Project - 3: Publishing Amazon SNS Messages Privately

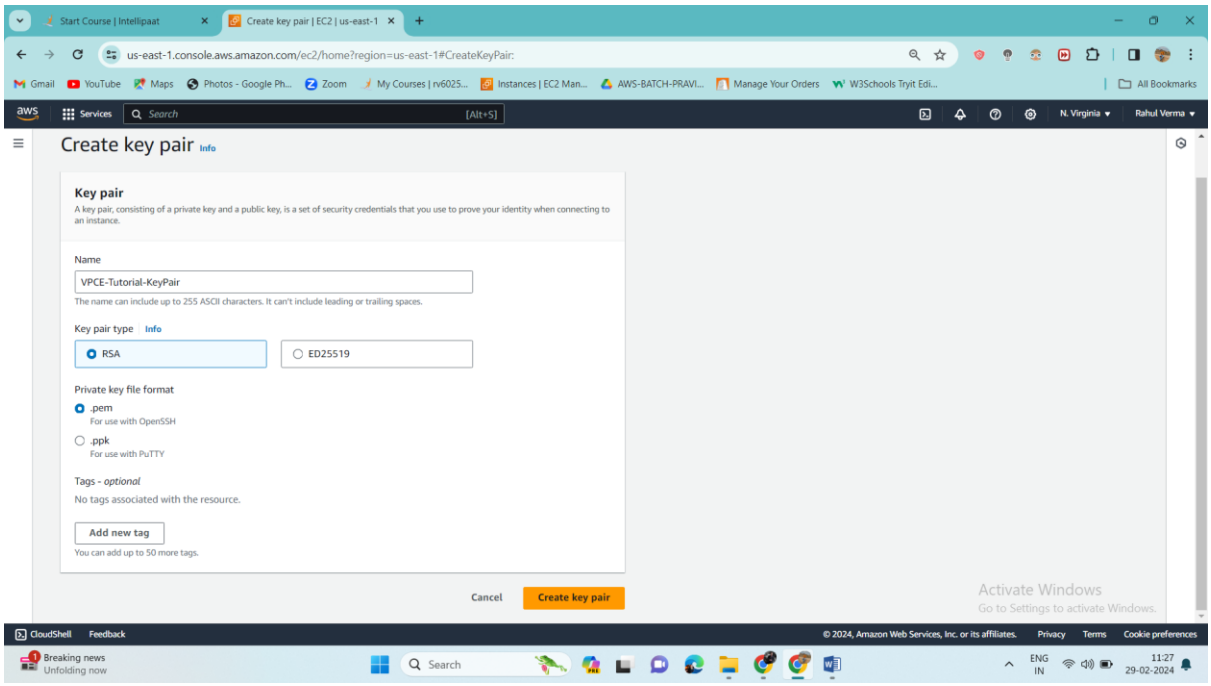
Industry: Healthcare

Problem Statement:

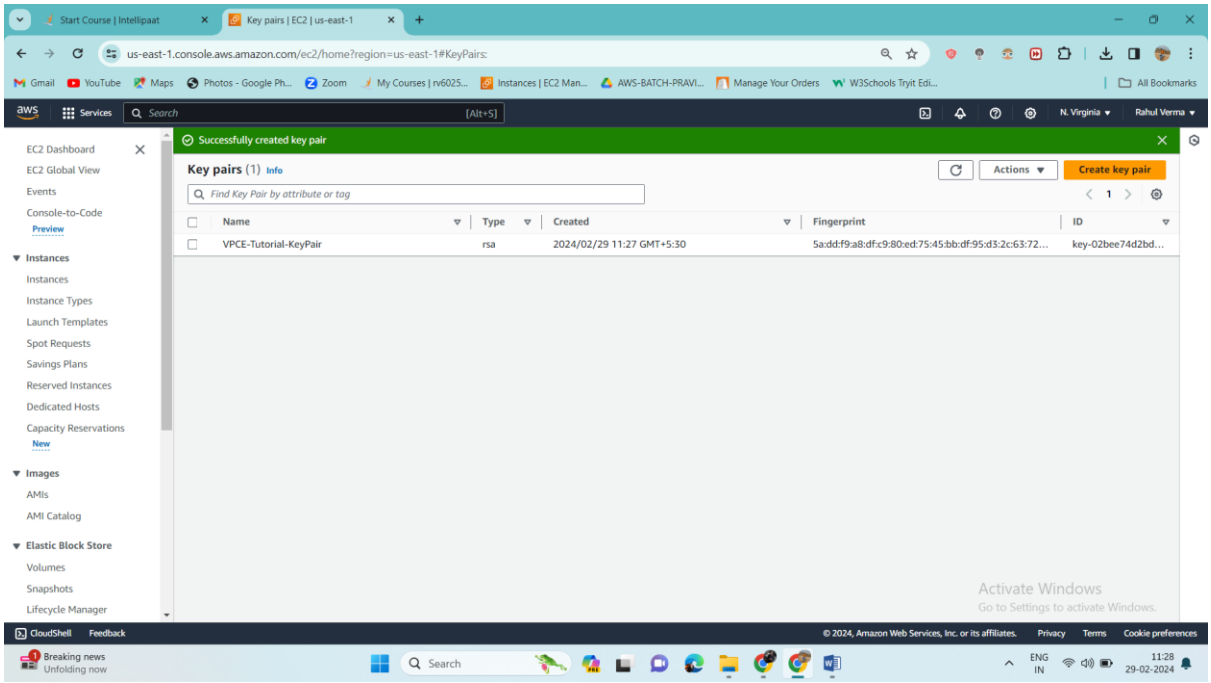
How to secure patient records online and send it privately to the intended party Topics: In this project, you will be working on a hospital project to send reports online and develop a platform so the patients can access the reports via mobile and push notifications. You will publish the report to an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

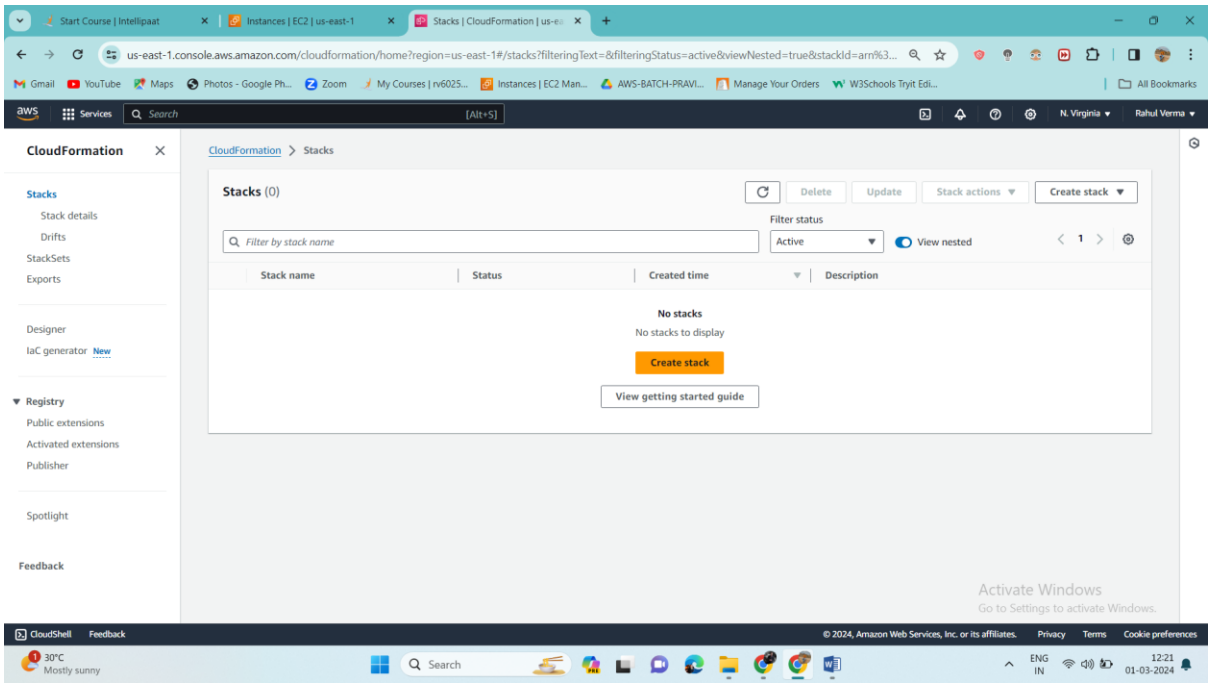
First let’s create a key pair VPCE-Tutorial-KeyPair



