

## **Project - 3**

### **Publishing Amazon SNS messages privately**

#### **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 notification. 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 message privately, you can improve the message delivery and receipt through Amazon SNS.

#### **Highlights:**

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

#### **Steps:**

- Click the create key pair
- Provide the name of the key pair as VPCE-Tutorial-Keypair
- Finally key pair is created
- Click the create stack
- Next upload the code-yaml file to create the necessary resource
- Provide the name for the stack as VPC-Tutorial-Stack
- Select the key pair which was created and SSH location as 0.0.0.0/0 in parameter
- And provide the necessary configuration
- Click the submit
- Finally the stack is created
- Connect to EC2 to instance which was created by cloud formation
- To check the instance lack of internet connectivity run the command ping amazon.com
- Click the create endpoint

- Provide the name for the endpoint
- Select the AWS service in service category
- Select the SNS of the region where the stack is created
- Select the VPC and subnet which was created by stack
- Select the security group which was created by stack
- Finally endpoint is created
- Navigate to SNS and Go into the Topic
- And click the create subscription
- Select the protocol as Email and provide the necessary in endpoint
- Finally subscription is created
- A subscription mail will be received to provided mail ID and confirm the same
- Navigate to EC2 and connect to Instance
- To publish the message by running the command by `aws sns publish --region aws-region --topic-arn sns-topic-arn --message "Necessary message"`
- Now the message will be received to the mail ID which is provided in the creation of subscription
- Also check weather message published successfully by navigating to lambda
- Click the lambda function which was created by stack
- Go to the monitor and go to view cloudwatch log
- Next go inside the log stream and the published message will be reflected.

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

VPCE-Tutorial-Keypair

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type [Info](#)

☒ RSA
 ☐ ED25519

Private key file format

☐ .pem  
For use with OpenSSH
 ☒ .ppk  
For use with PuTTY

Tags - optional

No tags associated with the resource.

VPCE-Tutorial-Keypair

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

Info

☒ RSA

☐ ED25519

Private key file format

☐ .pem

For use with OpenSSH

☒ .ppk

For use with PuTTY

Tags - optional

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Create key pair

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Preview

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity

Reservations

New

Successfully created key pair

Key pairs (2)

Info

Find Key Pair by attribute or tag

	Name	Type	Created	Fingerprint	ID
<input type="checkbox"/>	new	rsa	2024/04/02 21:09 GMT+5:30	3f:88:35:fc:3a:3d:48:ca:a4:22:02:01...	key-010k
<input type="checkbox"/>	VPCE-Tutorial-Keypair	rsa	2024/04/14 15:52 GMT+5:30	26:f4:70:af:62:06:62:3e:43:93:7a:7...	key-030k

CloudShellFeedback

© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

CloudFormation

Stacks

Create stack

Step 1

Create stack

Step 2

Specify stack details

Step 3

Configure stack options

Step 4

Review and create

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.

☒ Choose an existing template

Upload or choose an existing template.

☐ Use a sample template

Choose from our sample template library.

☐ Build from Application Composer

Create a template using a visual builder.

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

CloudShellFeedback

© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

### 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

Provide an Amazon S3 URL to your template.

☒ Upload a template file

Upload your template directly to the console.

☐ Sync from Git - *new*

Sync a template from your Git repository.

#### Upload a template file

Choose file

Project3Updated project 3.yaml

JSON or YAML formatted file

S3 URL: In progress

View in Application Composer

CloudFormation > Stacks > Create stack

Step 1  
[Create stack](#)

Step 2  
**Specify stack details**

Step 3  
Configure stack options

Step 4  
Review and create

## Specify stack details

### Provide a 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

Select AWS::EC2::KeyPair::KeyName

Step 3

Configure stack options

Step 4

Review and create

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

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

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.

Delete newly created resources during a rollback

Specify whether resources that were created during a failed operation should be deleted regardless of their deletion policy. [Learn more](#)

☒ Use deletion policy

Retains or deletes created resources according to their attached deletion policy.

☐ Delete all newly created resources

Deletes created resources during a rollback regardless of their attached deletion policy.

