



# 配置 Cisco Secure Dynamic Attributes Connector

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：

- [创建连接器，第 1 页](#)
- [创建适配器，第 8 页](#)
- [创建动态属性过滤器，第 13 页](#)

## 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 vCenter 连接器，第 7 页](#)
- [排除问题 Cisco Secure Dynamic Attributes Connector](#)
- [创建 AWS 连接器，第 1 页](#)
- [创建 Azure 连接器，第 2 页](#)
- [创建 Azure 服务标签连接器，第 3 页](#)
- [创建 Office 365 连接器，第 4 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（），然后单击连接器名称。

- 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 单击测试 (Test) 并确保测试成功后再保存连接器。

步骤 6 单击保存 (Save)。

步骤 7 确保“状态” (Status) 列中显示确定 (OK)。

下一步做什么

[创建适配器，第 8 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 (+)，然后单击连接器名称。
- 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。

值	说明
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 8 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 (+)，然后单击连接器名称。
- 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。

值	说明
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 单击测试 (Test) 并确保在保存连接器之前显示 **Test connection succeeded**。

步骤 6 单击保存 (Save)。

步骤 7 确保“状态”(Status) 列中显示确定 (OK)。

下一步做什么

[创建适配器，第 8 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 (+)，然后单击连接器名称。
- 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。
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 <a href="#">Office 365 IP 地址和 URL Web 服务</a> 。
实例名称	(必需。) 从列表中，单击实例名称。有关详细信息，请参阅 Microsoft 文档站点上的 <a href="#">Office 365 IP 地址和 URL Web 服务</a> 。

值	说明
禁用可选 API	(必需。) 输入 <b>true</b> 或 <b>false</b> 。

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 8 页](#)

## 创建 vCenter 连接器

这些主题讨论如何创建 vCenter 连接器。首先，您可以选择获取证书颁发机构链，这是安全连接到 vCenter 所必需的。

获取证书颁发机构链仅需要 vCenter 主机名；创建连接器需要用户名、密码和其他信息。

相关主题

[创建 vCenter 连接器，第 7 页](#)


## 获取 vCenter 连接器的证书颁发机构 (CA) 链

本主题讨论如何自动获取连接器或适配器的证书颁发机构更改。证书颁发机构链是根证书和所有从属证书；它需要与 vCenter 或 FMC 进行安全连接。

dynamic attributes connector 使您能够自动获取证书颁发机构链，但如果此程序由于某种原因不起作用，请参阅[手动获取证书颁发机构 \(CA\) 链](#)。

步骤 1 登录 Dynamic Attributes Connector。

步骤 2 执行以下任一操作：

- a) 要获取 vCenter CA 链，请单击[连接器](#)。
- b) 要获取 FMC 适配器 CA 链，请单击[适配器](#)。
- c) 请单击添加（）。

步骤 3 在名称字段中，输入名称以标识连接器或适配器。

步骤 4 在主机字段中，输入不含方案的连接器或适配器的主机名或 IP 地址（例如 [https://](#)）。

例如，[myvcenter.example.com](#) 或 [192.0.2.100:9090](#)

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。

无需其他信息即可获取证书 CA 链。

步骤 5 单击 获取。

步骤 6（可选。）展开证书 CA 链中的证书以进行验证。

### 示例

以下是成功获取 vCenter 连接器证书 CA 的示例。

展开对话框顶部的证书 CA 链会显示类似于以下内容的证书。



### 相关主题

[创建 vCenter 连接器](#)，第 7 页

## 创建 vCenter 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 (+)，然后单击连接器名称。
- 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	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。
主机	(必需。) 输入以下任意命令： <ul style="list-style-type: none"> <li>• vCenter 的完全限定主机名</li> <li>• vCenter 的 IP 地址</li> <li>• (可选。) A 端口</li> </ul> <p>请勿输入方案 (例如 <code>https://</code>) 或末尾斜杠。</p> <p>例如, <code>myvcenter.example.com</code> 或 <code>192.0.2.100:9090</code></p>
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	单击 <a href="#">获取</a> 以自动获取证书或，如果无法获取证书，请按照 <a href="#">手动获取证书颁发机构 (CA) 链</a> 中所述手动获取证书。

**步骤 5** 单击测试 (Test) 并确保在保存连接器之前显示 **Test connection succeeded**。

步骤 6 单击保存 (Save)。

下一步做什么

[创建适配器，第 8 页](#)