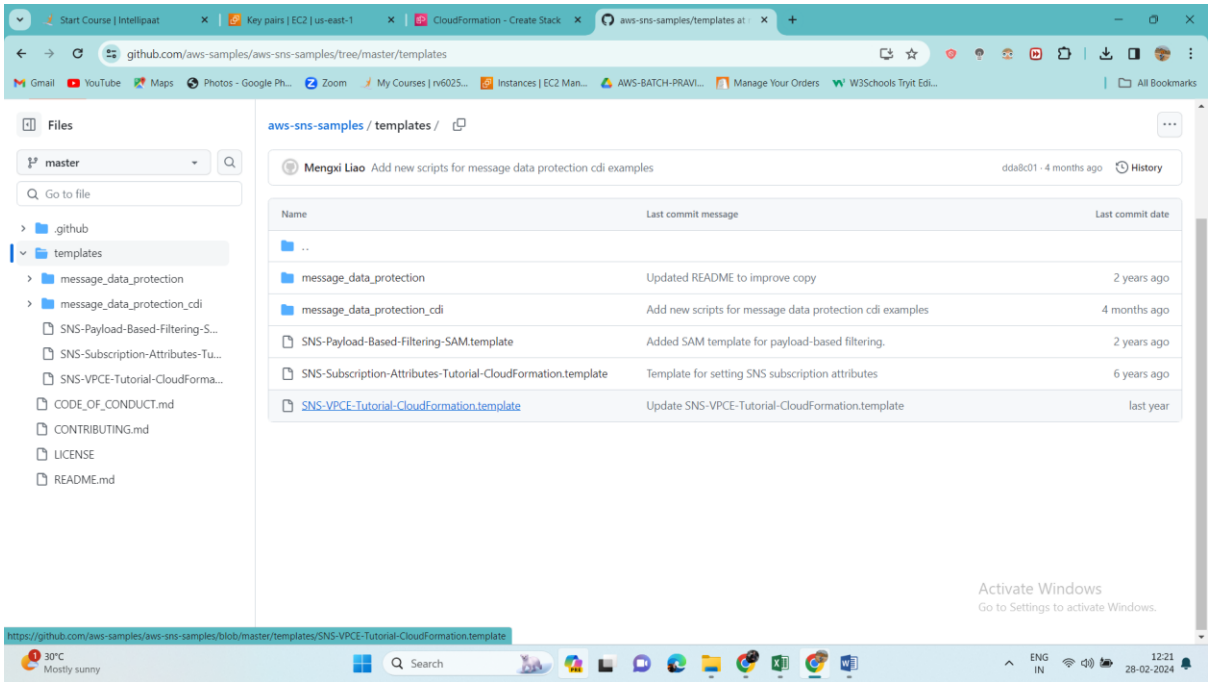
Successfully created



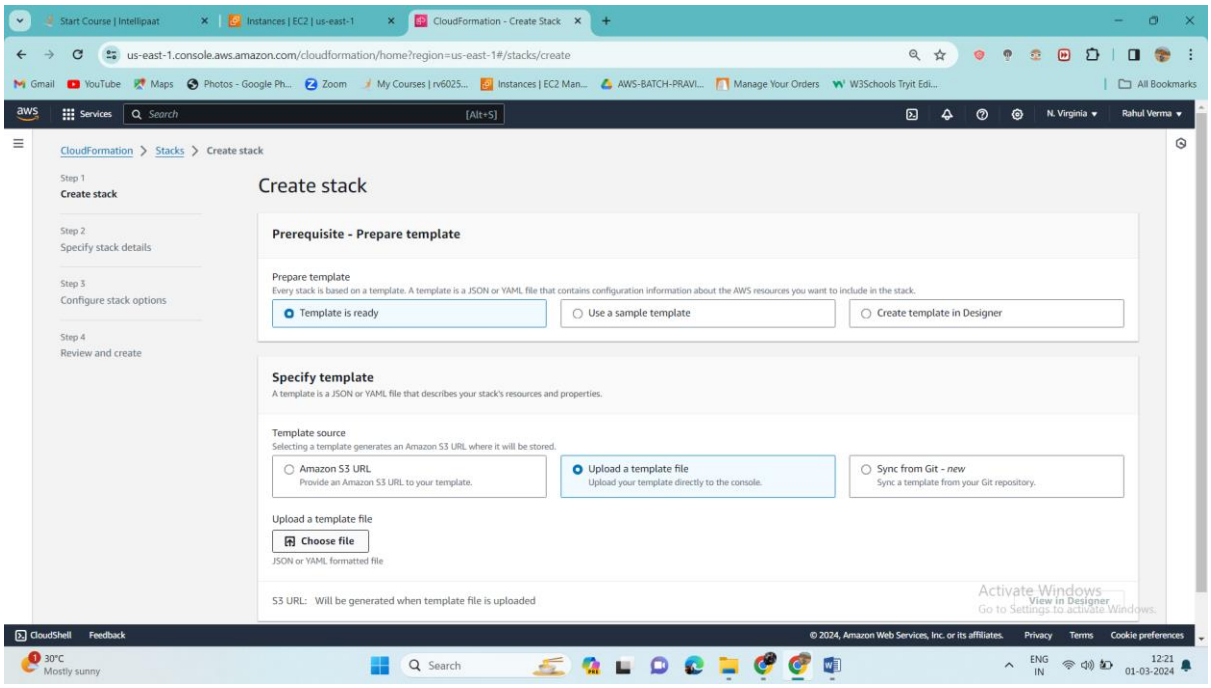
Now let’s create a stack



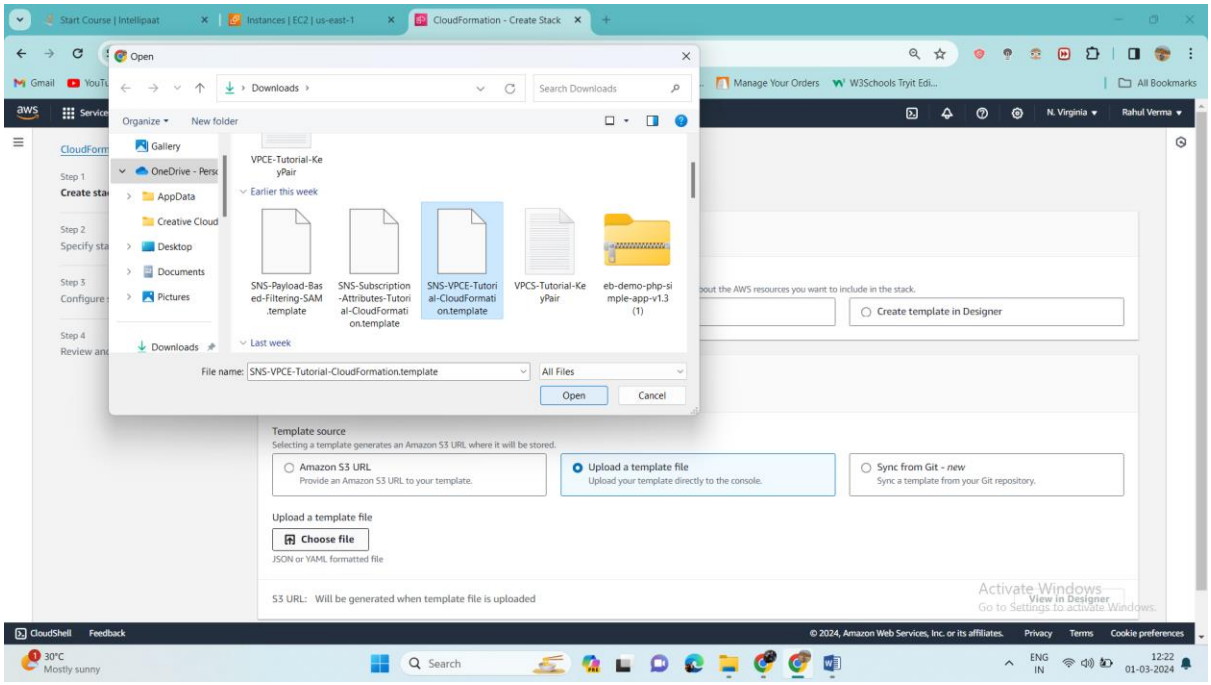
We are provided github link for this project we are gonna use the template from it.



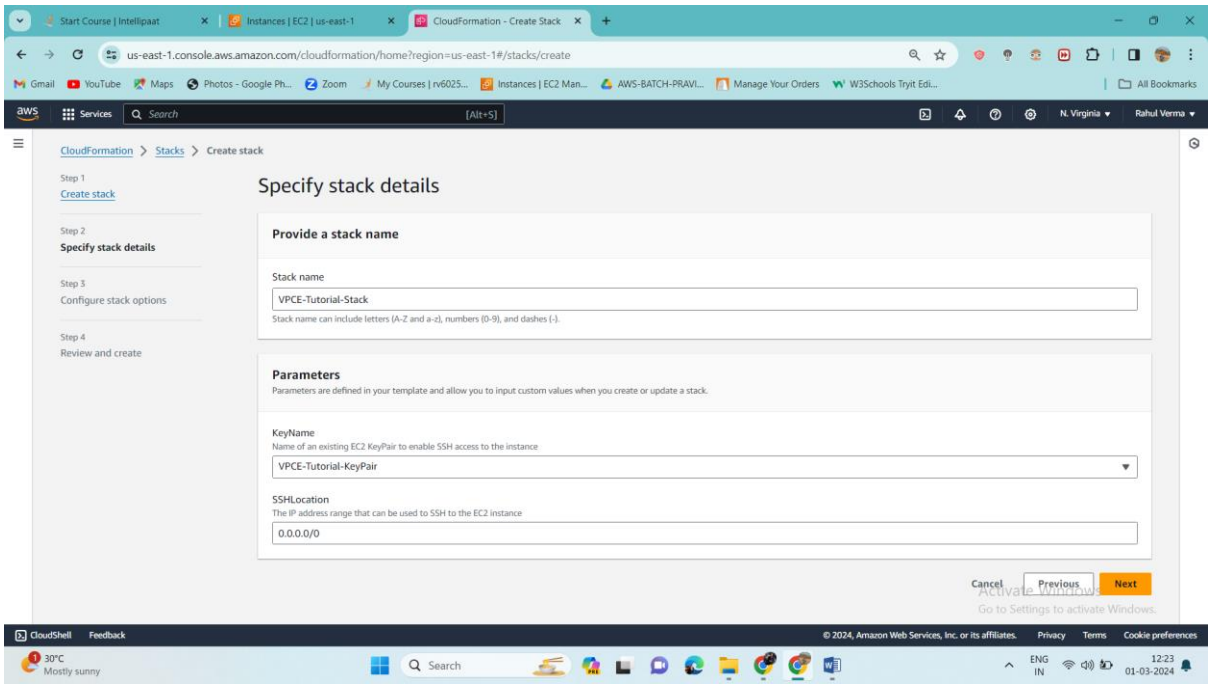
Will select template is ready and after that will select upload a template file option



