aws marketplace

Implementation Guide:

CrowdStrike Falcon Discover for Cloud

Table of Contents

Foreword

With CrowdStrike Discover for Cloud and Containers 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.

Commented [MOU1]: Link to your product page please.

Commented [MOU2]: This is probably my lack of familiarity with the lingo "What is content Discover for Cloud and Containers" mean? Please have hyperlinks.

Deleted: ~~delivers~~

Commented [MOU4]: Too big sentence, please break this for better readability.

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.

Deleted: As the only cloud-native, next-generation security solution of its kind,

Commented [MOU6]: Link to https://aws.amazon.com/ec2/

Commented [MOU7]: Link to https://aws.amazon.com/cloudtrail/

Commented [MOU8]: Link to https://aws.amazon.com/iam/

Commented [MOU9]: Link to it please

Commented [MOU10]: Link if possible?

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.

Deleted:

Commented [MOU11]: Are we doing this for current release? Seem to be missing in the walkthrough.

Deleted:

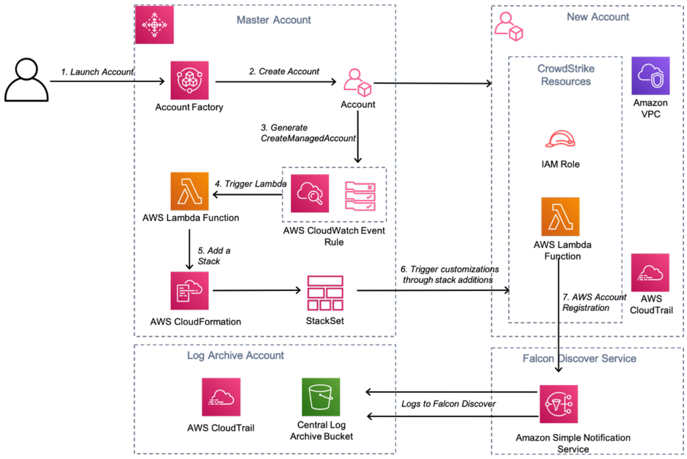


Figure 1 CrowdStrike Falcon Discover for Cloud and Containers Architecture Diagram

1) The Customer creates a new account using [Account Factory](#) 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.

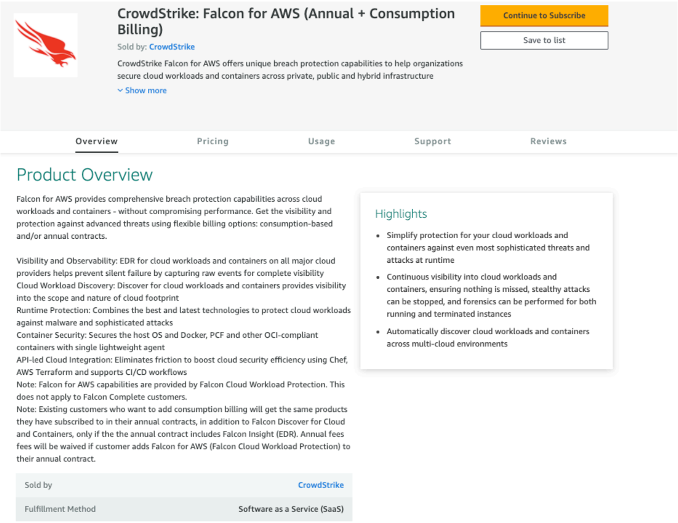
If you are new to AWS, see Getting Started with AWS: https://aws.amazon.com/getting-started/.

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).



CrowdStrike: Falcon for AWS (Annual + Consumption Billing)

Sold by: CrowdStrike

CrowdStrike Falcon for AWS offers unique breach protection capabilities to help organizations secure cloud workloads and containers across private, public and hybrid infrastructure

Product Overview

Falcon for AWS provides comprehensive breach protection capabilities across cloud workloads and containers - without compromising performance. Get the visibility and protection against advanced threats using flexible billing options: consumption-based and/or annual contracts.

