1. TITLE OF THE -PROJECT :-Design advanced amazon costumed vpc networking (amazon virtual private cloud).

2. INTRODUCTION AND OBJECTIVES OF THE PROJECT:-

Once finish the project , we will be able To implement advanced vpc infrastructure need to use below aws components

- Step1:- implementing subnets, firewalls, statefull and stateless firewalls
- Step 2:- implementing public and private subnets
- Step 3:- firewalls in aws vpc, security groups and network access control lists
- Step 4:- implementing 2 tier architecture using security groups
- Step 5:- implementing 2 tier architecture using NACLS
- Step 6:- implementing route tables, NAT gateways
- Step 7:- definations of vpc flow logs
- Step 8:- implementing internet gateways
- Step 9:- implementing vpc using aws cli sdks

3. PROJECT CATEGORY:-Cloud computing with aws.

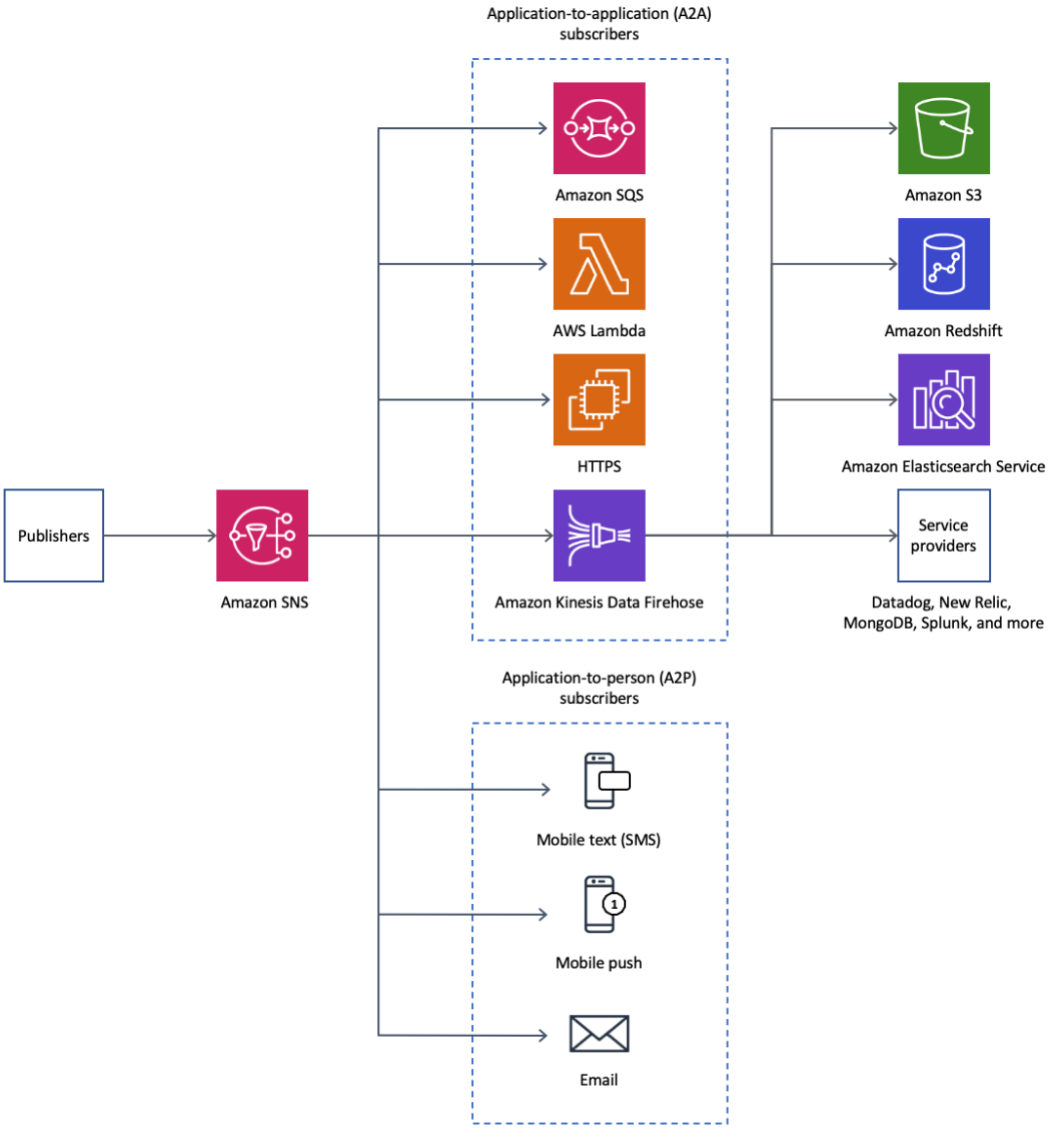
4. TOOLS/PLATFORM, HARDWARE & SOFTWARE REQUIREMENT SPECIFICATIONS :-

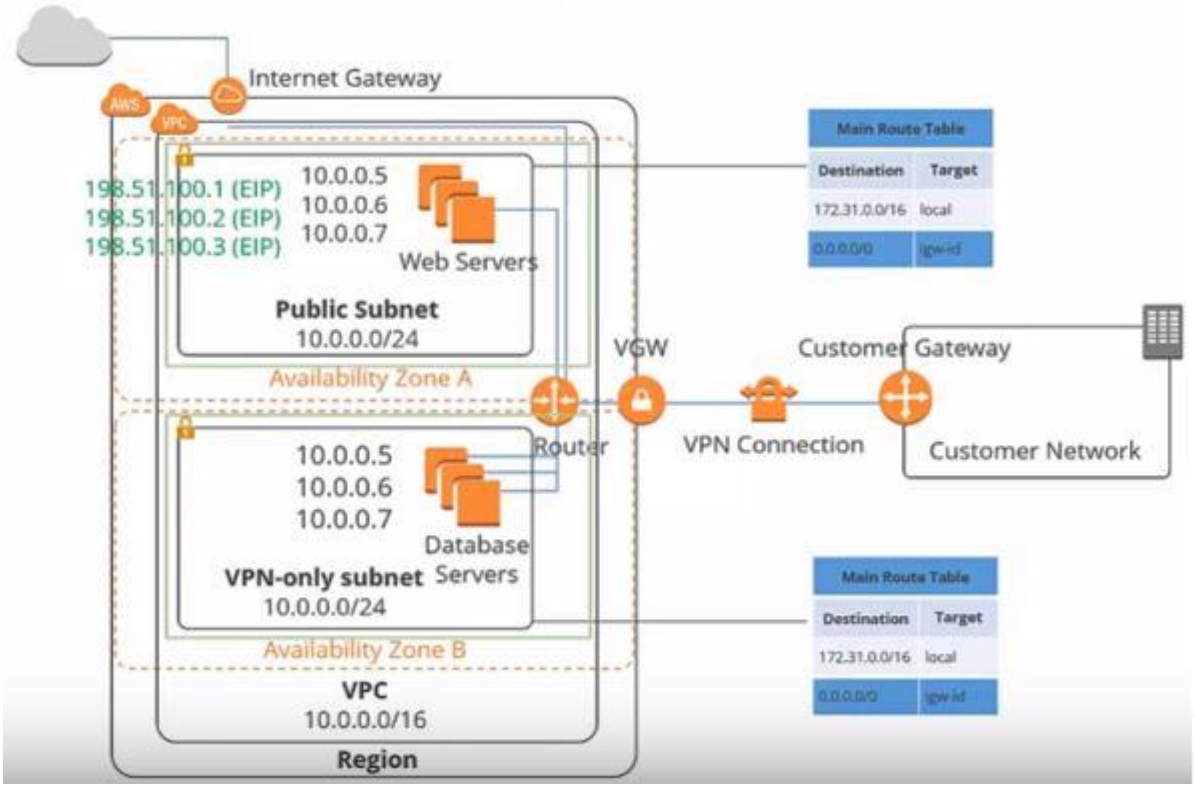
TOOLS :- PUTTY GEN,PUTTY.

5. PLATFORM:=AMAZON WEB SERVICE.

5.GOALS OF IMPLEMENTATION:-The implementation aims at seamless document sharing across the institution.

6.VPC DIAGRAM?


Application-to-application (A2A) subscribers
Amazon SQS
AWS Lambda
HTTPS
Amazon Kinesis Data Firehose
Publishers
Amazon SNS
Amazon S3
Amazon Redshift
Amazon Elasticsearch Service
Service providers
Datadog, New Relic, MongoDB, Splunk, and more
Application-to-person (A2P) subscribers
Mobile text (SMS)
Mobile push
Email



7.WHAT IS VPC?

=>Amazon Virtual Private Cloud (Amazon VPC) is a service that lets you launch AWS resources in a logically isolated virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 for most resources in your virtual private cloud, helping to ensure secure and easy access to resources and applications.

As one of AWS's foundational services, Amazon VPC makes it easy to customize your VPC's network configuration. You can create a public-facing subnet for your web servers that have access to the internet. It also lets you place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. Amazon VPC lets you to use multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Benefits of Using Amazon Virtual Private Cloud (Amazon VPC)

Secure and monitored network connections

Amazon VPC provides advanced security features that allow you to perform inbound and outbound filtering at the instance and subnet level. Additionally, you can store data in Amazon S3 and restrict access so that it's only accessible from instances inside your VPC. Amazon VPC

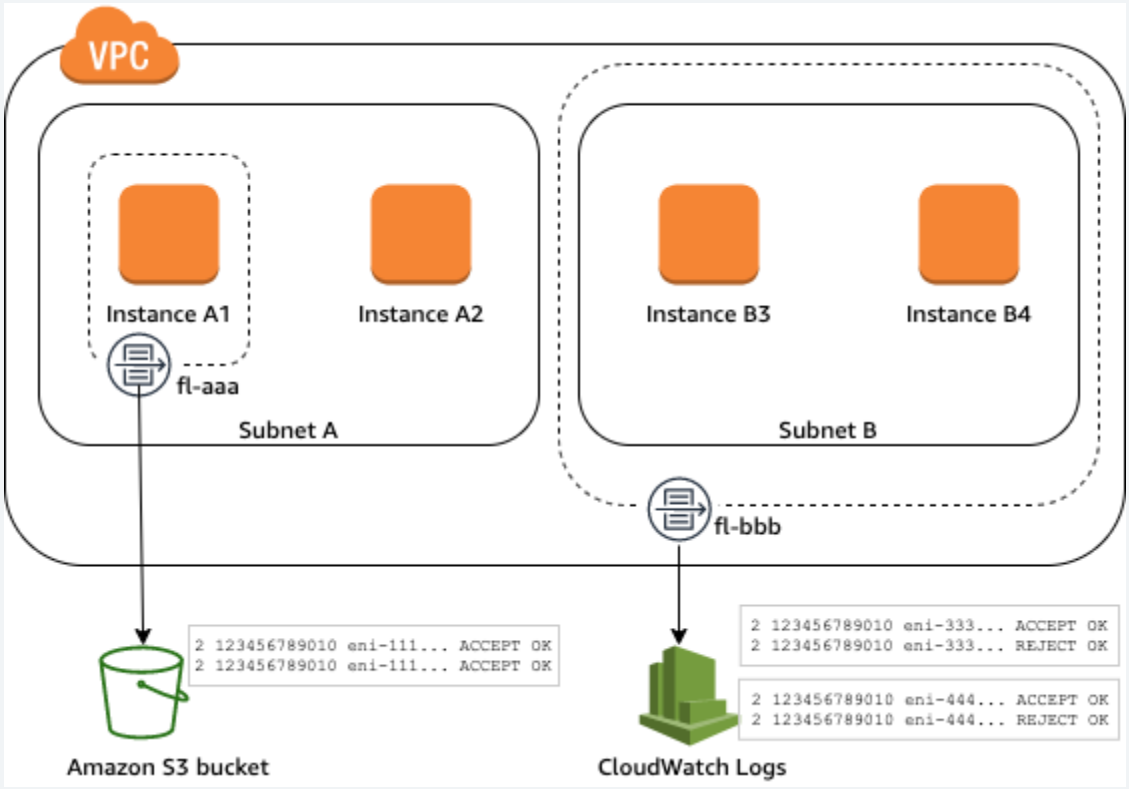
also has monitoring features that let you perform functions like out-of-band monitoring and inline traffic inspection, which help you screen and secure traffic.

Simple set-up and use

With Amazon VPC's simple set-up, you spend less time setting up, managing, and validating, so you can concentrate on building the applications that run in your VPCs. You can create a VPC easily using the AWS Management Console or Command Line Interface (CLI). Once you select from common network setups and find the best match for your needs, VPC automatically creates the subnets, IP ranges, route tables, and security groups you need. After configuring your network, you can easily validate it with Reachability Analyzer.

Customizable virtual network

Amazon VPC helps you control your virtual networking environment by letting you choose your own IP Address range, create your own subnets, and configure route tables to any available gateways. You can customize the network configuration by creating a public-facing subnet for your web servers that has access to the internet. Place your backend systems, such as databases or application servers, in a private-facing subnet. With Amazon VPC, you can ensure that your virtual private cloud is configured to fit your specific business needs.



8. WHAI IS SECURITY GROUPS?

=>A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC,

you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups.

If you launch an instance using the Amazon EC2 API or a command line tool and you don't specify a security group, the instance is automatically assigned to the default security group for the VPC. If you launch an instance using the Amazon EC2 console, you have an option to create a new security group for the instance.

For each security group, you add *rules* that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic. This section describes the basic things that you need to know about security groups for your VPC and their rules.

You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. For more information about the differences between security groups and network ACLs.

Default security group for your VPC

Your VPC automatically comes with a default security group. If you don't specify a different security group when you launch the instance, we associate the default security group with your instance.

Note

If you launch an instance in the Amazon EC2 console, the launch instance wizard automatically defines a "launch-wizard-*xx*" security group, which you can associate with the instance instead of the default security group.

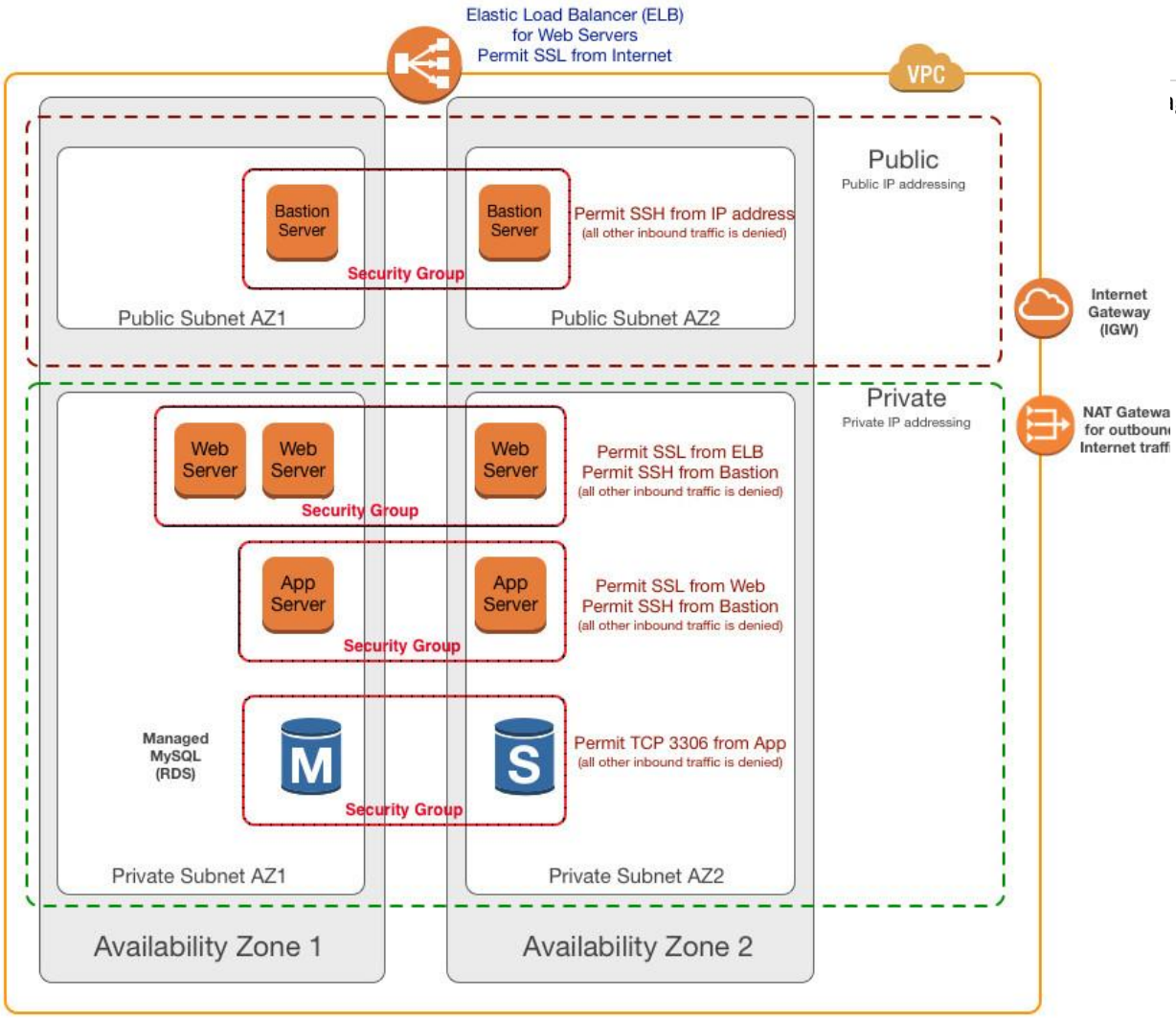
The following table describes the default rules for a default security group.

Inbound			
Source	**Protocol**	**Port range**	**Description**
The security group ID (sg-*xxxxxxxx*)	All	All	Allow inbound traffic from network interfaces (and their associated instances) that are assigned to the same security group.
Outbound			
Destination	**Protocol**	**Port range**	**Description**
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic. This rule is added by default if you create a VPC with an IPv6 CIDR block or if you associate an IPv6 CIDR block with your existing VPC.

You can change the rules for the default security group.

=You can't delete a default security group. If you try to delete the default security group, you get the following error: `Client.CannotDelete: the specified group: "sg-51530134" name: "default" cannot be deleted by a user.`

If you've modified the outbound rules for your security group, we do not automatically add an outbound rule for IPv6 traffic when you associate an IPv6 block with your VPC.



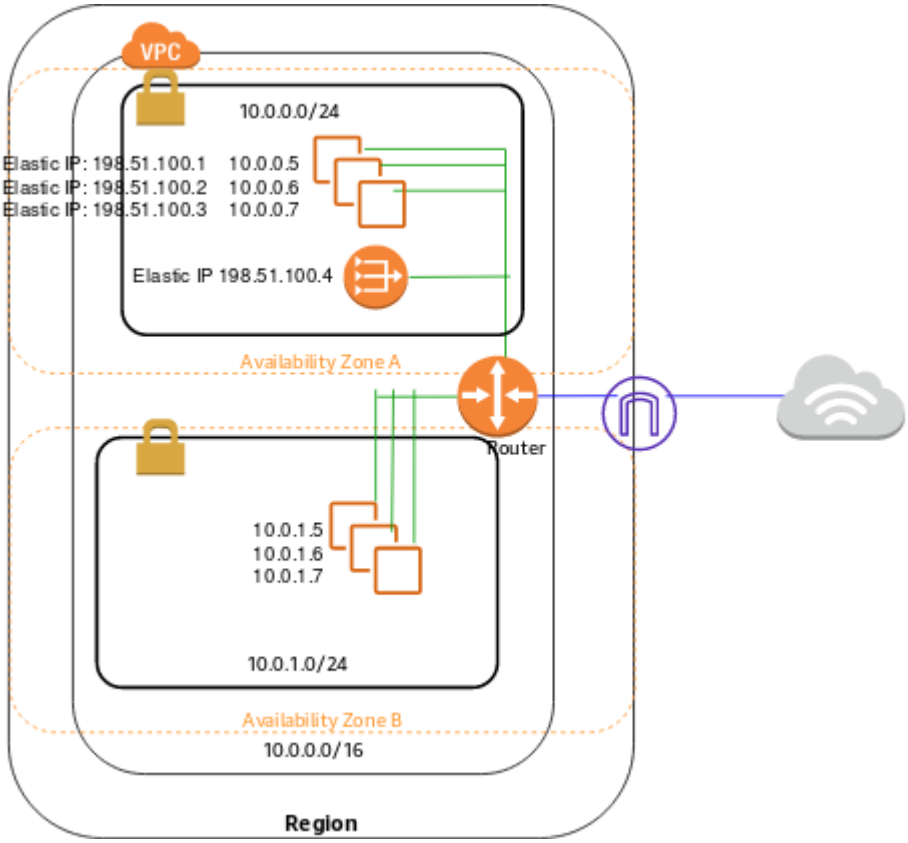
9.PRIVATE AND PUBLIC SUBNETS?

=>*The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet. We recommend this scenario if you want to run a public-facing web application, while maintaining back-end servers that aren't publicly accessible. A common example is a multi-tier website, with the web servers in a public subnet and the database servers in a private subnet. You can set up security and routing so that the web servers can communicate with the database servers.*

The instances in the public subnet can send outbound traffic directly to the internet, whereas the instances in the private subnet can't. Instead, the instances in the private subnet can access the internet by using a network address translation (NAT) gateway that resides in the public subnet. The database servers can connect to the internet for software updates using the NAT gateway, but the internet cannot establish connections to the database servers.

This scenario can also be optionally configured for IPv6—you can use the VPC wizard to create a VPC and subnets with associated IPv6 CIDR blocks. Instances launched into the subnets can receive IPv6 addresses, and communicate using IPv6. Instances in the private subnet can use an egress-only internet gateway to connect to the internet over IPv6, but the internet cannot establish connections to the private instances over IPv6. For more information about IPv4 and IPv6 addressing, see IP Addressing in your VPC.

For information about managing your EC2 instance software, see Managing software on your Linux instance in the *Amazon EC2 User Guide for Linux Instances*.



The configuration for this scenario includes the following:

- A VPC with a size /16 IPv4 CIDR block (example: 10.0.0.0/16). This provides 65,536 private IPv4 addresses.
- A public subnet with a size /24 IPv4 CIDR block (example: 10.0.0.0/24). This provides 256 private IPv4 addresses. A public subnet is a subnet that's associated with a route table that has a route to an internet gateway.
- A private subnet with a size /24 IPv4 CIDR block (example: 10.0.1.0/24). This provides 256 private IPv4 addresses.
- An internet gateway. This connects the VPC to the internet and to other AWS services.
- Instances with private IPv4 addresses in the subnet range (examples: 10.0.0.5, 10.0.1.5). This enables them to communicate with each other and other instances in the VPC.
- Instances in the public subnet with Elastic IPv4 addresses (example: 198.51.100.1), which are public IPv4 addresses that enable them to be reached from the internet. The instances can have public IP addresses assigned at launch instead of Elastic IP addresses. Instances in the private subnet are back-end servers that don't need to accept incoming traffic from the internet and therefore

do not have public IP addresses; however, they can send requests to the internet using the NAT gateway (see the next bullet).

- A NAT gateway with its own Elastic IPv4 address. Instances in the private subnet can send requests to the internet through the NAT gateway over IPv4 (for example, for software updates).
- A custom route table associated with the public subnet. This route table contains an entry that enables instances in the subnet to communicate with other instances in the VPC over IPv4, and an entry that enables instances in the subnet to communicate directly with the internet over IPv4.
- The main route table associated with the private subnet. The route table contains an entry that enables instances in the subnet to communicate with other instances in the VPC over IPv4, and an entry that enables instances in the subnet to communicate with the internet through the NAT gateway over IPv4.

For more information about subnets, see VPCs and subnets. For more information about internet gateways, see Internet gateways. For more information about NAT gateways, see NAT gateways.

10. NETWORK ACLS??

=>A *network access control list (ACL)* is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. For more information about the differences between security groups and network ACLs, see Compare security groups and network ACLs.

Network ACL basics

The following are the basic things that you need to know about network ACLs:

- Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.
- You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.
- You can associate a network ACL with multiple subnets. However, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.
- A network ACL contains a numbered list of rules. We evaluate the rules in order, starting with the lowest numbered rule, to determine whether traffic is allowed

in or out of any subnet associated with the network ACL. The highest number that you can use for a rule is 32766. We recommend that you start by creating rules in increments (for example, increments of 10 or 100) so that you can insert new rules where you need to later on.

- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Network ACLs are stateless, which means that responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

There are quotas (limits) for the number of network ACLs per VPC, and the number of rules per network ACL. For more information, see Amazon VPC quotas.

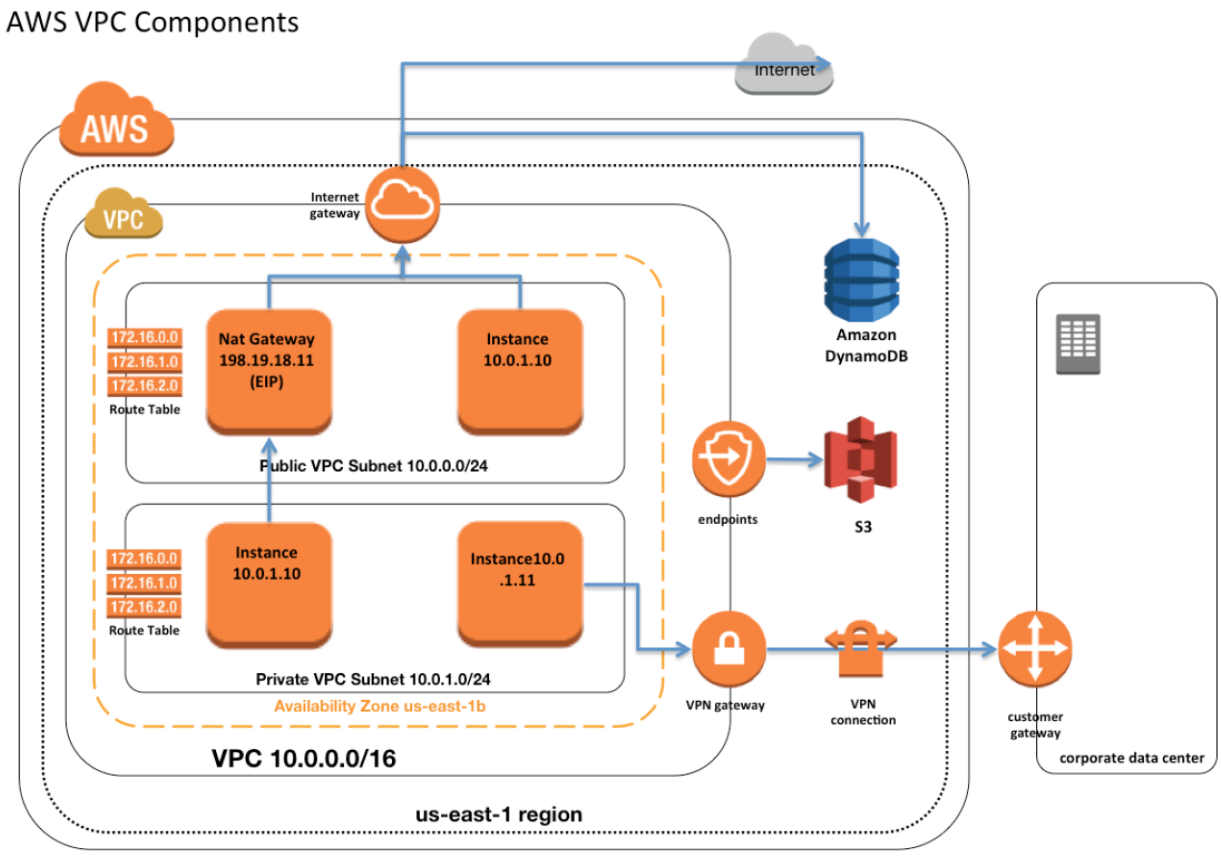
Network ACL rules

You can add or remove rules from the default network ACL, or create additional network ACLs for your VPC. When you add or remove rules from a network ACL, the changes are automatically applied to the subnets that it's associated with.

The following are the parts of a network ACL rule:

- **Rule number**. Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that might contradict it.
- **Type**. The type of traffic; for example, SSH. You can also specify all traffic or a custom range.
- **Protocol**. You can specify any protocol that has a standard protocol number. For more information, see Protocol Numbers. If you specify ICMP as the protocol, you can specify any or all of the ICMP types and codes.
- **Port range**. The listening port or port range for the traffic. For example, 80 for HTTP traffic.
- **Source**. [Inbound rules only] The source of the traffic (CIDR range).
- **Destination**. [Outbound rules only] The destination for the traffic (CIDR range).
- **Allow/Deny**. Whether to *allow* or *deny* the specified traffic.

If you add a rule using a command line tool or the Amazon EC2 API, the CIDR range is automatically modified to its canonical form. For example, if you specify `100.68.0.18/18` *for the CIDR range, we create a rule with a* `100.68.0.0/18` *CIDR range.*



11. ABOUT NACL AND SECURITY GROUP?

It adds a security layer to EC2 instances that control both inbound and outbound traffic at the instance level.

What is NACL?

NACL also adds an additional layer of security associated with subnets that control both inbound and outbound traffic at the subnet level.

Combining Security Group and NACL

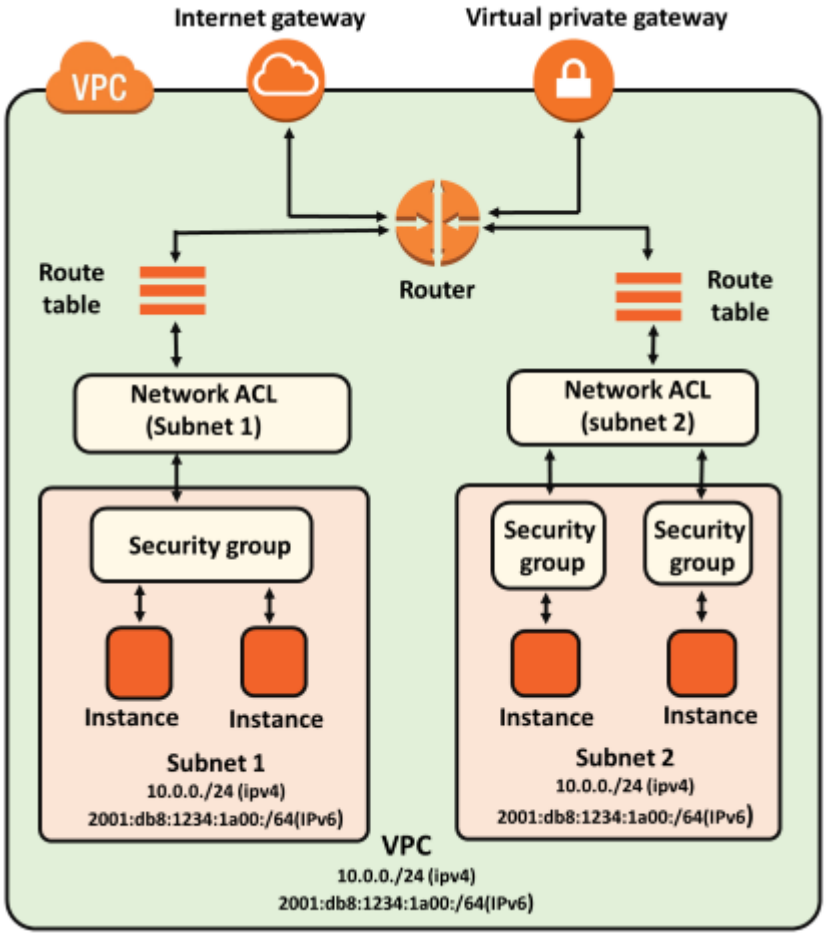
Maximum number of rules that exist per NACL: 20

Maximum number of rules that can exist per Security Group: 50

Maximum number of Security Groups that can exist per instance: 5

Maximum number of rules that can exist per instance: 5*50 + 20 = 270

Differences b/w Security Group and NACL



Comparison of Security Groups and Network ACLs

The following table summarizes the basic differences between security groups and network ACLs.

Security Group	Network ACL
Operates at the instance level (first layer of defense)	Operates at the subnet level (second layer of defense)
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (backup layer of defense, so you don't have to rely on someone specifying the security group)

Why do we need a Data Pipeline?

Let's consider an example of javaTpoint which focusses on the technical content. The following are the main goals:

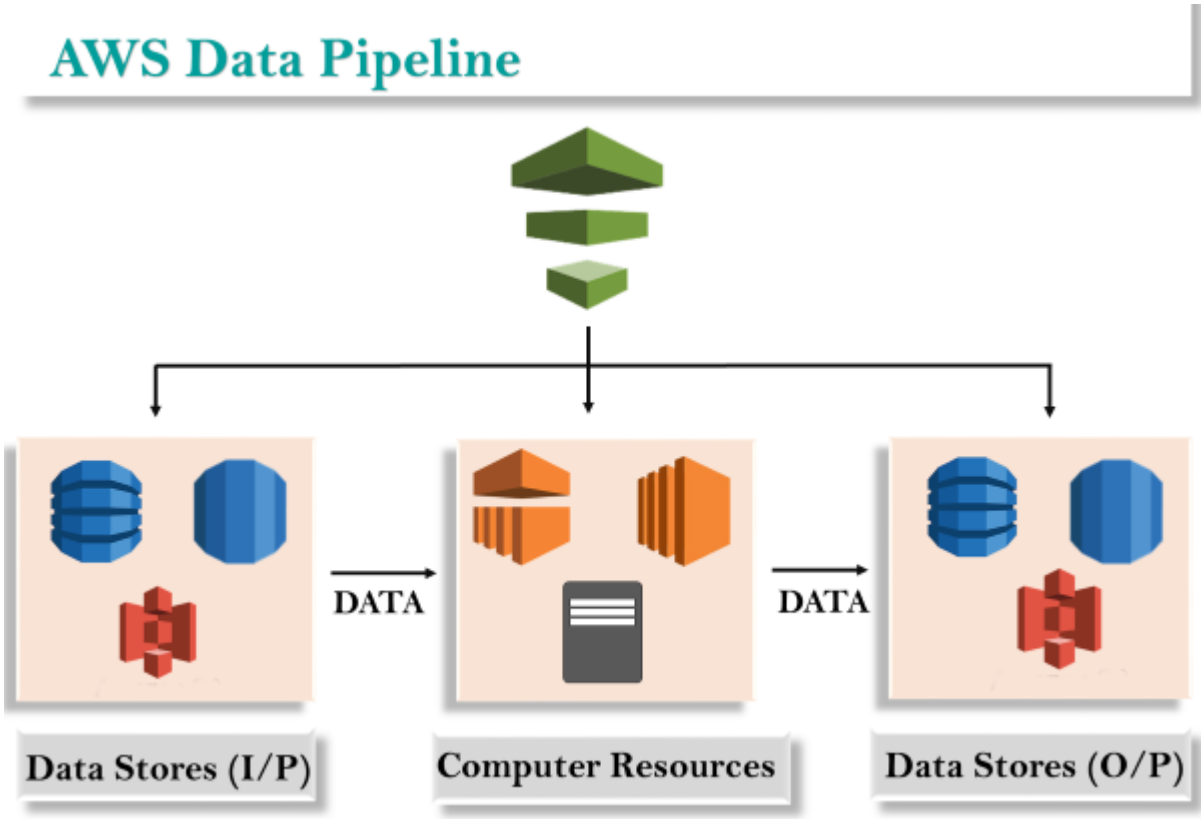
- **Improve the content:** Display the content what the customers want to see in the future. In this way, content can be enhanced.
- **Manage application efficiently:** To keep track of all the activities in an application and storing the data in an existing database rather than storing the data in a new database.
- **Faster:** To improve the business faster but at a cheaper rate.

Achieving the above goals might be a difficult task as a huge amount of data is stored in different formats, so analyzing, storing and processing of data becomes very complex. The various tools are used to store different formats of data. The feasible solution for such a situation is to use the **Data Pipeline.** Data Pipeline integrates the data which is spread across different data sources, and it also processes the data on the same location.

What is a Data Pipeline?

AWS Data Pipeline is a web service that can access the data from different services and analyzes, processes the data at the same location, and then stores the data to different AWS services such as DynamoDB, Amazon S3, etc.

For example, using data pipeline, you can archive your web server logs to the Amazon S3 bucket on daily basis and then run the EMR cluster on these logs that generate the reports on the weekly basis.



12. INTERNET GATEWAYS?

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. For more information, see Enable internet access.

An internet gateway supports IPv4 and IPv6 traffic. It does not cause availability risks or bandwidth constraints on your network traffic.

There's no additional charge for having an internet gateway in your account.

Enable internet access

To enable access to or from the internet for instances in a subnet in a VPC, you must do the following.

- Create an internet gateway and attach it to your VPC.
- Add a route to your subnet's route table that directs internet-bound traffic to the internet gateway.
- Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
- Ensure that your network access control lists and security group rules allow the relevant traffic to flow to and from your instance.

Public and private subnets

If a subnet is associated with a route table that has a route to an internet gateway, it's known as a *public subnet*. If a subnet is associated with a route table that does not have a route to an internet gateway, it's known as a *private subnet*.

In your public subnet's route table, you can specify a route for the internet gateway to all destinations not explicitly known to the route table (`0.0.0.0/0` for IPv4 or `::/0` for IPv6). Alternatively, you can scope the route to a narrower range of IP addresses; for example, the public IPv4 addresses of your company's public endpoints outside of AWS, or the Elastic IP addresses of other Amazon EC2 instances outside your VPC.

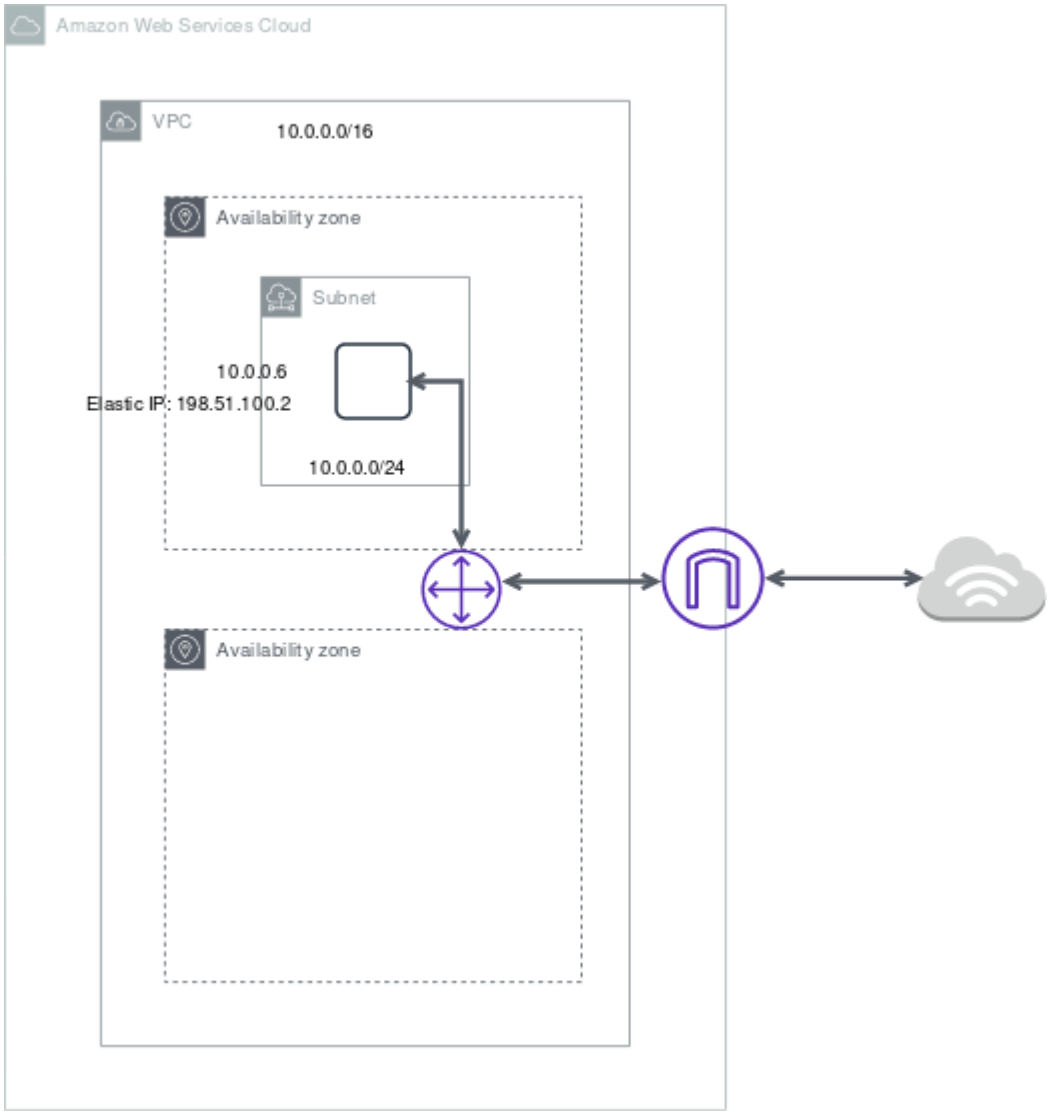
IP addresses and NAT

To enable communication over the internet for IPv4, your instance must have a public IPv4 address or an Elastic IP address that's associated with a private IPv4 address on your instance. Your instance is only aware of the private (internal) IP address space defined within the VPC and

subnet. The internet gateway logically provides the one-to-one NAT on behalf of your instance, so that when traffic leaves your VPC subnet and goes to the internet, the reply address field is set to the public IPv4 address or Elastic IP address of your instance, and not its private IP address. Conversely, traffic that's destined for the public IPv4 address or Elastic IP address of your instance has its destination address translated into the instance's private IPv4 address before the traffic is delivered to the VPC.

To enable communication over the internet for IPv6, your VPC and subnet must have an associated IPv6 CIDR block, and your instance must be assigned an IPv6 address from the range of the subnet. IPv6 addresses are globally unique, and therefore public by default.

In the following diagram, Subnet 1 in the VPC is a public subnet. It's associated with a custom route table that points all internet-bound IPv4 traffic to an internet gateway. The instance has an Elastic IP address, which enables communication with the internet.



To provide your instances with internet access without assigning them public IP addresses, you can use a NAT device instead. A NAT device enables instances in a private subnet to connect to the internet, but prevents hosts on the internet from initiating connections with the instances. For more information, see NAT devices for your VPC.

Internet access for default and nondefault VPCs

The following table provides an overview of whether your VPC automatically comes with the components required for internet access over IPv4 or IPv6.

Component	Default VPC	Nondefault VPC
Internet gateway	Yes	Yes, if you created the VPC using the first or second option in the VPC wizard. Otherwise, you must manually create and attach the internet gateway.
Route table with route to internet gateway for IPv4 traffic (0.0.0.0/0)	Yes	Yes, if you created the VPC using the first or second option in the VPC wizard. Otherwise, you must manually create the route table and add the route.
Route table with route to internet gateway for IPv6 traffic (::/0)	No	Yes, if you created the VPC using the first or second option in the VPC wizard, and if you specified the option to associate an IPv6 CIDR block with the VPC. Otherwise, you must manually create the route table and add the route.
Public IPv4 address automatically assigned to instance launched into subnet	Yes (default subnet)	No (nondefault subnet)
IPv6 address automatically assigned to instance launched into subnet	No (default subnet)	No (nondefault subnet)

For more information about default VPCs, see Default VPC and default subnets. For more information about using the VPC wizard to create a VPC with an internet gateway, see VPC with a single public subnet or VPC with public and private subnets (NAT).

For more information about IP addressing in your VPC, and controlling how instances are assigned public IPv4 or IPv6 addresses, see IP Addressing in your VPC.

When you add a new subnet to your VPC, you must set up the routing and security that you want for the subnet.

Add an internet gateway to your VPC

The following describes how to manually create a public subnet and attach an internet gateway to your VPC to support internet access.

Tasks

- Create a subnet
- Create and attach an internet gateway
- Create a custom route table
- Create a security group for internet access
- Assign an Elastic IP address to an instance
- Detach an internet gateway from your VPC
- Delete an internet gateway
- API and command overview

Create a subnet

To add a subnet to your VPC

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Subnets**, **Create subnet**.
3. Specify the subnet details as needed:.
    - **Name tag**: Optionally provide a name for your subnet. Doing so creates a tag with a key of `Name` and the value that you specify.
    - **VPC**: Choose the VPC for which you're creating the subnet.
    - **Availability Zone**: Optionally choose an Availability Zone or Local Zone in which your subnet will reside, or leave the default **No Preference** to let AWS choose an Availability Zone for you.

      For information about the Regions that support Local Zones, see Available Regions in the *Amazon EC2 User Guide for Linux Instances*.
    - **IPv4 CIDR block**: Specify an IPv4 CIDR block for your subnet, for example, `10.0.1.0/24`. For more information, see VPC and subnet sizing for IPv4.
    - **IPv6 CIDR block**: (Optional) If you've associated an IPv6 CIDR block with your VPC, choose **Specify a custom IPv6 CIDR**. Specify the hexadecimal pair value for the subnet, or leave the default value.