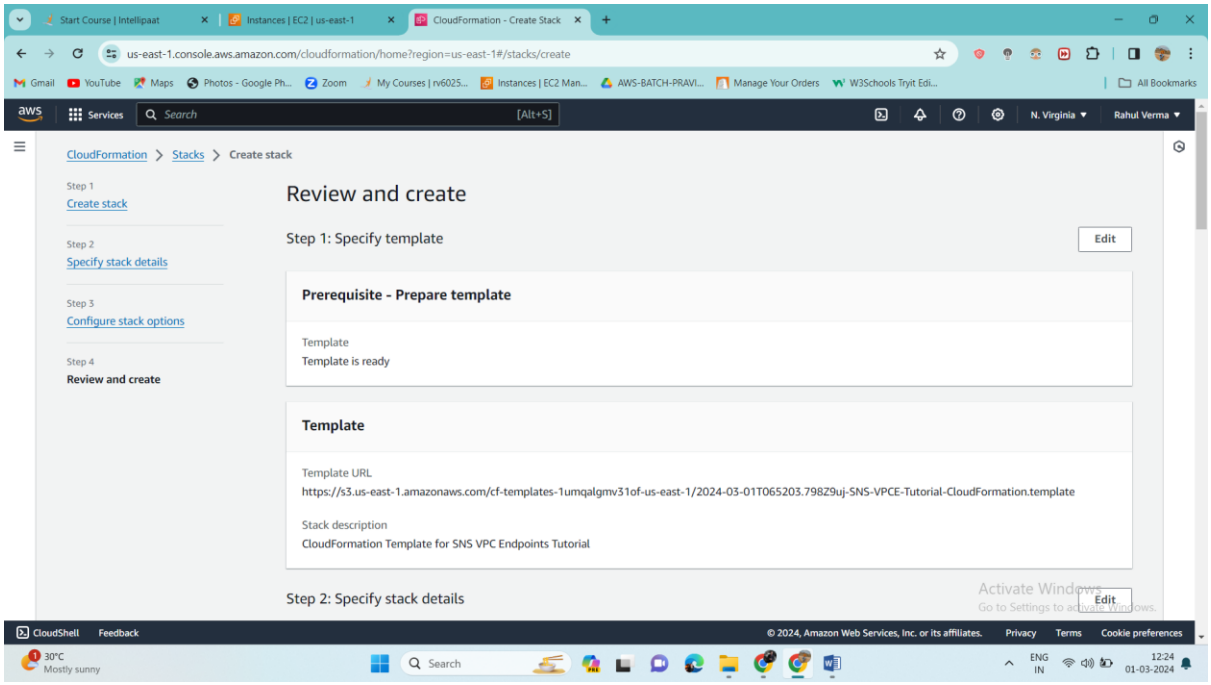
Now we will choose our template file



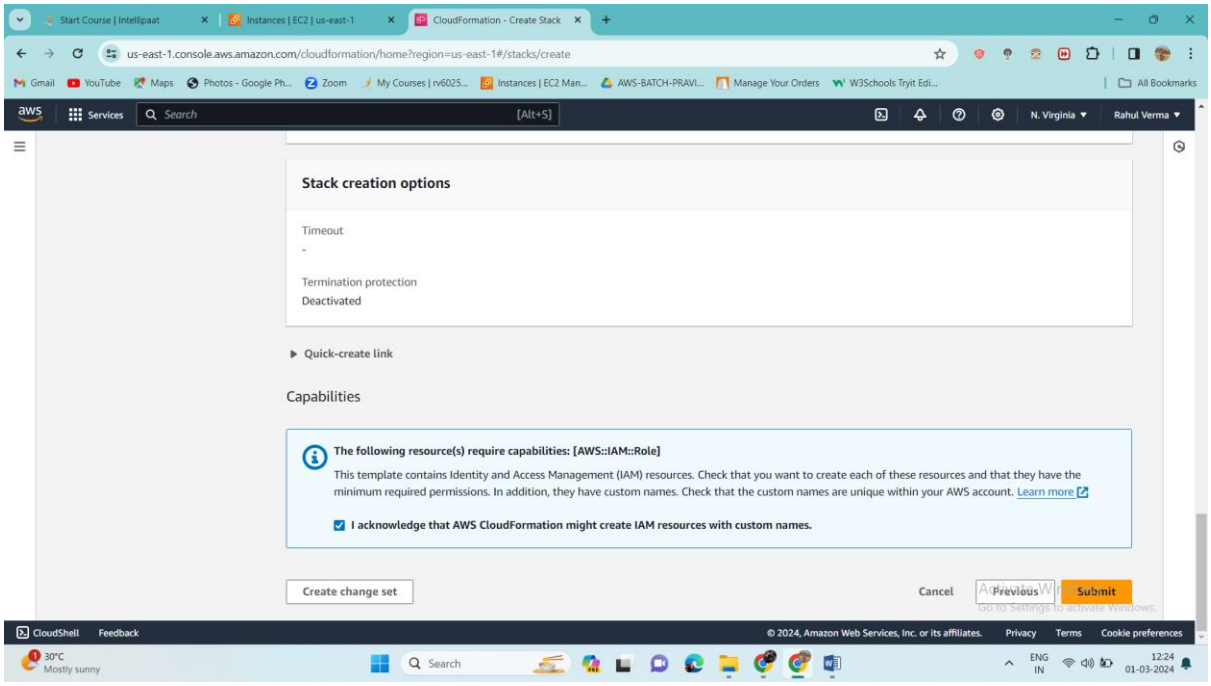
Our stack name is VPCE-Tutorial-Stack and key pair which we have created