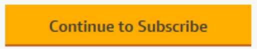
Visibility and Observability: EDR for cloud workloads and containers on all major cloud providers helps prevent silent failure by capturing raw events for complete visibility
Cloud Workload Discovery: Discover for cloud workloads and containers provides visibility into the scope and nature of cloud footprint
Runtime Protection: Combines the best and latest technologies to protect cloud workloads against malware and sophisticated attacks
Container Security: Secures the host OS and Docker, PCF and other OCI-compliant containers with single lightweight agent
API-led Cloud Integration: Eliminates friction to boost cloud security efficiency using Chef, AWS Terraform and supports CI/CD workflows
Note: Falcon for AWS capabilities are provided by Falcon Cloud Workload Protection. This does not apply to Falcon Complete customers.
Note: Existing customers who want to add consumption billing will get the same products they have subscribed to in their annual contracts, in addition to Falcon Discover for Cloud and Containers, only if the the annual contract includes Falcon Insight (EDR). Annual fees fees will be waived if customer adds Falcon for AWS (Falcon Cloud Workload Protection) to their annual contract.

Sold by	CrowdStrike
Fulfillment Method	Software as a Service (SaaS)

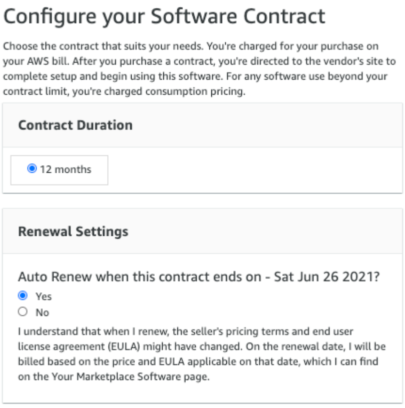
Highlights

- Simplify protection for your cloud workloads and containers against even most sophisticated threats and attacks at runtime
- Continuous visibility into cloud workloads and containers, ensuring nothing is missed, stealthy attacks can be stopped, and forensics can be performed for both running and terminated instances
- Automatically discover cloud workloads and containers across multi-cloud environments

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**.



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.

Contract Duration

● 12 months

Renewal Settings

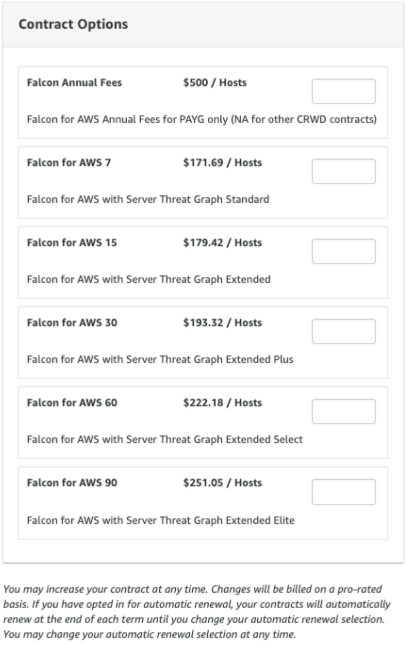
Auto Renew when this contract ends on - Sat Jun 26 2021?

● Yes
○ No

I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find on the Your Marketplace Software page.

Step 1.3: Select Contract Options

Select the Contract Options to be activated with your contract.



Contract Options

Falcon Annual Fees	**$500 / Hosts**	Falcon for AWS Annual Fees for PAYG only (NA for other CRWD contracts)
Falcon for AWS 7	**$171.69 / Hosts**	Falcon for AWS with Server Threat Graph Standard
Falcon for AWS 15	**$179.42 / Hosts**	Falcon for AWS with Server Threat Graph Extended
Falcon for AWS 30	**$193.32 / Hosts**	Falcon for AWS with Server Threat Graph Extended Plus
Falcon for AWS 60	**$222.18 / Hosts**	Falcon for AWS with Server Threat Graph Extended Select
Falcon for AWS 90	**$251.05 / Hosts**	Falcon for AWS with Server Threat Graph Extended Elite

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.

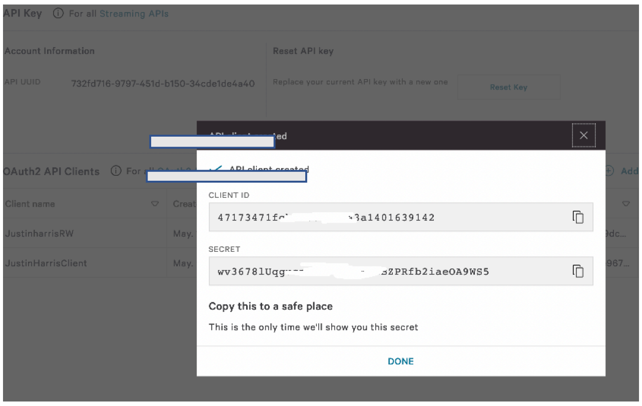
Configuration: Solution to deploy

Setup consists of the following tasks.

