

# Project - 3: Publishing Amazon SNS Messages Privately

**Industry:** Healthcare

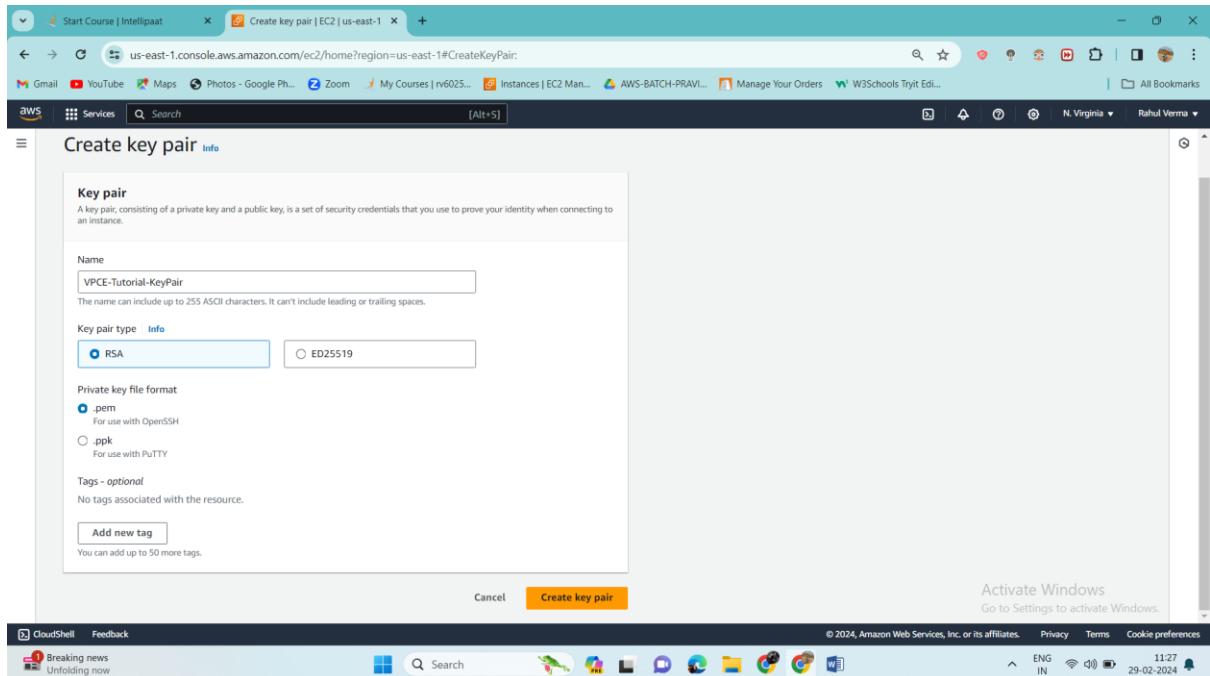
## **Problem Statement:**

How to secure patient records online and send it privately to the intended party Topics: In this project, you will be working on a hospital project to send reports online and develop a platform so the patients can access the reports via mobile and push notifications.

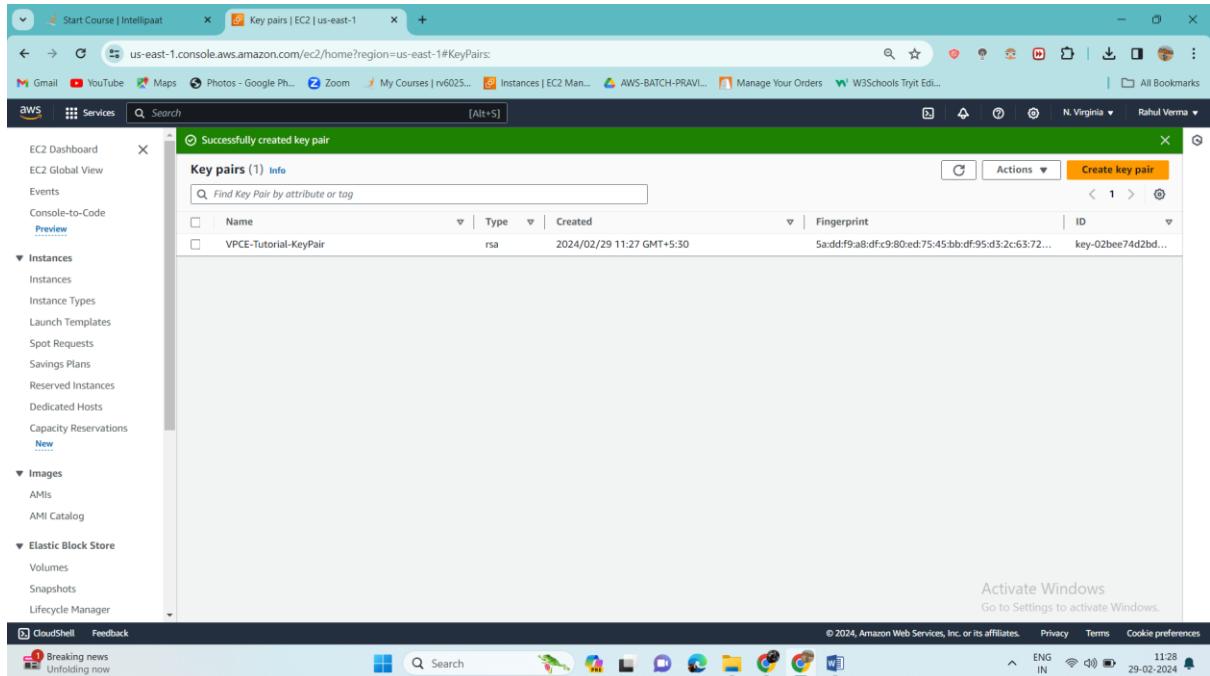
You will publish the report to an Amazon SNS keeping it secure and private. Your message will be hosted on an EC2 instance within your Amazon VPC. By publishing the messages privately, you can improve the message delivery and receipt through Amazon SNS. Highlights:

1. AWS CloudFormation to create a VPC
2. Connect VPC with AWS SNS
3. Publish message privately with SNS

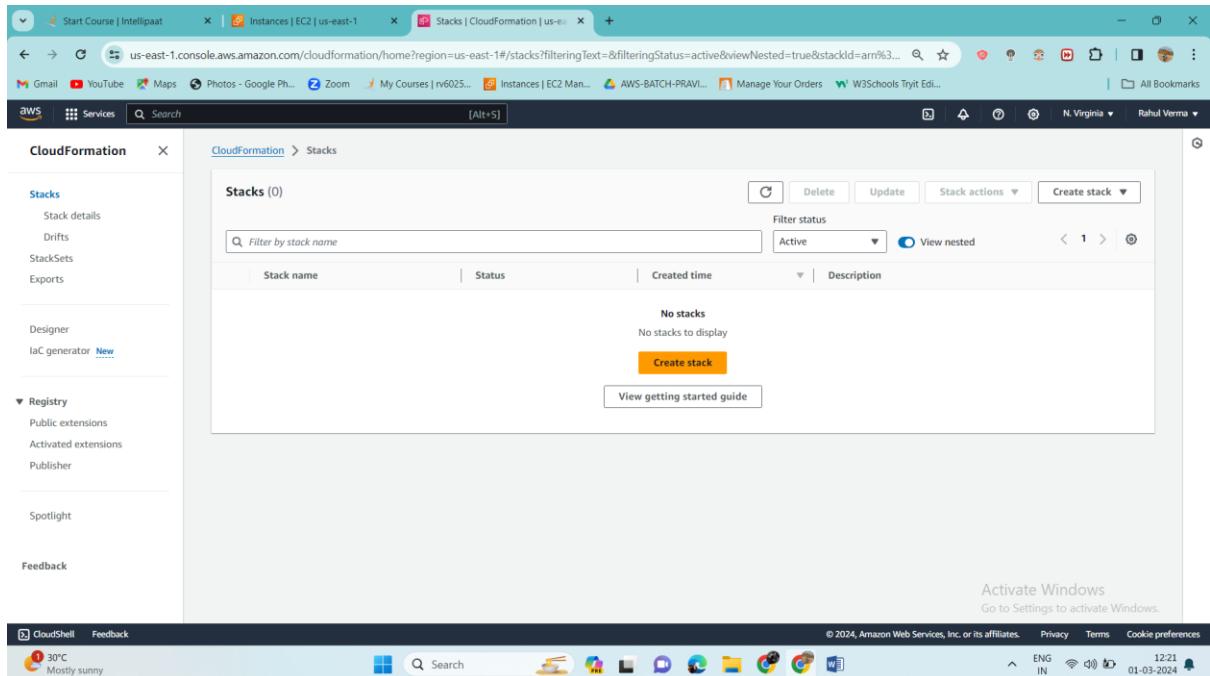
First let's create a key pair `VPCE-Tutorial-KeyPair`



