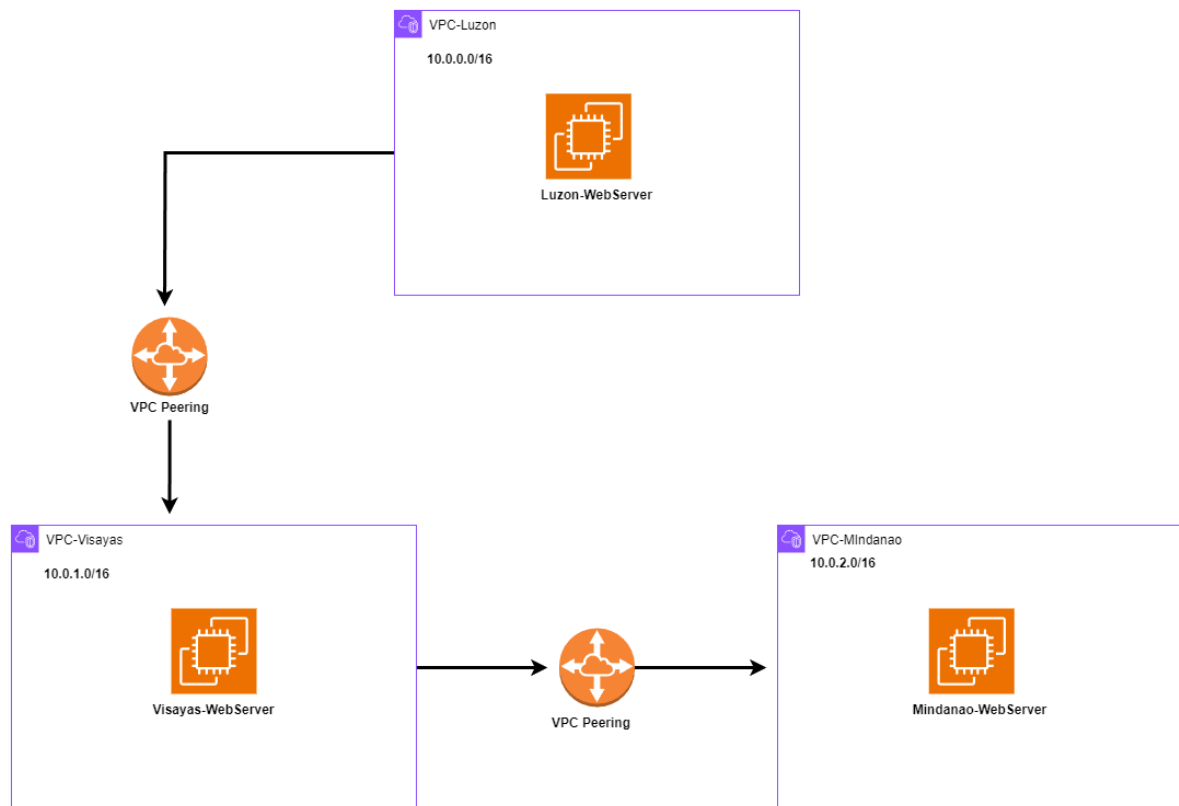


## Guided Lab: Setting up VPC Peering

### Description

Amazon Virtual Private Cloud (VPC) Peering allows private networking connections between different VPCs, enabling resources in separate VPCs to communicate as if they are within the same network. This lab will guide you through the process of creating and testing VPC peering connections using three distinct VPCs, each hosting an Amazon EC2 instance. This setup will help you understand the network connectivity and security configurations necessary for VPC peering.



### Prerequisites

This lab assumes you have basic knowledge of IP addressing & network subnets, and familiarity with AWS core services like EC2 (Elastic Compute Cloud).

If you find any gaps in your knowledge, consider taking the following lab:

- Creating a Custom Virtual Private Cloud (VPC) from scratch
- Creating an Amazon EC2 instance (Linux)
- Setting up a Web server on an EC2 instance

### Objectives

In this lab, you will:

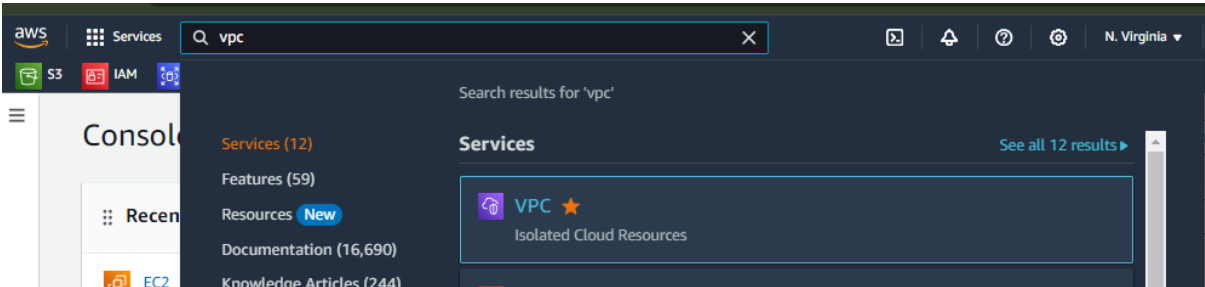
- Learn how to configure VPC peering between multiple VPCs.

- Demonstrate inter-VPC communication through EC2 instances.
- Understand the security and routing implications of VPC peering.

[Subscribe to access AWS PlayCloud Labs](#)

Lab Steps

Preparing your environment



- 
- 
- 

Your VPCs (4) Info						
Last updated less than a minute ago						
Actions						
Create VPC						
Search						
< 1 >						
<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	
<input type="checkbox"/>	-	<a href="#">vpc-0678b78645a8bbea6</a>	Available	192.168.5.0/26	-	
<input type="checkbox"/>	VPC-Luzon	<a href="#">vpc-0225d1915f2848ef9</a>	Available	10.0.0.0/16	-	
<input type="checkbox"/>	VPC-Visayas	<a href="#">vpc-0b1e659facd1a2160</a>	Available	10.1.0.0/16	-	
<input type="checkbox"/>	VPC-Mindanao	<a href="#">vpc-0ba5da60375a7f1f8</a>	Available	10.2.0.0/16	-	

- 
- 
- 

Subnets (6) Info						
Last updated 1 minute ago						
Actions						
Create subnet						
Find resources by attribute or tag						
< 1 >						
<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	
<input type="checkbox"/>	-	<a href="#">subnet-027fdf5b1620e47c2</a>	Available	<a href="#">vpc-0678b78645a8bbea6</a>	192.168.5.32/28	
<input type="checkbox"/>	-	<a href="#">subnet-010a5c8d7ad1535f8</a>	Available	<a href="#">vpc-0678b78645a8bbea6</a>	192.168.5.16/28	
<input type="checkbox"/>	-	<a href="#">subnet-09992b4a60665de...</a>	Available	<a href="#">vpc-0678b78645a8bbea6</a>	192.168.5.0/28	
<input type="checkbox"/>	subnet-mindanao	<a href="#">subnet-0a9fd9064eb5dbcb9</a>	Available	<a href="#">vpc-0ba5da60375a7f1f8</a>   <a href="#">VPC-Mindanao</a>	10.2.1.0/24	
<input type="checkbox"/>	subnet-visayas	<a href="#">subnet-0f530789775ff68df</a>	Available	<a href="#">vpc-0b1e659facd1a2160</a>   <a href="#">VPC-Visayas</a>	10.1.1.0/24	
<input type="checkbox"/>	subnet-luzon	<a href="#">subnet-0754bb4c4b2cbb85b</a>	Available	<a href="#">vpc-0225d1915f2848ef9</a>   <a href="#">VPC-Luzon</a>	10.0.1.0/24	

