Distribuisci connettore attributo dinamico sicuro in FMC

Sommario

Introduzione

In questo documento viene descritto Cisco Secure Dynamic Attribute Connector In FMC.

Sfondo - Problema

CSDAC (Cisco Secure Dynamic Attributes Connector) può essere integrato in FMC (Firepower Management Center), fornendo lo stesso livello di funzionalità dell'applicazione CSDAC standalone e di CSDAC in CDO. Per CSDAC standalone, solleva i clienti dal sovraccarico di amministrazione e manutenzione di una macchina separata per CSDAC. In qualità di amministratore di rete, desidero che le interfacce programmatiche siano facilmente integrabili e aggiornate con le modifiche apportate ai provider esterni dell'ambiente dinamico. Questa integrazione risolve il problema della raccolta di attributi da ambienti cloud in continua evoluzione senza implementare una policy.

Soluzione (riepilogo)

È ora possibile configurare CSDAC in FMC per recuperare gli attributi dei tag da Azure, vCenter, AWS, GCP, Office 365 e dai tag di servizio di Azure, fornendo la parità delle funzionalità con CSDAC e CSDAC autonomi in CDO.

- È ora possibile scegliere di utilizzare
  - CSDAC in FMC (o)
  - CSDAC in CDO (o)
  - CSDAC autonomo
- Mercato di destinazione: azienda, provider di servizi

Connettore degli attributi dinamici nel riepilogo di FMC

Connettore attributi dinamici FMC:

- Schermata del dashboard per creare e utilizzare le funzionalità di Dynamic Attribute Connector.
- Interfaccia utente di FMC per configurare i connettori del carico di lavoro di origine (AWS, Azure, vCenter, Office 365, GCP)
- Interfaccia utente di FMC per definire filtri attributi dinamici per creare oggetti dinamici

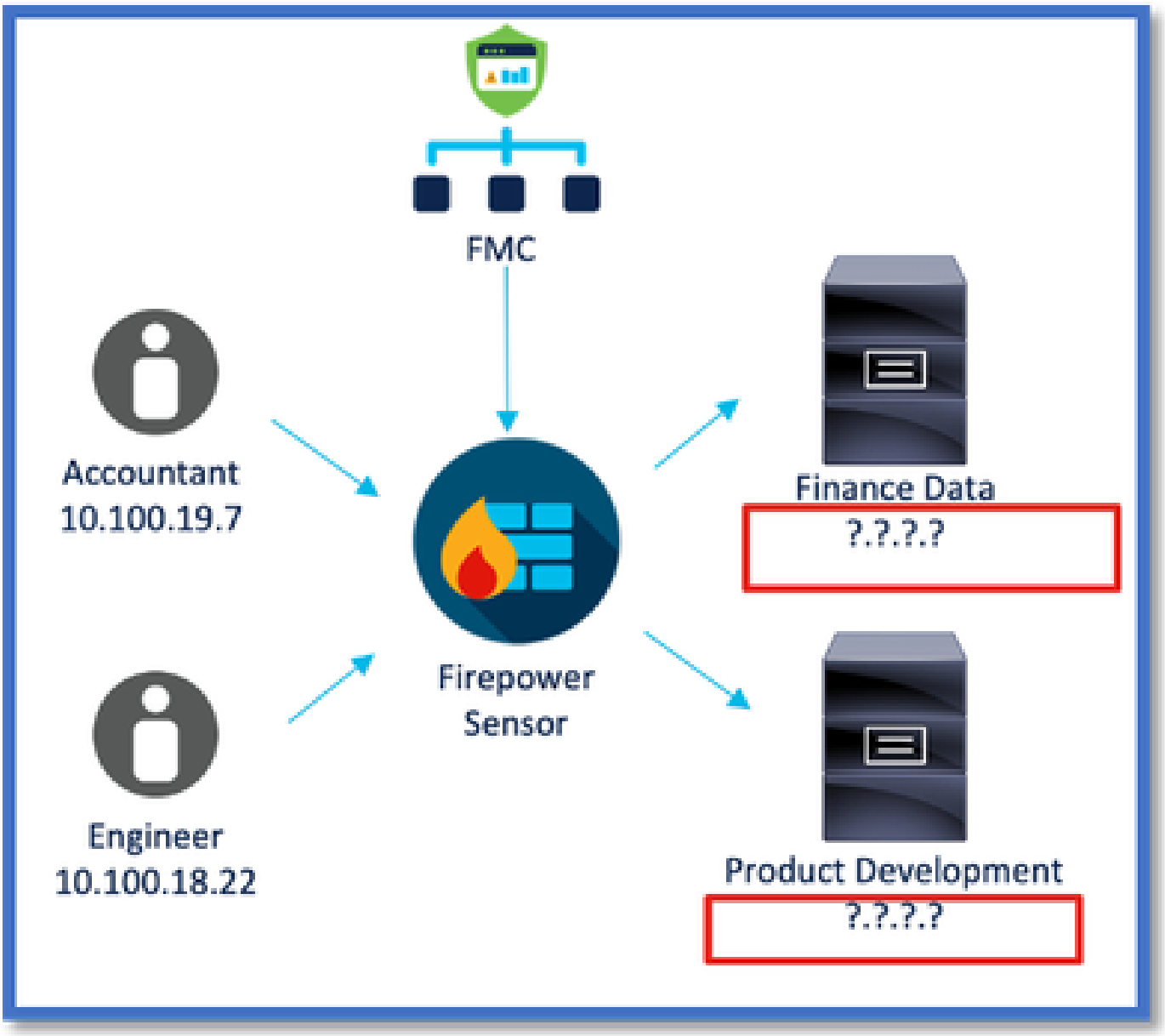
Esempi di distribuzione

CSDAC locale

L'anno scorso ho distribuito una macchina virtuale dedicata per CSDAC per raccogliere gli attributi dagli account AWS e Azure.

Il problema

Ora, la mia organizzazione è passata al cloud e non posso distribuire e gestire una macchina virtuale dedicata per CSDAC nel mio ambiente.



Opzione 1: utilizzare il connettore degli attributi dinamici incorporato in FMC

È possibile risolvere il problema utilizzando il connettore degli attributi dinamici incorporato in FMC. Gli oggetti dinamici creati possono essere utilizzati nei criteri di accesso.

Opzione 2: utilizzare il connettore degli attributi dinamici fornito dal cloud in CDO

È possibile risolvere il problema utilizzando il connettore Attributi dinamici in CDO. Gli oggetti dinamici creati possono essere utilizzati in

- CDO FMC distribuito tramite cloud
- CDO FMC locale

Prerequisiti, Piattaforme supportate, Licenze

Minimo piattaforme software e hardware supportate

Versione minima di Gestione supportata	Dispositivi gestiti	Versione minima dispositivo gestito supportato richiesta	Note
CCP 7.4	Qualsiasi FTD supportato	Qualsiasi FTD 7.0+	

* Dynamic Attributes Connector non è supportato sui dispositivi gestiti da FDM

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:
· Cisco Firewall Management Center con versione 7.4
· Cisco Firepower Threat Defense con versione 7.4 o successive.
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Dettagli funzionalità

Panoramica di CSDAC standalone (versione corrente - 7.4)

Cisco Secure Dynamic Attributes Connector consente di utilizzare tag di diverse piattaforme di servizi cloud nelle regole di controllo di accesso di Firewall Management Center (FMC).

Il CSDAC locale è installabile su un computer Linux e supporta il recupero di attributi da:

- AWS,Azure,VMware vCenter e NSX-T,Office 365,Codici di matricola di Azure,GCP,GitHub.

CSDAC in CDO Panoramica (Attualmente rilasciato - 7.4)

Supporta le stesse funzionalità di CSDAC locale senza la necessità di installare e mantenere

un'applicazione dedicata.

Il connettore vCenter non è attualmente supportato in CDO.

Supporta l'invio degli attributi ricevuti a un FMC distribuito tramite cloud e a un FMC locale in CDO.

CSDAC in FMC

Supporta le stesse funzionalità di CSDAC standalone senza la necessità di installare e mantenere un'applicazione dedicata.

CSDAC in FMC supporta il recupero di attributi da:

- AWS,Azure,VMware vCenter e NSX-T,Office 365,Codici di matricola di Azure,GCP,GitHub

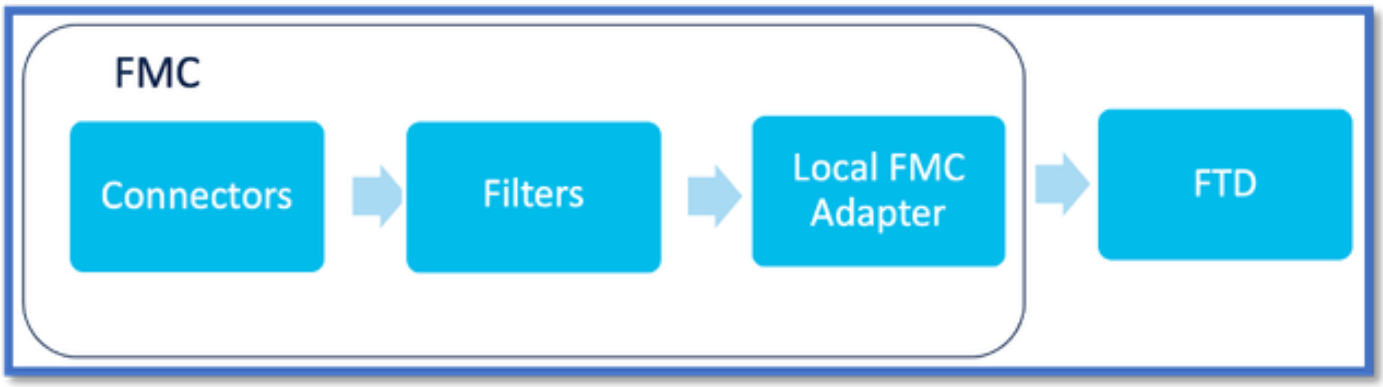
Non è presente alcuna configurazione esplicita dell'adattatore, in quanto è locale rispetto a FMC.

