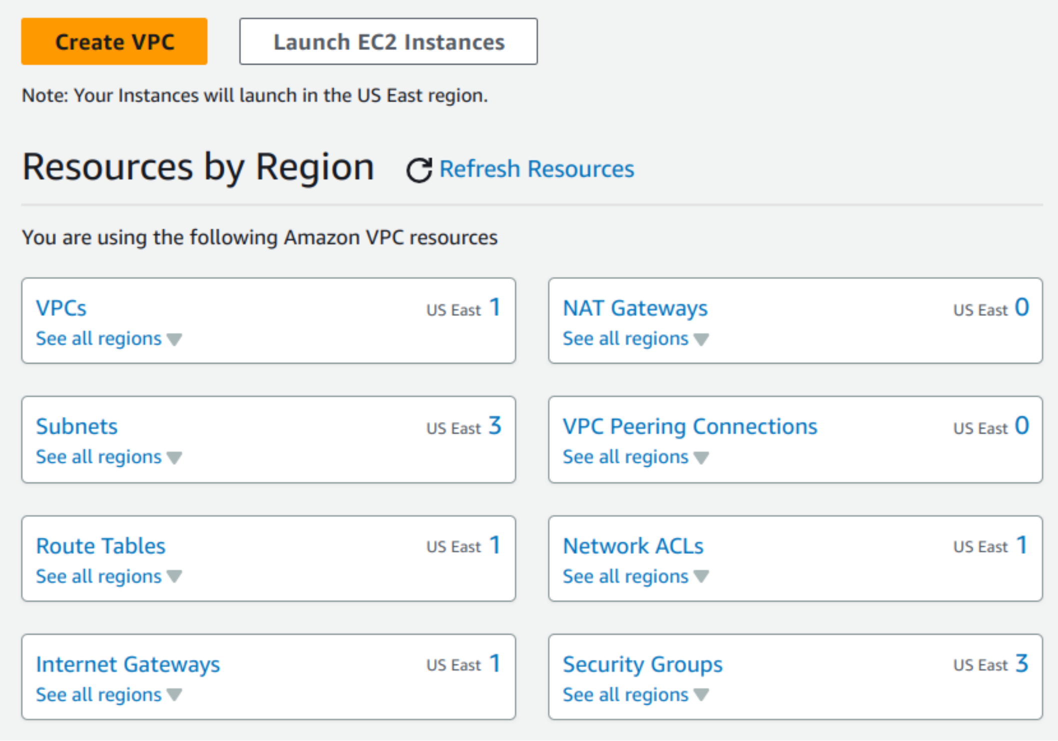
AWS Networking Hands-on

Day 4 **5th July 2023**

Creating a VPC and EC2 instances

Step 1 - Login to the AWS management console and browse to the VPC console.



Note: Your Instances will launch in the US East region.

Resources by Region

You are using the following Amazon VPC resources

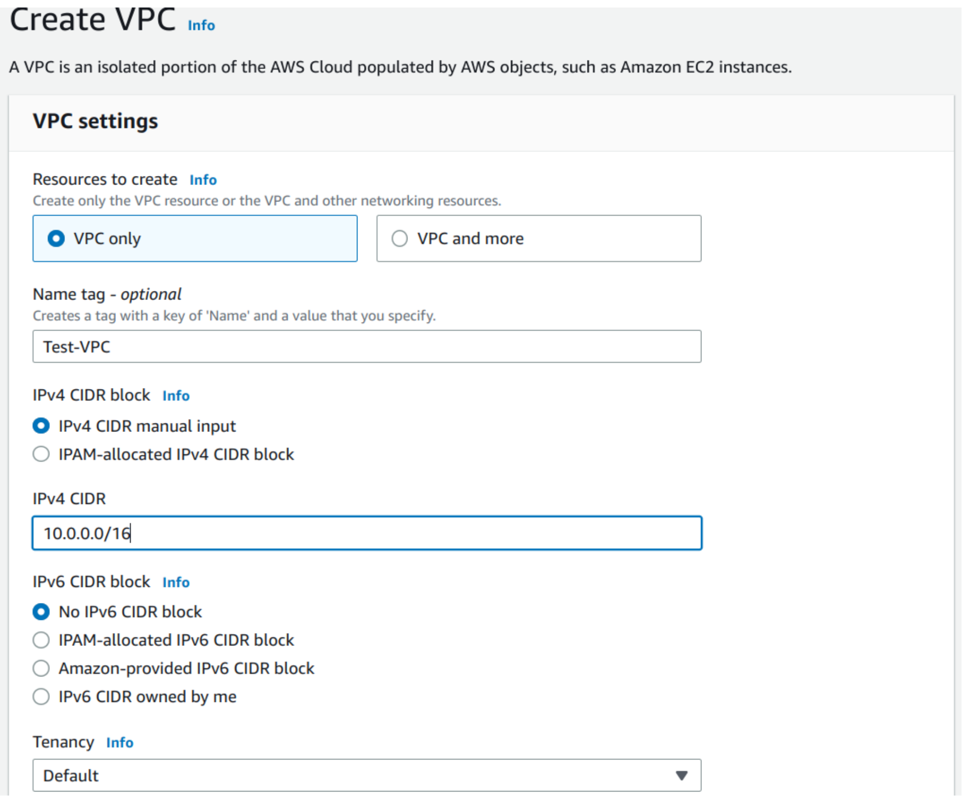
VPCs See all regions ▼	US East 1	NAT Gateways See all regions ▼	US East 0
Subnets See all regions ▼	US East 3	VPC Peering Connections See all regions ▼	US East 0
Route Tables See all regions ▼	US East 1	Network ACLs See all regions ▼	US East 1
Internet Gateways See all regions ▼	US East 1	Security Groups See all regions ▼	US East 3

Step 2 - Click on “Create VPC”.

Enter the following values -

- **Name tag:** Test-VPC
- **IPv4 CIDR block:** Select “IPv4 CIDR manual input”
- **IPv4 CIDR:** 10.0.0.0/16
- **IPV6 CIDR:** Select “No IPv6 CIDR block”
- **Tenancy:** Select “default”
  - Tenancy can be applied to instances launched in this VPC to be default or dedicated instances.
- **Tags:** Tags are used for searching and filtering the resources based on the key:value pair of the tags.

Click on “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.

Test-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

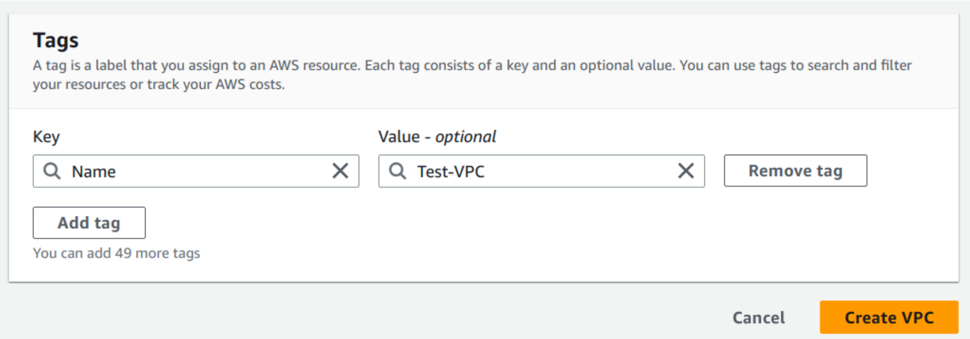
○ IPAM-allocated IPv6 CIDR block

○ 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.

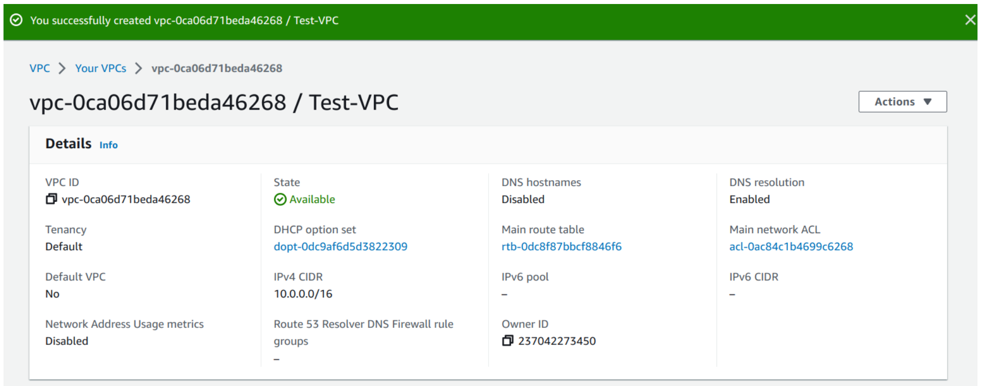
Key	Value - *optional*	
Name	Test-VPC	Remove tag

Add tag

You can add 49 more tags

Cancel Create VPC

Step 3 - Review that the VPC was created successfully.



You successfully created vpc-0ca06d71beda46268 / Test-VPC

VPC > Your VPCs > vpc-0ca06d71beda46268

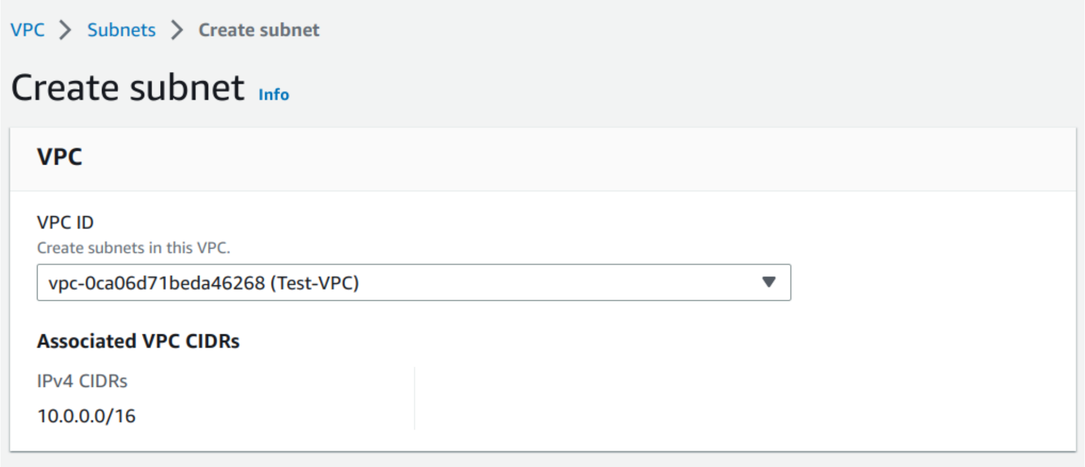
vpc-0ca06d71beda46268 / Test-VPC

Actions ▼

Details Info

VPC ID vpc-0ca06d71beda46268	State ✓ Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0dc9af6d5d3822309	Main route table rtb-0dc8f87bbcf8846f6	Main network ACL acl-0ac84c1b4699c6268
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –	IPv6 CIDR –
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 237042273450	

Step 4 - Create Public Subnets inside the VPC.



Create subnet Info

VPC

VPC ID

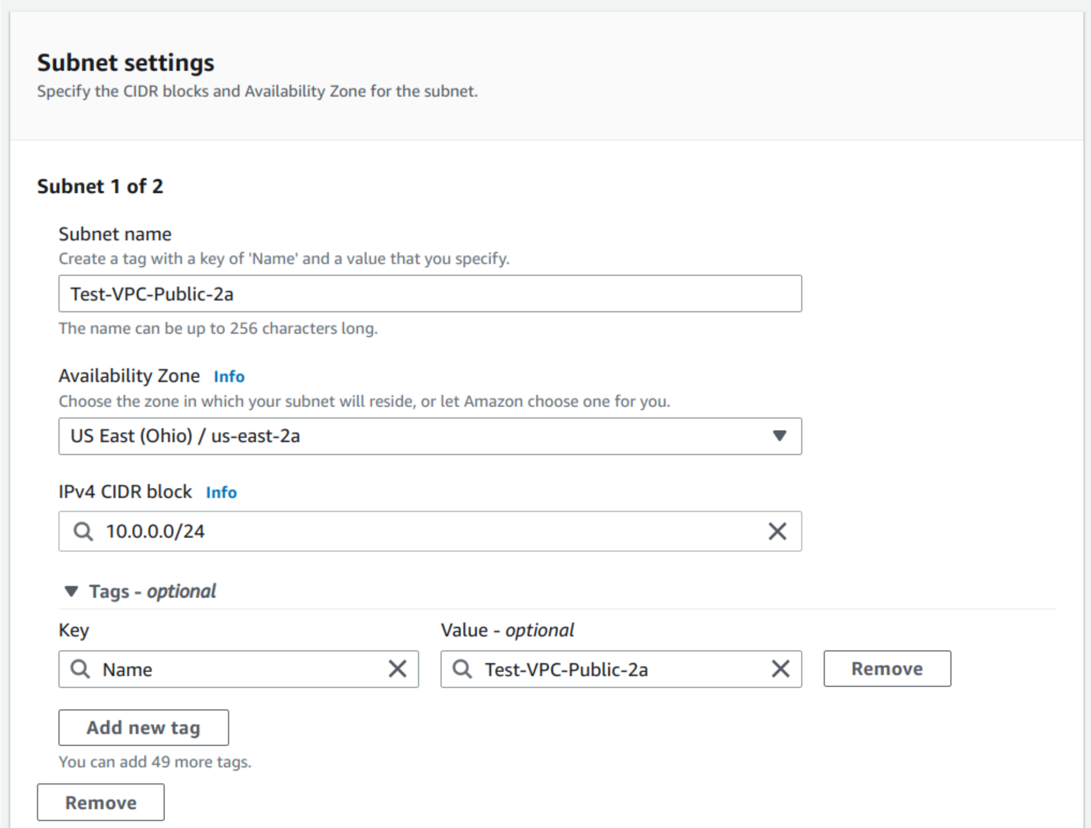
Create subnets in this VPC.

vpc-0ca06d71beda46268 (Test-VPC)

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16


Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Test-VPC-Public-2a

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.

US East (Ohio) / us-east-2a

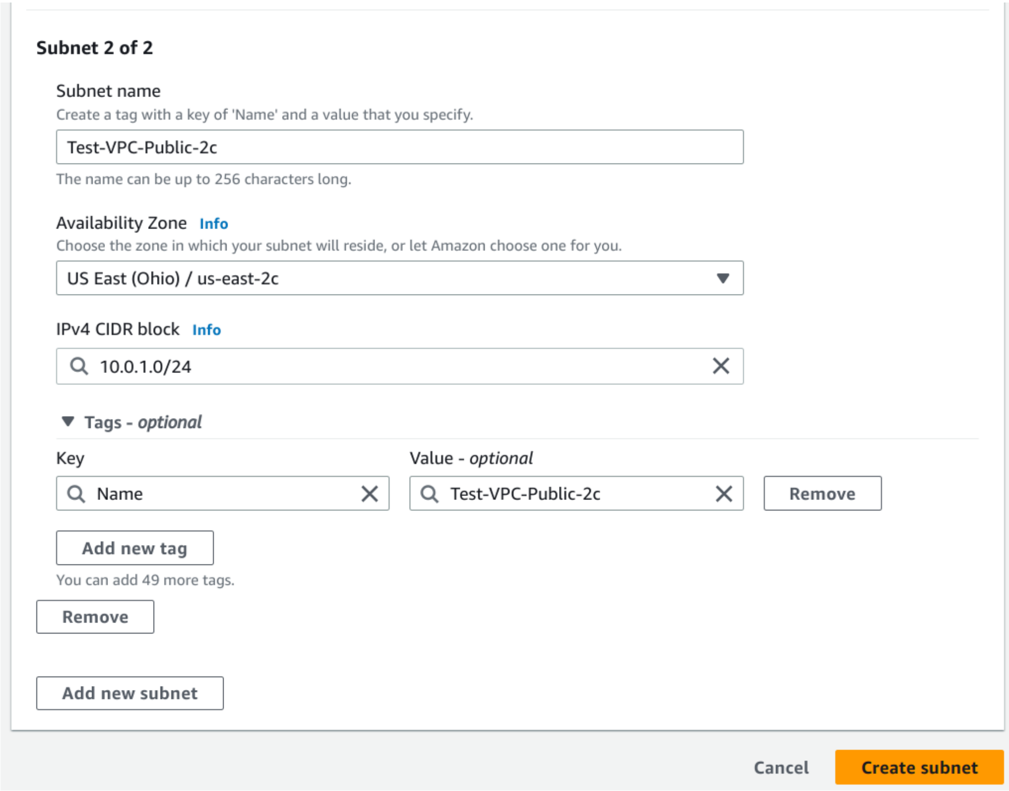
IPv4 CIDR block Info

10.0.0.0/24

Tags - *optional*

Key	Value - *optional*
Name	Test-VPC-Public-2a

You can add 49 more tags.



