

Assignment #2 VPC, EC2 and RDS

1

Assignment #3VPC Peering & IAM Implementation

Darpankumar Jayantilal Patel,

8868275

Joel Belanger,

Nikolas Mader,

INFO2350-25W-Sec1

Amarpreet Singh

2025-03-12

Assignment #2 VPC, EC2 and RDS

2

Table of Contents

Table of Contents	2
Assignment #3 VPC Peering & IAM Implementation	3
Section 1: Practical Work	3
Task 1: VPC Peering - Practical Implementation	3
Screenshots.....	3
Screenshots.....	4

Assignment #3 VPC Peering & IAM Implementation

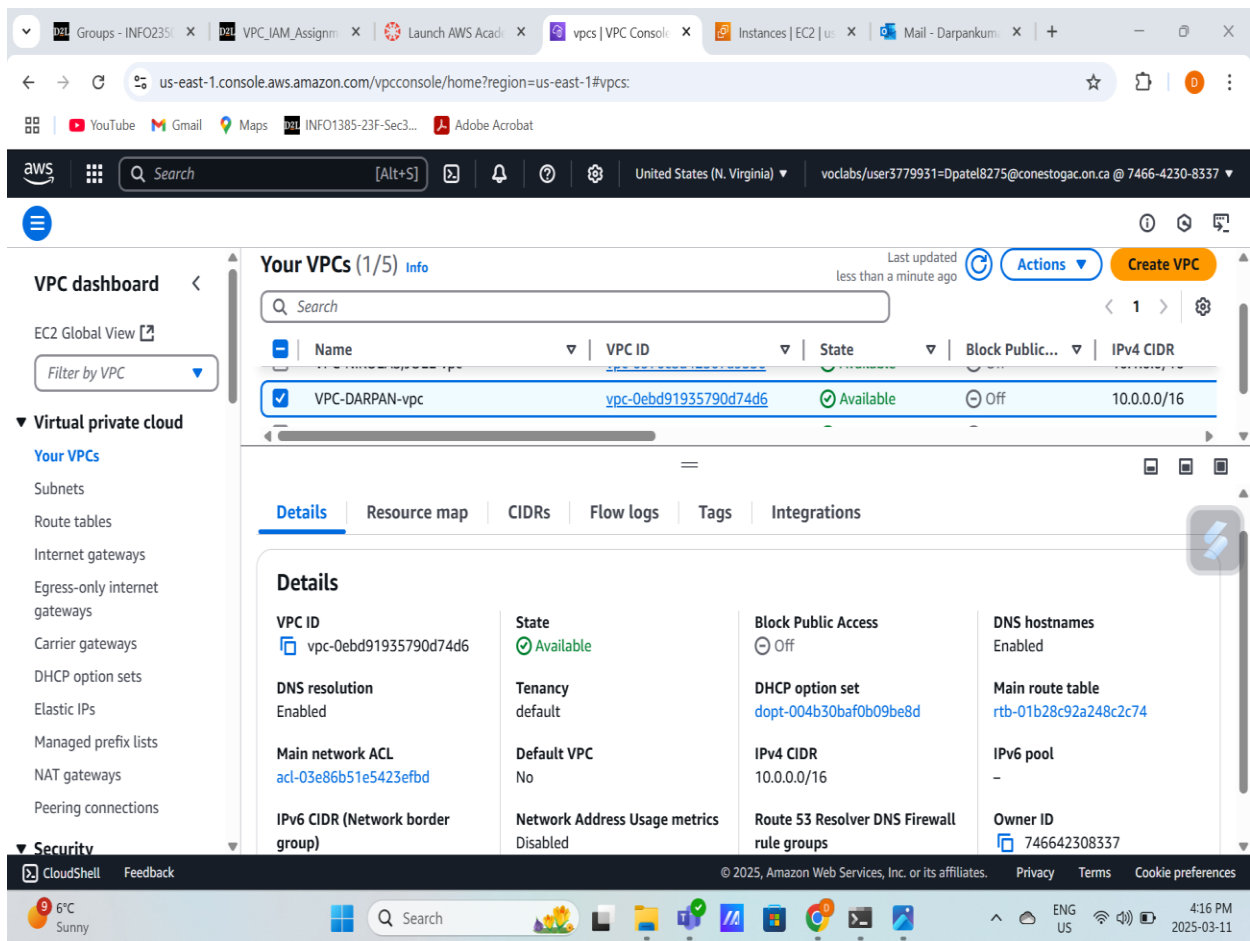
Section 1: Practical Work

Task 1: VPC Peering - Practical Implementation

Step 1: Created Two Separate VPCs

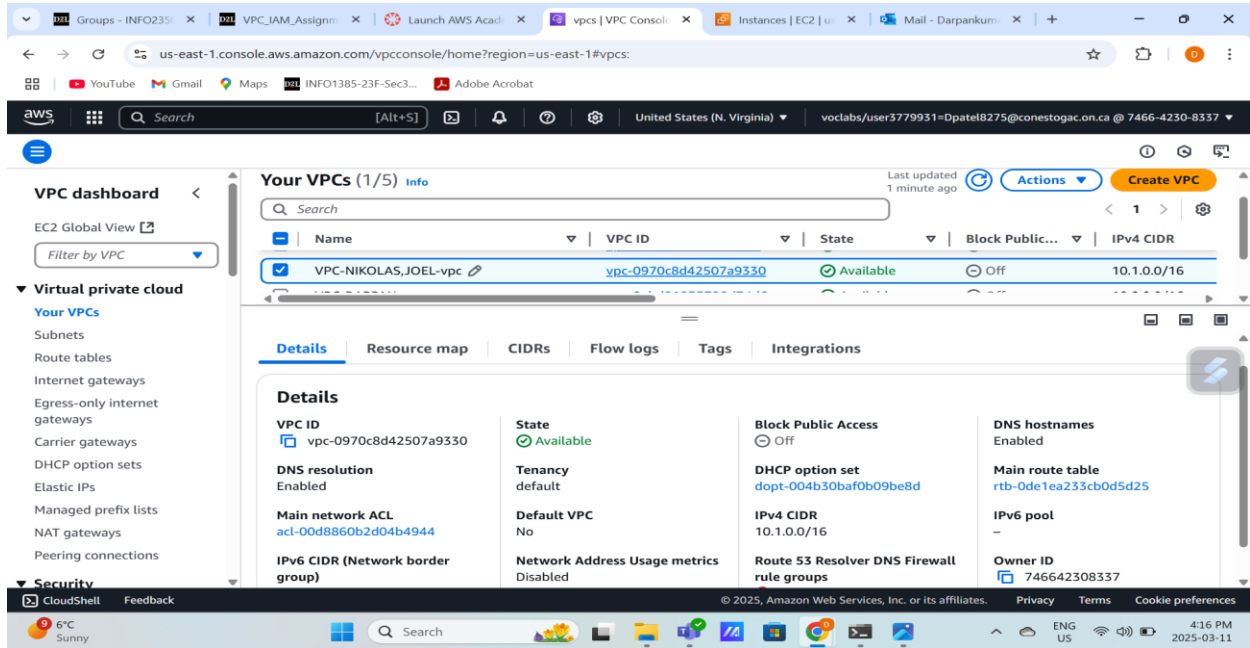
- VPC-DARPAN: 10.0.0.0/16
- VPC-NIKOLAS, JOEL: 10.1.0.0/16

