在内部FMC上为动态O365对象部署CSDAC

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 网络图
- Ubuntu 20.04上的CSDAC部署
- 创建Office 365连接器
- 创建vCenter连接器

验证

故障排除

相关信息

简介

本文档介绍如何在本地FMC上为Dynamic Microsoft 365对象部署和集成CSDAC与Ubuntu 20.04上的Ansible。

先决条件

要求

思科建议您了解以下主题：

- 基本的Linux命令。
- 基本Python、Docker和Ansible知识。
- Office 365基础知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行7.2.5版本的思科防火墙管理中心虚拟(FMCv)VWware。
- 思科安全动态属性连接器(CSDAC)版本2.2。
- Ubuntu 4vCPU/8GB版本20.04。
- Docker版本24.0.6
- Python 3.8.10。
- Ansible 2.12.10。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

思科安全动态属性(CSDAC)允许从云提供商收集网络和IP地址等数据，并将其发送到思科安全防火墙管理中心，以便在访问控制策略规则中使用。

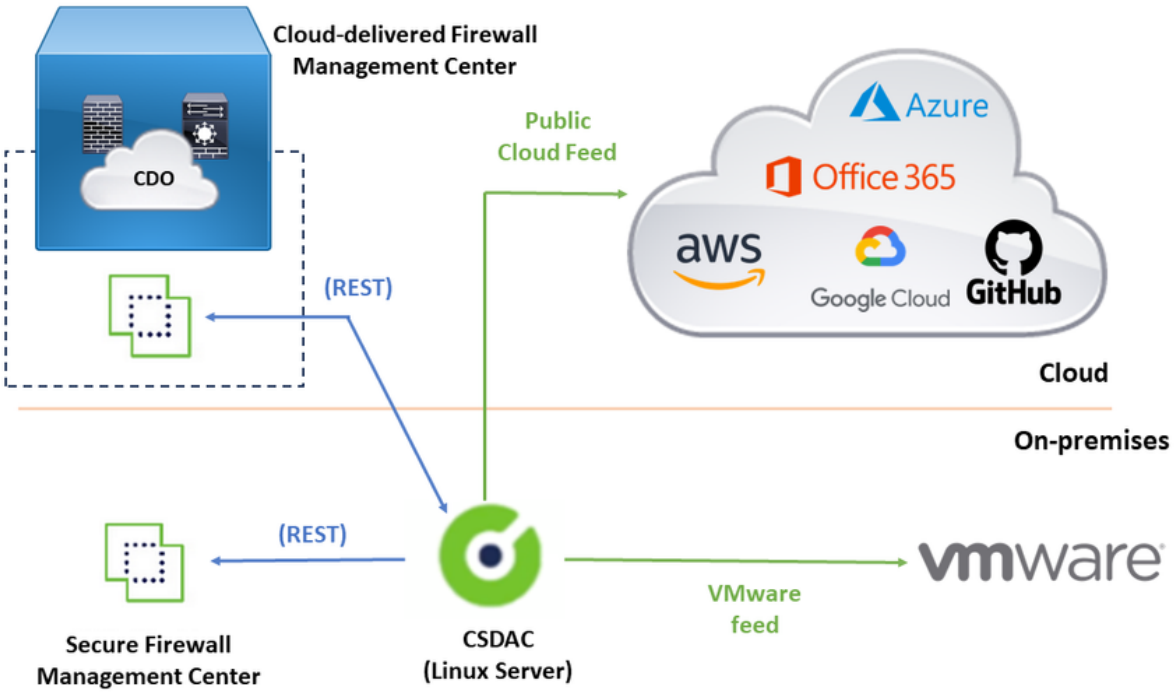
Cisco Secure Dynamic Attributes Connector允许使用各种云服务平台的服务标签和类别，例如AWS、Github、Google Cloud、Azure、Azure Service Tags、Microsoft Office 365和vCenter。

由于工作负载的动态性质和IP地址重叠的必然性，在虚拟、云和容器环境中，IP地址等网络结构不可靠。有时，必须在非网络结构(如虚拟机(VM)名称或安全组)上定义策略规则。因此，即使在IP地址或VLAN发生更改时，防火墙策略也具有持久性。这些标记和属性可以使用在Ubuntu、CentOs或Red Hat Enterprise Linux虚拟机上运行的动态属性连接器Docker容器来收集。如果您希望在CentOS或Red Hat上安装CSDAC，请参阅正式文档指南。

Ubuntu主机上的动态属性连接器使用Ansible Collection安装。Cisco Secure Dynamic Attributes支持2种类型的适配器。

- 内部安全防火墙管理中心。
- 云交付的防火墙管理中心。

本文重点介绍如何通过内部安全防火墙管理中心在Ubuntu主机上为Microsoft Office 365云服务部署思科安全动态属性连接。

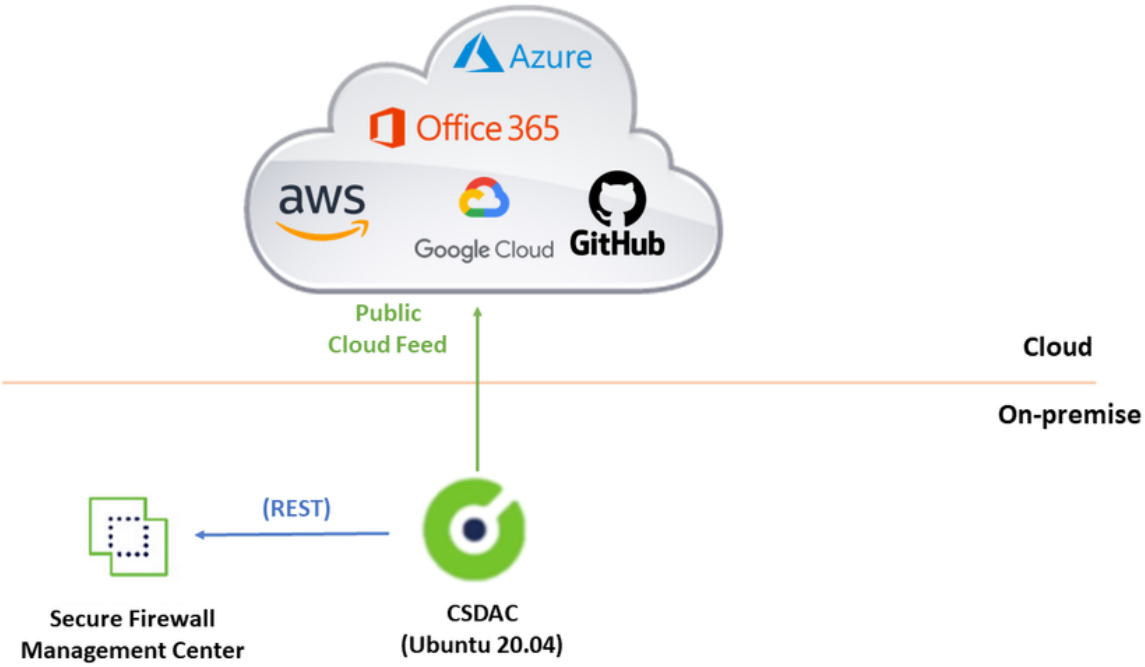


配置

本节分为以下部分：

- Ubuntu 20.04上的CSDAC部署。
- 创建Office 365连接器。
- 创建vCenter连接器。

网络图



Ubuntu 20.04上的CSDAC部署

本节讨论如何在Ubuntu上安装必备软件。

步骤 1：未安装Validate Docker。

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

Command 'docker' not found.
```

⚠ 警告：如果安装了Docker，请查阅Docker文档将其卸载。

步骤 2： 更新Ubuntu存储库。

```
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
....
```

步骤 3：确认Python版本。

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

⚠ 警告：如果Python版本早于3.6，则必须安装版本3.6或更高版本。

步骤 4：安装公用库。

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

步骤 5： 安装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
...
```

