

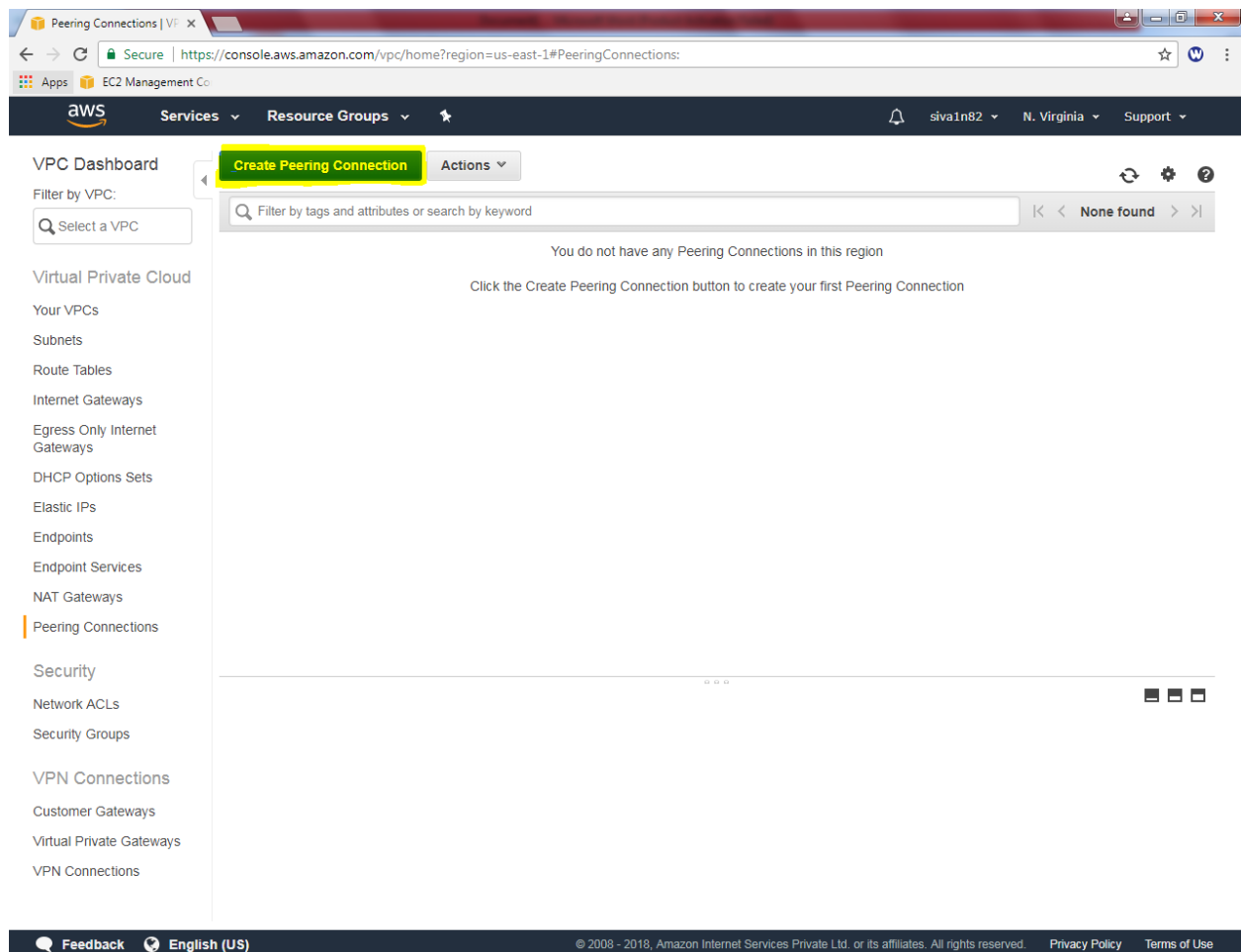
## Lab 12

### VPC Peering Lab – 3 of 3

Goto “N.Virginia”region,

Goto VPC Dashboard,

Click “Peering connections”



Click “Create Peering Connections”.

In peering Connection,

Peering Connection name tag: VPC Peer Ohio\_NVG

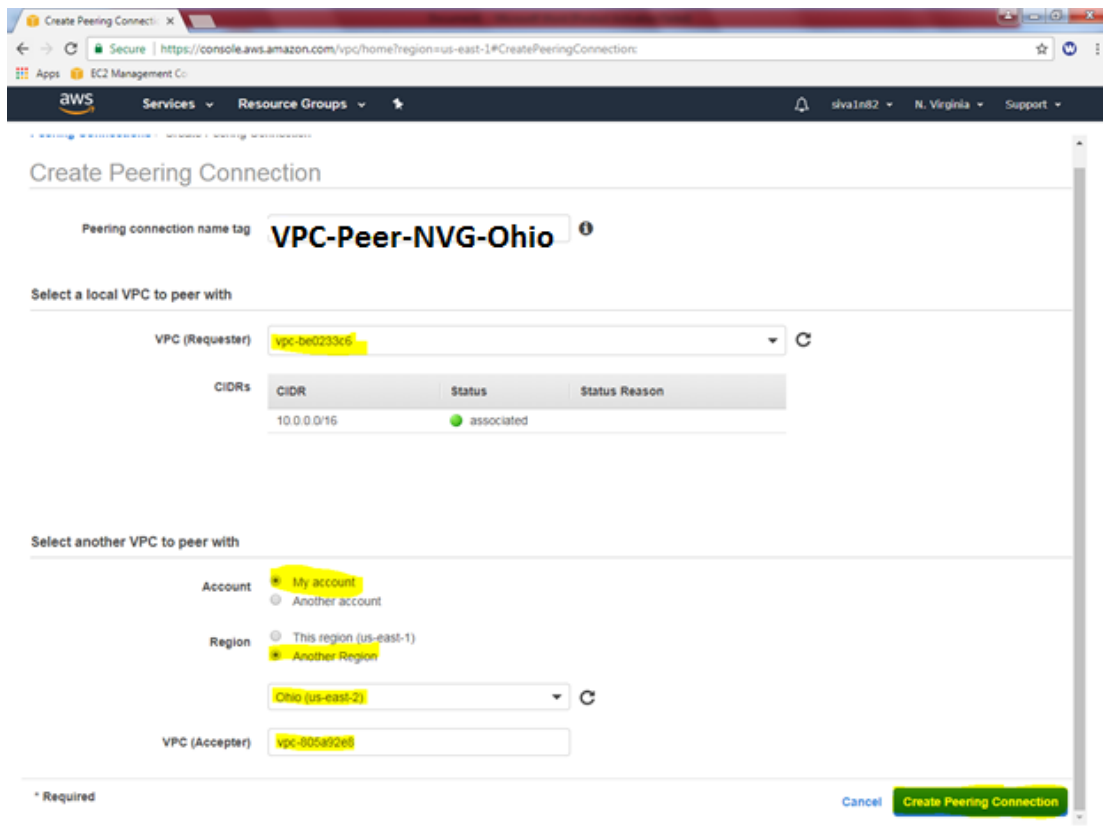
VPC Requestor : VPC\_North Virginia

Account : MyAccount

Region : Another Region

Select: Ohio

VPC Acceptor : VPC\_Ohio (type VPC ID of VPC Ohio).



Create Peering Connection

Peering connection name tag **VPC-Peer-NVG-Ohio**

Select a local VPC to peer with

VPC (Requester) **vpc-b60233c6**

CIDRs	Status	Status Reason
10.0.0.0/16	associated	

Select another VPC to peer with

Account **My account**

Region **Ohio (us-east-2)**

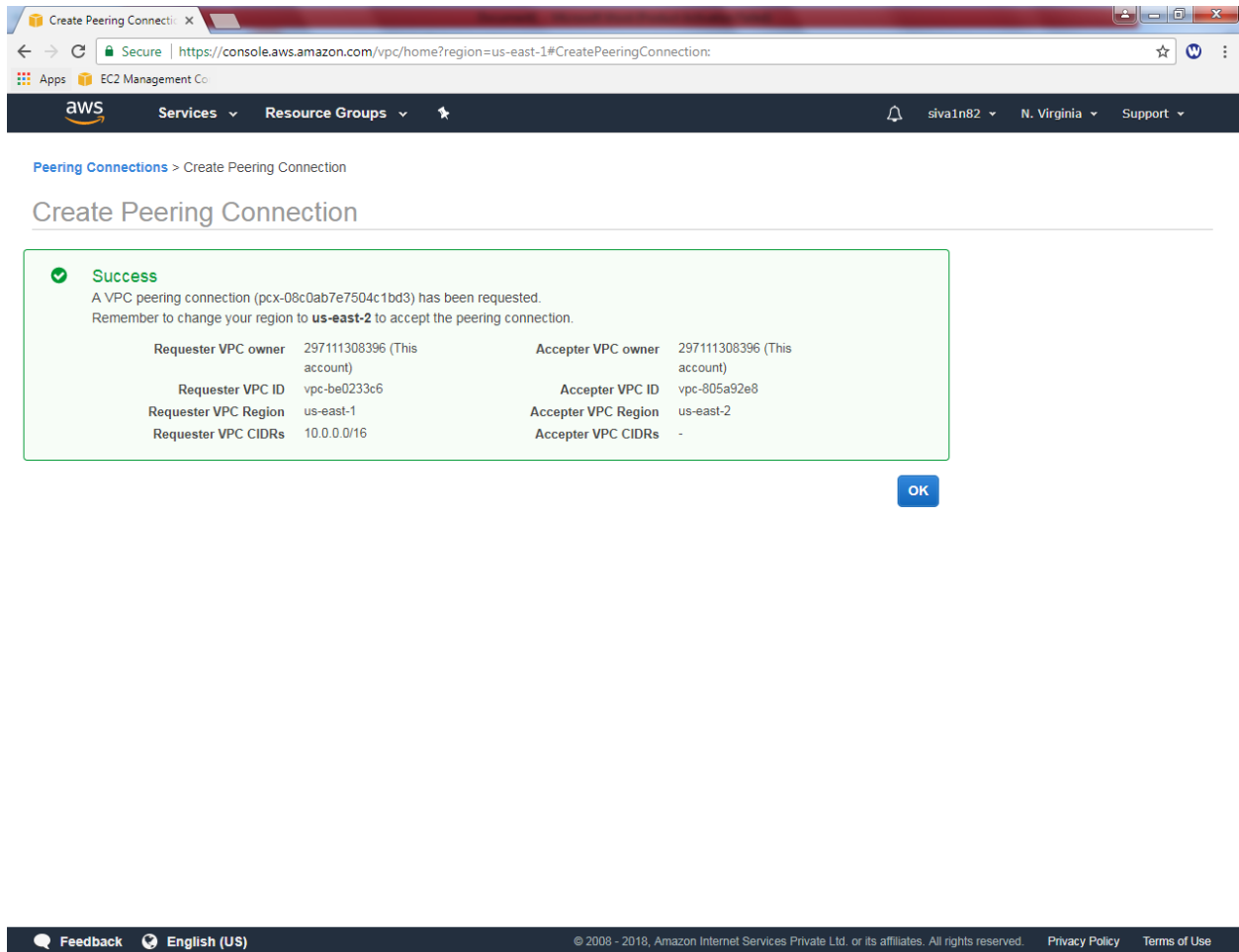
VPC (Acceptor) **vpc-80549268**

\* Required

Cancel **Create Peering Connection**

Click "Create Peering Connection".

VPC Peering Created successfully.



The screenshot shows the AWS Management Console interface. The browser address bar displays the URL: <https://console.aws.amazon.com/vpc/home?region=us-east-1#CreatePeeringConnection:>. The console header includes the AWS logo, navigation tabs for Services and Resource Groups, and user information for 'siva1n82' in the 'N. Virginia' region. The main content area is titled 'Create Peering Connection' and displays a green success message. Below the message is a table comparing the requester and acceptor VPC details. An 'OK' button is located at the bottom right of the success message box. The footer contains a feedback link, language selection (English (US)), and copyright information.

