**Implementation Guide:**

**CrowdStrike Falcon Discover for Cloud**

Table of Contents

[Foreword 3](#_Toc44430235)

[Solution overview and features 4](#_Toc44430236)

[Benefits of CrowdStrike Discover for Cloud and Containers 4](#_Toc44430237)

[Architecture diagram 5](#_Toc44430238)

[Pre-requisites 6](#_Toc44430239)

[Deployment and Configuration Steps 7](#_Toc44430240)

[**Configuration: Solution to deploy** 9](#_Toc44430241)

[The cloud formation template will create a stackset named CROWDSTRIKE-FALCON-ROLES 16](#_Toc44430242)

[The cloud formation template will create a lambda function that is triggered by Cloudwatch Events. 16](#_Toc44430243)

[Additional resources 17](#_Toc44430244)

[Partner contact information 18](#_Toc44430245)

# Foreword

With [CrowdStrike Discover for Cloud and Containers](https://www.crowdstrike.com/cloud-security-products/falcon-cloud-workload-protection/) you can gain immediate and comprehensive visibility into all managed endpoints equipped with CrowdStrike Falcon workload security, and unmanaged assets across all accounts. In addition, Discover for Cloud and Containers is able to cross boundaries to see Amazon Virtual Private Cloud (Amazon VPC) and subnets, and collect data from all endpoints — even those that are unmanaged — as well as all hybrid infrastructures. The rich AWS content Discover for Cloud and Containers allows organizations to quickly understand and prioritize instances and immediately ensure that the Falcon sensor is fully deployed, dramatically improving organizations’ security postures.

The purpose of this Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure CrowdStrike Discover for Cloud and Containers 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 CrowdStrike** Discover for Cloud and Containers

CrowdStrike Discover for Cloud and Containers offers streamlined integration not available with other third-party solutions. This integration saves organizations the time and expense of trying to develop these capabilities in-house. Discover for Cloud and Containers offers the following benefits:

* **Identifies security gaps with comprehensive and consistent visibility across all** [Amazon Elastic Compute Cloud (Amazon EC2)](https://aws.amazon.com/ec2/) **instances and endpoints:**By uniquely combining information from Discover for Cloud and Containers and AWS metadata, security teams are able to baseline existing Amazon EC2 deployments instantly across all regions and subsequently monitor [AWS CloudTrail](https://aws.amazon.com/cloudtrail/) logs for any modifications to the environment. This holistic asset management across entire data center and AWS cloud resources allows you to identify unmanaged assets — pinpointing security gaps and closing them.
* **Prioritizes detections for faster and more effective response:** Discover for Cloud and Containers 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 [AWS Identity and Access Management (IAM)](https://aws.amazon.com/iam/) 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 center with workloads running on-premises and in the cloud, which can impede a consistent level of security. Discover for Cloud and Containers 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. Discover for Cloud and Containers 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, Discover for Cloud and Containers deploys instantly and scales easily with no hit to performance and no requirement to reboot. It is powered by the [Falcon sensor](https://www.crowdstrike.com/endpoint-security-products/falcon-for-aws/), 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 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 hosting your CloudTrail logs. CrowdStrike 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.

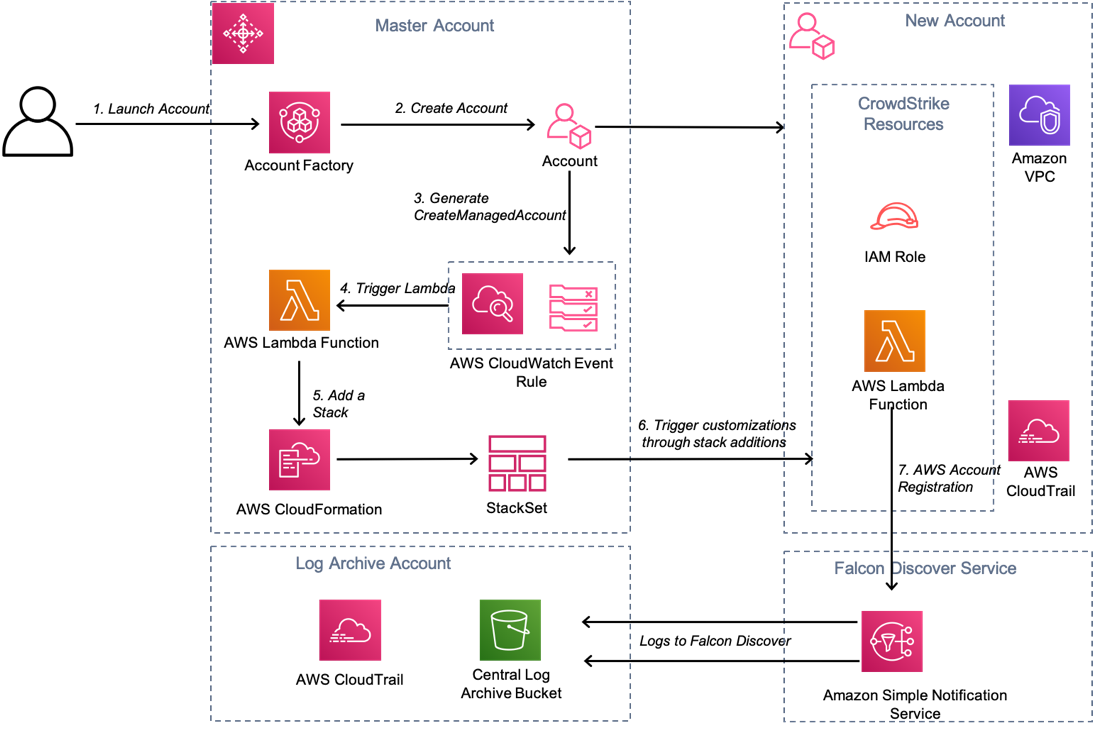


Figure 1 CrowdStrike Falcon Discover for Cloud and Containers Architecture Diagram

The Customer creates a new account using [Account Factory](https://docs.aws.amazon.com/controltower/latest/userguide/account-factory.html) with in AWS Control Tower Master account.

Account factory creates a new AWS account and applies baselines and guardrails on the newly created account.

On completion of account creation a CreateManagedAccount is generated

The CloudWatch event rule triggers a Lambda function that will generate account specific parameters

The custom parameters are passed to the StackSet that is applied to the new account.

The stack creates an additional IAM role and a Lambda custom resource. The role 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"*

The custom Lambda resource will register the account with CrowdStrike Discover for Cloud using an API call. The role arn together with details of the log archive s3 bucket are passed in a HTTP POST to the api.

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 secrets manager in the master account.

* Falcon Cloud API ClientID
* Falcon Cloud API Client Secret

Crowdstrike will pass an ExternalID as an additional authentication mechanism when trying to assume a role in the log archive account to read the log files, we recommend that you become familiar with the following article.

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/>.

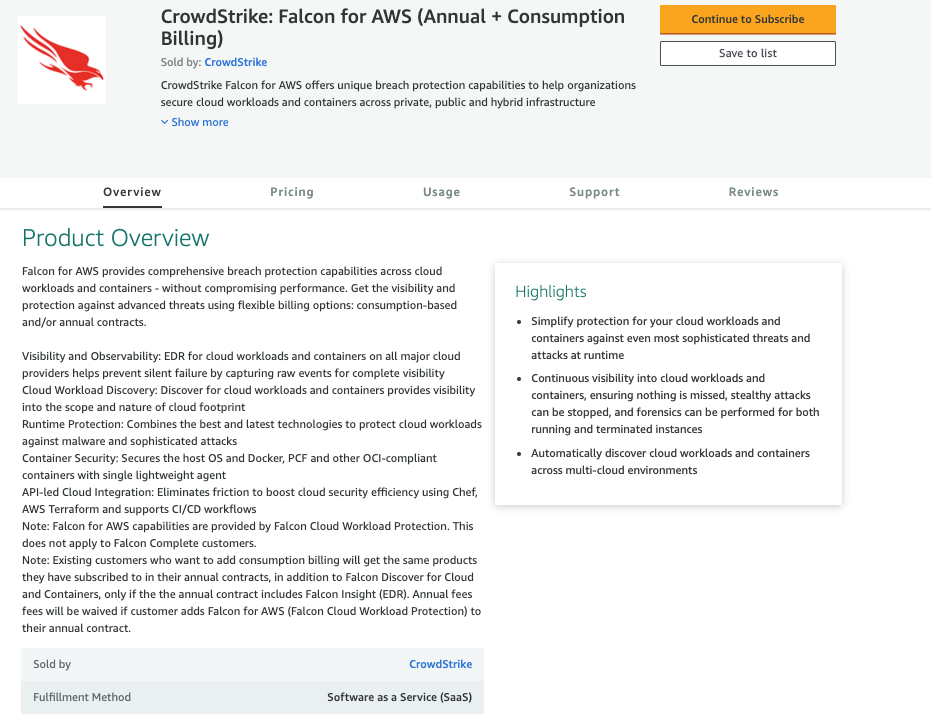
For additional information on AWS Marketplace, see <https://aws.amazon.com/marketplace/help/about-us?ref_=footer_nav_about_aws_marketplace>.