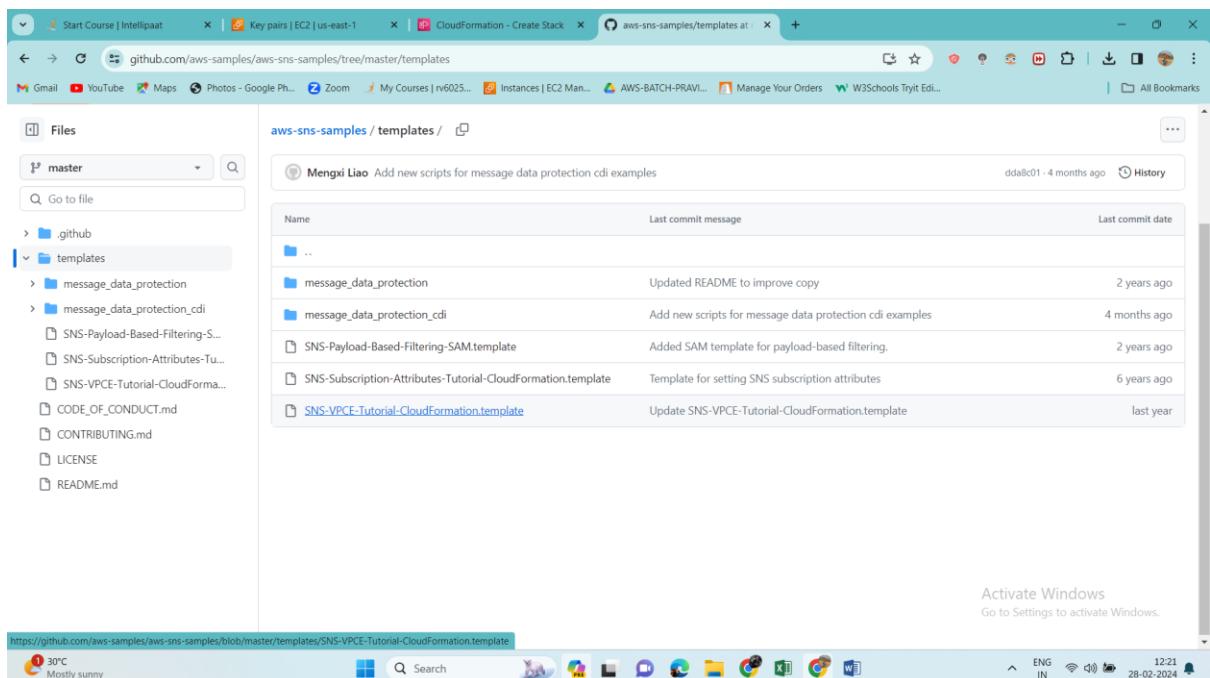
Successfully created



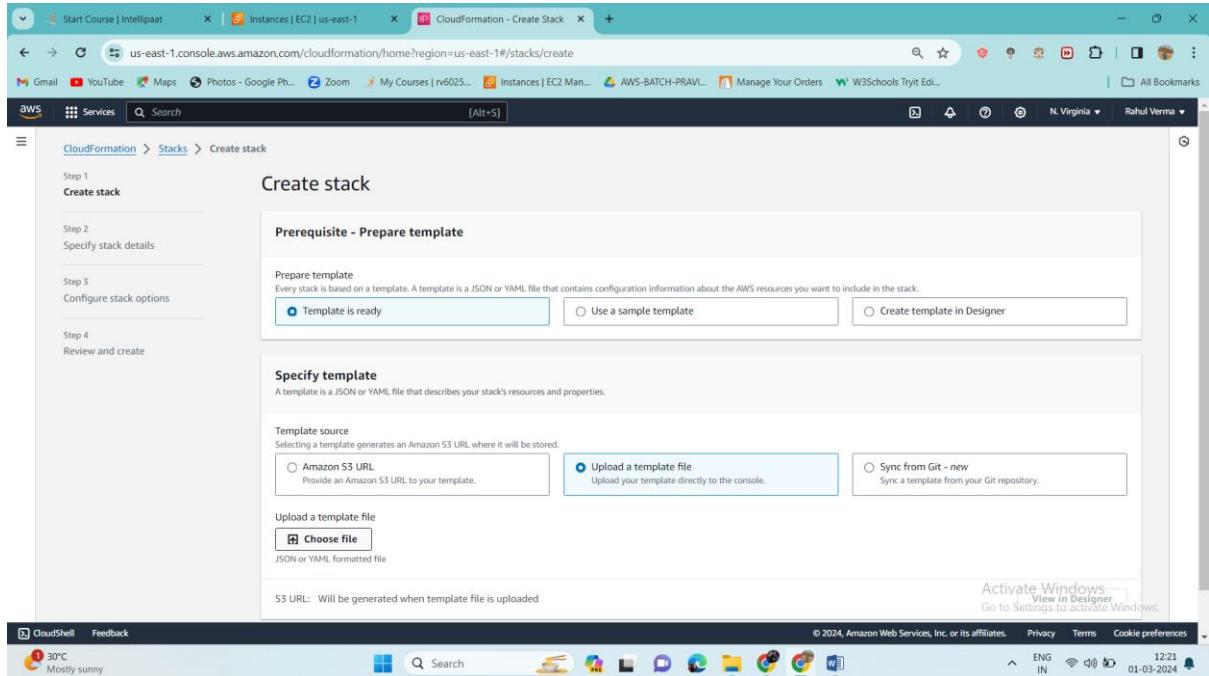
## Now let's create a stack



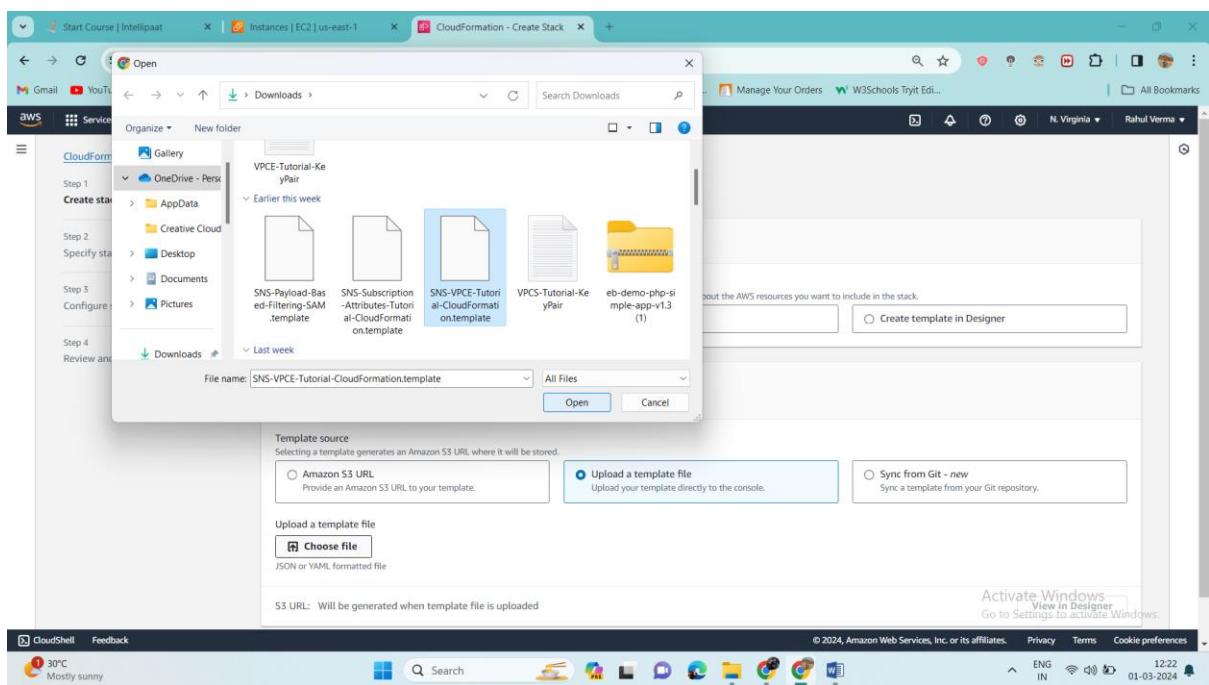
We are provided github link for this project we are gonna use the template from it.



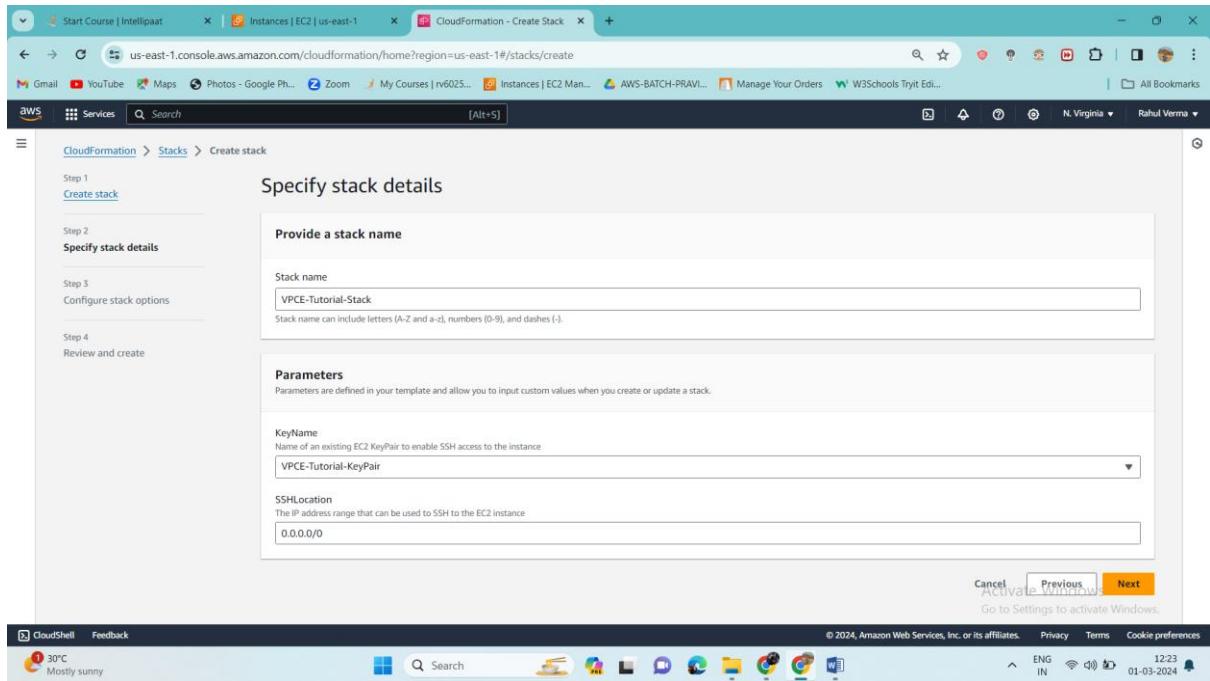
Will select template is ready and after that will select upload a template file option



