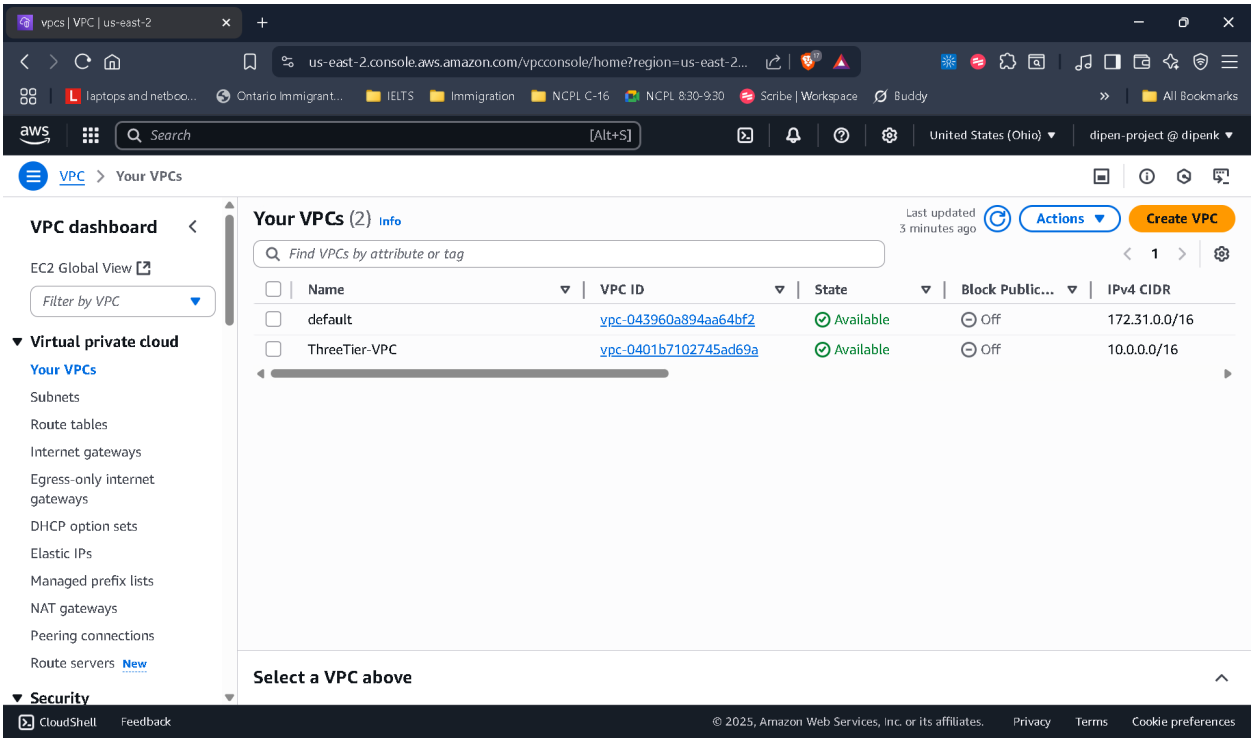
# Step by step guide

## Phase 1

## 1. Create a VPC

Go to: **VPC Dashboard → Your VPCs → Create VPC**

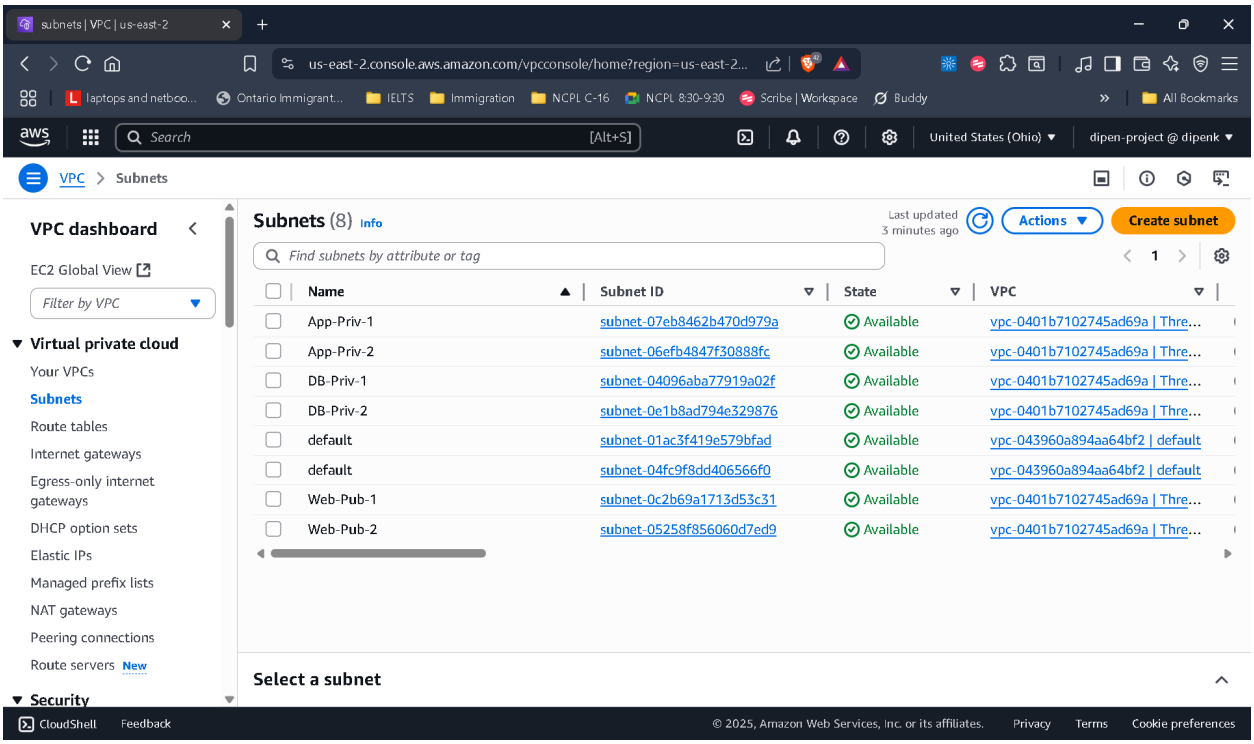
| Field | Value |
|---|---|
| **Name tag** | ThreeTier-VPC |
| **IPv4 CIDR block** | 10.0.0.0/16 |
| **Tenancy** | Default |
| IPv6 CIDR block | No IPv6 for now |
| **Enable DNS Hostnames** | Yes (important for public DNS resolution) |



## 2. Create Subnets

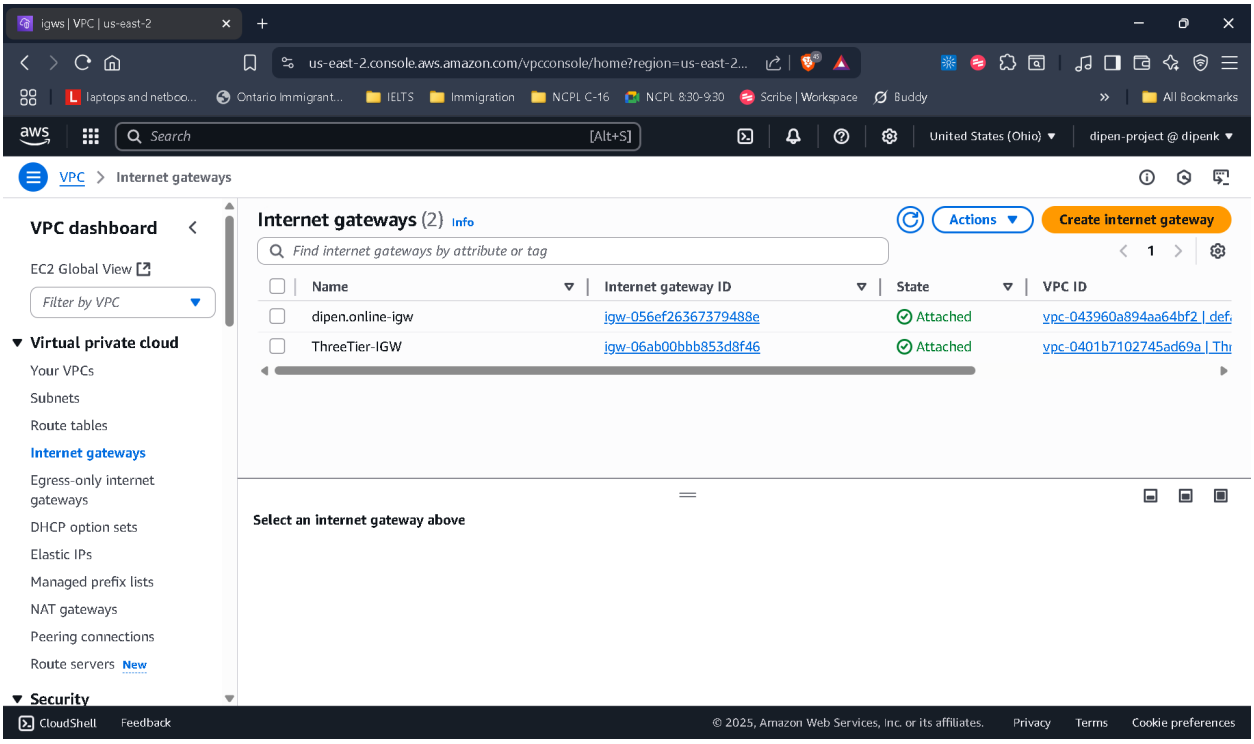
1. Go to **VPC Dashboard → Subnets → Create subnet**
2. Select your VPC: ThreeTier-VPC
3. Create **one at a time**:
    - **Name Tag**: Use names from table above (e.g., Web-Pub-1)
    - **Availability Zone**: Choose us-east-1a, us-east-1b, etc.
    - **IPv4 CIDR**: e.g., 10.0.1.0/24

| Tier | AZ | Subnet Name | CIDR Block | Type |
|---|---|---|---|---|
| Web Tier | AZ1 | Web-Pub-1 | 10.0.1.0/24 | Public |
| Web Tier | AZ2 | Web-Pub-2 | 10.0.2.0/24 | Public |
| App Tier | AZ1 | App-Priv-1 | 10.0.3.0/24 | Private |
| App Tier | AZ2 | App-Priv-2 | 10.0.4.0/24 | Private |
| DB Tier | AZ1 | DB-Priv-1 | 10.0.5.0/24 | Private |
| DB Tier | AZ2 | DB-Priv-2 | 10.0.6.0/24 | Private |



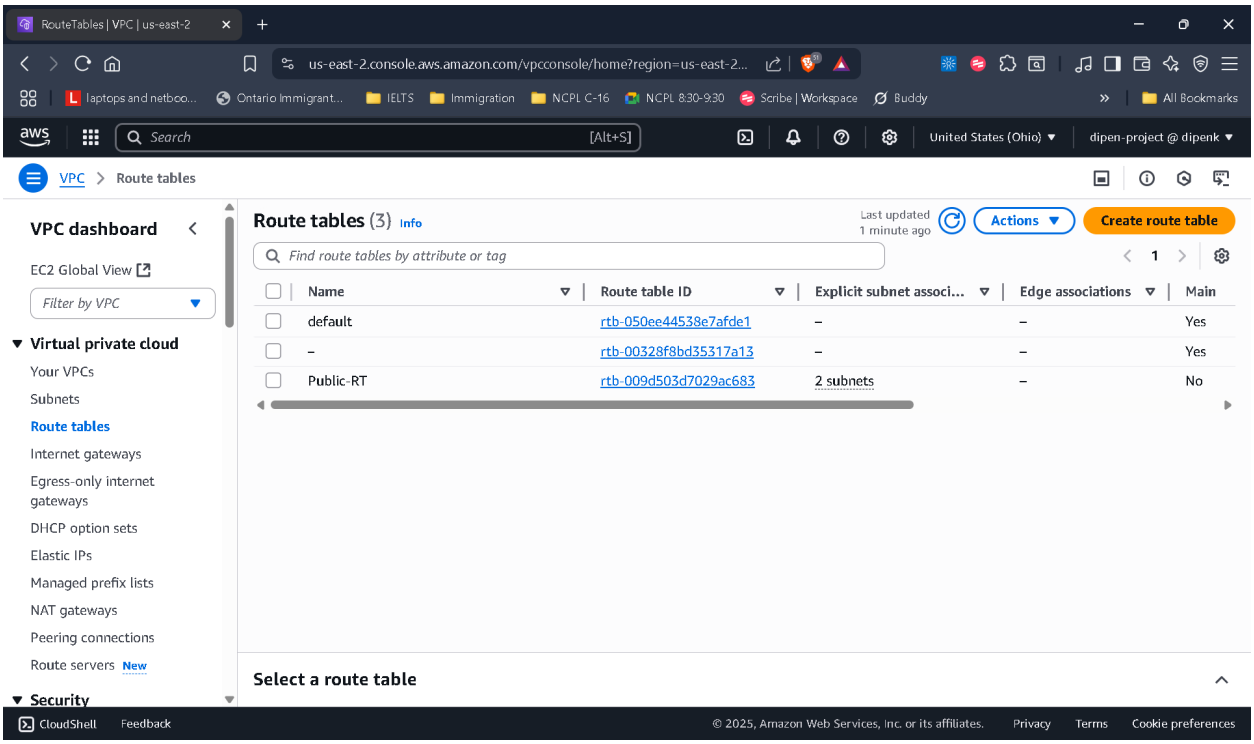
## 3. Create and Attach IGW

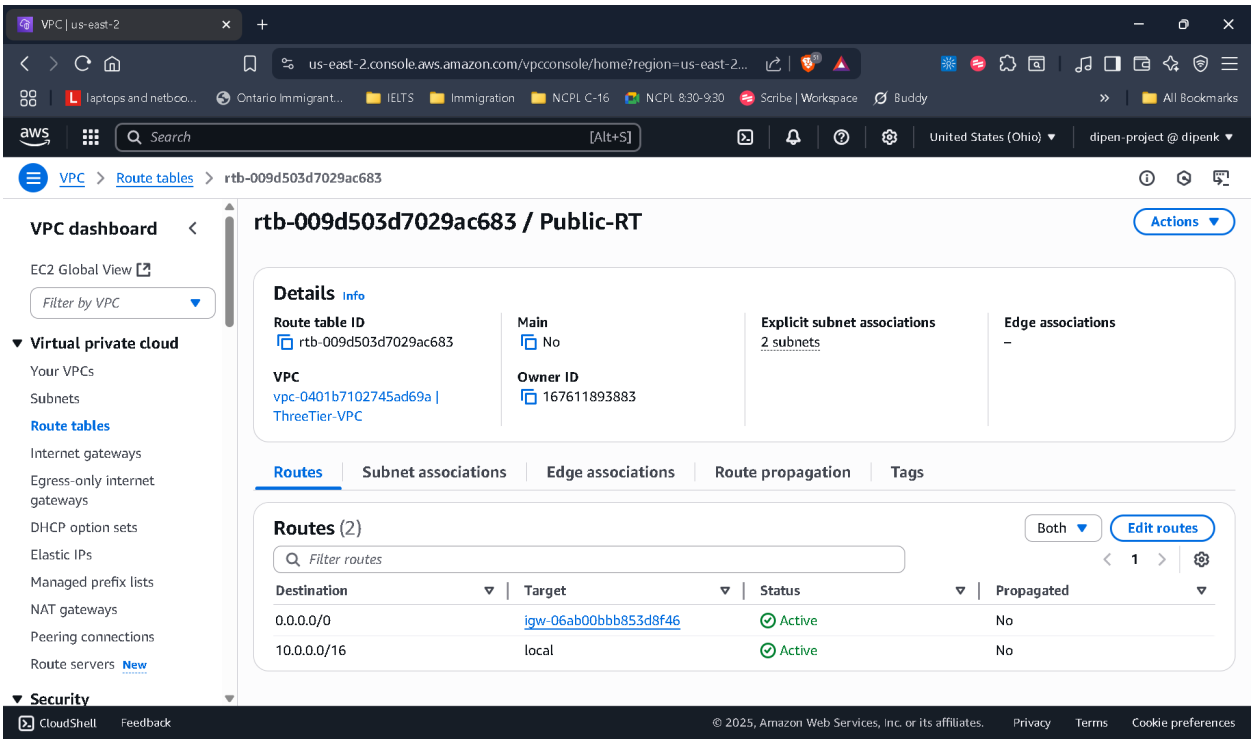
1. Go to **VPC Dashboard → Internet Gateways → Create Internet Gateway**
2. **Name**: ThreeTier-IGW
3. Click **Create Internet Gateway**
4. After creation, **select it → Actions → Attach to VPC**
5. Choose your VPC: ThreeTier-VPC