- 
- 
- 

Internet gateways (4) Info

Q Search

< 1 > ⚙

☐

Name

☐

-

☐

my-internet-gateway-luzon

☐

my-internet-gateway-visayas

☐

my-internet-gateway-mindanao

igw-036eed36a30098d5c

igw-04b9916f14f29d52d

igw-0376a047e1104f582

igw-0b4ba5d845414c66d

Attached

Attached

Attached

Attached

vpc-0678b78645a8bbea6

vpc-0225d1915f2848ef9 | VPC-Luzon

vpc-0b1e659facd1a2160 | VPC-Visayas

vpc-0ba5da60375a7f1f8 | VPC-Mindanao

654

654

654

654

Route tables (4) Info

Last updated less than a minute ago

Q Find resources by attribute or tag

< 1 > ⚙

☐

Name

☐

-

☐

-

☐

-

☐

-

rtb-0db91ab854dec43e1

rtb-0c40c9ef2ddc7de5b

rtb-00e86f0c967148fa1

rtb-06a1b115fa983f0e6

3 subnets

-

-

-

-

-

-

-

Yes

Yes

Yes

Yes

vpc-0678b78645a8bbea6

vpc-08ed3326dbeaf7eb2 | VPC-Mindanao

vpc-09a2e1c78341c7bbd | VPC-Visayas

vpc-0d31a487a1843a80c | VPC-Luzon

- - 
  -

## Edit routes

### Route 1

Destination  
10.0.0/16

Target

local

Status

✓ Active

Q local X

Propagated

No

### Route 2

Destination

Q 0.0.0/0 X

Target

Internet Gateway

Status

✓ Active

Q igw-04b9916f14f29d52d X

Propagated

No

Remove

Add route

Cancel

Preview

Save changes

✓ Updated routes for rtb-03902dd95bedd1b21 successfully

► Details

VPC > Route tables > rtb-03902dd95bedd1b21

## rtb-03902dd95bedd1b21

Actions

### Details Info

Route table ID

rtb-03902dd95bedd1b21

Main

Yes

Explicit subnet associations

-

Edge associations

-

VPC

vpc-0225d1915f2848ef9 |  
VPC-Luzon

Owner ID

654654537193

Routes

Subnet associations

Edge associations

Route propagation

Tags

### Routes (2)

Both

Edit routes

Q Filter routes

< 1 > ⚙

Destination	Target	Status	Propagated
0.0.0/0	<a href="#">igw-04b9916f14f29d52d</a>	✓ Active	No
10.0.0/16	local	✓ Active	No

Updated routes for rtb-03cb14a50dd9cf6e7 successfully

Details

VPC > Route tables > rtb-03cb14a50dd9cf6e7

rtb-03cb14a50dd9cf6e7

Actions

Details Info

Route table ID

rtb-03cb14a50dd9cf6e7

VPC

vpc-0b1e659facd1a2160 | VPC-Visayas

Main

Yes

Owner ID

654654537193

Explicit subnet associations

-

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both

Edit routes

Filter routes

< 1 >

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0376a047e1104f582	Active	No
10.1.0.0/16	local	Active	No

•

○

Updated routes for rtb-0793950943c439f6b successfully

Details

VPC > Route tables > rtb-0793950943c439f6b

rtb-0793950943c439f6b

Actions

Details Info

Route table ID

rtb-0793950943c439f6b

VPC

vpc-0ba5da60375a7f1f8 | VPC-Mindanao

Main

Yes

Owner ID

654654537193

Explicit subnet associations

-

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both

Edit routes

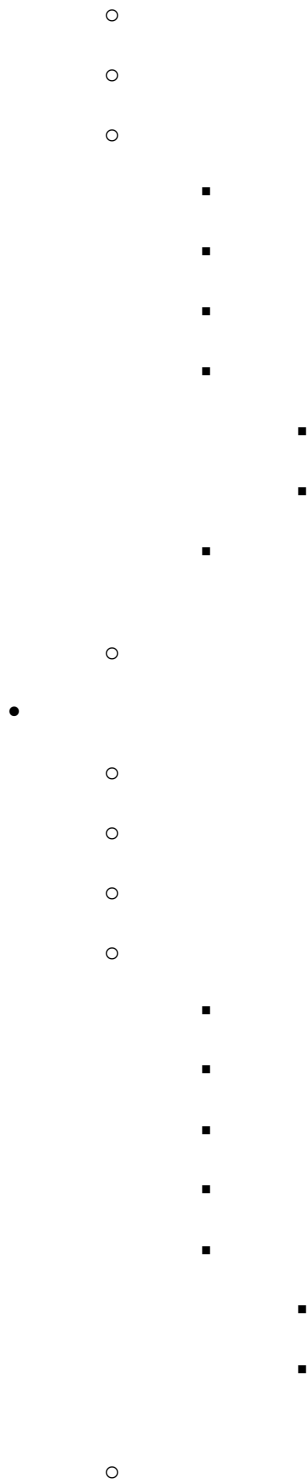
Filter routes

< 1 >

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0b4ba5d845414c66d	Active	No
10.2.0.0/16	local	Active	No

•

○



Instances (3) [Info](#)

Connect

Instance state ▾

Actions ▾

Launch instances

Running ▾

< 1 >

<input type="checkbox"/>	Name	Instance ID	Instance state	Instanc...	Status check	Alarm status	Availabi...
<input type="checkbox"/>	Mindanao-WebServer	i-006fd1de...	Running	t2.micro	2/2 checks pa	<a href="#">View alarms</a>	us-east-1c
<input type="checkbox"/>	Luzon-WebServer	i-01cc52e7...	Running	t2.micro	2/2 checks pa	<a href="#">View alarms</a>	us-east-1d
<input type="checkbox"/>	Visayas-WebServer	i-0954fb7f...	Running	t2.micro	2/2 checks pa	<a href="#">View alarms</a>	us-east-1b

The EC2 instances in the three VPCs are not connected yet because each VPC is isolated by default, with no routes or permissions set up to allow them to communicate with each other. Without establishing VPC peering connections and configuring the necessary routing and security settings, these instances remain isolated within their own separate networks.

To check this, follow the following steps:

- Please note that you can choose any Web-Server you want to connect with via SSH to do this step.***

[EC2](#) > [Instances](#) > [i-01cc52e724d78b741](#) > Connect to instance

## Connect to instance Info

Connect to your instance i-01cc52e724d78b741

### EC2 Instance Connect Session Manager

Instance ID  
 i-01cc52e724d78b741 (Luzon-W...)

