Cisco Secure Dynamic Attributes Connector

以下主题讨论如何配置和使用Cisco Secure Dynamic Attributes Connector。

关于 Cisco Secure Dynamic Attributes Connector

Cisco Secure Dynamic Attributes Connector 让您能够在 Cisco Secure Firewall Management Center (CDO) 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。

支持的连接器

我们目前支持：

表 *1:* 按 *Cisco Secure Dynamic Attributes Connector* 版本和平台列出的受支持连接器列表

CSDAC 版本/平台	AWS	修饰器	GitHub	Google Cloud	Azure	Azure 服务标签	ISE	LDAP	Microsoft Office 365	VMware vCenter
版本 1.1（本地）	是	否	不支持	不支持	是	是	否	不支持	是	是
版本 2.0（本地）	是	不支持	是	是	是	是	否	不支持	是	是
云交付 (思科防御协调器)	是	不支持	是	是	是	是	否	不支持	是	否

有关连接器的详细信息：

- Amazon Web Services (AWS)

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

- GitHub
- Google Cloud

  有关详细信息，请参阅 Google 云文档中的设置环境。

- Microsoft Azure

  有关详情，请参阅 Azure 文档网站上的本页面。

- 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。

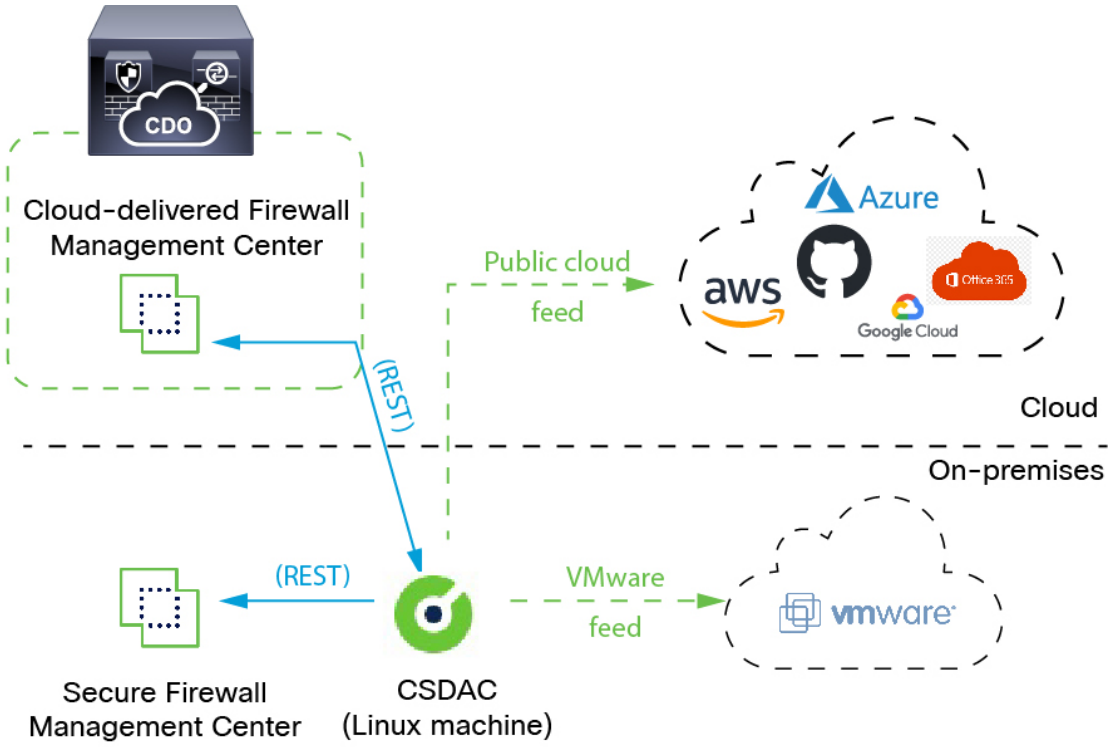
- Office 365

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

工作原理

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。

下图显示了系统的总体运行情况。



1. 连接器包含要查询的标签和容器。

   例如，这些标签通常会定义动态分配的网络和 IP 地址，您无法为其创建访问控制规则。来自连接器的持续源存储在 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 AWS 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动态属性过滤器。

3. dynamic attributes connector 定义的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。

   您可以创建以下类型的适配器：

   - 本地设备的 本地防火墙管理中心。

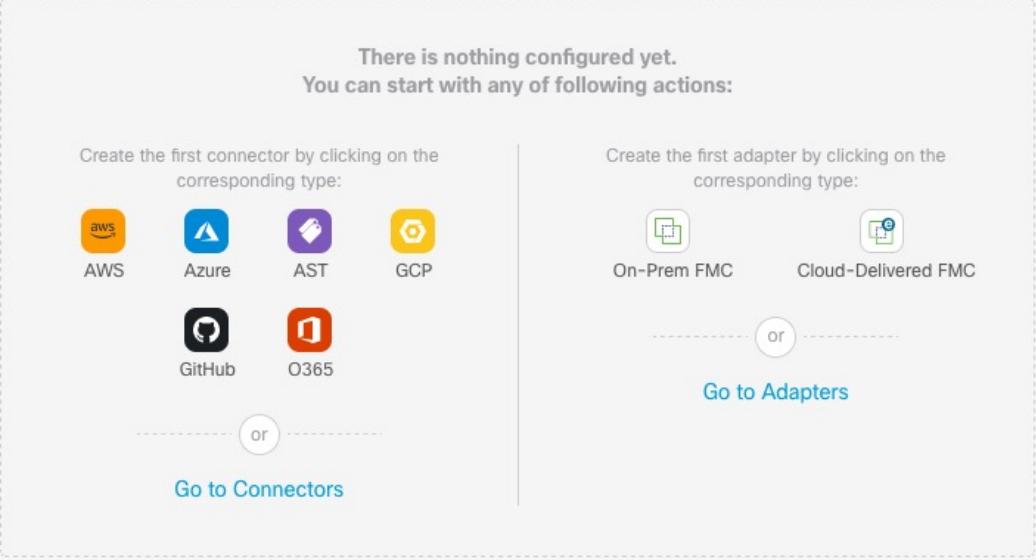
     此类 设备可能由 思科防御协调器 (CDO) 管理，或者它也可能是独立设备。

   - 云交付的防火墙管理中心 适用于 CDO 管理的设备。

关于控制面板

要访问 Cisco Secure Dynamic Attributes Connector 控制面板，请登录 CDO 并点击页面顶部的 **工具和服务 (Tools & Services)** > **动态属性连接 (Dynamic Attributes Connector)** > **控制面板 (Dashboard)**。

Cisco Secure Dynamic Attributes Connector 控制面板页面会显示连接器、适配器和过滤器的状态。以下是未配置系统的控制面板示例：