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

# Deployment and Configuration Steps

**Step 1.1: Subscribe to Falcon for AWS (Annual + Consumption Billing) on AWS Marketplace.**

Locate the **AWS (Annual + Consumption Billing)** in the AWS Marketplace (<https://aws.amazon.com/marketplace/pp/B081QWWMB6?qid=1593190522787&sr=0-7&ref_=srh_res_product_title>).

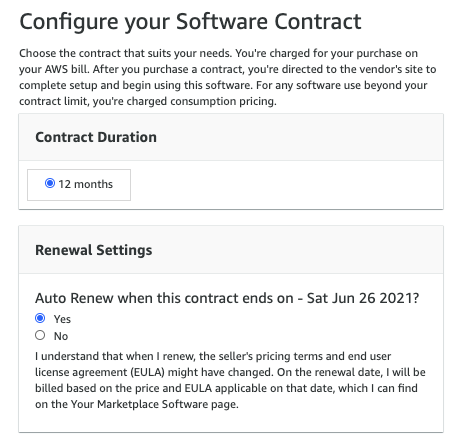


Click on the **Continue to Subscribe** button.



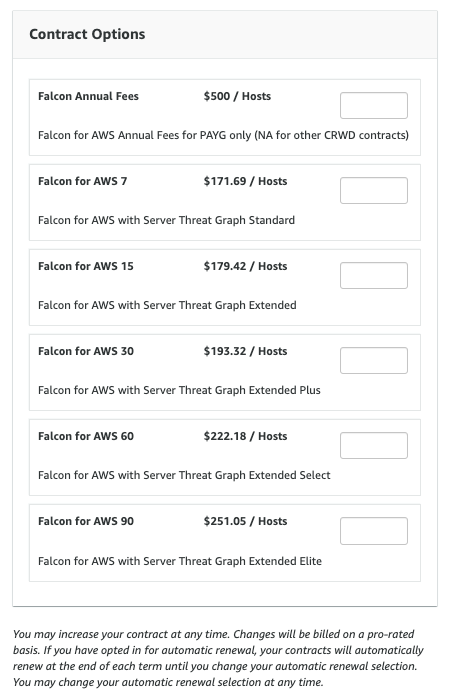
**Step 1.2: Guidance on Contract Duration and Renewal**

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



**Step 1.3: Select Contract Options**

Select the Contract Options to be activated with your contract.



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

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

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

## **Configuration: Solution to deploy**

Setup will consist of the following tasks.

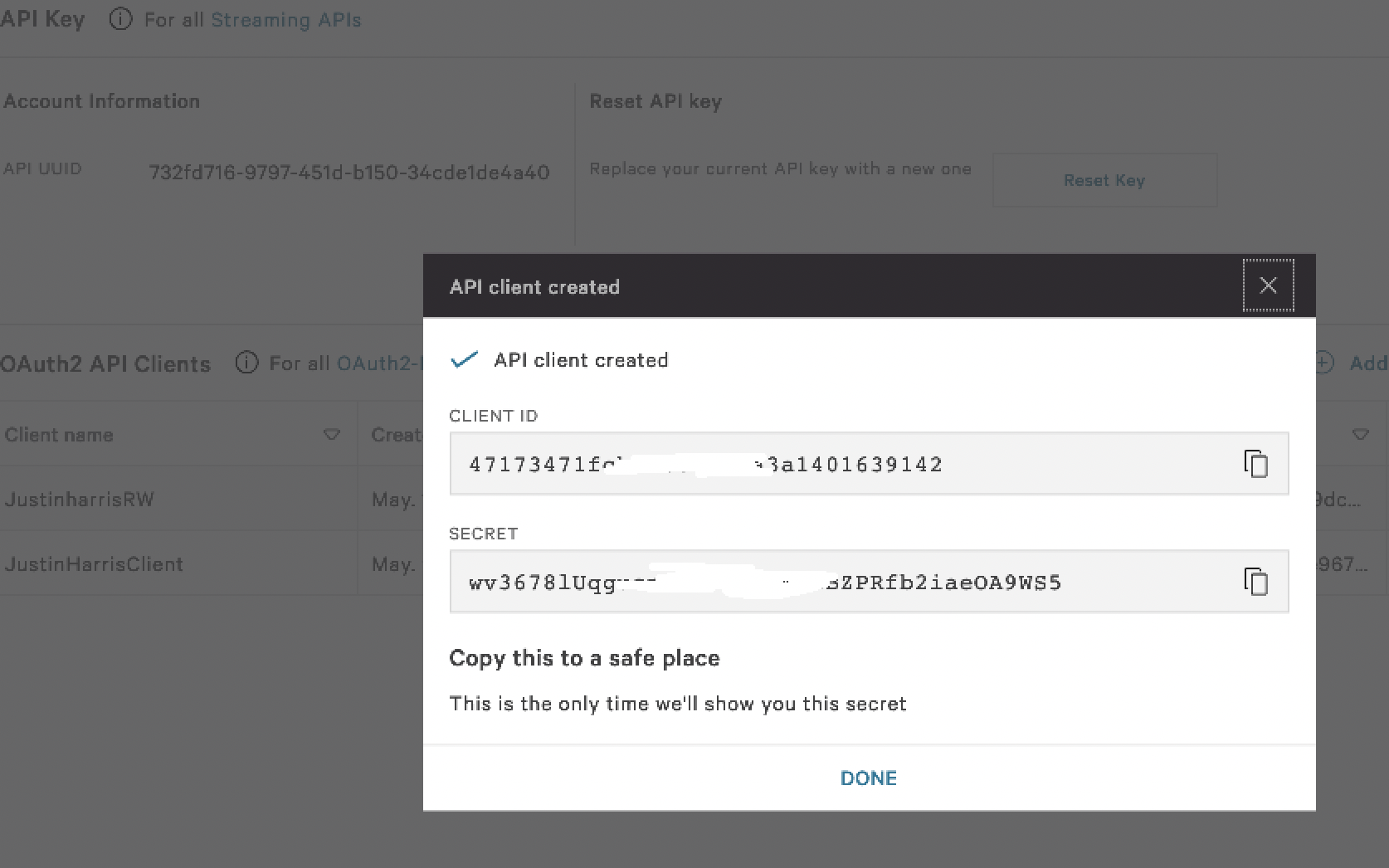
1. Download the code from the GitHub repository to a local machine that has access to the control tower master account and the control tower log archive account.
2. Create an S3 staging bucket in the log-archive account
3. Load the CloudFormation template in the log-archive account.
4. Create an S3 staging bucket in the master account.
5. Load the CloudFormation template in the master account.

**Step 3.1:** Generate Crowdstrike Falcon API Keys

First login to the Crowdstrike console and go to Support -> “API Clients and Keys”

Obtain CrowdStrike Falcon Oauth2 keys from the Falcon Console.

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



**Step 3.2:** Download the code from <https://github.com/jhseceng/control-tower>

The GitHub repository contains the following folder structure.

* log-archive-acct – Folder containing all the files required to deploy the CloudFormation template in the Control Tower log-archive account
* master-acct - Folder containing all the files required to deploy the CloudFormation template in the Control Tower master account
* src – Folder containing the lambda source files
* Documentation – Documentation folder

A file named ‘create\_staging\_bucket’ is also included to assist with the setup of the required S3 buckets.

**Step 3.2:** Create an S3 staging bucket in the log-archive account

Navigate to the root of the folders downloaded from github.

master % ls -al

total 24

drwxrwxr-x@ 8 jharris staff 256 5 Jul 01:14 .

drwx------@ 151 jharris staff 4832 5 Jul 01:20 ..