Screenshots



Assignment #2 VPC, EC2 and RDS

4

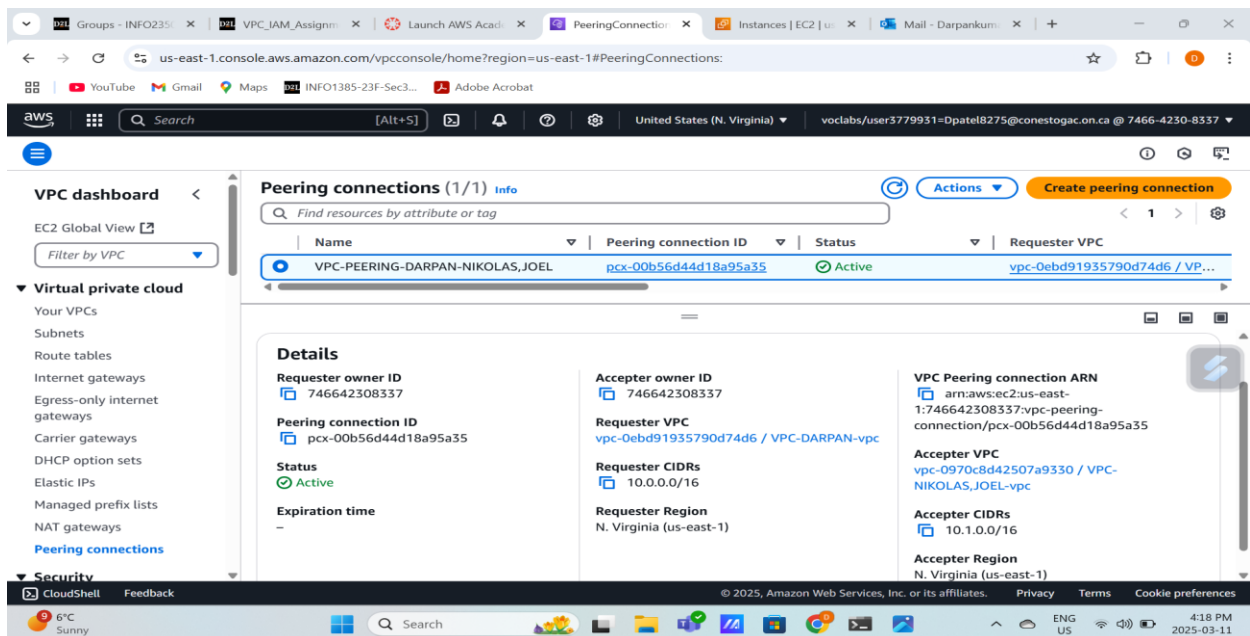


Step 2: Establish VPC Peering.

I established a VPC Peering Connection from **VPC-DARPAN** to **VPC-NIKOLAS, JOEL**.

The peer accepted the request via the AWS console.

Screenshots



Assignment #2 VPC, EC2 and RDS

5

The screenshot shows the AWS VPC console for a peering connection with ID `pcx-00b56d44d18a95a35`. The connection is active and established between two VPCs in the `us-east-1` region.

Field	Value
Requester owner ID	746642308337
Requester VPC	vpc-0ebd91935790d74d6 / VPC-DARPAN-vpc
Requester CIDRs	10.0.0.0/16
Requester Region	N. Virginia (us-east-1)
Accepter owner ID	746642308337
Accepter VPC	vpc-0970c8d42507a9330 / VPC-NIKOLAS,JOEL-vpc
Accepter CIDRs	10.1.0.0/16
Accepter Region	N. Virginia (us-east-1)
VPC Peering connection ARN	arn:aws:ec2:us-east-1:746642308337:vpc-peering-connection/pcx-00b56d44d18a95a35
Status	Active
Expiration time	-

DNS settings

Requester VPC ([vpc-0ebd91935790d74d6 / VPC-DARPAN-vpc](#))

[Edit DNS settings](#)

The screenshot shows the DNS settings for the VPC peering connection. Both DNS resolution options are currently disabled.

DNS settings

[Edit DNS settings](#)

Requester VPC ([vpc-0ebd91935790d74d6 / VPC-DARPAN-vpc](#))

Info

Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses

Disabled

Accepter VPC ([vpc-0970c8d42507a9330 / VPC-NIKOLAS,JOEL-vpc](#))

Info

Allow requester VPC to resolve DNS of hosts in accepter VPC to private IP addresses

Disabled

Assignment #2 VPC, EC2 and RDS

6

Step 3: Route Tables Are Updated

1. **VPC-DARPAN** Route Table has been modified.

Destination: 10.1.0.0/16

Target: Peering Connection

Screenshots:

The screenshot displays the AWS Management Console interface for the route table `rtb-09a2ea7d17447ee16 / VPC-DARPAN-rtb-public`. The left sidebar shows navigation options under 'Virtual private cloud' and 'Security'. The main content area shows the route table details and a list of routes.

Details Info

Route table ID rtb-09a2ea7d17447ee16	Main No	Explicit subnet associations subnet-0bac812d238c50814 / VPC-DARPAN-subnet-public1-us-east-1a	Edge associations -
VPC vpc-0ebd91935790d74d6 VPC-DARPAN-vpc	Owner ID 746642308337		

Routes (3)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-032cbcb5a4b42339f	Active	No
10.0.0.0/16	local	Active	No
10.1.0.0/16	pcx-00b56d44d18a95a35	Active	No

Assignment #2 VPC, EC2 and RDS

7

2. **VPC-NIKOLAS, JOEL** Route Table has been modified.

