Cloud Network & Access Control Architecture for Internal Applications
AWS Implementation Report

---

1. Introduction

This project demonstrates how to design a secure cloud network architecture in AWS for hosting an internal application that must be accessible to employees while remaining protected from external threats.

Previously, systems were directly exposed to the internet without firewall rules, which led to security incidents. The goal of this project is to redesign the network using proper subnet segregation, firewall controls, and access restrictions following cloud security best practices.

---

2. Objectives

- Design a Virtual Private Cloud (VPC)
- Create subnet segregation (Public and Private)
- Assign IP ranges correctly
- Configure Security Groups and Network ACLs
- Restrict administrative access (SSH) to authorized user only
- Allow application access only through HTTP/HTTPS from internal network
- Simulate insecure configuration and then fix it
- Deploy a working web application in the private subnet using Docker

---

3. High Level Architecture

- Public Subnet: Represents employee network and bastion access
- Private Subnet: Hosts the internal web application
- NAT Gateway: Allows private subnet outbound internet access
- Internet Gateway: Provides internet access to public subnet

Architecture Flow:

Admin (Laptop) → SSH → Public EC2 (Bastion) → SSH → Private EC2 (Web App)
Employees (Public EC2) → HTTP/HTTPS → Private EC2 (Web App)

---

4. Network Design

VPC

- CIDR Block: 10.0.0.0/16

Subnets

Subnet	CIDR	Purpose
Public Subnet	10.0.1.0/24	Employee machines and Bastion
Private Subnet	10.0.2.0/24	Web application server

---

5. Internet Gateway and Route Tables

Public Route Table

Destination	Target
0.0.0.0/0	Internet Gateway

Associated with Public Subnet.

Private Route Table (Before NAT)

Destination	Target
10.0.0.0/16	local

Private subnet had no internet access initially.

---

6. Simulating the Insecure Design (Before Fix)

A security group was created with the following rule:

Type	Port	Source
All Traffic	All	0.0.0.0/0

This exposed the server completely to the internet and demonstrated the real-world mistake that led to security incidents.

(Screenshot included)

---

7. Secure Security Group Configuration (After Fix)

Security Group – Public EC2 (Employees/Bastion)

Type	Port	Source
SSH	22	Admin Public IP
All Traffic	All	0.0.0.0/0

Security Group – Private EC2 (Web App)

Type	Port	Source
HTTP	80	10.0.1.0/24
HTTPS	443	10.0.1.0/24
SSH	22	10.0.1.0/24

This ensures:

- Only employees can access the application
- Only admin can SSH through bastion
- No direct internet access to the application server

---

8. Network ACL Configuration (Defense in Depth)

Private Subnet NACL – Inbound

Rule	Port	Source	Action
100	80	10.0.1.0/24	ALLOW
110	443	10.0.1.0/24	ALLOW
120	22	10.0.1.0/24	ALLOW
130	1024-65535	10.0.1.0/24	ALLOW
*	ALL	0.0.0.0/0	DENY

---

9. NAT Gateway Implementation

Initially, the private EC2 could not install packages because it had no internet access. To resolve this while maintaining security:

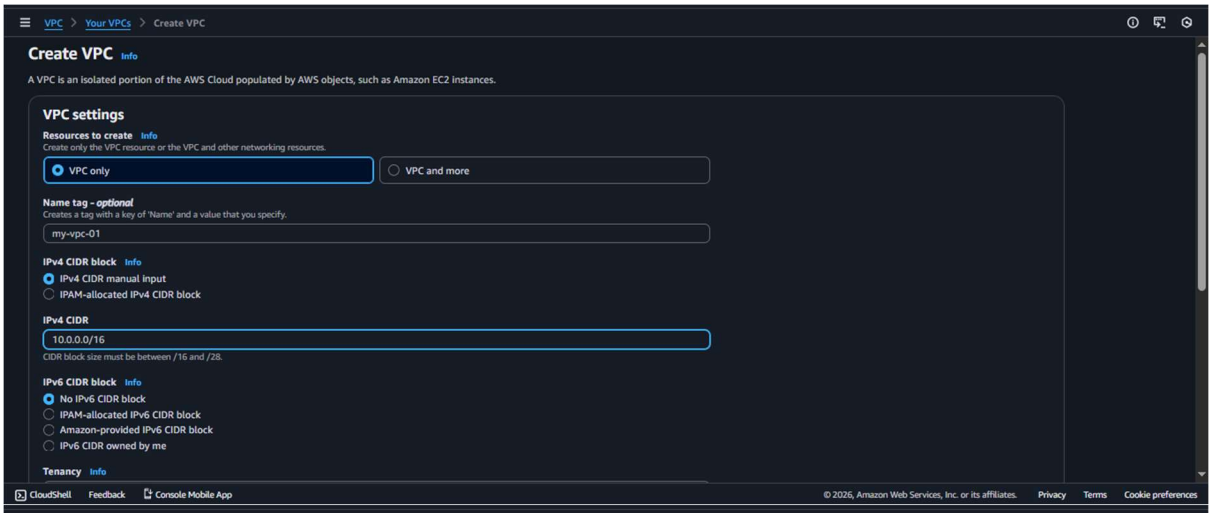
- An Elastic IP was allocated
- NAT Gateway was created in Public Subnet
- Private Route Table updated:

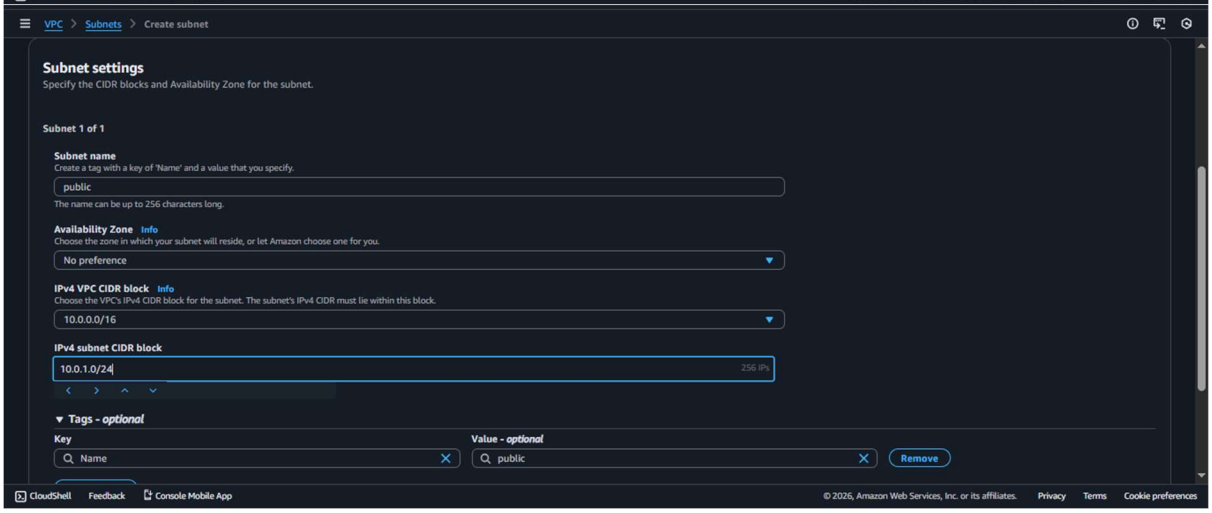
Destination	Target
0.0.0.0/0	NAT Gateway

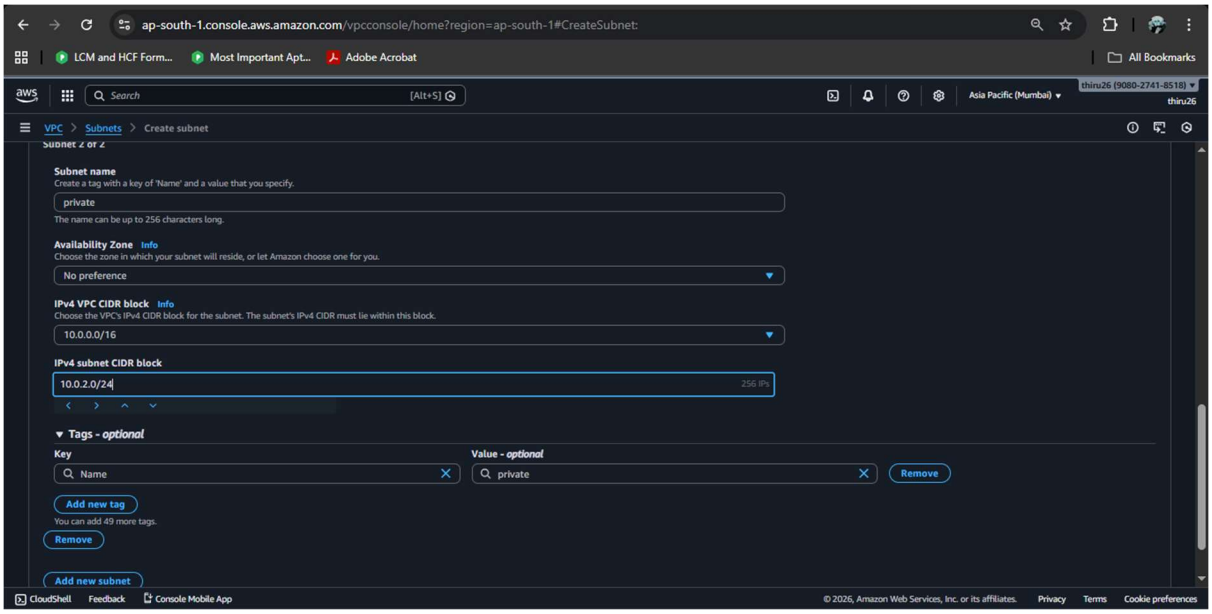
This allowed outbound internet access without allowing inbound traffic.

10. Screenshots of steps involved:

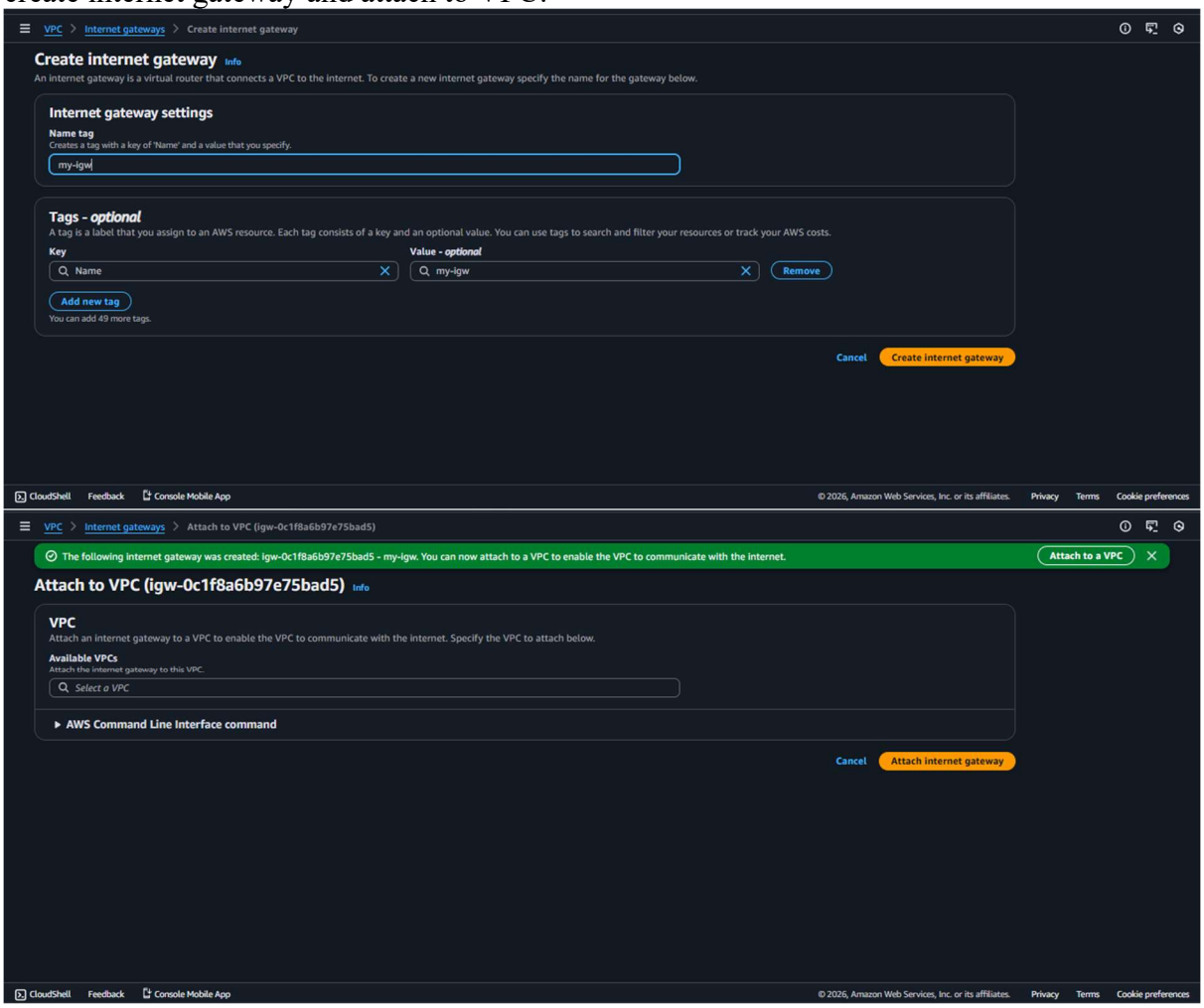
Create VPC and subnets:



