Task 5.3D

CLOUD COMPUTING

Creating a VPC Peering Connection

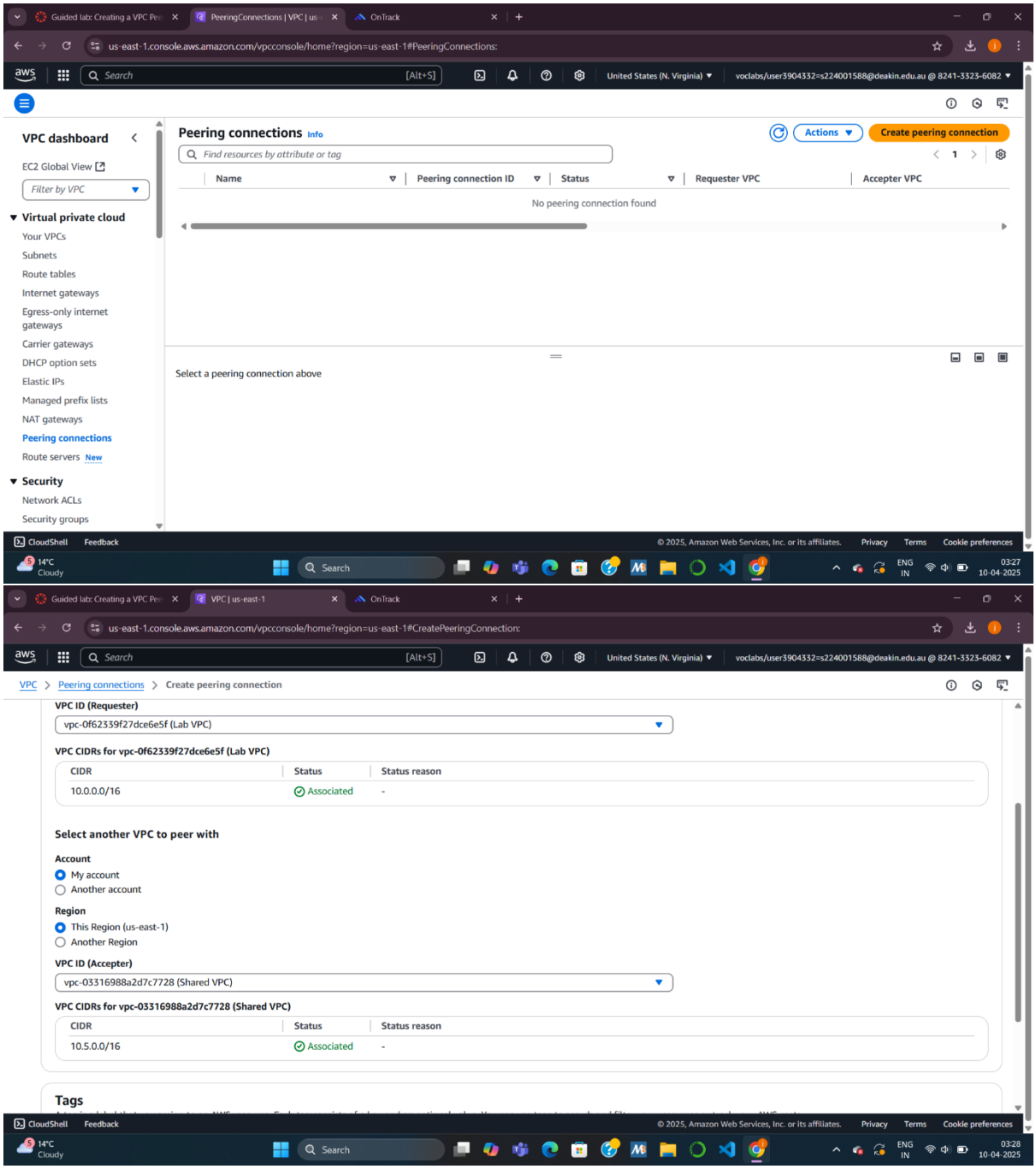
Task 1: Creating a VPC Peering Connection

What you're doing:

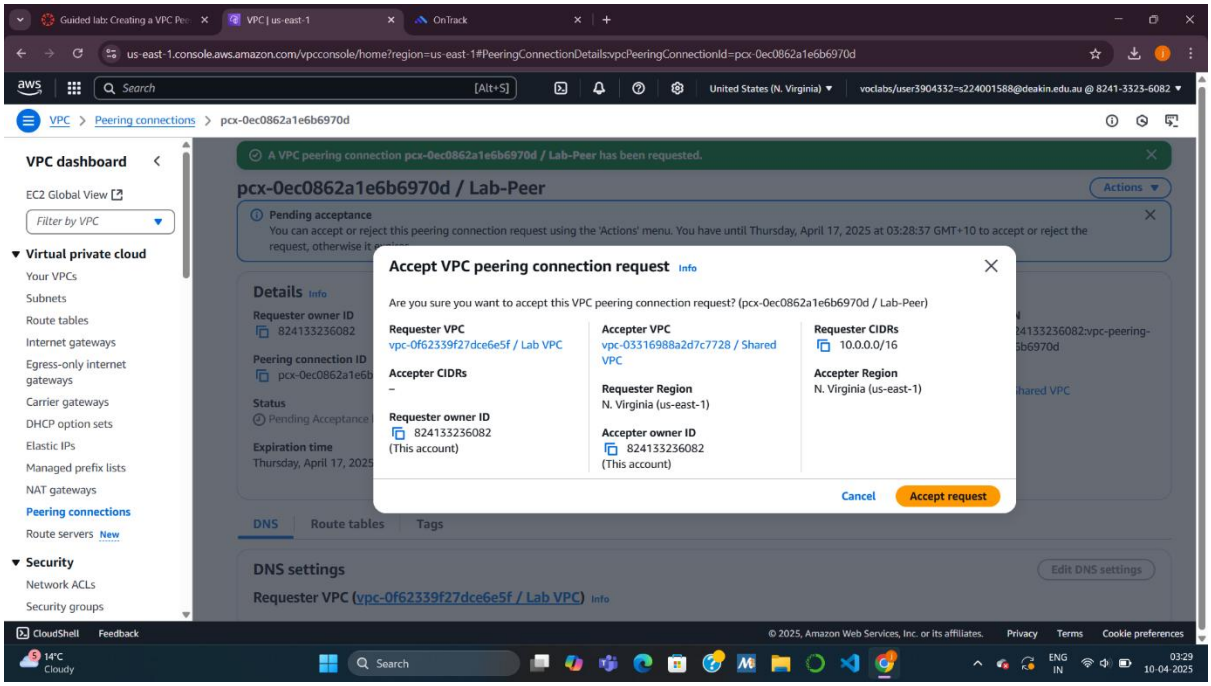
Establishing a **private link** between two VPCs—**Lab VPC** (has an EC2 application) and **Shared VPC** (has a database).