-rw-rw-r--@ 1 jharris staff 625 5 Jul 01:14 README.md

-rw-rw-r--@ 1 jharris staff 4922 5 Jul 01:14 create\_staging\_bucket.py

drwxrwxr-x@ 3 jharris staff 96 5 Jul 01:14 documentation

drwxrwxr-x@ 6 jharris staff 192 5 Jul 01:14 log-archive-acct

drwxrwxr-x@ 9 jharris staff 288 5 Jul 01:14 master-acct

drwxrwxr-x@ 4 jharris staff 128 5 Jul 01:14 src

The python script takes a number of mandatory and optional arguments

jharris@ML-C02ZP8ZVMD6P control-tower-master % python3 create\_staging\_bucket.py -h

usage: create\_staging\_bucket.py [-h] -r AWS\_REGION [-b S3BUCKET] -a {master-acct,log-archive-acct}

Get Params to create lambda bucket

optional arguments:

-h, --help show this help message and exit

-r AWS\_REGION, --aws\_region AWS\_REGION

-b S3BUCKET, --s3bucket S3BUCKET

<S3 Bucket Name> Optional will default to "crowdstrike-staging-<account>-account-xxx where xxx is a random string"

-a {master-acct,log-archive-acct}, --account {master-acct,log-archive-acct}

Account where the bucket will be created, choices=['master-acct', 'log-archive-acct'],

Run the python script python3 create\_staging\_bucket.py -r <region> -a log-archive-acct -b <optional bucket name>

The script will print the files uploaded and the name of the s3 bucket created

Uploading file log-archive-acct/add\_S3\_notification.zip:

Uploading file log-archive-acct/register\_logarchive\_account.zip:

Uploading file log-archive-acct/layer.zip:

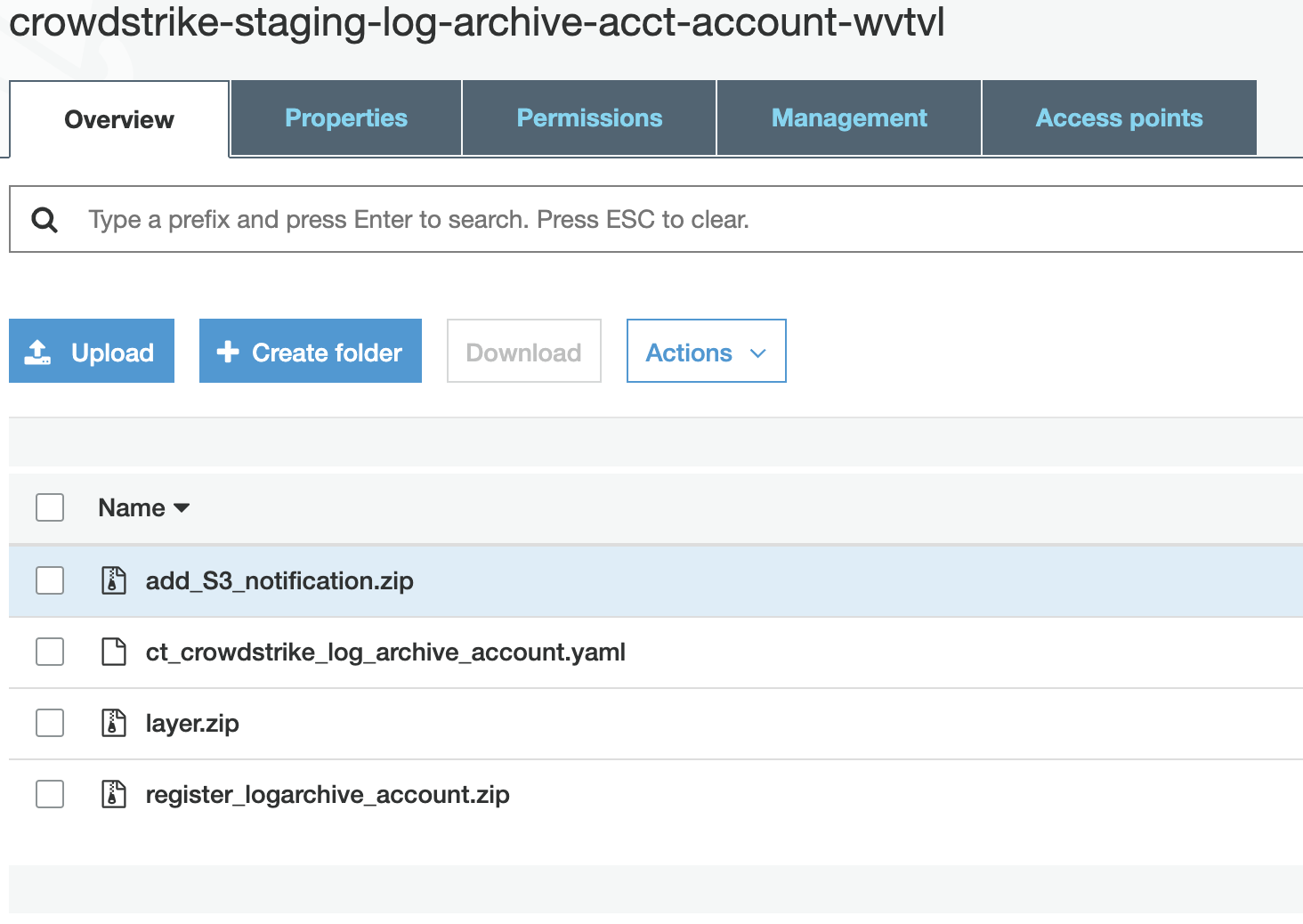
Setting file layer.zip ACL to public-read

Uploading file log-archive-acct/ct\_crowdstrike\_log\_archive\_account.yaml:

#### Created S3 Bucket crowdstrike-staging-log-archive-acct-account-wvtvl

### Use this bucket name as the Lambda bucket name in your template

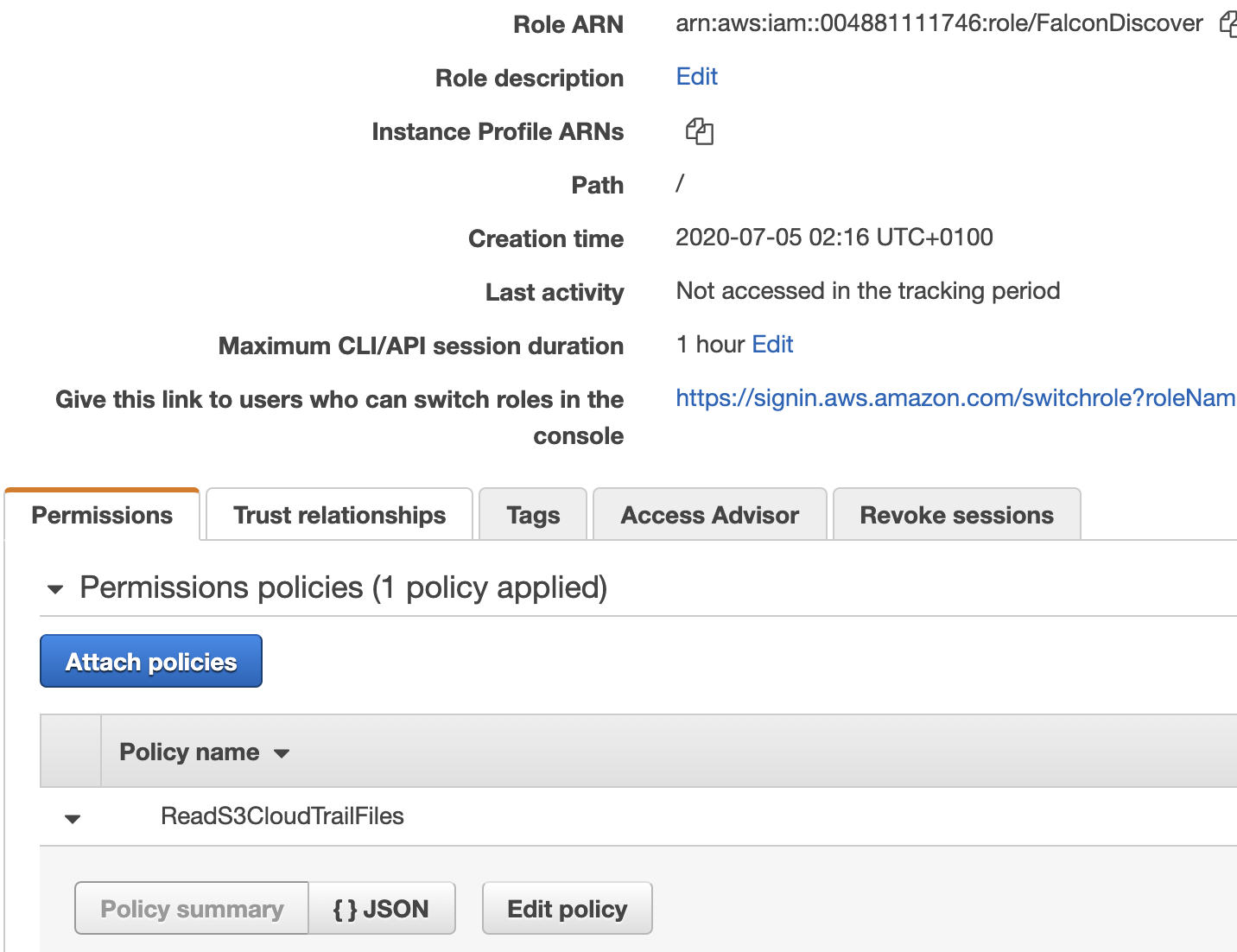
Go to the log archive account in AWS Control Tower and make a note of the account number and verify the contents of the S3 bucket.

