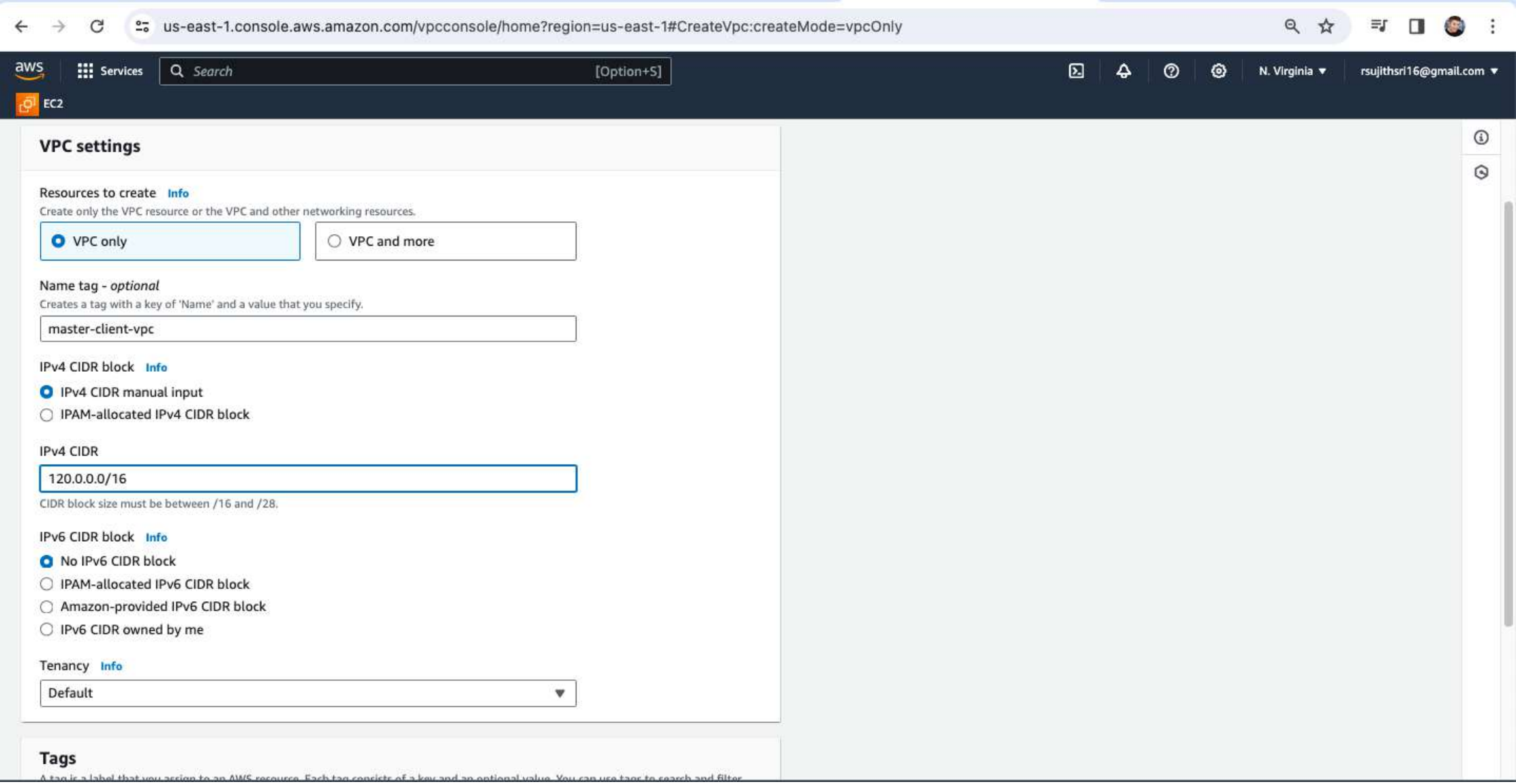
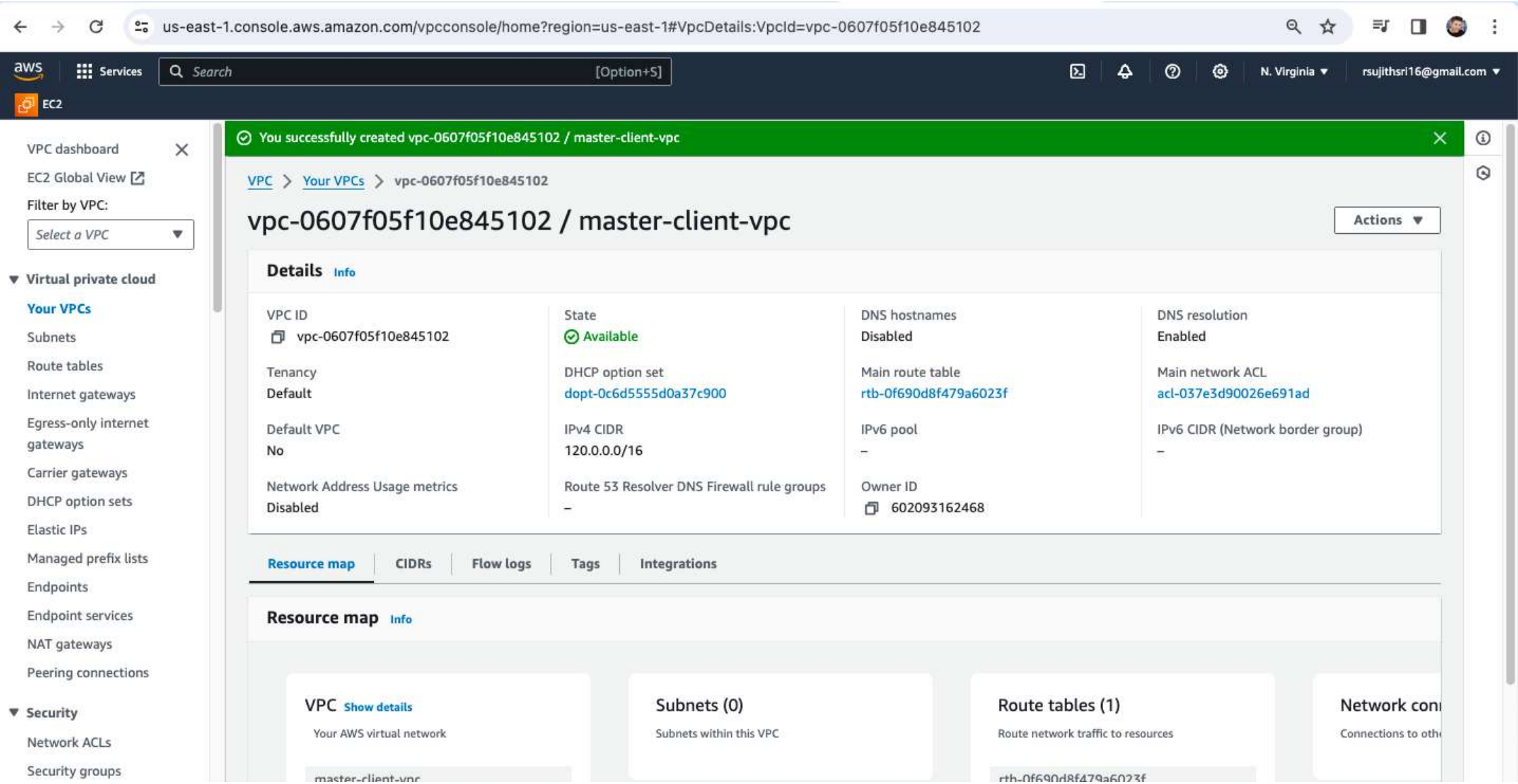
Problem Statement:

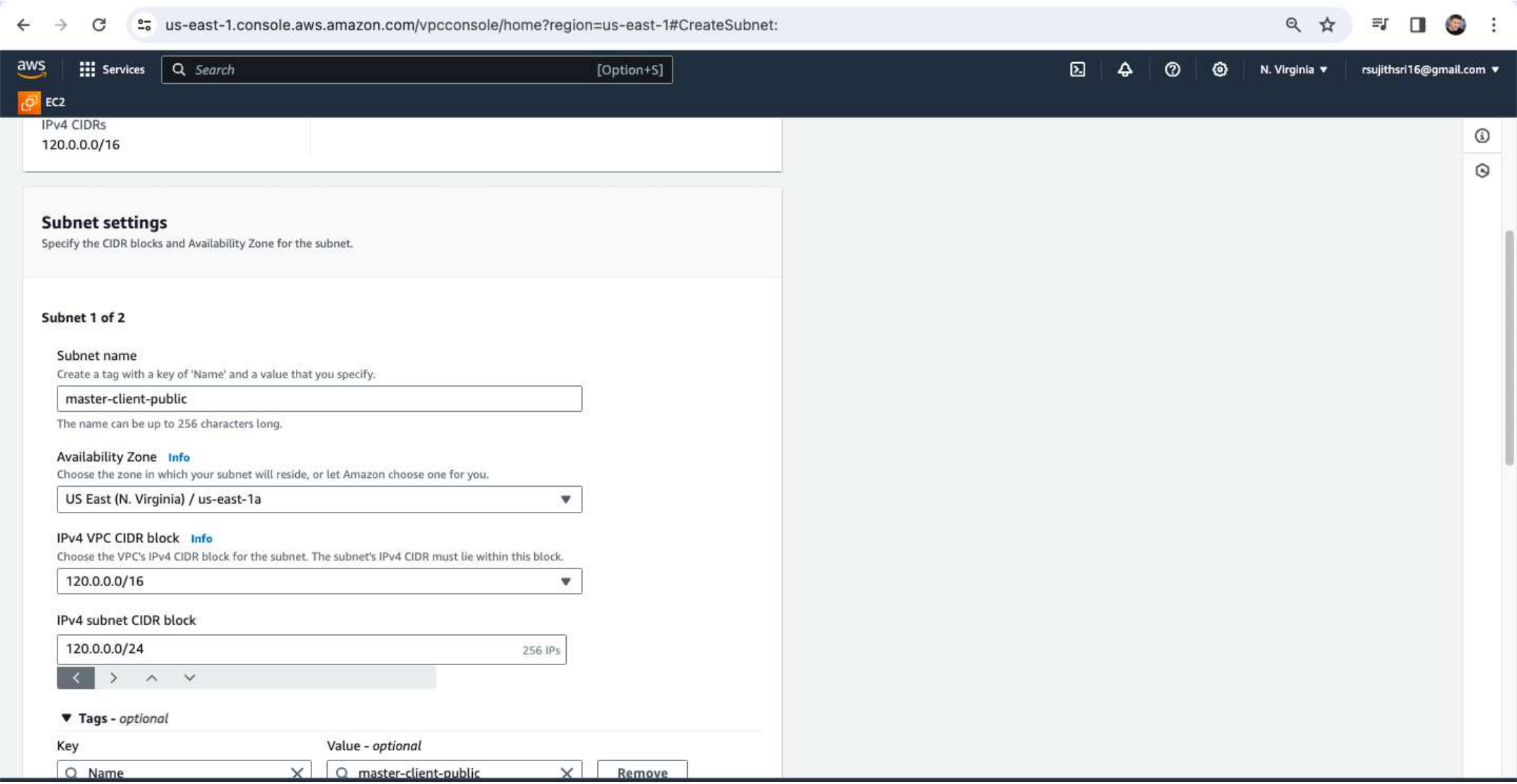
Working for an organization, you are required to provide them a safe and secure environment for the deployment of their resources. They might require different types of connectivity. Implement the following to fulfill the requirements of the company.