Subnet 2 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Test-VPC-Public-2c
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.
US East (Ohio) / us-east-2c

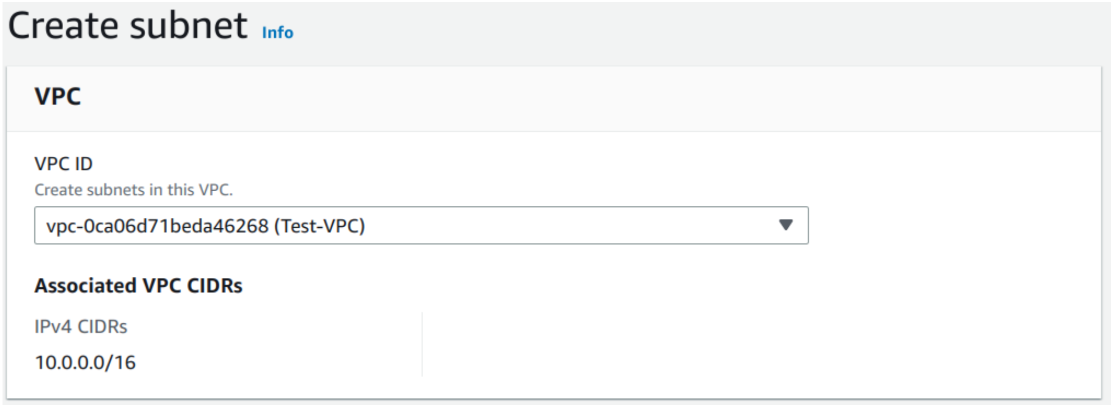
IPv4 CIDR block Info
10.0.1.0/24

Tags - *optional*

Key	Value - *optional*
Name	Test-VPC-Public-2c

You can add 49 more tags.

Step 5 - Create Private Subnets in the VPC.



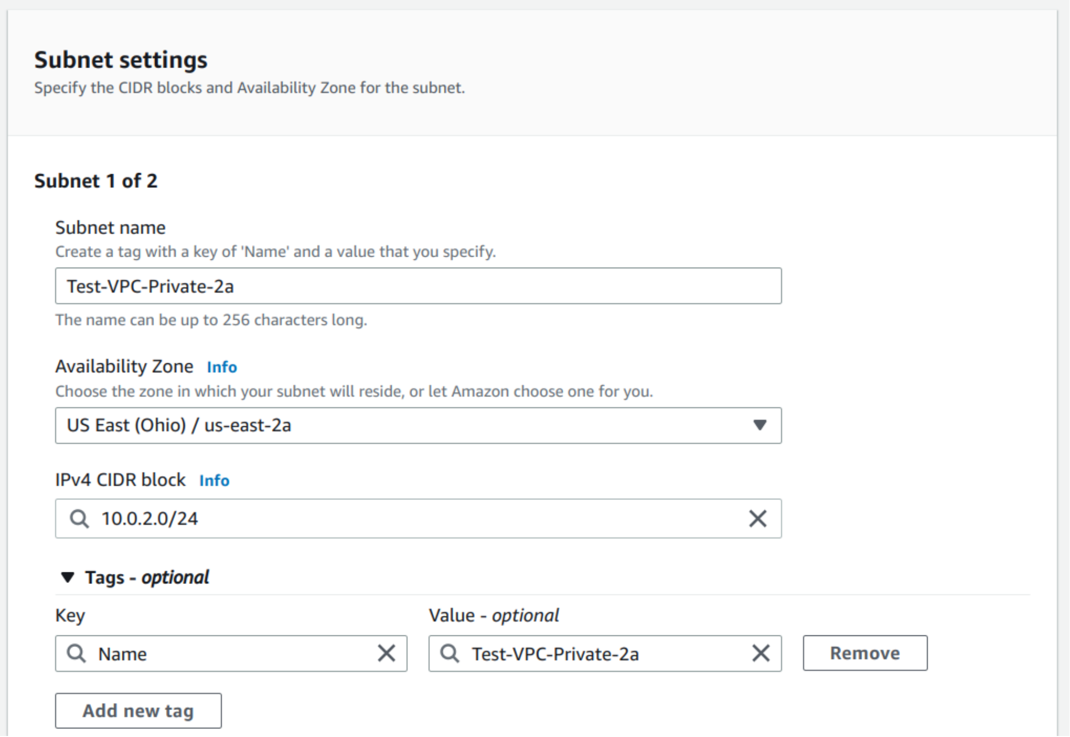
Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0ca06d71beda46268 (Test-VPC)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16



Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Test-VPC-Private-2a

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.

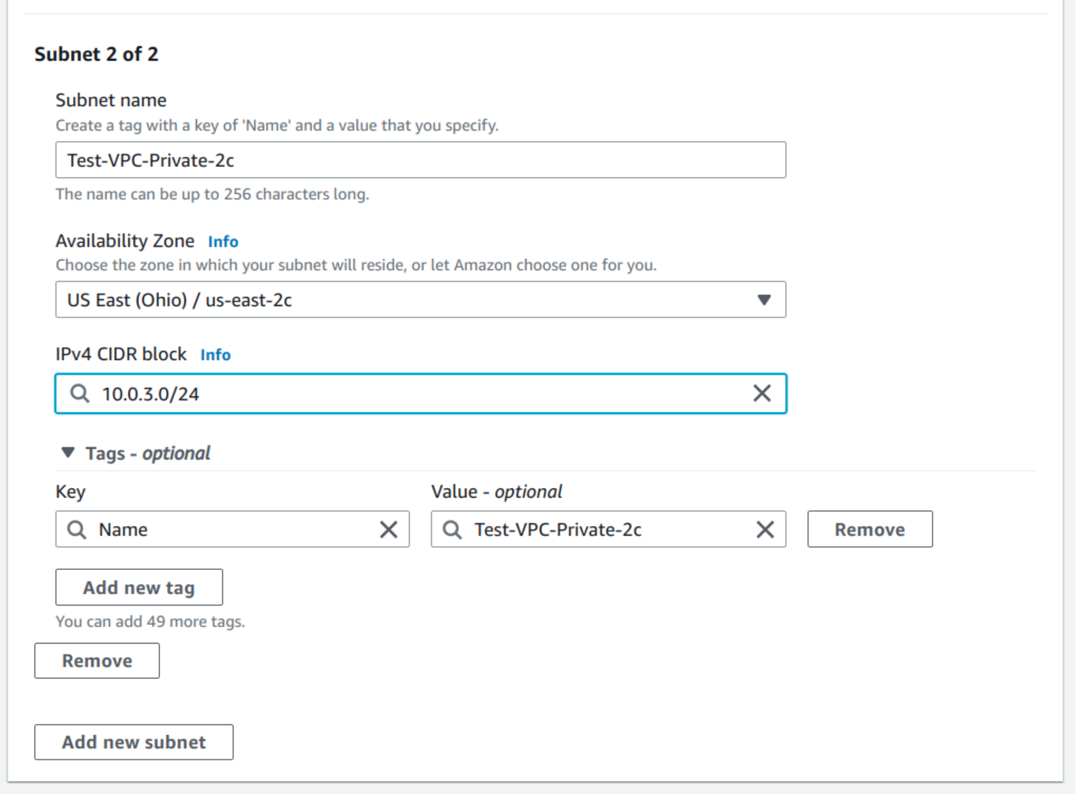
US East (Ohio) / us-east-2a ▼

IPv4 CIDR block Info

10.0.2.0/24

▼ Tags - *optional*

Key	Value - *optional*
Name	Test-VPC-Private-2a



Subnet 2 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Test-VPC-Private-2c

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.

US East (Ohio) / us-east-2c ▼

IPv4 CIDR block Info

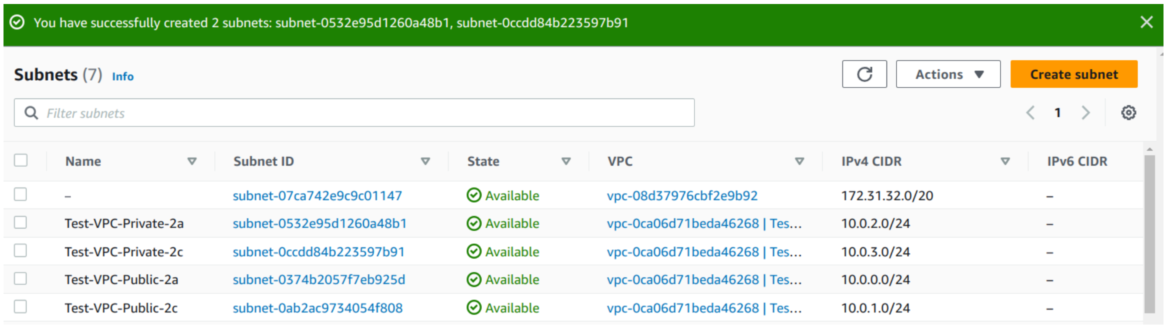
10.0.3.0/24

▼ Tags - *optional*

Key	Value - *optional*
Name	Test-VPC-Private-2c

You can add 49 more tags.

Step 6 - Review the created subnets.

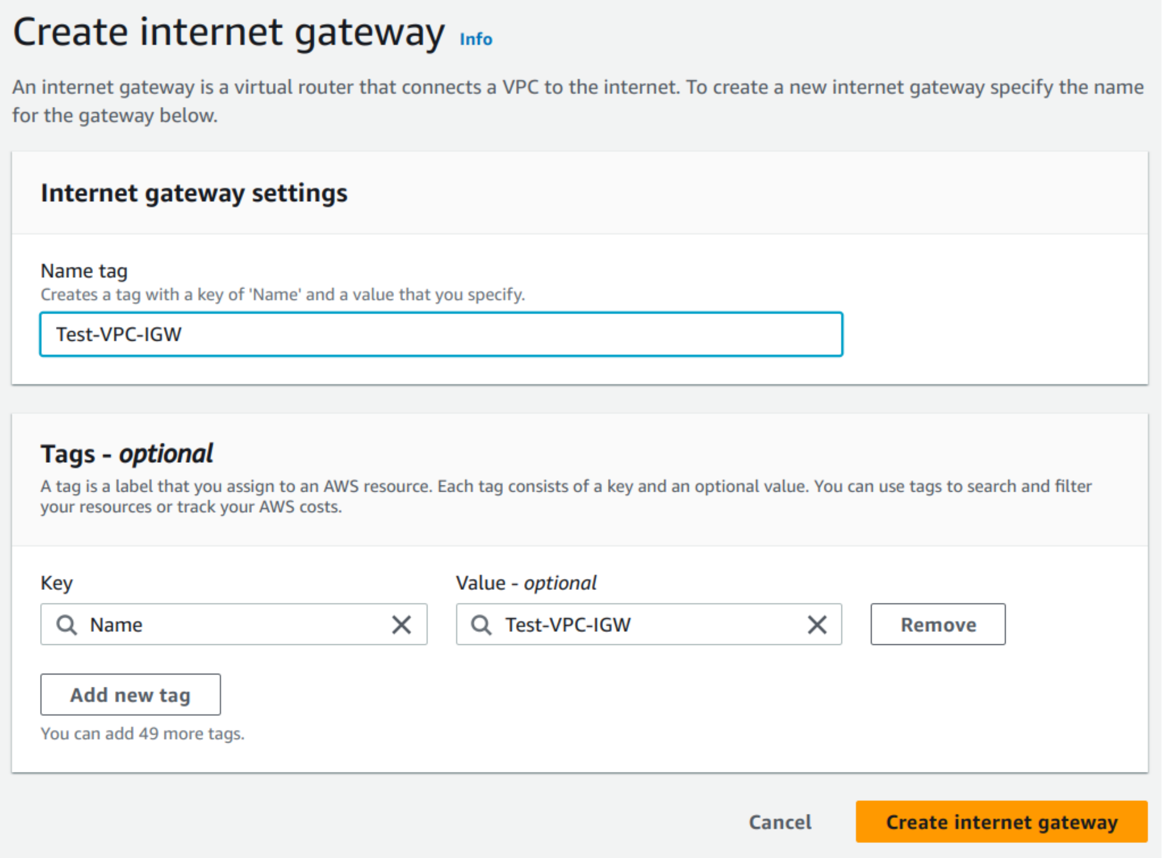


You have successfully created 2 subnets: subnet-0532e95d1260a48b1, subnet-0ccdd84b223597b91

Subnets (7) Info

□	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
□	–	subnet-07ca742e9c9c01147	✓ Available	vpc-08d37976cbf2e9b92	172.31.32.0/20	–
□	Test-VPC-Private-2a	subnet-0532e95d1260a48b1	✓ Available	vpc-0ca06d71beda46268 | Tes...	10.0.2.0/24	–
□	Test-VPC-Private-2c	subnet-0ccdd84b223597b91	✓ Available	vpc-0ca06d71beda46268 | Tes...	10.0.3.0/24	–
□	Test-VPC-Public-2a	subnet-0374b2057f7eb925d	✓ Available	vpc-0ca06d71beda46268 | Tes...	10.0.0.0/24	–
□	Test-VPC-Public-2c	subnet-0ab2ac9734054f808	✓ Available	vpc-0ca06d71beda46268 | Tes...	10.0.1.0/24	–

Step 7 - Create an Internet gateway and attach it to the VPC.



Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

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

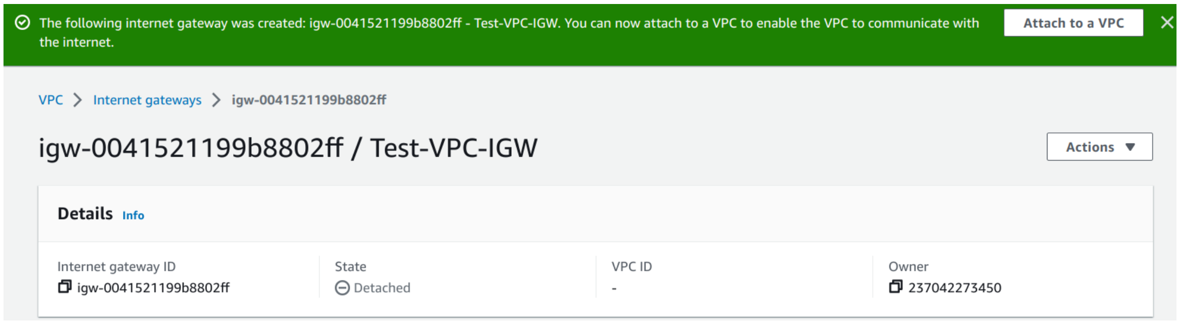
Test-VPC-IGW

Tags - *optional*

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

Key	Value - *optional*
Name	Test-VPC-IGW

You can add 49 more tags.

