Déploiement de CSDAC pour les objets O365 dynamiques sur FMC sur site

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Diagramme du réseau
  - Déploiement de CSDAC sur Ubuntu 20.04
  - Créer un connecteur Office 365
  - Créer un connecteur vCenter
- Vérifier
- Dépannage
- Informations connexes

Introduction

Ce document décrit comment déployer et intégrer CSDAC pour les objets Microsoft 365 dynamiques sur FMC On-prem avec Ansible sur Ubuntu 20.04.

Conditions préalables

Exigences

Cisco vous recommande de connaître les sujets suivants :

- Commandes Linux de base.
- Connaissances de base Python, Docker et Ansible.
- Connaissances de base d'Office 365.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Firewall Management Center Virtual (FMCv) VWware 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.
- Ansible 2.12.10.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le CSDAC (Cisco Secure Dynamic Attributes) permet de collecter des données telles que des réseaux et des adresses IP auprès de fournisseurs cloud et de les envoyer au Cisco Secure Firewall Management Center afin qu'elles puissent être utilisées dans les règles de contrôle d'accès.

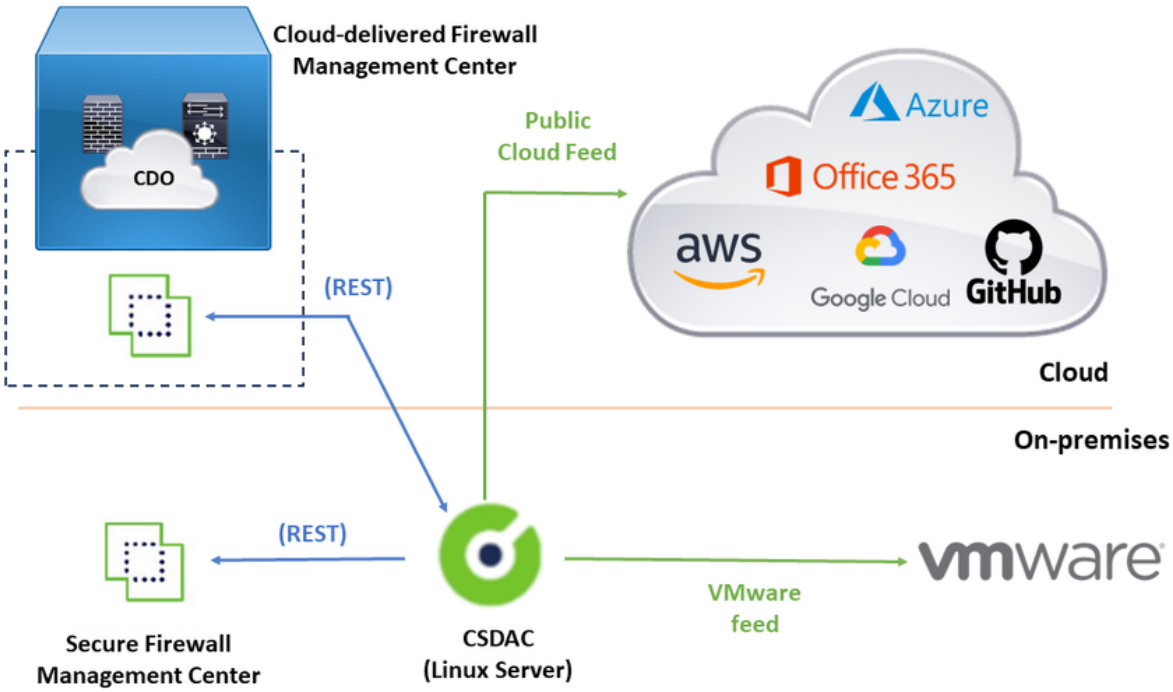
Le connecteur d'attributs dynamiques sécurisés Cisco permet d'utiliser des balises et des catégories de service à partir de diverses plates-formes de services cloud telles qu'AWS, Github, Google Cloud, Azure, Azure Service Tags, Microsoft Office 365 et vCenter.

Les constructions réseau telles que les adresses IP ne sont pas fiables dans les environnements virtuels, cloud et conteneurs en raison de la nature dynamique des charges de travail et du chevauchement inévitable des adresses IP. Parfois, des règles de stratégie doivent être définies sur des constructions non réseau telles que le nom de la machine virtuelle (VM) ou le groupe de sécurité. Par conséquent, les politiques de pare-feu sont persistantes même lorsque l'adresse IP ou le VLAN change. Ces balises et attributs peuvent être collectés à l'aide de conteneurs Docker de connecteur d'attributs dynamiques exécutés sur des machines virtuelles Ubuntu, CentOs ou Red Hat Enterprise Linux. Si vous souhaitez installer CSDAC sur CentOS ou Red Hat, reportez-vous au guide de documentation officiel.

Le connecteur d'attributs dynamiques sur l'hôte Ubuntu est installé à l'aide d'Ansible Collection. Cisco Secure Dynamic Attributes prend en charge 2 types d'adaptateurs.

- Centre de gestion du pare-feu sécurisé sur site.
- Centre de gestion des pare-feu fourni dans le cloud.

Cet article porte sur le déploiement de Cisco Secure Dynamic Attributes Connect sur un hôte Ubuntu pour le service cloud Microsoft Office 365 avec Secure Firewall Management Center sur site.

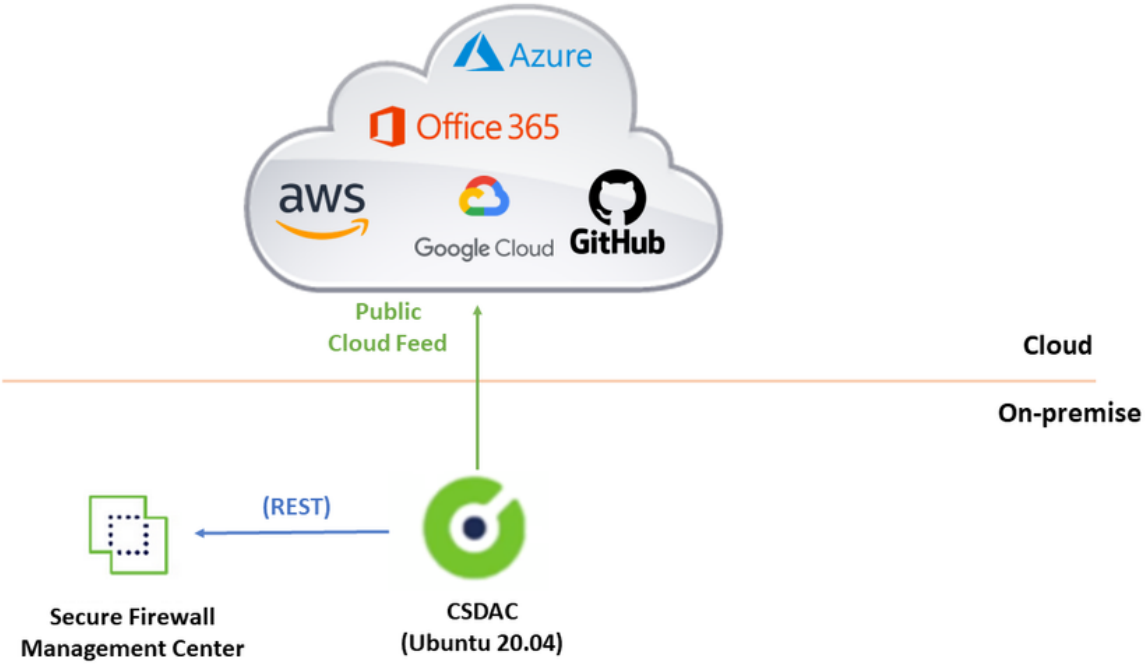


Configurer

Cette section est divisée en sections suivantes :

- Déploiement de CSDAC sur Ubuntu 20.04.
- Créez un connecteur Office 365.
- Créer un connecteur vCenter.

Diagramme du réseau



Déploiement de CSDAC sur Ubuntu 20.04

Cette section explique comment installer les logiciels requis sur Ubuntu.

Étape 1: Valider Docker n'est pas installé.

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

Command 'docker' not found.
```

⚠ Avertissement : Si Docker est installé, consultez sa documentation pour le désinstaller.

Étape 2: Mettez à jour les référentiels Ubuntu.

