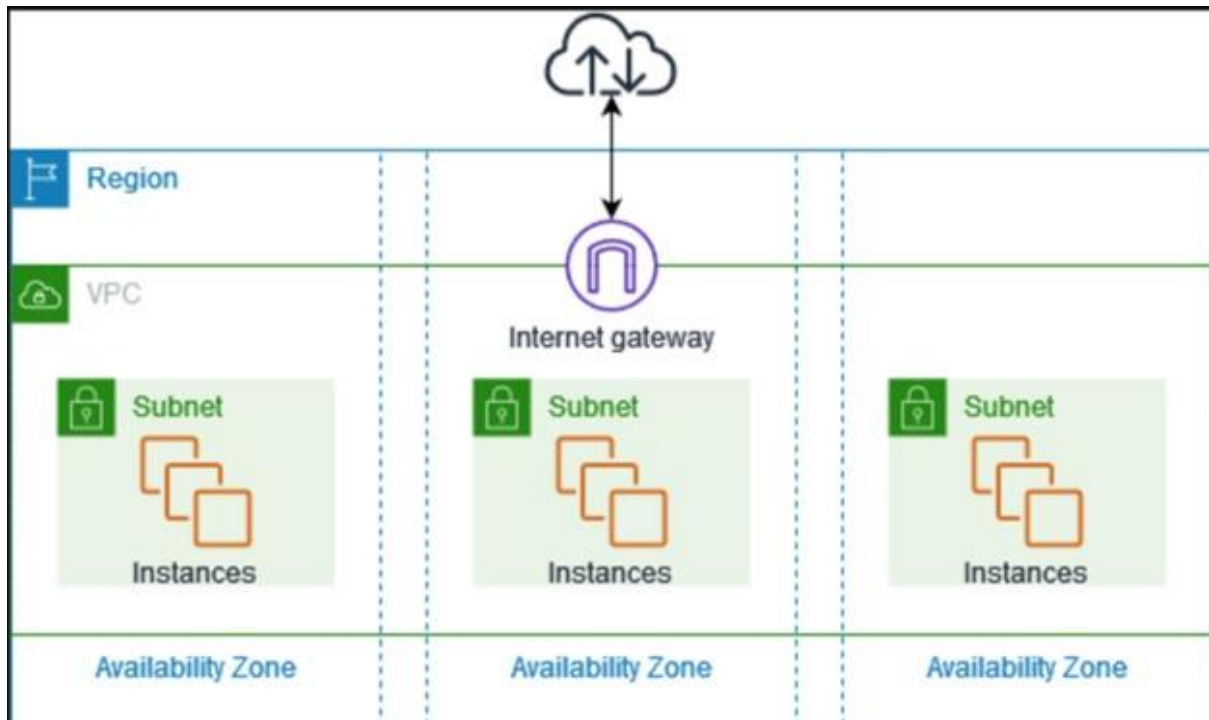


VPC Experiment



Navigate to VPC dashboard.

The screenshot shows the AWS VPC dashboard for the United States (N. Virginia) region. The dashboard includes a sidebar with navigation links for VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections, Security, Network ACLs, Security groups, PrivateLink, and VPC endpoints. The main content area displays a table of resources by region, with a 'Refresh Resources' button. The table lists various VPC resources and their counts in the United States region.

Resource	United States
VPCs	1
Subnets	6
Route Tables	1
Internet Gateways	1
Egress-only Internet Gateways	0
NAT Gateways	0
VPC Peering Connections	0
Network ACLs	1
Security Groups	1
Customer Gateways	0

Additional information on the right side of the dashboard includes Service Health, Settings, and AWS Network Manager.

Create a VPC with custom name and IPv4

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)
Create only the VPC, resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

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

VPC-exp

IPv4 CIDR block [Info](#)
☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Now head to subnets section and create two subnets

Subnets (6) [Info](#)

Find resources by attribute or tag

<input type="checkbox"/>	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
<input type="checkbox"/>	-	subnet-04e891439e6b894bb	Available	vpc-05be0f705e22ddbcc	Off	172.31.80.0/20
<input type="checkbox"/>	-	subnet-01ab915c6259c7cd8	Available	vpc-05be0f705e22ddbcc	Off	172.31.32.0/20
<input type="checkbox"/>	-	subnet-04a01d37795c29b7a	Available	vpc-05be0f705e22ddbcc	Off	172.31.64.0/20
<input type="checkbox"/>	-	subnet-025f2066194a878c9	Available	vpc-05be0f705e22ddbcc	Off	172.31.48.0/20
<input type="checkbox"/>	-	subnet-02d76ab94ed883f63	Available	vpc-05be0f705e22ddbcc	Off	172.31.16.0/20
<input type="checkbox"/>	-	subnet-098f843f36fe9c5c8	Available	vpc-05be0f705e22ddbcc	Off	172.31.0.0/20

Select a subnet

This Is a public subnet for web server

Create subnet [Info](#)

VPC
VPC ID
Create subnets in this VPC.
vpc-0212ee3c9390511e1 (VPC-exp)

Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
web-subnet
The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / us-east-1a

This is a private subnet for DB

The screenshot shows the 'Create subnet' page in the AWS Management Console. The breadcrumb navigation is 'VPC > Subnets > Create subnet'. The page is titled 'Associated VPC CIDRs' and shows 'IPv4 CIDRs' as '10.0.0.0/16'. Below this is the 'Subnet settings' section with the instruction 'Specify the CIDR blocks and Availability Zone for the subnet.' Under 'Subnet 1 of 1', there are three fields: 'Subnet name' with the value 'db-subnet', 'Availability Zone' set to 'No preference', and 'IPv4 VPC CIDR block' set to '10.0.0.0/16'. At the bottom, the 'IPv4 subnet CIDR block' is set to '10.0.2.0/24' with a note '256 IPs'.