Advanced options

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Step 2: Specify stack details

Edit

Provide a stack name

Stack name

VPCE-Tutorial-Stack

Parameters (2)

Q Search

< 1 > ⚙

Key	Value
KeyName	VPCE-Tutorial-Keypair
SSHLocation	0.0.0.0/0

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Termination protection

Deactivated

► Quick-create link

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Create change set

Cancel

Previous

Submit

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

CloudFormation > Stacks > VPCE-Tutorial-Stack

Stacks (1)

Filter by stack name

Filter status

Active

View nested

< 1 >

Stacks

VPCE-Tutorial-Stack

2024-04-14 16:00:59 UTC+0530

CREATE\_IN\_PROGRESS

VPCE-Tutorial-Stack

Delete

Update

Stack actions

Create stack

< Stack info

Events

Resources

Outputs

Parameters

>

Events (1)

Detect root cause

Search events

Timestamp	Logical ID	Status
2024-04-14 16:00:59 UTC+0530	VPCE-Tutorial-Stack	CREATE_IN_PROGRESS

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

CloudFormation > Stacks > VPCE-Tutorial-Stack

Stacks (1)

Filter by stack name

Filter status

Active

View nested

< 1 >

Stacks

VPCE-Tutorial-Stack

2024-04-14 16:00:59 UTC+0530

CREATE\_COMPLETE

VPCE-Tutorial-Stack

Delete

Update

Stack actions

Create stack

< Stack info

Events

Resources

Outputs

Parameters

>

Events (65)

Detect root cause

Search events

Timestamp	Logical ID	Status
2024-04-14 16:03:34 UTC+0530	VPCE-Tutorial-Stack	CREATE_COMPLETE
2024-04-14 16:03:33 UTC+0530	ECInstanceProfile	CREATE_COMPLETE

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

CloudFormation > Stacks > VPCE-Tutorial-Stack

Stacks (1)

Filter by stack name

Filter status

Active

View nested

< 1 >

Stacks

VPCE-Tutorial-Stack

2024-04-14 16:00:59 UTC+0530

CREATE\_COMPLETE

Events (65)

Detect root cause

Search events

Timestamp	Logical ID	Status
2024-04-14 16:02:07 UTC+0530	SNSTopic	CREATE_COMPLETE
2024-04-14 16:02:04 UTC+0530	EC2Instance	CREATE_COMPLETE
2024-04-14 16:01:47 UTC+0530	VPCGatewayAttachment	CREATE_COMPLETE
2024-04-14 16:01:38 UTC+0530	LambdaPermission2	CREATE_COMPLETE
2024-04-14 16:01:38 UTC+0530	LambdaPermission1	CREATE_COMPLETE

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity

Reservations

Instances (1)

Find Instance by attribute or tag (case-sensitive)

Instance state = running

Clear filters

1

Launch instances

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
	VPCE-Tutorial...	i-0b7c4be8e4221e974	Running	t2.micro	2/2 checks passed	View alarms

Select an instance

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity

Reservations

EC2 > Security Groups > sg-03ffaab71bb4c92e1 - Tutorial Security Group

sg-03ffaab71bb4c92e1 - Tutorial Security Group

Actions

Details

Security group name	Security group ID	Description	VPC ID
Tutorial Security Group	sg-03ffaab71bb4c92e1	Security group for SNS VPC endpoint tutorial	vpc-0987eba7ebe1bf9cb
Owner	Inbound rules count	Outbound rules count	
891377014436	2 Permission entries	1 Permission entry	

Inbound rulesOutbound rulesTags

ec2-user@ip-10-0-0-199:~\$ ping amazon.com

PING amazon.com (52.94.236.248) 56(84) bytes of data.

## Create endpoint [Info](#)

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.

task

#### 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

#### Find services to connect to

An elastic network interface that allow you to connect to resources in a private subnet

#### Find endpoint services

Find services shared with you by service name

### Services (1)

Search

Service Name = com.amazonaws.us-east-1.sns

Clear filters

< 1 >

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

### VPC

Select the VPC in which to create the endpoint

#### VPC

The VPC in which to create your endpoint.

vpc-0987eba7ebe1bf9cb (VPCE-Tutorial-VPC)

#### Additional settings

##### DNS name

☒ Enable DNS name [Info](#)

Associates a private hosted zone with the VPC that contains a record set that enables you to leverage Amazon's private network connectivity to the service while making requests to the service's default public endpoint DNS name. To use this feature, ensure that the attributes 'Enable DNS hostnames' and 'Enable DNS support' are enabled for your VPC.