```
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
....
```

Étape 3: Confirmez la version de Python.

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

Avertissement : Si la version de Python est antérieure à 3.6, vous devez installer la version 3.6 ou ultérieure.

Étape 4: Installez les bibliothèques communes.

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

Étape 5: Installez 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
...
```

Étape 6: Vérifiez la version Ansible.

```
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
```

Remarque : Il est normal pour Ansible de référencer Python 2.x. Le connecteur utilise toujours Python 3.6.

Étape 7: Obtenez le logiciel Dynamic Attributes Connector avec 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
```

Étape 8: Accédez au répertoire csdac.

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

Étape 9: Installez le service de rassemblement.

```
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] => {}

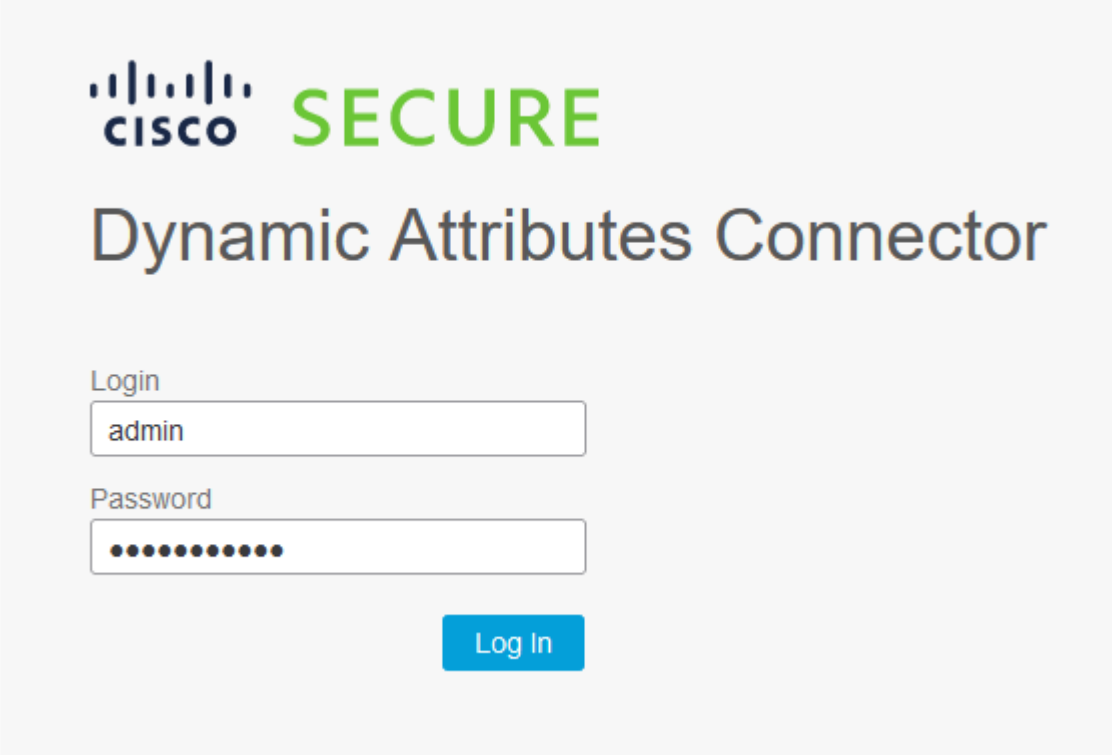
MSG:

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
```

Avertissement : En cas d'échec de l'installation en raison de « Permissions deny with Docker daemon socket », prenez en compte l'ID de bogue Cisco CSCwh58312 ou contactez le centre d'assistance technique Cisco.

Étape 10: Connectez-vous au connecteur en utilisant l'adresse IP CSDAC à l'aide du protocole HTTPS.

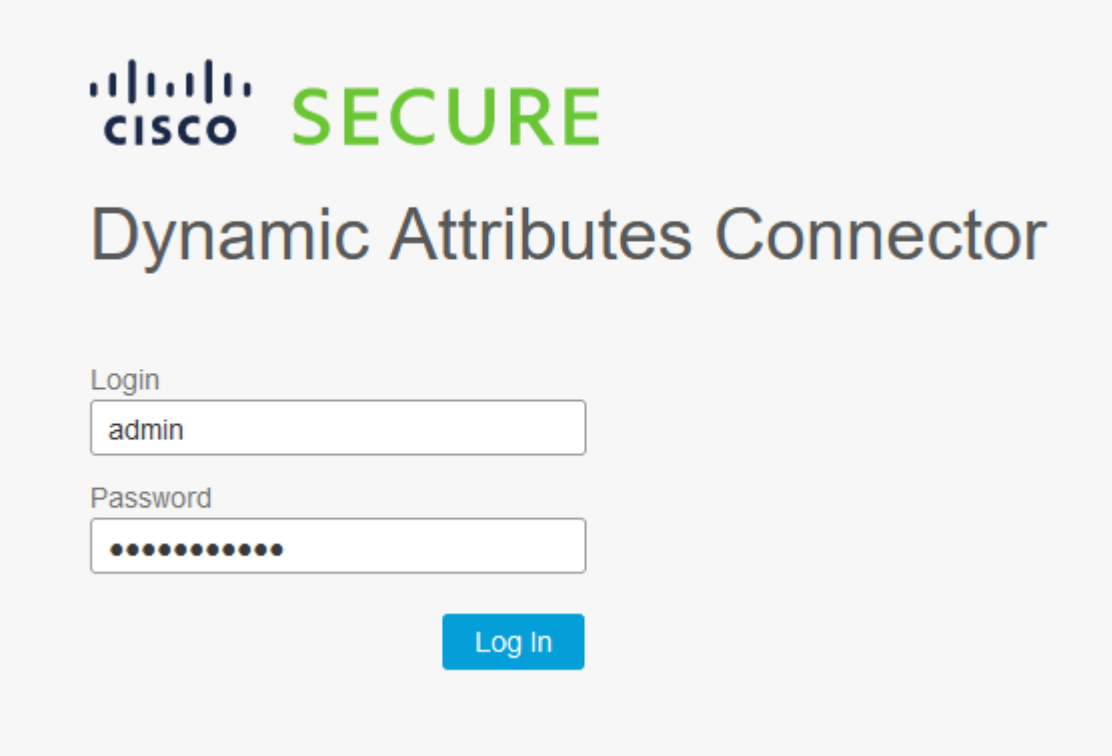


Remarque : La connexion initiale est le nom d'utilisateur « admin » et le mot de passe «

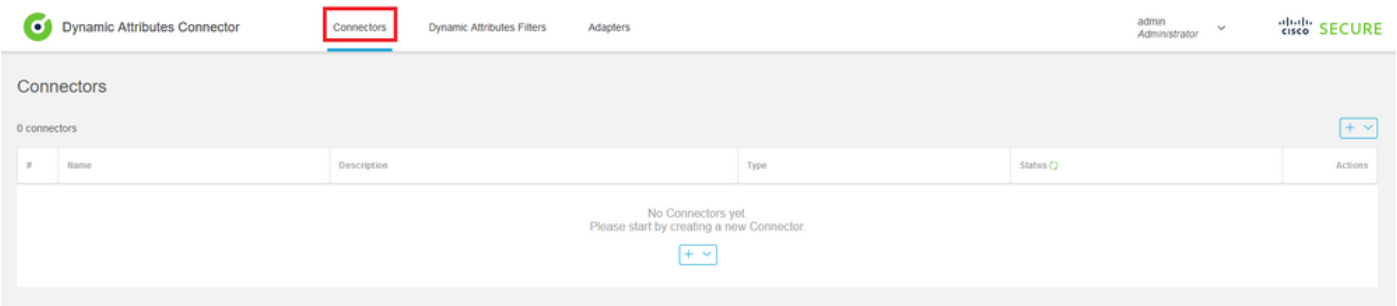
admin ». Le système demande une modification de mot de passe après la première connexion réussie.

Créer un connecteur Office 365

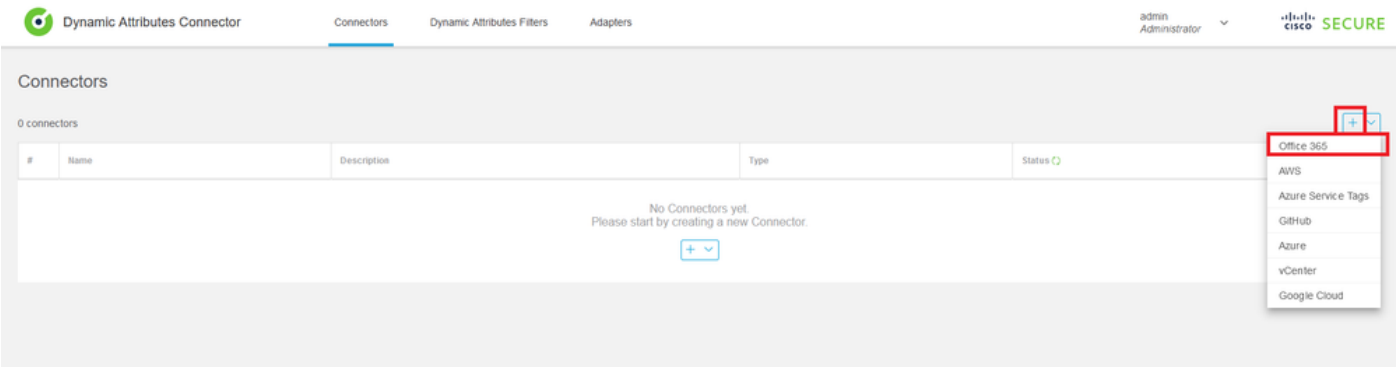
Étape 1: Connectez-vous au connecteur d'attributs dynamiques.



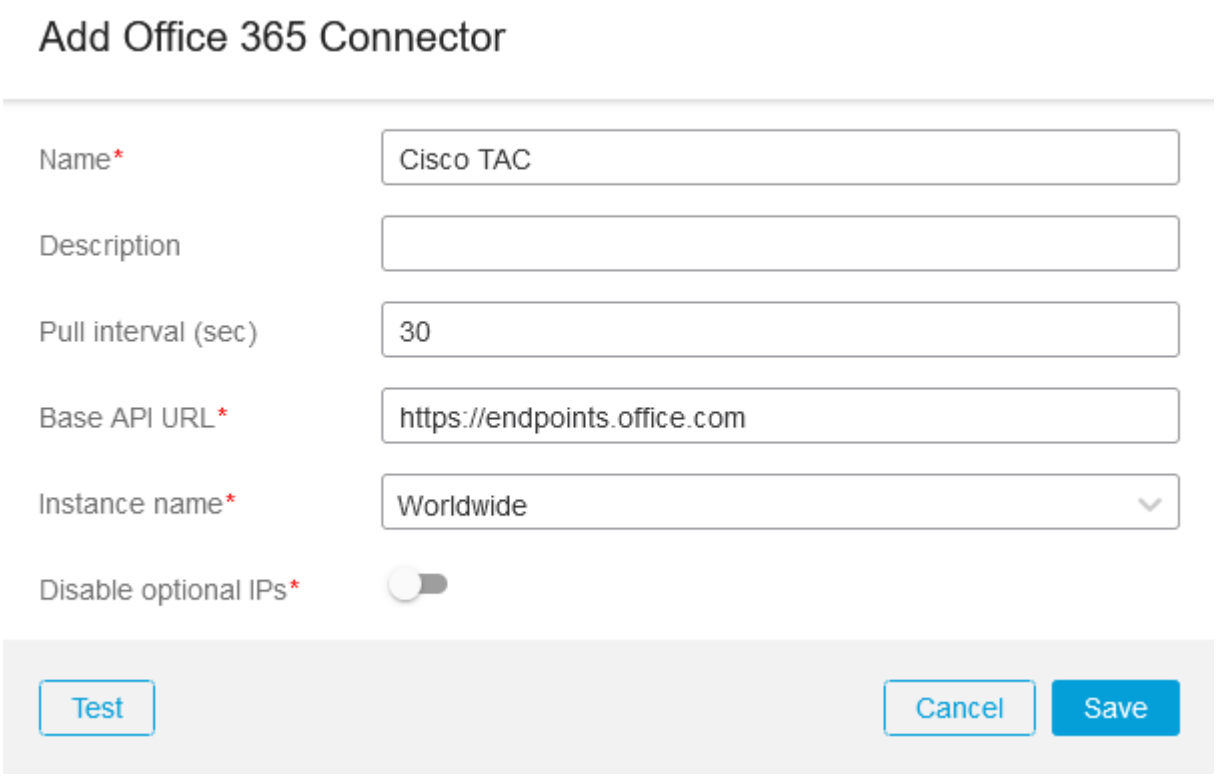
Étape 2: Cliquez sur Connecteurs.



Étape 3: Ajoutez un connecteur Office 365 : cliquez sur l'icône Ajouter (+), puis sur Office 365.



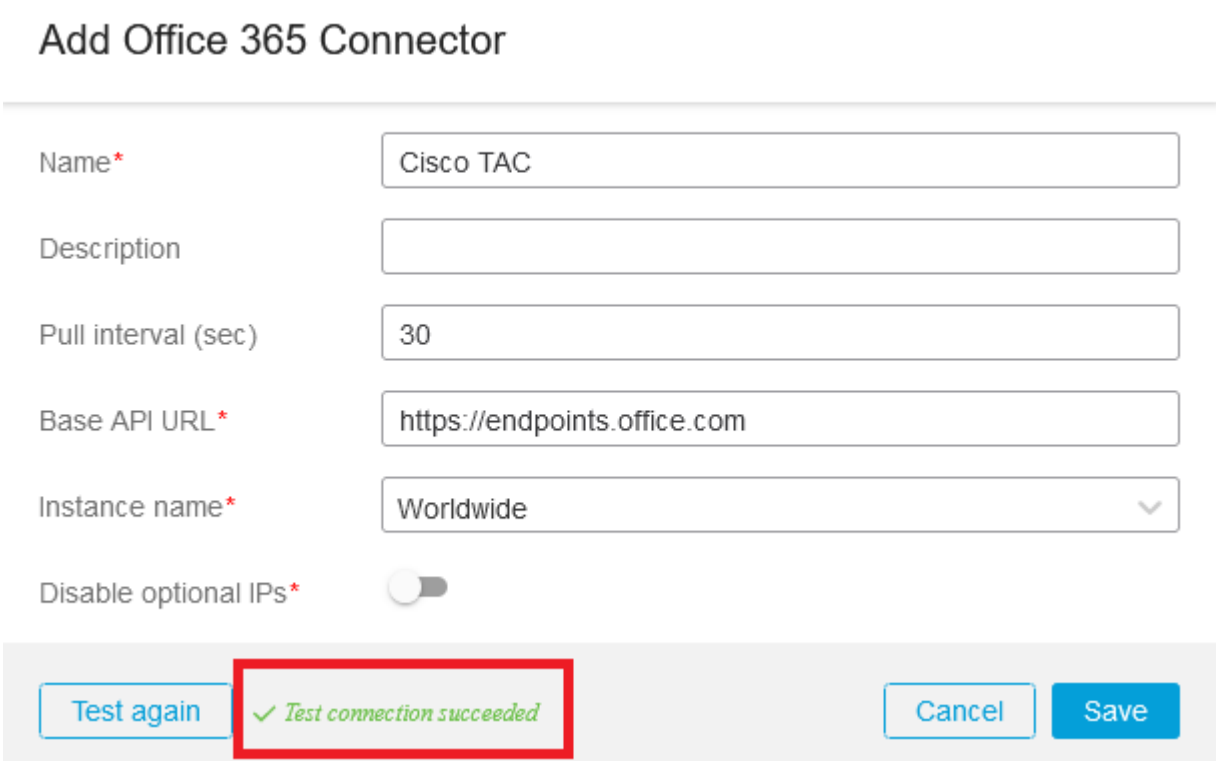
Étape 4: Configurez le connecteur avec les adresses IP facultatives Name, Base API URL, Instance Name et Enable ou Disable.