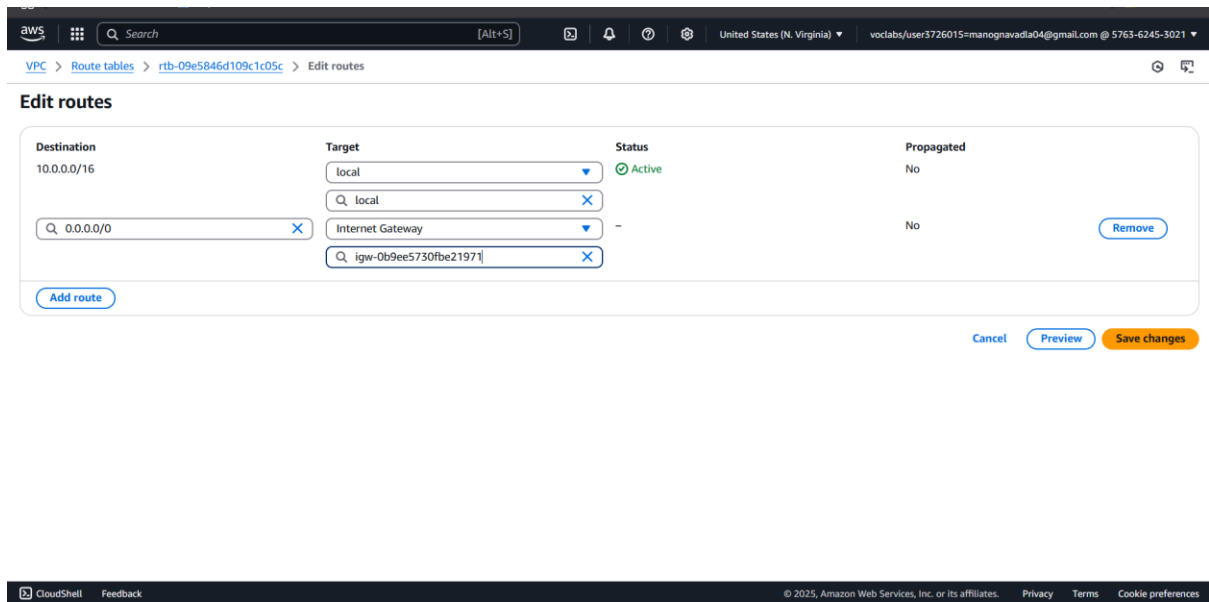
Now we are creating a Internet Gateway: provide a name to it.

The screenshot shows the 'Create internet gateway' page in the AWS Management Console. The breadcrumb navigation is 'VPC > Internet gateways > Create internet gateway'. The page is titled 'Create internet gateway' with an 'Info' icon. Below the title is a description: '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.' The 'Internet gateway settings' section has a 'Name tag' field with the value 'gateway-1'. Below this is the 'Tags - optional' section with a description: '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.' There are two tag fields: 'Key' with the value 'Name' and 'Value - optional' with the value 'gateway-1'. There are 'Add new tag' and 'Remove' buttons. At the bottom right are 'Cancel' and 'Create internet gateway' buttons.

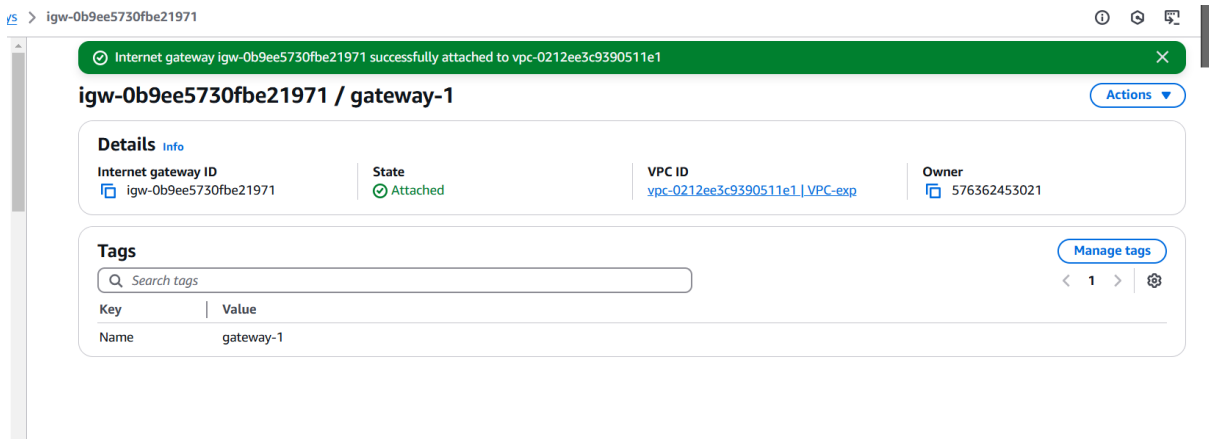
Then create a Route Table

The screenshot shows the 'Create route table' page in the AWS Management Console. The breadcrumb navigation is 'VPC > Route tables > Create route table'. The page is titled 'Create route table' with an 'Info' icon. Below the title is a description: 'A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.' The 'Route table settings' section has a 'Name - optional' field with the value 'route-table' and a 'VPC' dropdown menu with the value 'vpc-0212ee3c9390511e1 (VPC-exp)'. Below this is the 'Tags' section with a description: '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.' There are two tag fields: 'Key' with the value 'Name' and 'Value - optional' with the value 'route-table'. There are 'Add new tag' and 'Remove' buttons. At the bottom right are 'Cancel' and 'Create route table' buttons.