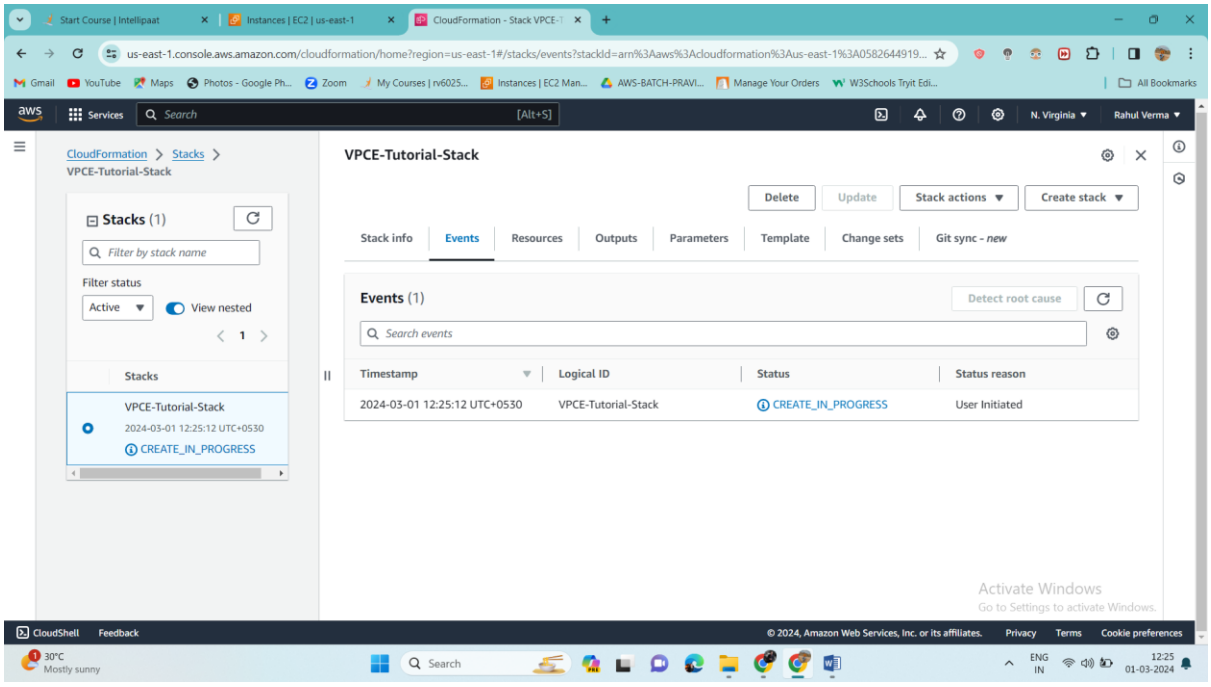
Rest default settings



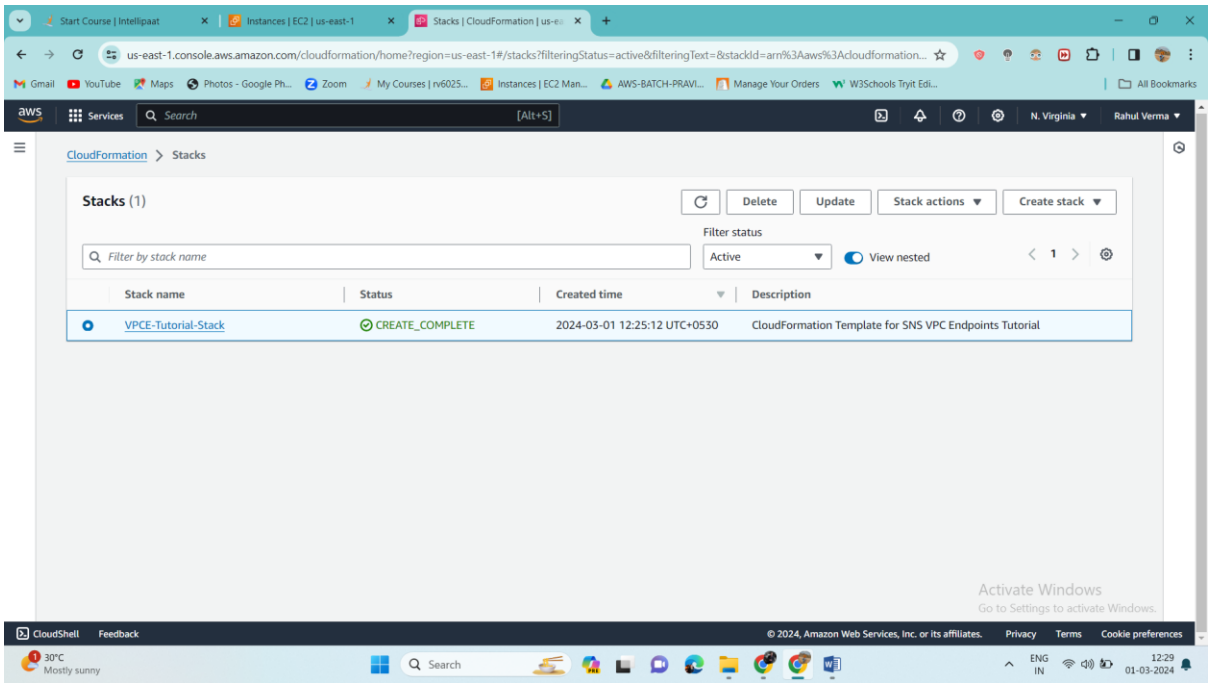
Acknowledge and submit



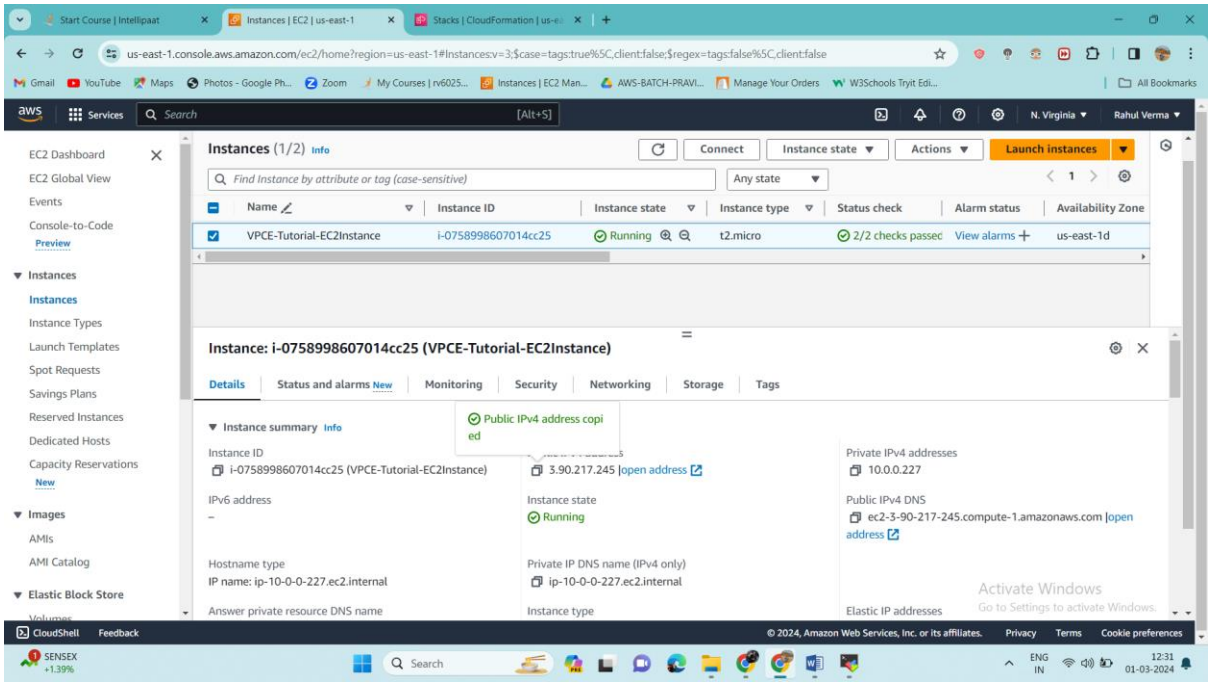
Our stack is under process



Now it created successfully

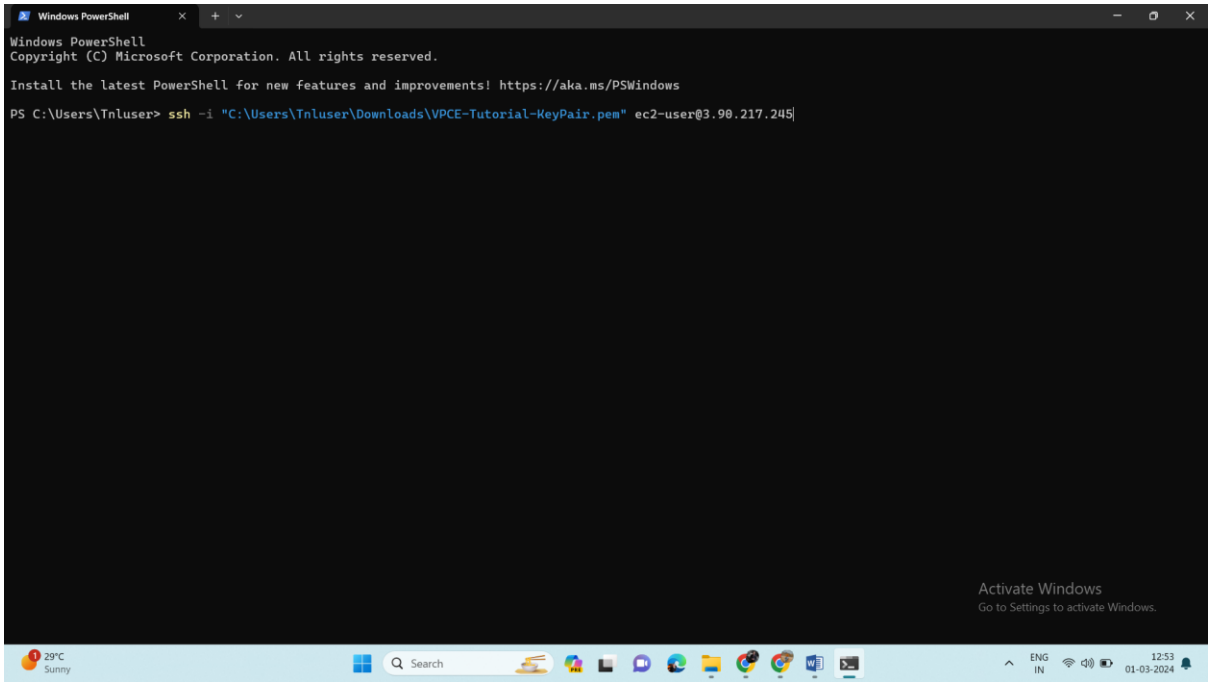


Let’s connect to our EC2 instance

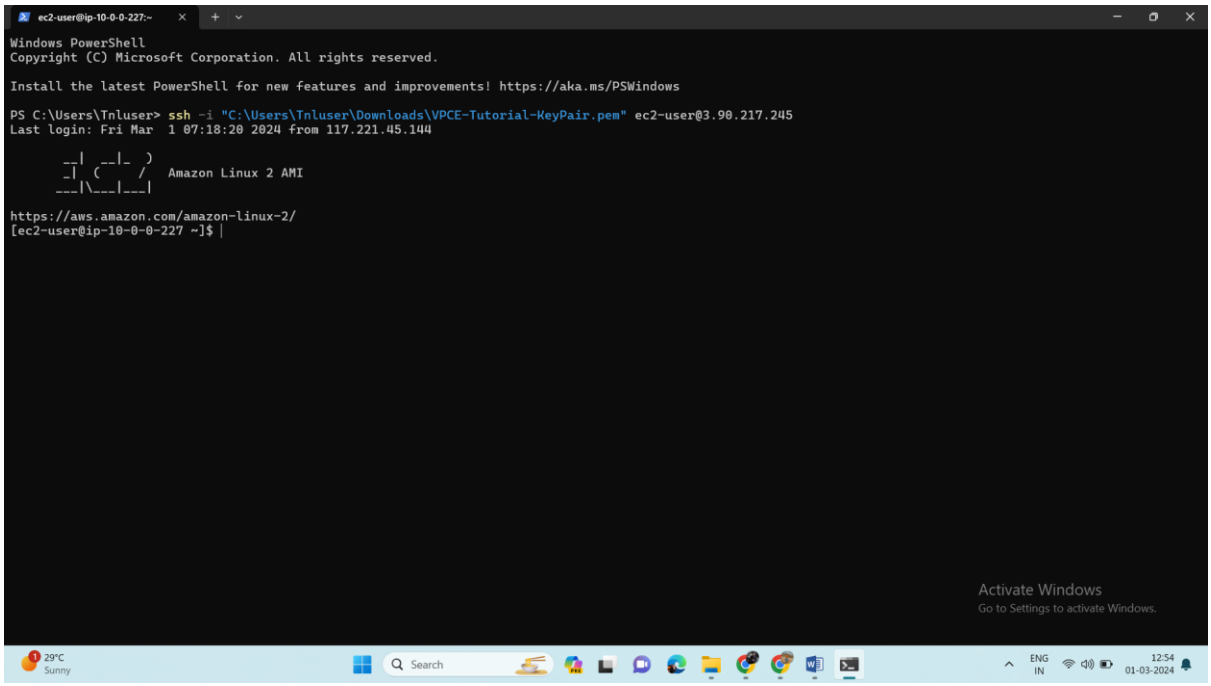


We are using cmd

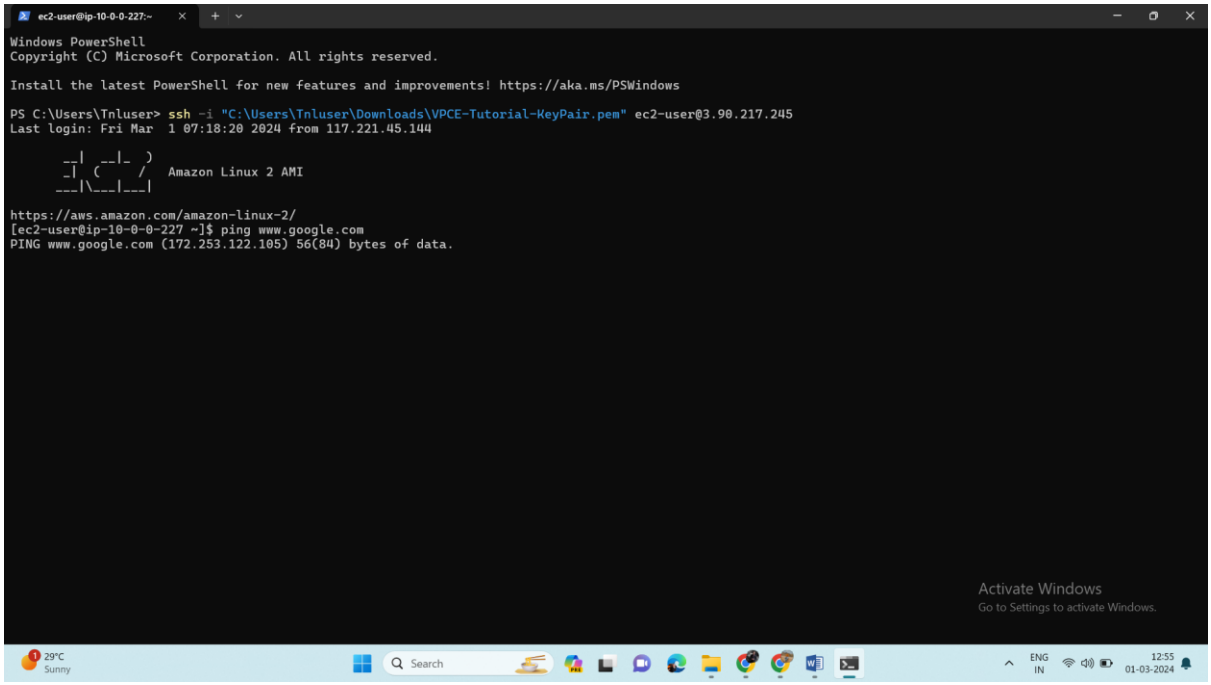
ssh –i “C:\Users\Tnluser\Downloads\VPCE-Tutorial-KeyPair.Pem” ec2-user@(instance ip)



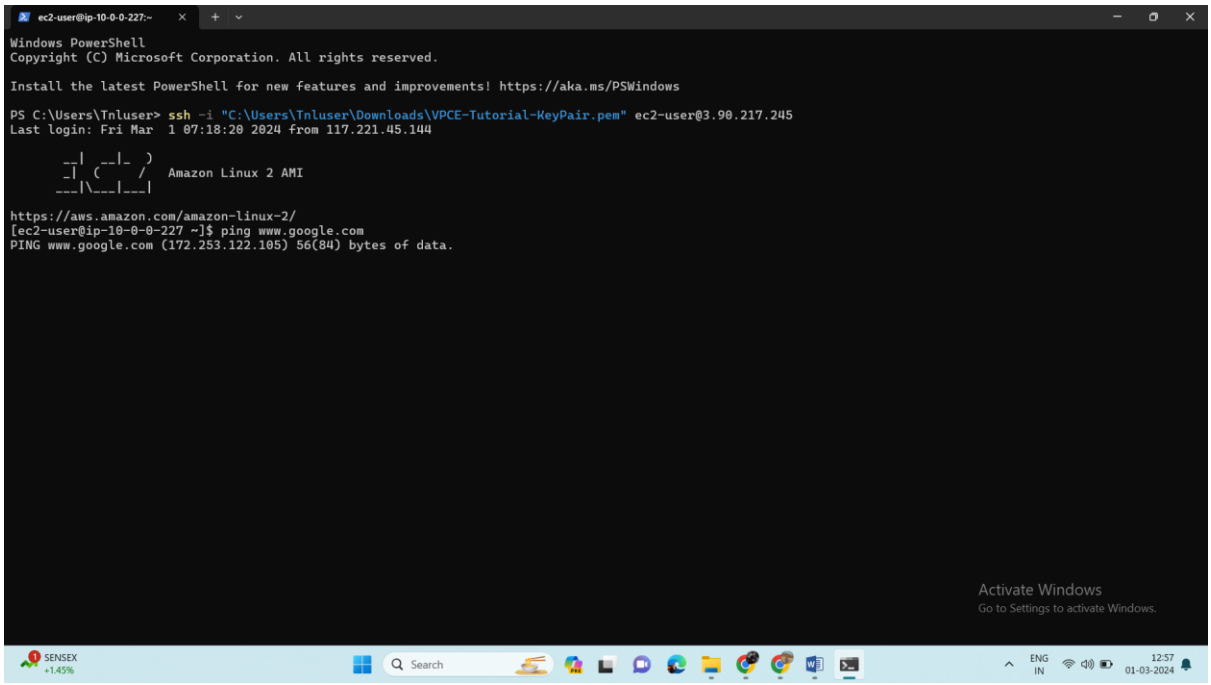
We have successfully logged in



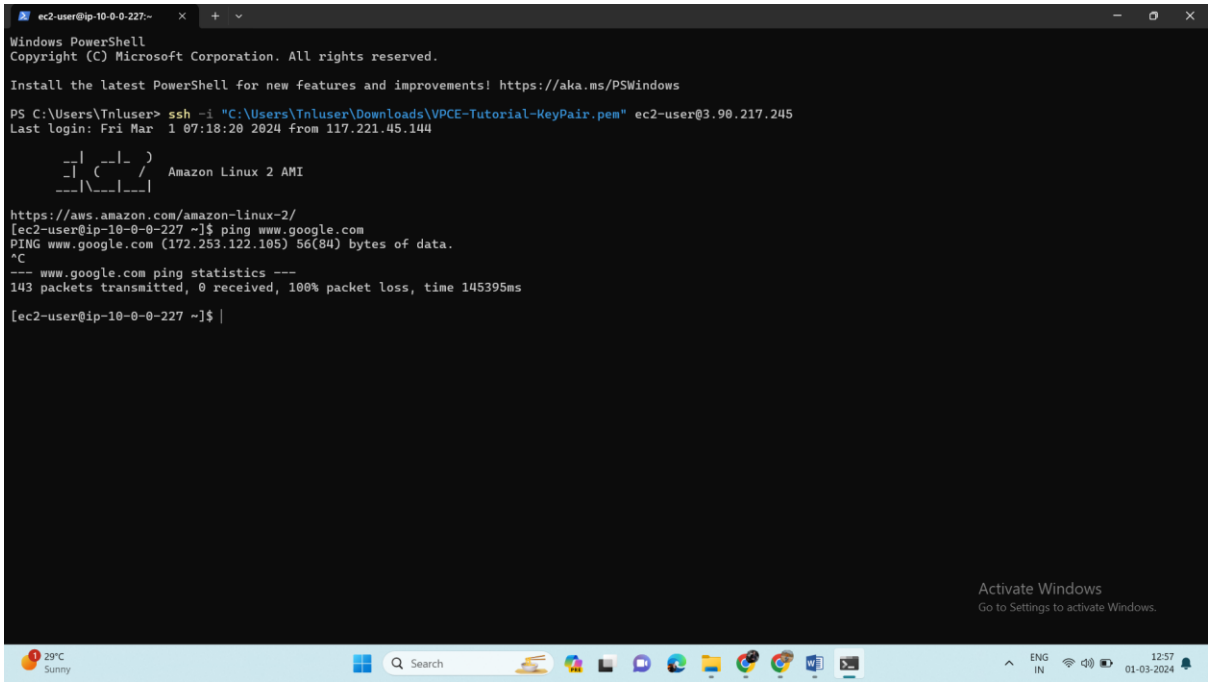
Now to check internet in our ec2 will ping google (we have ping it at 12:55 PM)



