AWS – Secrets Manager

-Hands-on guide.

Mr. Subramanyam Tirumani Vemala

https://www.linkedin.com/in/subbulinkedin/

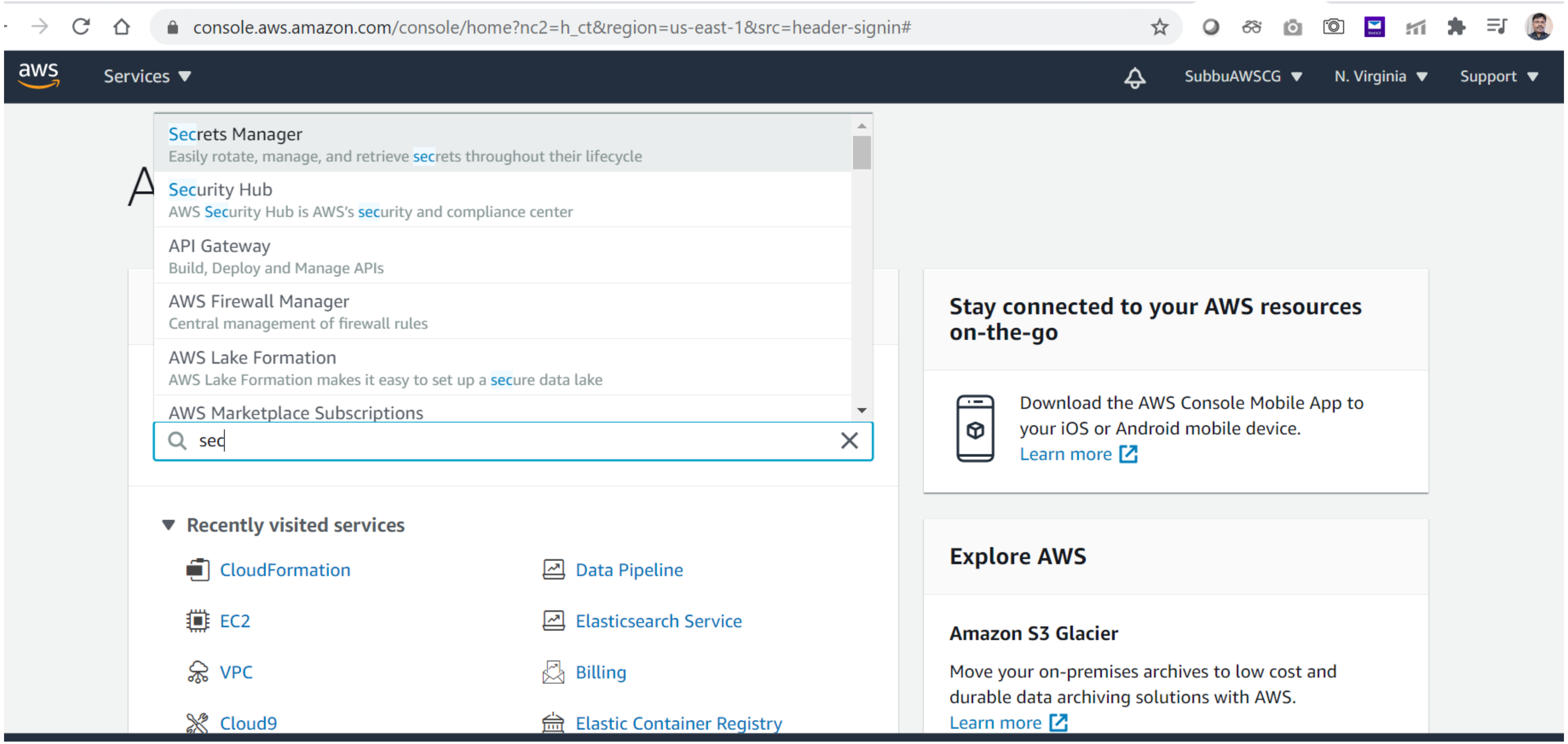
About AWS Secrets Manager:

- AWS Secrets Manager helps you to securely encrypt, store, and retrieve credentials for your databases and other services.
- Instead of hardcoding credentials in your apps, you can make calls to Secrets Manager to retrieve your credentials whenever needed.
- Secrets Manager helps you protect access to your IT resources and data by enabling you to rotate and manage access to your secrets.
- It is always a best practice to use the Secrets Manager, rather than hard coding or configuring in the code.

Pre-requisites:

1. AWS account.
2. AWS CLI.

Login to your AWS account – search for Secrets Manager:



console.aws.amazon.com/console/home?nc2=h_ct&region=us-east-1&src=header-signin#

Secrets Manager
Easily rotate, manage, and retrieve secrets throughout their lifecycle

Security Hub
AWS Security Hub is AWS's security and compliance center

API Gateway
Build, Deploy and Manage APIs

AWS Firewall Manager
Central management of firewall rules

AWS Lake Formation
AWS Lake Formation makes it easy to set up a secure data lake

AWS Marketplace Subscriptions

sec

▼ Recently visited services

Stay connected to your AWS resources on-the-go

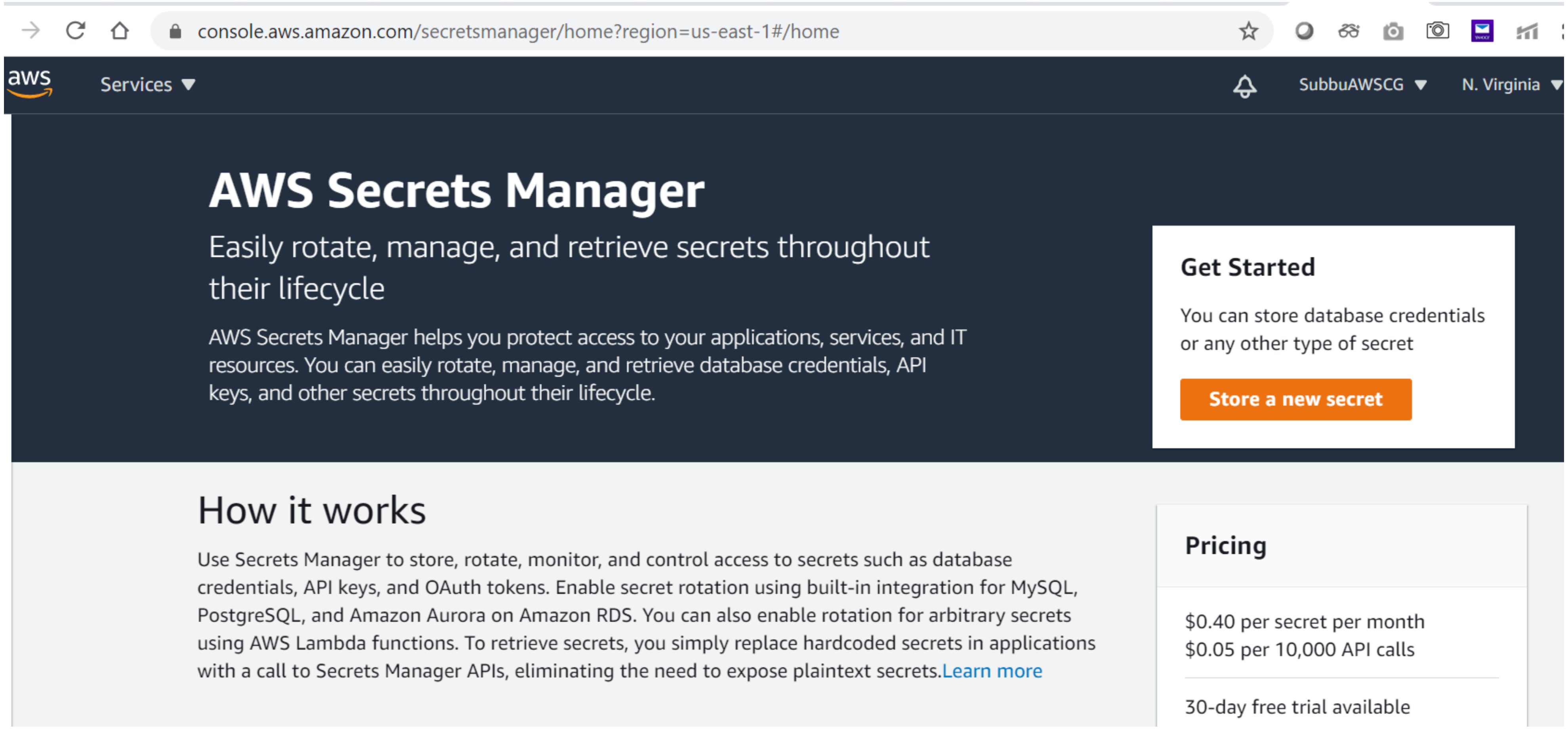
Download the AWS Console Mobile App to your iOS or Android mobile device.
Learn more

Explore AWS

Amazon S3 Glacier

Move your on-premises archives to low cost and durable data archiving solutions with AWS.
Learn more

Click on Store a new Secret:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/home
aws
Services ▼
SubbuAWSCG ▼
N. Virginia ▼

AWS Secrets Manager

Easily rotate, manage, and retrieve secrets throughout their lifecycle

AWS Secrets Manager helps you protect access to your applications, services, and IT resources. You can easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

