

Bereitstellung von CSDAC für dynamische O365-Objekte im lokalen FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[CSDAC-Bereitstellung unter Ubuntu 20.04](#)

[Erstellen eines Office 365-Connectors](#)

[vCenter-Connector erstellen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie CSDAC für dynamische Microsoft 365-Objekte auf dem lokalen FMC mit Ansible auf Ubuntu 20.04 bereitgestellt und integriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie folgende Themen kennen:

- Grundlegende Linux-Befehle.
- Grundlegendes Python-, Docker- und Ansible-Wissen
- Grundlegendes Office 365-Wissen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Firewall Management Center Virtual (FMCv) VMware mit Version 7.2.5.
- Cisco Secure Dynamic Attributes Connector (CSDAC) Version 2.2.
- Ubuntu 4vCPU/8GB Version 20.04.

- Docker-Version 24.0.6
- Python 3.8.10
- 2.12.10.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Cisco Secure Dynamic Attributes (CSDAC) ermöglichen die Erfassung von Daten wie Netzwerken und IP-Adressen von Cloud Providern und deren Übermittlung an das Cisco Secure Firewall Management Center, sodass diese in den Richtlinien für die Zugriffskontrolle verwendet werden können.

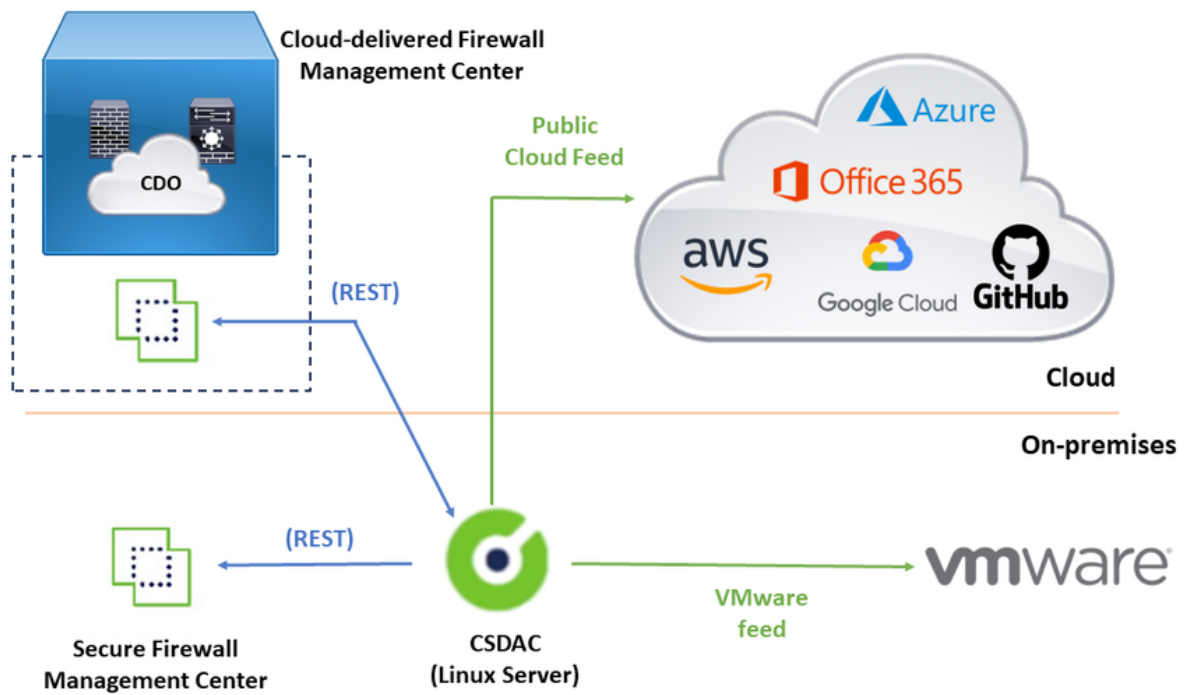
Der Cisco Secure Dynamic Attributes Connector ermöglicht die Verwendung von Service-Tags und Kategorien von verschiedenen Cloud-Service-Plattformen wie AWS, Github, Google Cloud, Azure, Azure Service Tags, Microsoft Office 365 und vCenter.

Netzwerkstrukturen wie IP-Adressen sind in virtuellen, Cloud- und Container-Umgebungen nicht zuverlässig, da die Workloads dynamisch sind und sich die IP-Adressen nicht überschneiden müssen. In manchen Fällen müssen Richtlinien für Konstrukte außerhalb des Netzwerks definiert werden, z. B. den Namen des virtuellen Systems (VM) oder die Sicherheitsgruppe. Daher sind Firewall-Richtlinien selbst dann persistent, wenn sich die IP-Adresse oder das VLAN ändern. Diese Tags und Attribute können mithilfe dynamischer Attribute-Connector Docker-Container gesammelt werden, die auf virtuellen Ubuntu-, CentOS- oder Red Hat Enterprise Linux-Systemen ausgeführt werden. Wenn Sie CSDAC auf CentOS oder Red Hat installieren möchten, lesen Sie das [offizielle Handbuch](#).

Der Connector für dynamische Attribute auf dem Ubuntu-Host wird mithilfe der Ansible Collection installiert. Cisco Secure Dynamic Attributes unterstützt zwei Arten von Adaptern.

- Sicheres Firewall-Management-Center vor Ort
- Über die Cloud bereitgestelltes Firewall Management Center

Dieser Artikel befasst sich mit der Bereitstellung von Cisco Secure Dynamic Attributes Connect auf Ubuntu-Hosts für Microsoft Office 365 Cloud-Services mit standortbasiertem Secure Firewall Management Center.