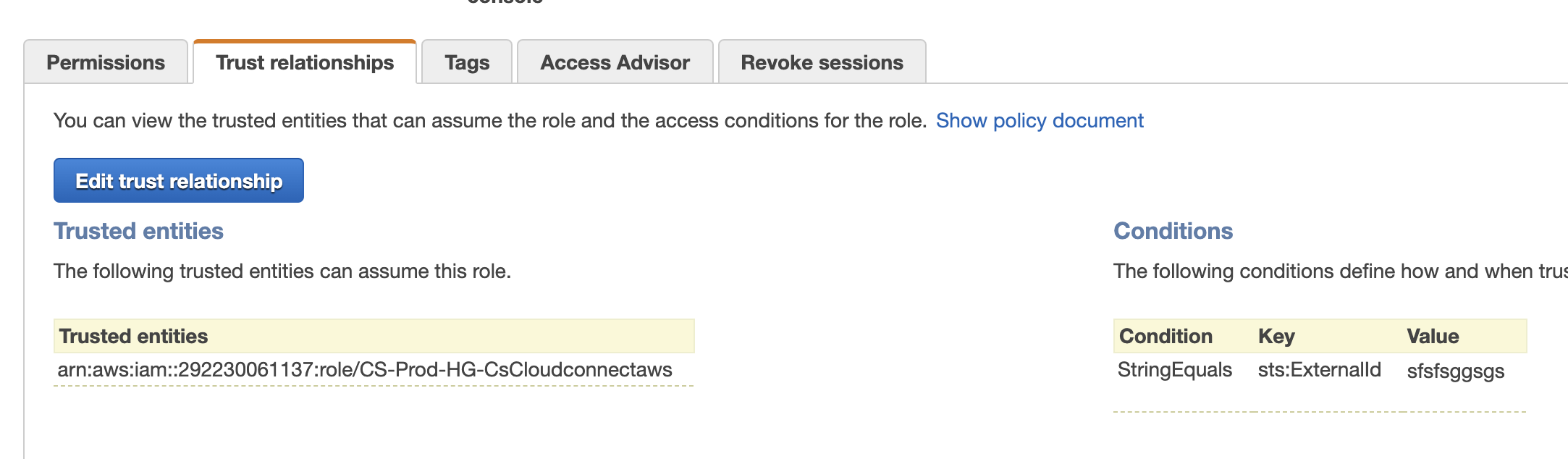


**Step 3.3:** Load the CloudFormation template in the log-archive account

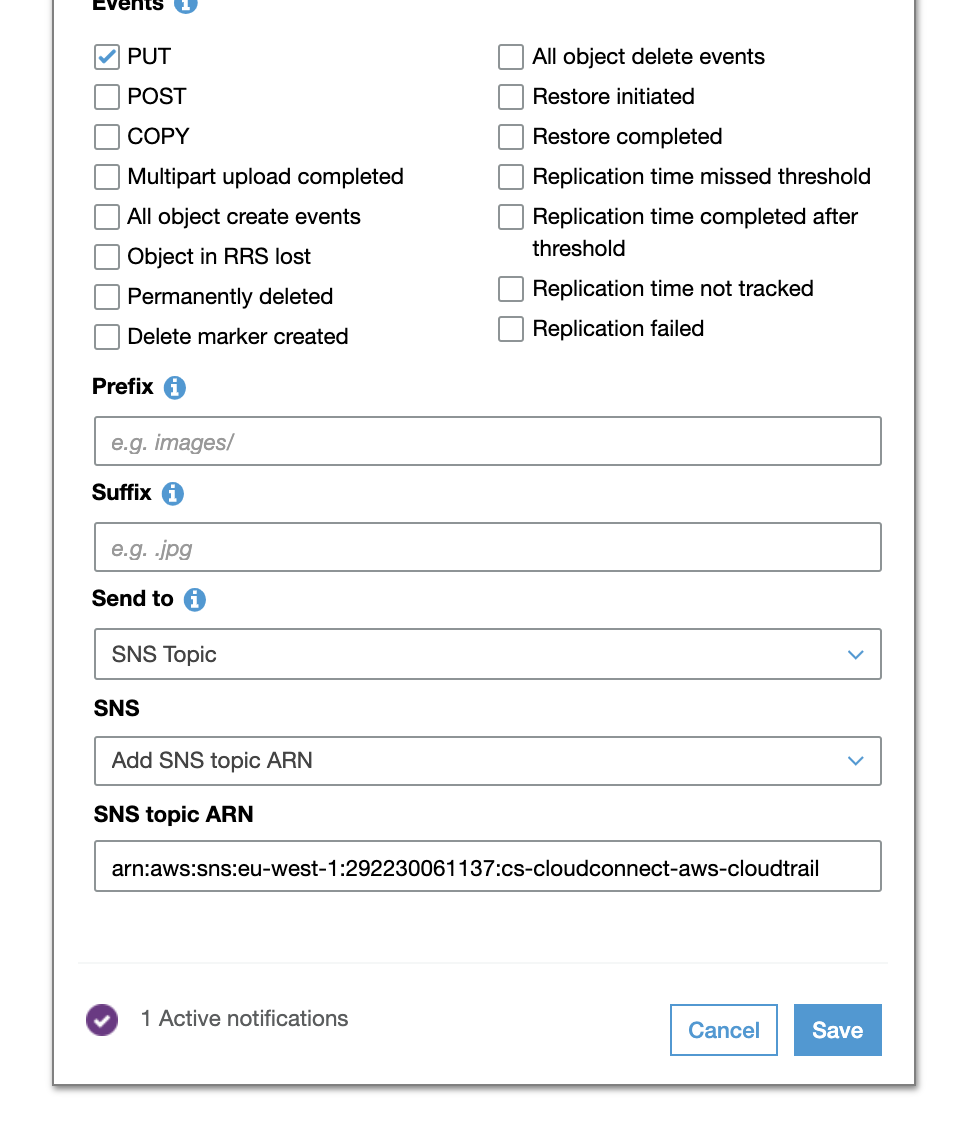
Go to the audit account and apply the CloudFormation template “ct\_crowdstrike\_log\_archive\_account.yaml”.

The CloudFormation template will create a Role name “FalconDiscover” in the log archive account that will permit read access to objects in the s3 bucket. The role is restricted so that only the IAM role “a*rn:aws:iam::292230061137:role/CS-Prod-HG-CsCloudconnectaws”* can assume the role in the account to read the log files.





The template will also create an S3 bucket event notification that will send an SNS notification to the Crowdstrike SNS topic “arn:aws:sns:(region):292230061137:cs-cloudconnect-aws-cloudtrail”



**Step 3.4:** Create an S3 staging bucket in the Control Tower master account

Navigate to the root of the folders downloaded from github.

master % ls -al

total 24

drwxrwxr-x@ 8 jharris staff 256 5 Jul 01:14 .

drwx------@ 151 jharris staff 4832 5 Jul 01:20 ..

