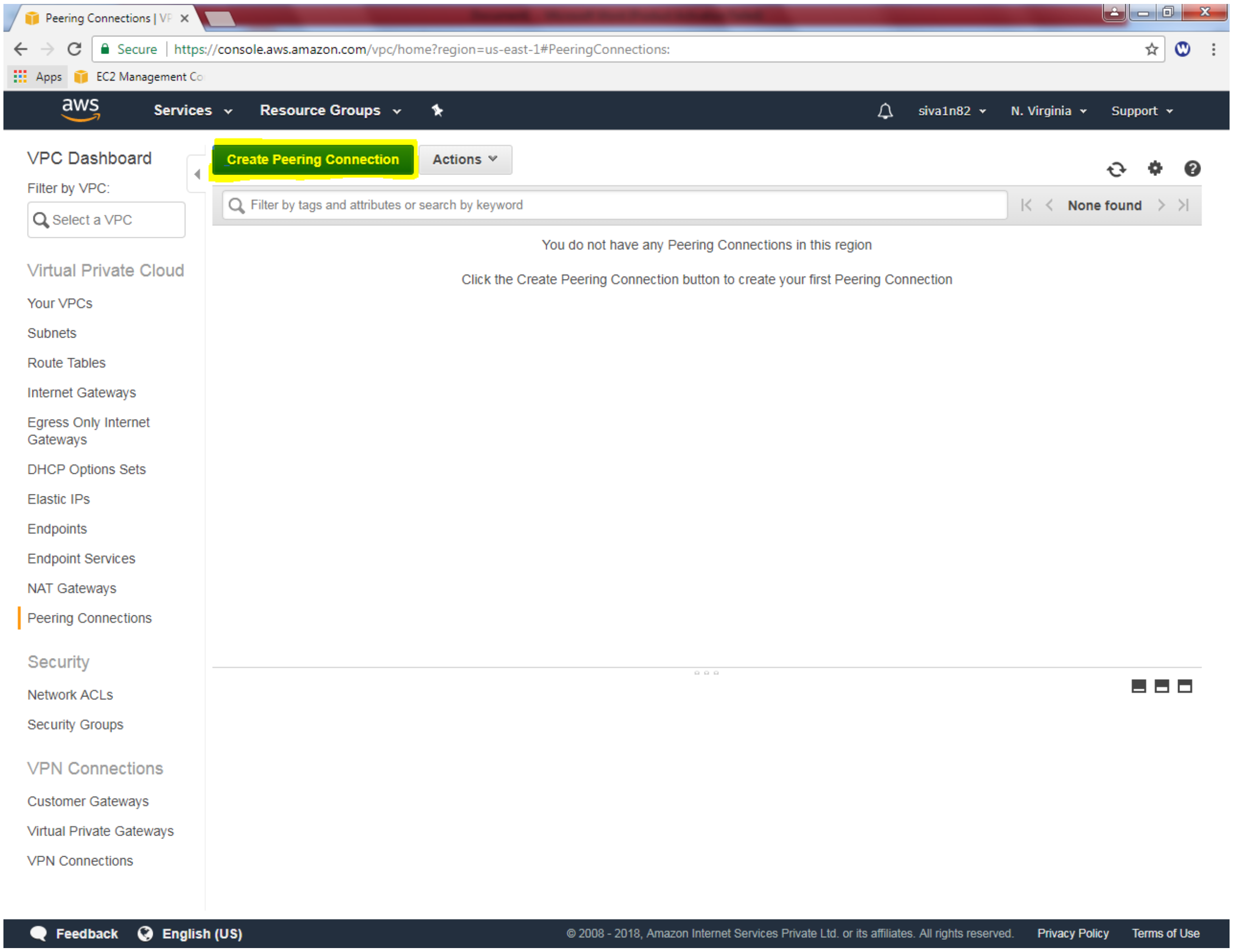
Lab 12

VPC Peering Lab – 3 of 3

Goto “N.Virginia”region,

Goto VPC Dashboard,

Click “Peering connections”



https://console.aws.amazon.com/vpc/home?region=us-east-1#PeeringConnections:

You do not have any Peering Connections in this region

Click the Create Peering Connection button to create your first Peering Connection

Click “Create Peering Connections”.

In peering Connection,

Peering Connection name tag: VPC Peer Ohio_NVG

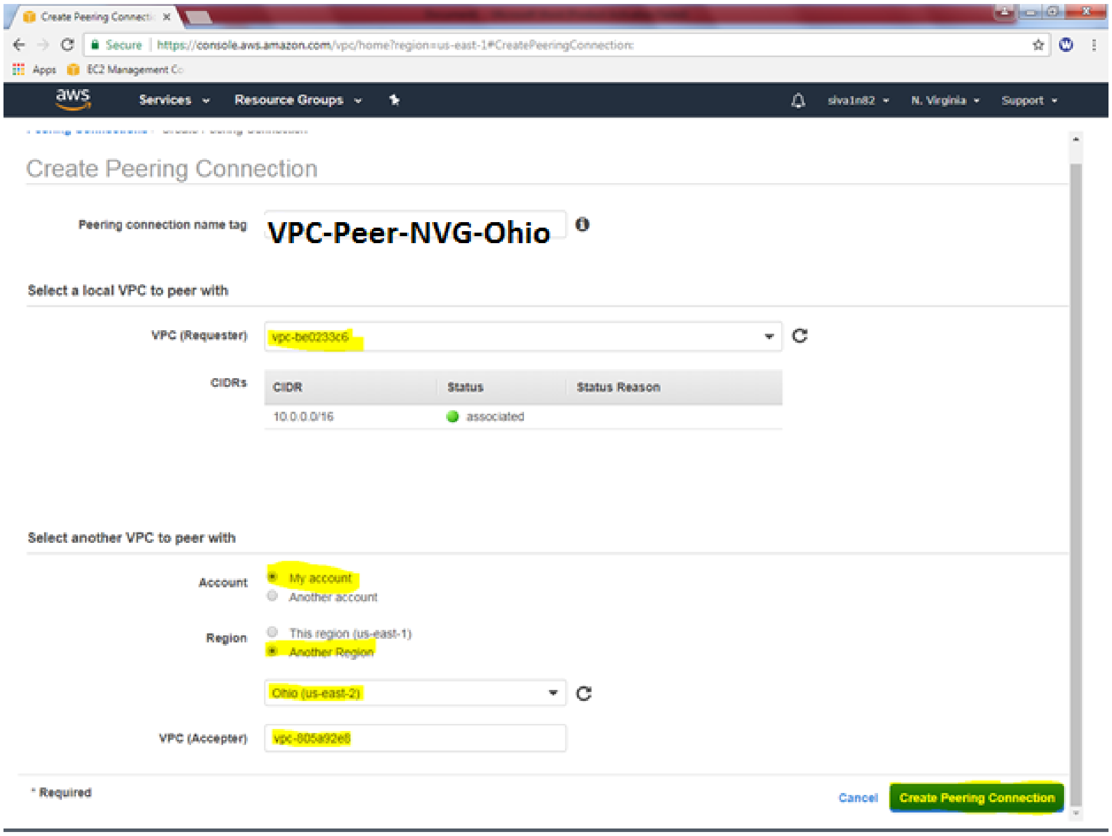
VPC Requestor : VPC_North Virginia

Account : MyAccount

Region : Another Region

Select: Ohio

VPC Accepter : 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-be0233c6

CIDRs

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

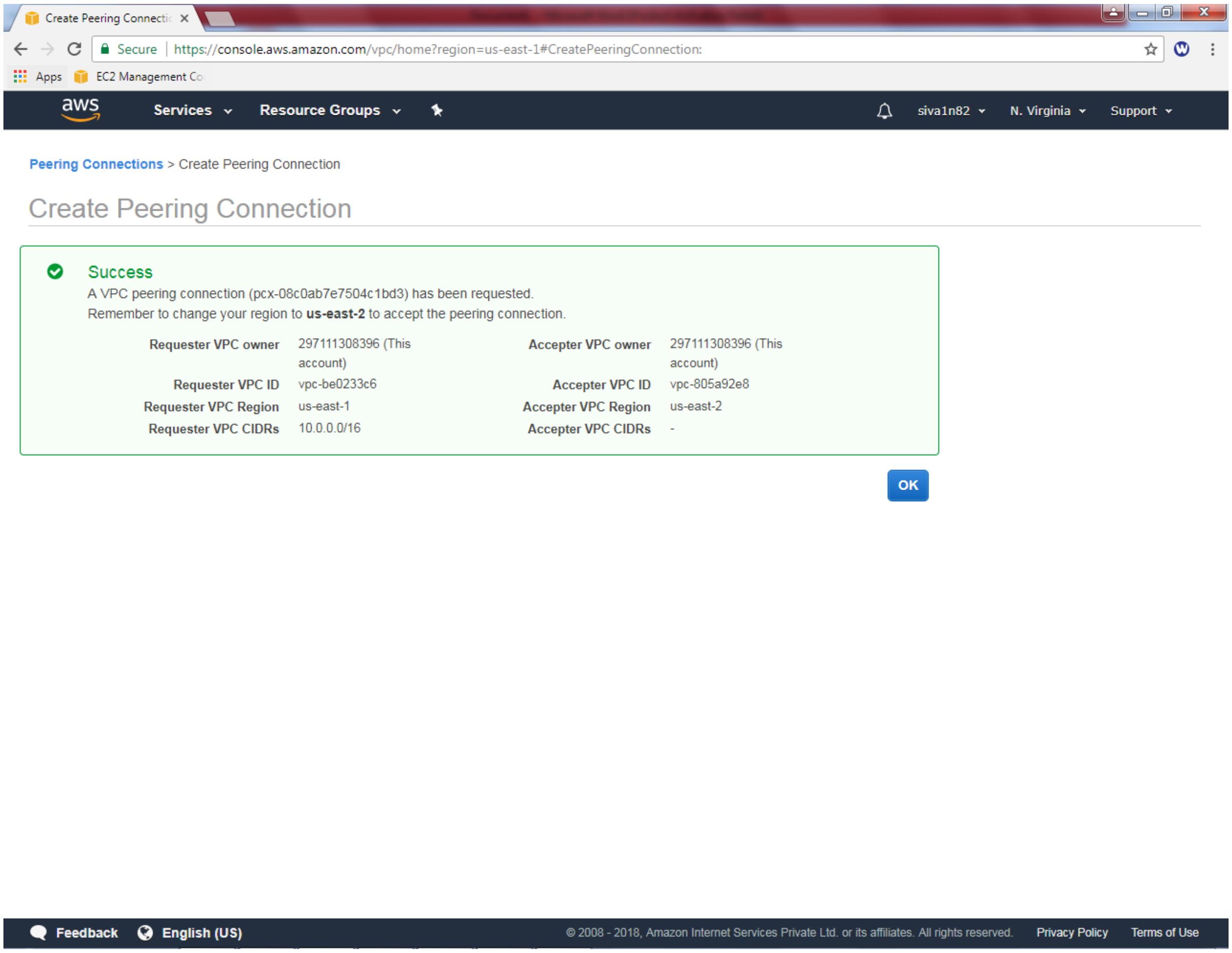
Ohio (us-east-2)

VPC (Accepter): vpc-805a92e8

* Required

Click “Create Peering Connection”.

VPC Peering Created successfully.



Create Peering Connecti
Secure | https://console.aws.amazon.com/vpc/home?region=us-east-1#CreatePeeringConnection:
Apps
EC2 Management Co
aws
Services
Resource Groups
siva1n82
N. Virginia
Support
Peering Connections > Create Peering Connection