Peering Connections > Create Peering Connection

## Create Peering Connection

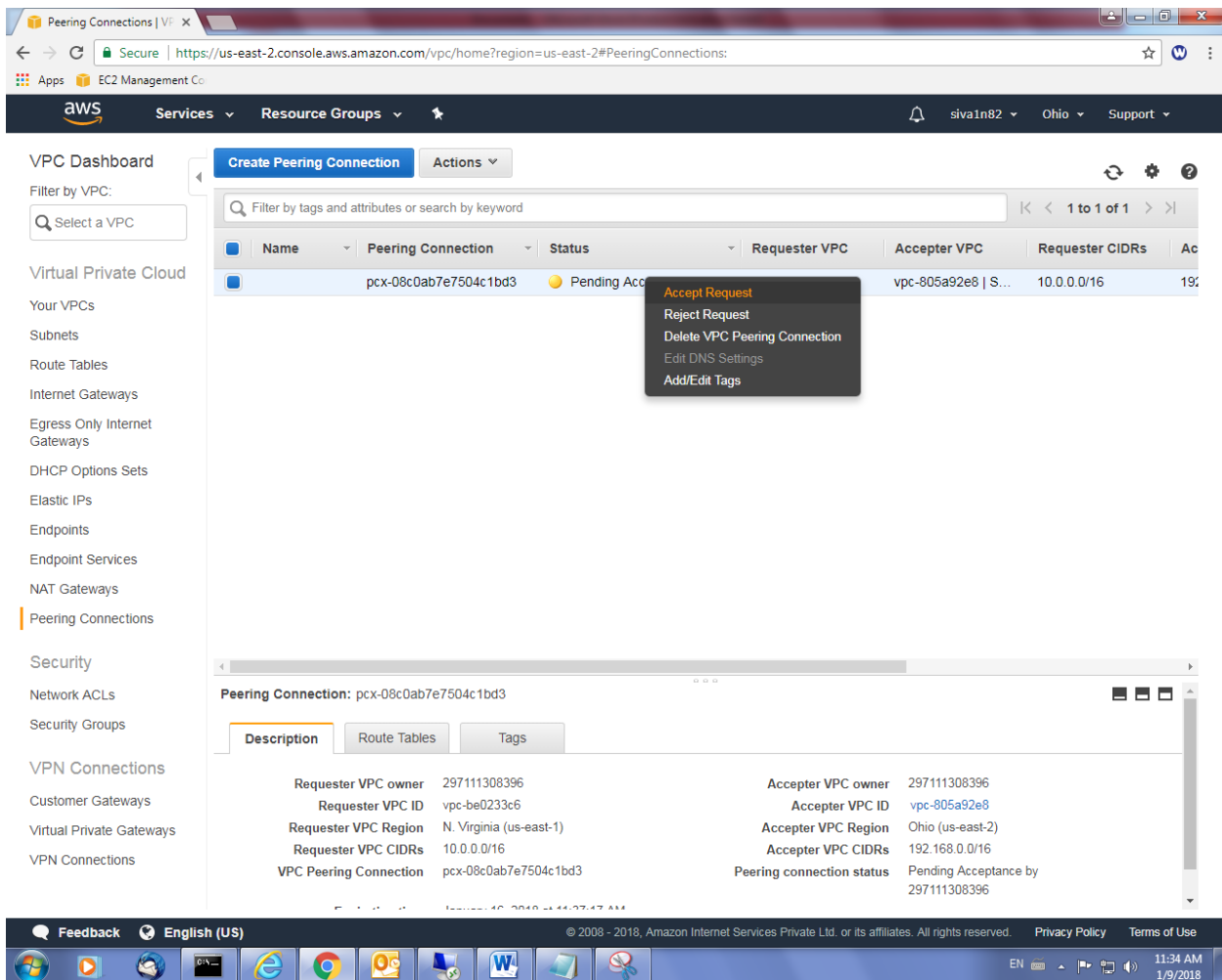
**Success**  
A VPC peering connection (pcx-08c0ab7e7504c1bd3) has been requested.  
Remember to change your region to **us-east-2** to accept the peering connection.

Requester VPC owner	297111308396 (This account)	Accepter VPC owner	297111308396 (This account)
Requester VPC ID	vpc-be0233c6	Accepter VPC ID	vpc-805a92e8
Requester VPC Region	us-east-1	Accepter VPC Region	us-east-2
Requester VPC CIDRs	10.0.0.0/16	Accepter VPC CIDRs	-

OK

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Go to Ohio region, Peering connections



The screenshot shows the AWS Management Console interface for the Ohio region. The left sidebar displays the VPC Dashboard with various navigation links. The main content area shows a list of VPC Peering Connections. One connection, 'pcx-08c0ab7e7504c1bd3', is in a 'Pending Acceptance' state. A context menu is open over this connection, showing options: 'Accept Request', 'Reject Request', 'Delete VPC Peering Connection', 'Edit DNS Settings', and 'Add/Edit Tags'. Below the list, the details for the selected peering connection are displayed, including requester and acceptor VPC information and the current status of 'Pending Acceptance by 297111308396'.

Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs
pcx-08c0ab7e7504c1bd3		Pending Acceptance	vpc-be0233c6	vpc-805a92e8	10.0.0.0/16	192.168.0.0/16

Peering Connection: pcx-08c0ab7e7504c1bd3			
Description	Route Tables	Tags	
Requester VPC owner	297111308396	Accepter VPC owner	297111308396
Requester VPC ID	vpc-be0233c6	Accepter VPC ID	vpc-805a92e8
Requester VPC Region	N. Virginia (us-east-1)	Accepter VPC Region	Ohio (us-east-2)
Requester VPC CIDRs	10.0.0.0/16	Accepter VPC CIDRs	192.168.0.0/16
VPC Peering Connection	pcx-08c0ab7e7504c1bd3	Peering connection status	Pending Acceptance by 297111308396

Click "Accept Request".

**Accept VPC Peering Connection Request** ✕

Are you sure you want to accept this VPC peering connection request (pcx-08c0ab7e7504c1bd3)?

Requester Account ID	297111308396 (This account)	Accepter Account ID	297111308396 (This account)
Requester VPC ID	vpc-be0233c6	Accepter VPC ID	<a href="#">vpc-805a92e8</a>
Requester VPC Region	us-east-1	Accepter VPC Region	us-east-2
Requester VPC CIDR	10.0.0.0/16	Accepter VPC CIDR	192.168.0.0/16

[Cancel](#) [Yes, Accept](#)

Click “Yes Accept”.

**Accept VPC Peering Connection Request** ✕

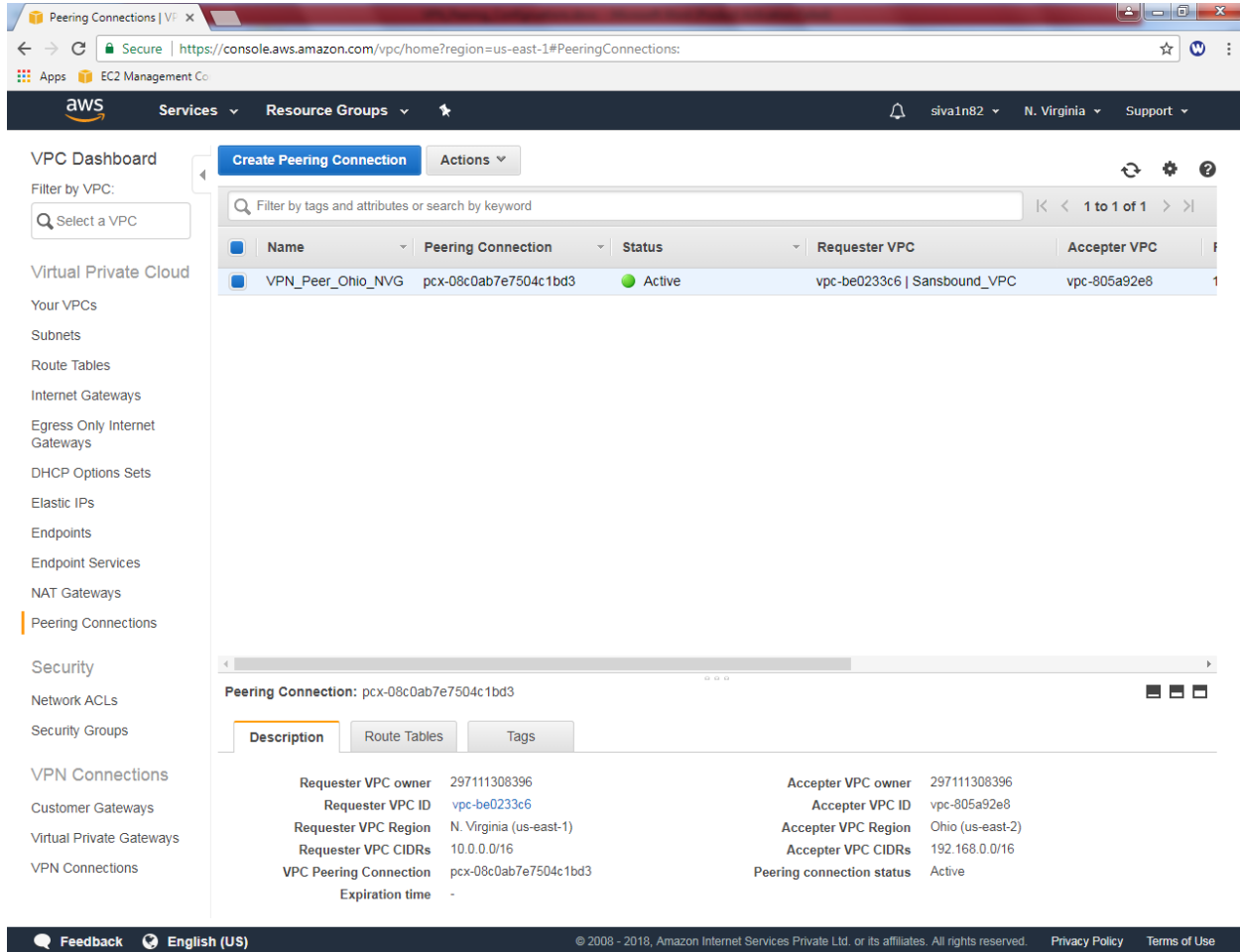
Your VPC Peering Connection has been established.

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. [Learn more](#)

[Modify my route tables now](#)

[Close](#)

VPC Status of N.Virginia is active.



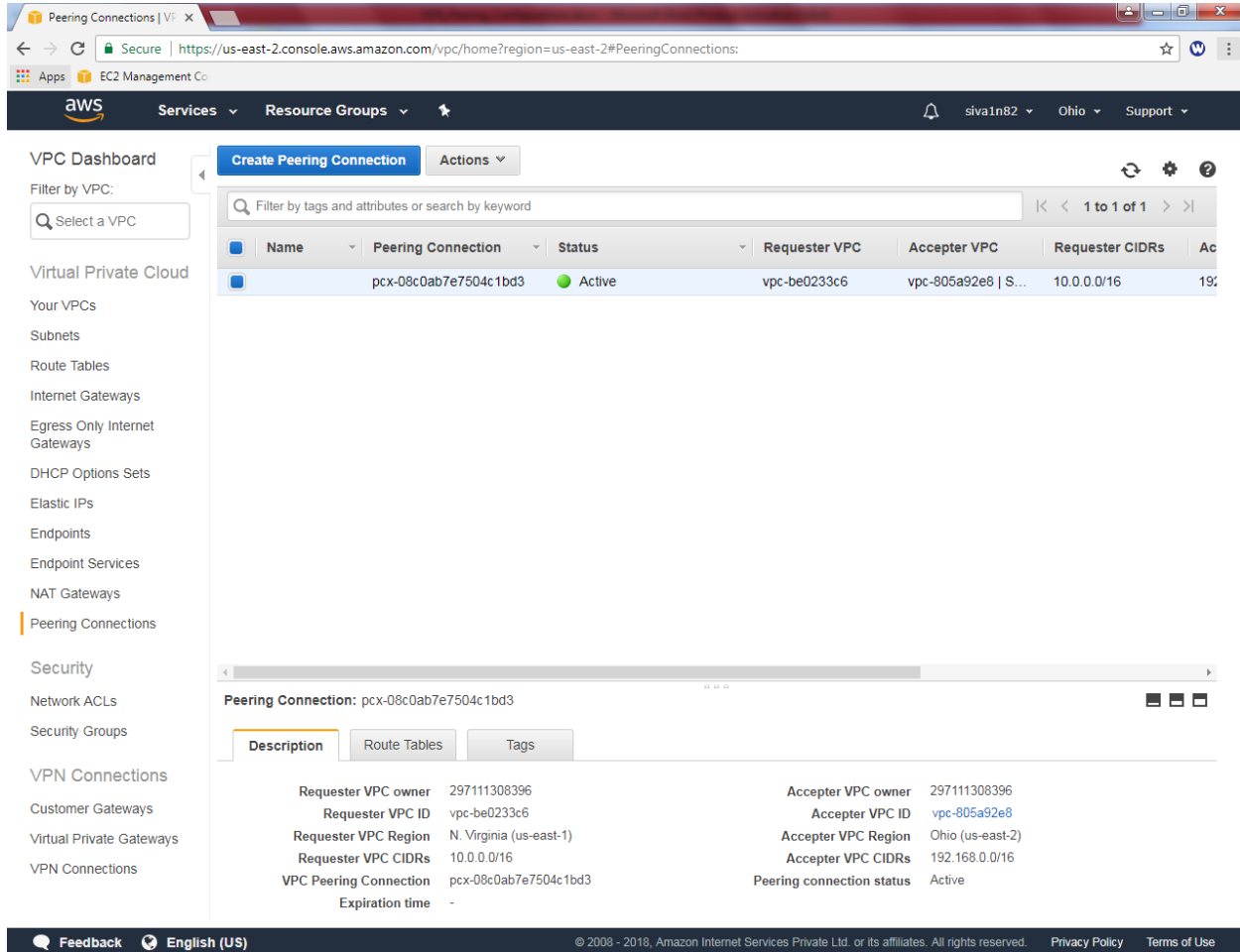
The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area displays the 'Peering Connections' page for the 'us-east-1' region. A table lists the peering connections, showing one active connection named 'VPN\_Peer\_Ohio\_NVG' between VPCs 'vpc-be0233c6 | Sansbound\_VPC' (Requester) and 'vpc-805a92e8' (Accepter). Below the table, the details for the selected peering connection are shown, including the Requester VPC owner, ID, Region, CIDR, and the Accepter VPC owner, ID, Region, CIDR, and the Peering connection status.

