主机身份源

以下主题提供有关主机身份源的信息：

概述：主机数据收集

由于Firepower系统被动监控流经网络的流量，因此，它会根据既定的定义（称为指纹）比较特定数据包报头值以及来自网络流量的其他唯一数据，以确定关于网络上主机的信息，包括：

- 主机（包括网桥、路由器、负载均衡器和 NAT 设备等网络设备）数量和类型
- 基本网络拓扑数据，包括从网络上的发现点到主机的跳数
- 主机上运行的操作系统
- 主机上的应用以及与这些应用关联的用户

如果系统无法识别主机的操作系统，则您可以创建自定义客户端或服务器指纹。系统将使用这些指纹来识别新主机。您可以将指纹映射到漏洞数据库 (VDB) 中的系统，以便在使用自定义指纹识别主机时显示适当的漏洞信息。

注释 除从受监控网络流量中收集主机数据以外，系统还可以从导出的 NetFlow 记录收集主机数据，并且您可以使用 Nmap 扫描和主机输入功能主动添加主机数据。

主机身份源的要求和必备条件

型号支持

任意。

支持的域

任意，但自定义指纹除外，它仅限 枝叶。

用户角色

- 管理员
- 发现管理员，但第三方数据和自定义映射除外。

确定系统可以检测的主机操作系统

要了解系统可以进行指纹识别的确切操作系统，请查看在创建自定义操作系统指纹过程中显示的可用指纹的列表。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击 **Create Custom Fingerprint**。

步骤 4 查看**操作系统漏洞映射**部分的下拉列表中的选项列表。这些选项是系统可以进行指纹识别的操作系统。

下一步做什么

根据需要，请参阅识别主机操作系统 ， 第 2 页。

识别主机操作系统

如果系统无法正确识别主机的操作系统（例如，操作系统在“主机配置文件”中显示为“未知”，或者识别的操作系统不正确），则请尝试下面的策略。

过程

尝试以下策略之一：

- 检查“网络发现身份冲突设置”。
- 创建主机的自定义指纹。
- 对主机运行 Nmap 扫描。
- 使用主机输入功能将数据导入到网络映射中。
- 手动输入操作系统信息。

自定义指纹

系统包含系统用于识别其检测的每个主机上的操作系统的操作系统指纹。然而，有时系统会因为不存在与操作系统匹配的指纹而无法识别主机操作系统，或者错误地识别主机操作系统。要纠正此问题，可创建自定义指纹，指纹提供未知或识别错误的操作系统所独有的操作系统特征模式，以便提供用于标识的操作系统名称。

如果系统无法匹配主机操作系统，则无法识别主机漏洞，因为系统通过其操作系统指纹为每个主机派生漏洞列表。例如，如果系统检测到运行 Microsoft Windows 的主机，则表明系统存储了 Microsoft Windows 漏洞列表，其根据检测到的 Windows 操作系统将该列表添加至该主机的主机配置文件。

例如，如果网络上有多个运行新试用版 Microsoft Windows 的设备，则系统无法确定操作系统，或无法将漏洞映射到主机。然而，知道系统拥有 Microsoft Windows 的漏洞列表，您可能想要为某个主机创建自定义指纹，以帮助识别运行相同操作系统的其他主机。可将 Microsoft Windows 漏洞列表的映射纳入指纹中，以便将该列表与匹配指纹的每个主机关联。

创建自定义指纹时，管理中心将为运行相同操作系统的任何主机列出与该指纹关联的漏洞集。如果创建的自定义指纹没有任何漏洞映射，则系统将使用该指纹来分配在其中提供的自定义操作系统信息。当系统看到之前检测的主机发出的新流量时，系统用新指纹信息更新主机。首次检测到使用该操作系统的任何新主机时，系统还会使用新的指纹来识别这些主机。

在创建自定义指纹前，应确定主机未被正确识别的原因，从而确定自定义指纹是否为可行的解决方案。

可使用系统创建两种类型的指纹：

- 客户端指纹，这种指纹根据 SYN 数据包识别操作系统，主机连接网络上的另一主机上运行的 TCP 应用时，会发送这种数据包。
- 服务器指纹，这种指纹根据 SYN-ACK 数据包识别操作系统，主机使用这种数据包来响应通向运行的 TCP 应用的传入连接。

注释 如果客户端和服务器指纹均与相同的主机匹配，将会使用客户端指纹。

创建指纹后，必须先将其激活，然后系统才可以将其与主机关联。

相关主题

为客户端创建自定义指纹，第 6 页
为服务器创建自定义指纹，第 8 页

管理指纹

指纹创建和激活后，可编辑指纹以便做出更改或添加漏洞映射。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。如果系统正在等待数据以便创建指纹，将会每 10 秒自动刷新页面，直到指纹已创建。

步骤 3 管理自定义指纹：

- 激活/停用 - 激活或停用指纹，如激活和停用指纹，第 4 页中所述。
- 创建 - 创建指纹，如为客户端创建自定义指纹，第 6 页和为服务器创建自定义指纹，第 8 页中所述。
- 编辑 - 编辑指纹，如编辑活动指纹，第 5 页和编辑非活动指纹，第 5 页中所述。
- 删除 - 点击要删除的指纹旁边的 **删除**（ ），并点击**确定 (OK)** 以进行确认。只能删除已停用的指纹。

激活和停用指纹

必须先激活自定义指纹，然后系统才能将其用于识别主机。新指纹激活后，系统会将其用于重新识别先前发现的主机并发现新的主机。

如果想要停止使用指纹，可将其停用。停用指纹后，该指纹就不再可用，但仍可保留其在系统中。停用指纹后，对于使用该指纹的主机，操作系统被标记为未知。如果再次检测到这些主机，并且这些主机与不同的活动指纹匹配，则该活动指纹将对其进行识别。