Come funziona

I connettori vengono utilizzati per ottenere attributi da AWS, Azure, o365, vCenter.

La scheda locale viene quindi utilizzata per salvare questi attributi semplificati e i relativi mapping IP in FMC come oggetti dinamici.

FMC invia la mappatura in tempo reale a FTD (senza distribuzione).



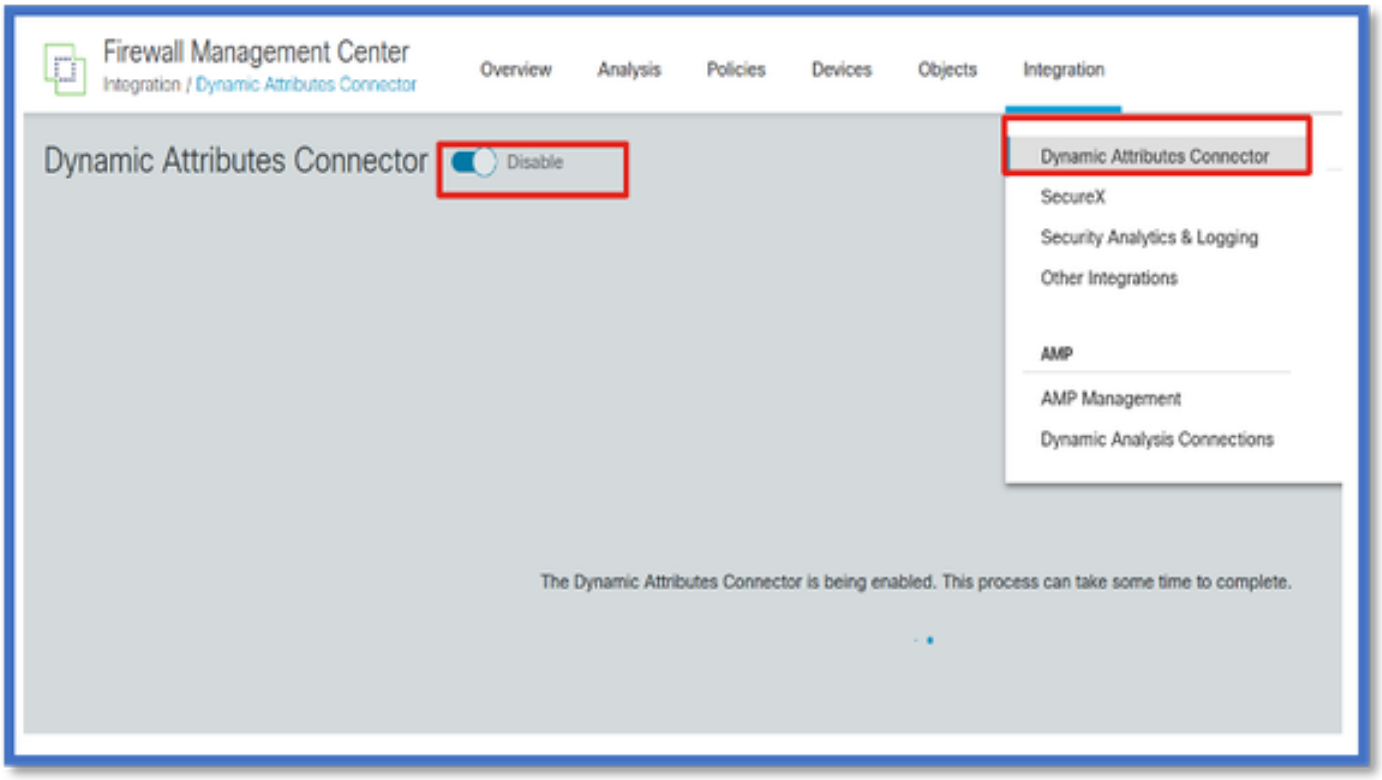
Abilita CSDAC in FMC

Selezionare Integrazione > Connettore attributi dinamici.

Utilizzare il pulsante Attiva/disattiva per attivare il connettore.

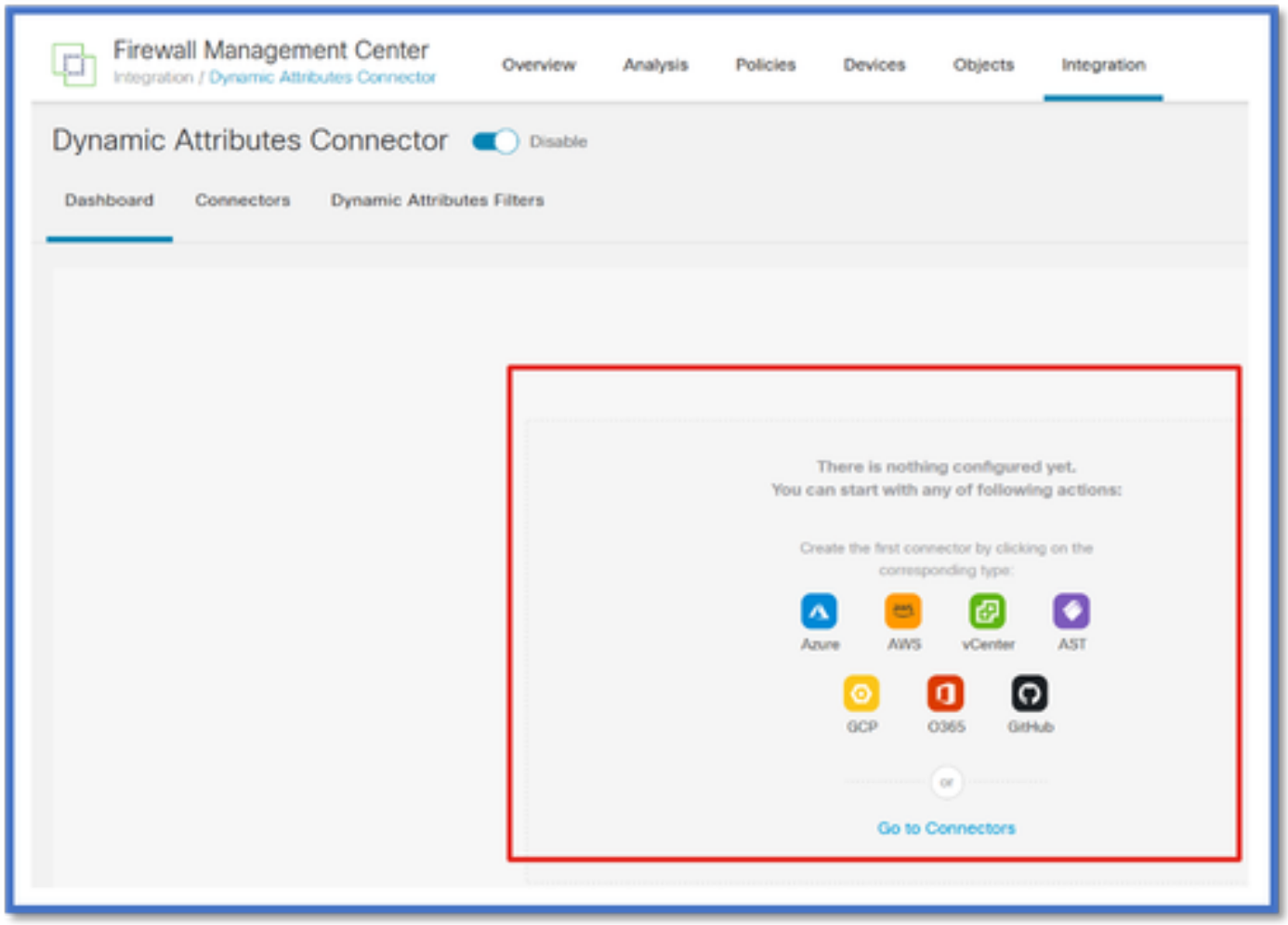
FMC impiega alcuni minuti per scaricare e visualizzare le immagini e i contenitori del docker.

Questa impostazione può essere configurata solo nel dominio globale FMC.