- Open an SSH client.
- Locate your private key file. The default location is `C:\Users\<username>\Downloads`.
- Run this command, if necessary:  
 `chmod 400 "my-key-pair.pem"`
- Connect to your instance using the following command:  
 `ssh -i my-key-pair.pem ec2-user@ip-10-0-1-70`

Command copied

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

```
ec2-user@ip-10-0-1-70:~$ cd Downloads/  
nEIL@So1 MINGW64 ~/Downloads$ ssh -i "test.pem" ec2-user@192.168.5.27  
ssh: connect to host 192.168.5.27 port 22: Connection timed out  
  
nEIL@So1 MINGW64 ~/Downloads$ ssh -i "my-key-pair.pem" ec2-user@52.91.130.103  
The authenticity of host '52.91.130.103 (52.91.130.103)' can't be established.  
ED25519 key fingerprint is SHA256:rvcisNtX8boTtwGc2MuCFvgP04P/69JIjXwgZvtSaw.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '52.91.130.103' (ED25519) to the list of known hosts.  
#_  
+###_ Amazon Linux 2023  
~~~|#####  
~~~~~|####\  
~~~~~||##|\_____|  
~~~~~|V/'->  
~~~~~|_\_'<-__/_\___|  
~~~~~|_/'_<-__/_\___|  
[ec2-user@ip-10-0-1-70 ~]$
```

2. Ping the Visayas-WebServer's by copying their Private IP address using the command:  
`ping <Visayas-WebServer's- Private-IPV4-address>`
  - a. Hit Enter
  - b. In few seconds, Hit CTRL + C on your keyboard to exit the ping.





The screenshot displays the AWS Management Console's EC2 Instances page. At the top, there's a search bar and filters. Below, a table lists three instances: Visayas-WebServer, Mindanao-WebServer (selected), and Luzon-WebServer. All are in a 'Running' state. A terminal window is open for the selected instance, showing a successful SSH connection to an Amazon Linux 2023 instance. The terminal output includes the AWS logo, login history, and a ping test to 10.2.1.45 which shows 100% packet loss.

Below the terminal, the details for instance **i-006fd1de18ee89380 (Mindanao-WebServer)** are shown. The 'Instance summary' tab is active, displaying fields like Instance ID, Public IPv4 address (34.201.36.58), Private IPv4 address (10.2.1.45), Instance state (Running), and Instance type (t2.micro).

4. This confirms that these 3 web servers are not connected. To connect this servers, we need to do the following next steps...

### Configuring VPC Peering Connections

1. Navigate back to the VPC Dashboard

The screenshot shows the AWS VPC Dashboard search results for 'vpc'. The left sidebar contains navigation links for EC2, IAM, and VPC. The main content area shows search results for 'vpc', including 'VPC' (Isolated Cloud Resources) and 'AWS Firewall Manager' (Central management of firewall rules).

2. Search for the **Peering connections** in the **Left-side-bar**

**VPC dashboard** X

EC2 Global View

Filter by VPC ▾

▼ Virtual private cloud

- Your VPCs**
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections**

**Your VPCs (4) Info**

Last updated less than a minute ago Actions ▾ **Create VPC**

Search

<input type="checkbox"/>	Name ▾	VPC ID ▾	State ▾	IPv4 CIDR ▾	IPv6 CIDR
<input type="checkbox"/>	VPC-Luzon	<a href="#">vpc-0c9b9d3789582340d</a>	Available	10.0.0.0/16	-
<input type="checkbox"/>	-	<a href="#">vpc-0678b78645a8bbea6</a>	Available	192.168.5.0/26	-
<input type="checkbox"/>	VPC-Mindanao	<a href="#">vpc-0e0f8c7358fea1599</a>	Available	10.2.0.0/16	-
<input type="checkbox"/>	VPC-Visayas	<a href="#">vpc-0a1f3f357c0351278</a>	Available	10.1.0.0/16	-

Select a VPC above

### 3. Peer VPC-Luzon with VPC-Visayas by Clicking **Create peering connection**

**VPC dashboard** X

EC2 Global View

Filter by VPC ▾

▼ Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections**

**Peering connections Info**

Find resources by attribute or tag

Actions ▾ **Create peering connection**

Name	Peering connection ID	Status	Requester VPC	Accepter VPC
No peering connection found				

Select a peering connection above

a. Name – *optional* : **PC-Luzon-to-Visayas**

b. Select a local VPC to peer with:

- - VPC ID (Requester) : **VPC-Luzon**
  - VPC ID (Acceptor) : **VPC-Visayas**

### Peering connection settings

#### Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.


PC-Luzon-to-Visayas

#### Select a local VPC to peer with

VPC ID (Requester)

vpc-0225d1915f2848ef9 (VPC-Luzon)

VPC CIDRs for vpc-0225d1915f2848ef9 (VPC-Luzon)

CIDR	Status	Status reason
10.0.0.0/16	 Associated	-

#### Select another VPC to peer with

Account

- ☒ My account  
☐ Another account


Region

- ☒ This Region (us-east-1)  
☐ Another Region

VPC ID (Accepter)

vpc-0b1e659facd1a2160 ( VPC-Visayas)

VPC CIDRs for vpc-0b1e659facd1a2160 ( VPC-Visayas)

CIDR	Status	Status reason
10.1.0.0/16	 Associated	-

c. Click **Create peering connection**

**VPC dashboard** X

EC2 Global View

Filter by VPC ▼

- Virtual private cloud
  - Your VPCs
  - Subnets
  - Route tables
  - Internet gateways
  - Egress-only internet gateways
  - Carrier gateways
  - DHCP option sets
  - Elastic IPs
  - Managed prefix lists
  - Endpoints
  - Endpoint services
  - NAT gateways
  - Peering connections
- Security
  - Network ACLs
  - Security groups
- DNS firewall
  - Rule groups
  - Domain lists
- Network Firewall
  - Firewalls
  - Firewall policies
  - Network Firewall rule groups
  - TLS inspection configurations
  - Network Firewall resource groups

**A VPC peering connection pcx-0749831565d3e427d / PC-Luzon-to-Visayas has been requested.**

VPC > Peering connections > pcx-0749831565d3e427d

**pcx-0749831565d3e427d / PC-Luzon-to-Visayas** Actions ▼

**Pending acceptance**  
You can accept or reject this peering connection request using the 'Actions' menu. You have until Tuesday, July 2, 2024 at 14:40:01 GMT+8 to accept or reject the request, otherwise it expires.

**Details Info**

Requester owner ID 654654537193	Accepter owner ID 654654537193	VPC Peering connection ARN arn:aws:ec2:us-east-1:654654537193:vpc-peering-connection/pcx-0749831565d3e427d
Peering connection ID pcx-0749831565d3e427d	Requester VPC vpc-0225d1915f2848ef9 / VPC-Luzon	Accepter VPC vpc-0b1e659facd1a2160 / VPC-Visayas
Status Pending Acceptance by 654654537193	Requester CIDRs 10.0.0.0/16	Accepter CIDRs -
Expiration time Tuesday, July 2, 2024 at 14:40:01 GMT+8	Requester Region N. Virginia (us-east-1)	Accepter Region N. Virginia (us-east-1)

DNS | Route tables | Tags

**DNS settings** Edit DNS settings

Requester VPC ([vpc-0225d1915f2848ef9 / VPC-Luzon](#))

**Info**

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

Accepter VPC ([vpc-0b1e659facd1a2160 / VPC-Visayas](#))

**Info**

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

d. Accept the peering requests in each VPC's dashboard.

