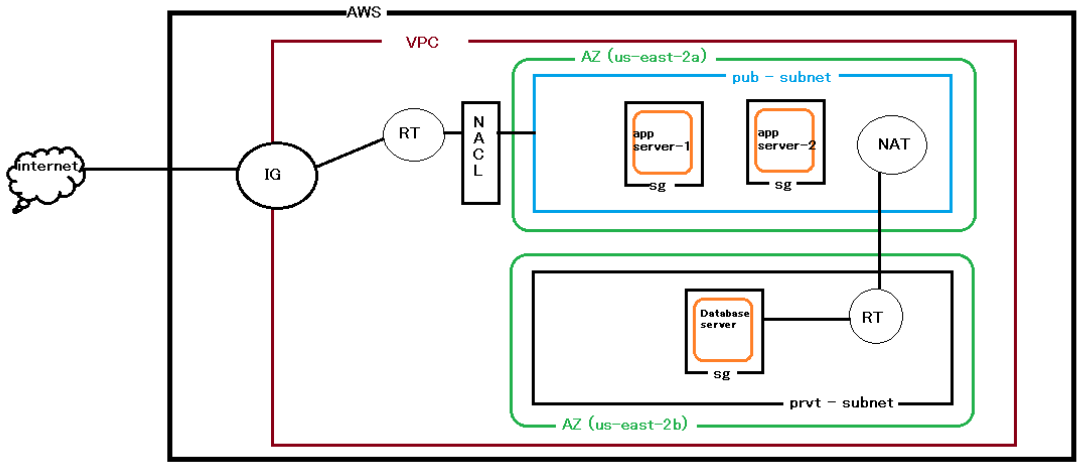
Custom VPC with EC2 to S3, EFS and EC2 to RDS



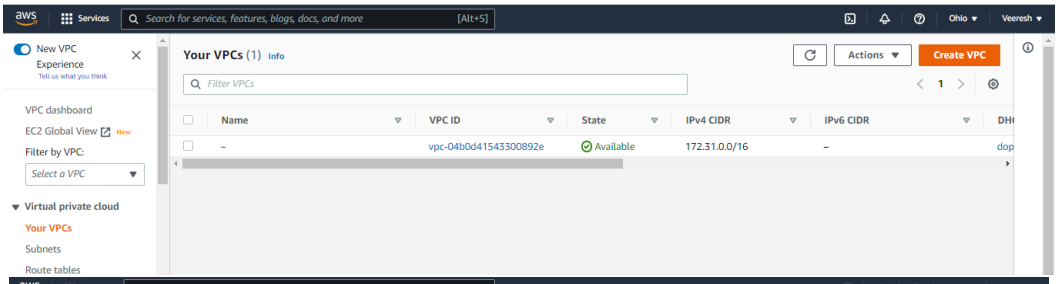
VPC - Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

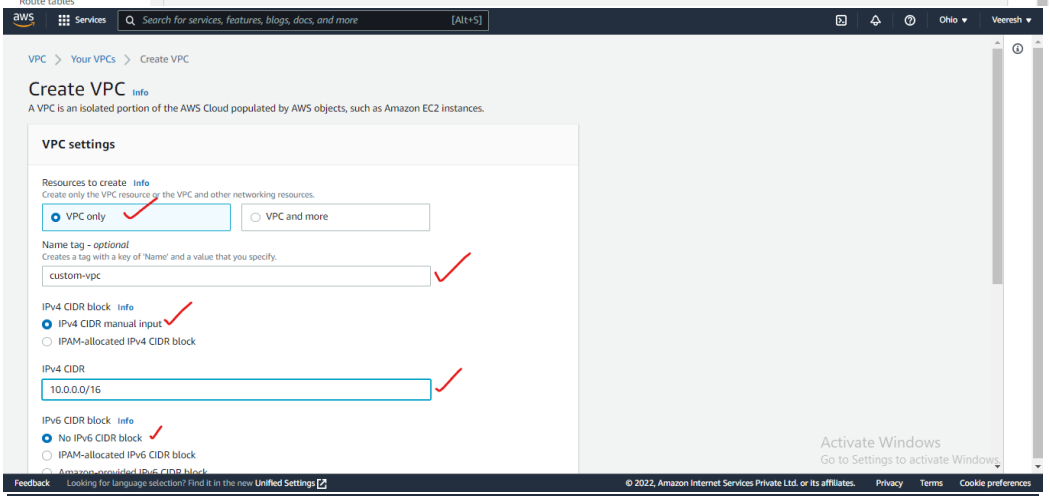
Virtual Private Cloud (VPC) lets you have a virtual network, so that you can select your own IP address range, create your own subnets and configure your route tables and network gateways. Here is a quick guide on how to setup VPC on Amazon Web Services (AWS).

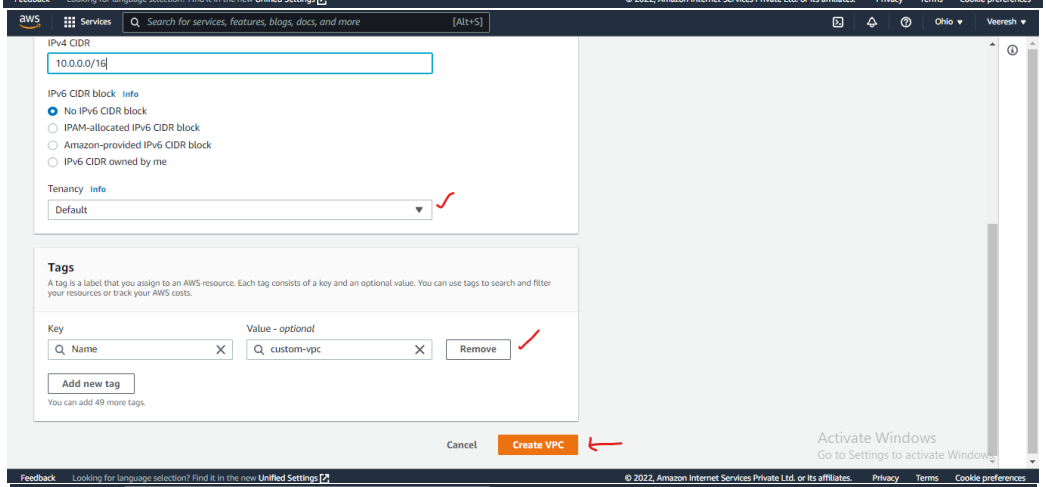
PART – 1 : VPC and subnets creation

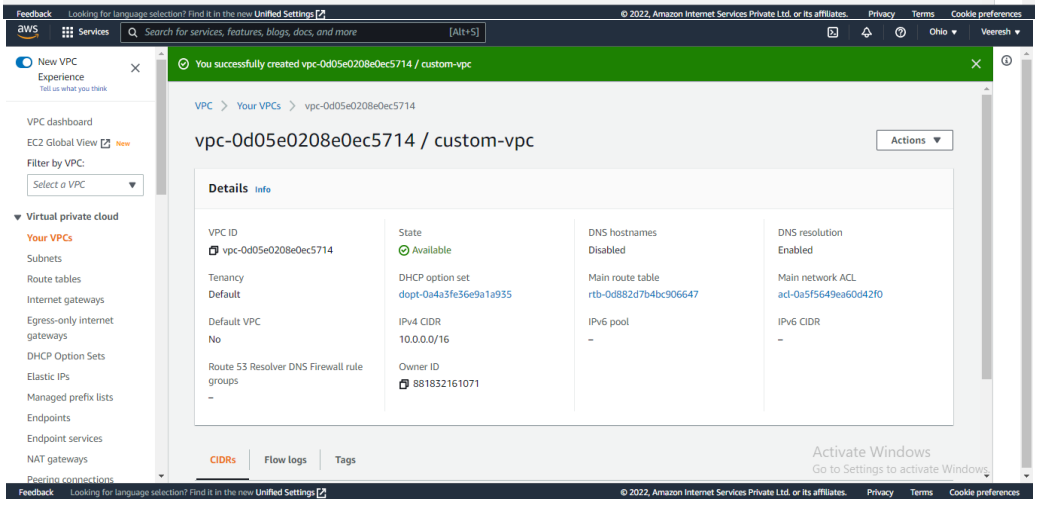
Step 1 : Creating VPC

- Goto aws console vpc dashboard and select Create VPC.
- VPC settings --> Resource to create – VPC only, Name tag – add a name to Custom VPC, IPV4 CIDR – 10.0.0.0/16 (to the 16 mask bit value there will be 65536 IP's are generating into this VPC), Tenancy – Default.
- And create VPC


Your VPCs (1) Info
Actions
Create VPC
Filter VPCs
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
vpc-04b0d41543300892e
Available
172.31.0.0/16
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables

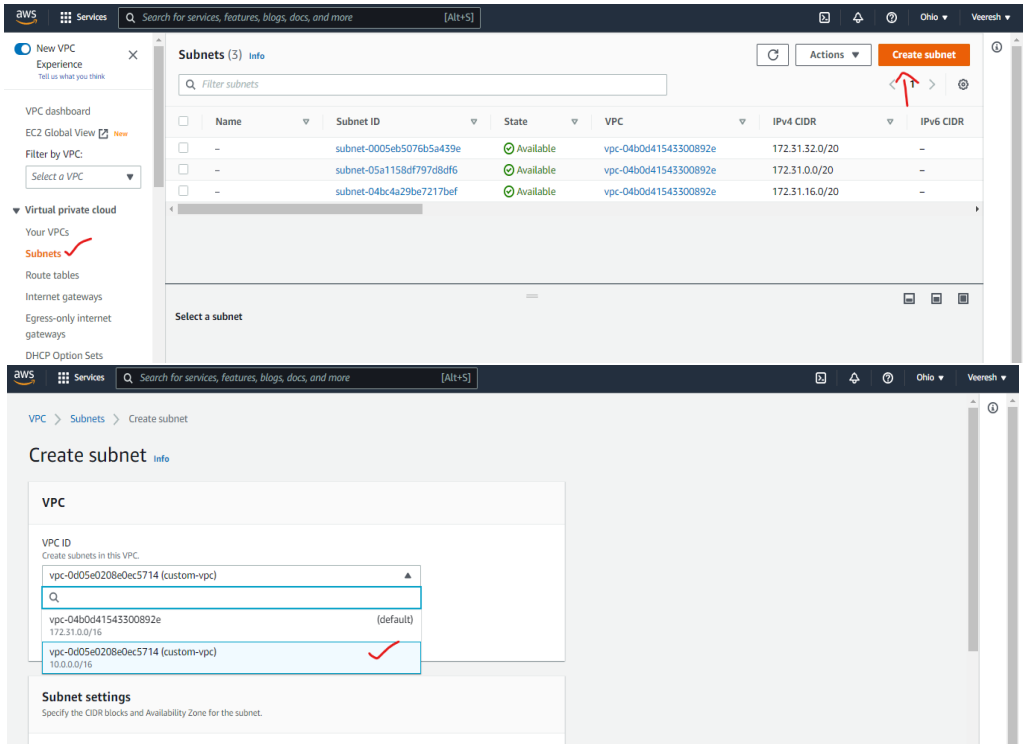

VPC > Your VPCs > Create VPC
Create VPC Info
A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.
VPC settings
Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only
VPC and more
Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
custom-vpc
IPv4 CIDR block Info
IPv4 CIDR manual input
IPAM-allocated IPv4 CIDR block
IPv4 CIDR
10.0.0.0/16
IPv6 CIDR block Info
No IPv6 CIDR block
IPAM-allocated IPv6 CIDR block
Activate Windows
Go to Settings to activate Windows.
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

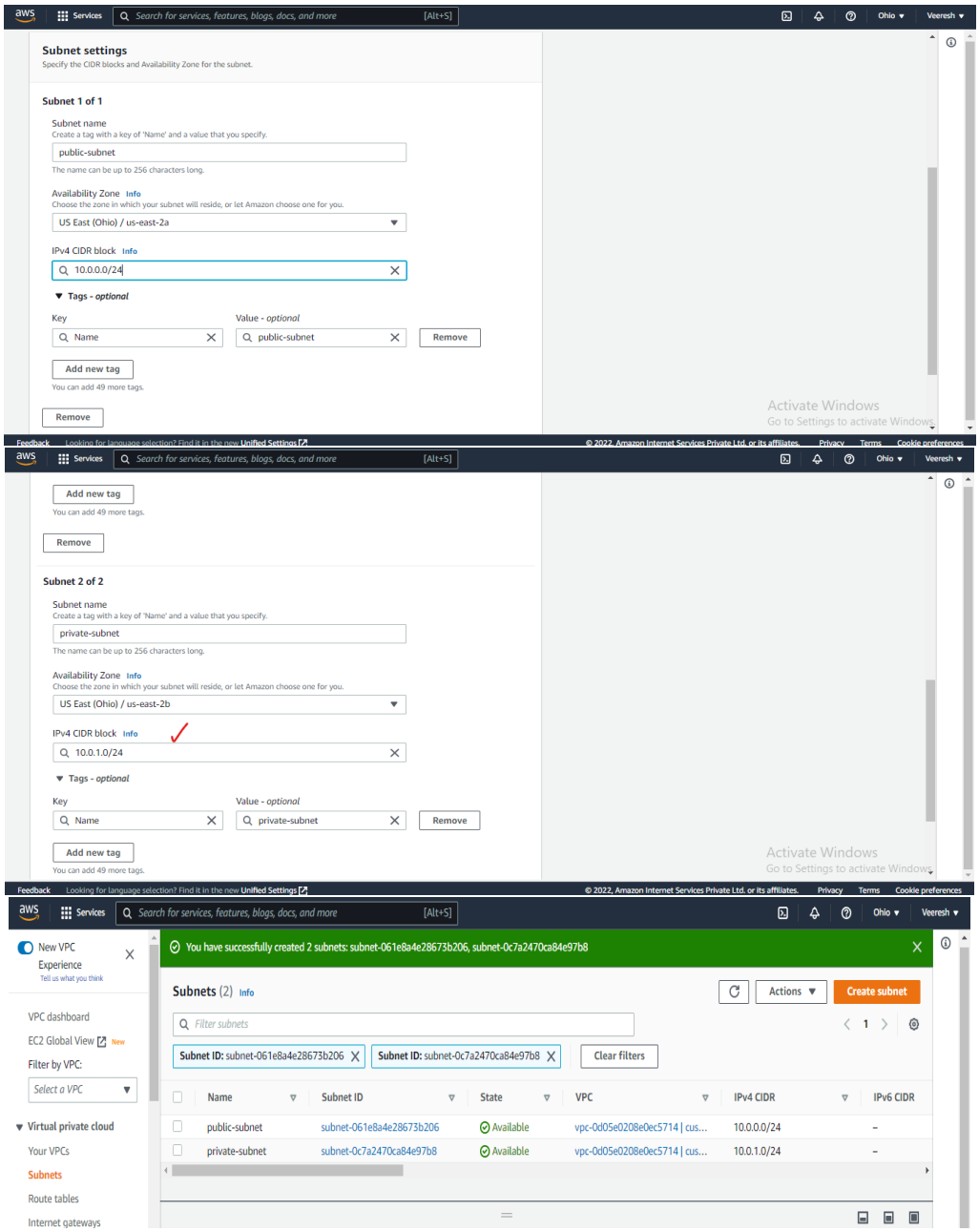

IPv4 CIDR
10.0.0.0/16
IPv6 CIDR block Info
No IPv6 CIDR block
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me
Tenancy Info
Default
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
custom-vpc
Remove
Add new tag
You can add 49 more tags.
Cancel
Create VPC
Activate Windows
Go to Settings to activate Windows.
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences


You successfully created vpc-0d05e0208e0ec5714 / custom-vpc
VPC > Your VPCs > vpc-0d05e0208e0ec5714
vpc-0d05e0208e0ec5714 / custom-vpc
Actions
Details Info
VPC ID
vpc-0d05e0208e0ec5714
State
Available
DNS hostnames
Disabled
DNS resolution
Enabled
Tenancy
Default
DHCP option set
dopt-0a4a3fe36e9a1a935
Main route table
rtb-0d882d7b4bc906647
Main network ACL
acl-0a5f5649ea60d42f0
Default VPC
No
IPv4 CIDR
10.0.0.0/16
IPv6 pool
IPv6 CIDR
Route 53 Resolver DNS Firewall rule groups
Owner ID
881832161071
CIDRs
Flow logs
Tags
Activate Windows
Go to Settings to activate Windows.
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

Step 2 : Creating private and public Subnets and attach to custom VPC.

- In the VPC dashboard click subnet - > create subnet.
- VPC ID – select the custom vpc wich are previously created.
- Subnet settings --> subnet name – public subnet, Availability Zone – select one Az, ipv4 cidr block – 10.0.0.0/24 (to the 24 mask bit value there will be 256 IP's are generating into this subnet)
- Add new subnet --> subnet name – private subnet, Availability Zone – select different Az compare to public subnet, ipv4 cidr block – 10.0.1.0/24 (to the 24 mask bit value there will be 256 IP's are generating into this subnet , make sure the IP's are not overlap with other subnet)
- And create the subnets.





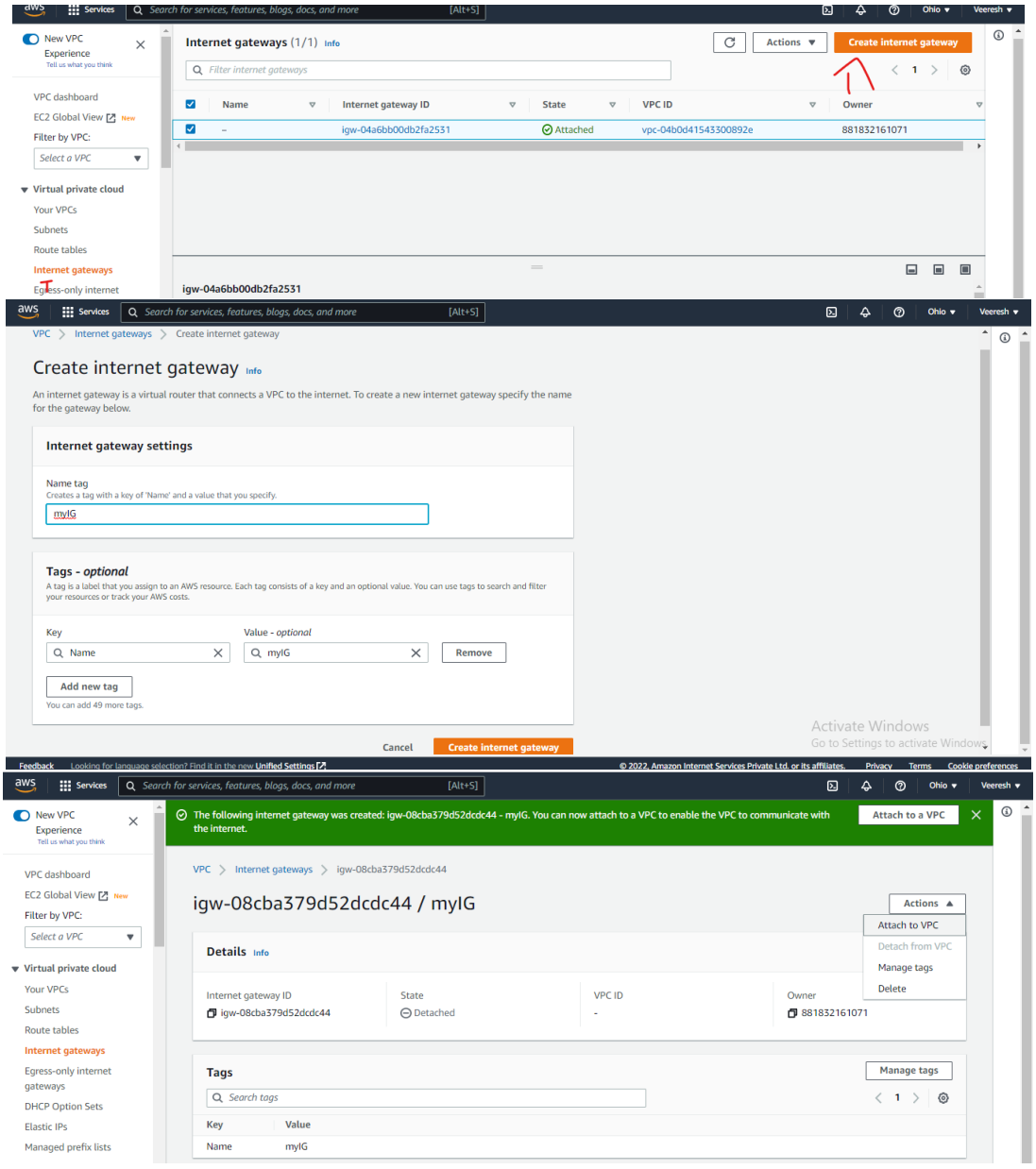
Step 3 : Access the internet from the outside world to the VPC, Internet gateway are used and Public subnets are associated with a route table that directs subnet traffic to the internet using an Internet Gateway.