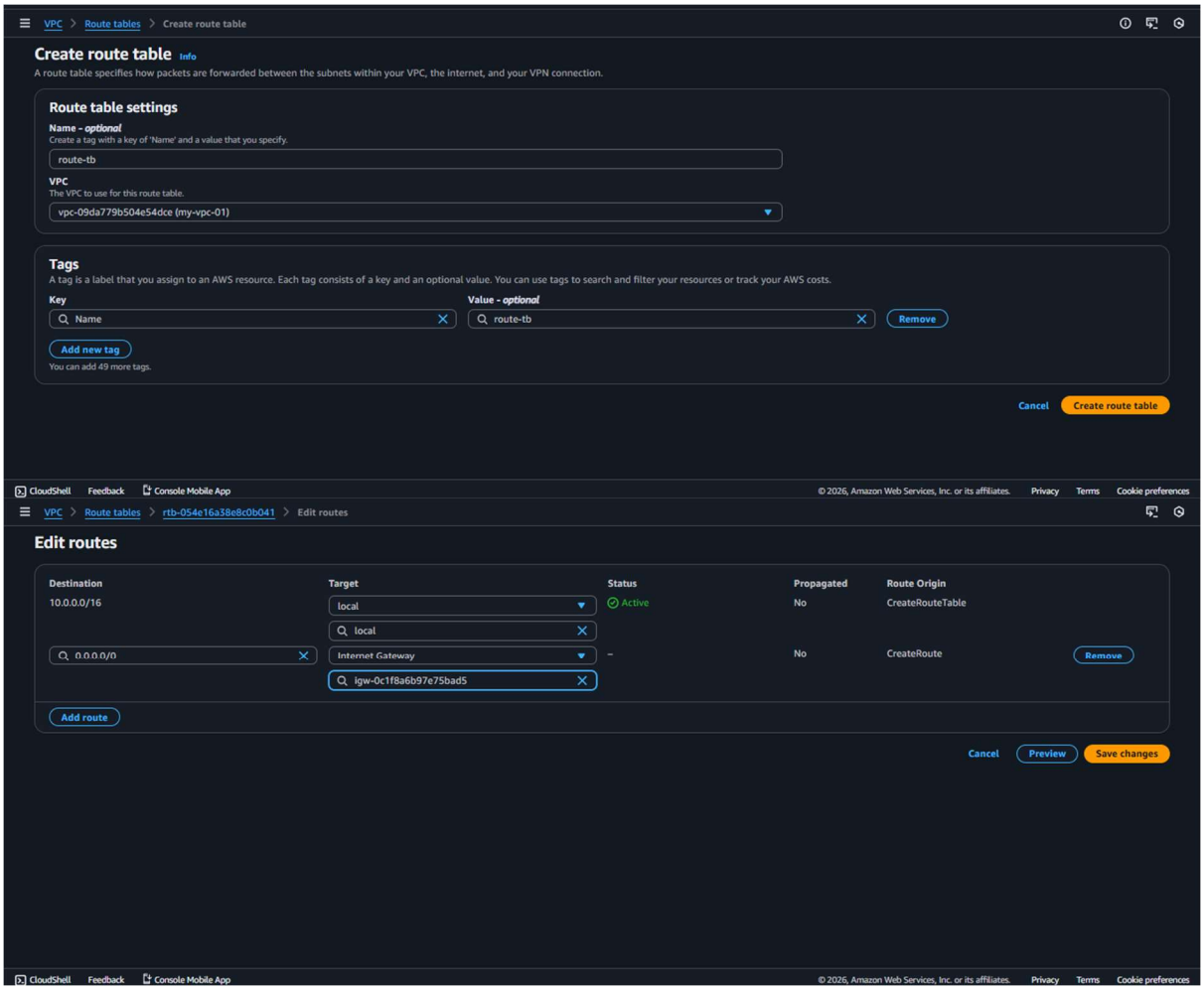




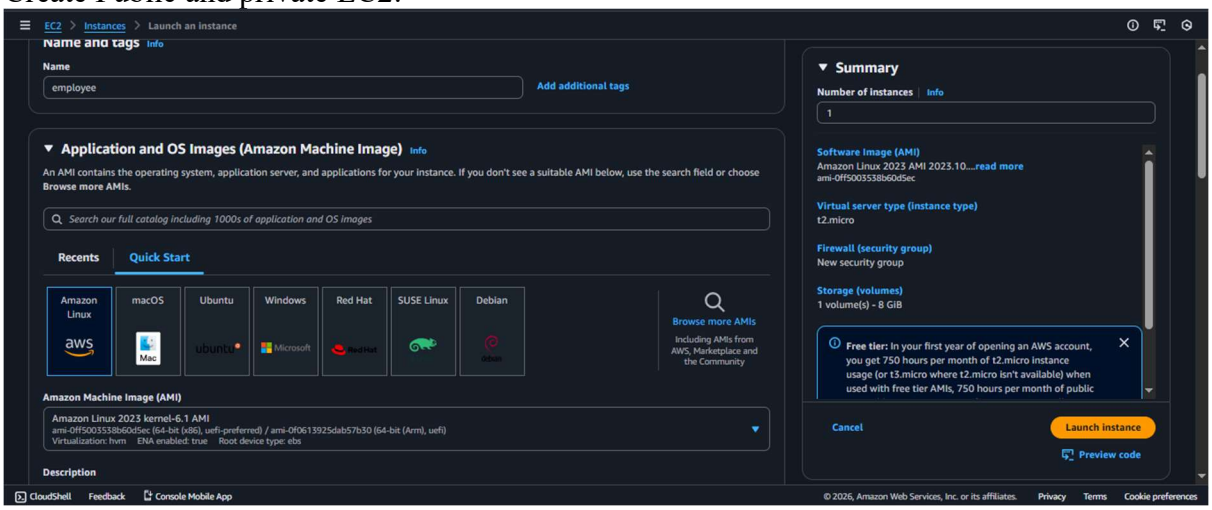
create internet gateway and attach to VPC:

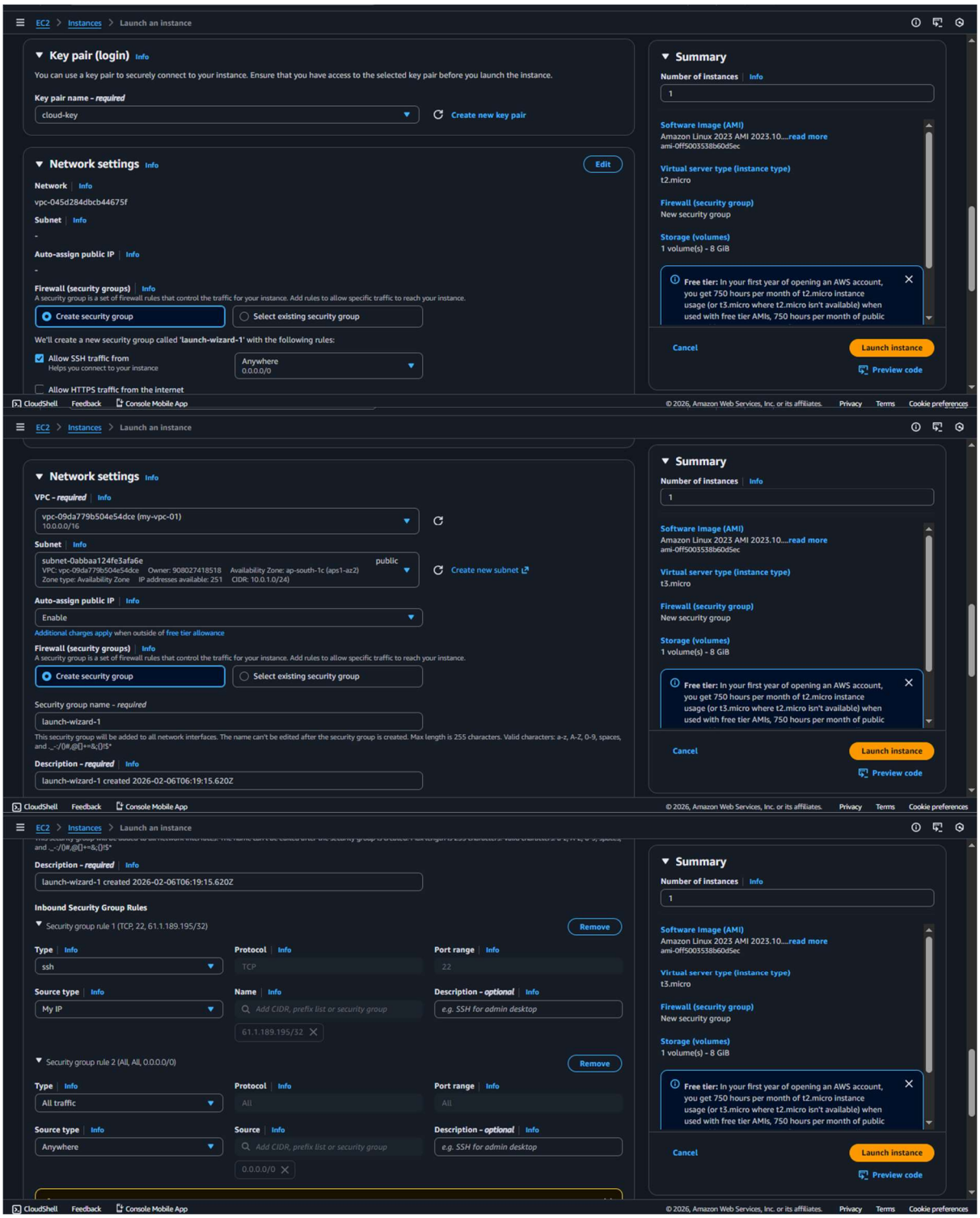


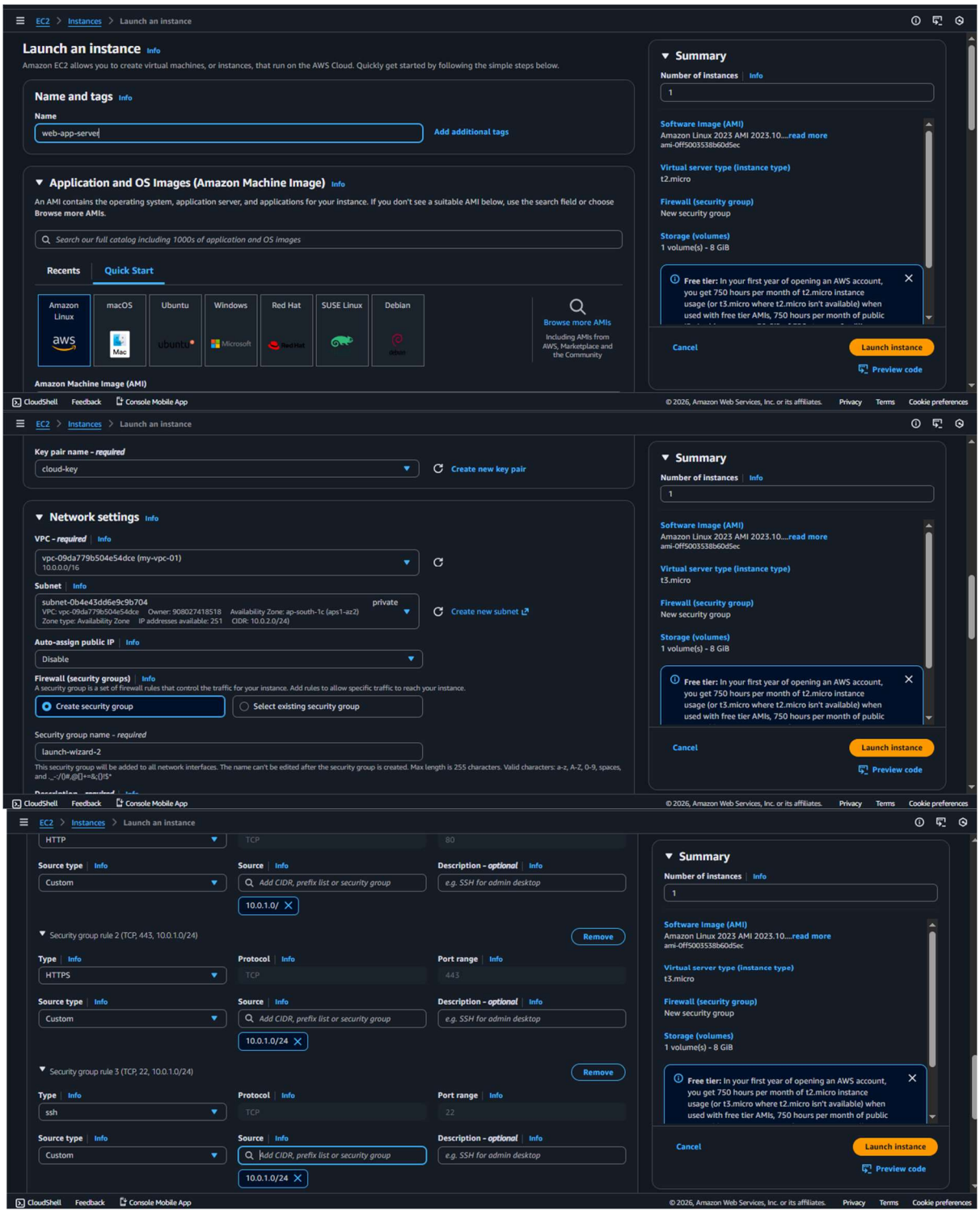
Add route to internet gateway:



Create Public and private EC2:

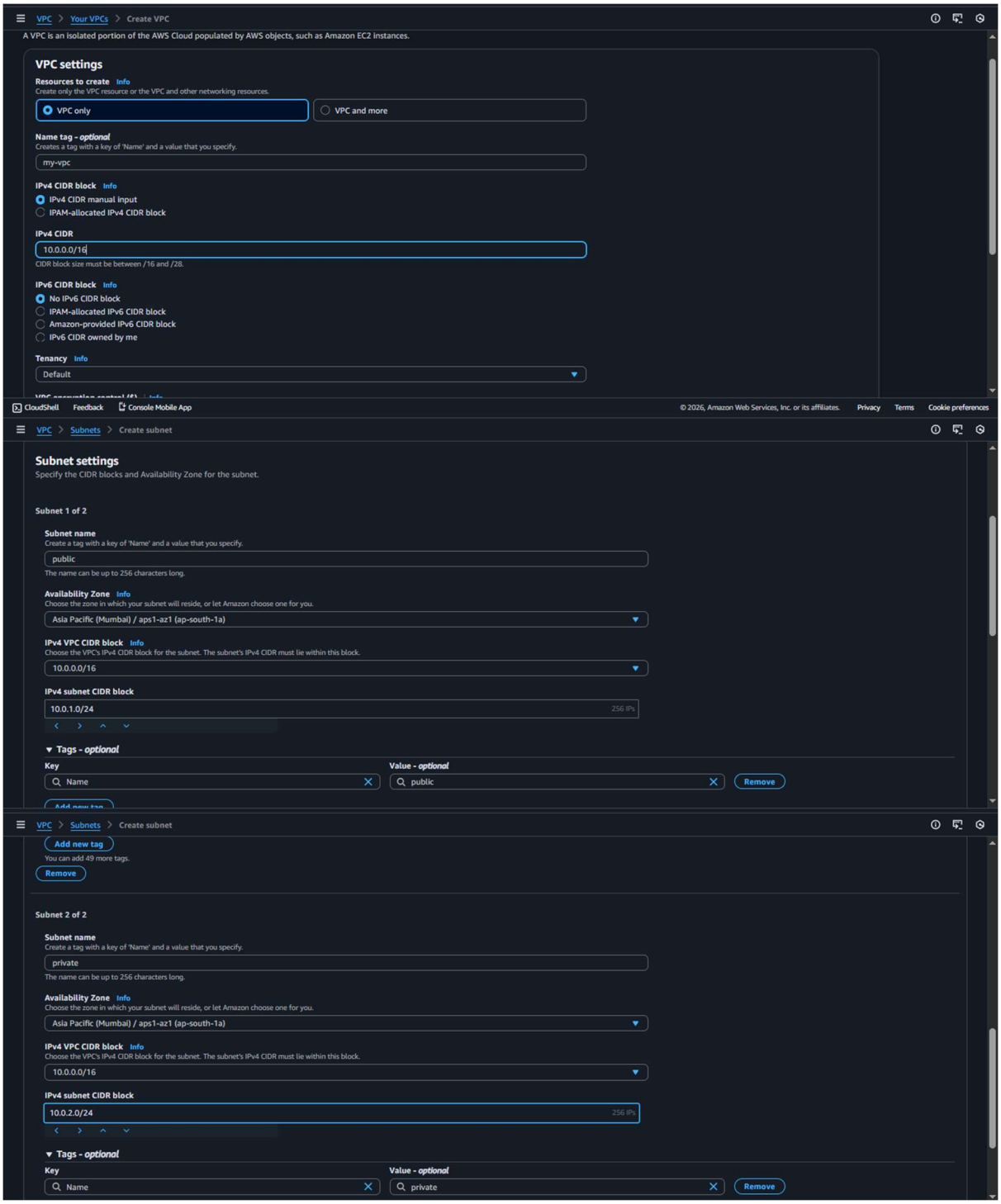


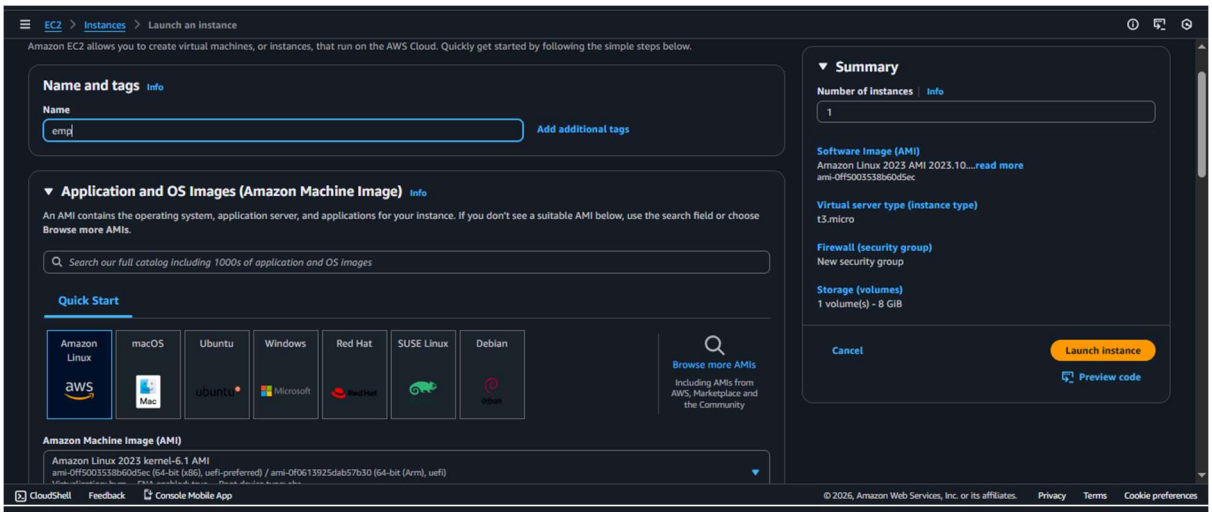

EC2 > Instances > Launch an instance
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
cloud-key
Create new key pair
Network settings Info
Edit
Network Info
vpc-045d284dbcb44675f
Subnet Info
-
Auto-assign public IP Info
-
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
Helps you connect to your instance
Anywhere
0.0.0.0/0
Allow HTTPS traffic from the internet
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.10....read more
ami-0ff5003538b60d5ec
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public
Cancel
Launch instance
Preview code
CloudShell Feedback Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
EC2 > Instances > Launch an instance
Network settings Info
VPC - required Info
vpc-09da779b504e54dce (my-vpc-01)
10.0.0.0/16
Subnet Info
subnet-0abbaa124fe3afa6e public
VPC: vpc-09da779b504e54dce Owner: 908027418518 Availability Zone: ap-south-1c (aps1-az2)
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
Security group name - required
launch-wizard-1
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard-1 created 2026-02-06T06:19:15.620Z
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.10....read more
ami-0ff5003538b60d5ec
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public
Cancel
Launch instance
Preview code
CloudShell Feedback Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
EC2 > Instances > Launch an instance
Description - required Info
launch-wizard-1 created 2026-02-06T06:19:15.620Z
Inbound Security Group Rules
Security group rule 1 (TCP, 22, 61.1.189.195/32)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
My IP
Name Info
Add CIDR, prefix list or security group
61.1.189.195/32
Description - optional Info
e.g. SSH for admin desktop
Security group rule 2 (All, All, 0.0.0.0/0)
Remove
Type Info
All traffic
Protocol Info
All
Port range Info
All
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security group
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.10....read more
ami-0ff5003538b60d5ec
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public
Cancel
Launch instance
Preview code
CloudShell Feedback Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