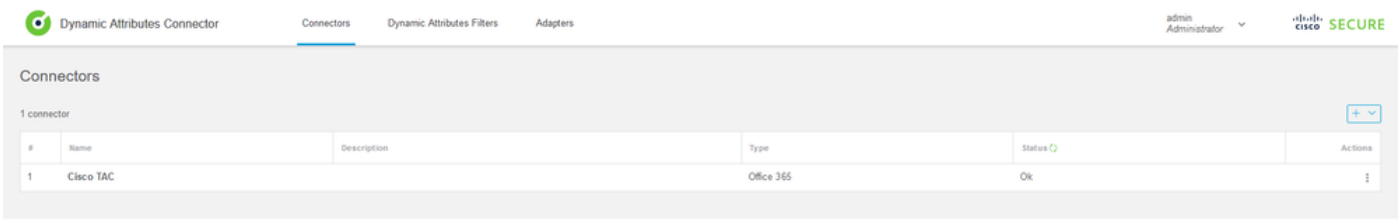
Considérons le suivant :

- L'intervalle d'extraction par défaut est de 30 secondes.
- L'URL de l'API de base est l'URL permettant de récupérer des informations Office 365. Consultez le service Web d'adresse IP et d'URL d'Office 365 sur le guide de documentation Microsoft.

Étape 5: Cliquez sur « Test » et assurez-vous que le test réussit avant d'enregistrer la configuration du connecteur.

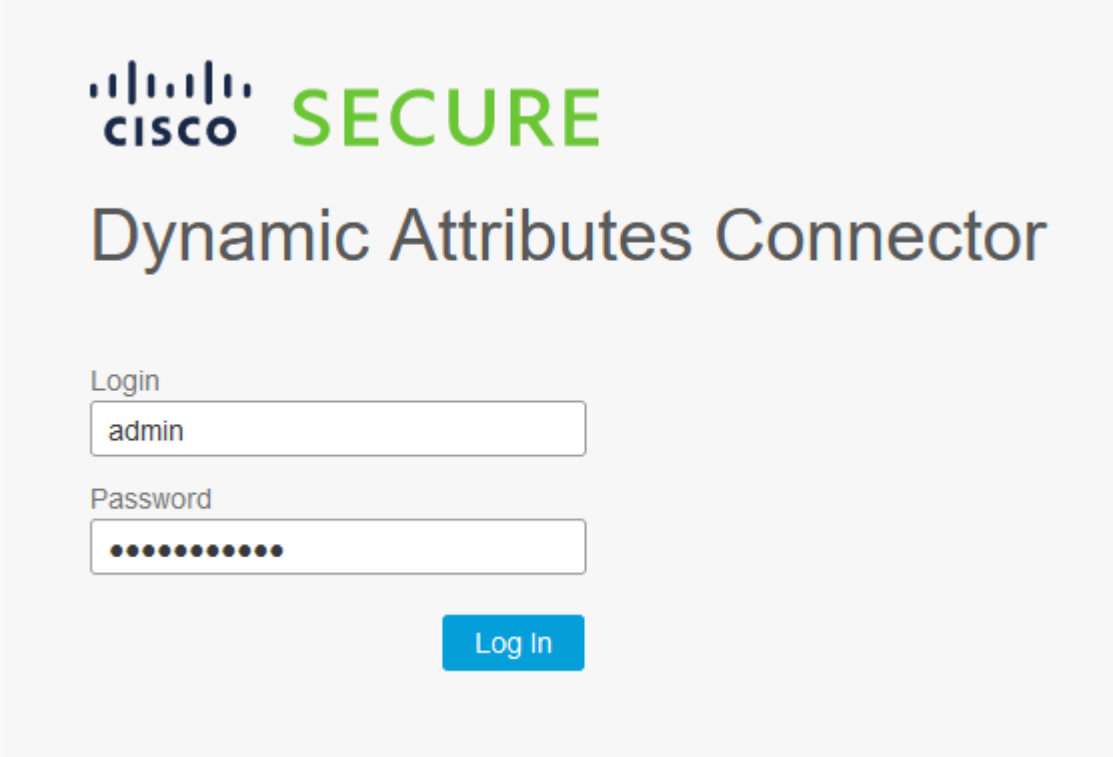


Étape 6: Enregistrez et vérifiez que l'état est « OK ».

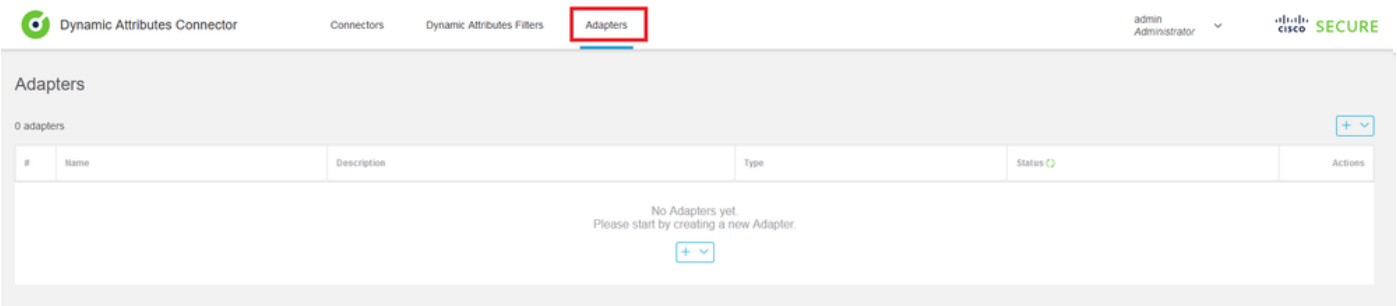


Créer un connecteur vCenter

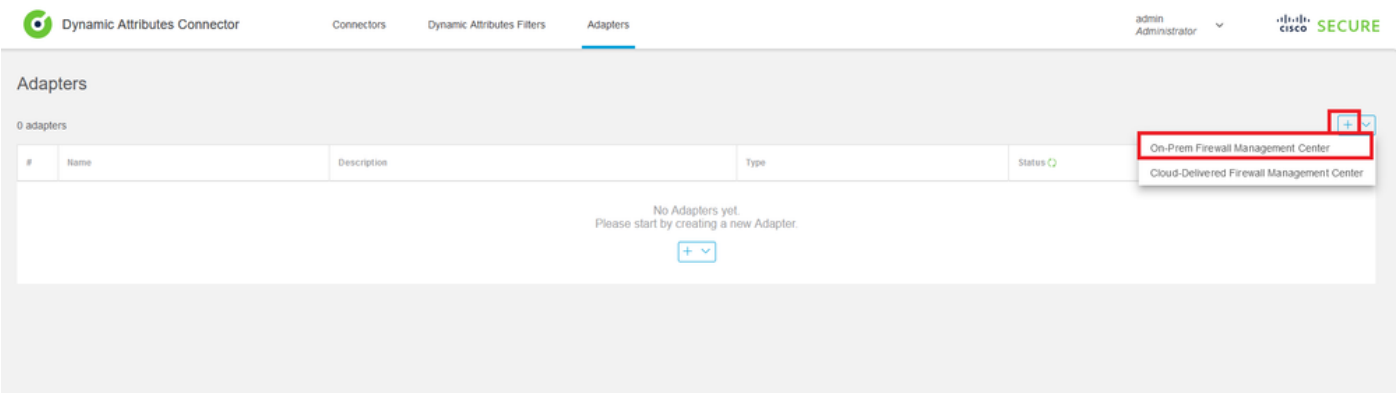
Étape 1: Connectez-vous au connecteur d'attributs dynamiques.



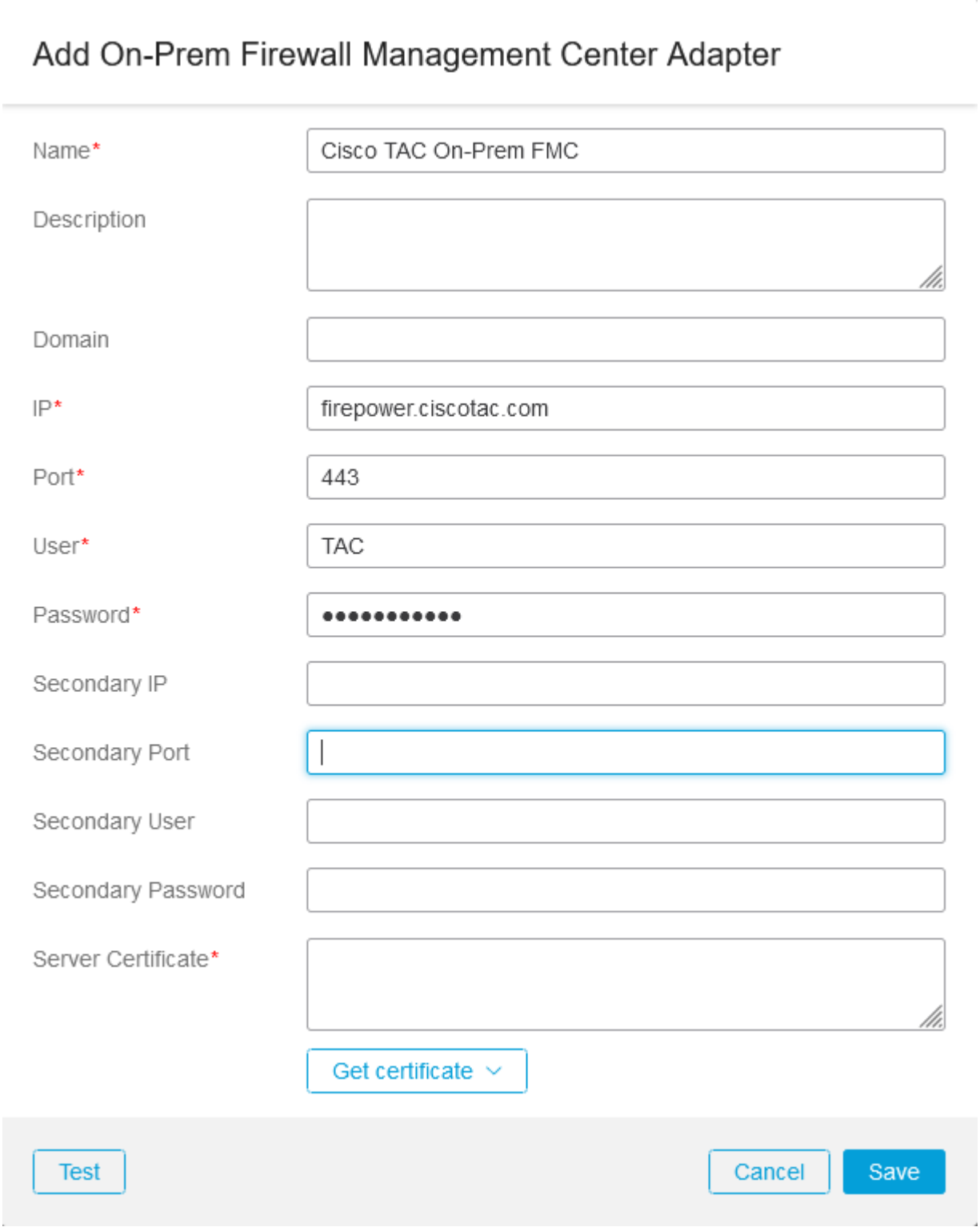
Étape 2: Cliquez sur « Adaptateurs ».



Étape 3: Ajouter un nouvel adaptateur : cliquez sur l'icône Ajouter (+), puis sur « Centre de gestion des pare-feu sur site ».



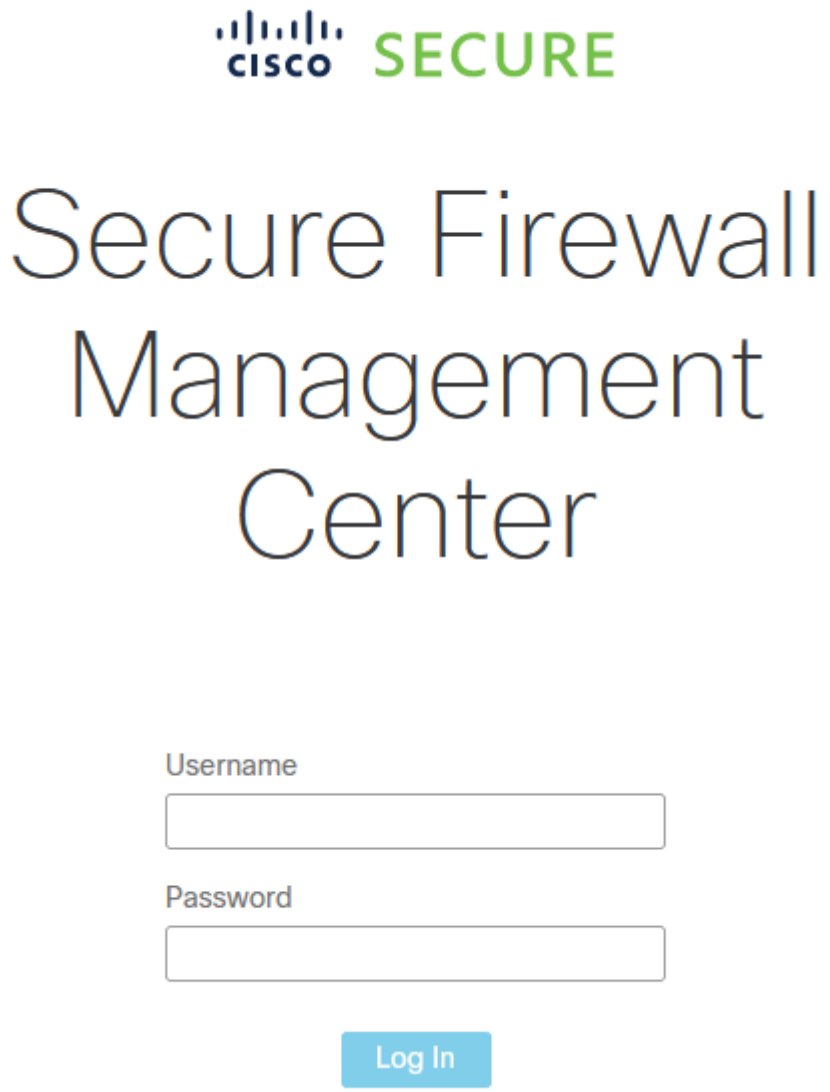
Étape 4: Configurez la carte avec le nom, l'adresse IP, le port et l'utilisateur/le mot de passe.



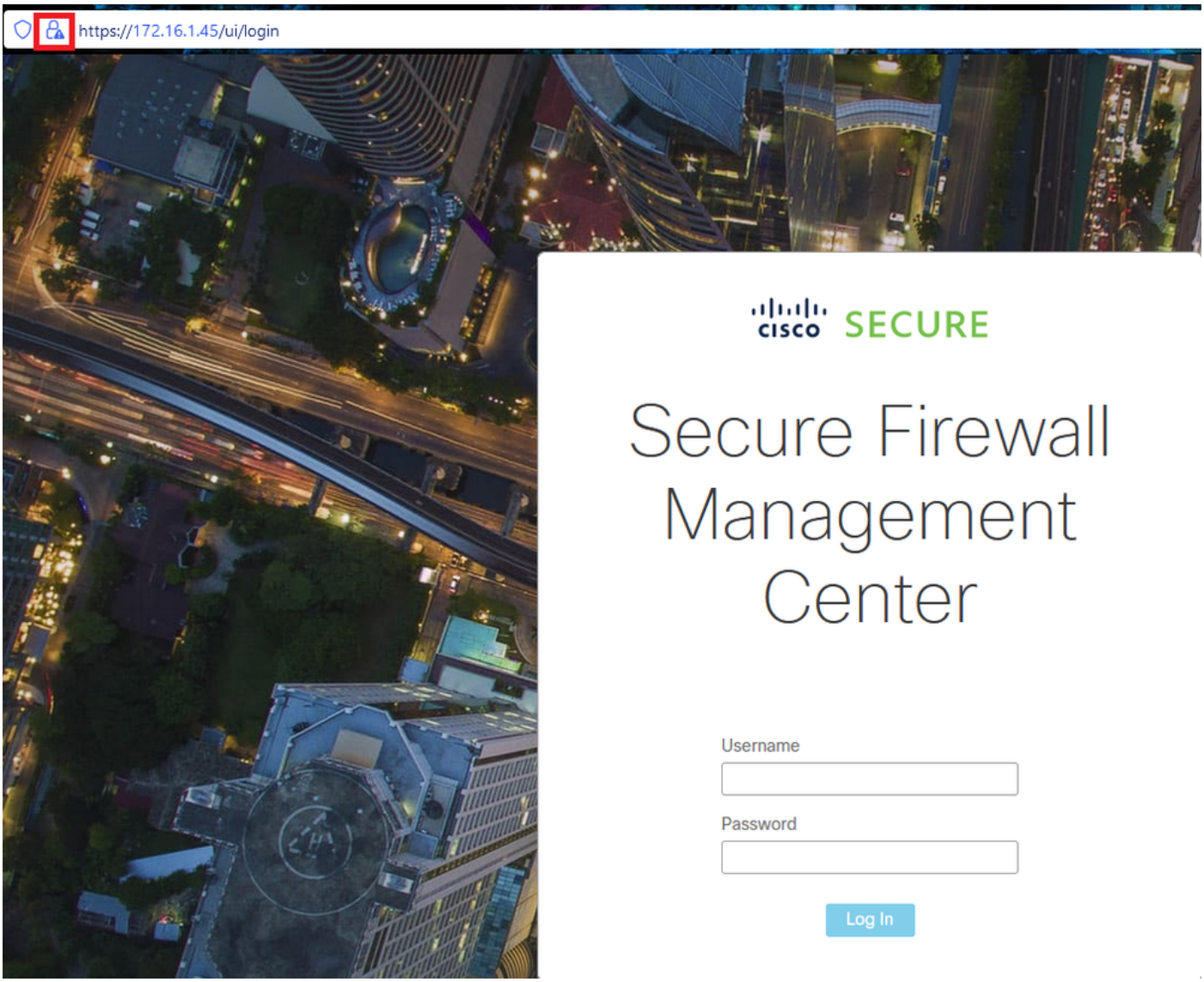
