FMCでのセキュアなダイナミック属性コネクタ の展開

内容

<u>はじめに</u>

<u> 背景 – 問題</u>

<u>ソリューション(概要)</u>

FMCでのダイナミック属性コネクタの概要

導入例

<u>オンプレミスCSDAC</u>

<u>問題</u>

<u>オプション1:FMC内に構築されたダイナミック属性コネクタを使用する</u> <u>オプション2:クラウド提供のダイナミック属性コネクタをCDOで使用する</u>

前提条件、サポート対象プラットフォーム、ライセンス

<u>サポートされる最低限のソフトウェアおよびハードウェアプラットフォーム</u>

<u>使用するコンポーネント</u>

機能の詳細

<u>スタンドアロンCSDACの概要(現在リリースされている – 7.4)</u>

<u>CDOでのCSDACの概要(現在リリースされている – 7.4)</u>

<u>FMCでのCSDAC</u>

<u>仕組み</u>

<u>コネクタの設定</u>

FMCでのCSDAC

<u>動的オブジェクト</u>

<u>ACポリシー</u>

<u>設定:アクセスポリシー</u>

<u>プラットフォームの制限</u>

トラブルシューティング/診断

<u>コネクタの確認</u>

<u>コネクタタブからのコネクタの表示</u>

<u>属性フィルタの確認</u>

<u>FMCのUIでダイナミックオブジェクトを確認する</u>

<u>CSDACヘルスアラート</u>

<u>トラブルシューティングのCSDAC</u>

<u>CSDACの生成のトラブルシューティング</u>

<u>CLIのトラブルシューティング</u>

<u>CSDACデバッグモード</u>

<u>デバッグ付きログメッセージ</u>

<u>トラブルシューティングのウォークスルーの問題例</u>

問題とトラブルシューティングの概要

<u>問題:</u>

```
<u>トラブルシューティング:</u>
トラブルシューティングバンドルの準備
IPのタグ属性を確認します
<u>チェックの概要</u>
```

<u>Q&A</u>

はじめに

このドキュメントでは、FMCのCisco Secure Dynamic Attribute Connector(DAC)について説明します。

背景 – 問題

CSDAC(Cisco Secure Dynamic Attributes Connector)をFMC(Firepower Management Center)に統 合すると、スタンドアロンのCSDACアプリケーションおよびCDOのCSDACと同じレベルの機能 を提供できます。スタンドアロンCSDACでは、CSDAC用の個別マシンの管理と保守のオーバー ヘッドから顧客を解放します。ネットワーク管理者として、プログラマチックインターフェイス を統合し、外部のダイナミック環境プロバイダーの変更に合わせて最新の状態を維持しやすくし たいと考えています。この統合により、ポリシーを導入することなく、動的に変化するクラウド 環境から属性を収集するという問題が解決されます。

ソリューション(概要)

CSDACをFMCで構成して、Azure、vCenter、AWS、GCP、Office 365、およびAzure Service Tagからタグ属性を取得できるようになりました。これにより、CDOのスタンドアロンCSDACお よびCSDACと同等の機能が提供されます。

- を使用する方法を選択できます
 - FMCのCSDAC(または)
 - CDOのCSDAC (または)
 - スタンドアロンCSDAC
- ターゲット市場:エンタープライズ、サービスプロバイダー

FMCでのダイナミック属性コネクタの概要

FMCダイナミック属性コネクタ:

- 動的属性コネクタ機能を構築および操作するためのダッシュボード画面。
- ソースワークロードコネクタ(AWS、Azure、vCenter、Office 365、GCP)を構成するための FMC UI
- ・ダイナミックオブジェクトを作成するダイナミック属性フィルタを定義するFMC UI

導入例

オンプレミスCSDAC

昨年、AWSおよびAzureアカウントから属性を収集するために、CSDAC専用のVMをデプロイし ました。

問題

現在、組織がクラウドに移行したため、自分の環境にCSDAC専用の仮想マシンを導入して管理することができません。



オプション1:FMC内に構築されたダイナミック属性コネクタを使用する

この問題は、FMC内に組み込まれたダイナミック属性コネクタを使用して修正できます。これに よって作成されたダイナミックオブジェクトは、アクセスポリシーで使用できます。