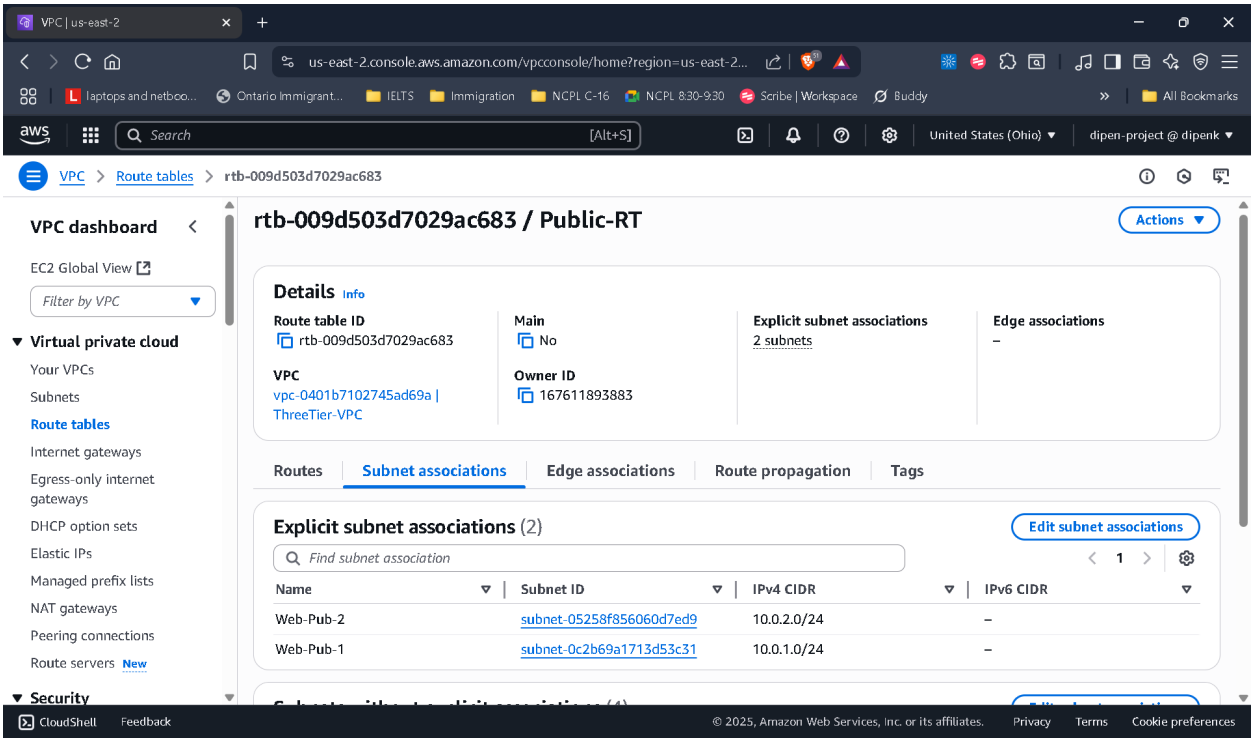


## 4. Public Route Table

1. **VPC Dashboard → Route Tables → Create Route Table**
2. **Name**: Public-RT
3. **VPC**: Select ThreeTier-VPC
4. Click **Create**
5. Select Public-RT → **Routes tab → Edit routes**
6. Click **Add route**:
    - **Destination**: 0.0.0.0/0
    - **Target**: Choose the Internet Gateway (ThreeTier-IGW)
7. Click **Save changes**
8. Now go to **Subnet Associations → Edit subnet associations**
    - Select: Web-Pub-1 and Web-Pub-2
    - Click **Save**

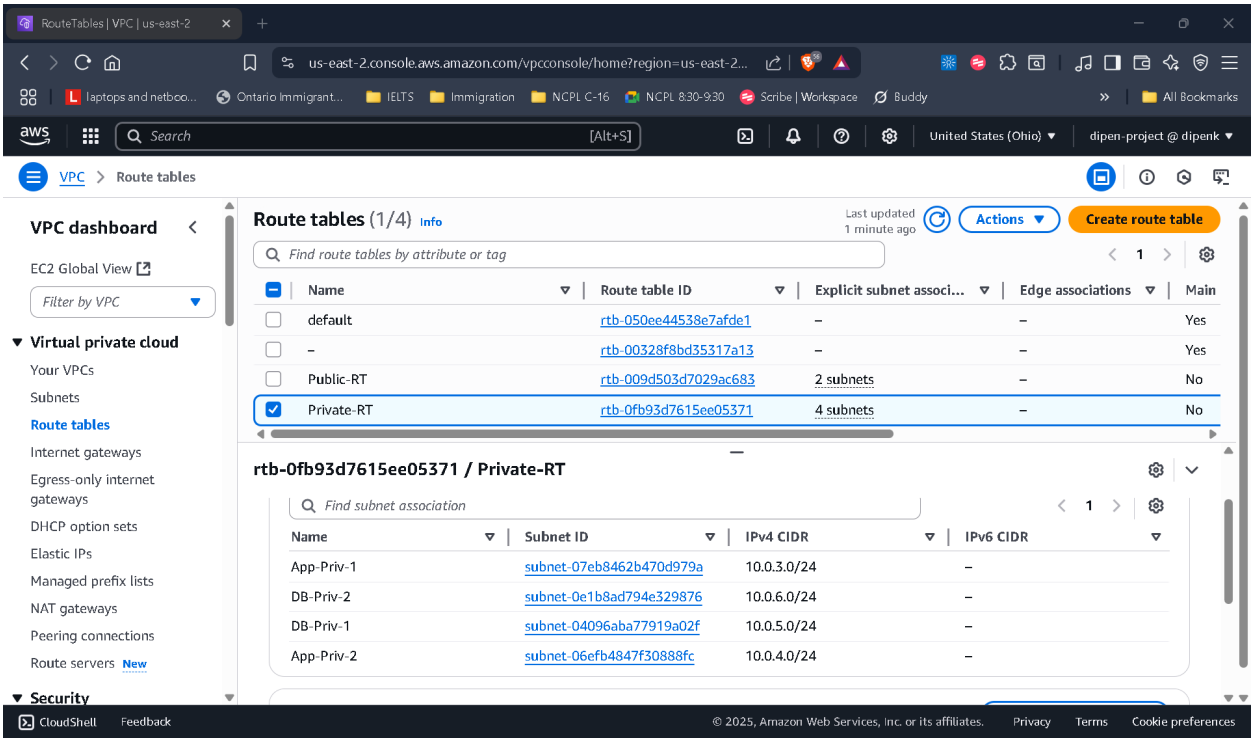



VPC | us-east-2
us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2...
Search [Alt+S]
United States (Ohio)
dipen-project @ dipenk
VPC > Route tables > rtb-009d503d7029ac683
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New
Security
rtb-009d503d7029ac683 / Public-RT
Actions
Details Info
Route table ID
rtb-009d503d7029ac683
Main
No
Explicit subnet associations
2 subnets
Edge associations
–
VPC
vpc-0401b7102745ad69a | ThreeTier-VPC
Owner ID
167611893883
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
0.0.0.0/0
igw-06ab00bbb853d8f46
Active
No
10.0.0.0/16
local
Active
No
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


VPC | us-east-2
us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2...
Search [Alt+S]
United States (Ohio)
dipen-project @ dipenk
VPC > Route tables > rtb-009d503d7029ac683
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
Route servers New
Security
rtb-009d503d7029ac683 / Public-RT
Actions
Details Info
Route table ID
rtb-009d503d7029ac683
Main
No
Explicit subnet associations
2 subnets
Edge associations
–
VPC
vpc-0401b7102745ad69a | ThreeTier-VPC
Owner ID
167611893883
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (2)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Web-Pub-2
subnet-05258f856060d7ed9
10.0.2.0/24
–
Web-Pub-1
subnet-0c2b69a1713d53c31
10.0.1.0/24
–
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

## 5. Private Route Table

1. Back in **Route Tables → Create Route Table**
2. **Name**: Private-RT
3. **VPC**: Select ThreeTier-VPC
4. Click **Create**
5. **No need to add route to IGW**
6. Go to **Subnet Associations → Edit subnet associations**
    - Select: App-Priv-1, App-Priv-2, DB-Priv-1, DB-Priv-2
    - Click **Save**



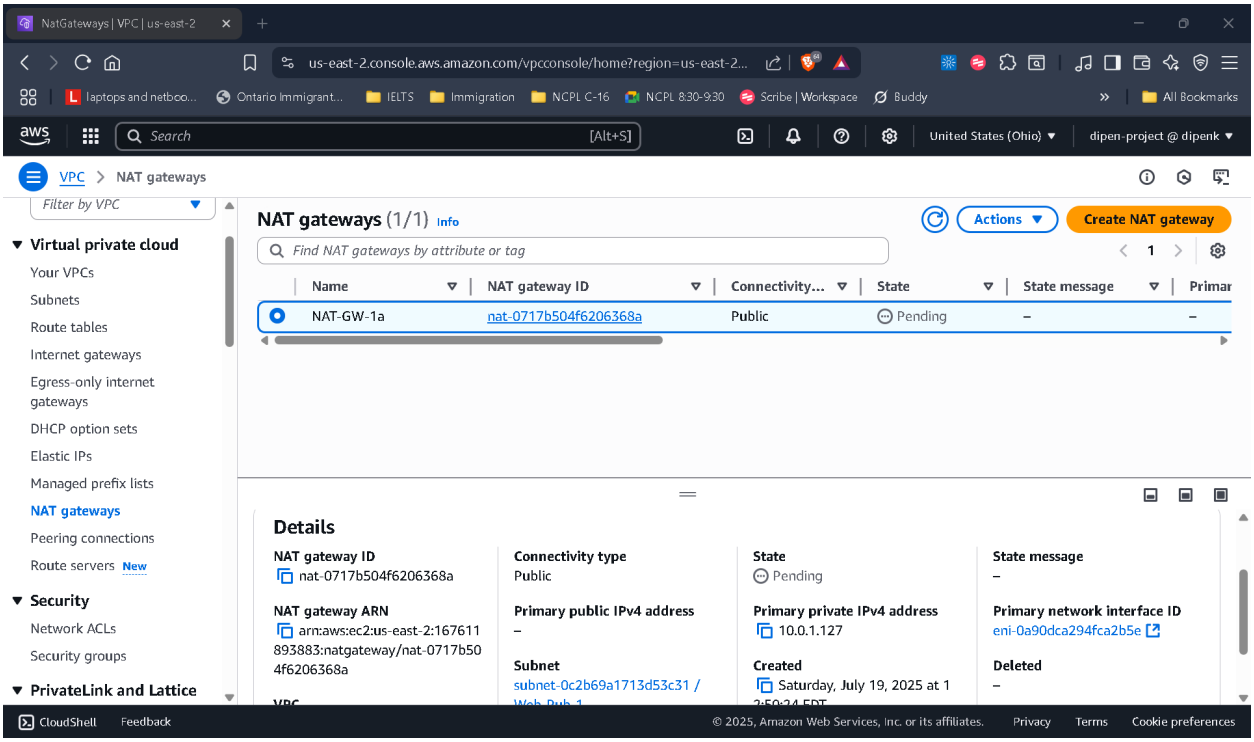

**[ Web-Pub-1, Web-Pub-2 ] --> Public-RT --> IGW --> Internet**

**[ App-Priv-1..DB-Priv-2 ] --> Private-RT --> (internal only)**

## Create a NAT Gateway

1. Go to **VPC Dashboard → NAT Gateways → Create NAT Gateway**
2. **Name**: NAT-GW-AZ1
3. **Subnet**: Select Web-Pub-1 (public subnet)
4. **Elastic IP**: Click “Allocate Elastic IP” → choose it
5. Click **Create NAT Gateway**

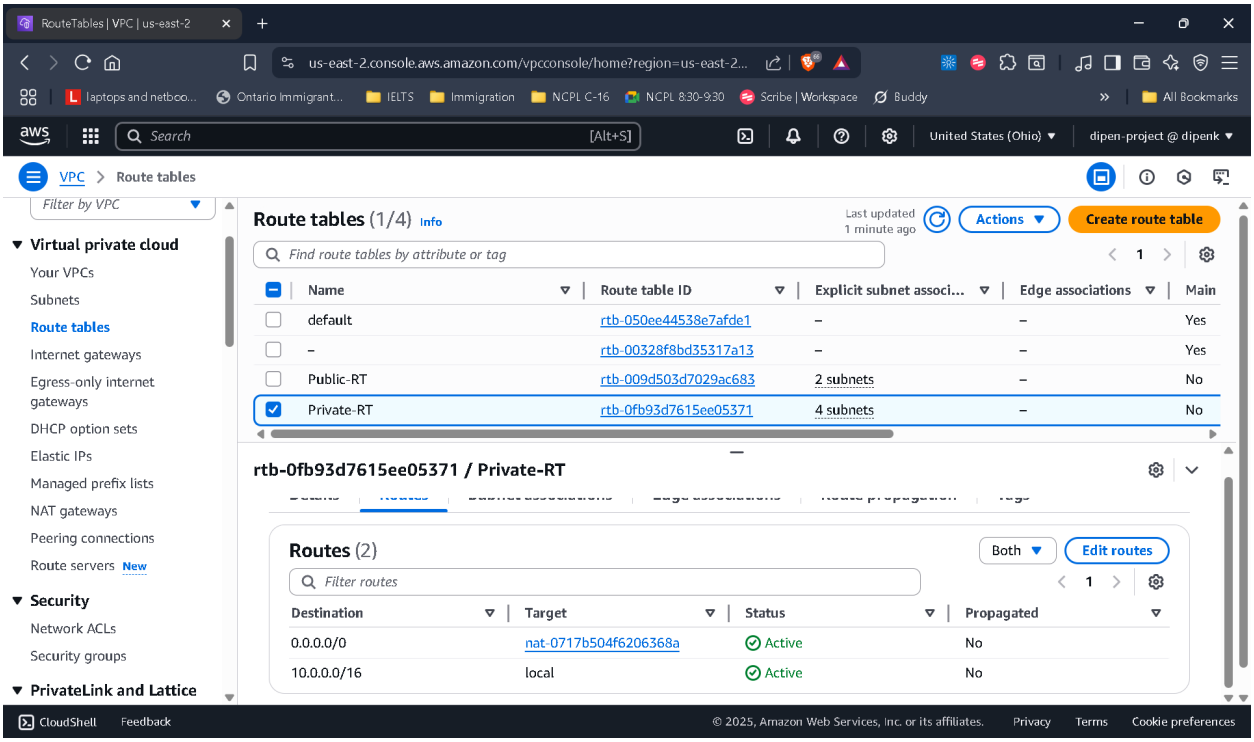
Wait for status to show as Available.



