Cisco Secure Dynamic Attributes Connector 구성

동적 속성 커넥터를 설치하고 액세스 제어 규칙에서 사용할 수 있는 동적 네트워크 데이터를 management center에 제공하기 위해 커넥터, 동적 속성 필터 및 어댑터를 구성합니다.

동적 속성 커넥터를 사용하면 액세스 제어 규칙에서 사용할 수 있는 동적 네트워크 데이터를 management center에 제공하도록 커넥터를 구성할 수 있습니다.

자세한 내용은 다음 항목을 참고하십시오.

- 커넥터 생성, 1 페이지
- 어댑터 생성, 17 페이지
- 동적 속성 필터 생성, 26 페이지

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 ***1: Cisco Secure Dynamic Attributes Connector*** 버전 및 플랫폼별 지원되는 커넥터 목록

CSDAC 버전/플랫폼	**AWS**	**Git-** 허브	**Google Cloud**	**Azure**	**Azure** 서비스 태그	**Microsoft Office 365**	**VMware vCenter**
버전 1.1(온프레미스)	예	아니요	아니요	예	예	예	예
버전 2.0(온프레미스)	예	예	예	예	예	예	예
클라우드 제공(Cisco Defense Orchestrator)	예	예	예	예	예	예	아니요

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 center(으)로 전송할 수 있는 최소 권한으로 서비스 계정을 설정하는 방법을 설명합니다. 이러한 속성의 목록은 Amazon Web Services Connector - 사용자 권한 및 가져온 데이터 정보, 2 페이지의 내용을 참조하십시오.

시작하기 전에

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

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.

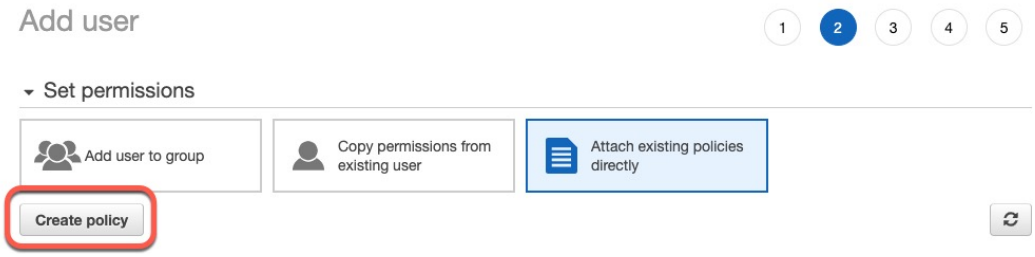
참고 이는 사용자의 키를 검색할 수 있는 유일한 기회입니다.

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, 3 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, 2 페이지에 설명된 권한 이상의 사용자를 생성합니다.

단계 1 동적 속성 커넥터에 로그인합니다.

단계 2 **Connector(**커넥터**)**를 클릭합니다.

단계 3 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 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
Name(이름**)**	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
Description(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 5 커넥터를 저장하기 전에 **Test(**테스트**)**를 클릭하고 테스트가 성공했는지 확인합니다.

단계 6 **Save(**저장**)**를 클릭합니다.

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

다음에 수행할 작업

어댑터 생성, 17 페이지

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, 4 페이지 섹션을 참조하십시오.

시작하기 전에

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

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.

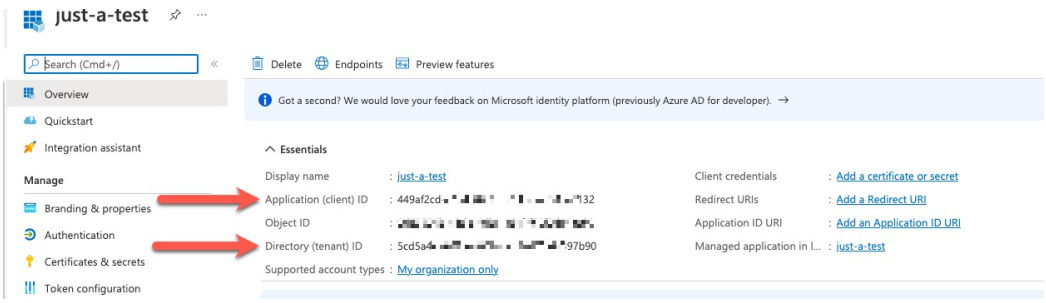
단계 **5** **Name(**이름**)** 필드에 이 애플리케이션을 식별하는 이름을 입력합니다.

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** **Add a 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** Azure Connector를 설정하는 데 필요하므로 클라이언트 값을 클립보드에 복사합니다.

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

단계 **14** 구독 ID를 클립 보드에 복사합니다.

단계 **15** 구독 페이지에서 구독의 이름을 클릭합니다.

