**Implementation Guide:**

**Crowdstrike Falcon Discover for Cloud**

Table of Contents

[Foreword 3](#_Toc42098927)

[Solution overview and features 4](#_Toc42098928)

[Architecture diagram 4](#_Toc42098929)

[Pre-requisites 5](#_Toc42098930)

[Deployment and Configuration Steps 6](#_Toc42098931)

[Configuration: Set up Additional configuration [SaaS vs AMI] 7](#_Toc42098932)

[Configuration: Solution to deploy [if any automation included as part the solution] 7](#_Toc42098933)

[What to expect 7](#_Toc42098934)

[Best Practices 7](#_Toc42098935)

[Solution Estimated Pricing 7](#_Toc42098936)

[FAQs 7](#_Toc42098937)

[Additional resources 7](#_Toc42098938)

[Partner contact information 7](#_Toc42098939)

# Foreword

With Crowdstrike Falcon Discover for Cloud you can gain immediate and comprehensive visibility into all managed endpoints equipped with CrowdStrike Falcon endpoint security, and unmanaged assets across all accounts. In addition, Falcon Discover for AWS is able to cross boundaries to see virtual private clouds (VPCs) and subnets, and collect data from all endpoints — even those that are unmanaged — as well as all hybrid infrastructures. The rich AWS content Falcon Discover delivers allows organizations to quickly understand and prioritize instances and immediately ensure that the Falcon agent is fully deployed, dramatically improving organizations’ security postures.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure Crowdstrike Falcon Discover for Cloud in an AWS Control Tower environment while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

# Solution overview and features

### **Benefits of Falcon Discover for AWS**

As the only cloud-native, next-generation security solution of its kind, Falcon Discover for AWS offers streamlined integration not available with other third-party solutions, and saves organizations the time and expense of trying to develop these capabilities in-house. Falcon Discover for AWS offers the following benefits:

**Identifies security gaps with comprehensive and consistent visibility across all EC2 instances and endpoints:**By uniquely combining information from Falcon Discover and AWS metadata, security teams are able to baseline existing EC2 deployments instantly across all regions and subsequently monitor cloud trail logs for any modifications to the environment. This holistic asset management across all data centers and AWS cloud resources allows you to identify unmanaged assets — pinpointing security gaps and closing them.

**Prioritizes detections for faster and more effective response:** Falcon Discover for AWS delivers rich AWS metadata on EC2 instances, so that unprotected assets and impacted systems are quickly prioritized. It provides the critical answers analysts need such as: Is this system internet accessible? Does it have Amazon IAM ( identity and access management) roles applied with elevated privileges? Is it on the same Amazon VPC as critical assets? Armed with this context-rich information, organizations can apply proactive measures to dramatically improve their security posture

**Ensures consistent security across hybrid environments:** As organizations move to the cloud, they are implementing hybrid data centers with workloads running on-premises and in the cloud, which can impede a consistent level of security. Falcon Discover for AWS provides visibility across all assets whether they are on-premises or EC2 instances in AWS. In addition, this visibility extends to both managed and unmanaged assets — allowing organizations to quickly ensure that all assets are being protected.

**Conserves resources with easy deployment and integrated management:** Often security teams find they must pivot across a variety of tools and workflows as they attempt to span physical, virtual and cloud environments. Falcon Discover for AWS is one tool that provides instant visibility and control over existing on-premises endpoints and EC2 instances without requiring any additional agents, or installing scripts that can burden teams and slow performance. As a cloud-native security tool, Falcon Discover deploys instantly and scales easily with no hit to performance and no requirement to reboot. It is powered by the Falcon sensor, a single lightweight agent, and managed via the unified Falcon console.

# Architecture diagram

Falcon Discover for Cloud and Containers has read-only access to your EC2 metadata. This minimizes the security impact to your AWS infrastructure. It calls AWS APIs on your behalf using a cross account IAM role, and it also processes [AWS CloudTrail](https://aws.amazon.com/cloudtrail/) logs.

Falcon Discover for Cloud and Containers monitors CloudTrail logs stored in your log archive account S3 bucket. When a new log file is written to the bucket and SNS notification is sent to an SNS topic hosted in a Crowdstrike account. Crowdstrike will require the ability to assume an IAM role that allows the s3:GetObject permissions on the S3 bucket (and all keys) hosting your CloudTrail logs. Crowdstike will analyse the logs in the log file, if an event of interest is found it will make an api call to the account where the log was created and gather information about the resources that have been created.