4. Choose **Create**.

For more information about subnets, see VPCs and subnets.

Create and attach an internet gateway

After you create an internet gateway, attach it to your VPC.

To create an internet gateway and attach it to your VPC

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Internet Gateways**, and then choose **Create internet gateway**.
3. Optionally name your internet gateway.
4. Optionally add or remove a tag.

   [Add a tag] Choose **Add tag** and do the following:
   - For **Key**, enter the key name.
   - For **Value**, enter the key value.

   [Remove a tag] Choose **Remove** to the right of the tag's Key and Value.
5. Choose **Create internet gateway**.
6. Select the internet gateway that you just created, and then choose **Actions, Attach to VPC**.
7. Select your VPC from the list, and then choose **Attach internet gateway**.

Create a custom route table

When you create a subnet, we automatically associate it with the main route table for the VPC. By default, the main route table doesn't contain a route to an internet gateway. The following procedure creates a custom route table with a route that sends traffic destined outside the VPC to the internet gateway, and then associates it with your subnet.

To create a custom route table

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Route Tables**, and then choose **Create route table**.

3. In the **Create route table** dialog box, optionally name your route table, then select your VPC, and then choose **Create route table**.
4. Select the custom route table that you just created. The details pane displays tabs for working with its routes, associations, and route propagation.
5. On the **Routes** tab, choose **Edit routes**, **Add route**, and add the following routes as necessary. Choose **Save changes** when you're done.
    - For IPv4 traffic, specify `0.0.0.0/0` in the **Destination** box, and select the internet gateway ID in the **Target** list.
    - For IPv6 traffic, specify `::/0` in the **Destination** box, and select the internet gateway ID in the **Target** list.
6. On the **Subnet associations** tab, choose **Edit subnet associations**, select the check box for the subnet, and then choose **Save associations**.

For more information, see Route tables for your VPC.

Create a security group for internet access

By default, a VPC security group allows all outbound traffic. You can create a new security group and add rules that allow inbound traffic from the internet. You can then associate the security group with instances in the public subnet.

To create a security group and associate it with your instances

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Security Groups**, and then choose **Create Security Group**.
3. In the **Create Security Group** dialog box, specify a name for the security group and a description. Select the ID of your VPC from the **VPC** list, and then choose **Yes, Create**.
4. Select the security group. The details pane displays the details for the security group, plus tabs for working with its inbound rules and outbound rules.
5. On the **Inbound Rules** tab, choose **Edit**. Choose **Add Rule**, and complete the required information. For example, select **HTTP** or **HTTPS** from the **Type** list, and enter the **Source** as `0.0.0.0/0` for IPv4 traffic, or `::/0` for IPv6 traffic. Choose **Save** when you're done.
6. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
7. In the navigation pane, choose **Instances**.

8. Select the instance, choose **Actions**, then **Networking**, and then select **Change Security Groups**.
9. In the **Change Security Groups** dialog box, clear the check box for the currently selected security group, and select the new one. Choose **Assign Security Groups**.

For more information, see Security groups for your VPC.

Assign an Elastic IP address to an instance

After you've launched an instance into the subnet, you must assign it an Elastic IP address if you want it to be reachable from the internet over IPv4.

Note

If you assigned a public IPv4 address to your instance during launch, then your instance is reachable from the internet, and you do not need to assign it an Elastic IP address. For more information about IP addressing for your instance, see IP Addressing in your VPC.

To allocate an Elastic IP address and assign it to an instance using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Elastic IPs**.
3. Choose **Allocate new address**.
4. Choose **Allocate**.

   Note

   If your account supports EC2-Classic, first choose **VPC**.

5. Select the Elastic IP address from the list, choose **Actions**, and then choose **Associate address**.
6. Choose **Instance** or **Network interface**, and then select either the instance or network interface ID. Select the private IP address with which to associate the Elastic IP address, and then choose **Associate**.

For more information, see Elastic IP addresses.

Detach an internet gateway from your VPC

If you no longer need internet access for instances that you launch into a nondefault VPC, you can detach an internet gateway from a VPC. You can't detach an internet gateway if the VPC has resources with associated public IP addresses or Elastic IP addresses.

To detach an internet gateway

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Elastic IPs** and select the Elastic IP address.
3. Choose **Actions**, **Disassociate address**. Choose **Disassociate address**.
4. In the navigation pane, choose **Internet Gateways**.
5. Select the internet gateway and choose **Actions, Detach from VPC**.
6. In the **Detach from VPC** dialog box, choose **Detach internet gateway**.

Delete an internet gateway

If you no longer need an internet gateway, you can delete it. You can't delete an internet gateway if it's still attached to a VPC.

To delete an internet gateway

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Internet Gateways**.
3. Select the internet gateway and choose **Actions**, **Delete internet gateway**.
4. In the **Delete internet gateway** dialog box, enter `delete`, and choose **Delete internet gateway**.

API and command overview

You can perform the tasks described on this page using the command line or an API. For more information about the command line interfaces and a list of available API actions, see Access Amazon VPC.

Create an internet gateway

- create-internet-gateway (AWS CLI)
- New-EC2InternetGateway (AWS Tools for Windows PowerShell)

Attach an internet gateway to a VPC

- attach-internet-gateway (AWS CLI)
- Add-EC2InternetGateway (AWS Tools for Windows PowerShell)

Describe an internet gateway

- describe-internet-gateways (AWS CLI)
- Get-EC2InternetGateway (AWS Tools for Windows PowerShell)

Detach an internet gateway from a VPC

- detach-internet-gateway (AWS CLI)
- Dismount-EC2InternetGateway (AWS Tools for Windows PowerShell)

Delete an internet gateway

- delete-internet-gateway (AWS CLI)
- Remove-EC2InternetGateway (AWS Tools for Windows PowerShell)

13.NAT GATEWAYS?

A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.

The NAT gateway replaces the source IPv4 address of the instances with the private IP address of the NAT gateway. When sending response traffic to the instances, the NAT device translates the addresses back to the original source IPv4 addresses.

When you create a NAT gateway, you specify one of the following connectivity types:

- **Public** – (Default) Instances in private subnets can connect to the internet through a public NAT gateway, but cannot receive unsolicited inbound connections from the internet. You create a public NAT gateway in a public subnet and must associate an elastic IP address with the NAT gateway at creation. You route traffic from the NAT gateway to the internet gateway for the VPC. Alternatively, you can use a public NAT gateway to connect to other VPCs or

your on-premises network. In this case, you route traffic from the NAT gateway through a transit gateway or a virtual private gateway.

- **Private** – Instances in private subnets can connect to other VPCs or your on-premises network through a private NAT gateway. You can route traffic from the NAT gateway through a transit gateway or a virtual private gateway. You cannot associate an elastic IP address with a private NAT gateway. You can attach an internet gateway to a VPC with a private NAT gateway, but if you route traffic from the private NAT gateway to the internet gateway, the internet gateway drops the traffic.

Pricing

NAT gateway hourly usage and data processing rates apply. Amazon EC2 charges for data transfer also apply. For more information, see Amazon VPC Pricing.

Contents

NAT gateway basics

Each NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone. There is a quota on the number of NAT gateways that you can create in each Availability Zone. For more information, see Amazon VPC quotas.

If you have resources in multiple Availability Zones and they share one NAT gateway, and if the NAT gateway's Availability Zone is down,

resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.

The following characteristics and rules apply to NAT gateways:

- A NAT gateway supports the following protocols: TCP, UDP, and ICMP.
- NAT gateways are not supported for IPv6 traffic—use an outbound-only (egress-only) internet gateway instead. For more information, see Egress-only internet gateways.
- A NAT gateway supports 5 Gbps of bandwidth and automatically scales up to 45 Gbps. If you require more bandwidth, you can split your resources into multiple subnets and create a NAT gateway in each subnet.
- A NAT gateway can support up to 55,000 simultaneous connections to each unique destination. This limit also applies if you create approximately 900 connections per second to a single destination (about 55,000 connections per minute). If the destination IP address, the destination port, or the protocol (TCP/UDP/ICMP) changes, you can create an additional 55,000 connections. For more than 55,000 connections, there is an increased chance of connection errors due to port allocation errors. These errors can be monitored by viewing the `ErrorPortAllocation` CloudWatch metric for your NAT gateway. For more information, see Monitor NAT gateways using Amazon CloudWatch.
- You can associate exactly one Elastic IP address with a public NAT gateway. You cannot disassociate an Elastic IP address from a NAT gateway after it's created. To use a different Elastic IP address for your NAT gateway, you must create a new NAT gateway with the required address, update your route tables, and then delete the existing NAT gateway if it's no longer required.
- A private NAT gateway receives an available private IP address from the subnet in which it is configured. You cannot detach this private IP address and you cannot attach additional private IP addresses.
- You cannot associate a security group with a NAT gateway. You can associate security groups with your instances to control inbound and outbound traffic.
- You can use a network ACL to control the traffic to and from the subnet for your NAT gateway. NAT gateways use ports 1024–65535. For more information, see Network ACLs.
- A NAT gateway receives a network interface that's automatically assigned a private IP address from the IP address range of the subnet. You can view the

network interface for the NAT gateway using the Amazon EC2 console. For more information, see Viewing details about a network interface. You cannot modify the attributes of this network interface.

- A NAT gateway cannot be accessed through a ClassicLink connection that is associated with your VPC.
- You cannot route traffic to a NAT gateway through a VPC peering connection, a Site-to-Site VPN connection, or AWS Direct Connect. A NAT gateway cannot be used by resources on the other side of these connections.

Control the use of NAT gateways

By default, IAM users do not have permission to work with NAT gateways. You can create an IAM user policy that grants users permissions to create, describe, and delete NAT gateways. For more information, see Identity and access management for Amazon VPC.

Work with NAT gateways

You can use the Amazon VPC console to create and manage your NAT gateways. You can also use the Amazon VPC wizard to create a VPC with a public subnet, a private subnet, and a NAT gateway. For more information, see VPC with public and private subnets (NAT).

Tasks

- Create a NAT gateway
- Tag a NAT gateway
- Delete a NAT gateway

Create a NAT gateway

To create a NAT gateway, enter an optional name, a subnet, and an optional connectivity type. With a public NAT gateway, you must specify an available elastic IP address. A private NAT gateway receives a primary

private IP address selected at random from its subnet. You cannot detach the primary private IP address or add secondary private IP addresses.

To create a NAT gateway

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **NAT Gateways**.
3. Choose **Create NAT Gateway** and do the following:
    a. (Optional) Specify a name for the NAT gateway. This creates a tag where the key is `Name` and the value is the name that you specify.
    b. Select the subnet in which to create the NAT gateway.
    c. For **Connectivity type**, select **Private** to create a private NAT gateway or **Public** (the default) to create a public NAT gateway.
    d. (Public NAT gateway only) For **Elastic IP allocation ID**, select an Elastic IP address to associate with the NAT gateway.
    e. (Optional) For each tag, choose **Add new tag** and enter the key name and value.
    f. Choose **Create a NAT Gateway**.
4. The initial status of the NAT gateway is `Pending`. After the status changes to `Available`, the NAT gateway is ready for you to use. Add a route to the NAT gateway to the route tables for the private subnets and add routes to the route table for the NAT gateway.

    If the status of the NAT gateway changes to `Failed`, there was an error during creation. For more information, see NAT gateway creation fails.

Tag a NAT gateway

You can tag your NAT gateway to help you identify it or categorize it according to your organization's needs. For information about working with tags, see Tagging your Amazon EC2 resources in the Amazon EC2 User Guide for Linux Instances.

Cost allocation tags are supported for NAT gateways. Therefore, you can also use tags to organize your AWS bill and reflect your own cost structure. For more information, see Using cost allocation tags in the AWS Billing and Cost Management User Guide. For more information

about setting up a cost allocation report with tags, see Monthly cost allocation report in About AWS Account Billing.

Delete a NAT gateway

If you no longer need a NAT gateway, you can delete it. After you delete a NAT gateway, its entry remains visible in the Amazon VPC console for about an hour, after which it's automatically removed. You cannot remove this entry yourself.

Deleting a NAT gateway disassociates its Elastic IP address, but does not release the address from your account. If you delete a NAT gateway, the NAT gateway routes remain in a `blackhole` status until you delete or update the routes.

To delete a NAT gateway

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **NAT Gateways**.
3. Select the radio button for the NAT gateway, and then choose **Actions**, **Delete NAT gateway**.
4. When prompted for confirmation, enter `delete` and then choose **Delete**.
5. If you no longer need the Elastic IP address that was associated with a public NAT gateway, we recommend that you release it. For more information, see Release an Elastic IP address.

NAT gateway scenarios

The following are example use cases for public and private NAT gateways.

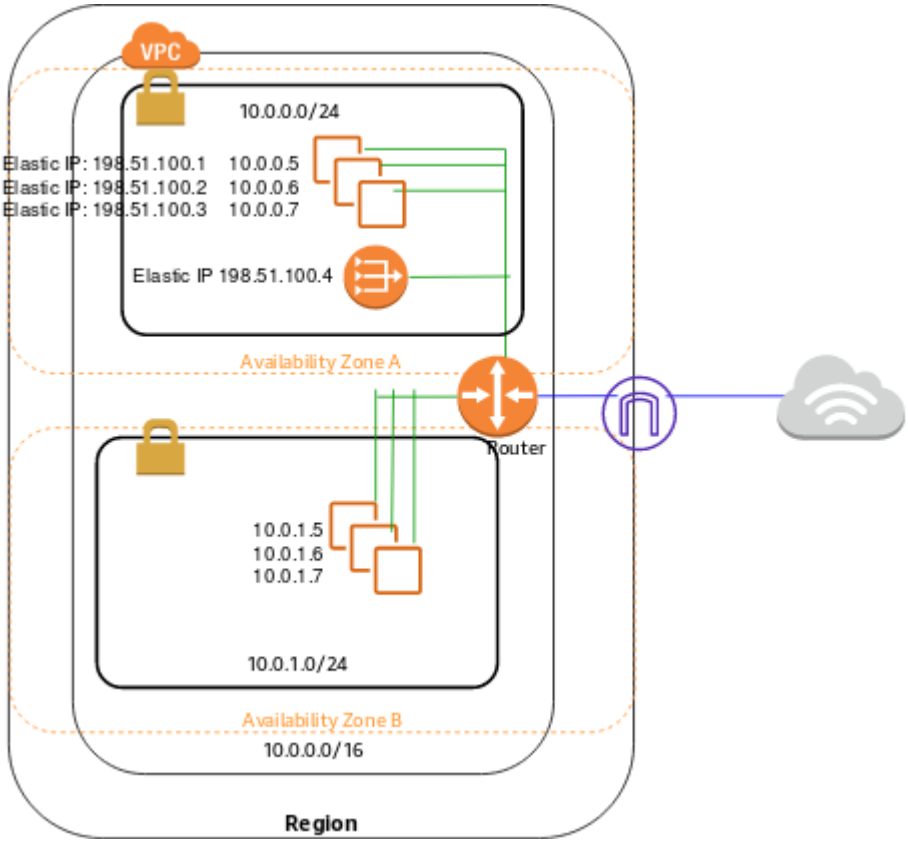
Scenarios

- Access the internet from a private subnet
- Allow access to your network from allow-listed IP addresses

Scenario: Access the internet from a private subnet

You can use a public NAT gateway to enable instances in a private subnet to send outbound traffic to the internet, but the internet cannot establish connections to the instances.

The following diagram illustrates the architecture for this use case. The public subnet in Availability Zone A contains the NAT gateway. The private subnet in Availability Zone B contains instances. The router sends internet bound traffic from the instances in the private subnet to the NAT gateway. The NAT gateway sends the traffic to the internet gateway, using the elastic IP address for the NAT gateway as the source IP address.



The following is the route table associated with the public subnet in Availability Zone A. The first entry is the default entry for local routing in the VPC; it enables the instances in the VPC to communicate with each other. The second entry sends all other subnet traffic to the internet gateway; this enables the NAT gateway to access the internet.

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*internet-gateway-id*

The following is the route table associated with the private subnet in Availability Zone B. The first entry is the default entry for local routing in the VPC; it enables the instances in the VPC to communicate with each other. The second entry sends all other subnet traffic, such as internet bound traffic, to the NAT gateway.

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

Test the public NAT gateway

After you've created your NAT gateway and updated your route tables, you can ping remote addresses on the internet from an instance in your private subnet to test whether it can connect to the internet. For an example of how to do this, see Test the internet connection.

If you can connect to the internet, you can also test whether internet traffic is routed through the NAT gateway:

- Trace the route of traffic from an instance in your private subnet. To do this, run the `traceroute` command from a Linux instance in your private subnet. In the output, you should see the private IP address of the NAT gateway in one of the hops (usually the first hop).
- Use a third-party website or tool that displays the source IP address when you connect to it from an instance in your private subnet. The source IP address should be the elastic IP address of the NAT gateway.

If these tests fail, see Troubleshoot NAT gateways.

Test the internet connection

The following example demonstrates how to test whether an instance in a private subnet can connect to the internet.

1. Launch an instance in your public subnet (use this as a bastion host). For more information, see Launch an instance into your subnet. In the launch wizard, ensure that you select an Amazon Linux AMI, and assign a public IP address to your instance. Ensure that your security group rules allow inbound SSH traffic from the range of IP addresses for your local network, and outbound SSH traffic to the IP address range of your private subnet (you can also use `0.0.0.0/0` for both inbound and outbound SSH traffic for this test).
2. Launch an instance in your private subnet. In the launch wizard, ensure that you select an Amazon Linux AMI. Do not assign a public IP address to your instance. Ensure that your security group rules allow inbound SSH traffic from the private IP address of your instance that you launched in the public subnet, and all outbound ICMP traffic. You must choose the same key pair that you used to launch your instance in the public subnet.
3. Configure SSH agent forwarding on your local computer, and connect to your bastion host in the public subnet. For more information, see To configure SSH agent forwarding for Linux or macOS or To configure SSH agent forwarding for Windows (PuTTY).
4. From your bastion host, connect to your instance in the private subnet, and then test the internet connection from your instance in the private subnet. For more information, see To test the internet connection.

To configure SSH agent forwarding for Linux or macOS

1. From your local machine, add your private key to the authentication agent.

   For Linux, use the following command.

   ```
   ssh-add -c mykeypair.pem
   ```

   For macOS, use the following command.

   ```
   ssh-add -K mykeypair.pem
   ```

2. Connect to your instance in the public subnet using the `-A` option to enable SSH agent forwarding, and use the instance's public address, as shown in the following example.

   ```
   ssh -A ec2-user@54.0.0.123
   ```

To configure SSH agent forwarding for Windows (PuTTY)

1. Download and install Pageant from the PuTTY download page, if not already installed.
2. Convert your private key to .ppk format. For more information, see Converting your private key using PuTTYgen in the *Amazon EC2 User Guide for Linux Instances*.
3. Start Pageant, right-click the Pageant icon on the taskbar (it may be hidden), and choose **Add Key**. Select the .ppk file that you created, enter the passphrase if necessary, and choose **Open**.
4. Start a PuTTY session and connect to your instance in the public subnet using its public IP address. For more information, see Connecting to your Linux instance. In the **Auth** category, ensure that you select the **Allow agent forwarding** option, and leave the **Private key file for authentication** box blank.

To test the internet connection

1. From your instance in the public subnet, connect to your instance in your private subnet by using its private IP address as shown in the following example.

```
ssh ec2-user@10.0.1.123
```

2. From your private instance, test that you can connect to the internet by running the `ping` command for a website that has ICMP enabled.

```
ping ietf.org
PING ietf.org (4.31.198.44) 56(84) bytes of data.
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=47
time=86.0 ms
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=47
time=75.6 ms
...
```

   Press **Ctrl+C** on your keyboard to cancel the `ping` command. If the `ping` command fails, see Instances cannot access the internet.
3. (Optional) If you no longer require your instances, terminate them. For more information, see Terminate your instance in the *Amazon EC2 User Guide for Linux Instances*.

Scenario: Allow access to your network from allow-listed IP addresses

Instead of assigning each instance a separate IP address from the IP address range that is allowed to access your on-premises network, you

can create a subnet in your VPC with the allowed IP address range, create a private NAT gateway in the subnet, and route the traffic from your VPC destined for your on-premises network through the NAT gateway.

Migrate from a NAT instance

If you're already using a NAT instance, you can replace it with a NAT gateway. To do this, you can create a NAT gateway in the same subnet as your NAT instance, and then replace the existing route in your route table that points to the NAT instance with a route that points to the NAT gateway. To use the same Elastic IP address for the NAT gateway that you currently use for your NAT instance, you must first also disassociate the Elastic IP address from your NAT instance and then associate it with your NAT gateway when you create the gateway.

If you change your routing from a NAT instance to a NAT gateway, or if you disassociate the Elastic IP address from your NAT instance, any current connections are dropped and have to be re-established. Ensure that you do not have any critical tasks (or any other tasks that operate through the NAT instance) running.

API and CLI overview

You can perform the tasks described on this page using the command line or API. For more information about the command line interfaces and a list of available API operations, see Access Amazon VPC.

Create a NAT gateway

- create-nat-gateway (AWS CLI)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)
- CreateNatGateway (Amazon EC2 Query API)

Describe a NAT gateway

- describe-nat-gateways (AWS CLI)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)
- DescribeNatGateways (Amazon EC2 Query API)

Tag a NAT gateway

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)
- CreateTags (Amazon EC2 Query API)

Delete a NAT gateway

- delete-nat-gateway (AWS CLI)
- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)
- DeleteNatGateway (Amazon EC2 Query API)

14.AWS CLI SDK?

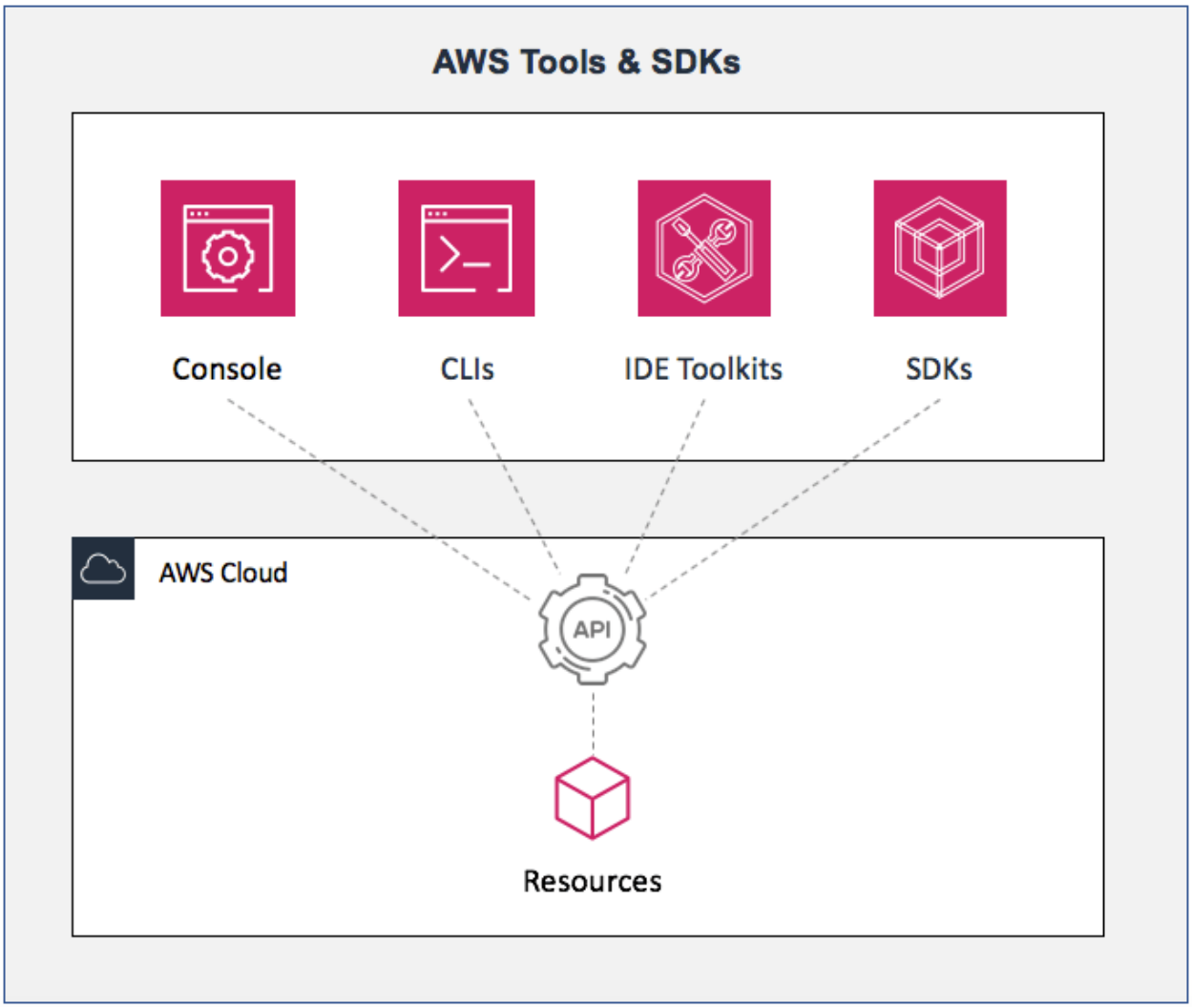
AWS CLI(Command Line Interface)

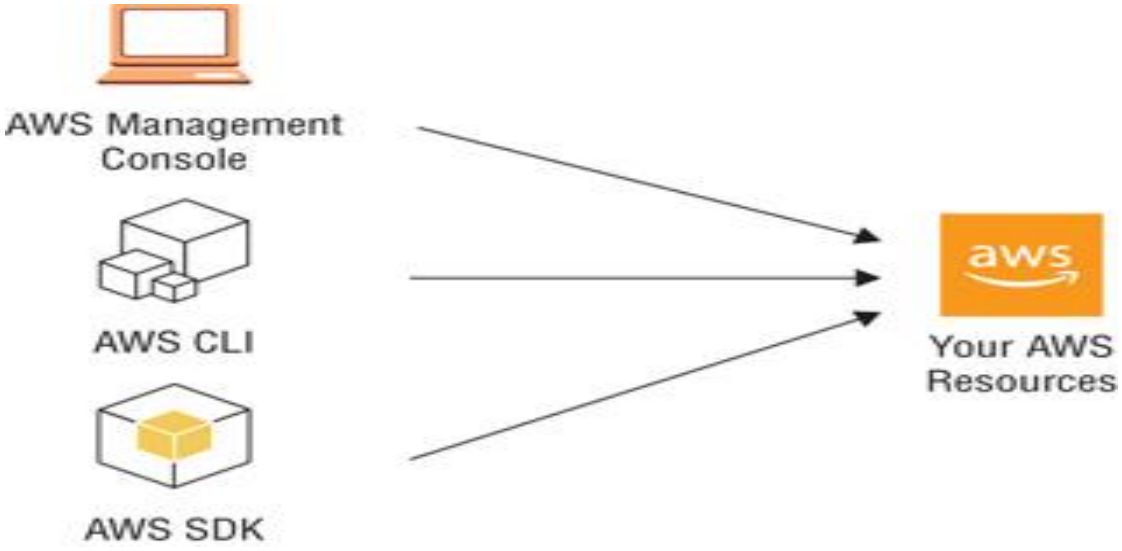
- The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.
- The AWS CLI v2 offers several new features including improved installers, new configuration options such as AWS Single Sign-On (SSO), and various interactive features.

AWS SDK(Software Development Kit)

- The AWS SDK for JavaScript is a collection of software tools for the creation of applications and libraries that use Amazon Web Services (AWS) resources

- The AWS SDK(software development kit) for browser-based development allows developers to access AWS from JavaScript code running directly in the browser.
- To use the AWS SDK for JavaScript, developers need only download the appropriate SDK – there are no other software requirements. However, access to the SDK environment requires an AWS account and access keys.





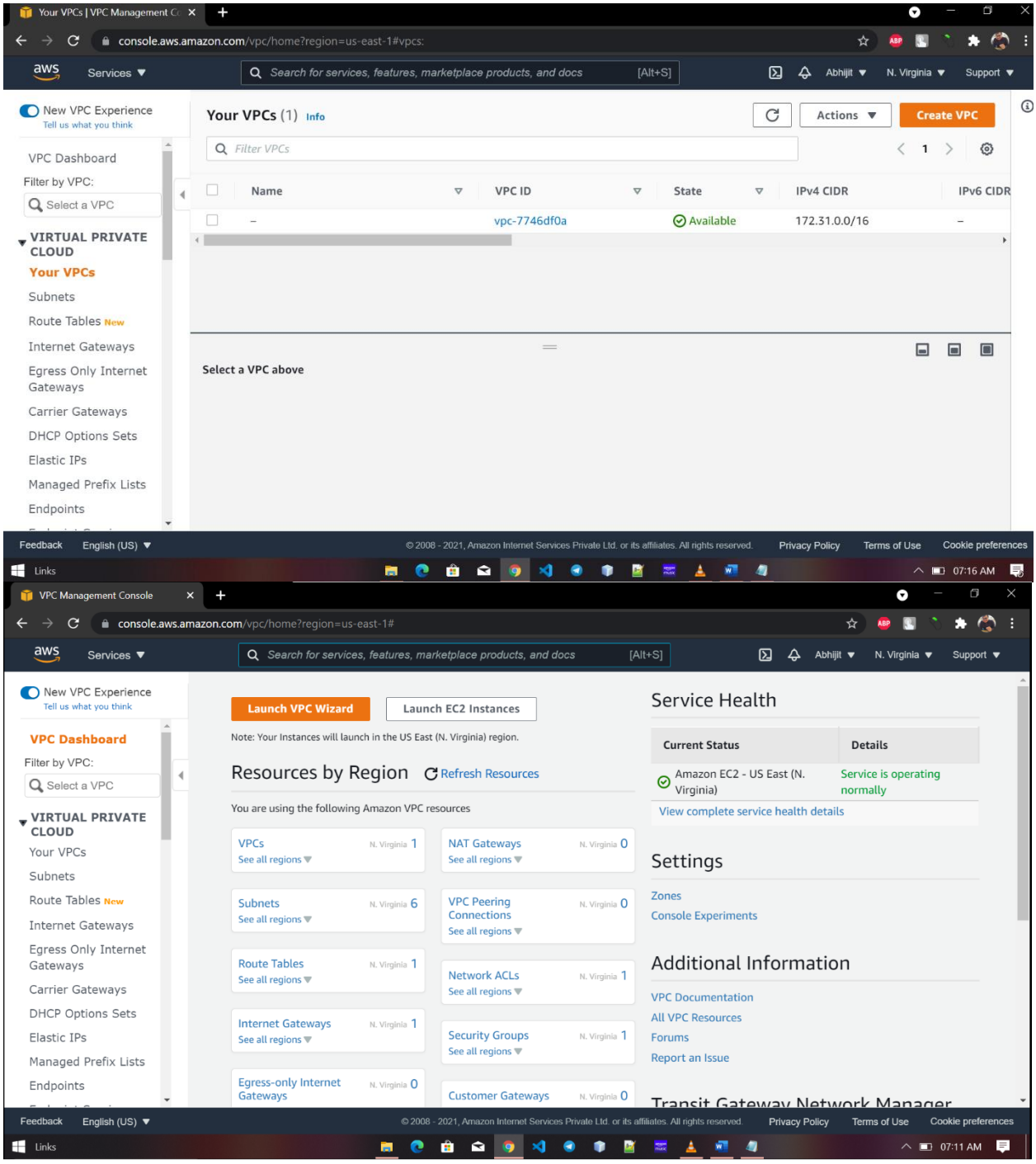
STEPS INVOLVED IN THE PROCESS:-

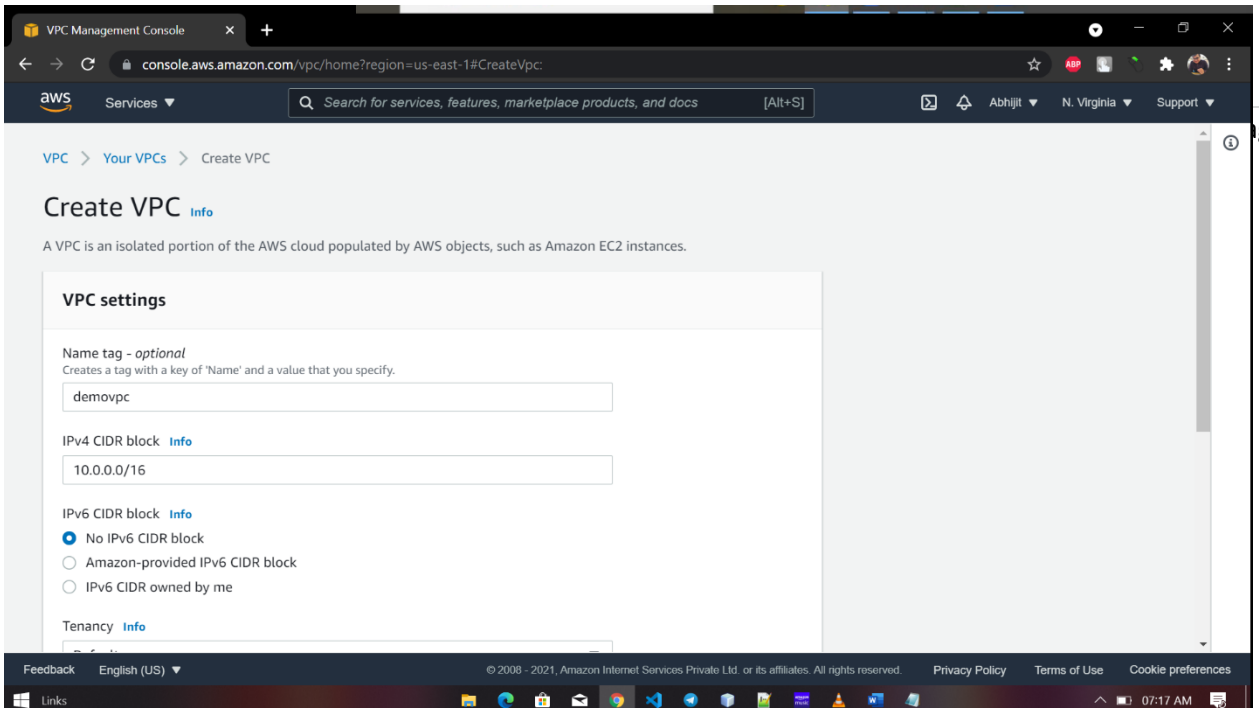
```
step 1:- login to vpc dashboard and create your vpc
ex:- 192.168.0.0/16

step 2:- create your own internet gateways and attach with
       your vpc

step 3:- click on subnets and create public and private subnets
         under your vpc

N.B :- public subnet will have internet connectivity

step 4:- create two different networks for public and private
         subnets

ex:- for public 192.168.1.0/24
             for private 192.168.2.0/24

step 5:- now create route tables for public and private subnets

step 6:- edit the route table,add subnets to your public and
         private routes

step 7:- for public route ,we need internet connectivity so add
        your internet gateways to public route

step 8:- create two security groups for public and private
subnets

step 9:- add one ec2 instances each on public and private subnets
         and check connectivity


adding nat gateway:-
------------------
NAT Gateway is a highly available AWS managed service that makes it
easy to connect to the Internet from instances within a private subnet
in an Amazon Virtual Private Cloud
```

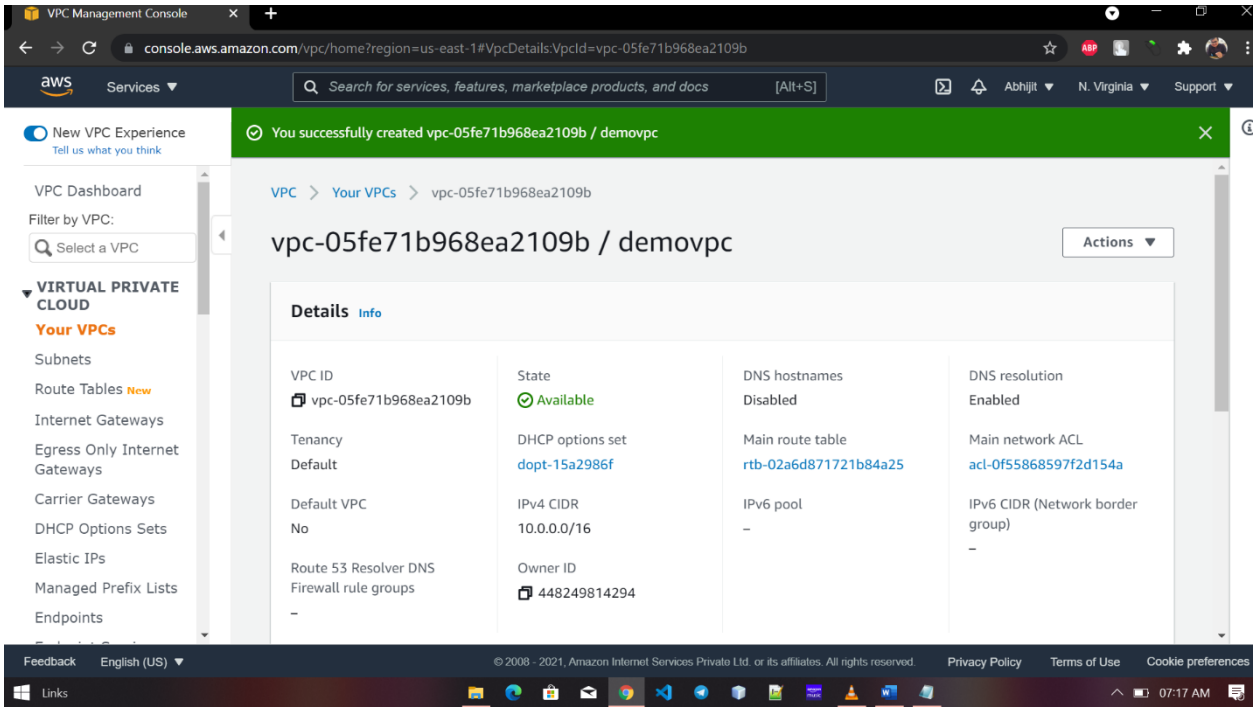
```
configurating nat gateway:-
---------------------------
step 1:- login to vpc console, under route table click on nat
        gateways

step 2:- add elastic ip to your nat gateway and attach with your
         public subnet

step 3:- now add your nat gateway to your private route


configuring NACL:-
------------------
step 1:- login to your vpc console , select nacl and create your
customize nacl under your vpc

step 2:- edit your nacl and add public subnet and test connectivity

step 3:- edit nacl inbound and outbound roles

creating vpc on using aws cli:-
-------------------------------
step 1:- create a user profile on iam and add as an administrator

step 2:- launch an amazon linux instance, type aws configure

step 3:- add your created users credenticals(access key and secret
access key), and setup your region

step 4:- create customed vpc
         --------------------
         type the below commands to create your customed vpc

         aws ec2 create-vpc --cidr-block 10.0.0.0/16 --region

         us-east-2 (select your network and region code)

step 5:- create a public subnet:-
         ------------------------
         aws ec2 create-subnet --availability-zone us-east-1a --vpc-id
vpc00ffd55cba38412c2 --cidr-block 10.0.1.0/24 --region us-east-1


step 6:- create an internet gateway:-
         ----------------------------
         aws ec2 create-internet-gateway --vpc-id vpc00ffd55cba38412c2


step 7:- attach an internet gateway:-
         ----------------------------
         aws ec2 attach-internet-gateway --internet-gateway-id igw-
04eaf702a0a55b393 --         vpc-id vpc-00ffd55cba38412c2 --region us-
east-1
```

THE SCREENSHOTS OF THE STEPS INVOLVED:

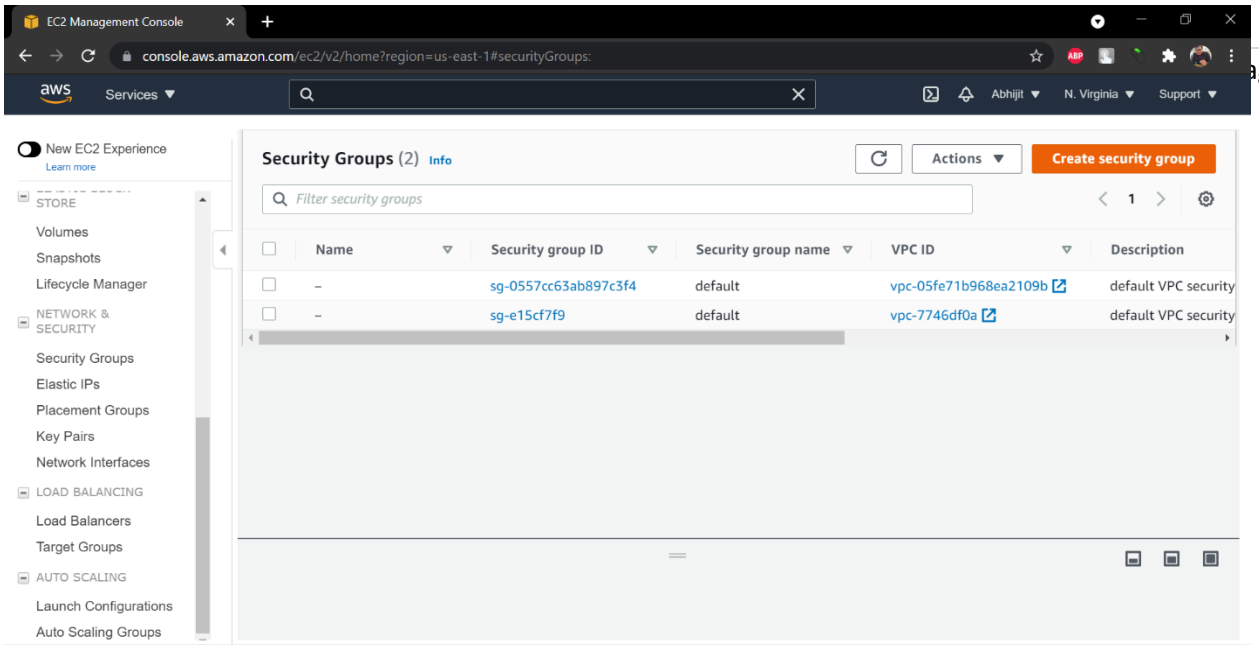
STEP 2-creation of vpc (step 1)