您可以通过控制面板来执行的操作包括：

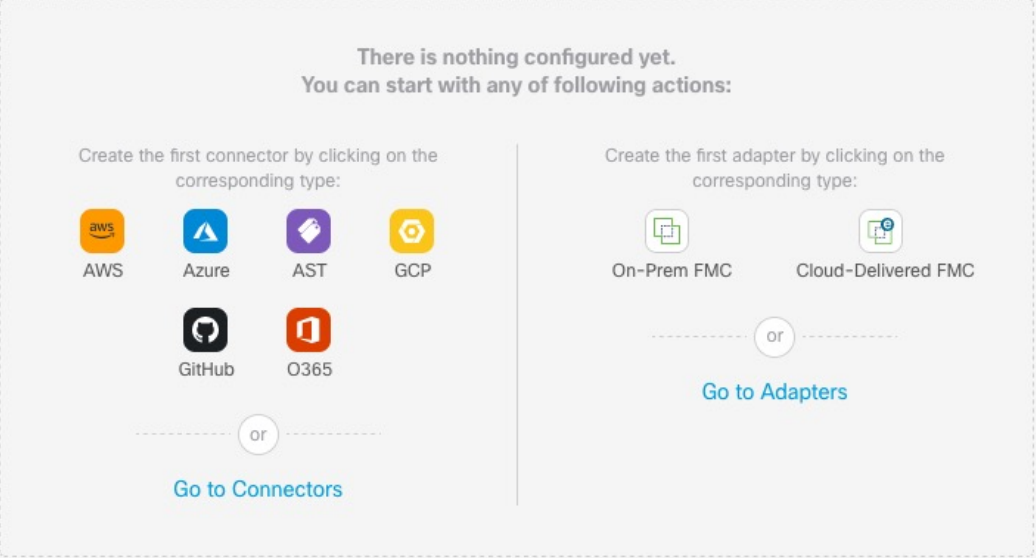
- 添加、编辑和删除连接器、动态属性过滤器和适配器。
- 了解连接器、动态属性过滤器和适配器之间的关系。
- 查看警告和错误。

相关主题

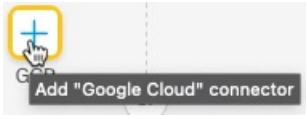
- 未配置系统的控制面板， 第 4 页
- 已配置系统的控制面板， 第 5 页
- 添加、编辑或删除连接器， 第 7 页
- 添加、编辑或删除动态属性过滤器， 第 8 页
- 添加、编辑或删除适配器， 第 10 页

未配置系统的控制面板

未配置系统的 Cisco Secure Dynamic Attributes Connector 控制面板页面示例：



控制面板最初显示您可以为系统配置的所有类型的连接器和适配器。您可以执行以下任何操作：

- 将鼠标指针悬停在连接器或适配器上，然后点击 

新建一个。
- 点击**转到连接器 (Go to Connectors)** 以添加、编辑或删除连接器（适用于同时创建、编辑或删除多个连接器）。

  有关详细信息，请参阅创建连接器，第 11 页。
- 点击**转到适配器 (Go to Adapters)** 以添加、编辑或删除适配器（适用于同时创建、编辑或删除多个适配器）。

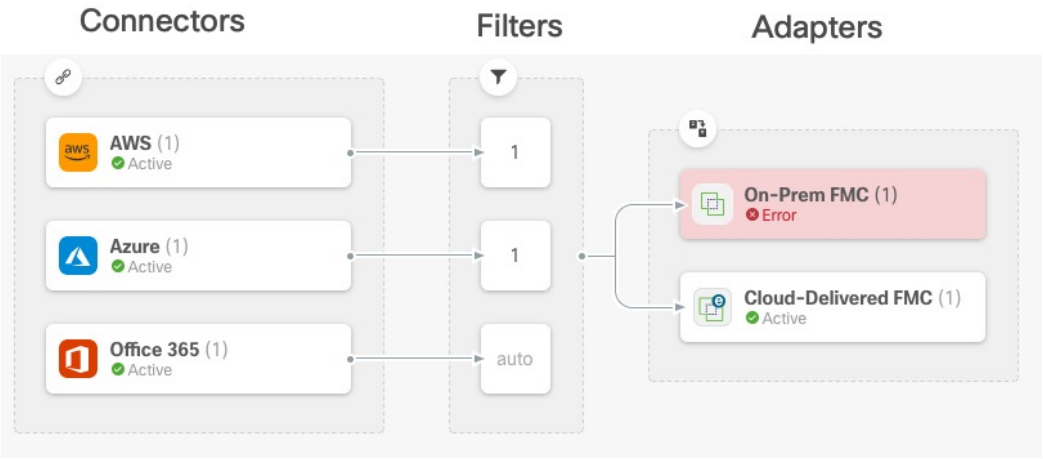
  有关详细信息，请参阅创建适配器，第 23 页。

相关主题

- 已配置系统的控制面板，第 5 页
- 添加、编辑或删除连接器，第 7 页
- 添加、编辑或删除动态属性过滤器，第 8 页
- 添加、编辑或删除适配器，第 10 页

已配置系统的控制面板

已配置系统的 Cisco Secure Dynamic Attributes Connector 控制面板页面示例：



控制面板显示以下内容（从左到右）：

“连接器”(Connectors) 列	“过滤器”(Filters) 列	“适配器”(Adapters) 列
连接器列表，其中包含指示每种类型的配置数量的编号。连接器会收集可以发送到已配置适配器的动态属性。动态属性过滤器会指定要发送的数据。 点击 以查看有关所有已配置连接器的详细信息。您还可以点击连接器的名称来添加、编辑或删除连接器；或者查看有关它们的详细信息。有关详细信息，请参阅添加、编辑或删除连接器，第 7 页。	与每个连接器关联的动态属性过滤器列表，其中带有一个数字，表示每个过滤器与连接器关联的数量。 点击 以查看有关所有已配置过滤器的详细信息。您还可以点击过滤器的名称来添加、编辑或删除过滤器；或者查看有关它们的详细信息。有关详细信息，请参阅添加、编辑或删除动态属性过滤器，第 8 页。	适配器列表。适配器会使用已配置的动态属性过滤器从已配置的连接器接收动态对象；这些动态对象可用于访问控制策略，而无需部署它们。 点击 以查看有关所有已配置适配器的详细信息。您还可以点击适配器的名称来添加、编辑或删除适配器；或者查看有关它们的详细信息。有关详细信息，请参阅添加、编辑或删除适配器，第 10 页。

注释 某些连接器（例如 Outlook 365 和 Azure 服务标记）会自动提取可用的动态对象，而无需使用动态属性过滤器。这些连接器在 列中显示为**自动 (Auto)**。

