

온프레미스 FMC에서 동적 O365 개체에 CSDAC 배포

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[Ubuntu 20.04의 CSDAC 배포](#)

[Office 365 커넥터 만들기](#)

[vCenter 커넥터 생성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Ubuntu 20.04의 Ansible과 함께 온프레미스 FMC에서 Dynamic Microsoft 365 개체용 CSDAC를 배포하고 통합하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- 기본 Linux 명령.
- 기본 Python, Docker, Ansible Knowledge입니다.
- 기본 Office 365 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 7.2.5 릴리스를 실행하는 Cisco FMCv(Firewall Management Center Virtual) VMware
- Cisco CSDAC(Secure Dynamic Attributes Connector) 릴리스 2.2.
- Ubuntu 4vCPU/8GB 릴리스 20.04.
- Docker 릴리스 24.0.6.

- 파이썬 3.8.10
- Ansible 2.12.10.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

CSDAC(Cisco Secure Dynamic Attributes)를 사용하면 클라우드 제공자로부터 네트워크 및 IP 주소와 같은 데이터를 수집하여 Cisco Secure Firewall Management Center에 전송하여 액세스 제어 정책 규칙에서 사용할 수 있습니다.

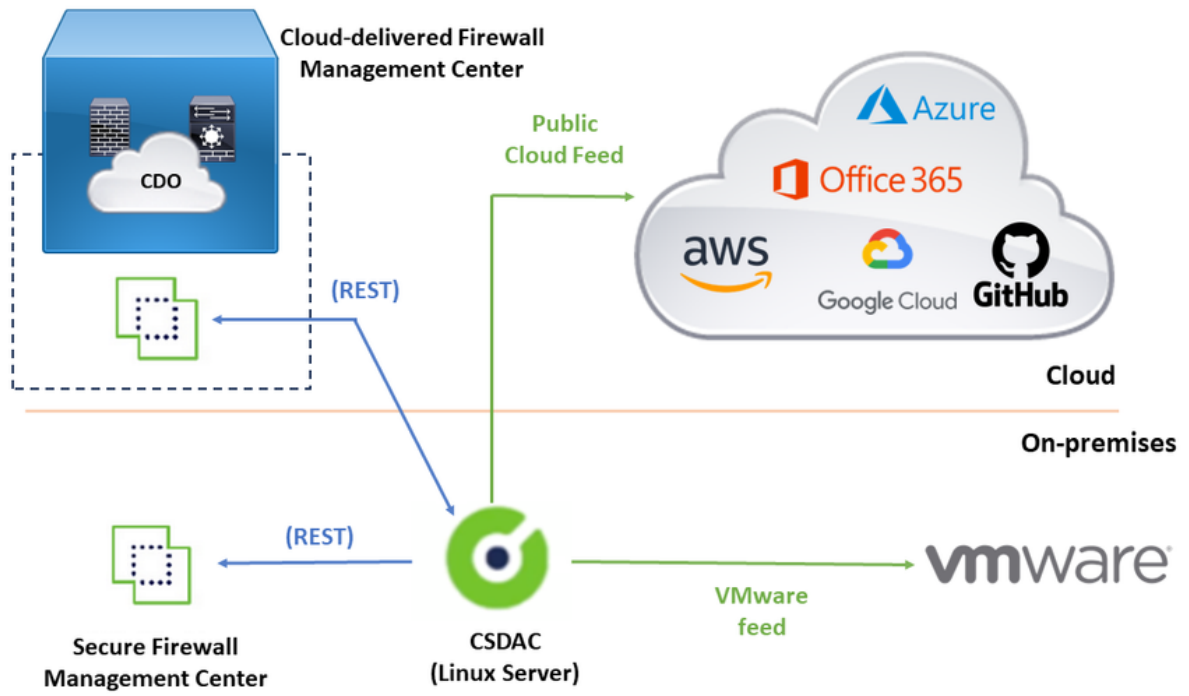
Cisco Secure Dynamic Attributes Connector에서는 AWS, Github, Google Cloud, Azure, Azure Service Tags, Microsoft Office 365, vCenter 등 다양한 클라우드 서비스 플랫폼의 서비스 태그 및 범주를 사용할 수 있습니다.

IP 주소와 같은 네트워크 구조는 워크로드의 동적 특성과 IP 주소 중복의 불가피성으로 인해 가상, 클라우드 및 컨테이너 환경에서 신뢰할 수 없습니다. 때로는 VM(가상 머신) 이름 또는 보안 그룹과 같은 비 네트워크 구문에 정책 규칙을 정의해야 합니다. 따라서 IP 주소 또는 VLAN이 변경되더라도 방화벽 정책은 유지됩니다. 이러한 태그와 특성은 Ubuntu, CentOS 또는 Red Hat Enterprise Linux 가상 머신에서 실행되는 동적 특성 커넥터 Docker 컨테이너를 사용하여 수집할 수 있습니다. CentOS 또는 Red Hat에 CSDAC를 설치하려면 [공식 설명서](#) 가이드를 [참조하십시오](#).

Ubuntu 호스트의 동적 특성 커넥터는 Ansible Collection을 사용하여 설치됩니다. Cisco Secure Dynamic Attributes는 2가지 유형의 어댑터를 지원합니다.

- 온프레미스 보안 방화벽 관리 센터
- 클라우드 기반 방화벽 관리 센터.

이 문서에서는 Cisco Secure Dynamic Attributes Connect on Ubuntu host for Microsoft Office 365 cloud service with on-prem Secure Firewall Management Center를 구축하는 방법을 중점적으로 다룹니다.