步骤 6：检验Ansible版本。

```
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
```

注意：Ansible引用Python 2.x是正常的。连接器仍使用Python 3.6。

步骤 7：使用Ansible获取动态属性连接器软件。

```
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
```

步骤 8:: 转到csdac目录。

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

步骤 9：安装集群服务。

```
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:

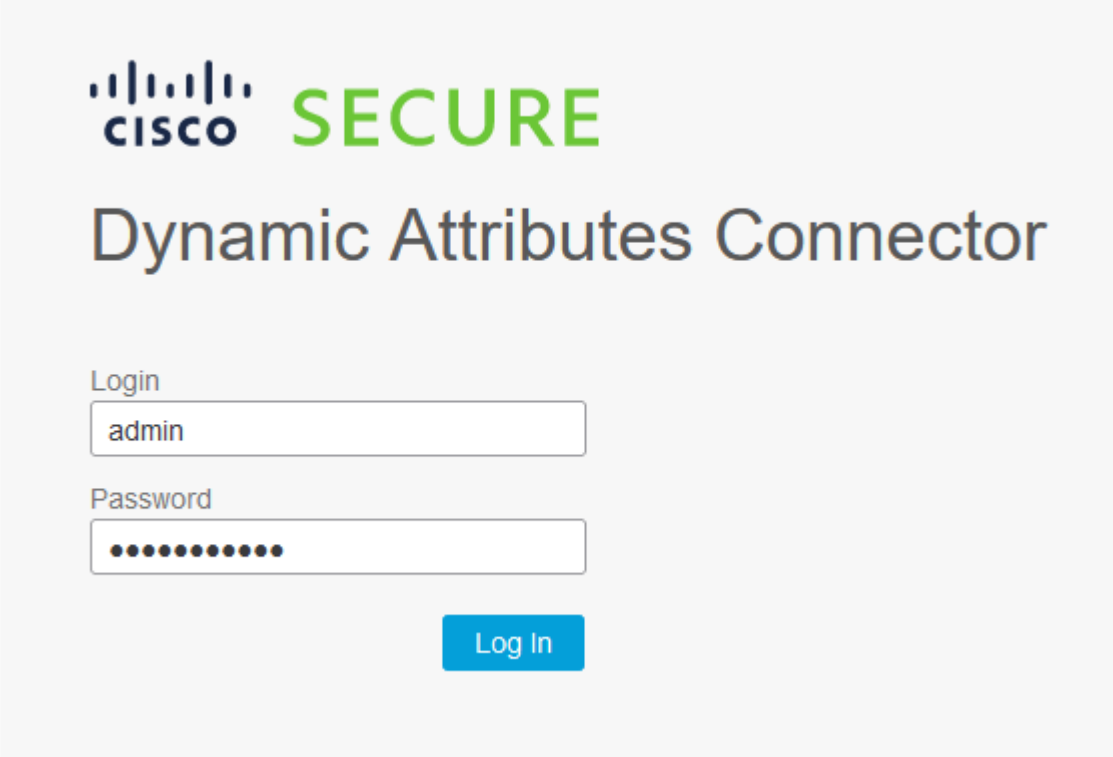
