Project 3 – Publishing Amazon SNS Messages Privately

Project: Publishing Amazon SNS messages privately

Industry: Healthcare

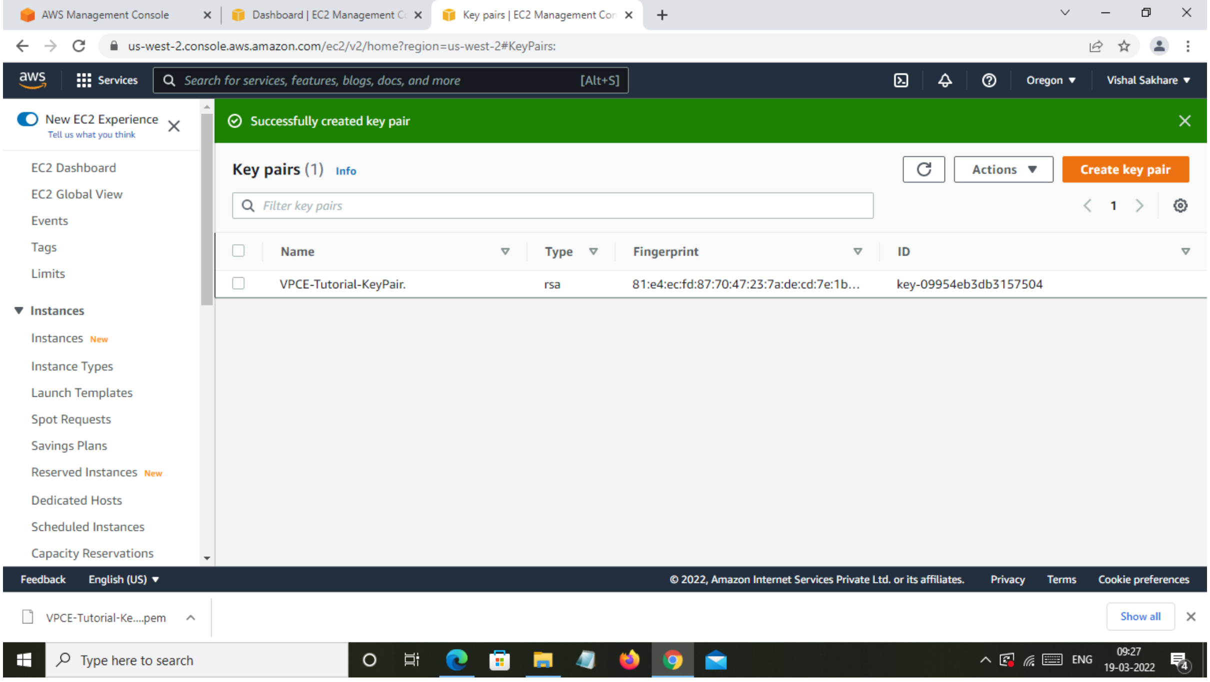
Problem Statement: How to secure patient records online and send it privately to the intended party

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.

Highlights:

- AWS CloudFormation to create a VPC
- Connect VPC with AWS SNS
- Publish message privately with SNS

Step 1: Create an Amazon EC2 Key Pair



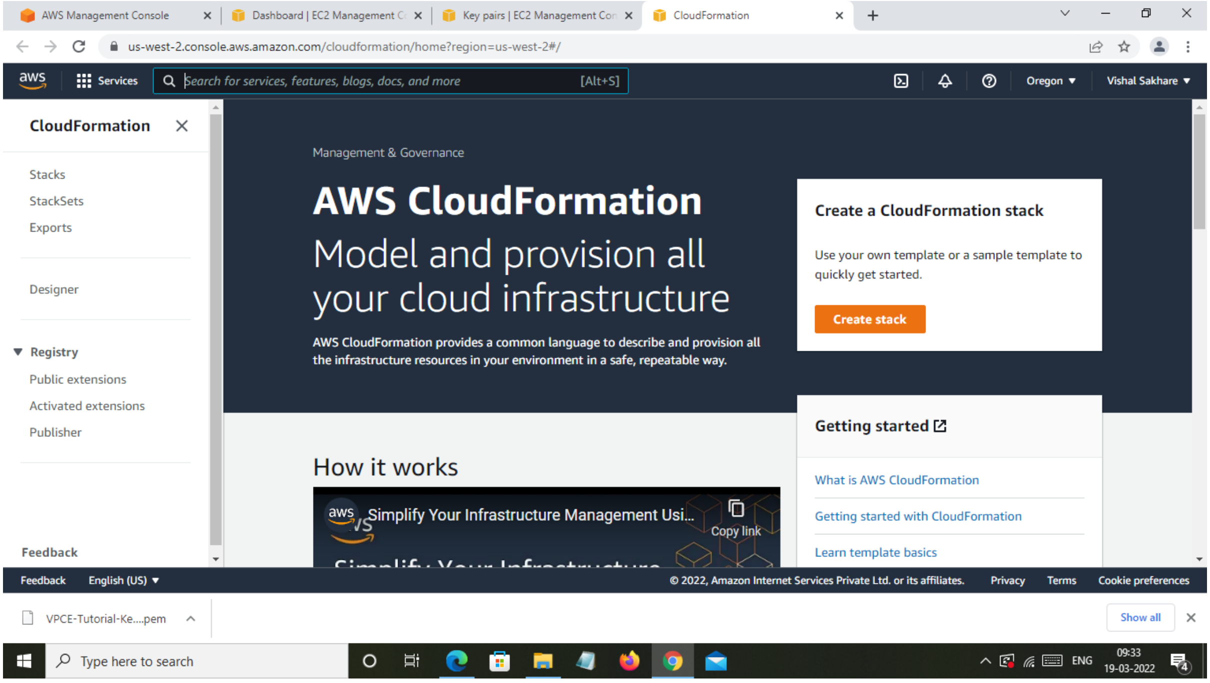
us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#KeyPairs:

Successfully created key pair

Key pairs (1)

Name	Type	Fingerprint	ID
VPCE-Tutorial-KeyPair.	rsa	81:e4:ec:fd:87:70:47:23:7a:de:cd:7e:1b...	key-09954eb3db3157504

Step 2: Create the AWS Resources



us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/

Management & Governance

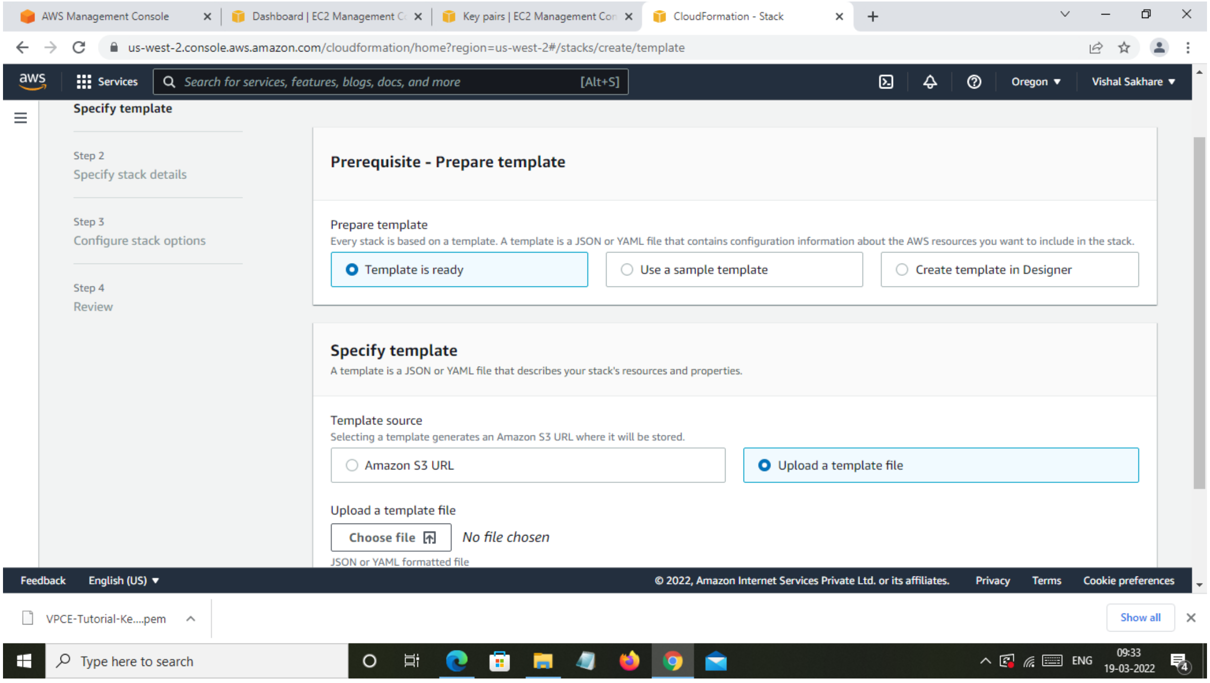
AWS CloudFormation

Model and provision all your cloud infrastructure

AWS CloudFormation provides a common language to describe and provision all the infrastructure resources in your environment in a safe, repeatable way.

Create a CloudFormation stack

Use your own template or a sample template to quickly get started.



AWS Management Console | Dashboard | EC2 Management C | Key pairs | EC2 Management Con | CloudFormation - Stack

us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/create/template

Services | Search for services, features, blogs, docs, and more [Alt+S] | Oregon ▾ | Vishal Sakhare ▾

Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

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.