控制面板会指明对象是否可用。控制面板页面会每 15 秒刷新一次，但您可以随时点击页面顶部的**刷新**（ ）来立即刷新。如果问题仍然存在，请检查网络连接。

相关主题

- 添加、编辑或删除连接器，第 7 页
- 添加、编辑或删除动态属性过滤器，第 8 页
- 添加、编辑或删除适配器，第 10 页

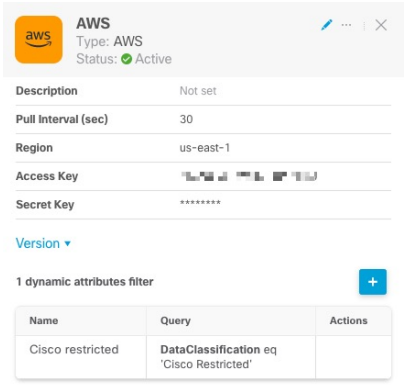
添加、编辑或删除连接器

通过控制面板，您可以查看或编辑连接器。您可以点击连接器的名称以查看该连接器的所有实例，

也可以点击  以查看以下其他选项：

- **转到连接器**可同时查看所有连接器；您可以在此处添加、编辑和删除连接器。
- **添加连接器 (Add Connector)** > **类型**以添加指定类型的连接器。

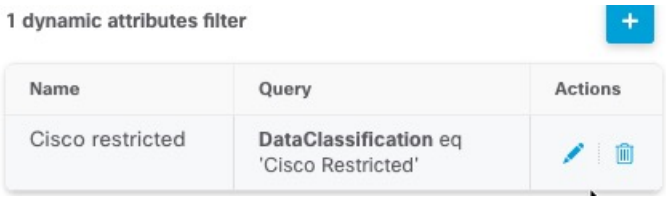
点击连接器列 () 中的任意连接器可显示更多相关信息；示例如下：



您有以下选择：

- 点击 编辑图标 （ ） 以编辑此连接器。
- 点击 更多图标 （ ） 以查看其他选项。
- 点击 关闭面板。
- 点击**版本 (Version)** 以显示 dynamic attributes connector 的版本。如果思科 TAC 需要，您可以选择将版本复制到剪贴板。

通过面板底部的表格，您可以添加动态属性过滤器；或编辑或删除连接器。示例如下：



点击添加图标（ ）以便为此连接器添加动态属性过滤器。有关详细信息，请参阅创建动态属性过滤器，第 25 页。

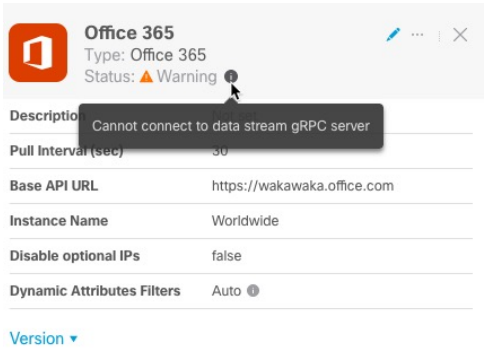
将鼠标指针悬停在“操作”(Actions) 列上，以编辑或删除指示的连接器。

查看错误信息

要查看连接器的错误信息，请执行以下操作：

1. 在控制面板上，点击显示错误的连接器的名称。
2. 在右侧窗格中，点击 **信息** （ ）。

   示例如下。



3. 要解决此问题，请按照创建 Office 365 连接器， 第 22 页中所述编辑连接器设置。
4. 如果您无法解决问题，请点击**版本 (Version)** 并将版本复制到文本文件。
5. 获取 CDO 租户 ID，如中所述 获取租户 ID， 第 30 页
6. 向思科 TAC 提供所有这些信息。https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

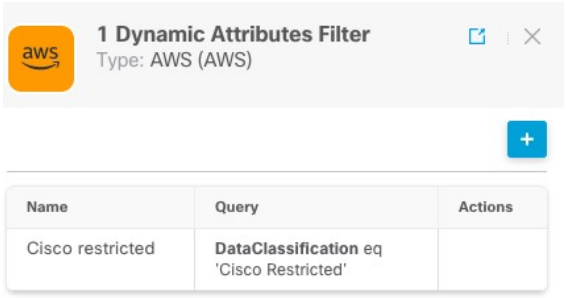
添加、编辑或删除动态属性过滤器

控制面板让您能够添加、编辑或删除动态属性过滤器。您可以点击过滤器的名称以查看该过滤器的所有实例，也可以点击 以查看下列附加选项：

- **转至动态属性过滤器**以查看所有已配置的动态属性过滤器。您可以在此处添加、编辑或删除动态属性过滤器。
- **添加动态属性过滤器**以添加过滤器。

有关添加动态属性过滤器的详细信息，请参阅创建动态属性过滤器， 第 25 页。

点击过滤器列 ( ) 中的任何适配器以显示有关它的详细信息；如下所示：



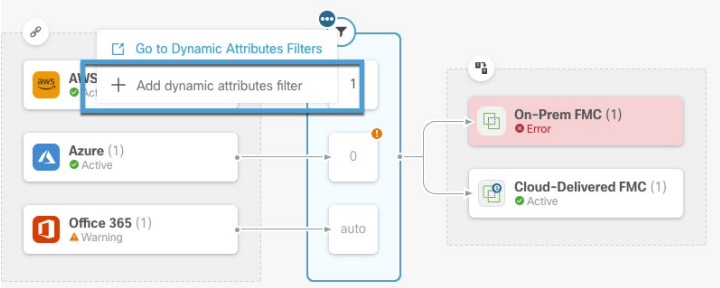
注释 某些连接器（例如 Outlook 365 和 Azure 服务标记）会自动提取可用的动态对象，而无需使用动态属性过滤器。这些连接器在 列中显示为**自动 (Auto)**。

您有以下选择：

- 点击过滤器实例可查看与连接器关联的动态属性过滤器的摘要信息。
- 点击 添加图标 （ ） 以添加新的动态属性过滤器。

  有关详细信息，请参阅创建动态属性过滤器，第 25 页。
- 在表示指明的连接器没有关联的动态属性过滤器的过滤器列 ( ) 中点击 。如果没有关联的过滤器，连接器将无法向 管理中心 发送任何内容。

  解决此问题的一种方法是点击过滤器列中的 ，然后点击**添加动态属性过滤器 (Add Dynamic Attributes Filter)**。示例如下。



- 点击 以添加、编辑或删除过滤器。
- 点击 关闭面板。

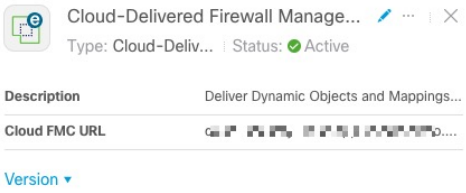
添加、编辑或删除适配器

通过控制面板，您可以查看或编辑适配器。您可以点击适配器的名称以查看该适配器的所有实例，

也可以点击 以查看以下其他选项：

- **转到适配器**以同时查看所有适配器；您可以在此处添加、编辑和删除适配器。
- **添加适配器 (Add Adapter)** > **类型**以添加指定类型的适配器。

