



Cisco Secure Dynamic Attributes Connector 구성 가이드 2.0

초판: 2021년 6월 1일

최종 변경: 2022년 7월 8일

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차

Full Cisco Trademarks with Software License ?

장 1	Cisco Dynamic Attributes Connector 정보 1
	Cisco Secure Dynamic Attributes Connector 정보 1
장 2	Cisco Secure Dynamic Attributes Connector 설치 5
	지원되는 운영 체제 및 서드파티 소프트웨어 5
	사전 요건 소프트웨어 설치 6
	사전 요건 소프트웨어 설치 - CentOS 7
	사전 요건 소프트웨어 설치 - RHEL 8
	사전 요건 소프트웨어 설치 - Ubuntu 9
	Cisco Secure Dynamic Attributes Connector 설치 11
	Cisco Secure Dynamic Attributes Connector 업그레이드 13
장 3	Cisco Secure Dynamic Attributes Connector 구성 15
	커넥터 생성 15
	Amazon Web Services Connector - 사용자 권한 및 가져온 데이터 정보 16
	Cisco Secure Dynamic Attributes Connector에 대한 최소 권한이 있는 AWS 사용자 생성 16
	AWS Connector 생성 17
	Azure Connector - 사용자 권한 및 가져온 데이터 정보 18
	Cisco Secure Dynamic Attributes Connector에 대한 최소 권한이 있는 Azure 사용자 생성 19
	Azure 커넥터 생성 21
	Azure 서비스 태그 커넥터 생성 22

- GitHub 커넥터 생성 23
- Google Cloud Connector - 사용자 권한 및 가져온 데이터 정보 23
 - Cisco Secure Dynamic Attributes Connector에 대한 최소 권한이 있는 Google Cloud 사용자 생성 24
 - Google Cloud 커넥터 생성 25
- Office 365 커넥터 생성 26
- vCenter 커넥터 - 사용자 권한 및 가져온 데이터 정보 27
 - vCenter 커넥터에 대한 CA(Certificate Authority) 체인 가져오기 27
 - vCenter 커넥터 생성 29
- 어댑터 생성 31
 - Dynamic Attributes Connector용 Secure Firewall Management Center 사용자 생성 31
 - CA(Certificate Authority) 체인 수동으로 가져오기 32
 - 온프레미스 Firewall Management Center 어댑터에 대한 CA(Certificate Authority) 체인 가져오기 36
 - 온프레미스 Firewall Management Center 어댑터를 생성하는 방법 37
 - 클라우드 사용 Firewall Management Center 어댑터 생성 39
 - 기본 URL 및 API 토큰 가져오기 39
 - 클라우드 사용 Firewall Management Center 어댑터를 생성하는 방법 39
- 동적 속성 필터 생성 40
 - 동적 속성 필터 예 42

- 장 4 액세스 제어 정책에서 동적 개체 사용 45
 - 액세스 제어 규칙의 동적 개체 정보 45
 - 동적 속성 필터를 사용하여 액세스 제어 규칙 생성 45

- 장 5 동적 속성 커넥터 문제 해결 47
 - 오류 메시지 문제 해결 47
 - 트러블슈팅 툴 49
 - CA(Certificate Authority) 체인 수동으로 가져오기 51

- 부록 A: 안전한 인터넷 액세스 55
 - 보안 요건 55

인터넷 액세스 요구 사항 55

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. 모든 권리 보유.



1 장

Cisco Dynamic Attributes Connector 정보

Cisco Secure Dynamic Attributes Connector을 사용하면 클라우드 제공자에서 데이터(예: 네트워크 및 IP 주소)를 수집하여 Cisco Secure Firewall Management Center(management center)로 전송하여 액세스 제어 규칙에 사용할 수 있습니다.

다음 항목에서는 동적 속성 커넥터에 대한 배경 정보를 제공합니다.

- [Cisco Secure Dynamic Attributes Connector 정보, 1 페이지](#)

Cisco Secure Dynamic Attributes Connector 정보

Cisco Secure Dynamic Attributes Connector를 사용하면 Secure Firewall Management Center(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 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

커넥터에 대한 추가 정보:

- AWS(Amazon Web Services)

자세한 내용은 [Amazon 설명서 사이트](#)에서 [AWS 리소스 태그 지정](#)과 같은 리소스를 참조하십시오.

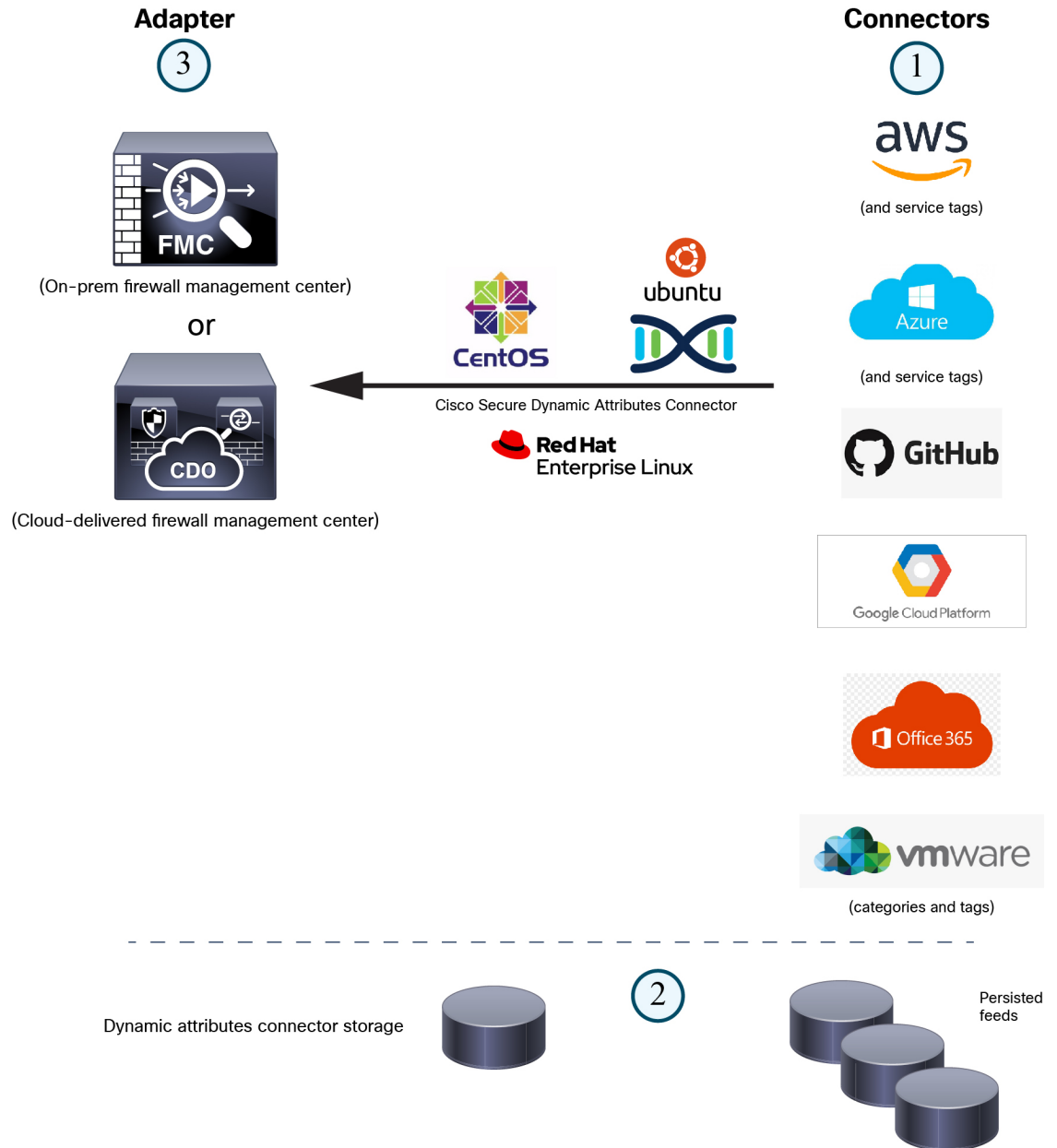
- GitHub
- Google Cloud
자세한 내용은 Google Cloud 설명서의 [환경 설정](#)을 참조하십시오.
- Microsoft Azure
자세한 내용은 Azure 설명서 사이트의 [이 페이지](#)를 참조하십시오.
- Microsoft Azure 서비스 태그
자세한 내용은 [Microsoft TechNet의 가상 네트워크 서비스 태그](#)와 같은 리소스를 참조하십시오.
- Office 365
자세한 내용은 docs.microsoft.com에서 [Office 365 URL 및 IP 주소 범위](#)를 참조하십시오.
- vCenter 및 NSX-T에서 관리하는 VMware 범주 및 태그
자세한 내용은 [VMware 설명서 사이트에서 vSphere 태그 및 속성](#)과 같은 리소스를 참조하십시오.

