Déployer un connecteur d'attribut dynamique sécurisé dans FMC

Table des matières

Introduction

Ce document décrit le connecteur d'attribut dynamique sécurisé Cisco dans FMC.

Contexte - Problème

CSDAC (Cisco Secure Dynamic Attributes Connector) peut être intégré dans FMC (Firepower Management Center), offrant le même niveau de fonctionnalité que l'application CSDAC autonome et CSDAC dans CDO. Pour le CSDAC autonome, il évite aux clients les frais généraux liés à l'administration et à la maintenance d'une machine séparée pour le CSDAC. En tant qu'administrateur réseau, je souhaite que les interfaces de programmation soient faciles à intégrer et qu'elles soient à jour avec les modifications apportées aux fournisseurs d'environnement dynamique externes. Cette intégration résout le problème de la collecte d'attributs dans des environnements cloud en évolution dynamique sans déployer de stratégie.

Solution (résumé)

CSDAC peut désormais être configuré dans FMC pour récupérer des attributs de balise à partir d'Azure, vCenter, AWS, GCP, Office 365 et les balises de service Azure, fournissant une parité de fonctionnalité avec les CSDAC et CSDAC autonomes dans CDO.

- Vous pouvez maintenant choisir d'utiliser
  - CSDAC dans FMC (ou)
  - CSDAC dans CDO (ou)
  - CSDAC autonome
- Marché cible : entreprise, fournisseur de services

Connecteur d'attributs dynamiques dans le résumé FMC

Connecteur d'attributs dynamiques FMC :

- Tableau de bord pour créer et utiliser les fonctionnalités du connecteur d'attribut dynamique.
- Interface utilisateur FMC pour configurer les connecteurs de charge de travail source (AWS, Azure, vCenter, Office 365, GCP)
- Interface utilisateur FMC pour définir des filtres d'attributs dynamiques afin de créer des objets dynamiques

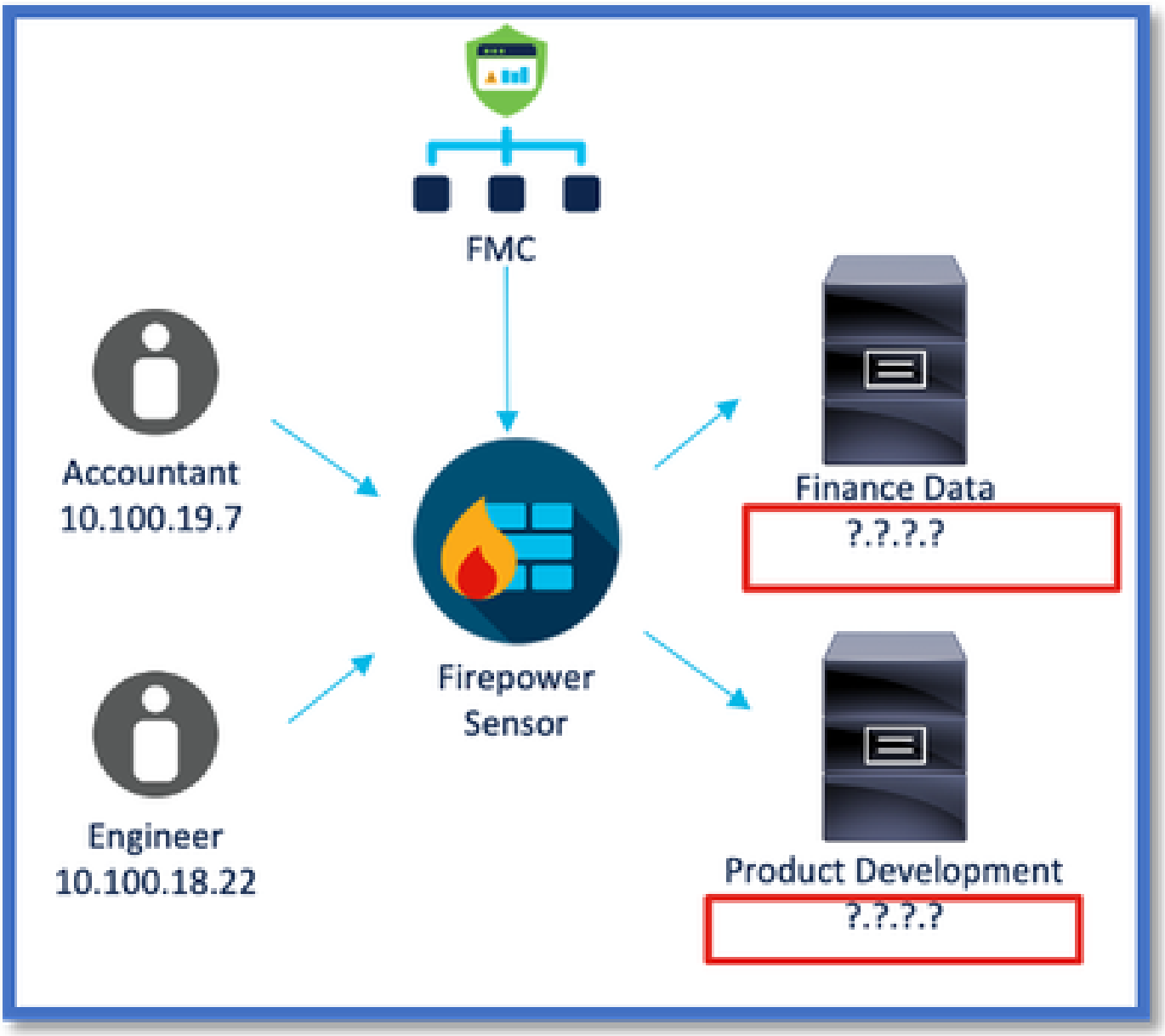
Exemples de déploiement

CSDAC sur site

L'année dernière, j'ai déployé une machine virtuelle dédiée pour CSDAC afin de collecter les attributs de mes comptes AWS et Azure.

Le problème

À présent, mon entreprise est passée au cloud et je ne peux pas déployer et gérer une machine virtuelle dédiée pour CSDAC dans mon environnement.



Option 1 : Utiliser le connecteur d'attributs dynamiques intégré à FMC

Vous pouvez résoudre le problème à l'aide du connecteur d'attributs dynamiques intégré à FMC. Les objets dynamiques qu'il crée peuvent être utilisés dans la stratégie d'accès.

Option 2 : utiliser le connecteur d'attributs dynamiques fourni dans le cloud dans CDO

Vous pouvez résoudre le problème en utilisant le connecteur d'attributs dynamiques dans CDO. Les objets dynamiques qu'il crée peuvent être utilisés dans

- CDO Cloud-Delivery FMC
- CDO FMC sur site

Conditions préalables, plates-formes prises en charge, licences

Plates-formes logicielles et matérielles minimales prises en charge

Version min. du gestionnaire supportée	Périphériques gérés	Version minimale du périphérique géré prise en charge requise	Remarques
FMC 7.4	Tout FTD pris en charge	Toute version 7.0+ FTD	

* Le connecteur d'attributs dynamiques n'est pas pris en charge sur les périphériques gérés par FDM

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :
· Cisco Firewall Management Center 7.4
· Cisco Firepower Threat Defense version 7.4 ou ultérieure.
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Détails des fonctionnalités

Présentation du CSDAC autonome (version actuelle - 7.4)

Le connecteur d'attributs dynamiques sécurisés Cisco vous permet d'utiliser des balises provenant de diverses plates-formes de services cloud dans les règles de contrôle d'accès du Centre de gestion des pare-feu (FMC).

Le CSDAC sur site peut être installé sur une machine Linux. Il prend en charge l'obtention d'attributs auprès de :

- AWS, Azure, VMware vCenter et NSX-T, Office 365, balises de service Azure, GCP, GitHub.

CSDAC dans CDO Aperçu (Version actuelle - 7.4)

Prend en charge la même fonctionnalité que le CSDAC sur site sans avoir à installer et à gérer une application dédiée.

Le connecteur vCenter n'est actuellement pas pris en charge dans CDO.

Prend en charge l'envoi des attributs reçus au FMC fourni dans le cloud et au FMC sur site dans CDO.

CSDAC dans FMC

Prend en charge la même fonctionnalité que le CSDAC autonome sans avoir besoin d'installer et de gérer une application dédiée.

CSDAC dans FMC prend en charge l'obtention d'attributs à partir de :

- AWS, Azure, VMware vCenter et NSX-T, Office 365, balises de service Azure, GCP, GitHub

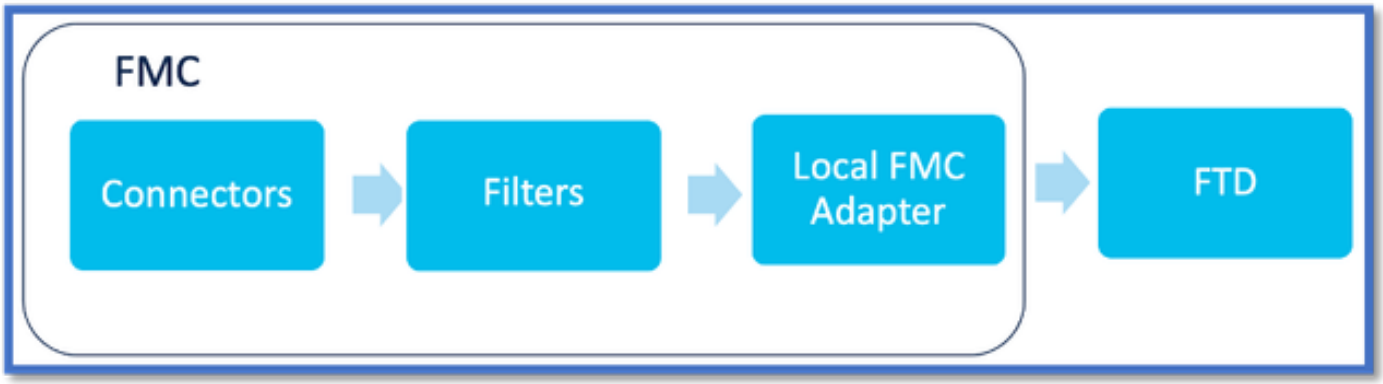
Il n'y a pas de configuration d'adaptateur explicite ici car elle est locale à FMC.

