Cycle 08 AWS Homework - VPC

Explore, Understand and Document your Findings

1. Completing VPC Configurations

Info:

- A **Virtual Private Cloud (VPC)** is a logically isolated network in AWS where we can launch AWS resources.
- **Subnetting** divides the VPC CIDR block into smaller subnets. These subnets can be classified as public or private based on route table configurations.
- **Public Subnets** have a route to the Internet Gateway, allowing instances to be accessed from the internet.
- **Private Subnets** have no direct route to the internet, so instances in them are isolated unless configured with a NAT Gateway for outbound access.
- **Availability Zones (AZs)** offer high availability. By distributing resources across AZs, we reduce the risk of a single point of failure.
- Creating 2 public and 2 private subnets in different AZs ensures high availability and fault tolerance.

---

2. Internet Gateway & Routing

Info:

- An **Internet Gateway (IGW)** is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet.
- **Route Tables** determine how network traffic is directed.
- For public access:
  - A route table associated with a public subnet must include a route `0.0.0.0/0 → IGW`.

    - EC2 instances in public subnets must also have a **public IP** and a **security group** allowing inbound SSH or ICMP.
- Verifying internet access using `ping 8.8.8.8` confirms proper routing and IGW setup.

---

3. NACL vs Security Groups

Info:

- **Network Access Control Lists (NACLs)** operate at the subnet level and support stateless traffic filtering (both inbound and outbound rules must be defined).
- **Security Groups** are virtual firewalls for EC2 instances and are stateful (return traffic is automatically allowed).
- Use case:
    - NACL is useful to enforce broad network rules like blocking an IP range.
    - Security Groups are ideal for instance-level access control.
- By denying SSH from a specific IP in NACL and allowing only your IP in the Security Group, you can observe how layered security affects connectivity.
- Tools like `telnet` or `nc` (netcat) can test if specific ports are open or blocked.

---

4. Bastion Host Setup

Info:

- A **bastion host** is an EC2 instance that acts as a jump server to securely access private instances.
- The bastion is placed in a **public subnet** with a public IP and open SSH port (22).
- Private instances (without public IPs) reside in private subnets and are not directly reachable from the internet.
- **SSH agent forwarding** lets your local SSH agent securely pass authentication through the bastion to the private instance.

- The format used to access a private instance via bastion:

```
sql
CopyEdit
ssh -A -J user@bastion-ip user@private-ip
```

- This ensures secure access while keeping private resources isolated from public exposure.

---

5. Research on NAT Gateway

Info:

- A **NAT Gateway** allows private instances to initiate outbound connections to the internet while preventing inbound connections from the internet.
- NAT is required for private subnets if the instances need to:
  - Download updates
  - Access external APIs
  - Upload logs to S3, etc.
- NAT Gateway is deployed in a **public subnet**.
- The route table of the **private subnet** should have:
  - Route: `0.0.0.0/0 → NAT Gateway`
- In contrast, public subnets route `0.0.0.0/0 → IGW`.

Task 1: VPC & Subnetting Lab

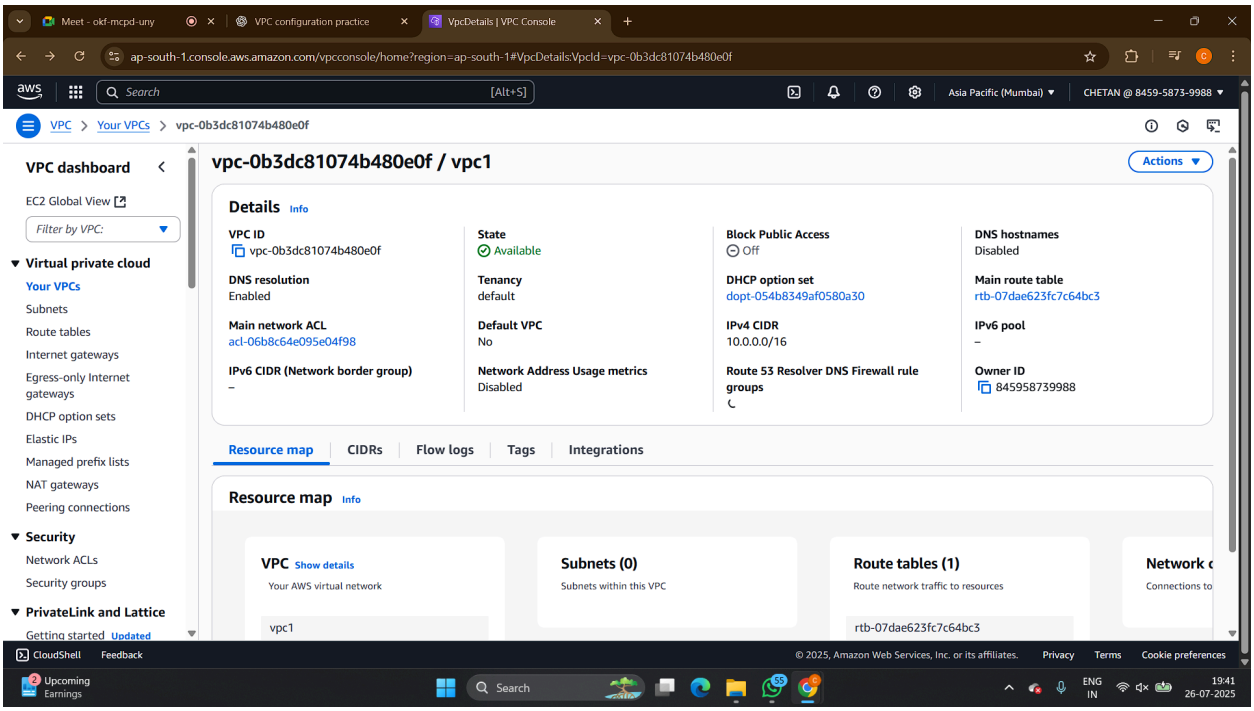
Steps:

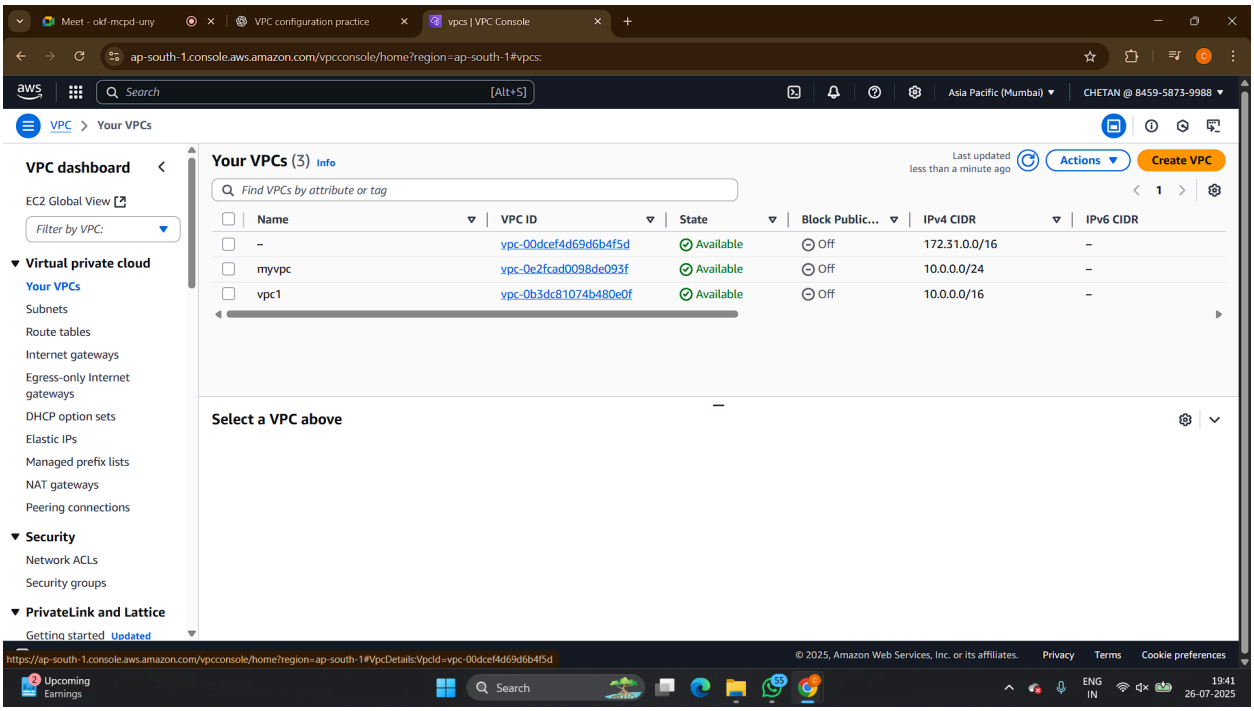
- Create a custom VPC with CIDR: `10.1.0.0/16`
- Create 2 public subnets:
  - `10.1.1.0/24` in `ap-south-1a`
  - `10.1.2.0/24` in `ap-south-1b`

