

## Task 5.3D

### CLOUD COMPUTING

#### Creating a VPC Peering Connection

##### **Task 1: Creating a VPC Peering Connection**

###### **What you're doing:**

Establishing a **private link** between two VPCs—**Lab VPC** (has an EC2 application) and **Shared VPC** (has a database).

###### **Steps:**

- Open the **VPC dashboard**.
- Go to **Peering Connections**, click **Create**.
- Name it **Lab-Peer**.
- Select **Lab VPC** as **Requester**, **Shared VPC** as **Acceptor**.
- Click **Create**.
- After creation, **accept the request** to activate the connection.

The screenshot shows the AWS VPC Peering Connections console in the AWS Management Console. The top navigation bar includes tabs for 'Guided lab: Creating a VPC Peering Connection' and 'PeeringConnections | VPC | us-east-1'. The main content area is titled 'Peering connections' and displays a table with columns: Name, Peering connection ID, Status, Requester VPC, and Acceptor VPC. A search bar at the top allows filtering by attribute or tag. Below the table, a message says 'No peering connection found'. A large central text area says 'Select a peering connection above' with three small icons below it. On the left sidebar, under 'Virtual private cloud', 'Peering connections' is selected. Under 'Security', 'Network ACLs' and 'Security groups' are listed. The bottom part of the screenshot shows the 'Create peering connection' wizard. Step 1: 'VPC ID (Requester)' shows 'vpc-0f62339f27dce6e5f (Lab VPC)'. Step 2: 'VPC CIDRs for vpc-0f62339f27dce6e5f (Lab VPC)' lists '10.0.0.0/16' with status 'Associated'. Step 3: 'Select another VPC to peer with' includes sections for 'Account' (radio button selected for 'My account'), 'Region' (radio button selected for 'This Region (us-east-1)'), and 'VPC ID (Acceptor)' (dropdown menu showing 'vpc-03316988a2d7c7728 (Shared VPC)'). Step 4: 'VPC CIDRs for vpc-03316988a2d7c7728 (Shared VPC)' lists '10.5.0.0/16' with status 'Associated'. Step 5: 'Tags' is currently empty. The bottom navigation bar includes links for 'CloudShell', 'Feedback', and social media sharing.

A screenshot of the AWS VPC Peering Connections page. A modal dialog box is open, asking if the user wants to accept a VPC peering connection request. The modal shows details about the requester and accepter, including their VPC IDs, owner IDs, and regions. The 'Accept request' button is highlighted.

A screenshot of the AWS VPC Peering Connections page showing the 'Create peering connection' wizard. Step 1: Select a local VPC to peer with. The requester VPC is selected as 'vpc-0703652ebf134e573 (Lab VPC)'. Step 2: Select another VPC to peer with. The accepter VPC is selected as 'vpc-0eeb7e0b5f60d916e (Shared VPC)'.

## Task 2: Configuring Route Tables

**What you're doing:**

Telling each VPC **how to reach the other** using the new peering connection.

**Subtasks:**

**For Lab VPC:**

- Go to **Route Tables**.
- Select **Lab Public Route Table**.
- Add a route:

- **Destination:** 10.5.0.0/16 (CIDR of Shared VPC)
- **Target:** Peering connection Lab-Peer
- Save changes.

#### For Shared VPC:

- Select **Shared-VPC Route Table**.
- Add a route:
  - **Destination:** 10.0.0.0/16 (CIDR of Lab VPC)
  - **Target:** Peering connection Lab-Peer
- Save changes.

The screenshot shows the 'Edit routes' section of the AWS VPC Route Table configuration. There are two routes listed:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
10.5.0.0/16	Peering Connection	-	No

At the bottom right, there are 'Cancel', 'Preview', and 'Save changes' buttons.

Guided lab: Creating a VPC Peering Connection

VPC | us-east-1

OnTrack

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-04f0c7b4b1c1f09d5

aws Search [Alt+S] United States (N. Virginia) vocabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082

VPC > Route tables > rtb-04f0c7b4b1c1f09d5

Updated routes for rtb-04f0c7b4b1c1f09d5 / Lab Private Route Table successfully

rtb-04f0c7b4b1c1f09d5 / Lab Private Route Table Actions

Virtual private cloud

Your VPCs Subnets Route tables Internet gateways Egress-only Internet gateways Carrier gateways DHCP option sets Elastic IPs Managed prefix lists NAT gateways Peering connections Route servers New

