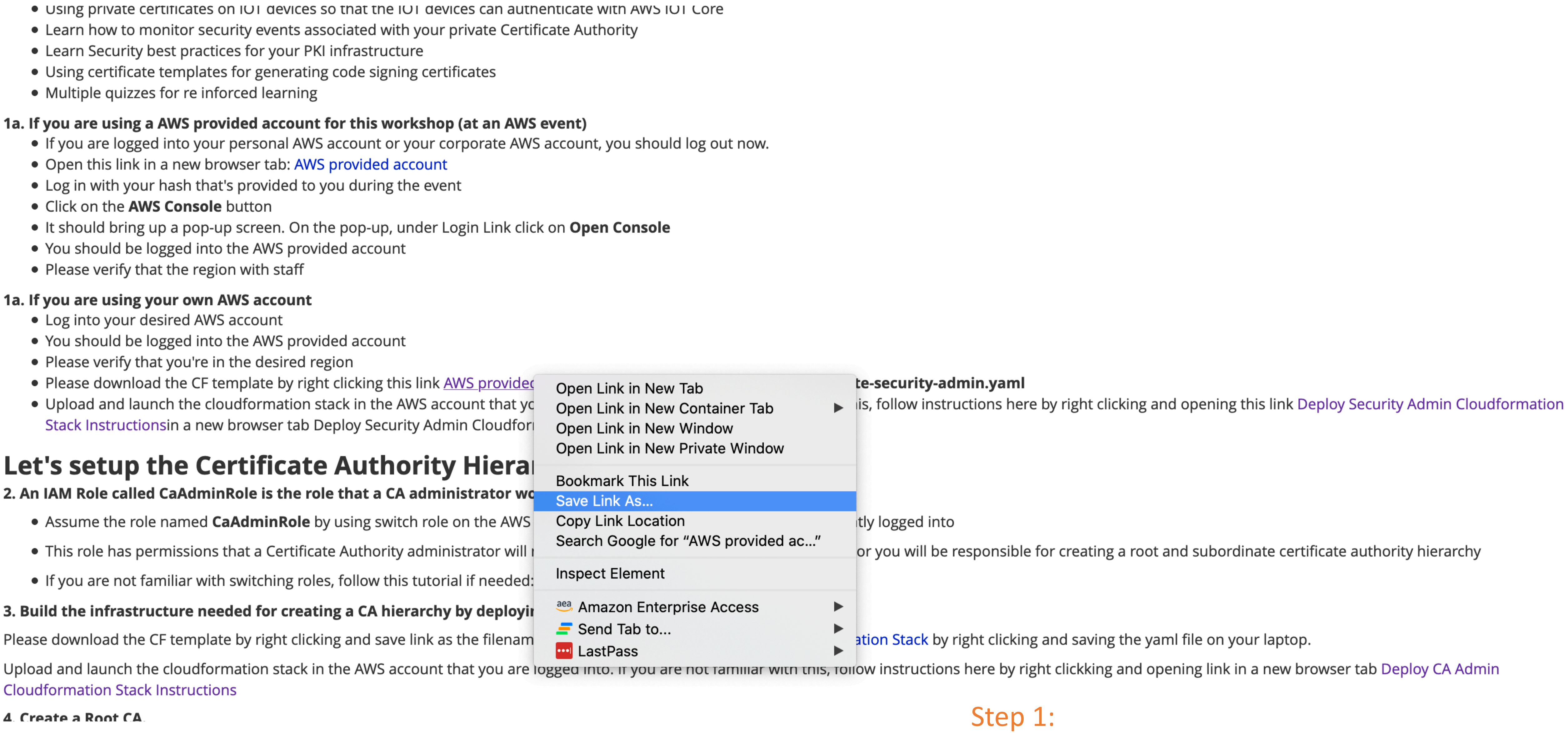


- Using private certificates on IOT devices so that the IOT devices can authenticate with AWS IOT Core
- Learn how to monitor security events associated with your private Certificate Authority
- Learn Security best practices for your PKI infrastructure
- Using certificate templates for generating code signing certificates
- Multiple quizzes for re inforced learning

1a. If you are using a AWS provided account for this workshop (at an AWS event)