Name	Peering Connection	Status	Requester VPC	Accepter VPC
VPN_Peer_Ohio_NVG	pcx-08c0ab7e7504c1bd3	Active	vpc-be0233c6   Sansbound_VPC	vpc-805a92e8

Peering Connection: pcx-08c0ab7e7504c1bd3	
Requester VPC owner	297111308396
Requester VPC ID	vpc-be0233c6
Requester VPC Region	N. Virginia (us-east-1)
Requester VPC CIDRs	10.0.0.0/16
VPC Peering Connection	pcx-08c0ab7e7504c1bd3
Expiration time	-
Accepter VPC owner	297111308396
Accepter VPC ID	vpc-805a92e8
Accepter VPC Region	Ohio (us-east-2)
Accepter VPC CIDRs	192.168.0.0/16
Peering connection status	Active

VPC Status of Ohio is active.



**VPC Dashboard**

Filter by VPC:

Virtual Private Cloud

- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections**

**Security**

- Network ACLs
- Security Groups

**VPN Connections**

- Customer Gateways
- Virtual Private Gateways
- VPN Connections

**Peering Connections**

Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs
	pcx-08c0ab7e7504c1bd3	Active	vpc-be0233c6	vpc-805a92e8   S...	10.0.0.0/16	192.168.0.0/16

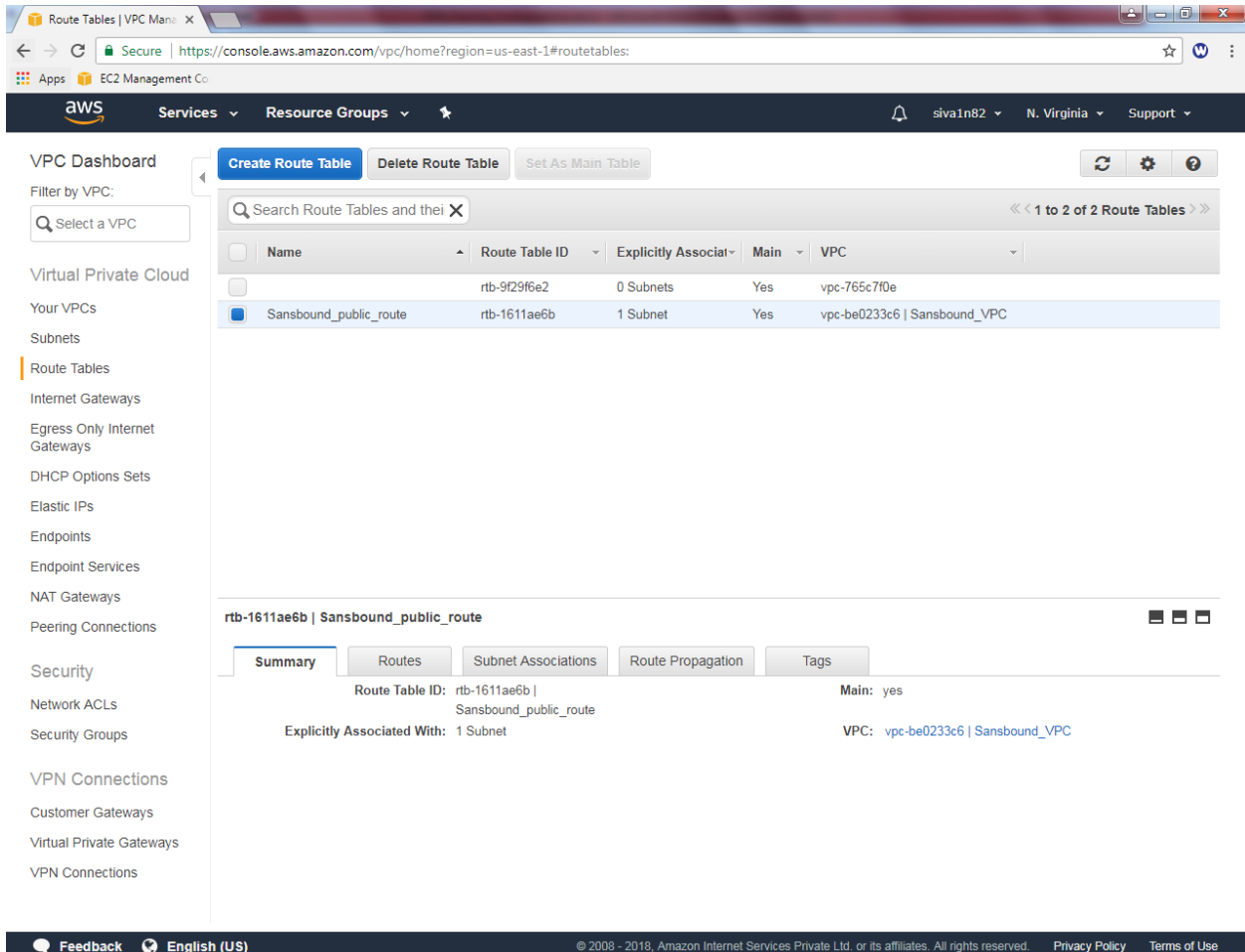
**Peering Connection: pcx-08c0ab7e7504c1bd3**

**Description**

Requester VPC owner	297111308396	Accepter VPC owner	297111308396
Requester VPC ID	vpc-be0233c6	Accepter VPC ID	vpc-805a92e8
Requester VPC Region	N. Virginia (us-east-1)	Accepter VPC Region	Ohio (us-east-2)
Requester VPC CIDRs	10.0.0.0/16	Accepter VPC CIDRs	192.168.0.0/16
VPC Peering Connection	pcx-08c0ab7e7504c1bd3	Peering connection status	Active
Expiration time	-		

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

If you try to connect the LAN Segment through RDP will not connect. Because we need to add route table for Ohio subnet in N.Virginia public route table.



The screenshot shows the AWS Management Console interface for Route Tables. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, Security, and VPN Connections. The main content area displays a list of route tables. The selected route table, 'Sansbound\_public\_route' (ID: rtb-1611ae6b), is shown in a detailed view below the list. This view includes tabs for Summary, Routes, Subnet Associations, Route Propagation, and Tags. The Summary tab is active, showing that the route table is the main route table for the VPC 'vpc-be0233c6 | Sansbound\_VPC' and is explicitly associated with 1 subnet.

Name	Route Table ID	Explicitly Associat	Main	VPC
Sansbound_public_route	rtb-1611ae6b	1 Subnet	Yes	vpc-be0233c6   Sansbound_VPC

**rtb-1611ae6b | Sansbound\_public\_route**

**Summary**

Route Table ID: rtb-1611ae6b | Sansbound\_public\_route

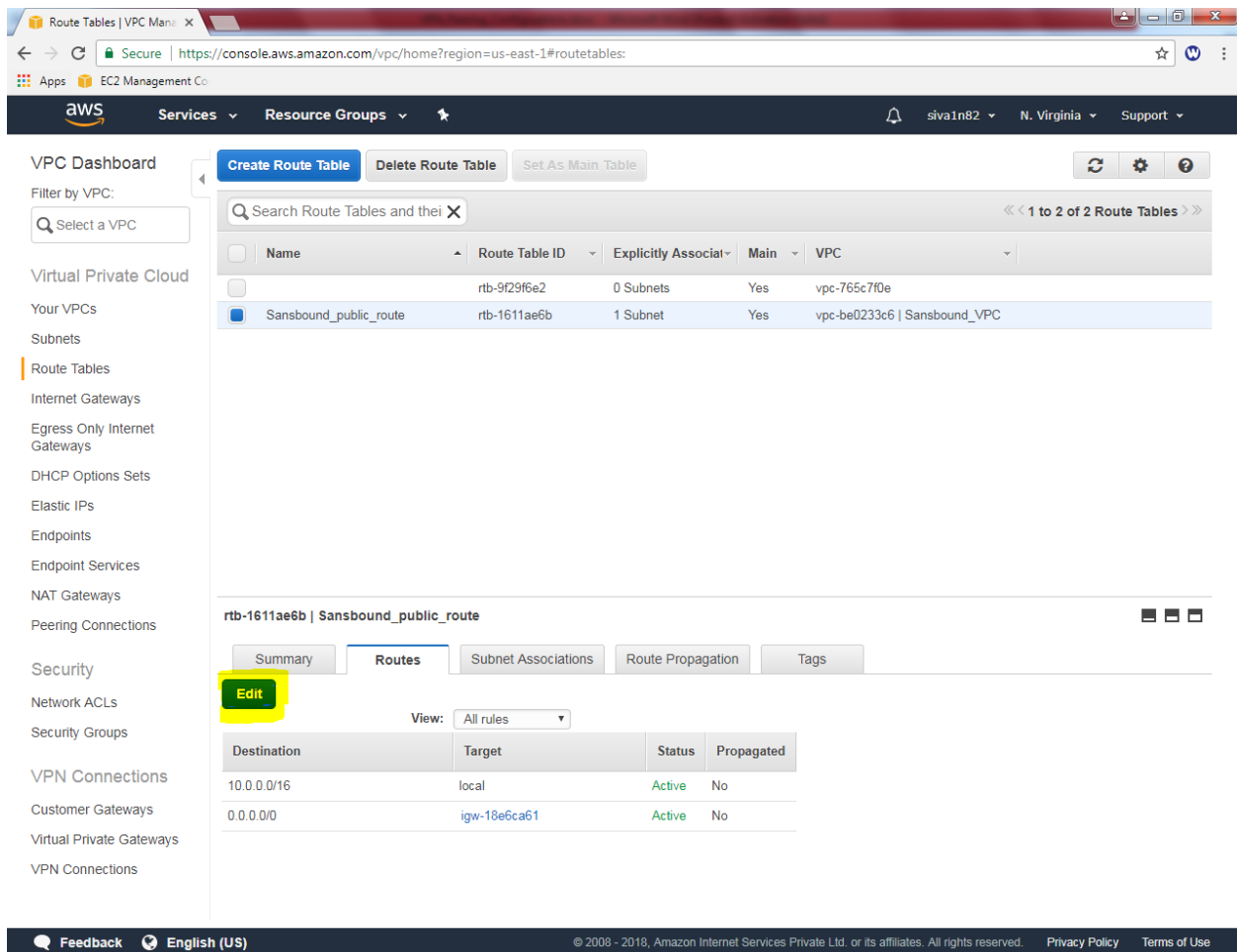
Main: yes

Explicitly Associated With: 1 Subnet

VPC: vpc-be0233c6 | Sansbound\_VPC



In Sansbound public route, select route and click “Edit”.



The screenshot shows the AWS Management Console VPC Dashboard. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area displays a list of Route Tables. The 'Sansbound\_public\_route' is selected, and the 'Edit' button is highlighted. Below the list, the 'Routes' tab is active, showing a table of routes.

Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-9f29f6e2	0 Subnets	Yes	vpc-765c7f0e
<input checked="" type="checkbox"/> Sansbound_public_route	rtb-1611ae6b	1 Subnet	Yes	vpc-be0233c6   Sansbound_VPC

rtb-1611ae6b | Sansbound\_public\_route

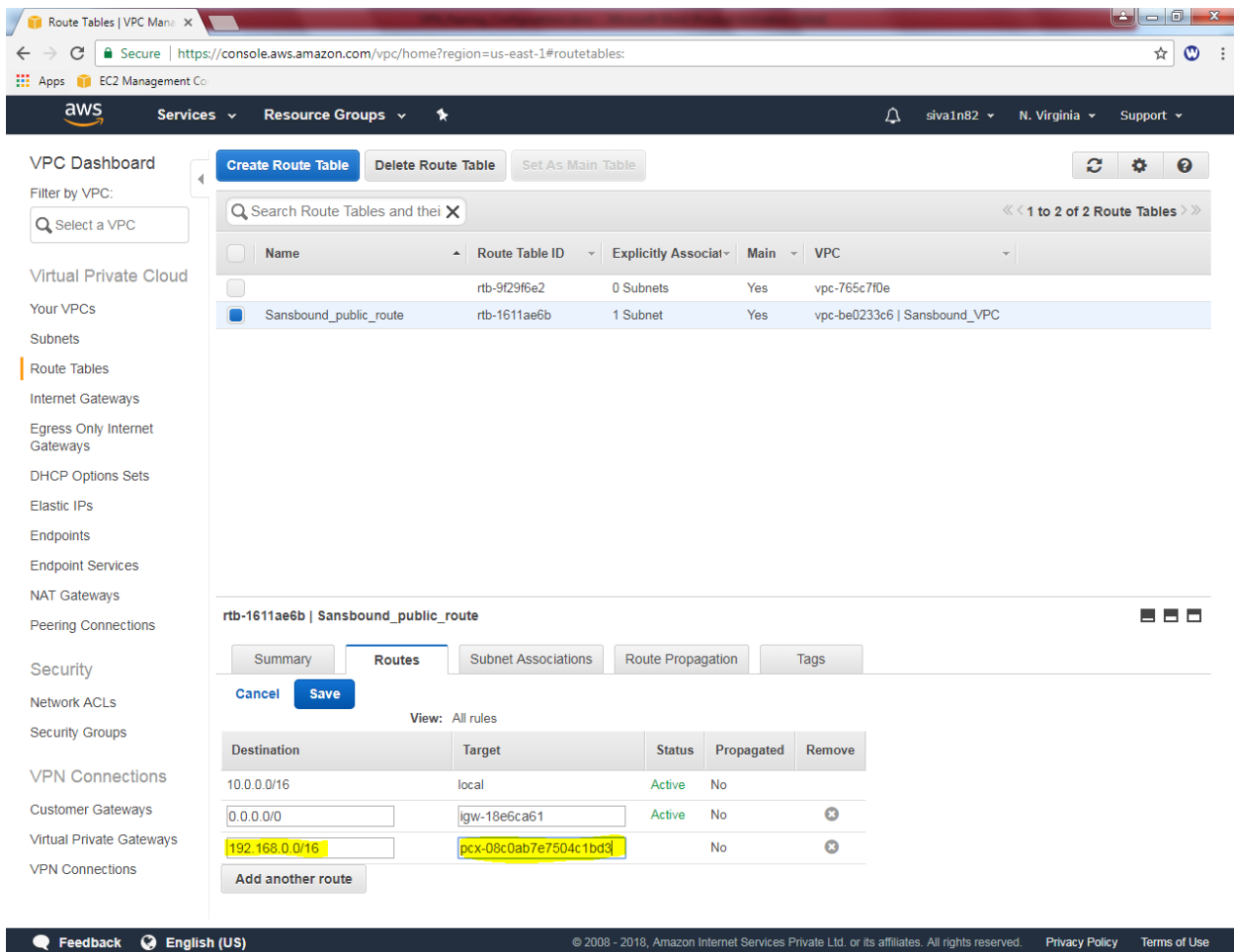
Summary Routes Subnet Associations Route Propagation Tags

**Edit**

View: All rules

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-18e6ca61	Active	No

Click “Add another route” and type 192.168.0.0/16 ohio subnet and select “pcx-\*” as target.



The screenshot shows the AWS Management Console interface for the VPC Dashboard. The left sidebar contains navigation links for various VPC resources. The main content area displays a list of route tables. The 'Sansbound\_public\_route' (rtb-1611ae6b) is selected, and its 'Routes' tab is active. Below the tab, there is a table of routes. A new route is being added with the destination '192.168.0.0/16' and the target 'pcx-08c0ab7e7504c1bd3'.

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	igw-18e6ca61	Active	No	✕
192.168.0.0/16	pcx-08c0ab7e7504c1bd3	No	No	✕

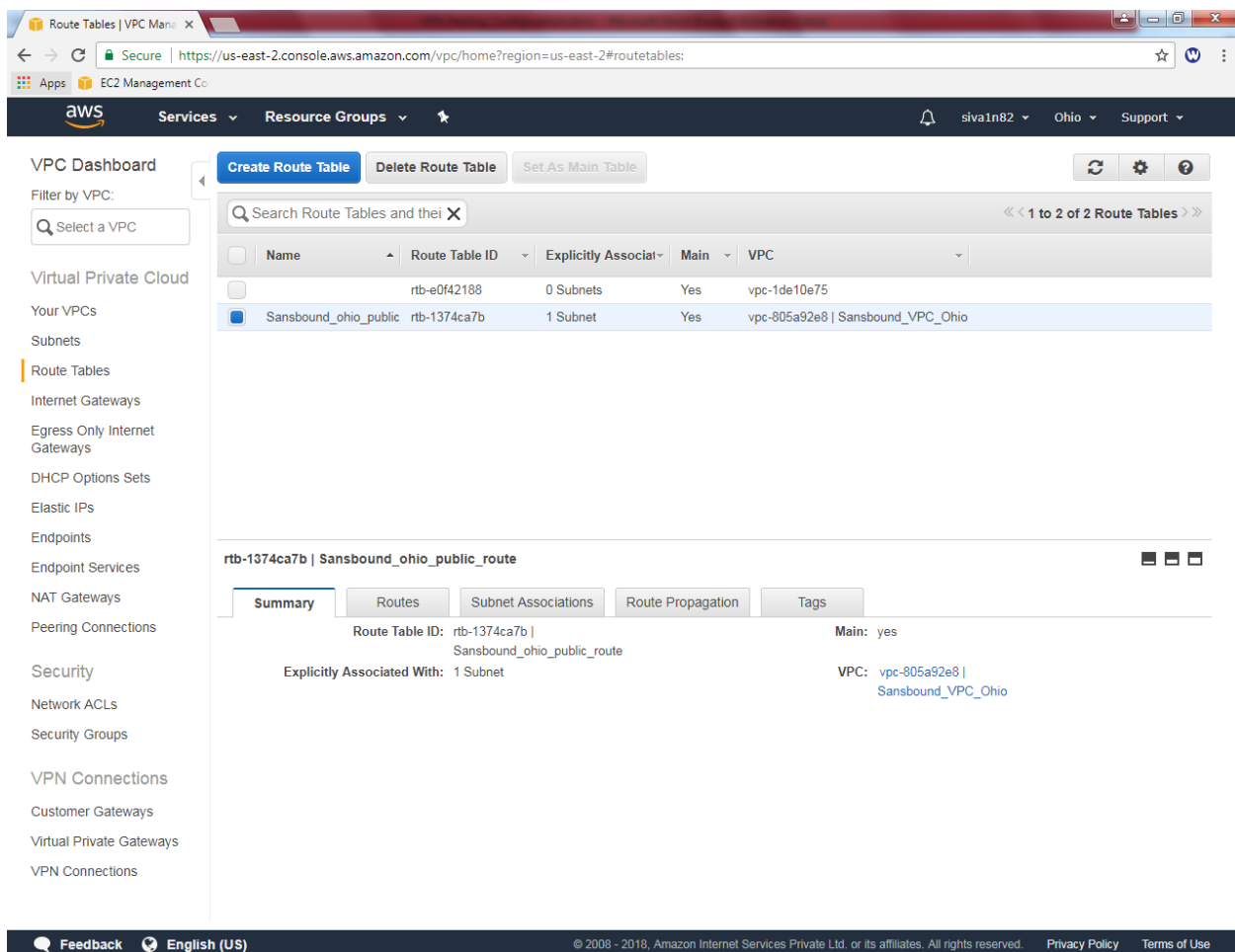
Buttons: Add another route, Cancel, Save

Then click save.

Goto ohio region,

Goto VPC Dashboard,

Click route table, then select “Sansbound\_Ohio\_public”



The screenshot shows the AWS Management Console VPC Dashboard for the Ohio region. The left sidebar contains a navigation menu with categories like Virtual Private Cloud, Security, and VPN Connections. The main content area displays a table of route tables. The selected route table, 'Sansbound\_ohio\_public' (ID: rtb-1374ca7b), is highlighted. Below the table, the 'Summary' tab is active, showing details such as the Route Table ID, Main status (yes), and the VPC it is associated with (vpc-805a92e8 | Sansbound\_VPC\_Ohio).

Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-e0f42188	0 Subnets	Yes	vpc-1de10e75
<input checked="" type="checkbox"/> Sansbound_ohio_public	rtb-1374ca7b	1 Subnet	Yes	vpc-805a92e8   Sansbound_VPC_Ohio

**rtb-1374ca7b | Sansbound\_ohio\_public\_route**

**Summary**

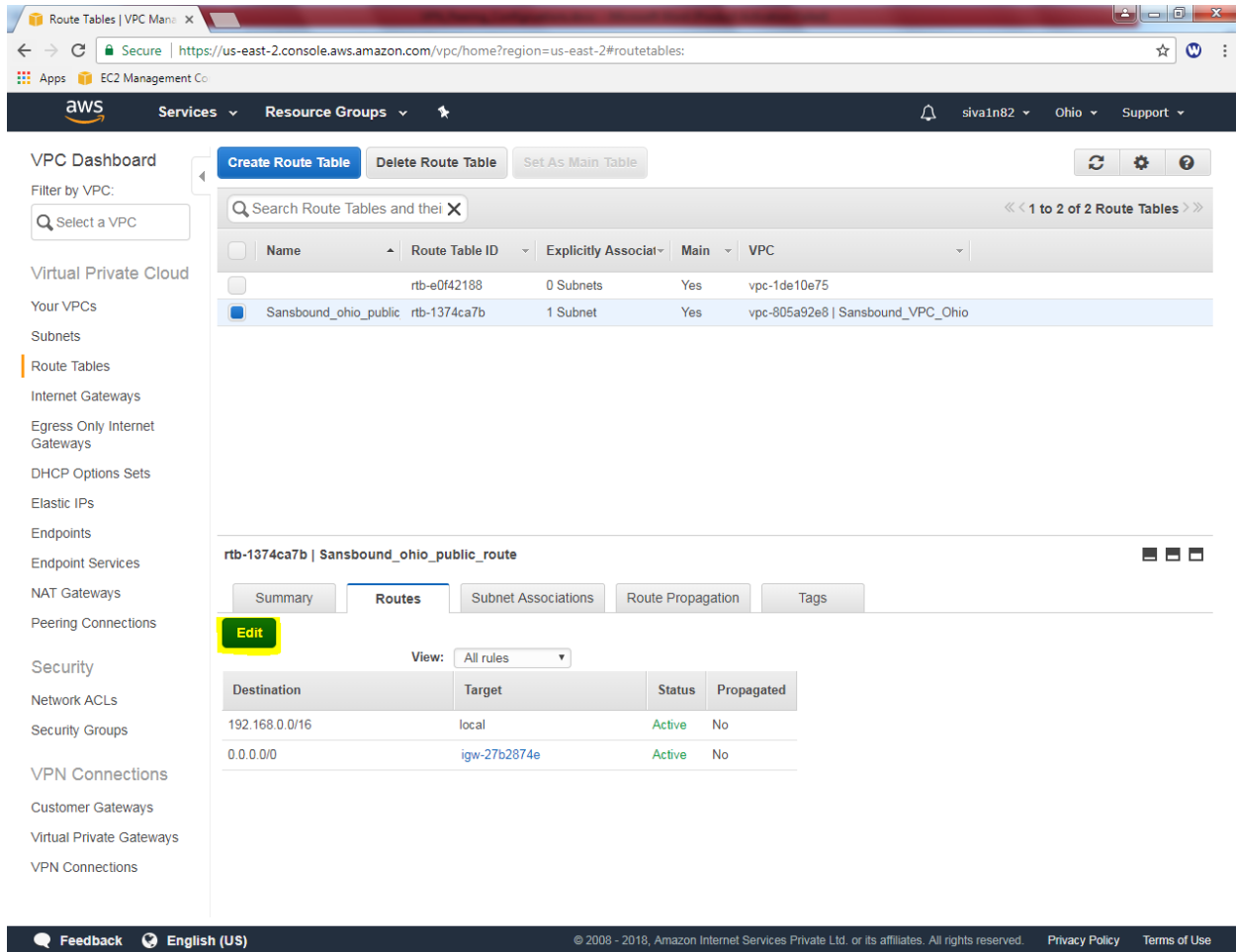
Route Table ID: rtb-1374ca7b | Sansbound\_ohio\_public\_route

Main: yes

Explicitly Associated With: 1 Subnet

VPC: vpc-805a92e8 | Sansbound\_VPC\_Ohio

In Sansbound\_ohio\_public routing table, route option and then click “Edit”



The screenshot shows the AWS Management Console interface. The left sidebar contains the VPC Dashboard menu with options like Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area displays the 'Route Tables' page for the 'vpc-805a92e8 | Sansbound\_VPC\_Ohio' VPC. A table lists two route tables: 'rtb-e0f42188' (0 Subnets) and 'Sansbound\_ohio\_public' (1 Subnet). The 'Sansbound\_ohio\_public' route table is selected, and its details are shown below. The 'Routes' tab is active, displaying a table of routes. The 'Edit' button is highlighted in yellow.

Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-e0f42188	0 Subnets	Yes	vpc-1de10e75
Sansbound_ohio_public	rtb-1374ca7b	1 Subnet	Yes	vpc-805a92e8   Sansbound_VPC_Ohio

**rtb-1374ca7b | Sansbound\_ohio\_public\_route**

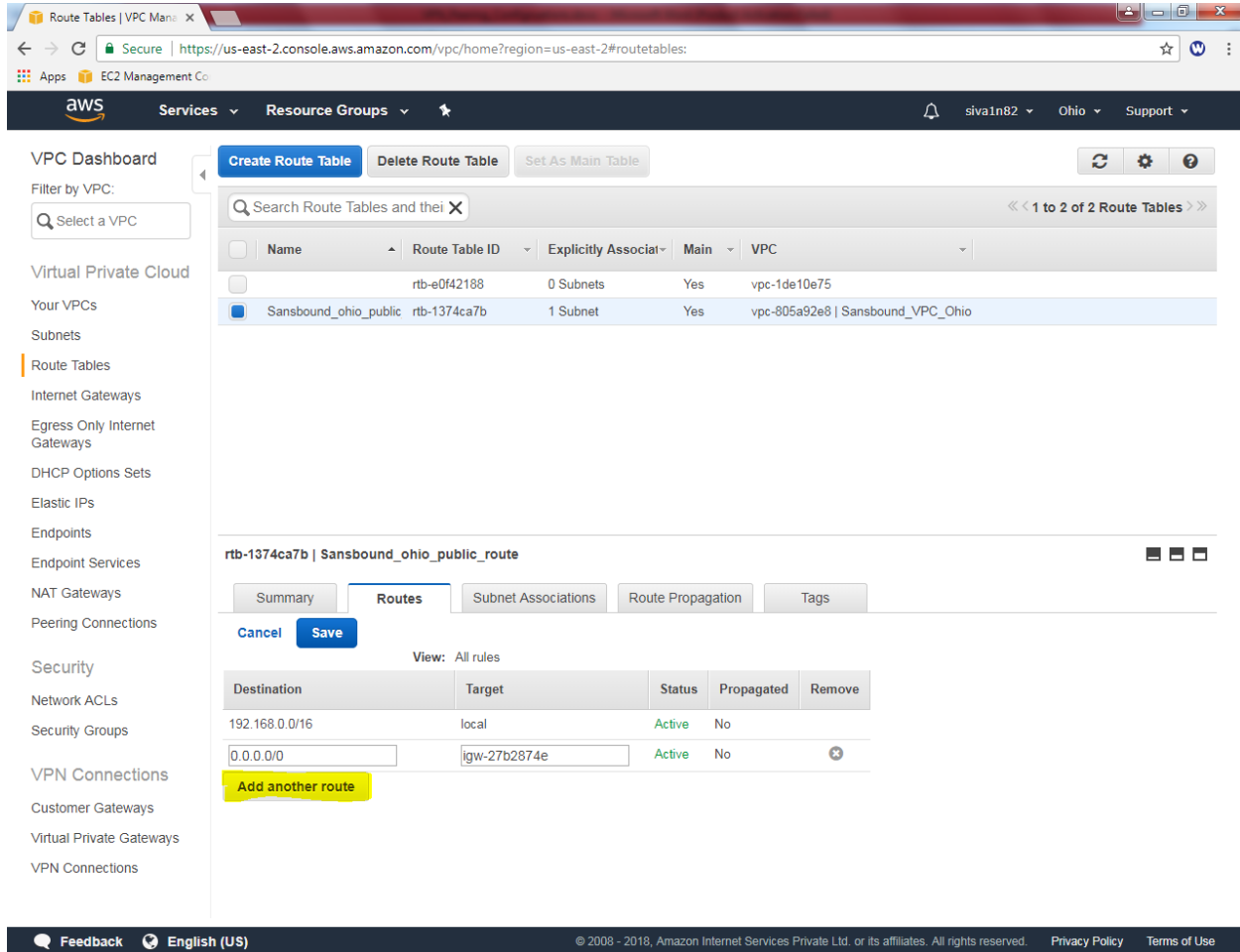
Summary Routes Subnet Associations Route Propagation Tags

**Edit**

View: All rules

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	igw-27b2874e	Active	No

Click “Add another route”



The screenshot shows the AWS Management Console interface. The left sidebar displays the VPC Dashboard with various VPC-related services listed. The main content area shows the configuration for the route table `rtb-1374ca7b` (Sansbound\_ohio\_public). The `Routes` tab is selected, showing a table of routes. The table has columns for Destination, Target, Status, Propagated, and Remove. Two routes are listed: one for `192.168.0.0/16` pointing to `local` (Active), and another for `0.0.0.0/0` pointing to `igw-27b2874e` (Active). A yellow button labeled "Add another route" is visible at the bottom of the route table.

Route Tables | VPC Main

Secure | <https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#routetables>

Apps EC2 Management Co

aws Services Resource Groups

Filter by VPC: Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their

<< 1 to 2 of 2 Route Tables >>

Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-e0f42188	0 Subnets	Yes	vpc-1de10e75
Sansbound_ohio_public	rtb-1374ca7b	1 Subnet	Yes	vpc-805a92e8   Sansbound_VPC_Ohio

rtb-1374ca7b | Sansbound\_ohio\_public\_route

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

View: All rules

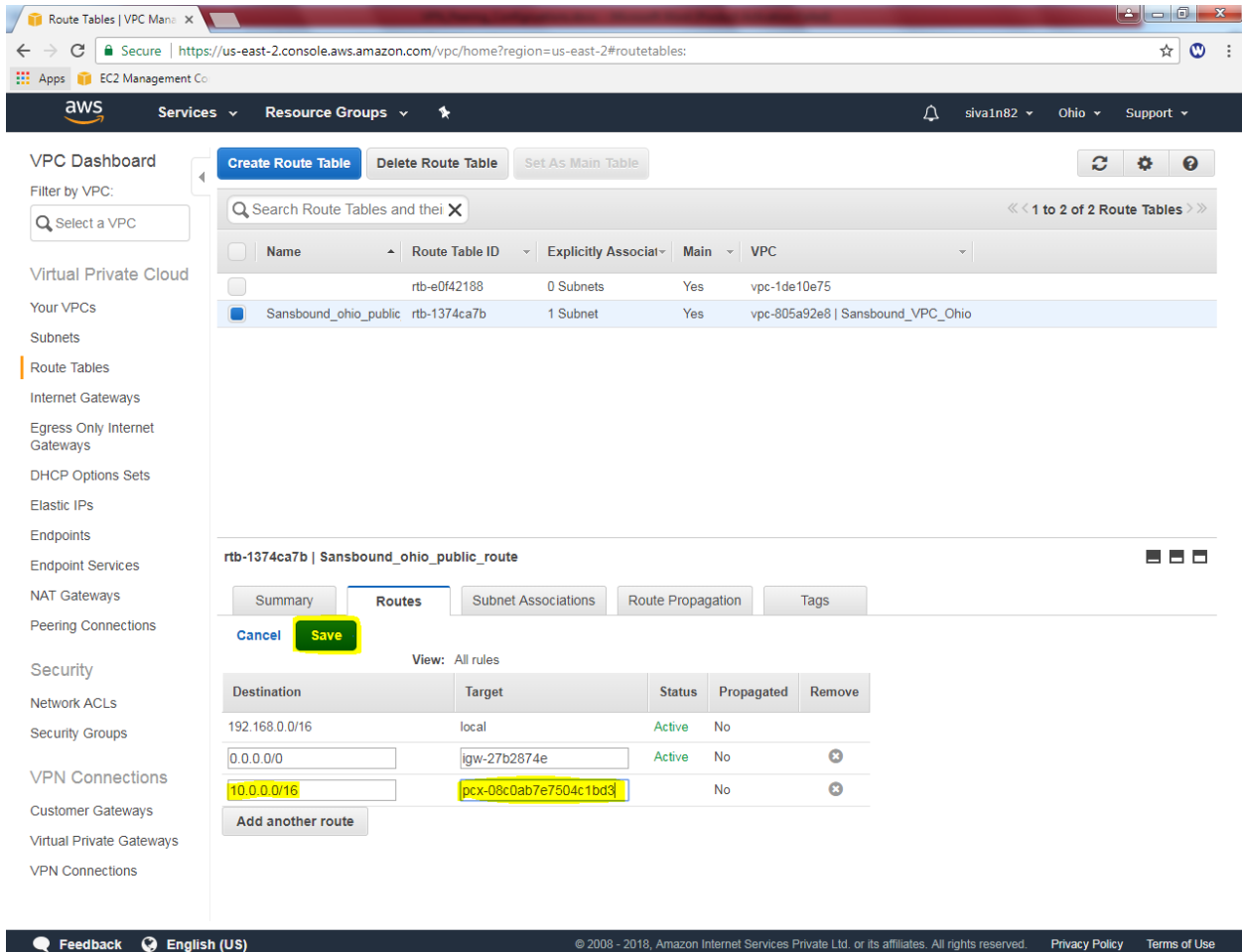
Destination	Target	Status	Propagated	Remove
192.168.0.0/16	local	Active	No	
0.0.0.0/0	igw-27b2874e	Active	No	

Add another route

Feedback English (US)

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

In Sansbound\_Ohio\_public\_route table type N.Virginia subnet 10.0.0.0/16 and select target as “pcx-”



The screenshot shows the AWS Management Console interface for configuring a route table. The left sidebar displays the navigation menu with categories like VPC Dashboard, Virtual Private Cloud, Security, and VPN Connections. The main content area shows the 'Route Tables' page for the 'us-east-2' region. A table lists the available route tables, with 'Sansbound\_ohio\_public' (rtb-1374ca7b) selected. Below this, the 'Routes' tab for the selected route table is active, showing a list of routes. The 'Destination' column contains '10.0.0.0/16', and the 'Target' column contains 'pcx-08c0ab7e7504c1bd3'. The 'Status' column shows 'Active', and the 'Propagated' column shows 'No'. A 'Save' button is highlighted in yellow.

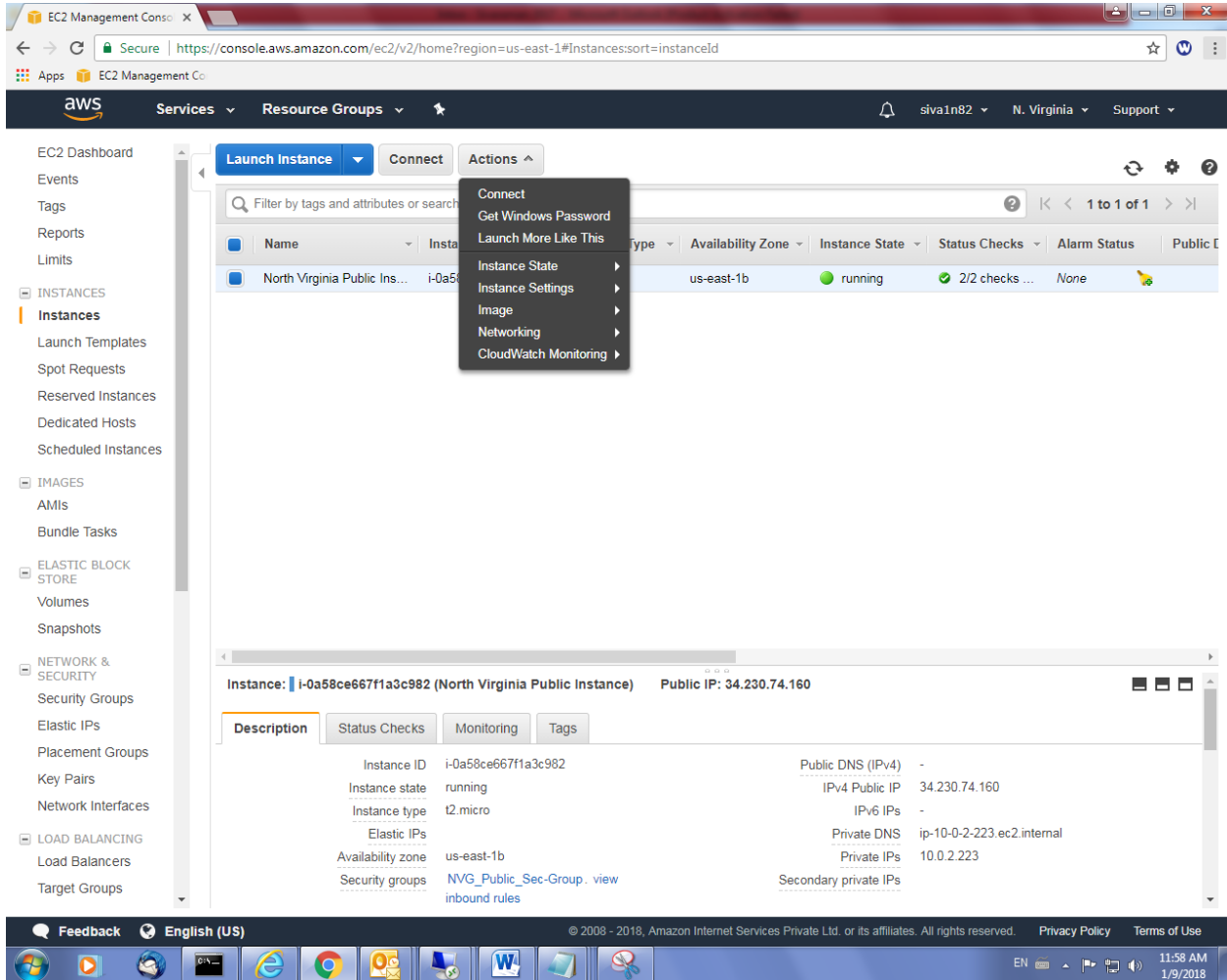
Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-e0f42188	0 Subnets	Yes	vpc-1de10e75
<input checked="" type="checkbox"/> Sansbound_ohio_public	rtb-1374ca7b	1 Subnet	Yes	vpc-805a92e8   Sansbound_VPC_Ohio

Destination	Target	Status	Propagated	Remove
192.168.0.0/16	local	Active	No	
0.0.0.0/0	igw-27b2874e	Active	No	✕
10.0.0.0/16	pcx-08c0ab7e7504c1bd3	No	No	✕

Goto North virginia, click EC2 service to get login credentials.