Comment ça fonctionne

Les connecteurs sont utilisés pour obtenir des attributs à partir d'AWS, Azure, o365, vCenter.

L'adaptateur local est ensuite utilisé pour enregistrer ces attributs rationalisés et ses mappages IP dans FMC en tant qu'objets dynamiques.

FMC envoie le mappage en temps réel à FTD (sans déploiement).



Activer CSDAC dans FMC

Accédez à Intégration > Connecteur d'attributs dynamiques.

Utilisez le bouton bascule pour activer le connecteur.

FMC prend quelques minutes pour télécharger et afficher les images et les conteneurs du docker.

Ce paramètre ne peut être configuré que dans le domaine global FMC.

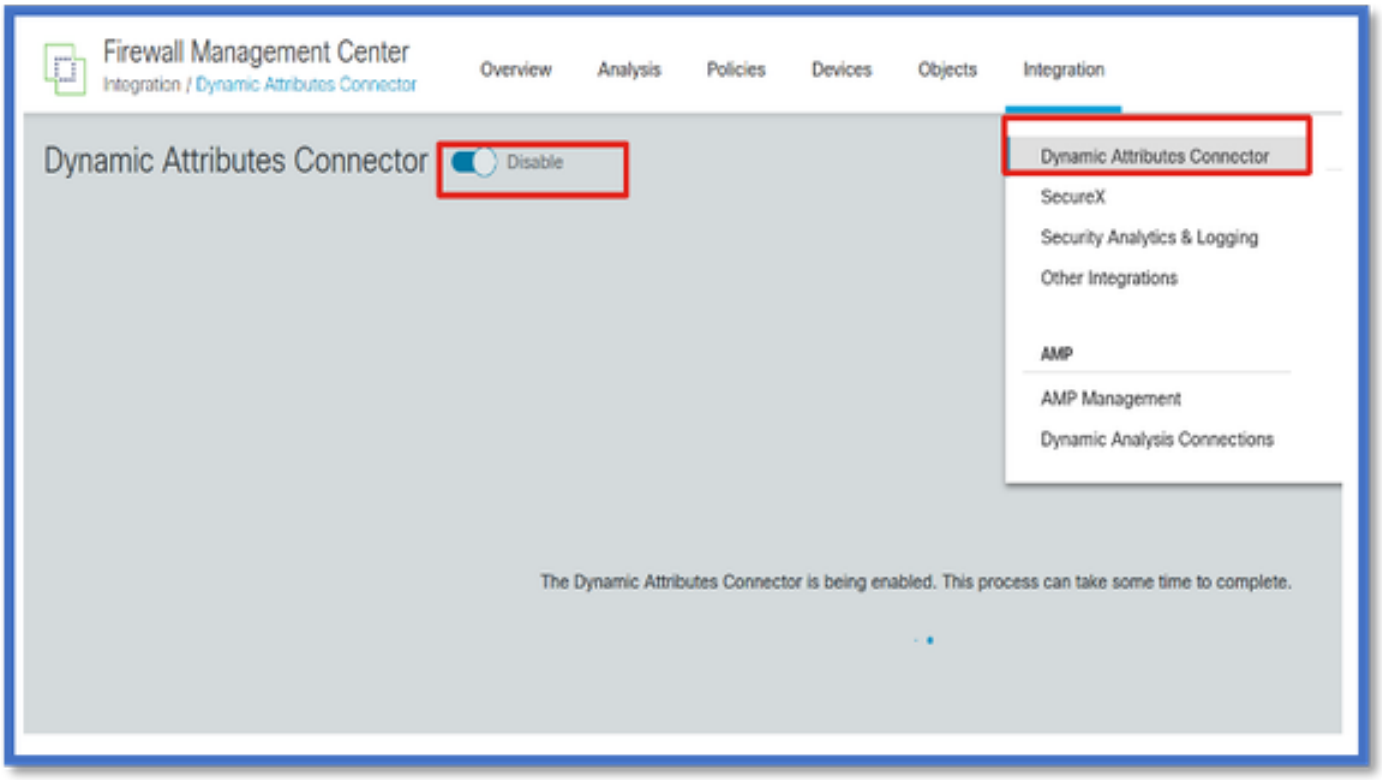
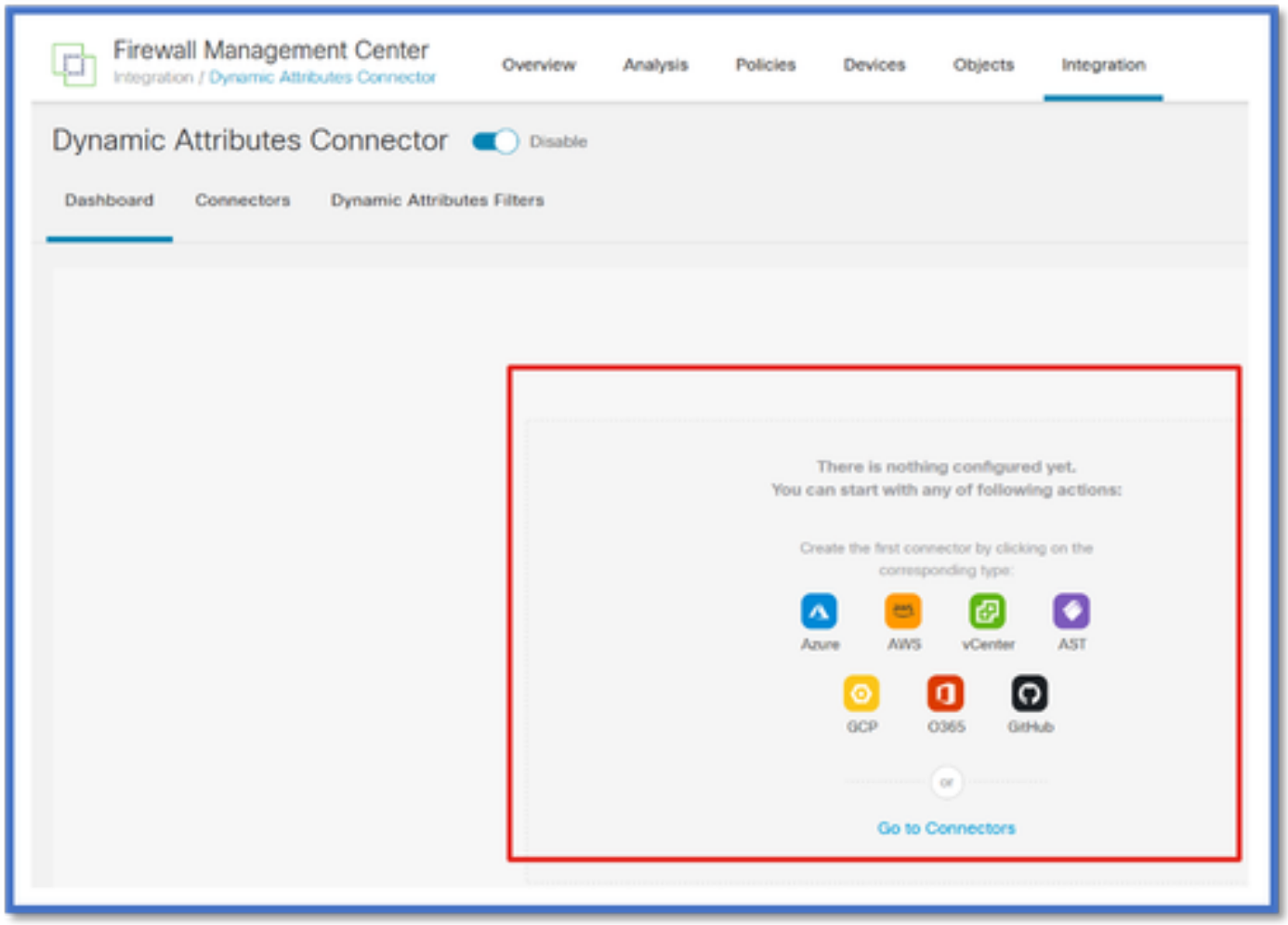