- If you are logged into your personal AWS account or your corporate AWS account, you should log out now.
- Open this link in a new browser tab: AWS provided account
- Log in with your hash that's provided to you during the event
- Click on the **AWS Console** button
- It should bring up a pop-up screen. On the pop-up, under Login Link click on **Open Console**
- You should be logged into the AWS provided account
- Please verify that the region with staff

1a. If you are using your own AWS account

- Log into your desired AWS account
- You should be logged into the AWS provided account
- Please verify that you're in the desired region
- Please download the CF template by right clicking this link AWS provided **te-security-admin.yaml**
- Upload and launch the cloudformation stack in the AWS account that yc is, follow instructions here by right clicking and opening this link Deploy Security Admin Cloudformation Stack Instructionsin a new browser tab Deploy Security Admin Cloudfor

Let's setup the Certificate Authority Hiera

2. An IAM Role called CaAdminRole is the role that a CA administrator wo

- Assume the role named **CaAdminRole** by using switch role on the AWS tly logged into
- This role has permissions that a Certificate Authority administrator will or you will be responsible for creating a root and subordinate certificate authority hierarchy
- If you are not familiar with switching roles, follow this tutorial if needed:

3. Build the infrastructure needed for creating a CA hierarchy by deployi

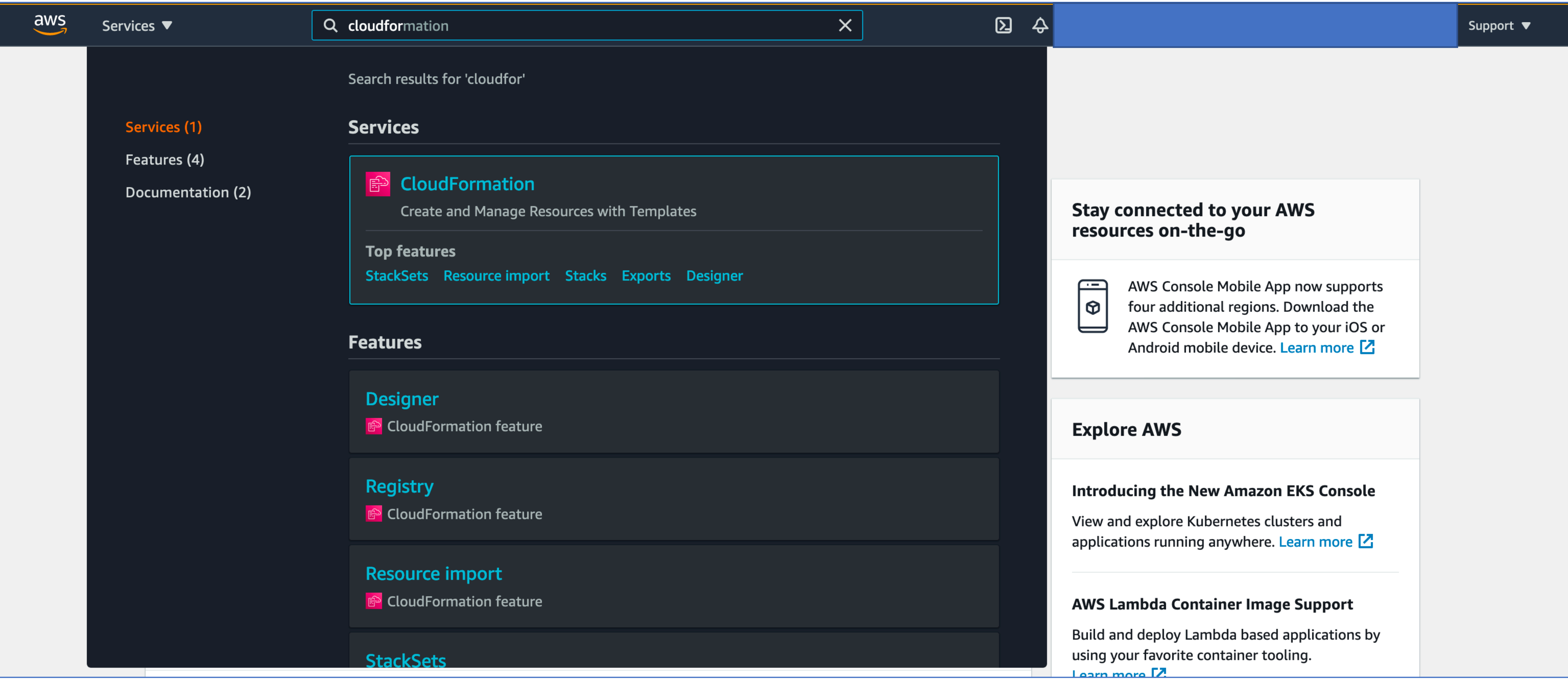
Please download the CF template by right clicking and save link as the filenam ation Stack by right clicking and saving the yaml file on your laptop.