Get Started

You can store database credentials or any other type of secret

How it works

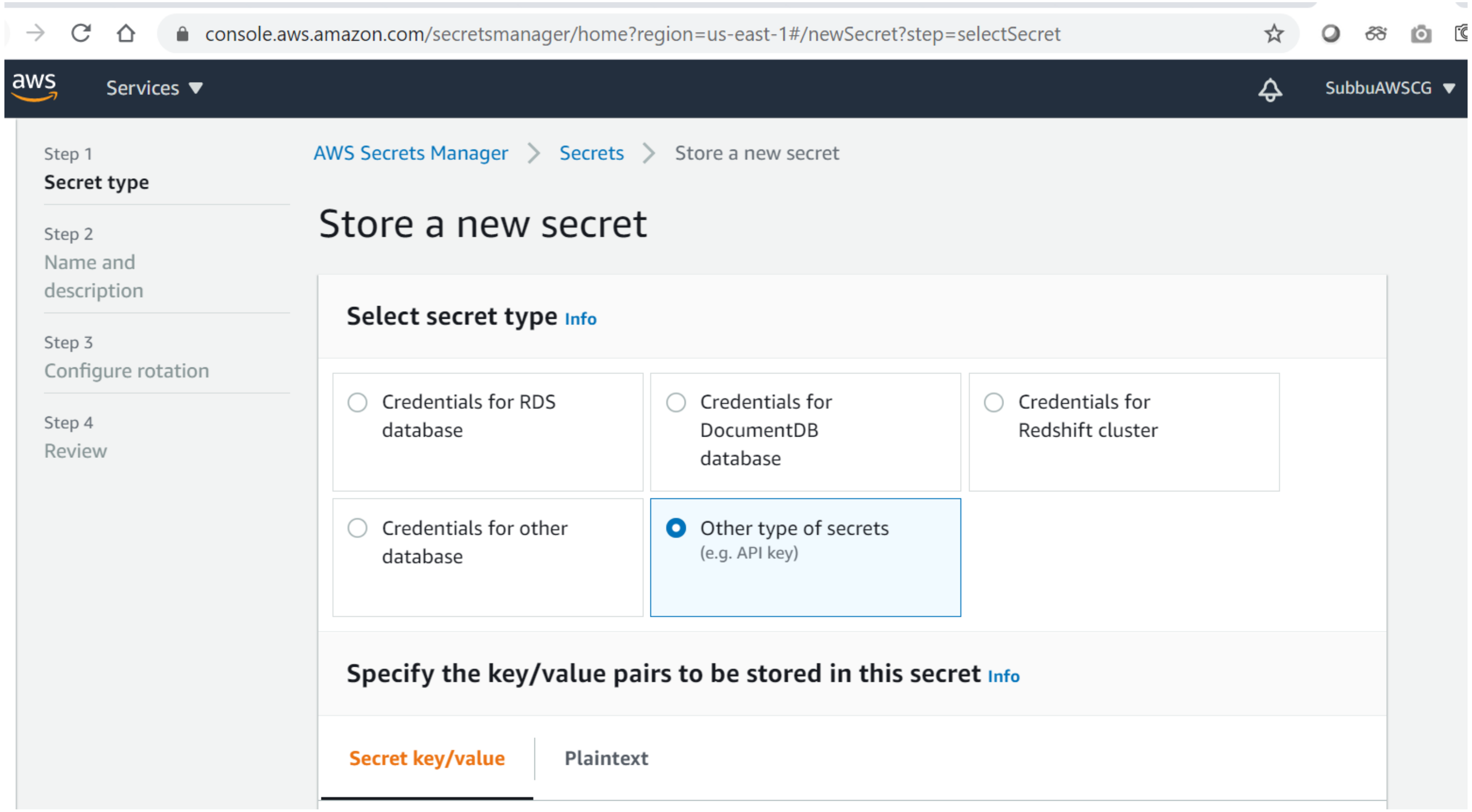
Use Secrets Manager to store, rotate, monitor, and control access to secrets such as database credentials, API keys, and OAuth tokens. Enable secret rotation using built-in integration for MySQL, PostgreSQL, and Amazon Aurora on Amazon RDS. You can also enable rotation for arbitrary secrets using AWS Lambda functions. To retrieve secrets, you simply replace hardcoded secrets in applications with a call to Secrets Manager APIs, eliminating the need to expose plaintext secrets.Learn more

Pricing

$0.40 per secret per month
$0.05 per 10,000 API calls

30-day free trial available

Choose the type of secret you want to create:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/newSecret?step=selectSecret

Step 1
Secret type

Step 2
Name and description

Step 3
Configure rotation

Step 4
Review

AWS Secrets Manager > Secrets > Store a new secret

Store a new secret

Select secret type Info

○ Credentials for RDS database

○ Credentials for DocumentDB database

○ Credentials for Redshift cluster

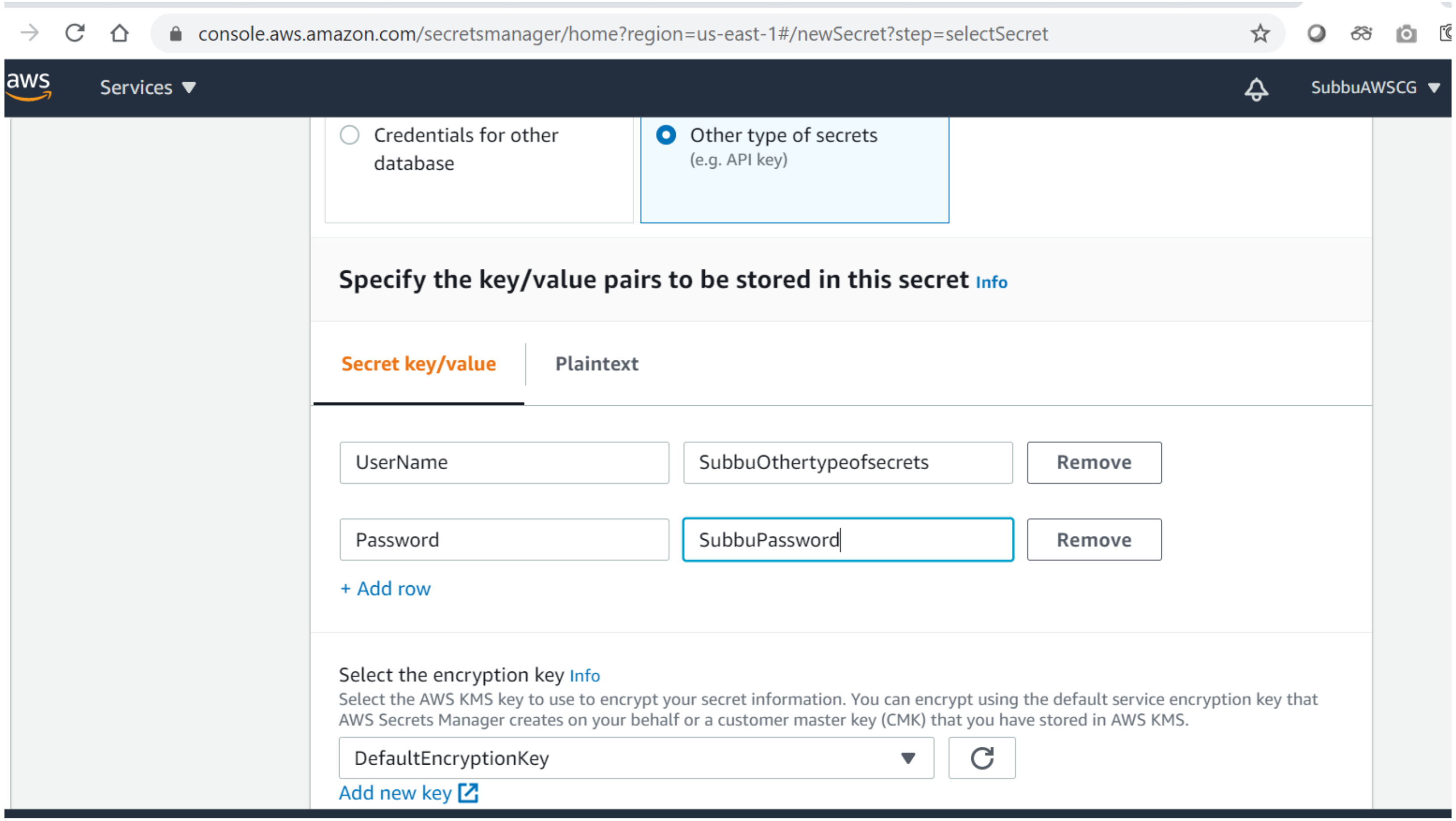
○ Credentials for other database

● Other type of secrets (e.g. API key)

Specify the key/value pairs to be stored in this secret Info

Secret key/value | Plaintext

Create the desired Keys and Values:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/newSecret?step=selectSecret

○ Credentials for other database

● Other type of secrets
(e.g. API key)

Specify the key/value pairs to be stored in this secret Info

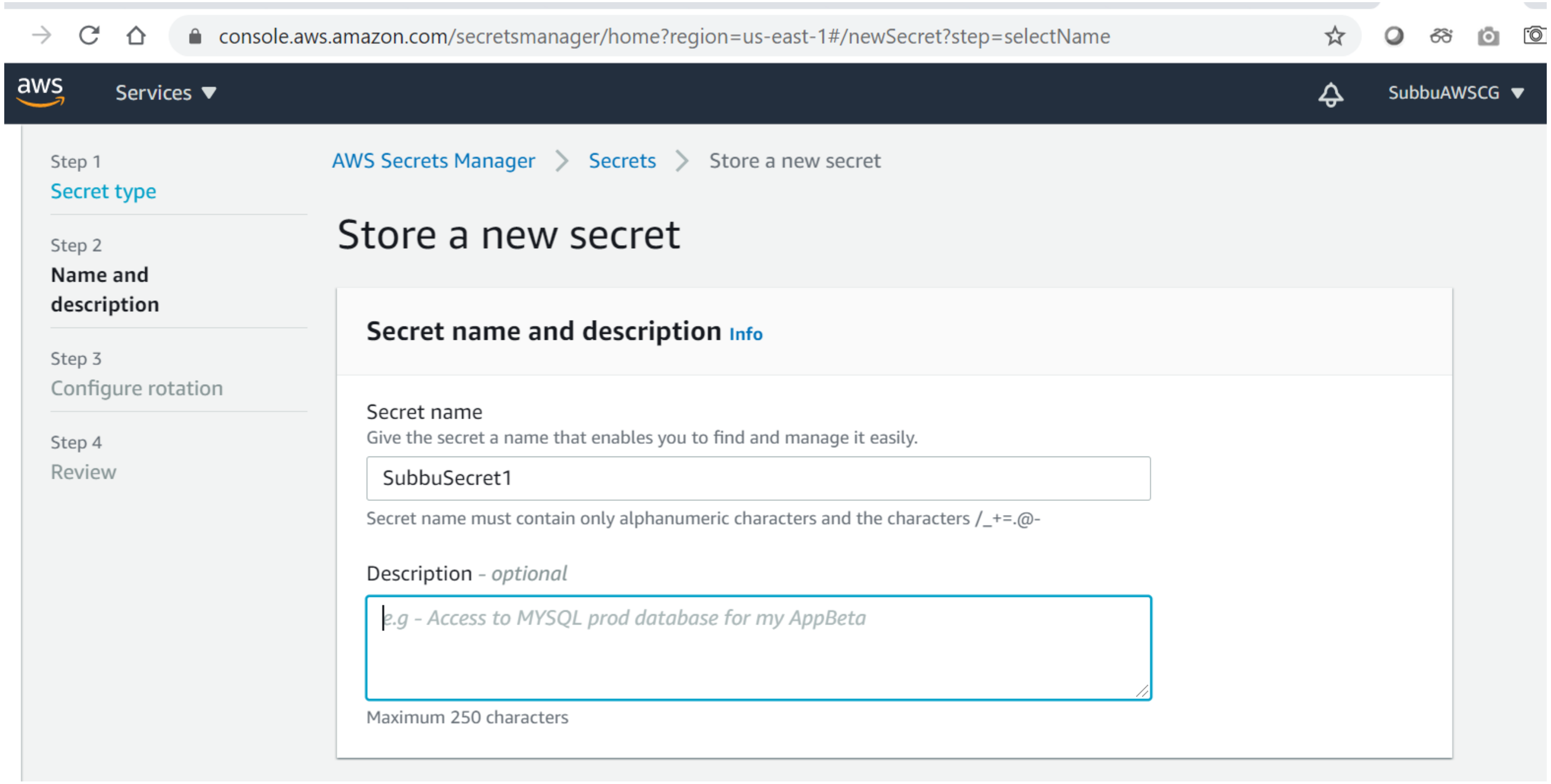
UserName	SubbuOthertypeofsecrets	Remove
Password	SubbuPassword	Remove

