Project: Segregation of Management Traffic via VPC Peering in AWS

Description:

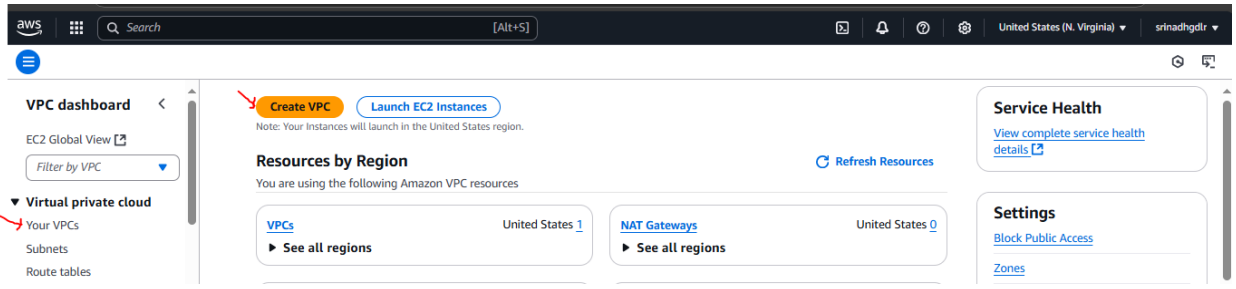
Designed and implemented a secure network architecture using Amazon VPC Peering to isolate management traffic from application traffic. This separation enhanced security by enforcing network segmentation, reduced the risk of lateral movement in case of a breach, and optimized traffic flow between critical infrastructure components. The solution involved:

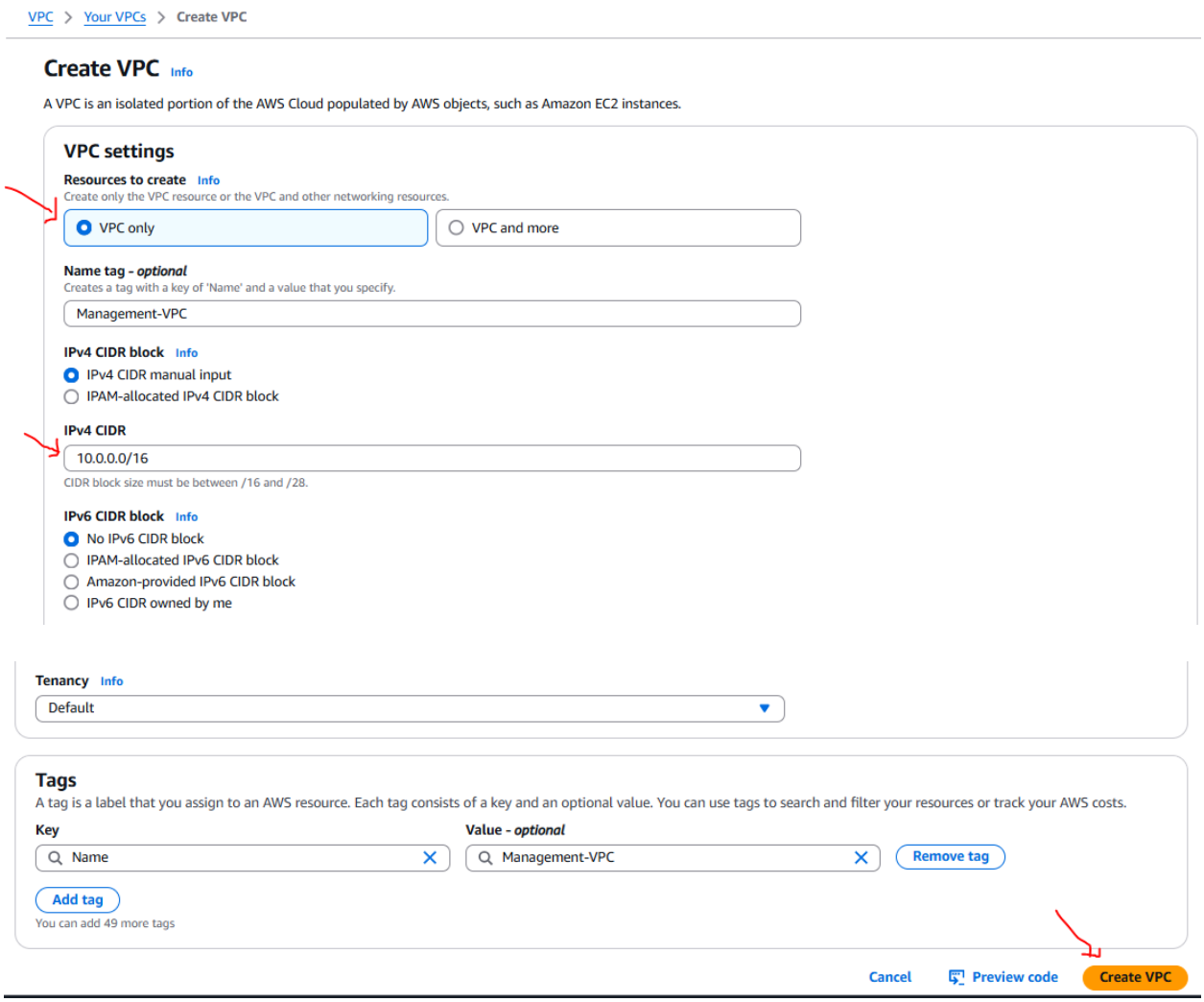
Creating separate VPCs for management and application layers
Establishing VPC Peering connections with controlled route table propagation
Implementing strict security group to enforce least privilege access
Monitoring and validating traffic flows using VPC Flow Logs

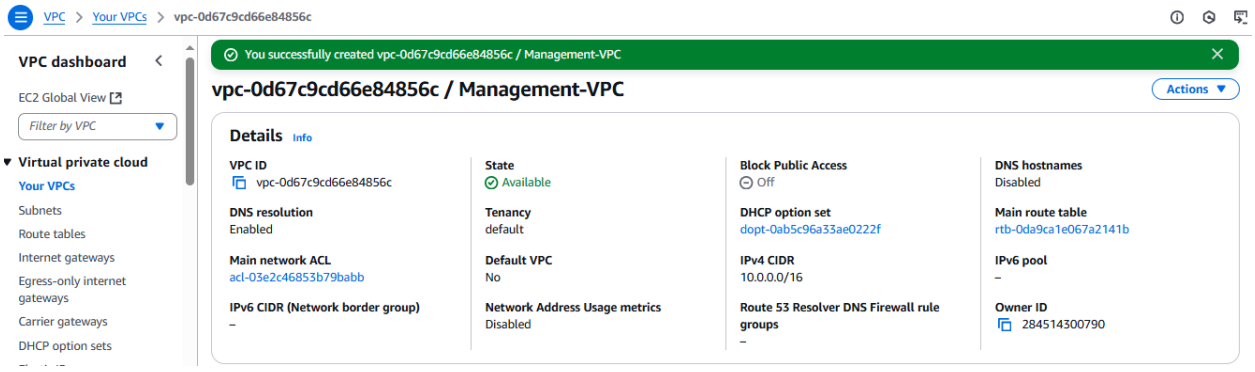
Goal:
Create two VPCs:
VPC-A (Management VPC)
VPC-B (Application VPC)
Then, establish a VPC Peering Connection between them to allow controlled communication, maintaining traffic separation.

Implementation Steps
Step 1: Create VPC-A (Management VPC)

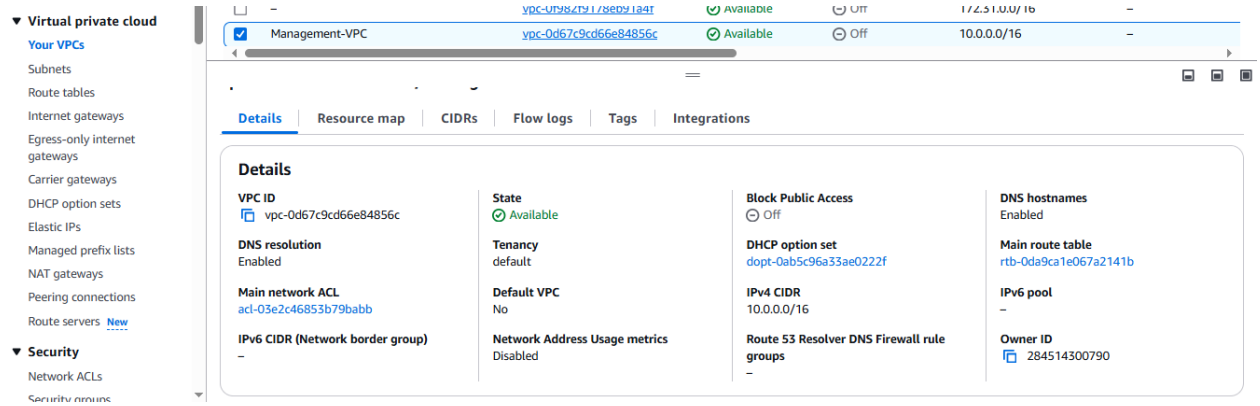
1. In the AWS Console, Go to **VPC Console → Your VPCs → Create VPC**
2. Choose **VPC only**
3. Fill in:
    - **Name tag**: Management-VPC
    - **IPv4 CIDR block**: 10.0.0.0/16
    - Leave the rest default
4. Click **Create VPC**




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.
Management-VPC
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
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
Name
Value - optional
Management-VPC
Remove tag
Add tag
You can add 49 more tags
Cancel
Preview code
Create VPC

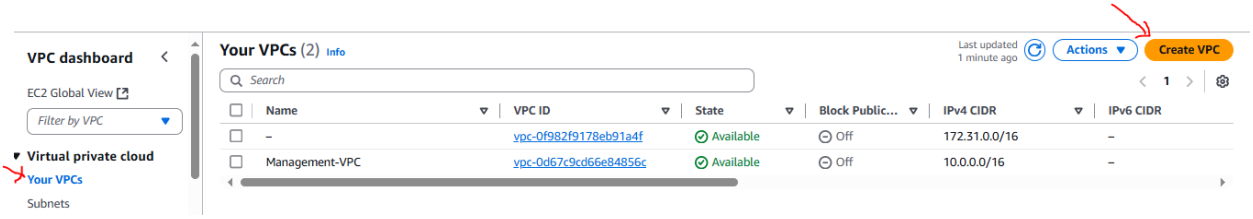

VPC > Your VPCs > vpc-0d67c9cd66e84856c
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
You successfully created vpc-0d67c9cd66e84856c / Management-VPC
vpc-0d67c9cd66e84856c / Management-VPC
Actions
Details Info
VPC ID
vpc-0d67c9cd66e84856c
State
Available
Block Public Access
Off
DNS hostnames
Disabled
DNS resolution
Enabled
Tenancy
default
DHCP option set
dopt-0ab5c96a33ae0222f
Main route table
rtb-0da9ca1e067a2141b
Main network ACL
acl-03e2c46853b79babb
Default VPC
No
IPv4 CIDR
10.0.0.0/16
IPv6 pool
–
IPv6 CIDR (Network border group)
–
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
–
Owner ID
284514300790

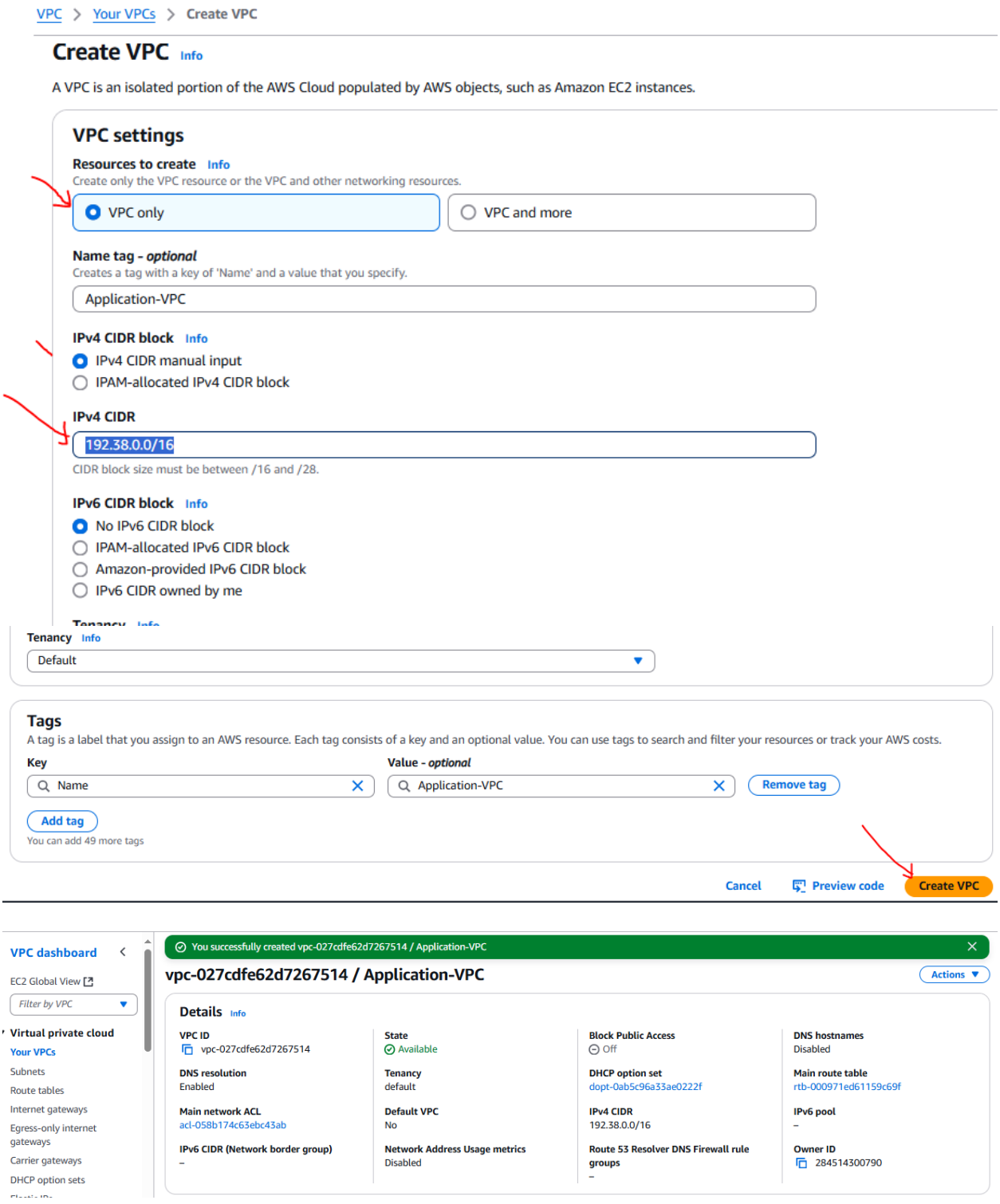
- From the Management-VPC Actions drop down, select Edit VPC settings and Enable DNS hostnames in DNS Settings



Step 2: Create VPC-B (Application VPC)

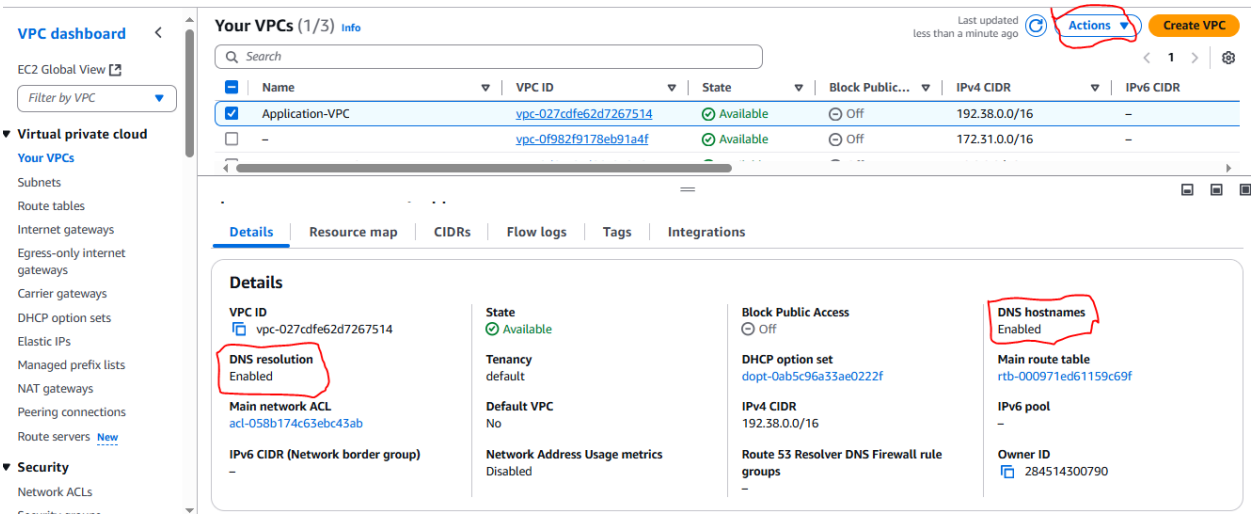
1. Go to **VPC Console → Your VPCs → Create VPC**
2. Choose **VPC only**
3. Fill in:
    - **Name tag**: Application-VPC
    - **IPv4 CIDR block**: 192.38.0.0/16
    - Keep default settings
4. Click **Create VPC**




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.
Application-VPC
IPv4 CIDR block Info
IPv4 CIDR manual input
IPAM-allocated IPv4 CIDR block
IPv4 CIDR
192.38.0.0/16
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
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
Name
Value - optional
Application-VPC
Remove tag
Add tag
You can add 49 more tags
Cancel
Preview code
Create VPC

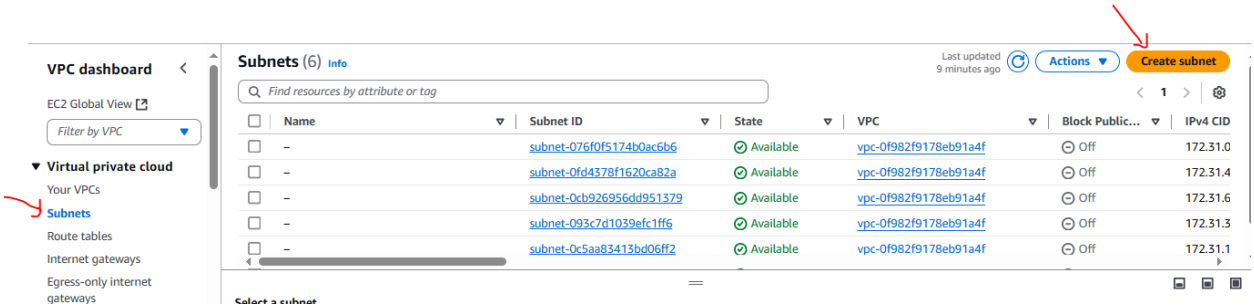
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
You successfully created vpc-027cdfe62d7267514 / Application-VPC
vpc-027cdfe62d7267514 / Application-VPC
Actions
Details Info
VPC ID
vpc-027cdfe62d7267514
State
Available
Block Public Access
Off
DNS hostnames
Disabled
DNS resolution
Enabled
Tenancy
default
DHCP option set
dopt-0ab5c96a33ae0222f
Main route table
rtb-000971ed61159c69f
Main network ACL
acl-058b174c63ebc43ab
Default VPC
No
IPv4 CIDR
192.38.0.0/16
IPv6 pool
–
IPv6 CIDR (Network border group)
–
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
–
Owner ID
284514300790

