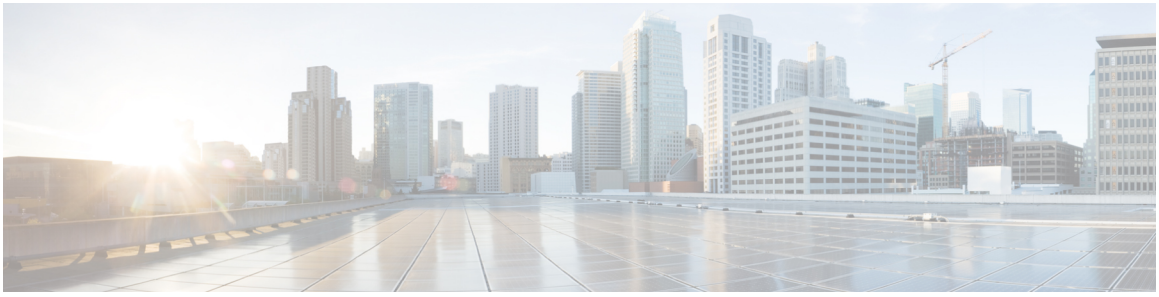
《Cisco Secure Dynamic Attributes Connector 配置指南》

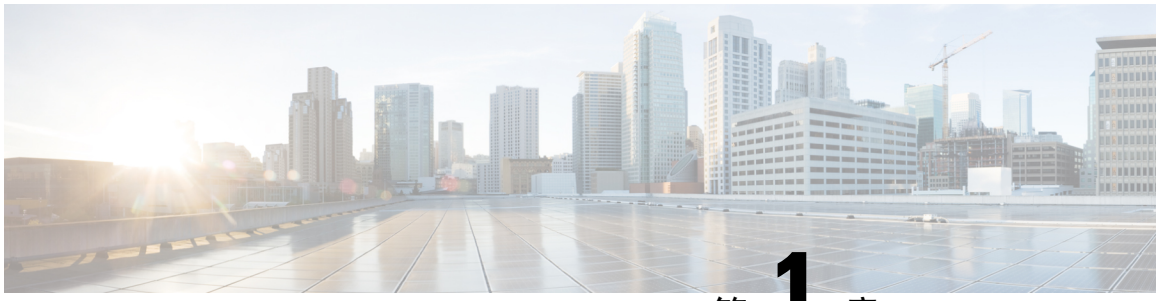
首次发布日期: 2021 年 6 月 1 日

上次修改日期: 2022 年 3 月 2 日

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



目 录



第 1 章

关于 Cisco Dynamic Attributes Connector

Cisco Secure Dynamic Attributes Connector 让您能够从云提供商收集数据（例如网络和 IP 地址）并将其发送到 Firepower 管理中心，以便将其用于访问控制规则中。

以下主题提供有关 dynamic attributes connector 的背景：

关于 Cisco Secure Dynamic Attributes Connector

Cisco Secure Dynamic Attributes Connector 让您能够在 Firepower 管理中心 (FMC) 访问控制规则中使用来自各种云服务平台的服务标签和类别。

由于工作负载的动态性质和 IP 地址重叠的必然性，网络结构（例如 IP 地址）在虚拟、云和容器环境中并不可靠。客户需要根据非网络结构（例如虚拟机名称或安全组）定义策略规则，以便即使 IP 地址或 VLAN 发生更改，防火墙策略也能保持不变。

我们目前支持：

- Microsoft Azure 服务器标签

  有关详细信息，请参阅 Microsoft TechNet 上的虚拟网络服务标签等资源

- Amazon Web 服务 (AWS) 服务标签

  有关更多信息，请参阅 Amazon 文档站点上的标记 AWS 资源等资源

- Office 365

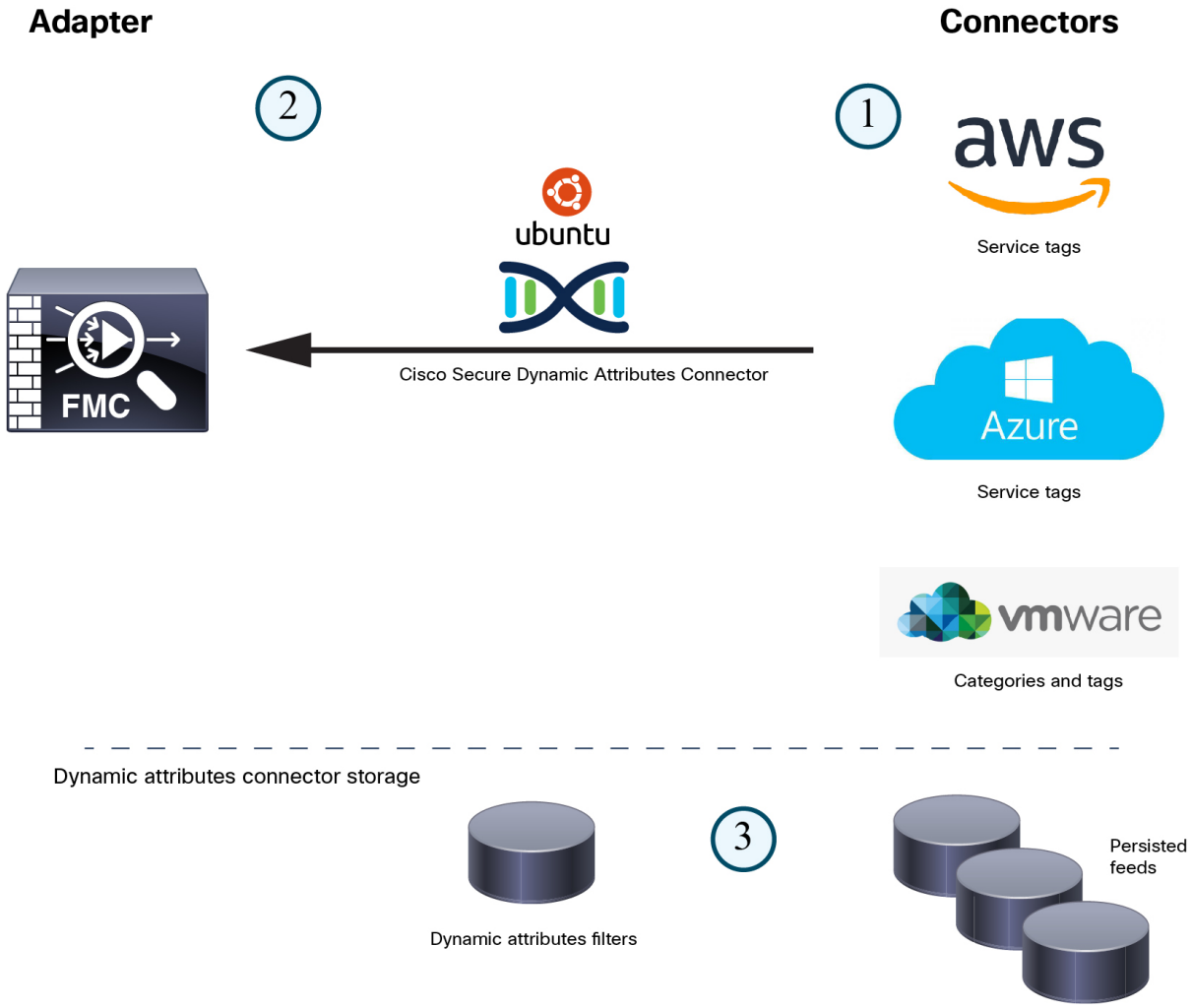
  有关详细信息，请参阅 docs.microsoft.com 上的 Office 365 URL 和 IP 地址范围。

- vCenter 和 NSX-T 管理的 VMware 类别和标签

  有关详细信息，请参阅 VMware 文档站点中 vSphere 标签和属性等资源

您可以使用在 Ubuntu 虚拟机上运行的 dynamic attributes connector Docker 容器来收集这些标签和属性。使用 Ansible 集合在 Ubuntu 主机上安装 dynamic attributes connector。