Select the encryption key Info

Select the AWS KMS key to use to encrypt your secret information. You can encrypt using the default service encryption key that AWS Secrets Manager creates on your behalf or a customer master key (CMK) that you have stored in AWS KMS.

DefaultEncryptionKey ▼

Name the new Secret:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/newSecret?step=selectName
aws
Services ▼
SubbuAWSCG ▼

Step 1
Secret type

Step 2
Name and description

Step 3
Configure rotation

Step 4
Review

AWS Secrets Manager > Secrets > Store a new secret

Store a new secret

Secret name and description Info

Secret name
Give the secret a name that enables you to find and manage it easily.

SubbuSecret1

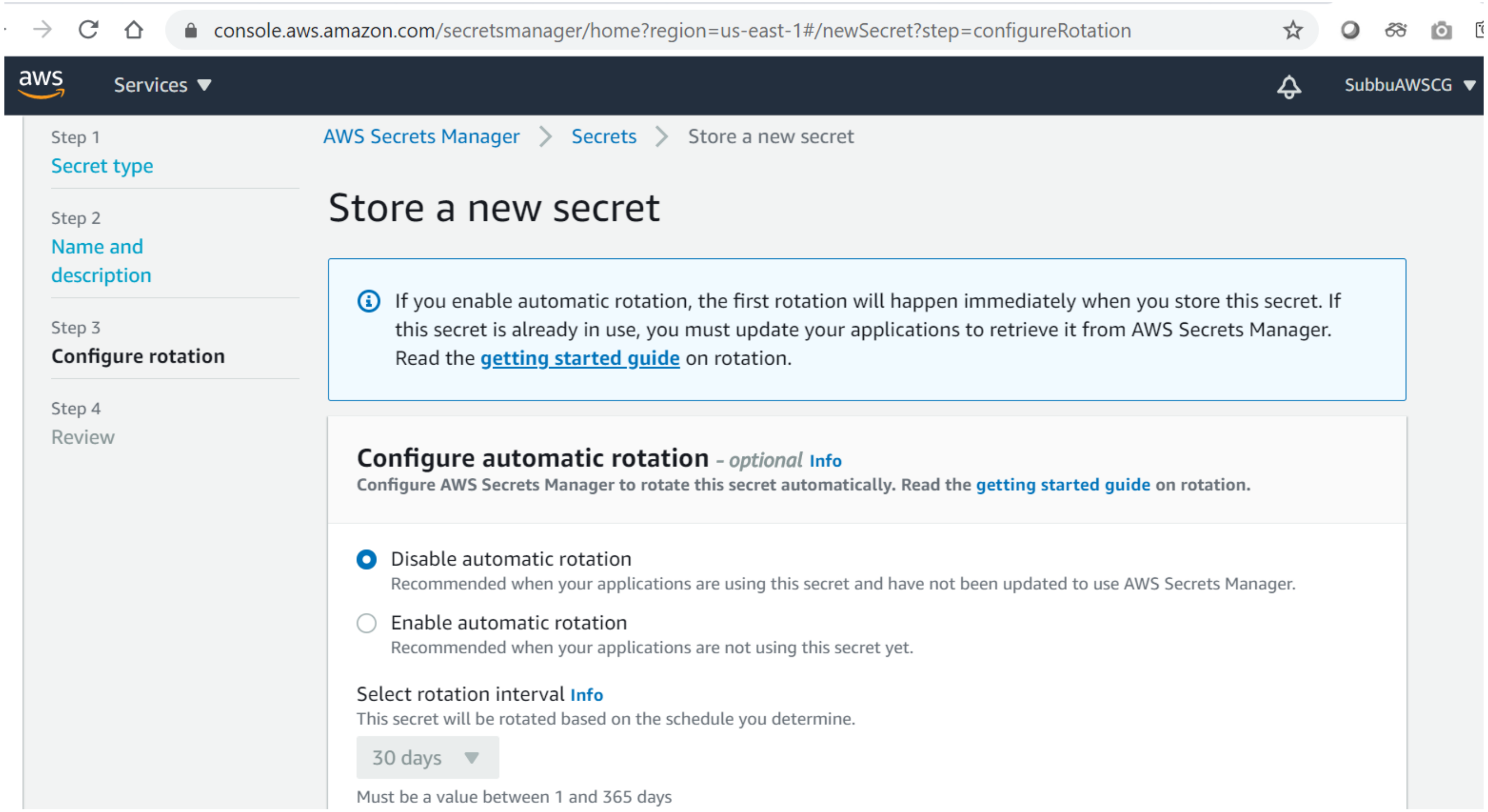
Secret name must contain only alphanumeric characters and the characters /_+=.@-

Description - *optional*

e.g - Access to MYSQL prod database for my AppBeta

Maximum 250 characters

Choose the automatic rotation for more protection if needed:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/newSecret?step=configureRotation
aws
Services ▼
SubbuAWSCG ▼

Step 1
Secret type

Step 2
Name and description

Step 3
Configure rotation

Step 4
Review

AWS Secrets Manager > Secrets > Store a new secret

Store a new secret

If you enable automatic rotation, the first rotation will happen immediately when you store this secret. If this secret is already in use, you must update your applications to retrieve it from AWS Secrets Manager. Read the getting started guide on rotation.

Configure automatic rotation - *optional* Info

Configure AWS Secrets Manager to rotate this secret automatically. Read the getting started guide on rotation.

● Disable automatic rotation
Recommended when your applications are using this secret and have not been updated to use AWS Secrets Manager.

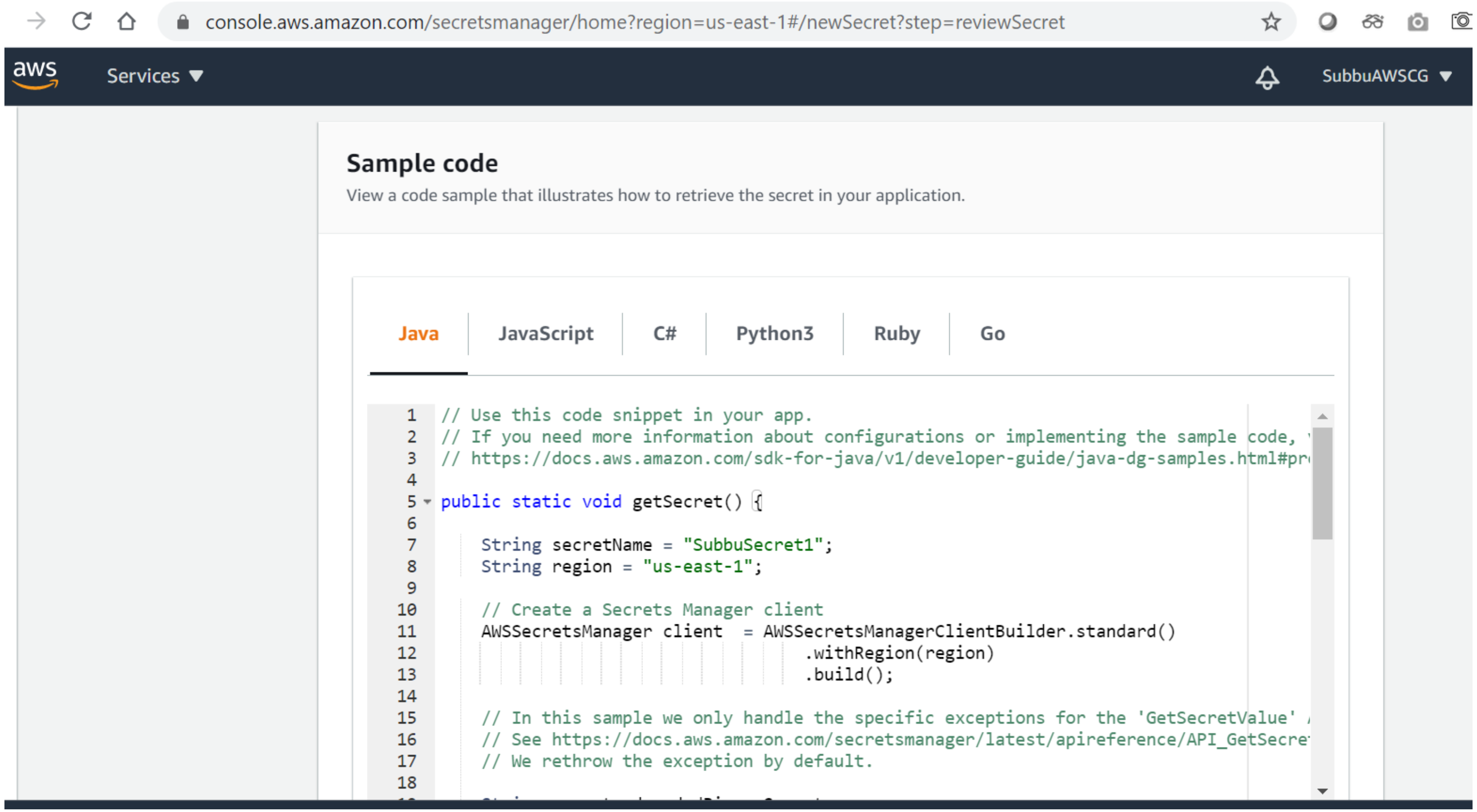
○ Enable automatic rotation
Recommended when your applications are not using this secret yet.

