Secure Dynamic Attribute Connector implementeren in FMC

Inhoud

Inleiding

Dit document beschrijft over Cisco Secure Dynamic Attribute Connector in FMC.

Achtergrond - Probleem

CSDAC (Cisco Secure Dynamic Attributes Connector) kan in FMC (Firepower Management Center) worden geïntegreerd en biedt dezelfde functionaliteit als de standalone CSDAC-toepassing en CSDAC in CDO. Voor standalone CSDAC, bevrijdt het klanten van de overheadkosten van het beheer en het onderhoud van een afzonderlijke machine voor CSDAC. Als Netwerkbeheerder wil ik dat de programmatische interfaces eenvoudig te integreren zijn en up-to-date blijven met wijzigingen in externe dynamische omgevingsproviders. Deze integratie lost het probleem op van het verzamelen van eigenschappen van dynamisch veranderende cloudomgevingen zonder het implementeren van een beleid.

Oplossing (samenvatting)

CSDAC kan nu in FMC worden geconfigureerd om tagkenmerken te halen van Azure, vCenter, AWS, GCP, Office 365 en Azure Service Tags, waardoor functiepariteit wordt geboden met de standalone CSDAC en CSDAC in CDO.

- U kunt nu kiezen
  - CSDAC in VCC (of)
  - CSDAC in CDO (of)
  - Standalone CSDAC
- Doelmarkt: Ondernemingen, Serviceprovider

Dynamic Attributes Connector in VCC Samenvatting

FMC Dynamic Attributes Connector:

- Dashboard scherm om de Dynamic Attribute Connector te bouwen en te bedienen.
- FMC UI voor configureren van connectors voor bronwerkbelasting (AWS, Azure, vCenter, Office 365, GCP)
- FMC UI om dynamische attribuut filters te definiëren om Dynamische objecten te maken

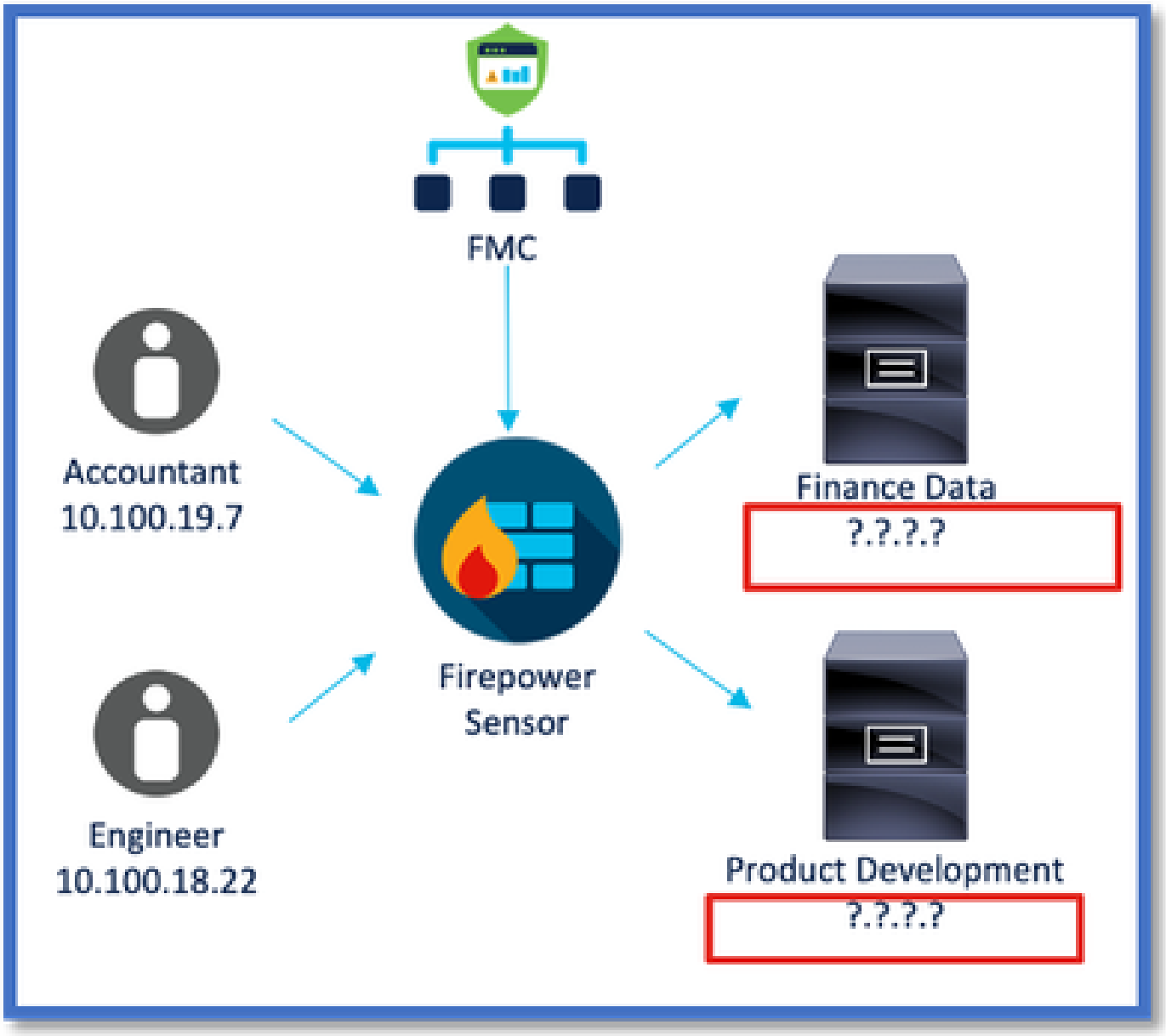
Implementatievoorbeelden

CSDAC op voorhand

Vorig jaar heb ik een speciale VM voor CSDAC ingezet om attributen van mijn AWS- en Azure-accounts te verzamelen.

Het probleem

Nu is mijn organisatie naar Cloud verhuisd, en kan ik geen speciale Virtual Machine voor CSDAC implementeren en beheren in mijn omgeving.



Optie 1: Gebruik de Dynamic Attributes Connector die in FMC is gebouwd

U kunt het probleem oplossen met Dynamic Attributes Connector die in FMC is gebouwd. De dynamische objecten die hiermee gemaakt zijn, kunnen gebruikt worden in het toegangsbeleid.

Optie 2: Gebruik in de cloud geleverde Dynamic Attributes Connector in CDO

U kunt het probleem oplossen met Dynamic Attributes Connector in CDO. De dynamische

objecten die hiermee gemaakt zijn, kunnen gebruikt worden in

- CDO cloudgeleverd FMC
- CDO on-prem FMC

Voorwaarden, ondersteunde platforms, licentiëring

Minimale ondersteunde software- en hardwareplatforms

Min. ondersteunde Manager versie	Beheerde apparaten	Min. ondersteunde versie van beheerde apparaat vereist	Opmerkingen
VCC 7.4	Alle door FTD ondersteunde producten	Any 7.0+ FTD	

* Dynamic Attributes Connector wordt niet ondersteund op FDM-beheerde apparaten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:
· Cisco Firewall Management Center met 7.4
· Cisco Firepower Threat Defense met 7.4 of hoger.
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Functiedetails

Standalone CSDAC Overzicht (momenteel uitgebracht - 7.4)

Met de Cisco Secure Dynamic Attributes Connector kunt u tags van verschillende cloud-serviceplatforms gebruiken in de toegangscontroleregels van Firewall Management Center (FMC).

On-Prem CSDAC is op een Linux Machine te installeren, ondersteunt het verkrijgen van eigenschappen van:

- AWS, Azure, VMware vCenter en NSX-T, Office 365, Azure-servicetags, GCP, GitHub.

CSDAC in CDO Overzicht (Huidige release - 7.4)

Ondersteunt dezelfde functionaliteit als On-Prem CSDAC zonder dat u een speciale toepassing

hoeft te installeren en onderhouden.

vCenter-connector wordt momenteel niet ondersteund in CDO.

Ondersteunt het verzenden van de ontvangen attributen naar het in de cloud geleverde FMC en On-Prem FMC in CDO.

CSDAC in VCC

Ondersteunt dezelfde functionaliteit als Standalone CSDAC zonder dat een speciale applicatie geïnstalleerd en onderhouden hoeft te worden.

CSDAC in FMC ondersteunt het verkrijgen van eigenschappen van:

- AWS, Azure, VMware vCenter en NSX-T, Office 365, Azure-servicetags, GCP, GitHub

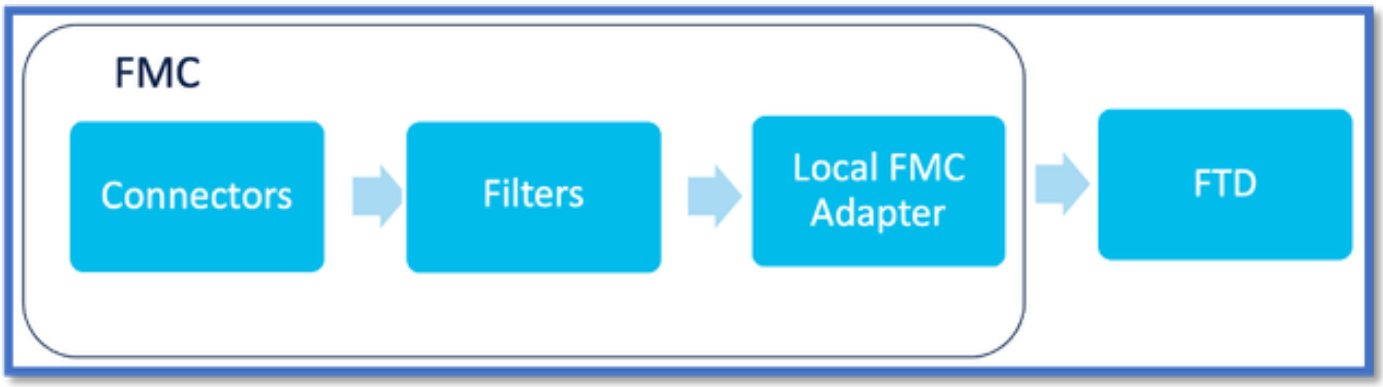
Er is hier geen expliciete adapterconfiguratie aangezien het lokaal is aan FMC.

