

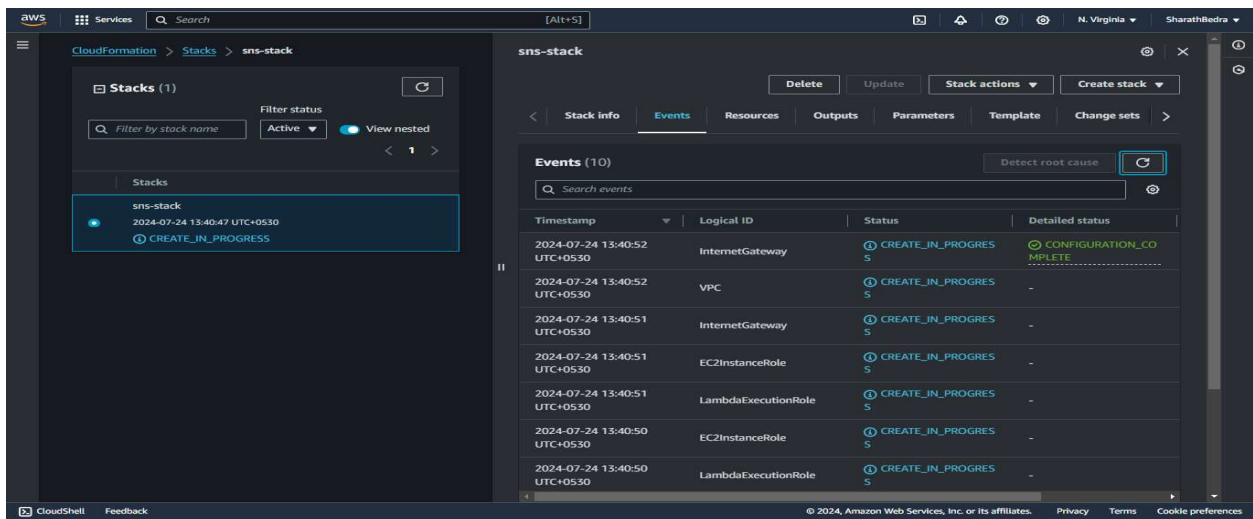
## Project 3 – Publishing Amazon SNS Messages Privately;

The template that we are going to use(<https://github.com/aws-samples/aws-sns-samples/blob/master/templates/SNS-VPCE-Tutorial-CloudFormation.template>);

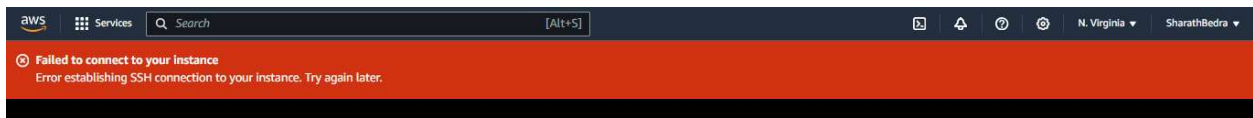
```
SNS Message.yaml - Notepad
File Edit Format View Help
AWSTemplateFormatVersion: 2010-09-09
Description: CloudFormation Template for SNS VPC Endpoints Tutorial
Parameters:
  KeyName:
    Description: Name of an existing EC2 KeyPair to enable SSH access to the instance
    Type: AWS::EC2::KeyPair::KeyName
    ConstraintDescription: must be the name of an existing EC2 KeyPair.
  SSHLocation:
    Description: The IP address range that can be used to SSH to the EC2 instance
    Type: String
    MinLength: '9'
    MaxLength: '18'
    Default: '0.0.0.0/0'
    AllowedPattern: '(\d{1,3})\.\d{1,3})\.\d{1,3})\.\d{1,3})/(\d{1,2})'
    ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.
Mappings:
  RegionMap:
    us-east-1:
      AMI: ami-428aa838
    us-east-2:
      AMI: ami-710e2414
    us-west-1:
      AMI: ami-4a787a2a
    us-west-2:
      AMI: ami-7f43f307
    ap-northeast-1:
      AMI: ami-c2680fa4
    ap-northeast-2:
      AMI: ami-3e04a450
    ap-southeast-1:
      AMI: ami-4f89f533
    ap-southeast-2:
      AMI: ami-3b708c5a
    ap-south-1:
      AMI: ami-3b2f7954
    ca-central-1:
```

