AWS PROJECT3

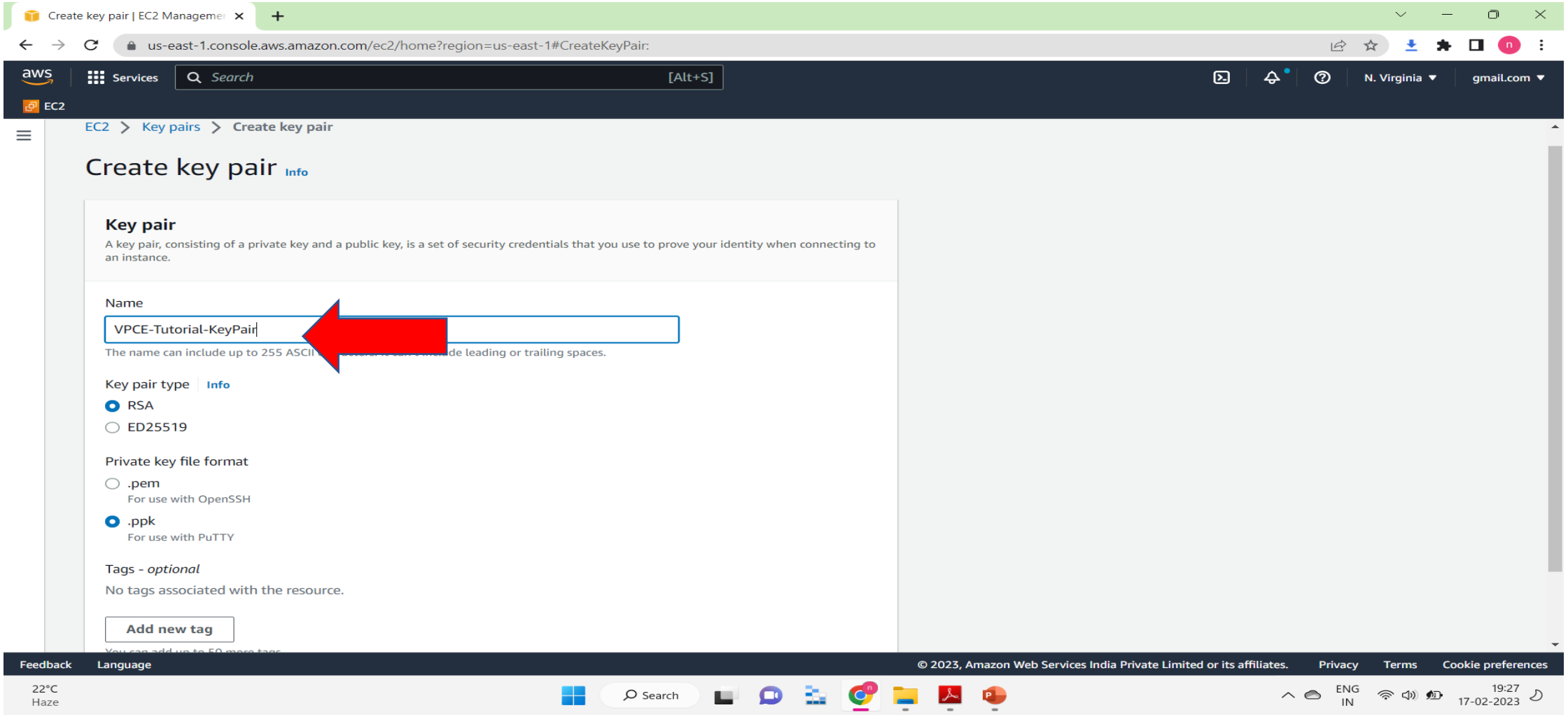
NAME: NIVEDITA PATHAK

COURSE: MASTER'S IN DEVOPS ARCHITECT

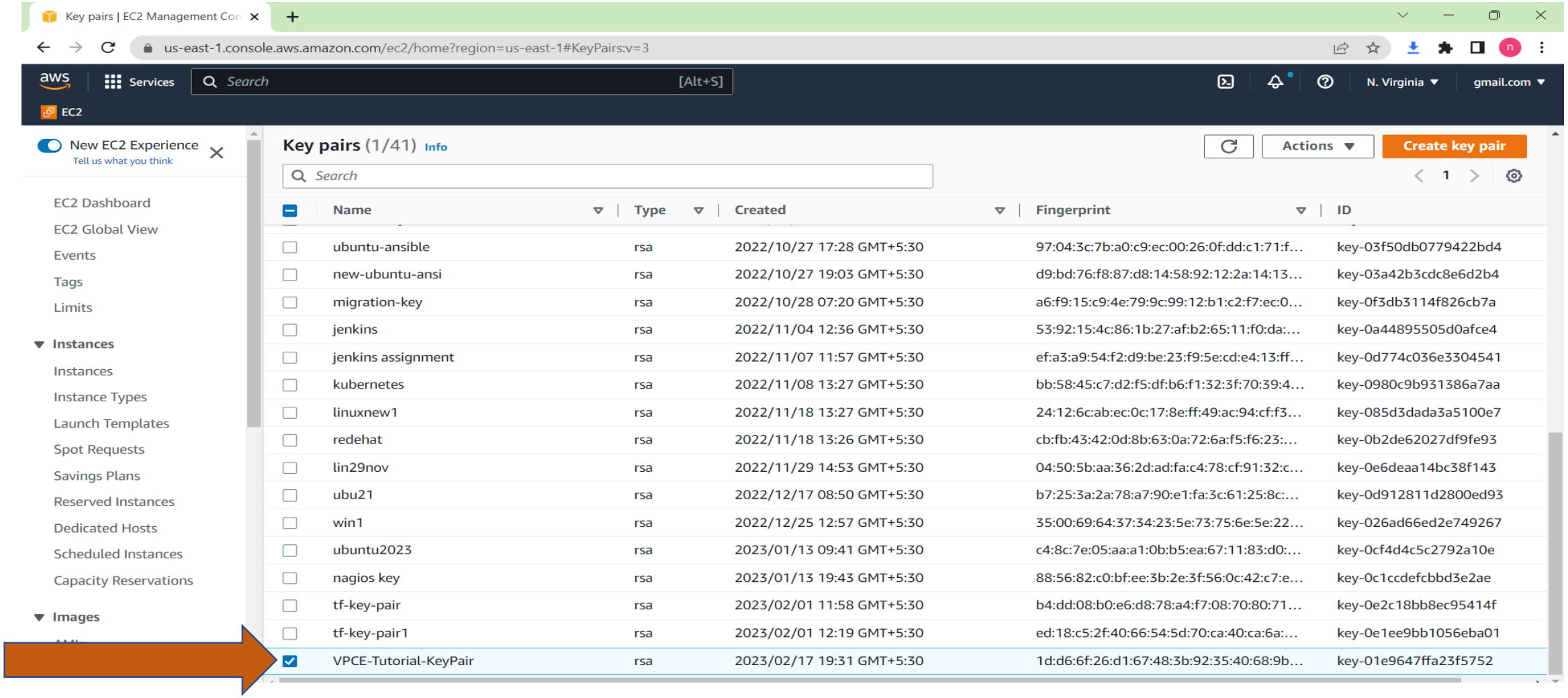
Project 3 – Publishing Amazon SNS Messages Privately

- **Project:** 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 which 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