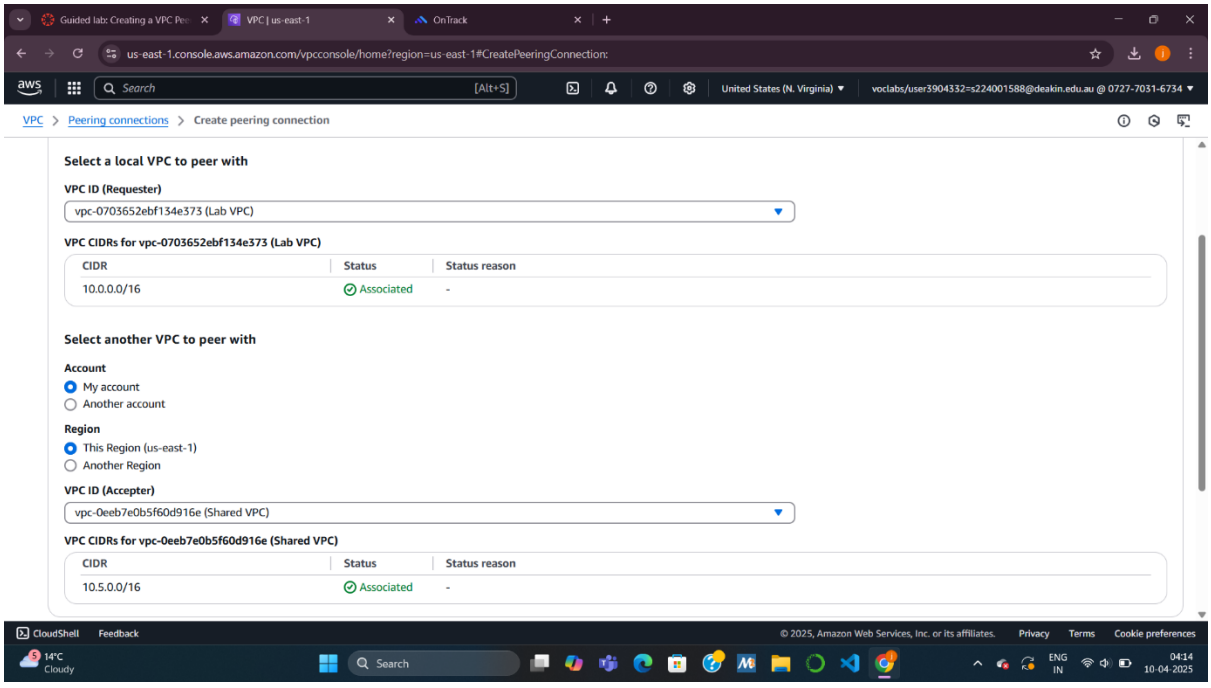
Steps:

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


Guided lab: Creating a VPC Pee
PeeringConnections | VPC | us-
OnTrack
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#PeeringConnections:
Search
[Alt+S]
United States (N. Virginia)
voclabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082
VPC dashboard
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
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Security groups
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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
14°C
Cloudy
Search
ENG
IN
03:27
10-04-2025

Guided lab: Creating a VPC Pee
VPC | us-east-1
OnTrack
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreatePeeringConnection:
Search
[Alt+S]
United States (N. Virginia)
voclabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082
VPC > Peering connections > Create peering connection
VPC ID (Requester)
vpc-0f62339f27dce6e5f (Lab VPC)
VPC CIDRs for vpc-0f62339f27dce6e5f (Lab VPC)
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-03316988a2d7c7728 (Shared VPC)
VPC CIDRs for vpc-03316988a2d7c7728 (Shared VPC)
CIDR
Status
Status reason
10.5.0.0/16
Associated
-
Tags
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
14°C
Cloudy
Search
ENG
IN
03:28
10-04-2025





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:

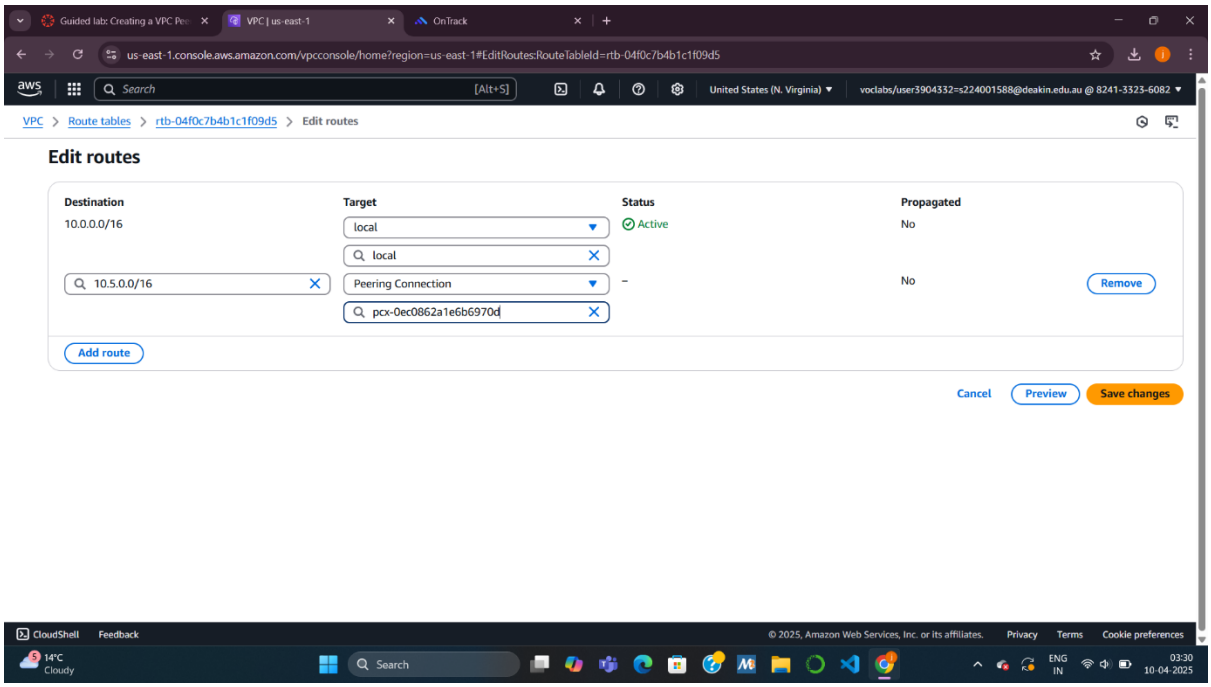
- Go to **Route Tables**.
- Select **Lab Public Route Table**.
- Add a route:

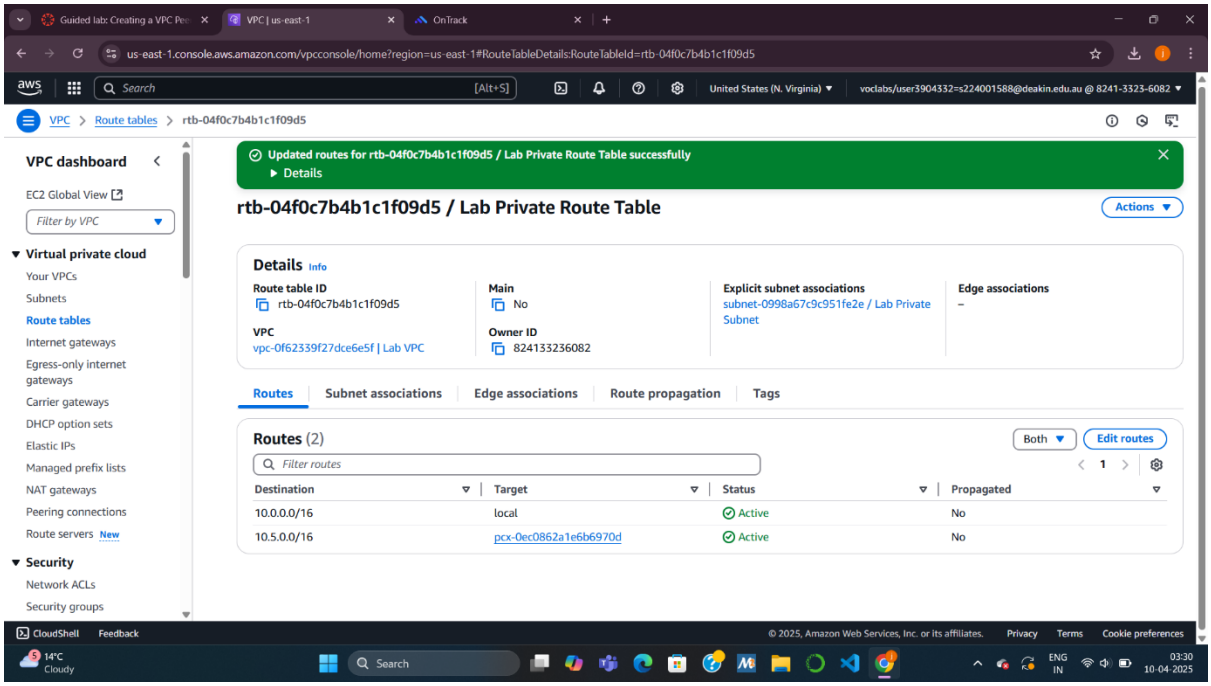
- **Destination**: 10.5.0.0/16 (CIDR of Shared VPC)
- **Target**: Peering connection Lab-Peer