Now we will choose our template file



Our stack name is VPCE-Tutorial-Stack and key pair which we have created



CloudFormation - Create Stack

Specify stack details

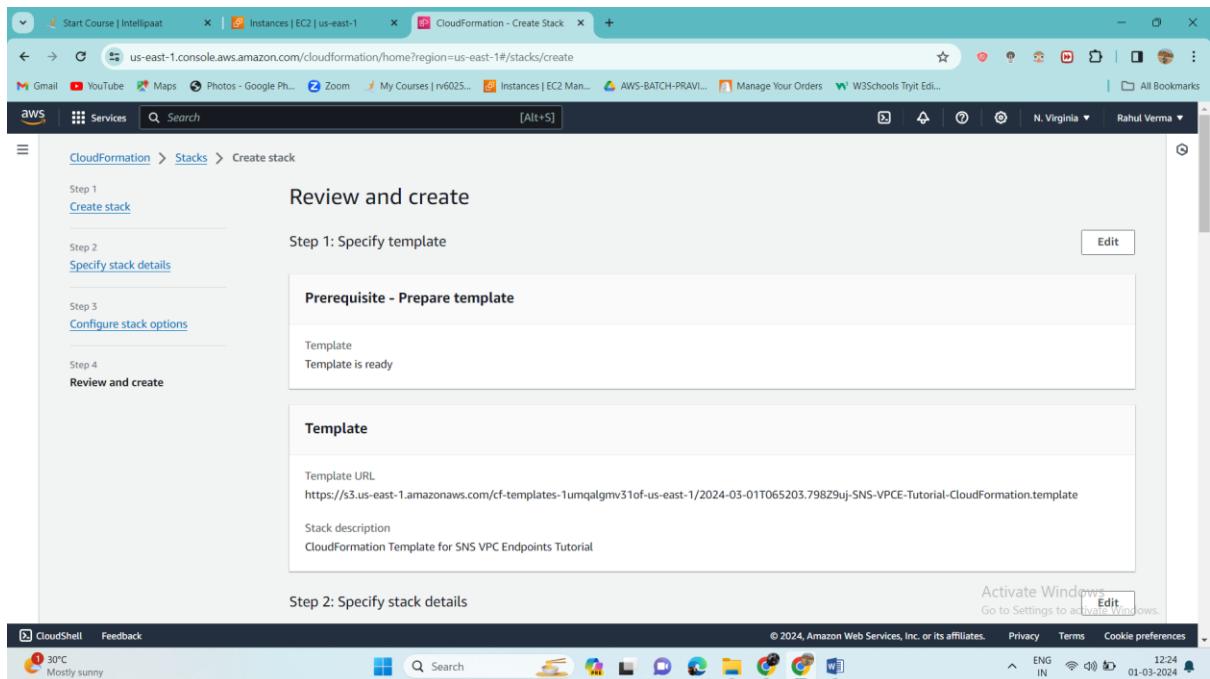
Stack name: VPCE-Tutorial-Stack

Parameters

KeyName: VPCE-Tutorial-KeyPair

SSHLocation: 0.0.0.0/0

Rest default settings



CloudFormation - Create Stack

Review and create

Step 1: Specify template

Prerequisite - Prepare template

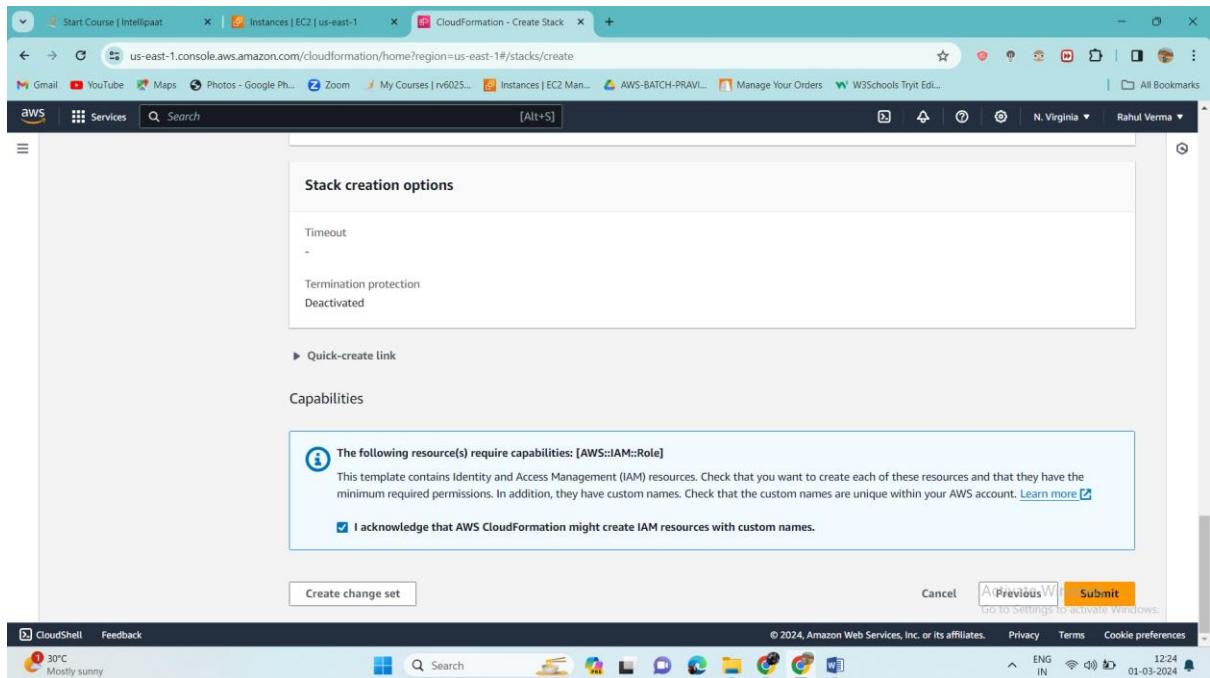
Template: Template is ready

Template URL: <https://s3.us-east-1.amazonaws.com/cf-templates-1umqalgrmv31of-us-east-1/2024-03-01T065203.798Z9uj-5NS-VPCE-Tutorial-CloudFormation.template>

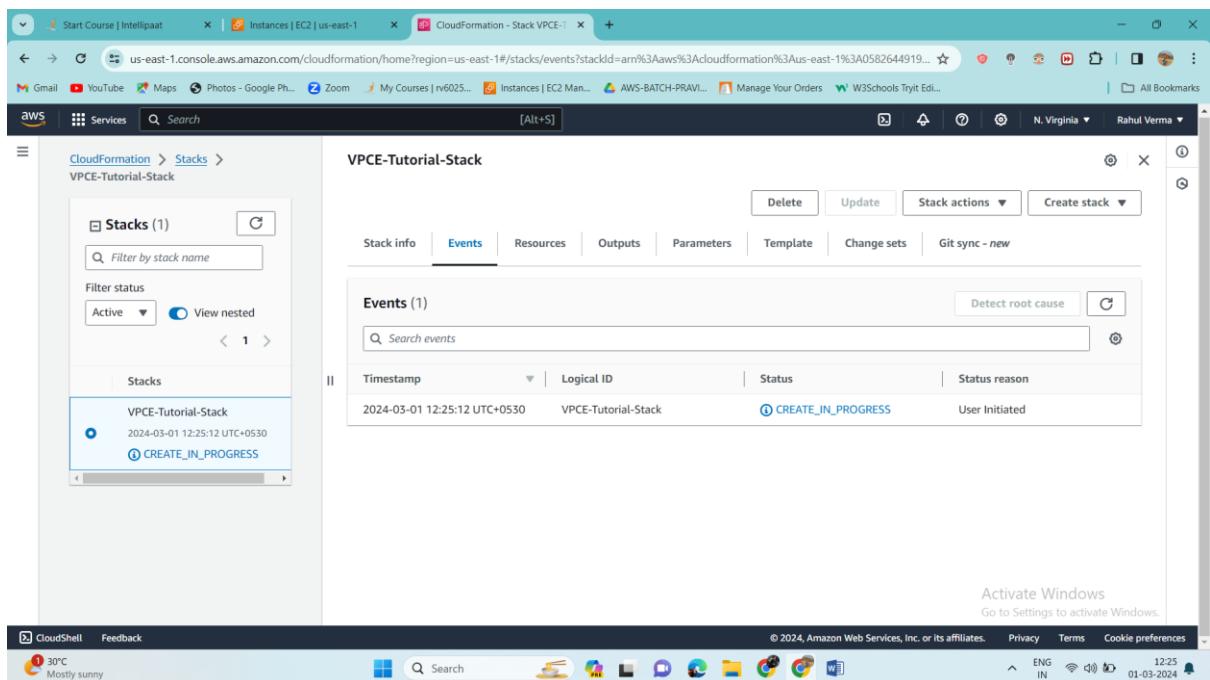
Stack description: CloudFormation Template for SNS VPC Endpoints Tutorial

Step 2: Specify stack details

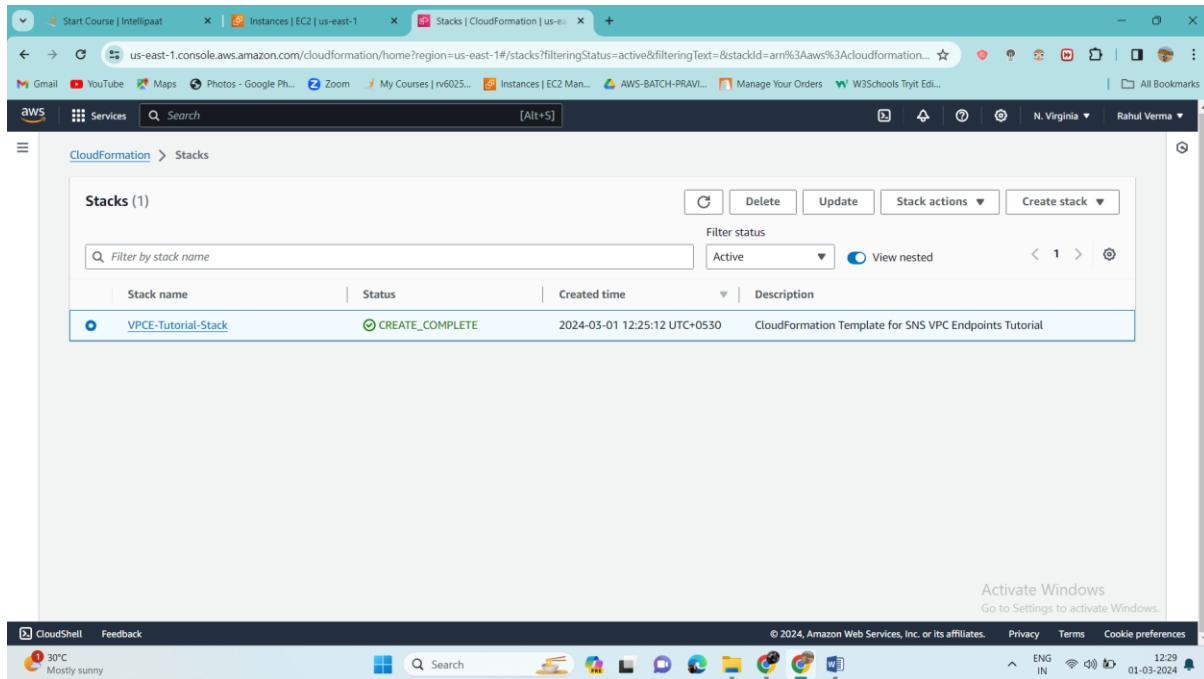
# Acknowledge and submit



# Our stack is under process

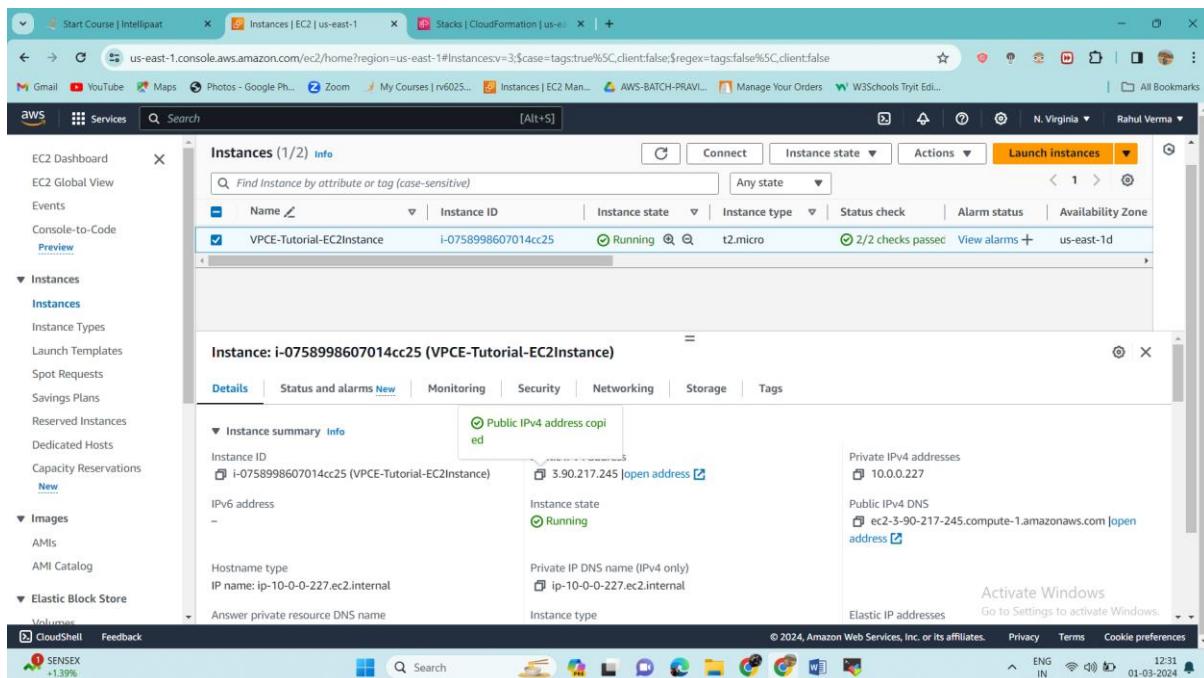


# Now it created successfully



The screenshot shows the AWS CloudFormation console with a single stack named 'VPCE-Tutorial-Stack' in the 'CREATE\_COMPLETE' status. The stack was created on 2024-03-01 at 12:25:12 UTC+0530. The description is 'CloudFormation Template for SNS VPC Endpoints Tutorial'. The AWS navigation bar at the top includes links for Start Course, Instances, Stacks, and CloudFormation. The bottom navigation bar shows CloudShell, Feedback, and various system icons.