•

- Click on the **Actions** and Click on **Accept request**

**VPC dashboard** X

EC2 Global View

Filter by VPC ▼

- Virtual private cloud
  - Your VPCs
  - Subnets

**A VPC peering connection pcx-0749831565d3e427d / PC-Luzon-to-Visayas has been requested.**

VPC > Peering connections > pcx-0749831565d3e427d

**pcx-0749831565d3e427d / PC-Luzon-to-Visayas** Actions ▼

**Pending acceptance**  
You can accept or reject this peering connection request using the 'Actions' menu. You have until Tuesday, July 2, 2024 at 14:40:01 GMT+8 to accept or reject the request, otherwise it expires.

**Details Info**

Accept request  
Reject request  
Edit DNS settings  
Manage tags  
Delete peering connection

•

- Click **Accept request**

Accept VPC peering connection request [Info](#)

Are you sure you want to accept this VPC peering connection request? (pcx-0749831565d3e427d / PC-Luzon-to-Visayas)

Requester VPC vpc-0225d1915f2848ef9 / VPC-Luzon	Accepter VPC vpc-0b1e659facd1a2160 / VPC-Visayas	Requester CIDRs 10.0.0.0/16
Accepter CIDRs –	Requester Region N. Virginia (us-east-1)	Accepter Region N. Virginia (us-east-1)
Requester owner ID 654654537193 (This account)	Accepter owner ID 654654537193 (This account)	

Cancel

Accept request

#### 4. Peer VPC-Visayas with VPC-Mindanao

a. Repeat the same process but using the following configuration:

- - Name – *optional* : **PC-Visayas-to-Mindanao**
  - Select a local VPC to peer with:
    - VPC ID (Requester) : **VPC-Visayas**
    - VPC ID (Accepter) : **VPC-Mindanao**

## Create peering connection

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately.

### Info

#### Peering connection settings

##### Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

#### Select a local VPC to peer with

##### VPC ID (Requester)

##### VPC CIDRs for vpc-0b1e659facd1a2160 ( VPC-Visayas)

CIDR	Status	Status reason
10.1.0.0/16	✔ Associated	-

#### Select another VPC to peer with

##### Account

- ☒ My account  
☐ Another account

##### Region

- ☒ This Region (us-east-1)  
☐ Another Region

##### VPC ID (Acceptor)

##### VPC CIDRs for vpc-0ba5da60375a7f1f8 (VPC-Mindanao)

CIDR	Status	Status reason
10.2.0.0/16	✔ Associated	-

- 

- Click **Create peering connection**

b. Accept the peering requests.

**Your VPC peering connection (pcx-0996a5ecc3d250eff | PC-Visayas-to-Mindanao) has been established.**  
 To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables.

[Modify my route tables now](#)

[Info](#)

[VPC](#) > [Peering connections](#) > pcx-0996a5ecc3d250eff

## pcx-0996a5ecc3d250eff / PC-Visayas-to-Mindanao

Actions ▼

Details
Info

Requester owner ID 654654537193	Acceptor owner ID 654654537193	VPC Peering connection ARN arn:aws:ec2:us-east-1:654654537193:vpc-peering-connection/pcx-0996a5ecc3d250eff
Peering connection ID pcx-0996a5ecc3d250eff	Requester VPC <a href="#">vpc-0b1e659facd1a2160 / VPC-Visayas</a>	Acceptor VPC <a href="#">vpc-0ba5da60375a7f1f8 / VPC-Mindanao</a>
Status <span style="color: green; font-weight: bold;">✔ Active</span>	Requester CIDRs 10.1.0.0/16	Acceptor CIDRs 10.2.0.0/16
Expiration time -	Requester Region N. Virginia (us-east-1)	Acceptor Region N. Virginia (us-east-1)

## Updating Route Tables

We also need to update the route tables for the peered VPC to send and receive traffic.

### 1. Navigate to the Route tables

**Route tables (4)** [Info](#)

Last updated 9 minutes ago

Actions ▼

[Create route table](#)

< 1 >

<input type="checkbox"/>	Name ▼	Route table ID ▲	Expli... ▼	Edge... ▼	Main ▼	VPC
<input type="checkbox"/>	-	<a href="#">rtb-03902dd95bedd1b21</a>	-	-	Yes	<a href="#">vpc-0225d1915f2848ef9   VPC-Luzon</a>
<input type="checkbox"/>	-	<a href="#">rtb-03cb14a50dd9cf6e7</a>	-	-	Yes	<a href="#">vpc-0b1e659facd1a2160   VPC-Visayas</a>
<input type="checkbox"/>	-	<a href="#">rtb-0793950943c439f6b</a>	-	-	Yes	<a href="#">vpc-0ba5da60375a7f1f8   VPC-Mindanao</a>
<input type="checkbox"/>	-	<a href="#">rtb-0db91ab854dec43e1</a>	3 subnets	-	Yes	<a href="#">vpc-0678b78645a8bbee6</a>

### 2.Add routes to direct traffic to the peered VPCs using the peering connection IDs:

a. VPC-Luzon route table:

- - Click **Edit routes**
  - Add in **Destination: 10.1.0.0/16**
    - **Target: Peering Connection**  
*PC-Luzon-to-Visayas*

### Edit routes

**Route 1**  
Destination  
10.0.0.0/16  
  
Propagated  
No

Target  
local  
local

Status  
Active

**Route 2**  
Destination  
0.0.0.0/0  
  
Propagated  
No

Target  
Internet Gateway  
igw-04b9916f14f29d52d

Status  
Active

Remove

**Route 3**  
Destination  
10.1.0.0/16  
  
Propagated  
No

Target  
Peering Connection  
pcx-0749831565d3e427d  
Use: "pcx-0749831565d3e427d"  
pcx-0749831565d3e427d (PC-Luzon-to-Visayas)

Status  
-

Remove

Add route

Cancel Preview Save changes

- - **Save changes**



Updated routes for rtb-03902dd95bedd1b21 successfully

Details

VPC > Route tables > rtb-03902dd95bedd1b21

rtb-03902dd95bedd1b21

Actions

Details
Info

Route table ID rtb-03902dd95bedd1b21	Main Yes	Explicit subnet associations -	Edge associations -
VPC vpc-0225d1915f2848ef9   VPC-Luzon	Owner ID 654654537193		

Routes
Subnet associations
Edge associations
Route propagation
Tags

Routes (3)
Both
Edit routes

Filter routes

Destination	Target	Status	Propagated
0.0.0.0/1	pcx-0749831565d3e427d	Active	No
0.0.0.0/0	igw-04b9916f14f29d52d	Active	No
10.0.0.0/16	local	Active	No

b, VPC-Visayas route table:

- Click **Edit routes**
  - Add in **Destination : 10.2.0.0/16**
    - Target : Peering Connection PC-Visayas-to-Mindanao**

## Edit routes

### Route 1

Destination  
10.1.0.0/16

Target

local ▼  
Q local X

Status

✓ Active

Propagated  
No

### Route 2

Destination

Q 0.0.0.0/0 X

Target

Internet Gateway ▼  
Q igw-0376a047e1104f582 X

Status

✓ Active

Propagated  
No

Remove

### Route 3

Destination

Q 10.2.0.0/16 X

Target

Peering Connection ▼  
Q pcx-0996a5ecc3d250eff X  
Use: "pcx-0996a5ecc3d250eff"  
pcx-0996a5ecc3d250eff (PC-Visayas-to-Mindanao)  
pcx-0749831565d3e427d (PC-Luzon-to-Visayas)

Status

-

Propagated  
No

Remove

Add route

- - Add another route with the following configuration:
    - **Destination : 10.0.0.0/16**
    - **Target : Peering Connection  
PC-Luzon-to-Visayas**

### Route 3

Destination

Q 10.2.0.0/16
X

Target

Peering Connection
▼

Q pcx-0996a5ecc3d250eff
X

Status

-

Propagated

No

Remove

---

### Route 4

Destination

Q 10.0.0.0/16
X

Target

Peering Connection
▼

Q pcx-0749831565d3e427d
X

Use: "pcx-0749831565d3e427d"

pcx-0996a5ecc3d250eff (PC-Visayas-to-Mindanao)

pcx-0749831565d3e427d (PC-Luzon-to-Visayas)

Status

-

Propagated

No

Remove

Add route

- 

- Save changes

Updated routes for rtb-03cb14a50dd9cf6e7 successfully
X

▶ Details

VPC > Route tables > rtb-03cb14a50dd9cf6e7

rtb-03cb14a50dd9cf6e7

Actions ▼

Details
Info

Route table ID

rtb-03cb14a50dd9cf6e7

VPC

vpc-0b1e659facd1a2160 | VPC-Visayas

Main

Yes

Owner ID

654654537193

Explicit subnet associations

-

Edge associations

-

Routes
Subnet associations
Edge associations
Route propagation
Tags

Routes (4)

Both ▼

Edit routes

Q Filter routes

Destination
▼
Target
▼
Status
▼
Propagated
▼

0.0.0.0/0
igw-0376a047e1104f582
Active
No

10.0.0.0/16
pcx-0749831565d3e427d
Active
No

10.1.0.0/16
local
Active
No

10.2.0.0/16
pcx-0996a5ecc3d250eff
Active
No

c. VPC-Mindanao route table:

- Click **Edit routes**
  - Add in **Destination : 10.1.0.0/16**
    - Target : Peering Connection**  
**PC-Visayas-to-Mindanao**

VPC > Route tables > rtb-0/95950945c459f6b > Edit routes

## Edit routes

Route	Destination	Target	Status	Propagated	Actions
Route 1	10.2.0.0/16	local	Active	No	
Route 2	0.0.0.0/0	Internet Gateway	Active	No	Remove
Route 3	10.1.0.0/16	Peering Connection	-	No	Remove

Add route

- Save changes

Updated routes for rtb-0793950943c439f6b successfully

Details

VPC > Route tables > rtb-0793950943c439f6b

rtb-0793950943c439f6b

Actions

Details Info

Route table ID

rtb-0793950943c439f6b

VPC

vpc-0ba5da60375a7f1f8 | VPC-Mindanao

Main

Yes

Owner ID

654654537193

Explicit subnet associations

-

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (3)

Both

Edit routes

Filter routes

< 1 >

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0b4ba5d845414c66d	Active	No
10.1.0.0/16	pcx-0996a5ecc3d250eff	Active	No
10.2.0.0/16	local	Active	No

3. Lastly, we need to configure the **Security Group for Each Instances**:

Think of a security group in AWS as a bouncer at a nightclub. The security group/bouncer checks each visitor (data packet) at the door (instance). They have a list of rules that determine who can enter (inbound rules) and who can leave (outbound rules) based on specific criteria such as the visitor's appearance (IP addresses), their invitation (ports), and the type of event they're attending (protocols).

a. Navigate to the EC2 dashboard and look for **Security Groups** under **Network & Security** in the left-side-bar and Click on it.

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

▼ Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

▼ Load Balancing

Load Balancers

Target Groups

Trust Stores [New](#)

▼ Auto Scaling

Auto Scaling Groups

Settings

Resources

EC2 Global view

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)0

Auto Scaling Groups0

Dedicated Hosts0

Elastic IPs0

Instances0

Key pairs0

Load balancers0

Placement groups0

Security groups4

Snapshots0

Volumes0

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Migrate a server

Note: Your instances will launch in the US East (N. Virginia) Region

Instance alarms

View in CloudWatch

0 in alarm

0 OK

0 insufficient data

Service health

AWS Health Dashboard

✖

An error occurred  
An error occurred retrieving service health information

Diagnose with Amazon Q

Zones

Zone name

Zone ID

## b. SG-Luzon inbound rules Configuration:

- Copy the Security **Security group ID** of **SG-Visayas**

☰

### Security Groups (1/7) [Info](#)

🔄

Actions ▾

Export security groups to CSV ▾

Create security group

🔍 Find resources by attribute or tag

< 1 > ⚙️

<input type="checkbox"/>	Name ▾	Security group ID ▾	Security group na... ▲	VPC ID ▾	Description
<input type="checkbox"/>	-	<a href="#">sg-0c5da37574511e5a6</a>	default	<a href="#">vpc-0b1e659facd1a2160</a> 🔗	default VPC security grou
<input type="checkbox"/>	-	<a href="#">sg-06fdb1e5720014bfe</a>	default	<a href="#">vpc-0225d1915f2848ef9</a> 🔗	default VPC security grou
<input type="checkbox"/>	-	<a href="#">sg-029e1560c369ade99</a>	default	<a href="#">vpc-0678b78645a8bbea6</a> 🔗	default VPC security grou
<input type="checkbox"/>	-	<a href="#">sg-0f6e556bda83a1298</a>	default	<a href="#">vpc-0ba5da60375a7f1f8</a> 🔗	default VPC security grou
<input type="checkbox"/>	-	<a href="#">sg-0ef3725f3d48bdf8f</a>	SG-Luzon	<a href="#">vpc-0225d1915f2848ef9</a> 🔗	SG for Luzon
<input type="checkbox"/>	-	<a href="#">sg-0ec88656fb111553c</a>	SG-Mindanao	<a href="#">vpc-0ba5da60375a7f1f8</a> 🔗	SG for Mindanao
<input checked="" type="checkbox"/>	-	<a href="#">sg-003057a26ee9c6aad</a>	SG-Visayas	<a href="#">vpc-0b1e659facd1a2160</a> 🔗	SG for Visayas

◀

#### sg-003057a26ee9c6aad - SG-Visayas

Details

Inbound rules

Outbound rules

Tags

Details

✔️ [sg-003057a26ee9c6aad](#)