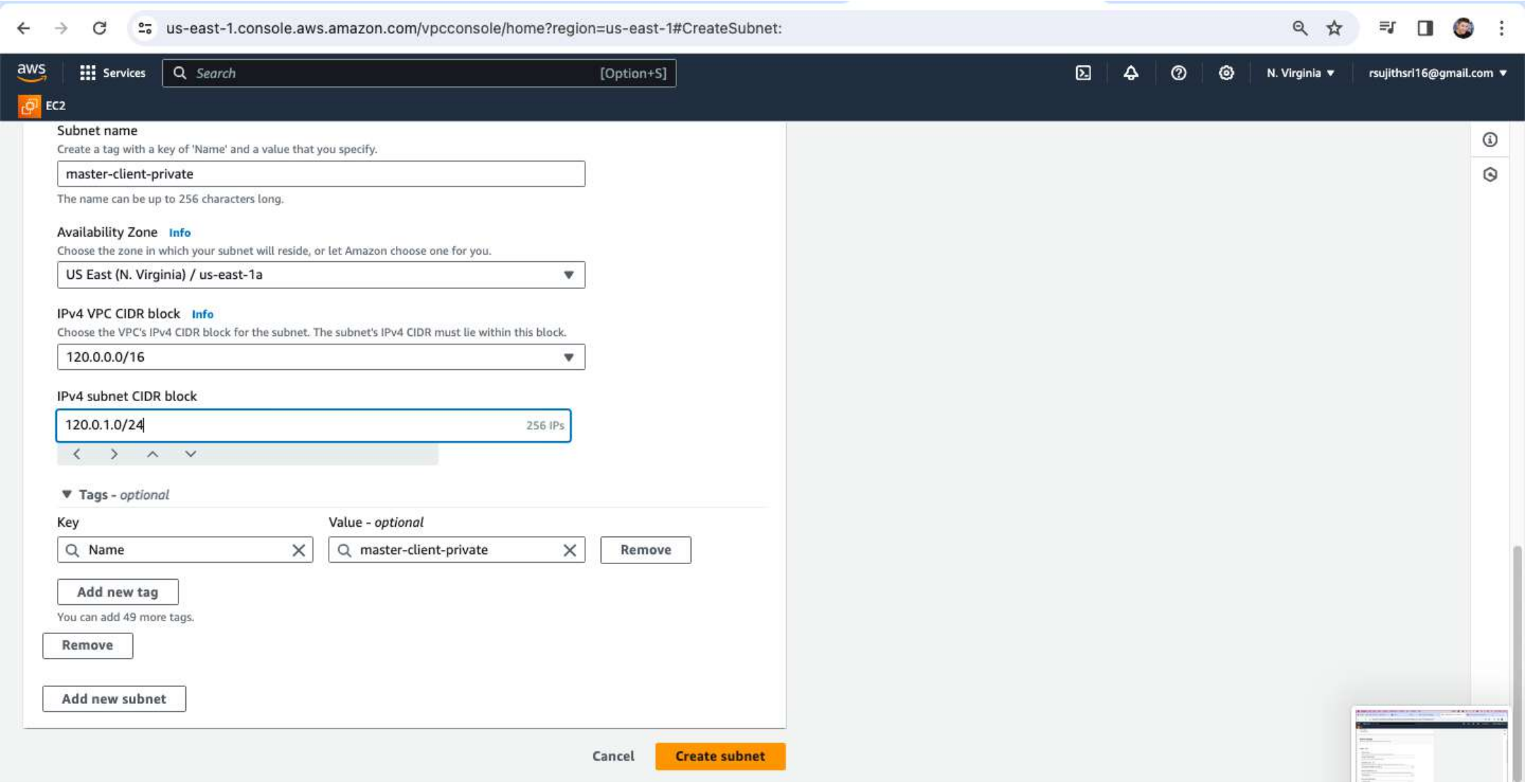
Tasks To Be Performed:

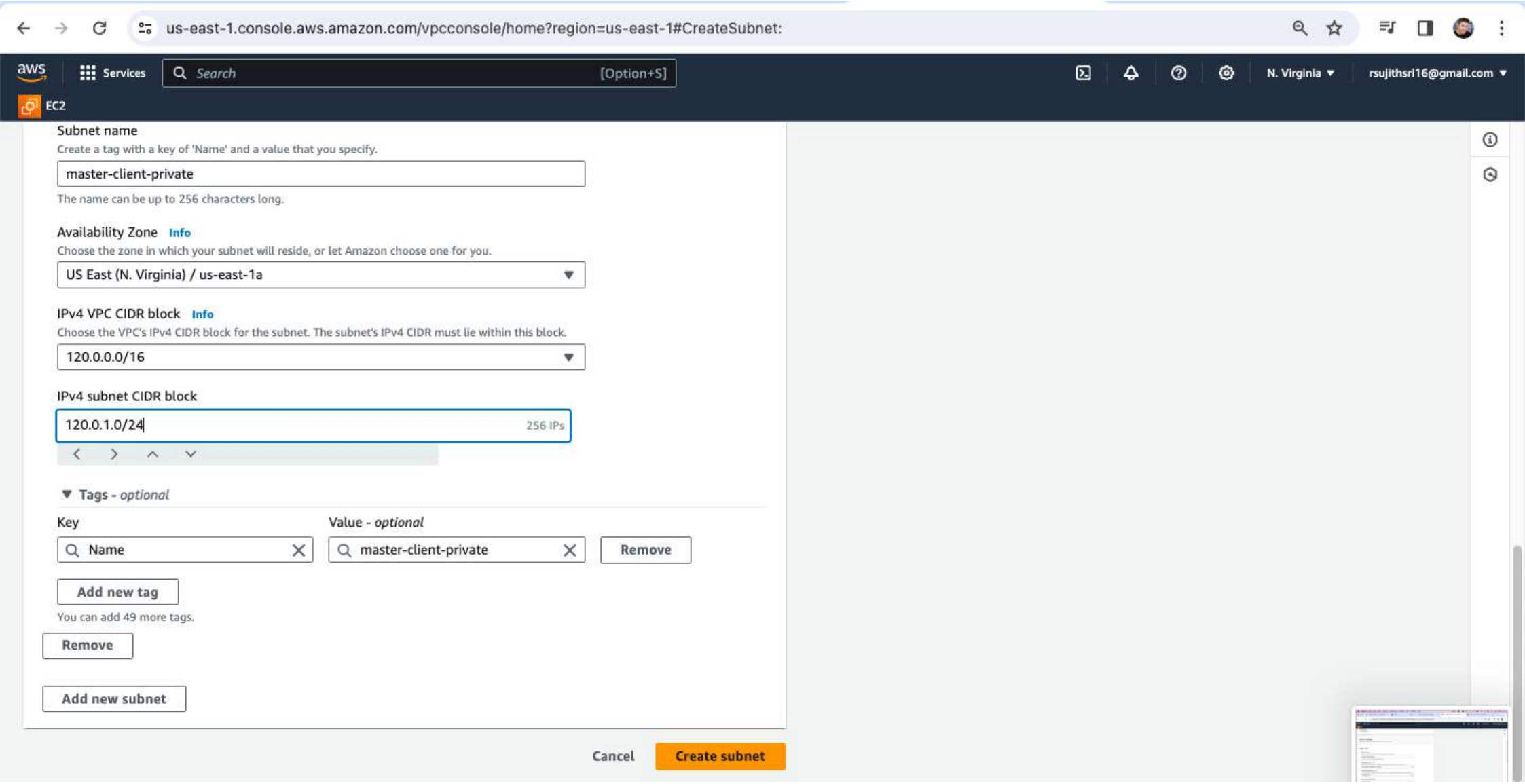
1. Create 2 EC2 instances in any public subnet of any VPC and name them Master and Client.
2. Using security groups, make sure that the Client instance can only be accessed (SSH) through the Master instance.

