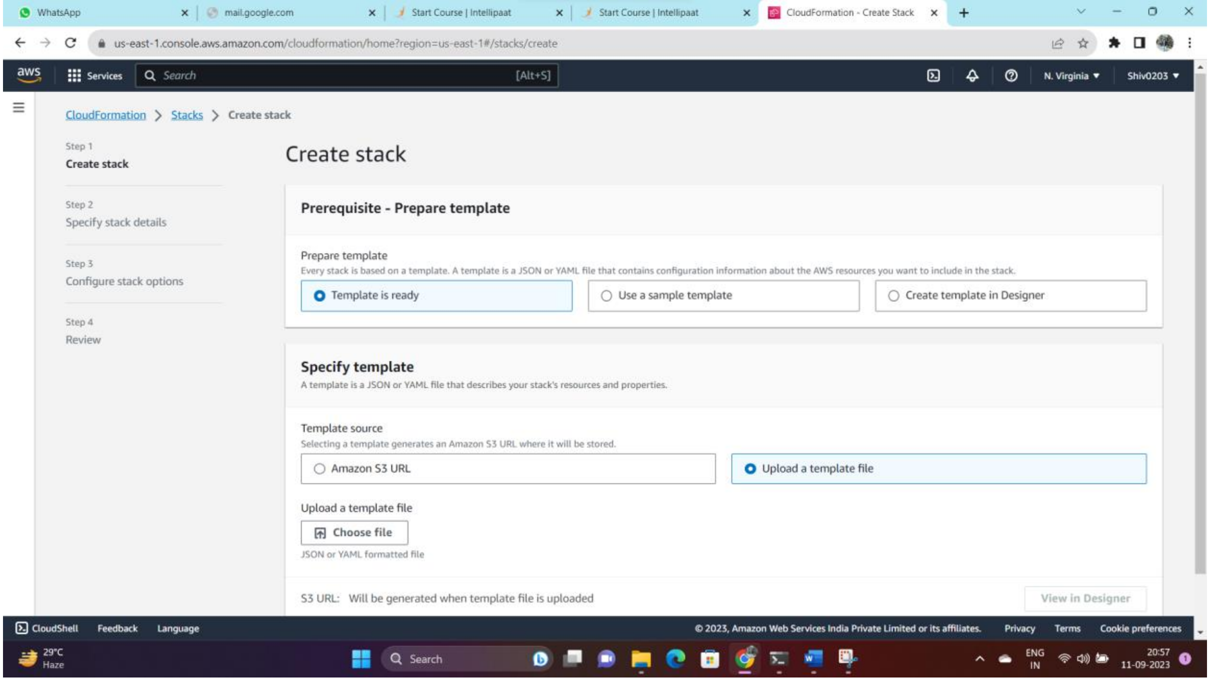
Project – 3

Publishing Amazon SNS Messages Privately:

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

---

1. Go to Cloud Formation page and click on create . select upload template and upload the VPC template . Then click on next.



CloudFormation > Stacks > Create stack

Step 1 Create stack
Step 2 Specify stack details
Step 3 Configure stack options
Step 4 Review

Create stack

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.

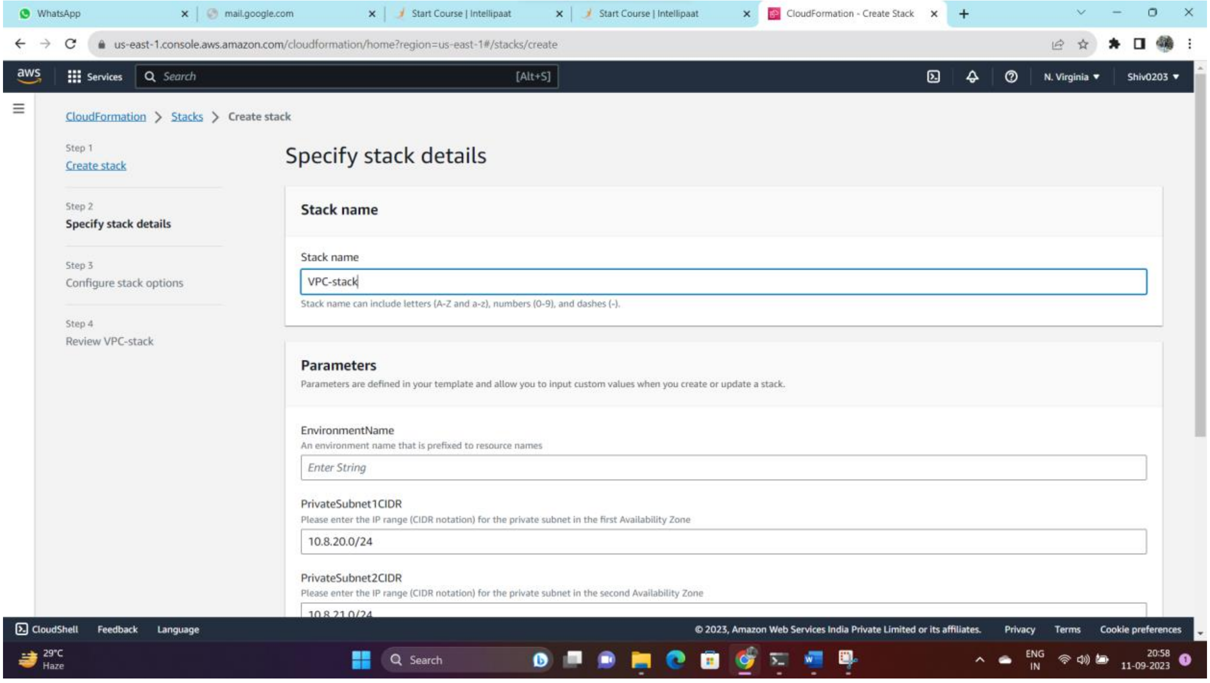
Template source
Selecting a template generates an Amazon S3 URL where it will be stored.
○ Amazon S3 URL ● Upload a template file