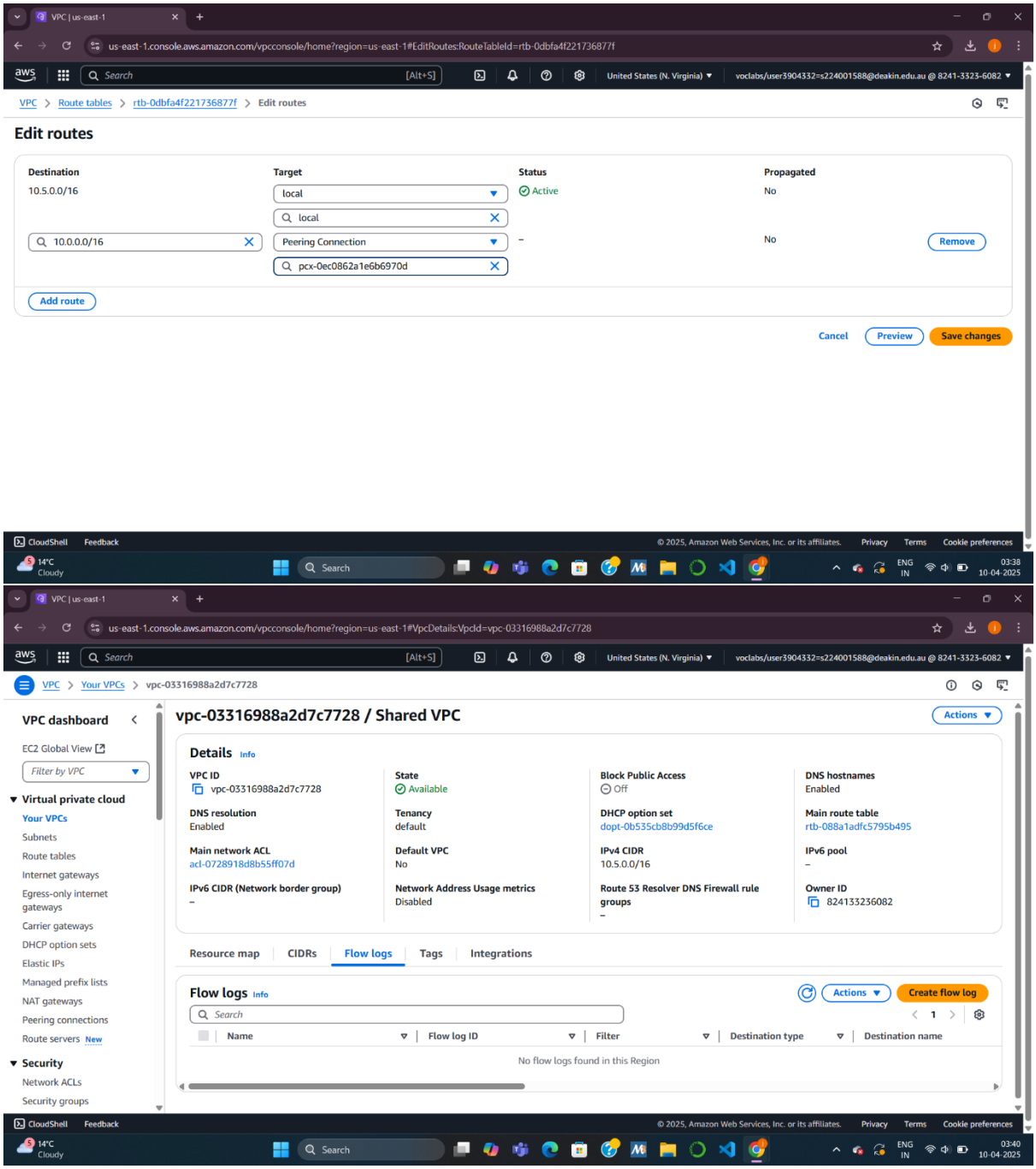
- Save changes.

For Shared VPC:

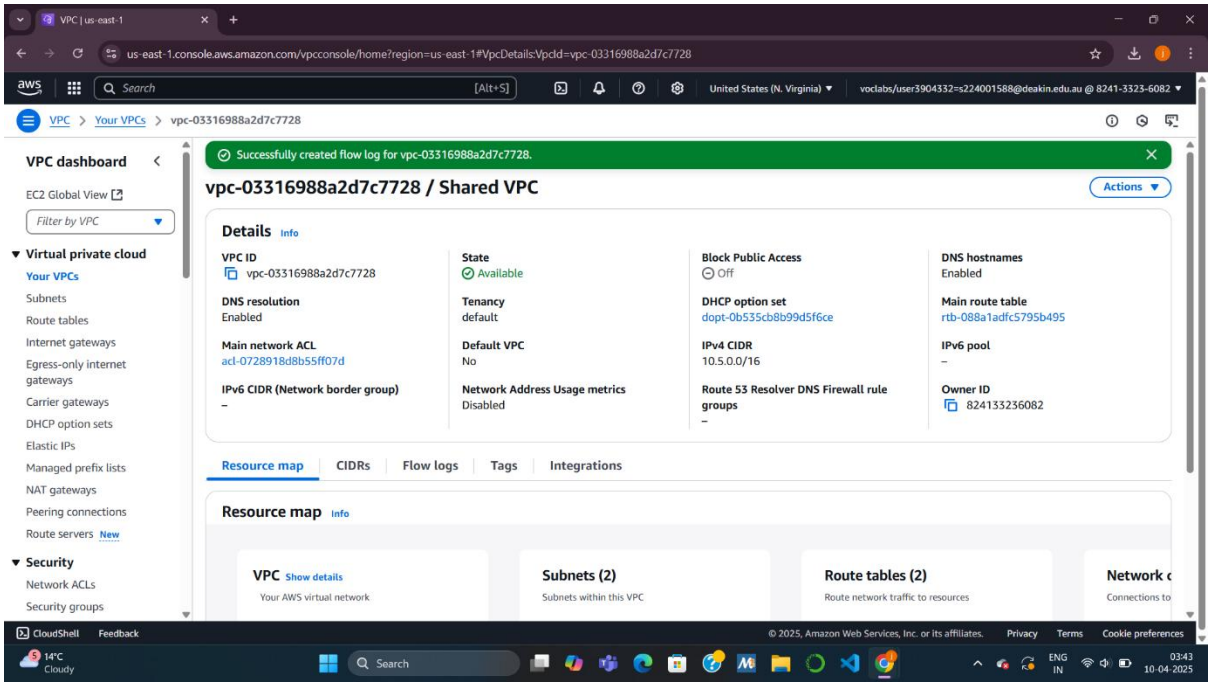
- Select **Shared-VPC Route Table**.
- Add a route:
  - **Destination**: 10.0.0.0/16 (CIDR of Lab VPC)
  - **Target**: Peering connection Lab-Peer
- Save changes.