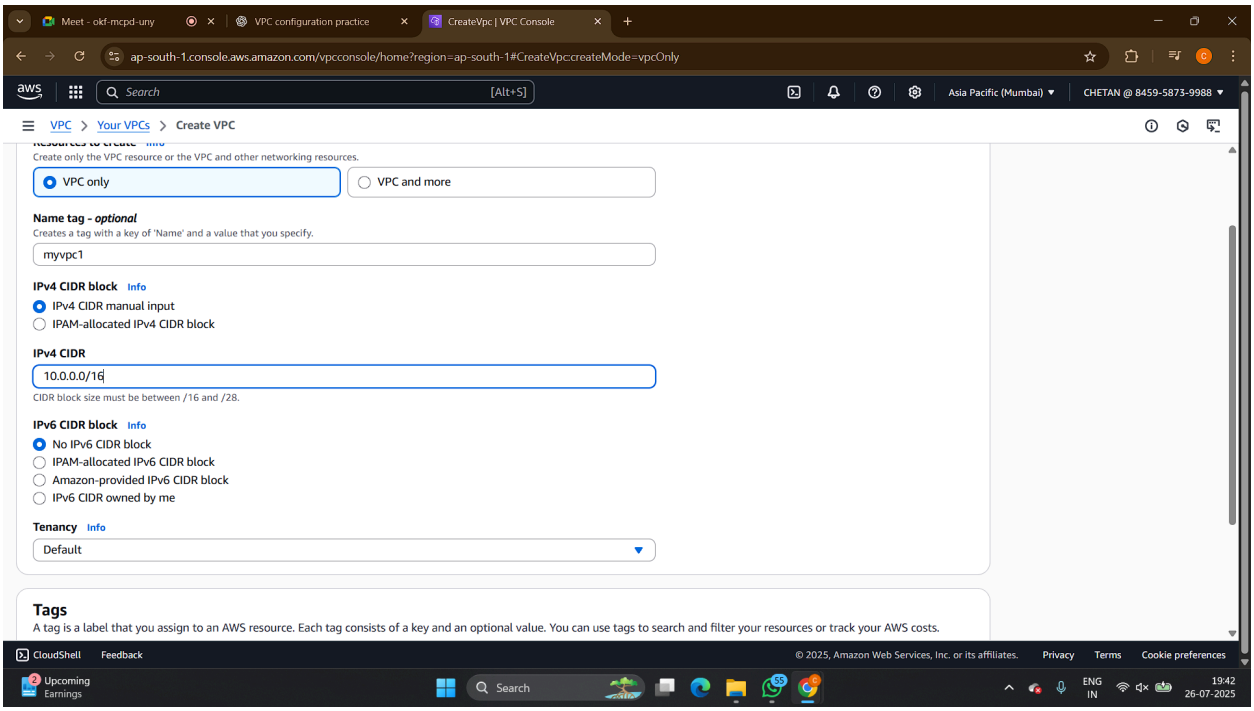
- Create 2 private subnets:
  - `10.1.3.0/24` in `ap-south-1a`
  - `10.1.4.0/24` in `ap-south-1b`

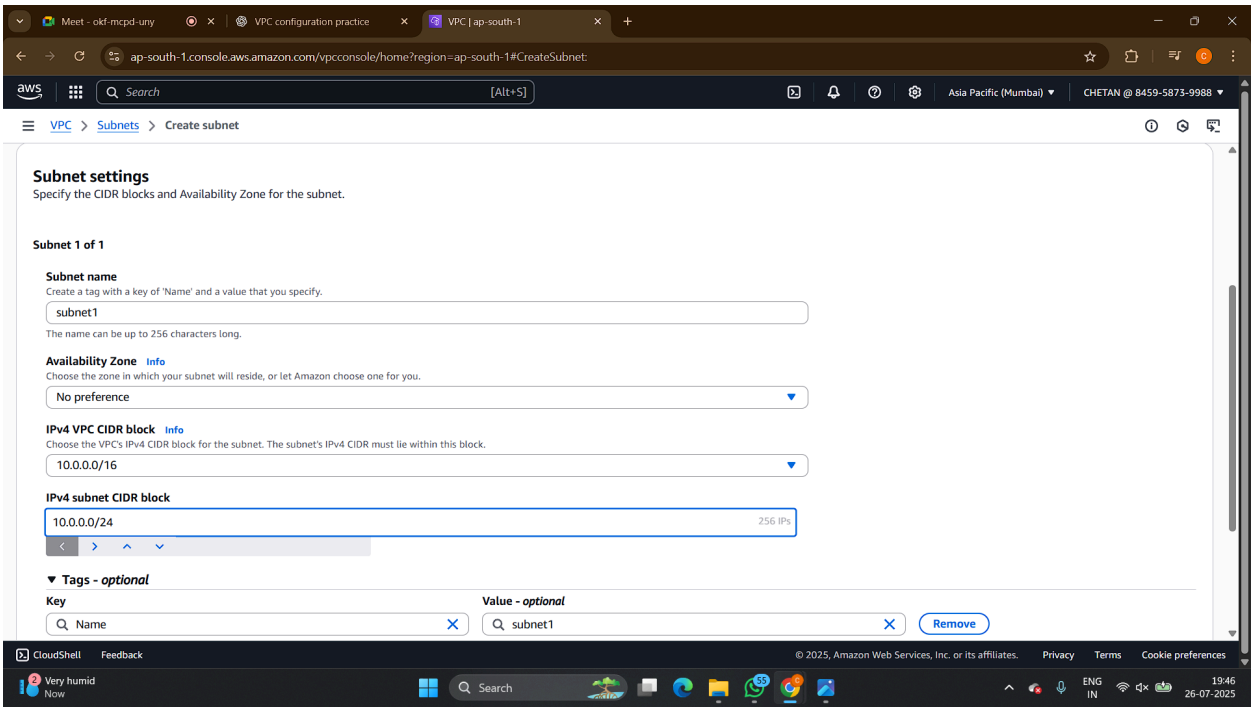
Deliverable:

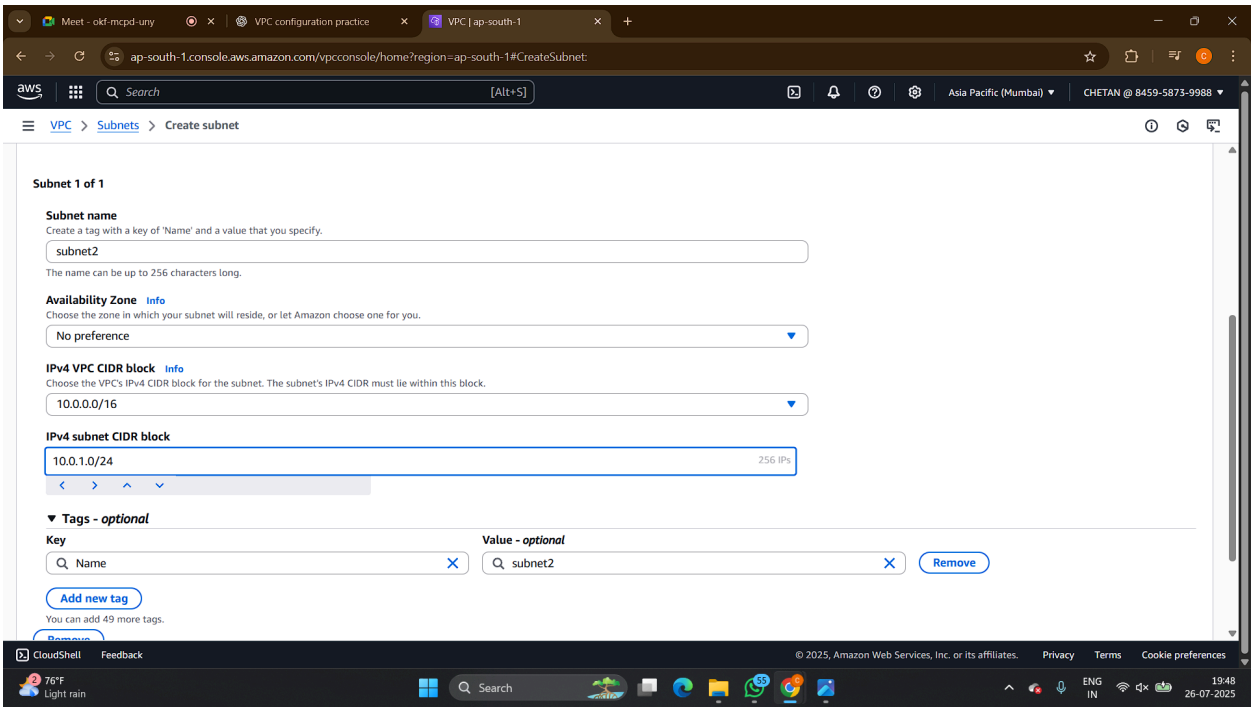
- Screenshot of VPC with all 4 subnets showing CIDR and AZ mapping in the Subnets page.