Please login in to https://172.16.1.53 to configure csdac application

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



警告：如果由于“Permissions denied with Docker daemon socket”导致安装失败，请考虑思科漏洞ID CSCwh58312或联系思科TAC。

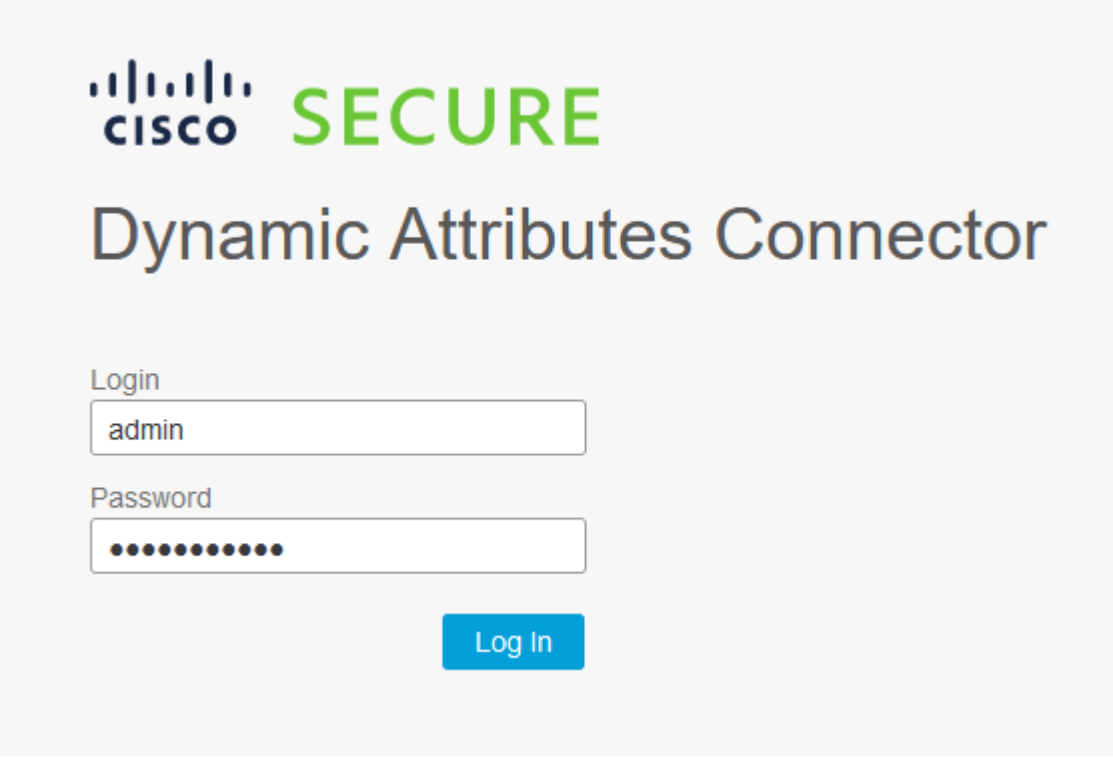
步骤 10： 使用HTTPS协议使用CSDAC IP地址登录到连接器。



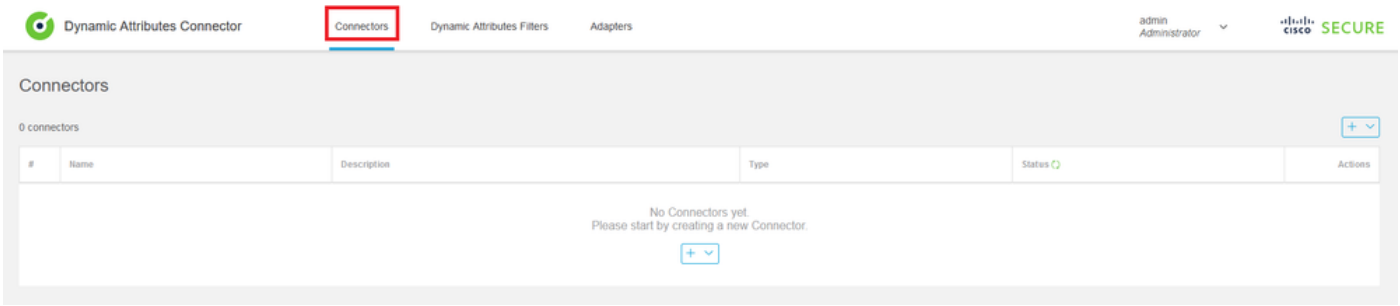
注意：初始登录用户名是“admin”，密码是“admin”。 在首次成功登录后，系统会要求更改密码。

创建Office 365连接器

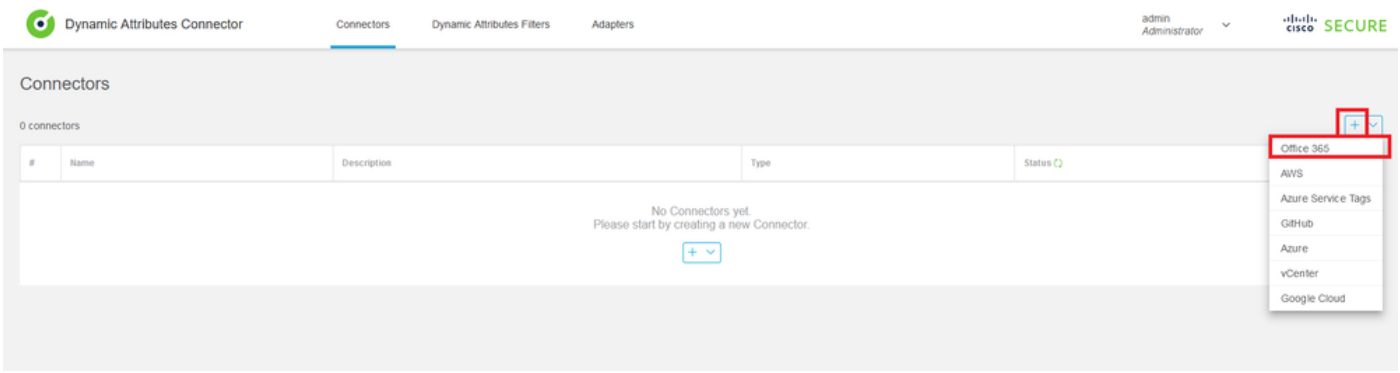
步骤 1：登录到动态属性连接器。