Dashboard CSDAC

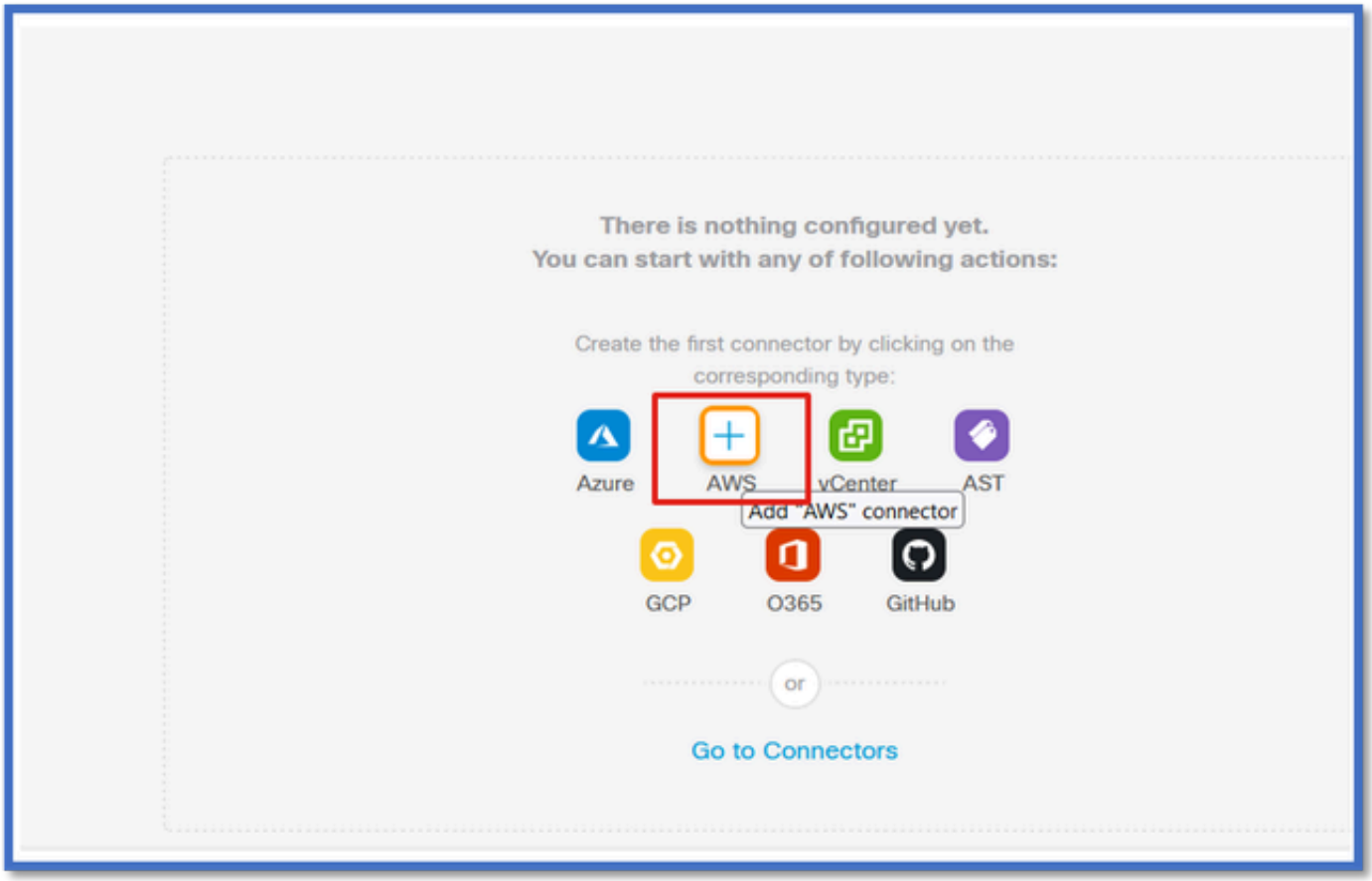
Dopo aver abilitato CSDAC, all'utente viene visualizzata la pagina CSDAC Dashboard. Dashboard viene utilizzato sia per configurare che per visualizzare i connettori consolidati e per filtrare.



Configura connettori

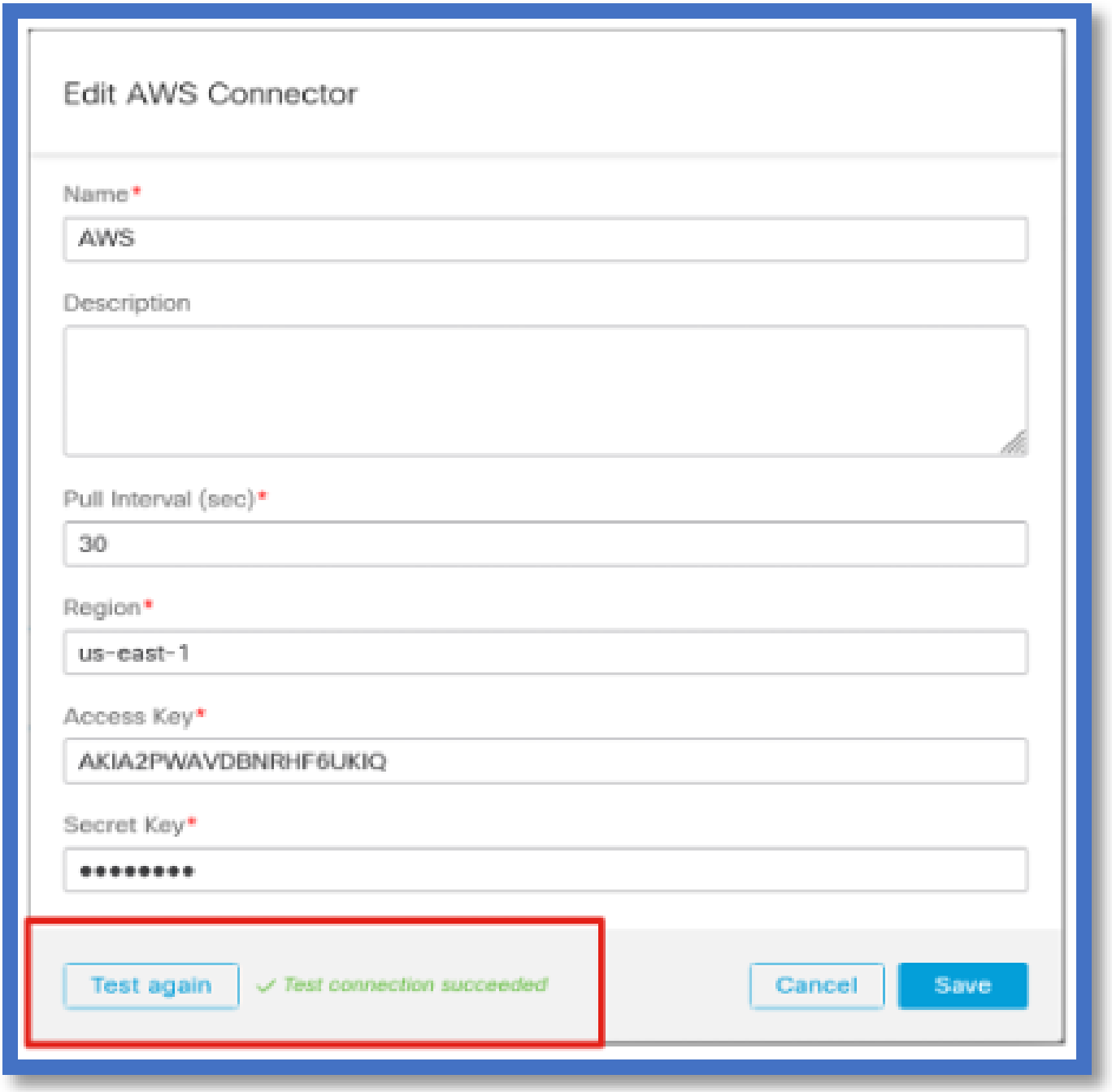
Aggiungi connettori dal dashboard

Nel quadro comandi, fare clic sull'icona del connettore desiderato per aggiungerlo.



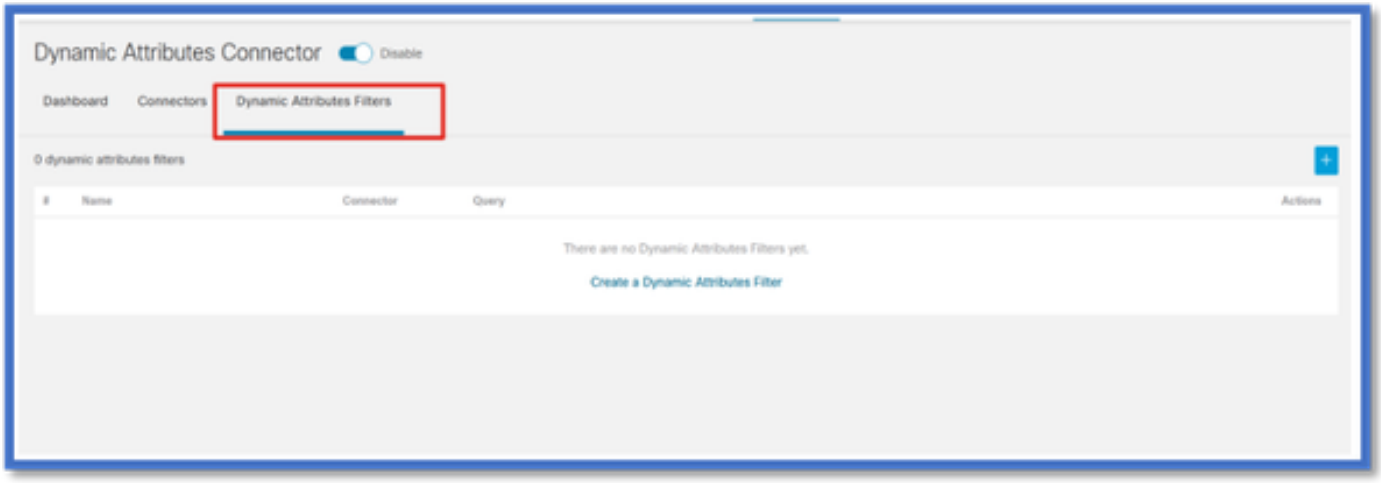
Configurare un intervallo di tempo (nel campo Intervallo di pull) in modo che i connettori possano recuperare le informazioni dai provider con la periodicità configurata.