Actions → Connect



The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and LOAD BALANCING. The main content area displays a table of EC2 instances. The first instance, 'North Virginia Public Instance' (ID: i-0a58ce667f1a3c982), is in the 'running' state. The 'Actions' dropdown menu is open, showing options like 'Connect', 'Get Windows Password', 'Launch More Like This', 'Instance State', 'Instance Settings', 'Image', 'Networking', and 'CloudWatch Monitoring'. Below the table, the details for the selected instance are shown, including its ID, state, type, availability zone, security groups, and public IP address (34.230.74.160).

Name	Instance ID	Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public IP
North Virginia Public Instance	i-0a58ce667f1a3c982	t2.micro	us-east-1b	running	2/2 checks ...	None	34.230.74.160

Instance: i-0a58ce667f1a3c982 (North Virginia Public Instance) Public IP: 34.230.74.160

Description	
Instance ID	i-0a58ce667f1a3c982
Instance state	running
Instance type	t2.micro
Elastic IPs	
Availability zone	us-east-1b
Security groups	NVG_Public_Sec-Group, inbound rules
Public DNS (IPv4)	-
IPv4 Public IP	34.230.74.160
IPv6 IPs	-
Private DNS	ip-10-0-2-223.ec2.internal
Private IPs	10.0.2.223
Secondary private IPs	

Click get password.

### Connect To Your Instance ✕

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download Remote Desktop File](#)

When prompted, connect to your instance using the following details:

<b>Public IP</b>	34.230.74.160
<b>User name</b>	Administrator
<b>Password</b>	<a href="#">Get Password</a>

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

[Close](#)

Choose the \*.pem file and decrypt the password.



Goto ohio region, select the instance and Actions → Connect.

The screenshot shows the AWS Management Console interface. On the left is a navigation sidebar with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The main content area displays a table of EC2 instances. One instance, 'Ohio Public Instance' with ID 'i-088923f3e8eba7ebd', is selected. A 'Connect' button is visible above the table, and a dropdown menu is open, showing options: 'Connect', 'Get Windows Password', 'Launch More Like This', 'Instance State', 'Instance Settings', 'Image', 'Networking', and 'CloudWatch Monitoring'. Below the table, the details for the selected instance are shown, including its state (running), type (t2.micro), and various IP addresses.

Name	Instance ID	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
Ohio Public I...	i-088923f3e8eba7ebd	us-east-2b	running	2/2 checks ...	None	

Instance: **i-088923f3e8eba7ebd (Ohio Public Instance)** Public IP: 18.221.200.147

Description		Status Checks	Monitoring	Tags
Instance ID	i-088923f3e8eba7ebd	Public DNS (IPv4)	-	
Instance state	running	IPv4 Public IP	18.221.200.147	
Instance type	t2.micro	IPv6 IPs	-	
Elastic IPs		Private DNS	ip-192-168-2-197.us-east-2.compute.internal	
Availability zone	us-east-2b	Private IPs	192.168.2.197	
Security groups	Ohio_Public_Sec_Group . view	Secondary private IPs		

## Connect To Your Instance

×

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download Remote Desktop File](#)

When prompted, connect to your instance using the following details:

<b>Public IP</b>	18.221.200.147
<b>User name</b>	Administrator
<b>Password</b>	<a href="#">Get Password</a>

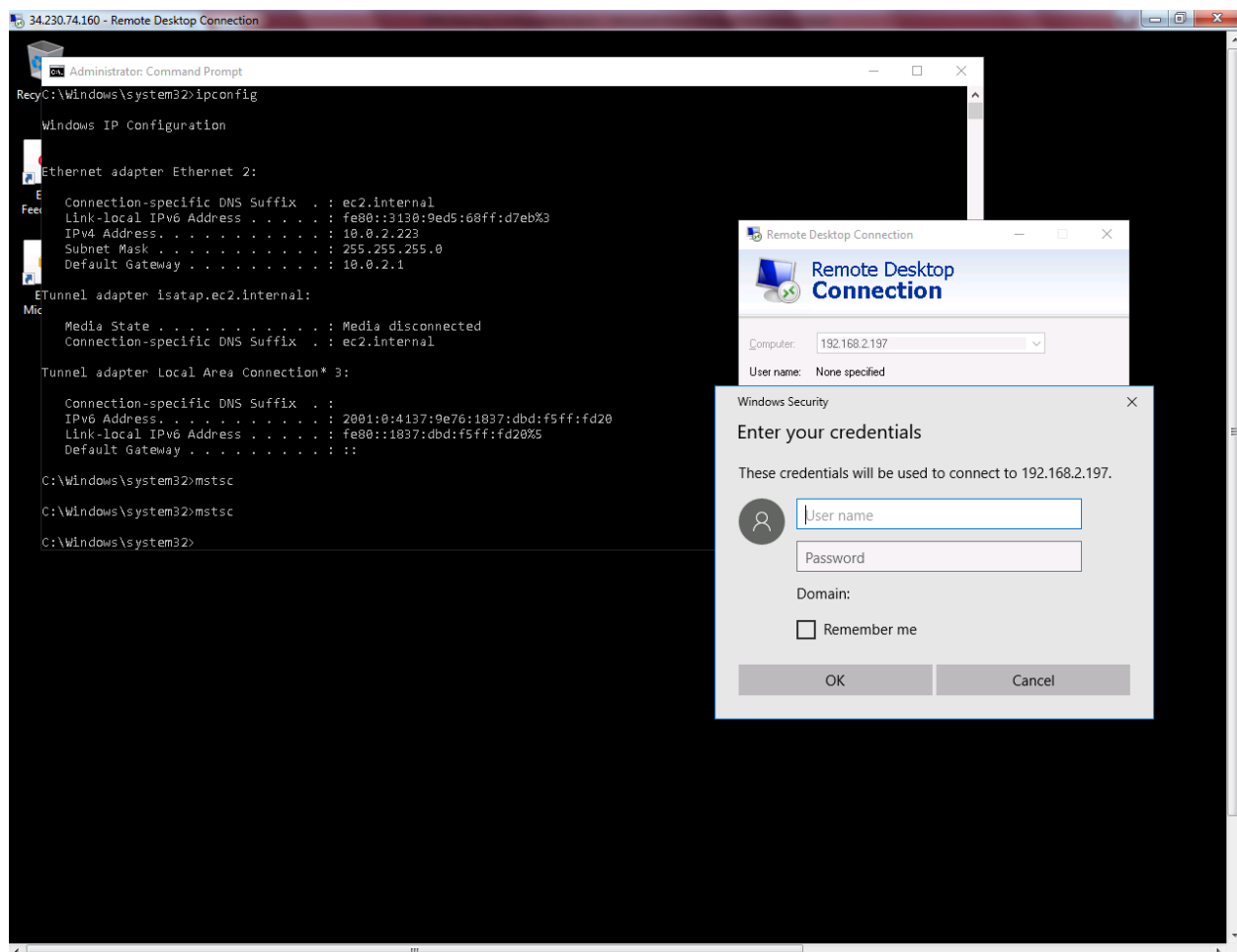
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

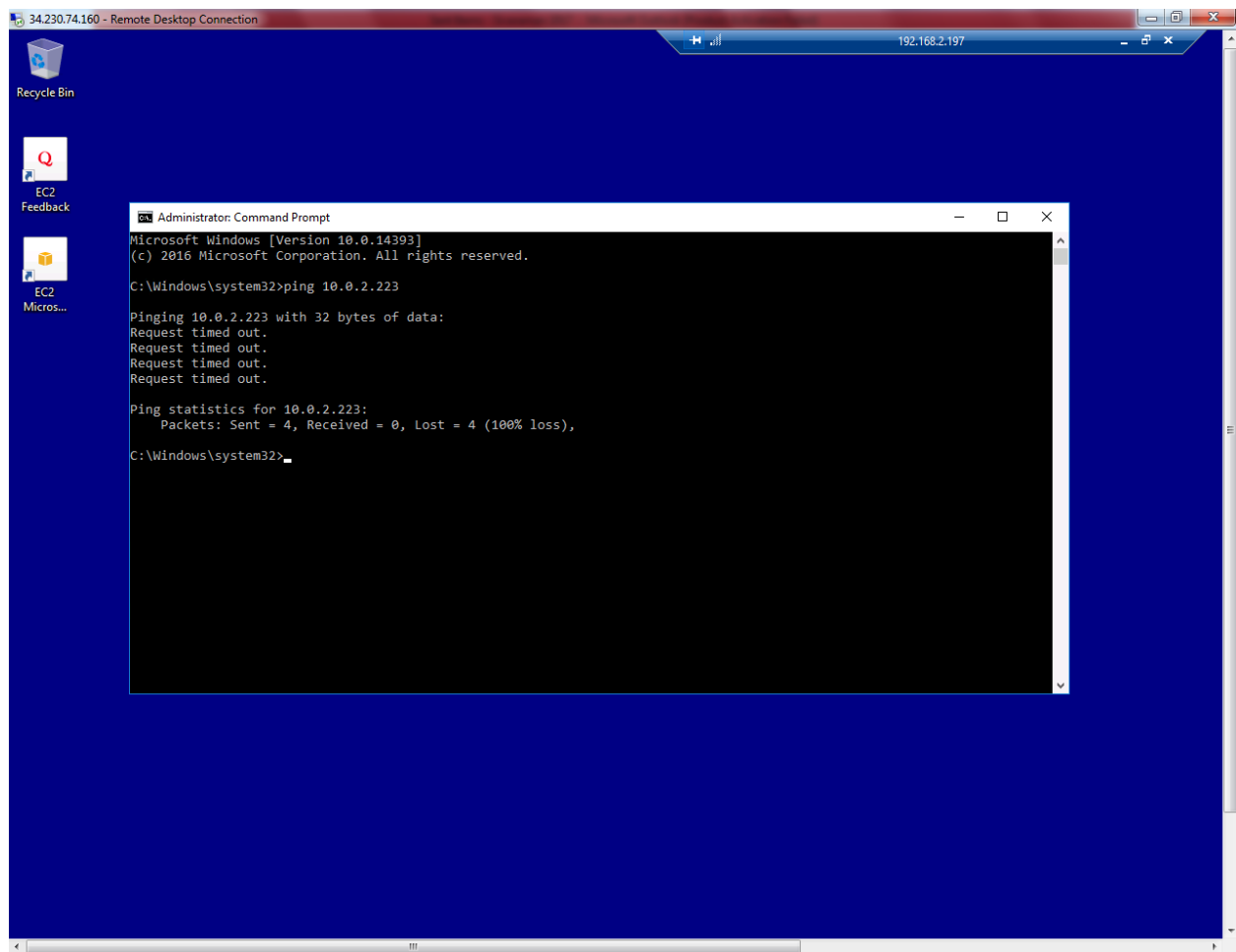
[Close](#)

Choose the \*.pem file and decrypt the password.