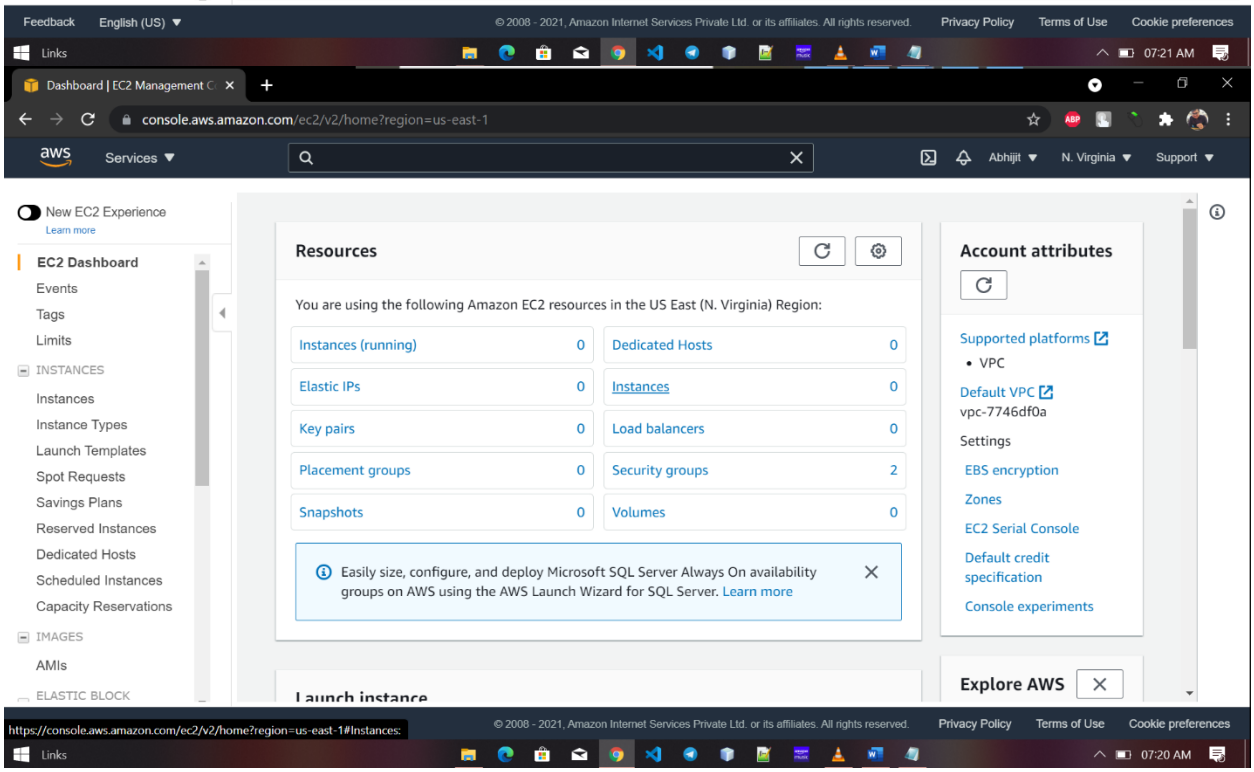


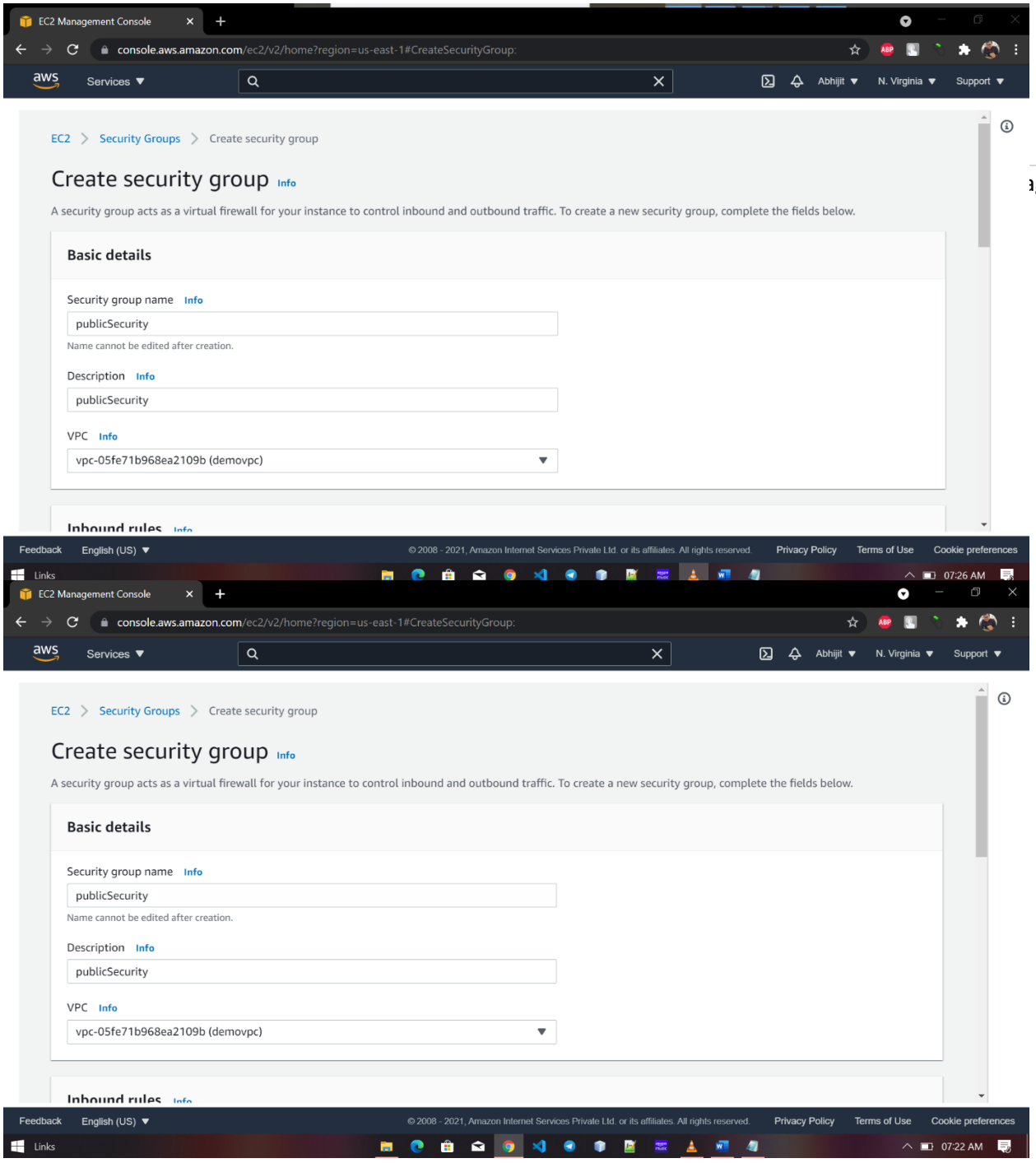

VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpc:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
VPC > Your VPCs > Create VPC
Create VPC Info
A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.
VPC settings
Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
demovpc
IPv4 CIDR block Info
10.0.0.0/16
IPv6 CIDR block Info
No IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me
Tenancy Info
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:17 AM

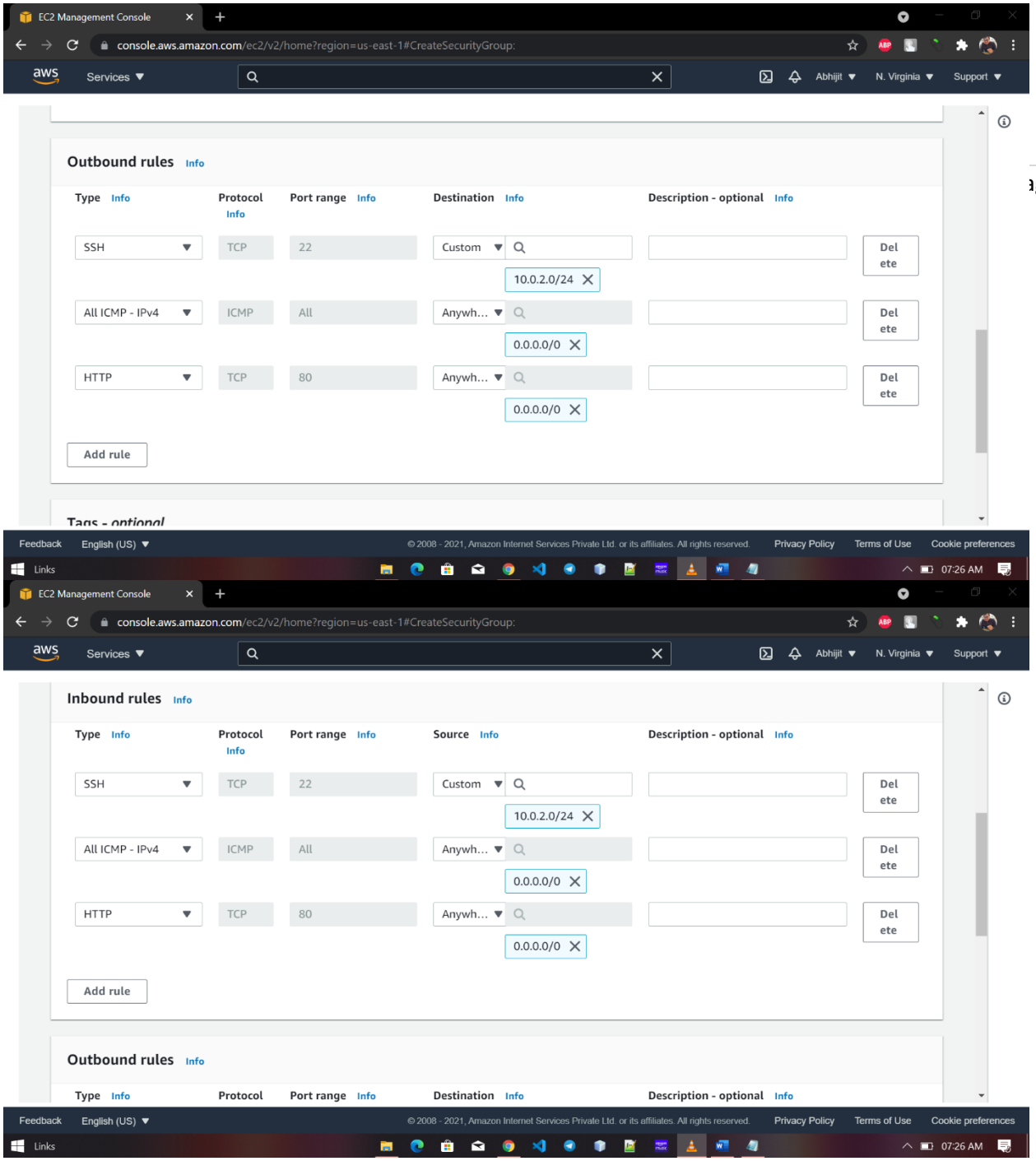

VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#VpcDetails:VpcId=vpc-05fe71b968ea2109b
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New VPC Experience
Tell us what you think
You successfully created vpc-05fe71b968ea2109b / demovpc
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
VPC > Your VPCs > vpc-05fe71b968ea2109b
vpc-05fe71b968ea2109b / demovpc
Actions
Details Info
VPC ID
vpc-05fe71b968ea2109b
State
Available
DNS hostnames
Disabled
DNS resolution
Enabled
Tenancy
Default
DHCP options set
dopt-15a2986f
Main route table
rtb-02a6d871721b84a25
Main network ACL
acl-0f55868597f2d154a
Default VPC
No
IPv4 CIDR
10.0.0.0/16
IPv6 pool
-
IPv6 CIDR (Network border group)
-
Route 53 Resolver DNS Firewall rule groups
-
Owner ID
448249814294
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:17 AM

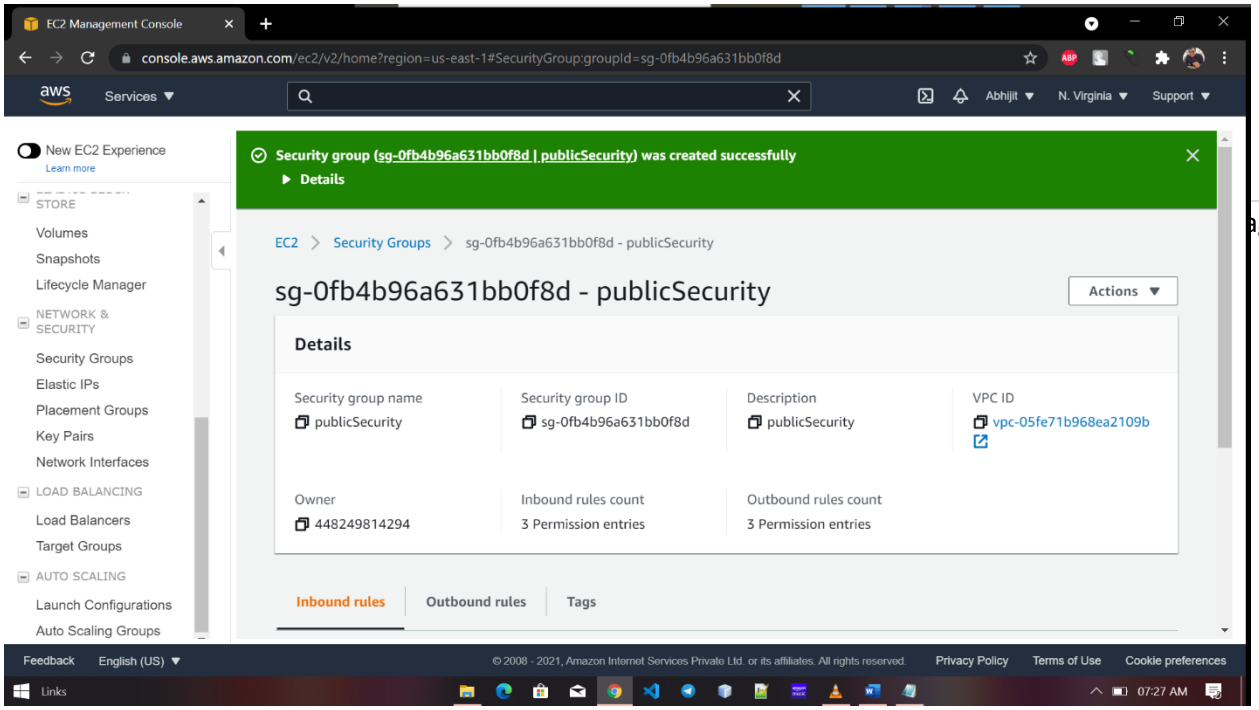
STEP 2-creation of security groups public and private (step 2)

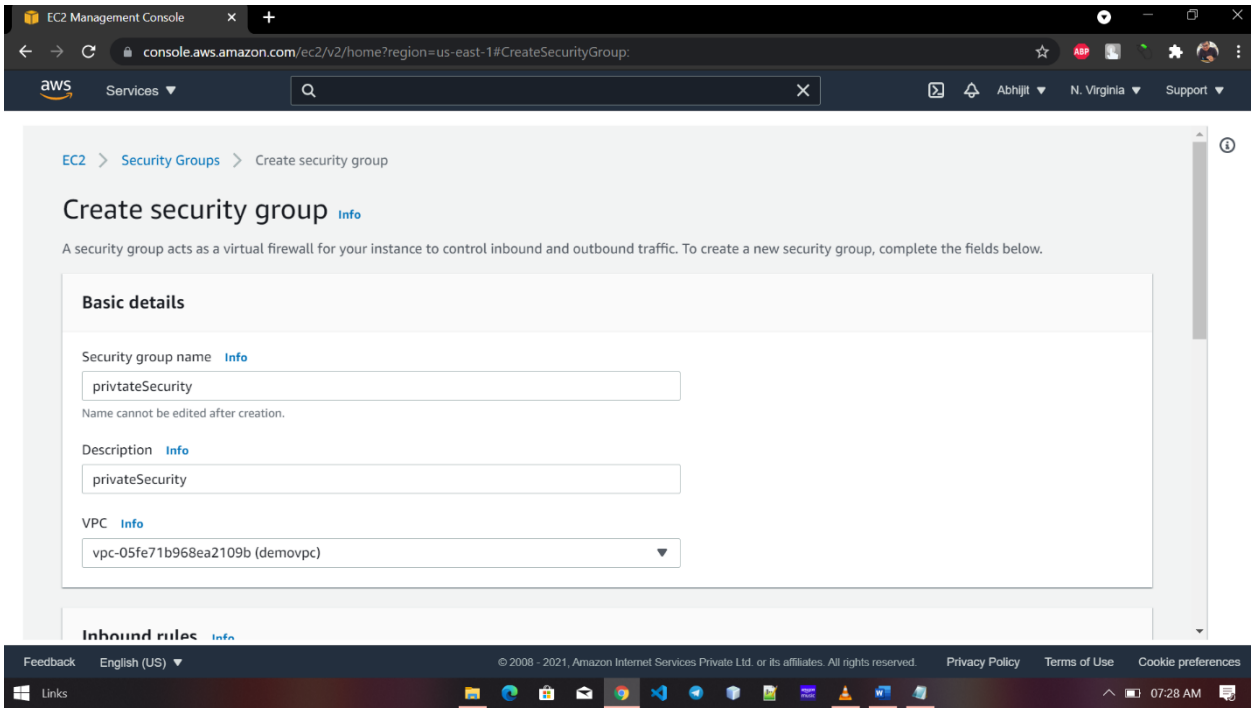


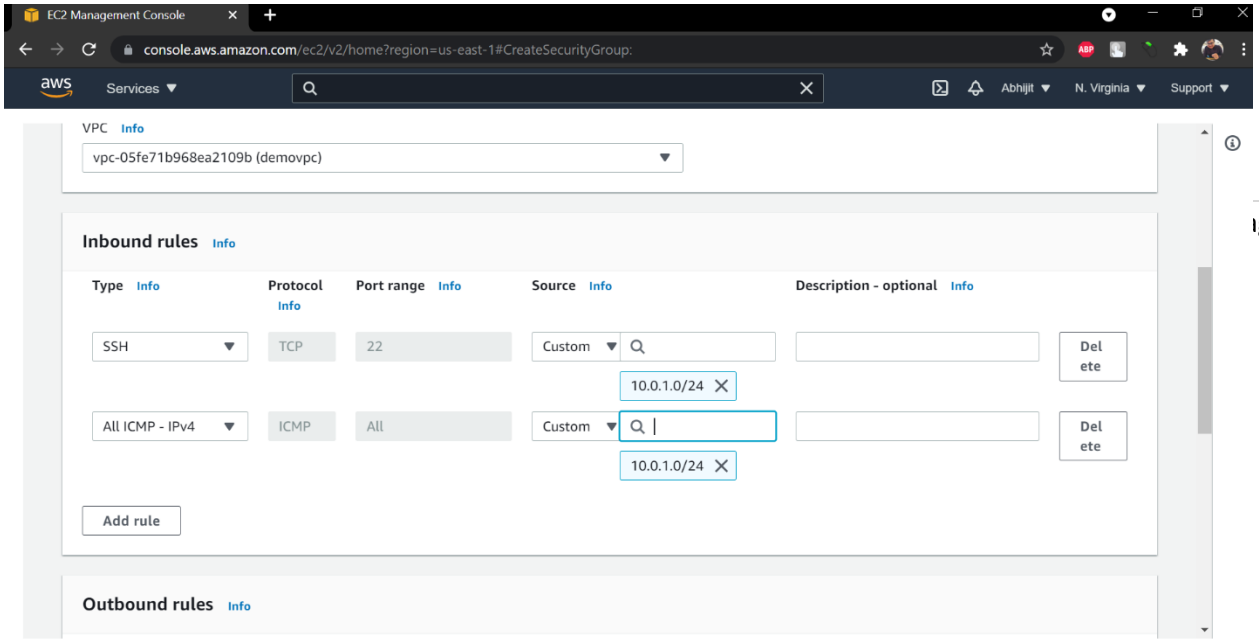


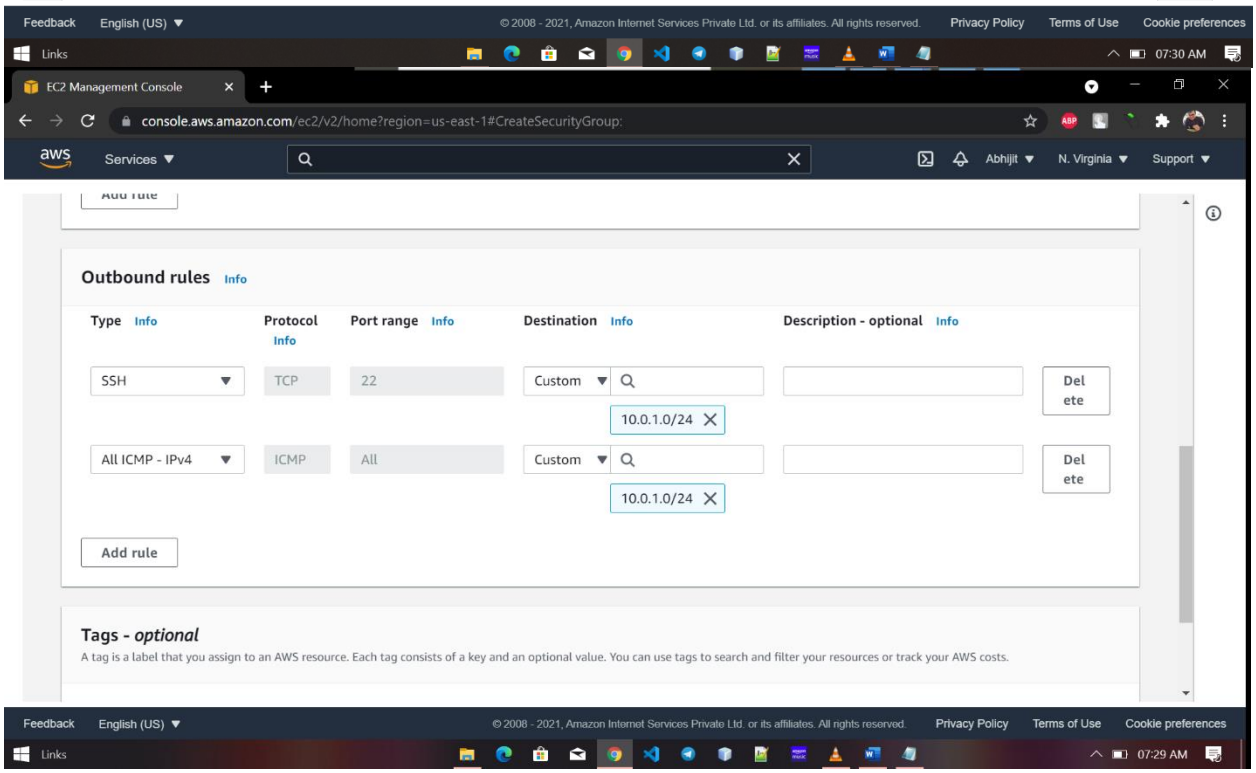

EC2 Management Console
console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateSecurityGroup:
aws
Services
Abhijit
N. Virginia
Support
EC2 > Security Groups > Create security group
Create security group Info
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.
Basic details
Security group name Info
publicSecurity
Name cannot be edited after creation.
Description Info
publicSecurity
VPC Info
vpc-05fe71b968ea2109b (demovpc)
Inbound rules Info
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:26 AM
EC2 Management Console
console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateSecurityGroup:
aws
Services
Abhijit
N. Virginia
Support
EC2 > Security Groups > Create security group
Create security group Info
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.
Basic details
Security group name Info
publicSecurity
Name cannot be edited after creation.
Description Info
publicSecurity
VPC Info
vpc-05fe71b968ea2109b (demovpc)
Inbound rules Info
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:22 AM

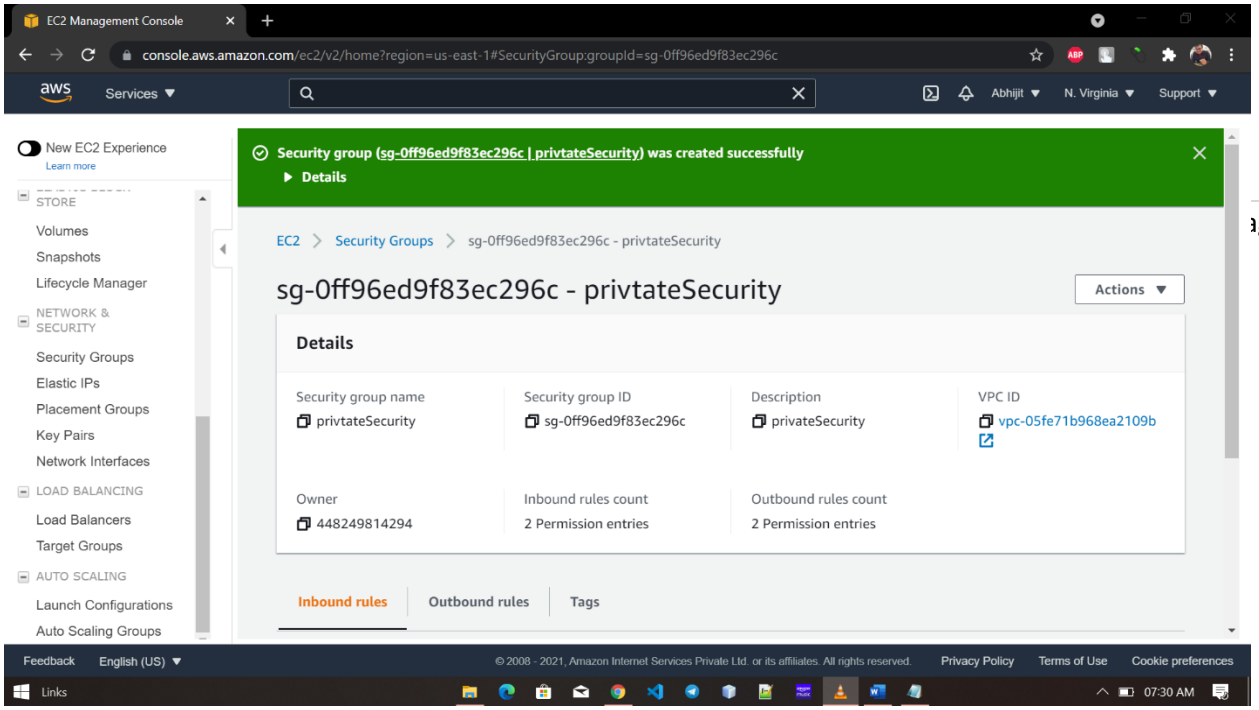

EC2 Management Console
console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateSecurityGroup:
aws
Services
Abhijit
N. Virginia
Support
Outbound rules Info
Type Info
Protocol Info
Port range Info
Destination Info
Description - optional Info
SSH
TCP
22
Custom
10.0.2.0/24
Delete
All ICMP - IPv4
ICMP
All
Anywh...
0.0.0.0/0
Delete
HTTP
TCP
80
Anywh...
0.0.0.0/0
Delete
Add rule
Tags - optional
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:26 AM
EC2 Management Console
console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateSecurityGroup:
aws
Services
Abhijit
N. Virginia
Support
Inbound rules Info
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
SSH
TCP
22
Custom
10.0.2.0/24
Delete
All ICMP - IPv4
ICMP
All
Anywh...
0.0.0.0/0
Delete
HTTP
TCP
80
Anywh...
0.0.0.0/0
Delete
Add rule
Outbound rules Info
Type Info
Protocol
Port range Info
Destination Info
Description - optional Info
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:26 AM


EC2 Management Console
console.aws.amazon.com/ec2/v2/home?region=us-east-1#SecurityGroup:groupId=sg-0fb4b96a631bb0f8d
Services
Abhijit
N. Virginia
Support
New EC2 Experience
Learn more
Volumes
Snapshots
Lifecycle Manager
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
AUTO SCALING
Launch Configurations
Auto Scaling Groups
Security group (sg-0fb4b96a631bb0f8d | publicSecurity) was created successfully
Details
EC2 > Security Groups > sg-0fb4b96a631bb0f8d - publicSecurity
sg-0fb4b96a631bb0f8d - publicSecurity
Actions
Details
Security group name
publicSecurity
Security group ID
sg-0fb4b96a631bb0f8d
Description
publicSecurity
VPC ID
vpc-05fe71b968ea2109b
Owner
448249814294
Inbound rules count
3 Permission entries
Outbound rules count
3 Permission entries
Inbound rules
Outbound rules
Tags
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:27 AM

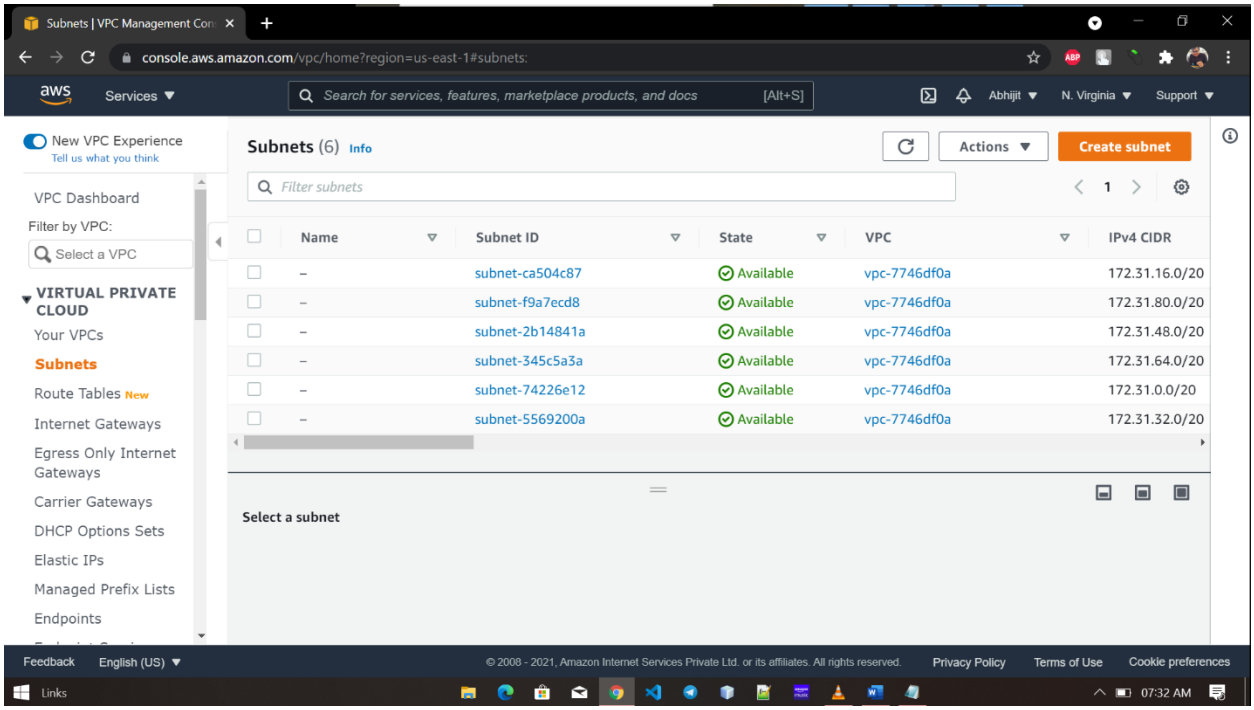

EC2 Management Console
console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateSecurityGroup:
Services
Abhijit
N. Virginia
Support
EC2 > Security Groups > Create security group
Create security group
Info
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.
Basic details
Security group name
Info
privtateSecurity
Name cannot be edited after creation.
Description
Info
privateSecurity
VPC
Info
vpc-05fe71b968ea2109b (demovpc)
Inbound rules
Info
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:28 AM

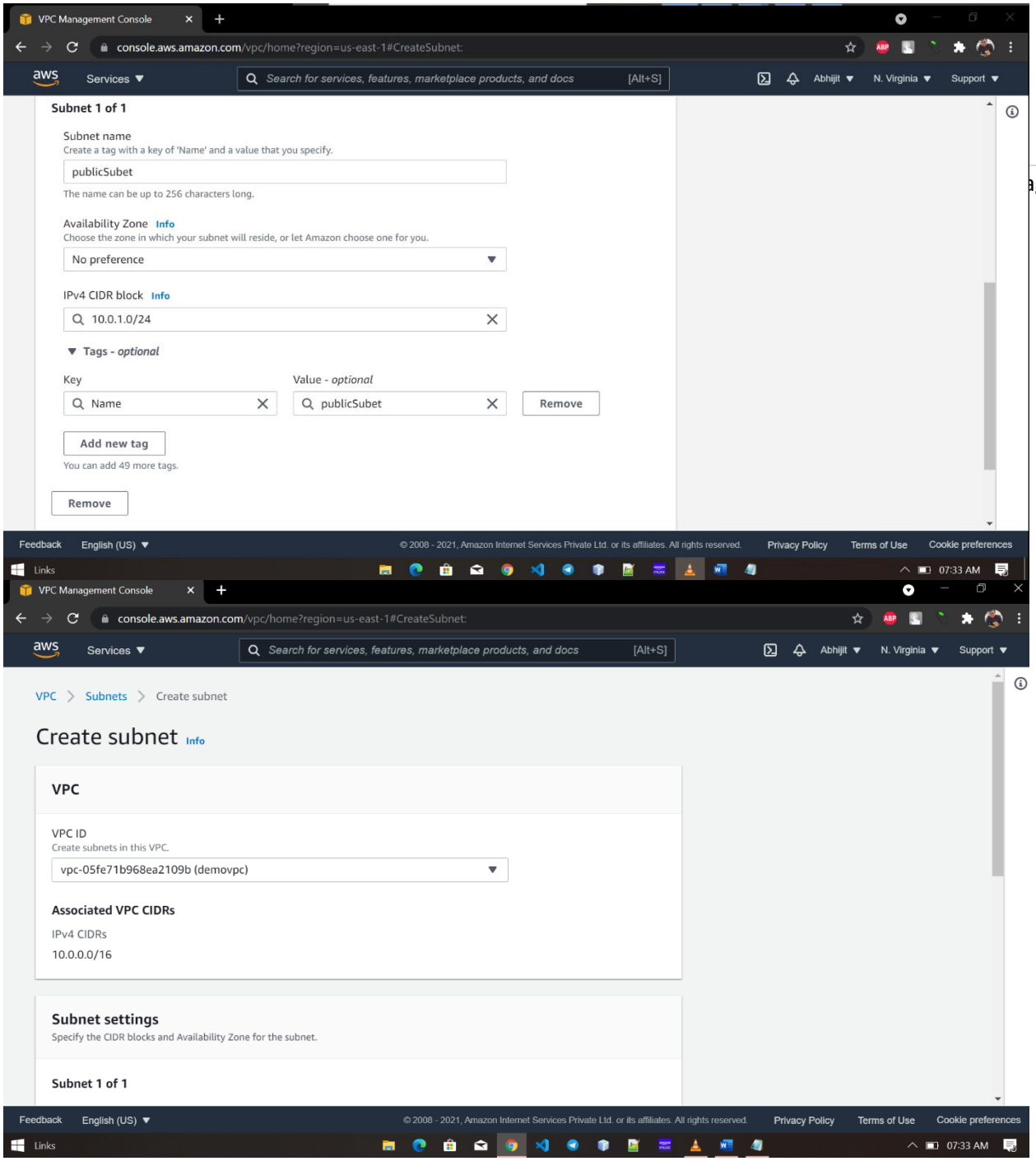

EC2 Management Console
console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateSecurityGroup:
aws
Services
Abhijit
N. Virginia
Support
VPC Info
vpc-05fe71b968ea2109b (demovpc)
Inbound rules Info
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
SSH
TCP
22
Custom
10.0.1.0/24
Delete
All ICMP - IPv4
ICMP
All
Custom
10.0.1.0/24
Delete
Add rule
Outbound rules Info

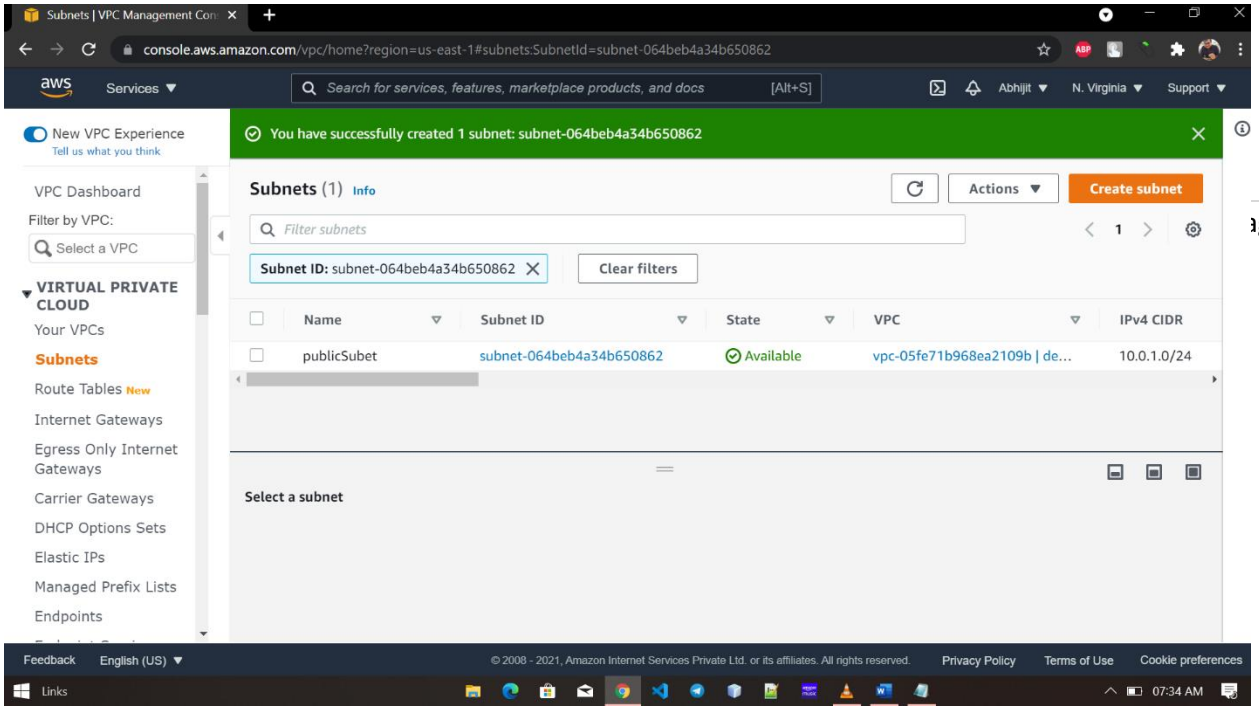

Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:30 AM
EC2 Management Console
console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateSecurityGroup:
aws
Services
Abhijit
N. Virginia
Support
Outbound rules Info
Type Info
Protocol Info
Port range Info
Destination Info
Description - optional Info
SSH
TCP
22
Custom
10.0.1.0/24
Delete
All ICMP - IPv4
ICMP
All
Custom
10.0.1.0/24
Delete
Add rule
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.
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:29 AM

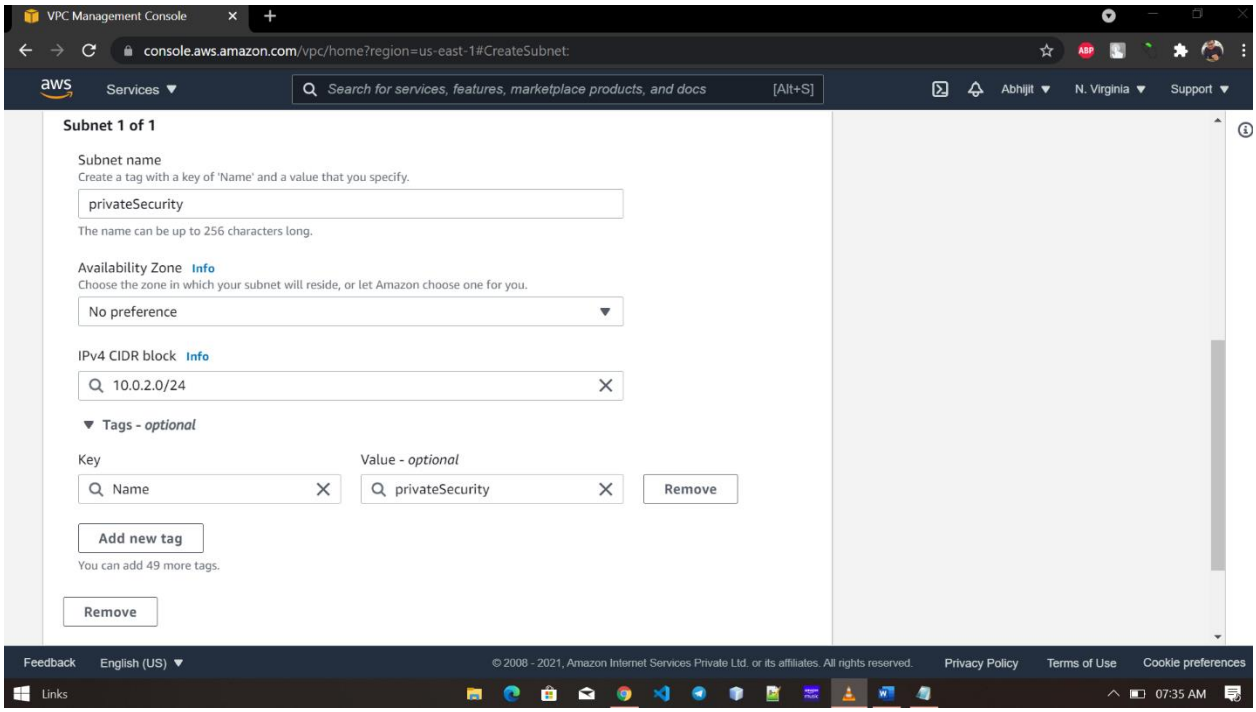


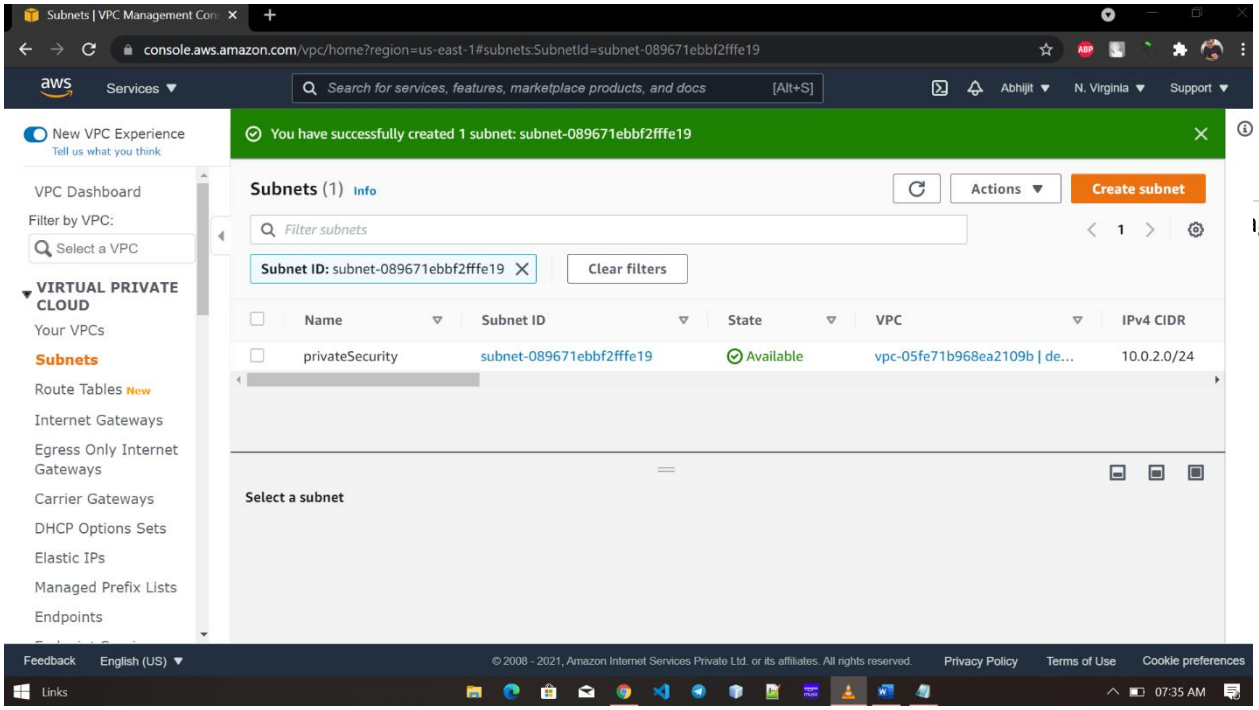
STEP 3:-creation of subnet- public and private (step 3)



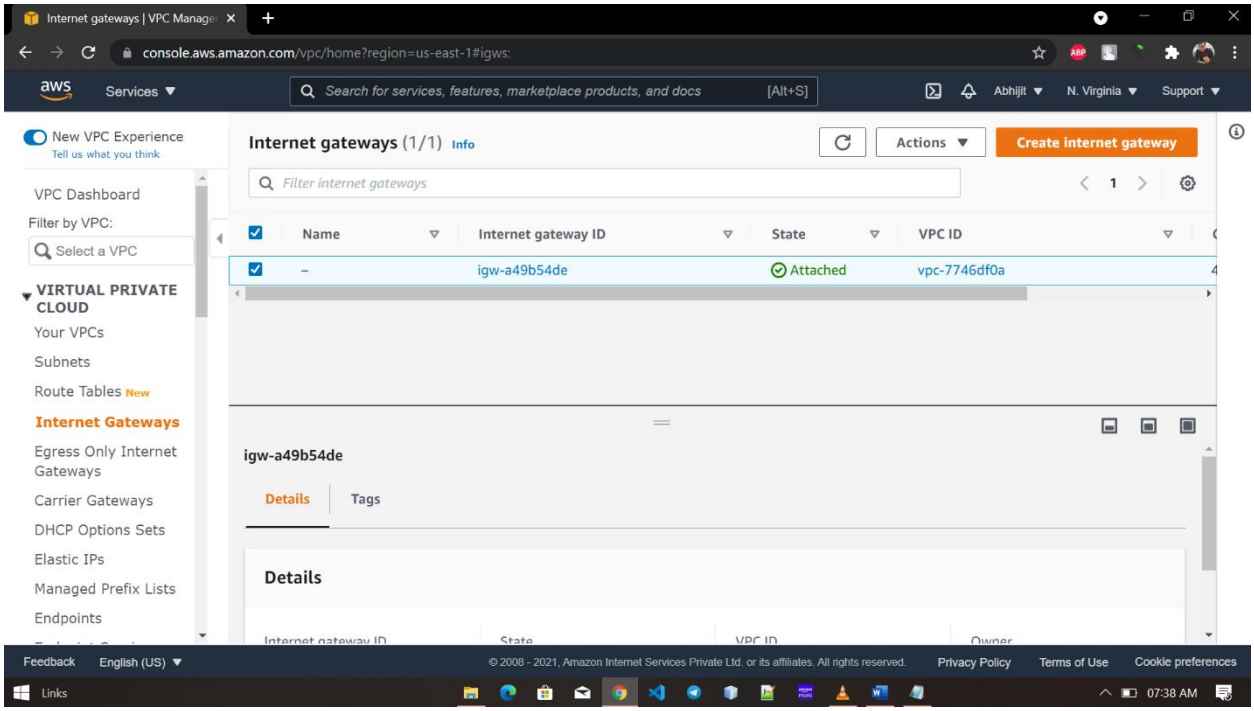

VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#CreateSubnet:
aws
Services
Search for services, features, marketplace products, and docs
[Alt+S]
Abhijit
N. Virginia
Support
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
publicSubet
The 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.
No preference
IPv4 CIDR block Info
10.0.1.0/24
Tags - optional
Key
Value - optional
Name
publicSubet
Remove
Add new tag
You can add 49 more tags.
Remove
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:33 AM
VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#CreateSubnet:
aws
Services
Search for services, features, marketplace products, and docs
[Alt+S]
Abhijit
N. Virginia
Support
VPC
Subnets
Create subnet
Create subnet Info
VPC
VPC ID
Create subnets in this VPC.
vpc-05fe71b968ea2109b (demovpc)
Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 1
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:33 AM