Hoe het werkt

Connectors worden gebruikt om kenmerken te verkrijgen van AWS, Azure, o365, vCenter.

Lokale adapter wordt vervolgens gebruikt om deze gestroomlijnde eigenschappen en de IP-toewijzingen in FMC op te slaan als dynamische objecten.

FMC stuurt de mapping realtime naar FTD (zonder inzet).



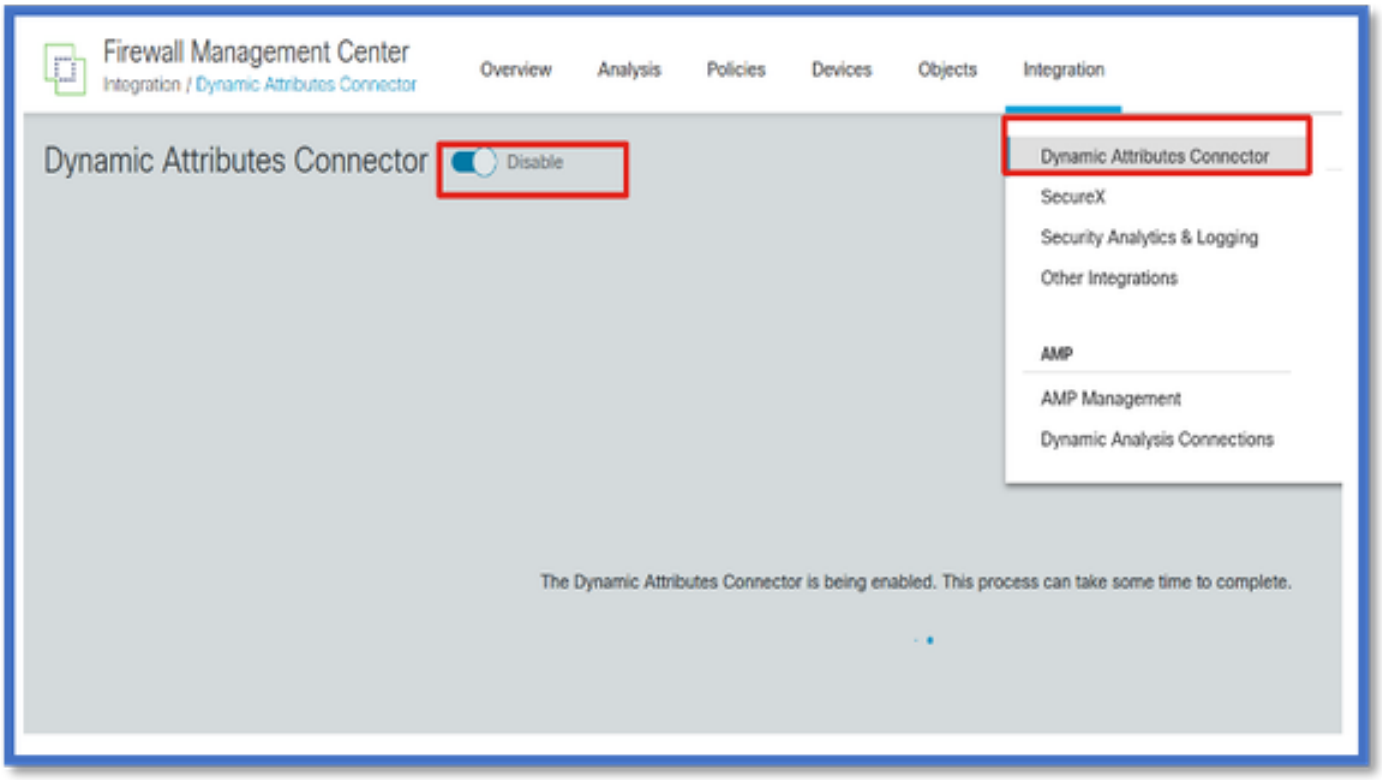
CSDAC in VCC inschakelen

Navigeer naar Integratie > Dynamic Attributes Connector.

Gebruik de knop Schakelen om de -aansluiting in te schakelen.

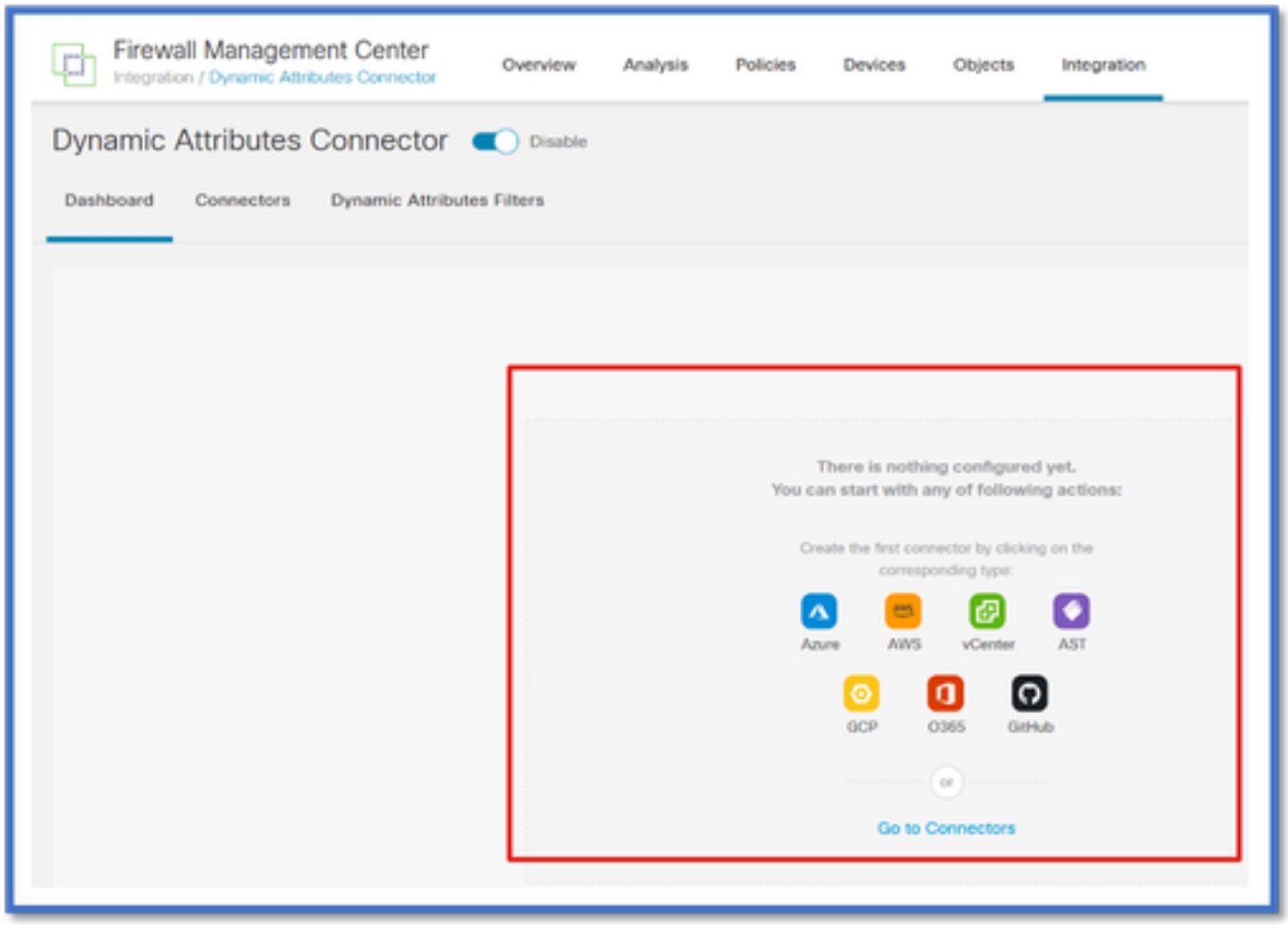
FMC duurt een paar minuten om de havenbeelden en containers te downloaden en te brengen.

Dit kan alleen worden geconfigureerd in FMC global domain.