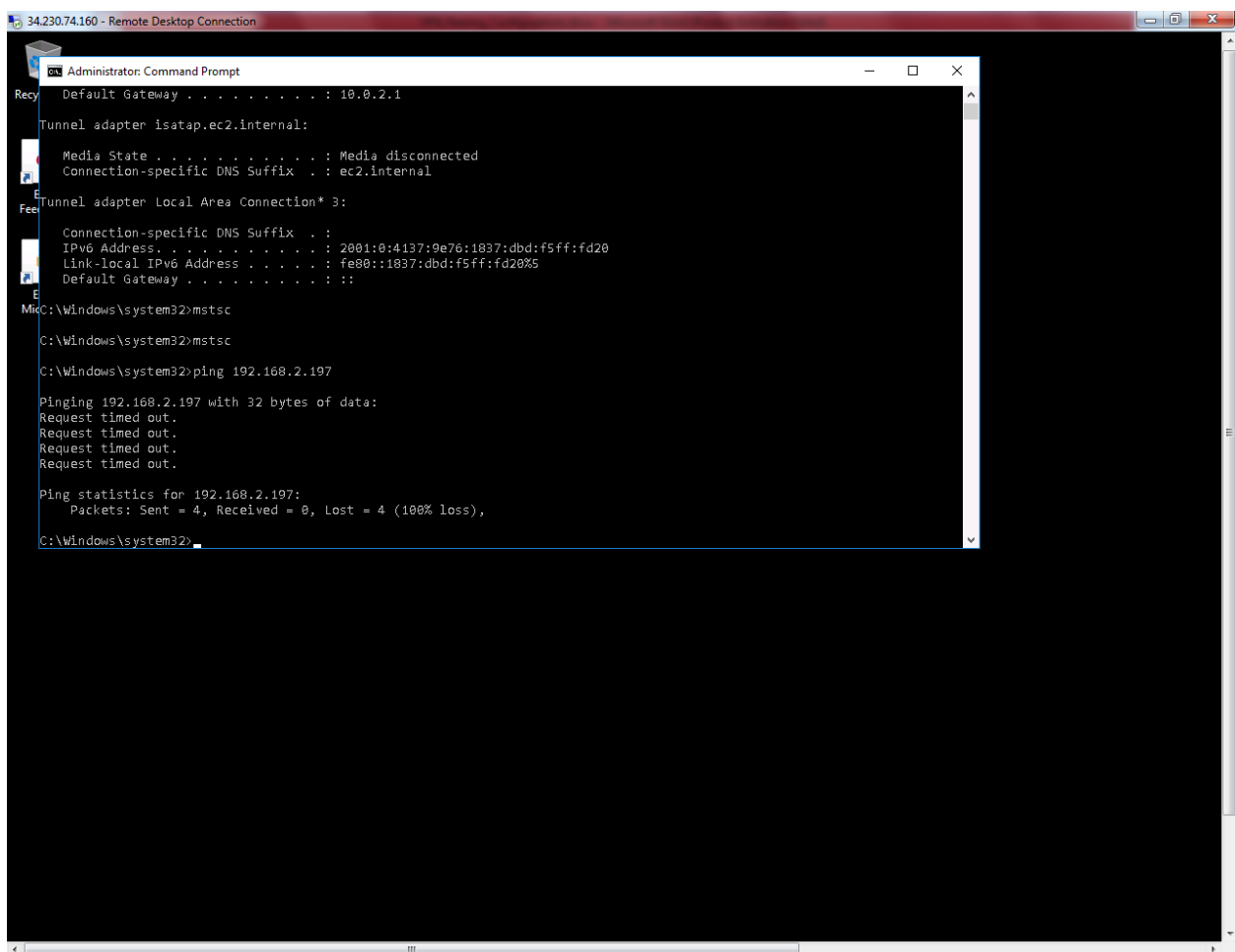
Try to connect RDP of Ohio subnet from N.Virginia.



Try to ping 10.0.2.223 (N.Virginia) subnet from Ohio subnet 192.168.2.0/24. But we are unable to ping due ICMP was not permitted in Security Group of North Virginia.



Try to ping 192.168.2.197 subnet from North Virginia subnet 10.0.2.0/24. But we are unable to ping due ICMP was not permitted in Security Group of Ohio.

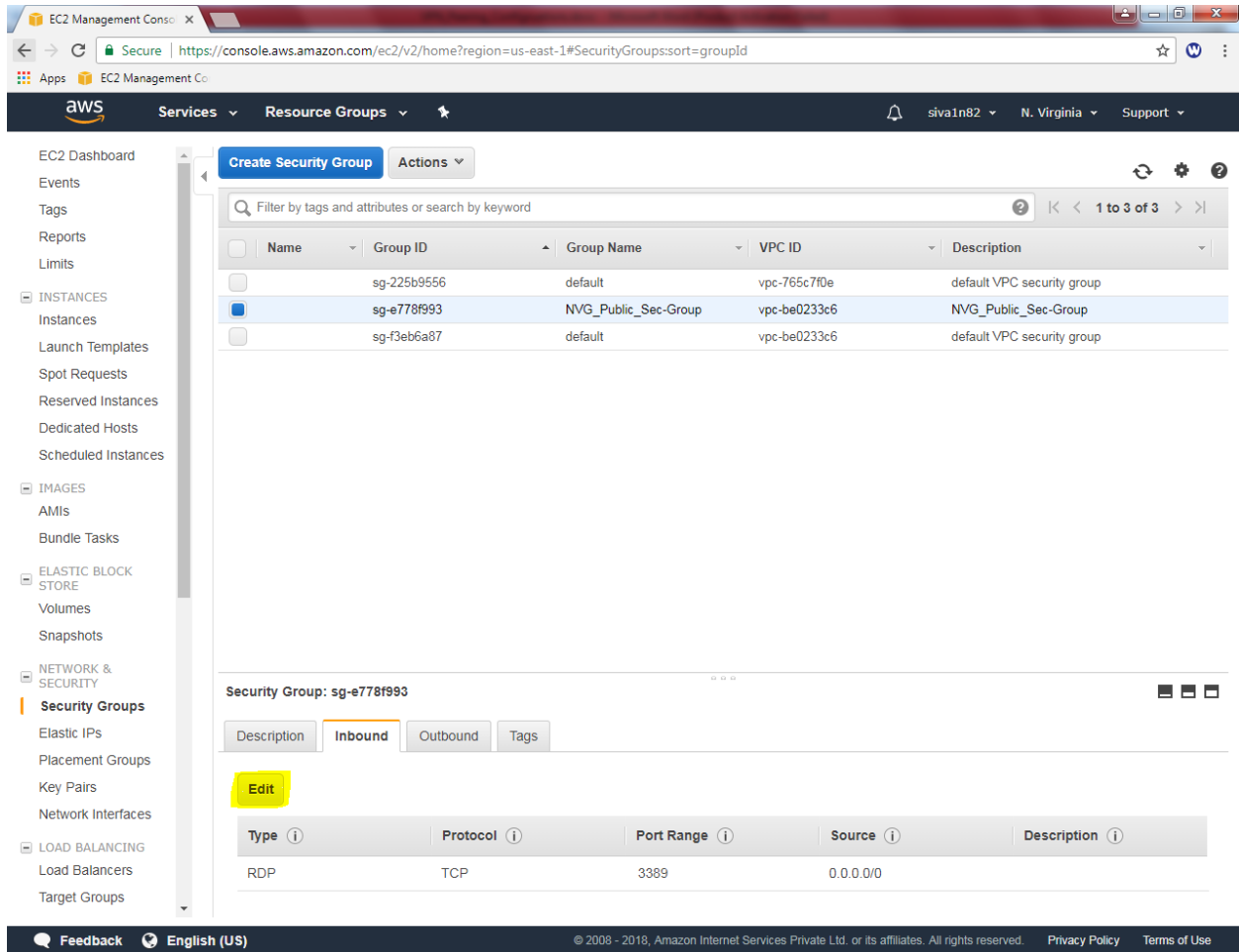


```
Administrator: Command Prompt
Default Gateway . . . . . : 10.0.2.1
Tunnel adapter isatap.ec2.internal:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : ec2.internal
Tunnel adapter Local Area Connection* 3:
    Connection-specific DNS Suffix  . :
    IPv6 Address . . . . . : 2001:0:4137:9e76:1837:dbd:f5ff:fd20
    Link-local IPv6 Address . . . . . : fe80::1837:dbd:f5ff:fd20%5
    Default Gateway . . . . . : ::
C:\Windows\system32>mstsc
C:\Windows\system32>mstsc
C:\Windows\system32>ping 192.168.2.197

Pinging 192.168.2.197 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.197:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Windows\system32>
```

In Security Group, select inbound rule, click “Edit”



The screenshot shows the AWS Management Console interface for the EC2 Management Console. The left sidebar contains a navigation menu with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and LOAD BALANCING. The 'Security Groups' link under NETWORK & SECURITY is highlighted. The main content area shows a list of security groups. The group 'sg-e778f993' is selected, and its details are shown below. The 'Inbound' tab is active, and the 'Edit' button is highlighted in yellow. The inbound rule table shows a single rule for RDP access on port 3389 from 0.0.0.0/0.

Name	Group ID	Group Name	VPC ID	Description
	sg-225b9556	default	vpc-765c7f0e	default VPC security group
	sg-e778f993	NVG_Public_Sec-Group	vpc-be0233c6	NVG_Public_Sec-Group
	sg-f3eb6a87	default	vpc-be0233c6	default VPC security group

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	0.0.0.0/0	

Click “Add rule” Select Custom ICMP Echo Request 0.0.0.0/0

**Edit inbound rules** ✕

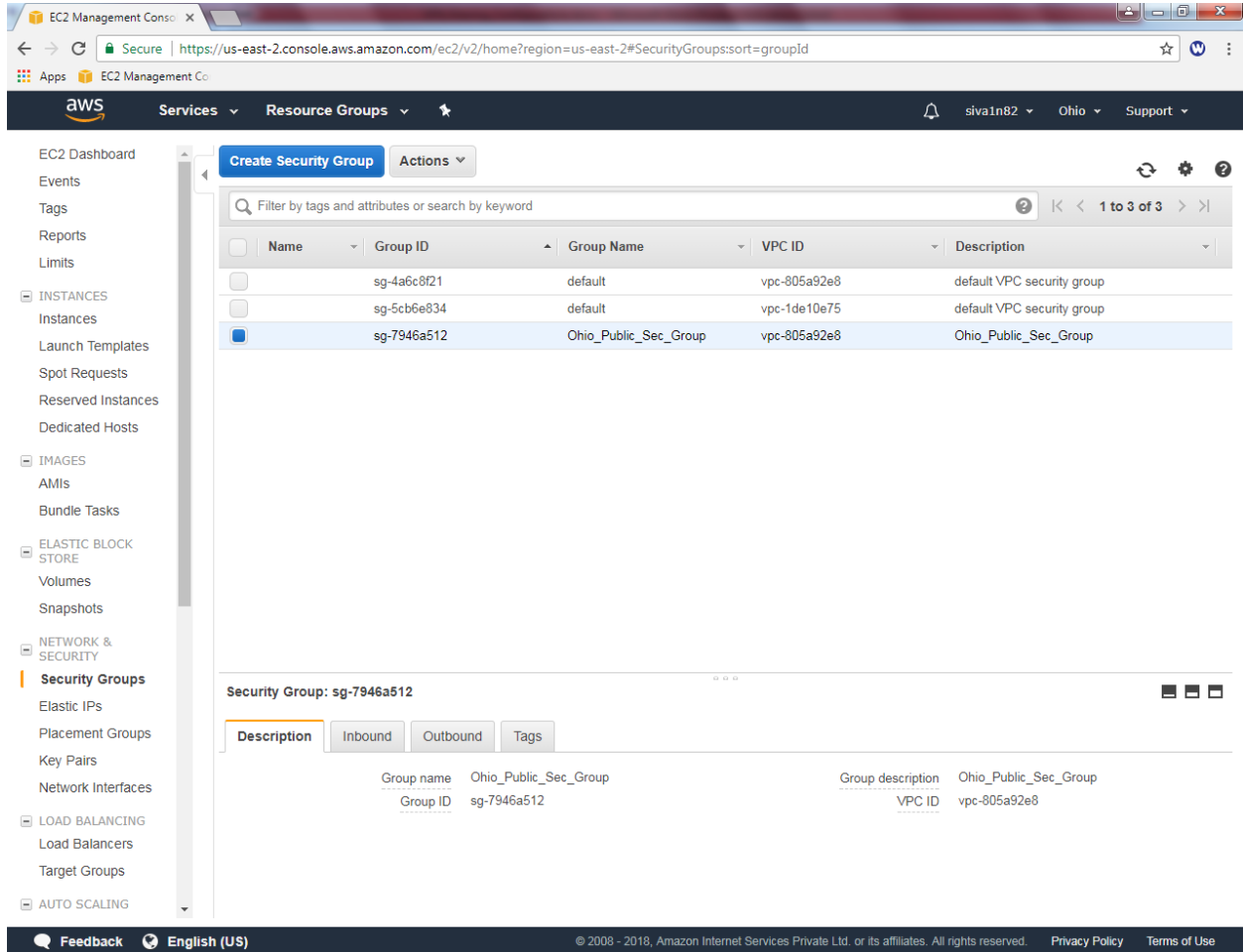
Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ	
RDP ▾	TCP	3389	Custom ▾ 0.0.0.0/0	e.g. SSH for Admin Desktop	✕
Custom ICMP ▾	Echo Request ▾	N/A	Custom ▾ <b>0.0.0.0/0</b>	e.g. SSH for Admin Desktop	✕

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Save

In Ohio region, ohio public security group,



The screenshot shows the AWS Management Console for the Ohio region. The left sidebar lists various services, with 'Security Groups' highlighted under 'NETWORK & SECURITY'. The main content area displays a table of security groups. The group 'sg-7946a512' (Ohio\_Public\_Sec\_Group) is selected. Below the table, the 'Description' tab is active, showing the group's name, ID, description, and VPC ID.