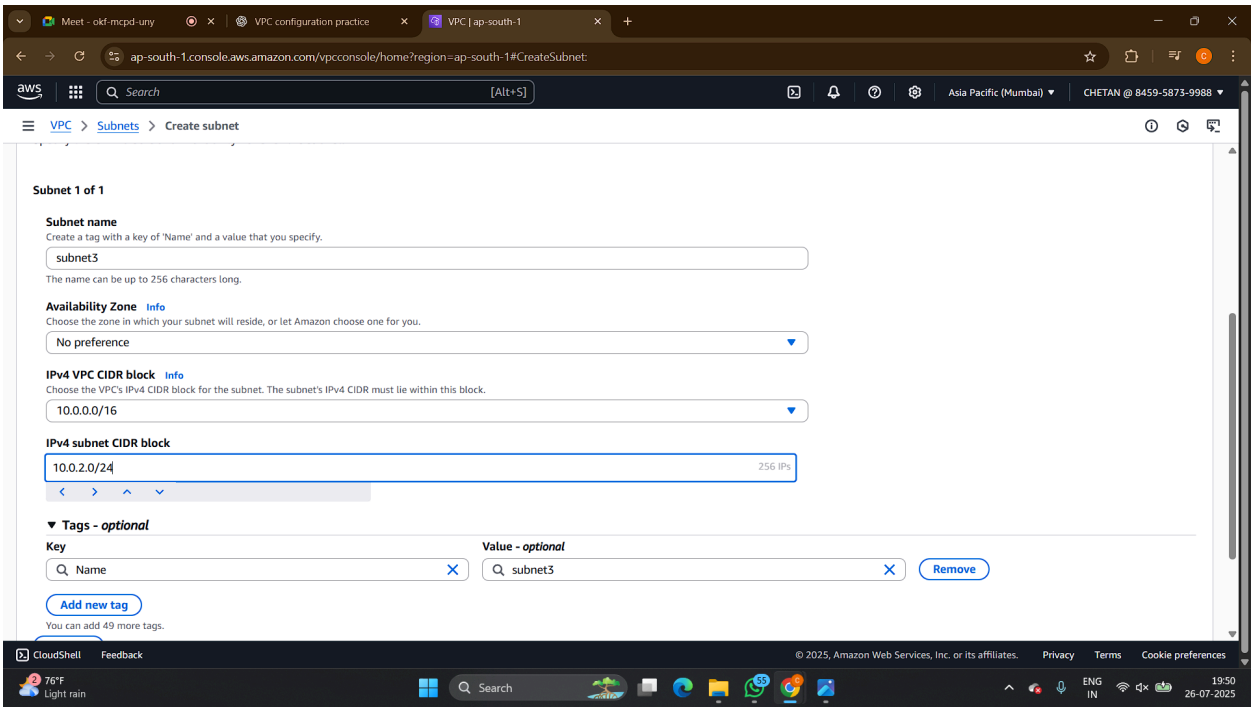


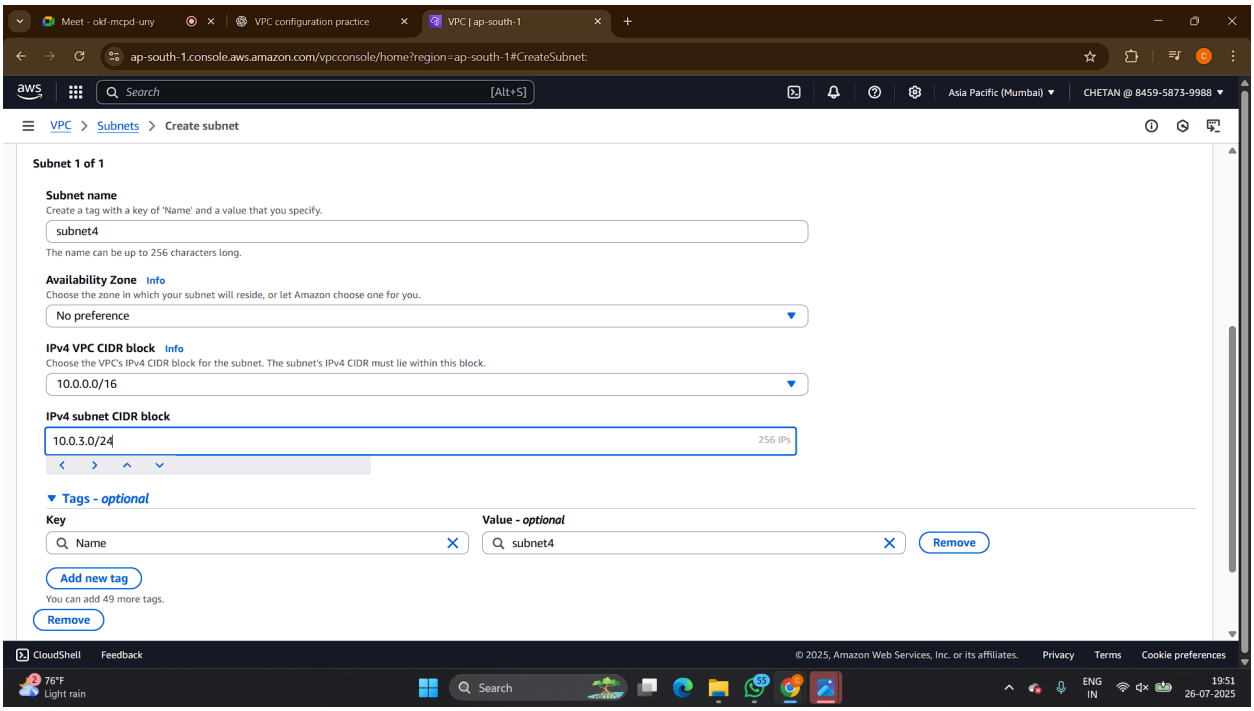

Meet - okf-mcpd-uny
VPC configuration practice
vpcs | VPC Console
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#vpcs:
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Your VPCs
VPC dashboard
EC2 Global View
Filter by VPC:
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
PrivateLink and Lattice
Getting started Updated
Your VPCs (3) Info
Last updated less than a minute ago
Actions
Create VPC
Find VPCs by attribute or tag
Name
VPC ID
State
Block Public...
IPv4 CIDR
IPv6 CIDR
– vpc-00dcef4d69d6b4f5d Available Off 172.31.0.0/16 –
myvpc vpc-0e2fcad0098de093f Available Off 10.0.0.0/24 –
vpc1 vpc-0b3dc81074b480e0f Available Off 10.0.0.0/16 –
Select a VPC above
https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#VpcDetails:VpcId=vpc-00dcef4d69d6b4f5d
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Upcoming Earnings
Search
ENG IN
19:41
26-07-2025

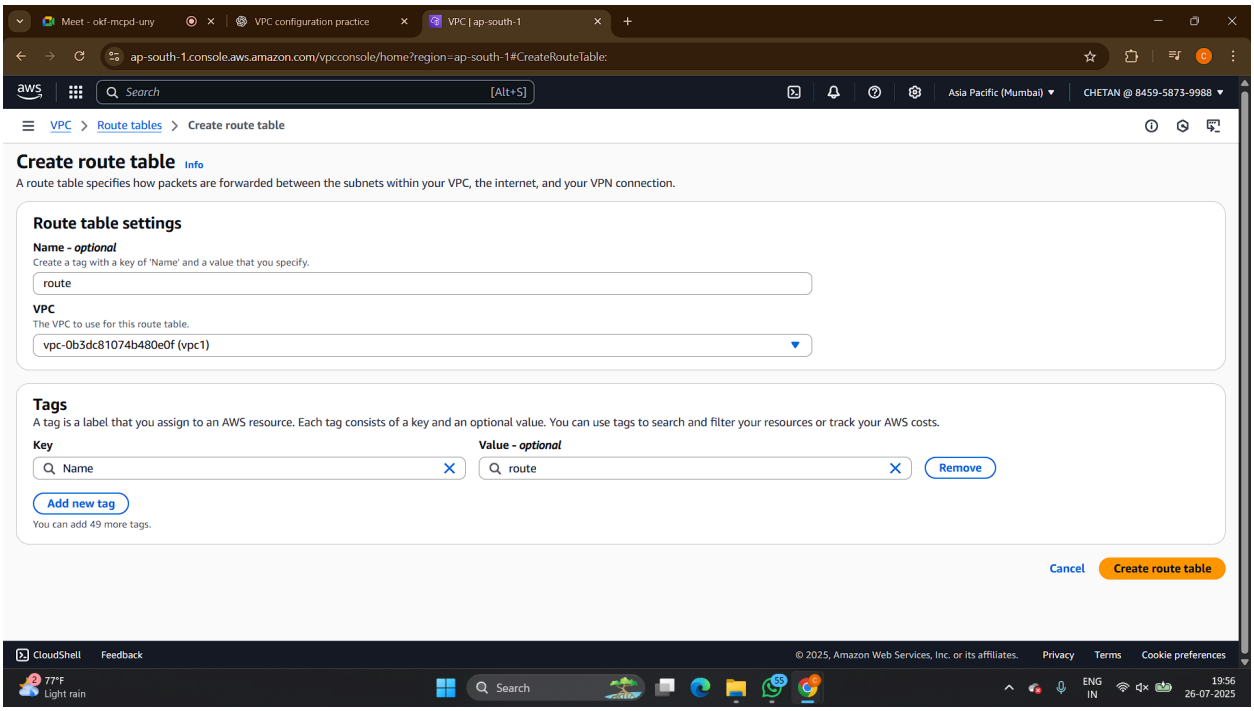

Meet - okf-mcpd-uny
VPC configuration practice
CreateVpc | VPC Console
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateVpc:createMode=vpcOnly
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Your VPCs > Create VPC
Create only the VPC resource or the VPC and 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.
myvpc1
IPv4 CIDR block Info
IPv4 CIDR manual input
IPAM-allocated IPv4 CIDR block
IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me
Tenancy Info
Default
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Upcoming Earnings
Search
ENG IN
19:42
26-07-2025