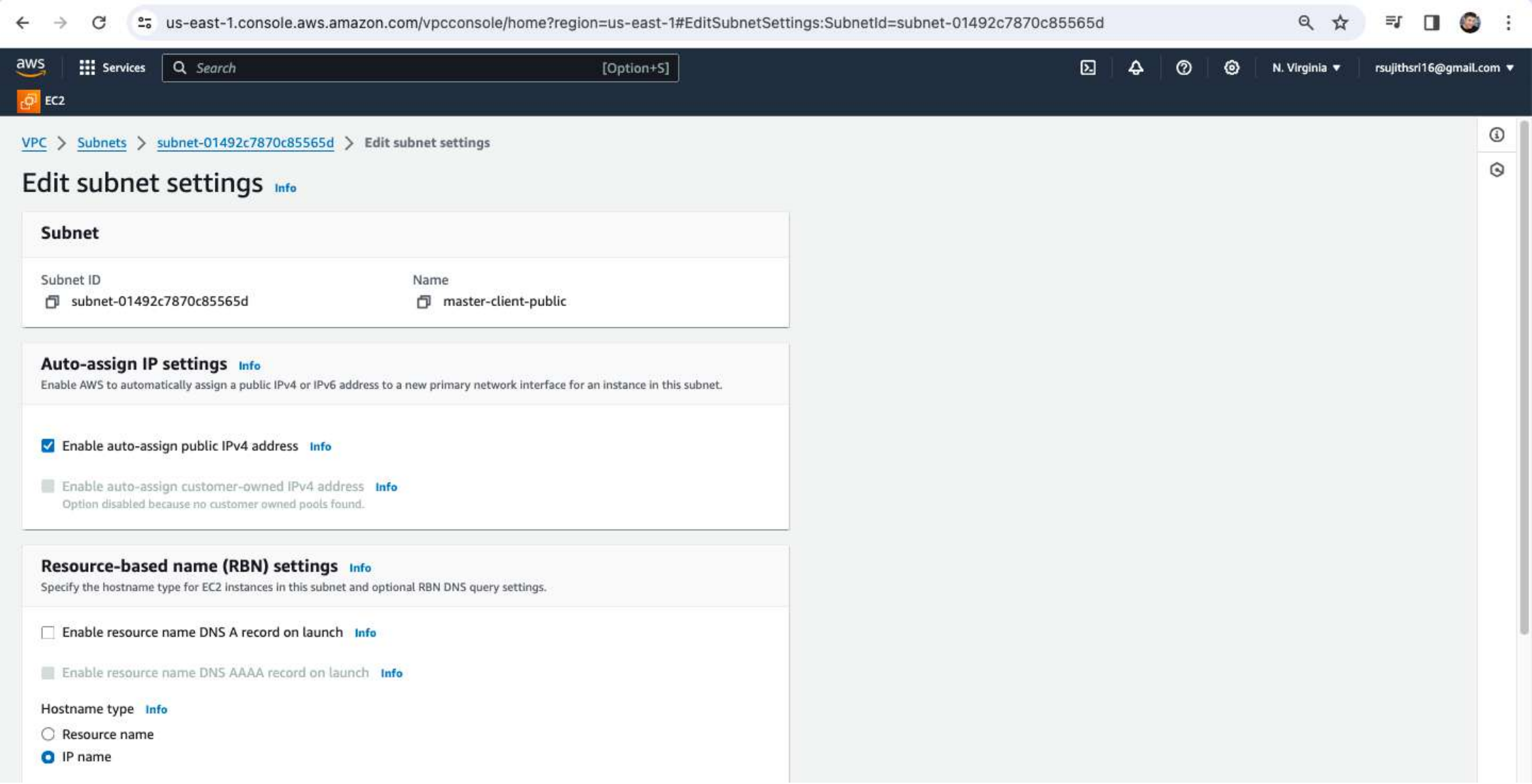

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateVpc:createMode=vpcOnly
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
VPC settings
Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only
VPC and more
Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
master-client-vpc
IPv4 CIDR block Info
IPv4 CIDR manual input
IPAM-allocated IPv4 CIDR block
IPv4 CIDR
120.0.0.0/16
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me
Tenancy Info
Default
Tags

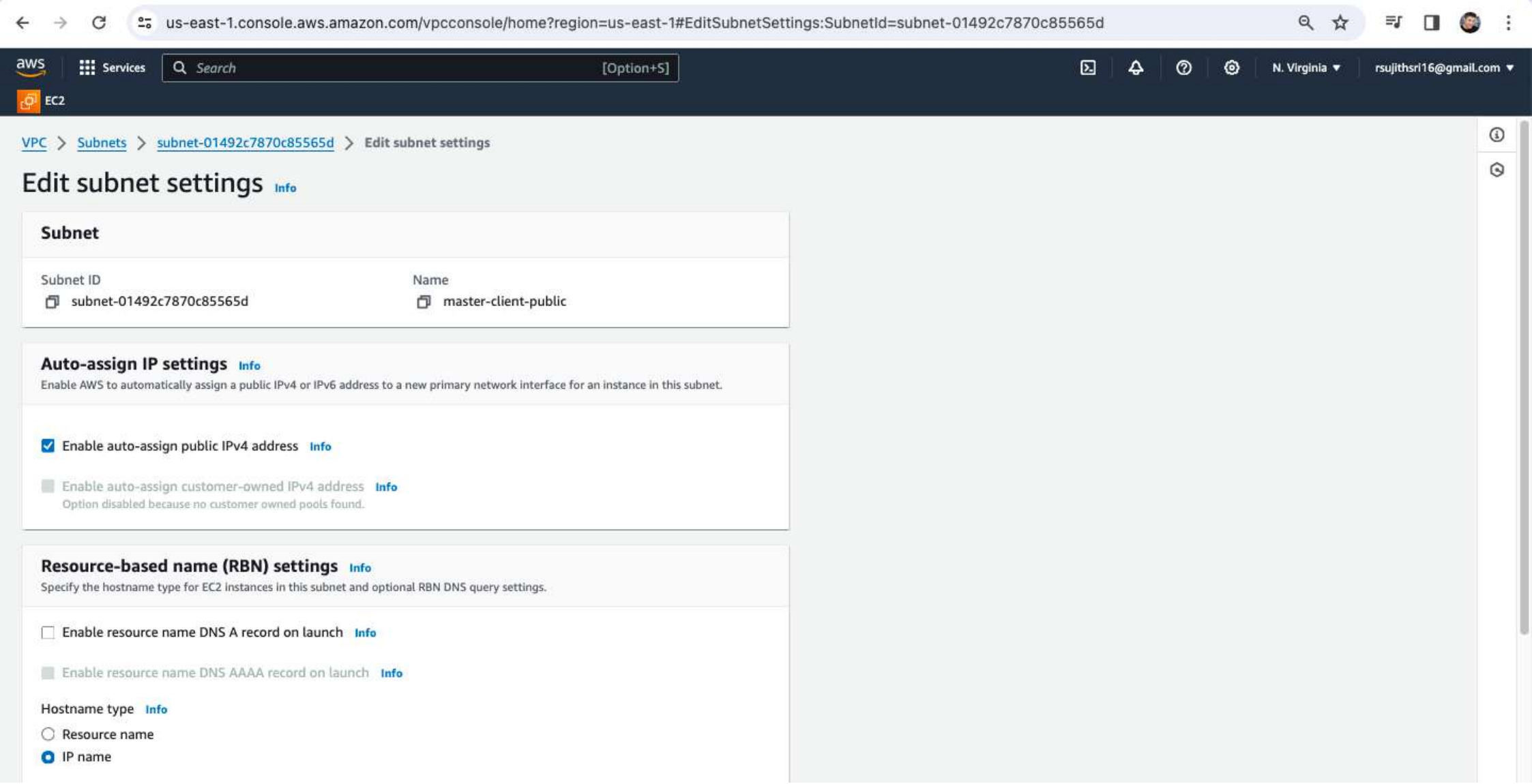

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#VpcDetails:VpcId=vpc-0607f05f10e845102
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
You successfully created vpc-0607f05f10e845102 / master-client-vpc
VPC > Your VPCs > vpc-0607f05f10e845102
vpc-0607f05f10e845102 / master-client-vpc
Actions
Details Info
VPC ID
vpc-0607f05f10e845102
State
Available
DNS hostnames
Disabled
DNS resolution
Enabled
Tenancy
Default
DHCP option set
dopt-0c6d5555d0a37c900
Main route table
rtb-0f690d8f479a6023f
Main network ACL
acl-037e3d90026e691ad
Default VPC
No
IPv4 CIDR
120.0.0.0/16
IPv6 pool
–
IPv6 CIDR (Network border group)
–
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
–
Owner ID
602093162468
Resource map
CIDRs
Flow logs
Tags
Integrations
Resource map Info
VPC Show details
Your AWS virtual network
Subnets (0)
Subnets within this VPC
Route tables (1)
Route network traffic to resources
Network con
Connections to oth

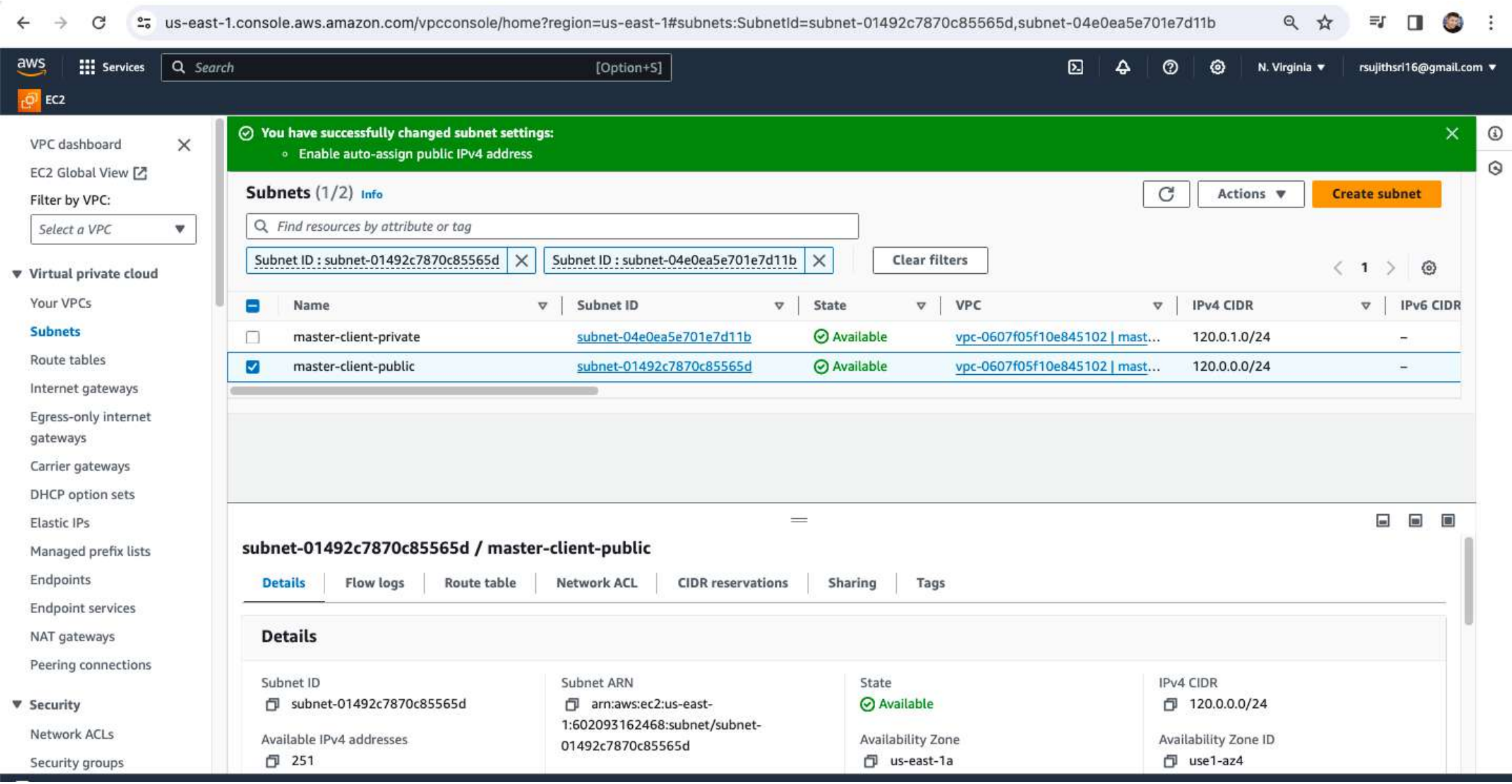

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
IPv4 CIDRs
120.0.0.0/16
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 2
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
master-client-public
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
120.0.0.0/16
IPv4 subnet CIDR block
120.0.0.0/24
256 IPs
Tags - optional
Key
Value - optional
Name
master-client-public
Remove