-rw-rw-r--@ 1 jharris staff 625 5 Jul 01:14 README.md

-rw-rw-r--@ 1 jharris staff 4922 5 Jul 01:14 create\_staging\_bucket.py

drwxrwxr-x@ 3 jharris staff 96 5 Jul 01:14 documentation

drwxrwxr-x@ 6 jharris staff 192 5 Jul 01:14 log-archive-acct

drwxrwxr-x@ 9 jharris staff 288 5 Jul 01:14 master-acct

drwxrwxr-x@ 4 jharris staff 128 5 Jul 01:14 src

The python script takes a number of mandatory and optional arguments

jharris@ML-C02ZP8ZVMD6P control-tower-master % python3 create\_staging\_bucket.py -h

usage: create\_staging\_bucket.py [-h] -r AWS\_REGION [-b S3BUCKET] -a {master-acct,log-archive-acct}

Get Params to create lambda bucket

optional arguments:

-h, --help show this help message and exit

-r AWS\_REGION, --aws\_region AWS\_REGION

-b S3BUCKET, --s3bucket S3BUCKET

<S3 Bucket Name> Optional will default to "crowdstrike-staging-<account>-account-xxx where xxx is a random string"

-a {master-acct,log-archive-acct}, --account {master-acct,log-archive-acct}

Account where the bucket will be created, choices=['master-acct', 'log-archive-acct'],

Run the python script python3 create\_staging\_bucket.py -r <region> -a master-acct -b <optional bucket name>

The script will print the files uploaded and the name of the s3 bucket created

Uploading file master-acct/ct\_crowdstrike\_master\_account.yaml:

Uploading file master-acct/crowdstrikeAccts\_lambda.zip:

Uploading file master-acct/create\_stackset\_lambda.zip:

Uploading file master-acct/layer.zip:

**Setting file layer.zip ACL to public-read**

Uploading file master-acct/ct\_crowdstrike\_stackset.yaml:

**Setting file ct\_crowdstrike\_stackset.yaml ACL to public-read**

Uploading file master-acct/register\_new\_account.zip:

Uploading file master-acct/add\_stackset\_to\_acct\_lambda.zip:

#### Created S3 Bucket crowdstrike-staging-master-acct-account-8t8q6

### Use this bucket name as the Lambda bucket name in your template

***Note: Two files were created with “public-read” permissions. These permissions are required as they are zip files that are required by the stackset that is pushed to new accounts created in account factory.***

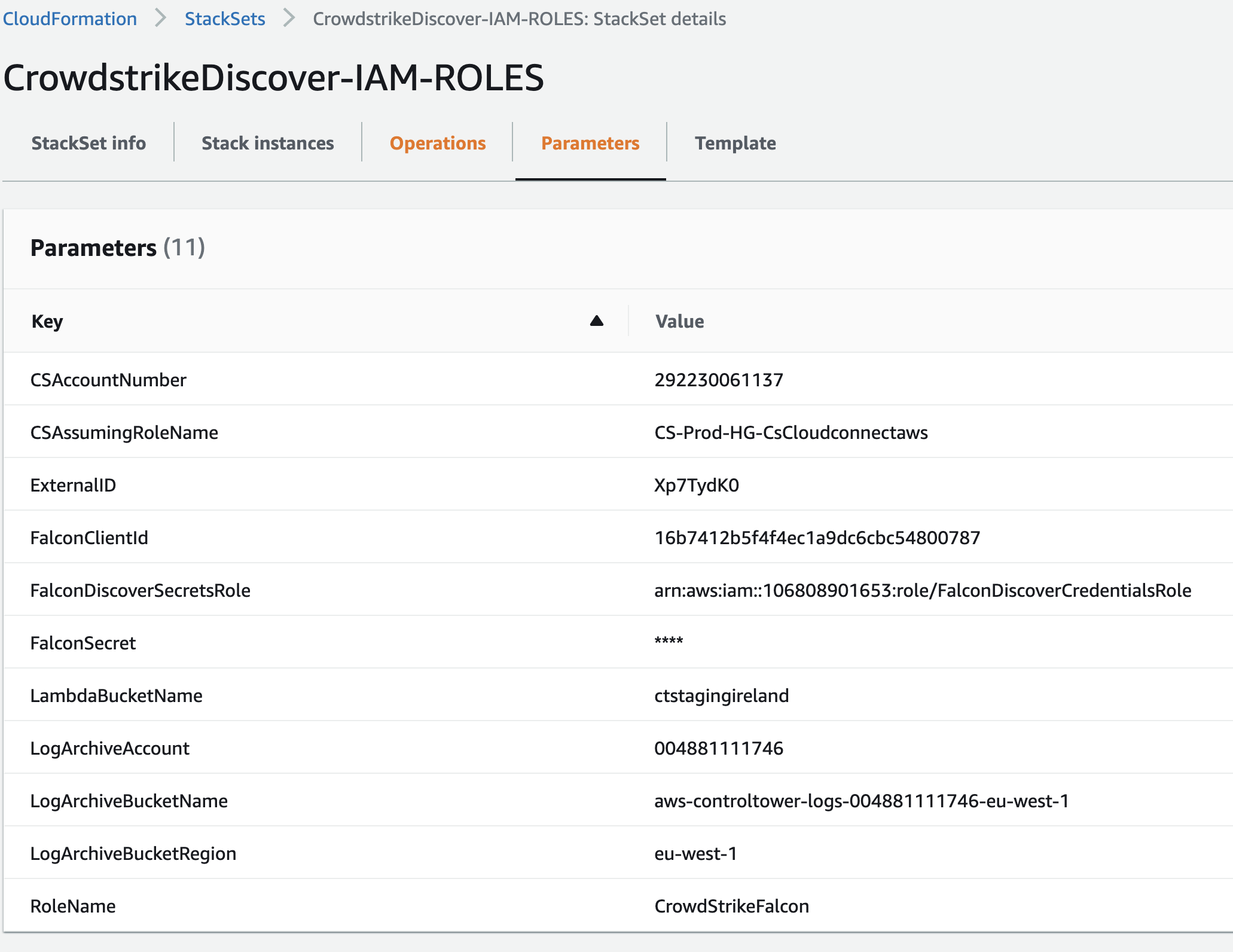
Go to the log archive account in AWS Control Tower and make a note of the account number and verify the contents of the S3 bucket.