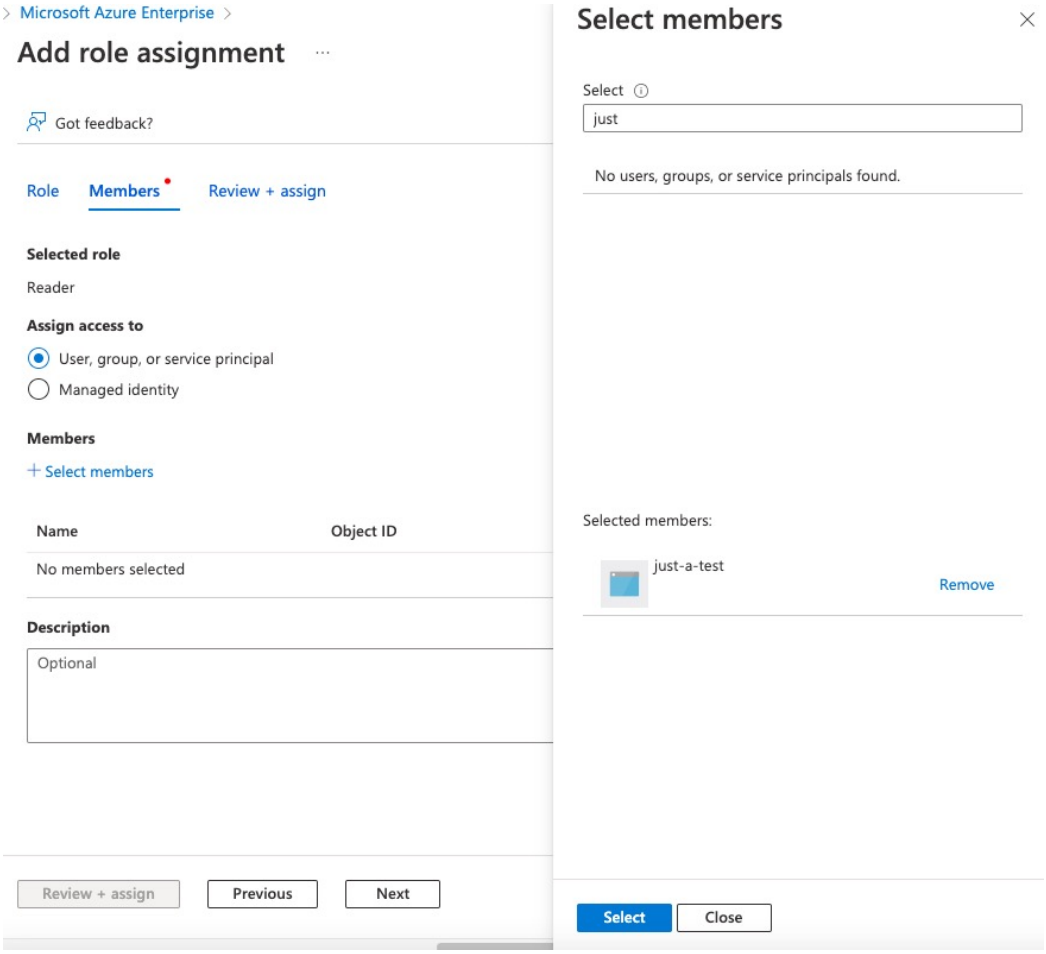
단계 **16** **Access Control (IAM)(**액세스 제어**(IAM))**를 클릭합니다.

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, 7 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, 5 페이지에 설명된 권한 이상의 Azure 사용자를 생성합니다.

단계 **1** 동적 속성 커넥터에 로그인합니다.

단계 **2** **Connector(**커넥터**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 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
Name(이름**)**	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
Description(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 **5** **Test(**테스트**)**를 클릭하고 커넥터를 저장하기 전에 **Test connection succeeded**이 표시되는지 확인합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

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

다음에 수행할 작업

어댑터 생성, 17 페이지

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.

단계 **1** 동적 속성 커넥터에 로그인합니다.

단계 **2** **Connector(**커넥터**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 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
Name(이름**)**	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
Description(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 **5** **Test(**테스트**)**를 클릭하고 커넥터를 저장하기 전에 **Test connection succeeded**이 표시되는지 확인합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

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

다음에 수행할 작업

어댑터 생성, 17 페이지

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.

단계 **1** 동적 속성 커넥터에 로그인합니다.

단계 **2** **Connector(**커넥터**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 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** **Name(**이름**)**과 선택적 설명을 입력합니다.

단계 **5** (선택 사항). **Pull Interval(**끌어오기 간격**)** 필드에서 동적 속성 커넥터가 GitHub에서 IP 주소를 검색하는 빈도를 초 단위로 변경합니다. 기본값은 21,600초(6시간)입니다,

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.

다음에 수행할 작업

어댑터 생성, 17 페이지

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 center(으)로 전송할 수 있는 최소 권한으로 서비스 계정을 설정하는 방법을 설명합니다. 이러한 속성의 목록은 Google Cloud Connector - 사용자 권한 및 가져온 데이터 정보, 9 페이지의 내용을 참조하십시오.

시작하기 전에

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

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.

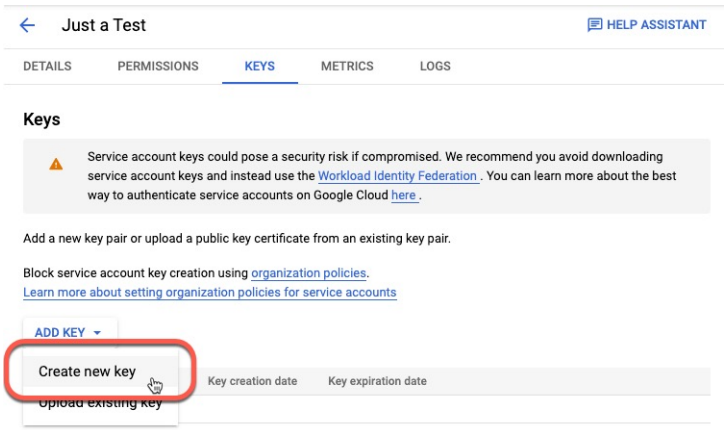
단계 **7** **Done(**완료**)**을 클릭합니다.

