

## **Module 5: Case Study - 1**

## **Problem Statement:**

You work for XYZ Corporation and based on the expansion requirements of your corporation you have been asked to create and set up a distinct Amazon VPC for the production and development team. You are expected to perform the following tasks for the respective VPCs.

### **Production Network:**

1. Design and build a 4-tier architecture.
2. Create 5 subnets out of which 4 should be private named app1, app2, dbcache and db and one should be public, named web.
3. Launch instances in all subnets and name them as per the subnet that they have been launched in.
4. Allow dbcache instance and app1 subnet to send internet requests.
5. Manage security groups and NACLs.

---

### **Development Network:**

1. Design and build 2-tier architecture with two subnets named web and db and launch instances in both subnets and name them as per the subnet names.
2. Make sure only the web subnet can send internet requests.
3. Create peering connection between production network and development network.
4. Setup connection between db subnets of both production network and development network respectively.

# Created a VPC with name Production-Network-VPC

Start Cour... x Home | EC... x SecurityGr... x subnets | V... x EC2 Instar... x VpcDetails x IP Subnet... x FREE Adv... x +

← → ↻ 🏠 🔍 ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#VpcDetails:VpcId=vpc-0f489e02b770223dd 🔍 ☆ 📁 ⬇️ 🌐 ⋮

aws

Services 🔍 Search [Alt+S]

📺 🔔 ⓘ ⚙️ Mumbai ▾ prakash24 ▾

EC2 EC2 Image Builder S3 IAM VPC

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

Endpoints

Endpoint services

NAT gateways

Peering connections

▼ Security

VPC > Your VPCs > vpc-0f489e02b770223dd

vpc-0f489e02b770223dd / Production-Network-VPC-vpc Actions ▾

Details Info

|   |   |   |   |
|---|---|---|---|
| VPC ID<br>📄 vpc-0f489e02b770223dd         | State<br>✅ Available                            | DNS hostnames<br>Enabled                  | DNS resolution<br>Enabled                 |
| Tenancy<br>Default                        | DHCP option set<br>dopt-0913a800f5fbf361b       | Main route table<br>rtb-047a56a6594122622 | Main network ACL<br>acl-0080075863857ba94 |
| Default VPC<br>No                         | IPv4 CIDR<br>10.0.0.0/24                        | IPv6 pool<br>-                            | IPv6 CIDR (Network border group)<br>-     |
| Network Address Usage metrics<br>Disabled | Route 53 Resolver DNS Firewall rule groups<br>- | Owner ID<br>📄 654654393526                |   |

Resource map Info

Resource map

CIDRs

Flow logs

Tags

Integrations

VPC Show details

Your AWS virtual network

Subnets (5)

Subnets within this VPC

Route tables (6)

Route network traffic to resources

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Created 5 subnet in the Production-Network-VPC app1, app2, dbcache and db (Private) and web (Public).

Start Cour... x

Home | EC... x

SecurityGr... x

subnets | \ x

EC2 Instan... x

subnets | \ x

IP Subnet... x

FREE Adv... x

+

—

🔍

🌐

📄

🔗

⋮

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#subnets:vpcid=vpc-0f489e02b770223dd

aws

Services

Search

[Alt+S]

🔍

🔔

?

⚙️

Mumbai ▾

prakash24 ▾

EC2

EC2 Image Builder

S3

IAM

VPC

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

Endpoints

Endpoint services

NAT gateways

Peering connections

▼ Security

Network ACLs

Subnets (1/5)

Info

Last updated 3 minutes ago

🔄

Actions ▾

Create subnet

🔍 Find resources by attribute or tag

VPC : vpc-0f489e02b770223dd

✕

Clear filters

< 1 >

⚙️

| <input checked="" type="checkbox"/> | Name  | Subnet ID                | State     | VPC                           |
|-------------------------------------|---|--------------------------|-----------|-------------------------------|
| <input checked="" type="checkbox"/> | Production-Network-VPC-subnet-private-app2    | subnet-08f14dcf7d541d2e8 | Available | vpc-0f489e02b770223dd   Produ |
| <input type="checkbox"/>            | Production-Network-VPC-subnet-public-web      | subnet-046b8e80fca1740d9 | Available | vpc-0f489e02b770223dd   Produ |
| <input type="checkbox"/>            | Production-Network-VPC-subnet-private-db      | subnet-0802f5e8c8b6435e1 | Available | vpc-0f489e02b770223dd   Produ |
| <input type="checkbox"/>            | Production-Network-VPC-subnet-private-app1    | subnet-0cbc8e31b508dec31 | Available | vpc-0f489e02b770223dd   Produ |
| <input type="checkbox"/>            | Production-Network-VPC-subnet-private-dbcache | subnet-03a7be0abda47c656 | Available | vpc-0f489e02b770223dd   Produ |

subnet-08f14dcf7d541d2e8 / Production-Network-VPC-subnet-private-app2

Details

Flow logs

Route table

Network ACL

CIDR reservations

Sharing

Tags

Details

Subnet ID

Subnet ARN

State

IPv4 CIDR

subnet-08f14dcf7d541d2e8

arn:aws:ec2:ap-south-

Available

10.0.0.192/27

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences



Created a VPC with name Development-Network-VPC

Start Cour... x

Home | EC... x

SecurityGr... x

subnets | \... x

EC2 Instan... x

VpcDetails... x

IP Subnet... x

FREE Adv... x

+

-

x

← → ↻ 🏠 🔍 ☆ 📁 📑 ⬇️ 👤 ⋮

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#VpcDetails:VpcId=vpc-013deaed419e530ef

aws Services 🔍 Search [Alt+S]