点击适配器列 ( ) 中的任何适配器以显示有关它的详细信息；如下所示：



您有以下选择：

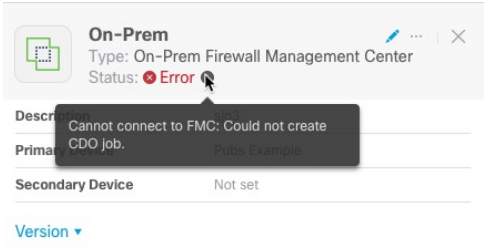
- 点击 编辑图标 （ ） 以编辑此连接器。
- 点击 更多图标 （ ） 以查看其他选项。
- 点击**版本 (Version)** 以显示 dynamic attributes connector 的版本。如果思科 TAC 需要，您可以选择将版本复制到剪贴板。
- 点击 以添加、编辑或删除适配器。您还可以在生成的页面上查看错误详细信息。
- 点击 关闭面板。

查看错误信息

要查看适配器的错误信息，请执行以下操作：

1. 在控制面板上，点击显示了错误的适配器的名称。
2. 在右侧窗格中，点击 **信息** （ ）。

   示例如下。



3. 要解决此错误，请确保 本地防火墙管理中心 已正确载入。有关详细信息，请参阅使用思科防御协调器管理 *FMC* 中的载入 FMC（主题链接）。
4. 如果您无法解决问题，请点击**版本 (Version)** 并将版本复制到文本文件。
5. 获取 CDO 租户 ID，如中所述 获取租户 ID，第 30 页
6. 向思科 TAC 提供所有这些信息。https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

相关主题

- 创建适配器，第 23 页

创建连接器

连接器是云服务的接口。连接器从云服务检索网络信息，以便网络信息可用于CDO上的访问控制策略。

我们支持以下内容：

表 *2:* 按 ***Cisco Secure Dynamic Attributes Connector*** 版本和平台列出的受支持连接器列表

CSDAC 版本/平台	AWS	修饰器	GitHub	Google Cloud	Azure	Azure 服务标签	ISE	LDAP	Microsoft Office 365	VMware vCenter
版本 1.1（本地）	是	否	不支持	不支持	是	是	否	不支持	是	是
版本 2.0（本地）	是	不支持	是	是	是	是	否	不支持	是	是
云交付 (思科防御协调器)	是	不支持	是	是	是	是	否	不支持	是	否

有关详细信息，请参阅以下各节之一：

Amazon Web 服务连接器 - 关于用户权限和导入的数据

Cisco Secure Dynamic Attributes Connector 会将动态属性从 AWS 导入 CDO，以便用于访问控制策略。

动态属性已导入

我们从 AWS 导入以下动态属性：

- 标签，可用于组织 AWS EC2 资源的用户定义的键值对。

  有关更多信息，请参阅 AWS 文档中的标记 EC2 资源

- AWS 中虚拟机的 *IP* 地址。

所需的最低权限

Cisco Secure Dynamic Attributes Connector 要求用户至少具有允许 `ec2:DescribeTags` 和 `ec2:DescribeInstances` 以便能够导入动态属性的策略。

创建对 Cisco Secure Dynamic Attributes Connector 具有最小权限的 AWS 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 CDO 发送动态属性。有关这些属性的列表，请参阅 Amazon Web 服务连接器 - 关于用户权限和导入的数据，第 11 页。

开始之前

您必须已设置 Amazon Web 服务 (AWS) 帐户。有关执行此操作的更多信息，请参阅 AWS 文档中的此文章。

过程

步骤 1 以具有网络管理员角色的用户身份登录 AWS 控制台。

步骤 2 在控制面板中，点击**安全、身份和合规性 (Security, Identity & Compliance)** > **IAM**。

步骤 3 点击**访问管理 (Access Management)** > **用户 (Users)**。

步骤 4 点击**添加用户 (Add Users)**。

步骤 5 在**用户名 (User Name)** 字段中，输入用于标识用户的名称。

步骤 6 点击**访问密钥 - 编程访问 (Access Key - Programmatic Access)**。

步骤 7 在“设置权限”(Set permissions) 页面中，点击**下一步 (Next)** 而不授予用户任何访问权限；稍后执行此操作。

步骤 8 如果需要，向用户添加标签。

步骤 9 点击**创建用户**。

步骤 10 点击 **Download.csv**，将用户的密钥下载到计算机。

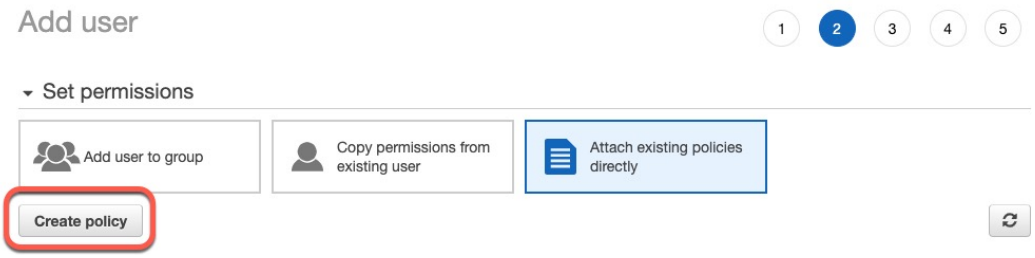
注释 这是您检索用户密钥的唯一机会。

步骤 11 点击**关闭 (Close)**。

步骤 12 在身份和访问管理 (IAM) 页面的左侧列中，点击**访问管理 (Access Management)** > **策略 (Policies)**。

步骤 13 点击**创建策略**。

步骤 14 在“创建策略”(Create Policy) 页面中，点击 **JSON**。



步骤 15 在字段中输入以下策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeTags",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

步骤 16 点击**下一步 (Next)**。

步骤 17 点击**审核 (Review)**。

步骤 18 在“查看策略”(Review Policy) 页面中输入请求的信息，然后点击**创建策略 (Create Policy)**。

步骤 19 在“策略”(Policies) 页面上，在搜索字段中输入全部或部分策略名称，然后按 Enter 键。

步骤 20 点击您刚刚创建的策略。

步骤 21 点击**操作 (Actions)** > **附加 (Attach)**。

步骤 22 如有必要，请在搜索字段中输入全部或部分用户名，然后按 Enter 键。

步骤 23 点击**附加策略 (Attach Policy)**。

下一步做什么

创建 AWS 连接器，第 13 页。

创建 AWS 连接器

此任务讨论如何配置将数据从 AWS 发送到 CDO 以用于访问控制策略的连接器。

开始之前

创建至少具有创建对 Cisco Secure Dynamic Attributes Connector 具有最小权限的 AWS 用户，第 12 页中所述权限的用户。