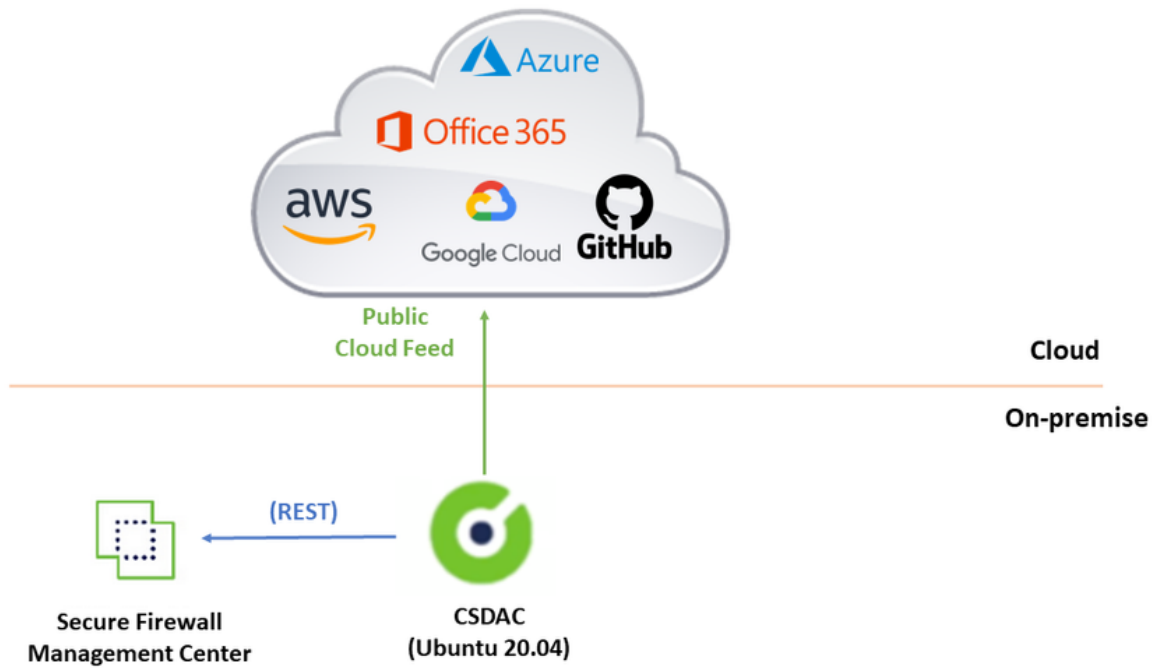


구성

이 섹션은 다음 섹션으로 구분됩니다.

- Ubuntu 20.04에서 CSDAC 배포.
- Office 365 커넥터를 만듭니다.
- vCenter 커넥터를 생성합니다.

네트워크 다이어그램



Ubuntu 20.04의 CSDAC 배포

이 섹션에서는 Ubuntu에 필수 소프트웨어를 설치하는 방법에 대해 설명합니다.

1단계: Docker가 설치되어 있는지 확인합니다.

```
root@tac:/home/tac# docker --version
```

```
Command 'docker' not found.
```

⚠ 경고: Docker가 설치되어 있는 경우 Docker 설명서를 참조하여 제거하십시오.


2단계: Ubuntu 저장소 업데이트

```
root@tac:/home/tac# sudo apt -y update && sudo apt -y upgrade
```

```
Hit:1 http://security-ubuntu-site/ubuntu focal-security InRelease
Hit:2 http://ubuntu-repository-web-site/ubuntu focal InRelease
Hit:3 http://ubuntu-repository-web-site/ubuntu focal-updates InRelease
Hit:4 http://ubuntu-repository-web-site/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
334 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree
....
```

3단계: Python 버전을 확인합니다.

```
root@tac:/home/tac# /usr/bin/python3 --version
Python 3.8.10
```

 경고: Python 버전이 3.6 이전인 경우 버전 3.6 이상을 설치해야 합니다.

4단계: 공통 라이브러리를 설치합니다.

```
root@tac:/home/tac# sudo apt -y install software-properties-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
...
```


5단계: Ansible 설치

```
root@tac:/home/tac# sudo apt-add-repository -y -u ppa:ansible/ansible && sudo apt -y install ansible
Hit:1 http://security-ubuntu-site/ubuntu focal-security InRelease
Get:2 http://personal-package-archive-site/ansible/ansible/ubuntu focal InRelease [18.0 kB]
Hit:3 http://ubuntu-repository-web-siteubuntu focal InRelease
Hit:4 http://ubuntu-repository-web-site/ubuntu focal-updates InRelease
Hit:5 http://ubuntu-repository-web-site/ubuntu focal-backports InRelease
Get:6 http://personal-package-archive-site/ansible/ansible/ubuntu focal/main amd64 Packages [1 132 B]
Get:7 http://personal-package-archive-site/ansible/ansible/ubuntu focal/main i386 Packages [1 132 B]
Get:8 http://personal-package-archive-site/ansible/ansible/ubuntu focal/main Translation-en [756 B]
Fetched 21.1 kB in 3s (7 526 B/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
...
```

6단계: Ansible 버전을 확인합니다.

```
root@tac:/home/tac# ansible --version
ansible [core 2.12.10]
config file = /etc/ansible/ansible.cfg
configured module search path = ['/root/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
ansible python module location = /usr/lib/python3/dist-packages/ansible
ansible collection location = /root/.ansible/collections:/usr/share/ansible/collections
executable location = /usr/bin/ansible
python version = 3.8.10 (default, May 26 2023, 14:05:08) [GCC 9.4.0]
```

```
jinja version = 2.10.1
libyaml = True
```

 참고: Ansible이 Python 2.x를 참조하는 것은 정상입니다. 커넥터는 여전히 Python 3.6을 사용합니다.

7단계: Ansible로 Dynamic Attributes Connector 소프트웨어를 가져옵니다.

```
root@tac:/home/tac# ansible-galaxy collection install cisco.csdac
Starting galaxy collection install process
Process install dependency map
Starting collection install process
Downloading https://galaxy-ansible-site/download/cisco-csdac-2.2.1.tar.gz to /root/.ansible/tmp/ansible
Downloading https://galaxy-ansible-site/download/community-crypto-2.15.1.tar.gz to /root/.ansible/tmp/a
Installing 'cisco.csdac:2.2.1' to '/root/.ansible/collections/ansible_collections/cisco/csdac'
cisco.csdac:2.2.1 was installed successfully
Installing 'community.crypto:2.15.1' to '/root/.ansible/collections/ansible_collections/community/crypt
Downloading https://galaxy-ansible-site/download/community-general-7.4.0.tar.gz to /root/.ansible/tmp/a
community.crypto:2.15.1 was installed successfully
Installing 'community.general:7.4.0' to '/root/.ansible/collections/ansible_collections/community/gener
community.general:7.4.0 was installed successfully
```

8단계: csdac 디렉토리로 이동합니다.

```
root@tac:/home/tac# cd ~/.ansible/collections/ansible_collections/cisco/csdac/
```

9단계: Muster 서비스를 설치합니다.

```
root@tac:~/.ansible/collections/ansible_collections/cisco/csdac# ansible-playbook default_playbook.yml
BECOME password:
[WARNING]: provided hosts list is empty, only localhost is available. Note that
the implicit localhost does not match 'all'
[WARNING]: running playbook inside collection cisco.csdac

PLAY [localhost] *****

TASK [Gathering Facts] *****
ok: [localhost]

TASK [cisco.csdac.csdac : Define Python Interpreter] *****
ok: [localhost]

...

TASK [cisco.csdac.csdac : verify that core services are started] *****
ok: [localhost]
```

```
TASK [cisco.csdac.csdac : verify that core services are started] *****
ok: [localhost]

TASK [cisco.csdac.csdac : verify that core services are started] *****
ok: [localhost]

TASK [cisco.csdac.csdac : verify that core services are started] *****
ok: [localhost]

TASK [cisco.csdac.csdac : Post task] *****
ok: [localhost] => {}
```