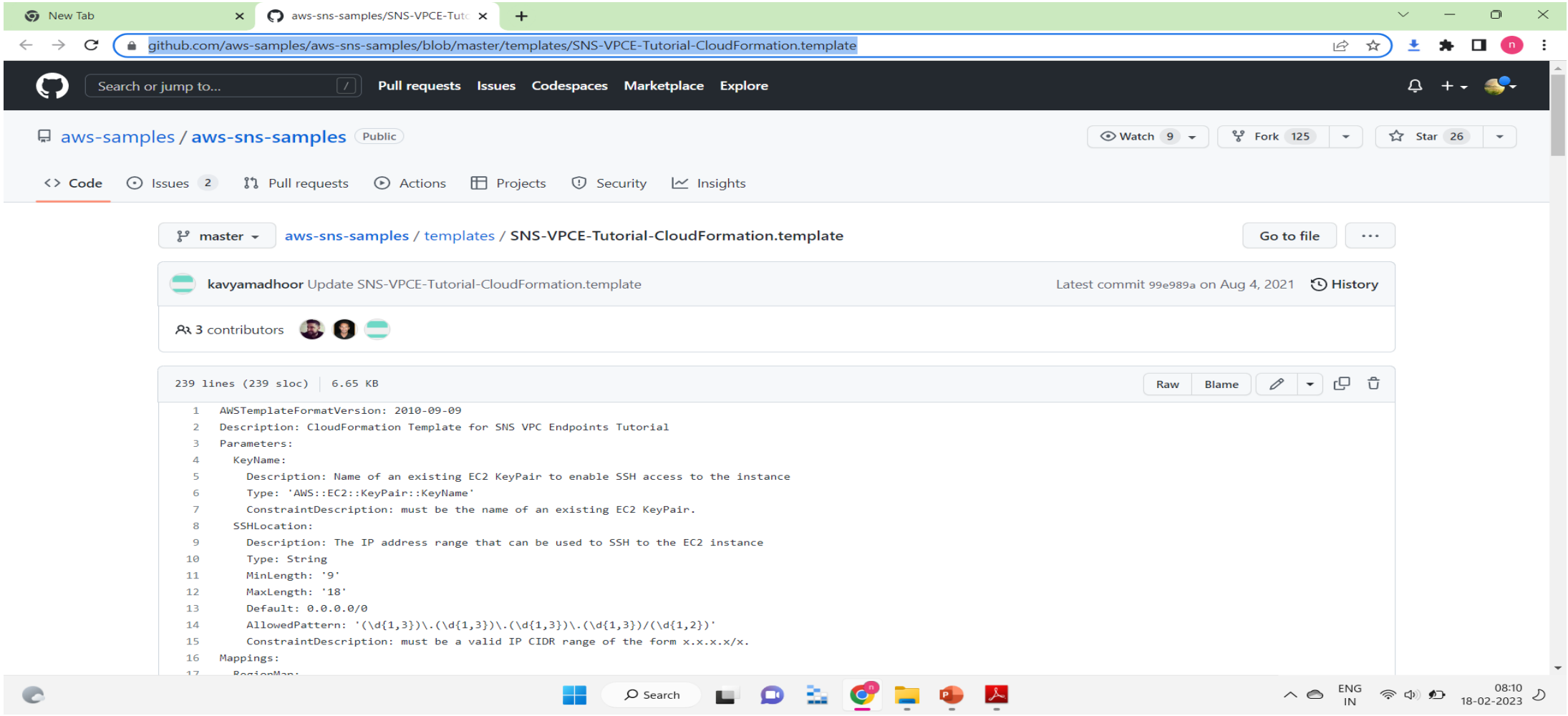
1.went to create key pair



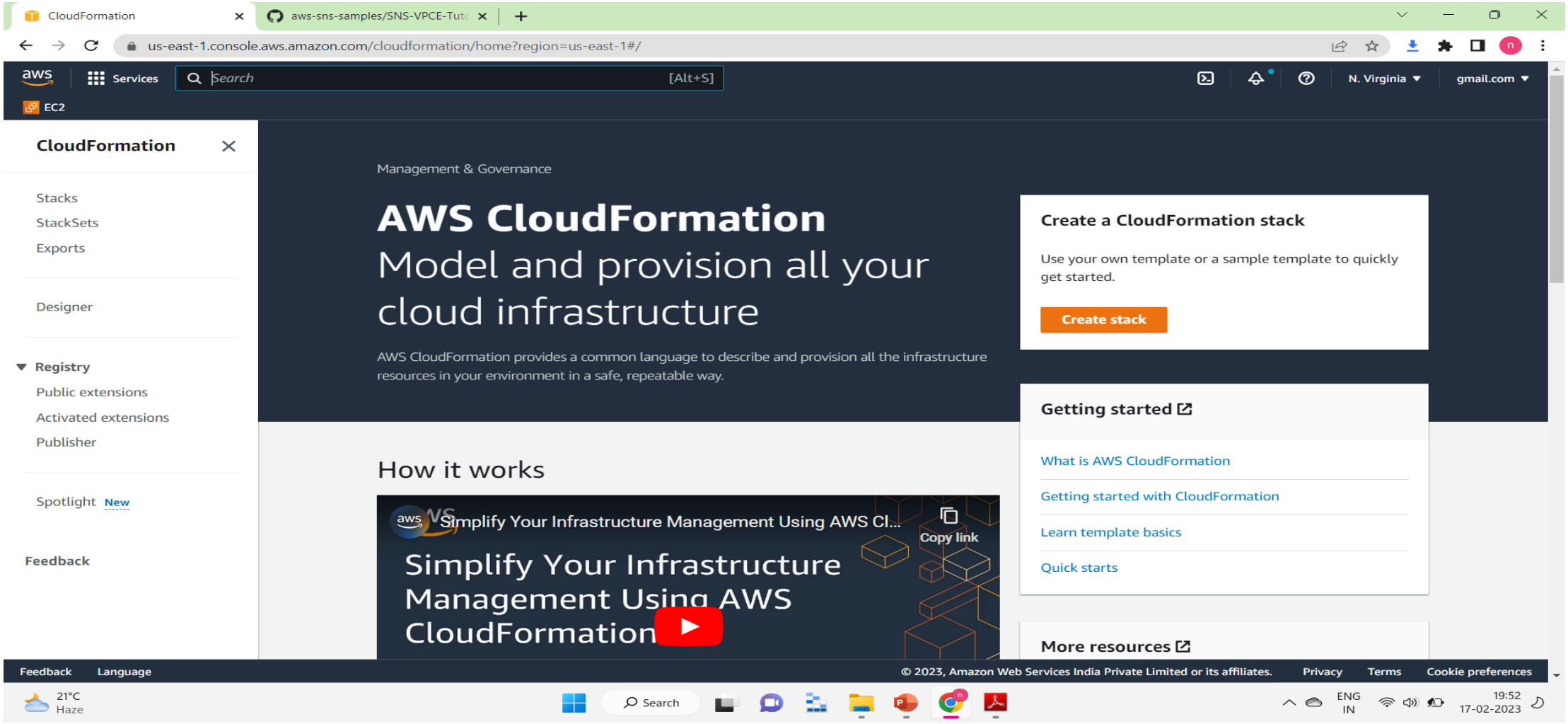
created key-pair

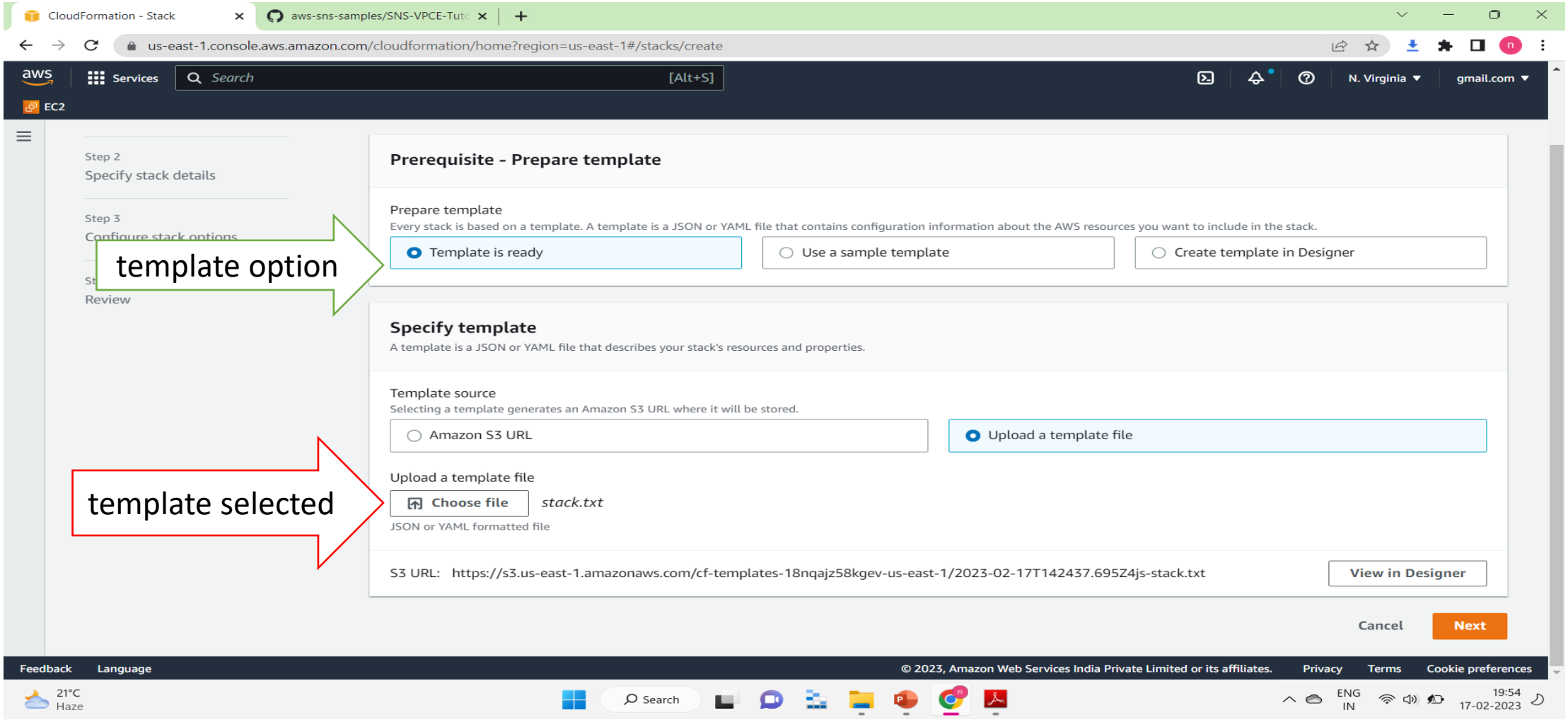


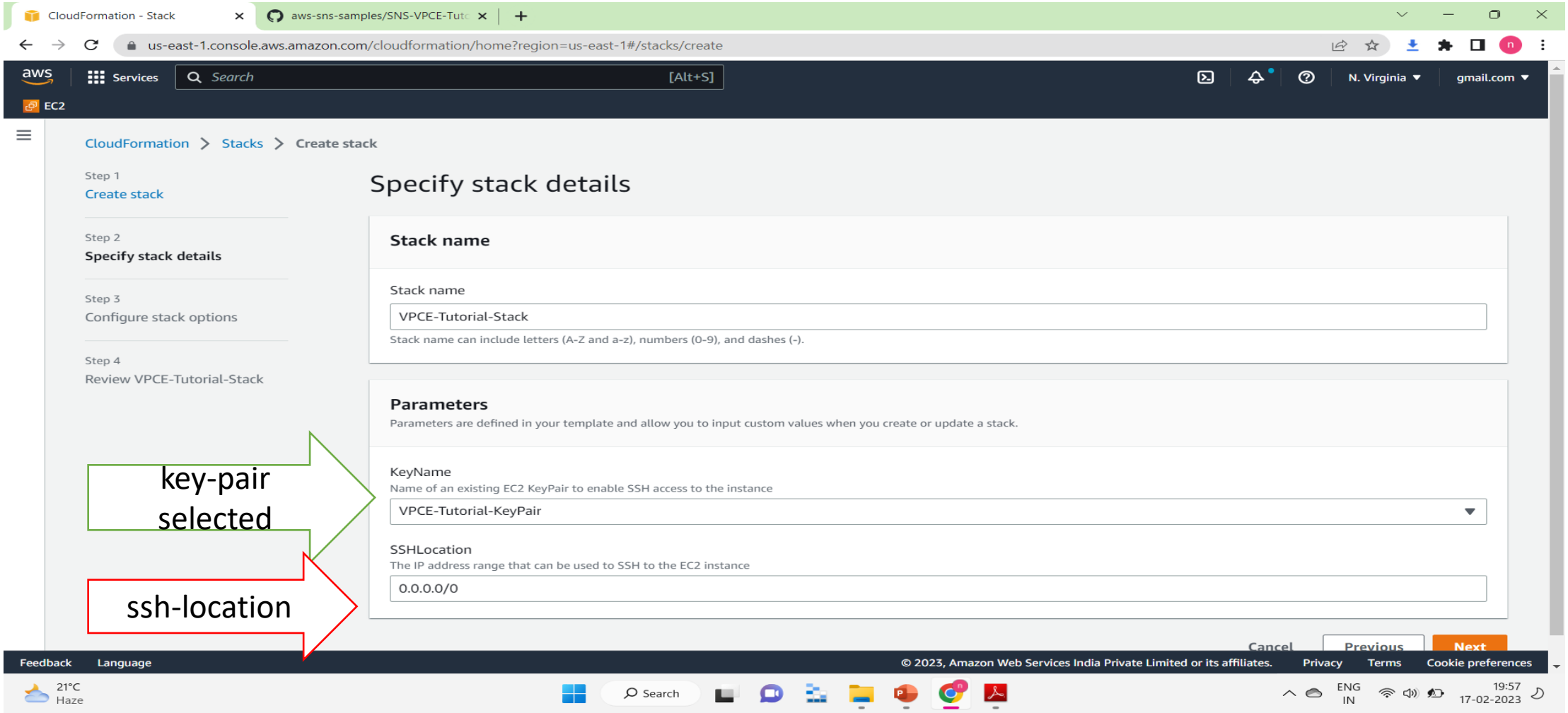
step 2. went to github to **download the template file**