Upload and launch the cloudformation stack in the AWS account that you are logged into. If you are not familiar with this, follow instructions here by right clickking and opening link in a new browser tab Deploy CA Admin Cloudformation Stack Instructions

4. Create a Root CA

Step 1:

- Right Click -> Save Link As…



Search results for 'cloudfor'

Services

CloudFormation

Create and Manage Resources with Templates

Top features

StackSets Resource import Stacks Exports Designer

Features

Designer

CloudFormation feature

Registry

CloudFormation feature

Resource import

CloudFormation feature

StackSets

Stay connected to your AWS resources on-the-go

AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

Explore AWS

Introducing the New Amazon EKS Console

View and explore Kubernetes clusters and applications running anywhere. Learn more

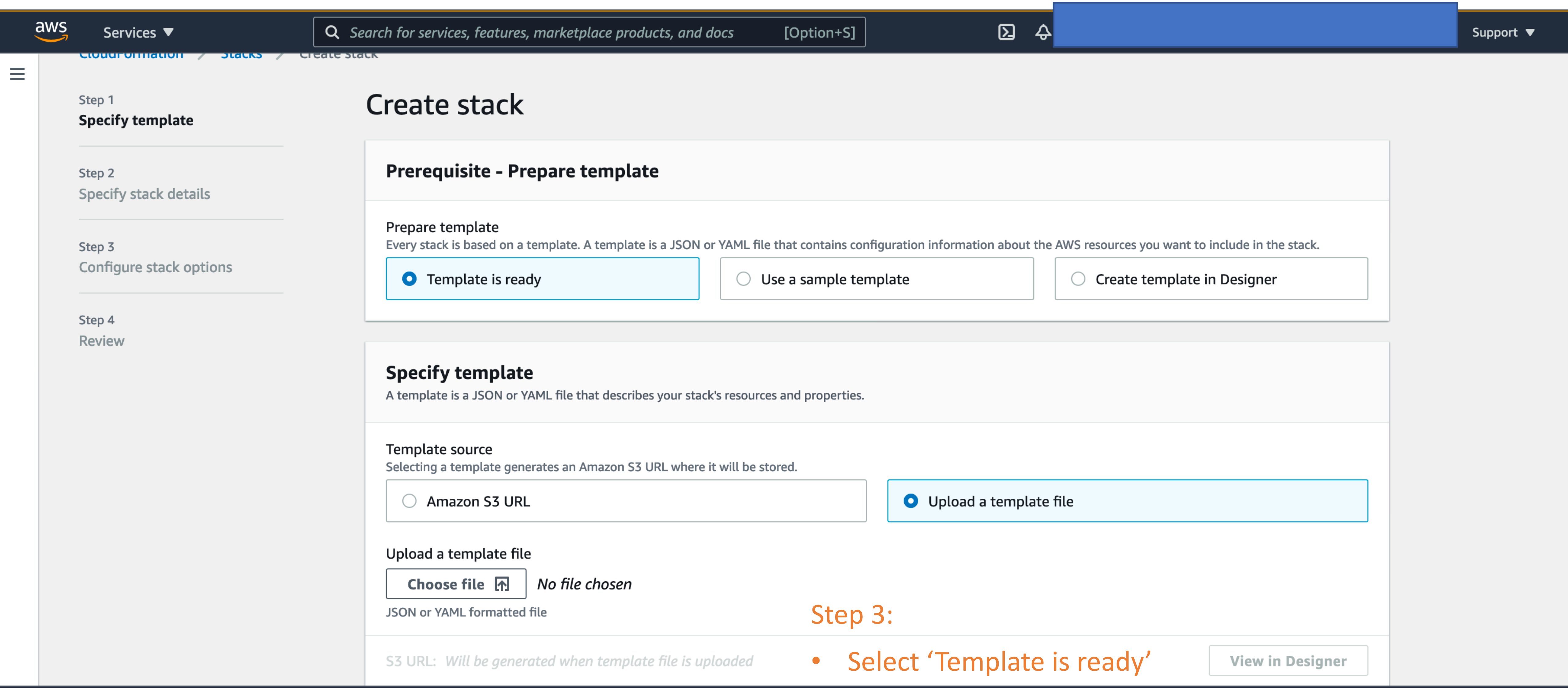
AWS Lambda Container Image Support

Build and deploy Lambda based applications by using your favorite container tooling.