MSG:

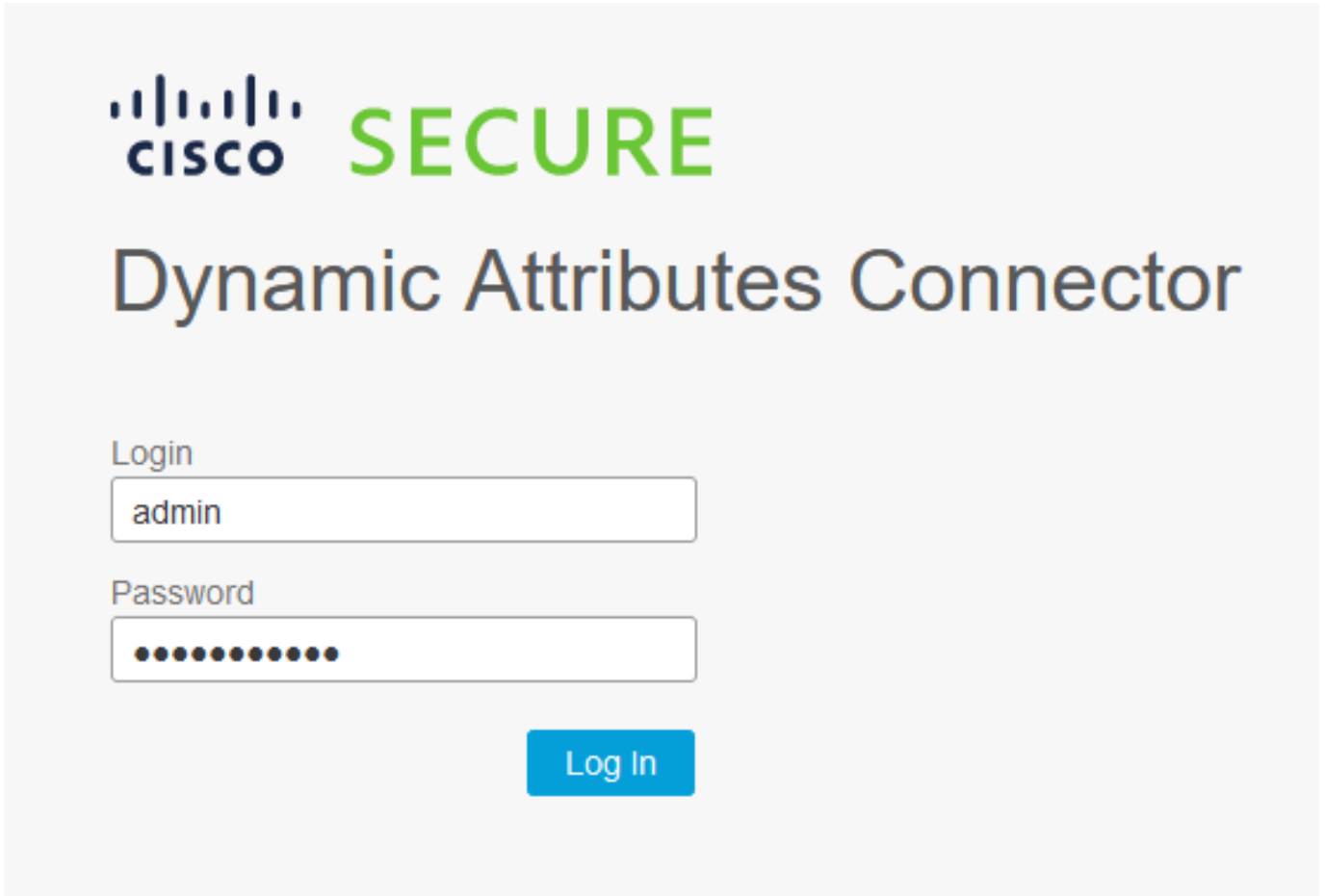
Please login in to <https://172.16.1.53> to configure csdac application

```
PLAY RECAP *****
localhost : ok=72 changed=8 unreachable=0 failed=0 skipped=35 rescued=0 ignored=0
```




경고: 'Docker 데몬 소켓에서 권한이 거부됨'으로 인해 설치에 실패한 경우 Cisco 버그 ID CSCwh58312를 고려하거나 Cisco TAC에 문의하십시오.

10단계: HTTPS 프로토콜을 사용하는 CSDAC IP 주소를 사용하여 커넥터에 로그인합니다.



The image shows a login interface for Cisco Secure Dynamic Attributes Connector. At the top left is the Cisco logo, followed by the word "SECURE" in green. Below that is the title "Dynamic Attributes Connector" in a large, dark blue font. The login section includes a "Login" label above a text input field containing "admin". Below that is a "Password" label above a password input field filled with black dots. A blue "Log In" button is positioned to the right of the password field.

 참고: 초기 로그인은 사용자 이름 'admin', 비밀번호 'admin'입니다. 시스템은 첫 번째 로그인 성공 후 비밀번호 변경을 요청합니다.

Office 365 커넥터 만들기

1단계: 동적 특성 커넥터에 로그인합니다.



