



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，第 1 页](#)
- [互联网接入要求，第 1 页](#)

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 |

| 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）。