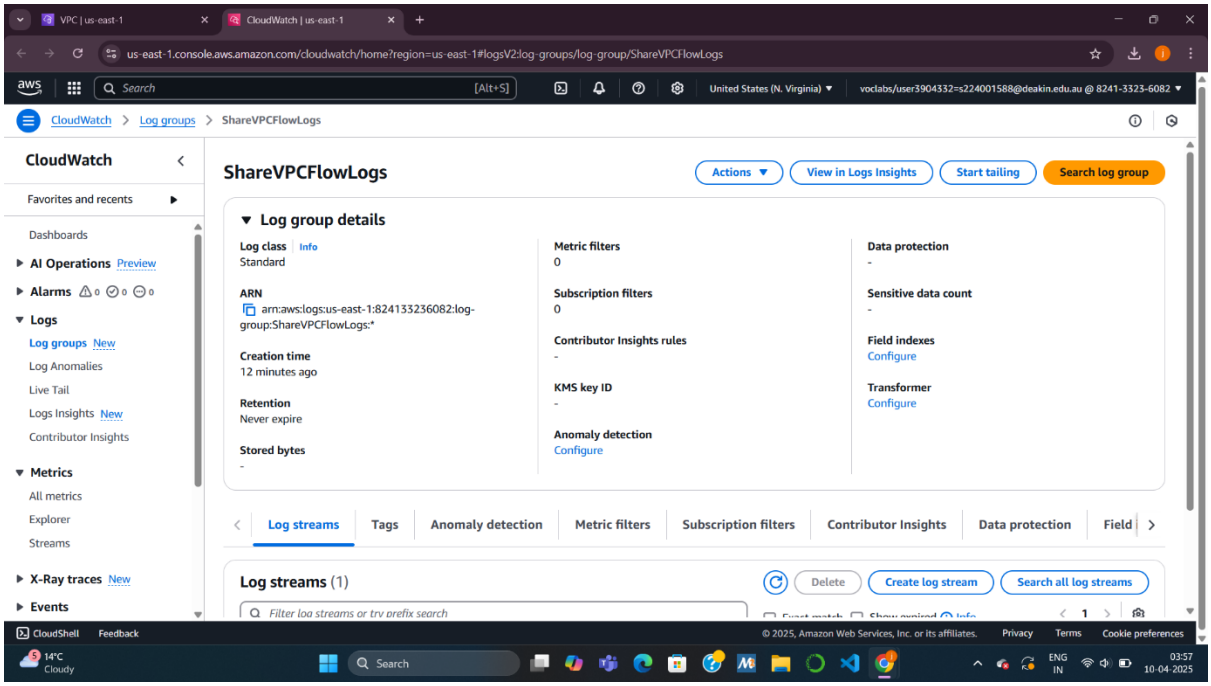


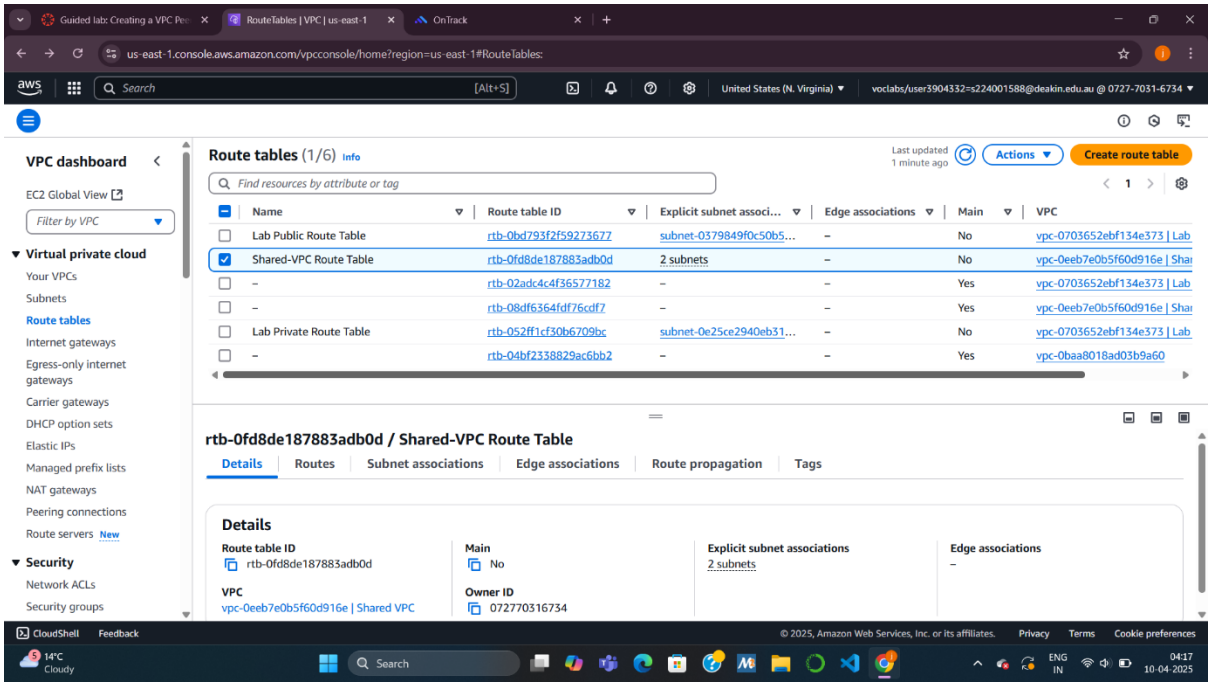

Guided lab: Creating a VPC Per
VPC | us-east-1
OnTrack
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-04f0c7b4b1c1f09d5
Search
[Alt+S]
United States (N. Virginia)
voclabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082
VPC
Route tables
rtb-04f0c7b4b1c1f09d5
VPC dashboard
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
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Security groups
Updated routes for rtb-04f0c7b4b1c1f09d5 / Lab Private Route Table successfully
Details
rtb-04f0c7b4b1c1f09d5 / Lab Private Route Table
Actions
Details Info
Route table ID
rtb-04f0c7b4b1c1f09d5
Main
No
Explicit subnet associations
subnet-0998a67c9c951fe2e / Lab Private Subnet
Edge associations
–
VPC
vpc-0f62339f27dce6e5f | Lab VPC
Owner ID
824133236082
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No
10.5.0.0/16
pcx-0ec0862a1e6b6970d
Active
No
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
14°C
Cloudy
Search
ENG
IN
03:30
10-04-2025


VPC | us-east-1
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditRoutes:RouteTableId=rtb-0dbfa4f221736877f
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
local
10.0.0.0/16
Peering Connection
–
No
Remove
pcx-0ec0862a1e6b6970d
Add route
Cancel
Preview
Save changes
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
14°C
Cloudy
Search
ENG
IN
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
Search [Alt+S]
United States (N. Virginia)
voclabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082
VPC > Your VPCs > vpc-03316988a2d7c7728
VPC dashboard
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
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Security groups
vpc-03316988a2d7c7728 / Shared VPC
Actions
Details Info
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-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
CIDRs
Flow logs
Tags
Integrations
Flow logs Info
Actions
Create flow log
Search
Name
Flow log ID
Filter
Destination type
Destination name
No flow logs found in this Region
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
14°C
Cloudy
Search
ENG
IN
03:40
10-04-2025