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 정책을 규칙을 정의해야 합니다.

Ubuntu, CentOS 또는 Red Hat Enterprise Linux 가상 머신에서 실행되는 동적 속성 컨넥터 Docker 컨테이너를 사용하여 이러한 태그 및 속성을 수집할 수 있습니다. Ansible 컬렉션을 사용하여 Ubuntu 호스트에 동적 속성 컨넥터를 설치합니다.

다음 그림은 시스템이 상위 레벨에서 작동하는 방식을 보여줍니다.



1. 커넥터는 쿼리할 태그 및 컨테이너를 포함합니다.

예를 들어, 일반적으로 이러한 태그는 액세스 제어 규칙을 생성할 수 없는 동적으로 할당된 네트워크 및 IP 주소를 정의합니다. 커넥터의 지속적인 피드는 빠른 액세스를 위해 동적 속성 커넥터에 저장됩니다.

2. 태그 정보는 액세스 제어 규칙에서 사용해야 하는 정보를 정의하는 동적 속성 필터를 생성하는 동적 속성 커넥터에서 유지됩니다.

예를 들어 AWS가 Accounting and Finance Departments 가상 머신에 대한 네트워크를 정의하는 경우, Finance 네트워크만 지정하는 동적 속성 필터를 생성할 수 있습니다.

3. 동적 속성 커넥터에서 정의한 어댑터는 이러한 동적 속성 필터를 동적 개체로 수신하고 사용자가 액세스 제어 규칙에서 이를 사용할 수 있도록 합니다.

다음 유형의 어댑터를 생성할 수 있습니다.

- 온프레미스 Management Center 디바이스의 경우 온프레미스 Firewall Management Center.
이 유형의 Management Center 디바이스는 Cisco Defense Orchestrator(CDO)에서 관리할 수도 있고 독립형일 수도 있습니다.
- CDO에서 관리하는 디바이스의 경우 클라우드 사용 *Firewall Management Center*.

관련 항목

[사전 요건 소프트웨어 설치](#), 6 페이지



2 장

Cisco Secure Dynamic Attributes Connector 설치

이 장에서는 지원되는 모든 운영 체제에 Cisco Dynamic Attributes Connector를 설치하는 방법을 설명합니다.

- [지원되는 운영 체제 및 서드파티 소프트웨어, 5 페이지](#)
- [사전 요건 소프트웨어 설치, 6 페이지](#)
- [Cisco Secure Dynamic Attributes Connector 설치, 11 페이지](#)
- [Cisco Secure Dynamic Attributes Connector 업그레이드, 13 페이지](#)

지원되는 운영 체제 및 서드파티 소프트웨어

동적 속성 커넥터에는 다음 요구 사항이 적용됩니다.

- Ubuntu 18.04 또는 20.04
- CentOS 7 Linux
- Red Hat Enterprise Linux (RHEL) 7 또는 8
- Python 3.6.x
- Ansible 2.9 이상

모든 운영 체제에 대한 최소 요구 사항:

- CPU 4개
- 8GB RAM
- 100GB 사용 가능한 디스크 공간

다음과 같이 가상 머신의 크기를 조정하는 것이 좋습니다.

- 커넥터 50개, 커넥터당 필터 5개 및 워크로드 20,000개 가정: CPU 4개, 8GB RAM; 100GB의 사용 가능한 디스크 공간

- 커넥터 125개, 커넥터당 필터 5개 및 워크로드 50,000개 가정: CPU 8개, 16GBRAM, 사용 가능한 디스크 공간 100GB



참고 가상 머신의 크기를 적절하게 조정하지 않으면 동적 속성 커넥터가 실패하거나 시작되지 않을 수 있습니다.

vCenter 속성을 사용하려면 다음 항목도 필요합니다.

- vCenter 6.7
- 가상 머신에 VMware Tools를 설치해야 합니다.

사전 요건 소프트웨어 설치

시작하기 전에

물리적 또는 가상 설정이 있고 시스템이 온프레미스 Firewall Management Center 또는 클라우드 사용 Firewall Management Center와 통신할 수 있는지 확인합니다.

단계 1 (선택 사항). Ubuntu 시스템이 인터넷 프록시 뒤에 있는 경우 텍스트 편집기를 사용하여 `/etc/environment`를 편집하여 다음 변수를 내보내 인터넷과의 통신을 활성화합니다.

변수	값
<code>export http_proxy</code>	HTTP 프록시와 함께 사용합니다. <code>user:pass@host-or-ip:port</code>
<code>export https_proxy</code>	HTTPS 프록시와 함께 사용합니다. <code>user:pass@host-or-ip:port</code>
<code>export no_proxy</code>	프록시 구성을 제거합니다. <code>export no_proxy="localhost,127.0.0.1"</code>

예:

다음 인증을 사용하지 않는 HTTP 프록시

```
vi /etc/environment
export http_proxy="myproxy.example.com:8181"
```

다음 인증을 사용하는 HTTPS 프록시:

```
vi /etc/environment
export https_proxy="ben.smith:bens-password@myproxy.example.com:8181"
```

단계 2 다른 명령 창을 사용하여 설정을 확인합니다.

```
env grep | proxy
```

결과 예:

```
http_proxy=myproxy.example.com:8181
```

단계 3 다음 섹션 중 하나를 계속 진행합니다.

관련 항목

[사전 요건 소프트웨어 설치 - Ubuntu](#), 9 페이지

[사전 요건 소프트웨어 설치 - CentOS](#), 7 페이지

[사전 요건 소프트웨어 설치 - RHEL](#), 8 페이지

사전 요건 소프트웨어 설치 - CentOS

시작하기 전에

다음은 모두 수행합니다.

- 시스템이 지원되는 운영 체제 및 서드파티 소프트웨어, 5 페이지에 설명된 사전 요건을 충족하는지 확인합니다.
- (선택 사항). 동적 속성 커넥터에 대한 프록시 액세스가 필요한 경우 [사전 요건 소프트웨어 설치](#), 6 페이지의 내용을 참조하십시오.

단계 1 Docker가 설치되어 있지 않은지 확인하고 설치되어 있으면 제거합니다.

```
docker --version
```

Docker가 설치되어 있으면 [Ubuntu에서 Docker 엔진 제거](#)에 설명된 대로 제거합니다.

단계 2 저장소를 업데이트하고 업그레이드합니다.

