

AWS – Secrets Manager

-Hands-on guide.

Mr. Subramanyam Tirumani Vemala

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



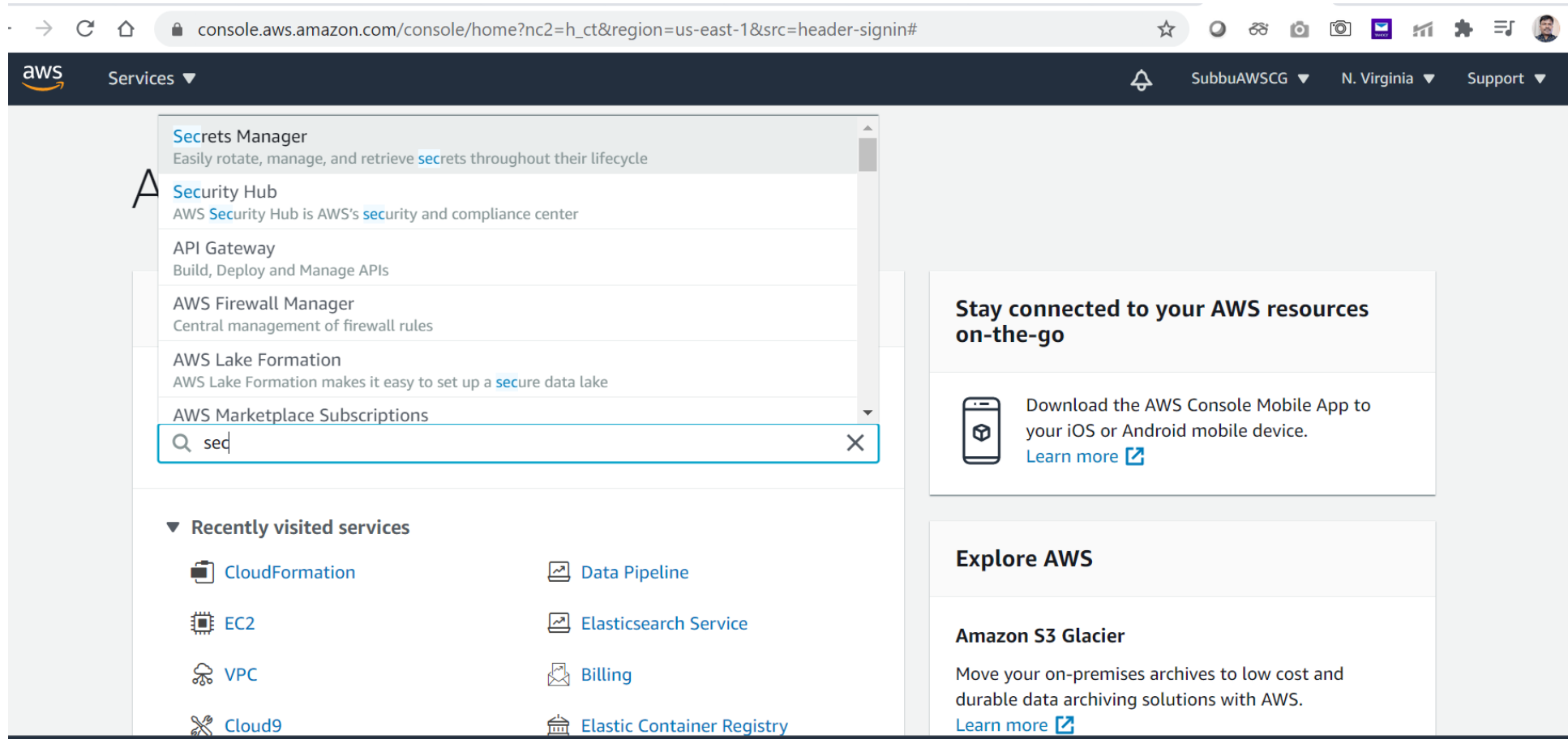
About AWS Secrets Manager:

- 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.

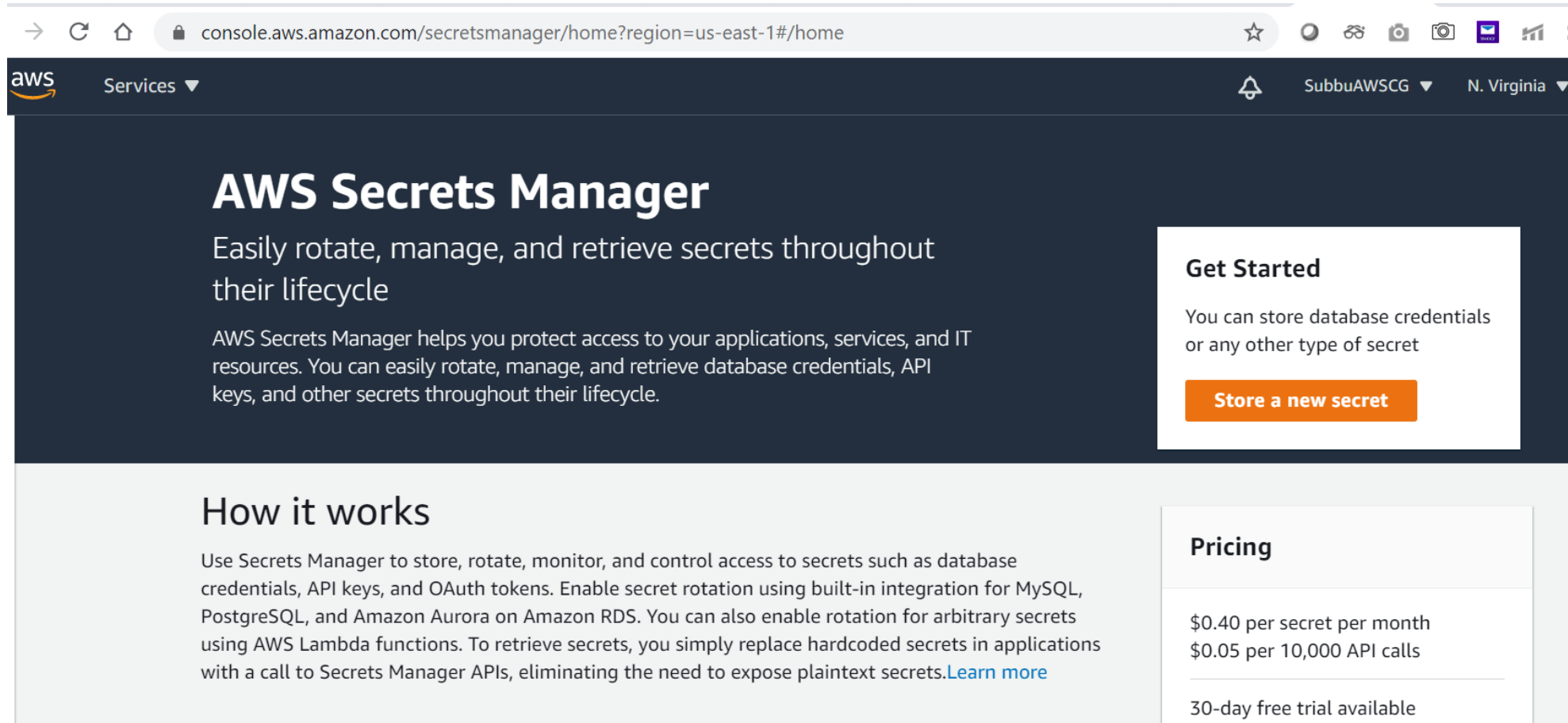
Pre-requisites:

