Cycle 08 AWS Homework

AWS Hands-On Lab – VPC, NAT Gateway, Bastion Host, and Network Concepts

Primary Task: VPC with Public and Private Subnets

Objective:

Recreate a basic AWS VPC environment to understand routing, connectivity, and NAT Gateway usage.

Step-by-Step Implementation

1. Create a VPC

- CIDR block: `10.0.0.0/16`
- Name the VPC for identification

2. Create Subnets

- Public Subnet: `10.0.1.0/24` (enable auto-assign public IP)
- Private Subnet: `10.0.2.0/24` (disable auto-assign public IP)

3. Create and Attach Internet Gateway

- Create an Internet Gateway
- Attach it to the VPC
- Update the public subnet's route table with `0.0.0.0/0` via the IGW

4. Set Up NAT Gateway

- Allocate an Elastic IP
- Launch NAT Gateway in the public subnet using the Elastic IP
- Modify the private subnet's route table:
  - Route all traffic (`0.0.0.0/0`) to the NAT Gateway

5. Launch EC2 Instances

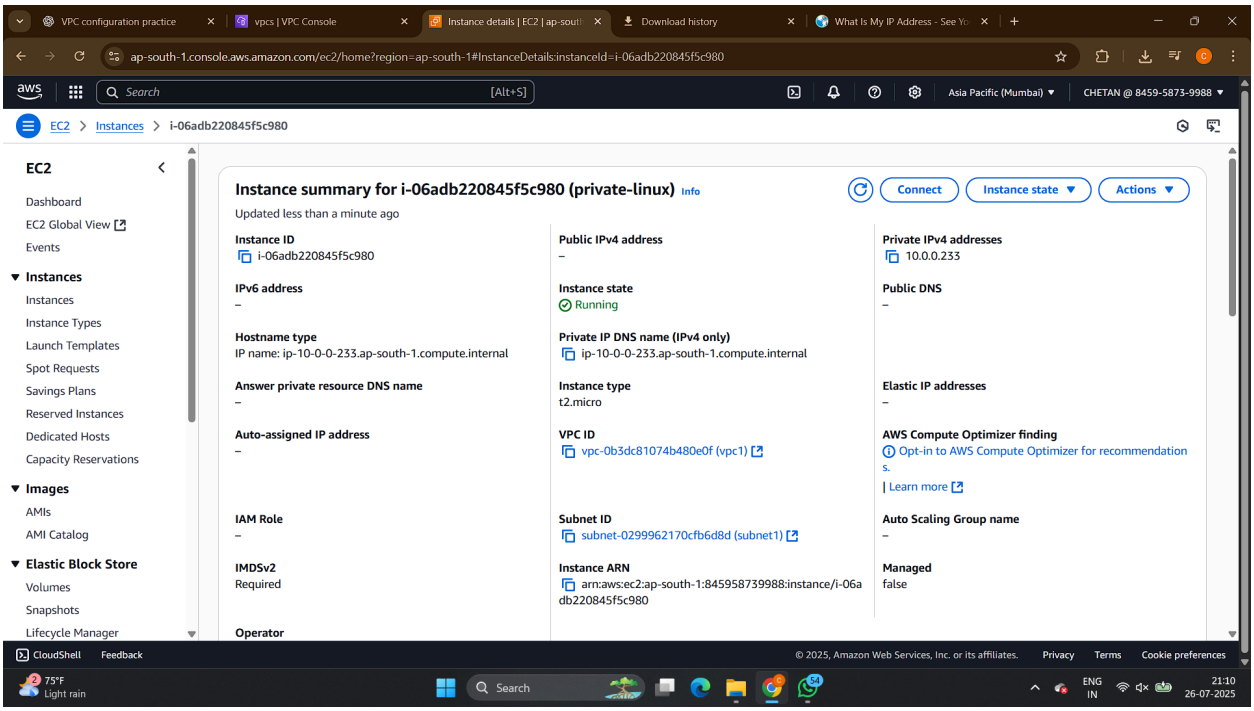
- Public EC2 instance:
  - Select public subnet
  - Enable auto-assign public IP
  - Use Amazon Linux 2 or Ubuntu
- Private EC2 instance:
  - Select private subnet
  - Do not assign public IP