下图显示了系统的总体运行情况。



如图所示：

1. 连接器（当前为 AWS、Azure 和 vCenter）包含要查询的标签和容器。

   通常，这些标签会定义动态分配的网络和 IP 地址（比方说），而这些内容无法写入访问控制规则。来自连接器的源存储在 dynamic attributes connector 上，以便快速访问。

2. 标签信息会保留在您创建动态属性过滤器的 dynamic attributes connector 上，这些过滤器会定义哪些信息必须用于访问控制规则中。

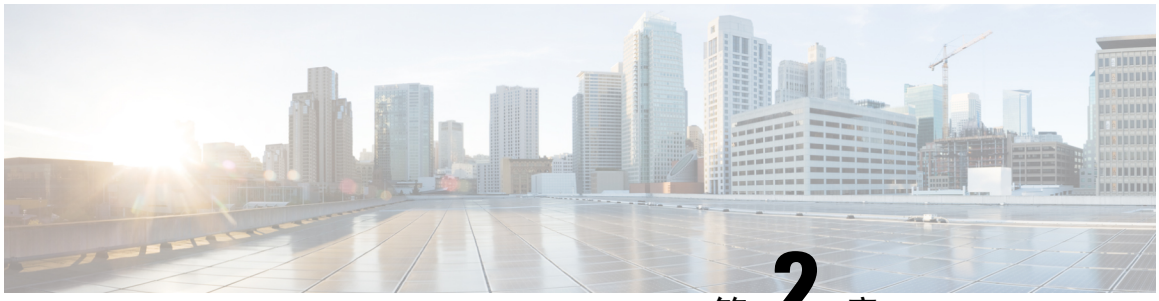
   例如，如果 vCenter 为记帐和财务部门虚拟机定义网络，则可以创建仅指定财务网络的过滤器。

3. dynamic attributes connector 定义的 FMC 适配器会将这些动态属性过滤器作为动态对象接收，并允许您将它们用于访问控制规则中。


什么是 Cisco Dynamic Attributes Connector?

相关主题

安装必备软件，第 6 页



第 2 章

配置 Cisco Secure Dynamic Attributes Connector

安装 dynamic attributes connector 并配置适配器、连接器和动态过滤器，以便为 FMC 提供可用于访问控制规则的动态网络数据。

有关详细信息，请参阅以下主题：

支持的操作系统和第三方软件

dynamic attributes connector 需要满足以下条件：

- Ubuntu 18.04
- Python 3.6.x
- Ansible 2.9 或更高版本

如果您想使用 vCenter 属性，我们还要求：

- vCenter 6.7
- VMware 工具必须安装在虚拟机上

安装必备软件

开始之前

确保您已设置物理或虚拟设置，并且系统可以与FMC通信。有关详细信息，请参阅支持的操作系统和第三方软件，第 5 页。

步骤 1 （可选。）如果您的Ubuntu计算机位于互联网代理后面，请使用文本编辑器来编辑 `/etc/environment` 以导出以下变量，从而实现与互联网的通信。

变量	值
export http_proxy	与 HTTP 代理配合使用。 *user*:*pass*@*host-or-ip*:*port*
export https_proxy	将此用于 HTTPS 代理。 *user*:*pass*@*host-or-ip*:*port*
export no_proxy	删除代理配置。 **export no_proxy="localhost,127.0.0.1"**

示例：

不使用身份验证的 HTTP 代理：

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

使用身份验证的 HTTPS 代理：

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

步骤 2 使用不同的命令窗口来确认设置：

```
env grep | proxy
```

示例结果：

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

步骤 3 继续执行以下部分之一。

相关主题

安装必备软件 - Ubuntu，第 7 页

安装必备软件 - Ubuntu

步骤 1 确保未安装 Docker，如已安装，请将其卸载。

```
docker --version
```

如已安装 Docker，请按照在 Ubuntu 上卸载 Docker 引擎中的说明进行卸载。

步骤 2 更新存储库。

```
sudo apt -y update
```

步骤 3 确认您的 Python 版本。

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

如果版本低于 3.6，则必须安装版本 3.6.x。

步骤 4 安装 Python 3.6。

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

步骤 5 安装通用库。

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

步骤 6 安装 Ansible。

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

步骤 7 验证 Ansible 版本。

```
ansible --version
```

示例如下。

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

注释 Ansible 会引用前面的输出显示的 Python 2.x 是正常的。连接器仍会使用 Python 3.6。

下一步做什么

按照 安装Cisco Secure Dynamic Attributes Connector， 第 8 页 中所述安装连接器。

要选择停止对 dynamic attributes connector 使用代理，请编辑 `/etc/environment` 并删除代理配置。

安装Cisco Secure Dynamic Attributes Connector

关于安装

本主题介绍如何安装 Cisco Secure Dynamic Attributes Connector。您必须以具有 `sudo` 权限的用户身份安装连接器，但也能以非特权用户身份运行连接器。

准备工作

确保您的系统具有以下必备软件：

- Ubuntu 18.04
- Python 3.6.x
- Ansible 2.9 或更高版本

如果您想使用 vCenter 属性，我们还要求：

- vCenter 6.7
- VMware 工具必须安装在虚拟机上

要安装必备软件，请参阅安装必备软件，第 6 页。

查看自述文件

有关最新的安装信息，请参阅自述文件：

https://galaxy.ansible.com/cisco/csdac

获取 Dynamic Attributes Connector 软件

要获取 dynamic attributes connector 软件的最新版本，请运行以下命令：

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

安装 muster 服务

muster 服务是 dynamic attributes connector 的另一个名称。

从 `~/.ansible/collections/ansible_collections/cisco/csdac` 目录运行以下命令。

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

Syntax Description

--ask-become-pass	系统会提示您输入 **sudo** 密码。在计算机上启用了 sudo 时为必填。

--extra-vars	以下可选的额外变量使能够让 dynamic attributes connector 使用代理。使用的值必须与您按照 安装必备软件，第 6 页 中的说明配置的 /etc/environment 中的值匹配。 • **csdac_proxy_enabled=true** • **csdac_http_proxy_url=http://***PROXY_URL* **csdac_https_proxy_url=***PROXY_URL* 以下可选的额外变量可以创建自签名证书，您可以将其用于安全连接到 dynamic attributes connector。如果省略这些参数，dynamic attributes connector 将使用默认证书。 • **csdac_certificate_domain** 自动生成的证书的域名。默认值为主自动检测到的主机名（由 ansible 检测） • **csdac_certificate_country_name** 两个字母的国家/地区代码。（默认值为 `US`） • **csdac_certificate_organization_name** 组织名称。（默认值为 `Cisco`） • **csdac_certificate_organization_unit_name** • 组织单位名称（默认值为 `Cisco`）

使用默认证书的安装示例

例如，要使用默认选项来安装软件：

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

使用可选证书的安装示例

例如，要使用可选证书来安装软件：

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

创建证书后，将其导入用于访问连接器的网络浏览器。证书在 `~/csdac/app/config/certs` 目录中创建。

查看安装日志

安装日志的位置如下：

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

使用您的证书连接到 dynamic attributes connector

如果您有证书和密钥，请将其放在 Ubuntu 计算机上的 `~/csdac/app/config/certs` 目录中。

执行上述任务后，通过输入以下命令重新启动 dynamic attributes connector 的 Docker 容器：

```
docker restart muster-ui
```