删除指纹会将其从系统中完全删除。停用指纹后，即可将其删除。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击要激活或停用的指纹旁边的滑块。

注释 激活选项仅当创建的指纹有效时才可用。如果滑块不可用，请尝试重新创建指纹。

编辑活动指纹

如果指纹处于活动状态，可修改指纹名称、描述、自定义操作系统显示，并向其映射额外的漏洞。

可以修改指纹名称、描述、自定义操作系统显示，并向其映射额外的漏洞。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**

步骤 3 点击想要编辑的指纹旁的 **编辑**（）。

步骤 4 必要时修改指纹名称、描述和自定义操作系统显示。

步骤 5 如果要删除漏洞映射，请点击页面的**预定义操作系统产品映射 (Pre-Defined OS Product Maps)** 部分中映射旁边的**删除 (Delete)**。

步骤 6 如果要为漏洞映射添加额外的操作系统，请选择**产品 (Product)**，且在适用的情况下，选择**主要版本 (Major Version)**、**次要版本 (Minor Version)**、**修订版本 (Revision Version)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)**，然后点击**添加操作系统定义 (Add OS Definition)**。

漏洞映射会添加到**预定义操作系统产品映射 (Pre-Defined OS Product Maps)** 列表。

步骤 7 点击**保存 (Save)**。

编辑非活动指纹

如果指纹处于非活动状态，可修改指纹的所有元素，并将其重新提交至 Cisco Secure Firewall Management Center。这包括创建指纹时指定的所有属性，如指纹类型、目标 IP 地址与端口、漏洞映射等。编辑非活动指纹并将其提交时，会将它重新提交至系统，如果指纹是客户端指纹，必须先将流量重新发送至设备，然后才可以将其激活。请注意，对于非活动指纹，仅可选择单一漏洞映射。激活指纹后，可将额外的操作系统和版本映射至其漏洞列表。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击想要编辑的指纹旁的 **编辑**（）。

步骤 4 请在必要时更改指纹：

- 如果要修改客户端指纹，请参阅为客户端创建自定义指纹，第 6 页。
- 如果要修改服务器指纹，请参阅为服务器创建自定义指纹，第 8 页。

步骤 5 单击**保存**。

下一步做什么

- 如已修改客户端指纹，切记将流量从主机发送至收集指纹的设备。

为客户端创建自定义指纹

客户端指纹根据 SYN 数据包识别操作系统，主机连接网络上的另一主机上运行的 TCP 应用时，会发送这种数据包。

如果 管理中心不与受监控的主机直接联系，指定客户端指纹属性时，可以指定管理中心管理的离想要为其设置指纹的主机最近的设备。

开始指纹设置流程之前，获取想要为其设置指纹的主机的以下相关信息：

- 主机与管理中心或用于获取指纹的设备之间的网络跳数。（思科强烈建议将管理中心或设备直接连接到与主机所连接到的同一子网）。
- 连接至主机所在网络的（管理中心或设备上的）网络接口。
- 主机的实际操作系统供应商、产品和版本。
- 访问主机以便生成客户端流量。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击 **Create Custom Fingerprint**。

步骤 4 从**设备**下拉列表中，选择要用于收集指纹的 管理中心或设备。

步骤 5 输入**指纹名称 (Fingerprint Name)**。

步骤 6 输入**指纹说明 (Fingerprint Description)**。

步骤 7 从**指纹类型 (Fingerprint Type)** 列表中，选择**客户端 (Client)**。

步骤 8 在**目标 IP 地址 (Target IP Address)** 字段中，输入要为其设置指纹的主机的 IP 地址。

请注意，指纹仅会基于流向和来自您指定的主机IP地址的流量，而不是主机的任何其他IP地址（如果其拥有）。

步骤 9 在**目标距离 (Target Distance)** 字段中，输入主机与之前选择用于收集指纹的设备之间的网络跳数。

注意 此跳数必须是至主机的实际物理网络跳数，与系统检测到的跳数不一定相同。

步骤 10 从**接口 (Interface)** 列表中，选择连接到主机所在网段的网络接口。

注意 由于多个原因，思科建议**不要**将受管设备上的传感接口用于设置指纹。首先，如果传感接口位于 SPAN 端口之上，指纹技术将不起作用。另外，如果使用设备上的传感接口，设备在其收集指纹所花的时间内会停止监控网络。不过，可使用管理接口或任何其他可用网络接口来执行指纹收集。如果不知道哪个接口是设备上的传感接口，请参阅用于设置指纹的特定型号的《安装指南》。

步骤 11 如果要在设置指纹的主机的主机配置文件中显示自定义信息（或者如果要设置指纹的主机不在**操作系统漏洞映射**部分中），请选择**使用自定义操作系统显示**，并对于以下各项提供要显示的值：

- 在**供应商字符串 (Vendor String)** 字段中，输入操作系统的供应商名称。例如，Microsoft Windows 的供应商为 Microsoft。
- 在**产品字符串 (Product String)** 字段中，输入操作系统的产品名称。例如，Microsoft Windows 2000 的产品名称为 Windows。
- 在**版本字符串 (Version String)** 字段中，输入操作系统的版本号。例如，Microsoft Windows 2000 的版本号为 2000。

步骤 12 在“操作系统漏洞映射”(OS Vulnerability Mappings) 部分中，选择要用于漏洞映射的操作系统、产品和版本。

如果要使用指纹来识别匹配主机的漏洞，或者如果不分配自定义的操作系统显示信息，则必须在此部分指定**供应商 (Vendor)** 和**产品 (Product)** 值。