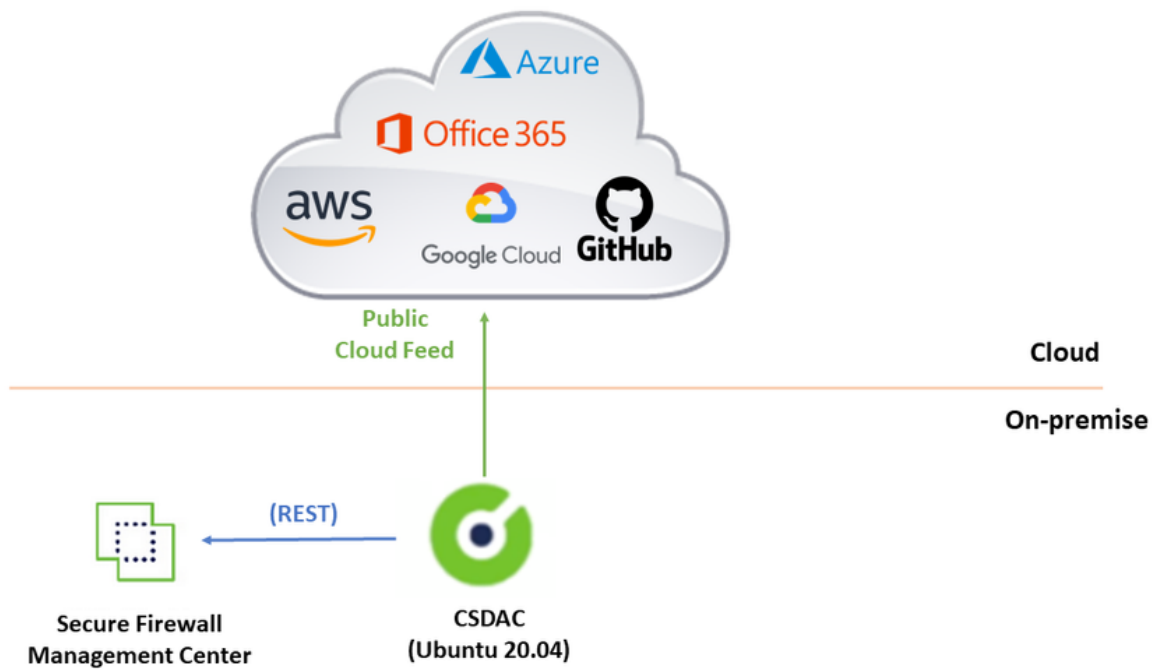


Konfigurieren

Dieser Abschnitt ist in die folgenden Abschnitte unterteilt:

- CSDAC-Bereitstellung unter Ubuntu 20.04.
- Office 365-Connector erstellen
- Erstellen Sie vCenter Connector.

Netzwerkdiagramm



CSDAC-Bereitstellung unter Ubuntu 20.04

In diesem Abschnitt wird beschrieben, wie Sie erforderliche Software unter Ubuntu installieren.

Schritt 1: Validate Docker ist nicht installiert.

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

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

⚠️ Warnung: Wenn Docker installiert ist, deinstallieren Sie es in der Dokumentation zu Docker.


Schritt 2: Aktualisieren von Ubuntu-Repositories

```
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
....
```

Schritt 3: Bestätigen Sie die Python-Version.

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

 **Warnung:** Wenn die Python-Version älter als 3.6 ist, müssen Sie Version 3.6 oder höher installieren.

Schritt 4: Installieren der allgemeinen Bibliotheken.

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

Schritt 5: Installieren von Ansible

```
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
...
```

Schritt 6: Überprüfen der Ansible-Version

```
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
```

 Hinweis: Es ist normal, dass Ansible auf Python 2.x verweist. Der Connector verwendet weiterhin Python 3.6.

Schritt 7: Holen Sie sich Dynamic Attributes Connector-Software mit Ansible.

```
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
```

Schritt 8: Wechseln zum csdac-Verzeichnis.

