Cisco Secure Dynamic Attributes Connector

다음 주제에서는 Cisco Secure Dynamic Attributes Connector를 구성하고 사용하는 방법에 대해 설명합니다.

관련 정보 Cisco Secure Dynamic Attributes Connector

동적 속성 커넥터를 사용하면 Secure Firewall Management Center 액세스 제어 규칙에서 다양한 클라우드 서비스 플랫폼의 서비스 태그 및 범주를 사용할 수 있습니다.

지원되는 커넥터

현재 지원하는 커넥터:

표 *1: Cisco Secure Dynamic Attributes Connector* 버전 및 플랫폼 별 지원되는 커넥터 목록

CSDAC 버전/플랫폼	AWS	Azure	Azure 서비스 태그	일반 텍스트	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	확대
버전 1.1(온프레미스)	예	예	예	아니요	아니요	아니요	예	예	아니요	아니요
버전 2.0(온프레미스)	예	예	예	아니요	아니요	예	예	예	아니요	아니요
버전 2.2(온프레미스)	예	예	예	아니요	예	예	예	예	아니요	아니요
버전 2.3(온프레미스)	예	예	예	예	예	예	예	예	예	
클라우드 제공(Cisco Defense Orchestrator)	예	예	예	아니요	예	예	예	아니요	아니요	아니요
Secure Firewall Management Center 7.4.1	예	예	예	예	예	예	예	예	예	예

커넥터에 대한 추가 정보:

- AWS(Amazon Web Services)

  자세한 내용은 Amazon 설명서 사이트에서 AWS 리소스 태그 지정과 같은 리소스를 참조하십시오.

- 지정한 IP 주소의 일반 텍스트 목록입니다.
- Microsoft Azure

  자세한 내용은 Azure 설명서 사이트의 이 페이지를 참조하십시오.

- Microsoft Azure 서비스 태그

  자세한 내용은 Microsoft TechNet의 가상 네트워크 서비스 태그와 같은 리소스를 참조하십시오.

- Office 365 IP 주소

  자세한 내용은 docs.microsoft.com에서 Office 365 URL 및 IP 주소 범위를 참조하십시오.

- vCenter 및 NSX-T에서 관리하는 VMware 범주 및 태그

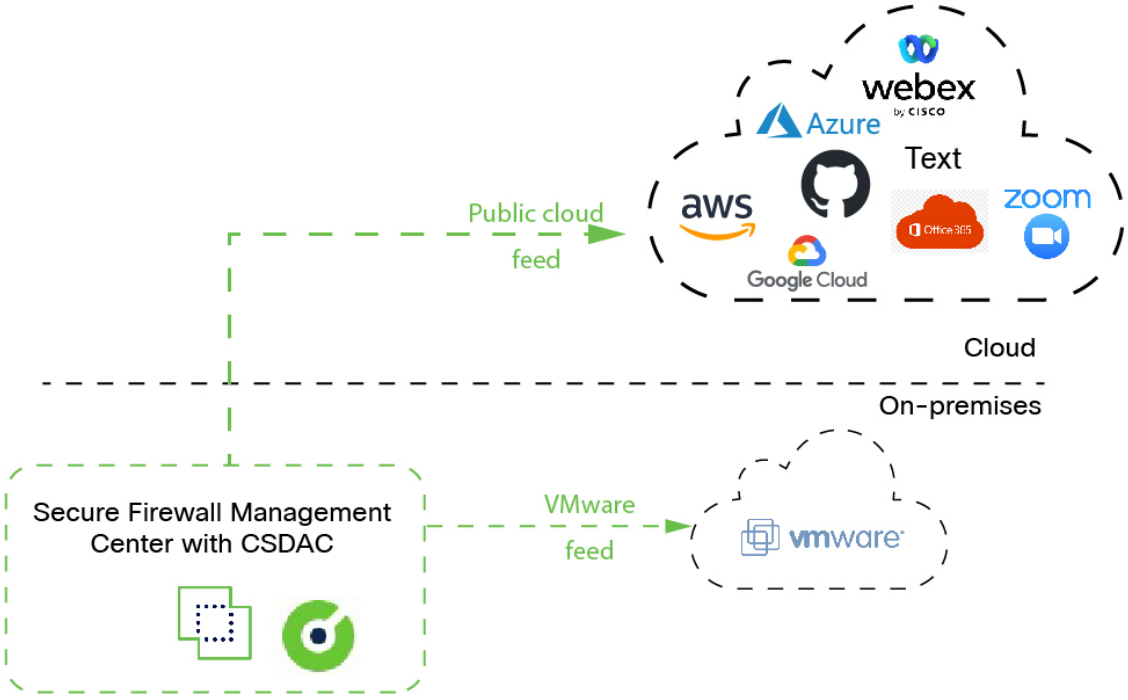
  자세한 내용은 VMware 설명서 사이트에서 vSphere 태그 및 속성과 같은 리소스를 참조하십시오.

- Webex IP 주소
- Zoom IP 주소

운영 방식

IP 주소와 같은 네트워크 구성은 워크로드의 동적 속성과 IP 주소 중복의 불가피성으로 인해 가상, 클라우드 및 컨테이너 환경에서 신뢰할 수 없습니다. 고객은 IP 주소 또는 VLAN이 변경되는 경우에도 방화벽 정책이 유지되도록 VM 이름 또는 보안 그룹과 같은 비 네트워크 구문을 기반으로 정책 규칙을 정의해야 합니다.

다음 그림은 시스템이 상위 레벨에서 작동하는 방식을 보여줍니다.



- 시스템에서는 특정 퍼블릭 클라우드 제공자를 지원합니다.

  이 주제에서는 지원되는 커넥터(해당 제공자에 대한 연결)에 대해 설명합니다.

관련 항목

- Cisco Secure Dynamic Attributes Connector 활성화, 4 페이지
- 대시보드 정보, 7 페이지

Cisco Secure Dynamic Attributes Connector 기록

기능	최소 **Management Center**	최소 **Threat Defense**	세부 사항

기능	최소 **Management Center**	최소 **Threat Defense**	세부 사항
Cisco Secure Dynamic Attributes Connector	7.4.0	7.4.0	이 기능이 도입되었습니다. Cisco Secure Dynamic Attributes Connector이 이제 Secure Firewall Management Center에 포함됩니다. 동적 속성 커넥터를 사용하여 매니지드 디바이스에 구축할 필요 없이 액세스 제어 규칙에서 Microsoft Azure와 같은 클라우드 기반 플랫폼의 IP 주소를 가져올 수 있습니다. 추가 정보: • 이 제품이 포함된 동적 속성 커넥터:관련 정보 Cisco Secure Dynamic Attributes Connector, 1 페이지 • 독립형 동적 속성 커넥터: Cisco Secure Dynamic Attributes Connector 구성 가이드 신규/수정된 화면: **Integration(통합)** > **Cisco Dynamic Attributes Connector(Cisco 동적 속성 커넥터)**

Cisco Secure Dynamic Attributes Connector 시스템 요구 사항

Cisco Secure Dynamic Attributes Connector에는 다음과 같은 메모리 요구 사항이 있습니다.

FMCv: RAM의 양	**Secure Firewall Management Center** 하드웨어 모델	최대 **(**커넥터 **+ Azure AD** 영역**)** 수
32GB 이상	Firepower 1000, Firepower 1600, vFMC	10
64GB 이상	Firepower 2500, Firepower 2600,vFMC 300	20
128GB 이상	Firepower 4500, Firepower 4600	30

위의 제한은 가상 머신과 물리적 머신 모두에 적용됩니다.

구축 문제가 발생할 수 있으므로, 시스템은 사용자가 위의 제한을 초과하지 않도록 방지합니다.

Cisco Secure Dynamic Attributes Connector 활성화

이 작업에서는 Secure Firewall Management Center에서 Cisco Secure Dynamic Attributes Connector를 활성화하는 방법에 대해 설명합니다. 동적 속성 커넥터는 클라우드 네트워킹 제품의 개체를 management center 액세스 제어 규칙에서 사용할 수 있도록 하는 통합입니다.

프로시저

단계 1 아직 하지 않았다면 에 로그인합니다.Secure Firewall Management Center

단계 2 **Integration(통합)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)** 버튼을 클릭합니다.

단계 3 **Enabled(활성화)**로 설정합니다.

단계 4 동적 속성 커넥터이 활성화되어 있는 동안에는 메시지가 표시됩니다.

오류가 발생하면 다시 시도하십시오. 오류가 계속되면 Cisco TAC에 문의하십시오.

Docker 컨테이너의 네트워크 및 서브넷 구성

Cisco Secure Dynamic Attributes Connector에서는 Docker 컨테이너를 사용하여 Secure Firewall Management Center의 커넥터 데이터를 검색합니다. Secure Firewall Management Center 관리 인터페이스 및 네트워크에서 사용되는 다른 IP 주소와의 충돌을 방지하기 위해, 필요에 따라 이 섹션에서 설명하는 명령을 사용하여 Docker IP 주소 및 범위를 변경할 수 있습니다.

Docker 네트워크 정보

동적 속성 커넥터에서 Docker 데몬을 사용하려면 다음 네트워크가 필요합니다.

- Docker 데몬에서 내부적으로 사용하는 `docker0`.
- `veth`*`number`*로 명명된 일련의 IPv6 네트워크.

  이는 동적 속성 커넥터에서 사용하는 내부 브리지 네트워크입니다.
- 이름이 b`br-`*`number`*인 동적 속성 커넥터 커넥터에서 사용하는 Docker 브리지 네트워크.

동적 속성 커넥터 활성화 전에는 `docker0`이라는 이름의 Docker 인터페이스가 하나만 있으며, 172.18.0.1/16으로 설정됩니다.

Docker 네트워크 및 서브넷 변경

Cisco Secure Dynamic Attributes Connector 활성화, 4 페이지에 설명된 대로 먼저 동적 속성 커넥터를 활성화합니다.

Docker 네트워크 및 서브넷을 변경하려면 루트 권한이 있는 사용자로 `/usr/local/sf/bin/change_docker_subnet.sh -b` *`CIDR-network`* `-s` *`address-pool-size`*를 실행합니다.

- `-b` *`CIDR-network`*는 CIDR 표기법으로 네트워크 기본 주소 풀을 설정합니다.
- `-s` *`address-pool-size`*는 네트워크 기본 주소에 대한 넷마스크를 설정합니다. 이 옵션을 사용하면 네트워크 범위가 기존 네트워크 범위와 중복되는 경우 기본 주소 범위의 주소 수를 제한할 수 있습니다. 특히 시스템에서 사용 가능한 RAM을 초과하지 않도록 Secure Firewall Management Center 모델에 대해 특정 `-s` 값을 사용하는 것이 좋습니다. (Docker 컨테이너는 동적 속성 커넥터

커넥터에서 사용되며 해당 제한이 Cisco Secure Dynamic Attributes Connector 시스템 요구 사항, 4 페이지에 표시됩니다.)

중요 Docker에 할당하는 네트워크는 내부 네트워크 범위에 속해야 하며, Secure Firewall Management Center 또는 내부 네트워크의 다른 디바이스에서 사용하는 네트워크와 충돌하지 않아야 합니다.

예

다음 테이블에는 예가 나와 있습니다.

Secure Firewall Management Center 모델	권장 **-s** 값	샘플 **-b** 값	**Cisco Secure Dynamic Attributes Connector** 사용된 컨테이너 주소
Firepower 1000, Firepower 1600, vFMC	27 (넷마스크 255.255.255.224)	172.19.0.0/16	IP 주소 30개 `docker0`: 172.19.0.1 `172.19.0.32/27` 서브넷이 있는 브리지 네트워크 `br-number` 게이트웨이 `172.19.0.33` `172.19.0.38/27`, `172.19.0.39/27`등의 네트워크에서 생성된 커넥터
Firepower 2500, Firepower 2600, vFMC 300	26 (넷마스크 255.255.255.192)	192.168.0.0/16	62개의 IP 주소 `docker0`: 192.168.1.1 서브넷 `192.168.1.64/26`이 있는 브리지 네트워크 `br-number` 게이트웨이 `192.168.1.65` `192.168.1.71/26`, `192.168.1.72/26`등의 네트워크에서 생성된 커넥터
Firepower 4500, Firepower 4600	25 (넷마스크 255.255.255.128)	192.168.0.0/16	126개의 IP 주소 `docker0`: 192.168.1.1 서브넷 `192.168.1.128/25`가 있는 브리지 네트워크 `br-number` 게이트웨이 `192.168.1.129` `192.168.1.136/25`, `192.168.1.135/25` 등의 네트워크에서 생성된 커넥터

참조를 위해 전체 명령은 다음과 같습니다.

```
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 27
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 26
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 25
```

네트워크 확인

네트워크 설정을 확인하려면 `sudo docker network inspect muster-net`을 입력합니다. 명령 결과는 JSON 형식으로 표시됩니다.

문제 해결

다음은 이 명령을 사용하여 발생할 수 있는 일반적인 오류에 대한 몇 가지 해결책입니다.

오류**:** `풀 서브넷 값은 크기보다 클 수 없습니다.`
솔루션: `-s`의 값을 CIDR 네트워크 값보다 작게 변경합니다.

예를 들면 다음과 같습니다.

INCORRECT: `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 8`

CORRECT: `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 20`

오류**:** 명령 실행 후 **Docker** 네트워크가 잘못되었습니다**.**
솔루션: Docker 데몬을 재시작합니다. `sudo pmtool restartbyid docker`

오류**:** **`unix:///var/run/docker.sock`**에서 **`Docker`** 데몬에 연결할 수 없습니다**.** **`Docker`** 데몬이 실행 중입니까**?**
솔루션: Docker를 재시작합니다. `pmtool restartbyid docker`

오류**:** 입력은 비워둘 수 없습니다**.**
`-s` 매개변수가 필요합니다.