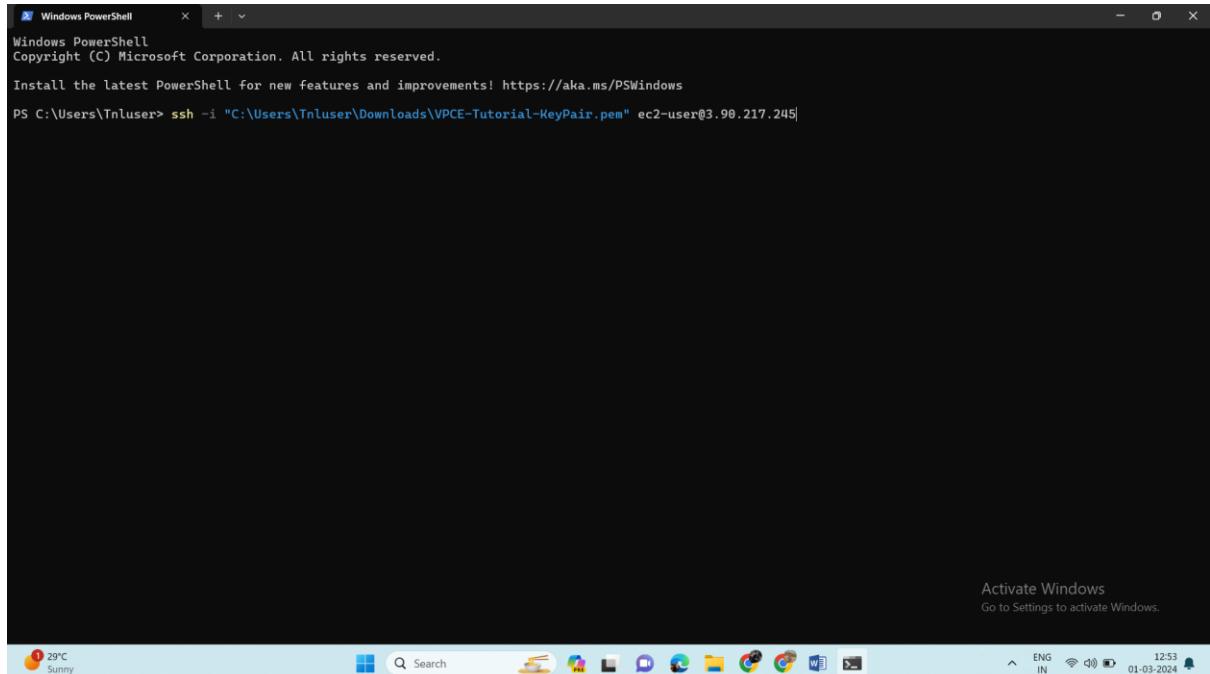
## Let's connect to our EC2 instance



The screenshot shows the AWS EC2 console with a list of instances. One instance, 'VPCE-Tutorial-EC2Instance' (i-0758998607014cc25), is shown in the 'Running' state. The instance type is t2.micro and it has passed 2/2 checks. The instance is located in the 'us-east-1d' availability zone. The AWS navigation bar at the top includes links for Start Course, Instances, Stacks, and CloudFormation. The bottom navigation bar shows CloudShell, Feedback, and various system icons.

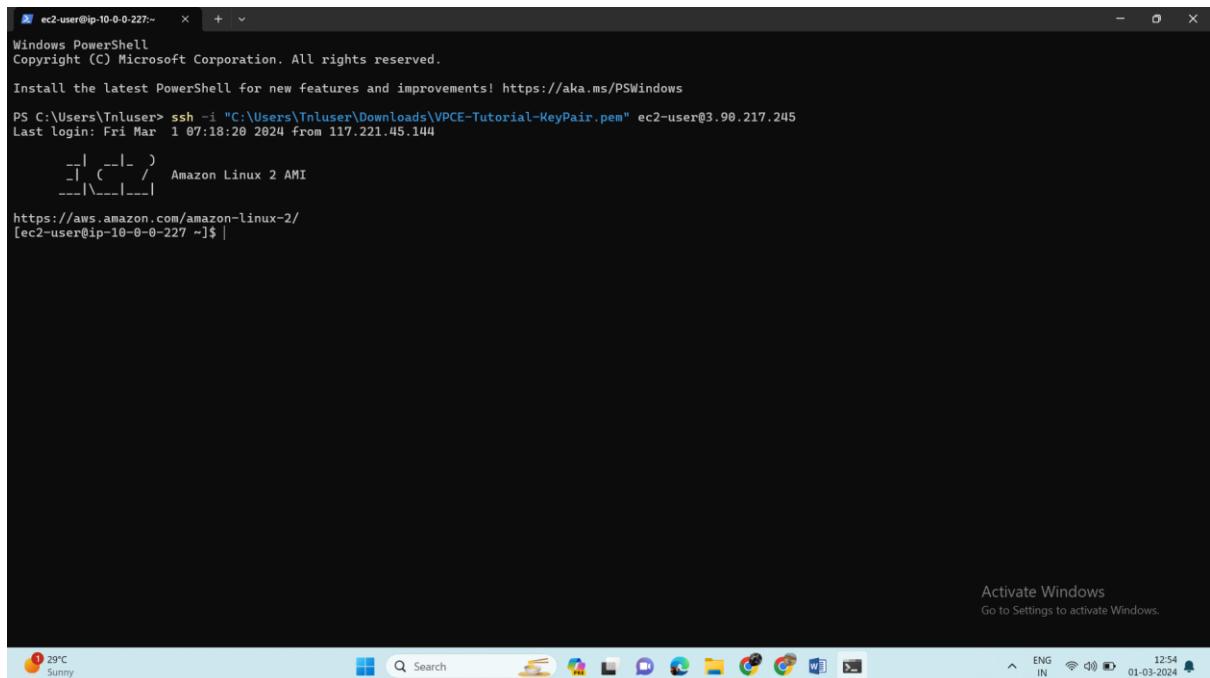
We are using cmd

```
ssh -i "C:\Users\Tnluser\Downloads\VPCE-Tutorial-KeyPair.Pem"  
ec2-user@(instance ip)
```



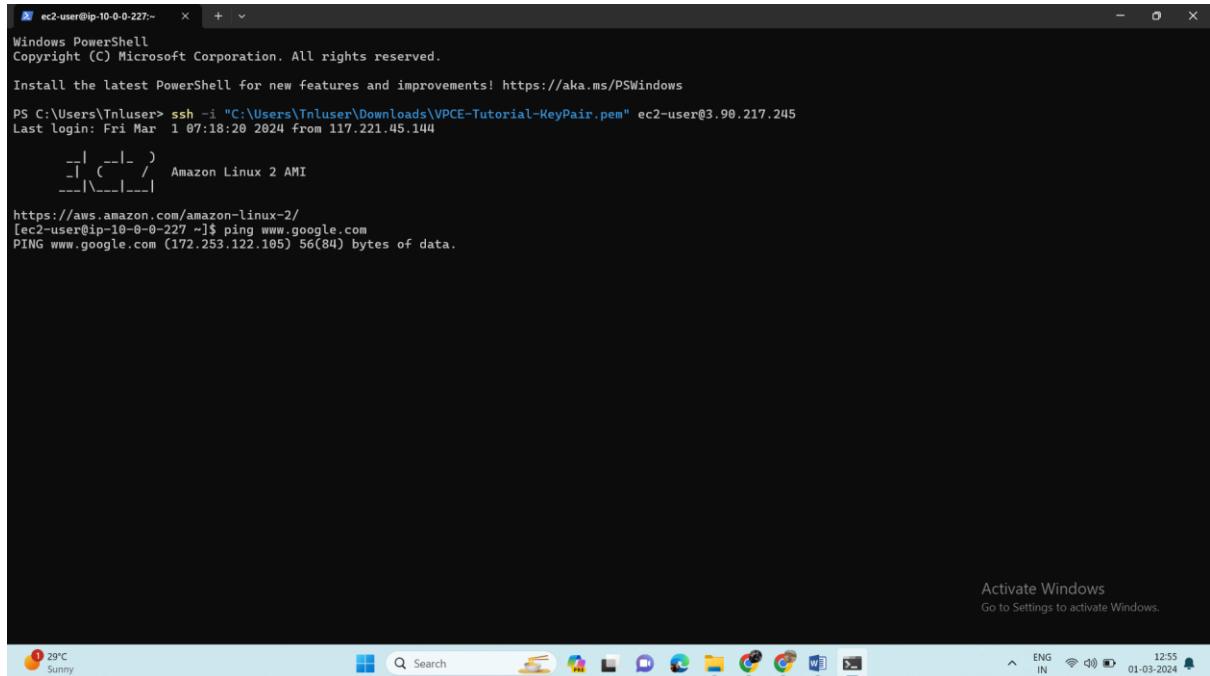
A screenshot of a Windows PowerShell window titled "Windows PowerShell". The command "ssh -i "C:\Users\Tnluser\Downloads\VPCE-Tutorial-KeyPair.Pem" ec2-user@(instance ip)" is typed into the window. The window is set against a dark background with a light blue taskbar at the bottom. The taskbar shows various icons for apps like File Explorer, Edge, and File History. The system tray on the right shows the date (01-03-2024), time (12:53), and battery status.

We have successfully logged in



A screenshot of a Windows PowerShell window titled "ec2-user@ip-10-0-0-227:~". The command "ssh -i "C:\Users\Tnluser\Downloads\VPCE-Tutorial-KeyPair.pem" ec2-user@3.98.217.245" was run, resulting in a successful login. The prompt shows the user is now on an Amazon Linux 2 AMI. The window has the same dark theme and light blue taskbar as the previous screenshot. The taskbar icons and system tray information are also present.

Now to check internet in our ec2 will ping google (we have ping it at 12:55 PM)



```
ec2-user@ip-10-0-0-227:~ + + 
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

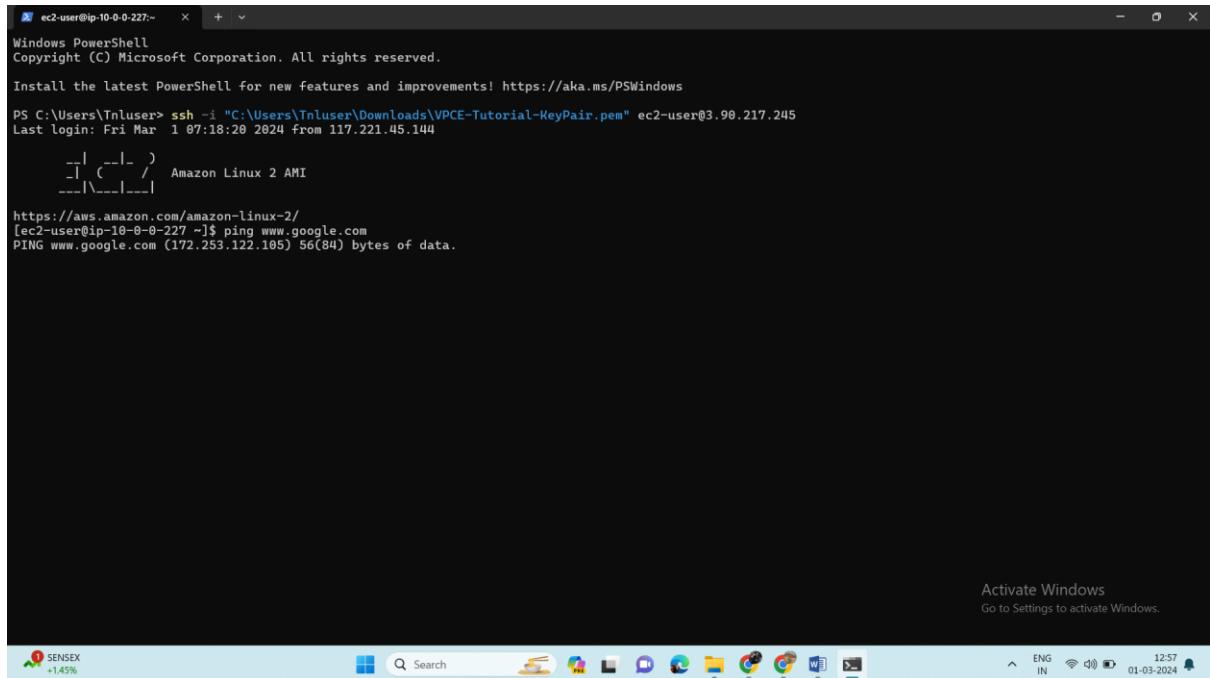
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Tnuser> ssh -i "C:\Users\Tnuser\Downloads\VPCE-Tutorial-KeyPair.pem" ec2-user@3.90.217.245
Last login: Fri Mar  1 07:18:20 2024 from 117.221.45.144
[ec2-user@ip-10-0-0-227 ~]$ ping www.google.com
PING www.google.com (172.253.122.105) 56(84) bytes of data.

Activate Windows
Go to Settings to activate Windows.

29°C
Sunny
12:55 01-03-2024
```