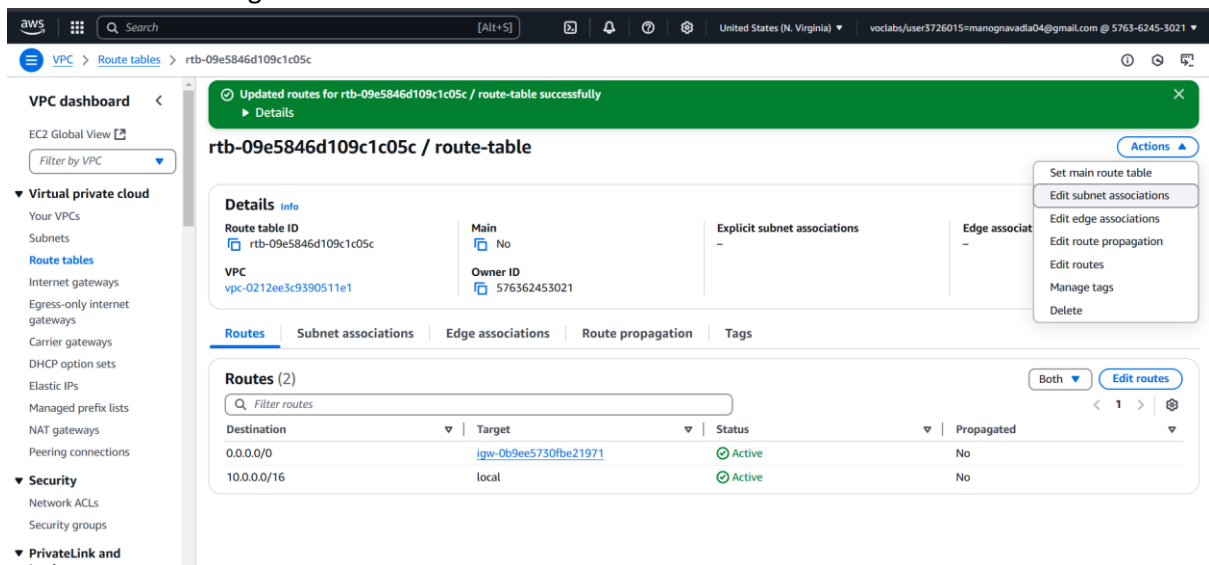
Now we should edit routes for that and add a rule. i.e add Internet Gateway and provide your gateway.



now we should connect our VPC to our gateway.



under route actions go for “edit subnet associations”



Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

☐

Name

▼

Subnet ID

▼

IPv4 CIDR

▼

IPv6 CIDR

▼

Route table ID

▼

☐

db-subnet

[subnet-048b1f32093761192](#)

10.0.2.0/24

–

[Main \(rtb-09430566e51b86053\)](#)

☒

web-subnet

[subnet-05abc2a9adb9c1546](#)

10.0.1.0/24

–

[rtb-09e5846d109c1c05c / route-table](#)

Selected subnets

subnet-05abc2a9adb9c1546 / web-subnet

✕

Cancel

Save associations

[illegible][illegible]

Security group rule 2 (TCP, 80, 0.0.0.0/0)

Type	Protocol	Port range
ssh	TCP	22

Security group rule 3 (TCP, 443, 0.0.0.0/0)

Type	Protocol	Port range
HTTPS	TCP	443

Summary

- Number of instances: 1
- Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...
- Virtual server type (instance type): t2.micro
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier.

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

```
#!/bin/bash
```

```
sudo su
```

```
yum update -y
```

```
yum install httpd -y
```

```
cd /var/www/html
```

```
echo "MyGoogle" > index.html
```

```
service httpd start
```

```
chkconfig httpd on
```

User data - optional

Upload a file with your user data or enter it in the field.

[Choose file](#)

```
#!/bin/bash
sudo su
yum update -y
yum install httpd -y
cd /var/www/html
echo "22bd1a053k" > index.html
service httpd start
chkconfig httpd on
```

☐ User data has already been base64 encoded

Summary

- Number of instances: 1
- Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...
- Virtual server type (instance type): t2.micro
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier.

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

create an EC2 instance for DB server and write the code under Additional Details (same as previous).

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

EC2 > Instances > Launch an instance

Allow tags in metadata [Info](#)

Select

User data - optional [Info](#)

Upload a file with your user data or enter it in the field.

[Choose file](#)

```
#!/bin/bash
sudo su
yum update -y
yum install httpd -y
cd /var/www/html
echo "MyGoogle" > index.html
service httpd start
chkconfig httpd on
```

☐ User data has already been base64 encoded

Summary

Number of instances [Info](#)

1

Software image (AMI)

Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-08b95b3a93e0654d19

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

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

EC2 > Instances > i-0075799f475234453

Instance summary for i-0075799f475234453 (DB_Inst) [Info](#)

Updated less than a minute ago

Instance ID	i-0075799f475234453	Public IPv4 address	-	Private IPv4 addresses	10.0.2.169
IPv6 address	-	Instance state	Running	Public IPv4 DNS	-
Hostname type	IP name: ip-10-0-2-169.ec2.internal	Private IP DNS name (IPv4 only)	ip-10-0-2-169.ec2.internal	Elastic IP addresses	-
Answer private resource DNS name	-	Instance type	t2.micro	AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address	-	VPC ID	vpc-0b727b650efe059c4 (VPC_Exp)	Auto Scaling Group name	-
IAM Role	-	Subnet ID	subnet-0334824a6ffb10c28 (my_private_subnet)	Managed	false
IMDSv2	Required	Instance ARN	arn:aws:ec2:us-east-1:743185590498:instance/i-0075799f475234453		
Operator	-				