Immettere le credenziali del provider per ottenere gli attributi di tag. Una volta configurato il connettore, è possibile verificarlo facendo clic sul pulsante Test.



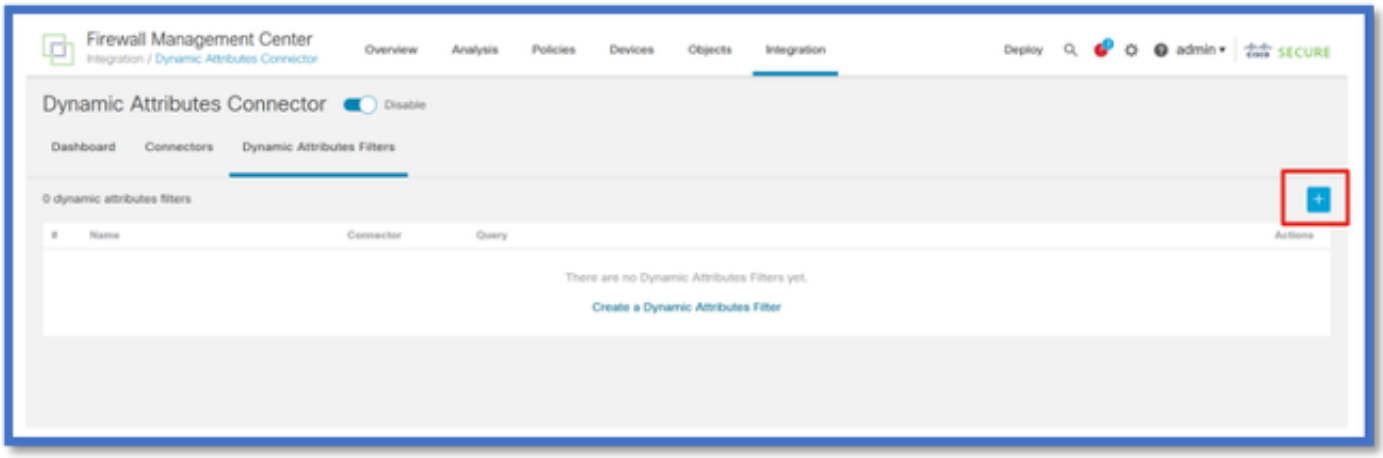
Configura filtri

Fare clic sulla scheda "Filtri attributi dinamici" nel menu "Connettore attributi dinamici" per accedere alla pagina Filtri attributi dinamici.



Aggiunta di filtri

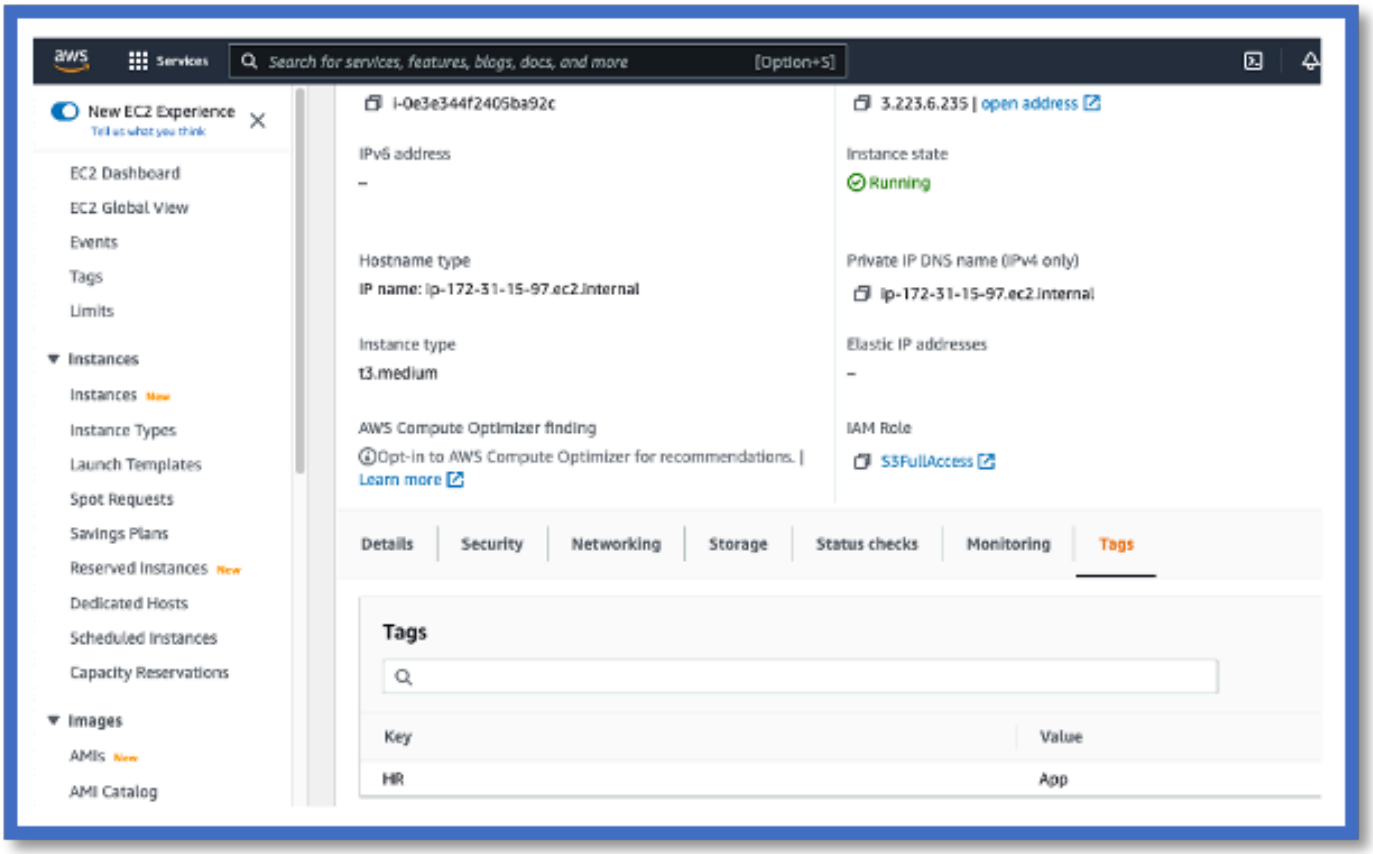
Fare clic sul pulsante + per creare un filtro per i connettori attributo.



Aggiungi tag AWS

Si supponga, ad esempio, di essere interessati alla chiave ‘HR’ e al valore ‘App’ nei carichi di lavoro AWS.

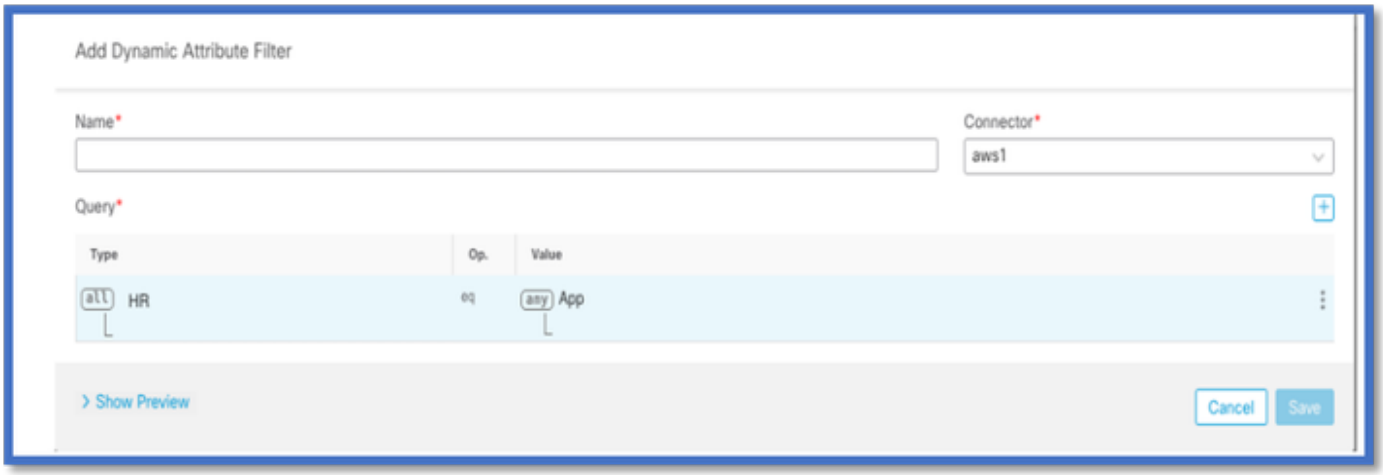
Questo è come apparirebbe in AWS.