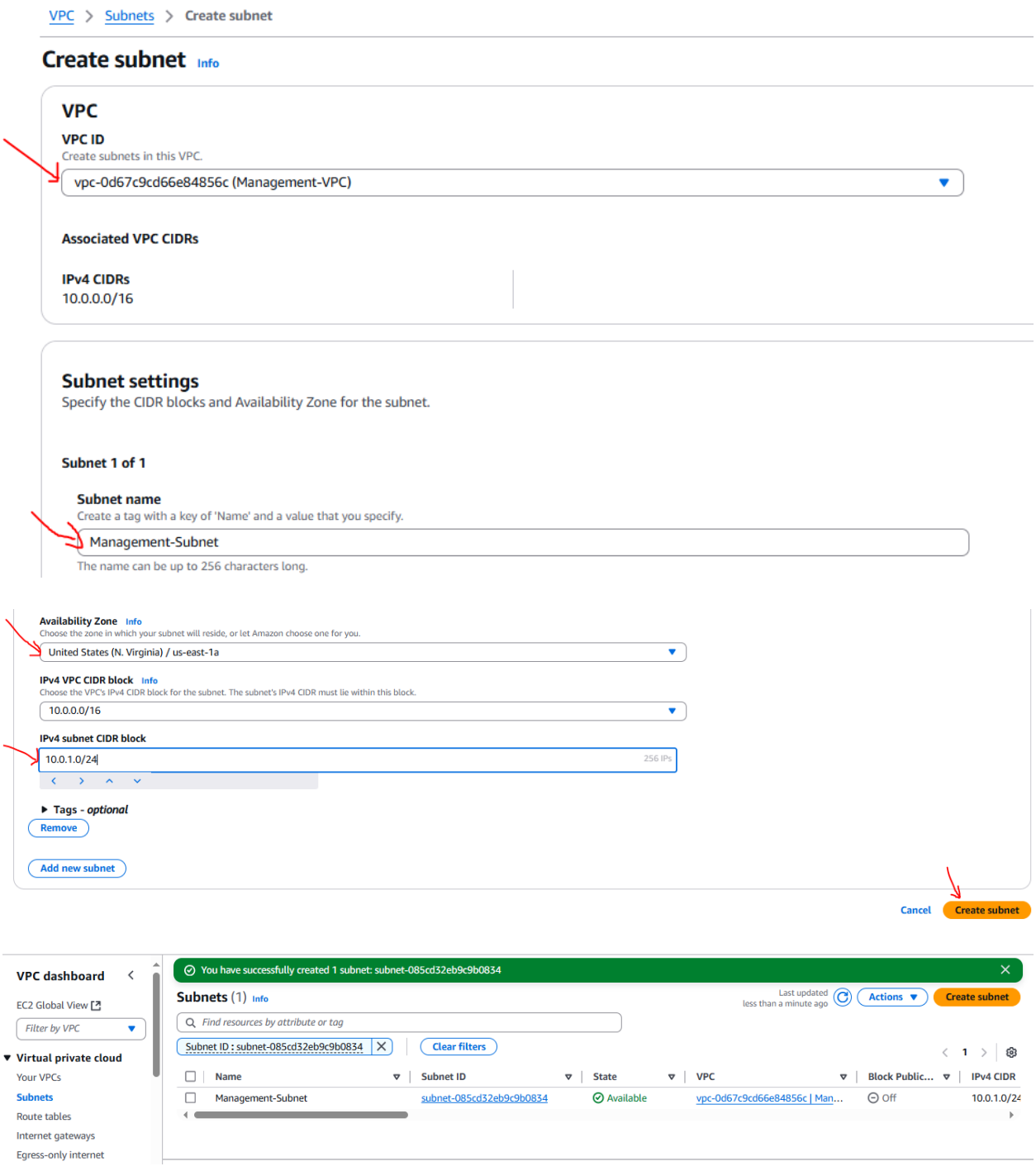
- From the Application-VPC Actions drop down, select Edit VPC settings and Enable DNS hostnames in DNS Settings



Step 3: Create Subnets in Each VPC

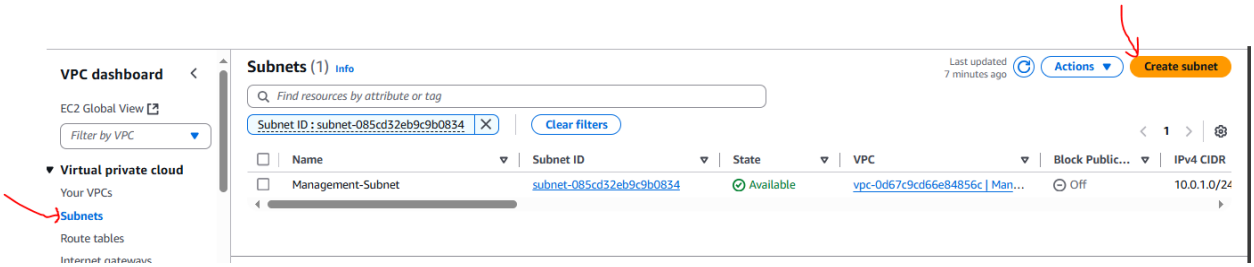
1. In the VPC Dashboard Go to **Subnets → Create Subnet**
2. Select Management-VPC
    - Name: Management-Subnet
    - AZ: Choose us-east-1a
    - CIDR block: 10.0.1.0/24

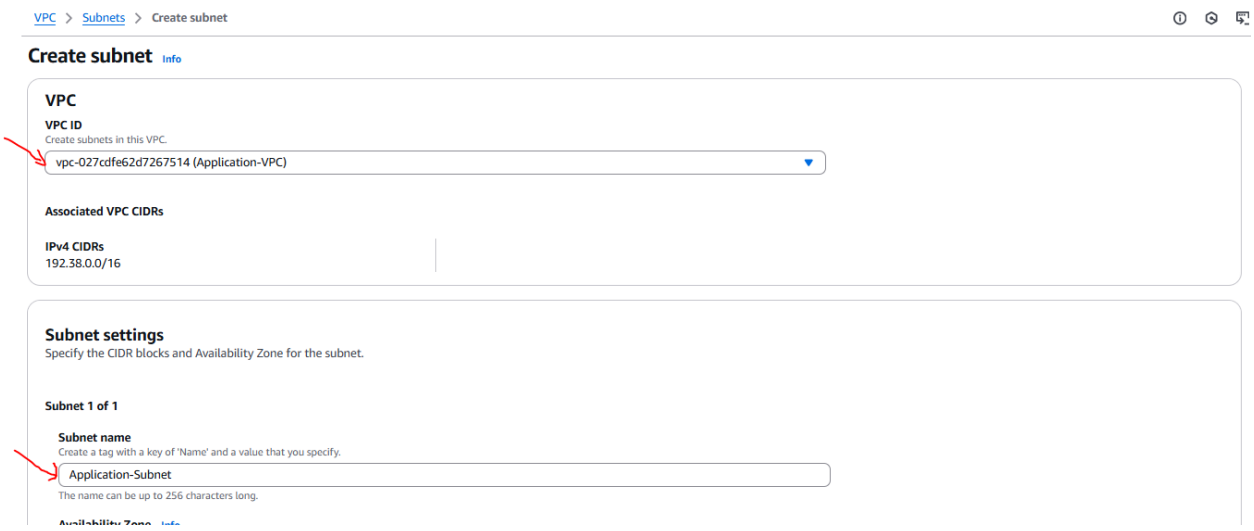


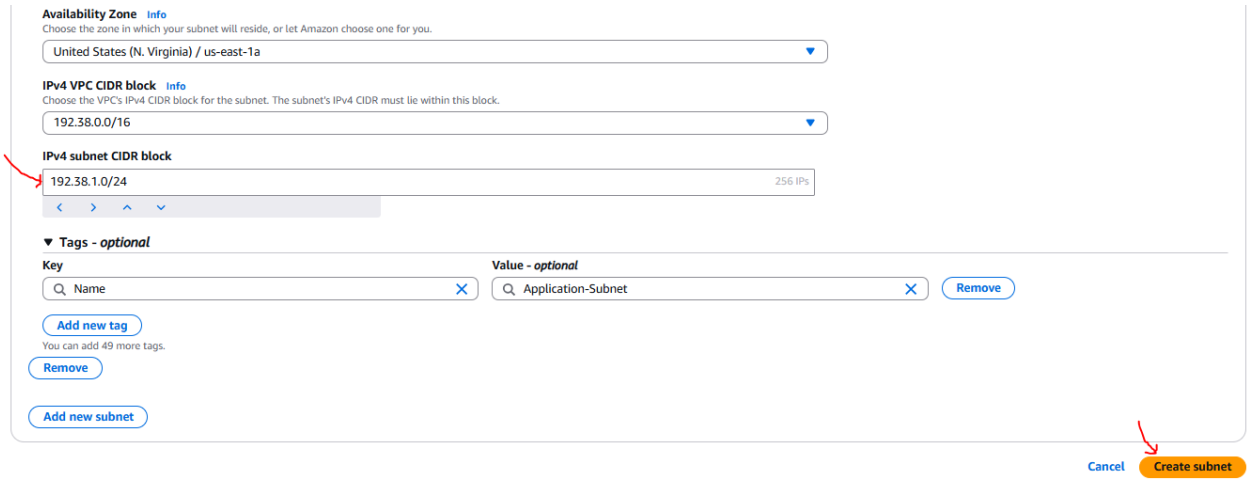


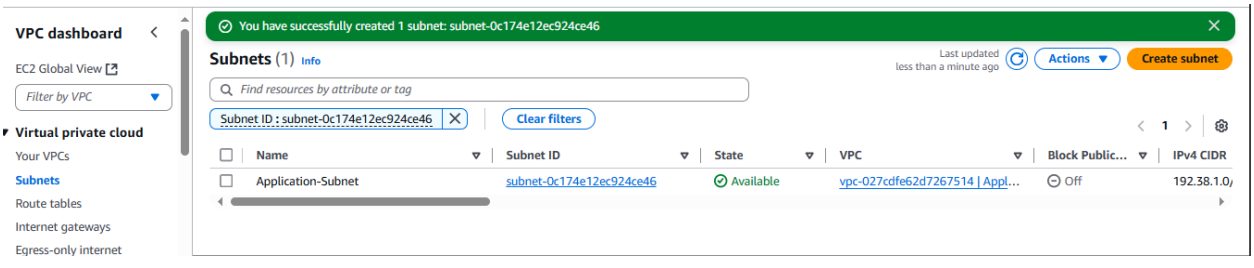
3. Create the subnet for Application-VPC

   - Name: Application-Subnet
   - AZ: Choose us-east-1a
   - CIDR block: 192.38.1.0/24


VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Subnets (1) Info
Find resources by attribute or tag
Subnet ID : subnet-085cd32eb9c9b0834
Clear filters
Last updated 7 minutes ago
Actions
Create subnet
Name
Subnet ID
State
VPC
Block Public...
IPv4 CIDR
Management-Subnet
subnet-085cd32eb9c9b0834
Available
vpc-0d67c9cd66e84856c | Man...
Off
10.0.1.0/24


VPC > Subnets > Create subnet
Create subnet Info
VPC
VPC ID
Create subnets in this VPC.
vpc-027cdfe62d7267514 (Application-VPC)
Associated VPC CIDRs
IPv4 CIDRs
192.38.0.0/16
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.
Application-Subnet
The name can be up to 256 characters long.

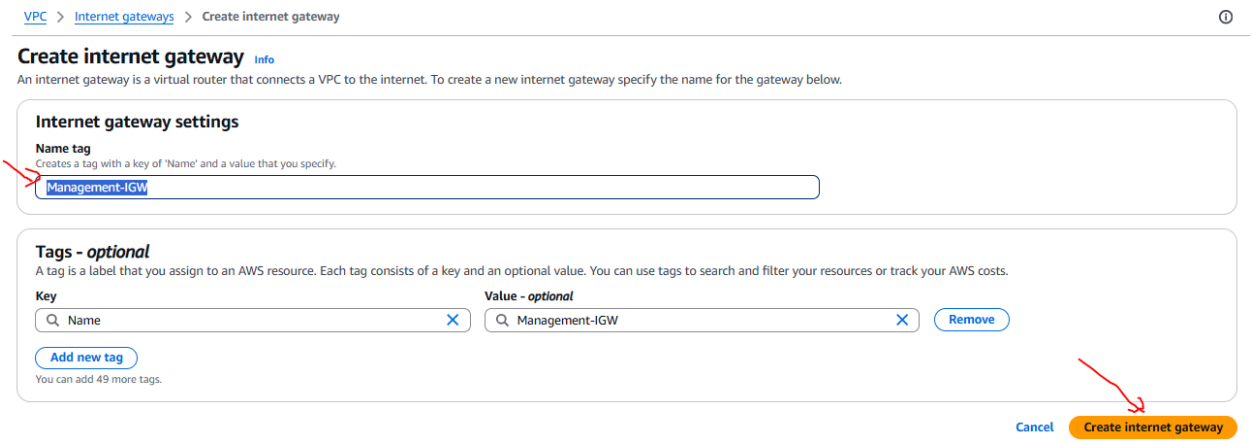

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / us-east-1a
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
192.38.0.0/16
IPv4 subnet CIDR block
192.38.1.0/24
256 IPs
Tags - optional
Key
Value - optional
Name
Application-Subnet
Remove
Add new tag
You can add 49 more tags.
Remove
Add new subnet
Cancel
Create subnet

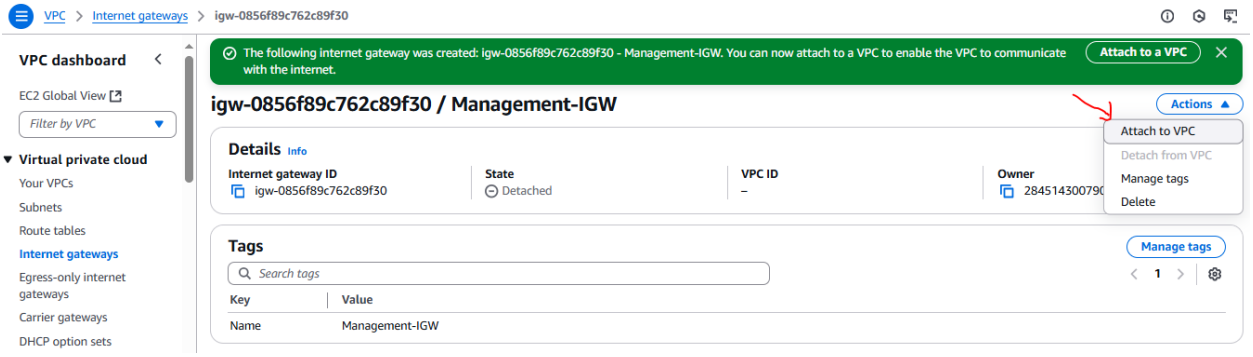

VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet
You have successfully created 1 subnet: subnet-0c174e12ec924ce46
Subnets (1) Info
Find resources by attribute or tag
Subnet ID : subnet-0c174e12ec924ce46
Clear filters
Last updated less than a minute ago
Actions
Create subnet
Name
Subnet ID
State
VPC
Block Public...
IPv4 CIDR
Application-Subnet
subnet-0c174e12ec924ce46
Available
vpc-027cdfe62d7267514 | Appl...
Off
192.38.1.0/

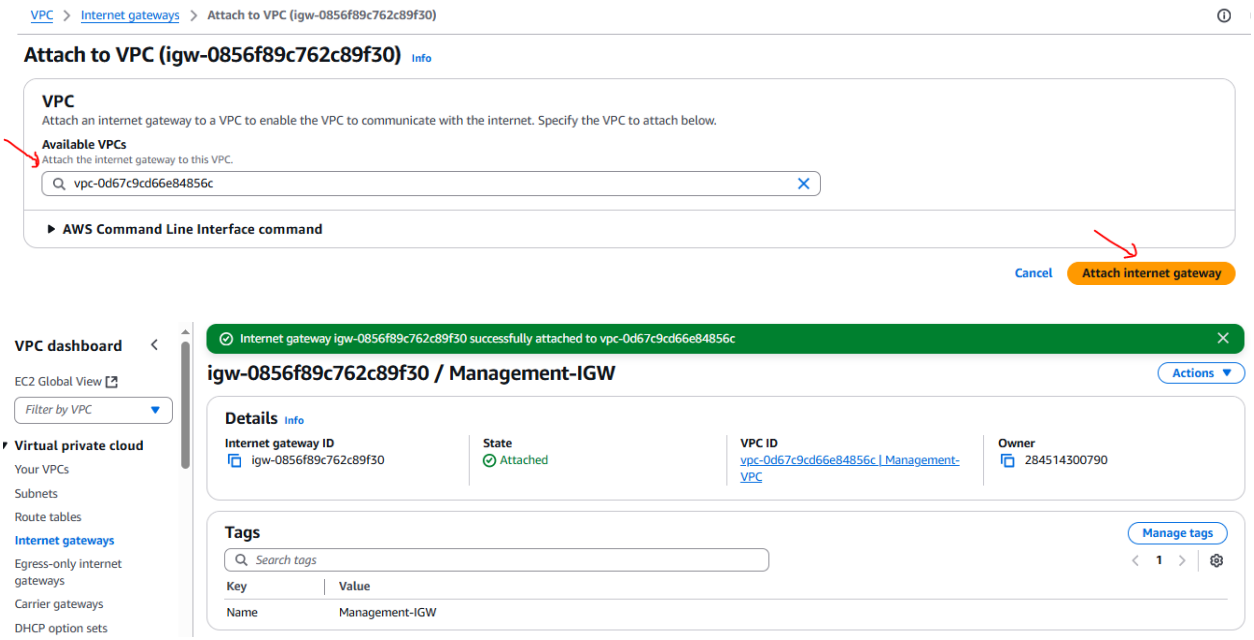
Step 4: Create Internet Gateways

1. Go to **Internet Gateways → Create Internet Gateway**
2. Name: Management-IGW, click on Create internet gateway
3. From the Actions drop down choose Attach to VPC and select Management-VPC
4. Repeat the above three steps for Application-VPC