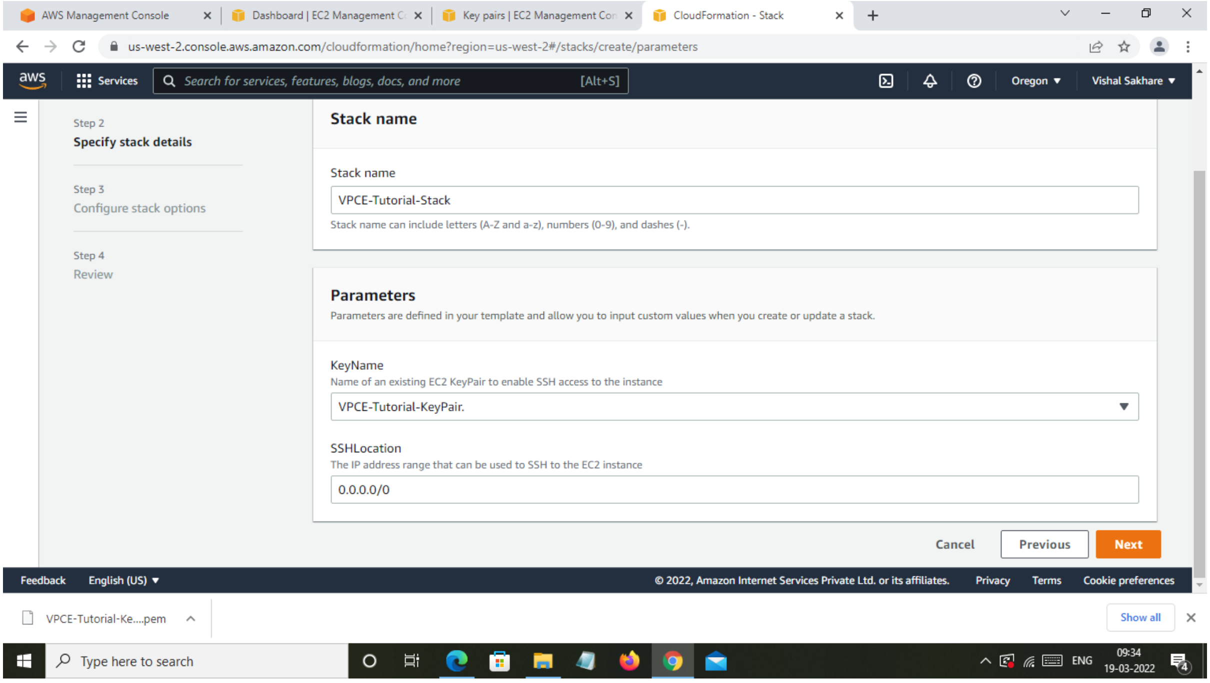
○ Amazon S3 URL ● Upload a template file

Upload a template file
Choose file *No file chosen*
JSON or YAML formatted file

Feedback English (US) ▾ © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

VPCE-Tutorial-Ke....pem Show all

Type here to search ENG 09:33 19-03-2022



AWS Management Console | Dashboard | EC2 Management C | Key pairs | EC2 Management Con | CloudFormation - Stack

us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/create/parameters

Services | Search for services, features, blogs, docs, and more [Alt+S] | Oregon ▾ | Vishal Sakhare ▾

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

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. ▾

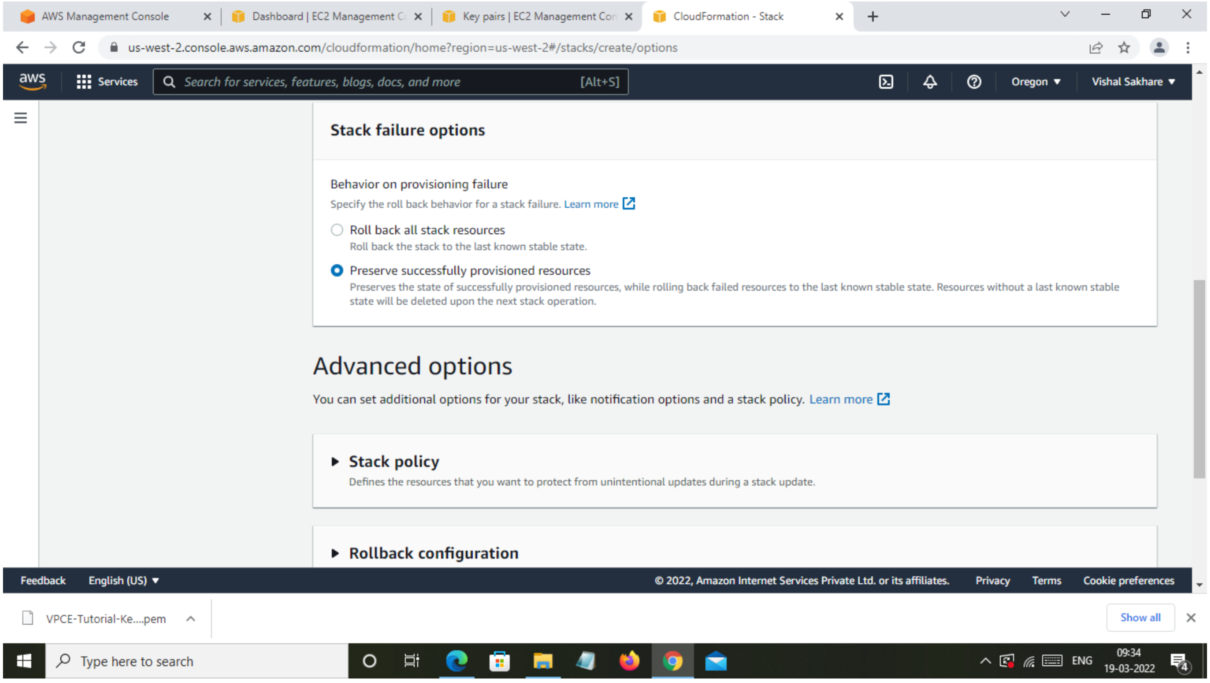
SSHLocation
The IP address range that can be used to SSH to the EC2 instance
0.0.0.0/0

Cancel Previous Next

Feedback English (US) ▾ © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

VPCE-Tutorial-Ke....pem Show all

Type here to search ENG 09:34 19-03-2022



AWS Management Console | Dashboard | EC2 Management C | Key pairs | EC2 Management Con | CloudFormation - Stack

us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/create/options

Services | Search for services, features, blogs, docs, and more [Alt+S] | Oregon ▼ | Vishal Sakhare ▼

Stack failure options

Behavior on provisioning failure

Specify the roll back behavior for a stack failure. Learn more

○ Roll back all stack resources
Roll back the stack to the last known stable state.

● Preserve successfully provisioned resources
Preserves the state of successfully provisioned resources, while rolling back failed resources to the last known stable state. Resources without a last known stable state will be deleted upon the next stack operation.

Advanced options

You can set additional options for your stack, like notification options and a stack policy. Learn more

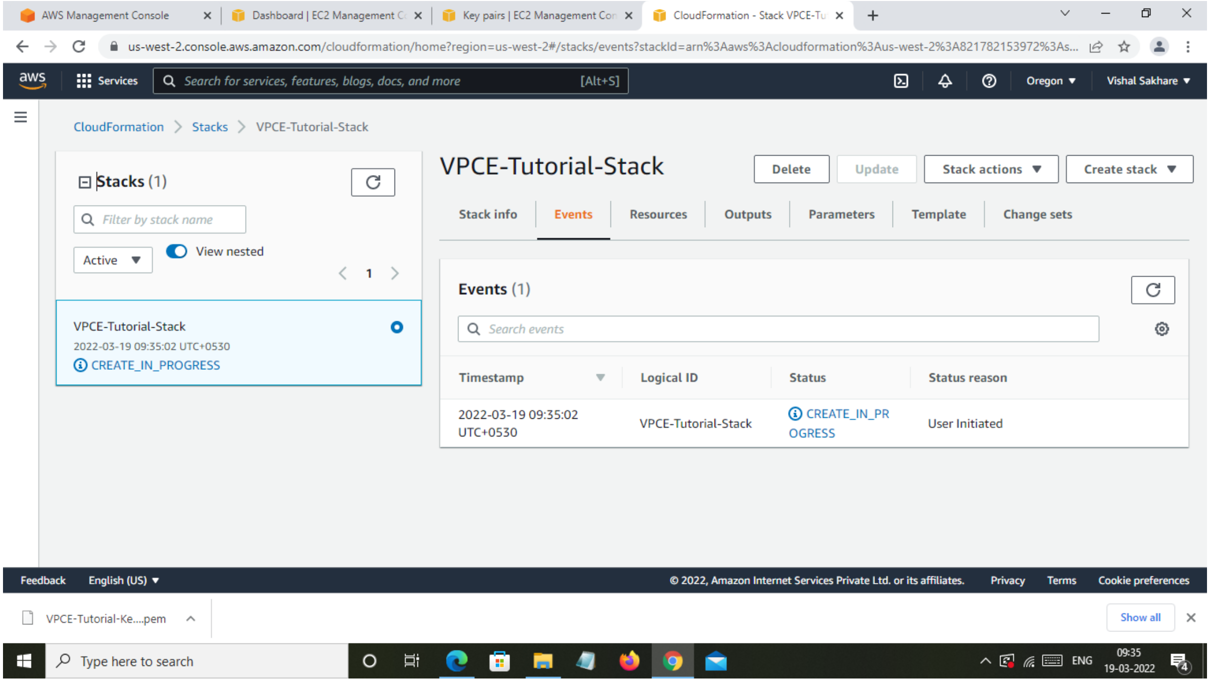
▸ **Stack policy**
Defines the resources that you want to protect from unintentional updates during a stack update.

▸ **Rollback configuration**

Feedback | English (US) ▼ | © 2022, Amazon Internet Services Private Ltd. or its affiliates. | Privacy | Terms | Cookie preferences

VPCE-Tutorial-Ke....pem | Show all

Type here to search | ENG | 09:34 19-03-2022



AWS Management Console | Dashboard | EC2 Management C | Key pairs | EC2 Management Con | CloudFormation - Stack VPCE-Tu

us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/events?stackId=arn%3Aaws%3Acloudformation%3Aus-west-2%3A821782153972%3As...

Services | Search for services, features, blogs, docs, and more [Alt+S] | Oregon ▼ | Vishal Sakhare ▼

CloudFormation > Stacks > VPCE-Tutorial-Stack

Stacks (1)

Filter by stack name

Active ▼ | View nested | 1

VPCE-Tutorial-Stack
2022-03-19 09:35:02 UTC+0530
CREATE_IN_PROGRESS

VPCE-Tutorial-Stack

Delete | Update | Stack actions ▼ | Create stack ▼

Stack info | Events | Resources | Outputs | Parameters | Template | Change sets

Events (1)