Upload a template file
Choose file
JSON or YAML formatted file

S3 URL: Will be generated when template file is uploaded

WhatsApp
mail.google.com
Start Course | Intellipaat
CloudFormation - Create Stack
us-east-1.console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/create
Services
Search
[Alt+S]
N. Virginia
Shiv0203
View in Designer
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
29°C Haze
20:57 11-09-2023

2. Give your VPC a name and click on next. And click on create .



CloudFormation > Stacks > Create stack

Step 1 Create stack
Step 2 Specify stack details
Step 3 Configure stack options
Step 4 Review VPC-stack

Specify stack details

Stack name

Stack name
VPC-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.

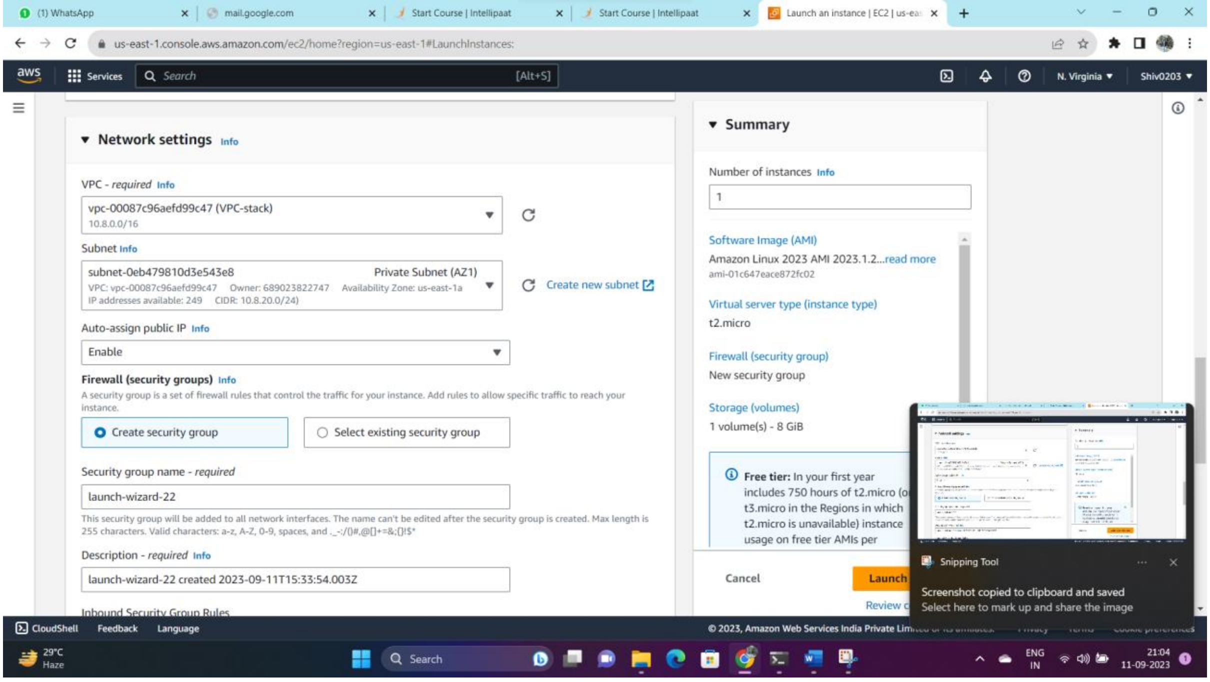
EnvironmentName
An environment name that is prefixed to resource names
Enter String

PrivateSubnet1CIDR
Please enter the IP range (CIDR notation) for the private subnet in the first Availability Zone
10.8.20.0/24

PrivateSubnet2CIDR
Please enter the IP range (CIDR notation) for the private subnet in the second Availability Zone
10.8.21.0/24

us-east-1.console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/create
Services
Search
N. Virginia
Shiv0203
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
20:58 11-09-2023

3. Next step is to launch an instance using the VPC that we have created . So go to the EC2 instance and click on launch instance . Make sure to select the VPC that we have created and select Enable as auto-assign public IP.



us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

▼ Network settings Info

VPC - *required* Info
vpc-00087c96aefd99c47 (VPC-stack)
10.8.0.0/16

Subnet Info
subnet-0eb479810d3e543e8 Private Subnet (AZ1)
VPC: vpc-00087c96aefd99c47 Owner: 689023822747 Availability Zone: us-east-1a
IP addresses available: 249 CIDR: 10.8.20.0/24)

Create new subnet

Auto-assign public IP Info
Enable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*
launch-wizard-22
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info
launch-wizard-22 created 2023-09-11T15:33:54.003Z

Inbound Security Group Rules

▼ Summary

Number of instances Info
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.1.2...read more
ami-01c647eace872fc02

Virtual server type (instance type)
t2.micro

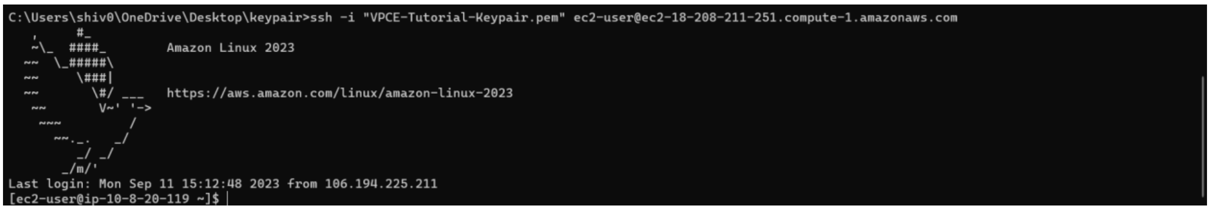
Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (o t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per