📄 SG-Visayas

📄 [sg-003057a26ee9c6aad](#)

Description

📄 SG for Visayas

VPC ID

📄 [vpc-0b1e659facd1a2160](#)

🔗

Owner

Inbound rules count

Outbound rules count

- - Click on the Security group ID of SG-Luzon

**Security Groups (1/7)** [Info](#) [Actions](#) [Export security groups to CSV](#) [Create security group](#)

Find resources by attribute or tag

	Name	Security group ID	Security group na...	VPC ID	Description
<input type="checkbox"/>	-	<a href="#">sg-0c5da37574511e5a6</a>	default	<a href="#">vpc-0b1e659facd1a2160</a>	default VPC security grou
<input type="checkbox"/>	-	<a href="#">sg-06fdb1e5720014bfe</a>	default	<a href="#">vpc-0225d1915f2848ef9</a>	default VPC security grou
<input type="checkbox"/>	-	<a href="#">sg-029e1560c369ade99</a>	default	<a href="#">vpc-0678b78645a8bbea6</a>	default VPC security grou
<input type="checkbox"/>	-	<a href="#">sg-0f6e556bda83a1298</a>	default	<a href="#">vpc-0ba5da60375a7f1f8</a>	default VPC security grou
<input checked="" type="checkbox"/>	-	<a href="#">sg-0ef3725f3d48bdf8f</a>	SG-Luzon	<a href="#">vpc-0225d1915f2848ef9</a>	SG for Luzon
<input type="checkbox"/>	-	<a href="#">sg-0ec8861fb111553c</a>	SG-Mindanao	<a href="#">vpc-0ba5da60375a7f1f8</a>	SG for Mindanao
<input type="checkbox"/>	-	<a href="#">sg-003097a28ee9c6aad</a>	SG-Visayas	<a href="#">vpc-0b1e659facd1a2160</a>	SG for Visayas

**sg-0ef3725f3d48bdf8f - SG-Luzon**

Details | **Inbound rules** | Outbound rules | Tags

**Inbound rules (1)** [Manage tags](#) [Edit inbound rules](#)

Search

	Name	Security group rule ID	IP version	Type	Protocol
<input type="checkbox"/>	-	sgr-0a386eefa6db8ff94	IPv4	SSH	TCP

You will be redirected to the SG-Visayas Dashboard

- - Click **Edit inbound rules**



EC2 > Security Groups > sg-0ef3725f3d48bdf8f - SG-Luzon

## sg-0ef3725f3d48bdf8f - SG-Luzon

Actions ▾

**Details**

Security group name SG-Luzon	Security group ID sg-0ef3725f3d48bdf8f	Description SG for Luzon	VPC ID <a href="#">vpc-0225d1915f2848ef9</a>
Owner 654654537193	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

**Inbound rules** | Outbound rules | Tags

**Inbound rules (1)** Manage tags Edit inbound rules

<input type="checkbox"/>	Name ▾	Security group rule ID ▾	IP version ▾	Type ▾	Protocol ▾
<input type="checkbox"/>	-	sgr-0a386eefa6d134f94	IPv4	SSH	TCP

- - Click **Add rule** and Add following the Inbound rules configuration:
    - Type : **All ICMP – IPv4**
    - Paste the Security Group ID of SG-Visayas in the **Source**

**Inbound rule 2** Delete

Security group rule ID  
-

Type Info  
All ICMP - IPv4 ▾

Protocol Info  
ICMP

Port range Info  
All

Source type Info  
Custom ▾

Source Info  
 X  
 X

Description - optional Info

Add rule

Cancel Preview changes Save rules

- - Click **Save rules**

### c. SG-Visayas inbound rules Configuration:

- - Follow the same process as **Step 3-b** but with the following inbound rules instead:
    - Type : **All ICMP – IPv4**
    - Paste the Security Group ID of **SG-Luzon** in the **Source**
    - Type : **All ICMP – IPv4**
    - Paste the Security Group ID of **SG-Mindanao** in the **Source**
    - Click Save

EC2 > Security Groups > sg-003057a26ee9c6aad - SG-Visayas

## sg-003057a26ee9c6aad - SG-Visayas

Actions ▼

**Details**

Security group name SG-Visayas	Security group ID sg-003057a26ee9c6aad	Description SG for Visayas	VPC ID <a href="#">vpc-0b1e659facd1a2160</a>
Owner 654654537193	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

**Inbound rules** | Outbound rules | Tags

**Inbound rules (3)** Manage tags Edit inbound rules

<input type="checkbox"/>	Name ▼	Security group rule ID ▼	IP version ▼	Type ▼	Protocol
<input type="checkbox"/>	-	sgr-06675c006271c0283	-	All ICMP - IPv4	ICMP
<input type="checkbox"/>	-	sgr-02207dc63231254d5	-	All ICMP - IPv4	ICMP
<input type="checkbox"/>	-	sgr-0d2756c5715409ff9	IPv4	SSH	TCP

### d. SG-Mindanao inbound rules Configuration:

- - Similar to the previous step, add the following inbound rules for this SG:
    - Type : **All ICMP – IPv4**
    - Paste the Security Group ID of **SG-Visayas** in the **Source**

Inbound security group rules successfully modified on security group (sg-0ec88656fb111553c | SG-Mindanao)

Details

EC2 > Security Groups > sg-0ec88656fb111553c - SG-Mindanao

sg-0ec88656fb111553c - SG-Mindanao

Actions

Details

Security group name SG-Mindanao	Security group ID sg-0ec88656fb111553c	Description SG for Mindanao	VPC ID <a href="#">vpc-0ba5da60375a7f1f8</a>
Owner 654654537193	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules

Outbound rules

Tags

Inbound rules (2)

Manage tags

Edit inbound rules

Search

< 1 > ⚙

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol
<input type="checkbox"/>	-	sgr-0e351f3c2e8e1c5cf	-	All ICMP - IPv4	ICMP
<input type="checkbox"/>	-	sgr-0c29917434e5ae01b	IPv4	SSH	TCP

## Testing Connectivity

1. Similar to **Instance Test Coonnection** section, SSH into each instance from your local machine.

a. **SSH to the Visayas-WebServer:**

EC2 > Instances > i-0954fb7f317c9d436 > Connect to instance

## Connect to instance Info

Connect to your instance i-0954fb7f317c9d436 (Visayas-WebServer)

EC2 Instance Connect

Session Manager

SSH client

Instance ID  
i-0954fb7f317c9d436 (Visayas-WebServer)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is my-key-pair.pem.
3. Run this command, if necessary, to ensure your key is not public:  
chmod 400 "my-key-pair.pem"
4. Connect to your instance using its Public IP:  
44.202.211.12

Example:  
ssh -i "my-key-pair.pem" ec2-user@44.202.211.12

**Note:** In most cases, the guessed username is correct. However, if the AMI owner has changed the default AMI username.