Learn more

Step 2:

- Navigate to CloudFormation



Services ▼

Search for services, features, marketplace products, and docs [Option+S]

[redacted]

Support ▼

CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

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.

● 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

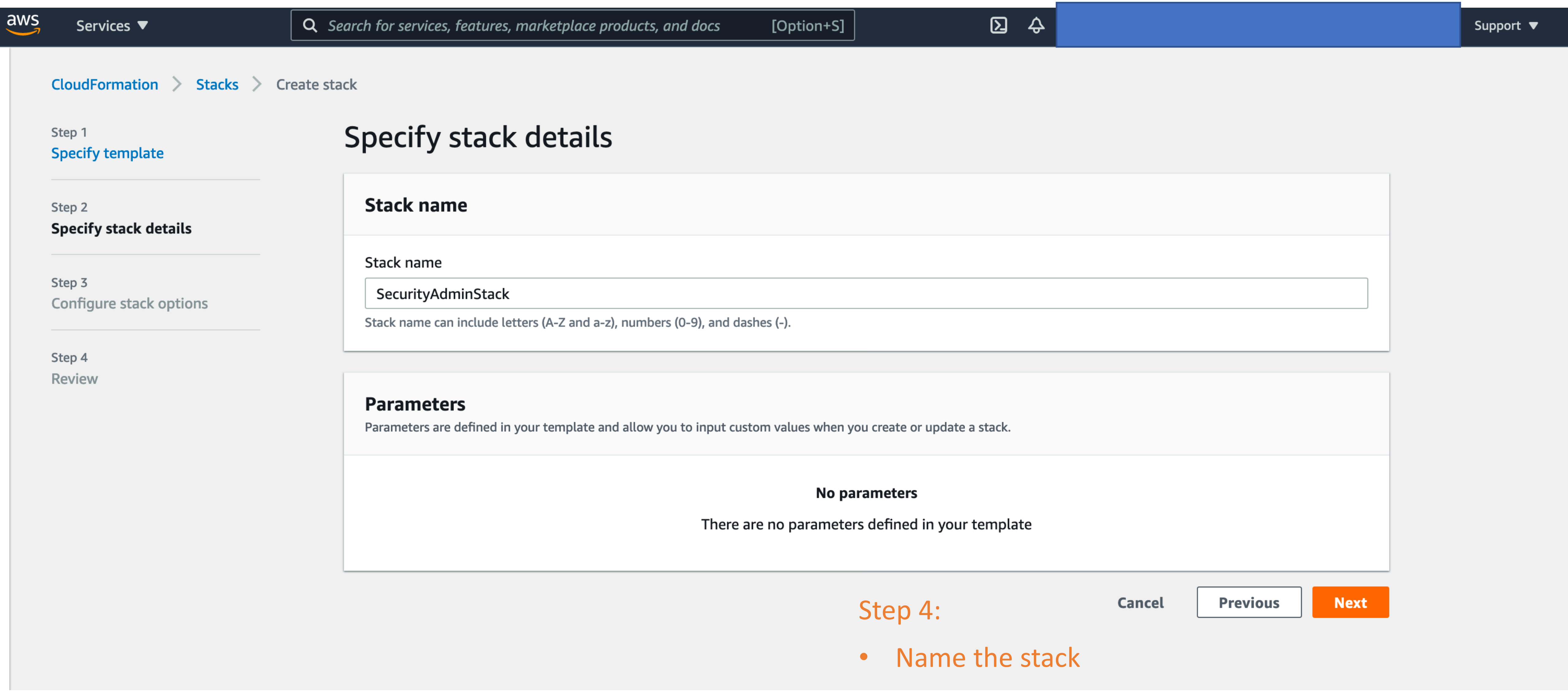
Upload a template file
Choose file *No file chosen*
JSON or YAML formatted file

S3 URL: *Will be generated when template file is uploaded*

View in Designer

Step 3:

- Select ‘Template is ready’
- Select ‘Upload a template file
- Choose File -> Select the YAML you downloaded



[redacted]

Specify stack details

Stack name

Stack name

SecurityAdminStack

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

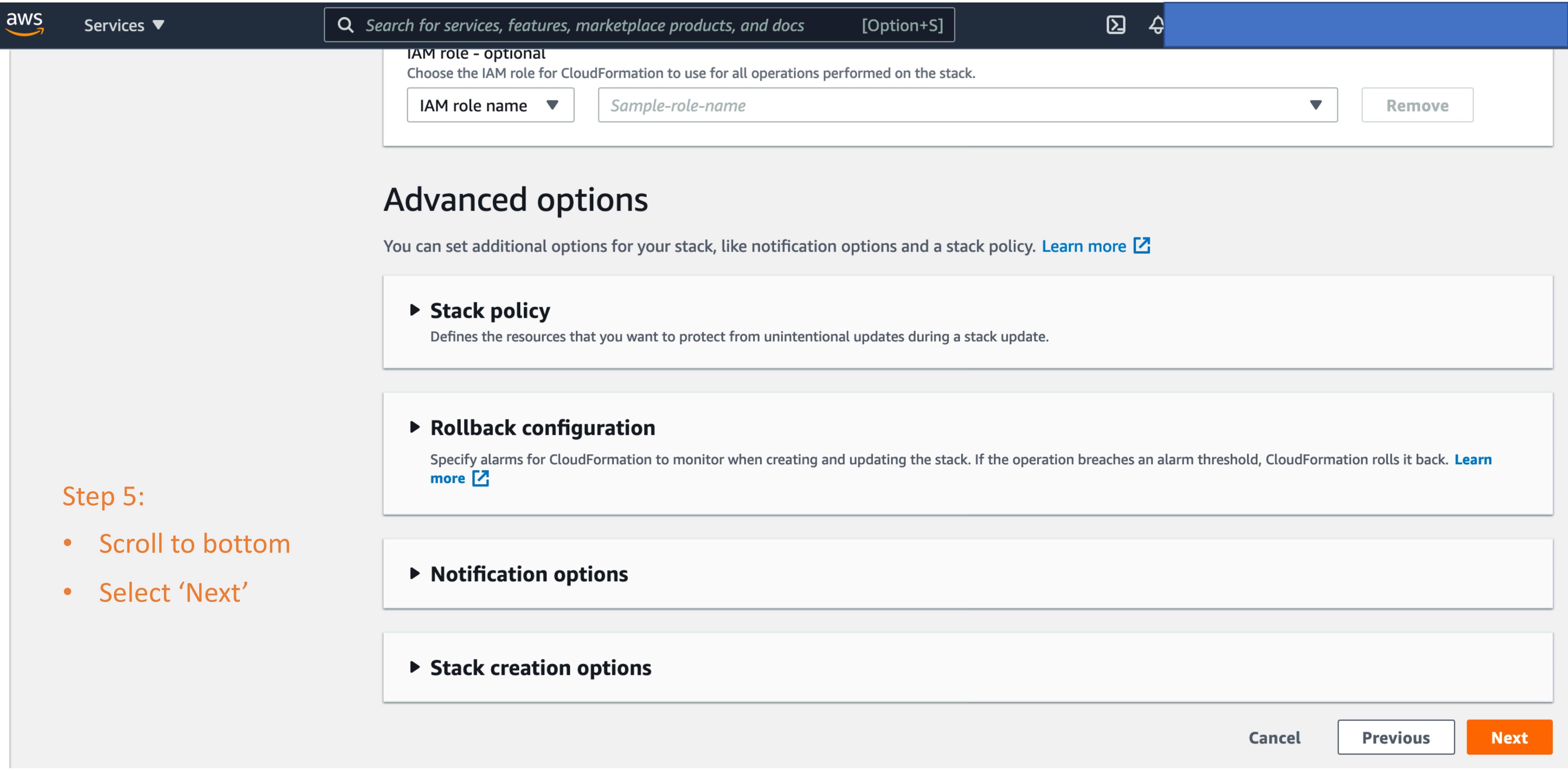
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

No parameters

There are no parameters defined in your template

Step 4:

- Name the stack



aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]

[redacted]

IAM role - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name ▼ | Sample-role-name ▼ | Remove