Snipping Tool
Screenshot copied to clipboard and saved
Select here to mark up and share the image

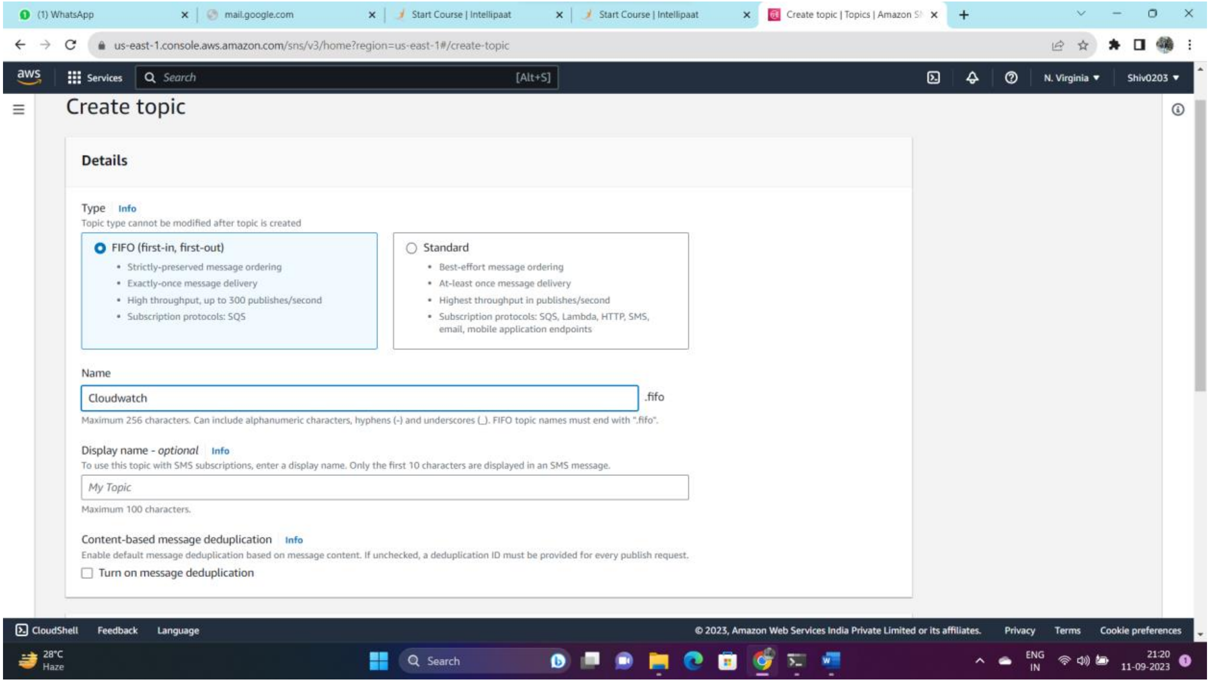
4. Once the instance is created successfully open the ssh terminal and connect the instance using the following command : ssh -i "key-name" ec2-user@hostname .



```
C:\Users\shiv0\OneDrive\Desktop\keypair>ssh -i "VPCE-Tutorial-Keypair.pem" ec2-user@ec2-18-208-211-251.compute-1.amazonaws.com
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Mon Sep 11 15:12:48 2023 from 106.194.225.211
[ec2-user@ip-10-8-20-119 ~]$
```

5. If the terminal connects then try connecting it to any public endpoint using the following command : “ping amazon.com” . If you start receiving the ms then it means your connecting is successful.

6. Now to connect your VPC to your SNS we need to create SNS topic . So go to SNS page and click on create .



us-east-1.console.aws.amazon.com/sns/v3/home?region=us-east-1#/create-topic
Services
Search
[Alt+S]
N. Virginia ▾
Shiv0203 ▾

Create topic

Details

Type Info
Topic type cannot be modified after topic is created

● FIFO (first-in, first-out)
- Strictly-preserved message ordering
- Exactly-once message delivery
- High throughput, up to 300 publishes/second
- Subscription protocols: SQS

○ Standard
- Best-effort message ordering
- At-least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

Name
Cloudwatch .fifo
Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (_). FIFO topic names must end with ".fifo".

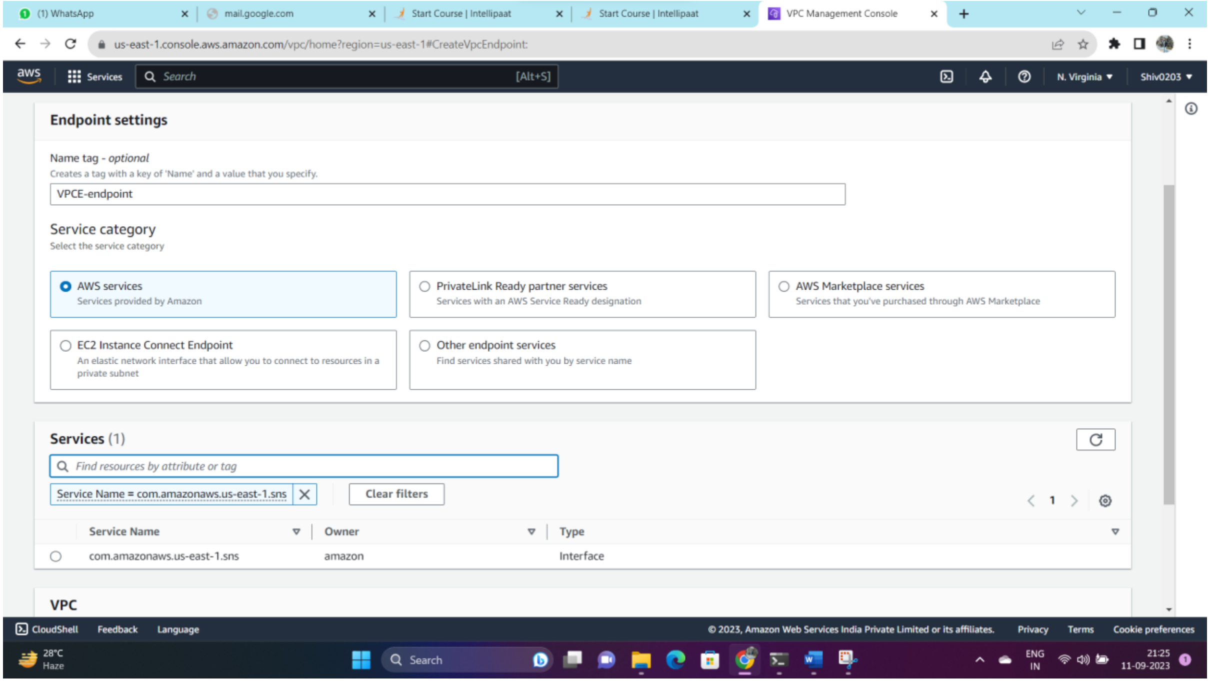
Display name - *optional* Info
To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.
My Topic
Maximum 100 characters.