相关主题

[创建 vCenter 连接器，第 7 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此以用于访问控制策略。

首先，您可以选择获取证书颁发机构链，这是安全连接到 FMC 所必需的。

获取证书颁发机构链仅需要 FMC 主机名；创建适配器需要用户名、密码和其他信息。

相关主题

[如何创建 思科防御协调器 适配器](#)

[为动态属性连接器创建安全防火墙管理器用户，第 8 页](#)

[如何创建 Firewall Management Center 适配器，第 11 页](#)

[获取 vCenter 连接器的证书颁发机构 \(CA\) 链，第 5 页](#)

[排除问题 Cisco Secure Dynamic Attributes Connector](#)

## 为动态属性连接器创建安全防火墙管理器用户

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。



### User Configuration

User Name

Real Name

Authentication  Use External Authentication Method

Password

Confirm Password

Maximum Number of Failed Logins  (0 = Unlimited)

Minimum Password Length

Days Until Password Expiration  (0 = Unlimited)

Days Before Password Expiration Warning

Options

Force Password Reset on Login

Check Password Strength

Exempt from Browser Session Timeout

---

### User Role Configuration

Default User Roles

Administrator

External Database User (Read Only)

Security Analyst

Security Analyst (Read Only)

Security Approver

Intrusion Admin

Access Admin

Network Admin

Maintenance User

Discovery Admin

Threat Intelligence Director (TID) User

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 [如何创建 Firewall Management Center 适配器](#)，第 11 页

#### 相关主题

[如何创建 思科防御协调器 适配器](#)

[为动态属性连接器创建安全防火墙管理器用户](#)，第 8 页

[如何创建 Firewall Management Center 适配器](#)，第 11 页

[获取 vCenter 连接器的证书颁发机构 \(CA\) 链](#)，第 5 页

## 排除问题 Cisco Secure Dynamic Attributes Connector

# 获取 Firewall Management Center 适配器的证书颁发机构 (CA) 链

本主题讨论如何自动获取连接器或适配器的证书颁发机构更改。证书颁发机构链是根证书和所有从属证书；它需要与 vCenter 或 FMC 进行安全连接。

dynamic attributes connector 使您能够自动获取证书颁发机构链，但如果此程序由于某种原因不起作用，请参阅[手动获取证书颁发机构 \(CA\) 链](#)。

---

**步骤 1** 登录 Dynamic Attributes Connector。

**步骤 2** 执行以下任一操作：

- a) 要获取 vCenter CA 链，请单击[连接器](#)。
- b) 要获取 FMC 适配器 CA 链，请单击[适配器](#)。
- c) 请单击添加（**+**）。

**步骤 3** 在 **名称** 字段中，输入名称以标识连接器或适配器。

**步骤 4** 在 **主机** 字段中，输入不含方案的连接器或适配器的主机名或 IP 地址（例如 **https://**）。

例如，**myvcenter.example.com** 或 **192.0.2.100:9090**

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。

无需其他信息即可获得证书 CA 链。

**步骤 5** 单击 **获取**。

**步骤 6** （可选。）展开证书 CA 链中的证书以进行验证。

---

## 示例

以下是成功获取 vCenter 连接器证书 CA 的示例。

**Add FMC Adapter**

Name\* i Certificate chain was successfully fetched. Here are certificate details (priority order descending):  
> firepower - 1 certificate

Descri > firepower - 1 certificate

Domai

IP\* firepower

Port\* 14733

User\* rest

Password\* .....

Secondary IP firepower

Secondary Port 14833

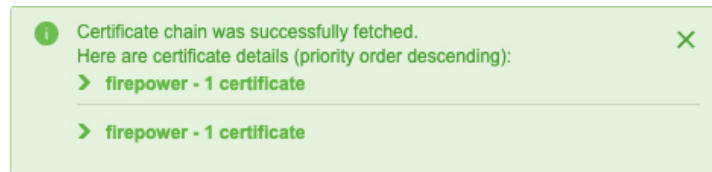
Secondary User

Secondary Password

FMC Server Certificate\* Updated: 3IN CERTIFICATE-----

Test Cancel Save

展开对话框顶部的证书 CA 链会显示类似于以下内容的证书。



#### 相关主题

[如何创建 思科防御协调器 适配器](#)