## Update Private Route Table to Use NAT

1. Go to **Route Tables → Select Private-RT**
2. Click **Routes tab → Edit routes**
3. **Add route**:
    - **Destination**: 0.0.0.0/0
    - **Target**: Your newly created **NAT Gateway**

Click **Save Changes**



# Phase 2

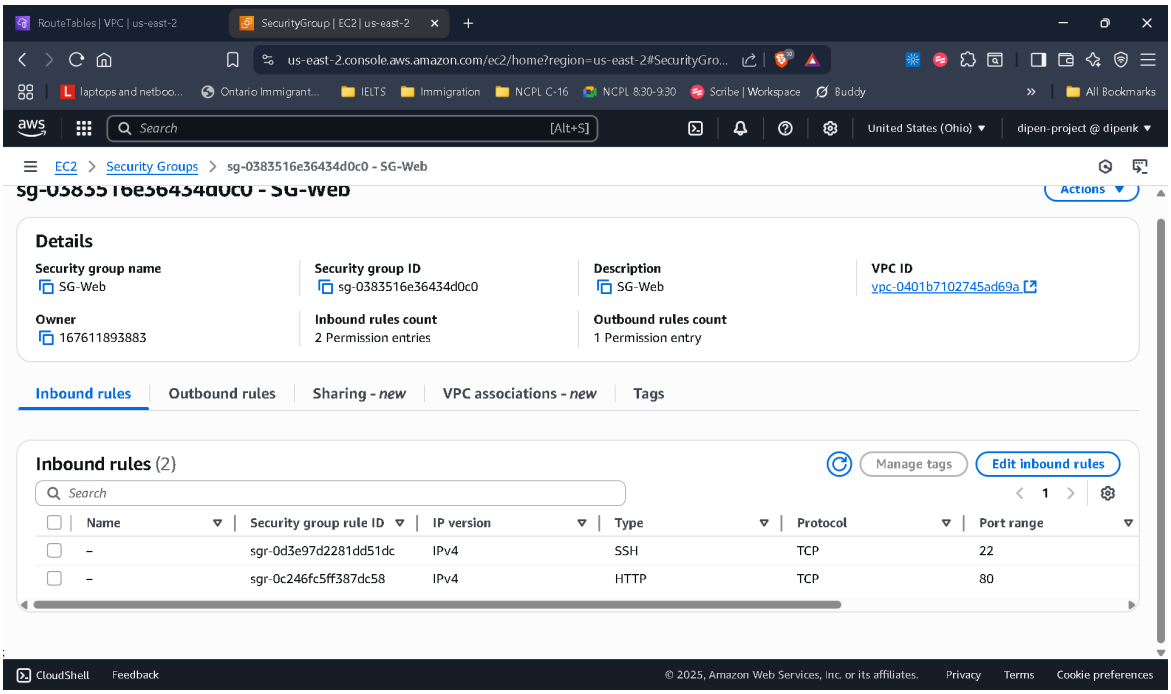
## SG Design for 3-Tier Architecture

| SG Name | Attached To | Inbound Rules From | Outbound |
|---|---|---|---|
| `SG-Web` | Web EC2 / ALB | 0.0.0.0/0: HTTP (80), SSH (22) | All traffic |
| `SG-App` | App EC2 | `SG-Web`: TCP 3000 (custom app port) | All traffic |
| `SG-DB` | RDS DB | `SG-App`: TCP 3306 (MySQL/Aurora) | All traffic |

## Create Security Groups

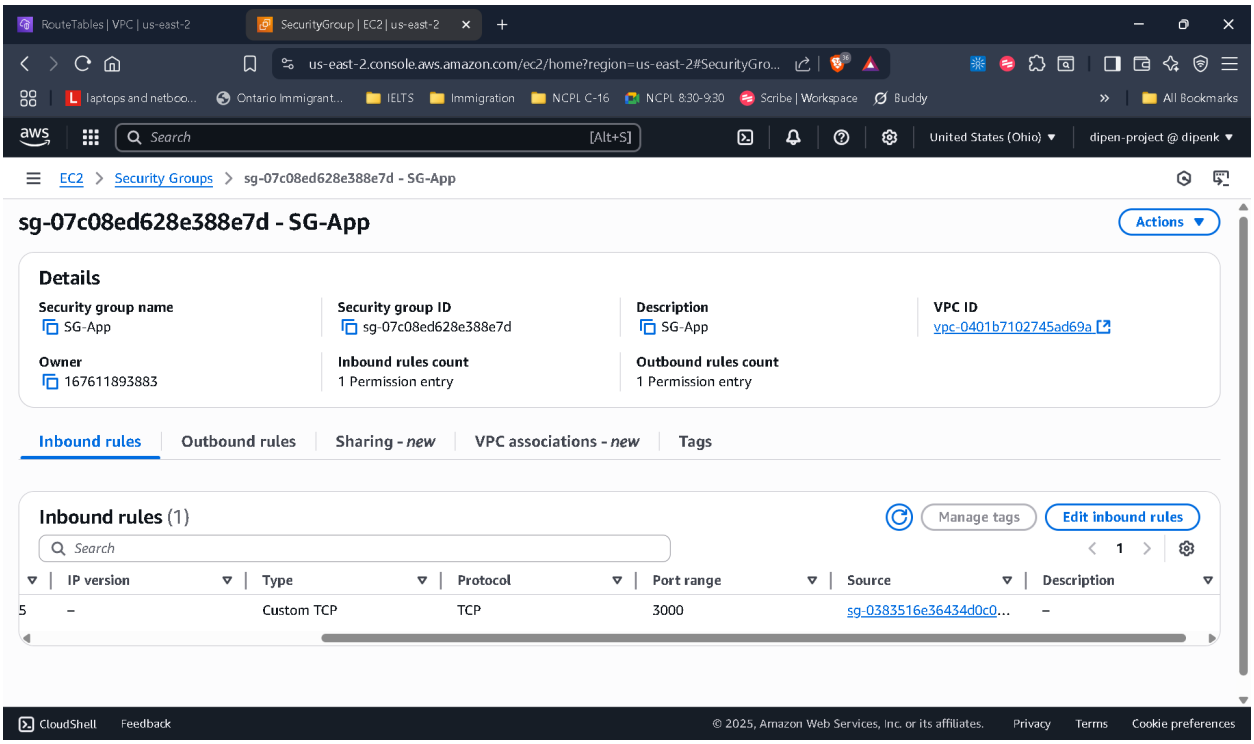
### SG-Web (Web Tier)

1. Go to **EC2 → Security Groups → Create Security Group**
2. **Name**: SG-Web
3. **VPC**: ThreeTier-VPC
4. **Inbound Rules**:
    - Type: HTTP | Port: 80 | Source: 0.0.0.0/0
    - Type: SSH | Port: 22 | Source: your IP (My IP) *(or restrict it later)*
5. **Outbound**: Allow all (default)



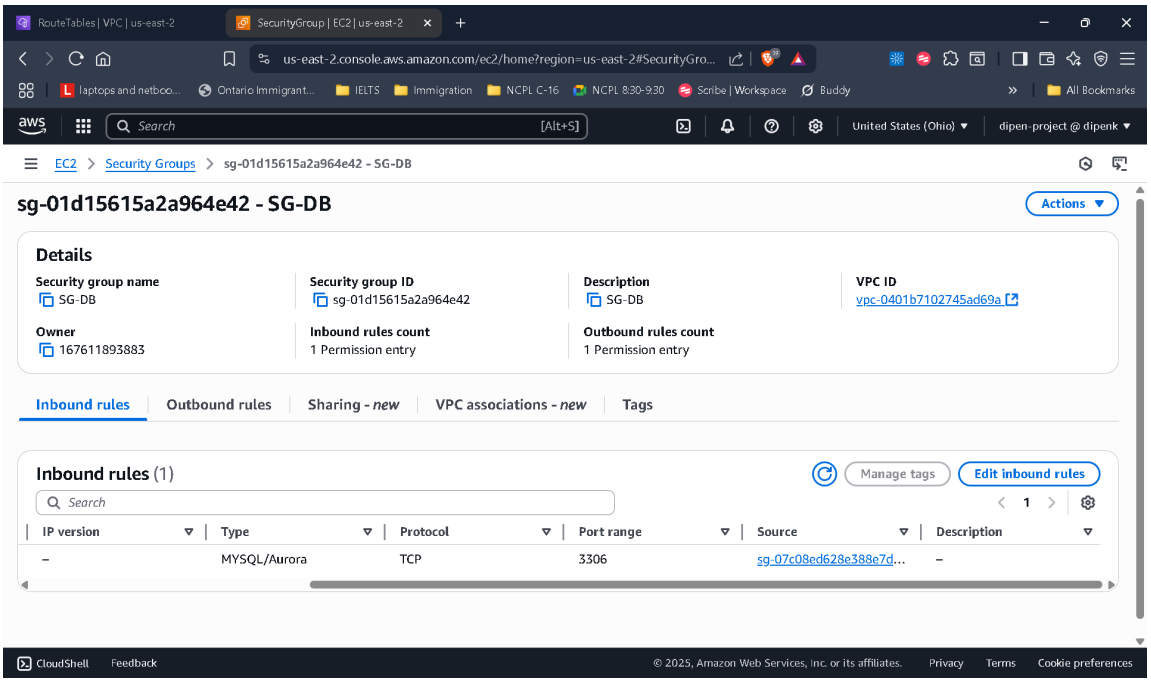
## SG-App (App Tier)

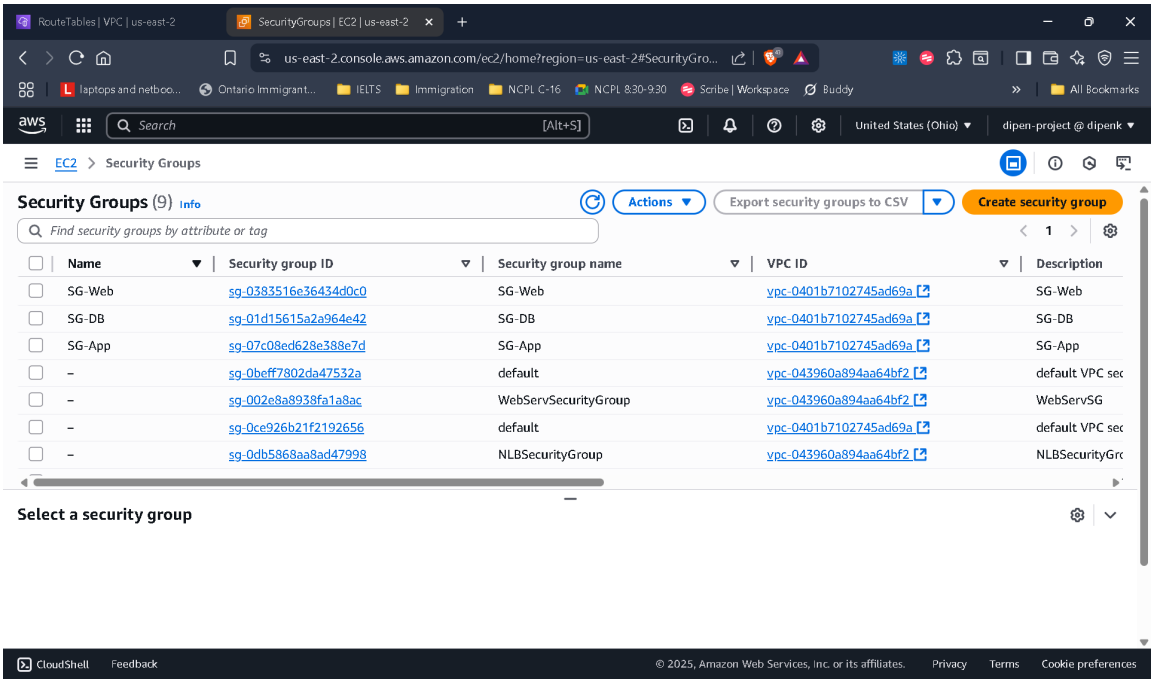
1. **Name**: SG-App
2. Inbound Rules:
    - Type: Custom TCP | Port: 3000 *(or your backend port)* | Source: SG-Web
3. Outbound: Allow all



## SG-DB (Database Tier)

1. **Name**: SG-DB
2. Inbound Rules:
    - Type: MySQL/Aurora | Port: 3306 | Source: SG-App
3. Outbound: Allow all