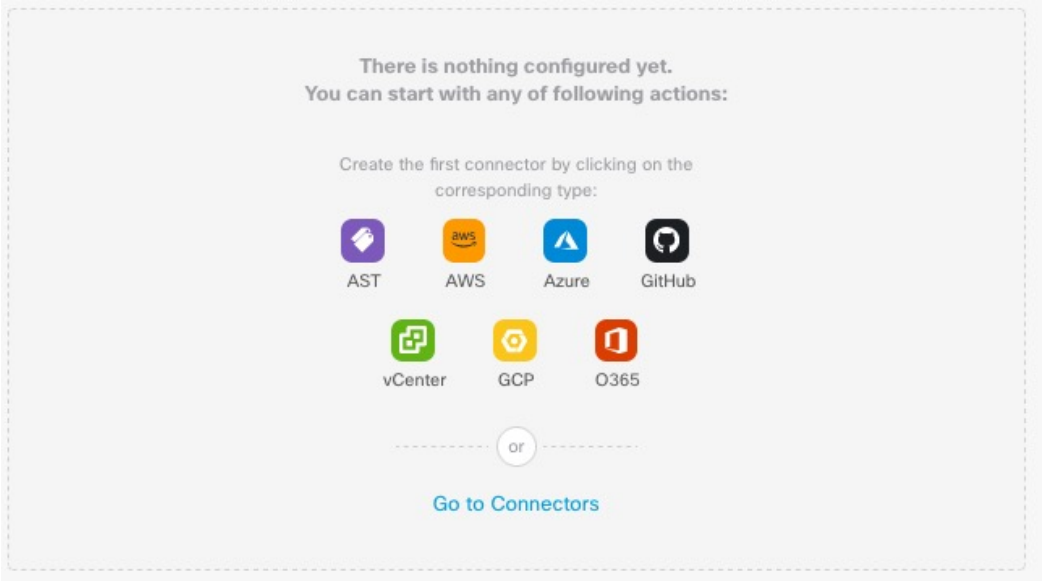
오류**:** `풀 크기` **`(32)`**`는` **`32`**`보다 크거나` **`0`**`보다 작을 수 없습니다.`
솔루션: `-s`의 값을 0보다 크고 32보다 작도록 변경합니다.

대시보드 정보

Cisco Secure Dynamic Attributes Connector 대시보드에 액세스하려면 Secure Firewall Manager에 로그인하고 페이지 상단에 있는 **Integration(**통합**)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)**을 클릭합니다.

Cisco Secure Dynamic Attributes Connector가 활성화되지 않은 경우, 슬라이더를 이동하여 활성화합니다. 이 프로세스를 완료하는 데 몇 분이 걸릴 수 있습니다.

Cisco Secure Dynamic Attributes Connector Dashboard(대시보드) 페이지에는 커넥터, 어댑터 및 필터의 상태가 한눈에 표시됩니다. 다음은 구성되지 않은 시스템의 대시보드 예입니다.



대시보드로 수행할 수 있는 작업은 다음과 같습니다.

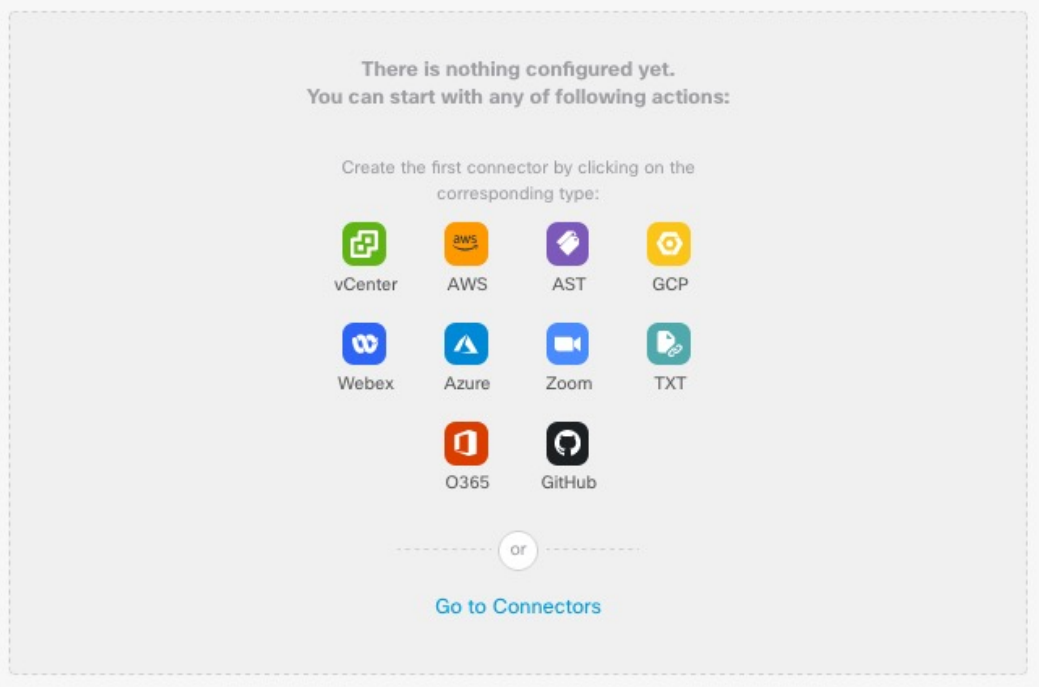
- 커넥터 및 동적 특성 필터를 추가, 편집 및 삭제합니다.
- 커넥터 및 동적 특성 필터가 서로 어떻게 관련되어 있는지 확인합니다.
- 경고 및 오류 보기

관련 주제

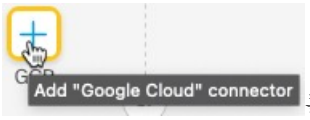
- 구성되지 않은 시스템의 대시보드, 8 페이지
- 구성된 시스템의 대시보드, 9 페이지
- 커넥터 추가, 편집 또는 삭제, 11 페이지
- 동적 속성 필터 추가, 편집 또는 삭제, 12 페이지

구성되지 않은 시스템의 대시보드

구성되지 않은 시스템의 샘플 Cisco Secure Dynamic Attributes Connector 대시보드 페이지:



처음에는 시스템에 대해 구성할 수 있는 모든 유형의 커넥터 가 대시보드에 표시됩니다. 다음 중 하나를 수행할 수 있습니다.

- 커넥터 위에 마우스 포인터를 올리고 

를 클릭하여 새 커넥터 또는 어댑터를 생성합니다.
- 커넥터를 추가, 수정 또는 삭제하려면 **Go to Connectors(**커넥터로 이동**)**를 클릭합니다(여러 커넥터를 동시에 생성, 수정 또는 삭제할 때 유용).

  자세한 내용은 커넥터 생성, 14 페이지을 참고하십시오.

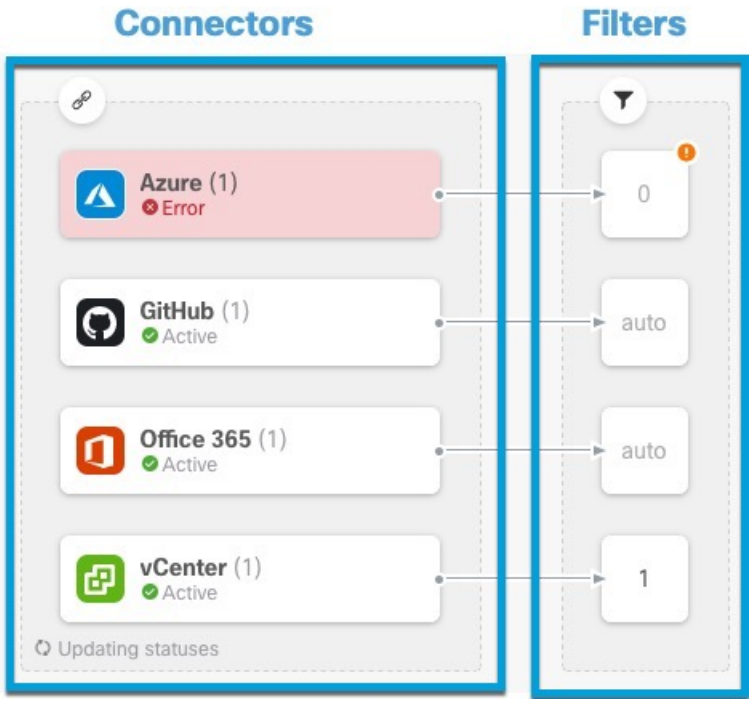
관련 주제**:**

- 구성된 시스템의 대시보드, 9 페이지
- 커넥터 추가, 편집 또는 삭제, 11 페이지
- 동적 속성 필터 추가, 편집 또는 삭제, 12 페이지

구성된 시스템의 대시보드

구성된 시스템의 샘플 Cisco Secure Dynamic Attributes Connector 대시보드 페이지:

그림의 영역을 클릭하여 자세히 알아보거나 그림 아래에 있는 링크 중 하나를 클릭합니다.



1 커넥터 생성, 14 페이지
2 동적 속성 필터 생성, 33 페이지

Dashboard(대시보드)에는 다음이 표시됩니다(왼쪽에서 오른쪽으로).

커넥터 열	필터 열
구성된 각 유형의 수를 나타내는 숫자가 있는 커넥터 목록입니다. 커넥터는 Secure Firewall Manager로 전송될 수 있는 동적 속성을 수집합니다. 동적 특성 필터는 전송할 데이터를 지정합니다. 구성된 모든 커넥터에 대한 자세한 정보를 보려면 을 클릭합니다. 커넥터의 이름을 클릭하여 커넥터를 추가, 편집 또는 삭제할 수도 있습니다. 또는 관련 세부 정보를 볼 수 있습니다. 자세한 내용은 커넥터 추가, 편집 또는 삭제, 11 페이지을 참고하십시오.	커넥터와 연결된 각 필터의 수를 나타내는 숫자와 함께 각 커넥터와 연결된 동적 속성 필터의 목록입니다. 구성된 모든 필터에 대한 자세한 정보를 보려면 을 클릭합니다. 필터의 이름을 클릭하여 필터를 추가, 편집 또는 삭제할 수도 있습니다. 또는 관련 세부 정보를 볼 수 있습니다. 자세한 내용은 동적 속성 필터 추가, 편집 또는 삭제, 12 페이지을 참고하십시오.

참고 Outlook 365 및 Azure 서비스 태그와 같은 일부 커넥터는 동적 속성 필터 없이 사용 가능한 동적 개체를 자동으로 가져옵니다. 이러한 커넥터는 열에 **Auto(**자동**)**로 표시됩니다.

Dashboard(대시보드)에는 개체의 사용 가능 여부가 표시됩니다. Dashboard(대시보드) 페이지는 15초마다 새로 고쳐지지만 언제든지 페이지 상단의 **Refresh(**새로 고침**)**( )을 클릭하여 즉시 새로 고칠 수 있습니다. 문제가 계속되면 네트워크 연결을 확인하십시오.

관련 주제**:**

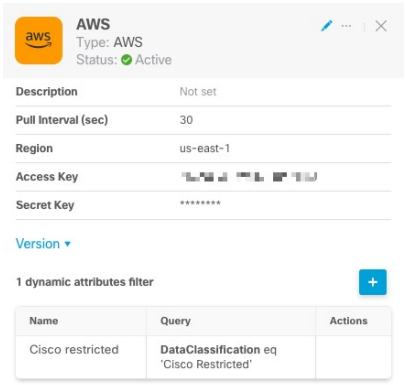
- 커넥터 추가, 편집 또는 삭제, 11 페이지
- 동적 속성 필터 추가, 편집 또는 삭제, 12 페이지

커넥터 추가, 편집 또는 삭제

Dashboard(대시보드)에서는 커넥터를 보거나 수정할 수 있습니다. 커넥터의 이름을 클릭하여 해당 커넥터의 모든 인스턴스를 보거나 를 클릭하여 다음 추가 옵션을 볼 수 있습니다.

- 모든 커넥터를 동시에 보려면 **Connectors(**커넥터**)**로 이동합니다. 여기에서 커넥터를 추가, 수정 및 삭제할 수 있습니다.
- **Add Connector** > ***type(***커넥터 유형 추가***)***을 클릭하여 표시된 유형의 커넥터를 추가합니다.

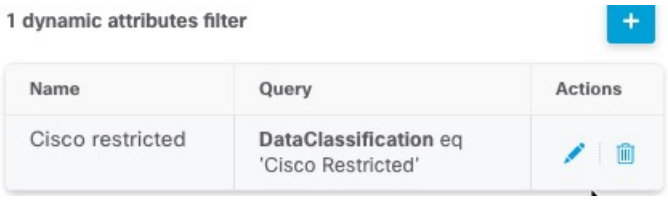
커넥터 열에서 커넥터( )를 클릭하면 해당 커넥터에 대한 추가 정보가 표시됩니다. 예는 다음과 같습니다.



다음 옵션을 이용할 수 있습니다.

- 이 커넥터를 편집하려면 수정 아이콘( )를 클릭합니다.
- 추가 옵션을 보려면 추가 아이콘( )를 클릭합니다.
- 패널을 닫으려면 를 클릭합니다.
- **Version(**버전**)**을 클릭하여 버전을 표시합니다. Cisco TAC에 필요한 경우 선택적으로 버전을 클립보드에 복사할 수 있습니다.

패널의 맨 아래에 있는 테이블을 사용하여 동적 속성 필터를 추가할 수 있습니다. 또는 동적 속성 커넥터 커넥터를 편집하거나 삭제할 수 있습니다. 다음은 샘플입니다.



이 커넥터에 대한 동적 특성 필터를 추가하려면 아이콘 추가(+)를 클릭합니다. 자세한 내용은 동적 속성 필터 생성, 33 페이지을 참고하십시오.

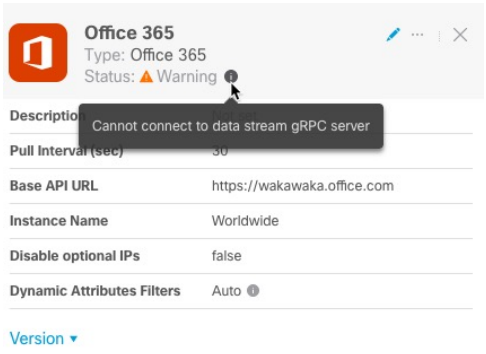
Actions(작업) 열 위로 마우스 포인터를 이동하여 표시된 커넥터를 편집하거나 삭제합니다.

오류 정보 보기

커넥터에 대한 오류 정보를 보려면 다음을 수행합니다.

1. Dashboard(대시보드)에서 오류를 표시하는 커넥터의 이름을 클릭합니다.
2. 오른쪽 창에서 정보(ⓘ)을 클릭합니다.

   예는 다음과 같습니다.