Dynamic Attributes Connector

Login

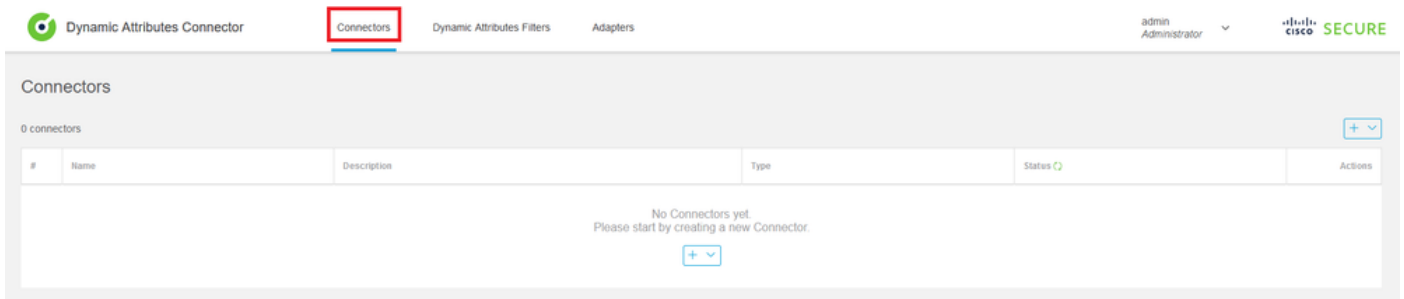
admin

Password

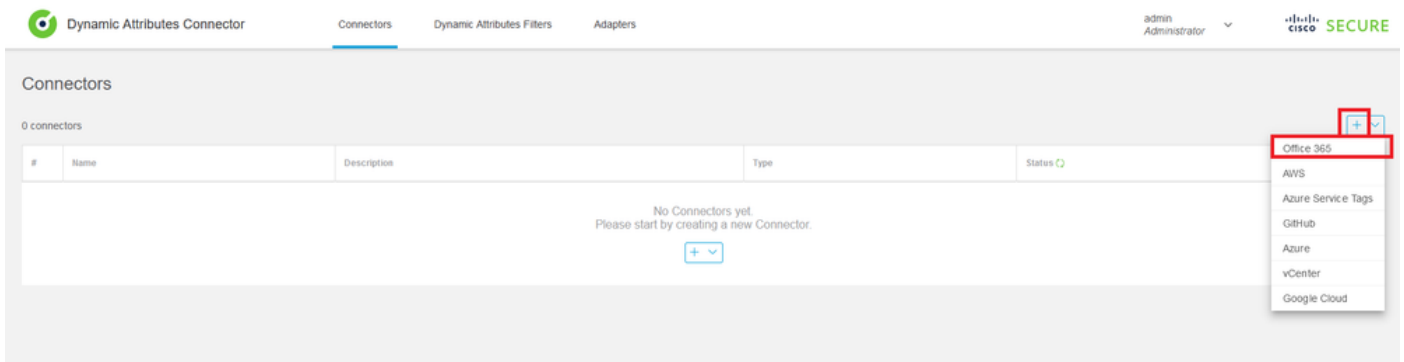
●●●●●●●●●●

Log In

2단계: '커넥터'를 클릭합니다.



3단계: Office 365 커넥터 추가: 추가 아이콘(+)을 클릭한 다음 'Office 365'를 클릭합니다.



4단계: Name(이름), Base API URL, Instance Name(인스턴스 이름), Enable(활성화) 또는 Disable(비활성화) 선택적 IP로 커넥터를 구성합니다.

Add Office 365 Connector

Name*	<input type="text" value="Cisco TAC"/>
Description	<input type="text"/>
Pull interval (sec)	<input type="text" value="30"/>
Base API URL*	<input type="text" value="https://endpoints.office.com"/>
Instance name*	<input type="text" value="Worldwide"/>
Disable optional IPs*	<input type="checkbox"/>

Test

Cancel

Save

다음 사항을 고려하십시오.

- Pull Interval 기본값은 30초입니다.
- 기본 API URL은 Office 365 정보를 검색하는 URL입니다. Microsoft 설명서에서 [Office 365 IP 주소 및 URL 웹](#) 서비스를 참조하십시오.

5단계: 커넥터 구성을 저장하기 전에 'Test'(테스트)를 클릭하고 테스트가 성공했는지 확인합니다.

Add Office 365 Connector

Name*

Description

Pull interval (sec)

Base API URL*

Instance name*

Disable optional IPs*

✓ Test connection succeeded

6단계: 저장하고 상태가 'OK'인지 확인합니다.

#	Name	Description	Type	Status	Actions
1	Cisco TAC		Office 365	Ok	

vCenter 커넥터 생성

1단계: 동적 특성 커넥터에 로그인합니다.



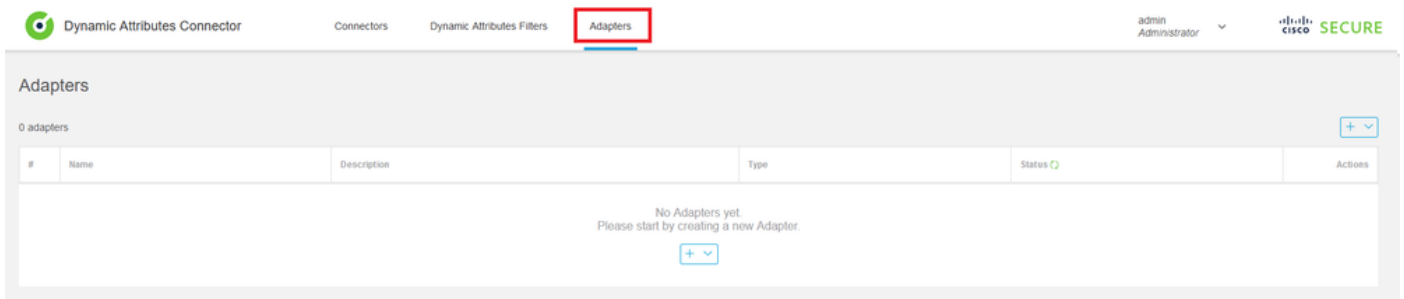
Dynamic Attributes Connector

Login

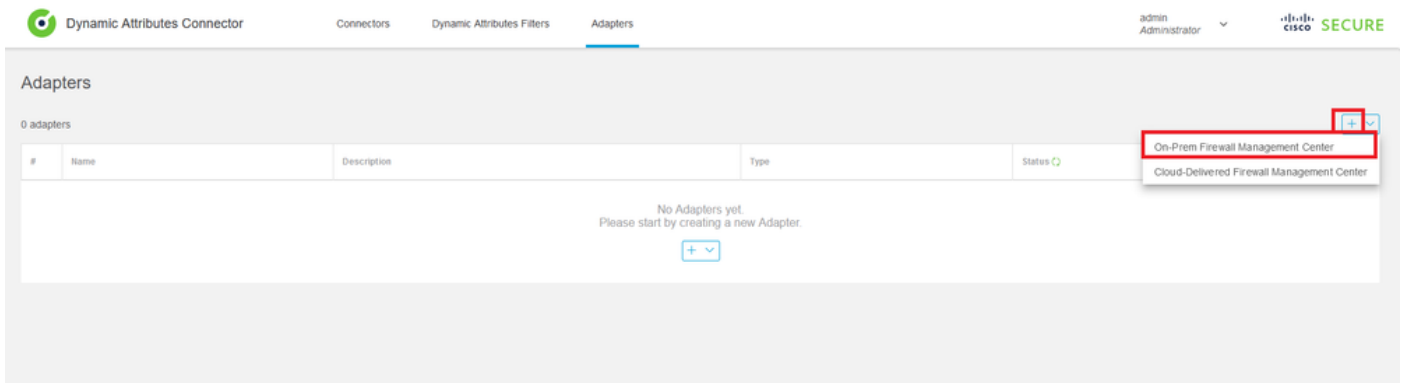
Password

Log In

2단계: '어댑터'를 클릭합니다.