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



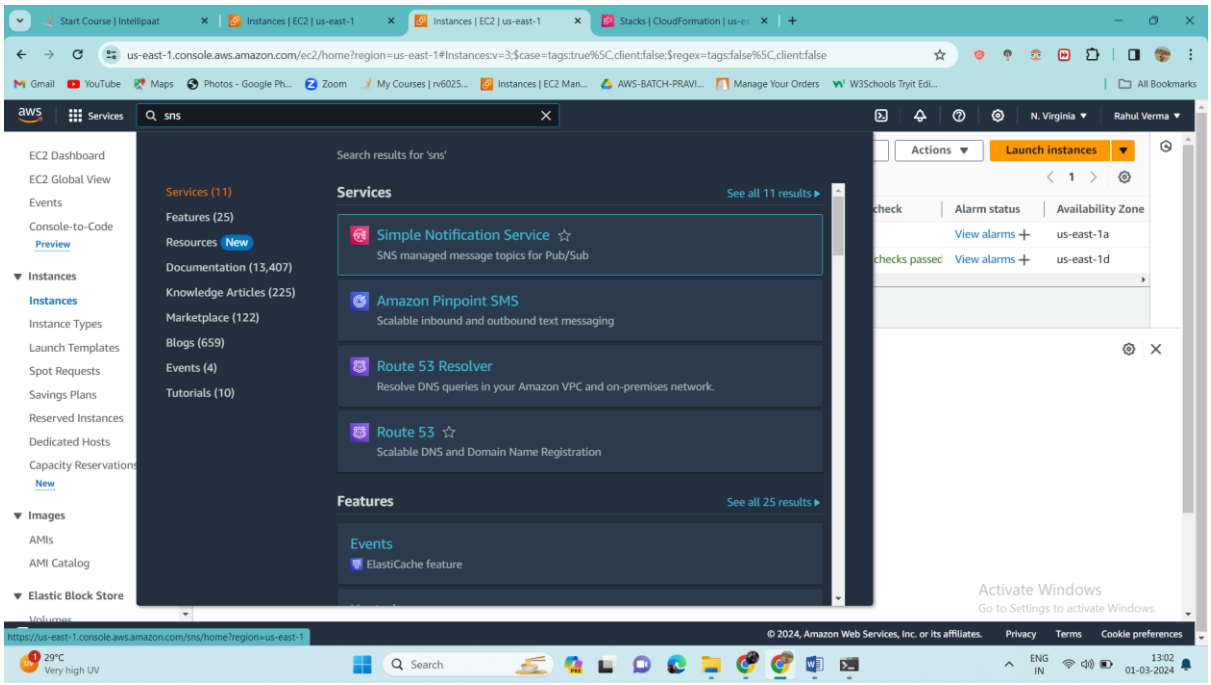
We have cancel it by ctrl+c



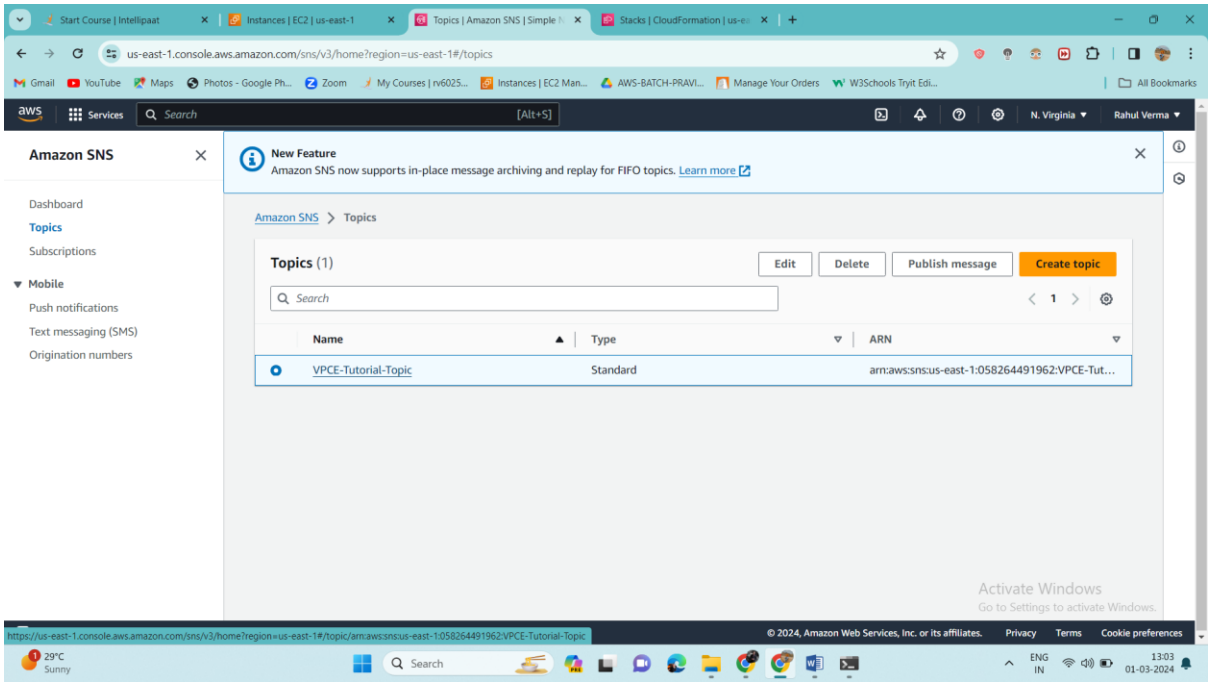
Now To verify that the instance lacks connectivity to Amazon SNS

We will attempt to publish a message to topic

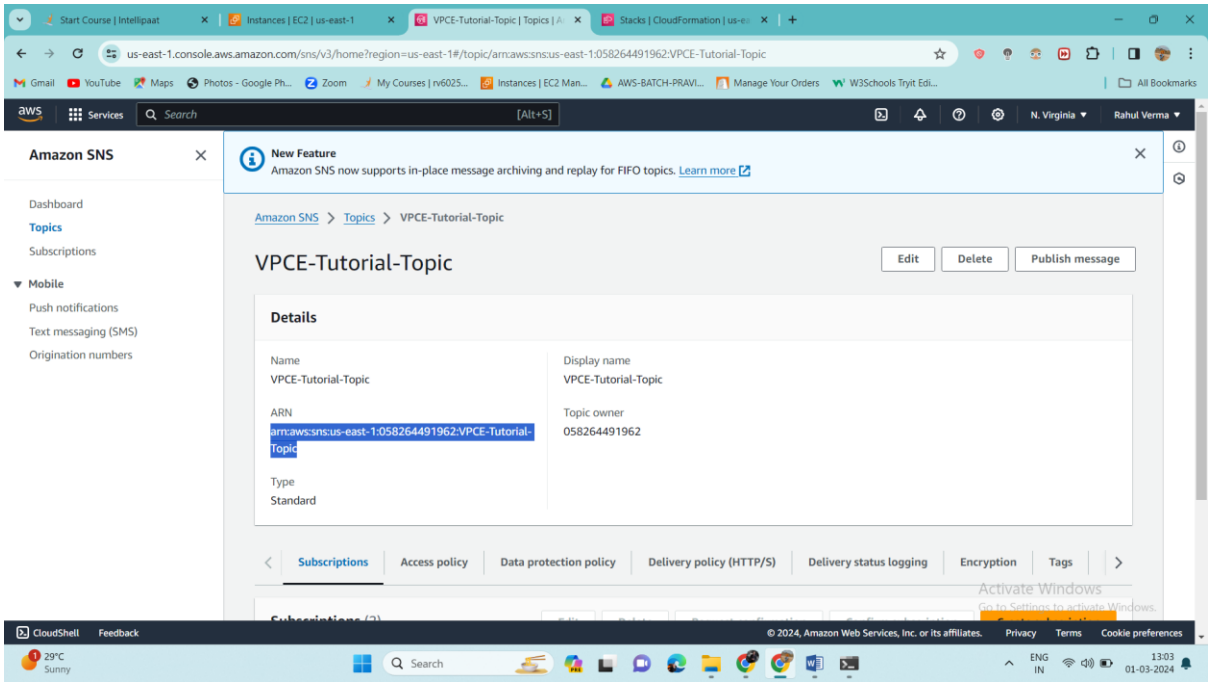
For that first will go to sns in our aws console