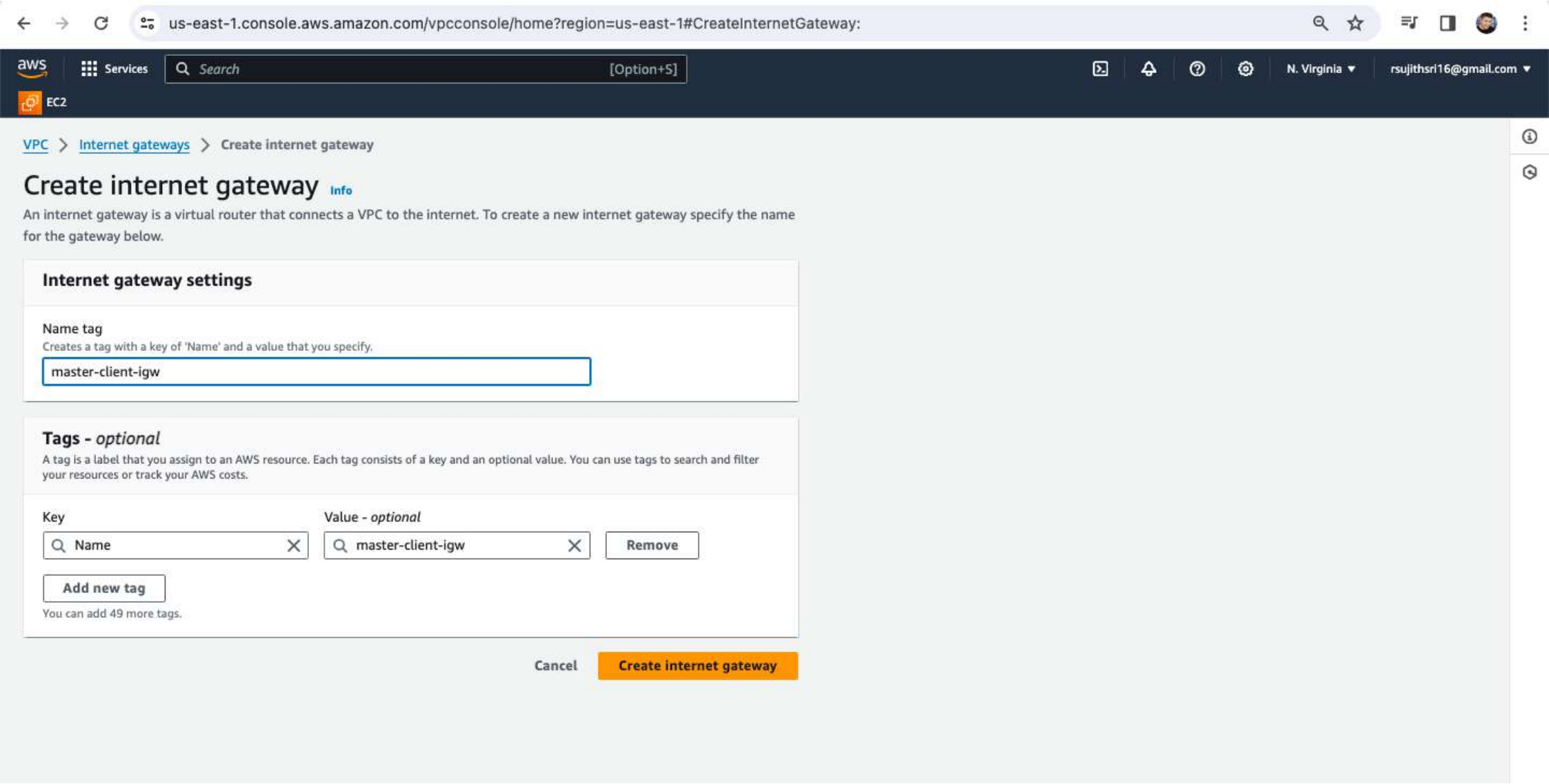

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
master-client-private
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
120.0.0.0/16
IPv4 subnet CIDR block
120.0.1.0/24
256 IPs
Tags - optional
Key
Value - optional
Name
master-client-private
Remove
Add new tag
You can add 49 more tags.
Remove
Add new subnet
Cancel
Create subnet

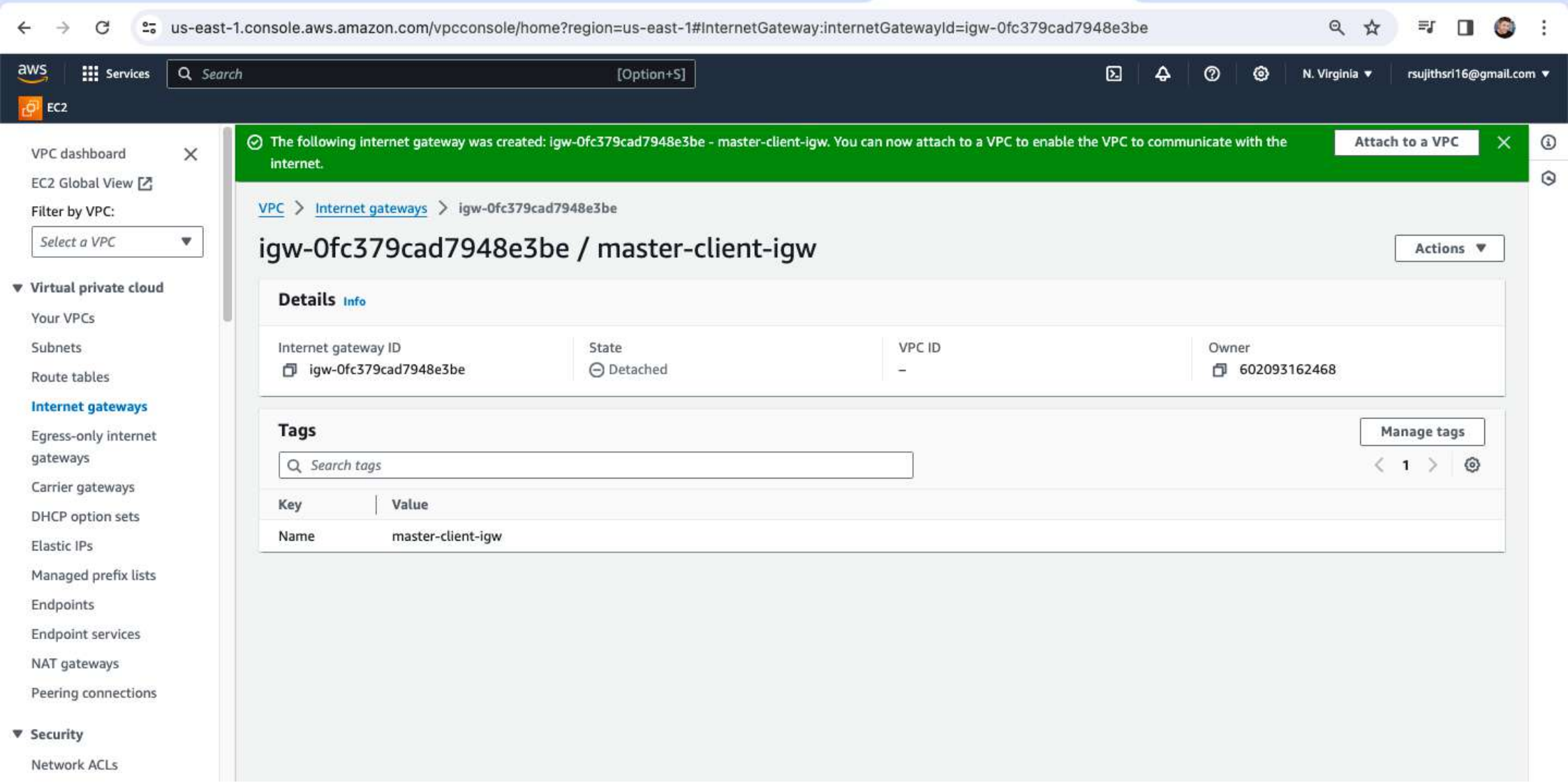

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
master-client-private
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
120.0.0.0/16
IPv4 subnet CIDR block
120.0.1.0/24
256 IPs
Tags - optional
Key
Value - optional
Name
master-client-private
Remove
Add new tag
You can add 49 more tags.
Remove
Add new subnet
Cancel
Create subnet