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, 11 페이지의 내용을 참조하십시오.

Google Cloud 커넥터 생성

시작하기 전에

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

단계 **1** 동적 속성 커넥터에 로그인합니다.

단계 **2** **Connector(**커넥터**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 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
Name(이름**)**	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
Description(설명**)**	선택적 설명.

값	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 **5** 커넥터를 저장하기 전에 **Test(**테스트**)**를 클릭하고 테스트가 성공했는지 확인합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

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

다음에 수행할 작업

어댑터 생성, 17 페이지

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.

단계 **1** 동적 속성 커넥터에 로그인합니다.

단계 **2** **Connector(**커넥터**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 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
Name(이름**)**	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
Description(설명**)**	선택적 설명.
Pull Interval(끌어오기 간격**)**	(기본값 30초) Azure에서 IP 매핑을 검색하는 간격입니다.

값	설명
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 **5** **Save(저장)**를 클릭합니다.

단계 **6** Status(상태) 열에 **Ok(확인)**가 표시되는지 확인합니다.

다음에 수행할 작업

어댑터 생성, 17 페이지

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 커넥터에 대한 CA(Certificate Authority) 체인 가져오기

이 주제에서는 커넥터 또는 어댑터에 대한 인증 기관 체인을 자동으로 가져오는 방법을 설명합니다. 인증 기관 체인은 루트 인증서 및 모든 하위 인증서입니다. 이는 vCenter 또는 management center를 안전하게 연결하는 데 필요합니다.

동적 속성 커넥터를 사용하면 인증 기관 체인을 자동으로 가져올 수 있지만 어떤 이유로든 이 절차가 작동하지 않을 경우 CA(Certificate Authority) 체인 수동으로 가져오기, 18 페이지 섹션을 참조하십시오.

단계 **1** 동적 속성 커넥터에 로그인합니다.

단계 **2** 다음 중 하나를 수행합니다.

a) vCenter CA 체인을 가져오려면 **Connectors(**커넥터**)**를 클릭합니다.

b) 관리 센터 어댑터 CA 체인을 가져오려면 **Adapters(**어댑터**)**를 클릭합니다.

c) 추가(+) 버튼을 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 커넥터 또는 어댑터를 식별하는 이름을 입력합니다.

단계 **4** **Host(**호스트**)** 필드에 커넥터 또는 어댑터의 호스트 이름 또는 IP 주소(예: **https://**)를 입력합니다.

예: **`myvcenter.example.com`** 또는 **`192.0.2.100:9090`**

입력하는 호스트 이름 또는 IP는 안전하게 연결하는 데 사용되는 CA 인증서의 일반 이름과 정확히 일치해야 합니다.

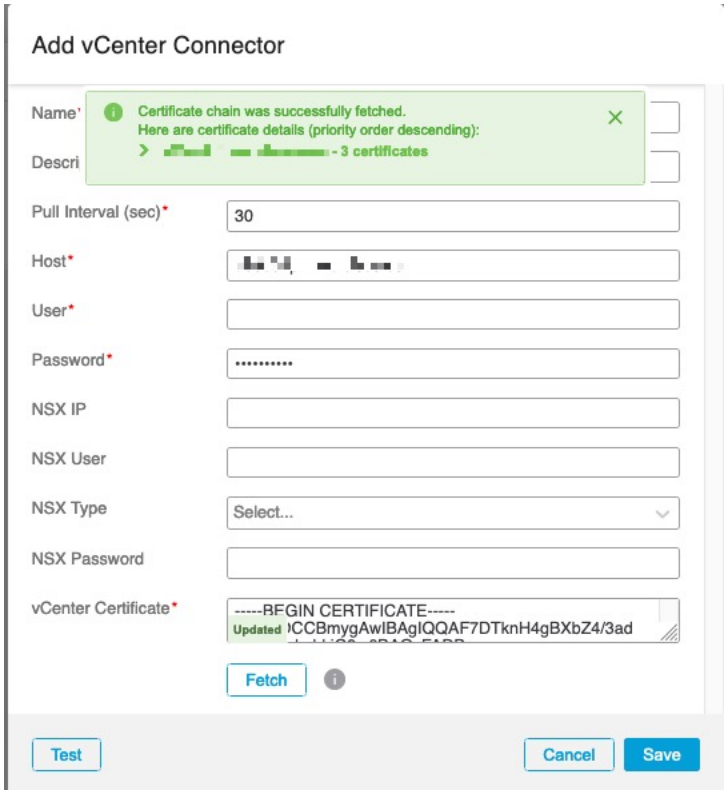
인증서 CA 체인을 가져오는 데 다른 정보는 필요하지 않습니다.

단계 **5** **Fetch(**가져오기**)**를 클릭합니다.

단계 **6** (선택 사항). 인증서 CA 체인에서 인증서를 확장하여 확인합니다.

예

다음은 vCenter 커넥터에 대한 성공적인 인증서 CA 가져오기의 예입니다.



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

vCenter 커넥터 생성

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

시작하기 전에

신뢰할 수 없는 인증서를 사용하여 vCenter와 통신하는 경우 CA(Certificate Authority) 체인 수동으로 가져오기, 18 페이지 섹션을 참조하십시오.

단계 **1** 동적 속성 커넥터에 로그인합니다.