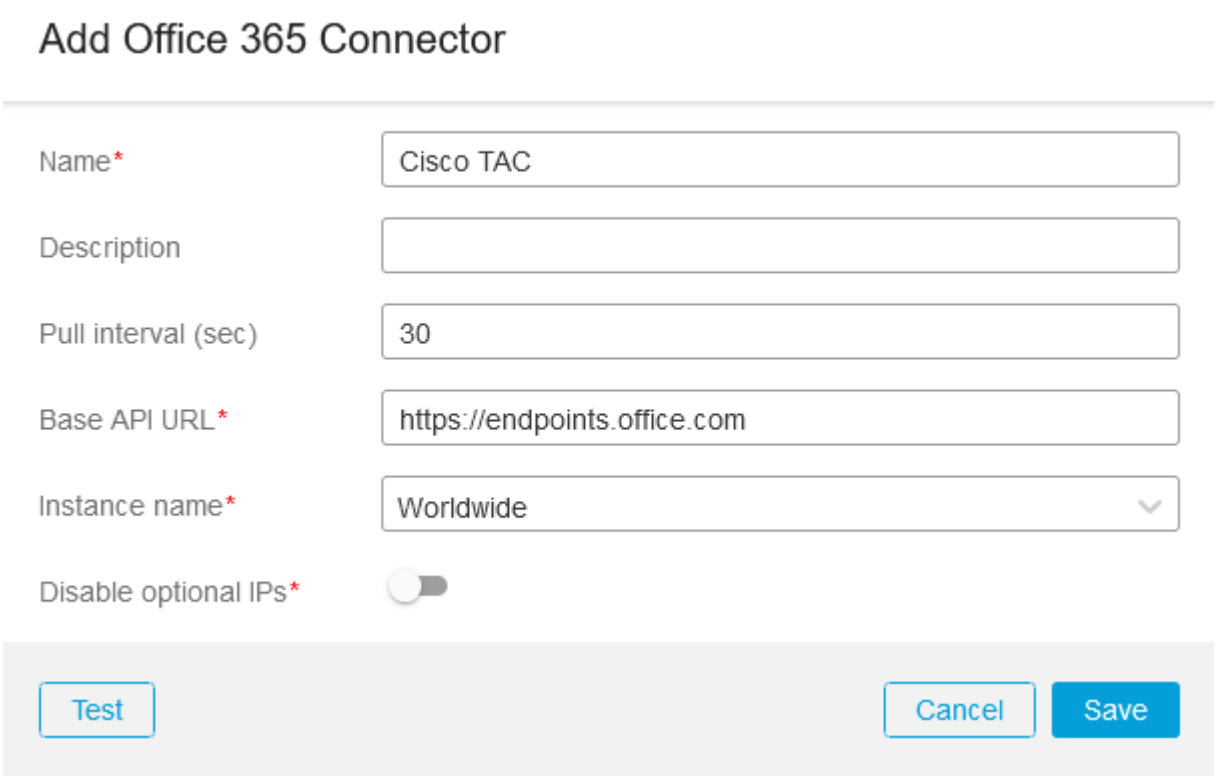
步骤 2：单击“Connectors”。



步骤 3：添加Office 365连接器：点击添加图标(+)，然后点击“Office 365”。



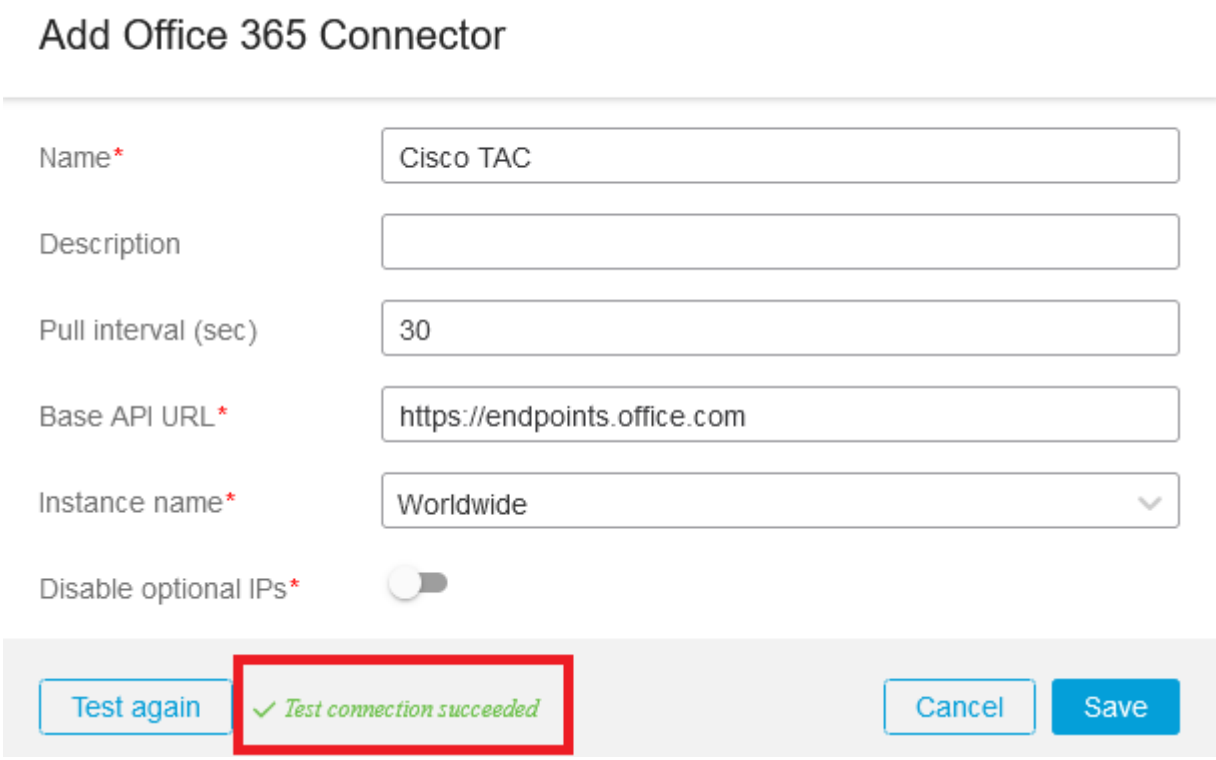
步骤 4：使用Name、Base API URL、Instance Name和Enable or Disable optional IPs配置连接器。



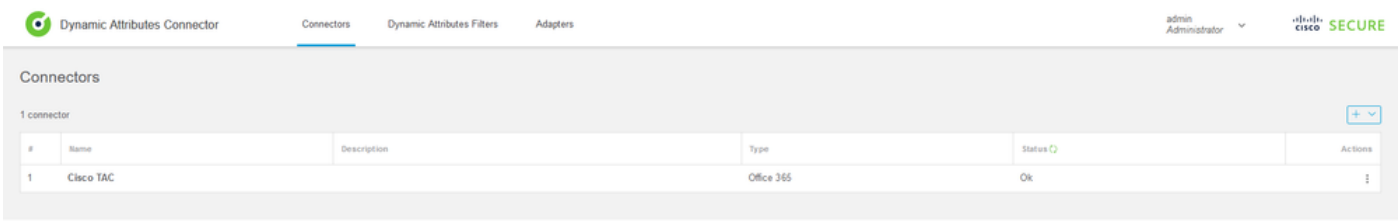
考虑下一点：

- 拉取间隔默认为30秒。
- 基本API URL是用于检索Office 365信息的URL。请参阅Microsoft文档指南上的[Office 365 IP地址和URL Web服务]。

步骤 5： 单击“测试”，确保在保存连接器配置之前测试成功。