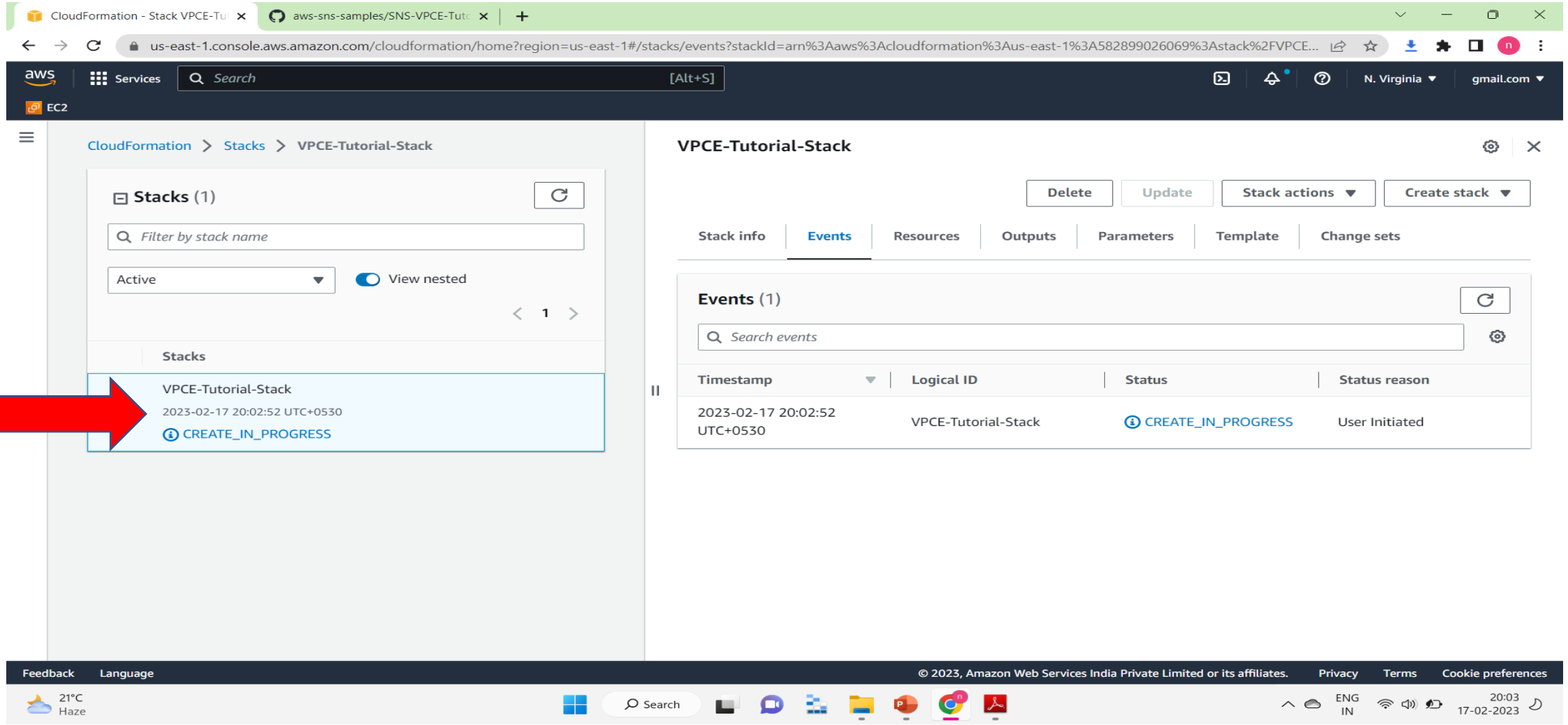
Step3. went to create stack



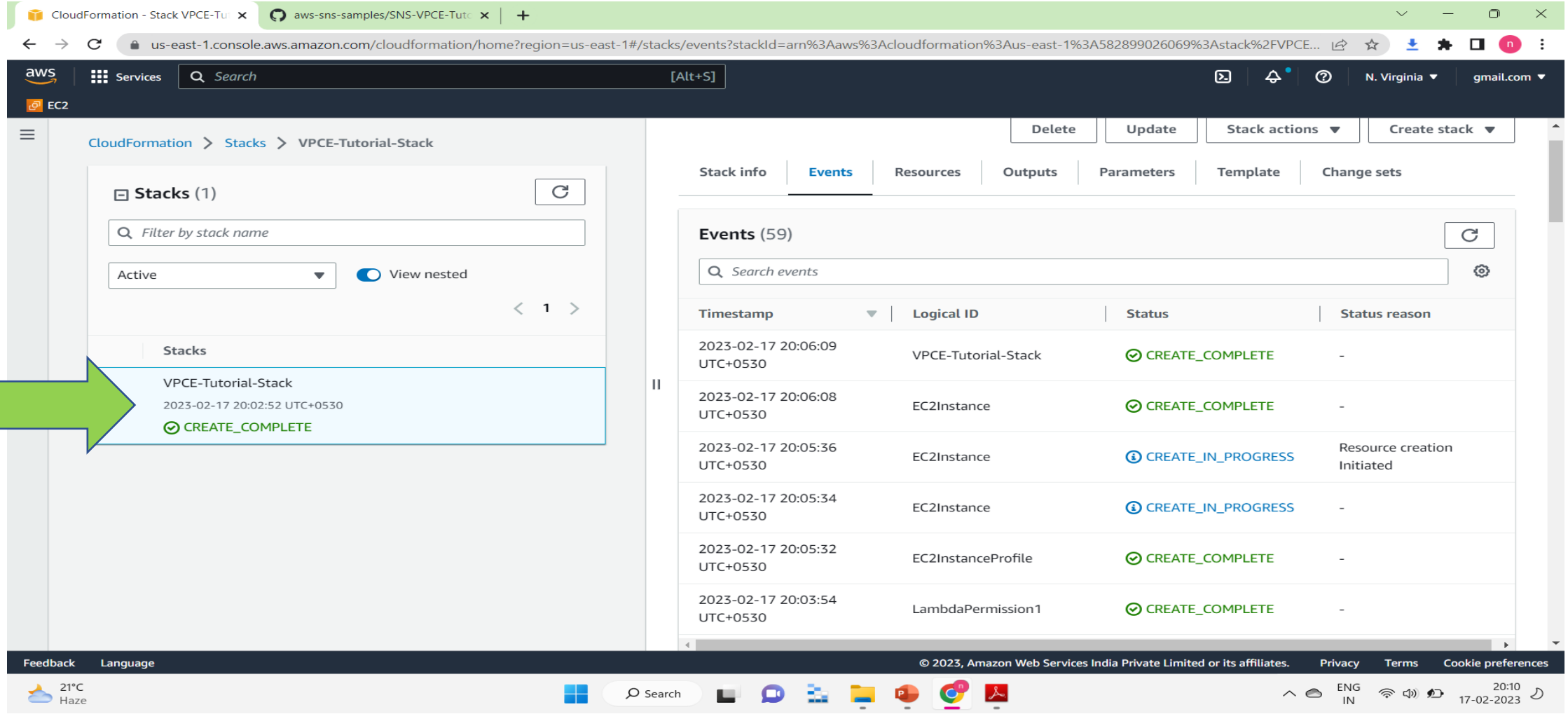

CloudFormation - Stack
aws-sns-samples/SNS-VPCE-Tut
us-east-1.console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/create
aws
Services
Search
[Alt+S]
N. Virginia
gmail.com
EC2
Step 2
Specify stack details
Step 3
Configure stack options
Review
template option
Prerequisite - Prepare template
Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.
Template is ready
Use a sample template
Create template in Designer
Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.
Template source
Selecting a template generates an Amazon S3 URL where it will be stored.
Amazon S3 URL
Upload a template file
template selected
Upload a template file
Choose file
stack.txt
JSON or YAML formatted file
S3 URL: https://s3.us-east-1.amazonaws.com/cf-templates-18nqajz58kgev-us-east-1/2023-02-17T142437.695Z4js-stack.txt
View in Designer
Cancel
Next
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
21°C
Haze
Search
ENG
IN
19:54
17-02-2023


CloudFormation - Stack
aws-sns-samples/SNS-VPCE-Tut
us-east-1.console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/create
aws
Services
Search
[Alt+S]
N. Virginia
gmail.com
EC2
CloudFormation > Stacks > Create stack
Step 1
Create stack
Step 2
Specify stack details
Step 3
Configure stack options
Step 4
Review VPCE-Tutorial-Stack
Specify stack details
Stack name
Stack name
VPCE-Tutorial-Stack
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
KeyName
Name of an existing EC2 KeyPair to enable SSH access to the instance
VPCE-Tutorial-KeyPair
SSHLocation
The IP address range that can be used to SSH to the EC2 instance
0.0.0.0/0
key-pair selected
ssh-location
Cancel
Previous
Next
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
21°C
Haze
Search
ENG
IN
19:57
17-02-2023