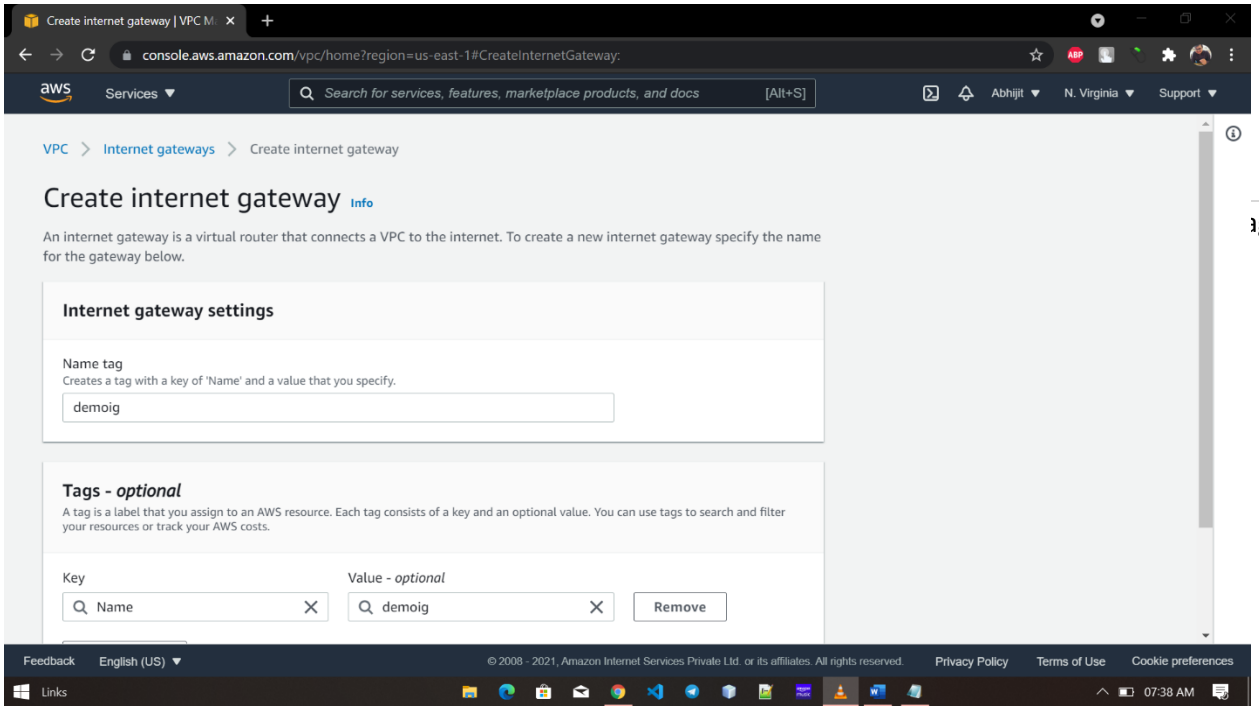

Subnets | VPC Management Con
console.aws.amazon.com/vpc/home?region=us-east-1#subnets:SubnetId=subnet-064beb4a34b650862
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New VPC Experience
Tell us what you think
You have successfully created 1 subnet: subnet-064beb4a34b650862
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Subnets (1) Info
Actions
Create subnet
Filter subnets
Subnet ID: subnet-064beb4a34b650862
Clear filters
Name
Subnet ID
State
VPC
IPv4 CIDR
publicSubet
subnet-064beb4a34b650862
Available
vpc-05fe71b968ea2109b | de...
10.0.1.0/24
Select a subnet
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:34 AM

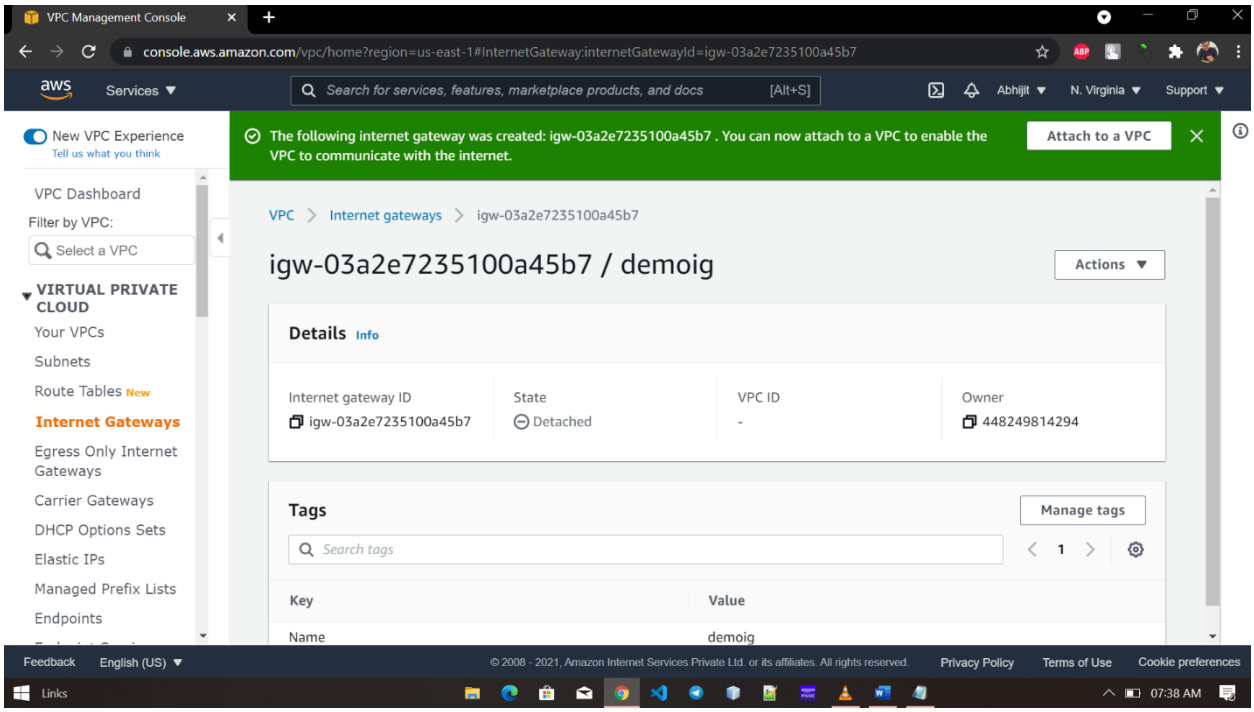

VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#CreateSubnet:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
privateSecurity
The 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.
No preference
IPv4 CIDR block Info
10.0.2.0/24
Tags - optional
Key
Value - optional
Name
privateSecurity
Remove
Add new tag
You can add 49 more tags.
Remove
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:35 AM

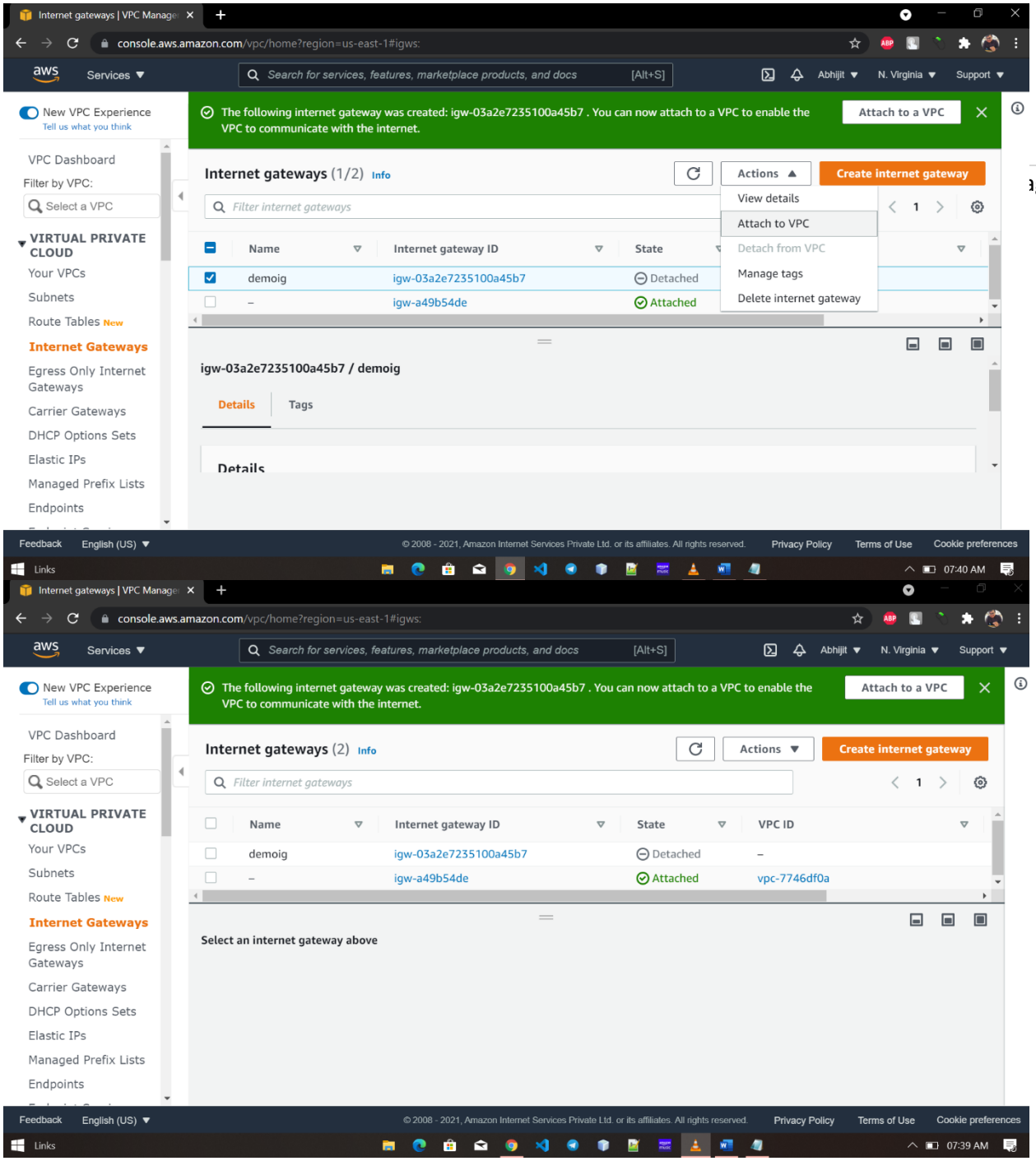


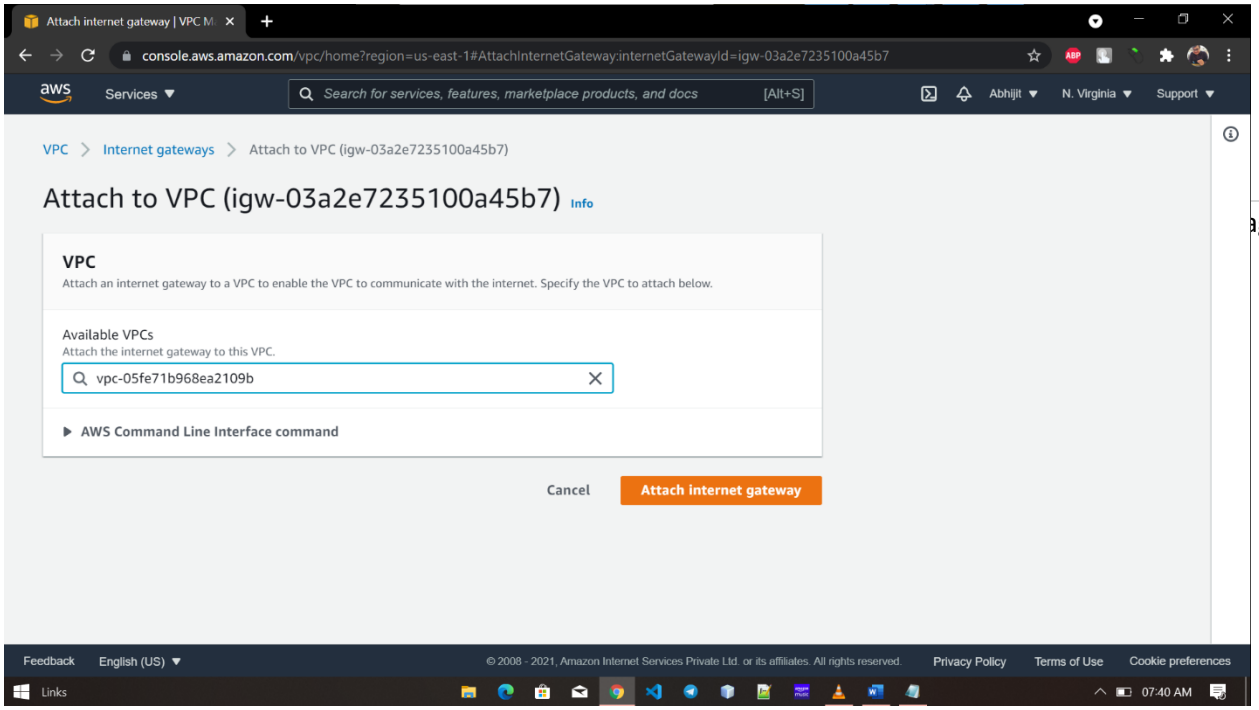
STEP 4:-creation of internet gateway and attaching it (step 4)

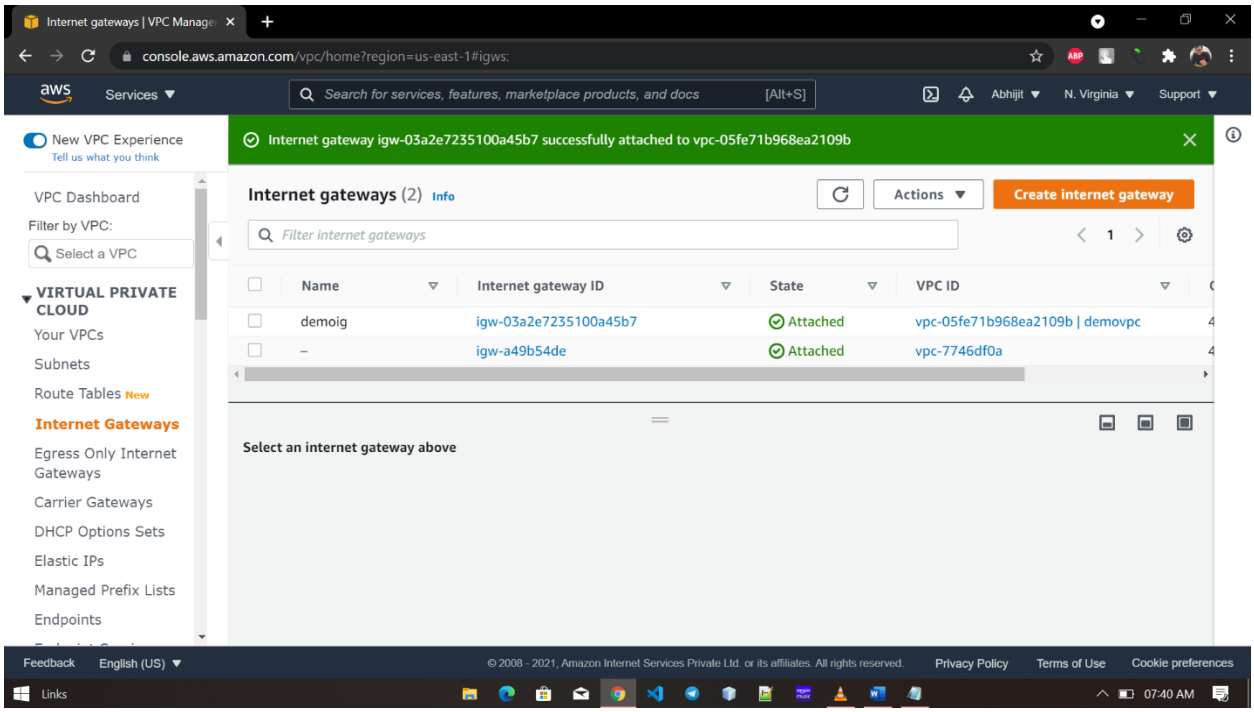



Create internet gateway | VPC M
console.aws.amazon.com/vpc/home?region=us-east-1#CreateInternetGateway:
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
VPC > Internet gateways > Create internet gateway
Create internet gateway Info
An internet 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.
demoig
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
demoig
Remove
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:38 AM

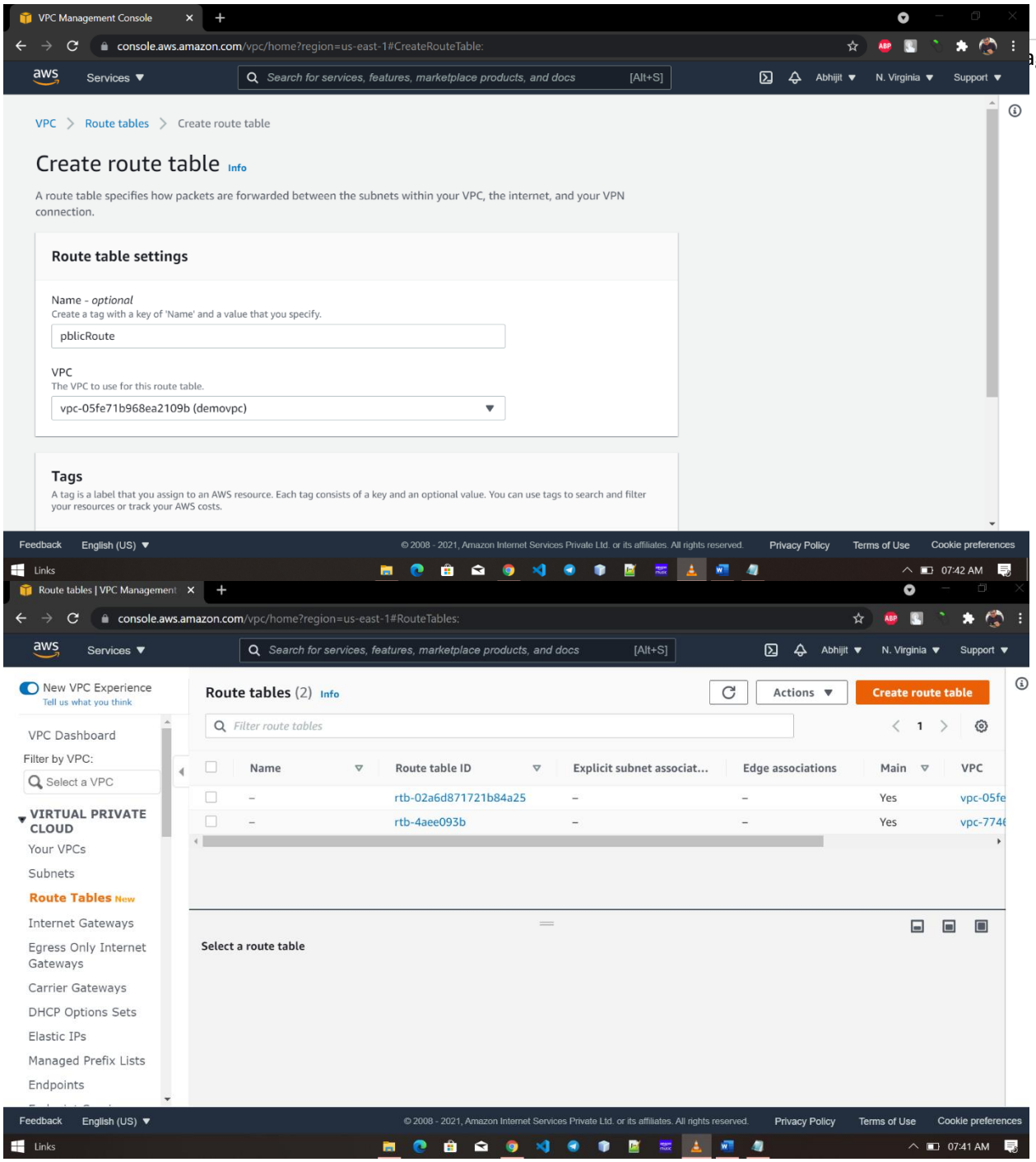

VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#InternetGateway:internetGatewayId=igw-03a2e7235100a45b7
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New VPC Experience
Tell us what you think
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
The following internet gateway was created: igw-03a2e7235100a45b7 . You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
VPC > Internet gateways > igw-03a2e7235100a45b7
igw-03a2e7235100a45b7 / demoig
Actions
Details Info
Internet gateway ID
igw-03a2e7235100a45b7
State
Detached
VPC ID
-
Owner
448249814294
Tags
Manage tags
Search tags
1
Key
Value
Name
demoig
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:38 AM

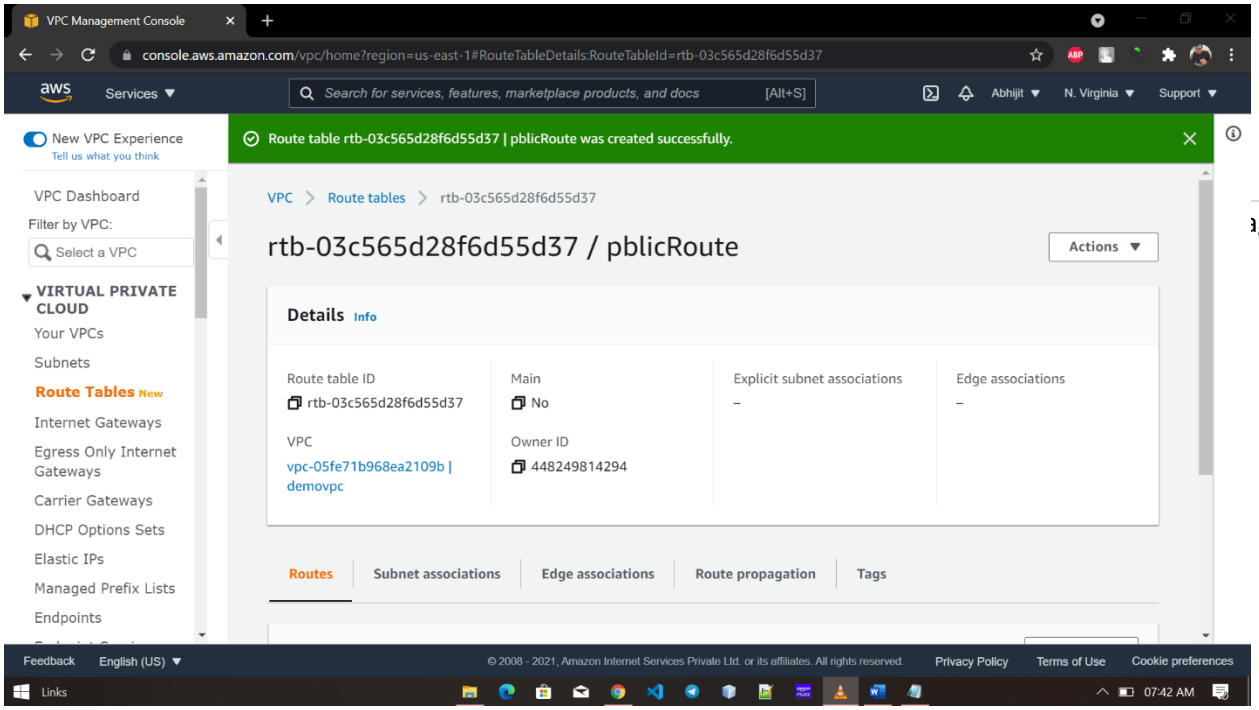

Internet gateways | VPC Manage
console.aws.amazon.com/vpc/home?region=us-east-1#igws:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New VPC Experience
Tell us what you think
The following internet gateway was created: igw-03a2e7235100a45b7 . You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Internet gateways (1/2) Info
Actions
Create internet gateway
Filter internet gateways
View details
Attach to VPC
Detach from VPC
Manage tags
Delete internet gateway
Name
Internet gateway ID
State
demoig
igw-03a2e7235100a45b7
Detached
–
igw-a49b54de
Attached
igw-03a2e7235100a45b7 / demoig
Details
Tags
Details
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:40 AM
Internet gateways | VPC Manage
console.aws.amazon.com/vpc/home?region=us-east-1#igws:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New VPC Experience
Tell us what you think
The following internet gateway was created: igw-03a2e7235100a45b7 . You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Internet gateways (2) Info
Actions
Create internet gateway
Filter internet gateways
Name
Internet gateway ID
State
VPC ID
demoig
igw-03a2e7235100a45b7
Detached
–
–
igw-a49b54de
Attached
vpc-7746df0a
Select an internet gateway above
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:39 AM

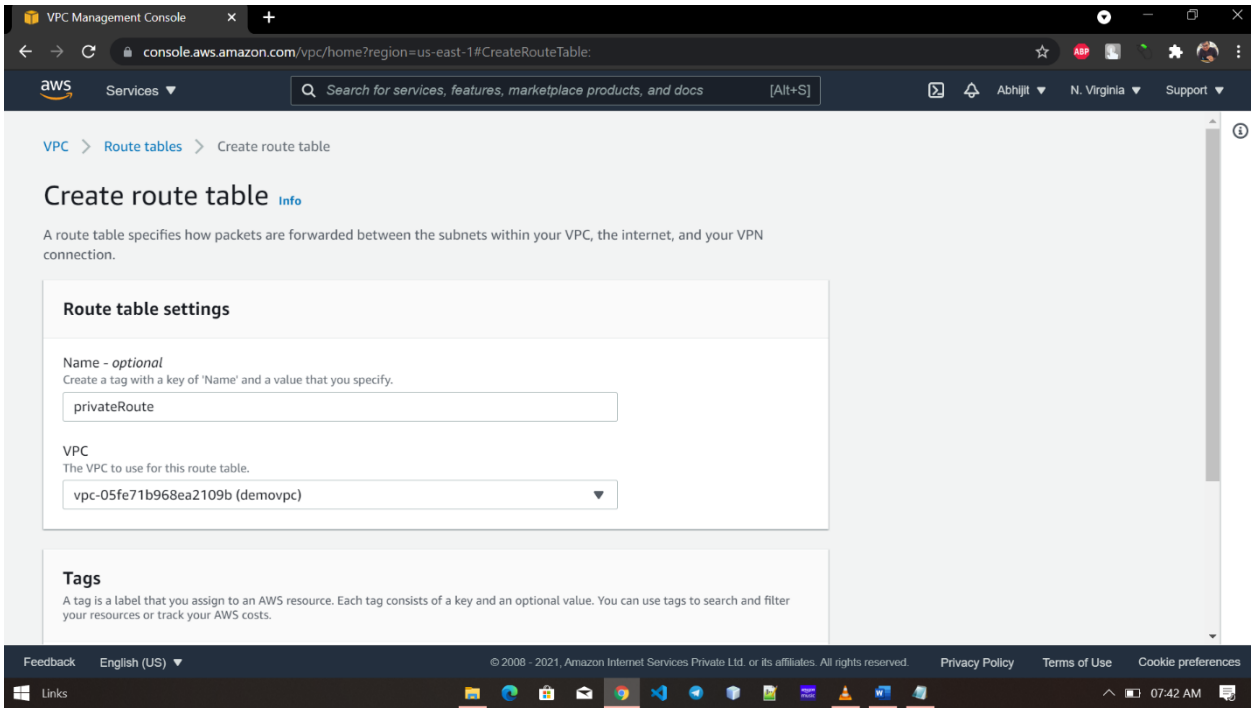

Attach internet gateway | VPC M
console.aws.amazon.com/vpc/home?region=us-east-1#AttachInternetGateway:internetGatewayId=igw-03a2e7235100a45b7
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
VPC > Internet gateways > Attach to VPC (igw-03a2e7235100a45b7)
Attach to VPC (igw-03a2e7235100a45b7) 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-05fe71b968ea2109b
AWS Command Line Interface command
Cancel
Attach internet gateway
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:40 AM

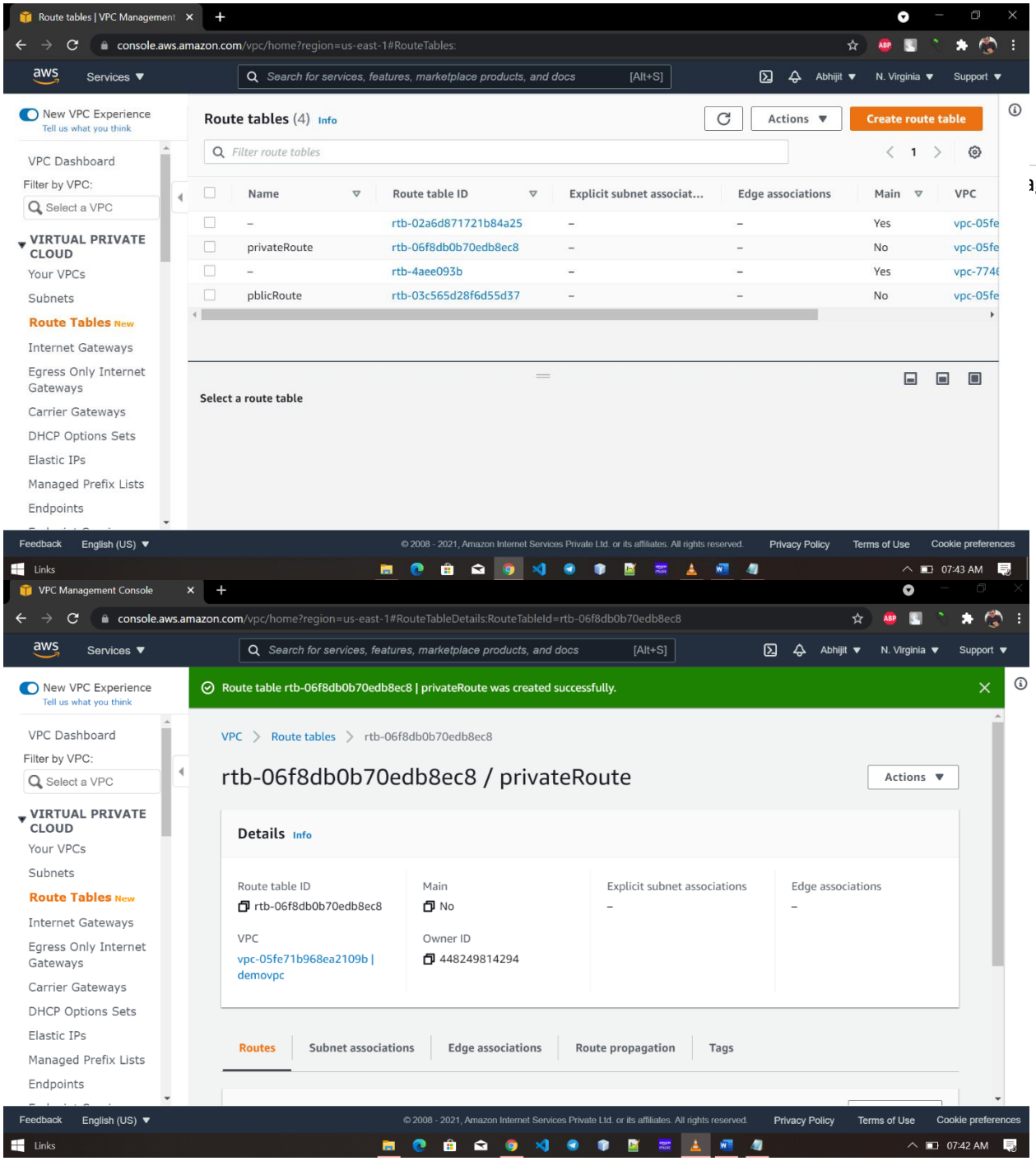

Internet gateways | VPC Manage
console.aws.amazon.com/vpc/home?region=us-east-1#igws:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New VPC Experience
Tell us what you think
Internet gateway igw-03a2e7235100a45b7 successfully attached to vpc-05fe71b968ea2109b
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Internet gateways (2) Info
Actions
Create internet gateway
Filter internet gateways
Name
Internet gateway ID
State
VPC ID
demoig
igw-03a2e7235100a45b7
Attached
vpc-05fe71b968ea2109b | demovpc
–
igw-a49b54de
Attached
vpc-7746df0a
Select an internet gateway above
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:40 AM

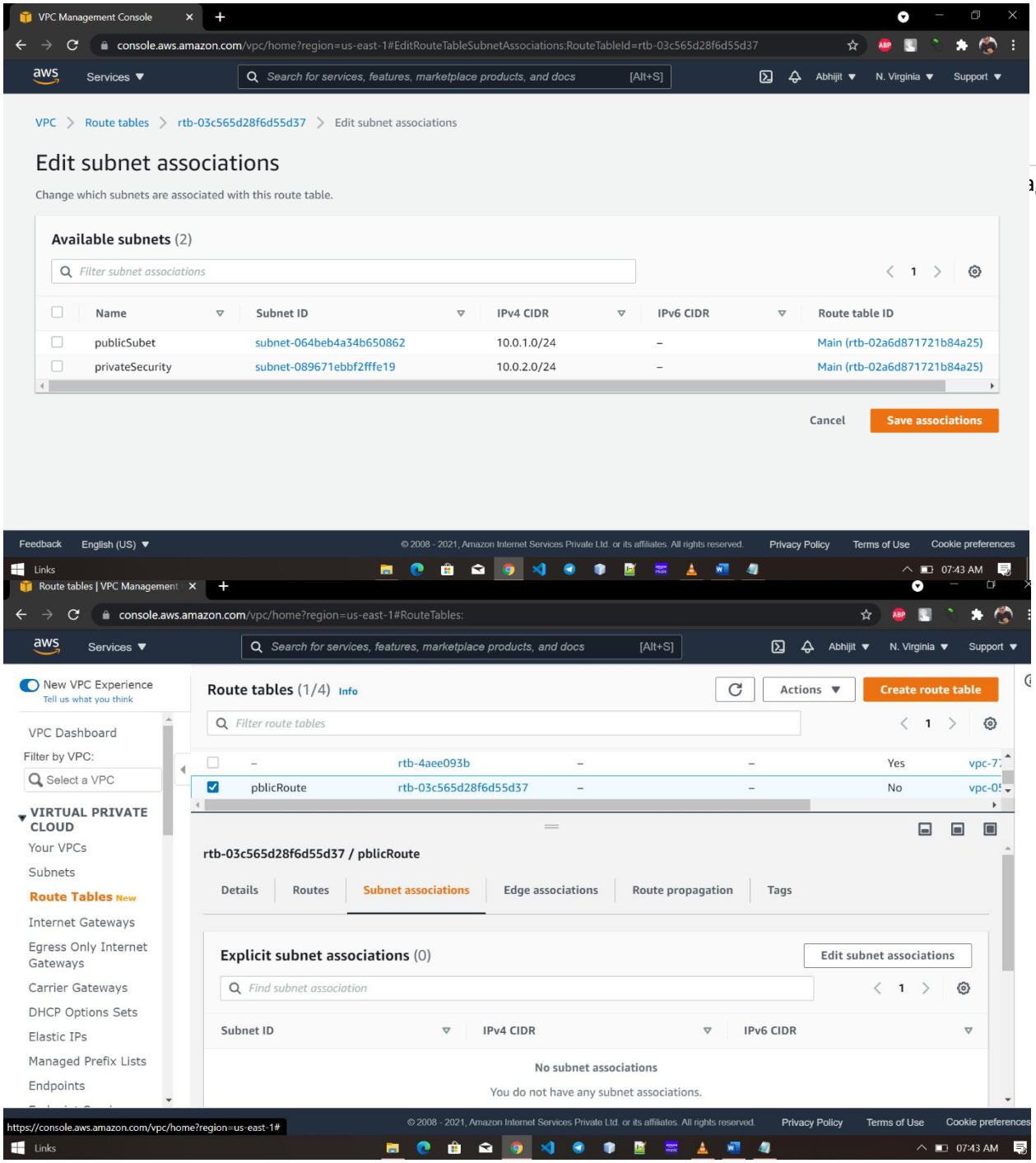
STEP 5:-creation of route table and connecting to respective networks (step 5)

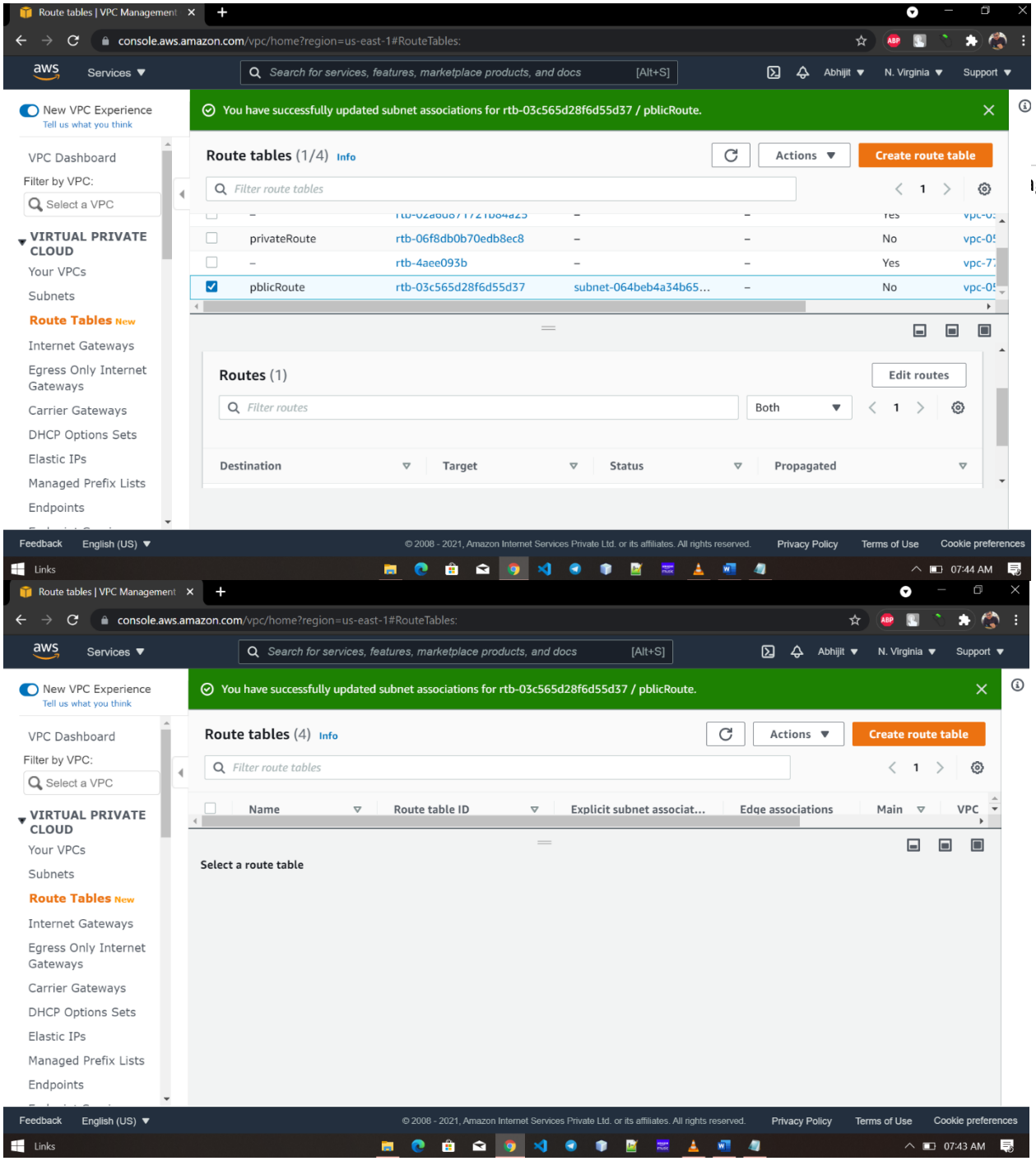


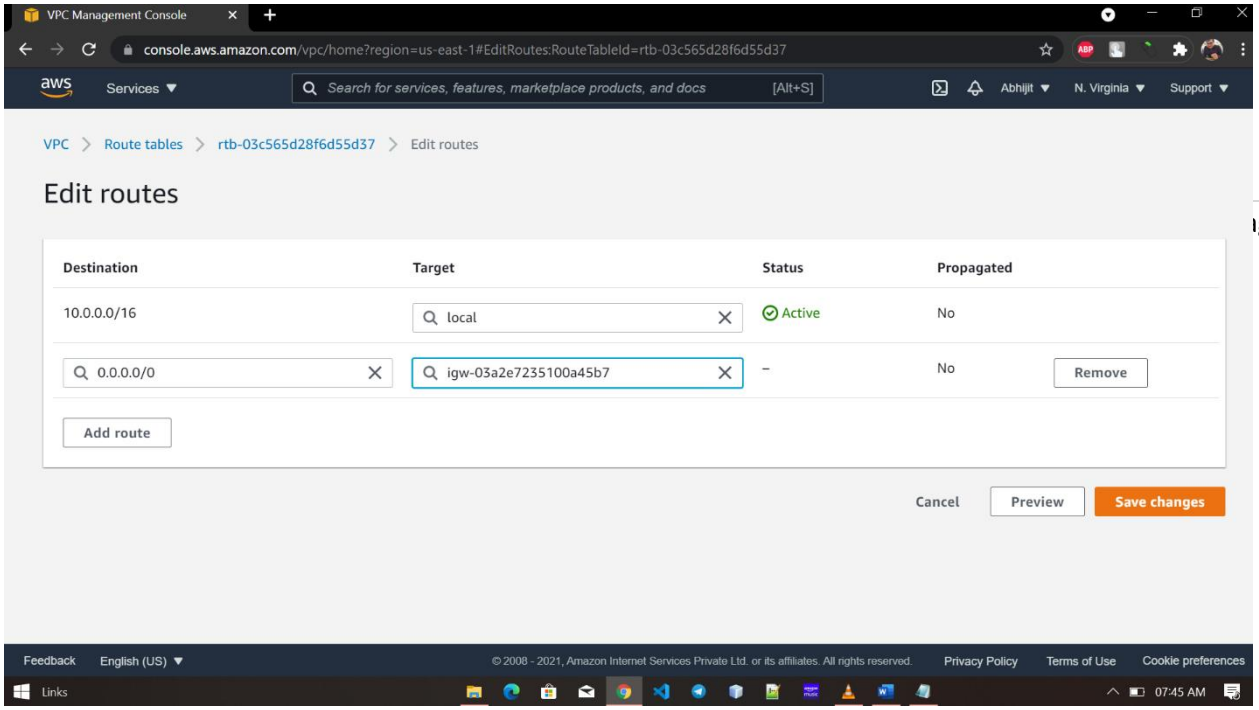

VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-03c565d28f6d55d37
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New VPC Experience
Tell us what you think
Route table rtb-03c565d28f6d55d37 | pblicRoute was created successfully.
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
VPC > Route tables > rtb-03c565d28f6d55d37
rtb-03c565d28f6d55d37 / pblicRoute
Actions
Details Info
Route table ID
rtb-03c565d28f6d55d37
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-05fe71b968ea2109b | demovpc
Owner ID
448249814294
Routes
Subnet associations
Edge associations
Route propagation
Tags
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:42 AM