Create Peering Connection

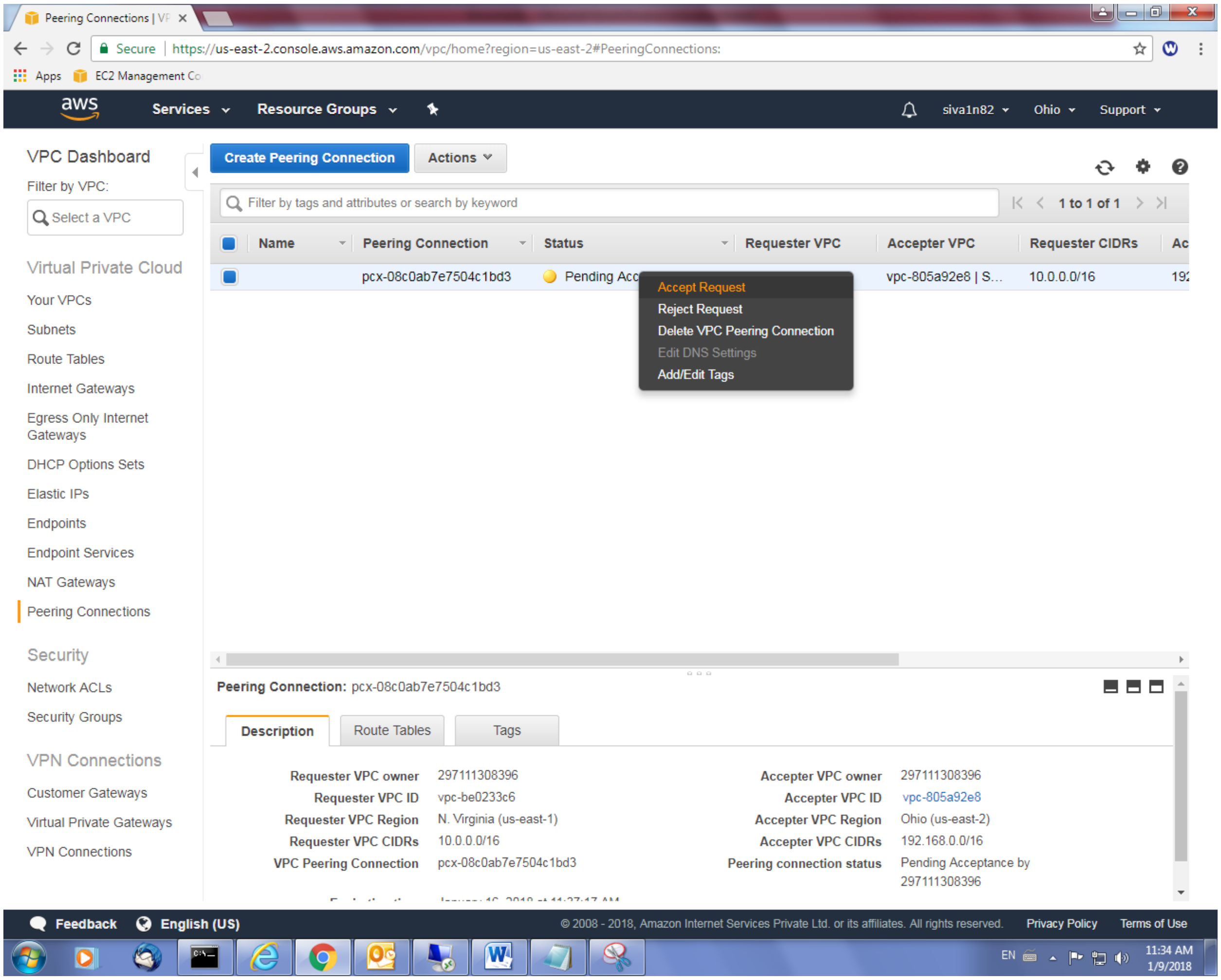
Success

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

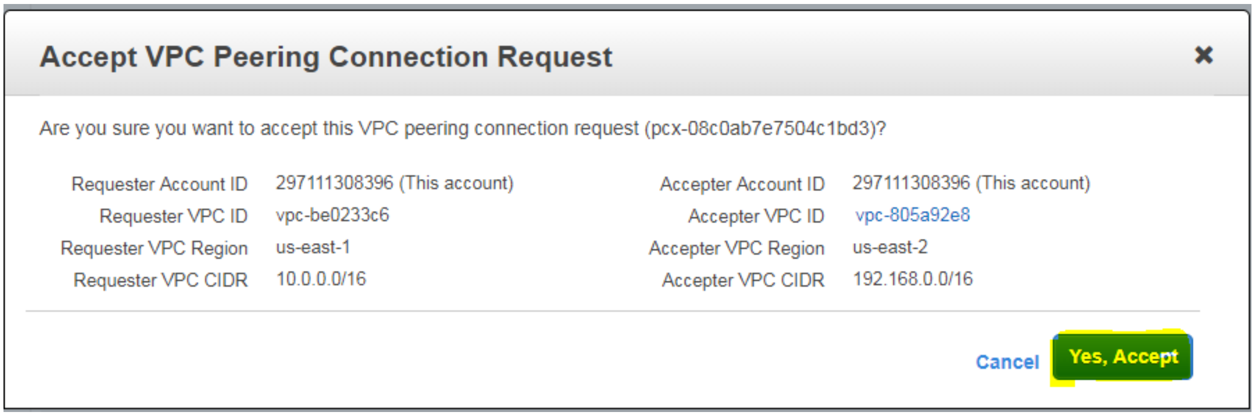


Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Ac
	pcx-08c0ab7e7504c1bd3	Pending Acc		vpc-805a92e8 | S...	10.0.0.0/16	192

Peering Connection: pcx-08c0ab7e7504c1bd3

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”.

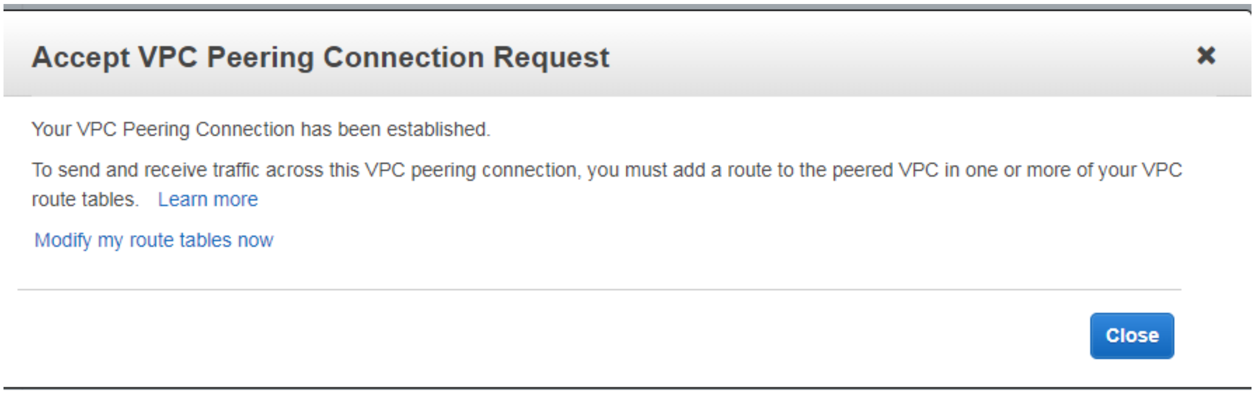


Accept VPC Peering Connection Request

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	vpc-805a92e8
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

Click “Yes Acccept”.



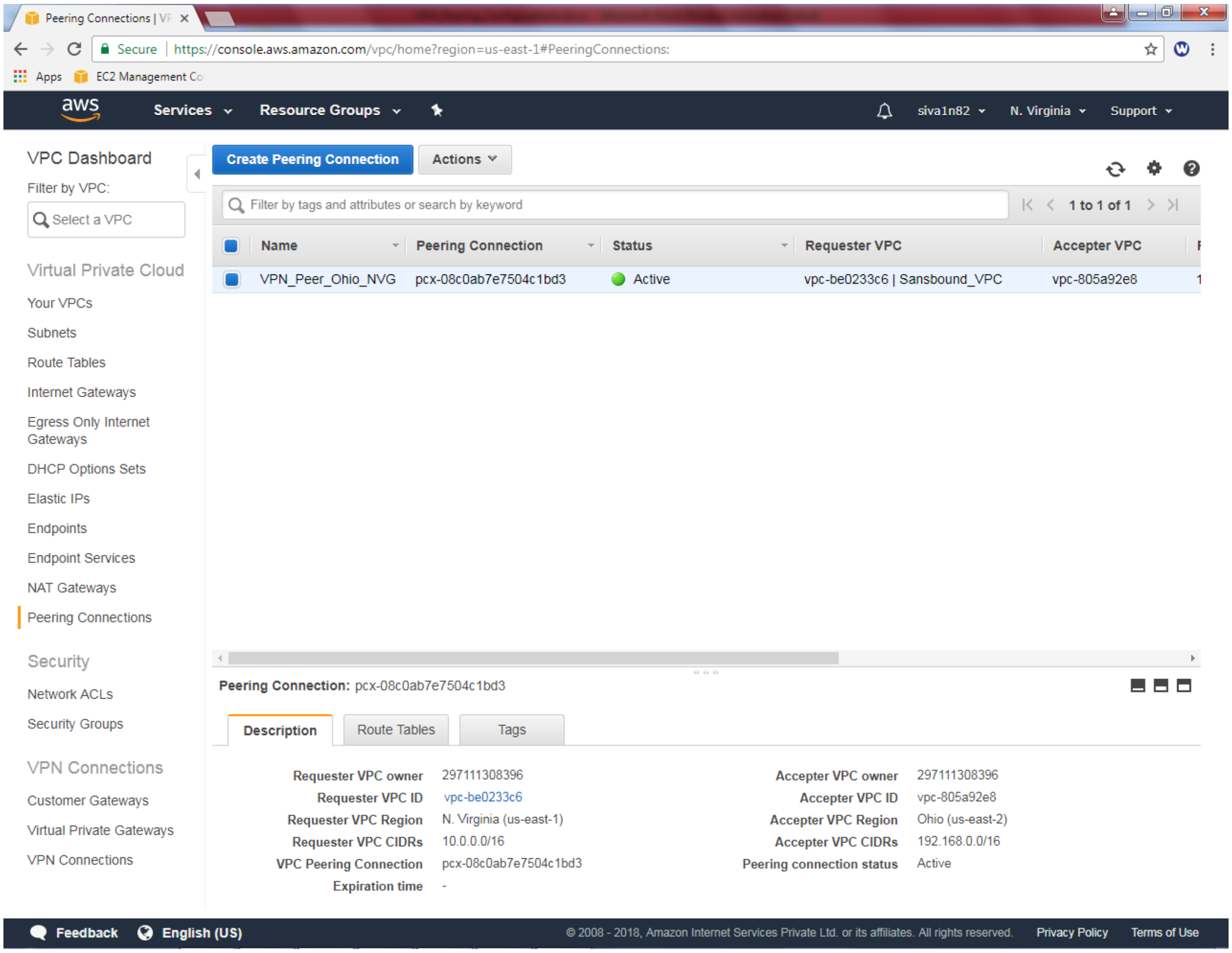
Accept VPC Peering Connection Request

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

VPC Status of N.Virginia is active.

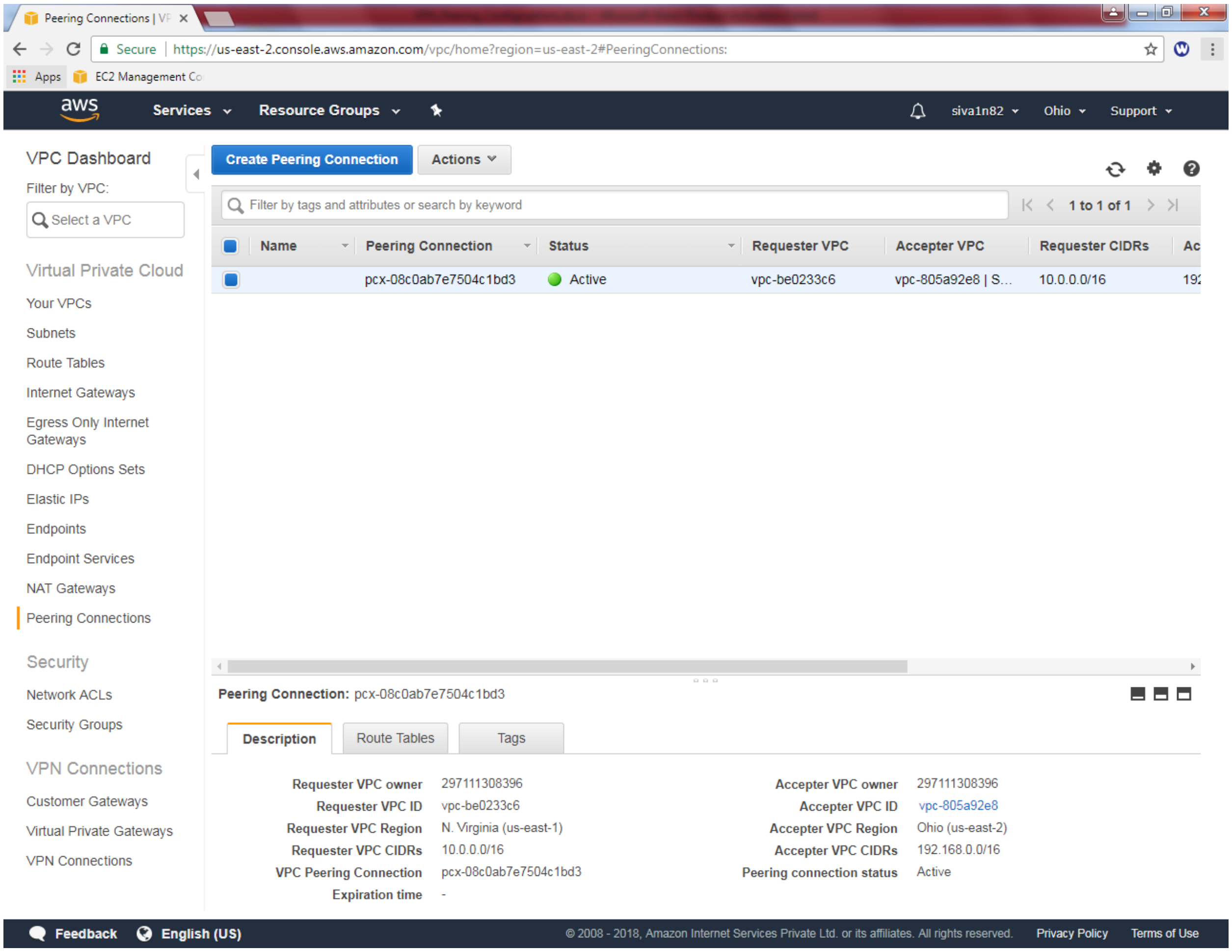


Name	Peering Connection	Status	Requester VPC	Accepter VPC
VPN_Peer_Ohio_NVG	pcx-08c0ab7e7504c1bd3	● Active	vpc-be0233c6 | Sansbound_VPC	vpc-805a92e8

Peering Connection: pcx-08c0ab7e7504c1bd3

Requester VPC owner	297111308396	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	-		

VPC Status of Ohiio is active.



