FMC에서 보안 동적 특성 커넥터 구축

목차

소개

이 문서에서는 FMC의 Cisco Secure Dynamic Attribute Connector에 대해 설명합니다.

배경 - 문제

CSDAC(Cisco Secure Dynamic Attributes Connector)는 FMC(Firepower Management Center)에 통합되어 CDO의 독립형 CSDAC 애플리케이션 및 CSDAC와 동일한 수준의 기능을 제공할 수 있습니다. 독립형 CSDAC의 경우, CSDAC를 위한 별도의 머신을 관리하고 유지 보수하는 오버헤드에서 고객이 안심할 수 있습니다. 네트워크 관리자로서 프로그래밍 방식의 인터페이스를 손쉽게 통합하고 외부 동적 환경 제공자의 변경 사항을 최신 상태로 유지하고자 합니다. 이러한 통합으로 정책을 구축하지 않고도 동적으로 변화하는 클라우드 환경에서 속성을 수집할 수 있는 문제가 해결됩니다.

솔루션(요약)

이제 CSDAC를 FMC에서 구성하여 Azure, vCenter, AWS, GCP, Office 365 및 Azure Service Tags에서 태그 특성을 가져올 수 있으며, CDO의 독립형 CSDAC 및 CSDAC와 기능 패리티를 제공합니다.

- 이제 다음을 사용하도록 선택할 수 있습니다
  - FMC의 CSDAC(또는)
  - CDO의 CSDAC(또는)
  - 독립형 CSDAC
- 대상 시장: 대기업, 서비스 공급자

FMC 요약의 동적 특성 커넥터

FMC 동적 특성 커넥터:

- Dashboard(대시보드) 화면에서 Dynamic Attribute Connector 기능을 구축하고 운영할 수 있습니다.
- 소스 워크로드 커넥터(AWS, Azure, vCenter, Office 365, GCP)를 구성하기 위한 FMC UI
- 동적 개체를 만들기 위해 동적 특성 필터를 정의하는 FMC UI

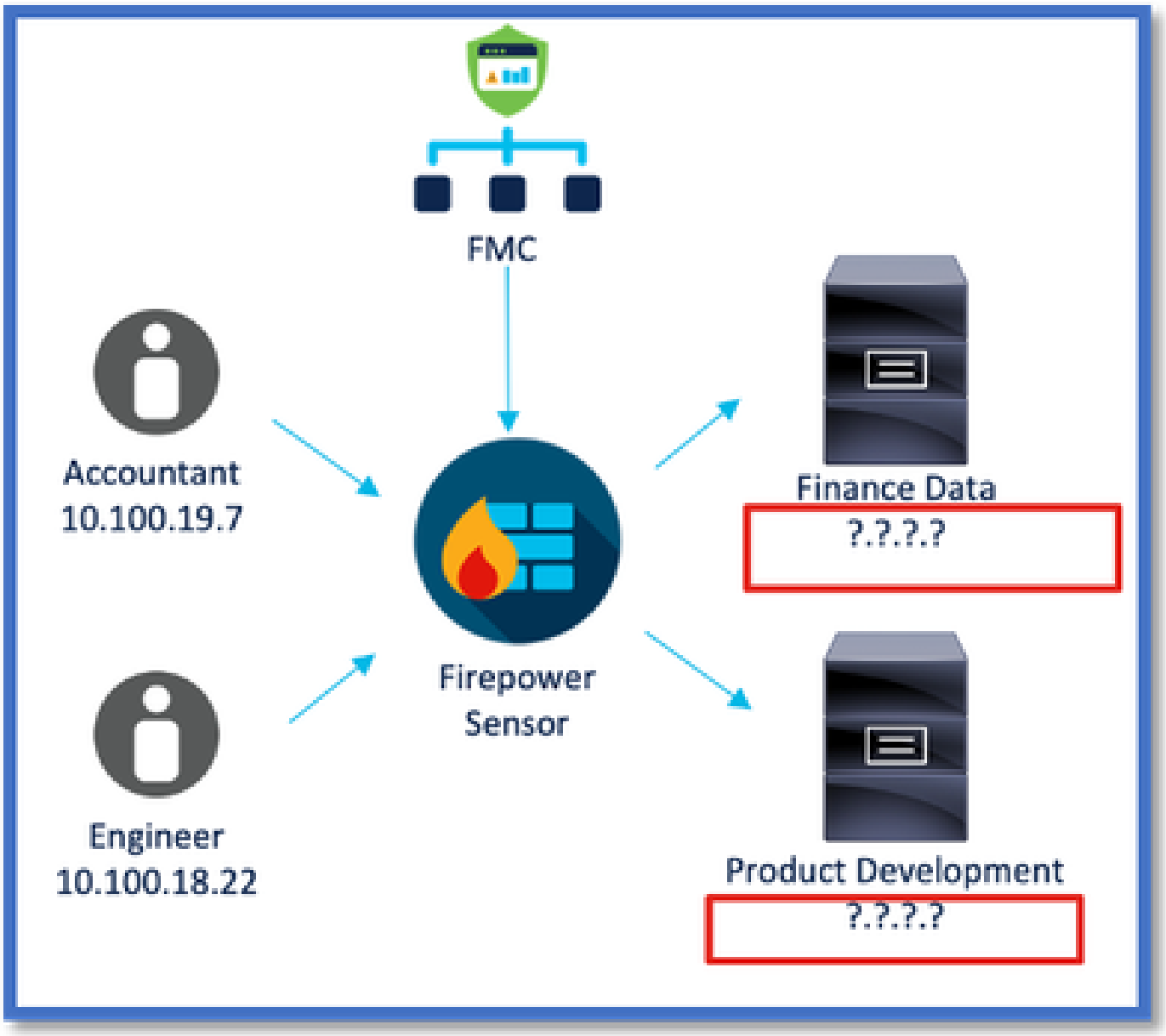
구축 예

온프레미스 CSDAC

작년에 CSDAC용 전용 VM을 배포하여 AWS 및 Azure 계정에서 특성을 수집했습니다.

문제

이제 우리 조직은 클라우드로 이전했으며, 내 환경에서는 CSDAC용 전용 가상 머신을 구축하고 관리할 수 없습니다.



옵션 1: FMC 내부에 구축된 동적 특성 커넥터 사용

FMC에 내장된 동적 특성 커넥터를 사용하여 문제를 해결할 수 있습니다. 여기에서 생성한 동적 객체를 액세스 정책에서 사용할 수 있습니다.

옵션 2: CDO에서 클라우드 제공 Dynamic Attributes 커넥터 사용

CDO에서 Dynamic Attributes Connector를 사용하여 문제를 해결할 수 있습니다. 생성된 동적 개체를

- CDO 클라우드 제공 FMC

- CDO 온프레미스 FMC

사전 요구 사항, 지원되는 플랫폼, 라이센싱

최소 지원 소프트웨어 및 하드웨어 플랫폼

지원되는 최소 관리자 버전	관리되는 디바이스	최소 지원 관리되는 디바이스 버전 필요	참고
FMC 7.4	지원되는 모든 FTD	모든 7.0+ FTD	

* FDM 관리 디바이스에서는 동적 특성 커넥터가 지원되지 않습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.
· Cisco Firewall Management Center 실행 7.4
· Cisco Firepower Threat Defense 7.4 이상
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

기능 세부사항

독립형 CSDAC 개요(현재 릴리스 - 7.4)

Cisco Secure Dynamic Attributes Connector를 사용하면 FMC(Firewall Management Center) 액세스 제어 규칙에서 다양한 클라우드 서비스 플랫폼의 태그를 사용할 수 있습니다.

On-Prem CSDAC는 Linux 시스템에 설치할 수 있으며 다음에서 특성 가져오기를 지원합니다.

- AWS,Azure,VMware vCenter 및 NSX-T,Office 365,Azure 서비스 태그,GCP,GitHub.

CDO 개요의 CSDAC(현재 릴리스 - 7.4)

전용 애플리케이션을 설치 및 유지 관리할 필요 없이 온프레미스 CSDAC와 동일한 기능을 지원합니다.

vCenter 커넥터는 현재 CDO에서 지원되지 않습니다.

수신된 특성을 CDO의 클라우드 제공 FMC 및 온프레미스 FMC로 전송하도록 지원합니다.

FMC의 CSDAC

전용 애플리케이션을 설치 및 유지 관리할 필요 없이 독립형 CSDAC와 동일한 기능을 지원합니다.

FMC의 CSDAC는 다음에서 특성 가져오기를 지원합니다.

- AWS,Azure,VMware vCenter 및 NSX-T,Office 365,Azure 서비스 태그,GCP,GitHub

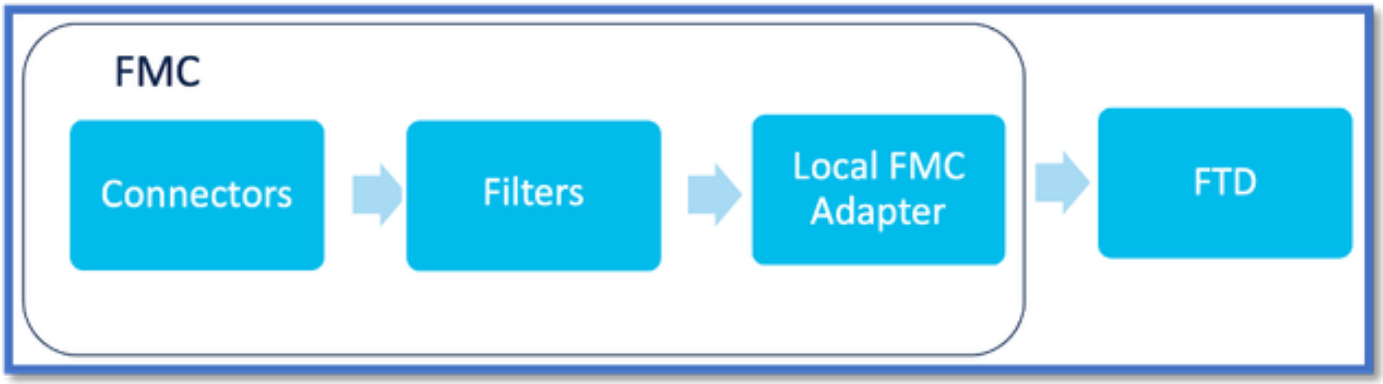
FMC에 로컬이므로 여기에 명시적 어댑터 컨피그레이션이 없습니다.