过程

步骤 1 登录CDO。

步骤 2 请点击 工具和服务 (Tools & Services) > 动态属性连接器 (Dynamic Attributes Connector) > 连接器 (Connectors)。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑连接器：点击编辑图标 （  ）。
- 编辑连接器：点击删除图标 （  ）。

步骤 4 输入以下信息。

值	说明
Name	（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 点击测试 **(Test)** 并确保测试成功后再保存连接器。

步骤 6 点击保存 **(Save)**。

步骤 7 确保“状态”(Status) 列中显示确定 **(OK)**。

Azure 连接器 - 关于用户权限和导入的数据

Cisco Secure Dynamic Attributes Connector 会将动态属性从 Azure 导入 CDO，以便用于访问控制策略。

动态属性已导入

我们从 Azure 导入以下动态属性：

- 标签，与资源、资源组和订用关联的键值对。

有关详情，请参阅 Microsoft 文档中的本页面。

- Azure 中虚拟机的 *IP* 地址。

所需的最低权限

Cisco Secure Dynamic Attributes Connector 要求至少具有**读者 (Reader)** 权限的用户才能导入动态属性。

创建对 Cisco Secure Dynamic Attributes Connector 具有最小权限的 Azure 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 CDO 发送动态属性。有关这些属性的列表，请参阅 Azure 连接器 - 关于用户权限和导入的数据， 第 14 页。

开始之前

您必须已经拥有 Microsoft Azure 帐户。要进行设置，请参阅 Azure 文档站点上的本页面。

过程

步骤 1 以订用所有者的身份登录到 Azure 门户。

步骤 2 点击 **Azure Active Directory**。

步骤 3 查找要设置的应用的 Azure Active Directory 实例。

步骤 4 点击**添加 (Add)** > **应用注册 (App registration)**。

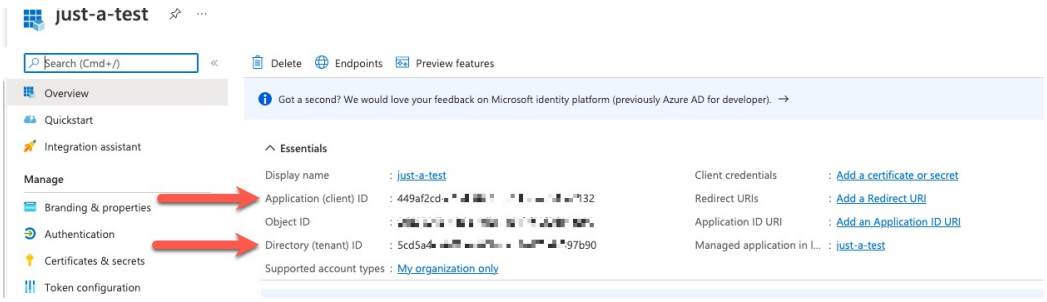
步骤 5 在 **名称 (Name)** 字段中，输入用于标识此应用的名称。

步骤 6 在此页面上输入贵组织所要求的其他信息。

步骤 7 点击**注册 (Register)**。

步骤 8 在下一页上，记录下客户端 ID（也称为应用 *ID*）和租户 ID（也称为目录 *ID*）。

示例如下。



步骤 9 点击**添加证书或密钥 (Add a certificate or secret)**。

步骤 10 点击**新建客户端密钥 (New Client Secret)**。

步骤 11 输入请求的信息，然后点击**添加 (Add)**。

步骤 12 将客户端**值**复制到剪贴板，因为您需要它来设置 Azure 连接器。

步骤 13 返回到 Azure 门户主页面，然后点击**订用 (Subscriptions)**。

步骤 14 将订用 ID 复制到剪贴板。

步骤 15 在订用页面上，点击订用的名称。

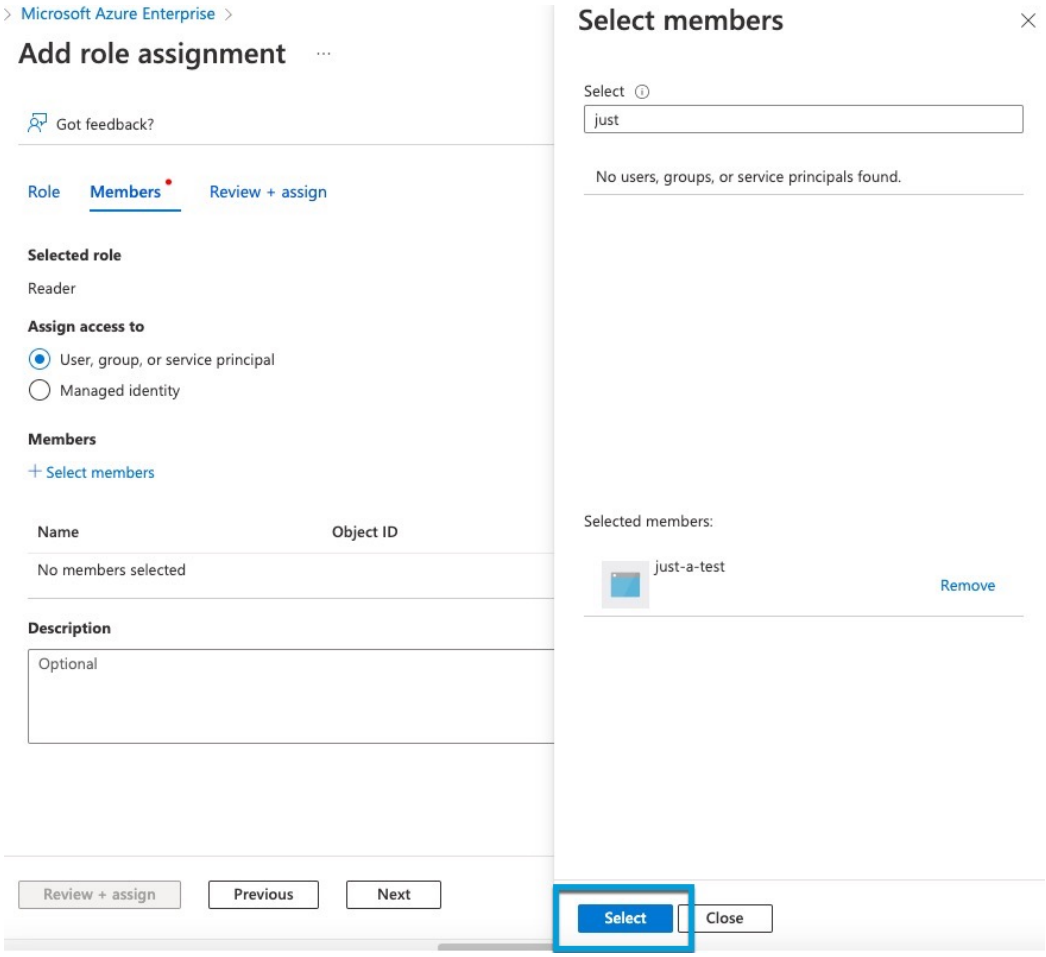
步骤 16 点击**访问控制 (IAM) (Access Control [IAM])**。