EC2 EC2 Image Builder S3 IAM VPC

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

Endpoints

Endpoint services

NAT gateways

Peering connections

▼ Security

VPC > Your VPCs > vpc-013deaed419e530ef

vpc-013deaed419e530ef / Development-Network-VPC-vpc

Actions ▾

Details Info

|                               |  |                       |                                  |
|-------------------------------|--|-----------------------|----------------------------------|
| VPC ID                        | State                                      | DNS hostnames         | DNS resolution                   |
| 📄 vpc-013deaed419e530ef       | 🟢 Available                                | Enabled               | Enabled                          |
| Tenancy                       | DHCP option set                            | Main route table      | Main network ACL                 |
| Default                       | dopt-0913a800f5fbf361b                     | rtb-0cf0b7aca139115ce | acl-00f34f9b94a1db75b            |
| Default VPC                   | IPv4 CIDR                                  | IPv6 pool             | IPv6 CIDR (Network border group) |
| No                            | 10.0.0.0/16                                | -                     | -                                |
| Network Address Usage metrics | Route 53 Resolver DNS Firewall rule groups | Owner ID              |                                  |
| Disabled                      | -  | 📄 654654393526        |                                  |

Resource map Info

VPC Show details

Your AWS virtual network

Subnets (2)

Subnets within this VPC

Route tables (3)

Route network traffic to resources

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## Created 2 subnet inside Development-Network-VPC with name of DB (private) and Web (Public)

The screenshot displays the AWS Management Console interface for the 'Development-Network-VPC'. The left sidebar shows the 'VPC dashboard' with a list of resources including Subnets, Route tables, Internet gateways, and NAT gateways. The main content area shows the 'Subnets (1/2)' list, which contains two subnets: 'Development-Network-VPC-subnet-public-Web' and 'Development-Network-VPC-subnet-private-DB'. The 'Development-Network-VPC-subnet-private-DB' subnet is selected, and its details are shown below the list. The details include the Subnet ID, Subnet ARN, State (Available), and IPv4 CIDR (10.0.128.0/20).

**Subnets (1/2)**

| Name                                      | Subnet ID                | State     | VPC                   |
|---|--------------------------|-----------|-----------------------|
| Development-Network-VPC-subnet-public-Web | subnet-03e752069c3122fe5 | Available | vpc-013deaed419e530ef |
| Development-Network-VPC-subnet-private-DB | subnet-0f1fa7592d07c8d15 | Available | vpc-013deaed419e530ef |

**subnet-0f1fa7592d07c8d15 / Development-Network-VPC-subnet-private-DB**

**Details**

| Subnet ID                | Subnet ARN  | State     | IPv4 CIDR     |
|--------------------------|---|-----------|---------------|
| subnet-0f1fa7592d07c8d15 | arn:aws:ec2:ap-south-1:123456789012:subnet/subnet-0f1fa7592d07c8d15 | Available | 10.0.128.0/20 |

# Launch instances in all 5 subnet in Production-Network-VPC

Start Cour

Instances

SecurityGr

subnets

EC2 Insta

subnets

IP Subnet

FREE Adv

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

Mumbai

prakash24

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 (6)

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 |
|--------------------------|-------------------------|---------------------|----------------|---------------|-------------------|--------------|
| <input type="checkbox"/> | Public-ec2-Pro-Web      | i-0df572e6e601fbecd | Running        | t2.micro      | 2/2 checks passed | View alarms  |
| <input type="checkbox"/> | Private-ec2-Pro-App1    | i-044f18afd3046e944 | Running        | t2.micro      | 2/2 checks passed | View alarms  |
| <input type="checkbox"/> | Private-ec2-Pro-dbcache | i-033beeace37fba7b8 | Running        | t2.micro      | 2/2 checks passed | View alarms  |
| <input type="checkbox"/> | Private-ec2-Pro-App2    | i-0a0ebd15a5535262a | Running        | t2.nano       | Initializing      | View alarms  |
| <input type="checkbox"/> | Private-ec2-Pro-db      | i-0c9a800e558facef6 | Running        | t2.nano       | 2/2 checks passed | View alarms  |

Select an instance

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## Launch instances in all 2 subnet in Development-Network-VPC

The screenshot displays the AWS Management Console for the 'ap-south-1' region. The left sidebar shows the navigation menu with 'Instances' selected. The main content area shows the 'Instances (2)' page, filtered by 'VPC ID = vpc-013deaed419e530ef'. Two instances are listed: 'Public-ec2-Dev-Web' (Running) and 'Private-ec2-Dev-db' (Initializing). A 'Select an instance' dialog box is open at the bottom.

**Instances (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

VPC ID = vpc-013deaed419e530ef Clear filters

| <input type="checkbox"/> | Name               | Instance ID         | Instance state | Instance type | Status check      | Alarm status                |
|--------------------------|--------------------|---------------------|----------------|---------------|-------------------|-----------------------------|
| <input type="checkbox"/> | Public-ec2-Dev-Web | i-0ac3204f1414f0b3d | Running        | t2.small      | 2/2 checks passed | <a href="#">View alarms</a> |
| <input type="checkbox"/> | Private-ec2-Dev-db | i-0439329449c54df8a | Running        | t2.small      | Initializing      | <a href="#">View alarms</a> |

Select an instance

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



# List of all route tables in Production-Network-VPC

Start Course

Instances

RouteTables

Connect to in

EC2 Instance

IP Subnet Cal

FREE Advance

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTables:vpcId=vpc-0f489e02b770223dd

aws Services Search [Alt+S]

EC2 EC2 Image Builder S3 IAM VPC

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

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Route tables (6) Info

Last updated less than a minute ago

Actions

Create route table

Find resources by attribute or tag

VPC : vpc-0f489e02b770223dd

Clear filters

| <input type="checkbox"/> | Name                                       | Route table ID                        | Explicit subnet associ...                | Edge asso |
|--------------------------|--|---------------------------------------|--|-----------|
| <input type="checkbox"/> | Production-Network-VPC-rtb-private-db      | <a href="#">rtb-09c1ddd0c3ef2c11f</a> | <a href="#">subnet-0802f5e8c8b643...</a> | -         |
| <input type="checkbox"/> | Production-Network-VPC-rtb-private-app2    | <a href="#">rtb-00b4bfb1da0886cfa</a> | <a href="#">subnet-08f14dcf7d541d...</a> | -         |
| <input type="checkbox"/> | Production-Network-VPC-rtb-private-dbcache | <a href="#">rtb-02bf59e454f12161e</a> | <a href="#">subnet-03a7be0abda47c...</a> | -         |
| <input type="checkbox"/> | Production-Network-VPC-rtb-Main            | <a href="#">rtb-047a56a6594122622</a> | -  | -         |
| <input type="checkbox"/> | Production-Network-VPC-rtb-private-app1    | <a href="#">rtb-00fcc32b87b70b5f0</a> | <a href="#">subnet-0cbc8e31b508de...</a> | -         |
| <input type="checkbox"/> | Production-Network-VPC-rtb-public-Web      | <a href="#">rtb-0252e9bb32039226b</a> | <a href="#">subnet-046b8e80fca174...</a> | -         |