## Creating the Stack;

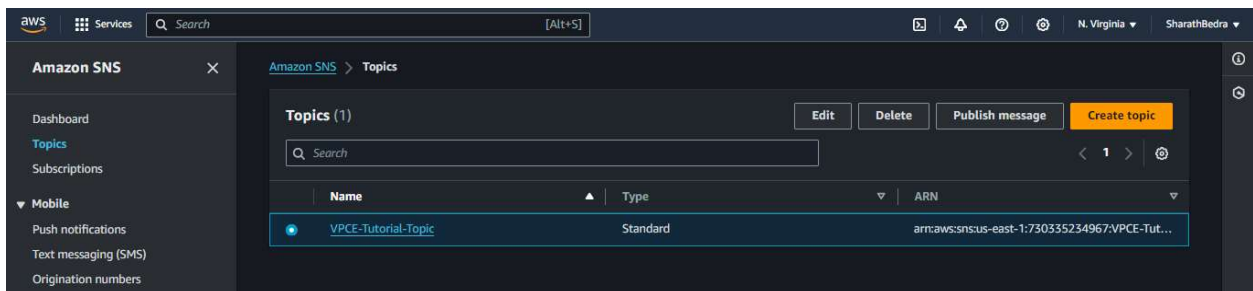
The screenshot shows the AWS Management Console interface for creating a new CloudFormation stack. The breadcrumb navigation at the top indicates the path: CloudFormation > Stacks > Create stack. On the left, a sidebar shows the four steps of the process: Step 1: Create stack, Step 2: Specify stack details (currently active), Step 3: Configure stack options, and Step 4: Review and create. The main content area is titled 'Specify stack details' and contains two sections: 'Provide a stack name' and 'Parameters'. In the 'Provide a stack name' section, the 'Stack name' field is populated with 'sns-stack', and a note below it states: 'Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 9/128.' In the 'Parameters' section, there are two parameters: 'KeyName' with a dropdown menu showing 'kattappa' (the description is 'Name of an existing EC2 KeyPair to enable SSH access to the instance') and 'SSHLocation' with a text input field containing '0.0.0.0/0' (the description is 'The IP address range that can be used to SSH to the EC2 instance'). At the bottom right of the form, there are three buttons: 'Cancel', 'Previous', and 'Next'.



There is no Internet Access to our EC2 Instance;



SNS Topic got created;



## Creating Amazon VPC endpoint for Amazon SNS;

The screenshot displays the AWS Management Console interface for creating a VPC endpoint. The top navigation bar shows the AWS logo, 'Services' menu, a search bar, and the current region 'N. Virginia' with the user 'SharathBeda'.

### Create endpoint

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.  
Endpoint-1

**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)

Search: Service Name = com.amazonaws.us-east-1.sns [X] 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-0b80bc9ee0f381ea9 (VPCE-Tutorial-VPC) [X]

#### Additional settings

##### Subnets (1/6)

Availability Zone	Subnet ID	Designate IP addresses	IPv4 address	IPv6 address
<input checked="" type="checkbox"/> us-east-1a (use1-az2)	subnet-0c23414b5e46b6859	<input type="checkbox"/>		
<input type="checkbox"/> us-east-1b (use1-az4)	No subnet available	<input type="checkbox"/>		
<input type="checkbox"/> us-east-1c (use1-az6)	No subnet available	<input type="checkbox"/>		
<input type="checkbox"/> us-east-1d (use1-az1)	No subnet available	<input type="checkbox"/>		
<input type="checkbox"/> us-east-1e (use1-az3)	No subnet available	<input type="checkbox"/>		
<input type="checkbox"/> us-east-1f (use1-az5)	No subnet available	<input type="checkbox"/>		

**IP address type**

- ☒ IPv4
- ☐ IPv6
- ☐ Dualstack

##### Security groups (1/2)

Group ID	Group name	VPC ID	Description
<input checked="" type="checkbox"/> sg-0341545f735802638	Tutorial Security Group	vpc-0b80bc9ee0f381ea9	Security group for SNS VPC endpoint tutorial
<input type="checkbox"/> sg-02561d16b7609f60a	default	vpc-0b80bc9ee0f381ea9	default VPC security group

sg-0341545f735802638 [X]

##### Policy

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.

**VPC dashboard** [X]

**EC2 Global View** [X]

**Virtual private cloud**  
Your VPCs

**Successfully created VPC endpoint**  
vpce-05367bd67d924ab2e

**Endpoints (1/1)**  
Search: [X] Actions [v] Create endpoint

Name	VPC endpoint ID	VPC ID	Service name	Endpoint type	Sta
<input checked="" type="checkbox"/> Endpoint-1	vpce-05367bd67d924ab2e	vpc-0b80bc9ee0f381ea9	com.amazonaws.us-east-1.sns	Interface	[X]

## Publishing a Message;

**Amazon SNS** > **Topics** > **VPCE-Tutorial-Topic** > **Publish message**

### Publish message to topic

**Message details**

Topic ARN  
arn:aws:sns:us-east-1:730335234967:VPCE-Tutorial-Topic

Subject - *optional*  
  
Maximum 100 printable ASCII characters

Time to Live (TTL) - *optional* [Info](#)  
This setting applies only to mobile application endpoints. The number of seconds that the push notification service has to deliver the message to the endpoint.

