

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. 14

Additional resources 18

CrowdStrike Resources 18

CrowdStrike Contact Information 19

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.

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 [Amazon Simple Storage Service](#) (Amazon S3) bucket. When a new log file is written to the S3 bucket, an [Amazon Simple Notification Service](#) (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.

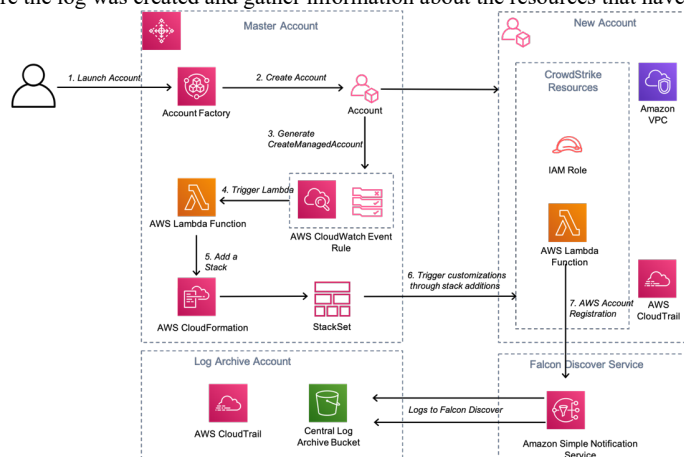


Figure 1 CrowdStrike Falcon Discover for Cloud and Containers Architecture Diagram

- 1) The Customer creates a new AWS account using [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

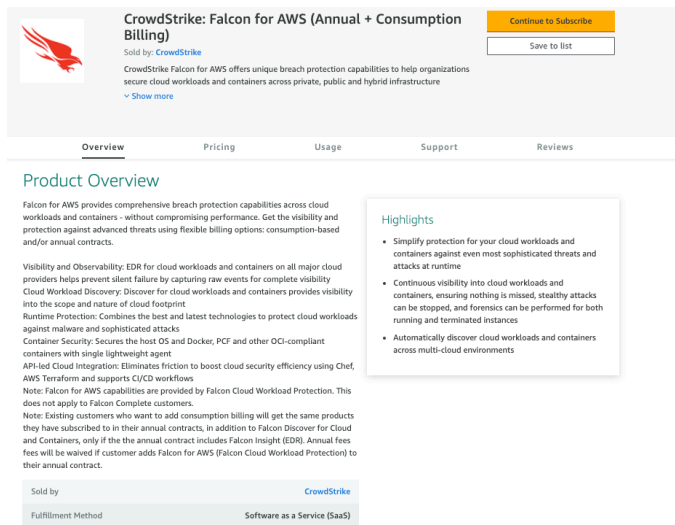
<https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html>

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

[Show more](#)

[Continue to Subscribe](#)

[Save to list](#)

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.

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

Sold by: [CrowdStrike](#)

Fulfillment Method: [Software as a Service \(SaaS\)](#)

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.

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.

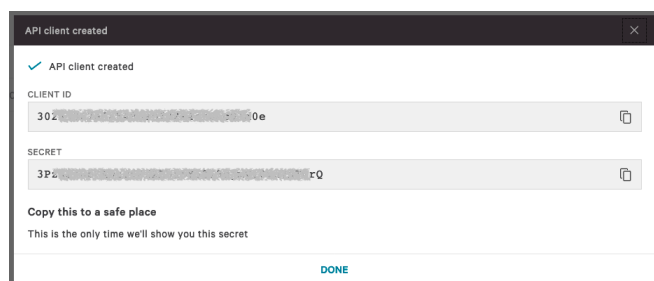
- 1) Load the CloudFormation template in the log-archive account.
- 2) Load the CloudFormation template in the master account.

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.

Summary

Role ARN

am:aws:iam::00488...:role/FalconDiscover

Role description

[Edit](#)

Instance Profile ARNs

[+](#)

Path

/

Creation time

2020-07-07 00:23 UTC+0100

Last activity

Not accessed in the tracking period

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=FalconDiscover&account=00488...>

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

▼ Permissions policies (2 policies applied)

Attach policies

Policy name	Policy type
DescribeAPICalls	Inline policy
ReadS3CloudTrailFiles	Inline policy

Role ARN

am:aws:iam::00488...:role/FalconDiscover

Role description

[Edit](#)

Instance Profile ARNs

[+](#)

Path

/

Creation time

2020-07-07 00:23 UTC+0100

Last activity

Not accessed in the tracking period

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=FalconDiscover&account=00488...>

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

Edit trust relationship

Trusted entities

The following trusted entities can assume this role.