Name	Group ID	Group Name	VPC ID	Description
	sg-4a6c8f21	default	vpc-805a92e8	default VPC security group
	sg-5cb6e834	default	vpc-1de10e75	default VPC security group
<input checked="" type="checkbox"/>	sg-7946a512	Ohio_Public_Sec_Group	vpc-805a92e8	Ohio_Public_Sec_Group

**Security Group: sg-7946a512**

**Description** | Inbound | Outbound | Tags

Group name	Ohio_Public_Sec_Group	Group description	Ohio_Public_Sec_Group
Group ID	sg-7946a512	VPC ID	vpc-805a92e8

Click "Inbound" rule, then click "Edit".



Click "Add rule" Select Custom ICMP Echo Request 0.0.0.0/0

Edit inbound rules

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
Custom ICMP	Echo Reque	N/A	Custom 0.0.0.0/16	e.g. SSH for Admin Desktop

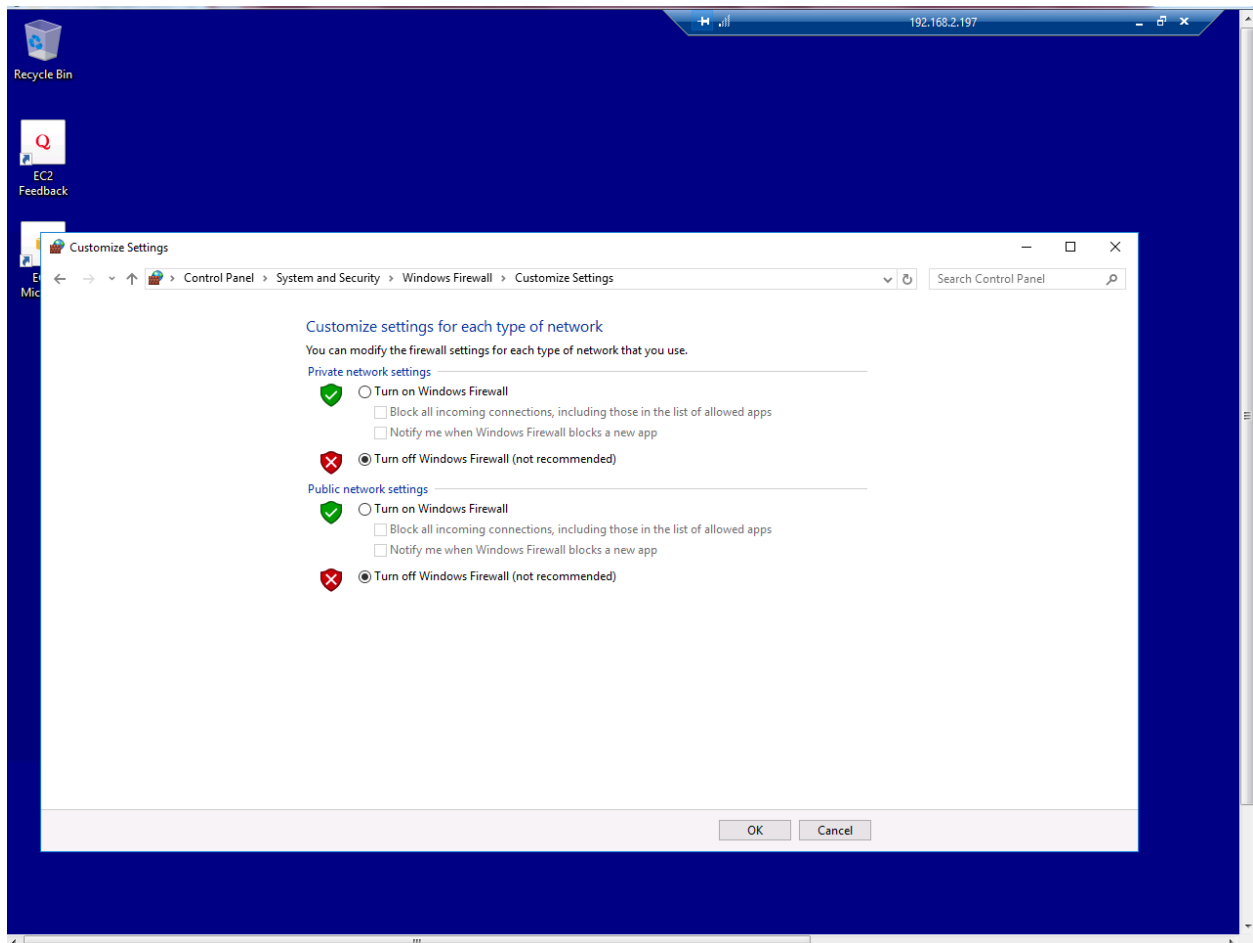
Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

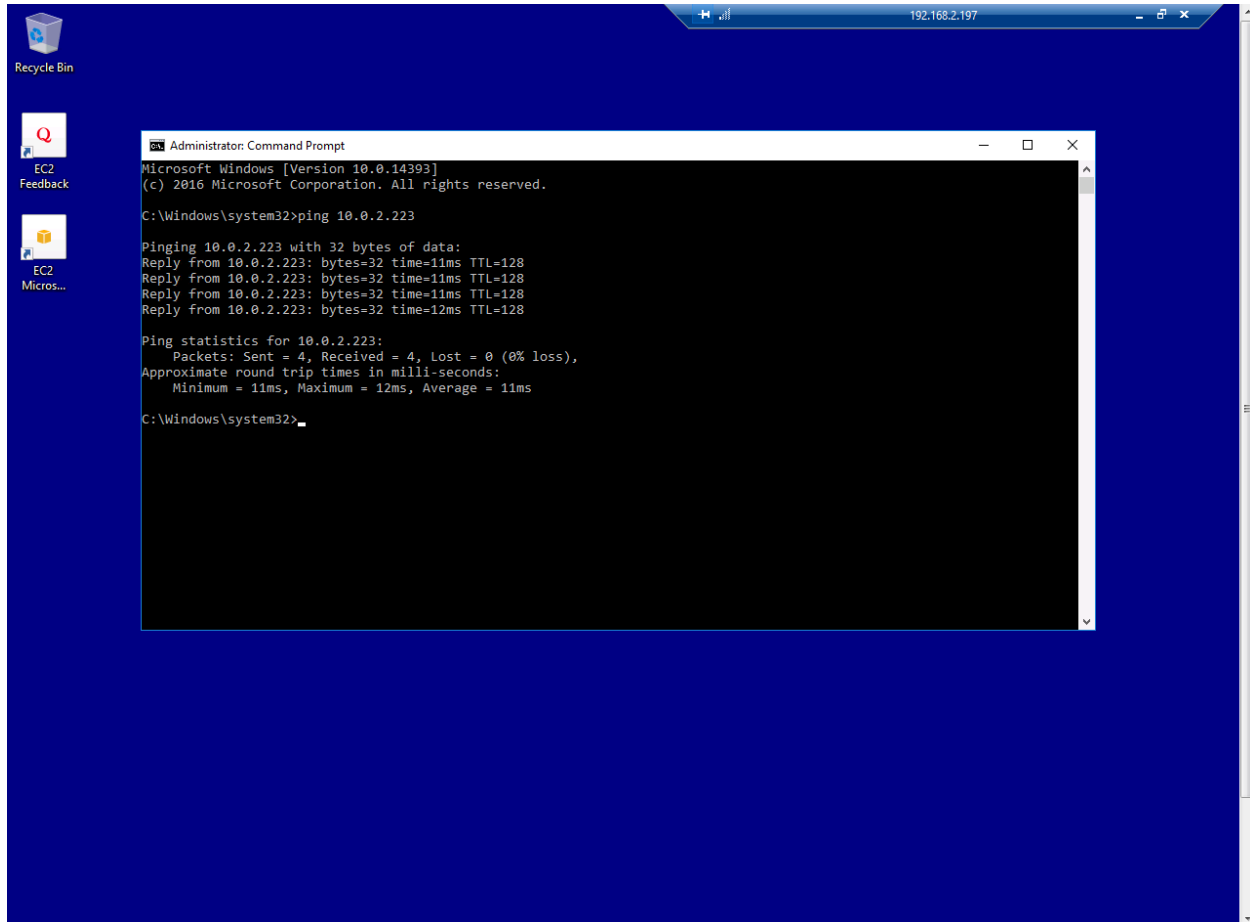
Cancel Save

Then try to ping LAN segment IP will not ping due to firewall is turned on in Windows Server 2016. We need to **Turn off on both Servers (North Virginia and Ohio).**

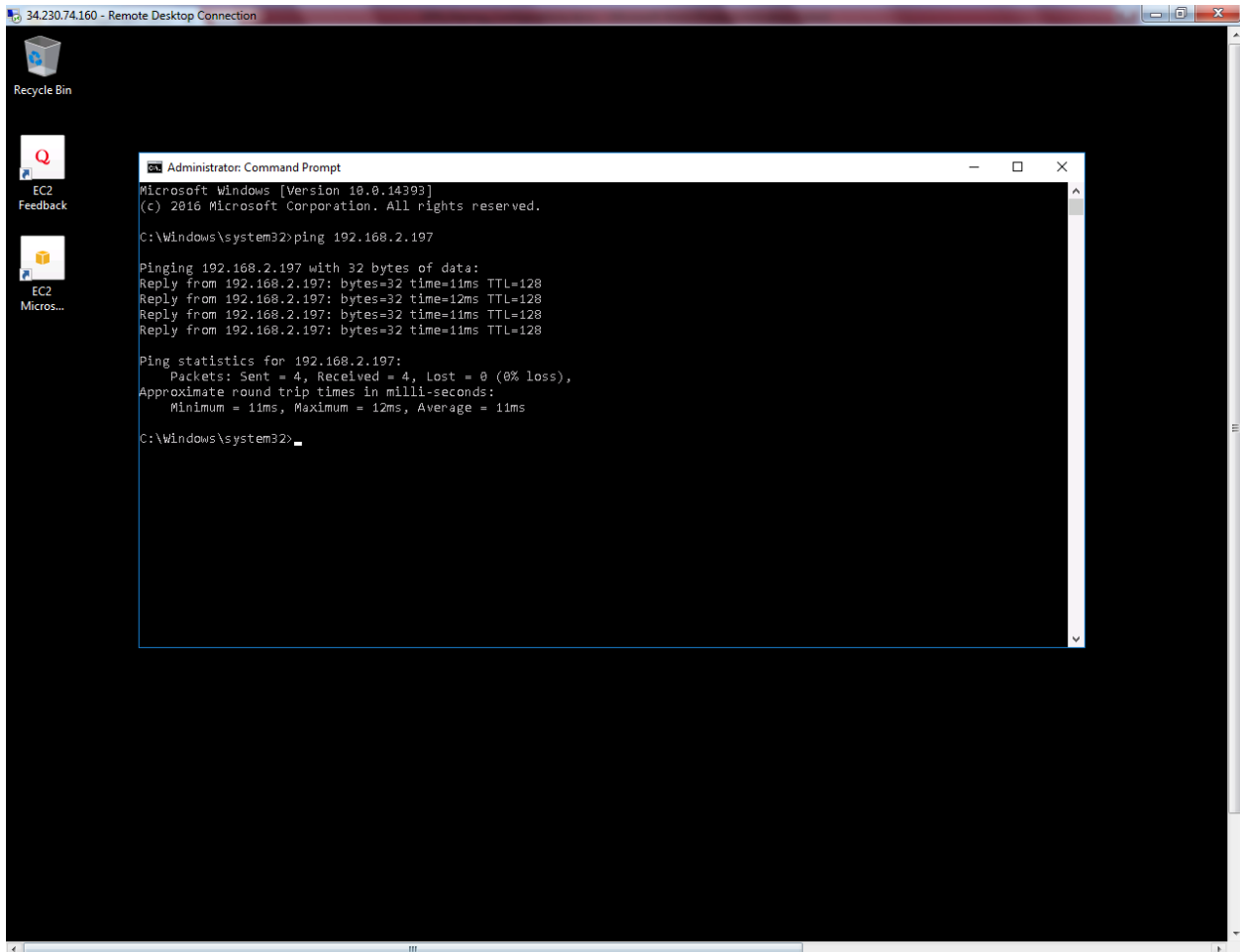
In windows 2016 server, Right click start menu click command prompt and type `firewall.cpl` to get windows firewall. Click “Turn windows firewall on or off”.



Now We are able ping 10.0.2.223 North Virginia host from Ohio subnet 192.168.2.0/24



Now We are able ping 192.168.2.197 Ohio host from North Virginia subnet 10.0.2.0/24 subnet.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 192.168.2.197

Pinging 192.168.2.197 with 32 bytes of data:
Reply from 192.168.2.197: bytes=32 time=11ms TTL=128
Reply from 192.168.2.197: bytes=32 time=12ms TTL=128
Reply from 192.168.2.197: bytes=32 time=11ms TTL=128
Reply from 192.168.2.197: bytes=32 time=11ms TTL=128

Ping statistics for 192.168.2.197:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 12ms, Average = 11ms

C:\Windows\system32>
```