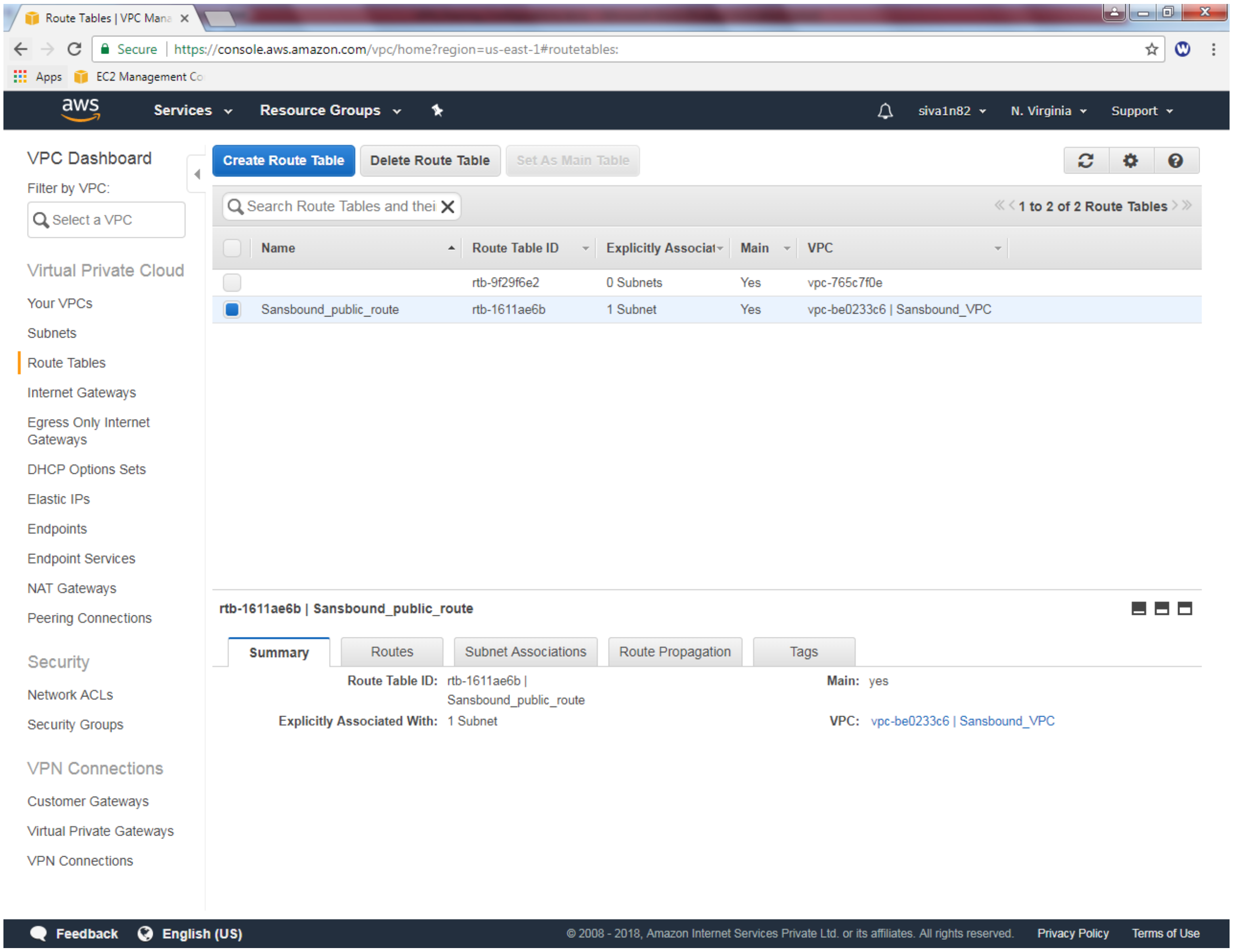
Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Ac
	pcx-08c0ab7e7504c1bd3	● Active	vpc-be0233c6	vpc-805a92e8 | S...	10.0.0.0/16	192

Peering Connection: pcx-08c0ab7e7504c1bd3

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	-		

Feedback
English (US)
© 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.



	Name	Route Table ID	Explicitly Associat	Main	VPC
□		rtb-9f29f6e2	0 Subnets	Yes	vpc-765c7f0e
☑	Sansbound_public_route	rtb-1611ae6b	1 Subnet	Yes	vpc-be0233c6 | Sansbound_VPC

rtb-1611ae6b | Sansbound_public_route

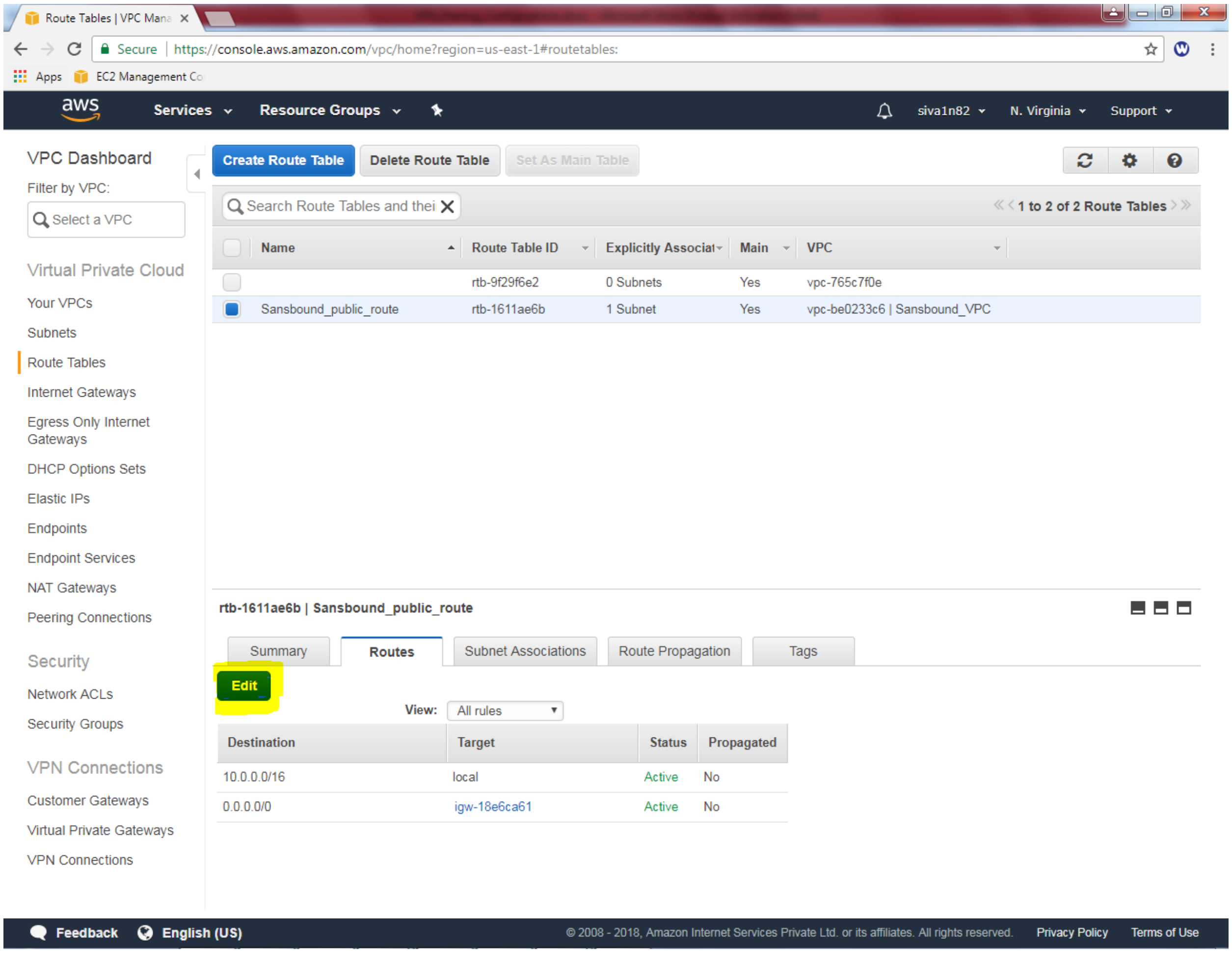
Route Table ID: rtb-1611ae6b | Sansbound_public_route

Main: yes

Explicitly Associated With: 1 Subnet

VPC: vpc-be0233c6 | Sansbound_VPC

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



	Name	Route Table ID	Explicitly Associat	Main	VPC
□		rtb-9f29f6e2	0 Subnets	Yes	vpc-765c7f0e
■	Sansbound_public_route	rtb-1611ae6b	1 Subnet	Yes	vpc-be0233c6 | Sansbound_VPC

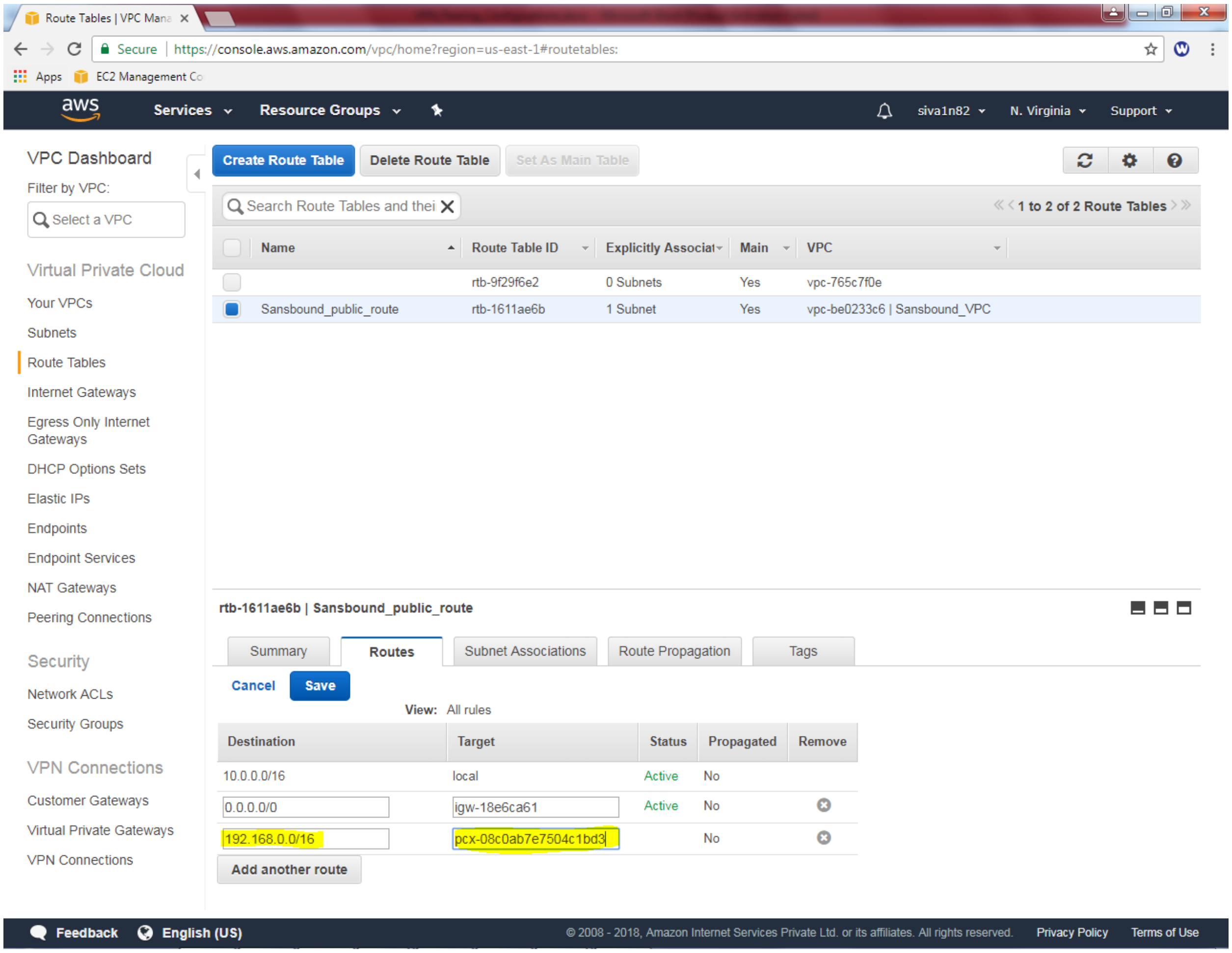
rtb-1611ae6b | Sansbound_public_route

View: All rules

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

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

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



Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-9f29f6e2	0 Subnets	Yes	vpc-765c7f0e
Sansbound_public_route	rtb-1611ae6b	1 Subnet	Yes	vpc-be0233c6 | Sansbound_VPC