3. 이 문제를 해결하려면 Office 365 커넥터 생성, 27 페이지에 설명된 대로 커넥터 설정을 편집합니다.
4. 문제를 해결할 수 없는 경우 **Version(**버전**)**을 클릭하고 버전을 텍스트 파일에 복사합니다.
5. 이 모든 정보를 Cisco TAC에 제공합니다.

동적 속성 필터 추가, 편집 또는 삭제

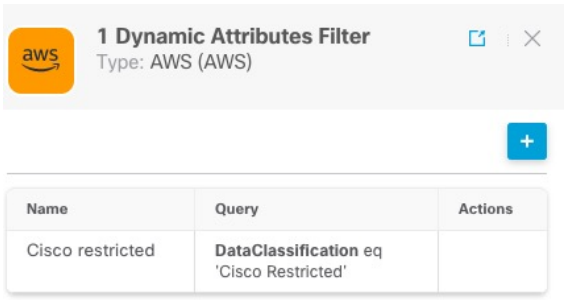
대시보드를 사용하면 동적 특성 필터를 추가, 편집 또는 삭제할 수 있습니다. 필터 이름을 클릭하여

해당 필터의 모든 인스턴스를 보거나 다음 추가 옵션에 대해 을 클릭할 수 있습니다.

- **Go to Dynamic Attributes Filters(**동적 속성 필터로 이동**)**를 클릭하여 구성된 모든 동적 속성 필터를 확인합니다. 여기에서 동적 속성 필터를 추가, 편집 또는 삭제할 수 있습니다.
- **Add Dynamic Attributes Filters(**동적 속성 필터 추가**)**를 클릭하여 필터를 추가합니다.

동적 특성 필터 추가에 대한 자세한 내용은 동적 속성 필터 생성, 33 페이지의 내용을 참조하십시오.

예는 다음과 같습니다.



참고 Outlook 365 및 Azure 서비스 태그와 같은 일부 커넥터는 동적 속성 필터 없이 사용 가능한 동적 개체를 자동으로 가져옵니다. 이러한 커넥터는 열에 **Auto(**자동**)**로 표시됩니다.

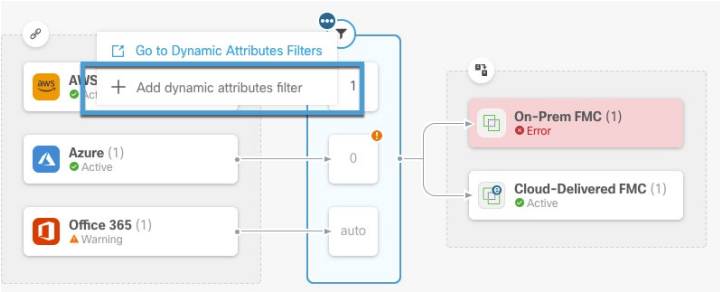
다음 옵션을 이용할 수 있습니다.

- 커넥터와 연결된 동적 특성 필터에 대한 요약 정보를 보려면 필터 인스턴스를 클릭합니다.
- 아이콘 추가( )를 클릭하여 새 동적 특성 필터를 추가합니다.

  자세한 내용은 동적 속성 필터 생성, 33 페이지을 참고하십시오.

- 필터 열( )에서 을 클릭하면 표시된 커넥터에 연결된 동적 특성 필터가 없음을 나타냅니다. 연결된 필터가 없으면 커넥터는 management center에 아무것도 전송할 수 없습니다.

  이 문제를 해결하는 한 가지 방법은 필터 열에서 을 클릭하고 **Add Dynamic Attributes Filter(**동적 속성 필터 추가**)**를 클릭하는 것입니다. 다음은 샘플입니다.



- 필터를 추가, 편집 또는 삭제하려면 을 클릭합니다.

• 패널을 닫으려면 ×를 클릭합니다.

커넥터 생성

커넥터는 클라우드 서비스와의 인터페이스입니다. 커넥터는 management center의 액세스 제어 정책에서 네트워크 정보를 사용할 수 있도록 클라우드 서비스에서 네트워크 정보를 검색합니다.

다음을 지원합니다.

표 *2: Cisco Secure Dynamic Attributes Connector* 버전 및 플랫폼 별 지원되는 커넥터 목록

CSDAC 버전/플랫폼	**AWS**	**Azure**	**Azure** 서비스 태그	일반 텍스트	**GitHub**	**Google Cloud**	**Microsoft Office 365**	**vCenter**	**Webex**	확대
버전 1.1(온프레미스)	예	예	예	아니요	아니요	아니요	예	예	아니요	아니요
버전 2.0(온프레미스)	예	예	예	아니요	아니요	예	예	예	아니요	아니요
버전 2.2(온프레미스)	예	예	예	아니요	예	예	예	예	아니요	아니요
버전 2.3(온프레미스)	예	예	예	예	예	예	예	예	예	
클라우드 제공(Cisco Defense Orchestrator)	예	예	예	아니요	예	예	예	아니요	아니요	아니요
Secure Firewall Management Center 7.4.1	예	예	예	예	예	예	예	예	예	예

자세한 내용은 다음 섹션 중 하나를 참조하십시오.

Amazon Web Services Connector - 사용자 권한 및 가져온 데이터 정보

Cisco Secure Dynamic Attributes Connector는 액세스 제어 정책에 사용할 동적 속성을 AWS에서 management center로 가져옵니다.

동적 속성 가져옴

AWS에서 다음 동적 속성을 가져옵니다.

• 태그 - AWS EC2 리소스를 구성하는 데 사용할 수 있는 사용자 정의 키-값 쌍입니다.

자세한 내용은 AWS 설명서의 EC2 리소스에 태그 지정을 참조하십시오.

- AWS에 있는 가상 머신의 *IP* 주소입니다.

최소 권한 필요

Cisco Secure Dynamic Attributes Connector에서는 최소한 `ec2:DescribeTags` 및 `ec2:DescribeInstances`가 동적 속성을 가져올 수 있도록 허용하는 정책을 보유한 사용자가 필요합니다.

Cisco Secure Dynamic Attributes Connector에 대한 최소 권한이 있는 AWS 사용자 생성

이 작업에서는 동적 속성을 management center로 전송할 수 있는 최소 권한으로 서비스 계정을 설정하는 방법을 설명합니다. 이러한 속성의 목록은 Amazon Web Services Connector - 사용자 권한 및 가져온 데이터 정보, 14 페이지 섹션을 참조하십시오.

시작하기 전에

AWS(Amazon Web Services) 계정이 이미 설정되어 있어야 합니다. 자세한 내용은 AWS 설명서에서 이 문서를 참조하십시오.

프로시저

단계 **1** 관리자 역할의 사용자로 AWS 콘솔에 로그인합니다.

단계 **2** Dashboard(대시보드)에서 **Security, Identity & Compliance(**보안**, ID** 및 컴플라이언스**)** > **IAM**을 클릭합니다.

단계 **3** **Access Management(**액세스 관리**)** > **Users(**사용자**)**를 클릭합니다.

단계 **4** **Add Users(**사용자 추가**)**를 클릭합니다.

단계 **5** **User Name(**사용자 이름**)** 필드에 사용자를 식별하는 이름을 입력합니다.

단계 **6** **Access Key - Programmatic Access(**액세스 키 - 프로그래밍 액세스**)**를 클릭합니다.

단계 **7** Set permissions(권한 설정) 페이지에서 사용자에게 액세스 권한을 부여하지 않고 **Next(**다음**)**를 클릭합니다. 나중에 이 작업을 수행합니다.

단계 **8** 원하는 경우 사용자에게 태그를 추가합니다.

단계 **9** **Create User**(사용자 생성)를 클릭합니다.

단계 **10** **Download.csv**를 클릭하여 사용자의 키를 컴퓨터에 다운로드합니다.

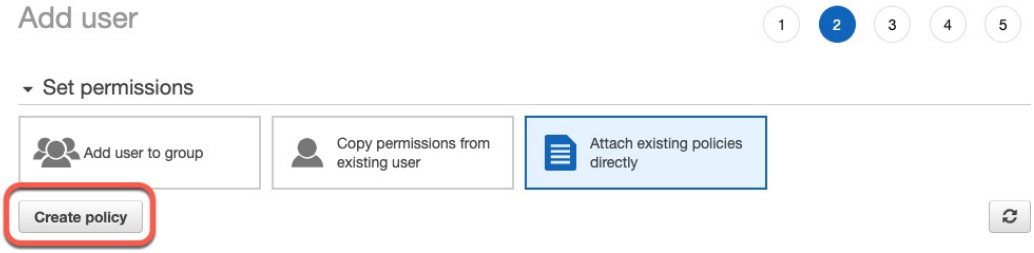
참고 이는 사용자의 키를 검색할 수 있는 유일한 기회입니다.

단계 **11** **Close(**닫기**)**를 클릭합니다.

단계 **12** 왼쪽 열의 Identity and Access Management(IAM) 페이지에서 **Access Management(**액세스 관리 > **Policies(**정책**)**를 클릭합니다.

단계 **13** **Create Policy(**정책 생성**)**를 클릭합니다.

단계 **14** Create Policy(정책 생성) 페이지에서 **JSON**을 클릭합니다.



단계 **15** 필드에 다음 정책을 입력합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeTags",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

단계 **16** **Next(**다음**)**를 클릭합니다.

단계 **17** **Review(**검토**)**를 클릭합니다.

단계 **18** Review Policy(정책 검토) 페이지에서 요청된 정보를 입력하고 **Create Policy(**정책 생성**)**를 클릭합니다.

단계 **19** Policies(정책) 페이지에서 검색 필드에 정책 이름의 전체 또는 일부를 입력하고 Enter를 누릅니다.

단계 **20** 방금 생성한 정책을 클릭합니다.

단계 **21** **Actions(**작업**)** > **Attach(**연결**)**를 클릭합니다.

단계 **22** 필요한 경우 검색 필드에 사용자 이름의 전체 또는 일부를 입력하고 Enter를 누릅니다.

단계 **23** **Attach Policy(**정책 연결**)**를 클릭합니다.

다음에 수행할 작업

AWS Connector 생성, 16 페이지.

AWS Connector 생성

이 작업에서는 액세스 제어 정책에 사용하기 위해 AWS에서 management center로 데이터를 전송하는 커넥터를 구성하는 방법을 설명합니다.

시작하기 전에

Cisco Secure Dynamic Attributes Connector에 대한 최소 권한이 있는 AWS 사용자 생성, 15 페이지에 설명된 권한 이상의 사용자를 생성합니다.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)** 버튼을 클릭합니다.

단계 **3** **Connector(**커넥터**)**를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 아이콘 추가( )을 클릭한 다음 커넥터의 이름을 클릭합니다.
- 커넥터 편집 또는 삭제: 추가 ( )을 클릭한 다음 행의 끝에서 **Edit(**편집**)** 또는 **Delete(**삭제**)**를 클릭합니다.

단계 **5** 다음 정보를 입력합니다.

값	설명
이름	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
설명	선택적 설명.
Pull Interval(끌어오기 간격**)**	(기본값 30초) AWS에서 IP 매핑을 검색하는 간격입니다.
Region(지역**)**	(필수) AWS 지역 코드를 입력합니다.
Access Key(액세스 키**)**	(필수) 액세스 키를 입력합니다.
Secret Key(암호 키**)**	(필수) 암호 키를 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** Status(상태) 열에 **Ok(**확인**)**가 표시되는지 확인합니다.

Azure Connector - 사용자 권한 및 가져온 데이터 정보

Cisco Secure Dynamic Attributes Connector는 액세스 제어 정책에 사용할 동적 속성을 Azure에서 management center로 가져옵니다.

동적 속성 가져옴

Azure에서 다음 동적 속성을 가져옵니다.

- *Tags(*태그*)*, 리소스, 리소스 그룹 및 구독과 연결된 키-값 쌍입니다.

  자세한 내용은 Microsoft 설명서에서 이 페이지를 참조하십시오.

- Azure에 있는 가상 머신의 *IP* 주소입니다.

최소 권한 필요

Cisco Secure Dynamic Attributes Connector에서 동적 속성을 가져오려면 최소한 독자 권한이 있는 사용자가 필요합니다.

Cisco Secure Dynamic Attributes Connector에 대한 최소 권한이 있는 Azure 사용자 생성

이 작업에서는 동적 속성을 management center로 전송할 수 있는 최소 권한으로 서비스 계정을 설정하는 방법을 설명합니다. 이러한 속성의 목록은 Azure Connector - 사용자 권한 및 가져온 데이터 정보, 17 페이지 섹션을 참조하십시오.

시작하기 전에

Microsoft Azure 계정이 이미 있어야 합니다. 새로 설정하려면 Azure 설명서 사이트에서 이 페이지를 참조하십시오.

프로시저

단계 **1** 구독의 소유자로 Azure 포털에 로그인합니다.

단계 **2** **Azure Active Directory**를 클릭합니다.

단계 **3** 설정할 애플리케이션에 대한 Azure Active Directory의 인스턴스를 찾습니다.

단계 **4** **Add(추가)** > **App registration(앱 등록)**을 클릭합니다.

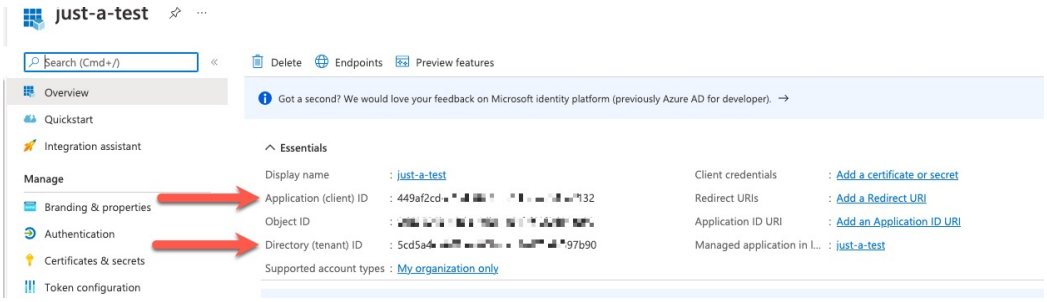
단계 **5** **Name(이름)** 필드에 이 애플리케이션을 식별하는 이름을 입력합니다.

단계 **6** 조직의 요구에 따라 이 페이지에 기타 정보를 입력합니다.

