

Bereitstellung eines sicheren dynamischen Attributkonnektors in FMC

Inhalt

[Einleitung](#)

[Hintergrund - Problem](#)

[Lösung \(Zusammenfassung\)](#)

[Dynamic Attributes Connector in FMC - Zusammenfassung](#)

[Bereitstellungsbeispiele](#)

[CSDAC vor Ort](#)

[Das Problem](#)

[Option 1: In FMC integrierten Connector für dynamische Attribute verwenden](#)

[Option 2: Verwendung des Cloud-basierten Dynamic Attributes Connectors in CDO](#)

[Voraussetzungen, unterstützte Plattformen, Lizenzierung](#)

[Mindestanzahl unterstützter Software- und Hardwareplattformen](#)

[Verwendete Komponenten](#)

[Funktionsdetails](#)

[Eigenständige CSDAC-Übersicht \(Derzeit veröffentlicht - 7.4\)](#)

[CSDAC in CDO Übersicht \(Derzeit veröffentlicht - 7.4\)](#)

[CSDAC in FMC](#)

[So funktioniert es](#)

[Connectors konfigurieren](#)

[CSDAC in FMC](#)

[Dynamische Objekte](#)

[Wechselstromrichtlinie](#)

[Konfiguration: Zugriffsrichtlinie](#)

[Plattformgrenzen](#)

[Fehlerbehebung/Diagnose](#)

[Überprüfen der Anschlüsse](#)

[Anzeigen von Anschlüssen auf der Registerkarte "Anschlüsse"](#)

[Attributfilter überprüfen](#)

[Überprüfen der dynamischen Objekte in der FMC-Benutzeroberfläche](#)

[CSDAC-Statuswarnungen](#)

[CSDAC bei Fehlerbehebung](#)

[Erstellen einer CSDAC-Fehlerbehebung](#)

[CLI-Fehlerbehebung](#)

[CSDAC-Debug-Modus](#)

[Protokollierte Nachrichten mit Debug](#)

[Beispielproblem bei der Fehlerbehebung - exemplarische Vorgehensweise](#)

[Überblick über Probleme und Fehlerbehebung](#)

[Problem:](#)

[Fehlerbehebung:](#)

[Fehlerbehebtes Paket vorbereiten](#)

[Tag-Attribute für eine IP-Adresse anzeigen](#)

[Zusammenfassung der Prüfungen](#)

[Fragen und Antworten](#)

Einleitung

In diesem Dokument wird der Cisco Secure Dynamic Attribute Connector in FMC beschrieben.

Hintergrund - Problem

CSDAC (Cisco Secure Dynamic Attributes Connector) kann in FMC (FirePOWER Management Center) integriert werden und bietet den gleichen Funktionsumfang wie die eigenständige CSDAC-Anwendung und CSDAC in CDO. Bei eigenständiger CSDAC entfällt der Verwaltungsaufwand und die Wartung eines separaten Systems für CSDAC. Als Netzwerkadministrator möchte ich, dass sich die Programmschnittstellen leicht integrieren lassen und mit den Änderungen an externen Anbietern dynamischer Umgebungen auf dem neuesten Stand sind. Diese Integration löst das Problem, Attribute aus dynamisch wechselnden Cloud-Umgebungen zu erfassen, ohne eine Richtlinie bereitzustellen.

Lösung (Zusammenfassung)

CSDAC kann jetzt in FMC konfiguriert werden, um Tag-Attribute aus Azure, vCenter, AWS, GCP, Office 365 und Azure Service Tags abzurufen, sodass Funktionsparität mit dem eigenständigen CSDAC und CSDAC in CDO gewährleistet ist.

- Sie können nun auswählen,
 - CSDAC im FÜZ (oder)
 - CSDAC in CDO (oder)
 - Standalone-CSDAC
- Zielmarkt: Enterprise, Service Provider

Dynamic Attributes Connector in FMC - Zusammenfassung

FMC Dynamic Attributes Connector:

- Dashboard-Bildschirm zum Erstellen und Betreiben der Dynamic Attribute Connector-Funktionen.
- FMC-Benutzeroberfläche zum Konfigurieren von Connectors für Quellworkloads (AWS, Azure, vCenter, Office 365, GCP)
- FMC-Benutzeroberfläche zur Definition dynamischer Attributfilter zur Erstellung dynamischer Objekte

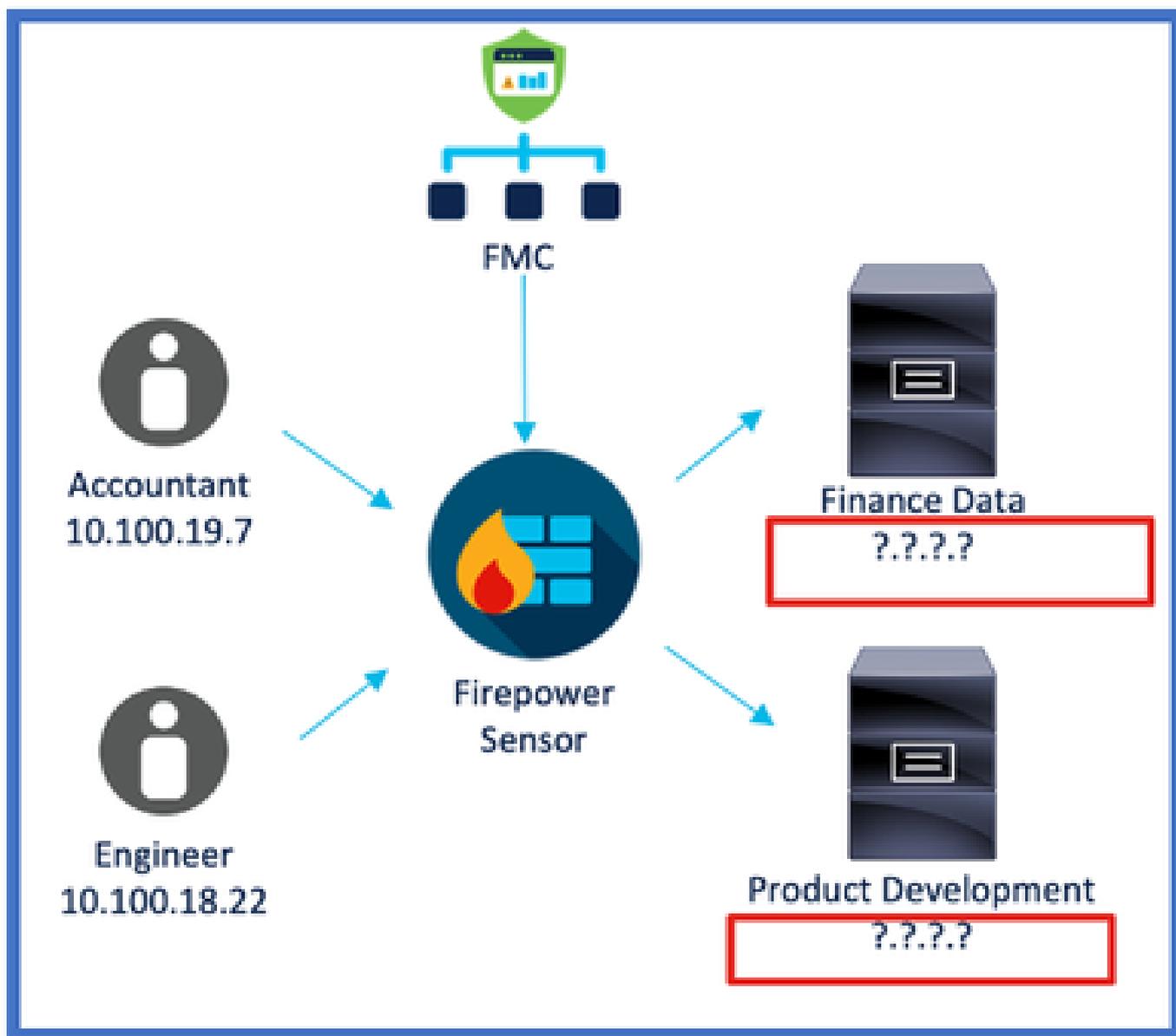
Bereitstellungsbeispiele

CSDAC vor Ort

Im vergangenen Jahr habe ich eine dedizierte VM für CSDAC bereitgestellt, um Attribute von meinen AWS- und Azure-Konten zu erfassen.

Das Problem

Nun ist meine Organisation in die Cloud umgestiegen, und ich kann in meiner Umgebung kein dediziertes virtuelles System für CSDAC bereitstellen und verwalten.



Option 1: In FMC integrierten Connector für dynamische Attribute verwenden

Sie können das Problem beheben, indem Sie den in FMC integrierten Dynamic Attributes Connector verwenden. Die von ihm erstellten dynamischen Objekte können in der Zugriffsrichtlinie verwendet werden.