要为所有版本的操作系统映射漏洞，请仅指定**供应商**和**产品**值。

注释 并非**主要版本 (Major Version)**、**次要版本 (Minor Version)**、**修订版本 (Revision Version)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)** 下拉列表中的所有选项均可应用至选择的操作系统。此外，如果列表中没有显示与想要设置指纹的操作系统匹配的定义，可将这些值留空。请注意，如果不在指纹中创建任何操作系统漏洞映射，则系统无法使用指纹来为指纹识别的主机分配漏洞列表。

示例：

如果想要自定义指纹将 Redhat Linux 9 的漏洞列表分配到匹配主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为主要版本。

示例：

要添加所有版本的 Palm 操作系统，请从 **供应商**列表中选择 **PalmSource, Inc.**，从**产品**列表中选择 **Palm 操作系统**，并让所有其他列表保持其默认设置。

步骤 13 点击**创建**。

状态会短暂显示 `New`，然后切换至 `Pending`，此状态会保持不变，直到发现匹配指纹的流量。发现流量后，状态会切换至就绪 `(Ready)`。

“自定义指纹”(Custom Fingerprint) 状态页面每隔 10 秒进行刷新，直到其收到来自所述主机的数据。

步骤 14 将指定的 IP 地址用作目标 IP 地址，访问您尝试为其设置指纹的主机，并发起至设备的 TCP 连接。

要创建准确的指纹，收集指纹的设备**必须**发现流量。如果通过交换机进行连接，系统可能不会发现流向系统而不是设备的流量。

示例：

从想要为其设置指纹的主机访问 管理中心的 Web 界面，或者从主机使用 SSH 登录至 管理中心。如果使用的是 SSH，请使用以下命令，其中，localIPv6address 是在步骤 7 中指定的当前已分配到主机的 IPv6 地址，DCmanagementIPv6address 是 管理中心 的管理 IPv6 地址。然后，Custom Fingerprint 页面重新加载，其状态为“就绪”。

```
ssh -b localIPv6address DCmanagementIPv6address
```

下一步做什么

- 激活指纹，如激活和停用指纹 ， 第 4 页中所述。

为服务器创建自定义指纹

服务器指纹根据 SYN-ACK 数据包识别操作系统，主机使用这种数据包来响应通向运行的 TCP 应用的传入连接。在开始之前，应获取关于想要为其设置指纹的主机的以下信息：

- 主机与用于获取指纹的设备之间的网络跳数。思科强烈建议将设备上不使用的接口直接连接到主机所连接到的相同子网。
- 连接至主机所在网络的（设备上的）网络接口。
- 主机的实际操作系统供应商、产品和版本。
- 未在使用的 IP 地址，并在主机所在网络上得到授权。

提示 如果 管理中心不与受监控的主机直接联系，指定服务器指纹属性时，可以指定离想要为其设置指纹的主机最近的受管设备。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击 **Create Custom Fingerprint**。

步骤 4 从**设备**列表中，选择要用于收集指纹的 管理中心或受管设备。

步骤 5 输入**指纹名称 (Fingerprint Name)**。

步骤 6 输入**指纹说明 (Fingerprint Description)**。

步骤 7 从**指纹类型 (Fingerprint Type)** 列表中，选择**服务器 (Server)** 以显示服务器指纹选项。

步骤 8 在**目标 IP 地址 (Target IP Address)** 字段中，输入要为其设置指纹的主机的 IP 地址。

请注意，指纹仅会基于流向和来自您指定的主机IP地址的流量，而不是主机的任何其他IP地址（如果其拥有）。

注意　只可以使用运行 5.2 及更高版本的设备捕获 IPv6 指纹。

步骤 9 在**目标距离 (Target Distance)** 字段中，输入主机与之前选择用于收集指纹的设备之间的网络跳数。

注意　此跳数必须是至主机的实际物理网络跳数，与系统检测到的跳数不一定相同。

步骤 10 从**接口 (Interface)** 列表中，选择连接到主机所在网段的网络接口。

注意　由于多个原因，思科建议**不要**将受管设备上的传感接口用于设置指纹。首先，如果传感接口位于 SPAN 端口之上，指纹技术将不起作用。另外，如果使用设备上的传感接口，设备在其收集指纹所花的时间内会停止监控网络。不过，可使用管理接口或任何其他可用网络接口来执行指纹收集。如果不知道哪个接口是设备上的传感接口，请参阅用于设置指纹的特定型号的《安装指南》。

步骤 11 点击**获取活动端口 (Get Active Ports)**。

步骤 12 在**服务器端口**字段中，输入想要设备选择用于收集指纹以便向其发起联系的端口，或者从**获取活动端口**下拉列表选择端口。

可使用主机上已知开放的任何服务器端口（例如，80，如果主机正在运行网络服务器）。

步骤 13 在**源 IP 地址 (Source IP Address)** 字段中，输入应用于尝试与主机通信的 IP 地址。

应使用经授权可在网络上使用，但目前未在使用的源 IP 地址，例如，当前未在使用的 DHCP 池地址。创建指纹时，这可防止临时访问另一离线主机。

创建指纹时，应从网络发现策略的监控中排除该IP地址。否则，网络映射和发现事件视图中将会出现大量关于该 IP 地址代表的主机的不准确信息。

步骤 14 在**源子网掩码 (Source Subnet Mask)** 字段中，输入正在使用的 IP 地址的子网掩码。

步骤 15 如果 **Source Gateway** 字段显示，输入应用于建立至主机的路由的默认网关 IP 地址。

步骤 16 如果要在设置指纹的主机的主机配置文件中显示自定义信息，或者如果要使用的指纹名称在“操作系统定义”(OS Definition) 部分中不存在，则可以在“自定义操作系统显示”(Custom OS Display) 部分中选择**使用自定义操作系统显示 (Use Custom OS Display)**。