Select a route table

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# List of all route tables in Development-Network-VPC

Start Course

Instances | EC2

RouteTables

Connect to in

EC2 Instance

IP Subnet Cal

FREE Advanc

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTables:vpclid=vpc-013deaed419e530ef

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

Mumbai

prakash24

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

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Route tables (3)

Info

Last updated less than a minute ago

Actions

Create route table

Find resources by attribute or tag

VPC : vpc-013deaed419e530ef

Clear filters

| <input type="checkbox"/> | Name                                   | Route table ID                        | Explicit subnet associ...                 | Edge asso |
|--------------------------|--|---------------------------------------|---|-----------|
| <input type="checkbox"/> | Development-Network-VPC-rtb-private-DB | <a href="#">rtb-0c2ba03e7c626bb07</a> | <a href="#">subnet-0f1fa7592d07c8d...</a> | -         |
| <input type="checkbox"/> | Development-Network-VPC-rtb-Main       | <a href="#">rtb-0cf0b7aca139115ce</a> | -   | -         |
| <input type="checkbox"/> | Development-Network-VPC-rtb-public     | <a href="#">rtb-0ef5f04b2d25764dc</a> | <a href="#">subnet-03e752069c3122...</a>  | -         |

Select a route table

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

# List of all NAT Gateway for both the network

Start Course

Instances

NatGateways

Connect to in

EC2 Instance

IP Subnet Cal

FREE Advance

← → ↺ 🏠 🔍 ☆ 📌 👤

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#NatGateways:

🔍 Search [Alt+S]

📺 🔔 ⓘ ⚙️ Mumbai prakash24

EC2 EC2 Image Builder S3 IAM VPC

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

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

NAT gateways (2) Info

Find resources by attribute or tag

|                       | Name  | NAT gateway ID                        | Connectivity... | State       | State message |
|-----------------------|---|---------------------------------------|-----------------|-------------|---------------|
| <input type="radio"/> | Development-Network-VPC-nat-public1-ap-south-1a | <a href="#">nat-075502843136bce79</a> | Public          | ✓ Available | -             |
| <input type="radio"/> | Production-Network-VPC-nat-public1-ap-south-1a  | <a href="#">nat-0150459d9d2f086d4</a> | Public          | ✓ Available | -             |

Select a NAT gateway

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

# List of all Internet Gateway for both the network

Start Course

Instances

igws

VPC Co

Connect to in

EC2 Instance

IP Subnet Cal

FREE Advance

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#igws:

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

Mumbai

prakash24

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

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Internet gateways (3)

Search

|                          | Name                        | Internet gateway ID                   | State    | VPC ID  | Owner |
|--------------------------|-----------------------------|---------------------------------------|----------|---|-------|
| <input type="checkbox"/> | -                           | <a href="#">igw-05362d1c5ca88e515</a> | Attached | <a href="#">vpc-09da02eb16a97ff13</a>                 | 654   |
| <input type="checkbox"/> | Production-Network-VPC-igw  | <a href="#">igw-0883336073f6da4e1</a> | Attached | <a href="#">vpc-0f489e02b770223dd</a>   Production... | 654   |
| <input type="checkbox"/> | Development-Network-VPC-igw | <a href="#">igw-0a0c1c4f10193bbb9</a> | Attached | <a href="#">vpc-013deaed419e530ef</a>   Developmen... | 654   |

Select an internet gateway above

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences



# Public instance of Production-Network-VPC

Start Course | Intellipaat

Instances | EC2 | ap-sou

Instances | EC2 | ap-sou

IP Subnet Calculator for

FREE Advanced Subnet C

← → ↺ 🏠 🔍 ☆ 📁 👤

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,...

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

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 (1/7)

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 |
|-------------------------------------|--------------------|---------------------|----------------|---------------|--------------|--------------|
| <input checked="" type="checkbox"/> | Public-ec2-Pro-Web | i-0df572e6e601fbecd | Running        | t2.micro      | Initializing | View alarms  |
| <input type="checkbox"/>            | Public-ec2-Dev-Web | i-0ac3204f1414f0b3d | Running        | t2.small      | -            | View alarms  |
| <input type="checkbox"/>            | Private-ec2-Dev-db | i-0439329449c54df8a | Stopped        | t2.small      | -            | View alarms  |

i-0df572e6e601fbecd (Public-ec2-Pro-Web)

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

Instance summary

Info

Instance ID

i-0df572e6e601fbecd (Public-ec2-Pro-Web)

IPv6 address

-

Hostname type

IP name: ip-10-0-0-7.ap-south-1.compute.internal

Public IPv4 address

13.126.73.237 | open address

Instance state

Running

Private IP DNS name (IPv4 only)

ip-10-0-0-7.ap-south-1.compute.internal

Private IPv4 addresses

10.0.0.7

Public IPv4 DNS

ec2-13-126-73-237.ap-south-1.compute.amazonaws.com | open address

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

We can see the public instance of Production-Network-VPC able to ping google.com mean having internet connectivity

The screenshot shows a web browser window with multiple tabs open, including 'Start Course | Intel...', 'Instances | EC2 | a...', 'Instances | EC2 | a...', 'EC2 Instance Conn...', 'IP Subnet Calculat...', and 'FREE Advanced Su...'. The active tab is 'EC2 Instance Conn...'. The browser address bar shows the URL: `ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?addressFamily=ipv4&connType=standard&instanceId=i-0df572e6e601fbee...`. The AWS console header is visible, showing the 'aws' logo, 'Services' menu, a search bar, and navigation icons for EC2, EC2 Image Builder, S3, IAM, and VPC. The user is logged in as 'prakash24' in the 'Mumbai' region. The main content area displays a terminal window with the following output:

```
ubuntu@ip-10-0-0-7:~$ ping google.com
PING google.com (142.250.77.78) 56(84) bytes of data.
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=1 ttl=54 time=1.29 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=2 ttl=54 time=1.32 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=3 ttl=54 time=1.45 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=4 ttl=54 time=1.38 ms
```

Below the terminal output, the instance details are shown: `i-0df572e6e601fbee` (Public-ec2-Pro-Web). The PublicIPs are listed as `13.126.73.237` and the PrivateIPs as `10.0.0.7`. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for 'Privacy', 'Terms', and 'Cookie preferences'.