登录连接器

1. 通过 `https://ip-address` 访问 dynamic attributes connector
2. 登录。

   初始登录用户名为 `admin`，密码为 `admin`。第一次输入登录时会要求您更改密码。

获取证书颁发机构 (CA) 链

使用以下浏览器特定程序之一获取用于安全连接到 vCenter、NSX 或 FMC 的证书链。

证书链是根证书和所有从属证书。

您必须使用以下程序之一连接到以下设备：

- vCenter 或 NSX

  无需获取用于连接到 Azure 或 AWS 的证书链。

- 这种 FMC

获取证书链 - Mac（Chrome 和 Firefox）

使用此程序在 Mac OS 上使用 Chrome 和 Firefox 浏览器来获取证书链。

1. 打开终端窗口。
2. 输入以下命令。

   ```
   security verify-cert -P url[:port]
   ```

   其中 url 是 vCenter 或 FMC 的 URL（包括方案）。例如：

   ```
   security verify-cert -P https://myvcenter.example.com
   ```

   如果使用 NAT 或 PAT 访问 vCenter 或 FMC，可以按如下方式添加端口：

   ```
   security verify-cert -P https://myvcenter.example.com:12345
   ```

3. 将整个证书链保存到纯文本文件中。

   - 包括所有 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 分隔符。

- 排除任何无关的文本（例如，证书的名称和尖括号 (< and >) 中包含的任何文本以及尖括号本身。

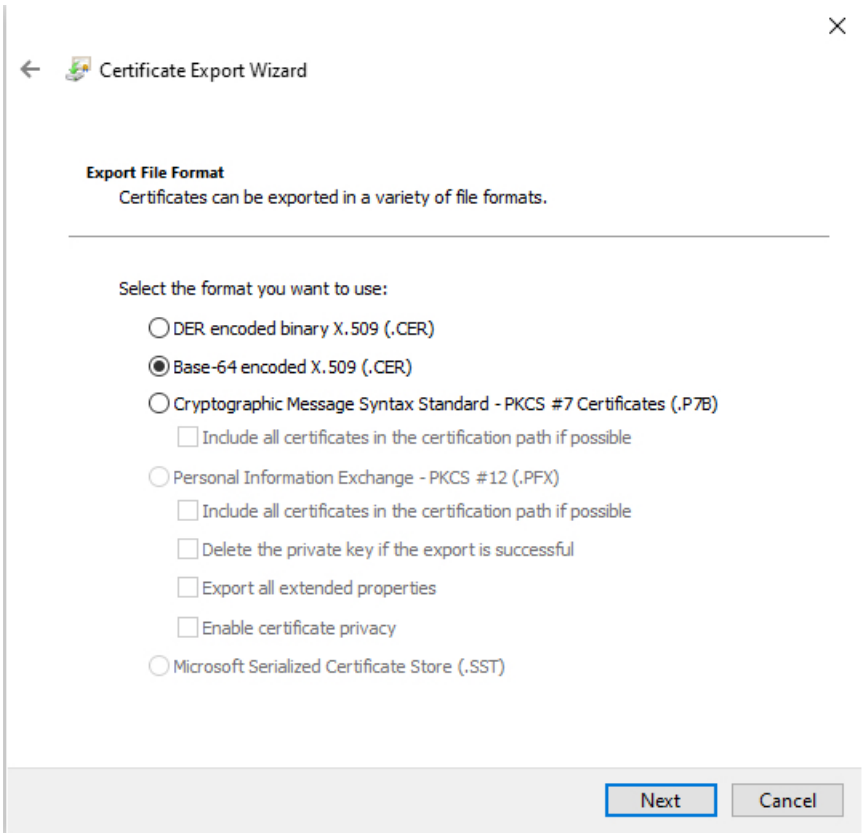
4. 对 vCenter 和 FMC 重复执行这些任务。

获取证书链 - Windows Chrome

使用此程序在 Windows 上使用 Chrome 浏览器来获取证书链。

1. 使用 Chrome 登录 vCenter 或 FMC。
2. 在浏览器地址栏中单击主机名左侧的锁图标。
3. 单击**证书 (Certificate)**。
4. 单击**认证路径 (Certification Path)** 选项卡。
5. 单击证书链中顶部的（即第一个）证书。
6. 单击**查看证书 (View Certificates)**。
7. 单击**详细信息 (Details)** 选项卡。
8. 单击**复制到文件 (Copy to File)**。
9. 按照提示创建包含整个证书链的 CER 格式证书文件。

   当系统提示您选择导出文件格式时，单击 **Base 64-Encoded X.509 (.CER)**，如下图所示。



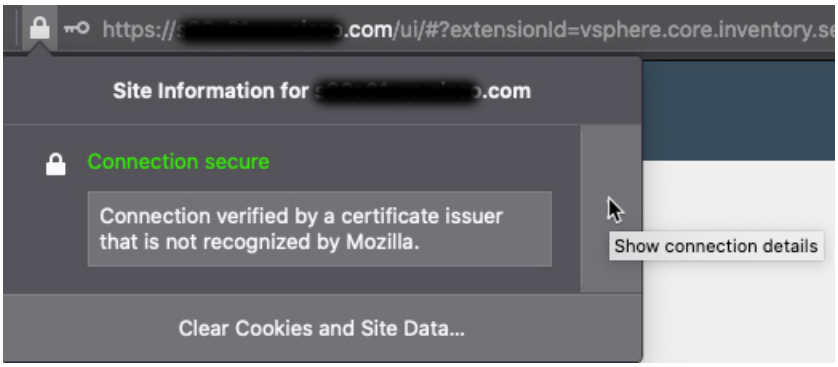
10. 按照提示完成导出。
11. 在文本编辑器中打开证书。
12. 对证书链中的所有证书重复此过程。

    您必须先按顺序将每个证书粘贴到文本编辑器中。
13. 对 vCenter 和 FMC 重复执行这些任务。

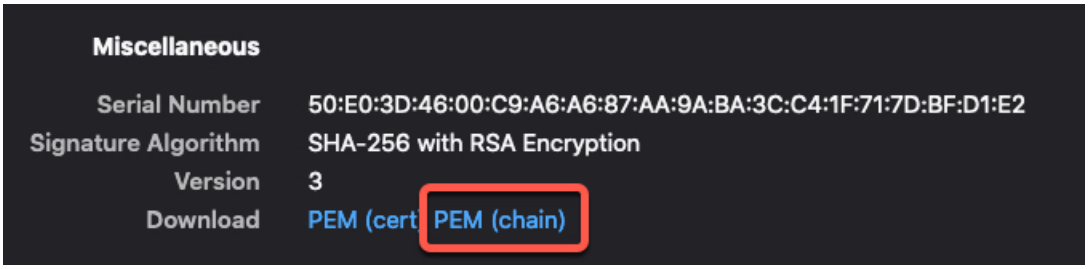
获取证书链 - Windows Firefox

使用以下程序为 Windows 或 Mac OS 上的 Firefox 浏览器来获取证书链。

1. 使用 Firefox 登录到 vCenter 或 FMC。
2. 单击主机名左侧的锁图标。
3. 单击右箭头（**显示连接详细信息**）。下图显示了一个示例。



4. 单击更多信息 **(More Information)**。
5. 单击查看证书 **(View Certificates)**。
6. 如果生成的对话框包含选项卡页面，请单击与顶层 CA 对应的选项卡页面。
7. 滚动到“其他”(Miscellaneous) 部分。
8. 单击下载行中的 **PEM**（链）**(PEM [chain])**。下图显示了一个示例。



9. 保存文件。
10. 对 vCenter 和 FMC 重复执行这些任务。

创建连接器

连接器是与云服务（当前为 Microsoft Azure、Amazon Web 服务 (AWS) 或 VMware vCenter）的接口。连接器从云服务检索网络信息，以便网络信息可用于 FMC 上的访问控制策略。

有关详细信息，请参阅以下各节之一：

相关主题

创建 AWS 连接器，第 14 页
创建 Azure 连接器，第 14 页
创建 Azure 服务标签连接器，第 15 页
创建 Office 365 连接器，第 16 页
创建 vCenter 连接器，第 17 页
排除问题 Cisco Secure Dynamic Attributes Connector，第 29 页