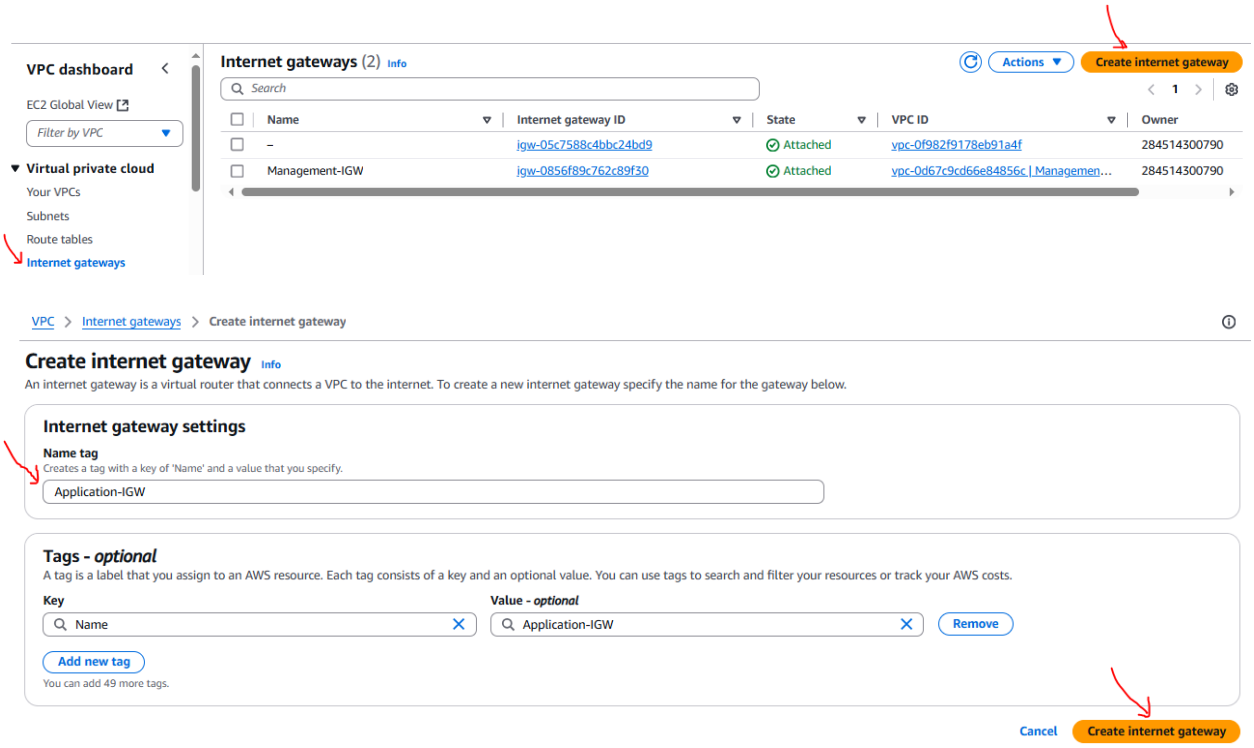
Internet Gateway (Management-IGW) for Management-VPC

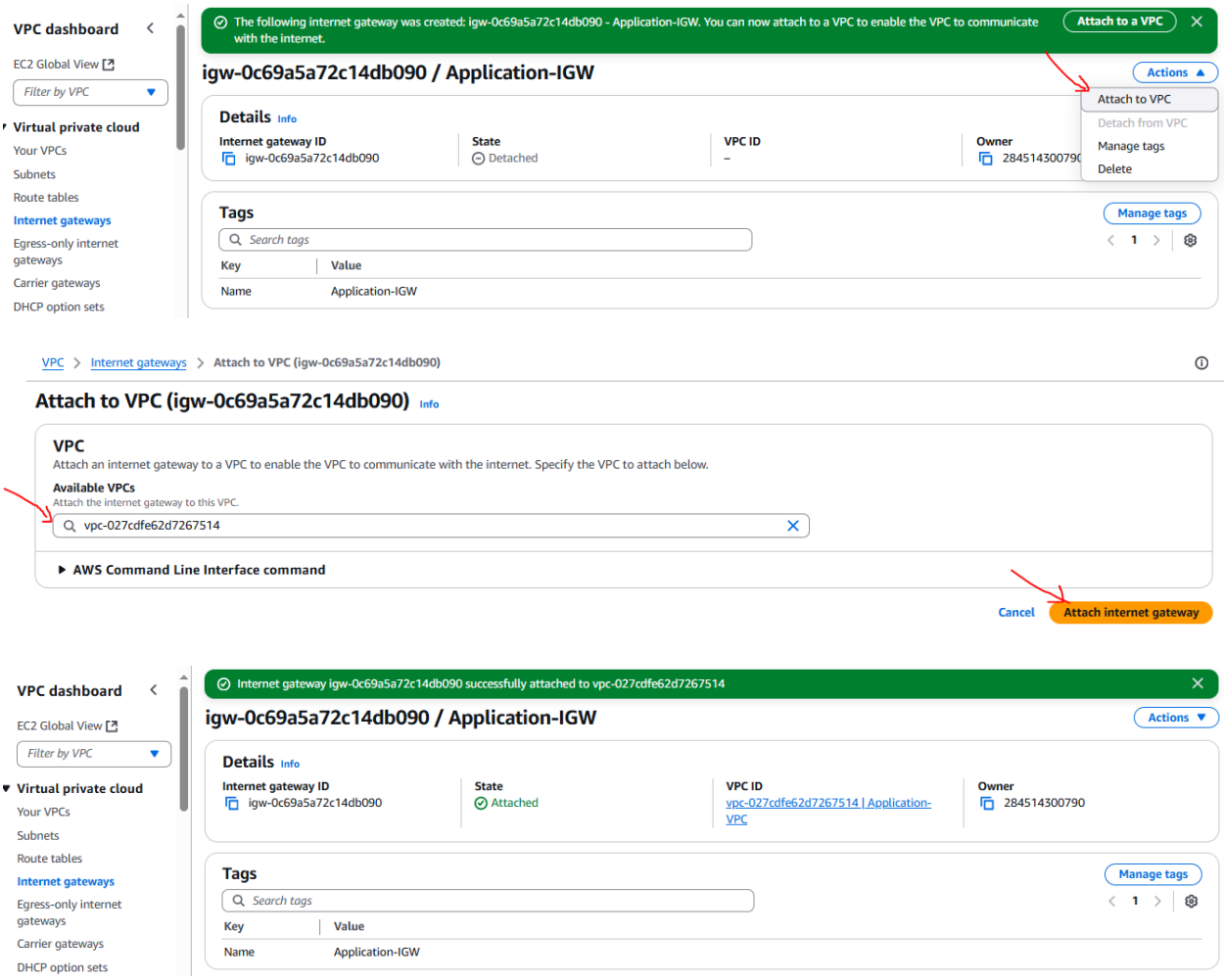






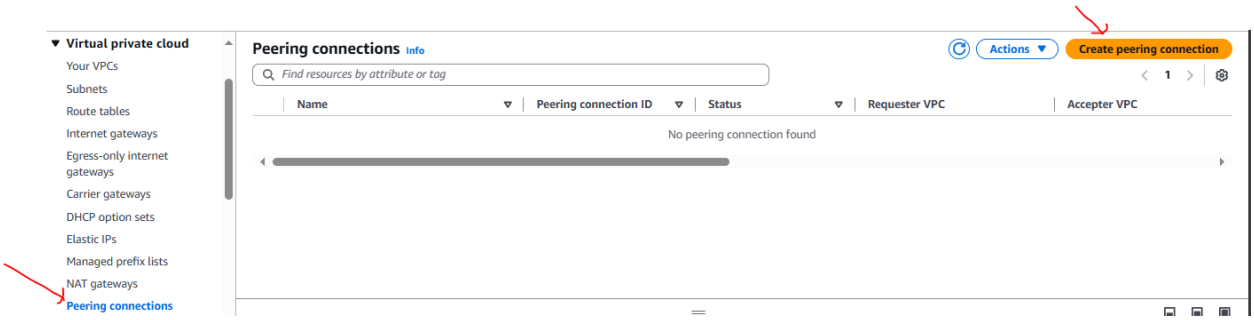
Internet Gateway (Application-IGW) for Application-VPC

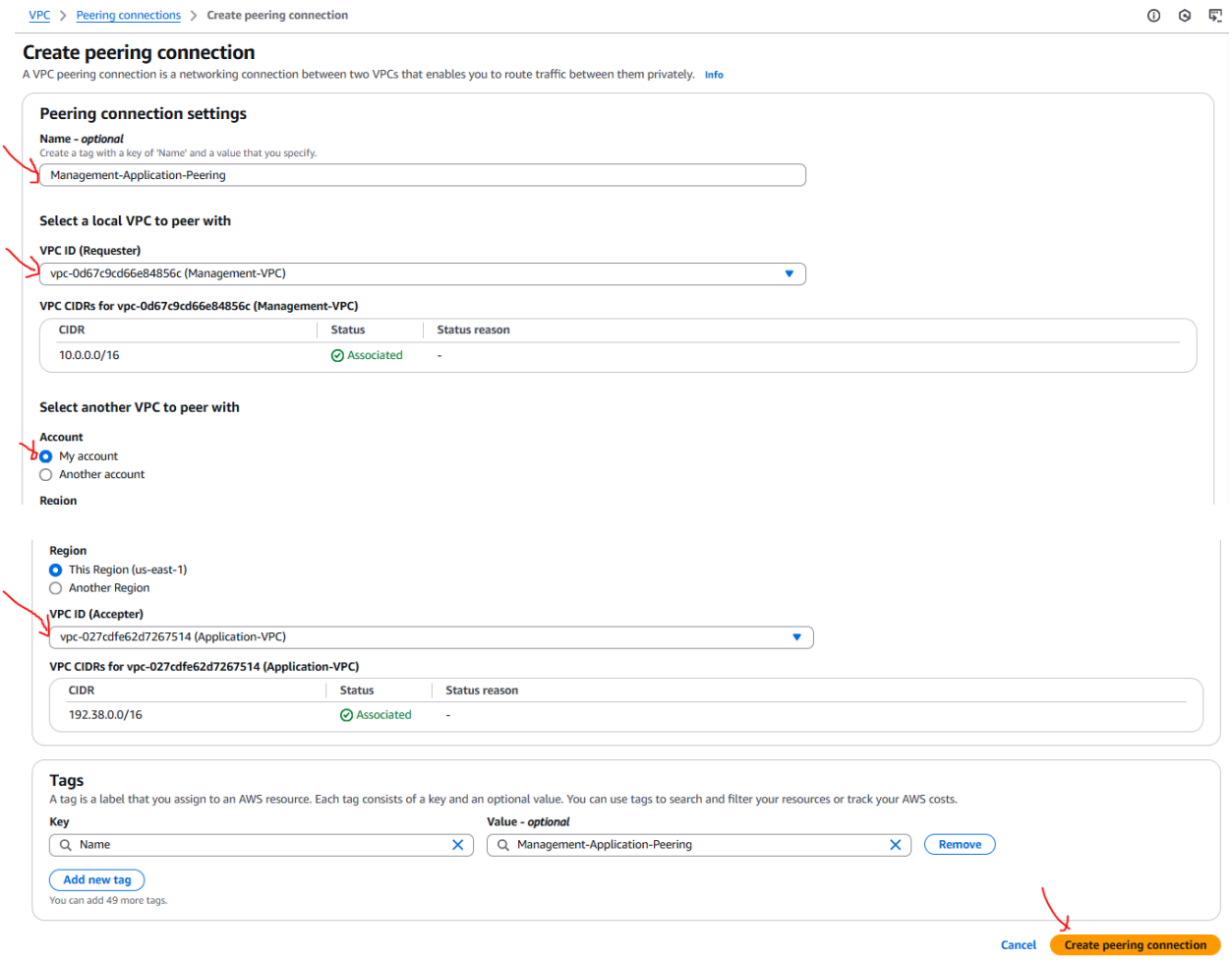


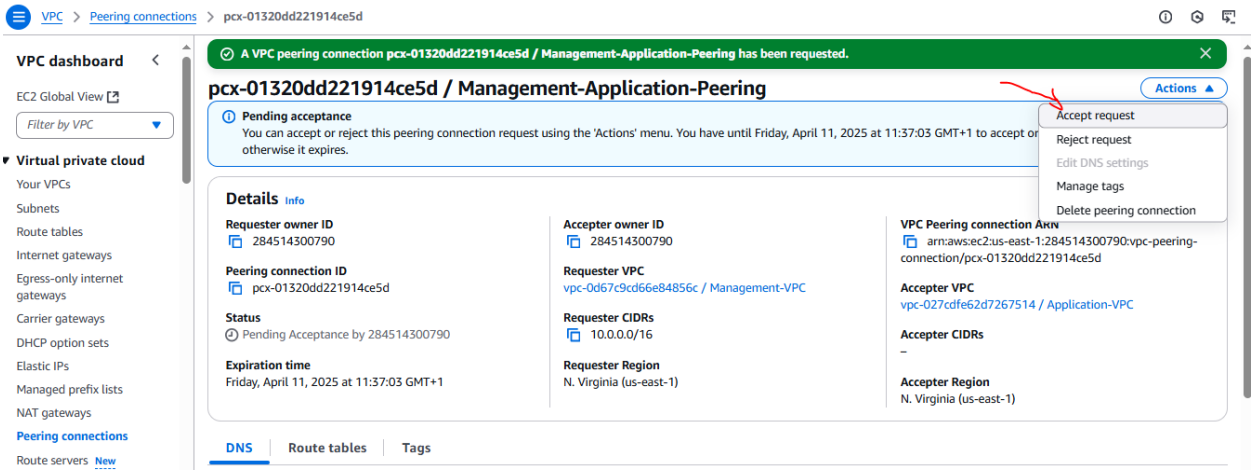


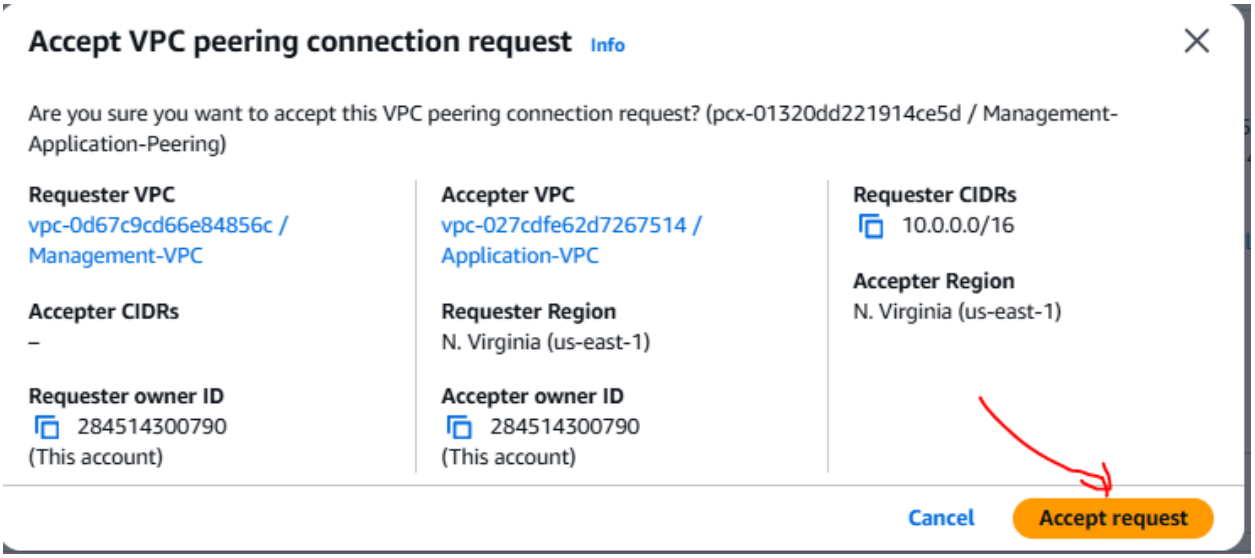
Step 5: Create VPC Peering Connection

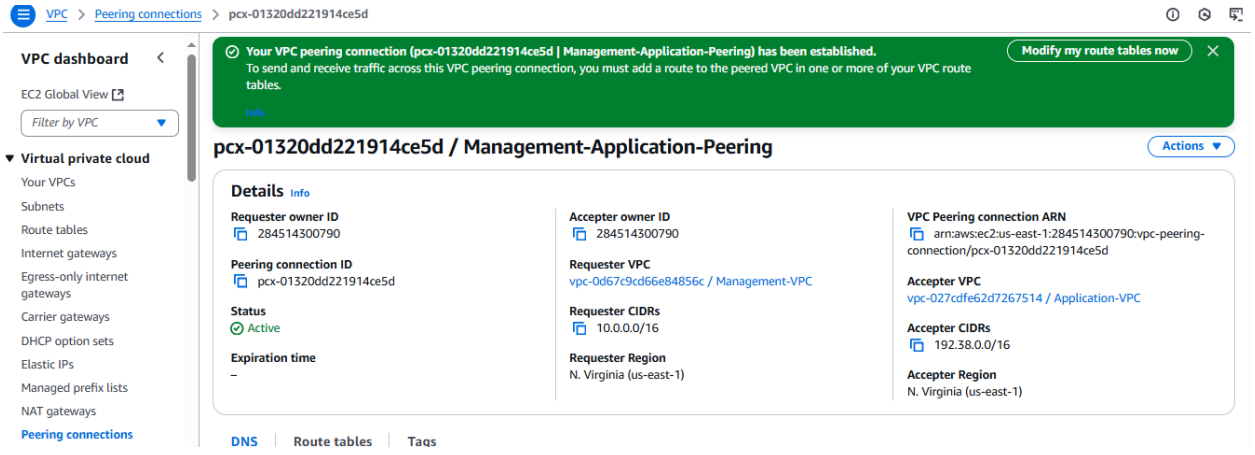
1. In the VPC Dashboard, Go to **Peering Connections → Create Peering Connection**
2. Name tag: Management-Application-Peering
3. Requester VPC: Management-VPC
4. Accepter VPC: Application-VPC (same account)
5. Click **Create Peering Connection**
6. Go back → Select the connection → Click **Actions → Accept request**

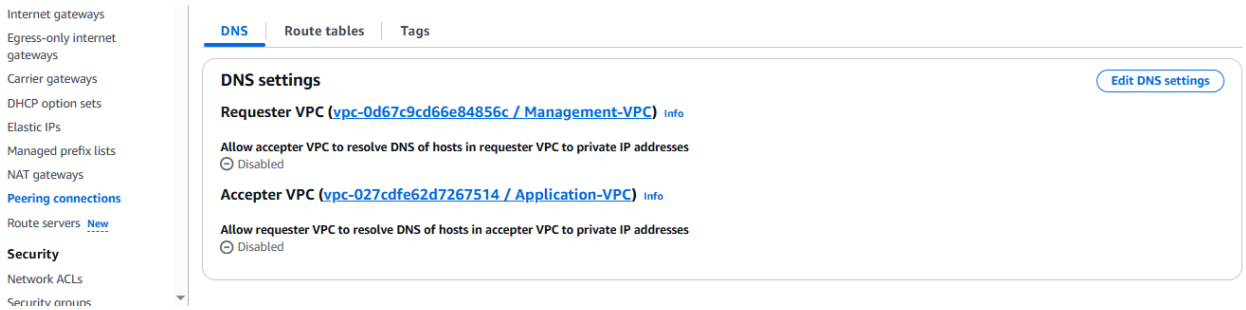

Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Peering connections Info
Actions
Create peering connection
Find resources by attribute or tag
Name
Peering connection ID
Status
Requester VPC
Accepter VPC
No peering connection found