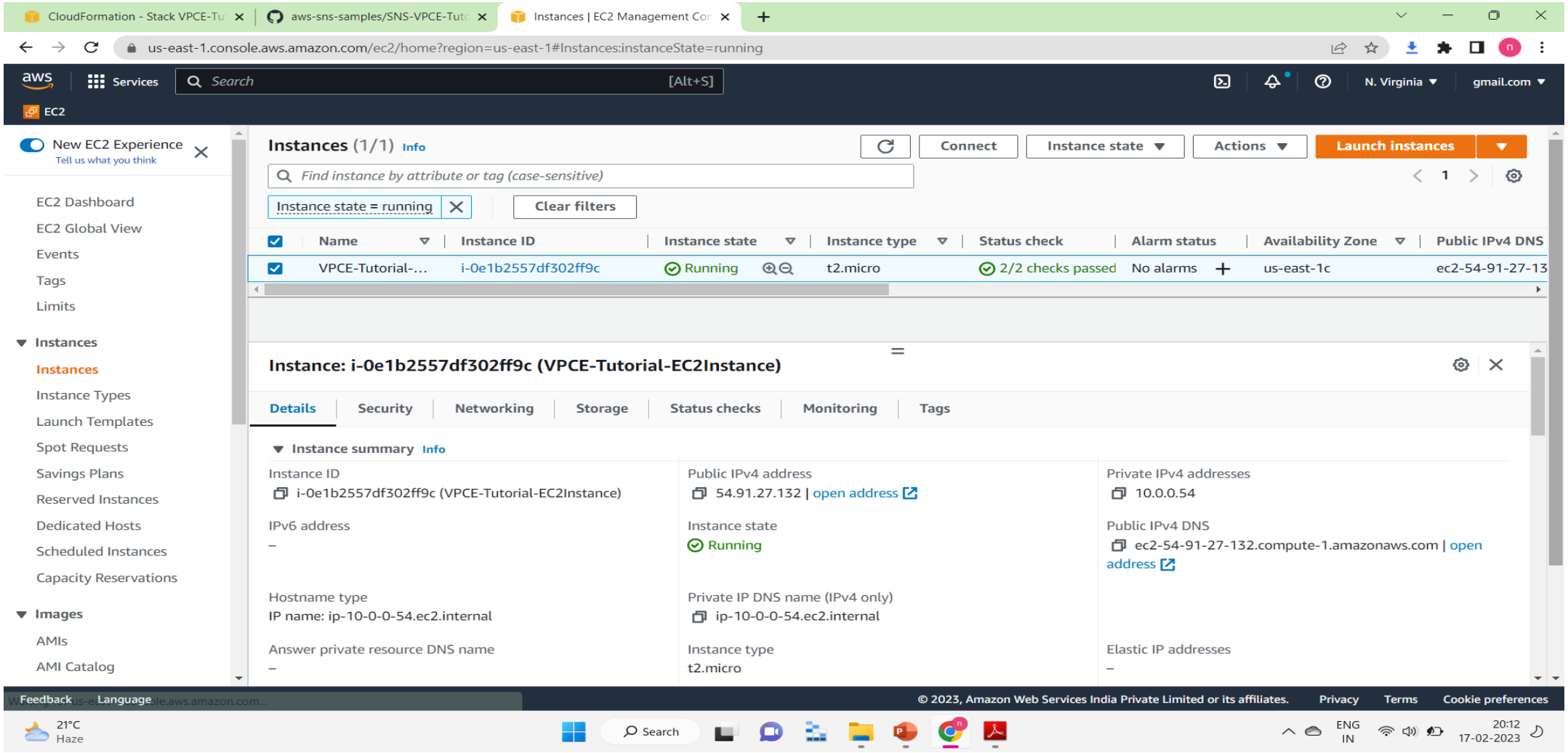
stack creation in progress

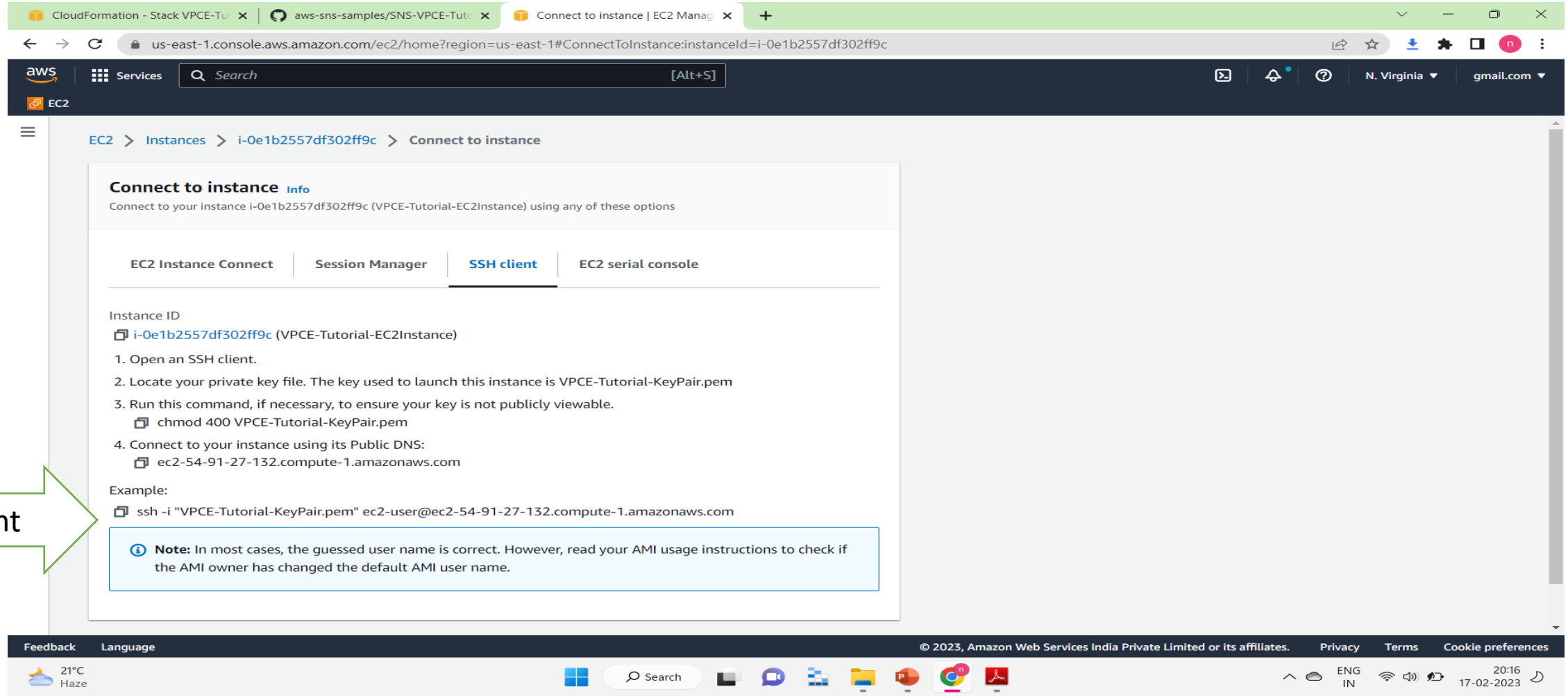


stack created



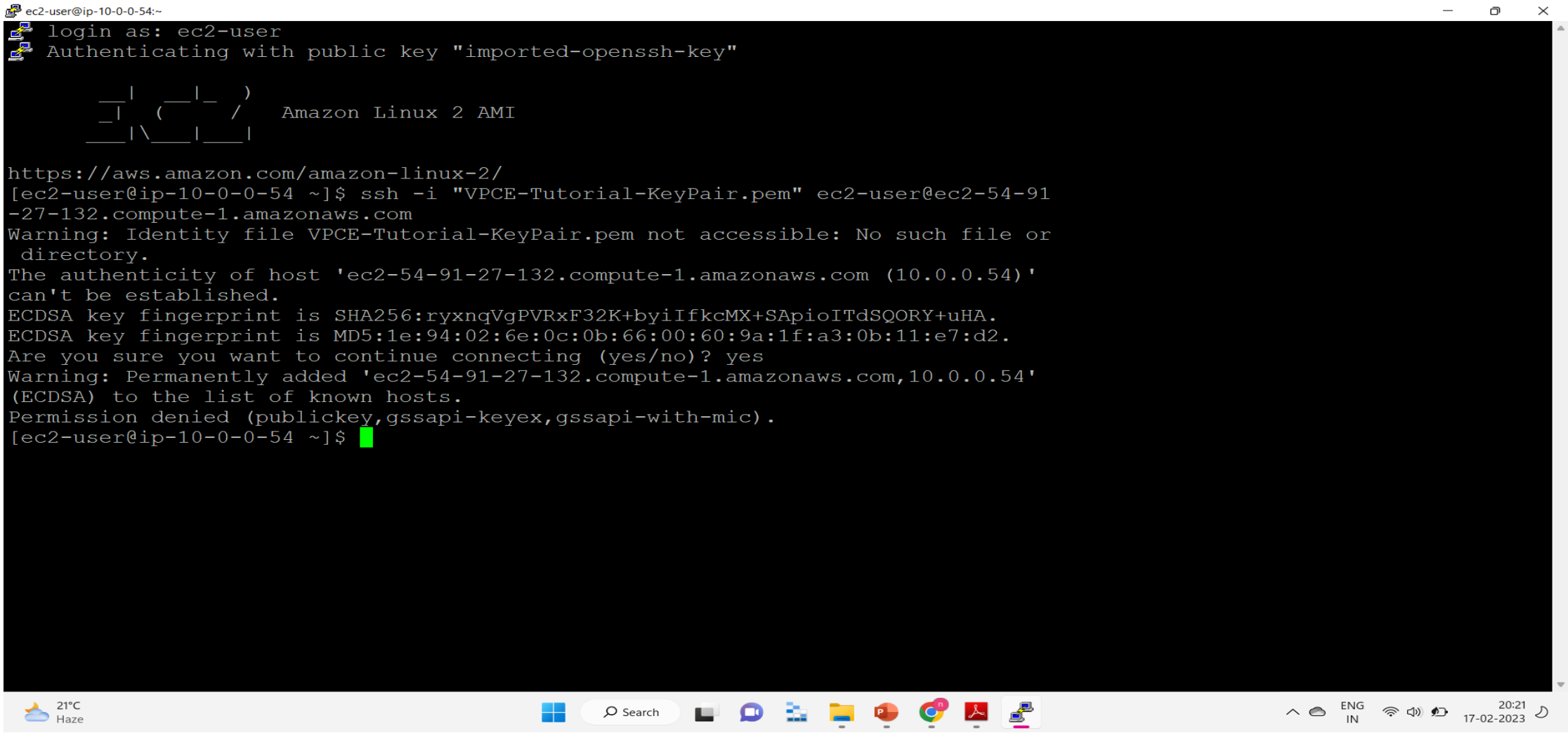
step4: instance connection establishment



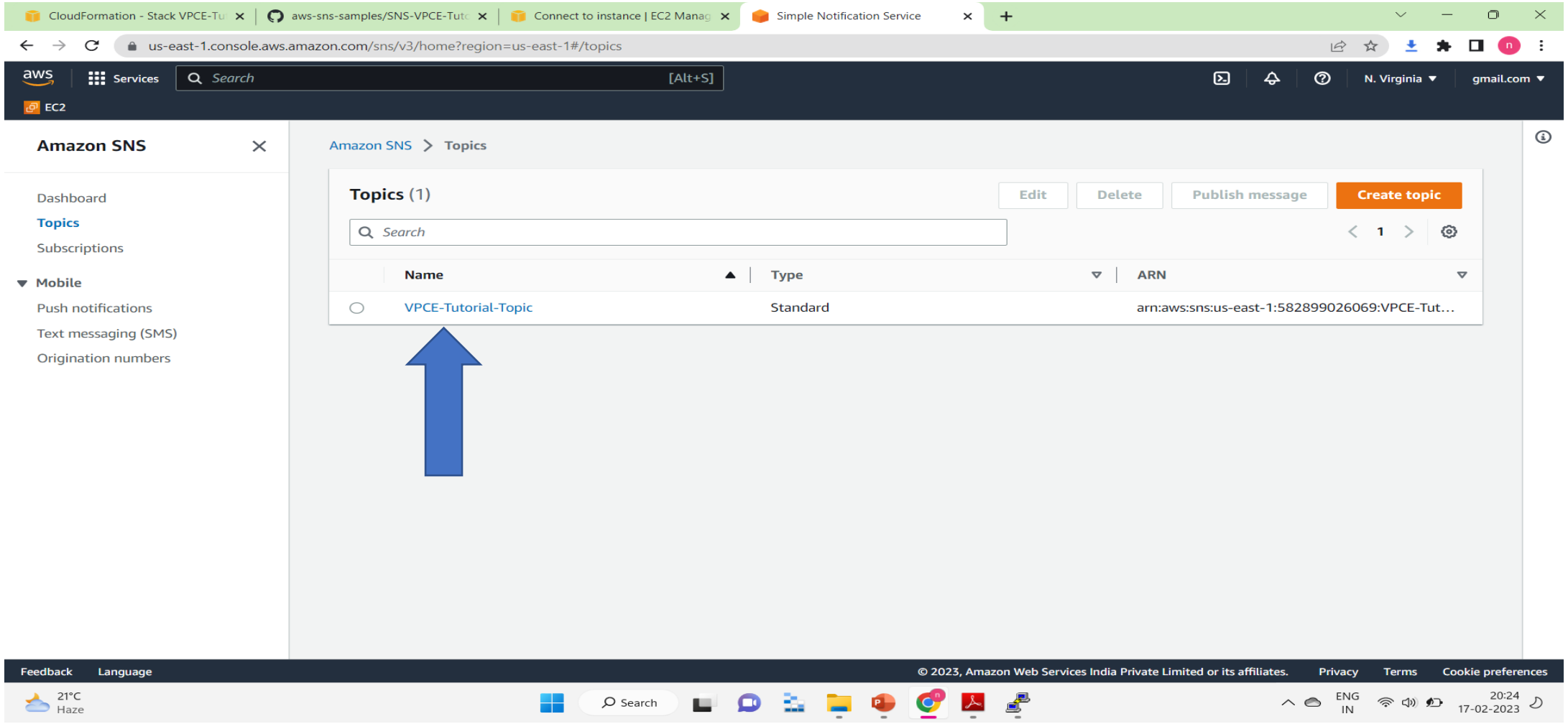

CloudFormation - Stack VPCE-Tu
aws-sns-samples/SNS-VPCE-Tute
Connect to instance | EC2 Manag
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ConnectToInstance:instanceId=i-0e1b2557df302ff9c
aws
Services
Search
[Alt+S]
N. Virginia
gmail.com
EC2
EC2 > Instances > i-0e1b2557df302ff9c > Connect to instance
Connect to instance Info
Connect to your instance i-0e1b2557df302ff9c (VPCE-Tutorial-EC2Instance) using any of these options
EC2 Instance Connect
Session Manager
SSH client
EC2 serial console
Instance ID
i-0e1b2557df302ff9c (VPCE-Tutorial-EC2Instance)
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is VPCE-Tutorial-KeyPair.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 VPCE-Tutorial-KeyPair.pem
4. Connect to your instance using its Public DNS:
ec2-54-91-27-132.compute-1.amazonaws.com
Example:
ssh -i "VPCE-Tutorial-KeyPair.pem" ec2-user@ec2-54-91-27-132.compute-1.amazonaws.com
Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
21°C
Haze
Search
ENG
IN
20:16
17-02-2023

sh-client

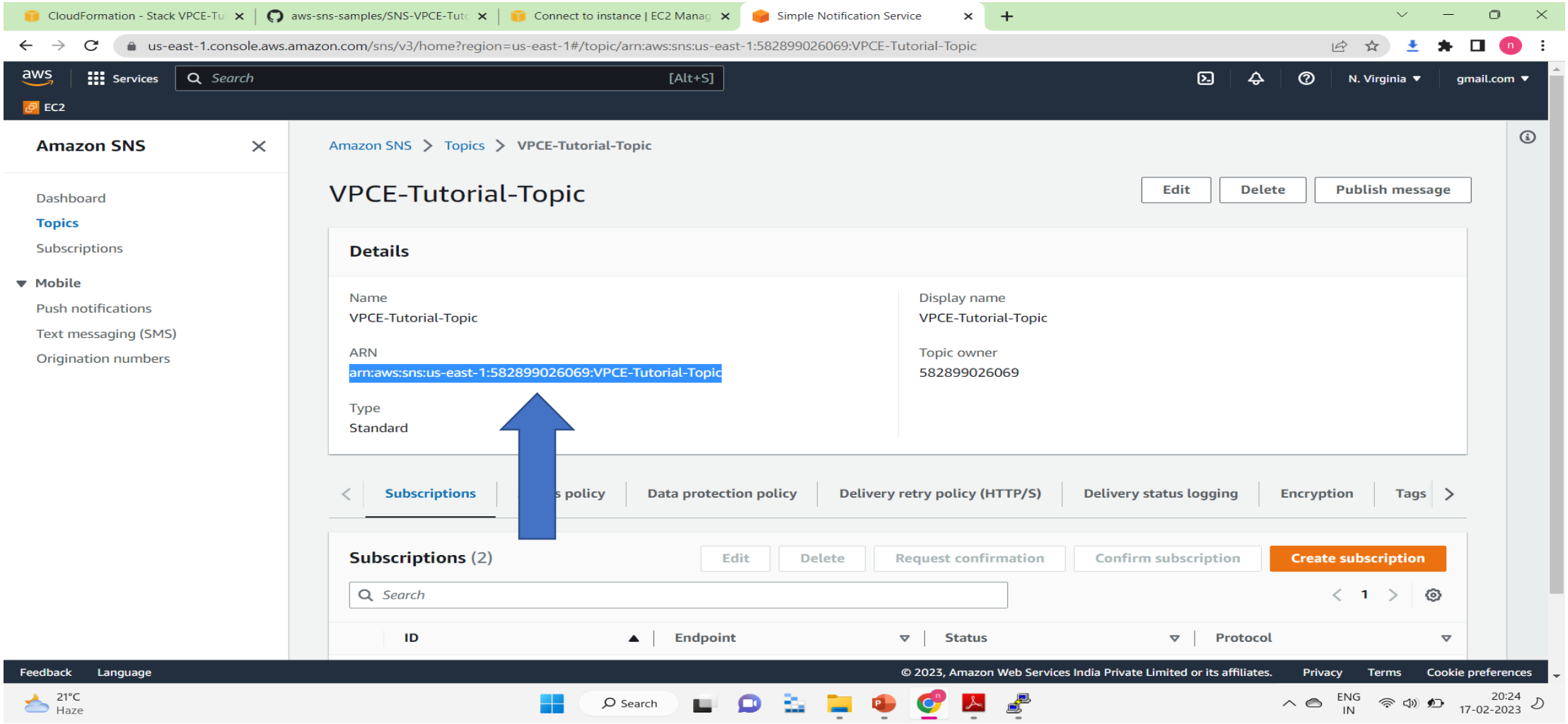
step5. checked permission of connection through ssh , which was denied