Avertissement : Créez un utilisateur FMC sur l'interface utilisateur dédiée à la connexion de la carte. L'utilisation d'un utilisateur existant peut créer des déconnexions inattendues sur CSDAC ou l'interface utilisateur du Centre de gestion du pare-feu sur site.

Remarque : La configuration du rôle d'utilisateur doit avoir des rôles « Administrateur », « Administrateur d'accès » ou « Administrateur réseau ». Utilisez le nom de domaine complet (FQDN) On-Prem Firewall Management Center dans le champ d'adresse IP.

Étape 5: Ouvrez L'Interface Utilisateur Du Centre De Gestion Sécurisée Du Pare-Feu Sur Site.



Étape 6: Téléchargez le certificat PEM HTTPS (chaîne) à partir du navigateur : Cliquez sur le cadenas HTTPS affiché sur le navigateur, Connexion sécurisée, Plus d'informations, Afficher le certificat, PEM (chaîne).

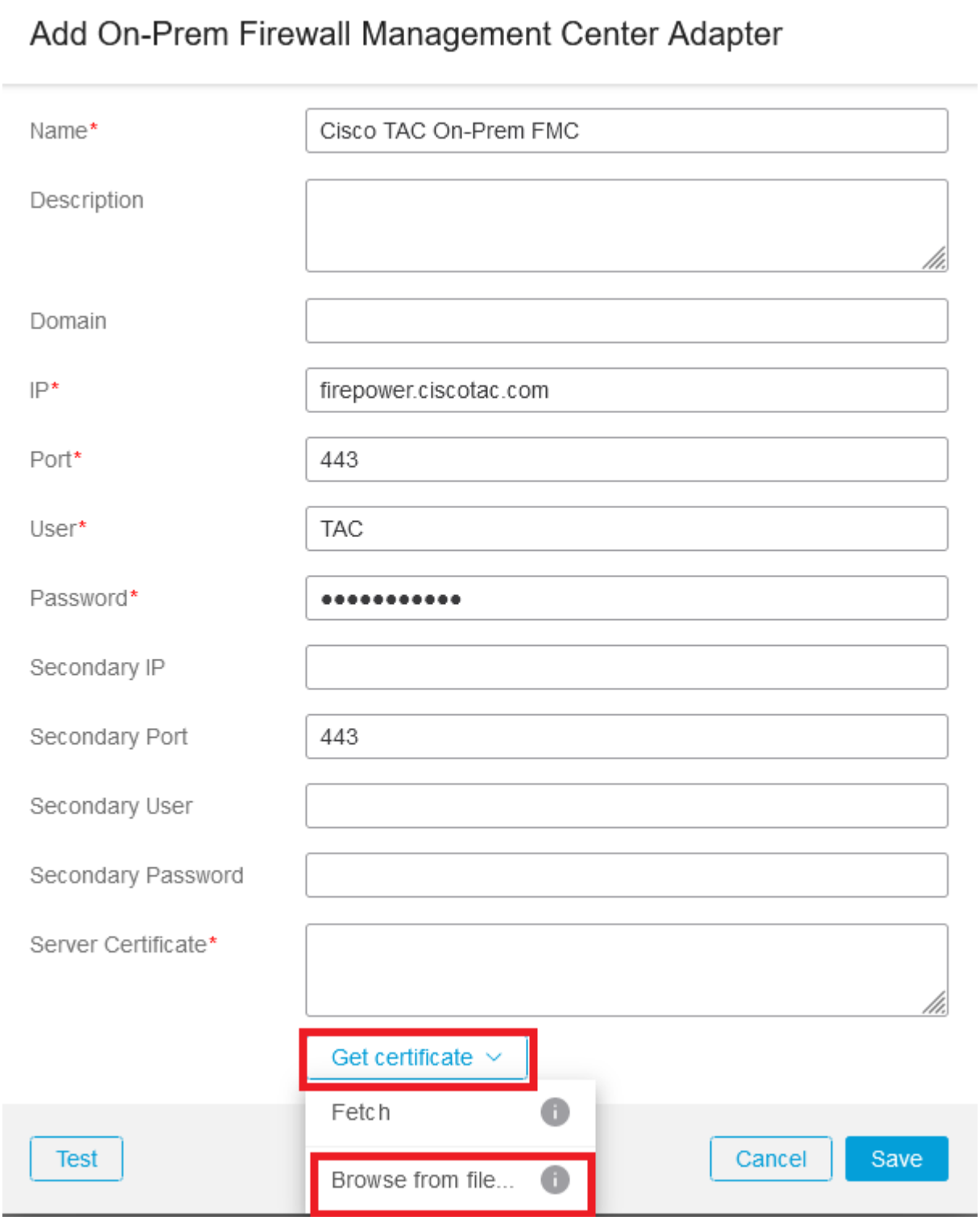




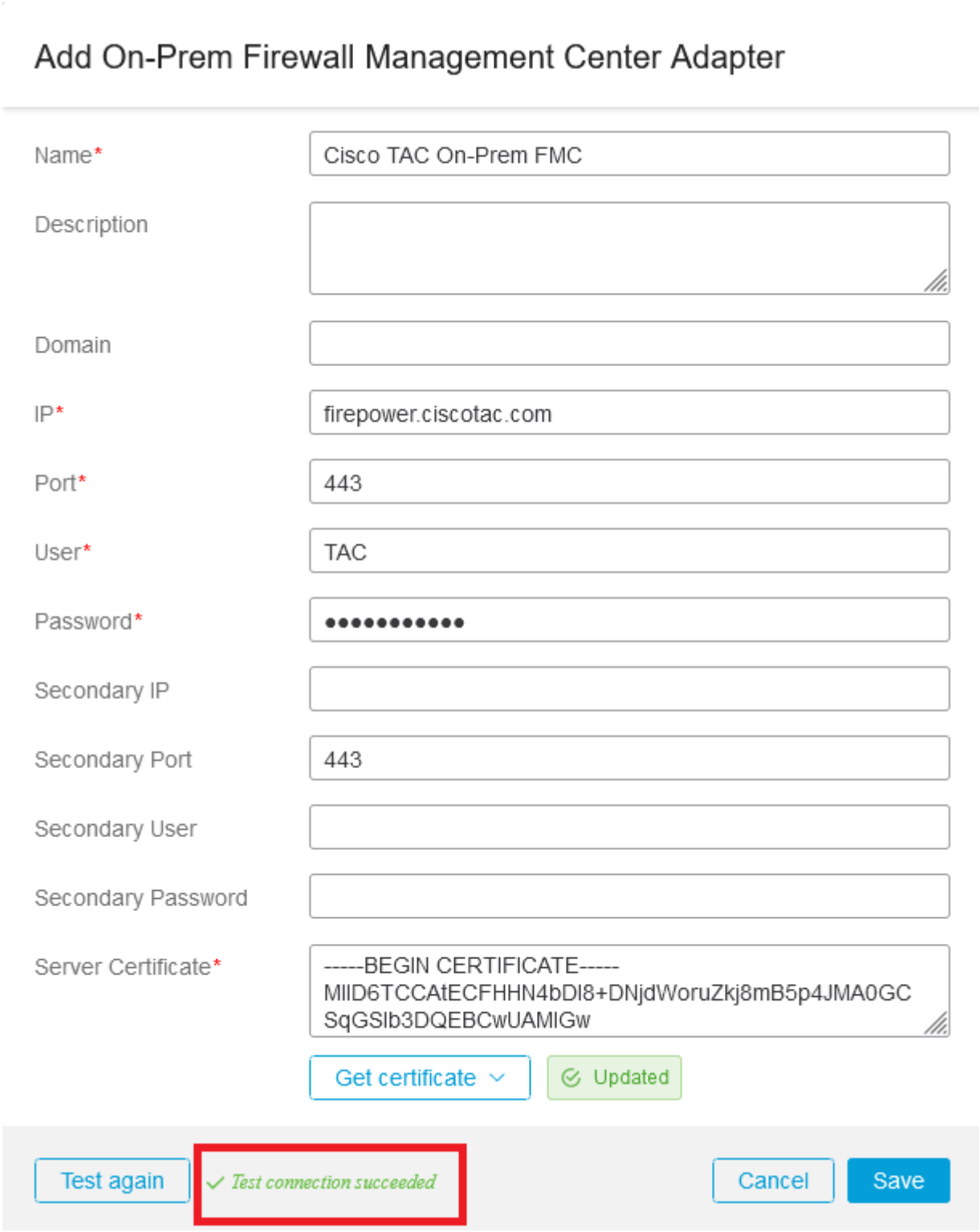
Cette opération télécharge un fichier .pem avec la chaîne de certificats.

Remarque : Les étapes de collecte du certificat HTTPS On-Prem Secure Firewall Management Center appartiennent au navigateur Firefox. Recherchez les étapes similaires si un autre navigateur est utilisé.