步骤 17 点击**添加 (Add)** > **添加角色分配 (Add role assignment)**。

步骤 18 点击**读者 (Reader)**，然后点击**下一步 (Next)**。

步骤 19 点击**选择成员 (Select Members)**。

步骤 20 在页面右侧，点击您注册的应用的名称，然后点击**选择 (Select)**。



步骤 21 点击**查看 + 分配 (Review + Assign)**，然后按照提示完成操作。

下一步做什么

请参阅创建 Azure 连接器，第 17 页。

创建 Azure 连接器

此任务讨论如何创建从 Azure 向 CDO 发送数据的连接器，以用于访问控制策略中。

开始之前

创建至少具有 创建对 Cisco Secure Dynamic Attributes Connector 具有最小权限的 Azure 用户，第 15 页 中所述权限的 Azure 用户。

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑连接器：点击编辑图标 （  ）。
- 编辑连接器：点击删除图标 （  ）。

步骤 4 输入以下信息。

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

步骤 6 点击**保存 (Save)**。

步骤 7 确保“状态”(Status) 列中显示**确定 (OK)**。

创建 Azure 服务标签连接器

本主题讨论了如何为 Azure 服务标签创建到 CDO 的连接器，以供在访问控制策略中使用。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。

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （ ），然后点击连接器名称。
- 编辑连接器：点击编辑图标 （ Edit ）。
- 编辑连接器：点击删除图标 （ Delete ）。

步骤 4 输入以下信息。

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

步骤 6 点击**保存 (Save)**。

步骤 7 确保“状态”(Status) 列中显示**确定 (OK)**。

创建 GitHub 连接器

此部分讨论如何创建将数据发送到 CDO 以用于访问控制策略的 GitHub 连接器。与这些标签关联的 IP 地址由 GitHub 进行维护。您不必创建动态属性过滤器。

有关详细信息，请参阅关于 GitHub 的 IP 地址。

注释 请勿更改 URL，否则将无法检索任何 IP 地址。

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （）， 然后点击连接器名称。
- 编辑连接器：点击编辑图标 （Edit）。
- 编辑连接器：点击删除图标 （Delete）。

步骤 4 输入**名称**和可选说明。

步骤 5 （可选。）在**提取间隔 (Pull Interval)** 字段中，更改动态属性连接器从 GitHub 检索 IP 地址的频率（以秒为单位）。默认值为 21,600 秒（6 小时）。

步骤 6 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 7 点击**保存 (Save)**。

步骤 8 确保“状态”(Status) 列中显示**确定 (OK)**。

Google 云连接器 - 关于用户权限和导入的数据

Cisco Secure Dynamic Attributes Connector 会将动态属性从 Google 云导入 CDO，以便用于访问控制策略。

动态属性已导入

我们会从 Google 云导入以下动态属性：

- 标签，可用于组织 Google 云资源的键值对。

  有关详细信息，请参阅 Google 云文档中的创建和管理标签。

- 网络标记，与组织、文件夹或项目关联的键值对。

有关详细信息，请参阅 Google 云文档中的创建和管理标签。

- Google 云中虚拟机的 *IP* 地址。

所需的最低权限

Cisco Secure Dynamic Attributes Connector 要求至少具有**基本** > **查看者**权限的用户才能导入动态属性。

创建对 Cisco Secure Dynamic Attributes Connector 具有最小权限的 Google 云用户

此任务讨论如何设置具有最低权限的服务帐户，以向 CDO 发送动态属性。有关这些属性的列表，请参阅 Google 云连接器 - 关于用户权限和导入的数据 ， 第 19 页。

开始之前

您必须已设置 Google 云帐户。有关执行此操作的详细信息，请参阅 Google 云文档中的设置环境。

过程

步骤 1 以所有者角色的用户身份登录您的 Google 云帐户。

步骤 2 点击**IAM 和管理 (IAM & Admin)** > **服务帐户 (Service Accounts)** > **创建服务帐户 (Create Service Account)**。

步骤 3 输入以下信息：

- **服务帐户名称**：用于标识此帐户的名称；例如，**CSDAC**。
- **服务帐户 ID**：应在您输入服务帐户名称后填写唯一值。
- **服务帐户说明**：输入可选说明。

有关服务帐户的详细信息，请参阅 Google 云文档中的了解服务帐户。

步骤 4 点击**创建并继续 (Create and Continue)**。

步骤 5 按照屏幕上的提示操作，直到显示“授予用户对此服务帐户的访问权限”部分。

步骤 6 授予用户**基本** > **查看者**角色。

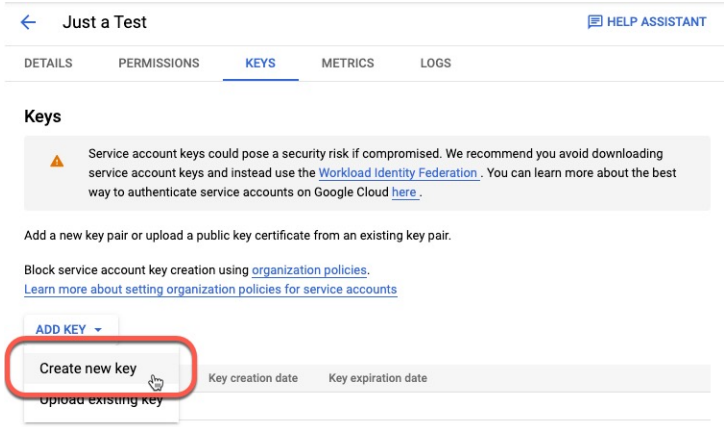
步骤 7 点击**完成 (Done)**。

系统将显示服务帐户列表。

步骤 8 点击您所创建的服务帐户一行末尾的 **更多**（⋮）。

步骤 9 点击**管理密钥 (Manage Keys)**。

步骤 10 点击**添加密钥 (Add Key)** > **创建新密钥 (Create New Key)**。



步骤 11 点击 **JSON**。

步骤 12 点击**创建 (Create)**。

JSON 密钥将下载到您的计算机。

步骤 13 配置 GCP 连接器时，请将密钥放在手边。

下一步做什么

请参阅创建 Google 云连接器，第 21 页。

创建 Google 云连接器

开始之前

准备好 Google 云 JSON 格式的服务帐户数据；它是设置连接器所必需的。

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （）， 然后点击连接器名称。
- 编辑连接器：点击编辑图标 （Edit）。
- 编辑连接器：点击删除图标 （Delete）。