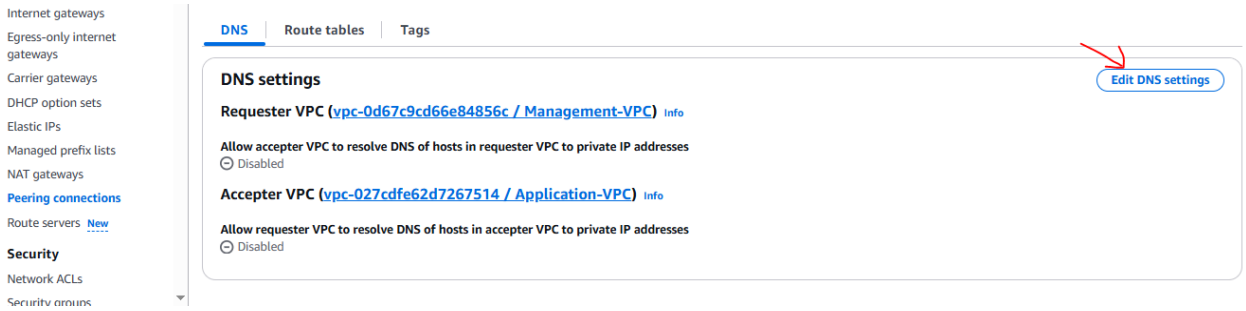

VPC > Peering connections > Create peering connection
Create peering connection
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Info
Peering connection settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
Management-Application-Peering
Select a local VPC to peer with
VPC ID (Requester)
vpc-0d67c9cd66e84856c (Management-VPC)
VPC CIDRs for vpc-0d67c9cd66e84856c (Management-VPC)
CIDR
Status
Status reason
10.0.0.0/16
Associated
-
Select another VPC to peer with
Account
My account
Another account
Region
Region
This Region (us-east-1)
Another Region
VPC ID (Accepter)
vpc-027cdfe62d7267514 (Application-VPC)
VPC CIDRs for vpc-027cdfe62d7267514 (Application-VPC)
CIDR
Status
Status reason
192.38.0.0/16
Associated
-
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
Management-Application-Peering
Remove
Add new tag
You can add 49 more tags.
Cancel
Create peering connection

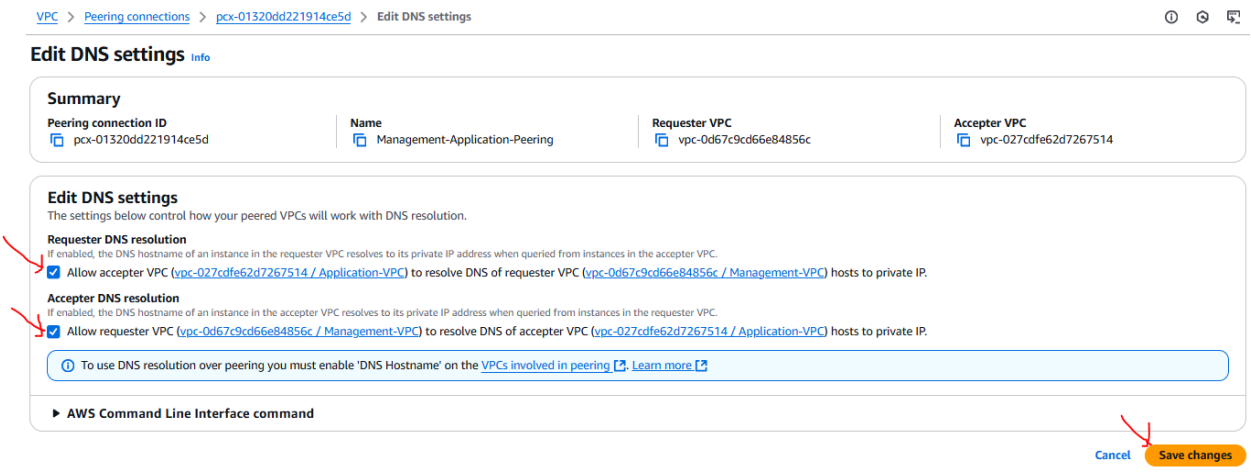

VPC > Peering connections > pcx-01320dd221914ce5d
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New
A VPC peering connection pcx-01320dd221914ce5d / Management-Application-Peering has been requested.
pcx-01320dd221914ce5d / Management-Application-Peering
Actions
Accept request
Reject request
Edit DNS settings
Manage tags
Delete peering connection
Pending acceptance
You can accept or reject this peering connection request using the 'Actions' menu. You have until Friday, April 11, 2025 at 11:37:03 GMT+1 to accept or
otherwise it expires.
Details Info
Requester owner ID
284514300790
Peering connection ID
pcx-01320dd221914ce5d
Status
Pending Acceptance by 284514300790
Expiration time
Friday, April 11, 2025 at 11:37:03 GMT+1
Accepter owner ID
284514300790
Requester VPC
vpc-0d67c9cd66e84856c / Management-VPC
Requester CIDRs
10.0.0.0/16
Requester Region
N. Virginia (us-east-1)
VPC Peering connection ARN
arn:aws:ec2:us-east-1:284514300790:vpc-peering-connection/pcx-01320dd221914ce5d
Accepter VPC
vpc-027cdfe62d7267514 / Application-VPC
Accepter CIDRs
–
Accepter Region
N. Virginia (us-east-1)
DNS
Route tables
Tags

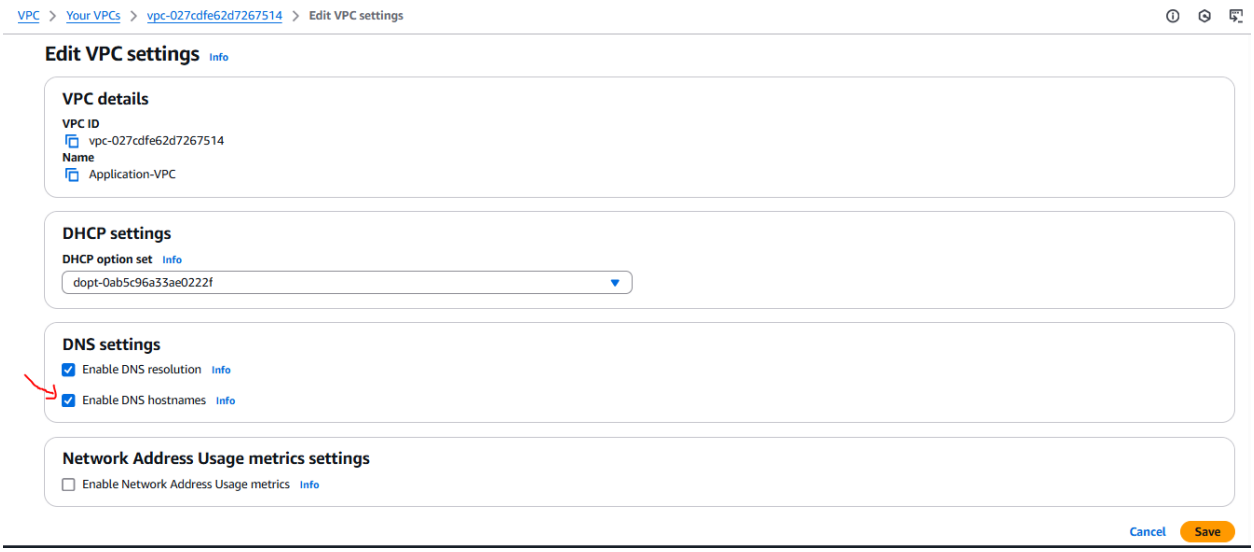

Accept VPC peering connection request Info
Are you sure you want to accept this VPC peering connection request? (pcx-01320dd221914ce5d / Management-Application-Peering)
Requester VPC
vpc-0d67c9cd66e84856c / Management-VPC
Accepter CIDRs
–
Requester owner ID
284514300790
(This account)
Accepter VPC
vpc-027cdfe62d7267514 / Application-VPC
Requester Region
N. Virginia (us-east-1)
Accepter owner ID
284514300790
(This account)
Requester CIDRs
10.0.0.0/16
Accepter Region
N. Virginia (us-east-1)
Cancel
Accept request

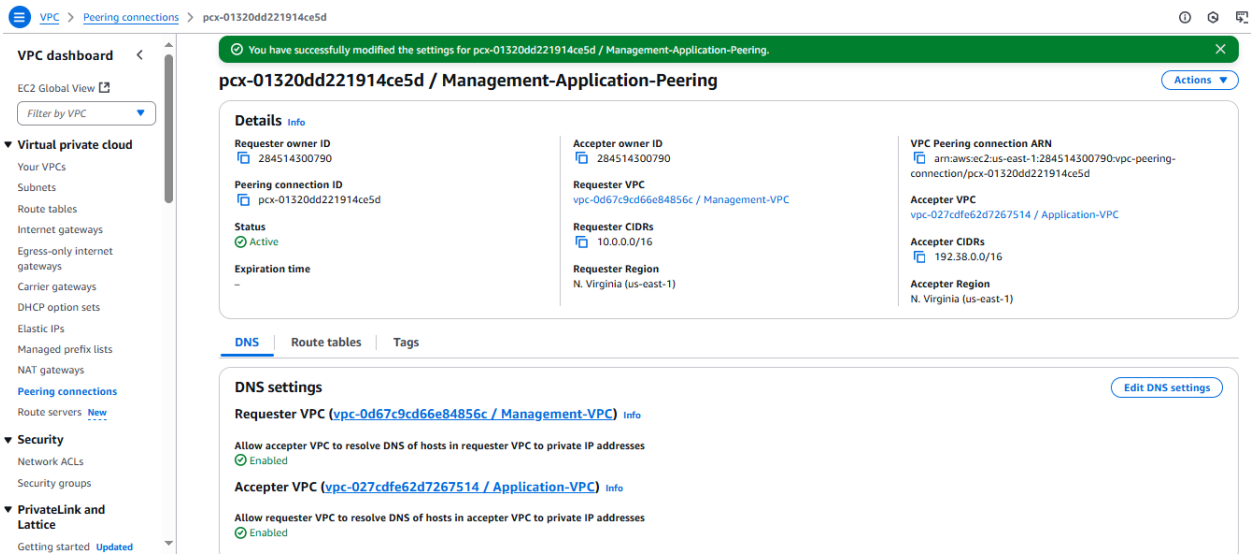

VPC > Peering connections > pcx-01320dd221914ce5d
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Your VPC peering connection (pcx-01320dd221914ce5d | Management-Application-Peering) has been established.
To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables.
Info
Modify my route tables now
pcx-01320dd221914ce5d / Management-Application-Peering
Actions
Details Info
Requester owner ID
284514300790
Peering connection ID
pcx-01320dd221914ce5d
Status
Active
Expiration time
–
Accepter owner ID
284514300790
Requester VPC
vpc-0d67c9cd66e84856c / Management-VPC
Requester CIDRs
10.0.0.0/16
Requester Region
N. Virginia (us-east-1)
VPC Peering connection ARN
arn:aws:ec2:us-east-1:284514300790:vpc-peering-connection/pcx-01320dd221914ce5d
Accepter VPC
vpc-027cdfe62d7267514 / Application-VPC
Accepter CIDRs
192.38.0.0/16
Accepter Region
N. Virginia (us-east-1)
DNS
Route tables
Tags


Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Security groups
DNS
Route tables
Tags
DNS settings
Edit DNS settings
Requester VPC (vpc-0d67c9cd66e84856c / Management-VPC) Info
Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses
Disabled
Accepter VPC (vpc-027cdfe62d7267514 / Application-VPC) Info
Allow requester VPC to resolve DNS of hosts in accepter VPC to private IP addresses
Disabled


Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Security groups
DNS
Route tables
Tags
DNS settings
Edit DNS settings
Requester VPC (vpc-0d67c9cd66e84856c / Management-VPC) Info
Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses
Disabled
Accepter VPC (vpc-027cdfe62d7267514 / Application-VPC) Info
Allow requester VPC to resolve DNS of hosts in accepter VPC to private IP addresses
Disabled

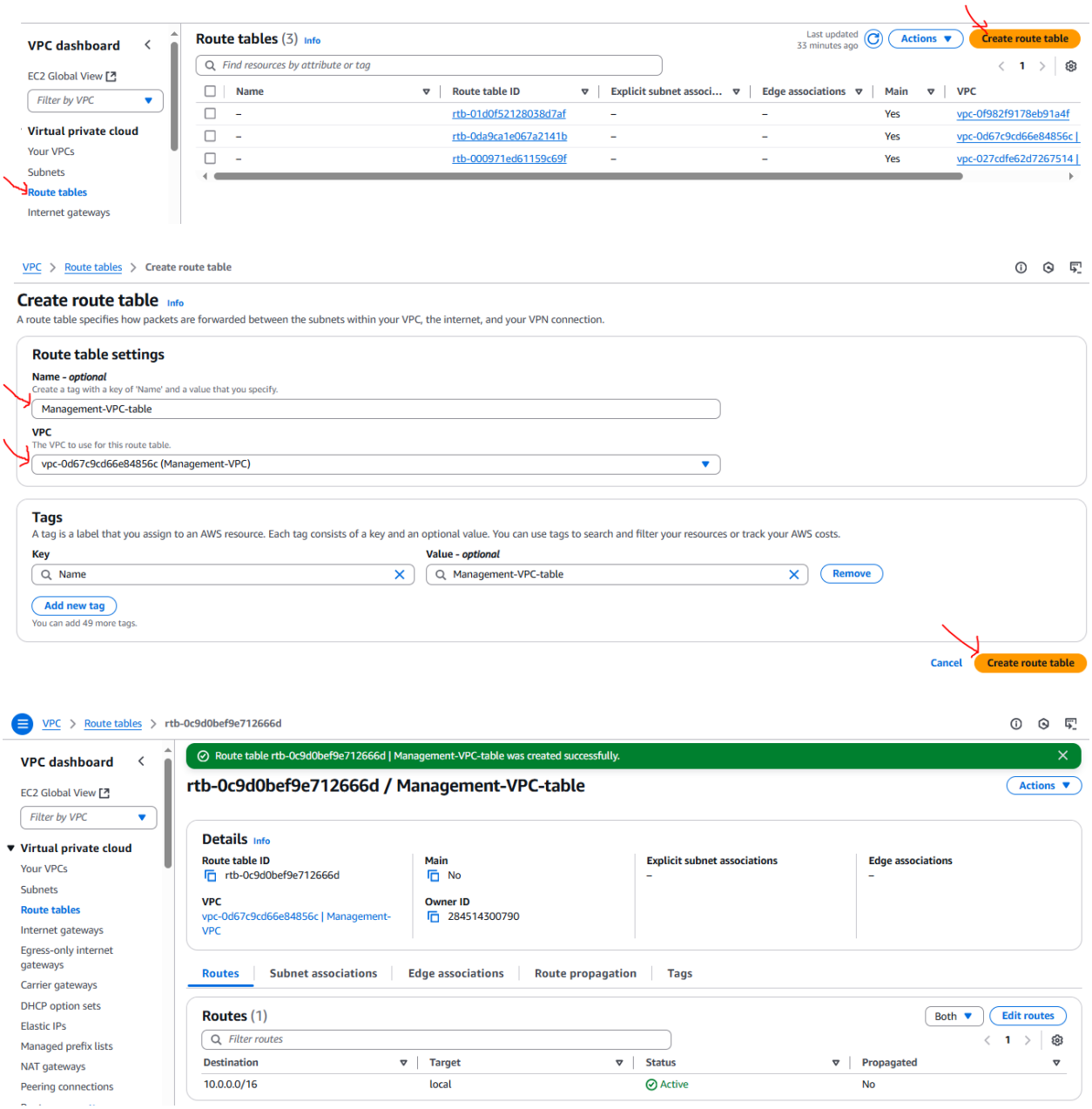

VPC > Peering connections > pcx-01320dd221914ce5d > Edit DNS settings
Edit DNS settings Info
Summary
Peering connection ID
pcx-01320dd221914ce5d
Name
Management-Application-Peering
Requester VPC
vpc-0d67c9cd66e84856c
Accepter VPC
vpc-027cdfe62d7267514
Edit DNS settings
The settings below control how your peered VPCs will work with DNS resolution.
Requester DNS resolution
If enabled, the DNS hostname of an instance in the requester VPC resolves to its private IP address when queried from instances in the accepter VPC.
Allow accepter VPC (vpc-027cdfe62d7267514 / Application-VPC) to resolve DNS of requester VPC (vpc-0d67c9cd66e84856c / Management-VPC) hosts to private IP.
Accepter DNS resolution
If enabled, the DNS hostname of an instance in the accepter VPC resolves to its private IP address when queried from instances in the requester VPC.
Allow requester VPC (vpc-0d67c9cd66e84856c / Management-VPC) to resolve DNS of accepter VPC (vpc-027cdfe62d7267514 / Application-VPC) hosts to private IP.
To use DNS resolution over peering you must enable 'DNS Hostname' on the VPCs involved in peering. Learn more
AWS Command Line Interface command
Cancel
Save changes





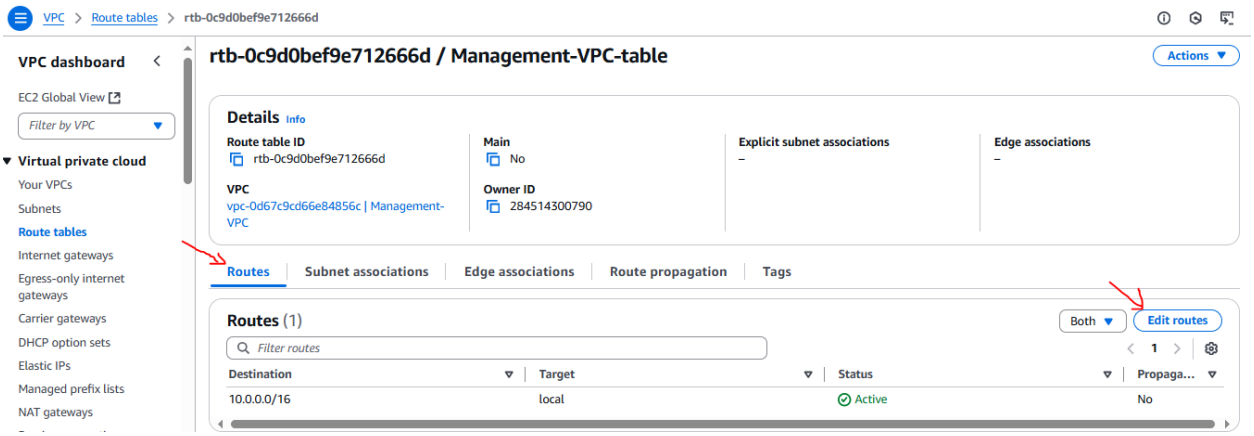
Step 6: Create Route tables

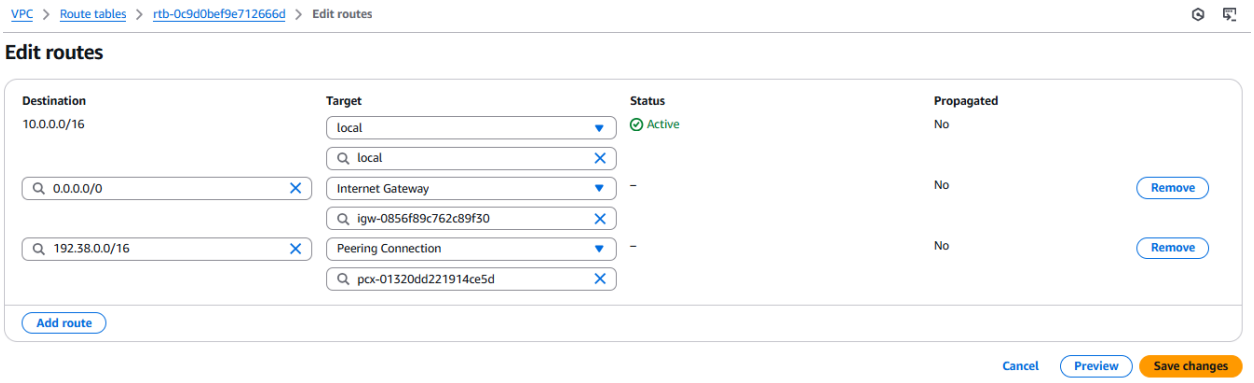
1. Navigate to VPC Dashboard, go to **Route tables** under the **Virtual Private Cloud** section
    - Click on Create route table button.
    - In the **Create Route Table** wizard:
        - **Name tag**: Management-VPC-table.
        - **VPC**: Select the Management-VPC from the dropdown list.
    - Click on **Create route table.**