创建 AWS 连接器

步骤 1 登录 Dynamic Attributes Connector。

步骤 2 单击**连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：单击 **添加**（+），然后单击 **AWS**。
- 编辑或删除连接器：单击 **更多**（⋮），然后单击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 AWS 检索 IP 映射的间隔。
地区	（必需。）输入您的 AWS 区域代码。
访问密钥	（必需。）输入访问密钥。
加密密钥	（必需。）输入加密密钥。

步骤 5 单击**保存 (Save)**。

步骤 6 确保“状态”(Status) 列中显示**确定 (OK)**。

下一步做什么

创建适配器， 第 18 页

创建 Azure 连接器

步骤 1 登录 Dynamic Attributes Connector。

步骤 2 单击**连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：单击 **添加**（+），然后单击 **Azure**。

- 编辑或删除连接器：单击 **更多**（⋮），然后单击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。
订用 ID	（必需。）输入 Azure 订用 ID。
租户 ID	（必需。）输入租户 ID。
客户端 ID	（必需。）输入您的客户端 ID。
客户端密钥	（必需。）输入您的客户端密钥。

步骤 5 单击**保存 (Save)**。

步骤 6 确保“状态”(Status) 列中显示**确定 (OK)**。

下一步做什么

创建适配器，第 18 页

创建 Azure 服务标签连接器

本主题讨论了如何为 Azure 服务标签创建连接器。Microsoft 会每周更新与这些标记的 IP 地址关联。有关详细信息，请参阅 Microsoft TechNet 上的虚拟网络服务标签。

步骤 1 登录 Dynamic Attributes Connector。

步骤 2 单击**连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：单击 **添加**（＋），然后单击 **Azure**。
- 编辑或删除连接器：单击 **更多**（⋮），然后单击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。
订用 ID	（必需。）输入 Azure 订用 ID。
租户 ID	（必需。）输入租户 ID。
客户端 ID	（必需。）输入您的客户端 ID。
客户端密钥	（必需。）输入您的客户端密钥。

步骤 5 单击**保存 (Save)**。

步骤 6 确保“状态”(Status) 列中显示**确定 (OK)**。

下一步做什么

创建适配器，第 18 页

创建 Office 365 连接器

本主题讨论了如何为 Office 365 标签创建连接器。Microsoft 会每周更新与这些标记的 IP 地址关联。有关详细信息，请参阅 docs.microsoft.com 上的 Office 365 URL 和 IP 地址范围。

步骤 1 登录 Dynamic Attributes Connector。

步骤 2 单击**连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：单击 **添加**（+），然后单击 **Azure**。
- 编辑或删除连接器：单击 **更多**（⋮），然后单击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。

值	说明
基本 API URL	（必需。）输入要从中检索 Office 365 信息的 URL（如果其与默认值不同）。有关详细信息，请参阅 Microsoft 文档站点上的 Office 365 IP 地址和 URL Web 服务。
实例名称	（必需。）输入实例名称。有关详细信息，请参阅 Microsoft 文档站点上的 Office 365 IP 地址和 URL Web 服务。
禁用可选 API	（必需。）输入 **true** 或 **false**。

步骤 5 单击**保存 (Save)**。

步骤 6 确保“状态”(Status) 列中显示**确定 (OK)**。

下一步做什么

创建适配器，第 18 页

创建 vCenter 连接器

开始之前

如果使用不受信任的证书与 vCenter 通信，请参阅获取证书颁发机构 (CA) 链，第 10 页。

步骤 1 登录 Dynamic Attributes Connector。

步骤 2 执行以下任一操作：

- 添加新连接器：单击 **添加**（  ），然后单击 **vCenter**。
- 编辑或删除连接器：单击 **更多**（  ），然后单击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 3 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	输入可选的说明。
提取间隔	（默认为 30 秒。）从 vCenter 检索 IP 映射的间隔。

值	说明
主机	（必需。）输入以下任意命令： • vCenter 的完全限定主机名 • vCenter 的 IP 地址 • （可选。）A 端口 请勿输入方案（例如 **`https://`**）或末尾斜杠。 例如，**`myvcenter.example.com`** 或 **`192.0.2.100:9090`**
用户	（必需。）输入至少具有只读角色的用户的用户名。用户名区分大小写。
密码	（必需。）输入用户的密码。
NSX IP	如果使用 vCenter 网络安全可视化 (NSX)，请输入其 IP 地址。
NSX 用户	输入至少具有审核员角色的 NSX 用户的用户名。
NSX 类型	输入 **NSX-T**。
NSX 密码	输入 NSX 用户的密码。
vCenter 证书	输入用于安全连接到 vCenter 或 NSX-T 的证书。有关详细信息，请参阅获取证书颁发机构 (CA) 链，第 10 页。

步骤 4 单击测试 **(Test)** 并确保在保存连接器之前显示 **Test connection succeded**。

步骤 5 单击保存 **(Save)**。

下一步做什么

创建适配器，第 18 页

创建适配器

适配器是与 FMC 的安全连接，您可以将来自云对象的网络信息推送到 FMC 以用于访问控制策略。

相关主题

为 Dynamic Attributes Connector 创建 FMC 用户，第 19 页
创建 FMC 适配器，第 20 页
管理 FMC 动态对象源订用，第 22 页
排除问题 Cisco Secure Dynamic Attributes Connector，第 29 页

为 Dynamic Attributes Connector 创建 FMC 用户

开始之前

我们建议您为 dynamic attributes connector 适配器创建 FMC 用户。创建专门的 FMC 用户可避免从 FMC 中意外注销等问题，因为 dynamic attributes connector 会定期使用 REST API 登录，以使用新的和更新的动态对象来更新 FMC。