Tableau de bord CSDAC

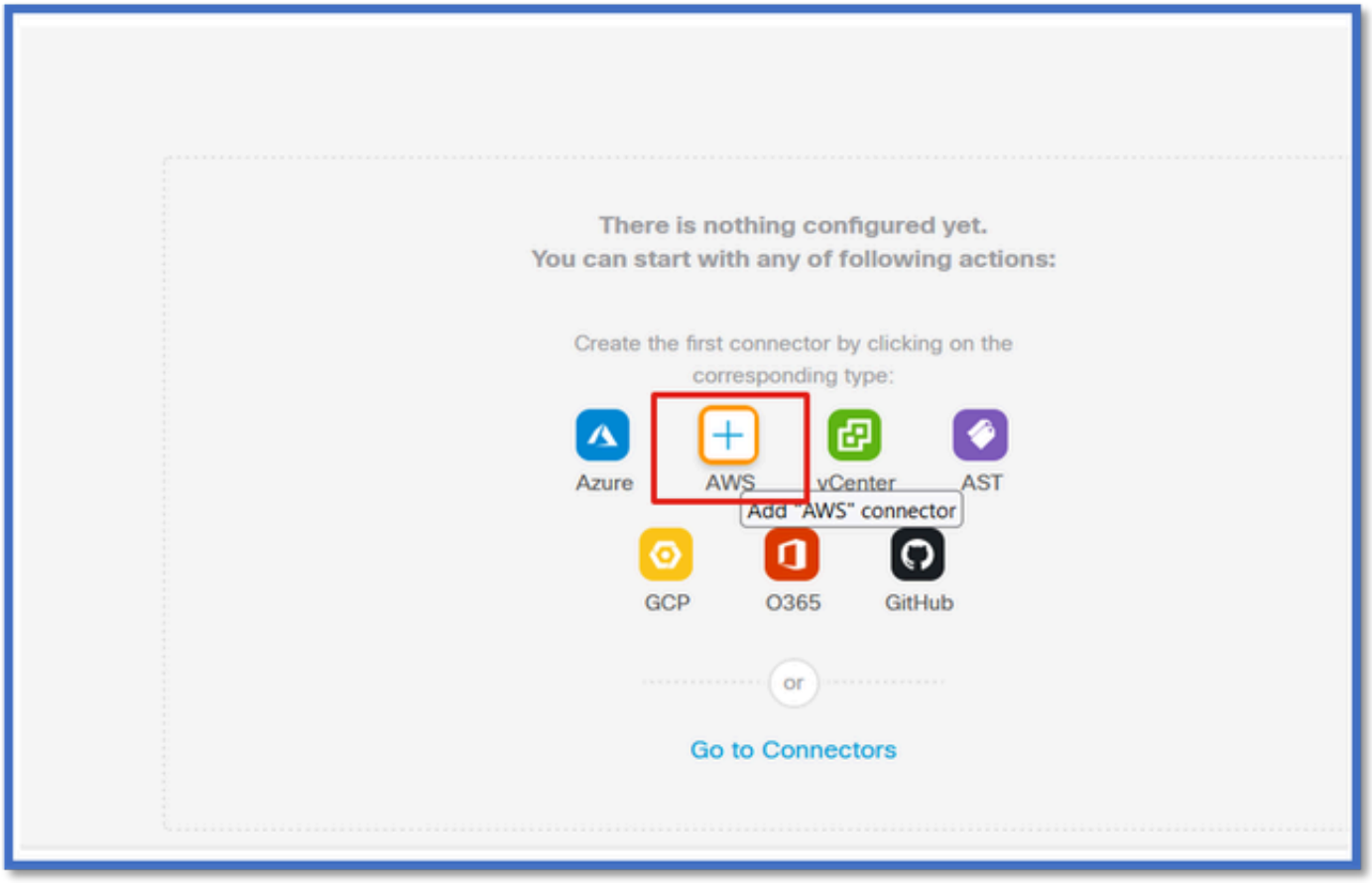
Après avoir activé CSDAC, l'utilisateur se voit présenter la page Tableau de bord CSDAC. Le tableau de bord permet de configurer et d'afficher les connecteurs et les filtres consolidés.



Configuration des connecteurs

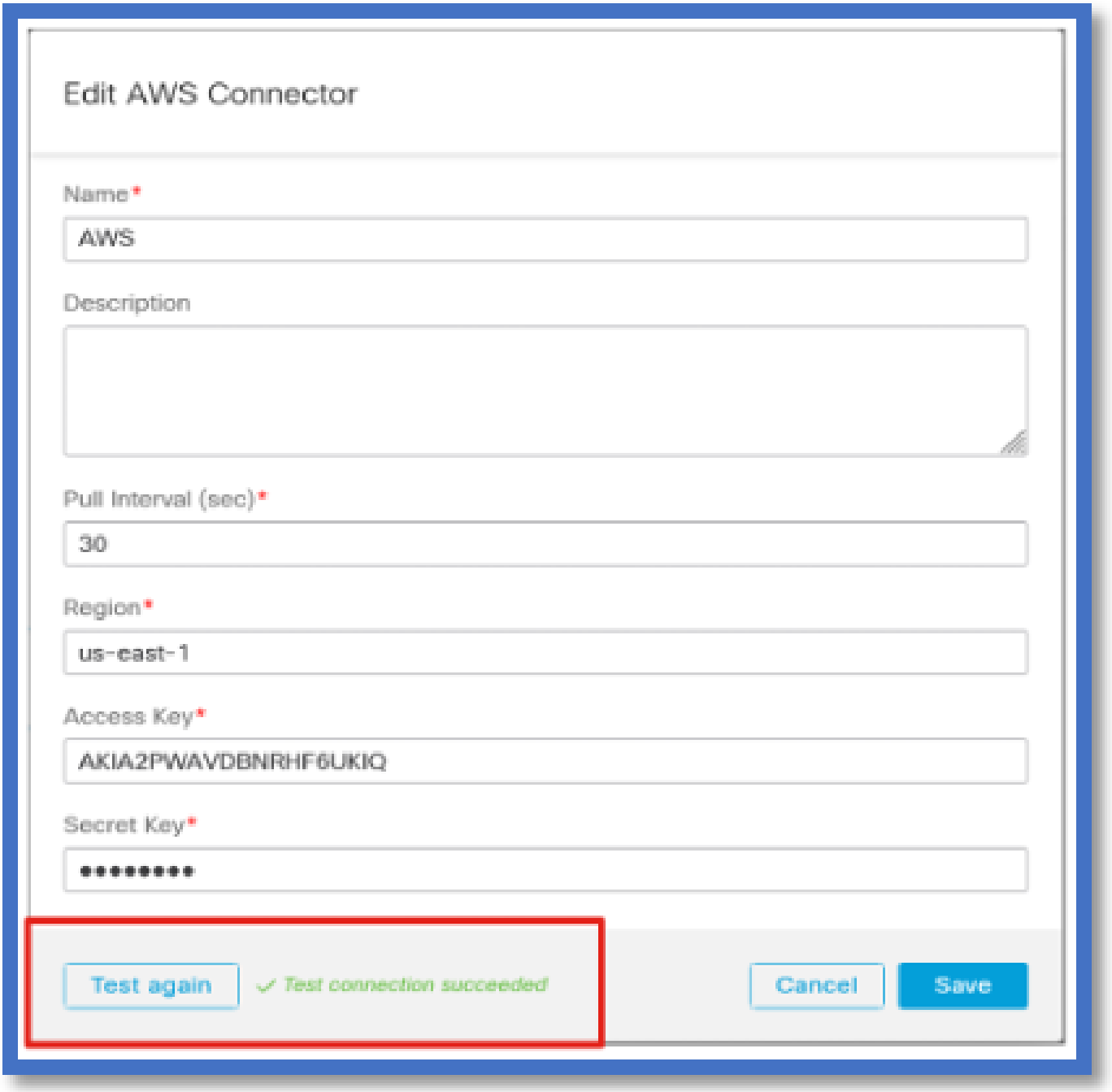
Ajouter des connecteurs du tableau de bord

Dans le tableau de bord, cliquez sur l'icône du connecteur souhaité pour l'ajouter.



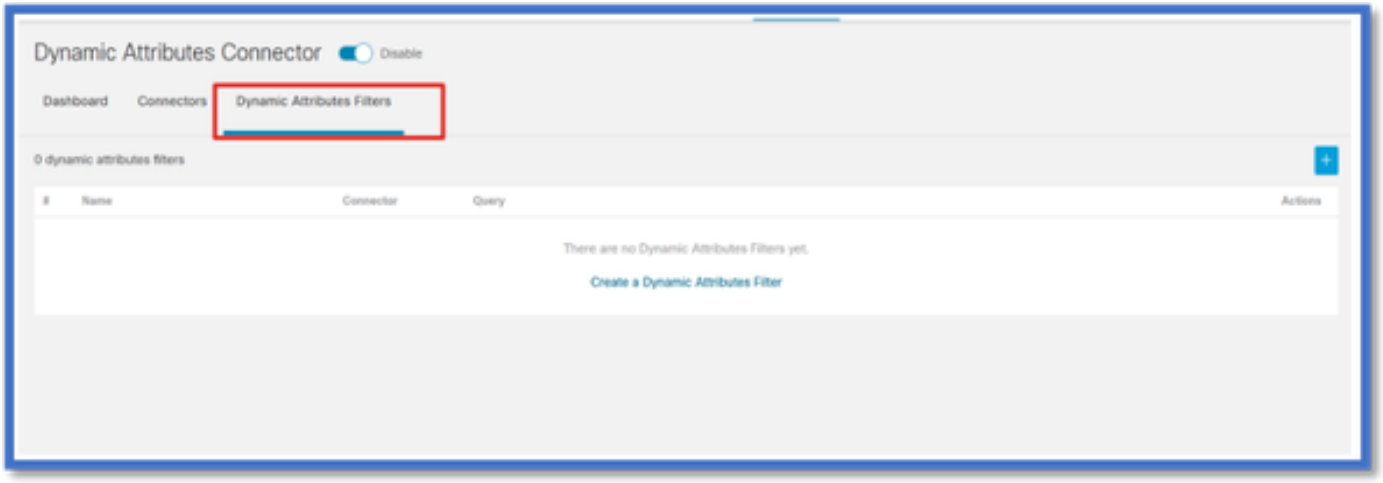
Configurez un intervalle de temps (dans le champ Intervalle d'extraction) pour que les connecteurs puissent extraire des informations des fournisseurs avec la périodicité configurée.

Entrez les informations d'identification du fournisseur pour obtenir les attributs de balise. Une fois le connecteur configuré, vous pouvez le tester en cliquant sur le bouton Test (Test).