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

Schritt 9: Installieren Sie den Musterdienst.

```
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:

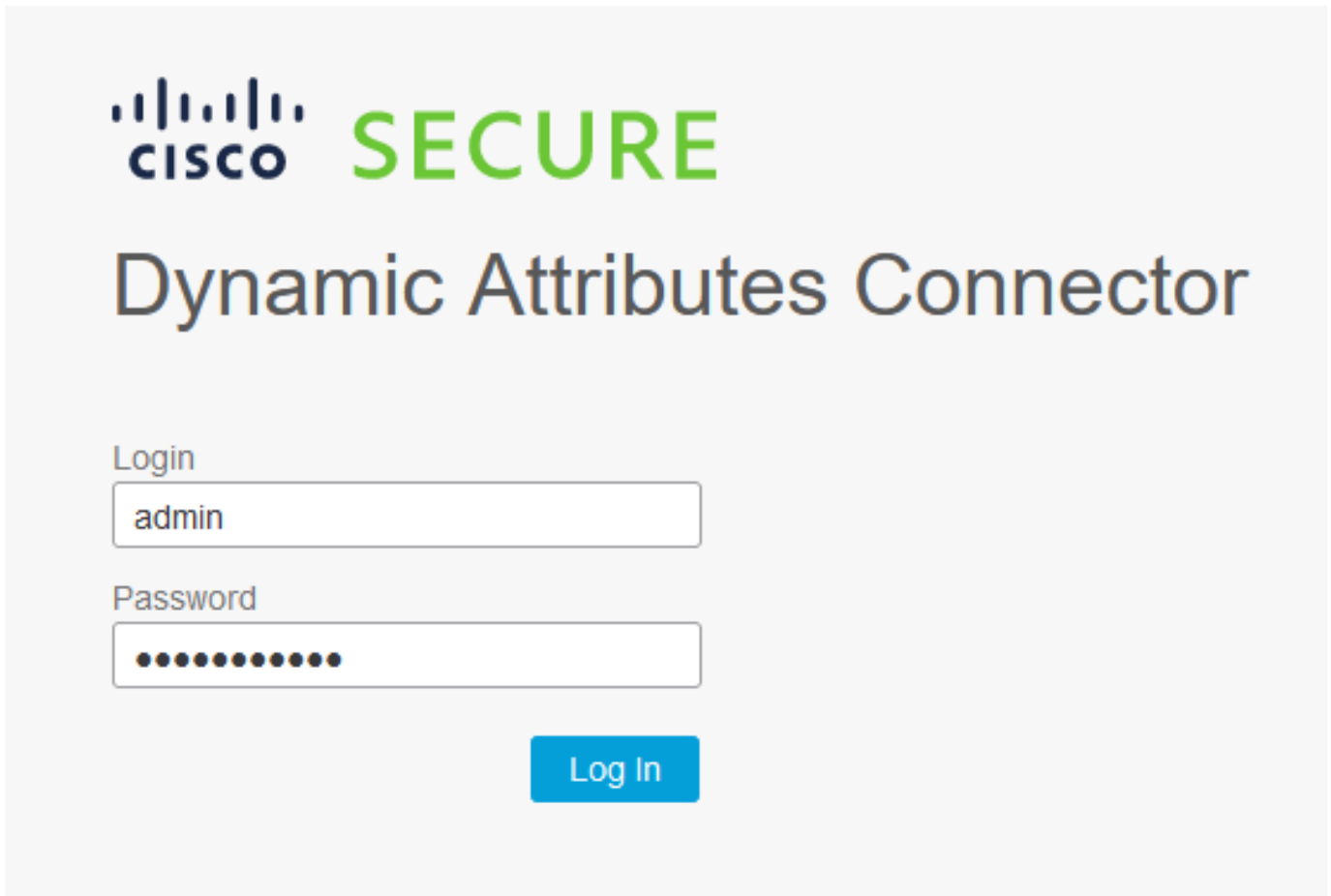
Please login in to <https://172.16.1.53> to configure csdac application

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




Warnung: Wenn die Installation aufgrund von "Mit Docker-Daemon-Socket verweigerte Berechtigungen" fehlschlägt, ziehen Sie die Cisco Bug-ID [CSCwh58312 in](#) Betracht, oder wenden Sie sich an das Cisco TAC.

Schritt 10: Melden Sie sich mit der CSDAC-IP-Adresse und dem HTTPS-Protokoll beim Connector an.



The screenshot shows the login interface for the Cisco Secure Dynamic Attributes Connector. At the top left is the Cisco logo, followed by the word "SECURE" in a large, green, sans-serif font. Below this, the title "Dynamic Attributes Connector" is displayed in a large, dark blue, sans-serif font. Underneath the title, there are two input fields. The first is labeled "Login" and contains the text "admin". The second is labeled "Password" and contains a series of black dots representing a masked password. Below the password field is a blue button with the text "Log In" in white.

 Hinweis: Bei der ersten Anmeldung handelt es sich um den Benutzernamen "admin" und das Kennwort "admin". Nach der ersten erfolgreichen Anmeldung fordert das System eine Kennwortänderung an.

Erstellen eines Office 365-Connectors

Schritt 1: Melden Sie sich beim Connector für dynamische Attribute an.



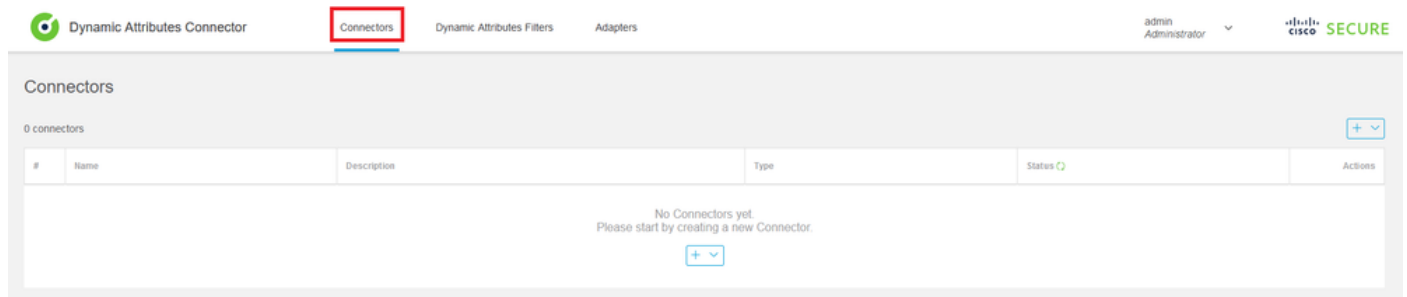
Dynamic Attributes Connector

Login

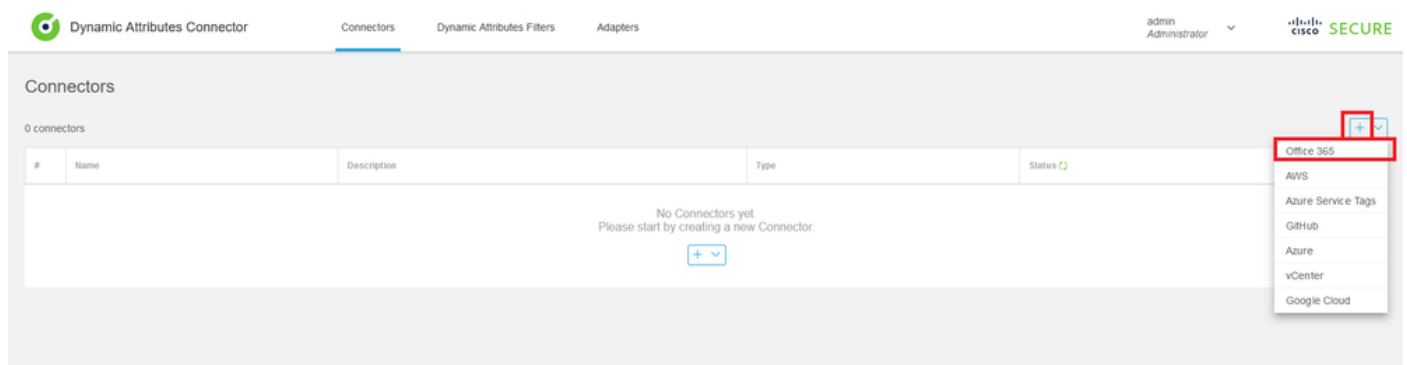
Password

Log In

Schritt 2: Klicken Sie auf "Anschlüsse".



Schritt 3: Fügen Sie einen Office 365-Connector hinzu: Klicken Sie auf das Symbol zum Hinzufügen (+) und dann auf "Office 365".



Schritt 4: Konfigurieren Sie den Connector mit Name, Basis-API-URL, Instanzname und

optionalen IPs aktivieren oder deaktivieren.

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

Betrachten wir die nächsten Punkte:

- Das Pull-Intervall beträgt standardmäßig 30 Sekunden.
- Die Basis-API-URL ist die URL zum Abrufen von Office 365-Informationen. Weitere Informationen finden Sie im Microsoft-Dokumentationsleitfaden unter der [Office 365-IP-Adresse und dem URL-Webdienst](#).

Schritt 5: Klicken Sie auf 'Test', und stellen Sie sicher, dass der Test erfolgreich ist, bevor Sie die Connector-Konfiguration speichern.

Add Office 365 Connector

Name*

Description

Pull interval (sec)

Base API URL*

Instance name*

Disable optional IPs*

✓ *Test connection succeeded*

Schritt 6: Speichern Sie, und vergewissern Sie sich, dass der Status "OK" lautet.

Dynamic Attributes Connector Connectors Dynamic Attributes Filters Adapters admin Administrator Cisco SECURE

Connectors

1 connector +

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

vCenter-Connector erstellen

Schritt 1: Melden Sie sich beim Connector für dynamische Attribute an.



Dynamic Attributes Connector

Login

Password

Log In

Schritt 2: Klicken Sie auf 'Adapter'.

The screenshot shows the Cisco Secure Dynamic Attributes Connector interface. The navigation menu at the top includes 'Connectors', 'Dynamic Attributes Filters', and 'Adapters', with 'Adapters' highlighted and enclosed in a red box. The main content area is titled 'Adapters' and shows '0 adapters'. Below this is a table with columns for '#', 'Name', 'Description', 'Type', 'Status', and 'Actions'. A message in the center of the table reads: 'No Adapters yet. Please start by creating a new Adapter.' with a '+ v' button below it.

Schritt 3: Fügen Sie einen neuen Adapter hinzu: Klicken Sie auf das Symbol Add (+) und dann auf "on-prem Firewall Management Center".

This screenshot shows the same interface as the previous one, but with the '+ v' button in the top right corner of the table area highlighted with a red box. A dropdown menu is open, showing two options: 'On-Prem Firewall Management Center' and 'Cloud-Delivered Firewall Management Center'. The first option is selected and also highlighted with a red box.