Content-based message deduplication Info
Enable default message deduplication based on message content. If unchecked, a deduplication ID must be provided for every publish request.
□ Turn on message deduplication

CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

Give a name to your SNS and click on create .

7. Then VPC endpoint is needed to Amazon SNS , for that go to VPC > select endpoints > select create endpoint > name it > select AWS services as category and search fo SNS and select is Services.



us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint:
Services
Search
[Alt+S]
N. Virginia ▾
Shiv0203 ▾

Endpoint settings

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

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)

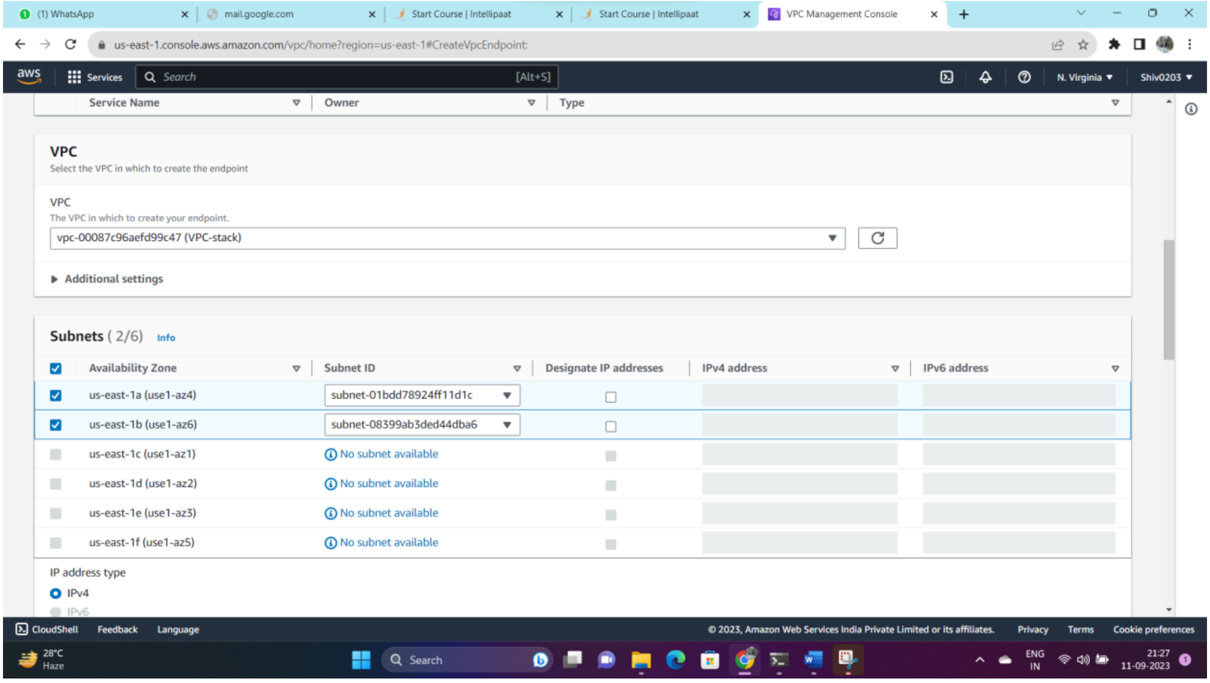
Find resources by attribute or tag
Service Name = com.amazonaws.us-east-1.sns
Clear filters

	Service Name	Owner	Type
○	com.amazonaws.us-east-1.sns	amazon	Interface

VPC

CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

8. Select the VPC that you have created before , then select the desired subnets and security groups as well . After that click on create.



us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint:

VPC

Select the VPC in which to create the endpoint

VPC

The VPC in which to create your endpoint.

vpc-00087c96aefd99c47 (VPC-stack)

▸ Additional settings

Subnets (2/6) Info

☑	Availability Zone	Subnet ID	Designate IP addresses	IPv4 address	IPv6 address
☑	us-east-1a (use1-az4)	subnet-01bdd78924ff11d1c	□		
☑	us-east-1b (use1-az6)	subnet-08399ab3ded44dba6	□		
□	us-east-1c (use1-az1)	No subnet available	□		
□	us-east-1d (use1-az2)	No subnet available	□		
□	us-east-1e (use1-az3)	No subnet available	□		
□	us-east-1f (use1-az5)	No subnet available	□		