1. AWS account.
2. AWS CLI.

Login to your AWS account – search for Secrets Manager:



Click on Store a new Secret:



The screenshot shows the AWS Secrets Manager console interface. At the top, the browser address bar displays the URL `console.aws.amazon.com/secretsmanager/home?region=us-east-1#/home`. The AWS navigation bar includes the logo, a 'Services' dropdown, a notification bell, the user name 'SubbuAWSCG', and the region 'N. Virginia'.

The main content area has a dark blue header with the title 'AWS Secrets Manager' and the subtitle 'Easily rotate, manage, and retrieve secrets throughout their lifecycle'. Below this, a paragraph explains that AWS Secrets Manager helps protect access to applications, services, and IT resources by managing database credentials, API keys, and other secrets.

On the right side, a 'Get Started' section contains the text 'You can store database credentials or any other type of secret' and a prominent orange button labeled 'Store a new secret'.

The lower section, titled 'How it works', describes the process of storing, rotating, monitoring, and controlling secrets like database credentials and API keys. It mentions built-in integrations for MySQL, PostgreSQL, and Amazon Aurora on Amazon RDS, as well as the ability to use AWS Lambda functions for arbitrary secrets. It concludes by stating that secrets are retrieved via API calls, eliminating the need for plaintext secrets, and provides a link to 'Learn more'.

On the right side of the lower section, a 'Pricing' box lists the costs: '\$0.40 per secret per month' and '\$0.05 per 10,000 API calls', with a note that a '30-day free trial' is available.

Choose the type of secret you want to create:

The screenshot shows the AWS Secrets Manager console interface. The browser address bar displays the URL: `console.aws.amazon.com/secretsmanager/home?region=us-east-1#/newSecret?step=selectSecret`. The top navigation bar includes the AWS logo, a 'Services' dropdown, and a user profile 'SubbuAWSCG'. The main content area is titled 'Store a new secret' and shows a four-step wizard: Step 1 (Secret type), Step 2 (Name and description), Step 3 (Configure rotation), and Step 4 (Review). Under 'Step 1 Secret type', there are five radio button options: 'Credentials for RDS database', 'Credentials for DocumentDB database', 'Credentials for Redshift cluster', 'Credentials for other database', and 'Other type of secrets (e.g. API key)'. The 'Other type of secrets' option is selected and highlighted with a blue border. Below the options, there is a section titled 'Specify the key/value pairs to be stored in this secret' with an 'Info' link. At the bottom, there are two tabs: 'Secret key/value' (which is active) and 'Plaintext'.

→ ↻ ⌂ console.aws.amazon.com/secretsmanager/home?region=us-east-1#/newSecret?step=selectSecret ☆ 🔍 📷 📄

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

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 ☆ 🔍 📷 📄

aws Services ▾ 🔔 SubbuAWSCG ▾

☐ 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

UserName	SubbuOthertypeofsecrets	Remove
Password	SubbuPassword	Remove

[+ Add row](#)

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 ▼ ↺

[Add new key](#) [🔗](#)

Name the new Secret:

The screenshot shows the AWS console interface for creating a new secret. The breadcrumb trail is 'AWS Secrets Manager > Secrets > Store a new secret'. The left sidebar shows four steps: 'Step 1 Secret type' (selected), 'Step 2 Name and description' (active), 'Step 3 Configure rotation', and 'Step 4 Review'. The main content area is titled 'Store a new secret' and contains a form for 'Secret name and description'. The 'Secret name' field contains 'SubbuSecret1' and has a note that it must contain only alphanumeric characters and /_+=.@-. The 'Description' field is optional and contains the placeholder text 'e.g - Access to MYSQL prod database for my AppBeta'.

→ ↻ 🏠 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:

The screenshot shows the AWS console interface for 'Store a new secret'. The breadcrumb trail is 'AWS Secrets Manager > Secrets > Store a new secret'. The left sidebar shows four steps: 'Step 1 Secret type', 'Step 2 Name and description', 'Step 3 Configure rotation' (which is the active step), and 'Step 4 Review'. The main content area is titled 'Store a new secret'. A light blue information box states: '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.' Below this is a section 'Configure automatic rotation - optional [Info](#)' with the instruction 'Configure AWS Secrets Manager to rotate this secret automatically. Read the [getting started guide](#) on rotation.' There are two radio button options: 'Disable automatic rotation' (selected) with the note 'Recommended when your applications are using this secret and have not been updated to use AWS Secrets Manager.', and 'Enable automatic rotation' with the note 'Recommended when your applications are not using this secret yet.' Below the options is a section 'Select rotation interval [Info](#)' with the text 'This secret will be rotated based on the schedule you determine.' and a dropdown menu currently set to '30 days'. At the bottom, it says 'Must be a value between 1 and 365 days'.

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

Info 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.