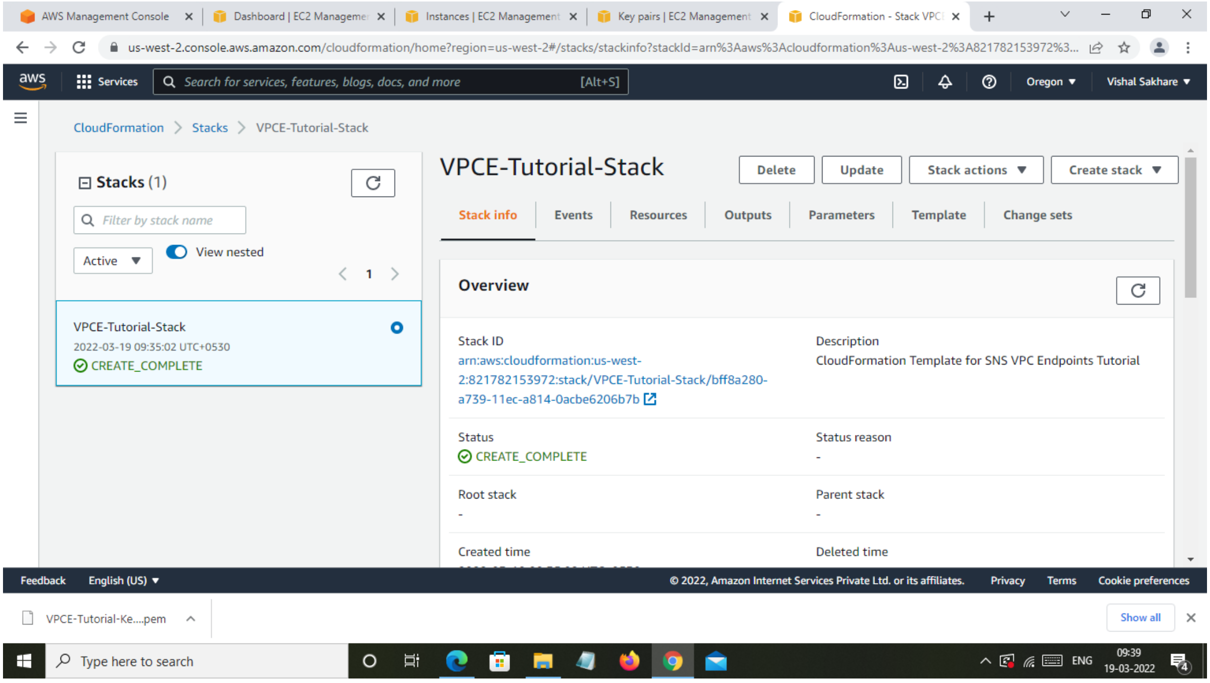
Search events

Timestamp	Logical ID	Status	Status reason
2022-03-19 09:35:02 UTC+0530	VPCE-Tutorial-Stack	CREATE_IN_PROGRESS	User Initiated

Feedback | English (US) ▼ | © 2022, Amazon Internet Services Private Ltd. or its affiliates. | Privacy | Terms | Cookie preferences

VPCE-Tutorial-Ke....pem | Show all

Type here to search | ENG | 09:35 19-03-2022


AWS Management Console
Dashboard | EC2 Manageme
Instances | EC2 Management
Key pairs | EC2 Management
CloudFormation - Stack VPC
us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/stackinfo?stackId=arn%3Aaws%3Acloudformation%3Aus-west-2%3A821782153972%3...
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Oregon
Vishal Sakhare
CloudFormation > Stacks > VPCE-Tutorial-Stack
Stacks (1)
Filter by stack name
Active
View nested
1
Delete
Update
Stack actions
Create stack
Stack info
Events
Resources
Outputs
Parameters
Template
Change sets
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
VPCE-Tutorial-Ke....pem
Show all
Type here to search
ENG
09:39
19-03-2022

VPCE-Tutorial-Stack
2022-03-19 09:35:02 UTC+0530
CREATE_COMPLETE

VPCE-Tutorial-Stack

Overview

Stack ID
arn:aws:cloudformation:us-west-2:821782153972:stack/VPCE-Tutorial-Stack/bff8a280-a739-11ec-a814-0acbe6206b7b

Description
CloudFormation Template for SNS VPC Endpoints Tutorial

Status
CREATE_COMPLETE

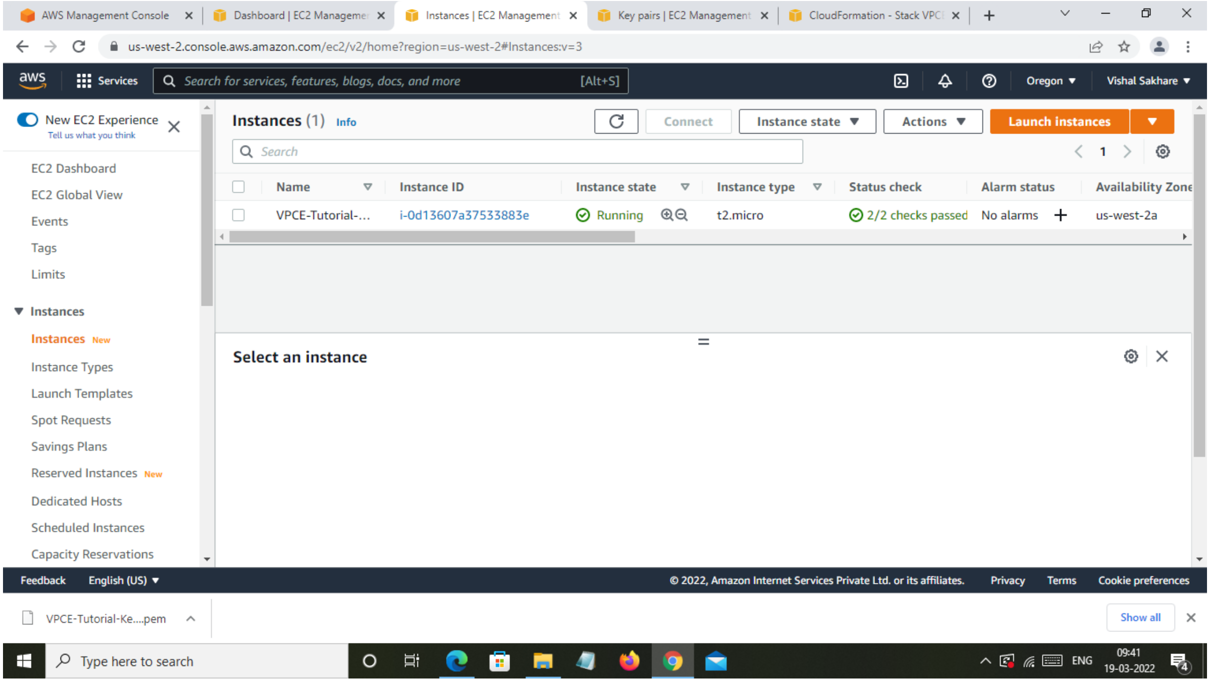
Status reason
-

Root stack
-

Parent stack
-

Created time

Deleted time



Instances (1) Info

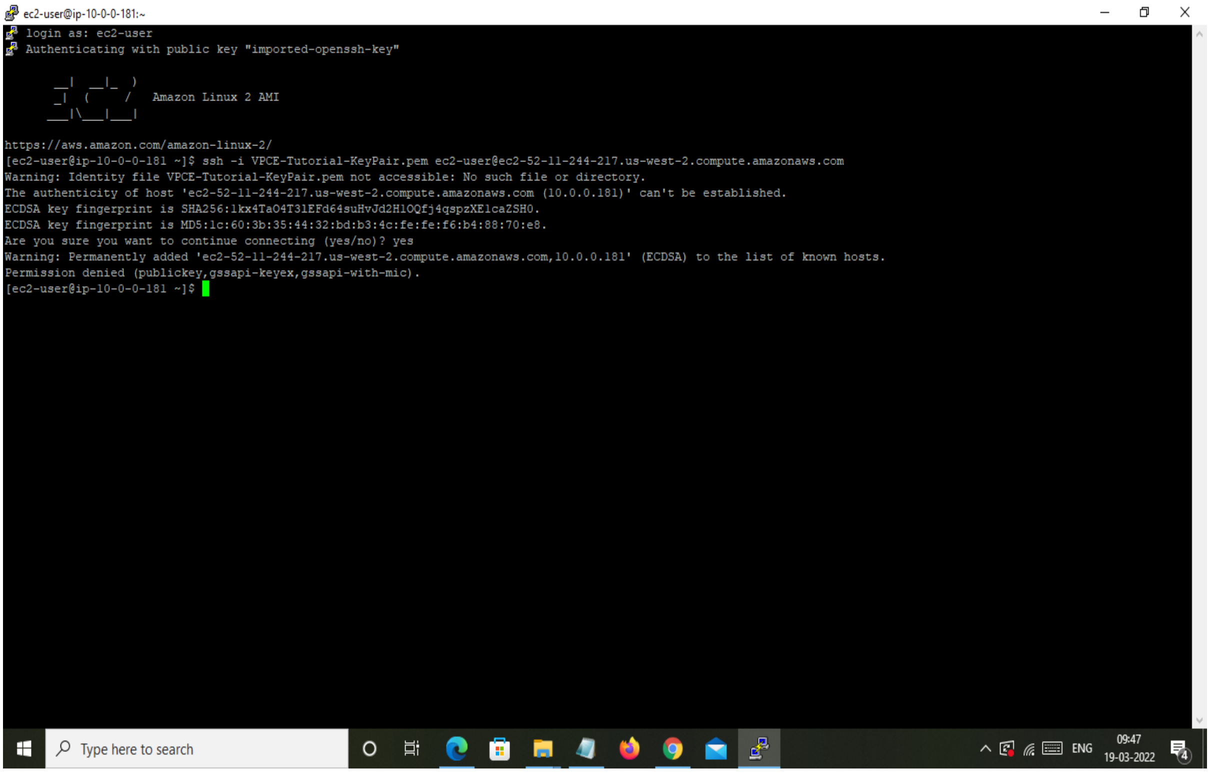
□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
□	VPCE-Tutorial-...	i-0d13607a37533883e	Running	t2.micro	2/2 checks passed	No alarms +	us-west-2a