단계 **7** **Register(등록)**를 클릭합니다.

단계 **8** 다음 페이지에서 클라이언트 ID(애플리케이션 *ID*라고도 함) 및 테넌트 ID(디렉터리 *ID*라고도 함)를 기록해 둡니다.

다음은 샘플입니다.

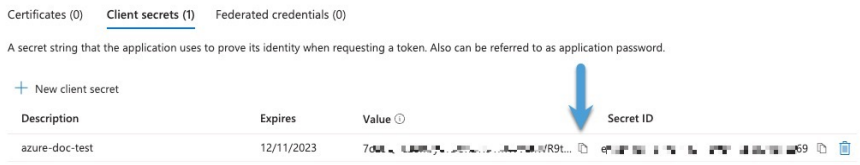


단계 **9** Client Credentials(클라이언트 자격 증명) 옆의 **Add certificate or secret(인증서 또는 암호 추가)**를 클릭합니다.

단계 **10** **New Client Secret(새 클라이언트 비밀번호)**을 클릭합니다.

단계 **11** 필요한 정보를 입력하고 **Add(추가)**를 클릭합니다.

단계 **12** **Value(값)** 필드의 값을 클립보드에 복사합니다. 이 값은 암호 ***ID***가 아니라 클라이언트 암호입니다.



단계 **13** 기본 Azure 포털 페이지로 돌아가서 **Subscriptions(**구독**)**를 클릭합니다.

단계 **14** 구독의 이름을 클릭합니다.

단계 **15** 구독 ID를 클립 보드에 복사합니다.

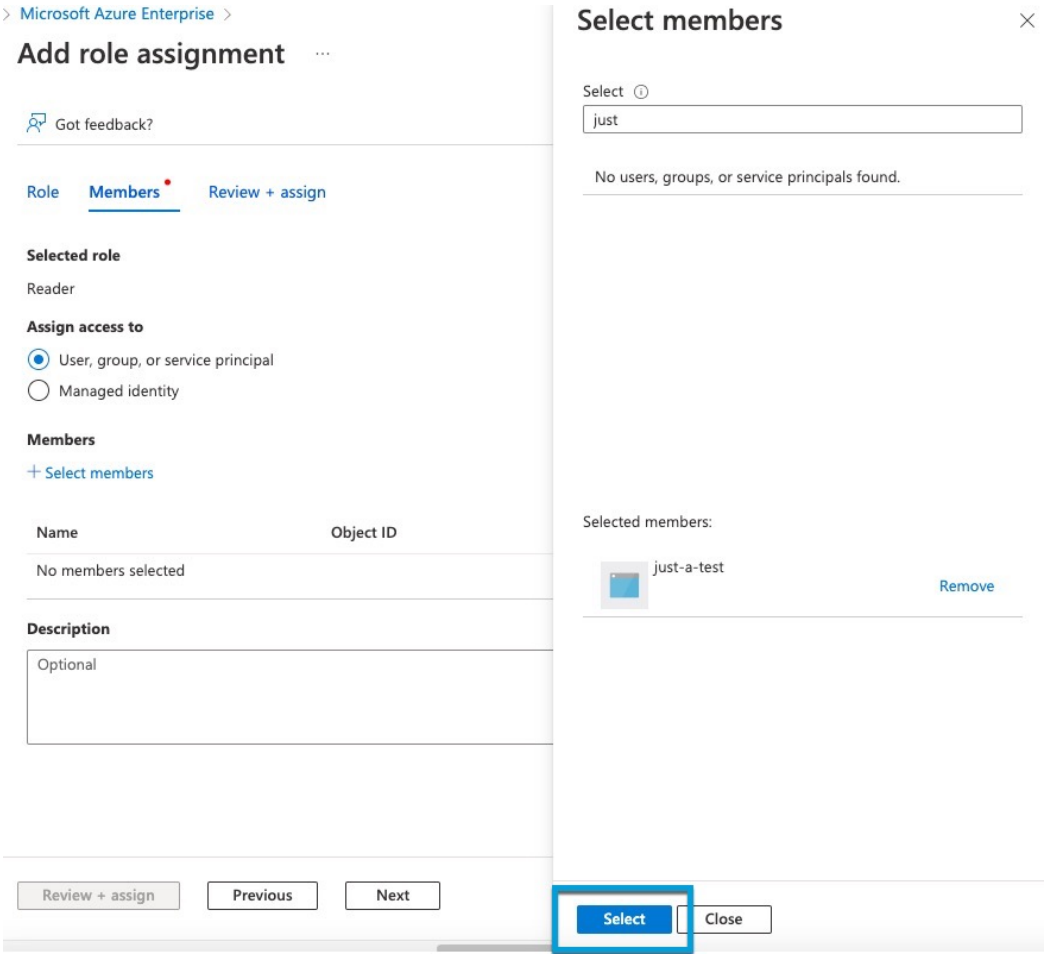
단계 **16** **Access Control (IAM)(**액세스 제어**(IAM))**를 클릭합니다.

단계 **17** **Add(**추가**)** > **Add role assignment(**역할 할당 추가**)**를 클릭합니다.

단계 **18** **Reader(**판독기**)**를 클릭하고 **Next(**다음**)**를 클릭합니다.

단계 **19** **Select Members(**구성원 선택**)**를 클릭합니다.

단계 **20** 페이지 오른쪽에서 등록한 앱의 이름을 클릭하고 **Select(**선택**)**를 클릭합니다.



단계 **21** **Review + Assign(**검토 + 할당**)**을 클릭하고 프롬프트에 따라 작업을 완료합니다.

다음에 수행할 작업

Azure 커넥터 생성, 20 페이지의 내용을 참조하십시오.

Azure 커넥터 생성

이 작업에서는 액세스 제어 정책에 사용하기 위해 Azure에서 management center로 데이터를 전송하는 커넥터를 생성하는 방법을 설명합니다.

시작하기 전에

Cisco Secure Dynamic Attributes Connector에 대한 최소 권한이 있는 Azure 사용자 생성, 18 페이지에 설명된 권한 이상의 Azure 사용자를 생성합니다.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(통합)** > **Cisco Dynamic Attributes Connector(Cisco 동적 속성 커넥터)** 버튼을 클릭합니다.

단계 **3** **Connector(커넥터)**를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 아이콘 추가( )을 클릭한 다음 커넥터의 이름을 클릭합니다.
- 커넥터 편집 또는 삭제: 추가 ( )을 클릭한 다음 행의 끝에서 **Edit(편집)** 또는 **Delete(삭제)**를 클릭합니다.

단계 **5** 다음 정보를 입력합니다.

값	설명
이름	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
설명	선택적 설명.
Pull Interval(끌어오기 간격)	(기본값 30초) Azure에서 IP 매핑을 검색하는 간격입니다.
Subscription Id(구독 ID)	(필수) Azure 구독 ID를 입력합니다.
Tenant Id(테넌트 ID)	(필수) 테넌트 ID를 입력합니다.
Client Id(클라이언트 ID)	(필수) 클라이언트 ID를 입력합니다.
Client Secret(클라이언트 비밀번호)	(필수) 클라이언트 암호를 입력합니다.

단계 **6** **Save(저장)**를 클릭합니다.

단계 **7** Status(상태) 열에 **Ok(확인)**가 표시되는지 확인합니다.

Azure 서비스 태그 커넥터 생성

이 항목에서는 액세스 제어 정책에서 사용하기 위해 management center에 연결할 Azure 서비스 태그용 커넥터를 생성하는 방법을 설명합니다. 이러한 태그와의 IP 주소 연결은 Microsoft에서 매주 업데이트합니다.

자세한 내용은 Microsoft TechNet의 가상 네트워크 서비스 태그를 참조하십시오.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)** 버튼을 클릭합니다.

단계 **3** **Connector(**커넥터**)**를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 아이콘 추가(+)을 클릭한 다음 커넥터의 이름을 클릭합니다.
- 커넥터 편집 또는 삭제: 추가 (⋮)을 클릭한 다음 행의 끝에서 **Edit(**편집**)** 또는 **Delete(**삭제**)**를 클릭합니다.

단계 **5** 다음 정보를 입력합니다.

값	설명
이름	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
설명	선택적 설명.
Pull Interval(끌어오기 간격**)**	(기본값 30초) Azure에서 IP 매핑을 검색하는 간격입니다.
Subscription Id(구독 **ID)**	(필수) Azure 구독 ID를 입력합니다.
Tenant Id(테넌트 **ID)**	(필수) 테넌트 ID를 입력합니다.
Client Id(클라이언트 **ID)**	(필수) 클라이언트 ID를 입력합니다.
Client Secret(클라이언트 비밀번호**)**	(필수) 클라이언트 암호를 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** Status(상태) 열에 **Ok(**확인**)**가 표시되는지 확인합니다.

일반 텍스트 커넥터 생성

이 작업은 수동으로 유지하고 선택한 간격(기본값은 30초)으로 검색할 IP 주소의 임시 목록을 생성하는 방법을 설명합니다. 언제든지 원할 때 주소 목록을 업데이트할 수 있습니다.

시작하기 전에

IP 주소가 포함된 텍스트 파일을 생성하여 management center에서 액세스할 수 있는 웹 서버에 배치합니다. IP 주소는 CIDR 표기법을 포함할 수 있습니다. 텍스트 파일에는 줄당 IP 주소가 하나만 있어야 합니다.

텍스트 파일당 최대 10,000개의 IP 주소를 지정할 수 있습니다.

참고 IP 주소에 체계(**`http://`** 또는 **`https://`**)를 포함하지 마십시오.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(통합)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)** 버튼을 클릭합니다.

단계 **3** **Connector(커넥터)**를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 아이콘 추가( )을 클릭한 다음 커넥터의 이름을 클릭합니다.
- 커넥터 편집 또는 삭제: 추가 ( )을 클릭한 다음 행의 끝에서 **Edit(편집)** 또는 **Delete(삭제)**를 클릭합니다.

단계 **5** **Name(이름)**과 선택적 설명을 입력합니다.

단계 **6** (선택 사항). **Pull Interval(끌어오기 간격)** 필드에서 동적 속성 커넥터가 GitHub에서 IP 주소를 검색하는 빈도를 초 단위로 변경합니다. 기본값은 30초입니다.

단계 **7** **URLs(URL)** 필드에 IP 주소를 검색할 각 URL을 한 줄에 하나씩 입력합니다.

단계 **8** (선택 사항). 웹 서버에 대한 보안 연결을 위해 인증서 체인이 필요한 경우 다음과 같은 방법을 사용할 수 있습니다.

- **Get Certificate(인증서 가져오기)** > **Fetch(가져오기)**를 클릭하여 인증서를 자동으로 가져오거나, 불가능할 경우 CA(Certificate Authority) 체인 수동으로 가져오기, 36 페이지에 설명된 대로 수동으로 인증서를 가져옵니다.
- 이전에 다운로드한 인증서 체인을 업로드하려면 **Get Certificate(인증서 가져오기)** > **Browse from file(파일에서 찾아보기)**를 클릭합니다.

단계 **9** 커넥터를 저장하기 전에 **Test(테스트)**를 클릭하고 테스트가 성공했는지 확인합니다.

단계 **10** **Save(저장)**를 클릭합니다.

단계 **11** Status(상태) 열에 **Ok(확인)**가 표시되는지 확인합니다.

GitHub 커넥터 생성

이 섹션에서는 액세스 제어 정책에서 사용하기 위해 management center에 데이터를 전송하는 GitHub 커넥터를 생성하는 방법을 설명합니다. 이러한 태그와 연결된 IP 주소는 GitHub에서 유지 관리합니다. 동적 속성 필터를 생성할 필요가 없습니다.

자세한 내용은 GitHub의 IP 주소 정보를 참조하십시오.

참고 URL을 변경하면 IP 주소를 검색할 수 없으므로 URL을 변경하지 마십시오.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)** 버튼을 클릭합니다.

단계 **3** **Connector(**커넥터**)**를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 아이콘 추가()을 클릭한 다음 커넥터의 이름을 클릭합니다.
- 커넥터 편집 또는 삭제: 추가 ()을 클릭한 다음 행의 끝에서 **Edit(**편집**)** 또는 **Delete(**삭제**)**를 클릭합니다.

단계 **5** **Name(**이름**)**과 선택적 설명을 입력합니다.

단계 **6** (선택 사항). **Pull Interval(**끌어오기 간격**)** 필드에서 동적 속성 커넥터가 GitHub에서 IP 주소를 검색하는 빈도를 초 단위로 변경합니다. 기본값은 21,600초(6시간)입니다,

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** Status(상태) 열에 **Ok(**확인**)**가 표시되는지 확인합니다.

Google Cloud Connector - 사용자 권한 및 가져온 데이터 정보

Cisco Secure Dynamic Attributes Connector는 액세스 제어 정책에 사용하기 위해 Google Cloud에서 management center로 동적 속성을 가져옵니다.

동적 속성 가져옴

Google Cloud에서 다음 동적 속성을 가져옵니다.

- Google Cloud 리소스를 구성하는 데 사용할 수 있는 키-값 쌍인 라벨입니다.

  자세한 내용은 Google Cloud 설명서에서 라벨 생성 및 관리를 참조하십시오.

- 조직, 폴더 또는 프로젝트와 연결된 키-값 쌍인 네트워크 태그입니다.

  자세한 내용은 Google Cloud 설명서에서 태그 생성 및 관리를 참조하십시오.

- Google Cloud에 있는 가상 머신의 *IP* 주소입니다.

최소 권한 필요

Cisco Secure Dynamic Attributes Connector에서 동적 속성을 가져오려면 최소한 기본 > 뷰어 권한이 있는 사용자가 필요합니다.

Cisco Secure Dynamic Attributes Connector에 대한 최소 권한이 있는 Google Cloud 사용자 생성

이 작업에서는 동적 속성을 management center로 전송할 수 있는 최소 권한으로 서비스 계정을 설정하는 방법을 설명합니다. 이러한 속성의 목록은 Google Cloud Connector - 사용자 권한 및 가져온 데이터 정보, 24 페이지 섹션을 참조하십시오.

시작하기 전에

Google Cloud 계정을 이미 설정했어야 합니다. 자세한 내용은 Google Cloud 설명서의 환경 설정을 참조하십시오.

프로시저

단계 **1** 소유자 역할의 사용자로 Google Cloud 계정에 로그인합니다.