Figure 1 Crowdstrike Falcon Discover Architecture Diagram

The Customer creates a new account with account factory

An Amazon CloudWatch Event on the master account triggers a lambda function which will create an additional stack that will be applied to the new account. The stack will create an additional IAM role that will allow Crowdstrike to assume a role with the following permissions.   
*"ec2:DescribeInstances",  
"ec2:DescribeImages",   
"ec2:DescribeNetworkInterfaces",  
"ec2:DescribeVolumes",  
"ec2:DescribeVpcs",  
"ec2:DescribeRegions",  
"ec2:DescribeSubnets",  
"ec2:DescribeNetworkAcls",  
"ec2:DescribeSecurityGroups",  
"iam:ListAccountAliases"*

Pre-requisites

Customers will require the following

* Subscription to Falcon Discover for Cloud & Containers OR the Falcon Cloud Workload Protection Bundle
* Subscription to Falcon Insight

The following Parameters will be stored in AWS.

* CSAccountNumber=<Crowdstrike AWS Account Number>
* CSAssumingRoleName=<Crowdstike Assuming Role Name>

Before you implement this solution, we recommend that you become familiar with How to Use an External ID When Granting Access to Your AWS Resources to a Third Party

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html>

If you are new to AWS, see Getting Started with AWS: <https://aws.amazon.com/getting-started/>.

For additional information on AWS Marketplace, see <https://aws.amazon.com/marketplace/help/about-us?ref_=footer_nav_about_aws_marketplace>.

To get started with AWS Control Tower, check out the <https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html>

# <NEED HELP HERE>

# Deployment and Configuration Steps

**Step 1.1: Subscribe to <PARTNER-NAME product-name > on AWS Marketplace.**

Locate the **<PARTNER-SOLUTION NAME>** in the AWS Marketplace (<https://aws-marketplace-link-for-partnerproduct.html>).

<AWS Marketplace Launch Page ScreenShot>

Click on the **Continue to Subscribe** button.



**Step 1.2: Guidance on Contract Duration and Renewal <might vary for each partner>**

In the new screen, you can configure your contract. You can select the **Contract Duration** and set the **Renewal Settings**.

<Contract duration page ScreenShot>

**Step 1.3: Select Contract Options**

Select the Contract Options to be activated with your contract.

<Any Contract Options Screenshot>

**Step 1.4: Create the Contract and Pay**

Once you have configured your contract, you can click on the Create contract button.

<[Optional] – Marketplace Contract creaton screenshot>

You will be prompted to confirm the contract. If you agree to the pricing, select the **Pay Now** button.

**Step 1.5: Set up Account**

If SaaS offering: Customer will be redirected to partner portal. Partner should include any additional steps needed here.

If AMI Offering: Customer would need to deploy some templates provided by partner or quick start. Include the steps.