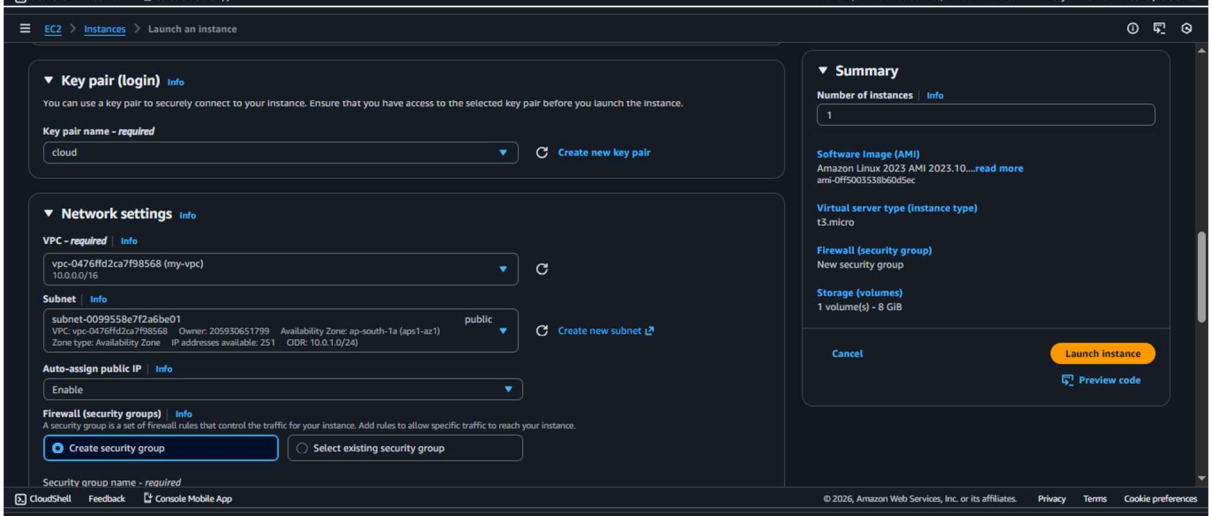

EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
web-app-server
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.10....read more
ami-0ff5003538b60d5ec
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public
Cancel
Launch instance
Preview code
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

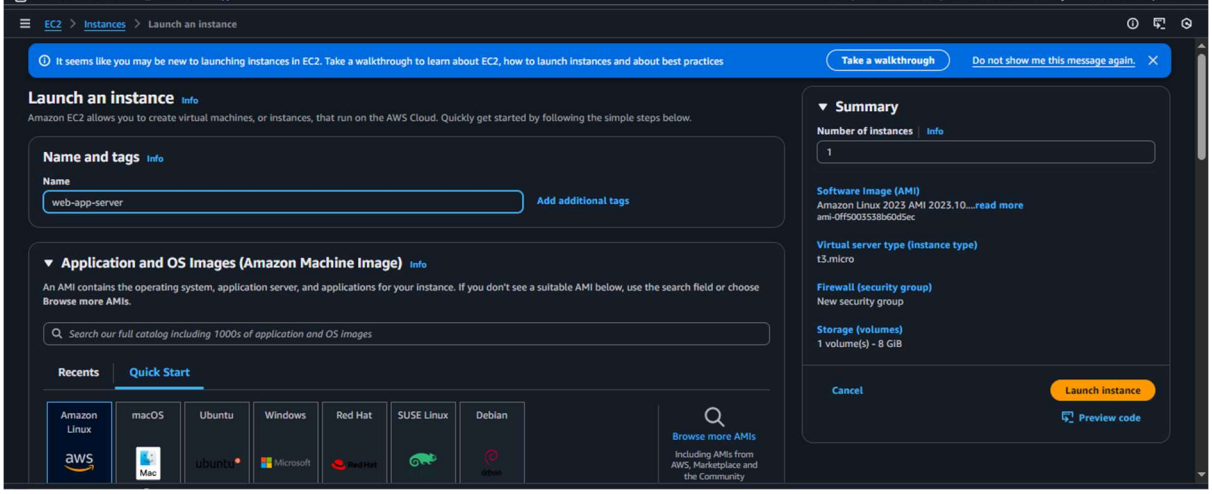
EC2 > Instances > Launch an instance
Key pair name - required
cloud-key
Create new key pair
Network settings Info
VPC - required Info
vpc-09da779b504e54dce (my-vpc-01)
10.0.0.0/16
Subnet Info
subnet-0b4e43dd6e9c9b704
private
VPC: vpc-09da779b504e54dce Owner: 908027418518 Availability Zone: ap-south-1c (aps1-az2)
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.2.0/24)
Create new subnet
Auto-assign public IP Info
Disable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
launch-wizard-2
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.10....read more
ami-0ff5003538b60d5ec
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public
Cancel
Launch instance
Preview code
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

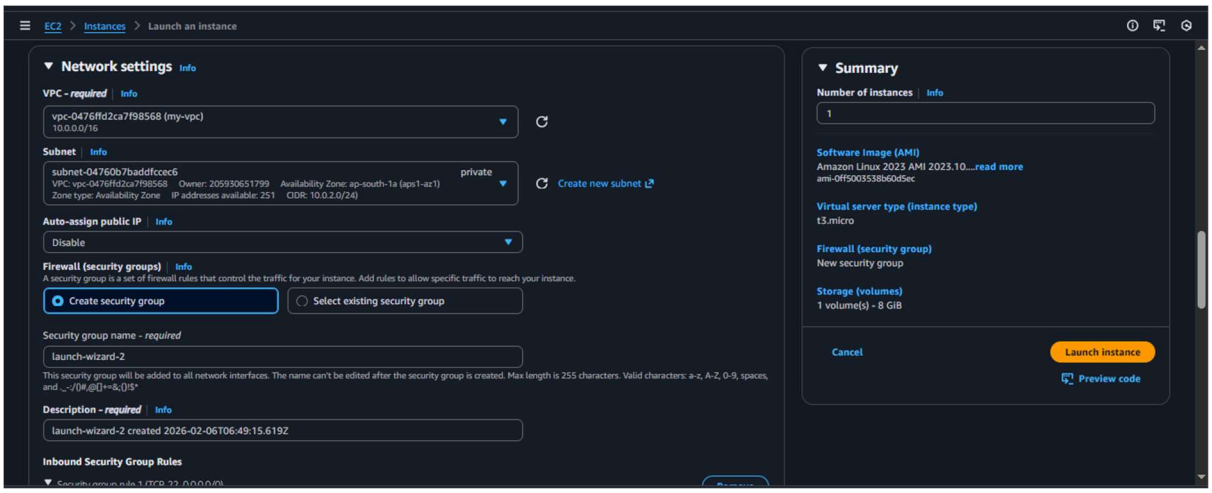
EC2 > Instances > Launch an instance
HTTP
TCP
80
Source type Info
Custom
Source Info
Add CIDR, prefix list or security group
Description - optional Info
e.g. SSH for admin desktop
10.0.1.0/
Security group rule 2 (TCP, 443, 10.0.1.0/24)
Remove
Type Info
HTTPS
Protocol Info
TCP
Port range Info
443
Source type Info
Custom
Source Info
Add CIDR, prefix list or security group
Description - optional Info
e.g. SSH for admin desktop
10.0.1.0/24
Security group rule 3 (TCP, 22, 10.0.1.0/24)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Custom
Source Info
Add CIDR, prefix list or security group
Description - optional Info
e.g. SSH for admin desktop
10.0.1.0/24
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.10....read more
ami-0ff5003538b60d5ec
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public
Cancel
Launch instance
Preview code
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


VPC > Your VPCs > Create VPC
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.
my-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
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
VPC > Subnets > Create subnet
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.
public
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.
Asia Pacific (Mumbai) / aps1-az1 (ap-south-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.
10.0.0.0/16
IPv4 subnet CIDR block
10.0.1.0/24
256 IPs
Tags - optional
Key
Value - optional
Name
public
Remove
Add new tag
You can add 49 more tags.
Remove
Subnet 2 of 2
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private
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.
Asia Pacific (Mumbai) / aps1-az1 (ap-south-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.
10.0.0.0/16
IPv4 subnet CIDR block
10.0.2.0/24
256 IPs
Tags - optional
Key
Value - optional
Name
private
Remove

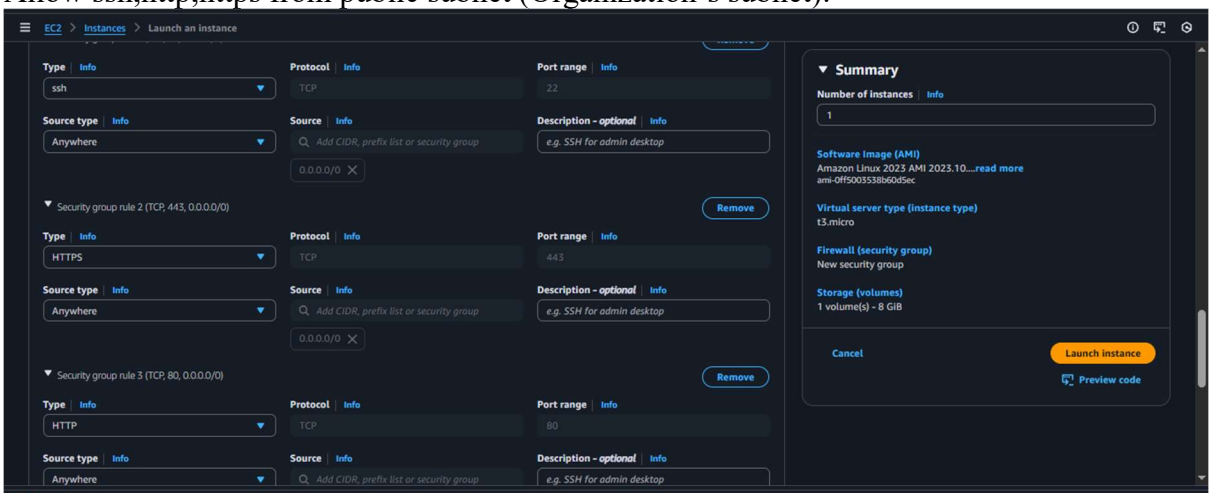

EC2 > Instances > Launch an instance
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
emp
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.
Search our full catalog including 1000s of application and OS images
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Amazon Linux 2023 kernel-6.1 AMI
ami-0ff5003538b60d5ec (64-bit (x86), uefi-preferred) / ami-0f0613925dab57b30 (64-bit (Arm), uefi)
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.10....read more
ami-0ff5003538b60d5ec
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

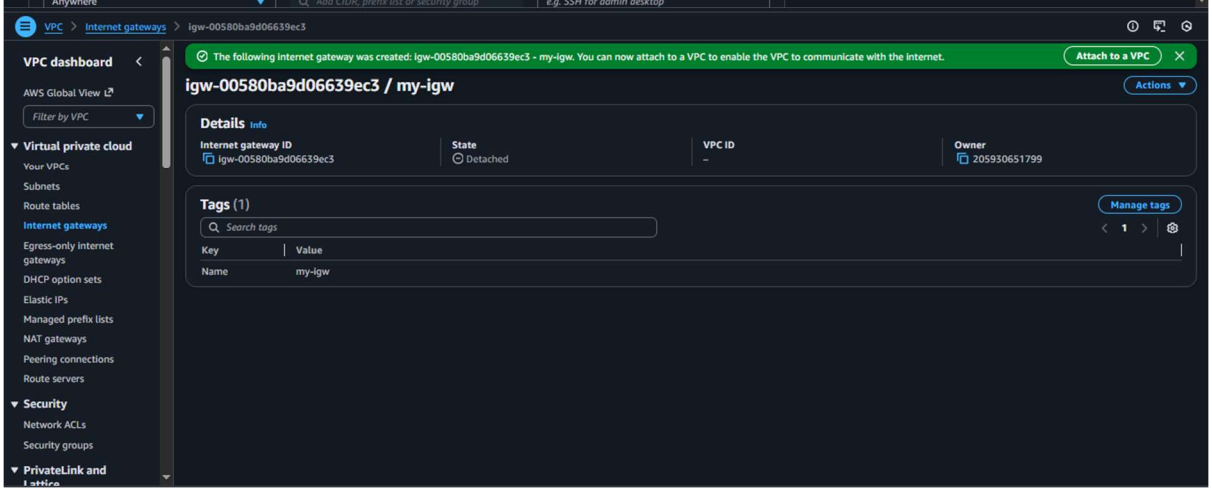

EC2 > Instances > Launch an instance
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
cloud
Create new key pair
Network settings Info
VPC - required Info
vpc-0476ffd2ca7f98568 (my-vpc)
10.0.0.0/16
Subnet Info
subnet-0099558e7f2a6be01
public
VPC: vpc-0476ffd2ca7f98568 Owner: 205930651799 Availability Zone: ap-south-1a (aps1-az1)
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24)
Create new subnet
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
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.10....read more
ami-0ff5003538b60d5ec
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