Option 2: Verwendung des Cloud-basierten Dynamic Attributes Connectors in CDO

Sie können das Problem beheben, indem Sie Dynamic Attributes Connector in CDO verwenden. Die von ihr erstellten dynamischen Objekte können in

- CDO Cloud-Delivery FMC
- CDO FMC vor Ort

Voraussetzungen, unterstützte Plattformen, Lizenzierung

Mindestanzahl unterstützter Software- und Hardwareplattformen

Min. unterstützte Manager-Version	Verwaltete Geräte	Min. unterstützte Version des verwalteten Geräts erforderlich	Hinweise
FMC 7.4	Alle FTD-unterstützten	Beliebige FTD 7.0+	

* Dynamic Attributes Connector wird auf FDM-verwalteten Geräten nicht unterstützt.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Firewall Management Center mit 7.4
- Cisco Firepower Threat Defense mit Version 7.4 oder höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Funktionsdetails

Eigenständige CSDAC-Übersicht (Derzeit veröffentlicht - 7.4)

Mit dem Cisco Secure Dynamic Attributes Connector können Sie Tags von verschiedenen Cloud-Service-Plattformen in den Zugriffskontrollregeln des Firewall Management Center (FMC) verwenden.

CSDAC kann vor Ort auf einem Linux-Computer installiert werden und unterstützt das Abrufen von Attributen von:

- AWS, Azure, VMware vCenter und NSX-T, Office 365, Azure Service Tags, GCP, GitHub.

CSDAC in CDO Übersicht (Derzeit veröffentlicht - 7.4)

Unterstützt dieselben Funktionen wie On-Prem CSDAC, ohne dass eine dedizierte Anwendung installiert und gewartet werden muss.

Der vCenter-Connector wird derzeit in CDO nicht unterstützt.

Unterstützt das Senden der empfangenen Attribute an Cloud-basierte FMC und On-Prem FMC in CDO.

CSDAC in FMC

Unterstützt dieselben Funktionen wie Standalone-CSDAC, ohne dass eine dedizierte Anwendung installiert und gewartet werden muss.

CSDAC in FMC unterstützt das Abrufen von Attributen aus:

- AWS, Azure, VMware vCenter und NSX-T, Office 365, Azure Service Tags, GCP, GitHub

Es gibt hier keine explizite Adapterkonfiguration, da diese für FMC lokal ist.

So funktioniert es

Connectors werden verwendet, um Attribute von AWS, Azure, o365, vCenter abzurufen.

Der lokale Adapter wird dann verwendet, um diese optimierten Attribute und ihre IP-Zuordnungen in FMC als dynamische Objekte zu speichern.

FMC sendet die Zuordnung in Echtzeit an FTD (ohne Bereitstellung).



Aktivieren von CSDAC in FMC

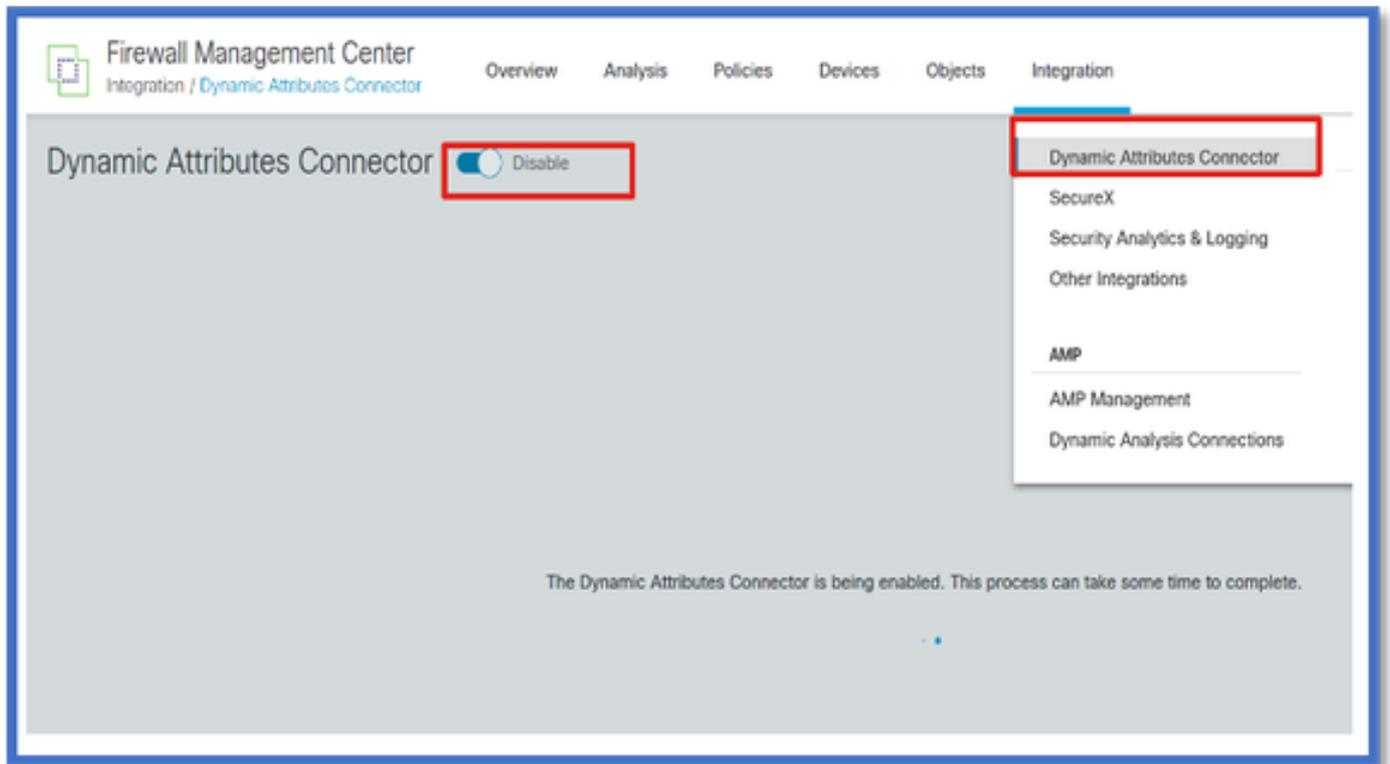
Navigieren Sie zu Integration > Dynamic Attributes Connector.

Verwenden Sie die Umschalttaste, um den Anschluss zu aktivieren.

FMC benötigt nur wenige Minuten zum Herunterladen und Aufrufen der Docker-Images und -

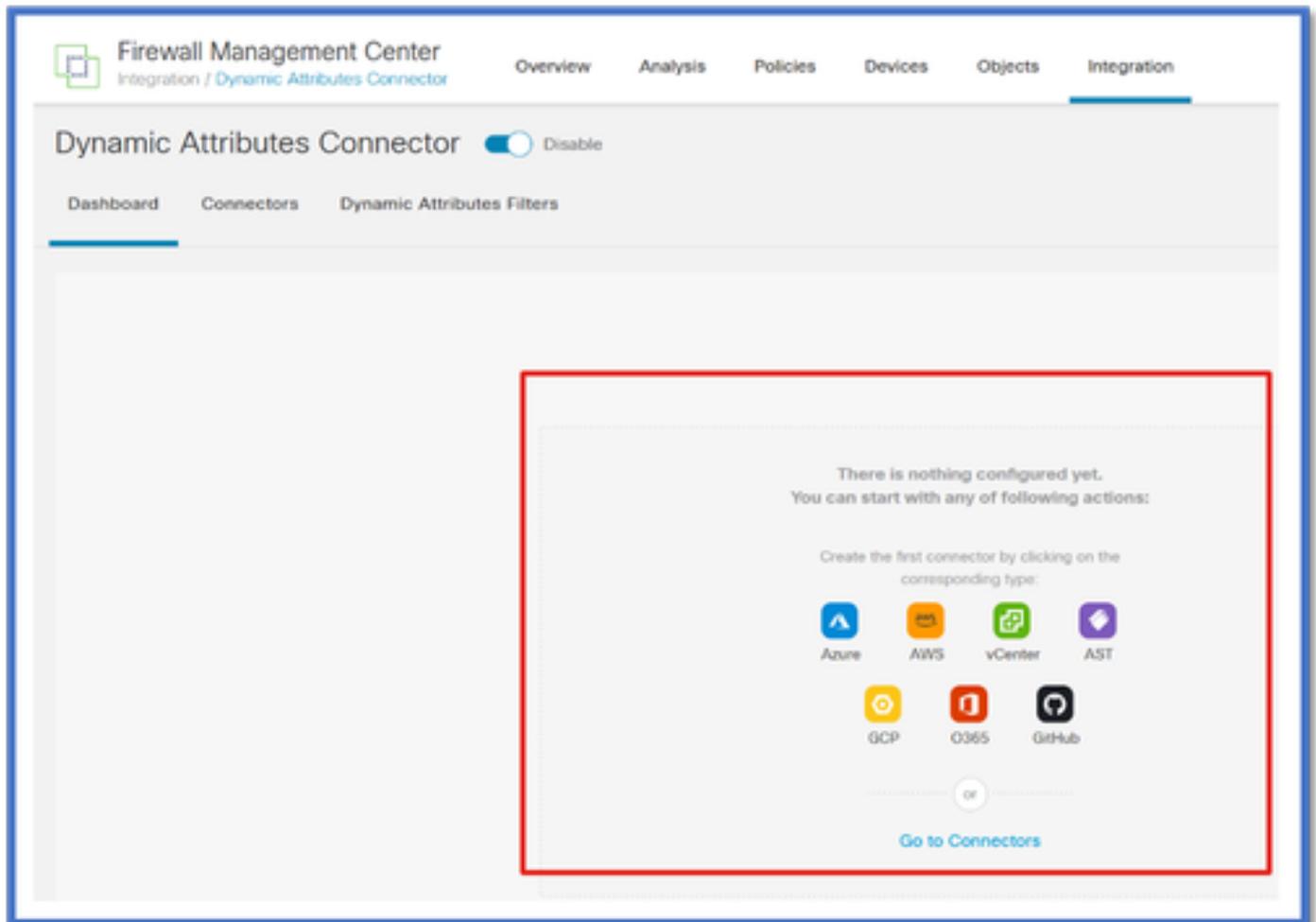
Container.