## Configuration: Set up Additional configuration [SaaS vs AMI]

**Step 2.1: Log into the Partner UI**

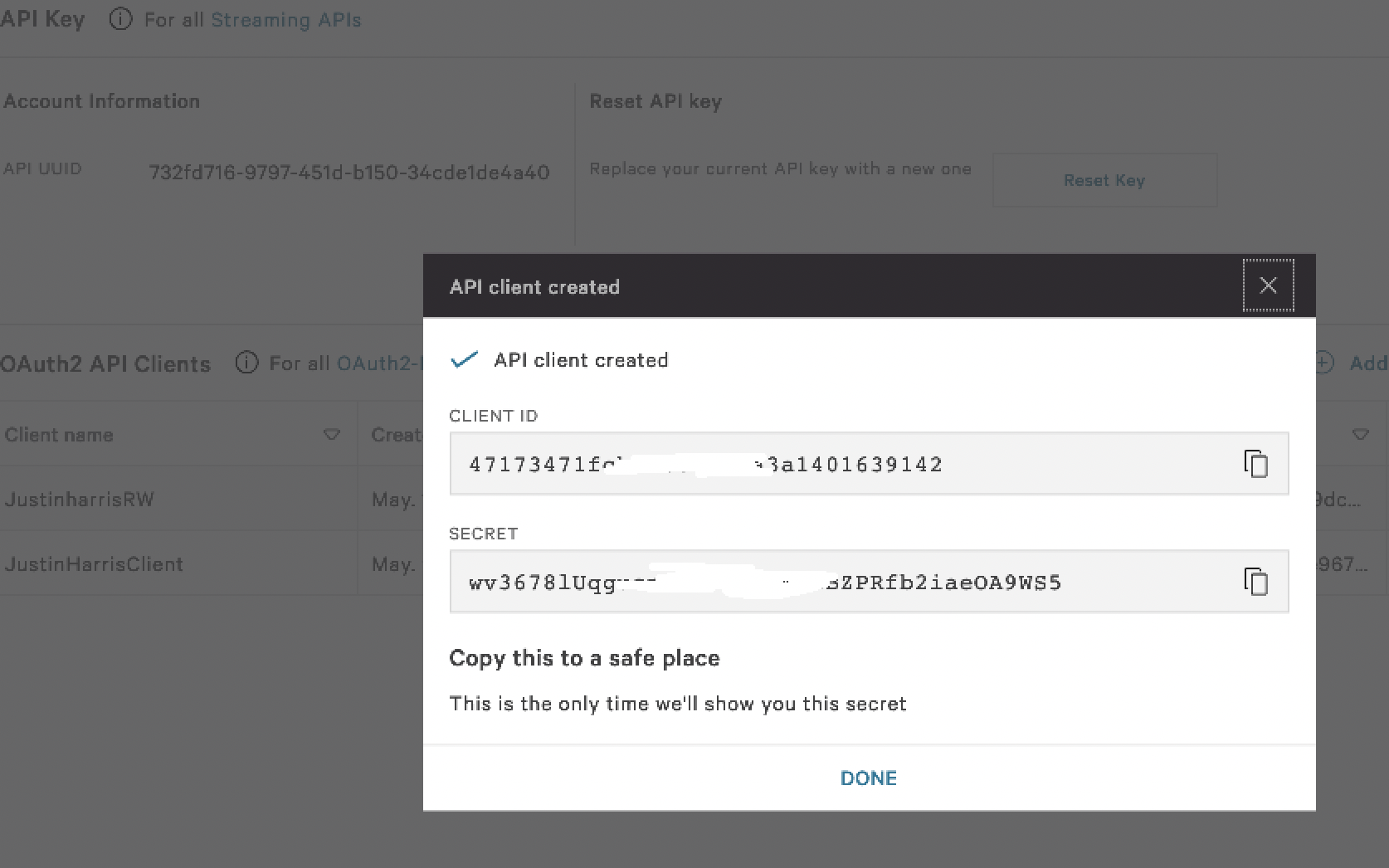
**Step 2.2: Getting Started**

## Configuration: Solution to deploy [if any automation included as part the solution]

**Step 3.1:** Download the code from <Link to our github repository>

Obtain Crowdstrike Falcon Oauth2 keys from the Falcon Console.

Copy the CLIENT ID and SECRET and these will be used in the template.