Now for private db instance give name bootstrap-private-db, choose amazon linux AMI, choose t2.micro instance type, Use ppk keypair, in network setting, add vpc, choose db-subnet and name sg's

EC2 > Instances > Launch an instance

Network settings

VPC - required [Info](#)
vpc-0212ee3c9390511e1 (VPC-exp)
10.0.0.0/16

Subnet [Info](#)
subnet-048b1f32093761192 db-subnet
VPC: vpc-0212ee3c9390511e1 Owner: 576362453021 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.2.0/24 [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

Security group name - required
launch-wizard-2
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-./!@#%&'()*~+-=|:;:[]{}^`<.,>?"'
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-./!@#%&'()*~+-=|:;:[]{}^`<.,>?"'
Description - required [Info](#)
launch-wizard-2 created 2025-03-27T06:15:42.281Z

Summary

Number of instances [Info](#)
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-071226ecf16aa7d96

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier [Read more about the free tier](#)

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

In the inbound security group rules, remove ssh and add MYSQL/Aurora, this will enable the range of communication in between the public and private subnet

EC2 > Instances > Launch an instance

☒ Create security group ☐ Select existing security group

Security group name - required
private-sg
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-./!@#%&'()*~+-=|:;:[]{}^`<.,>?"'
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-./!@#%&'()*~+-=|:;:[]{}^`<.,>?"'
Description - required [Info](#)
launch-wizard-2 created 2025-03-27T06:15:42.281Z

Inbound Security Group Rules
▼ Security group rule 1 (TCP; 3306, 10.0.2.0/24) [Remove](#)

Type	Protocol	Port range	Source type	Source	Description - optional
MYSQL/Aurora	TCP	3306	Custom	10.0.2.0/24	e.g. SSH for admin desktop

[Add security group rule](#)

Advanced network configuration

Summary

Number of instances [Info](#)
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-071226ecf16aa7d96

Virtual server type (instance type)
t2.micro

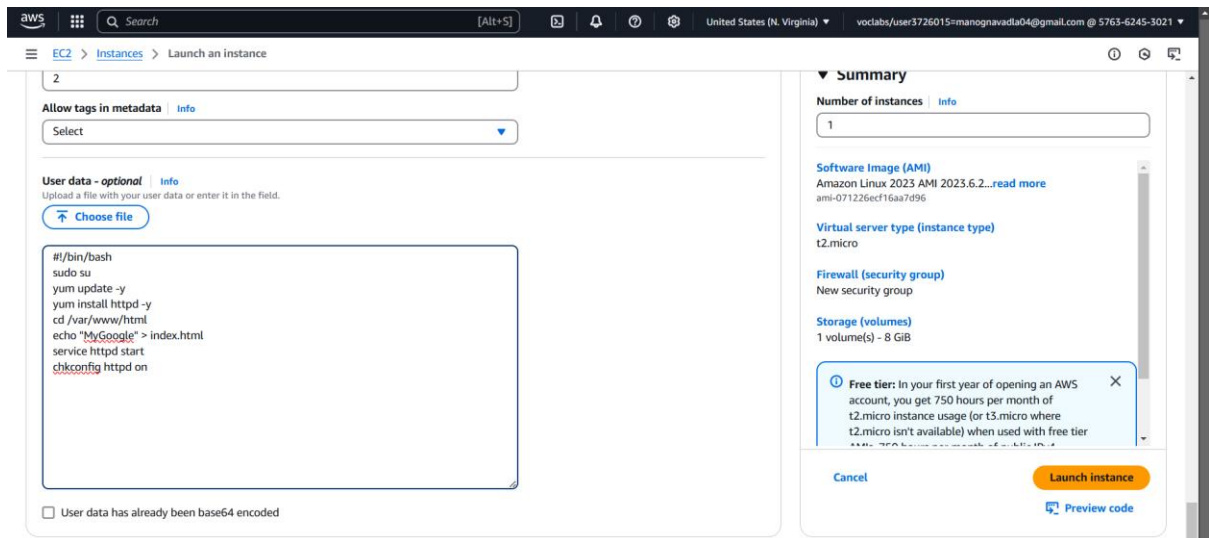
Firewall (security group)
New security group

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

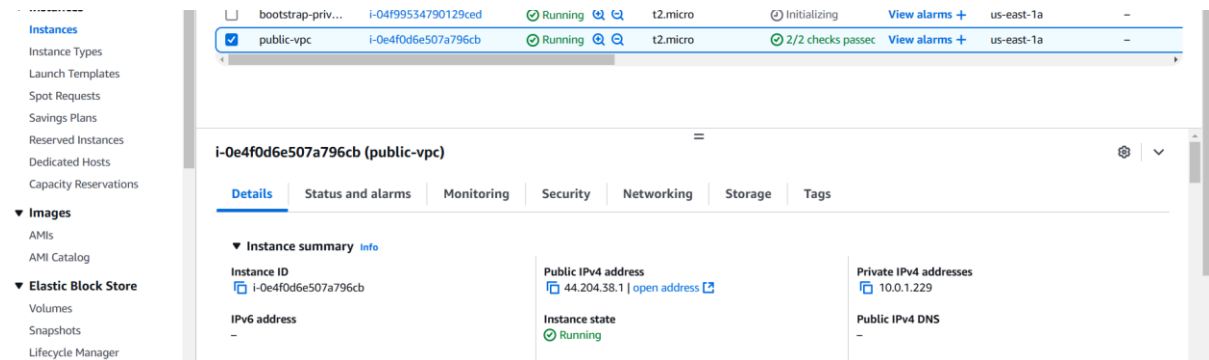
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier [Read more about the free tier](#)