Dies kann nur in der globalen FMC-Domäne konfiguriert werden.



CSDAC-Dashboard

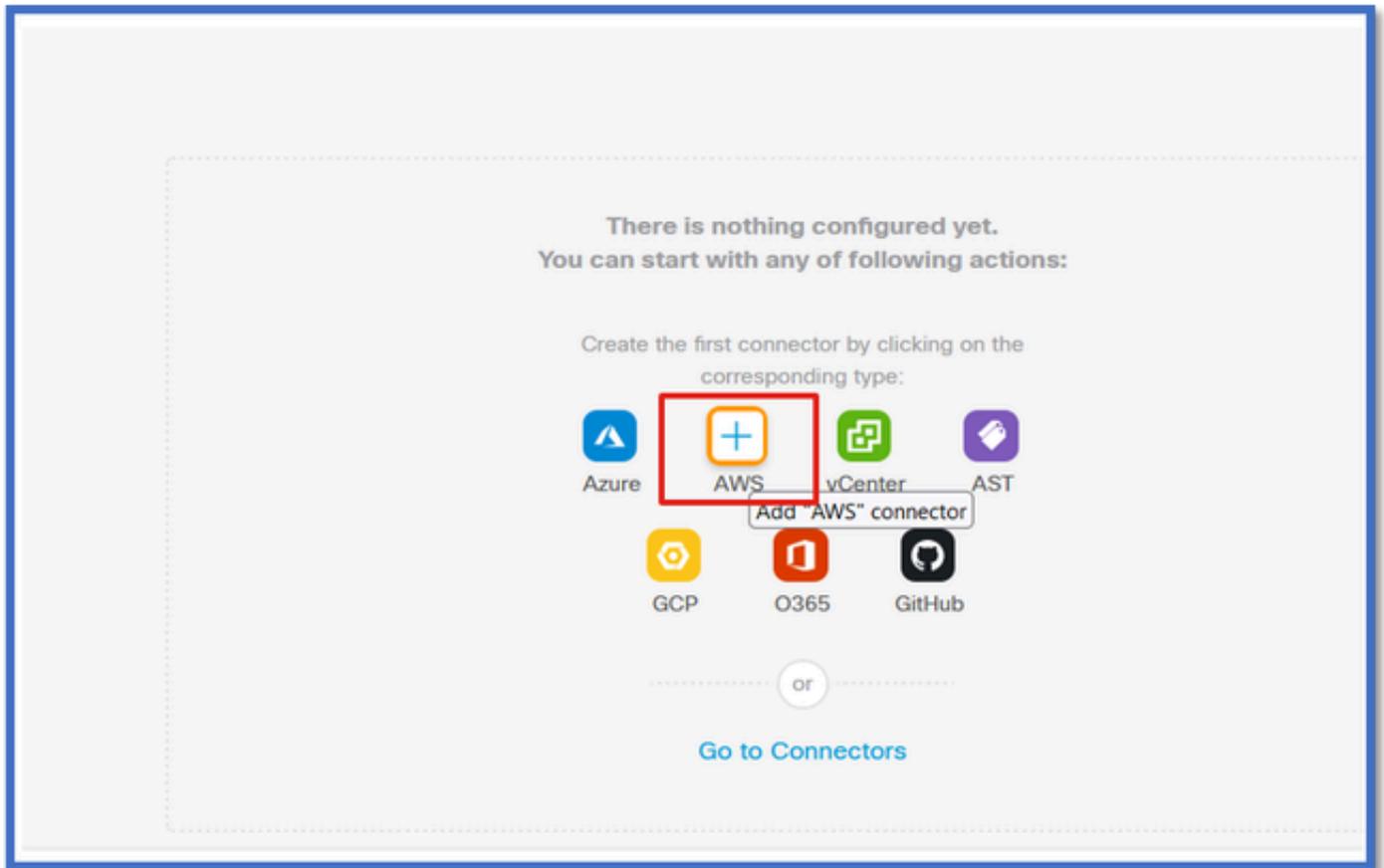
Nach der Aktivierung von CSDAC wird dem Benutzer die Seite "CSDAC Dashboard" angezeigt. Das Dashboard dient zum Konfigurieren und Anzeigen konsolidierter Connectors und Filter.



Connectors konfigurieren

Hinzufügen von Connectors über das Dashboard

Klicken Sie im Dashboard auf das Symbol für den gewünschten Connector, um ihn hinzuzufügen.



Konfigurieren Sie ein Zeitintervall (im Feld "Pull Interval" (Pull-Intervall)), sodass die Connectors Informationen von Anbietern mit der konfigurierten Periodizität abrufen können.

Geben Sie die Anmeldeinformationen des Anbieters ein, um die Tag-Attribute abzurufen. Nachdem Sie den Connector konfiguriert haben, können Sie den Connector testen, indem Sie auf die Schaltfläche Test klicken.

Edit AWS Connector

Name*
AWS

Description

Pull Interval (sec)*
30

Region*
us-east-1

Access Key*
AKIA2PWAVDBNRHF6UKIQ

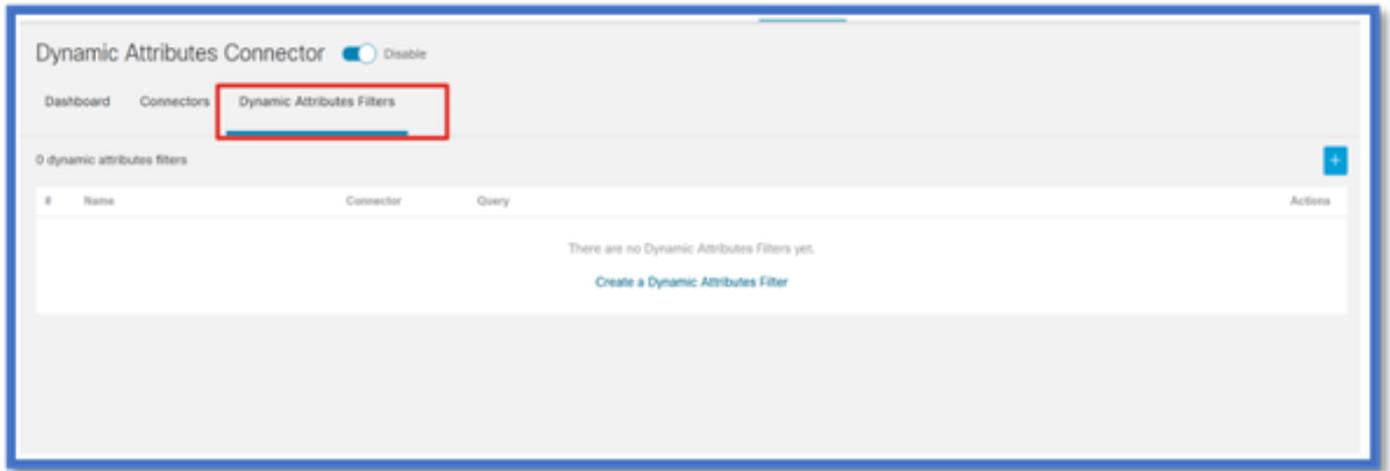
Secret Key*

Test again ✓ Test connection succeeded

Cancel Save

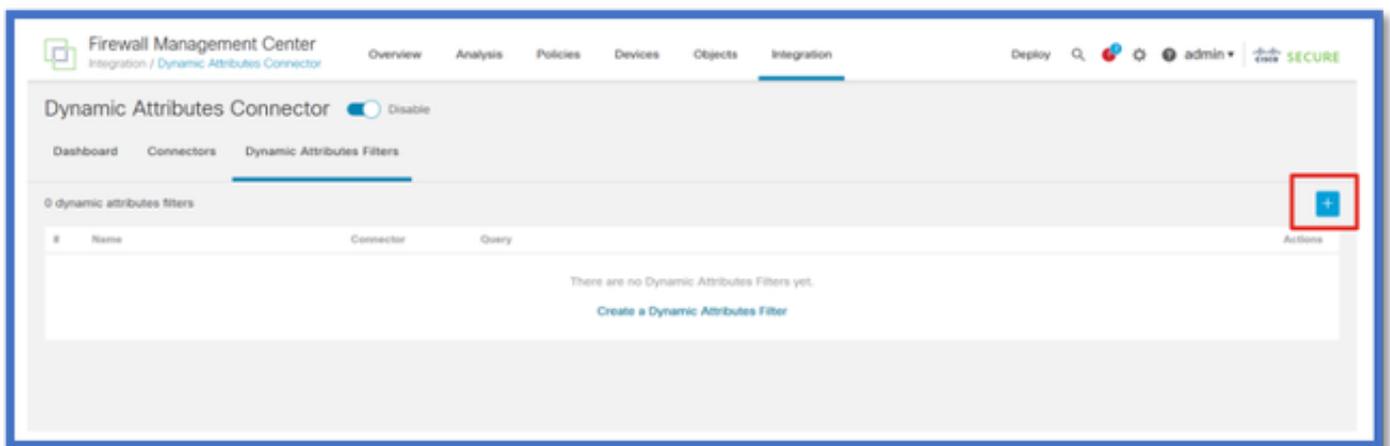
Filter konfigurieren

Klicken Sie im Menü "Dynamic Attributes Connector" auf die Registerkarte "Dynamic Attribute Filters", um zur Seite "Dynamic Attributes Filters" zu gelangen.