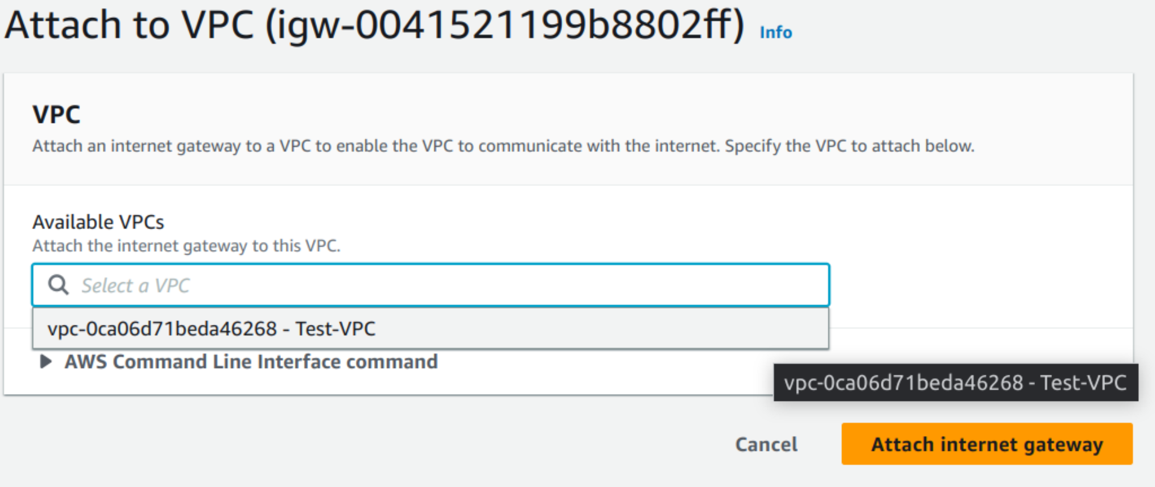


The following internet gateway was created: igw-0041521199b8802ff - Test-VPC-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.

igw-0041521199b8802ff / Test-VPC-IGW

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-0041521199b8802ff	⊖ Detached	-	237042273450



Attach to VPC (igw-0041521199b8802ff) Info

VPC

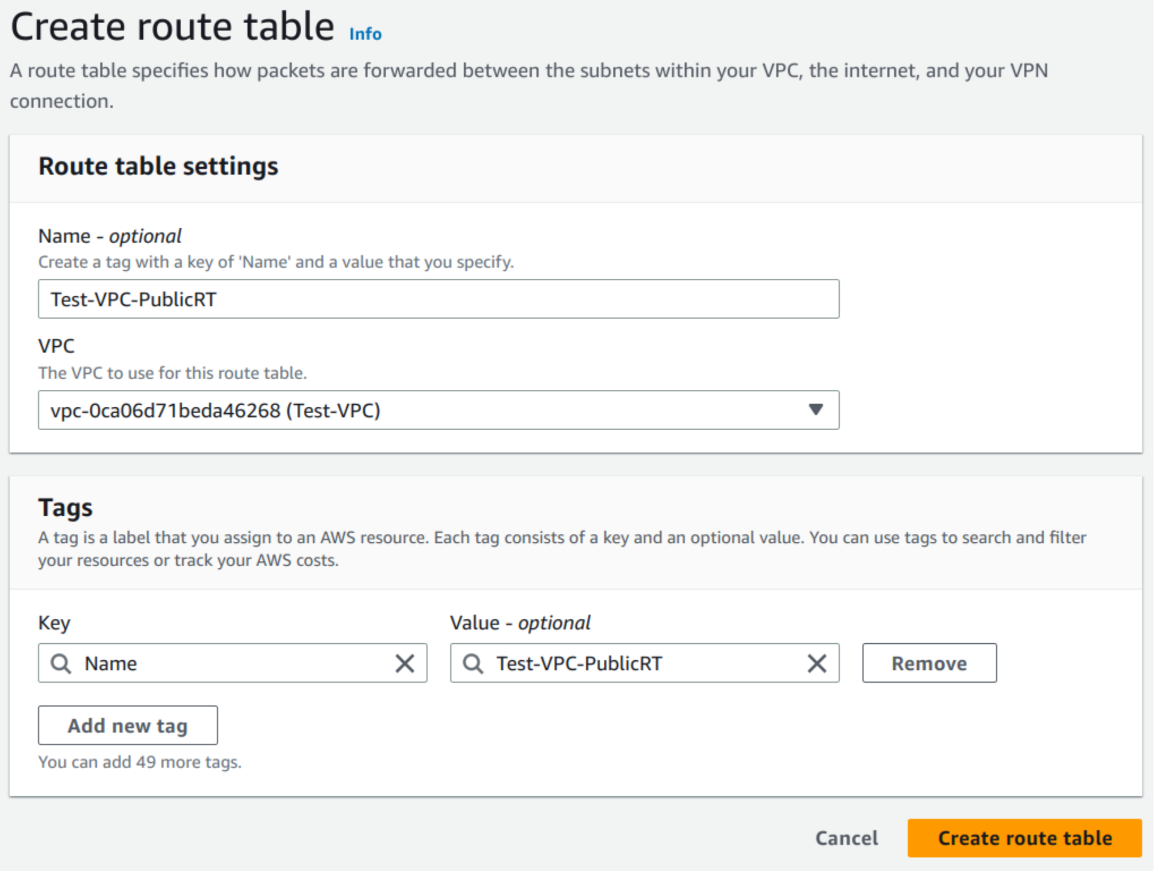
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

Select a VPC
vpc-0ca06d71beda46268 - Test-VPC
AWS Command Line Interface command
vpc-0ca06d71beda46268 - Test-VPC
Cancel
Attach internet gateway

Step 8 - Create a Route table for the public subnets.



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.

Test-VPC-PublicRT

VPC

The VPC to use for this route table.

vpc-0ca06d71beda46268 (Test-VPC)

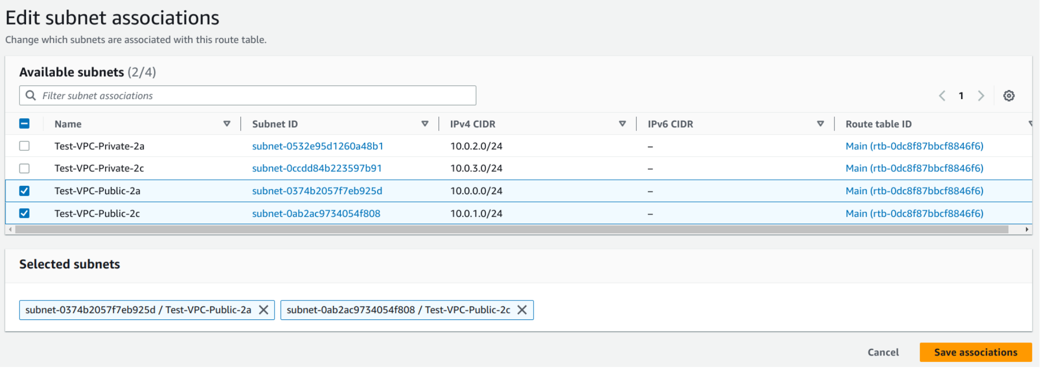
Tags

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	Test-VPC-PublicRT

You can add 49 more tags.

Step 9 - Edit the subnet association of the route table and routes to forward the internet faced traffic to the internet gateway.



Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

Filter subnet associations

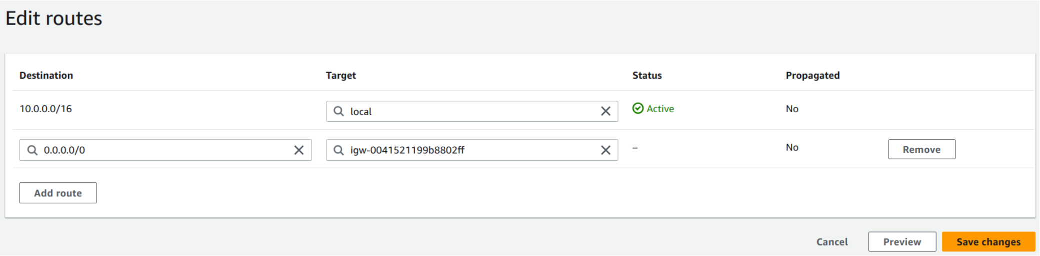
	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☐	Test-VPC-Private-2a	subnet-0532e95d1260a48b1	10.0.2.0/24	–	Main (rtb-0dc8f87bbcf8846f6)
☐	Test-VPC-Private-2c	subnet-0ccdd84b223597b91	10.0.3.0/24	–	Main (rtb-0dc8f87bbcf8846f6)
☑	Test-VPC-Public-2a	subnet-0374b2057f7eb925d	10.0.0.0/24	–	Main (rtb-0dc8f87bbcf8846f6)
☑	Test-VPC-Public-2c	subnet-0ab2ac9734054f808	10.0.1.0/24	–	Main (rtb-0dc8f87bbcf8846f6)

Selected subnets

subnet-0374b2057f7eb925d / Test-VPC-Public-2a

subnet-0ab2ac9734054f808 / Test-VPC-Public-2c

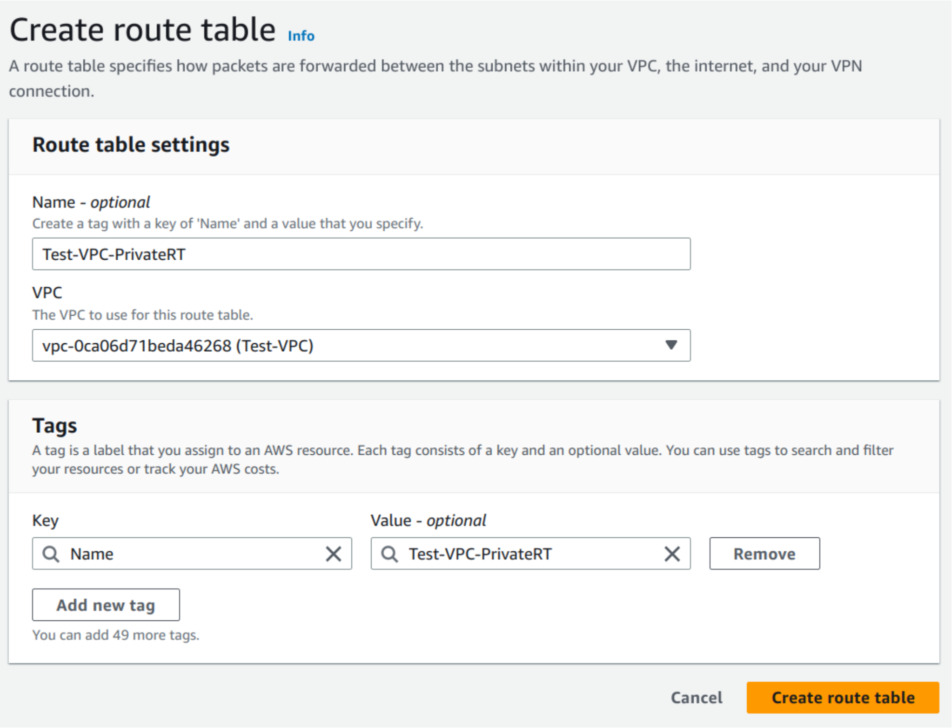
The default route shows that the traffic for the resources within the VPCs IPv4 CIDR range is forwarded to the local target.



Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-0041521199b8802ff	–	No

Step 10 - Create a Route table for private subnets.



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.

Test-VPC-PrivateRT

VPC

The VPC to use for this route table.

vpc-0ca06d71beda46268 (Test-VPC)

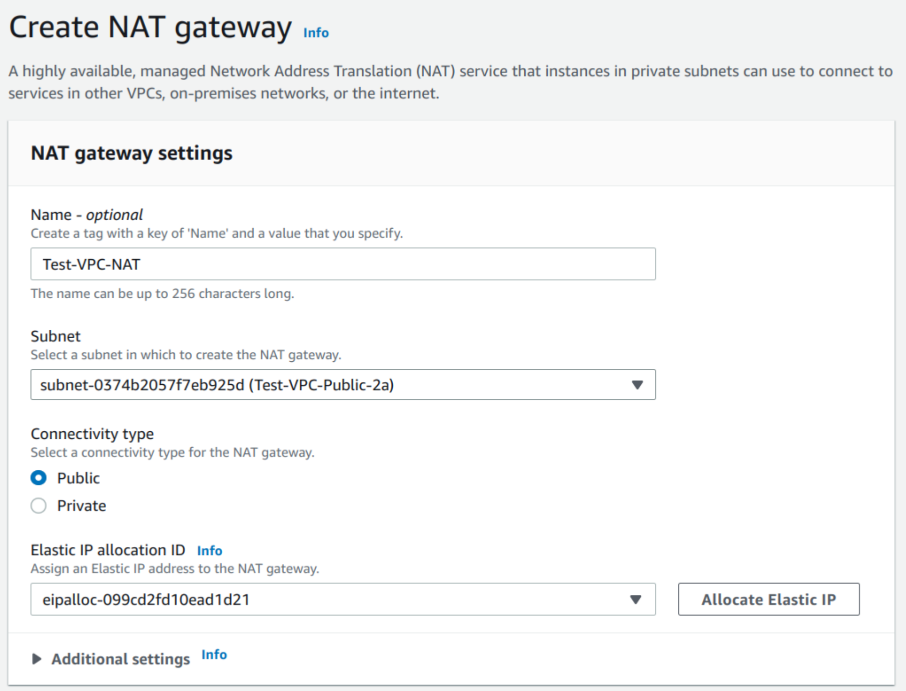
Tags

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	Test-VPC-PrivateRT

You can add 49 more tags.

Step 11 - Create a NAT gateway in one of the public subnet and allocate Elastic IP to it.



Create NAT gateway Info

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

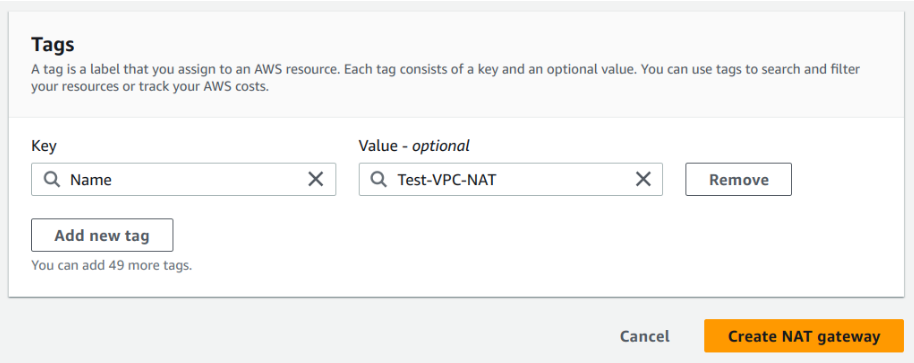
NAT gateway settings

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

Subnet
Select a subnet in which to create the NAT gateway.
subnet-0374b2057f7eb925d (Test-VPC-Public-2a) ▼

Connectivity type
Select a connectivity type for the NAT gateway.
● Public
○ Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
eipalloc-099cd2fd10ead1d21 ▼



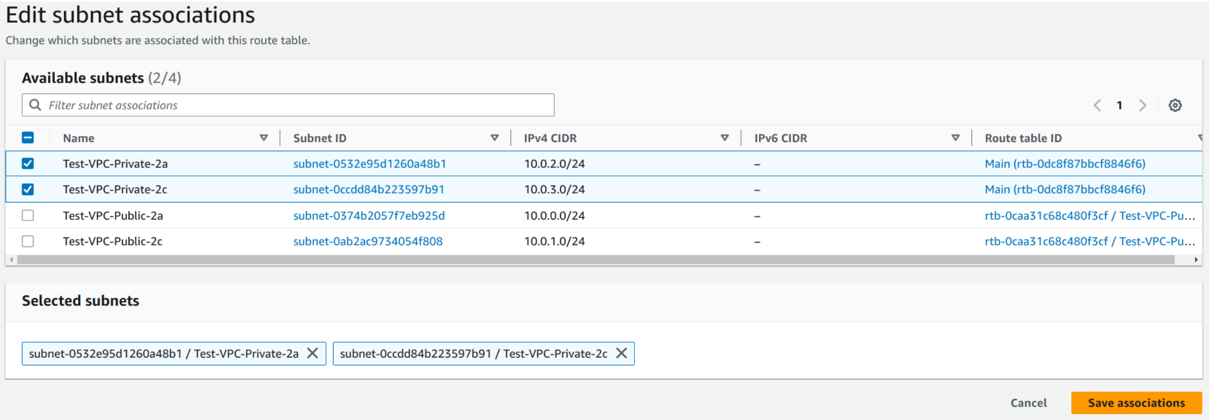
Tags

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	Test-VPC-NAT

You can add 49 more tags.

Step 12 - Edit subnet association for the private route table.



Edit subnet associations

Change which subnets are associated with this route table.

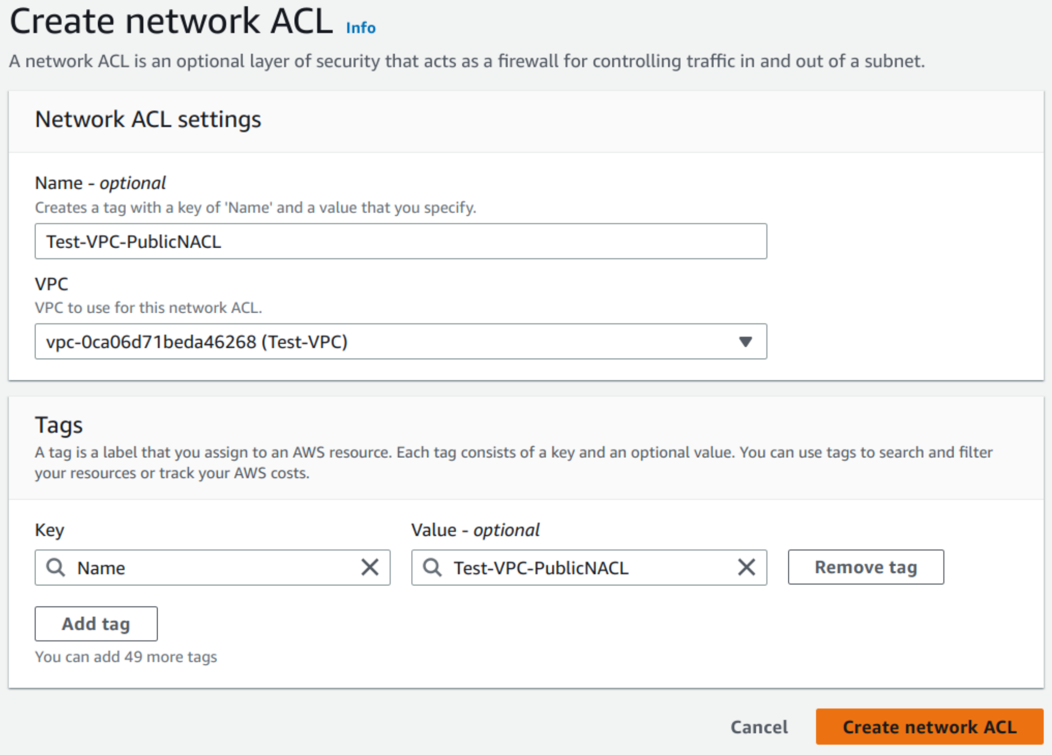
Available subnets (2/4)

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	Test-VPC-Private-2a	subnet-0532e95d1260a48b1	10.0.2.0/24	–	Main (rtb-0dc8f87bbcf8846f6)
☑	Test-VPC-Private-2c	subnet-0ccdd84b223597b91	10.0.3.0/24	–	Main (rtb-0dc8f87bbcf8846f6)
□	Test-VPC-Public-2a	subnet-0374b2057f7eb925d	10.0.0.0/24	–	rtb-0caa31c68c480f3cf / Test-VPC-Pu...
□	Test-VPC-Public-2c	subnet-0ab2ac9734054f808	10.0.1.0/24	–	rtb-0caa31c68c480f3cf / Test-VPC-Pu...