オプション2:クラウド提供のダイナミック属性コネクタをCDOで使用する

この問題は、CDOのダイナミック属性コネクタを使用して修正できます。作成された動的オブジ

ェクトは、

- CDOクラウド提供FMC
- CDOオンプレミスFMC

前提条件、サポート対象プラットフォーム、ライセンス

サポートされる最低限のソフトウェアおよびハードウェアプラットフォーム

サポートされる Managerの最小バー ジョン	管理対象デバイス	サポートされる管理 対象デバイスの最小 バージョンが必要	注意事項
FMC 7.4	サポートされる任意 のFTD	任意の7.0以降のFTD	

*動的属性コネクタは、FDM管理対象デバイスではサポートされません

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ 7.4を実行するCisco Firewall Management Center
- ・ 7.4以降を実行するCisco Firepower Threat Defense

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

機能の詳細

スタンドアロンCSDACの概要(現在リリースされている – 7.4)

Cisco Secure Dynamic Attributes Connectorを使用すると、Firewall Management Center(FMC)ア クセスコントロールルールのさまざまなクラウドサービスプラットフォームのタグを使用できま す。

オンプレミスCSDACはLinuxマシンにインストール可能で、次の場所からの属性の取得をサポートします。

 AWS、Azure、VMware vCenterおよびNSX-T、Office 365、Azureサービスタグ、GCP、 GitHub。

CDOでのCSDACの概要(現在リリースされている – 7.4)

専用アプリケーションをインストールしてメンテナンスする必要がなく、オンプレミスの CSDACと同じ機能をサポート

vCenterコネクタは、現在CDOではサポートされていません。

CDOのクラウド配信FMCとオンプレミスFMCへの受信属性の送信をサポート

FMCでのCSDAC

スタンドアロンCSDACと同じ機能をサポートし、専用アプリケーションをインストールして維持 する必要はありません。

FMCのCSDACは次からの属性の取得をサポートしています:

 AWS、Azure、VMware vCenterおよびNSX-T、Office 365、Azureサービスタグ、GCP、 GitHub

FMCに対してローカルであるため、明示的なアダプタ設定はありません。

仕組み

コネクタは、AWS、Azure、o365、vCenterから属性を取得するために使用されます。

次に、ローカルアダプタを使用して、これらの合理化された属性とそのIPマッピングをFMCにダ イナミックオブジェクトとして保存します。

FMCはマッピングをリアルタイムでFTDに送信します(展開なし)。



FMCでCSDACを有効にします

「統合」>「動的属性コネクタ」にナビゲートします。

[切り替え]ボタンを使用して、コネクタを有効にします。

FMCでは、Dockerイメージとコンテナをダウンロードして起動するのに数分かかります。

これは、FMCグローバルドメインでのみ設定できます。



CSDACダッシュボード

CSDACを有効にすると、CSDACダッシュボードページが表示されます。ダッシュボードは、統 合コネクタとフィルタの設定と表示の両方に使用されます。

Firewall Management Center Integration / Dynamic Attributes Connector	Overview	Analysis	Policies	Devices	Objects	Integration
Dynamic Attributes Connector	Disable s Filters					
			You c	There is nothi an start with a sale the first corr corresp	ing configuree any of followin mector by clickin conding type:	f yet. ng actions: g on the
			A	AWS GCP GC to	vCenter vCenter 0365 Gith or Connectors	AST

コネクタの設定

ダッシュボードからコネクタを追加

ダッシュボードで、追加するコネクタのアイコンをクリックします。



コネクタが設定された周期性を持つプロバイダから情報をプルできるように、時間間隔(「プル 間隔」フィールド)を設定します。

プロバイダーの資格情報を入力して、タグ属性を取得します。コネクタを設定したら、「テスト」ボタンをクリックしてコネクタをテストできます。

Name*			
AWS			
Description			
			lti
Pull Interval (se	c)*		
30			
Region*			
us-cast-1			
Access Key*			
AKIA2PWAVD	BNRHF6UKIQ		
Secret Key*			
•••••			