단계 **2** **IAM & Admin(IAM** 및 관리자**)** > **Service Accounts(**서비스 계정**)** > **Create Service Account(**서비스 계정 생성**)**를 클릭합니다.

단계 **3** 다음 정보를 입력합니다.

- **Service account name(**서비스 계정 이름**)**: 이 계정을 식별하기 위한 이름입니다. 예를 들면 **CSDAC** 입니다.
- **Service account ID(**서비스 계정 **ID)**: 서비스 계정 이름을 입력한 후 고유한 값으로 채워져야 합니다.
- **Service account description(**서비스 계정 설명**)**: 선택적 설명을 입력합니다.

서비스 계정에 대한 자세한 내용은 Google Cloud 설명서의 서비스 계정 이해를 참조하십시오.

단계 **4** **Create and Continue(**생성 후 계속**)**를 클릭합니다.

단계 **5** Grant users access to this service account(이 서비스 계정에 대한 사용자 액세스 권한 부여) 섹션이 표시될 때까지 화면의 프롬프트를 따릅니다.

단계 **6** 사용자에게 **Basic(**기본**)** > **Viewer(**뷰어**)** 역할을 부여합니다.

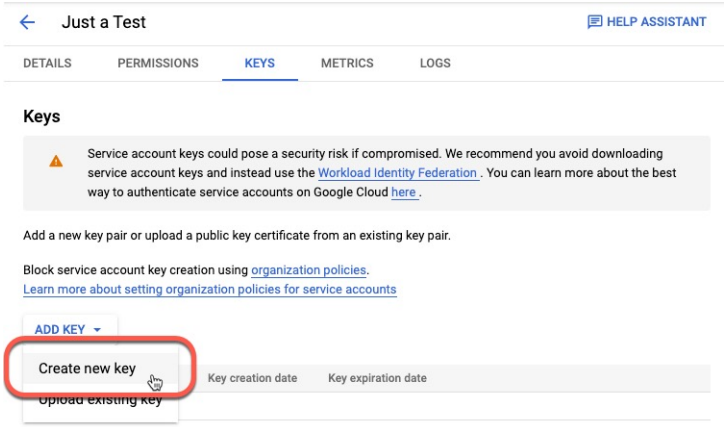
단계 **7** **Done(**완료**)**을 클릭합니다.

서비스 계정 목록이 표시됩니다.

단계 **8** 생성한 서비스 계정의 행 끝에서 추가 (⋮)을 클릭합니다.

단계 **9** **Manage Keys(**키 관리**)**를 클릭합니다.

단계 **10** **Add Key(**키 추가**)** > **Create New Key(**새 키 생성**)**를 클릭합니다.



단계 **11** **JSON**을 클릭합니다.

단계 **12** **Create(**생성**)**를 클릭합니다.

JSON 키가 컴퓨터에 다운로드됩니다.

단계 **13** GCP 커넥터를 구성할 때 키를 잘 보관하십시오.

다음에 수행할 작업

Google Cloud 커넥터 생성, 26 페이지의 내용을 참조하십시오.

Google Cloud 커넥터 생성

시작하기 전에

Google Cloud JSON 형식의 서비스 계정 데이터를 준비합니다. 이는 커넥터를 설정하는 데 필요합니다.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)** 버튼을 클릭합니다.

단계 **3** **Connector(**커넥터**)**를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 아이콘 추가(+)을 클릭한 다음 커넥터의 이름을 클릭합니다.
- 커넥터 편집 또는 삭제: 추가 (⋮)을 클릭한 다음 행의 끝에서 **Edit(**편집**)** 또는 **Delete(**삭제**)**를 클릭합니다.

단계 **5** 다음 정보를 입력합니다.

값	설명
이름	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
설명	선택적 설명.
Pull Interval(끌어오기 간격**)**	(기본값 30초) AWS에서 IP 매핑을 검색하는 간격입니다.
GCP region(GCP 지역**)**	(필수) Google Cloud가 있는 GCP 지역을 입력합니다. 자세한 내용은 Google Cloud 설명서에서 지역 및 영역을 참조하십시오.
Service account(서비스 계정**)**	Google Cloud 서비스 계정의 JSON 코드를 붙여넣습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** Status(상태) 열에 **Ok(**확인**)**가 표시되는지 확인합니다.

Office 365 커넥터 생성

이 작업에서는 액세스 제어 정책에서 사용하기 위해 management center에 데이터를 전송하기 위한 Office 365 태그용 커넥터를 생성하는 방법을 설명합니다. 이러한 태그와 연결된 IP 주소는 Microsoft에서 매주 업데이트합니다. 데이터를 사용하기 위해 동적 속성 필터를 만들 필요는 없습니다.

자세한 내용은 docs.microsoft.com에서 Office 365 URL 및 IP 주소 범위를 참조하십시오.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)** 버튼을 클릭합니다.

단계 **3** **Connector(**커넥터**)**를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 아이콘 추가(+)을 클릭한 다음 커넥터의 이름을 클릭합니다.
- 커넥터 편집 또는 삭제: 추가 (⋮)을 클릭한 다음 행의 끝에서 **Edit(**편집**)** 또는 **Delete(**삭제**)**를 클릭합니다.

단계 **5** 다음 정보를 입력합니다.

값	설명
이름	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
설명	선택적 설명.

값	설명
Pull Interval(끌어오기 간격**)**	(기본값 30초) Azure에서 IP 매핑을 검색하는 간격입니다.
Base API URL(기본 **API URL)**	(필수) 기본값과 다른 경우 Office 365 정보를 검색할 URL을 입력합니다. 자세한 내용은 Microsoft 설명서 사이트에서 Office 365 IP 주소 및 URL 웹 서비스를 참조하십시오.
Instance name(인스턴스 이름**)**	(필수) 목록에서 인스턴스 이름을 클릭합니다. 자세한 내용은 Microsoft 설명서 사이트에서 Office 365 IP 주소 및 URL 웹 서비스를 참조하십시오.
Disable optional IPs(선택적 **IP** 비활성화**)**	(필수) **true** 또는 **false**을 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** Status(상태) 열에 **Ok(**확인**)**가 표시되는지 확인합니다.

vCenter 커넥터 - 사용자 권한 및 가져온 데이터 정보

Cisco Secure Dynamic Attributes Connector는 액세스 제어 정책에 사용하기 위해 동적 속성을 vCenter에서 management center로 가져옵니다.

동적 속성 가져옴

vCenter에서 다음 동적 속성을 가져옵니다.

- 운영 체제
- *MAC* 주소
- *IP* 주소
- *NSX* 태그

최소 권한 필요

Cisco Secure Dynamic Attributes Connector에서 동적 속성을 가져오려면 최소한 읽기 전용 권한이 있는 사용자가 필요합니다.

vCenter 커넥터 생성

이 작업에서는 VMware vCenter용 커넥터를 생성하여 액세스 제어 정책에서 사용하기 위해 management center에 데이터를 전송하는 방법을 설명합니다.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(통합)** > **Cisco Dynamic Attributes Connector(Cisco 동적 속성 커넥터)** 버튼을 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

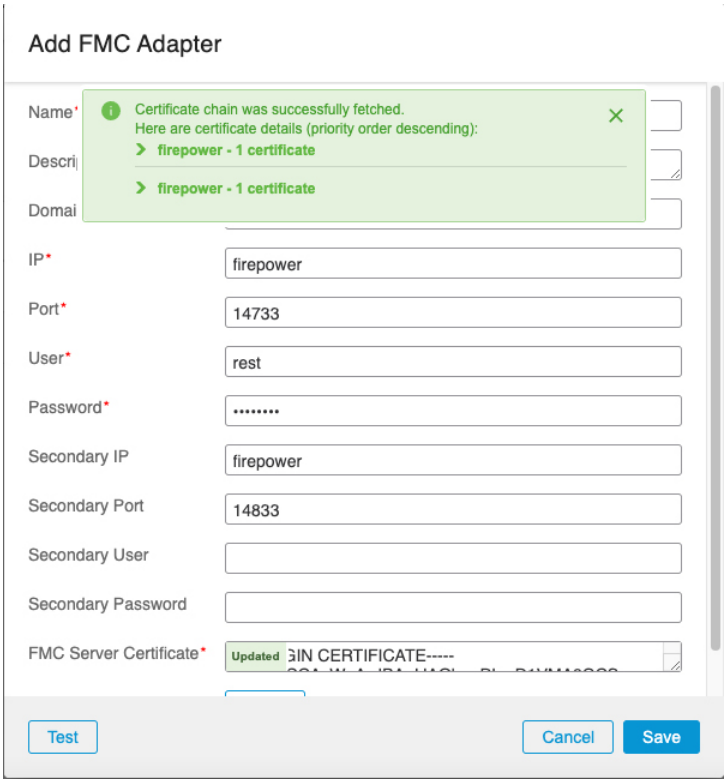
- 새 커넥터 추가: 아이콘 추가(+)을 클릭한 다음 커넥터의 이름을 클릭합니다.
- 커넥터 편집 또는 삭제: 추가 (⋮)을 클릭한 다음 행의 끝에서 **Edit(편집)** 또는 **Delete(삭제)**를 클릭합니다.

단계 **4** 다음 정보를 입력합니다.

값	설명
이름	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
설명	필요에 따라 설명을 입력합니다.
Pull Interval(끌어오기 간격)	(기본값 30초) vCenter에서 IP 매핑을 검색하는 간격입니다.
Host(호스트)	(필수) 다음을 입력합니다. • vCenter의 정규화된 호스트 이름 • vCenter IP 주소 • (선택 사항). 포트 체계(예: **`https://`**) 또는 후행 슬래시를 입력하지 마십시오. 예: **`myvcenter.example.com`** 또는 **`192.0.2.100:9090`**
User(사용자)	(필수) 최소한 읽기 전용 역할이 있는 사용자의 사용자 이름을 입력합니다. 사용자 이름은 대/소문자를 구분합니다.
Password(비밀번호)	(필수) 사용자의 비밀번호를 입력합니다.
NSX IP	vCenter NSX(Network Security Visualization)를 사용하는 경우 IP 주소를 입력합니다.
NSX User(NSX 사용자)	최소 감사자 역할이 있는 NSX 사용자의 사용자 이름을 입력합니다.
NSX Type(NSX 유형)	**NSX-T**를 입력합니다.
NSX Password(NSX 비밀번호)	NSX 사용자의 비밀번호를 입력합니다.

값	설명
vCenter Certificate(vCenter 인증서)	다음과 같은 옵션이 있습니다. • CA(Certificate Authority) 체인 수동으로 가져오기, 36 페이지에서 설명한 대로 가져온 CA(인증 기관) 체인을 붙여넣습니다. • **Fetch(**가져오기**)**를 클릭하여 인증서를 자동으로 가져오거나, 불가능할 경우 CA(Certificate Authority) 체인 수동으로 가져오기, 36 페이지에 설명된 대로 수동으로 인증서를 가져옵니다. • **Get Certificate(**인증서 가져오기**)** > **Fetch(**가져오기**)**를 클릭하여 인증서를 자동으로 가져오거나, 불가능할 경우 CA(Certificate Authority) 체인 수동으로 가져오기, 36 페이지에 설명된 대로 수동으로 인증서를 가져옵니다. • 이전에 다운로드한 인증서 체인을 업로드하려면 **Get Certificate(**인증서 가져오기**)** > **Browse from file(**파일에서 찾아보기**)**를 클릭합니다.

다음은 인증서 체인을 성공적으로 가져오는 예시입니다.



대화 상자 상단에서 인증서 CA 체인을 확장하면 다음과 유사한 인증서가 표시됩니다.

이 방법으로 인증서를 가져올 수 없는 경우 CA(Certificate Authority) 체인 수동으로 가져오기, 36 페이지에서 설명한 대로 인증서 체인을 수동으로 가져올 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Webex 커넥터 생성

이 섹션에서는 액세스 제어 정책에서 사용하기 위해 management center에 데이터를 전송하는 Webex 커넥터를 생성하는 방법을 설명합니다. 이러한 태그와 연결된 IP 주소는 Webex에서 유지 관리합니다. 동적 속성 필터를 생성할 필요가 없습니다.

자세한 내용은 Webex 호출을 위한 포트 참조를 참고하십시오.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)** 버튼을 클릭합니다.

단계 **3** **Connector(**커넥터**)**를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 아이콘 추가(+)을 클릭한 다음 커넥터의 이름을 클릭합니다.
- 커넥터 편집 또는 삭제: 추가 (⋮)을 클릭한 다음 행의 끝에서 **Edit(**편집**)** 또는 **Delete(**삭제**)**를 클릭합니다.

단계 **5** 다음 정보를 입력합니다.

값	설명
이름	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
설명	선택적 설명.
Pull Interval(끌어오기 간격**)**	(기본값 30초) Webex에서 IP 매핑을 검색하는 간격입니다.
Provider Reserved IPs(공급자 예약 **IP)**	(필수) (필수) 예약된 IP 주소를 검색하려면 활성화합니다.

단계 **6** 커넥터를 저장하기 전에 **Test(**테스트**)**를 클릭하고 테스트가 성공했는지 확인합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** Status(상태) 열에 **Ok(**확인**)**가 표시되는지 확인합니다.

Zoom 커넥터 생성

이 섹션에서는 액세스 제어 정책에서 사용하기 위해 management center에 데이터를 전송하는 Zoom 커넥터를 생성하는 방법을 설명합니다. 이러한 태그와 연결된 IP 주소는 Zoom에서 유지 관리합니다. 동적 속성 필터를 생성할 필요가 없습니다.

자세한 내용은 Zoom 네트워크 방화벽 또는 프록시 서버 설정을 참고하십시오.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)** 버튼을 클릭합니다.

단계 **3** **Connector(**커넥터**)**를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 아이콘 추가(⊕)을 클릭한 다음 커넥터의 이름을 클릭합니다.
- 커넥터 편집 또는 삭제: 추가 (⋮)을 클릭한 다음 행의 끝에서 **Edit(**편집**)** 또는 **Delete(**삭제**)**를 클릭합니다.

단계 **5** 다음 정보를 입력합니다.

값	설명
이름	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
설명	선택적 설명.
Pull Interval(끌어오기 간격**)**	(기본값 30초) Zoom에서 IP 매핑을 검색하는 간격입니다.
Provider Reserved IPs(공급자 예약 **IP)**	(필수) 예약된 IP 주소를 검색하려면 활성화합니다.