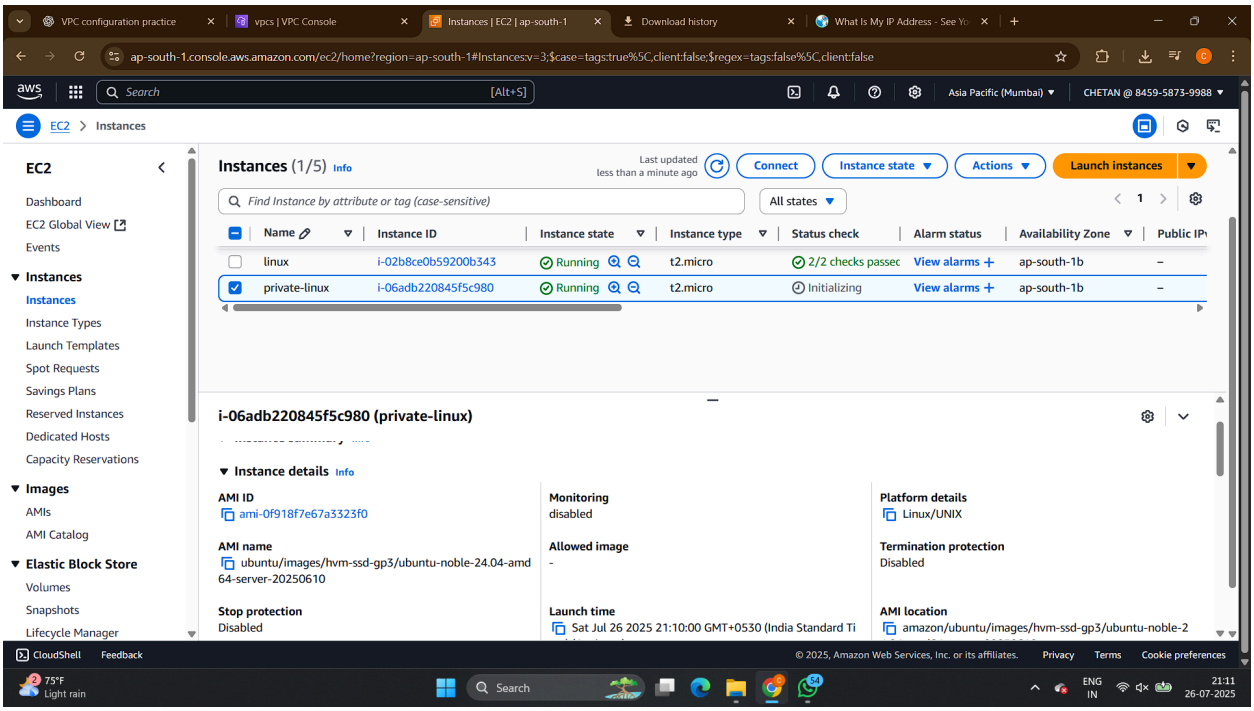
6. Verification

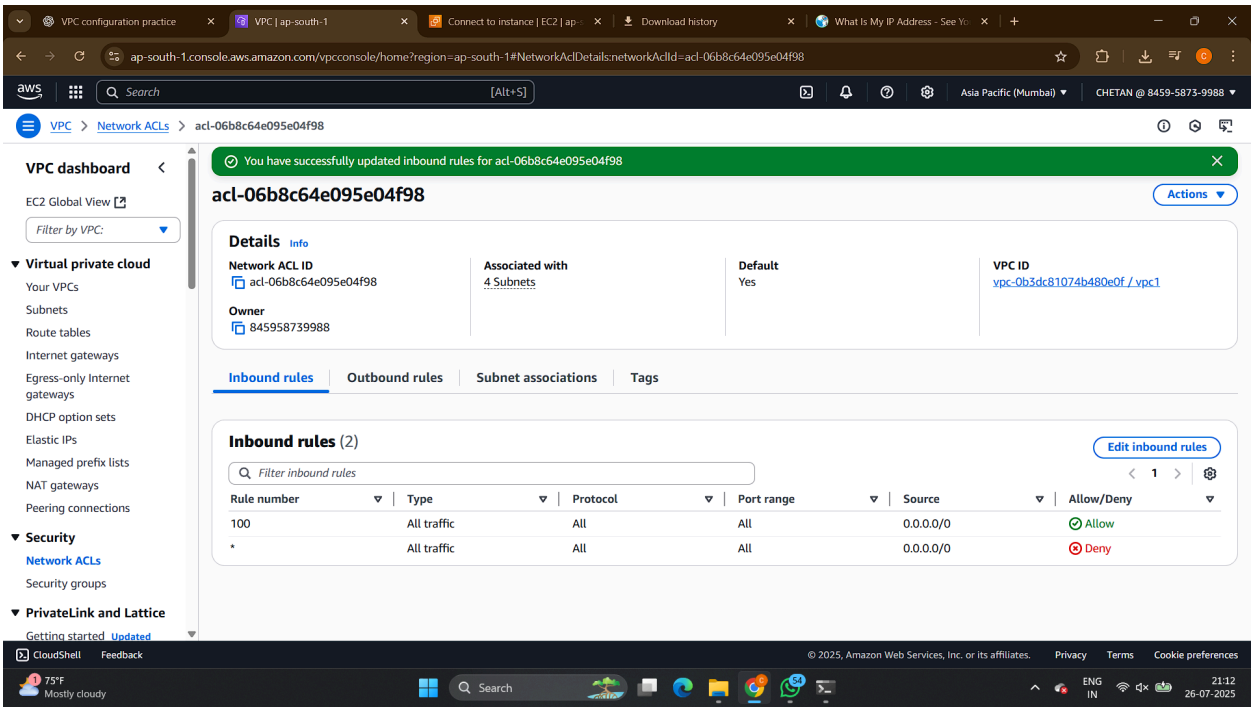
- From the public instance, run: `ping 8.8.8.8` → should succeed
- From the private instance:
  - Before NAT Gateway: ping should fail
  - After NAT Gateway: ping should succeed

7. Cleanup

- Terminate EC2 instances
- Release Elastic IP
- Delete NAT Gateway, subnets, route tables, IGW, and the VPC


VPC configuration practice
vpcs | VPC Console
Instance details | EC2 | ap-south-1
Download history
What Is My IP Address - See Yo
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-06adb220845f5c980
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
EC2 > Instances > i-06adb220845f5c980
EC2
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Instance summary for i-06adb220845f5c980 (private-linux) Info
Updated less than a minute ago
Connect
Instance state
Actions
Instance ID
i-06adb220845f5c980
IPv6 address
–
Hostname type
IP name: ip-10-0-0-233.ap-south-1.compute.internal
Answer private resource DNS name
–
Auto-assigned IP address
–
Public IPv4 address
–
Instance state
Running
Private IP DNS name (IPv4 only)
ip-10-0-0-233.ap-south-1.compute.internal
Instance type
t2.micro
VPC ID
vpc-0b3dc81074b480e0f (vpc1)
Subnet ID
subnet-0299962170cfb6d8d (subnet1)
Instance ARN
arn:aws:ec2:ap-south-1:845958739988:instance/i-06adb220845f5c980
Private IPv4 addresses
10.0.0.233
Public DNS
–
Elastic IP addresses
–
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
Learn more
Auto Scaling Group name
–
Managed
false
IAM Role
–
IMDSv2
Required
Operator
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
75°F
Light rain
Search
ENG
IN
21:10
26-07-2025