VPC | us-east-1
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#VpcDetails:VpcId=vpc-03316988a2d7c7728
Search [Alt+S]
United States (N. Virginia)
voclabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082
VPC > Your VPCs > vpc-03316988a2d7c7728
VPC dashboard
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
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Security groups
Successfully created flow log for vpc-03316988a2d7c7728.
vpc-03316988a2d7c7728 / Shared VPC
Actions
Details Info
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-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
CIDRs
Flow logs
Tags
Integrations
Resource map Info
VPC Show details
Your AWS virtual network
Subnets (2)
Subnets within this VPC
Route tables (2)
Route network traffic to resources
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
14°C
Cloudy
Search
ENG
IN
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
Search [Alt+S]
United States (N. Virginia)
voclabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082
CloudWatch > Log groups > ShareVPCFlowLogs
CloudWatch
Favorites and recents
Dashboards
AI Operations Preview
Alarms
Logs
Log groups New
Log Anomalies
Live Tail
Logs Insights New
Contributor Insights
Metrics
All metrics
Explorer
Streams
X-Ray traces New
Events
ShareVPCFlowLogs
Actions
View in Logs Insights
Start tailing
Search log group
Log group details
Log class Info
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
Configure
Transformer
Configure
Log streams
Tags
Anomaly detection
Metric filters
Subscription filters
Contributor Insights
Data protection
Field
Log streams (1)
Delete
Create log stream
Search all log streams
Filter log streams or try prefix search
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
14°C
Cloudy
Search
ENG
IN
03:57
10-04-2025



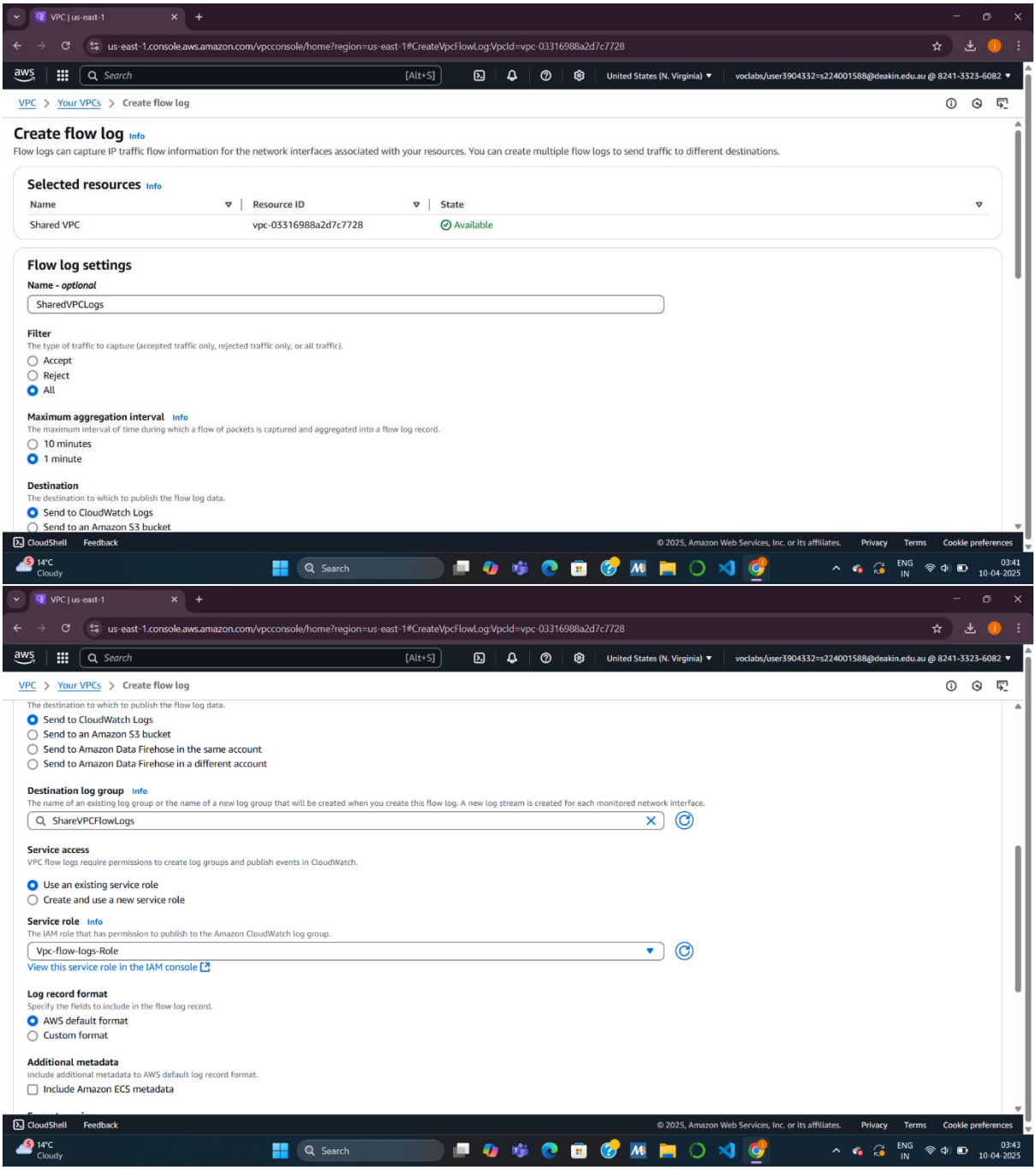
Task 3: Enabling VPC Flow Logs

What you're doing:

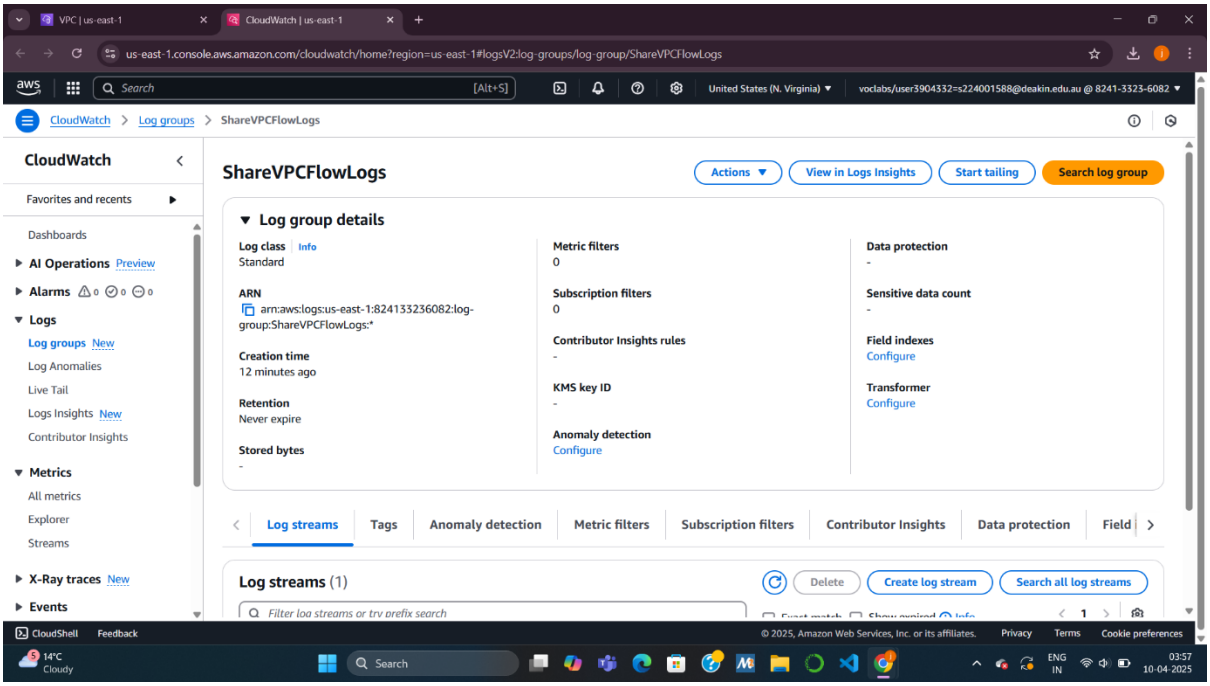
Setting up **logs** to monitor network traffic **in Shared VPC**.