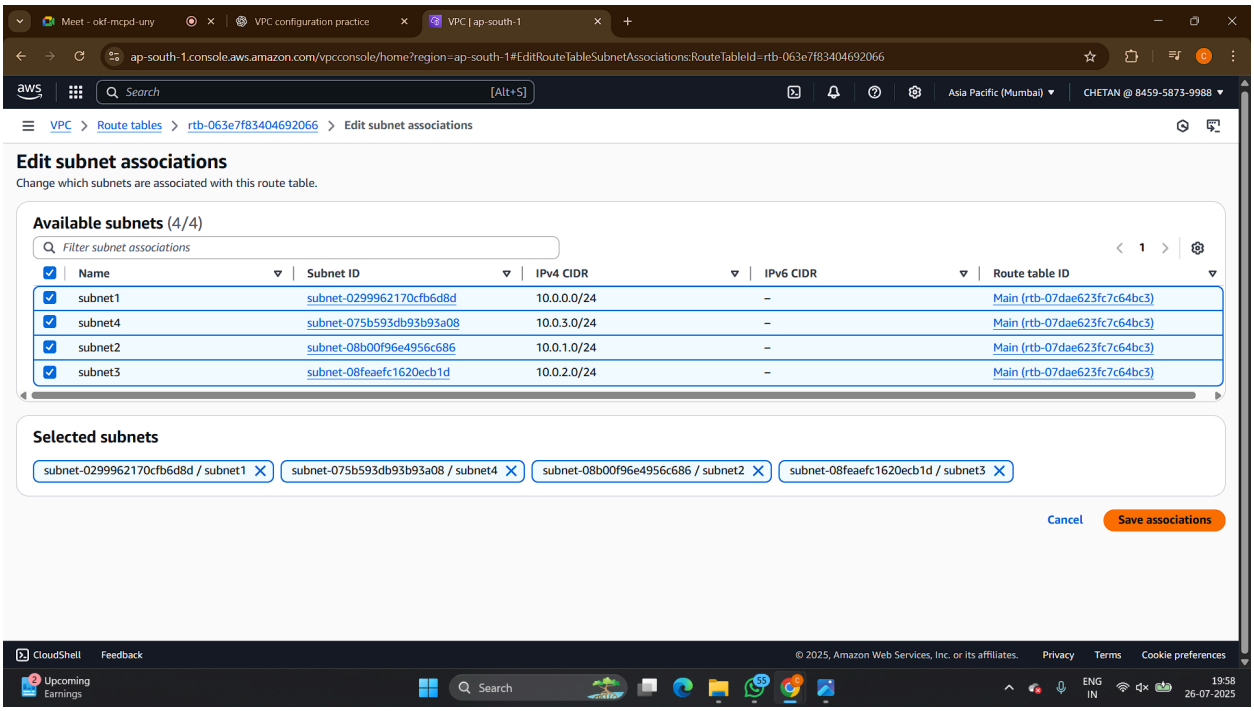

Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateSubnet:
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Subnets > Create subnet
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
subnet1
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.
No preference
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
10.0.0.0/24
256 IPs
Tags - optional
Key
Value - optional
Name
subnet1
Remove
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Very humid
Now
Search
ENG
IN
19:46
26-07-2025

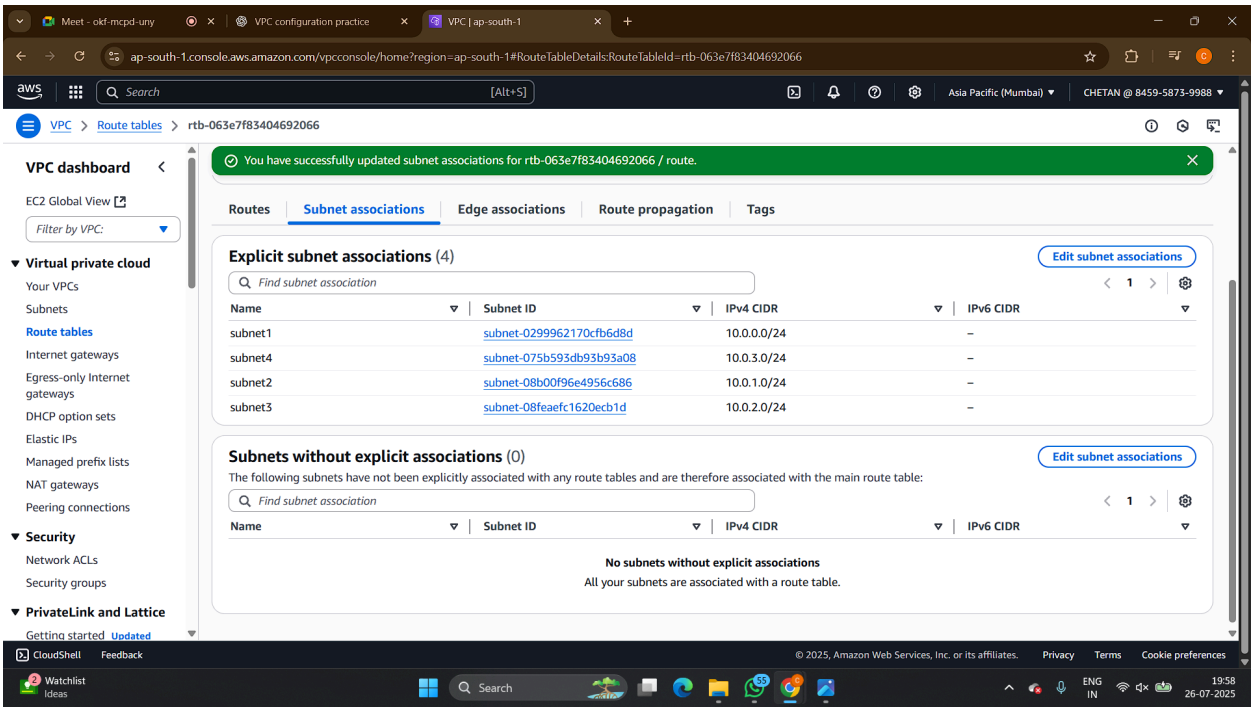

Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateSubnet:
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Subnets > Create subnet
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
subnet2
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.
No preference
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
subnet2
Remove
Add new tag
You can add 49 more tags.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
76°F
Light rain
Search
ENG
IN
19:48
26-07-2025

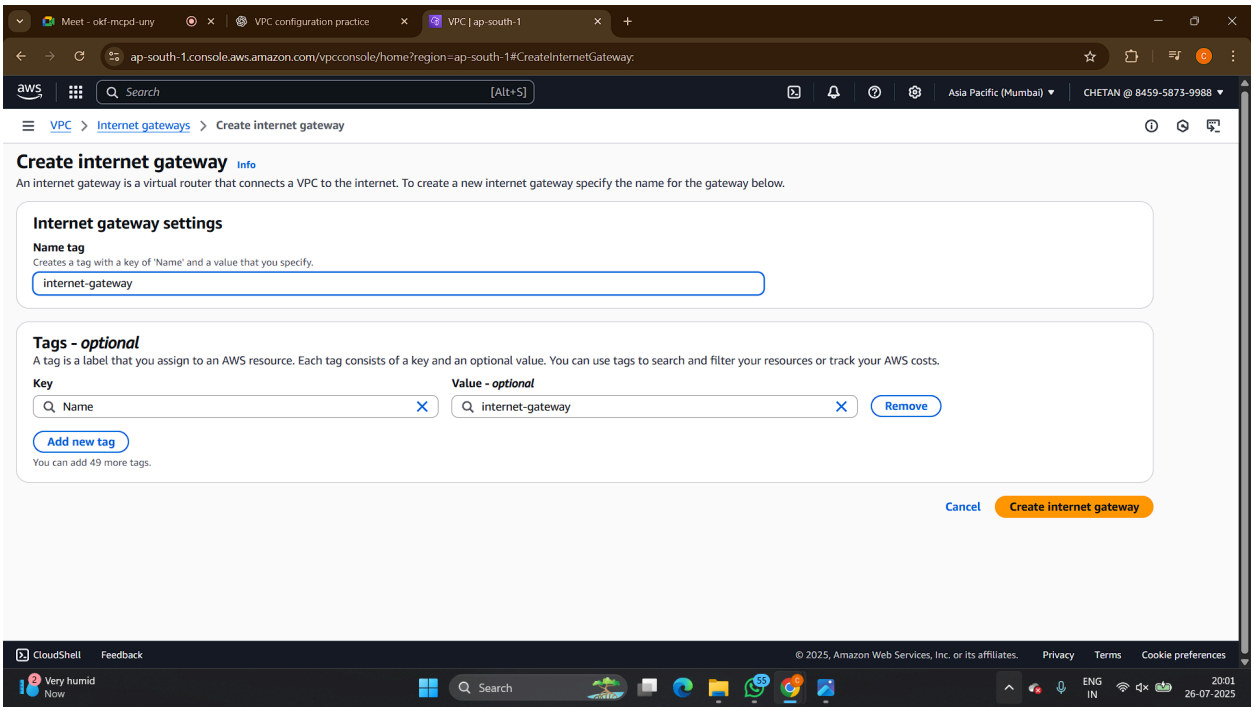

Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateSubnet:
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Subnets > Create subnet
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
subnet3
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.
No preference
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
subnet3
Remove
Add new tag
You can add 49 more tags.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
76°F
Light rain
Search
ENG
IN
19:50
26-07-2025

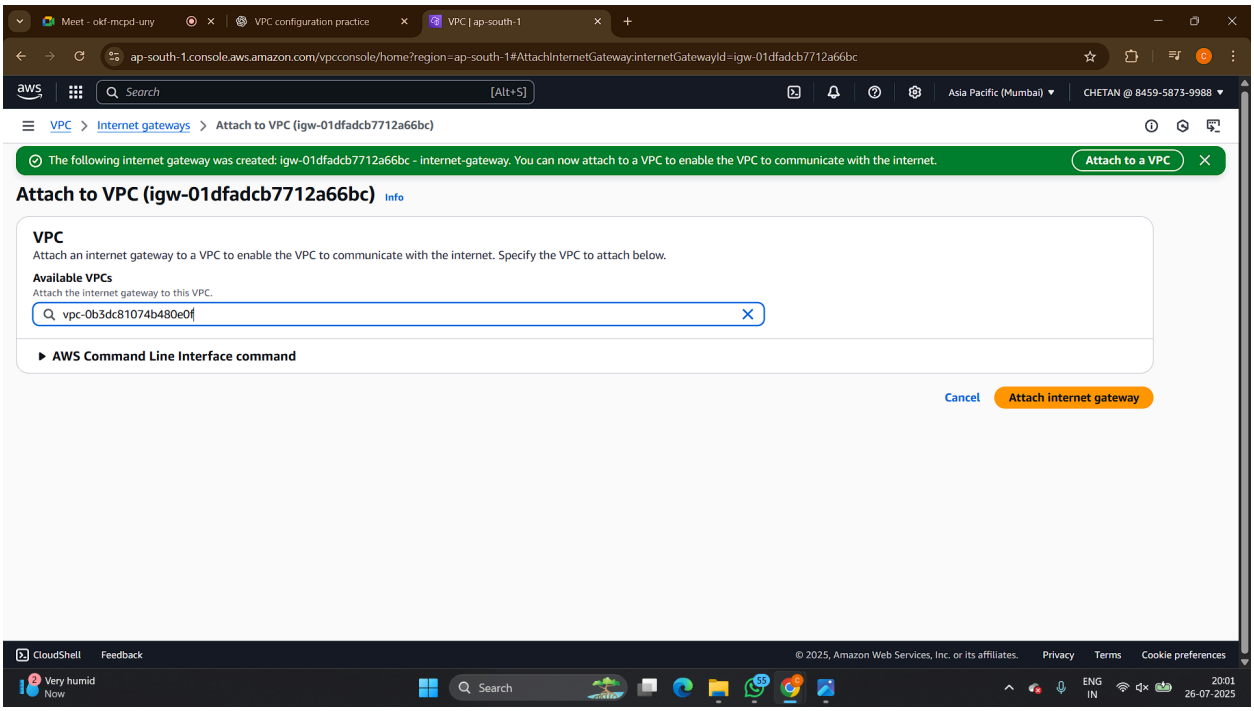

Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateSubnet:
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Subnets > Create subnet
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
subnet4
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.
No preference
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
10.0.3.0/24
256 IPs
Tags - optional
Key
Value - optional
Name
subnet4
Remove
Add new tag
You can add 49 more tags.
Remove
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
76°F
Light rain
Search
ENG
IN
19:51
26-07-2025