CSDAC-Dashboard

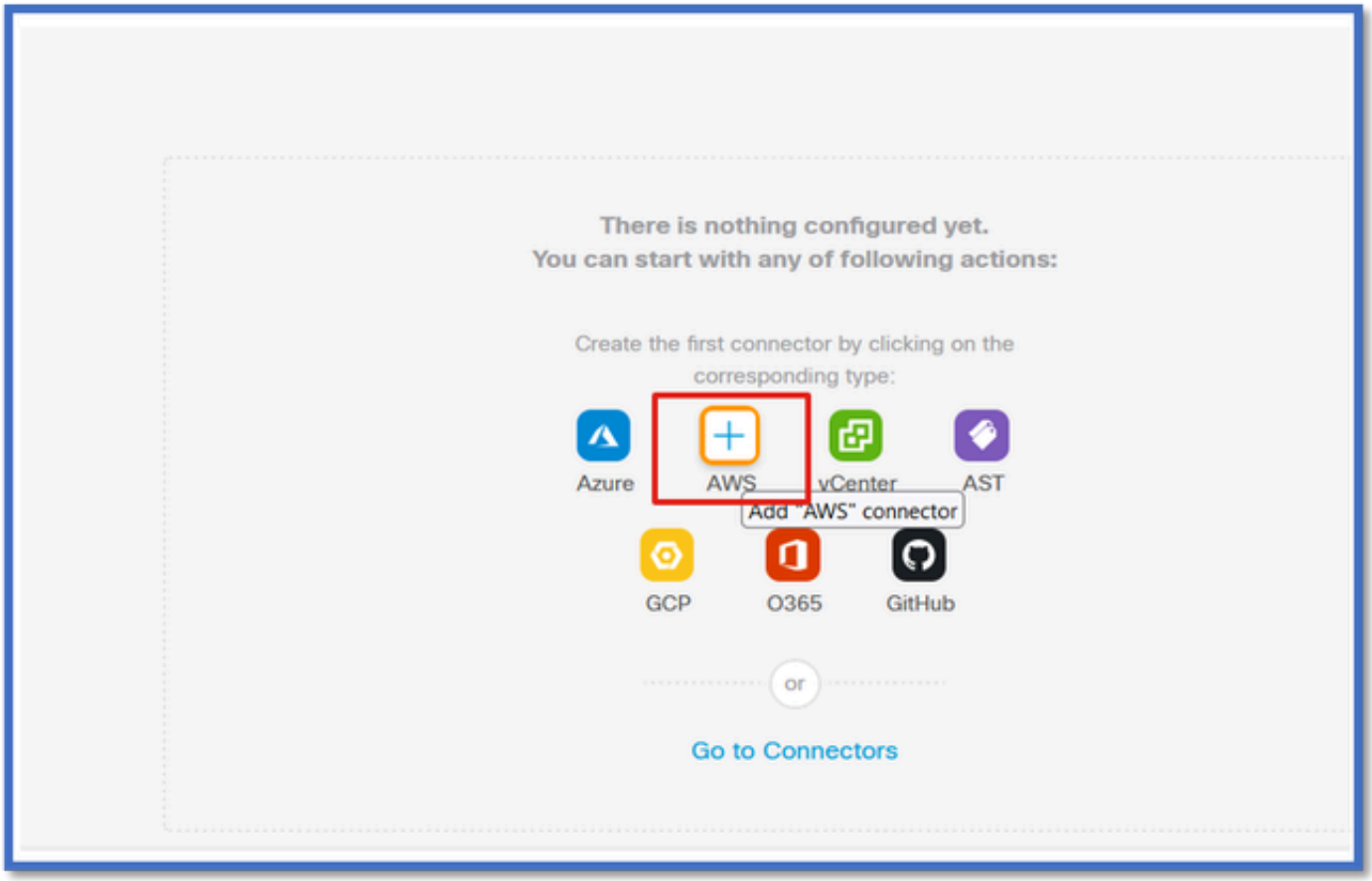
Na het inschakelen van CSDAC wordt de gebruiker getoond met de CSDAC Dashboard-pagina. Dashboard wordt gebruikt om zowel geconsolideerde connectors als filter te configureren en weer te geven.



Connectors configureren

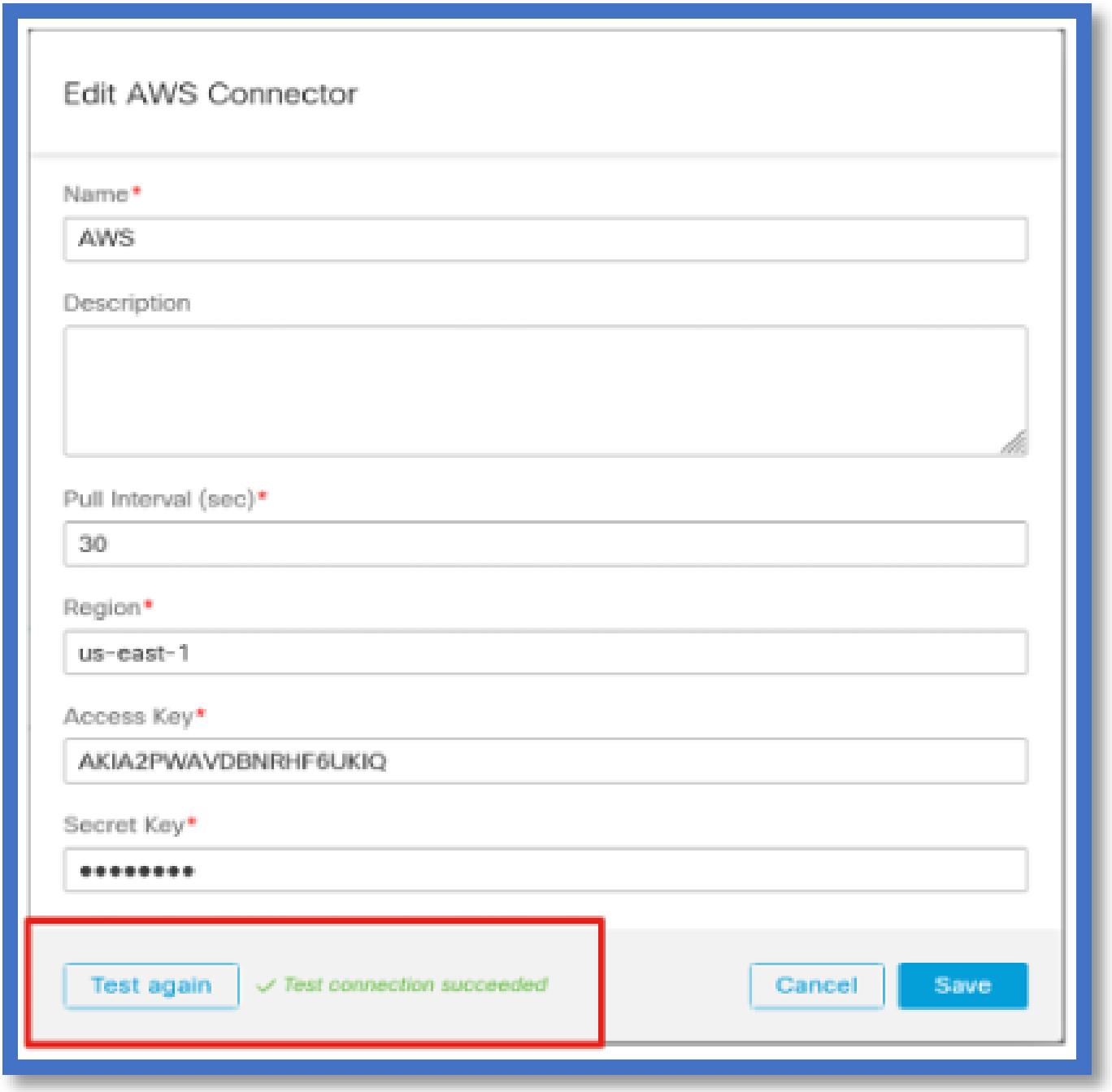
Connectors toevoegen vanaf Dashboard

Klik op het Dashboard pictogram voor de gewenste connector om het toe te voegen.



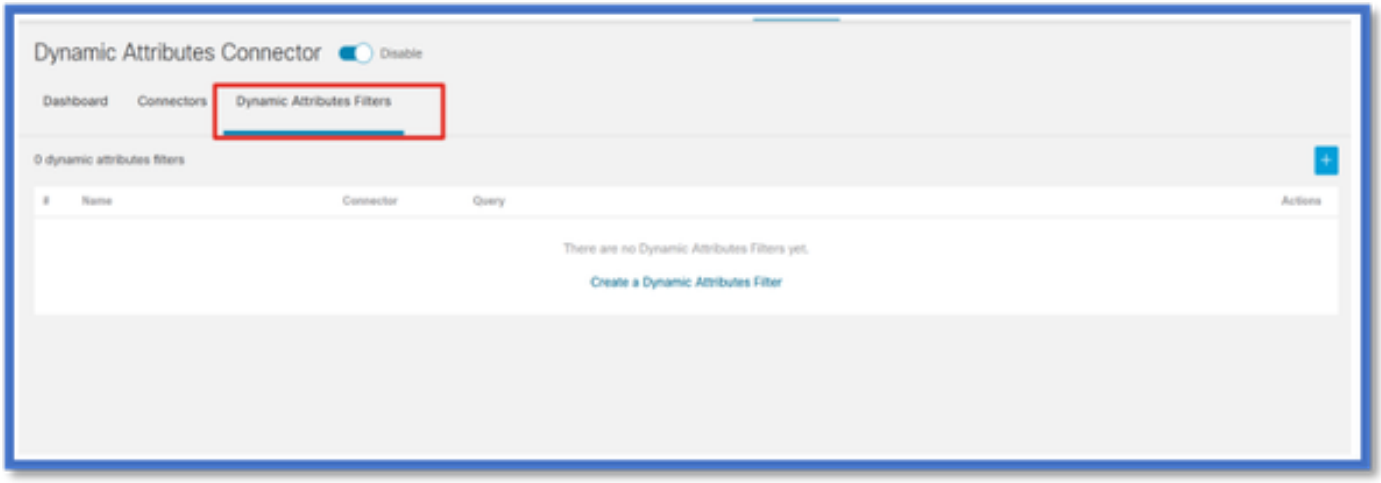
Configureer een tijdsinterval (in het veld Trek interval) zodat de connectors informatie van providers met de ingestelde frequentie kunnen ophalen.