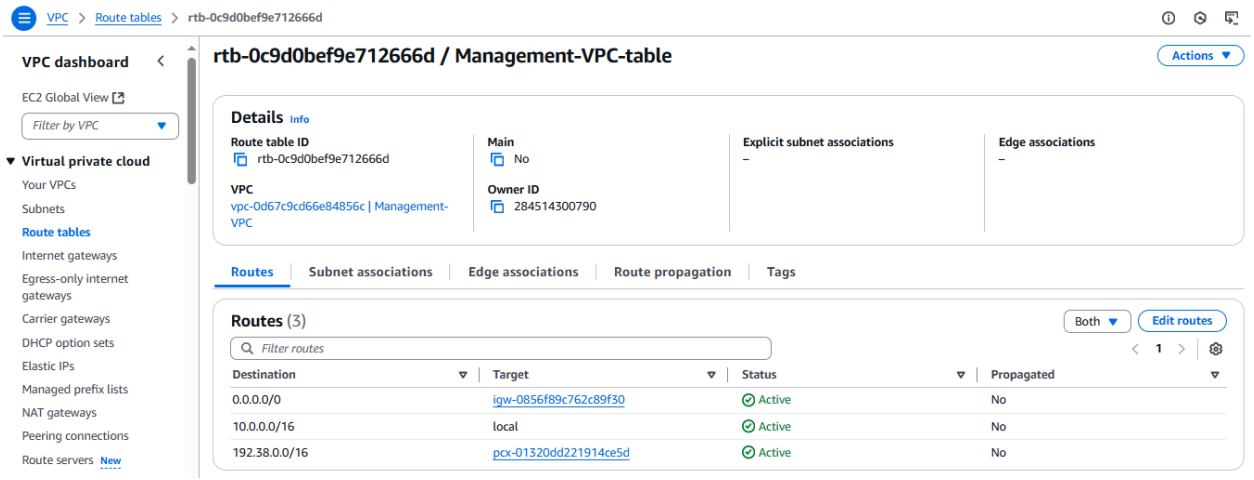


2. Add Routes to the Route Table

- Under the **Routes** tab, click **Edit routes** and then **Add route**.
- Specify the destination and target for the route. Common destinations include:
  - For local traffic within the VPC, the destination would be 0.0.0.0/0 (or a specific IP range for the network you wish to route).
  - To route traffic to the Internet Gateway (for internet-bound traffic), the target will be the **Internet Gateway** (igw-0856f89c762c89f30).
  - For VPC peering, choose the **VPC Peering Connection** as the target.
- After adding the desired routes, click **Save changes**.



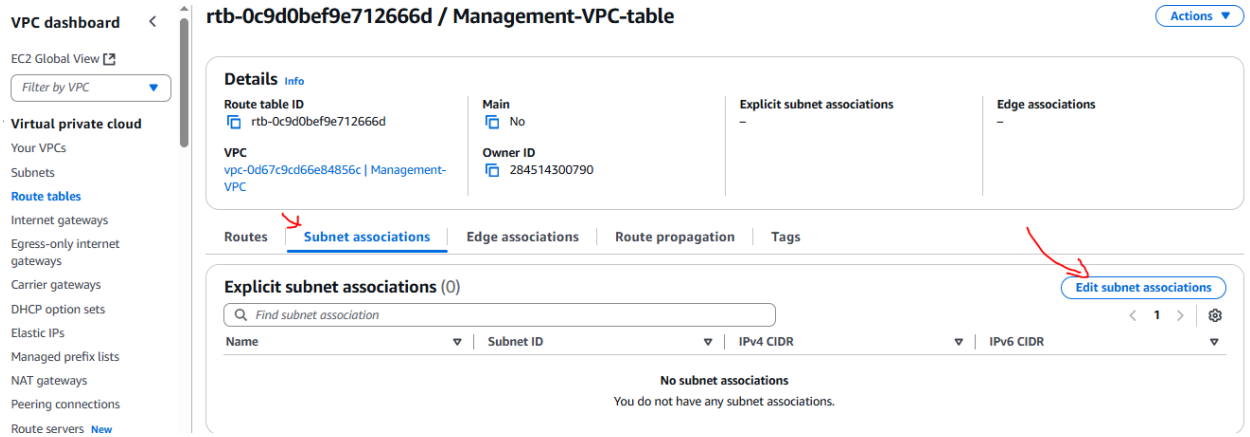


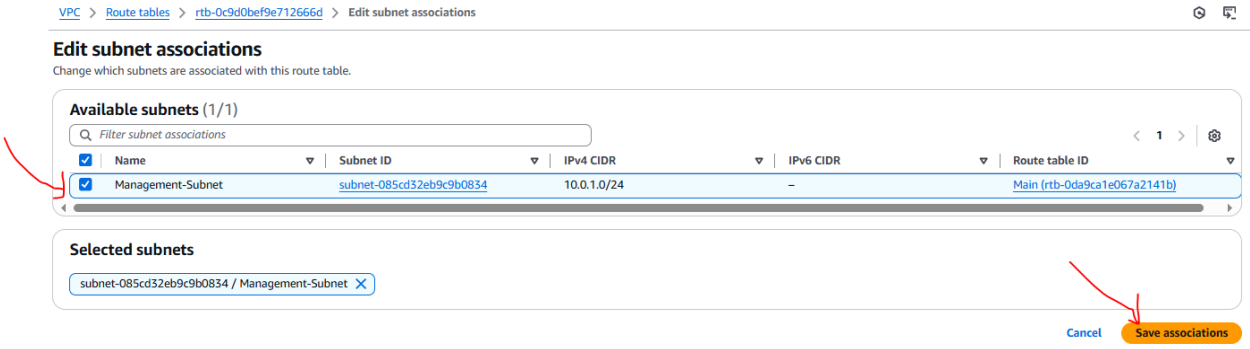


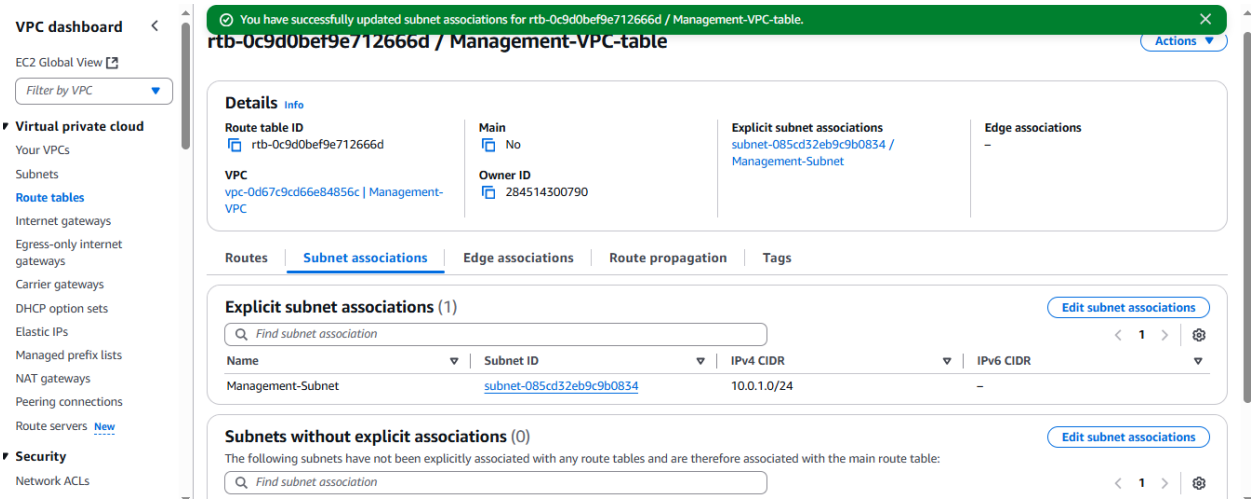
3. Associate the Route Table with a Subnet

- Go to the **Subnet associations** tab in the route table.
- Click **Edit subnet associations**.

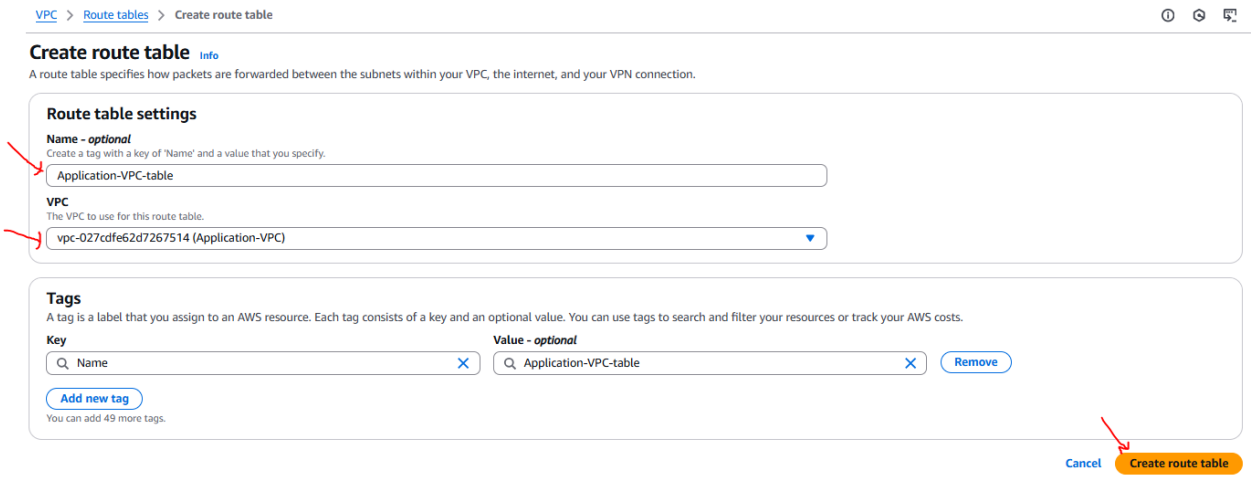
- Select the subnets that you want to associate with the route table. If you want a subnet to route traffic via this route table, select it from the list.
- Click **Save associations**.

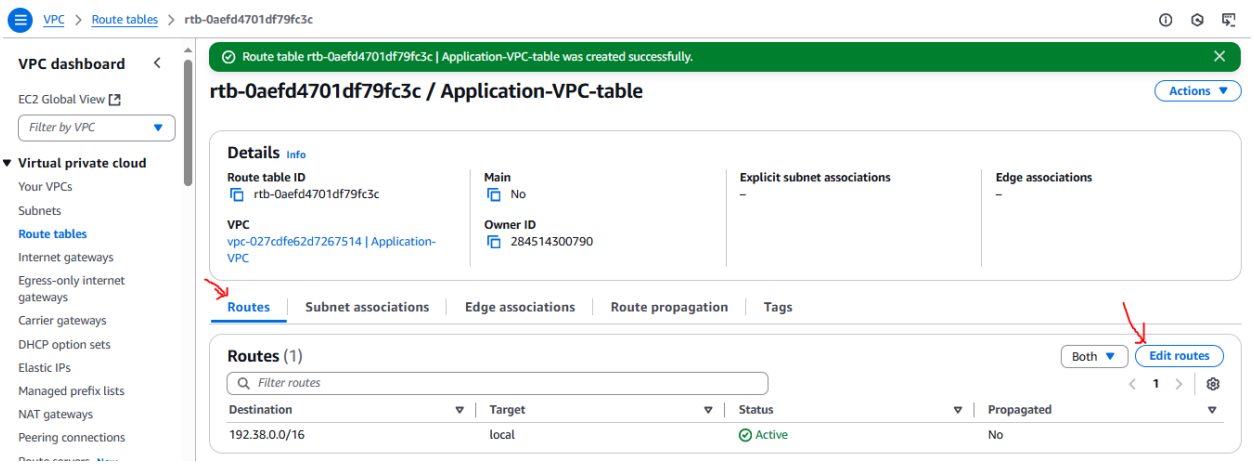


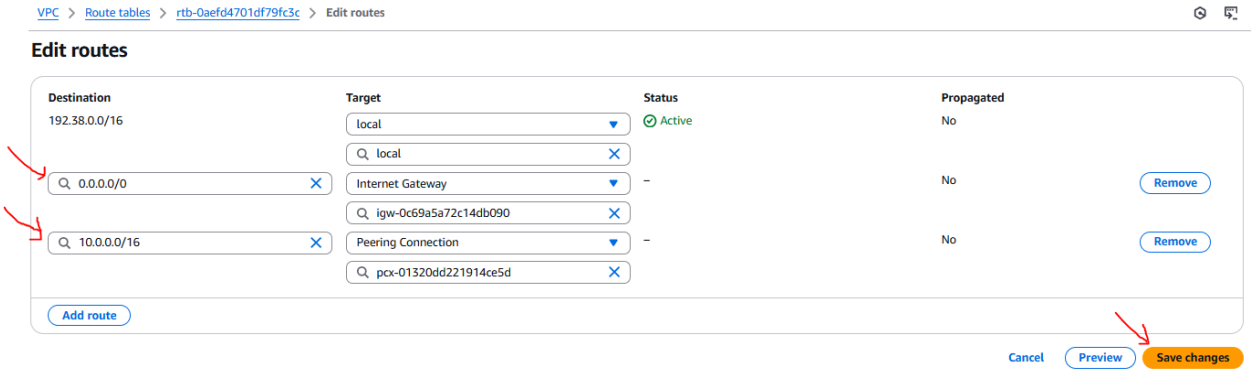


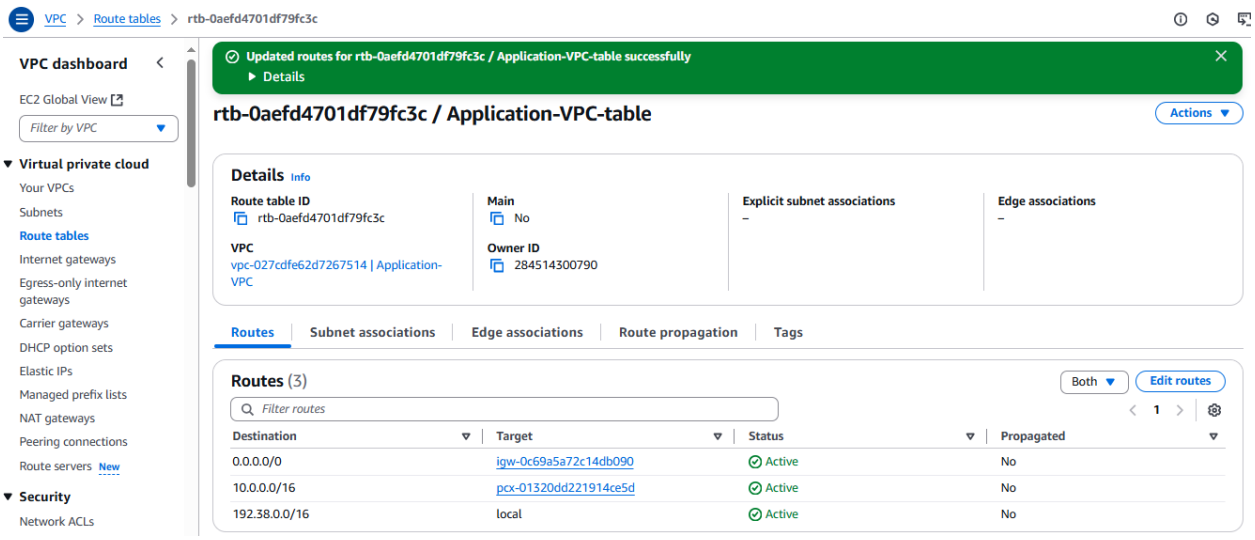


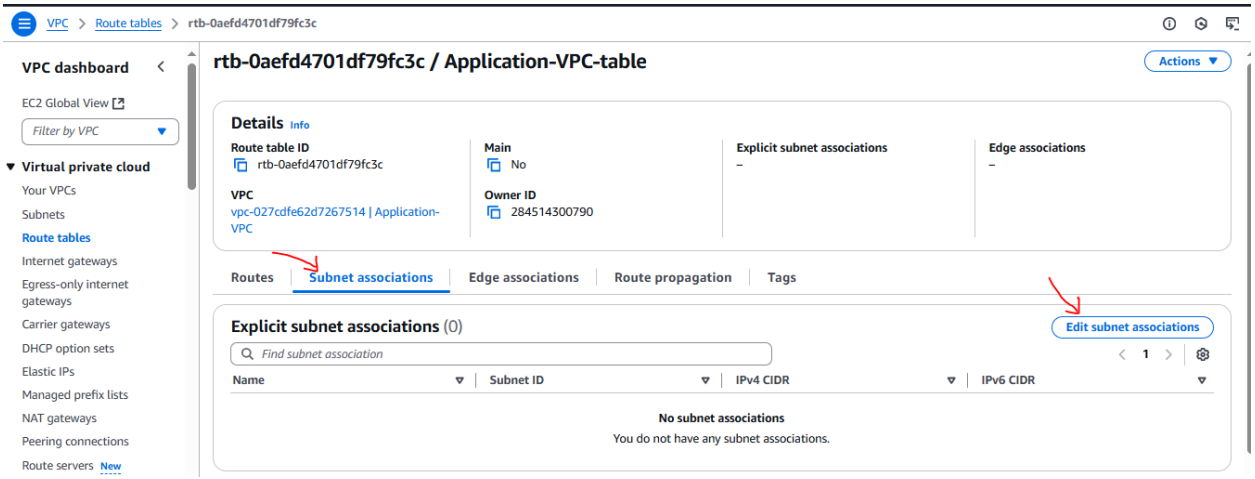
Repeat the above steps for creation of route table (Application-VPC-table) for Application-VPC