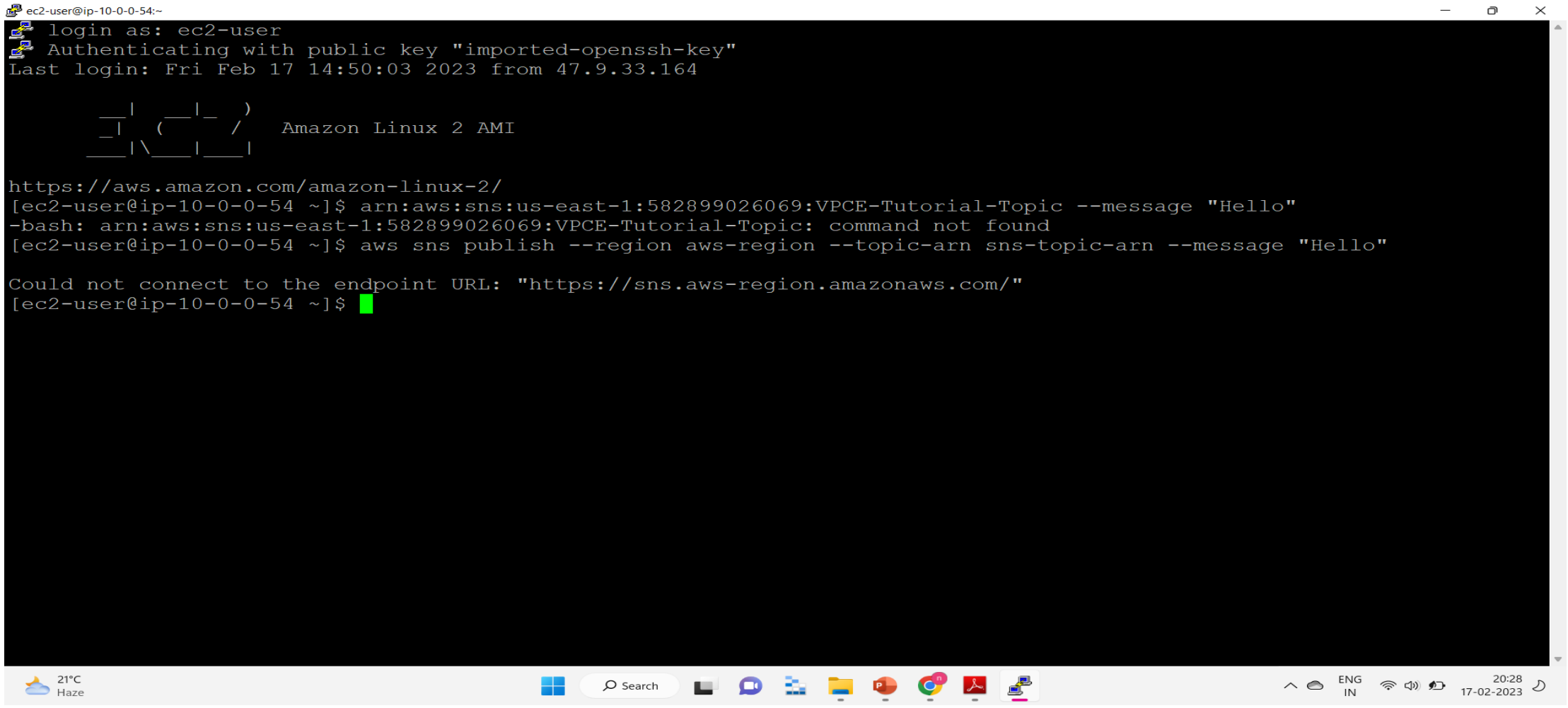
step 6. Went to SNS



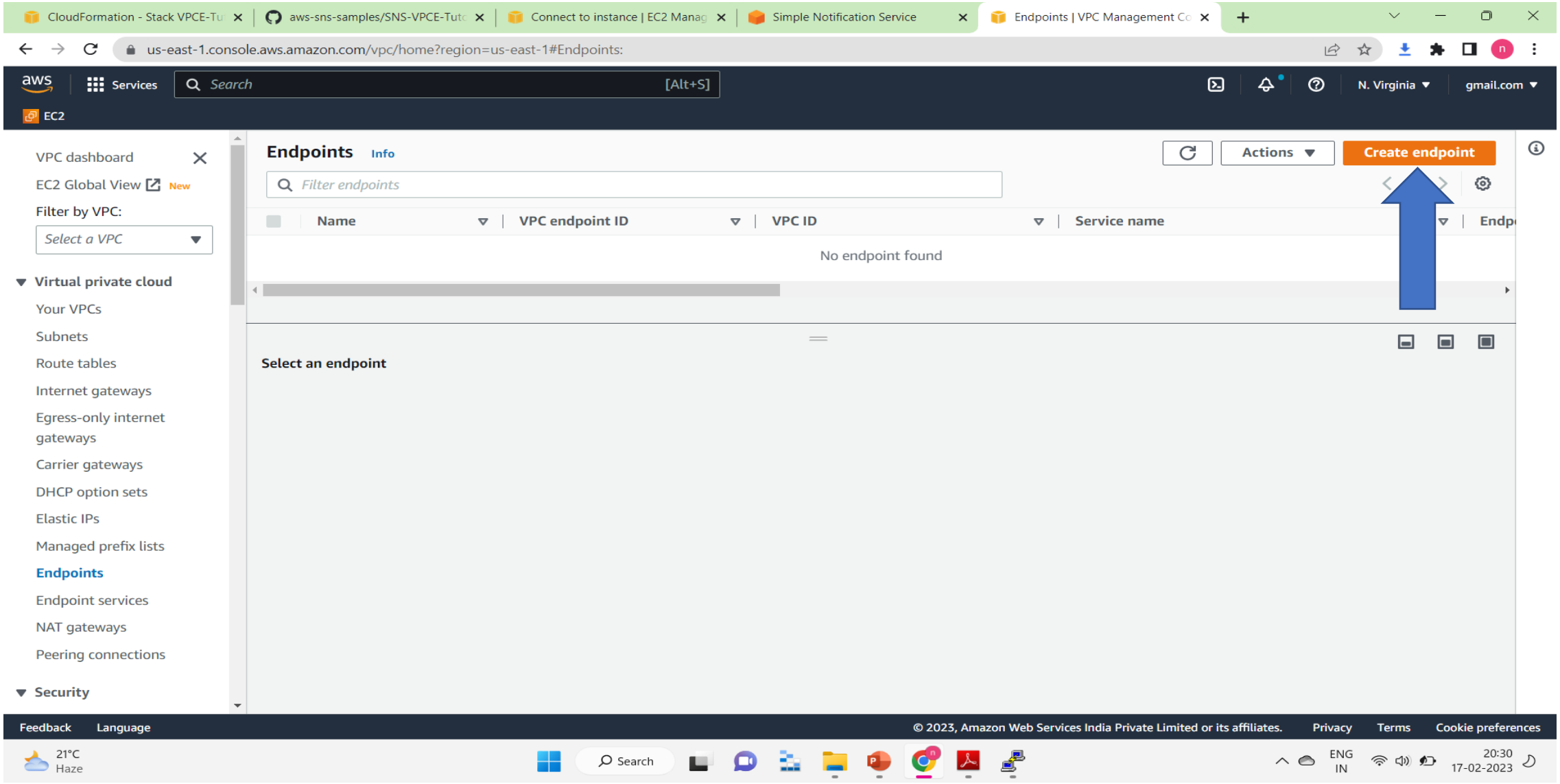
copied ARN

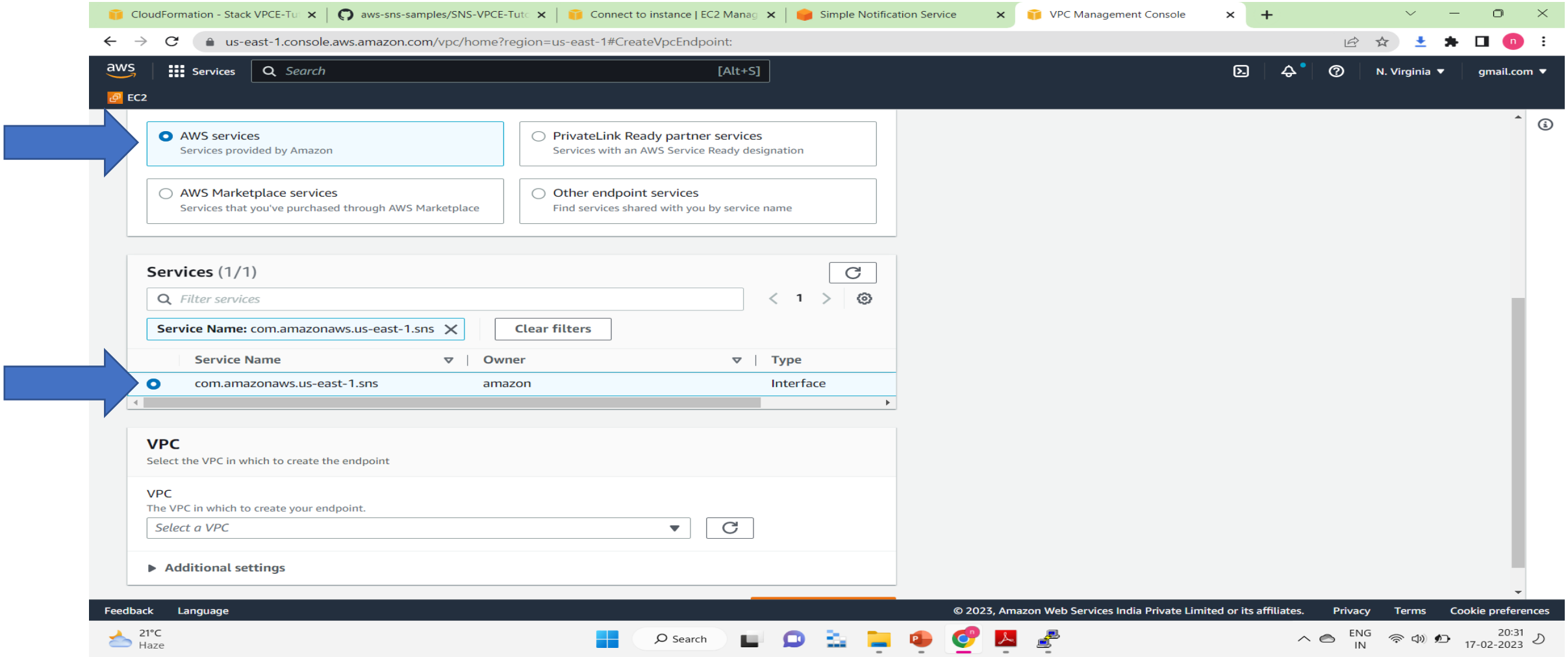

CloudFormation - Stack VPCE-Tu
aws-sns-samples/SNS-VPCE-Tut
Connect to instance | EC2 Manag
Simple Notification Service
us-east-1.console.aws.amazon.com/sns/v3/home?region=us-east-1#/topic/arn:aws:sns:us-east-1:582899026069:VPCE-Tutorial-Topic
Services
Search
[Alt+S]
N. Virginia
gmail.com
EC2
Amazon SNS
Dashboard
Topics
Subscriptions
Mobile
Push notifications
Text messaging (SMS)
Origination numbers
Amazon SNS > Topics > VPCE-Tutorial-Topic
VPCE-Tutorial-Topic
Edit
Delete
Publish message
Details
Name
VPCE-Tutorial-Topic
ARN
arn:aws:sns:us-east-1:582899026069:VPCE-Tutorial-Topic
Type
Standard
Display name
VPCE-Tutorial-Topic
Topic owner
582899026069
Subscriptions
Data protection policy
Delivery retry policy (HTTP/S)
Delivery status logging
Encryption
Tags
Subscriptions (2)
Edit
Delete
Request confirmation
Confirm subscription
Create subscription
Search
ID
Endpoint
Status
Protocol
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
21°C
Haze
Search
ENG
IN
20:24
17-02-2023

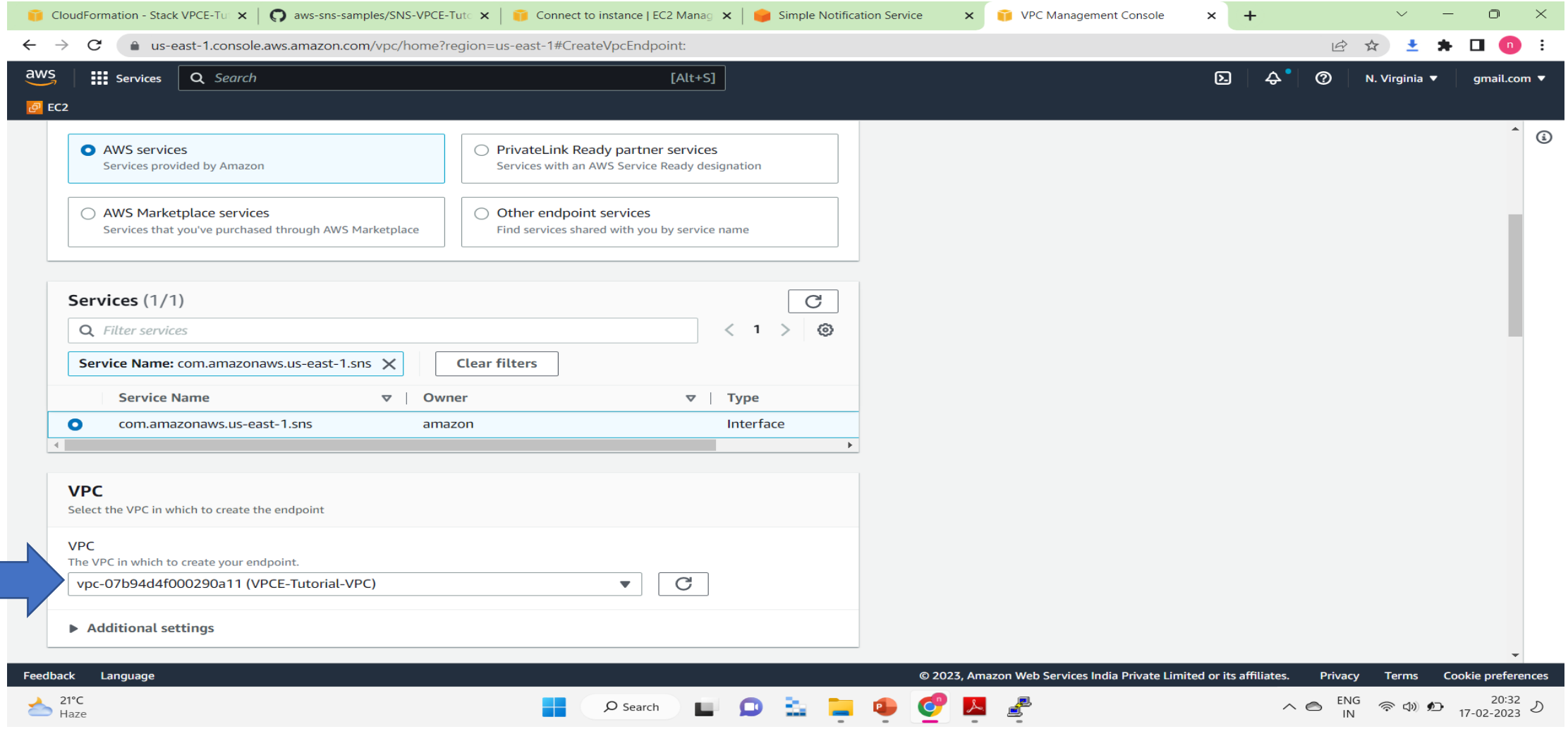
step 7. checked publish attempt, which failed