Voer de referenties van de provider in om de tagkenmerken te verkrijgen. Zodra u de connector hebt geconfigureerd, kunt u de connector testen door op de Test-knop te klikken.



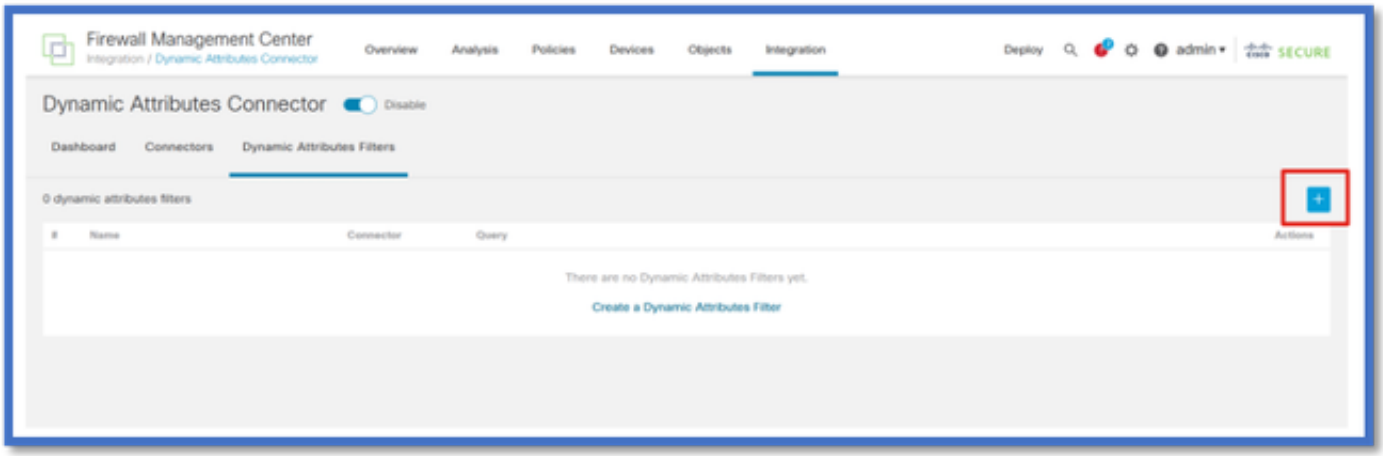
Filters configureren

Klik op het tabblad "Filters dynamische kenmerken" in het menu "Connector dynamische kenmerken" om naar de pagina Filters dynamische kenmerken te gaan.



Filters toevoegen

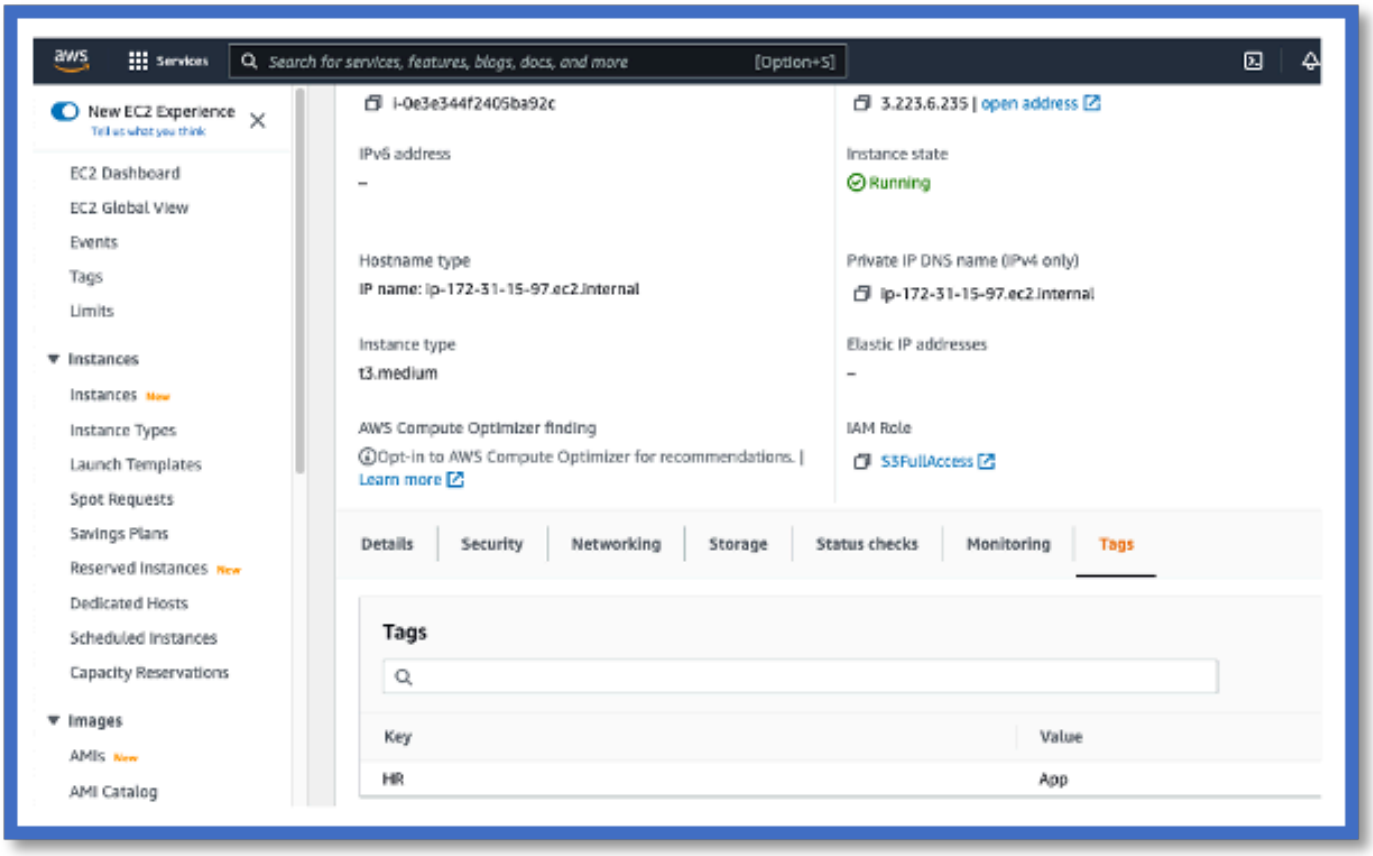
Klik op de knop + om een filter voor attribuut connectors te maken.



AWS-tags toevoegen

We kunnen er bijvoorbeeld van uitgaan dat u geïnteresseerd bent in de belangrijkste ‘HR’ en waarde ‘App’ in AWS werkbelasting.

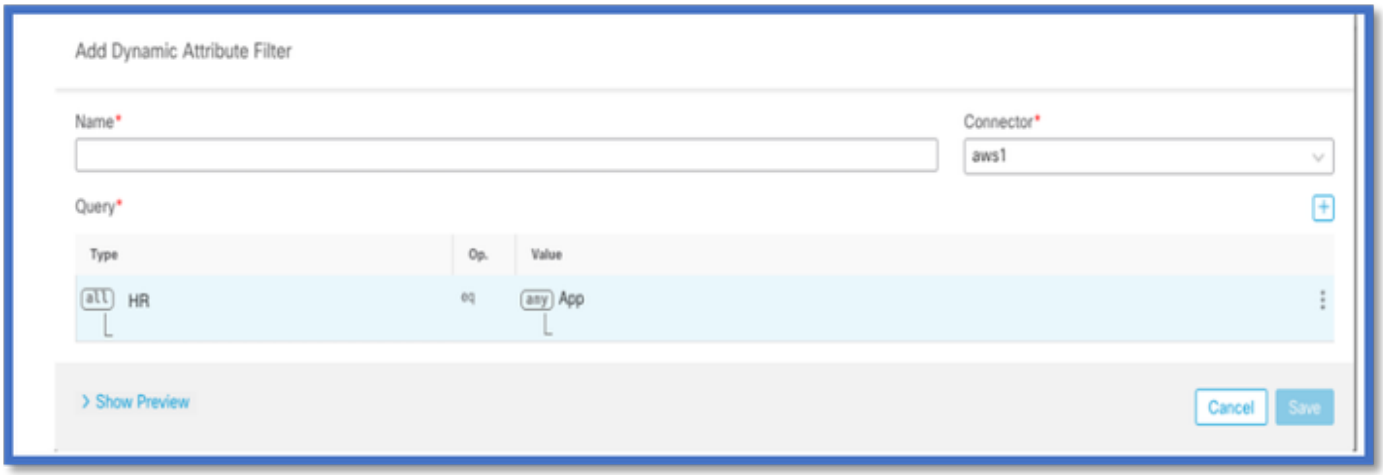
Zo zou het eruit zien bij AWS.