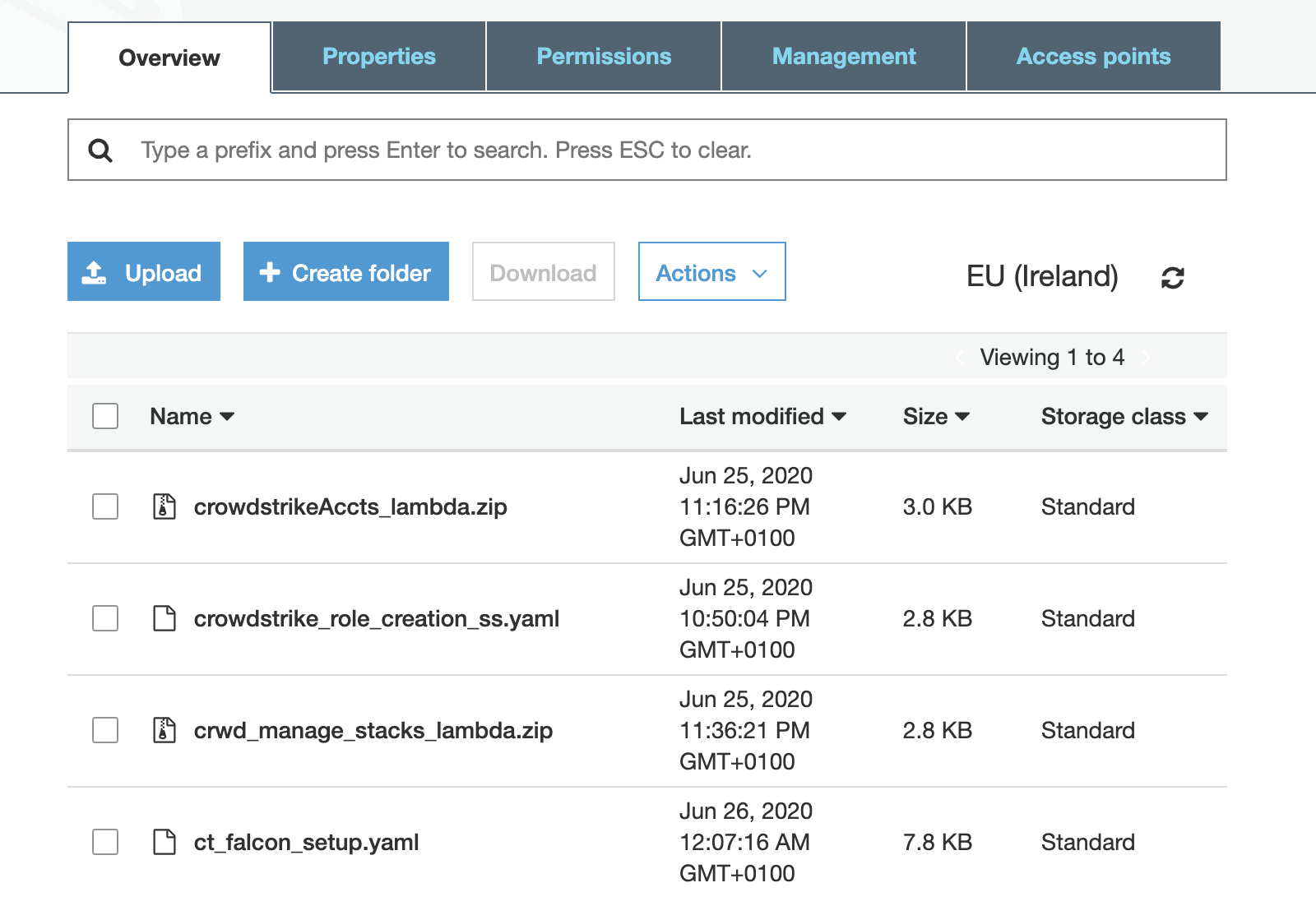
Goto the log archive account in Control Tower and make a note of the account number and bucket name.

**Step 3.2:** Login in to MASTER account in AWS Control Tower and deploy the solution

First create an S3 bucket to store the deployment files.

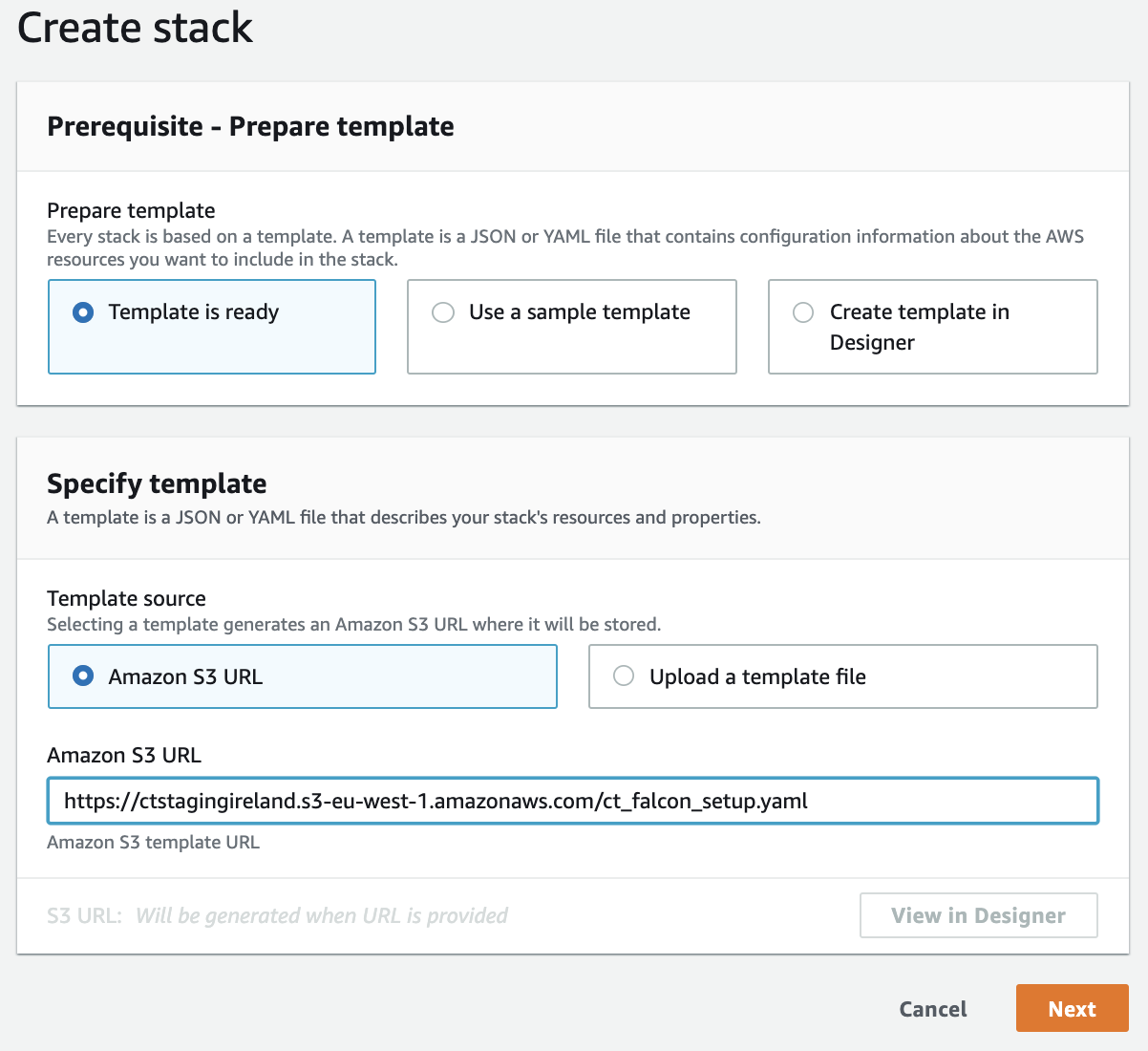
***Create an S3 bucket and upload the files***