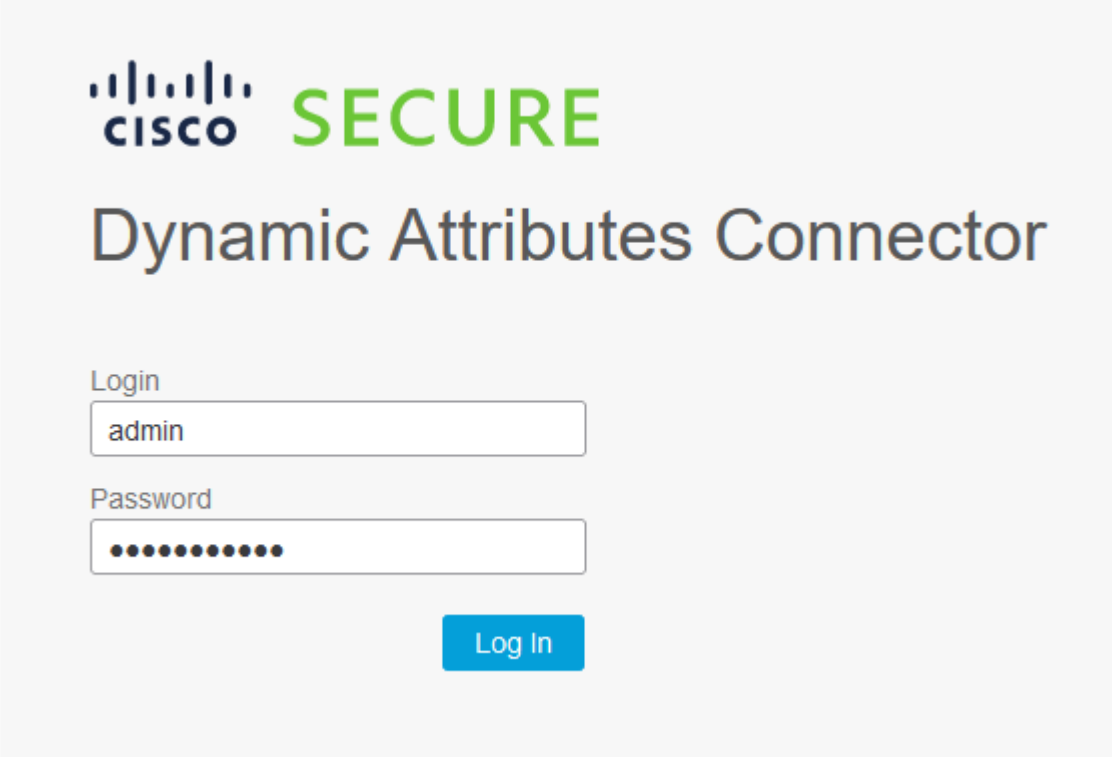


步骤 6：保存并确保状态为“OK”。

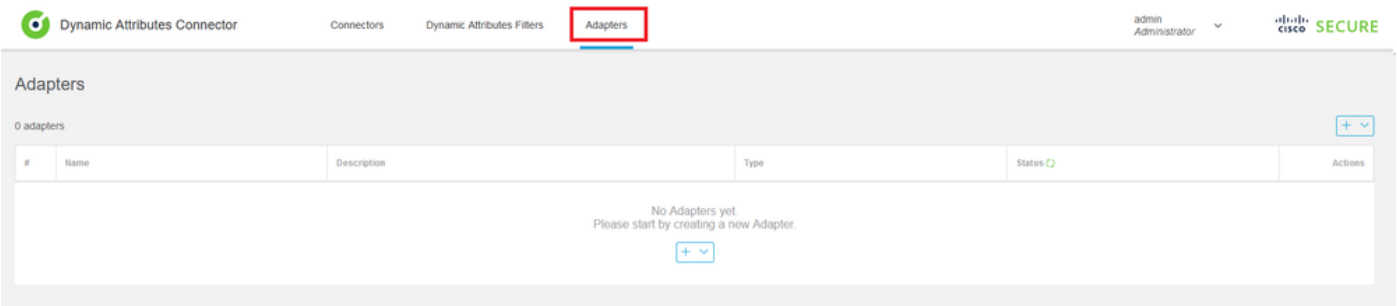


创建vCenter连接器

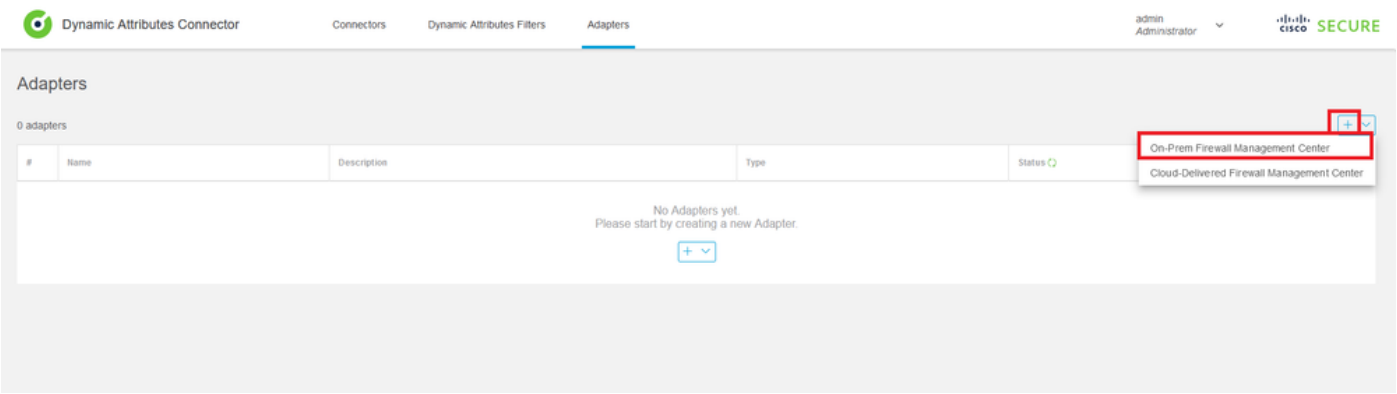
步骤 1：登录到动态属性连接器。



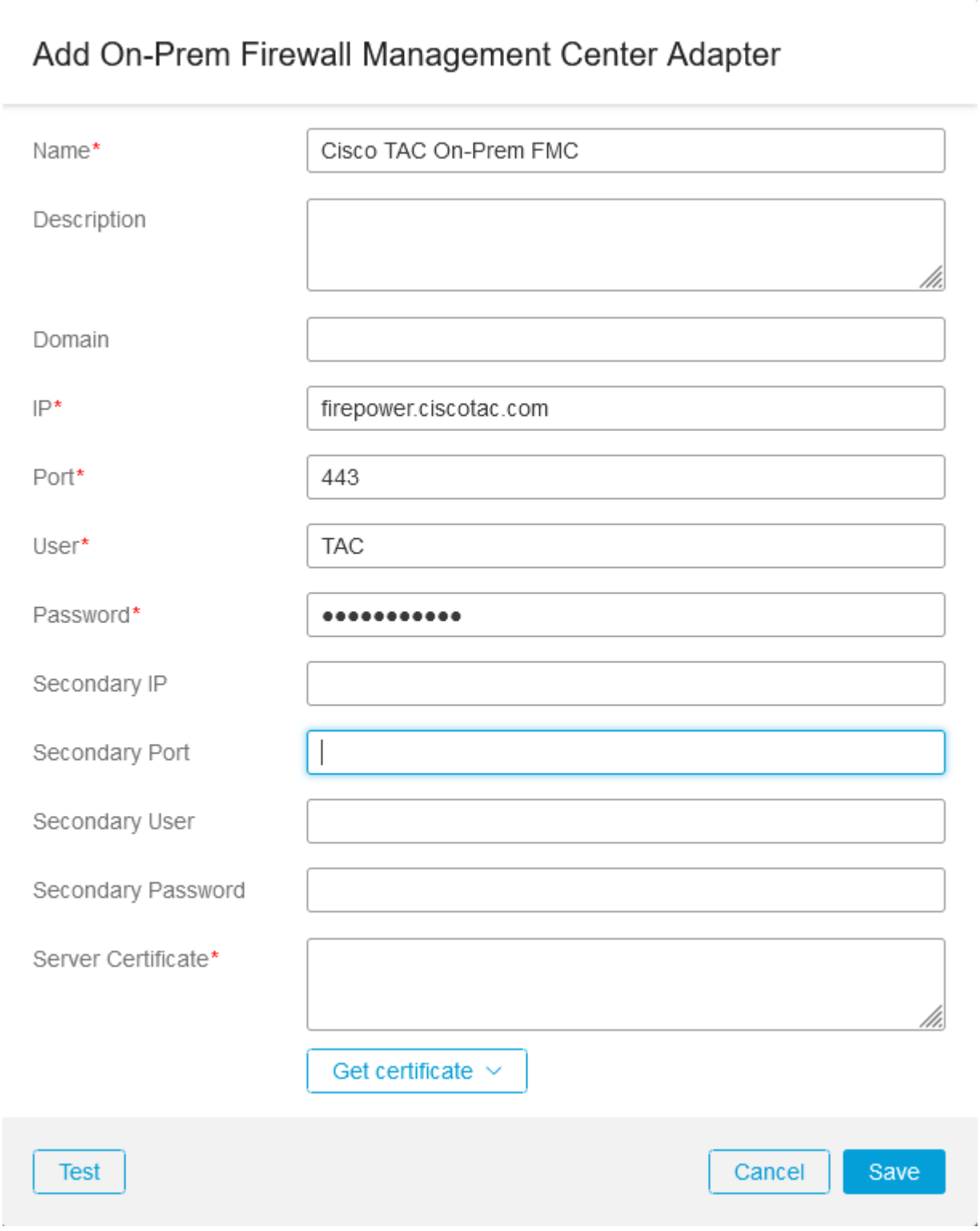
步骤 2：单击“Adapters”。



步骤 3：添加新适配器：点击Add（添加）图标(+)，然后点击on-prem Firewall Management Center（本地防火墙管理中心）。



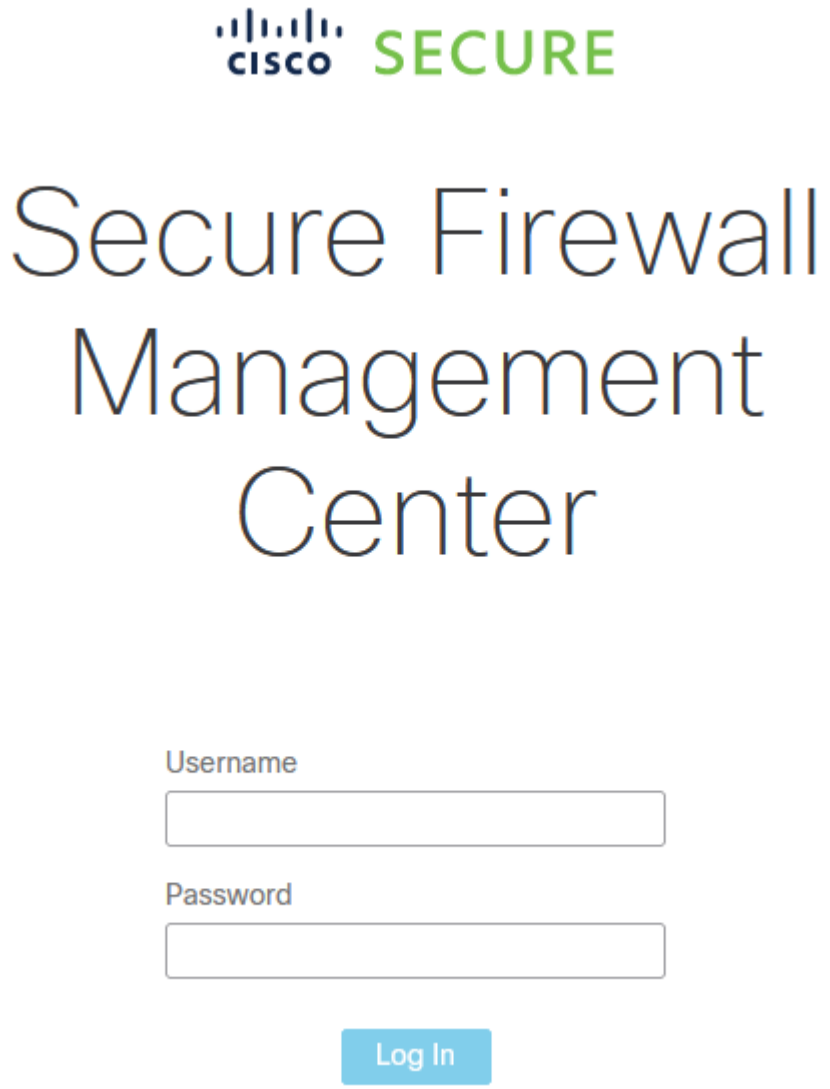
步骤 4： 使用名称、IP地址、端口和用户/密码配置适配器。



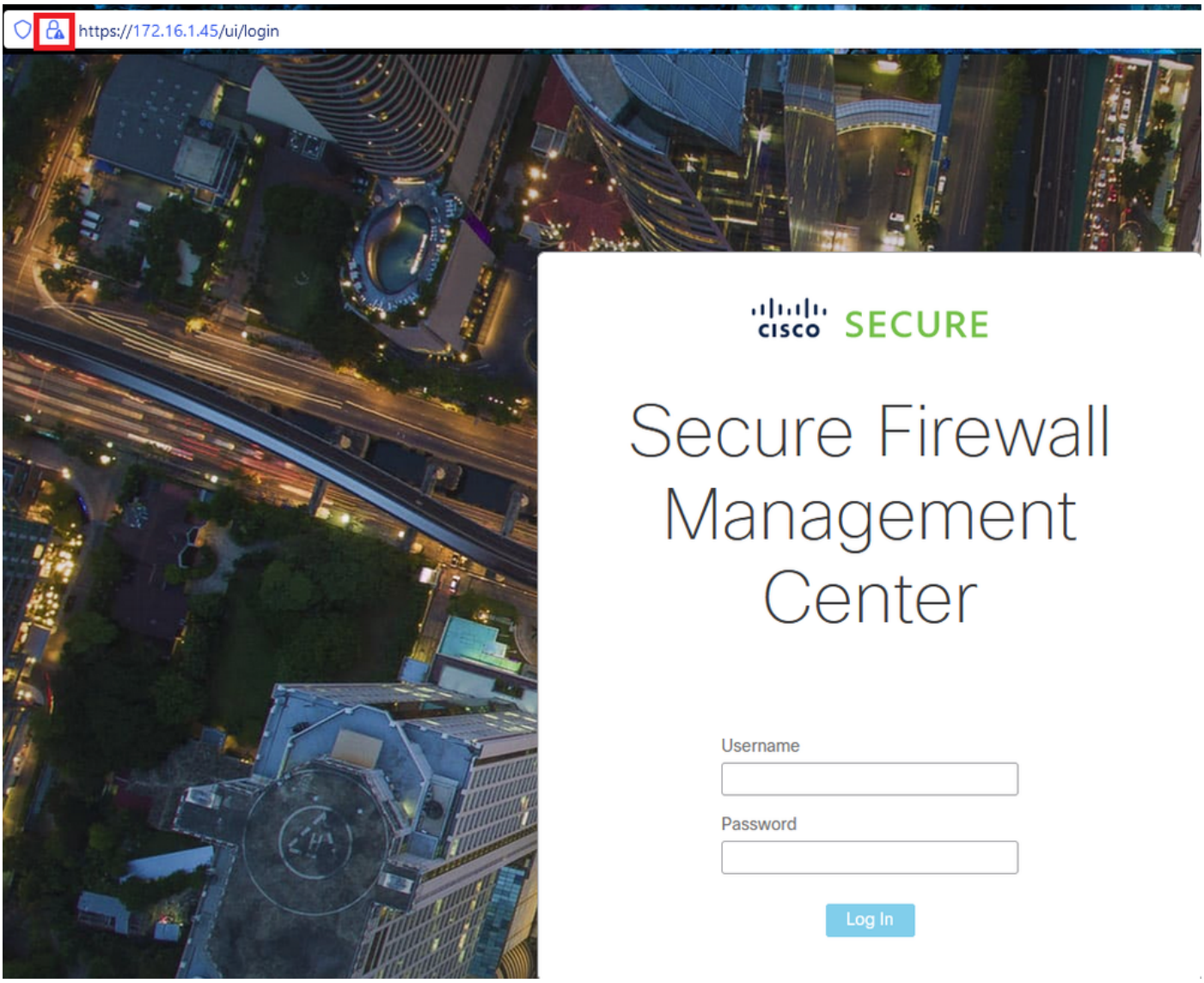