CSDAC in VCC

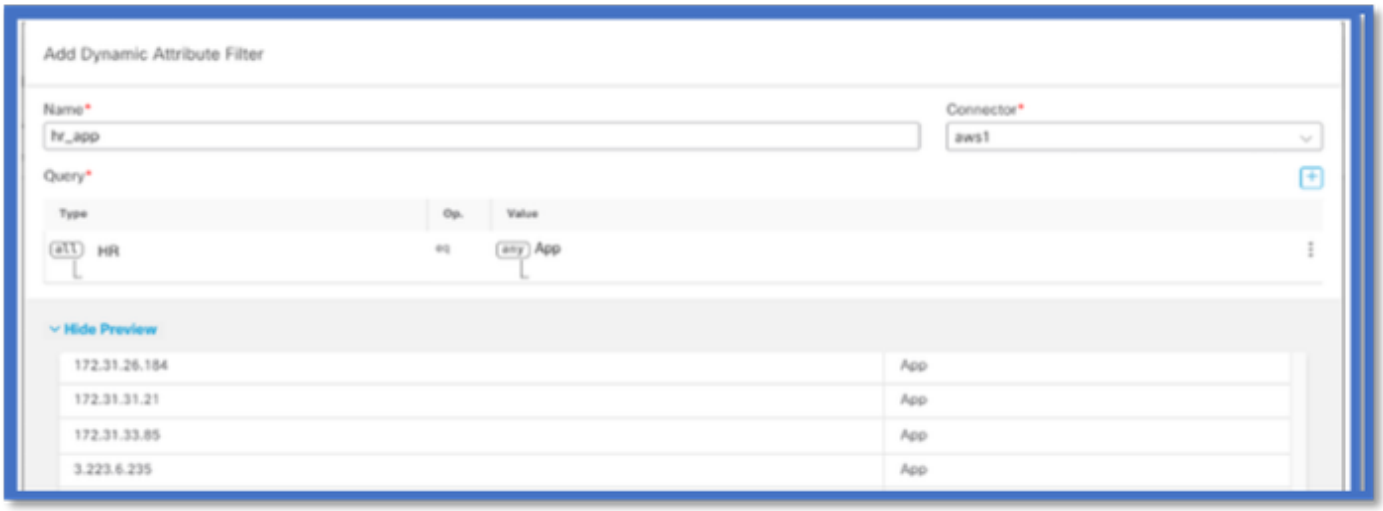
Je kunt een ‘HR = App’ regel creëren door op de + knop te klikken.

De lokale FMC-adapter stuurt de overeenkomende IP-adressen als dynamische objecttoewijzingen naar FMC



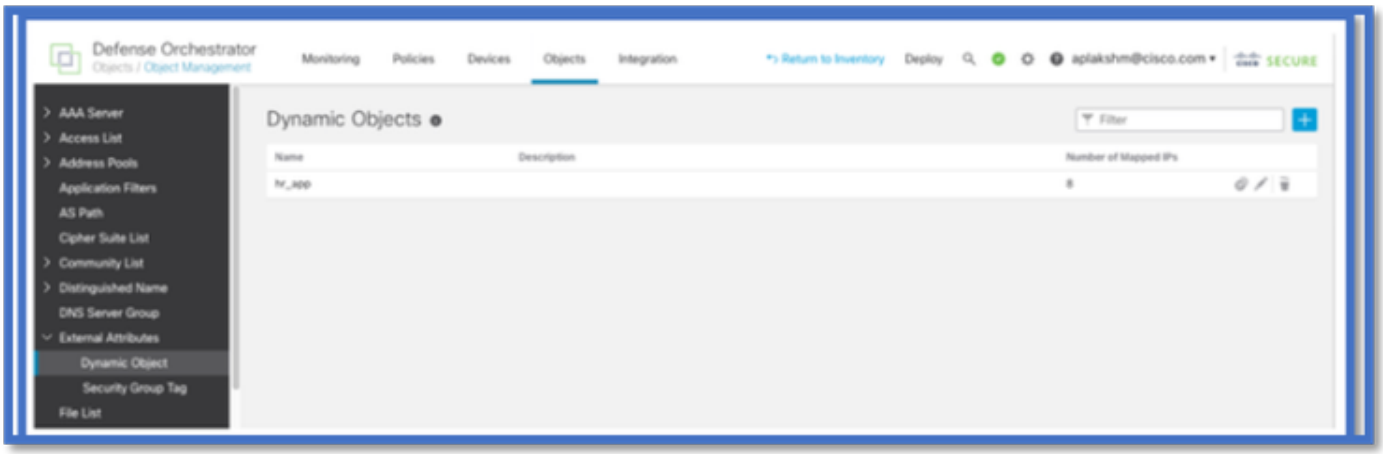
Voorbeeld

U kunt ook de overeenkomende IP-adressen van een bepaald attributenregel bekijken door op ‘Weergeven’ te klikken | Knop Voorbeeld verbergen.



Dynamische objecten

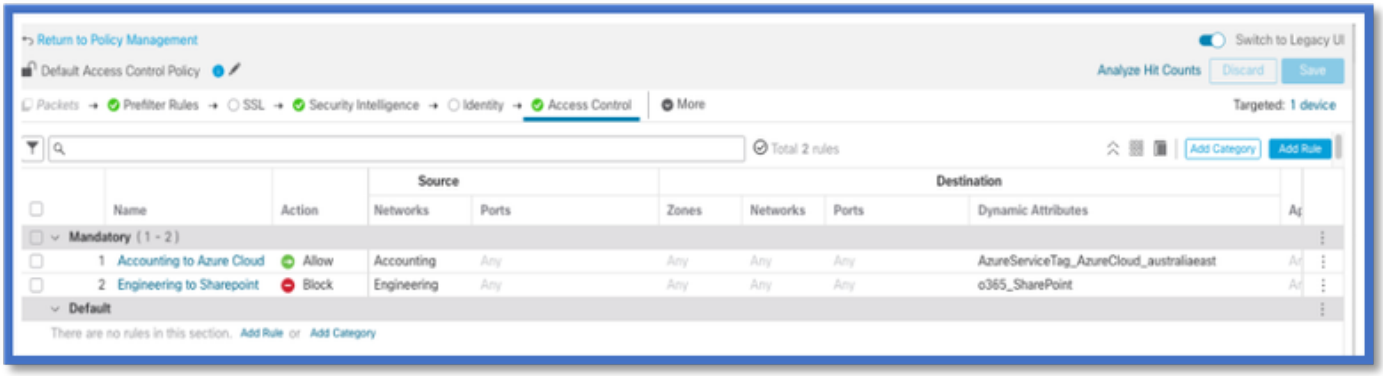
Bekijk de Dynamische objecten die door CSDAC zijn gemaakt in Objecten > Externe kenmerken, Dynamisch object in FMC



AC-beleid

Configuratie: toegangsbeleid

In FMC kunt u toegangsbeleid toevoegen om de ontvangen dynamische objecten toe te staan of te blokkeren via Dynamic Attribute Connector.



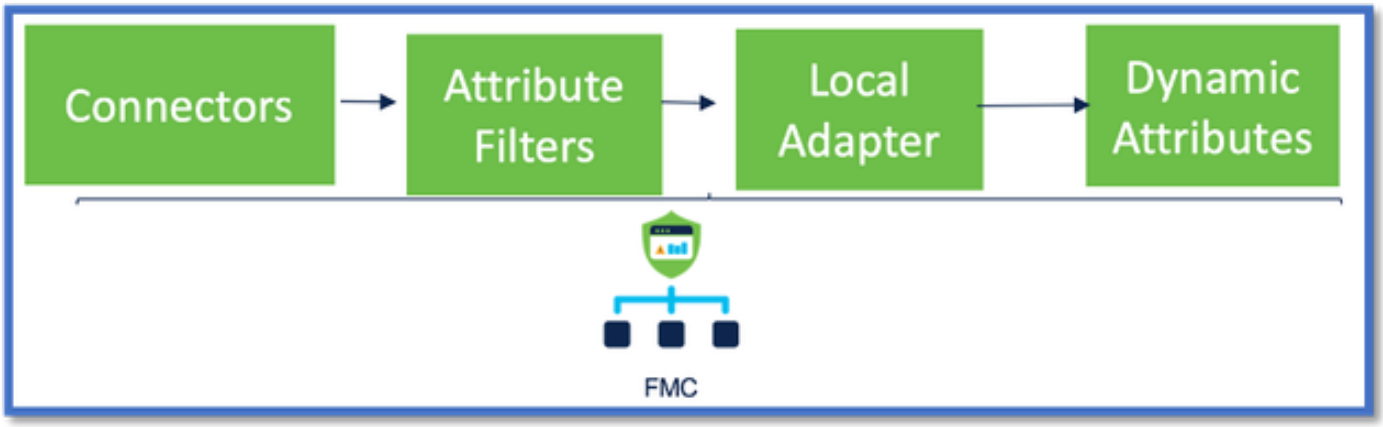
Platformlimieten

- De limieten van de connector zijn gebaseerd op beschikbaar FMC-geheugen.
- vFMC zou een extra geheugen van 1 GB nodig hebben om 5 connectors te ondersteunen
- Azure AD realm is ook in de limiet opgenomen, aangezien het ook een CSDAC-container is.

Models	Aantal ondersteunde connectors	Platforms	Limiet op basis van geheugen
Basis	Alleen Azure AD	1600	32 GB
Klein	5	vFMC	> 32 GB
Gemiddeld	10	VCC 300, 2600	>= 64 GB
Groot	20	4600	>= 128 GB

Problemen oplossen/diagnostiek

Problemen oplossen kan het best worden uitgevoerd door dynamische objecten van CSDAC Connectors naar Dynamics Attributes in FMC te overtrekken. Veel interne logboeken verwijzen naar deze functie als ‘muster’. U kunt in systeemstaat langs de uitzendingsketen gluren om problemen te isoleren. CSDAC gebruikt Docker containers. Berichten en namen van logbestanden en andere bestanden moeten worden aangeduid als "docker"



Controleer de connectors

Zorg er eerst voor dat connectors verbinding kunnen maken met vCenter-, AWS- of Azure-servers.