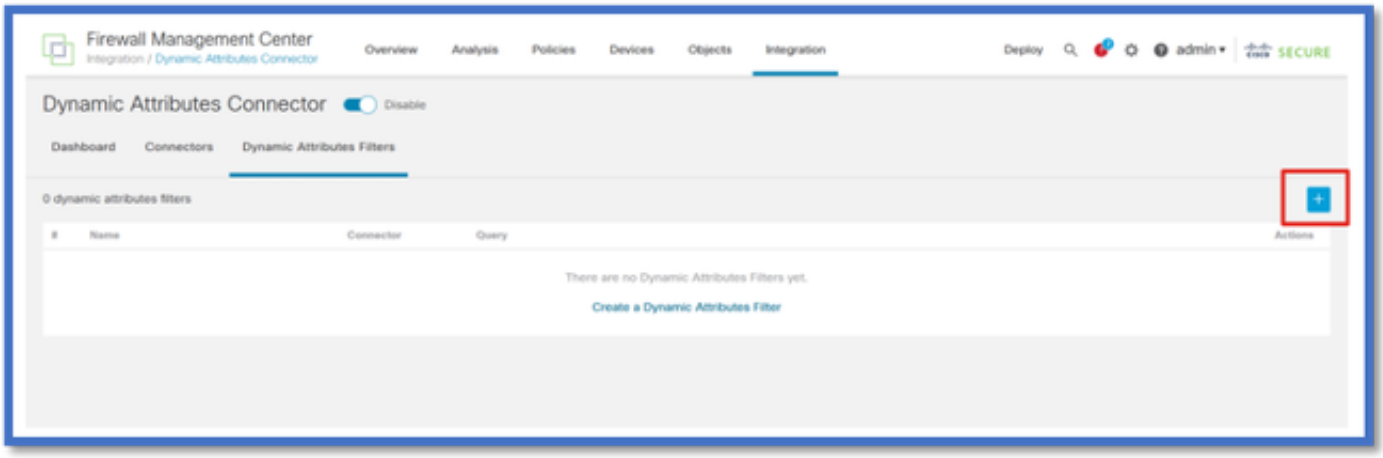
Configuration des filtres

Cliquez sur l'onglet « Filtres d'attributs dynamiques » du menu « Connecteur d'attributs dynamiques » pour accéder à la page Filtres d'attributs dynamiques.



Ajout de filtres

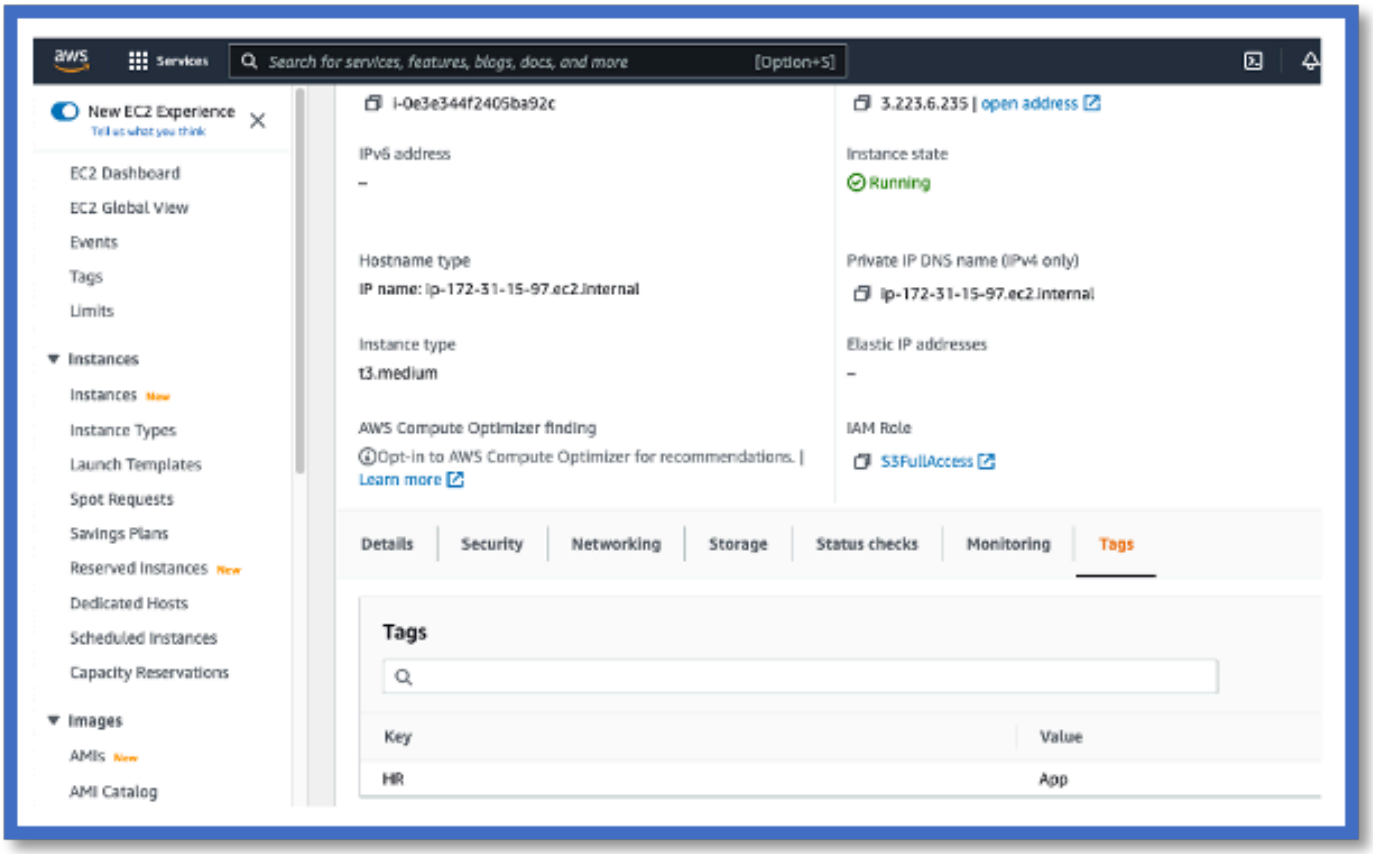
Cliquez sur le bouton + pour créer un filtre pour les connecteurs d'attribut.



Ajouter des balises AWS

Par exemple, nous pouvons supposer que vous êtes intéressé par la clé « RH » et la valeur « App » dans les charges de travail AWS.

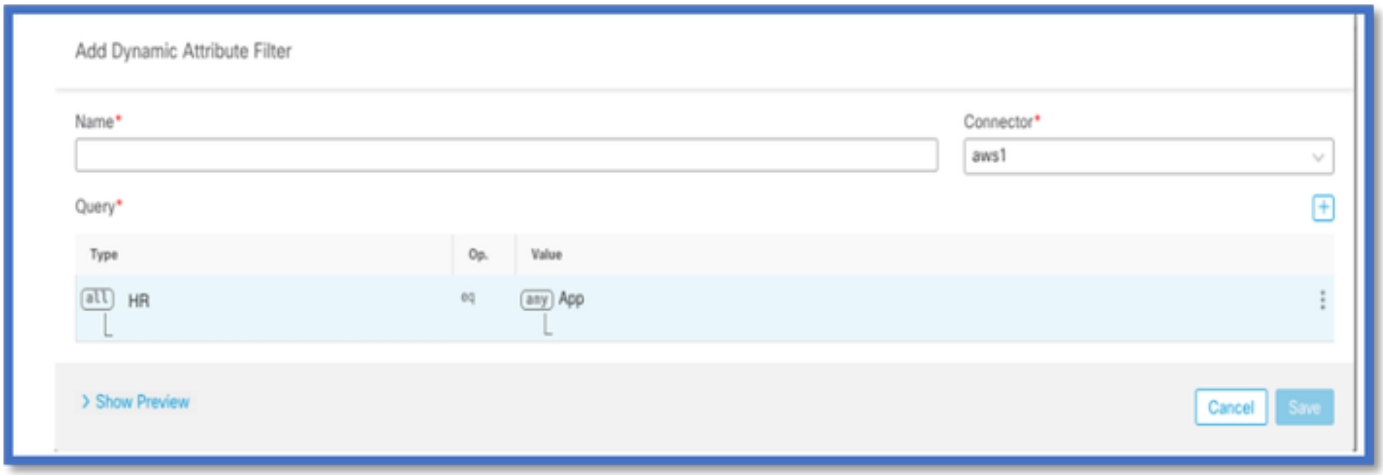
Voilà à quoi ça ressemblerait dans AWS.



CSDAC dans FMC

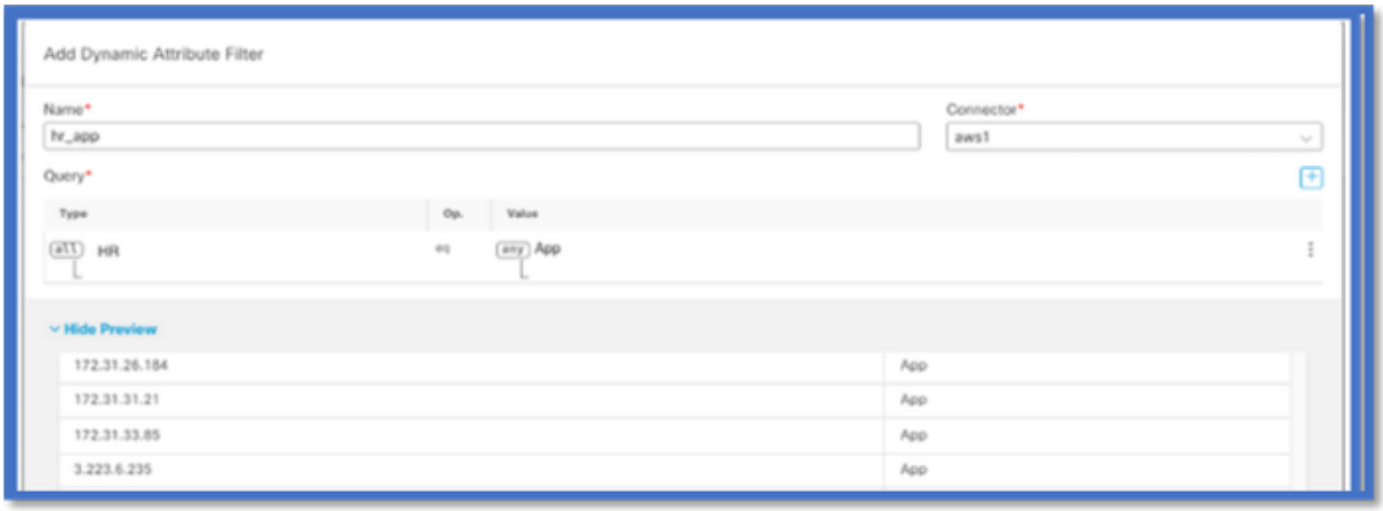
Vous pouvez créer une règle « HR = App » en cliquant sur le bouton +.