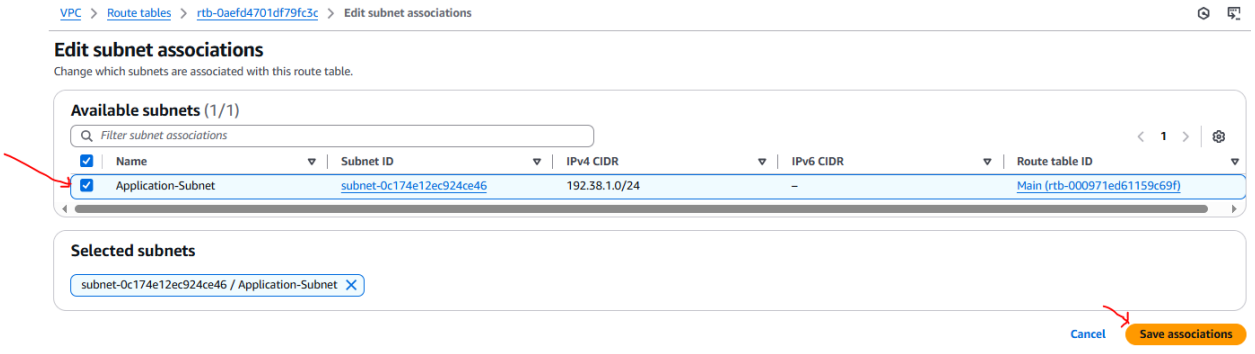


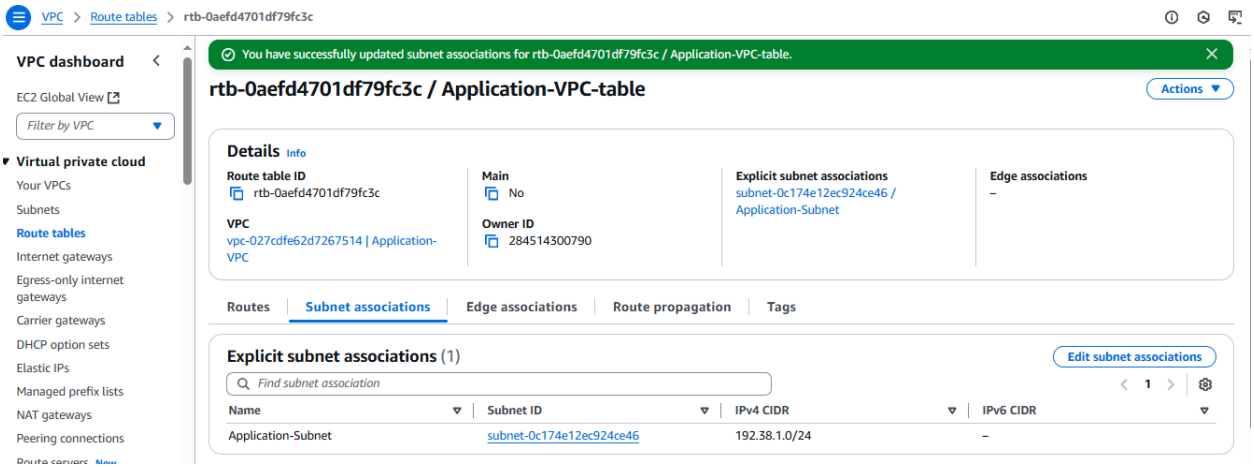





VPC > Route tables > rtb-0aefd4701df79fc3c
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Updated routes for rtb-0aefd4701df79fc3c / Application-VPC-table successfully
Details
rtb-0aefd4701df79fc3c / Application-VPC-table
Actions
Details Info
Route table ID
rtb-0aefd4701df79fc3c
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-027cdfe62d7267514 | Application-VPC
Owner ID
284514300790
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (3)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
0.0.0.0/0
igw-0c69a5a72c14db090
Active
No
10.0.0.0/16
pcx-01320dd221914ce5d
Active
No
192.38.0.0/16
local
Active
No


VPC > Route tables > rtb-0aefd4701df79fc3c
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New
rtb-0aefd4701df79fc3c / Application-VPC-table
Actions
Details Info
Route table ID
rtb-0aefd4701df79fc3c
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-027cdfe62d7267514 | Application-VPC
Owner ID
284514300790
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (0)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
No subnet associations
You do not have any subnet associations.


VPC > Route tables > rtb-0aefd4701df79fc3c > Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (1/1)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
Application-Subnet
subnet-0c174e12ec924ce46
192.38.1.0/24
–
Main (rtb-000971ed61159c69f)
Selected subnets
subnet-0c174e12ec924ce46 / Application-Subnet
Cancel
Save associations



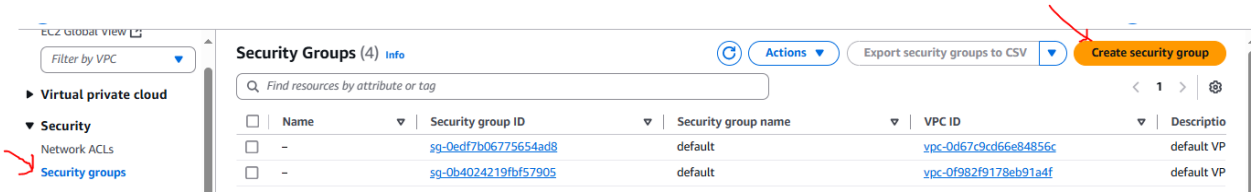
4. Verify the Route Table Association

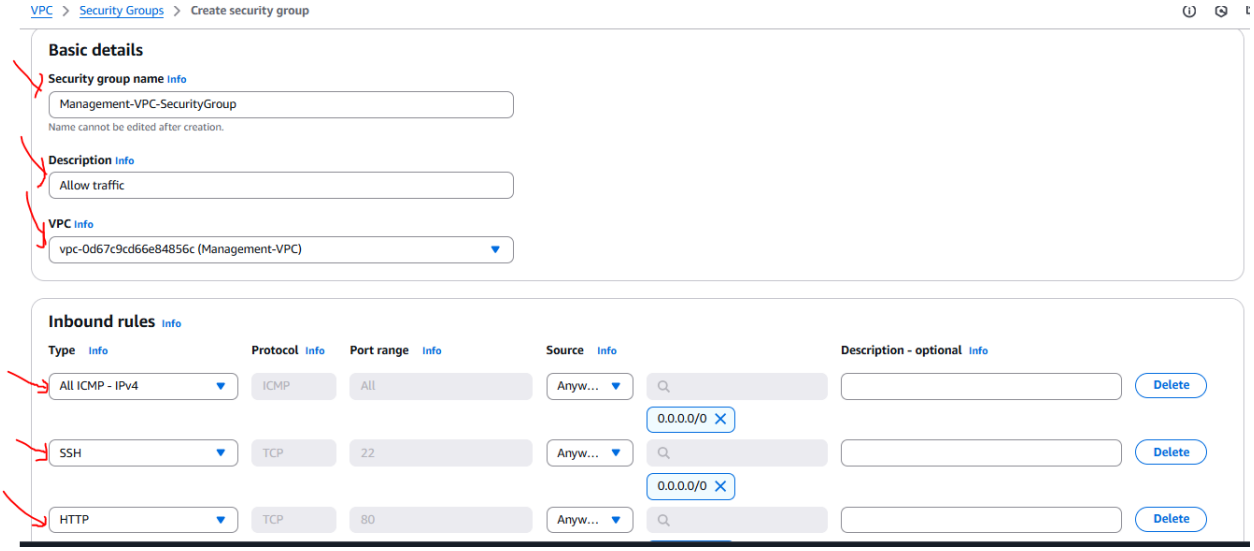
- You can confirm that the subnets are properly associated by navigating to **Subnets** under the **VPC** dashboard and checking which route table is listed for each subnet.
- You can also see the active routes by selecting the route table and checking the **Routes** tab.

Step 7: Create Security Groups

Allow only necessary traffic between VPCs:

1. Go to **Security Groups**
2. For Management-VPC-SecurityGroup, allow inbound traffic:
    - Source: Anywhere
    - Protocol: As required (All ICMP-IPv4, SSH, HTTP)
3. Similarly, configure Application-VPC-SecurityGroup to allow only required inbound connections





Outbound rules Info

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info	
All traffic	All	All	Anyw... 0.0.0.0/0		Delete

Add rule

⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

Tags - *optional*

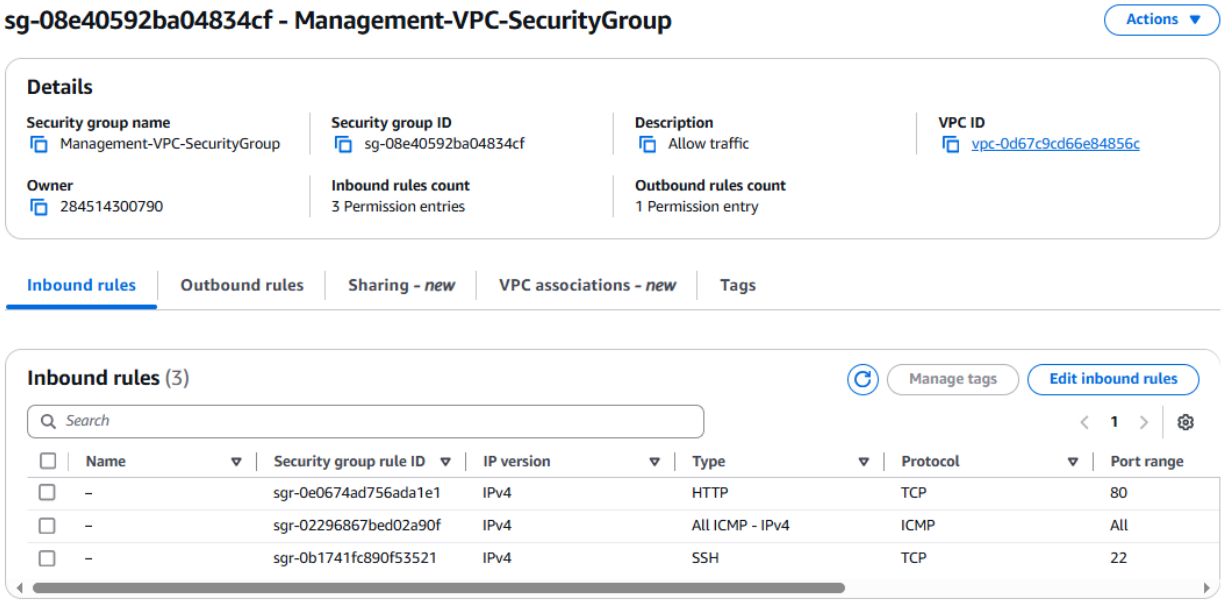
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

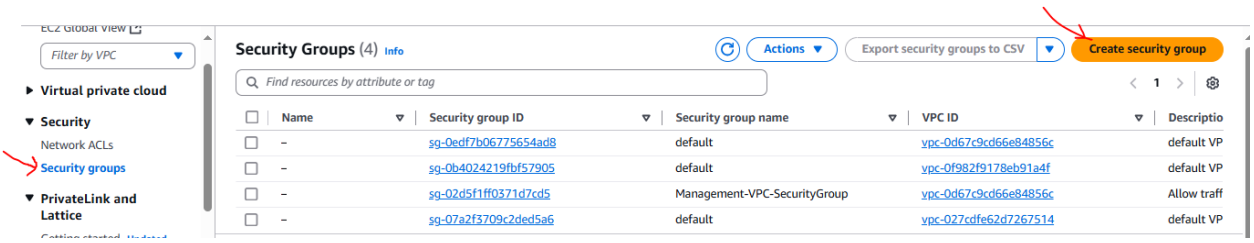
Add new tag

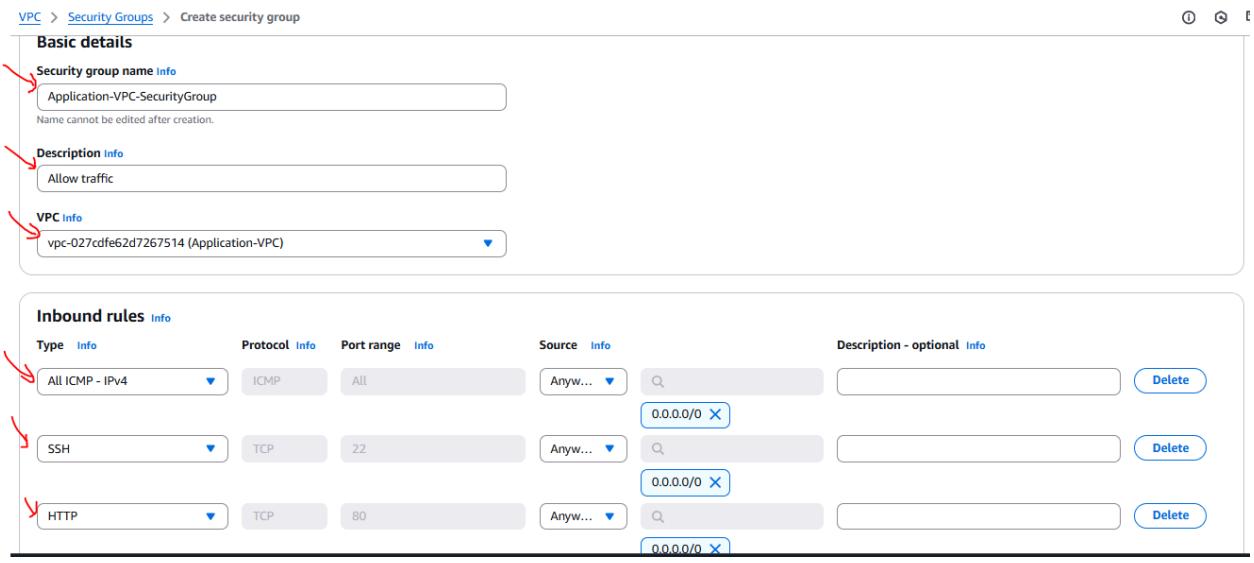
You can add up to 50 more tags

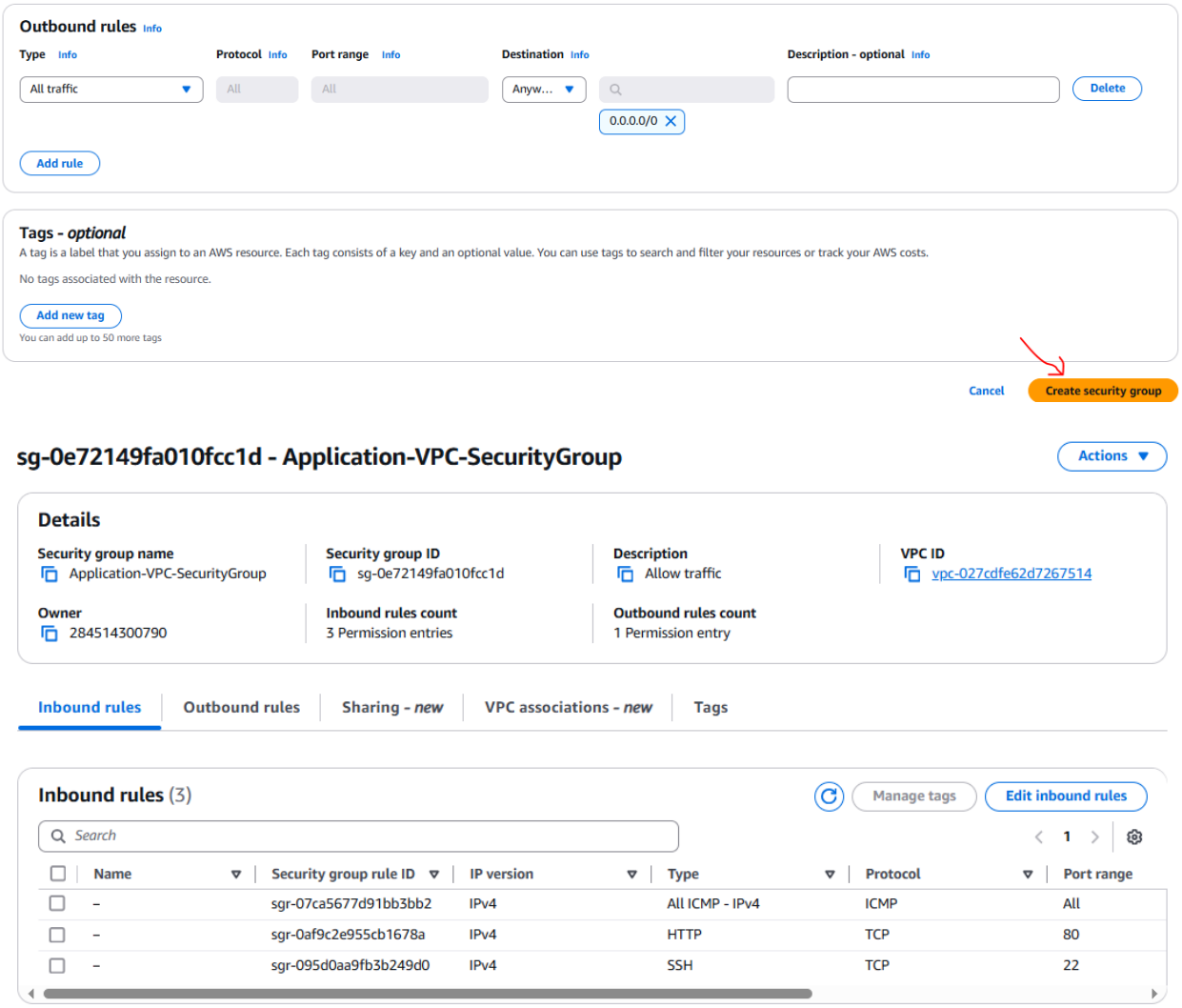
Cancel | Create security group



Create Application-VPC-Security Group







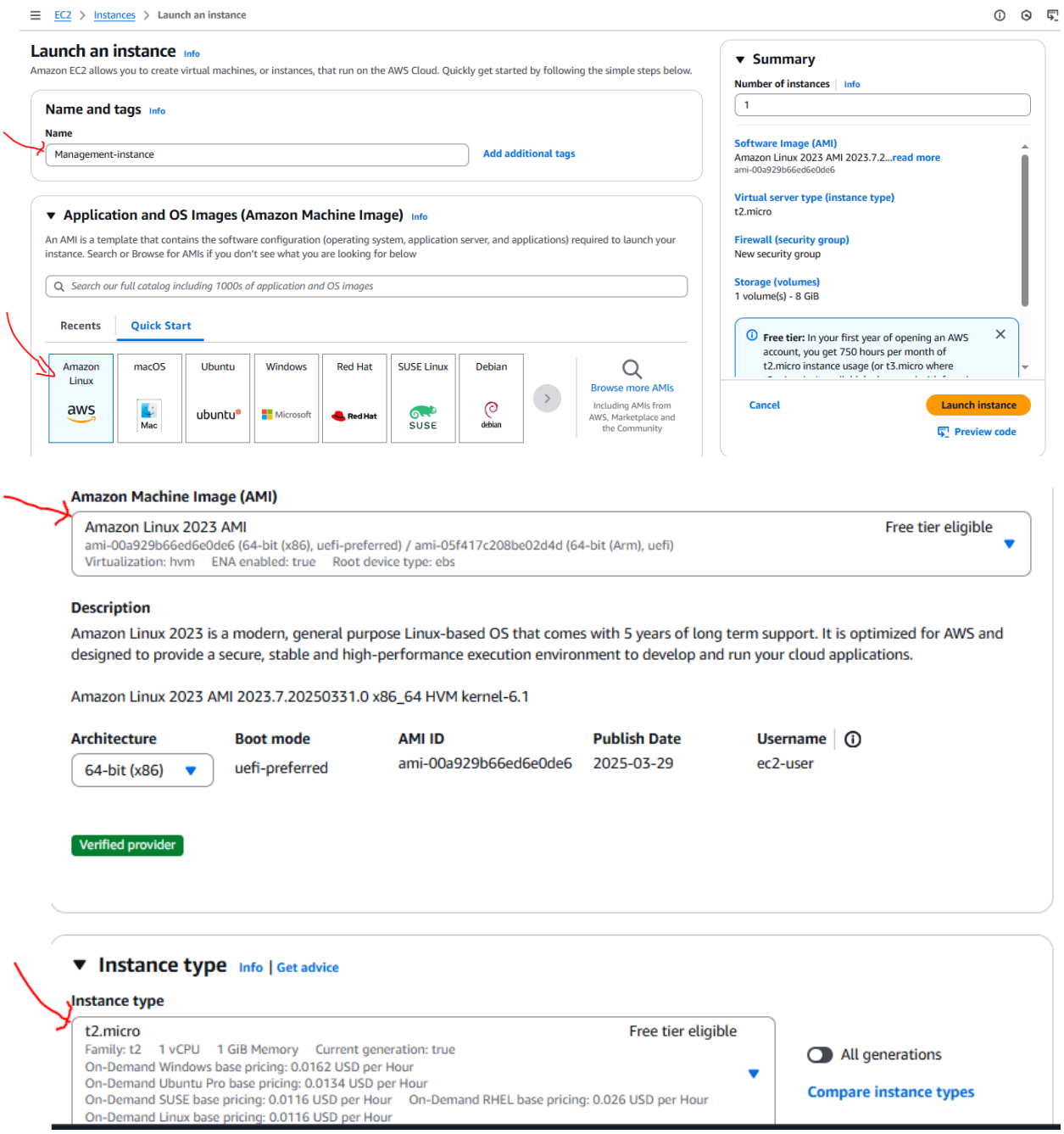
Step 8: Launch EC2 Instances (for testing) in each VPC