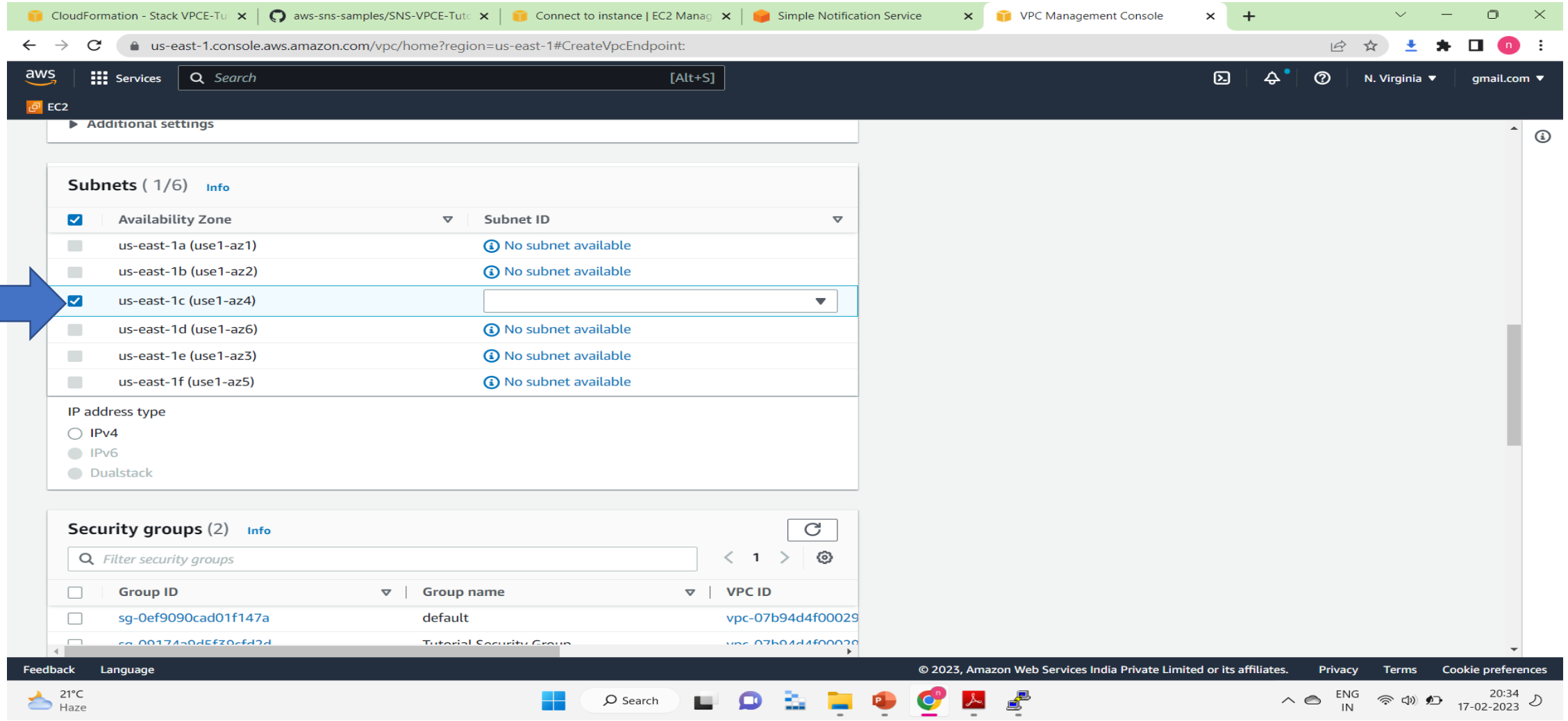


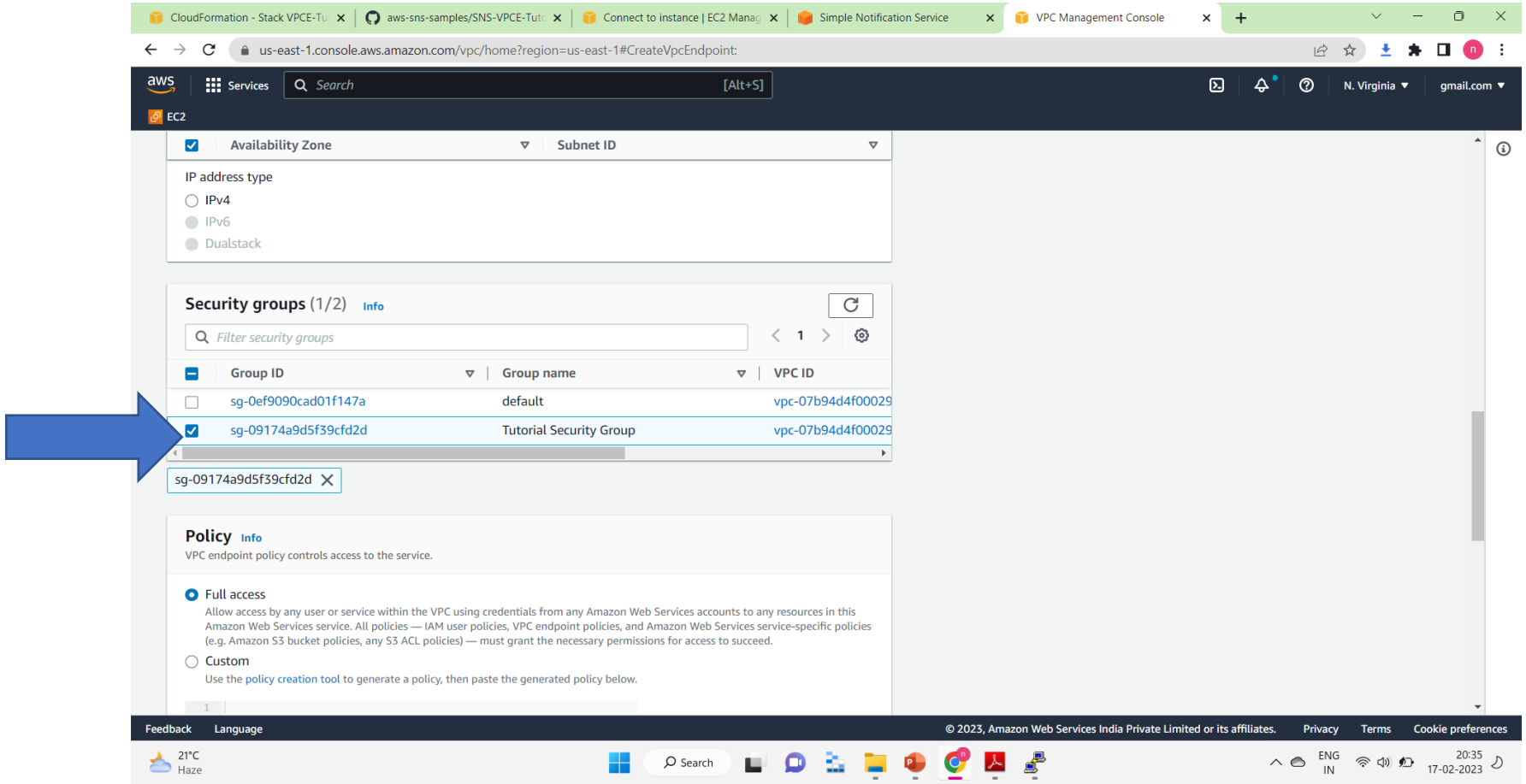
step 8: went to vpc → to create Endpoint



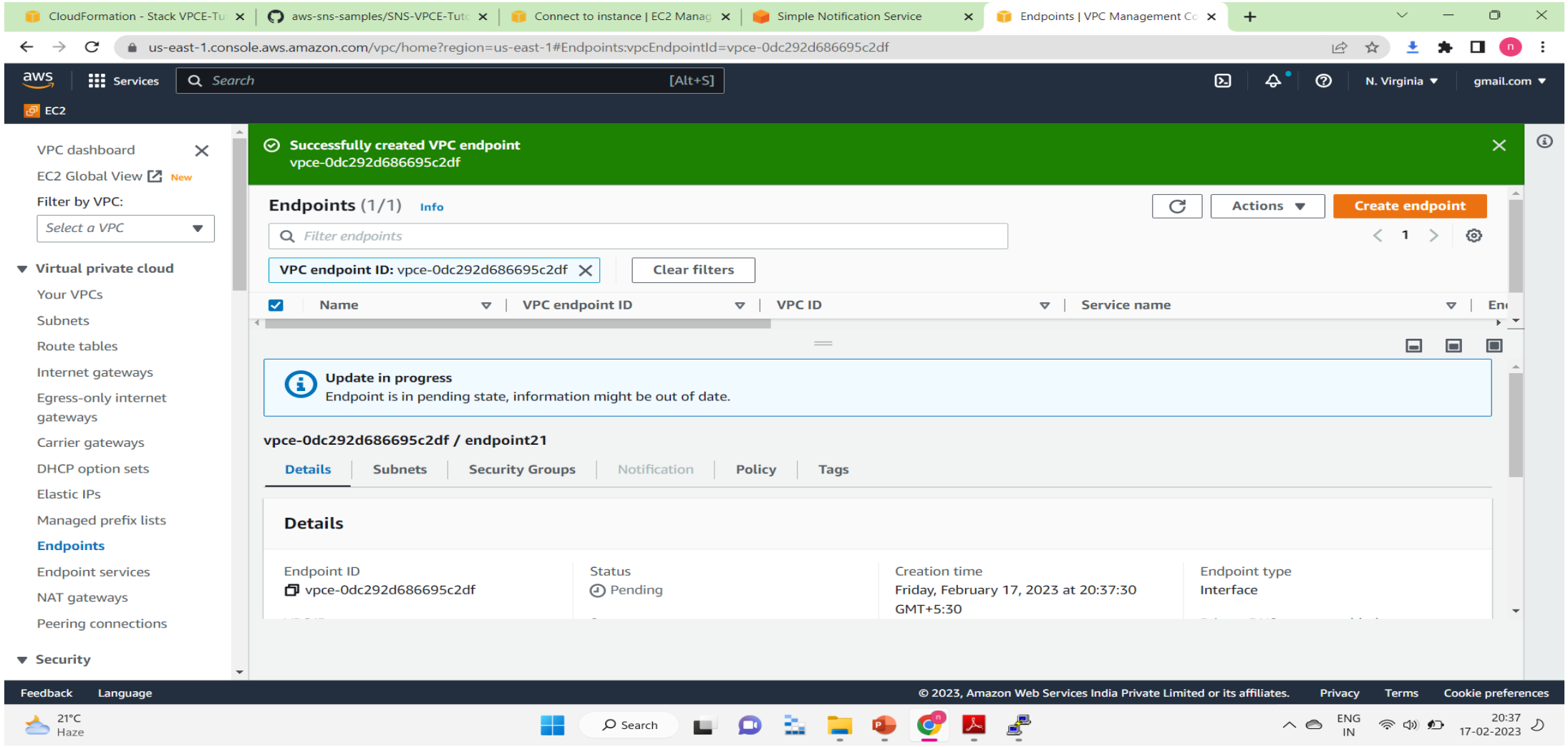

CloudFormation - Stack VPCE-Tu
aws-sns-samples/SNS-VPCE-Tut
Connect to instance | EC2 Manag
Simple Notification Service
VPC Management Console
us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint:
aws
Services
Search
[Alt+S]
N. Virginia
gmail.com
EC2
AWS services
Services provided by Amazon
PrivateLink Ready partner services
Services with an AWS Service Ready designation
AWS Marketplace services
Services that you've purchased through AWS Marketplace
Other endpoint services
Find services shared with you by service name
Services (1/1)
Filter services
1
Service Name: com.amazonaws.us-east-1.sns
Clear filters
Service Name
Owner
Type
com.amazonaws.us-east-1.sns
amazon
Interface
VPC
Select the VPC in which to create the endpoint
VPC
The VPC in which to create your endpoint.
Select a VPC
Additional settings
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
21°C
Haze
Search
ENG
IN
20:31
17-02-2023