Destination: 10.0.0.0/16

Target: Peer Connection

Screenshots:

The screenshot displays the AWS Management Console interface for a Route Table. The browser address bar shows the URL: `us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-095a312e42e0a1a53`. The console header includes the AWS logo, a search bar, and the current region (United States (N. Virginia)). The breadcrumb navigation shows: `VPC > Route tables > rtb-095a312e42e0a1a53`. The main content area is titled `rtb-095a312e42e0a1a53 / VPC-NIKOLAS,JOEL-rtb-public`. On the left, a navigation sidebar lists various VPC resources, with 'Route tables' selected. The 'Details' section provides the following information:

Property	Value
Route table ID	rtb-095a312e42e0a1a53
Main	No
Explicit subnet associations	subnet-04eb43adf7707cef2 / VPC-NIKOLAS,JOEL-subnet-public1-us-east-1a
Edge associations	-
VPC	vpc-0970c8d42507a9330 VPC-NIKOLAS,JOEL-vpc
Owner ID	746642308337

Below the details, there are tabs for 'Routes', 'Subnet associations', 'Edge associations', 'Route propagation', and 'Tags'. The 'Routes' tab is active, showing a list of 3 routes. A search bar for routes is present above the table. The routes table is as follows:

Destination	Target	Status	Propagated
0.0.0.0/0	igw-09193b9c9a23a638e	Active	No
10.0.0.0/16	pcx-00b56d44d18a95a35	Active	No
10.1.0.0/16	local	Active	No

The footer of the console shows the copyright notice: © 2025, Amazon Web Services, Inc. or its affiliates. The system tray at the bottom of the image shows the date and time: 4:22 PM, 2025-03-11.

Assignment #2 VPC, EC2 and RDS

8

Step 4: Update Security Groups

In **VPC-DARPAN**, change the security group to accept inbound traffic from **10.1.0.0/16**.

Screenshots:

The screenshot shows the AWS Management Console interface for a Security Group. The breadcrumb navigation is **VPC > Security Groups > sg-0c6b8defb8b707c21 - SG FOR VPC1**. The main content area displays the following details:

- Security group name:** SG FOR VPC1
- Security group ID:** sg-0c6b8defb8b707c21
- Description:** ALLOW TRAFFIC FROM VPC2
- VPC ID:** vpc-0ebd91935790d74d6
- Owner:** 746642308337
- Inbound rules count:** 2 Permission entries
- Outbound rules count:** 1 Permission entry

Below the details, there are tabs for **Inbound rules**, **Outbound rules**, **Sharing - new**, **VPC associations - new**, and **Tags**. The **Inbound rules** tab is active, showing a table with one rule:

Name	Security group rule ID	IP version	Type	Protocol
-	sgr-0e0438af8f7a61fb6	IPv4	All traffic	All

The screenshot shows the AWS Management Console interface for the same Security Group, but viewed from the **EC2** console. The breadcrumb navigation is **EC2 > Security Groups > sg-0c6b8defb8b707c21 - SG FOR VPC1**. The details section is identical to the VPC console view. The **Inbound rules** tab is active, showing a table with one rule:

Type	Protocol	Port range	Source	Description
All traffic	All	All	10.1.0.0/16	ALLOW TRAFFIC FROM

Assignment #2 VPC, EC2 and RDS

9

In VPC-NIKOLAS, JOEL, change the security group to accept inbound traffic from 10.0.0.0/16.

Screenshots:

The screenshot shows the AWS VPC console for the security group 'sg-078481e1ac5dff14e - SG FOR VPC2'. The 'Details' section includes:

- Security group name:** SG FOR VPC2
- Security group ID:** sg-078481e1ac5dff14e
- Description:** ALLOW TRAFFIC FROM VPC1
- VPC ID:** vpc-0970c8d42507a9330
- Owner:** 746642308337
- Inbound rules count:** 2 Permission entries
- Outbound rules count:** 1 Permission entry

The 'Inbound rules' tab is active, showing a table with one rule:

Name	Security group rule ID	IP version	Type	Protocol
-	sgr-04ed851e49065ba61	IPv4	All traffic	All