L'adaptateur FMC local envoie les adresses IP correspondantes sous forme de mappages d'objets dynamiques à FMC



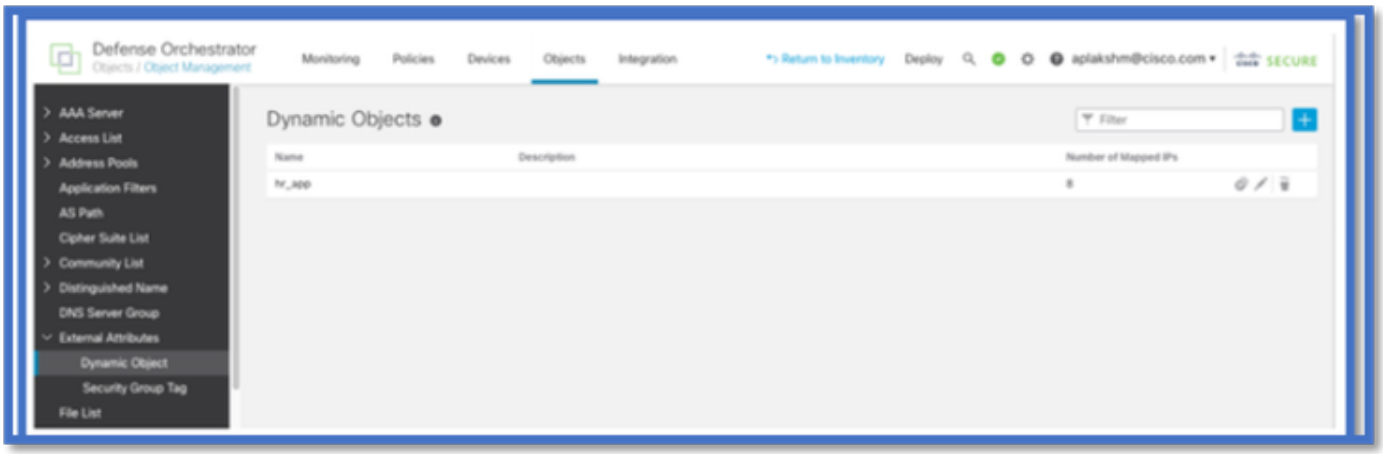
Aperçu

Vous pouvez également afficher les adresses IP correspondantes d'une règle d'attribut particulière en cliquant sur le bouton « Afficher » | Masquer le bouton Aperçu.



Objets dynamiques

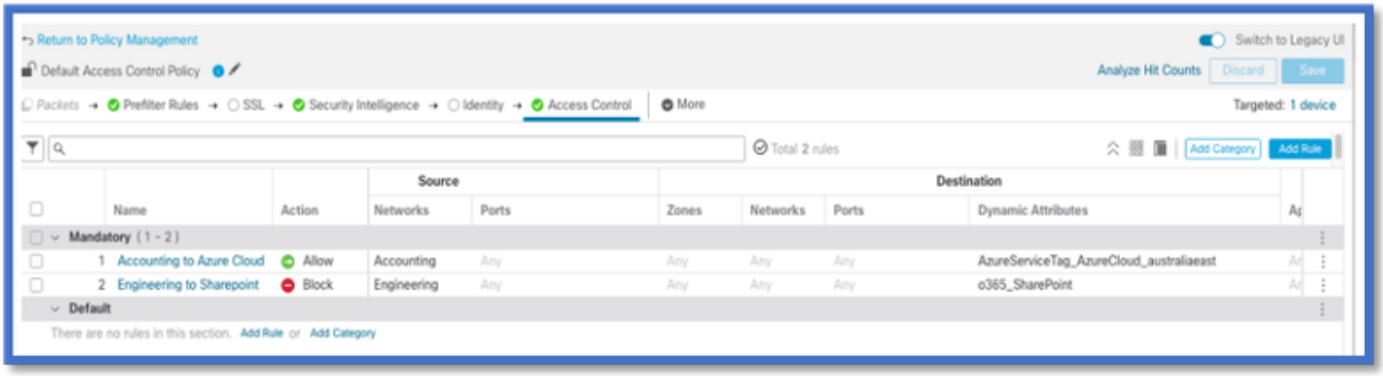
Affichez les objets dynamiques créés par CSDAC dans Objets > Attributs externes, Objet dynamique dans FMC



Politique CA

Configuration : politique d'accès

Dans FMC, ajoutez une stratégie d'accès pour autoriser ou bloquer les objets dynamiques reçus à partir du connecteur d'attribut dynamique.



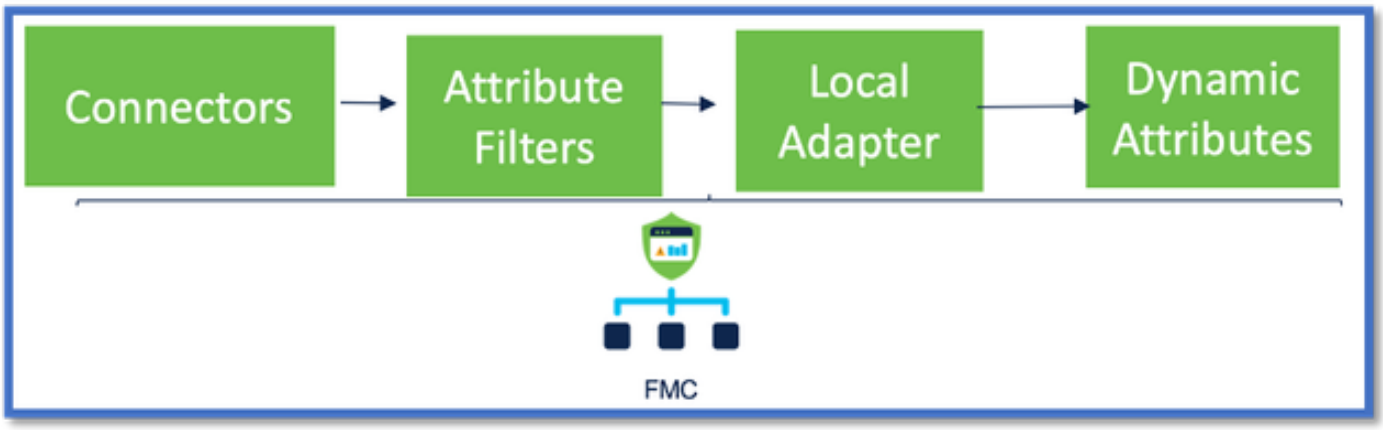
Limites de plate-forme

- Les limites des connecteurs sont basées sur la mémoire FMC disponible.
- vFMC nécessite une mémoire supplémentaire de 1 Go pour prendre en charge 5 connecteurs
- Le domaine Azure AD est également inclus dans la limite, car il s'agit également d'un conteneur CSDAC.

Modèles	Nombre de connecteurs pris en charge	Plates-formes	Limite basée sur la mémoire
De Base	Azure AD uniquement	1600	32 Go
Petite entreprise	5	vFMC	> 32 Go
Moyen	10	vFMC 300, 2600	>= 64 Go
Grand	20	4600	>= 128 Go

Dépannage / Diagnostics

Le dépannage s'effectue de préférence en traçant le ou les objets dynamiques depuis les connecteurs CSDAC vers les attributs dynamiques dans FMC.De nombreux journaux internes désignent cette fonctionnalité par le terme « rassemblement ». Vous pouvez examiner l'état du système le long de la chaîne de diffusion pour isoler les problèmes. CSDAC utilise des conteneurs Docker. Les messages et les noms des journaux et d'autres fichiers doivent être appelés « docker »



Vérification des connecteurs

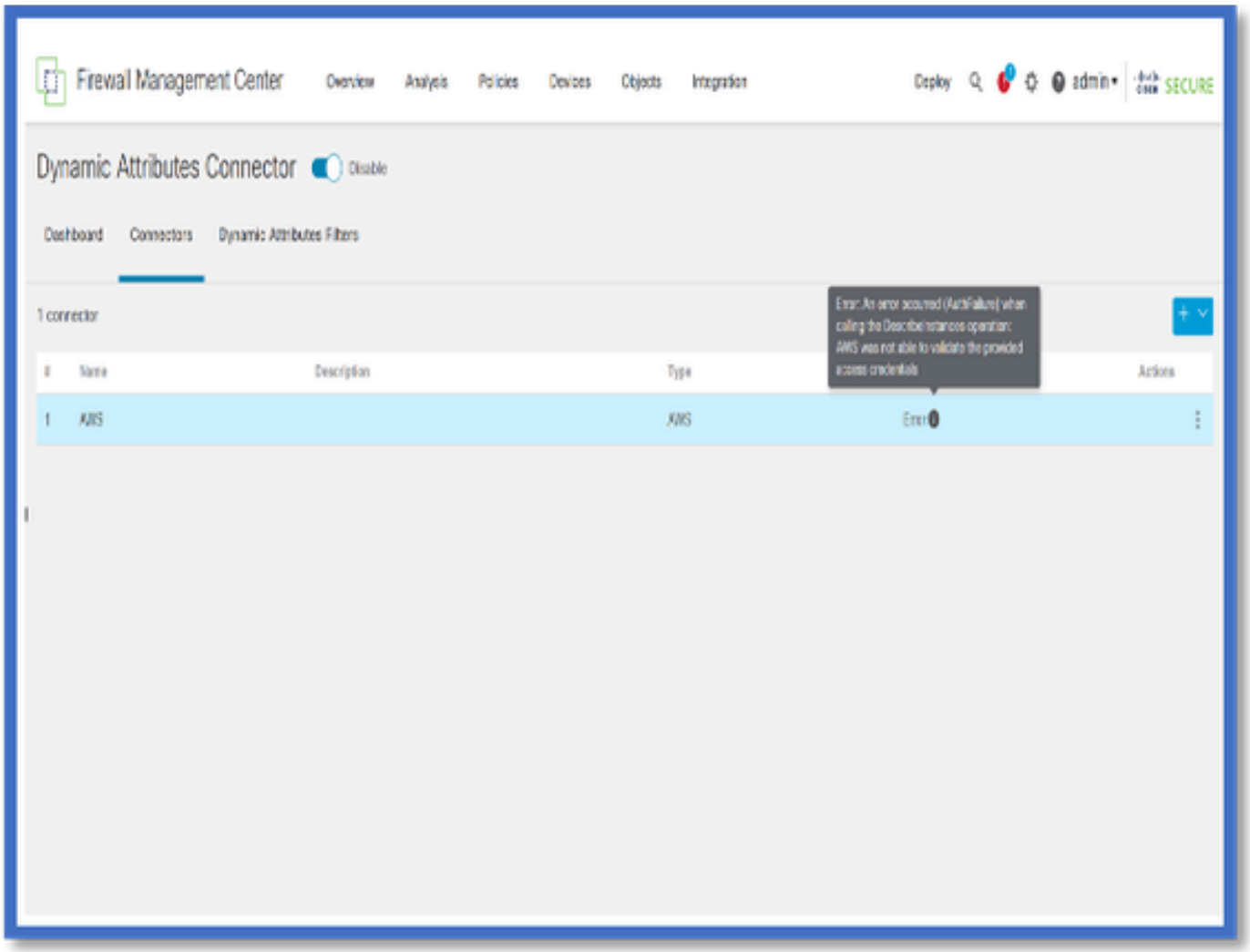
Assurez-vous d'abord que les connecteurs peuvent se connecter aux serveurs vCenter, AWS ou Azure.