Schritt 4: Konfigurieren Sie den Adapter mit Name, IP-Adresse, Port und Benutzer/Kennwort.


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

 **Warnung:** Erstellen Sie einen neuen FMC-Benutzer auf der Benutzeroberfläche, die der Adapterverbindung zugewiesen ist. Die Verwendung eines vorhandenen Benutzers kann zu unerwarteten Abmeldungen auf der Benutzeroberfläche von CSDAC oder dem

 standortbasierten Firewall Management Center führen.

 Hinweis: Die Benutzerrollenkonfiguration muss über die Rollen 'Administrator', 'Zugriffsadministrator' oder 'Netzwerkadministrator' verfügen. Verwenden Sie im Feld für die IP-Adresse den FQDN des standortbasierten Firewall Management Center.

Schritt 5: Öffnen Sie die Benutzeroberfläche von Firewall Secure Management Center vor Ort.



Secure Firewall Management Center

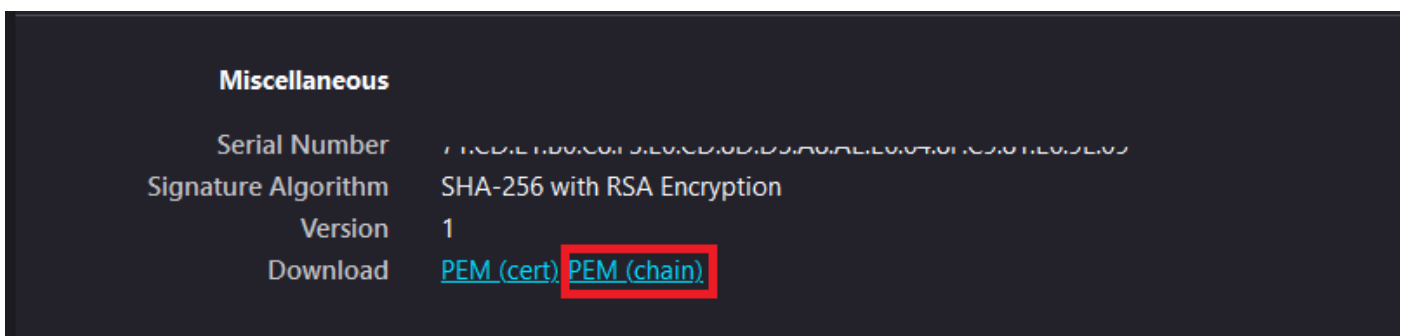
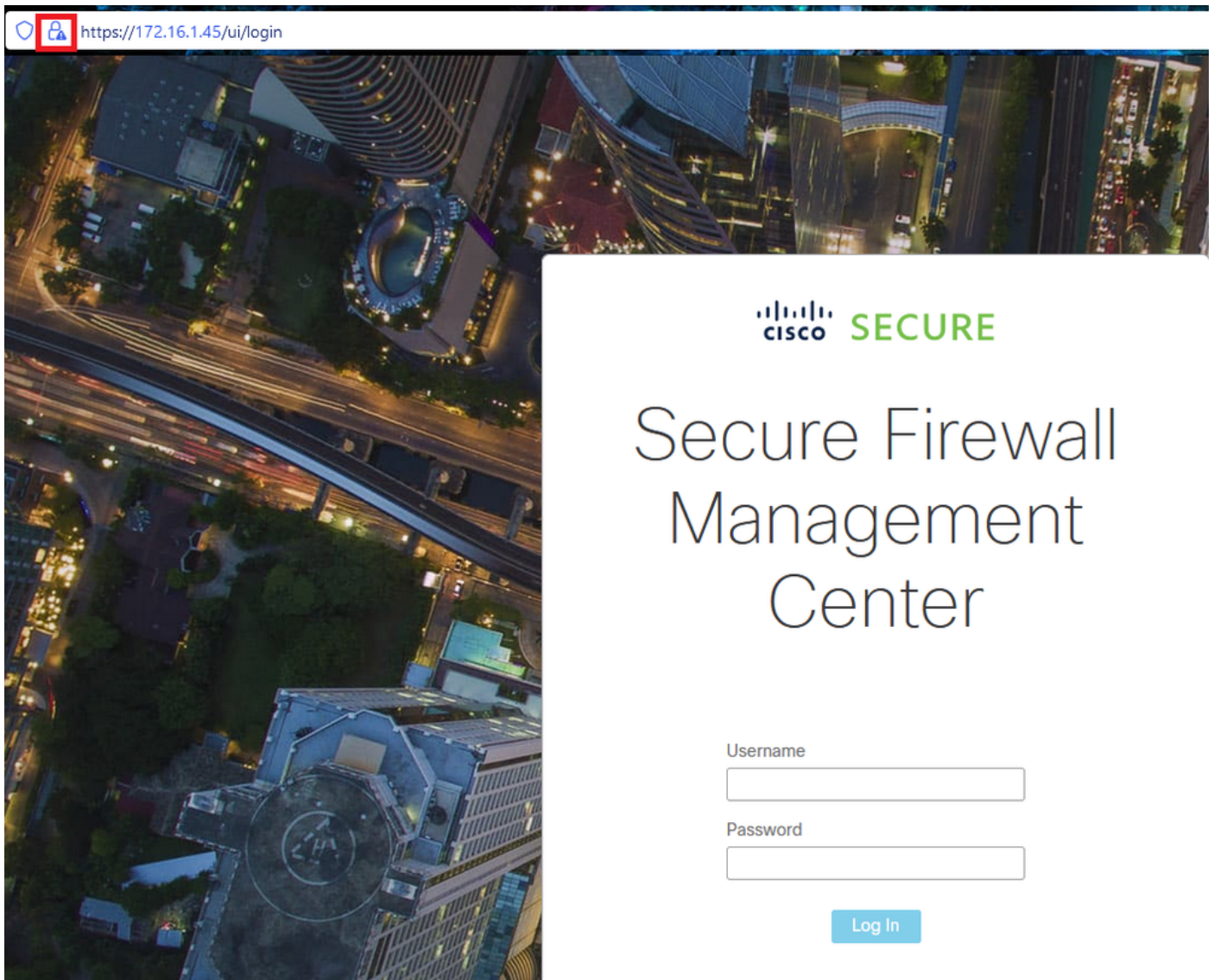
Username

Password


Log In

Schritt 6: Herunterladen HTTPS PEM (Kette) Zertifikat aus dem Browser: Klicken Sie auf HTTPS

Vorhängeschloss angezeigt im Browser, Sichere Verbindung, Weitere Informationen, Zertifikat anzeigen, PEM (Kette).



Lädt eine PEM-Datei mit der Zertifikatskette herunter.

 Hinweis: Die Schritte zum Erfassen des Zertifikats HTTPS On-Prem Secure Firewall Management Center gehören zum Firefox-Browser. Suchen Sie nach ähnlichen Schritten, wenn Sie einen anderen Browser verwenden.

Schritt 7: Öffnen Sie Dynamic Attributes Connector und klicken Sie auf 'Zertifikat abrufen' und 'Aus Datei durchsuchen...!'.

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="text"/>
Server Certificate*	<input type="text"/>

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

TestCancelSave

Schritt 8: Laden Sie das PEM-Zertifikat hoch, und klicken Sie auf "TEST", um sicherzustellen,


dass der Test erfolgreich ist.

Add On-Prem Firewall Management Center Adapter

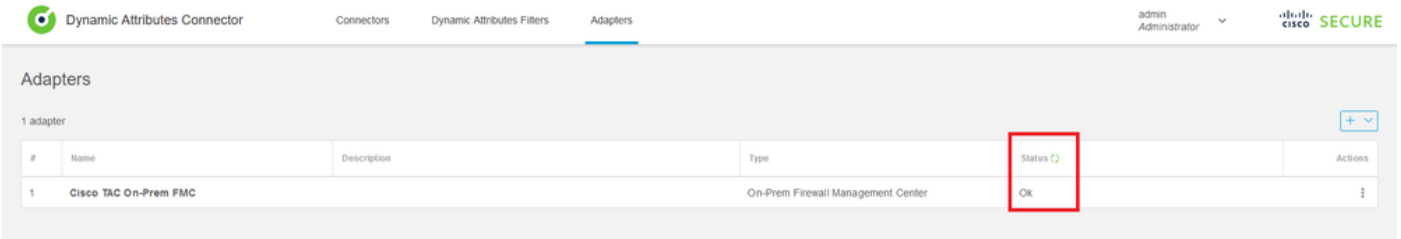
Name*	<input type="text" value="Cisco TAC On-Prem FMC"/>
Description	<input type="text"/>
Domain	<input type="text"/>