1) 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.



CLIENT ID

47173471fc[redacted]3a1401639142

SECRET

wv3678lUqg[redacted]3ZPRfb2iaeOA9WS5

Copy this to a safe place

This is the only time we'll show you this secret

Step 3.2: Download the code from https://github.com/CrowdStrike/Cloud-AWS

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

Note: A file named 'create_staging_bucket.py' is also included to assist with the setup of the required S3 buckets. It is recommended that the script is used to setup the buckets as it sets specific permissions for two objects in the master account.

Deleted: Download the code from https://github.com/jhseceng/control-tower

Commented [MOU12]: You may want to point to a public document for this.

Commented [MOU13]: It will be helpful to define API Scopes to select here? Any direct references will be very helpful to the reader.

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

Deleted: Download the code from https://github.com/jhseceng/control-tower

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'],
```

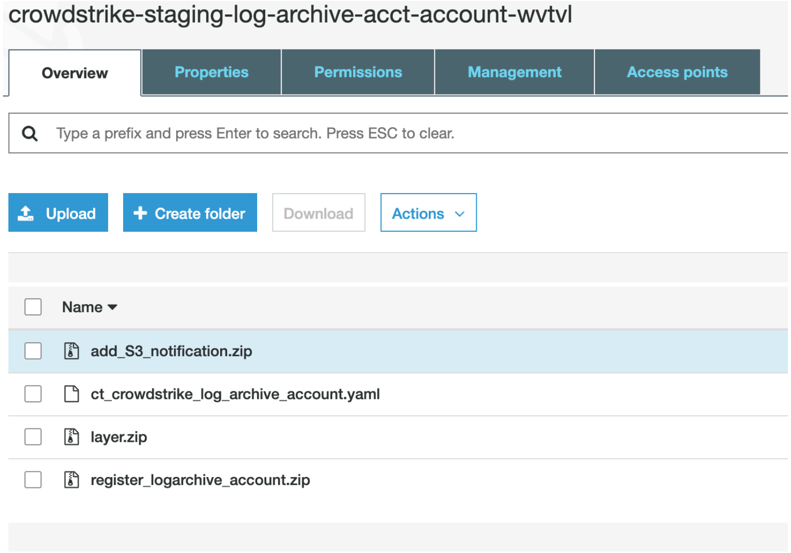
Run the python script *python3 create_staging_bucket.py -r <region> -a log-archive-acct -b <optional bucket name>*

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.



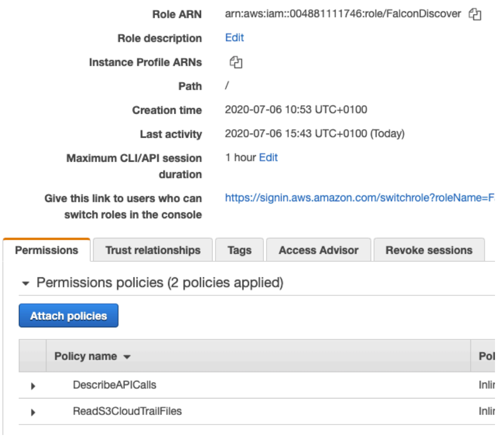
crowdstrike-staging-log-archive-acct-account-wvtvl

- □ add_S3_notification.zip
- □ ct_crowdstrike_log_archive_account.yaml
- □ layer.zip
- □ register_logarchive_account.zip

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*".

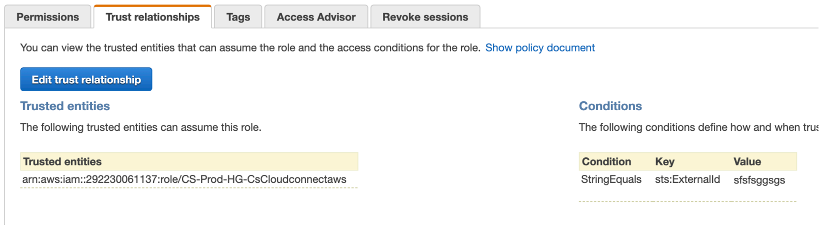
The CloudFormation template will create a Role name "FalconDiscover" in the log archive account that will permit read access to objects in the s3 bucket and discover resources in the account. The role is restricted so that only the IAM role "*arn:aws:iam::292230061137:role/CS-Prod-HG-CsCloudconnectaws"*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



Role ARN	arn:aws:iam::004881111746:role/FalconDiscover
Role description	Edit