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

In Advanced setting, scroll to the end and in user-data and add bootstrap script



Now go to the public instance web-server2, now we can see the public IPv4 address and copy it



Go to : 44.204.38.1 search in browser, we can see the output, so it can be exposed



<input checked="" type="checkbox"/>	bootstrap-private-db	i-04f99534790129ced	Running	View logs	t2.micro	Initializing	View alarms +	us-east-1a	-
<input type="checkbox"/>	public-vpc	i-0e4f0d6e507a796cb	Running	View logs	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-

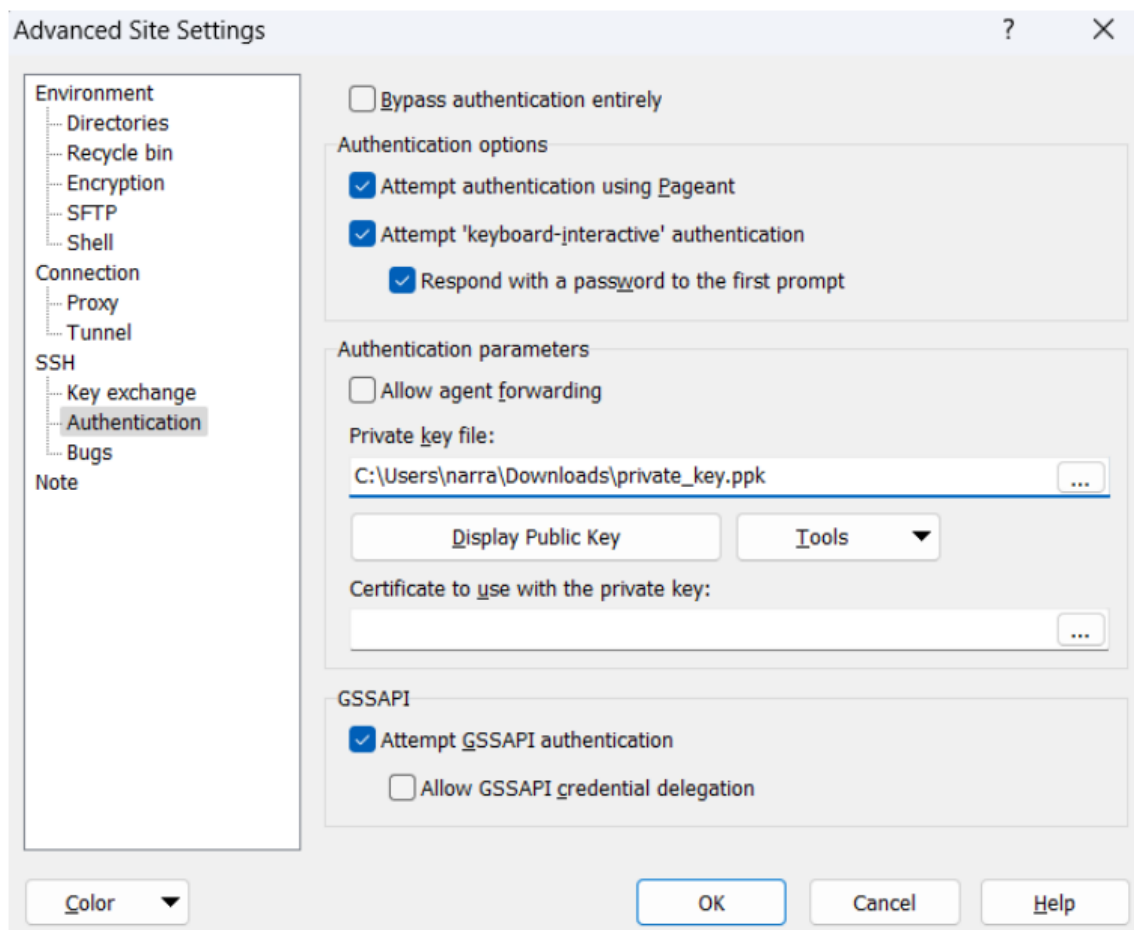
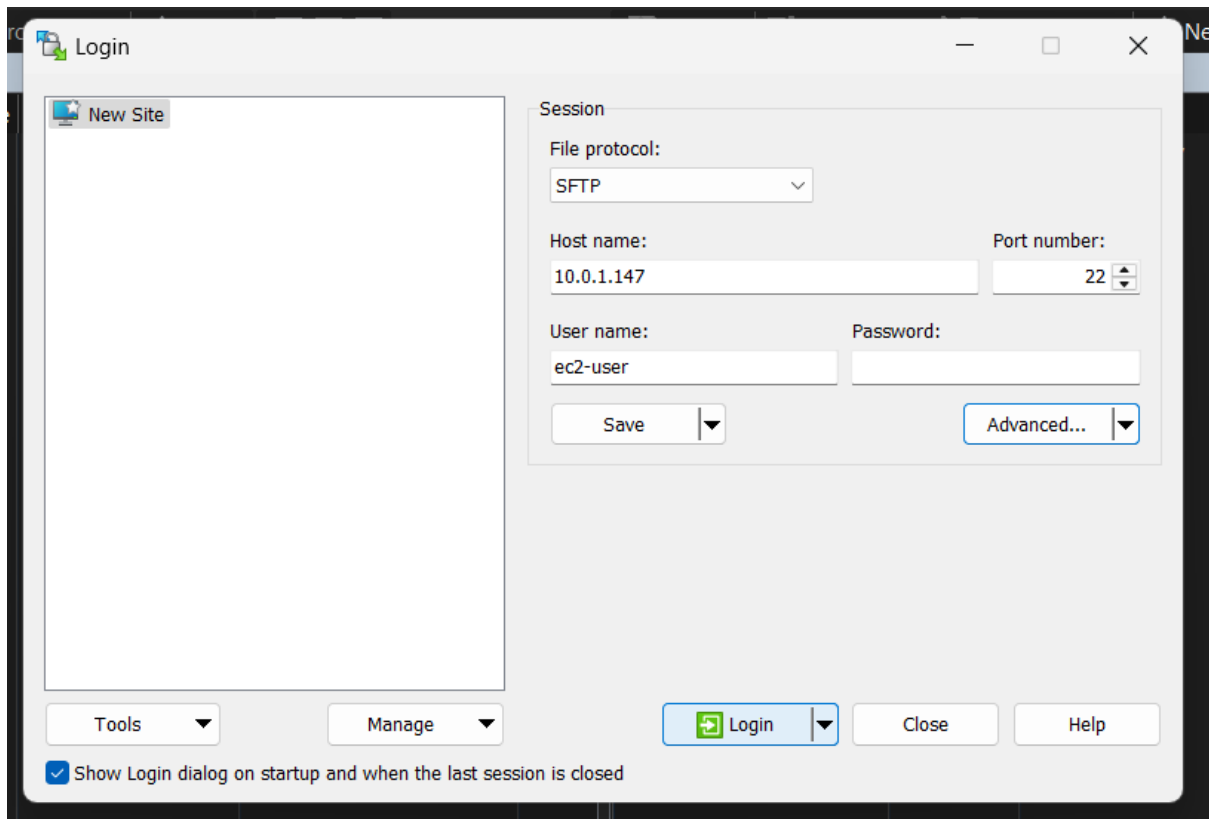
```
C:\Windows\System32>cd C:\Users\Sirim\Downloads