단계 **2** **Connector(**커넥터**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 새 커넥터 추가: 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
Name(이름**)**	(필수) 이 커넥터를 고유하게 식별할 이름을 입력합니다.
Description(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.
vCenter Certificate(vCenter 인증서**)**	

단계 **5** **Test(**테스트**)**를 클릭하고 커넥터를 저장하기 전에 **Test connection succeeded**이 표시되는지 확인합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

어댑터 생성, 17 페이지

어댑터 생성

어댑터는 액세스 제어 정책에서 사용하기 위해 클라우드 개체에서 네트워크 정보를 푸시하는 management center에 대한 보안 연결입니다.

먼저 management center에 안전하게 연결하는 데 필요한 인증 기관 체인을 선택적으로 가져올 수 있습니다.

인증 기관 체인을 가져오는 경우에는 management center 호스트 이름만 필요합니다. 어댑터를 생성하려면 사용자 이름, 비밀번호 및 기타 정보가 필요합니다.

Dynamic Attributes Connector용 Secure Firewall Management Center 사용자 생성

동적 속성 커넥터 어댑터에 대한 전용 management center 사용자를 생성하는 것이 좋습니다. 전용 management center 사용자를 생성하면 management center에서 예기치 않은 로그아웃과 같은 문제를 방지할 수 있습니다. 동적 속성 커넥터는 REST API를 사용하여 주기적으로 로그인하여 신규 및 업데이트된 동적 개체로 management center를 업데이트하기 때문입니다.

management center 사용자는 최소한 Access Admin(액세스 관리자) 권한이 있어야 합니다.

단계 **1** 아직 하지 않았다면 management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Users(**사용자**)** 버튼을 클릭합니다.

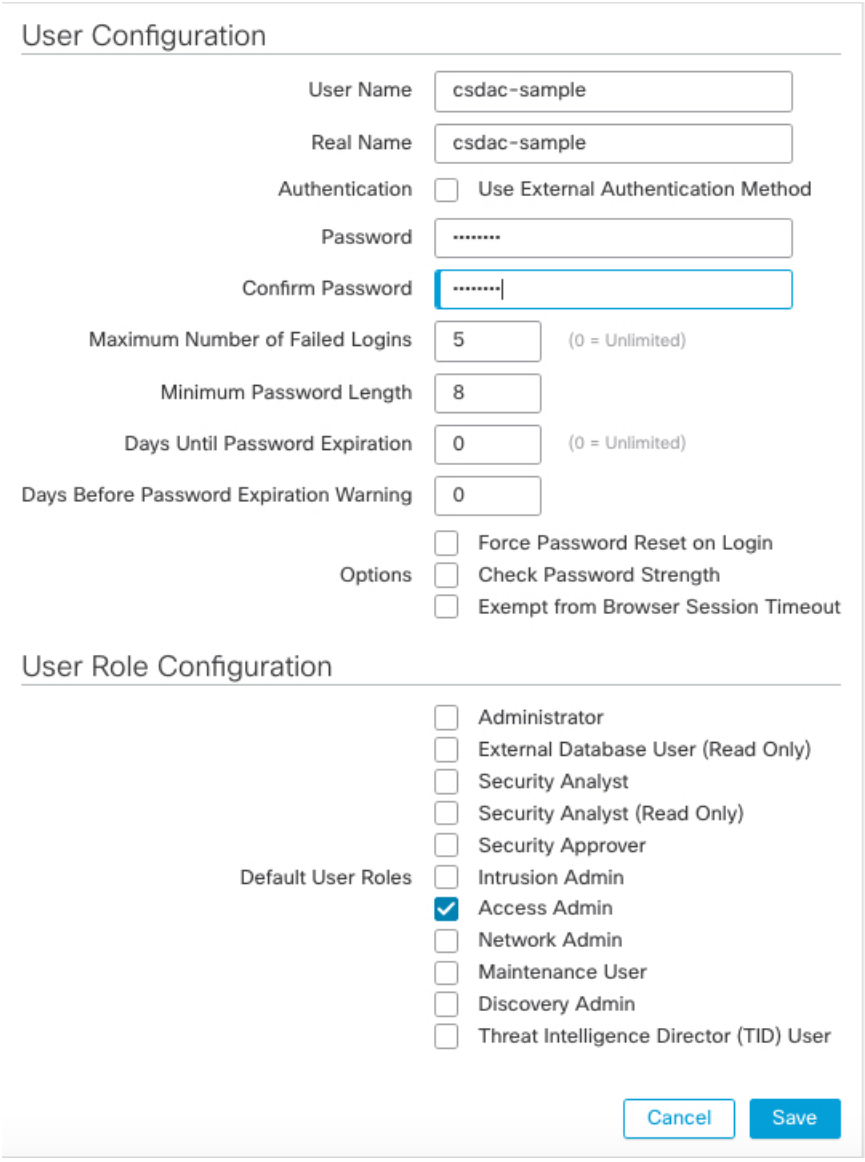
단계 **3** **Create User**(사용자 생성)를 클릭합니다.

단계 **4** 사용자를 생성하는 데 필요한 정보를 입력합니다.

단계 **5** User Role Configuration(사용자 역할 구성) 아래에서 다음 기본 역할 또는 동일한 권한 수준의 맞춤형 역할을 선택합니다.

- 관리자
- 액세스 관리자
- 네트워크 관리자

다음 그림은 예를 보여줍니다.



REST 작업을 허용하기에 충분한 권한이 있는 맞춤형 역할 또는 충분한 권한이 있는 다른 기본 역할을 선택할 수도 있습니다. 기본 역할에 대한 자세한 내용은 사용자 계정에 대한 장의 사용자 역할 섹션을 참조하십시오.