Select an instance

Step 3: Confirm That Your Amazon EC2 Instance Lacks Internet Access

To connect to your Amazon EC2 instance

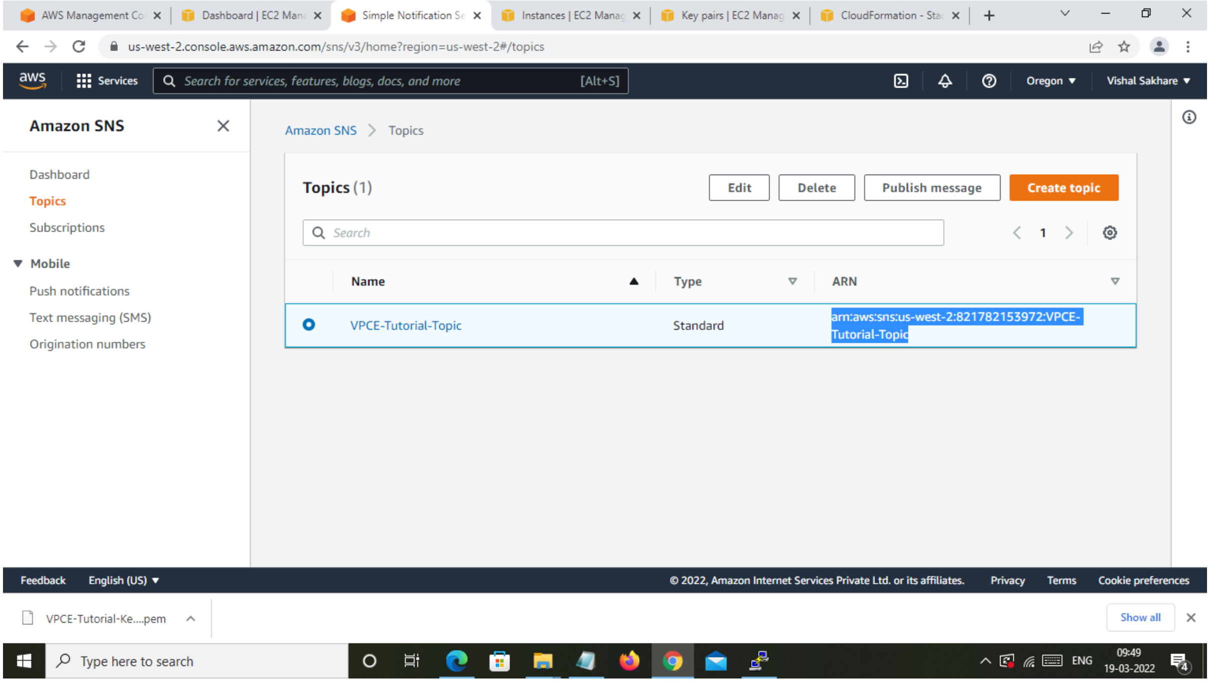
connection attempt fails



ec2-user@ip-10-0-0-181:~

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-181 ~]$ ssh -i VPCE-Tutorial-KeyPair.pem ec2-user@ec2-52-11-244-217.us-west-2.compute.amazonaws.com
Warning: Identity file VPCE-Tutorial-KeyPair.pem not accessible: No such file or directory.
The authenticity of host 'ec2-52-11-244-217.us-west-2.compute.amazonaws.com (10.0.0.181)' can't be established.
ECDSA key fingerprint is SHA256:1kx4TaO4T31EFd64suHvJd2H1OQfj4qspzXE1caZSH0.
ECDSA key fingerprint is MD5:1c:60:3b:35:44:32:bd:b3:4c:fe:fe:f6:b4:88:70:e8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-52-11-244-217.us-west-2.compute.amazonaws.com,10.0.0.181' (ECDSA) to the list of known hosts.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-0-181 ~]$
```

To verify that the instance lacks connectivity to Amazon SNS

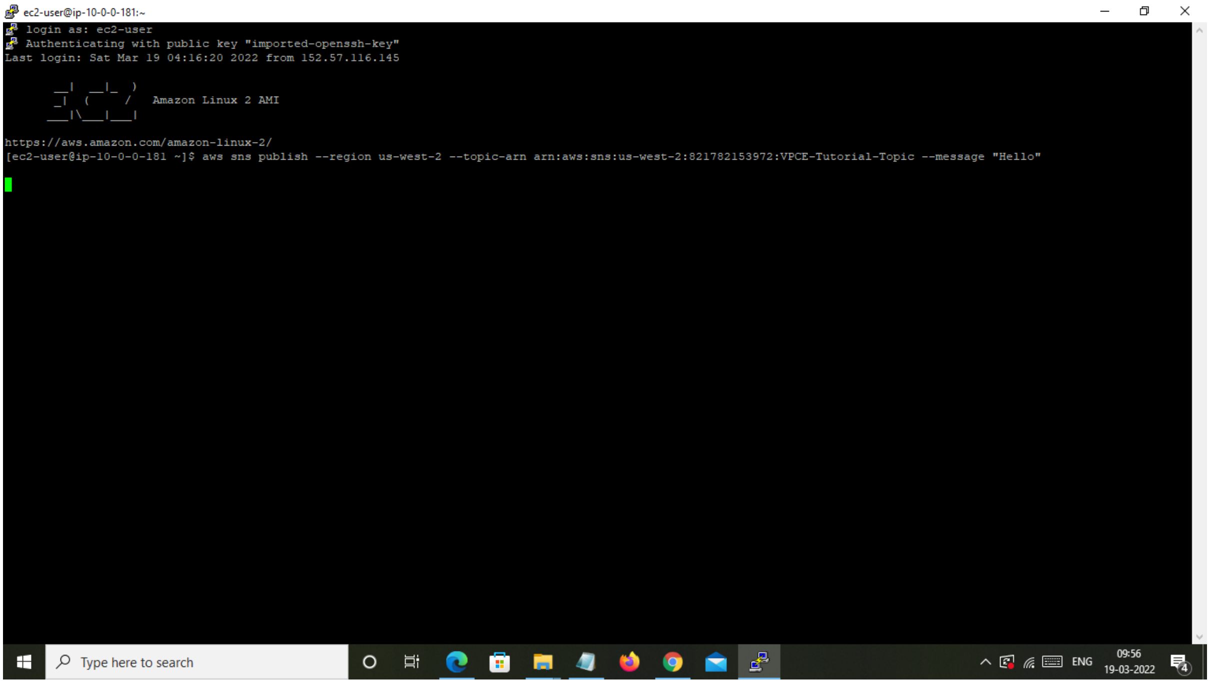


us-west-2.console.aws.amazon.com/sns/v3/home?region=us-west-2#/topics

Topics (1)

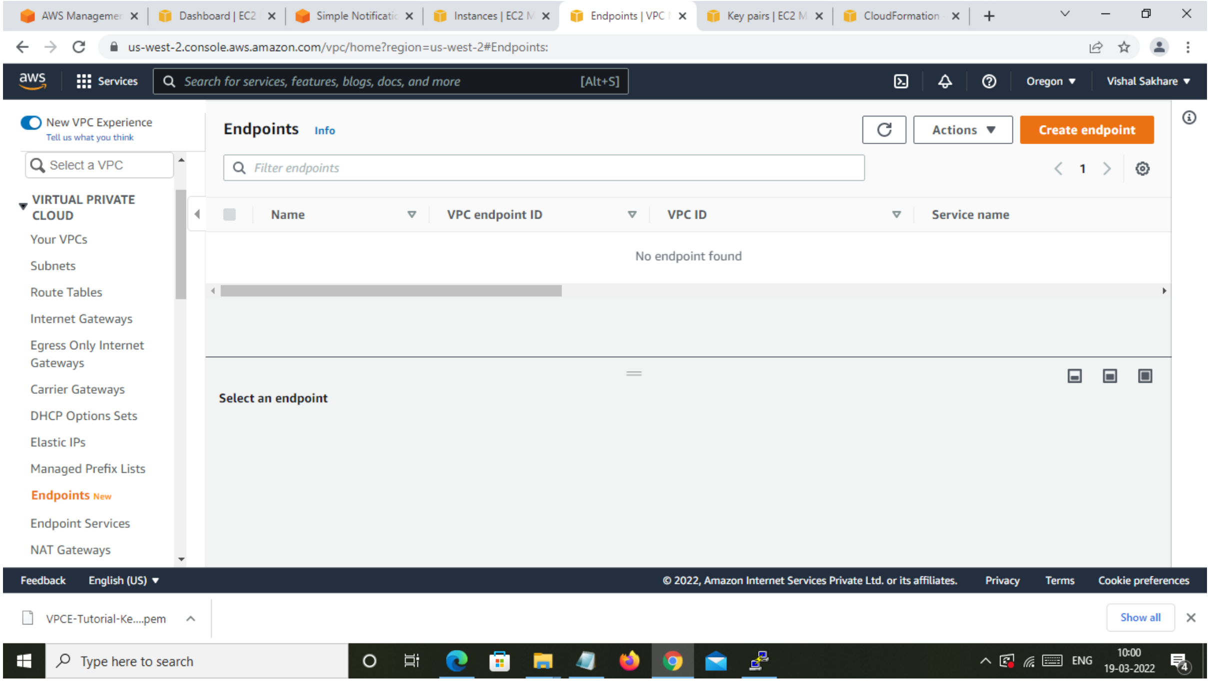
	Name	Type	ARN
●	VPCE-Tutorial-Topic	Standard	arn:aws:sns:us-west-2:821782153972:VPCE-Tutorial-Topic

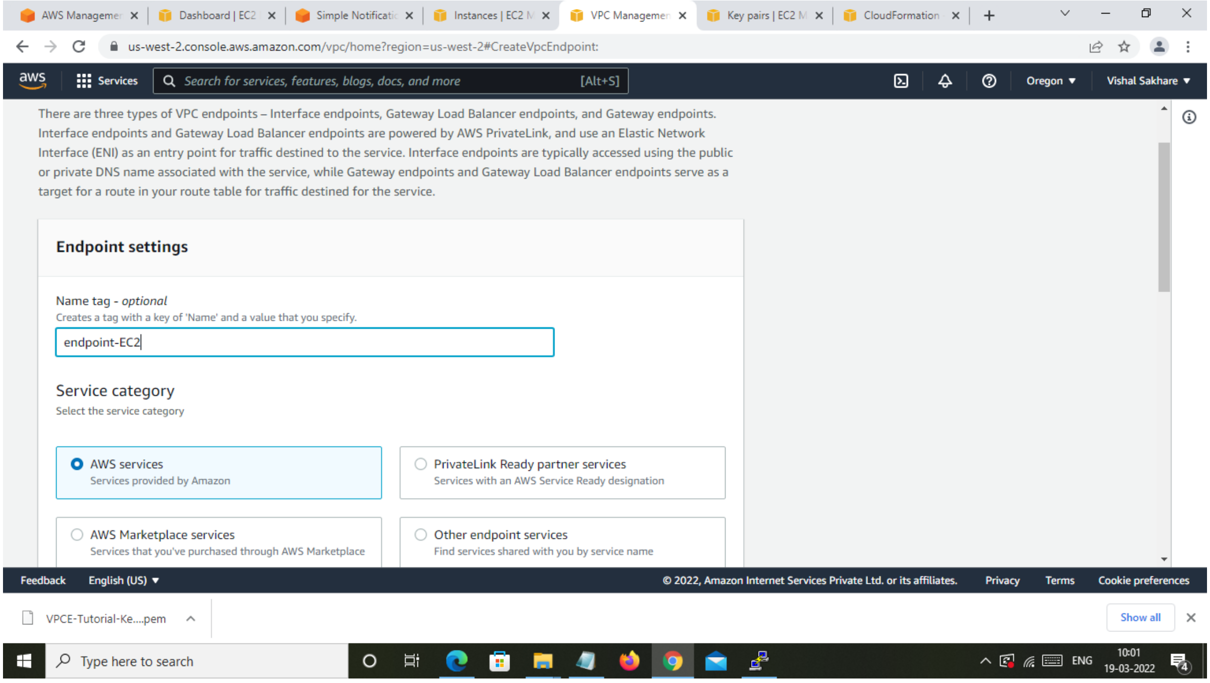
the publish attempt fails



```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Sat Mar 19 04:16:20 2022 from 152.57.116.145