警告：在专用于适配器连接的UI上创建新的FMC用户。使用现有用户可能会在CSDAC或内部防火墙管理中心UI上创建意外注销。

注意：用户角色配置必须具有“管理员”、“访问管理员”或“网络管理员”角色。在IP地址字段上使用内部防火墙管理中心FQDN。

步骤 5：打开内部防火墙安全管理中心UI。



步骤 6： 从浏览器下载HTTPS PEM（链）证书：点击浏览器上显示的HTTPS挂锁、Secure Connection、More Information、View Certificate、PEM（链）。

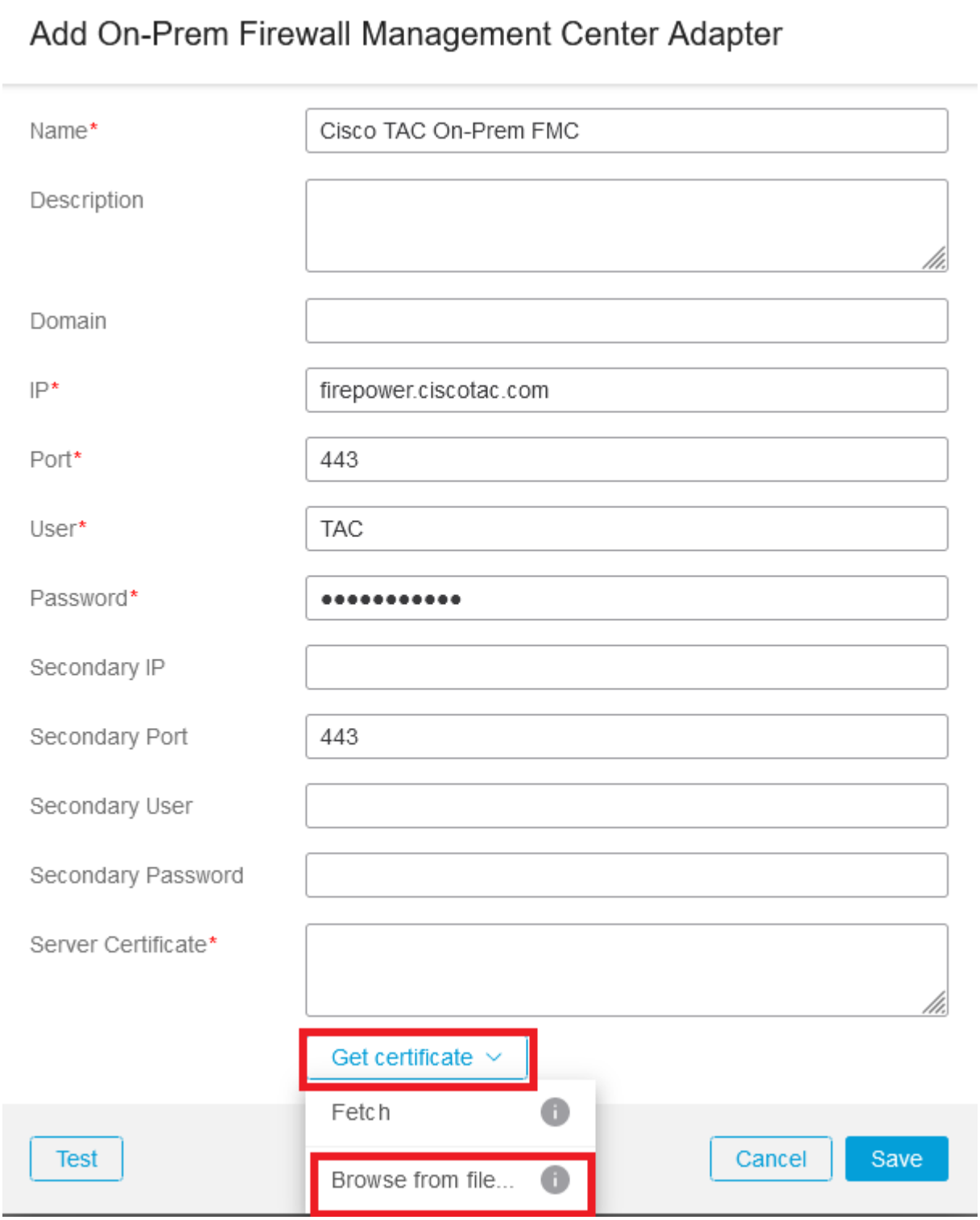




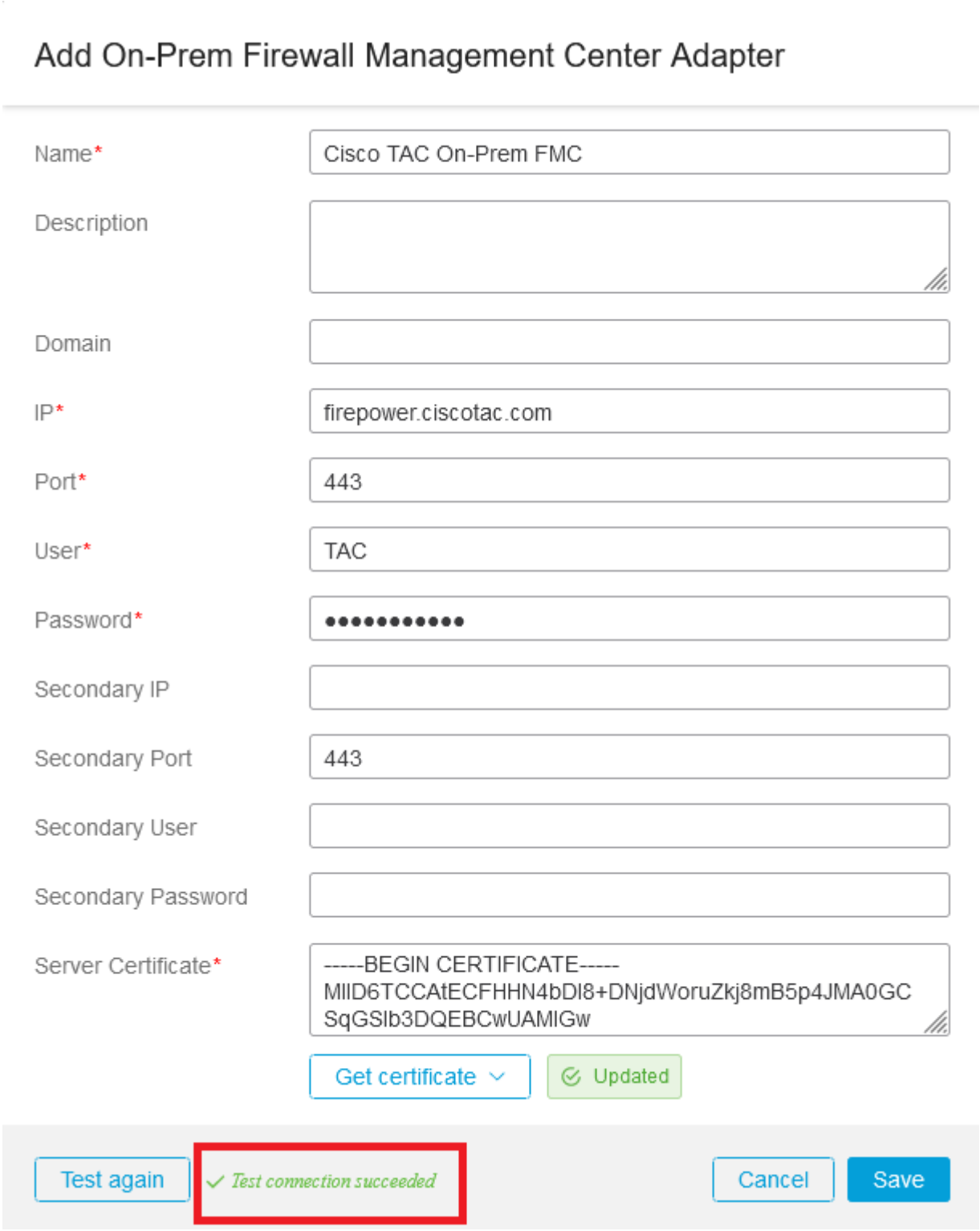
这会下载带有证书链的.pem文件。

注意：收集HTTPS内部安全防火墙管理中心证书的步骤属于Firefox浏览器。如果使用其他浏览器，请查找类似的步骤。