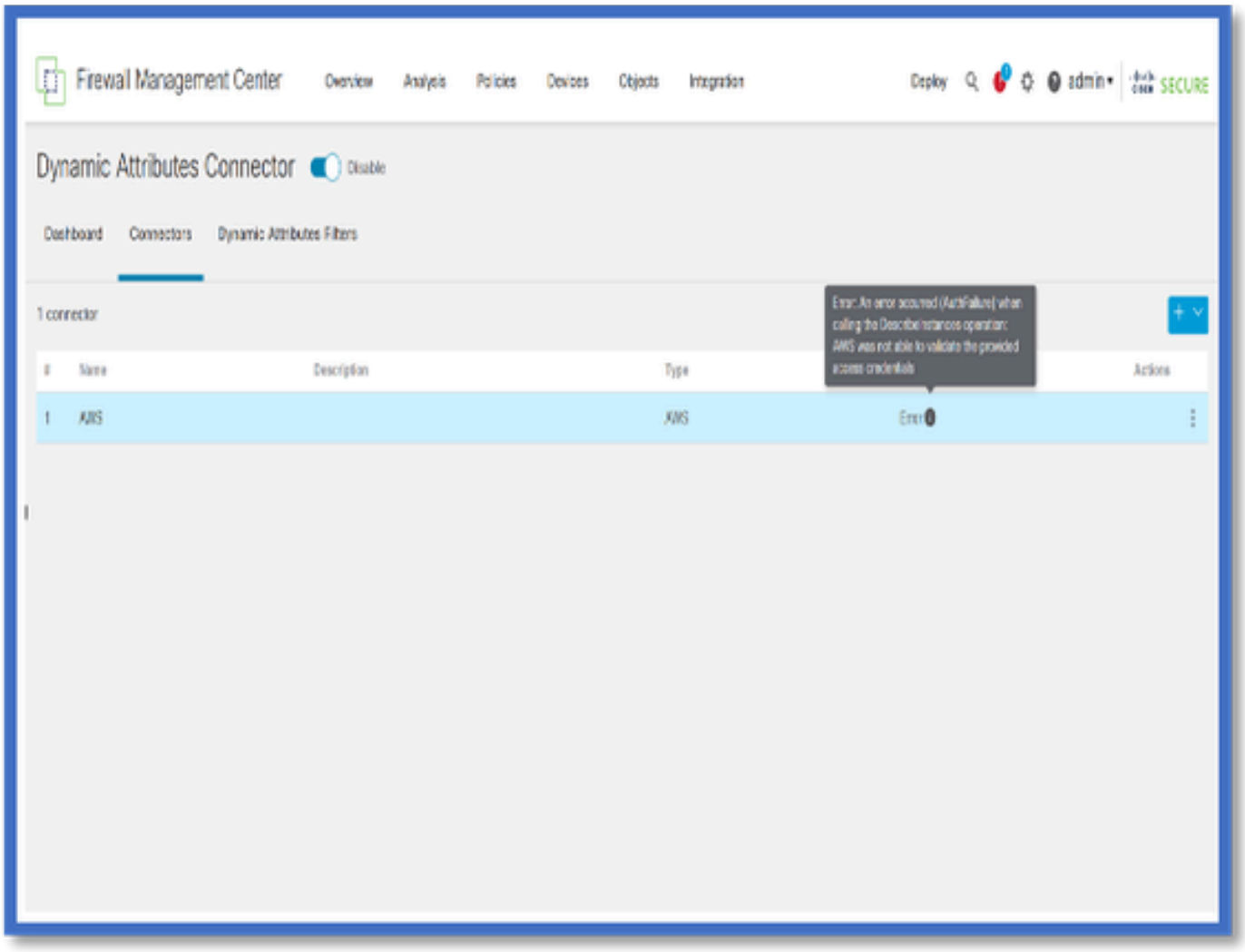
Als Connectors niet goed zijn geconfigureerd, kunnen downstream-processen geen taginformatie

verkrijgen.

Connectors bekijken via het tabblad Connectors

De status van de connector wordt weergegeven in het statusveld en elke 15 seconden bijgewerkt.

Hier zien we dat de connector niet kan authenticeren met de meegeleverde referenties.



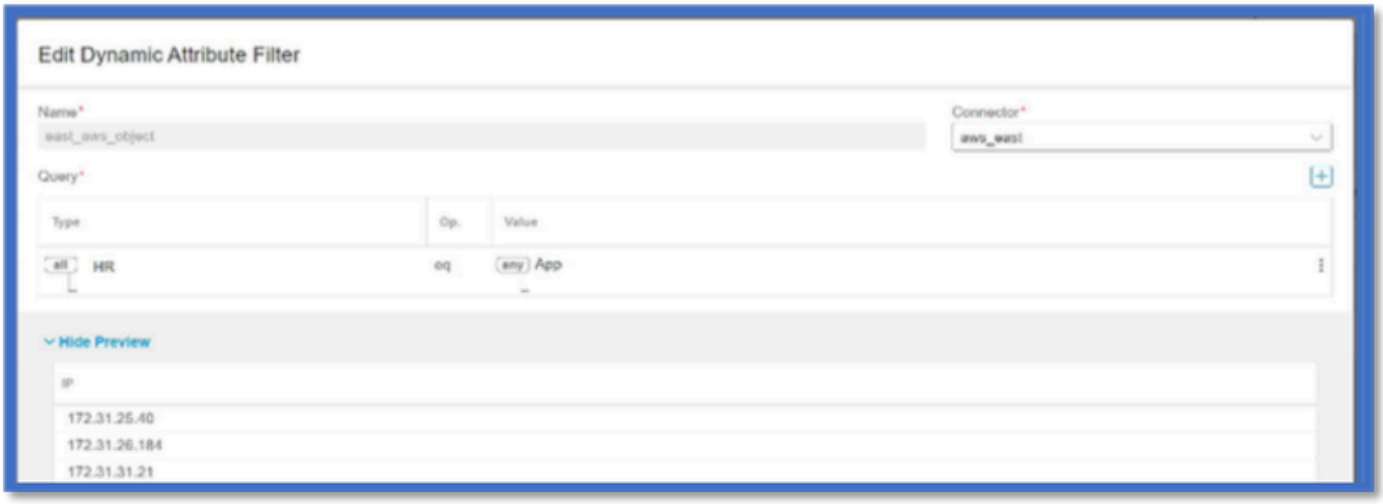
De kenmerkfilters controleren

Zorg ervoor dat de voorvertoning in Regel de overeenkomende IP-adressen voor uw queryvoorwaarde toont.

Als er geen overeenkomende IP-adressen zijn, kan FMC de dynamische objecttoewijzingen niet krijgen.

De kenmerkfilters controleren

Controleer of Dynamic Attribute IP-toewijzingen in de voorbeeldweergave beschikbaar zijn. Toon voorbeeldknop is beschikbaar op Dynamic Attribute Filter bewerken pop-up.



Controleer de dynamische objecten in de FMC UI

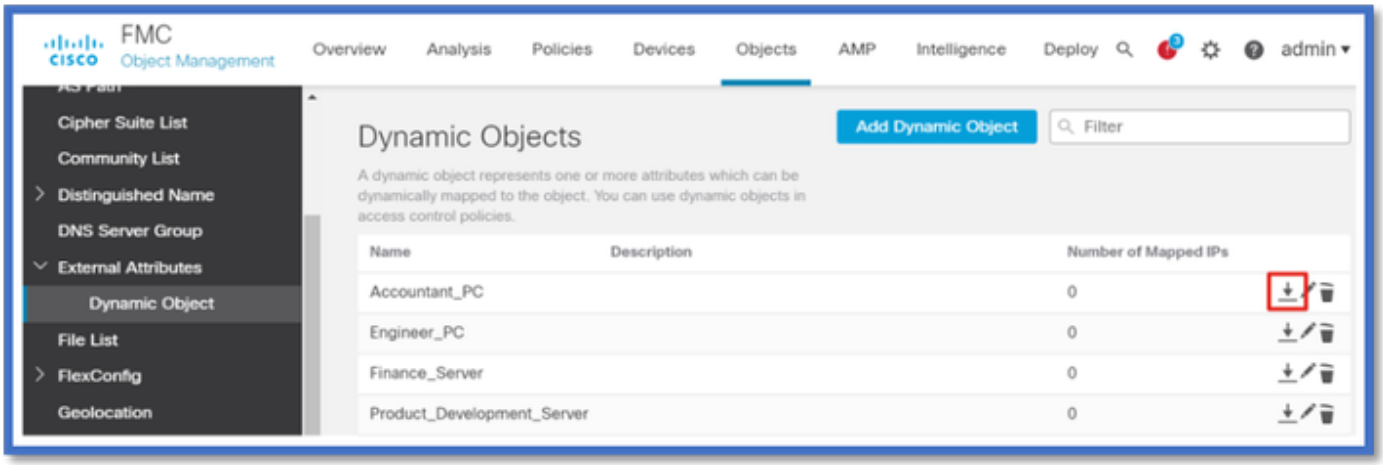
Controleer eerst of de FMC-server de banden bevat die u verwacht.