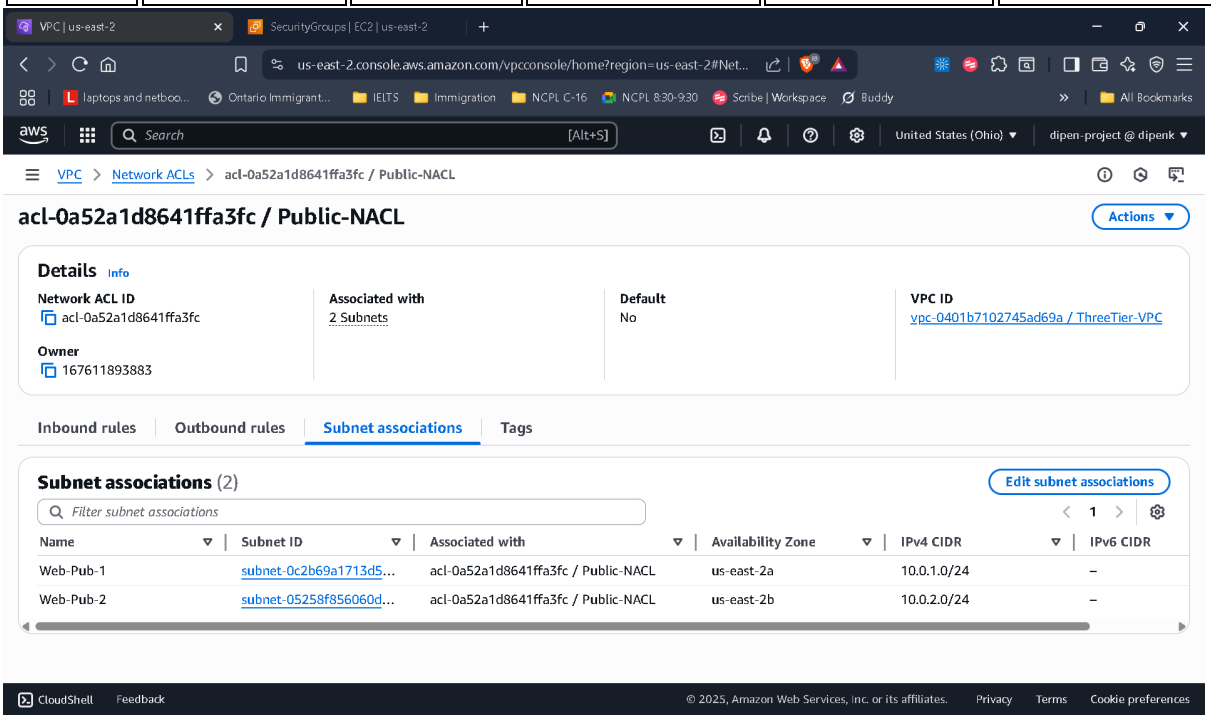



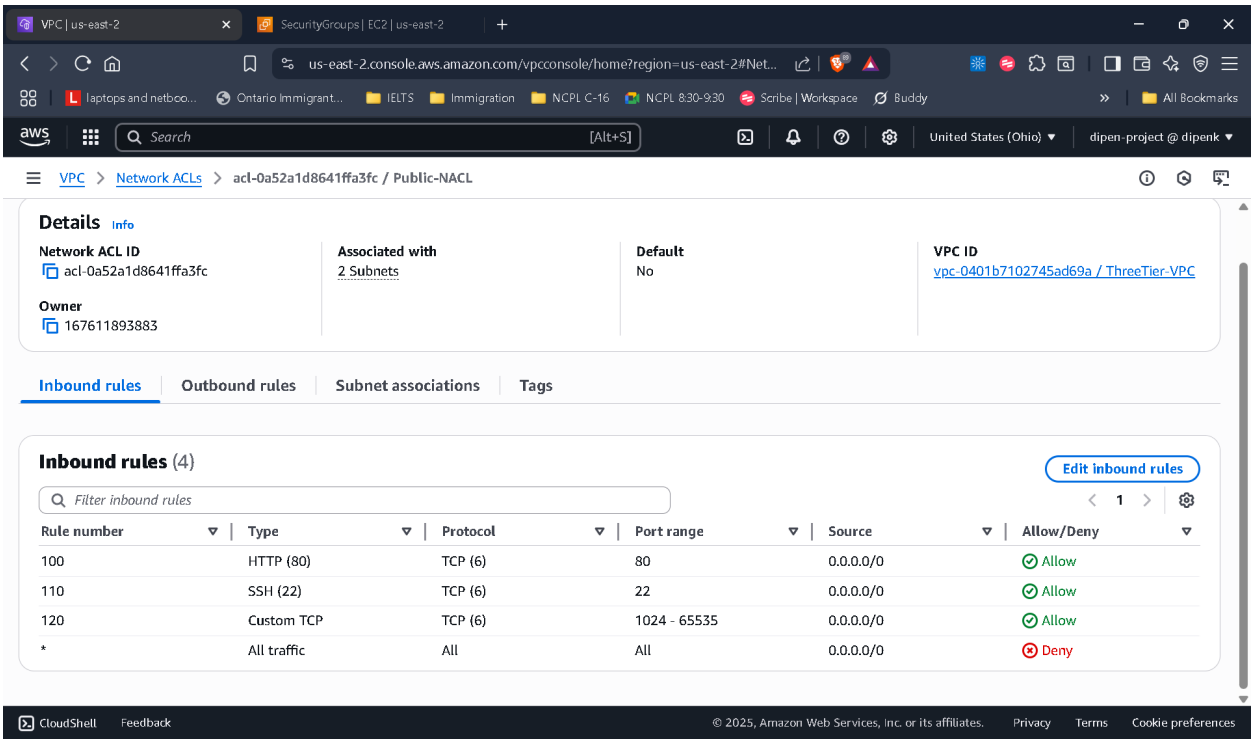
## Public NACL

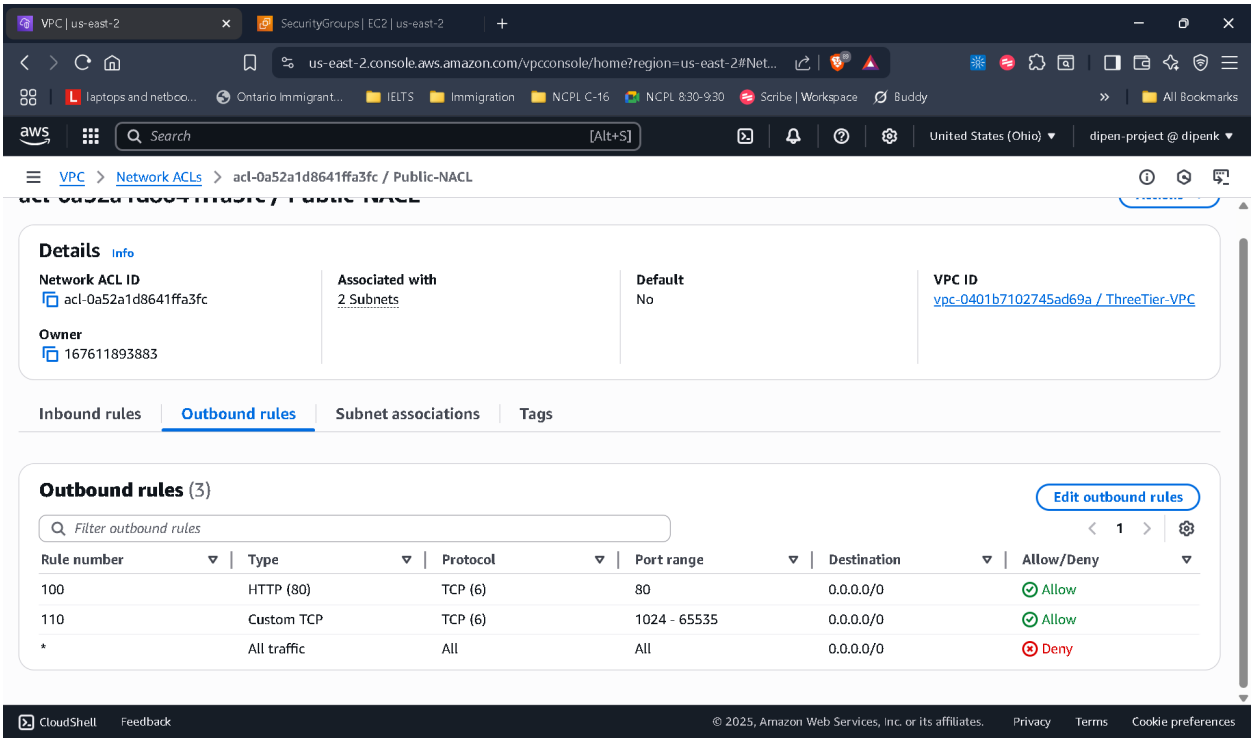
1. Go to **VPC Dashboard → Network ACLs → Create NACL**
2. **Name**: Public-NACL
3. **VPC**: ThreeTier-VPC
4. Click **Create**
5. Click on the new NACL → **Subnet Associations**
    - Associate: Web-Pub-1, Web-Pub-2

| Rule # | Type | Protocol | Port Range | Source | Allow/Deny |
|---|---|---|---|---|---|
| 100 | HTTP | TCP | 80 | 0.0.0.0/0 | ALLOW |
| 110 | SSH | TCP | 22 | your IP CIDR | ALLOW |
| 120 | Ephemeral | TCP | 1024–65535 | 0.0.0.0/0 | ALLOW |
| * | ALL | ALL | ALL | 0.0.0.0/0 | DENY |

| Rule # | Type | Protocol | Port Range | Destination | Allow/Deny |
|---|---|---|---|---|---|
| 100 | HTTP | TCP | 80 | 0.0.0.0/0 | ALLOW |
| 110 | Ephemeral | TCP | 1024–65535 | 0.0.0.0/0 | ALLOW |
| * | ALL | ALL | ALL | 0.0.0.0/0 | DENY |




VPC | us-east-2
SecurityGroups | EC2 | us-east-2
us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#Net...
Search [Alt+S]
United States (Ohio)
dipen-project @ dipenk
VPC > Network ACLs > acl-0a52a1d8641ffa3fc / Public-NACL
Details Info
Network ACL ID
acl-0a52a1d8641ffa3fc
Associated with
2 Subnets
Default
No
VPC ID
vpc-0401b7102745ad69a / ThreeTier-VPC
Owner
167611893883
Inbound rules
Outbound rules
Subnet associations
Tags
Inbound rules (4)
Edit inbound rules
Filter inbound rules
Rule number | Type | Protocol | Port range | Source | Allow/Deny
100 | HTTP (80) | TCP (6) | 80 | 0.0.0.0/0 | Allow
110 | SSH (22) | TCP (6) | 22 | 0.0.0.0/0 | Allow
120 | Custom TCP | TCP (6) | 1024 - 65535 | 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


VPC | us-east-2
SecurityGroups | EC2 | us-east-2
us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#Net...
Search [Alt+S]
United States (Ohio)
dipen-project @ dipenk
VPC > Network ACLs > acl-0a52a1d8641ffa3fc / Public-NACL
Details Info
Network ACL ID
acl-0a52a1d8641ffa3fc
Associated with
2 Subnets
Default
No
VPC ID
vpc-0401b7102745ad69a / ThreeTier-VPC
Owner
167611893883
Inbound rules
Outbound rules
Subnet associations
Tags
Outbound rules (3)
Edit outbound rules
Filter outbound rules
Rule number | Type | Protocol | Port range | Destination | Allow/Deny
100 | HTTP (80) | TCP (6) | 80 | 0.0.0.0/0 | Allow
110 | Custom TCP | TCP (6) | 1024 - 65535 | 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

## Private NACL

Repeat above process for Private-NACL and associate:

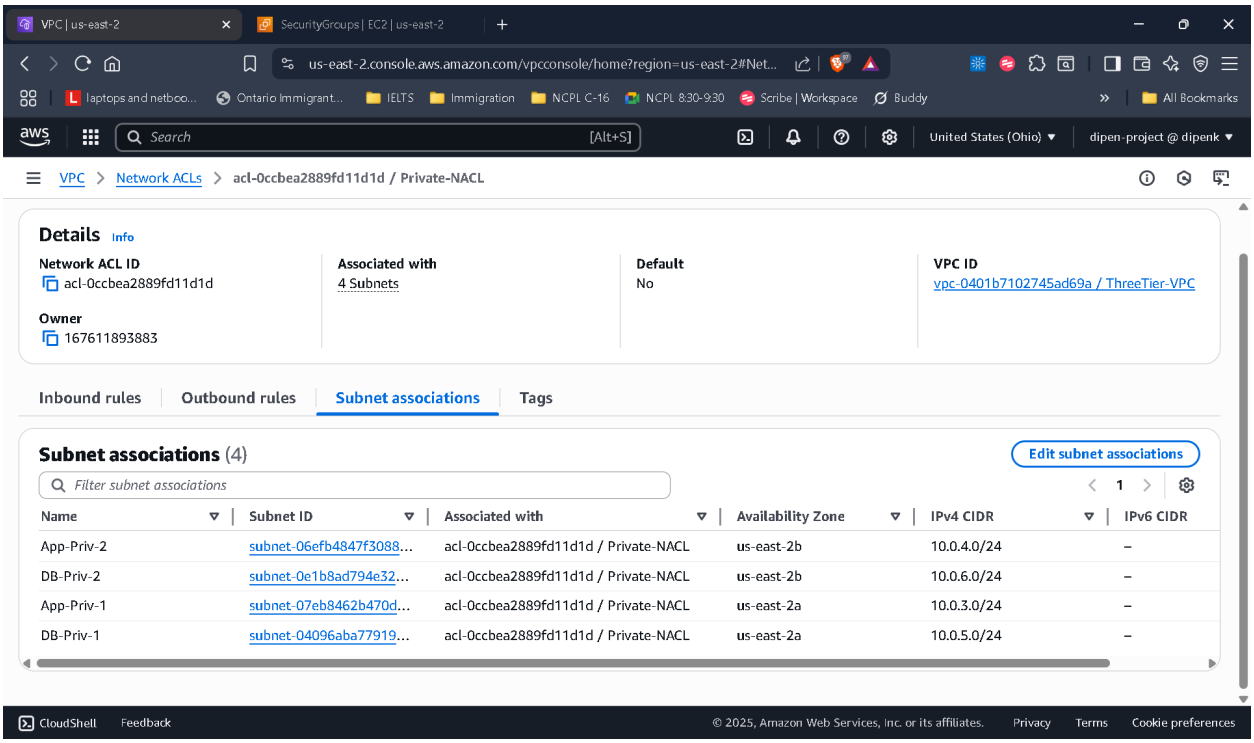
- App-Priv-1
- App-Priv-2
- DB-Priv-1
- DB-Priv-2

