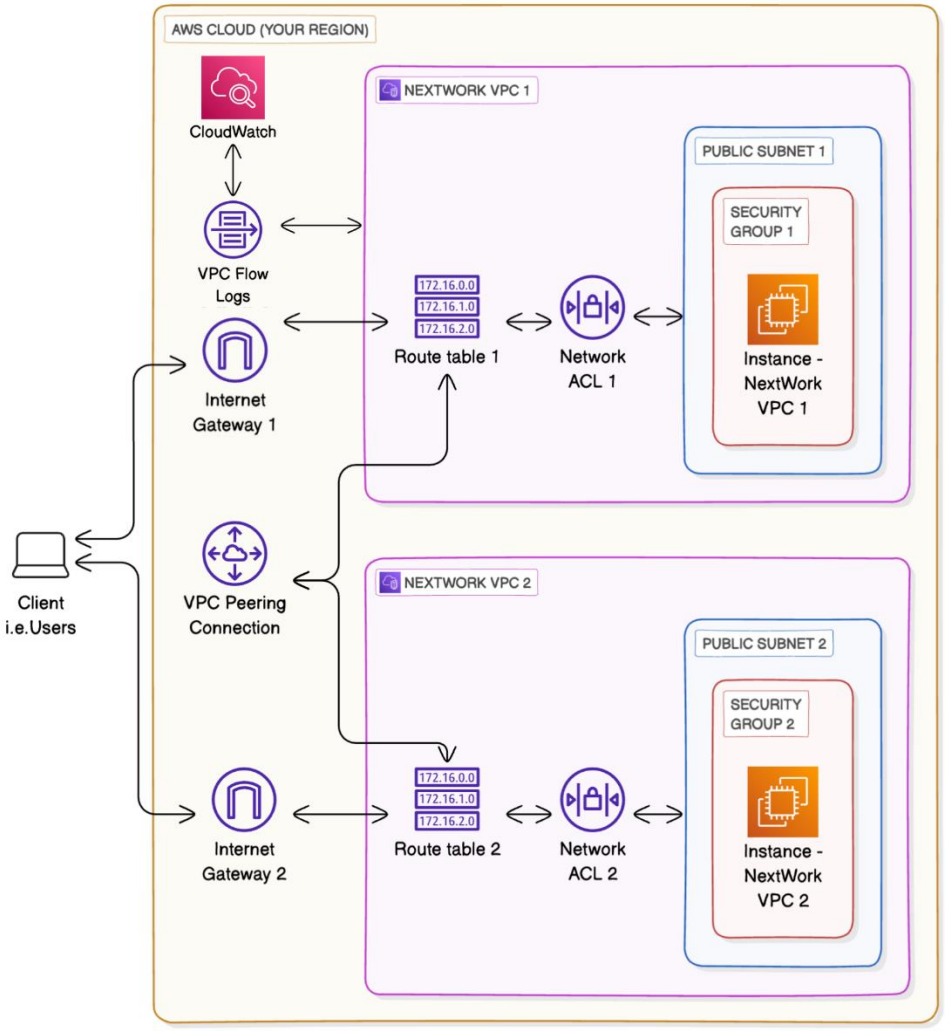
VPC Monitoring with Flow Logs

Get ready to:

1. Set up two VPCs and test their peering connection.
2. Set up VPC Flow Logs that collect network traffic data.
3. Analyse network traffic using CloudWatch's Log Insights.