Let's check after two min if internet is working it should have sent packages.



```
ec2-user@ip-10-0-0-227:~ + + 
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

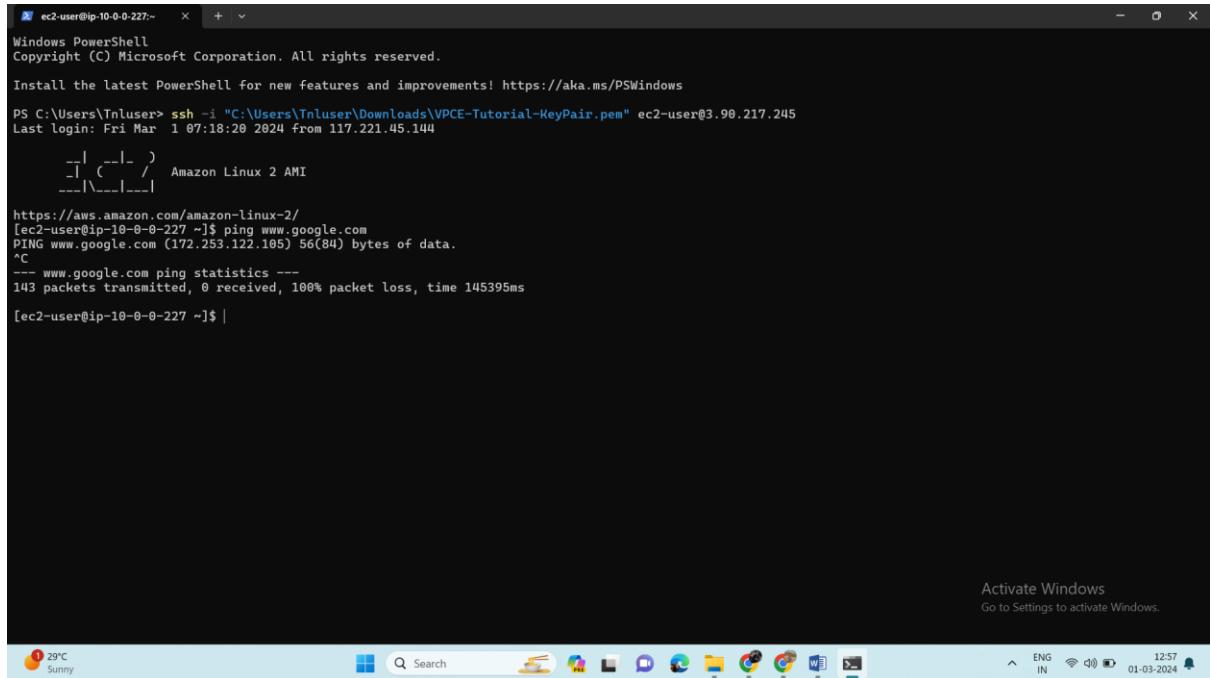
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Tnuser> ssh -i "C:\Users\Tnuser\Downloads\VPCE-Tutorial-KeyPair.pem" ec2-user@3.90.217.245
Last login: Fri Mar  1 07:18:20 2024 from 117.221.45.144
[ec2-user@ip-10-0-0-227 ~]$ ping www.google.com
PING www.google.com (172.253.122.105) 56(84) bytes of data.

Activate Windows
Go to Settings to activate Windows.

SENSEX +1.45%
12:57 01-03-2024
```

We have cancel it by **ctrl+c**



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Tnuser> ssh -i "C:\Users\Tnuser\Downloads\VPCE-Tutorial-KeyPair.pem" ec2-user@3.90.217.245
Last login: Fri Mar  1 07:18:28 2024 from 117.221.45.144
[ec2-user@ip-10-0-0-227 ~]$ ^C
[ec2-user@ip-10-0-0-227 ~]$
```

Activate Windows  
Go to Settings to activate Windows.

29°C Sunny

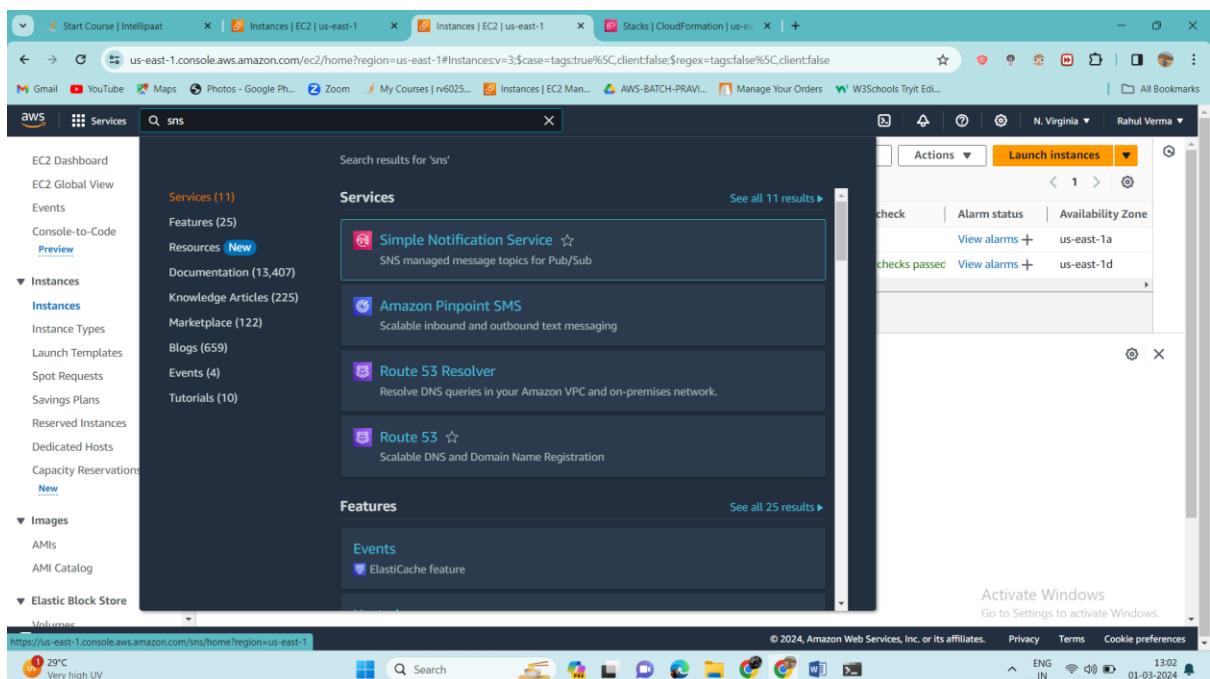
Search

ENG IN 12:57 01-03-2024

Now To verify that the instance lacks connectivity to Amazon SNS

We will attempt to publish a message to topic

For that first will go to sns in our aws console



Start Course | Intellipaat | Instances | EC2 | us-east-1 | Instances | EC2 | us-east-1 | Stacks | CloudFormation | us-east-1 | +

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instancesv3=\$case=true%5C;client=false;\$regex=tags:false%5C;client=false

Gmail YouTube Maps Photos - Google Photos Zoom My Courses | n6025... Instances | EC2 Man... AWS-BATCH-PRAVI... Manage Your Orders W3Schools Tryit Edit... All Bookmarks N. Virginia Rahul Verma

aws Services

Search results for 'sns'

Services (11)

Simple Notification Service ☆ SNS managed message topics for Pub/Sub

Amazon Pinpoint SMS Scalable inbound and outbound text messaging

Route 53 Resolver Resolve DNS queries in your Amazon VPC and on-premises network.

Route 53 ☆ Scalable DNS and Domain Name Registration

Features (25)

Events (4)

Tutorials (10)

Events

Elasticache feature

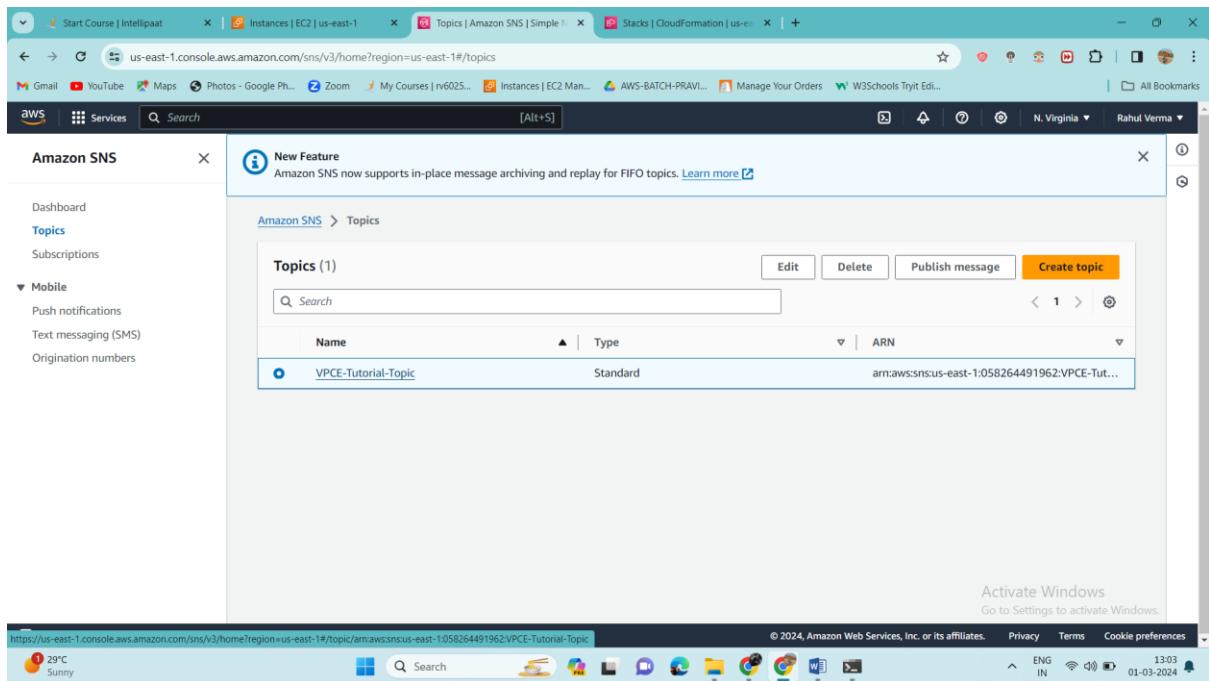
Activate Windows  
Go to Settings to activate Windows.

29°C Very high UV

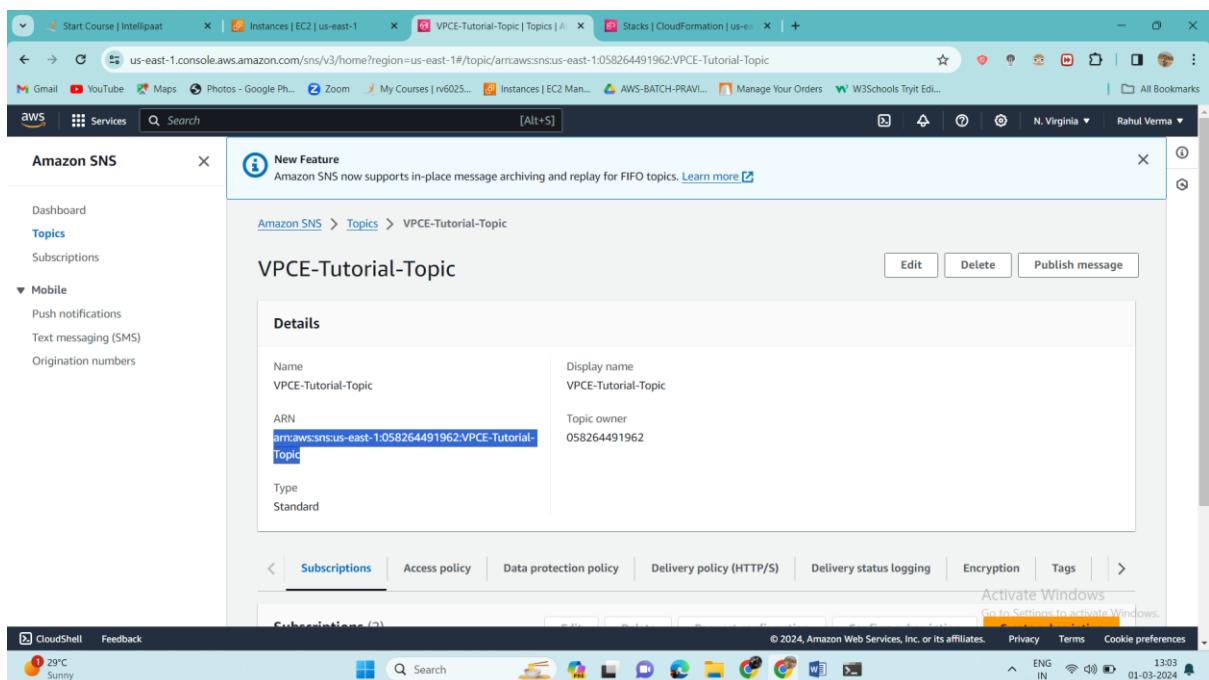
Search

ENG IN 13:02 01-03-2024

Now copy the arn of topic

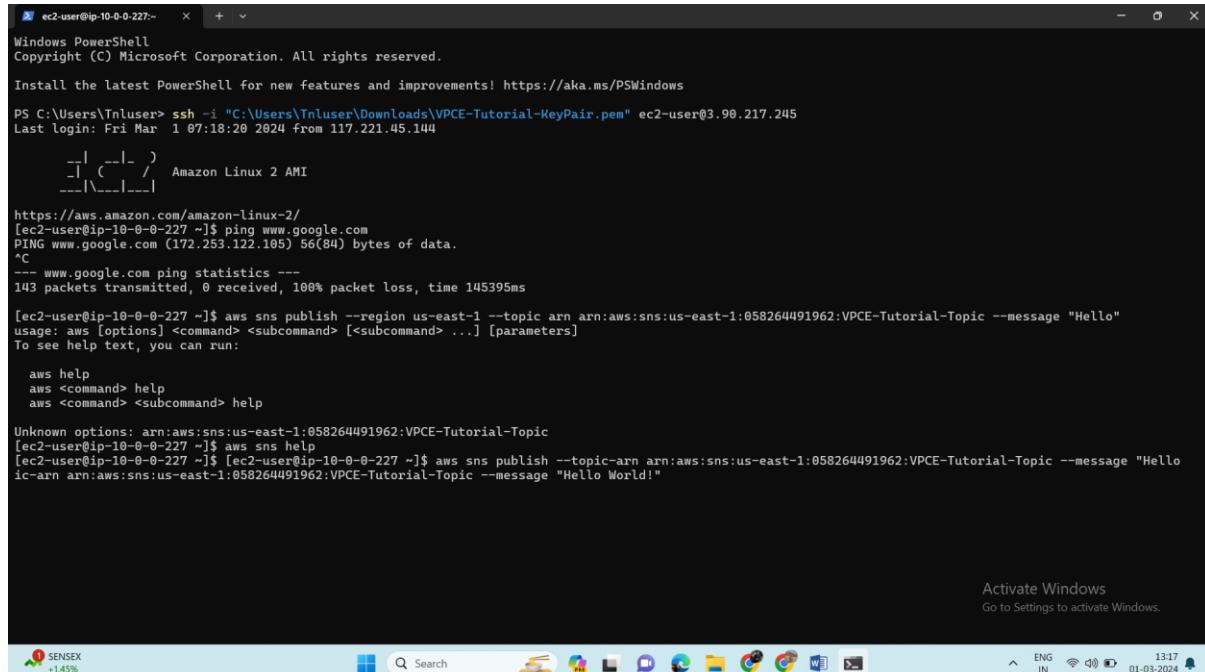


Arn copied



And by this command will publish our message