VPC configuration practice
vpcs | VPC Console
Instances | EC2 | ap-south-1
Download history
What Is My IP Address - See Yo
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
EC2 > Instances
EC2
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Instances (1/5) 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
Public IP
linux
i-02b8ce0b59200b343
Running
t2.micro
2/2 checks passed
View alarms
ap-south-1b
private-linux
i-06adb220845f5c980
Running
t2.micro
Initializing
View alarms
ap-south-1b
i-06adb220845f5c980 (private-linux)
Instance details Info
AMI ID
ami-0f918f7e67a3323f0
AMI name
ubuntu/images/hvm-ssd-gp3/ubuntu-noble-24.04-amd64-server-20250610
Stop protection
Disabled
Monitoring
disabled
Allowed image
-
Launch time
Sat Jul 26 2025 21:10:00 GMT+0530 (India Standard Ti
Platform details
Linux/UNIX
Termination protection
Disabled
AMI location
amazon/ubuntu/images/hvm-ssd-gp3/ubuntu-noble-2
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
75°F
Light rain
Search
ENG
IN
21:11
26-07-2025




```
Microsoft Windows [Version 10.0.26120.4741]
(c) Microsoft Corporation. All rights reserved.

C:\Users\cheta>cd downloads

C:\Users\cheta\Downloads>ssh -i "mykey.pem" ubuntu@13.233.155.114
ssh: connect to host 13.233.155.114 port 22: Connection timed out

C:\Users\cheta\Downloads>
```