## We can Connect to your instance i-044f18afd3046e944 (Private-ec2-Pro-App1) using public instance

The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a search bar, and various service icons (EC2, EC2 Image Builder, S3, IAM, VPC). The main content area displays a terminal window titled "System information as of Wed Sep 25 02:53:45 UTC 2024". The terminal output shows system statistics, security maintenance status, and update information. At the bottom, a summary box identifies the instance as "i-0df572e6e601fbecd (Public-ec2-Pro-Web)" and lists its public and private IP addresses.

System information as of Wed Sep 25 02:53:45 UTC 2024

```
System load: 0.24          Processes:           104
Usage of /:  20.7% of 7.57GB Users logged in:       0
Memory usage: 20%          IPv4 address for eth0: 10.0.0.157
Swap usage:  0%
```

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`

The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in `/usr/share/doc/*/copyright`.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.

To run a command as administrator (user "root"), use "`sudo <command>`".  
See "`man sudo_root`" for details.

ubuntu@ip-10-0-0-157:~\$

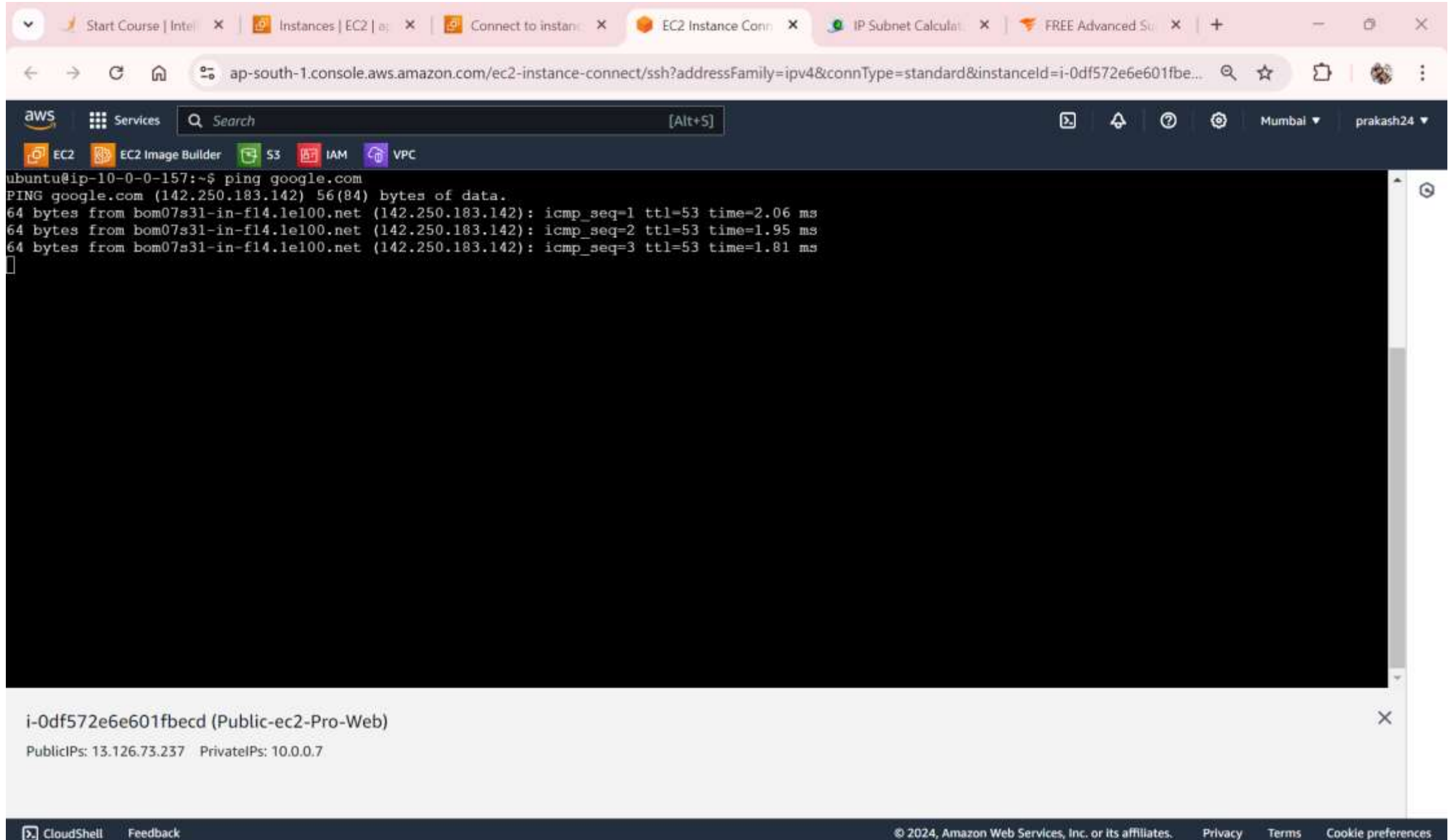
i-0df572e6e601fbecd (Public-ec2-Pro-Web)

PublicIPs: 13.126.73.237 PrivateIPs: 10.0.0.7

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# Allow inter (Private-ec2-Pro-App1) using NAT Gateway