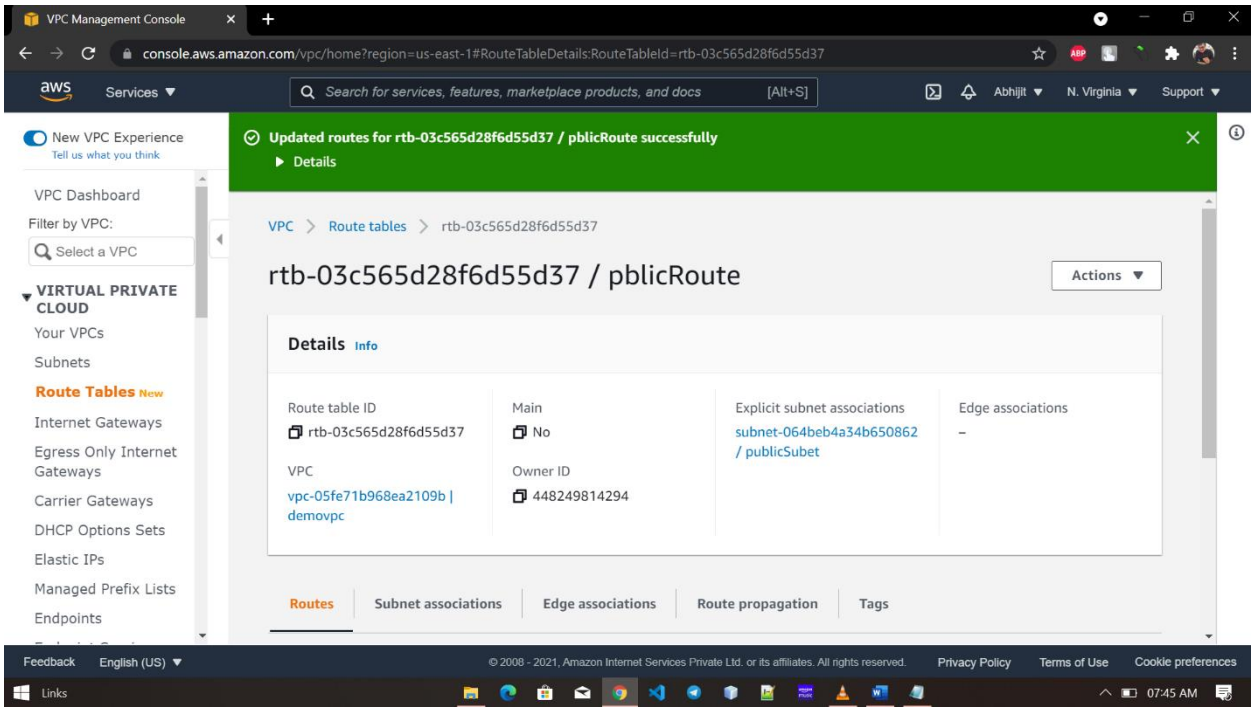

VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#CreateRouteTable:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
VPC > Route tables > Create route table
Create route table Info
A route table specifies how packets are 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.
privateRoute
VPC
The VPC to use for this route table.
vpc-05fe71b968ea2109b (demovpc)
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.
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:42 AM

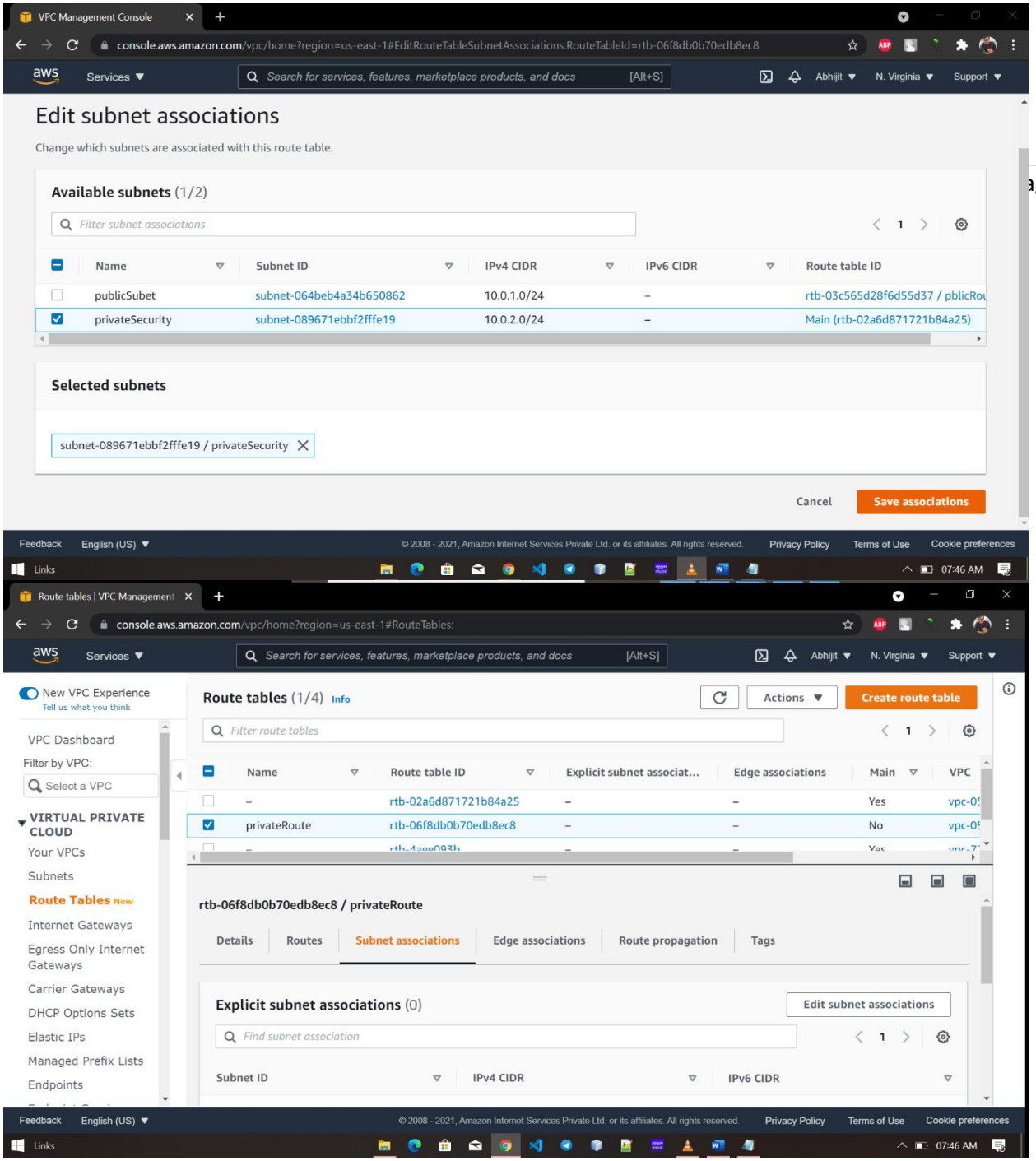

Route tables | VPC Management
console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New VPC Experience
Tell us what you think
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Route tables (4) Info
Actions
Create route table
Filter route tables
Name
Route table ID
Explicit subnet associat...
Edge associations
Main
VPC
rtb-02a6d871721b84a25
privateRoute
rtb-06f8db0b70edb8ec8
rtb-4aee093b
pblicRoute
rtb-03c565d28f6d55d37
Select a route table
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
07:43 AM
VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-06f8db0b70edb8ec8
Route table rtb-06f8db0b70edb8ec8 | privateRoute was created successfully.
VPC > Route tables > rtb-06f8db0b70edb8ec8
rtb-06f8db0b70edb8ec8 / privateRoute
Actions
Details Info
Route table ID
rtb-06f8db0b70edb8ec8
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-05fe71b968ea2109b | demovpc
Owner ID
448249814294
Routes
Subnet associations
Edge associations
Route propagation
Tags
07:42 AM

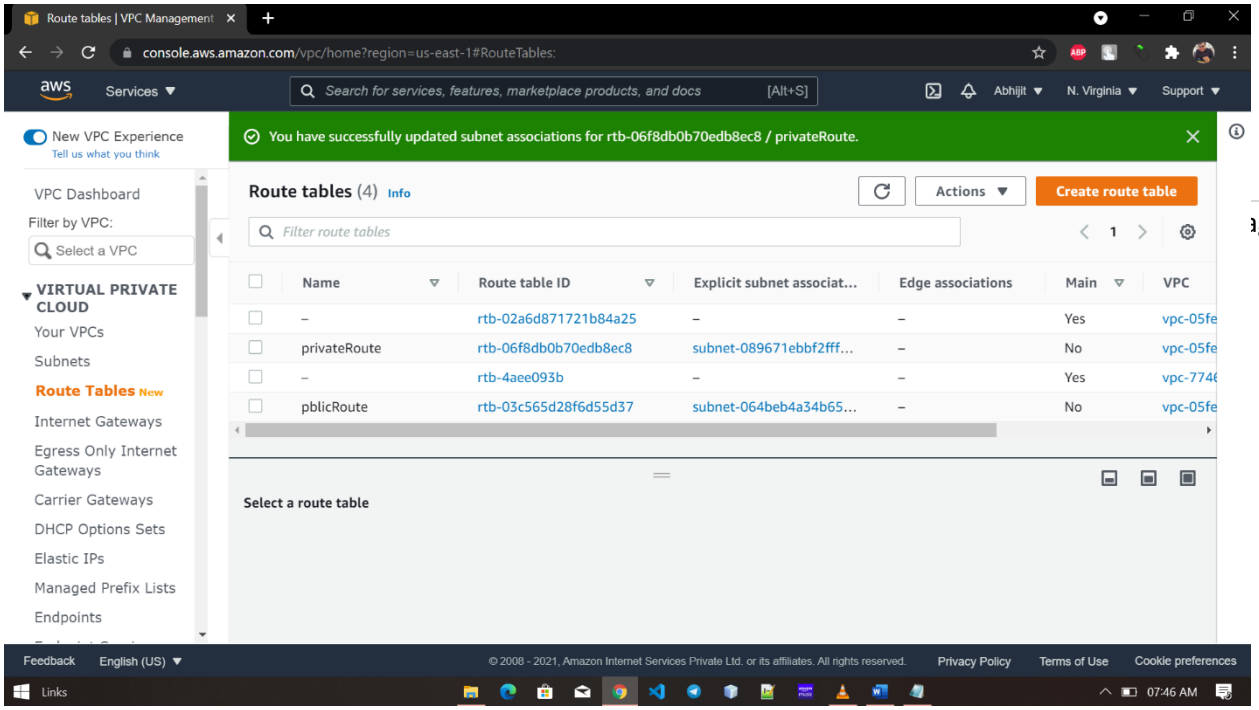

VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-03c565d28f6d55d37
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
VPC > Route tables > rtb-03c565d28f6d55d37 > Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (2)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
publicSubet
subnet-064beb4a34b650862
10.0.1.0/24
Main (rtb-02a6d871721b84a25)
privateSecurity
subnet-089671ebbf2fffe19
10.0.2.0/24
Main (rtb-02a6d871721b84a25)
Cancel
Save associations
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Route tables | VPC Management
console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables:
New VPC Experience
Tell us what you think
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Route tables (1/4) Info
Actions
Create route table
Filter route tables
rtb-4aee093b
Yes
pblicRoute
rtb-03c565d28f6d55d37
No
rtb-03c565d28f6d55d37 / pblicRoute
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (0)
Edit subnet associations
Find subnet association
Subnet ID
IPv4 CIDR
IPv6 CIDR
No subnet associations
You do not have any subnet associations.
https://console.aws.amazon.com/vpc/home?region=us-east-1#
07:43 AM


Route tables | VPC Management
console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New VPC Experience
Tell us what you think
You have successfully updated subnet associations for rtb-03c565d28f6d55d37 / pblicRoute.
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Route tables (1/4) Info
Actions
Create route table
Filter route tables
privateRoute rtb-06f8db0b70edb8ec8 No
rtb-4aee093b Yes
pblicRoute rtb-03c565d28f6d55d37 subnet-064beb4a34b65... No
Routes (1)
Edit routes
Filter routes
Both
Destination
Target
Status
Propagated
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:44 AM
Route tables (4) Info
Name
Route table ID
Explicit subnet associat...
Edge associations
Main
VPC
Select a route table
07:43 AM

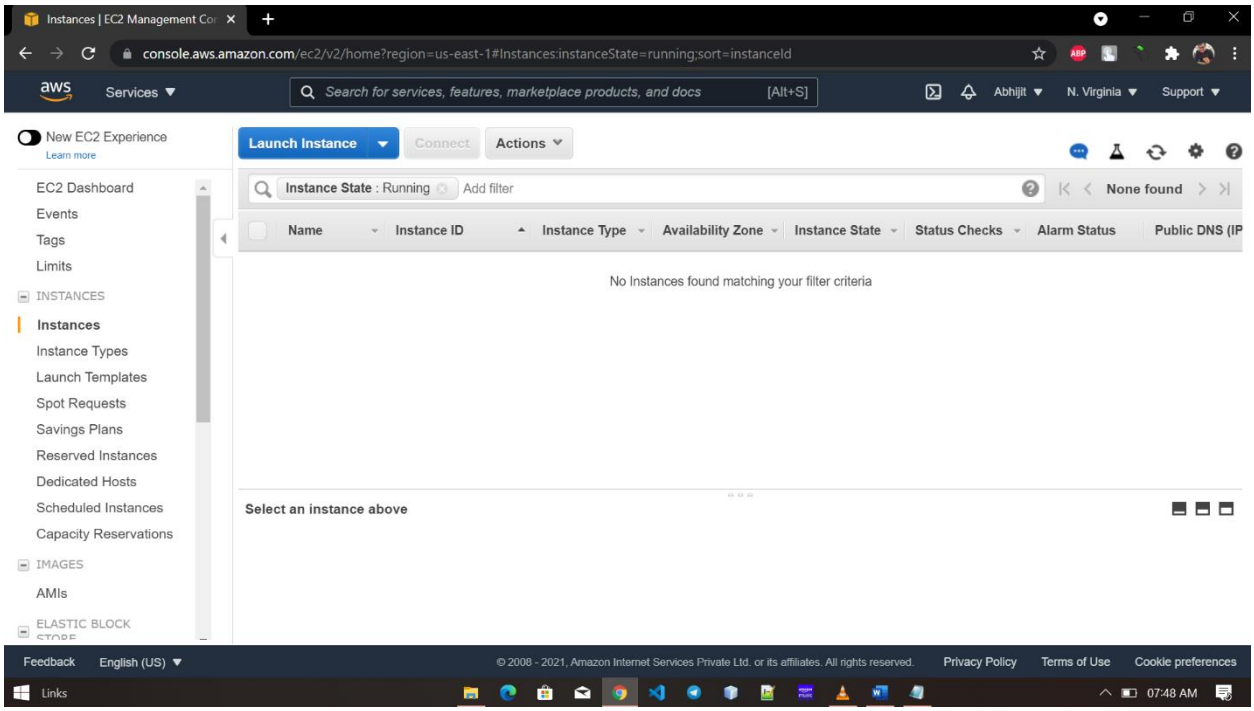

VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#EditRoutes:RouteTableId=rtb-03c565d28f6d55d37
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
VPC > Route tables > rtb-03c565d28f6d55d37 > Edit routes
Edit routes
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No
0.0.0.0/0
igw-03a2e7235100a45b7
-
No
Remove
Add route
Cancel
Preview
Save changes
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:45 AM

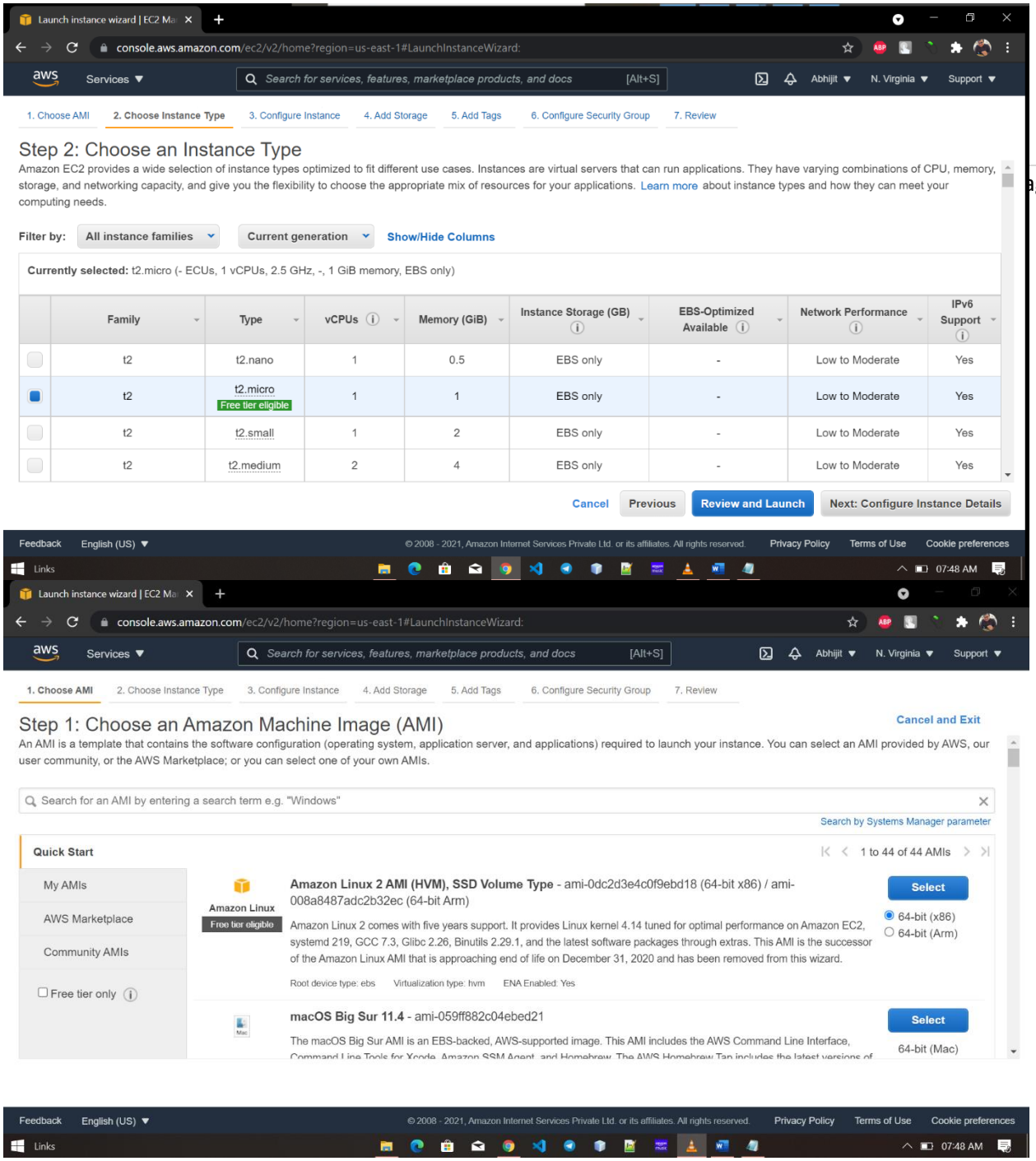

VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-03c565d28f6d55d37
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New VPC Experience
Tell us what you think
Updated routes for rtb-03c565d28f6d55d37 / pblicRoute successfully
Details
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
VPC > Route tables > rtb-03c565d28f6d55d37
rtb-03c565d28f6d55d37 / pblicRoute
Actions
Details Info
Route table ID
rtb-03c565d28f6d55d37
Main
No
Explicit subnet associations
subnet-064beb4a34b650862 / publicSubet
Edge associations
-
VPC
vpc-05fe71b968ea2109b | demovpc
Owner ID
448249814294
Routes
Subnet associations
Edge associations
Route propagation
Tags
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:45 AM

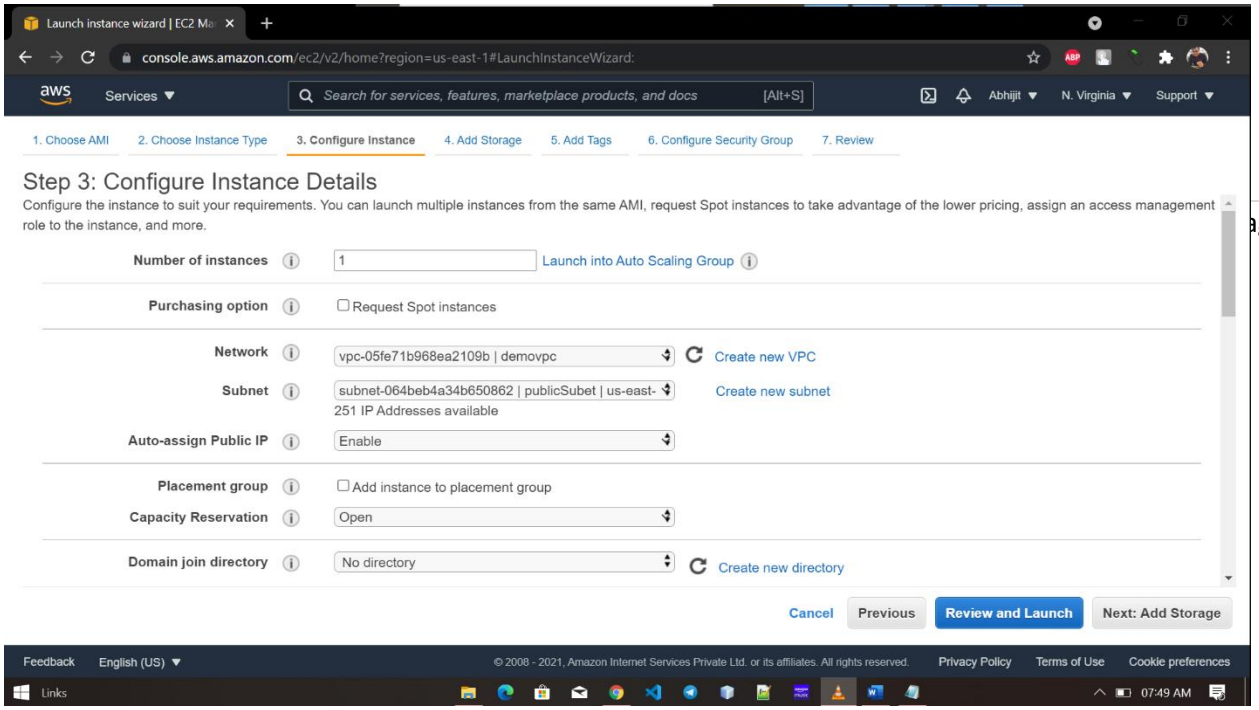

VPC Management Console
console.aws.amazon.com/vpc/home?region=us-east-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-06f8db0b70edb8ec8
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (1/2)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
publicSubet
subnet-064beb4a34b650862
10.0.1.0/24
–
privateSecurity
subnet-089671ebbf2fffe19
10.0.2.0/24
–
Main (rtb-02a6d871721b84a25)
Selected subnets
subnet-089671ebbf2fffe19 / privateSecurity
Cancel
Save associations
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:46 AM
Route tables | VPC Management
console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables:
New VPC Experience
Tell us what you think
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Route tables (1/4) Info
Actions
Create route table
Filter route tables
Name
Route table ID
Explicit subnet associat...
Edge associations
Main
VPC
rtb-02a6d871721b84a25
Yes
privateRoute
rtb-06f8db0b70edb8ec8
No
rtb-06f8db0b70edb8ec8 / privateRoute
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (0)
Edit subnet associations
Find subnet association
Subnet ID
IPv4 CIDR
IPv6 CIDR

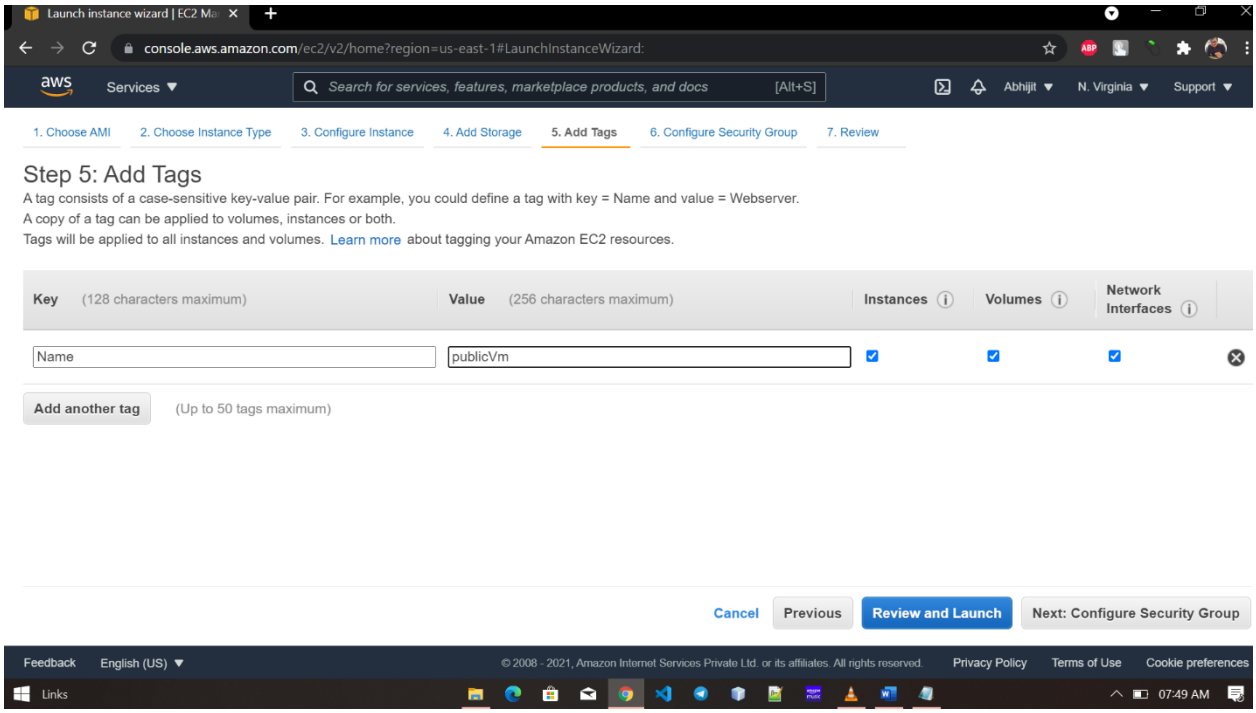


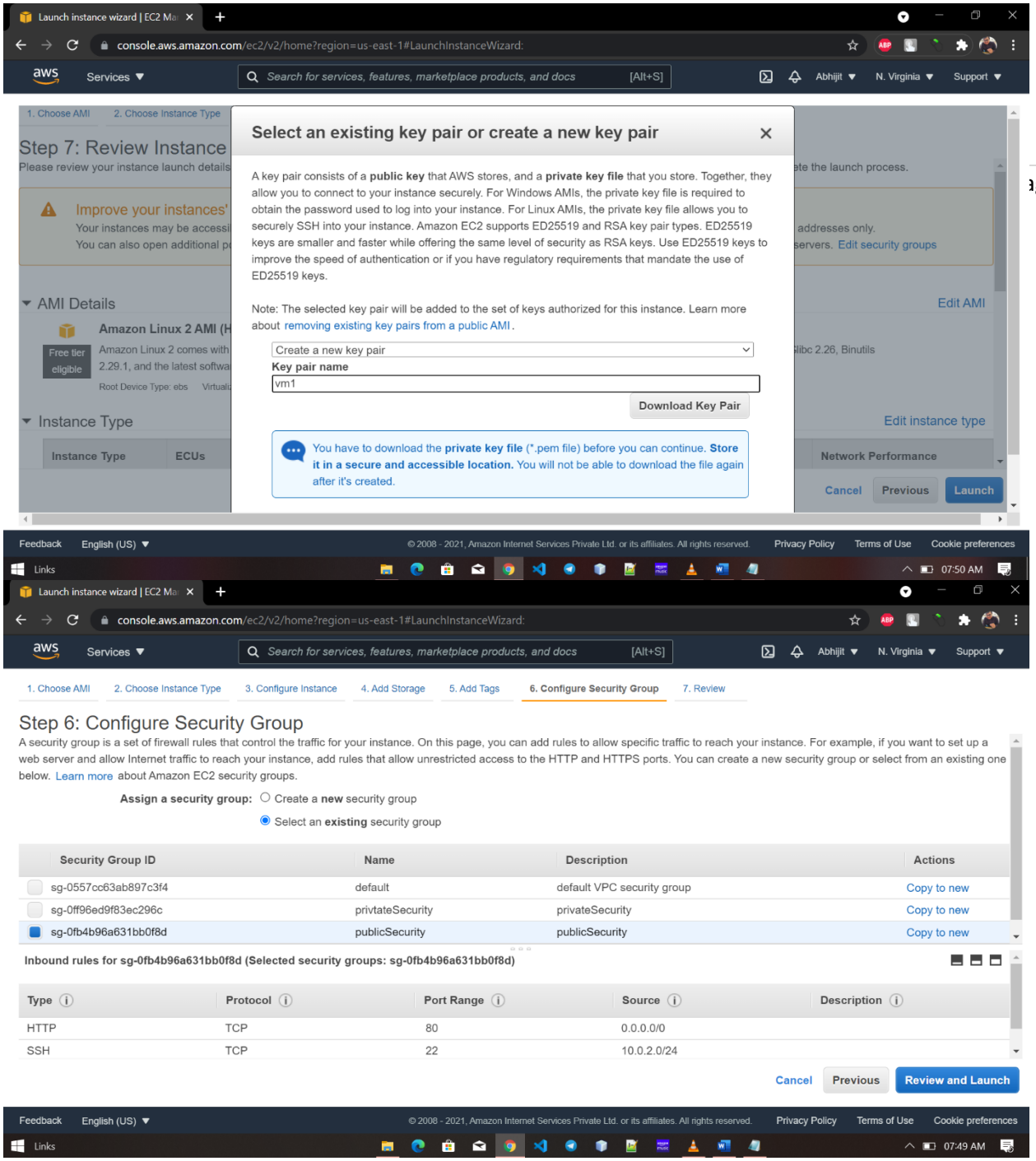
STEP 6:-creation of instance (step 6)

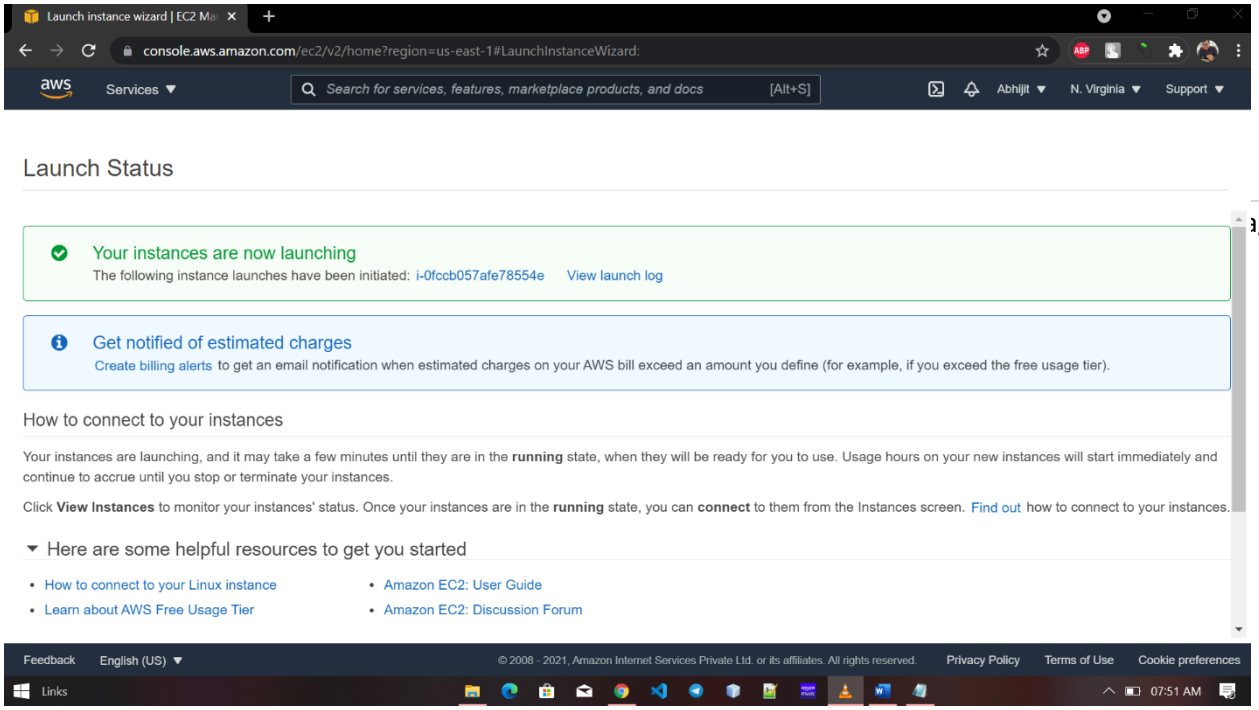


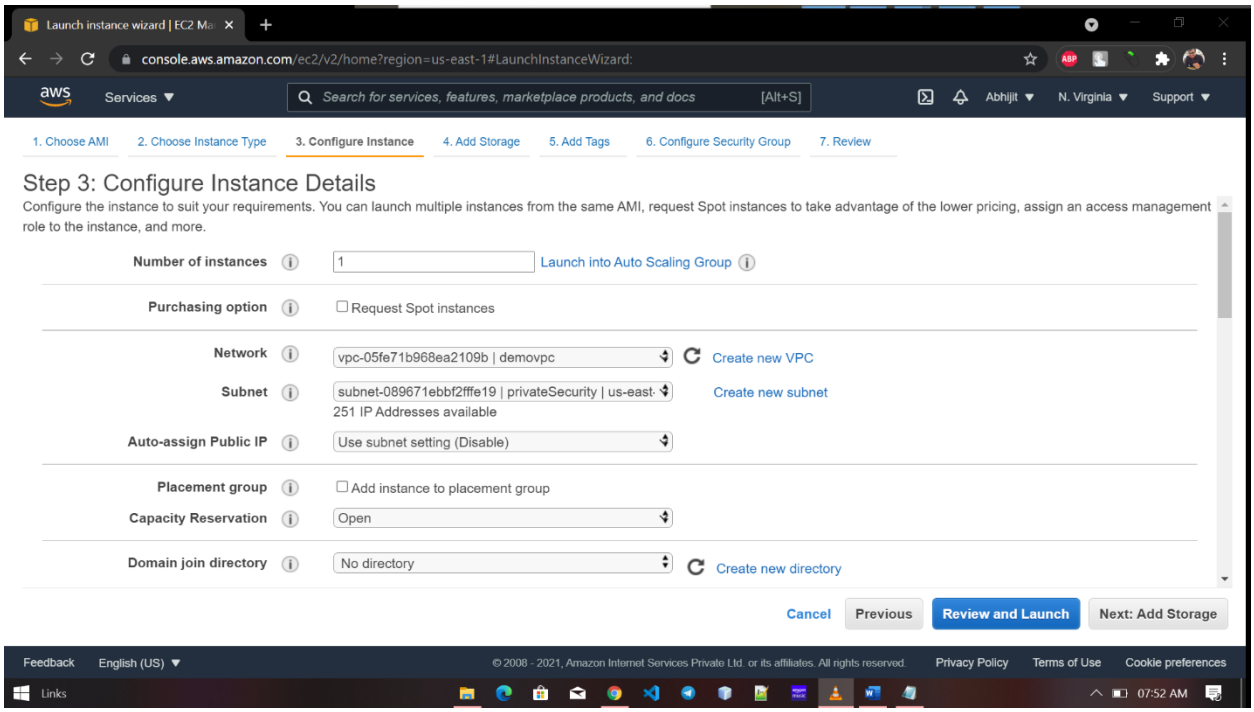

Launch instance wizard | EC2 Ma
console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by:
All instance families
Current generation
Show/Hide Columns
Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)
Family
Type
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
IPv6 Support
t2 t2.nano 1 0.5 EBS only - Low to Moderate Yes
t2 t2.micro Free tier eligible 1 1 EBS only - Low to Moderate Yes
t2 t2.small 1 2 EBS only - Low to Moderate Yes
t2 t2.medium 2 4 EBS only - Low to Moderate Yes
Cancel
Previous
Review and Launch
Next: Configure Instance Details
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:48 AM
Step 1: Choose an Amazon Machine Image (AMI)
Cancel and Exit
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.
Search for an AMI by entering a search term e.g. "Windows"
Search by Systems Manager parameter
Quick Start
1 to 44 of 44 AMIs
My AMIs
AWS Marketplace
Community AMIs
Free tier only
Amazon Linux
Free tier eligible
Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0dc2d3e4c0f9ebd18 (64-bit x86) / ami-008a8487adc2b32ec (64-bit Arm)
Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
Select
64-bit (x86)
64-bit (Arm)
macOS Big Sur 11.4 - ami-059ff882c04ebed21
The macOS Big Sur AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface,
Select
64-bit (Mac)

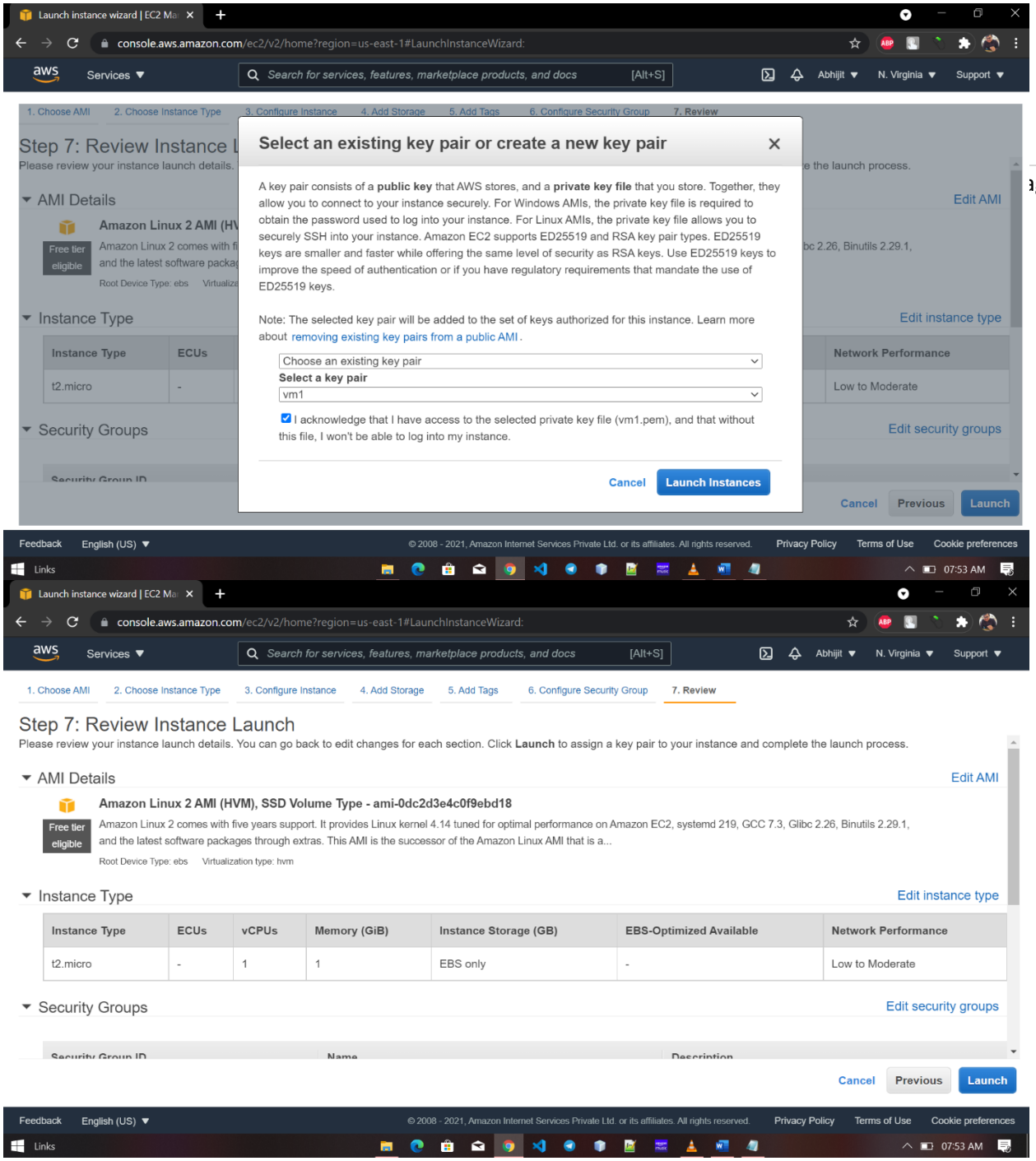

Launch instance wizard | EC2 Ma
console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-05fe71b968ea2109b | demovpc
Create new VPC
Subnet
subnet-064beb4a34b650862 | publicSubet | us-east-
Create new subnet
251 IP Addresses available
Auto-assign Public IP
Enable
Placement group
Add instance to placement group
Capacity Reservation
Open
Domain join directory
No directory
Create new directory
Cancel
Previous
Review and Launch
Next: Add Storage
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:49 AM


Launch instance wizard | EC2 Ma
console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 5: Add Tags
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.
Key (128 characters maximum)
Value (256 characters maximum)
Instances
Volumes
Network Interfaces
Name
publicVm
Add another tag
(Up to 50 tags maximum)
Cancel
Previous
Review and Launch
Next: Configure Security Group
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:49 AM

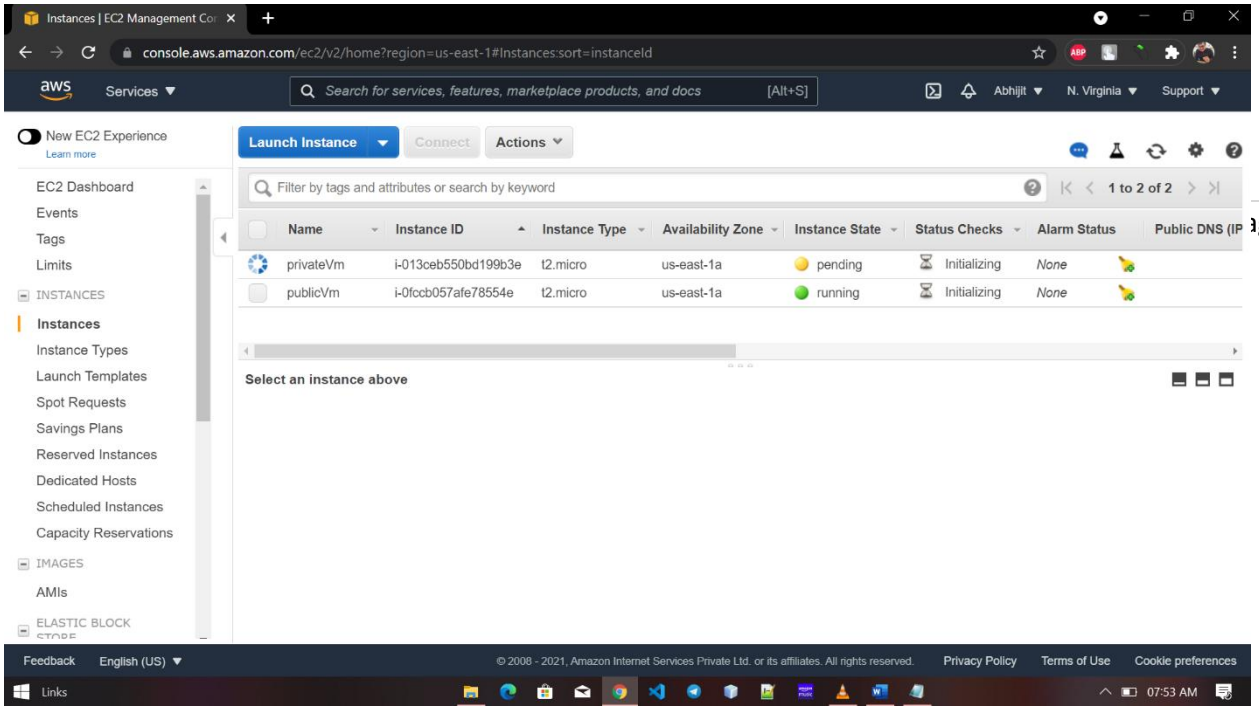

Launch instance wizard | EC2 Ma
console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
Step 7: Review Instance
Please review your instance launch details
Improve your instances'
AMI Details
Amazon Linux 2 AMI (H
Free tier eligible
Instance Type
Instance Type
ECUs
Edit AMI
Edit instance type
Network Performance
Cancel
Previous
Launch
Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types. ED25519 keys are smaller and faster while offering the same level of security as RSA keys. Use ED25519 keys to improve the speed of authentication or if you have regulatory requirements that mandate the use of ED25519 keys.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Create a new key pair
Key pair name
vm1
Download Key Pair
You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:50 AM
Launch instance wizard | EC2 Ma
console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.
Assign a security group: Create a new security group
Select an existing security group
Security Group ID
Name
Description
Actions
sg-0557cc63ab897c3f4
default
default VPC security group
Copy to new
sg-0ff96ed9f83ec296c
privtateSecurity
privateSecurity
Copy to new
sg-0fb4b96a631bb0f8d
publicSecurity
publicSecurity
Copy to new
Inbound rules for sg-0fb4b96a631bb0f8d (Selected security groups: sg-0fb4b96a631bb0f8d)
Type
Protocol
Port Range
Source
Description
HTTP
TCP
80
0.0.0.0/0
SSH
TCP
22
10.0.2.0/24
Cancel
Previous
Review and Launch
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:49 AM