3단계: 새 어댑터를 추가합니다. 추가 아이콘(+)을 클릭한 다음 'on-prem Firewall Management Center'를 클릭합니다.



4단계: 이름, IP 주소, 포트, 사용자/비밀번호로 어댑터를 구성합니다.

Add On-Prem Firewall Management Center Adapter


Name*	<input type="text" value="Cisco TAC On-Prem FMC"/>
Description	<input type="text"/>
Domain	<input type="text"/>
IP*	<input type="text" value="firepower.ciscotac.com"/>
Port*	<input type="text" value="443"/>
User*	<input type="text" value="TAC"/>
Password*	<input type="password" value="●●●●●●●●"/>
Secondary IP	<input type="text"/>
Secondary Port	<input type="text"/>
Secondary User	<input type="text"/>
Secondary Password	<input type="password"/>
Server Certificate*	<input type="text"/>
	<input type="button" value="Get certificate v"/>

Test

Cancel

Save

⚠ 경고: 어댑터 연결 전용 UI에서 새 FMC 사용자를 만듭니다. 기존 사용자를 사용하면 CSDAC 또는 On-Prem Firewall Management Center UI에서 예기치 않은 로그아웃이 발생할 수 있습니다.

 참고: 사용자 역할 구성에는 '관리자', '액세스 관리자' 또는 '네트워크 관리자' 역할이 있어야 합니다. IP 주소 필드에서 온프레미스 방화벽 관리 센터 FQDN을 사용합니다.

5단계: 온프레미스 방화벽 Secure Management Center UI를 엽니다.



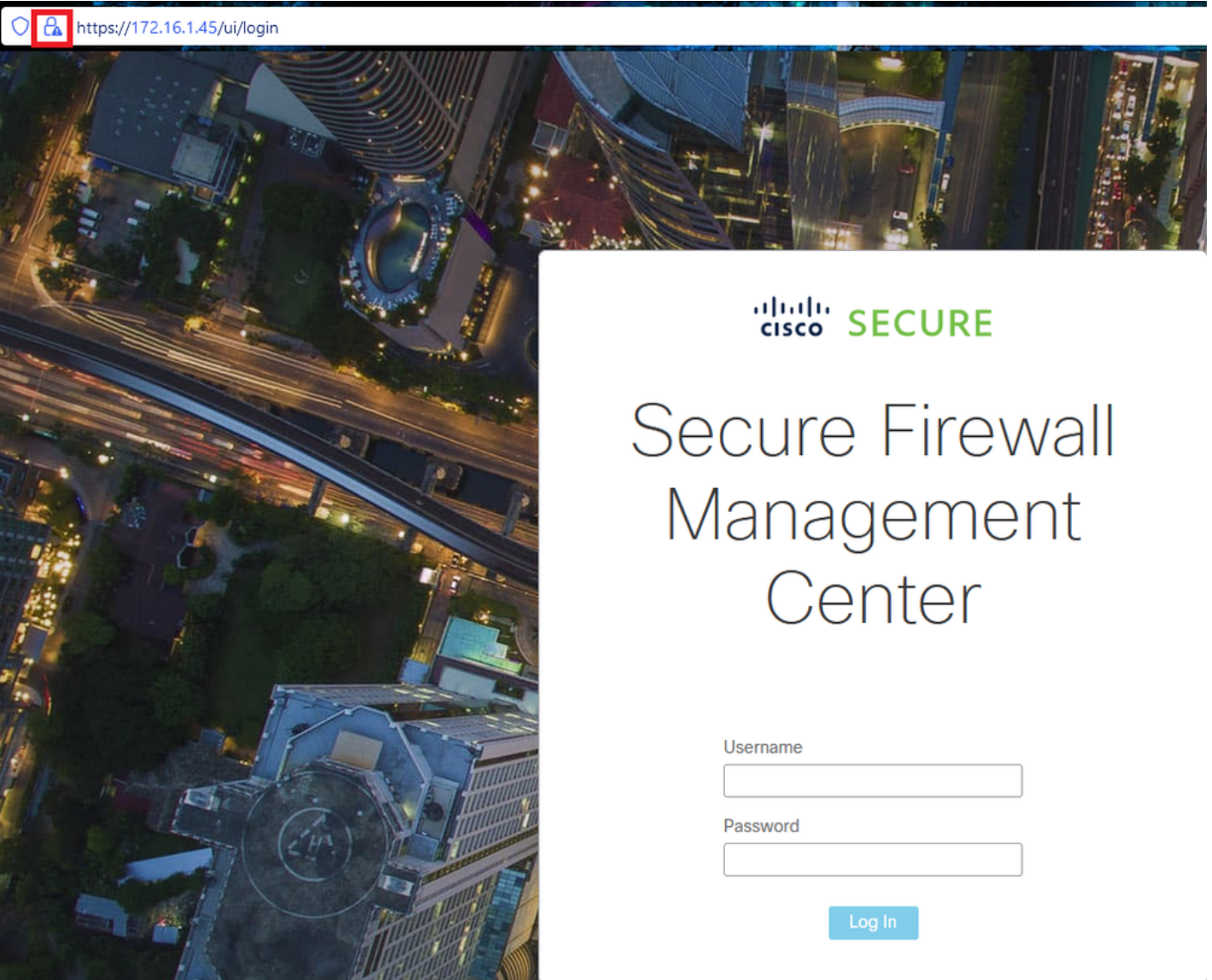
Secure Firewall Management Center

Username

Password


Log In

6단계: 브라우저에서 HTTPS PEM(chain) 인증서 다운로드: 브라우저에 표시된 HTTPS 자물쇠, Secure Connection, More Information, View Certificate, PEM(chain)을 클릭합니다.



Miscellaneous	
Serial Number	7 7C021700C0F3E6C00B057A0A2E0701C031E02E0
Signature Algorithm	SHA-256 with RSA Encryption
Version	1
Download	PEM (cert) PEM (chain)

인증서 체인이 있는 .pem 파일을 다운로드합니다.

 참고: Firefox 브라우저에 속하는 HTTPS On-Prem Secure Firewall Management Center 인증서를 수집하는 단계. 다른 브라우저가 사용되는 경우 유사한 단계를 찾습니다.