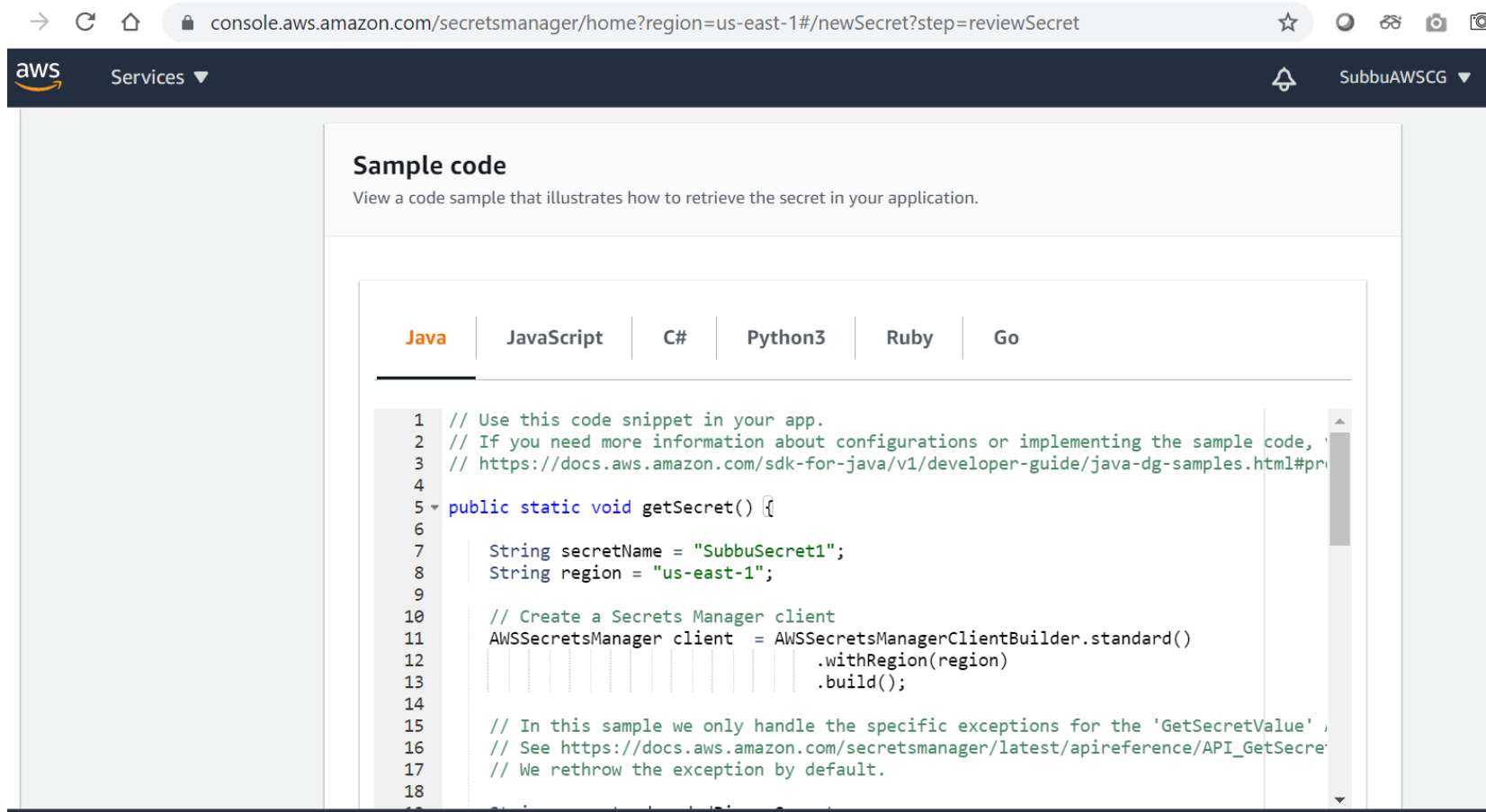
- ☒ **Disable automatic rotation**
Recommended when your applications are using this secret and have not been updated to use AWS Secrets Manager.
- ☐ **Enable automatic rotation**
Recommended when your applications are not using this secret yet.

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

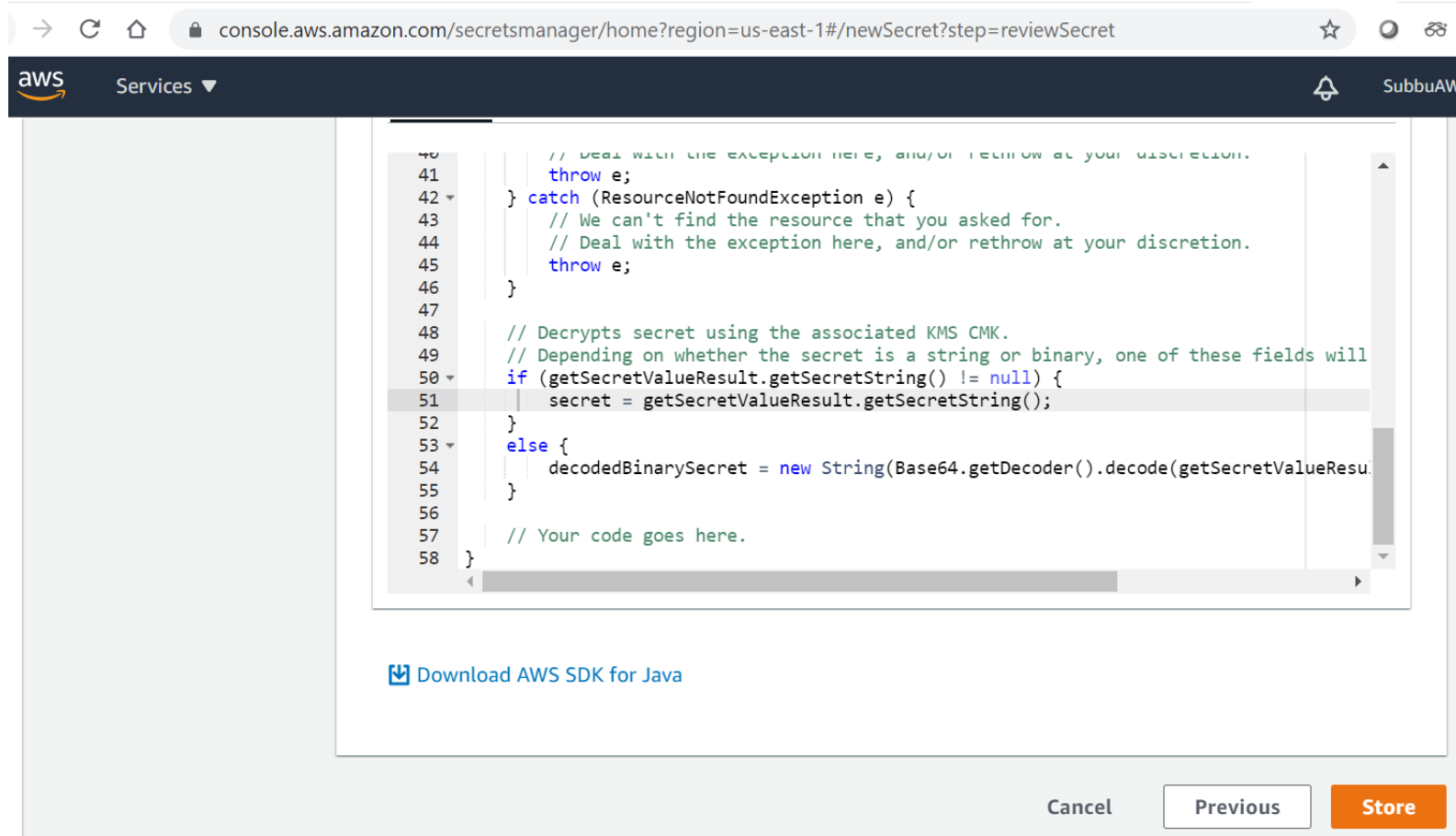
Use the generated code snippet, to have API calls in the code, based on the language:



The screenshot shows the AWS Secrets Manager console in a web browser. The address bar displays the URL: `console.aws.amazon.com/secretsmanager/home?region=us-east-1#/newSecret?step=reviewSecret`. The page title is "Sample code" with a subtitle "View a code sample that illustrates how to retrieve the secret in your application." Below this, there are tabs for different programming languages: Java, JavaScript, C#, Python3, Ruby, and Go. The "Java" tab is selected, showing a code snippet for retrieving a secret. The code is as follows:

```
1 // Use this code snippet in your app.
2 // If you need more information about configurations or implementing the sample code,
3 // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/java-dg-samples.html#pr
4
5 public static void getSecret() {
6
7     String secretName = "SubbuSecret1";
8     String region = "us-east-1";
9
10    // Create a Secrets Manager client
11    AWSSecretsManager client = AWSSecretsManagerClientBuilder.standard()
12        .withRegion(region)
13        .build();
14
15    // In this sample we only handle the specific exceptions for the 'GetSecretValue'
16    // See https://docs.aws.amazon.com/secretsmanager/latest/apireference/API_GetSecre
17    // We rethrow the exception by default.
18
```

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



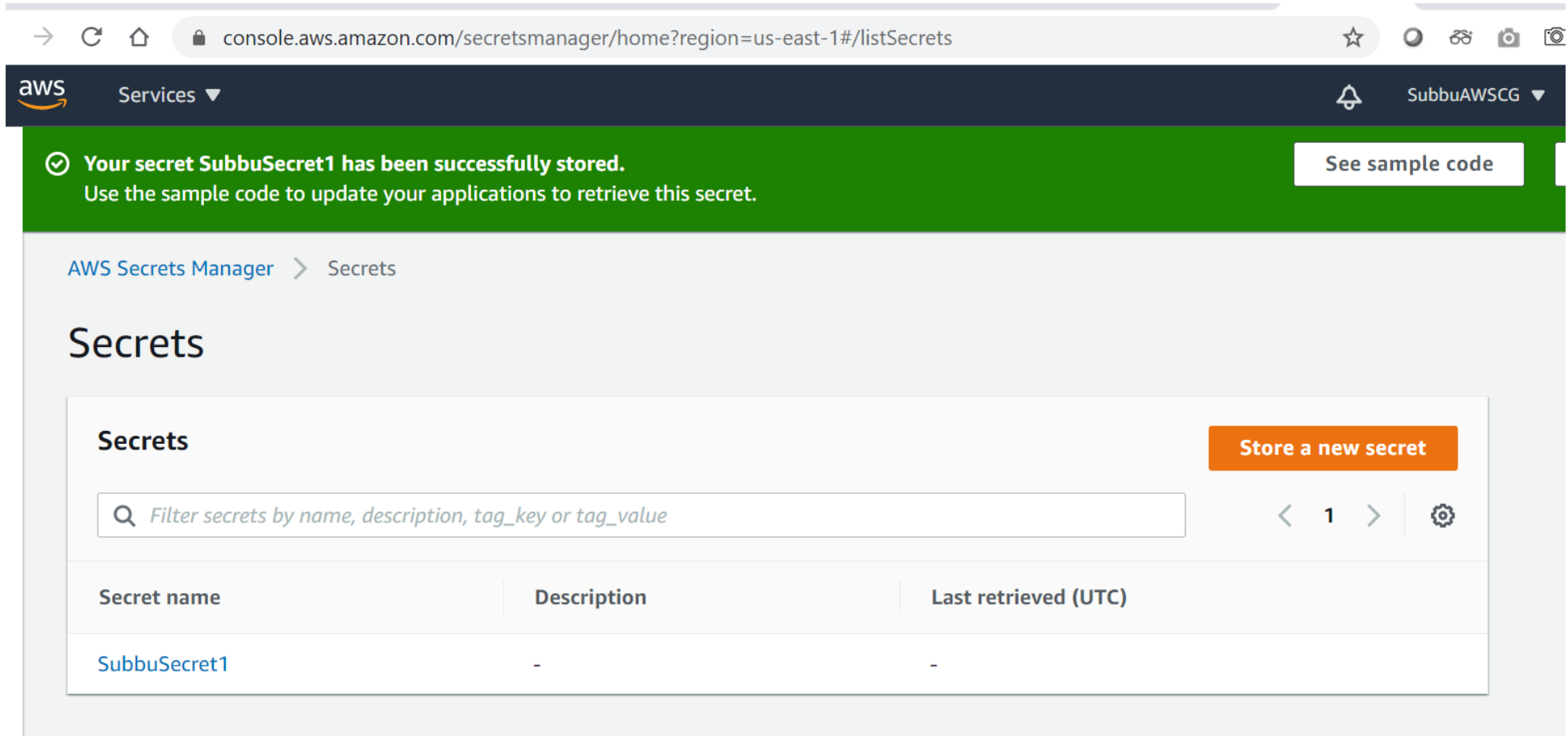
The screenshot shows the AWS console interface for reviewing a secret. The browser address bar displays the URL: `console.aws.amazon.com/secretsmanager/home?region=us-east-1#/newSecret?step=reviewSecret`. The AWS header bar includes the logo, a 'Services' dropdown, and a user profile 'SubbuAW5'. The main content area features a code editor with a Java snippet for handling secret retrieval. The code includes comments and logic to handle both string and binary secrets. A 'Download AWS SDK for Java' link is positioned below the code editor. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Store'.

```
40 // Deal with the exception here, and/or rethrow at your discretion.
41 throw e;
42 } catch (ResourceNotFoundException e) {
43     // We can't find the resource that you asked for.
44     // Deal with the exception here, and/or rethrow at your discretion.
45     throw e;
46 }
47
48 // Decrypts secret using the associated KMS CMK.
49 // Depending on whether the secret is a string or binary, one of these fields will
50 if (getSecretValueResult.getSecretString() != null) {
51     secret = getSecretValueResult.getSecretString();
52 }
53 else {
54     decodedBinarySecret = new String(Base64.getDecoder().decode(getSecretValueResult.getSecretBinary()));
55 }
56
57 // Your code goes here.
58 }
```

[Download AWS SDK for Java](#)