Instance Profile ARNs	
Path	/
Creation time	2020-07-06 10:53 UTC+0100
Last activity	2020-07-06 15:43 UTC+0100 (Today)
Maximum CLI/API session duration	1 hour Edit
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=F

Permissions policies (2 policies applied)

Policy name	Pol
DescribeAPICalls	Inlir
ReadS3CloudTrailFiles	Inlir



You can view the trusted entities that can assume the role and the access conditions for the role. Show policy document

Trusted entities

The following trusted entities can assume this role.

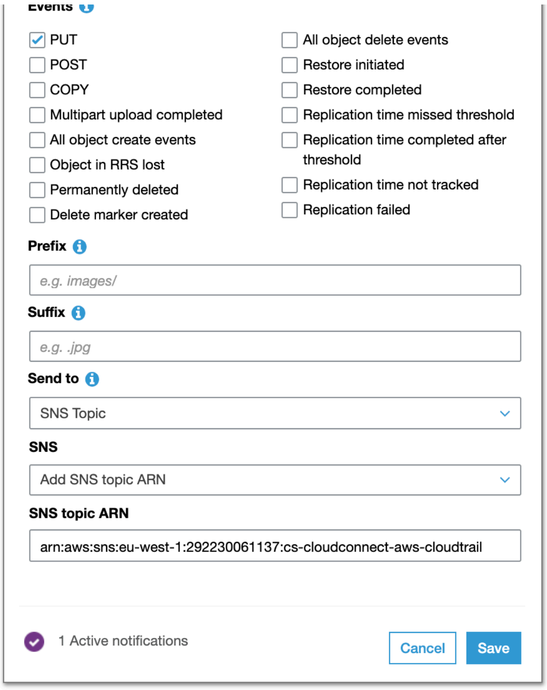
Trusted entities
arn:aws:iam::292230061137:role/CS-Prod-HG-CsCloudconnectaws

Conditions

The following conditions define how and when trus

Condition	Key	Value
StringEquals	sts:ExternalId	sfsfsggsgs

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"



Events

☑ PUT
□ POST
□ COPY
□ Multipart upload completed
□ All object create events
□ Object in RRS lost
□ Permanently deleted
□ Delete marker created
□ All object delete events
□ Restore initiated
□ Restore completed
□ Replication time missed threshold
□ Replication time completed after threshold
□ Replication time not tracked
□ Replication failed

Prefix

e.g. images/

Suffix

e.g. .jpg

Send to

SNS Topic

SNS

Add SNS topic ARN

SNS topic ARN

arn:aws:sns:eu-west-1:292230061137:cs-cloudconnect-aws-cloudtrail

1 Active notifications

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

Deleted: Download the code from https://github.com/jhseceng/control-tower

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"*.

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

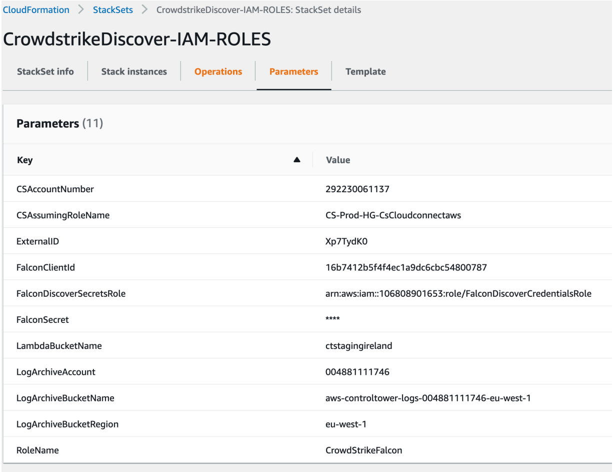
LogArchiveAccount: AWS account number where the log archive bucket bucket that was created by Control Tower

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

LogArchiveBucketRegion: The region where the cloudwatch 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

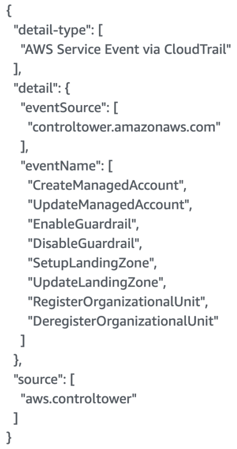

CloudFormation > StackSets > CrowdstrikeDiscover-IAM-ROLES: StackSet details
StackSet info