Now copy the arn of topic

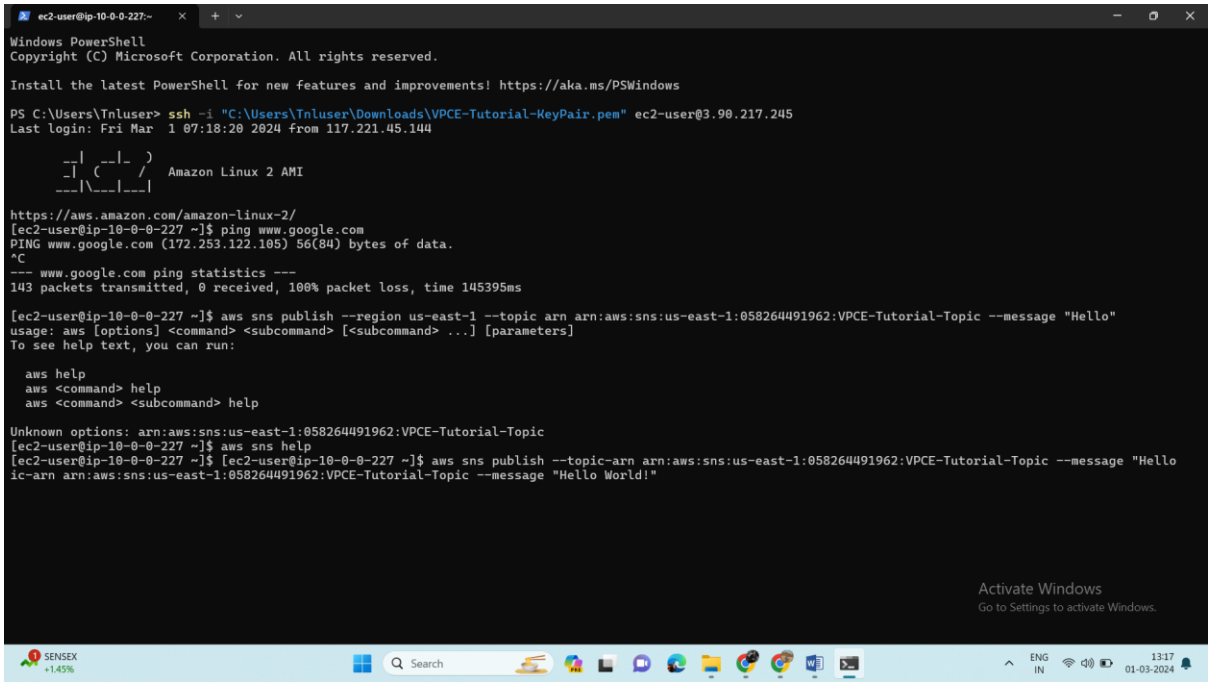


Arn copied

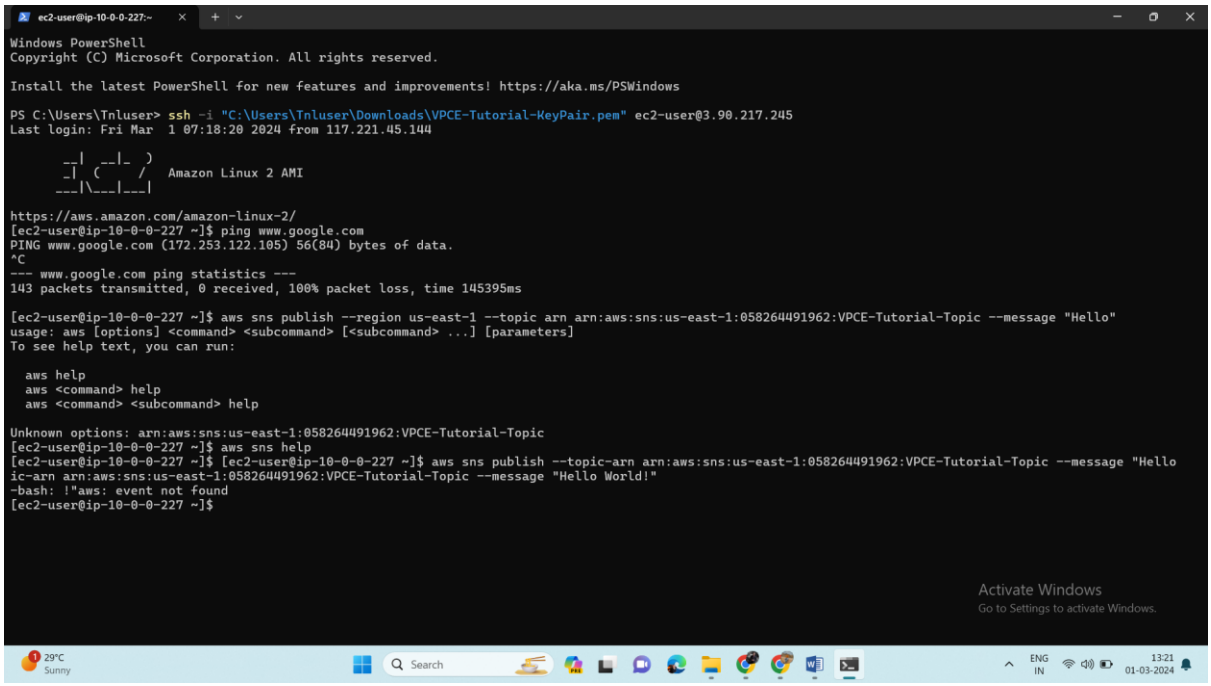


And by this command will publish our message

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

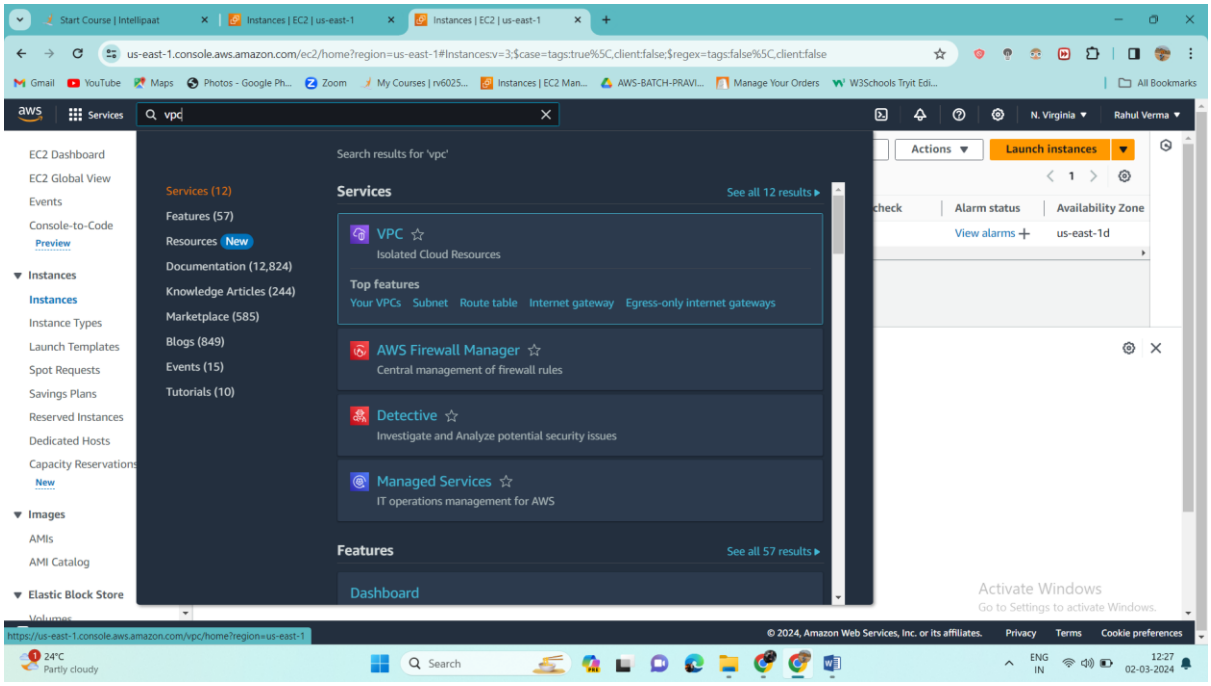


It fails to publish

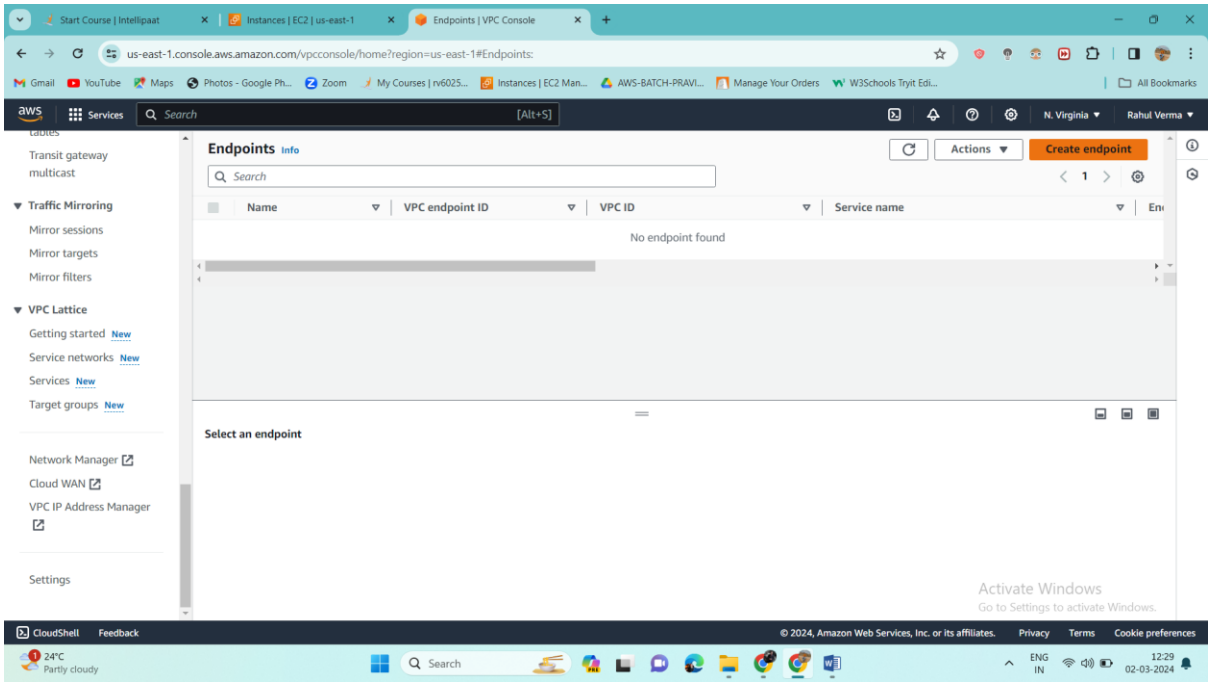


To connect the VPC to Amazon SNS, you define an interface VPC endpoint. After you add the endpoint, you can log in to the Amazon EC2 instance in your VPC, and from there you can use the Amazon SNS API. You can publish messages to the topic, and the messages are published privately. They stay within the 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

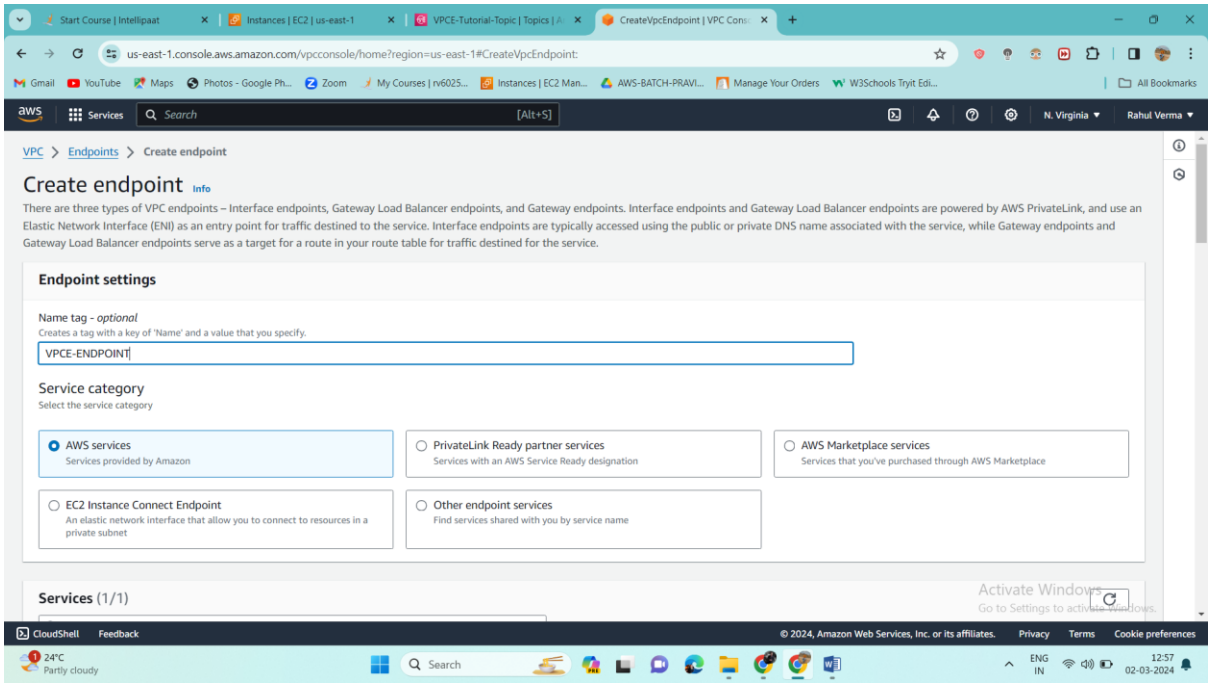
Let’s create end point now so go to vpc in amazon console