7단계: Dynamic Attributes Connector를 열고 'Get certificate'(인증서 가져오기) 및 'Browse from file...(파일에서 찾아보기...)'을 클릭합니다.

Add On-Prem Firewall Management Center Adapter

Name*	<input type="text" value="Cisco TAC On-Prem FMC"/>
Description	<input type="text"/>
Domain	<input type="text"/>
IP*	<input type="text" value="firepower.ciscotac.com"/>
Port*	<input type="text" value="443"/>
User*	<input type="text" value="TAC"/>
Password*	<input type="password" value="●●●●●●●●"/>
Secondary IP	<input type="text"/>
Secondary Port	<input type="text" value="443"/>
Secondary User	<input type="text"/>
Secondary Password	<input type="password"/>
Server Certificate*	<input type="text"/>

Get certificate ▾
Fetch ⓘ
Browse from file... ⓘ

8단계: .pem 인증서를 업로드하고 'TEST'를 클릭하여 테스트가 성공했는지 확인합니다.

Add On-Prem Firewall Management Center Adapter

Name*

Cisco TAC On-Prem FMC

Description

Domain

IP*

firepower.ciscotac.com

Port*

443

User*

TAC

Password*

●●●●●●●●●●

Secondary IP

Secondary Port

443

Secondary User

Secondary Password

Server Certificate*

```
-----BEGIN CERTIFICATE-----  
MIID6TCCAIECFHHN4bDI8+DNjdWoruZkj8mB5p4JMA0GC  
SqGSib3DQEBCwUAMIGw
```

Get certificate ▾


🔄 Updated

Test again

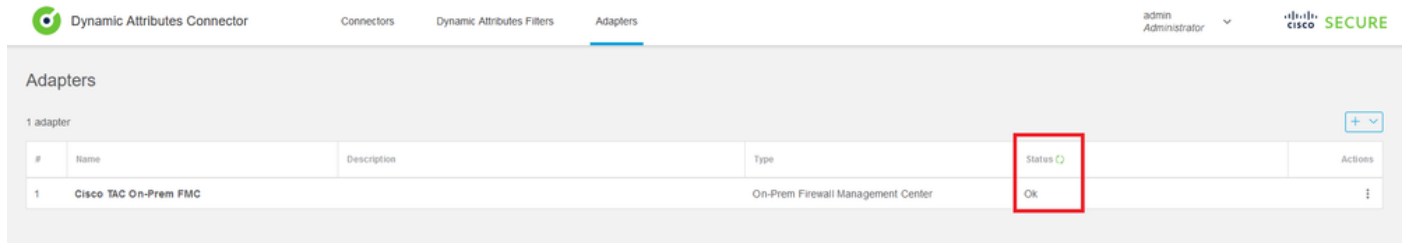
✓ Test connection succeeded


Cancel

Save

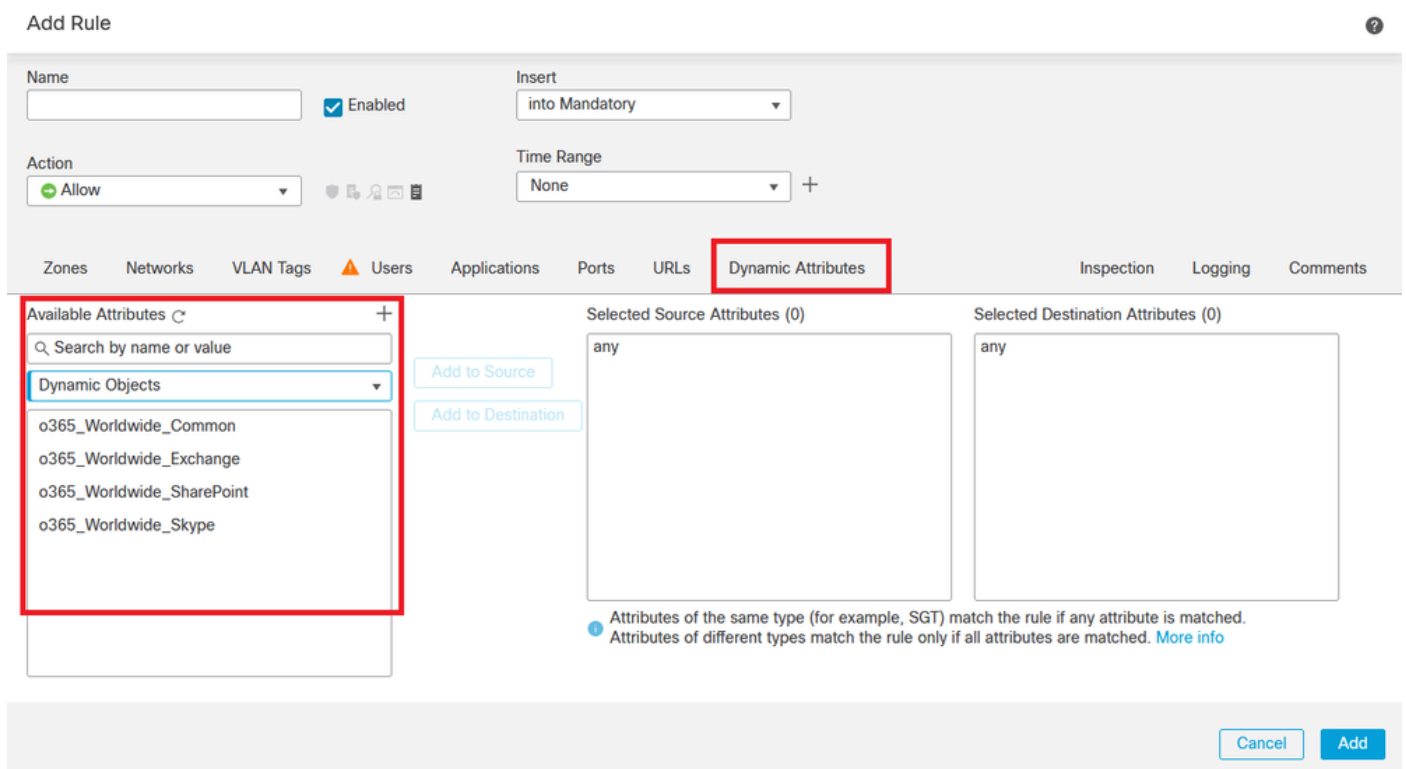
 경고: Ubuntu 컴퓨터에 구성된 DNS 서버가 온프레미스 방화벽 관리 센터 FQDN을 확인할 수 있는지 확인하십시오. 그렇지 않으면 테스트가 실패할 수 있습니다.