Cancel Previous Store

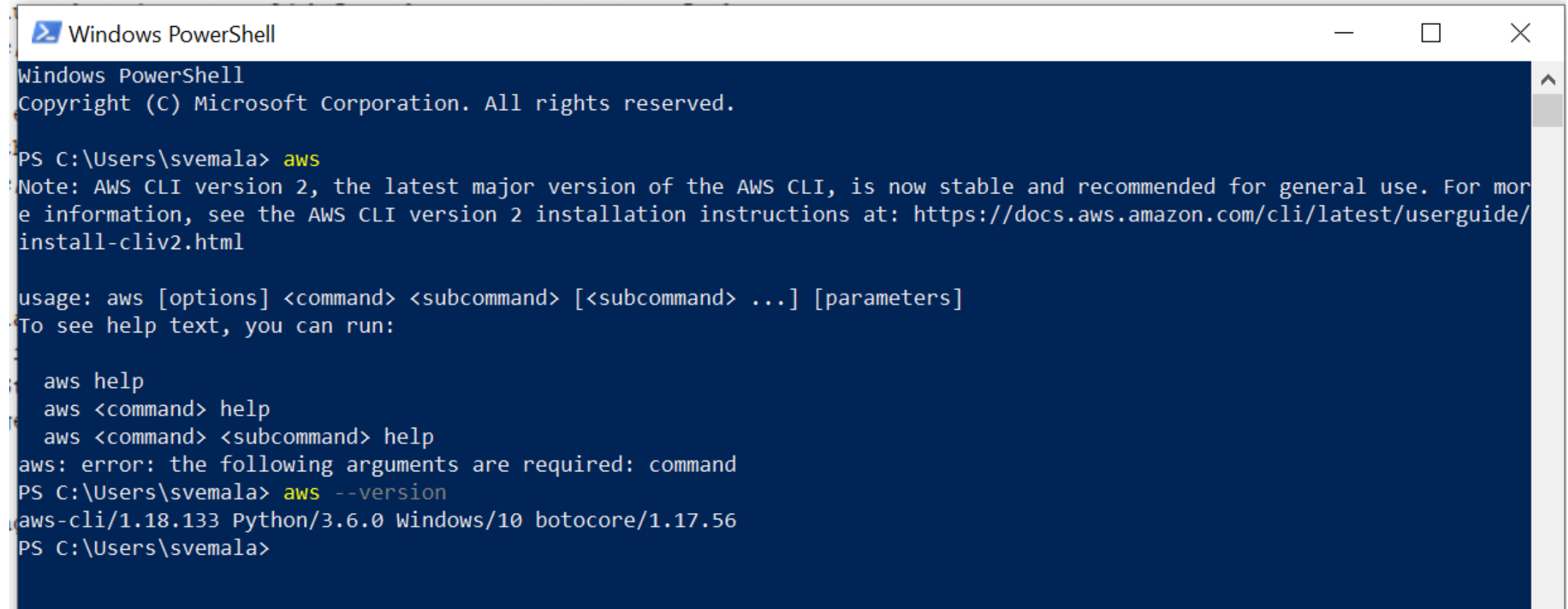
Now Secret has been created:



The screenshot displays the AWS Secrets Manager console interface. At the top, a green notification banner states: "Your secret SubbuSecret1 has been successfully stored. Use the sample code to update your applications to retrieve this secret." with a "See sample code" button. Below the notification, the breadcrumb "AWS Secrets Manager > Secrets" is visible. The main heading "Secrets" is followed by a "Store a new secret" button. A search bar with the placeholder "Filter secrets by name, description, tag_key or tag_value" is present. Below the search bar, a table lists the secrets:

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 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>
```

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:

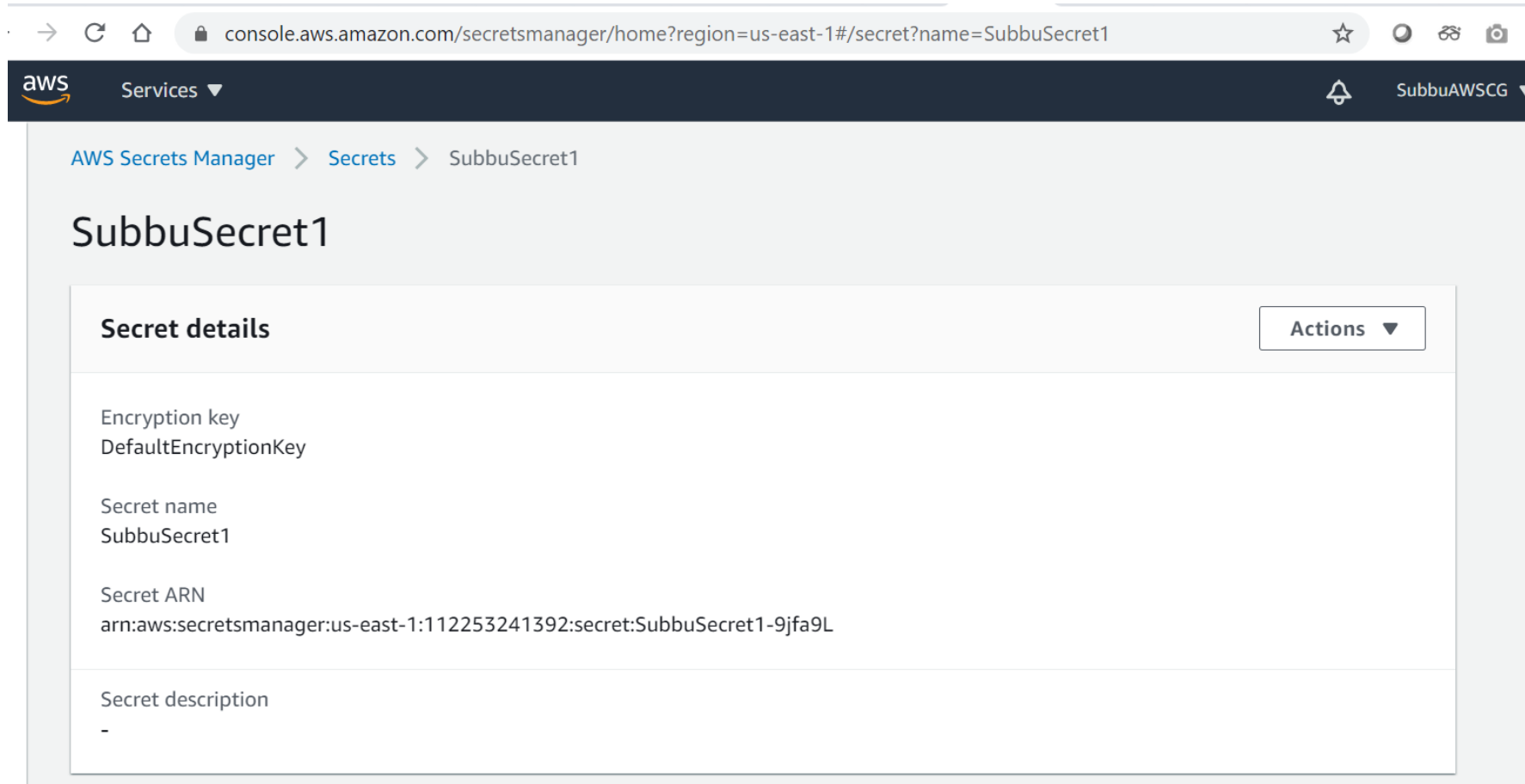
```
PS C:\Users\svemala> aws secretsmanager get-secret-value --secret-id SubbuSecret1 --version-stage AWSCURRENT
{
  "ARN": "arn:aws:secretsmanager:us-east-1:112253241392:secret:SubbuSecret1-9jfa9L",
  "Name": "SubbuSecret1",
  "VersionId": "49b8431a-f442-45d0-a954-03eb9aecf298",
  "SecretString": "{\"UserName\":\"SubbuOthertypeofsecrets\",\"Password\":\"SubbuPa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

```
PS C:\Users\svemala>
```

You can view the Secrets list:



The screenshot displays the AWS Secrets Manager console interface. The browser's address bar shows the URL `console.aws.amazon.com/secretsmanager/home?region=us-east-1#/secret?name=SubbuSecret1`. The AWS navigation bar at the top includes the AWS logo, a 'Services' dropdown, a notification bell, and the user profile 'SubbuAWSCG'. The breadcrumb trail indicates the path: `AWS Secrets Manager > Secrets > SubbuSecret1`. The main heading for the page is `SubbuSecret1`. Below this, a 'Secret details' section is shown, which includes an 'Actions' dropdown menu. The details are organized into four rows: 'Encryption key' with the value 'DefaultEncryptionKey', 'Secret name' with the value 'SubbuSecret1', 'Secret ARN' with the value 'arn:aws:secretsmanager:us-east-1:112253241392:secret:SubbuSecret1-9jfa9L', and 'Secret description' with the value '-'. The interface uses a clean, modern design with a light gray background and white content boxes.