Filter hinzufügen

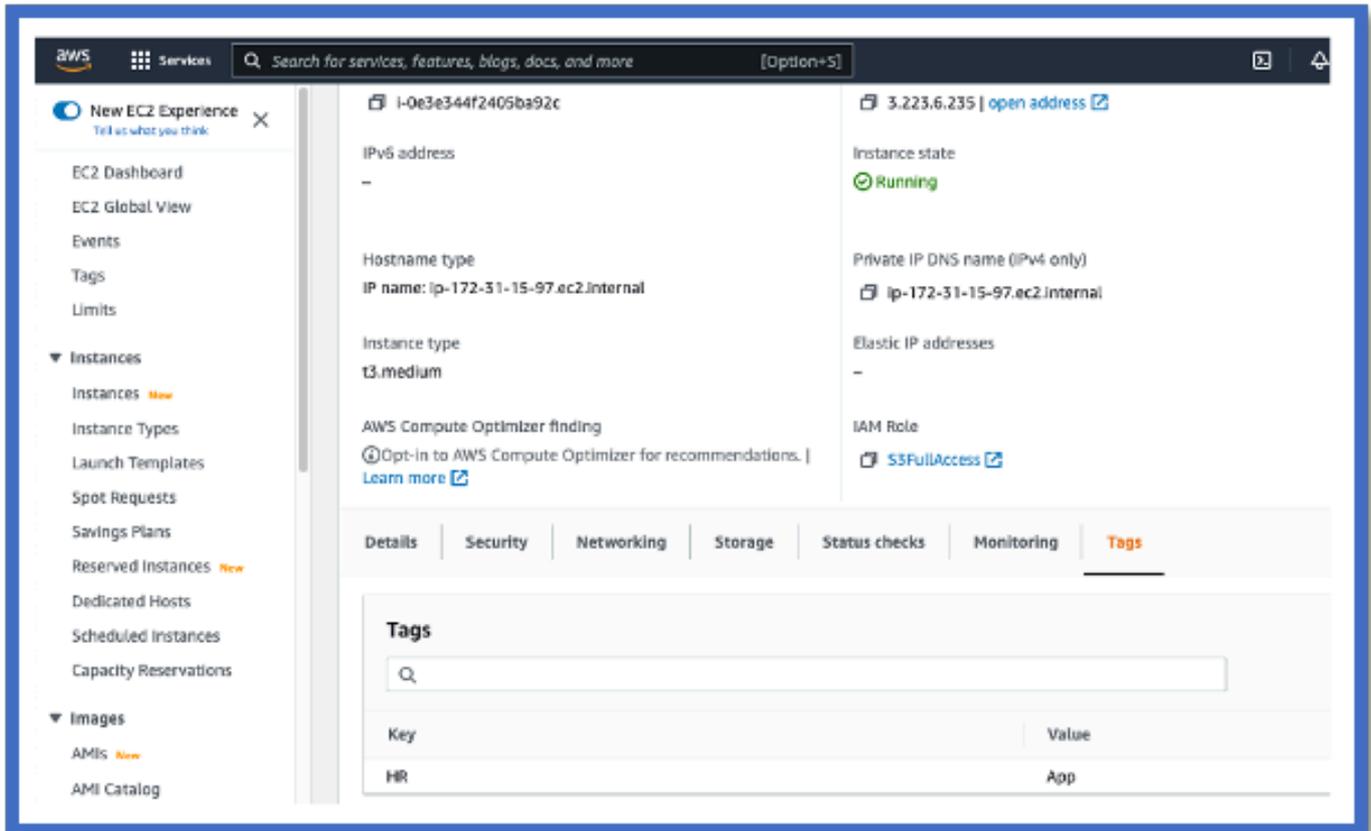
Klicken Sie auf die Schaltfläche +, um einen Filter für Attributverbindungen zu erstellen.



AWS-Tags hinzufügen

Wir können beispielsweise davon ausgehen, dass Sie sich für die wichtigsten Aspekte im Zusammenhang mit der Personalabteilung und dem Wert der Anwendung bei AWS-Workloads interessieren.

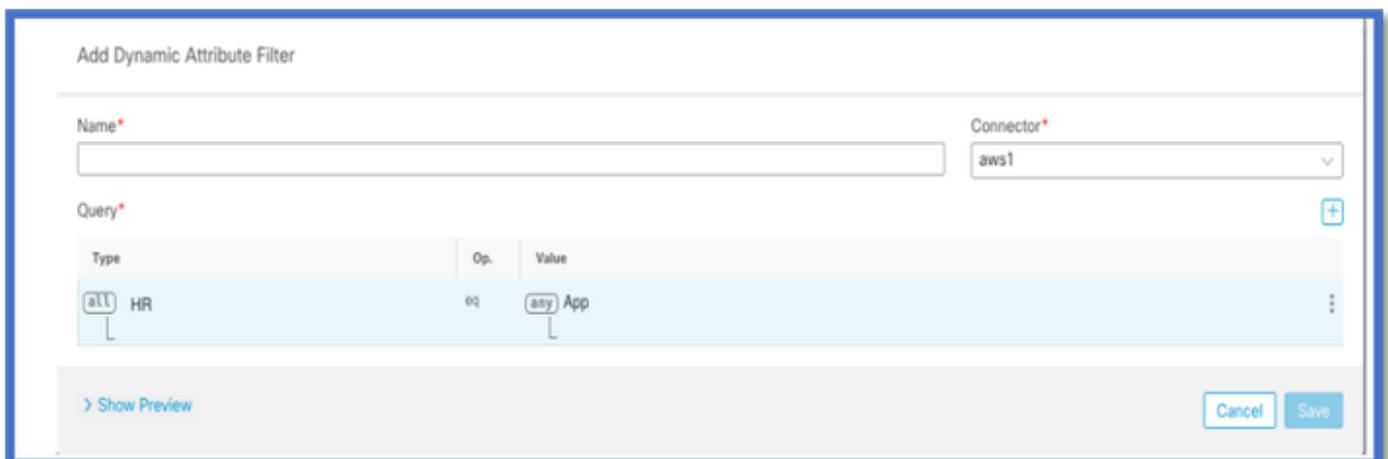
So würde es in AWS aussehen.



CSDAC in FMC

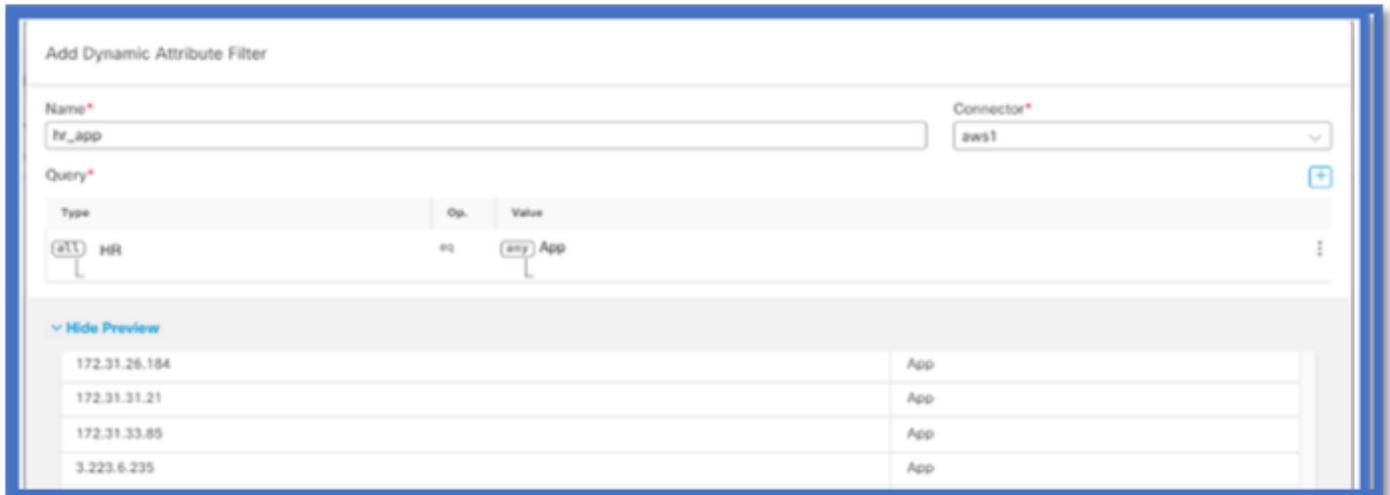
Sie können eine Regel "HR gleich App" erstellen, indem Sie auf die Schaltfläche + klicken.