FMC 用户必须至少具有访问管理员权限。

步骤 1 如果尚未登录，请登录FMC。

步骤 2 请单击 **系统** > **用户**。

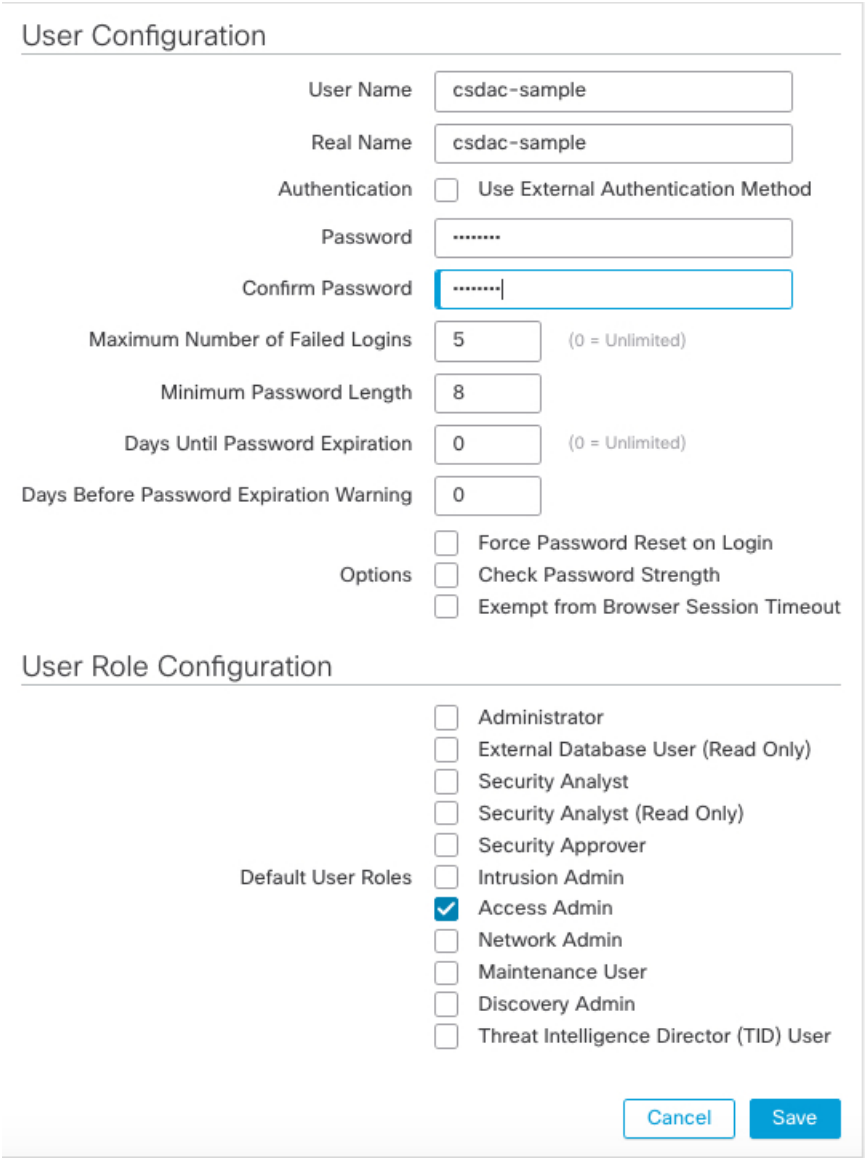
步骤 3 单击**创建用户 (Create User)**。

步骤 4 输入创建用户所需的信息。

步骤 5 在用户角色配置下，选中以下任何默认角色或具有相同权限级别的自定义角色：

- **管理员**
- **访问管理员**
- **网络管理员**

下图显示了一个示例。



您还可以选择具有足够权限的自定义角色以允许 REST 操作，或者选择具有足够权限的不同默认角色。有关默认角色的详细信息，请参阅有关用户帐户的章节中的“用户角色”部分。

下一步做什么

请参阅 创建 FMC 适配器，第 20 页

创建 FMC 适配器

本主题讨论了如何创建适配器，以便将动态对象从 dynamic attributes connector 推送 FMC 到。

开始之前

请参阅为 Dynamic Attributes Connector 创建 FMC 用户，第 19 页。

步骤 1 如果尚未登录，请登录 dynamic attributes connector。

步骤 2 单击**适配器 (Adapters)**。

步骤 3 执行以下任一操作：

- 添加新适配器：单击 **添加**（+），然后单击 **FMC**。
- 编辑或删除适配器：单击 **更多**（⋮），然后单击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入可标识适配器的唯一名称。
说明	适配器的可选说明。
域	输入要在其中创建动态对象的 FMC 域。将字段留空以便在全局域中创建动态对象。 例如，**`Global/MySubdomain`**
IP	（必需。）输入您的 FMC 的主机名或 IP 地址。 您输入的主机名或 IP 必须与用于安全连接的 CA 证书的通用名称完全匹配。
端口	（必需。）输入 FMC 使用的 TLS 端口。
用户	（必需。）输入至少具有网络管理员角色的 FMC 用户的名称。
密码	（必需。）输入用户的密码。
辅助 IP	（仅限高可用性。）输入辅助 FMC 的主机名或 IP 地址。 您输入的主机名或 IP 必须与用于安全连接的 CA 证书的通用名称完全匹配。
辅助端口	（仅限高可用性。）输入辅助 FMC 使用的 TLS 端口。
辅助用户	（仅限高可用性。）输入至少具有网络管理员角色的辅助 FMC 用户的名称。
辅助密码	（仅限高可用性。）输入用户的密码。
FMC 服务器证书 (FMC Server Certificate)	粘贴您找到的 CA 证书链，如获取证书颁发机构 (CA) 链，第 10 页中所述。

步骤 5 单击**保存 (Save)**。

相关主题

排除问题 Cisco Secure Dynamic Attributes Connector，第 29 页

管理 FMC 动态对象源订用

如何在 FMC 中为以下对象启用动态对象源订用：

- Azure 服务标签
- Office 365

您无需按照此程序使用以下内容：

- AWS
- Azure
- vCenter

步骤 1 如果尚未登录，请登录 FMC。

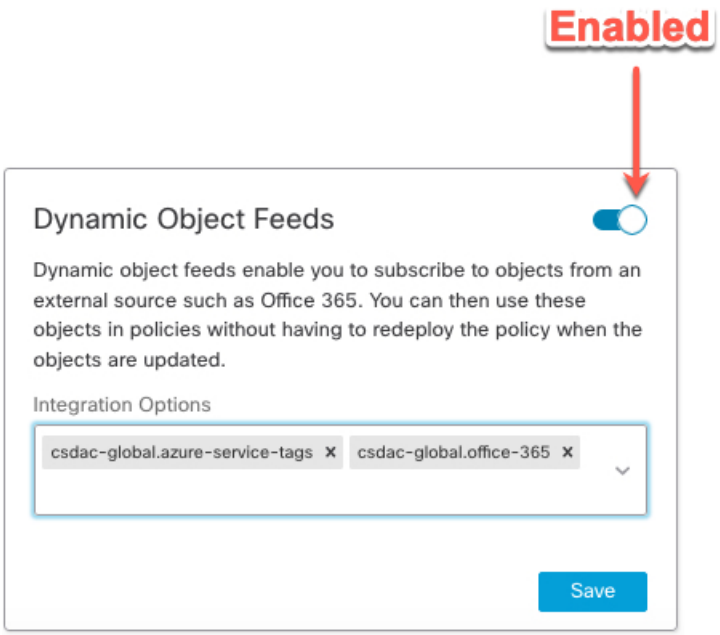
步骤 2 请单击 **系统** > **集成**。

步骤 3 单击**云服务 (Cloud Services)**。

步骤 4 在“动态对象源”(Dynamic Object Feeds) 旁边，向右滑动滑块以启用或向左滑动以禁用。

步骤 5 单击动态对象源以启用。

下图显示了如何同时启用 Azure 服务标签和 Office 365。



步骤 6 要取消订用，请单击动态对象源名称旁边的 **x**。

步骤 7 单击**保存 (Save)**。

创建动态属性过滤器

使用 Cisco Secure Dynamic Attributes Connector 定义的动态属性过滤器会在 FMC 中显示为可在访问控制策略中使用的动态属性。例如，您可以将财务部门对 AWS 服务器的访问权限限制为 Microsoft Active Directory 中定义的财务组成员。

注释 不能为 Office 365 或 Azure 服务标签创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

有关详情，请参阅：

- 在 Amazon 文档站点上标记 AWS 资源

有关访问控制规则的详细信息，请参阅使用动态属性过滤器来创建访问控制规则，第 27 页。

开始之前

完成以下所有任务：

- 安装必备软件，第 6 页
- 创建连接器，第 13 页
- 创建适配器，第 18 页

步骤 1 登录 Dynamic Attributes Connector。

步骤 2 单击**动态属性过滤器 (Dynamic Attributes Filters)** 选项卡。

执行以下任一操作：

- 添加新过滤器：单击 **添加**（ ）。
- 编辑或删除过滤器：单击 **更多**（ ），然后单击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 3 输入以下信息。

项目	说明
名称	用于在访问控制策略和 FMC 对象管理器（**外部属性** > **动态对象**）中标识动态过滤器（作为动态对象）的唯一名称。
连接器	在列表中单击要使用的连接器的名称。

项目	说明
查询	• 添加新过滤器查询：单击 **添加**（ ） • 编辑或删除现有过滤器查询：单击 **更多**（ ），然后单击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 要添加或编辑查询，请输入以下信息。

项目	说明
密钥	单击列表中的一个键。密钥会从连接器获取。
操作	单击以下选项之一： • **等于 (Equals)** 会将密钥与值完全匹配。 • **包含 (Contains)** 会将键与值匹配（如果值的任何部分匹配）。
值	单击**任意 (Any)** 或**全部 (All)**，然后单击列表中的一个或多个值。单击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 5 单击**显示预览 (Show Preview)** 以便显示查询返回的网络或 IP 地址的列表。

步骤 6 完成后，单击**保存 (Save)**。

步骤 7 （可选。）验证 FMC 中的动态对象。

a) 至少要以具有网络管理员角色的用户身份登录 FMC。

b) 单击**对象 (Objects)** > **对象管理器 (Object Manager)**。

c) 在左侧窗格中，单击**外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。
您创建的动态属性查询应显示为动态对象。