Stack instances
Operations
Parameters
Template

CrowdstrikeDiscover-IAM-ROLES

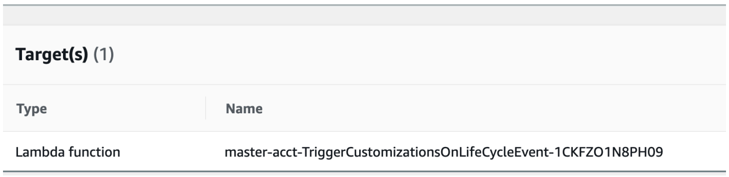
Parameters (11)

Key	Value
CSAccountNumber	292230061137
CSAssumingRoleName	CS-Prod-HG-CsCloudconnectaws
ExternalID	Xp7TydK0
FalconClientId	16b7412b5f4f4ec1a9dc6cbc54800787
FalconDiscoverSecretsRole	arn:aws:iam::106808901653:role/FalconDiscoverCredentialsRole
FalconSecret	****
LambdaBucketName	ctstagingireland
LogArchiveAccount	004881111746
LogArchiveBucketName	aws-controltower-logs-004881111746-eu-west-1
LogArchiveBucketRegion	eu-west-1
RoleName	CrowdStrikeFalcon

- CloudWatch rule to trigger a lambda function



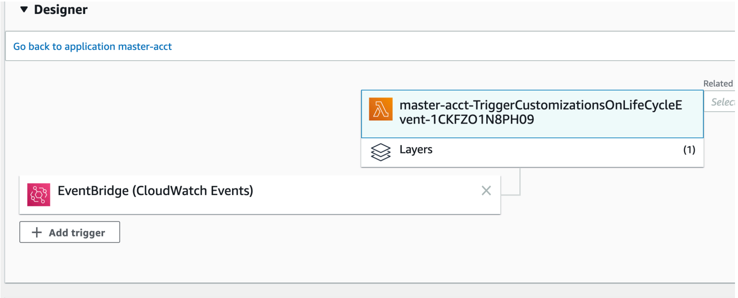
```
{
 "detail-type": [
  "AWS Service Event via CloudTrail"
 ],
 "detail": {
  "eventSource": [
   "controltower.amazonaws.com"
  ],
  "eventName": [
   "CreateManagedAccount",
   "UpdateManagedAccount",
   "EnableGuardrail",
   "DisableGuardrail",
   "SetupLandingZone",
   "UpdateLandingZone",
   "RegisterOrganizationalUnit",
   "DeregisterOrganizationalUnit"
  ]
 },
 "source": [
  "aws.controltower"
 ]
}
```



Target(s) (1)

Type	Name
Lambda function	master-acct-TriggerCustomizationsOnLifeCycleEvent-1CKFZO1N8PH09

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



▼ Designer

Go back to application master-acct

Related

Selec

master-acct-TriggerCustomizationsOnLifeCycleEvent-1CKFZO1N8PH09

Layers (1)

EventBridge (CloudWatch Events)

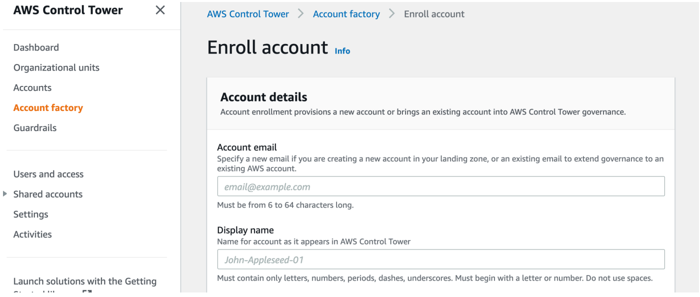
＋ Add trigger

- Lambda function to register the master account with Crowdstrike Falcon

Step 3.6: Verification Steps

Create a new account in account factory

Formatted: Line spacing: single



AWS Control Tower > Account factory > Enroll account

Enroll account Info

Account details

Account enrollment provisions a new account or brings an existing account into AWS Control Tower governance.

Account email

Specify a new email if you are creating a new account in your landing zone, or an existing email to extend governance to an existing AWS account.

email@example.com