CSDAC in FMC

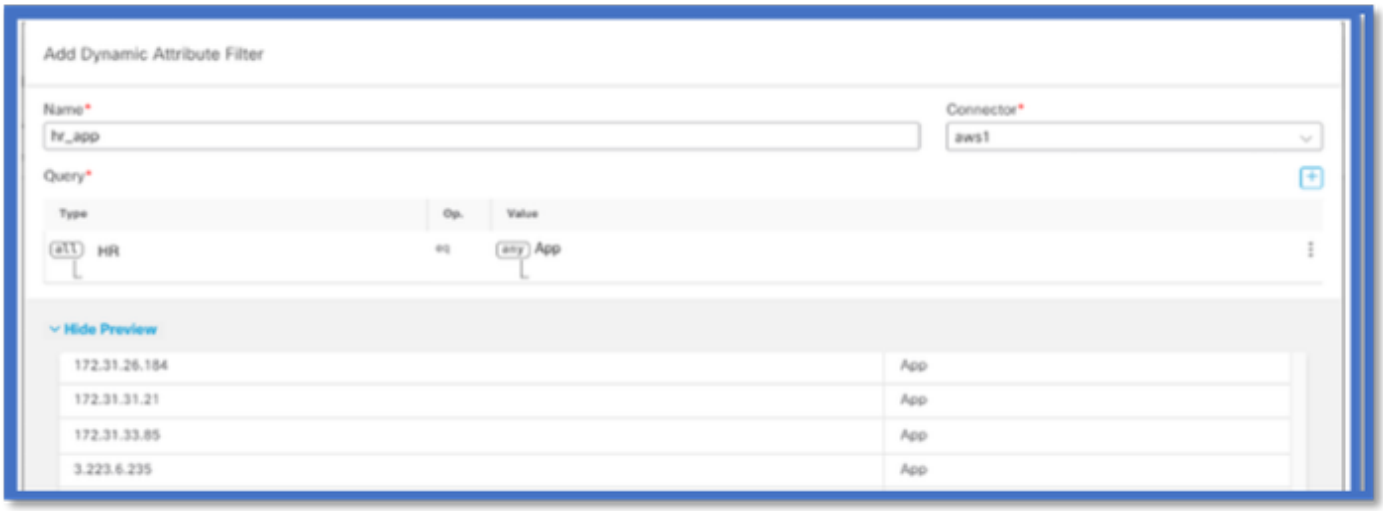
È possibile creare una regola "HR equals App" facendo clic sul pulsante +.

La scheda locale del CCP invierà gli indirizzi IP corrispondenti come mapping dinamici degli oggetti al CCP



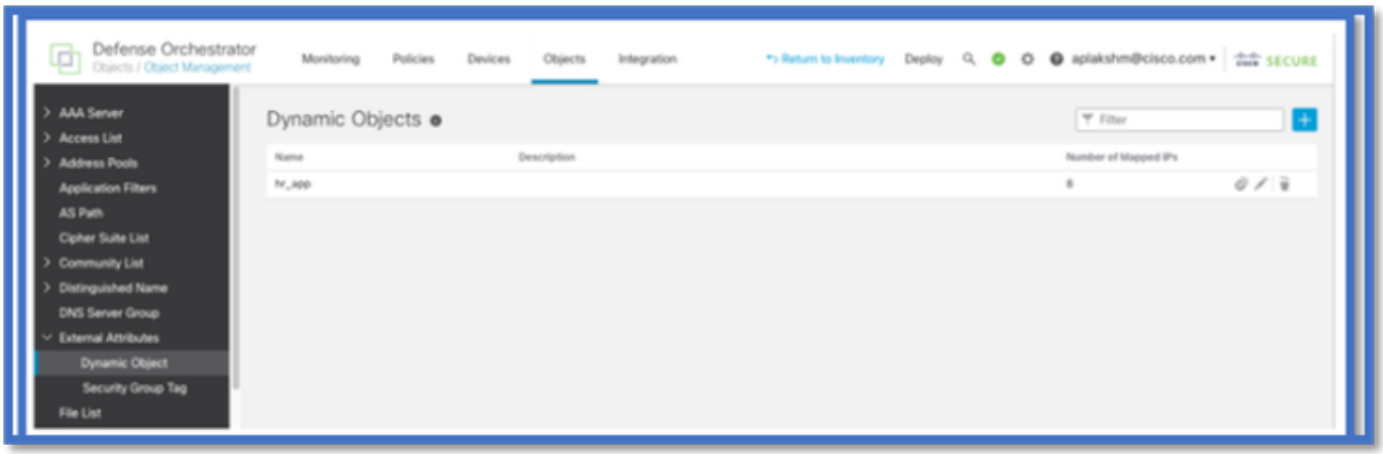
Anteprima

È inoltre possibile visualizzare gli indirizzi IP corrispondenti di una determinata regola dell'attributo facendo clic sul pulsante Mostra | Pulsante "Nascondi anteprima".



Oggetti dinamici

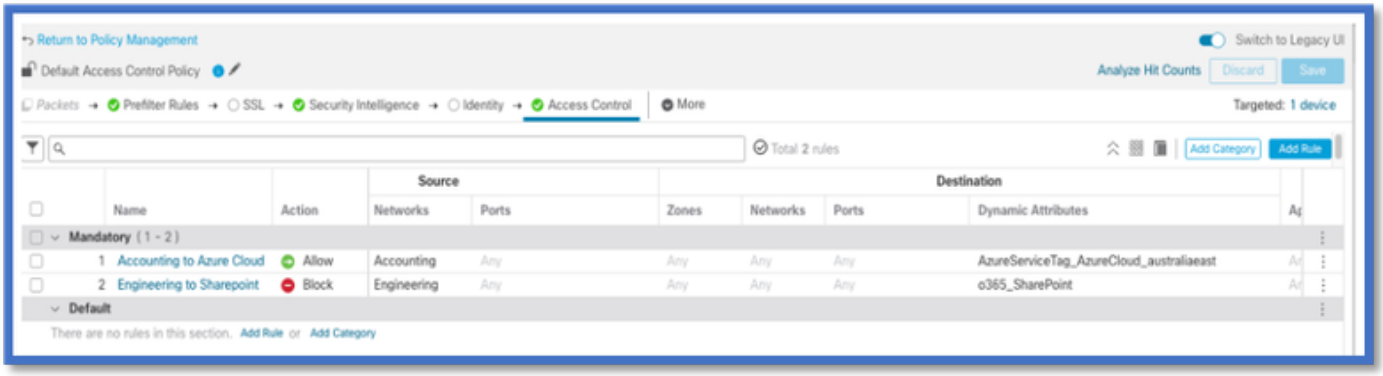
Visualizzare gli oggetti dinamici creati da CSDAC in Oggetti > Attributi esterni, Oggetto dinamico in FMC



Criterio AC

Configurazione: criteri di accesso

In FMC aggiungere criteri di accesso per consentire o bloccare gli oggetti dinamici ricevuti da Dynamic Attribute Connector.



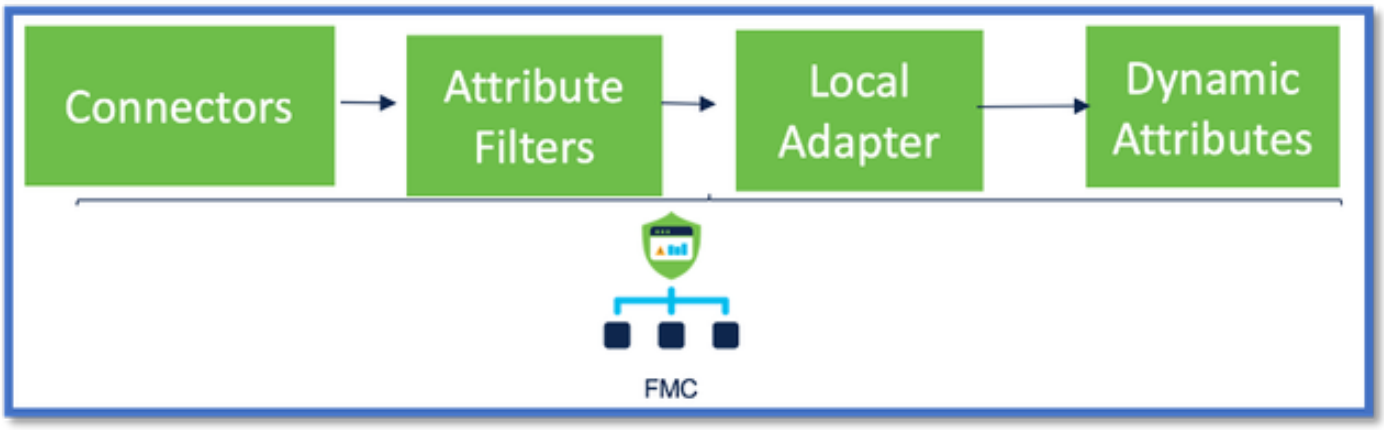
Limiti piattaforma

- I limiti dei connettori sono basati sulla memoria FMC disponibile.
- vFMC necessita di 1 GB di memoria in più per supportare 5 connettori
- Anche l'area di autenticazione di Azure AD è inclusa nel limite, in quanto è anche un contenitore CSDAC.

Modelli	N. di connettori supportati	Piattaforme	Limite basato sulla memoria
Base	Solo Azure AD	1600	32 GB
Piccole	5	vFMC	> 32 GB
Media	10	vFMC 300, 2600	>= 64 GB
Grande	20	4600	>= 128 GB

Risoluzione dei problemi/Diagnostica

La risoluzione dei problemi viene eseguita in modo ottimale tracciando gli oggetti dinamici dai connettori CSDAC agli attributi di Dynamics in FMC. Molti registri interni fanno riferimento a questa funzionalità come 'raccolta'. È possibile visualizzare lo stato del sistema lungo la catena di trasmissione per isolare i problemi. CSDAC utilizza contenitori Docker. I messaggi e i nomi dei registri e di altri file devono essere denominati "docker"



Controllare i connettori

Verificare innanzitutto che i connettori possano connettersi ai server vCenter, AWS o Azure.