```
aws sns publish --region us-east-1 --topic arn arn:aws:sns:us-east-1:058264491962:VPCE-Tutorial-Topic --message "Hello"
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

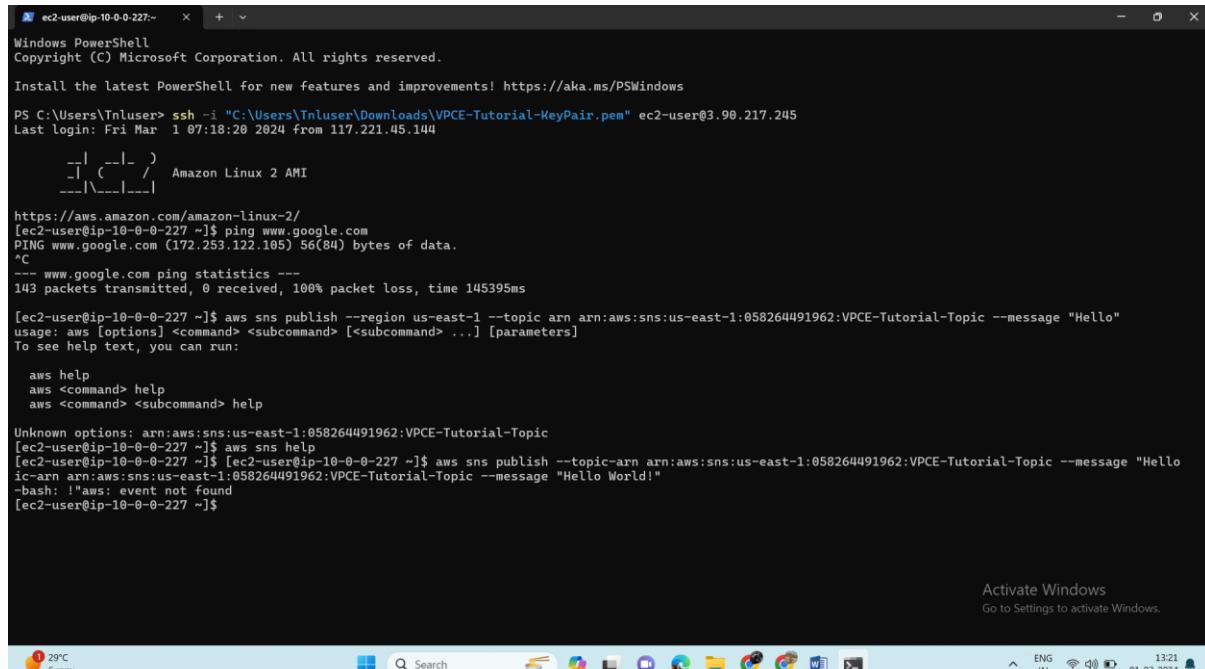
PS C:\Users\Tnuser> ssh -i "C:\Users\Tnuser\Downloads\VPCE-Tutorial-KeyPair.pem" ec2-user@3.98.217.245
Last login: Fri Mar 1 07:18:20 2024 from 117.221.45.144
__| _--|_ )
__| | ( _ / Amazon Linux 2 AMI
__| | \_ |__|_ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-227 ~]$ ping www.google.com
PING www.google.com (172.253.122.105) 56(84) bytes of data.
^C
--- www.google.com ping statistics ---
143 packets transmitted, 0 received, 100% packet loss, time 145395ms

[ec2-user@ip-10-0-0-227 ~]$ aws sns publish --region us-east-1 --topic arn arn:aws:sns:us-east-1:058264491962:VPCE-Tutorial-Topic --message "Hello"
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:
aws help
aws <command> help
aws <command> <subcommand> help

Unknown options: arn:aws:sns:us-east-1:058264491962:VPCE-Tutorial-Topic
[ec2-user@ip-10-0-0-227 ~]$ aws sns help
[ec2-user@ip-10-0-0-227 ~]$ aws sns publish --topic-arn arn:aws:sns:us-east-1:058264491962:VPCE-Tutorial-Topic --message "Hello World!"
```

It fails to publish



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Tnuser> ssh -i "C:\Users\Tnuser\Downloads\VPCE-Tutorial-KeyPair.pem" ec2-user@3.98.217.245
Last login: Fri Mar 1 07:18:20 2024 from 117.221.45.144
__| _--|_ )
__| | ( _ / Amazon Linux 2 AMI
__| | \_ |__|_ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-227 ~]$ ping www.google.com
PING www.google.com (172.253.122.105) 56(84) bytes of data.
^C
--- www.google.com ping statistics ---
143 packets transmitted, 0 received, 100% packet loss, time 145395ms

[ec2-user@ip-10-0-0-227 ~]$ aws sns publish --region us-east-1 --topic arn arn:aws:sns:us-east-1:058264491962:VPCE-Tutorial-Topic --message "Hello"
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:
aws help
aws <command> help
aws <command> <subcommand> help

Unknown options: arn:aws:sns:us-east-1:058264491962:VPCE-Tutorial-Topic
[ec2-user@ip-10-0-0-227 ~]$ aws sns help
[ec2-user@ip-10-0-0-227 ~]$ aws sns publish --topic-arn arn:aws:sns:us-east-1:058264491962:VPCE-Tutorial-Topic --message "Hello World!"
```

To connect the VPC to Amazon SNS, you define an interface VPC endpoint. After you add the endpoint, you can log in to the Amazon EC2 instance in your VPC, and from there you can use the Amazon SNS API. You can publish messages to the topic, and the messages are published privately. They stay within the AWS network, and they don't travel the public internet. Note that the instance still lacks access to other AWS services and endpoints on the internet.

Let's create end point now so go to vpc in amazon console

Now create endpoint

## Let's configure

Start Course | Intellipaat Instances | EC2 | us-east-1 VPC-E-Tutorial-Topic | Topics CreateVpcEndpoint | VPC Cons...

Gmail YouTube Maps Photos - Google Ph... Zoom My Courses | rv6025... Instances | EC2 Man... AWS-BATCH-PRAVI... Manage Your Orders W3Schools Try It... All Bookmarks

**aws Services** **Search** [Alt+S]

**VPC** > **Endpoints** > Create endpoint

## Create endpoint Info

There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and Gateway endpoints. Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an Elastic Network Interface (ENI) as an entry point for traffic destined to the service. Interface endpoints are typically accessed using the public or private DNS name associated with the service, while Gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.

### Endpoint settings

Name tag - optional  
Creates a tag with a key of 'Name' and a value that you specify.

### Service category

Select the service category

AWS services Services provided by Amazon

PrivateLink Ready partner services Services with an AWS Service Ready designation

AWS Marketplace services Services that you've purchased through AWS Marketplace

EC2 Instance Connect Endpoint An elastic network interface that allow you to connect to resources in a private subnet

Other endpoint services Find services shared with you by service name

### Services (1/1)

Activate Windows Go to Settings to activate Windows

CloudShell Feedback

24°C Partly cloudy

Search

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

EN IN 02-03-2024

### Select services, VPC & Subnet

Start Course | Intellipaat

Instances | EC2 | us-east-1

VPCE-Tutorial-Topic | Topics |

CreateVpcEndpoint | VPC Cons...

Gmail YouTube Maps Photos - Google Ph... Zoom My Courses | rv6025... Instances | EC2 Man... AWS-BATCH-PRAVI... Manage Your Orders W3Schools Tryit Edi...

All Bookmarks

Services

Search

Services (1/1)

Service Name = com.amazonaws.us-east-1.sns

Clear filters

Service Name

Owner

Type

VPC

Select the VPC in which to create the endpoint

VPC

The VPC in which to create your endpoint.

vpc-04c831766fcda436ae (VPCE-Tutorial-VPN)

Additional settings

DNS name

Enable DNS name

Associates a private hosted zone with the VPC that contains a record set that enables you to leverage Amazon's private network connectivity to the service while making requests to the service's default public endpoint DNS name. To use this feature, ensure that the attributes 'Enable DNS hostnames' and 'Enable DNS support' are enabled for your VPC.