운영 방식

커넥터는 AWS, Azure, o365, vCenter에서 특성을 가져오는 데 사용됩니다.

그런 다음 로컬 어댑터를 사용하여 이러한 간소화된 특성과 해당 IP 매핑을 FMC에 동적 객체로 저장합니다.

FMC는 매핑 실시간 정보를 FTD로 전송합니다(구축 없음).



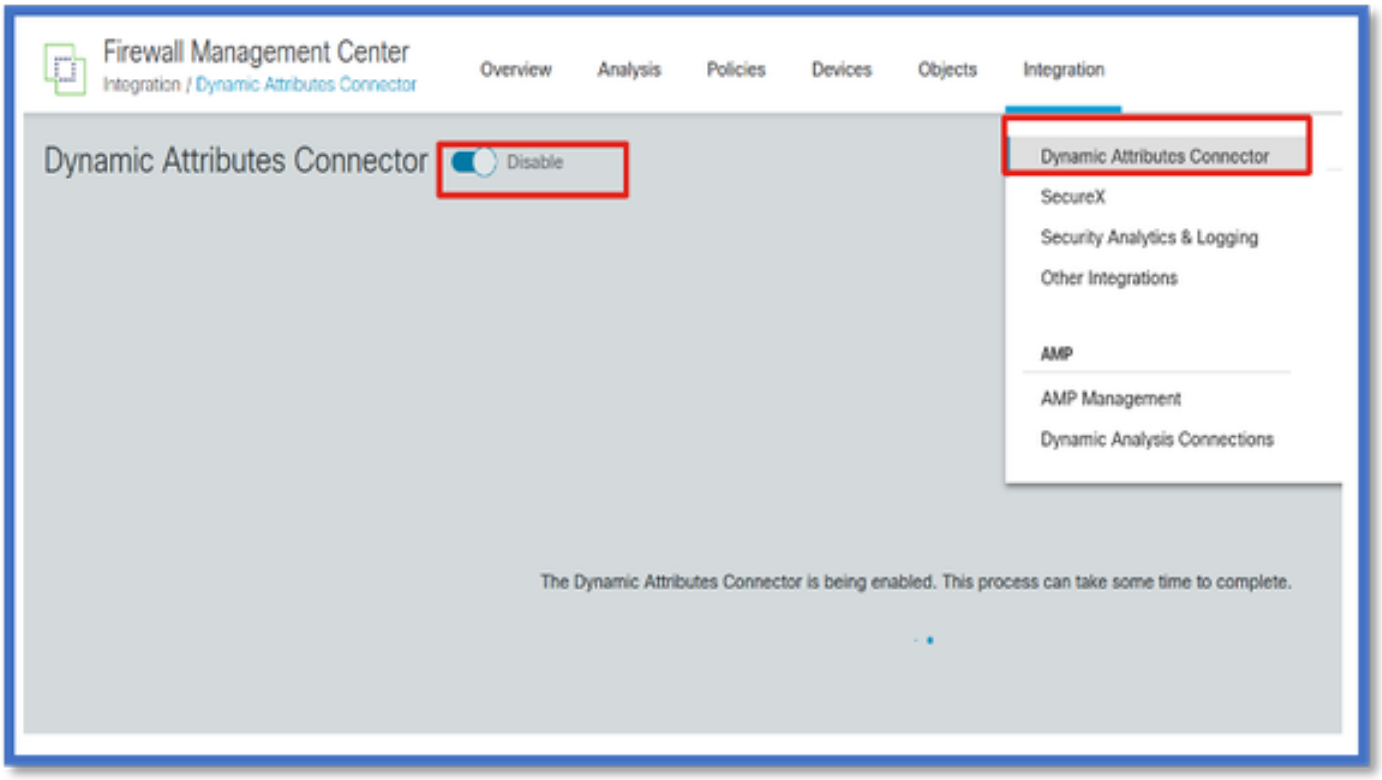
FMC에서 CSDAC 사용

Integration(통합) > Dynamic Attributes Connector로 이동합니다.

Toggle(토글) 버튼을 사용하여 커넥터를 활성화합니다.

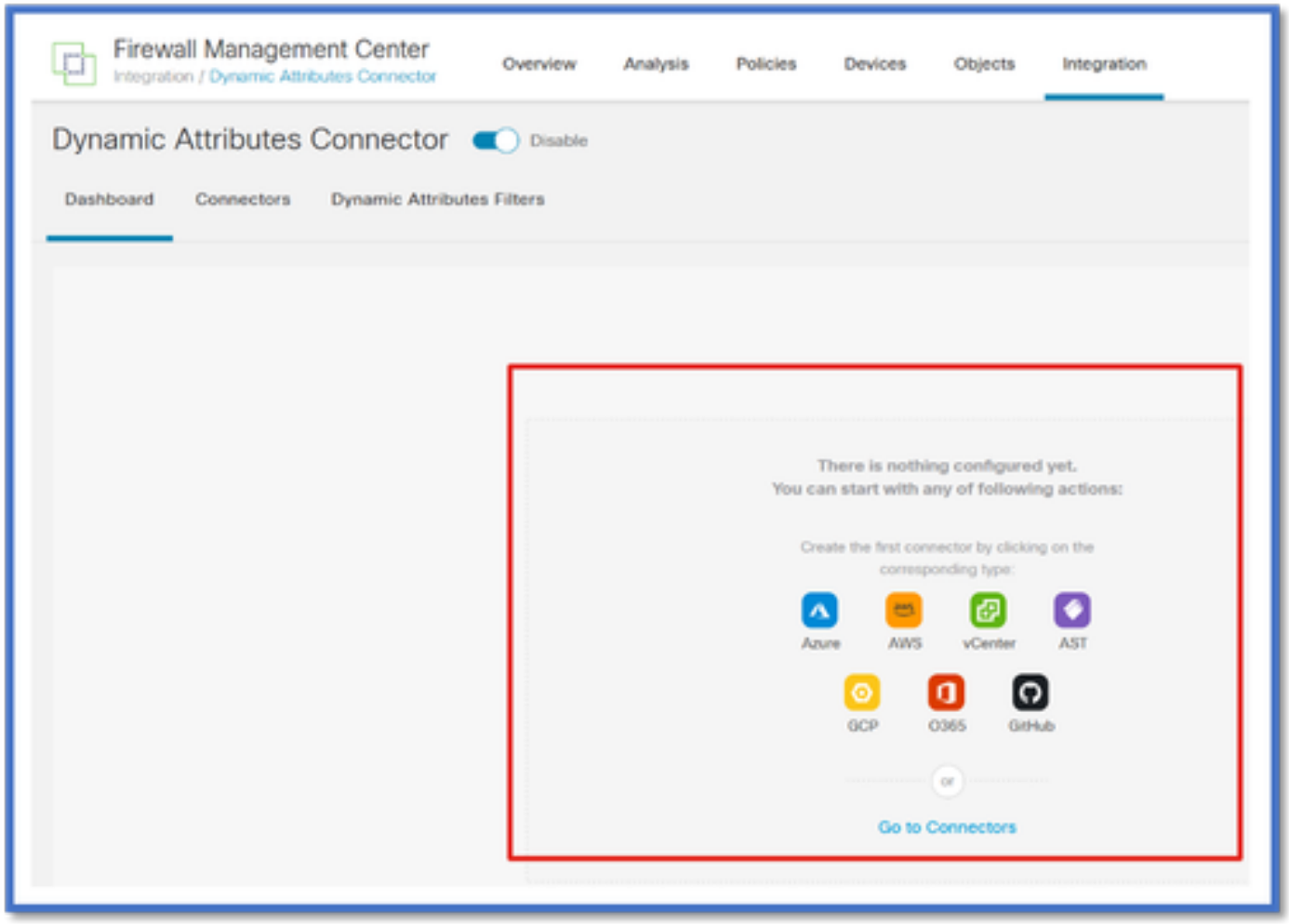
FMC는 docker 이미지 및 컨테이너를 다운로드하고 가져오는 데 몇 분 정도 소요됩니다.

이는 FMC 전역 도메인에서만 구성할 수 있습니다.