다음에 수행할 작업

어댑터 생성, 17 페이지

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

이 절차를 사용하기 전에 다음에서 인증 기관 체인 자동 가져오기에 대한 섹션을 참조하십시오.

- vCenter 커넥터 생성, 15 페이지
- 어댑터 생성, 17 페이지

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 FMC에 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.

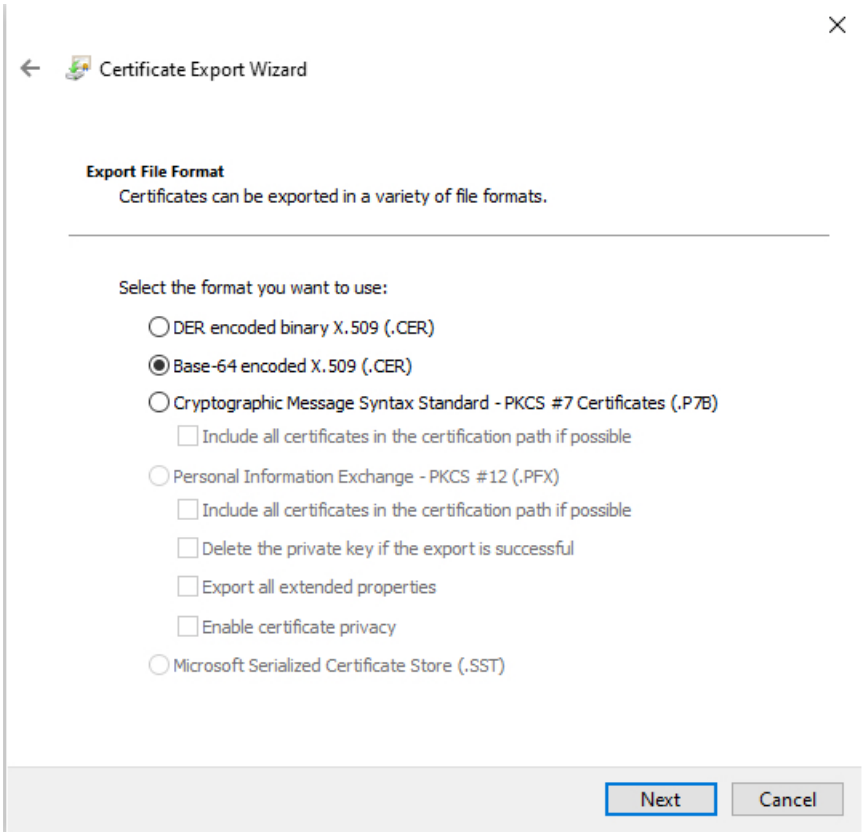
인증서 체인 가져오기 - **Windows Chrome**

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.



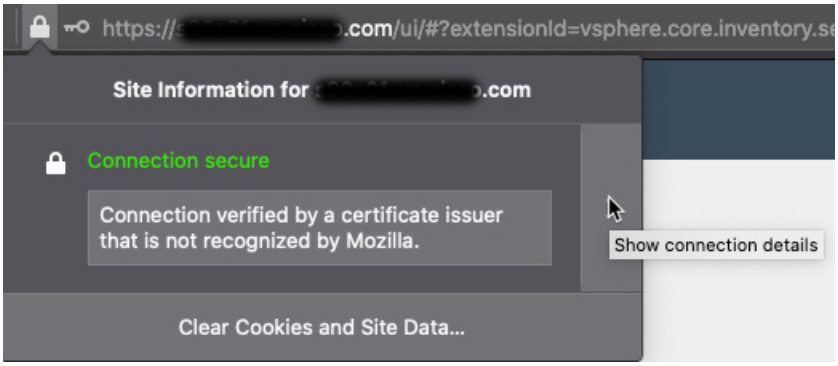
10. 프롬프트에 따라 내보내기를 완료합니다.
11. 텍스트 편집기에서 인증서를 엽니다.
12. 체인의 모든 인증서에 대해 프로세스를 반복합니다.

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

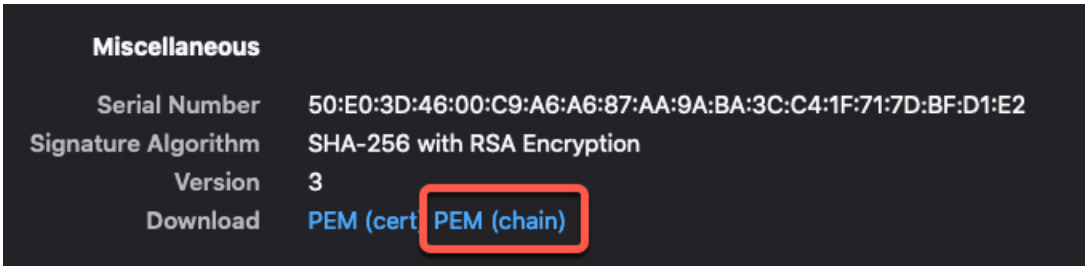
인증서 체인 가져오기 - Windows Firefox

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.

온프레미스 Firewall Management Center 어댑터에 대한 CA(Certificate Authority) 체인 가져오기

이 주제에서는 커넥터 또는 어댑터에 대한 인증 기관 체인을 자동으로 가져오는 방법을 설명합니다. 인증 기관 체인은 루트 인증서 및 모든 하위 인증서입니다. 이는 vCenter 또는 management center를 안전하게 연결하는 데 필요합니다.

