CSM 3.x -向资产中添加IDS传感器和模块

目录

简介

本文档提供有关如何在思科安全管理器(CSM)中添加入侵检测系统(IDS)传感器和模块的信息（包括Catalyst 6500交换机上的IDSM、路由器上的NM-CIDS和ASA上的AIP-SSM）。

注意：CSM 3.2不支持IPS 6.2。CSM 3.3中支持此功能。

先决条件

要求

本文档假设CSM和IDS设备已安装并正常工作。

使用的组件

本文档中的信息基于CSM 3.0.1。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

将设备添加到安全管理器资产

将设备添加到安全管理器时，会引入设备的识别信息范围，例如设备的DNS名称和IP地址。添加设

备后，设备会显示在安全管理器设备资产中。只有在将设备添加到资产后，才能在安全管理器中管理设备。

您可以使用以下方法将设备添加到安全管理器资产：

- 从网络添加设备。
- 添加尚未连接到网络的新设备
- 从设备和凭证存储库(DCR)添加一个或多个设备。
- 从配置文件添加一个或多个设备。

注意：本文档重点介绍方法：添加尚未连接到网络的新设备。

添加IDS传感器和模块的步骤

使用Add New Device选项将单个设备添加到安全管理器资产。您可以使用此选项进行预调配。您可以在系统中创建设备，向设备分配策略，并在收到设备硬件之前生成配置文件。

当您收到设备硬件时，必须准备由安全管理器管理的设备。有关详细信息，请参阅准备供安全管理器管理的设备。

此过程说明如何添加新的IDS传感器和模块：

1. 单击工具栏中的Device View按钮。

   系统将显示Devices页面。

2. 在设备选择器中单击Add按钮。

   系统将显示New Device - Choose Method页面，其中包含四个选项。

3. 选择Add New Device，然后单击Next。

   系统将显示New Device - Device Information页面。

4. 在相应的字段中输入设备信息。

   有关详细信息，请参阅提供设备信息-新设备部分。

5. 单击 完成。

   系统执行设备验证任务：

   - 如果数据不正确，系统会生成错误消息并显示发生错误的页面，并带有与之对应的红色错误图标。
   - 如果数据正确，设备会添加到资产中，并显示在设备选择器中。

提供设备信息—新设备

请完成以下步骤：

1. 为新设备选择设备类型：

    a. 选择顶级设备类型文件夹以显示支持的设备系列。

    b. 选择设备系列文件夹以显示支持的设备类型。

        a. 选择Cisco Interfaces and Modules > Cisco Network Modules 以添加Cisco IDS Access Router Network Module。同样地，选择Cisco Interfaces and Modules > Cisco Services Modules 以添加图中所示的AIP-SSM和IDSM模块。

        b. 选择Security and VPN > Cisco IPS 4200 Series Sensors以将Cisco IDS 4210传感器添加到CSM资产中。

    c. 选择设备类型。

        注意：添加设备后，无法更改设备类型。

        该设备类型的系统对象ID显示在SysObjectId字段中。默认情况下会选择第一个系统对象ID。如果需要，您可以选择其他选项。

2. 输入设备身份信息，例如IP类型（静态或动态）、主机名、域名、IP地址和显示名称。

3. 输入设备操作系统信息，例如操作系统类型、映像名称、目标操作系统版本、情景和操作模式。

4. 系统将显示Auto Update或CNS-Configuration Engine字段，具体取决于您选择的设备类型：

    - Auto Update -为PIX防火墙和ASA设备显示。
    - CNS-Configuration Engine —为Cisco IOS®路由器显示。

    注意：此字段对于Catalyst 6500/7600和FWSM设备处于非活动状态。

5. 请完成以下步骤：

    - Auto Update -点击箭头显示服务器列表。选择管理设备的服务器。如果服务器未出现在列表中，请完成以下步骤：

        a. 单击箭头，然后选择+添加服务器...系统将显示Server Properties对话框。

        b. 在必填字段中输入信息。

        c. Click OK.新服务器将添加到可用服务器列表中。

    - CNS-Configuration Engine -显示不同信息，具体取决于您选择的是静态IP类型还是动态IP类型：

        Static -点击箭头显示配置引擎列表。选择管理设备的配置引擎。如果列表中未显示配置引擎，请完成以下步骤：

a. 点击箭头，然后选择+ Add Configuration Engine...系统将显示Configuration Engine Properties对话框。

b. 在必填字段中输入信息。

c. Click OK.新的配置引擎会添加到可用配置引擎列表中。

- Dynamic -点击箭头以显示服务器列表。选择管理设备的服务器。如果服务器未出现在列表中，请完成以下步骤：

a. 单击箭头，然后选择+添加服务器...系统将显示Server Properties对话框。

b. 在必填字段中输入信息。

c. Click OK.新服务器将添加到可用服务器列表中。

6. 请完成以下步骤：

- 要在安全管理器中管理设备，请选中Manage in Cisco Security Manager复选框。这是默认设置。
- 如果要添加的设备的唯一功能是充当VPN终端，请取消选中Manage in Cisco Security Manager复选框。

安全管理器不会在此设备上管理配置或上传或下载配置。

7. 选中Security Context of Unmanaged Device复选框以管理其父设备（PIX防火墙、ASA或FWSM）未由安全管理器管理的安全情景。

您可以将PIX防火墙、ASA或FWSM分区到多个安全防火墙，也称为安全情景。每个环境都是一个独立的系统，具有自己的配置和策略。您可以在安全管理器中管理这些独立情景，即使父级（PIX防火墙、ASA或FWSM）不由安全管理器管理。

注意：仅当在设备选择器中选择的设备是防火墙设备（如PIX防火墙、ASA或FWSM）时，此字段才处于活动状态。

8. 选中在IPS Manager中管理复选框以便在IPS Manager中管理Cisco IOS路由器。

仅当从设备选择器中选择了Cisco IOS路由器时，此字段才处于活动状态。

注意：IPS Manager只能在具有IPS功能的Cisco IOS路由器上管理IPS功能。有关详细信息，请参阅IPS文档。

如果选中Manage in IPS Manager复选框，还必须选中Manage in Cisco Security Manager复选框。

如果所选设备是IDS，则此字段处于非活动状态。但是，由于IPS Manager管理IDS传感器，因此该复选框处于选中状态。

如果所选设备是PIX防火墙、ASA或FWSM，此字段将处于非活动状态，因为IPS管理器不管理这些设备类型。

9. 单击 完成。

   系统执行设备验证任务：

   - 如果输入的数据不正确，系统会生成错误消息并显示出现错误的页面。
   - 如果输入的数据正确，设备会添加到资产中，并显示在设备选择器中。

故障排除

使用本部分可排除配置故障。

错误消息

将IPS添加到CSM时，显示`Invalid device： Could not deduce the SysObjId for the platform type`错误消息。

解决方案

要解决此错误消息，请完成以下步骤。

1. 在Windows中停止CSM守护程序服务，然后选择Program Files > CSCOpx > MDC > athena > config > Directory，从中可以找到`VMS-SysObjID.xml`。
2. 在CSM系统上，使用最新的`VMS-SysObjID.xml` 文件替换默认情况下位于`C:\Program Files\CSCOpx\MDC\athena\config\directory`中的原始VMS-SysObjID.xml文件。
3. 重新启动CSM守护程序管理器服务(CRMDmgtd)，然后再次尝试添加或发现受影响的设备。

相关信息

- Cisco Security Manager支持页面
- Cisco入侵检测系统支持页
- 技术支持和文档 - Cisco Systems

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）。