CSDAC 대시보드

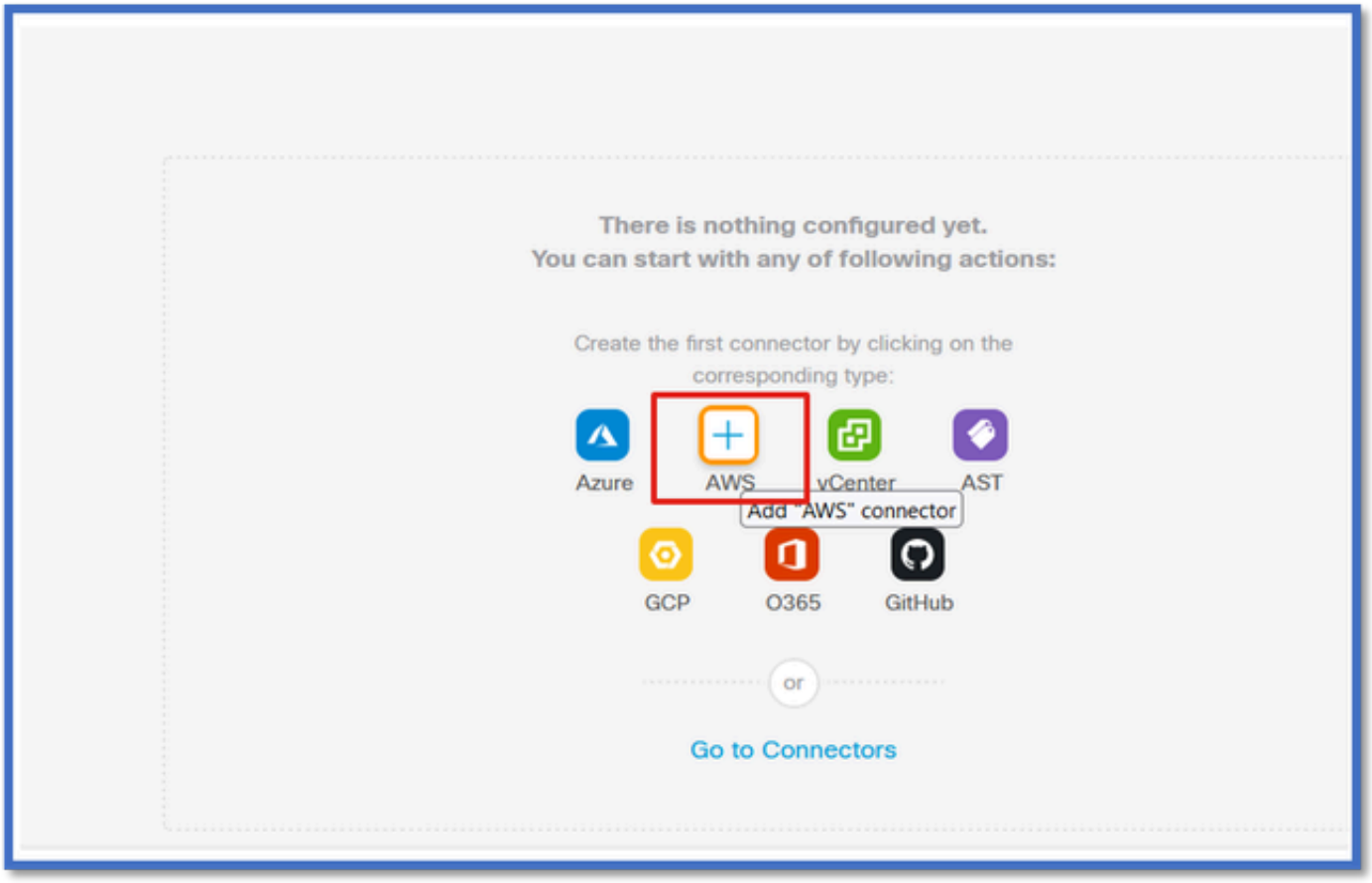
CSDAC를 활성화하면 사용자에게 CSDAC Dashboard(CSDAC 대시보드) 페이지가 표시됩니다. 대시보드는 통합된 커넥터 및 필터를 구성하고 확인하는 데 사용됩니다.



커넥터 구성

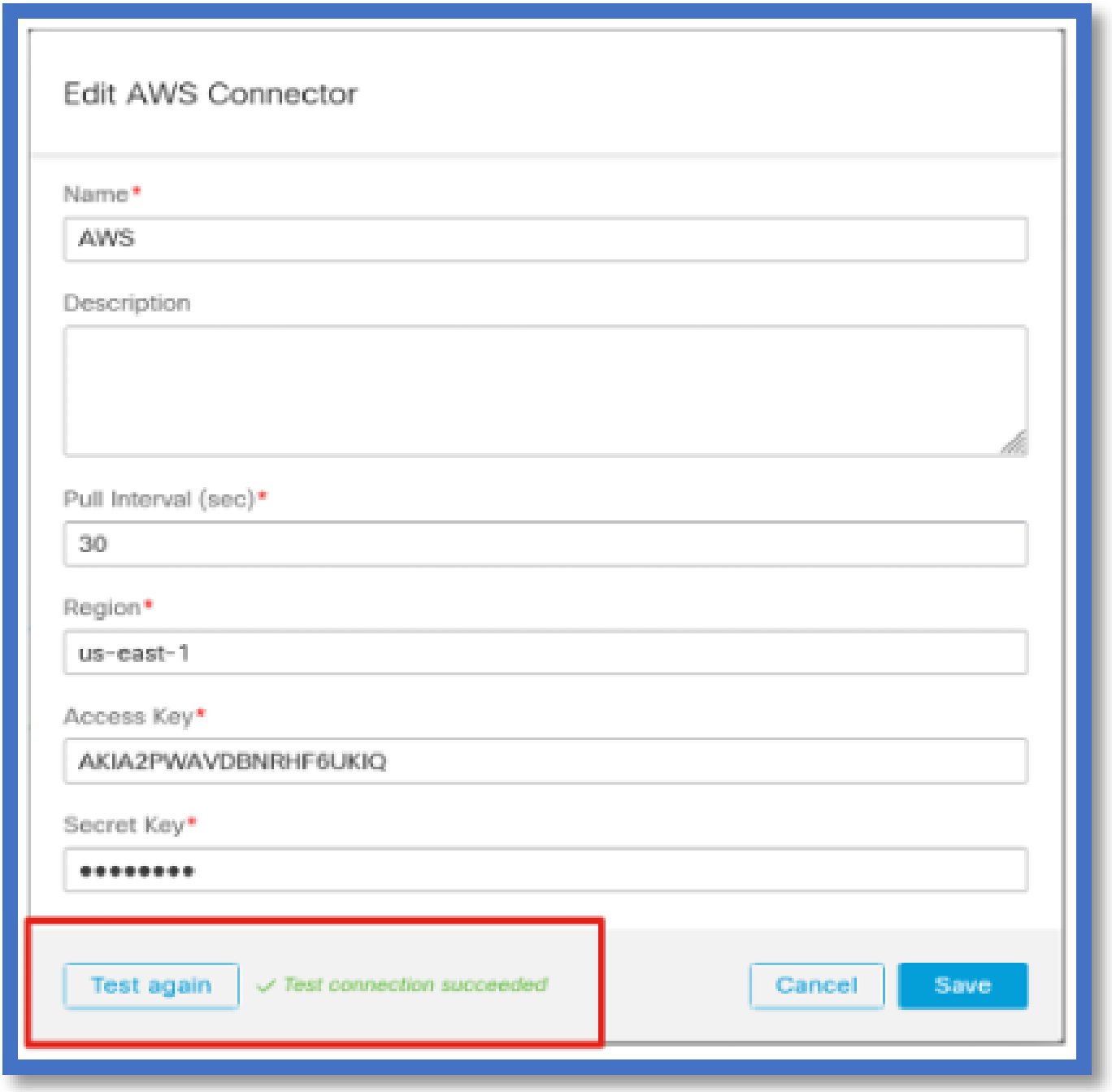
대시보드에서 커넥터 추가

Dashboard(대시보드)에서 원하는 커넥터의 아이콘을 클릭하여 추가합니다.



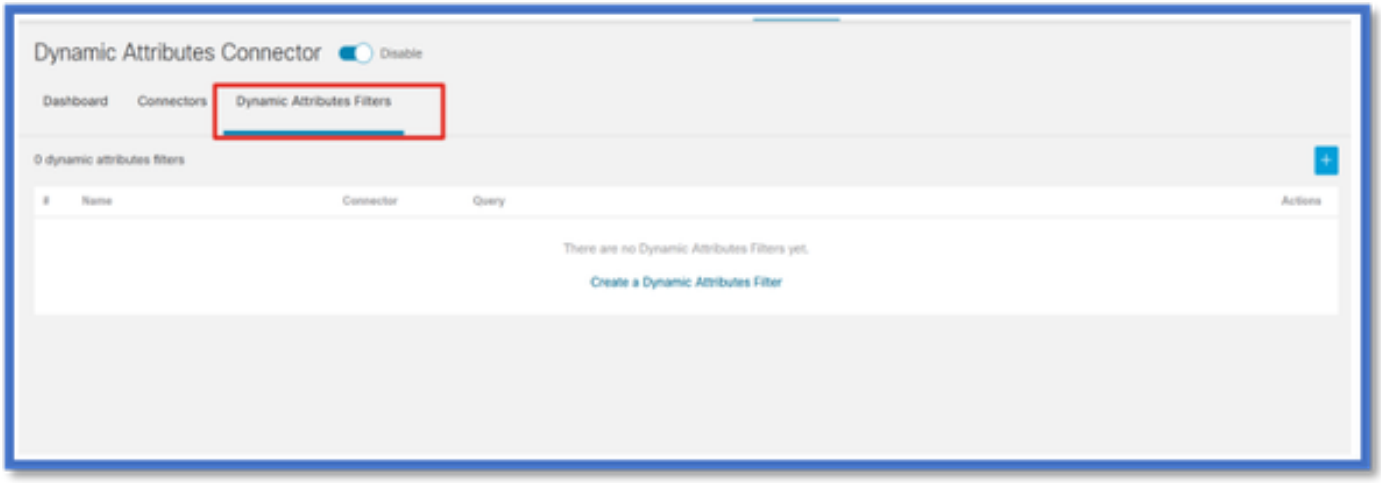
커넥터가 구성된 주기성을 가진 공급자로부터 정보를 가져올 수 있도록 Pull Interval 필드에 시간 간격을 구성합니다.

태그 특성을 가져올 공급자 자격 증명을 입력합니다. 커넥터를 구성했으면 Test Button(테스트 버튼)을 클릭하여 커넥터를 테스트할 수 있습니다.