DNS record IP type

IPv4

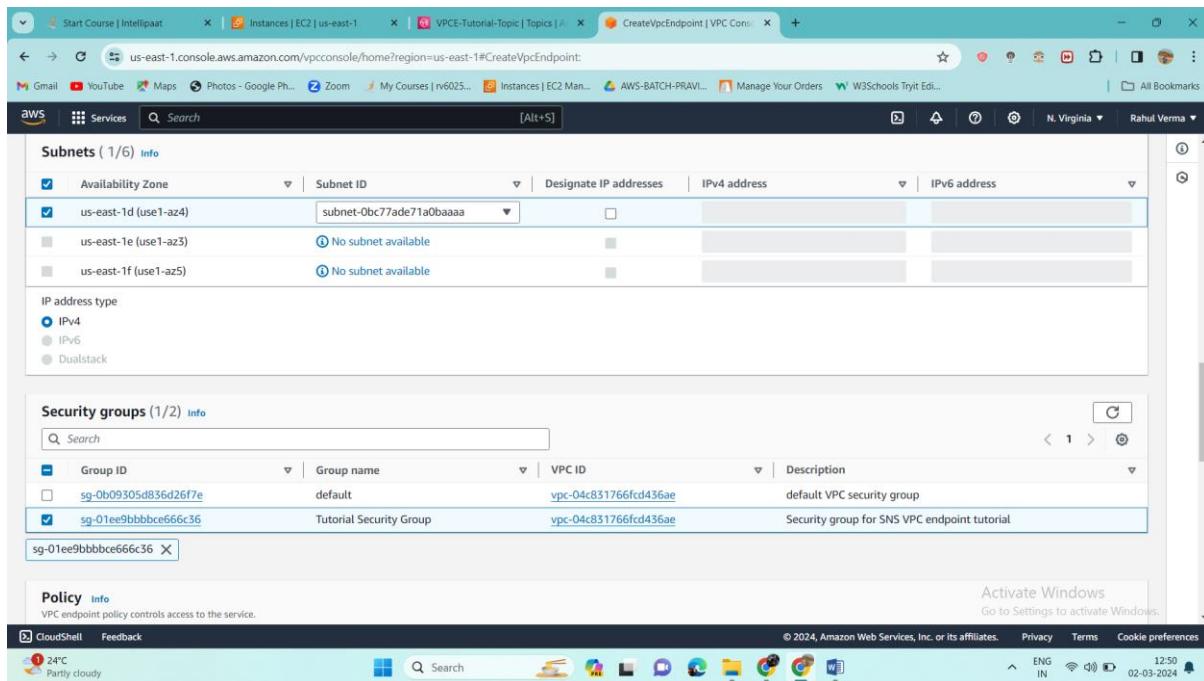
IPv6

Dualstack

Service defined

Activate Windows  
Go to Settings to activate Windows.

## Select security group



Subnets (1/6) [Info](#)

Availability Zone	Subnet ID	Designate IP addresses	IPv4 address	IPv6 address
us-east-1d (use1-az4)	subnet-0bc77ade71a0baaaa	<input type="checkbox"/>		
us-east-1e (use1-az3)		<small> ⓘ No subnet available</small>		
us-east-1f (use1-az5)		<small> ⓘ No subnet available</small>		

IP address type: IPv4

Security groups (1/2) [Info](#)

Group ID	Group name	VPC ID	Description
sg-0b09305db836d26f7e	default	vpc-04c831766fcd436ae	default VPC security group
sg-01ee9bbbbc666c36	Tutorial Security Group	vpc-04c831766fcd436ae	Security group for SNS VPC endpoint tutorial

sg-01ee9bbbbc666c36 [X](#)

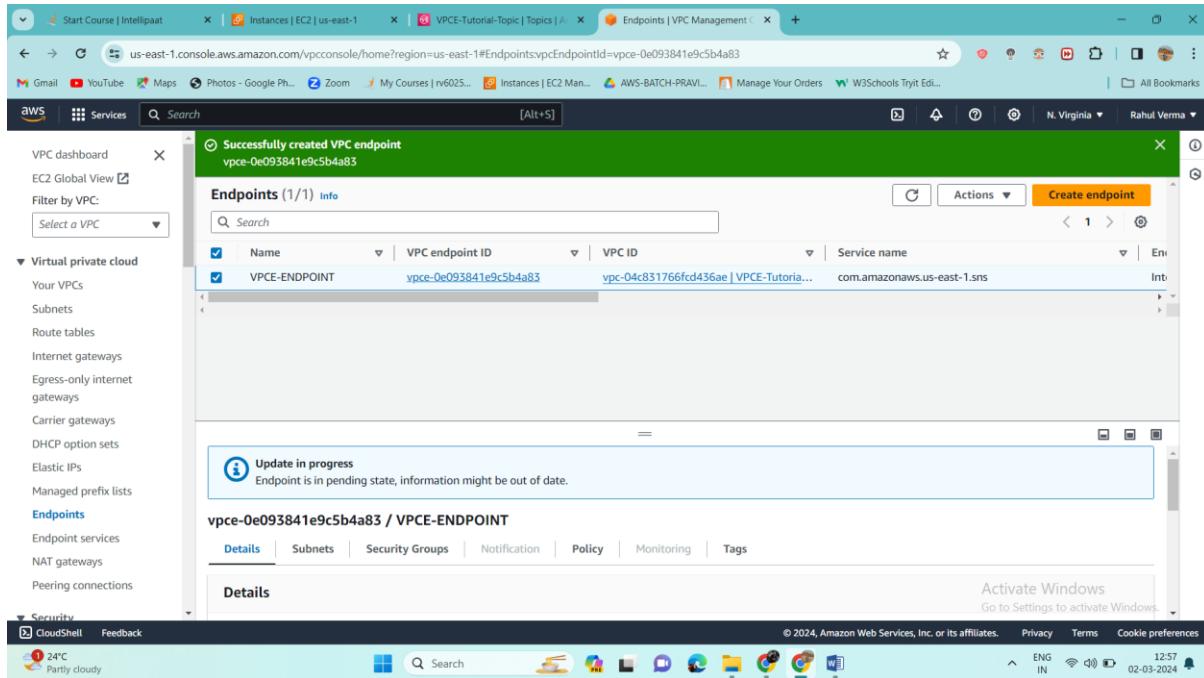
Policy [Info](#)

VPC endpoint policy controls access to the service.

Activate Windows  
Go to Settings to activate Windows

CloudShell Feedback 24°C Partly cloudy 12:50 02-03-2024 ENG IN

## Our endpoint is created



Start Course | Intellipaat | Instances | EC2 | us-east-1 | VPCE-Tutorial-Topic | Topics | CreateVpcEndpoint | VPC Con...

Subnets (1/6) [Info](#)

Availability Zone	Subnet ID	Designate IP addresses	IPv4 address	IPv6 address
us-east-1d (use1-az4)	subnet-0bc77ade71a0baaaa	<input type="checkbox"/>		
us-east-1e (use1-az3)		<small> ⓘ No subnet available</small>		
us-east-1f (use1-az5)		<small> ⓘ No subnet available</small>		

IP address type: IPv4

Security groups (1/2) [Info](#)

Group ID	Group name	VPC ID	Description
sg-0b09305db836d26f7e	default	vpc-04c831766fcd436ae	default VPC security group
sg-01ee9bbbbc666c36	Tutorial Security Group	vpc-04c831766fcd436ae	Security group for SNS VPC endpoint tutorial

sg-01ee9bbbbc666c36 [X](#)

Policy [Info](#)

VPC endpoint policy controls access to the service.

Activate Windows  
Go to Settings to activate Windows

CloudShell Feedback 24°C Partly cloudy 12:50 02-03-2024 ENG IN

Success message: Successfully created VPC endpoint vpce-0e093841e9c5b4a83

Endpoints (1/1) [Info](#)

Name	VPC endpoint ID	VPC ID	Service name
VPCE-ENDPOINT	vpce-0e093841e9c5b4a83	vpc-04c831766fcd436ae	com.amazonaws.us-east-1.sns

Update in progress  
Endpoint is in pending state, information might be out of date.

vpce-0e093841e9c5b4a83 / VPCE-ENDPOINT

Details Subnets Security Groups Notification Policy Monitoring Tags

Activate Windows  
Go to Settings to activate Windows

CloudShell Feedback 24°C Partly cloudy 12:57 02-03-2024 ENG IN

Let's connect to our ec2 instance once again

Note we have stopped it so its IP is changed now

```
ec2-user@ip-10-0-0-227: ~ + - x
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

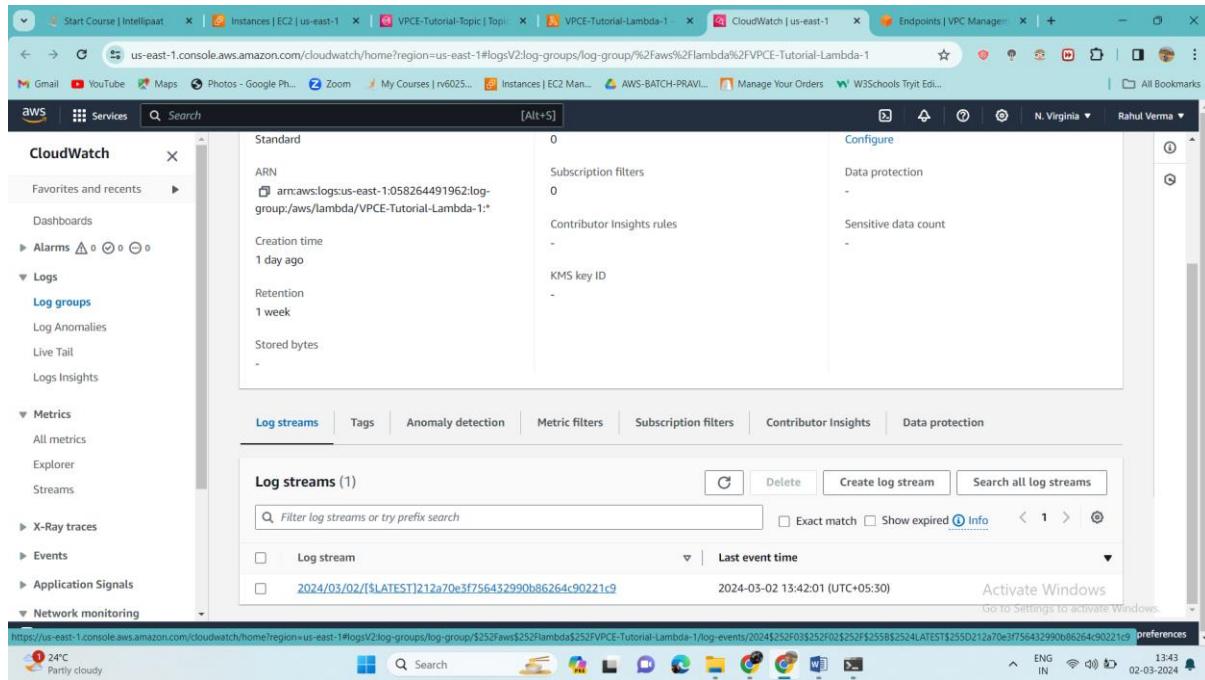
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Tnuser\Downloads> ssh -i "C:\Users\Tnuser\Downloads\VPCE-Tutorial-KeyPair.pem" ec2-user@54.211.253.61
The authenticity of host '54.211.253.61 (54.211.253.61)' can't be established.
ED25519 key fingerprint is SHA256:uJ/p1r9yAewpn5KH/BgGvh9BLIU9BB5bZhScxjnRD4.
This host key is known by the following other names/addresses:
  C:\Users\Tnuser/.ssh/known_hosts:8: 3.96.217.245
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '54.211.253.61' (ED25519) to the list of known hosts.
Last login: Fri Mar  1 07:24:07 2024 from 117.221.45.144
  _\ _-|_ )  Amazon Linux 2 AMI
  _\(_ /|---|_
---\_\_||_---|_

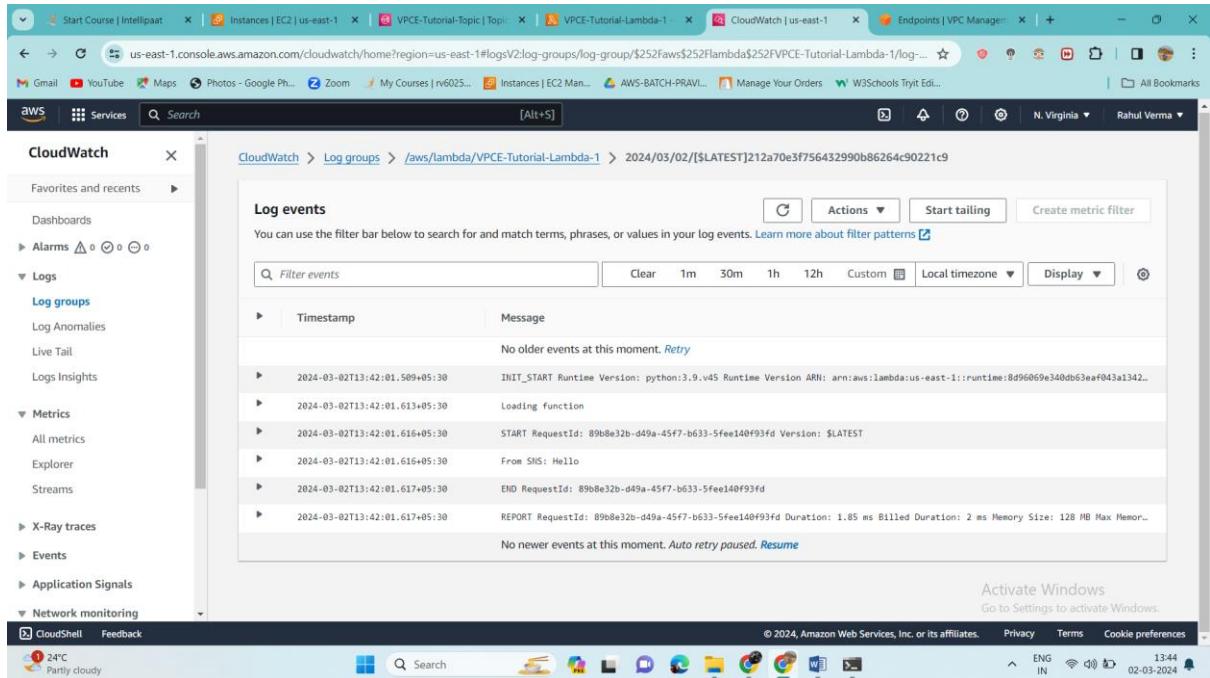
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-227 ~]$ |
```