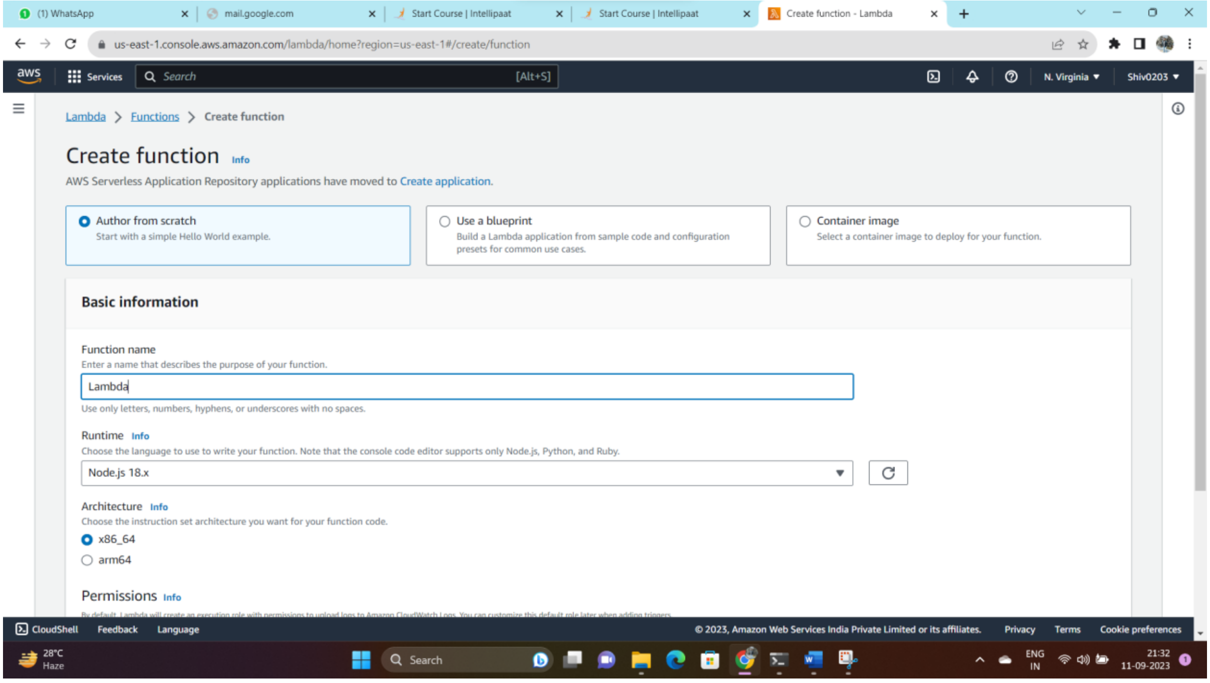
IP address type

● IPv4

○ IPv6

9. Now we also need Lambda functions to receive messages from Amazon SNS and the log events from Cloudwatch logs . So for that go to Lambda page and click on create.

Give it a name and click on create .



us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/create/function

Lambda > Functions > Create function

Create function Info

AWS Serverless Application Repository applications have moved to Create application.

● Author from scratch
Start with a simple Hello World example.

○ Use a blueprint
Build a Lambda application from sample code and configuration presets for common use cases.

○ Container image
Select a container image to deploy for your function.

Basic information

Function name

Enter a name that describes the purpose of your function.

Lambda

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info

Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Node.js 18.x

Architecture Info

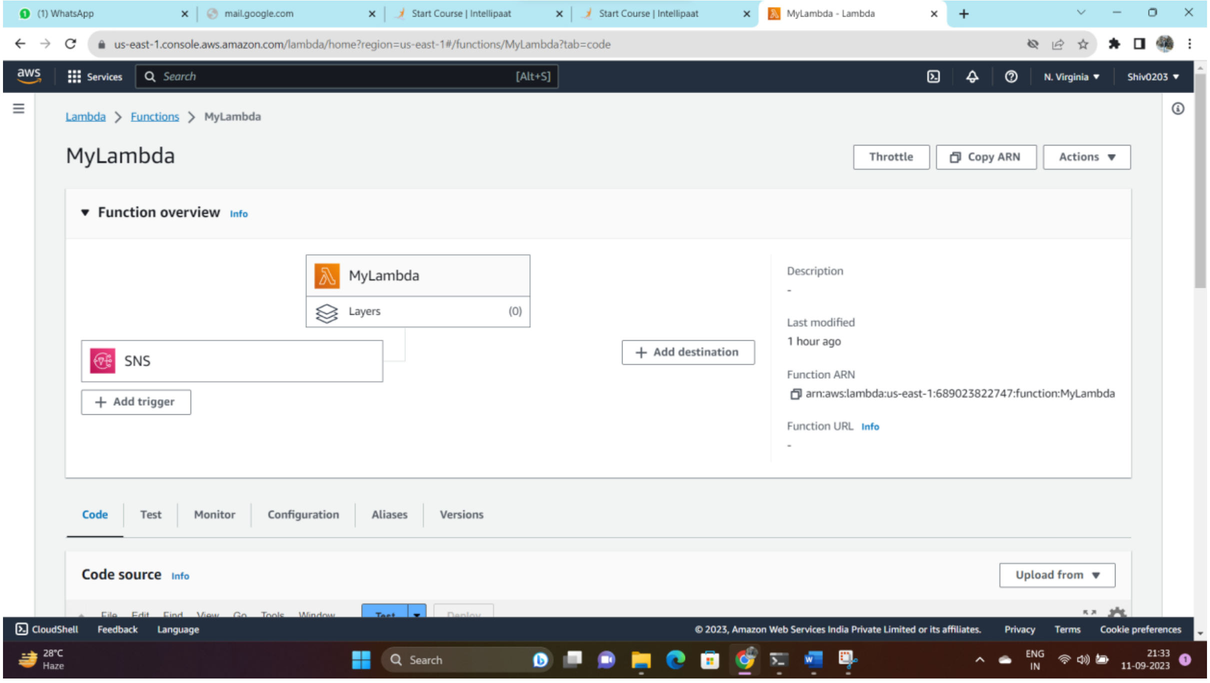
Choose the instruction set architecture you want for your function code.