对于以下项提供想要在主机配置文件中显示的值：

- 在**供应商字符串 (Vendor String)** 字段中，输入操作系统的供应商名称。例如，Microsoft Windows 的供应商为 Microsoft。
- 在**产品字符串 (Product String)** 字段中，输入操作系统的产品名称。例如，Microsoft Windows 2000 的产品名称为 Windows。
- 在**版本字符串 (Version String)** 字段中，输入操作系统的版本号。例如，Microsoft Windows 2000 的版本号为 2000。

步骤 17 在“操作系统漏洞映射”(OS Vulnerability Mappings) 部分中，选择要用于漏洞映射的操作系统、产品和版本。

如果要使用指纹来识别匹配主机的漏洞，或者如果不分配自定义的操作系统显示信息，则必须在此部分指定供应商和产品名称。

要为所有版本的操作系统映射漏洞，请仅指定供应商和产品名称。

注释 并非**主要版本 (Major Version)**、**次要版本 (Minor Version)**、**修订版本 (Revision Version)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)** 下拉列表中的所有选项均可应用至选择的操作系统。此外，如果列表中没有显示与想要设置指纹的操作系统匹配的定义，可将这些值留空。请注意，如果不在指纹中创建任何操作系统漏洞映射，则系统无法使用指纹来为指纹识别的主机分配漏洞列表。

示例：

如果想要自定义指纹将 Redhat Linux 9 的漏洞列表分配到匹配主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

示例：

要添加所有版本的 Palm 操作系统，请从 **供应商 (Vendor)** 列表中选择 **PalmSource, Inc.**，从**产品 (Product)** 列表中选择 **Palm 操作系统 (Palm OS)**，并让所有其他列表保持其默认设置。

步骤 18 点击**创建**。

“自定义指纹”(Custom Fingerprint) 状态页面每 10 秒刷新一次并应以“就绪”状态重新加载。

注释 如果目标系统在设置指纹的过程中停止响应，状态将会显示`错误：无响应 (ERROR: No Response)` 消息。如果看到此消息，请再次提交指纹。等待 3 至 5 分钟（时长可能因目标系统而异），点击 **编辑**（ ） 访问“自定义指纹”(Custom Fingerprint) 页面，然后点击**创建 (Create)**。

下一步做什么

- 激活指纹，如激活和停用指纹 ， 第 4 页中所述。

主机输入数据

您可以通过从第三方导入网络映射数据来扩充网络映射。您还可使用主机输入功能，只需使用 Web 界面修改操作系统或应用身份，或删除应用协议、协议、主机属性或客户端。

系统可协调来自多个源的数据，以确定操作系统或应用的当前身份。

从网络映射中删除受影响的主机后，将会丢弃除第三方漏洞之外的所有数据。有关设置脚本或导入文件的详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

要将已导入数据纳入影响关联中，必须将数据映射至数据库中的操作系统和应用定义。

第三方数据使用要求

可以从网络上的第三方系统导入发现数据。但是，要启用将入侵和发现数据结合使用的功能（例如思科建议、自适应配置文件或影响评估），应将其中尽可能多的元素映射到对应的定义。考虑对使用第三方数据的以下要求：

- 如果拥有在您的网络资产上有特定数据的第三方系统，则可使用主机输入功能导入该数据。但是，由于第三方可能会以不同的方式命名产品，因此必须将第三方供应商、产品和版本映射到对应的思科产品定义。映射产品后，必须在 管理中心配置中为影响评估启用漏洞映射，以允许影响关联。对于无版本或无供应商的应用协议，需要在 管理中心配置中映射应用协议的漏洞。
- 如果导入来自第三方的修补程序信息，并想要将修补程序修补的所有漏洞标记为无效，则必须将第三方修补程序的名称映射至数据库中的定义。修补程序针对的所有漏洞随后会从添加该修补程序所在的主机中移除。
- 如果导入来自第三方的操作系统和应用协议漏洞，并想将其用于影响关联，则必须将第三方漏洞标识字符串映射至数据库中的漏洞。请注意，尽管许多客户端拥有相关的漏洞，而且客户端用于影响评估，但不能导入和映射第三方客户端漏洞。映射漏洞后，必须在 管理中心配置中为影响评估启用第三方漏洞映射。要使没有供应商或版本信息的应用协议映射到漏洞，管理用户还必须在 管理中心配置中映射应用的漏洞。
- 如果导入应用数据并要将该数据用于影响关联，则必须将每个应用协议的供应商字符串映射到对应的应用协议定义。

相关主题

映射第三方产品，第 11 页
映射第三方产品修补程序，第 13 页
映射第三方漏洞，第 14 页
创建自定义产品映射，第 15 页

第三方产品映射

如果通过用户输入功能将第三方数据添加至网络映射，则必须将第三方使用的供应商、产品和版本名称映射到思科产品定义。将产品映射到思科定义后，将根据这些定义分配漏洞。

类似地，如果正在导入第三方修补程序信息，如修补程序管理产品，则必须将修补程序的名称映射至适当供应商和产品以及数据库中的相应修补程序。

映射第三方产品

如果从第三方导入数据，则必须将思科产品映射到第三方名称，以分配漏洞并使用该数据执行影响关联。映射产品可以将思科漏洞信息与第三方产品名称关联，这样，系统就可使用该数据执行影响关联。

如果使用主机输入导入功能导入数据，还可以在导入过程中，使用 AddScanResult 函数将第三方产品映射至操作系统和应用漏洞。

例如，如果从将 Apache Tomcat 列为应用的第三方导入数据，并且知道它是该产品的第 6 版，则可以添加第三方映射，其中：

- **供应商名称 (Vendor Name)** 设置为 `Apache`。
- **产品名称 (Product Name)** 设置为 `Tomcat`。
- **Apache** 是从**供应商 (Vendor)** 下拉列表中选择。
- **Tomcat** 是从**产品 (Product)** 下拉列表中选择。
- **6** 是从**版本 (Version)** 下拉列表中选择。