•

- Lets ping the other servers Private IP address

ping <Luzon-WebServer-private-IPv4-Address>

The screenshot displays the AWS Management Console 'Instances' page with three EC2 instances: Mindanao-WebServer, Luzon-WebServer, and Visayas-WebServer. The Luzon-WebServer is selected. Below the console, a terminal window shows a successful SSH connection to the Luzon-WebServer. The terminal output includes the Amazon Linux 2023 logo and a successful ping to 10.0.1.70. To the right of the terminal, a sidebar shows instance details for 'i-01cc52e724d78b741 (Luzon-WebServer)', including its Private IPv4 address (10.0.1.70) and an AWS Compute Optimizer finding.

Name	Instance ID	Instance state	Instanc...	Status check	Alarm status	Availabi...	Public I...
Mindanao-WebServer	i-006fd1de...	Running	t2.micro	2/2 checks p	View alarms +	us-east-1c	-
Luzon-WebServer	i-01cc52e7...	Running	t2.micro	2/2 checks p	View alarms +	us-east-1d	-
Visayas-WebServer	i-0954fb7f...	Running	t2.micro	2/2 checks p	View alarms +	us-east-1b	-

```

ec2-user@ip-10-1-1-54:~$ ssh -i "my-key-pair.pem" ec2-user@44.202.211.12
Last login: Tue Jun 25 07:33:14 2024 from 119.111.230.25
[ec2-user@ip-10-1-1-54 ~]$ ping 10.0.1.70
PING 10.0.1.70 (10.0.1.70) 56(84) bytes of data:
64 bytes from 10.0.1.70: icmp_seq=1 ttl=127 time=0.794 ms
64 bytes from 10.0.1.70: icmp_seq=2 ttl=127 time=0.870 ms
64 bytes from 10.0.1.70: icmp_seq=3 ttl=127 time=0.905 ms
64 bytes from 10.0.1.70: icmp_seq=4 ttl=127 time=0.885 ms
64 bytes from 10.0.1.70: icmp_seq=5 ttl=127 time=0.849 ms
64 bytes from 10.0.1.70: icmp_seq=6 ttl=127 time=0.894 ms
64 bytes from 10.0.1.70: icmp_seq=7 ttl=127 time=0.829 ms
^C
--- 10.0.1.70 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6145ms
rtt min/avg/max/mdev = 0.794/0.860/0.905/0.036 ms
[ec2-user@ip-10-1-1-54 ~]$
  
```

Private IPv4 address copied  
10.0.1.70  
Public IPv4 DNS  
-  
Elastic IP addresses  
-  
AWS Compute Optimizer finding  
User: arn:aws:iam::654654537193:user/Playcloud-LSJz6uFQ0n is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: \* because no identity-based policy allows the compute-optimizer:Ge tEnrollmentStatus action

This time we can received packets from Luzon-WebServer

- 

- ping Mindanao-WebServer

ping <Mindanao-WebServer-private-IPv4-Address>

Instances (1/3) Info

Refresh
Connect
Instance state
Actions
Launch instances

All states

1

	Name	Instance ID	Instance state	Instanc...	Status check	Alarm status	Availabi...	Public I...
<input checked="" type="checkbox"/>	Mindanao-WebServer	i-006fd1de...	Running	t2.micro	2/2 checks p	View alarms +	us-east-1c	-
<input type="checkbox"/>	Luzon-WebServer	i-01cc52e7...	Running	t2.micro	2/2 checks p	View alarms +	us-east-1d	-
<input type="checkbox"/>	Visayas-WebServer	i-0954fb7f...	Running	t2.micro	2/2 checks p	View alarms +	us-east-1b	-

i-006fd1de18ee89380 (Mindanao-WebServer)

Storage

Tags

Private IPv4 addresses

10.2.1.45

Public IPv4 DNS

-

Elastic IP addresses

ec2-user@ip-10-1-1-54:~

```

[ec2-user@ip-10-1-1-54 ~]$ ping 10.2.1.45
PING 10.2.1.45 (10.2.1.45) 56(84) bytes of data.
64 bytes from 10.2.1.45: icmp_seq=1 ttl=127 time=0.772 ms
64 bytes from 10.2.1.45: icmp_seq=2 ttl=127 time=1.03 ms
64 bytes from 10.2.1.45: icmp_seq=3 ttl=127 time=0.795 ms
64 bytes from 10.2.1.45: icmp_seq=4 ttl=127 time=0.847 ms
64 bytes from 10.2.1.45: icmp_seq=5 ttl=127 time=0.692 ms
64 bytes from 10.2.1.45: icmp_seq=6 ttl=127 time=0.790 ms
^C
--- 10.2.1.45 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5176ms
rtt min/avg/max/mdev = 0.692/0.821/1.031/0.104 ms
[ec2-user@ip-10-1-1-54 ~]$

```

[EC2](#) > [Instances](#) > [i-01cc52e724d78b741](#) > Connect to instance

## Connect to instance Info

Connect to your instance i-01cc52e724d78b741 (Luzon-WebServer) using any of these options

EC2 Instance Connect

Session Manager

**SSH client**

EC2 serial console

Instance ID  
 **i-01cc52e724d78b741** (Luzon-WebServer)

- Open an SSH client.
- Locate your private key file. The key used to launch this instance is my-key-pair.pem.
- Run this command, if necessary, to ensure your key file has the right permissions:  
 `chmod 400 "my-key-pair.pem"`
- Connect to your instance using its Public IP: **52.91.130.103**

Example:

`ssh -i "my-key-pair.pem" ec2-user@52.91.130.103`

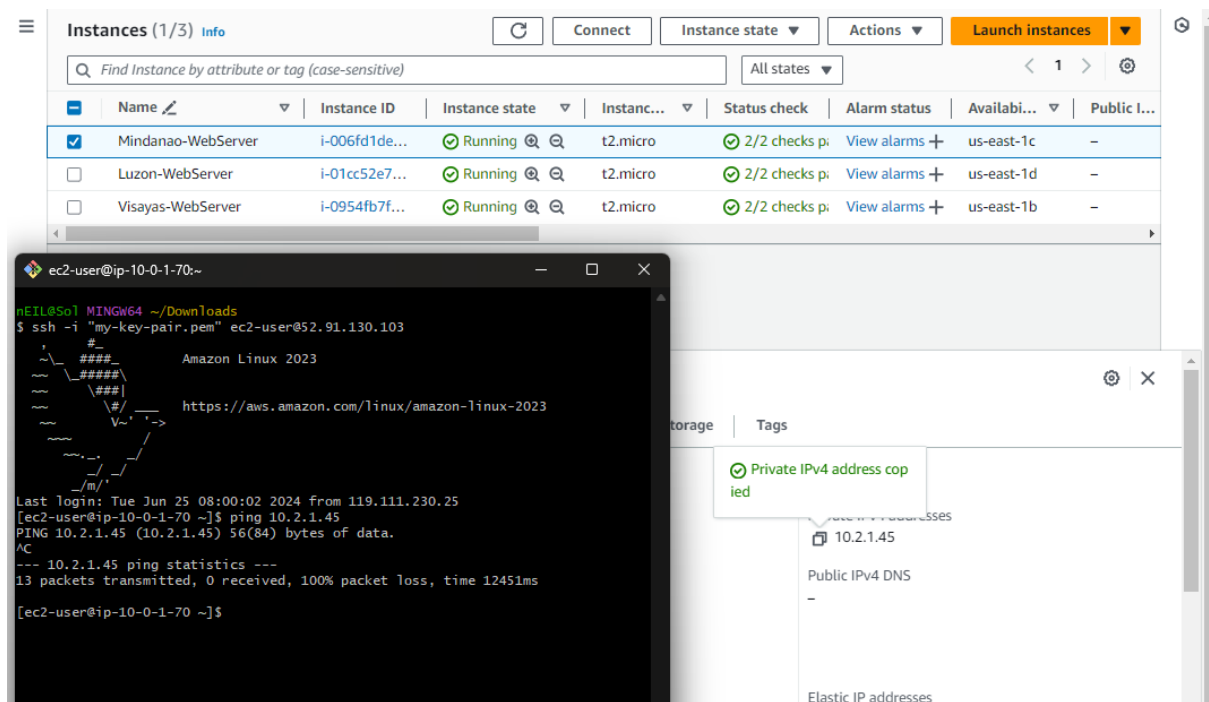
**Note:** In most cases, the guessed username is correct. However, you must specify the username if the AMI owner has changed the default AMI user name.

```
ec2-user@ip-10-0-1-70:~$ ssh -i "/Downloads/my-key-pair.pem" ec2-user@52.91.130.103
Warning: Permanently added host 52.91.130.103 (SSH-2.0-openssh_8.9p1 Ubuntu 22.04 LTS).
ec2-user@ip-10-0-1-70:~$ cat /etc/os-release
NAME="Amazon Linux 2023"
VERSION="2023"
ID="amzn-linux-2023"
PRETTY_NAME="Amazon Linux 2023"
ANSI_COLOR="0;32"
LOGO="https://aws.amazon.com/linux/amazon-linux-2023/"
CPE_ID_RECORD=true
VENDOR_URL="https://aws.amazon.com/linux/amazon-linux-2023/"
SUPPORT="https://aws.amazon.com/linux/amazon-linux-2023/support"
DOCUMENTATION="https://docs.aws.amazon.com/linux/latest/ug/index.html"
BOUTIQUE="https://aws.amazon.com/boutique/linux/amazon-linux-2023/"
Last login: Tue Jun 25 07:56:51 2024 from 119.111.230.25
[ec2-user@ip-10-0-1-70 ~]$
```

- ping <Visayas-WebServer-private-IPv4-Address>

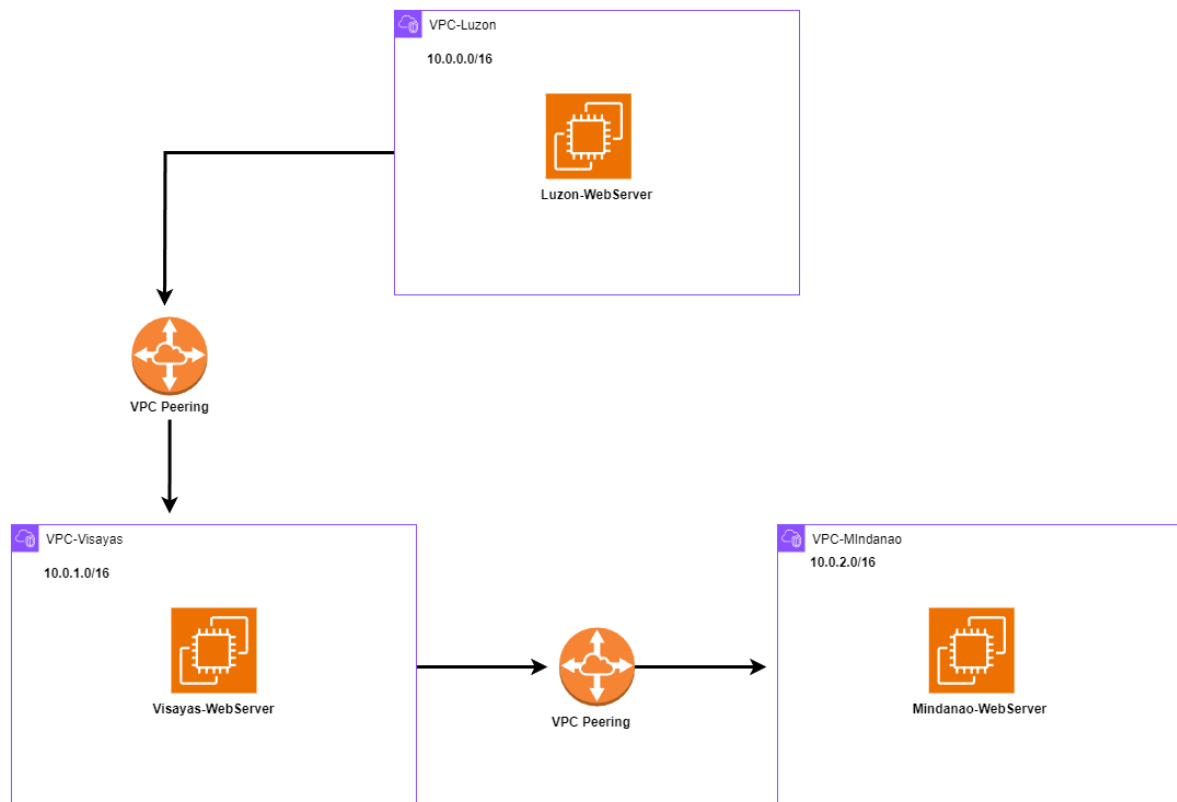


- ```
ping <Mindanao-WebServer-private-IPv4-Address>
```



---

We can't ping the Mindanao-WebServer. Why is that? The reason for this is because VPC Peering is **not transitive**, meaning that if VPC-Luzon is peered with VPC-Visayas, and VPC-Visayas is peered with VPC-Mindanao, VPC-Luzon cannot communicate directly with VPC-Mindanao through VPC-Visayas. Each peering connection is a one-to-one relationship that does not automatically extend beyond the two VPCs directly involved.



---

That's it! Congratulations! This lab has effectively demonstrated the setup and testing of VPC Peering across multiple VPCs, illustrating how resources in different VPCs can communicate securely and efficiently. Throughout the lab, you've configured and verified network connections, thereby acquiring practical skills in managing complex network architectures on AWS. This prepares you for real-world scenarios that involve interconnected VPC environments.

One critical insight from this exercise is the non-transitive nature of VPC Peering. As observed, while VPC-Luzon could communicate with VPC-Visayas and VPC-Visayas could interact with VPC-Mindanao, there was no direct communication between VPC-Luzon and VPC-Mindanao. This limitation highlights that each VPC Peering connection is an isolated, one-to-one relationship and does not inherently allow indirect routing through a third VPC. Understanding this characteristic is essential for network architects in planning and structuring AWS environments, ensuring that connectivity requirements are met efficiently without relying on transitive peering capabilities.



By internalizing the constraints and capabilities of VPC Peering, you can better design solutions that are both scalable and secure, addressing complex networking challenges with strategic configurations.