Security

Network ACLs Security groups

CloudShell Feedback

14°C Cloudy

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 03:30 10-04-2025

**Details** Info

Route table ID: rtb-04f0c7b4b1c1f09d5 Main: No

VPC: vpc-0f62339f27dce6e5f | Lab VPC Owner ID: 824133236082

Explicit subnet associations: subnet-0998a67c9c951fe2e / Lab Private Subnet

Edge associations: -

**Routes** Subnet associations Edge associations Route propagation Tags

**Routes (2)**

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
10.5.0.0/16	pxx-0ec0862a1e6b6970d	Active	No

VPC | us-east-1

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditRoutes:RouteTableId=rtb-0dbfa4f221736877f

aws Search [Alt+S] United States (N. Virginia) voclabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082

VPC > Route tables > rtb-0dbfa4f221736877f > Edit routes

### Edit routes

Destination	Target	Status	Propagated
10.5.0.0/16	local	Active	No
Q 10.0.0.0/16	local	-	No
Q pxc-0ec0862a1e6b6970d	Peering Connection	-	No

Add route Remove Cancel Preview Save changes

CloudShell Feedback 14°C Cloudy 03:38 10-04-2025

VPC | us-east-1 us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#VpcDetails:VpcId=vpc-03316988a2d7c7728

aws Search [Alt+S] United States (N. Virginia) voclabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082

VPC > Your VPCs > vpc-03316988a2d7c7728 Actions

### vpc-03316988a2d7c7728 / Shared VPC

#### Details Info

VPC ID	vpc-03316988a2d7c7728	State	Available	Block Public Access	Off	DNS hostnames	Enabled
DNS resolution	Enabled	Tenancy	default	DHCP option set	dopt-0b555cb8099d5f6ce	Main route table	rtb-088a1adfc5795b495
Main network ACL	acl-0728918d8b55ff07d	Default VPC	No	IPv4 CIDR	10.5.0.0/16	IPv6 pool	-
IPv6 CIDR (Network border group)	-	Network Address Usage metrics	Disabled	Route 53 Resolver DNS Firewall rule groups	-	Owner ID	824133236082

Resource map CIDs Flow logs Tags Integrations

#### Flow logs Info

Name	Flow log ID	Filter	Destination type	Destination name
No flow logs found in this Region				

Actions Create flow log

VPC | us-east-1

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#vpcDetailsVpcId=vpc-03316988a2d7c7728

aws Search [Alt+S] United States (N. Virginia) vocabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082

VPC > Your VPCs > vpc-03316988a2d7c7728

Successfully created flow log for vpc-03316988a2d7c7728.

### vpc-03316988a2d7c7728 / Shared VPC

**Details**

VPC ID vpc-03316988a2d7c7728	State Available	Block Public Access Off	DNS hostnames Enabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-0b535cb8b99d5f6ce	Main route table rtb-088a1adc5795b495
Main network ACL acl-0728918d8b55ff07d	Default VPC No	IPv4 CIDR 10.5.0.0/16	IPv6 pool -
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 824133236082

Resource map CIDRs Flow logs Tags Integrations

**Resource map**

VPC Show details Your AWS virtual network Subnets (2) Subnets within this VPC Route tables (2) Route network traffic to resources Network connections Connections to

CloudShell Feedback 14°C Cloudy 03:43 10-04-2025

VPC | us-east-1

CloudWatch | us-east-1

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/ShareVPCFlowLogs

aws Search [Alt+S] United States (N. Virginia) vocabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082

CloudWatch > Log groups > ShareVPCFlowLogs

### ShareVPCFlowLogs

**Log group details**

Log class Standard	Metric filters 0	Data protection
ARN arn:aws:logs:us-east-1:824133236082:log-group:ShareVPCFlowLogs:*	Subscription filters 0	Sensitive data count
Creation time 12 minutes ago	Contributor Insights rules -	Field indexes
Retention Never expire	KMS key ID -	Transformer
Stored bytes -	Anomaly detection Configure	Configure

Actions View in Logs Insights Start tailing Search log group

Log streams (1)

Log streams Delete Create log stream Search all log streams Filter log streams or trv prefix search

CloudShell Feedback 14°C Cloudy 03:57 10-04-2025

The screenshot shows the AWS VPC Route Tables console. On the left, there's a sidebar with navigation links like 'VPC dashboard', 'Virtual private cloud', and 'Security'. The main area displays a table of route tables with columns for Name, Route table ID, Explicit subnet associations, Edge associations, Main, and VPC. One row is selected: 'Shared-VPC Route Table' (rtb-0fd8de187883adb0d), which has 2 subnets associated with it. Below the table, a detailed view for the selected route table is shown, including its details (Route table ID: rtb-0fd8de187883adb0d, Main: No, Owner ID: 072770316734), explicit subnet associations (2 subnets), and edge associations (none). The status bar at the bottom indicates it's from 2025, and the browser toolbar shows various icons.