该映射会使 Apache Tomcat 6 的任何漏洞分配到其应用列出了 Apache Tomcat 的主机。

请注意，对于无版本或无供应商的应用，必须在 Cisco Secure Firewall Management Center配置中为应用类型映射漏洞。尽管许多客户端具有关联的漏洞，而且客户端用于影响评估，但不能导入和映射第三方客户端漏洞。

提示 如已在另一 Cisco Secure Firewall Management Center上创建了第三方映射，则将其导出后可导入至此管理中心。然后，可根据自己的需求编辑已导入的映射。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新的映射集，请点击**创建产品映射集 (Create Product Map Set)**。
- 编辑 - 要编辑现有映射集，请点击要修改的映射集旁边的**编辑**（）。如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**映射集名称 (Mapping Set Name)**。

步骤 5 输入**说明**。

步骤 6 您有两种选择：

- 创建 - 要映射第三方产品，请点击**添加产品映射 (Add Product Map)**。
- 编辑 - 要编辑现有第三方产品映射集，请点击要修改的映射集旁边的**编辑**（）。如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 7 输入第三方产品使用的**供应商字符串 (Vendor String)**。

步骤 8 输入第三方产品使用的**产品字符串 (Product String)**。

步骤 9 输入第三方产品使用的**版本字符串 (Version String)**。

步骤 10 在“产品映射”部分中，从以下字段为漏洞映射选择要使用的操作系统、产品和版本：**供应商**、**产品**、**主要版本**、**次要版本**、**修订版本**、**内部版本**、**补丁**和**扩展版本** 。

示例：

如果要运行其名称包含第三方字符串的产品的主机使用 Red Hat Linux 9 的漏洞，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

步骤 11 点击**保存 (Save)**。

映射第三方产品修补程序

如果将修补程序名称映射至数据库中一组特定的修补程序，则可从第三方修补程序管理应用中导入数据，并对一组主机应用该修补程序。修补程序名称导入至主机后，对于该主机，系统会将修补程序针对的所有漏洞标记为无效。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新的映射集，请点击**创建产品映射集 (Create Product Map Set)**。
- 编辑 - 要编辑现有映射集，请点击要修改的映射集旁边的**编辑**（）。如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**映射集名称 (Mapping Set Name)**。

步骤 5 输入**说明**。

步骤 6 您有两种选择：

- 创建 - 要映射第三方产品，请点击**添加修补程序映射 (Add Fix Map)**。
- 编辑 - 要编辑现有第三方产品映射，请点击映射旁边的**编辑**（）。如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 7 在**第三方修补程序名称 (Third-Party Fix Name)** 字段中，输入要映射的修补程序的名称。

步骤 8 在**产品映射 (Product Mappings)** 部分中，从以下字段为修补程序映射选择要使用的操作系统、产品和版本：

- **Vendor**
- **Product**
- **主要版本 (Major Version)**
- **次要版本 (Minor Version)**
- **修订版本 (Revision Version)**
- **构建**
- **修补**
- **分机**

示例：

如果想要映射将 Red Hat Linux 9 的修补程序分配到应用补丁的主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

步骤 9 点击 **Save**，以保存修补程序映射。

映射第三方漏洞

要将第三方的漏洞信息添加至VDB，必须将每个导入的漏洞的第三方标识字符串映射至任何现有的SVID、Bugtraq或SID。为漏洞创建映射之后，该映射适用于已导入网络映射中主机的所有漏洞，且可为这些漏洞执行影响关联。

必须为第三方漏洞启用影响关联，才能允许关联发生。对于无版本或无供应商的应用，还必须在Cisco Secure Firewall Management Center配置中为应用类型映射漏洞。

尽管许多客户端拥有关联的漏洞，而且客户端用于影响评估，但不能将第三方客户端漏洞用于影响评估。

提示 如已在另一 Cisco Secure Firewall Management Center上创建了第三方映射，则将其导出后可导入至此管理中心。然后，可根据自己的需求编辑已导入的映射。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新漏洞集，请点击**创建漏洞映射集 (Create Vulnerability Map Set)**。
- 编辑 - 要编辑现有漏洞集，请点击漏洞集旁边的**编辑**（）。如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击 **Add Vulnerability Map**。

步骤 5 在**漏洞 ID (Vulnerability ID)** 字段中输入第三方漏洞标识。

步骤 6 输入**漏洞说明 (Vulnerability Description)**。

步骤 7 或者：

- 在 **Snort 漏洞 ID 映射**字段中输入 Snort ID。
- 在 **SVID 映射 (SVID Mappings)** 字段中输入旧版漏洞 ID。
- 在 **Bugtraq 漏洞 ID 映射 (Bugtraq Vulnerability ID Mappings)** 字段中输入 Bugtraq 标识号。

步骤 8 点击**添加 (Add)**。

相关主题

启用网络发现漏洞影响评估

自定义产品映射

可以使用产品映射来确保由第三方输入的服务器与适当的思科定义相关联。定义并激活产品映射后，具有映射供应商字符串的受监控主机上的所有服务器或客户端都使用自定义产品映射。为此，您可能想要为网络中带有特定供应商字符串的服务器映射漏洞，而不是显式地为服务器设置供应商、产品和版本。

创建自定义产品映射

如果系统无法将服务器映射到VDB中的供应商和产品，您可以手动创建映射。激活自定义产品映射后，系统会将指定供应商和产品的漏洞映射到出现该供应商字符串的网络映射中的所有服务器。

注释 自定义产品映射将应用于所有出现应用协议的位置，无论应用数据的源为何（如Nmap、主机输入功能或Firepower系统自身）。然而，如果使用主机输入功能导入的数据的第三方漏洞映射与通过自定义产品映射设置的映射发行冲突，则输入出现时，第三方漏洞映射将覆盖自定义产品映射并使用第三方漏洞映射设置。