Internet gateway,

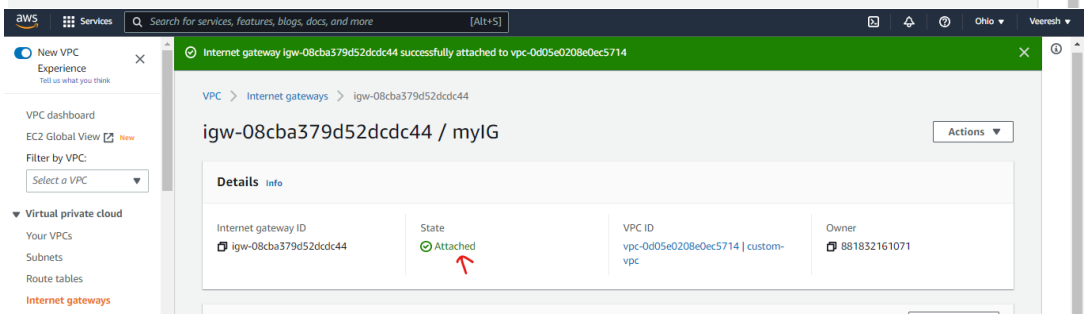
- From the VPC dashboard select Internet gateway and click create internet gateway.
- Give the name of IG for identification and create internet gateway.
- Attach this Internet gateway to the custom VPC.

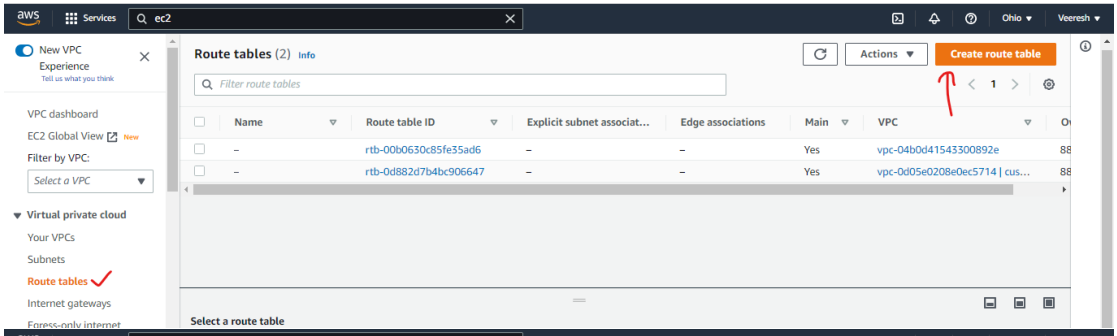
Route tables,

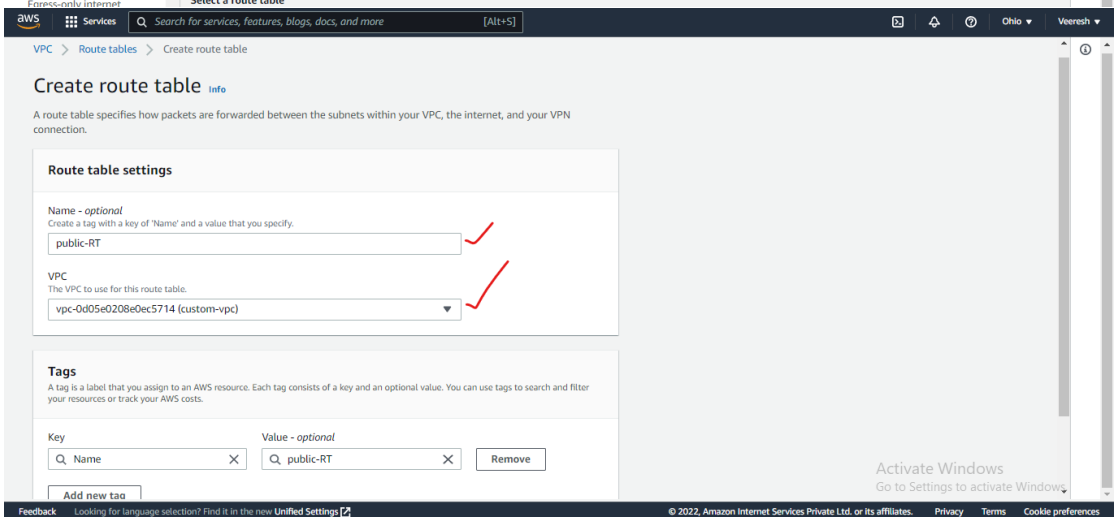
- From the VPC dashboard select Route tables and click create Route tables.
- Name – public RT, VPC – select the custom VPC and create it.
- Associate this Route tables with the public subnet from the subnet association --> edit subnet associations --> select public subnet and save associates.
- Now goto the Routes --> Edit routes --> destination – 0.0.0.0/0 and Target – internet gateway select it which are previously created and save changes.

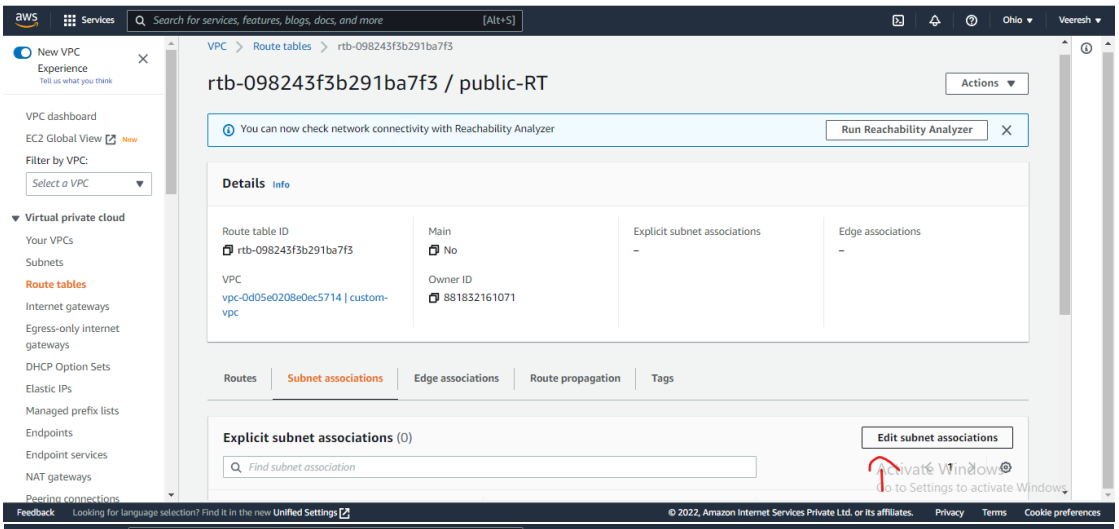


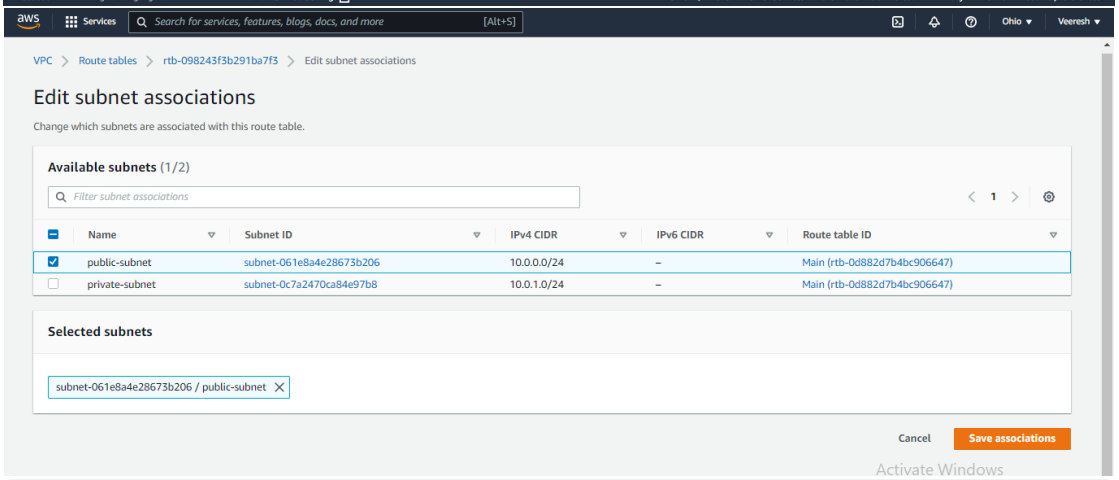

Services
Search for services, features, blogs, docs, and more [Alt+S]
Ohio
Veeresh
VPC > Internet gateways > Attach to VPC (igw-08cba379d52dcdc44)
Attach to VPC (igw-08cba379d52dcdc44) Info
VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.
Available VPCs
Attach the internet gateway to this VPC.
Select a VPC
vpc-0d05e0208e0ec5714 - custom-vpc
AWS Command Line Interface command
Cancel
Attach internet gateway

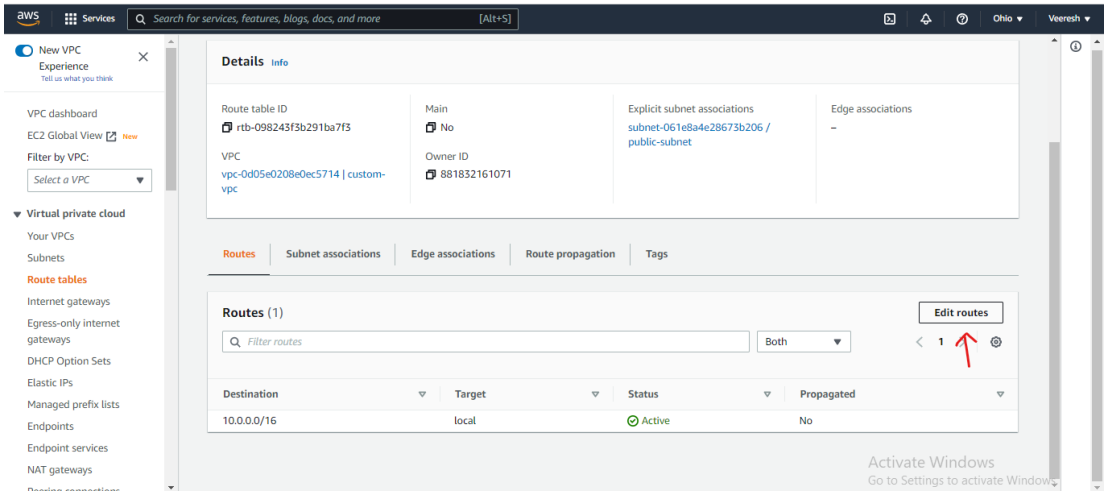

Services
Search for services, features, blogs, docs, and more [Alt+S]
Ohio
Veeresh
New VPC Experience
Tell us what you think
Internet gateway igw-08cba379d52dcdc44 successfully attached to vpc-0d05e0208e0ec5714
VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
VPC > Internet gateways > igw-08cba379d52dcdc44
igw-08cba379d52dcdc44 / myIG
Actions
Details Info
Internet gateway ID
igw-08cba379d52dcdc44
State
Attached
VPC ID
vpc-0d05e0208e0ec5714 | custom-vpc
Owner
881832161071

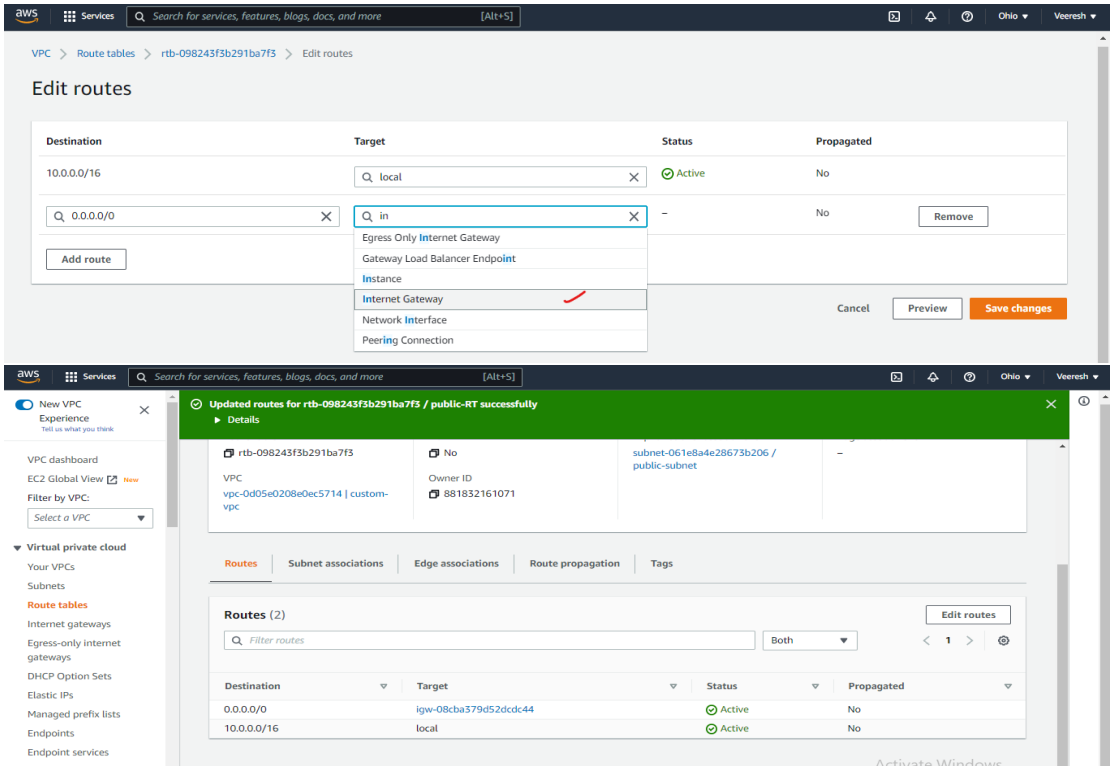

Services
ec2
Ohio
Veeresh
New VPC Experience
Tell us what you think
Route tables (2) Info
Actions
Create route table
Filter route tables
Name
Route table ID
Explicit subnet associat...
Edge associations
Main
VPC
rtb-00b0630c85fe35ad6
Yes
vpc-04b0d41543300892e
rtb-0d882d7b4bc906647
Yes
vpc-0d05e0208e0ec5714 | cus...
VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet
Select a route table


Services
Search for services, features, blogs, docs, and more [Alt+S]
Ohio
Veeresh
VPC > Route tables > Create route table
Create route table Info
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
public-RT
VPC
The VPC to use for this route table.
vpc-0d05e0208e0ec5714 (custom-vpc)
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
Name
public-RT
Remove
Add new tag
Activate Windows
Go to Settings to activate Windows.
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Ohio
Veeresh
New VPC Experience
Tell us what you think
VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP Option Sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
VPC > Route tables > rtb-098243f3b291ba7f3
rtb-098243f3b291ba7f3 / public-RT
Actions
You can now check network connectivity with Reachability Analyzer
Run Reachability Analyzer
Details Info
Route table ID
rtb-098243f3b291ba7f3
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0d05e0208e0ec5714 | custom-vpc
Owner ID
881832161071
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (0)
Edit subnet associations
Find subnet association
Activate Windows
Go to Settings to activate Windows.
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