The screenshot displays the AWS Management Console interface. At the top, the browser address bar shows the URL: `ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?addressFamily=ipv4&connType=standard&instanceId=i-0df572e6e601fbedc...`. The console header includes the AWS logo, a search bar, and navigation links for EC2, EC2 Image Builder, S3, IAM, and VPC. The main content area features a terminal window for an EC2 instance. The terminal output shows a successful ping to google.com from the instance's private IP address.

```
ubuntu@ip-10-0-0-157:~$ ping google.com
PING google.com (142.250.183.142) 56(84) bytes of data:
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=1 ttl=53 time=2.06 ms
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=2 ttl=53 time=1.95 ms
64 bytes from bom07s31-in-f14.1e100.net (142.250.183.142): icmp_seq=3 ttl=53 time=1.81 ms
```

Below the terminal window, the instance details for `i-0df572e6e601fbedc (Public-ec2-Pro-Web)` are visible, showing Public IPs: 13.126.73.237 and Private IPs: 10.0.0.7.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



We can see the public instance of Development-Network-VPC able to ping google.com mean having internet connectivity i-0ac3204f1414f0b3d (Public-ec2-Dev-Web)

Start Cour...Instances | EC2 Instan...RouteTabl...Connect to...EC2 Instan...IP Subnet...FREE Adv...+ -

← → ↻ 🏠 ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-south-1&connType=standard&instanceId=i-0ac3204f1414f0b3d... 🔍 ☆ 📁 👤

aws Services 🔍 Search [Alt+S]

EC2 EC2 Image Builder S3 IAM VPC

```
ubuntu@ip-10-0-8-222:~$ ping google.com
PING google.com (142.250.183.174) 56(84) bytes of data.
64 bytes from bom07s32-in-f14.1e100.net (142.250.183.174): icmp_seq=1 ttl=113 time=2.06 ms
64 bytes from bom07s32-in-f14.1e100.net (142.250.183.174): icmp_seq=2 ttl=113 time=2.13 ms
64 bytes from bom07s32-in-f14.1e100.net (142.250.183.174): icmp_seq=3 ttl=113 time=1.79 ms

```

i-0ac3204f1414f0b3d (Public-ec2-Dev-Web)

PublicIPs: 52.66.205.32 PrivateIPs: 10.0.8.222

## Connect to your instance i-0439329449c54df8a (Private-ec2-Dev-db) using any of these options

The screenshot displays the AWS Management Console interface. The browser's address bar shows the URL: `ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-south-1&connType=standard&instanceId=i-0ac3204f1414f0b3...`. The console header includes the AWS logo, a search bar, and navigation links for EC2, EC2 Image Builder, S3, IAM, and VPC. The main content area is a terminal window showing a shell session on an Ubuntu instance. The user has executed the command `ping google.com`, and the output shows three successful ping requests with response times of 4.54 ms, 1.80 ms, and 1.82 ms. The instance details at the bottom of the terminal window are:

```
i-0ac3204f1414f0b3d (Public-ec2-Dev-Web)
PublicIPs: 52.66.205.32 PrivateIPs: 10.0.8.222
```

The footer of the console shows the CloudShell logo, a feedback link, and the copyright notice: © 2024, Amazon Web Services, Inc. or its affiliates. Links for Privacy, Terms, and Cookie preferences are also present.

# A Perring Connection to connect both of VPC Production Network and Development Network

Start Cour...

PeeringCo...

EC2 Instan...

vpcs | VPC

Instances

IP Subnet

FREE Adv...

amazon w...

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#PeeringConnectionDetails:vpcPeeringConnectionId=pcx-0ef0...

aws Services Search [Alt+S]

EC2 EC2 Image Builder S3 IAM VPC

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

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

A VPC peering connection pcx-0ef0b456008a6c5e5 / my-pc-prod-dev-01 has been requested.

VPC > Peering connections > pcx-0ef0b456008a6c5e5

pcx-0ef0b456008a6c5e5 / my-pc-prod-dev-01

Pending acceptance

You can accept or reject this peering connection request using the 'Actions' menu. You have until Wednesday 2 October 2024 at 08:59:11 GMT+5:30 to accept or reject the request, otherwise it expires.

Details Info

Requester owner ID

654654393526

Peering connection ID

pcx-0ef0b456008a6c5e5

Status

Pending Acceptance by 654654393526

Expiration time

Wednesday 2 October 2024 at 08:59:11 GMT+5:30

Acceptor owner ID

654654393526

Requester VPC

vpc-0f489e02b770223dd / Production-Network-VPC-vpc

Requester CIDRs

10.0.0.0/24

Requester Region

Mumbai (ap-south-1)

VPC Peering connection ARN

arn:aws:ec2:ap-south-1:654654393526:vpc-peering-connection/pcx-0ef0b456008a6c5e5

Acceptor VPC

vpc-09abc9cb7e8f6f76f / Development-Network-VPC-vpc

Acceptor CIDRs

-

Acceptor Region

Mumbai (ap-south-1)