Select rotation interval Info
This secret will be rotated based on the schedule you determine.

30 days ▼

Must be a value between 1 and 365 days

Use the generated code snippet, to have API calls in the code, based on the language:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/newSecret?step=reviewSecret
aws
Services ▼
SubbuAWSCG ▼

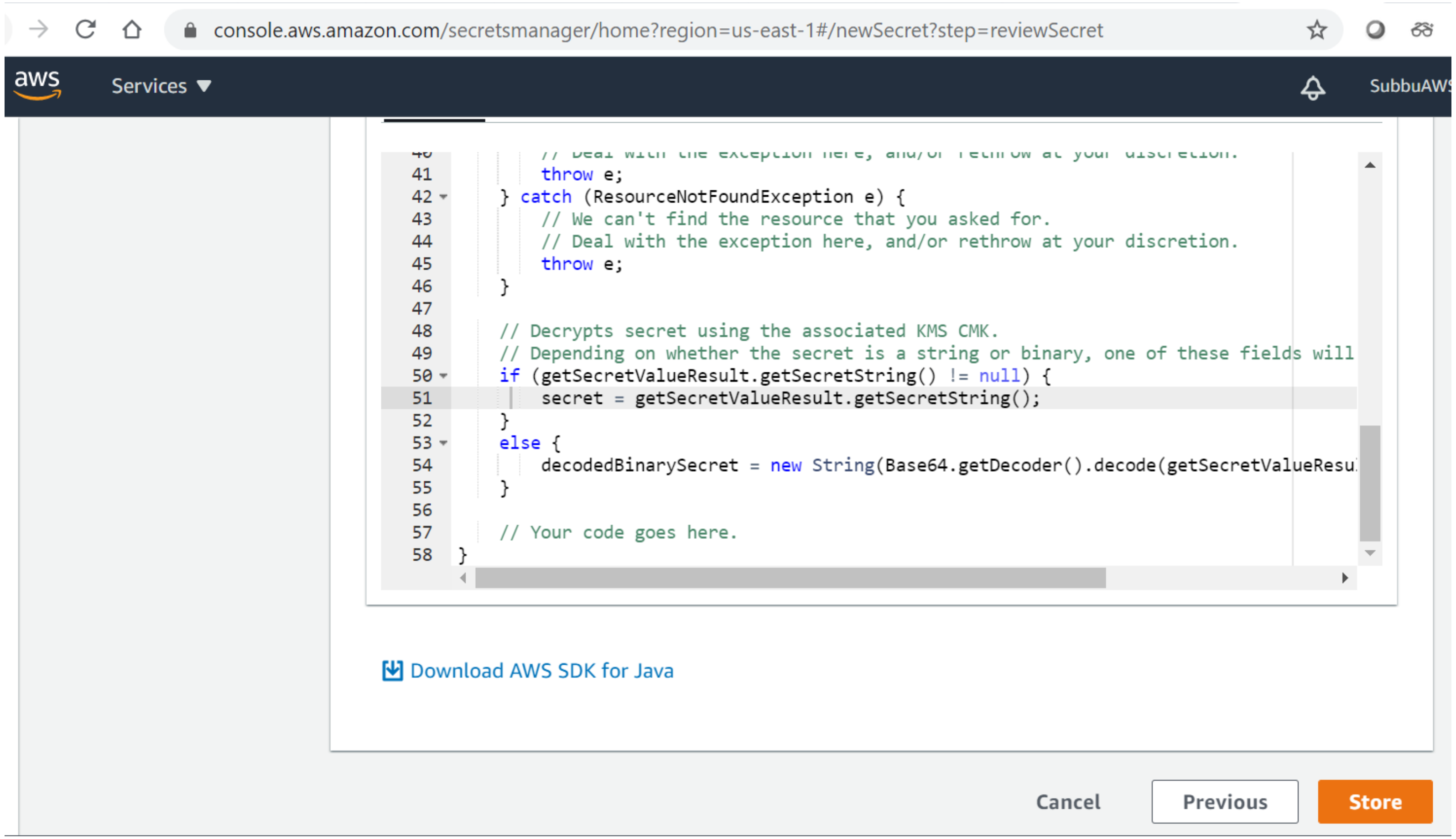
Sample code

View a code sample that illustrates how to retrieve the secret in your application.

Java
JavaScript
C#
Python3
Ruby
Go

```java
// Use this code snippet in your app.
// If you need more information about configurations or implementing the sample code, '
// https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/java-dg-samples.html#pr

public static void getSecret() {

    String secretName = "SubbuSecret1";
    String region = "us-east-1";

    // Create a Secrets Manager client
    AWSSecretsManager client  = AWSSecretsManagerClientBuilder.standard()
                                    .withRegion(region)
                                    .build();

    // In this sample we only handle the specific exceptions for the 'GetSecretValue' /
    // See https://docs.aws.amazon.com/secretsmanager/latest/apireference/API_GetSecre
    // We rethrow the exception by default.

```

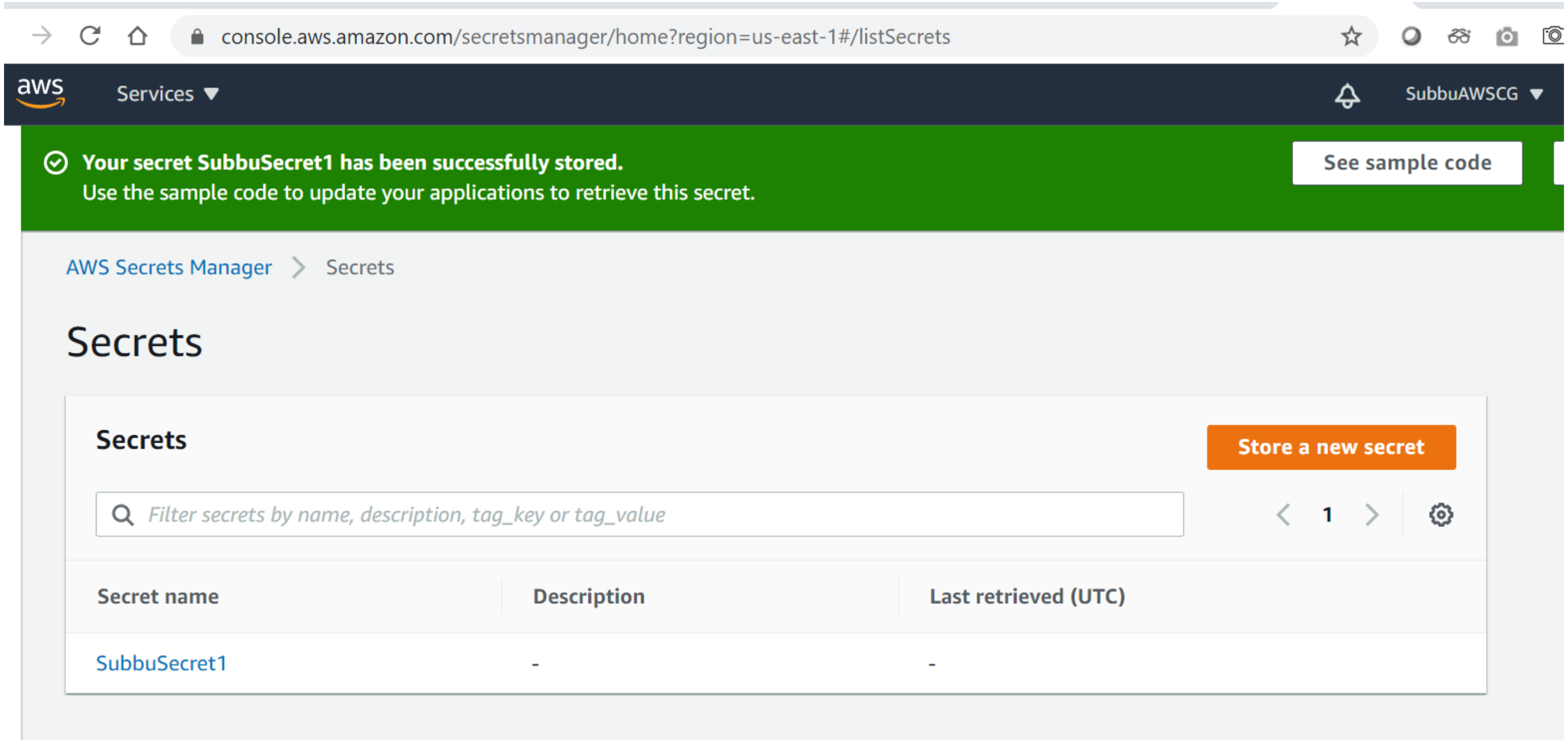
You can add your business logic in that code snippet too:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/newSecret?step=reviewSecret
aws
Services ▼
SubbuAWS
Download AWS SDK for Java
Cancel
Previous
Store

```
        // Deal with the exception here, and/or rethrow at your discretion.
        throw e;
    } catch (ResourceNotFoundException e) {
        // We can't find the resource that you asked for.
        // Deal with the exception here, and/or rethrow at your discretion.
        throw e;
    }

    // Decrypts secret using the associated KMS CMK.
    // Depending on whether the secret is a string or binary, one of these fields will
    if (getSecretValueResult.getSecretString() != null) {
        secret = getSecretValueResult.getSecretString();
    }
    else {
        decodedBinarySecret = new String(Base64.getDecoder().decode(getSecretValueResu
    }

    // Your code goes here.
}
```

Now Secret has been created:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/listSecrets
aws
Services ▼
SubbuAWSCG ▼

Your secret SubbuSecret1 has been successfully stored.
Use the sample code to update your applications to retrieve this secret.