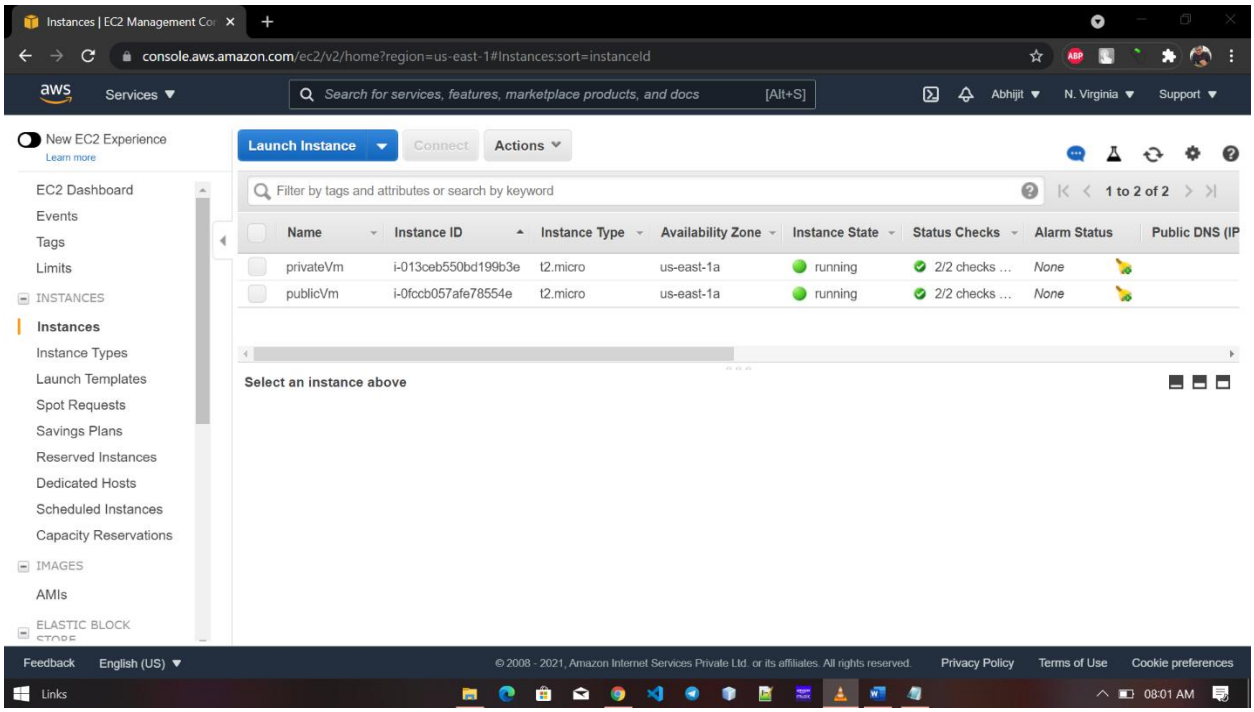

Launch instance wizard | EC2 Ma
console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
Launch Status
Your instances are now launching
The following instance launches have been initiated: i-0fccb057afe78554e View launch log
Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).
How to connect to your instances
Your instances are launching, and it may take a few minutes until they are in the running state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.
Click View Instances to monitor your instances' status. Once your instances are in the running state, you can connect to them from the Instances screen. Find out how to connect to your instances.
Here are some helpful resources to get you started
How to connect to your Linux instance
Learn about AWS Free Usage Tier
Amazon EC2: User Guide
Amazon EC2: Discussion Forum
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:51 AM


Launch instance wizard | EC2 Ma
console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-05fe71b968ea2109b | demovpc
Create new VPC
Subnet
subnet-089671ebbf2fffe19 | privateSecurity | us-east-
Create new subnet
251 IP Addresses available
Auto-assign Public IP
Use subnet setting (Disable)
Placement group
Add instance to placement group
Capacity Reservation
Open
Domain join directory
No directory
Create new directory
Cancel
Previous
Review and Launch
Next: Add Storage
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:52 AM

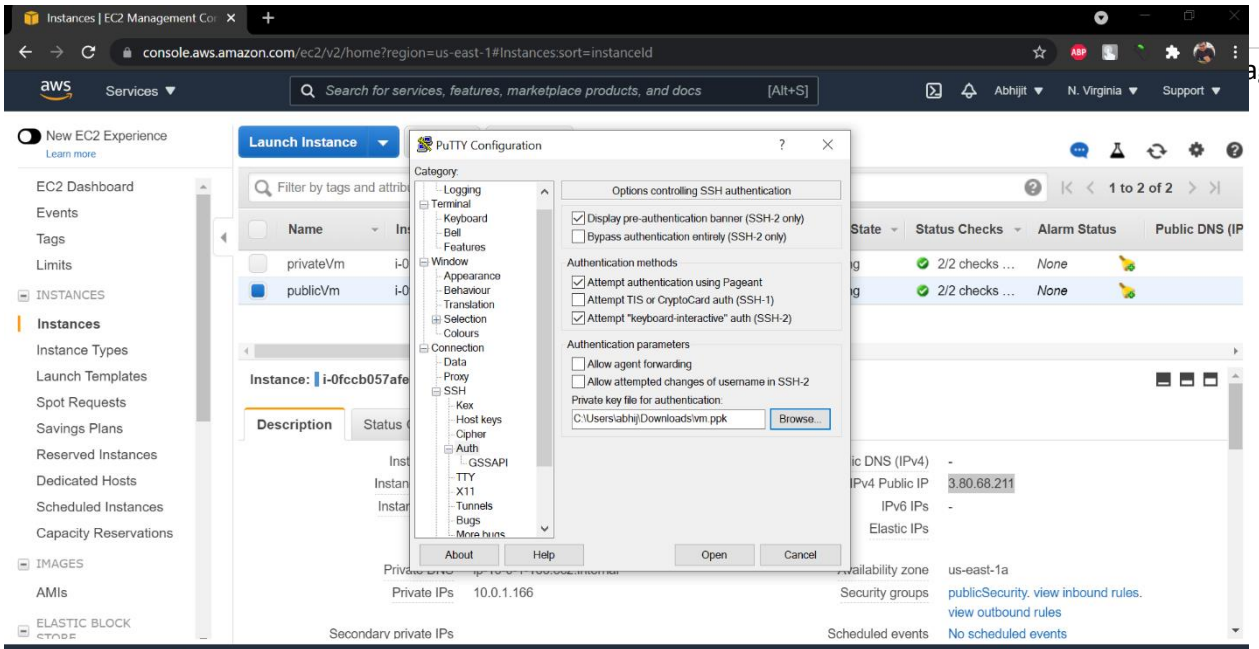

Launch instance wizard | EC2 Ma
console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 7: Review Instance L
Please review your instance launch details.
AMI Details
Edit AMI
Amazon Linux 2 AMI (HV
Free tier eligible
Root Device Type: ebs
Instance Type
Edit instance type
Instance Type
ECUs
t2.micro
Network Performance
Low to Moderate
Security Groups
Edit security groups
Cancel
Previous
Launch
Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types. ED25519 keys are smaller and faster while offering the same level of security as RSA keys. Use ED25519 keys to improve the speed of authentication or if you have regulatory requirements that mandate the use of ED25519 keys.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Choose an existing key pair
Select a key pair
vm1
I acknowledge that I have access to the selected private key file (vm1.pem), and that without this file, I won't be able to log into my instance.
Cancel
Launch Instances
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:53 AM

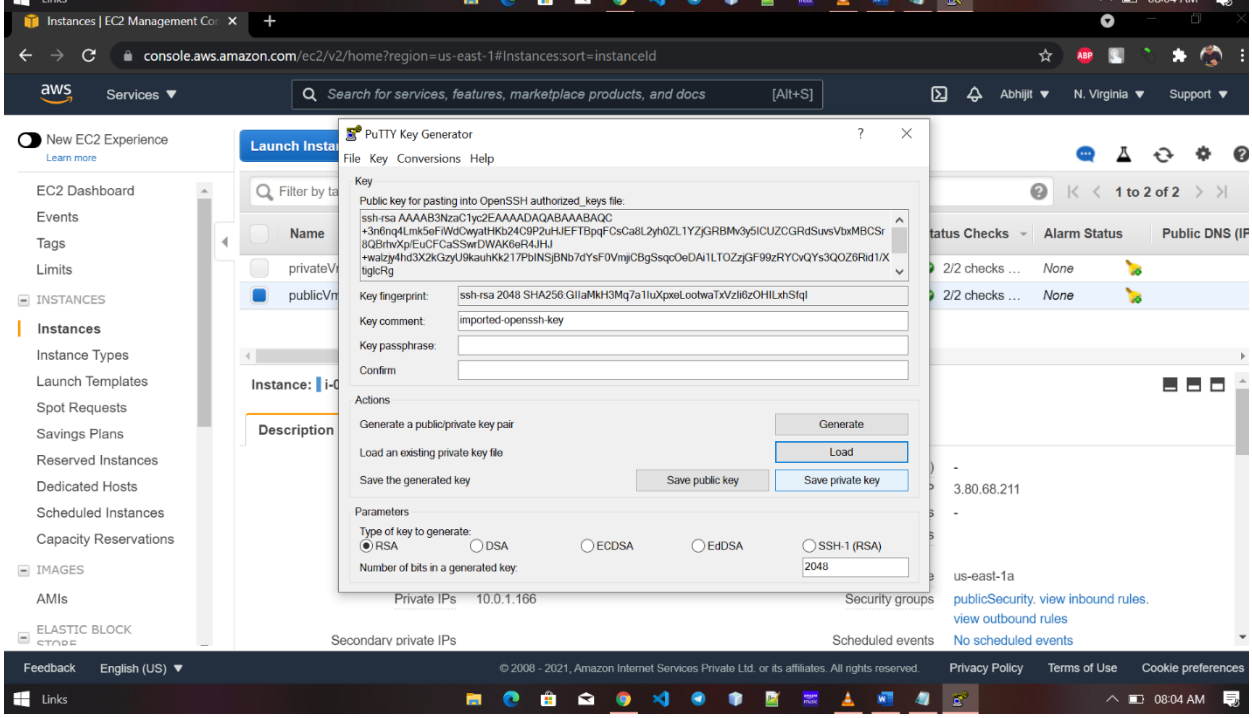
Launch instance wizard | EC2 Ma
console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 7: Review Instance Launch
Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.
AMI Details
Edit AMI
Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0dc2d3e4c0f9ebd18
Free tier eligible
Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is a...
Root Device Type: ebs
Virtualization type: hvm
Instance Type
Edit instance type
Instance Type
ECUs
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
t2.micro
1
1
EBS only
Low to Moderate
Security Groups
Edit security groups
Security Group ID
Name
Description
Cancel
Previous
Launch
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:53 AM

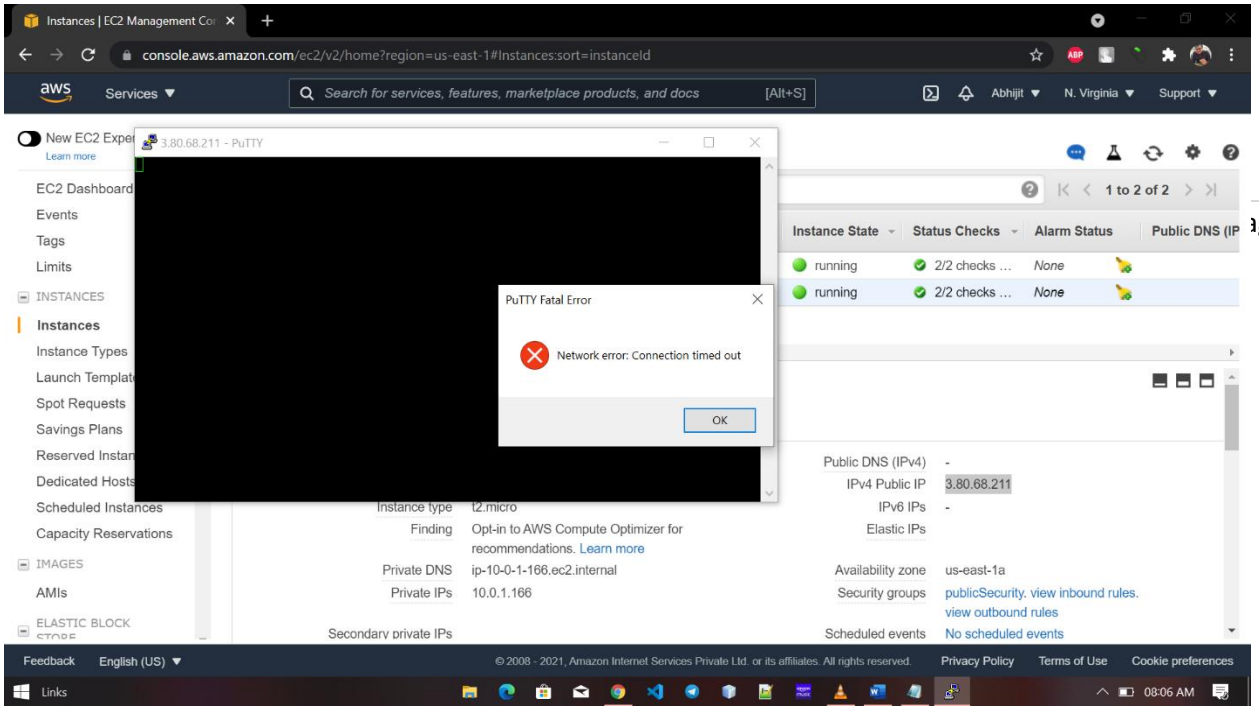

Instances | EC2 Management Co
console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:sort=instanceId
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New EC2 Experience
Learn more
EC2 Dashboard
Events
Tags
Limits
INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
ELASTIC BLOCK STORE
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
1 to 2 of 2
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IP
privateVm i-013ceb550bd199b3e t2.micro us-east-1a pending Initializing None
publicVm i-0fccb057afe78554e t2.micro us-east-1a running Initializing None
Select an instance above
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
07:53 AM


Instances | EC2 Management Co
console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:sort=instanceId
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New EC2 Experience
Learn more
EC2 Dashboard
Events
Tags
Limits
INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
ELASTIC BLOCK STORE
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
1 to 2 of 2
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IP
privateVm i-013ceb550bd199b3e t2.micro us-east-1a running 2/2 checks ... None
publicVm i-0fccb057afe78554e t2.micro us-east-1a running 2/2 checks ... None
Select an instance above
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
08:01 AM

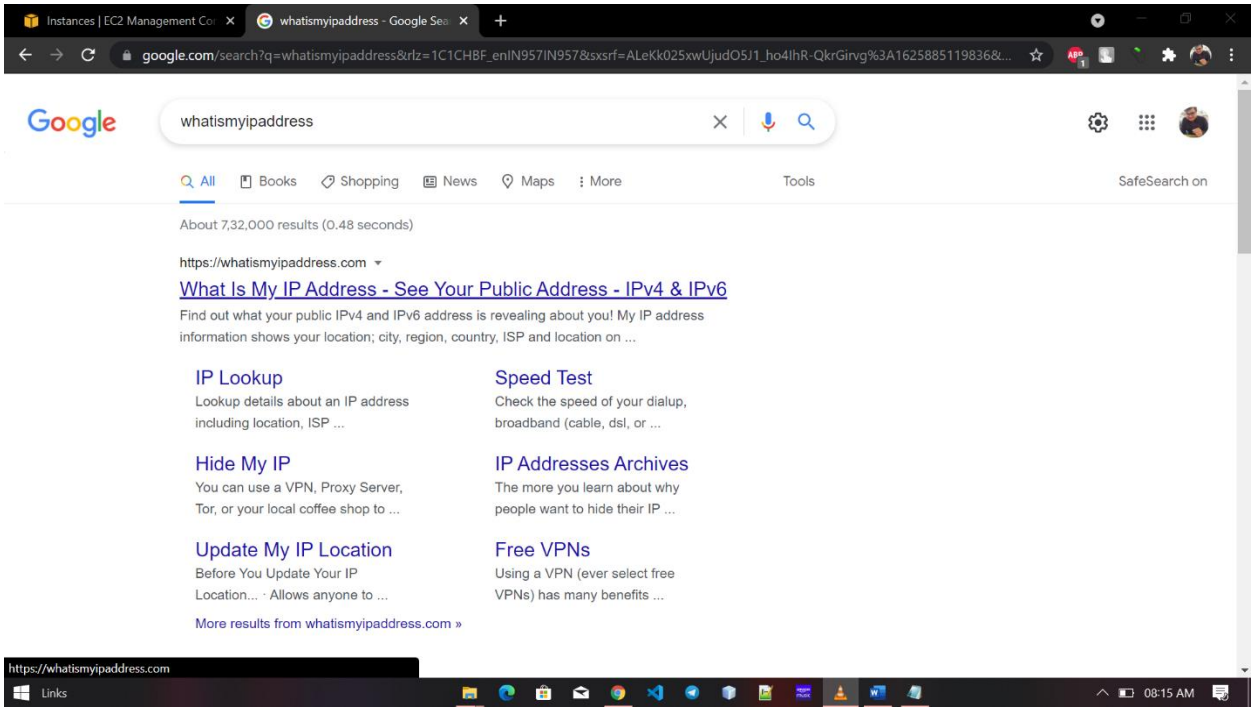
STEP 7:-logging in to the pblic network (checking its working (failed)) (step 7)

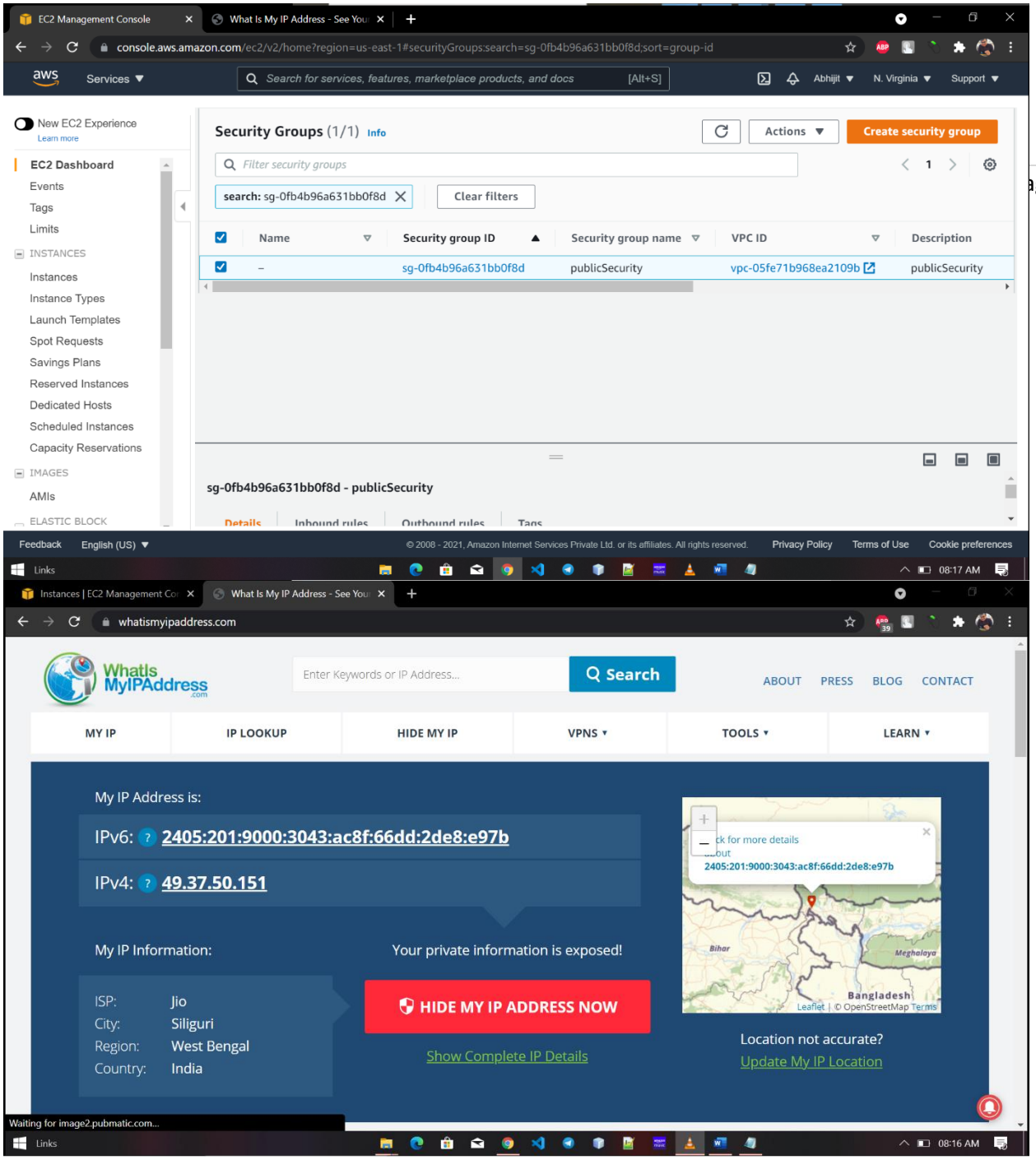


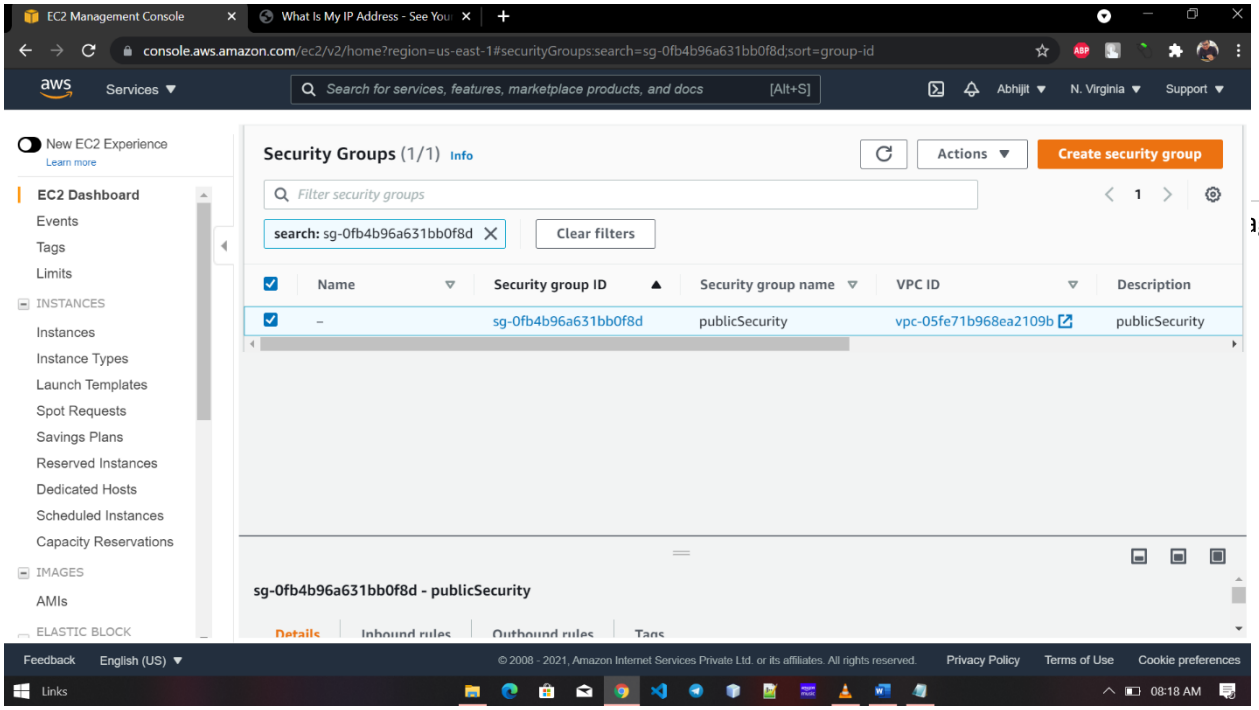


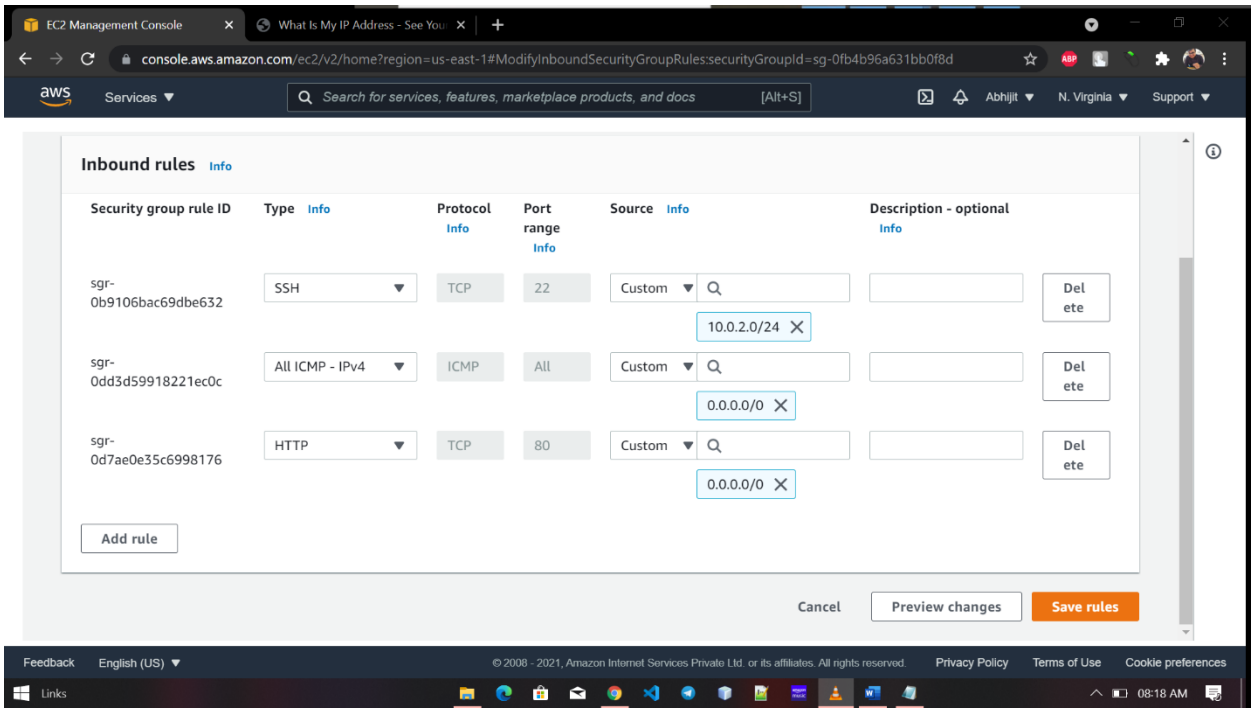


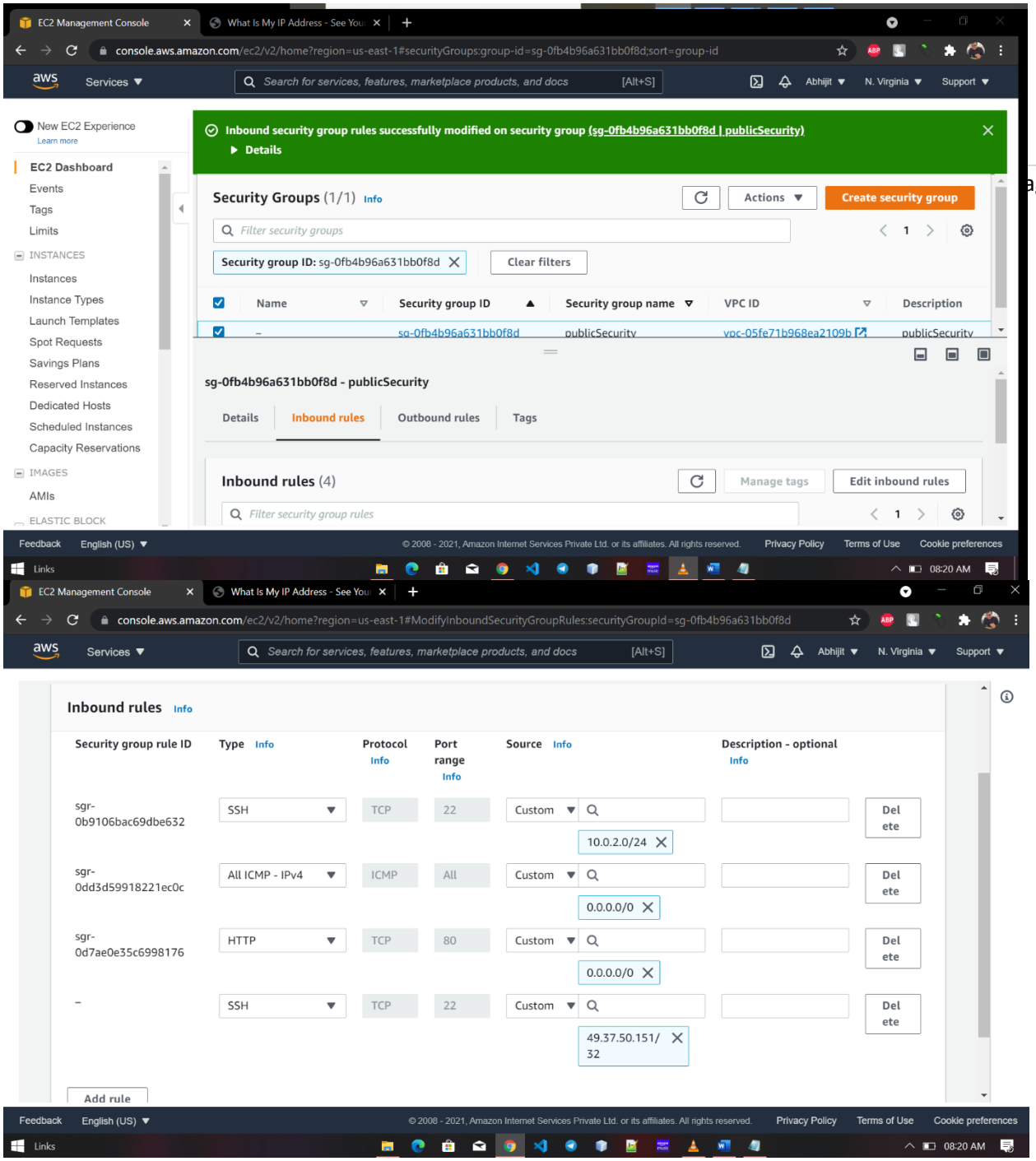
STEP 8-adding our own ip to gain access to public network and trying again to login (step 8)

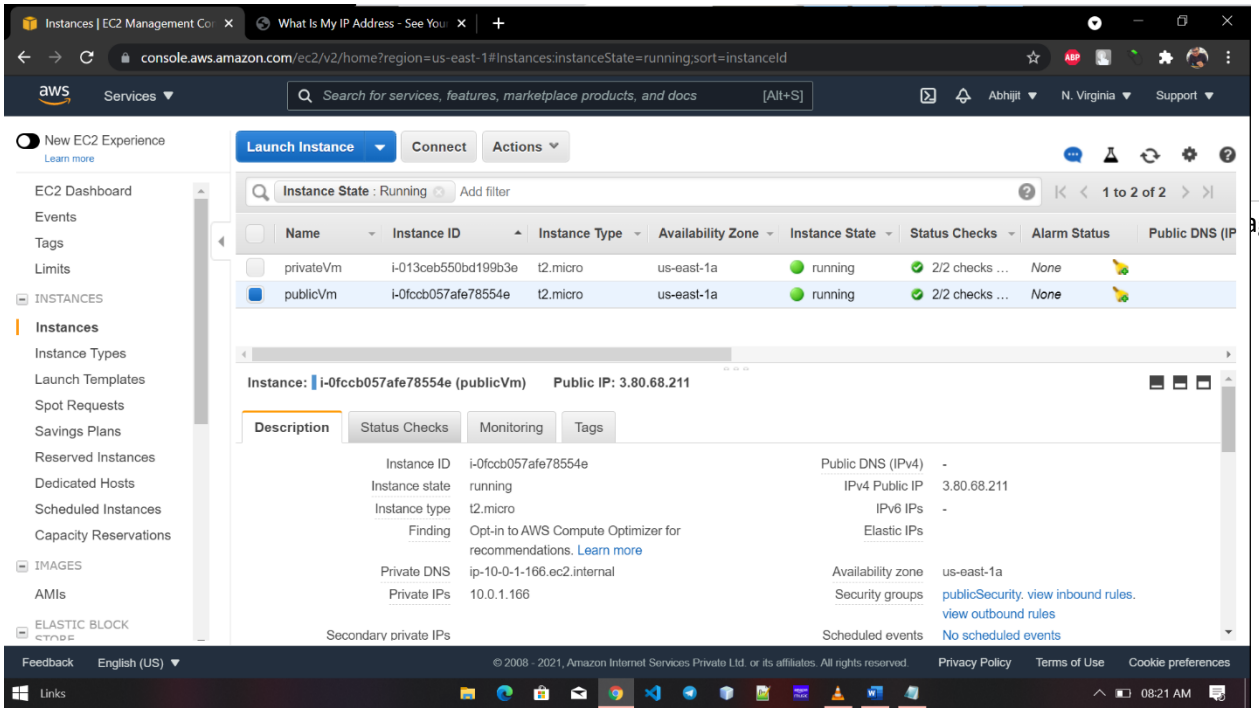


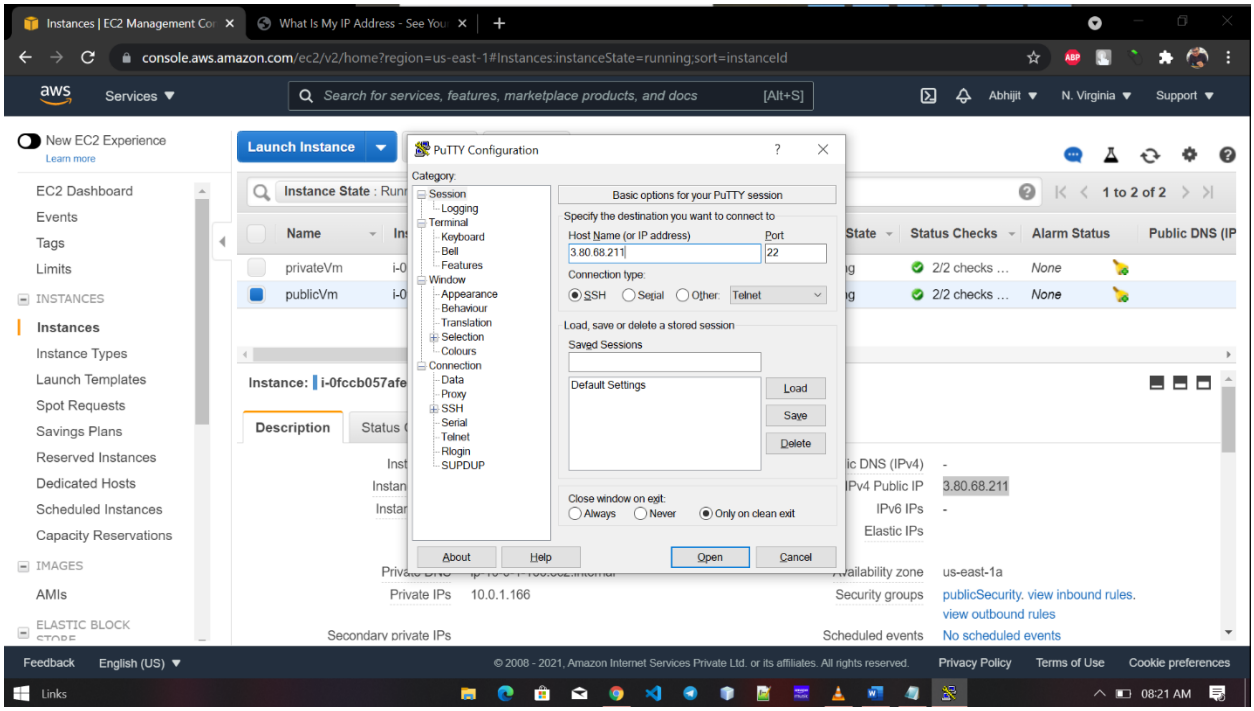

EC2 Management Console
What Is My IP Address - See Your
console.aws.amazon.com/ec2/v2/home?region=us-east-1#securityGroups:search=sg-0fb4b96a631bb0f8d;sort=group-id
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New EC2 Experience
Learn more
EC2 Dashboard
Events
Tags
Limits
INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
ELASTIC BLOCK
Security Groups (1/1) Info
Actions
Create security group
Filter security groups
search: sg-0fb4b96a631bb0f8d
Clear filters
Name
Security group ID
Security group name
VPC ID
Description
sg-0fb4b96a631bb0f8d
publicSecurity
vpc-05fe71b968ea2109b
publicSecurity
sg-0fb4b96a631bb0f8d - publicSecurity
Details
Inbound rules
Outbound rules
Tags
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
08:17 AM
Instances | EC2 Management Co
What Is My IP Address - See Your
whatismyipaddress.com
WhatIsMyIPAddress.com
Enter Keywords or IP Address...
Search
ABOUT
PRESS
BLOG
CONTACT
MY IP
IP LOOKUP
HIDE MY IP
VPNS
TOOLS
LEARN
My IP Address is:
IPv6: 2405:201:9000:3043:ac8f:66dd:2de8:e97b
IPv4: 49.37.50.151
My IP Information:
ISP: Jio
City: Siliguri
Region: West Bengal
Country: India
Your private information is exposed!
HIDE MY IP ADDRESS NOW
Show Complete IP Details
2405:201:9000:3043:ac8f:66dd:2de8:e97b
Bihar
Meghalaya
Bangladesh
Leaflet | © OpenStreetMap Terms
Location not accurate?
Update My IP Location
Waiting for image2.pubmatic.com...
Links
08:16 AM

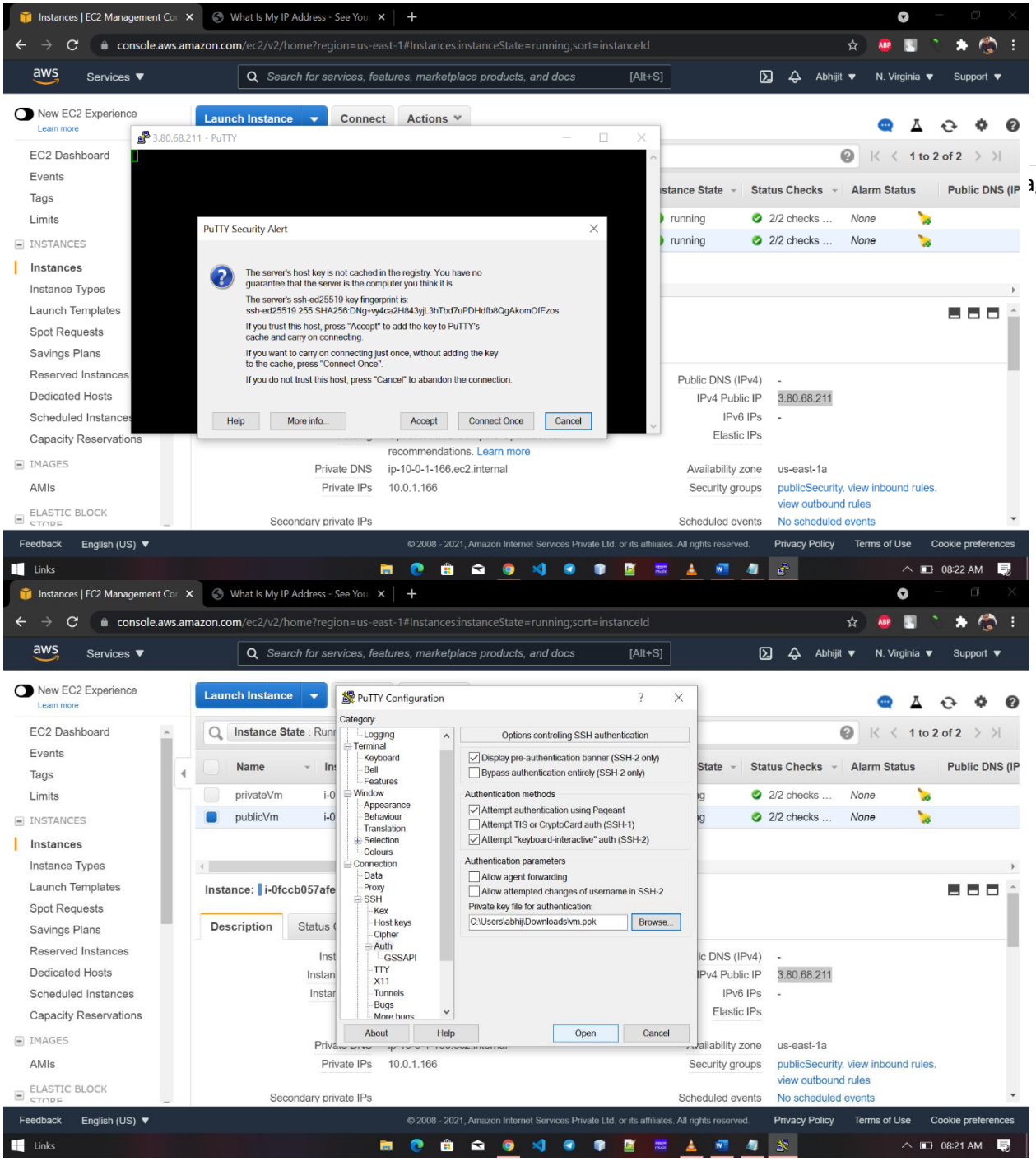

EC2 Management Console
What Is My IP Address - See Your
console.aws.amazon.com/ec2/v2/home?region=us-east-1#securityGroups:search=sg-0fb4b96a631bb0f8d;sort=group-id
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New EC2 Experience
Learn more
EC2 Dashboard
Events
Tags
Limits
INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
ELASTIC BLOCK
Security Groups (1/1) Info
Actions
Create security group
Filter security groups
search: sg-0fb4b96a631bb0f8d
Clear filters
Name
Security group ID
Security group name
VPC ID
Description
sg-0fb4b96a631bb0f8d
publicSecurity
vpc-05fe71b968ea2109b
publicSecurity
sg-0fb4b96a631bb0f8d - publicSecurity
Details
Inbound rules
Outbound rules
Tags
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
08:18 AM

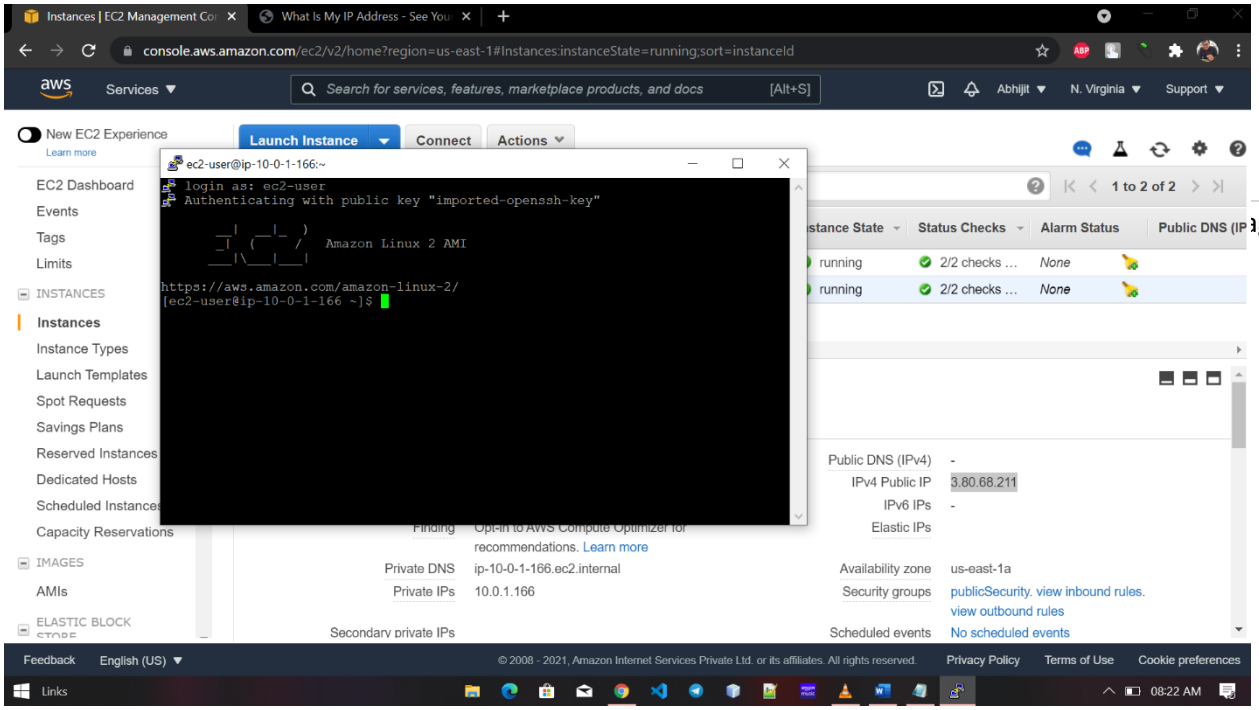

EC2 Management Console
What Is My IP Address - See Your
console.aws.amazon.com/ec2/v2/home?region=us-east-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-0fb4b96a631bb0f8d
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
Inbound rules Info
Security group rule ID
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
sgr-0b9106bac69dbe632
SSH
TCP
22
Custom
10.0.2.0/24
Delete
sgr-0dd3d59918221ec0c
All ICMP - IPv4
ICMP
All
Custom
0.0.0.0/0
Delete
sgr-0d7ae0e35c6998176
HTTP
TCP
80
Custom
0.0.0.0/0
Delete
Add rule
Cancel
Preview changes
Save rules
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
08:18 AM