##### DNS record IP type

☒ IPv4

☐ IPv6

☐ Dualstack

☐ Service defined



Dualstack

Service defined

Subnets ( 1/6) Info

<input checked="" type="checkbox"/>	Availability Zone ▾	Subnet ID ▾	Designate IP addresses	IPv4 address ▾	IPv6 address ▾
<input checked="" type="checkbox"/>	us-east-1a (use1-az4)	subnet-0b0bf8768...	<input type="checkbox"/>		
<input type="checkbox"/>	us-east-1b (use1-az6)	<div>No subnet available</div>	<input type="checkbox"/>		
<input type="checkbox"/>	us-east-1c (use1-az1)	<div>No subnet available</div>	<input type="checkbox"/>		
<input type="checkbox"/>	us-east-1d (use1-az2)	<div>No subnet available</div>	<input type="checkbox"/>		
<input type="checkbox"/>	us-east-1e (use1-az3)	<div>No subnet available</div>	<input type="checkbox"/>		
<input type="checkbox"/>	us-east-1f (use1-az5)	<div>No subnet available</div>	<input type="checkbox"/>		

IP address type

☒ IPv4

☐ IPv6

☐ Dualstack

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

IP address type

☒ IPv4

☐ IPv6

☐ Dualstack

Security groups (1/2) Info

Search

< 1 > ⚙

<input type="checkbox"/>	Group ID ▾	Group name ▾	VPC ID ▾	Description
<input type="checkbox"/>	sg-01a511750da82821d	default	vpc-0987eba7ebe1bf9cb	default VPC security group
<input checked="" type="checkbox"/>	sg-03ffaab71bb4c92e1	Tutorial Security Group	vpc-0987eba7ebe1bf9cb	Security group for SNS VPC endp

sg-03ffaab71bb4c92e1 X

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 account to any resources in this Amazon Web Services account. All policies — IAM user policies, VPC

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

JSON Line 1, Column 1 ⚙ Errors: 0 ⚠ Warnings: 0

Code blocks in square or curly brackets can be expanded and collapsed with CTRL+Enter or Command+Enter.

Tags

Key

Q Name X

Q task X

Remove

Add new tag

You can add 49 more tags.

Value - optional

CancelCreate endpoint

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

VPC dashboard

EC2 Global View

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

Successfully created VPC endpoint

vpce-002e59a913e9d8fd3

Endpoints (1/1)

task

vpce-002e59a913e9d8fd3

vpce-0987eba7ebe1bf9cb | VPCE-Tutori...

com.amazonaws.us-east-1

Update in progress

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

vpce-002e59a913e9d8fd3 / task

Details

Subnets

Security Groups

Notification

Policy

Monitoring

Tags

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

Amazon SNS

Subscriptions

Create subscription

Create subscription

Details

Topic ARN

arn:aws:sns:us-east-1:891377014436:VPCE-Tutorial-Topic

Protocol

The type of endpoint to subscribe

Email

Endpoint

An email address that can receive notifications from Amazon SNS.

naveenrajasekaran2000@gmail.com

After your subscription is created, you must confirm it.

Subscription filter policy - optional

This policy filters the messages that a subscriber receives.

Redrive policy (dead-letter queue) - optional

Send undeliverable messages to a dead-letter queue.

Cancel

Create subscription

AWS Notification - Subscription Confirmation Inbox x



**VPCE-Tutorial-Topic** <no-reply@sns.amazonaws.com>  
to me ▾

6:17 PM (0 minutes ago) ☆ 😊 ↩ ⋮

You have chosen to subscribe to the topic:  
**arn:aws:sns:us-east-1:891377014436:VPCE-Tutorial-Topic**

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):  
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

↩ Reply   ↪ Forward   😊

Amazon SNS

Dashboard

Topics

Subscriptions

▼ Mobile

Push notifications

Text messaging (SMS)

Origination numbers

Amazon SNS > Topics > VPCE-Tutorial-Topic > Subscription: f8eb1fa1-bb80-41f0-bf40-a0b3f12fbaa6

Subscription: f8eb1fa1-bb80-41f0-bf40-a0b3f12fbaa6

EditDelete

Details

ARN

arn:aws:sns:us-east-1:891377014436:VPCE-Tutorial-Topic:f8eb1fa1-bb80-41f0-bf40-a0b3f12fbaa6