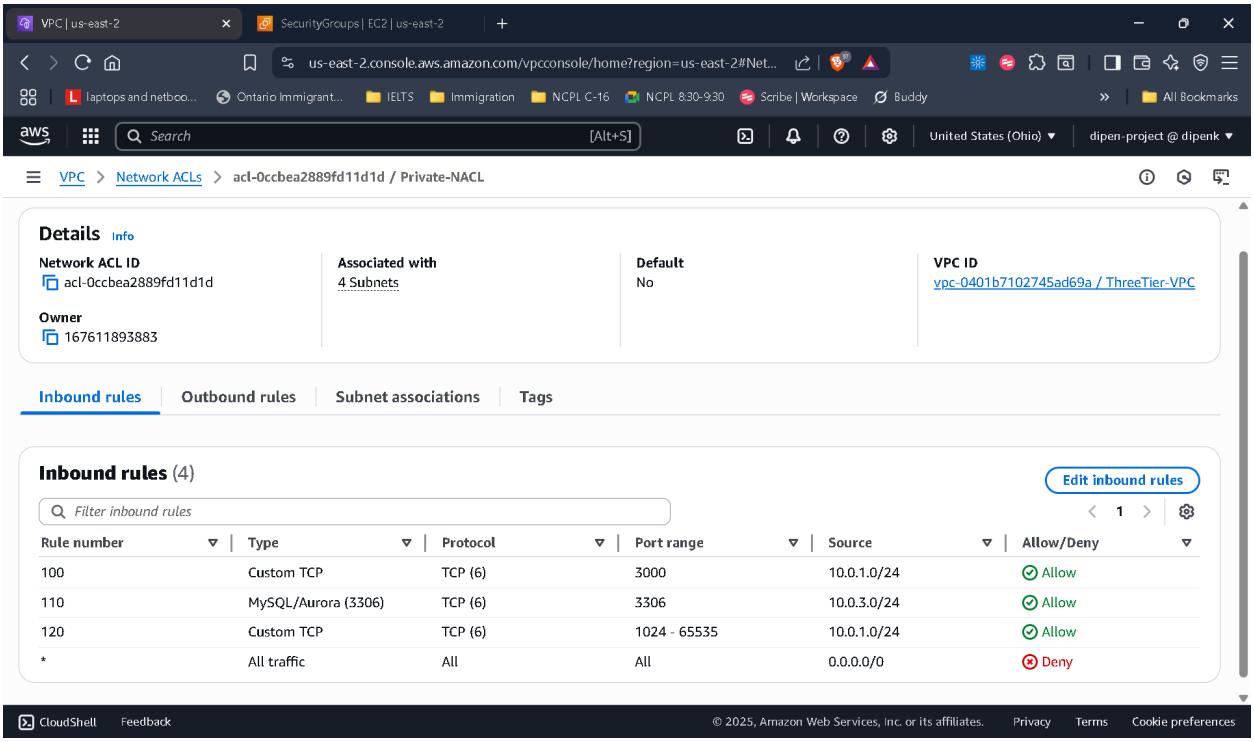
Inbound rules

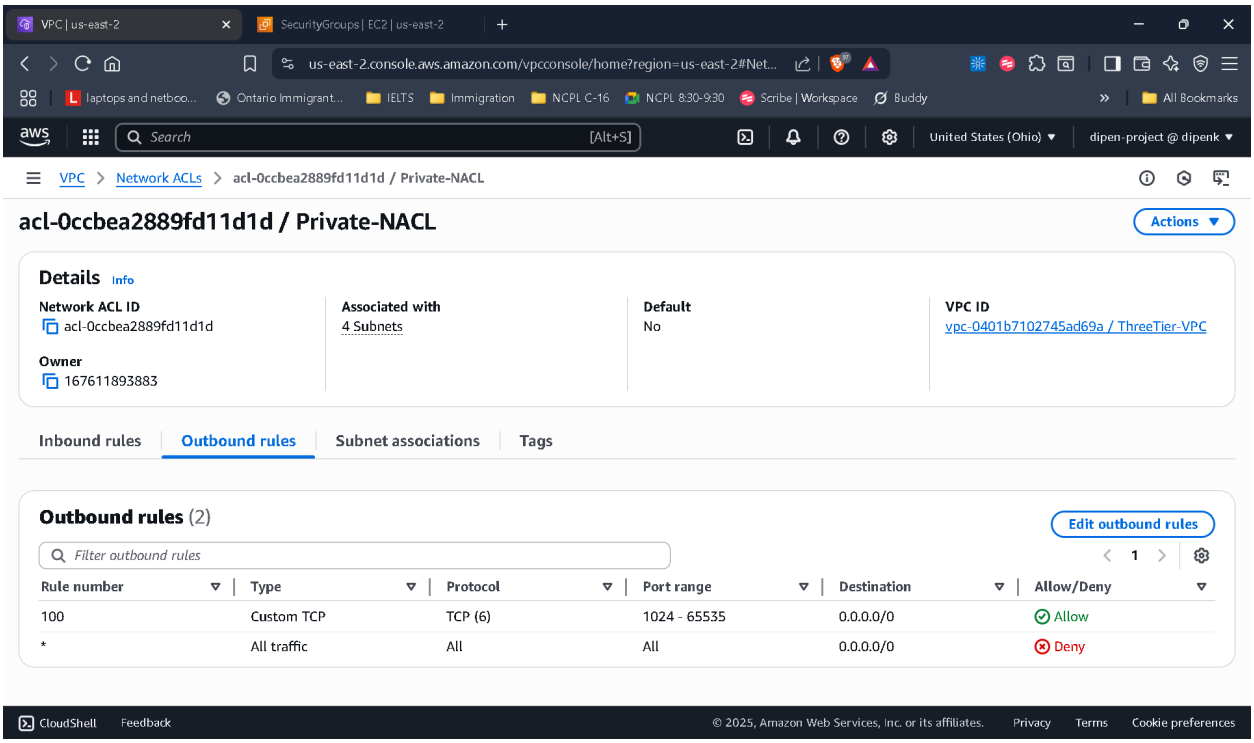
| Rule # | Type | Port Range | Source | Allow/Deny |
|---|---|---|---|---|
| 100 | Custom TCP | 3000 | 10.0.1.0/24 | ALLOW |
| 110 | MySQL | 3306 | 10.0.3.0/24 | ALLOW |
| 120 | Ephemeral | 1024–65535 | 10.0.1.0/24 | ALLOW |
| * | ALL | ALL | 0.0.0.0/0 | DENY |

Outbound rules

| Rule # | Type | Port Range | Destination | Allow/Deny |
|---|---|---|---|---|
| 100 | Ephemeral | 1024–65535 | 0.0.0.0/0 | ALLOW |
| * | ALL | ALL | 0.0.0.0/0 | DENY |

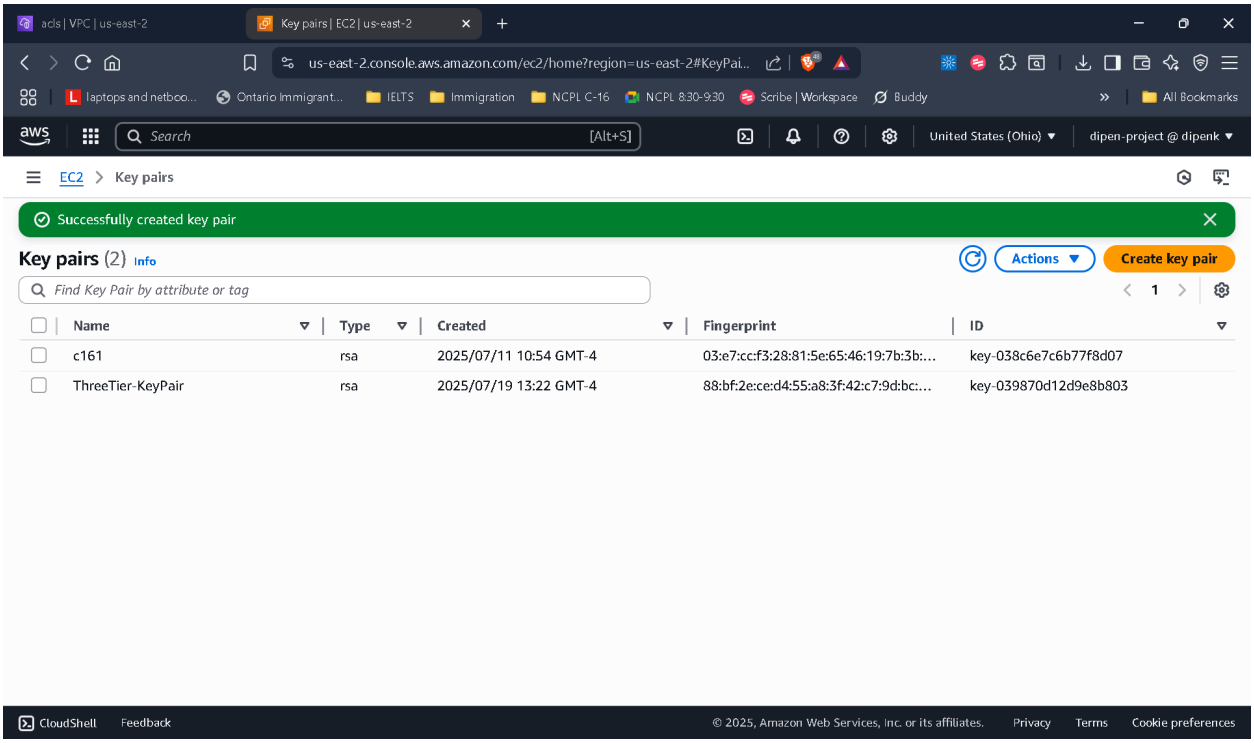

VPC | us-east-2
SecurityGroups | EC2 | us-east-2
us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#Net...
Search [Alt+S]
United States (Ohio)
dipen-project @ dipenk
VPC > Network ACLs > acl-0ccbea2889fd11d1d / Private-NACL
Details Info
Network ACL ID
acl-0ccbea2889fd11d1d
Associated with
4 Subnets
Default
No
VPC ID
vpc-0401b7102745ad69a / ThreeTier-VPC
Owner
167611893883
Inbound rules
Outbound rules
Subnet associations
Tags
Subnet associations (4)
Edit subnet associations
Filter subnet associations
Name
Subnet ID
Associated with
Availability Zone
IPv4 CIDR
IPv6 CIDR
App-Priv-2
subnet-06efb4847f3088...
acl-0ccbea2889fd11d1d / Private-NACL
us-east-2b
10.0.4.0/24
–
DB-Priv-2
subnet-0e1b8ad794e32...
acl-0ccbea2889fd11d1d / Private-NACL
us-east-2b
10.0.6.0/24
–
App-Priv-1
subnet-07eb8462b470d...
acl-0ccbea2889fd11d1d / Private-NACL
us-east-2a
10.0.3.0/24
–
DB-Priv-1
subnet-04096aba77919...
acl-0ccbea2889fd11d1d / Private-NACL
us-east-2a
10.0.5.0/24
–
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


VPC | us-east-2
SecurityGroups | EC2 | us-east-2
us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#Net...
Search [Alt+S]
United States (Ohio)
dipen-project @ dipenk
VPC > Network ACLs > acl-0ccbea2889fd11d1d / Private-NACL
Details Info
Network ACL ID
acl-0ccbea2889fd11d1d
Associated with
4 Subnets
Default
No
VPC ID
vpc-0401b7102745ad69a / ThreeTier-VPC
Owner
167611893883
Inbound rules
Outbound rules
Subnet associations
Tags
Inbound rules (4)
Edit inbound rules
Filter inbound rules
Rule number
Type
Protocol
Port range
Source
Allow/Deny
100
Custom TCP
TCP (6)
3000
10.0.1.0/24
Allow
110
MySQL/Aurora (3306)
TCP (6)
3306
10.0.3.0/24
Allow
120
Custom TCP
TCP (6)
1024 - 65535
10.0.1.0/24
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


VPC | us-east-2
SecurityGroups | EC2 | us-east-2
us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#Net...
Search
[Alt+S]
United States (Ohio)
dipen-project @ dipenk
VPC > Network ACLs > acl-0ccbea2889fd11d1d / Private-NACL
acl-0ccbea2889fd11d1d / Private-NACL
Actions
Details Info
Network ACL ID
acl-0ccbea2889fd11d1d
Associated with
4 Subnets
Default
No
VPC ID
vpc-0401b7102745ad69a / ThreeTier-VPC
Owner
167611893883
Inbound rules
Outbound rules
Subnet associations
Tags
Outbound rules (2)
Edit outbound rules
Filter outbound rules
Rule number
Type
Protocol
Port range
Destination
Allow/Deny
100
Custom TCP
TCP (6)
1024 - 65535
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

## Create a Key Pair (for SSH into EC2)

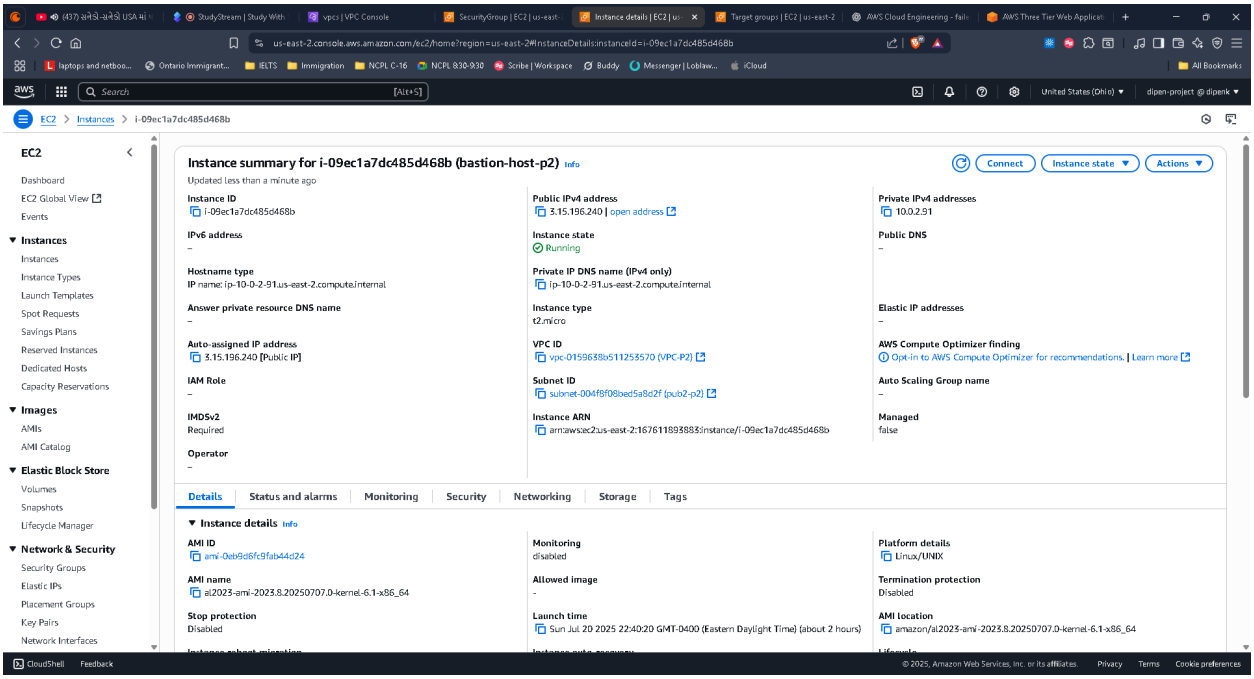
1. Go to **EC2 Dashboard → Key Pairs → Create Key Pair**
2. **Name**: ThreeTier-KeyPair
3. **Key pair type**: RSA (recommended for SSH)
4. **Private key format**: .pem (for Linux/Mac)
5. Click **Create key pair**
6. File will download as: ThreeTier-KeyPair.pem