第7步：打开动态属性连接器，然后点击“获取证书”(Get certificate)和“从文件……”(Browse from file...)。

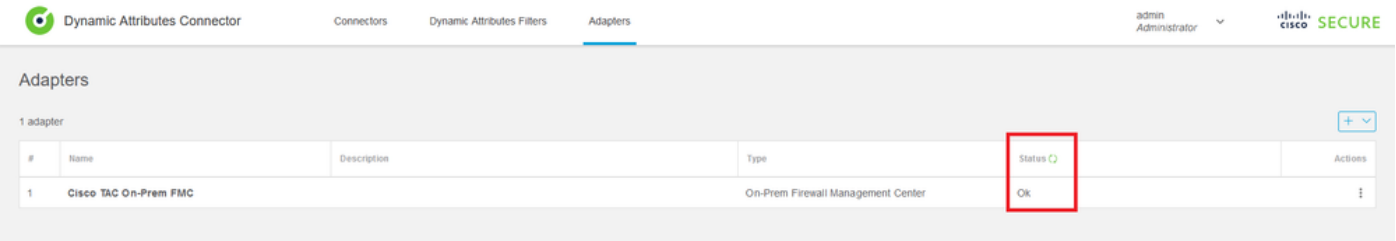


步骤 8::上传.pem证书并单击“测试”以确保测试成功。



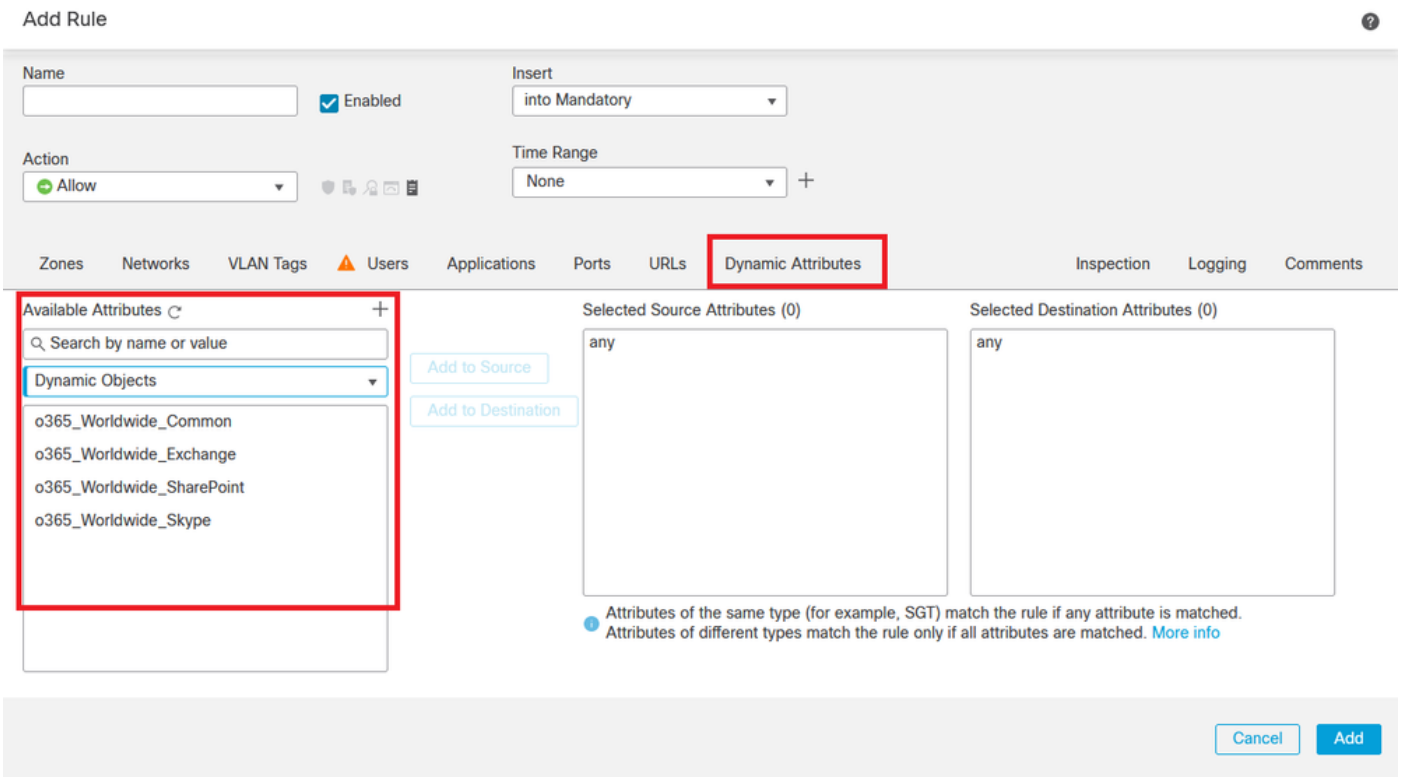
警告：确保Ubuntu计算机上配置的DNS服务器可以解析内部防火墙管理中心FQDN，否则，测试可能会失败。

步骤 9： 保存并确保状态为“OK”。



注意：无法为Office 365创建动态属性筛选器。

步骤 10：开始在内部防火墙管理中心UI上使用动态Office 365属性创建访问控制策略规则。

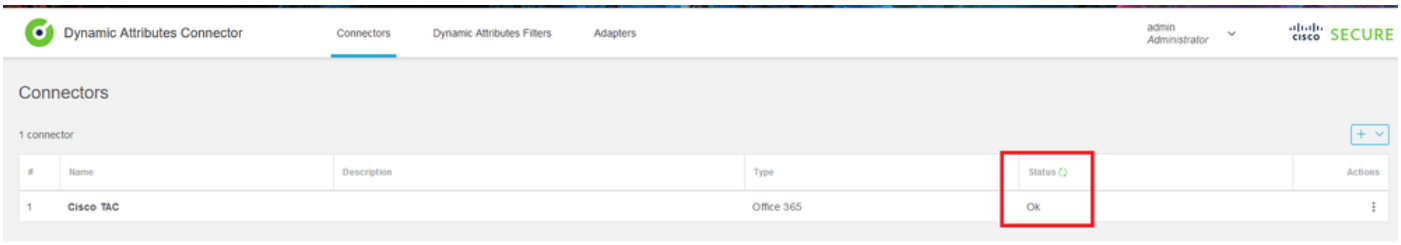


验证

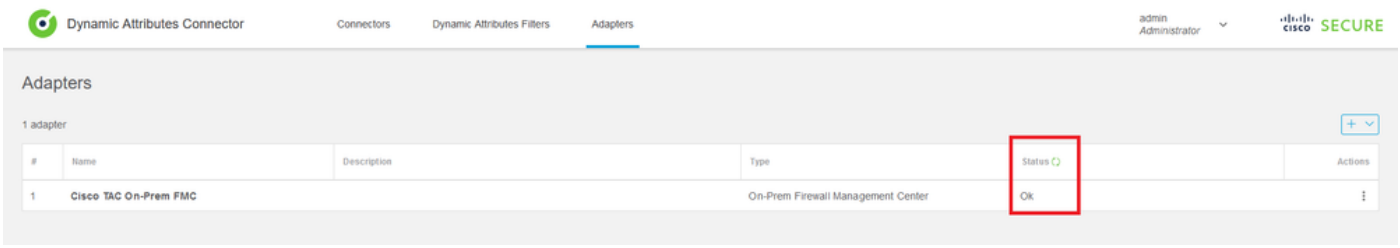
验证Ubuntu上核心服务、连接器和适配器的容器状态。