→ ↻ 🏠 🔒 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 ▾

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:

The screenshot shows the AWS Secrets Manager console interface. The browser address bar displays the URL: `console.aws.amazon.com/secretsmanager/home?region=us-east-1#/secret?name=SubbuSecret1`. The AWS logo and 'Services' menu are visible in the top navigation bar, along with a user profile labeled 'SubbuAWSCG'. The main content area is divided into two sections:

- Secret value** [Info](#): This section contains the instruction 'Retrieve and view the secret value.' and a button labeled 'Retrieve secret value'.
- Rotation configuration** [Info](#): This section contains the following details:
 - Rotation status**: Indicated as 'Disabled' with a minus icon.
 - Rotation Interval**: Described as 'The schedule you have set for credentials rotation', with a value of '-'.
 - AWS Lambda function**: Described as 'The AWS Lambda function that has permissions to rotate this secret.', with a value of '-'. A button labeled 'Edit rotation' is located in the top right corner of this section.

View of Secrets values:

The screenshot displays the AWS Secrets Manager console interface. The browser address bar shows the URL: `console.aws.amazon.com/secretsmanager/home?region=us-east-1#/secret?name=SubbuSecret1`. The AWS logo and 'Services' dropdown are visible in the top navigation bar, along with a user profile 'SubbuAWSCG'.

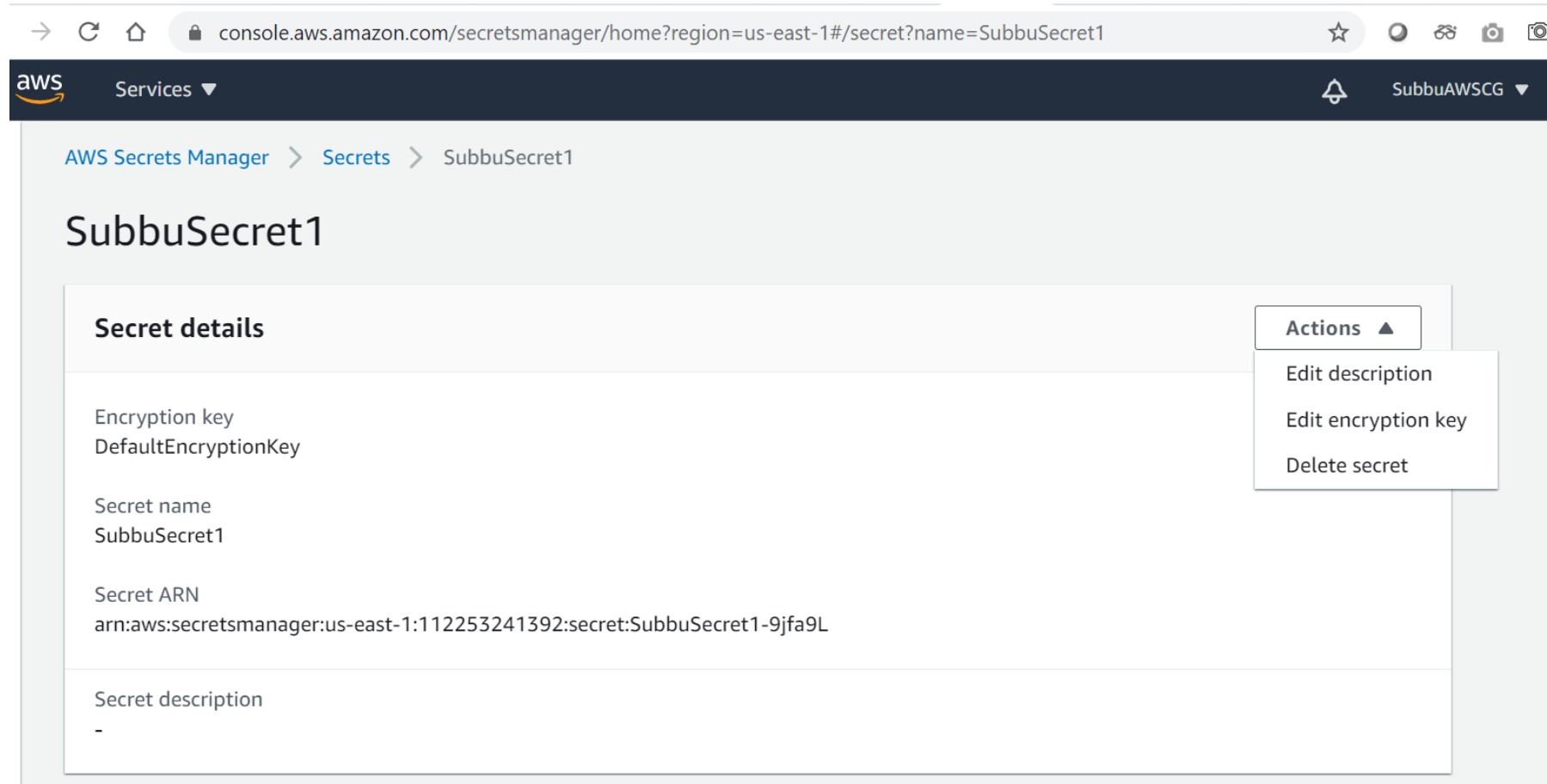
The main content area is divided into sections:

- Tags:** A section at the top with an 'Edit tags' button.
- Secret value:** A section with a title 'Secret value' and an 'Info' link. Below the title is the instruction 'Retrieve and view the secret value.' To the right are 'Close' and 'Edit' buttons.
- Secret key/value / Plaintext:** A tabbed interface with two tabs: 'Secret key/value' (selected) and 'Plaintext'.
- Table:** A table with two columns: 'Secret Key' and 'Secret Value'. It contains two rows of data:

Secret Key	Secret Value
UserName	SubbuOthertypeofsecrets
Password	SubbuPassword
- Rotation configuration:** A section at the bottom with a title 'Rotation configuration' and an 'Info' link. To the right is an 'Edit rotation' button.

Below the rotation configuration section, the text 'Rotation status' is partially visible.