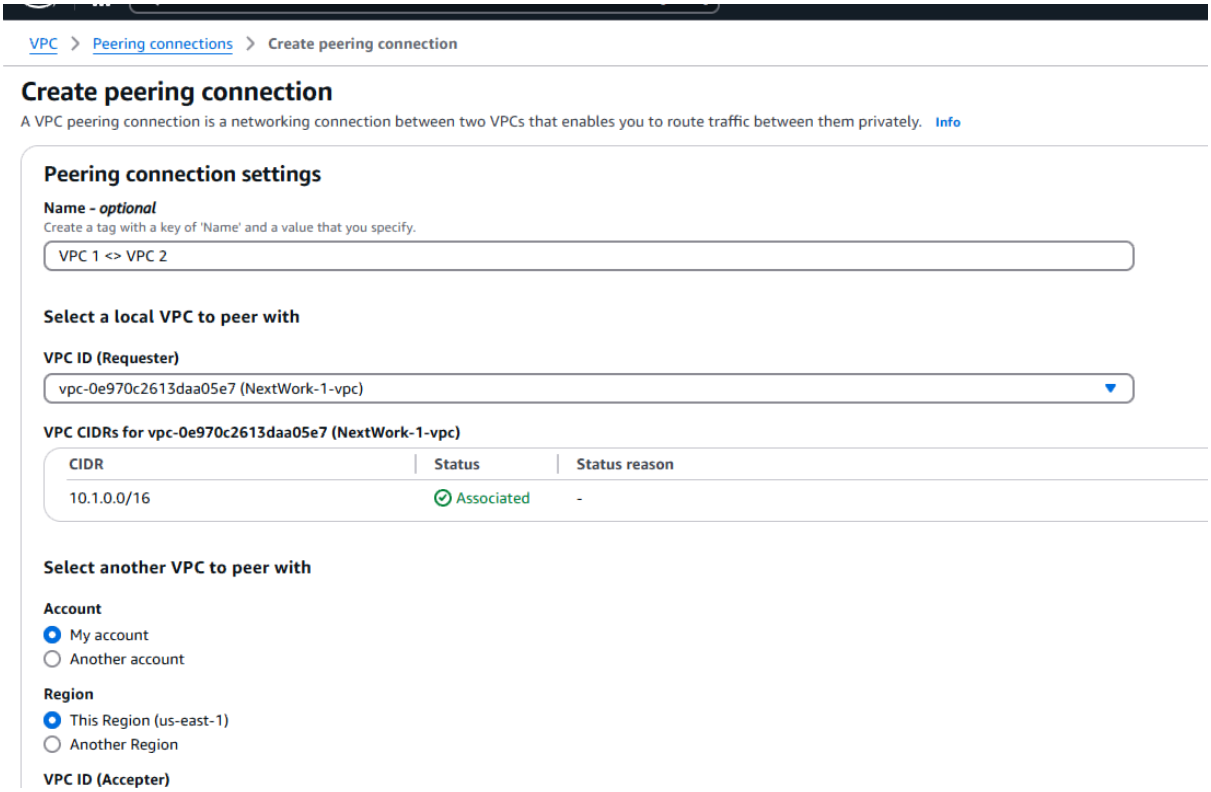


Create a Peering Connection and Configure Route Tables

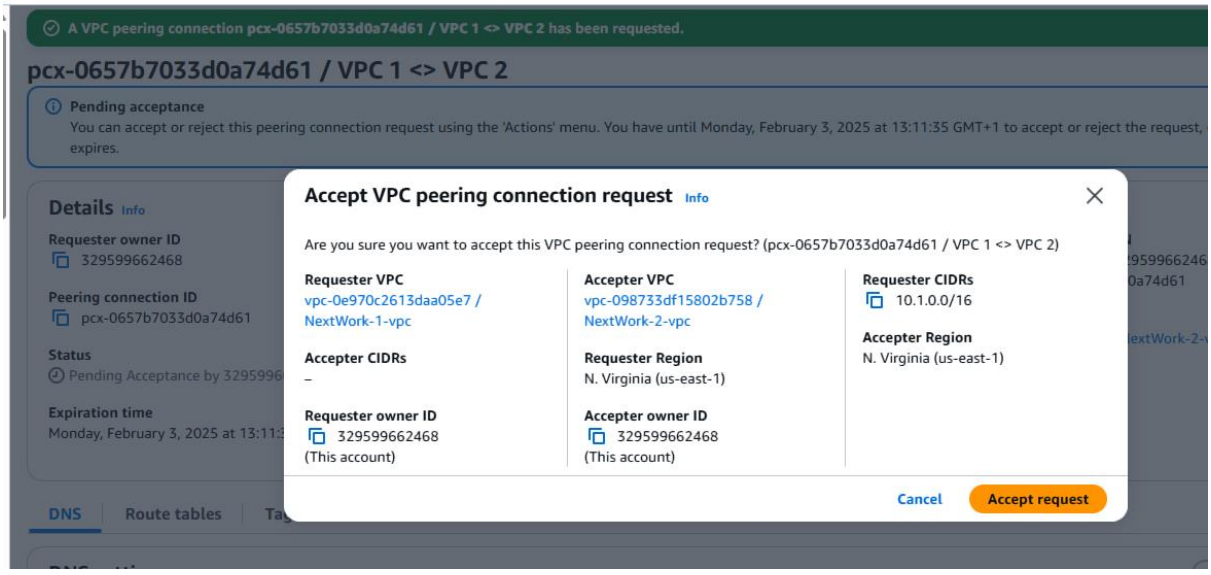
Head to the VPC console, click on **Peering connections** on the left-hand navigation panel.