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-181 ~]$ aws sns publish --region us-west-2 --topic-arn arn:aws:sns:us-west-2:821782153972:VPCE-Tutorial-Topic --message "Hello"
```

Step 4: Create an Amazon VPC Endpoint for Amazon SNS





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-EC2

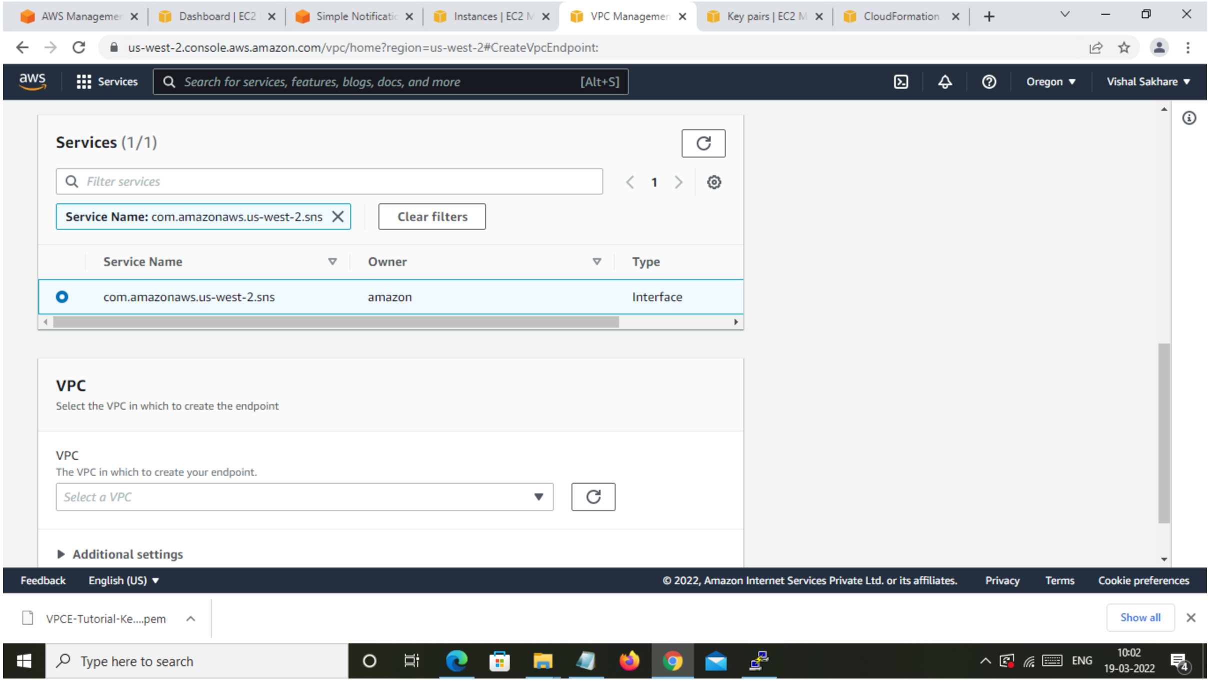
Service category
Select the service category

● 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

○ Other endpoint services
Find services shared with you by service name



Services (1/1)

Filter services

Service Name: com.amazonaws.us-west-2.sns ✕ | Clear filters

	Service Name	Owner	Type
●	com.amazonaws.us-west-2.sns	amazon	Interface

VPC

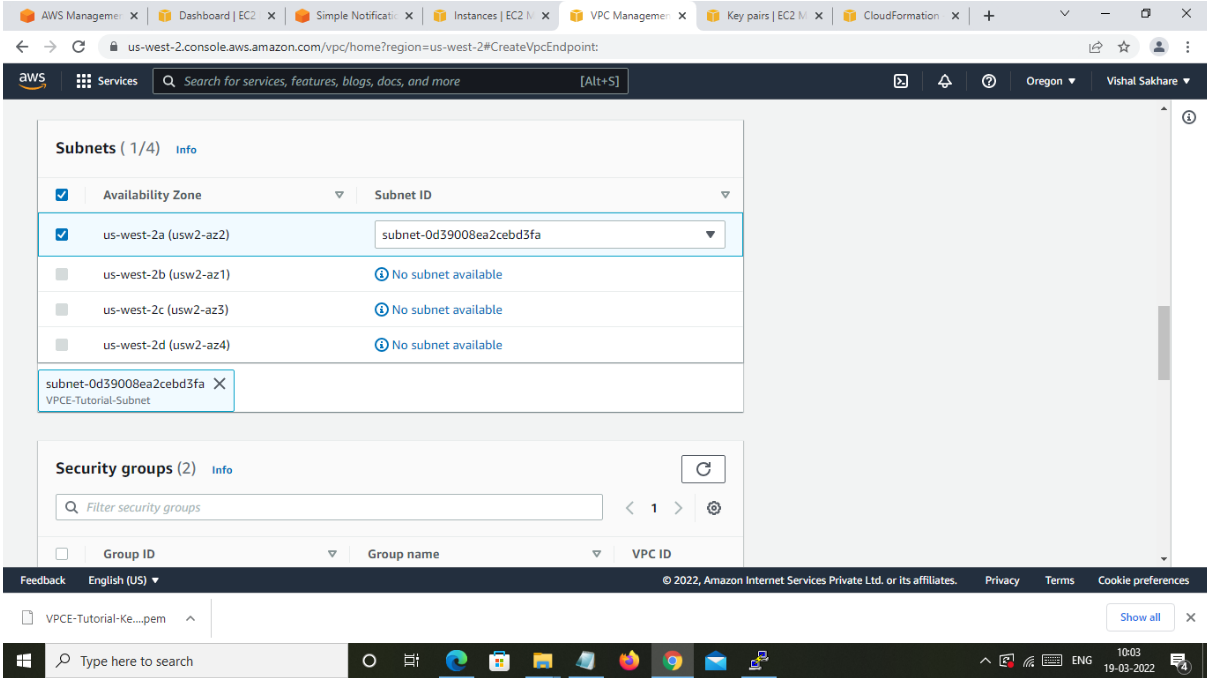
Select the VPC in which to create the endpoint

VPC

The VPC in which to create your endpoint.

Select a VPC ▼

▶ Additional settings



Subnets (1/4) Info

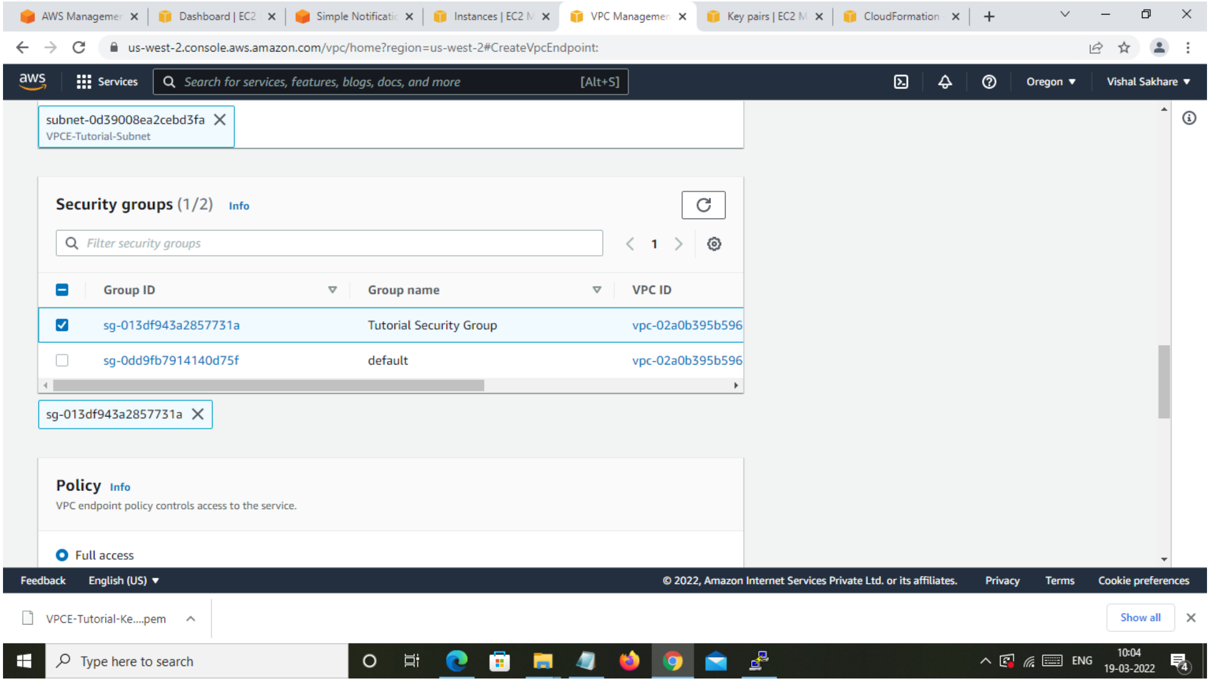
☑	Availability Zone	Subnet ID
☑	us-west-2a (usw2-az2)	subnet-0d39008ea2cebd3fa ▼
□	us-west-2b (usw2-az1)	ⓘ No subnet available
□	us-west-2c (usw2-az3)	ⓘ No subnet available
□	us-west-2d (usw2-az4)	ⓘ No subnet available

subnet-0d39008ea2cebd3fa ✕
VPCE-Tutorial-Subnet

Security groups (2) Info

Filter security groups

□	Group ID	Group name	VPC ID


AWS Manageme | Dashboard | EC2 | Simple Notificati | Instances | EC2 | VPC Managemen | Key pairs | EC2 | CloudFormation
Services
Search for services, features, blogs, docs, and more [Alt+S]
Oregon ▼ Vishal Sakhare ▼
Feedback English (US) ▼
© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences
VPCE-Tutorial-Ke....pem
Show all
Type here to search
ENG 10:04 19-03-2022

us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#CreateVpcEndpoint:

subnet-0d39008ea2cebd3fa
VPCE-Tutorial-Subnet

Security groups (1/2) Info

Filter security groups

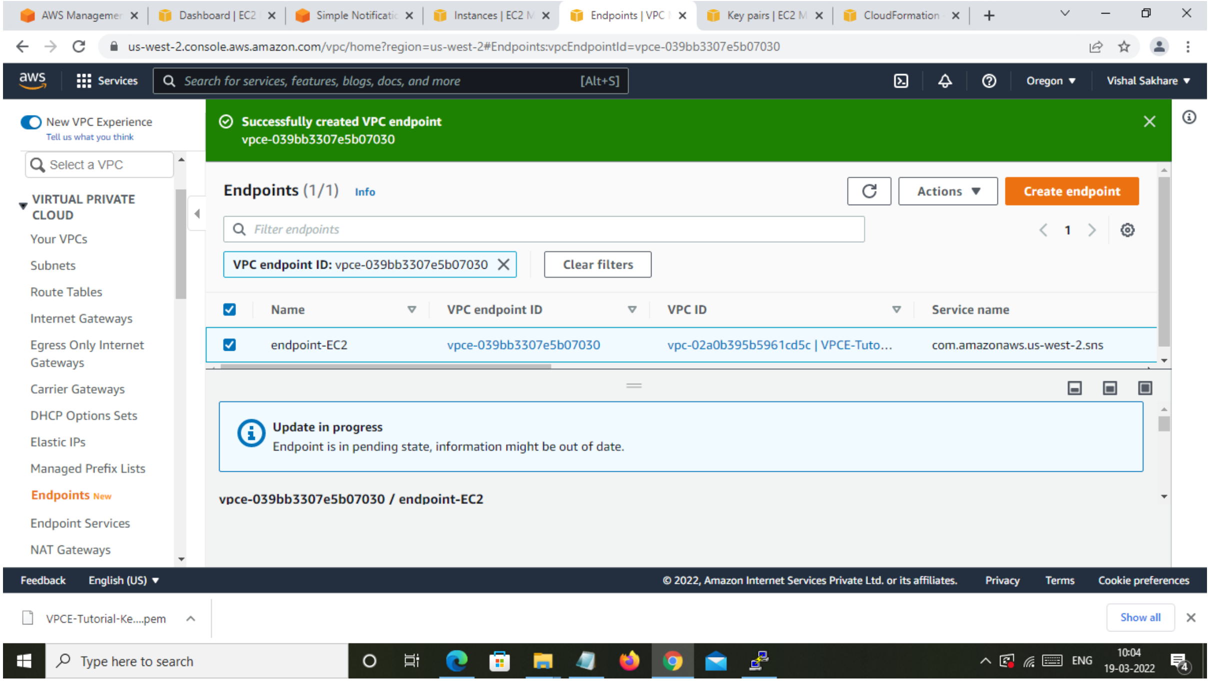
	Group ID	Group name	VPC ID
☑	sg-013df943a2857731a	Tutorial Security Group	vpc-02a0b395b596
□	sg-0dd9fb7914140d75f	default	vpc-02a0b395b596

sg-013df943a2857731a

Policy Info

VPC endpoint policy controls access to the service.

● Full access



us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#Endpoints:vpcEndpointId=vpce-039bb3307e5b07030

Successfully created VPC endpoint
vpce-039bb3307e5b07030

Endpoints (1/1) Info

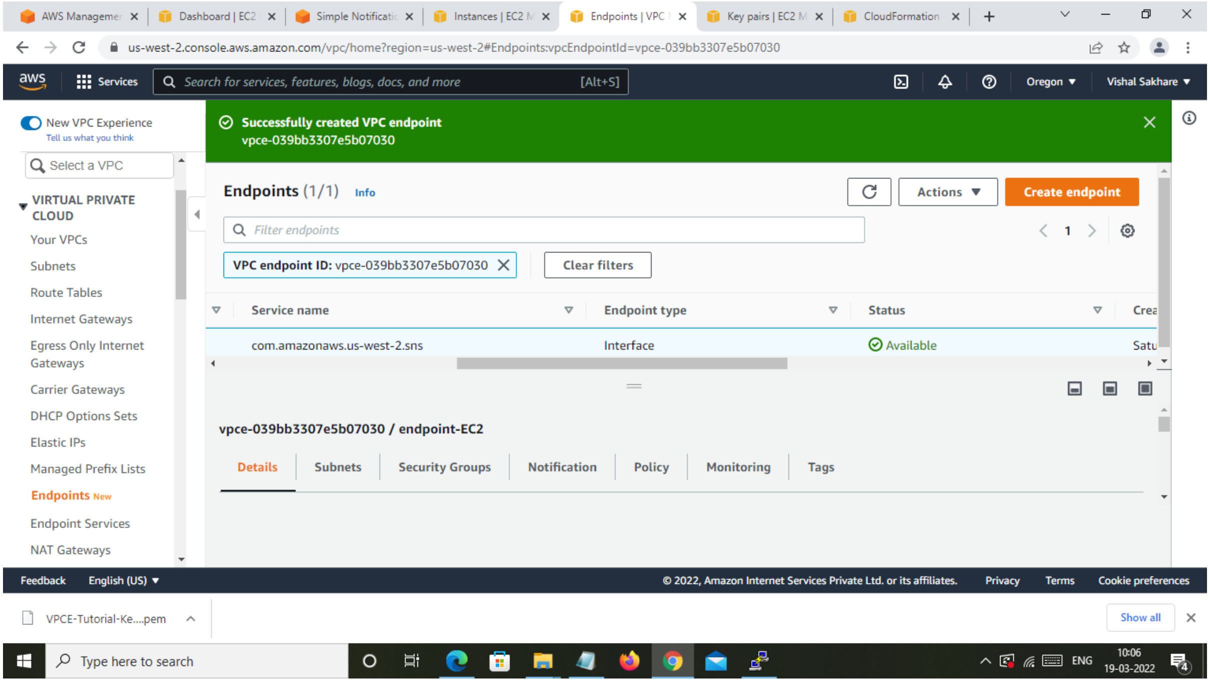
Filter endpoints

VPC endpoint ID: vpce-039bb3307e5b07030

	Name	VPC endpoint ID	VPC ID	Service name
☑	endpoint-EC2	vpce-039bb3307e5b07030	vpc-02a0b395b5961cd5c | VPCE-Tuto...	com.amazonaws.us-west-2.sns

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

vpce-039bb3307e5b07030 / endpoint-EC2



us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#Endpoints:vpcEndpointId=vpce-039bb3307e5b07030

Successfully created VPC endpoint
vpce-039bb3307e5b07030

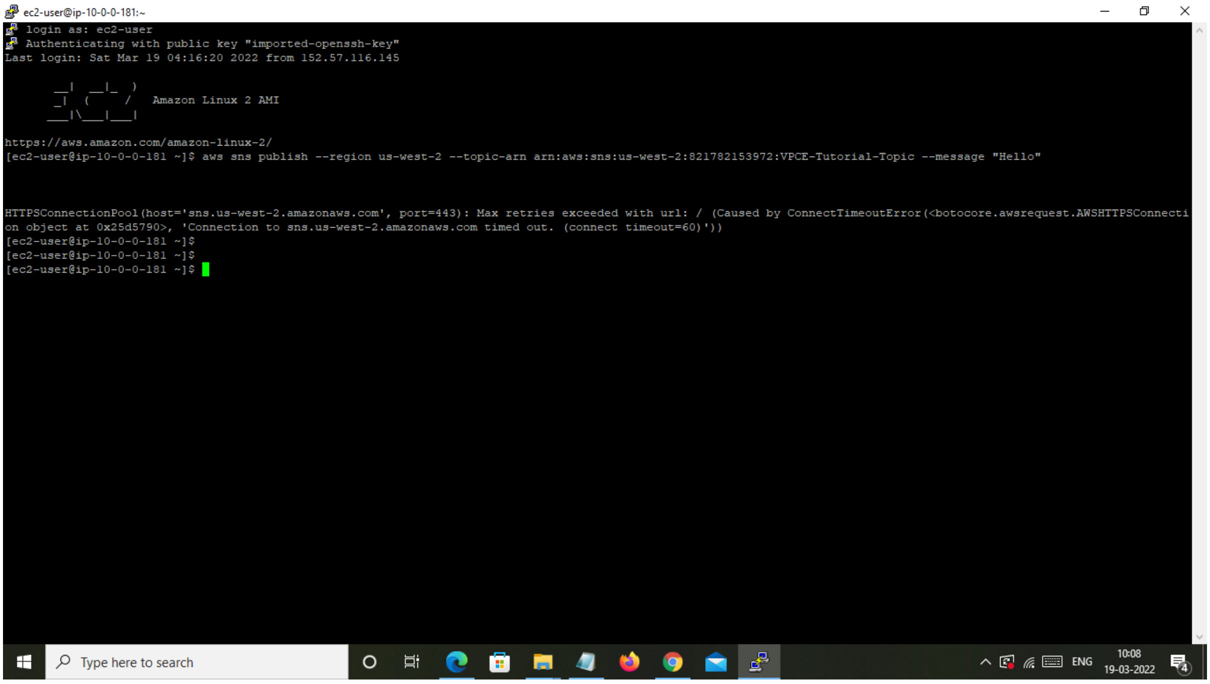
Endpoints (1/1) Info

VPC endpoint ID: vpce-039bb3307e5b07030

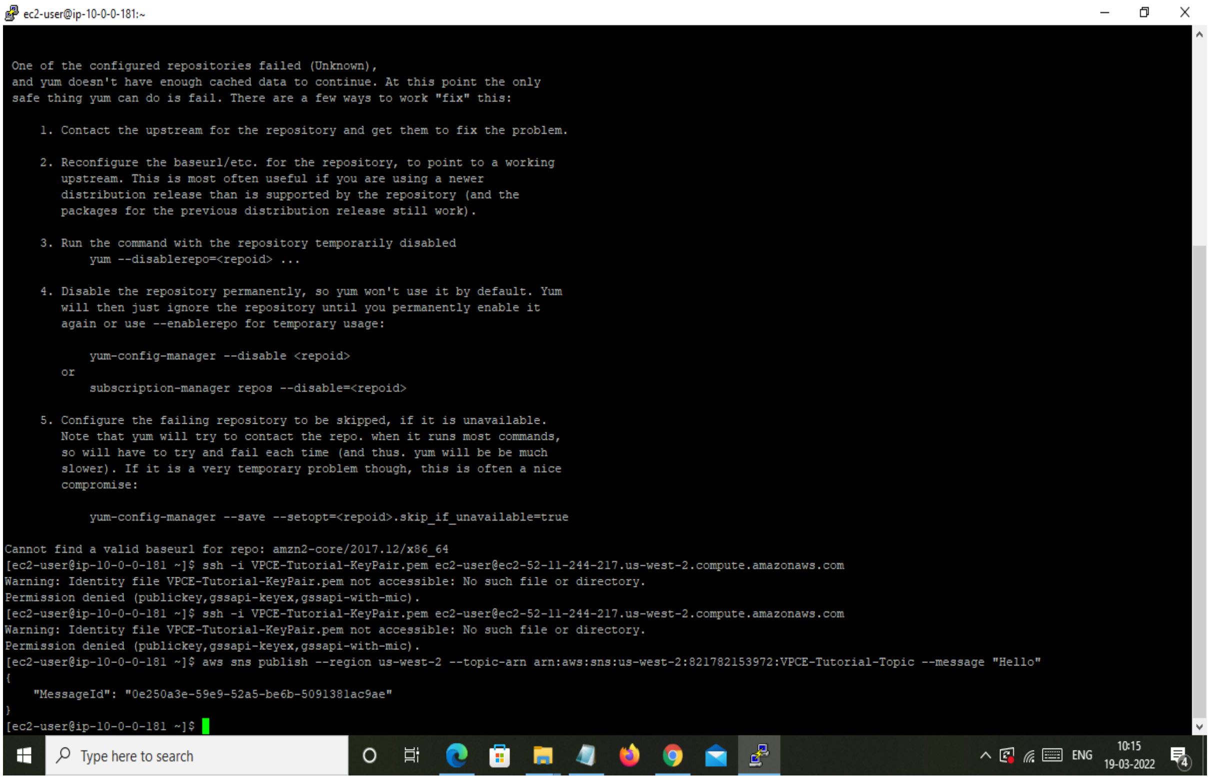
Service name	Endpoint type	Status	Crea
com.amazonaws.us-west-2.sns	Interface	✓ Available	Satu

vpce-039bb3307e5b07030 / endpoint-EC2

To publish a message

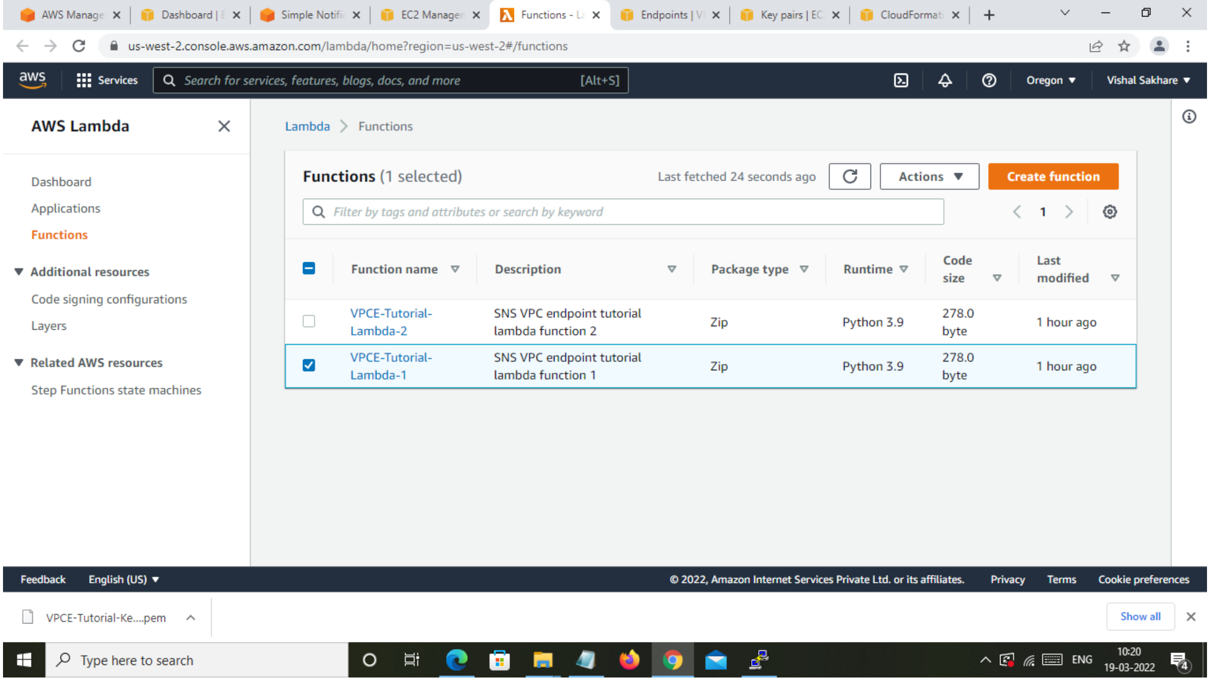