CentOS 7:

```
sudo yum -y update && sudo yum -y upgrade
```

단계 3 epel 저장소를 설치합니다.

CentOS 7:

```
sudo yum -y install epel-release
```

단계 4 (CentOS 7만 해당) Python 3을 설치합니다.

```
sudo yum install -y python3 libselenium-python3
```

단계 5 Ansible을 설치합니다.

CentOS 7:

```
sudo yum install -y ansible
```

단계 6 Ansible 버전이 2.9 이상인지 확인합니다.

CentOS 7:

```
ansible --version
ansible 2.9.24
  config file = /etc/ansible/ansible.cfg
  configured module search path = [u'/home/admin/.ansible/plugins/modules',
u'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python2.7/site-packages/ansible
  executable location = /usr/bin/ansible
  python version = 2.7.5 (default, Apr  2 2020, 13:16:51) [GCC 4.8.5 20150623 (Red Hat 4.8.5-39)]
```

참고 위의 출력에 나와 있는 것처럼 Ansible에서 Python 2.x를 참조하는 것은 정상입니다. 커넥터는 여전히 Python 3을 사용합니다.

다음에 수행할 작업

[Cisco Secure Dynamic Attributes Connector 설치, 11 페이지](#)에 설명된 대로 커넥터를 설치합니다.

필요에 따라 동적 속성 커넥터에서 프록시 사용을 중지하려면 `/etc/environment`를 편집하고 프록시 구성을 제거합니다.

사전 요건 소프트웨어 설치 - RHEL

시작하기 전에

다음은 모두 수행합니다.

- 시스템이 [지원되는 운영 체제 및 서드파티 소프트웨어, 5 페이지](#)에 설명된 사전 요건을 충족하는지 확인합니다.
- (선택 사항). 동적 속성 커넥터에 대한 프록시 액세스가 필요한 경우 [사전 요건 소프트웨어 설치, 6 페이지](#)의 내용을 참조하십시오.

단계 1 Docker가 설치되어 있지 않은지 확인하고 설치되어 있으면 제거합니다.

```
docker --version
```

Docker가 설치되어 있으면 [Ubuntu에서 Docker 엔진 제거](#)에 설명된 대로 제거합니다.

단계 2 저장소를 업데이트합니다.

RHEL 7:

```
sudo yum -y update && sudo yum -y upgrade
```

RHEL 8:

```
sudo dnf -y update && sudo dnf -y upgrade
```

단계 3 epel 저장소를 설치합니다.

RHEL 7:

```
sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

RHEL 8:

```
sudo dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

단계 4 (RHEL 7만 해당) Python 3을 설치합니다.

```
sudo yum install -y python3 libselenium-python3
```

단계 5 Ansible을 설치합니다.

RHEL 7:

```
sudo yum -y install ansible
```

RHEL 8:

```
sudo dnf install -y ansible
```

단계 6 Ansible 버전을 확인합니다.

```
ansible --version
```

예는 다음과 같습니다.

RHEL 7:

```
ansible 2.9.24
  config file = /etc/ansible/ansible.cfg
  configured module search path = [u'/home/stevej/.ansible/plugins/modules',
u'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python2.7/site-packages/ansible
  executable location = /usr/bin/ansible
  python version = 2.7.5 (default, Mar 20 2020, 17:08:22) [GCC 4.8.5 20150623 (Red Hat 4.8.5-39)]
```

참고 위의 출력에 나와 있는 것처럼 Ansible에서 Python 2.x를 참조하는 것은 정상입니다. 커넥터는 여전히 Python 3을 사용합니다.

RHEL 8:

```
ansible 2.9.24
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/home/stevej/.ansible/plugins/modules',
'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python3.6/site-packages/ansible
  executable location = /usr/bin/ansible
  python version = 3.6.8 (default, Mar 18 2021, 08:58:41) [GCC 8.4.1 20200928 (Red Hat 8.4.1-1)]
```

다음에 수행할 작업

[Cisco Secure Dynamic Attributes Connector 설치](#), 11 페이지에 설명된 대로 커넥터를 설치합니다.

필요에 따라 동적 속성 커넥터에서 프록시 사용을 중지하려면 `/etc/environment`를 편집하고 프록시 구성을 제거합니다.

사전 요건 소프트웨어 설치 - Ubuntu

단계 1 Docker가 설치되어 있지 않은지 확인하고 설치되어 있으면 제거합니다.

```
docker --version
```

Docker가 설치되어 있으면 [Ubuntu에서 Docker 엔진 제거](#)에 설명된 대로 제거합니다.

단계 2 저장소를 업데이트합니다.

```
sudo apt -y update && sudo apt -y upgrade
```

단계 3 Python 버전을 확인합니다.

```
/usr/bin/python3 --version
```

버전이 3.6 이전인 경우 버전 3.6.x를 설치해야 합니다.

단계 4 Python 3.6을 설치합니다.

```
sudo apt -y install python3.6
```

단계 5 공통 라이브러리를 설치합니다.

```
sudo apt -y install software-properties-common
```

단계 6 Ansible을 설치합니다.

```
sudo apt-add-repository -y -u ppa:ansible/ansible && sudo apt -y install ansible
```

단계 7 Ansible 버전을 확인합니다.

```
ansible --version
```

예는 다음과 같습니다.

```
ansible --version
ansible 2.9.19
  config file = /etc/ansible/ansible.cfg
  configured module search path = [u'/home/admin/.ansible/plugins/modules',
u'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python2.7/dist-packages/ansible
  executable location = /usr/bin/ansible
  python version = 2.7.17 (default, Feb 27 2021, 15:10:58) [GCC 7.5.0]
```

참고 위의 출력에 나와 있는 것처럼 Ansible에서 Python 2.x를 참조하는 것은 정상입니다. 커넥터는 여전히 Python 3.6을 사용합니다.

다음에 수행할 작업

[Cisco Secure Dynamic Attributes Connector 설치](#), 11 페이지에 설명된 대로 커넥터를 설치합니다.

필요에 따라 동적 속성 커넥터에서 프록시 사용을 중지하려면 `/etc/environment`를 편집하고 프록시 구성을 제거합니다.

Cisco Secure Dynamic Attributes Connector 설치

설치 정보

이 항목에서는 Cisco Secure Dynamic Attributes Connector 설치에 대해 설명합니다. `sudo` 권한이 있는 사용자로 커넥터를 설치해야 하지만 권한이 없는 사용자로도 실행할 수 있습니다.

시작하기 전에

시스템에 다음 사전 요건 소프트웨어가 있는지 확인합니다.

- Ubuntu 18.04 또는 20.04
- CentOS 7 Linux
- Red Hat Enterprise Linux (RHEL) 7 또는 8
- Python 3.6.x
- Ansible 2.9 이상

모든 운영 체제에 대한 최소 요구 사항:

- CPU 4개
- 8GB RAM
- 100GB 사용 가능한 디스크 공간

다음과 같이 가상 머신의 크기를 조정하는 것이 좋습니다.

- 커넥터 50개, 커넥터당 필터 5개 및 워크로드 20,000개 가정: CPU 4개, 8GB RAM; 100GB의 사용 가능한 디스크 공간
- 커넥터 125개, 커넥터당 필터 5개 및 워크로드 50,000개 가정: CPU 8개, 16GBRAM, 사용 가능한 디스크 공간 100GB



참고 가상 머신의 크기를 적절하게 조정하지 않으면 동적 속성 커넥터가 실패하거나 시작되지 않을 수 있습니다.

vCenter 속성을 사용하려면 다음 항목도 필요합니다.

- vCenter 6.7
- 가상 머신에 VMware Tools를 설치해야 합니다.