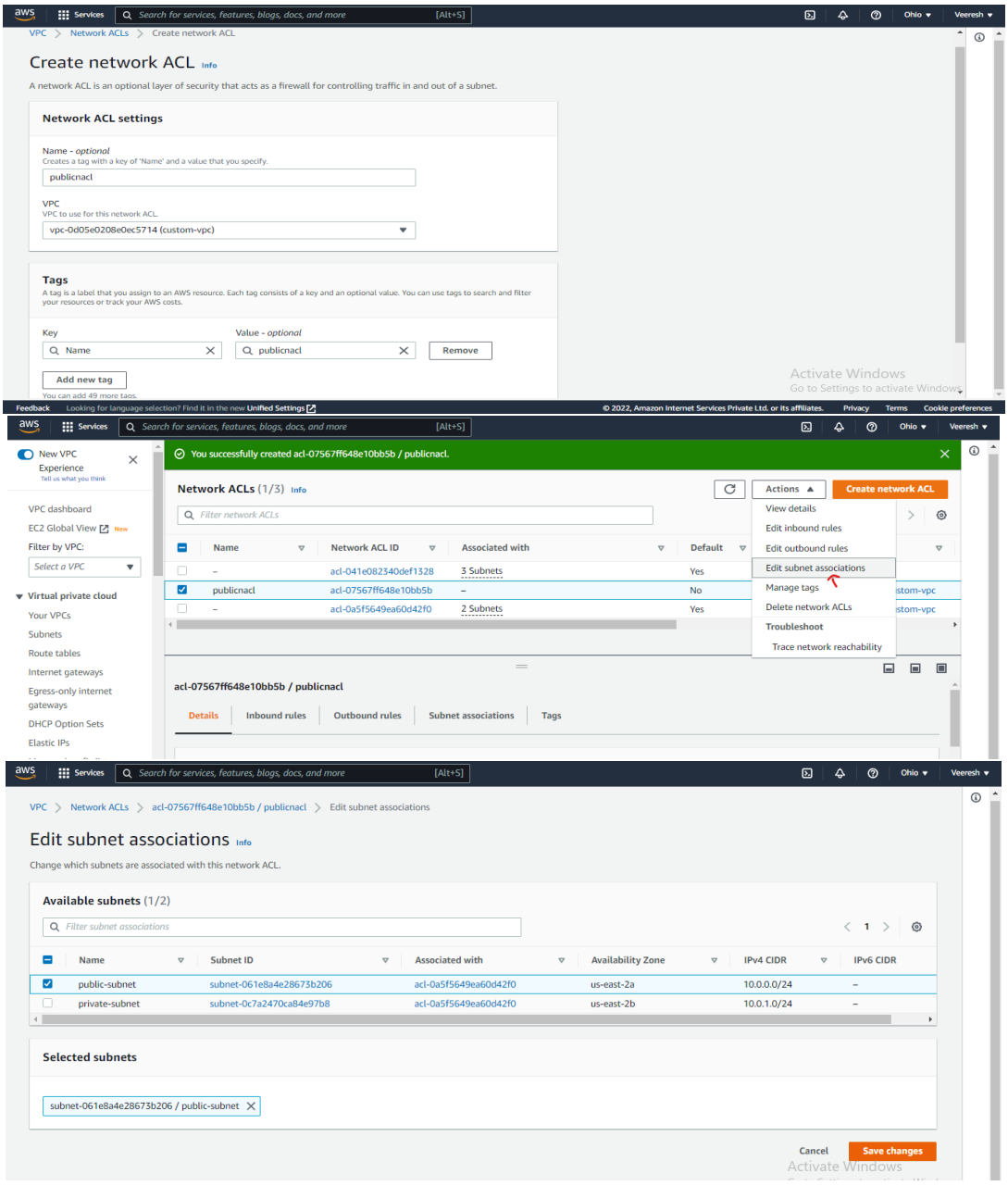

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Ohio
Veeresh
VPC > Route tables > rtb-098243f3b291ba7f3 > Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (1/2)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
public-subnet
subnet-061e8a4e28673b206
10.0.0.0/24
–
Main (rtb-0d882d7b4bc906647)
private-subnet
subnet-0c7a2470ca84e97b8
10.0.1.0/24
–
Main (rtb-0d882d7b4bc906647)
Selected subnets
subnet-061e8a4e28673b206 / public-subnet
Cancel
Save associations
Activate Windows

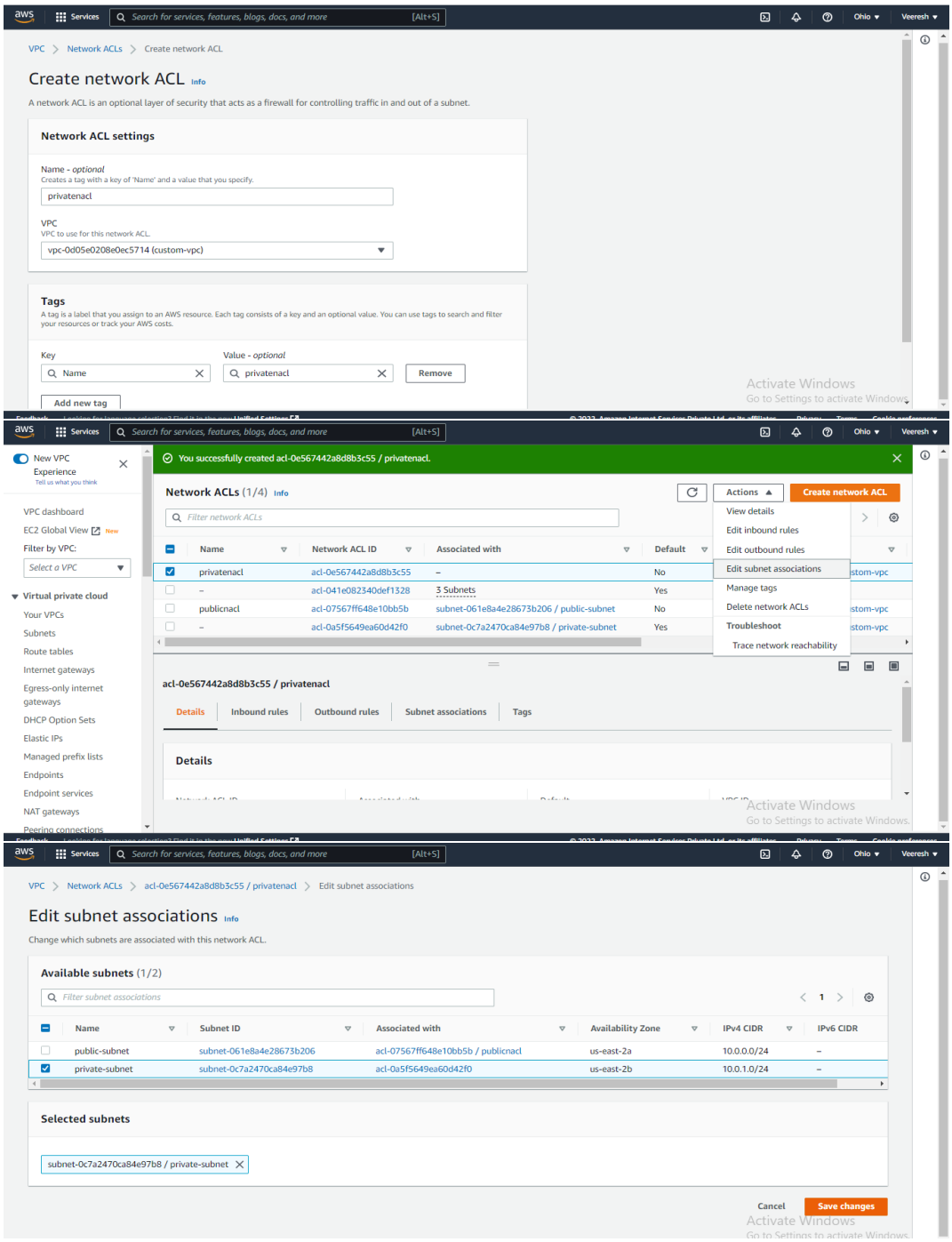

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Ohio
Veeresh
New VPC Experience
Tell us what you think
VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP Option Sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Details Info
Route table ID
rtb-098243f3b291ba7f3
Main
No
Explicit subnet associations
subnet-061e8a4e28673b206 / public-subnet
Edge associations
–
VPC
vpc-0d05e0208e0ec5714 | custom-vpc
Owner ID
881832161071
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (1)
Edit routes
Filter routes
Both
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No
Activate Windows
Go to Settings to activate Windows.



Step 4: Create the NACL an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

- From the VPC dashboard select network ACL and click create network ACL.
- Name – publicnacl, VPC – select the custom VPC. And create.
- Goto the NACL, select public nacl --> actions--> Edit subnet association --> select public subnet and save changes.
- Similarly create one more NACL for private subnet and give the subnet association as private subnet.
- As per present on going task, give the allow all traffic of inbound and outbound rules to the public NACL and Deny the all traffic of inbound and outbound rules to the private NACL.

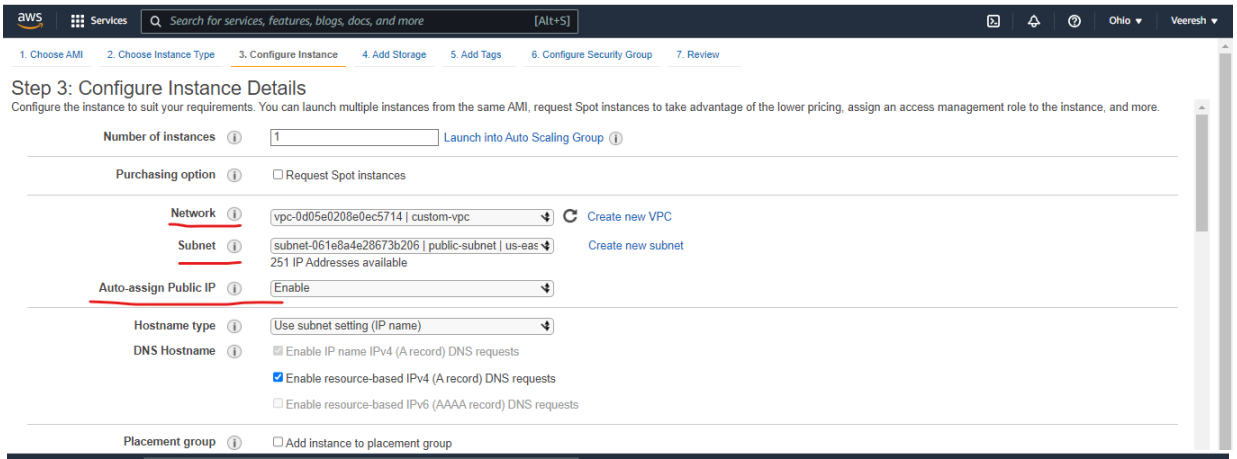

Create network ACL
A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.
Network ACL settings
Name - optional
publicnacl
VPC
vpc-0d05e0208e0ec5714 (custom-vpc)
Tags
Key
Name
Value - optional
publicnacl
Remove
Add new tag
You can add 49 more tags.
You successfully created acl-07567ff648e10bb5b / publicnacl.
Network ACLs (1/3)
Actions
Create network ACL
View details
Edit inbound rules
Edit outbound rules
Edit subnet associations
Manage tags
Delete network ACLs
Troubleshoot
Trace network reachability
acl-07567ff648e10bb5b / publicnacl
Details
Inbound rules
Outbound rules
Subnet associations
Tags
Edit subnet associations
Change which subnets are associated with this network ACL.
Available subnets (1/2)
public-subnet
subnet-061e8a4e28673b206
private-subnet
subnet-0c7a2470ca84e97b8
Selected subnets
subnet-061e8a4e28673b206 / public-subnet
Cancel
Save changes

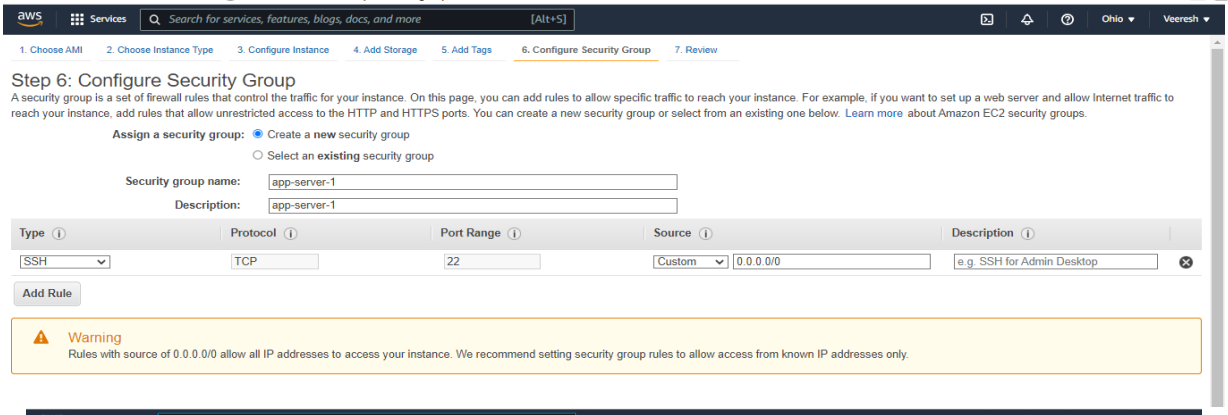


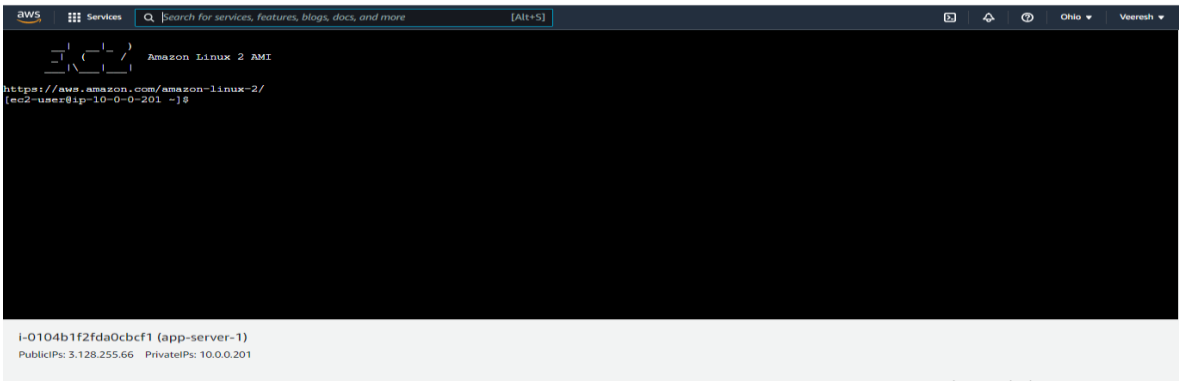
PART – 2 : Access S3 from EC2 Instance with in custom VPC

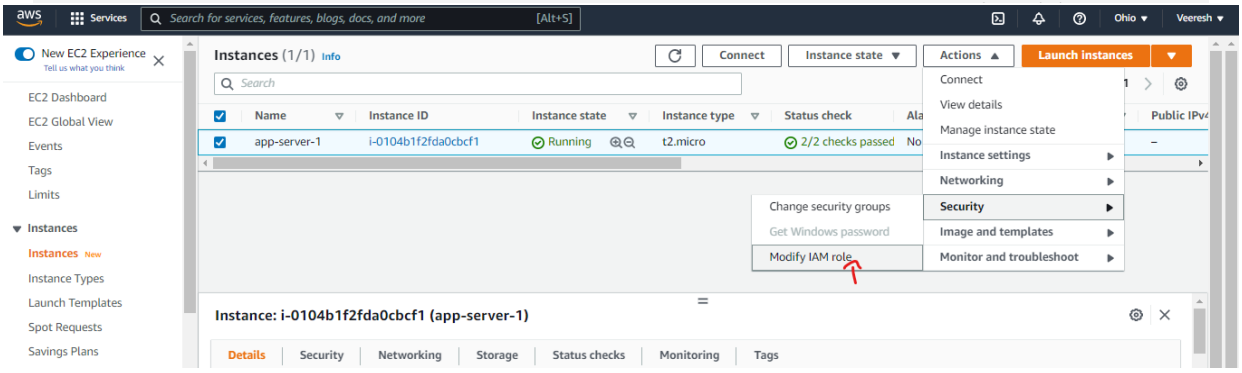
- Launch amazon linux EC2 instance as configure like, Network – select custom VPC, subnet – select public subnet , Auto-assign public IP – Enable it. And launch it.
- To get access S3 to the EC2 instance , Create a IAM role of S3 and attach it to the EC2 instance(app-server-1) as , select machine --> action --> security --> Modify IAM role --> select the role of S3 --> update IAM role.

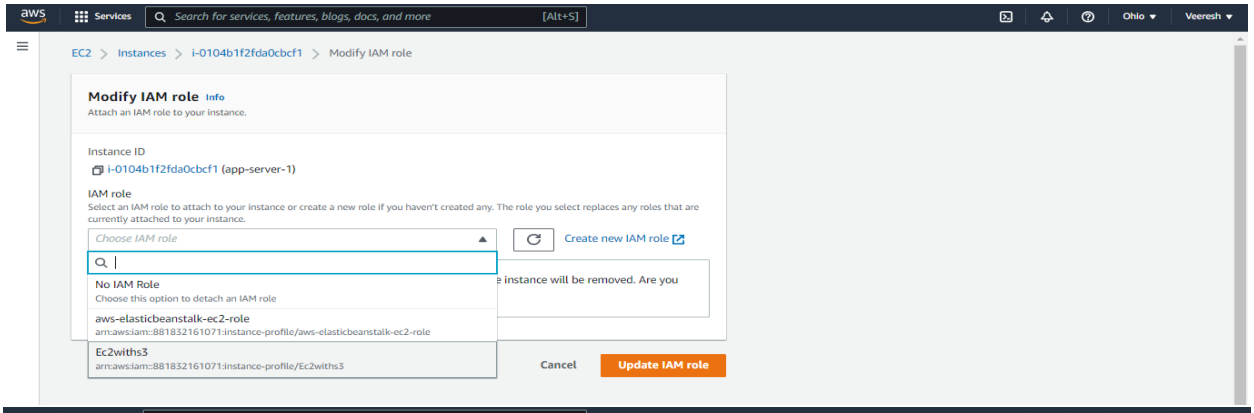
- Connect app-server-1, and switch to root user the give the command as “aws s3 ls” we can get the list buckets which are available in the Amazon S3.