步骤 4 输入以下信息。

值	说明
Name	（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。
GCP 区域	（必需。）输入您的 Google 云所在的 GCP 区域。有关详细信息，请参阅 Google 云文档中的区域和地区。
服务帐户	粘贴 Google 云服务帐户的 JSON 代码。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存 (Save)**。

步骤 7 确保“状态”(Status) 列中显示**确定 (OK)**。

创建 Office 365 连接器

此任务讨论如何为 Office 365 标记创建连接器，从而将数据发送到 CDO 以便用于访问控制策略。Microsoft 会每周更新与这些标记的 IP 地址关联。您不必创建动态属性过滤器即可使用数据。

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

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （ ），然后点击连接器名称。
- 编辑连接器：点击编辑图标 （ Edit ）。
- 编辑连接器：点击删除图标 （ Delete ）。

步骤 4 输入以下信息。

值	说明
Name	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。

值	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 Office 365 IP 地址和 URL Web 服务。
实例名称	（必需。）从列表中，点击实例名称。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 IP	（必需。）输入 **true** 或 **false**。

步骤 5 点击**保存 (Save)**。

步骤 6 确保“状态”(Status) 列中显示**确定 (OK)**。

创建适配器

适配器 是与 CDO 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。

您可以创建以下适配器：

- 本地防火墙管理中心 适用于现场 管理中心 设备。
- 云交付的防火墙管理中心 适用于 CDO 管理的设备。

注释 您必须具有**超级管理员**用户角色才能创建第一个 云交付的防火墙管理中心 适配器。要查看或修改现有适配器，您必须拥有管理员或超级管理员用户角色。

如何创建 本地防火墙管理中心 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 CDO 到。

开始之前

按照使用思科防御协调器来管理安全和网络设备联机帮助中的载入管理中心中所述，将防火墙管理器载入思科防御协调器。

所需的用户角色：

- 超级管理员

过程

步骤 1 登录 CDO。

步骤 2 请点击 **工具和服务** > **动态属性连接器** > **适配器**。

步骤 3 要添加适配器，请点击 添加图标 （ ） > 本地防火墙管理中心。

步骤 4 要编辑或删除适配器，请点击编辑图标 （ Edit ） 或 删除图标 （ Delete ）。

步骤 5 添加或编辑以下信息。

值	说明
Name	（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。
主设备	在列表中点击与您的租户关联的管理中心的 IP 地址。
辅助设备	（可选。）如果您有辅助 本地防火墙管理中心，请在列表中点击其名称。

步骤 6 点击**确定 (OK)**。

如何创建 云交付的防火墙管理中心 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 CDO 到。

开始之前

所需的用户角色：

- 超级管理员

过程

步骤 1 以具有超级管理员角色的用户身份登录 CDO。

步骤 2 请点击 **工具和服务** > **动态属性连接器** > **适配器**。

步骤 3 要添加适配器，请点击 添加图标 （ ） > 云交付的防火墙管理中心。

步骤 4 要编辑或删除适配器，请点击编辑图标 （ Edit ） 或 删除图标 （ Delete ）。

步骤 5 编辑以下信息。

值	说明
Name	（必需。）输入可标识适配器的唯一名称。

值	说明
说明	适配器的可选说明。
云 FMC URL	从列表中，点击您的 云交付的防火墙管理中心 的URL。

步骤 6 点击**测试 (Test)** 并确保测试成功后再保存适配器。

步骤 7 点击**保存 (Save)**。

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 CDO 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 您不能为 GitHub、Office 365 或 Azure Service Tags 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 28 页。

开始之前

完成以下所有任务：

- 创建连接器，第 11 页

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **动态属性过滤器 (Dynamic Attributes Filters)**。

步骤 3 执行以下任一操作：

- 添加新过滤器：点击添加图标 （ ）
- 编辑过滤器：点击编辑图标 （ Edit ）
- 删除过滤器：点击删除图标 （ 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 CDO 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	在列表中点击要使用的连接器的名称。
查询	• 添加新过滤器：点击添加图标 （） • 编辑过滤器：点击编辑图标 （） • 删除过滤器：点击删除图标 （）

步骤 5 要添加或编辑查询，请输入以下信息。

项目	说明
密钥	点击列表中的一个键。密钥会从连接器获取。
操作	点击以下选项之一： • **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	点击**任意 (Any)** 或**全部 (All)**，然后点击列表中的一个或多个值。点击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 6 点击**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，点击**保存 (Save)**。

步骤 8 （可选。）验证 CDO 中的动态对象。

a) 登录 CDO。

b) 请点击 **策略 (策略)** > **FTD 策略 (FTD Policies)**。

c) 点击**对象 (Objects)** > **对象管理器 (Object Manager)**。

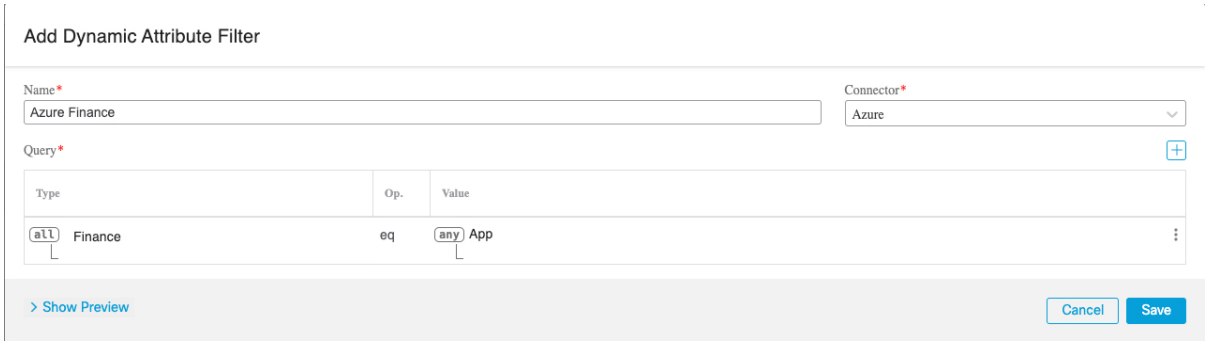
d) 在左侧窗格中，点击**外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。
您创建的动态属性查询应显示为动态对象。