Selected subnets

subnet-0532e95d1260a48b1 / Test-VPC-Private-2a ✕ subnet-0ccdd84b223597b91 / Test-VPC-Private-2c ✕

Step 13 - Create NACL for a public subnet.



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*
Creates a tag with a key of 'Name' and a value that you specify.
Test-VPC-PublicNACL

VPC
VPC to use for this network ACL.
vpc-0ca06d71beda46268 (Test-VPC)

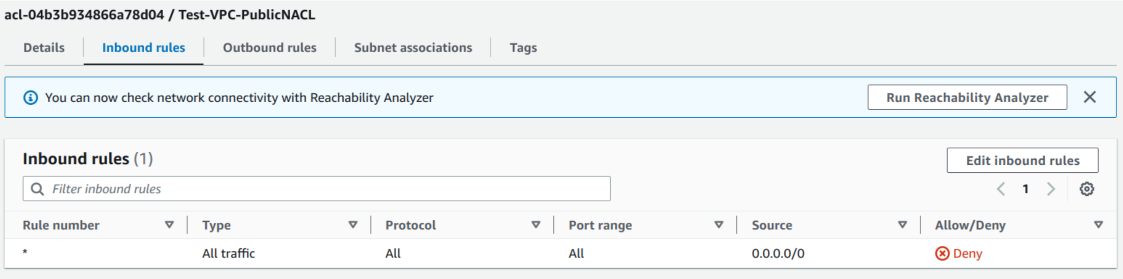
Tags

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	Test-VPC-PublicNACL

You can add 49 more tags

By default all the inbound traffic to the NACL is denied in custom NACL



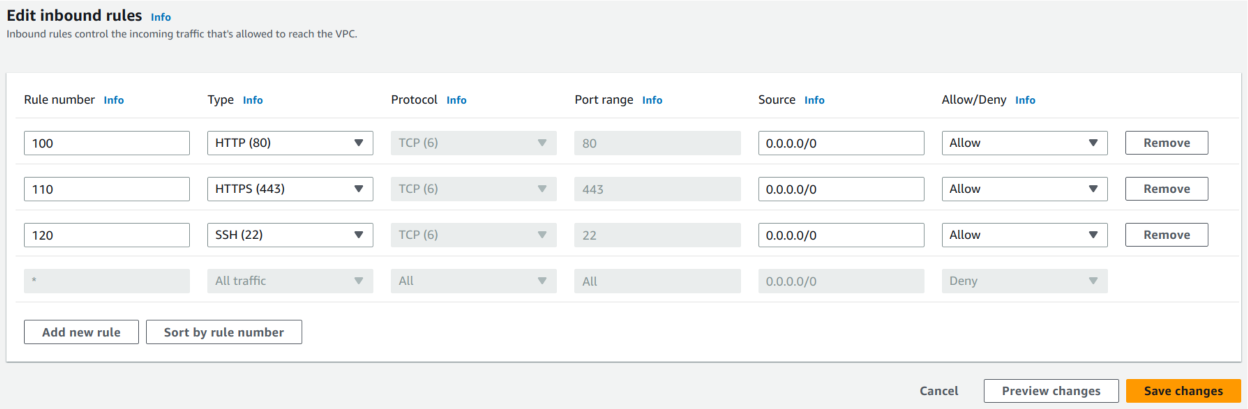
acl-04b3b934866a78d04 / Test-VPC-PublicNACL

You can now check network connectivity with Reachability Analyzer

Inbound rules (1)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

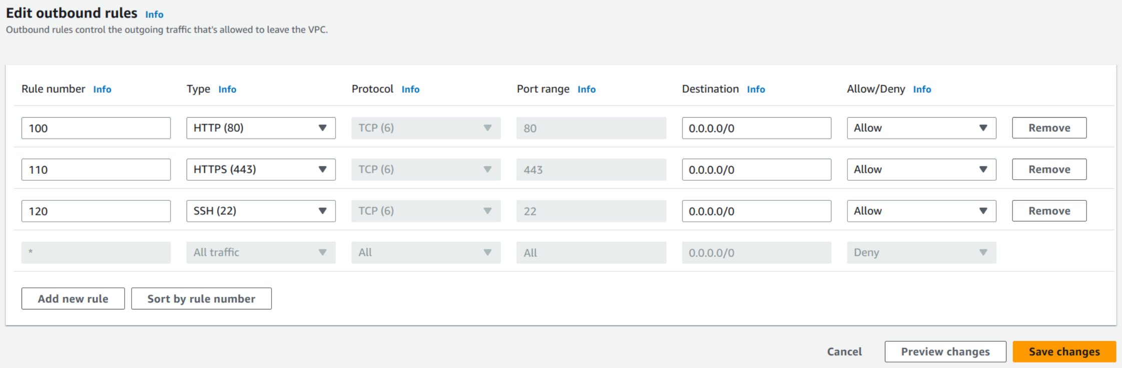
Step 14 - Edit inbound and outbound rules in NACL of a public subnet.



Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the VPC.

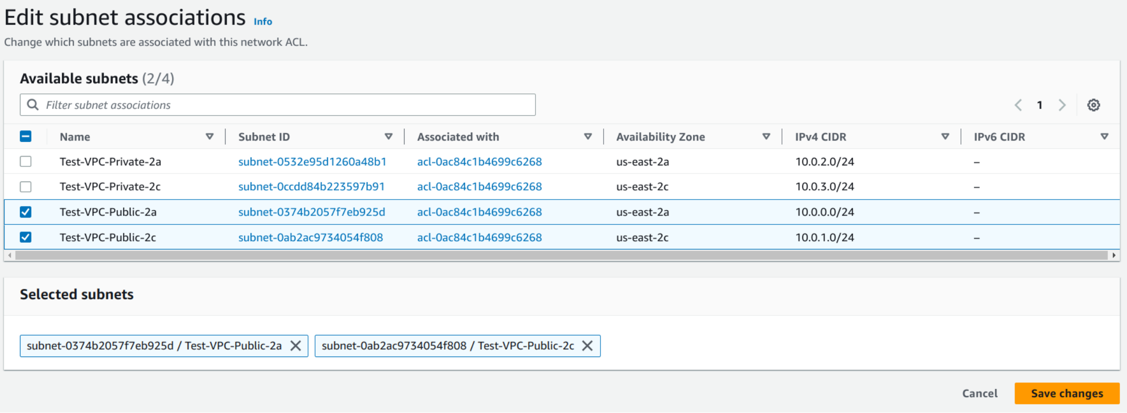
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
110	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow
120	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny



Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the VPC.

Rule number	Type	Protocol	Port range	Destination	Allow/Deny	
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow	Remove
110	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow	Remove
120	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	



Edit subnet associations Info

Change which subnets are associated with this network ACL.

Available subnets (2/4)

	Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
□	Test-VPC-Private-2a	subnet-0532e95d1260a48b1	acl-0ac84c1b4699c6268	us-east-2a	10.0.2.0/24	–
□	Test-VPC-Private-2c	subnet-0ccdd84b223597b91	acl-0ac84c1b4699c6268	us-east-2c	10.0.3.0/24	–
☑	Test-VPC-Public-2a	subnet-0374b2057f7eb925d	acl-0ac84c1b4699c6268	us-east-2a	10.0.0.0/24	–
☑	Test-VPC-Public-2c	subnet-0ab2ac9734054f808	acl-0ac84c1b4699c6268	us-east-2c	10.0.1.0/24	–

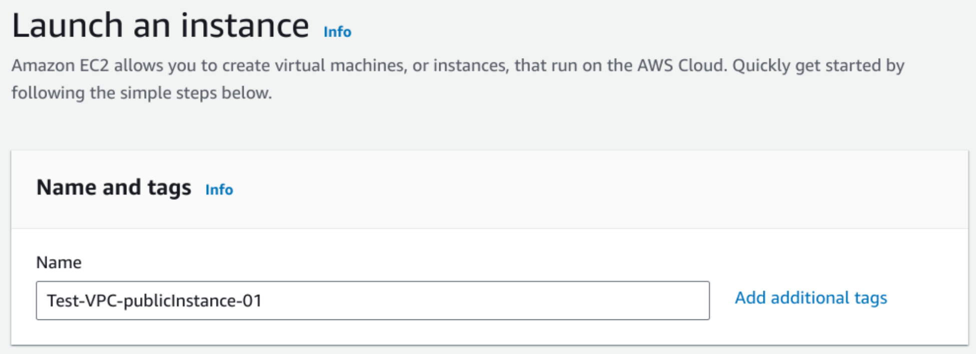
Selected subnets

subnet-0374b2057f7eb925d / Test-VPC-Public-2a

subnet-0ab2ac9734054f808 / Test-VPC-Public-2c

Step 15 - Browse to the EC2 console and launch a new instance with the following configurations.

- **Name:** “Test-VPC-publicInstance-01”
- **AMI:** Amazon Linux 2023
- **Instance type:** t2.micro
- **Key pair:** Create a new key pair - “publicInstancePem”
- **VPC:** Custom VPC created in previous steps
- **Subnet:** Public subnet - “Test-VPC-public-2a”
- **Auto-assign Public IP:** Enable
- **Security group:** Create new group, allow ssh, http, https, and ICMP.

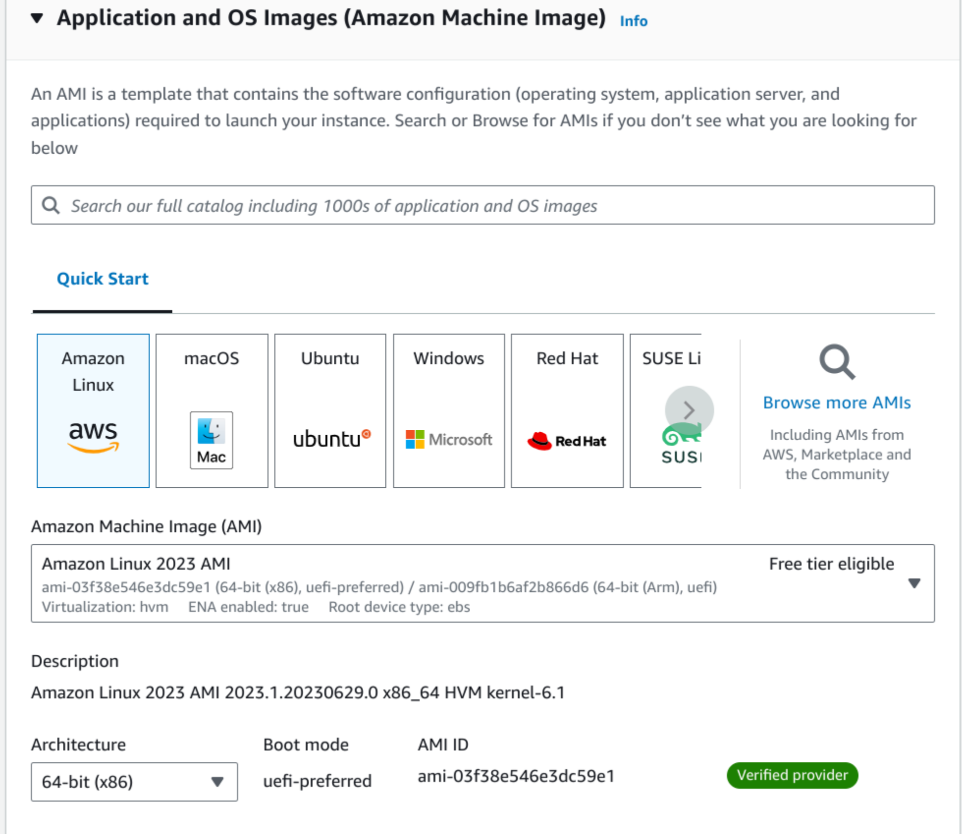


Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: Test-VPC-publicInstance-01



▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

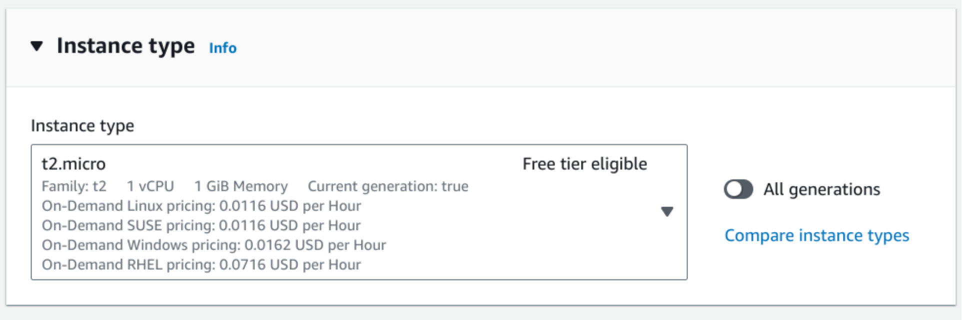
Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-03f38e546e3dc59e1 (64-bit (x86), uefi-preferred) / ami-009fb1b6af2b866d6 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.1.20230629.0 x86_64 HVM kernel-6.1

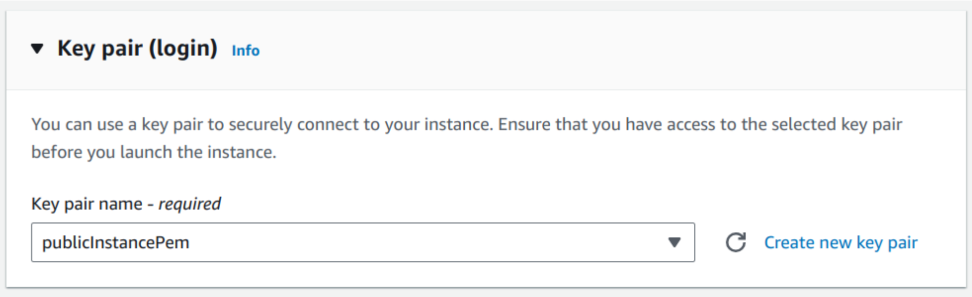
Architecture	Boot mode	AMI ID	
64-bit (x86) ▼	uefi-preferred	ami-03f38e546e3dc59e1	Verified provider



▼ Instance type Info

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour

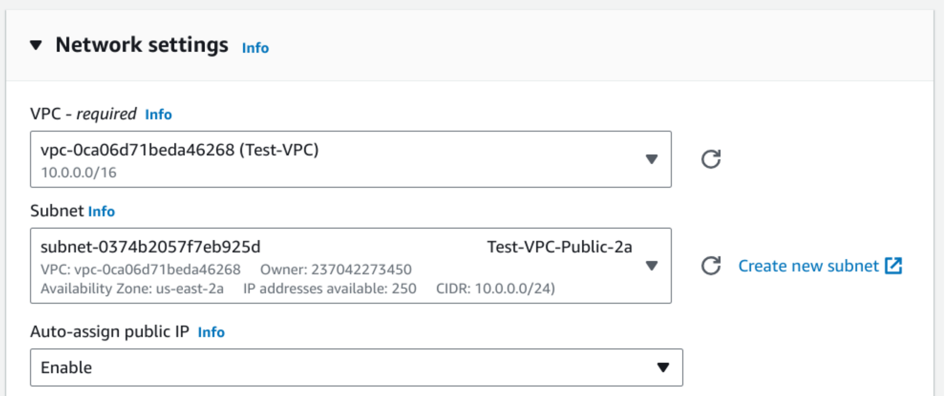


▼ Key pair (login) Info

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*

publicInstancePem ▼



▼ **Network settings** Info

VPC - *required* Info

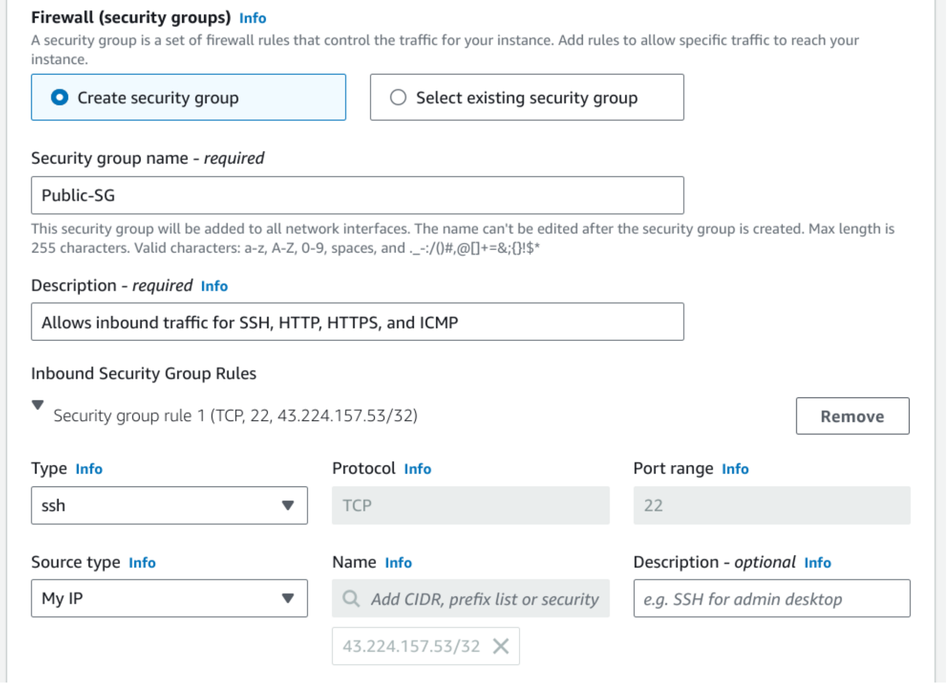
vpc-0ca06d71beda46268 (Test-VPC)
10.0.0.0/16