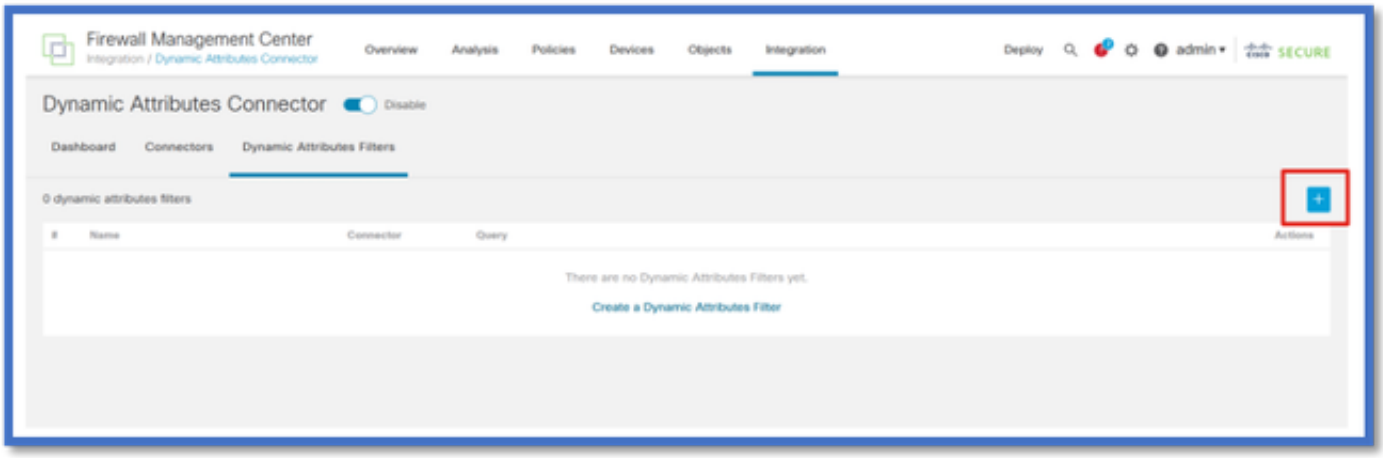
필터 구성

"Dynamic Attributes Connector" 메뉴의 "Dynamic Attribute Filters" 탭을 클릭하여 Dynamic Attributes Filters 페이지로 이동합니다.



필터 추가

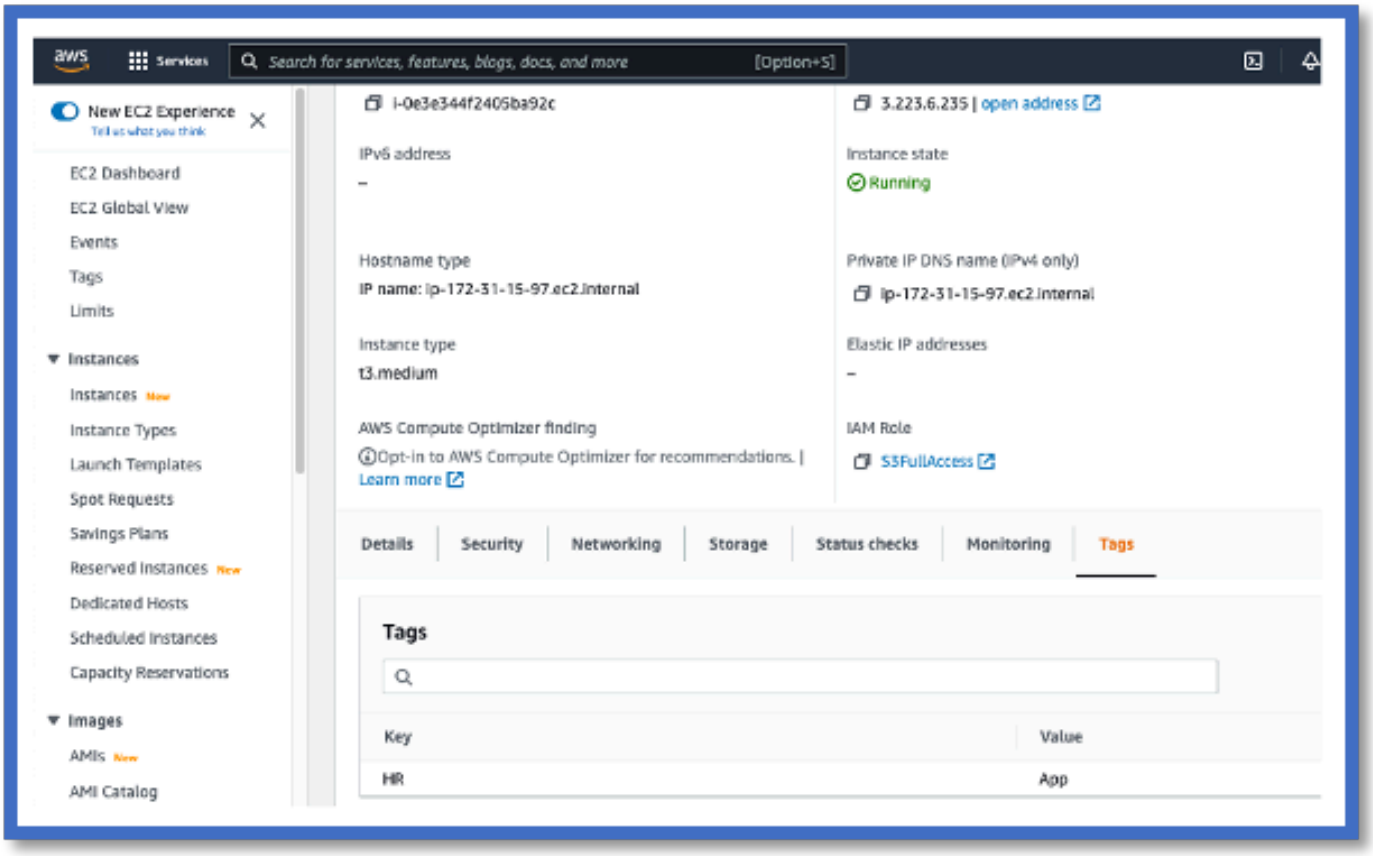
+ 버튼을 클릭하여 특성 커넥터에 대한 필터를 생성합니다.



AWS 태그 추가

예를 들어, AWS 워크로드의 핵심 'HR' 및 가치 'App'에 관심이 있다고 가정할 수 있습니다.

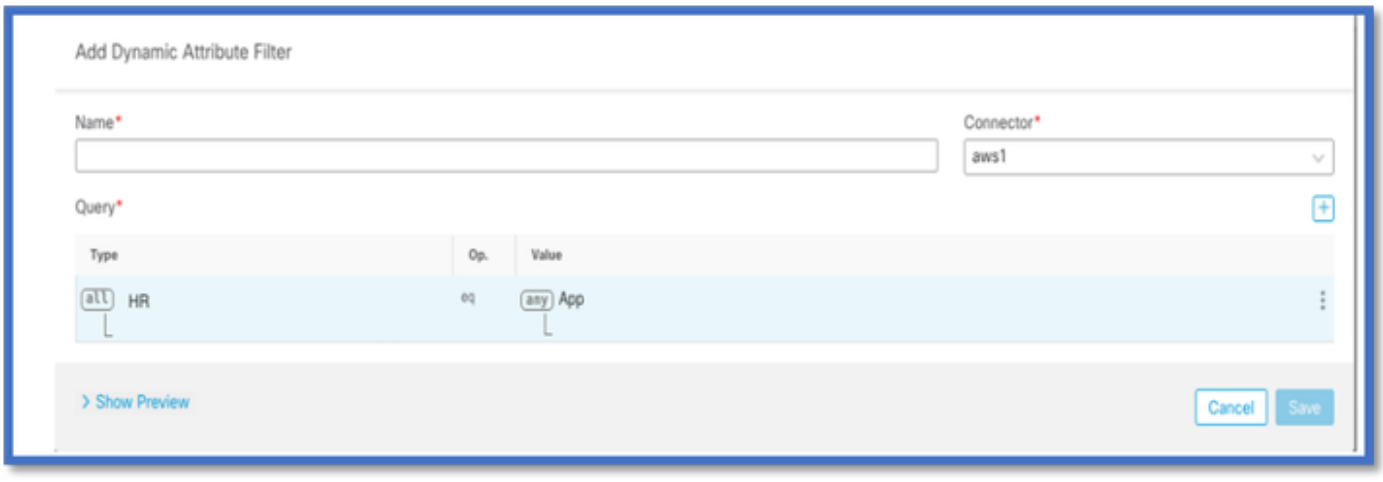
이것이 AWS의 모습입니다.