フィルタの設定

「動的属性コネクタ」メニューの「動的属性フィルタ」タブをクリックして、「動的属性フィル タ」ページに移動します。

Dynamic Attributes Connector Consultation Disable Dashboard Connectors Dynamic Attributes Filters						
0 dynamic attributes filters						
8 Name Connector	Query	Actions				
There are no Dynamic Attributes Filters yet. Create a Dynamic Attributes Filter						

フィルタの追加

+ボタンをクリックして、属性コネクタのフィルタを作成します。

Firewall Management Center Overview	Analysis Policies Devices Objects Integration	Deploy Q, 🦑 🗘 🕢 admin •
Dynamic Attributes Connector 🗨 Disable		
Dashboard Connectors Dynamic Attributes Filters		
0 dynamic attributes filters		
# Name Connector	Query	Actiona
	There are no Dynamic Attributes Filters yet.	
	Create a Cynamic Autobas Prov	

AWSタグの追加

たとえば、AWSワークロードのキー「HR」と値「App」に関心があると仮定できます。

これはAWSで表示される内容です。

aws 🗰 services Q Search	for services, features, blogs, docs, and more [Option+5]	L A
New EC2 Experience X	☐ i-0e3e344f2405ba92c	🗇 3.223.6.235 open address 🗹
EC2 Dashboard EC2 Global View Events	IPv6 address - Hostname type	Private IP DNS name (IPv4 only)
Limits	IP name: ip-172-31-15-97.ec2.internal	ip-172-31-15-97.ec2.internal Elastic IP addresses
Instances Instances Instance Types Launch Templates	t3.medium AWS Compute Optimizer finding ③Opt-in to AWS Compute Optimizer for recommendations.	IAM Role
Spot Requests Savings Plans Reserved Instances	Details Security Networking Storage St	atus checks Monitoring Tags
Dedicated Hosts Scheduled Instances Capacity Reservations	Tags ଦ	
Mis New	Кеу	Value
AMI Catalog	HR	Арр

FMCでのCSDAC

+ボタンをクリックすると、「HR equals App」ルールを作成できます。

ローカルFMCアダプタは、一致するIPアドレスをダイナミックオブジェクトマッピングとして FMCに送信します

Add Dynamic Attribute Filter			
Name*		Connector* aws1	~ +
Туре	Op. Value		
	eq (any) App		:
> Show Preview			Cancel Save

プレビュー

特定の属性ルールに一致するIPアドレスを表示するには、 | [プレビューを表示しない]ボタン

Add Dynamic Attribute Filter			
Namo*		Connector*	
hr_app		aws1	
Tune	On. Value		0
RH (119)	eq (etc) App		1
~ Hide Preview			
172.31.26.184		App	
172.31.31.21		App	
172.31.33.85		App	
3.223.6.235		App	

動的オブジェクト

FMCのObjects > External Attributes, Dynamic ObjectでCSDACによって作成された動的オブジェ クトを表示します

Defense Orchestrator Otjects / Object Management	Monitoring	Policies	Devices (Objects Integration	*> Return to Inventory	Deploy Q	• •	aplakshm@cisco.com	tere s	ECURE
> AAA Server > Access List	Dynamic Ob	jects o						T Filter		•
> Address Pools	Name		Descr	lption				Number of Mapped IPs		
Application Filters	hr_app								01	÷.
AS Puth										
Cipher Suite List										
> Community List										
> Distinguished Name										
DNS Server Group										
 External Attributes 										
Dynamic Object										
File List										