Subnet Info

subnet-0374b2057f7eb925d Test-VPC-Public-2a
VPC: vpc-0ca06d71beda46268 Owner: 237042273450
Availability Zone: us-east-2a IP addresses available: 250 CIDR: 10.0.0.0/24)

Auto-assign public IP Info

Enable



Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*

Public-SG

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

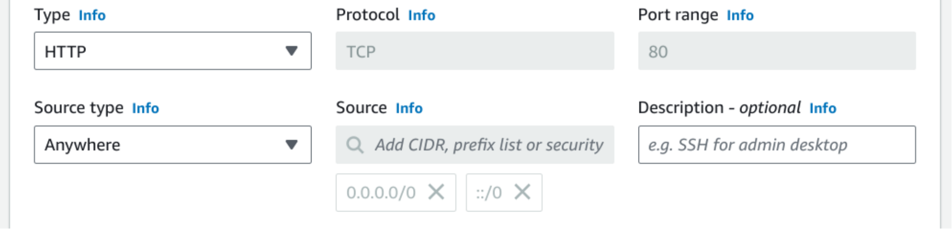
Description - *required* Info

Allows inbound traffic for SSH, HTTP, HTTPS, and ICMP

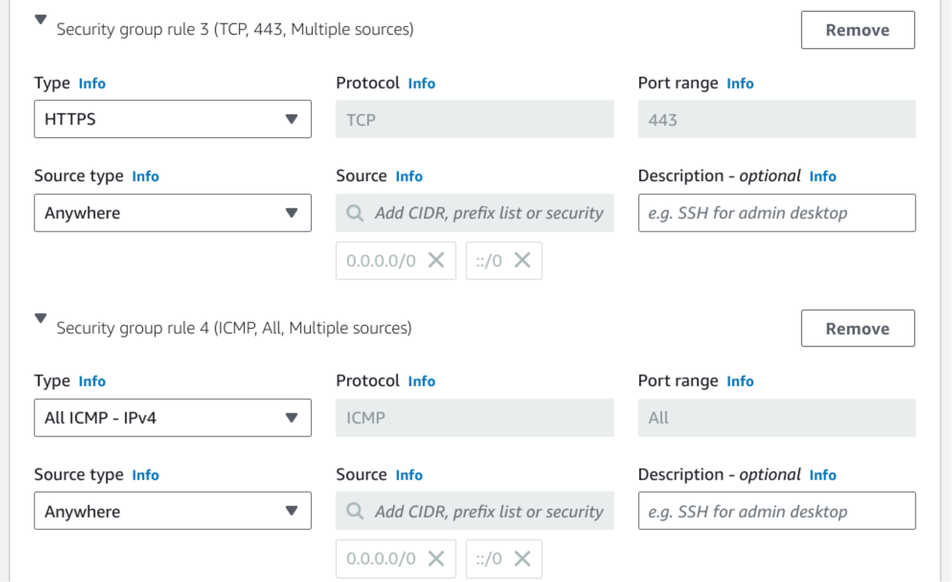
Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 43.224.157.53/32)

Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Name Info	Description - *optional* Info
My IP	Add CIDR, prefix list or security 43.224.157.53/32 ✕	e.g. SSH for admin desktop



Type Info	Protocol Info	Port range Info
HTTP	TCP	80
Source type Info	Source Info	Description - *optional* Info
Anywhere	Add CIDR, prefix list or security 0.0.0.0/0 ✕ ::/0 ✕	e.g. SSH for admin desktop



▼ Security group rule 3 (TCP, 443, Multiple sources)

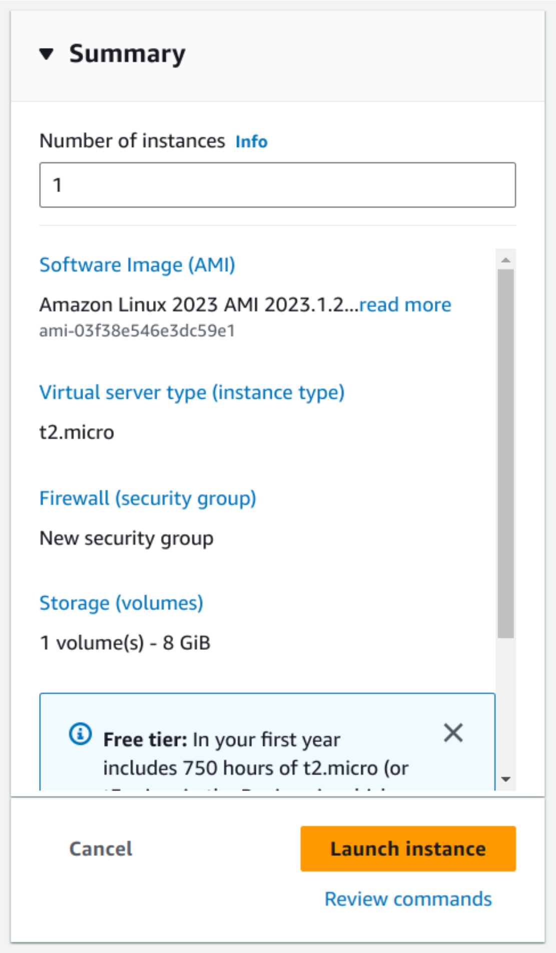
Type Info	Protocol Info	Port range Info
HTTPS ▼	TCP	443

Source type Info	Source Info	Description - *optional* Info
Anywhere ▼	*Add CIDR, prefix list or security* 0.0.0.0/0 ✕ ::/0 ✕	*e.g. SSH for admin desktop*

▼ Security group rule 4 (ICMP, All, Multiple sources)

Type Info	Protocol Info	Port range Info
All ICMP - IPv4 ▼	ICMP	All

Source type Info	Source Info	Description - *optional* Info
Anywhere ▼	*Add CIDR, prefix list or security* 0.0.0.0/0 ✕ ::/0 ✕	*e.g. SSH for admin desktop*



▼ **Summary**

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.1.2...read more
ami-03f38e546e3dc59e1

Virtual server type (instance type)

t2.micro

Firewall (security group)

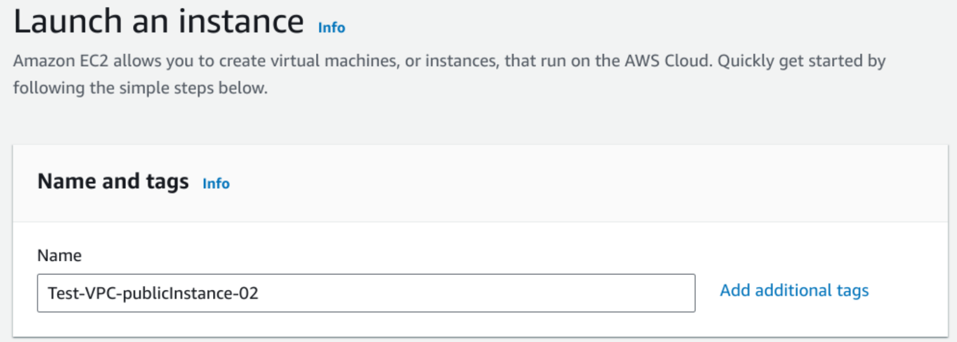
New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year
includes 750 hours of t2.micro (or

- **Name:** “Test-VPC-publicInstance-02”
- **AMI:** Amazon Linux 2023
- **Instance type:** t2.micro
- **Key pair:** Create a new key pair - “publicInstancePem”
- **VPC:** Custom VPC created in previous steps
- **Subnet:** Public subnet - “Test-VPC-public-2c”
- **Auto-assign Public IP:** Enable
- **Security group:** Use existing security group “Public-SG”



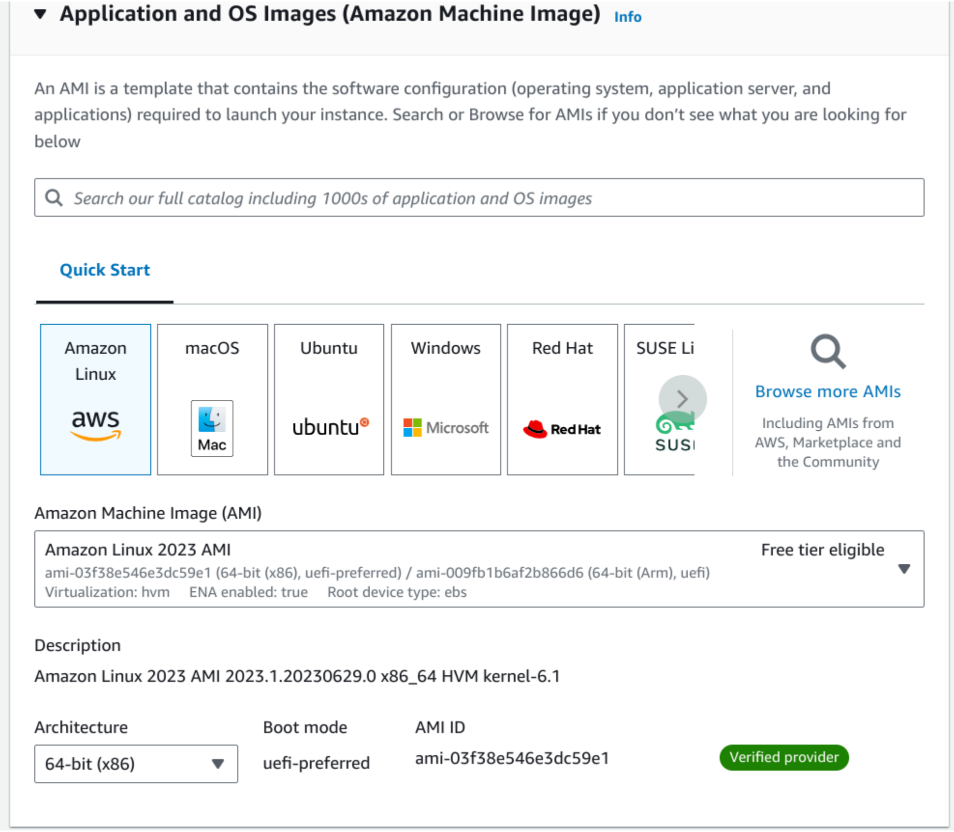
Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

Test-VPC-publicInstance-02



▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don’t see what you are looking for below

Search our full catalog including 1000s of application and OS images
Quick Start
Amazon Linux
aws
macOS
Mac
Ubuntu
ubuntu
Windows
Microsoft
Red Hat
Red Hat
SUSE Li
SUSE
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible
ami-03f38e546e3dc59e1 (64-bit (x86), uefi-preferred) / ami-009fb1b6af2b866d6 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

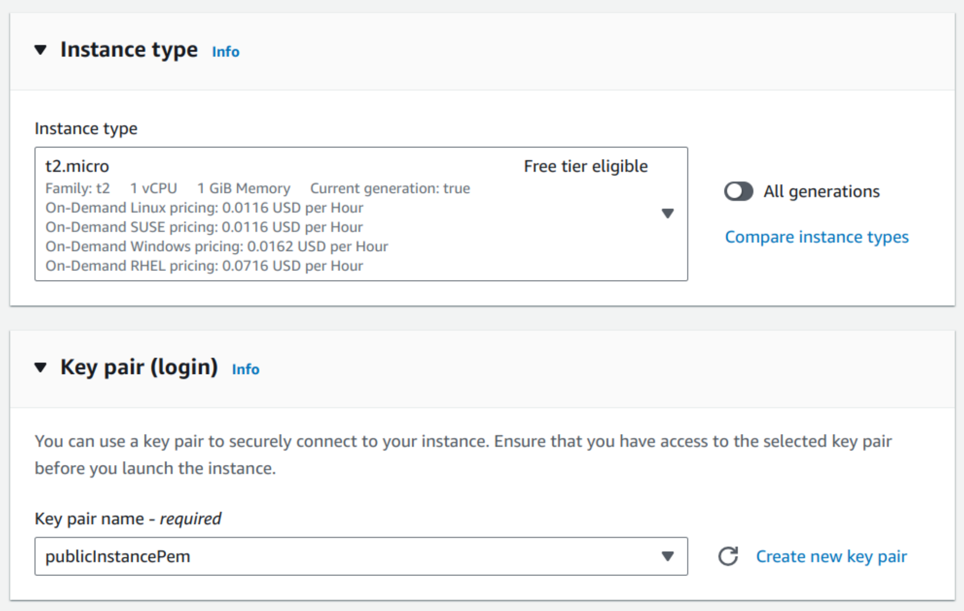
Description

Amazon Linux 2023 AMI 2023.1.20230629.0 x86_64 HVM kernel-6.1

Architecture: 64-bit (x86)

Boot mode: uefi-preferred

AMI ID: ami-03f38e546e3dc59e1



▼ **Instance type** Info

Instance type

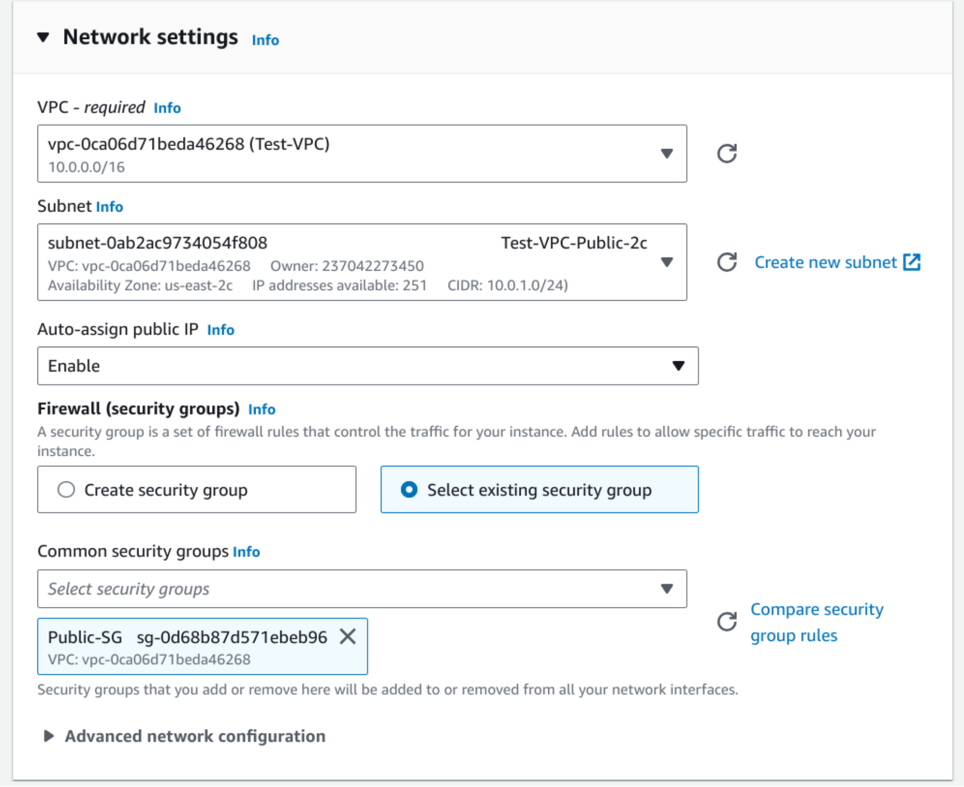
t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour

▼ **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*

publicInstancePem



▼ **Network settings** Info

VPC - *required* Info

vpc-0ca06d71beda46268 (Test-VPC)
10.0.0.0/16

Subnet Info

subnet-0ab2ac9734054f808 Test-VPC-Public-2c
VPC: vpc-0ca06d71beda46268 Owner: 237042273450
Availability Zone: us-east-2c IP addresses available: 251 CIDR: 10.0.1.0/24)

Auto-assign public IP Info

Enable

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

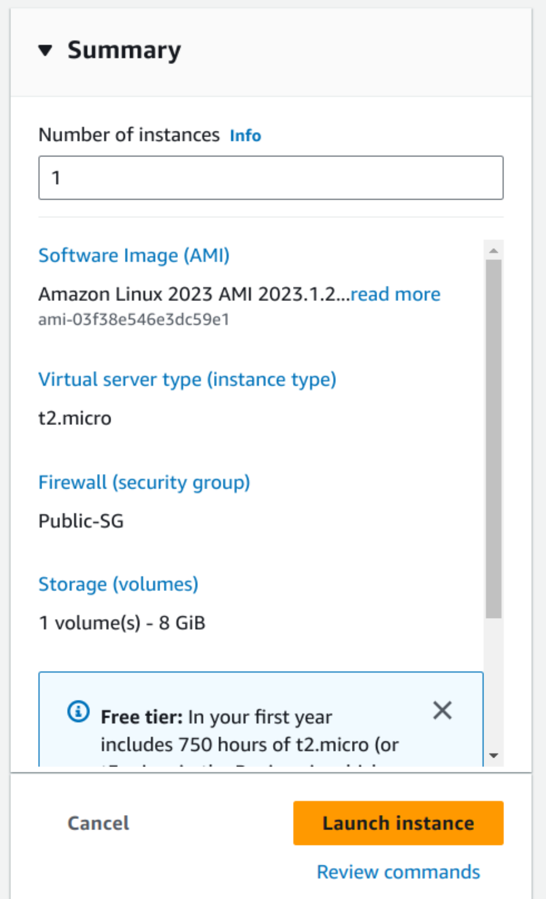
Common security groups Info

Select security groups

Public-SG sg-0d68b87d571ebeb96 ✕
VPC: vpc-0ca06d71beda46268

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 2023.1.2...read more
ami-03f38e546e3dc59e1

Virtual server type (instance type)

t2.micro

Firewall (security group)

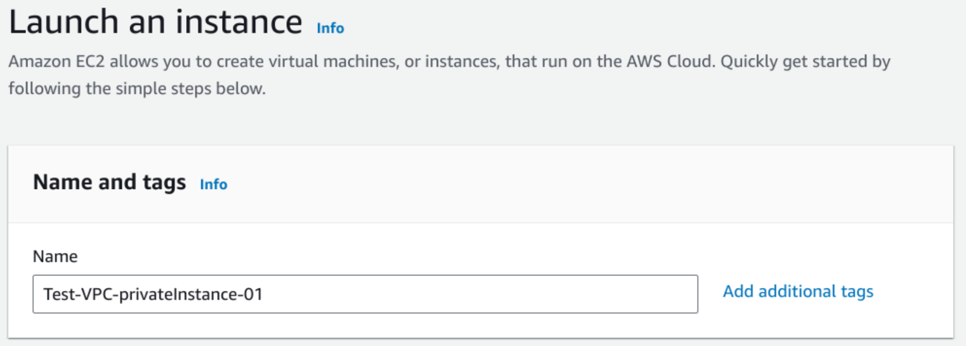
Public-SG

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or

- **Name:** “Test-VPC-privateInstance-01”
- **AMI:** Amazon Linux 2023
- **Instance type:** t2.micro
- **Key pair:** Create a new key pair - “privateInstancePem”
- **VPC:** Custom VPC created in previous steps
- **Subnet:** Private subnet - “Test-VPC-Private-2a”
- **Auto-assign Public IP:** Disable
- **Security group:** Create a new security group and allow SSH, and ICMP from public and private security groups.



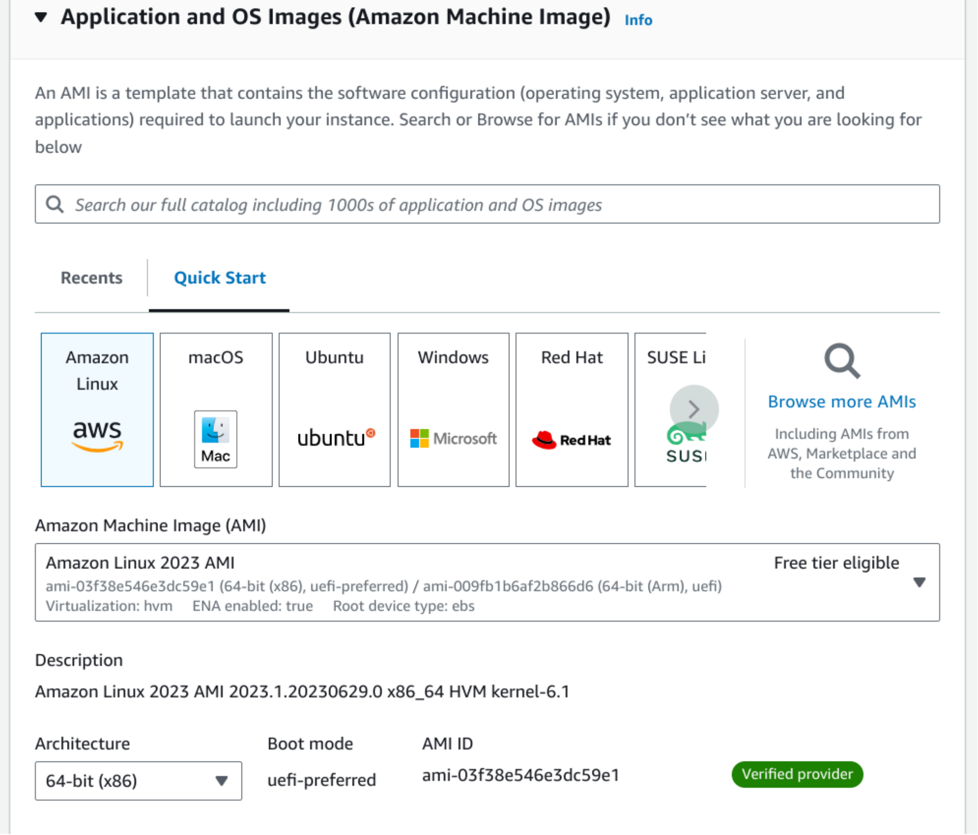
Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

Test-VPC-privateInstance-01



▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

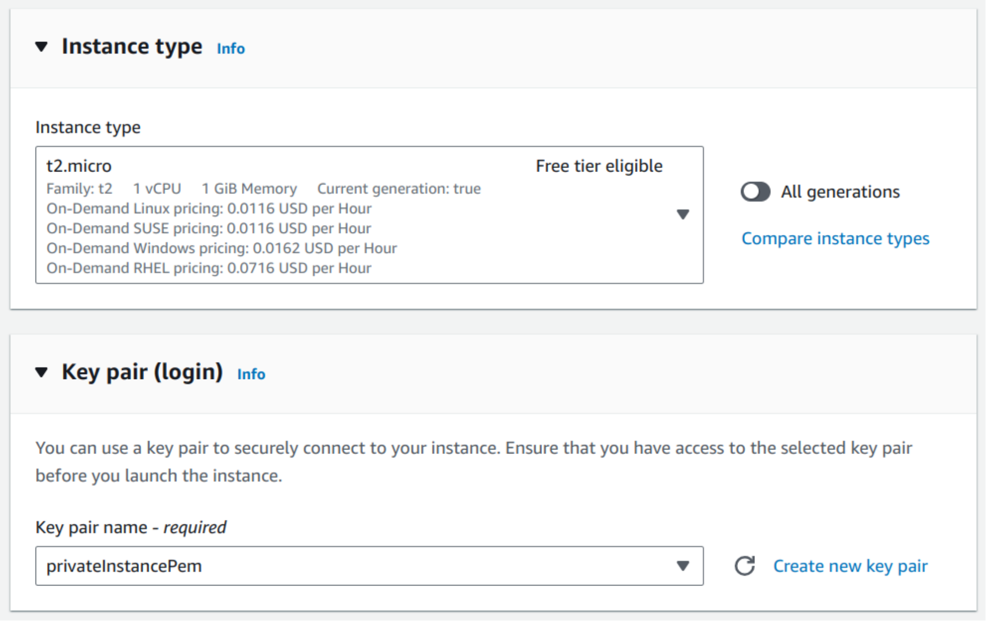
Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible
ami-03f38e546e3dc59e1 (64-bit (x86), uefi-preferred) / ami-009fb1b6af2b866d6 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.1.20230629.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	
64-bit (x86) ▼	uefi-preferred	ami-03f38e546e3dc59e1	Verified provider



▼ Instance type Info

Instance type

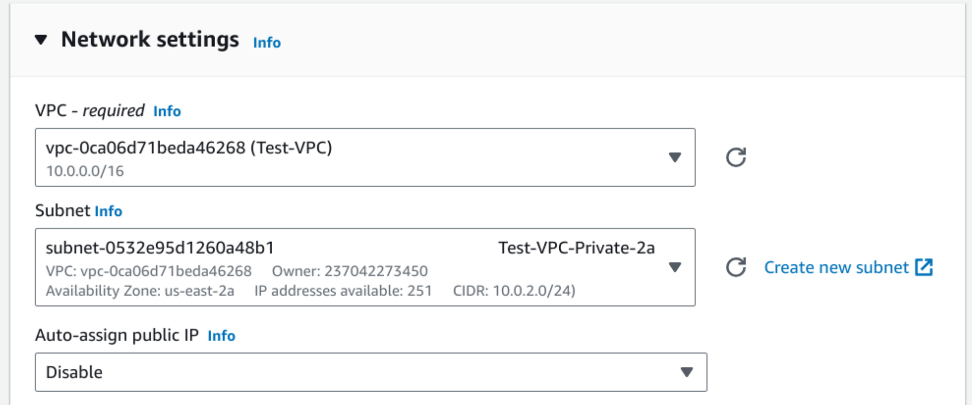
t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour

▼ 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*

privateInstancePem ▼



▼ **Network settings** Info

VPC - *required* Info

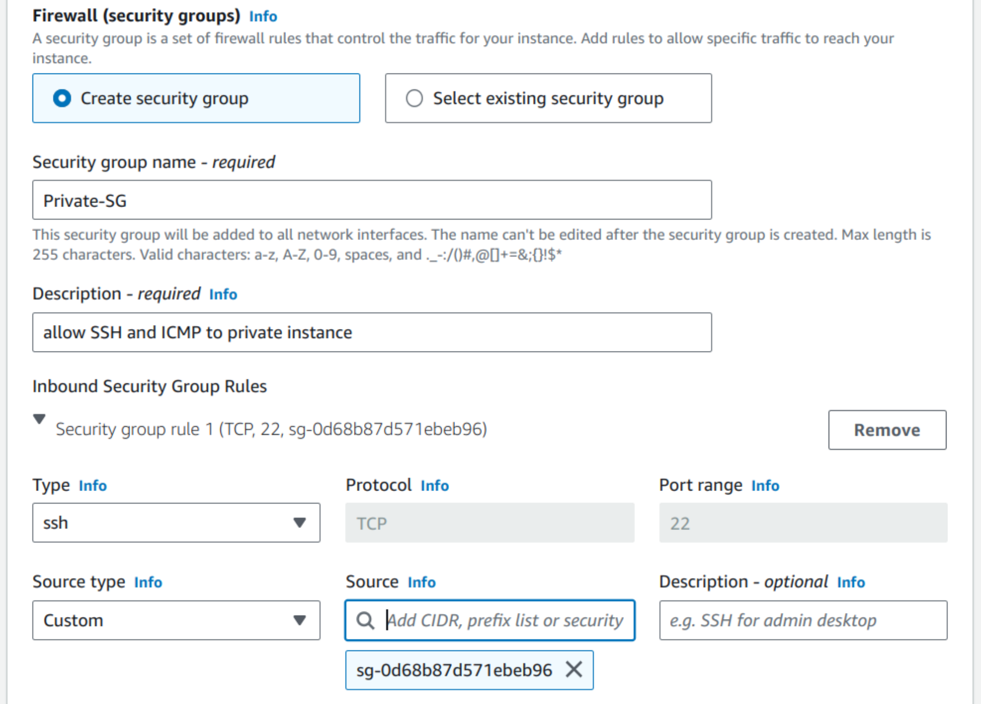
vpc-0ca06d71beda46268 (Test-VPC)
10.0.0.0/16

Subnet Info

subnet-0532e95d1260a48b1 Test-VPC-Private-2a
VPC: vpc-0ca06d71beda46268 Owner: 237042273450
Availability Zone: us-east-2a IP addresses available: 251 CIDR: 10.0.2.0/24)

Auto-assign public IP Info

Disable



Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*

Private-SG

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

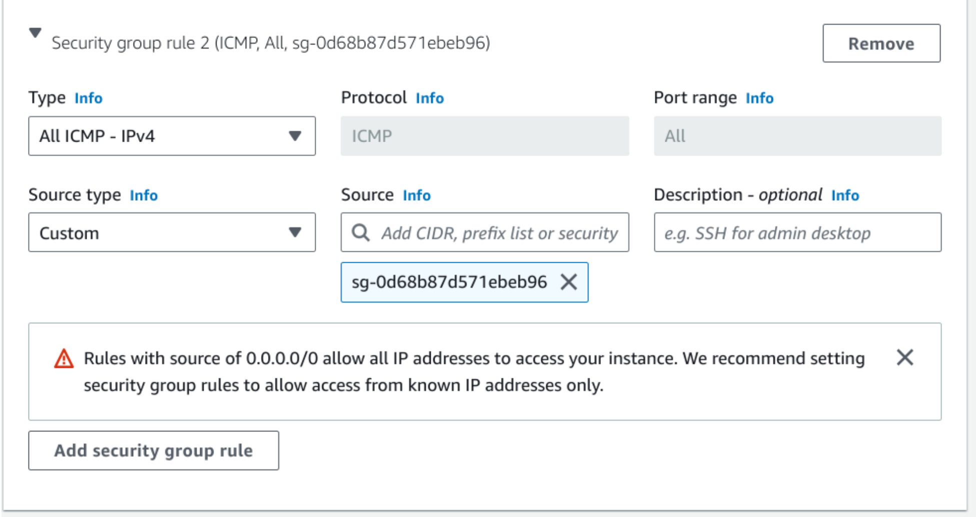
allow SSH and ICMP to private instance

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, sg-0d68b87d571ebeb96)

Type Info	Protocol Info	Port range Info
ssh	TCP	22

Source type Info	Source Info	Description - *optional* Info
Custom	*Add CIDR, prefix list or security* sg-0d68b87d571ebeb96 ✕	*e.g. SSH for admin desktop*

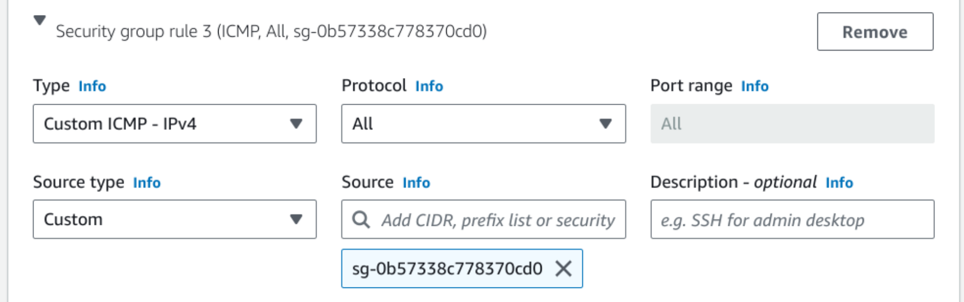


▼ Security group rule 2 (ICMP, All, sg-0d68b87d571ebeb96)

Type Info	Protocol Info	Port range Info
All ICMP - IPv4	ICMP	All

Source type Info	Source Info	Description - *optional* Info
Custom	*Add CIDR, prefix list or security* sg-0d68b87d571ebeb96 ✕	*e.g. SSH for admin desktop*

⚠ 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. ✕



Security group rule 3 (ICMP, All, sg-0b57338c778370cd0)