相关主题

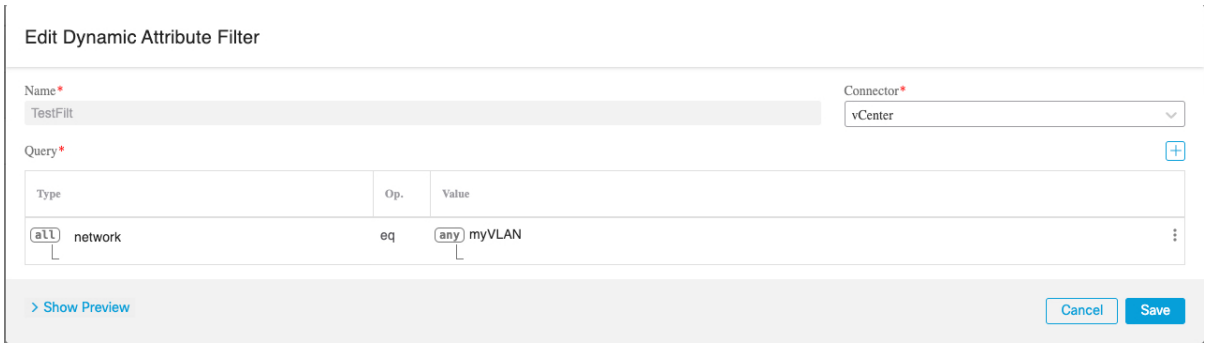
动态属性过滤器示例，第 24 页

动态属性过滤器示例

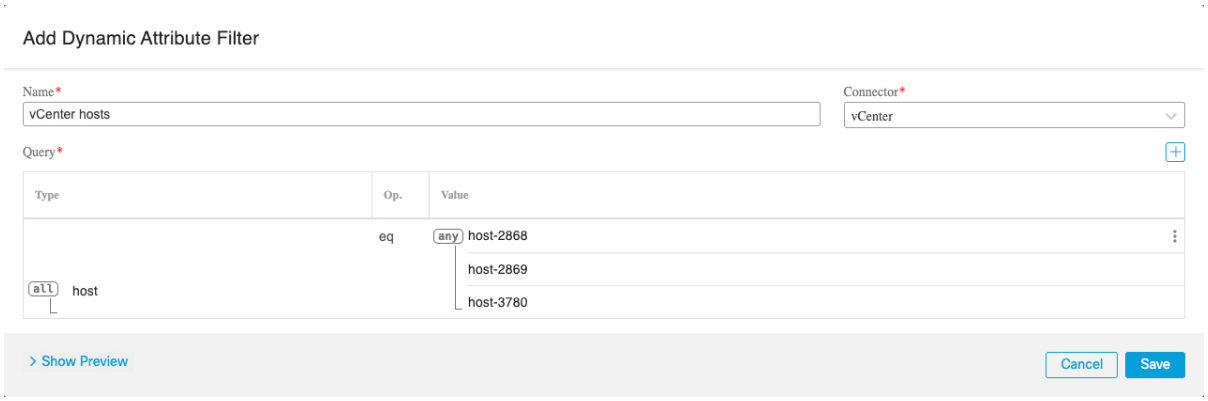
本主题提供了设置动态属性过滤器的一些示例。

示例：vCenter

以下示例显示了一个条件：VLAN。

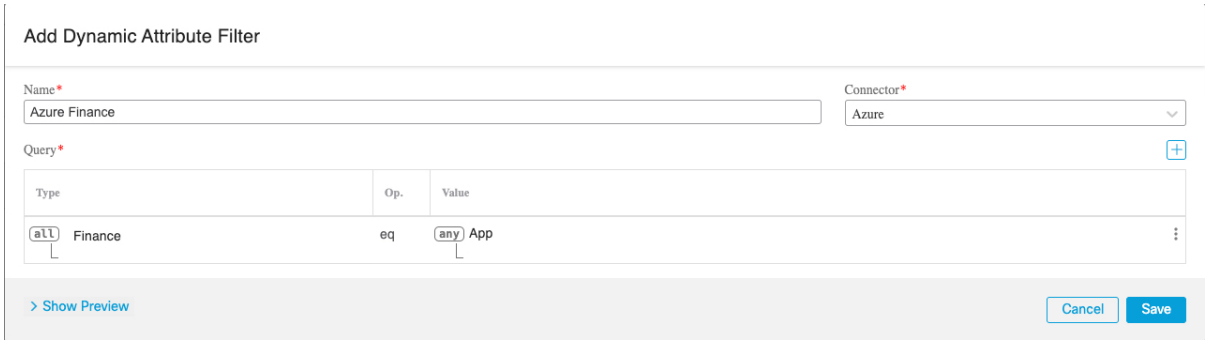


以下示例显示了使用 OR 连接的三个条件：查询匹配三个主机中的任何一个。



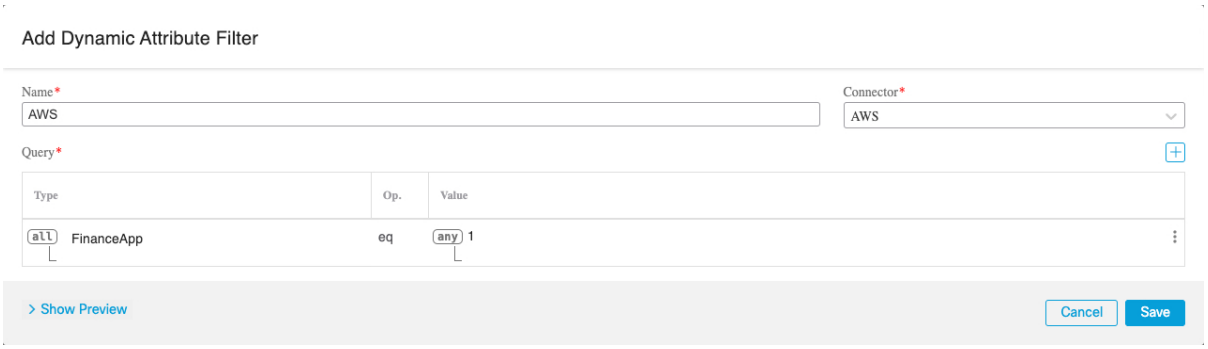
示例：Azure

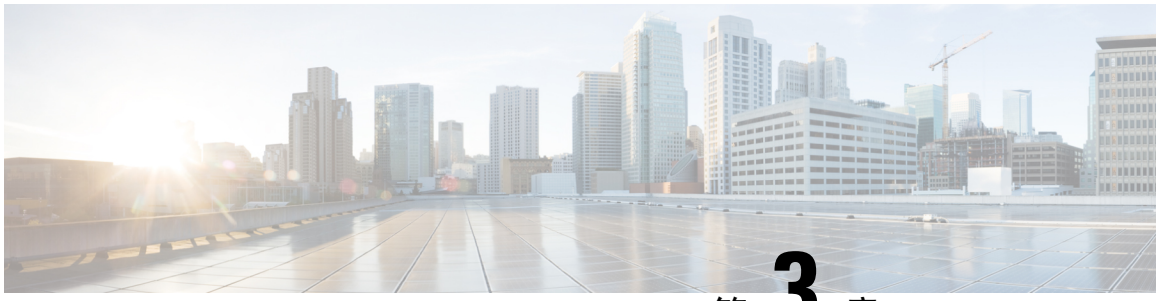
以下示例显示了一个条件：标记为财务应用的服务器。



示例：AWS

以下示例显示了一个条件：值为 1 的 FinanceApp。


Add Dynamic Attribute Filter
Name*
AWS
Connector*
AWS
Query*
Type
Op.
Value
all
FinanceApp
eq
any
1
> Show Preview
Cancel
Save



