

Implementation Guide:

CrowdStrike Falcon Discover for Cloud

Table of Contents

| Foreword | 3 |
|---|----|
| Solution overview and features | 4 |
| Benefits of CrowdStrike Discover for Cloud and Containers | 4 |
| Architecture diagram | 5 |
| Pre-requisites | 6 |
| Deployment and Configuration Steps | 7 |
| Configuration: Solution to deploy | 9 |
| Create or Enroll an account in to AWS Control Tower using account factory | 13 |
| Additional resources | 17 |
| CrowdStrike Resources | 17 |
| CrowdStrike Contact Information | 17 |

Foreword

With <u>CrowdStrike Discover for Cloud and Containers</u> 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 <u>Amazon Virtual Private Cloud</u> (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 <u>AWS Marketplace</u> customer to seamlessly activate, deploy and configure CrowdStrike Discover for Cloud and Containers in an <u>AWS Control Tower</u> 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) 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 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) 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, 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 <u>Amazon Simple Storage Service</u> (Amazon S3) bucket. When a new log file is written to the S3 bucket, an <u>Amazon Simple Notification Service</u> (Amazon SNS) notification is sent to the 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 analyze 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.

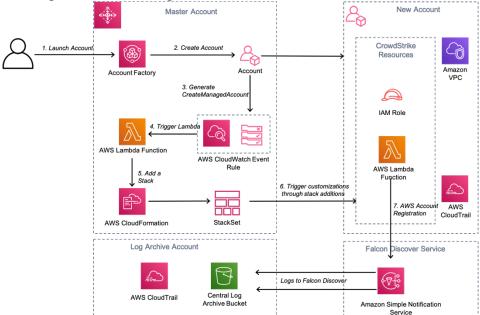


Figure 1 CrowdStrike Falcon Discover for Cloud and Containers Architecture Diagram

- 1) The Customer creates a new AWS account using <u>Account Factory</u> with in AWS Control Tower Master account.
- 2) Account factory creates a new AWS account and applies baselines and guardrails on the newly created account.
- 3) On completion of account creation a "CreateManagedAccount" event notification is generated https://docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html#create-managed-account
- 4) The CloudWatch event rule triggers a Lambda function that will generate account specific parameters
- 5) The custom parameters are passed to the StackSet that is applied to the new account.
- 6) 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 Crowdstrike.

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" 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 The externalid is a string of random characters.

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

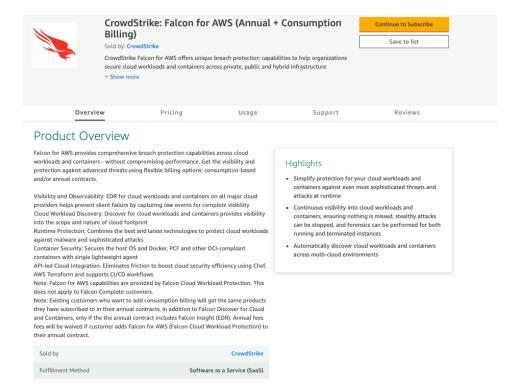
For additional information on AWS Marketplace, see https://aws.amazon.com/marketplace/help/about-us?ref = footer nav about aws marketplace.

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.

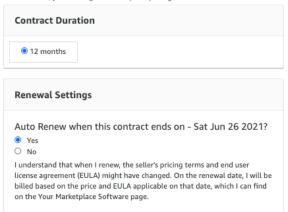
Continue to Subscribe

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**.

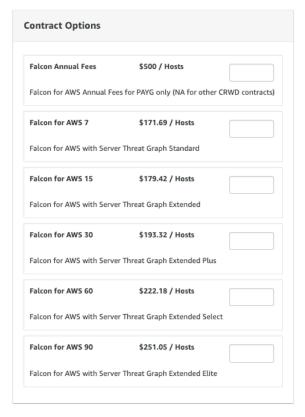
Configure your Software Contract

Choose the contract that suits your needs. You're charged for your purchase on your AWS bill. After you purchase a contract, you're directed to the vendor's site to complete setup and begin using this software. For any software use beyond your contract limit, you're charged consumption pricing.



Step 1.3: Select Contract Options

Select the Contract Options to be activated with your contract.



You may increase your contract at any time. Changes will be billed on a pro-rated basis. If you have opted in for automatic renewal, your contracts will automatically renew at the end of each term until you change your automatic renewal selection. You may change your automatic renewal selection at any time.

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 consists of the following tasks.

- 1) Load the CloudFormation template in the log-archive account.
- 2) Load the CloudFormation template in the master account.