rtb-1611ae6b | Sansbound_public_route

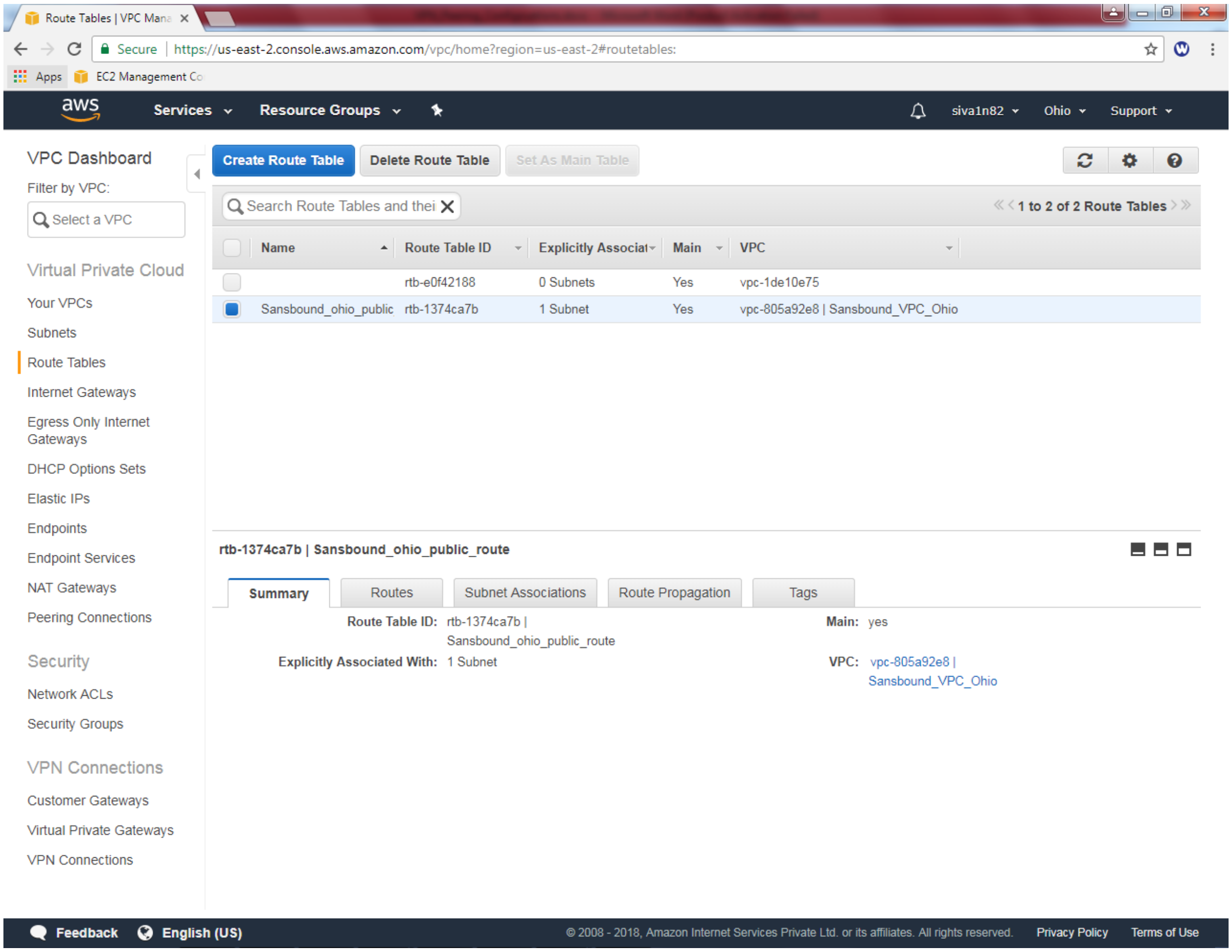
Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	igw-18e6ca61	Active	No	⊗
192.168.0.0/16	pcx-08c0ab7e7504c1bd3		No	⊗

Then click save.

Goto ohio region,

Goto VPC Dashboard,

Click route table, then select “Sansbound_Ohio_public”



	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

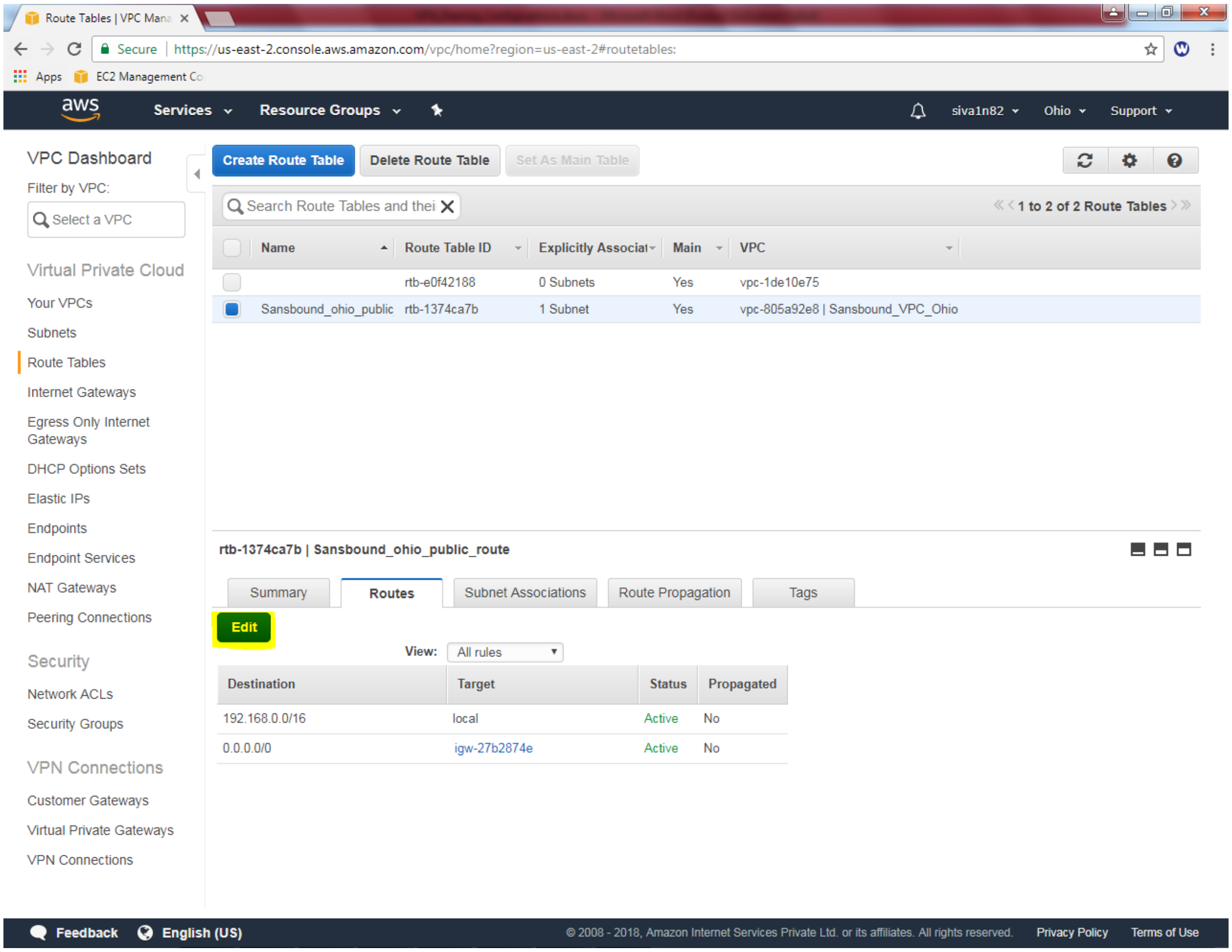
Route Table ID: rtb-1374ca7b | Sansbound_ohio_public_route

Explicitly Associated With: 1 Subnet

Main: yes

VPC: vpc-805a92e8 | Sansbound_VPC_Ohio

In Sansbound_ohio_public routing table, route option and then click “Edit”

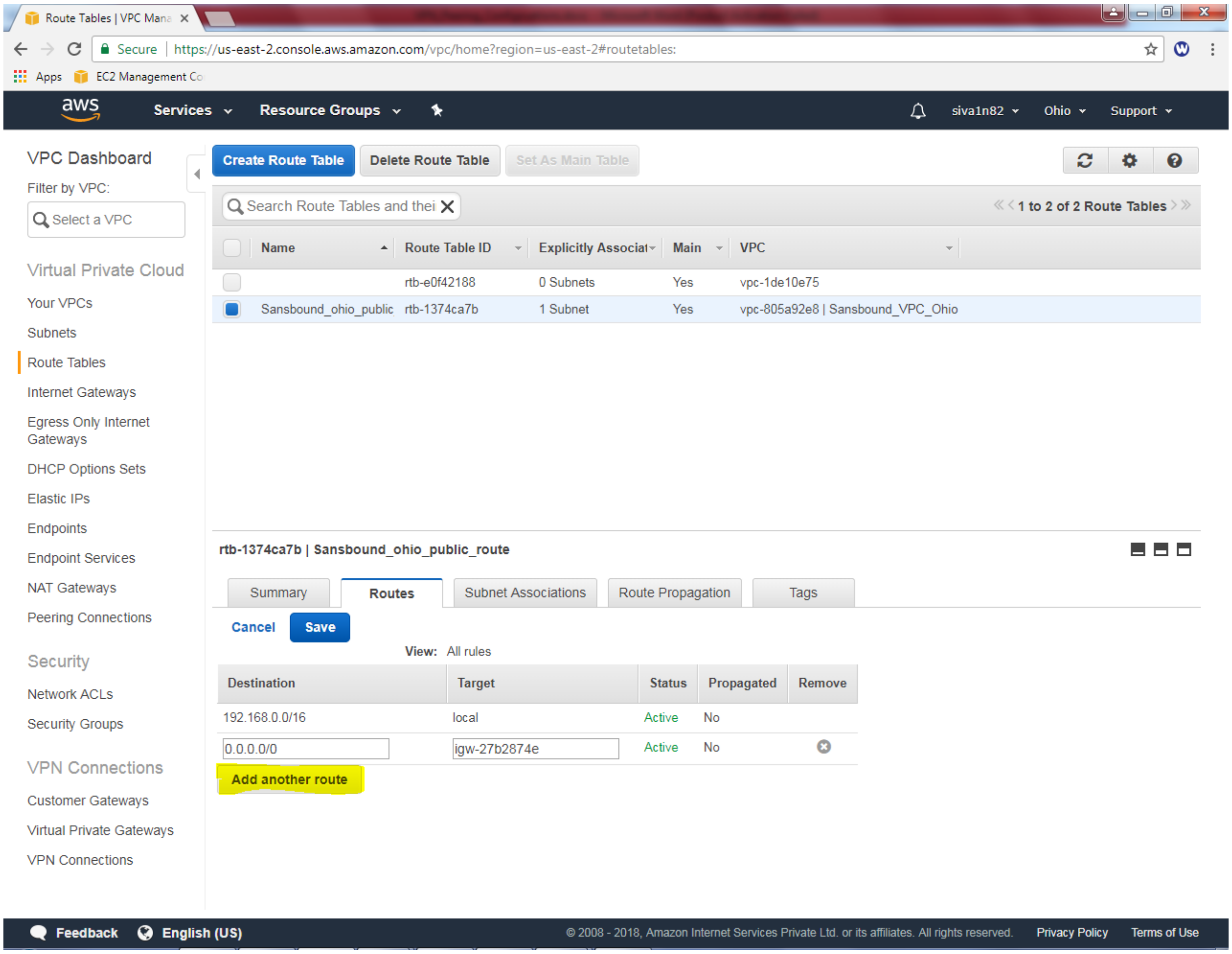


	Name	Route Table ID	Explicitly Associat	Main	VPC
□		rtb-e0f42188	0 Subnets	Yes	vpc-1de10e75
☑	Sansbound_ohio_public	rtb-1374ca7b	1 Subnet	Yes	vpc-805a92e8 | Sansbound_VPC_Ohio

rtb-1374ca7b | Sansbound_ohio_public_route

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”