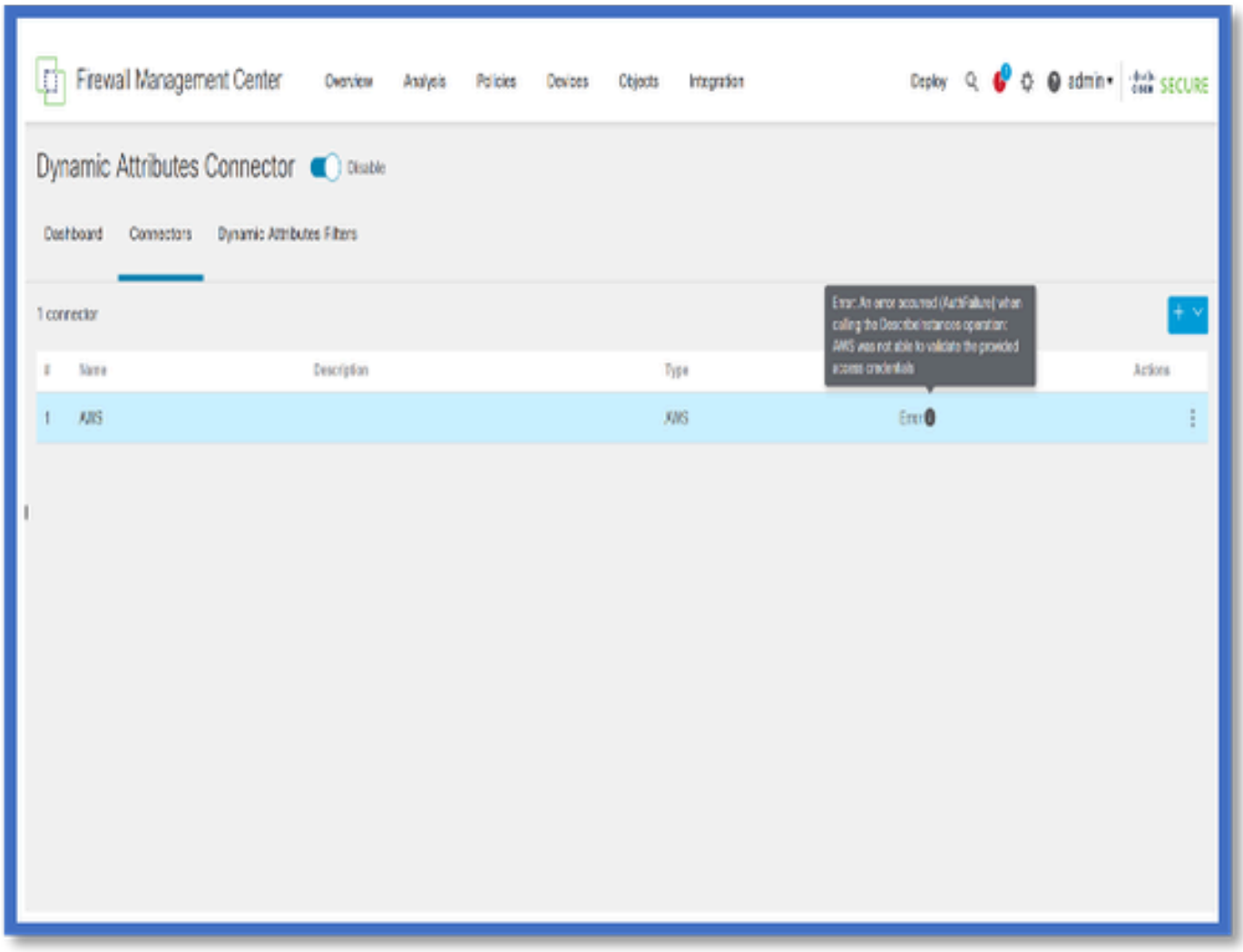
Se i connettori non sono configurati correttamente, i processi a valle non possono ottenere

informazioni sui tag.

Visualizzare i connettori dalla scheda Connettori

Lo stato del connettore viene visualizzato nel campo di stato e aggiornato ogni 15 secondi.

Il connettore non è stato in grado di eseguire l'autenticazione con le credenziali fornite.



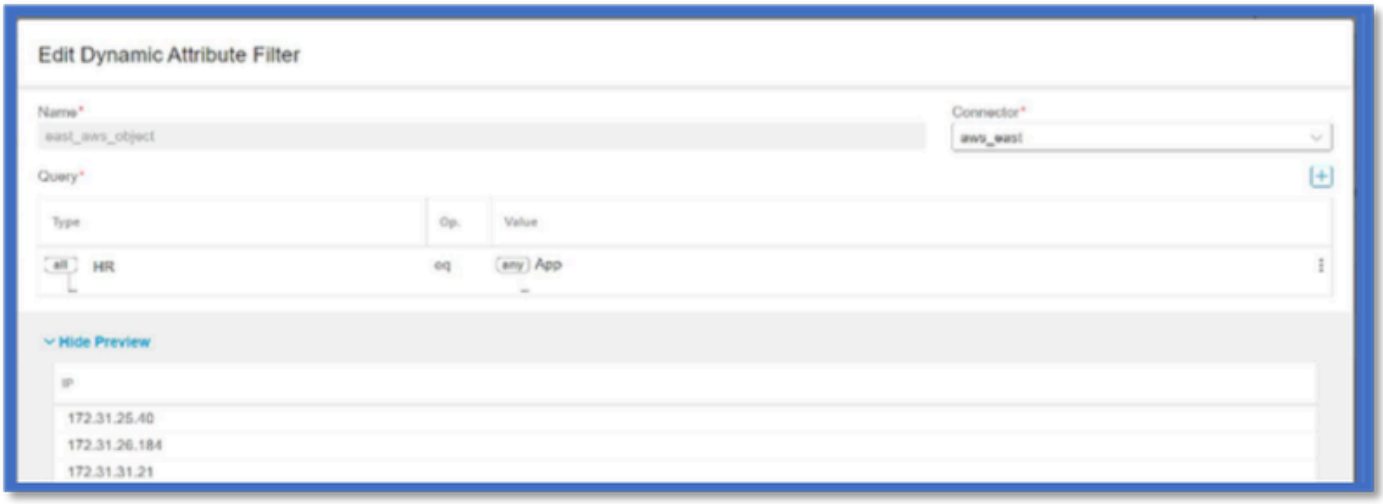
Controllare i filtri attributi

Verificare che nell'anteprima della regola siano visualizzati gli indirizzi IP corrispondenti alla condizione della query.

Se non esistono indirizzi IP corrispondenti, il servizio FMC non è in grado di ottenere le mappature dinamiche degli oggetti.

Controllo dei filtri attributi

Verificare che i mapping IP degli attributi dinamici siano disponibili in Anteprima. Il pulsante Mostra anteprima è disponibile nel popup di modifica del filtro attributi dinamici.



Controllare gli oggetti dinamici nell'interfaccia utente di FMC

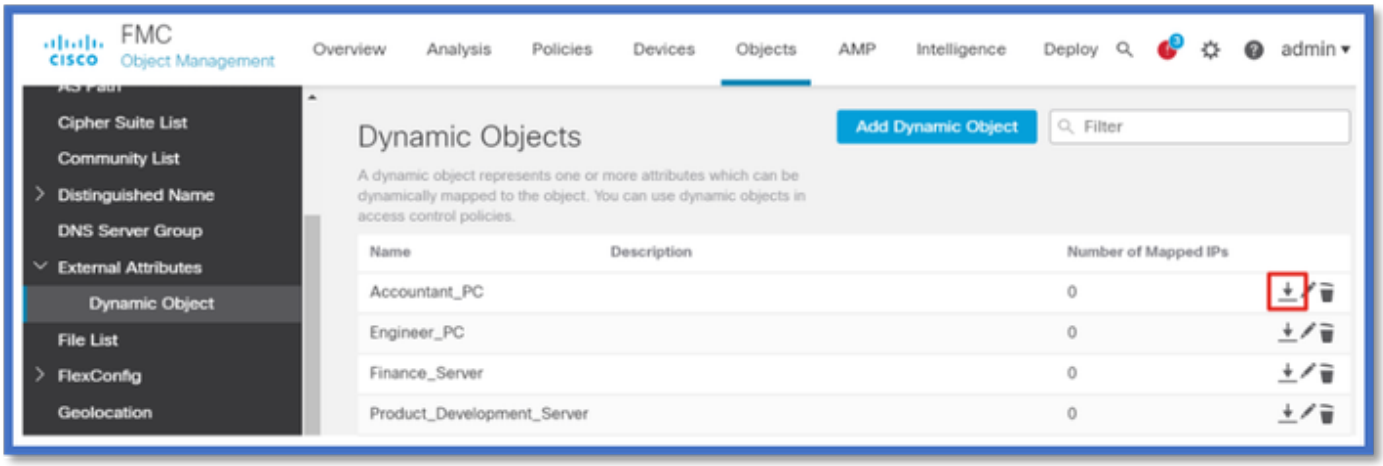
Verificare innanzitutto che il server FMC contenga i binding previsti.