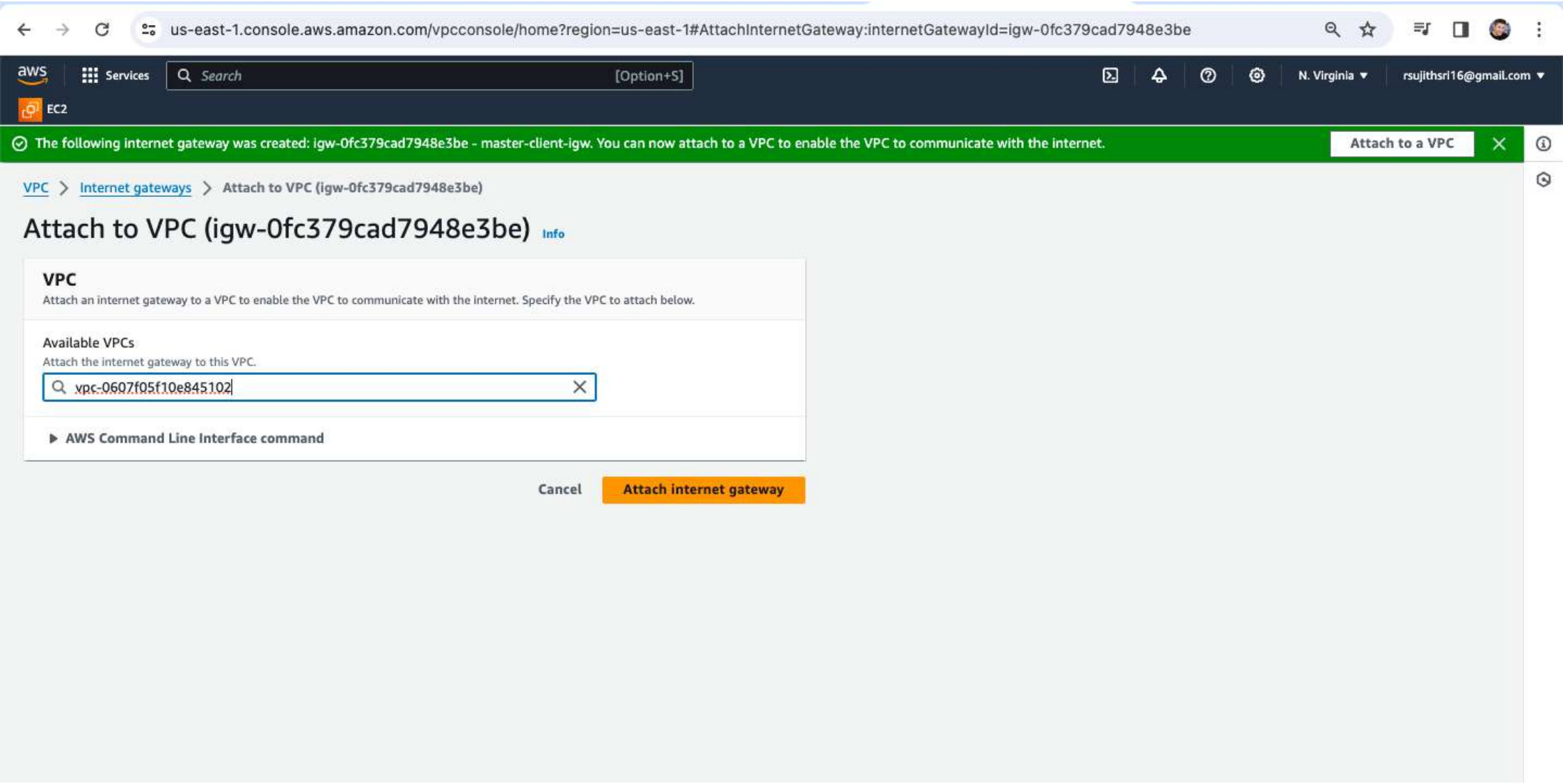

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditSubnetSettings:SubnetId=subnet-01492c7870c85565d
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
VPC > Subnets > subnet-01492c7870c85565d > Edit subnet settings
Edit subnet settings Info
Subnet
Subnet ID
subnet-01492c7870c85565d
Name
master-client-public
Auto-assign IP settings Info
Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.
Enable auto-assign public IPv4 address Info
Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.
Resource-based name (RBN) settings Info
Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.
Enable resource name DNS A record on launch Info
Enable resource name DNS AAAA record on launch Info
Hostname type Info
Resource name
IP name

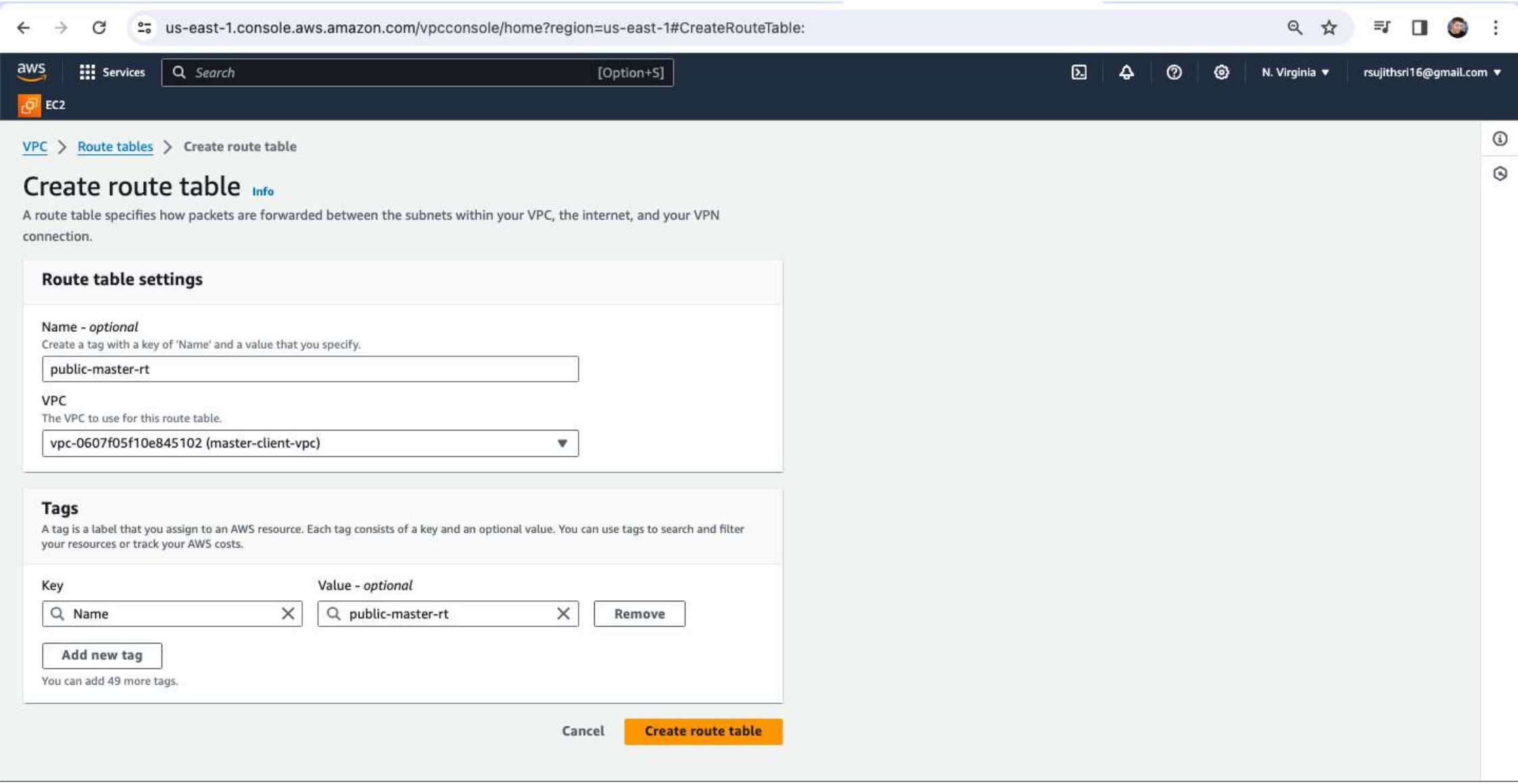

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditSubnetSettings:SubnetId=subnet-01492c7870c85565d
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
VPC > Subnets > subnet-01492c7870c85565d > Edit subnet settings
Edit subnet settings Info
Subnet
Subnet ID
subnet-01492c7870c85565d
Name
master-client-public
Auto-assign IP settings Info
Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.
Enable auto-assign public IPv4 address Info
Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.
Resource-based name (RBN) settings Info
Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.
Enable resource name DNS A record on launch Info
Enable resource name DNS AAAA record on launch Info
Hostname type Info
Resource name
IP name

