**Publishing Amazon SNS Messages Privately**

**Project 3:**

**Problem Statement**: How to secure patient records online and send them 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 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.

**Steps to Solve:**

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

**Solution:**

1. Create AWS resources using Cloud Formation template. In this case, the template has been downloaded from GitHub site. The stack for this tutorial includes the following resources:

● A VPC and the associated networking resources, including a subnet, a security group, an internet gateway, and a route table.

● An Amazon EC2 instance that's launched into the subnet in the VPC.

● An Amazon SNS topic.

● Two AWS Lambda functions. These functions receive messages that are published to the Amazon SNS topic, and they log events in CloudWatch Logs.

● Amazon CloudWatch metrics and logs.

● An IAM role that allows the Amazon EC2 instance to use Amazon SNS, and an IAM role that allows the Lambda functions to write to CloudWatch

1. Create a KeyPair in EC2 console as below.

A screenshot of a computer

Description automatically generated

1. Go to AWS Cloud Formation and create stack.
2. On the Select Template page, choose Upload a template to Amazon S3 and select the file.
3. Keep other options as default and click Submit after reviewing.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Confirm that your Amazon EC2 instance lacks internet access. Verify this by logging into the instance. Open putty and enter Public IP of EC2 instance. Also, convert pem file to ppk using puttygen and then load the ppk file in SSH -> Authentication option. Once done, login as ec2-user. Now attempt to connect to any public endpoint such as amazon.com.

A screenshot of a computer screen

Description automatically generated

1. To verify that the instance lacks internet connectivity to Amazon SNS. Open Amazon SNS console and create a Topic. Once created, copy the ARN to publish a sample message. The publish attempt would fail.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A black background with colorful stripes

Description automatically generated

1. Create an Amazon VPC Endpoint for Amazon SNS. To connect the VPC to Amazon SNS, you define an interface VPC endpoint. After you add the endpoint, you can log in to the Amazon EC2 instance in your VPC, and from there you can use the Amazon SNS API. You can publish messages to the topic, and the messages are published privately. They stay within the AWS network, and they don't travel the public internet. Note that the instance still lacks access to other AWS services and endpoints on the internet.
2. Open the Amazon VPC console and choose Endpoints. Create an endpoint as below.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

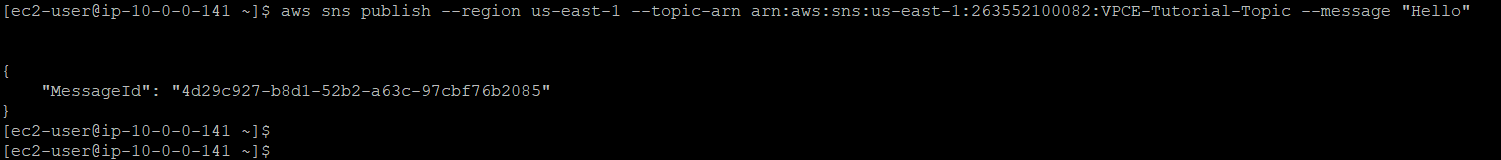
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Once the endpoint becomes available, publish a message to your Amazon SNS topic. Run the same command to publish a message to SNS.



1. Verify your message deliveries. When the Amazon SNS topic receives a message, it fans out the message by sending it to the two subscribing Lambda functions. When these functions receive the message, they log the event to CloudWatch logs. To verify that your message delivery succeeded, check that the functions were invoked, and check that the CloudWatch logs were updated.
2. To verify that the Lambda functions were invoked, open the AWS Lambda console and choose Functions.

A screenshot of a computer

Description automatically generated

1. Choose Lambda1 and select Monitoring. Check the Invocation count graph. This graph shows the number of times the Lambda function has been run. The invocation count matches the number of times you published a message to the topic.

A screenshot of a computer

Description automatically generated

1. To verify that the CloudWatch logs were updated, open the CloudWatch console and choose Logs.

A screenshot of a computer

Description automatically generated

1. Check the logs that were written by the Lambda functions. Choose the log group and log stream.

A screenshot of a computer

Description automatically generated

1. Check that the log includes the entry From SNS: Hello

A screenshot of a computer

Description automatically generated

1. Do the same for another log group.

A screenshot of a computer

Description automatically generated

1. By adding an endpoint for Amazon SNS to a VPC, we were able to publish a message to a topic from within the network that's managed by the VPC. The message was published privately without being exposed to the public internet.