동적 속성 커넥터를 사용하면 인증 기관 체인을 자동으로 가져올 수 있지만 어떤 이유로든 이 절차가 작동하지 않을 경우 CA(Certificate Authority) 체인 수동으로 가져오기, 18 페이지 섹션을 참조하십시오.

단계 **1** 동적 속성 커넥터에 로그인합니다.

단계 **2** 다음 중 하나를 수행합니다.

a) vCenter CA 체인을 가져오려면 **Connectors(**커넥터**)**를 클릭합니다.

b) 관리 센터 어댑터 CA 체인을 가져오려면 **Adapters(**어댑터**)**를 클릭합니다.

c) 추가(➕) 버튼을 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 커넥터 또는 어댑터를 식별하는 이름을 입력합니다.

단계 **4** **Host(**호스트**)** 필드에 커넥터 또는 어댑터의 호스트 이름 또는 IP 주소(예: **https://**)를 입력합니다.

예: **`myvcenter.example.com`** 또는 **`192.0.2.100:9090`**

입력하는 호스트 이름 또는 IP는 안전하게 연결하는 데 사용되는 CA 인증서의 일반 이름과 정확히 일치해야 합니다.

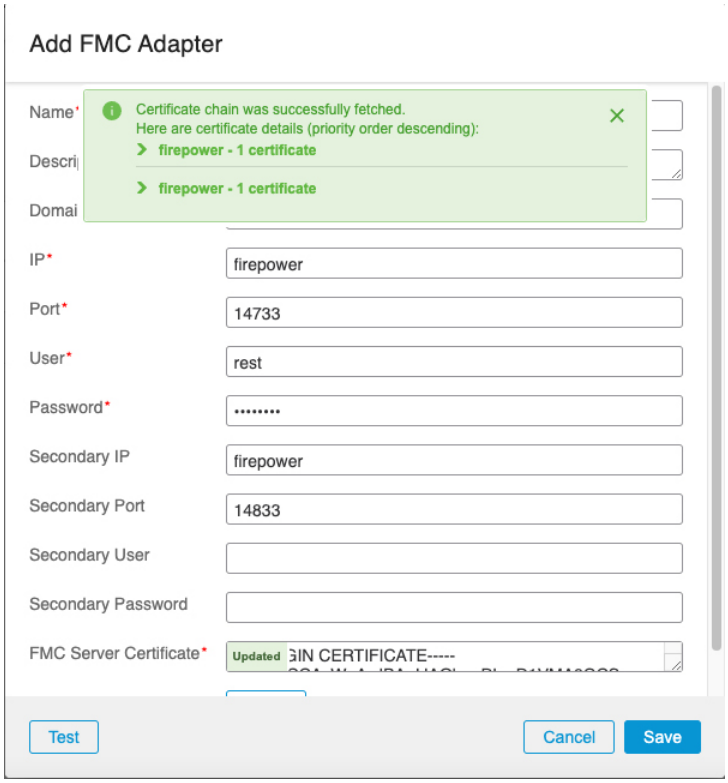
인증서 CA 체인을 가져오는 데 다른 정보는 필요하지 않습니다.

단계 **5** **Fetch(**가져오기**)**를 클릭합니다.

단계 **6** (선택 사항). 인증서 CA 체인에서 인증서를 확장하여 확인합니다.

예

다음은 vCenter 커넥터에 대한 성공적인 인증서 CA 가져오기의 예입니다.



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

온프레미스 Firewall Management Center 어댑터를 생성하는 방법

이 주제에서는 동적 개체를 동적 속성 커넥터에서 management center로 푸시하기 위한 어댑터를 생성하는 방법을 설명합니다.

시작하기 전에

Dynamic Attributes Connector용 Secure Firewall Management Center 사용자 생성, 17 페이지의 내용을 참조하십시오.

단계 **1** 동적 속성 커넥터에 로그인합니다.

단계 **2** **Adapters(**어댑터**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 새 어댑터 추가: 추가(➕)를 클릭한 다음 온프레미스 Firewall Management Center를 클릭합니다.

- 어댑터 편집 또는 삭제: 추가 (⋮)을 클릭한 다음 행의 끝에서 **Edit(편집)** 또는 **Delete(삭제)**를 클릭합니다.

단계 **4** 다음 정보를 입력합니다.

값	설명
Name(이름)	(필수) 이 어댑터를 식별하기 위한 고유한 이름을 입력합니다.
Description(설명)	어댑터에 대한 선택적 설명입니다.
Domain(도메인)	동적 개체를 생성할 Secure Firewall Management Center Virtual 도메인을 입력합니다. 전역 도메인에서 동적 개체를 생성하려면 필드를 비워 둡니다. 예: **`Global/MySubdomain`**
IP	(필수) Secure Firewall Management Center Virtual의 호스트 이름 또는 IP 주소를 입력합니다. 입력하는 호스트 이름 또는 IP는 안전하게 연결하는 데 사용되는 CA 인증서의 일반 이름과 정확히 일치해야 합니다.
Port(포트)	(필수) Secure Firewall Management Center Virtual에서 사용하는 TLS 포트를 입력합니다.
User(사용자)	(필수) 최소한 Network Admin(네트워크 관리자) 역할이 있는 Secure Firewall Management Center Virtual 사용자의 이름을 입력합니다.
Password(비밀번호)	(필수) 사용자의 비밀번호를 입력합니다.
Secondary IP(보조 IP)	(고가용성만 해당) Secure Firewall Management Center Virtual의 호스트 이름 또는 IP 주소를 입력합니다. 입력하는 호스트 이름 또는 IP는 안전하게 연결하는 데 사용되는 CA 인증서의 일반 이름과 정확히 일치해야 합니다.
Secondary Port(보조 포트)	(고가용성만 해당) 보조 Secure Firewall Management Center Virtual에서 사용하는 TLS 포트를 입력합니다.
Secondary User(보조 사용자)	(고가용성만 해당) 최소한 Network Admin(네트워크 관리자) 역할이 있는 보조 Secure Firewall Management Center Virtual 사용자의 이름을 입력합니다.
Secondary Password(보조 비밀번호)	(고가용성만 해당) 사용자의 비밀번호를 입력합니다.
Server Certificate(서버 인증서)	인증서를 자동으로 가져오려면 **Fetch(가져오기)**를 클릭합니다. 그렇게 할 수 없는 경우 CA(Certificate Authority) 체인 수동으로 가져오기, 18 페이지에 설명된 대로 수동으로 인증서를 가져옵니다.