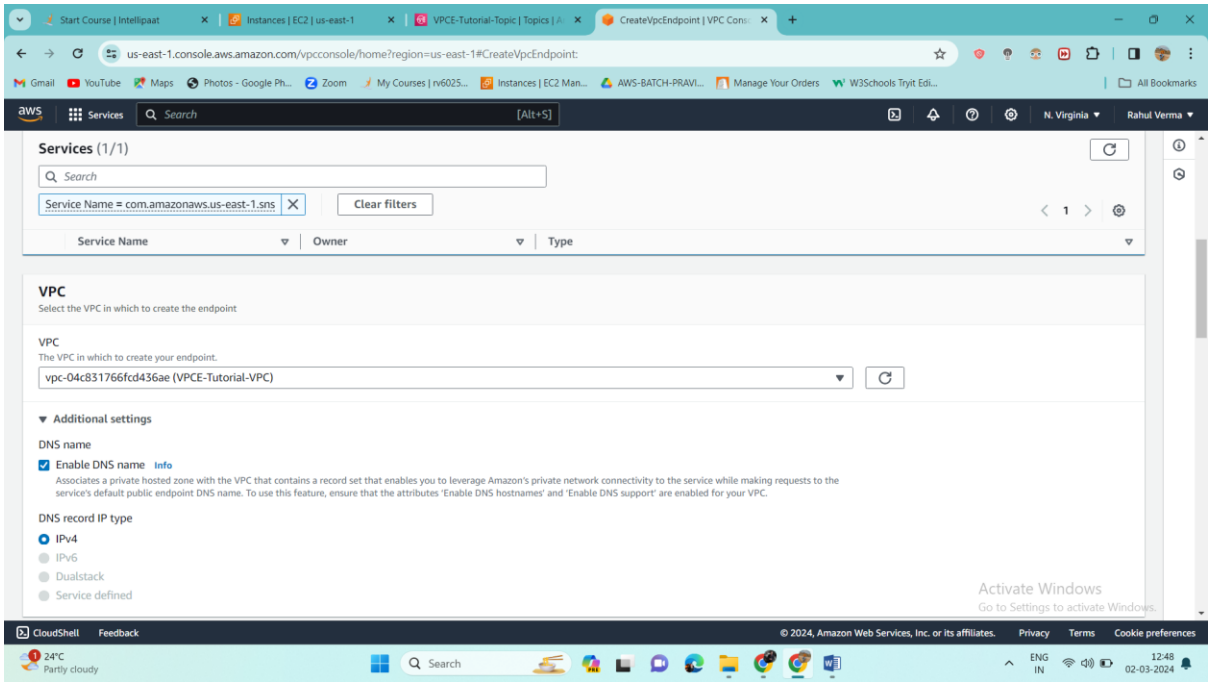
Now create endpoint



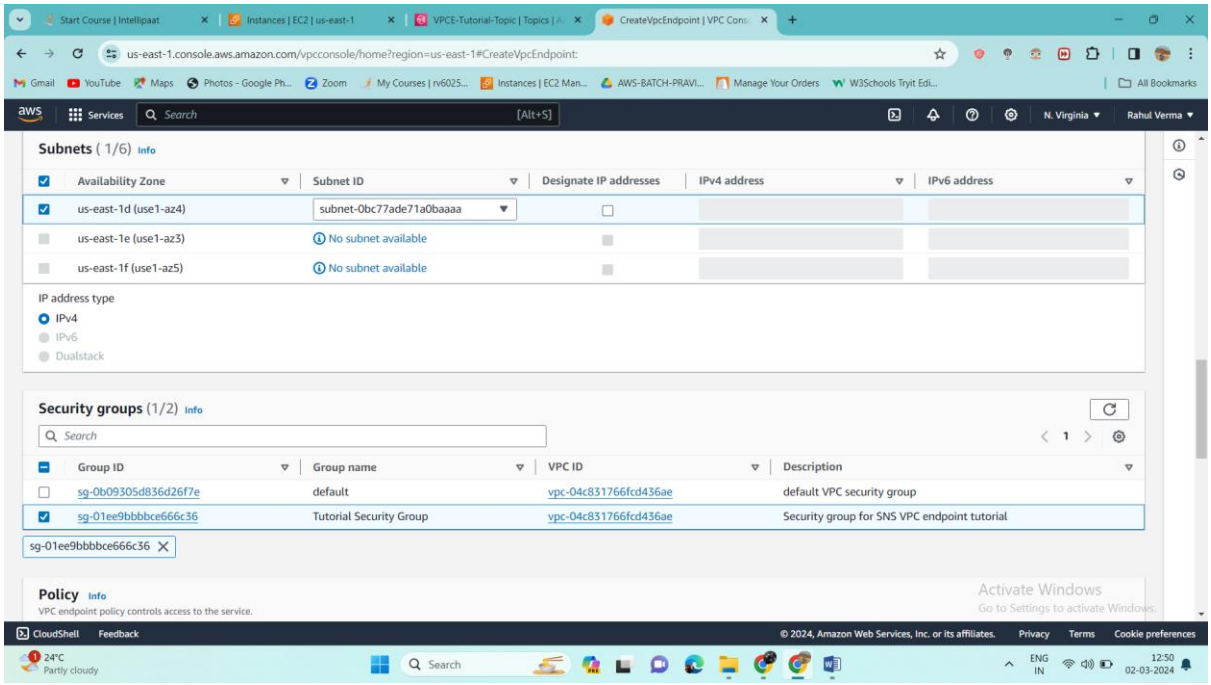
Let’s configure



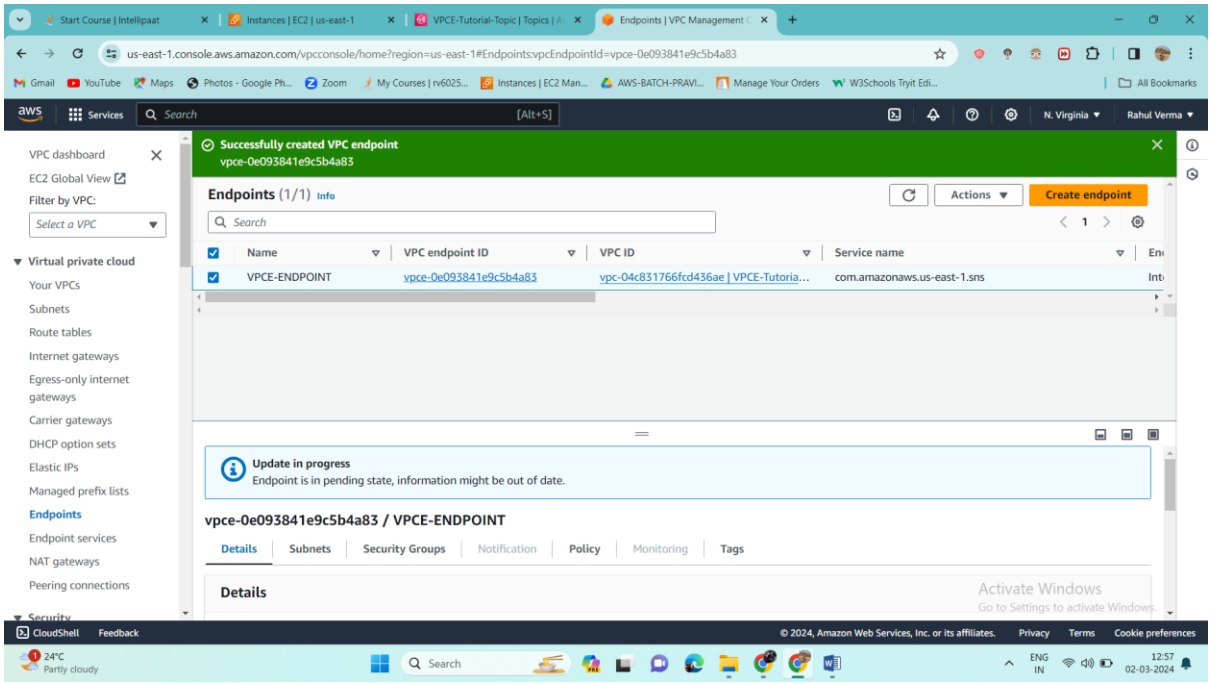
Select services, VPC & Subnet



Select security group

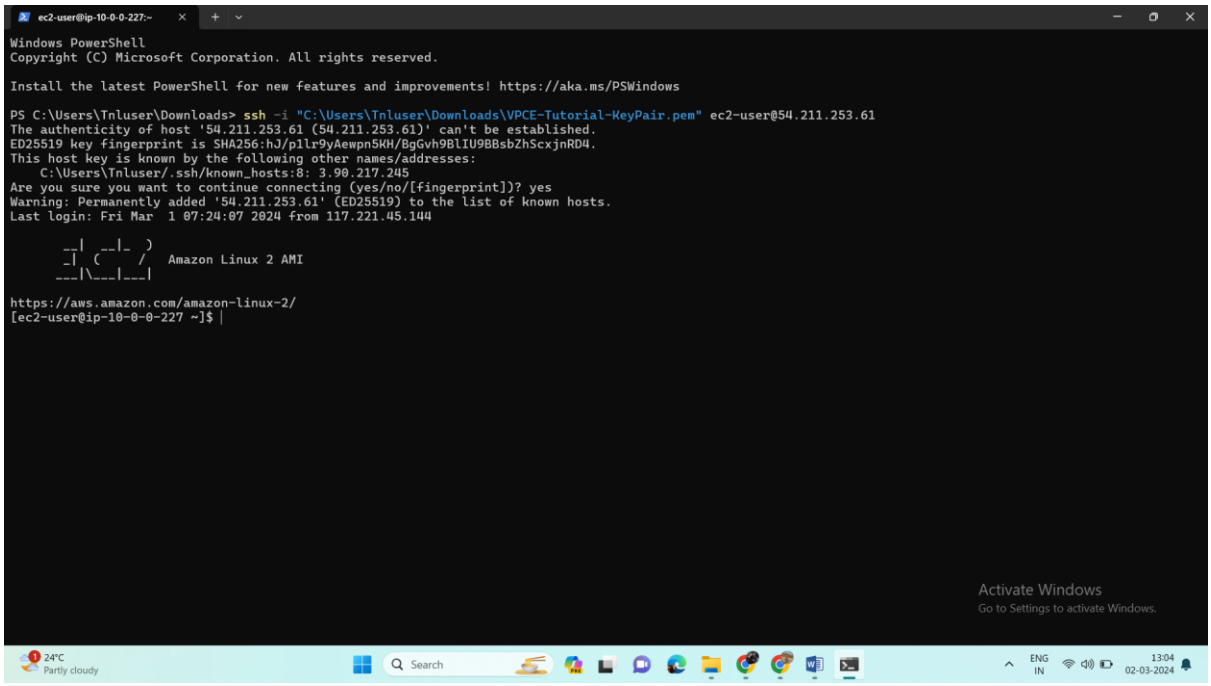


Our endpoint is created



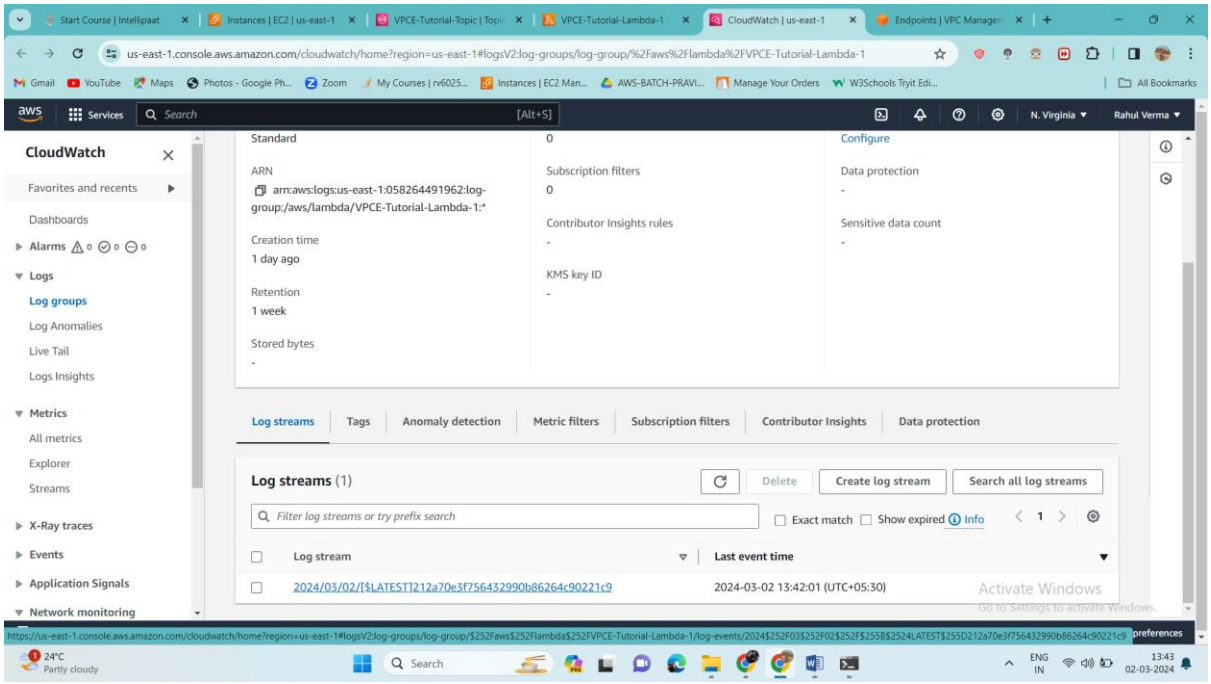
Let’s connect to our ec2 instance once again

Note we have stopped it so it’s IP is changed now