Si les connecteurs ne sont pas configurés correctement, les processus en aval ne peuvent pas obtenir d'informations de balise.

Afficher les connecteurs dans l'onglet Connecteurs

L'état du connecteur est affiché dans le champ d'état et mis à jour toutes les 15 secondes.

Ici, nous voyons que le connecteur n'a pas pu s'authentifier en utilisant les informations d'identification fournies.



Vérifier les filtres d'attributs

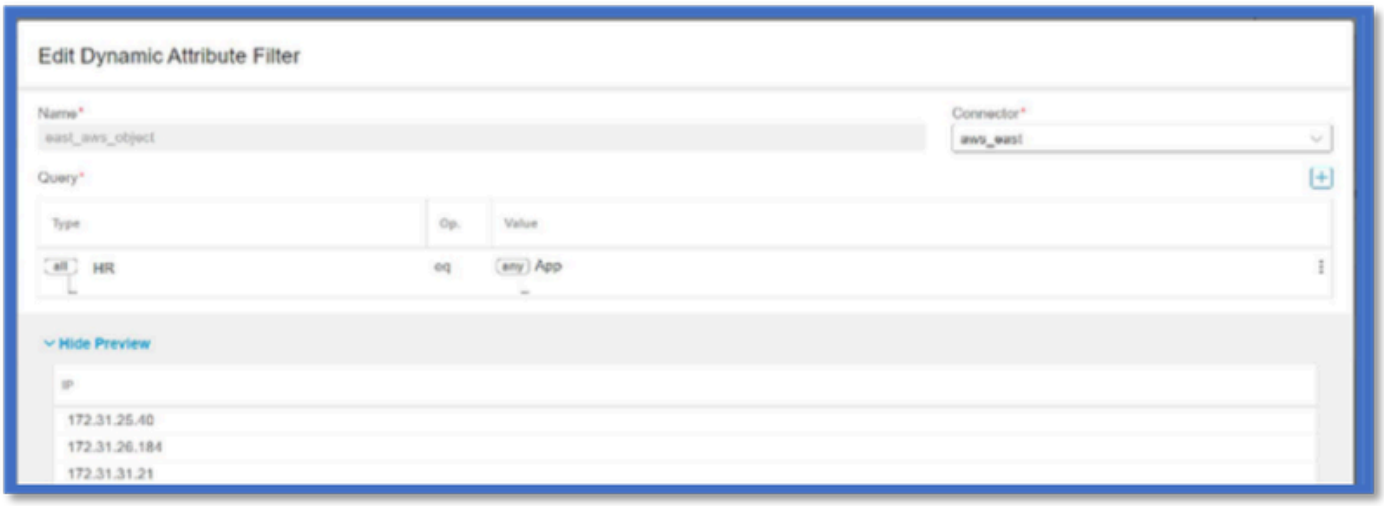
Assurez-vous que l'aperçu de la règle affiche les adresses IP correspondantes pour votre condition de requête.

Si aucune adresse IP ne correspond, FMC ne peut pas obtenir les mappages d’objets

dynamiques.

Vérification des filtres d'attributs

Vérifiez que les mappages IP d'attribut dynamique sont disponibles dans l'aperçu. Le bouton Afficher l'aperçu est disponible dans la fenêtre contextuelle Modifier le filtre d'attribut dynamique.



Vérification des objets dynamiques dans l'interface utilisateur FMC

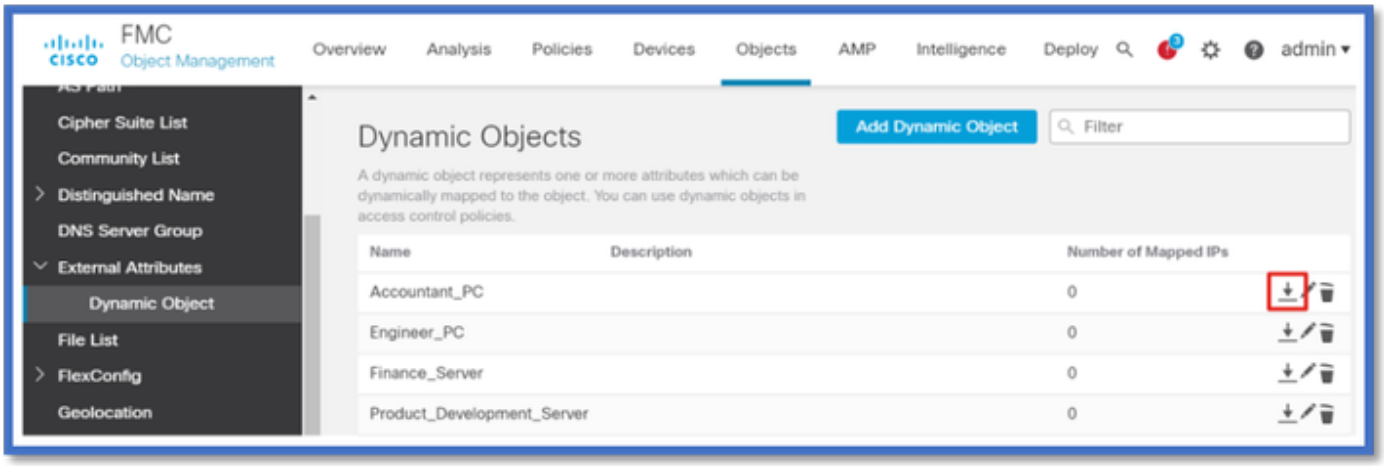
Assurez-vous d'abord que le serveur FMC contient les liaisons attendues.

- Sous Gestion des objets, onglet Objets externes, cochez la case Objets dynamiques pour les liaisons.
- Si FMC n'obtient pas les liaisons, alors FTD ne peut pas les obtenir.

Vérifiez FMC Health Monitor et Notifications pour les alertes d'état CSDAC.

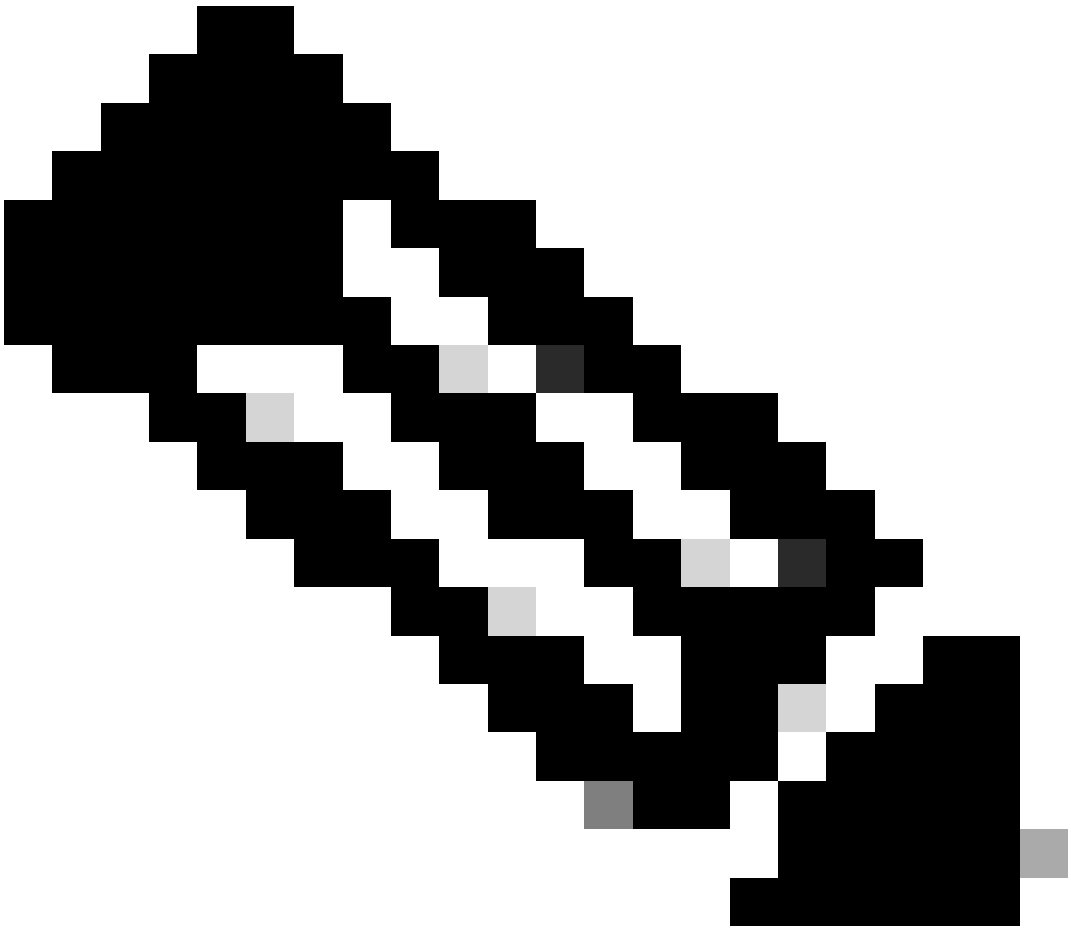
Vérification des objets dynamiques

Le Gestionnaire d'objets FMC vous permet de télécharger les adresses IP d'objets dynamiques actuelles.