● x86_64

○ arm64

Permissions Info

10. Once the function is created attach the SNS topic to to receive the cloudwatch logs .



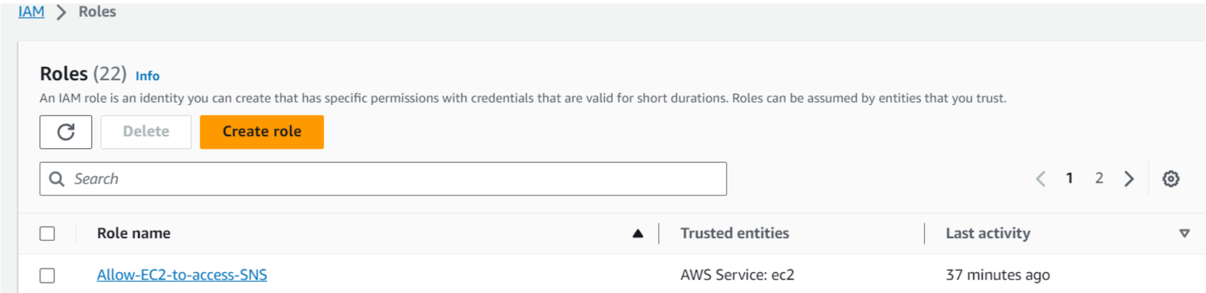
Description
-

Last modified
1 hour ago

Function ARN
arn:aws:lambda:us-east-1:689023822747:function:MyLambda

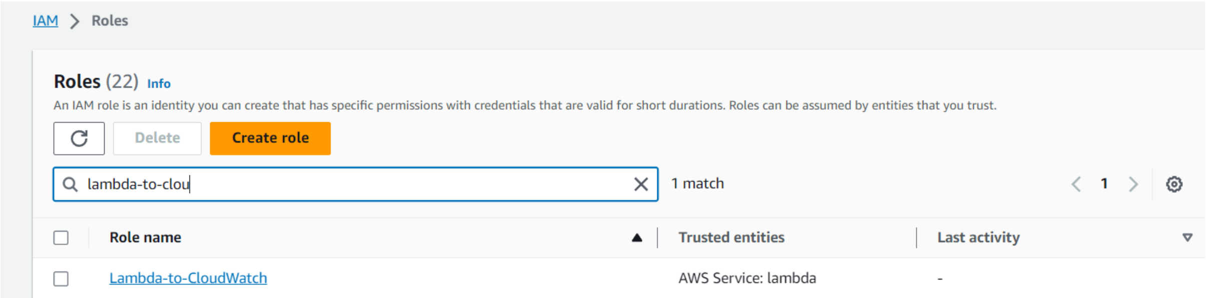
Function URL Info
-

11. Now we need two roles , 1 to allow the ec2 instance to access SNS and 2 to allow Lambda function to access the CloudWatch logs. So go to the IAM page and create two roles as shown below:



An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

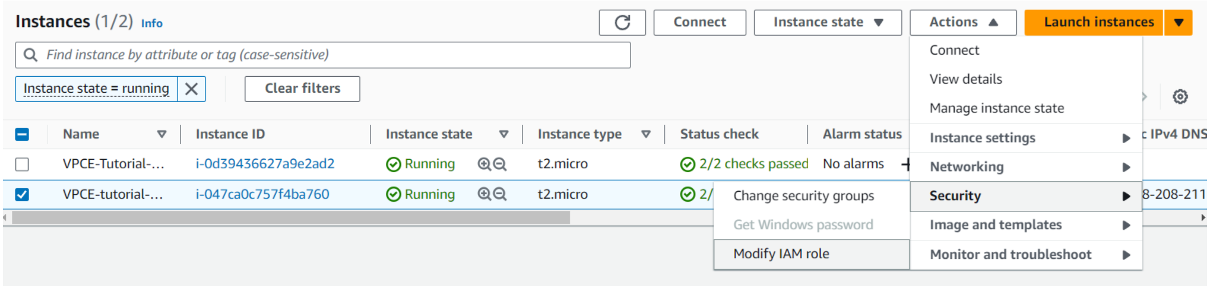
□	Role name ▲	Trusted entities	Last activity
□	Allow-EC2-to-access-SNS	AWS Service: ec2	37 minutes ago



An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name ▲	Trusted entities	Last activity
□	Lambda-to-CloudWatch	AWS Service: lambda	-