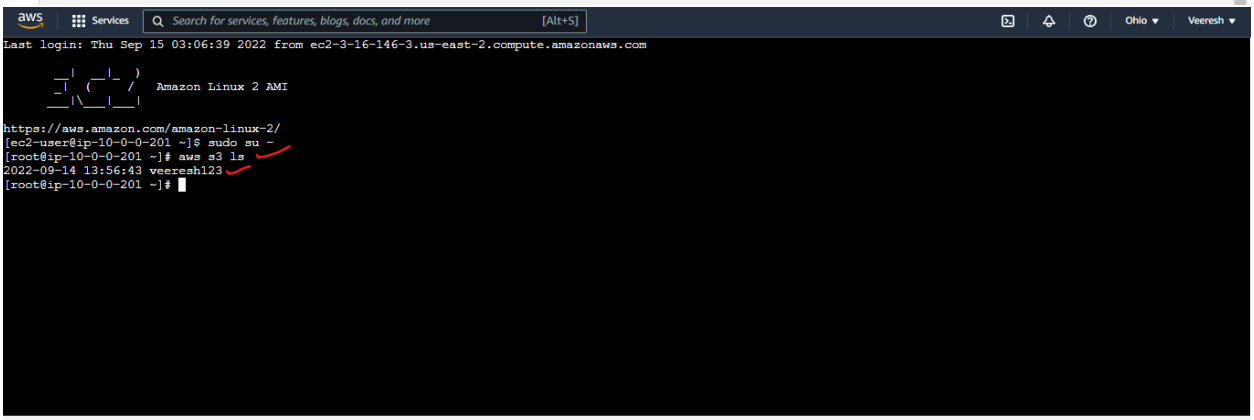




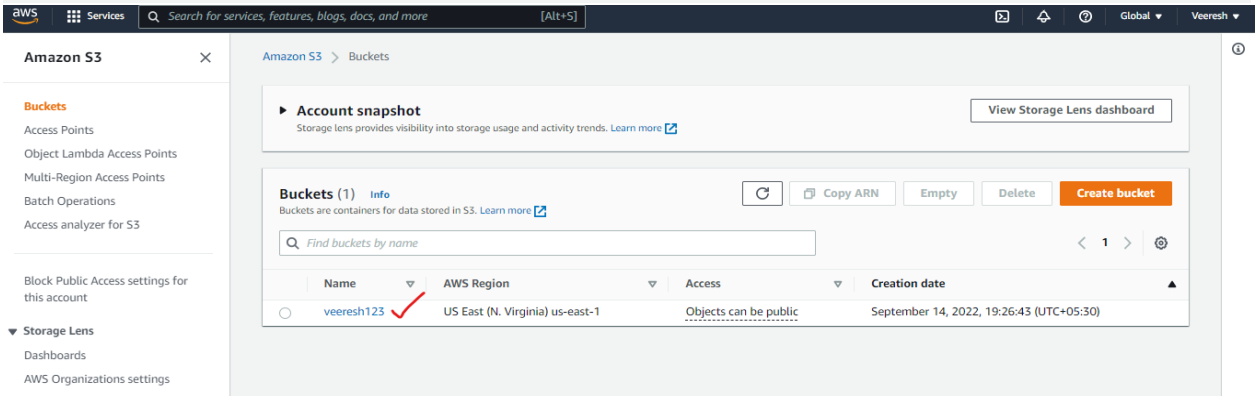








i-0104b1f2fda0cbcf1 (app-server-1)
PublicIPs: 3.128.255.66 PrivateIPs: 10.0.0.201



PART – 3 : Elasic File System with in custom VPC

Step 1:

- Goto to aws console launch one more amazon linux instance assign name as app-server-2 , app-server-1 are already created. 2 instances launch from us-east-2a public subnet from custom vpc.
- Connect the app-server-1 (instance) and run below commands and instructions,

sudo su - //switch root user

yum update –y //update packages

sudo yum install –y amazon-efs-utils //to install EFS utility

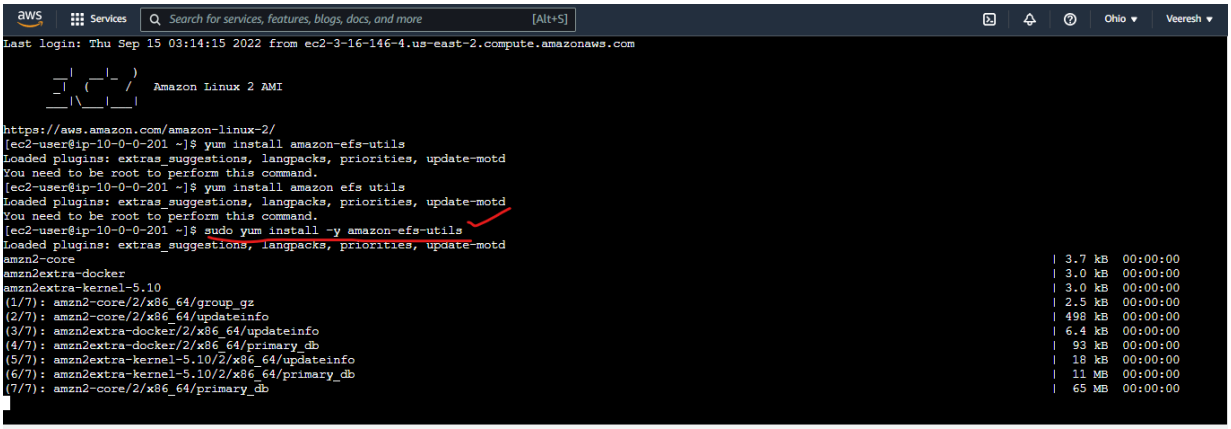
sudo service nfs status //to check the status of nfs at initial it will be inactive state we need to active it by below command

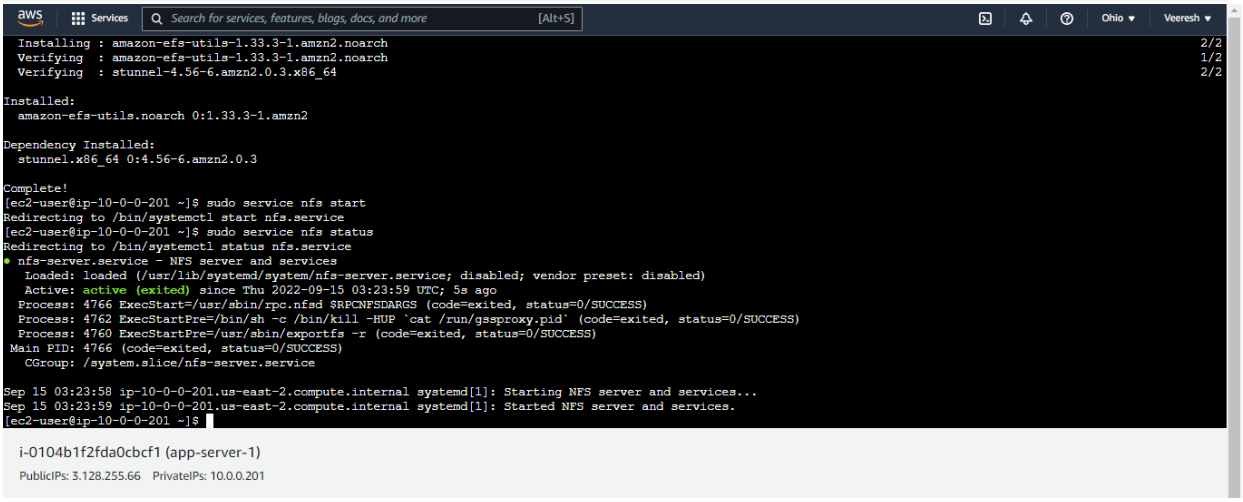
sudo service nfs start

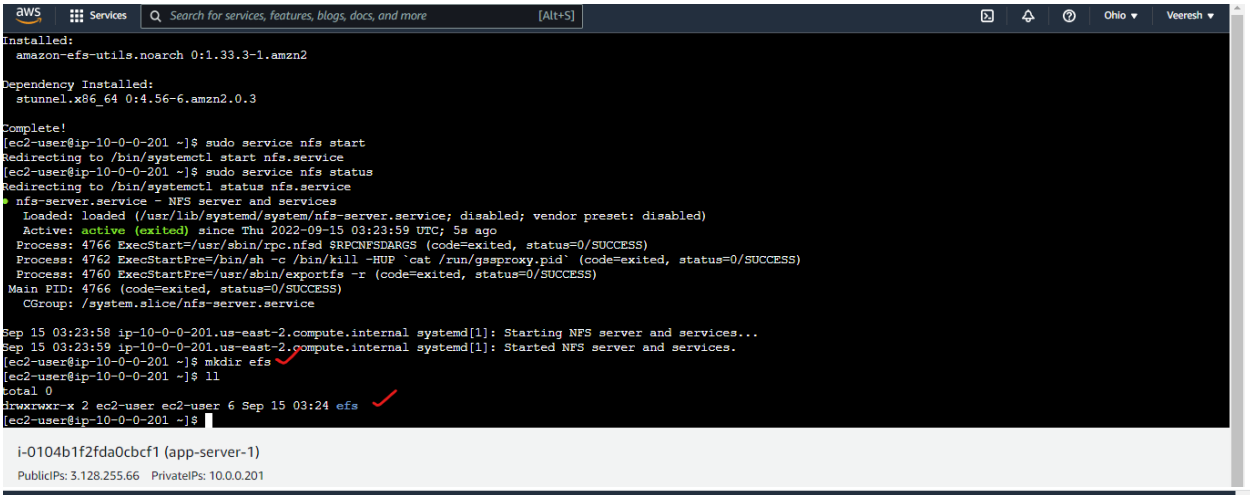
sudo service nfs status //now the status of nfs has been activated.

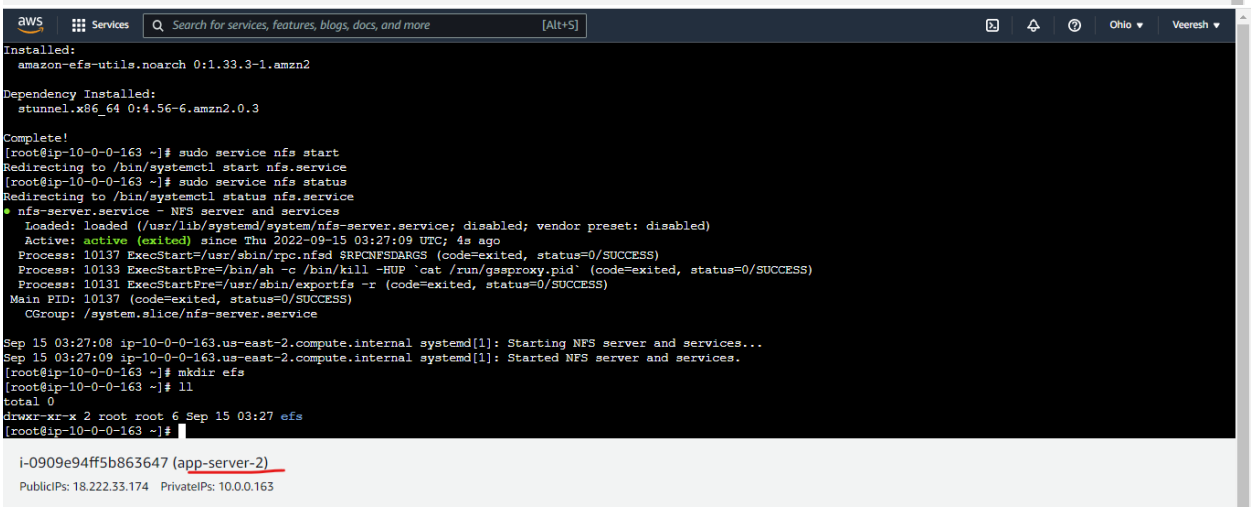
mkdir efs //create a directory of efs is mandatory

- Continue and do the same process to the app-server-2 machine.



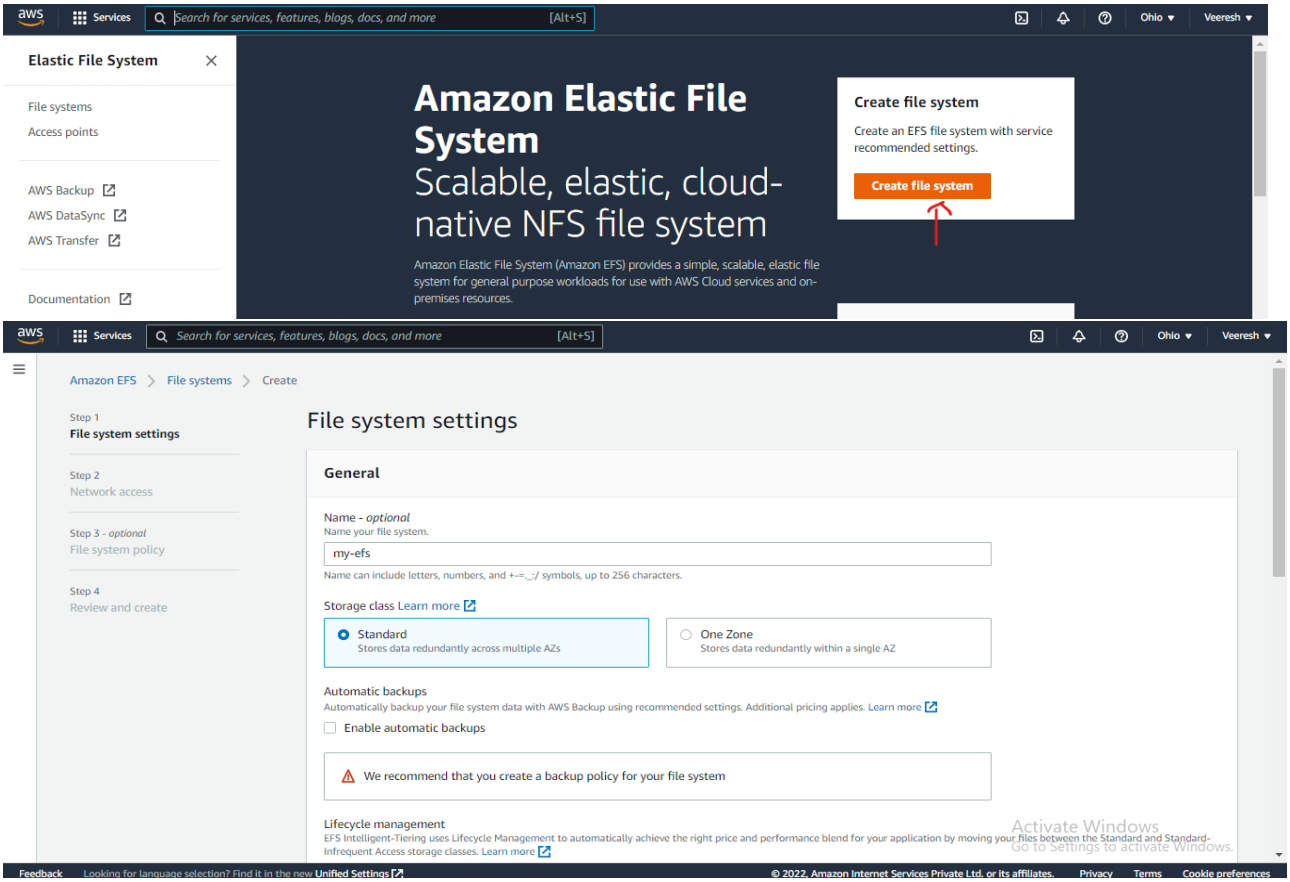


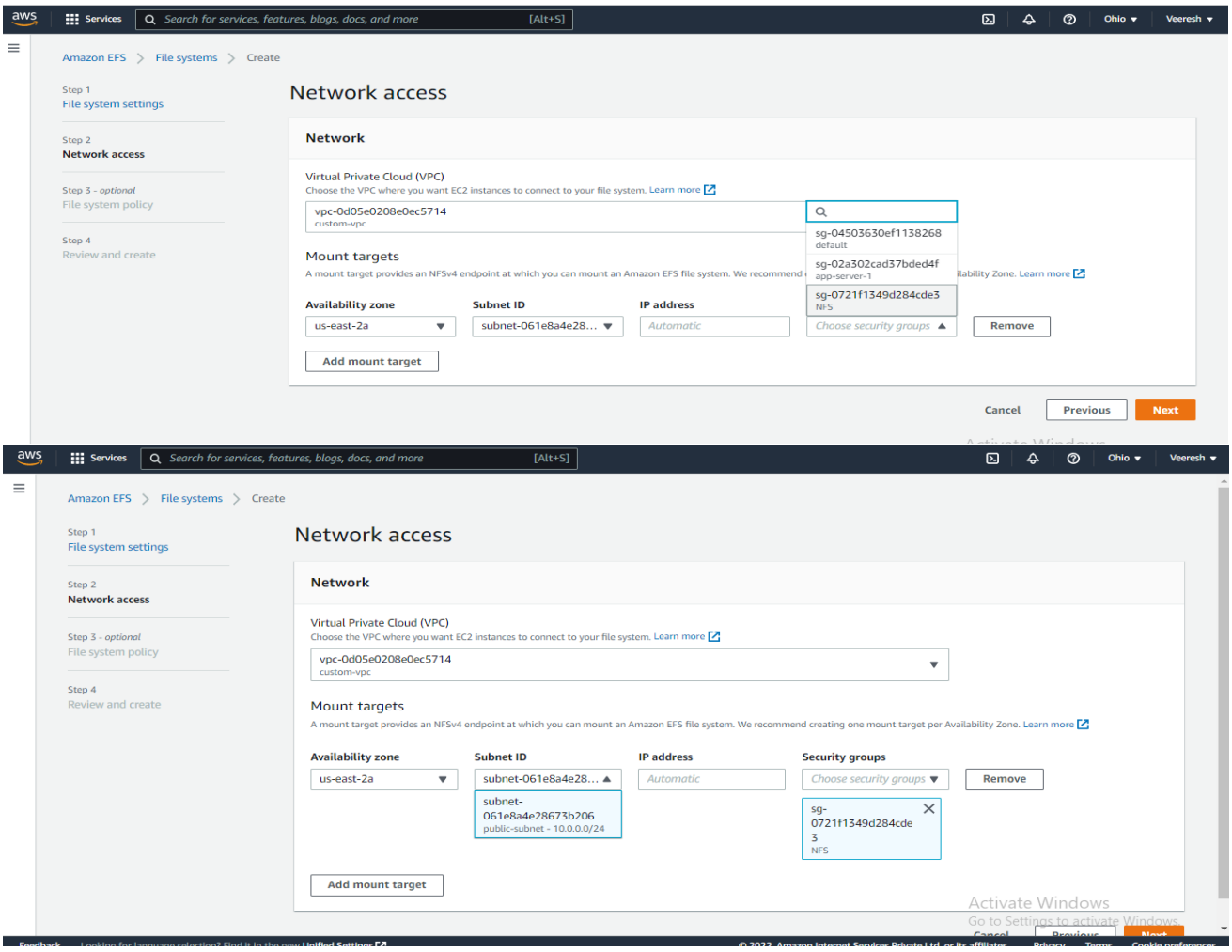




Step 2: Now goto the Amazon EFS >> create filesystem

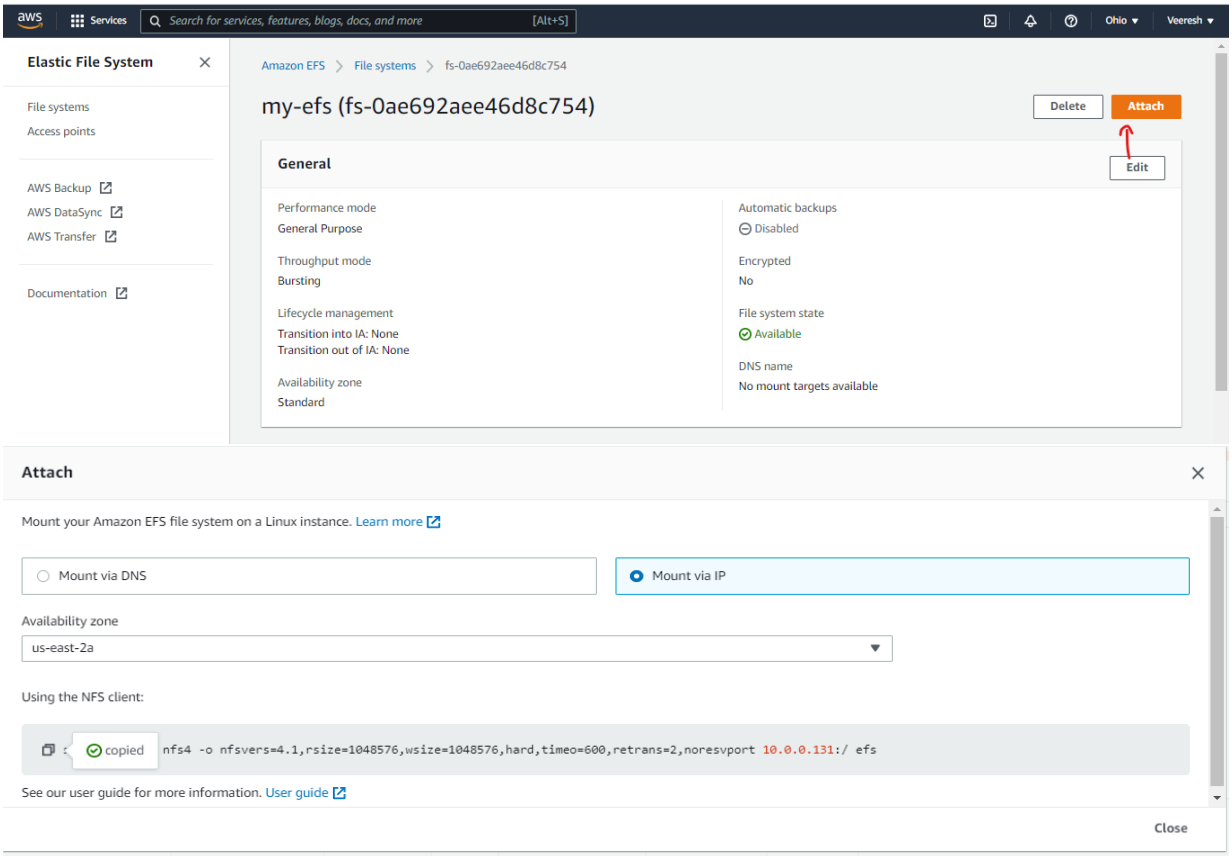
- Name > as per requirement give the name
- Storage class > standard.
- For the practice purpose uncheck the Enable the automatic backups.
- And remaining things are kept default , move to 2nd step network access.
- Network access , make sure the instances and efs are in same custom vpc, to the mount targets add the security group which consists of NFS protocol. and create file system.