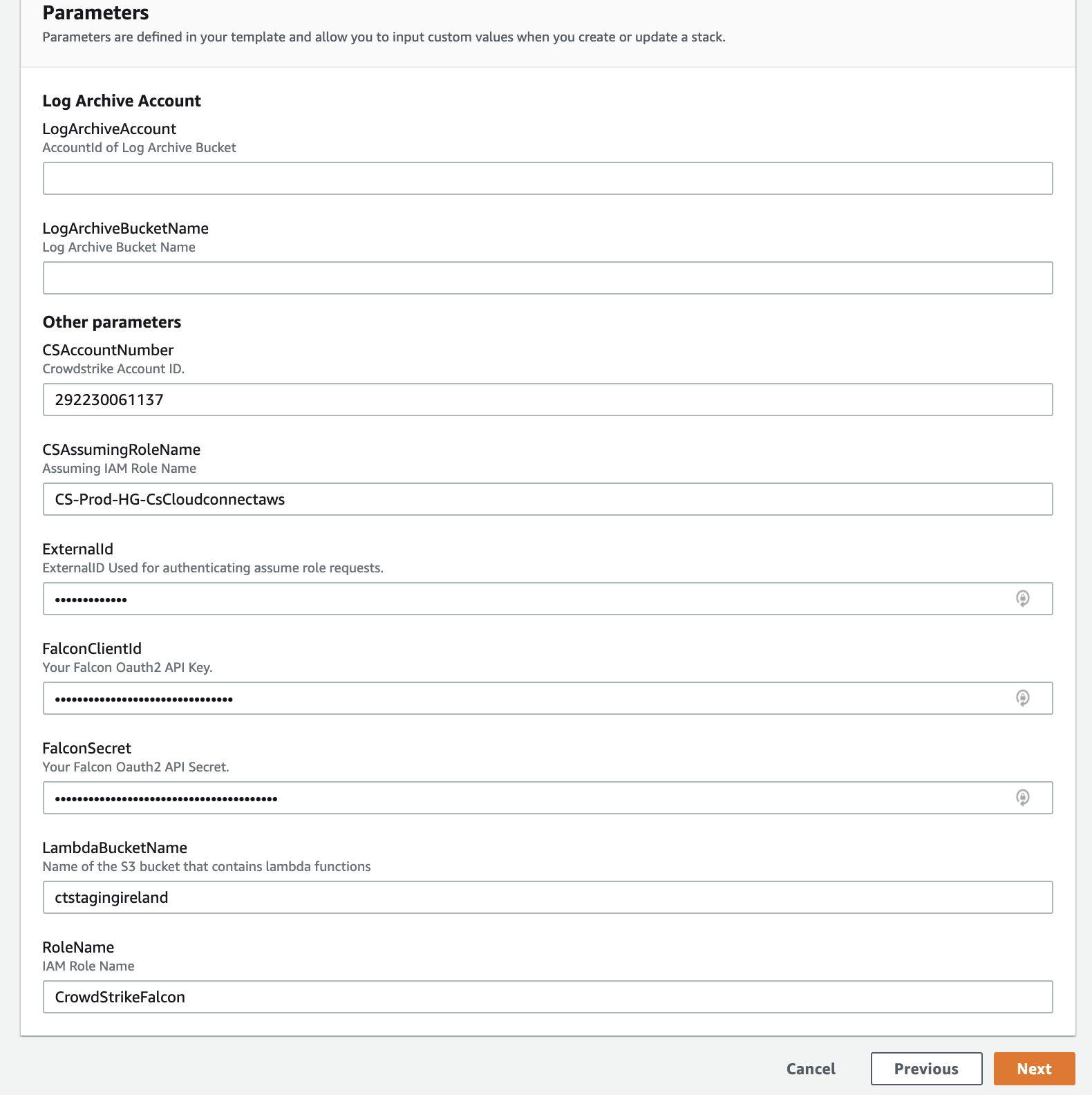
1. ct\_falcon\_setup.yaml
2. crwd\_manage\_stacks\_lambda.zip
3. crowdstrikeAccts\_lambda.zip
4. [crowdstrike\_role\_creation\_ss.yaml](https://ctstagingireland.s3-eu-west-1.amazonaws.com/crowdstrike_role_creation_ss.yaml)