Der lokale FMC-Adapter sendet die entsprechenden IP-Adressen als dynamische Objektzuordnungen an FMC.



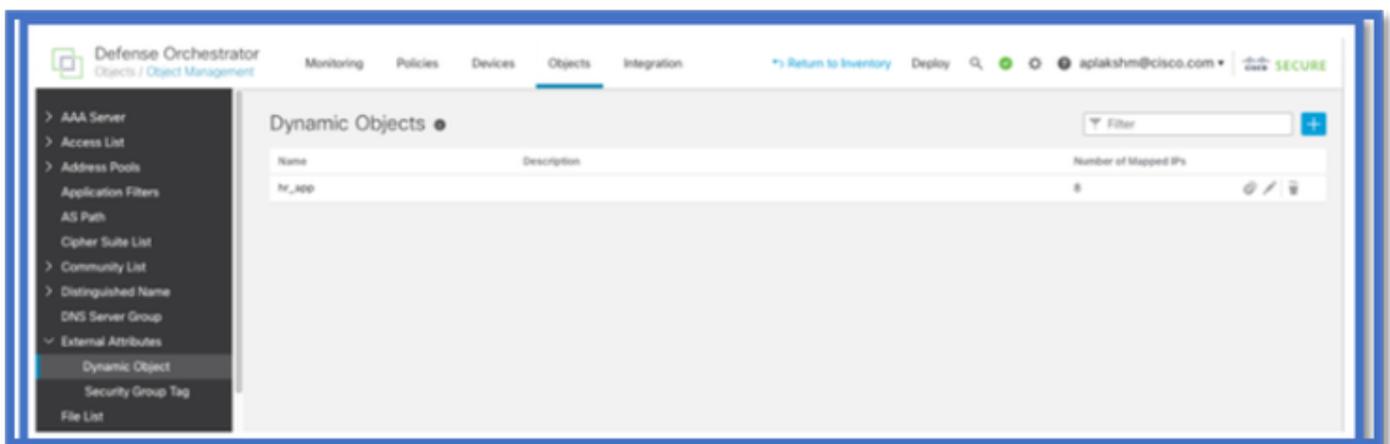
Vorschau

Sie können auch die übereinstimmenden IP-Adressen einer bestimmten Attributregel anzeigen, indem Sie auf die Schaltfläche "Show" (Anzeigen) | Schaltfläche "Vorschau ausblenden".



Dynamische Objekte

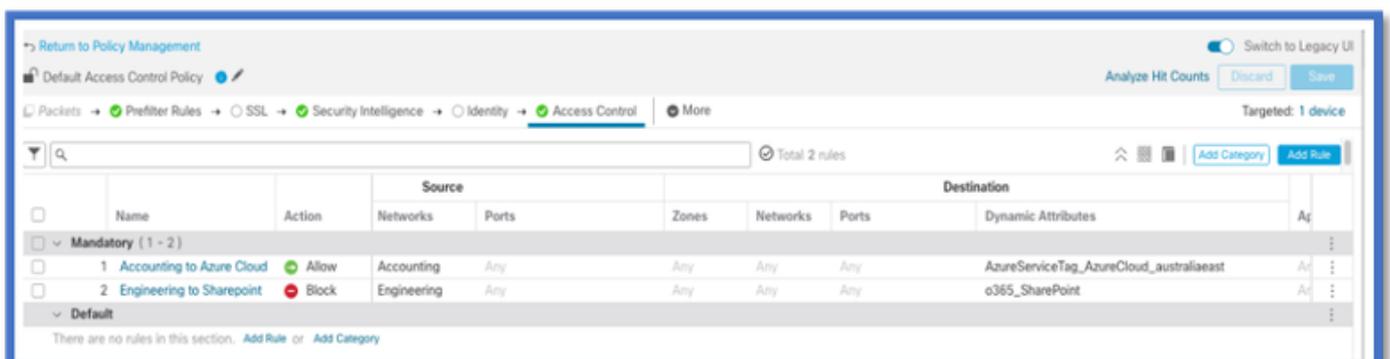
Zeigen Sie die von CSDAC erstellten dynamischen Objekte unter Objekte > Externe Attribute, Dynamisches Objekt in FMC an.



Wechselstromrichtlinie

Konfiguration: Zugriffsrichtlinie

Fügen Sie in FMC eine Zugriffsrichtlinie hinzu, um die empfangenen dynamischen Objekte vom Dynamic Attribute Connector zu erlauben oder zu blockieren.



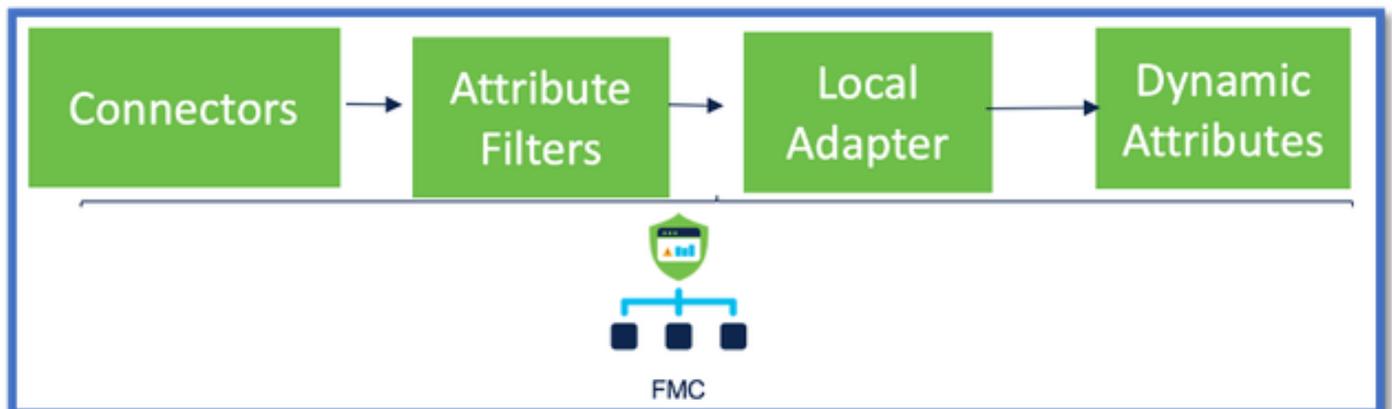
Plattformgrenzen

- Die Anzahl der Anschlüsse basiert auf dem verfügbaren FMC-Speicher.
- vFMC benötigt einen zusätzlichen Arbeitsspeicher von 1 GB, um 5 Anschlüsse zu unterstützen.
- Azure AD-Bereich ist ebenfalls im Limit enthalten, da es sich ebenfalls um einen CSDAC-Container handelt.

Modelle	Anzahl unterstützter Anschlüsse	Plattformen	Speicherbasiertes Limit
Grundlegend	Nur Azure AD	1600	32 GB
Klein	5	vFMC	> 32 GB
Mittel	10	vFMC 300, 2600	>= 64 GB
Groß	20	4600	>= 128 GB

Fehlerbehebung/Diagnose

Die Fehlerbehebung wird am besten durch die Nachverfolgung dynamischer Objekte von CSDAC-Connectors zu Dynamics-Attributen in FMC durchgeführt. Viele interne Protokolle bezeichnen diese Funktion als "zusammenbringen". Sie können einen Blick in den Systemstatus entlang der Übertragungskette werfen, um Probleme zu isolieren. CSDAC verwendet Docker-Container. Meldungen und Namen von Protokollen und anderen Dateien müssen als "Docker" bezeichnet werden.