9단계: 저장하고 상태가 'OK'인지 확인합니다.



 참고: Office 365에 대해 동적 특성 필터를 만들 수 없습니다.

10단계: On-Prem Firewall Management Center UI에서 동적 Office 365 특성을 사용하여 액세스 제어 정책 규칙을 만들기 시작합니다.



다음을 확인합니다.

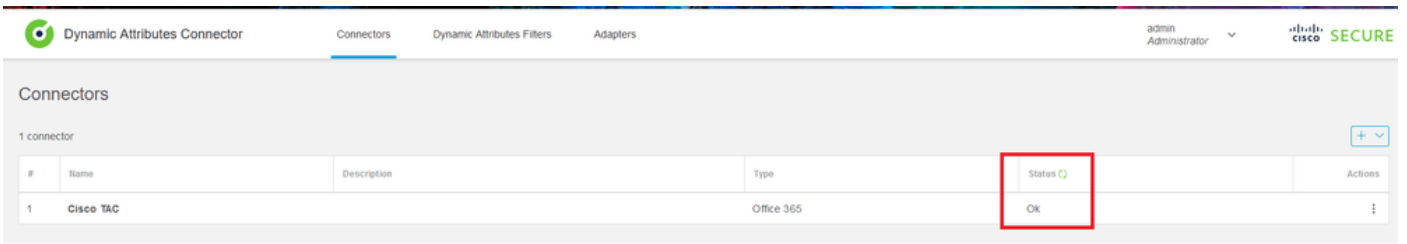
Ubuntu에서 코어 서비스, 커넥터 및 어댑터의 컨테이너 상태를 확인합니다.

```

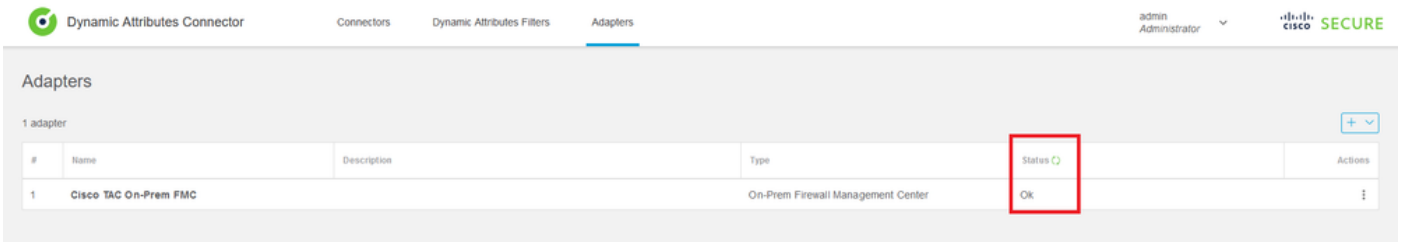
root@tac://# docker ps -a
CONTAINER ID IMAGE COMMAND CREATED
44f71f675ff1 public.ecr.aws/e6e4t5f5/muster_fmadapter:2.2.0-latest "/docker-entrypoint..." 12 hours
88826cf0742f public.ecr.aws/e6e4t5f5/muster_o365_connector:2.2.0-latest "/docker-entrypoint..." 13 hours
4c2c73d351e2 public.ecr.aws/e6e4t5f5/muster_envoy:2.2.0-latest "/docker-entrypoint..." 2 days ago
67f3afae2165 public.ecr.aws/e6e4t5f5/muster_ui:2.2.0-latest "/docker-entrypoint..." 2 days ago
722a764c54e9 public.ecr.aws/e6e4t5f5/muster_ui_backend:2.2.0-latest "/docker-entrypoint..." 2 days ago
038654545f30 public.ecr.aws/e6e4t5f5/muster_bee:2.2.0-latest "/bin/sh -c /app/bee" 2 days ago
90cfd7e3a28b public.ecr.aws/e6e4t5f5/muster_etcd:2.2.0-latest "etcd" 2 days ago

```

CSDAC UI에서 커넥터 상태를 확인합니다.