[为动态属性连接器创建安全防火墙管理器用户](#)，第 8 页

[如何创建 Firewall Management Center 适配器](#)，第 11 页

[获取 vCenter 连接器的证书颁发机构 \(CA\) 链](#)，第 5 页

[排除问题 Cisco Secure Dynamic Attributes Connector](#)

## 如何创建 Firewall Management Center 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[为动态属性连接器创建安全防火墙管理器用户](#)，第 8 页。

步骤 1 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 现场 Firepower Management Center Virtual 域。将字段留空以便在全局域中创建动态对象。 例如, <b>Global/MySubdomain</b>
IP	(必需。) 输入您的 现场 Firepower Management Center Virtual 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 现场 Firepower Management Center Virtual 使用的 TLS 端口。
用户	(必需。) 输入至少具有网络管理员角色的 现场 Firepower Management Center Virtual 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 现场 Firepower Management Center Virtual 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 现场 Firepower Management Center Virtual 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 现场 Firepower Management Center Virtual 用户的名称。
辅助密码	(仅限高可用性。) 输入用户的密码。
<b>FMC 服务器证书 (FMC Server Certificate)</b>	单击获取以自动获取证书或, 如果无法获取证书, 请按照 <a href="#">手动获取证书颁发机构(CA)链</a> 中所述手动获取证书。

步骤 5 单击测试 (Test) 并确保测试成功后再保存适配器。

步骤 6 单击保存 (Save)。

#### 相关主题

- [如何创建 思科防御协调器 适配器](#)
- [为动态属性连接器创建安全防火墙管理器用户](#)，第 8 页
- [如何创建 Firewall Management Center 适配器](#)，第 11 页
- [获取 vCenter 连接器的证书颁发机构 \(CA\) 链](#)，第 5 页
- [排除问题 Cisco Secure Dynamic Attributes Connector](#)

## 创建动态属性过滤器

使用 Cisco 安全动态属性连接器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对象。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](#)。

#### 开始之前

完成以下所有任务：

- [安装必备软件](#)
- [创建连接器](#)，第 1 页
- [创建适配器](#)，第 8 页

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 4 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。
查询	<ul style="list-style-type: none"> <li>• 添加新过滤器：单击添加（）。</li> <li>• 编辑或删除过滤器：单击更多（），然后单击行末尾的编辑（<b>Edit</b>）或删除（<b>Delete</b>）。</li> <li>• 添加新过滤器：单击添加图标（）</li> <li>• 编辑过滤器：单击编辑图标（ <b>Edit</b>）</li> <li>• 删除过滤器：单击删除图标（ <b>Delete</b>）</li> </ul>

**步骤 5** 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： <ul style="list-style-type: none"> <li>• <b>等于 (Equals)</b> 会将密钥与值完全匹配。</li> <li>• <b>包含 (Contains)</b> 会将键与值匹配（如果值的任何部分匹配）。</li> </ul>
值	单击任意 ( <b>Any</b> ) 或全部 ( <b>All</b> )，然后单击列表中的一个或多个值。单击添加其他值 ( <b>Add another value</b> ) 以便向查询中添加值。

**步骤 6** 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 7** 完成后，单击保存 (**Save**)。

**步骤 8** （可选。）验证 FMC 中的动态对象。

- 至少要具有网络管理员角色的用户身份登录 FMC。
- 单击对象 (**Objects**) > 对象管理器 (**Object Manager**)。
- 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 15 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。

#### Edit Dynamic Attribute Filter

Name\*  Connector\*

Query\* +

Type	Op.	Value
<input type="radio"/> all network	eq	<input type="radio"/> any myVLAN

[> Show Preview](#)

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。

#### Add Dynamic Attribute Filter

Name\*  Connector\*

Query\* +

Type	Op.	Value
<input type="radio"/> all host	eq	<input type="radio"/> any host-2868
		host-2869
		host-3780

[> Show Preview](#)

### 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。

#### Add Dynamic Attribute Filter

Name\*  Connector\*

Query\* +

Type	Op.	Value
<input type="radio"/> all Finance	eq	<input type="radio"/> any App

[> Show Preview](#)

**示例: AWS**

以下示例显示了一个条件: 值为 1 的 FinanceApp。

Add Dynamic Attribute Filter

Name\*  Connector\*

Query\*

Type	Op.	Value
<input type="text" value="all"/> FinanceApp	eq	<input type="text" value="any"/> 1

[> Show Preview](#)