### Task 3: Enabling VPC Flow Logs

#### What you're doing:

Setting up **logs** to monitor network traffic in **Shared VPC**.

#### Steps:

- Go to **Your VPCs**, select **Shared VPC**.
- Open **Flow logs** tab, click **Create flow log**.
- Set:
  - **Name:** SharedVPCLogs
  - **Aggregation interval:** 1 minute
  - **Destination:** CloudWatch Logs
  - **Log group:** ShareVPCFlowLogs
  - **IAM Role:** vpc-flow-logs-Role
- Create log.
- Click the **log group name** to view in CloudWatch.

VPC | us-east-1

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateVpcFlowLog:VpcId=vpc-03316988a2d7c7728

aws Search [Alt+S] United States (N. Virginia) vocabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082

VPC > Your VPCs > Create flow log

### Create flow log Info

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple flow logs to send traffic to different destinations.

**Selected resources Info**

Name	Resource ID	State
Shared VPC	vpc-03316988a2d7c7728	Available

**Flow log settings**

**Name - optional**

**Filter**  
The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).  
 Accept  
 Reject  
 All

**Maximum aggregation interval Info**  
The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.  
 10 minutes  
 1 minute

**Destination**  
The destination to which to publish the flow log data.  
 Send to CloudWatch Logs  
 Send to an Amazon S3 bucket

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 03:41 ENG IN 10-04-2025

VPC | us-east-1

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateVpcFlowLog:VpcId=vpc-03316988a2d7c7728

aws Search [Alt+S] United States (N. Virginia) vocabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082

VPC > Your VPCs > Create flow log

### Create flow log Info

The destination to which to publish the flow log data.

Send to CloudWatch Logs  
 Send to an Amazon S3 bucket  
 Send to Amazon Data Firehose in the same account  
 Send to Amazon Data Firehose in a different account

**Destination log group Info**  
The name of an existing log group or the name of a new log group that will be created when you create this flow log. A new log stream is created for each monitored network interface.

**Service access**  
VPC flow logs require permissions to create log groups and publish events in CloudWatch.

Use an existing service role  
 Create and use a new service role

**Service role Info**  
The IAM role that has permission to publish to the Amazon CloudWatch log group.

[View this service role in the IAM console](#)

**Log record format**  
Specify the fields to include in the flow log record.  
 AWS default format  
 Custom format

**Additional metadata**  
Include additional metadata to AWS default log record format.  
 Include Amazon ECS metadata

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 03:43 ENG IN 10-04-2025

The screenshot shows the AWS CloudWatch Log Groups interface. On the left, a sidebar navigation includes AI Operations, Alarms, Logs (with Log groups selected), Metrics, X-Ray traces, and Events. The main content area displays the 'ShareVPCFlowLogs' log group details. Key information shown includes:

- Log group details:**
  - Log class: Standard
  - ARN: arn:aws:logs:us-east-1:824133236082:log-group:ShareVPCFlowLogs:\*
  - Creation time: 12 minutes ago
  - Retention: Never expire
  - Stored bytes: -
- Metric filters:** 0
- Subscription filters:** 0
- Contributor Insights rules:** -
- KMS key ID:** -
- Anomaly detection:** Configure
- Data protection:** Sensitive data count, Field indexes, Transformer

Below the details, a tabbed section shows 'Log streams' (selected), Tags, Anomaly detection, Metric filters, Subscription filters, Contributor Insights, Data protection, and Field. The 'Log streams' tab contains a table with one entry:

Log stream	Last event time	Last event ID	Size
CloudShell	12 minutes ago	1	1.2 KB

At the bottom of the page, there are buttons for Actions, View in Logs Insights, Start tailing, and Search log group.

The screenshot shows the AWS VPC console. The left sidebar includes VPC dashboard, EC2 Global View, Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only Internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections, Route servers), and Route (Network ACLs, Security groups). The main content area shows the 'vpc-03316988a2d7c7728 / Shared VPC' details. A green success message at the top states "Successfully created flow log for vpc-03316988a2d7c7728." The 'Details' tab shows the following configuration:

VPC ID: vpc-03316988a2d7c7728	State: Available	Block Public Access: Off	DNS hostnames: Enabled
DNS resolution: Enabled	Tenancy: default	DHCP option set: dopt-0b555cb899d5f6ce	Main route table: rtb-088a1adfc5795b495
Main network ACL: acl-0728918d8b55ff07d	Default VPC: No	IPv4 CIDR: 10.5.0.0/16	IPv6 pool: -
IPv6 CIDR (Network border group): -	Network Address Usage metrics: Disabled	Route 53 Resolver DNS Firewall rule groups: -	Owner ID: 824133236082

Below the details, tabs for Resource map, CIDs, Flow logs, Tags, and Integrations are visible. The 'Resource map' tab shows a grid of resources:

VPC	Subnets	Route tables	Network
Show details	(2)	(2)	(2)
Your AWS virtual network	Subnets within this VPC	Route network traffic to resources	Connections to

At the bottom of the page, there are buttons for Actions, Resource map, CIDs, Flow logs, Tags, Integrations, and a search bar.