Étape 7 : Ouvrez Dynamic Attributes Connector et cliquez sur « Get certificate » et « Browse from file... ».

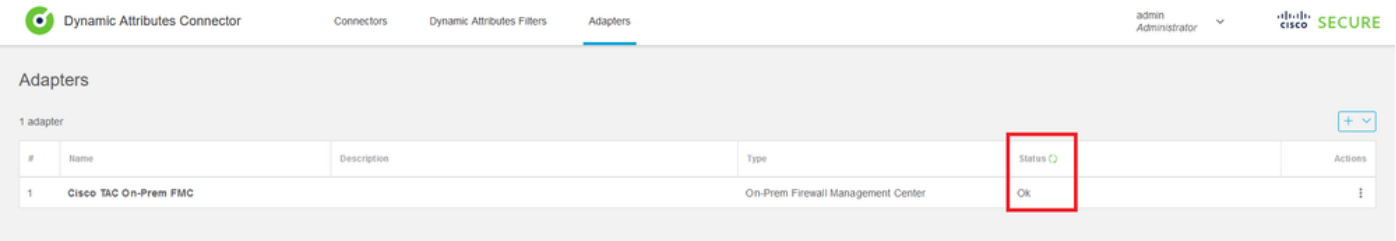


Étape 8: Téléchargez le certificat .pem et cliquez sur « TEST » pour vous assurer que le test réussit.



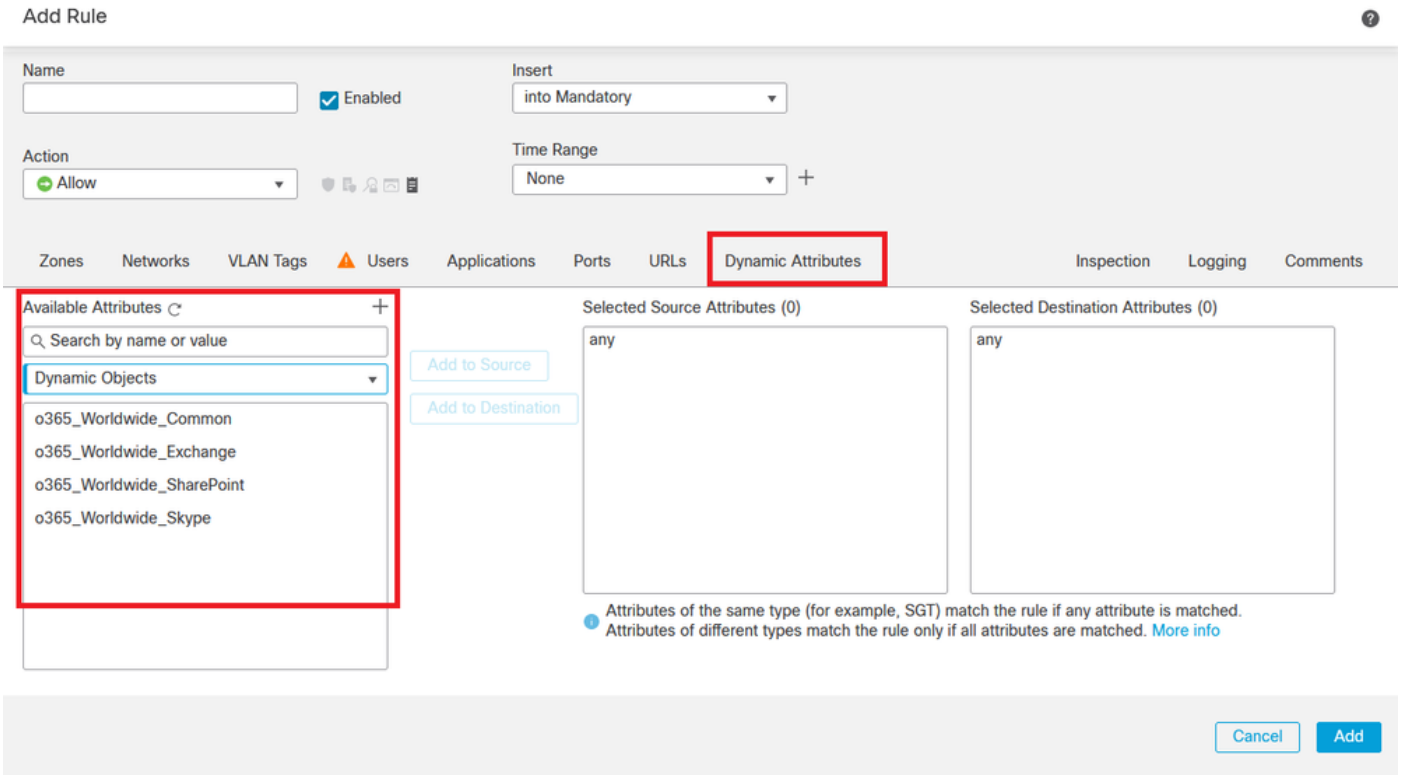
Avertissement : Assurez-vous que les serveurs DNS configurés sur l'ordinateur Ubuntu peuvent résoudre le nom de domaine complet (FQDN) On-Prem Firewall Management Center, sinon le test peut échouer.

Étape 9: Enregistrez et vérifiez que l'état est « OK ».



Remarque : Impossible de créer des filtres d'attributs dynamiques pour Office 365.

Étape 10: Commencez à créer des règles de stratégie de contrôle d'accès avec des attributs Office 365 dynamiques sur l'interface utilisateur du Centre de gestion du pare-feu sur site.

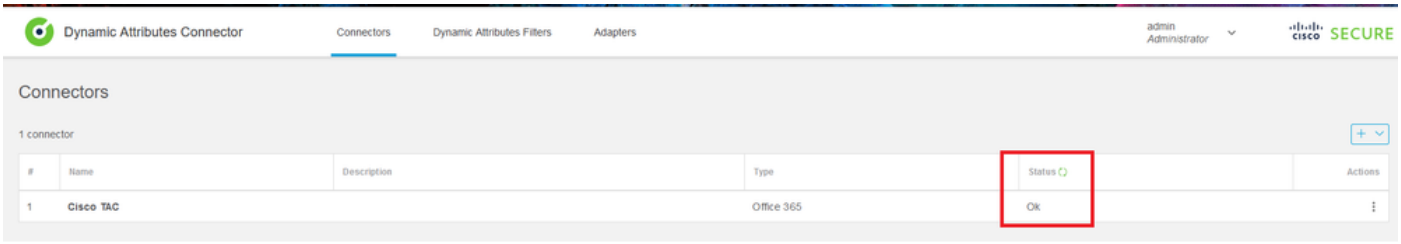


Vérifier

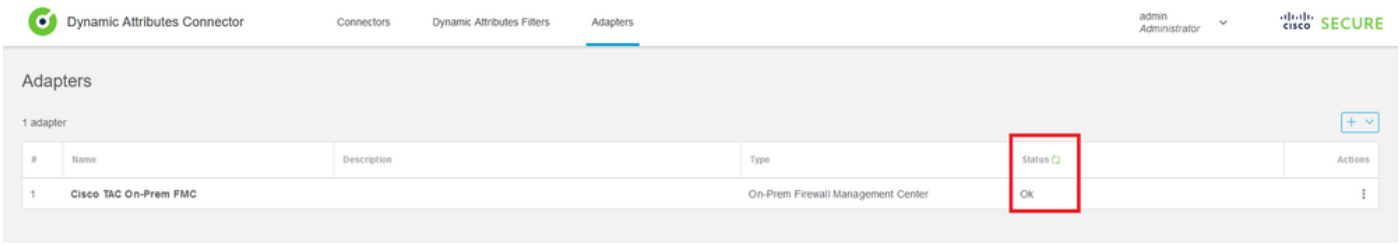
Vérifiez l'état du conteneur sur Ubuntu pour les services, les connecteurs et les adaptateurs principaux.