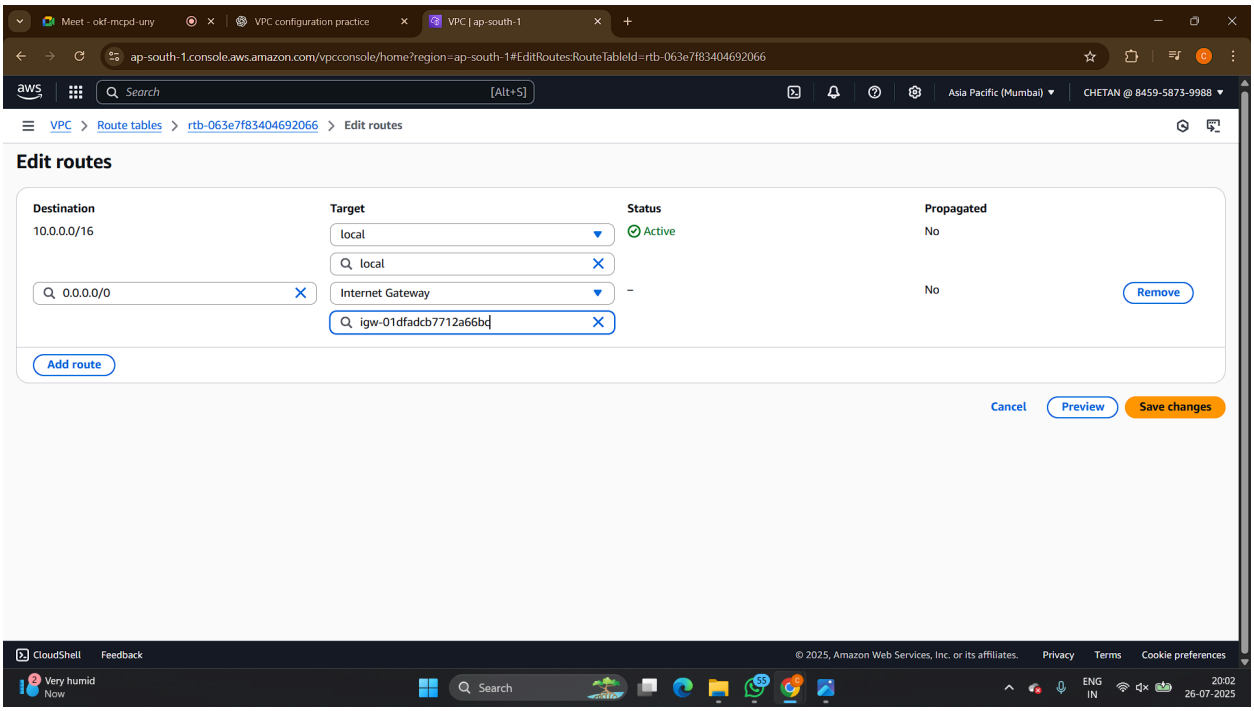

Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateRouteTable:
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Route tables > Create route table
Create route table Info
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
route
VPC
The VPC to use for this route table.
vpc-0b3dc81074b480e0f (vpc1)
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Name
Value - optional
route
Remove
Add new tag
You can add 49 more tags.
Cancel
Create route table
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
77°F
Light rain
Search
ENG
IN
19:56
26-07-2025

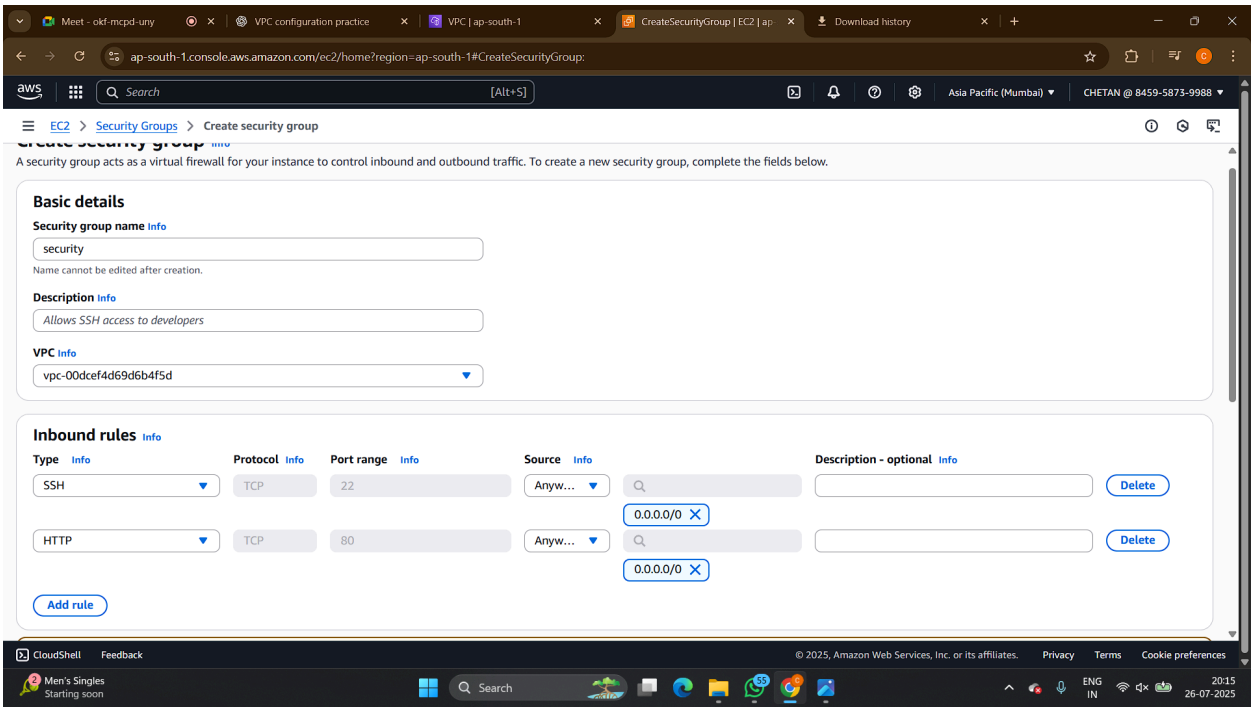

Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-063e7f83404692066
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Route tables > rtb-063e7f83404692066 > Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (4/4)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
subnet1 subnet-0299962170cfb6d8d 10.0.0.0/24 – Main (rtb-07dae623fc7c64bc3)
subnet4 subnet-075b593db93b93a08 10.0.3.0/24 – Main (rtb-07dae623fc7c64bc3)
subnet2 subnet-08b00f96e4956c686 10.0.1.0/24 – Main (rtb-07dae623fc7c64bc3)
subnet3 subnet-08feaefc1620ecb1d 10.0.2.0/24 – Main (rtb-07dae623fc7c64bc3)
Selected subnets
subnet-0299962170cfb6d8d / subnet1
subnet-075b593db93b93a08 / subnet4
subnet-08b00f96e4956c686 / subnet2
subnet-08feaefc1620ecb1d / subnet3
Cancel
Save associations
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Upcoming Earnings
Search
ENG
IN
19:58
26-07-2025