Step 2.1: 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 2.2: Download the code from https://github.com/CrowdStrike/Cloud-AWS

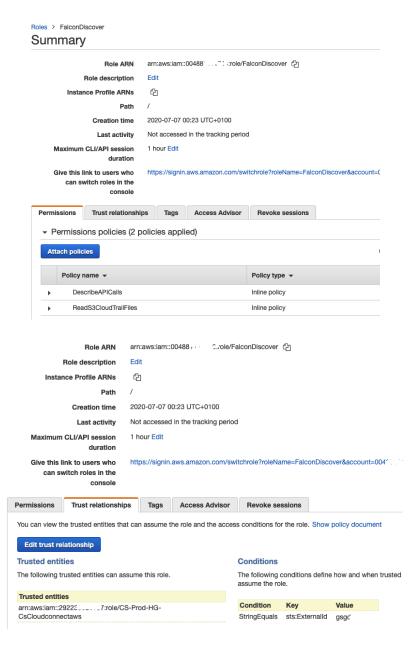
The GitHub repository contains the following folder structure.

- Control-Tower/log-archive-acct Folder containing the CloudFormation template for the Control Tower log-archive account
- Control-Tower/master-acct Folder containing the CloudFormation template for the Control Tower master account

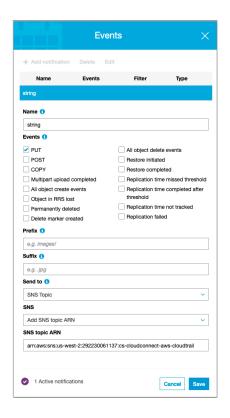
Step 2.3: Load the CloudFormation template in the log-archive account

Log in to the log archive account and apply the CloudFormation template "ct crowdstrike log archive account.yaml" from the log-archive-acct folder.

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 and discover resources in the account. The role is restricted so that only the IAM role "arn: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 2.4: Load the CloudFormation template in the master account

Go to the master account and apply the CloudFormation template "ct crowdstrike master account.yaml" from the master-acct folder.

Description of Parameters

FalconClientId: Your Falcon Oauth2 API Key from the Crowdstrike Console

FalconSecret: Your Falcon Oauth2 API Secret from the Crowdstrike Console

ExternalId: String of random characters.

https://docs.aws.amazon.com/IAM/latest/UserGuide/id roles create for-user externalid.html

CSAccountNumber: The number supplied in the template '292230061137' should NOT be changed unless directed by Crowdstrike

LambdaBucketName: The name of the S3 bucket that was created by the script run in step 3.4

RoleName: This name may be modified as required.

CSAssumingRoleName: The name supplied in the template 'CS-Prod-HG-CsCloudconnectaws' should NOT be changed unless directed by Crowdstrike

LogArchiveAccount: AWS account number where the log archive bucket that was created by Control Tower

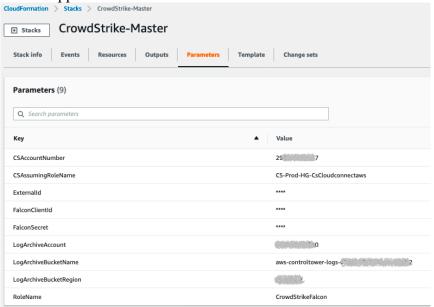


LogArchiveBucketName: The name of the CloudTrail log archive bucket that was created by Control Tower

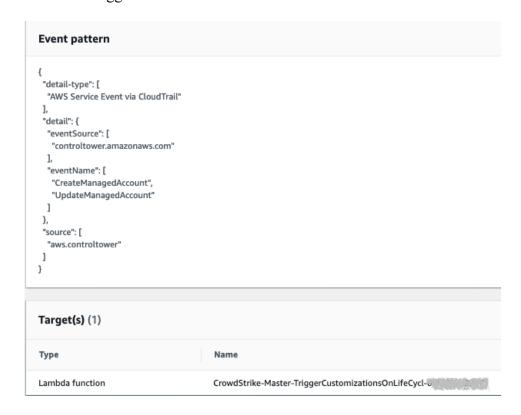
LogArchiveBucketRegion: The region where the CloudTrail log archive bucket that was created by Control Tower

The CloudFormation template will create the following resources in the account

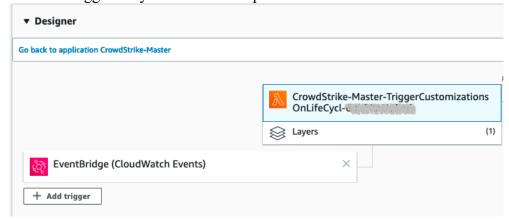
StackSet that will be applied to new accounts