See sample code
AWS Secrets Manager > Secrets

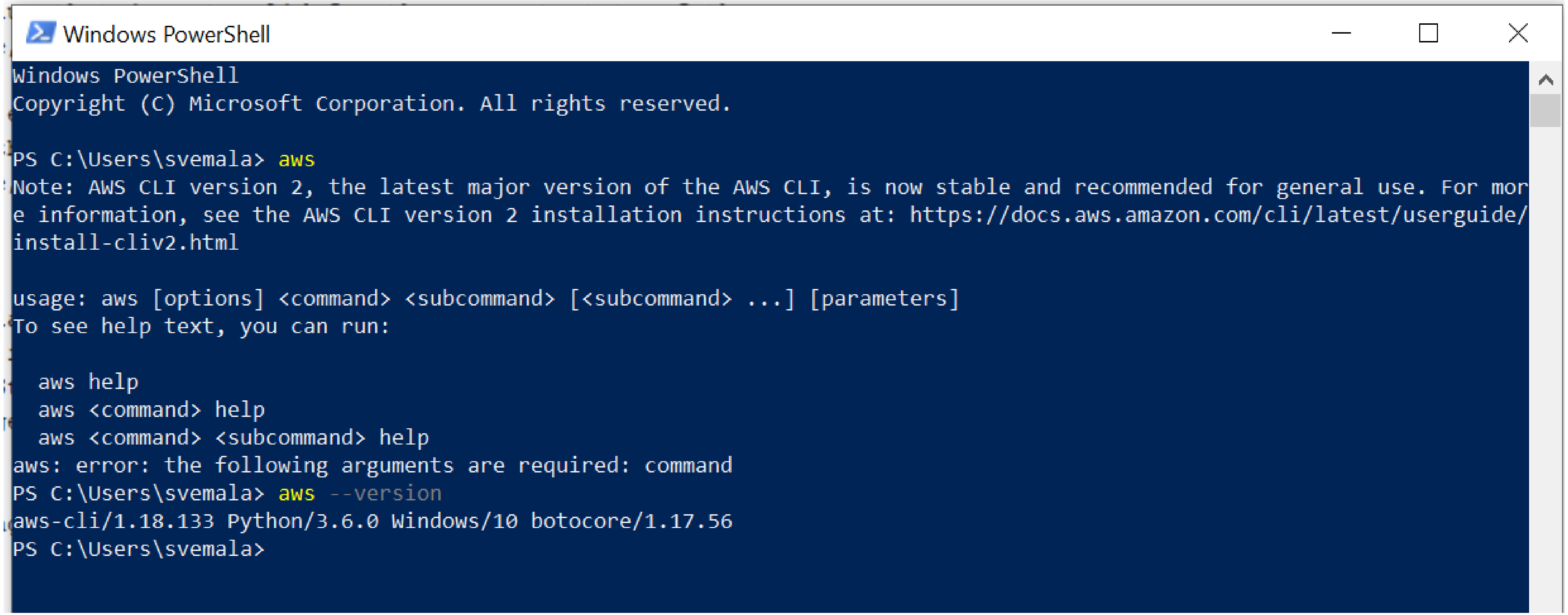
Secrets

Secrets

Store a new secret
Filter secrets by name, description, tag_key or tag_value
1

Secret name	Description	Last retrieved (UTC)
SubbuSecret1	-	-

Install the AWS CLI and check for its existence as below:

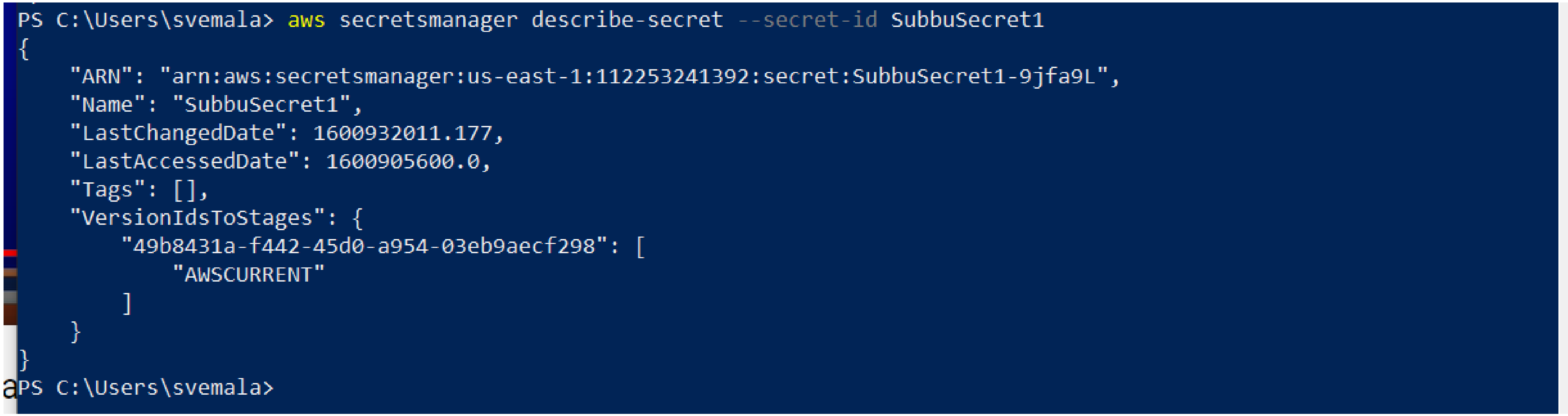


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\svemala> aws
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For mor
e information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/
install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: the following arguments are required: command
PS C:\Users\svemala> aws --version
aws-cli/1.18.133 Python/3.6.0 Windows/10 botocore/1.17.56
PS C:\Users\svemala>
```

Commands used:

```
Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.


PS C:\Users\svemala> aws

Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation
instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html


usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]

To see help text, you can run:


  aws help

  aws <command> help

  aws <command> <subcommand> help

aws: error: the following arguments are required: command

PS C:\Users\svemala> aws --version

aws-cli/1.18.133 Python/3.6.0 Windows/10 botocore/1.17.56

PS C:\Users\svemala>
```

You can view the created secret excluding keys and values:

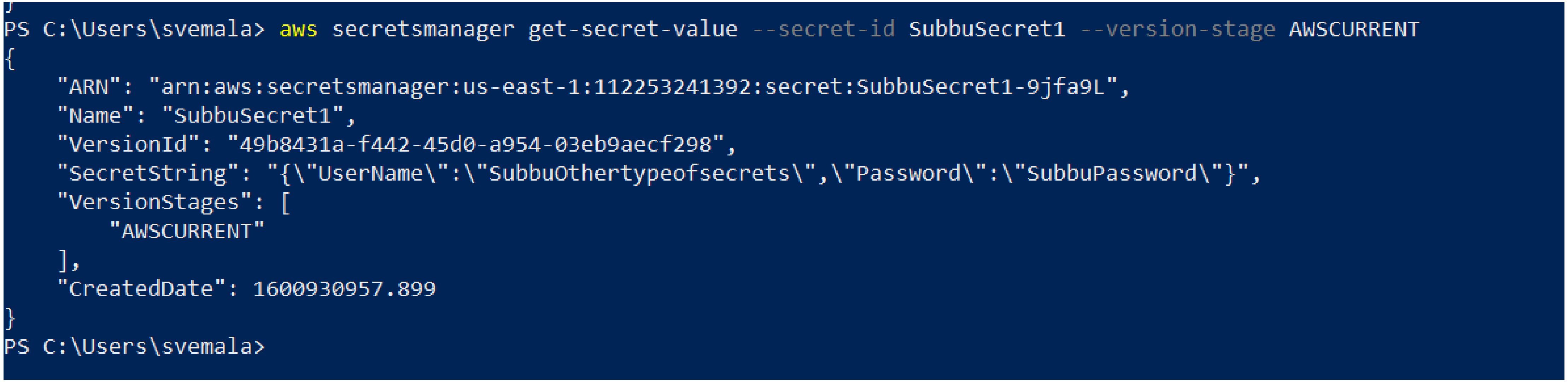


```
PS C:\Users\svemala> aws secretsmanager describe-secret --secret-id SubbuSecret1
{
    "ARN": "arn:aws:secretsmanager:us-east-1:112253241392:secret:SubbuSecret1-9jfa9L",
    "Name": "SubbuSecret1",
    "LastChangedDate": 1600932011.177,
    "LastAccessedDate": 1600905600.0,
    "Tags": [],
    "VersionIdsToStages": {
        "49b8431a-f442-45d0-a954-03eb9aecf298": [
            "AWSCURRENT"
        ]
    }
}
PS C:\Users\svemala>
```

Command used:

```
PS C:\Users\svemala> aws secretsmanager describe-secret --secret-id tutorials/SubbuSecret1