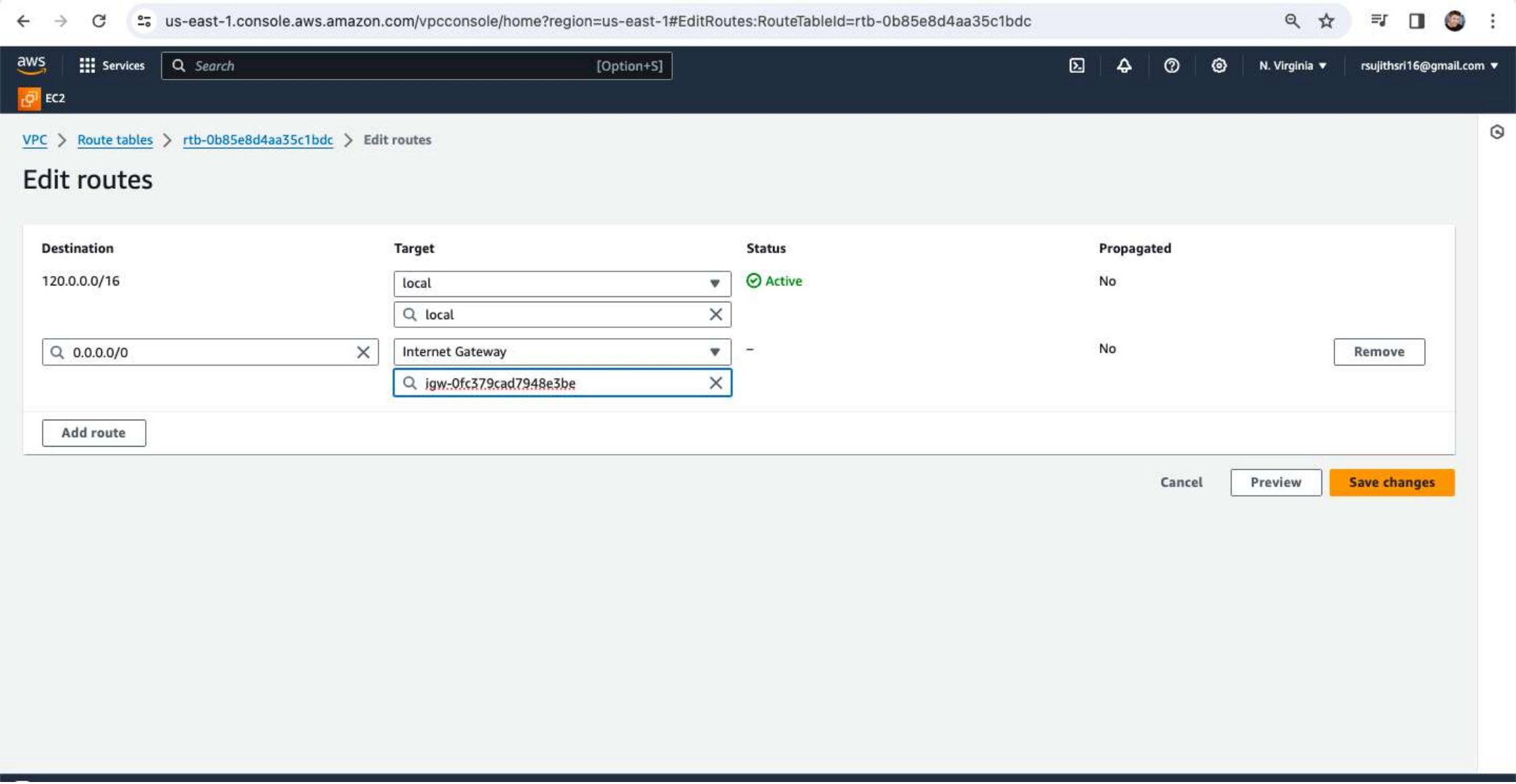

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#subnets:SubnetId=subnet-01492c7870c85565d,subnet-04e0ea5e701e7d11b
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
You have successfully changed subnet settings:
Enable auto-assign public IPv4 address
Subnets (1/2) Info
Actions
Create subnet
Find resources by attribute or tag
Subnet ID : subnet-01492c7870c85565d
Subnet ID : subnet-04e0ea5e701e7d11b
Clear filters
Name
Subnet ID
State
VPC
IPv4 CIDR
IPv6 CIDR
master-client-private
subnet-04e0ea5e701e7d11b
Available
vpc-0607f05f10e845102 | mast...
120.0.1.0/24
master-client-public
subnet-01492c7870c85565d
Available
vpc-0607f05f10e845102 | mast...
120.0.0.0/24
subnet-01492c7870c85565d / master-client-public
Details
Flow logs
Route table
Network ACL
CIDR reservations
Sharing
Tags
Details
Subnet ID
subnet-01492c7870c85565d
Subnet ARN
arn:aws:ec2:us-east-1:602093162468:subnet/subnet-01492c7870c85565d
State
Available
IPv4 CIDR
120.0.0.0/24
Available IPv4 addresses
251
Availability Zone
us-east-1a
Availability Zone ID
use1-az4

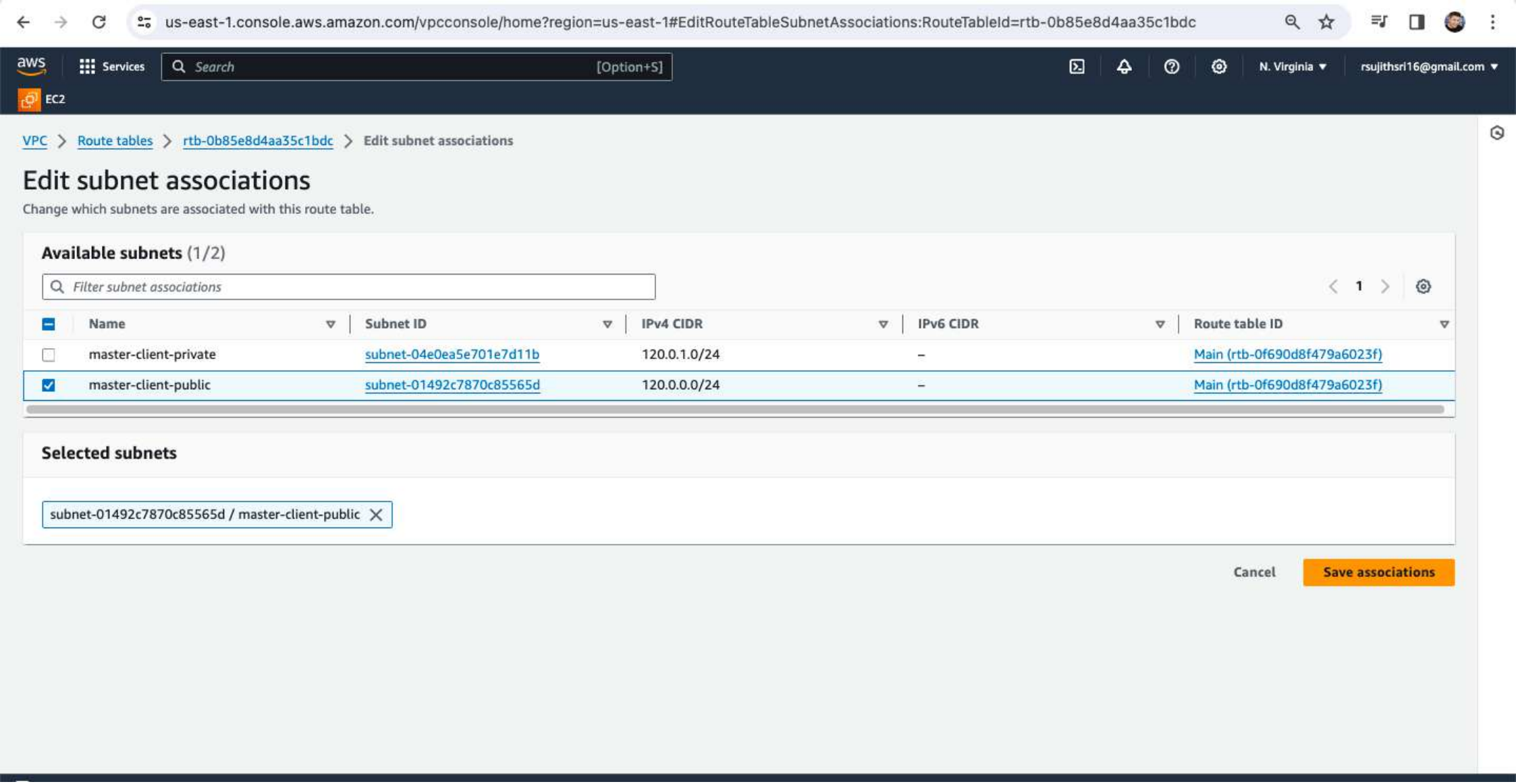

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateInternetGateway:
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
VPC
Internet gateways
Create internet gateway
Create internet gateway
Info
An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.
Internet gateway settings
Name tag
Creates a tag with a key of 'Name' and a value that you specify.
master-client-igw
Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
master-client-igw
Remove
Add new tag
You can add 49 more tags.
Cancel
Create internet gateway

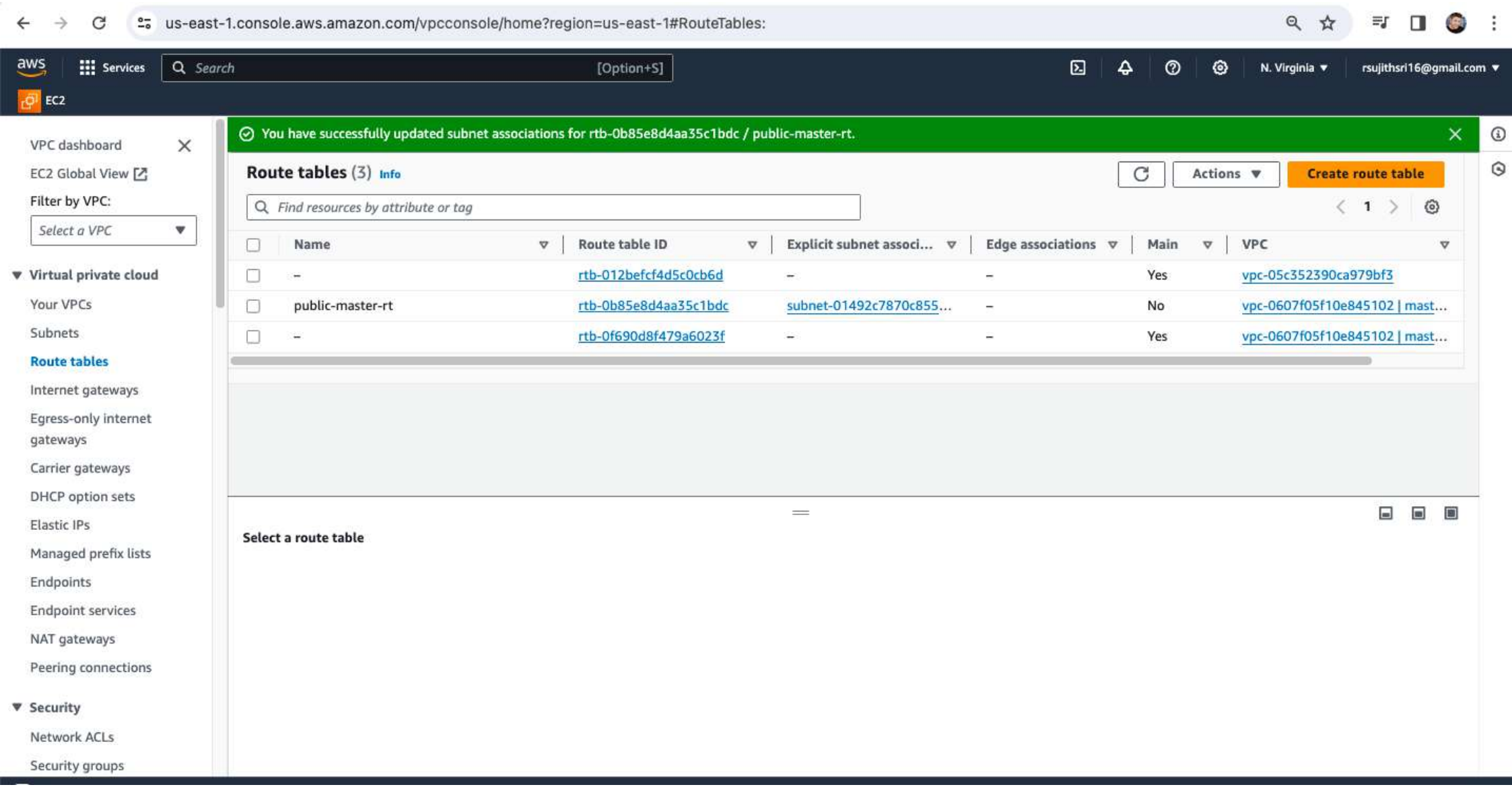

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#InternetGateway:internetGatewayId=igw-0fc379cad7948e3be
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
The following internet gateway was created: igw-0fc379cad7948e3be - master-client-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
VPC > Internet gateways > igw-0fc379cad7948e3be
igw-0fc379cad7948e3be / master-client-igw
Actions
Details Info
Internet gateway ID
igw-0fc379cad7948e3be
State
Detached
VPC ID
–
Owner
602093162468
Tags
Manage tags
Search tags
1
Key
Value
Name
master-client-igw