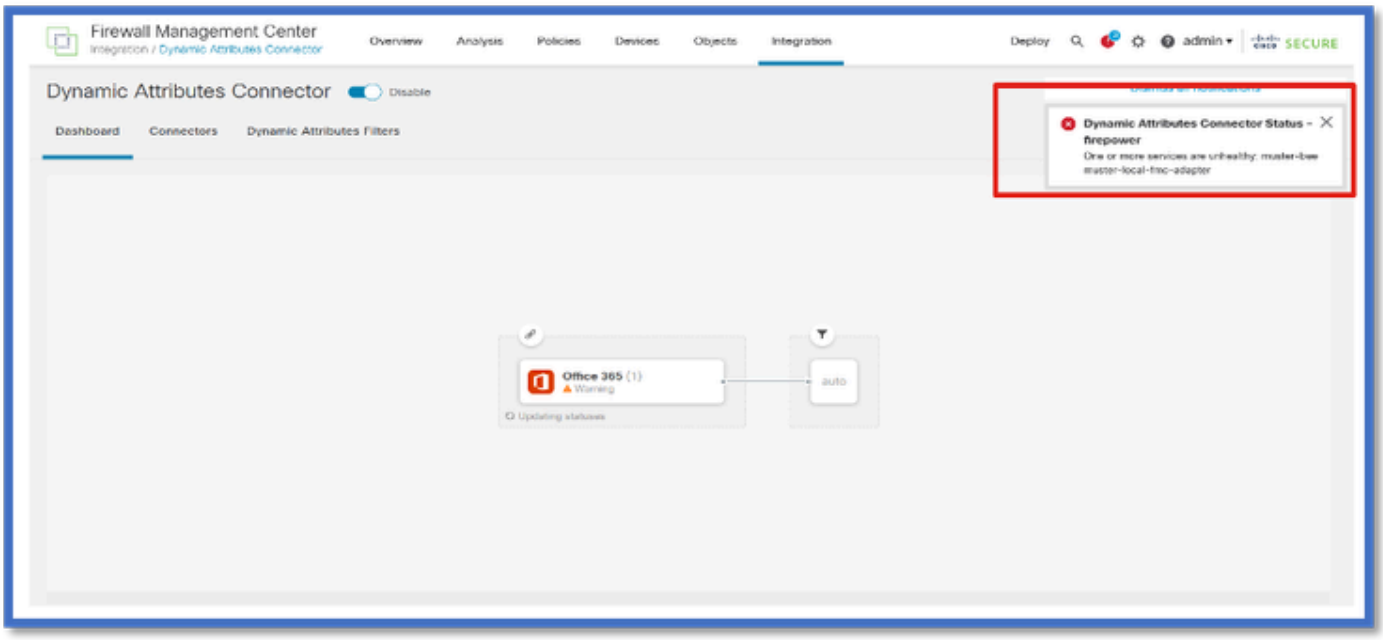


Alertes de santé CSDAC

Le Gestionnaire des tâches de FMC affiche des alertes d'intégrité si un service principal, y compris le connecteur d'attributs dynamiques, est en panne. L'alerte contient des informations sur le nom et l'état du service.

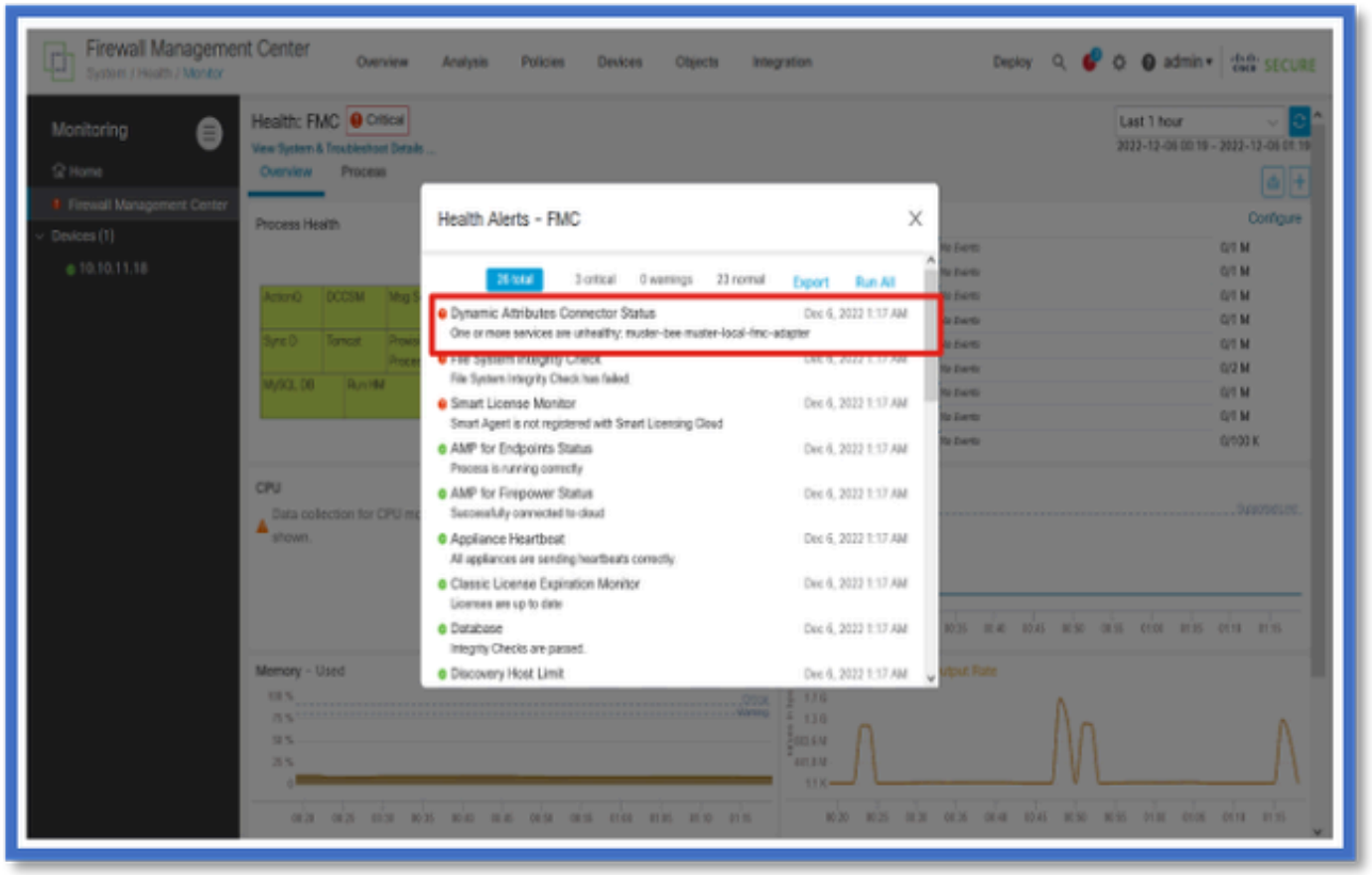


Remarque : nous avons toujours le nom « rassembleur » dans plusieurs notifications et il est nécessaire ici de fournir un nom de service pour obtenir des informations détaillées.



Ici, nous voyons que muster-bee et muster-local-fmc-adapter sont « malsains ».

Si une erreur indique l'un des services principaux, des journaux de dépannage doivent être collectés pour le débogage.



CSDAC en dépannage

Génération d'un dépannage CSDAC

- Les journaux CSDAC sont automatiquement collectés lors de la génération du dépannage FMC.L'offre groupée contient l'état du Docker, les journaux et les données nécessaires pour déboguer le problème hors connexion.
- Il est recommandé d'activer le mode de débogage CSDAC avant de reproduire l'erreur pour laquelle des journaux de dépannage sont collectés .

À partir de /usr/local/sf/csdac call ./muster-cli debug-on

Recherchez les journaux CSDAC dans untarred Troubleshoot dans ces dossiers :

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

Contient les données stockées dans la base de données etcd.

/results-XX/command-output/csdac_troubleshoot /log

Il contient les journaux des conteneurs docker.