Überprüfen der Anschlüsse

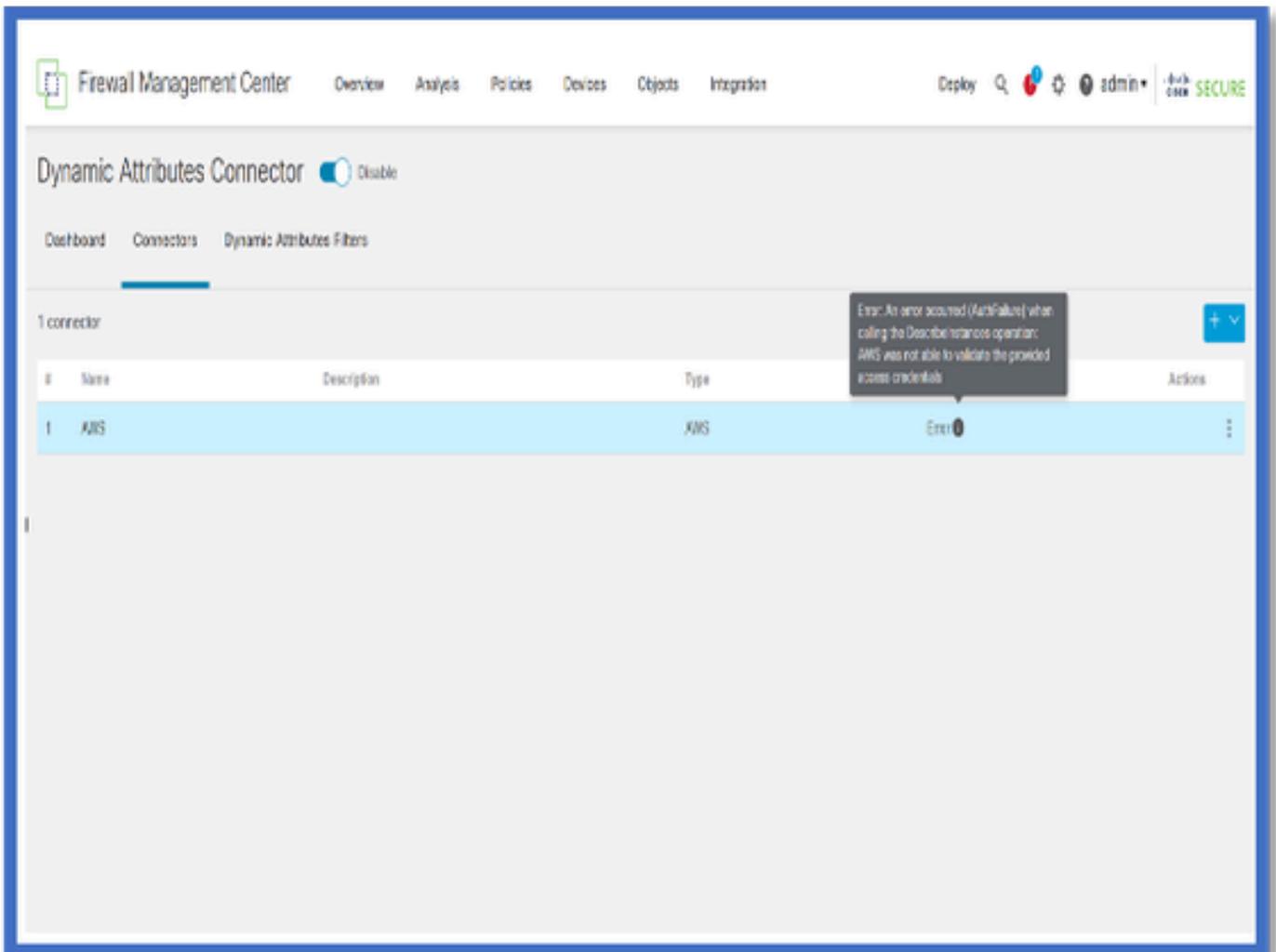
Stellen Sie zunächst sicher, dass Connectors eine Verbindung zu vCenter-, AWS- oder Azure-Servern herstellen können.

Wenn Connectors nicht richtig konfiguriert sind, können Downstream-Prozesse keine Tag-Informationen abrufen.

Anzeigen von Anschlüssen auf der Registerkarte "Anschlüsse"

Der Verbindungsstatus wird im Statusfeld angezeigt und alle 15 Sekunden aktualisiert.

In diesem Beispiel konnte der Connector die angegebenen Anmeldeinformationen nicht verwenden.



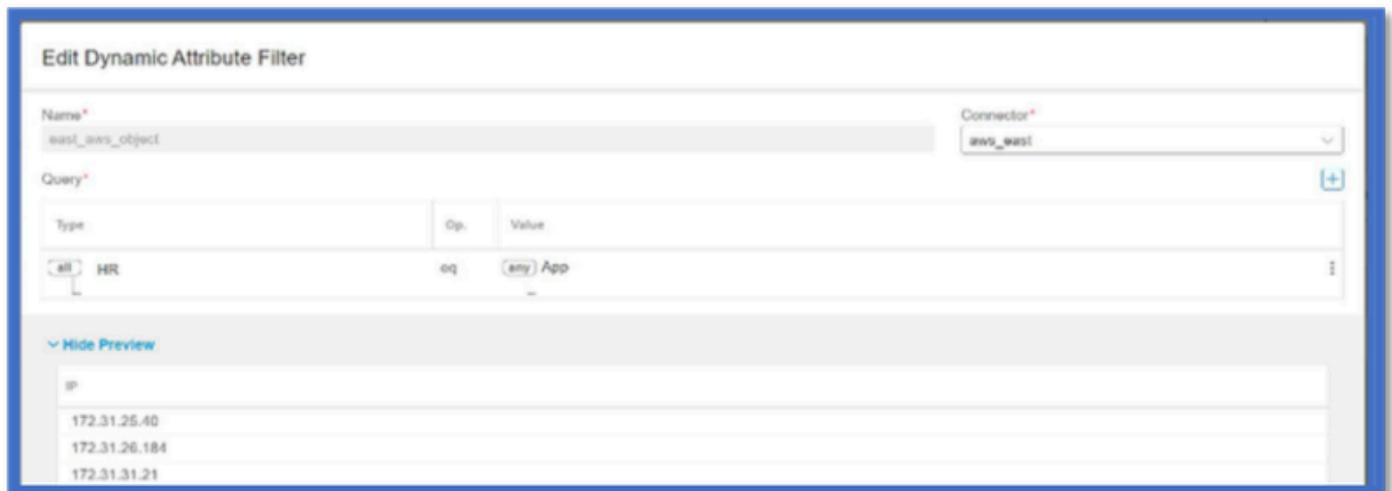
Attributfilter überprüfen

Stellen Sie sicher, dass in der Regelvorschau die übereinstimmenden IP-Adressen für die Abfragebedingung angezeigt werden.

Wenn keine übereinstimmenden IP-Adressen vorhanden sind, kann FMC die dynamischen Objektzuordnungen nicht abrufen.

Attributfilter überprüfen

Überprüfen Sie, ob dynamische Attribut-IP-Zuordnungen in der Vorschau verfügbar sind. Die Schaltfläche Vorschau anzeigen ist im Popup-Fenster zum Bearbeiten von dynamischen Attributfiltern verfügbar.



Überprüfen der dynamischen Objekte in der FMC-Benutzeroberfläche

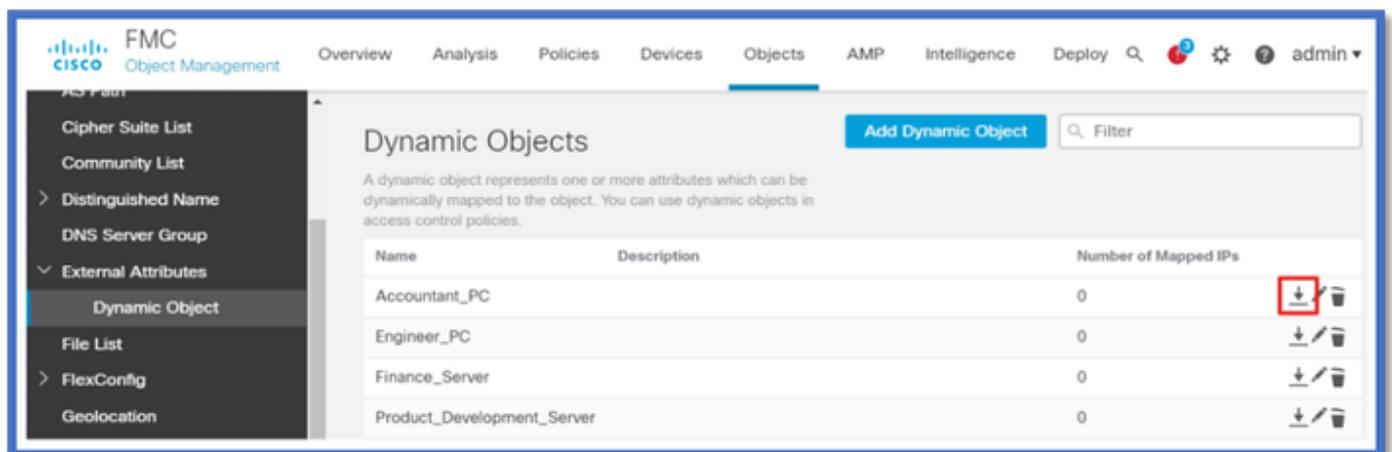
Stellen Sie zunächst sicher, dass der FMC-Server die erwarteten Bindungen enthält.

- Aktivieren Sie auf der Registerkarte Externe Objekte unter Objektverwaltung das Kontrollkästchen Dynamische Objekte für Bindungen.
- Wenn FMC die Bindungen nicht erhält, kann FTD sie nicht erhalten.

Überprüfen Sie den FMC-Zustandsmonitor und die Benachrichtigungen auf CSDAC-Zustandswarnungen.