• CloudWatch rule to trigger a lambda function



• Lambda function triggered by CloudWatch to push the StackSet to a new account



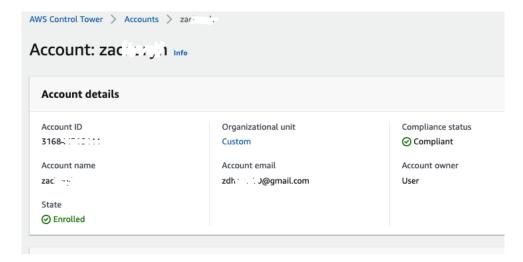
Lambda function to register the master account with Crowdstrike Falcon

Step 2.5: Verification Steps

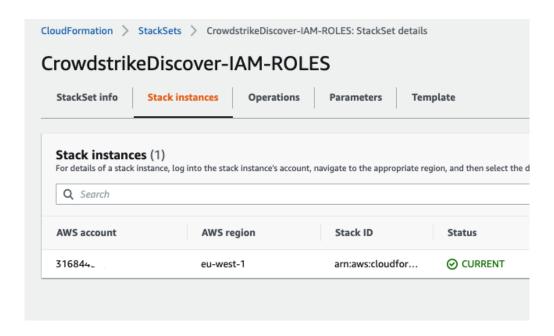
<u>Create or Enroll an account</u> in to AWS Control Tower using account factory.



Once the account has been created (usually takes around 30 minutes), check the status of the account



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



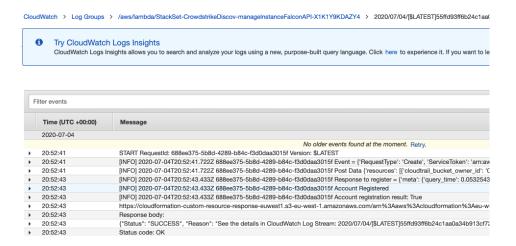
Log into the new account and check that the StackSet has been applied.

The StackSet will configure two resources

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

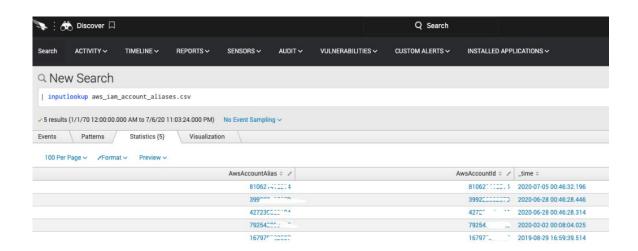
Verify that the IAM role has been configured in the new account Roles > CrowdStrikeFalcon Summary arn:aws:iam::31684/312....:role/CrowdStrikeFalcon Role ARN Role description Edit Instance Profile ARNs 2020-07-04 21:52 UTC+0100 Creation time 2020-07-06 14:16 UTC+0100 (Today) Last activity Maximum CLI/API session duration Give this link to users who can https://signin.aws.amazon.com/switchrole?roleName=CrowdStrikeFalcon&account=3168.4 5: 4 switch roles in the console Trust relationships Access Advisor Revoke sessions ▼ Permissions policies (1 policy applied) Attach policies O Add Policy name -Policy type * DescribeAPICalls Inline policy

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

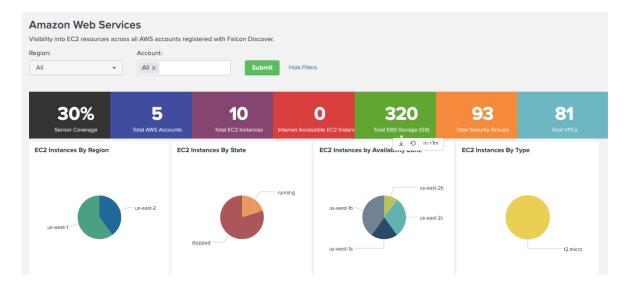


Step 2.6: Check the Discover accounts

Log into the Crowdstrike console and check the account status. Navigate to *Discover – Amazon Web Services - Accounts*. The screen below will show the accounts that have been added



Accounts and resources will begin to appear in the dashboard



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

CrowdStrike website

To check out different CrowdStrike AWS Marketplace Listings

CrowdStrike AWS Marketplace Listings

To learn more about Falcon Cloud Workload Protection product

CrowdStrike Falcon Cloud Workload Protection Website

CrowdStrike Falcon Cloud Workload Protection Data sheet

CrowdStrike Contact Information

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

Email: aws@crowdstrike.com
For questions around support Email: support@crowdstrike.com
Email: support@crowdstrike.com

For additional information and contact details - **Website:** https://www.crowdstrike.com/contact-us/