단계 **6** 커넥터를 저장하기 전에 **Test(**테스트**)**를 클릭하고 테스트가 성공했는지 확인합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** Status(상태) 열에 **Ok(**확인**)**가 표시되는지 확인합니다.

동적 속성 필터 생성

Cisco Secure Dynamic Attributes Connector를 사용하여 정의하는 동적 속성 필터는 management center에서 액세스 제어 정책에서 사용할 수 있는 동적 개체로 표시됩니다. 예를 들어 재무 부서의 AWS 서버에 대한 액세스를 Microsoft Active Directory에 정의된 재무 그룹의 멤버로만 제한할 수 있습니다.

참고 Generic Text, Office 365, Azure Service Tags, Webex 또는 Zoom에 대한 동적 속성 필터는 생성할 수 없습니다. 이러한 유형의 클라우드 개체는 자체 IP 주소를 제공합니다.

액세스 제어 규칙에 대한 자세한 내용은 동적 속성 필터를 사용하여 액세스 제어 규칙 생성, 39 페이지의 내용을 참조하십시오.

시작하기 전에

커넥터 생성, 14 페이지

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(통합)** > **Cisco Dynamic Attributes Connector(Cisco 동적 속성 커넥터)** 버튼을 클릭합니다.

단계 **3** **Dynamic Attributes Filters(동적 속성 필터)**를 클릭합니다.

- 새 커넥터 추가: 아이콘 추가(+)을 클릭한 다음 커넥터의 이름을 클릭합니다.
- 커넥터 편집 또는 삭제: 추가 (⋮)을 클릭한 다음 행의 끝에서 **Edit(편집)** 또는 **Delete(삭제)**를 클릭합니다.

단계 **4** 다음 정보를 입력합니다.

항목	설명
이름	액세스 제어 정책 및 management center 개체 관리자(**External Attributes(외부 속성)** > **Dynamic Object(동적 개체)**)에서 동적 필터를 동적 개체로 식별하기 위한 고유한 이름입니다.
Connector(커넥터)	목록에서 사용할 커넥터의 이름을 클릭합니다.
Query(쿼리)	• 새 필터 추가: 아이콘 추가(+)을 클릭합니다. • 필터 편집 또는 삭제: 추가 (⋮)을 클릭한 다음 행의 끝에서 **Edit(편집)** 또는 **Delete(삭제)**를 클릭합니다.

단계 **5** 쿼리를 추가하거나 편집하려면 다음 정보를 입력합니다.

항목	설명
Key(키)	목록에서 키를 클릭합니다. 키는 커넥터에서 가져옵니다.
Operation(작업)	다음 중 하나를 클릭합니다. • 같음은 키를 값과 정확히 일치시킵니다. • 포함은 값의 일부가 일치하는 경우 키를 값과 일치시킵니다.
Values(값)	**Any(임의)** 또는 **All(모두)**을 클릭하고 목록에서 하나 이상의 값을 클릭합니다. 쿼리에 값을 추가하려면 **Add another value(다른 값 추가)**를 클릭합니다.

단계 **6** **Show Preview(미리보기 표시)**를 클릭하여 쿼리에서 반환된 네트워크 또는 IP 주소 목록을 표시합니다.

단계 **7** 모두 마쳤으면 **Save(저장)**를 클릭합니다.

단계 **8** (선택 사항). management center에서 동적 개체를 확인합니다.

a) 최소한 네트워크 관리자 역할이 있는 사용자로 management center에 로그인합니다.

b) **Objects(개체)** > **Object Management(개체 관리)**를 클릭합니다.

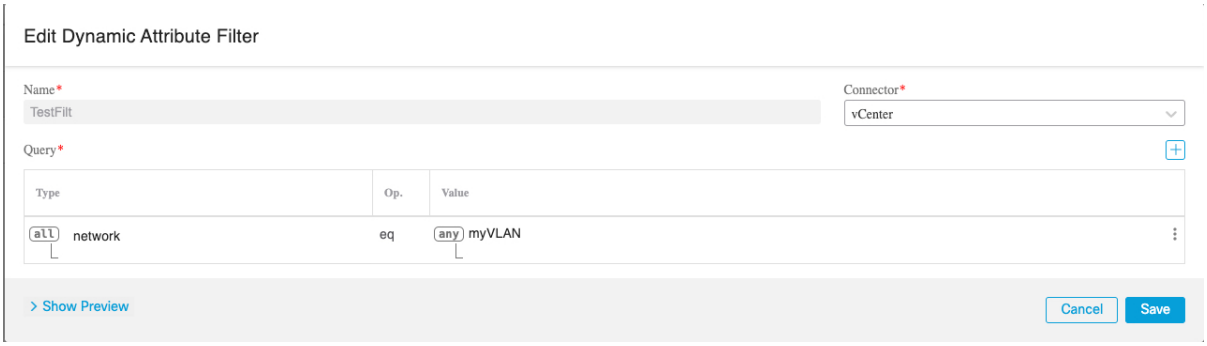
c) 왼쪽 창에서 **External Attributes(외부 속성)** > **Dynamic Object(동적 개체)**를 클릭합니다. 생성한 동적 속성 쿼리는 동적 개체로 표시되어야 합니다.

동적 속성 필터 예

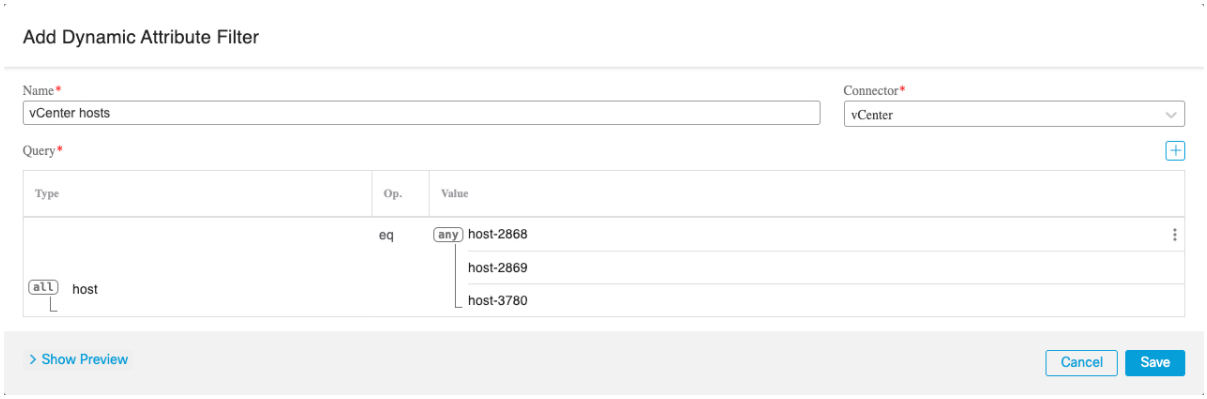
이 항목에서는 동적 속성 필터를 설정하는 몇 가지 예를 제공합니다.

예: vCenter

다음 예에서는 VLAN이라는 하나의 기준을 보여줍니다.

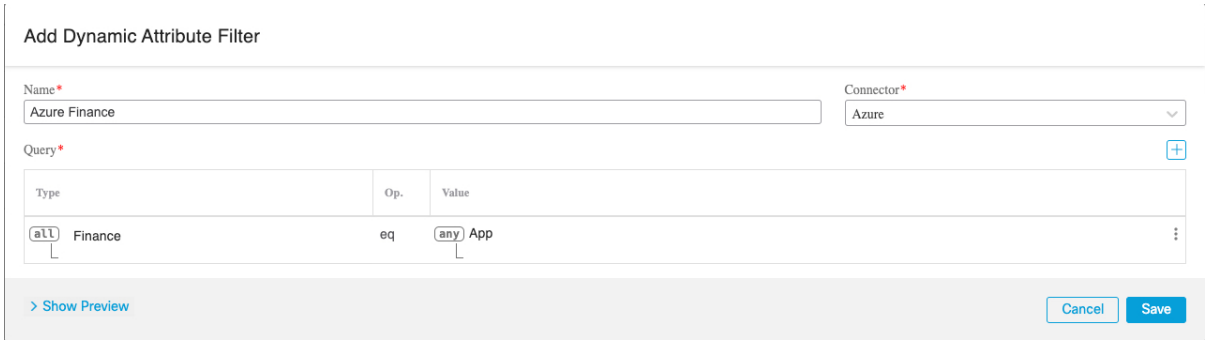


다음 예는 OR로 조인된 3개의 기준을 보여줍니다. 쿼리는 3개의 호스트 중 하나와 일치합니다.



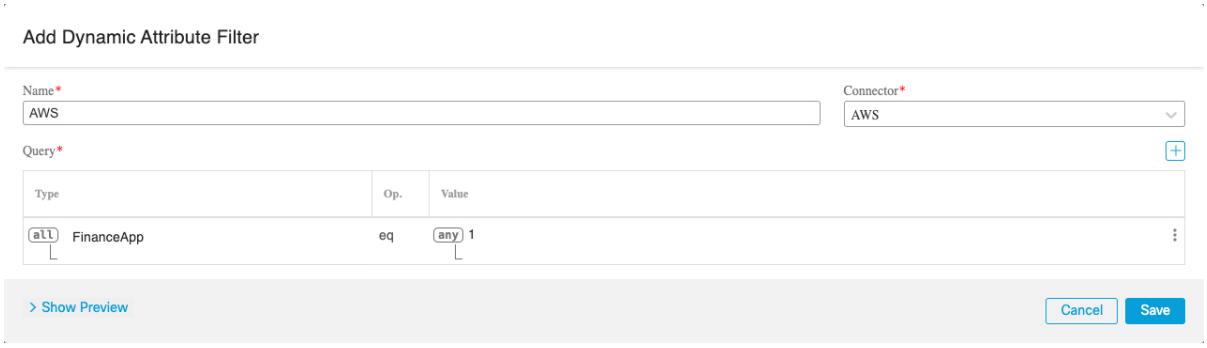
예: **Azure**

다음 예는 하나의 기준, 즉 금융 앱으로 태그가 지정된 서버를 보여줍니다.



예: **AWS**

다음 예는 하나의 기준, 즉 값이 1인 금융 앱을 보여줍니다.



CA(Certificate Authority) 체인 수동으로 가져오기

인증 기관 체인을 자동으로 가져올 수 없는 경우 다음 브라우저별 절차 중 하나를 사용하여 vCenter, NSX 또는 Management Center에 안전하게 연결하는 데 사용되는 인증서 체인을 가져옵니다.

인증서 체인은 루트 인증서 및 모든 하위 인증서입니다.

다음 절차 중 하나를 사용하여 다음에 연결해야 합니다.

- vCenter 또는 NSX

  Azure 또는 AWS에 연결하기 위해 인증서 체인을 가져올 필요는 없습니다.

- Management Center

인증서 체인 가져오기 - Mac(Chrome 및 Firefox)

Mac OS에서 Chrome 및 Firefox 브라우저를 사용하여 인증서 체인을 가져오려면 이 절차를 수행합니다.

1. 터미널 창을 엽니다.
2. 다음 명령을 입력합니다.

   ```
   security verify-cert -P url[:port]
   ```

   여기서 URL은 vCenter 또는 Management Center에 대한 URL(구성표 포함)입니다. 예를 들면 다음과 같습니다.

   ```
   security verify-cert -P https://myvcenter.example.com
   ```

   NAT 또는 PAT를 사용하여 vCenter 또는 management center에 액세스하는 경우 다음과 같이 포트를 추가할 수 있습니다.

   ```
   security verify-cert -P https://myvcenter.example.com:12345
   ```

3. 전체 인증서 체인을 일반 텍스트 파일로 저장합니다.
   - 모든-----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 구분 기호를 포함합니다.
   - 관련 없는 텍스트(예: 인증서의 이름 및 꺾쇠괄호(< 및 >)에 포함된 텍스트 및 꺾쇠괄호 자체)는 제외합니다.
4. vCenter 및 Management Center 둘 다에 대해 이 작업을 반복합니다.

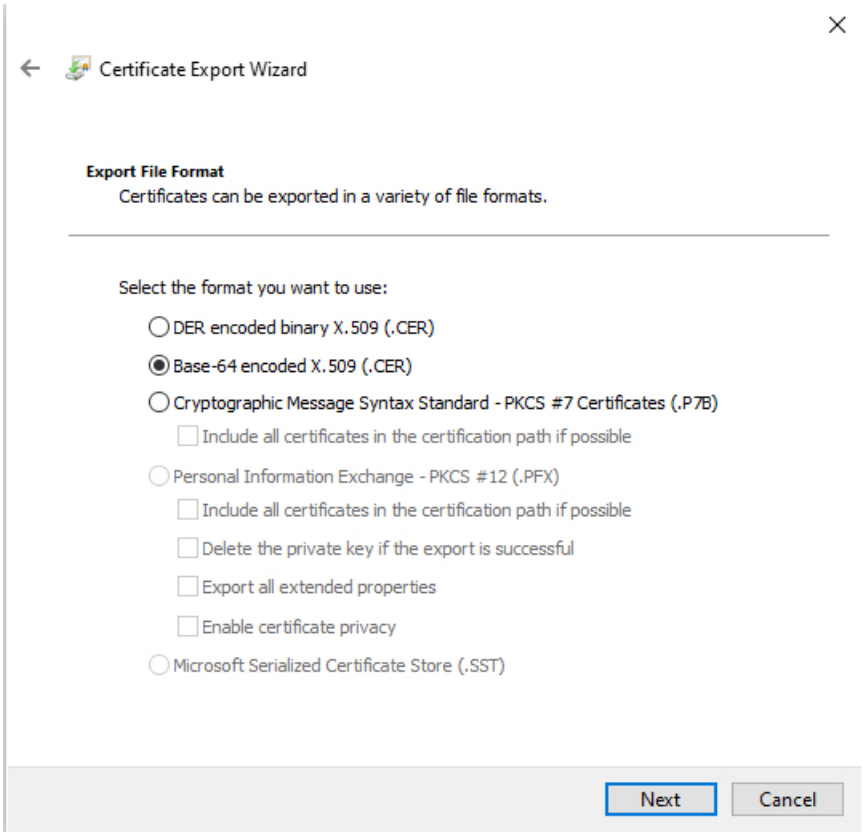
인증서 체인 가져오기 - Windows Chrome

Windows에서 Chrome 브라우저를 사용하여 인증서 체인을 가져오려면 이 절차를 사용합니다.