Trusted entities
am:aws:iam::2922...:role/CS-Prod-HG-CsCloudconnectaws

Conditions

The following conditions define how and when trusted assume the role.

Condition	Key	Value
StringEquals	sts:Externalid	gsgc

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

+ Add notification

Delete

Edit

Name	Events	Filter	Type
string			

Name

string

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:us-west-2:292230061137:cs-cloudconnect-aws-cloudtrail

1 Active notifications

Cancel

Save

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

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

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

ExternalId: Enter a String of random characters.

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

FalconClientId: Your Falcon OAuth2 API Key from the Crowdstrike Console

FalconSecret: Your Falcon OAuth2 API Secret from the Crowdstrike Console

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

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

RoleName: This name may be modified as required

The CloudFormation template will create the following resources in the account

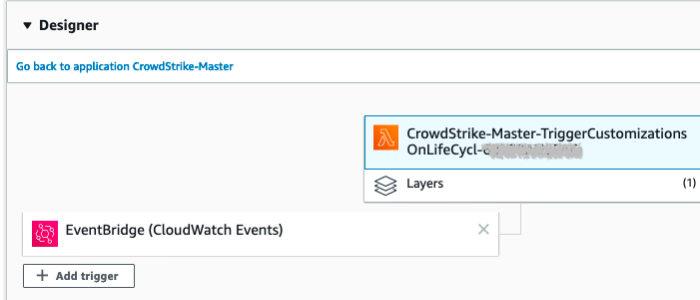
- StackSet that will be applied to new accounts

Stack info	Events	Resources	Outputs	Parameters	Template	Change sets
Parameters (8)						
<div>Q Search parameters</div>						
Key	▲	Value	▼	Resolved value	▼	
CSAccountNumber		25		-		
CSAssumingRoleName		CS-Prod-HG-CsCloudconnectaws		-		
ExternalId		****		-		
FalconClientId		****		-		
FalconSecret		****		-		
LogArchiveAccount		OC		-		
LogArchiveBucketRegion		eu- st-1		-		
RoleName		CrowdStrikeFalcon		-		

- CloudWatch rule to trigger a lambda function

Event pattern	
<pre>{ "detail-type": ["AWS Service Event via CloudTrail"], "detail": { "eventSource": ["controltower.amazonaws.com"], "eventName": ["CreateManagedAccount", "UpdateManagedAccount"] }, "source": ["aws.controltower"] }</pre>	
Target(s) (1)	
Type	Name
Lambda function	CrowdStrike-Master-TriggerCustomizationsOnLifeCycle

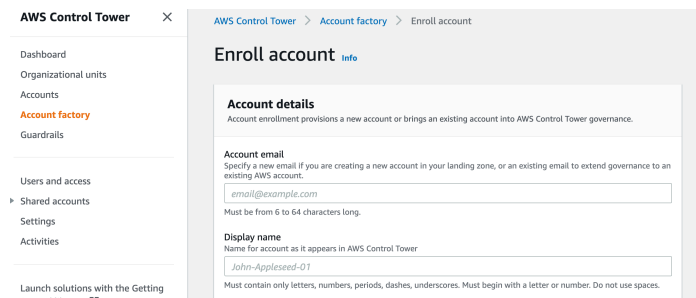
- Lambda function triggered by CloudWatch to push the StackSet to a new account



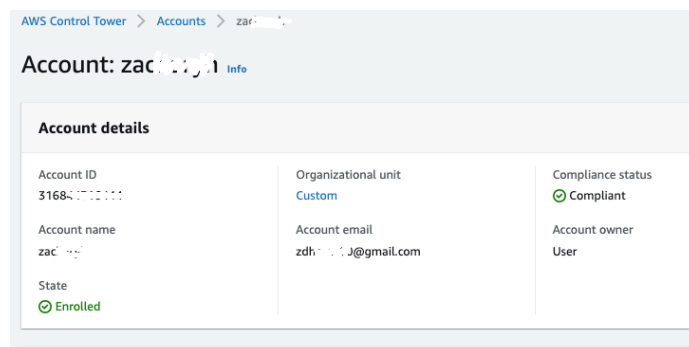
- Lambda function to register the master account with CrowdStrike Falcon

Step 2.5: Verification Steps

[Create or Enroll an account](#) in to AWS Control Tower using account factory.



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



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

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

CrowdStrikeDiscover-IAM-ROLES

StackSet info

Stack instances

Operations

Parameters

Template

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

Q Search

AWS account	AWS region	Stack ID	Status
316844-	eu-west-1	arn:aws:cloudfor...	<div>CURRENT</div>

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

Summary

Role ARN	arn:aws:iam::316847312111: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=316847312111> 

Permissions
Trust relationships
Tags
Access Advisor
Revoke sessions


Permissions policies (1 policy applied)

Attach policies

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.