## Task 4: Testing the VPC Peering Connection

**What you're doing:**

Ensuring the **Lab VPC EC2 instance** can connect to the **Shared VPC database**.

**Steps:**

- Copy the **public IP of the EC2** from AWS Details, open in browser.
- You'll see the **inventory app** asking to configure database.
- Click **Settings**:

- Enter **database endpoint**, DB name, username, password.
- Save and confirm it connects to show **inventory data**.

This proves **peering is working**, since the database is not internet-accessible—only reachable through peering.

Endpoint: inventory-db.cnj6hdmgdc0e.us-east-1.rds.amazonaws.com

Database: Inventory

Username: admin

Password: lab-password

**Save**

Store	Item	Quantity
Puerto Rico	Amazon Echo	12
Paris	Amazon Dot	3
Detroit	Amazon Tap	5

**+ Add Inventory**

This page was generated by instance i-08c8725bb1478b629 in Availability Zone us-east-1a.



## Task 5: Analyzing the VPC Flow Logs

**What you're doing:**

Viewing the logs to **inspect network traffic** between the app and database.

## Steps:

- Go back to the **CloudWatch log group**.
- Open a **Log stream** (eni-...).
- Look for entries showing:
  - Traffic from EC2 to DB (ports like **3306**).
  - Source and destination **IP addresses**.
  - Status like **ACCEPT/OK**.

The screenshots show the AWS CloudWatch Log Stream interface. The top screenshot displays the log group configuration page, showing the ARN, creation time, retention period, and stored bytes. It also lists the log streams under the 'Log streams' tab, showing one entry: eni-0e686673d4a8300e3-all. The bottom screenshot shows the detailed log events for this stream. The log events table has columns for Timestamp and Message. The messages show traffic details and status codes, such as '1744223082 ACCEPT OK'. The interface includes a filter bar at the top and various navigation and search options.

Timestamp	Message
2025-04-09T18:23:10.000Z	2 072770316734 eni-0e686673d4a8300e3 - - - - - 1744222990 1744223021 - NODATA
2025-04-09T18:24:24.000Z	2 072770316734 eni-0e686673d4a8300e3 10.0.0.193 10.5.2.199 50632 3306 6 9 1035 1744223064 1744223072 ACCEPT OK
2025-04-09T18:24:24.000Z	2 072770316734 eni-0e686673d4a8300e3 10.5.2.199 10.0.0.193 3306 50632 6 7 536 1744223064 1744223072 ACCEPT OK
2025-04-09T18:24:24.000Z	2 072770316734 eni-0e686673d4a8300e3 10.0.0.193 10.5.2.199 50648 3306 6 9 713 1744223064 1744223072 ACCEPT OK
2025-04-09T18:24:24.000Z	2 072770316734 eni-0e686673d4a8300e3 10.5.2.199 10.0.0.193 3306 50648 6 7 830 1744223064 1744223072 ACCEPT OK

Screenshot of a dual-monitor setup showing AWS CloudWatch Log Events and AWS Academy assignments.

**Top Monitor (CloudWatch Log Events):**

- URL: us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/ShareVPCFlowLogs/log-events/eni-0e686673d4a8300e3-all
- Log group: ShareVPCFlowLogs
- Log stream: eni-0e686673d4a8300e3-all
- Timestamp range: 2025-04-09T18:23:10.000Z to 2025-04-09T18:24:47.000Z
- Log entries (partial list):
  - 2025-04-09T18:23:10.000Z 2 072770316734 eni-0e686673d4a8300e3 - - - - - 1744222990 1744223021 - NODATA
  - 2025-04-09T18:24:24.000Z 2 072770316734 eni-0e686673d4a8300e3 10.0.0.193 10.5.2.199 50632 3306 6 9 1035 1744223064 1744223072 ACCEPT OK
  - 2025-04-09T18:24:24.000Z 2 072770316734 eni-0e686673d4a8300e3 10.5.2.199 10.0.0.193 3306 50632 6 7 536 1744223064 1744223072 ACCEPT OK
  - 2025-04-09T18:24:24.000Z 2 072770316734 eni-0e686673d4a8300e3 10.0.0.193 10.5.2.199 50648 3306 6 9 713 1744223064 1744223072 ACCEPT OK
  - 2025-04-09T18:24:24.000Z 2 072770316734 eni-0e686673d4a8300e3 10.5.2.199 10.0.0.193 3306 50648 6 7 838 1744223064 1744223072 ACCEPT OK
  - 2025-04-09T18:24:24.000Z 2 072770316734 eni-0e686673d4a8300e3 10.0.0.193 10.5.2.199 50616 3306 6 8 617 1744223087 1744223088 ACCEPT OK
  - 2025-04-09T18:24:47.000Z 2 072770316734 eni-0e686673d4a8300e3 10.5.2.199 10.0.0.193 3306 50616 6 6 428 1744223087 1744223088 ACCEPT OK
- No newer events at this moment. Auto retrying... [Pause](#)