단계 **5** 어댑터를 저장하기 전에 **Test(테스트)**를 클릭하고 테스트가 성공했는지 확인합니다.

단계 6 **Save(**저장**)**를 클릭합니다.

클라우드 사용 Firewall Management Center 어댑터 생성

이 주제에서는 동적 속성 커넥터에서 Cisco Defense Orchestrator의 매니지드 관리 센터로 동적 개체를 푸시하는 어댑터를 생성하는 방법을 설명합니다.

클라우드 사용 Firewall Management Center을(를) 생성하려면 먼저 다음 정보를 확인하십시오.기본 URL 및 API 토큰 가져오기, 25 페이지

기본 URL 및 API 토큰 가져오기

이 작업에서는 클라우드 사용 Firewall Management Center 어댑터를 생성하는 데 필요한 CDO에서 URL 및 API 토큰을 가져오는 방법을 설명합니다.

시작하기 전에

이 섹션에서 설명하는 작업을 완료하려면 CDO 슈퍼 관리자여야 합니다.

단계 1 슈퍼 관리자 역할의 사용자로 CDO에 로그인합니다.

단계 2 페이지의 오른쪽 상단에서 **Settings(**설정**)**를 클릭합니다.

단계 3 **General Settings(**일반 설정**)**를 클릭합니다.

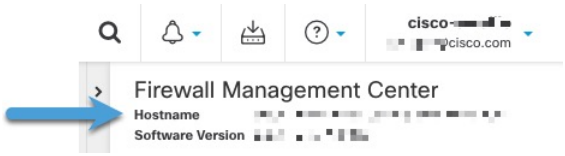
단계 4 API Token(API 토큰) 옆에 있는 **Refresh(**새로 고침**)**를 클릭합니다.

단계 5 나중에 사용할 수 있도록 API 토큰을 텍스트 파일에 복사합니다.

단계 6 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center** 버튼을 클릭합니다.

단계 7 동적 속성 커넥터 데이터를 전송할 관리 센터의 이름을 클릭합니다.

단계 8 **https://**가 앞에 오는 **Hostname(**호스트 이름**)**의 값은 기본 URL입니다.
예를 들면 다음과 같습니다.



다음에 수행할 작업

클라우드 사용 Firewall Management Center 어댑터를 생성하는 방법, 25 페이지.

클라우드 사용 Firewall Management Center 어댑터를 생성하는 방법

이 작업에서는 동적 속성 커넥터에서 CDO에서 관리하는 디바이스로 데이터를 전송하는 클라우드 사용 Firewall Management Center 어댑터를 생성하는 방법을 설명합니다.

시작하기 전에

이 작업을 완료하려면 먼저 CDO에서 관리 센터 기본 URL 및 API 토큰을 가져와야 합니다. 자세한 내용은 기본 URL 및 API 토큰 가져오기, 25 페이지를 참고하십시오.

단계 **1** 동적 속성 커넥터에 로그인합니다.

단계 **2** **Adapters(**어댑터**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 새 어댑터 추가: 추가(+)를 클릭한 다음 클라우드 사용 **Firewall Management Center**를 클릭합니다.
- 어댑터 편집 또는 삭제: 추가 (⋮)을 클릭한 다음 행의 끝에서 **Edit(**편집**)** 또는 **Delete(**삭제**)**를 클릭합니다.

단계 **4** 다음 정보를 입력합니다.

값	설명
Name(이름**)**	(필수) 이 어댑터를 식별하기 위한 고유한 이름을 입력합니다.
Description(설명**)**	어댑터에 대한 선택적 설명입니다.
Base Url(기본 **URL)**	(필수) 기본 URL 및 API 토큰 가져오기, 25 페이지에서 찾은 기본 URL을 사용합니다.
API Token(API 토큰**)**	(필수) 기본 URL 및 API 토큰 가져오기, 25 페이지에서 찾은 API 토큰을 사용합니다.

단계 **5** 어댑터를 저장하기 전에 **Test(**테스트**)**를 클릭하고 테스트가 성공했는지 확인합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

동적 속성 필터 생성, 26 페이지.

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 GitHub, Office 365 또는 Azure 서비스 태그에 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 생성의 내용을 참조하십시오.

시작하기 전에

다음 작업을 모두 완료합니다.

- 사전 요건 소프트웨어 설치
- 커넥터 생성, 1 페이지
- 어댑터 생성, 17 페이지

단계 **1** 동적 속성 커넥터에 로그인합니다.