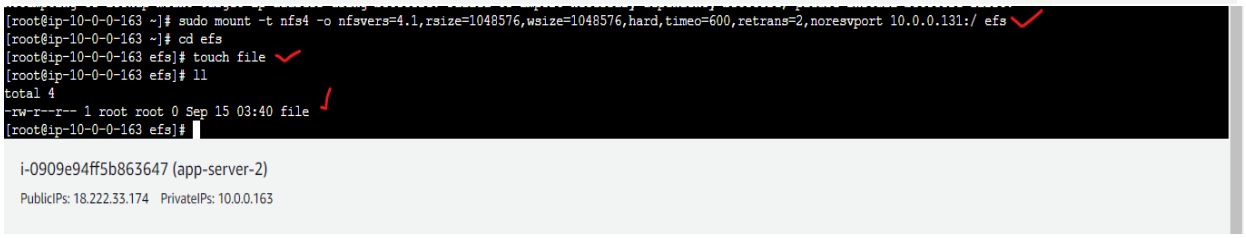

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Ohio
Veeresh
Elastic File System
File systems
Access points
AWS Backup
AWS DataSync
AWS Transfer
Documentation
Amazon Elastic File System
Scalable, elastic, cloud-native NFS file system
Amazon Elastic File System (Amazon EFS) provides a simple, scalable, elastic file system for general purpose workloads for use with AWS Cloud services and on-premises resources.
Create file system
Create an EFS file system with service recommended settings.
Create file system
Amazon EFS
File systems
Create
Step 1
File system settings
Step 2
Network access
Step 3 - optional
File system policy
Step 4
Review and create
File system settings
General
Name - optional
Name your file system.
my-efs
Name can include letters, numbers, and +-=._:/ symbols, up to 256 characters.
Storage class Learn more
Standard
Stores data redundantly across multiple AZs
One Zone
Stores data redundantly within a single AZ
Automatic backups
Automatically backup your file system data with AWS Backup using recommended settings. Additional pricing applies. Learn more
Enable automatic backups
We recommend that you create a backup policy for your file system
Lifecycle management
EFS Intelligent-Tiering uses Lifecycle Management to automatically achieve the right price and performance blend for your application by moving your files between the Standard and Standard-Infrequent Access storage classes. Learn more
Activate Windows
Go to Settings to activate Windows.
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences



Step 3: Into the file system > attach, in the attach to Mount the EFS file system which are created are on a linux instance by using the bellow steps, connect the app-server-2 instance ,

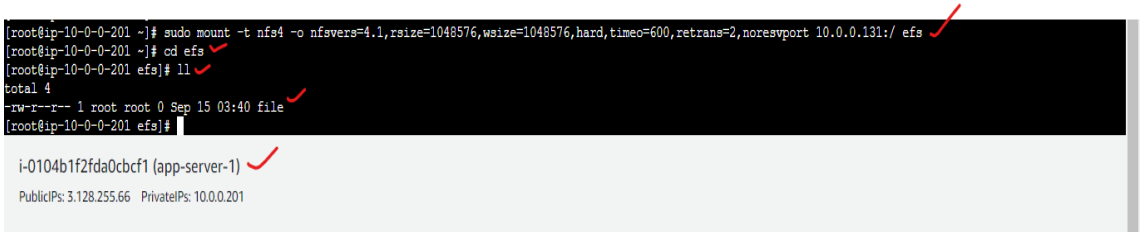
- Sudo su -
- sudo mount –t nfs4 –o ----------:/ efs //this taken from the EFS attach Mount via IP > using the NFS client
- cd efs //open the efs directory
- touch file //create the new file
- ll //check the list





Step 4: connect the another instance (app-server-1) follow the below commands.

- sudo su -
- sudo mount –t nfs4 –o ----------:/ efs //this taken from the EFS attach Mount via IP > using the NFS client
- cd efs //open the efs directory
- ll // check the list and we will get the file which are created in the app-server-2 instance.



This part of exercise will provide some details about the how the Amazon EFS are works on instances. Since the EFS file system supports accessing files mounted on EC2 instances simultaneously.

PART – 4: Setup RDS and connect with EC2 in AWS custom VPC

Setup RDS and connect with EC2, this complete setup are into the creating on private subnet for secure the Database.

Step 1:

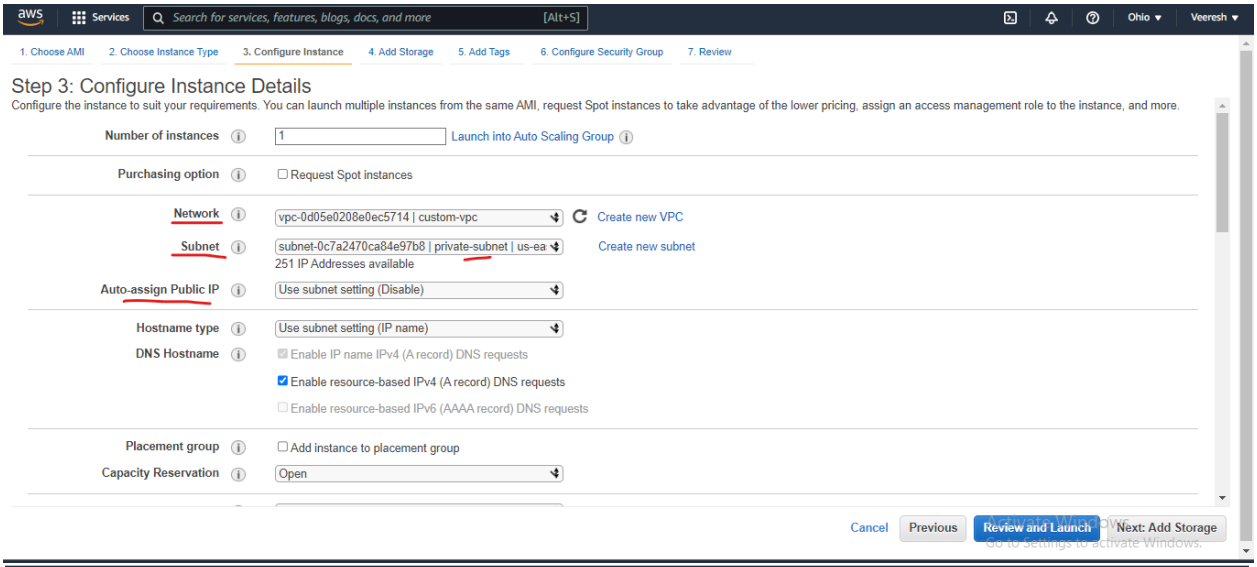
- Launch amazon linux EC2 instance (Database-server) as configure like, Network – select custom VPC, subnet – select private subnet , Auto-assign public IP – Disable it, Security group give the Mysql/aurora 3306 port and protocol And launch it.
- The Database-server are in private subnet which doesn't assign the public IP. We are unable to connect it direct. We need to take the access of Database-server from the app-server-1.
- Then connect the "app-server-1" , switch root user and create a file and add the pem key encrypted data into it.

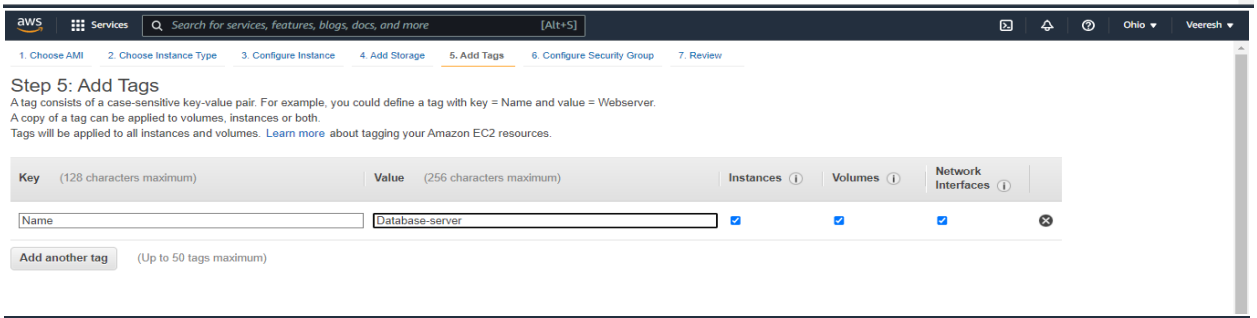
#vim ec2-key.pem //create a file and it on edit mode add the data of Database-server pem file (which are used to launch instance).save it

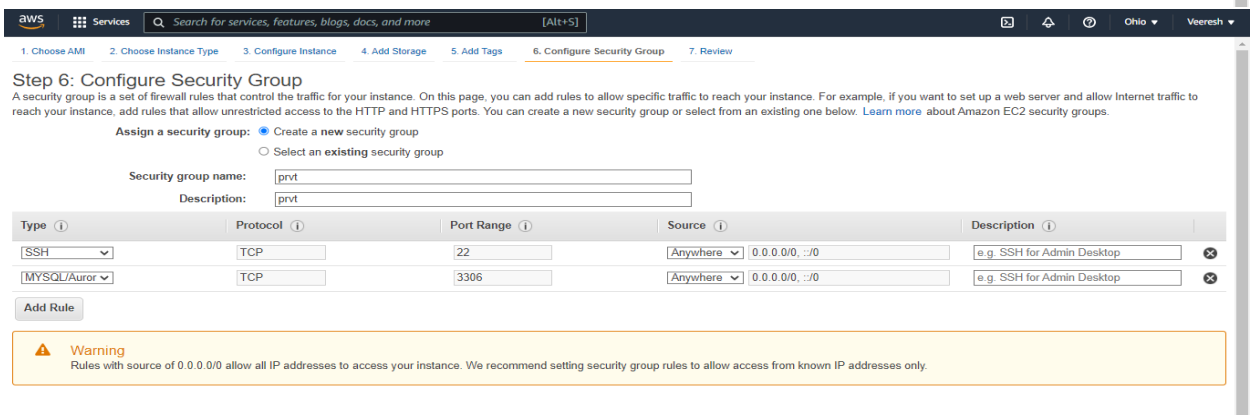
#chmod 400 ec2-key.pem // To protect a file against accidental overwriting

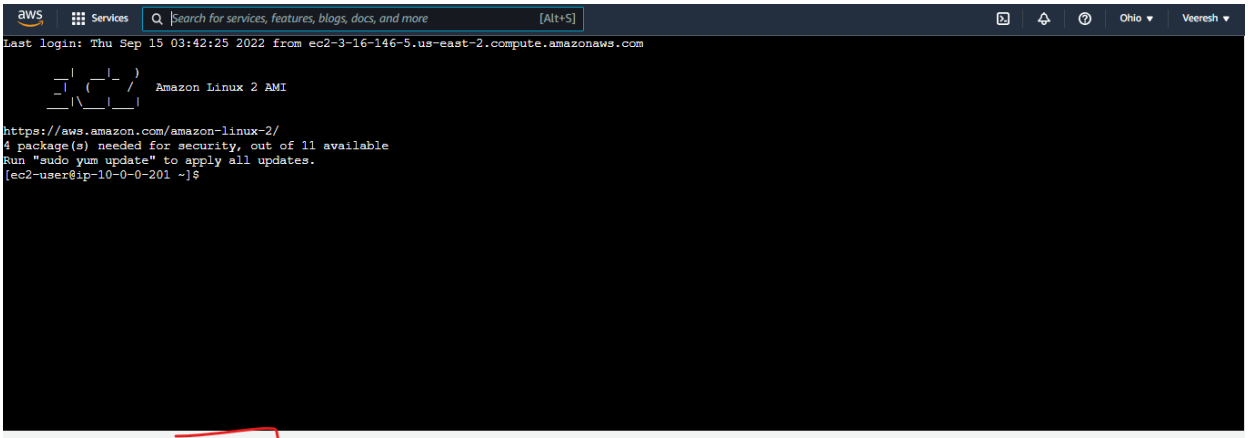
#ssh ec2-user@10.0.1.77 -i ec2-key.pem //10.0.1.77 is the private IP of Database-server

Now enter "yes" command then we will login into the Database-server. Switch to root user, ping google.com check there is no response from google website due to the internet access are not access into this server.


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Ohio
Veeresh
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
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 lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-0d05e0208e0ec5714 | custom-vpc
Create new VPC
Subnet
subnet-0c7a2470ca84e97b8 | private-subnet | us-ea
Create new subnet
251 IP Addresses available
Auto-assign Public IP
Use subnet setting (Disable)
Hostname type
Use subnet setting (IP name)
DNS Hostname
Enable IP name IPv4 (A record) DNS requests
Enable resource-based IPv4 (A record) DNS requests
Enable resource-based IPv6 (AAAA record) DNS requests
Placement group
Add instance to placement group
Capacity Reservation
Open
Cancel
Previous
Review and Launch
Next: Add Storage

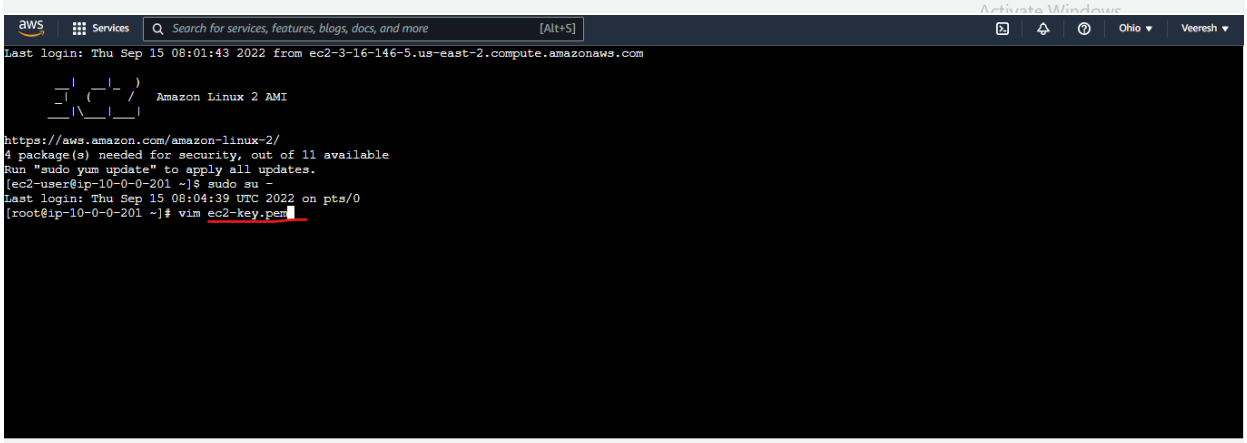

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Ohio
Veeresh
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 5: Add Tags
A tag consists of a case-sensitive key-value pair. For example, you could 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
Network Interfaces
Name
Database-server
Add another tag
(Up to 50 tags maximum)


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Ohio
Veeresh
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:
prvt
Description:
prvt
Type
Protocol
Port Range
Source
Description
SSH
TCP
22
Anywhere
0.0.0.0/0, ::/0
e.g. SSH for Admin Desktop
MYSQL/Auror
TCP
3306
Anywhere
0.0.0.0/0, ::/0
e.g. SSH for Admin Desktop
Add Rule
Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.