12. Once the roles are created attach the EC2-to-SNS to your EC2 instance .

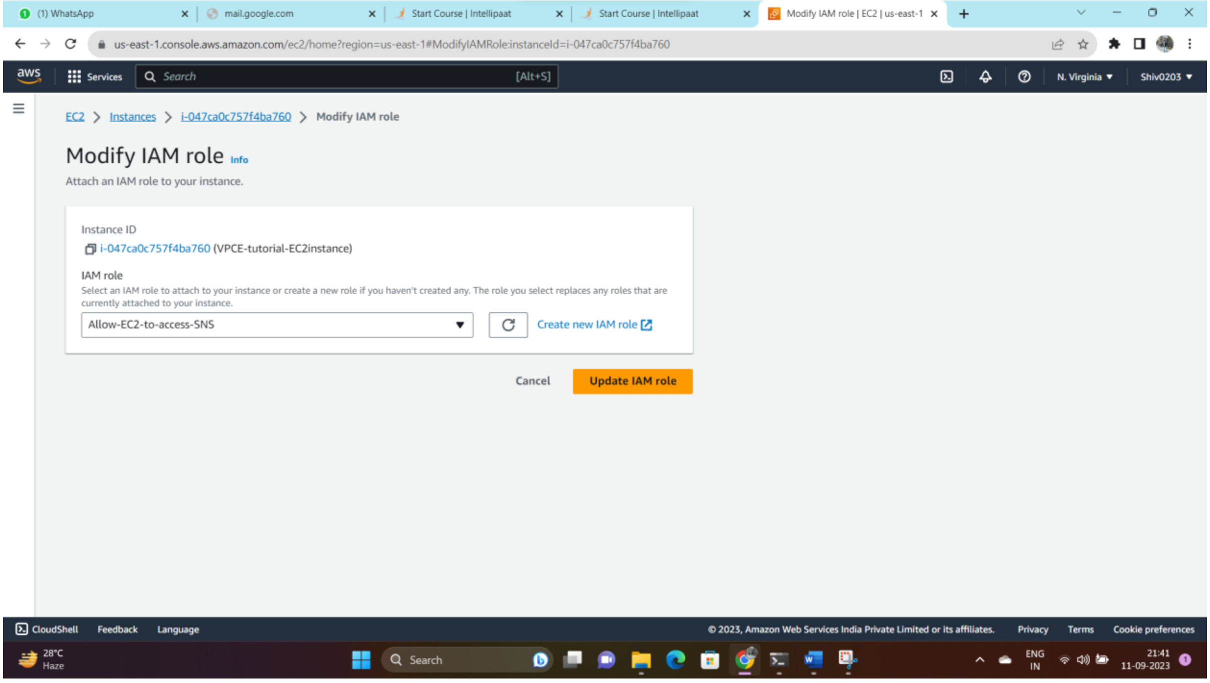


Instances (1/2) Info

Find instance by attribute or tag (case-sensitive)

Instance state = running

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	VPCE-Tutorial-...	i-0d39436627a9e2ad2	Running	t2.micro	2/2 checks passed	No alarms
☑	VPCE-tutorial-...	i-047ca0c757f4ba760	Running	t2.micro	2/	



us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ModifyIAMRole:instanceId=i-047ca0c757f4ba760

EC2 > Instances > i-047ca0c757f4ba760 > Modify IAM role

Modify IAM role Info

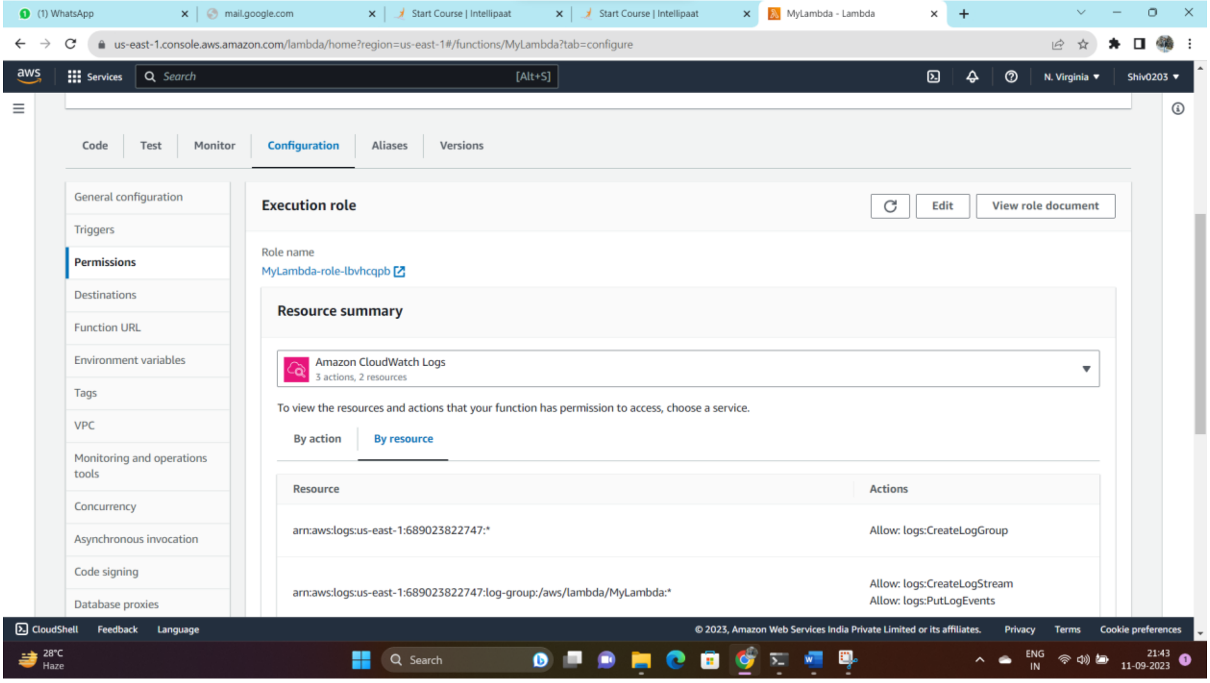
Attach an IAM role to your instance.