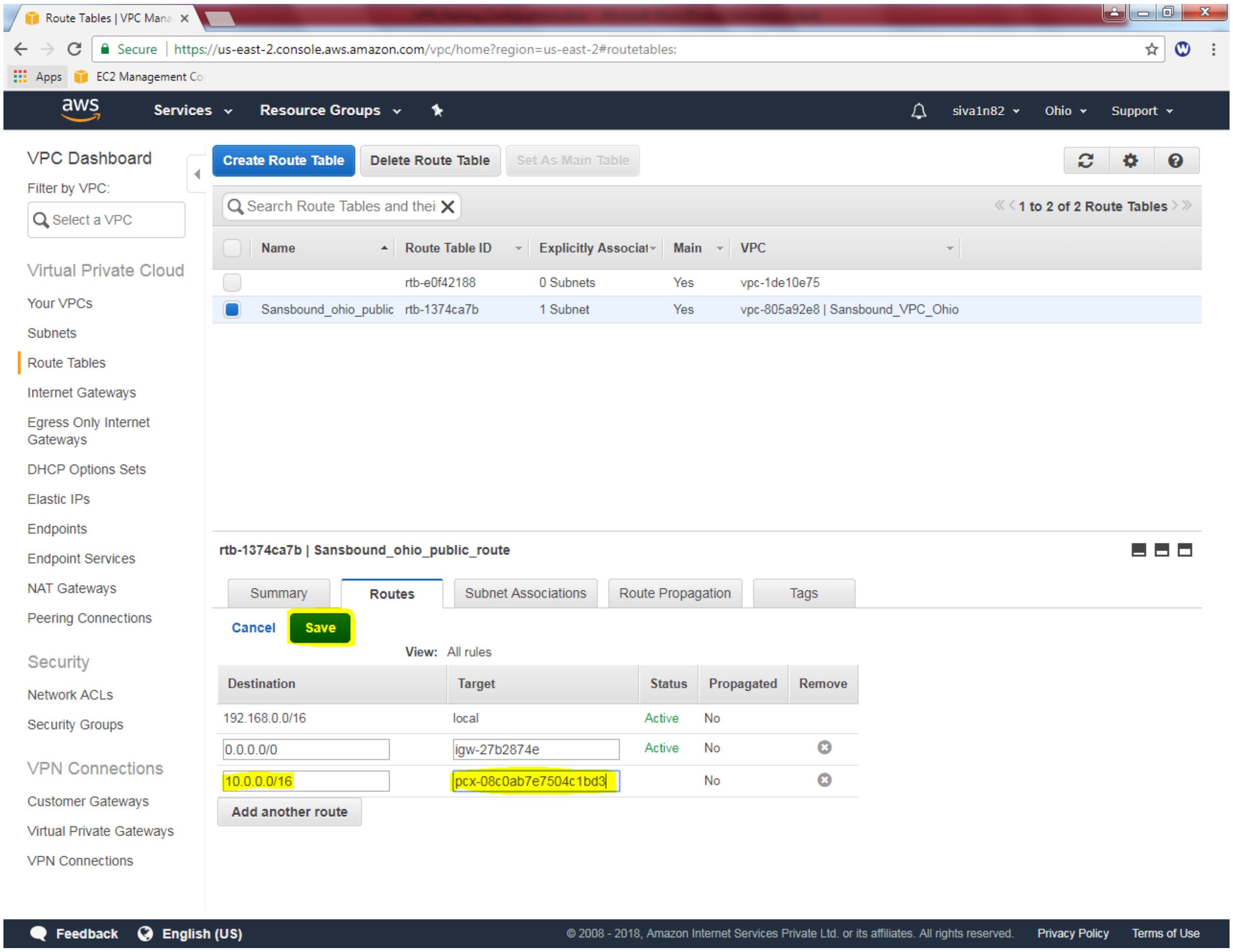
Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-e0f42188	0 Subnets	Yes	vpc-1de10e75
Sansbound_ohio_public	rtb-1374ca7b	1 Subnet	Yes	vpc-805a92e8 | Sansbound_VPC_Ohio

rtb-1374ca7b | Sansbound_ohio_public_route

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	⊗

In Sansbound_Ohio_public_route table type N.Virginia subnet 10.0.0.0/16 and select target as **“pcx-*”**



	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

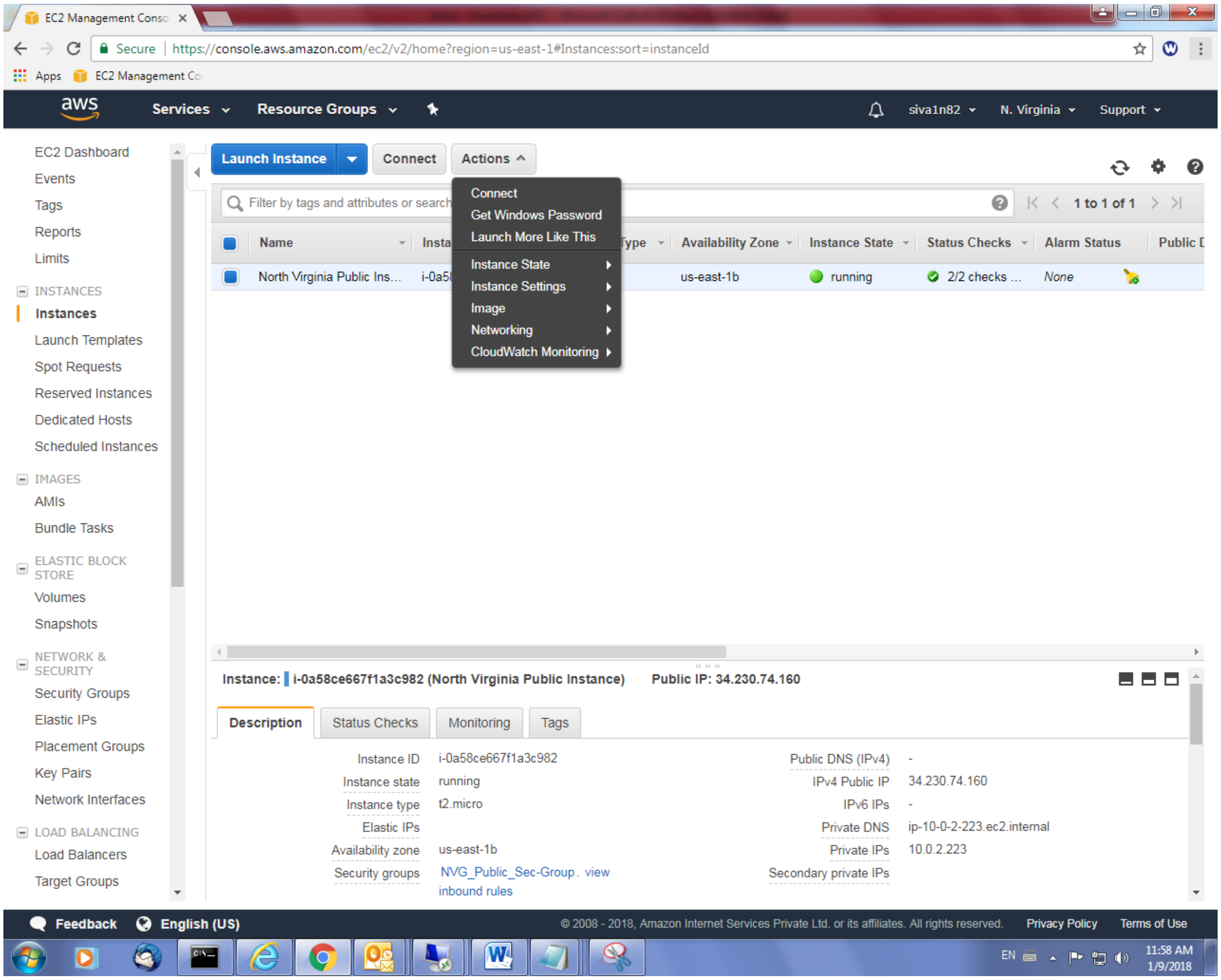
View: All rules

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

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

Actions → Connect

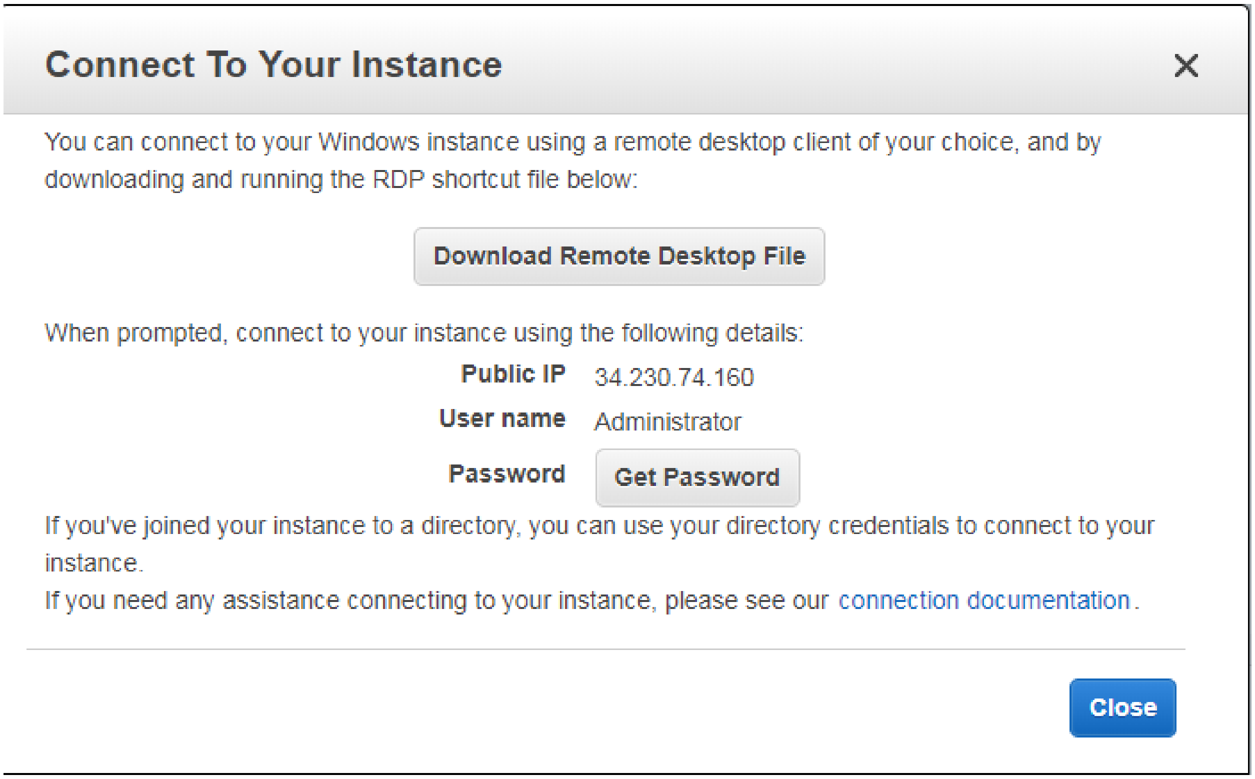


Name	Insta	Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public D
North Virginia Public Ins...	i-0a5		us-east-1b	running	2/2 checks ...	None	

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

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

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

Public IP 34.230.74.160

User name Administrator

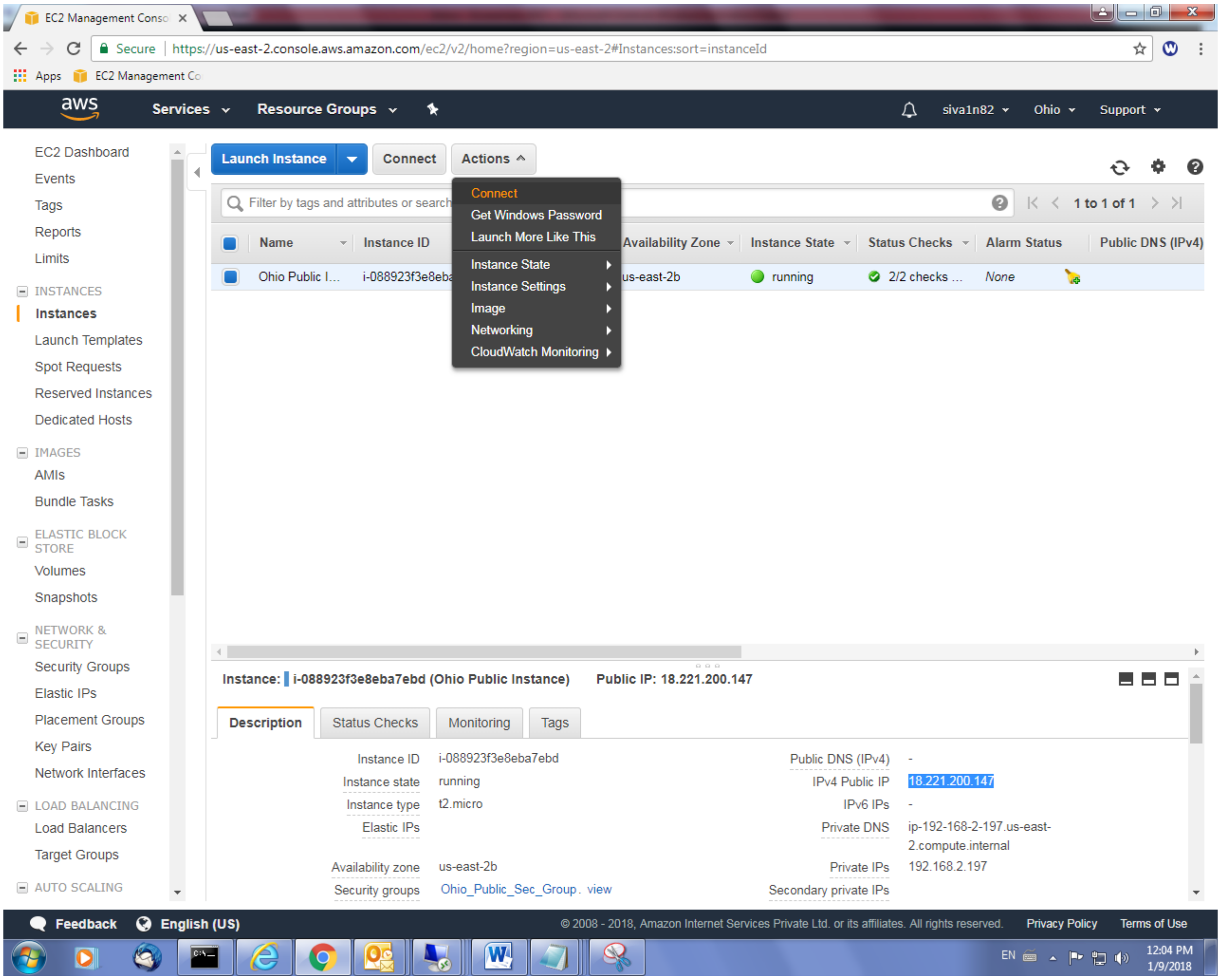
Password

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.