第 3 章

在访问控制策略中使用动态对象

通过 dynamic attributes connector，您可以在访问控制规则中配置动态过滤器（在 FMC 中可视为动态对象）。

关于访问控制规则中的动态对象

在连接器上保存动态属性过滤器后，动态对象会自动从 dynamic attributes connector 推送到定义的 FMC 适配器。

您可以在访问控制规则的“动态属性”(Dynamic Attributes) 选项卡页面上使用这些动态对象，这类似于使用安全组标记 (SGT) 的方式。您可以将动态对象添加为源或目标属性；例如，在访问控制阻止规则中，您可以将财务动态对象添加为目标属性，以阻止通过匹配规则中其他条件的对象访问财务服务器。

使用动态属性过滤器来创建访问控制规则

本主题讨论如何使用动态对象（这些动态对象以您之前创建的动态属性过滤器来命名）创建访问控制规则。

开始之前

创建动态属性过滤器，如创建动态属性过滤器， 第 23 页中所述。

步骤 1 至少要以具有网络管理员角色的用户身份登录 FMC。

步骤 2 依次单击**策略 (Policies)** > **访问控制 (Access Control)**。

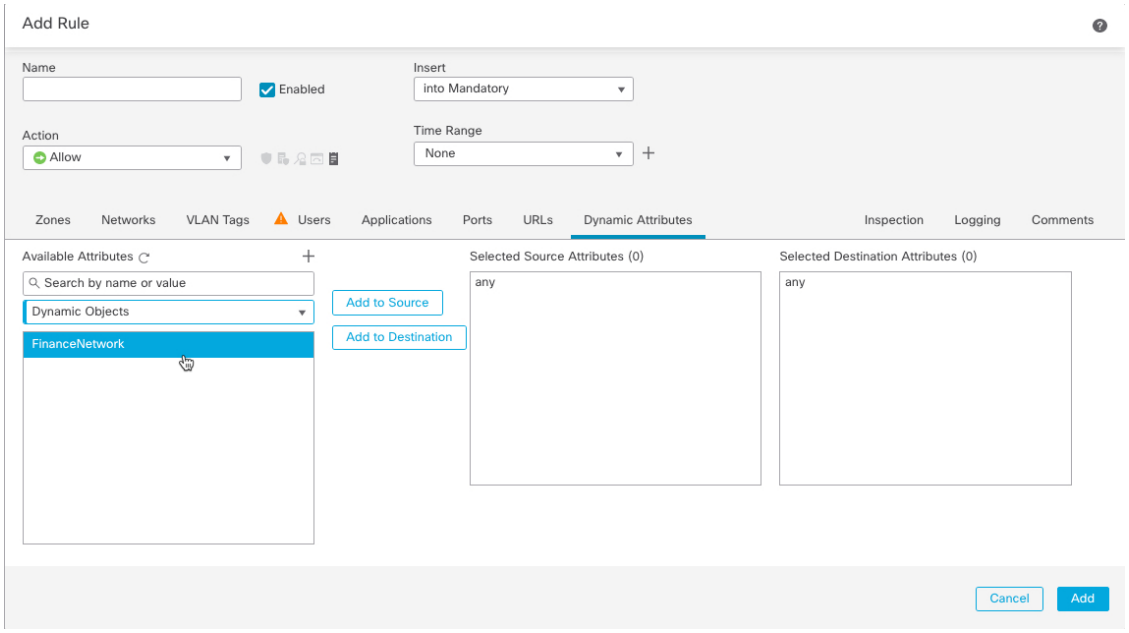
步骤 3 单击访问控制策略旁边的 **编辑**（ ）。

步骤 4 单击**添加规则 (Add Rule)**。

步骤 5 单击**动态属性 (Dynamic Attributes)** 选项卡。

步骤 6 在“可用属性”(Available Attributes) 部分中，单击列表中的**动态对象 (Dynamic Objects)**。

下图显示了一个示例。



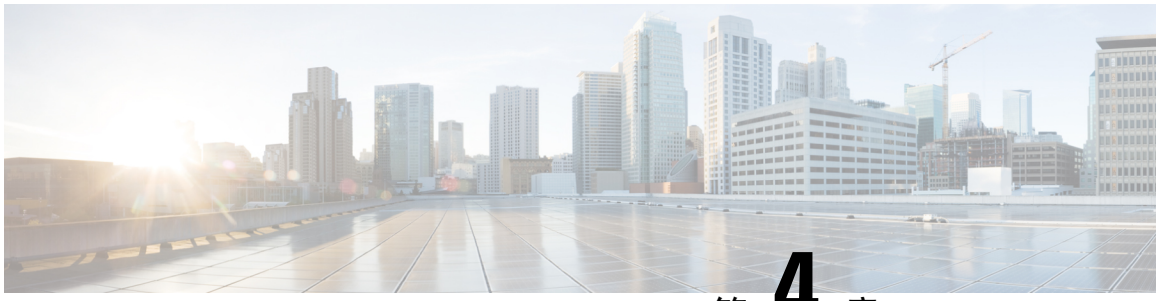
前面的示例显示了一个名为 `FinanceNetwork` 的动态对象，该对象对应于 Dynamic Attributes Connector 中创建的动态属性过滤器。

步骤 7 将所需对象添加到源或目标属性。

步骤 8 如果需要，向规则中添加其他条件。

下一步做什么

《*Firepower* 管理中心配置指南》中的“访问控制”章节。（链接到章节）



第 4 章

Dynamic Attributes Connector 故障排除

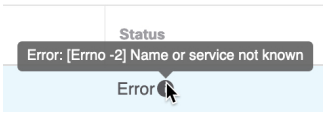
如何对 dynamic attributes connector 进行问题故障排除，包括使用提供的工具。

排除问题 Cisco Secure Dynamic Attributes Connector

本主题为您在使用 dynamic attributes connector 时可能会遇到的问题提供了建议的解决方案。

问题：名称或服务未知错误

当您将鼠标悬停在适配器或连接器的错误条件上时，此错误将显示为工具提示。示例如下；实际可能看起来有所不同。



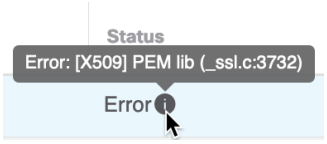
解决方案：编辑连接器或适配器，然后检查：

- 主机名末尾的斜杠
- 主机名开头的方案（例如，`https://`）
- 验证密码是否正确
- 对于适配器，请验证 **FMC 服务器证书 (FMC Server Certificate)** 字段的内容。

  有关详细信息，请参阅获取证书颁发机构 (CA) 链， 第 10 页。

问题：[X509 PEM 库]

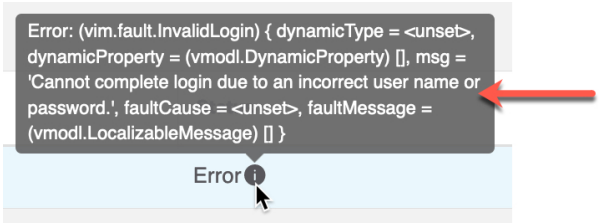
当您将鼠标悬停在连接器的错误条件上时，此错误将显示为工具提示。



解决方案：编辑连接器并检查 CA 链。有关详细信息，请参阅获取证书颁发机构 (CA) 链，第 10 页。

问题：用户名或密码不正确

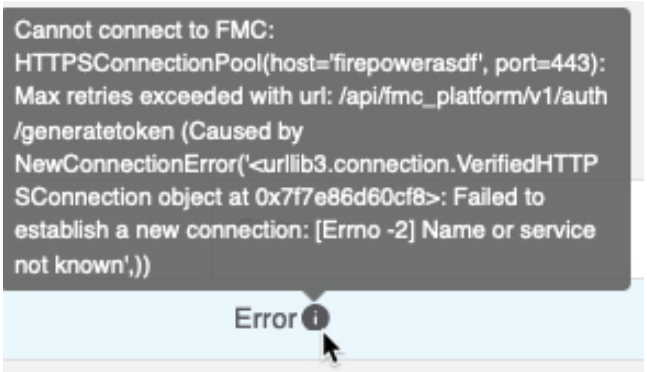
当您将鼠标悬停在连接器的错误条件上时，此错误将显示为工具提示。



解决方案：编辑连接器并更改用户名或密码。

问题：适配器超时或最大重试次数错误

当您将鼠标悬停在适配器的错误条件上时，此错误将显示为工具提示。



解决方案：请执行以下所有操作：

- 验证 **FMC 服务器证书 (FMC Server Certificate)** 字段的内容。
- 确保您在 **IP** 字段中输入的值与证书的通用名称完全匹配。