Must be from 6 to 64 characters long.

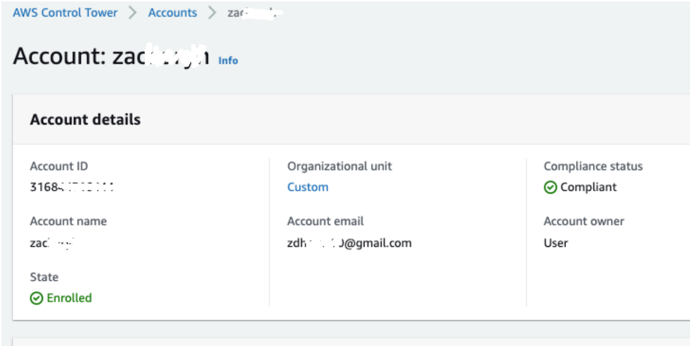
Display name

Name for account as it appears in AWS Control Tower

John-Appleseed-01

Must contain only letters, numbers, periods, dashes, underscores. Must begin with a letter or number. Do not use spaces.

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



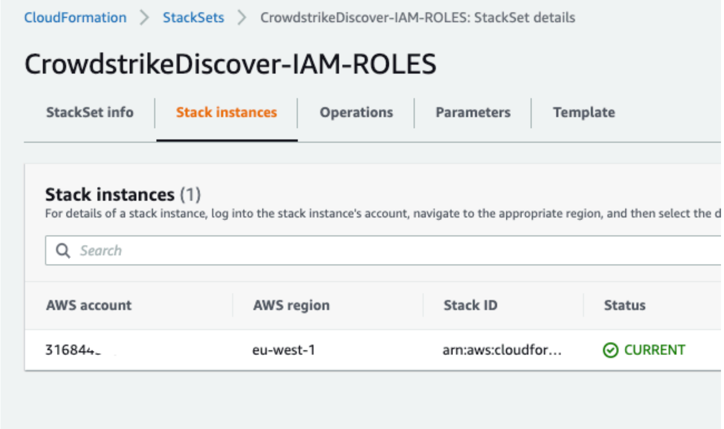
AWS Control Tower > Accounts > za[redacted]

Account: zac[redacted] Info

Account details

Account ID 3168[redacted]	Organizational unit Custom	Compliance status ✓ Compliant
Account name zac[redacted]	Account email zdh[redacted]J@gmail.com	Account owner User
State ✓ Enrolled		

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



CloudFormation > StackSets > CrowdstrikeDiscover-IAM-ROLES: StackSet details

CrowdstrikeDiscover-IAM-ROLES

Stack instances (1)

For details of a stack instance, log into the stack instance's account, navigate to the appropriate region, and then select the d

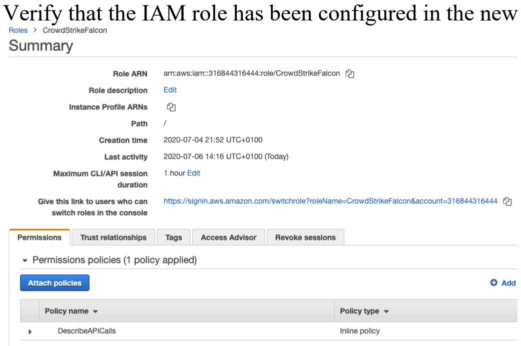
AWS account	AWS region	Stack ID	Status
316844_	eu-west-1	arn:aws:cloudfor...	✓ CURRENT

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

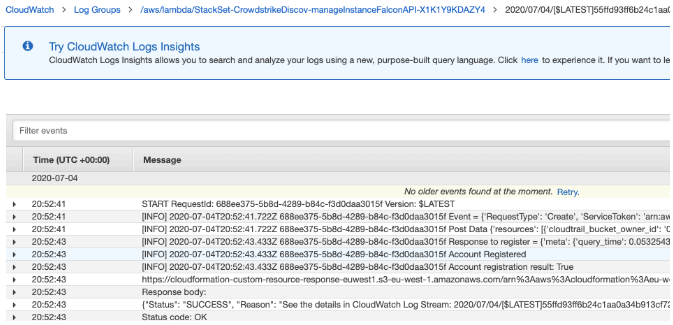
Summary

Role ARN	arn:aws:iam::316844316444:role/CrowdStrikeFalcon
Role description	Edit
Instance Profile ARNs	
Path	/
Creation time	2020-07-04 21:52 UTC+0100
Last activity	2020-07-06 14:16 UTC+0100 (Today)
Maximum CLI/API session duration	1 hour Edit
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=CrowdStrikeFalcon&account=316844316444

Permissions policies (1 policy applied)

Policy name	Policy type
DescribeAPICalls	Inline policy

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



CloudWatch > Log Groups > /aws/lambda/StackSet-CrowdstrikeDiscov-manageInstanceFalconAPI-X1K1Y9KDAZY4 > 2020/07/04/[$LATEST]55ffd93ff6b24c1aa(

Try CloudWatch Logs Insights
CloudWatch Logs Insights allows you to search and analyze your logs using a new, purpose-built query language. Click here to experience it. If you want to le

Filter events