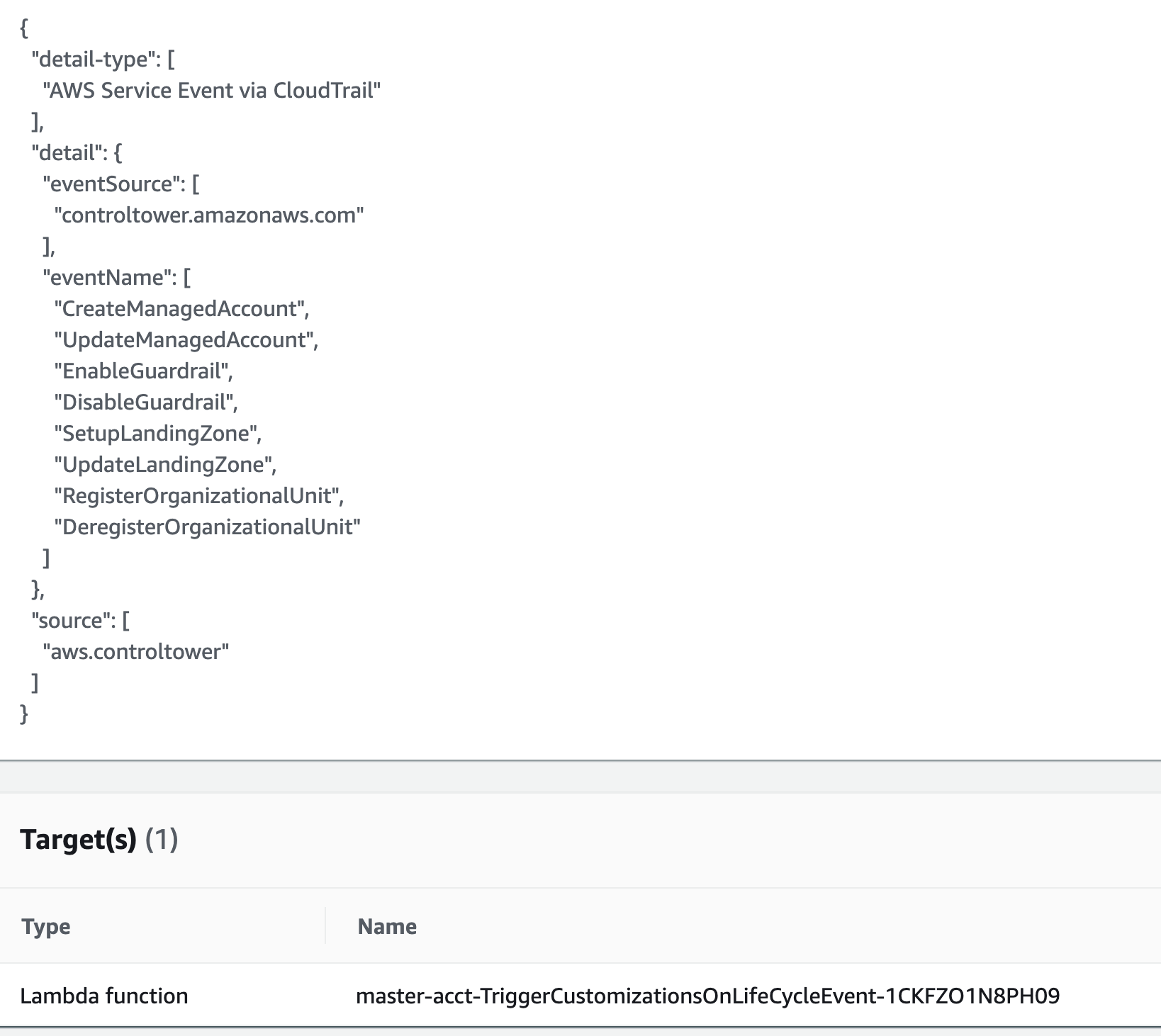
**Step 3.5:** Load the CloudFormation template in the master account

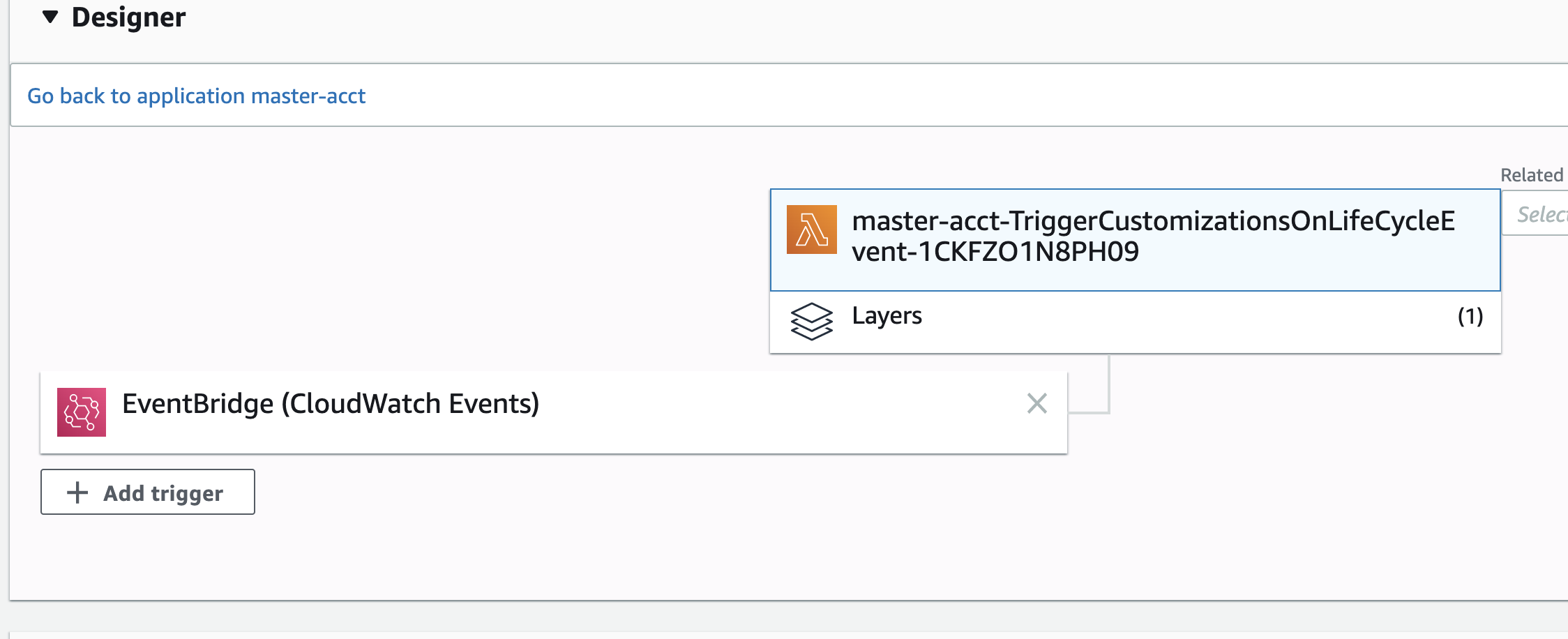
Go to the master account and apply the CloudFormation template *“ct\_crowdstrike\_master\_account.yaml”*.

The CloudFormation template will create the following resources in the account

* Stackset that will be applied to new accounts



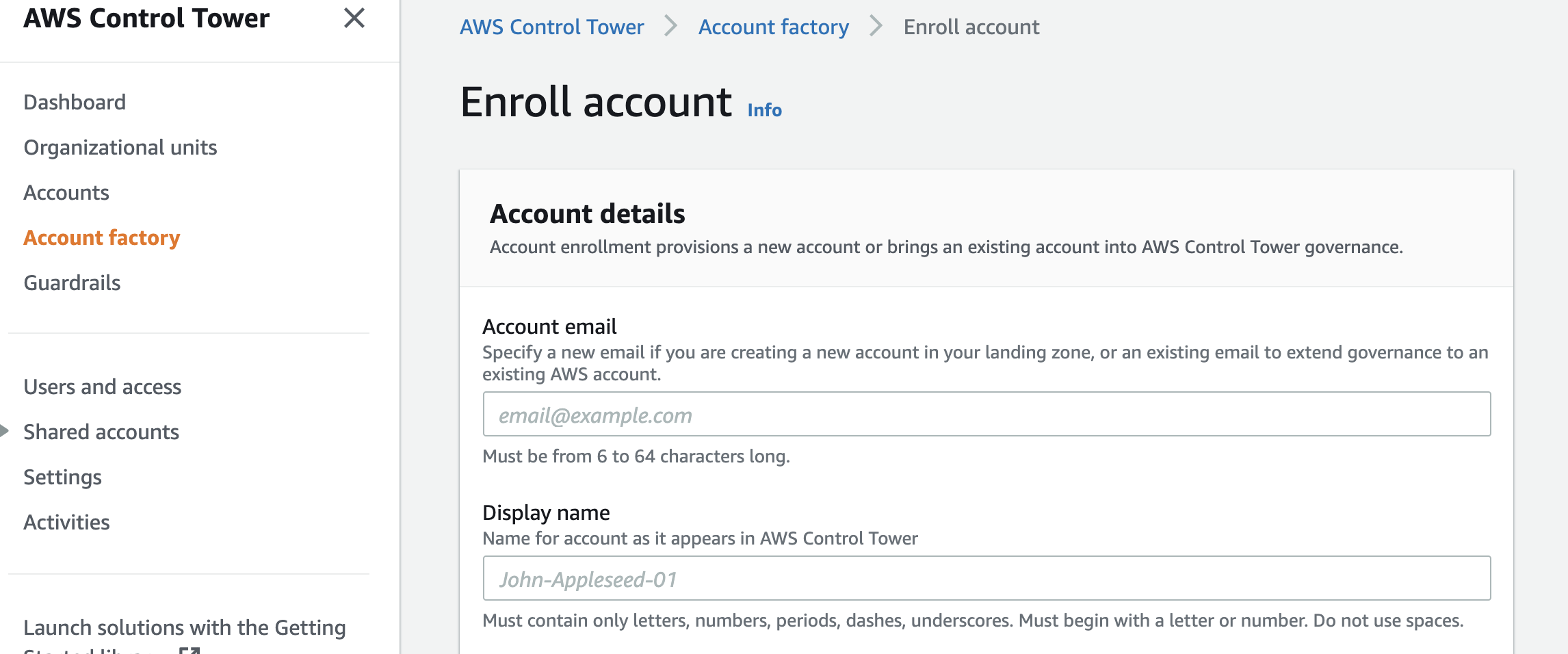
* Cloudwatch rule to trigger a lambda function  
  