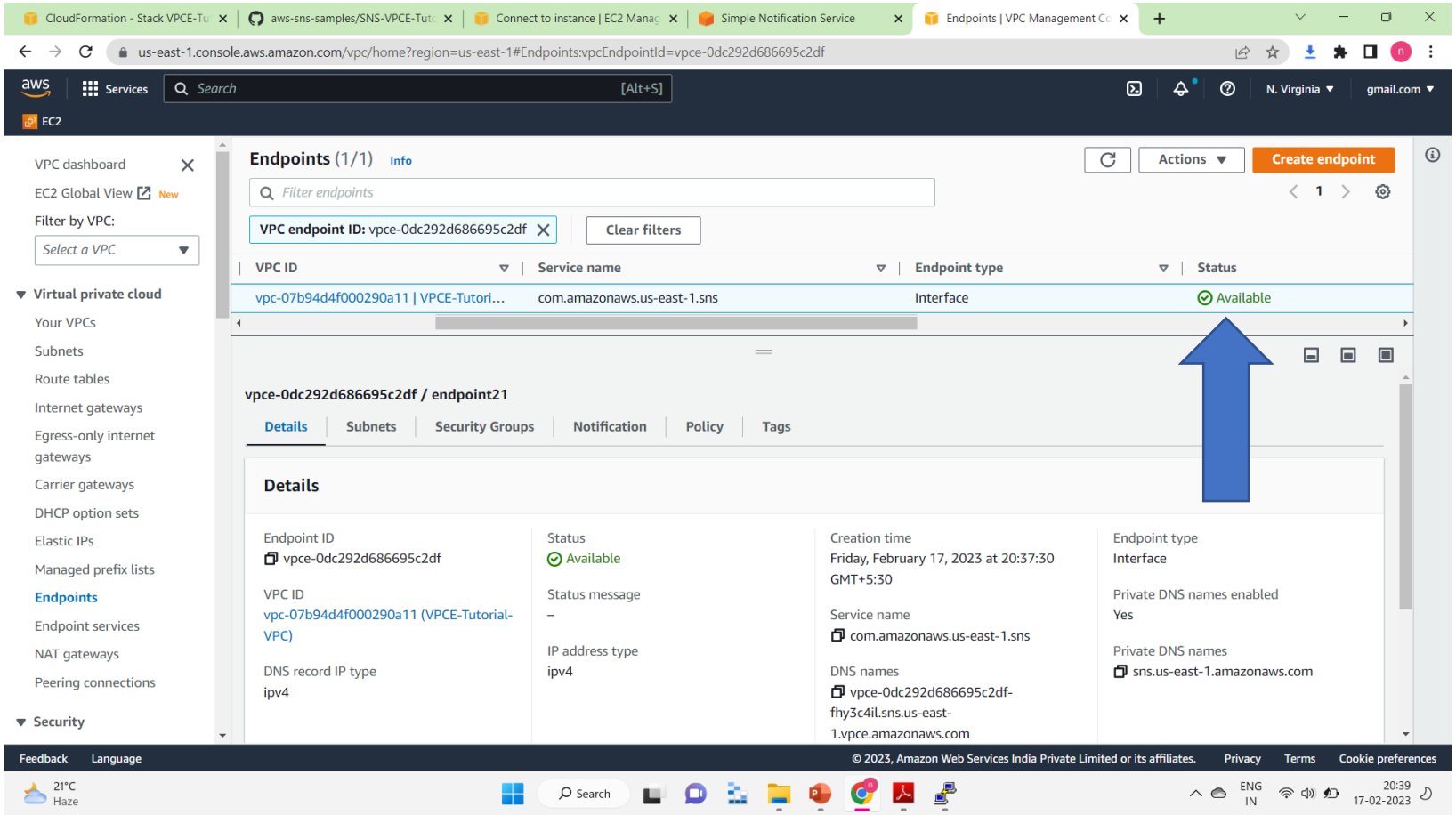

CloudFormation - Stack VPCE-Tu
aws-sns-samples/SNS-VPCE-Tuto
Connect to instance | EC2 Manag
Simple Notification Service
VPC Management Console
us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint:
aws
Services
Search
[Alt+S]
N. Virginia
gmail.com
EC2
AWS services
Services provided by Amazon
PrivateLink Ready partner services
Services with an AWS Service Ready designation
AWS Marketplace services
Services that you've purchased through AWS Marketplace
Other endpoint services
Find services shared with you by service name
Services (1/1)
Filter services
1
Service Name: com.amazonaws.us-east-1.sns
Clear filters
Service Name
Owner
Type
com.amazonaws.us-east-1.sns
amazon
Interface
VPC
Select the VPC in which to create the endpoint
VPC
The VPC in which to create your endpoint.
vpc-07b94d4f000290a11 (VPCE-Tutorial-VPC)
Additional settings
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
21°C
Haze
Search
ENG
IN
20:32
17-02-2023


CloudFormation - Stack VPCE-Tu
aws-sns-samples/SNS-VPCE-Tut
Connect to instance | EC2 Manag
Simple Notification Service
VPC Management Console
us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint:
aws
Services
Search
[Alt+S]
N. Virginia
gmail.com
EC2
Additional settings
Subnets (1/6) Info
Availability Zone
Subnet ID
us-east-1a (use1-az1)
No subnet available
us-east-1b (use1-az2)
No subnet available
us-east-1c (use1-az4)
us-east-1d (use1-az6)
No subnet available
us-east-1e (use1-az3)
No subnet available
us-east-1f (use1-az5)
No subnet available
IP address type
IPv4
IPv6
Dualstack
Security groups (2) Info
Filter security groups
Group ID
Group name
VPC ID
sg-0ef9090cad01f147a
default
vpc-07b94d4f00029
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
21°C
Haze
Search
ENG
IN
20:34
17-02-2023


CloudFormation - Stack VPCE-Tu
aws-sns-samples/SNS-VPCE-Tute
Connect to instance | EC2 Manag
Simple Notification Service
VPC Management Console
us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint:
aws
Services
Search
[Alt+S]
N. Virginia
gmail.com
EC2
Availability Zone
Subnet ID
IP address type
IPv4
IPv6
Dualstack
Security groups (1/2) Info
Filter security groups
1
Group ID
Group name
VPC ID
sg-0ef9090cad01f147a
default
vpc-07b94d4f00029
sg-09174a9d5f39cfd2d
Tutorial Security Group
vpc-07b94d4f00029
sg-09174a9d5f39cfd2d
Policy Info
VPC endpoint policy controls access to the service.
Full access
Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.
Custom
Use the policy creation tool to generate a policy, then paste the generated policy below.
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
21°C
Haze
Search
ENG
IN
20:35
17-02-2023

VPC Endpoint created

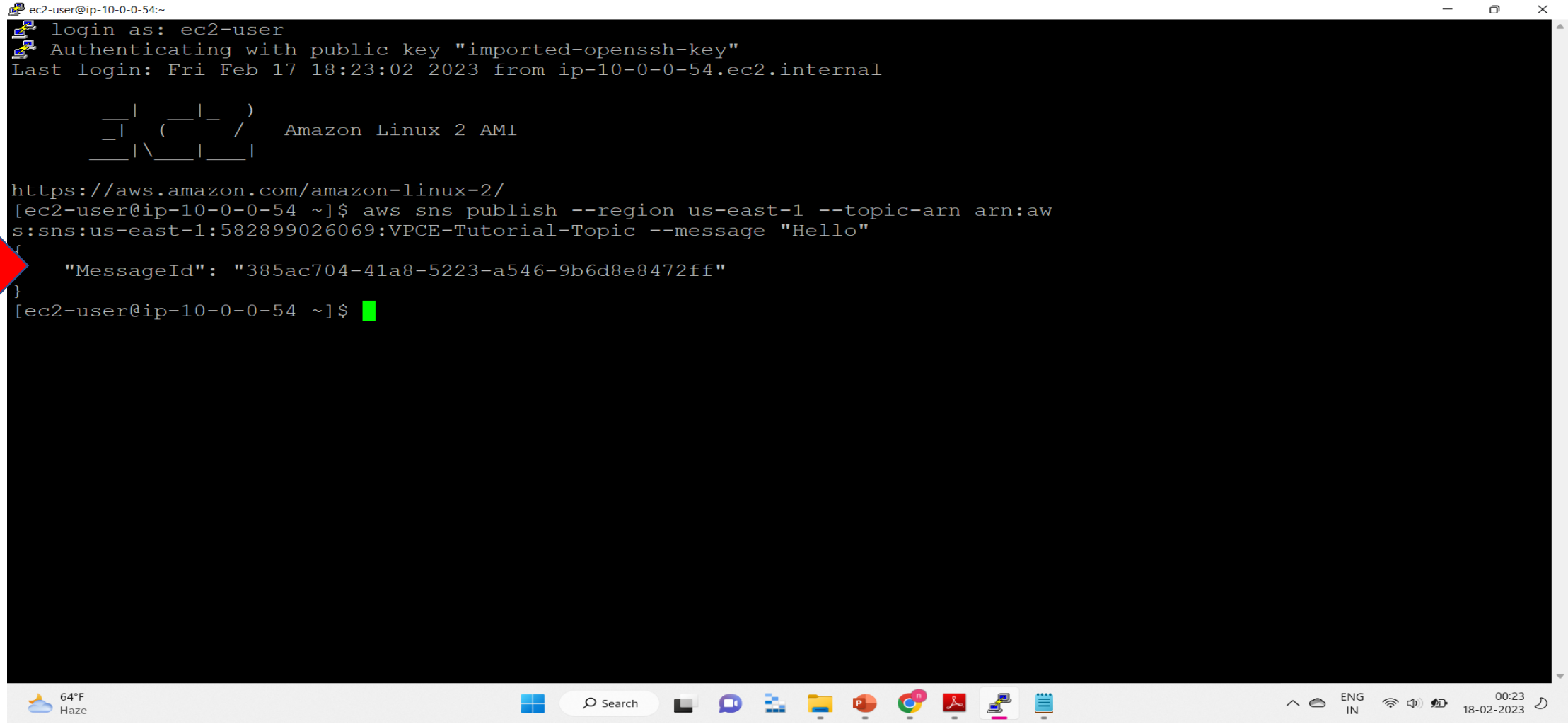



CloudFormation - Stack VPCE-Tu
aws-sns-samples/SNS-VPCE-Tute
Connect to instance | EC2 Manag
Simple Notification Service
Endpoints | VPC Management Co
us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#Endpoints:vpcEndpointId=vpce-0dc292d686695c2df
aws
Services
Search
[Alt+S]
N. Virginia
gmail.com
EC2
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Endpoints (1/1)
Info
Actions
Create endpoint
Filter endpoints
VPC endpoint ID: vpce-0dc292d686695c2df
Clear filters
VPC ID
Service name
Endpoint type
Status
vpc-07b94d4f000290a11 | VPCE-Tutori...
com.amazonaws.us-east-1.sns
Interface
Available
vpce-0dc292d686695c2df / endpoint21
Details
Subnets
Security Groups
Notification
Policy
Tags
Details
Endpoint ID
vpce-0dc292d686695c2df
Status
Available
Status message
–
IP address type
ipv4
DNS record IP type
ipv4
Creation time
Friday, February 17, 2023 at 20:37:30 GMT+5:30
Service name
com.amazonaws.us-east-1.sns
DNS names
vpce-0dc292d686695c2df-fhy3c4il.sns.us-east-1.vpce.amazonaws.com
Endpoint type
Interface
Private DNS names enabled
Yes
Private DNS names
sns.us-east-1.amazonaws.com
VPC ID
vpc-07b94d4f000290a11 (VPCE-Tutorial-VPC)
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
21°C
Haze
Search
ENG
IN
20:39
17-02-2023

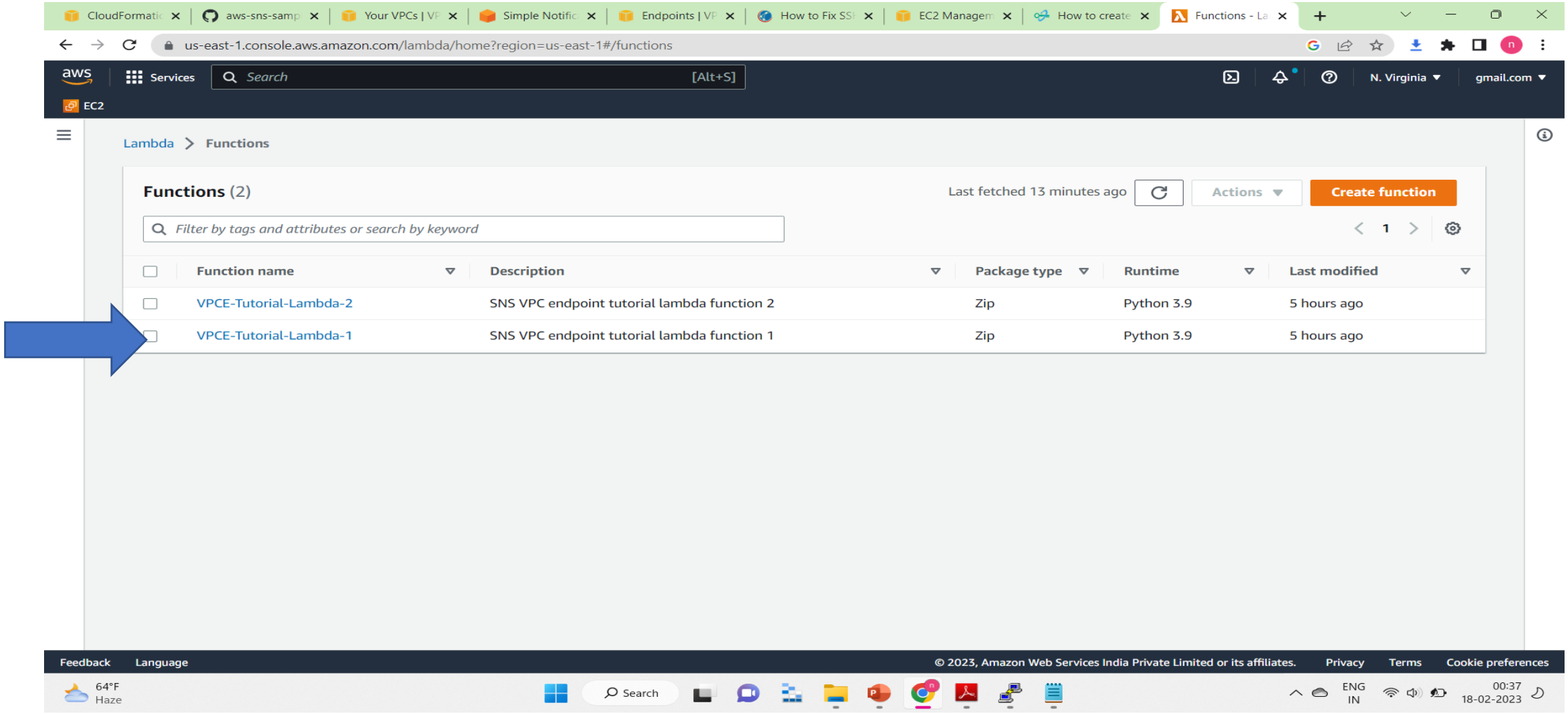
Step 9. on terminal, tried **to publish a message to SNS topic.**