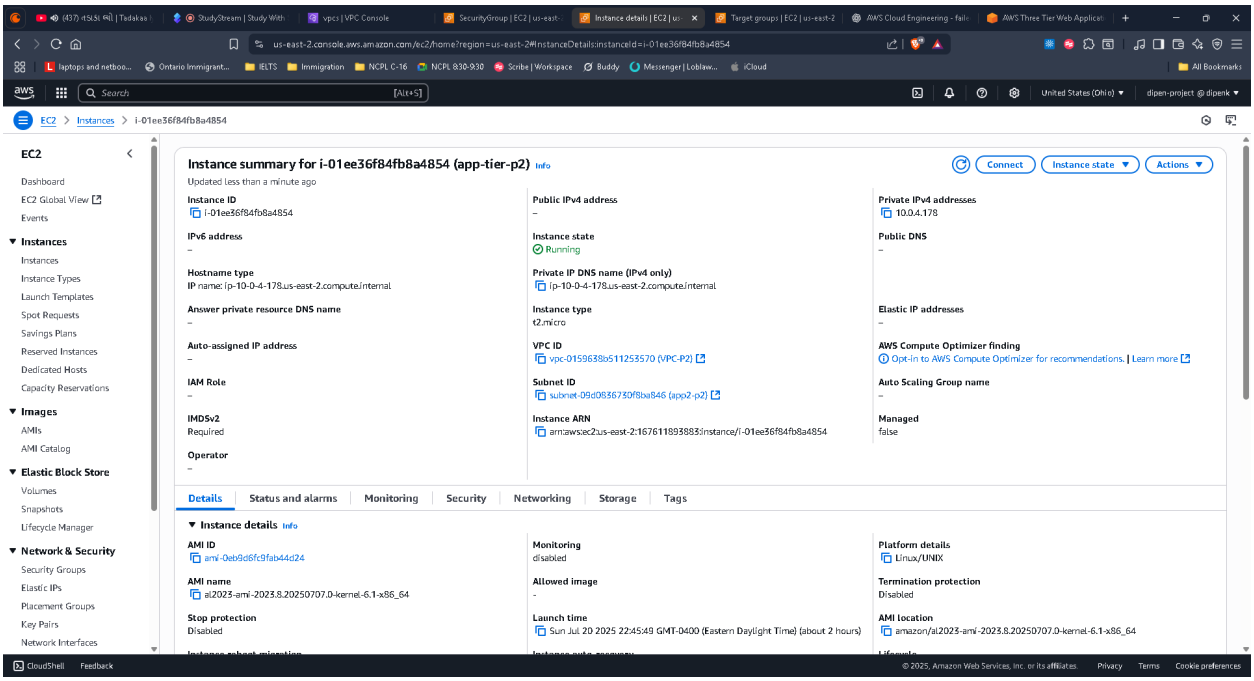
# Phase 3

# Launching Ec2 Instances

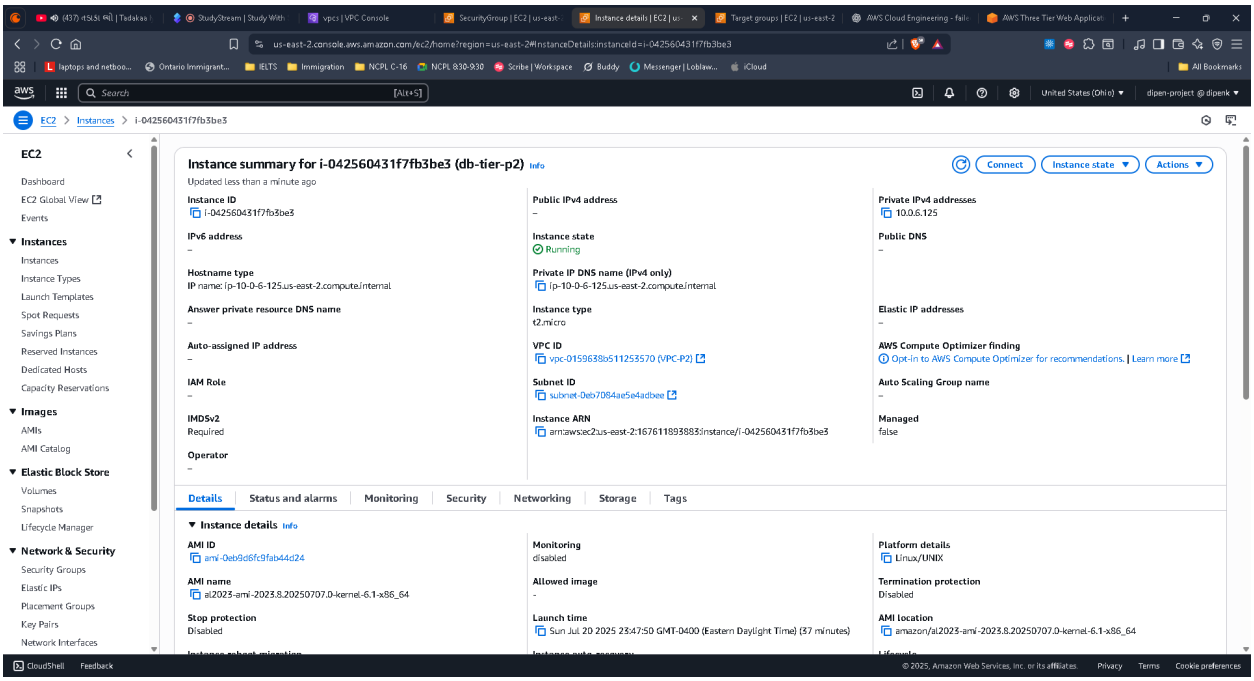
## Public Instance:




## App-tier Instance:



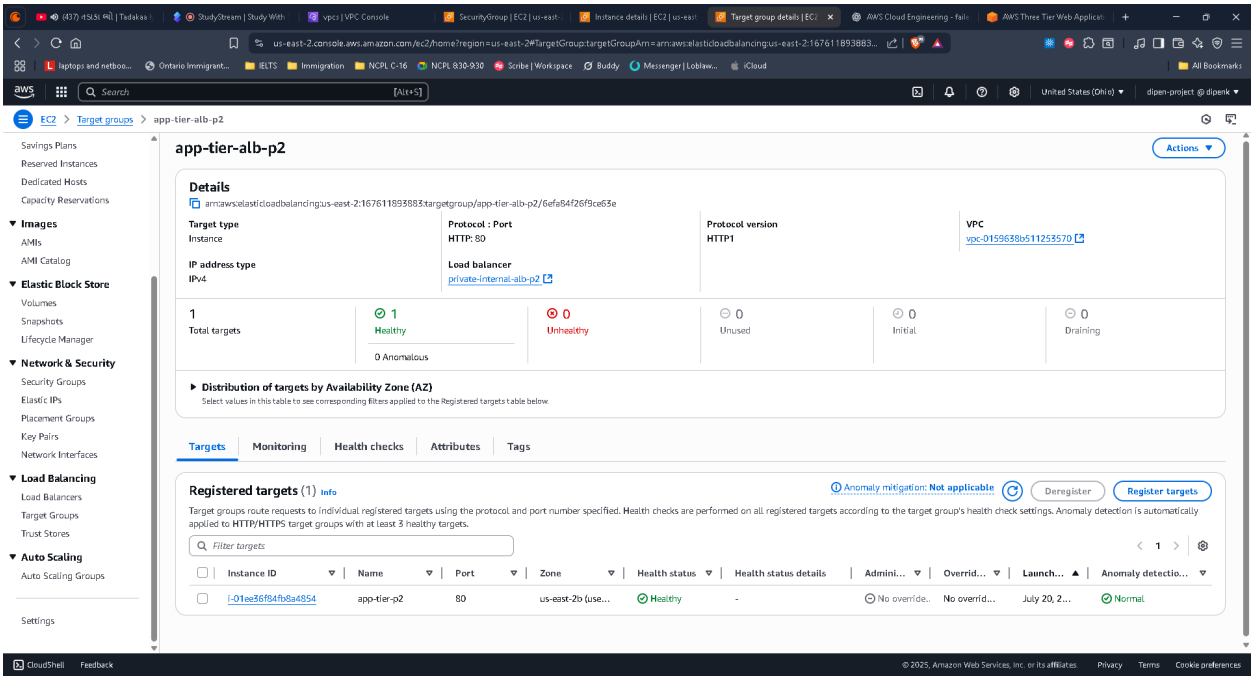
DB-tier-Instance:



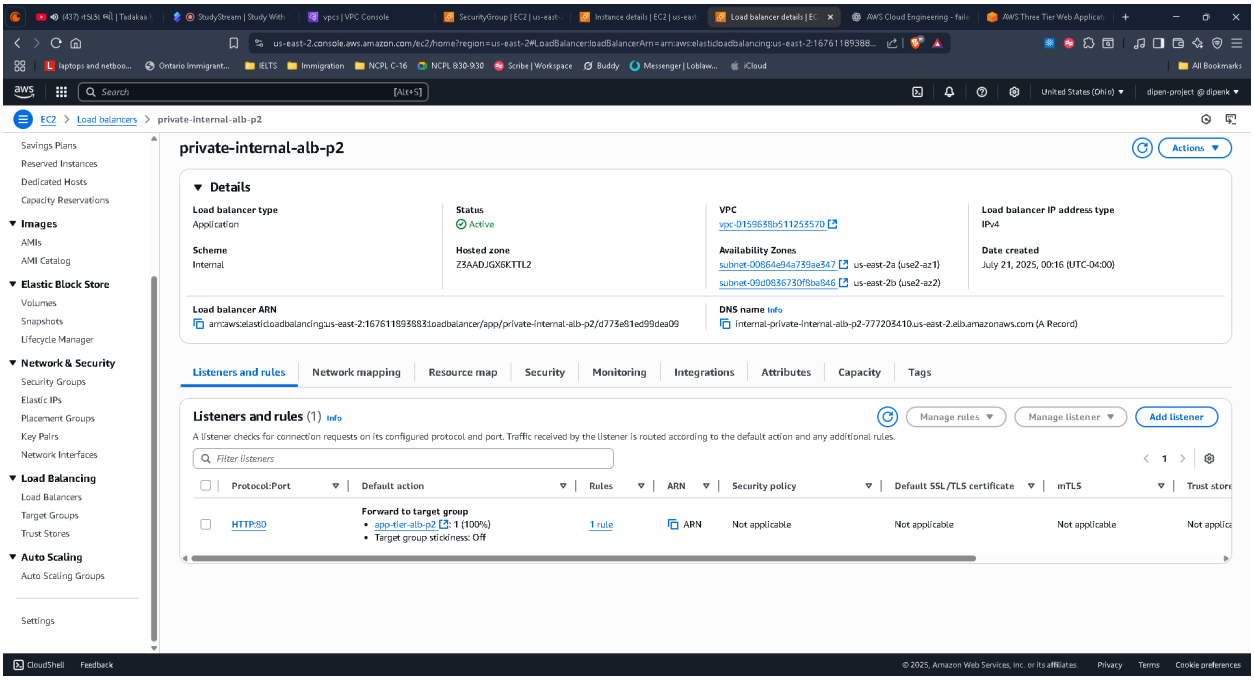
# Phase 4

# Creating Target Group & Application Load Balancer

## Target Group:




## Application Load Balancer:

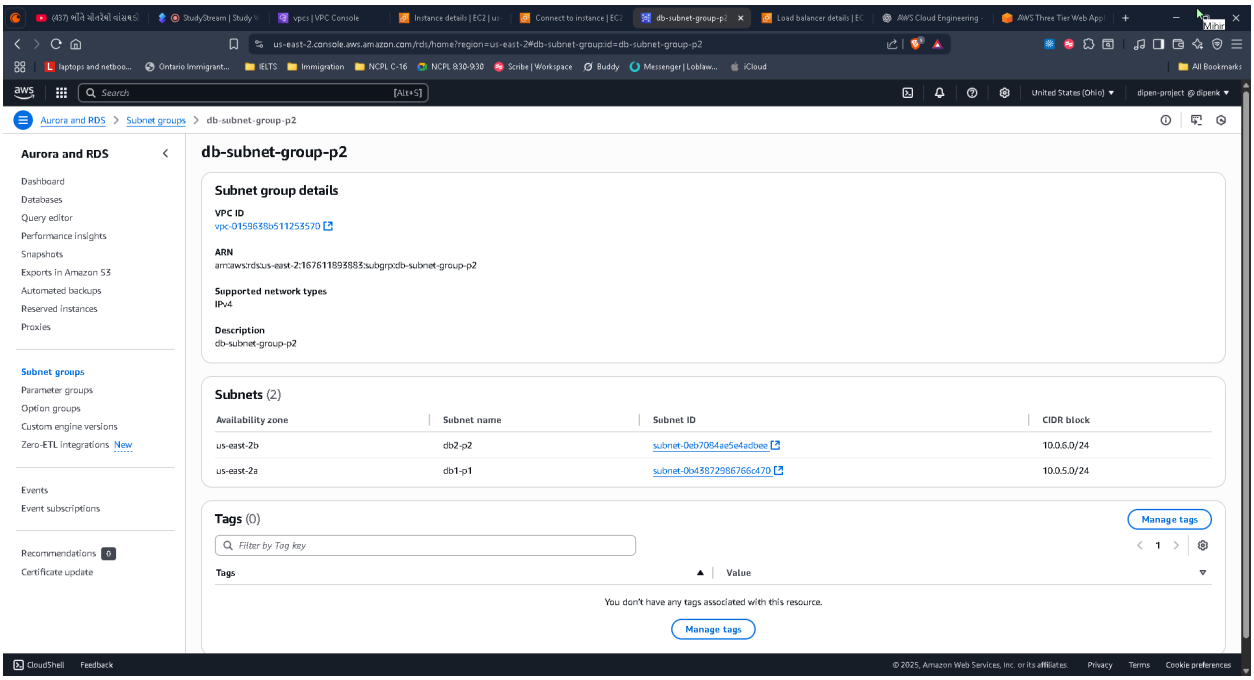


# Phase 5

# Database Tier (RDS Free Tier)

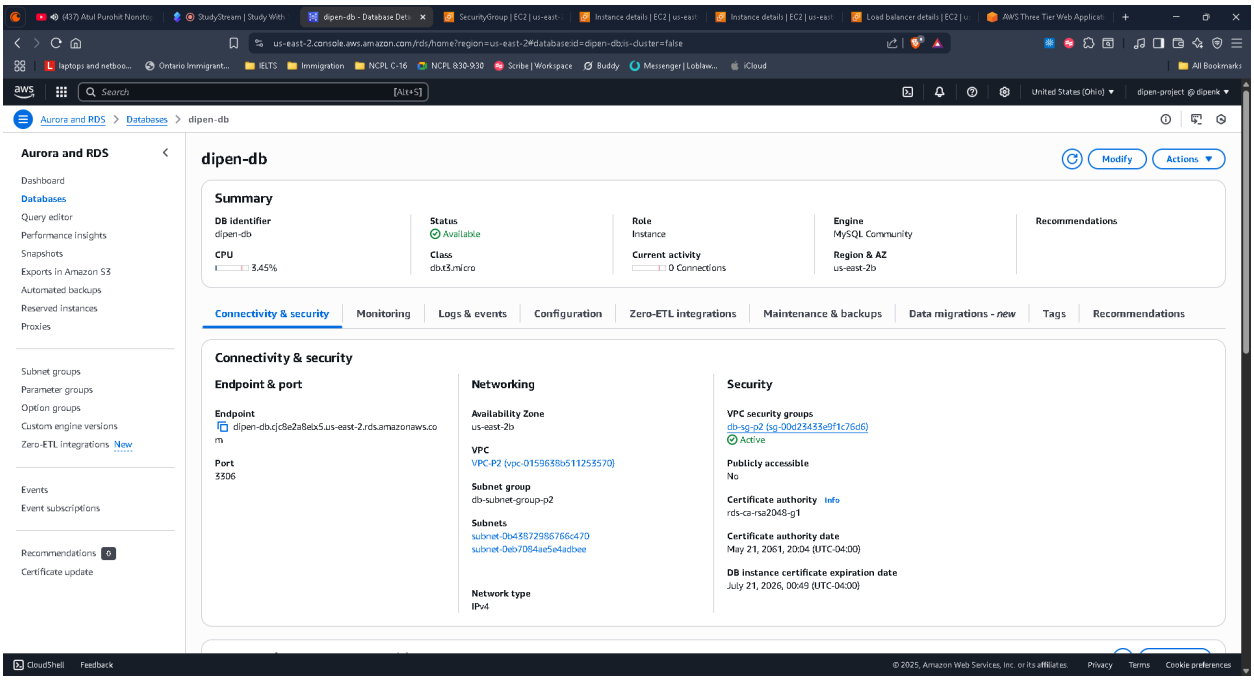
### Step 1: Create a DB Subnet Group

1. Go to **RDS > Subnet groups > Create DB subnet group**
2. Name: db-subnet-group-p2
3. VPC: Select your VPC (vpc-p2)
4. Add **2 subnets** (must be in different AZs):
    - db1-p2 (e.g., 10.0.5.0/24)
    - db2-p2 (e.g., 10.0.6.0/24)