ACポリシー

設定:アクセスポリシー

FMCで、ダイナミック属性コネクタから受信したダイナミックオブジェクトを許可またはブロッ クするアクセスポリシーを追加します。

➡ Return to P ■ Default Ac □ Packets →	Switch to Legacy UI Switch to Legacy UI Default Access Control Policy Packets → Prefitter Rules → OSL → Security Intelligence → Identity → Access Control More Targeted: 1 device									
TIQ					Ø Total 2 ru	les	📯 🏭 🔳 🛛 Add Category	Add Ri		
			Source			Destina		itination		
	Name	Action	Networks	Ports	Zones	Networks	Ports	Dynamic Attributes	Ap	
🗌 🗸 Man	datory (1 - 2)									1
	1 Accounting to Azure Cloud	Allow	Accounting	Any		Any		AzureServiceTag_AzureCloud_australiaeast		1
0	2 Engineering to Sharepoint	Block	Engineering	Any	Any	Any	Any	o365_SharePoint	Ar	+
 Defa 	ult									1
There ar	e no rules in this section. Add R	tule or Add Catego	iry .							

プラットフォームの制限

- ・コネクタの制限は、使用可能なFMCメモリに基づいています。
- vFMCでは、5つのコネクタをサポートするために追加の1 GBメモリが必要です
- Azure ADレルムもCSDACコンテナーであるため、制限に含まれています。

モデル	サポートされるコネ クタの数	プラットフォーム	メモリに基づく制限
基本	Azure ADのみ	1600	32 GB
小	5	vFMC	32 GB超
中	10	vFMC 300、2600	>= 64 GB
×	20	4600	128 GB以上

トラブルシューティング/診断

トラブルシューティングは、FMCでCSDACコネクタからDynamics属性に対する動的オブジェク トをトレースすることによって実行するのが最適です。多くの内部ログでは、この機能を「マス ター」と呼んでいます。ブロードキャストチェーンに沿ってシステム状態を確認し、問題を切り 分けることができます。CSDACはDockerコンテナを使用します。 ログやその他のファイルのメ ッセージと名前は「docker」と呼ぶ必要があります。



コネクタの確認

最初に、コネクタがvCenter、AWS、またはAzureサーバーに接続できることを確認します。

コネクタが正しく設定されていない場合、ダウンストリームプロセスはタグ情報を取得できません。

コネクタタブからのコネクタの表示

コネクタステータスはステータスフィールドに表示され、15秒ごとに更新されます。

ここで、コネクタが指定された資格情報を使用して認証できなかったことがわかります。

Firewall Management Center Overview	Analysis Policies Devices Objects Integr	asian Depky Q 💞 🗘 😡 admin 🔹 🔐 SECURE
Dynamic Attributes Connector 🇨 Disable		
Deshboard Connectors Dynamic Attributes Filters		
1 connector		Ensu: An error accurred (AutoFalure) when calling the Describel instances operation: AMIS an ort tible kit validate the provided
I Name Description	Type	access credentials Actions
1 AUS	<i>M</i> IS	Entr 0 E

属性フィルタの確認

ルールのプレビューに、クエリ条件に一致するIPアドレスが表示されていることを確認します。

一致するIPアドレスがない場合、FMCはダイナミックオブジェクトマッピングを取得できません 。

属性フィルタのチェック

ダイナミック属性IPマッピングがプレビューで使用できることを確認します。[プレビューを表示]ボタンは、[ダイナミックアトリビュートフィルタ]編集ポップアップで使用できます。

Edit Dynamic Attribute Filter							
Name* east_sws_object			Connector* ans_wast	~			
Query*	Op.	Value		+			
HR HR	eq	(any) App		I			
~ Hide Preview							
172.31.25.40 172.31.20.184							
172.31.31.21							

FMCのUIでダイナミックオブジェクトを確認する

最初に、FMCサーバに必要なバインディングが含まれていることを確認します。

- [オブジェクト管理]の[外部オブジェクト]タブで、[ダイナミックオブジェクト]の[バインド]をオンにします。
- FMCがバインディングを取得しない場合、FTDはバインディングを取得できません。