Now let's publish a message to our Topic

And let's check the cloud watch logs lambda 1



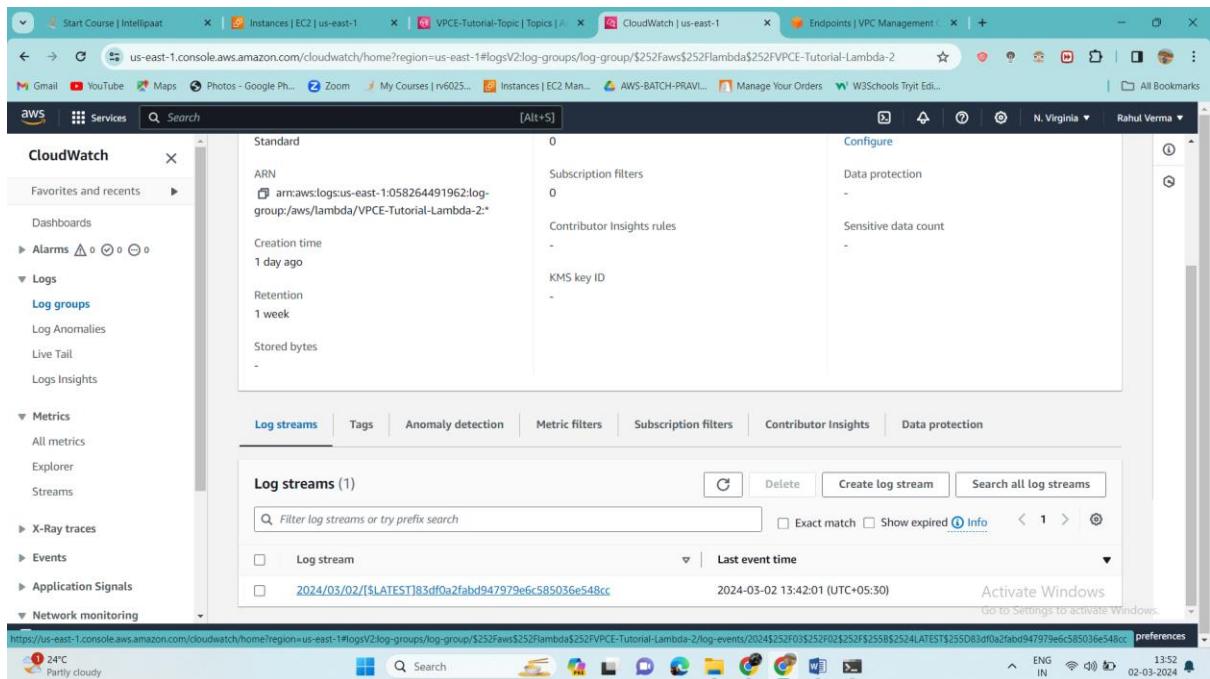
## We have successfully receive message from SNS



The screenshot shows the AWS CloudWatch Log Events page. The left sidebar is collapsed. The main area displays a table of log events. The first event is a placeholder message: "No older events at this moment. [Retry](#)". Subsequent events are timestamped at 2024-03-02T13:42:01.509+05:30, showing various stages of the Lambda function execution: INIT, Loading function, START, and REPORT. The REPORT event includes detailed metrics: Duration: 1.85 ms, Billed Duration: 2 ms, and Memory Size: 128 MB. The log entries are as follows:

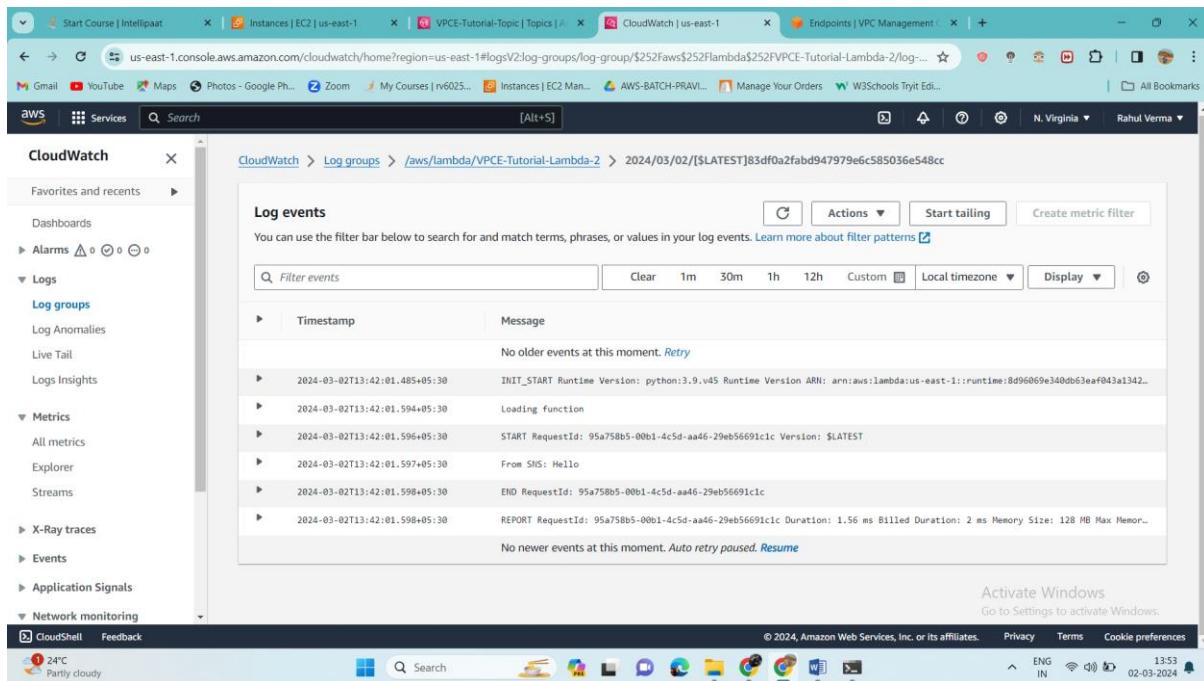
Timestamp	Message
2024-03-02T13:42:01.509+05:30	INIT_START Runtime Version: python:3.9.v45 Runtime Version ARN: arn:aws:lambda:us-east-1::runtime:8d96069e340db63eaf043a1342...
2024-03-02T13:42:01.613+05:30	Loading function
2024-03-02T13:42:01.616+05:30	START RequestId: 89b8e32b-d49a-45f7-b633-5fee140f93fd Version: \$LATEST
2024-03-02T13:42:01.616+05:30	From SNS: Hello
2024-03-02T13:42:01.617+05:30	END RequestId: 89b8e32b-d49a-45f7-b633-5fee140f93fd
2024-03-02T13:42:01.617+05:30	REPORT RequestId: 89b8e32b-d49a-45f7-b633-5fee140f93fd Duration: 1.85 ms Billed Duration: 2 ms Memory Size: 128 MB Max Memory Used: 128 MB

## Let's check it in second log lambda2



The screenshot shows the AWS CloudWatch Log Groups page. The left sidebar is collapsed. The main area displays a table of log streams. There is one entry for the log stream "2024/03/02/[\$LATEST]83df0a2fabd947979e6c585036e548cc". The log entry is timestamped at 2024-03-02 13:42:01 (UTC+05:30) and contains the message "Hello".

We have received in both the lambda functions



The screenshot shows the AWS CloudWatch Log Events interface. The left sidebar navigation includes 'CloudWatch' (selected), 'Favorites and recent', 'Logs' (selected), 'Log groups' (selected), 'Metrics', 'X-Ray traces', 'Events', 'Application Signals', and 'Network monitoring'. The main content area is titled 'Log events' and shows a table of log entries. The table has columns for 'Timestamp' and 'Message'. The first entry is 'No older events at this moment. [Retry](#)'. Subsequent entries show the Lambda function starting, receiving an SNS message, and processing it. The log entries are as follows:

Timestamp	Message
2024-03-02T13:42:01.485+05:30	INIT_START Runtime Version: python:3.9.v45 Runtime Version ARN: arn:aws:lambda:us-east-1::runtime:8d96069e340db63eaf043a1342..
2024-03-02T13:42:01.594+05:30	Loading function
2024-03-02T13:42:01.596+05:30	START RequestId: 95a758b5-00b1-4c5d-aa46-29eb56691c1c Version: \$LATEST
2024-03-02T13:42:01.597+05:30	From SNS: Hello
2024-03-02T13:42:01.598+05:30	END RequestId: 95a758b5-00b1-4c5d-aa46-29eb56691c1c
2024-03-02T13:42:01.598+05:30	REPORT RequestId: 95a758b5-00b1-4c5d-aa46-29eb56691c1c Duration: 1.56 ms Billed Duration: 2 ms Memory Size: 128 MB Max Memory Used: 128 MB
	No newer events at this moment. <a href="#">Auto retry paused.</a> <a href="#">Resume</a>

At the bottom of the interface, there are buttons for 'Activate Windows', 'CloudShell', 'Feedback', and a weather widget showing '24°C Partly cloudy'. The status bar at the bottom right shows 'ENG IN' and the date '02-03-2024'.

By adding an endpoint for Amazon SNS to a VPC, you were able to publish a message to a topic from within the network that's managed by the VPC. The message was published privately without being exposed to the public internet.