Type: Custom ICMP - IPv4

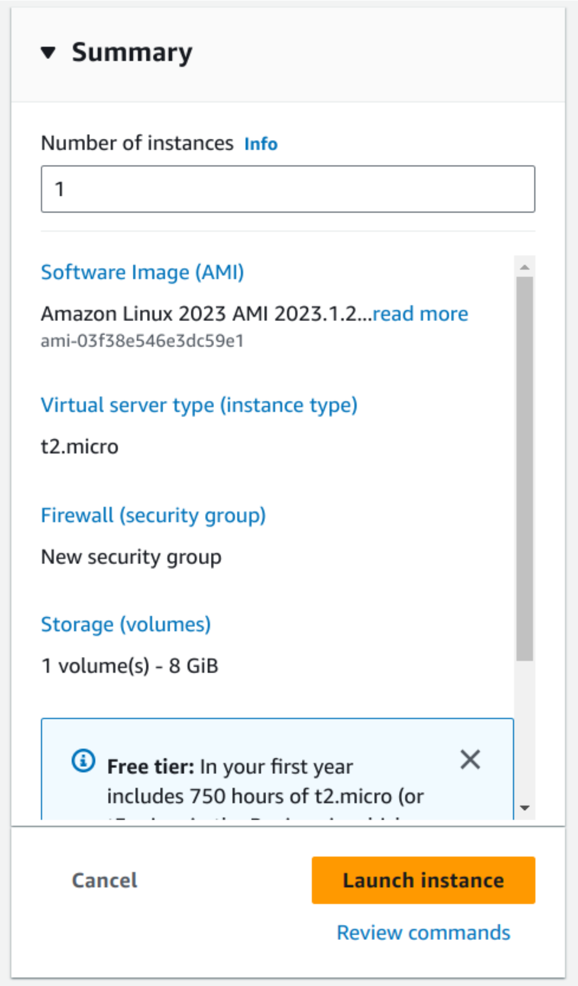
Protocol: All

Port range: All

Source type: Custom

Source: sg-0b57338c778370cd0

Description - *optional*: *e.g. SSH for admin desktop*



Summary

Number of instances: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.1.2...read more
ami-03f38e546e3dc59e1

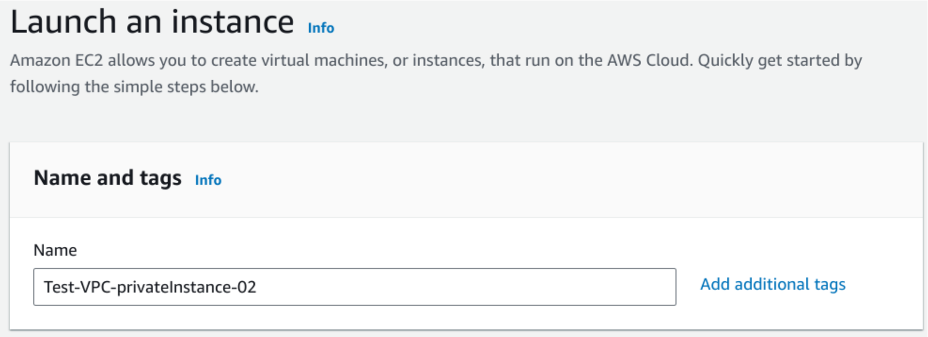
Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

Free tier: In your first year includes 750 hours of t2.micro (or

- **Name:** “Test-VPC-privateInstance-02”
- **AMI:** Amazon Linux 2023
- **Instance type:** t2.micro
- **Key pair:** Create a new key pair - “privateInstancePem”
- **VPC:** Custom VPC created in previous steps
- **Subnet:** Private subnet - “Test-VPC-Private-2c”
- **Auto-assign Public IP:** Disable
- **Security group:** Select the existing “Private-SG” security group.



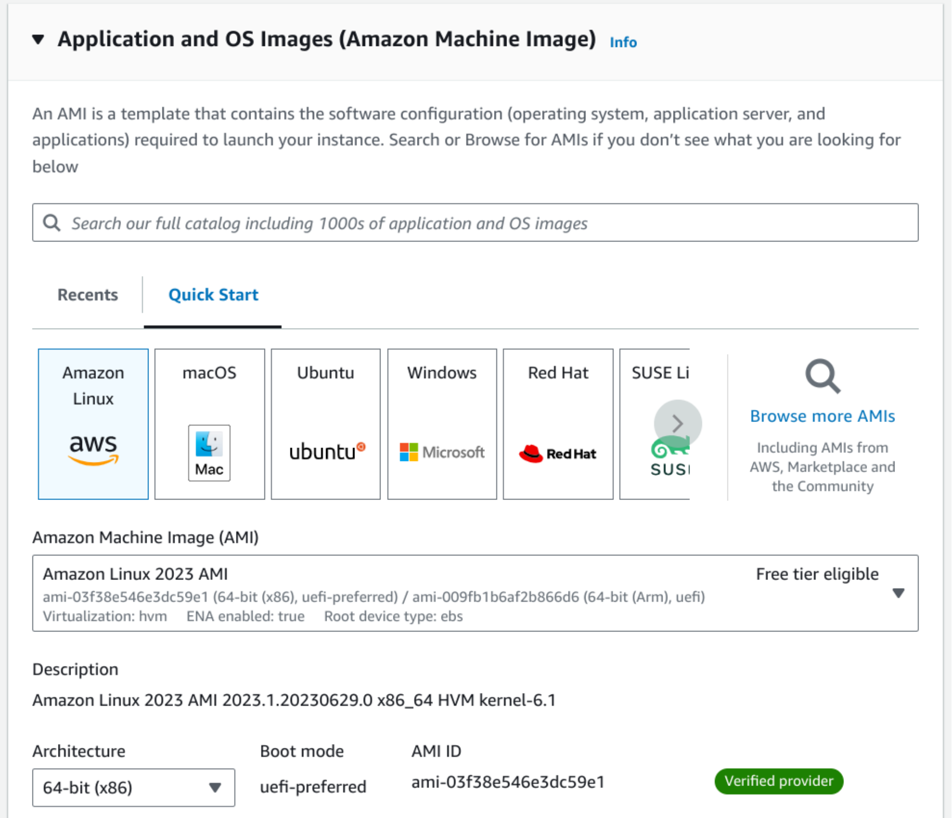
Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

Test-VPC-privateInstance-02



▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

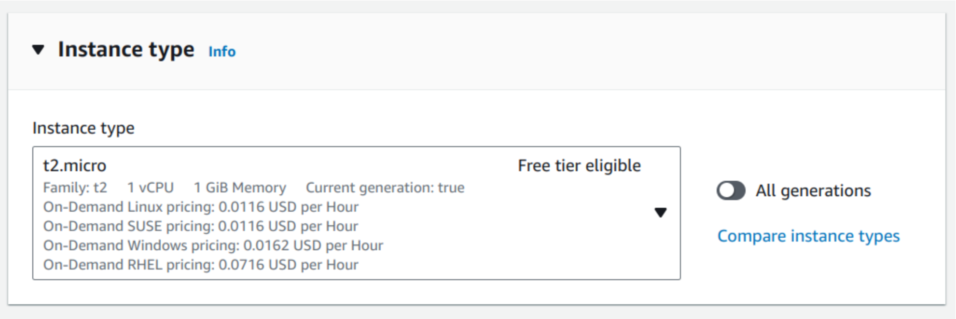
Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible
ami-03f38e546e3dc59e1 (64-bit (x86), uefi-preferred) / ami-009fb1b6af2b866d6 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.1.20230629.0 x86_64 HVM kernel-6.1

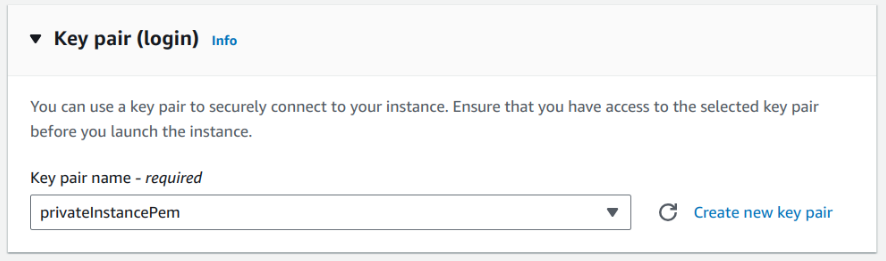
Architecture	Boot mode	AMI ID	
64-bit (x86) ▼	uefi-preferred	ami-03f38e546e3dc59e1	Verified provider



▼ Instance type Info

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour

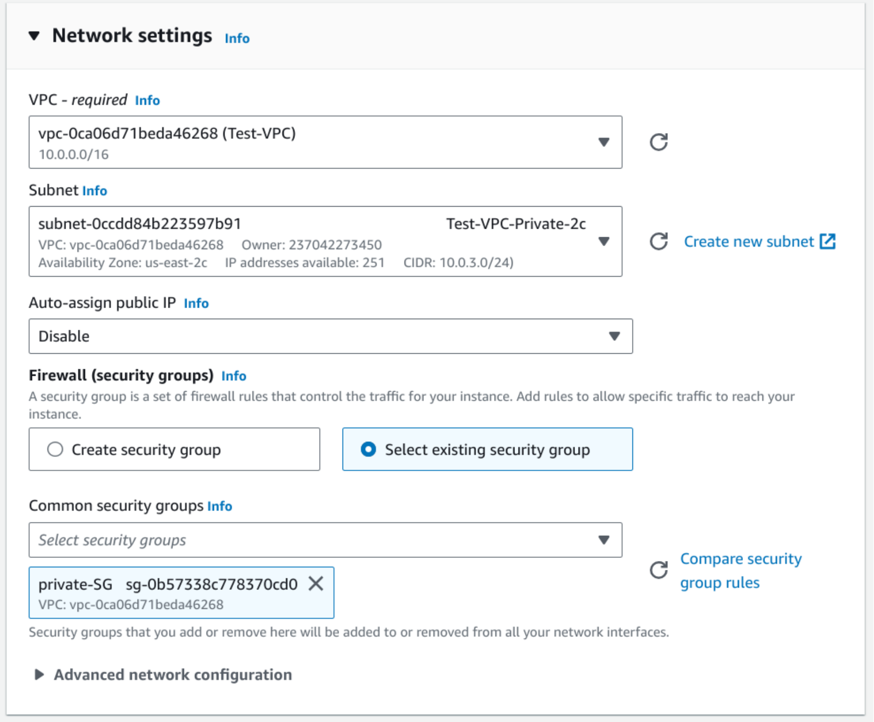


▼ **Key pair (login)** Info

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*

privateInstancePem ▼



▼ **Network settings** Info

VPC - *required* Info

vpc-0ca06d71beda46268 (Test-VPC)
10.0.0.0/16 ▼

Subnet Info

subnet-0ccdd84b223597b91 Test-VPC-Private-2c
VPC: vpc-0ca06d71beda46268 Owner: 237042273450
Availability Zone: us-east-2c IP addresses available: 251 CIDR: 10.0.3.0/24) ▼

Auto-assign public IP Info

Disable ▼

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group ● Select existing security group

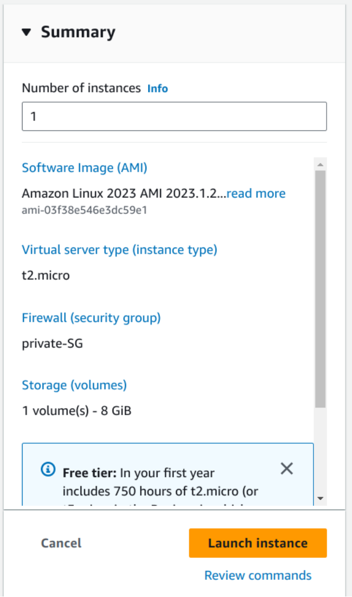
Common security groups Info

Select security groups ▼

private-SG sg-0b57338c778370cd0 ✕
VPC: vpc-0ca06d71beda46268

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 2023.1.2...read more
ami-03f38e546e3dc59e1

Virtual server type (instance type)
t2.micro

Firewall (security group)
private-SG

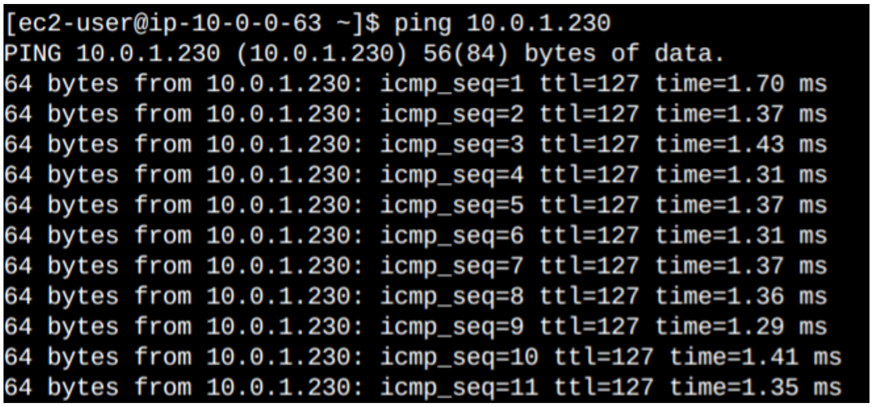
Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or

Step 16 - Use ping command with the private IP addresses of the instances to check if the instances within the VPC are able to communicate with each other.

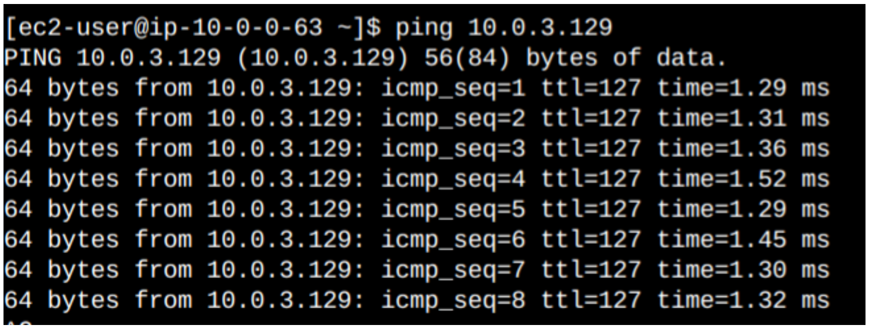
For this the security group of the instances should allow traffic for ICMP.

1. **Ping the public instance "*Test-VPC-publicInstance-02*" with private IP - 10.0.1.230, from the public instance "*Test-VPC-publicInstance-01*".**



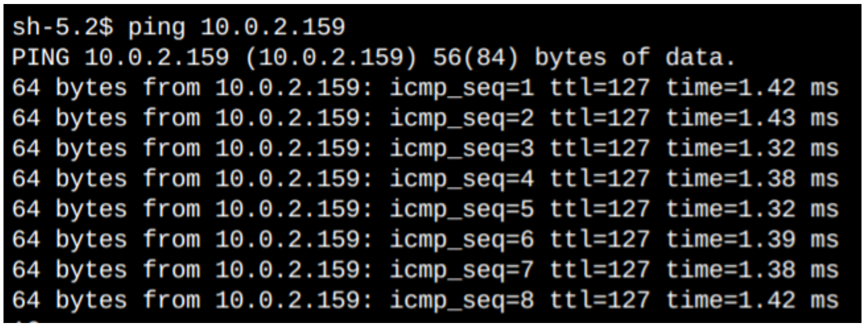
```
[ec2-user@ip-10-0-0-63 ~]$ ping 10.0.1.230
PING 10.0.1.230 (10.0.1.230) 56(84) bytes of data.
64 bytes from 10.0.1.230: icmp_seq=1 ttl=127 time=1.70 ms
64 bytes from 10.0.1.230: icmp_seq=2 ttl=127 time=1.37 ms
64 bytes from 10.0.1.230: icmp_seq=3 ttl=127 time=1.43 ms
64 bytes from 10.0.1.230: icmp_seq=4 ttl=127 time=1.31 ms
64 bytes from 10.0.1.230: icmp_seq=5 ttl=127 time=1.37 ms
64 bytes from 10.0.1.230: icmp_seq=6 ttl=127 time=1.31 ms
64 bytes from 10.0.1.230: icmp_seq=7 ttl=127 time=1.37 ms
64 bytes from 10.0.1.230: icmp_seq=8 ttl=127 time=1.36 ms
64 bytes from 10.0.1.230: icmp_seq=9 ttl=127 time=1.29 ms
64 bytes from 10.0.1.230: icmp_seq=10 ttl=127 time=1.41 ms
64 bytes from 10.0.1.230: icmp_seq=11 ttl=127 time=1.35 ms
```

2. **Ping the private instance "*Test-VPC-privateInstance-02*" with private IP - 10.0.3.129, from the public instance "*Test-VPC-publicInstance-01*".**