CloudWatch > Log Groups > /aws/lambda/StackSet-CrowdstrikeDiscov-manageinstanceFalconAPI-X1K1Y9KDAZY4 > 2020/07/04:[\$LATEST]559d93f96b24c1aa

 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

Filter events	
Time (UTC +00:00)	Message
2020-07-04	No older events found at the moment. Retry.
20:52:41	START RequestId: 688ee375-5bbd-4289-b84c-d3ddaa301f5f Version: \$LATEST
20:52:41	[INFO] 2020-07-04T20:52:41.722Z 688ee375-5bbd-4289-b84c-d3ddaa301f5f Event = {"RequestType": "Create", "ServiceToken": "arn:aws:iam::33aeuw-1:role/cloudwatch-log-streamer"} [CloudTrail Bucket Owner ID: 33aeuw-1]
20:52:41	[INFO] 2020-07-04T20:52:41.722Z 688ee375-5bbd-4289-b84c-d3ddaa301f5f Post Data {"Resources": [{"cloudtrail_bucket_owner_id": "33aeuw-1"}]}
20:52:43	[INFO] 2020-07-04T20:52:43.433Z 688ee375-5bbd-4289-b84c-d3ddaa301f5f Response to register = {"meta": {"Query time": "0.032545s"}}
20:52:43	[INFO] 2020-07-04T20:52:43.433Z 688ee375-5bbd-4289-b84c-d3ddaa301f5f Account Registered
20:52:43	[INFO] 2020-07-04T20:52:43.433Z 688ee375-5bbd-4289-b84c-d3ddaa301f5f Account registration result: True
20:52:43	https://cloudformation-custom-resource-response-us-east-1.s3.eu-west-1.amazonaws.com/am%3A3aeuw-1%3Acloudformation%3A3aeuw-1
20:52:43	Response body:
20:52:43	{"Status": "SUCCESS", "Reason": "See the details in CloudWatch Log Stream: 2020/07/04/[SLATEST]5f69b624c1a0a3ba391cf7d7e2"} [CloudTrail Bucket Owner ID: 33aeuw-1]

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

Discover

Search

Search ACTIVITY TIMELINE REPORTS SENSORS AUDIT VULNERABILITIES CUSTOM ALERTS INSTALLED APPLICATIONS

New Search

inputlookup aws_iam_account_aliases.csv

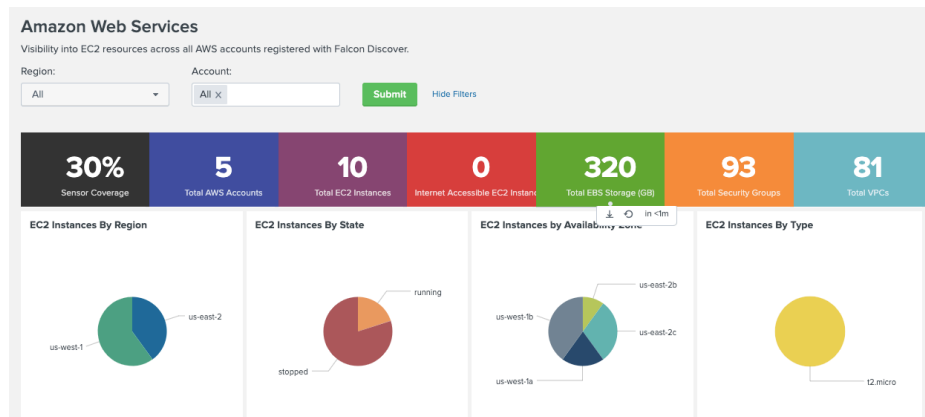
5 results (1/1/70 12:00:00.000 AM to 7/6/20 11:03:24.000 PM) No Event Sampling

Events Patterns Statistics (5) Visualization

100 Per Page Format Preview

AwsAccountAlias	AwsAccountid	_time
81062	81062	2020-07-05 00:46:32.196
399	3992	2020-06-28 00:46:28.446
42723	4272	2020-06-28 00:46:28.314
79254	79254	2020-02-02 00:08:04.025
16797	16797	2019-08-29 16:59:39.514

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/):

<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](#)



Deleted: 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

```
{
  "id": "7442533XXXX",
  "iam_role_arn": "arn:aws:iam::7442533XXXX:role/FalconDisc
over",
  "external_id": "Pxov0osucXXXXXXXX",
  "cloudtrail_bucket_owner_id": "00488111XXXX",
  "cloudtrail_bucket_region": "eu-west-1"
}
```

AWS AccountId : 7442533XXXX
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

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/>