C:\Users\Sirim\Downloads>ssh -i "vpcc.pem" ec2-user@3.83.154.0
The authenticity of host '3.83.154.0 (3.83.154.0)' can't be established.
ED25519 key fingerprint is SHA256:BL4IZgIBfQM0mz+4s/bkWi1580cdlaM2UieJUHUCFqU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.83.154.0' (ED25519) to the list of known hosts.

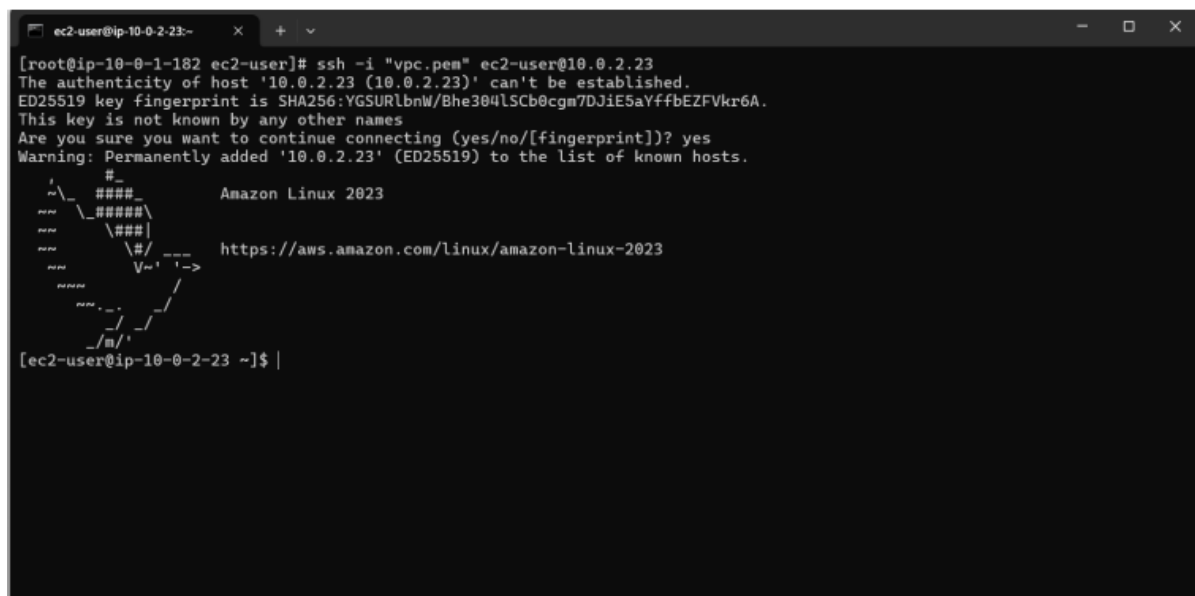
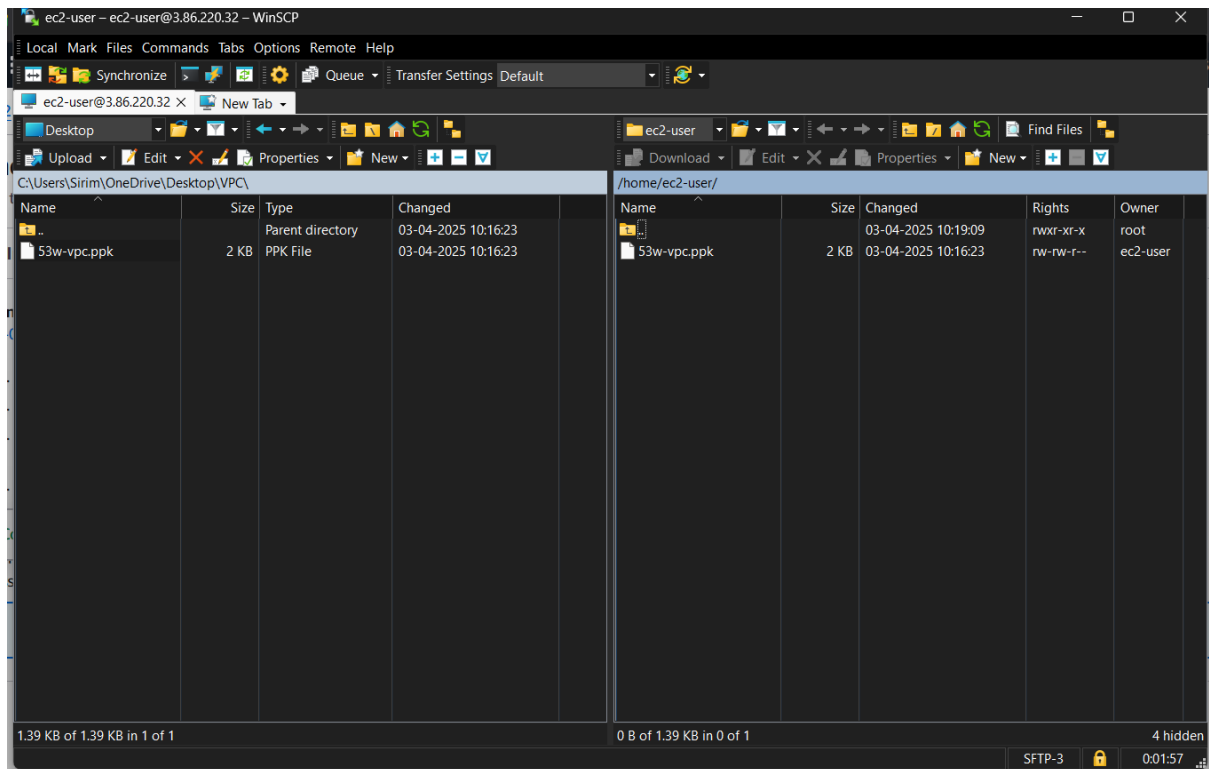
      #
    ~\_ ##### Amazon Linux 2023
  nnn \_#####\
nnnn \_###|
      \#/____'~>
      V~'
nnnn
      ~~~
      ~~~_~'
      _/  /
      _/  /
      _/m/'

[ec2-user@ip-10-0-1-156 ~]$ ssh -i "vpcc.pem" ec2-user@10.0.2.48
Warning: Identity file vpcc.pem not accessible: No such file or directory.
```