FMC의 CSDAC

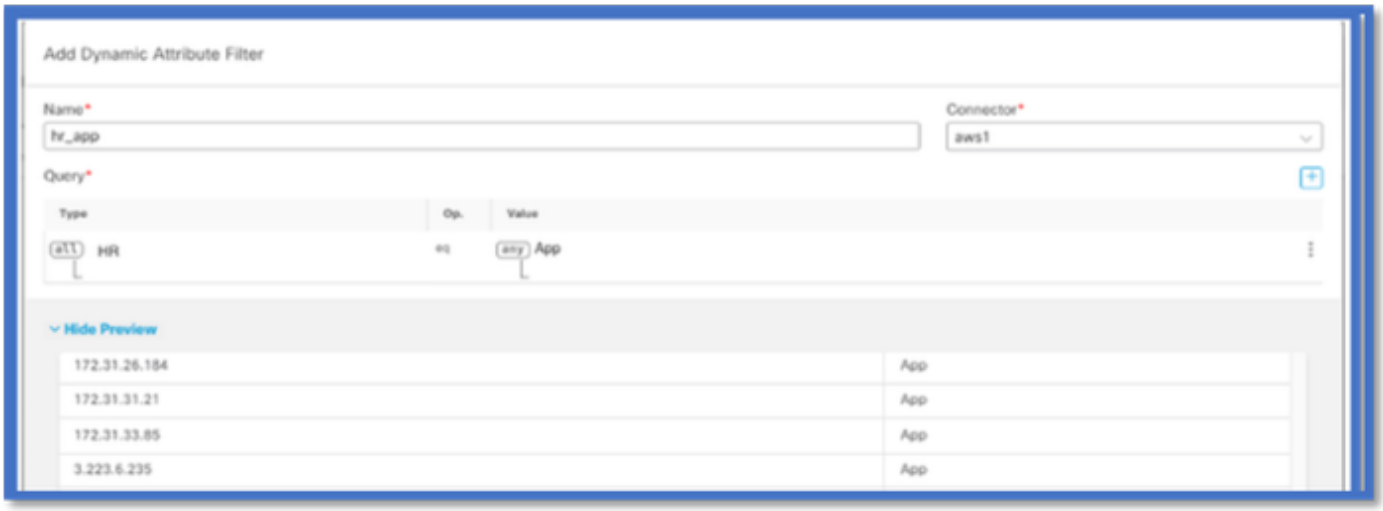
+ 버튼을 클릭하여 'HR equals App' 규칙을 생성할 수 있습니다.

로컬 FMC 어댑터는 일치하는 IP 주소를 FMC에 동적 개체 매핑으로 전송합니다



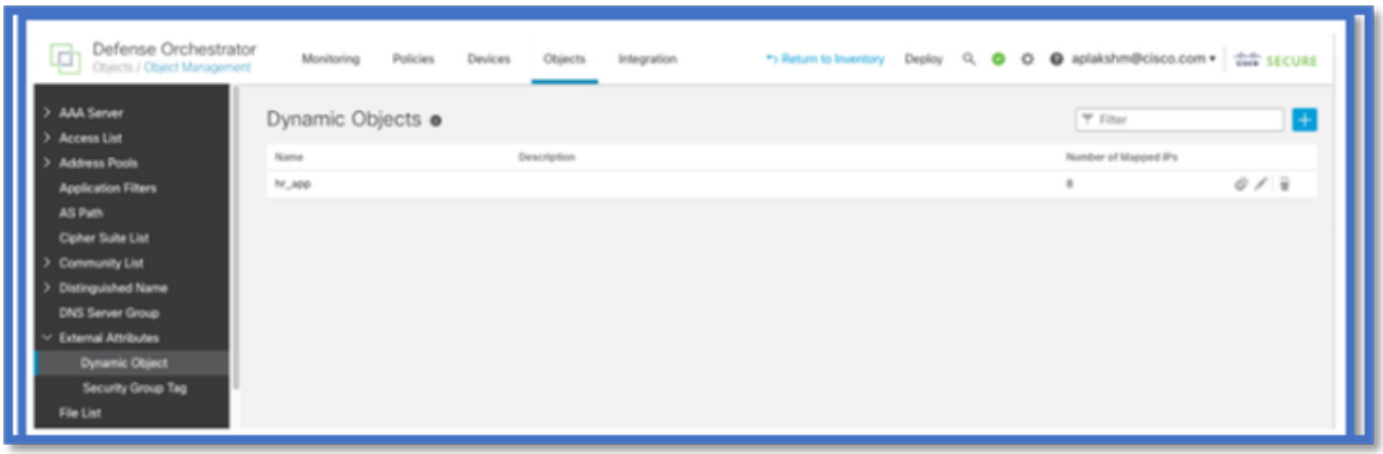
미리보기

'Show(표시)'를 클릭하여 특정 특성 규칙의 일치하는 IP 주소를 볼 수도 있습니다 | 미리보기 숨기기' 버튼



동적 개체

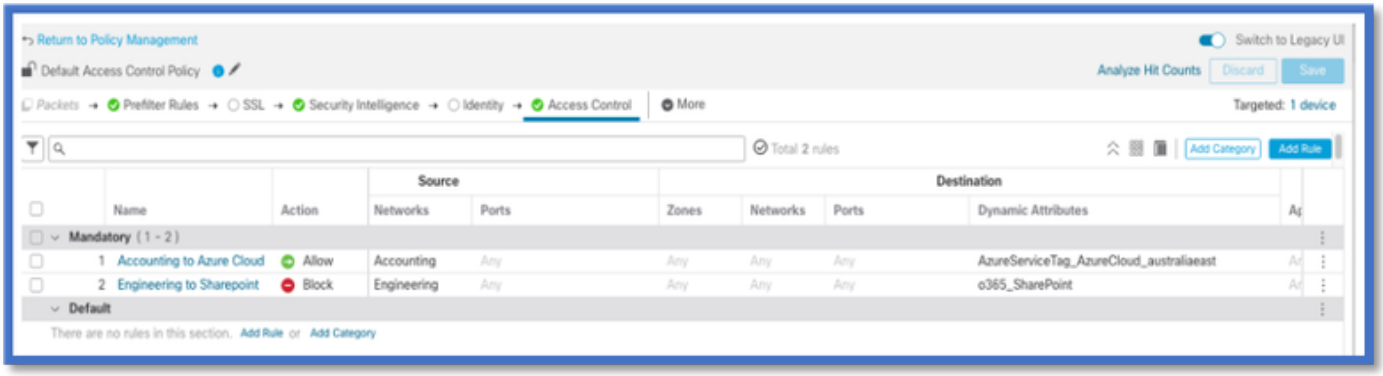
Objects(개체) > External Attributes(외부 특성), FMC의 Dynamic Object(동적 개체)에서 CSDAC에 의해 생성된 동적 개체를 봅니다.



AC 정책

컨피그레이션: 액세스 정책

FMC에서 Dynamic Attribute Connector에서 수신된 동적 객체를 허용하거나 차단하기 위한 액세스 정책을 추가합니다.



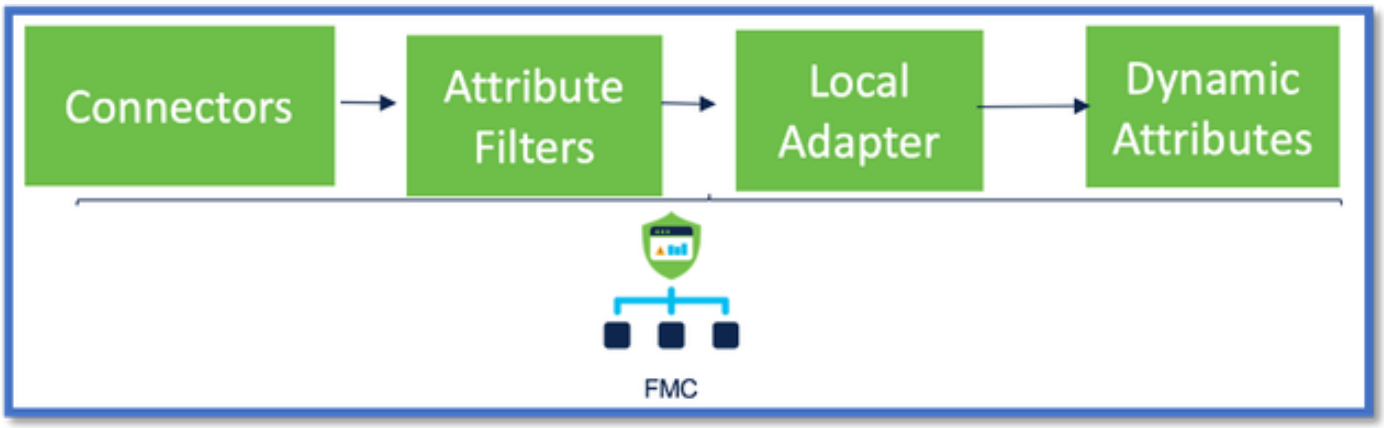
플랫폼 제한

- 커넥터 제한은 사용 가능한 FMC 메모리를 기반으로 합니다.
- vFMC는 5개의 커넥터를 지원하려면 추가 1GB 메모리가 필요합니다.
- 또한 CSDAC 컨테이너이므로 Azure AD 영역도 제한에 포함됩니다.

모델	지원되는 커넥터 수	플랫폼	메모리 기준 제한
기본	Azure AD만	1600	32GB
소형	5	vFMC	> 32GB
중간	10	vFMC 300, 2600	>= 64GB
크게	20	4600	>= 128GB

문제 해결/진단

트러블슈팅은 CSDAC 커넥터에서 FMC의 Dynamics 특성으로 동적 개체를 추적하여 수행하는 것이 가장 좋습니다.많은 내부 로그에서 이 기능을 'muster'로 참조합니다. 브로드캐스트 체인을 따라 시스템 상태를 미리 확인하여 문제를 격리할 수 있습니다. CSDAC는 Docker 컨테이너를 사용합니다. 로그 및 기타 파일의 메시지 및 이름은 "docker"로 참조해야 합니다.