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**

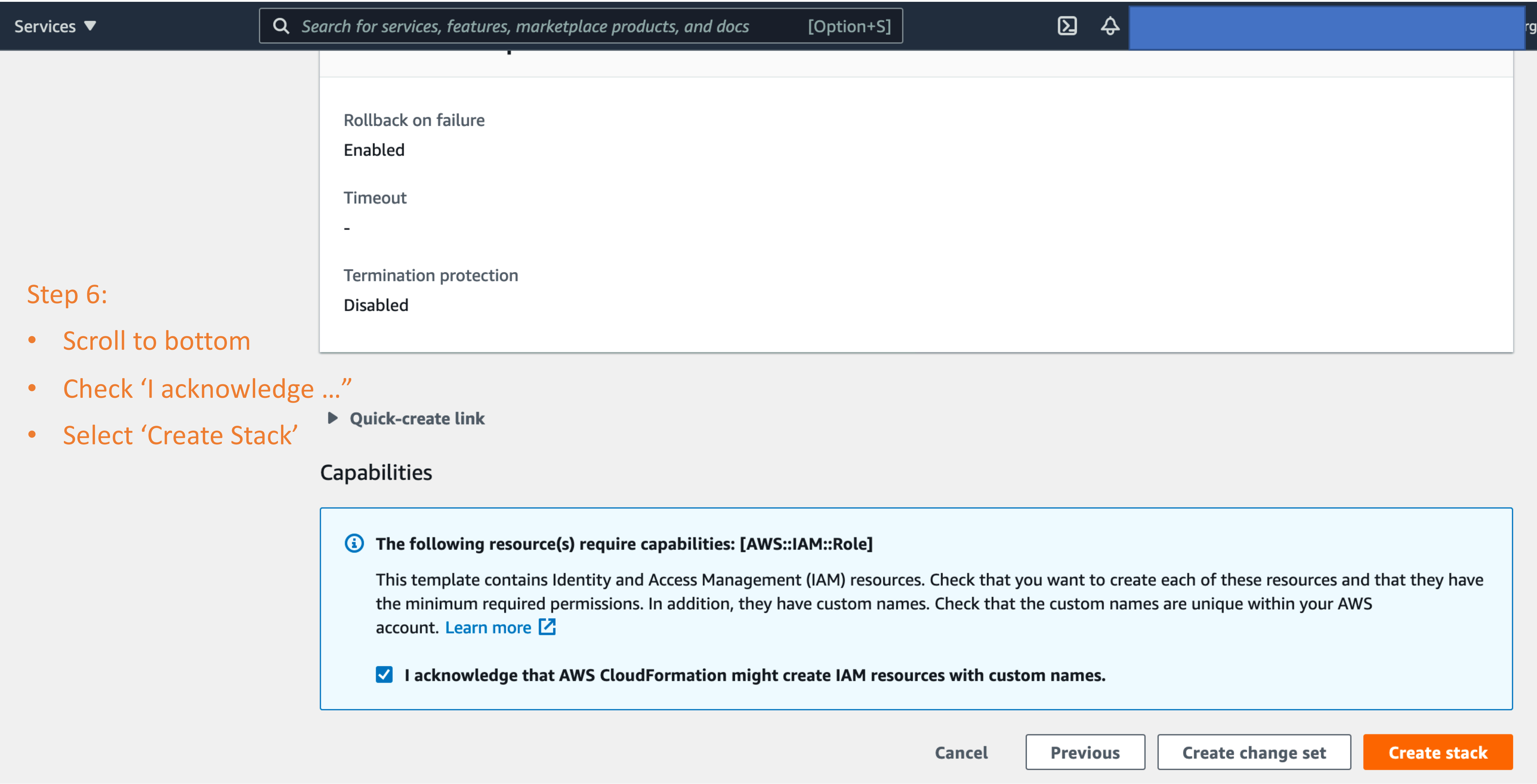
Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back. **Learn more**

▶ **Notification options**

▶ **Stack creation options**

Step 5:

- Scroll to bottom
- Select ‘Next’



Services ▼
Search for services, features, marketplace products, and docs [Option+S]
[redacted]

Step 6:

- Scroll to bottom
- Check ‘I acknowledge …”
- Select ‘Create Stack’

Rollback on failure
Enabled

Timeout
-

Termination protection
Disabled

▶ 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.**