Choose the *.pem file and decrypt the password.

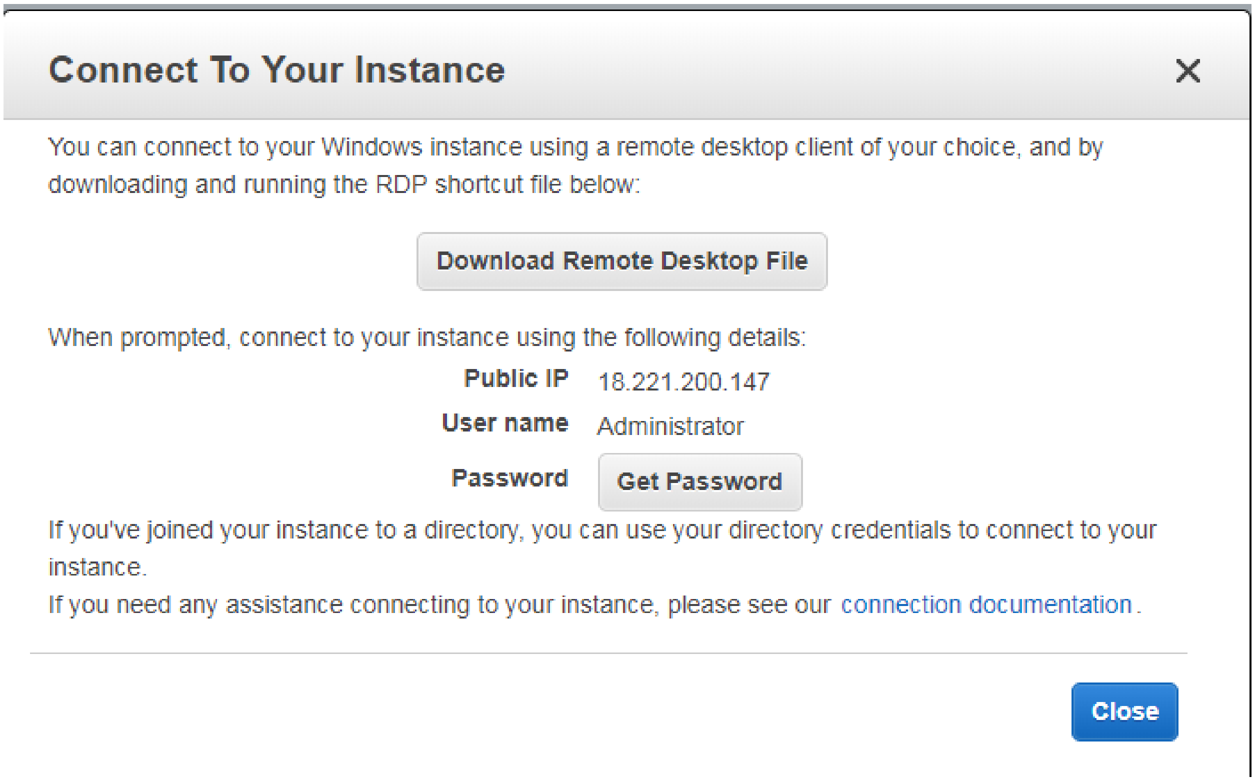
Goto ohio region, select the instance and Actions → Connect.



Name	Instance ID	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
Ohio Public I...	i-088923f3e8eba	us-east-2b	running	2/2 checks ...	None	

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

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:

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

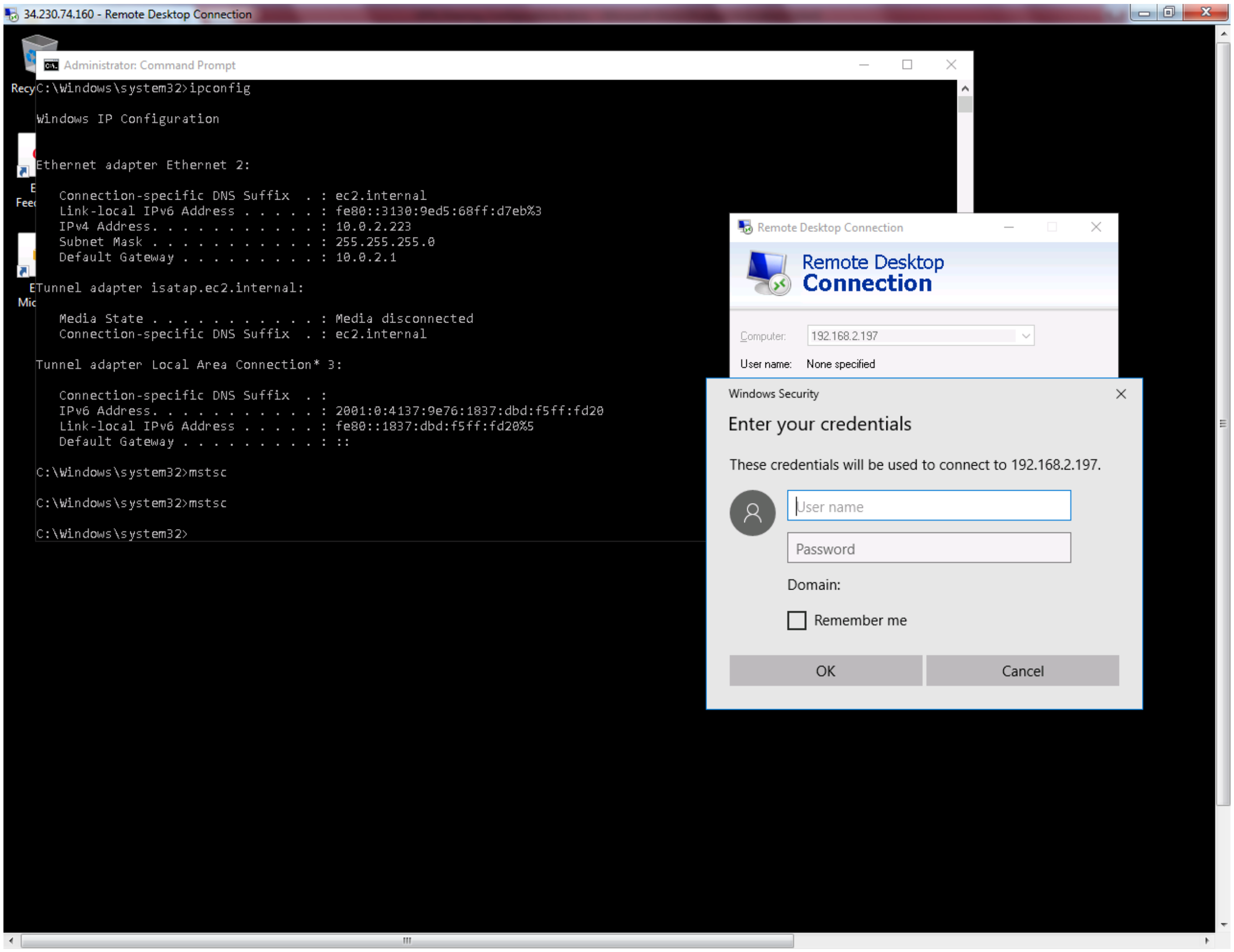
Public IP	18.221.200.147
User name	Administrator
Password	Get Password

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.

Choose the *.pem file and decrypt the password.

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


34.230.74.160 - Remote Desktop Connection
Administrator: Command Prompt
Remote Desktop Connection
Remote Desktop Connection
Windows Security
User name
Password
OK
Cancel

```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : ec2.internal
   Link-local IPv6 Address . . . . . : fe80::3130:9ed5:68ff:d7eb%3
   IPv4 Address. . . . . . . . . . . : 10.0.2.223
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   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>
```

Computer: 192.168.2.197

User name: None specified

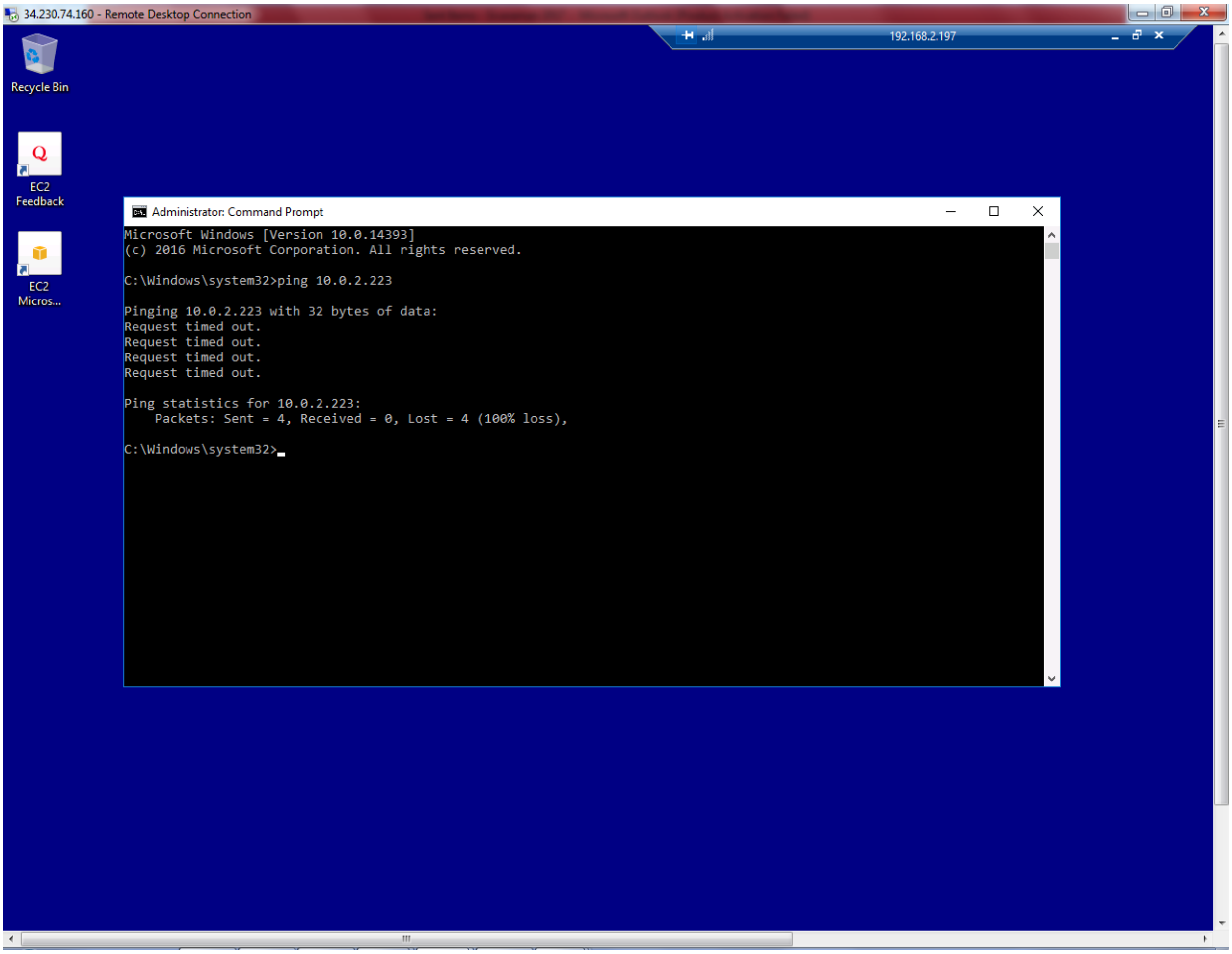
Enter your credentials

These credentials will be used to connect to 192.168.2.197.