```
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
```

从CSDAC UI验证连接器状态。

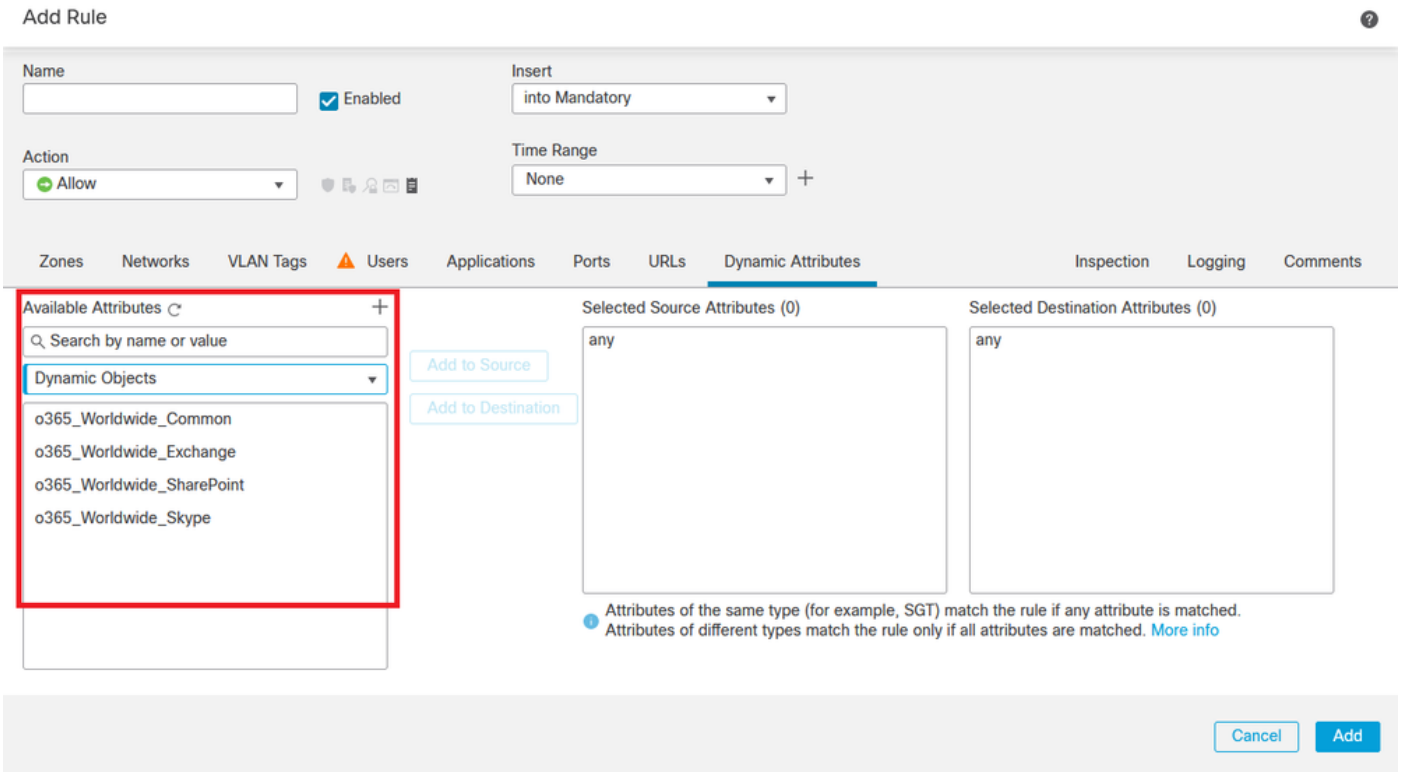


从CSDAC UI验证适配器状态。



在防火墙管理中心上验证Office 365动态属性。

创建或编辑访问控制策略规则，点击“动态属性”(Dynamic Attributes)，点击“可用属性”(Available Attributes)，然后选择“动态对象”(Dynamic Objects)。



注意：如果未列出Office 365动态对象，则集成可能存在问题。检查故障排除部分或联系思科TAC。

故障排除

如果Ansible存在安全动态属性连接器安装问题，请收集

“~/.ansible/collections/ansible_collection/cisco/csdac/logs/”目录中的“csdac.log”。

```
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
```

在此文件中找到安装失败日志。使用“cat”或“less”Linux命令将其打开，浏览故障日志，或联系Cisco TAC并提供此文件。

有时，Ansible安装由于“权限被拒绝”而失败。 浏览csdac.log文件并查找“permission denied”日志。

```
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
```

如果发现类似的日志，请考虑思科漏洞ID CSCwh58312或联系思科TAC以获得帮助。

如果“docker ps -a”指示容器关闭或要在出现问题时重新启动容器，可以使用“docker restart container-id”命令重新启动容器。

示例：使用容器ID“88826cf0742f”重新启动Office 365。

```
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
```

验证与CSDAC的连接，并验证是否在安全防火墙管理中心上创建对象。

```
> 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":[]
}
```

相关信息

有关思科安全动态属性(CSDAC)的其他文档，请访问此处：

关于Cisco动态属性连接器

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

安装和升级Cisco Secure Dynamic Attributes连接器

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

配置Cisco动态属性连接器

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

在访问控制策略中使用动态对象

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

动态属性连接器故障排除

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安装在Ubuntu 20.04中失败“Permission denied with Docker daemon socket”.

思科漏洞ID CSCwh58312。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。