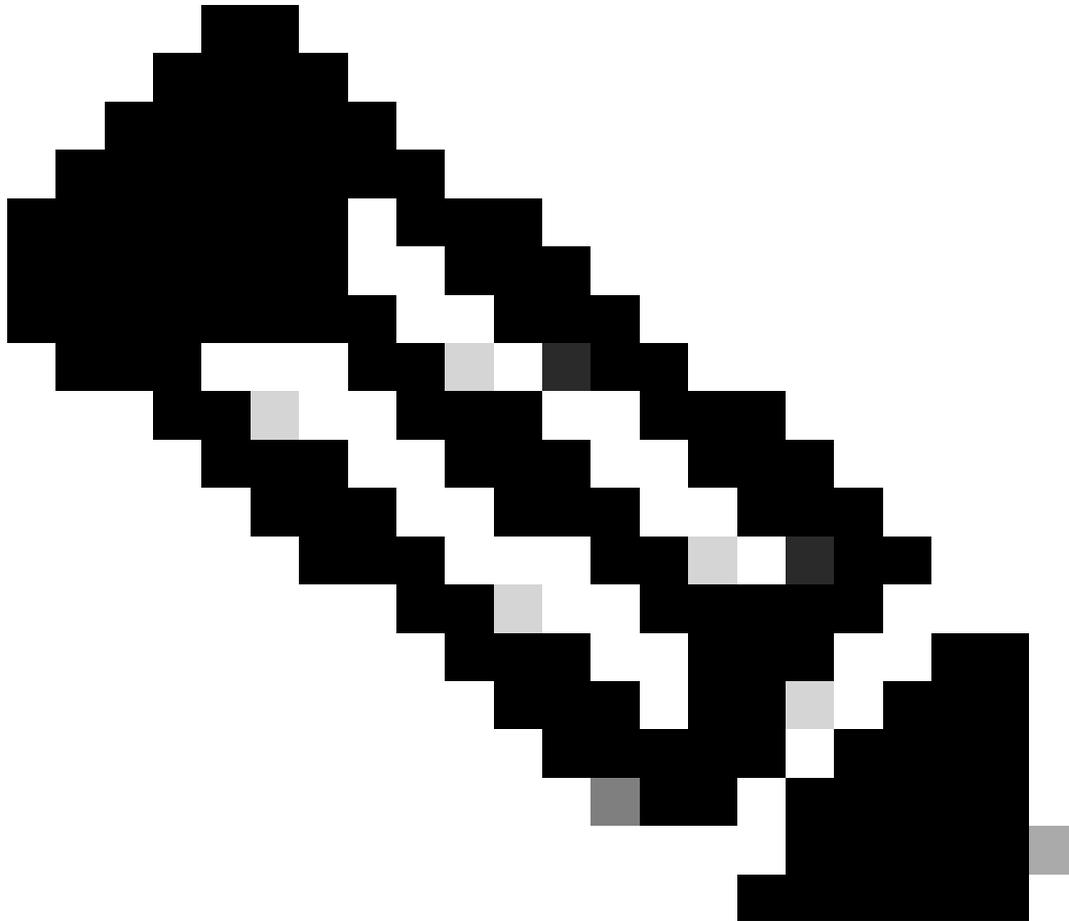
Überprüfen dynamischer Objekte

Mit dem FMC Object Manager können Sie aktuelle Dynamic Object IP-Adressen herunterladen.

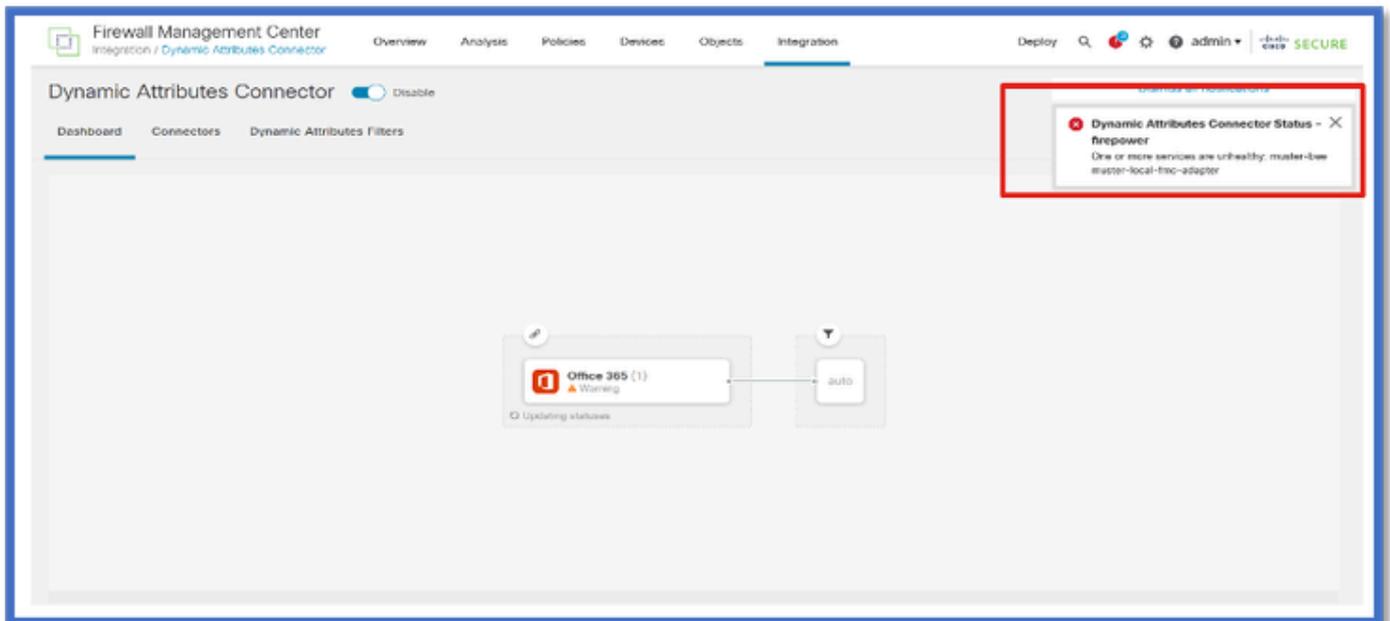


CSDAC-Statuswarnungen

Der Task-Manager von FMC zeigt Health Alerts an, wenn ein Kerndienst, einschließlich des Dynamic Attributes Connectors, ausgefallen ist. Die Warnmeldung enthält Informationen zu Servicename und -status.

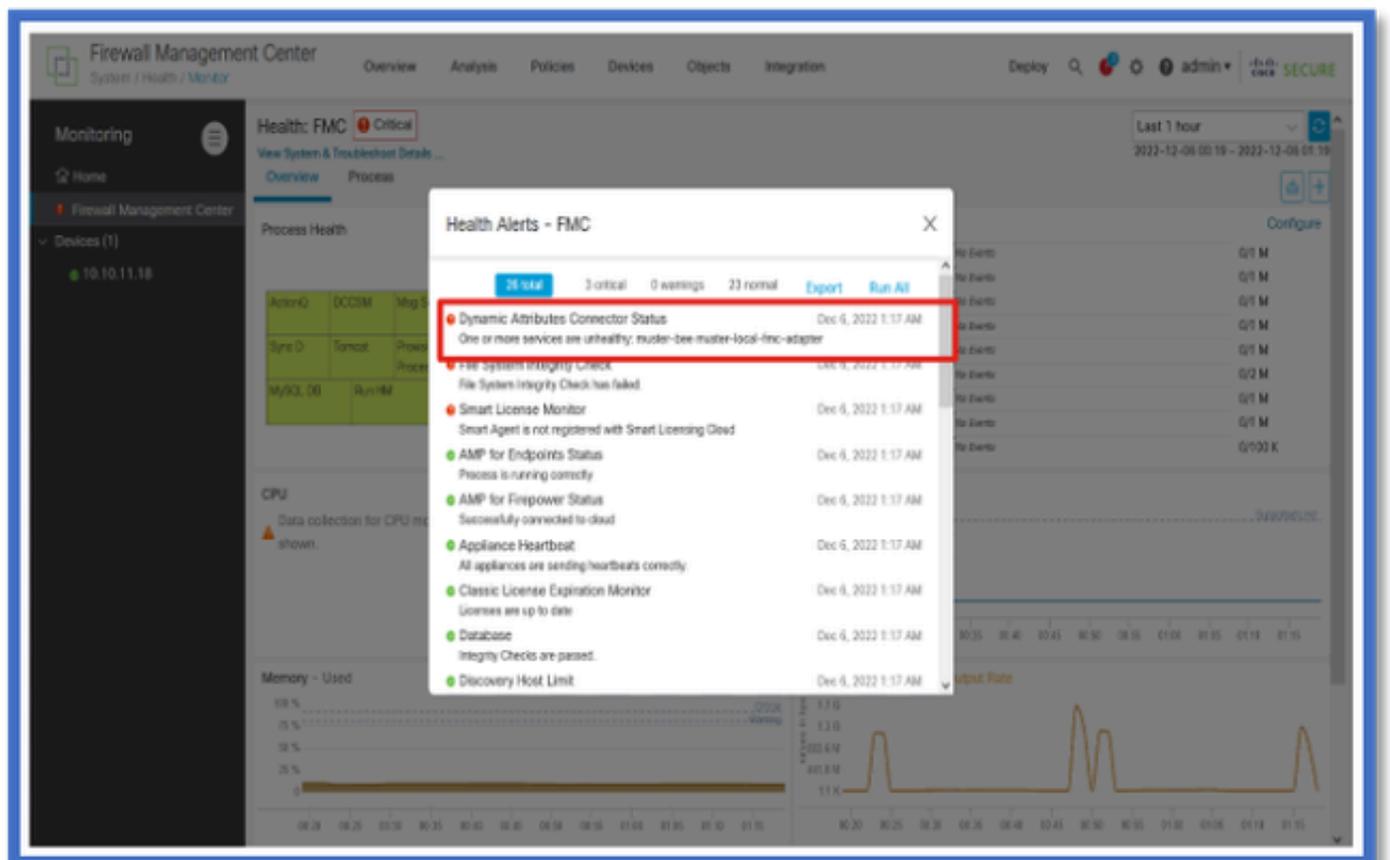


Hinweis: In mehreren Benachrichtigungen ist die Namensgebung "muster" immer noch vorhanden, und es muss hier ein Servicename für detaillierte Informationen angegeben werden.