DNS

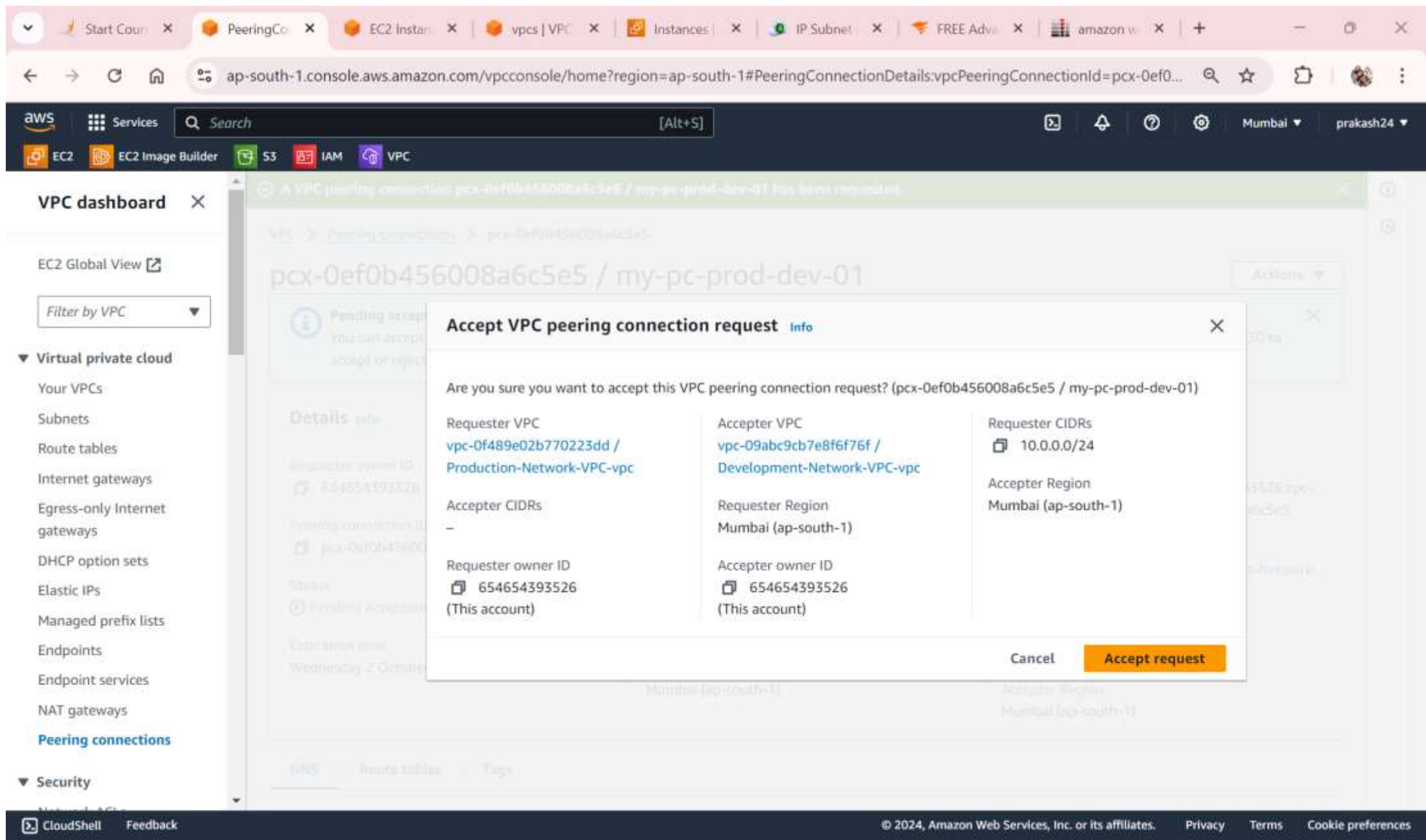
Route tables

Tags

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# Accepting a Pending Connection to by request VPC





## Defining a routes to communicate both DB Private subnet of both VPC

The screenshot shows the AWS Management Console interface for editing routes in a VPC. The browser tabs at the top include 'Inbox (721) - ratre.raj@g...', 'Instances | EC2 | ap-south-1', 'EditRoutes | VPC Console', 'PeeringConnectionDetails', and 'Start Course | Intellipaat'. The address bar shows the URL: `ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditRoutes:RouteTableId=rtb-09c1ddd0c3ef2c11f`.

The console header includes the AWS logo, a 'Services' menu, a search bar, and a navigation bar with icons for EC2, EC2 Image Builder, S3, IAM, and VPC. The user's location is set to Mumbai, and the user name is prakash24.

The breadcrumb navigation shows: `VPC > Route tables > rtb-09c1ddd0c3ef2c11f > Edit routes`.

### Edit routes

| Destination | Target             | Status | Propagated |        |
|-------------|--------------------|--------|------------|--------|
| 10.0.0.0/24 | local              | Active | No         |        |
| 10.2.0.0/24 | Peering Connection | Active | No         | Remove |

Buttons: Add route, Cancel, Preview, Save changes

Footer: CloudShell, Feedback, © 2024, Amazon Web Services, Inc. or its affiliates. Privacy, Terms, Cookie preferences

## Defining a routes to communicate both DB Private subnet of both VPC

The screenshot shows the AWS Management Console interface for editing a VPC route table. The breadcrumb navigation indicates the path: VPC > Route tables > rtb-048c8692d0a733bc3 > Edit routes. The main heading is "Edit routes".

| Destination | Target             | Status | Propagated |        |
|-------------|--------------------|--------|------------|--------|
| 10.2.0.0/24 | local              | Active | No         |        |
| 10.0.0.0/24 | Peering Connection | Active | No         | Remove |
| 0.0.0.0/0   | NAT Gateway        | Active | No         | Remove |

At the bottom of the table, there is an "Add route" button. At the bottom right of the console, there are three buttons: "Cancel", "Preview", and "Save changes".

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

We can see we can able to ping the private instance of Dev db subnet by using Private instance of production Db Subnet

Instances (1/4) info

Find Instance by attribute or tag (case-sensitive)

Instance state: running

| Name               | Instance ID         | Instance state | Instance type | Status check      |
|--------------------|---------------------|----------------|---------------|-------------------|
| Public-ec2-Pro-Web | i-0df572e6e01fbecd  | Running        | t2.micro      | 2/2 checks passed |
| Private-ec2-Pro-db | i-0c5a809e558facef6 | Running        | t2.nano       | 2/2 checks passed |
| Private-ec2-dev-db | i-06d4bd8a49a17ab4c | Running        | t2.small      | 2/2 checks passed |
| Public-ec2-dev-Web | i-02bad2a0fb1115828 | Running        | t2.small      | 2/2 checks passed |

**i-06d4bd8a49a17ab4c (Private-ec2-dev-db)**

Instance summary

Instance ID: i-06d4bd8a49a17ab4c (Private-ec2-dev-db)