단계 **2** **Dynamic Attributes Filters(**동적 속성 필터**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

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

단계 **4** 다음 정보를 입력합니다.

항목	설명
Name(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: 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.

항목	설명
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 Manager(**개체 관리자**)**를 클릭합니다.

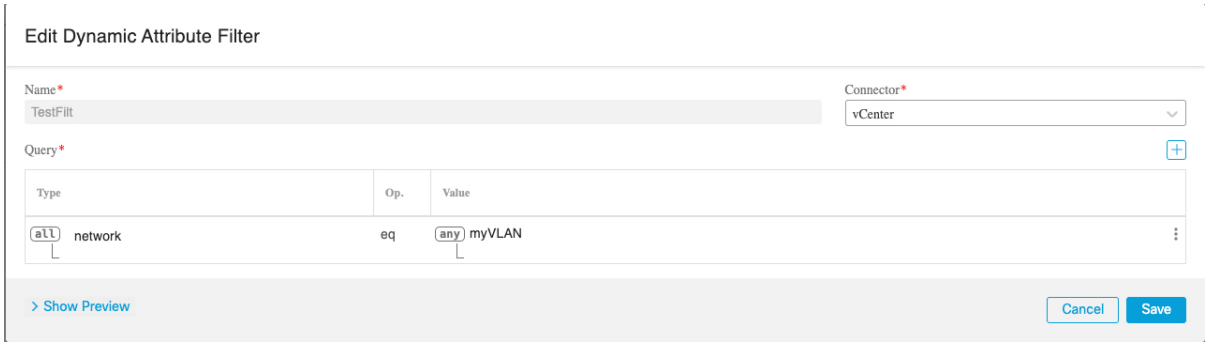
c) 왼쪽 창에서 **External Attributes(**외부 속성**)** > **Dynamic Object(**동적 개체**)**를 클릭합니다.
생성한 동적 속성 쿼리는 동적 개체로 표시되어야 합니다.

동적 속성 필터 예

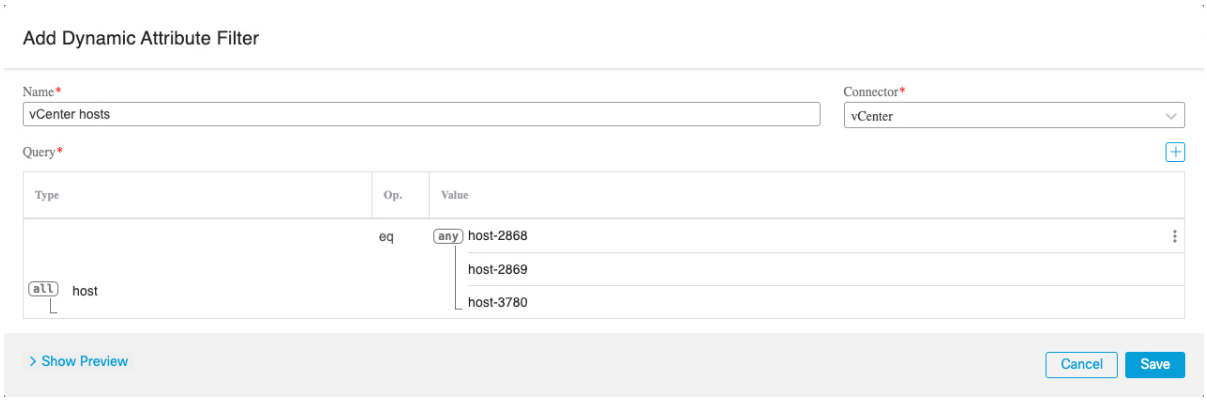
이 항목에서는 동적 속성 필터를 설정하는 몇 가지 예를 제공합니다.

예: vCenter

다음 예에서는 VLAN이라는 하나의 기준을 보여줍니다.

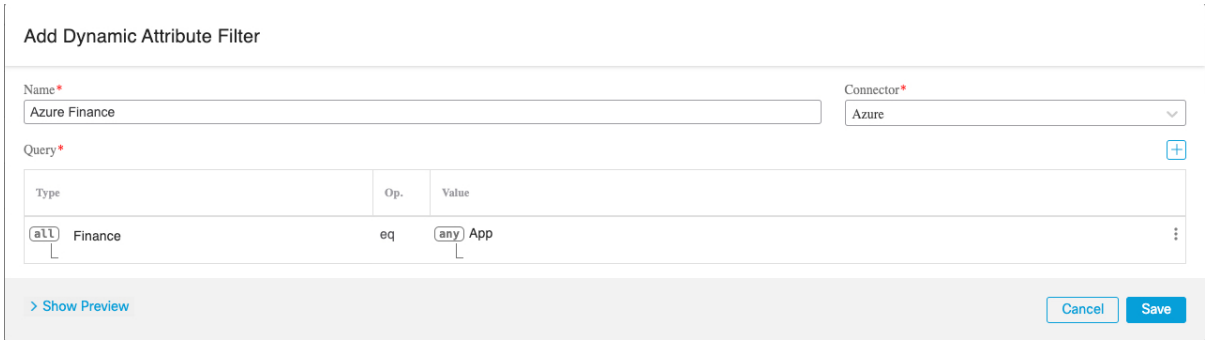


다음 예는 OR로 조인된 3개의 기준을 보여줍니다. 쿼리는 3개의 호스트 중 하나와 일치합니다.



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.