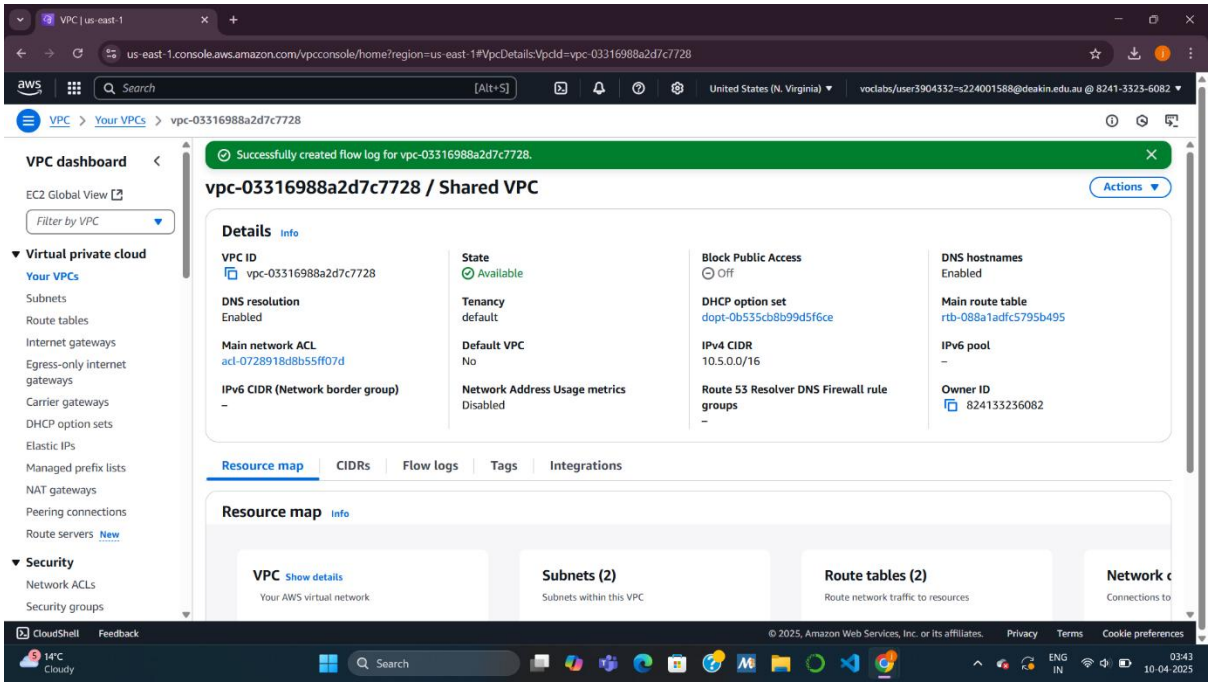
Steps:

- 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
Search [Alt+S]
United States (N. Virginia)
voclabs/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
SharedVPCLogs
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
14°C
Cloudy
Search
ENG
IN
03:41
10-04-2025

VPC | us-east-1
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateVpcFlowLog:VpcId=vpc-03316988a2d7c7728
Search [Alt+S]
United States (N. Virginia)
voclabs/user3904332=s224001588@deakin.edu.au @ 8241-3323-6082
VPC > Your VPCs > Create flow log
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.
ShareVPCFlowLogs
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.
Vpc-flow-logs-Role
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
14°C
Cloudy
Search
ENG
IN
03:43
10-04-2025





Task 4: Testing the VPC Peering Connection

What you're doing:

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

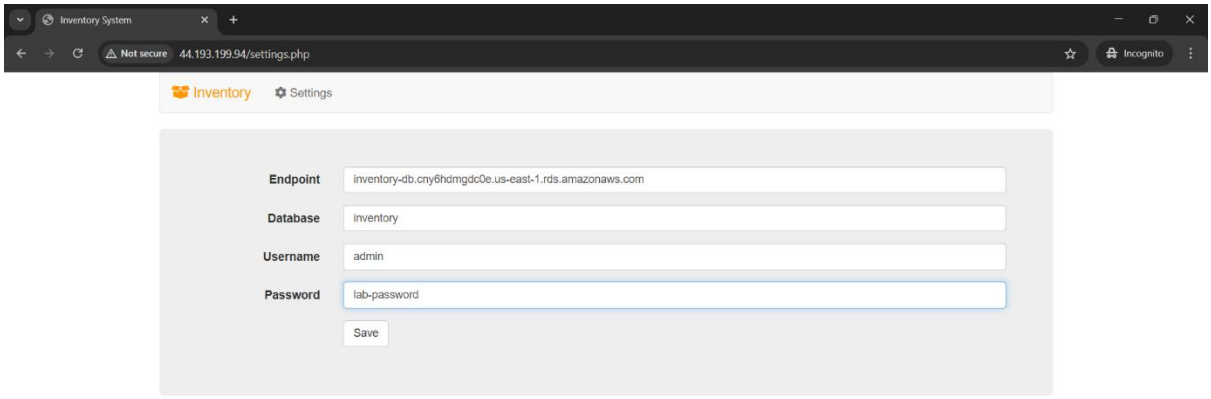
Steps:

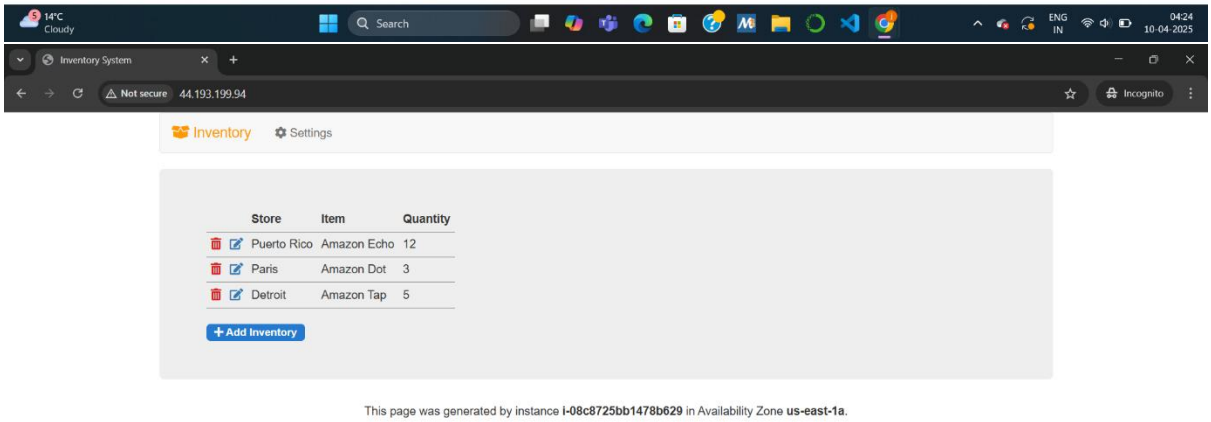
- Copy the **public IP of the EC2** from AWS Details, open in browser.
- You'll see the **inventory app** asking to configure database.
- Click **Settings**:

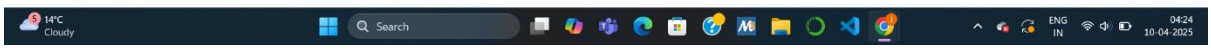
- Enter **database endpoint**, DB name, username, password.

- 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.