커넥터 확인

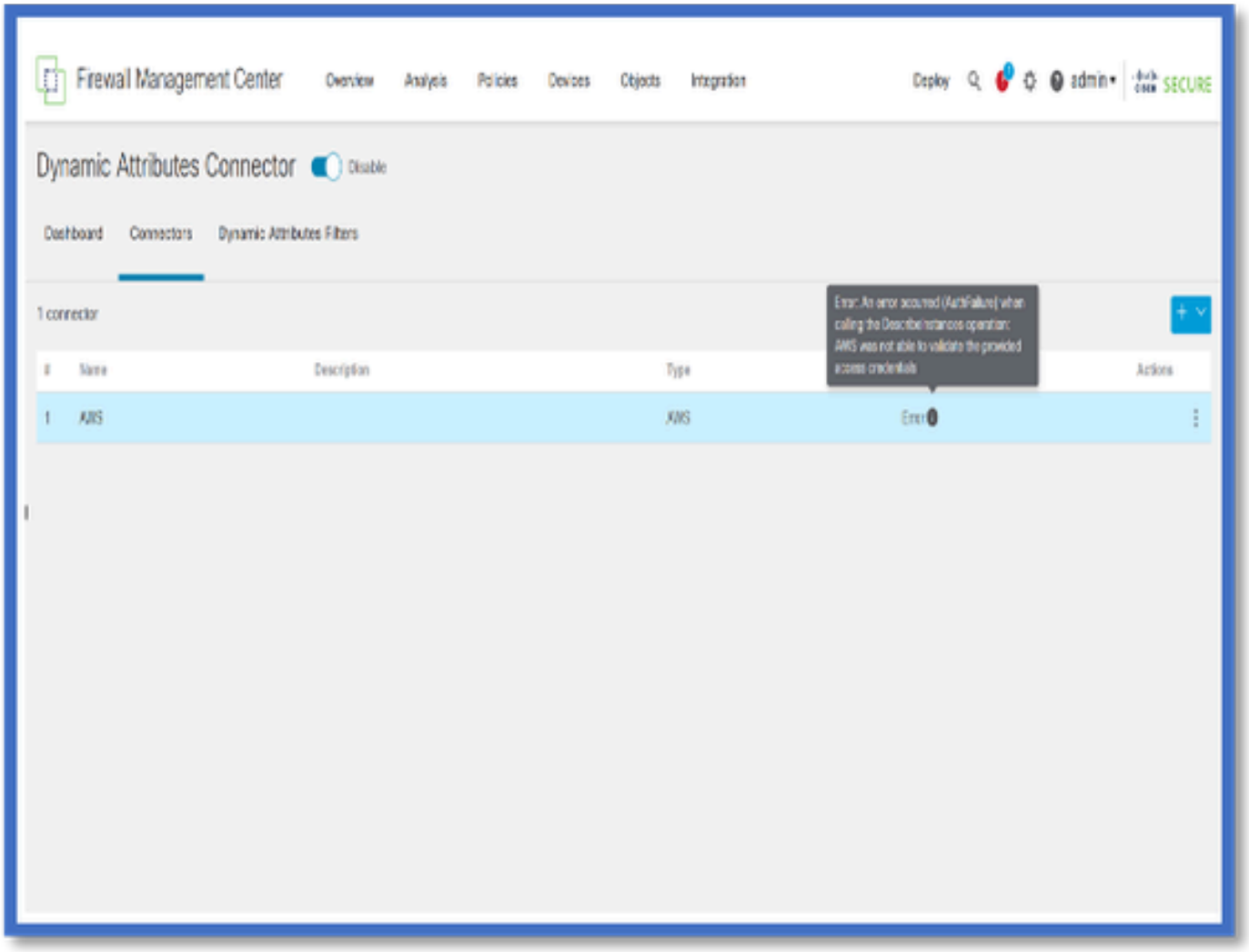
먼저 Connector가 vCenter, AWS 또는 Azure 서버에 연결할 수 있는지 확인합니다.

Connector가 올바르게 구성되지 않으면 다운스트림 프로세스에서 태그 정보를 가져올 수 없습니다
.

커넥터 탭에서 커넥터 보기

커넥터 상태는 상태 필드에 표시되며 15초마다 업데이트됩니다.

여기서는 커넥터가 제공된 자격 증명을 사용하여 인증할 수 없음을 확인합니다.



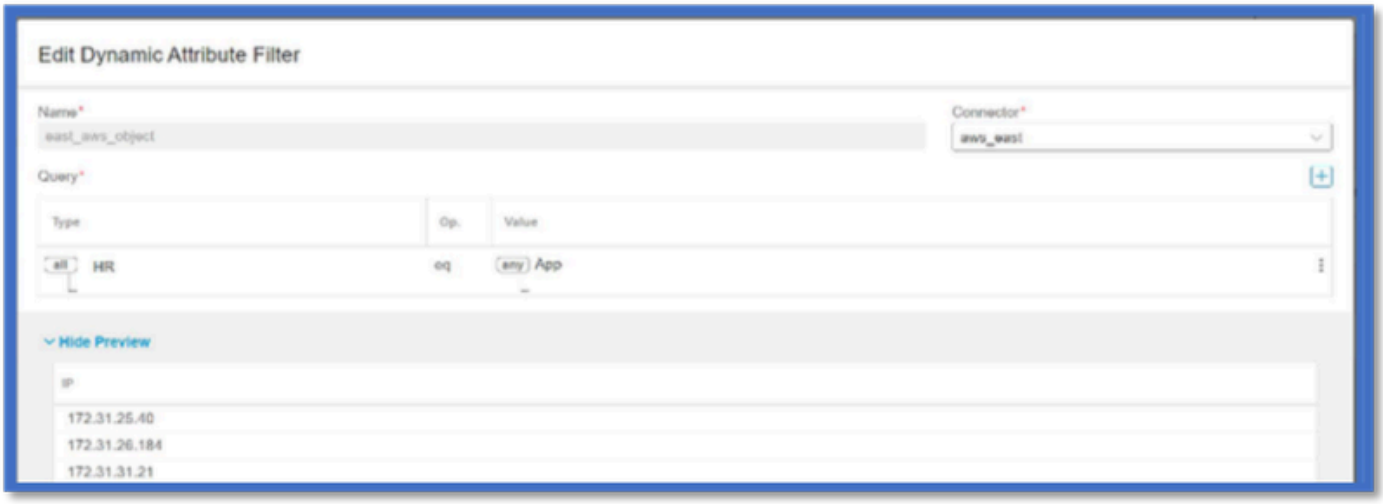
특성 필터 확인

Rule preview(규칙 미리 보기)에 쿼리 조건에 대해 일치하는 IP 주소가 표시되는지 확인합니다.

일치하는 IP 주소가 없는 경우 FMC는 동적 개체 매핑을 가져올 수 없습니다.

속성 필터 확인

Preview(미리 보기)에서 Dynamic Attribute IP(동적 특성) 매핑을 사용할 수 있는지 확인합니다. Show preview(미리 보기 표시) 버튼은 Dynamic Attribute Filter edit(동적 특성 필터 수정) 팝업에서 사용할 수 있습니다.



FMC UI에서 동적 개체 확인

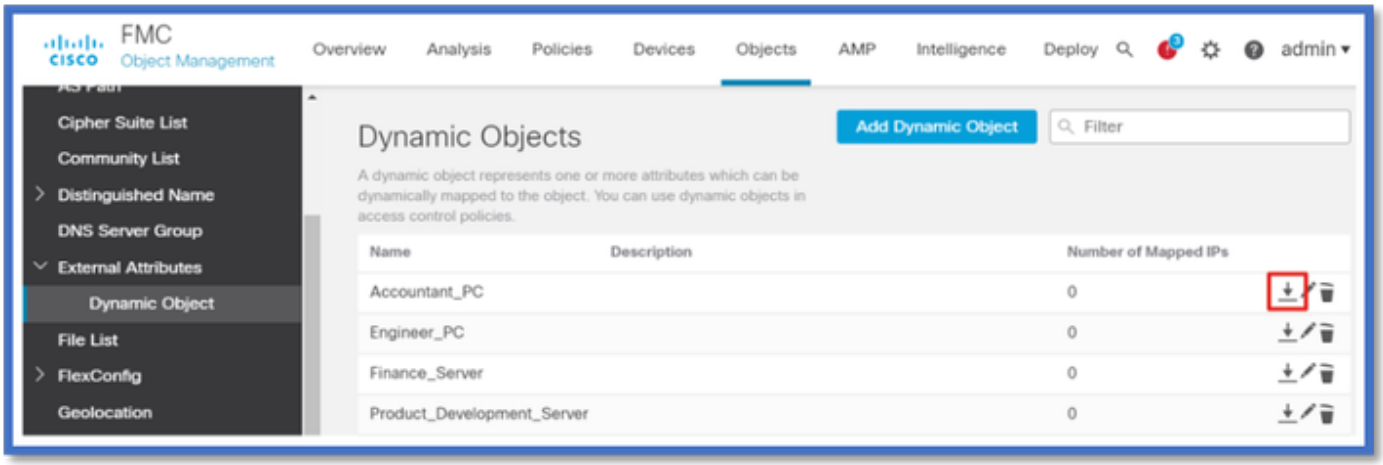
먼저 FMC 서버에 필요한 바인딩이 포함되어 있는지 확인합니다.

- Object Management(개체 관리), External Objects(외부 개체) 탭 아래에서 Dynamic Objects for bindings(동적 개체)를 확인합니다.
- FMC에서 바인딩을 가져오지 않으면 FTD에서 바인딩을 가져올 수 없습니다.

CSDAC 상태 알림에 대한 FMC 상태 모니터 및 알림을 확인합니다.