사전 요건 소프트웨어를 설치하려면 [사전 요건 소프트웨어 설치, 6 페이지](#) 섹션을 참조하십시오.

Readme와 릴리스 노트 보기

최신 설치 정보는 다음을 참조하십시오.

읽어보기: <https://galaxy.ansible.com/cisco/csdac>

릴리스 노트: [Cisco Secure Dynamic Attributes Connector 릴리스 노트](#)

Dynamic Attributes Connector 소프트웨어 다운로드

최신 버전의 동적 속성 커넥터 소프트웨어를 다운로드하려면 다음 명령을 실행합니다.

```
ansible-galaxy collection install cisco.csdac
```

소집 서비스 설치

소집 서비스는 동적 속성 커넥터의 또 다른 이름입니다.

~/ansible/collections/ansible_collections/cisco/csdac 디렉터리에서 다음 명령을 실행합니다.

```
ansible-playbook default_playbook.yml [--ask-become-pass] [--extra-vars " vars " ]
```

Syntax Description

--ask-become-pass sudo 비밀번호를 입력하라는 프롬프트가 표시됩니다. 시스템에서 sudo가 활성화된 경우 필요합니다.

--extra-vars 다음의 선택적 추가 변수는 동적 속성 커넥터가 프록시를 사용할 수 있도록 합니다. 사용하는 값은 [사전 요건 소프트웨어 설치, 6 페이지](#)에서 설명한 대로 구성된 /etc/environment의 값과 일치해야 합니다.

- **csdac_proxy_enabled=true**
- **csdac_http_proxy_url=http://PROXY_URL**
csdac_https_proxy_url=PROXY_URL

다음 추가 변수는 동적 속성 커넥터에 안전하게 연결하는 데 사용할 수 있는 자체 서명 인증서를 생성합니다. 이러한 매개 변수를 생략하면 동적 속성 커넥터는 기본 인증서를 사용합니다.

- **csdac_certificate_domain**
자동 생성된 인증서의 도메인 이름입니다. 기본값은 호스트의 자동 탐지 호스트 이름(ansible에 의해 탐지됨)입니다.
- **csdac_certificate_country_name**
2자로 된 국가 코드. (기본값은 US)
- **csdac_certificate_organization_name**
조직의 이름입니다. (기본값은 Cisco)
- **csdac_certificate_organization_unit_name**
조직 단위 이름(기본값은 Cisco)

기본 인증서를 사용한 설치 예

예를 들어 기본 옵션으로 소프트웨어를 설치하려면 다음을 수행합니다.

```
ansible-galaxy collection install cisco.csdac
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-playbook default_playbook.yml --ask-become-pass
```

선택적 인증서를 사용하는 설치 예

예를 들어, 선택적 인증서를 사용하여 소프트웨어를 설치하려면 다음을 수행합니다.

```
ansible-galaxy collection install cisco.csdac
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-playbook default_playbook.yml --ask-become-pass --extra-vars
"csdac_certificate_domain=domain.example.com csdac_certificate_country_name=US
csdac_certificate_organization_name=Cisco
csdac_certificate_organization_unit_name=Engineering"
```

인증서를 생성한 후 커넥터에 액세스하는 데 사용할 웹 브라우저로 가져옵니다. 인증서는 `~/csdac/app/config/certs` 디렉터리에 생성됩니다.

설치 로그 보기

설치 로그는 다음 위치에 있습니다.

```
~/ansible/collections/ansible_collections/cisco/csdac/logs/csdac.log
```

인증서를 사용하여 동적 속성 커넥터에 연결합니다.

인증서와 키가 있는 경우 가상 머신의 `~/csdac/app/config/certs` 디렉터리에 저장합니다.

이전 작업을 수행한 후 다음 명령을 입력하여 동적 속성 커넥터의 Docker 컨테이너를 다시 시작합니다.

```
docker restart muster-ui
```

커넥터에 로그인

1. `https://ip-address`에서 동적 속성 커넥터에 액세스합니다.
2. 로그인합니다.

초기 로그인은 사용자 이름 `admin`, 비밀번호는 `admin`입니다. 처음 로그인할 때 비밀번호를 변경해야 합니다.

Cisco Secure Dynamic Attributes Connector 업그레이드

이 항목에서는 이전 Cisco Secure Dynamic Attributes Connector에서 현재 버전으로 업그레이드하는 방법을 설명합니다. 이러한 작업은 Cisco Secure Dynamic Attributes Connector 버전 또는 운영 체제에 관계없이 수행할 수 있습니다.

단계 1 업그레이드할 시스템에 로그인합니다.

단계 2 다음 명령을 입력합니다.

```
ansible-galaxy collection install cisco.csdac --force
ansible-playbook default_playbook.yml --ask-become-pass
ansible-playbook default_playbook.yml --ask-become-pass [--extra-vars vars]
```

Syntax Description **--ask-become-pass** **sudo** 비밀번호를 입력하라는 프롬프트가 표시됩니다. 시스템에서 **sudo**가 활성화된 경우 필요합니다.

--extra-vars 다음의 선택적 추가 변수는 동적 속성 커넥터가 프록시를 사용할 수 있도록 합니다. 사용하는 값은 [사전 요건 소프트웨어 설치, 6 페이지](#)에서 설명한 대로 구성된 `/etc/environment`의 값과 일치해야 합니다.

- **csdac_proxy_enabled=true**
- **csdac_http_proxy_url=http://PROXY_URL**
csdac_https_proxy_url=PROXY_URL

다음 추가 변수는 동적 속성 커넥터에 안전하게 연결하는 데 사용할 수 있는 자체 서명 인증서를 생성합니다. 이러한 매개 변수를 생략하면 동적 속성 커넥터는 기본 인증서를 사용합니다.

- **csdac_certificate_domain**
자동 생성된 인증서의 도메인 이름입니다. 기본값은 호스트의 자동 탐지 호스트 이름(ansible에 의해 탐지됨)입니다.
- **csdac_certificate_country_name**
2자로 된 국가 코드. (기본값은 `us`)
- **csdac_certificate_organization_name**
조직의 이름입니다. (기본값은 `Cisco`)
- **csdac_certificate_organization_unit_name**
조직 단위 이름(기본값은 `Cisco`)

단계 3 업그레이드가 완료될 때까지 기다립니다.

단계 4 업그레이드 로그는 다음 위치에서 사용할 수 있습니다.

```
~/.ansible/collections/ansible_collections/cisco/csdac/logs/csdac.log
```

다음에 수행할 작업

[커넥터 생성, 15 페이지](#)의 내용을 참조하십시오.



3 장

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, 15 페이지
- 어댑터 생성, 31 페이지
- 동적 속성 필터 생성, 40 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 2: 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 지정](#)을 참조하십시오.
- AWS에 있는 가상 머신의 IP 주소입니다.

최소 권한 필요

Cisco Secure Dynamic Attributes Connector에서는 최소한 ec2:DescribeTags 및 ec2:DescribeInstances가 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, 16 페이지](#)의 내용을 참조하십시오.

시작하기 전에

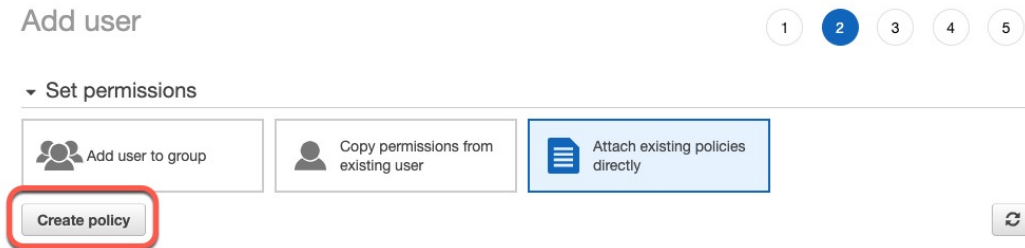
AWS(Amazon Web Services) 계정이 이미 설정되어 있어야 합니다. 자세한 내용은 AWS 설명서에서 [이 문서](#)를 참조하십시오.