1. Chrome을 사용하여 vCenter 또는 Management Center에 로그인합니다.
2. 브라우저 주소 표시줄에서 호스트 이름 왼쪽의 잠금을 클릭합니다.
3. **Certificate(**인증서**)**를 클릭합니다.

4. **Certificate Path(**인증서 경로**)** 탭을 클릭합니다.
5. 체인에서 상위(즉, 첫 번째) 인증서를 클릭합니다.
6. **View Certificate(**인증서 보기**)**를 클릭합니다.
7. **Details(**세부 정보**)** 탭을 클릭합니다.
8. **Copy to File(**파일에 복사**)**을 클릭합니다.
9. 프롬프트에 따라 전체 인증서 체인을 포함하는 CER 형식의 인증서 파일을 생성합니다.

   내보내기 파일 형식을 선택하라는 메시지가 표시되면 다음 그림에 나와 있는 것처럼 **Base 64-Encoded X.509 (.CER)**를 클릭합니다.



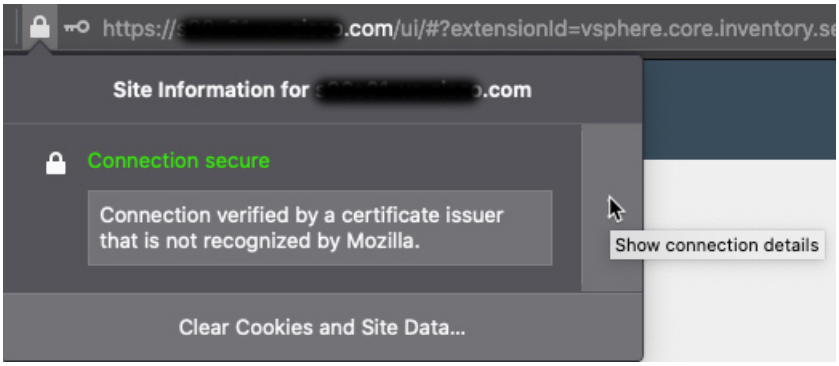
10. 프롬프트에 따라 내보내기를 완료합니다.
11. 텍스트 편집기에서 인증서를 엽니다.
12. 체인의 모든 인증서에 대해 프로세스를 반복합니다.

    텍스트 편집기에서 각 인증서를 맨 처음부터 마지막 순서로 붙여넣어야 합니다.
13. vCenter와 FMC 모두에 대해 이 작업을 반복합니다.

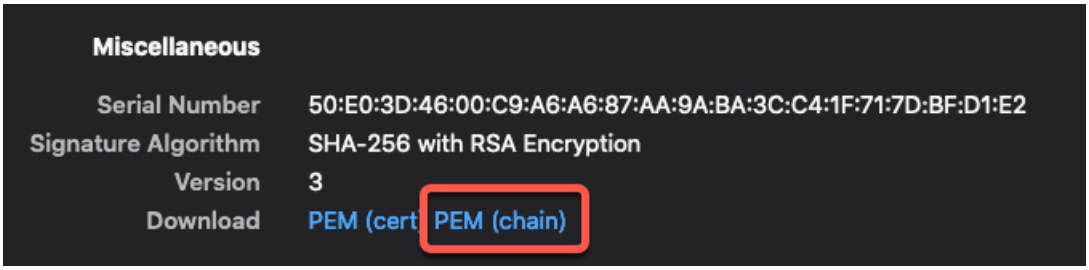
인증서 체인 가져오기 - Windows Firefox

Windows 또는 Mac OS에서 Firefox 브라우저에 대한 인증서 체인을 가져오려면 다음 절차를 사용합니다.

1. Firefox를 사용하여 vCenter 또는 Management Center에 로그인합니다.
2. 호스트 이름 왼쪽의 잠금을 클릭합니다.
3. 오른쪽 화살표(**Show connection details(**연결 세부 정보 표시**)**)를 클릭합니다. 다음 그림은 예를 보여줍니다.



4. **More Information(**추가 정보**)**을 클릭합니다.
5. **View Certificate(**인증서 보기**)**를 클릭합니다.
6. 결과 대화 상자에 탭 페이지가 있으면 최상위 CA에 해당하는 탭 페이지를 클릭합니다.
7. Miscellaneous(기타) 섹션으로 스크롤합니다.
8. Download(다운로드) 행에서 **PEM (chain)(PEM(**체인**))**을 클릭합니다. 다음 그림은 예를 보여줍니다.



9. 파일을 저장하십시오.
10. vCenter 및 Management Center 둘 다에 대해 이 작업을 반복합니다.

액세스 제어 정책에서 동적 개체 사용

동적 속성 커넥터를 사용하면 액세스 제어 규칙에서 동적 개체로 표시되는 동적 필터를 management center에서 구성할 수 있습니다.

액세스 제어 규칙의 동적 개체 정보

커넥터를 생성하고 커넥터에 동적 속성 필터를 저장하면 동적 개체가 동적 속성 커넥터에서 Secure Firewall Manager로 자동으로 푸시됩니다.

액세스 제어 규칙의 Dynamic Attributes(동적 속성) 탭 페이지에서 동적 개체를 사용할 수 있으며, 이는 SGT(Security Group Tags)를 사용한 것과 유사합니다. 동적 개체를 소스 또는 대상 속성으로 추가할 수 있습니다. 예를 들어 액세스 제어 차단 규칙에서 재무 동적 개체를 대상 속성으로 추가하여 규칙의 다른 기준과 일치하는 모든 개체로 재무 서버에 대한 액세스를 차단할 수 있습니다.

참고 Generic Text, Office 365, Azure Service Tags, Webex 또는 Zoom에 대한 동적 속성 필터는 생성할 수 없습니다. 이러한 유형의 클라우드 개체는 자체 IP 주소를 제공합니다.

동적 속성 필터를 사용하여 액세스 제어 규칙 생성

이 주제에서는 동적 개체를 사용하여 액세스 제어 규칙을 생성하는 방법을 설명합니다.

프로시저

단계 **1** management center에 로그인합니다.

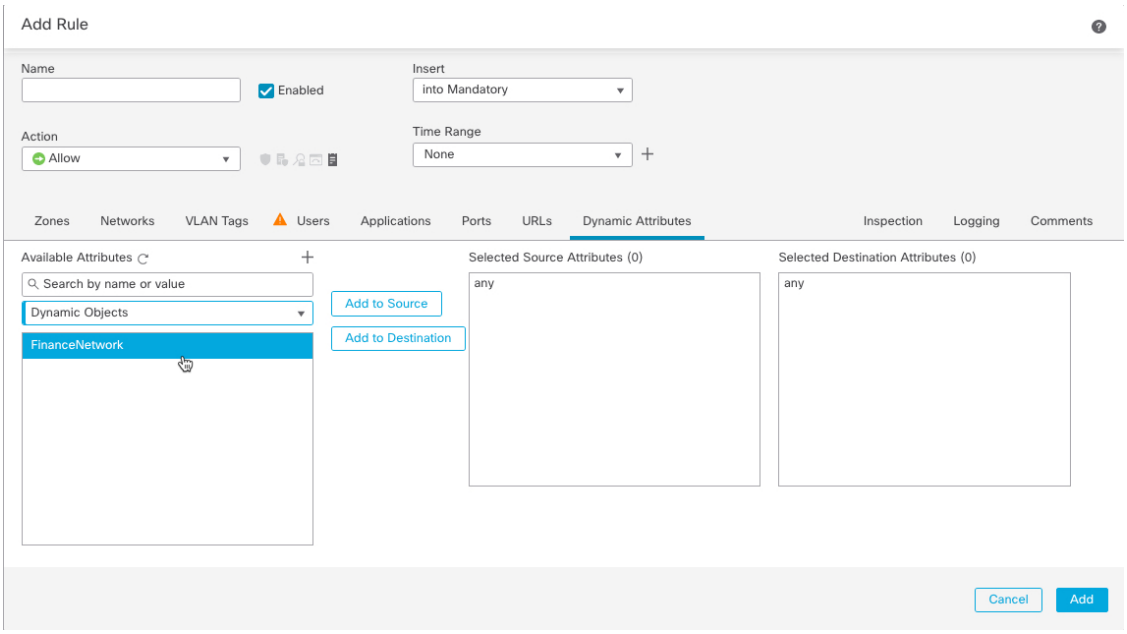
단계 **2** 액세스 제어 정책 옆에 있는 수정( )을 클릭합니다.

단계 **3** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **4** **Dynamic Attributes(**동적 속성**)** 탭을 클릭합니다.

단계 **5** Available Attributes(사용 가능한 속성) 섹션의 목록에서 **Dynamic Objects(**동적 개체**)**를 클릭합니다.

다음 그림은 예를 보여줍니다.



위의 예는 Cisco Secure Dynamic Attributes Connector에서 생성된 동적 속성 필터에 해당하는 `FinanceNetwork`라는 이름의 동적 개체를 보여줍니다.

단계 **6** 소스 또는 대상 속성에 원하는 개체를 추가합니다.

단계 **7** 원하는 경우 규칙에 다른 조건을 추가합니다.

다음에 수행할 작업

Cisco Secure Firewall Management Center 디바이스 구성 가이드의 액세스 제어 장(장에 대한 링크)

Cisco Secure Dynamic Attributes Connector 비활성화

클라우드 소스에서 동적 개체를 더 이상 수집하지 않으려면 다음 작업에서 설명하는 것과 같이 Cisco Secure Dynamic Attributes Connector에서 Secure Firewall Management Center를 비활성화할 수 있습니다.

프로시저

단계 **1** 아직 하지 않았다면 에 로그인합니다.Secure Firewall Management Center

단계 **2** **Integration(**통합**)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)** 버튼을 클릭합니다.

단계 **3** **Disabled(**비활성화**)**로 밉니다.

명령줄을 사용하여 문제 해결

Cisco에서는 고급 문제 해결을 지원하고 Cisco TAC를 사용하여 다음 문제 해결 툴을 제공합니다. 이러한 툴을 사용하려면 동적 속성 커넥터가 실행 중인 Ubuntu 호스트에 임의의 사용자로 로그인합니다.

컨테이너 상태 확인

동적 속성 커넥터 Docker 컨테이너 상태를 확인하려면 다음 명령을 입력합니다.

```
cd /usr/local/sf/csdac
sudo ./muster-cli status
```

샘플 출력은 다음과 같습니다.

```
================================================ CORE SERVICES
================================================
          Name                            Command               State                    Ports

-------------------------------------------------------------------------------------------------------------------
muster-bee                  /bin/sh -c /app/bee              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

muster-user-analysis       ./docker-entrypoint.sh run ...   Up      50070/tcp

============================ CONNECTORS AND ADAPTERS ============================
             Name                              Command               State     Ports
-------------------------------------------------------------------------------------
muster-connector-o365.1.muster   ./docker-entrypoint.sh run ...   Up      50070/tcp
```

동적 속성 커넥터 **Docker** 컨테이너 중지, 시작 또는 재시작

./muster-cli status에 컨테이너가 다운되었거나 문제 발생 시 컨테이너를 다시 시작하려는 경우 다음 명령을 입력할 수 있습니다.

정지 및 재시작:

```
cd ~/csdac/app
sudo ./muster-cli stop
sudo ./muster-cli start
```

시작만:

```
cd ~/csdac/app
sudo ./muster-cli start
```

애플리케이션 디버그 로깅 활성화 및 문제 해결 파일 생성

Cisco TAC에서 권장하는 경우 다음과 같이 디버그 로깅을 활성화하고 문제 해결 파일을 생성합니다.

```
cd ~/csdac/app
sudo ./muster-cli debug-on
sudo ./muster-cli ts-gen
```

문제 해결 파일 이름은 **ts-bundle-***timestamp***.tar**이며 동일한 디렉터리에 생성됩니다.

다음 표에는 문제 해결 파일 및 로그 파일의 위치가 나와 있습니다.

위치	포함 내용
/csdac/app/ts-bundle-*timestamp***/info**	`etcd` 데이터베이스 내용
/csdac/app/ts-bundle-*timestamp***/logs**	컨테이너 로그 파일
/csdac/app/ts-bundle-*timestamp***/status.log**	컨테이너 상태, 버전 및 이미지 상태

컨테이너에 대한 디버깅 활성화

다음과 같이 컨테이너의 이름을 먼저 가져온 경우 필요에 따라 개별 컨테이너에 대해 디버깅을 활성화할 수 있습니다.

```
cd /usr/local/sf/csdac
sudo ./muster-cli versions
```

샘플 출력은 다음과 같습니다.

```
CSDAC version: 1.0.0
CONTAINERS VERSIONS
CONTAINER                       | APP VERSION          | COMMIT
================================================================================
muster-bee                      | fmc7.4-13            |
944d50c6c384567693d6ecc5a31420de57f6ce2f
muster-envoy                    | fmc7.4-25            |
5e5f6d83164a4acbef5b106aa39e2e3f68fa738f
muster-local-fmc-adapter        | fmc7.4-17            |
c5902f818baa8e27d7c0b8027490dcacc28c0168
muster-ui-backend               | fmc7.4-64            |
165a1f5f0d763aa75829a30b5ffbddf0012682b6
muster-user-analysis            | fmc7.4-43            |
63cd64e29a92599908c3eb684d91e9f685d8c740
muster-connector-o365.1.muster | fmc7.4-8             |
28f075d315c8867f667b828970c9fbad35fa89cc
```

예를 들어, Office 365 커넥터에 대한 디버깅을 활성화하려면 다음 명령을 입력합니다.

```
sudo ./muster-cli container-debug-on muster-connector-o365.1.muster
```

해당 커넥터에 대한 디버깅을 비활성화하려면 다음 명령을 입력합니다.

```
sudo ./muster-cli container-debug-off muster-connector-o365.1.muster
```

동적 개체 확인

커넥터와 management center에서 개체를 생성하는지 확인하려면 management center에서 관리자로 다음 명령을 사용할 수 있습니다.

```
sudo tail f /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log
```

예: 성공적인 개체 생성

```
26-Aug-2021 12:41:35.912,[INFO],(DefenseCenterServiceImpl.java:1442)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-10
** REST Request [ CSM ]
```

```
** ID : 18b25356-fd6b-4cc4-8d27-bbccb52a6275
** URL: POST /audit
{
  "version": "7.1.0",
  "requestId": "18b25356-fd6b-4cc4-8d27-bbccb52a6275",
  "data": {
    "userName": "csdac-centos7",
    "subsystem": "API",
    "message": "POST
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f
/object/dynamicobjects Created (201) - The request has been fulfilled and resulted in a new
 resource being created",
    "sourceIP": "192.0.2.103",
    "domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time": "1629981695431"
  },
  "deleteList": []
}
```

Management Center를 사용하여 문제 해결

이 작업은 Secure Firewall Management Center의 문제 해결 파일을 생성하는 방법을 설명합니다.