EC2 Management Console
What Is My IP Address - See You
console.aws.amazon.com/ec2/v2/home?region=us-east-1#securityGroups:group-id=sg-0fb4b96a631bb0f8d;sort=group-id
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New EC2 Experience
Learn more
EC2 Dashboard
Events
Tags
Limits
INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
ELASTIC BLOCK
Inbound security group rules successfully modified on security group (sg-0fb4b96a631bb0f8d | publicSecurity)
Details
Security Groups (1/1) Info
Actions
Create security group
Filter security groups
Security group ID: sg-0fb4b96a631bb0f8d
Clear filters
Name
Security group ID
Security group name
VPC ID
Description
sg-0fb4b96a631bb0f8d
publicSecurity
vpc-05fe71b968ea2109b
publicSecurity
sg-0fb4b96a631bb0f8d - publicSecurity
Details
Inbound rules
Outbound rules
Tags
Inbound rules (4)
Manage tags
Edit inbound rules
Filter security group rules
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
08:20 AM
EC2 Management Console
What Is My IP Address - See You
console.aws.amazon.com/ec2/v2/home?region=us-east-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-0fb4b96a631bb0f8d
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
Inbound rules Info
Security group rule ID
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
sgr-0b9106bac69dbe632
SSH
TCP
22
Custom
10.0.2.0/24
Delete
sgr-0dd3d59918221ec0c
All ICMP - IPv4
ICMP
All
Custom
0.0.0.0/0
Delete
sgr-0d7ae0e35c6998176
HTTP
TCP
80
Custom
0.0.0.0/0
Delete
-
SSH
TCP
22
Custom
49.37.50.151/32
Delete
Add rule
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
08:20 AM

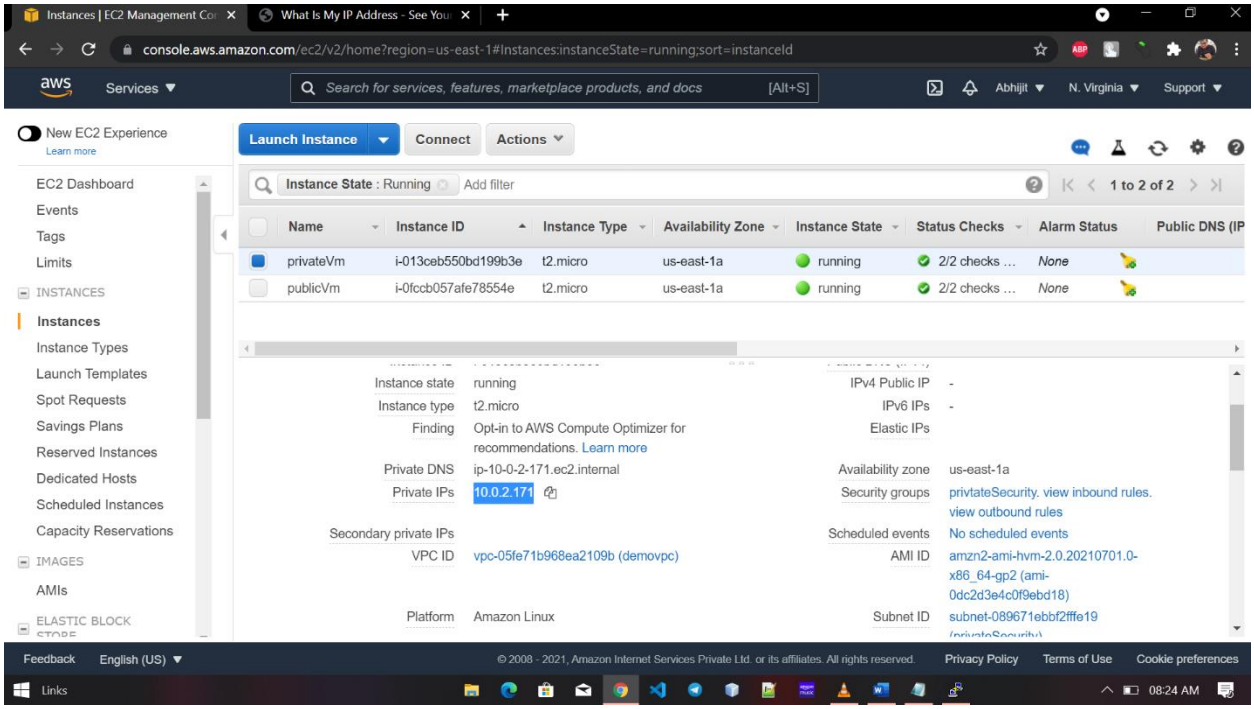

Instances | EC2 Management Co
What Is My IP Address - See You
console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:instanceState=running;sort=instanceId
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New EC2 Experience
Learn more
Launch Instance
Connect
Actions
EC2 Dashboard
Events
Tags
Limits
INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
Instance State : Running
Add filter
1 to 2 of 2
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IP
privateVm
i-013ceb550bd199b3e
t2.micro
us-east-1a
running
2/2 checks ...
None
publicVm
i-0fccb057afe78554e
t2.micro
us-east-1a
running
2/2 checks ...
None
Instance: i-0fccb057afe78554e (publicVm)
Public IP: 3.80.68.211
Description
Status Checks
Monitoring
Tags
Instance ID
i-0fccb057afe78554e
Instance state
running
Instance type
t2.micro
Finding
Opt-in to AWS Compute Optimizer for recommendations. Learn more
Private DNS
ip-10-0-1-166.ec2.internal
Private IPs
10.0.1.166
Secondary private IPs
Public DNS (IPv4)
-
IPv4 Public IP
3.80.68.211
IPv6 IPs
-
Elastic IPs
Availability zone
us-east-1a
Security groups
publicSecurity. view inbound rules. view outbound rules
Scheduled events
No scheduled events
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
08:21 AM

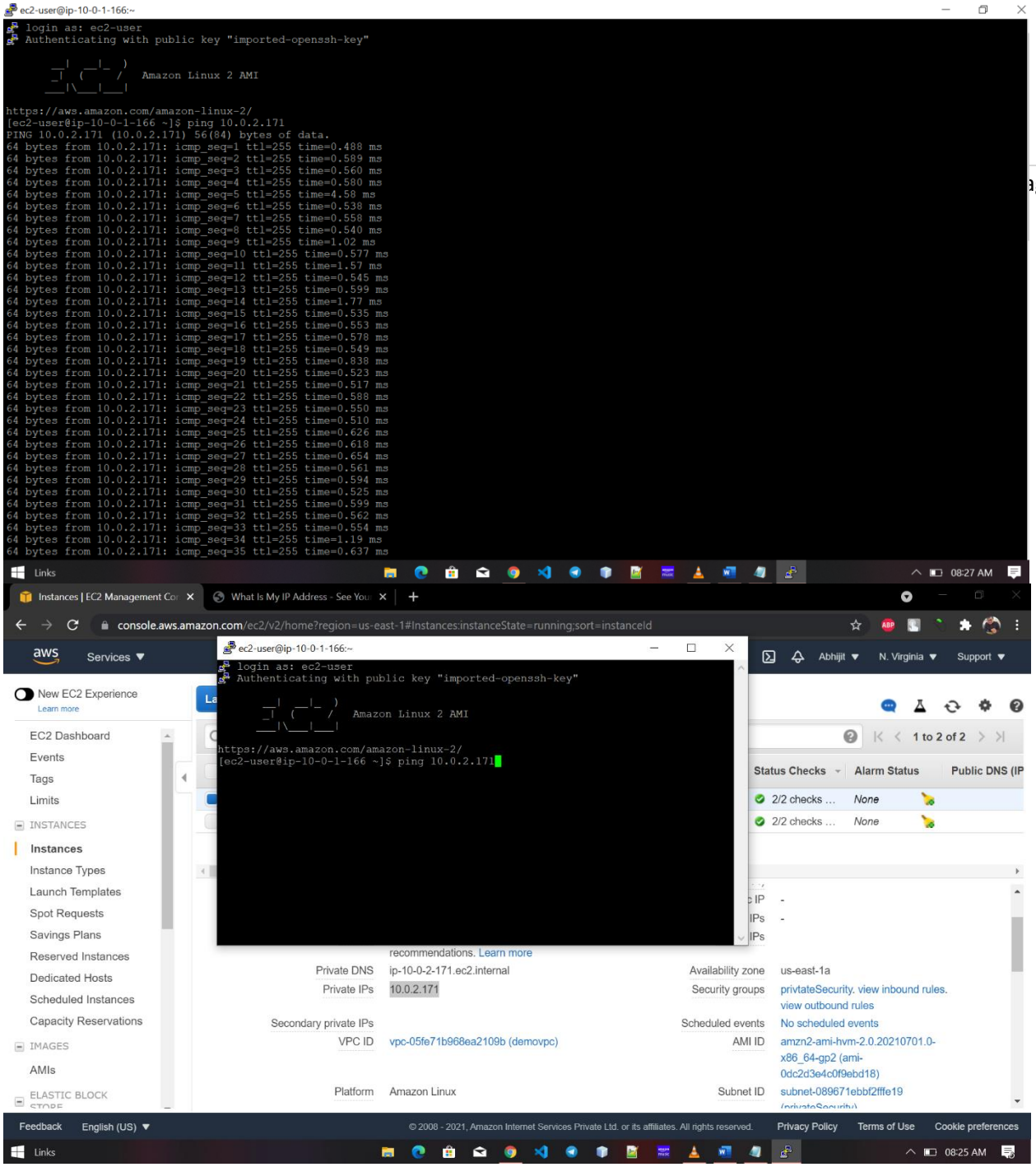

Instances | EC2 Management Co
What Is My IP Address - See You
console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:instanceState=running;sort=instanceId
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New EC2 Experience
Learn more
Launch Instance
EC2 Dashboard
Events
Tags
Limits
INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
1 to 2 of 2
privateVm
publicVm
2/2 checks ...
None
Description
Private IPs
10.0.1.166
Security groups
publicSecurity. view inbound rules. view outbound rules
Scheduled events
No scheduled events
PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
3.80.68.211
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel
3.80.68.211
us-east-1a
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
08:21 AM

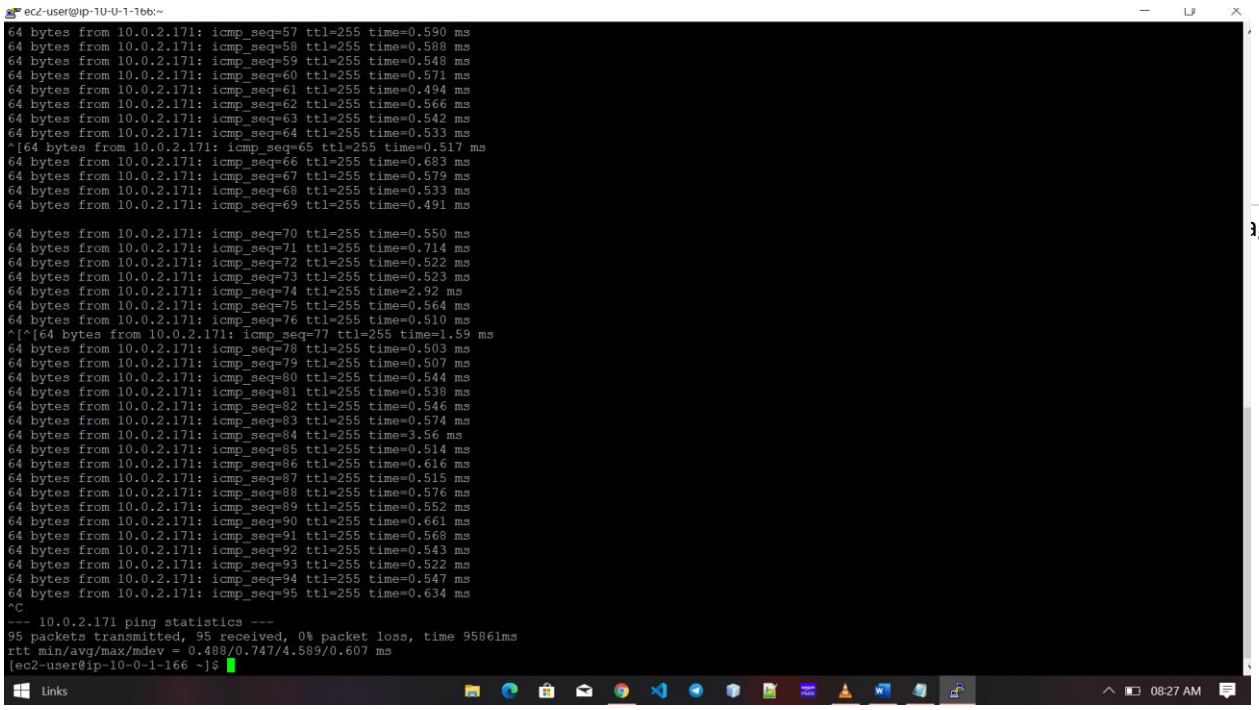

Instances | EC2 Management Cor
What Is My IP Address - See You
console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:instanceState=running;sort=instanceId
Services
Search for services, features, marketplace products, and docs [Alt+S]
Abhijit
N. Virginia
Support
New EC2 Experience
Learn more
Launch Instance
Connect
Actions
EC2 Dashboard
Events
Tags
Limits
INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
ELASTIC BLOCK STORE
3.80.68.211 - PuTTY
PuTTY Security Alert
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:DNg+vy4ca2H843yjL3hTbd7uPDHdfb8QgAkomOfFzos
If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".
If you do not trust this host, press "Cancel" to abandon the connection.
Help
More info...
Accept
Connect Once
Cancel
1 to 2 of 2
Status Checks
Alarm Status
Public DNS (IP
running
2/2 checks ...
None
Public DNS (IPv4)
IPv4 Public IP
3.80.68.211
IPv6 IPs
Elastic IPs
recommendations. Learn more
Private DNS
ip-10-0-1-166.ec2.internal
Private IPs
10.0.1.166
Availability zone
us-east-1a
Security groups
publicSecurity. view inbound rules.
view outbound rules
Secondary private IPs
Scheduled events
No scheduled events
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
08:22 AM
PuTTY Configuration
Category:
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Kex
Host keys
Cipher
Auth
GSSAPI
TTY
X11
Tunnels
Bugs
More bugs
Options controlling SSH authentication
Display pre-authentication banner (SSH-2 only)
Bypass authentication entirely (SSH-2 only)
Authentication methods
Attempt authentication using Pageant
Attempt TIS or CryptoCard auth (SSH-1)
Attempt "keyboard-interactive" auth (SSH-2)
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH-2
Private key file for authentication:
C:\Users\abhij\Downloads\vm.ppk
Browse...
About
Help
Open
Cancel
Name
privateVm
publicVm
Instance: i-0fccb057afe
Description
08:21 AM

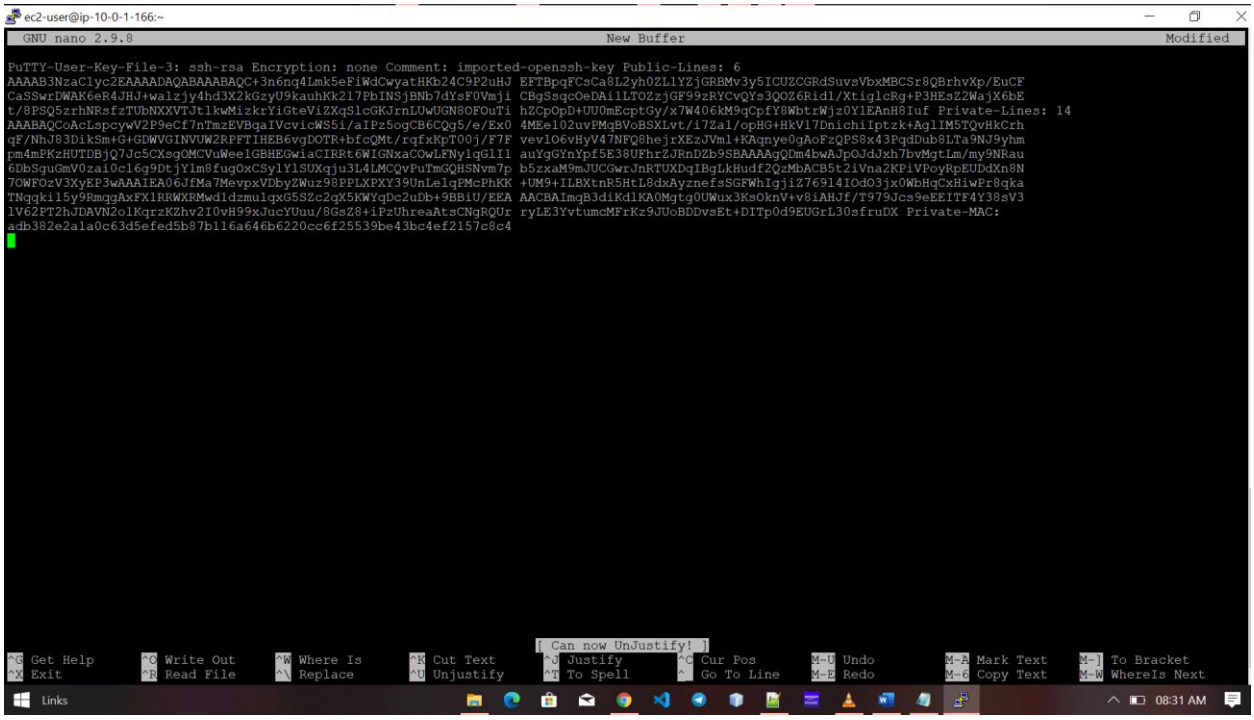


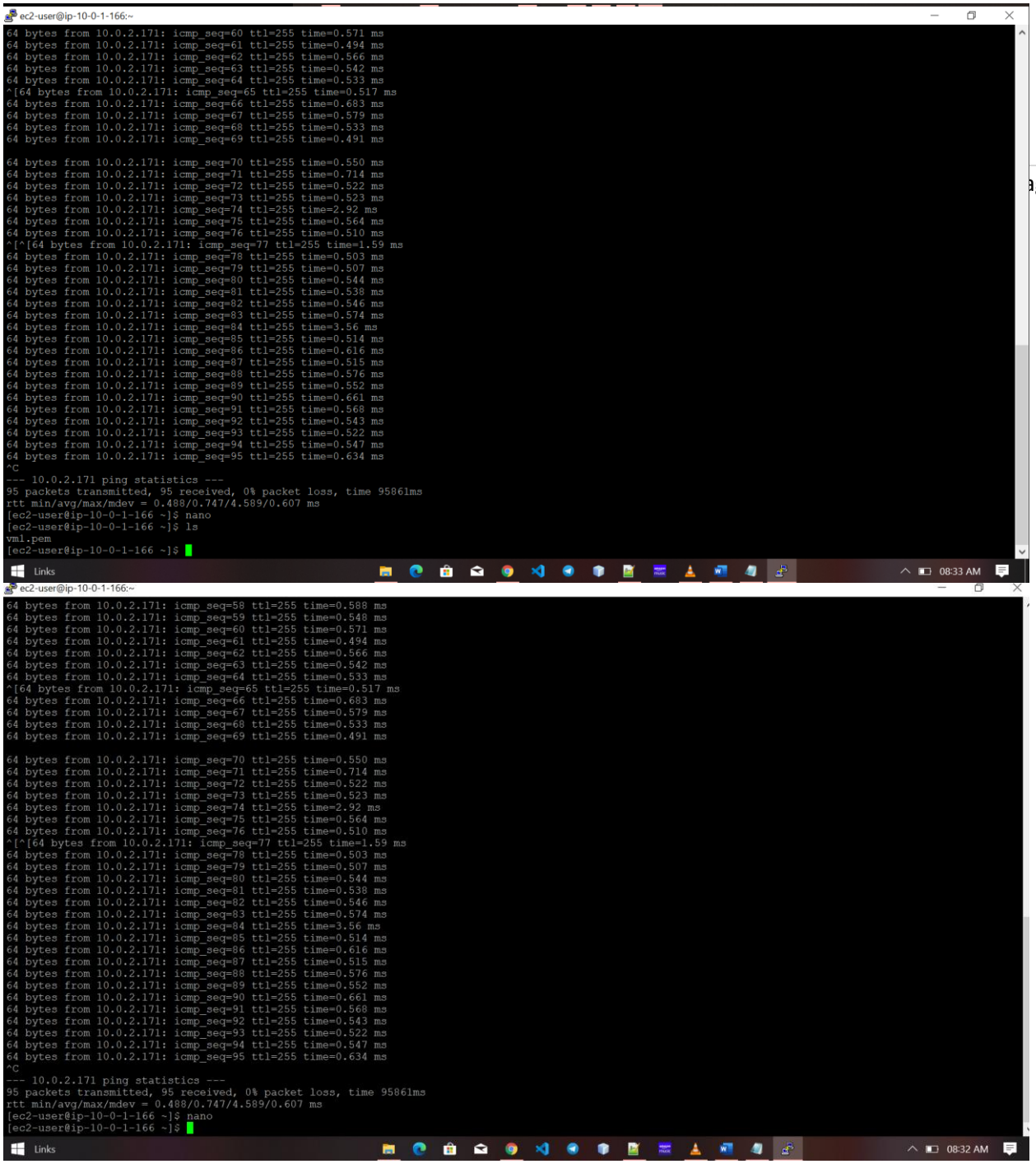
STEP 9:-public to private ssh (ping check from pblic to private using route gateway and connect it) (step 9)

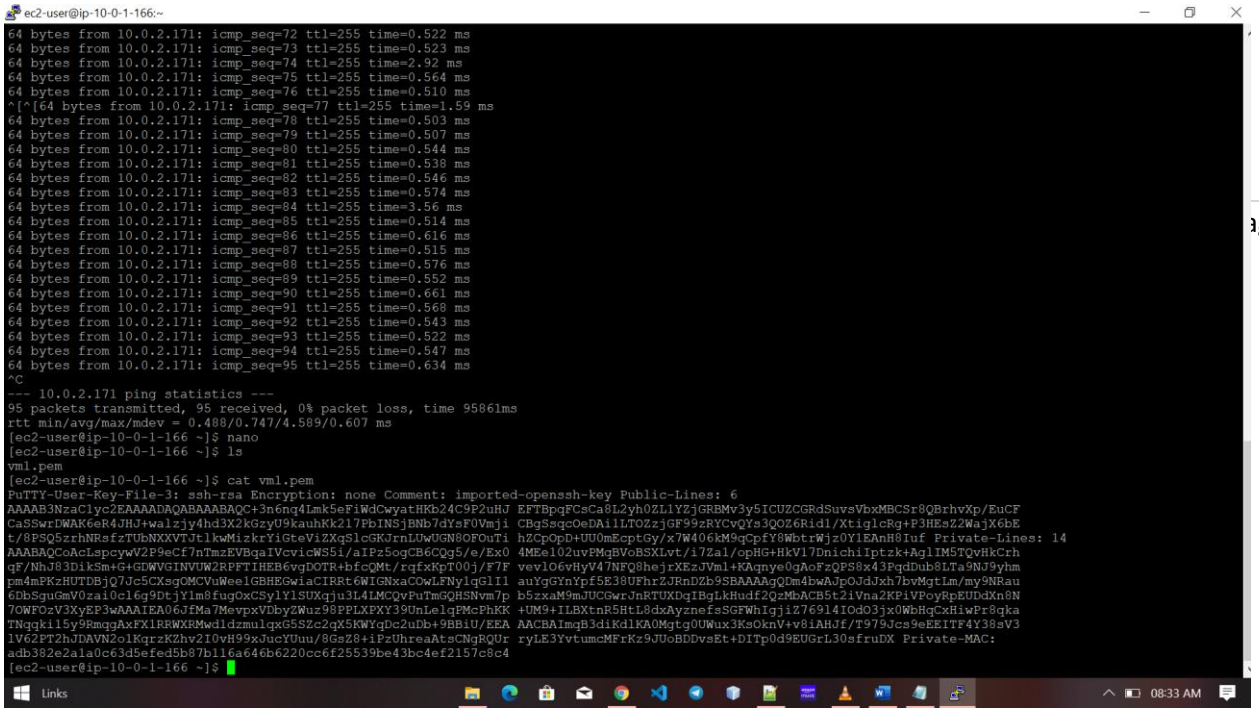


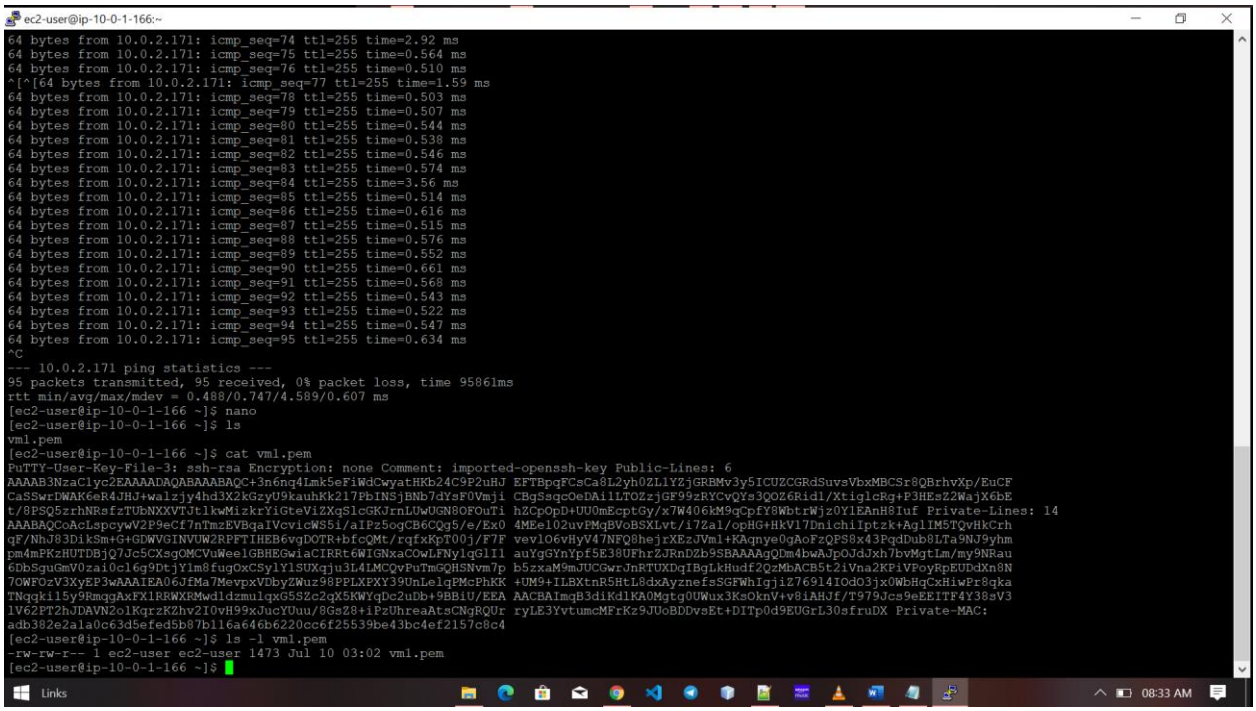

ec2-user@ip-10-0-1-166:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-166 ~]$ ping 10.0.2.171
PING 10.0.2.171 (10.0.2.171) 56(84) bytes of data.
64 bytes from 10.0.2.171: icmp_seq=1 ttl=255 time=0.488 ms
64 bytes from 10.0.2.171: icmp_seq=2 ttl=255 time=0.589 ms
64 bytes from 10.0.2.171: icmp_seq=3 ttl=255 time=0.560 ms
64 bytes from 10.0.2.171: icmp_seq=4 ttl=255 time=0.580 ms
64 bytes from 10.0.2.171: icmp_seq=5 ttl=255 time=4.58 ms
64 bytes from 10.0.2.171: icmp_seq=6 ttl=255 time=0.538 ms
64 bytes from 10.0.2.171: icmp_seq=7 ttl=255 time=0.558 ms
64 bytes from 10.0.2.171: icmp_seq=8 ttl=255 time=0.540 ms
64 bytes from 10.0.2.171: icmp_seq=9 ttl=255 time=1.02 ms
64 bytes from 10.0.2.171: icmp_seq=10 ttl=255 time=0.577 ms
64 bytes from 10.0.2.171: icmp_seq=11 ttl=255 time=1.57 ms
64 bytes from 10.0.2.171: icmp_seq=12 ttl=255 time=0.545 ms
64 bytes from 10.0.2.171: icmp_seq=13 ttl=255 time=0.599 ms
64 bytes from 10.0.2.171: icmp_seq=14 ttl=255 time=1.77 ms
64 bytes from 10.0.2.171: icmp_seq=15 ttl=255 time=0.535 ms
64 bytes from 10.0.2.171: icmp_seq=16 ttl=255 time=0.553 ms
64 bytes from 10.0.2.171: icmp_seq=17 ttl=255 time=0.578 ms
64 bytes from 10.0.2.171: icmp_seq=18 ttl=255 time=0.549 ms
64 bytes from 10.0.2.171: icmp_seq=19 ttl=255 time=0.838 ms
64 bytes from 10.0.2.171: icmp_seq=20 ttl=255 time=0.523 ms
64 bytes from 10.0.2.171: icmp_seq=21 ttl=255 time=0.517 ms
64 bytes from 10.0.2.171: icmp_seq=22 ttl=255 time=0.588 ms
64 bytes from 10.0.2.171: icmp_seq=23 ttl=255 time=0.550 ms
64 bytes from 10.0.2.171: icmp_seq=24 ttl=255 time=0.510 ms
64 bytes from 10.0.2.171: icmp_seq=25 ttl=255 time=0.626 ms
64 bytes from 10.0.2.171: icmp_seq=26 ttl=255 time=0.618 ms
64 bytes from 10.0.2.171: icmp_seq=27 ttl=255 time=0.654 ms
64 bytes from 10.0.2.171: icmp_seq=28 ttl=255 time=0.561 ms
64 bytes from 10.0.2.171: icmp_seq=29 ttl=255 time=0.594 ms
64 bytes from 10.0.2.171: icmp_seq=30 ttl=255 time=0.525 ms
64 bytes from 10.0.2.171: icmp_seq=31 ttl=255 time=0.599 ms
64 bytes from 10.0.2.171: icmp_seq=32 ttl=255 time=0.562 ms
64 bytes from 10.0.2.171: icmp_seq=33 ttl=255 time=0.554 ms
64 bytes from 10.0.2.171: icmp_seq=34 ttl=255 time=1.19 ms
64 bytes from 10.0.2.171: icmp_seq=35 ttl=255 time=0.637 ms
Links
08:27 AM
Instances | EC2 Management Co
What Is My IP Address - See You
console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:instanceState=running;sort=instanceId
aws
Services
Abhijit
N. Virginia
Support
New EC2 Experience
Learn more
EC2 Dashboard
Events
Tags
Limits
INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
ELASTIC BLOCK
1 to 2 of 2
Status Checks
Alarm Status
Public DNS (IP
2/2 checks ...
None
recommendations. Learn more
Private DNS
ip-10-0-2-171.ec2.internal
Private IPs
10.0.2.171
Availability zone
us-east-1a
Security groups
privtateSecurity. view inbound rules. view outbound rules
Secondary private IPs
Scheduled events
No scheduled events
VPC ID
vpc-05fe71b968ea2109b (demovpc)
AMI ID
amzn2-ami-hvm-2.0.20210701.0-x86_64-gp2 (ami-0dc2d3e4c0f9ebd18)
Platform
Amazon Linux
Subnet ID
subnet-089671ebbf2fffe19
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Links
08:25 AM

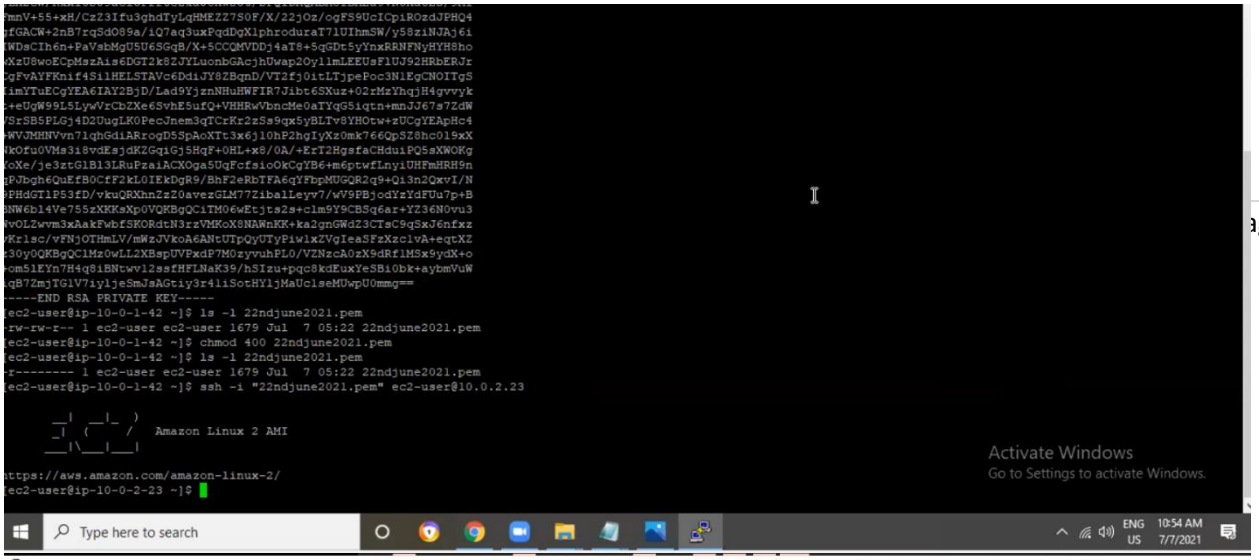

ec2-user@ip-10-0-1-166:~
64 bytes from 10.0.2.171: icmp_seq=57 ttl=255 time=0.590 ms
64 bytes from 10.0.2.171: icmp_seq=58 ttl=255 time=0.588 ms
64 bytes from 10.0.2.171: icmp_seq=59 ttl=255 time=0.548 ms
64 bytes from 10.0.2.171: icmp_seq=60 ttl=255 time=0.571 ms
64 bytes from 10.0.2.171: icmp_seq=61 ttl=255 time=0.494 ms
64 bytes from 10.0.2.171: icmp_seq=62 ttl=255 time=0.566 ms
64 bytes from 10.0.2.171: icmp_seq=63 ttl=255 time=0.542 ms
64 bytes from 10.0.2.171: icmp_seq=64 ttl=255 time=0.533 ms
^[64 bytes from 10.0.2.171: icmp_seq=65 ttl=255 time=0.517 ms
64 bytes from 10.0.2.171: icmp_seq=66 ttl=255 time=0.683 ms
64 bytes from 10.0.2.171: icmp_seq=67 ttl=255 time=0.579 ms
64 bytes from 10.0.2.171: icmp_seq=68 ttl=255 time=0.533 ms
64 bytes from 10.0.2.171: icmp_seq=69 ttl=255 time=0.491 ms
64 bytes from 10.0.2.171: icmp_seq=70 ttl=255 time=0.550 ms
64 bytes from 10.0.2.171: icmp_seq=71 ttl=255 time=0.714 ms
64 bytes from 10.0.2.171: icmp_seq=72 ttl=255 time=0.522 ms
64 bytes from 10.0.2.171: icmp_seq=73 ttl=255 time=0.523 ms
64 bytes from 10.0.2.171: icmp_seq=74 ttl=255 time=2.92 ms
64 bytes from 10.0.2.171: icmp_seq=75 ttl=255 time=0.564 ms
64 bytes from 10.0.2.171: icmp_seq=76 ttl=255 time=0.510 ms
^[^[64 bytes from 10.0.2.171: icmp_seq=77 ttl=255 time=1.59 ms
64 bytes from 10.0.2.171: icmp_seq=78 ttl=255 time=0.503 ms
64 bytes from 10.0.2.171: icmp_seq=79 ttl=255 time=0.507 ms
64 bytes from 10.0.2.171: icmp_seq=80 ttl=255 time=0.544 ms
64 bytes from 10.0.2.171: icmp_seq=81 ttl=255 time=0.538 ms
64 bytes from 10.0.2.171: icmp_seq=82 ttl=255 time=0.546 ms
64 bytes from 10.0.2.171: icmp_seq=83 ttl=255 time=0.574 ms
64 bytes from 10.0.2.171: icmp_seq=84 ttl=255 time=3.56 ms
64 bytes from 10.0.2.171: icmp_seq=85 ttl=255 time=0.514 ms
64 bytes from 10.0.2.171: icmp_seq=86 ttl=255 time=0.616 ms
64 bytes from 10.0.2.171: icmp_seq=87 ttl=255 time=0.515 ms
64 bytes from 10.0.2.171: icmp_seq=88 ttl=255 time=0.576 ms
64 bytes from 10.0.2.171: icmp_seq=89 ttl=255 time=0.552 ms
64 bytes from 10.0.2.171: icmp_seq=90 ttl=255 time=0.661 ms
64 bytes from 10.0.2.171: icmp_seq=91 ttl=255 time=0.568 ms
64 bytes from 10.0.2.171: icmp_seq=92 ttl=255 time=0.543 ms
64 bytes from 10.0.2.171: icmp_seq=93 ttl=255 time=0.522 ms
64 bytes from 10.0.2.171: icmp_seq=94 ttl=255 time=0.547 ms
64 bytes from 10.0.2.171: icmp_seq=95 ttl=255 time=0.634 ms
^C
--- 10.0.2.171 ping statistics ---
95 packets transmitted, 95 received, 0% packet loss, time 95861ms
rtt min/avg/max/mdev = 0.488/0.747/4.589/0.607 ms
[ec2-user@ip-10-0-1-166 ~]$
Links
08:27 AM

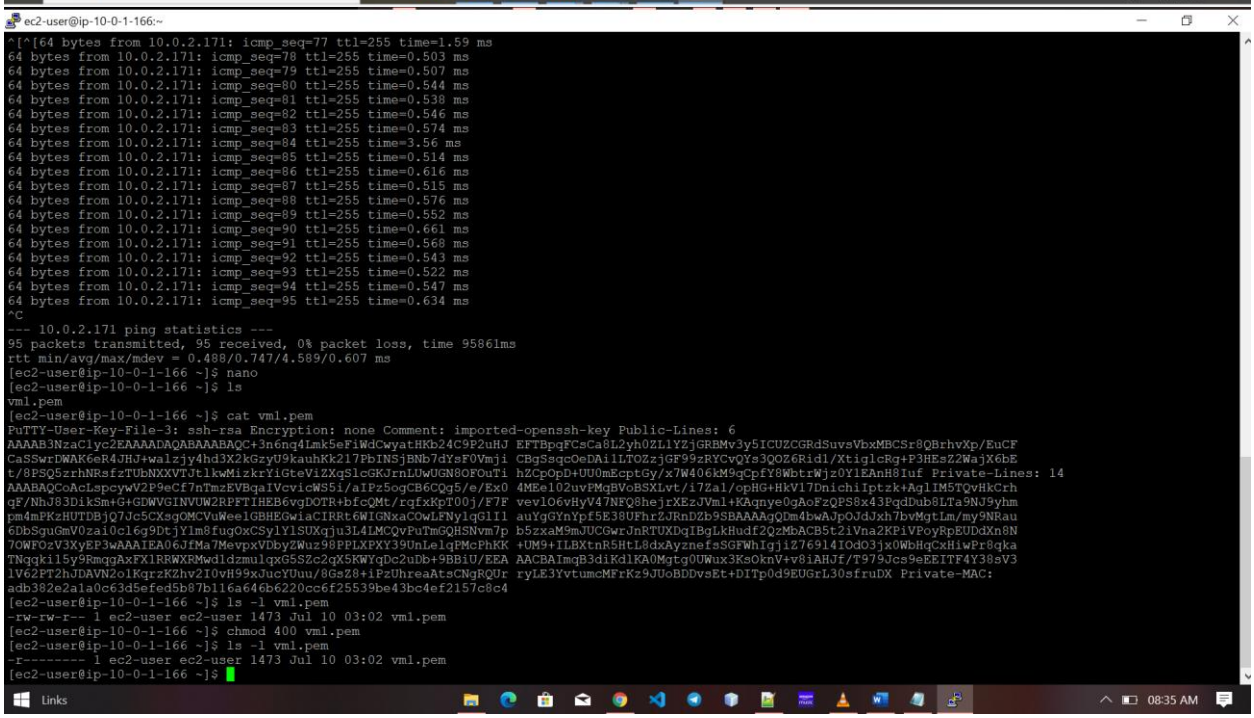

ec2-user@ip-10-0-1-166:~
GNU nano 2.9.8
New Buffer
Modified
PuTTY-User-Key-File-3: ssh-rsa Encryption: none Comment: imported-openssh-key Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAABAQC+3n6nq4Lmk5eFiWdCwyatHKb24C9P2uHJ EFTBpqFCsCa8L2yh0ZL1YZjGRBMv3y5ICUZCGRdSuvsVbxMBCSr8QBrhvXp/EuCF
CaSSwrDWAK6eR4JHJ+walzjy4hd3X2kGzyU9kauhKk217PbINSjBNb7dYsF0Vmji CBgSsqcOeDAi1LTOZzjGF99zRYCvQYs3QOZ6Ridl/XtiglcRq+P3HEsZ2WajX6bE
t/8PSQ5zrhNRsfzTUbNXXVTJtlkwMizkrYiGteViZXqSlcGKJrnLUwUGN8OFOuTi hZCpOpD+UU0mEcptGy/x7W406kM9qCpfY8WbtrWjz0YlEAnH8Iuf Private-Lines: 14
AAABAQCoAcLspcyWV2P9eCf7nTmzEVBqaIVcvicWS5i/aIPz5ogCB6CQg5/e/Ex0 4MEe102uvPMqBVoBSXLvt/i7Zal/opHG+HkV17DnichiIptzk+AglIM5TQvHkCrh
qF/NhJ83DikSm+G+GDWVGINVUW2RPFTIHEB6vgDOTR+bfcQMt/rqfxKpT00j/F7F vevlO6vHyV47NFQ8hejrXEzJVml+KAqnye0qAoFzQPS8x43PqdDub8LTa9NJ9yhm
pm4mPKzHUTDBjQ7Jc5CXsgOMCVuWeelGBHEGwiaCIRRt6WIGNxaCOwLFNylqGlI1 auYgGYnYpf5E38UFhrZJRnDZb9SBAAAAgQDm4bwAJpOJdJxh7bvMgtLm/my9NRau
6DbSguGmV0zai0cl6q9DtjYlm8fugOxCSylYlSUXqju3L4LMCQvPuTmGQHSNvm7p b5zxaM9mJUCGWrJnRTUXDqIBgLkHudf2QzMbACB5t2iVna2KPiVPoyRpEUDdXn8N
7OWFOzV3XyEP3wAAAIEAO6JfMa7MevpxVDbyZWuz98PPLXPXY39UnLelgPMcPhKK +UM9+ILBXtnR5HtL8dxAyznefsSGFWhIgjiZ76914IOdO3jxOWbHqCxHiwPr8qka
TNqqki15y9RmqgAxFXlRRWXRMwdldzmulqxG5SZc2qX5KWYqDc2uDb+9BBiU/EEA AACBAImqB3diKdlKAOMgtgOUWux3KsOknV+v8iAHJf/T979Jcs9eEEITf4Y38sV3
lV62PT2hJDAVN2olKqrzKZhv2IOvH99xJucYUuu/8GsZ8+iPzUhreaAtsCNgRQUr ryLE3YvtumcMFrKz9JUoBDDvsEt+DITp0d9EUGrL30sfruDX Private-MAC:
adb382e2a1a0c63d5efed5b87b116a646b6220cc6f25539be43bc4ef2157c8c4
{ Can now UnJustify! }
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Unjustify ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text M-W WhereIs Next
Links
08:31 AM