An error occurred (ResourceNotFoundException) when calling the DescribeSecret operation: Secrets Manager can't find the specified secret.
PS C:\Users\svemala> aws secretsmanager describe-secret --secret-id SubbuSecret1
{
    "ARN": "arn:aws:secretsmanager:us-east-1:112253241392:secret:SubbuSecret1-9jfa9L",
    "Name": "SubbuSecret1",
    "LastChangedDate": 1600932011.177,
    "LastAccessedDate": 1600905600.0,
    "Tags": [],
    "VersionIdsToStages": {
        "49b8431a-f442-45d0-a954-03eb9aecf298": [
            "AWSCURRENT"
        ]
    }
}
PS C:\Users\svemala>
```

You can view the created secret including keys and values:

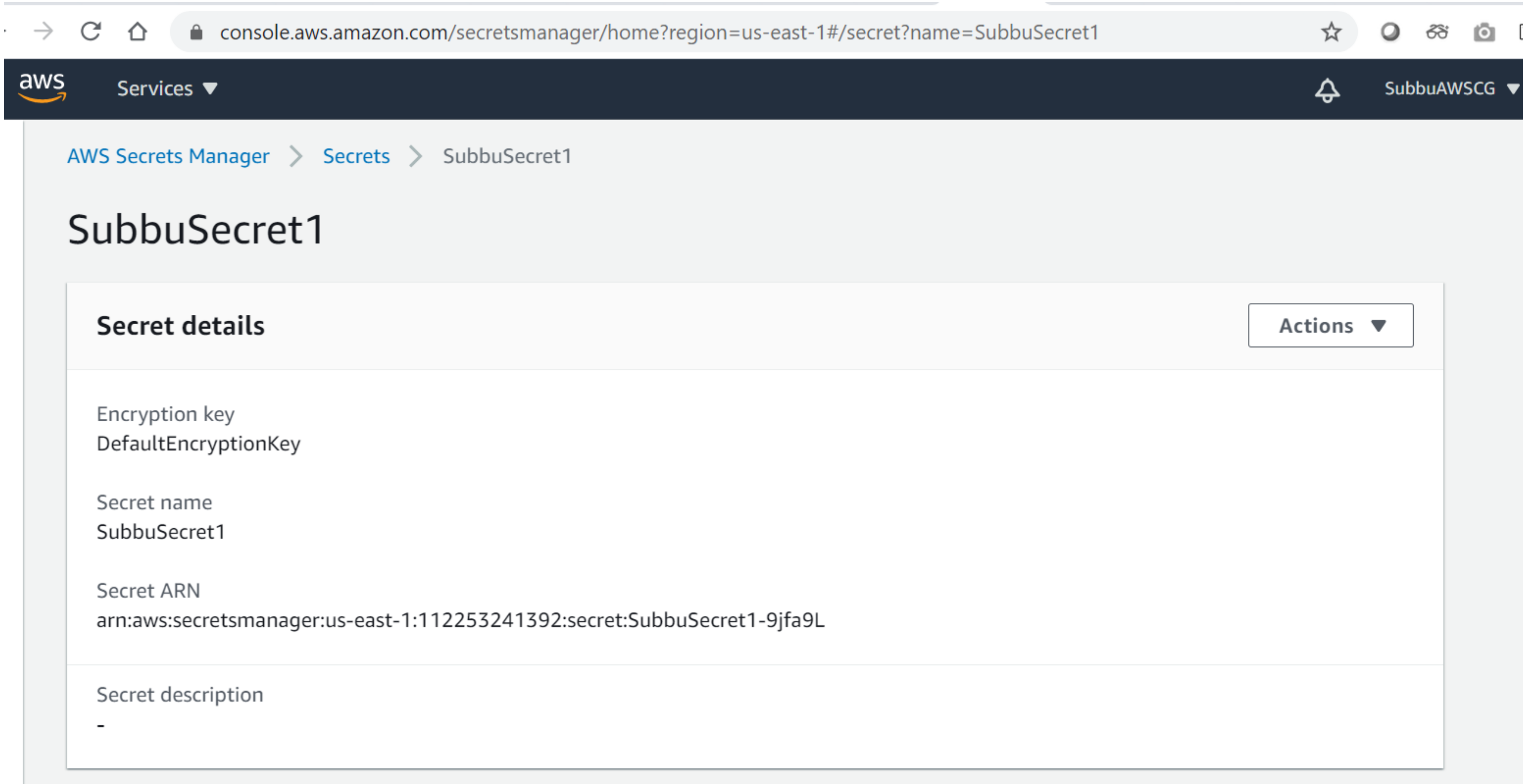


```
PS C:\Users\svemala> aws secretsmanager get-secret-value --secret-id SubbuSecret1 --version-stage AWSCURRENT
{
    "ARN": "arn:aws:secretsmanager:us-east-1:112253241392:secret:SubbuSecret1-9jfa9L",
    "Name": "SubbuSecret1",
    "VersionId": "49b8431a-f442-45d0-a954-03eb9aecf298",
    "SecretString": "{\"UserName\":\"SubbuOthertypeofsecrets\",\"Password\":\"SubbuPassword\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": 1600930957.899
}
PS C:\Users\svemala>
```

Command used:

```
PS C:\Users\svemala> aws secretsmanager get-secret-value --secret-id SubbuSecret1 --version-stage
AWSCURRENT
{
    "ARN": "arn:aws:secretsmanager:us-east-1:112253241392:secret:SubbuSecret1-9jfa9L",
    "Name": "SubbuSecret1",
    "VersionId": "49b8431a-f442-45d0-a954-03eb9aecf298",
    "SecretString": "{\"UserName\":\"SubbuOthertypeofsecrets\",\"Password\":\"SubbuPassword\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": 1600930957.899
}
PS C:\Users\svemala>
```

You can view the Secrets list:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/secret?name=SubbuSecret1

AWS Secrets Manager > Secrets > SubbuSecret1

SubbuSecret1

Secret details

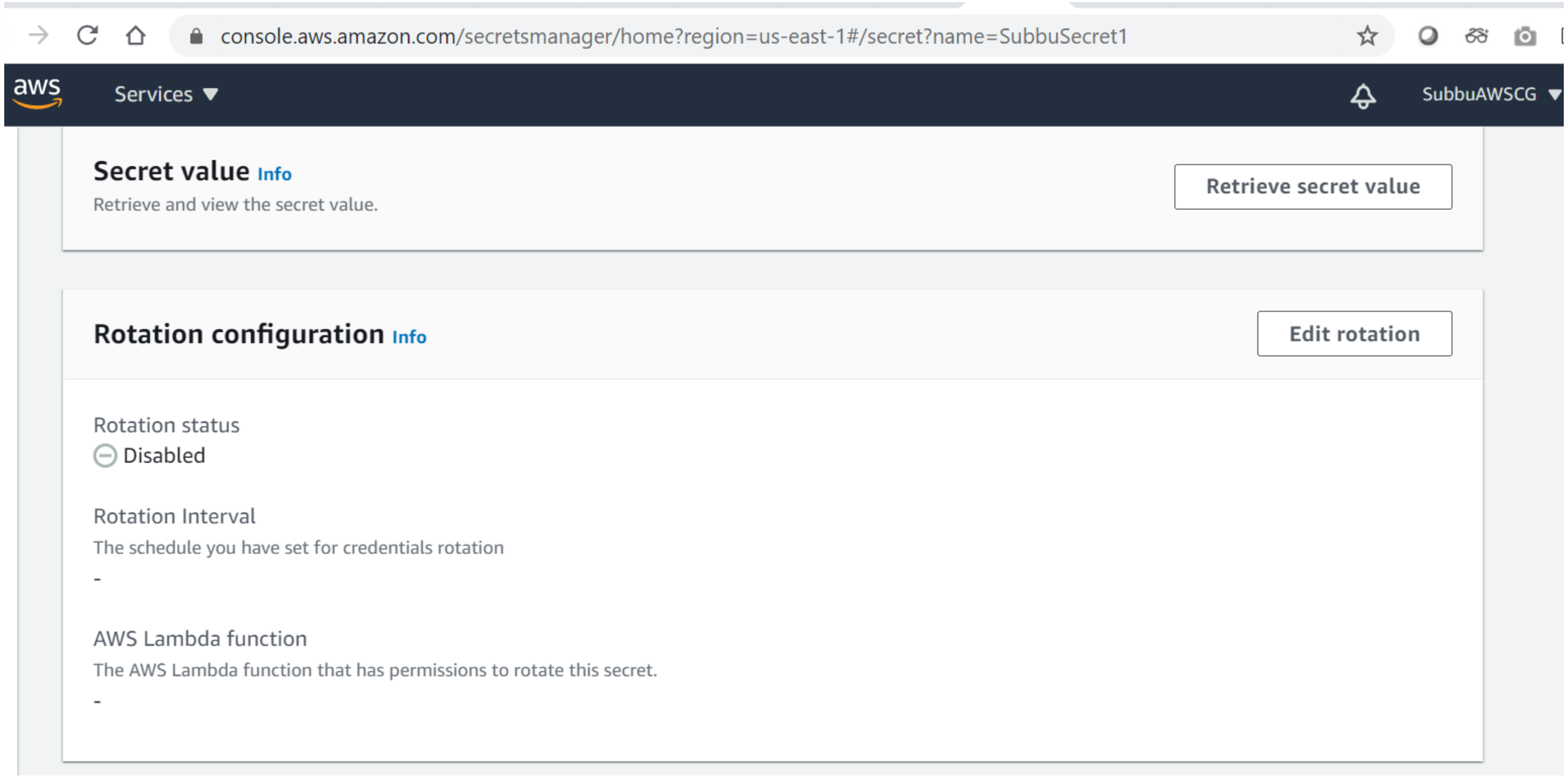
Encryption key
DefaultEncryptionKey

Secret name
SubbuSecret1

Secret ARN
arn:aws:secretsmanager:us-east-1:112253241392:secret:SubbuSecret1-9jfa9L

Secret description
-

Retrieve the created Secrets values:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/secret?name=SubbuSecret1
aws
Services ▼
SubbuAWSCG ▼

Secret value Info

Retrieve and view the secret value.

Retrieve secret value

Rotation configuration Info

Edit rotation

Rotation status

Disabled

Rotation Interval

The schedule you have set for credentials rotation

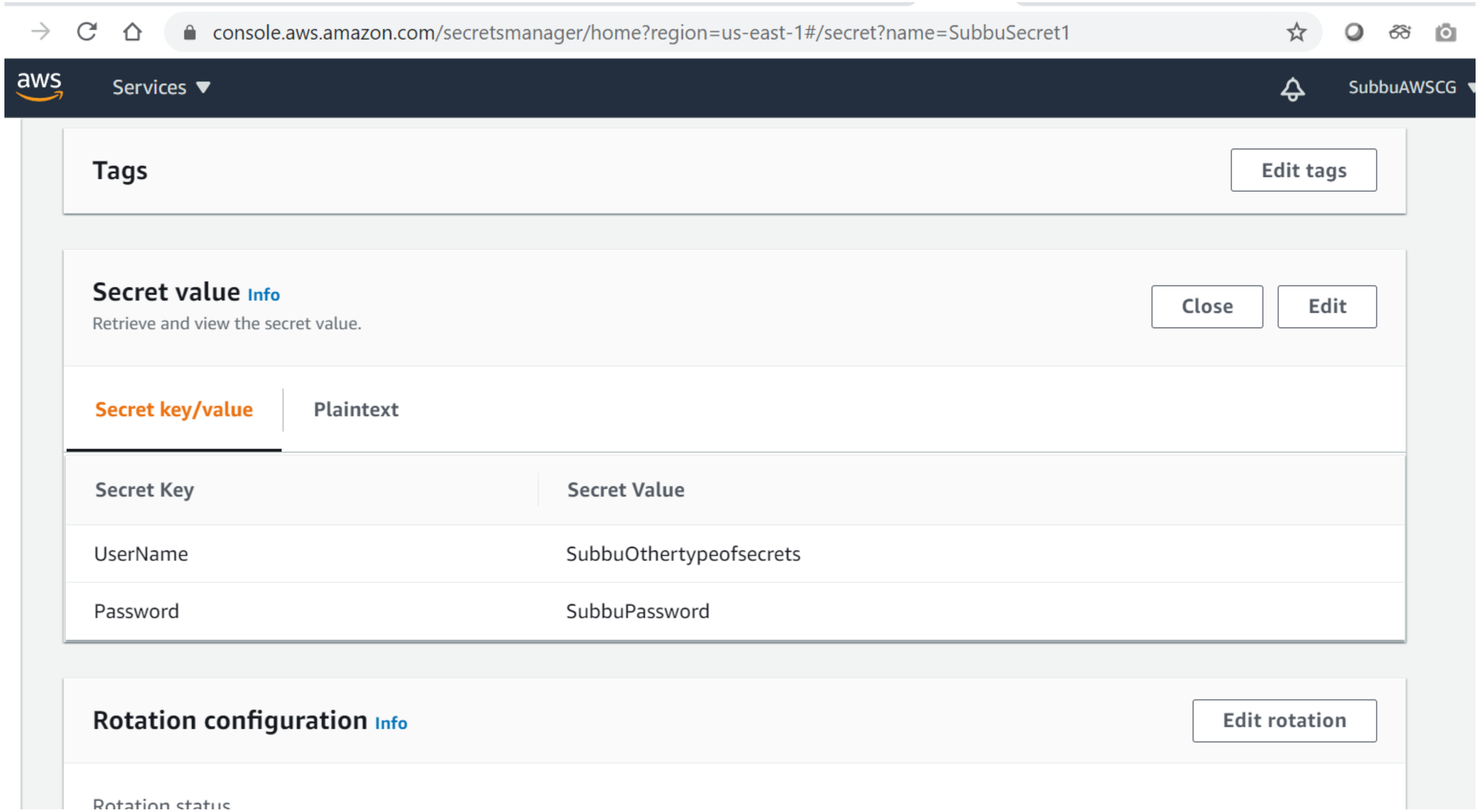
-

AWS Lambda function

The AWS Lambda function that has permissions to rotate this secret.

-

View of Secrets values:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/secret?name=SubbuSecret1
aws
Services ▼
SubbuAWSCG
Tags
Edit tags
Close
Edit
Edit rotation

Secret value Info

Retrieve and view the secret value.

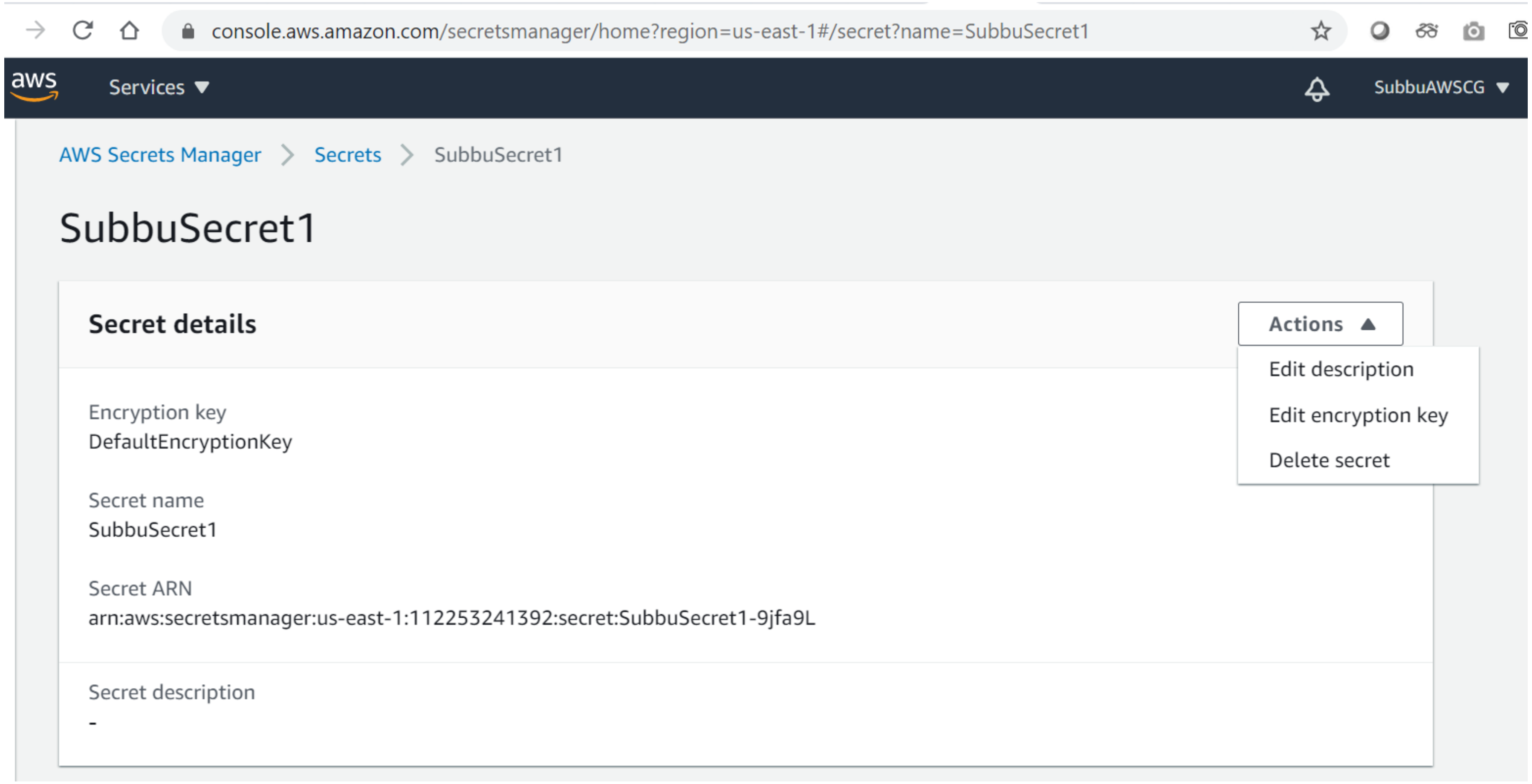
Secret key/value | Plaintext

Secret Key	Secret Value
UserName	SubbuOthertypeofsecrets
Password	SubbuPassword

Rotation configuration Info

Rotation status

Delete the Secrets if no more needed:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/secret?name=SubbuSecret1
aws
Services ▼
SubbuAWSCG ▼
AWS Secrets Manager > Secrets > SubbuSecret1

SubbuSecret1

Secret details

Actions ▲
Edit description
Edit encryption key
Delete secret