Click on **Create peering connection** in the right-hand corner.

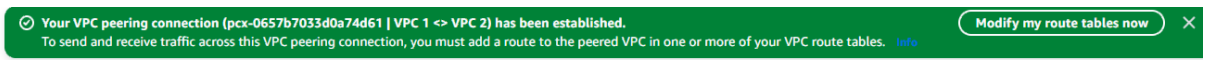
- Name your **Peering connection name** as VPC 1 <> VPC 2
- Select **NextWork-1-VPC** for your **VPC ID (Requester).**
- Under **Select another VPC to peer with,** make sure **My Account** is selected.
- For **Region,** select **This Region.**
- For **VPC ID (Accepter)**, select **NextWork-2-VPC**
- Click on **Create peering connection.**



- Your newly created peering connection isn't finished yet! The green success bar says the peering connection **has been requested.**
- On the next screen, select **Actions** and then select **Accept request...**
- Click on **Accept request** again on the pop-up panel.



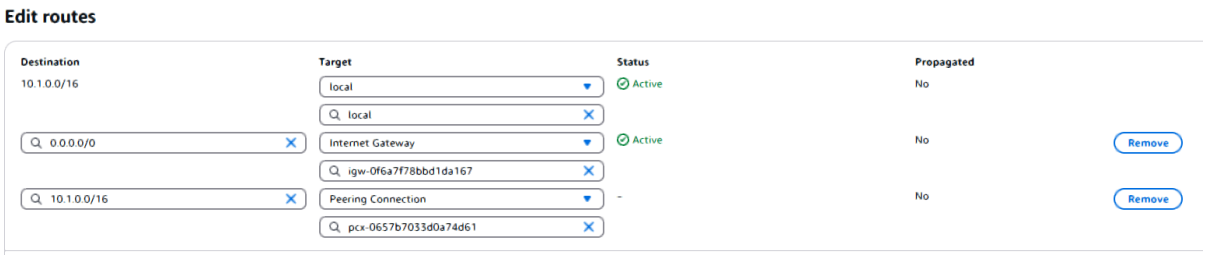
- Click on **Modify my route tables now** on the top right corner.



- A peering connection is all set now

Update VPC 1's route table

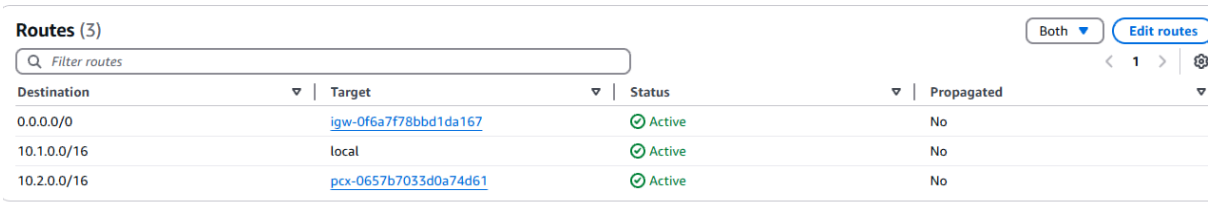
- Select the checkbox next to VPC 1's route table i.e. called **NextWork-1-rtb-public.**
- Scroll down and click on the **Routes** tab.
- Click **Edit routes.**
- Let's add a new route.
- Add a new route to **VPC 2** by entering the CIDR block 10.2.0.0/16 as our **Destination**.
- Under Target, select **Peering Connection.**
- Select **VPC 1 <> VPC 2**.



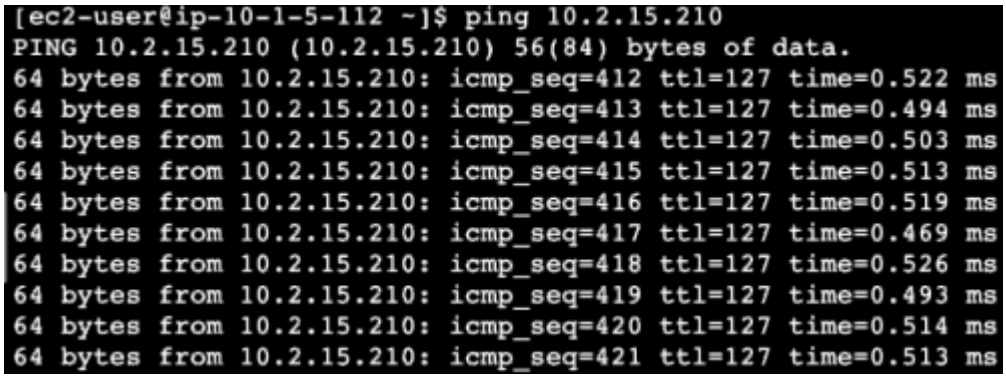
- Click **Save changes.**
- Confirm that the new route appears in VPC 1's **Routes** tab!