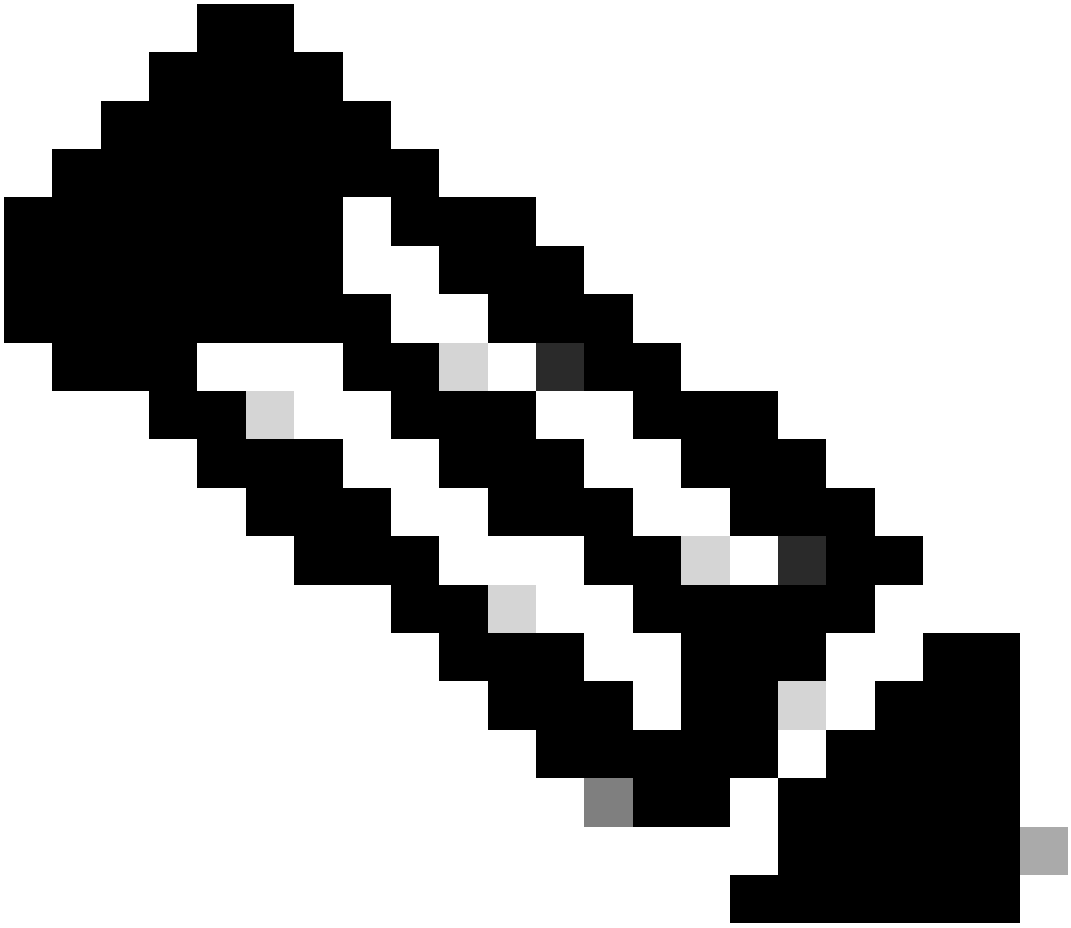
동적 객체 확인

FMC Object Manager에서는 현재 동적 개체 IP 주소를 다운로드할 수 있습니다.

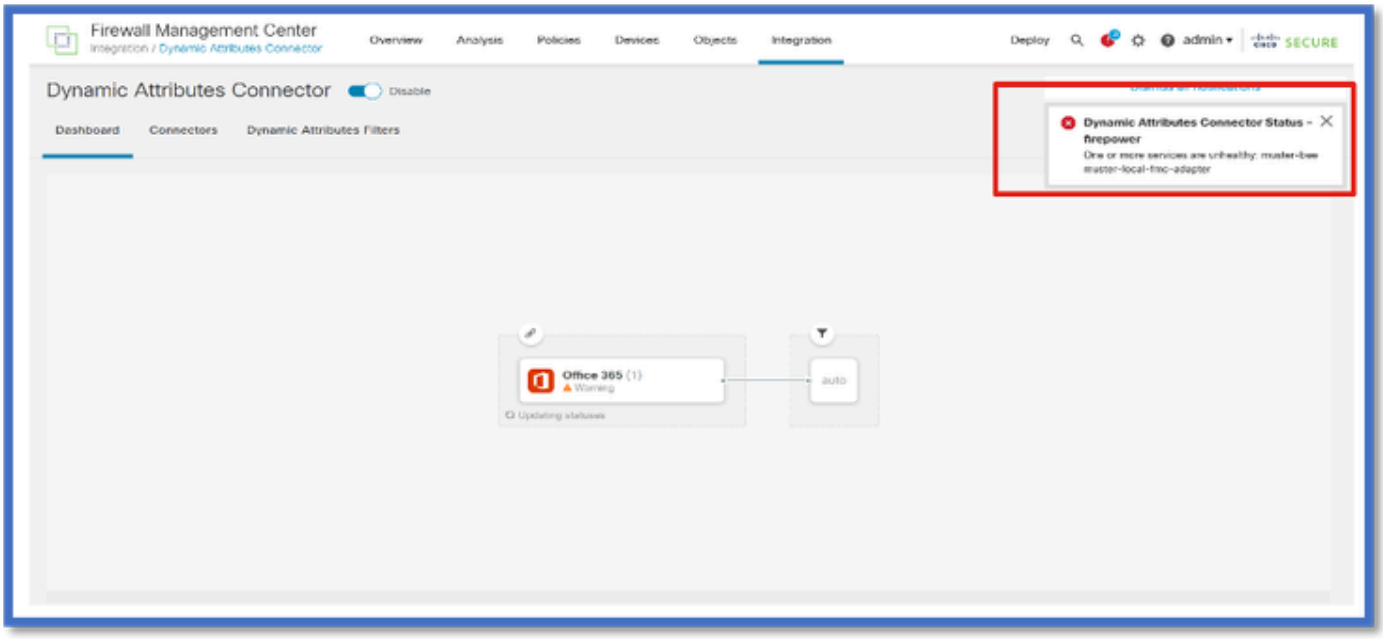


CSDAC 상태 알림

VMC의 Task Manager는 Dynamic Attributes Connector를 비롯한 핵심 서비스가 다운된 경우 Health Alerts를 표시합니다. 경고에는 서비스 이름 및 상태에 대한 정보가 포함되어 있습니다.

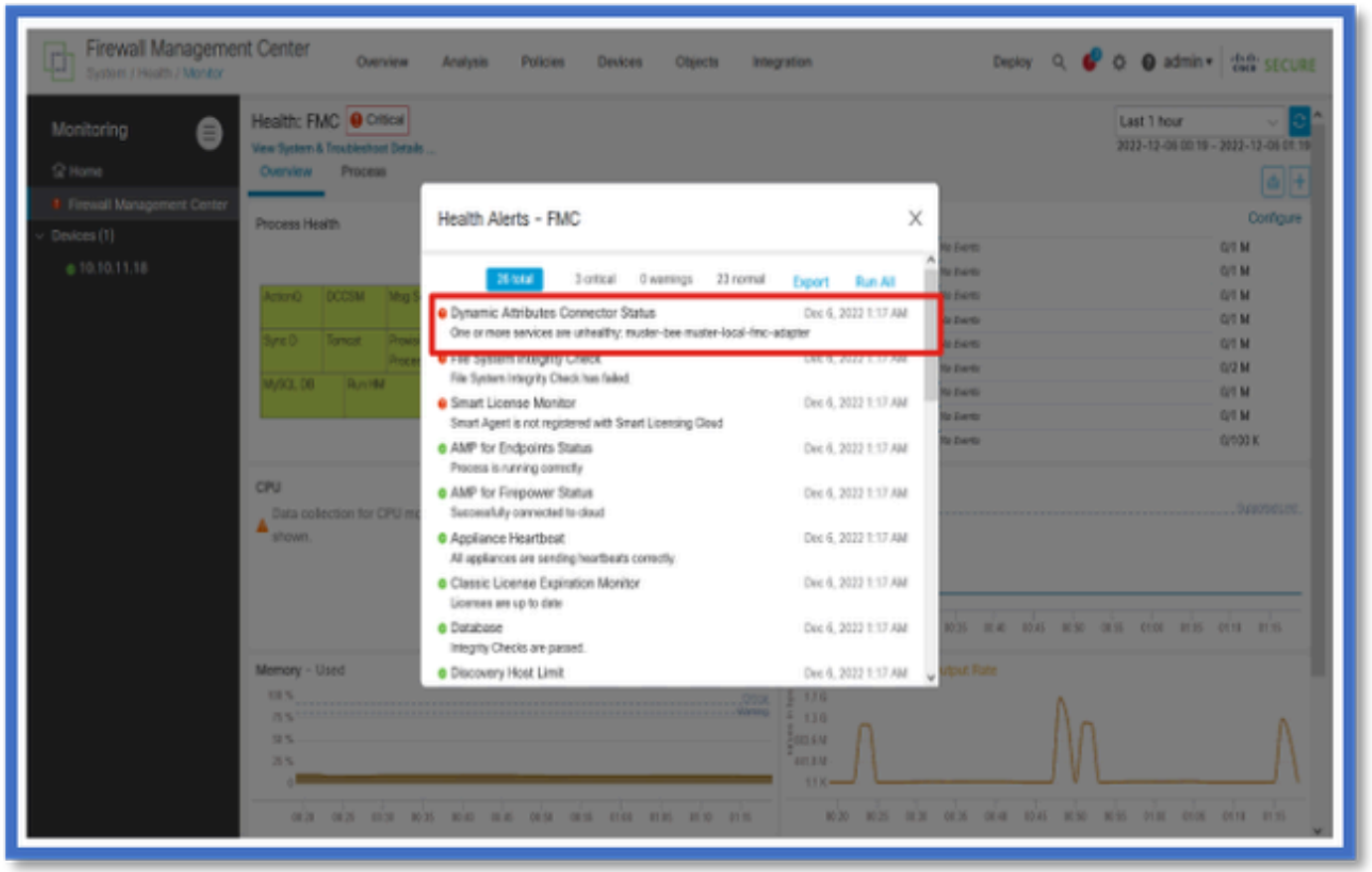


참고: 여전히 여러 알림에 "muster" 이름이 있으며, 자세한 정보를 보려면 여기에서 서비스 이름을 제공해야 합니다.