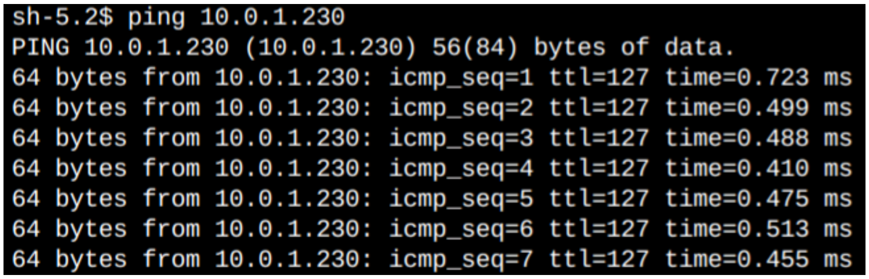
```
[ec2-user@ip-10-0-0-63 ~]$ ping 10.0.3.129
PING 10.0.3.129 (10.0.3.129) 56(84) bytes of data.
64 bytes from 10.0.3.129: icmp_seq=1 ttl=127 time=1.29 ms
64 bytes from 10.0.3.129: icmp_seq=2 ttl=127 time=1.31 ms
64 bytes from 10.0.3.129: icmp_seq=3 ttl=127 time=1.36 ms
64 bytes from 10.0.3.129: icmp_seq=4 ttl=127 time=1.52 ms
64 bytes from 10.0.3.129: icmp_seq=5 ttl=127 time=1.29 ms
64 bytes from 10.0.3.129: icmp_seq=6 ttl=127 time=1.45 ms
64 bytes from 10.0.3.129: icmp_seq=7 ttl=127 time=1.30 ms
64 bytes from 10.0.3.129: icmp_seq=8 ttl=127 time=1.32 ms
```

3. **Ping the private instance "*Test-VPC-privateInstance-01*" with private IP - 10.0.2.159, from the private instance "*Test-VPC-privateInstance-02*".**



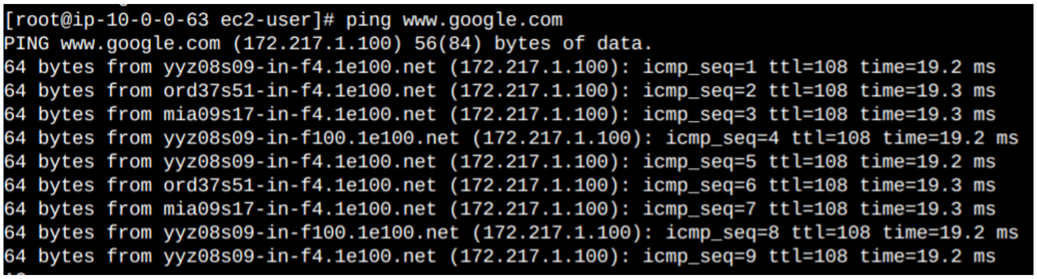
```
sh-5.2$ ping 10.0.2.159
PING 10.0.2.159 (10.0.2.159) 56(84) bytes of data.
64 bytes from 10.0.2.159: icmp_seq=1 ttl=127 time=1.42 ms
64 bytes from 10.0.2.159: icmp_seq=2 ttl=127 time=1.43 ms
64 bytes from 10.0.2.159: icmp_seq=3 ttl=127 time=1.32 ms
64 bytes from 10.0.2.159: icmp_seq=4 ttl=127 time=1.38 ms
64 bytes from 10.0.2.159: icmp_seq=5 ttl=127 time=1.32 ms
64 bytes from 10.0.2.159: icmp_seq=6 ttl=127 time=1.39 ms
64 bytes from 10.0.2.159: icmp_seq=7 ttl=127 time=1.38 ms
64 bytes from 10.0.2.159: icmp_seq=8 ttl=127 time=1.42 ms
```

4. **Ping the public instance “*Test-VPC-publicInstance-02*” with private IP - 10.0.1.230, from the private instance “*Test-VPC-privateInstance-02*”.**

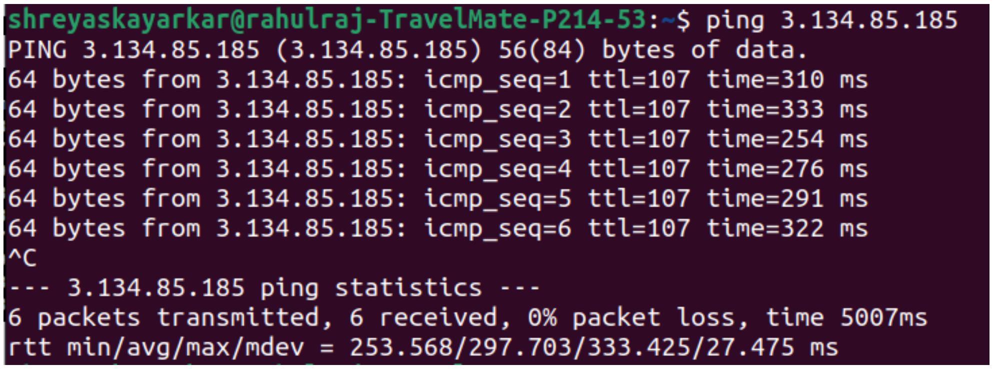


```
sh-5.2$ ping 10.0.1.230
PING 10.0.1.230 (10.0.1.230) 56(84) bytes of data.
64 bytes from 10.0.1.230: icmp_seq=1 ttl=127 time=0.723 ms
64 bytes from 10.0.1.230: icmp_seq=2 ttl=127 time=0.499 ms
64 bytes from 10.0.1.230: icmp_seq=3 ttl=127 time=0.488 ms
64 bytes from 10.0.1.230: icmp_seq=4 ttl=127 time=0.410 ms
64 bytes from 10.0.1.230: icmp_seq=5 ttl=127 time=0.475 ms
64 bytes from 10.0.1.230: icmp_seq=6 ttl=127 time=0.513 ms
64 bytes from 10.0.1.230: icmp_seq=7 ttl=127 time=0.455 ms
```

Step 17 - Run ping command in a public instance to check if the instance can connect to and from the public internet.

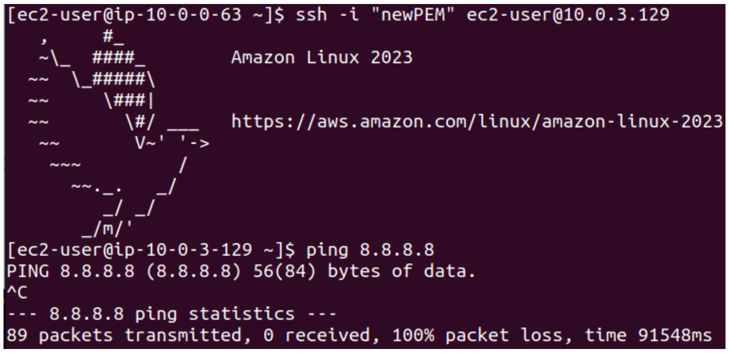


```
[root@ip-10-0-0-63 ec2-user]# ping www.google.com
PING www.google.com (172.217.1.100) 56(84) bytes of data.
64 bytes from yyz08s09-in-f4.1e100.net (172.217.1.100): icmp_seq=1 ttl=108 time=19.2 ms
64 bytes from ord37s51-in-f4.1e100.net (172.217.1.100): icmp_seq=2 ttl=108 time=19.3 ms
64 bytes from mia09s17-in-f4.1e100.net (172.217.1.100): icmp_seq=3 ttl=108 time=19.3 ms
64 bytes from yyz08s09-in-f100.1e100.net (172.217.1.100): icmp_seq=4 ttl=108 time=19.2 ms
64 bytes from yyz08s09-in-f4.1e100.net (172.217.1.100): icmp_seq=5 ttl=108 time=19.2 ms
64 bytes from ord37s51-in-f4.1e100.net (172.217.1.100): icmp_seq=6 ttl=108 time=19.3 ms
64 bytes from mia09s17-in-f4.1e100.net (172.217.1.100): icmp_seq=7 ttl=108 time=19.3 ms
64 bytes from yyz08s09-in-f100.1e100.net (172.217.1.100): icmp_seq=8 ttl=108 time=19.2 ms
64 bytes from yyz08s09-in-f4.1e100.net (172.217.1.100): icmp_seq=9 ttl=108 time=19.2 ms
```



```
shreyaskayarkar@rahulraj-TravelMate-P214-53:~$ ping 3.134.85.185
PING 3.134.85.185 (3.134.85.185) 56(84) bytes of data.
64 bytes from 3.134.85.185: icmp_seq=1 ttl=107 time=310 ms
64 bytes from 3.134.85.185: icmp_seq=2 ttl=107 time=333 ms
64 bytes from 3.134.85.185: icmp_seq=3 ttl=107 time=254 ms
64 bytes from 3.134.85.185: icmp_seq=4 ttl=107 time=276 ms
64 bytes from 3.134.85.185: icmp_seq=5 ttl=107 time=291 ms
64 bytes from 3.134.85.185: icmp_seq=6 ttl=107 time=322 ms
^C
--- 3.134.85.185 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 253.568/297.703/333.425/27.475 ms
```

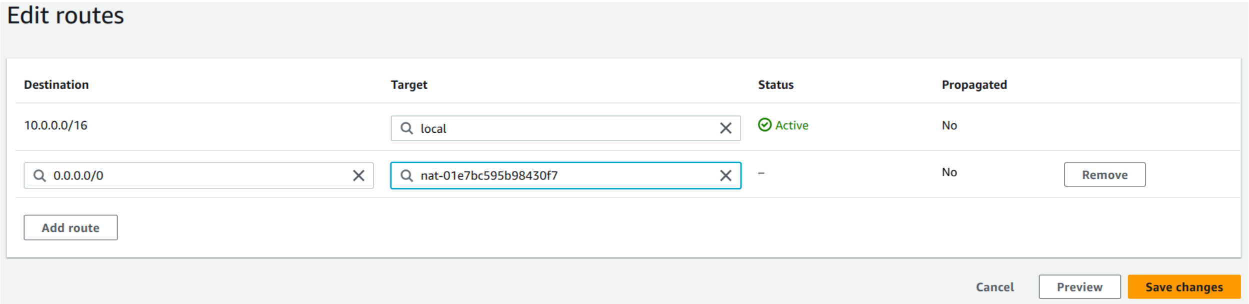
Step 18 - Run ping command in private instance to check if it can access the internet.



```
[ec2-user@ip-10-0-0-63 ~]$ ssh -i "newPEM" ec2-user@10.0.3.129
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-3-129 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
89 packets transmitted, 0 received, 100% packet loss, time 91548ms
```

Step 19 - The above snapshot shows that the private instance cannot access the internet as its route table does not have an entry for NAT gateway.

Edit route table of the private subnet to route the internet faced traffic to NAT gateway as the target.

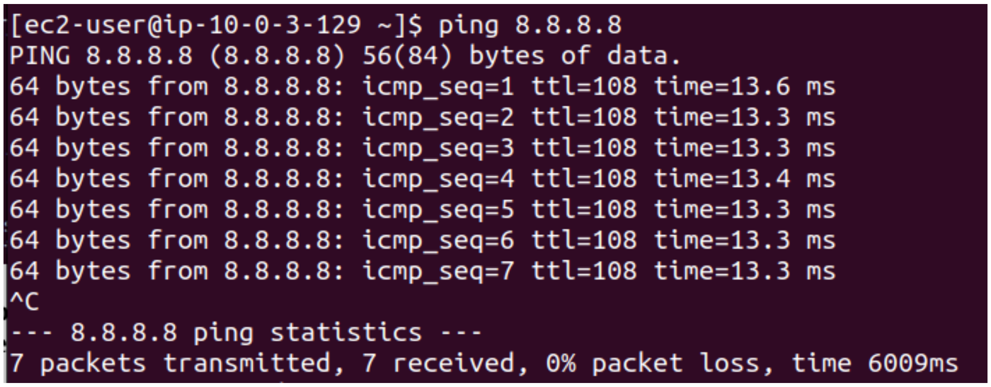


Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local	✓ Active	No	
0.0.0.0/0	nat-01e7bc595b98430f7	-	No	Remove

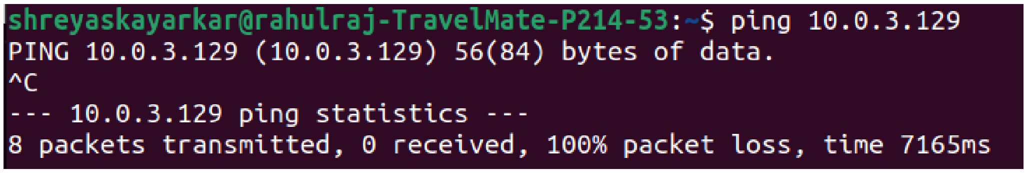
Step 20 - Save the changes and try to ping again.

It is visible that after attaching NAT gateway to the route table of the private subnet, the private instance can access the internet but it can not be accessed from the public internet.



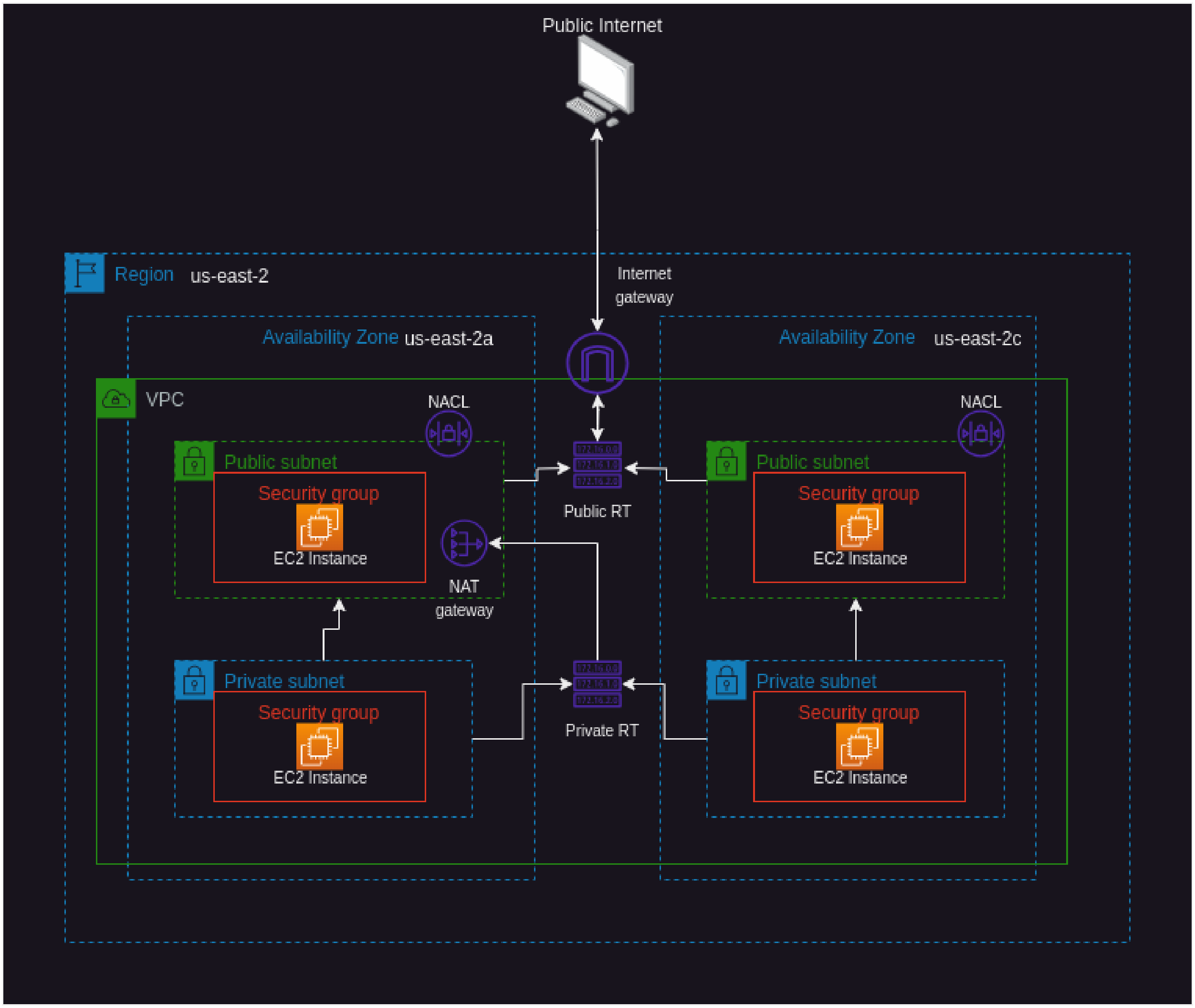
```
[ec2-user@ip-10-0-3-129 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=108 time=13.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=108 time=13.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=108 time=13.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=108 time=13.4 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=108 time=13.3 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=108 time=13.3 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=108 time=13.3 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
```

The below snapshot shows that the private instance is not accessible from the public internet.



```
shreyaskayarkar@rahulraj-TravelMate-P214-53:~$ ping 10.0.3.129
PING 10.0.3.129 (10.0.3.129) 56(84) bytes of data.
^C
--- 10.0.3.129 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7165ms
```

Architecture diagram for the above


Public Internet
Region
us-east-2
Internet gateway
Availability Zone
us-east-2a
Availability Zone
us-east-2c
VPC
NACL
NACL
Public subnet
Security group
EC2 Instance
Public RT
Public subnet
Security group
EC2 Instance
NAT gateway
Private subnet
Security group
EC2 Instance
Private RT
Private subnet
Security group
EC2 Instance