-
- 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, 17 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, 16 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, 31 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 페이지](#)를 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

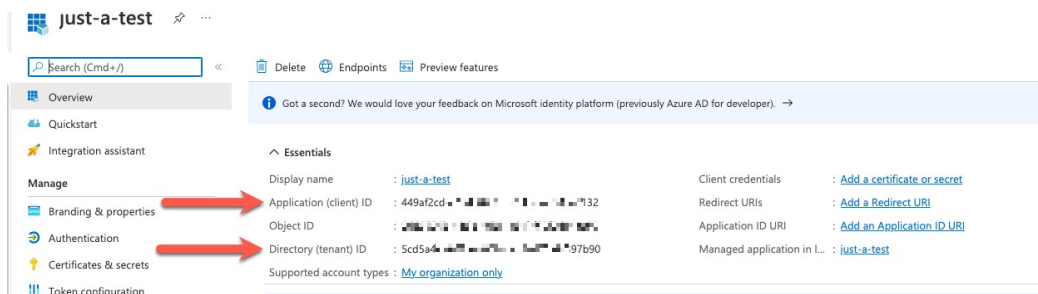
이 작업에서는 동적 속성을 management center로 전송할 수 있는 최소 권한으로 서비스 계정을 설정하는 방법을 설명합니다. 이러한 속성의 목록은 [Azure Connector - 사용자 권한 및 가져온 데이터 정보, 18 페이지](#) 섹션을 참조하십시오.

시작하기 전에

Microsoft Azure 계정이 이미 있어야 합니다. 새로 설정하려면 Azure 설명서 사이트에서 [이 페이지](#)를 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 ID라고도 함) 및 테넌트 ID(디렉터리 ID라고도 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.

Description	Expires	Value	Secret ID
Sample only	10/15/2022	r_Wk... 59wMK...	8fa75b1

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 등록된 앱의 이름을 클릭하고 **Select(선택)**를 클릭합니다.

> Microsoft Azure Enterprise >

Add role assignment

Got feedback?

Role **Members** Review + assign

Selected role
Reader

Assign access to
 User, group, or service principal
 Managed identity

Members
+ Select members

Name	Object ID
No members selected	

Description
Optional

Review + assign Previous Next

Select members

Select

just

No users, groups, or service principals found.

Selected members:

just-a-test	Remove
-------------	--------

Select Close

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

다음에 수행할 작업

[Azure 커넥터 생성, 21 페이지](#)의 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, 19 페이지](#)에 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, 31 페이지](#)

Azure 서비스 태그 커넥터 생성

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

자세한 내용은 [Microsoft TechNet의 가상 네트워크 서비스 태그](#)를 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, 31 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 정보](#)를 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, 31 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 관리](#)를 참조하십시오.
- 조직, 폴더 또는 프로젝트와 연결된 키-값 쌍인 네트워크 태그입니다.

자세한 내용은 Google Cloud 설명서에서 [태그 생성 및 관리](#)를 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, 23 페이지](#)의 내용을 참조하십시오.

시작하기 전에

Google Cloud 계정을 이미 설정했어야 합니다. 자세한 내용은 Google Cloud 설명서의 [환경 설정](#)을 참조하십시오.

단계 1 소유자 역할의 사용자 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 이해](#)를 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.

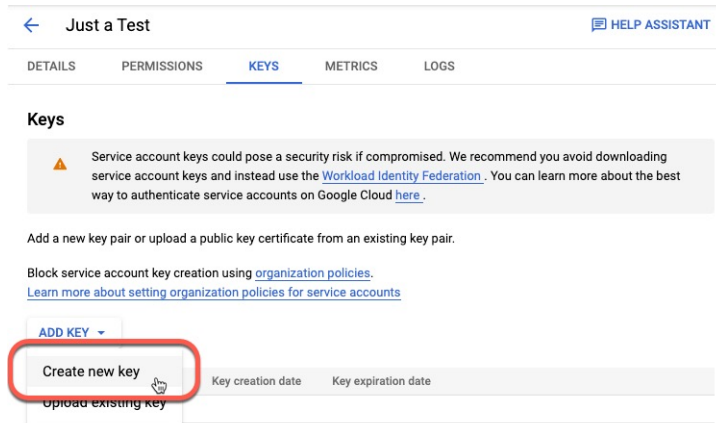
단계 7 **Done(완료)**을 클릭합니다.

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 JSON을 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, 25 페이지](#)의 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 영역 을 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, 31 페이지](#)

Office 365 커넥터 생성

이 작업에서는 액세스 제어 정책에서 사용하기 위해 **management center**에 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 범위](#)를 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 서비스 를 참조하십시오.
Instance name(인스턴스 이름)	(필수) 목록에서 인스턴스 이름을 클릭합니다. 자세한 내용은 Microsoft 설명서 사이트에서 Office 365 IP 주소 및 URL 웹 서비스 를 참조하십시오.
Disable optional IPs(선택적 IP 비활성화)	(필수) true 또는 false 를 입력합니다.

단계 5 **Save**(저장)를 클릭합니다.

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

다음에 수행할 작업

[어댑터 생성, 31 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, 32 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, 32 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. <ul style="list-style-type: none"> • 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, 31 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.

User Configuration

User Name

Real Name

Authentication Use External Authentication Method

Password

Confirm Password

Maximum Number of Failed Logins (0 = Unlimited)

Minimum Password Length

Days Until Password Expiration (0 = Unlimited)

Days Before Password Expiration Warning

Options

Force Password Reset on Login

Check Password Strength

Exempt from Browser Session Timeout

User Role Configuration

Default User Roles

Administrator

External Database User (Read Only)

Security Analyst

Security Analyst (Read Only)

Security Approver

Intrusion Admin

Access Admin

Network Admin

Maintenance User

Discovery Admin

Threat Intelligence Director (TID) User

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, 31 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, 29 페이지](#)
- [어댑터 생성, 31 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.

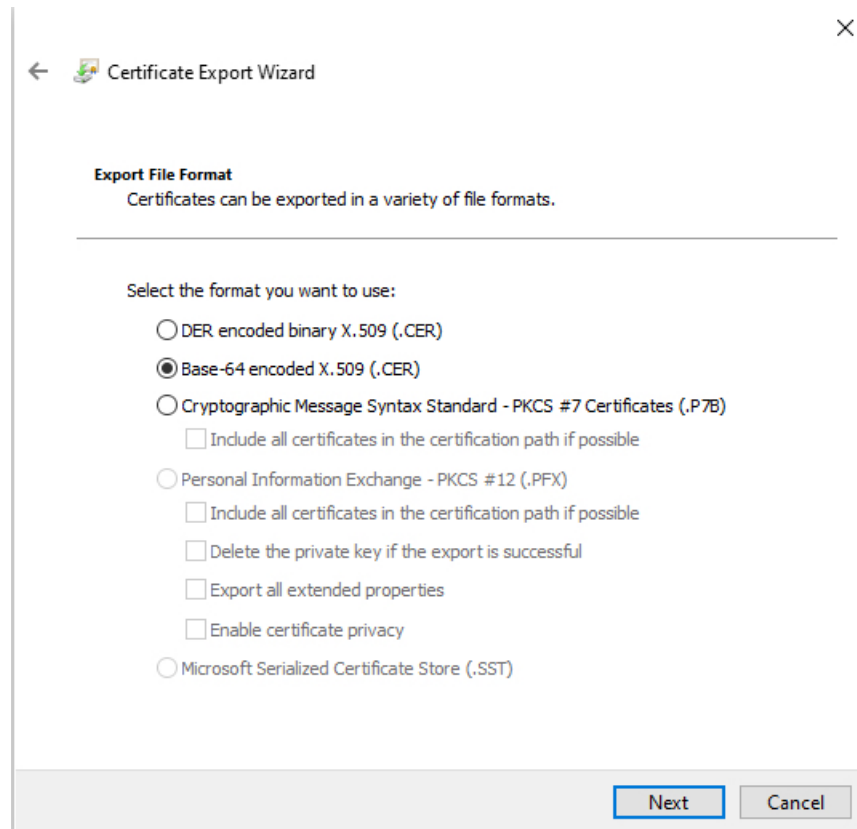
인증서 체인 가져오기 - Windows Chrome

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.