***Load the Cloudformation Template.***

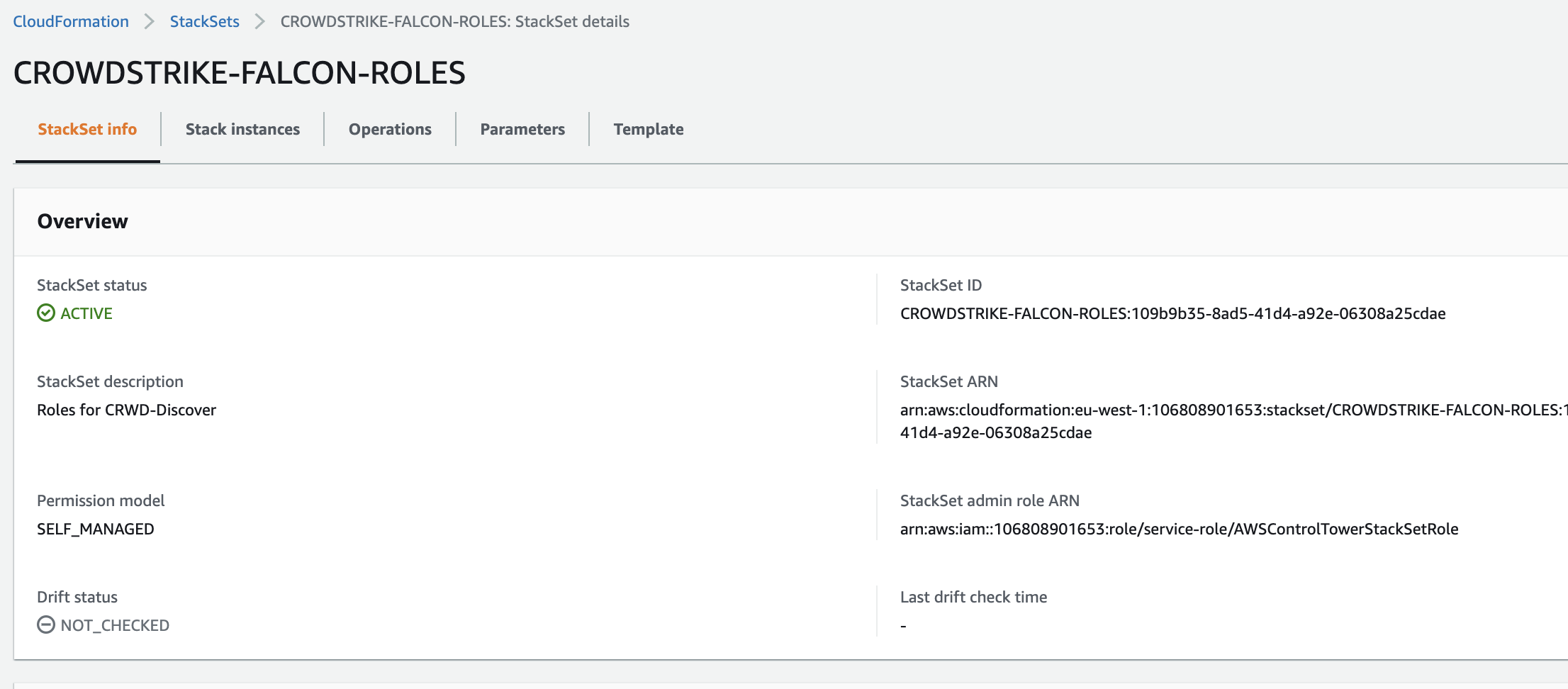
Copy the URL for ct\_falcon\_setup.yaml and load the template