여기서 muster-bee 및 muster-local-fmc-adapter가 "비정상"임을 알 수 있습니다.

오류가 코어 서비스를 나타내는 경우 디버그를 위해 문제 해결 로그를 수집해야 합니다.



트러블슈팅의 CSDAC

CSDAC 문제 해결 생성

- CSDAC 로그는 FMC 트러블슈팅을 생성하는 동안 자동으로 수집됩니다.번들에는 오프라인으로 문제를 디버깅하는 데 필요한 Docker 상태, 로그 및 데이터가 포함됩니다.
- 문제 해결 로그가 수집되는 오류를 재현하기 전에 CSDAC 디버그 모드를 활성화하는 것이 좋습니다.

/usr/local/sf/csdac 호출 ./muster-cli debug-on

다음 폴더에서 Troubleshoot(추적 안 함 문제 해결)에서 CSDAC 로그를 찾습니다.

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

여기에는 etcd 데이터베이스에 저장된 데이터가 포함됩니다.

/results-XX/명령 출력/csdac_troubleshoot /log

여기에는 docker 컨테이너의 로그가 포함됩니다.

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

컨테이너 상태, 버전 및 docker 이미지 세부사항이 표시됩니다.

CLI 문제 해결

muster-cli 스크립트를 사용하여 FMC CLI에서 CSDAC의 상태를 확인할 수 있습니다.

모든 서비스의 상태가 "Exitted(종료됨)"이거나 "Up(가동)"과 다른 경우 먼저 해당 컨테이너의 로그를 확인합니다.

컨테이너 이름은 로그를 가져오는 데 필요합니다. 출력에서 가져올 수 있습니다.

```
'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 디버그 모드

'muster-cli' 스크립트를 사용하여 디버그 로그를 설정 및 해제할 수 있습니다.기본적으로 컨테이너는 INFO level.INFO에 로깅되며 DEBUG만 지원되는 레벨입니다.

DEBUG level user를 활성화하려면 ./muster-cli debug-on.

이렇게 하면 문제 해결 생성 및 디버그 도움말에 대한 추가 정보가 제공됩니다.문제를 재현하는 동안 이 옵션을 활성화해야 합니다.

INFO 레벨로 돌아가려면 ./muster-cli debug-off를 사용합니다.

<#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
```

로깅된 메시지(디버그)

디버그 모드가 활성화된 경우 모든 docker 컨테이너 로그에는 디버그 메시지도 포함됩니다

docker 명령을 사용하여 실시간으로 로그 가져오기: docker logs -f <container_name>

아래 예에서 디버그 메시지는 gRPC 오류를 트리거한 항목을 표시합니다

<#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
```

트러블슈팅의 샘플 문제 연습

문제 및 문제 해결 개요

문제/장애:

가장 일반적인 문제는 FMC가 모든 동적 객체 매핑을 수신하지 않는다는 것입니다.

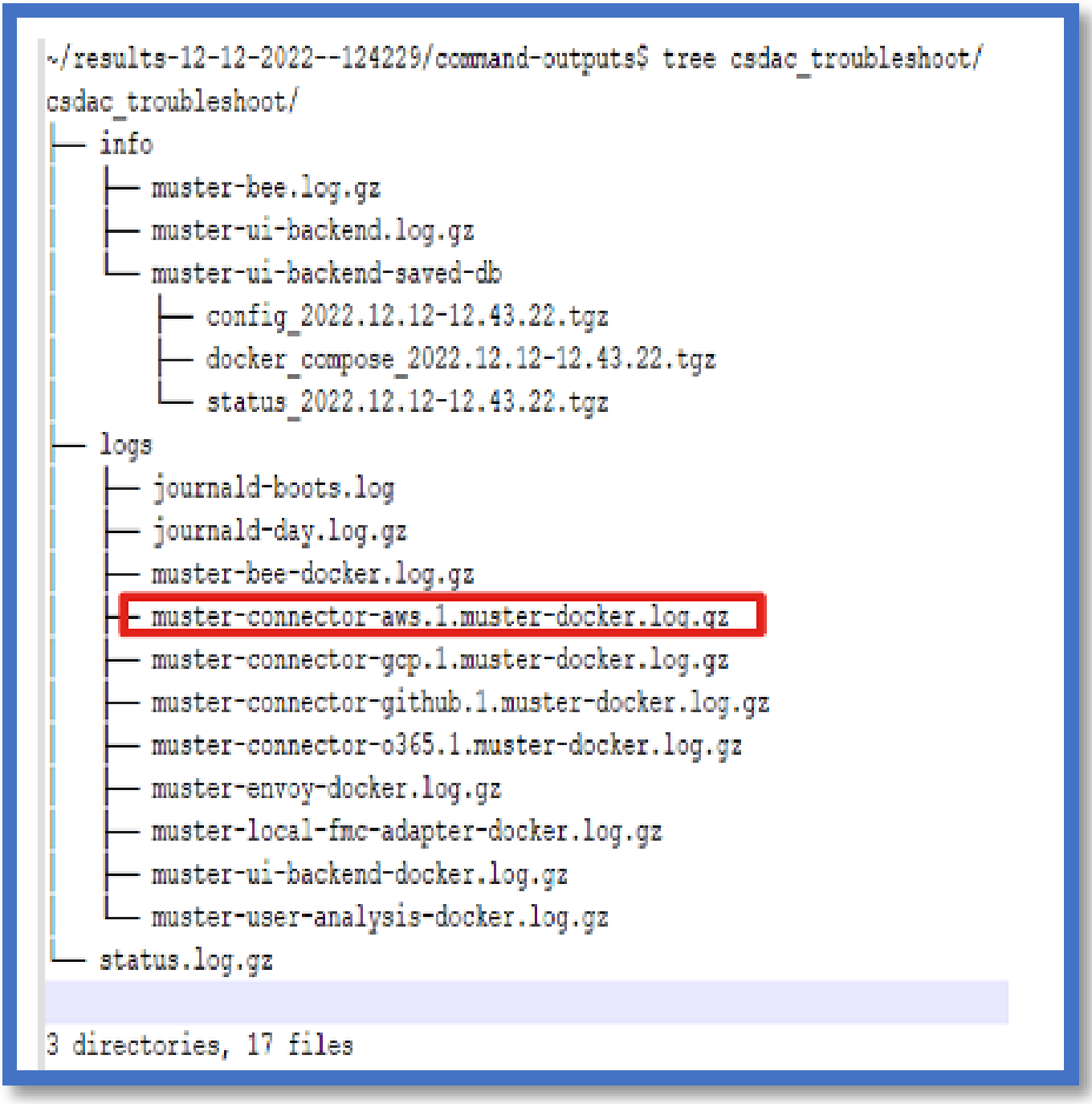
문제 해결:

이 문제를 해결하기 위해

- "muster-cli"에서 디버그 모드 활성화
- FMC UI에서 생성된 문제 해결 파일
- 수집된 Troubleshoot(문제 해결)에서 CSDAC AWS Connector 로그를 확인했습니다.
- CSDAC AWS Connector에서 AWS 인스턴스의 첫 번째 IP에 대해서만 쿼리했음을 발견했습니다.

트러블슈팅 번들 준비

- FMC CLI에서 ./muster-cli debug-on을 사용하여 디버그 모드를 활성화했습니다. muster-cli 툴은 /usr/local/sf/csdac에서 사용할 수 있습니다.
- 커넥터가 OK(확인) 상태가 될 때까지 기다린 다음 Dynamic Attribute Filters(동적 특성 필터)를 확인하여 문제를 다시 생성했습니다.
- FMC UI에서 문제 해결 로그를 수집하여 압축을 풀었습니다.AWS Connector 로그에서 스냅샷 내용을 확인했습니다



IP에 대한 태그 특성 확인

지정된 IP에 대한 태그 특성이 문제 해결 로그에 기록됩니다. AWS Connector의 경우 muster-connector-aws.1.muster-docker.log.gz를 살펴보았습니다

수표 요약

커넥터 및 어댑터 상태가 양호합니까?

해당 커넥터, 어댑터 페이지에서 상태를 확인합니다.

커넥터가 모든 매핑을 가져왔습니까?

일치하는 IP 주소에 대한 규칙 미리 보기를 확인합니다.

Connector Docker 로그를 확인하여 매핑을 올바르게 쿼리하고 있는지 확인합니다.

REST 서버가 커넥터에서 동적 태그 매핑을 수신했습니까?

FMC 동적 개체 페이지를 확인합니다.

FMC REST 서버가 CSDAC의 API 요청을 올바르게 처리했는지 확인하려면 USMS 로그(/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log)를 확인합니다.

질문과 대답

Q: 어떤 버전의 온프레미스 CSDAC가 ISE 커넥터를 지원합니까? 버전 7.4.0(빌드 1494)에도 이러한 커넥터가 표시되지 않습니까?

A: 이 패키지는 FMC 또는 CDO가 아닌 독립 실행형 CSDAC에 있습니다. 이를 테스트하려면 CSDAC 사용 가능한 패키지가 필요합니다.

Q: 릴리스되면 어떤 온프레미스 CSDAC 버전이 될까요?

A: 2.1.0일 수 있습니다.

Q: API가 설치된 기어가 있는 화면이 표시됩니다. 저는 그것이 CSDAC라고 생각하는데, 그것은 무엇을 의미합니까?

A: 이 CSDAC에는 API 탐색기가 내장되어 있으므로 해당 페이지에서 CSDAC에 API 호출을 수행할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.