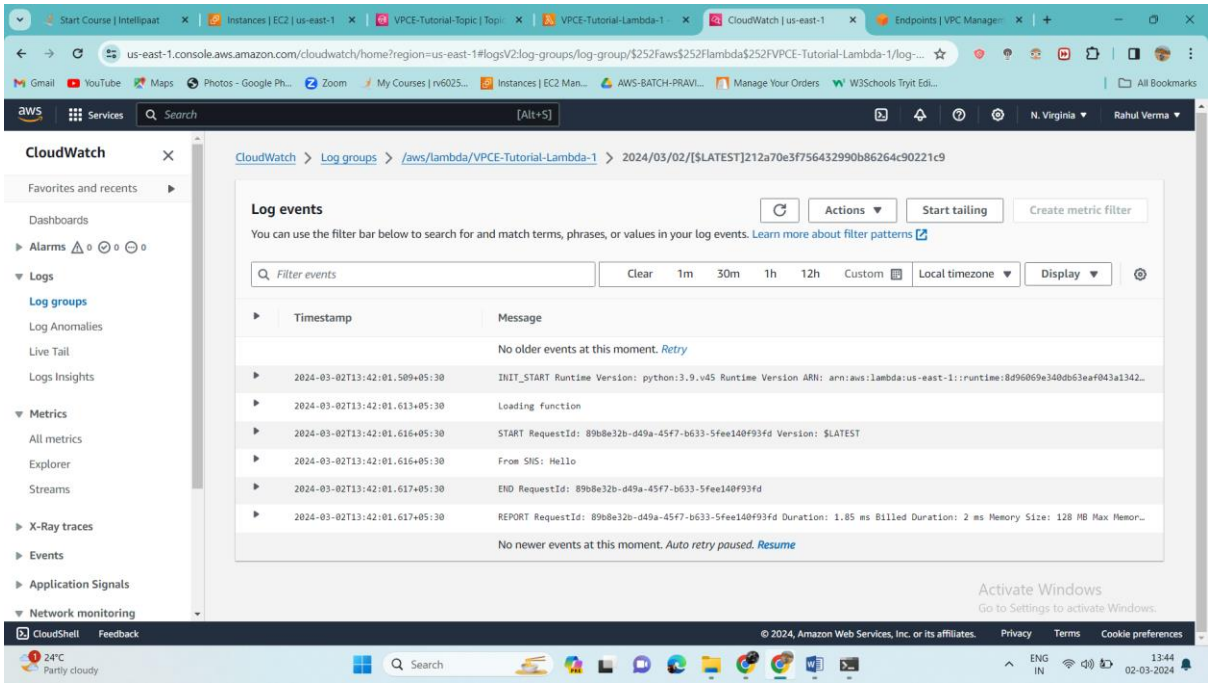


Now let’s publish a message to our Topic

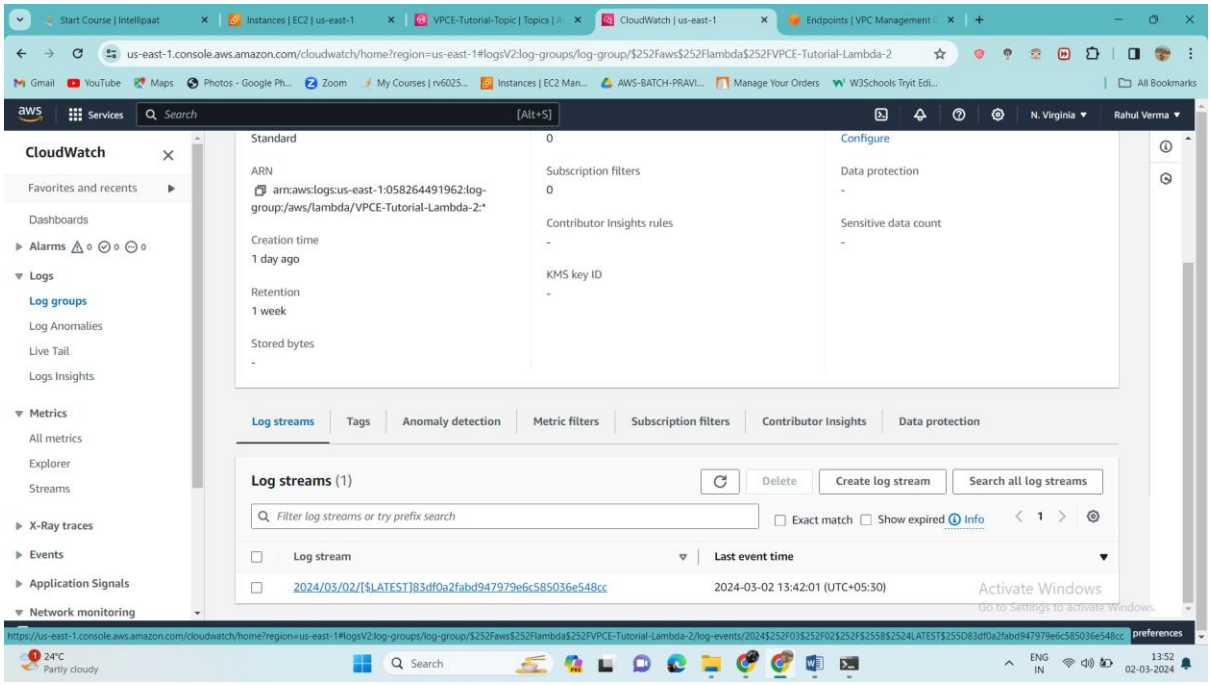
And let’s check the cloud watch logs lambda 1



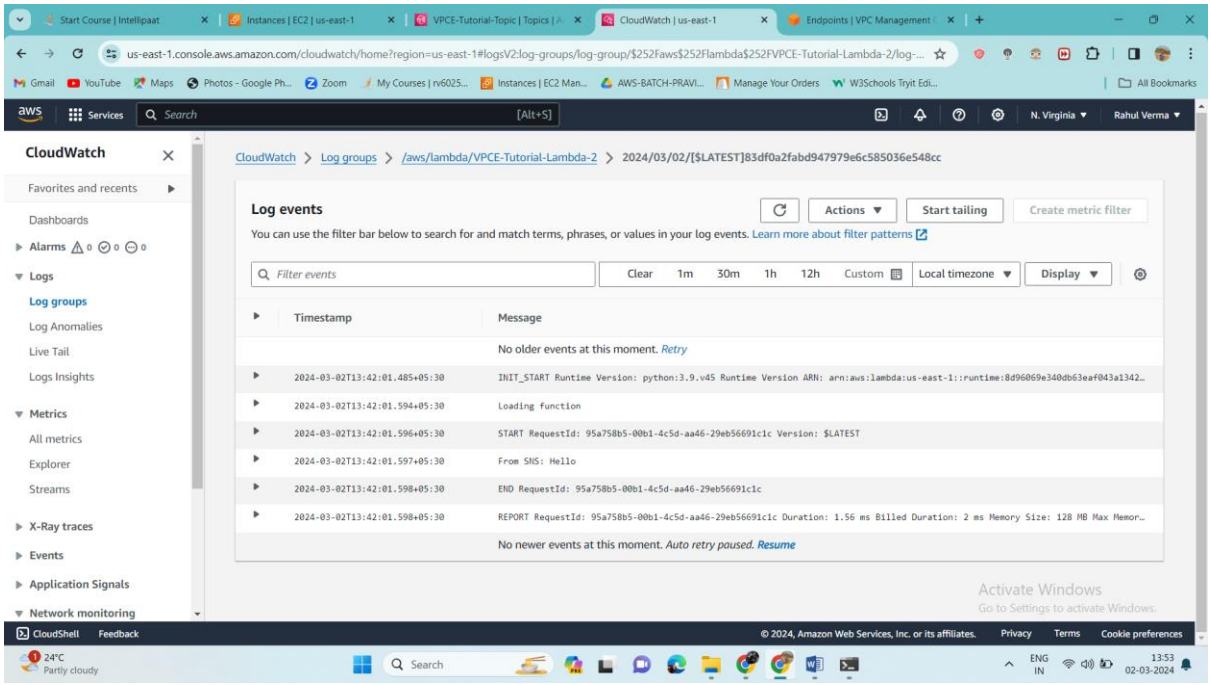
We have successfully receive message from SNS



Let’s check it in second log lambda2



We have received in both the lambda functions



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.