시작하기 전에

문제 해결에 대한 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드의 문제 해결 장을 참조하십시오.

프로시저

단계 **1** Secure Firewall Management Center에 로그인합니다.

단계 **2** 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)** 버튼을 클릭합니다.

단계 **3** 왼쪽 창에서 **Firewall Management Center**를 클릭합니다.

단계 **4** 상단에서 **System and Troubleshooting Details(**시스템 및 문제 해결 세부 정보**)**를 클릭합니다.

단계 **5** **Generate Troubleshooting Files(**문제 해결 파일 생성**)**를 클릭합니다.

단계 **6** Cisco TAC 또는 베타 조정자에게 파일을 제공합니다.

CA(Certificate Authority) 체인 수동으로 가져오기

인증 기관 체인을 자동으로 가져올 수 없는 경우 다음 브라우저별 절차 중 하나를 사용하여 vCenter, NSX 또는 Management Center에 안전하게 연결하는 데 사용되는 인증서 체인을 가져옵니다.

인증서 체인은 루트 인증서 및 모든 하위 인증서입니다.

다음 절차 중 하나를 사용하여 다음에 연결해야 합니다.

- vCenter 또는 NSX

Azure 또는 AWS에 연결하기 위해 인증서 체인을 가져올 필요는 없습니다.

- Management Center

인증서 체인 가져오기 - Mac(Chrome 및 Firefox)

Mac OS에서 Chrome 및 Firefox 브라우저를 사용하여 인증서 체인을 가져오려면 이 절차를 수행합니다.

1. 터미널 창을 엽니다.
2. 다음 명령을 입력합니다.

   ```
   security verify-cert -P url[:port]
   ```

   여기서 URL은 vCenter 또는 Management Center에 대한 URL(구성표 포함)입니다. 예를 들면 다음과 같습니다.

   ```
   security verify-cert -P https://myvcenter.example.com
   ```

   NAT 또는 PAT를 사용하여 vCenter 또는 management center에 액세스하는 경우 다음과 같이 포트를 추가할 수 있습니다.

   ```
   security verify-cert -P https://myvcenter.example.com:12345
   ```

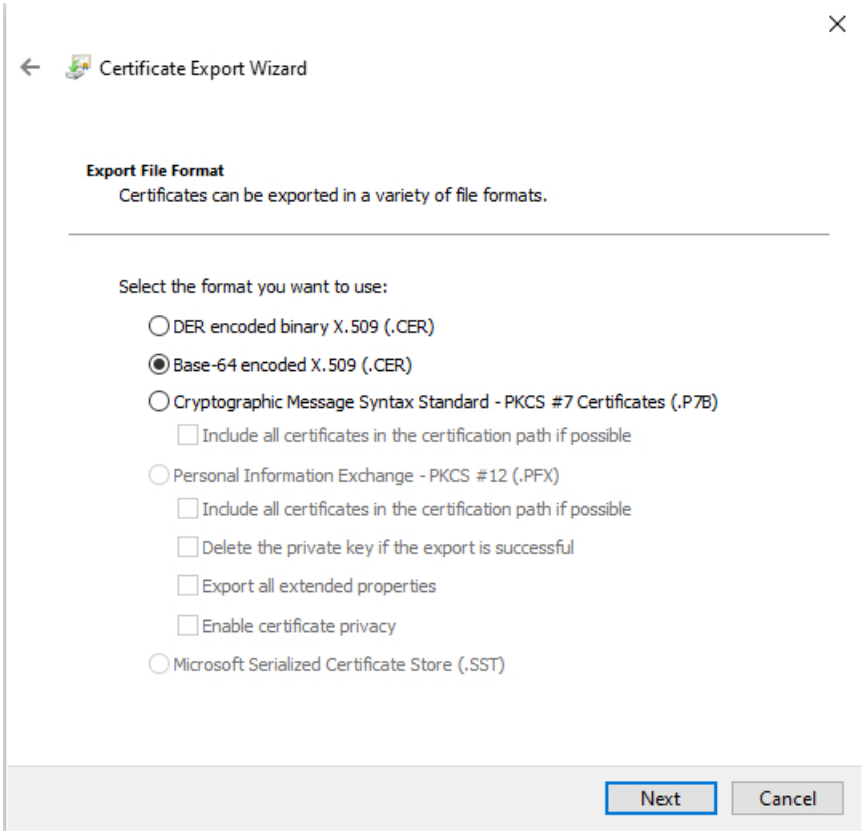
3. 전체 인증서 체인을 일반 텍스트 파일로 저장합니다.
   - 모든-----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 구분 기호를 포함합니다.
   - 관련 없는 텍스트(예: 인증서의 이름 및 꺾쇠괄호(< 및 >)에 포함된 텍스트 및 꺾쇠괄호 자체)는 제외합니다.
4. vCenter 및 Management Center 둘 다에 대해 이 작업을 반복합니다.

인증서 체인 가져오기 - Windows Chrome

Windows에서 Chrome 브라우저를 사용하여 인증서 체인을 가져오려면 이 절차를 사용합니다.

1. Chrome을 사용하여 vCenter 또는 Management Center에 로그인합니다.
2. 브라우저 주소 표시줄에서 호스트 이름 왼쪽의 잠금을 클릭합니다.
3. **Certificate(**인증서**)**를 클릭합니다.
4. **Certificate Path(**인증서 경로**)** 탭을 클릭합니다.
5. 체인에서 상위(즉, 첫 번째) 인증서를 클릭합니다.
6. **View Certificate(**인증서 보기**)**를 클릭합니다.
7. **Details(**세부 정보**)** 탭을 클릭합니다.
8. **Copy to File(**파일에 복사**)**을 클릭합니다.
9. 프롬프트에 따라 전체 인증서 체인을 포함하는 CER 형식의 인증서 파일을 생성합니다.

내보내기 파일 형식을 선택하라는 메시지가 표시되면 다음 그림에 나와 있는 것처럼 **Base 64-Encoded X.509 (.CER)**를 클릭합니다.



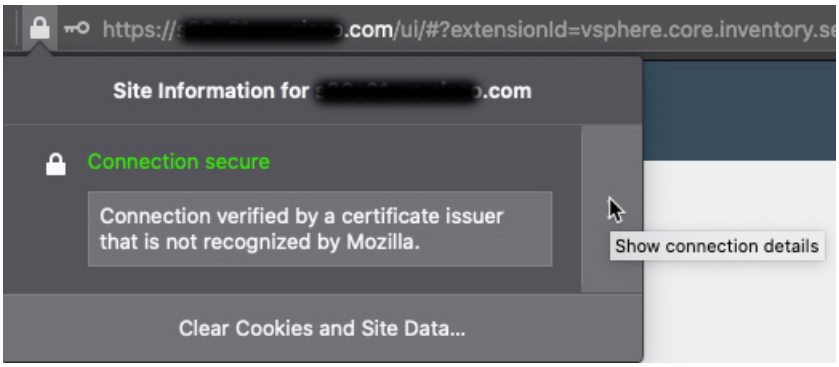
10. 프롬프트에 따라 내보내기를 완료합니다.
11. 텍스트 편집기에서 인증서를 엽니다.
12. 체인의 모든 인증서에 대해 프로세스를 반복합니다.

    텍스트 편집기에서 각 인증서를 맨 처음부터 마지막 순서로 붙여넣어야 합니다.
13. vCenter와 FMC 모두에 대해 이 작업을 반복합니다.

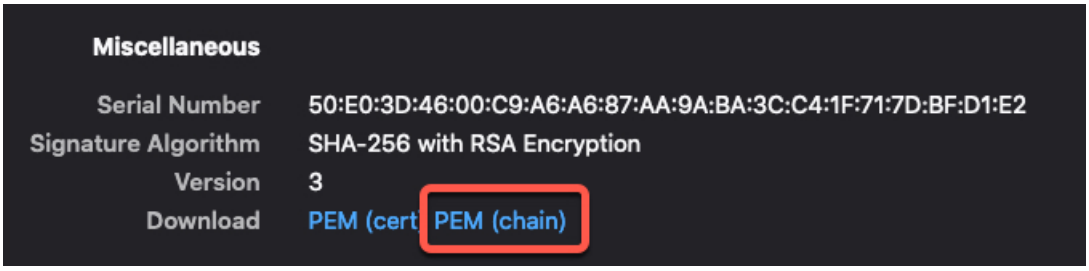
인증서 체인 가져오기 - Windows Firefox

Windows 또는 Mac OS에서 Firefox 브라우저에 대한 인증서 체인을 가져오려면 다음 절차를 사용합니다.

1. Firefox를 사용하여 vCenter 또는 Management Center에 로그인합니다.
2. 호스트 이름 왼쪽의 잠금을 클릭합니다.
3. 오른쪽 화살표(**Show connection details(**연결 세부 정보 표시**)**)를 클릭합니다. 다음 그림은 예를 보여줍니다.



4. **More Information(**추가 정보**)**을 클릭합니다.
5. **View Certificate(**인증서 보기**)**를 클릭합니다.
6. 결과 대화 상자에 탭 페이지가 있으면 최상위 CA에 해당하는 탭 페이지를 클릭합니다.
7. Miscellaneous(기타) 섹션으로 스크롤합니다.
8. Download(다운로드) 행에서 **PEM (chain)(PEM(**체인**))**을 클릭합니다. 다음 그림은 예를 보여줍니다.



9. 파일을 저장하십시오.
10. vCenter 및 Management Center 둘 다에 대해 이 작업을 반복합니다.

보안 요건

Cisco Secure Dynamic Attributes Connector를 보호하려면 보호된 내부 네트워크에 설치해야 합니다. 필요한 서비스와 사용 가능한 포트만 사용하도록 동적 속성 커넥터을 구성한 경우에도 공격이 모듈에 도달할 수 없는지 확인해야 합니다.

동적 속성 커넥터 및 management center가 동일한 네트워크에 상주하는 경우 management center를 동적 속성 커넥터와 동일한 보호된 내부 네트워크에 연결할 수 있습니다.

어플라이언스를 구축하는 방식과 상관없이 시스템 간 통신은 암호화됩니다. 하지만 DDoS(Distributed Denial of Service) 또는 중간자 공격(man-in-the-middle attack)등으로 어플라이언스 간 통신이 중단, 차단 또는 변조될 수 없도록 방지하는 단계를 수행해야 합니다.

인터넷 액세스 요구 사항

기본적으로 동적 속성 커넥터는 포트 443/tcp(HTTPS)에서 HTTPS를 사용하여 인터넷을 통해 Firepower System과 통신하도록 구성됩니다. 동적 속성 커넥터가 인터넷에 직접 액세스하지 않도록 하려면 프록시 서버를 구성할 수 있습니다.

다음 정보는 동적 속성 커넥터가 management center 및 외부 서버와 통신하는 데 사용되는 URL을 알려줍니다.

표 *3:* 동적 속성 커넥터 ***management center*** 액세스 요구 사항

URL	이유
https://*fmc-ip***/api/fmc_platform/v1/auth/generatetoken**	인증
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id***/object/dynamicobjects**	GET 및 POST 동적 개체
https://*fmc-ip***/api/fmc_config/ v1/domain/***domain-id***/object/dynamicobjects/***object-id***/mappings?action=add**	매핑 추가
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id*** /object/dynamicobjects/***object-id***/mappings?action=remove**	매핑 제거

표 *4:* 동적 속성 커넥터 ***vCenter*** 액세스 요구 사항

URL	이유
https://*vcenter-ip***/rest/com/vmware/cis/session**	인증
https://*vcenter-ip***/rest/vcenter/vm**	VM 정보 가져오기
https://*nsx-ip***/api/v1/fabric/virtual-machines/***vm-id***	가상 머신과 연결된 NSX-T 태그 가져오기

DockerHub에서 **Amazon ECR**로 마이그레이션

Cisco Secure Dynamic Attributes Connector의 도커 이미지는 Docker Hub에서 Amazon Elastic Container 레지스트리(Amazon ECR)로 마이그레이션되고 있습니다.

새 필드 패키지를 사용하려면 방화벽 또는 프록시를 통한 다음 모든 URL에 대한 액세스를 허용해야 합니다.

- https://public.ecr.aws
- https://csdac-cosign.s3.us-west-1.amazonaws.com

동적 속성 커넥터 **Azure** 액세스 요구 사항

동적 속성 커넥터는 내장된 SDK 메서드를 호출하여 인스턴스 정보를 가져옵니다. 이러한 메서드는 https://login.microsoft.com(인증용) 및 https://management.azure.com(인스턴스 정보 가져오기)을 내부적으로 호출합니다.

Cisco Secure Dynamic Attributes Connector 기록

기능	최소 **Management Center**	최소 **Threat Defense**	세부 사항
Cisco Secure Dynamic Attributes Connector	7.4.0	7.4.0	이 기능이 도입되었습니다. Cisco Secure Dynamic Attributes Connector이 이제 Secure Firewall Management Center에 포함됩니다. 동적 속성 커넥터를 사용하여 매니지드 디바이스에 구축할 필요 없이 액세스 제어 규칙에서 Microsoft Azure와 같은 클라우드 기반 플랫폼의 IP 주소를 가져올 수 있습니다. 추가 정보: • 이 제품이 포함된 동적 속성 커넥터:관련 정보 Cisco Secure Dynamic Attributes Connector, 1 페이지 • 독립형 동적 속성 커넥터: Cisco Secure Dynamic Attributes Connector 구성 가이드 신규/수정된 화면: **Integration(통합)** > **Cisco Dynamic Attributes Connector(Cisco** 동적 속성 커넥터**)**