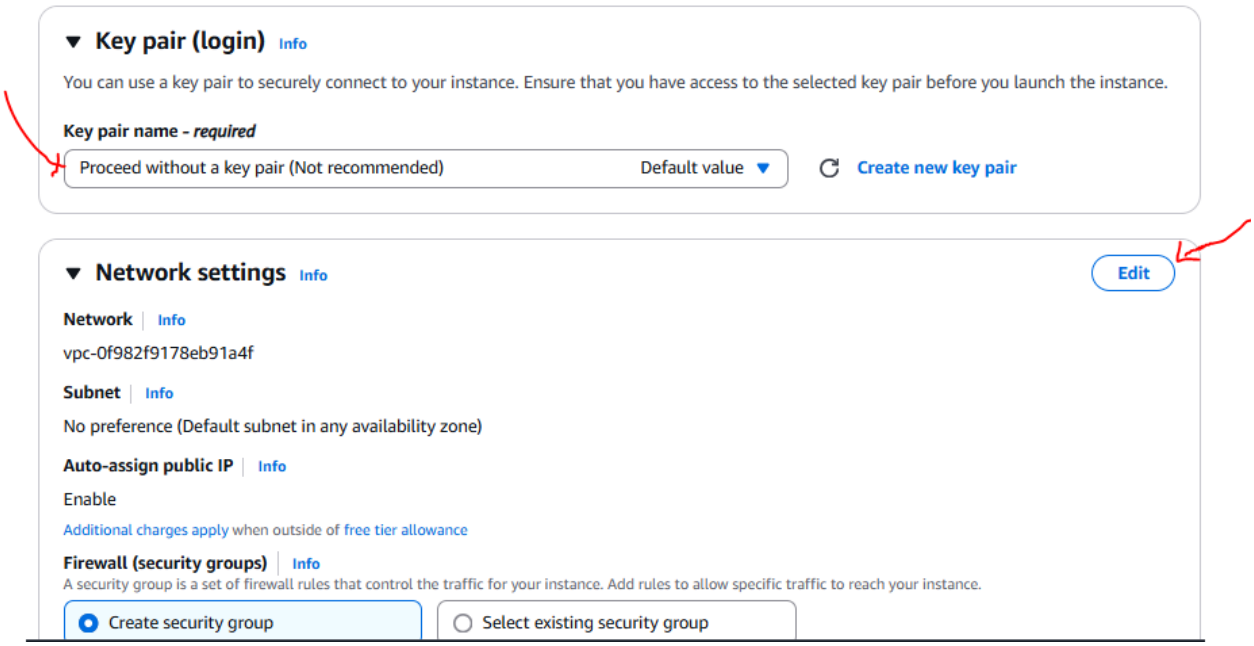
1. Go to **EC2** → Launch Instance
2. Choose Free Tier eligible AMI (Amazon Linux)
3. Instance type: t2.micro
4. Key pair: Proceed without keypair
5. Networking Setting: Edit

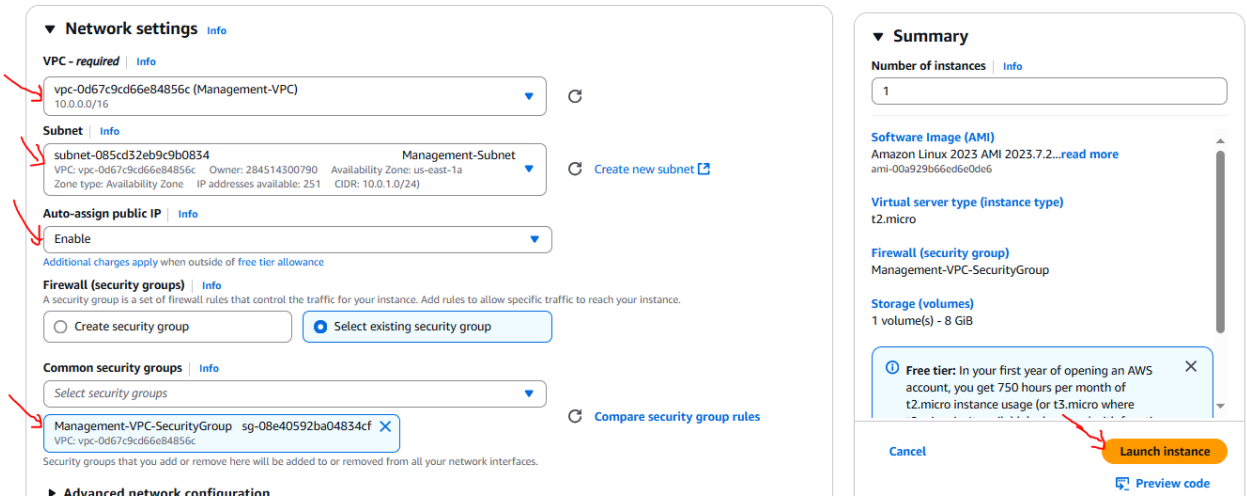
    - VPC: choose Management-VPC
    - Subnet: Management-subnet
    - Auto-assign public ip: enable
    - Firewall: Select existing Security Group (Management-VPC-SecurityGroup)

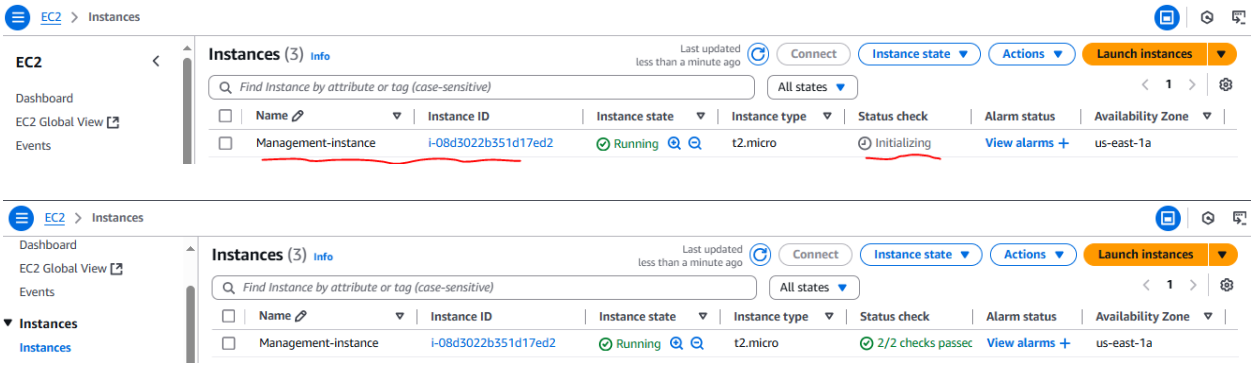
6. Leave default settings
7. Click Launch Instance
8. Use **private IPs** to test connectivity via SSH or ping (if ICMP allowed)

Create Management-instance

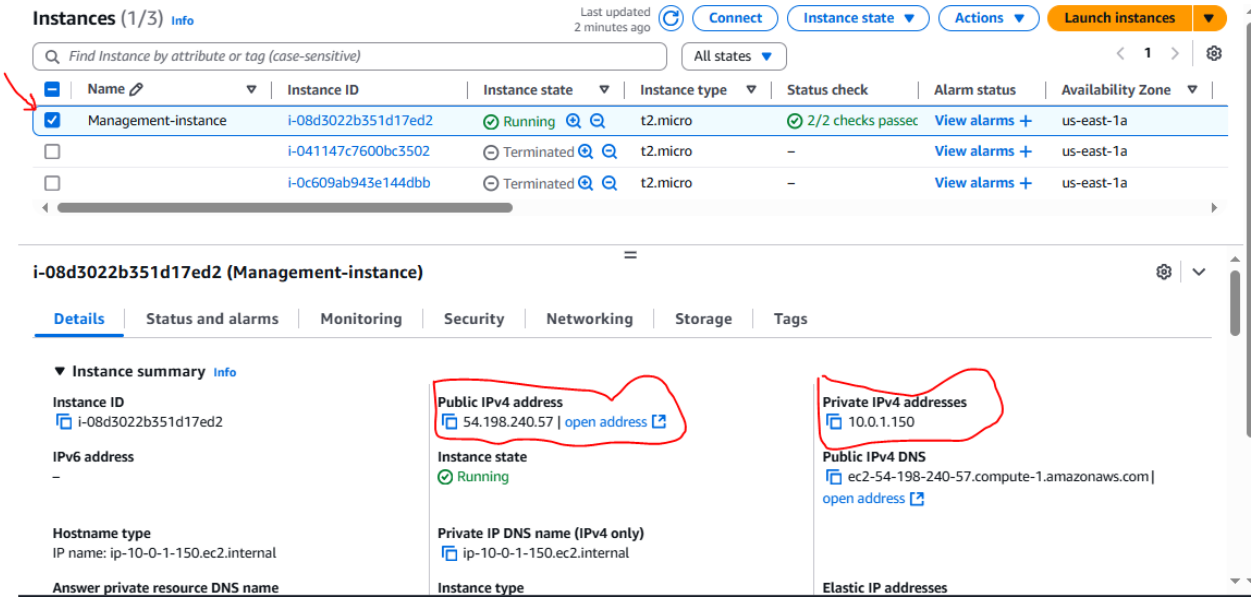



Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
Proceed without a key pair (Not recommended)
Default value
Create new key pair
Network settings Info
Edit
Network Info
vpc-0f982f9178eb91a4f
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance
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

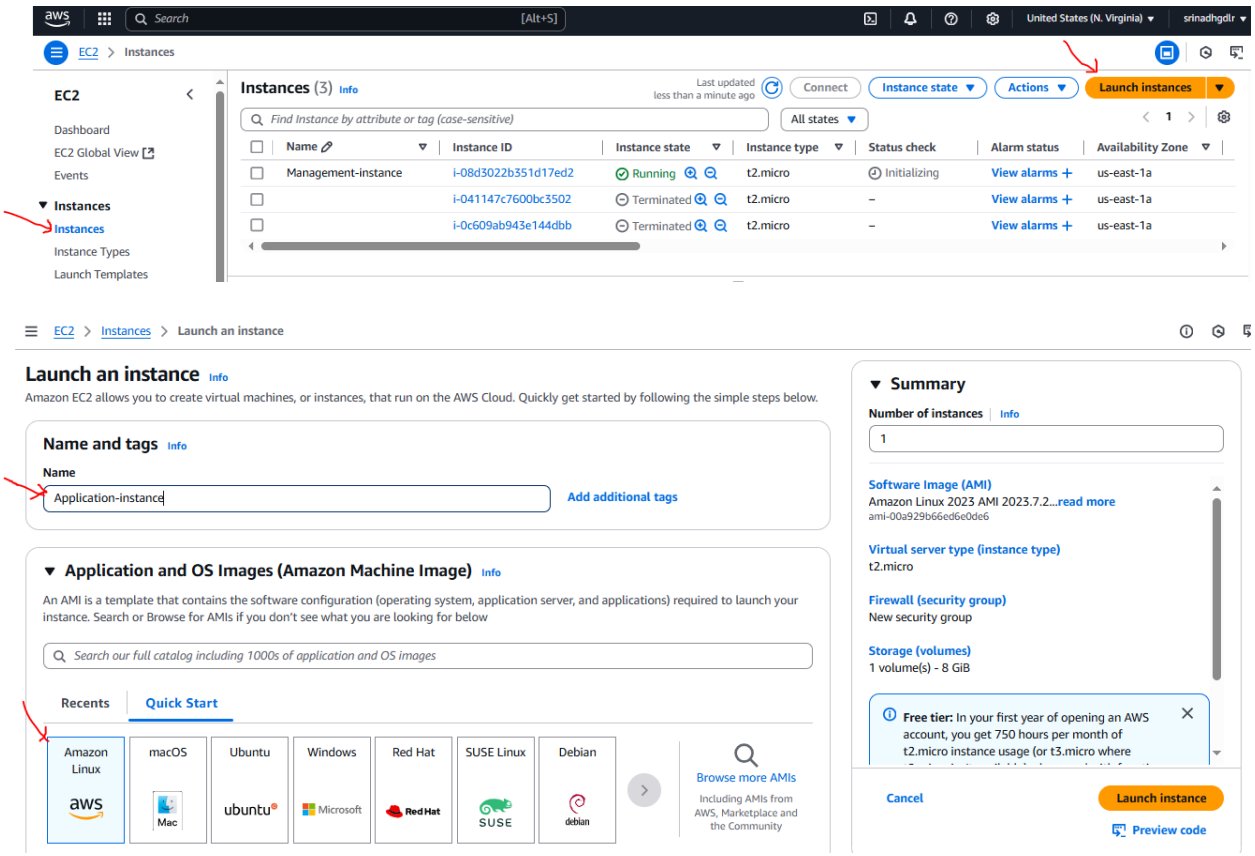

Network settings Info
VPC - required Info
vpc-0d67c9cd66e84856c (Management-VPC)
10.0.0.0/16
Subnet Info
subnet-085cd32eb9c9b0834 Management-Subnet
VPC: vpc-0d67c9cd66e84856c Owner: 284514300790 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24)
Create new subnet
Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance
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
Common security groups Info
Select security groups
Management-VPC-SecurityGroup sg-08e40592ba04834cf
VPC: vpc-0d67c9cd66e84856c
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Advanced network configuration
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.7.2...read more
ami-00a929b66ed6e0de6
Virtual server type (instance type)
t2.micro
Firewall (security group)
Management-VPC-SecurityGroup
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
Cancel
Launch instance
Preview code

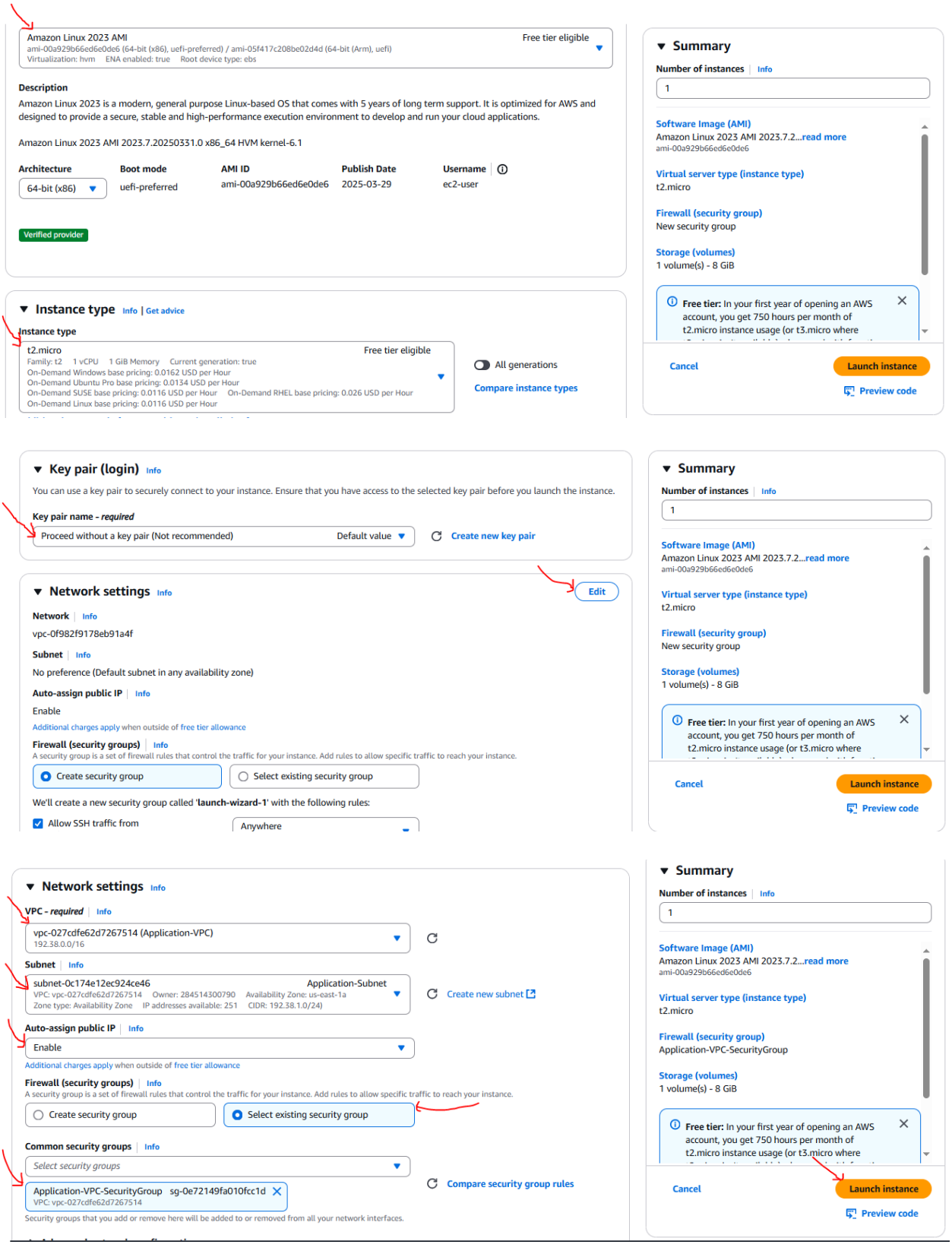

EC2 > Instances
EC2
Dashboard
EC2 Global View
Events
Instances (3) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Management-instance
i-08d3022b351d17ed2
Running
t2.micro
Initializing
View alarms
us-east-1a