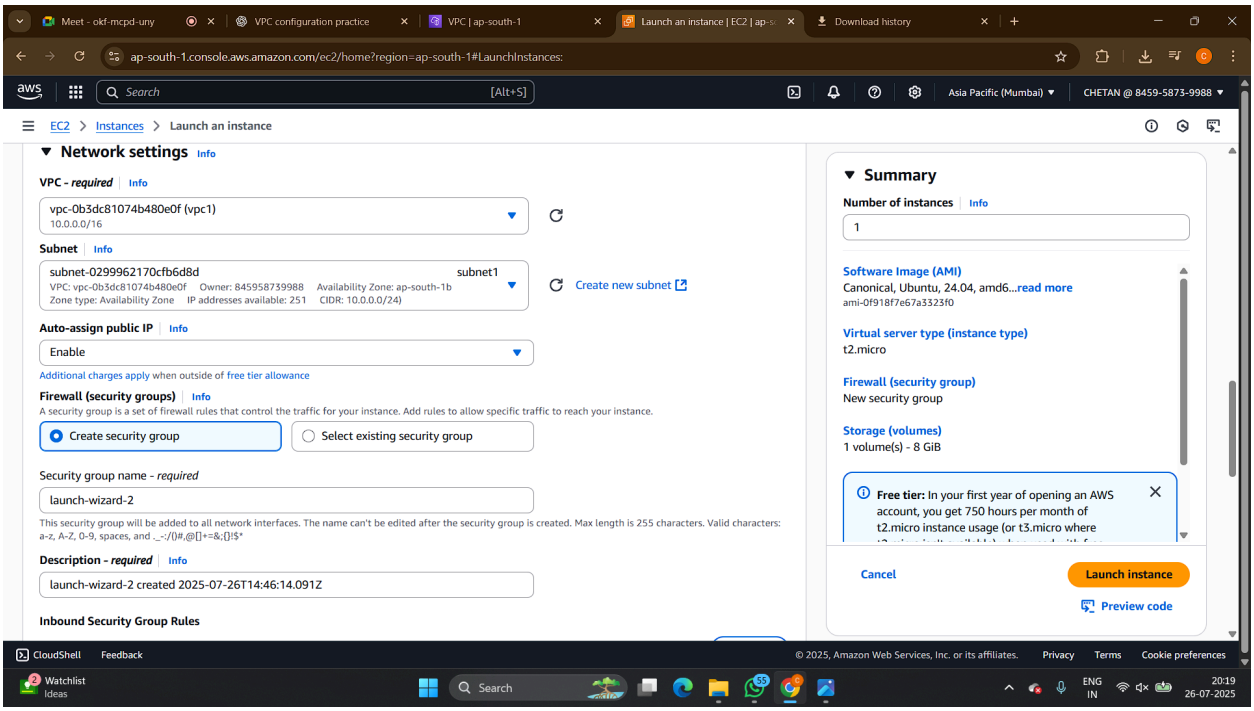

Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-063e7f83404692066
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Route tables > rtb-063e7f83404692066
VPC dashboard
EC2 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
Security
Network ACLs
Security groups
PrivateLink and Lattice
Getting started Updated
You have successfully updated subnet associations for rtb-063e7f83404692066 / route.
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (4)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
subnet1 subnet-0299962170cfb6d8d 10.0.0.0/24 –
subnet4 subnet-075b593db93b93a08 10.0.3.0/24 –
subnet2 subnet-08b00f96e4956c686 10.0.1.0/24 –
subnet3 subnet-08feaefc1620ecb1d 10.0.2.0/24 –
Subnets without explicit associations (0)
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:
No subnets without explicit associations
All your subnets are associated with a route table.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Watchlist Ideas
ENG IN
19:58 26-07-2025

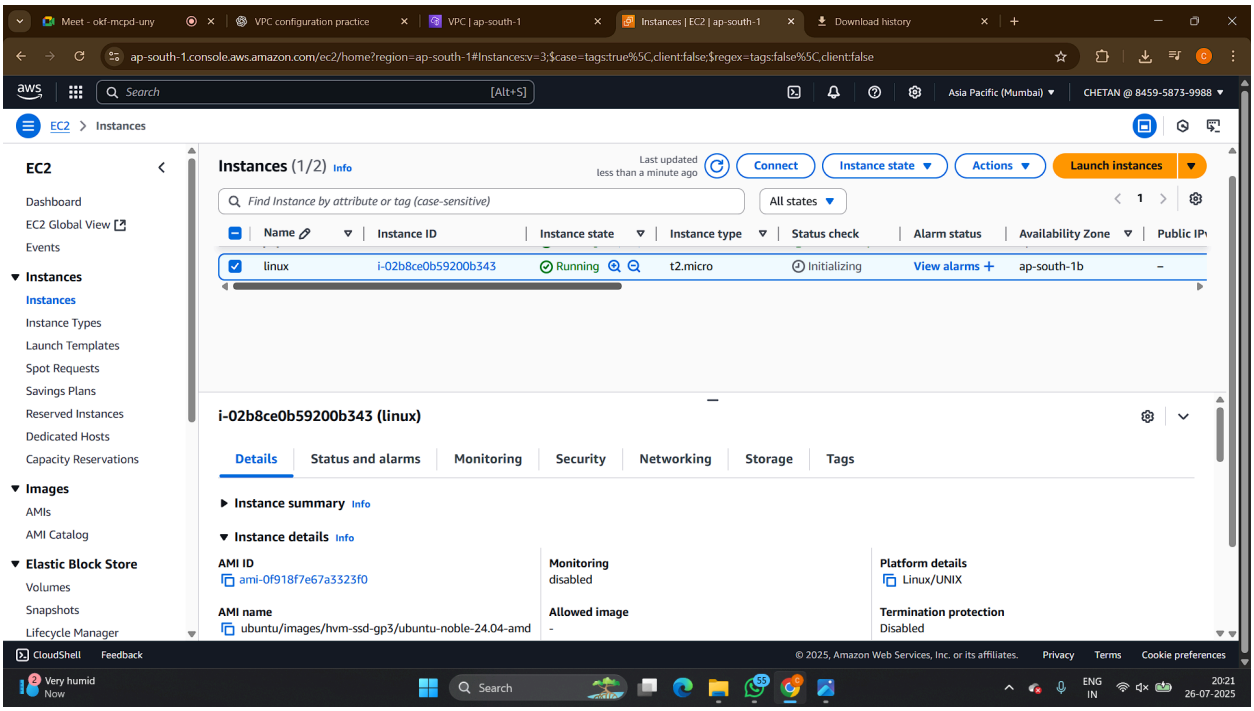

Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateInternetGateway:
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Internet gateways > Create internet gateway
Create internet gateway Info
An internet 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.
internet-gateway
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
internet-gateway
Remove
Add new tag
You can add 49 more tags.
Cancel
Create internet gateway
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Very humid Now
ENG IN
20:01 26-07-2025

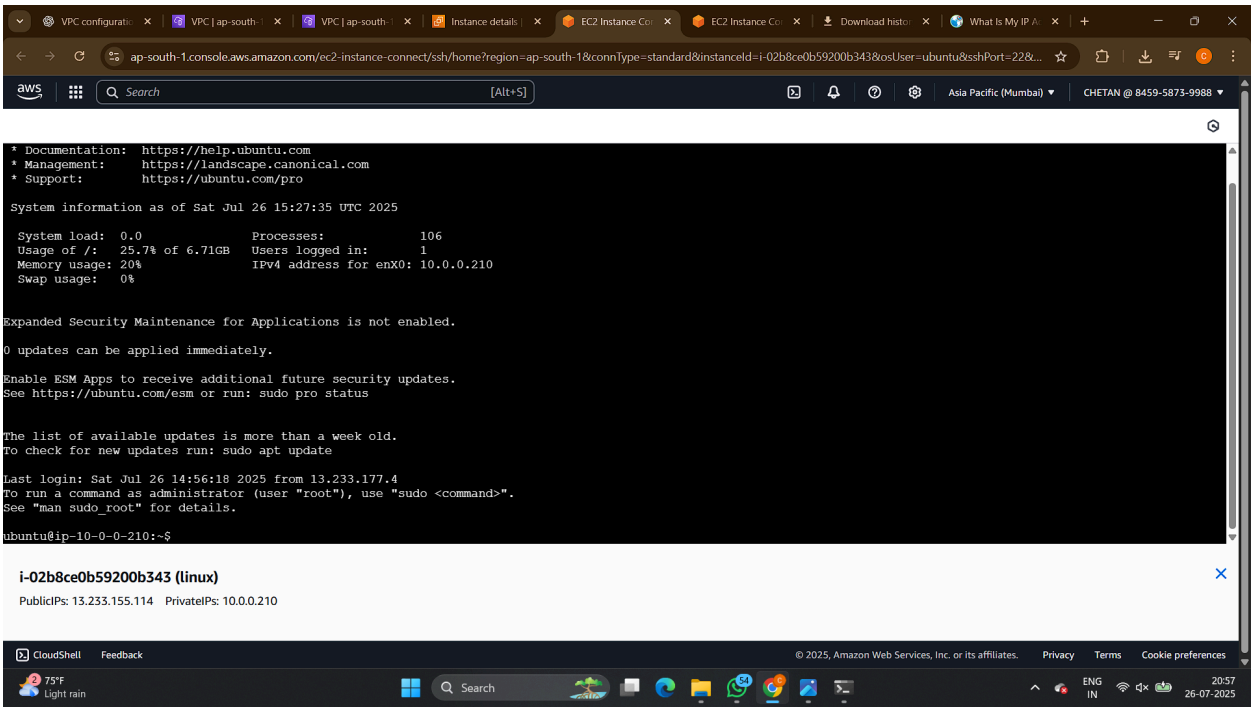

Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#AttachInternetGateway:internetGatewayId=igw-01dfadcb7712a66bc
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Internet gateways > Attach to VPC (igw-01dfadcb7712a66bc)
The following internet gateway was created: igw-01dfadcb7712a66bc - internet-gateway. You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
Attach to VPC (igw-01dfadcb7712a66bc) 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-0b3dc81074b480e0f
AWS Command Line Interface command
Cancel
Attach internet gateway
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Very humid
Now
Search
ENG
IN
20:01
26-07-2025