Copy the host name of public ec2 instance



Copy the ppk file to the ec2 instance



On yum update as there is no internet connection the update has failed

```
root@ip-10-0-2-23:/home/ec2-user$ sudo su
[root@ip-10-0-2-23 ec2-user]# yum update
*Amazon Linux 2023 repository
Amazon Linux 2023 repository
Errors during downloading metadata for repository 'amazonlinux':
- Curl error (28): Timeout was reached for https://al2023-repos-us-east-1-de612dc2.s3.dualstack.us-east-1.amazonaws.com/core/mirrors/2023.6.20250303/x86_64/mirror.list [Connection timeout after 30001 ms]
- Curl error (28): Timeout was reached for https://al2023-repos-us-east-1-de612dc2.s3.dualstack.us-east-1.amazonaws.com/core/mirrors/2023.6.20250303/x86_64/mirror.list [Connection timeout after 30000 ms]
Error: Failed to download metadata for repo 'amazonlinux': Cannot prepare internal mirrorlist: Interrupted by signal
Amazon Linux 2023 Kernel Livepatch repository
Error: Failed to download metadata for repo 'kernel-livepatch': Cannot prepare internal mirrorlist: Interrupted by signal
Ignoring repositories: amazonlinux, kernel-livepatch
Error encountered while trying to retrieve release update information: Unable to retrieve release info data. Interrupted by signal
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-10-0-2-23 ec2-user]#
```

To get internet connection we have to setup a NAT gateway in the public subnet

aws [Alt+S] United States (N. Virginia) voclato/user5729727=narapureth44@gmail.com @ 4375-7544-1207

VPC > NAT gateways > Create NAT gateway

Elastic IP address 34.194.101.173 (eipalloc-01c4647f575e64277) allocated.

Create NAT gateway [info](#)

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.
S3E-NAT
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-0f80d0b6afce9b48f (S3E-web-subnet)

Connectivity type
Select a connectivity type for the NAT gateway.
☒ Public
☐ Private

Elastic IP allocation ID [info](#)
Assign an Elastic IP address to the NAT gateway.
eipalloc-01c4647f575e64277 [Allocate Elastic IP](#)