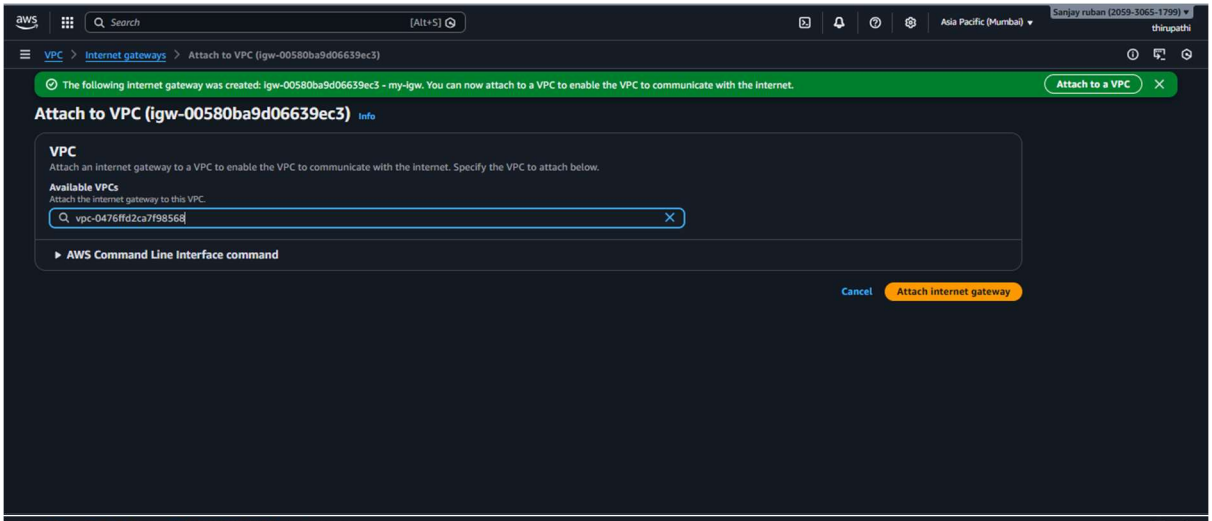

EC2 > Instances > Launch an instance
It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices
Take a walkthrough
Do not show me this message again.
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
web-app-server
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.10....read more
ami-0ff5003538b60d5ec
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code

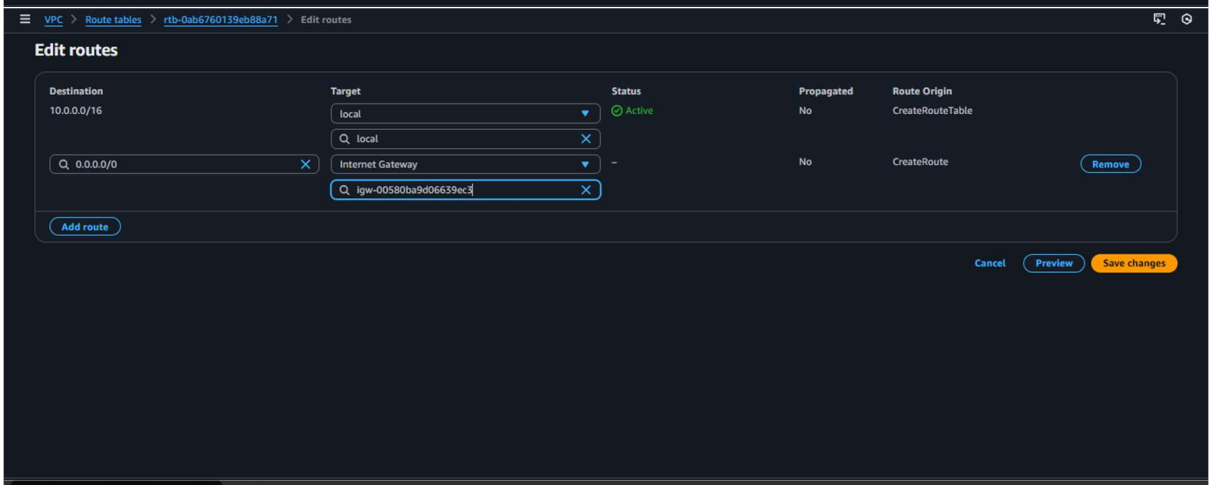


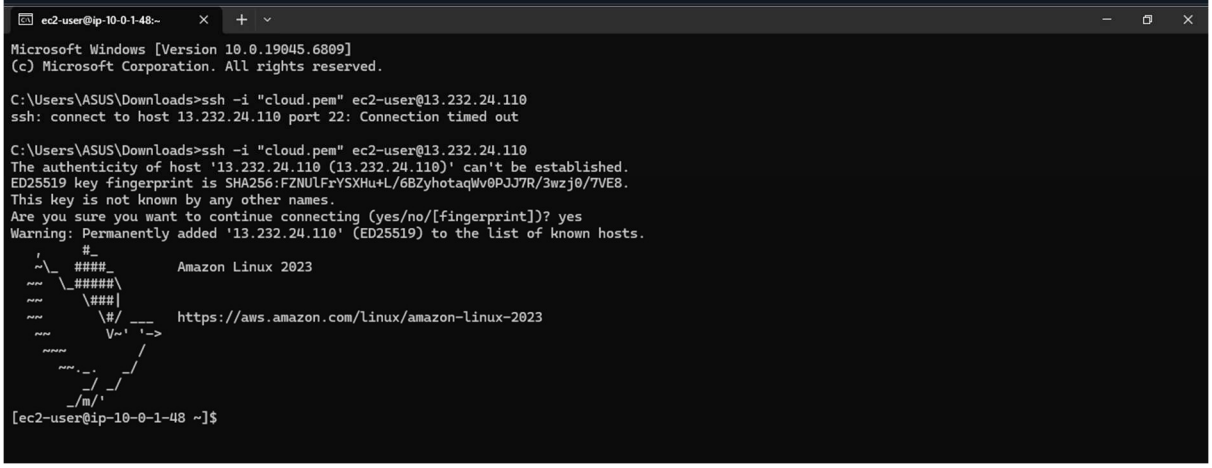
Allow ssh,http,https from public subnet (Organization's subnet):

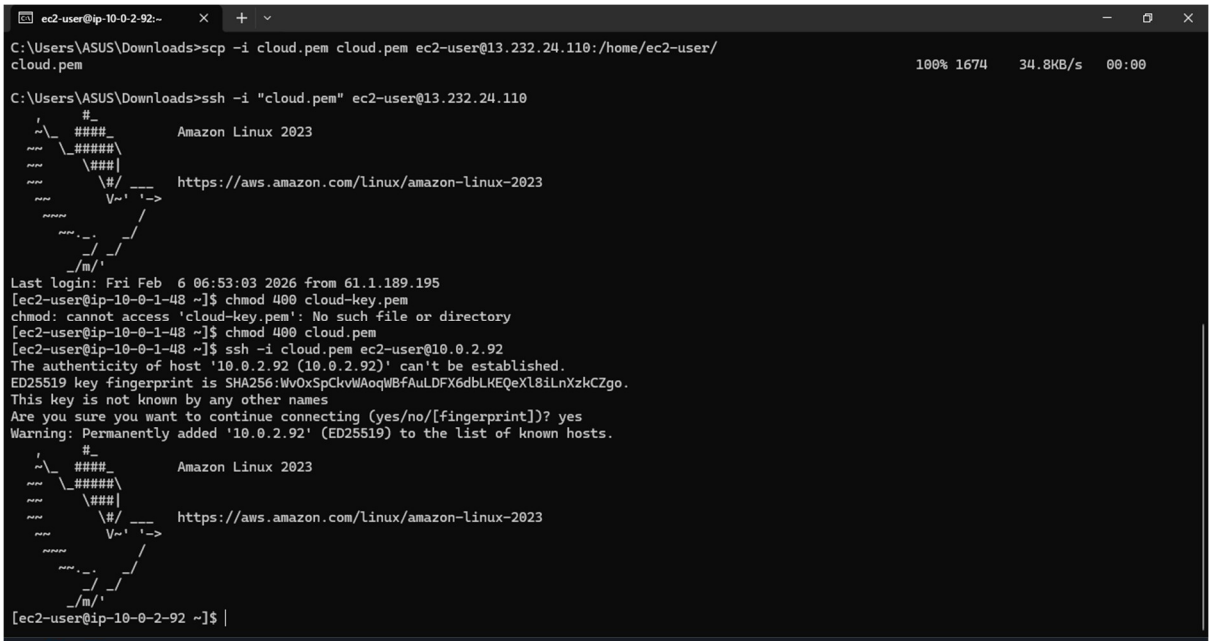


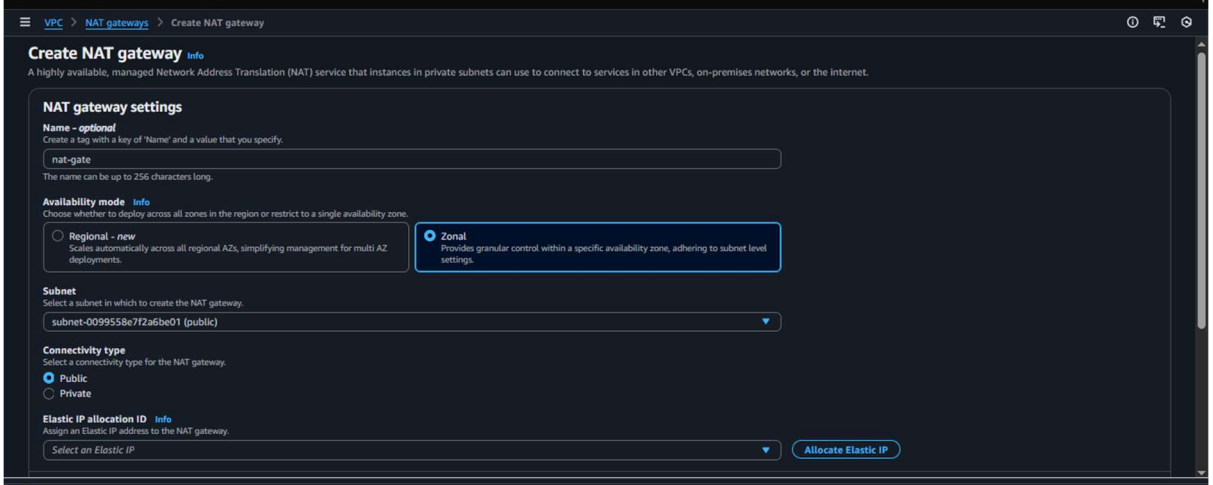


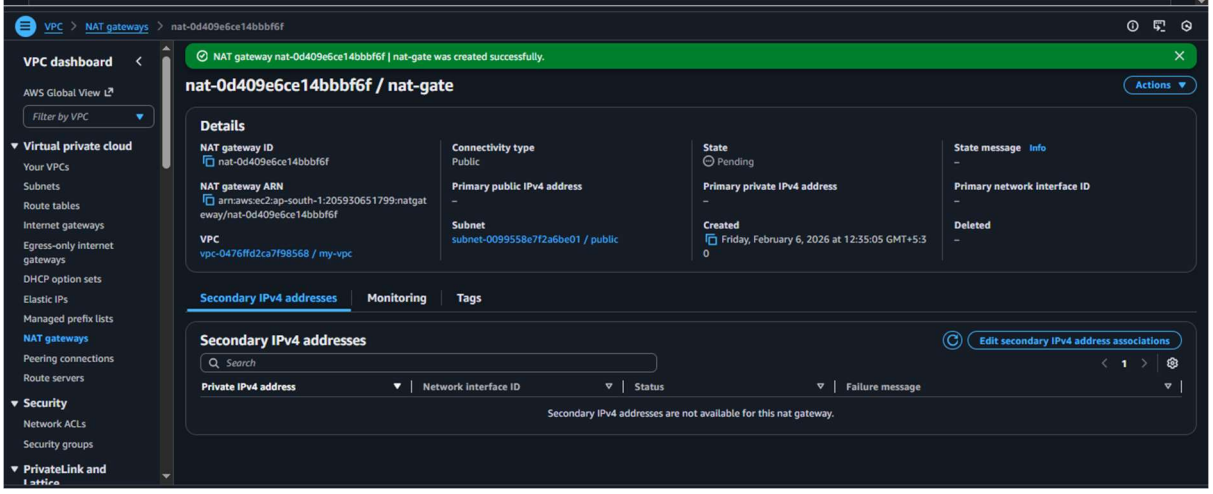

Search
[Alt+S]
Asia Pacific (Mumbai)
Sanjay ruban (2059-3065-1799)
thirupathi
VPC > Internet gateways > Attach to VPC (igw-00580ba9d06639ec3)
The following internet gateway was created: igw-00580ba9d06639ec3 - my-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
Attach to VPC (igw-00580ba9d06639ec3) 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.
vpc-0476ffd2ca7f98568
AWS Command Line Interface command
Cancel
Attach internet gateway