## Step 2: Launch RDS Instance (MySQL)

1. Go to **RDS > Databases > Create database**
2. Choose **Standard Create**
3. Engine: **MySQL**
4. Version: Latest **Free Tier eligible** (e.g., 8.x)
5. Template: **Free Tier**
6. DB Instance Identifier: dipen-db
7. Master username: admin
8. Password: Choose strong password (store it safely)
9. DB instance size: **db.t3.micro**
10. Storage: 20 GB (General Purpose SSD)



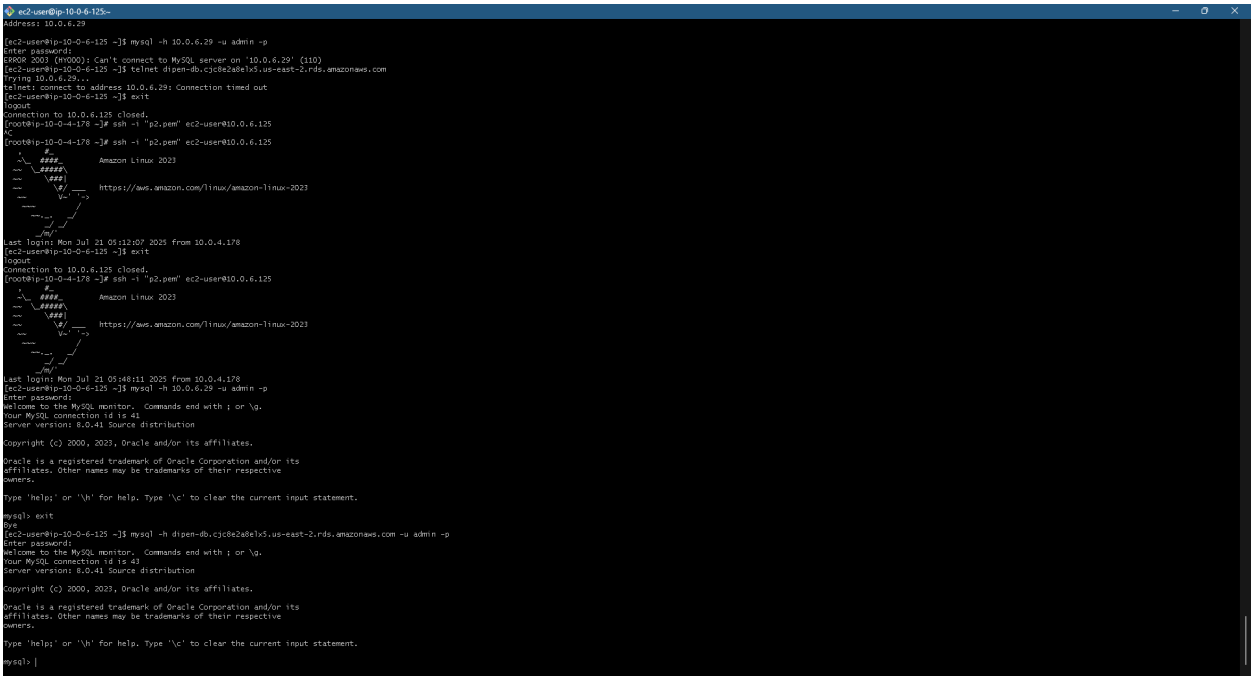
**Note: DB tier EC2 instance has **two SGs attached**:**

**1. db-sg-p2 → Accepts SSH from app tier SG**

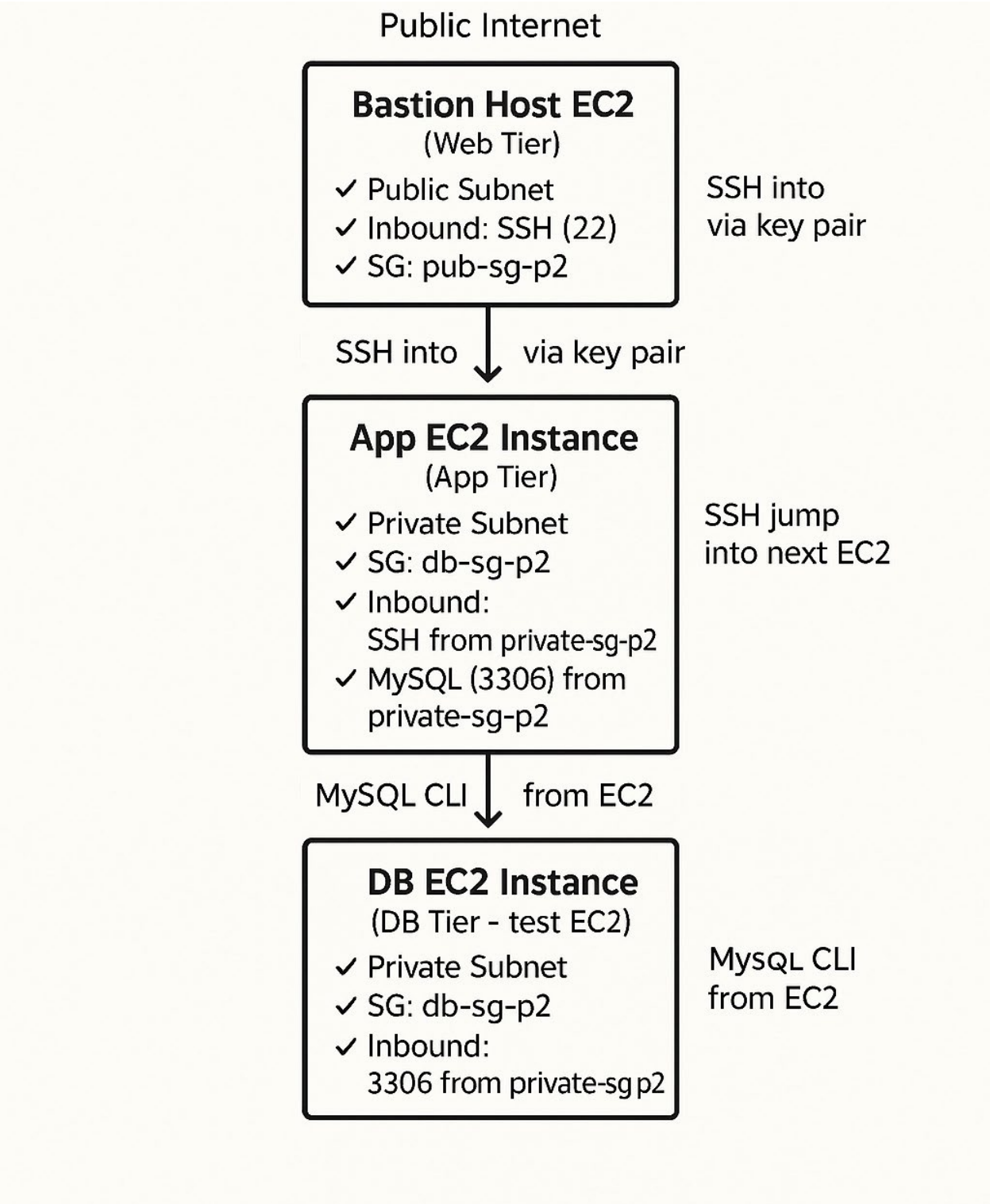
**2. private-sg-p2 → Enables outbound MySQL traffic to RDS**

**This dual SG setup allows full connectivity between layers while maintaining modular SG rules.**

## RDS Connection



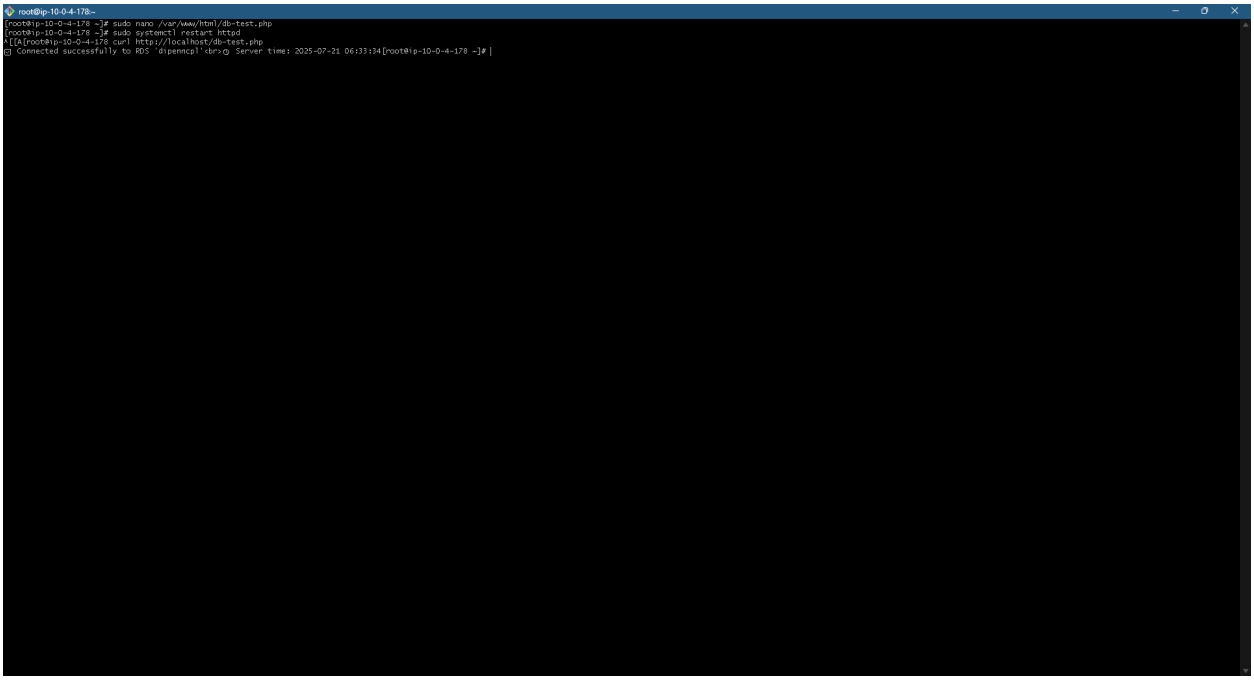
## Flowchart of RDS Connection



| Tier | Security Group | Inbound Allows From | Port(s) |
|---|---|---|---|
| Web Tier | pub-sg-p2 | My IP (SSH/HTTP) | 22, 80 |
| App Tier | private-sg-p2 | pub-sg-p2 | 22, 80 |
| DB Tier | db-sg-p2 | private-sg-p2 | 22, 3306 |
| RDS | db-sg-p2 | db-sg-p2 (self-ref) | 3306 |

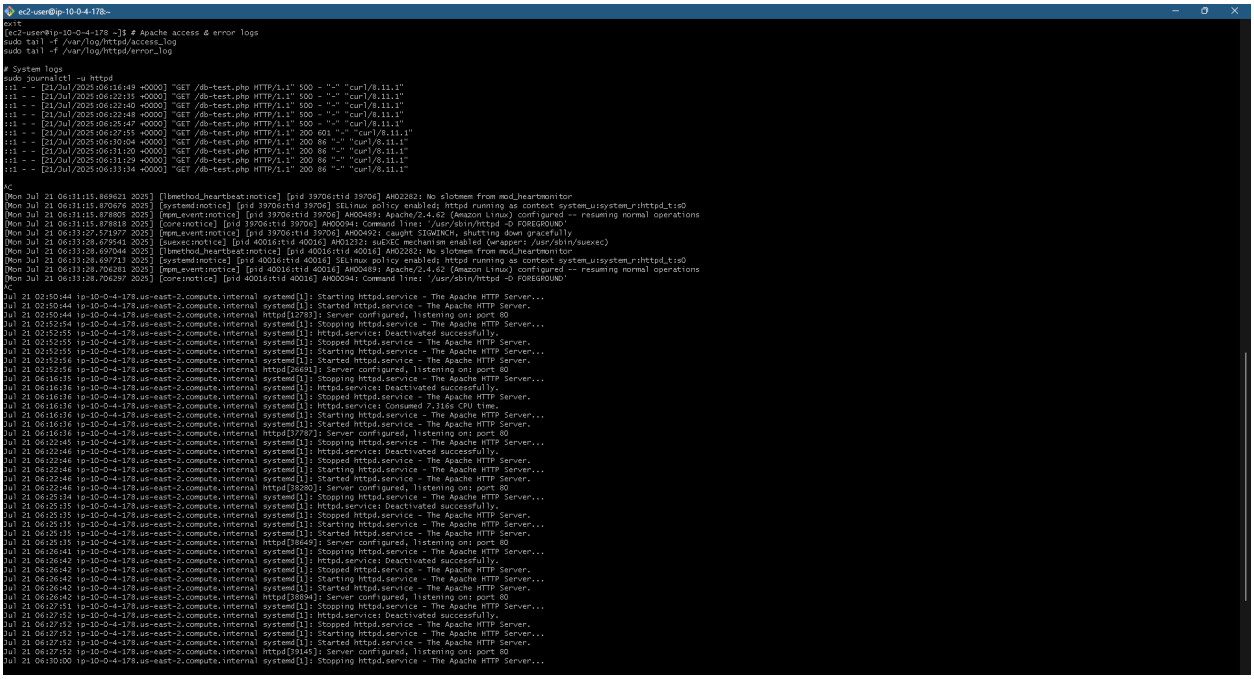
# Flow Check


root@ip-10-0-4-178:~
GNU nano 8.3 /var/www/html/db-test.php
<?php
ini_set('display_errors', 1);
error_reporting(E_ALL);
$host = "dipen-db.cjc8e2a8elx5.us-east-2.rds.amazonaws.com";
$user = "admin";
$pass = "90166Dipen";  // Replace this with the actual password
$db   = "dipenncpl";
$conn = new mysqli($host, $user, $pass, $db);
if ($conn->connect_error) {
die("❌ Connection failed: " . $conn->connect_error);
}
echo "✅ Connected successfully to RDS '{$db}'<br>";
echo "🕒 Server time: " . date("Y-m-d H:i:s");
?>
[ Read 18 lines ]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous ^B Back ^← Prev Word ^A Home ^P Prev Line M-▲ Scroll Up
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy M-W Where Was M-W Next ^F Forward ^→ Next Word ^E End ^N Next Line M-▼ Scroll Down