Public IPv4 address: -

Private IPv4 addresses: 10.2.0.141

Instance state: Running

Private IP DNS name (IPv4 only): ip-10-2-0-141.ap-south-1.compute.internal

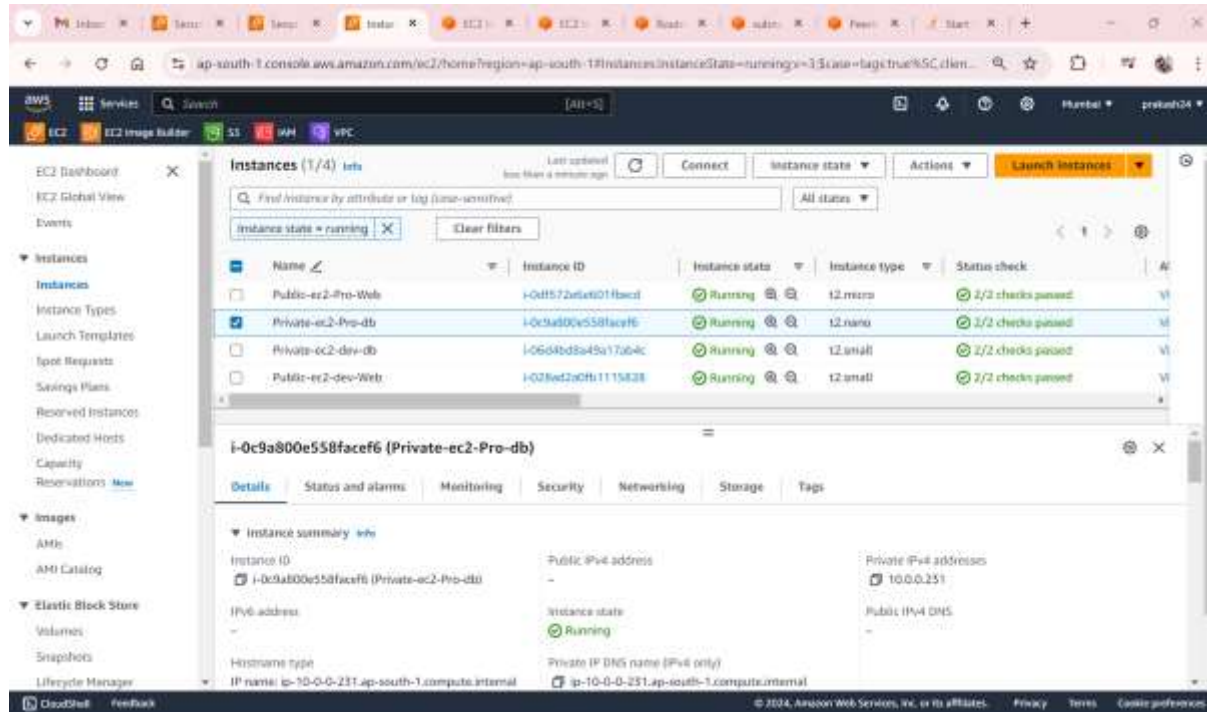
Instance type: t2.small

```
ubuntu@ip-10-2-0-231:~$ ping 10.2.0.141
PING 10.2.0.141 (10.2.0.141) 56(84) bytes of data:
64 bytes from 10.2.0.141: icmp_seq=1 ttl=64 time=0.488 ms
64 bytes from 10.2.0.141: icmp_seq=2 ttl=64 time=6.73 ms
64 bytes from 10.2.0.141: icmp_seq=3 ttl=64 time=0.485 ms
64 bytes from 10.2.0.141: icmp_seq=4 ttl=64 time=0.533 ms
64 bytes from 10.2.0.141: icmp_seq=5 ttl=64 time=0.516 ms
^C
```

**i-0df572e6e01fbecd (Public-ec2-Pro-Web)**

PublicPis: 65.1.65.149 - PrivatePis: 10.0.0.7

We can see we can able to ping the Private instance of production Db Subnet by using private instance of Dev db subnet



The screenshot shows the AWS Management Console for the 'ap-south-1' region. The 'Instances' page is active, displaying a list of four EC2 instances. The instance 'Private-ec2-Pro-db' is selected, and its details are shown in the lower pane. The instance is running and has a private IP address of 10.0.0.231.

| Name               | Instance ID         | Instance state | Instance type | Status check      |
|--------------------|---------------------|----------------|---------------|-------------------|
| Public-ec2-Pro-Web | i-0d572aef01fbac1   | Running        | t2.micro      | 2/2 checks passed |
| Private-ec2-Pro-db | i-0c9a800e558facef6 | Running        | t2.nano       | 2/2 checks passed |
| Private-ec2-dev-db | i-06d8d8a45a170b4c  | Running        | t2.small      | 2/2 checks passed |
| Public-ec2-dev-Web | i-028ad2a0fb1115828 | Running        | t2.small      | 2/2 checks passed |