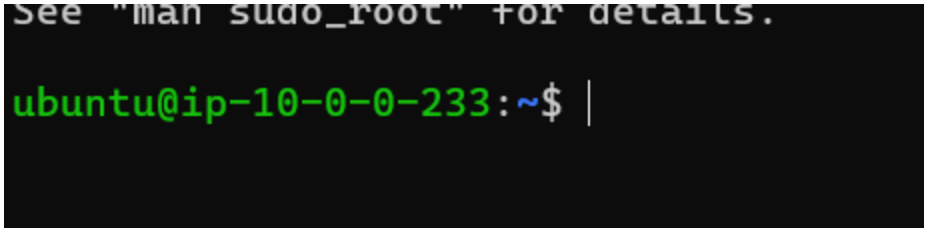
```
ubuntu@ip-10-0-0-210:~$ ping 10.0.0.233
PING 10.0.0.233 (10.0.0.233) 56(84) bytes of data.
```

```
5  sudo apt update
6  sudo apt install ipcalc
7  ipcalc 13.233.155.114
8  ipcalc 10.0.0.233
9  history
```

```
ubuntu@ip-10-0-0-210:~$ ipcalc 13.233.155.114
Address:   13.233.155.114       00001101.11101001.10011011. 01110010
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   13.233.155.0/24      00001101.11101001.10011011. 00000000
HostMin:   13.233.155.1         00001101.11101001.10011011. 00000001
HostMax:   13.233.155.254       00001101.11101001.10011011. 11111110
Broadcast: 13.233.155.255       00001101.11101001.10011011. 11111111
Hosts/Net: 254                   Class A

ubuntu@ip-10-0-0-210:~$ ipcalc 10.0.0.233
Address:   10.0.0.233           00001010.00000000.00000000. 11101001
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   10.0.0.0/24          00001010.00000000.00000000. 00000000
HostMin:   10.0.0.1             00001010.00000000.00000000. 00000001
HostMax:   10.0.0.254           00001010.00000000.00000000. 11111110
Broadcast: 10.0.0.255           00001010.00000000.00000000. 11111111
Hosts/Net: 254                   Class A, Private Internet
```

```
C:\Users\cheta>cd downloads

C:\Users\cheta\Downloads>sftp -i ~/Downloads/mykey.pem ubuntu@13.233.155.114
Connected to 13.233.155.114.
sftp> put mykey.pem
Uploading mykey.pem to /home/ubuntu/mykey.pem
mykey.pem
sftp>
```

```
ubuntu@ip-10-0-0-210:~$ ls
mykey.pem
ubuntu@ip-10-0-0-210:~$ ping 10.0.0.233
PING 10.0.0.233 (10.0.0.233) 56(84) bytes of data.
^A^H^C
--- 10.0.0.233 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8187ms

ubuntu@ip-10-0-0-210:~$ chmod 400 mykey.pem
ubuntu@ip-10-0-0-210:~$ ssh -i "mykey.pem" ubuntu@10.0.0.233
The authenticity of host '10.0.0.233 (10.0.0.233)' can't be established.
ED25519 key fingerprint is SHA256:R1Y02Y89pl4GunpQx5Ah8hn0wyZnQjlpf1ZofjCuJhA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.233' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sat Jul 26 16:17:17 UTC 2025

  System load:  0.0               Processes:             103
  Usage of /:   25.3% of 6.71GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for enX0: 10.0.0.233
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```



Conceptual Understanding

NAT Gateway vs. Internet Gateway

Feature	Internet Gateway (IGW)	NAT Gateway
Function	Allows public subnet internet access	Enables private subnet internet access
Placement	Attached to VPC	Deployed in a public subnet

Feature	Internet Gateway (IGW)	NAT Gateway
Inbound Access	Allowed (with correct security groups)	Not allowed (outbound only)
Use Case	Web servers needing public access	Private servers requiring software updates or outbound access

Why NAT Gateway Must Be in a Public Subnet

- A NAT Gateway needs internet access to forward outbound requests.
- Only a public subnet (with a route to an Internet Gateway) provides this capability.
- If placed in a private subnet, it cannot access the internet, defeating its purpose.

Bastion Host

Definition:

A bastion host is a secure EC2 instance in the public subnet that acts as a jump server to access private EC2 instances.

Use Case:

- Used to SSH into private EC2 instances securely
- Limits exposure of private instances to the internet
- Allows centralized monitoring and control of access

Steps:

1. Launch a Linux EC2 instance in the public subnet
2. SSH into bastion from local machine using public IP
3. From bastion, SSH into the private EC2 instance using its private IP

Optional Exploration Tasks

Task 1: Bastion Host Setup

- Launch a bastion host in the public subnet
- SSH into the private EC2 instance via the bastion using a shared key pair

Task 2: VPC Peering

- Create two separate VPCs
- Establish a VPC Peering connection between them
- Update route tables to allow traffic between them
- Launch instances in each VPC and test connectivity

Task 3: Network ACLs vs. Security Groups

Feature	Network ACLs	Security Groups
Scope	Subnet-level	Instance-level
State	Stateless (rules must be bidirectional)	Stateful (return traffic automatically allowed)
Rules	Evaluated in order by rule number	All rules evaluated together
Use Case	Broad restrictions or IP blocking	Fine-grained access control

Suggested EOD Status Report Format

Date: 08 August 2025

Name: [Your Name]

Tasks Completed:

- Created VPC with public and private subnets
- Configured Internet and NAT Gateways
- Deployed public and private EC2 instances
- Verified internet access and NAT functionality
- Set up bastion host for private instance access

Concepts Explored:

- VPC architecture and route table management
- Differences between NAT Gateway and Internet Gateway
- Bastion host security advantages
- Network ACLs vs. Security Groups

Learning Outcomes:

- Understood routing dependencies for internet access
- Gained hands-on practice with secure access patterns
- Learned to troubleshoot and test network connectivity

Screenshots Included:

- VPC setup
- Subnet configuration
- Route tables
- EC2 instance ping tests
- SSH sessions through bastion host