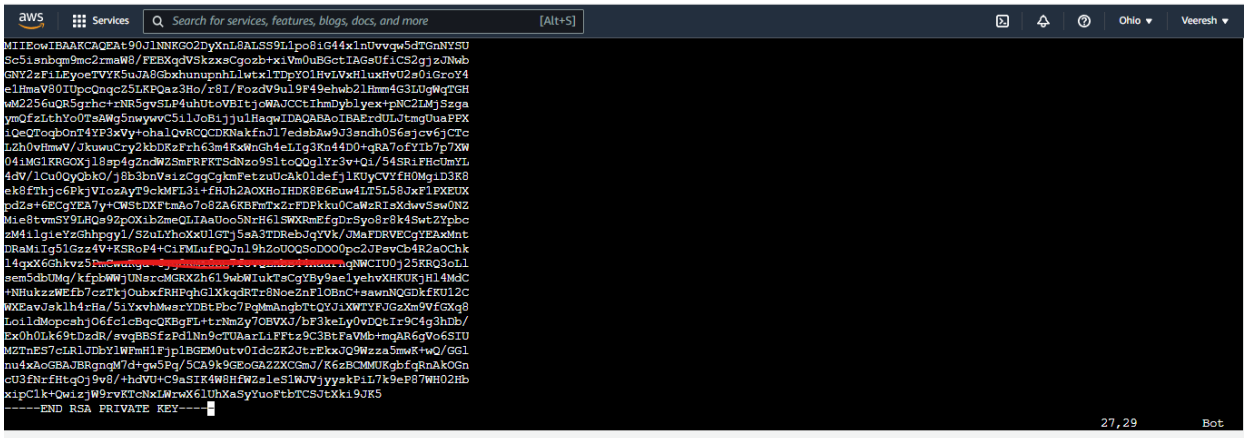
i-0104b1f2fda0cbcf1 (app-server-1)

PublicIPs: 3.128.255.66 PrivateIPs: 10.0.0.201



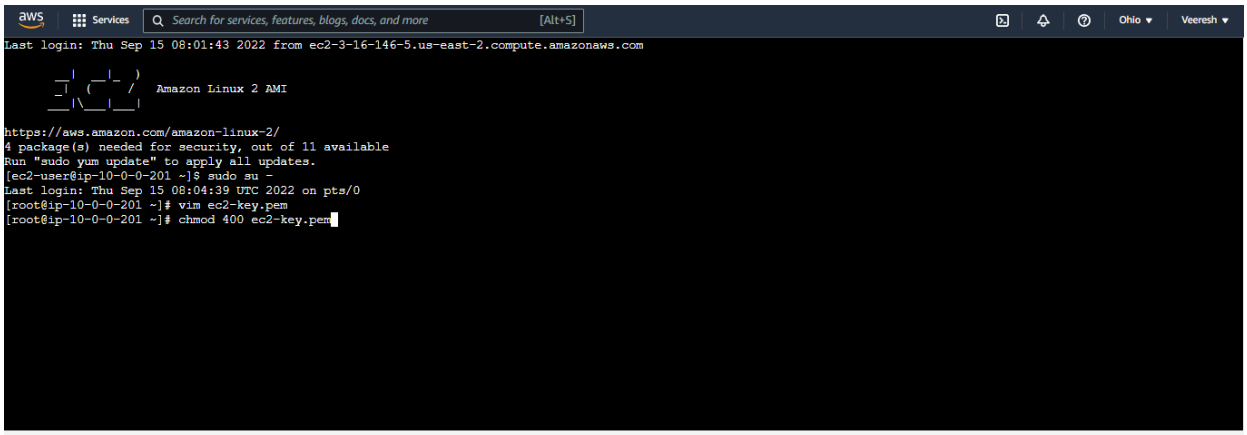
i-0104b1f2fda0cbcf1 (app-server-1)

PublicIPs: 3.128.255.66 PrivateIPs: 10.0.0.201



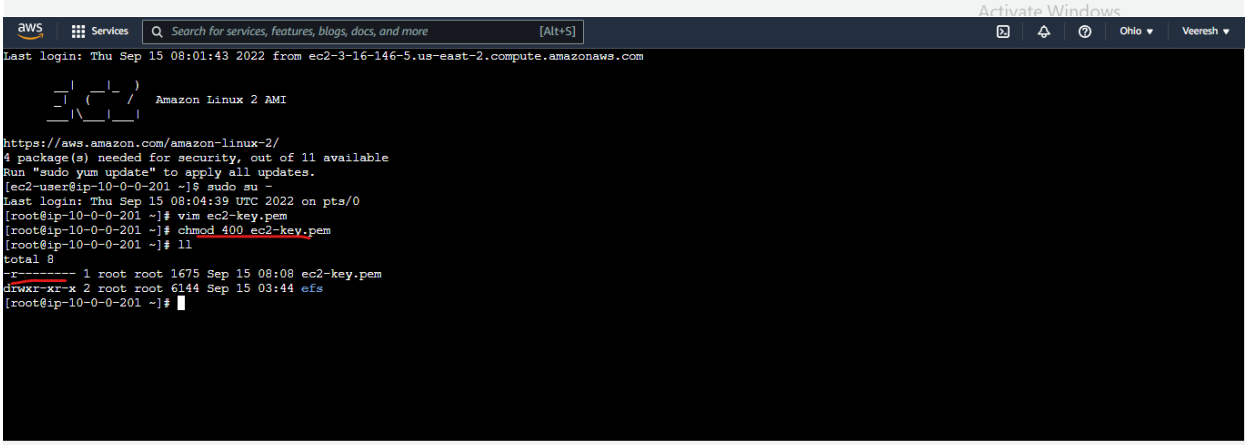
i-0104b1f2fda0cbcf1 (app-server-1)

PublicIPs: 3.128.255.66 PrivateIPs: 10.0.0.201



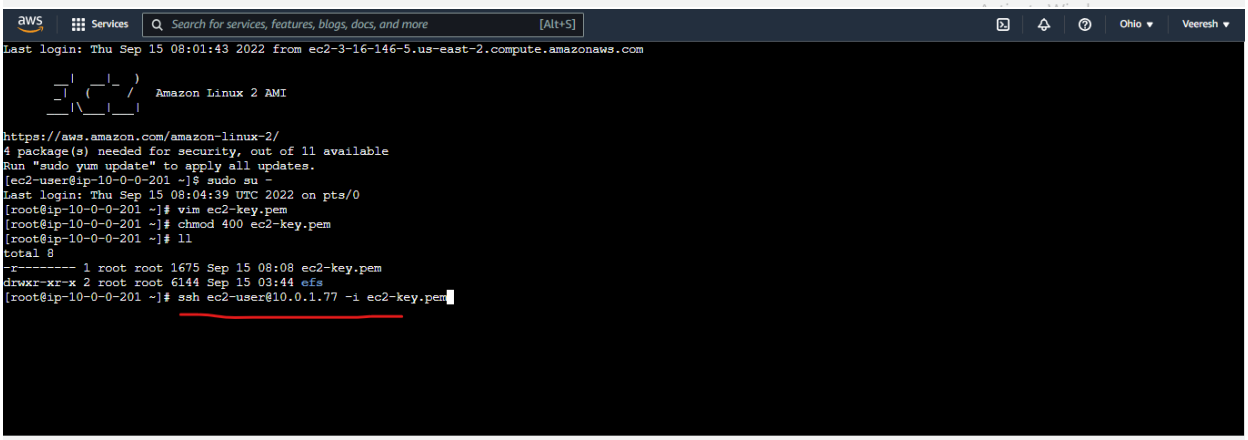
i-0104b1f2fda0cbcf1 (app-server-1)

PublicIPs: 3.128.255.66 PrivateIPs: 10.0.0.201



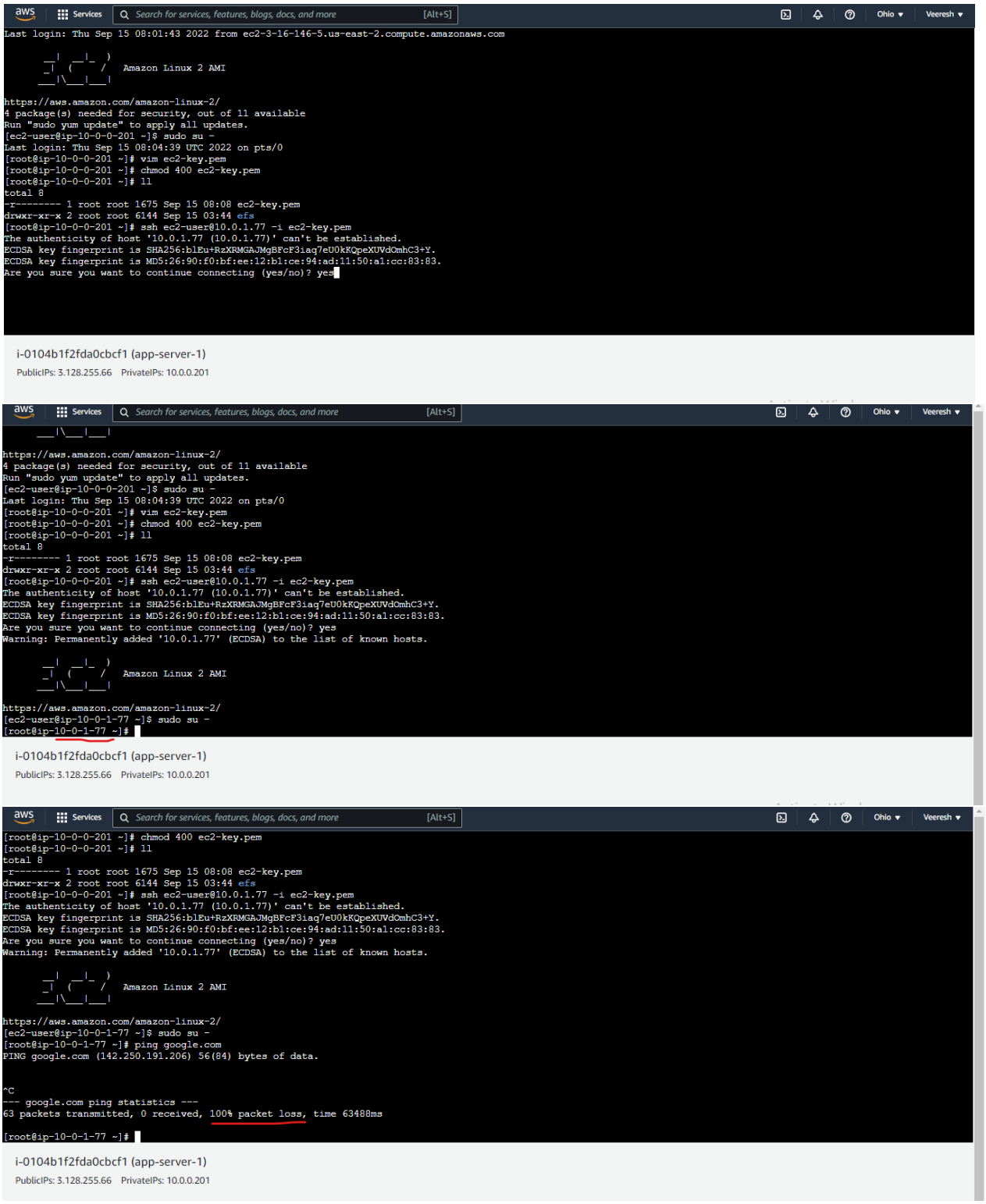
i-0104b1f2fda0cbcf1 (app-server-1)

PublicIPs: 3.128.255.66 PrivateIPs: 10.0.0.201



i-0104b1f2fda0cbcf1 (app-server-1)

PublicIPs: 3.128.255.66 PrivateIPs: 10.0.0.201



Step 2: NAT Gateway is a device used to enable the Database-server instance in a private subnet to connect to the internet. Create natgateway and route table as shown below,

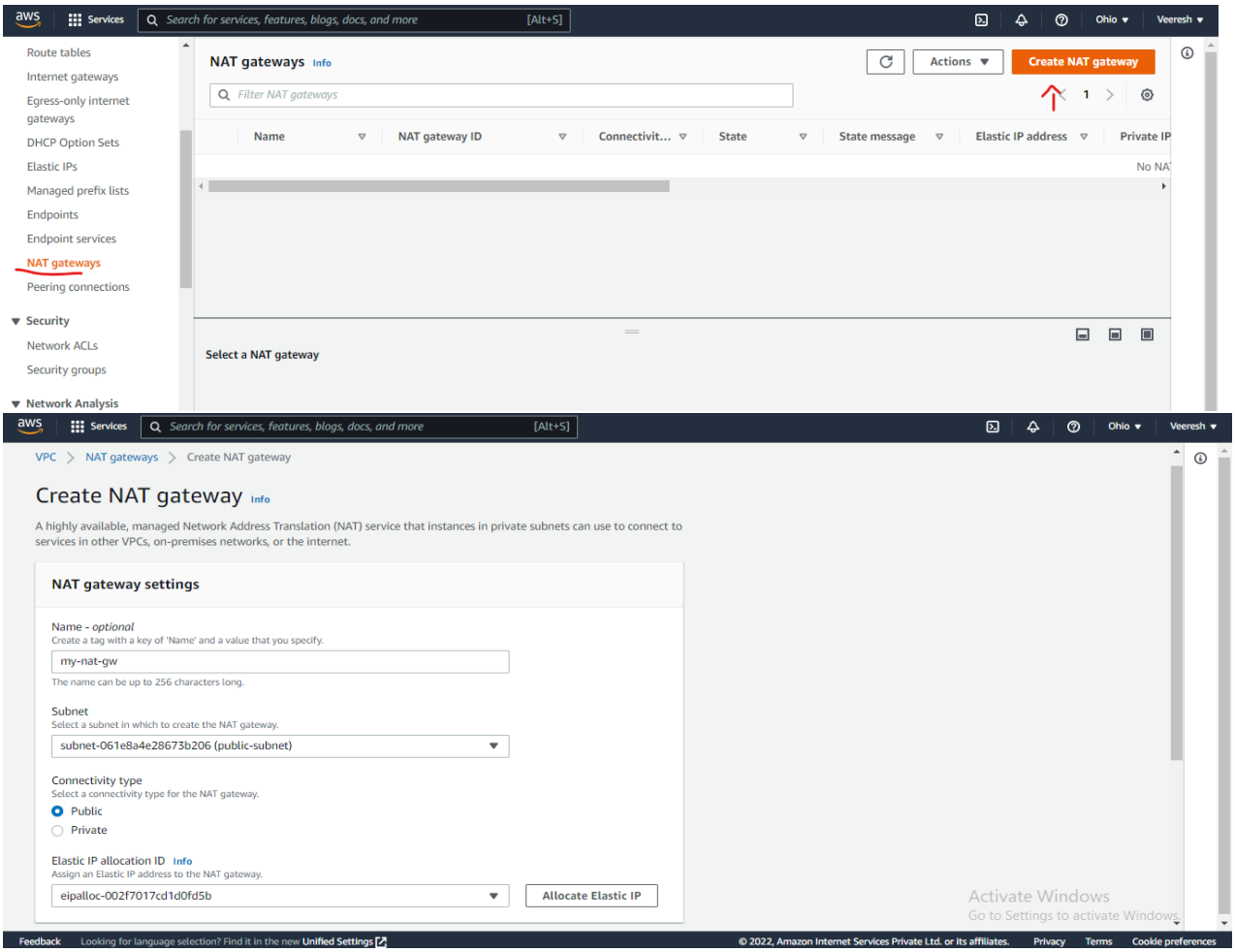
NAT gateway,

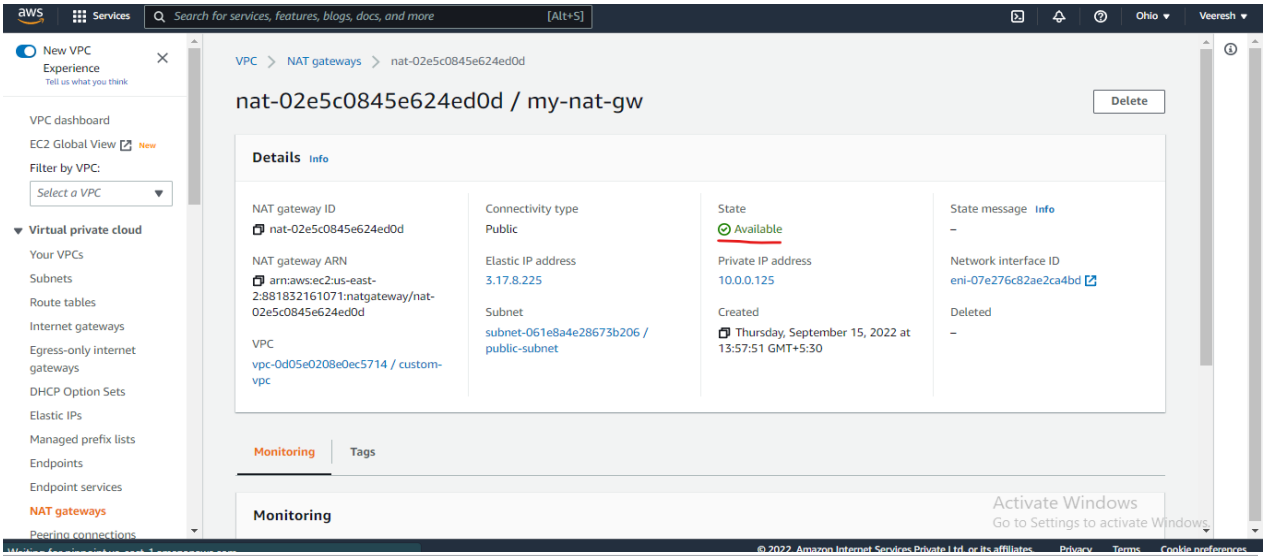
- From the VPC dashboard select NAT gateway and click create NAT gateway.
- Give the name of NAT gateway for identification.
- Subnet – public subnet, connectivity type public, allocate elastic IP and create NAT gateway.

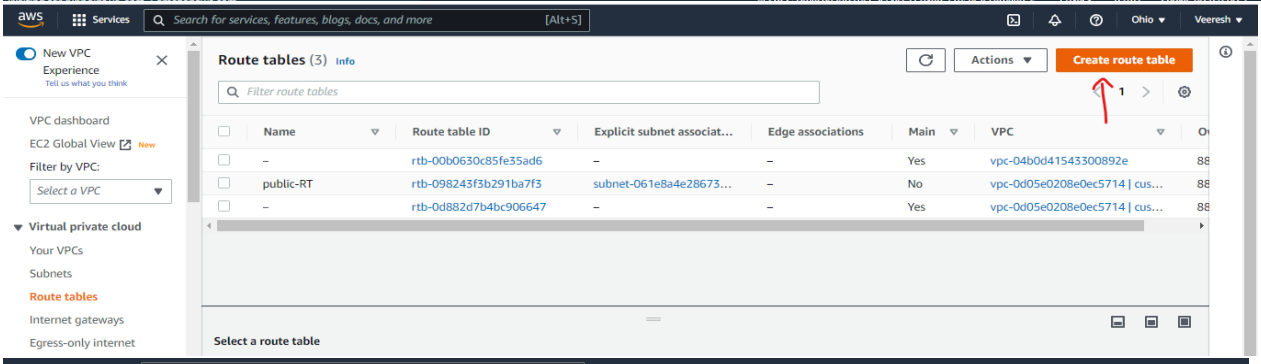
Route tables,

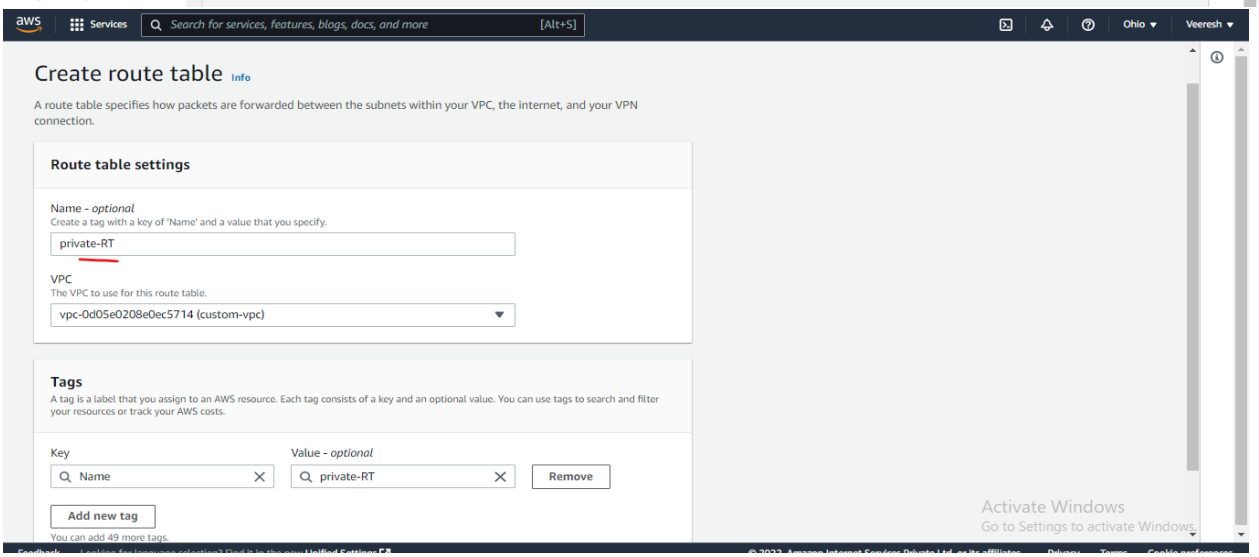
- From the VPC dashboard select Route tables and click create Route tables.
- Name – private RT, VPC – select the custom VPC and create it.
- Associate this Route tables with the private subnet from the subnet association --> edit subnet associations --> select private subnet and save associates.
- Now goto the Routes --> Edit routes --> destination – 0.0.0.0/0 and Target – NAT gateway select it which are previously created and save changes.