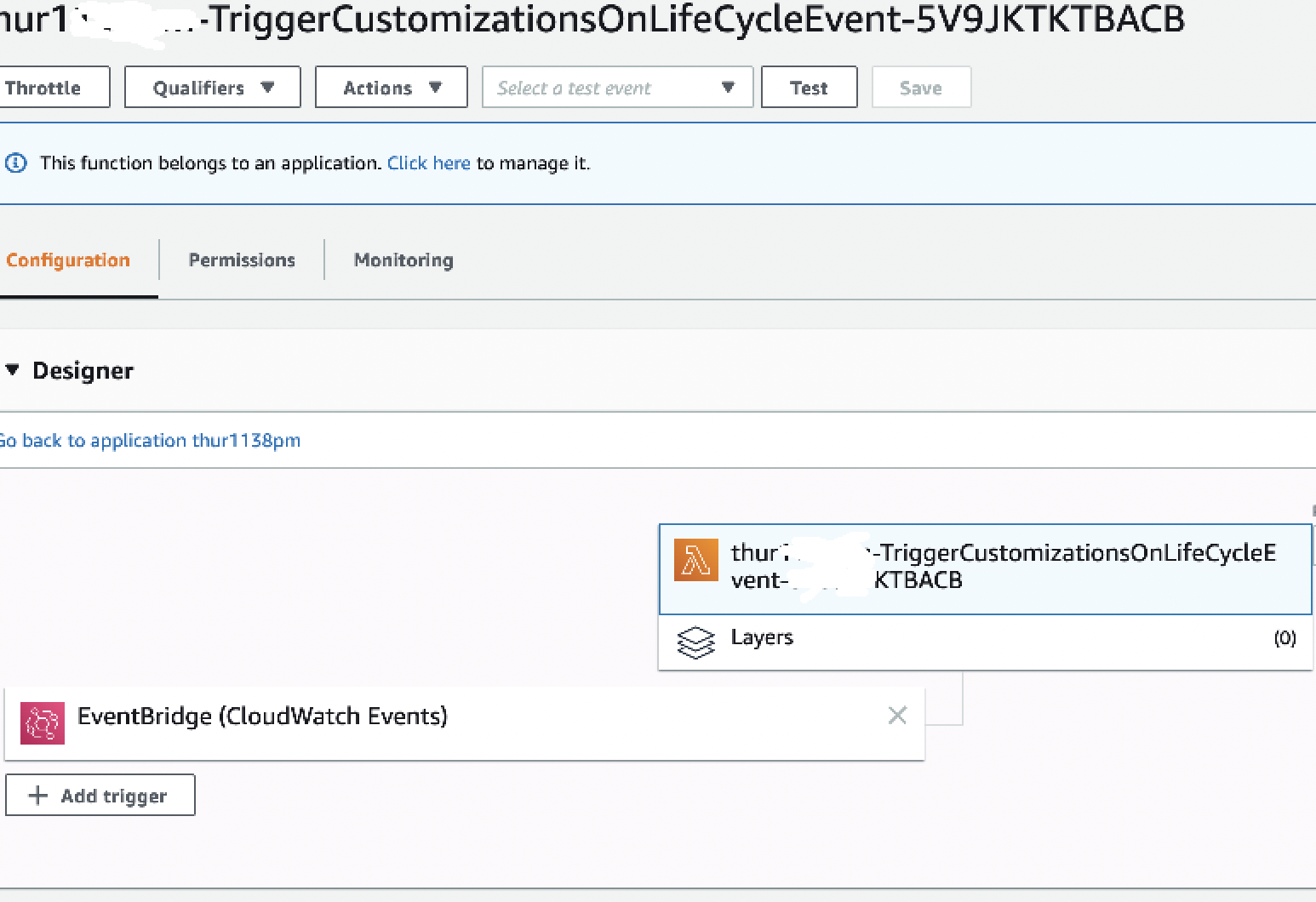


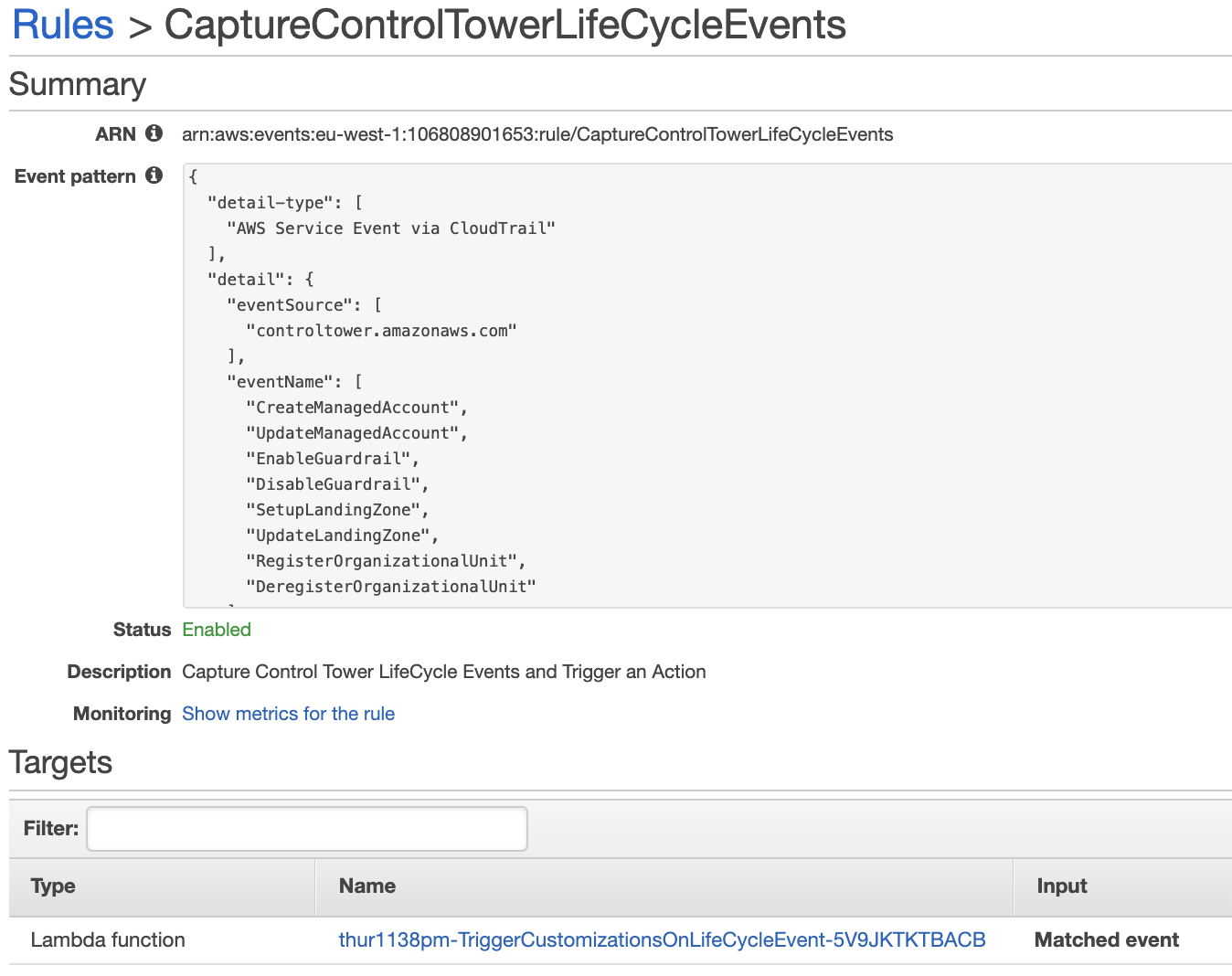
**Step 3.3:** Verification Steps

## The cloudformation template will create a stackset named CROWDSTRIKE-FALCON-ROLES



## The cloudformation template will create a lambda function that is triggered by Cloudwatch Events





**Step 4.1:** Any steps to validate that solution is properly deployed

**Step 4.2:** How to use

Call out a common example if possible. Example: If the solution is based on logging, walkthrough few ways of check Control Tower operational information.

Best Practices

Solution Estimated Pricing

FAQs

Additional resources

Partner contact information