- Nella scheda Oggetti esterni di Gestione oggetti verificare la presenza di associazioni negli oggetti dinamici.
- Se i binding non vengono ricevuti da FMC, FTD non è in grado di recuperarli.

Controllare gli avvisi e le notifiche di Health Monitor di Console Gestione configurazione server per gli avvisi sull'integrità CSDAC.

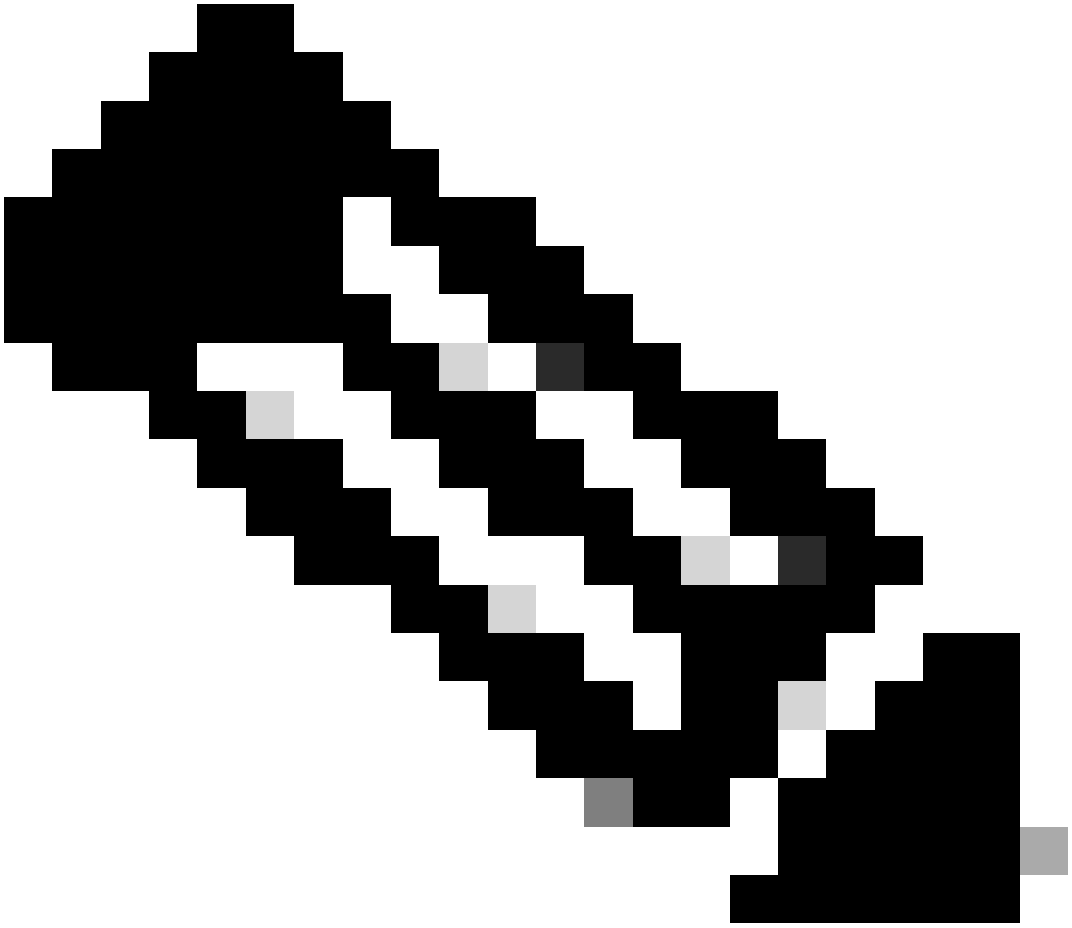
Controllo degli oggetti dinamici

FMC Object Manager consente di scaricare gli indirizzi IP correnti dell'oggetto dinamico.

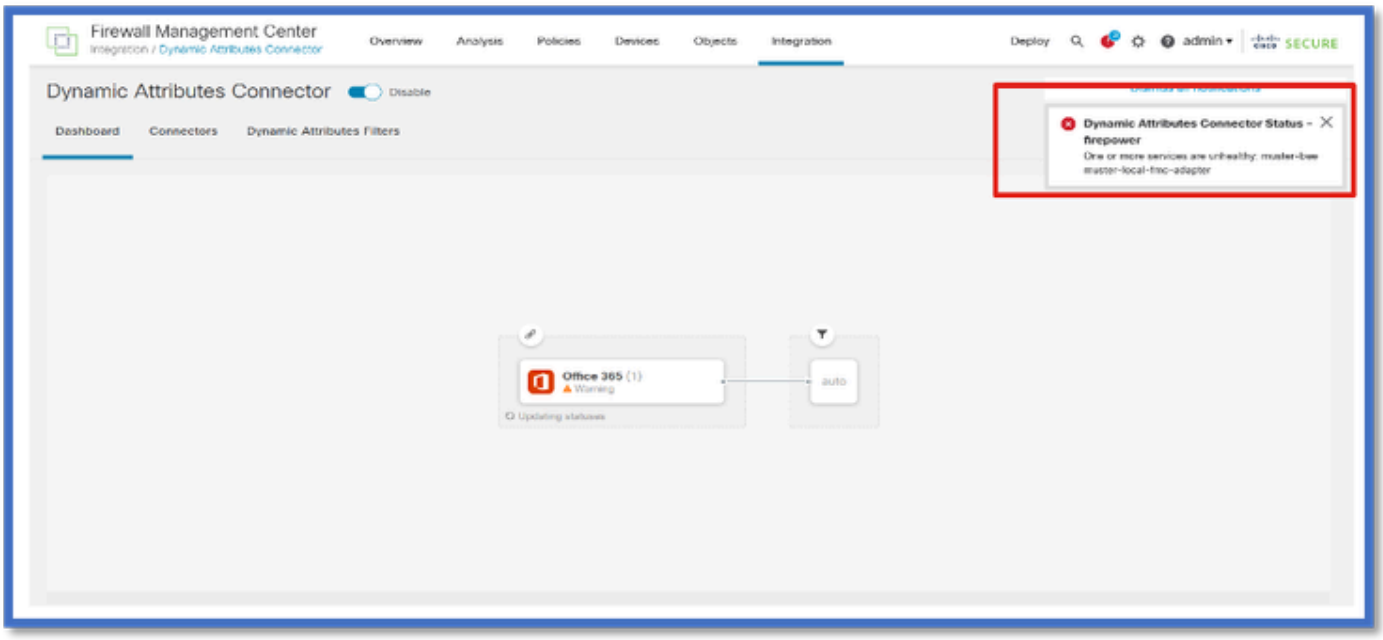


Avvisi sull'integrità CSDAC

In Gestione attività di FMC vengono visualizzati avvisi di integrità se un servizio di base, incluso il connettore degli attributi dinamici, è inattivo. L'avviso contiene informazioni relative al nome e allo stato del servizio.