可创建产品映射列表，然后通过激活或停用每份列表而一次性启用或禁用多个映射。指定将要映射到的供应商后，系统将更新产品列表，以仅包含该供应商提供的产品。

创建自定义产品映射后，必须激活自定义产品映射列表。激活自定义产品映射列表后，系统将更新出现指定供应商字符串的所有服务器。对于通过主机输入功能导入的数据，漏洞将更新，除非已为此服务器显式设置产品映射。

例如，如果贵公司将您的 Apache Tomcat Web 服务器的横幅修改为 `Internal Web Server`，则可将供应商字符串 `Internal Web Server` 映射到供应商 **Apache** 和产品 **Tomcat**，然后激活包含该映射的列表，出现标有 `Internal Web Server` 的服务器的所有主机均拥有数据库中的 Apache Tomcat 漏洞。

提示 可使用此功能将漏洞映至至本地入侵规则，只需将规则的 SID 映射至另一漏洞。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击**自定义产品映射 (Custom Product Mappings)**

步骤 3 点击 **Create Custom Product Mapping List**。

步骤 4 输入**自定义产品映射列表名称 (Custom Product Mapping List Name)**。

步骤 5 点击**添加供应商字符串 (Add Vendor String)**。

步骤 6 在**供应商字符串 (Vendor String)** 字段中，输入供应商字符串，该字符串标识应映射到所选供应商和产品值的应用。

步骤 7 从**供应商 (Vendor)** 下拉列表，选择要映射的供应商。

步骤 8 从**产品 (Product)** 下拉列表，选择要映射的产品。

步骤 9 点击**添加 (Add)**，以将已映射的供应商字符串添加到列表。

步骤 10 或者，在必要时，重复第 4 至 8 步，将额外的供应商字符串映射添加至列表。

步骤 11 单击**保存**。

下一步做什么

- 激活自定义产品映射列表。有关详细信息，请参阅 激活和停用自定义产品映射，第 16 页。

编辑自定义产品映射列表

可修改现有自定义产品映射列表，只需添加或移除供应商字符串或更改列表名称。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击**自定义产品映射 (Custom Product Mappings)**。

步骤 3 点击要编辑的产品映射列表旁边的 **编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 对列表进行更改，如创建自定义产品映射，第 15 页中所述。

步骤 5 完成后，点击 **Save**。

激活和停用自定义产品映射

可一次性启用或禁用整个自定义产品映射列表。激活自定义产品映射列表后，该列表上的每个映射均应用所有带有指定供应商字符串的应用，无论是通过受管设备检测到的，还是通过主机输入功能导入的。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击**自定义产品映射 (Custom Product Mappings)**。

步骤 3 点击要激活或停用的自定义产品映射列表旁边的滑块。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

配置主机输入客户端

主机输入功能允许您从另一台设备上运行的客户端程序更新 管理中心的网络映射。例如，您可以从网络映射添加或删除主机，或者更新主机操作系统和服务信息。有关详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

只有先从“主机输入客户端”页面将客户端添加到 管理中心的对等数据库，然后才能运行远程客户端。还必须将管理中心生成的身份验证证书复制至客户端。完成这些步骤之后，客户端可连接到管理中心。

在多域部署中，可以在任何域中创建客户端。身份验证证书允许客户端为与客户端证书的域关联的任何分叶域提交网络映射更新。如果您为祖先域创建证书（或如果您的证书域在添加后代域之后成为祖先域），则使用该证书的任何客户端都必须指定每个事务的目标分叶域，如《*Firepower* 系统主机输入 *API* 指南》中所述。

“主机输入客户端”(Host Input Client) 仅显示与当前域关联的客户端，因此，如果您要下载或撤销证书，请切换至创建客户端时所在的域。

此连接使用 TLS 1.2。

过程

步骤 1 选择**集成** > **其他集成**。

步骤 2 点击**主机输入客户端 (Host Input Client)**。

步骤 3 点击**创建客户端 (Create Client)**。

步骤 4 在 **Hostname** 字段中，输入运行主机输入客户端的主机的主机名称或 IP 地址。

注释 如果尚未配置 DNS 解析，请使用 IP 地址。

步骤 5 如果要对证书文件进行加密，请在**密码 (Password)** 字段中输入密码。

步骤 6 点击**保存 (Save)**。
主机输入服务将允许主机访问 管理中心上的 8307 端口，并会创建在客户端-服务器身份验证过程中使用的身份验证证书。

步骤 7 点击证书文件旁边的 **下载**（ ）。

步骤 8 将证书文件保存至客户端用于 SSL/TLS 身份验证的目录。

步骤 9 要撤消客户端的访问权限，请点击想要移除的主机旁边的 **删除**（ ）。

Nmap 扫描

Firepower 系统通过对网络上的流量进行被动分析构建网络映射。根据系统的情况，通过这种被动分析获取的信息有时可能并不完整。不过，您可以主动扫描主机，获取完整信息。例如，如果主机有

一台服务器在开放端口上运行，但该服务器在系统监控网络期间未收发流量，则系统不会向网络映射添加有关该服务器的信息。但是，如使用主动扫描程序直接扫描主机，则可检测到服务器的存在。

Firepower 系统与用于网络探索和安全审核的开源主动扫描程序 Nmap™ 集成。

使用 Nmap 扫描主机时，系统会：

- 将之前未检测到的开放端口上的服务器添加至该主机配置文件中的服务器列表。主机配置文件在“扫描结果”(Scan Results) 部分列出在已过滤或关闭 TCP 端口或 UDP 端口上检测到的任何服务器。默认情况下，Nmap 扫描 1660 多个 TCP 端口。