Hier sehen wir, dass muster-bee und muster-local-fmc-adapter "ungesund" sind.

Wenn ein Fehler auf einen der Kerndienste hinweist, müssen Fehlerbehebungsprotokolle zum Debuggen erfasst werden.



CSDAC bei Fehlerbehebung

Erstellen einer CSDAC-Fehlerbehebung

- CSDAC-Protokolle werden automatisch während der FMC-Fehlerbehebung erfasst. Das Paket enthält den Docker-Status, Protokolle und Daten, die zur Offline-Fehlerbehebung des Problems erforderlich sind.
- Es empfiehlt sich, den CSDAC-Debugmodus zu aktivieren, bevor Fehler wiedergegeben werden, für die Fehlerbehebungsprotokolle erfasst werden.

Aus /usr/local/sf/csdac Aufruf ./muster-cli debug-on

Suchen Sie die CSDAC-Protokolle in untarred Troubleshoot in folgenden Ordnern:

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

Dieser enthält die in der Datenbank etc. gespeicherten Daten.

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

Dieser enthält die Protokolle aus den Dockingcontainern.

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

Hier sehen Sie den Containerstatus, die Versionen und die Details zum Docker-Bild.

CLI-Fehlerbehebung

Das Skript muster-cli kann verwendet werden, um den Status von CSDAC aus der FMC-CLI zu überprüfen.

Wenn der Status für einen Dienst "Beendet" ist oder sich auf andere Weise von "Nach oben" unterscheidet, beginnen Sie mit der Überprüfung der Protokolle für diesen Container.

Der Containername wird zum Abrufen von Protokollen benötigt. Er kann aus der Ausgabe abgerufen werden.

```

root@firepower:/Volume/home/admin# cd /usr/local/sf/csdac/
root@firepower:/usr/local/sf/csdac# ./muster-cli status
===== CORE SERVICES =====
-----
Name                Command                State                Ports
-----
muster-bee          ./docker-entrypoint.sh run ... Up                127.0.0.1:15050->50050/tcp, 50443/tcp
muster-envoy        /docker-entrypoint.sh runs ... Up                127.0.0.1:6443->8443/tcp
muster-local-fmc-adapter ./docker-entrypoint.sh run ... Up
muster-ui-backend   ./docker-entrypoint.sh run ... Up                50031/tcp
===== CONNECTORS AND ADAPTERS =====
-----
Name                Command                State                Ports
-----
muster-connector-aws.2.muster          ./docker-entrypoint.sh run ... Up                50070/tcp
muster-connector-o365.1.muster         ./docker-entrypoint.sh run ... Up                50070/tcp

```

CSDAC-Debug-Modus

Das Skript 'muster-cli' kann verwendet werden, um die Debug-Protokolle ein- und auszuschalten. Standardmäßig werden die Container unter INFO level.INFO protokolliert, und DEBUG sind die einzigen unterstützten Ebenen.

Um Benutzer auf DEBUG-Ebene zu aktivieren: `./muster-cli debug-on`.

Dadurch stehen weitere Informationen zur Fehlerbehebung und Hilfe bei der Fehlerbehebung zur Verfügung. Diese Option muss aktiviert werden, während ein Problem reproduziert wird.

Um zur INFO-Ebene zurückzukehren, verwenden Sie: `./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
```

Protokollierte Nachrichten mit Debug

Wenn der Debug-Modus aktiviert ist, enthalten alle Docker-Containerprotokolle auch Debugmeldungen.

Abrufen von Protokollen in Echtzeit mithilfe der Docker-Befehle: `docker logs -f <Containername>`

Im folgenden Beispiel wird in der Debugmeldung angezeigt, was einen gRPC-Fehler ausgelöst hat.

<#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 connect to backend
```

Beispielproblem bei der Fehlerbehebung - exemplarische Vorgehensweise

Überblick über Probleme und Fehlerbehebung

Problem:

Das häufigste Problem ist, dass FMC nicht alle dynamischen Objektzuordnungen empfängt.

Fehlerbehebung:

Um das Problem zu beheben,

- Debug-Modus von "muster-cli" aktivieren
- Von FMC-UI generierte Problemlösungsdatei
- Überprüft, ob die AWS Connector-Anmeldungen von CSDAC die Fehlerbehebung erfasst haben.
- Es wurde festgestellt, dass CSDAC AWS Connector nur die erste IP in den AWS-Instanzen abgefragt hat.

Fehlerbehebtes Paket vorbereiten

- Von FMC CLI aus haben wir den Debug-Modus aktiviert, indem `./muster-cli debug-on` verwendet wird. Das Werkzeug `muster-cli` ist in `/usr/local/sf/csdac` verfügbar.
- Das Problem wurde neu erstellt, indem der Connector den Status "OK" erhalten hat und anschließend die Filter für dynamische Attribute überprüft wurden.
- Fehlerbehebungsprotokolle aus der FMC-Benutzeroberfläche gesammelt und extrahiert. AWS Connector-Protokolle auf Inhalt des Snapshots überprüft

```
~/results-12-12-2022--124229/command-outputs$ tree csdac_troubleshoot/
csdac_troubleshoot/
├── info
│   ├── muster-bee.log.gz
│   ├── muster-ui-backend.log.gz
│   └── muster-ui-backend-saved-db
│       ├── config_2022.12.12-12.43.22.tgz
│       ├── docker_compose_2022.12.12-12.43.22.tgz
│       └── status_2022.12.12-12.43.22.tgz
├── logs
│   ├── journald-boots.log
│   ├── journald-day.log.gz
│   ├── muster-bee-docker.log.gz
│   └── muster-connector-aws.1.muster-docker.log.gz
│       ├── muster-connector-gcp.1.muster-docker.log.gz
│       ├── muster-connector-github.1.muster-docker.log.gz
│       ├── muster-connector-o365.1.muster-docker.log.gz
│       ├── muster-envoy-docker.log.gz
│       ├── muster-local-fmc-adapter-docker.log.gz
│       ├── muster-ui-backend-docker.log.gz
│       └── muster-user-analysis-docker.log.gz
└── status.log.gz

3 directories, 17 files
```

Tag-Attribute für eine IP-Adresse anzeigen

Die Tag-Attribute für eine bestimmte IP werden in den Fehlerbehebungsprotokollen protokolliert. Für AWS Connector haben wir "muster-connector-aws.1.muster-docker.log.gz" untersucht.

Zusammenfassung der Prüfungen

Stehen Stecker- und Adapterstatus gut da?

Überprüfen Sie die Status auf den entsprechenden Seiten Connector (Anschluss), Adapter (Adapter).

Haben die Connectors alle Zuordnungen erhalten?

Überprüfen Sie die Regelvorschau auf übereinstimmende IP-Adressen.

Überprüfen Sie die Connector Docker-Protokolle, um festzustellen, ob die Zuordnungen korrekt abgefragt werden.

Hat der REST-Server dynamische Tag-Zuordnungen vom Connector erhalten?

Überprüfen Sie die Seite für dynamische FMC-Objekte.

Überprüfen Sie die USMS-Protokolle (in /opt/CSCOPx/MDC/log/operation/usmsharredsvcs.log), um festzustellen, ob der FMC-REST-Server die API-Anforderung von CSDAC ordnungsgemäß verarbeitet hat.

Fragen und Antworten

F: Welche Version des standortbasierten CSDAC unterstützt einen ISE-Connector, einen solchen sehe ich auch in Version 7.4.0 (Build 1494) nicht?

A: Dies ist in Standalone-CSDAC und nicht in FMC oder in CDO. Sie benötigen ein CSDAC-fähiges Paket, um dies zu testen.

F: Welche CSDAC-Version vor Ort wäre es, wenn sie veröffentlicht würde?

A: Wahrscheinlich 2.1.0.

F: Es wurde ein Bildschirm mit einem Gerät gezeigt, das über eine API verfügt. Ich denke, es ist CSDAC; was bedeutet das?

A: Der API-Explorer ist in diesem CSDAC integriert. Sie können von dieser Seite aus API-Aufrufe für CSDAC durchführen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.