```
Time (UTC +00:00)   Message
2020-07-04
                                        No older events found at the moment. Retry.
20:52:41   START RequestId: 688ee375-5b8d-4289-b84c-f3d0daa3015f Version: $LATEST
20:52:41   [INFO] 2020-07-04T20:52:41.722Z 688ee375-5b8d-4289-b84c-f3d0daa3015f Event = {'RequestType': 'Create', 'ServiceToken': 'arn:aw
20:52:41   [INFO] 2020-07-04T20:52:41.722Z 688ee375-5b8d-4289-b84c-f3d0daa3015f Post Data {'resources': [{'cloudtrail_bucket_owner_id': '0
20:52:43   [INFO] 2020-07-04T20:52:43.433Z 688ee375-5b8d-4289-b84c-f3d0daa3015f Response to register = {'meta': {'query_time': 0.0532543
20:52:43   [INFO] 2020-07-04T20:52:43.433Z 688ee375-5b8d-4289-b84c-f3d0daa3015f Account Registered
20:52:43   [INFO] 2020-07-04T20:52:43.433Z 688ee375-5b8d-4289-b84c-f3d0daa3015f Account registration result: True
20:52:43   https://cloudformation-custom-resource-response-euwest1.s3-eu-west-1.amazonaws.com/arn%3Aaws%3Acloudformation%3Aeu-w
20:52:43   Response body:
20:52:43   {"Status": "SUCCESS", "Reason": "See the details in CloudWatch Log Stream: 2020/07/04/[$LATEST]55ffd93ff6b24c1aa0a34b913cf72
20:52:43   Status code: OK
```

A script may be run post deployment to check the status of the accounts in Crowdstrike

The script is named "*check_discover_accounts.py*"
The script will check the status of the accounts and report any issues that require attention.
Example output

```
These accounts have problems
AWS AccountId : 7442533XXXX
Reason: Assume role failed. IAM role arn and/or external is invalid.
{
    "id": "7442533XXXX",
    "iam_role_arn": "arn:aws:iam::7442533XXXX:role/FalconDiscover",
    "external_id": "PxovOosucXXXXXXX",
    "cloudtrail_bucket_owner_id": "00488111XXXX",
    "cloudtrail_bucket_region": "eu-west-1"
}
AWS AccountId : 10680890XXXX
Reason: Assume role failed. IAM role arn and/or external is invalid.
{
    "id": "10680890XXXX",
    "iam_role_arn": "arn:aws:iam::10680890XXXX:role/CrowdStrikeFalcontest",
    "external_id": "afu79FB4XXXXXX",
    "cloudtrail_bucket_owner_id": "00488111XXXX",
    "cloudtrail_bucket_region": "eu-west-1"
}

These accounts are ok
      Account: 00488111XXXX
      Account: 31684431XXXX
```

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 product sales -
Email: sales@crowdstrike.com
For questions around support -
Email: support@crowdstrike.com
For additional information and contact details -
Website: https://www.crowdstrike.com/contact-us/