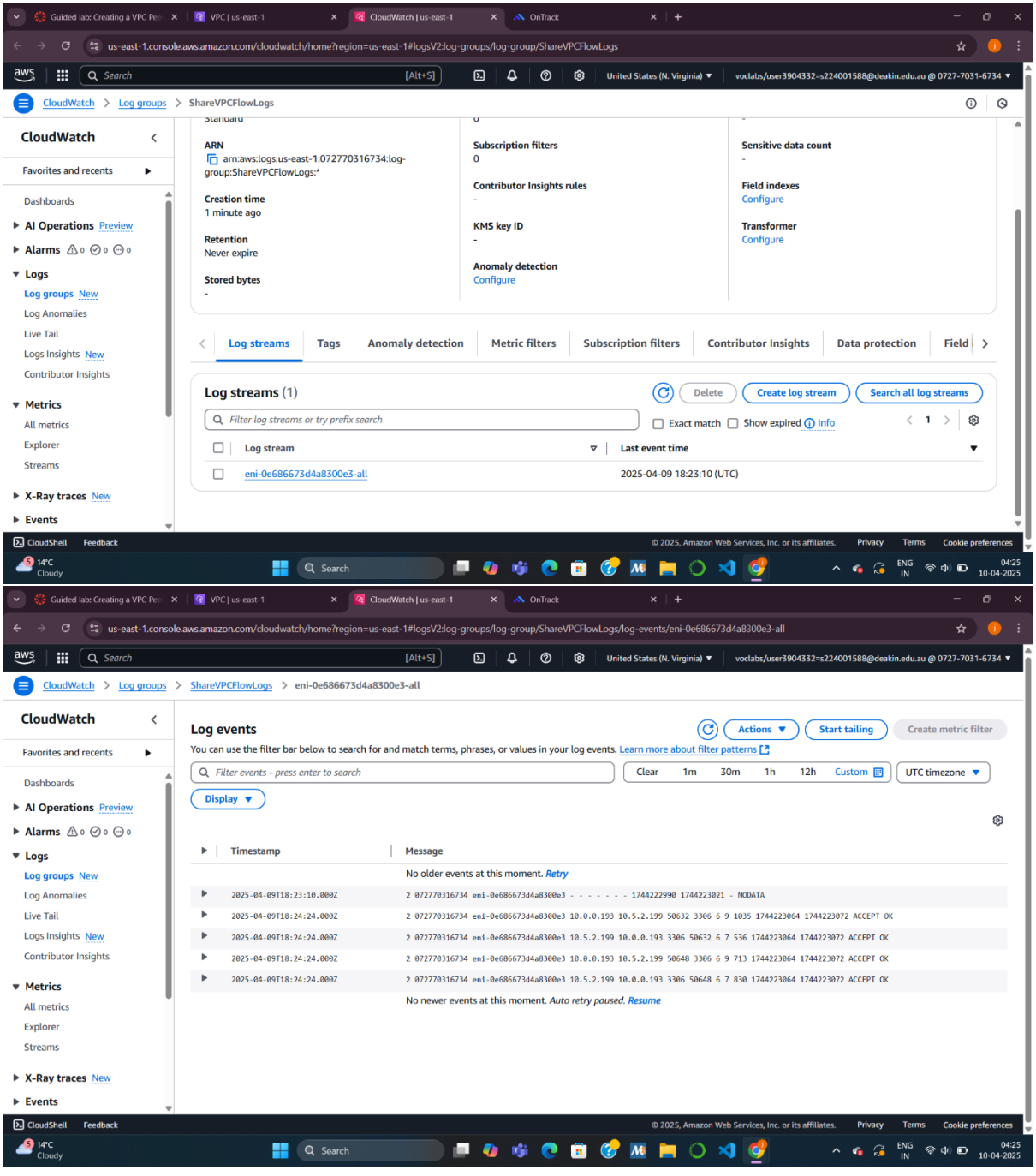
Task 5: Analyzing the VPC Flow Logs

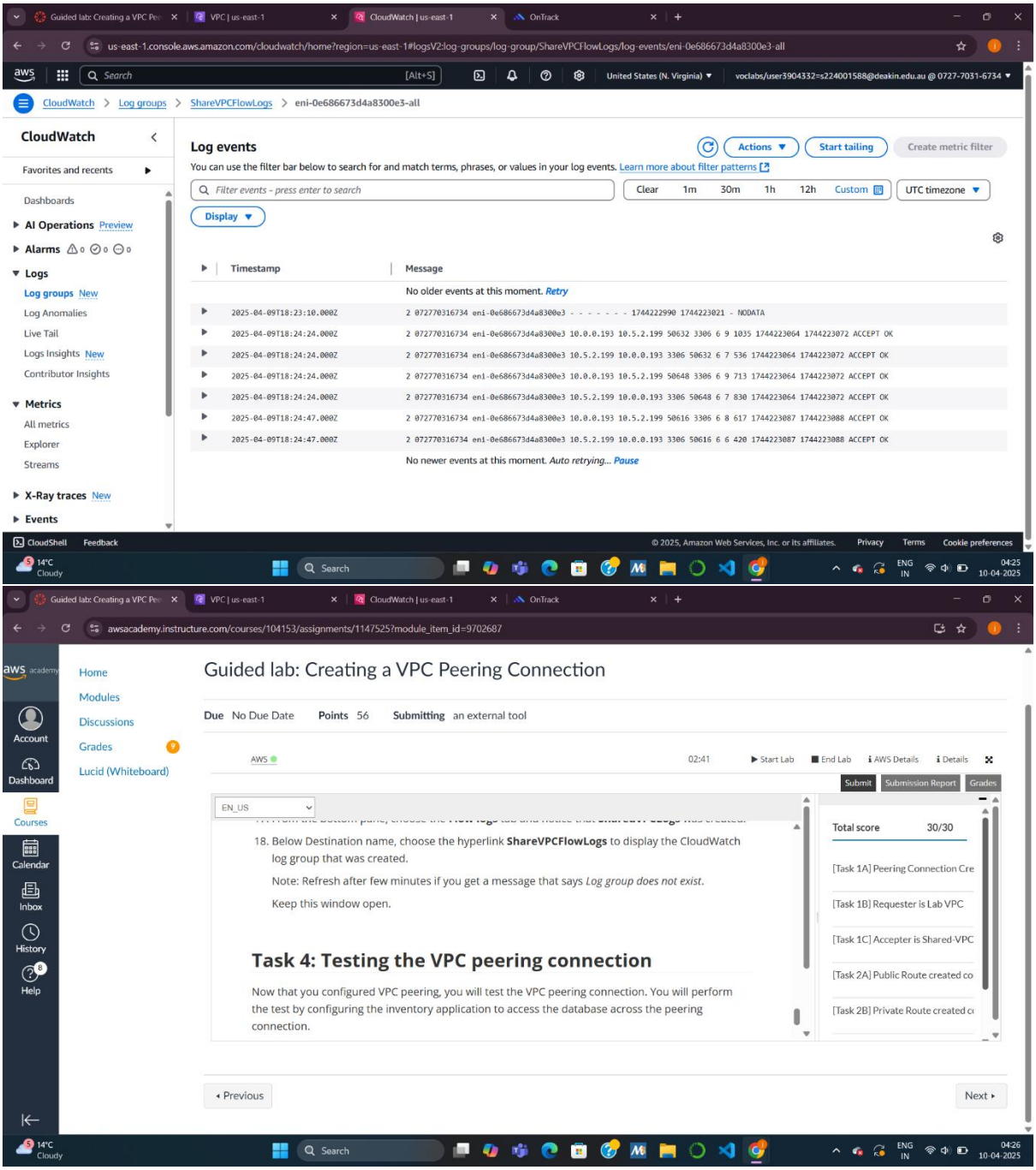
What you're doing:

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

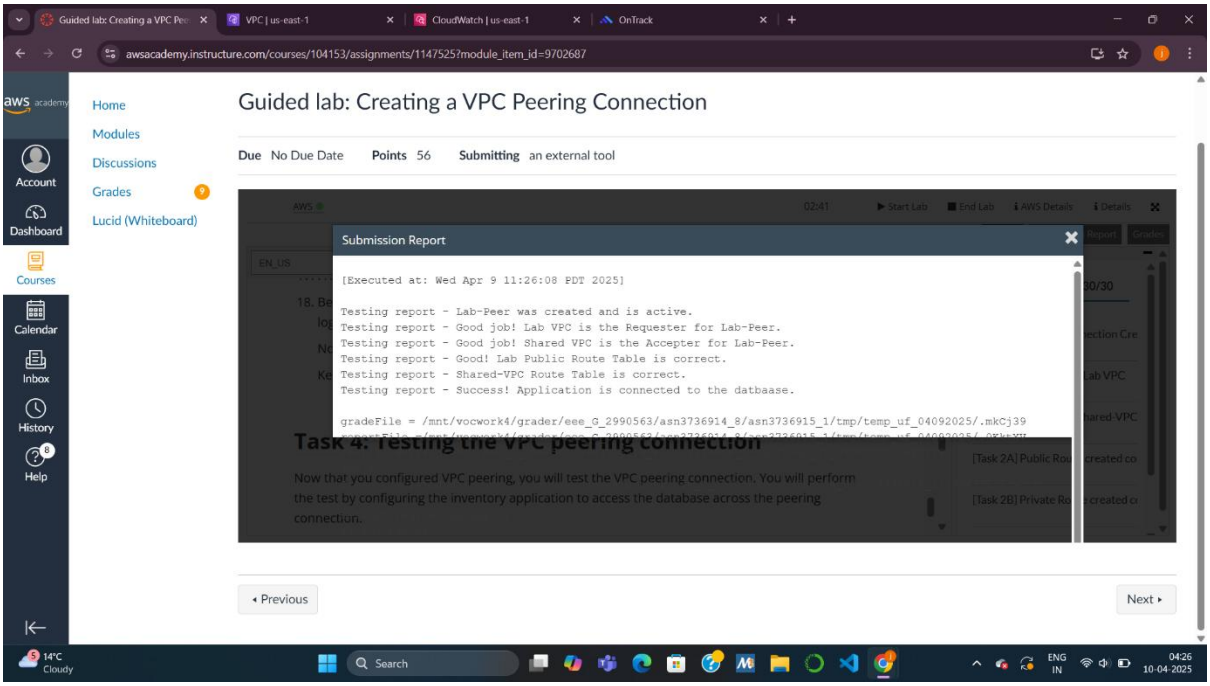
Steps:

- 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**.

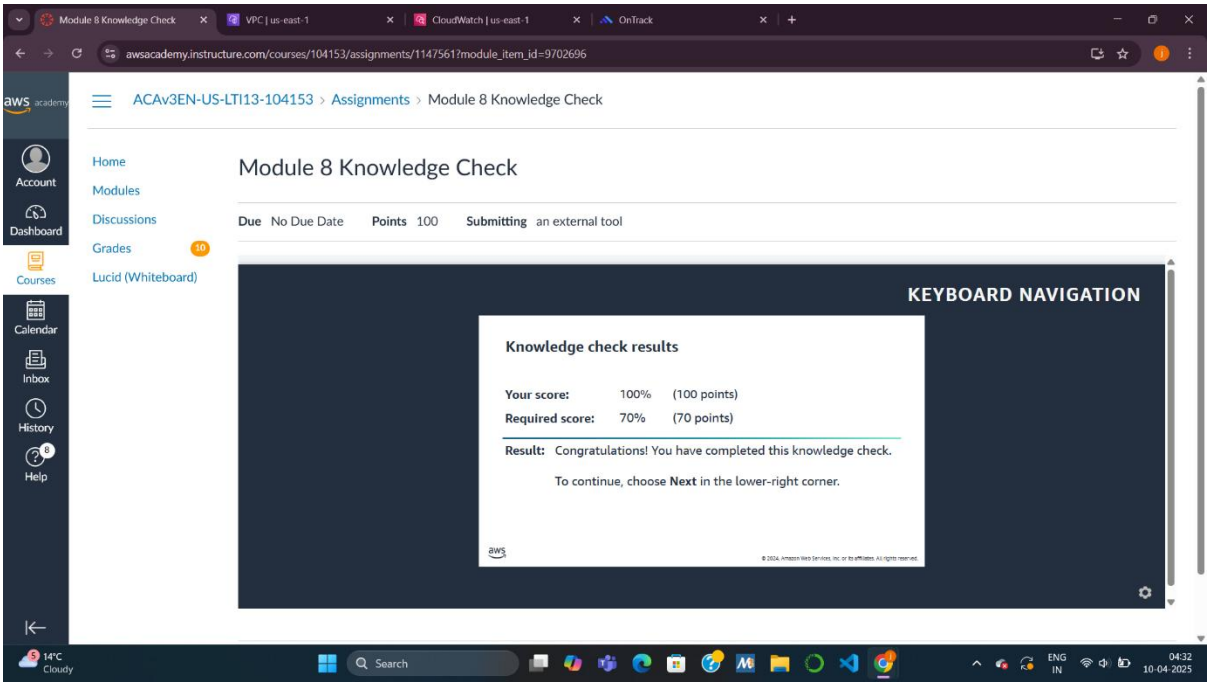



Guided lab: Creating a VPC Pe
VPC | us-east-1
CloudWatch | us-east-1
OnTrack
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/ShareVPCFlowLogs/log-events/eni-0e686673d4a8300e3-all
Search [Alt+S]
United States (N. Virginia)
voclabs/user3904332=s224001588@deakin.edu.au @ 0727-7031-6734
CloudWatch > Log groups > ShareVPCFlowLogs > eni-0e686673d4a8300e3-all
CloudWatch
Favorites and recents
Dashboards
AI Operations Preview
Alarms 0 0 0
Logs
Log groups New
Log Anomalies
Live Tail
Logs Insights New
Contributor Insights
Metrics
All metrics
Explorer
Streams
X-Ray traces New
Events
Log events
Actions
Start tailing
Create metric filter
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns
Filter events - press enter to search
Clear 1m 30m 1h 12h Custom
UTC timezone
Display
Timestamp
Message
No older events at this moment. Retry
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
2025-04-09T18:24:47.000Z 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 6 420 1744223087 1744223088 ACCEPT OK
No newer events at this moment. Auto retrying... Pause
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
14°C Cloudy
Search
ENG IN
04:25 10-04-2025

Guided lab: Creating a VPC Pe
VPC | us-east-1
CloudWatch | us-east-1
OnTrack
awsacademy.instructure.com/courses/104153/assignments/1147525?module_item_id=9702687
Home
Modules
Discussions
Grades
Lucid (Whiteboard)
Account
Dashboard
Courses
Calendar
Inbox
History
Help
Guided lab: Creating a VPC Peering Connection
Due No Due Date Points 56 Submitting an external tool
AWS
02:41
Start Lab
End Lab
AWS Details
Details
Submit
Submission Report
Grades
EN_US
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
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.
Total score 30/30
[Task 1A] Peering Connection Cre
[Task 1B] Requester is Lab VPC
[Task 1C] Accepter is Shared-VPC
[Task 2A] Public Route created co
[Task 2B] Private Route created c
Previous
Next
14°C Cloudy
Search
ENG IN
04:26 10-04-2025



MODULE 8 KNOWLEDGE CHECK:



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.