IP*	<input type="text" value="firepower.ciscotac.com"/>
Port*	<input type="text" value="443"/>
User*	<input type="text" value="TAC"/>
Password*	<input type="password" value="●●●●●●●●"/>
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" value="-----BEGIN CERTIFICATE-----
MIID6TCCAIECFHHN4bDI8+DNjdWoruZkj8mB5p4JMA0GC
SqGSib3DQEBCwUAMIGw"/>
	<input type="button" value="Get certificate"/> <input type="button" value="Updated"/>

Test connection succeeded

 **Warnung:** Stellen Sie sicher, dass die auf dem Ubuntu-Computer konfigurierten DNS-Server

 den FQDN des lokalen Firewall Management Center auflösen können, da andernfalls der Test fehlschlagen kann.

Schritt 9: Speichern Sie, und vergewissern Sie sich, dass der Status "OK" lautet.



Dynamic Attributes Connector

Connectors Dynamic Attributes Filters Adapters

admin Administrator

CISCO SECURE

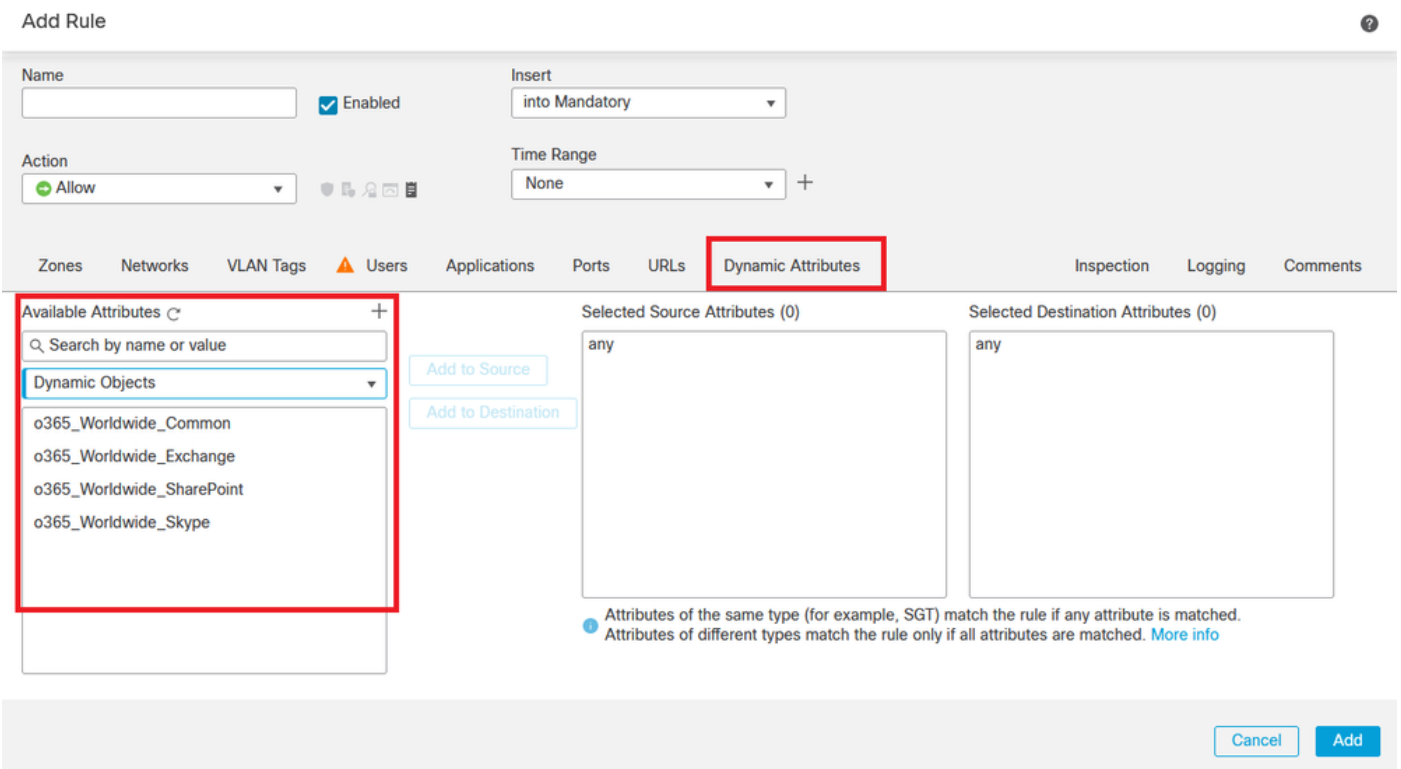
Adapters

1 adapter

#	Name	Description	Type	Status	Actions
1	Cisco TAC On-Prem FMC		On-Prem Firewall Management Center	OK	

 Hinweis: Für Office 365 können keine Filter für dynamische Attribute erstellt werden.

Schritt 10: Erstellen Sie Zugriffskontrollrichtlinien mit dynamischen Office 365-Attributen auf der Benutzeroberfläche des standortbasierten Firewall Management Centers.



Add Rule

Name Enabled Insert into Mandatory

Action Time Range None

Zones Networks VLAN Tags Users Applications Ports URLs **Dynamic Attributes** Inspection Logging Comments

Available Attributes +

Search by name or value

Dynamic Objects

o365_Worldwide_Common

o365_Worldwide_Exchange

o365_Worldwide_SharePoint

o365_Worldwide_Skype

Add to Source

Add to Destination

Selected Source Attributes (0)

any

Selected Destination Attributes (0)

any

Attributes of the same type (for example, SGT) match the rule if any attribute is matched. Attributes of different types match the rule only if all attributes are matched. [More info](#)

Cancel Add

Überprüfung

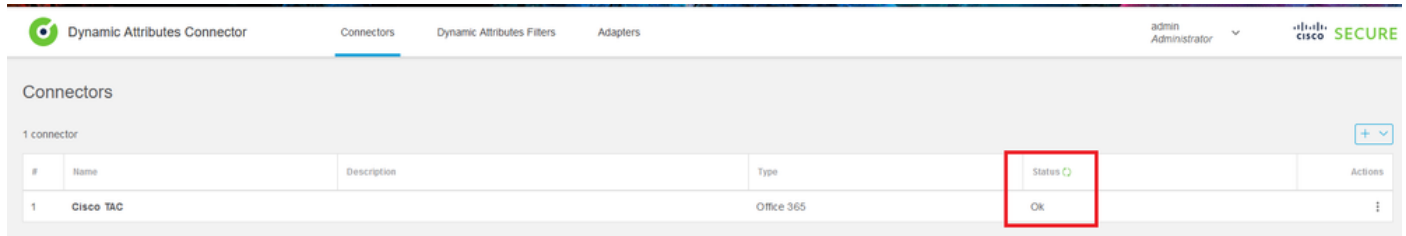
Überprüfen Sie den Containerstatus unter Ubuntu für Core-Services, Anschlüsse und Adapter.