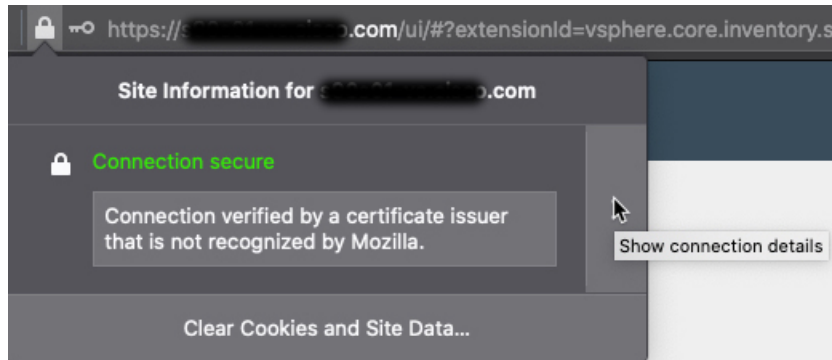


10. 프롬프트에 따라 내보내기를 완료합니다.
11. 텍스트 편집기에서 인증서를 엽니다.
12. 체인의 모든 인증서에 대해 프로세스를 반복합니다.
텍스트 편집기에서 각 인증서를 맨 처음부터 마지막 순서로 붙여넣어야 합니다.
13. vCenter와 FMC 모두에 대해 이 작업을 반복합니다.

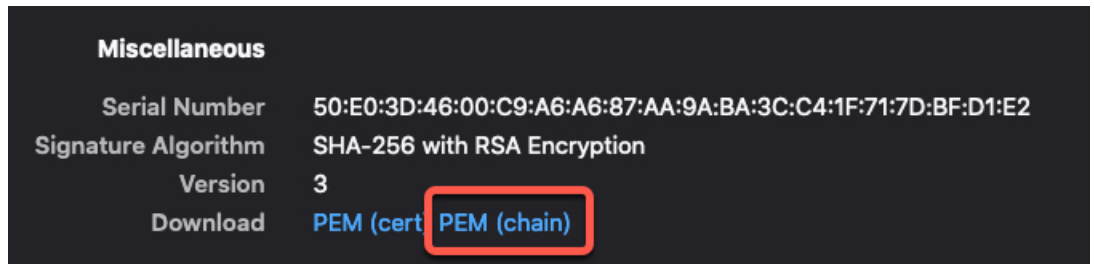
인증서 체인 가져오기 - Windows Firefox

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, 32 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.

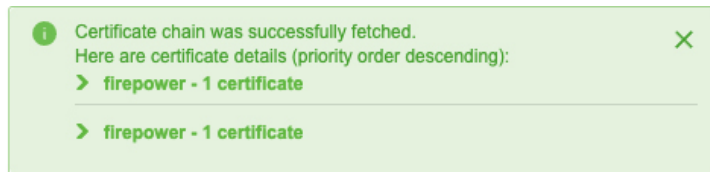
단계 5 **Fetch**(가져오기)를 클릭합니다.

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, 31 페이지](#)의 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 , 32 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, 39 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.

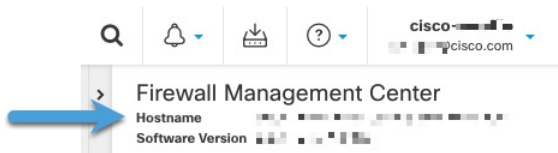
단계 5 나중에 사용할 수 있도록 API 토큰을 텍스트 파일에 복사합니다.

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, 39 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, 39 페이지](#)를 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, 39 페이지 에서 찾은 기본 URL을 사용합니다.
API Token (API 토큰)	(필수) 기본 URL 및 API 토큰 가져오기, 39 페이지 에서 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, 40 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 생성, 45 페이지](#)의 내용을 참조하십시오.

시작하기 전에

다음 작업을 모두 완료합니다.

- [사전 요건 소프트웨어 설치, 6 페이지](#)
- [커넥터 생성, 15 페이지](#)
- [어댑터 생성, 31 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)	<ul style="list-style-type: none"> • 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)	<p>다음 중 하나를 클릭합니다.</p> <ul style="list-style-type: none"> • 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.

- 최소한 네트워크 관리자 역할이 있는 사용자로 management center에 로그인합니다.
- Objects**(개체) > **Object Manager**(개체 관리자)를 클릭합니다.
- 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.

The screenshot shows the 'Edit Dynamic Attribute Filter' interface. The 'Name' field contains 'TestFilter' and the 'Connector' dropdown is set to 'vCenter'. Below, the 'Query' section is a table with three columns: 'Type', 'Op.', and 'Value'. The first row has 'all' in the Type column, 'network' in the Value column, and 'eq' in the Op. column. The second row has 'any' in the Type column and 'myVLAN' in the Value column. At the bottom left, there is a '> Show Preview' link, and at the bottom right, there are 'Cancel' and 'Save' buttons.

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

Add Dynamic Attribute Filter

Name* vCenter hosts Connector* vCenter

Query* +

Type	Op.	Value
<input type="checkbox"/> all host	eq	<input type="checkbox"/> any host-2868
		host-2869
		host-3780

> Show Preview Cancel Save

예: Azure

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

Add Dynamic Attribute Filter

Name* Azure Finance Connector* Azure

Query* +

Type	Op.	Value
<input type="checkbox"/> all Finance	eq	<input type="checkbox"/> any App

> Show Preview Cancel Save

예: AWS

다음 예는 하나의 기준, 즉 값이 1인 금융 앱을 보여줍니다.

Add Dynamic Attribute Filter

Name* AWS Connector* AWS

Query* +

Type	Op.	Value
<input type="checkbox"/> all FinanceApp	eq	<input type="checkbox"/> any 1

> Show Preview Cancel Save



4 장

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, 45 페이지](#)
- [동적 속성 필터를 사용하여 액세스 제어 규칙 생성, 45 페이지](#)

액세스 제어 규칙의 동적 개체 정보

동적 속성 필터를 커넥터에 저장하면 동적 개체가 동적 속성 커넥터에서 정의된 온프레미스 Firewall Management Center 또는 어댑터로 자동으로 푸시됩니다.

액세스 제어 규칙의 Dynamic Attributes(동적 속성) 탭 페이지에서 이러한 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 GitHub, Office 365 또는 Azure 서비스 태그에 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 개체(이러한 동적 개체의 이름은 이전에 생성한 동적 속성 필터의 이름을 따옴)를 사용하여 액세스 제어 규칙을 생성하는 방법을 설명합니다.