  如果系统识别在 Nmap 扫描中已确定的服务器且有对应的服务器定义，系统会将 Nmap 用于该服务器的名称映射至对应的思科服务器定义。

- 然后，将扫描结果与超过1500个已知操作系统指纹进行对比，确定操作系统，并为每个操作系统评分。分配给主机的操作系统是得分最高的操作系统指纹。

  系统会将 Nmap 操作系统名称映射至思科操作系统定义。

- 为添加的服务器和操作系统将漏洞分配至主机。

注意：

- 只有网络映射中存在主机，Nmap 才能将其结果附加至主机配置文件。
- 如果从网络映射中删除主机，则将丢弃该主机的任何 Nmap 扫描结果。

提示 有些扫描选项（例如，端口扫描）会显著增加低带宽网络的负载。请将此类扫描安排在网络使用量较低的时段运行。

有关用于扫描的基础 Nmap 技术的详细信息，请参阅 http://insecure.org/ 上的 Nmap 文档。

Nmap 补救选项

可以创建 Nmap 补救以定义 Nmap 扫描设置。Nmap 补救可用作关联策略中的响应，按需运行，或预定在特定时间运行。

请注意，Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 扫描主机以获取操作系统和服务器数据，则可能要设置定期扫描，随时更新任何 Nmap 提供的操作系统和服务器数据。

下表说明可在 Nmap 补救中配置的选项。

表 *1: Nmap* 补救选项

选项	说明	对应的 Nmap 选项
扫描事件中的哪个地址？(Scan Which Address(es) From Event?)	将 Nmap 扫描用作对关联规则的响应时，选择以下其中一个选项以控制扫描事件中的哪个地址，源主机的地址和/或目标主机的地址： • **扫描源地址和目标地址 (Scan Source and Destination Addresses)**，扫描事件中源 IP 地址和目标 IP 地址代表的主机。 • **仅扫描源地址 (Scan Source Address Only)**，扫描事件的源 IP 地址代表的主机。 • **仅扫描目标地址 (Scan Destination Address Only)**，扫描事件的目标 IP 地址代表的主机。	不适用
扫描类型 (Scan Types)	选择 Nmap 如何扫描端口： • **TCP 同步 (TCP Syn)** 扫描可以快速连接到数千个端口，无需使用完整的 TCP 握手。此选项可用于在以下主机上以隐形模式快速扫描，可发起但不完成 TCP 连接：`admin` 帐户拥有原始数据包访问权限的主机，或未运行 IPv6 的主机。如果主机确认在 TCP Syn 扫描中发送的 Syn 数据包，Nmap 会重置连接。 • **TCP 连接 (TCP Connect)** 扫描使用 `connect()` 系统调用，打开穿过主机操作系统的连接。如果 管理中心或受管设备上的 `admin` 用户在主机上没有原始数据包权限，或正在扫描IPv6网络，则可使用“TCP 连接”扫描。换句话说，在无法使用“TCP 同步”(TCP Syn) 扫描的情况下使用此选项。 • **TCP ACK** 扫描发送 ACK 数据包，检查端口是否已被过滤。 • **TCP 窗口 (TCP Window)** 扫描的工作方式与 TCP ACK 扫描相同，但也可确定端口已打开还是关闭。 • **TCP Maimon** 扫描使用 FIN/ACK 探针识别 BSD 派生系统。	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon**: `-sM`
扫描 UDP 端口 (Scan for UDP ports)	启用此选项，可扫描 UDP 端口以及 TCP 端口。请注意，扫描 UDP 端口可能比较耗时，因此，如果想快速扫描，请避免使用此选项。	`-sU`

选项	说明	对应的 Nmap 选项
使用事件中的端口 (Use Port From Event)	如果计划将补救用作关联政策中的响应，请启用此选项，使补救仅扫描在触发关联响应的事件中指定的端口。 • 选择**打开 (On)** 以扫描关联事件中的端口，而不是在 Nmap 补救配置过程中指定的端口。如果扫描关联事件中的端口，请注意，补救将扫描在 Nmap 补救配置过程中指定的 IP 地址上的端口。这些端口也会添加至补救的动态扫描目标。 • 选择**关闭 (Off)**，仅扫描在 Nmap 补救配置过程中指定的端口。 您也可以控制 Nmap 是否收集关于操作系统和服务器信息的信息。启用**使用事件中的端口 (Use Port From Event)** 选项，可扫描与新服务器关联的端口。	不适用
从报告检测引擎扫描 (Scan from reporting detection engine)	启用此选项，可从报告主机的检测引擎所驻留的设备扫描主机。 • 要从运行报告检测引擎的设备扫描，请选择**打开 (On)**。 • 要从已在补救中配置的设备扫描，请选择**关闭 (Off)**。	不适用
快速端口扫描 (Fast Port Scan)	启用此选项，仅扫描 `nmap-services` 文件中所列的 TCP 端口，而忽略其他端口设置，该文件位于执行扫描设备上的 `/var/sf/nmap/share/nmap/nmap-services` 目录中。请注意，不能同时使用此选项与**端口范围和扫描顺序 (Port Ranges and Scan Order)** 选项。 • 要仅扫描 `nmap-services` 文件中列出的端口，而忽略其他端口设置，请选择**打开 (On)**，该文件可在扫描设置上的 `/var/sf/nmap/share/nmap/nmap-services` 目录中找到。 • 要扫描所有 TCP 端口，请选择**关闭 (Off)**。	`-F`
端口范围和扫描顺序 (Port Ranges and Scan Order)	使用Nmap端口规范语法设置要扫描的特定端口及其扫描顺序。请注意，不能同时使用此选项与**快速端口扫描 (Fast Port Scan)** 选项。	`-p`
探测开放端口以获取供应商和版本信息(Probe open ports for vendor and version information)	启用此选项，可检测服务器供应商和版本信息。如果探测开放端口以获取服务器供应商和版本信息，Nmap将获取其用来识别服务器的服务器数据。然后，它会为该服务器替换思科服务器数据。 • 选择**On**，扫描主机上的开放端口以获取服务器信息，识别服务器厂商和版本。 • 选择**关闭 (Off)**，继续使用主机的思科服务器信息。	`-sV`