```
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 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 a
```

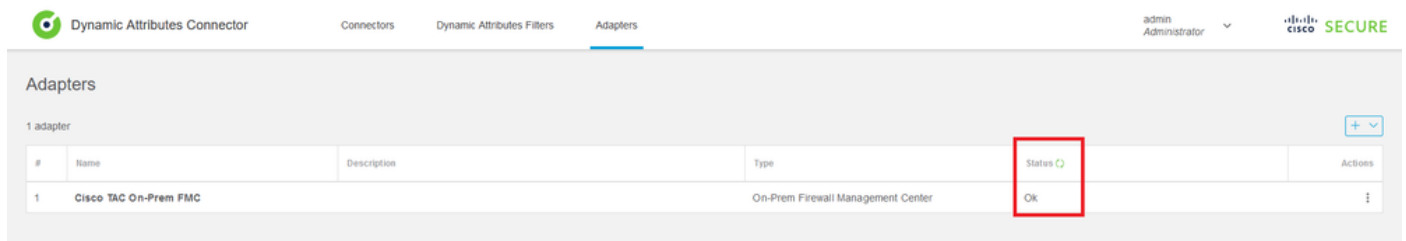
67f3afae2165 public.ecr.aws/e6e4t5f5/muster_ui:2.2.0-latest
 722a764c54e9 public.ecr.aws/e6e4t5f5/muster_ui_backend:2.2.0-latest
 038654545f30 public.ecr.aws/e6e4t5f5/muster_bee:2.2.0-latest
 90cfd7e3a28b public.ecr.aws/e6e4t5f5/muster_etcd:2.2.0-latest

"/docker-entrypoint..." 2 days a
 "./docker-entrypoint..." 2 days a
 "/bin/sh -c /app/bee" 2 days a
 "etcd" 2 days a

Überprüfen des Connector-Status über die CSDAC-Benutzeroberfläche

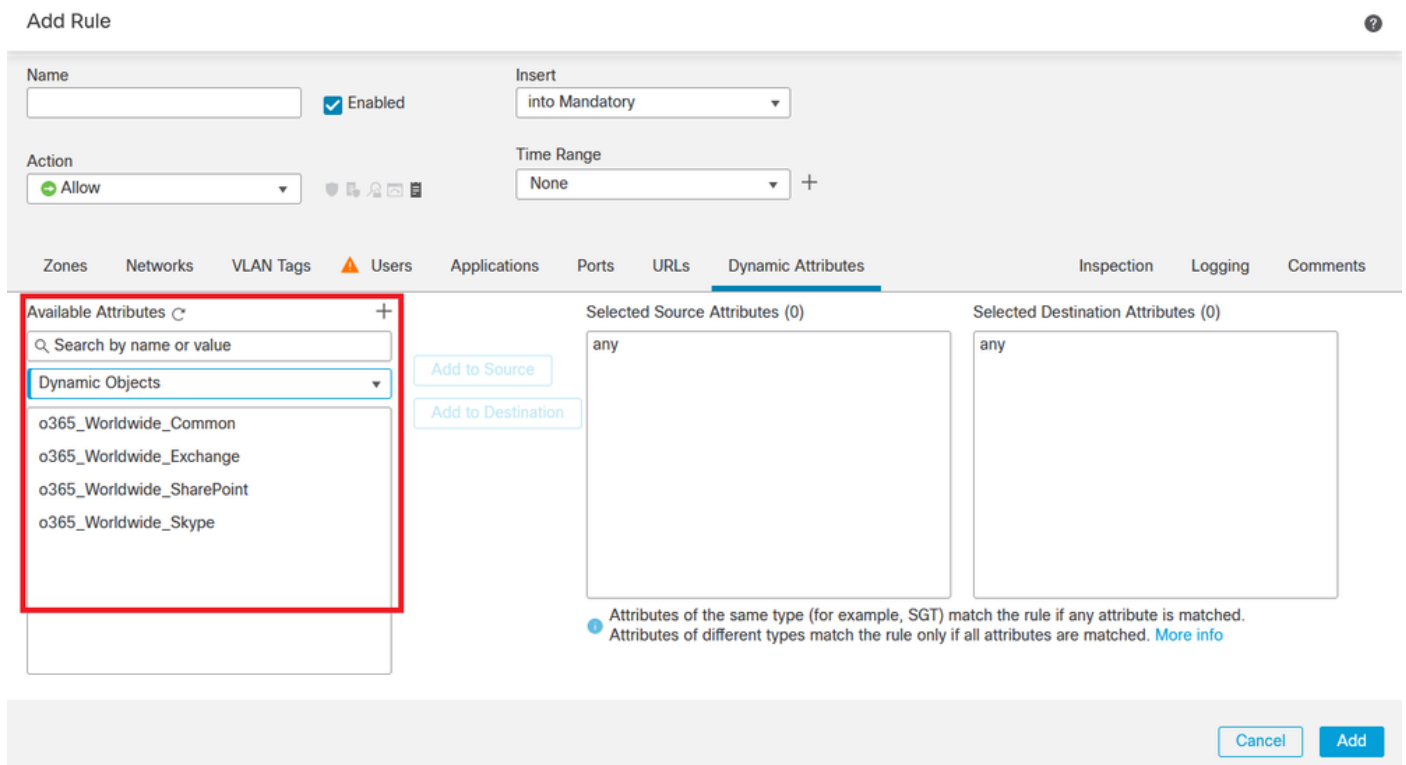



Überprüfen Sie den Adapterstatus über die CSDAC-Benutzeroberfläche.



Überprüfen der dynamischen Office 365-Attribute im Firewall Management Center

Erstellen oder bearbeiten Sie eine Zugriffskontrollrichtlinien-Regel, klicken Sie auf "Dynamic Attributes", klicken Sie auf "Available Attributes" und wählen Sie "Dynamic Objects".



 Hinweis: Wenn keine dynamischen Office 365-Objekte aufgelistet werden, kann die Integration fehlerhaft sein. Lesen Sie den Abschnitt zur Fehlerbehebung, oder wenden Sie sich an das Cisco TAC.

Fehlerbehebung

Bei Installationsproblemen des Connectors für sichere dynamische Attribute mit Ansible müssen Sie "csdac.log" im Verzeichnis "~/.ansible/collections/ansible_collection/cisco/csdac/logs/" erfassen.