시작하기 전에

[동적 속성 필터 생성, 40 페이지](#)에 설명된 대로 동적 속성 필터를 생성합니다.



참고 GitHub, Office 365 또는 Azure 서비스 태그에 대한 동적 속성 필터는 생성할 수 없습니다. 이러한 유형의 클라우드 개체는 자체 IP 주소를 제공합니다.

단계 1 Policies(정책) > Access Control(액세스 제어) 버튼을 클릭합니다.

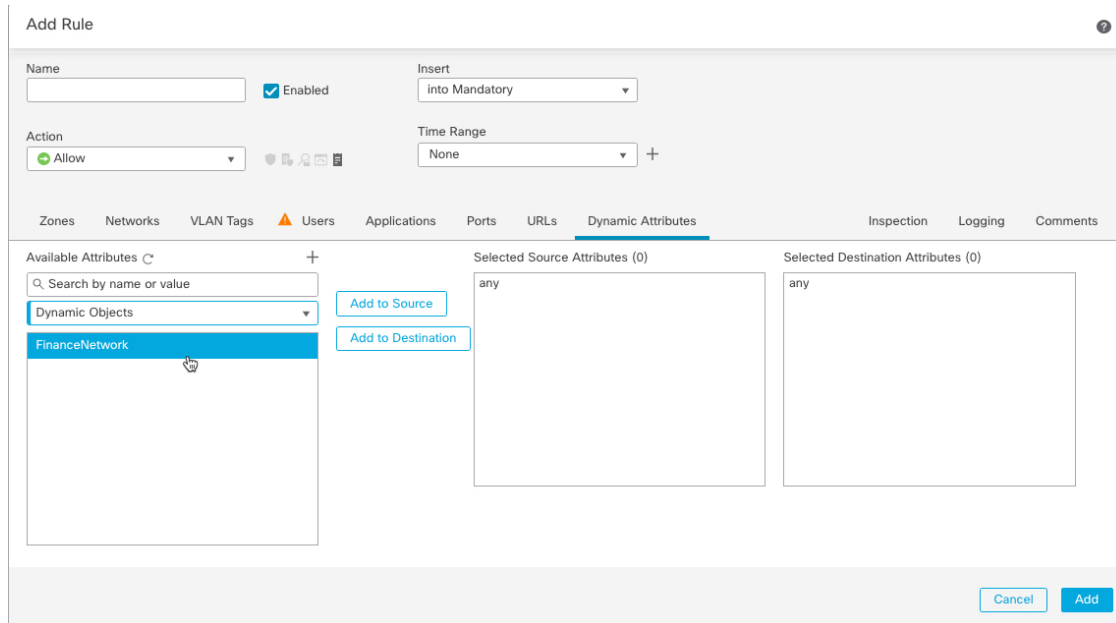
단계 2 액세스 제어 정책 옆에 있는 수정(✎)을 클릭합니다.

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 동적 속성 커넥터에서 생성된 동적 속성 필터에 해당하는 FinanceNetwork라는 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](#))



5 장

동적 속성 커넥터 문제 해결

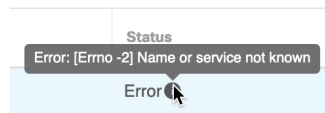
제공된 툴 사용을 포함하여 동적 속성 커넥터에서 문제를 해결하는 방법.

- 오류 메시지 문제 해결, 47 페이지
- 트러블슈팅 툴, 49 페이지
- CA(Certificate Authority) 체인 수동으로 가져오기, 51 페이지

오류 메시지 문제 해결

문제: 이름 또는 서비스를 알 수 없음 오류

이 오류는 커넥터의 오류 상태 위로 마우스를 이동하면 툴팁으로 표시됩니다. 예는 다음과 같으며, 다르게 표시될 수 있습니다.



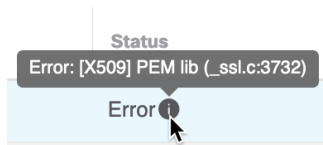
해결책: 커넥터를 수정하고 다음을 확인합니다.

- 호스트 이름의 후행 슬래시
- (온프레미스 Firewall Management Center 어댑터만 해당) 호스트 이름의 시작 부분에 있는 체계 (예: https://)
- 비밀번호가 올바른지 확인
- 온프레미스 Firewall Management Center 어댑터의 **FMC Server Certificate(FMC 서버 인증서)** 필드의 내용을 확인합니다.

자세한 내용은 [CA\(Certificate Authority\) 체인 수동으로 가져오기, 32 페이지](#)를 참고하십시오.

문제: [X509 PEM lib]

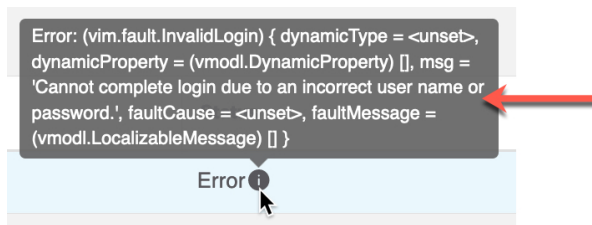
이 오류는 커넥터의 오류 조건 위에 마우스를 놓으면 툴팁으로 표시됩니다.



해결책: 커넥터를 편집하고 CA 체인을 확인합니다. 자세한 내용은 [CA\(Certificate Authority\) 체인 수동으로 가져오기, 32 페이지](#)를 참고하십시오.

문제: 잘못된 사용자 이름 또는 비밀번호

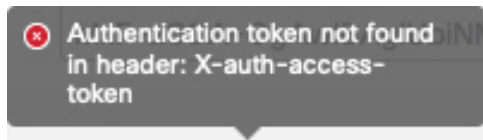
이 오류는 커넥터의 오류 조건 위에 마우스를 놓으면 툴팁으로 표시됩니다.



해결책: 커넥터를 편집하고 사용자 이름 또는 비밀번호를 변경합니다.

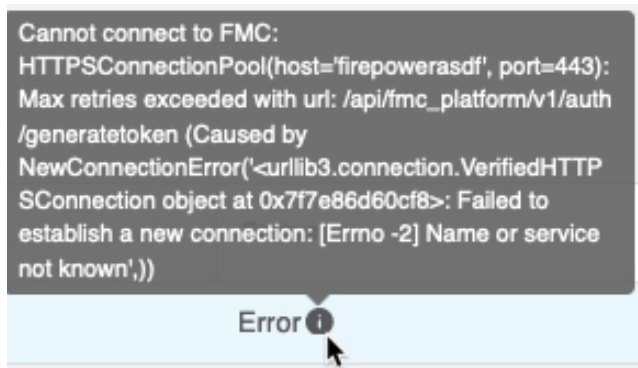
문제: 헤더에서 인증 토큰을 찾을 수 없음

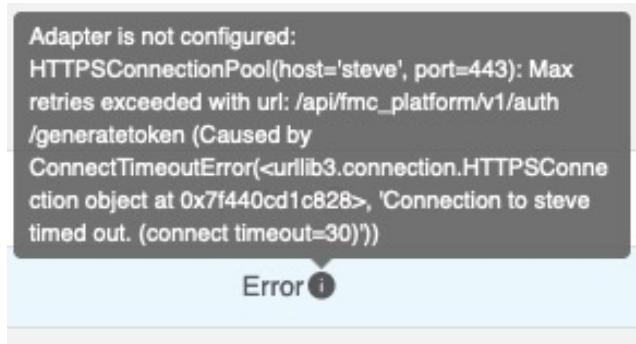
management center에 대한 충분한 권한이 없는 어댑터 사용자와의 연결을 테스트하려고 할 때 이 오류가 표시됩니다.