- aws sns publish --region us-east-1 --topic-arn arn:aw
  s:sns:us-east-1:582899026069:VPCE-Tutorial-Topic --message "Hello"

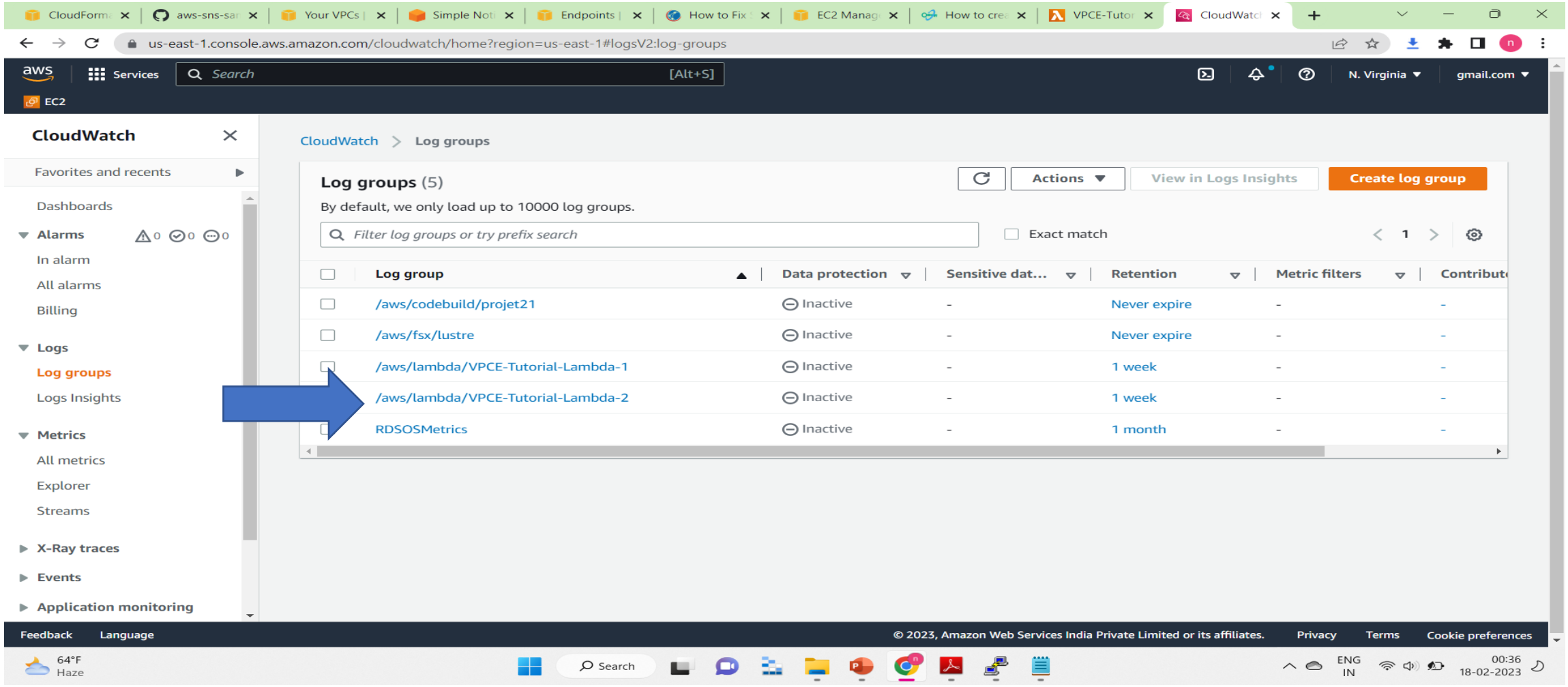
publish attempt succeeded, and Amazon SNS returned a message ID



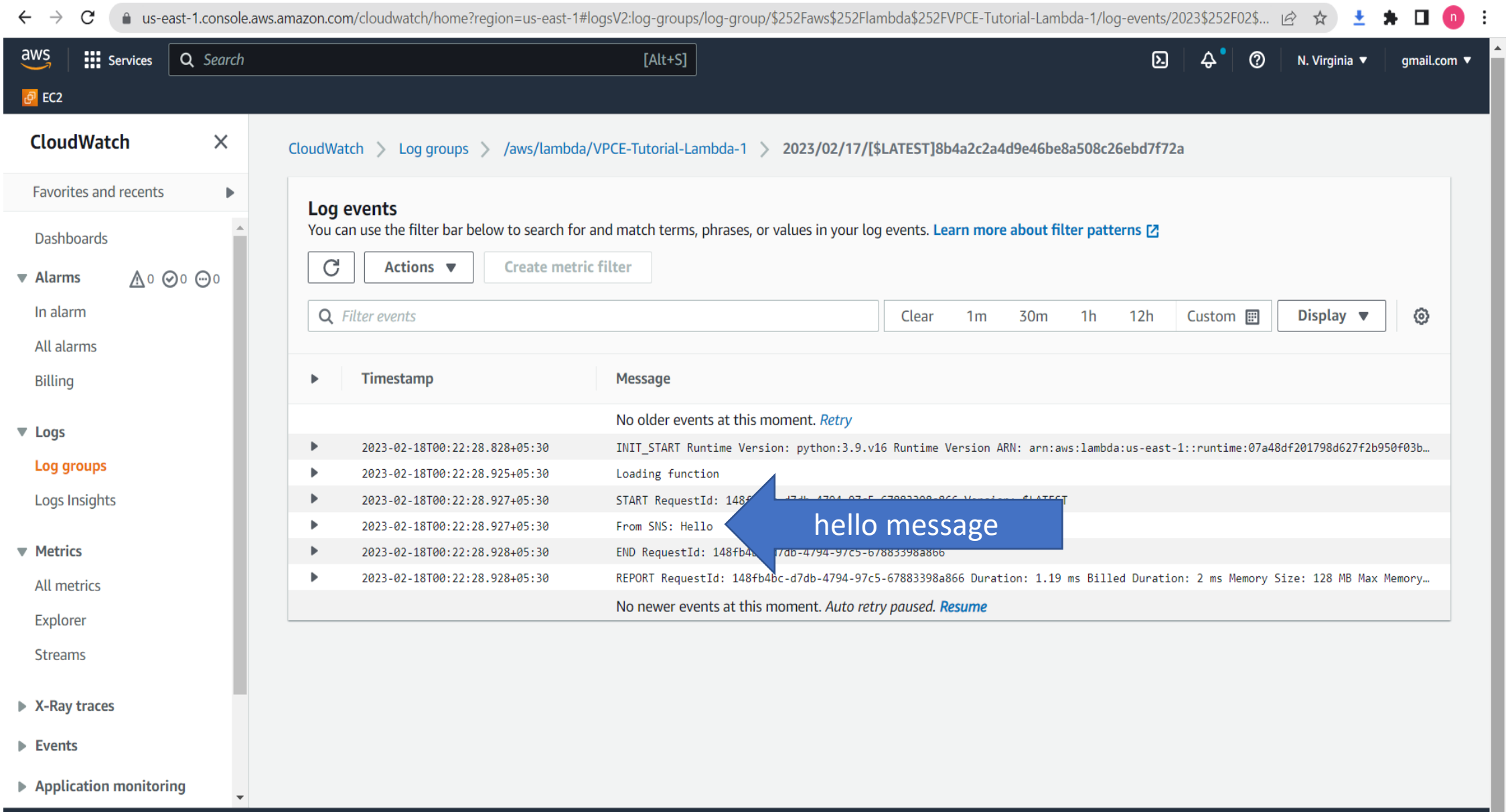
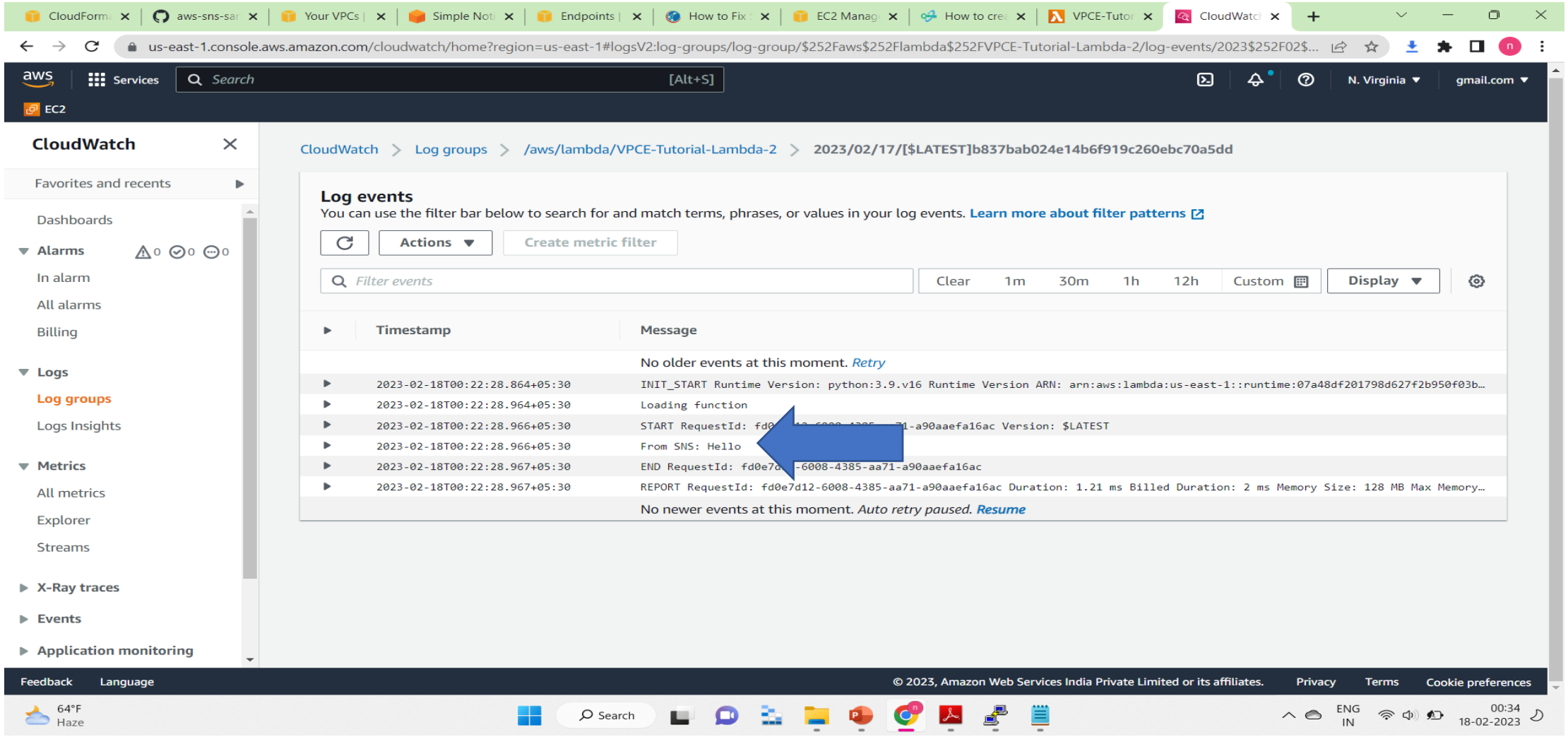
Step 10. **Verifed Message Deliveries: went to VPCE-Tutorial_lambda-1**



in log ,selected VPCE-Tutorial-Lambda1



verified that the CloudWatch logs updation : VPCE-Tutorial-Lambda-1



VPCE-Tutorial-Lambda-2