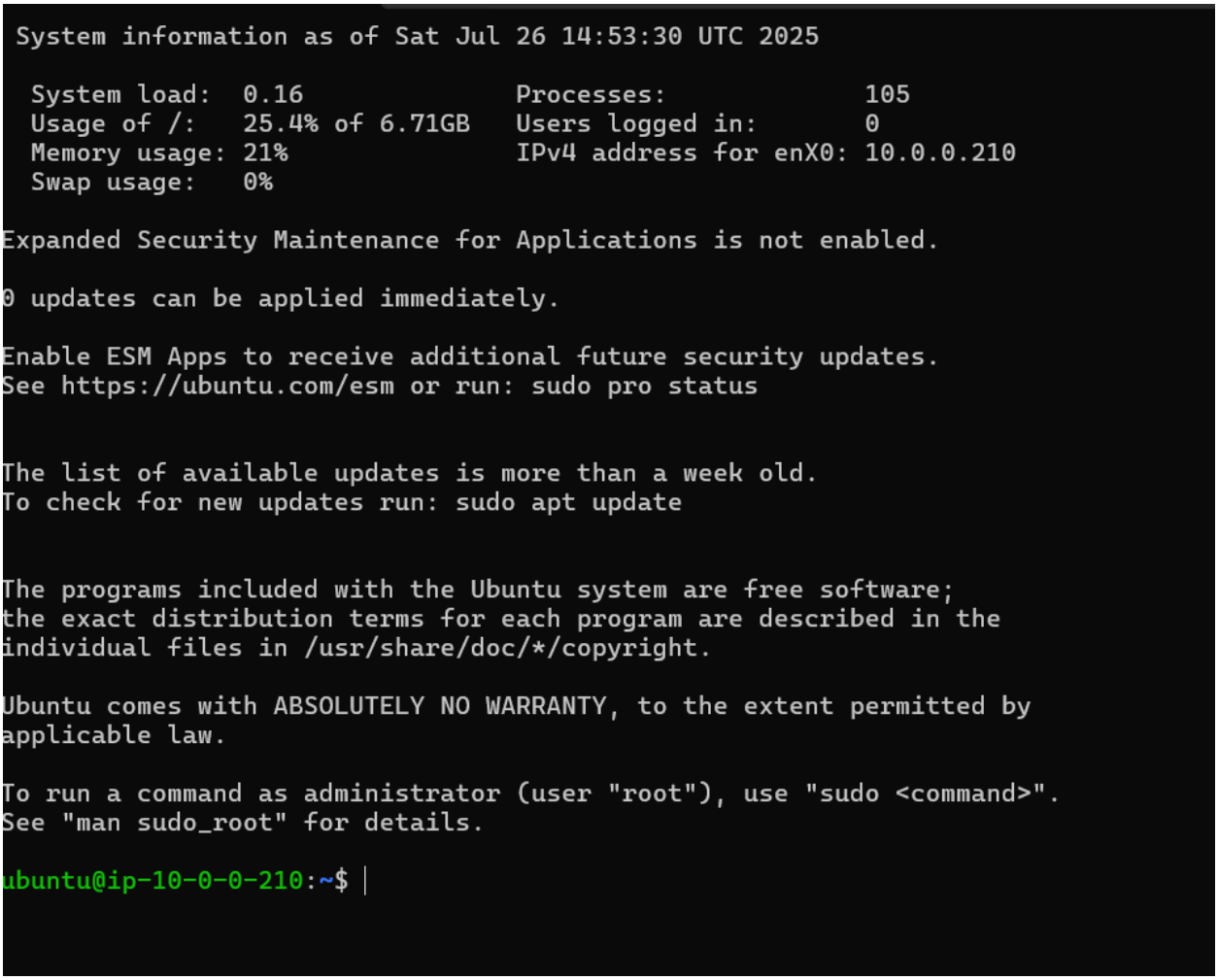

Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditRoutes:RouteTableId=rtb-063e7f83404692066
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Route tables > rtb-063e7f83404692066 > Edit routes
Edit routes
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No
local
0.0.0.0/0
Internet Gateway
–
No
Remove
igw-01dfadcb7712a66bc
Add route
Cancel
Preview
Save changes
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Very humid
Now
Search
ENG
IN
20:02
26-07-2025


Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
CreateSecurityGroup | EC2 | ap
Download history
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#CreateSecurityGroup:
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
EC2 > Security Groups > Create security group
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.
Basic details
Security group name Info
security
Name cannot be edited after creation.
Description Info
Allows SSH access to developers
VPC Info
vpc-00dcef4d69d6b4f5d
Inbound rules Info
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
SSH
TCP
22
Anyw...
0.0.0.0/0
Delete
HTTP
TCP
80
Anyw...
0.0.0.0/0
Delete
Add rule
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Men's Singles
Starting soon
Search
ENG
IN
20:15
26-07-2025


Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
Launch an instance | EC2 | ap-s
Download history
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
EC2 > Instances > Launch an instance
Network settings Info
VPC - required Info
vpc-0b3dc81074b480e0f (vpc1)
10.0.0.0/16
Subnet Info
subnet-0299962170cfb6d8d subnet1
VPC: vpc-0b3dc81074b480e0f Owner: 845958739988 Availability Zone: ap-south-1b
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.0.0/24)
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-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 ._-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard-2 created 2025-07-26T14:46:14.091Z
Inbound Security Group Rules
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6...read more
ami-0f918f7e67a3323f0
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Watchlist
Ideas
Search
ENG
IN
20:19
26-07-2025


Meet - okf-mcpd-uny
VPC configuration practice
VPC | ap-south-1
Instances | EC2 | ap-south-1
Download history
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 (1/2) 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
Initializing
View alarms
ap-south-1b
i-02b8ce0b59200b343 (linux)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance details Info
AMI ID
ami-0f918f7e67a3323f0
AMI name
ubuntu/images/hvm-ssd-gp3/ubuntu-noble-24.04-amd
Monitoring
disabled
Allowed image
-
Platform details
Linux/UNIX
Termination protection
Disabled
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Very humid
Now
Search
ENG
IN
20:21
26-07-2025


ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh/home?region=ap-south-1&connType=standard&instanceId=i-02b8ce0b59200b343&osUser=ubuntu&sshPort=22&...
Search
[Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Sat Jul 26 15:27:35 UTC 2025
System load: 0.0
Usage of /: 25.7% of 6.71GB
Memory usage: 20%
Swap usage: 0%
Processes: 106
Users logged in: 1
IPv4 address for enX0: 10.0.0.210
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Sat Jul 26 14:56:18 2025 from 13.233.177.4
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-10-0-0-210:~$
i-02b8ce0b59200b343 (linux)
PublicIPs: 13.233.155.114 PrivateIPs: 10.0.0.210
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
75°F
Light rain
Search
ENG
IN
20:57
26-07-2025



Task 2: Internet Gateway & Routing

Steps:

1. Create and attach an IGW to your custom VPC.
2. Create a public route table:
    - Add route: `0.0.0.0/0` → Internet Gateway
    - Associate this table with both public subnets.
3. Launch an EC2 instance in a public subnet:
    - Assign public IP
    - Use Amazon Linux 2 AMI or Ubuntu

- Security group: allow SSH (22) and ICMP (for ping)

Deliverables:

- Ping `8.8.8.8` from the EC2 terminal
- Screenshot of the route table showing `0.0.0.0/0` via IGW

Task 3: NACL vs Security Groups

Steps:

1. Create a new NACL and associate it with one public subnet.
2. NACL inbound rules:
   - Deny TCP port 22 from your home IP range (e.g., `123.45.67.89/32`)
   - Allow TCP port 80 from `0.0.0.0/0`
3. Security group:
   - Allow TCP port 22 only from your home IP
   - Allow TCP port 80 from `0.0.0.0/0`
4. Test using:
   - `telnet <instance-IP> 22` or `nc -zv <instance-IP> 22`
   - `telnet <instance-IP> 80`

Deliverable:

- Document observed connection results for both port 22 and 80

Task 4: Bastion Host Setup

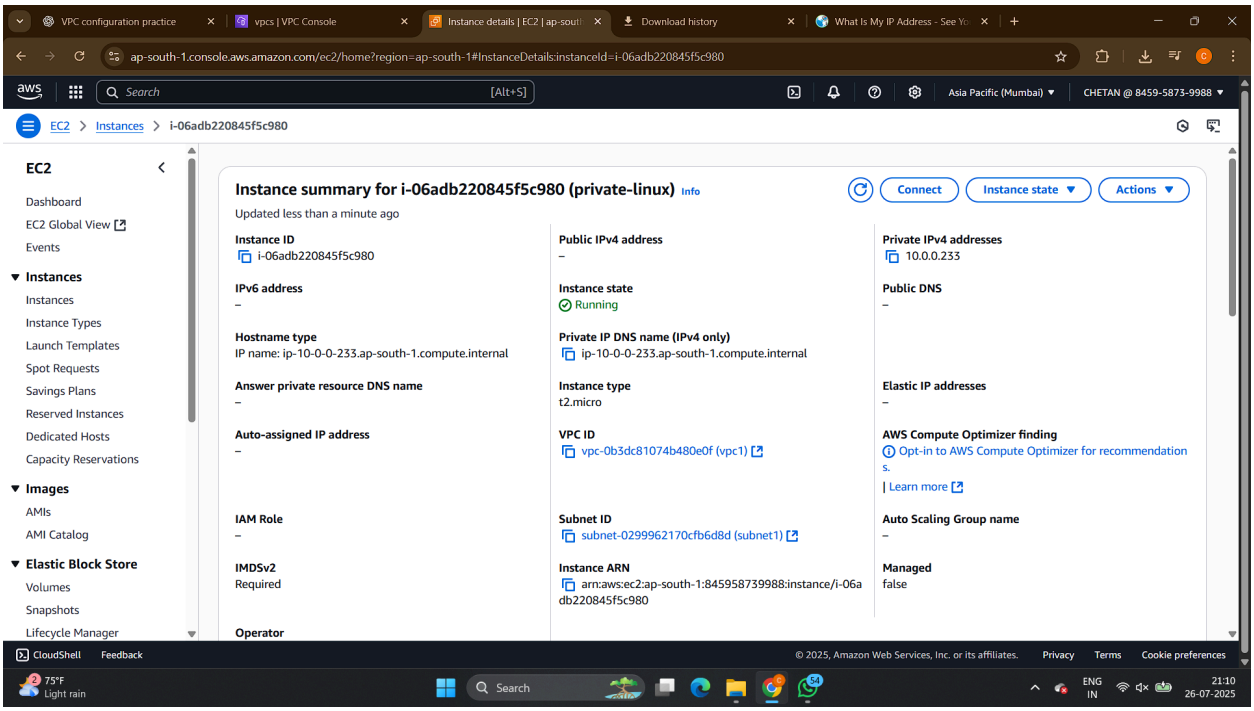
Steps:

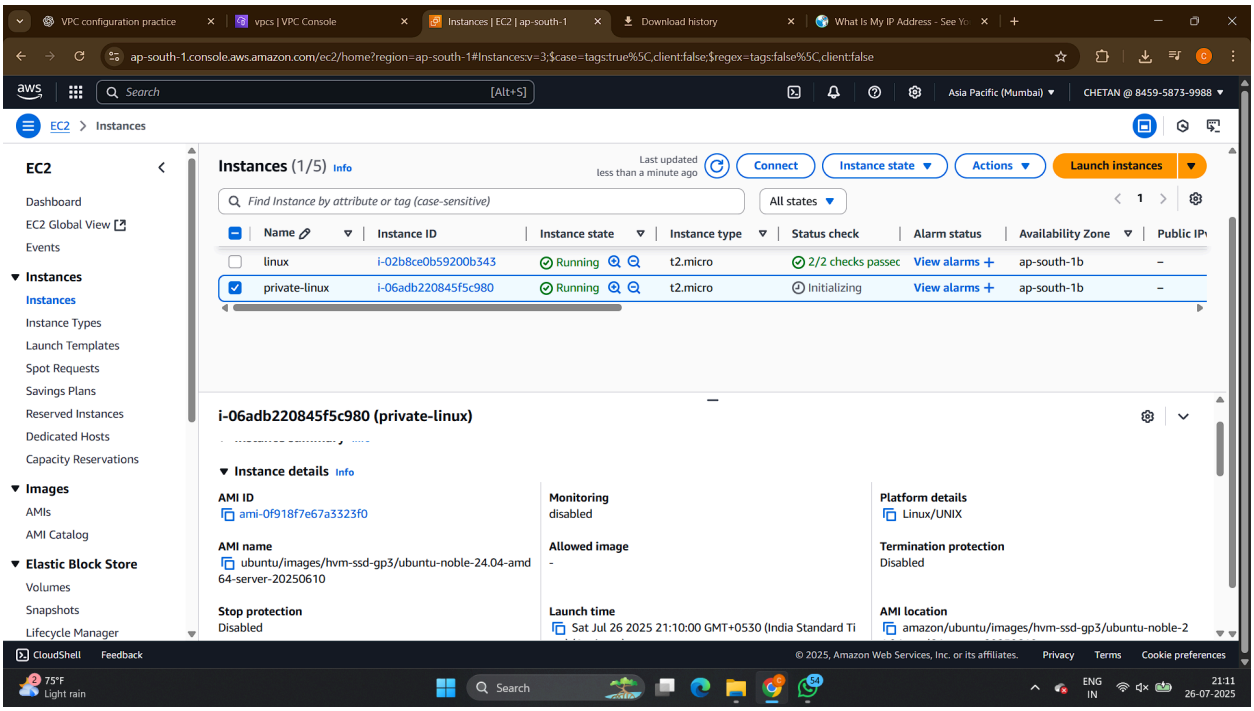
1. Launch a private EC2 instance in private subnet:
   - No public IP
   - Same key pair as the bastion
2. Launch a bastion EC2 in public subnet:

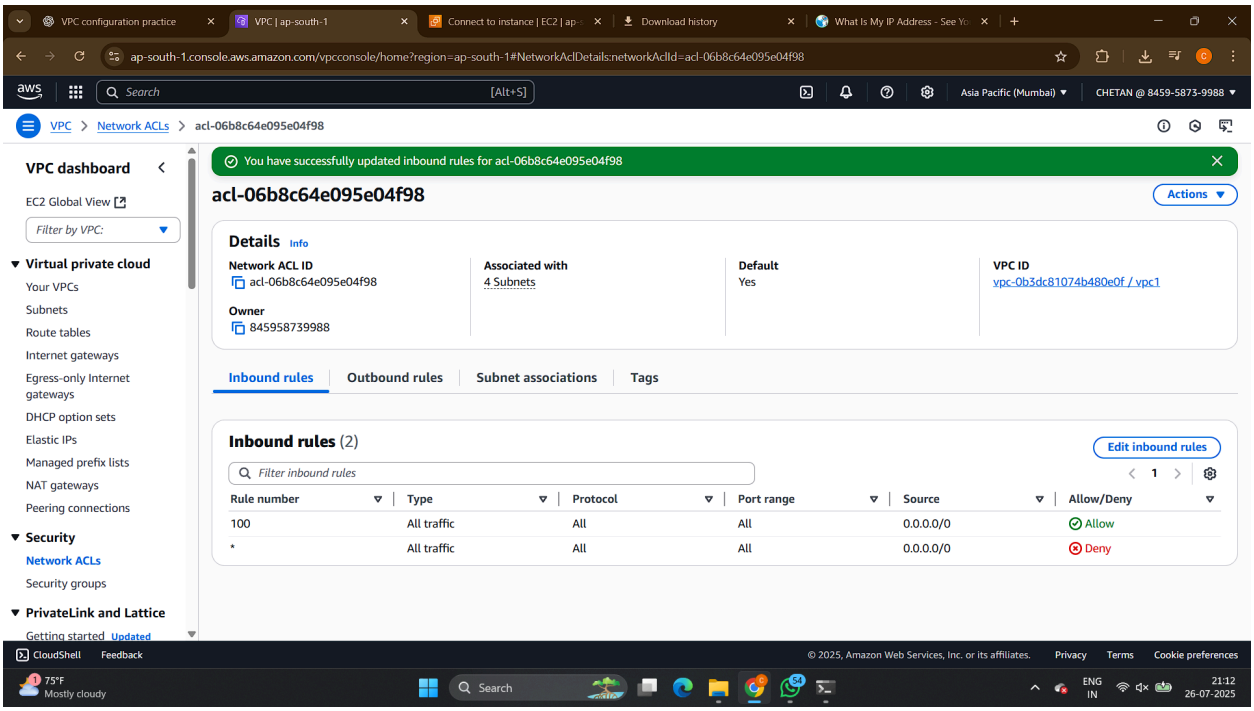
- Assign public IP
- Allow SSH (22) in security group

3. Enable SSH agent forwarding on your local machine:
   - `eval "$(ssh-agent)" && ssh-add your-key.pem`
   - Connect using:

```
kotlin
CopyEdit
ssh -A -J ec2-user@<bastion-IP> ec2-user@<private-IP>
```




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


VPC configuration practice
VPC | ap-south-1
Connect to instance | EC2 | ap-
Download history
What Is My IP Address - See Yo
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#NetworkAclDetails:networkAclId=acl-06b8c64e095e04f98
Search [Alt+S]
Asia Pacific (Mumbai)
CHETAN @ 8459-5873-9988
VPC > Network ACLs > acl-06b8c64e095e04f98
VPC dashboard
EC2 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
Security
Network ACLs
Security groups
PrivateLink and Lattice
Getting started Updated
You have successfully updated inbound rules for acl-06b8c64e095e04f98
acl-06b8c64e095e04f98
Actions
Details Info
Network ACL ID
acl-06b8c64e095e04f98
Associated with
4 Subnets
Default
Yes
VPC ID
vpc-0b3dc81074b480e0f / vpc1
Owner
845958739988
Inbound rules
Outbound rules
Subnet associations
Tags
Inbound rules (2)
Edit inbound rules
Filter inbound rules
Rule number
Type
Protocol
Port range
Source
Allow/Deny
100
All traffic
All
All
0.0.0.0/0
Allow
*
All traffic
All
All
0.0.0.0/0
Deny
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
75°F
Mostly cloudy
Search
ENG
IN
21:12
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.
```

```
See "man sudo_root" for details.

ubuntu@ip-10-0-0-233:~$
```

Deliverable:

- Screenshot showing successful SSH access into the private instance using the bastion

5. CIDR Calculation Exercise

What is Given:

- **Main network:** `192.168.0.0/16`
- This means we have IPs from `192.168.0.0` to `192.168.255.255` (a total of 65,536 IP addresses).

What is Required:

- 4 subnets for **dev**, each with **64 hosts**
- 2 subnets for **prod**, each with **128 hosts**

How to Choose Subnet Size:

- For 64 hosts → We need **64 IPs** → This fits in a **/26** subnet (62 usable IPs, 2 reserved)
- For 128 hosts → We need **128 IPs** → This fits in a **/25** subnet (126 usable IPs, 2 reserved)

Dev Subnets (/26 = 64 IPs)

Subnet Name	CIDR	IP Range
dev-subnet1	192.168.0.0/26	192.168.0.0 – 192.168.0.63
dev-subnet2	192.168.0.64/26	192.168.0.64 – 192.168.0.127
dev-subnet3	192.168.0.128/26	192.168.0.128 – 192.168.0.191
dev-subnet4	192.168.0.192/26	192.168.0.192 – 192.168.0.255

Prod Subnets (/25 = 128 IPs)

Subnet Name	CIDR	IP Range
prod-subnet1	192.168.1.0/25	192.168.1.0 – 192.168.1.127
prod-subnet2	192.168.1.128/25	192.168.1.128 – 192.168.1.255

Final Table:

Name	CIDR	Usable IP Range	Total IPs	Usable IPs
dev-subnet1	192.168.0.0/26	192.168.0.1 – 192.168.0.62	64	62
dev-subnet2	192.168.0.64/26	192.168.0.65 – 192.168.0.126	64	62
dev-subnet3	192.168.0.128/26	192.168.0.129 – 192.168.0.190	64	62
dev-subnet4	192.168.0.192/26	192.168.0.193 – 192.168.0.254	64	62
prod-subnet1	192.168.1.0/25	192.168.1.1 – 192.168.1.126	128	126
prod-subnet2	192.168.1.128/25	192.168.1.129 – 192.168.1.254	128	126