- Kijk onder Objectbeheer, tabblad Externe objecten, controleer Dynamische objecten op bindingen.
- Als FMC de bindingen niet krijgt, kan FTD ze niet krijgen.

Controleer FMC Health Monitor en meldingen voor CSDAC Health Alerts.

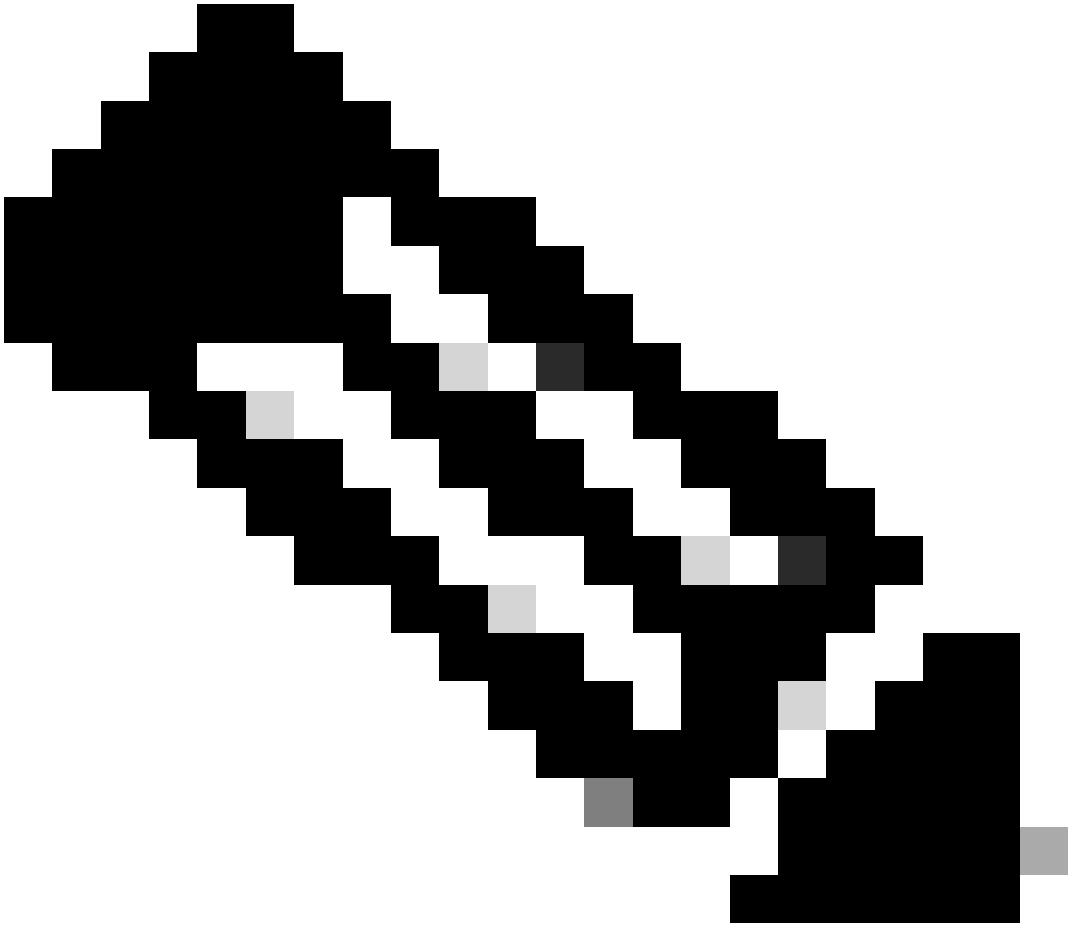
Dynamische objecten controleren

Met FMC Object Manager kunt u de huidige IP-adressen van Dynamic Object downloaden.

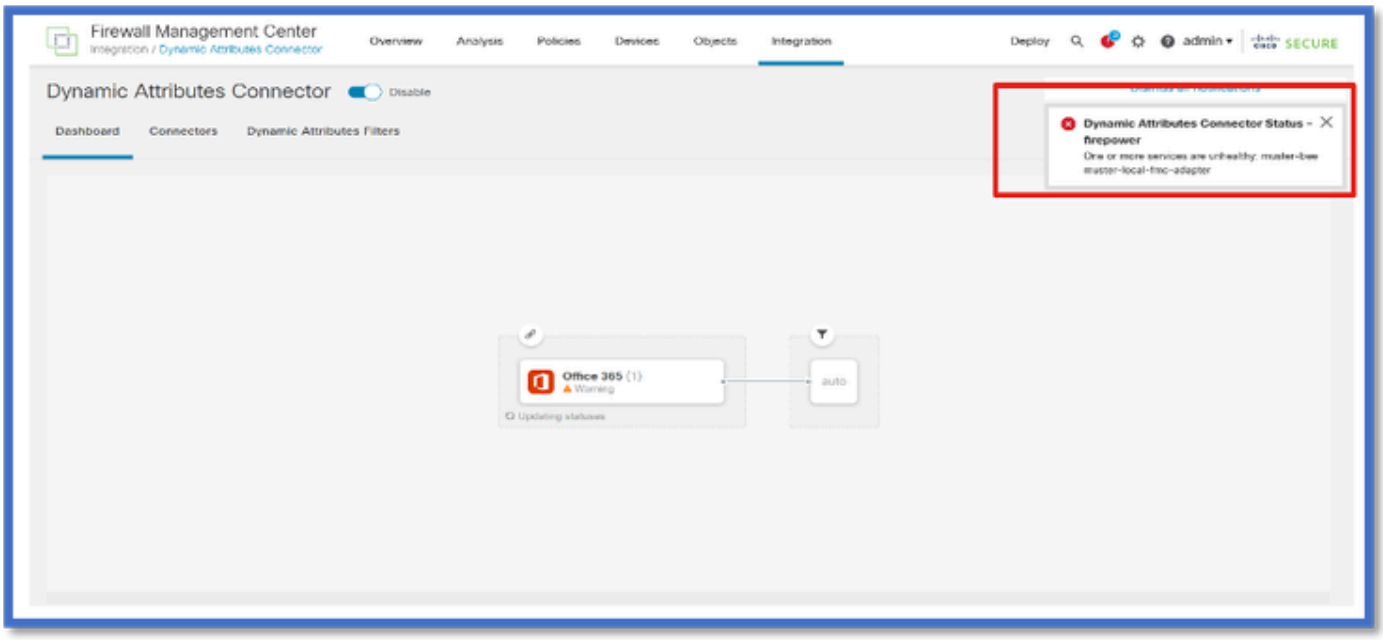


Waarschuwingen voor CSDAC-status

FMC's Task Manager geeft Health Alerts weer als een kerndienst, waaronder de Dynamic Attributes Connector, niet werkt. De waarschuwing bevat informatie over de servicenaam en de status van de service.

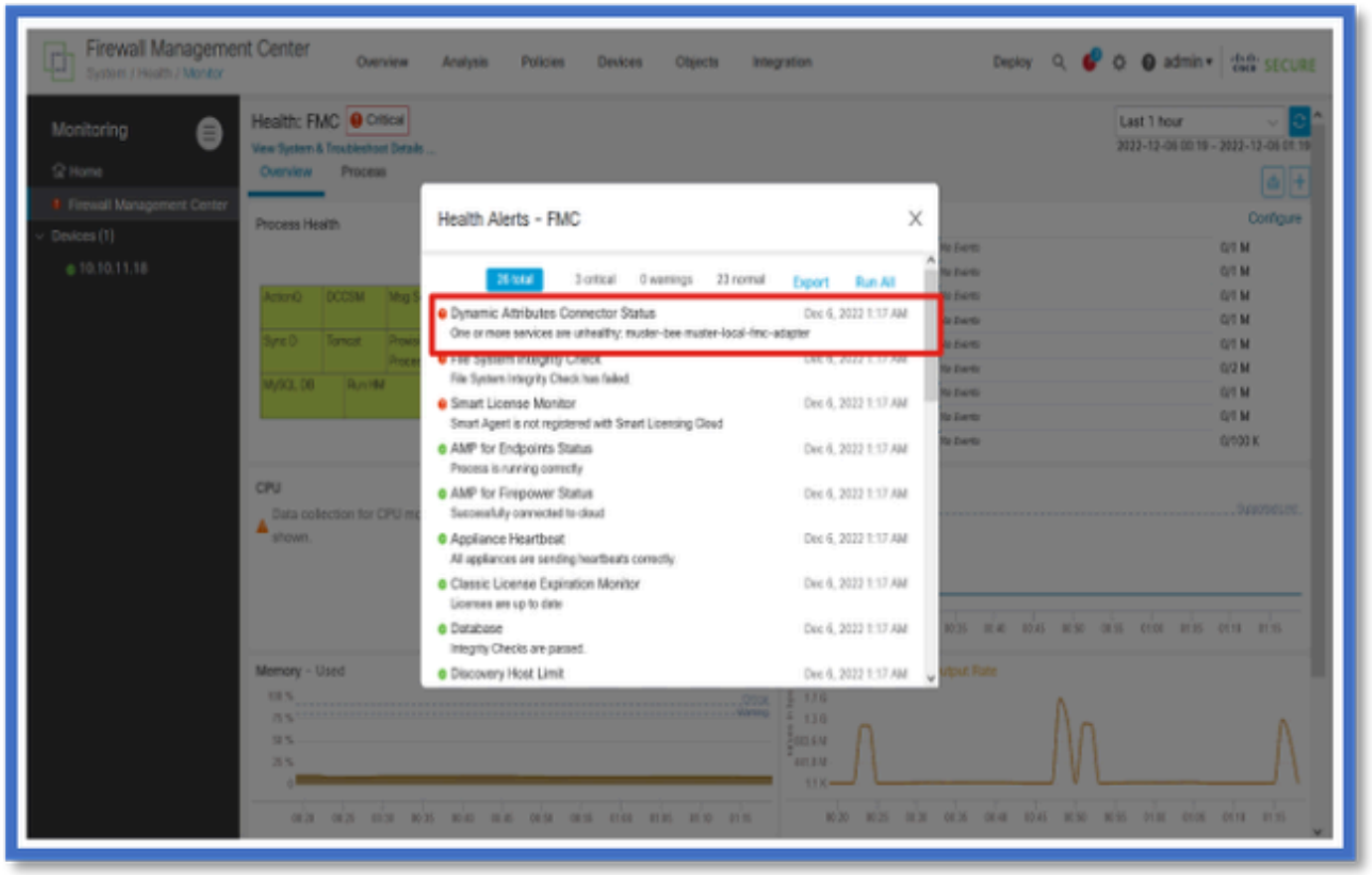


Opmerking: de naam "muster" staat nog steeds in verschillende meldingen en het is hier vereist om service name te geven voor gedetailleerde informatie.