Delete the Secrets if no more needed:



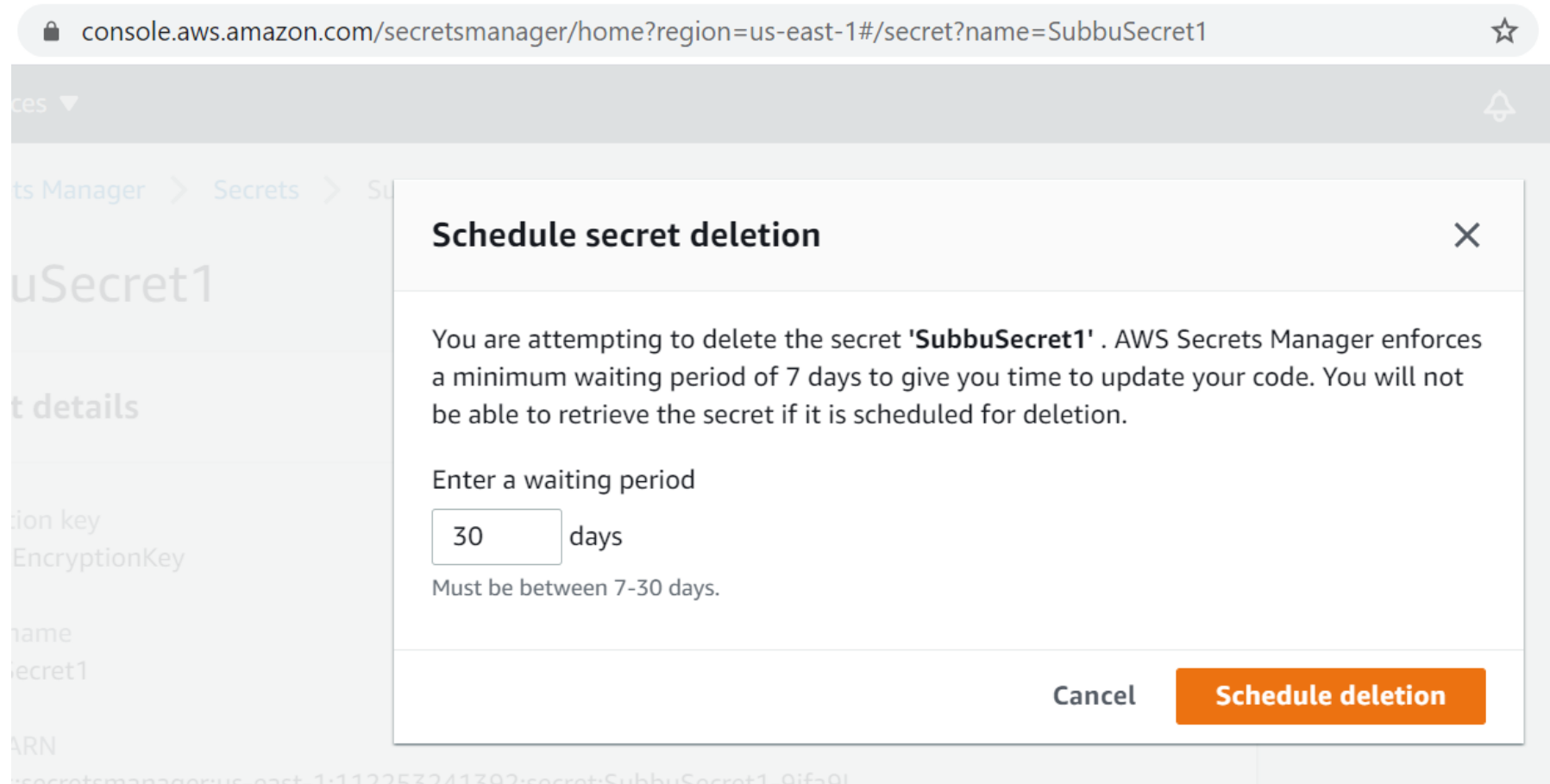
The screenshot shows the AWS Secrets Manager console interface. The browser address bar displays the URL: `console.aws.amazon.com/secretsmanager/home?region=us-east-1#/secret?name=SubbuSecret1`. The AWS logo and 'Services' dropdown are visible in the top navigation bar. The breadcrumb trail indicates the path: `AWS Secrets Manager > Secrets > SubbuSecret1`. The main heading is `SubbuSecret1`. Below this, the 'Secret details' section lists the following information:

- Encryption key: `DefaultEncryptionKey`
- Secret name: `SubbuSecret1`
- Secret ARN: `arn:aws:secretsmanager:us-east-1:112253241392:secret:SubbuSecret1-9jfa9L`
- Secret description: `-`

To the right of the details, an 'Actions' menu is open, showing three options:

- Edit description
- Edit encryption key
- Delete secret

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



The screenshot shows the AWS Secrets Manager console interface. A modal dialog titled "Schedule secret deletion" is open, overlaying the secret details for "SubbuSecret1". The dialog contains the following text: "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." Below this text is a form labeled "Enter a waiting period" with a text input field containing the number "30" and the word "days" next to it. A note below the input field states "Must be between 7-30 days." At the bottom right of the dialog are two buttons: "Cancel" and "Schedule deletion".

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

ces ▼

ts Manager > Secrets > SubbuSecret1

uSecret1

t details

tion key
EncryptionKey

name
Secret1

ARN
secretsmanager:us-east-1:112253241392:secret:SubbuSecret1-0ifa9l

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.