**Bottom Monitor (AWS Academy Assignment):**

- Assignment: Guided lab: Creating a VPC Peering Connection
- Due: No Due Date
- Points: 56
- Status: Submitting an external tool
- Score: 30/30
- Tasks completed:
  - [Task 1A] Peering Connection Created
  - [Task 1B] Requester is Lab VPC
  - [Task 1C] Acceptor is Shared-VPC
  - [Task 2A] Public Route created on peering connection
  - [Task 2B] Private Route created on peering connection
- Description of Task 18 (ShareVPCFlowLogs):
 

18. Below Destination name, choose the hyperlink [ShareVPCFlowLogs](#) to display the CloudWatch log group that was created.

Note: Refresh after few minutes if you get a message that says *Log group does not exist*.

Keep this window open.
- Task 4: Testing the VPC peering connection
- Description: Now that you configured VPC peering, you will test the VPC peering connection. You will perform the test by configuring the inventory application to access the database across the peering connection.

The screenshot shows a browser window with the URL [awsacademy.instructure.com/courses/104153/assignments/1147525/module\\_item\\_id=9702697](https://awsacademy.instructure.com/courses/104153/assignments/1147525/module_item_id=9702697). The page title is "Guided lab: Creating a VPC Peering Connection". The left sidebar includes links for Home, Modules, Discussions, Grades, and Lucid (Whiteboard). The main content area displays a "Submission Report" window with the following log:

```
[Executed at: Wed Apr 9 11:26:08 PDT 2025]
Testing report - Lab-Peer was created and is active.
Testing report - Good job! Lab VPC is the Requester for Lab-Peer.
Testing report - Good job! Shared VPC is the Acceptor for Lab-Peer.
Testing report - Good! Lab Public Route Table is correct.
Testing report - Shared-VPC Route Table is correct.
Testing report - Success! Application is connected to the database.
```

Below the log, a section titled "Task 4: Testing the VPC peering connection" instructs the user to perform a test by configuring the inventory application to access the database across the peering connection. The task status is shown as 00/30 completed.

## MODULE 8 KNOWLEDGE CHECK:

The screenshot shows a browser window with the URL [awsacademy.instructure.com/courses/104153/assignments/1147561/module\\_item\\_id=9702696](https://awsacademy.instructure.com/courses/104153/assignments/1147561/module_item_id=9702696). The page title is "ACAv3EN-US-LTI13-104153 > Assignments > Module 8 Knowledge Check". The left sidebar includes links for Home, Modules, Discussions, Grades, and Lucid (Whiteboard). The main content area displays a "Knowledge check results" window with the following information:

**KEYBOARD NAVIGATION**

Your score:	100% (100 points)
Required score:	70% (70 points)

**Result:** Congratulations! You have completed this knowledge check.  
To continue, choose Next in the lower-right corner.

## QUESTIONS:

1. Can you peer 2 VPCs that have the same CIDR ranges? Why?

No, we cannot peer two VPCs with overlapping CIDR blocks because routing will become ambiguous—the network won't know which destination is which, leading to potential IP conflicts and incorrect routing.

2. What route changes do you need to make after creating a peering connection?

we need to update the route tables in both VPCs to:

- Add a route to the peer VPC's CIDR block.
- Set the target as the peering connection.

This allows traffic to flow between the VPCs through the peering link.

3. If you have 3 VPCs: VPCA, VPCB, and VPCC; peering is configured between VPCA–VPCB and VPCB–VPCC, can you reach VPCC from VPCA? Why?

No, we cannot reach VPCC from VPCA because VPC peering is non-transitive. Even though both VPCA and VPCC are connected to VPCB, they cannot route traffic through it. we'd need to create a direct peering between VPCA and VPCC.