Domain:

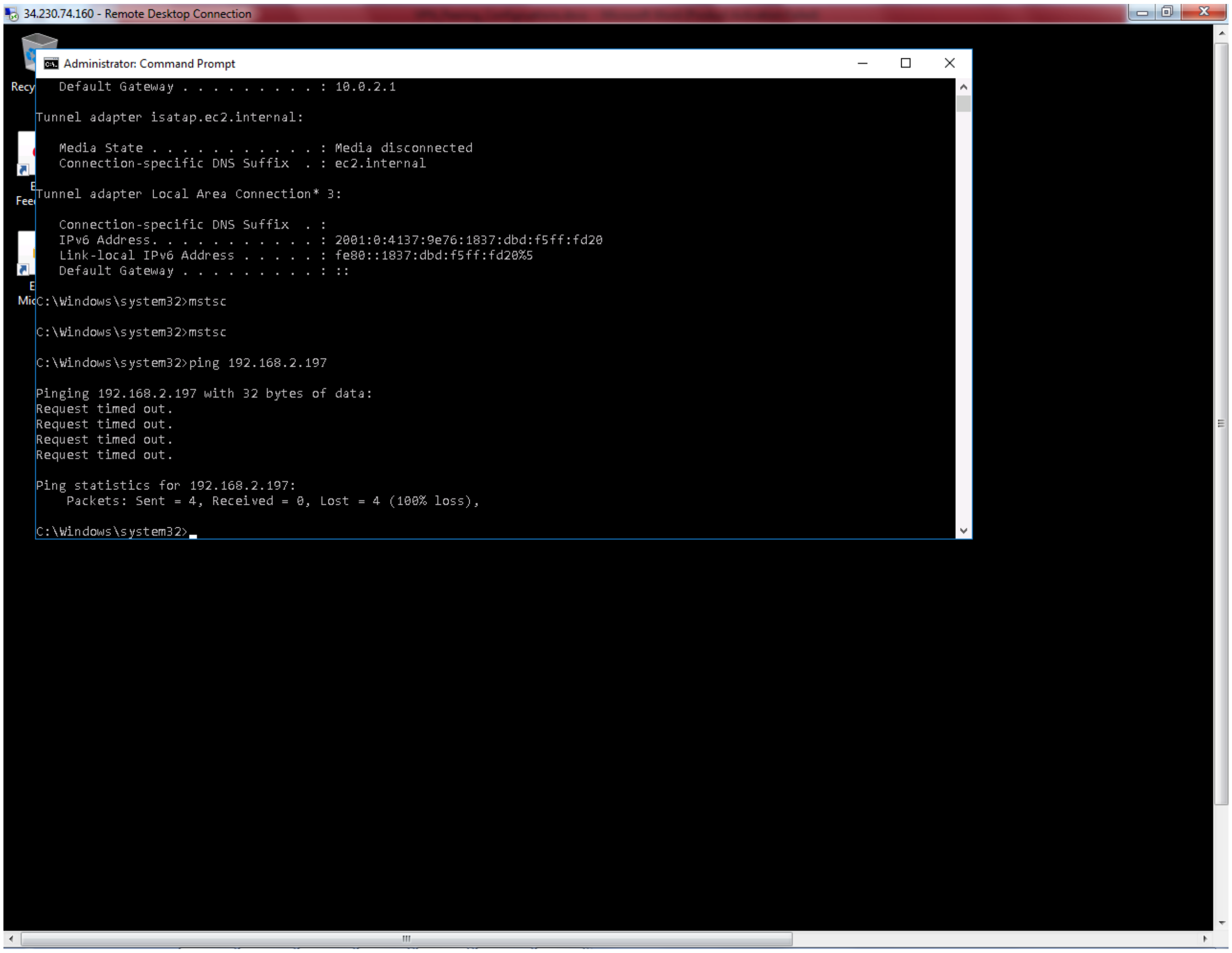
□ Remember me

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.


34.230.74.160 - Remote Desktop Connection
192.168.2.197
Recycle Bin
EC2 Feedback
EC2 Micros...
Administrator: Command Prompt

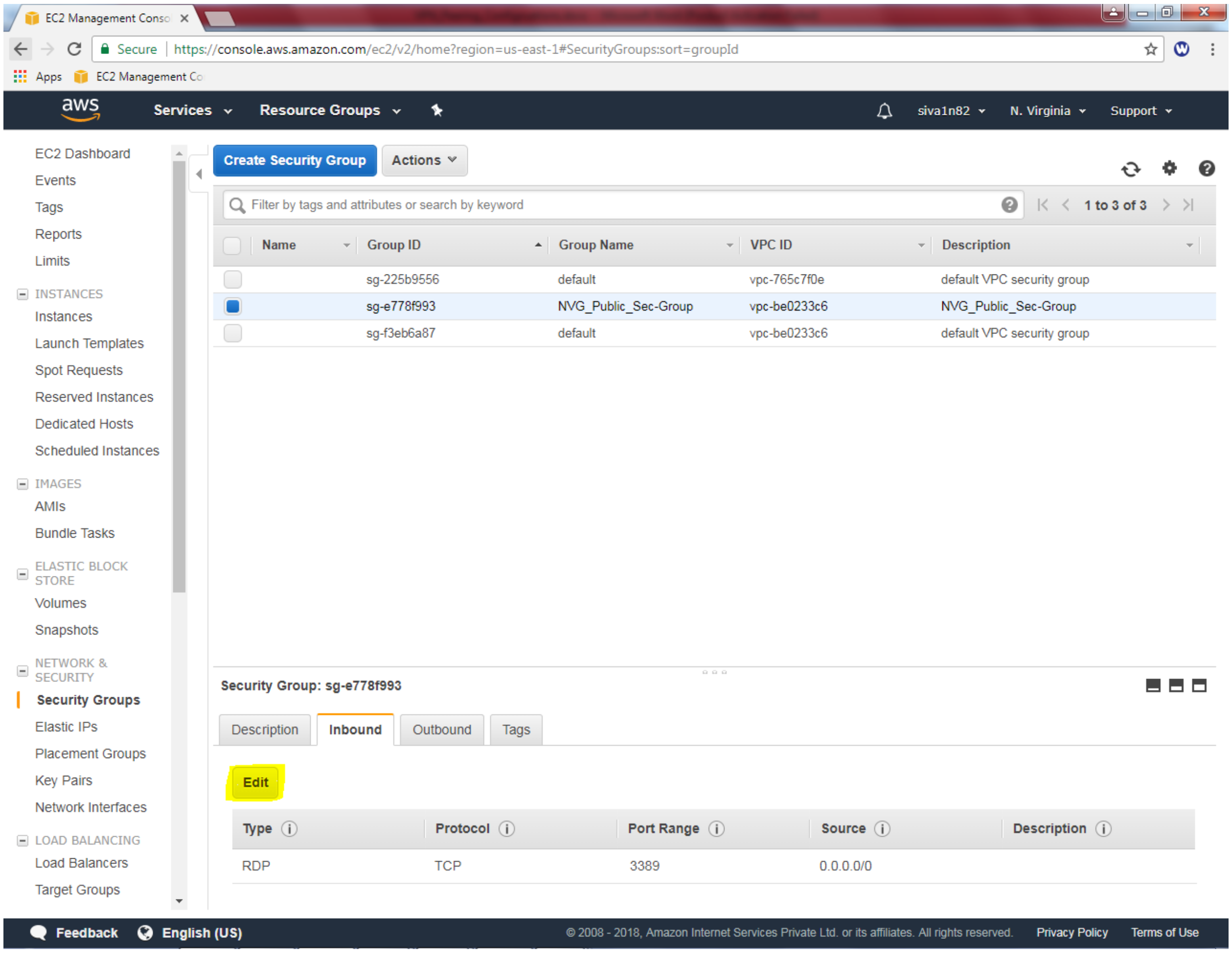
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.0.2.223