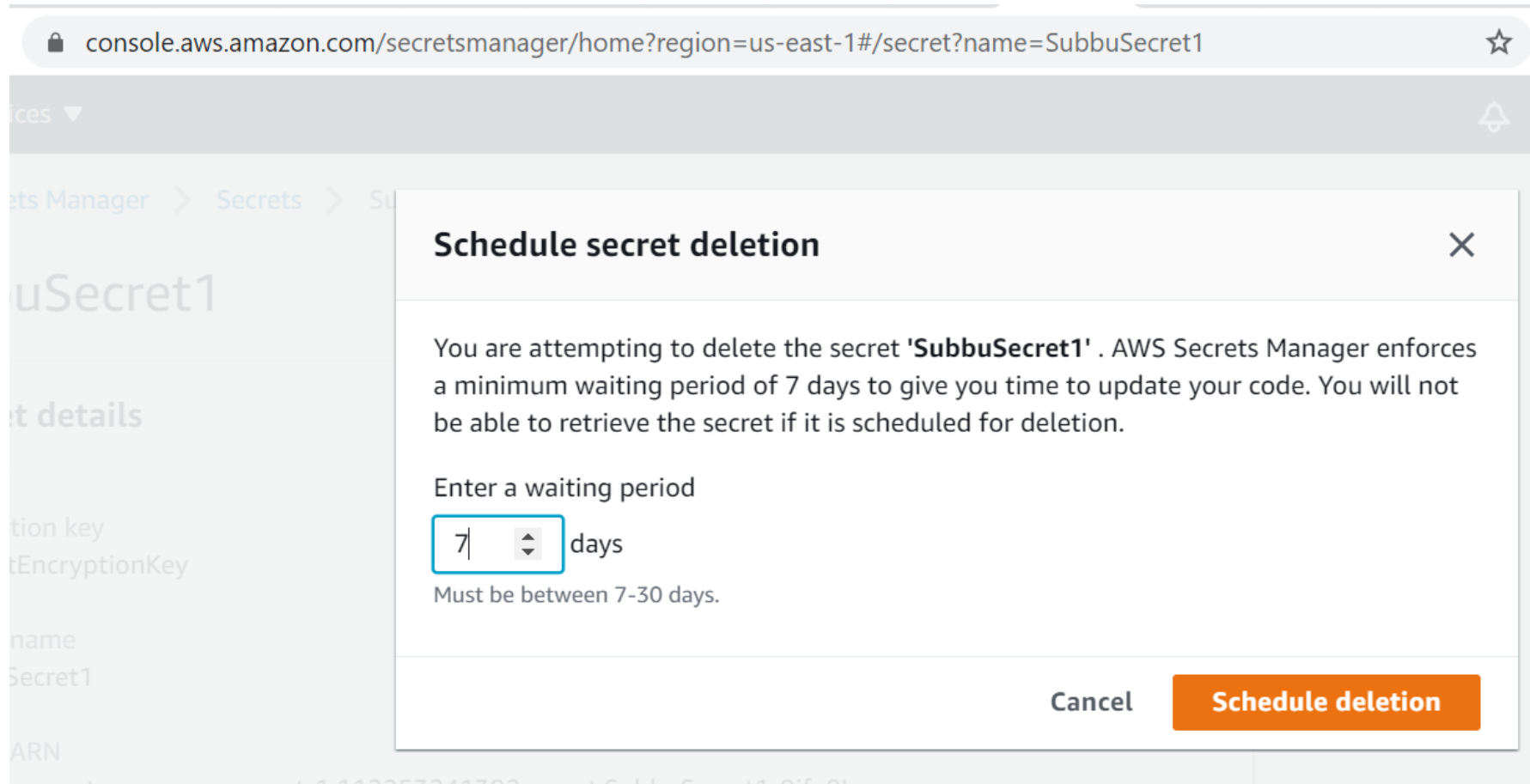
Enter a waiting period

30 days

Must be between 7-30 days.

Cancel Schedule deletion

Chosen 7 days as waiting:



The screenshot shows the AWS Secrets Manager console interface. A modal dialog titled "Schedule secret deletion" is open, displaying information about deleting the secret "SubbuSecret1". The dialog explains the 7-day waiting period and includes a field to enter the waiting period, which is currently set to 7 days. The background shows the secret's details, including its name, ARN, and encryption key.

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

Services ▾

Secrets Manager > Secrets > SubbuSecret1

SubbuSecret1

Secret details

Rotation key

EncryptionKey

name

Secret1

ARN

secretmanager:us-east-1:112357341302:secret:SubbuSecret1-0ifz0l

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.

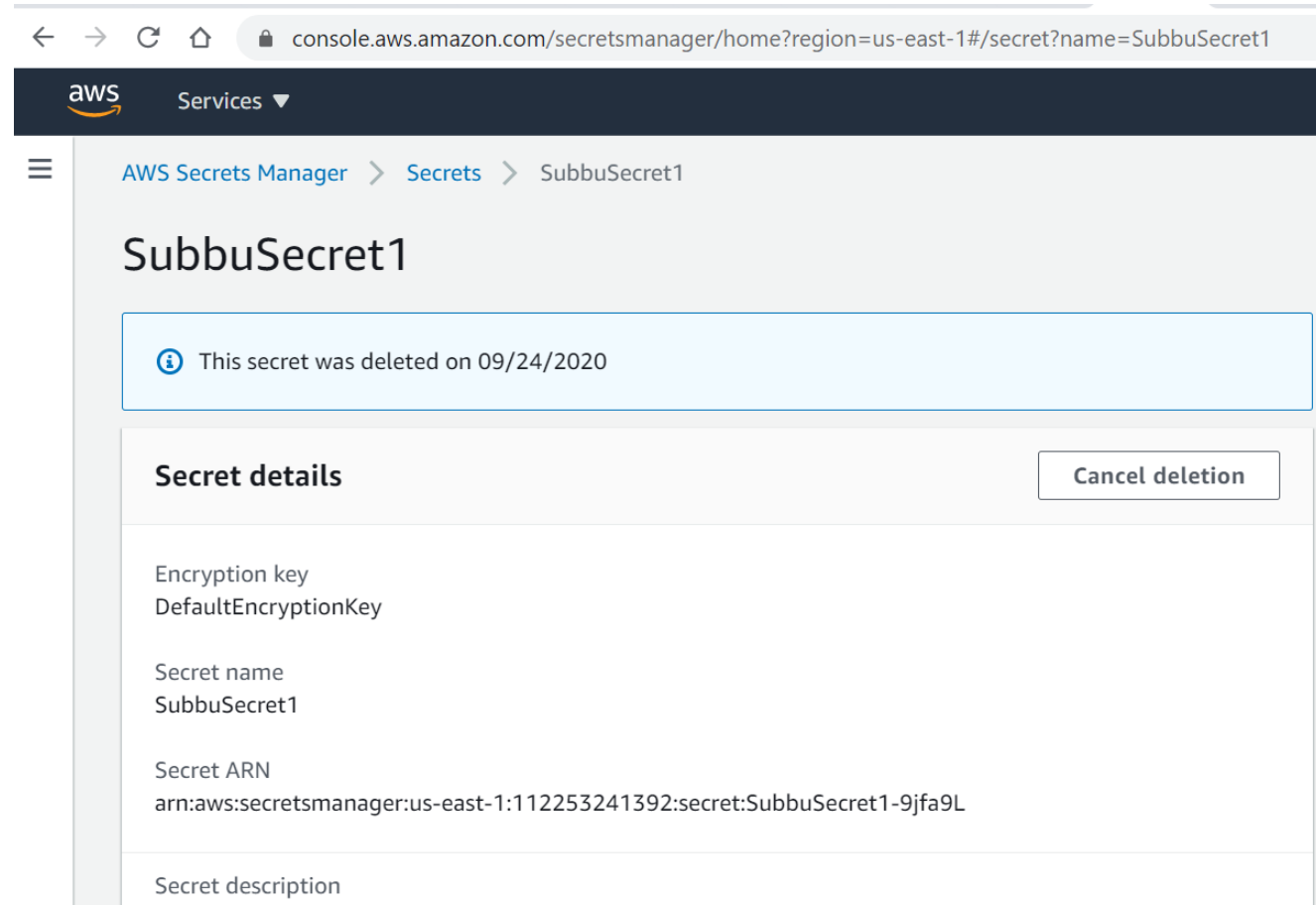
Enter a waiting period

7 days

Must be between 7-30 days.

Cancel Schedule deletion

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



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