```
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
```

In dieser Datei befinden sich Installationsprotokolle. Öffnen Sie es mit "cat"- oder "less"-Linux-Befehlen, durchsuchen Sie die Fehlerprotokolle, oder wenden Sie sich an das Cisco TAC, und stellen Sie diese Datei bereit.

Manchmal schlägt die Ansible-Installation aufgrund von "verweigerten Berechtigungen" fehl. Durchsuchen Sie die Datei "csdac.log", und suchen Sie nach Protokollen mit verweigerter Berechtigung.

```
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"
```

Wenn ähnliche Protokolle gefunden werden, verwenden Sie die Cisco Bug-ID [CSCwh58312](#), oder wenden Sie sich an das Cisco TAC.

Wenn 'docker ps -a' anzeigt, dass Container heruntergefahren sind oder bei Problemen Container neu gestartet werden, können Container mit dem 'docker restart container-id'-Befehl neu gestartet werden.

Beispiel: Office 365 mit Container-ID '88826cf0742f' wird neu gestartet.

```

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

```

Überprüfen der Verbindung mit CSDAC und Überprüfen, ob die Objekte im Secure Firewall Management Center erstellt wurden

```

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

root@firepower:/Volume/home/admin# cat /var/opt/CSCOpX/MDC/log/operation/usmshredsvcs.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/bulldynamicobjects Created (201) - The request has been fulfilled and resulted in a new reso
    "sourceIP": "172.16.1.53",
    "domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time": "1694971497660"}, "deleteList": []
  }
}

```

Zugehörige Informationen

Weitere Dokumente zu Cisco Secure Dynamic Attributes (CSDAC) finden Sie hier:

Informationen zum Cisco Dynamic Attributes Connector

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

Installation und Upgrade des Cisco Secure Dynamic Attributes Connectors

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

[connector/220/cisco-secure-dynamic-attributes-connector-v220/install-the-cisco-secure-dynamic-attributes-connector.html](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 Connector konfigurieren

<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>

Dynamische Objekte in Zugriffskontrollrichtlinien verwenden

<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>

Fehlerbehebung beim Connector für dynamische Attribute

<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>

Die Installation von CSDAC 2.2 schlug in Ubuntu 20.04 mit dem Befehl "Permission denied with Docker daemon socket" fehl.

Cisco Bug-ID [CSCwh58312](#).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.