* Lambda function triggered by CloudWatch to push the StackSet to a new account



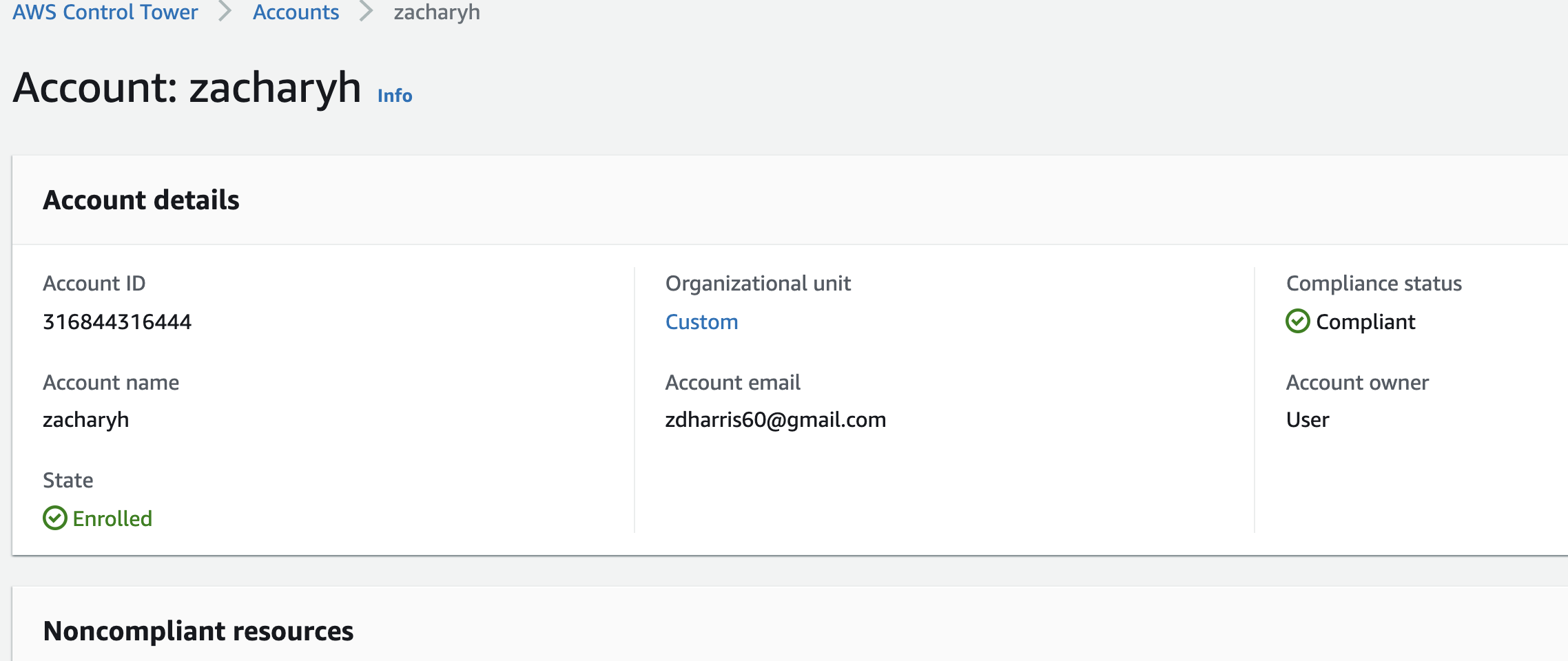
* Lambda function to register the master account with Crowdstrike Falcon

**Step 3.6:** Verification Steps

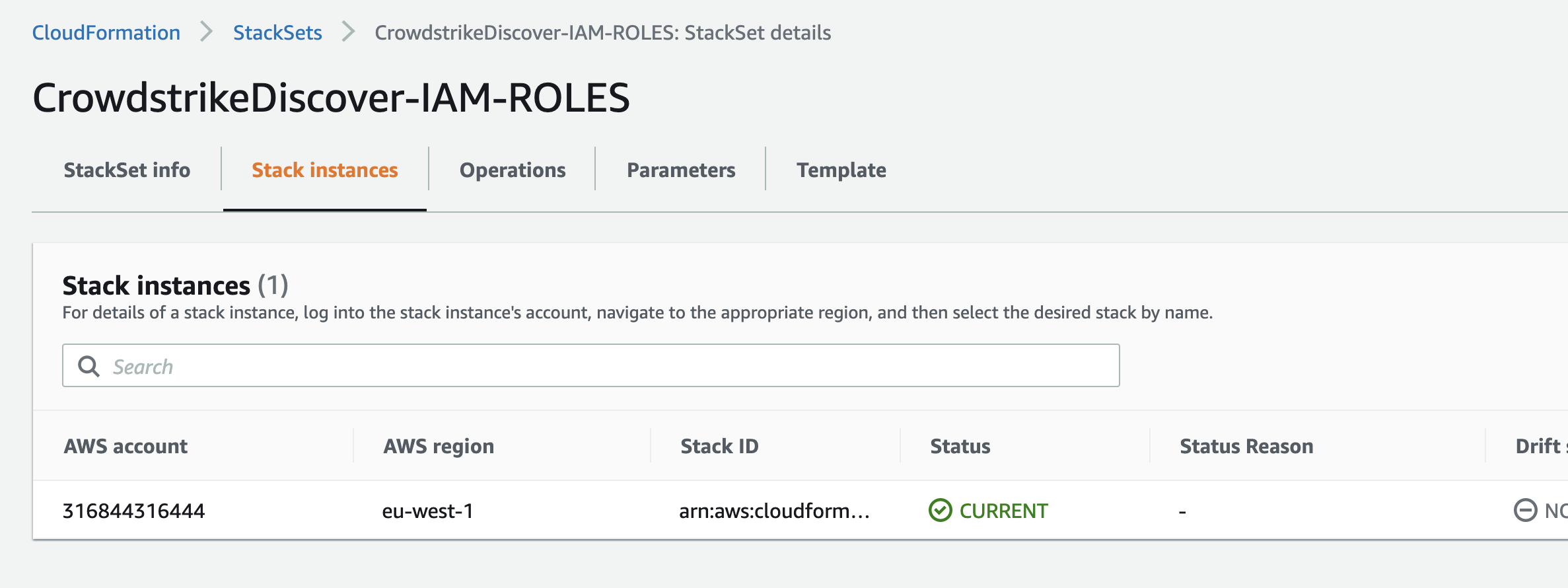
## Create a new account in account factory



Once the account has been created check that status of the account



Goto Cloudformation -> StackSets and verify that a stack instance exists.