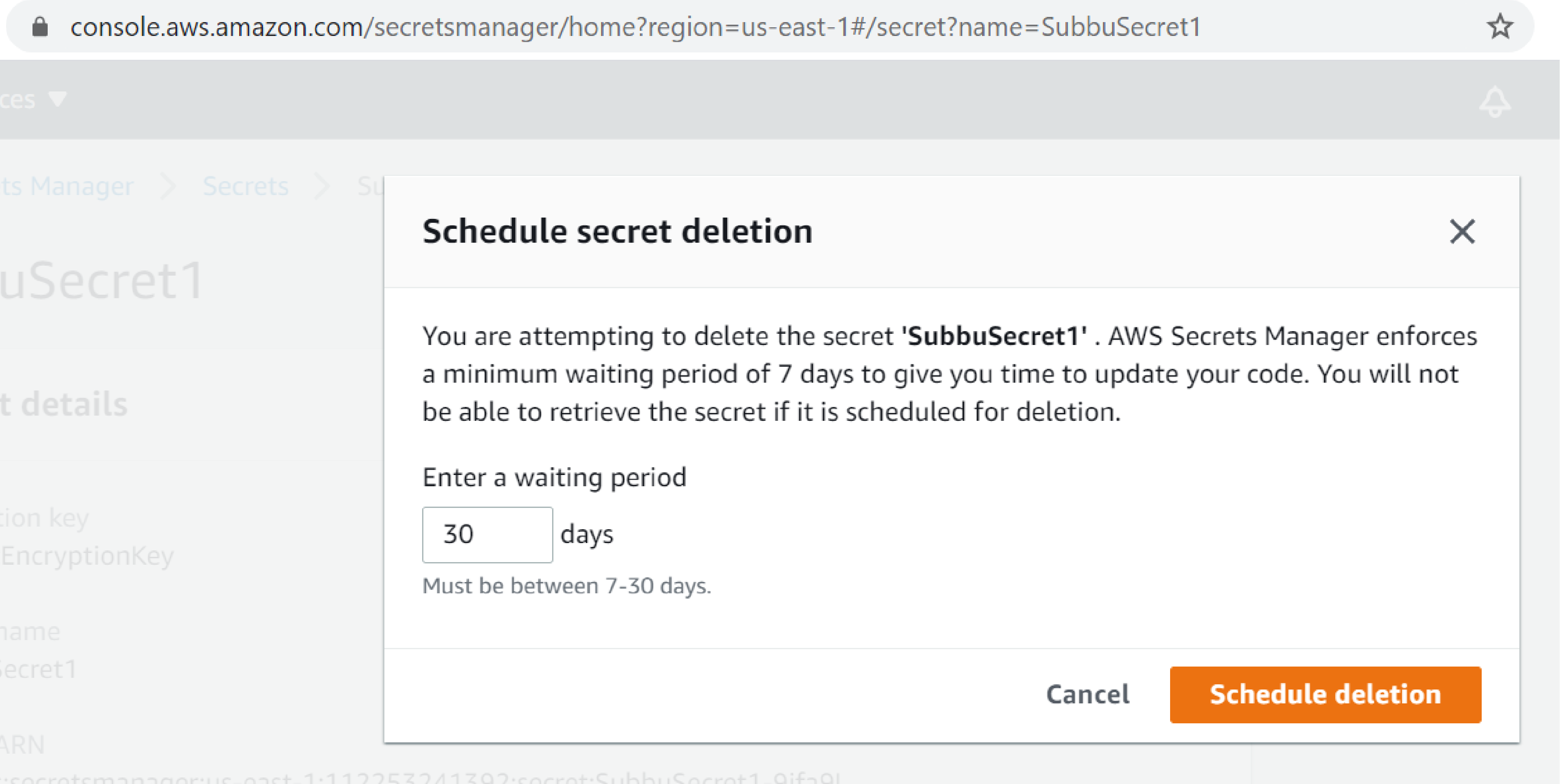
Encryption key
DefaultEncryptionKey

Secret name
SubbuSecret1

Secret ARN
arn:aws:secretsmanager:us-east-1:112253241392:secret:SubbuSecret1-9jfa9L

Secret description
-

Instantly we cannot delete, needs minimum of 7 to 30 days of waiting:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/secret?name=SubbuSecret1

Schedule secret deletion

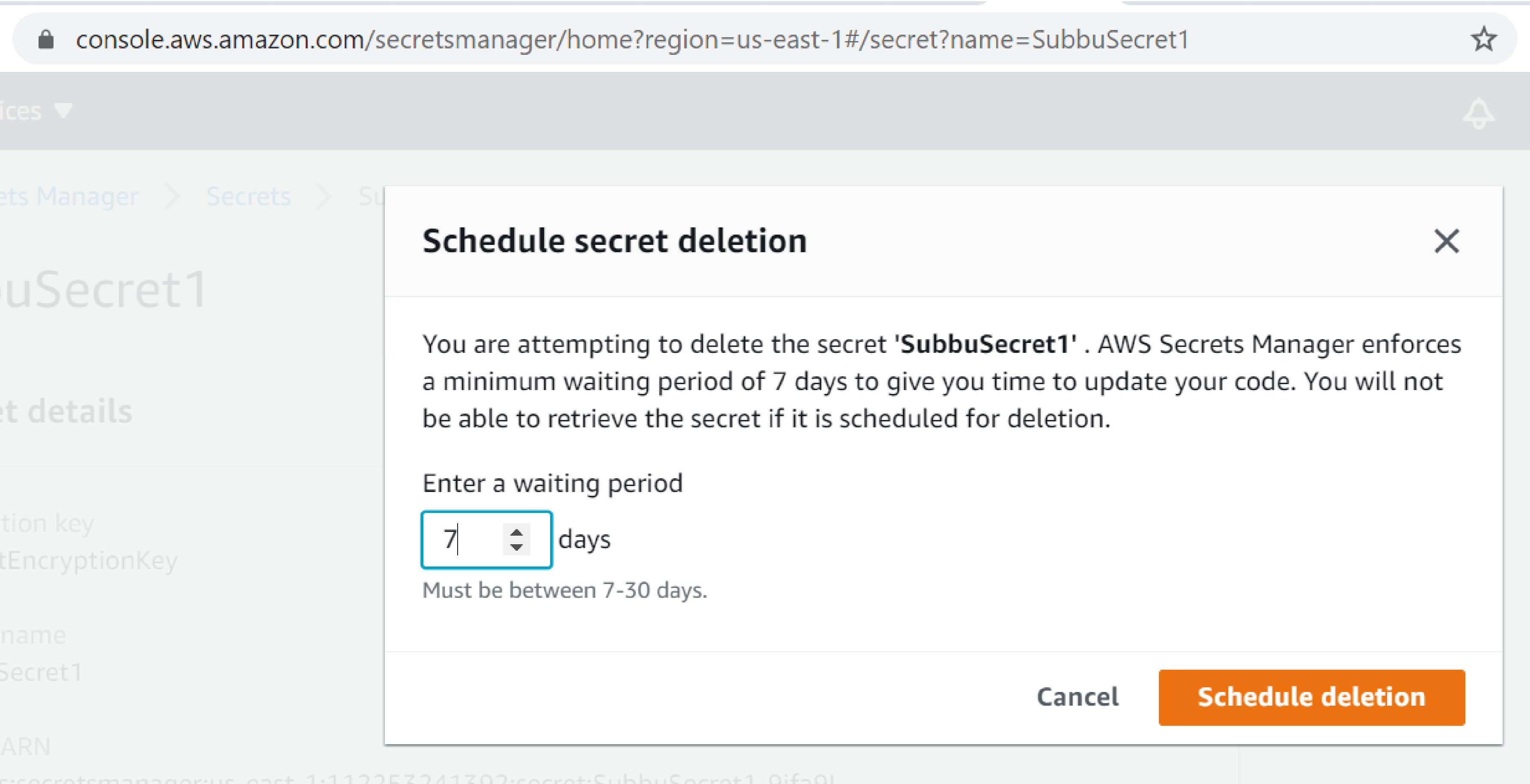
You are attempting to delete the secret **'SubbuSecret1'** . AWS Secrets Manager enforces a minimum waiting period of 7 days to give you time to update your code. You will not be able to retrieve the secret if it is scheduled for deletion.

Enter a waiting period

30 days

Must be between 7-30 days.

Chosen 7 days as waiting:



console.aws.amazon.com/secretsmanager/home?region=us-east-1#/secret?name=SubbuSecret1
ices ▼
ets Manager
Secrets
uSecret1
t details
tion key
tEncryptionKey
name
Secret1
ARN

Schedule secret deletion

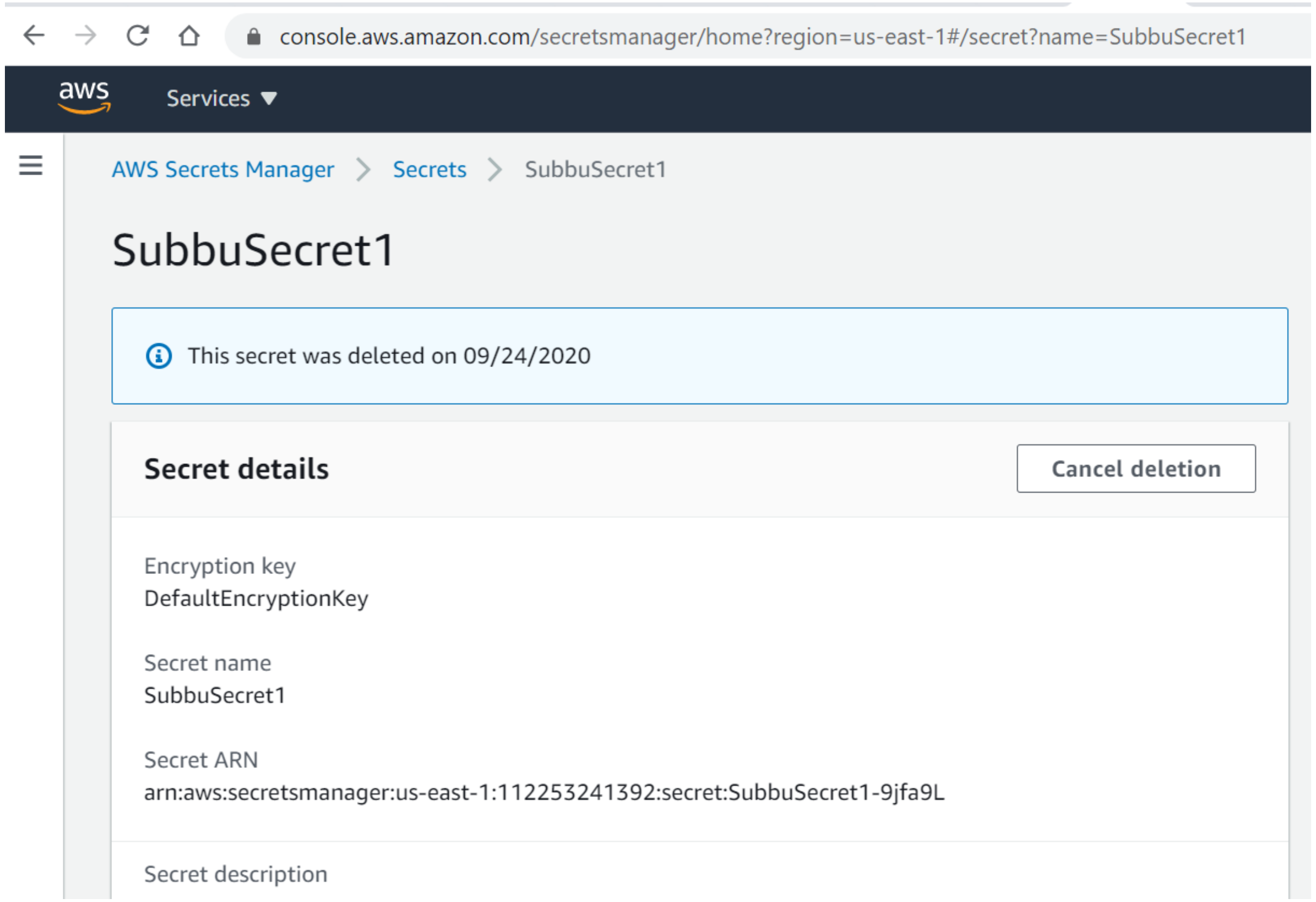
You are attempting to delete the secret **'SubbuSecret1'** . AWS Secrets Manager enforces a minimum waiting period of 7 days to give you time to update your code. You will not be able to retrieve the secret if it is scheduled for deletion.

Enter a waiting period

7 days

Must be between 7-30 days.

You can Cancel the “Delete Secret” request anytime, within the waiting time:


console.aws.amazon.com/secretsmanager/home?region=us-east-1#/secret?name=SubbuSecret1
aws
Services ▼
AWS Secrets Manager > Secrets > SubbuSecret1
Cancel deletion

SubbuSecret1

This secret was deleted on 09/24/2020

Secret details

Encryption key
DefaultEncryptionKey

Secret name
SubbuSecret1

Secret ARN
arn:aws:secretsmanager:us-east-1:112253241392:secret:SubbuSecret1-9jfa9L

Secret description

Appendix:

https://docs.aws.amazon.com/secretsmanager/index.html

https://docs.aws.amazon.com/cli/latest/reference/secretsmanager/index.html

https://docs.aws.amazon.com/secretsmanager/latest/userguide/tutorials_basic.html

https://docs.aws.amazon.com/secretsmanager/latest/userguide/manage_retrieve-secret.html