VPC > Route tables > rtb-0ab6760139eb88a71 > Edit routes
Edit routes
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16
local
Active
No
CreateRouteTable
local
0.0.0.0/0
Internet Gateway
-
No
CreateRoute
Remove
igw-00580ba9d06639ec3
Add route
Cancel
Preview
Save changes

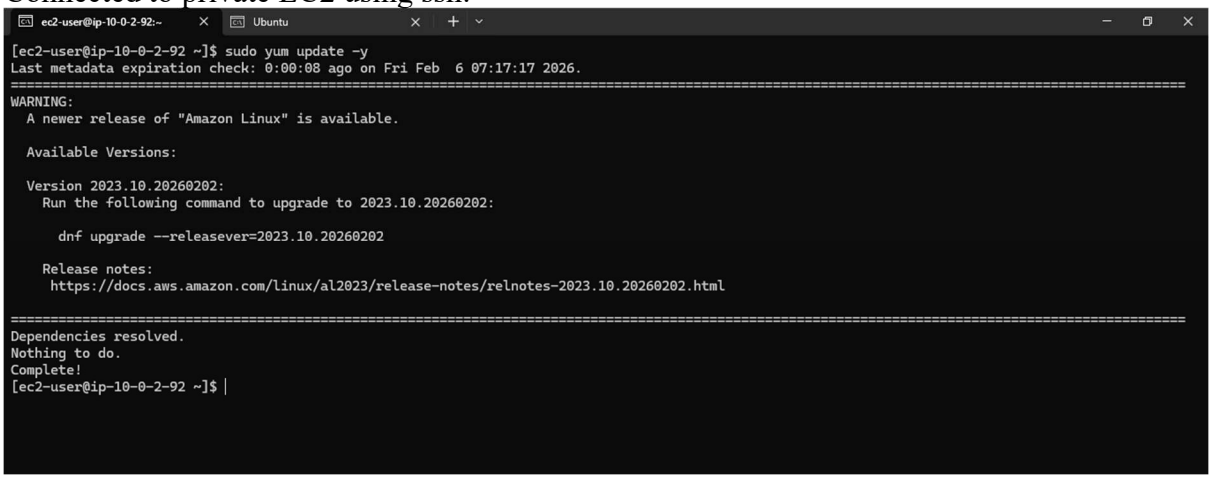

ec2-user@ip-10-0-1-48:~
Microsoft Windows [Version 10.0.19045.6809]
(c) Microsoft Corporation. All rights reserved.
C:\Users\ASUS\Downloads>ssh -i "cloud.pem" ec2-user@13.232.24.110
ssh: connect to host 13.232.24.110 port 22: Connection timed out
C:\Users\ASUS\Downloads>ssh -i "cloud.pem" ec2-user@13.232.24.110
The authenticity of host '13.232.24.110 (13.232.24.110)' can't be established.
ED25519 key fingerprint is SHA256:FZNUlFrYSXHu+L/6BZyhotaqWv0PJJ7R/3wzj0/7VE8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.232.24.110' (ED25519) to the list of known hosts.
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-1-48 ~]$


ec2-user@ip-10-0-2-92:~
C:\Users\ASUS\Downloads>scp -i cloud.pem cloud.pem ec2-user@13.232.24.110:/home/ec2-user/
cloud.pem 100% 1674 34.8KB/s 00:00
C:\Users\ASUS\Downloads>ssh -i "cloud.pem" ec2-user@13.232.24.110
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
Last login: Fri Feb 6 06:53:03 2026 from 61.1.189.195
[ec2-user@ip-10-0-1-48 ~]$ chmod 400 cloud-key.pem
chmod: cannot access 'cloud-key.pem': No such file or directory
[ec2-user@ip-10-0-1-48 ~]$ chmod 400 cloud.pem
[ec2-user@ip-10-0-1-48 ~]$ ssh -i cloud.pem ec2-user@10.0.2.92
The authenticity of host '10.0.2.92 (10.0.2.92)' can't be established.
ED25519 key fingerprint is SHA256:WvOxSpCkvWAoqWBfAuLDFX6dbLKEQeXl8iLnXzkCZgo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.92' (ED25519) to the list of known hosts.
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-2-92 ~]$

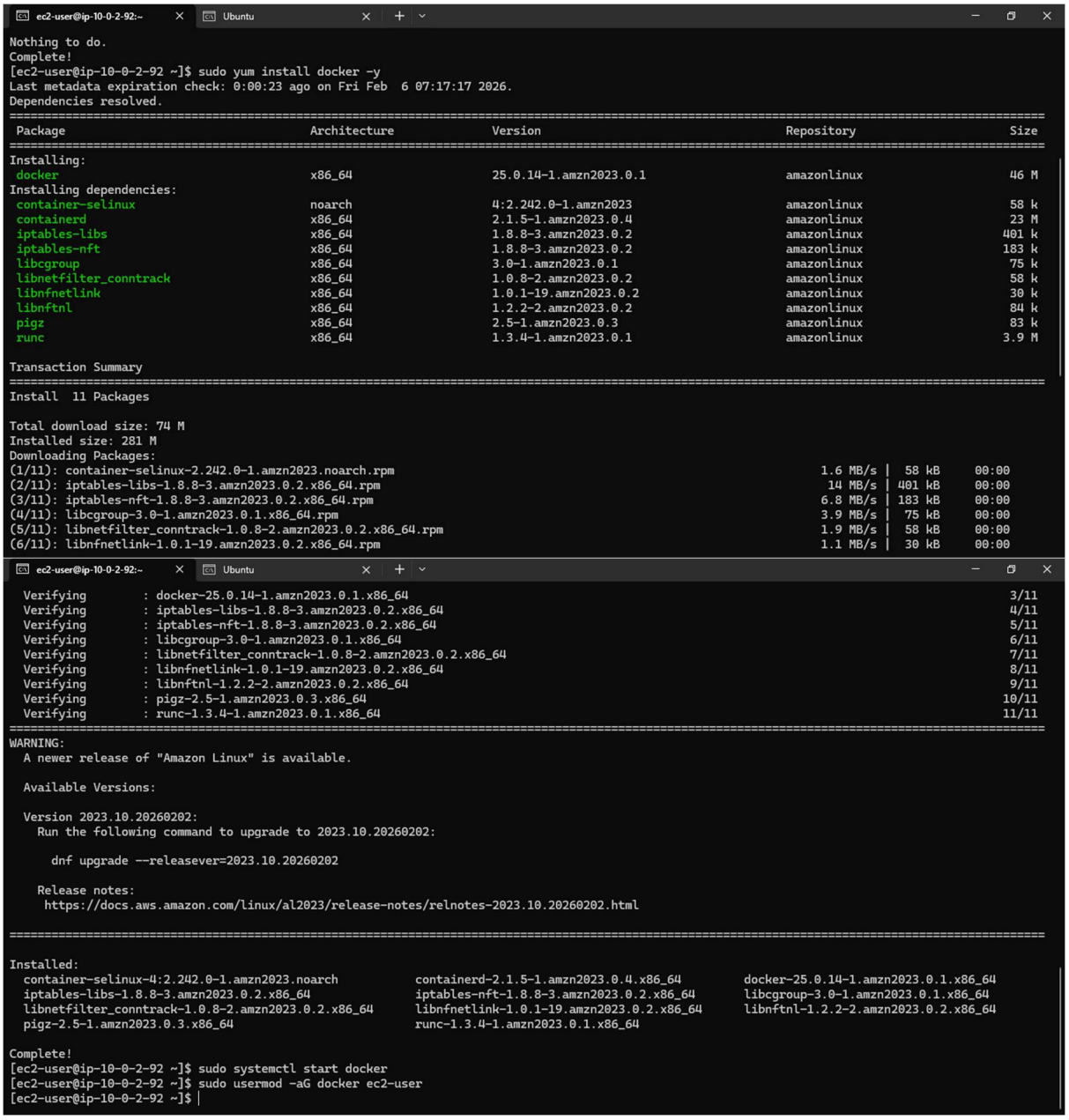

VPC > NAT gateways > Create NAT gateway
Create NAT gateway Info
A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.
NAT gateway settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
nat-gate
The name can be up to 256 characters long.
Availability mode Info
Choose whether to deploy across all zones in the region or restrict to a single availability zone.
Regional - new
Scales automatically across all regional AZs, simplifying management for multi AZ deployments.
Zonal
Provides granular control within a specific availability zone, adhering to subnet level settings.
Subnet
Select a subnet in which to create the NAT gateway.
subnet-0099558e7f2a6be01 (public)
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.
Select an Elastic IP
Allocate Elastic IP


VPC > NAT gateways > nat-0d409e6ce14bbbf6f
NAT gateway nat-0d409e6ce14bbbf6f | nat-gate was created successfully.
nat-0d409e6ce14bbbf6f / nat-gate
Actions
Details
NAT gateway ID
nat-0d409e6ce14bbbf6f
Connectivity type
Public
State
Pending
State message Info
NAT gateway ARN
arn:aws:ec2:ap-south-1:205930651799:natgateway/nat-0d409e6ce14bbbf6f
Primary public IPv4 address
Primary private IPv4 address
Primary network interface ID
VPC
vpc-0476ffd2ca7f98568 / my-vpc
Subnet
subnet-0099558e7f2a6be01 / public
Created
Friday, February 6, 2026 at 12:35:05 GMT+5:30
Deleted
Secondary IPv4 addresses
Monitoring
Tags
Secondary IPv4 addresses
Edit secondary IPv4 address associations
Search
Private IPv4 address
Network interface ID
Status
Failure message
Secondary IPv4 addresses are not available for this nat gateway.
VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Security
Network ACLs
Security groups
PrivateLink and Lattice