FMCヘルスモニタとCSDACヘルスアラート通知を確認します。

動的オブジェクトのチェック

FMC Object Managerを使用すると、現在のDynamic Object IPアドレスをダウンロードできます。

cisco Object Management	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹ (¢ 9	🛿 admin 🗸
Cipher Suite List Community List Distinguished Name Dynamic Objects A dynamic object represents one or more attributes which can be dynamically mapped to the object. You can use dynamic objects in					Add	Dynamic Object	Q, Fil	ler			
DNS Server Group ✓ External Attributes	Accountant_PC				Number of Mapped IPs 0						
File List > FlexConfig Geolocation	Engin Finan Produ	eer_PC ce_Server uct_Developm	ent_Server					0			±/11 ±/11 ±/11

CSDACヘルスアラート

ダイナミック属性コネクタなどのコアサービスがダウンした場合、FMCのタスクマネージャにヘルスアラートが表示されます。 アラートには、サービス名とステータスに関する情報が含まれます。



注:いくつかの通知には「マスター」という名前が残っています。ここでは、詳細情報 を提供するサービス名を指定する必要があります。

Firewall Management Center Overview	Analysis Policies Dev	cec Objects Integration	Deploy Q 🚱 🏠 🕢 admin 🗸 📩
Dynamic Attributes Connector Deshboard Connectors Dynamic Attributes Filters	Updaling statuses		Control of the information

ここでは、muster-beeとmuster-local-fmc-adapterが「異常」であることが確認できます。

errorがコアサービスのいずれかを示している場合は、デバッグ用にトラブルシューティングログ を収集する必要があります。



トラブルシューティングのCSDAC

CSDACの生成のトラブルシューティング

- FMCのトラブルシューティングの生成中に、CSDACログが自動的に収集されます。バンド ルには、Dockerのステータス、ログ、および問題をオフラインでデバッグするために必要 なデータが含まれています。
- トラブルシューティングログが収集されるエラーを再現する前に、CSDACデバッグモード を有効にすることを推奨します(推奨)。

/usr/local/sf/csdacから。/mster-cli debug-onを呼び出します。

次のフォルダでuntarredのCSDACログを探し、Troubleshootします。

/results-XX/command-outputs/csdac_troubleshoot/info

これには、etcdデータベースに保存されているデータが含まれます。

/results-XX/command-outputs/csdac_troubleshoot /log

これには、Dockerコンテナからのログが含まれます。

/results-XX/command-outputs/csdac_troubleshoot/status.log

コンテナのステータス、バージョン、およびDockerイメージの詳細が表示されます。

CLIのトラブルシューティング

muster-cliスクリプトを使用して、FMC CLIからCSDACのステータスを確認できます。

サービスのステータスが「Exited」であるか、または「Up」と異なる場合は、まずそのコンテナ のログをチェックします。

ログを取得するにはコンテナ名が必要です。出力から取得できます。

<pre>'root@firepower:/Volume/home/admin# cd /usr/local/sf/csdac/ root@firepower:/usr/local/sf/csdac# ./muster-cli status CORE SERVICES</pre>								
Name	Command	State	Ports					
muster-bee	./docker- <u>entrypoint.sh</u> run	Up	127.0.0.1:15050->50050/t	cp, 50443	3/tcp			
muster-envoy	/docker-entrypoint.sh runs	Up	127.0.0.1:6443->8443/tcp					
muster-local-tmc-adapter	./docker-entrypoint.sh run	Up						
muster- <u>ul</u> -backend	./docker-entrypoint.sh run	Up	50031/tcp					
======================================								
	Name		Command	State	Ports			
muster-connector-aws.2.muster			ker-entrypoint.sh run	Up	50070/ <u>tcp</u>			
muster-connector-o365.1.muster			ker- <u>entrypoint.sh</u> run	Up	50070/ <u>tcp</u>			

デバッグログのオンとオフを切り替えるには、「muster-cli」スクリプトを使用できます。デフォ ルトでは、コンテナはINFO level.INFOに記録され、DEBUGのみがサポートされているレベルで す。