The screenshot shows the AWS EC2 console for the security group 'sg-078481e1ac5dff14e - SG FOR VPC2'. The 'Details' section includes:

- Security group name:** SG FOR VPC2
- Security group ID:** sg-078481e1ac5dff14e
- Description:** ALLOW TRAFFIC FROM VPC1
- VPC ID:** vpc-0970c8d42507a9330
- Owner:** 746642308337
- Inbound rules count:** 2 Permission entries
- Outbound rules count:** 1 Permission entry

The 'Inbound rules' tab is active, showing a table with one rule:

Type	Protocol	Port range	Source	Description
All traffic	All	All	10.0.0.0/16	ALLOW TRAFFIC FROM

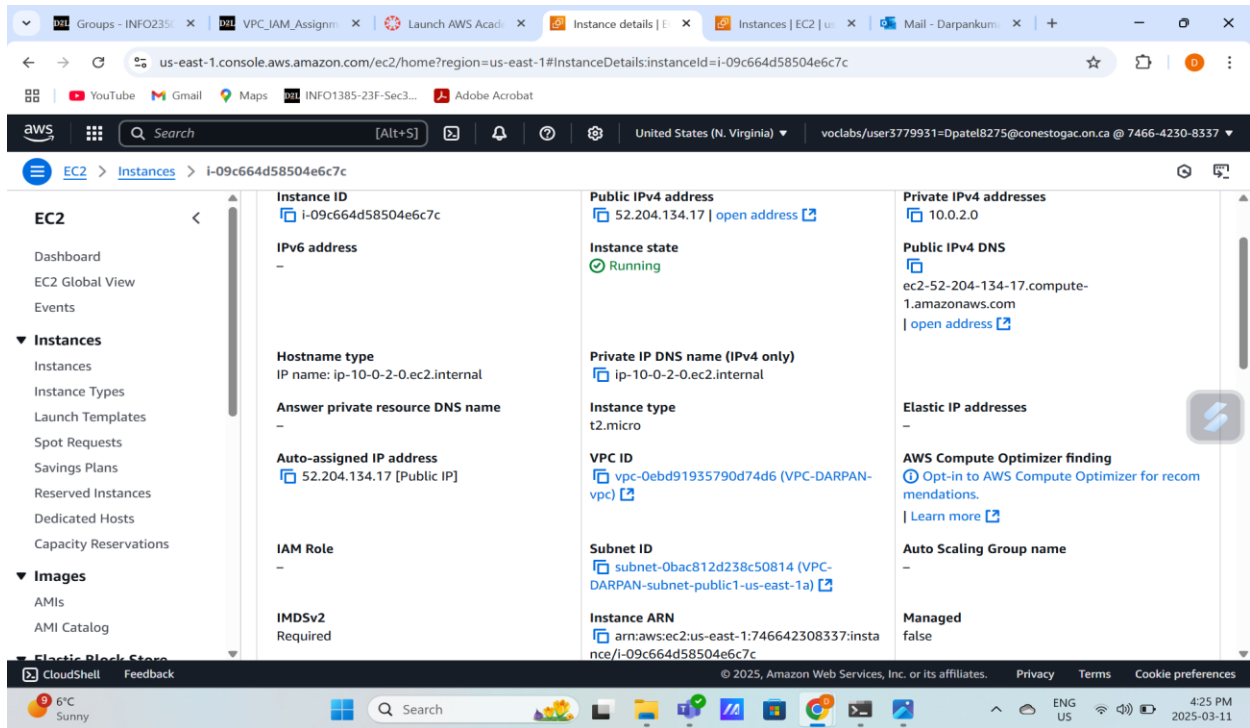
Assignment #2 VPC, EC2 and RDS

10

Step 5: Launched EC2 instances.

1. I launched an EC2 instance in **VPC-DARPAN** (Amazon Linux, t2.micro).
2. I launched another EC2 instance in **VPC-NIKOLAS, JOEL**.
3. I verified that each instance gets a private IP address.

Screenshots:



Observations:

- **VPC peering enables safe private communication between two independent VPCs.**
- **To permit traffic between VPCs, the route table must be updated properly.**
- **Security Groups must be set to allow inbound and outbound traffic.**
- **IAM enables granular access control, hence boosting security in the AWS environment.**
- **IAM Policies must be carefully assigned to guarantee that users and roles receive only the essential permissions.**