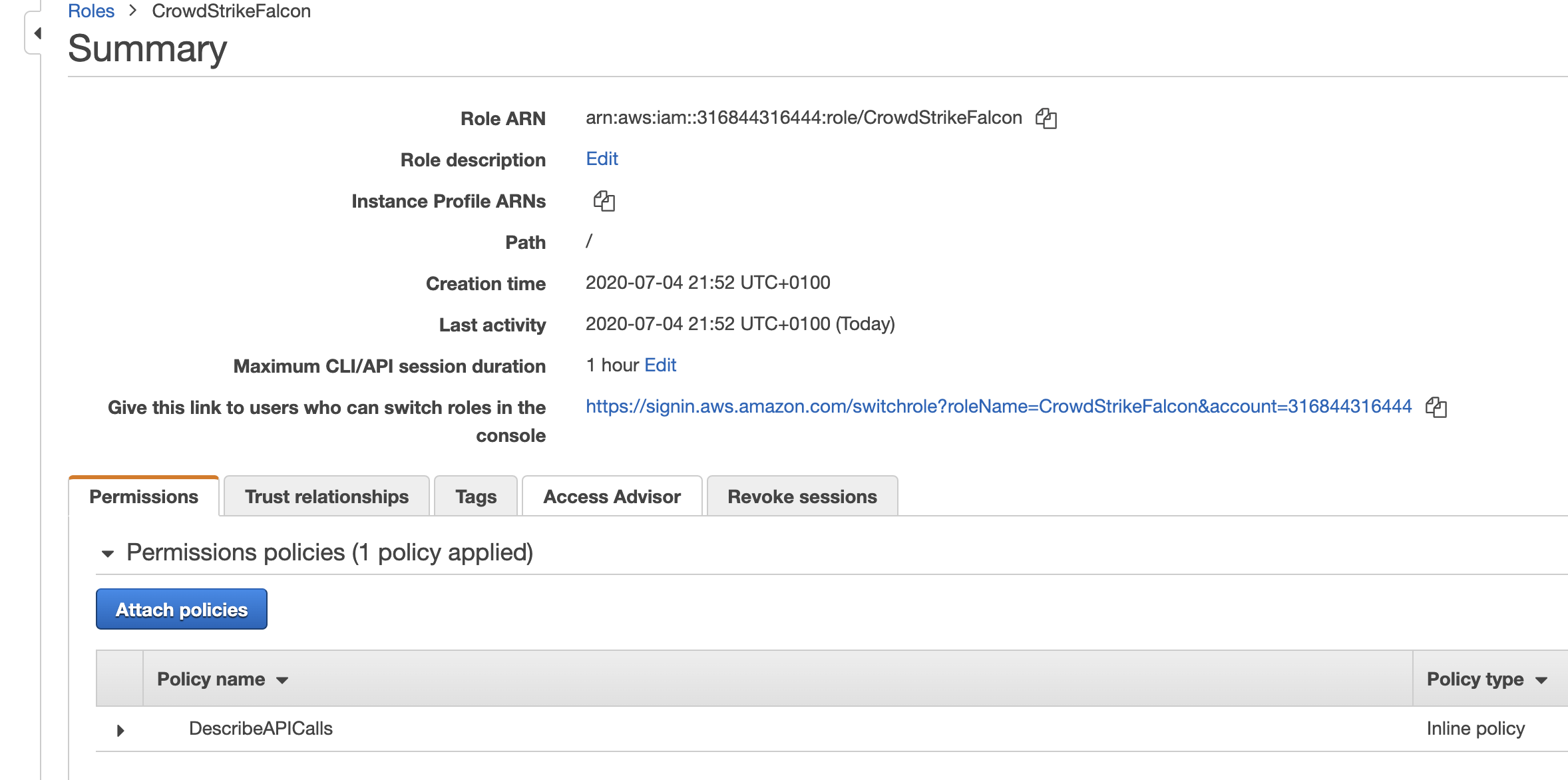


Log into the new account and check that the StackSet has been applied.

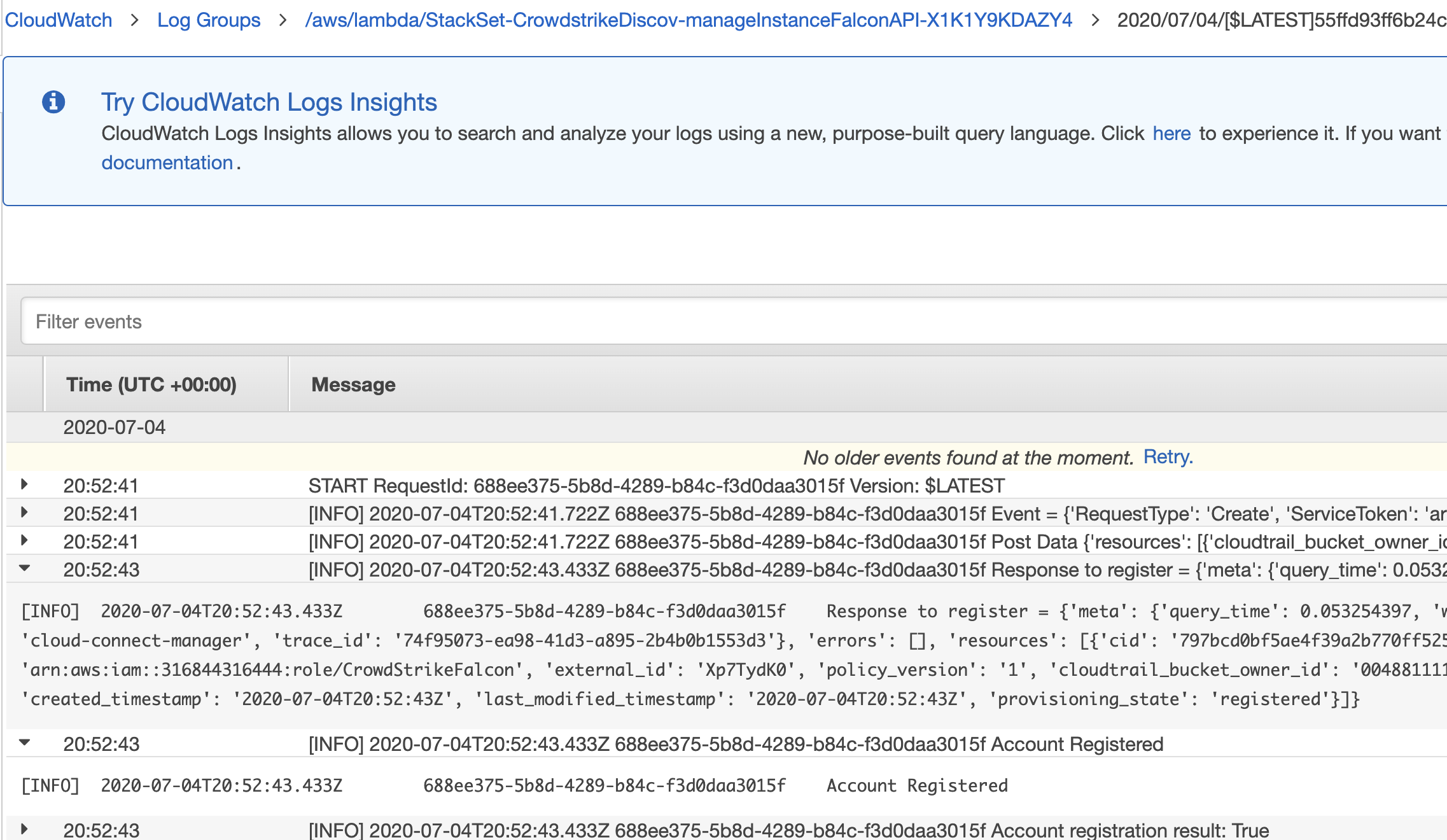
The StackSet will configure two resources

* IAM Role Named FalconDiscover
* Lambda Function to register the account with the Falcon Discover service

Verify that the IAM role has been configured in the new account



Go to CloudWatch and verify that the lambda function created has run and successfully and registered the account.



Additional resources

**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:**

<https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html>

CrowdStrike Resources

**To learn more about CrowdStrike**:

[CrowdStrike on APN](https://aws.amazon.com/partners/find/partnerdetails/?n=CrowdStrike&id=001E000001VAPbPIAX)

[CrowdStrike website](http://crowdstrike.com/)

**To check out different CrowdStrike AWS Marketplace Listings**

[CrowdStrike AWS Marketplace Listings](https://aws.amazon.com/marketplace/seller-profile?id=f4fb055a-5333-4b6e-8d8b-a4143ad7f6c7)

**To learn more about Falcon Cloud Workload Protection product**

[CrowdStrike Falcon Cloud Workload Protection Website](https://www.crowdstrike.com/cloud-security-products/falcon-cloud-workload-protection/)

[CrowdStrike Falcon Cloud Workload Protection Data sheet](https://www.crowdstrike.com/resources/data-sheets/falcon-cloud-workload-protection/)

CrowdStrike Contact Information

For questions regarding CrowdStrike offerings on AWS Marketplace or service integrations -

**Email:** [aws@crowdstrike.com](mailto:aws@crowdstrike.com)

For questions around product sales -

**Email:** [sales@crowdstrike.com](mailto:sales@crowdstrike.com)

For questions around support -

**Email:** [support@crowdstrike.com](mailto:support@crowdstrike.com)

For additional information and contact details -

**Website:** <https://www.crowdstrike.com/contact-us/>