Instance ID: i-047ca0c757f4ba760 (VPCE-tutorial-EC2instance)

IAM role: Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

Allow-EC2-to-access-SNS

13. Similarly attached the Lambda role to your Lambda function as well .



us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/MyLambda?tab=configure

Execution role

Role name: MyLambda-role-lbvhcqpb

Resource summary

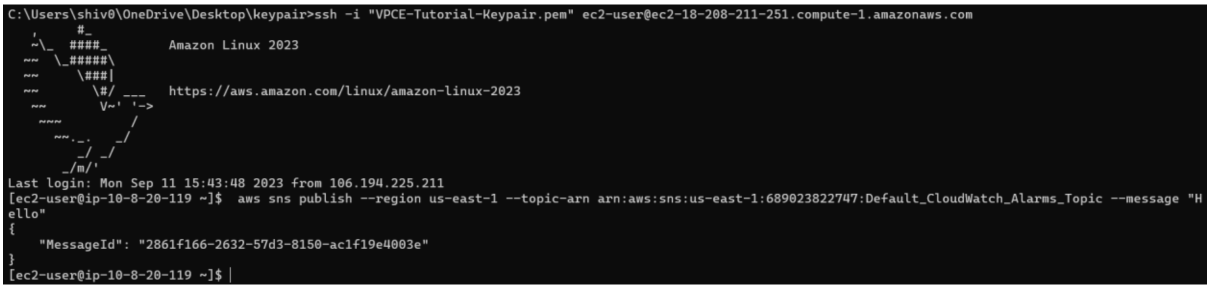
Amazon CloudWatch Logs
3 actions, 2 resources

To view the resources and actions that your function has permission to access, choose a service.

Resource	Actions
arn:aws:logs:us-east-1:689023822747:*	Allow: logs:CreateLogGroup
arn:aws:logs:us-east-1:689023822747:log-group:/aws/lambda/MyLambda:*	Allow: logs:CreateLogStream Allow: logs:PutLogEvents

Once both the roles are attached to their respective functions then its time to publish a message .

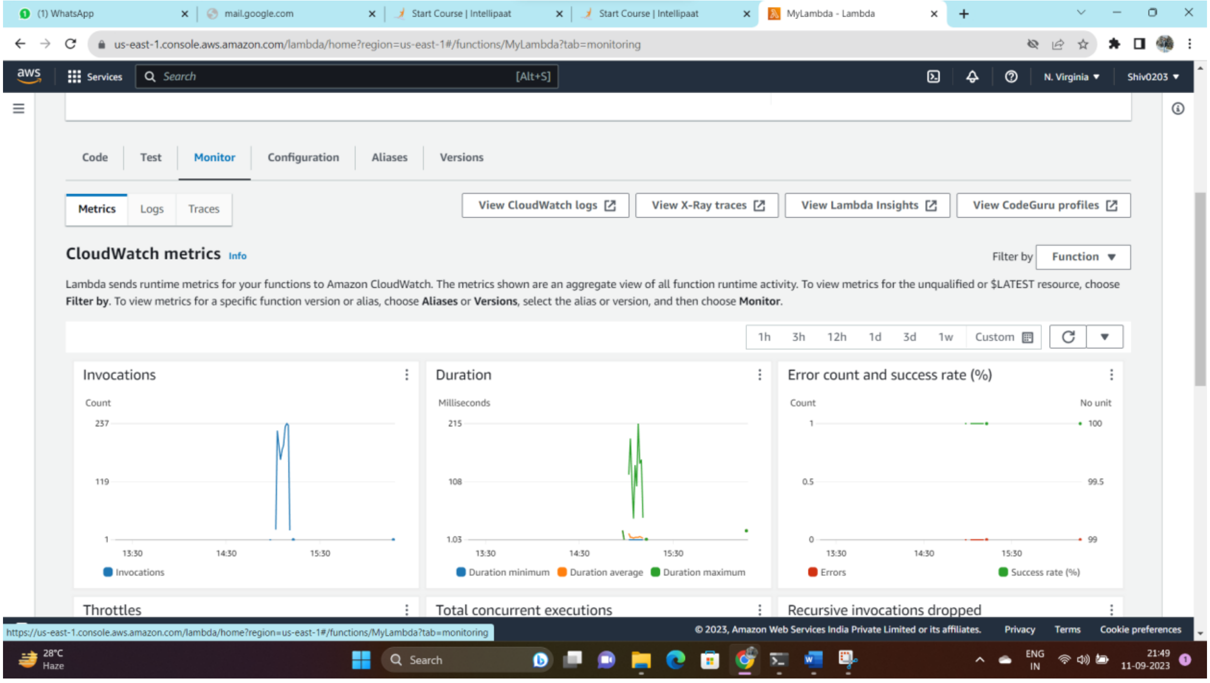
So go to your ssh , connect to it again . Attempt to publish the message using the following command : $ aws sns publish --region “your aws region” –topic-arn “your sns topic” –message “Hello”



```
C:\Users\shiv0\OneDrive\Desktop\keypair>ssh -i "VPCE-Tutorial-Keypair.pem" ec2-user@ec2-18-208-211-251.compute-1.amazonaws.com
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Mon Sep 11 15:43:48 2023 from 106.194.225.211
[ec2-user@ip-10-8-20-119 ~]$  aws sns publish --region us-east-1 --topic-arn arn:aws:sns:us-east-1:689023822747:Default_CloudWatch_Alarms_Topic --message "H
ello"
{
    "MessageId": "2861f166-2632-57d3-8150-ac1f19e4003e"
}
[ec2-user@ip-10-8-20-119 ~]$ |
```

Once you receive the message as seen above , it means that your message has been publish successfully.

14. Now go to your Lambda function > click on Monitor option and you will be able to see the graph in Invocations . It means that the message has been published . You can also check the message in cloudwatch logs directly.



Lambda sends runtime metrics for your functions to Amazon CloudWatch. The metrics shown are an aggregate view of all function runtime activity. To view metrics for the unqualified or $LATEST resource, choose **Filter by**. To view metrics for a specific function version or alias, choose **Aliases** or **Versions**, select the alias or version, and then choose **Monitor**.

Hence we have created a VPC using CloudWatch , attached the VPC to Amazon SNS and were able to publish a message successfully.