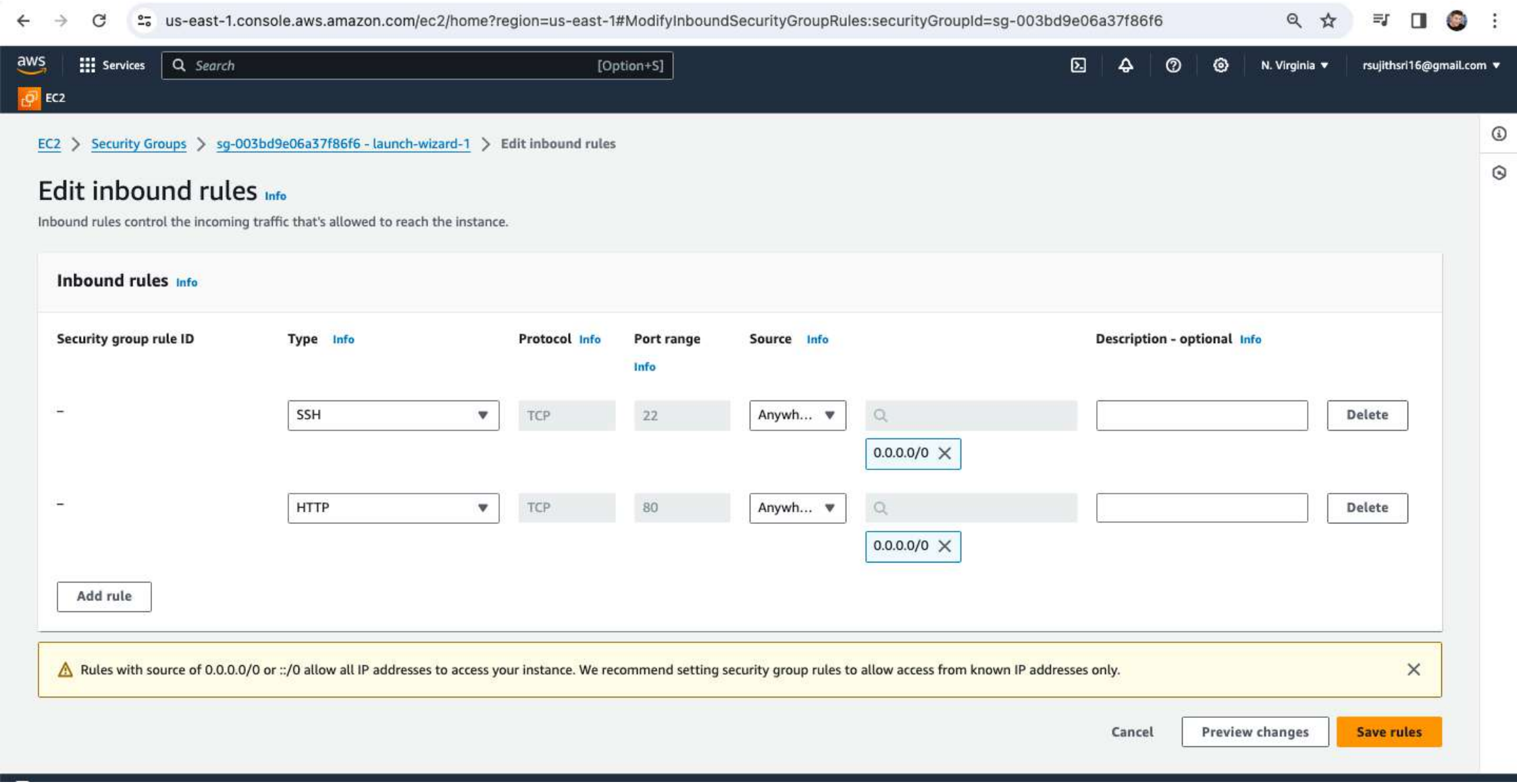

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#AttachInternetGateway:internetGatewayId=igw-0fc379cad7948e3be
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
The following internet gateway was created: igw-0fc379cad7948e3be - master-client-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
VPC
Internet gateways
Attach to VPC (igw-0fc379cad7948e3be)
Attach to VPC (igw-0fc379cad7948e3be) Info
VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.
Available VPCs
Attach the internet gateway to this VPC.
vpc-0607f05f10e845102
AWS Command Line Interface command
Cancel
Attach internet gateway

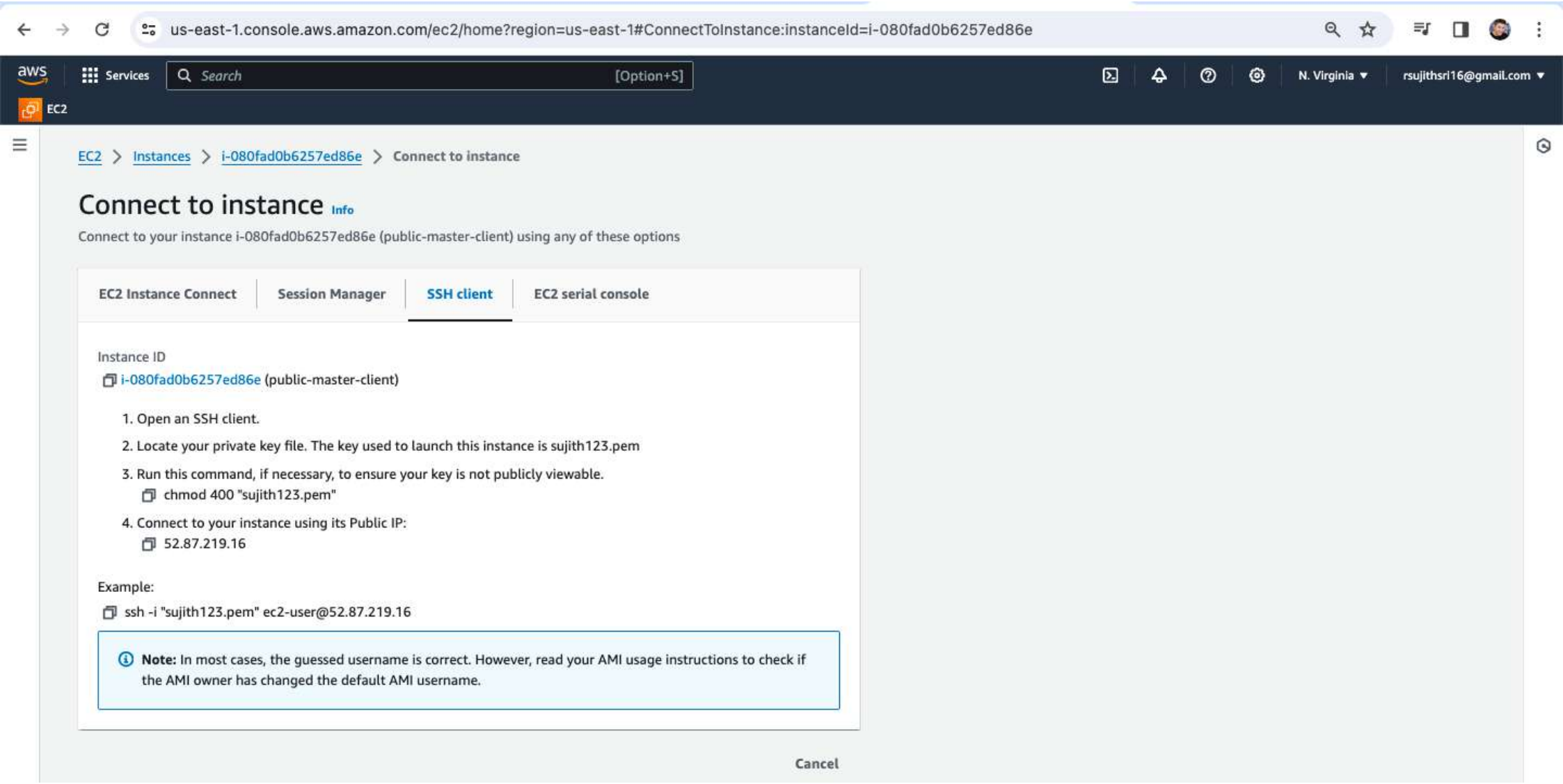

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateRouteTable:
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
VPC > Route tables > Create route table
Create route table Info
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
public-master-rt
VPC
The VPC to use for this route table.
vpc-0607f05f10e845102 (master-client-vpc)
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
public-master-rt
Remove
Add new tag
You can add 49 more tags.
Cancel
Create route table