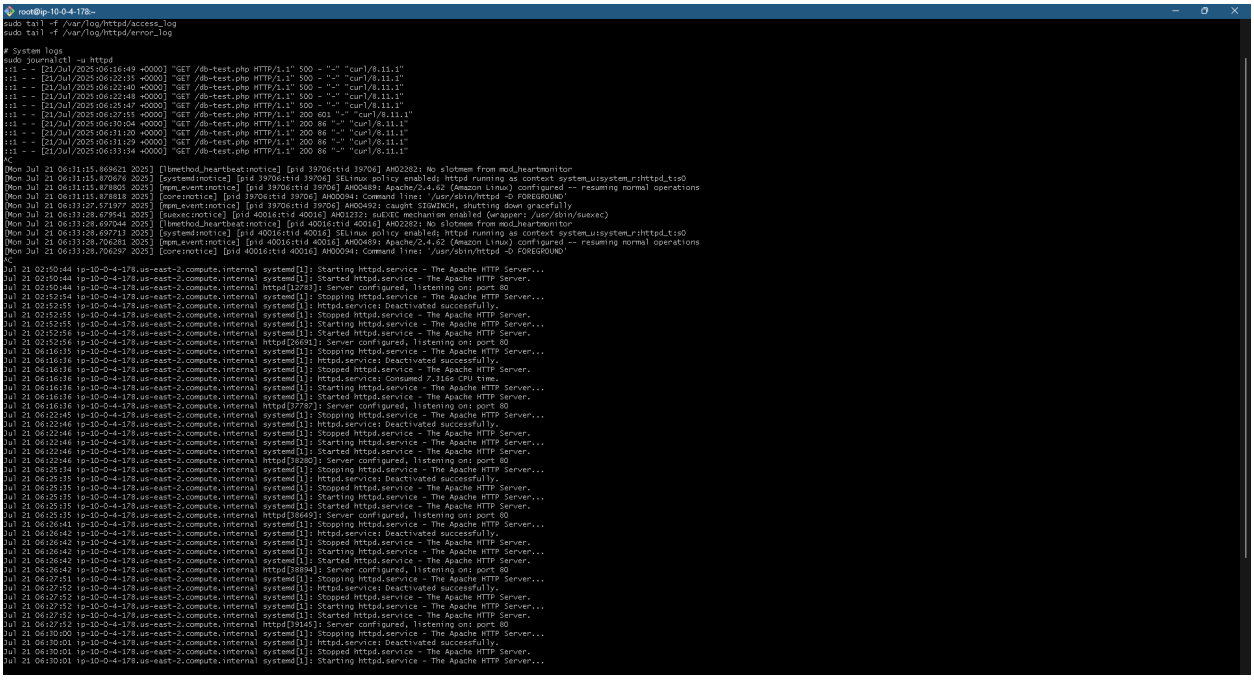

root@ip-10-0-4-178:~
[root@ip-10-0-4-178 ~]# sudo nano /var/www/html/db-test.php
[root@ip-10-0-4-178 ~]# sudo systemctl restart httpd
^[[A[root@ip-10-0-4-178 ~]# curl http://localhost/db-test.php
✅ Connected successfully to RDS 'dipenncpl'<br>🕒 Server time: 2025-07-21 06:33:34[root@ip-10-0-4-178 ~]#

# Logs checking

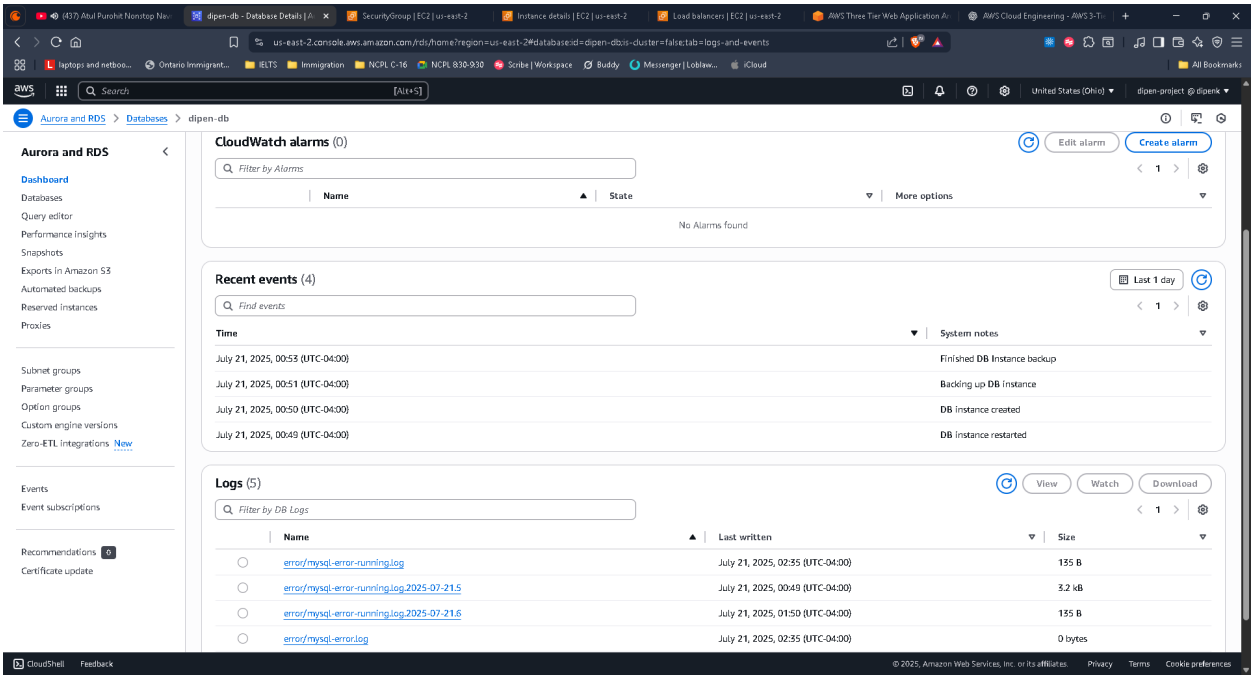
## Web Tier (Bastion)

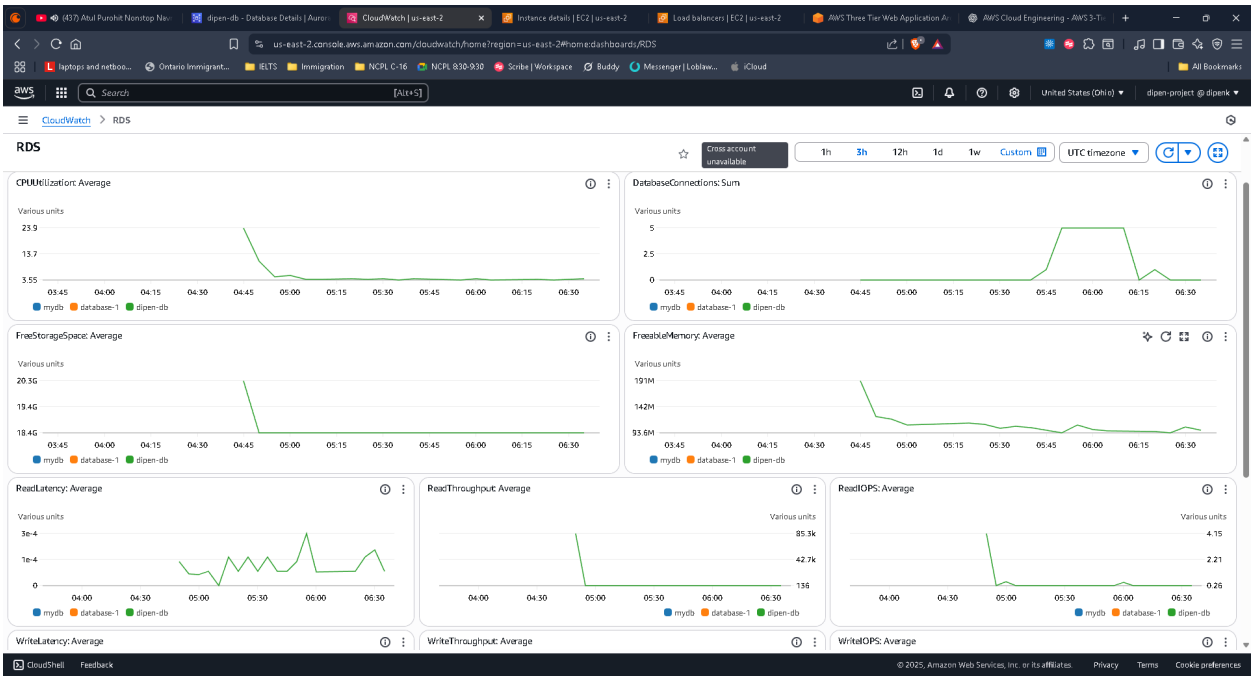


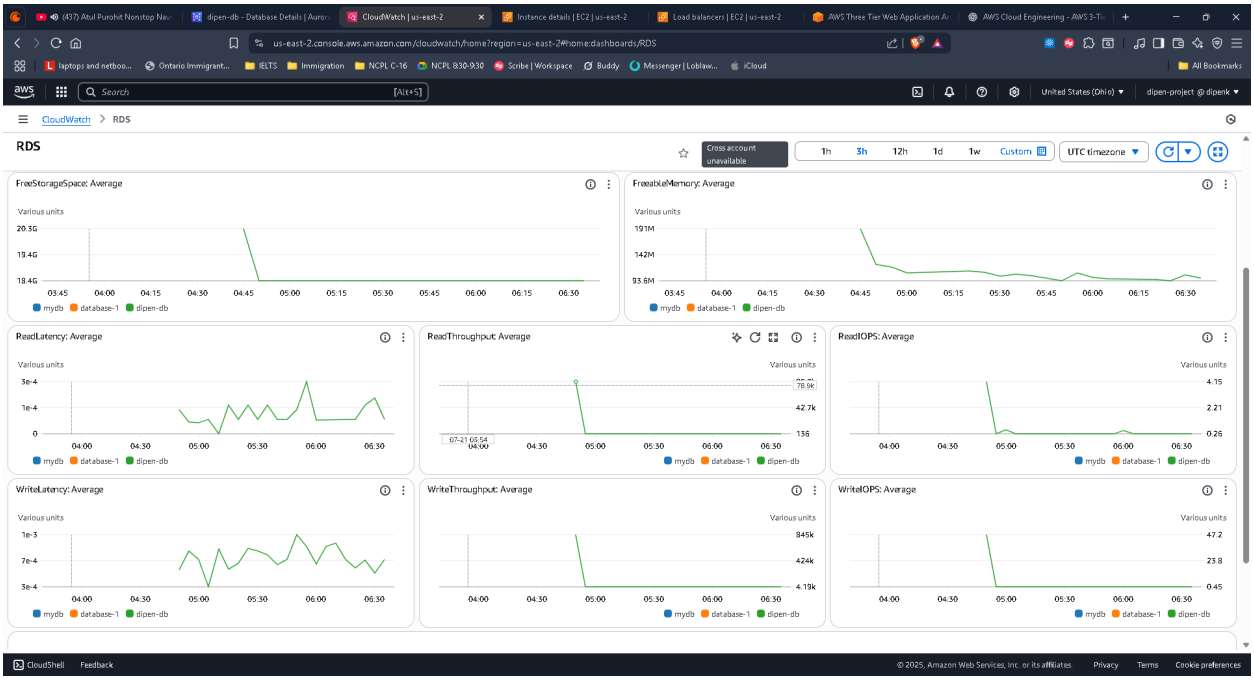

## App-tier EC2



# RDS Logs


Aurora and RDS > Databases > dipen-db
Aurora and RDS
Dashboard
Databases
Query editor
Performance insights
Snapshots
Exports in Amazon S3
Automated backups
Reserved instances
Proxies
Subnet groups
Parameter groups
Option groups
Custom engine versions
Zero-ETL integrations New
Events
Event subscriptions
Recommendations 0
Certificate update
CloudWatch alarms (0)
Edit alarm
Create alarm
Filter by Alarms
Name
State
More options
No Alarms found
Recent events (4)
Last 1 day
Find events
Time
System notes
July 21, 2025, 00:53 (UTC-04:00)
Finished DB Instance backup
July 21, 2025, 00:51 (UTC-04:00)
Backing up DB instance
July 21, 2025, 00:50 (UTC-04:00)
DB instance created
July 21, 2025, 00:49 (UTC-04:00)
DB instance restarted
Logs (5)
View
Watch
Download
Filter by DB Logs
Name
Last written
Size
error/mysql-error-running.log
July 21, 2025, 02:35 (UTC-04:00)
135 B
error/mysql-error-running.log.2025-07-21.5
July 21, 2025, 00:49 (UTC-04:00)
3.2 kB
error/mysql-error-running.log.2025-07-21.6
July 21, 2025, 01:50 (UTC-04:00)
135 B
error/mysql-error.log
July 21, 2025, 02:35 (UTC-04:00)
0 bytes
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


CloudWatch > RDS
RDS
Cross account unavailable
1h
3h
12h
1d
1w
Custom
UTC timezone
CPUUtilization: Average
DatabaseConnections: Sum
FreeStorageSpace: Average
FreeableMemory: Average
ReadLatency: Average
ReadThroughput: Average
ReadIOPS: Average
WriteLatency: Average
WriteThroughput: Average
WriteIOPS: Average
Various units
mydb
database-1
dipen-db
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


RDS
FreeStorageSpace: Average
FreeableMemory: Average
ReadLatency: Average
ReadThroughput: Average
ReadIOPS: Average
WriteLatency: Average
WriteThroughput: Average
WriteIOPS: Average
Various units
mydb
database-1
dipen-db