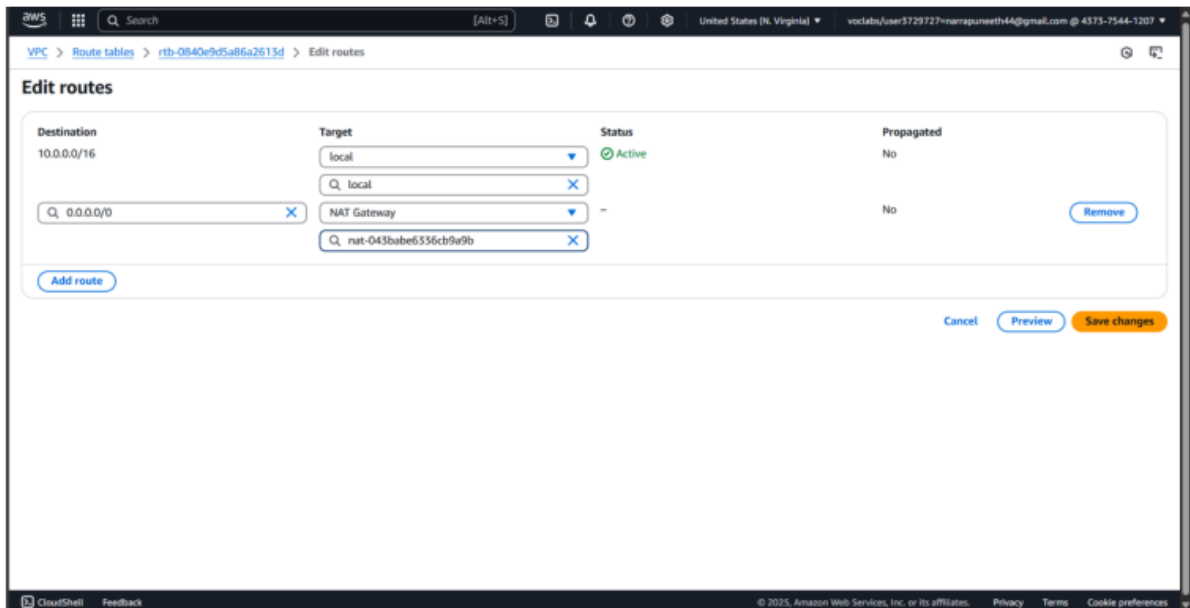
[Additional settings](#) [info](#)

Tags

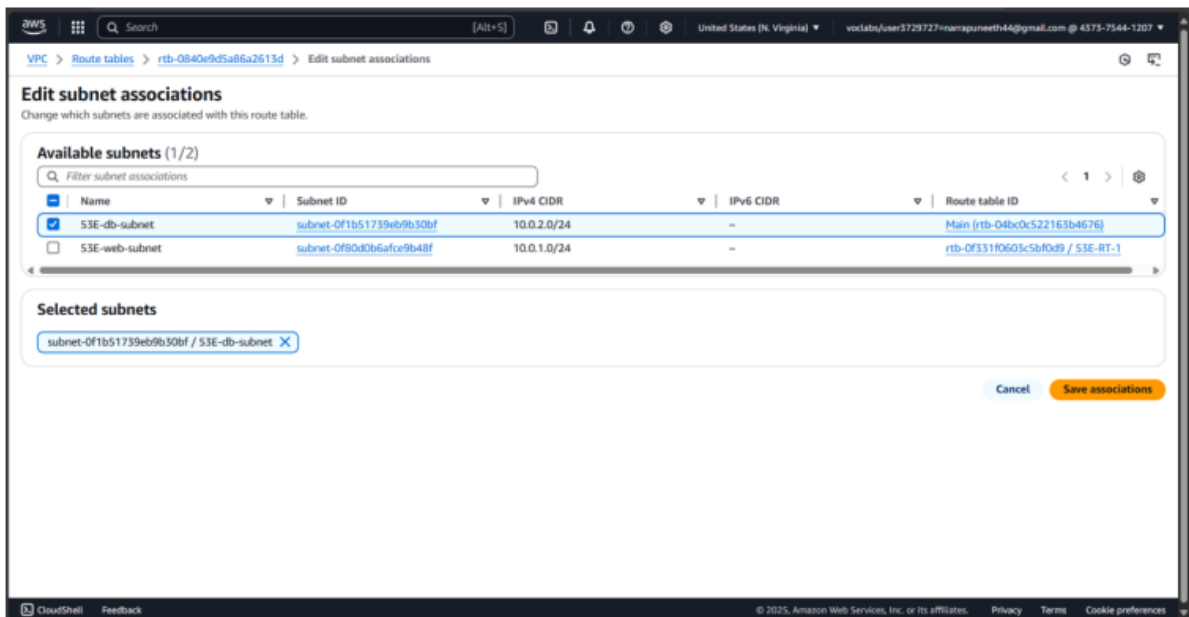
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
-----	------------------

Create a route table and edit the routes to add destination as 0.0.0.0 and the target as the NAT gateway



Add the subnet association to the route table and select the private subnet



After the NAT gateway and the route table are created the private database can access the internet and the update is successful.

```
[root@ip-10-0-2-14 ec2-user]# yum update
Amazon Linux 2023 repository      54 MB/s | 35 MB      00:00
Amazon Linux 2023 Kernel Livepatch repository 156 kB/s | 15 kB      00:00
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-10-0-2-14 ec2-user]# ping www.google.com
PING www.google.com (64.233.180.99) 56(84) bytes of data.
64 bytes from pe-in-f99.1e100.net (64.233.180.99): icmp_seq=1 ttl=57 time=2.64 m
s
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=2 ttl=57 time=2.26 m
s
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=3 ttl=57 time=2.41 m
s
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=4 ttl=57 time=2.00 m
s
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=5 ttl=57 time=2.11 m
s
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=6 ttl=57 time=2.09 m
s
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=7 ttl=57 time=2.19 m
s
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=8 ttl=57 time=2.15 m
s
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=9 ttl=57 time=1.93 m
s
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=10 ttl=57 time=2.33
ms
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=11 ttl=57 time=2.08 ms
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=12 ttl=57 time=2.68 ms
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=13 ttl=57 time=2.10 ms
64 bytes from on-in-f99.1e100.net (64.233.180.99): icmp_seq=14 ttl=57 time=1.95 ms
```