デバッグレベルのユーザを有効にするには、./moster-cli debug-onを実行します。

これにより、トラブルシューティングの生成とデバッグのヘルプに関する詳細情報が提供されま す。このオプションは、問題を再現するときに有効にする必要があります。

INFOレベルに戻るには、./muster-cli debug-offを使用します。

<#root>

root@firepower:/usr/local/sf/csdac# ./muster-cli debug-on

Recreating muster-bee ... Recreating muster-bee ... done Recreating muster-user-analysis ... done Recreating muster-local-fmc-adapter ... done Recreating muster-ui-backend ... done

デバッグ付きログメッセージ

デバッグモードを有効にすると、すべてのDockerコンテナログにもデバッグメッセージが含まれ ます

dockerコマンドを使用してリアルタイムでログを取得する: docker logs -f < container_name>

次の例では、デバッグメッセージによってgRPCエラーがトリガーされたことが示されています

<#root>

2022-12-12 14:33:29,649 [status_storage] DEBUG: Loading status from /app/status/aws.1_status.json... 2022-12-12 14:33:29,650 [status_storage] DEBUG: Loading status from /app/status/gcp.1_status.json... 2022-12-12 14:33:29,651 [status_storage] DEBUG: Loading status from /app/status/github.1_status.json... 2022-12-12 14:33:29,651 [status_storage] DEBUG: Loading status from /app/status/o365.1_status.json... 2022-12-12 14:33:43,279 [server] DEBUG: Got health status request.

2022-12-12 14:33:43,280 [bee_api] WARNING: Got gRPC error from BEE: StatusCode.UNAVAILABLE failed to con

トラブルシューティングのウォークスルーの問題例

問題とトラブルシューティングの概要

問題:

発生する最も一般的な問題は、FMCがすべてのダイナミックオブジェクトマッピングを受信しないことです。

トラブルシューティング:

この問題をトラブルシューティングするために、

- 「muster-cli」からのデバッグモードの有効化
- FMC UIから生成されたトラブルシューティングファイル
- トラブルシューティングで収集したCSDAC AWS Connectorのログを確認。
- CSDAC AWS ConnectorがAWSインスタンスの最初のIPのみを照会したことが判明しました。

トラブルシューティングバンドルの準備

- FMCのCLIから、./moster-cli debug-onを使用してデバッグモードを有効にしました。 muster-cliツールは、/usr/local/sf/csdacにあります。
- コネクタのステータスがOKになるのを待ってから、ダイナミックアトリビュートフィルタ をチェックして、問題を再現。
- FMC UIからトラブルシューティングログを収集し、それらを抽出しました。スナップショットの内容についてAWS Connectorログを確認しました。



IPのタグ属性を確認します

特定のIPのタグ属性は、トラブルシューティングログに記録されます。AWS Connectorについては、muster-connector-aws.1.muster-docker.log.gzを参照しました。

チェックの概要

コネクタとアダプタのステータスは良好ですか。

対応する「コネクタ」、「アダプタ」の各ページでステータスを確認します。

コネクタはすべてのマッピングを取得しましたか。

ー致するIPアドレスのルールプレビューを確認します。

コネクタDockerログを調べて、マッピングを正しく照会しているかどうかを確認します。

RESTサーバはコネクタから動的なタグマッピングを受信しましたか。

FMCのダイナミックオブジェクトページをチェックします。

USMSログ(/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log内)をチェックして、FMC RESTサーバがCSDACからのAPI要求を正しく処理したかどうかを確認します。

Q&A

Q:ISEコネクタをサポートするオンプレミスCSDACのバージョンを教えてください。バージョン 7.4.0(ビルド1494)でもそのようなコネクタは表示されません。

A:これはスタンドアロンCSDACであり、FMCまたはCDOにはありません。これをテストするには、CSDAC対応パッケージが必要です。

Q:リリース時のオンプレミスCSDACのバージョンを教えてください。

A:おそらく2.1.0。

Q:APIを重ねたギアの画面が表示されています。CSDACだと思いますが、これはどういう意味で すか。

A:このCSDACにはAPIエクスプローラが組み込まれているため、そのページから CSDACをAPI呼び出すことができます。 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。