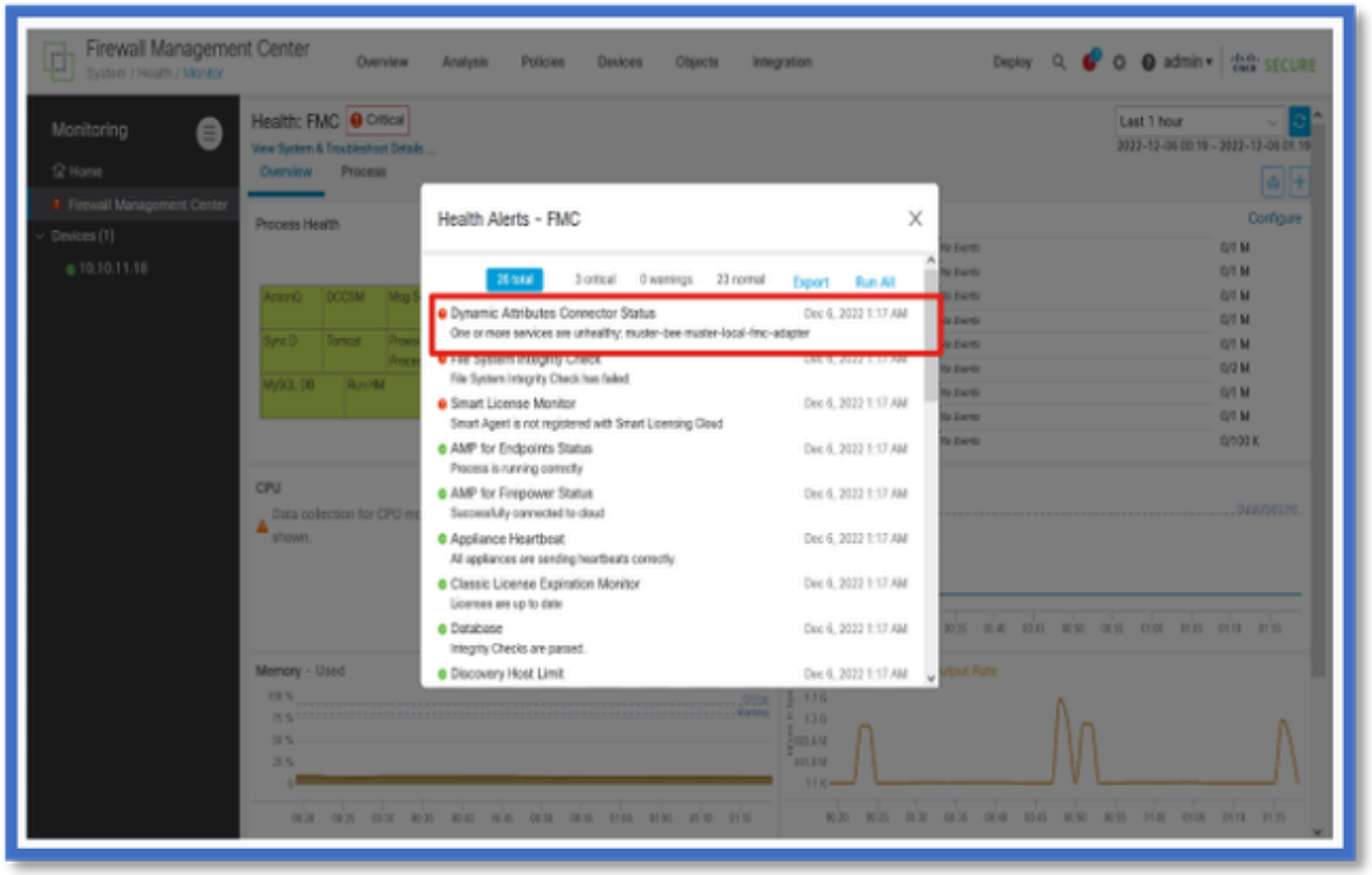


Nota: abbiamo ancora la denominazione "muster" in diverse notifiche ed è necessario qui per fornire il nome del servizio per informazioni dettagliate.



Qui vediamo che le api e gli adattatori locali-muster-fmc-non sono "sani".

Se l'errore indica uno dei servizi principali, è necessario raccogliere i log di risoluzione dei problemi per il debug.



CSDAC in Risoluzione dei problemi

Generazione di una risoluzione dei problemi CSDAC

- I registri CSDAC vengono raccolti automaticamente durante la generazione della risoluzione dei problemi FMC. Il bundle contiene lo stato del Docker, i registri e i dati necessari per eseguire il debug del problema offline.
- È buona norma abilitare la modalità di debug CSDAC prima di riprodurre l'errore per cui sono raccolti i log di risoluzione dei problemi.

Da /usr/local/sf/csdac chiamata ./muster-cli debug-on

Trova i registri CSDAC in Risoluzione dei problemi non risolti in queste cartelle:

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

Contiene i dati memorizzati nel database etcd.

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

Contiene i registri dai contenitori del docker.

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

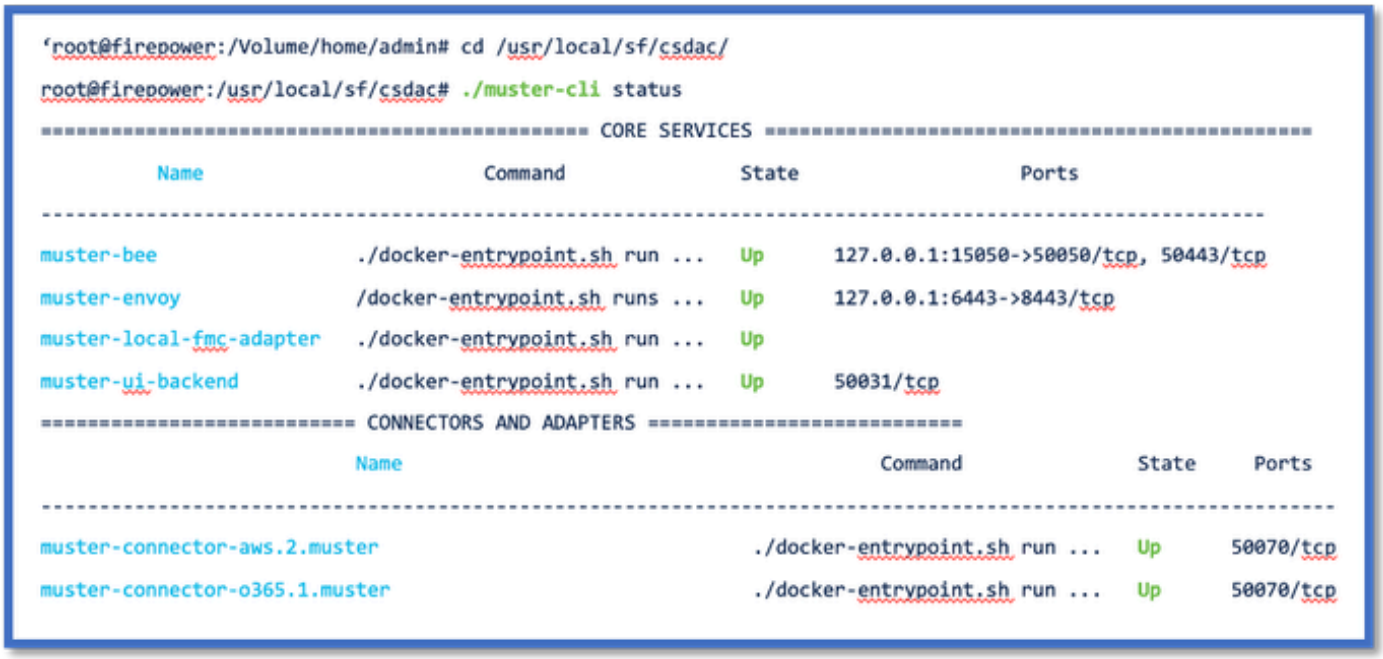
Mostra lo stato del contenitore, le versioni e i dettagli dell'immagine di ancoraggio.

Risoluzione dei problemi CLI

Lo script muster-cli può essere utilizzato per controllare lo stato di CSDAC dalla CLI di FMC.

Se lo stato di un servizio è "Exited" (Esci) o diverso da "Up" (Attivo), iniziare controllando i log relativi a tale contenitore.

Il nome del contenitore è necessario per ottenere i log; può essere ottenuto dall'output.



Modalità debug CSDAC

Lo script ‘muster-cli’ può essere usato per attivare e disattivare i log di debug.Per impostazione predefinita, i contenitori vengono registrati nella directory INFO level.INFO e DEBUG sono gli unici livelli supportati.

Per abilitare il comando DEBUG level user: ./muster-cli debug-on.

Fornisce ulteriori informazioni per la risoluzione dei problemi di generazione e per il debug.È necessario abilitare questa opzione durante la riproduzione di un problema.

Per tornare al livello INFO utilizzare: ./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
```

Messaggi registrati con debug

Quando la modalità di debug è attivata, tutti i log del contenitore del docker contengono anche i messaggi di debug

Ottenere i log in tempo reale utilizzando i comandi docker: docker logs -f <nome_contenitore>

Nell'esempio seguente, il messaggio di debug mostra la causa che ha causato l'errore 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
```

Esempio di problema con la risoluzione dei problemi Procedura dettagliata

Panoramica della risoluzione dei problemi

Problema:

Il problema più comune è che FMC non riceve tutte le mappature dinamiche degli oggetti.

Risoluzione dei problemi:

Per risolvere il problema,

- Abilitare la modalità di debug da "muster-cli"
- File generato per la risoluzione dei problemi dall'interfaccia utente di FMC
- Dopo aver verificato che il connettore CSDAC AWS ha eseguito l'accesso, è stata raccolta la risoluzione dei problemi.
- È stato rilevato che CSDAC AWS Connector ha richiesto solo il primo indirizzo IP nelle istanze di AWS.

Preparazione pacchetto di risoluzione dei problemi

- Dalla CLI di FMC è stata abilitata la modalità di debug con ./muster-cli debug-on. lo strumento muster-cli è disponibile in /usr/local/sf/csdac.
- Il problema è stato rigenerato attendendo che lo stato del connettore sia OK e quindi controllando i filtri degli attributi dinamici.
- Registri per la risoluzione dei problemi raccolti dall'interfaccia utente di FMC e estratti.Per il contenuto dello snapshot, controllare i registri del connettore AWS

Esaminare gli attributi del tag per un indirizzo IP

Gli attributi di tag per un determinato IP vengono registrati nei log di risoluzione dei problemi. Per il connettore AWS, abbiamo preso in considerazione muster-connector-aws.1.muster-docker.log.gz

Riepilogo dei controlli

Lo stato di Connettore e scheda è corretto?

Verificare gli stati nelle pagine Connettore, Scheda corrispondenti.

I connettori hanno ricevuto tutte le mappature?

Verificare che gli indirizzi IP corrispondano nell'anteprima della regola.

Controllare i registri del docker Connector per verificare se sta eseguendo correttamente una query sui mapping.

Il server REST ha ricevuto mapping di tag dinamici dal connettore?

Controllare la pagina Oggetti dinamici di FMC.

Controllare i registri USMS (in /opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log) per verificare se il server REST FMC ha elaborato correttamente la richiesta API da CSDAC.

Domande e risposte

D: Quale versione di CSDAC locale supporta un connettore ISE? Non vedo questo tipo di connettore neanche nella versione 7.4.0 (build 1494)?

R: Questa opzione è disponibile in CSDAC autonomo e non in FMC o CDO. Per verificarla, è necessario un pacchetto eseguibile CSDAC.

D: Quando rilasciato, quale versione CSDAC locale sarebbe?

R: Probabilmente 2.1.0.

D: È stato mostrato uno schermo con un ingranaggio dotato di API. Penso che sia il CSDAC; cosa significa?

R: API explorer è incorporato in questo CSDAC. Da questa pagina è possibile effettuare chiamate API a CSDAC.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).