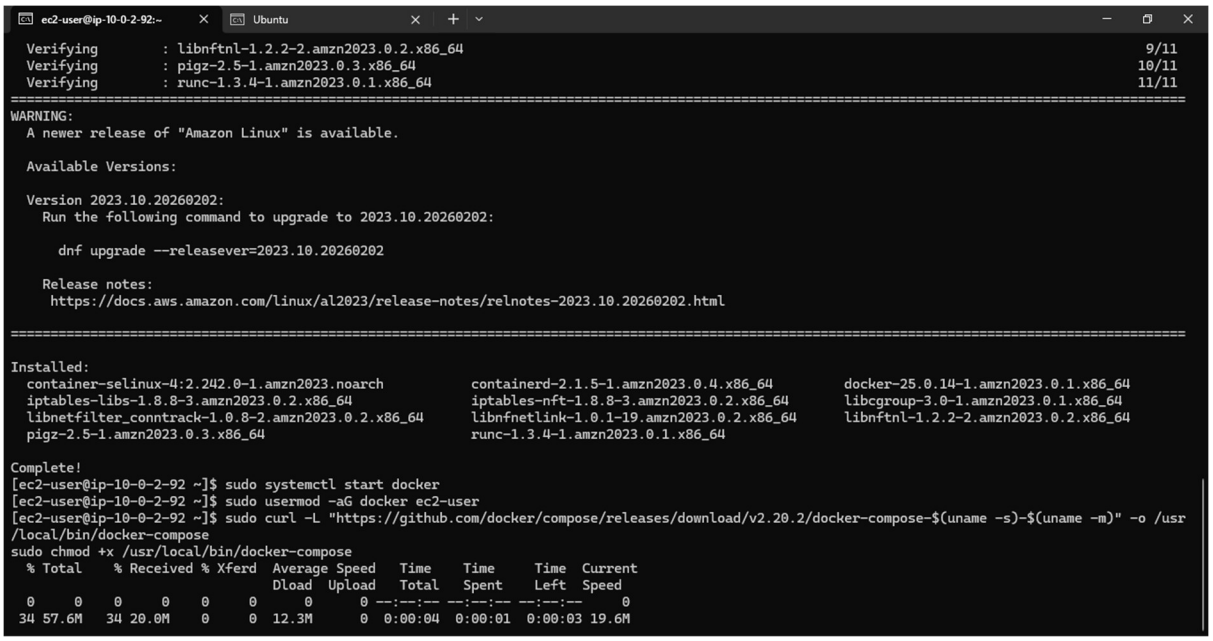
Connected to private EC2 using ssh:



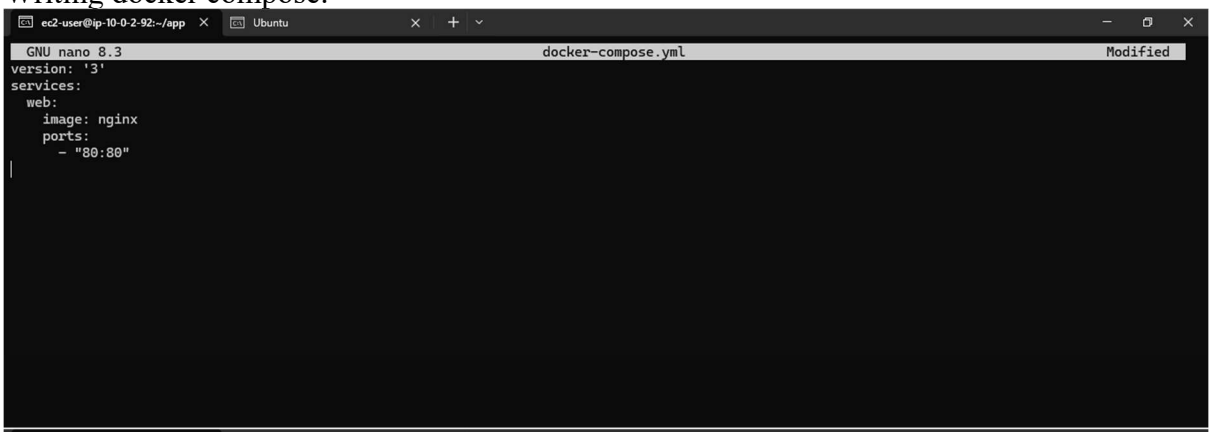
Update the system and install docker in it:

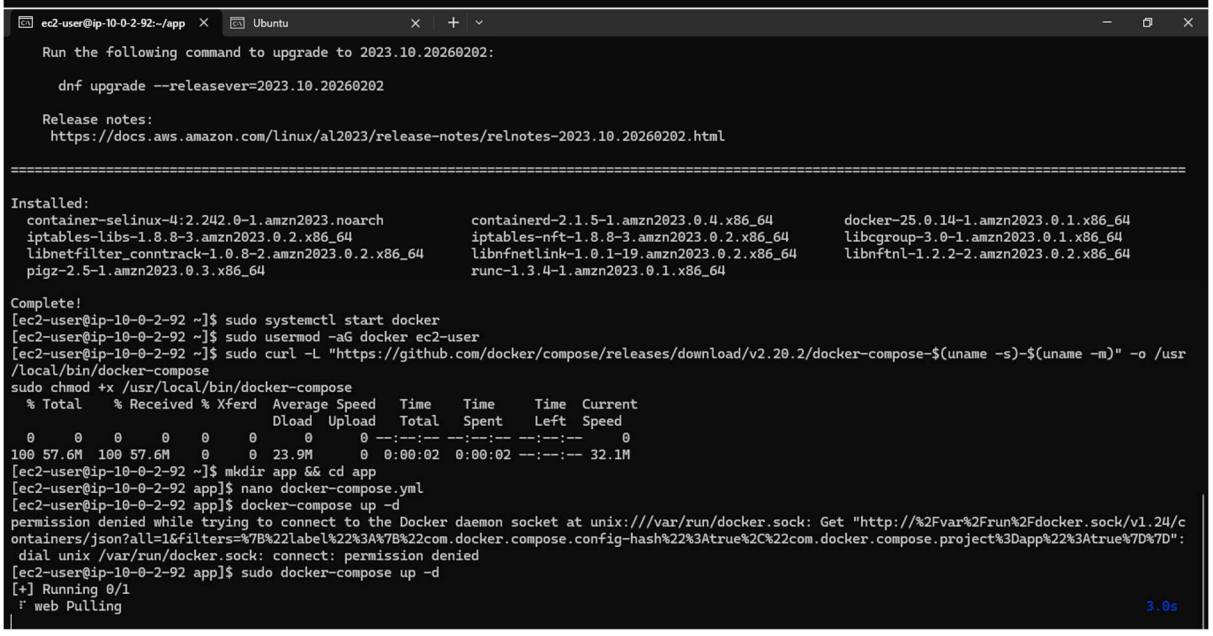


```
ec2-user@ip-10-0-2-92:~  Ubuntu
Nothing to do.
Complete!
[ec2-user@ip-10-0-2-92 ~]$ sudo yum install docker -y
Last metadata expiration check: 0:00:23 ago on Fri Feb  6 07:17:17 2026.
Dependencies resolved.
================================================================================
 Package                 Architecture  Version                    Repository  Size
================================================================================
Installing:
 docker                  x86_64        25.0.14-1.amzn2023.0.1     amazonlinux  46 M
Installing dependencies:
 container-selinux       noarch        4:2.242.0-1.amzn2023       amazonlinux  58 k
 containerd              x86_64        2.1.5-1.amzn2023.0.4       amazonlinux  23 M
 iptables-libs           x86_64        1.8.8-3.amzn2023.0.2       amazonlinux 401 k
 iptables-nft            x86_64        1.8.8-3.amzn2023.0.2       amazonlinux 183 k
 libcgroup               x86_64        3.0-1.amzn2023.0.1         amazonlinux  75 k
 libnetfilter_conntrack  x86_64        1.0.8-2.amzn2023.0.2       amazonlinux  58 k
 libnfnetlink            x86_64        1.0.1-19.amzn2023.0.2      amazonlinux  30 k
 libnftnl                x86_64        1.2.2-2.amzn2023.0.2       amazonlinux  84 k
 pigz                    x86_64        2.5-1.amzn2023.0.3         amazonlinux  83 k
 runc                    x86_64        1.3.4-1.amzn2023.0.1       amazonlinux 3.9 M

Transaction Summary
================================================================================
Install  11 Packages

Total download size: 74 M
Installed size: 281 M
Downloading Packages:
(1/11): container-selinux-2.242.0-1.amzn2023.noarch.rpm   1.6 MB/s |  58 kB  00:00
(2/11): iptables-libs-1.8.8-3.amzn2023.0.2.x86_64.rpm      14 MB/s | 401 kB  00:00
(3/11): iptables-nft-1.8.8-3.amzn2023.0.2.x86_64.rpm      6.8 MB/s | 183 kB  00:00
(4/11): libcgroup-3.0-1.amzn2023.0.1.x86_64.rpm           3.9 MB/s |  75 kB  00:00
(5/11): libnetfilter_conntrack-1.0.8-2.amzn2023.0.2.x86_64.rpm 1.9 MB/s |  58 kB  00:00
(6/11): libnfnetlink-1.0.1-19.amzn2023.0.2.x86_64.rpm     1.1 MB/s |  30 kB  00:00
ec2-user@ip-10-0-2-92:~  Ubuntu
  Verifying        : docker-25.0.14-1.amzn2023.0.1.x86_64                  3/11
  Verifying        : iptables-libs-1.8.8-3.amzn2023.0.2.x86_64             4/11
  Verifying        : iptables-nft-1.8.8-3.amzn2023.0.2.x86_64              5/11
  Verifying        : libcgroup-3.0-1.amzn2023.0.1.x86_64                   6/11
  Verifying        : libnetfilter_conntrack-1.0.8-2.amzn2023.0.2.x86_64    7/11
  Verifying        : libnfnetlink-1.0.1-19.amzn2023.0.2.x86_64             8/11
  Verifying        : libnftnl-1.2.2-2.amzn2023.0.2.x86_64                  9/11
  Verifying        : pigz-2.5-1.amzn2023.0.3.x86_64                       10/11
  Verifying        : runc-1.3.4-1.amzn2023.0.1.x86_64                     11/11
================================================================================
WARNING:
  A newer release of "Amazon Linux" is available.

  Available Versions:

  Version 2023.10.20260202:
    Run the following command to upgrade to 2023.10.20260202:

      dnf upgrade --releasever=2023.10.20260202

    Release notes:
     https://docs.aws.amazon.com/linux/al2023/release-notes/relnotes-2023.10.20260202.html

================================================================================

Installed:
  container-selinux-4:2.242.0-1.amzn2023.noarch          containerd-2.1.5-1.amzn2023.0.4.x86_64        docker-25.0.14-1.amzn2023.0.1.x86_64
  iptables-libs-1.8.8-3.amzn2023.0.2.x86_64              iptables-nft-1.8.8-3.amzn2023.0.2.x86_64      libcgroup-3.0-1.amzn2023.0.1.x86_64
  libnetfilter_conntrack-1.0.8-2.amzn2023.0.2.x86_64     libnfnetlink-1.0.1-19.amzn2023.0.2.x86_64     libnftnl-1.2.2-2.amzn2023.0.2.x86_64
  pigz-2.5-1.amzn2023.0.3.x86_64                         runc-1.3.4-1.amzn2023.0.1.x86_64

Complete!
[ec2-user@ip-10-0-2-92 ~]$ sudo systemctl start docker
[ec2-user@ip-10-0-2-92 ~]$ sudo usermod -aG docker ec2-user
[ec2-user@ip-10-0-2-92 ~]$
```