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

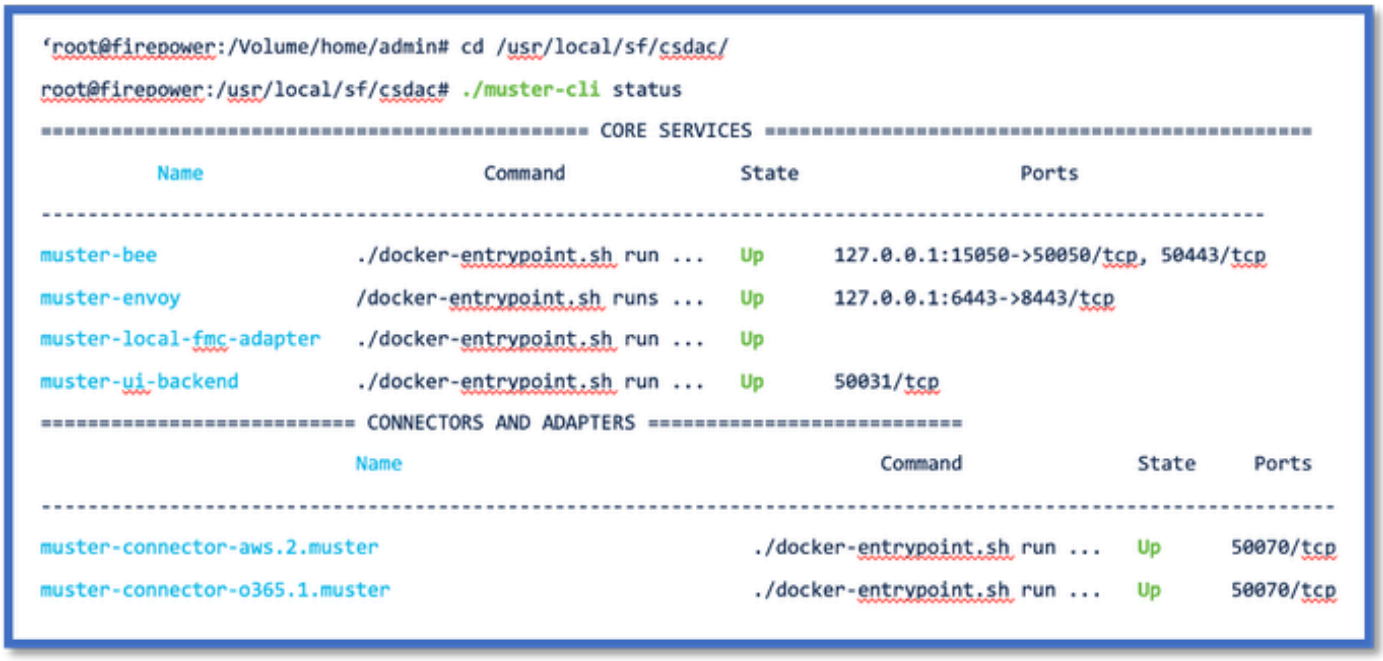
Affiche l'état du conteneur, les versions et les détails de l'image du docker.

Dépannage CLI

Le script muster-cli peut être utilisé pour vérifier l'état de CSDAC à partir de l'interface de ligne de commande FMC.

Si l'état d'un service est « Exited » ou différent de « Up », commencez par vérifier les journaux de ce conteneur.

Le nom du conteneur est nécessaire pour obtenir les journaux ; il peut être obtenu à partir du résultat.



Mode de débogage CSDAC

Le script « muster-cli » peut être utilisé pour activer et désactiver les journaux de débogage.Par défaut, les conteneurs sont consignés dans le fichier INFO level.INFO et DEBUG sont les seuls niveaux pris en charge.

Pour activer l'utilisateur de niveau DEBUG : ./muster-cli debug-on.

Cela fournirait plus d'informations pour la génération du dépannage et l'aide pour le débogage.Cette option doit être activée lors de la reproduction d'un problème.

Pour revenir au niveau INFO, utilisez : ./muster-cli debug-off.

<#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
```

Messages consignés avec le débogage

Lorsque le mode de débogage est activé, tous les journaux du conteneur docker contiennent également des messages de débogage

Obtenir des journaux en temps réel à l'aide des commandes docker : docker logs -f <nom_conteneur>

Dans l'exemple ci-dessous, le message de débogage indique ce qui a déclenché une erreur gRPC

<#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 cor
```

Exemple de problème avec la procédure pas à pas de dépannage

Présentation des problèmes et du dépannage

Problème :

Le problème le plus courant que nous rencontrons est que FMC ne reçoit pas tous les mappages d'objets dynamiques.

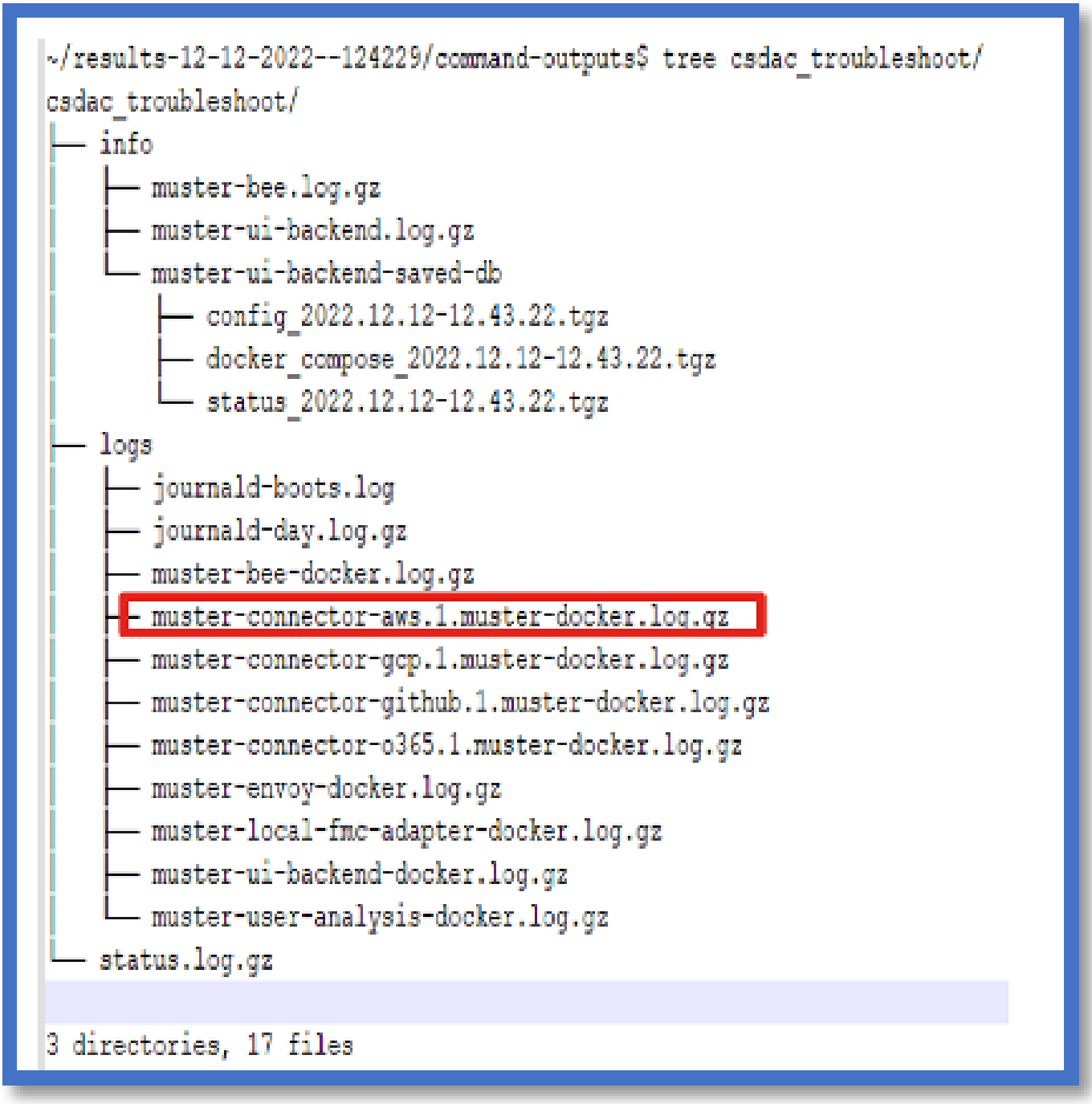
Dépannage :

Pour résoudre le problème, nous

- Activer le mode de débogage à partir de « muster-cli »
- Fichier de dépannage généré à partir de l'interface FMC
- Vérifiez que les journaux du connecteur AWS CSDAC se sont connectés et collecté le dépannage.
- Nous avons découvert que le connecteur CSDAC AWS n'a demandé que la première adresse IP dans les instances AWS.

Préparation du bundle de dépannage

- À partir de l’interface de ligne de commande FMC, nous avons activé le mode de débogage à l’aide de ./muster-cli debug-on. L’outil muster-cli est disponible dans /usr/local/sf/csdac.
- Recréez le problème en attendant que l'état du connecteur soit OK, puis en vérifiant les filtres d'attributs dynamiques.
- Collecte des journaux de dépannage à partir de l'interface utilisateur FMC et extraction de ceux-ci.Vérification du contenu des journaux du connecteur AWS pour le snapshot



Examinez les attributs de balise d'une adresse IP

Les attributs de balise pour une adresse IP donnée sont consignés dans les journaux de dépannage. Pour le connecteur AWS, nous avons examiné le fichier muster-connector-aws.1.muster-docker.log.gz

Récapitulatif des vérifications

L'état du connecteur et de l'adaptateur est-il correct ?

Vérifiez les états dans les pages Connecteur, Adaptateur correspondantes.

Les connecteurs ont-ils obtenu tous les mappages ?

Recherchez les adresses IP correspondantes dans l'aperçu de la règle.

Vérifiez les journaux du docker Connector pour voir s'il interroge correctement les mappages.

Le serveur REST a-t-il reçu des mappages de balises dynamiques du connecteur ?

Vérifiez la page des objets dynamiques FMC.

Consultez les journaux USMS (dans /opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log) pour voir si le serveur FMC REST a traité correctement la demande d'API de CSDAC.

Q&R

Q : Quelle version de CSDAC sur site prend en charge un connecteur ISE, je ne vois pas non plus un tel connecteur dans la version 7.4.0 (build 1494) ?

R : Il s'agit d'un CSDAC autonome et non d'un FMC ou d'un CDO. Vous devez disposer d'un package CSDAC ansible pour le tester.

Q : Une fois publiée, quelle serait la version sur site de CSDAC ?

R : Probablement 2.1.0.

Q : Un écran avec un engrenage qui a API déposé sur elle a été montré. Je pense que c'est la CSDAC ; qu'est-ce que cela signifie ?

R : L'explorateur d'API est intégré dans ce CSDAC, vous pouvez passer des appels d'API au CSDAC à partir de cette page.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.