```
 login as: ec2-user
 Authenticating with public key "imported-openssh-key"
Last login: Sat Mar 19 04:16:20 2022 from 152.57.116.145

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-181 ~]$ aws sns publish --region us-west-2 --topic-arn arn:aws:sns:us-west-2:821782153972:VPCE-Tutorial-Topic --message "Hello"



HTTPSConnectionPool(host='sns.us-west-2.amazonaws.com', port=443): Max retries exceeded with url: / (Caused by ConnectTimeoutError(<botocore.awsrequest.AWSHTTPSConnecti
on object at 0x25d5790>, 'Connection to sns.us-west-2.amazonaws.com timed out. (connect timeout=60)'))
[ec2-user@ip-10-0-0-181 ~]$
[ec2-user@ip-10-0-0-181 ~]$
[ec2-user@ip-10-0-0-181 ~]$
```



```

 One of the configured repositories failed (Unknown),
 and yum doesn't have enough cached data to continue. At this point the only
 safe thing yum can do is fail. There are a few ways to work "fix" this:

     1. Contact the upstream for the repository and get them to fix the problem.

     2. Reconfigure the baseurl/etc. for the repository, to point to a working
        upstream. This is most often useful if you are using a newer
        distribution release than is supported by the repository (and the
        packages for the previous distribution release still work).

     3. Run the command with the repository temporarily disabled
            yum --disablerepo=<repoid> ...

     4. Disable the repository permanently, so yum won't use it by default. Yum
        will then just ignore the repository until you permanently enable it
        again or use --enablerepo for temporary usage:

            yum-config-manager --disable <repoid>
        or
            subscription-manager repos --disable=<repoid>

     5. Configure the failing repository to be skipped, if it is unavailable.
        Note that yum will try to contact the repo. when it runs most commands,
        so will have to try and fail each time (and thus. yum will be be much
        slower). If it is a very temporary problem though, this is often a nice
        compromise:

            yum-config-manager --save --setopt=<repoid>.skip_if_unavailable=true

Cannot find a valid baseurl for repo: amzn2-core/2017.12/x86_64
[ec2-user@ip-10-0-0-181 ~]$ ssh -i VPCE-Tutorial-KeyPair.pem ec2-user@ec2-52-11-244-217.us-west-2.compute.amazonaws.com
Warning: Identity file VPCE-Tutorial-KeyPair.pem not accessible: No such file or directory.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-0-181 ~]$ ssh -i VPCE-Tutorial-KeyPair.pem ec2-user@ec2-52-11-244-217.us-west-2.compute.amazonaws.com
Warning: Identity file VPCE-Tutorial-KeyPair.pem not accessible: No such file or directory.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-0-181 ~]$ aws sns publish --region us-west-2 --topic-arn arn:aws:sns:us-west-2:821782153972:VPCE-Tutorial-Topic --message "Hello"
{
    "MessageId": "0e250a3e-59e9-52a5-be6b-509138lac9ae"
}
[ec2-user@ip-10-0-0-181 ~]$
```

Step 6: Verify Your Message Deliveries



us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2#/functions

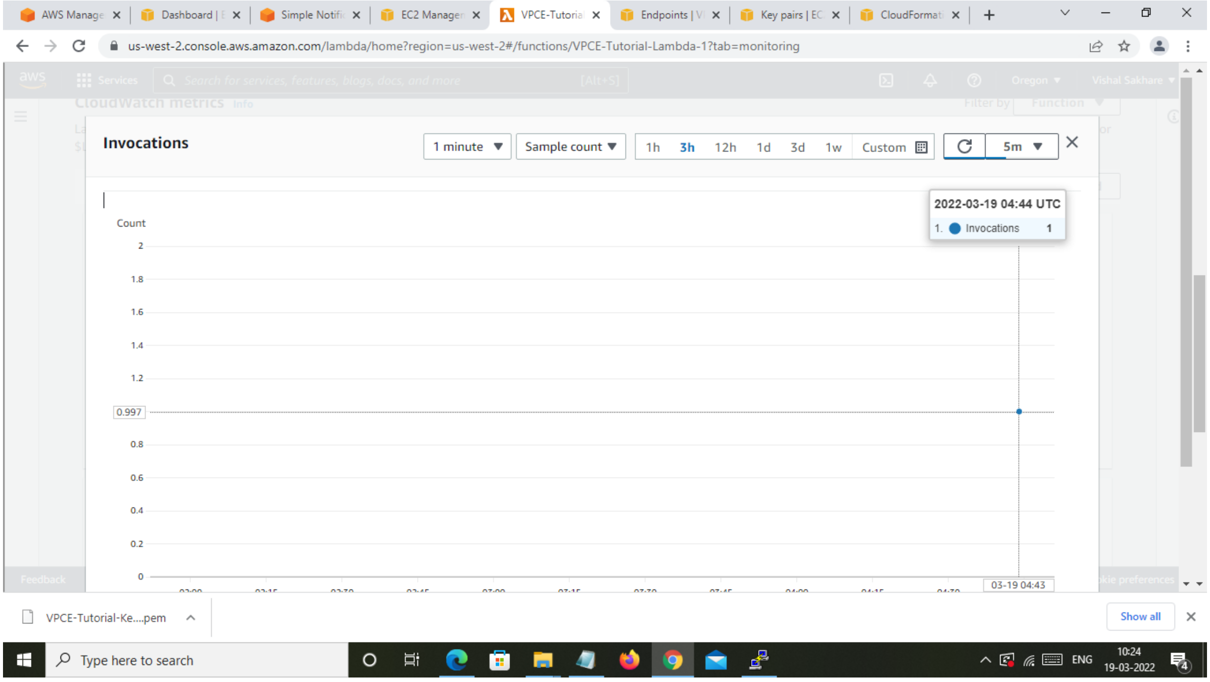
AWS Lambda

Lambda > Functions

Functions (1 selected) — Last fetched 24 seconds ago

	Function name	Description	Package type	Runtime	Code size	Last modified
□	VPCE-Tutorial-Lambda-2	SNS VPC endpoint tutorial lambda function 2	Zip	Python 3.9	278.0 byte	1 hour ago
☑	VPCE-Tutorial-Lambda-1	SNS VPC endpoint tutorial lambda function 1	Zip	Python 3.9	278.0 byte	1 hour ago

To verify that the Lambda functions were invoked

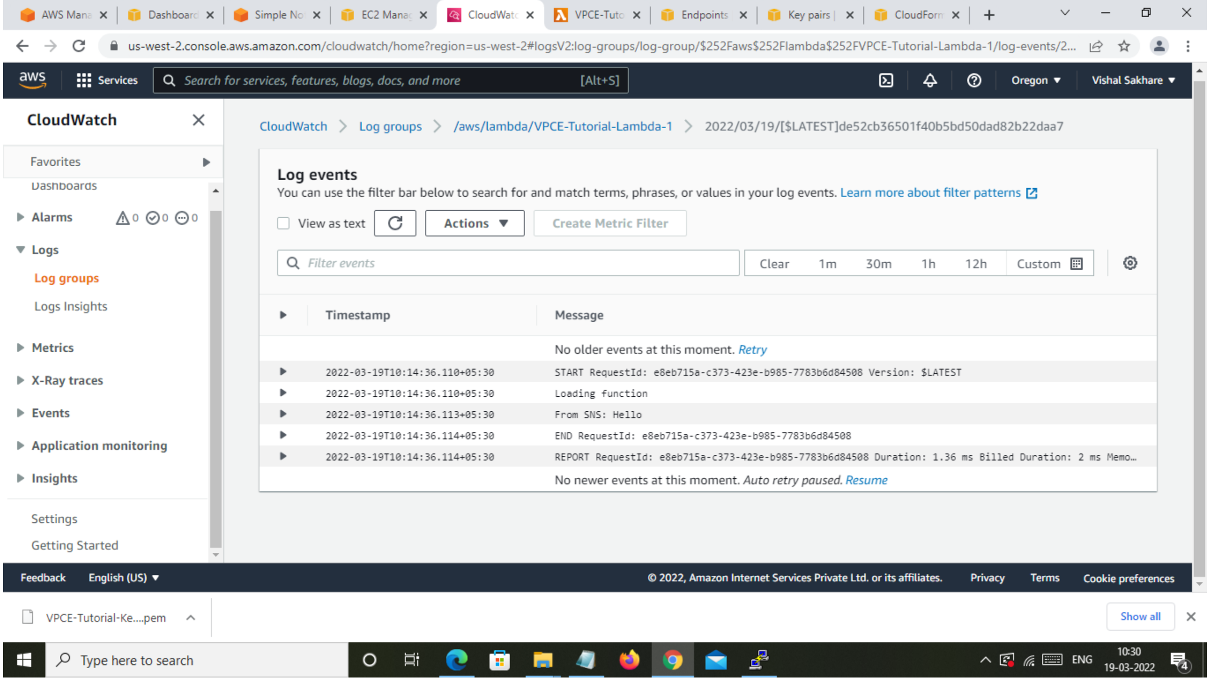


us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2#/functions/VPCE-Tutorial-Lambda-1?tab=monitoring

Invocations — 1 minute, Sample count, 3h, 5m

2022-03-19 04:44 UTC
1. Invocations 1

To verify that the CloudWatch logs were updated



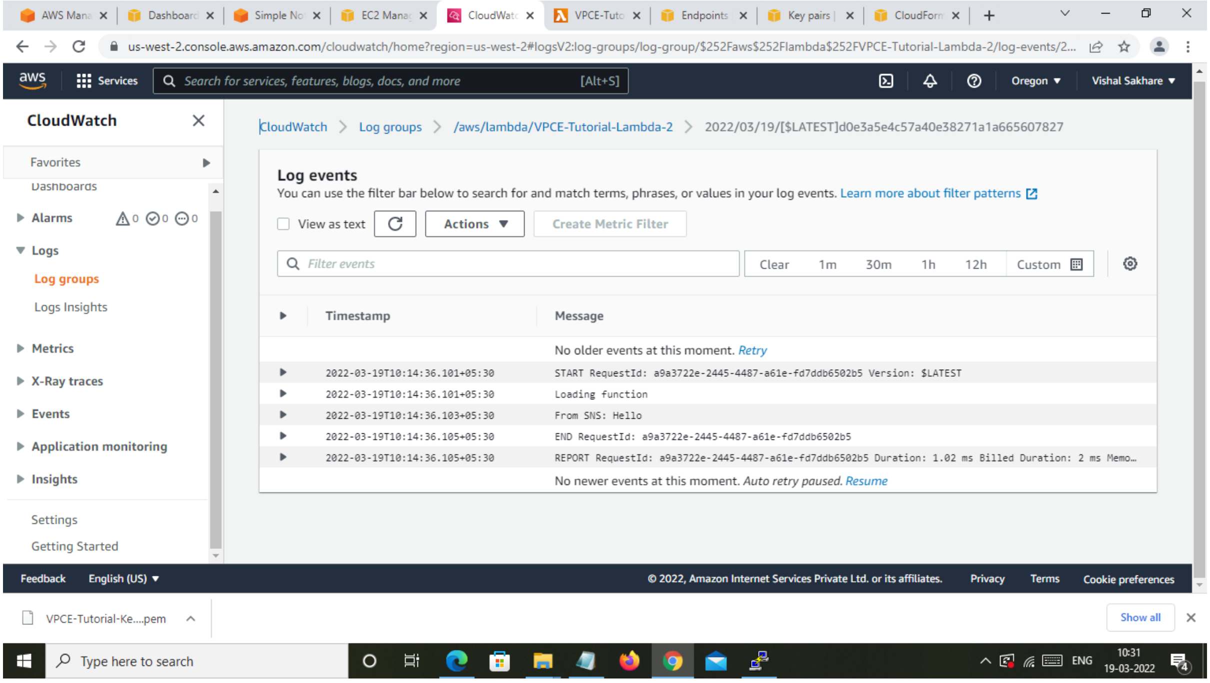
us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2#logsV2:log-groups/log-group/$252Faws$252Flambda$252FVPCE-Tutorial-Lambda-1/log-events/2...

CloudWatch > Log groups > /aws/lambda/VPCE-Tutorial-Lambda-1 > 2022/03/19/[$LATEST]de52cb36501f40b5bd50dad82b22daa7

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

```
Timestamp                      Message
                               No older events at this moment. Retry
2022-03-19T10:14:36.110+05:30  START RequestId: e8eb715a-c373-423e-b985-7783b6d84508 Version: $LATEST
2022-03-19T10:14:36.110+05:30  Loading function
2022-03-19T10:14:36.113+05:30  From SNS: Hello
2022-03-19T10:14:36.114+05:30  END RequestId: e8eb715a-c373-423e-b985-7783b6d84508
2022-03-19T10:14:36.114+05:30  REPORT RequestId: e8eb715a-c373-423e-b985-7783b6d84508 Duration: 1.36 ms Billed Duration: 2 ms Memo…
                               No newer events at this moment. Auto retry paused. Resume
```



us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2#logsV2:log-groups/log-group/$252Faws$252Flambda$252FVPCE-Tutorial-Lambda-2/log-events/2...

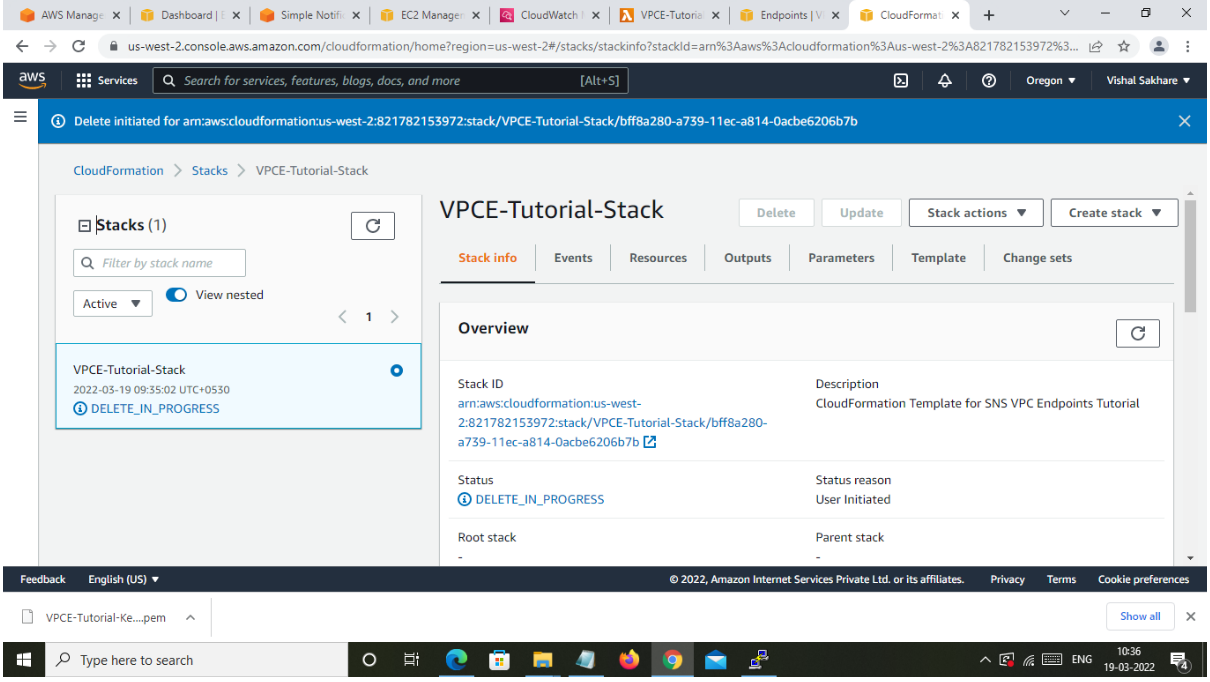
CloudWatch > Log groups > /aws/lambda/VPCE-Tutorial-Lambda-2 > 2022/03/19/[$LATEST]d0e3a5e4c57a40e38271a1a665607827

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

```
Timestamp                      Message
                               No older events at this moment. Retry
2022-03-19T10:14:36.101+05:30  START RequestId: a9a3722e-2445-4487-a61e-fd7ddb6502b5 Version: $LATEST
2022-03-19T10:14:36.101+05:30  Loading function
2022-03-19T10:14:36.103+05:30  From SNS: Hello
2022-03-19T10:14:36.105+05:30  END RequestId: a9a3722e-2445-4487-a61e-fd7ddb6502b5
2022-03-19T10:14:36.105+05:30  REPORT RequestId: a9a3722e-2445-4487-a61e-fd7ddb6502b5 Duration: 1.02 ms Billed Duration: 2 ms Memo…
                               No newer events at this moment. Auto retry paused. Resume
```

Step 7: Clean Up



us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/stackinfo?stackId=arn%3Aaws%3Acloudformation%3Aus-west-2%3A821782153972%3...

Delete initiated for arn:aws:cloudformation:us-west-2:821782153972:stack/VPCE-Tutorial-Stack/bff8a280-a739-11ec-a814-0acbe6206b7b

CloudFormation > Stacks > VPCE-Tutorial-Stack

Stacks (1)

VPCE-Tutorial-Stack
2022-03-19 09:35:02 UTC+0530
DELETE_IN_PROGRESS

VPCE-Tutorial-Stack

Overview

Stack ID
arn:aws:cloudformation:us-west-2:821782153972:stack/VPCE-Tutorial-Stack/bff8a280-a739-11ec-a814-0acbe6206b7b

Description
CloudFormation Template for SNS VPC Endpoints Tutorial

Status
DELETE_IN_PROGRESS

Status reason
User Initiated

Root stack
-

Parent stack
-

© 2022, Amazon Internet Services Private Ltd. or its affiliates.