```
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            "/docker-entrypoint.…"  2 days a
722a764c54e9 public.ecr.aws/e6e4t5f5/muster_ui_backend:2.2.0-latest    "./docker-entrypoint…"  2 days a
038654545f30 public.ecr.aws/e6e4t5f5/muster_bee:2.2.0-latest           "/bin/sh -c /app/bee"   2 days a
90cfd7e3a28b public.ecr.aws/e6e4t5f5/muster_etcd:2.2.0-latest          "etcd"                  2 days a
```

Vérifiez l'état du connecteur depuis l'interface utilisateur CSDAC.

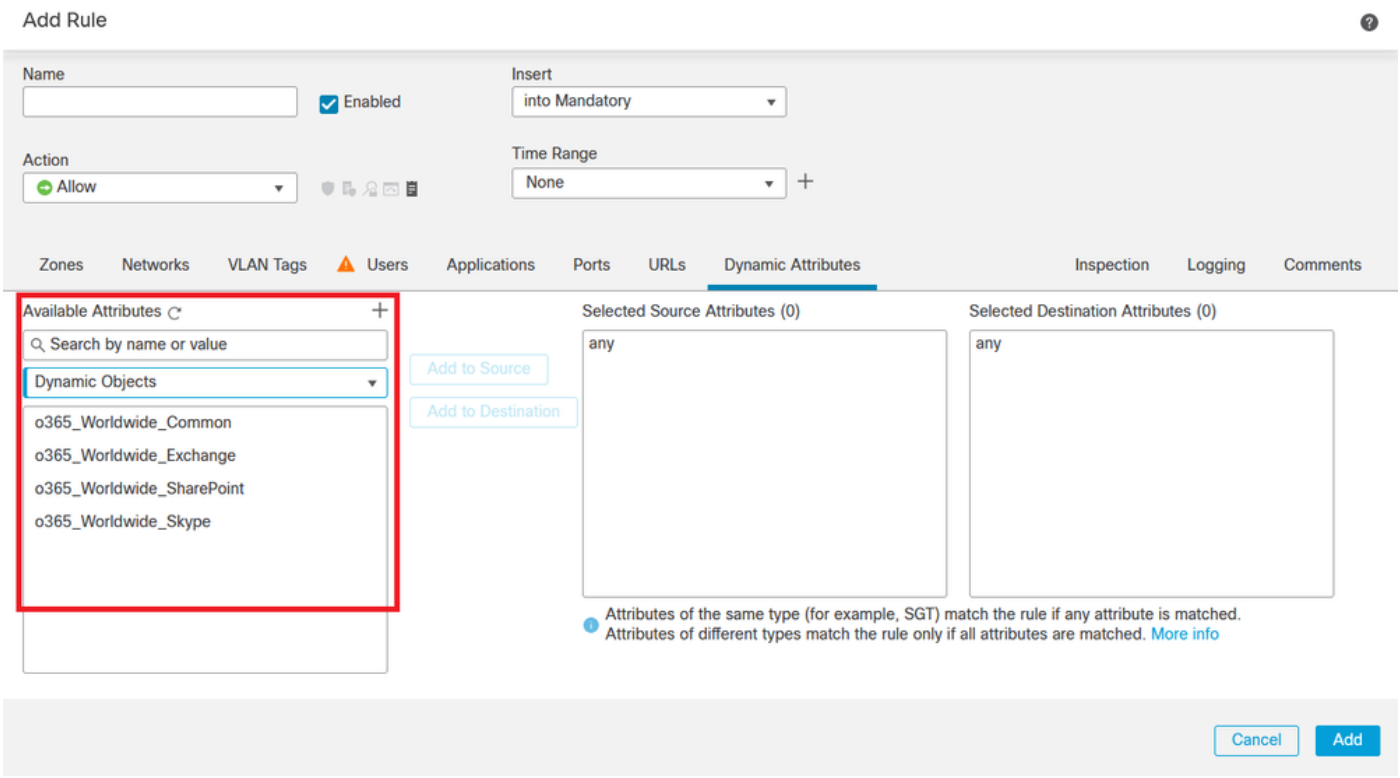


Vérifiez l'état de l'adaptateur depuis CSDAC UI.



Vérifiez les attributs dynamiques d'Office 365 dans Firewall Management Center.

Créez ou modifiez une règle de stratégie de contrôle d'accès, cliquez sur Attributs dynamiques, cliquez sur Attributs disponibles, puis sélectionnez Objets dynamiques.



Remarque : Si les objets dynamiques Office 365 ne sont pas répertoriés, il se peut que l'intégration présente un problème. Consultez la section de dépannage ou contactez le TAC Cisco.

Dépannage

En cas de problèmes d'installation du connecteur d'attributs dynamiques sécurisés avec Ansible, collectez « csdac.log » situé dans le répertoire « ~/.ansible/collections/ansible_collection/cisco/csdac/logs/ ».