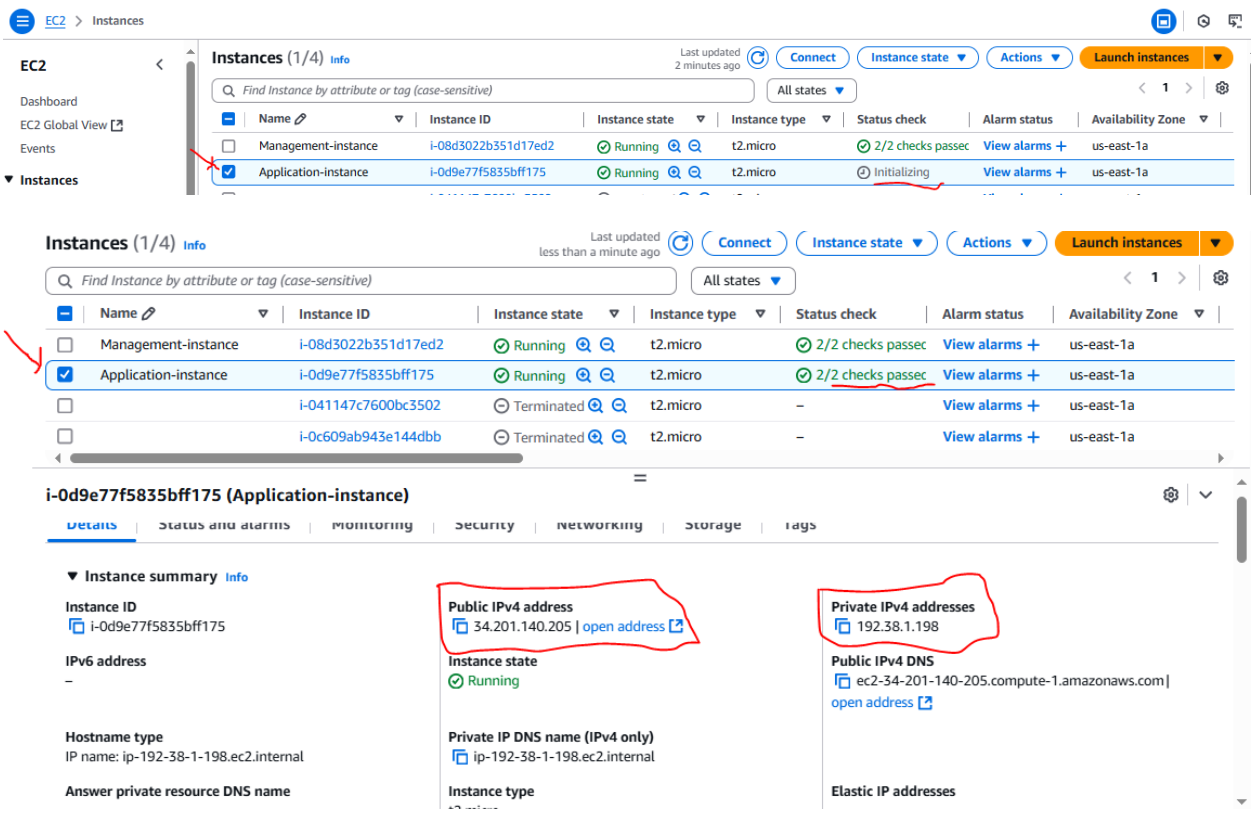
EC2 > Instances
Dashboard
EC2 Global View
Events
Instances
Instances
Instances (3) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Management-instance
i-08d3022b351d17ed2
Running
t2.micro
2/2 checks passed
View alarms
us-east-1a



Create Application-instance




Amazon Linux 2023 AMI
ami-00a929b66ed6e0de6 (64-bit (x86), uefi-preferred) / ami-05f417c208be02d4d (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs
Free tier eligible
Description
Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.
Amazon Linux 2023 AMI 2023.7.20250331.0 x86_64 HVM kernel-6.1
Architecture
64-bit (x86)
Boot mode
uefi-preferred
AMI ID
ami-00a929b66ed6e0de6
Publish Date
2025-03-29
Username
ec2-user
Verified provider
Instance type Info | Get advice
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour
All generations
Compare instance types
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.7.2...read more
ami-00a929b66ed6e0de6
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
Cancel
Launch instance
Preview code
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
Proceed without a key pair (Not recommended)
Default value
Create new key pair
Network settings Info
Edit
Network Info
vpc-0f982f9178eb91a4f
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance
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
We'll create a new security group called 'launch-wizard-1' with the following rules:
Allow SSH traffic from
Anywhere
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.7.2...read more
ami-00a929b66ed6e0de6
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
Cancel
Launch instance
Preview code
Network settings Info
VPC - required Info
vpc-027cdfe62d7267514 (Application-VPC)
192.38.0.0/16
Subnet Info
subnet-0c174e12ec924ce46
Application-Subnet
VPC: vpc-027cdfe62d7267514 Owner: 284514300790 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 192.38.1.0/24)
Create new subnet
Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance
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
Common security groups Info
Select security groups
Application-VPC-SecurityGroup sg-0e72149fa010fcc1d
VPC: vpc-027cdfe62d7267514
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.7.2...read more
ami-00a929b66ed6e0de6
Virtual server type (instance type)
t2.micro
Firewall (security group)
Application-VPC-SecurityGroup
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
Cancel
Launch instance
Preview code

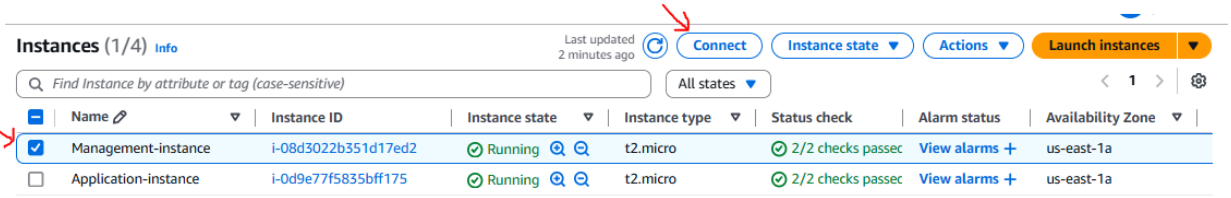


Step 9: Test and Monitor

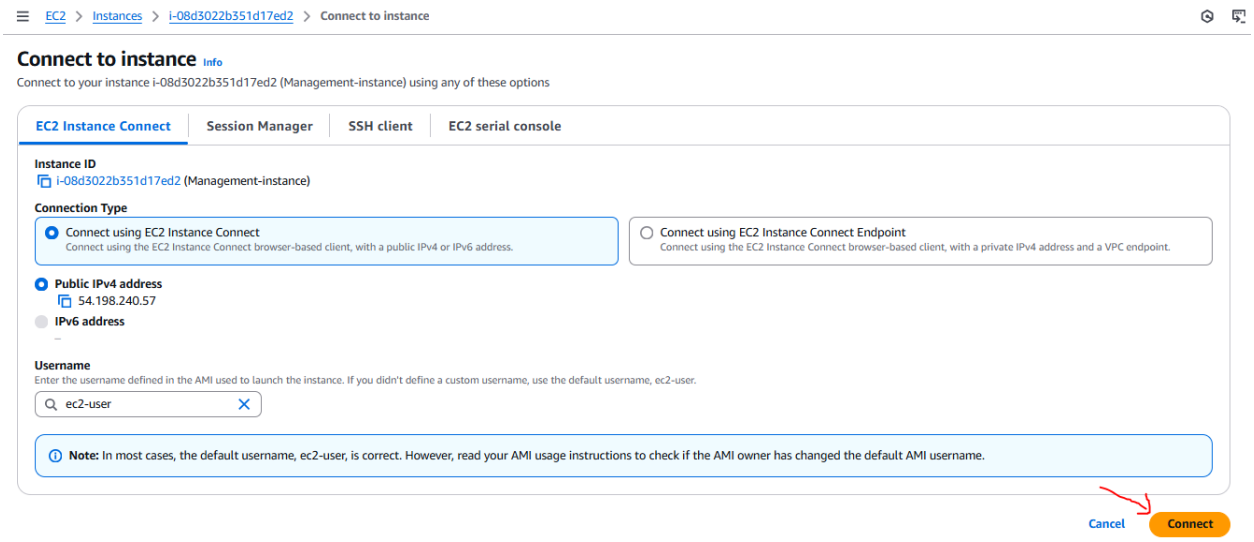
- SSH from Management EC2 to Application EC2 (or vice versa, depending on security rules)
- Enable **VPC Flow Logs** for each VPC to monitor traffic

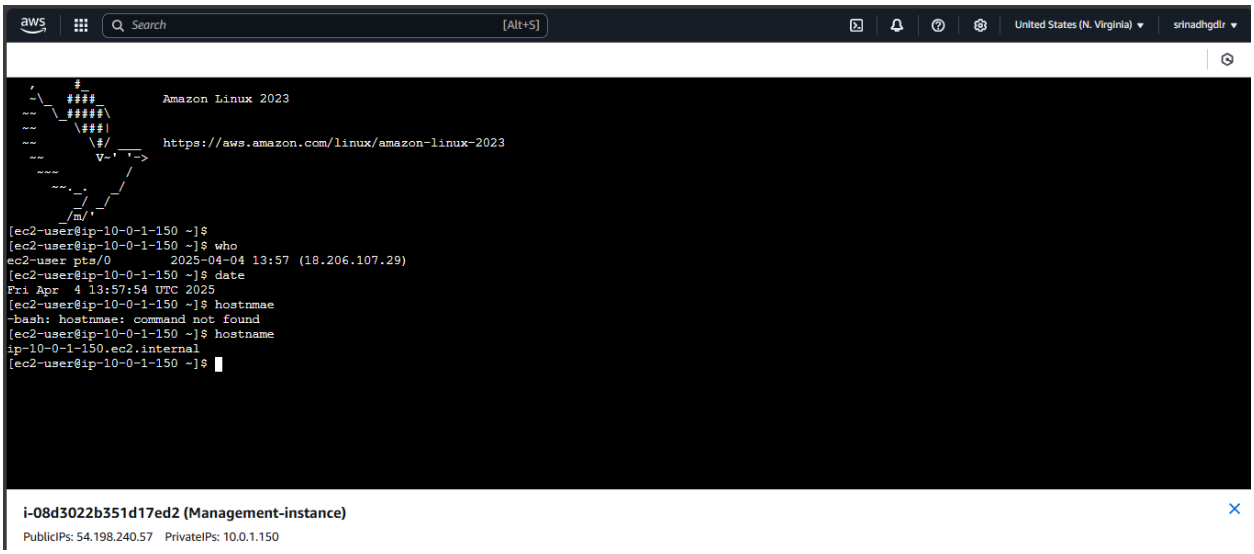
Connect to EC2 instance:

Choose Management-instance and click on connect button



Click on EC2 Instance Connect tab and click Connect





Ping **Private IPv4 addresses 198.38.1.198** of Application-instance from Management-instance

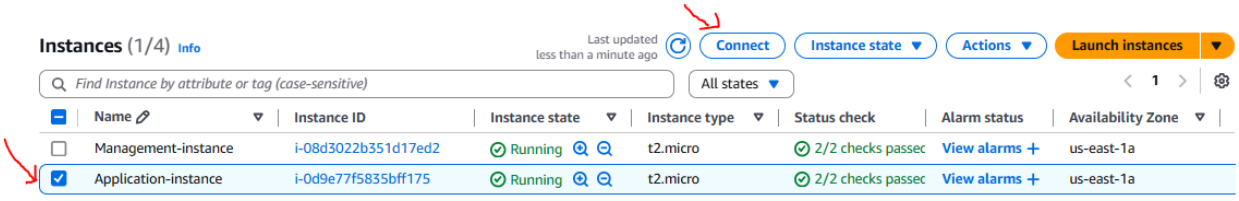
```
[ec2-user@ip-10-0-1-150 ~]$ ping 192.38.1.198
PING 192.38.1.198 (192.38.1.198) 56(84) bytes of data.
64 bytes from 192.38.1.198: icmp_seq=1 ttl=127 time=1.17 ms
64 bytes from 192.38.1.198: icmp_seq=2 ttl=127 time=1.25 ms
64 bytes from 192.38.1.198: icmp_seq=3 ttl=127 time=0.635 ms
64 bytes from 192.38.1.198: icmp_seq=4 ttl=127 time=0.850 ms
64 bytes from 192.38.1.198: icmp_seq=5 ttl=127 time=0.807 ms
64 bytes from 192.38.1.198: icmp_seq=6 ttl=127 time=0.821 ms
64 bytes from 192.38.1.198: icmp_seq=7 ttl=127 time=0.694 ms

64 bytes from 192.38.1.198: icmp_seq=8 ttl=127 time=1.07 ms
^C
--- 192.38.1.198 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7205ms
rtt min/avg/max/mdev = 0.635/0.912/1.252/0.210 ms
[ec2-user@ip-10-0-1-150 ~]$
```

i-08d3022b351d17ed2 (Management-instance)

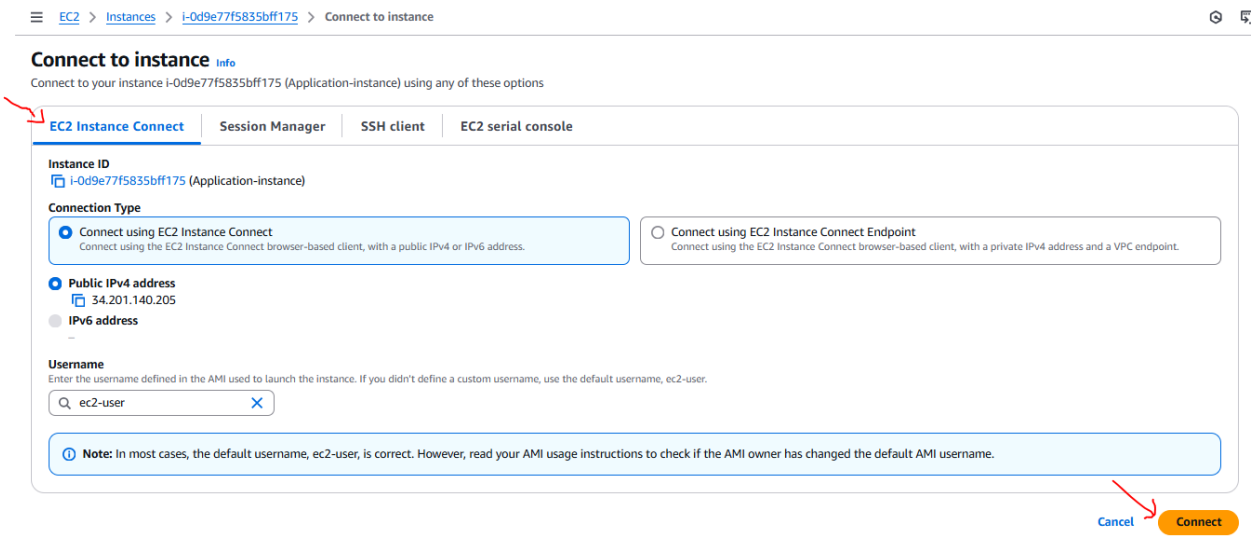
PublicIPs: 54.198.240.57 PrivateIPs: 10.0.1.150

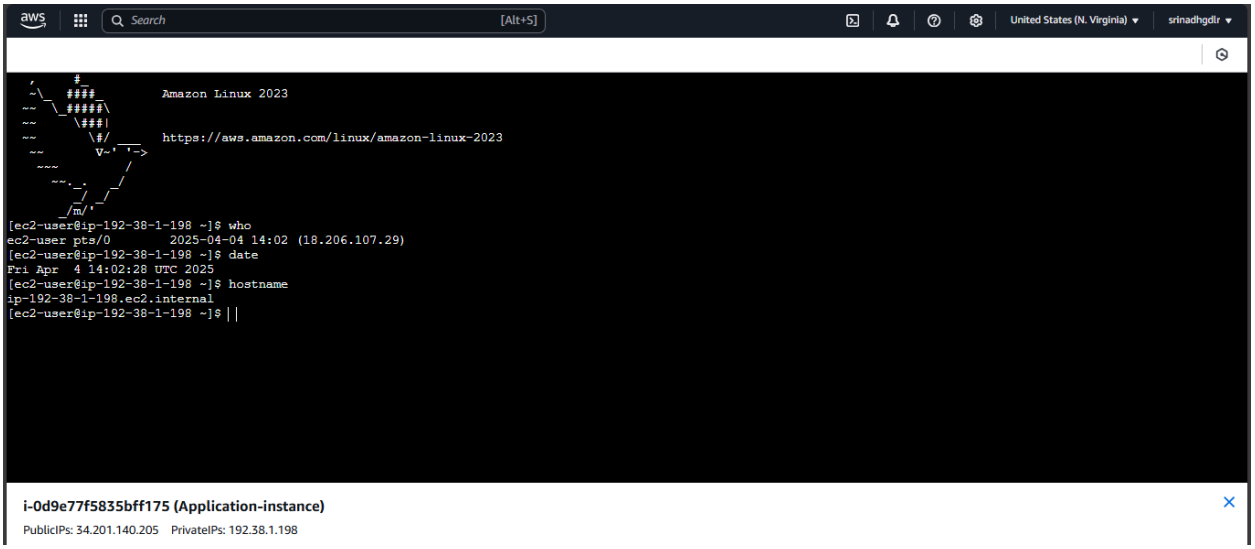
So, it is connecting and we can access resources of other VPC

Connect to Application-instance:

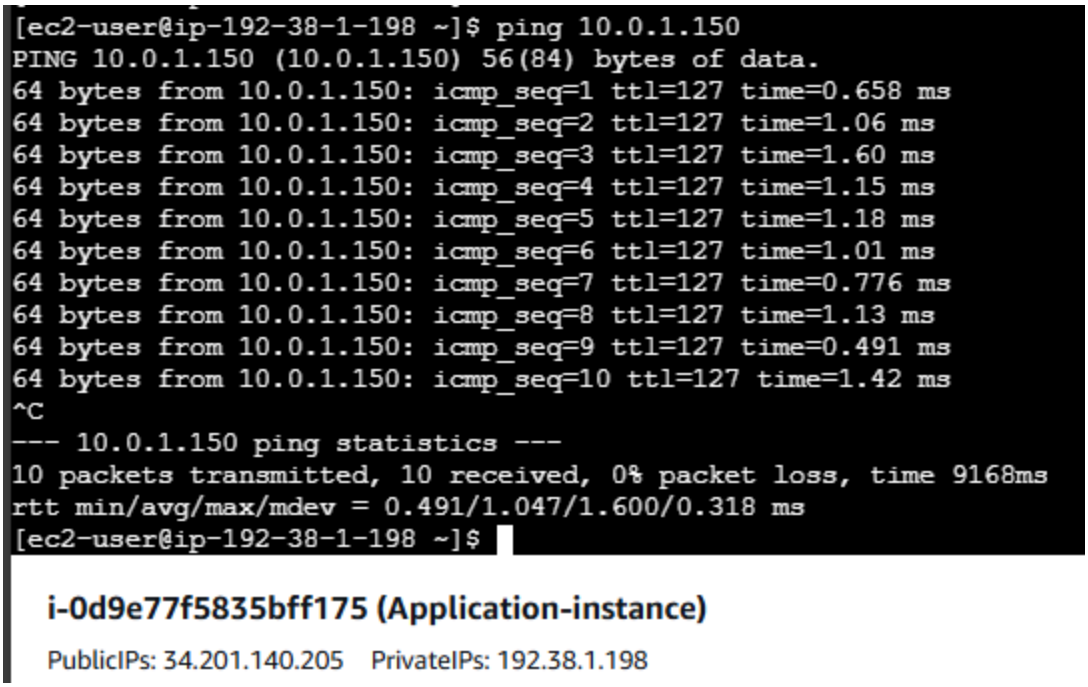


Click on EC2 Instance Connect tab and click Connect





Ping **Private IPv4 addresses 10.0.1.150** of Management-instance from the Application-instance



So, it is connecting and we can access resources of other VPC