Update VPC 2's route table

- The route table you're updating is **NextWork-2-rtb-public.**
- The **Destination** is the CIDR block 10.1.0.0/16



- You save your changes
- Revisit the **EC2 Instance Connect** tab that's connected to NextWork Public Server.



- You've successfully resolved the connectivity issue by setting up a peering architecture between VPC 1 and VPC 2!

- As an extension (this is optional!), validate this by trying to run the same **ping command** from your **local terminal.**
- Do you get ping replies here too?

```
PING 10.2.15.210 (10.2.15.210): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
```

- You can quit your local terminal's session now! Validating DONE 😳
- Another optional extension! Back in your EC2 Instance Connect tab, run the same ping command but add -c 5 to the end of the command.
- Your final result should look like ping 10.2.15.210 -c 5

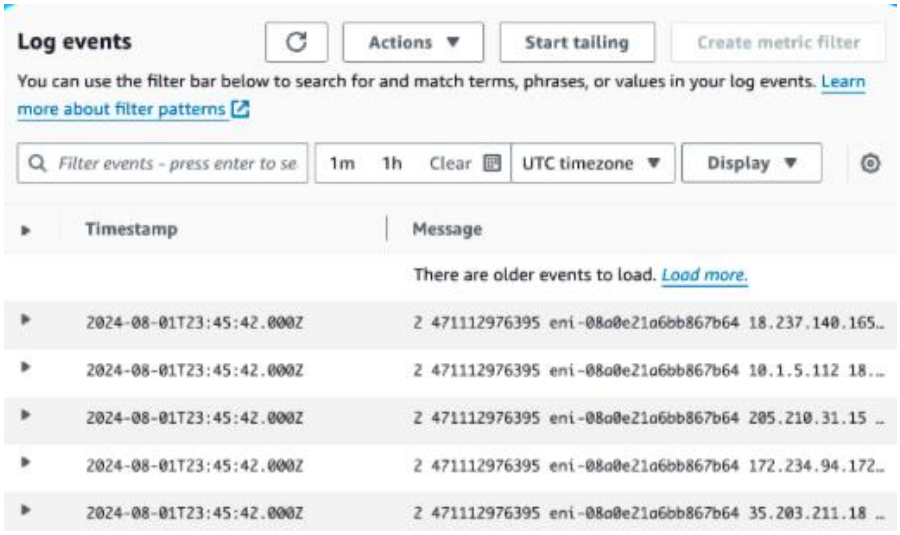
```
[ec2-user@ip-10-1-5-112 ~]$ ping 10.2.15.210 -c 5
PING 10.2.15.210 (10.2.15.210) 56(84) bytes of data.
64 bytes from 10.2.15.210: icmp_seq=1 ttl=127 time=0.539 ms
64 bytes from 10.2.15.210: icmp_seq=2 ttl=127 time=0.693 ms
64 bytes from 10.2.15.210: icmp_seq=3 ttl=127 time=0.500 ms
64 bytes from 10.2.15.210: icmp_seq=4 ttl=127 time=0.600 ms
64 bytes from 10.2.15.210: icmp_seq=5 ttl=127 time=0.537 ms

--- 10.2.15.210 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4141ms
rtt min/avg/max/mdev = 0.500/0.573/0.693/0.067 ms
```