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。

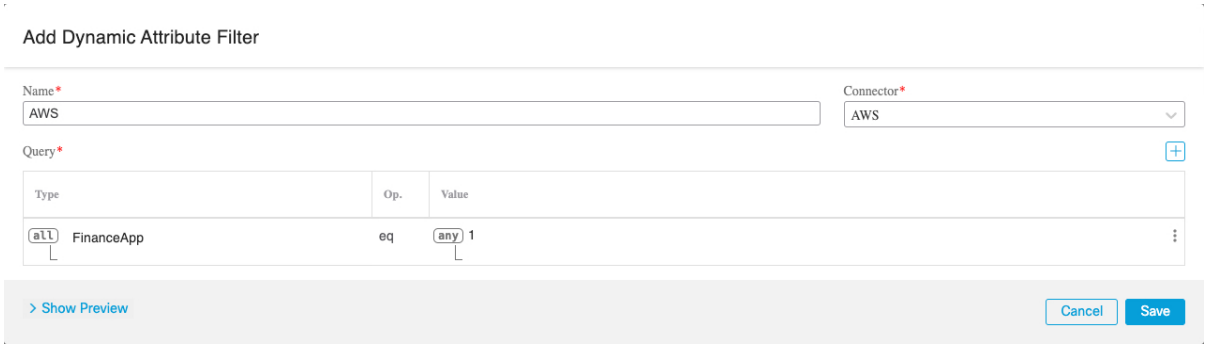
示例：Azure

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。



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 CDO 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 本地防火墙管理中心 或 云交付的防火墙管理中心 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。

注释 您不能为 GitHub、Office 365 或 Azure Service Tags 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。

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 25 页中所述。

注释 您不能为 GitHub、Office 365 或 Azure Service Tags 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。

过程

步骤 1 登录CDO。

步骤 2 请点击 **策略 (策略)** > **FTD 策略 (FTD Policies)**。

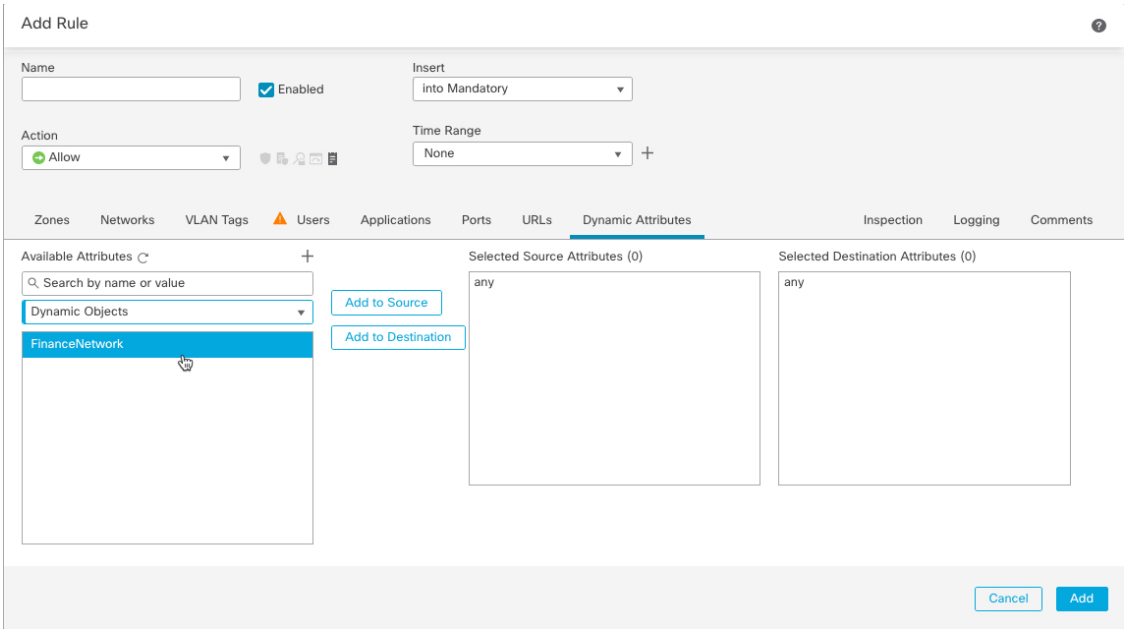
步骤 3 点击访问控制策略旁边的 **编辑**（ ）。

步骤 4 点击**添加规则 (Add Rule)**。

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

步骤 6 在“可用属性”(Available Attributes) 部分中，点击列表中的**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

《思科安全防火墙管理中心设备配置指南》中的“访问控制”一章（章节链接）

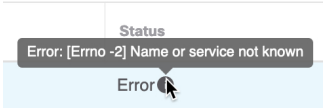
Dynamic Attributes Connector 故障排除

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

错误消息故障排除

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。

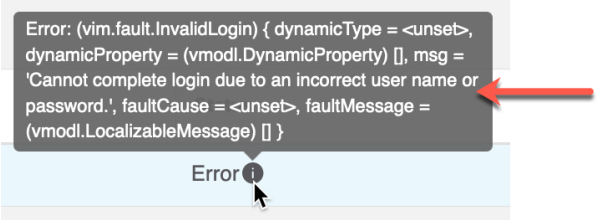


解决方案：编辑连接器或适配器，然后检查：

- 主机名末尾的斜杠
- 验证密码是否正确

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。

获取租户 ID

如果您需要有关 Cisco Secure Dynamic Attributes Connector 的帮助，则必须向思科 TAC 提供您的租户 ID，这样我们才能查看您的日志。

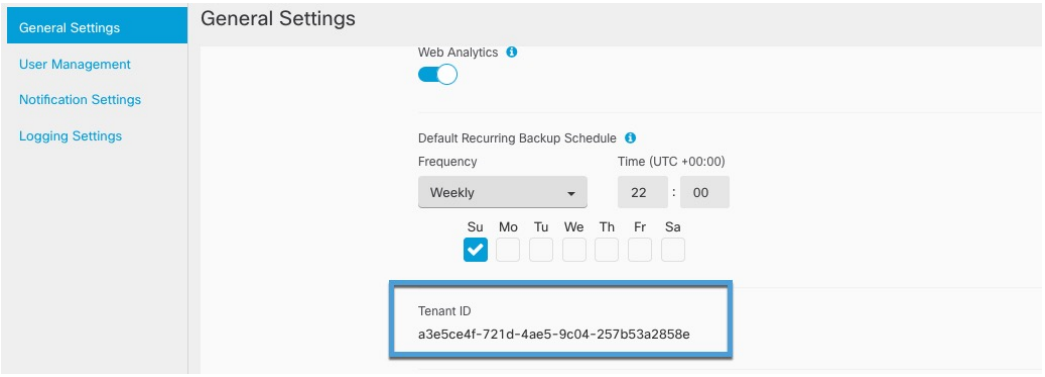
过程

步骤 1 登录CDO。

步骤 2 请点击 **设置 (Settings)** > **常规设置 (General Settings)**。

步骤 3 将您的租户 ID 复制到剪贴板以提供给思科 TAC。

示例如下。



当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。