Pinging 10.0.2.223 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.2.223:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>_
```

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.


34.230.74.160 - Remote Desktop Connection
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”

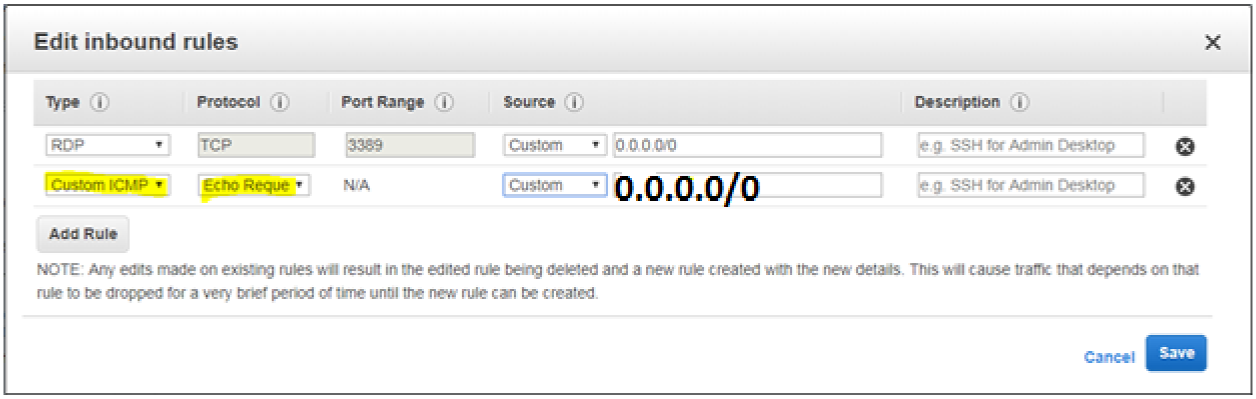


	Name	Group ID	Group Name	VPC ID	Description
□		sg-225b9556	default	vpc-765c7f0e	default VPC security group
☑		sg-e778f993	NVG_Public_Sec-Group	vpc-be0233c6	NVG_Public_Sec-Group
□		sg-f3eb6a87	default	vpc-be0233c6	default VPC security group

Security Group: sg-e778f993

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

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

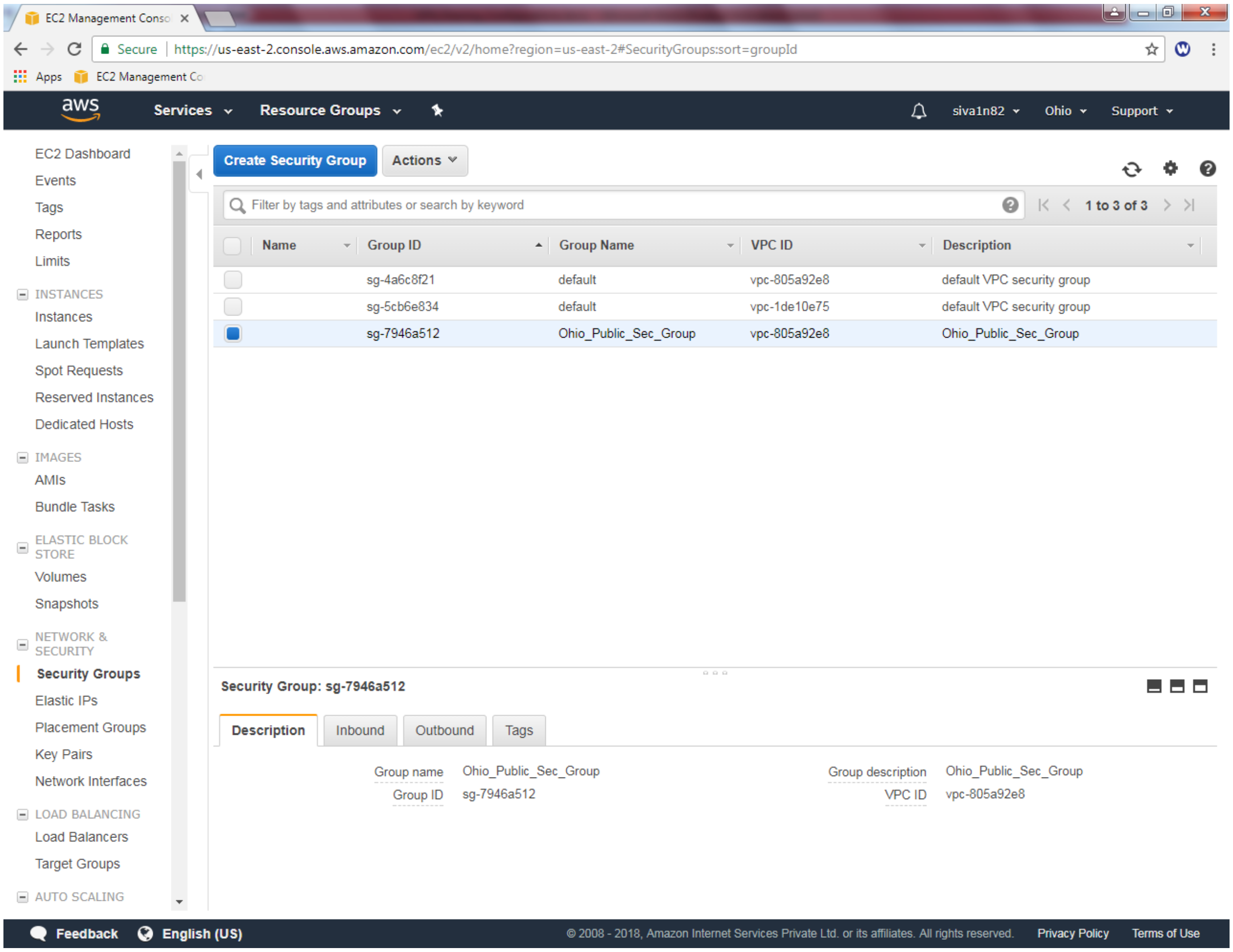


Edit inbound rules

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	0.0.0.0/0	e.g. SSH for Admin Desktop

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.

In Ohio region, ohio public security group,



	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
■		sg-7946a512	Ohio_Public_Sec_Group	vpc-805a92e8	Ohio_Public_Sec_Group

Security Group: sg-7946a512

Group name Ohio_Public_Sec_Group

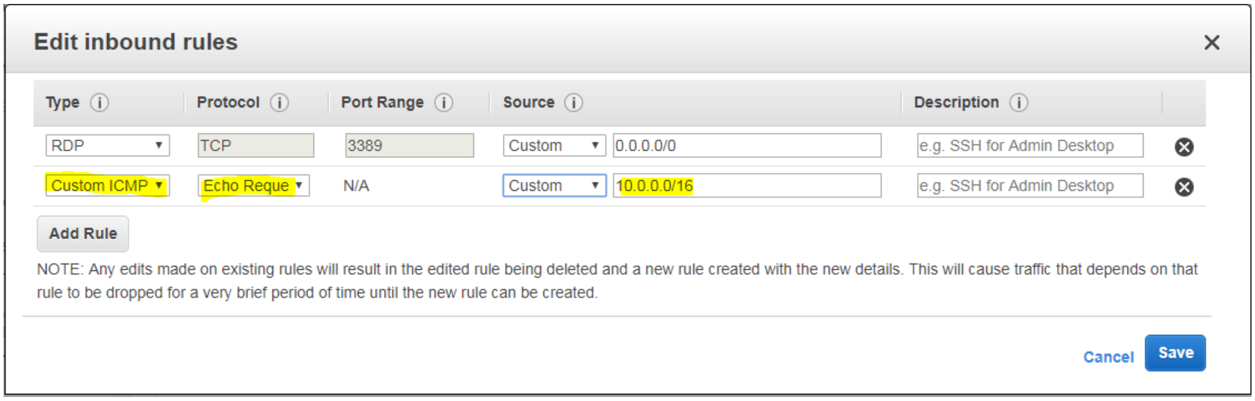
Group ID sg-7946a512

Group description Ohio_Public_Sec_Group

VPC ID vpc-805a92e8

Click “Inbound” rule, then click “Edit”.

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



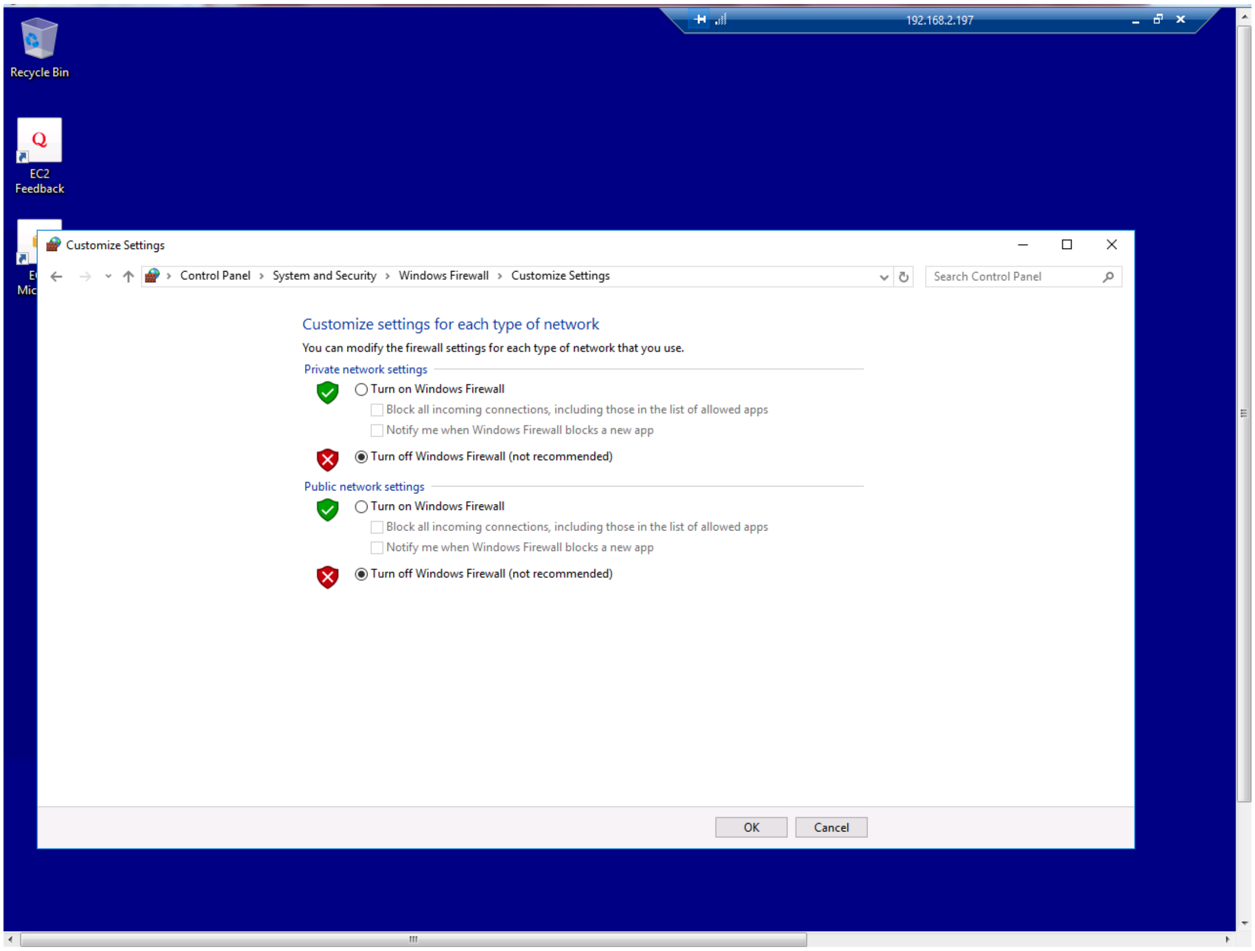
Edit inbound rules

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	10.0.0.0/16	e.g. SSH for Admin Desktop

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.

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".



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Public network settings

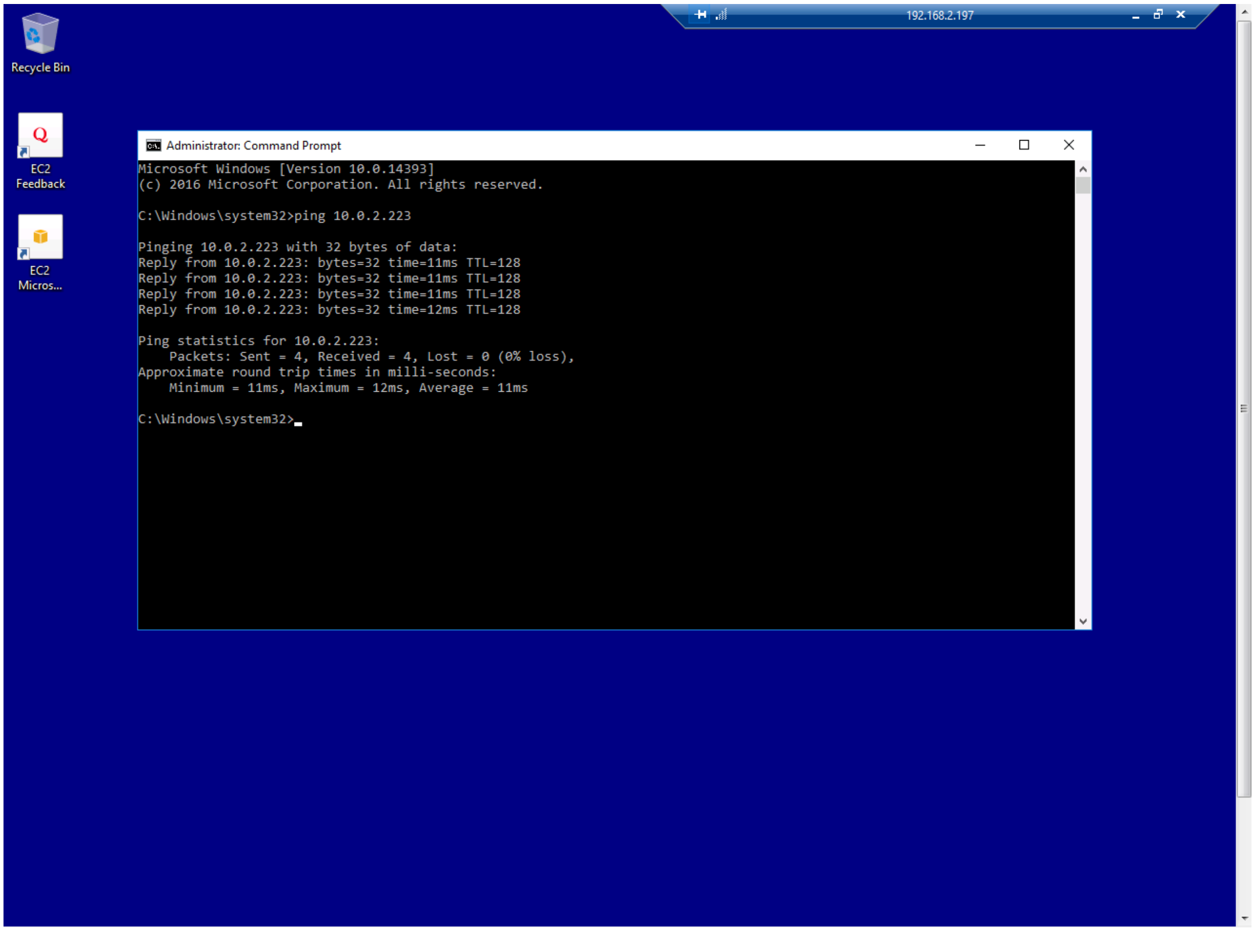
○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Firewall blocks a new app

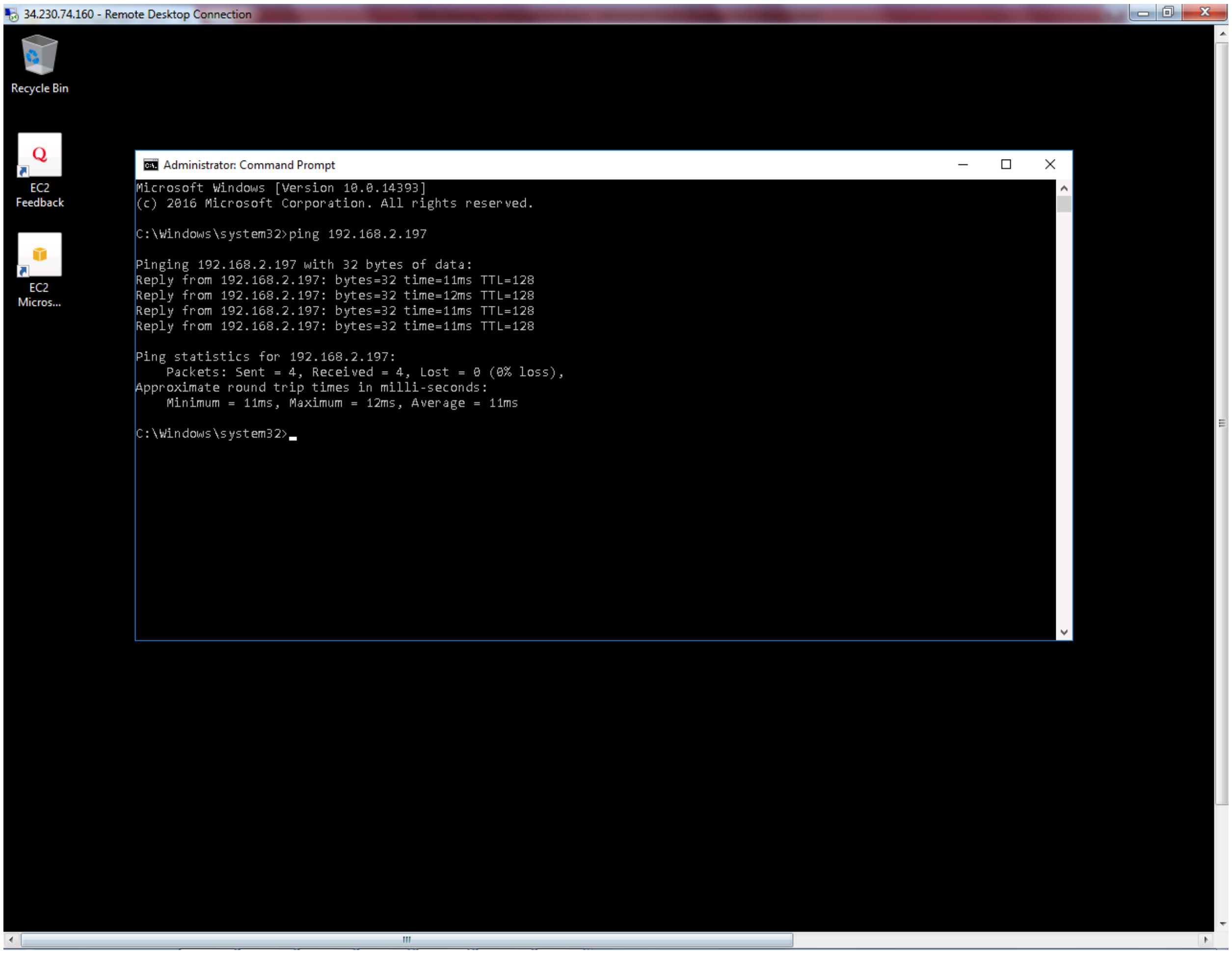
● Turn off Windows Firewall (not recommended)

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



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

C:\Windows\system32>ping 10.0.2.223

Pinging 10.0.2.223 with 32 bytes of data:
Reply from 10.0.2.223: bytes=32 time=11ms TTL=128
Reply from 10.0.2.223: bytes=32 time=11ms TTL=128
Reply from 10.0.2.223: bytes=32 time=11ms TTL=128
Reply from 10.0.2.223: bytes=32 time=12ms TTL=128

Ping statistics for 10.0.2.223:
    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>_
```

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


34.230.74.160 - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Micros...
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>_
```