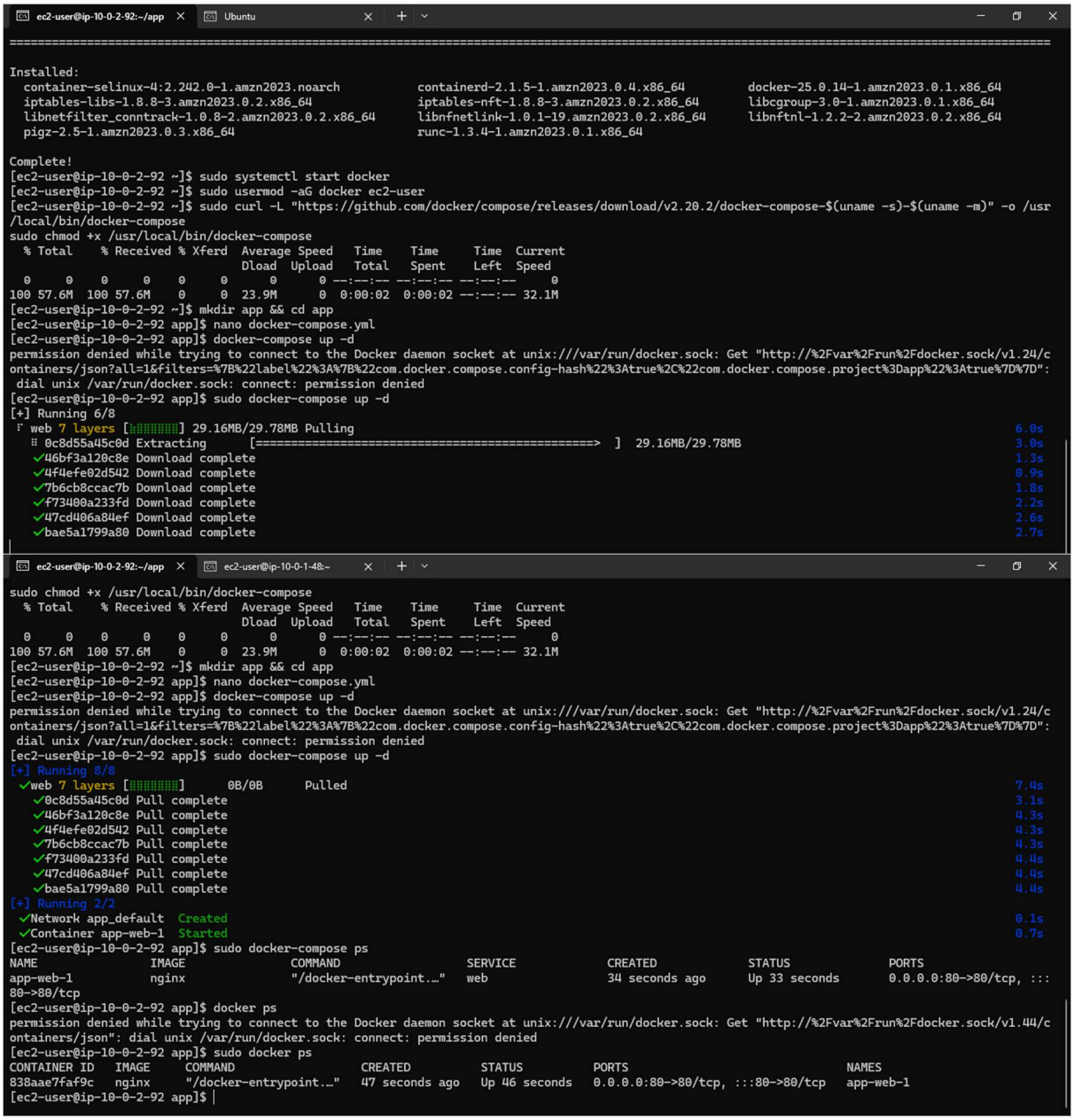


Writing docker compose:

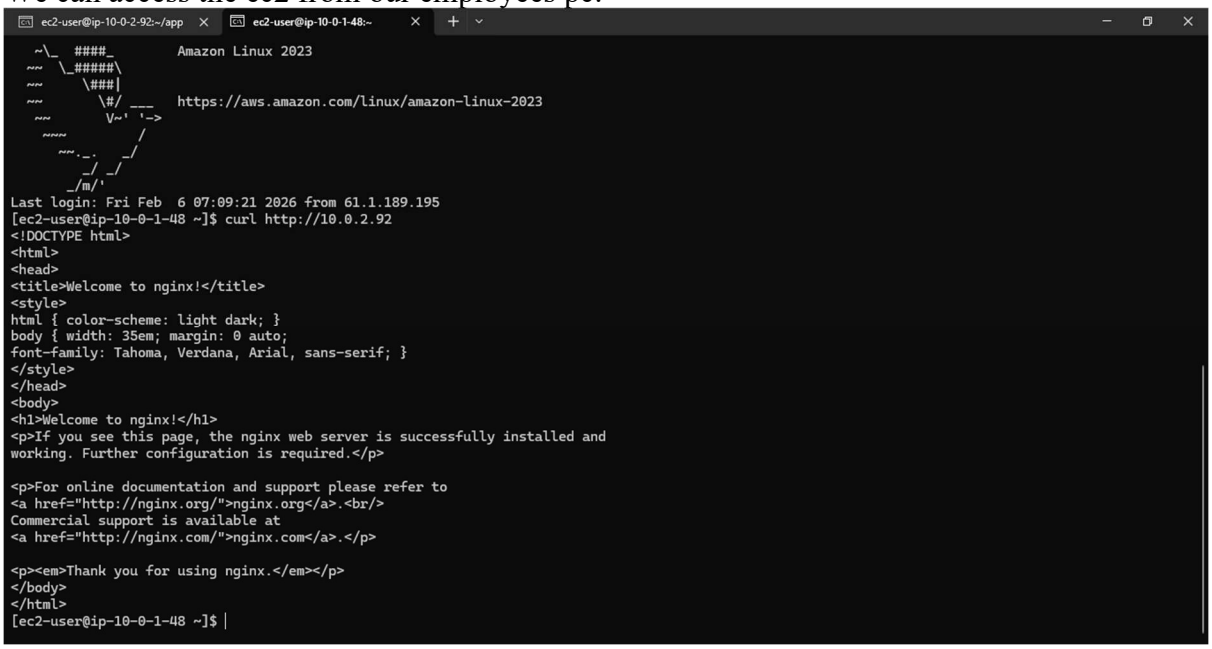




Execute Docker compose up


ec2-user@ip-10-0-2-92:~/app
Ubuntu
Installed:
container-selinux-4:2.242.0-1.amzn2023.noarch
containerd-2.1.5-1.amzn2023.0.4.x86_64
docker-25.0.14-1.amzn2023.0.1.x86_64
iptables-libs-1.8.8-3.amzn2023.0.2.x86_64
iptables-nft-1.8.8-3.amzn2023.0.2.x86_64
libcgroup-3.0-1.amzn2023.0.1.x86_64
libnetfilter_conntrack-1.0.8-2.amzn2023.0.2.x86_64
libnfnetlink-1.0.1-19.amzn2023.0.2.x86_64
libnftnl-1.2.2-2.amzn2023.0.2.x86_64
pigz-2.5-1.amzn2023.0.3.x86_64
runc-1.3.4-1.amzn2023.0.1.x86_64
Complete!
[ec2-user@ip-10-0-2-92 ~]$ sudo systemctl start docker
[ec2-user@ip-10-0-2-92 ~]$ sudo usermod -aG docker ec2-user
[ec2-user@ip-10-0-2-92 ~]$ sudo curl -L "https://github.com/docker/compose/releases/download/v2.20.2/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
sudo chmod +x /usr/local/bin/docker-compose
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 57.6M 100 57.6M 0 0 23.9M 0 0:00:02 0:00:02 --:--:-- 32.1M
[ec2-user@ip-10-0-2-92 ~]$ mkdir app && cd app
[ec2-user@ip-10-0-2-92 app]$ nano docker-compose.yml
[ec2-user@ip-10-0-2-92 app]$ docker-compose up -d
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/containers/json?all=1&filters=%7B%22label%22%3A%7B%22com.docker.compose.config-hash%22%3Atrue%2C%22com.docker.compose.project%3Dapp%22%3Atrue%7D%7D": dial unix /var/run/docker.sock: connect: permission denied
[ec2-user@ip-10-0-2-92 app]$ sudo docker-compose up -d
[+] Running 6/8
web 7 layers [⣿⣿⣿⣿⣿⣿⣿] 29.16MB/29.78MB Pulling 6.0s
0c8d55a45c0d Extracting [==========>] 29.16MB/29.78MB 3.0s
46bf3a120c8e Download complete 1.3s
4f4efe02d542 Download complete 0.9s
7b6cb8ccac7b Download complete 1.8s
f73400a233fd Download complete 2.2s
47cd406a84ef Download complete 2.6s
bae5a1799a80 Download complete 2.7s
ec2-user@ip-10-0-2-92:~/app
ec2-user@ip-10-0-1-48:~
sudo chmod +x /usr/local/bin/docker-compose
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 57.6M 100 57.6M 0 0 23.9M 0 0:00:02 0:00:02 --:--:-- 32.1M
[ec2-user@ip-10-0-2-92 ~]$ mkdir app && cd app
[ec2-user@ip-10-0-2-92 app]$ nano docker-compose.yml
[ec2-user@ip-10-0-2-92 app]$ docker-compose up -d
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/containers/json?all=1&filters=%7B%22label%22%3A%7B%22com.docker.compose.config-hash%22%3Atrue%2C%22com.docker.compose.project%3Dapp%22%3Atrue%7D%7D": dial unix /var/run/docker.sock: connect: permission denied
[ec2-user@ip-10-0-2-92 app]$ sudo docker-compose up -d
[+] Running 8/8
web 7 layers [⣿⣿⣿⣿⣿⣿⣿] 0B/0B Pulled 7.4s
0c8d55a45c0d Pull complete 3.1s
46bf3a120c8e Pull complete 4.3s
4f4efe02d542 Pull complete 4.3s
7b6cb8ccac7b Pull complete 4.3s
f73400a233fd Pull complete 4.4s
47cd406a84ef Pull complete 4.4s
bae5a1799a80 Pull complete 4.4s
[+] Running 2/2
Network app_default Created 0.1s
Container app-web-1 Started 0.7s
[ec2-user@ip-10-0-2-92 app]$ sudo docker-compose ps
NAME IMAGE COMMAND SERVICE CREATED STATUS PORTS
app-web-1 nginx "/docker-entrypoint.…" web 34 seconds ago Up 33 seconds 0.0.0.0:80->80/tcp, :::80->80/tcp
[ec2-user@ip-10-0-2-92 app]$ docker ps
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.44/containers/json": dial unix /var/run/docker.sock: connect: permission denied
[ec2-user@ip-10-0-2-92 app]$ sudo docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
838aae7faf9c nginx "/docker-entrypoint.…" 47 seconds ago Up 46 seconds 0.0.0.0:80->80/tcp, :::80->80/tcp app-web-1
[ec2-user@ip-10-0-2-92 app]$

We can access the ec2 from our employees pc:



---

11. Web Application Deployment (Docker)

Docker and Docker Compose were installed on the Private EC2.

A simple web application using Nginx was deployed using:

docker-compose.yml

- Nginx container exposed on port 80

Employees from Public EC2 successfully accessed the app using:

curl http://10.0.2.92

Direct access from internet was not possible.

---

12. Testing Results

Test	Result
Laptop → Private EC2	Blocked
Laptop → Public EC2	Allowed (SSH)
Public EC2 → Private EC2 (HTTP)	Allowed
Public EC2 → Private EC2 (SSH)	Allowed
Internet → Private EC2	Blocked

---

13. Security Best Practices Demonstrated

- Principle of Least Privilege
- Network Segmentation
- Bastion Host Access
- Defense in Depth (SG + NACL)
- Private Subnet Isolation
- Secure Administrative Access
- Controlled Application Ports

---

14. Conclusion

This project successfully redesigned an insecure cloud environment into a secure, segmented AWS architecture where:

- Internal applications are protected from internet exposure
- Employees can access the application safely
- Administrative access is tightly controlled
- Best practices in VPC design, routing, firewall rules, and subnet segregation are implemented

This architecture closely resembles real-world enterprise cloud security design.

---

15. Screenshots Attached

1. VPC and Subnets
2. Route Tables
3. Internet Gateway and NAT Gateway
4. Insecure Security Group (Before)
5. Secure Security Groups (After)
6. Network ACL rules
7. EC2 instances
8. Docker running web app
9. curl test from Public EC2

End of Report

[Rishikesh R]