**Message body**

Message structure

☒ **Identical payload for all delivery protocols.**  
The same payload is sent to endpoints subscribed to the topic, regardless of their delivery protocol.

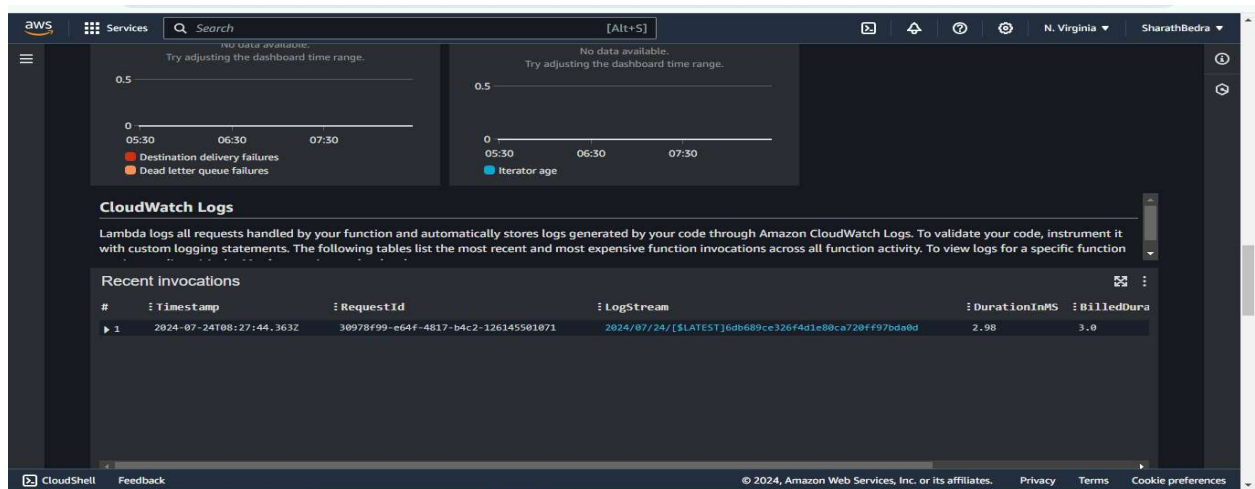
☐ **Custom payload for each delivery protocol.**  
Different payloads are sent to endpoints subscribed to the topic, based on their delivery protocol.

Message body to send to the endpoint

**Message attributes** [Info](#)  
Message attributes let you provide structured metadata items (such as timestamps, geospatial data, signatures, and identifiers) for the message.

Type	Name	Value	
<input type="text" value="Select attribute type"/>	<input type="text" value="Enter attribute name"/>	<input \"value2\"]"="" type="text" value="value or [\" value1\",=""/>	<input type="button" value="Remove"/>

## Verify whether message deliveries(Lambda Invocations);



## Verifying the Cloud Logs;

The screenshot displays the AWS CloudWatch console interface. The left sidebar contains navigation options: CloudWatch, Favorites and recents, Dashboards, Alarms, Logs, and Metrics. The main content area shows the 'Log events' page for a specific log group. The breadcrumb trail indicates the path: CloudWatch > Log groups > /aws/lambda/VPCE-Tutorial-Lambda-2 > 2024/07/24/[\$LATEST]6db689ce326f4d1e80ca720ff97bda0d. The 'Log events' section includes a search bar, a filter bar with a search input, and a table of log events. The table has two columns: 'Timestamp' and 'Message'. The log events are as follows:

Timestamp	Message
2024-07-24T08:27:44.284Z	INIT_START Runtime Version: python:3.9.v54 Runtime Version ARN: arn:aws:lambda:us-east-1::runtime:274...
2024-07-24T08:27:44.358Z	Loading function
2024-07-24T08:27:44.361Z	START RequestId: 30978f99-e64f-4817-b4c2-126145501071 Version: \$LATEST
2024-07-24T08:27:44.362Z	From SNS: Hello Intellipaat, This is Sherath
2024-07-24T08:27:44.363Z	END RequestId: 30978f99-e64f-4817-b4c2-126145501071
2024-07-24T08:27:44.363Z	REPORT RequestId: 30978f99-e64f-4817-b4c2-126145501071 Duration: 2.98 ms Billed Duration: 3 ms Memory...

The footer of the console shows the copyright notice: © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.