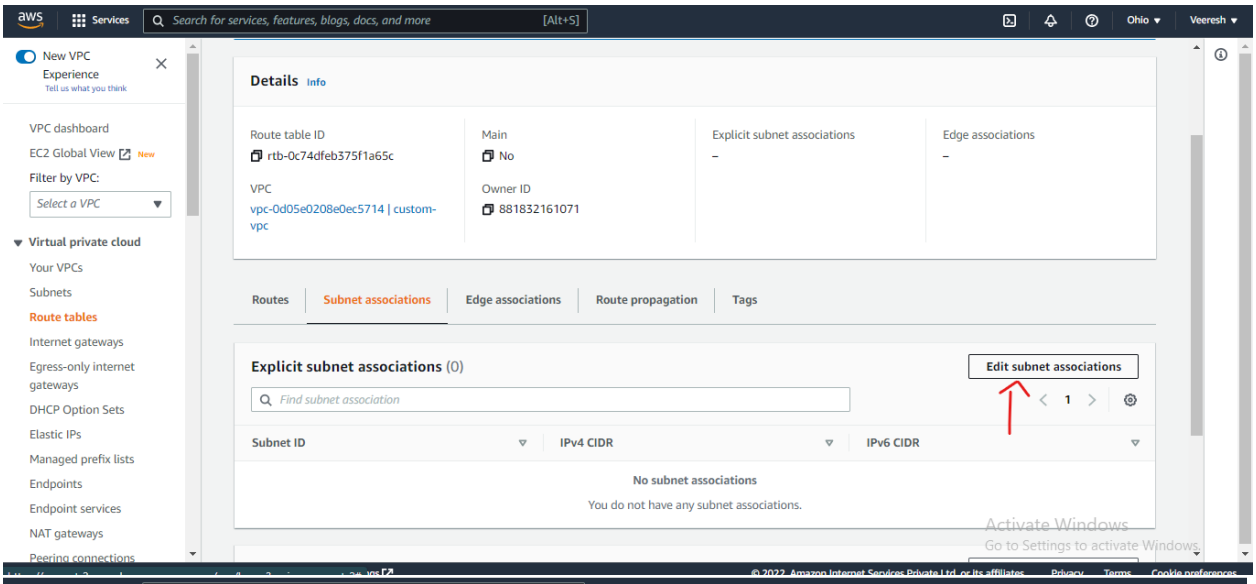
Now get back to the Database-server which are access from the app-server-1, then ping google.com we can get the response. Since we build a successful internet connection to the private subnet's Database-server.

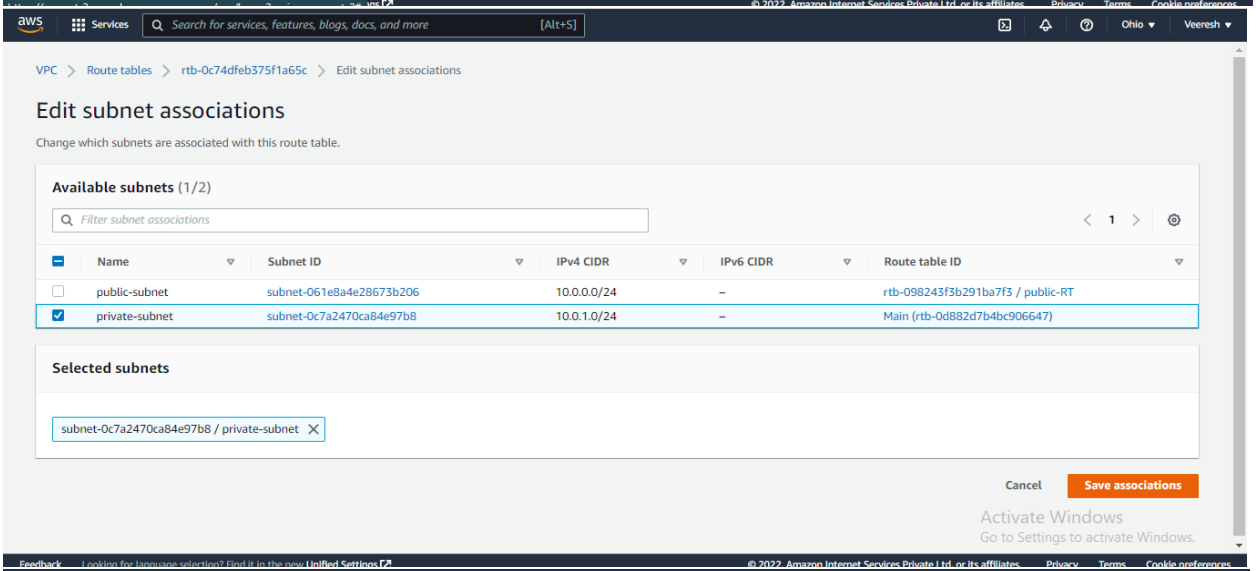


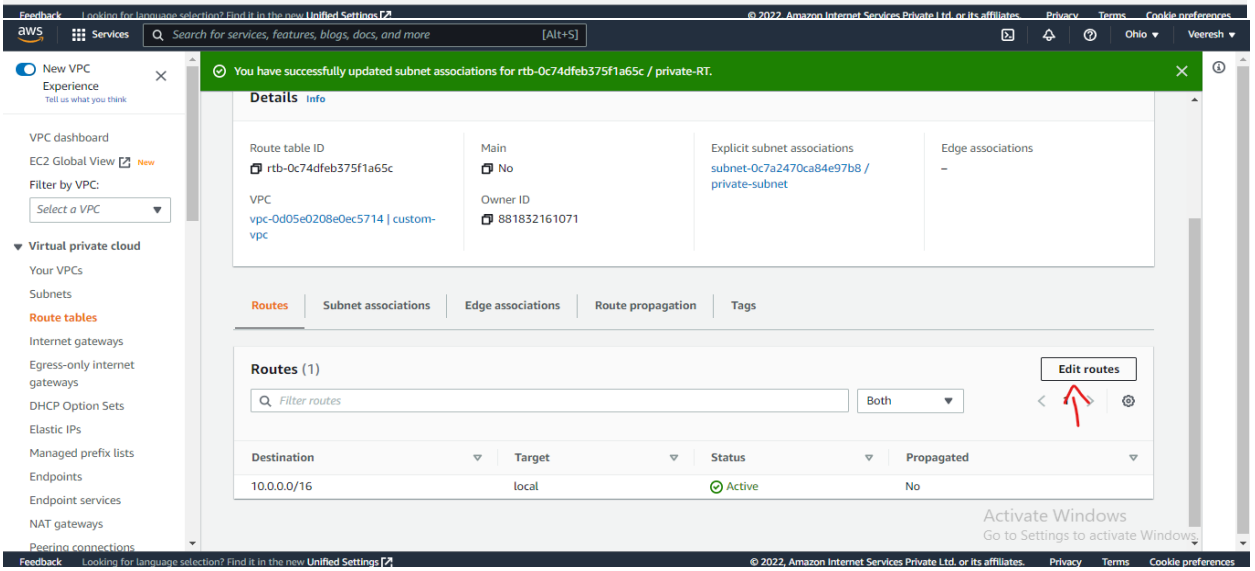

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Ohio
Veeresh
New VPC Experience
Tell us what you think
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP Option Sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
VPC > NAT gateways > nat-02e5c0845e624ed0d
nat-02e5c0845e624ed0d / my-nat-gw
Delete
Details Info
NAT gateway ID
nat-02e5c0845e624ed0d
NAT gateway ARN
arn:aws:ec2:us-east-2:881832161071:natgateway/nat-02e5c0845e624ed0d
VPC
vpc-0d05e0208e0ec5714 / custom-vpc
Connectivity type
Public
Elastic IP address
3.17.8.225
Subnet
subnet-061e8a4e28673b206 / public-subnet
State
Available
Private IP address
10.0.0.125
Created
Thursday, September 15, 2022 at 13:57:51 GMT+5:30
State message Info
-
Network interface ID
eni-07e276c82ae2ca4bd
Deleted
-
Monitoring
Tags
Monitoring
Activate Windows
Go to Settings to activate Windows.

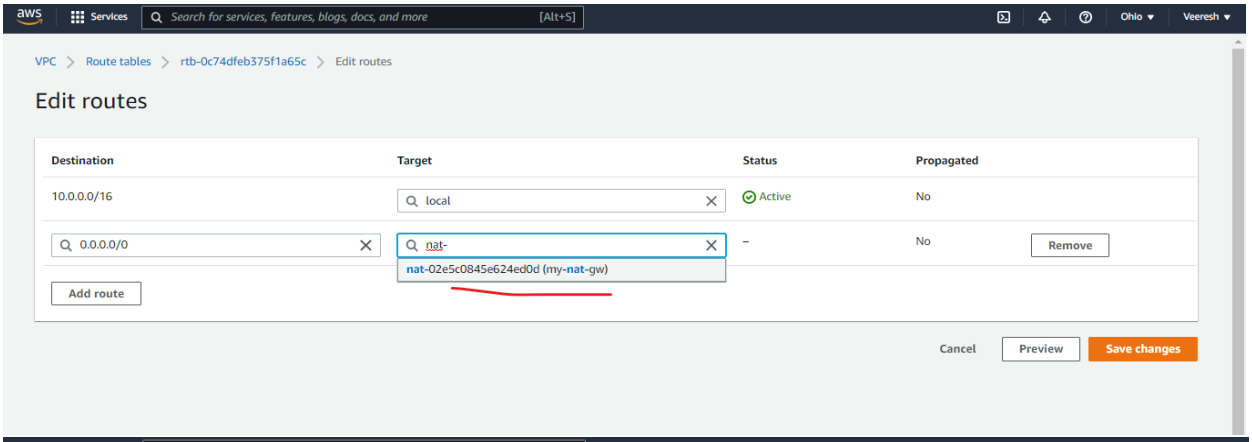

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Ohio
Veeresh
New VPC Experience
Tell us what you think
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet
Route tables (3) Info
Actions
Create route table
Filter route tables
Name
Route table ID
Explicit subnet associat...
Edge associations
Main
VPC
rtb-00b0630c85fe35ad6
-
-
Yes
vpc-04b0d41543300892e
public-RT
rtb-098243f3b291ba7f3
subnet-061e8a4e28673...
-
No
vpc-0d05e0208e0ec5714 | cus...
rtb-0d882d7b4bc906647
-
-
Yes
vpc-0d05e0208e0ec5714 | cus...
Select a route table

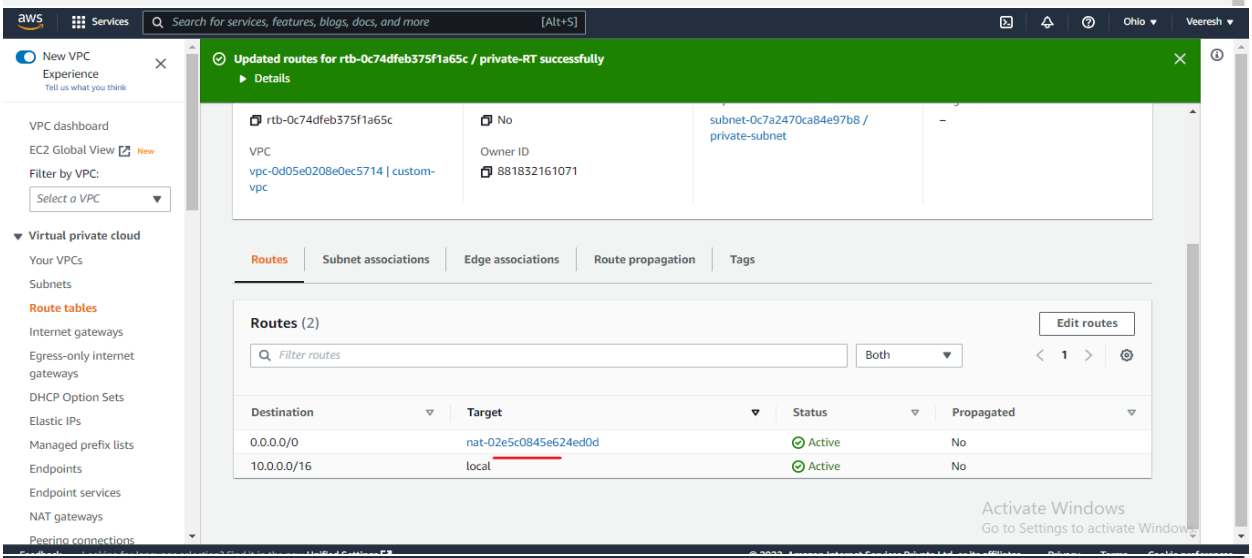

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Ohio
Veeresh
Create route table Info
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
private-RT
VPC
The VPC to use for this route table.
vpc-0d05e0208e0ec5714 (custom-vpc)
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
Name
private-RT
Remove
Add new tag
You can add 49 more tags.
Activate Windows
Go to Settings to activate Windows.

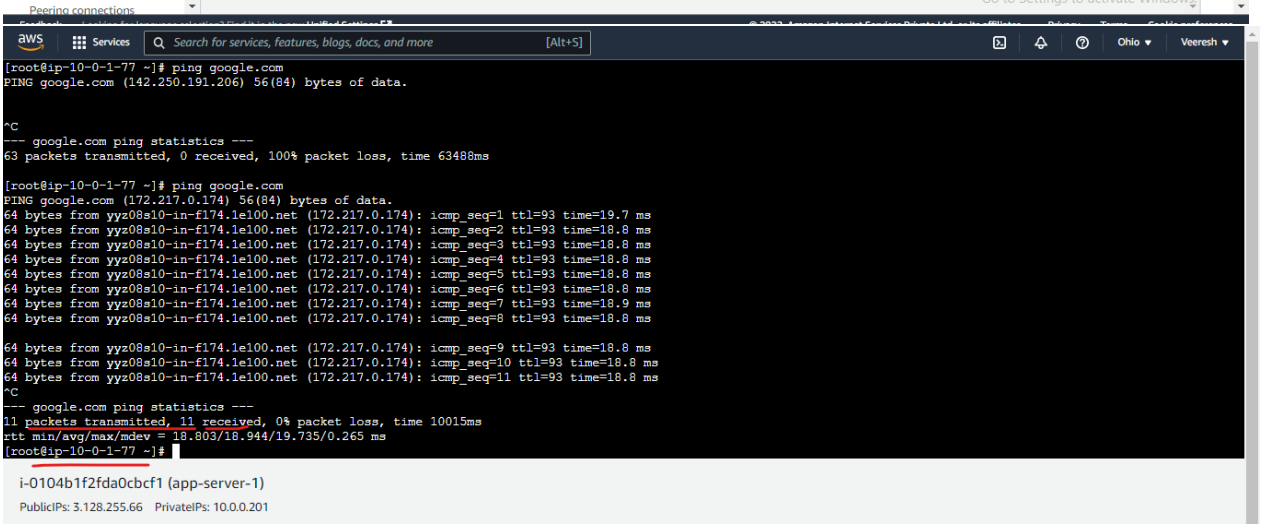

Details Info
Route table ID
rtb-0c74dfeb375f1a65c
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0d05e0208e0ec5714 | custom-vpc
Owner ID
881832161071
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (0)
Edit subnet associations
Find subnet association
Subnet ID
IPv4 CIDR
IPv6 CIDR
No subnet associations
You do not have any subnet associations.


VPC > Route tables > rtb-0c74dfeb375f1a65c > Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (1/2)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
public-subnet
subnet-061e8a4e28673b206
10.0.0.0/24
–
rtb-098243f3b291ba7f3 / public-RT
private-subnet
subnet-0c7a2470ca84e97b8
10.0.1.0/24
–
Main (rtb-0d882d7b4bc906647)
Selected subnets
subnet-0c7a2470ca84e97b8 / private-subnet
Cancel
Save associations


You have successfully updated subnet associations for rtb-0c74dfeb375f1a65c / private-RT.
Details Info
Route table ID
rtb-0c74dfeb375f1a65c
Main
No
Explicit subnet associations
subnet-0c7a2470ca84e97b8 / private-subnet
Edge associations
–
VPC
vpc-0d05e0208e0ec5714 | custom-vpc
Owner ID
881832161071
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (1)
Edit routes
Filter routes
Both
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No