有关详细信息，请参阅获取证书颁发机构 (CA) 链，第 10 页。

故障排除工具

为了帮助您进行高级故障排除和使用思科 TAC，我们提供L 以下故障排除工具。要使用这些工具，请以任何用户身份登录运行 dynamic attributes connector 的 Ubuntu 主机。

检查容器状态

要检查 dynamic attributes connector Docker 容器的状态，请输入以下命令：

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

输出示例如下：

```
============================== CORE SERVICES ==============================
      Name                      Command                  State    Ports
-----------------------------------------------------------------------------------------------------------
muster-bee     ./docker-entrypoint.sh run ...   Up             50049/tcp, 50050/tcp

muster-etcd    etcd                             Up             2379/tcp, 2380/tcp

muster-ui      /docker-entrypoint.sh runs ...   Up (healthy)
0.0.0.0:443->8443/tcp,:::443->8443/tcp
muster-ui-backend   ./docker-entrypoint.sh run ...   Up             50031/tcp

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

启用调试日志记录并生成故障排除文件

如果思科 TAC 建议这样做，请启用调试日志记录并生成故障排除文件，如下所示：

```
cd ~/csdac/app
sudo ./muster-cli debug-on
sudo ./muster-cli ts-gen
```

故障排除文件名为 **ts-bundle-***timestamp***.tar** 并在同一目录中创建。

下表显示了故障排除文件的位置以及故障排除文件中的日志。

位置	它包含的内容
/csdac/app/ts-bundle-*timestamp***/info**	`etcd` 数据库内容
/csdac/app/ts-bundle-*timestamp***/logs**	容器日志文件
/csdac/app/ts-bundle-*timestamp***/status.log**	容器状态、版本和映像状态

验证 FMC 上的动态对象

要验证连接器和适配器是否正在 FMC 上创建对象，您可以在 FMC 上以管理员身份使用以下命令：

```
sudo tail f /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log
```

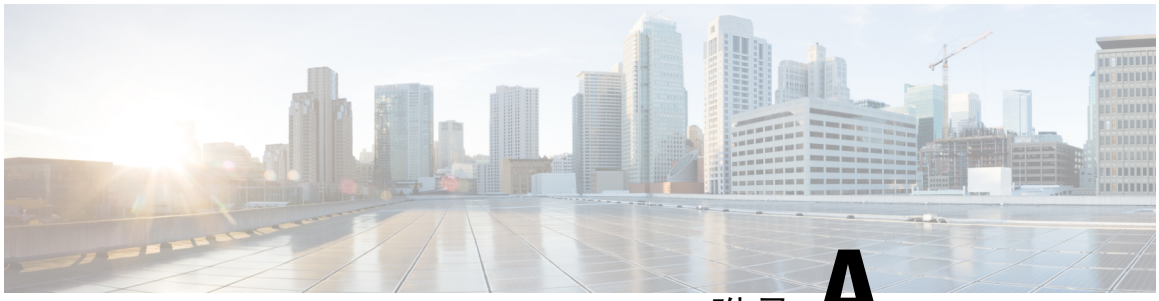
示例：成功创建对象

```
26-Aug-2021 12:41:35.912,[INFO],(DefenseCenterServiceImpl.java:1442)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-10
** REST Request [ CSM ]
** ID : 18b25356-fd6b-4cc4-8d27-bbccb52a6275
** URL: POST /audit
{
```

```
  "version": "7.1.0",
  "requestId": "18b25356-fd6b-4cc4-8d27-bbccb52a6275",
  "data": {
    "userName": "csdac-centos8",
    "subsystem": "API",
    "message": "POST
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f
/object/dynamicobjects Created (201) - The request has been fulfilled and resulted in a new
 resource being created",
    "sourceIP": "192.168.0.103",
    "domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time": "1629981695431"
  },
  "deleteList": []
}
```

示例：对象创建失败（在本例中是因为适配器用户没有足够的权限）：

```
26-Aug-2021 12:47:50.440,[INFO],(DefenseCenterServiceImpl.java:1442)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-2
** REST Request [ CSM ]
** ID : 58566831-7532-4d61-a579-2bbc3c325b2f
** URL: POST /audit
{
  "version": "7.1.0",
  "requestId": "58566831-7532-4d61-a579-2bbc3c325b2f",
  "data": {
    "userName": "csdac-centos8",
    "subsystem": "API",
    "message": "GET
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/
object/dynamicobjects/vCenter___CentOS_8__4 Forbidden (403) - The server understood the
request, but is refusing to fulfill it",
    "sourceIP": "192.168.0.103",
    "domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time": "1629982070404"
  },
  "deleteList": []
}
```



附录 A

安全和互联网接入

与云服务提供商和 FMC 通信时，dynamic attributes connector 使用的 URL 列表。

安全要求

为了保护Cisco Secure Dynamic Attributes Connector，应将其安装在受保护的内部网络中。虽然dynamic attributes connector被配置为仅提供必要的服务和端口，但您必须确保该防御中心不会受到攻击。

如果 dynamic attributes connector 和 Firepower 管理中心 (FMC) 位于同一个网络，您可以将 FMC 连接到与 dynamic attributes connector 相同的受保护内部网络。

无论如何部署设备，内部系统通信将始终加密。但是，您仍需采取措施，确保设备之间的通信不会出现中断、阻塞或受到篡改；例如，遭受分布式拒绝服务 (DDoS) 或中间人攻击。

互联网接入要求

默认情况下，dynamic attributes connector 会被配置为使用端口 443/tcp (HTTPS) 上的 HTTPS 通过互联网与 Firepower 系统通信。如果您不希望 dynamic attributes connector 直接访问互联网，则可以配置代理服务器。

以下信息会告知您 dynamic attributes connector 用来与 FMC 和外部服务器通信的 URL。

表 *1: Dynamic Attributes Connector FMC* 访问要求

URL	原因
https://*fmc-ip***/api/fmc_platform/v1/auth/generatetoken**	身份验证
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id***/object/dynamicobjects**	GET 和 POST 动态对象

安全和互联网接入

URL	原因
https://*fmc-ip***/api/fmc_config/ v1/domain/***domain-id***/object/dynamicobjects/***object-id***/mappings?action=add**	添加映射
https://*fmc-ip***/api/fmc_config/ v1/domain/***domain-id* **/object/dynamicobjects/***object-id***/mappings?action=remove**	删除映射

表 *2: Dynamic Attributes Connector vCenter* 访问要求

URL	原因
https://*vcenter-ip***/rest/com/vmware/cis/session**	身份验证
https://*vcenter-ip***/rest/vcenter/vm**	获取 VM 信息
https://*nsx-ip***/api/v1/fabric/virtual-machines/***vm-id*	获取与虚拟机关联的 NSX-T 标签

Dynamic Attributes Connector AWS 访问要求

dynamic attributes connector 会调用内置 SDK 方法获取实例信息。这些方法会根据 CSDAC UI 中的指定区域在内部查询服务终端 URL。这些信息记录在 AWS 网站 https://docs.aws.amazon.com/general/latest/gr/ec2-service.html 中。

Dynamic Attributes Connector Azure 访问要求

dynamic attributes connector 会调用内置 SDK 方法获取实例信息。这些方法会在内部调用 https://login.microsoft.com（用于身份验证）和 https://management.azure.com（用于获取实例信息）。