Hier zien we dat bijen en musters-lokaal-fmc-adapters "ongezond" zijn.

Als de fout op een van de kernservices wijst, dan moeten probleemoplossingslogboeken worden verzameld voor debug.



CSDAC bij probleemoplossing

Een CSDAC-probleemoplossing genereren

- CSDAC-logbestanden worden automatisch verzameld tijdens FMC Troubleshoot generation.De bundel bevat Docker-status, logbestanden en gegevens die nodig zijn om het probleem offline te verhelpen.
- De goede praktijk is aan het toelaten van CSDAC debug wijze alvorens fout te reproduceren waarvoor de logboeken van de probleemoplossing worden verzameld.

Van /usr/local/sf/csdac call ./muster-cli debug-on

Zoek de CSDAC-logbestanden in ongetraceerde probleemoplossing in deze mappen:

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

Dit bevat de gegevens die zijn opgeslagen in de ETCD-database.

/results-XX/commando-outputs/csdac_troubleshoot/log

Dit bevat de logboeken van de docker containers.

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

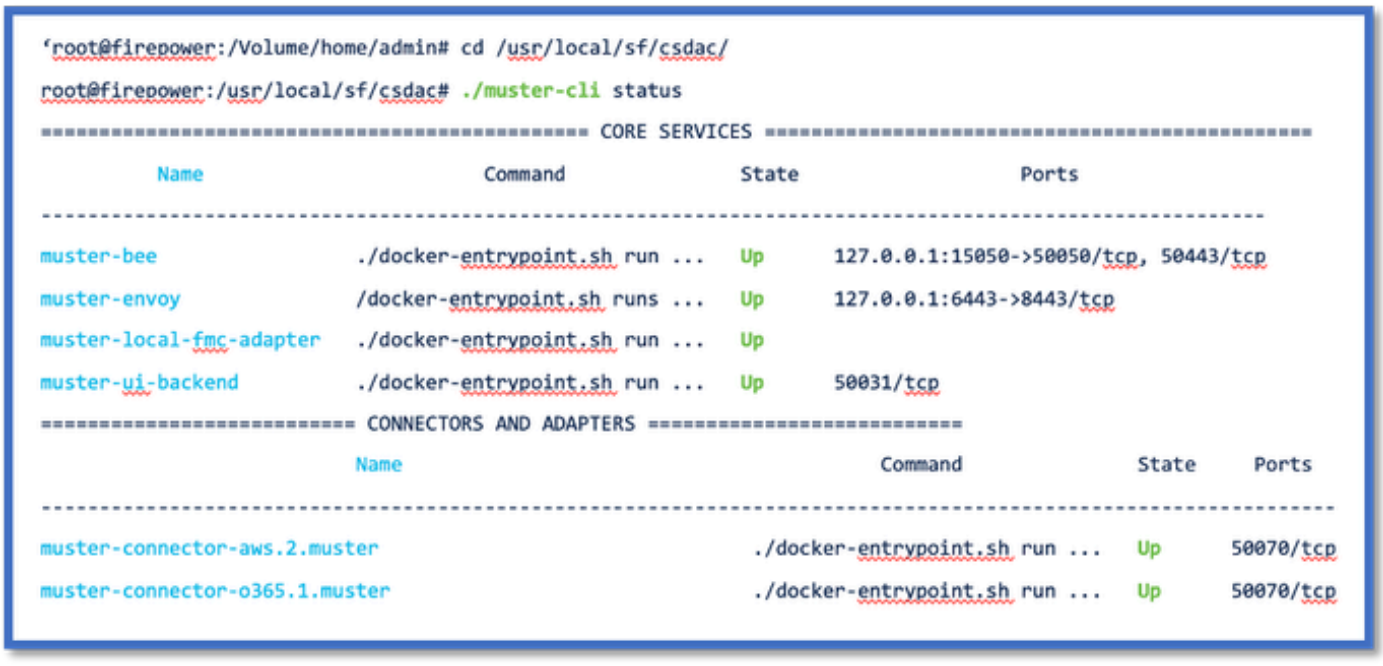
Dit toont de containerstatus, versies en de details van het havenbeeld.

CLI-probleemoplossing

Muster-cli script kan worden gebruikt om de status van CSDAC vanaf FMC CLI te controleren.

Als de status voor een service is "Afgesloten" of anders van "Omhoog", start dan door logboeken te controleren op die container.

De containernaam is nodig voor het verkrijgen van logboeken; het kan uit de output worden verkregen.



CSDAC-debugmodus

Het 'muster-cli' script kan worden gebruikt om de debug logs in en uit te schakelen.Standaard worden de containers gelogd op INFO level.INFO en DEBUG zijn de enige ondersteunde niveaus.

Om DEBUG level user: ./muster-cli debug-on in te schakelen.

Dit zou meer informatie voor probleemoplossing generatie en hulp met debug.Deze optie moet worden toegelaten terwijl het reproduceren van een probleem.

Om terug te keren naar het Info niveau gebruik: ./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
```

Vastgelegde berichten met Debug

Wanneer debug-modus is ingeschakeld zouden alle docker container logs ook debug berichten bevatten

Verkrijg logbestanden in real-time met docker commando's: docker logs -f <container_name>

In het onderstaande voorbeeld toont het debug-bericht wat een gRPC-fout heeft veroorzaakt

<#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
```

Probleem met probleemoplossing bij doorlopen van voorbeelden

Overzicht van problemen en probleemoplossing

Probleem:

Het meest voorkomende probleem dat we tegenkomen is dat het VCC niet alle dynamische objecttoewijzingen ontvangt.

Probleemoplossing:

Voor het oplossen van het probleem hebben we

- Debugmodus inschakelen vanaf "mustral-client"
- Geproduceerd probleemoplossingsbestand vanuit FMC UI
- Gecontroleerd of de CSDAC AWS Connector is aangemeld met de gegevens voor probleemoplossing.
- Kwam erachter dat CSDAC AWS Connector alleen voor eerste IP bevraagde in de AWS-instanties.

Voorbereiden van probleemoplossing

- Vanuit FMC CLI hebben we debug-modus ingeschakeld met ./muster-cli debug-on. muster-cli tool is beschikbaar in /usr/local/sf/csdac.
- Keerde het probleem door op de connector te wachten om status OK te hebben en vervolgens de filters Dynamic Attribute te controleren.
- Verzameld de probleemoplossingslogboeken van FMC UI en geëxtraheerd ze.Gecontroleerd de AWS Connector logboeken voor de inhoud van snapshot

Bekijk de tagkenmerken voor een IP

De tagkenmerken voor een bepaalde IP worden vastgelegd in de logboeken voor probleemoplossing. Voor AWS Connector hebben we gekeken naar muster-connector-aws.1.muster-docker.log.gz

Overzicht van controles

Ziet de connector- en adapterstatus er goed uit?

Controleer de status in de betreffende Connector, Adapterpagina's.

Hebben de Connectors alle toewijzingen gekregen?

Controleer de voorbeeldregel voor overeenkomende IP-adressen.

Controleer de logbestanden van de Connector om te zien of deze de toewijzingen correct bevragen.

Heeft de REST-server dynamische tag-toewijzingen ontvangen van de connector?

Controleer de pagina dynamische objecten van FMC.

Controleer de USMS-logbestanden (in /opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log) om te zien of de FMC REST-server de API-aanvraag van CSDAC correct heeft verwerkt.

Vraag en antwoord

V: Welke versie van CSDAC op locatie ondersteunt een ISE-connector, ik zie ook geen dergelijke connector in Versie 7.4.0 (build 1494)?

A: Dit is in Standalone CSDAC en niet in FMC of in CDO. u zou een CSDAC ansible pakket nodig hebben om dit te testen.

Q: Wanneer vrijgegeven, welke op-gebouw versie CSDAC het zou zijn?

A: Waarschijnlijk 2.1.0.

Q: Een scherm met een tandwiel dat API gelegd over het is getoond. Ik denk dat het CSDAC is; wat betekent dat?

A: API explorer is ingebouwd in deze CSDAC, kunt u API-oproepen naar CSDAC maken van die pagina.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.