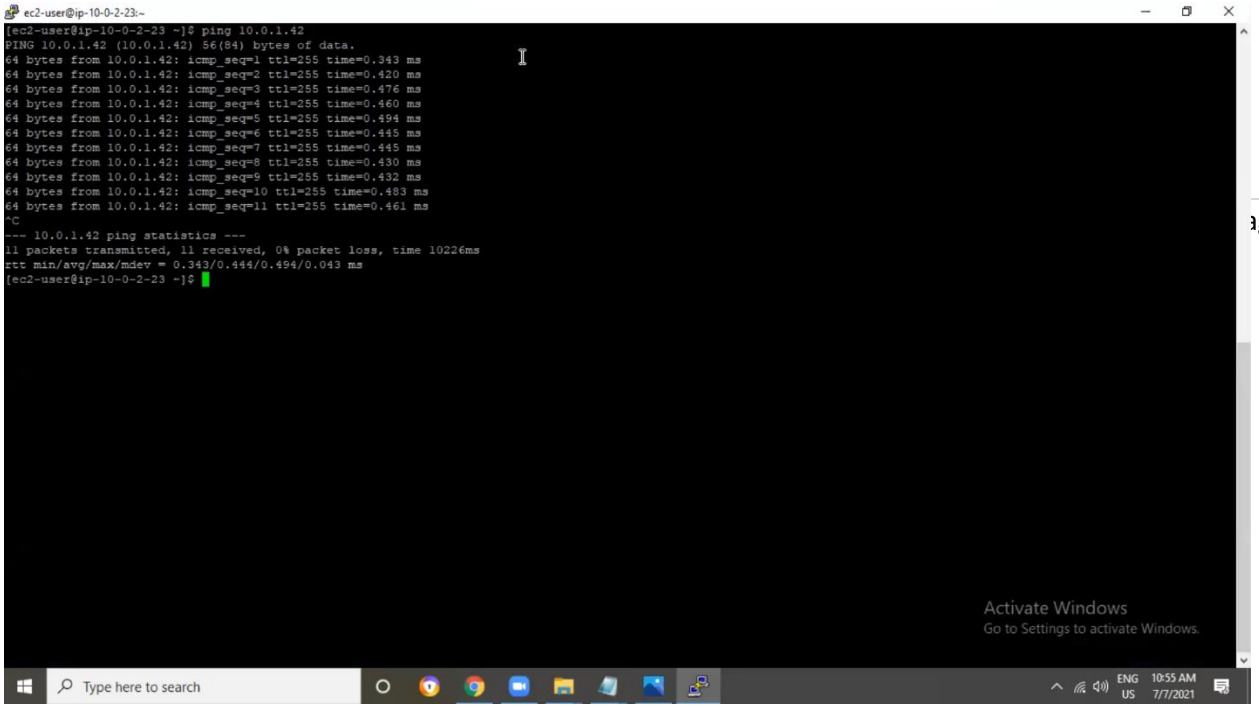

ec2-user@ip-10-0-1-166:~
64 bytes from 10.0.2.171: icmp_seq=60 ttl=255 time=0.571 ms
64 bytes from 10.0.2.171: icmp_seq=61 ttl=255 time=0.494 ms
64 bytes from 10.0.2.171: icmp_seq=62 ttl=255 time=0.566 ms
64 bytes from 10.0.2.171: icmp_seq=63 ttl=255 time=0.542 ms
64 bytes from 10.0.2.171: icmp_seq=64 ttl=255 time=0.533 ms
^[64 bytes from 10.0.2.171: icmp_seq=65 ttl=255 time=0.517 ms
64 bytes from 10.0.2.171: icmp_seq=66 ttl=255 time=0.683 ms
64 bytes from 10.0.2.171: icmp_seq=67 ttl=255 time=0.579 ms
64 bytes from 10.0.2.171: icmp_seq=68 ttl=255 time=0.533 ms
64 bytes from 10.0.2.171: icmp_seq=69 ttl=255 time=0.491 ms
64 bytes from 10.0.2.171: icmp_seq=70 ttl=255 time=0.550 ms
64 bytes from 10.0.2.171: icmp_seq=71 ttl=255 time=0.714 ms
64 bytes from 10.0.2.171: icmp_seq=72 ttl=255 time=0.522 ms
64 bytes from 10.0.2.171: icmp_seq=73 ttl=255 time=0.523 ms
64 bytes from 10.0.2.171: icmp_seq=74 ttl=255 time=2.92 ms
64 bytes from 10.0.2.171: icmp_seq=75 ttl=255 time=0.564 ms
64 bytes from 10.0.2.171: icmp_seq=76 ttl=255 time=0.510 ms
^[^[64 bytes from 10.0.2.171: icmp_seq=77 ttl=255 time=1.59 ms
64 bytes from 10.0.2.171: icmp_seq=78 ttl=255 time=0.503 ms
64 bytes from 10.0.2.171: icmp_seq=79 ttl=255 time=0.507 ms
64 bytes from 10.0.2.171: icmp_seq=80 ttl=255 time=0.544 ms
64 bytes from 10.0.2.171: icmp_seq=81 ttl=255 time=0.538 ms
64 bytes from 10.0.2.171: icmp_seq=82 ttl=255 time=0.546 ms
64 bytes from 10.0.2.171: icmp_seq=83 ttl=255 time=0.574 ms
64 bytes from 10.0.2.171: icmp_seq=84 ttl=255 time=3.56 ms
64 bytes from 10.0.2.171: icmp_seq=85 ttl=255 time=0.514 ms
64 bytes from 10.0.2.171: icmp_seq=86 ttl=255 time=0.616 ms
64 bytes from 10.0.2.171: icmp_seq=87 ttl=255 time=0.515 ms
64 bytes from 10.0.2.171: icmp_seq=88 ttl=255 time=0.576 ms
64 bytes from 10.0.2.171: icmp_seq=89 ttl=255 time=0.552 ms
64 bytes from 10.0.2.171: icmp_seq=90 ttl=255 time=0.661 ms
64 bytes from 10.0.2.171: icmp_seq=91 ttl=255 time=0.568 ms
64 bytes from 10.0.2.171: icmp_seq=92 ttl=255 time=0.543 ms
64 bytes from 10.0.2.171: icmp_seq=93 ttl=255 time=0.522 ms
64 bytes from 10.0.2.171: icmp_seq=94 ttl=255 time=0.547 ms
64 bytes from 10.0.2.171: icmp_seq=95 ttl=255 time=0.634 ms
^C
--- 10.0.2.171 ping statistics ---
95 packets transmitted, 95 received, 0% packet loss, time 95861ms
rtt min/avg/max/mdev = 0.488/0.747/4.589/0.607 ms
[ec2-user@ip-10-0-1-166 ~]$ nano
[ec2-user@ip-10-0-1-166 ~]$ ls
vm1.pem
[ec2-user@ip-10-0-1-166 ~]$
Links
08:33 AM
ec2-user@ip-10-0-1-166:~
64 bytes from 10.0.2.171: icmp_seq=58 ttl=255 time=0.588 ms
64 bytes from 10.0.2.171: icmp_seq=59 ttl=255 time=0.548 ms
64 bytes from 10.0.2.171: icmp_seq=60 ttl=255 time=0.571 ms
64 bytes from 10.0.2.171: icmp_seq=61 ttl=255 time=0.494 ms
64 bytes from 10.0.2.171: icmp_seq=62 ttl=255 time=0.566 ms
64 bytes from 10.0.2.171: icmp_seq=63 ttl=255 time=0.542 ms
64 bytes from 10.0.2.171: icmp_seq=64 ttl=255 time=0.533 ms
^[64 bytes from 10.0.2.171: icmp_seq=65 ttl=255 time=0.517 ms
64 bytes from 10.0.2.171: icmp_seq=66 ttl=255 time=0.683 ms
64 bytes from 10.0.2.171: icmp_seq=67 ttl=255 time=0.579 ms
64 bytes from 10.0.2.171: icmp_seq=68 ttl=255 time=0.533 ms
64 bytes from 10.0.2.171: icmp_seq=69 ttl=255 time=0.491 ms
64 bytes from 10.0.2.171: icmp_seq=70 ttl=255 time=0.550 ms
64 bytes from 10.0.2.171: icmp_seq=71 ttl=255 time=0.714 ms
64 bytes from 10.0.2.171: icmp_seq=72 ttl=255 time=0.522 ms
64 bytes from 10.0.2.171: icmp_seq=73 ttl=255 time=0.523 ms
64 bytes from 10.0.2.171: icmp_seq=74 ttl=255 time=2.92 ms
64 bytes from 10.0.2.171: icmp_seq=75 ttl=255 time=0.564 ms
64 bytes from 10.0.2.171: icmp_seq=76 ttl=255 time=0.510 ms
^[^[64 bytes from 10.0.2.171: icmp_seq=77 ttl=255 time=1.59 ms
64 bytes from 10.0.2.171: icmp_seq=78 ttl=255 time=0.503 ms
64 bytes from 10.0.2.171: icmp_seq=79 ttl=255 time=0.507 ms
64 bytes from 10.0.2.171: icmp_seq=80 ttl=255 time=0.544 ms
64 bytes from 10.0.2.171: icmp_seq=81 ttl=255 time=0.538 ms
64 bytes from 10.0.2.171: icmp_seq=82 ttl=255 time=0.546 ms
64 bytes from 10.0.2.171: icmp_seq=83 ttl=255 time=0.574 ms
64 bytes from 10.0.2.171: icmp_seq=84 ttl=255 time=3.56 ms
64 bytes from 10.0.2.171: icmp_seq=85 ttl=255 time=0.514 ms
64 bytes from 10.0.2.171: icmp_seq=86 ttl=255 time=0.616 ms
64 bytes from 10.0.2.171: icmp_seq=87 ttl=255 time=0.515 ms
64 bytes from 10.0.2.171: icmp_seq=88 ttl=255 time=0.576 ms
64 bytes from 10.0.2.171: icmp_seq=89 ttl=255 time=0.552 ms
64 bytes from 10.0.2.171: icmp_seq=90 ttl=255 time=0.661 ms
64 bytes from 10.0.2.171: icmp_seq=91 ttl=255 time=0.568 ms
64 bytes from 10.0.2.171: icmp_seq=92 ttl=255 time=0.543 ms
64 bytes from 10.0.2.171: icmp_seq=93 ttl=255 time=0.522 ms
64 bytes from 10.0.2.171: icmp_seq=94 ttl=255 time=0.547 ms
64 bytes from 10.0.2.171: icmp_seq=95 ttl=255 time=0.634 ms
^C
--- 10.0.2.171 ping statistics ---
95 packets transmitted, 95 received, 0% packet loss, time 95861ms
rtt min/avg/max/mdev = 0.488/0.747/4.589/0.607 ms
[ec2-user@ip-10-0-1-166 ~]$ nano
[ec2-user@ip-10-0-1-166 ~]$
Links
08:32 AM

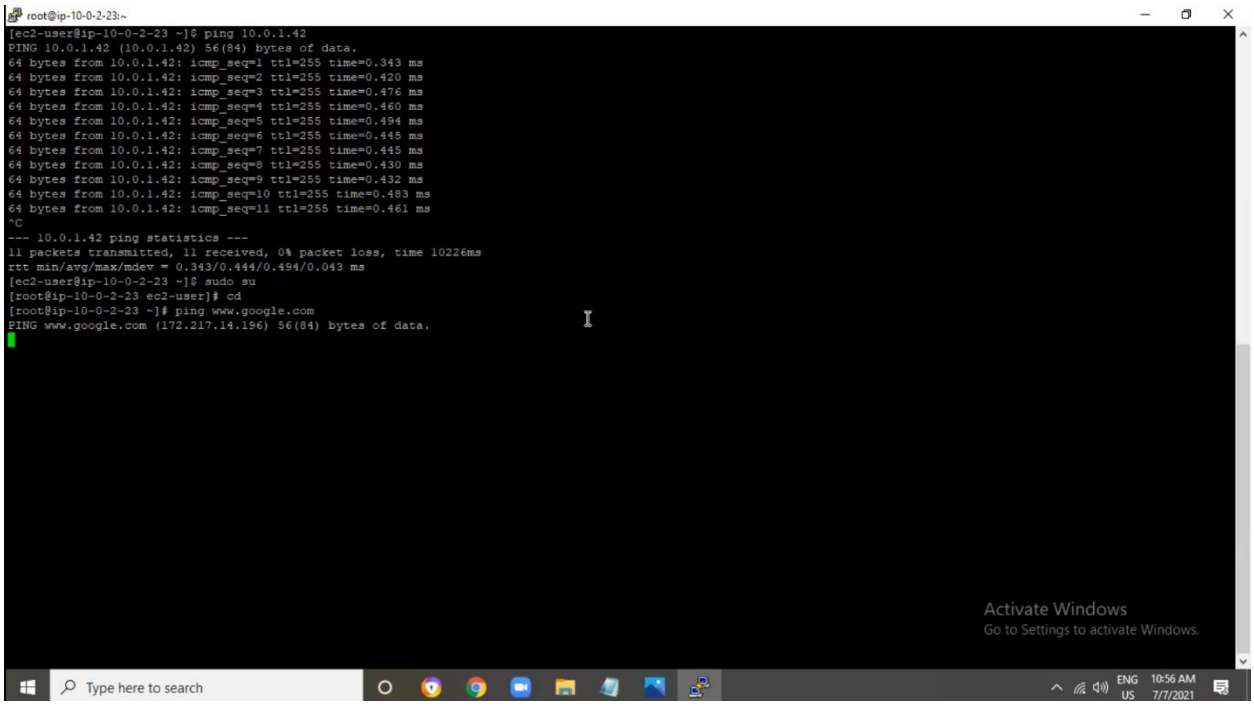

ec2-user@ip-10-0-1-166:~
64 bytes from 10.0.2.171: icmp_seq=72 ttl=255 time=0.522 ms
64 bytes from 10.0.2.171: icmp_seq=73 ttl=255 time=0.523 ms
64 bytes from 10.0.2.171: icmp_seq=74 ttl=255 time=2.92 ms
64 bytes from 10.0.2.171: icmp_seq=75 ttl=255 time=0.564 ms
64 bytes from 10.0.2.171: icmp_seq=76 ttl=255 time=0.510 ms
^[^[64 bytes from 10.0.2.171: icmp_seq=77 ttl=255 time=1.59 ms
64 bytes from 10.0.2.171: icmp_seq=78 ttl=255 time=0.503 ms
64 bytes from 10.0.2.171: icmp_seq=79 ttl=255 time=0.507 ms
64 bytes from 10.0.2.171: icmp_seq=80 ttl=255 time=0.544 ms
64 bytes from 10.0.2.171: icmp_seq=81 ttl=255 time=0.538 ms
64 bytes from 10.0.2.171: icmp_seq=82 ttl=255 time=0.546 ms
64 bytes from 10.0.2.171: icmp_seq=83 ttl=255 time=0.574 ms
64 bytes from 10.0.2.171: icmp_seq=84 ttl=255 time=3.56 ms
64 bytes from 10.0.2.171: icmp_seq=85 ttl=255 time=0.514 ms
64 bytes from 10.0.2.171: icmp_seq=86 ttl=255 time=0.616 ms
64 bytes from 10.0.2.171: icmp_seq=87 ttl=255 time=0.515 ms
64 bytes from 10.0.2.171: icmp_seq=88 ttl=255 time=0.576 ms
64 bytes from 10.0.2.171: icmp_seq=89 ttl=255 time=0.552 ms
64 bytes from 10.0.2.171: icmp_seq=90 ttl=255 time=0.661 ms
64 bytes from 10.0.2.171: icmp_seq=91 ttl=255 time=0.568 ms
64 bytes from 10.0.2.171: icmp_seq=92 ttl=255 time=0.543 ms
64 bytes from 10.0.2.171: icmp_seq=93 ttl=255 time=0.522 ms
64 bytes from 10.0.2.171: icmp_seq=94 ttl=255 time=0.547 ms
64 bytes from 10.0.2.171: icmp_seq=95 ttl=255 time=0.634 ms
^C
--- 10.0.2.171 ping statistics ---
95 packets transmitted, 95 received, 0% packet loss, time 95861ms
rtt min/avg/max/mdev = 0.488/0.747/4.589/0.607 ms
[ec2-user@ip-10-0-1-166 ~]$ nano
[ec2-user@ip-10-0-1-166 ~]$ ls
vm1.pem
[ec2-user@ip-10-0-1-166 ~]$ cat vm1.pem
PuTTY-User-Key-File-3: ssh-rsa Encryption: none Comment: imported-openssh-key Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAABAQC+3n6nq4Lmk5eFiWdCwyatHKb24C9P2uHJ EFTBpqFCsCa8L2yh0ZL1YZjGRBMv3y5ICUZCGRdSuvsVbxMBCSr8QBrhvXp/EuCF
CaSSwrDWAK6eR4JHJ+walzjy4hd3X2kGzyU9kauhKk217PbINSjBNb7dYsF0Vmji CBgSsqcOeDAi1LTOZzjGF99zRYCvQYs3QOZ6Rid1/XtiglcRg+P3HEsZ2WajX6bE
t/8PSQ5zrhNRsfzTUbNXXVTJtlkwMizkrYiGteViZXqSlcGKJrnLUwUGN8OFOuTi hZCpOpD+UU0mEcptGy/x7W406kM9qCpfY8WbtrWjz0YlEAnH8Iuf Private-Lines: 14
AAABAQCoAcLspcyWV2P9eCf7nTmzEVBqaIVcvicWS5i/aIPz5ogCB6CQg5/e/Ex0 4MEe102uvPMqBVoBSXLvt/i7Zal/opHG+HkVl7DnichiIptzk+AglIM5TQvHkCrh
qF/NhJ83DikSm+G+GDWVGINVUW2RPFTIHEB6vgDOTR+bfcQMt/rqfxKpT00j/F7F vevlO6vHyV47NFQ8hejrXEzJVml+KAqnye0gAoFzQPS8x43PqdDub8LTa9NJ9yhm
pm4mPKzHUTDBjQ7Jc5CXsgOMCVuWee1GBHEGwiaCIRRt6WIGNxaCOwLFNylqGlI1 auYgGYnYpf5E38UFhrZJRnDZb9SBAAAAgQDm4bwAJpOJdJxh7bvMgtLm/my9NRau
6DbSguGmV0zai0cl6g9DtjY1m8fugOxCSylY1SUXqju3L4LMCQvPuTmGQHSNvm7p b5zxaM9mJUCGwrJnRTUXDqIBgLkHudf2QzMbACB5t2iVna2KPiVPoyRpEUDdXn8N
7OWFOzV3XyEP3wAAAIEA06JfMa7MevpxVDbyZWuz98PPLXPXY39UnLelqPMcPhKK +UM9+ILBXtnR5HtL8dxAyznefsSGFWhIgjiZ769l4IOdO3jx0WbHqCxHiwPr8qka
TNqqki15y9RmqgAxFX1RRWXRMwd1dzmulqxG5SZc2qX5KWYqDc2uDb+9BBiU/EEA AACBAImqB3diKdlKA0Mgtg0UWux3KsOknV+v8iAHJf/T979Jcs9eEEITF4Y38sV3
lV62PT2hJDAVN2olKqrzKZhv2I0vH99xJucYUuu/8GsZ8+iPzUhreaAtsCNgRQUr ryLE3YvtumcMFrKz9JUoBDDvsEt+DITp0d9EUGrL30sfruDX Private-MAC:
adb382e2a1a0c63d5efed5b87b116a646b6220cc6f25539be43bc4ef2157c8c4
[ec2-user@ip-10-0-1-166 ~]$
Links
08:33 AM

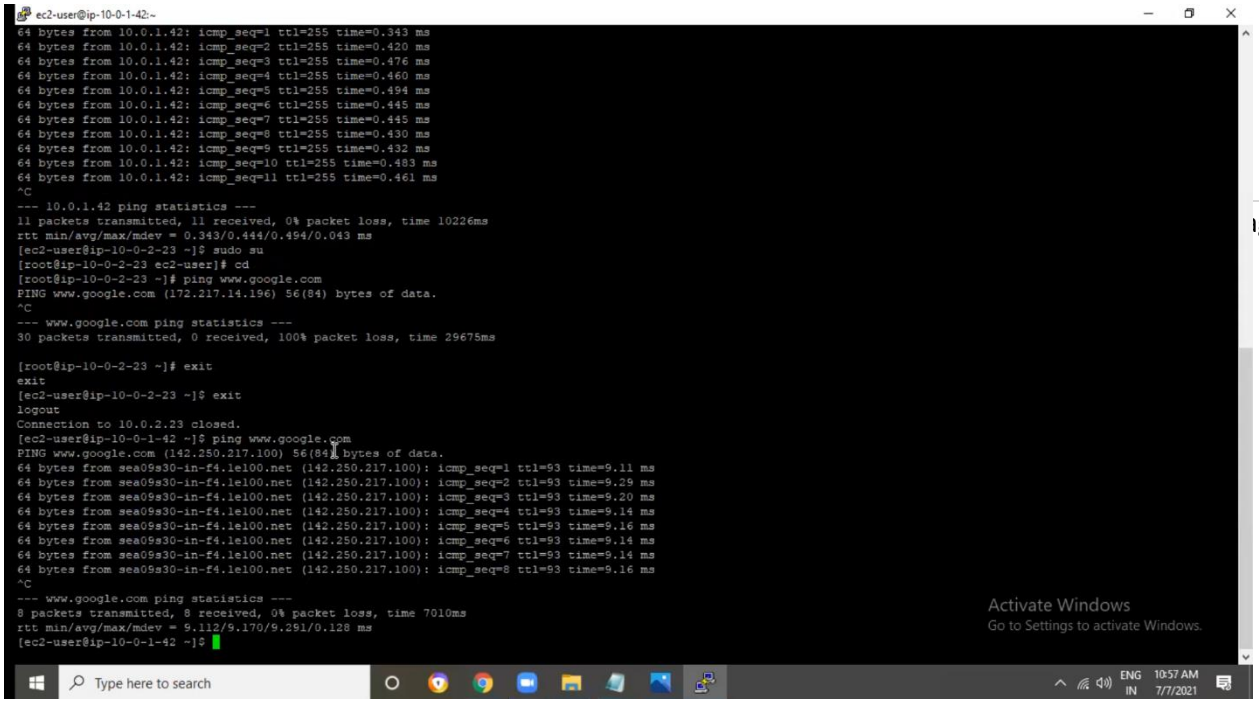

ec2-user@ip-10-0-1-166:~
64 bytes from 10.0.2.171: icmp_seq=74 ttl=255 time=2.92 ms
64 bytes from 10.0.2.171: icmp_seq=75 ttl=255 time=0.564 ms
64 bytes from 10.0.2.171: icmp_seq=76 ttl=255 time=0.510 ms
^[^[64 bytes from 10.0.2.171: icmp_seq=77 ttl=255 time=1.59 ms
64 bytes from 10.0.2.171: icmp_seq=78 ttl=255 time=0.503 ms
64 bytes from 10.0.2.171: icmp_seq=79 ttl=255 time=0.507 ms
64 bytes from 10.0.2.171: icmp_seq=80 ttl=255 time=0.544 ms
64 bytes from 10.0.2.171: icmp_seq=81 ttl=255 time=0.538 ms
64 bytes from 10.0.2.171: icmp_seq=82 ttl=255 time=0.546 ms
64 bytes from 10.0.2.171: icmp_seq=83 ttl=255 time=0.574 ms
64 bytes from 10.0.2.171: icmp_seq=84 ttl=255 time=3.56 ms
64 bytes from 10.0.2.171: icmp_seq=85 ttl=255 time=0.514 ms
64 bytes from 10.0.2.171: icmp_seq=86 ttl=255 time=0.616 ms
64 bytes from 10.0.2.171: icmp_seq=87 ttl=255 time=0.515 ms
64 bytes from 10.0.2.171: icmp_seq=88 ttl=255 time=0.576 ms
64 bytes from 10.0.2.171: icmp_seq=89 ttl=255 time=0.552 ms
64 bytes from 10.0.2.171: icmp_seq=90 ttl=255 time=0.661 ms
64 bytes from 10.0.2.171: icmp_seq=91 ttl=255 time=0.568 ms
64 bytes from 10.0.2.171: icmp_seq=92 ttl=255 time=0.543 ms
64 bytes from 10.0.2.171: icmp_seq=93 ttl=255 time=0.522 ms
64 bytes from 10.0.2.171: icmp_seq=94 ttl=255 time=0.547 ms
64 bytes from 10.0.2.171: icmp_seq=95 ttl=255 time=0.634 ms
^C
--- 10.0.2.171 ping statistics ---
95 packets transmitted, 95 received, 0% packet loss, time 95861ms
rtt min/avg/max/mdev = 0.488/0.747/4.589/0.607 ms
[ec2-user@ip-10-0-1-166 ~]$ nano
[ec2-user@ip-10-0-1-166 ~]$ ls
vm1.pem
[ec2-user@ip-10-0-1-166 ~]$ cat vm1.pem
PuTTY-User-Key-File-3: ssh-rsa Encryption: none Comment: imported-openssh-key Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAABAQC+3n6nq4Lmk5eFiWdCwyatHKb24C9P2uHJ EFTBpqFCsCa8L2yh0ZL1YZjGRBMv3y5ICUZCGRdSuvsVbxMBCSr8QBrhvXp/EuCF
CaSSwrDWAK6eR4JHJ+walzjy4hd3X2kGzyU9kauhKk217PbINSjBNb7dYsF0Vmji CBgSsqcOeDAi1LTOZzjGF99zRYCvQYs3QOZ6Rid1/XtiglcRg+P3HEsZ2WajX6bE
t/8PSQ5zrhNRsfzTUbNXXVTJtlkwMizkrYiGteViZXqSlcGKJrnLUwUGN8OFOuTi hZCpOpD+UU0mEcptGy/x7W406kM9qCpfY8WbtrWjz0YlEAnH8Iuf Private-Lines: 14
AAABAQCoAcLspcyWV2P9eCf7nTmzEVBqaIVcvicWS5i/aIPz5ogCB6CQg5/e/Ex0 4MEe102uvPMqBVoBSXLvt/i7Zal/opHG+HkVl7DnichiIptzk+AglIM5TQvHkCrh
qF/NhJ83DikSm+G+GDWVGINVUW2RPFTIHEB6vgDOTR+bfcQMt/rqfxKpT00j/F7F vevlO6vHyV47NFQ8hejrXEzJVml+KAqnye0gAoFzQPS8x43PqdDub8LTa9NJ9yhm
pm4mPKzHUTDBjQ7Jc5CXsgOMCVuWee1GBHEGwiaCIRRt6WIGNxaCOwLFNylqGlI1 auYgGYnYpf5E38UFhrZJRnDZb9SBAAAAgQDm4bwAJpOJdJxh7bvMgtLm/my9NRau
6DbSguGmV0zai0cl6g9DtjY1m8fugOxCSylY1SUXqju3L4LMCQvPuTmGQHSNvm7p b5zxaM9mJUCGwrJnRTUXDqIBgLkHudf2QzMbACB5t2iVna2KPiVPoyRpEUDdXn8N
7OWFOzV3XyEP3wAAAIEA06JfMa7MevpxVDbyZWuz98PPLXPXY39UnLelqPMcPhKK +UM9+ILBXtnR5HtL8dxAyznefsSGFWhIgjiZ769l4IOdO3jx0WbHqCxHiwPr8qka
TNqqki15y9RmqgAxFX1RRWXRMwd1dzmulqxG5SZc2qX5KWYqDc2uDb+9BBiU/EEA AACBAImqB3diKdlKA0Mgtg0UWux3KsOknV+v8iAHJf/T979Jcs9eEEITF4Y38sV3
lV62PT2hJDAVN2olKqrzKZhv2I0vH99xJucYUuu/8GsZ8+iPzUhreaAtsCNgRQUr ryLE3YvtumcMFrKz9JUoBDDvsEt+DITp0d9EUGrL30sfruDX Private-MAC:
adb382e2a1a0c63d5efed5b87b116a646b6220cc6f25539be43bc4ef2157c8c4
[ec2-user@ip-10-0-1-166 ~]$ ls -l vm1.pem
-rw-rw-r-- 1 ec2-user ec2-user 1473 Jul 10 03:02 vm1.pem
[ec2-user@ip-10-0-1-166 ~]$
Links
08:33 AM


mnV+55+xH/CzZ3Ifu3ghdTyLqHMEZZ7S0F/X/22jOz/ogFS9UcICpiROzdJPHQ4
fGACW+2nB7rqSdO89a/iQ7aq3uxPqdDqX1phroduraT7lUIhmSW/y58ziNJAj6i
WDsCIh6n+PaVsbMgU5U6SGqB/X+5CCQMVDDj4aT8+5qGDt5yYnxRRNFNyHYH8ho
kXzU8woECpMszAis6DGT2k8ZJYLuonbGAcjhUwap2Oy1lmLEEUsFlUJ92HRbERJr
gFvAYFKnif4SilHELSTAVc6DdiJY0ZBqnD/VT2fj0itLTjpePoc3NlEgCNOITgS
imYTuECgYEA6IAY2BjD/Lad9YjznNHuHWFIR7Jibt6SXuz+02rMzYhqjH4gvvyk
+eUgW99L5LywVrCbZXe65vhE5ufQ+VHHRwVbncMe0aTYqG5iqtn+mnJJ67s7ZdW
JSrSB5PLGj4D2OugLK0PecJnem3qTCrKr2zSs9qx5yBLTv8YHOtw+zUCgYEApHc4
WVJMHNVvn71qhGdiARrogD55pAoXTt3x6j10hP2hgIyXz0mk766QpSZ8hc019xX
kOfu0VMs3i8vdEsjdKZGqiGj5HqF+0HL+x8/0A/+ErT2HgsfaCHduiPQ5sXWOKg
oXe/je3ztGlBl3LRuPzaiACXOgA5UqFcfsioOkCgYB6+m6ptwfLnyiUHFmHRH9n
PJbgh6QuEfB0CfF2kL0IEkDgR9/BhF2eRbTFA6qYFbpMUGQR2q9+Qi3n2QxvI/N
PHdGT1P53fD/vkuQRXhnZzZ0avezGLM77ZibalLeyv7/wV9PBjodYzYdFUu7p+B
HW6b14Ve755zXKKsXp0VQKBgQCiTM06wEtjts2s+clm9Y9CBSq6ar+YZ36N0vu3
vOL2wvm3xAakFwbfSKORdtN3rzVMKoX8NAWnKK+ka2gnGWdZ3CTsC9qSxJ6nfxz
Krlsc/vFNjOTHmLV/mWzJVkoA6ANtUTpQyUTyPiwlxZVqIeaSFzXzclvA+eqtXZ
30y0QKBgQClMz0wLL2XBspUVPxdP7M0zyvuhPL0/VZNzcA0zX9dRf1MSx9ydX+o
om51EYn7H4q8iBNtwv12ssfHFLNaK39/hSIzu+pqc8kdEuxYe5Bi0bk+aybmVuW
qB7ZmjTGlV7iyljeSmJsAGtiy3r4liSotHYljMaUclseMUwpU0mmg==
-----END RSA PRIVATE KEY-----
[ec2-user@ip-10-0-1-42 ~]$ ls -l 22ndjune2021.pem
-rw-rw-r-- 1 ec2-user ec2-user 1679 Jul 7 05:22 22ndjune2021.pem
[ec2-user@ip-10-0-1-42 ~]$ chmod 400 22ndjune2021.pem
[ec2-user@ip-10-0-1-42 ~]$ ls -l 22ndjune2021.pem
-r-------- 1 ec2-user ec2-user 1679 Jul 7 05:22 22ndjune2021.pem
[ec2-user@ip-10-0-1-42 ~]$ ssh -i "22ndjune2021.pem" ec2-user@10.0.2.23
__| __|_)
_| (/ Amazon Linux 2 AMI
___|___|___|
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-2-23 ~]$
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG US
10:54 AM
7/7/2021


ec2-user@ip-10-0-1-166:~
^[^[64 bytes from 10.0.2.171: icmp_seq=77 ttl=255 time=1.59 ms
64 bytes from 10.0.2.171: icmp_seq=78 ttl=255 time=0.503 ms
64 bytes from 10.0.2.171: icmp_seq=79 ttl=255 time=0.507 ms
64 bytes from 10.0.2.171: icmp_seq=80 ttl=255 time=0.544 ms
64 bytes from 10.0.2.171: icmp_seq=81 ttl=255 time=0.538 ms
64 bytes from 10.0.2.171: icmp_seq=82 ttl=255 time=0.546 ms
64 bytes from 10.0.2.171: icmp_seq=83 ttl=255 time=0.574 ms
64 bytes from 10.0.2.171: icmp_seq=84 ttl=255 time=3.56 ms
64 bytes from 10.0.2.171: icmp_seq=85 ttl=255 time=0.514 ms
64 bytes from 10.0.2.171: icmp_seq=86 ttl=255 time=0.616 ms
64 bytes from 10.0.2.171: icmp_seq=87 ttl=255 time=0.515 ms
64 bytes from 10.0.2.171: icmp_seq=88 ttl=255 time=0.576 ms
64 bytes from 10.0.2.171: icmp_seq=89 ttl=255 time=0.552 ms
64 bytes from 10.0.2.171: icmp_seq=90 ttl=255 time=0.661 ms
64 bytes from 10.0.2.171: icmp_seq=91 ttl=255 time=0.568 ms
64 bytes from 10.0.2.171: icmp_seq=92 ttl=255 time=0.543 ms
64 bytes from 10.0.2.171: icmp_seq=93 ttl=255 time=0.522 ms
64 bytes from 10.0.2.171: icmp_seq=94 ttl=255 time=0.547 ms
64 bytes from 10.0.2.171: icmp_seq=95 ttl=255 time=0.634 ms
^C
--- 10.0.2.171 ping statistics ---
95 packets transmitted, 95 received, 0% packet loss, time 95861ms
rtt min/avg/max/mdev = 0.488/0.747/4.589/0.607 ms
[ec2-user@ip-10-0-1-166 ~]$ nano
[ec2-user@ip-10-0-1-166 ~]$ ls
vm1.pem
[ec2-user@ip-10-0-1-166 ~]$ cat vm1.pem
PuTTY-User-Key-File-3: ssh-rsa Encryption: none Comment: imported-openssh-key Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAABAQC+3n6nq4Lmk5eFiWdCwyatHKb24C9P2uHJ EFTBpqFCsCa8L2yh0ZL1YZjGRBMv3y5ICUZCGRdSuvsVbxMBCSr8QBrhvXp/EuCF
CaSSwrDWAK6eR4JHJ+walzjy4hd3X2kGzyU9kauhKk217PbINSjBNb7dYsF0Vmji CBgSsqcOeDAilLTOZzjGF99zRYCvQYs3QOZ6Rid1/XtiglcRg+P3HEsZ2WajX6bE
t/8PSQ5zrhNRsfzTUbNXXVTJtlkwMizkrYiGteViZXqSlcGKJrnLUwUGN8OFOuTi hZCpOpD+UU0mEcptGy/x7W406kM9qCpfY8WbtrWjz0Y1EAnH8Iuf Private-Lines: 14
AAABAQCoAcLspcywV2P9eCf7nTmzEVBqaIVcvicWS5i/aIPz5ogCB6CQg5/e/Ex0 4MEel02uvPMqBVoBSXLvt/i7Zal/opHG+HkV17DnichiIptzk+AglIM5TQvHkCrh
qF/NhJ83DikSm+G+GDWVGINVUW2RPFTIHEB6vgDOTR+bfcQMt/rqfxKpT00j/F7F vevlO6vHyV47NFQ8hejrXEzJVml+KAqnye0gAoFzQPS8x43PqdDub8LTa9NJ9yhm
pm4mPKzHUTDBjQ7Jc5CXsgOMCVuWeelGBHEGwiaCIRRt6WIGNxaCOwLFNylqGlI1 auYgGYnYpf5E38UFhrZJRnDZb9SBAAAAgQDm4bwAJpOJdJxh7bvMgtLm/my9NRau
6DbSguGmV0zai0cl6g9DtjYlm8fugOxCSylYlSUXqju3L4LMCQvPuTmGQHSNvm7p b5zxaM9mUCGwrJnRTUXDqIBgLkHudf2QzMbACB5t2iVna2KPiVPoyRpEUDdXn8N
7OWFOzV3XyEP3wAAAIEA06JfMa7MevpxVDbyZWuz98PPLXPXY39UnLelqPMcPhKK +UM9+ILBXtnR5HtL8dxAyznefsSGFWhIgjiZ76914IOdO3jx0WbHqCxHiwPr8qka
TNqqki15y9RmqgAxFXlRRWXRMwdldzmulqxG5SZc2qX5KWYqDc2uDb+9BBiU/EEA AACBAImqB3diKdlKA0Mgtg0UWux3KsOknV+v8iAHJf/T979Jcs9eEEITF4Y38sV3
lV62PT2hJDAVN2olKqrzKZhv2I0vH99xJucYUuu/8GsZ8+iPzUhreaAtsCNgRQUr ryLE3YvtumcMFrKz9JUoBDDvsEt+DITp0d9EUGrL30sfruDX Private-MAC:
adb382e2a1a0c63d5efed5b87b116a646b6220cc6f25539be43bc4ef2157c8c4
[ec2-user@ip-10-0-1-166 ~]$ ls -l vm1.pem
-rw-rw-r-- 1 ec2-user ec2-user 1473 Jul 10 03:02 vm1.pem
[ec2-user@ip-10-0-1-166 ~]$ chmod 400 vm1.pem
[ec2-user@ip-10-0-1-166 ~]$ ls -l vm1.pem
-r-------- 1 ec2-user ec2-user 1473 Jul 10 03:02 vm1.pem
[ec2-user@ip-10-0-1-166 ~]$
Links
08:35 AM


ec2-user@ip-10-0-2-23:~
[ec2-user@ip-10-0-2-23 ~]$ ping 10.0.1.42
PING 10.0.1.42 (10.0.1.42) 56(84) bytes of data.
64 bytes from 10.0.1.42: icmp_seq=1 ttl=255 time=0.343 ms
64 bytes from 10.0.1.42: icmp_seq=2 ttl=255 time=0.420 ms
64 bytes from 10.0.1.42: icmp_seq=3 ttl=255 time=0.476 ms
64 bytes from 10.0.1.42: icmp_seq=4 ttl=255 time=0.460 ms
64 bytes from 10.0.1.42: icmp_seq=5 ttl=255 time=0.494 ms
64 bytes from 10.0.1.42: icmp_seq=6 ttl=255 time=0.445 ms
64 bytes from 10.0.1.42: icmp_seq=7 ttl=255 time=0.445 ms
64 bytes from 10.0.1.42: icmp_seq=8 ttl=255 time=0.430 ms
64 bytes from 10.0.1.42: icmp_seq=9 ttl=255 time=0.432 ms
64 bytes from 10.0.1.42: icmp_seq=10 ttl=255 time=0.483 ms
64 bytes from 10.0.1.42: icmp_seq=11 ttl=255 time=0.461 ms
^C
--- 10.0.1.42 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10226ms
rtt min/avg/max/mdev = 0.343/0.444/0.494/0.043 ms
[ec2-user@ip-10-0-2-23 ~]$
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG US
10:55 AM
7/7/2021


root@ip-10-0-2-23:~
[ec2-user@ip-10-0-2-23 ~]$ ping 10.0.1.42
PING 10.0.1.42 (10.0.1.42) 56(84) bytes of data.
64 bytes from 10.0.1.42: icmp_seq=1 ttl=255 time=0.343 ms
64 bytes from 10.0.1.42: icmp_seq=2 ttl=255 time=0.420 ms
64 bytes from 10.0.1.42: icmp_seq=3 ttl=255 time=0.476 ms
64 bytes from 10.0.1.42: icmp_seq=4 ttl=255 time=0.460 ms
64 bytes from 10.0.1.42: icmp_seq=5 ttl=255 time=0.494 ms
64 bytes from 10.0.1.42: icmp_seq=6 ttl=255 time=0.445 ms
64 bytes from 10.0.1.42: icmp_seq=7 ttl=255 time=0.445 ms
64 bytes from 10.0.1.42: icmp_seq=8 ttl=255 time=0.430 ms
64 bytes from 10.0.1.42: icmp_seq=9 ttl=255 time=0.432 ms
64 bytes from 10.0.1.42: icmp_seq=10 ttl=255 time=0.483 ms
64 bytes from 10.0.1.42: icmp_seq=11 ttl=255 time=0.461 ms
^C
--- 10.0.1.42 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10226ms
rtt min/avg/max/mdev = 0.343/0.444/0.494/0.043 ms
[ec2-user@ip-10-0-2-23 ~]$ sudo su
[root@ip-10-0-2-23 ec2-user]# cd
[root@ip-10-0-2-23 ~]# ping www.google.com
PING www.google.com (172.217.14.196) 56(84) bytes of data.
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG US
10:56 AM
7/7/2021


ec2-user@ip-10-0-1-42:~
64 bytes from 10.0.1.42: icmp_seq=1 ttl=255 time=0.343 ms
64 bytes from 10.0.1.42: icmp_seq=2 ttl=255 time=0.420 ms
64 bytes from 10.0.1.42: icmp_seq=3 ttl=255 time=0.476 ms
64 bytes from 10.0.1.42: icmp_seq=4 ttl=255 time=0.460 ms
64 bytes from 10.0.1.42: icmp_seq=5 ttl=255 time=0.494 ms
64 bytes from 10.0.1.42: icmp_seq=6 ttl=255 time=0.445 ms
64 bytes from 10.0.1.42: icmp_seq=7 ttl=255 time=0.445 ms
64 bytes from 10.0.1.42: icmp_seq=8 ttl=255 time=0.430 ms
64 bytes from 10.0.1.42: icmp_seq=9 ttl=255 time=0.432 ms
64 bytes from 10.0.1.42: icmp_seq=10 ttl=255 time=0.483 ms
64 bytes from 10.0.1.42: icmp_seq=11 ttl=255 time=0.461 ms
^C
--- 10.0.1.42 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10226ms
rtt min/avg/max/mdev = 0.343/0.444/0.494/0.043 ms
[ec2-user@ip-10-0-2-23 ~]$ sudo su
[root@ip-10-0-2-23 ec2-user]# cd
[root@ip-10-0-2-23 ~]# ping www.google.com
PING www.google.com (172.217.14.196) 56(84) bytes of data.
^C
--- www.google.com ping statistics ---
30 packets transmitted, 0 received, 100% packet loss, time 29675ms
[root@ip-10-0-2-23 ~]# exit
exit
[ec2-user@ip-10-0-2-23 ~]$ exit
logout
Connection to 10.0.2.23 closed.
[ec2-user@ip-10-0-1-42 ~]$ ping www.google.com
PING www.google.com (142.250.217.100) 56(84) bytes of data.
64 bytes from sea09s30-in-f4.1e100.net (142.250.217.100): icmp_seq=1 ttl=93 time=9.11 ms
64 bytes from sea09s30-in-f4.1e100.net (142.250.217.100): icmp_seq=2 ttl=93 time=9.29 ms
64 bytes from sea09s30-in-f4.1e100.net (142.250.217.100): icmp_seq=3 ttl=93 time=9.20 ms
64 bytes from sea09s30-in-f4.1e100.net (142.250.217.100): icmp_seq=4 ttl=93 time=9.14 ms
64 bytes from sea09s30-in-f4.1e100.net (142.250.217.100): icmp_seq=5 ttl=93 time=9.16 ms
64 bytes from sea09s30-in-f4.1e100.net (142.250.217.100): icmp_seq=6 ttl=93 time=9.14 ms
64 bytes from sea09s30-in-f4.1e100.net (142.250.217.100): icmp_seq=7 ttl=93 time=9.14 ms
64 bytes from sea09s30-in-f4.1e100.net (142.250.217.100): icmp_seq=8 ttl=93 time=9.16 ms
^C
--- www.google.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 9.112/9.170/9.291/0.128 ms
[ec2-user@ip-10-0-1-42 ~]$
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
IN
10:57 AM
7/7/2021

Bibliography

Website used to gather information from :

- https://aws.amazon.com/free/

- https://aws.amazon.com/lightsail/projects/?trkCampaign=acq_paid_search_brand&sc_channel=PS&sc_campaign=acquisition_IN&sc_publisher=Google&sc_category=Cloud%20Computing&sc_country=IN&sc_geo=APAC&sc_outcome=acq&sc_detail=amazon%20lightsail&sc_content={ad%20group}&sc_matchtype=e&sc_segment=477000632060&sc_medium=ACQ-P|PS-GO|Brand|Desktop|SU|Cloud%20Computing|Lightsail|IN|EN|Sitelink&s_kwcid=AL!4422!3!477000632060!e!!g!!amazon%20lightsail&ef_id=CjwKCAjw3MSHBhB3EiwAxcaEuy0YzYkmLB_sm-FxG6N2eRz4kOtTweeGTjzSQtS1-yuYShj6PGUDTBoCBa8QAvD_BwE:G:s&s_kwcid=AL!4422!3!477000632060!e!!g!!amazon%20lightsail

- https://aws.amazon.com/lightsail/faq/?trkCampaign=acq_paid_search_brand&sc_channel=PS&sc_campaign=acquisition_IN&sc_publisher=Google&sc_category=Cloud%20Computing&sc_country=IN&sc_geo=APAC&sc_outcome=acq&sc_detail=amazon%20lightsail&sc_content={ad%20group}&sc_matchtype=e&sc_segment=477000632060&sc_medium=ACQ-P|PS-GO|Brand|Desktop|SU|Cloud%20Computing|Lightsail|IN|EN|Sitelink&s_kwcid=AL!4422!3!477000632060!e!!g!!amazon%20lightsail&ef_id=CjwKCAjw3MSHBhB3EiwAxcaEu9qzlf_35I238b0B1Yz7yo28jM2IpQX8PyHN1xf42ztHO4A3GaeMLhoCzKkQAvD_BwE:G:s&s_kwcid=AL!4422!3!477000632060!e!!g!!amazon%20lightsail

- https://aws.amazon.com/vpc/?vpc-blogs.sort-by=item.additionalFields.createdDate&vpc-blogs.sort-order=desc

- https://docs.aws.amazon.com/toolkit-for-visual-studio/latest/user-guide/vpc-tkv.html