Status

Confirmed

Endpoint

naveenrajasekaran2000@gmail.com

Protocol

EMAIL

Topic

VPCE-Tutorial-Topic

Subscription Principal

arn:aws:iam::891377014436:root

CloudShellFeedback

© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

```
[ec2-user@ip-10-0-0-199 ~]$ aws sns publish --region us-east-1 --topic-arn arn:aws:sns:us-east-1:891377014436:VPCE-Tutorial-Topic --message "we are executing project-3"
```

```
[ec2-user@ip-10-0-0-199 ~]$ aws sns publish --region us-east-1 --topic-arn arn:aws:sns:us-east-1:891377014436:VPCE-Tutorial-Topic --message "we are executing project-3"
{
  "MessageId": "f5042331-9ec7-51c4-a7ed-7da4481e2d82"
}
[ec2-user@ip-10-0-0-199 ~]$
```

1 of 3,342

## AWS Notification Message Inbox x



**VPCE-Tutorial-Topic** <no-reply@sns.amazonaws.com>

6:35 PM (5 minutes ago)



to me ▾

we are executing project-3

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:

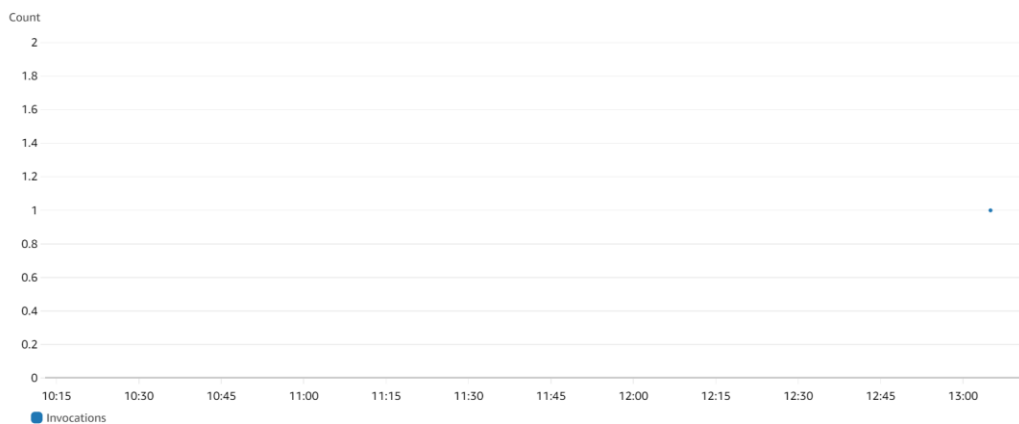
<https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:891377014436:VPCE-Tutorial-Topic:f8eb1fa1-bb80-41f0-bf40-a0b3f12fbaa6&Endpoint=naveenrajasekaran2000@gmail.com>

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at

<https://aws.amazon.com/support>

Reply

Forward



[View in metrics](#)

[Close](#)

CloudWatch

Favorites and revents

Dashboards

Alarms

Logs

Log groups

Log Anomalies

Live Tail

Logs Insights

Metrics

X-Ray traces

Events

Application Signals

Log events

Filter events - press enter to search

1m1h

Local timezone

Display

Timestamp

Message

No older events at this moment. [Retry](#)

▶

2024-04-14T18:35:29.290+05:30

INIT\_START Runtime Version: python:3.9.v50 Runtime Version ARN: arn:aws:lambda:us-eas...

▶

2024-04-14T18:35:29.363+05:30

Loading function

▶

2024-04-14T18:35:29.366+05:30

START RequestId: 9e82c7d6-9fb8-4fbd-88b1-2b9ba92a0576 Version: \$LATEST

▶

2024-04-14T18:35:29.366+05:30

From SNS: we are executing project-3

▶

2024-04-14T18:35:29.367+05:30

END RequestId: 9e82c7d6-9fb8-4fbd-88b1-2b9ba92a0576

▶

2024-04-14T18:35:29.367+05:30

REPORT RequestId: 9e82c7d6-9fb8-4fbd-88b1-2b9ba92a0576 Duration: 1.58 ms Billed Durat...

No newer events at this moment. [Auto retry paused. Resume](#)

Back to top