**i-0c9a800e558facef6 (Private-ec2-Pro-db)**

**Instance summary**

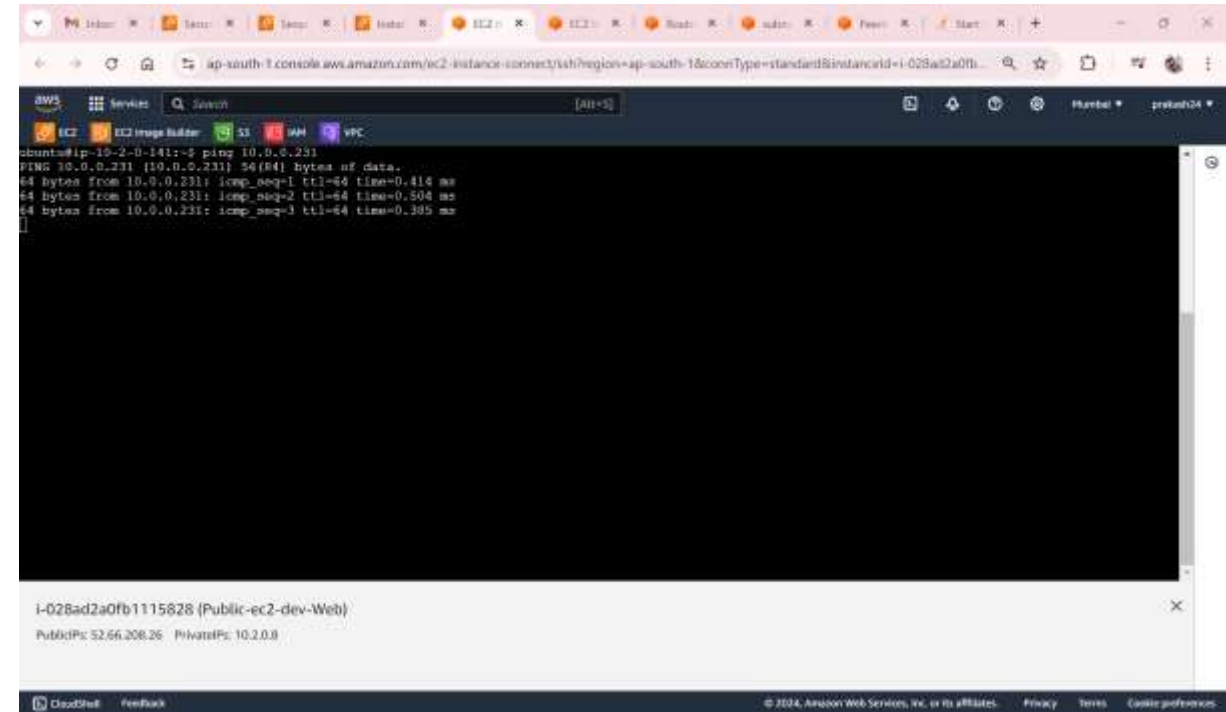
| Instance ID                              | Public IPv4 address | Private IPv4 addresses |
|--|---------------------|------------------------|
| i-0c9a800e558facef6 (Private-ec2-Pro-db) | -                   | 10.0.0.231             |

**Instance state**

Running

**Private IP DNS name (IPv4 only)**

ip-10-0-0-231.ap-south-1.compute.internal



The screenshot shows the AWS CloudShell interface. A terminal window displays the output of a ping command from the 'Public-ec2-dev-Web' instance to the 'Private-ec2-Pro-db' instance. The command is 'ping 10.0.0.231' and the output shows successful ping results.

```
ubuntu@ip-10-2-0-141:~$ ping 10.0.0.231
PING 10.0.0.231 (10.0.0.231): 56(84) bytes of data:
64 bytes from 10.0.0.231: icmp_seq=1 ttl=64 time=0.414 ms
64 bytes from 10.0.0.231: icmp_seq=2 ttl=64 time=0.504 ms
64 bytes from 10.0.0.231: icmp_seq=3 ttl=64 time=0.395 ms
```

**i-028ad2a0fb1115828 (Public-ec2-dev-Web)**

PublicIPs: 52.66.208.26 PrivateIPs: 10.2.0.8



In SG allow inbound rule ping using ALL ICMP IP4 by private production db

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-06d41...

aws Services Search [Alt+S] Mumbai prakash24

EC2 EC2 Image Builder S3 IAM VPC

EC2 > Security Groups > sg-06d412d07398def19 - private-sg-pro-db > Edit inbound rules

Edit inbound rules Info

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

Inbound rules Info

| Security group rule ID | Type Info       | Protocol Info | Port range Info | Source Info | Description - optional Info |        |
|------------------------|-----------------|---------------|-----------------|-------------|-----------------------------|--------|
| sgr-08e0dfe2faff214b3  | All ICMP - IPv4 | ICMP          | All             | Custom      | <div>10.20.128/28</div>     | Delete |
| sgr-0ccc04dad5e05a6c6  | SSH             | TCP           | 22              | Custom      | <div>0.0.0.0/0</div>        | Delete |

Add rule

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Preview changes Save rules

**In SG allow inbound rule ping using ALL ICMP IP4 by private development db**

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-00346...

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

Mumbaiprakash24

EC2 > Security Groups > sg-003461bb55aa26230 - private-sg-dev-db > Edit inbound rules

Edit inbound rules

Info

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

Inbound rules

Info

| Security group rule ID | Type            | Protocol | Port range | Source | Description - optional                                    |        |
|------------------------|-----------------|----------|------------|--------|---|--------|
|                        | Info            | Info     | Info       | Info   | Info  |        |
| sgr-057e8db0e5beb91d3  | SSH             | TCP      | 22         | Custom | <div><div></div><div>0.0.0.0/0</div><div></div></div>     | Delete |
| sgr-0f43ca3d403d388cc  | All ICMP - IPv4 | ICMP     | All        | Custom | <div><div></div><div>10.0.0.224/27</div><div></div></div> | Delete |

Add rule

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel

Preview changes

Save rules

## Using NACL we having allow the all traffic

The screenshot shows the AWS Management Console interface for editing inbound rules for a Network ACL. The breadcrumb navigation indicates the path: VPC > Network ACLs > acl-0080075863857ba94 > Edit inbound rules. The main heading is "Edit inbound rules" with an "Info" link. Below the heading, a note states: "Inbound rules control the incoming traffic that's allowed to reach the VPC."

| Rule number <a href="#">Info</a> | Type <a href="#">Info</a> | Protocol <a href="#">Info</a> | Port range <a href="#">Info</a> | Source <a href="#">Info</a> | Allow/Deny <a href="#">Info</a> |                         |
|----------------------------------|---------------------------|-------------------------------|---------------------------------|-----------------------------|---------------------------------|-------------------------|
| 100                              | All traffic ▼             | All ▼                         | All                             | 0.0.0.0/0                   | Allow ▼                         | <button>Remove</button> |
| *                                | All traffic ▼             | All ▼                         | All                             | 0.0.0.0/0                   | Deny ▼                          |                         |

At the bottom of the table area, there are two buttons: "Add new rule" and "Sort by rule number". At the bottom right of the console, there are three buttons: "Cancel", "Preview changes", and "Save changes".

The footer of the console includes "CloudShell", "Feedback", and copyright information: "© 2024, Amazon Web Services, Inc. or its affiliates." along with links for "Privacy", "Terms", and "Cookie preferences".