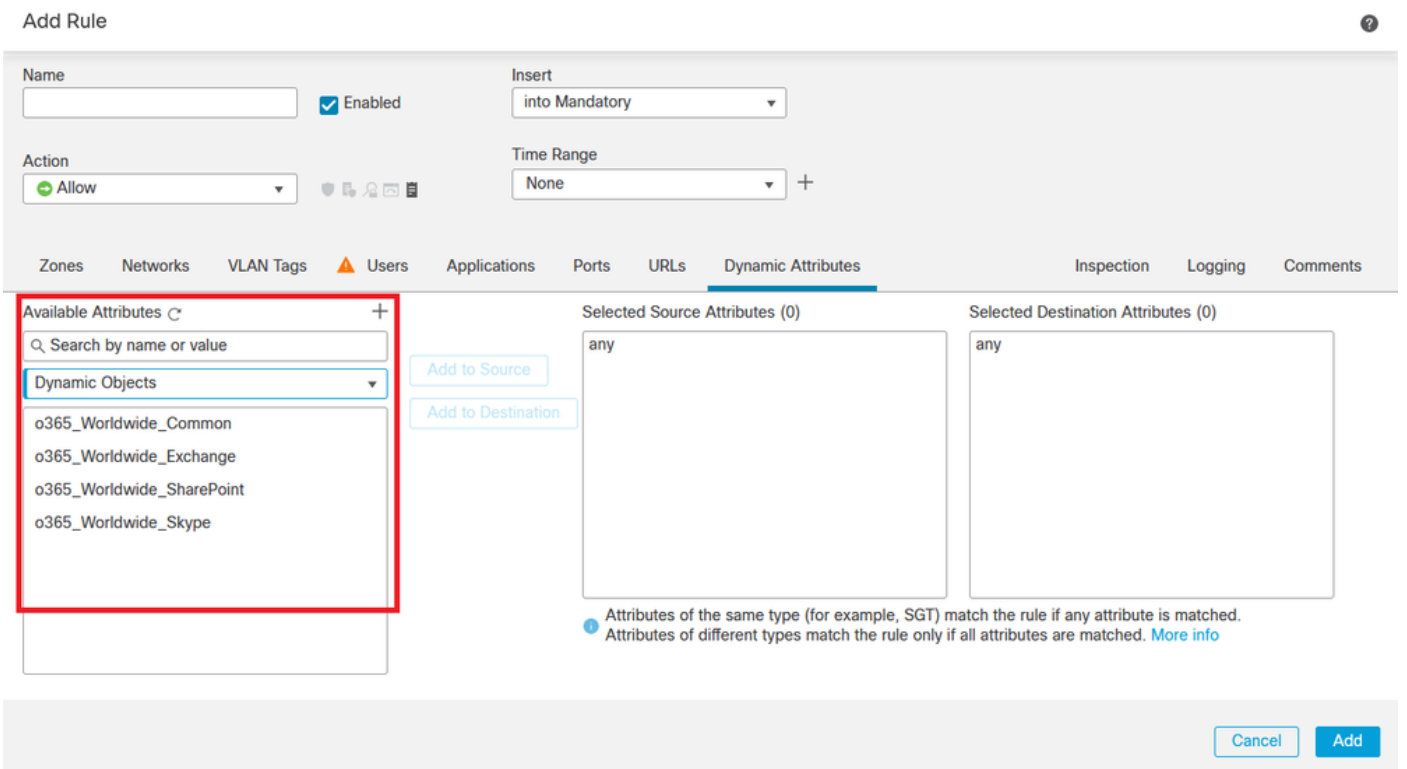


CSDAC UI에서 어댑터 상태를 확인합니다.



방화벽 관리 센터에서 Office 365 동적 특성을 확인합니다.

액세스 제어 정책 규칙을 만들거나 수정하고 'Dynamic Attributes'를 클릭하고 'Available Attributes'를 클릭한 후 'Dynamic Objects'를 선택합니다.



참고: Office 365 동적 개체가 나열되지 않으면 통합에 문제가 있을 수 있습니다. 문제 해결 섹션을 확인하거나 Cisco TAC에 문의하십시오.

문제 해결

Ansible의 Secure Dynamic Attributes Connector 설치 문제가 있는 경우

'~/ansible/collections/ansible_collection/cisco/csdac/logs/' 디렉터리에 있는 'csdac.log'를 수집합니다.

```
root@tac:~# cd ~/ansible/collections/ansible_collections/cisco/logs/
root@tac:~/ansible/collections/ansible_collections/cisco/csdac/logs# ls -lth
total 276K
-rw-r--r-- 1 root root 272K sep 14 15:37 csdac.log
```

설치 실패 로그가 이 파일에 있습니다. 'cat' 또는 'less' Linux 명령을 사용하여 열거나, 오류 로그를 탐색하거나, Cisco TAC에 문의하여 이 파일을 제공하십시오.

'권한이 거부되었습니다'로 인해 Ansible 설치가 실패하는 경우가 있습니다. csdac.log 파일을 탐색하고 '사용 권한 거부됨' 로그를 찾습니다.

```
TASK [cisco.csdac.csdac : print result of csdac command line start command (stderr)] ***
ok: [localhost] => {
  "muster_cli_start_result.stderr_lines": [
    "permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: ",
    "permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: ",
    "permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: ",
    "permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: ",
    "docker: permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docke",
    "See 'docker run --help'.",
    "docker: permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docke"
```

유사한 로그가 발견되면 Cisco 버그 ID CSCwh58312를 고려하거나 Cisco TAC에 문의하십시오.

'docker ps -a'가 컨테이너가 작동 중지되었거나 문제가 발생할 경우 컨테이너를 다시 시작하도록 나타내는 경우 'docker restart container-id' 명령을 사용하여 컨테이너를 다시 시작할 수 있습니다.

예: 컨테이너 ID가 '88826cf0742f'인 Office 365를 다시 시작합니다.

```
root@tac:~# docker ps -a
CONTAINER ID IMAGE COMMAND CREATED
44f71f675ff1 public.ecr.aws/e6e4t5f5/muster_fmc_adapter:2.2.0-latest "/docker-entrypoint..." 12 hour
88826cf0742f public.ecr.aws/e6e4t5f5/muster_o365_connector:2.2.0-latest "/docker-entrypoint..." 13 hour
```

```
root@tac:~# docker restart 88826cf0742f
```

```
root@tac:~# docker ps -a
CONTAINER ID IMAGE COMMAND CREATED
44f71f675ff1 public.ecr.aws/e6e4t5f5/muster_fmc_adapter:2.2.0-latest "/docker-entrypoint..." 12 hour
88826cf0742f public.ecr.aws/e6e4t5f5/muster_o365_connector:2.2.0-latest "/docker-entrypoint..." 13 hour
```

CSDAC와의 연결을 확인하고 개체가 Secure Firewall Management Center에 만들어졌는지 확인합니다.

```
> expert
sudoadmin@firepower:~$ sudo su -
Password:

root@firepower:/Volume/home/admin# cat /var/opt/CSC0px/MDC/log/operation/usmsharedsvcs.log
17-Sep-2023 17:24:58.046, [INFO], (DefenseCenterServiceImpl.java:1462)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-2
** REST Request [ CSM ]
** ID : ff3e6259-2417-48cc-8e5e-a41d0bd04b39
** URL: POST /audit
{
  "version":"7.2.5",
  "requestId":"ff3e6259-2417-48cc-8e5e-a41d0bd04b39",
  "data":{
    "userName":"TAC",
    "subsystem":"API",
    "message":"POST https://FMC-FQDN/api/fmc\_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/object/bulkdynamicobjects Created (201) - The request has been fulfilled and resulted in a new resource.
    "sourceIP":"172.16.1.53",
    "domainUuid":"e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time":"1694971497660"}, "deleteList":[]
  }
}
```

관련 정보

CSDAC(Cisco Secure Dynamic Attributes)와 관련된 추가 문서는 다음 위치에서 확인할 수 있습니다.

Cisco Dynamic Attributes 커넥터 정보

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/220/cisco-secure-dynamic-attributes-connector-v220/m_about-the-cisco-dynamic-attributes-connector_21.html

Cisco Secure Dynamic Attributes Connector 설치 및 업그레이드

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/220/cisco-secure-dynamic-attributes-connector-v220/install-the-cisco-secure-dynamic-attributes-connector.html>

Cisco Dynamic Attributes 커넥터 구성

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/220/cisco-secure-dynamic-attributes-connector-v220/configure-the-cisco-secure-dynamic-attributes-collector.html>

액세스 제어 정책에서 동적 개체 사용

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/220/cisco-secure-dynamic-attributes-connector-v220/use-dynamic-objects-in-access-control-rules.html>

동적 특성 커넥터 문제 해결

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/220/cisco-secure-dynamic-attributes-connector-v220/troubleshoot-the-dynamic-attributes-connector.html>

CSDAC 2.2 설치가 Ubuntu 20.04에서 "Docker 데몬 소켓으로 권한이 거부되었습니다."에 실패했습니다.

Cisco 버그 ID [CSCwh58312](#).

이 번역에 관하여

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