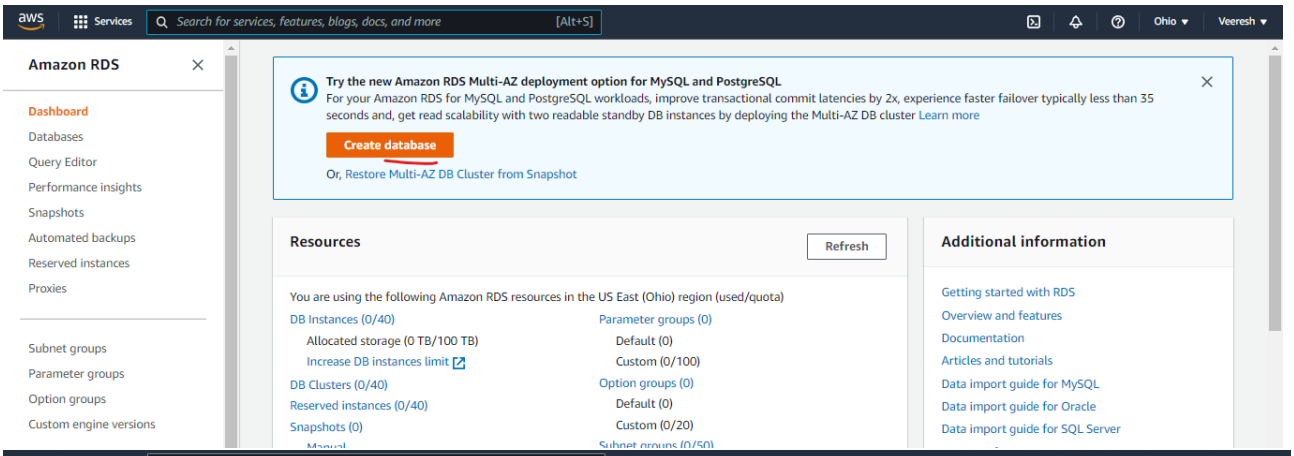


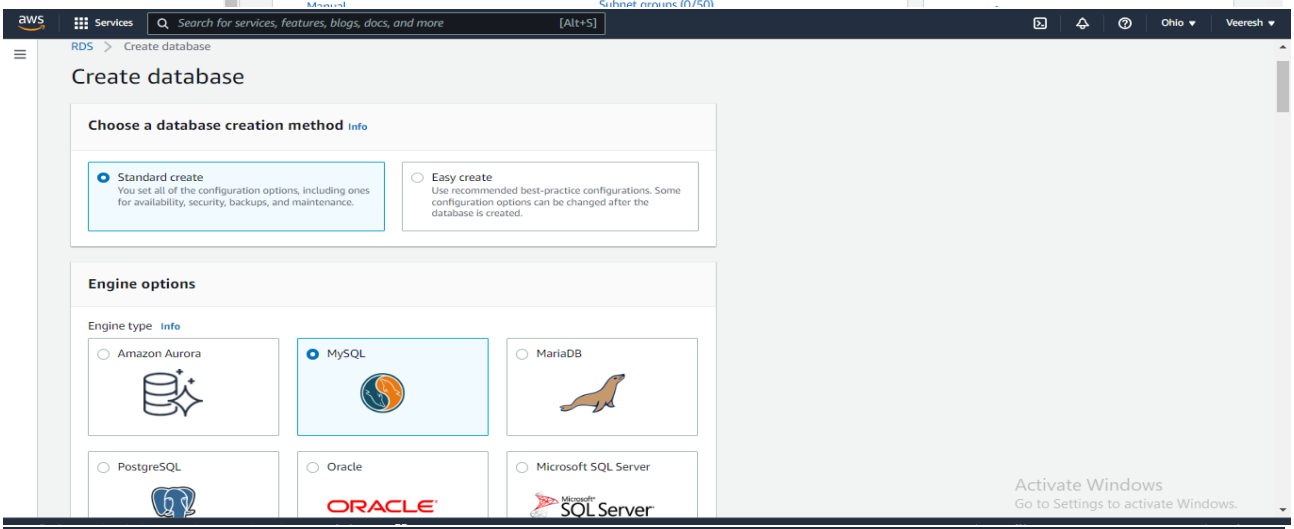


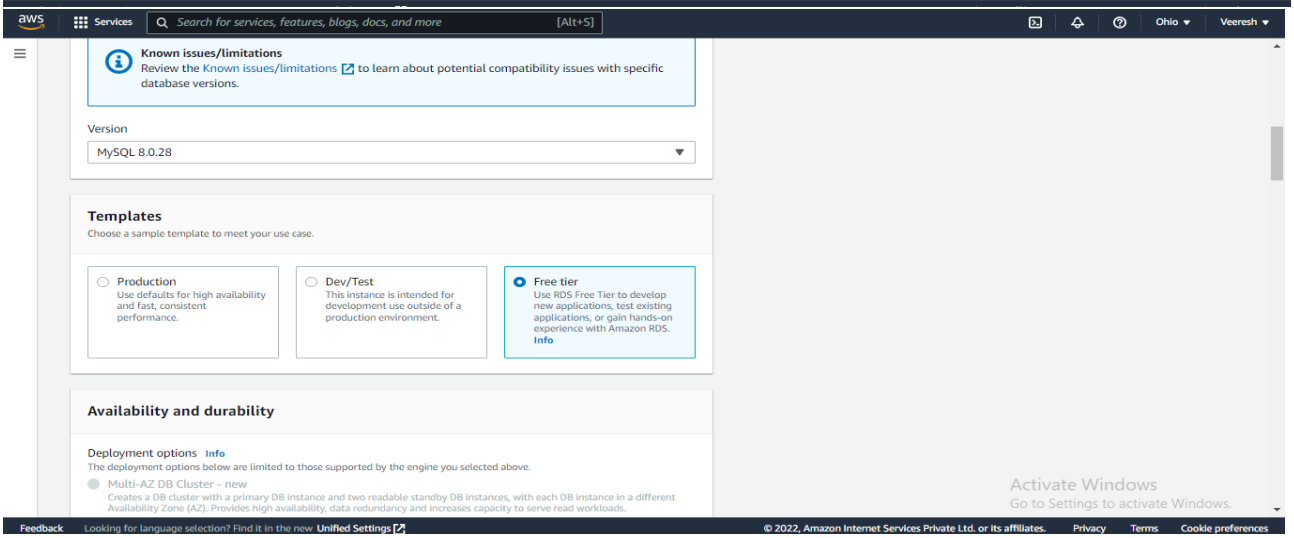
Step 3 : Creating Mysql Database and setup to EC2 (Database-server).

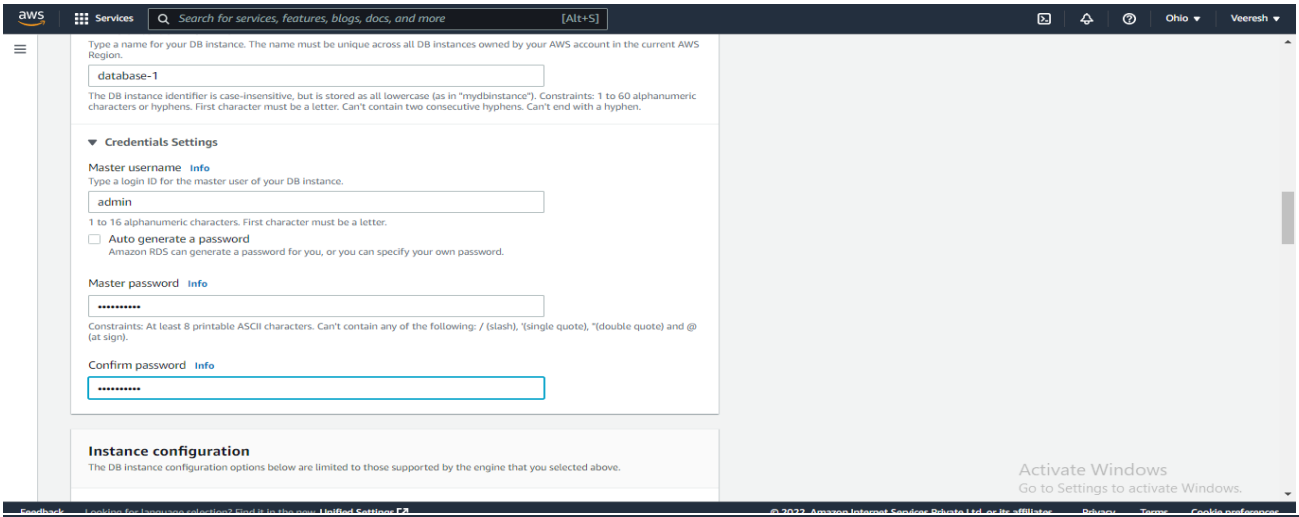
- Goto aws RDS dashboard then click “create database” .
- Engine options – Mysql , version – select updated version, Templates – free tier.
- Credential settings --> Master username – admin, Master password – give the own password.

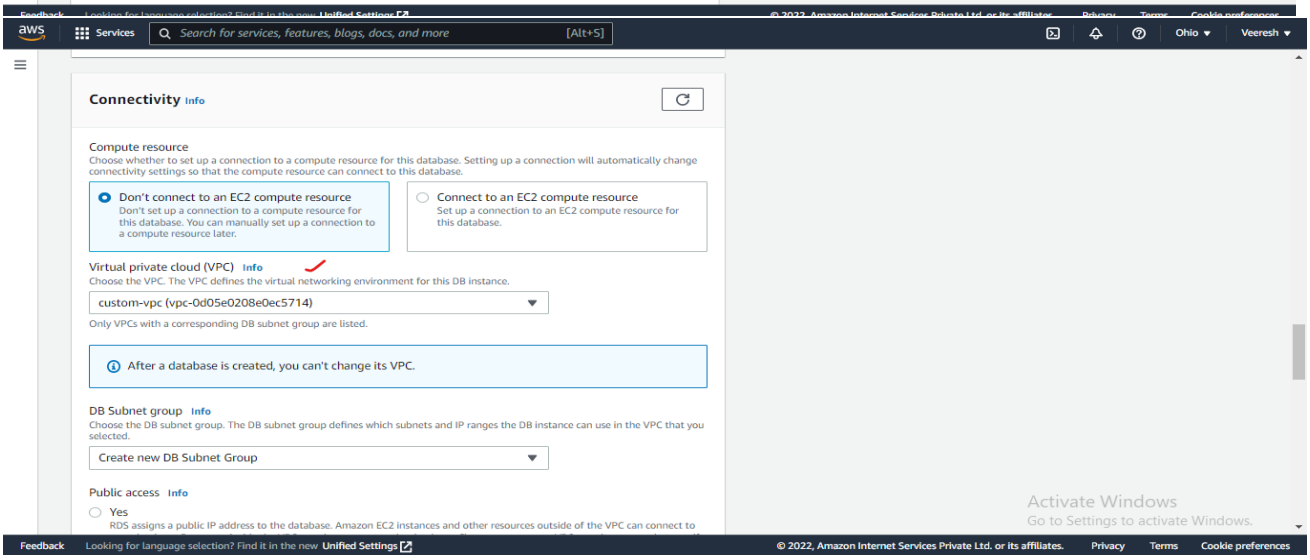
- Connectivity --> VPC – custom vpc, public access – no , VPC security group – add security group which are contain MYsql – 3306 port and protocol, Availability zone – private az.
- Create It. Copy the End point of database which will used to take this into to the ec2.

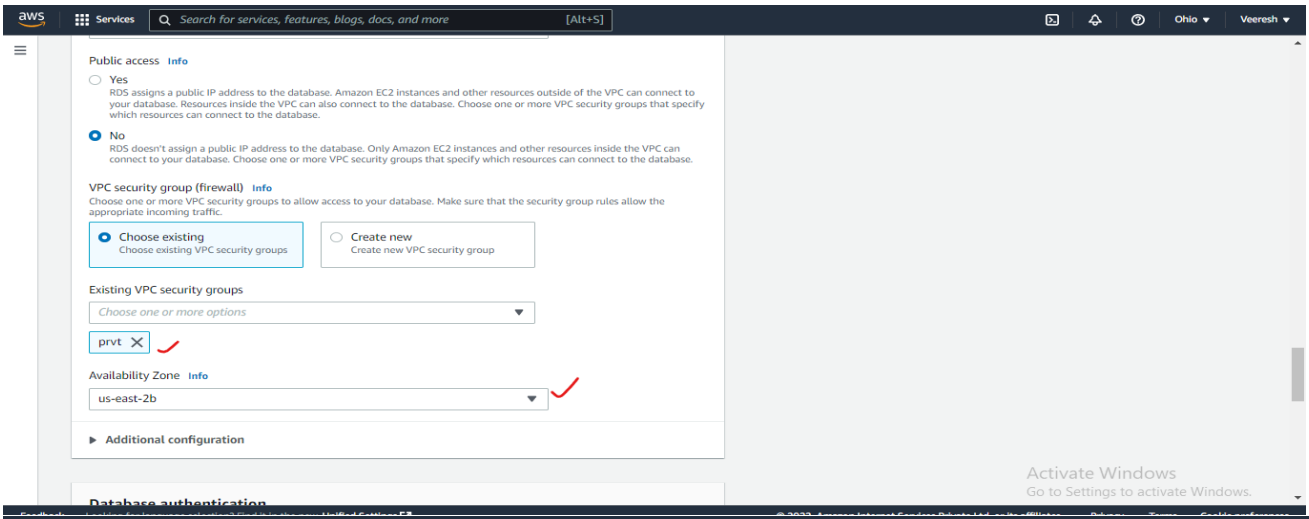


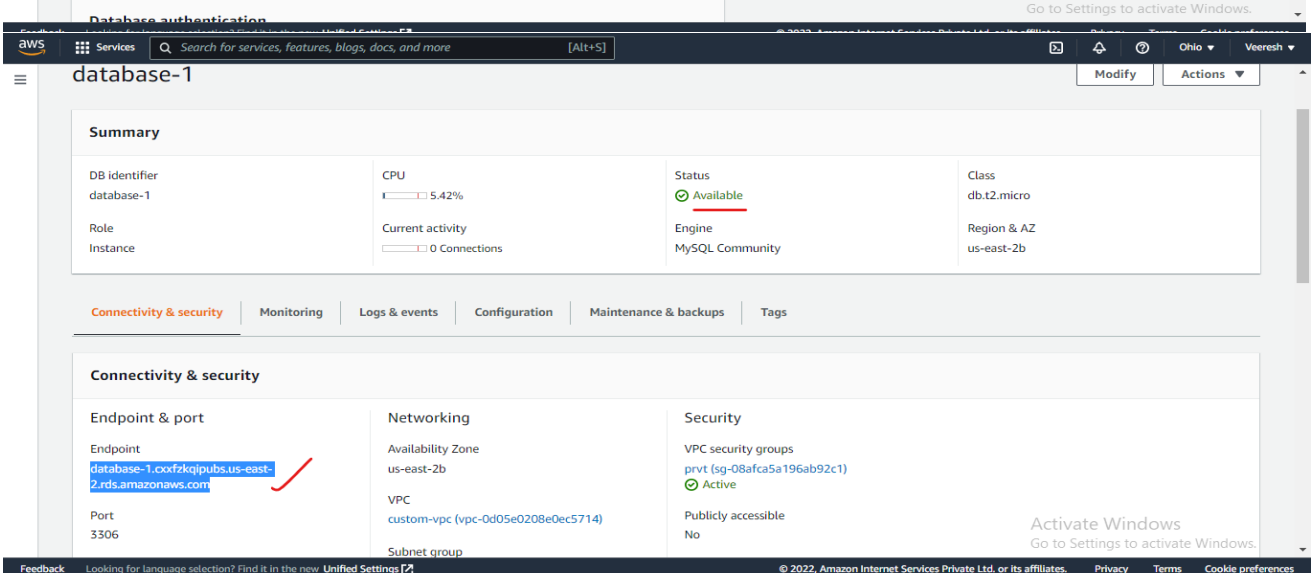





aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Ohio
Veeresh
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.
database-1
The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.
Credentials Settings
Master username Info
Type a login ID for the master user of your DB instance.
admin
1 to 16 alphanumeric characters. First character must be a letter.
Auto generate a password
Amazon RDS can generate a password for you, or you can specify your own password.
Master password Info
Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).
Confirm password Info
Instance configuration
The DB instance configuration options below are limited to those supported by the engine that you selected above.
Activate Windows
Go to Settings to activate Windows.


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Ohio
Veeresh
Connectivity Info
Compute resource
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.
Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.
Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.
Virtual private cloud (VPC) Info
Choose the VPC. The VPC defines the virtual networking environment for this DB instance.
custom-vpc (vpc-0d05e0208e0ec5714)
Only VPCs with a corresponding DB subnet group are listed.
After a database is created, you can't change its VPC.
DB Subnet group Info
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.
Create new DB Subnet Group
Public access Info
Yes
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to
Activate Windows
Go to Settings to activate Windows.
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences





Step 4 : to get the access of Mysql Database which are previously created to the Ec2 instance (Database-server) follow the below instructions,

- First connect the app-server-1 and login to the Database-server,
  by this command- #ssh ec2-user@10.0.1.77 -i ec2-key.pem

#sudo su - //switch to root user

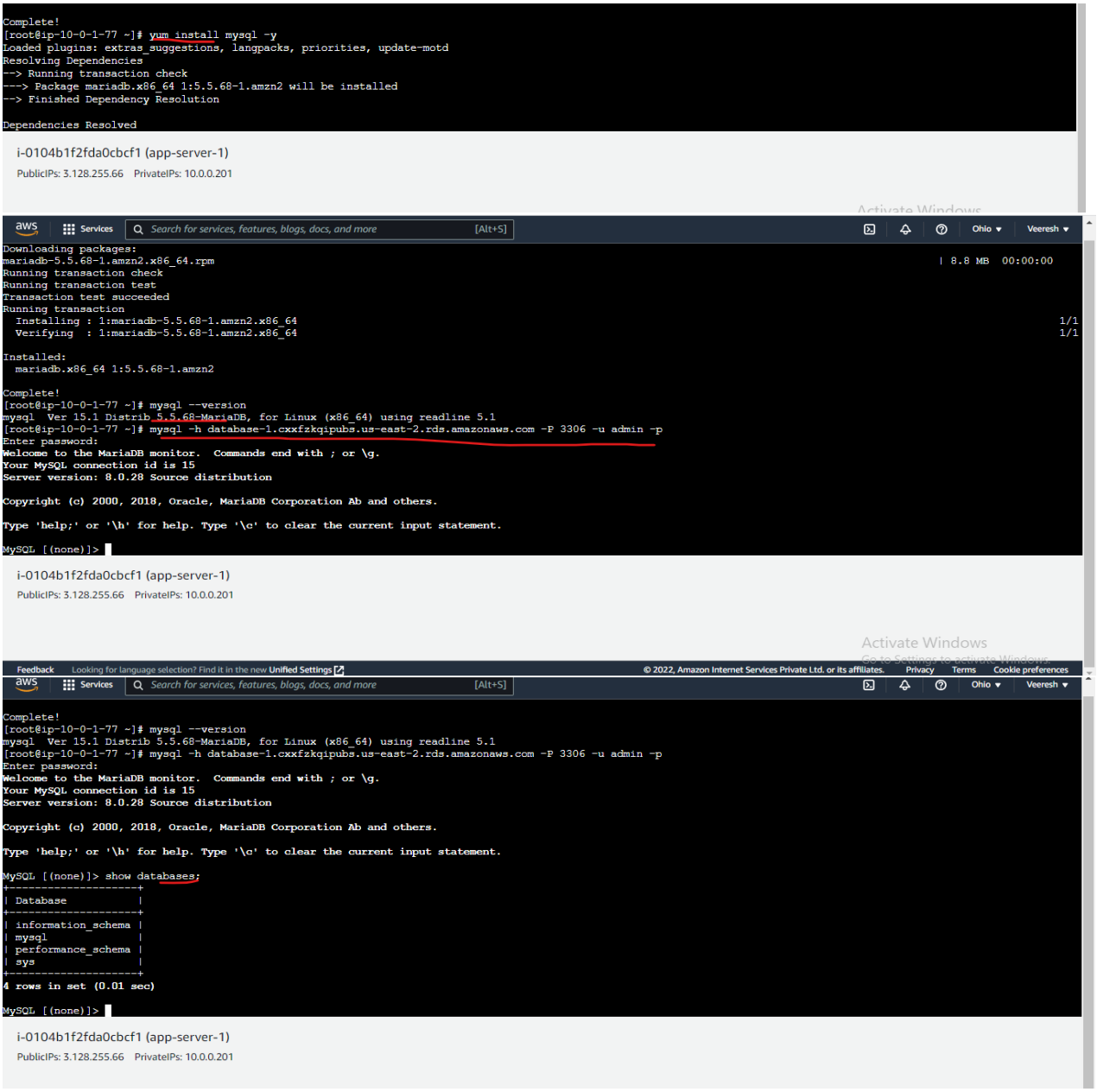
#yum update -y //update the all packages

#yum install mysql -y //install the myql appliation

#mysql --version //check the version of mysql

#mysql –h databaseendpoint –P 3306 –u admin -p

Give password and hit enter, then we get the access of database.



Conclusion: completed all the three exercises with in the custom VPC.