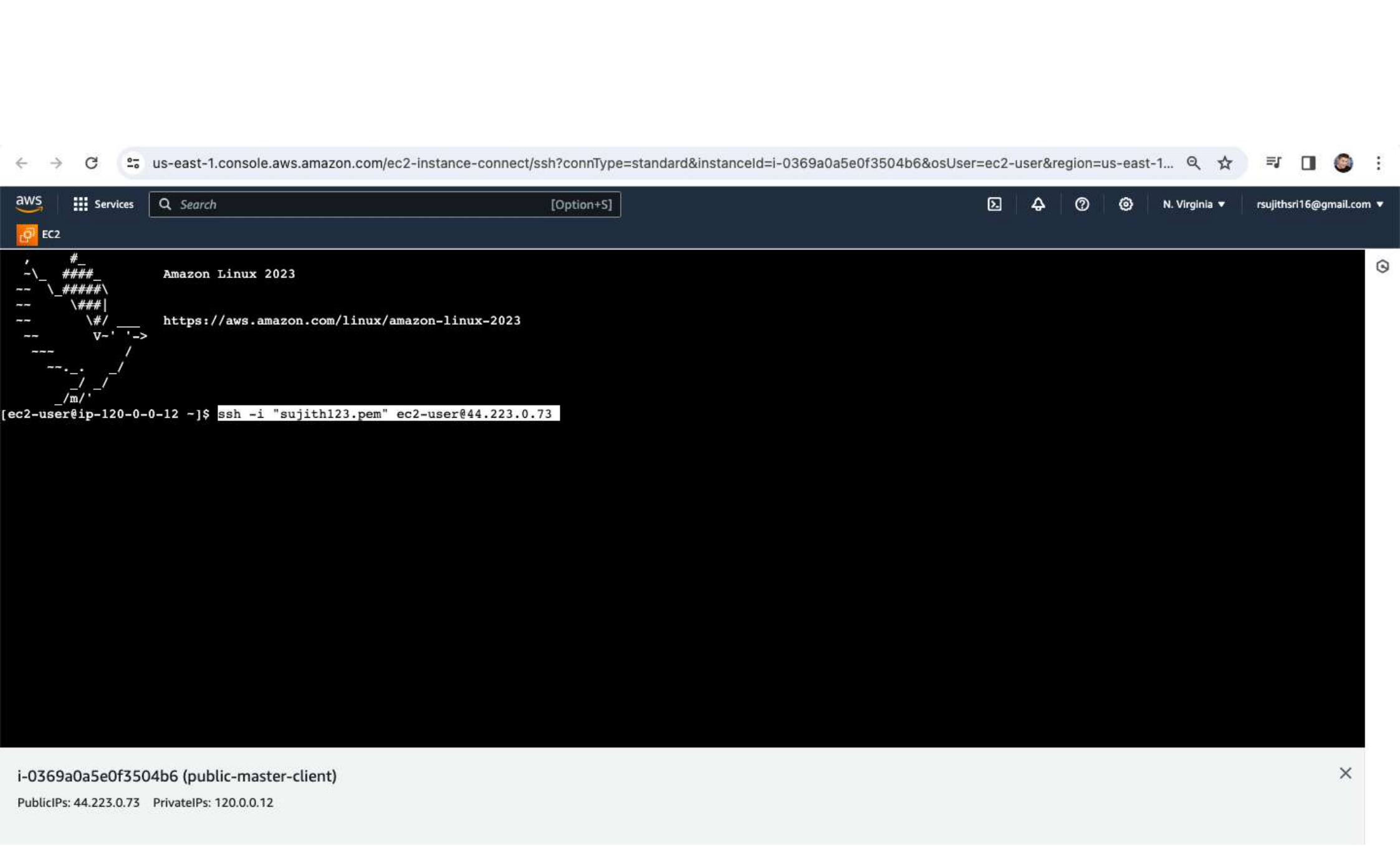

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditRoutes:RouteTableId=rtb-0b85e8d4aa35c1bdc
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
VPC
Route tables
rtb-0b85e8d4aa35c1bdc
Edit routes
Edit routes
Destination
Target
Status
Propagated
120.0.0.0/16
local
Active
No
local
0.0.0.0/0
Internet Gateway
–
No
Remove
igw-0fc379cad7948e3be
Add route
Cancel
Preview
Save changes

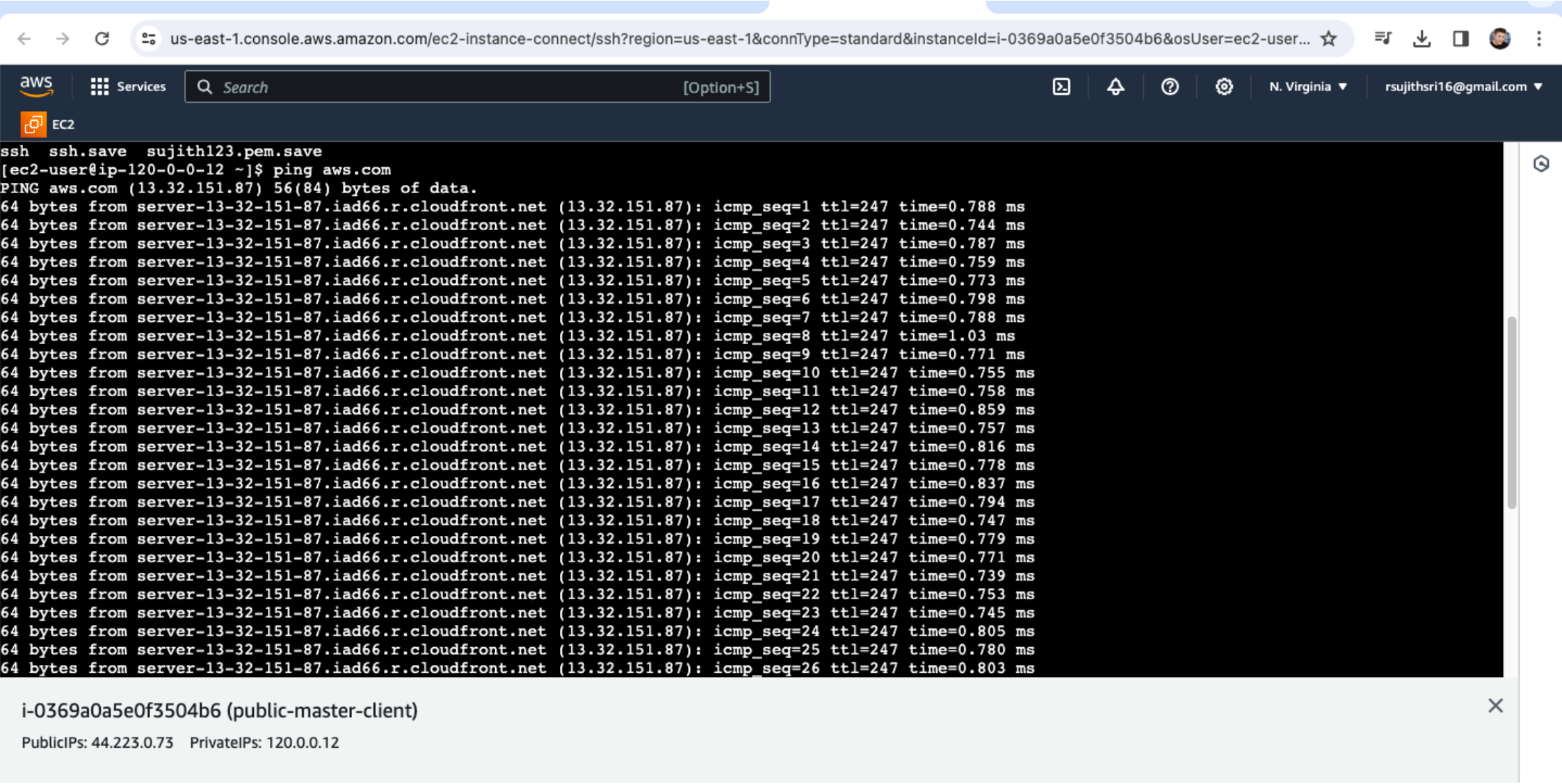

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-0b85e8d4aa35c1bdc
aws
Services
Search
[Option+S]
N. Virginia
rsujithsrl16@gmail.com
EC2
VPC > Route tables > rtb-0b85e8d4aa35c1bdc > Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (1/2)
Filter subnet associations
1
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
master-client-private
subnet-04e0ea5e701e7d11b
120.0.1.0/24
–
Main (rtb-0f690d8f479a6023f)
master-client-public
subnet-01492c7870c85565d
120.0.0.0/24
–
Main (rtb-0f690d8f479a6023f)
Selected subnets
subnet-01492c7870c85565d / master-client-public
Cancel
Save associations


us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTables:
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
VPC dashboard
EC2 Global View
Filter by VPC:
Select a 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
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
You have successfully updated subnet associations for rtb-0b85e8d4aa35c1bdc / public-master-rt.
Route tables (3) Info
Actions
Create route table
Find resources by attribute or tag
1
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
– rtb-012befcf4d5c0cb6d – – Yes vpc-05c352390ca979bf3
public-master-rt rtb-0b85e8d4aa35c1bdc subnet-01492c7870c855... – No vpc-0607f05f10e845102 | mast...
– rtb-0f690d8f479a6023f – – Yes vpc-0607f05f10e845102 | mast...
Select a route table


us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-003bd9e06a37f86f6
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
EC2 > Security Groups > sg-003bd9e06a37f86f6 - launch-wizard-1 > Edit inbound rules
Edit inbound rules Info
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules Info
Security group rule ID
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
-
SSH
TCP
22
Anywh...
0.0.0.0/0
Delete
-
HTTP
TCP
80
Anywh...
0.0.0.0/0
Delete
Add rule
Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Cancel
Preview changes
Save rules


us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ConnectToInstance:instanceId=i-080fad0b6257ed86e
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
EC2 > Instances > i-080fad0b6257ed86e > Connect to instance
Connect to instance Info
Connect to your instance i-080fad0b6257ed86e (public-master-client) using any of these options
EC2 Instance Connect
Session Manager
SSH client
EC2 serial console
Instance ID
i-080fad0b6257ed86e (public-master-client)
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is sujith123.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 "sujith123.pem"
4. Connect to your instance using its Public IP:
52.87.219.16
Example:
ssh -i "sujith123.pem" ec2-user@52.87.219.16
Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.
Cancel


us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0369a0a5e0f3504b6&osUser=ec2-user&region=us-east-1...
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-120-0-0-12 ~]$ ssh -i "sujith123.pem" ec2-user@44.223.0.73
i-0369a0a5e0f3504b6 (public-master-client)
PublicIPs: 44.223.0.73 PrivateIPs: 120.0.0.12


us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-0369a0a5e0f3504b6&osUser=ec2-user...
aws
Services
Search
[Option+S]
N. Virginia
rsujithsri16@gmail.com
EC2
ssh ssh.save sujith123.pem.save
[ec2-user@ip-120-0-0-12 ~]$ ping aws.com
PING aws.com (13.32.151.87) 56(84) bytes of data.
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=1 ttl=247 time=0.788 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=2 ttl=247 time=0.744 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=3 ttl=247 time=0.787 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=4 ttl=247 time=0.759 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=5 ttl=247 time=0.773 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=6 ttl=247 time=0.798 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=7 ttl=247 time=0.788 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=8 ttl=247 time=1.03 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=9 ttl=247 time=0.771 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=10 ttl=247 time=0.755 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=11 ttl=247 time=0.758 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=12 ttl=247 time=0.859 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=13 ttl=247 time=0.757 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=14 ttl=247 time=0.816 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=15 ttl=247 time=0.778 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=16 ttl=247 time=0.837 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=17 ttl=247 time=0.794 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=18 ttl=247 time=0.747 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=19 ttl=247 time=0.779 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=20 ttl=247 time=0.771 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=21 ttl=247 time=0.739 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=22 ttl=247 time=0.753 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=23 ttl=247 time=0.745 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=24 ttl=247 time=0.805 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=25 ttl=247 time=0.780 ms
64 bytes from server-13-32-151-87.iad66.r.cloudfront.net (13.32.151.87): icmp_seq=26 ttl=247 time=0.803 ms
i-0369a0a5e0f3504b6 (public-master-client)
PublicIPs: 44.223.0.73 PrivateIPs: 120.0.0.12