Analyze Flow Logs

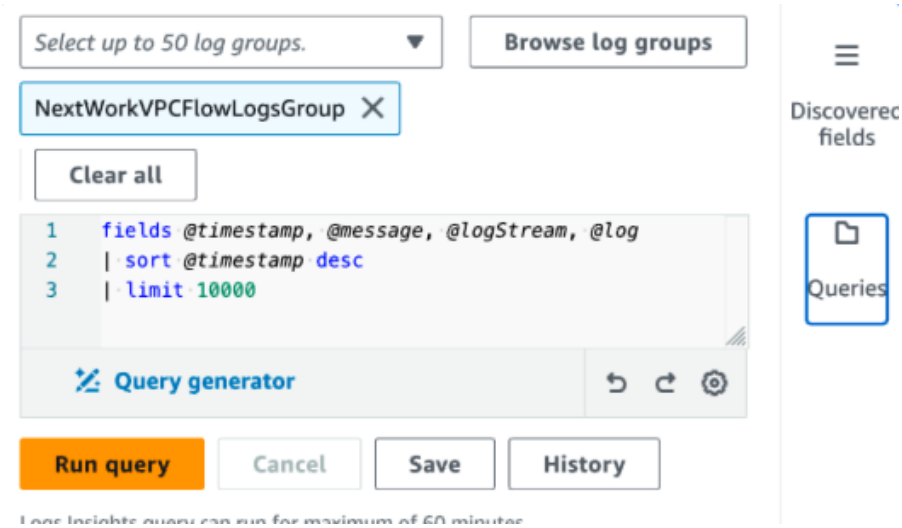
In this step, you're going to:

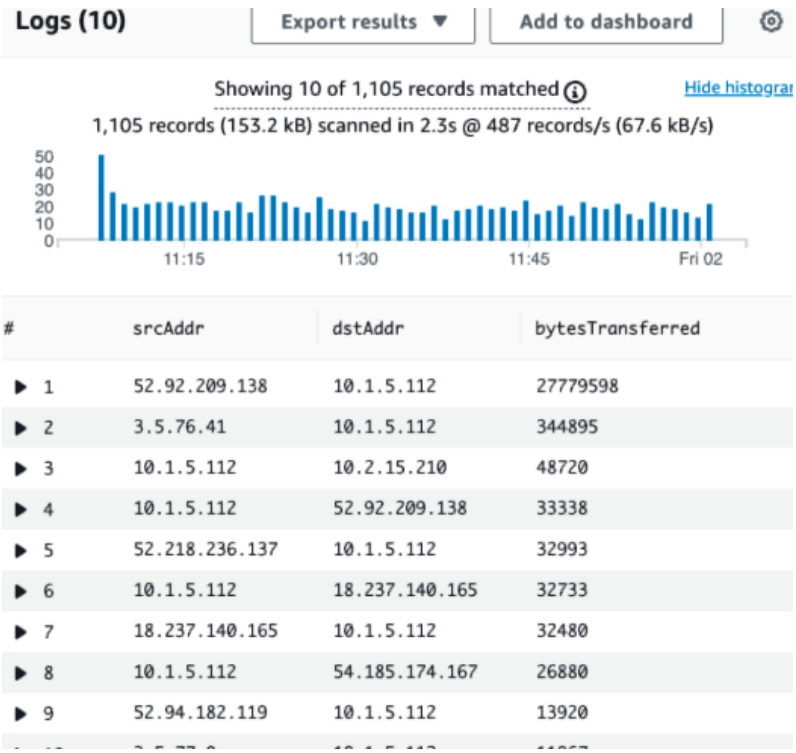
1. Review the flow logs recorded aboout VPC 1's public subnet.
2. Analyse the flow logs to get some tasty insights
3. Head to your **CloudWatch** console.
4. Select **Log groups** from the left-hand navigation panel.
5. Click into **NextWorkVPCFlowLogsGroup.**
6. Click into your log stream to see flow logs from EC2 Instance 1!



7. In the left-hand navigation panel, click on **Logs Insights.**
8. Select **NextWorkVPCFlowLogsGroup** from the **Select log group(s)** dropdown.
9. Select the **Queries** folder on the right-hand side.

10. Under **Flow Logs**, select **Top 10 byte transfers by source and destination IP addresses**.
11. Click **Apply,** and then **Run query.**





#	srcAddr	dstAddr	bytesTransferred
▶ 1	52.92.209.138	10.1.5.112	27779598
▶ 2	3.5.76.41	10.1.5.112	344895
▶ 3	10.1.5.112	10.2.15.210	48720
▶ 4	10.1.5.112	52.92.209.138	33338
▶ 5	52.218.236.137	10.1.5.112	32993
▶ 6	10.1.5.112	18.237.140.165	32733
▶ 7	18.237.140.165	10.1.5.112	32480
▶ 8	10.1.5.112	54.185.174.167	26880
▶ 9	52.94.182.119	10.1.5.112	13920