```
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
```

Les journaux des échecs d'installation se trouvent dans ce fichier. Ouvrez-le à l'aide des commandes Linux « cat » ou « less », explorez les journaux des défaillances ou contactez le TAC Cisco et fournissez ce fichier.

Parfois, l'installation d'Ansible échoue en raison des « autorisations refusées ». Explorez le fichier csdac.log et recherchez les journaux « autorisation refusée ».

```
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
```

Si des journaux similaires sont trouvés, examinez l'ID de bogue Cisco CSCwh58312 ou contactez le TAC Cisco pour obtenir de l'aide.

Si « docker ps -a » indique que les conteneurs sont hors service ou pour redémarrer les conteneurs en cas de problème, les conteneurs peuvent être redémarrés à l'aide de la commande « docker restart container-id ».

Exemple : Redémarrage d'Office 365 avec l'ID de conteneur « 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

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
```

Vérifiez la connexion avec CSDAC et validez si les objets sont créés sur le Centre de gestion du pare-feu sécurisé.

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

root@firepower:/Volume/home/admin# cat /var/opt/CSCOpx/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 reso
     "sourceIP":"172.16.1.53",
     "domainUuid":"e276abec-e0f2-11e3-8169-6d9ed49b625f",
     "time":"1694971497660"},"deleteList":[]
}
```

Informations connexes

D'autres documents relatifs aux attributs dynamiques sécurisés Cisco (CSDAC) sont disponibles ici :

À propos du connecteur d'attributs dynamiques Cisco

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 et mise à niveau du connecteur Cisco Secure Dynamic Attributes

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

Configuration du connecteur d'attributs dynamiques Cisco

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

Utiliser des objets dynamiques dans les stratégies de contrôle d'accès

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

Dépannage du connecteur d'attributs dynamiques

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

Échec de l'installation de CSDAC 2.2 « Autorisation refusée avec le socket démon Docker » dans Ubuntu 20.04.

ID de bogue Cisco CSCwh58312.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.