문제: 어댑터에 대한 시간 초과 또는 최대 재시도 오류

이 오류는 어댑터의 오류 조건 위에 마우스를 놓으면 툴팁으로 표시됩니다.





해결책: 다음을 모두 수행합니다.

- 관리 센터가 실행 중인지 확인합니다.
- **FMC Server Certificate(FMC 서버 인증서)** 필드의 내용을 확인합니다.
- **IP** 필드에 입력한 값이 인증서의 일반 이름과 정확히 일치하는지 확인합니다.

자세한 내용은 [CA\(Certificate Authority\) 체인 수동으로 가져오기, 32 페이지](#)를 참고하십시오.

트러블슈팅 툴

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 ~/csdac/app
sudo ./muster-cli status
```

샘플 출력은 다음과 같습니다.

```
===== CORE SERVICES =====
      Name                Command                State    Ports
-----
muster-bee      ./docker-entrypoint.sh run ...    Up          50049/tcp, 50050/tcp
muster-etcd     etcd                      Up          2379/tcp, 2380/tcp
muster-ui       /docker-entrypoint.sh runs ...    Up (healthy)
0.0.0.0:443->8443/tcp, :::443->8443/tcp
muster-ui-backend ./docker-entrypoint.sh run ...    Up          50031/tcp

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

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

동적 개체 확인

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

```
sudo tail -f /var/opt/CSCOpX/MDC/log/operation/usmshredsvcs.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": []
}
```

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, 29 페이지
- 어댑터 생성, 31 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.

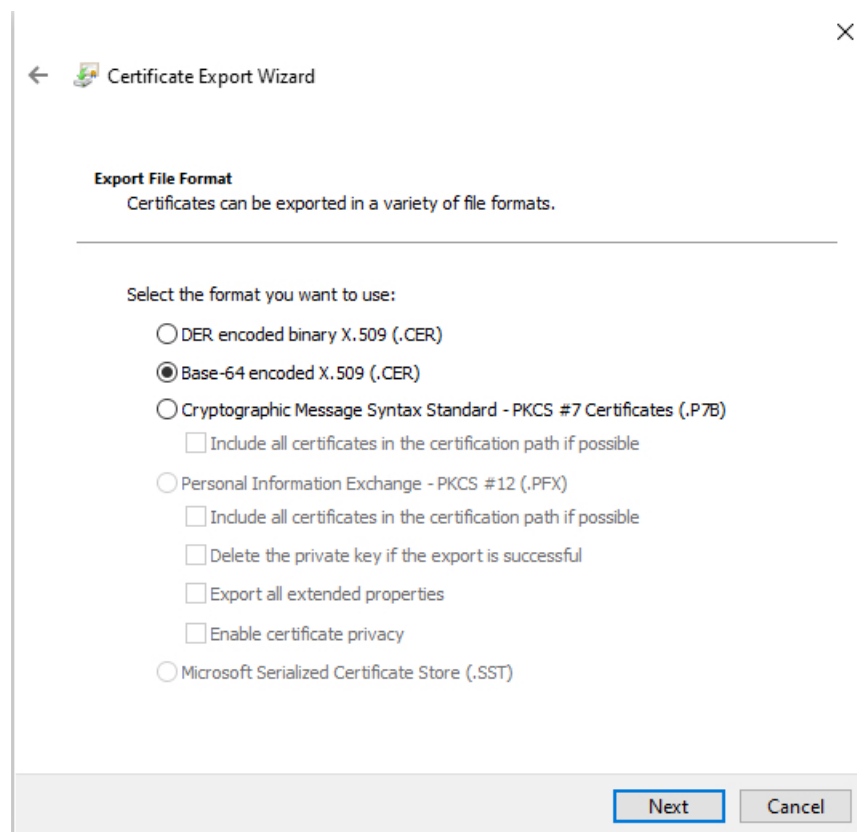
- 모든-----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 구분 기호를 포함합니다.
- 관련 없는 텍스트(예: 인증서의 이름 및 꺾쇠괄호(< 및 >)에 포함된 텍스트 및 꺾쇠괄호 자체)는 제외합니다.

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.

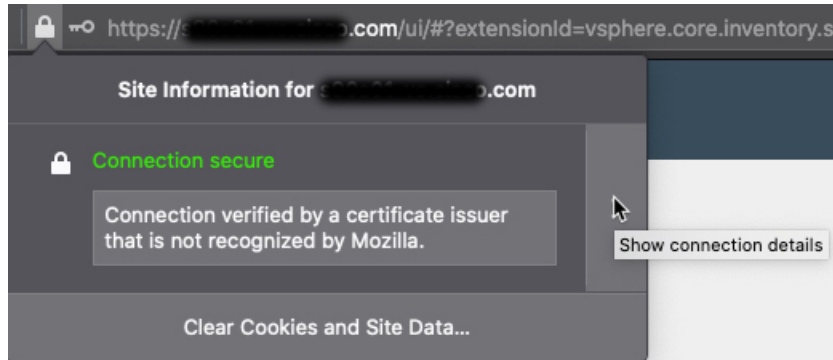


10. 프롬프트에 따라 내보내기를 완료합니다.
11. 텍스트 편집기에서 인증서를 엽니다.
12. 체인의 모든 인증서에 대해 프로세스를 반복합니다.
텍스트 편집기에서 각 인증서를 맨 처음부터 마지막 순서로 붙여넣어야 합니다.
13. vCenter와 FMC 모두에 대해 이 작업을 반복합니다.

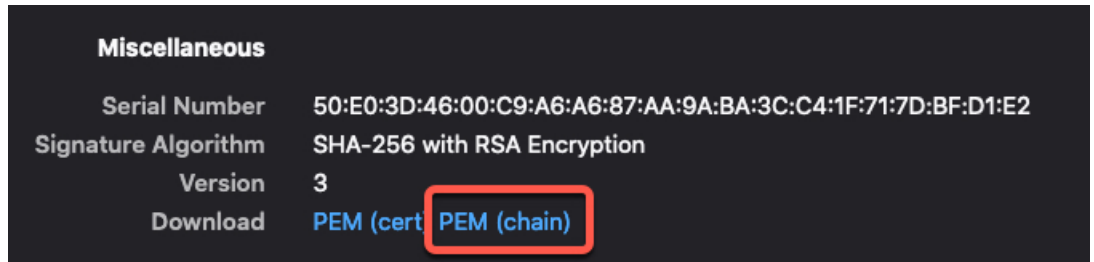
인증서 체인 가져오기 - Windows Firefox

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.



A 부록

안전한 인터넷 액세스

동적 속성 커넥터에서 클라우드 서비스 제공자 및 management center와 통신할 때 사용하는 URL의 목록입니다.

- 보안 요건, 55 페이지
- 인터넷 액세스 요구 사항, 55 페이지

보안 요건

Cisco Secure Dynamic Attributes Connector를 보호하려면 보호된 내부 네트워크에 설치해야 합니다. 필요한 서비스와 사용 가능한 포트만 사용하도록 동적 속성 커넥터를 구성한 경우에도 공격이 모퉁에 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
<code>https://fmc-ip/api/fmc_platform/v1/auth/generatetoken</code>	인증

URL	이유
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

동적 속성 커넥터 **AWS** 액세스 요구 사항

동적 속성 커넥터는 내장된 SDK 메서드를 호출하여 인스턴스 정보를 가져옵니다. 이러한 메서드는 지정된 지역을 기반으로 서비스 엔드포인트 URL을 내부적으로 쿼리합니다. 동적 속성 커넥터 AWS 웹 사이트 <https://docs.aws.amazon.com/general/latest/gr/ec2-service.html>에 설명되어 있습니다.

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.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.