选项	说明	对应的 Nmap 选项
服务版本强度 (Service Version Intensity)	选择适用于服务器版本的 Nmap 探针强度。 • 要使用更多探针进行更精确、更长久的扫描，请选择一个较大的数字。 • 要使用更少探针进行不太精确、更加快速的扫描，请选择一个较小的数字。	`--version-intensity` <强度>
检测操作系统 (Detect Operating System)	启用此选项，可检测主机的操作系统信息。 如果配置主机的操作系统检测，Nmap将扫描主机，并使用扫描结果创建每个操作系统的评级，反映操作系统在主机上运行的可能性。 • 选择 **On**，扫描主机获取信息，识别操作系统。 • 选择**关闭 (Off)**，继续使用主机的思科操作系统信息。	`-o`
将所有主机视为在线 (Treat All Hosts As Online)	启用此选项，可跳过主机发现过程，在目标范围内的每台主机上运行端口扫描。请注意，启用此选项时，Nmap 会忽略**主机发现方法 (Host Discovery Method)** 和**主机发现端口列表 (Host Discovery Port List)** 的设置。 • 要跳过主机发现过程，在目标范围中的每台主机上运行端口扫描，请选择**打开 (On)**。 • 要使用**主机发现方法 (Host Discovery Method)** 和**主机发现端口列表 (Host Discovery Port List)** 设置执行主机发现，并跳过任何不可用的主机上的端口扫描，请选择**关闭 (Off)**。	`-PN`

选项	说明	对应的 Nmap 选项
主机发现方法 (Host Discovery Method)	选择此选项，在**主机发现端口列表 (Host Discovery Port List)** 中列出的端口上，为目标范围中的所有主机执行主机发现，或者，如未列出端口，则在适用于主机发现方法的默认端口上执行。 然而，请注意，如也启用**将所有主机视为在线 (Treat All Hosts As Online)**，**主机发现方法 (Host Discovery Method)** 选项不起作用，也不执行主机发现。 选择 Nmap 进行测试以查看主机是否存在且可用时使用的方法： • 如果收到响应，**TCP SYN** 选项将发送设置了 SYN 标记的空 TCP 数据包，并认为主机可用。默认情况下，TCP SYN 扫描端口 80。请注意，TCP SYN 扫描不太可能被设有状态性防火墙规则的防火墙拦截。 • 如果收到响应，**TCP ACK** 选项将发送设置了 ACK 标志的空 TCP 数据包，并认为主机可用。默认情况下，TCP ACK 也扫描端口 80。请注意，TCP ACK 扫描不太可能被设有无状态防火墙规则的防火墙拦截。 • 如果端口不可达响应来自已关闭端口，**UDP** 选项将发送 UDP 数据包，并假设主机可用性。默认情况下，UDP 扫描端口 40125。	**TCP SYN**: `-PS` **TCP ACK**: `-PA` **UDP**: `-PU`
主机发现端口列表 (Host Discovery Port List)	指定在执行主机发现时要扫描的自定义端口列表，用逗号隔开。	主机发现方法端口列表
默认 NSE 脚本 (Default NSE Scripts)	启用此选项，可以运行默认 Nmap 脚本集，执行主机发现以及服务器、操作系统和漏洞检测。请登录 https://nmap.org/nsedoc/categories/default.html，查看默认脚本列表。 • 要运行默认 Nmap 脚本集，请选择**打开 (On)**。 • 要跳过默认 Nmap 脚本集，请选择**关闭 (Off)**。	`-sC`
计时模板 (Timing Template)	选择扫描过程的时间；选择的数字越大，扫描越快、越不全面。	**0**: `T0` (paranoid) **1**: `T1` (sneaky) **2**: `T2` (polite) **3**: `T3` (normal) **4**: `T4` (aggressive) **5**: `T5` (insane)

Nmap 扫描准则

尽管主动扫描可以获取宝贵信息，但过度使用 Nmap 等工具可能会使您的网络资源超载，甚至使重要的主机瘫痪。使用任何主动式扫描工具时，应遵循这些准则创建扫描策略，确保仅扫描需要扫描的主机和端口。

选择适当的扫描目标

配置 Nmap 时，可创建扫描目标以识别要扫描的主机。扫描目标包括一个 IP 地址、CIDR 块或八位字节 IP 地址范围、IP 地址范围或要扫描的 IP 地址或范围列表，以及一台或多台主机上的端口。

可通过以下方式指定目标：

- 对于 IPv6 主机：
  - 确切的 IP 地址（例如 `2001:DB8:1::178:ABCD`）
- 对于 IPv4 主机：
  - 精确的 IP 地址（例如，`192.168.1.101`）或 IP 地址列表（用逗号或空格隔开）
  - 使用 CIDR 表示法的 IP 地址块（例如，`192.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254（含）之间的 254 台主机）
  - 使用八位字节范围寻址的 IP 地址范围（例如，`192.168.0-255.1-254` 扫描 192.168.x.x 范围内的所有地址，但以 .0 和 .255 结尾的地址除外）
  - 使用连字符的 IP 地址范围（例如，`192.168.1.1 - 192.168.1.5` 扫描在 192.168.1.1 和 192.168.1.5（含）之间的六台主机）
  - 地址或范围列表，用逗号或空格隔开（例如，`192.168.1.0/24`，`194.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254（含）之间的 254 台主机，以及 194.168.1.1 和 194.168.1.254（含）之间的 254 台主机）

Nmap扫描的理想扫描目标包括有系统无法识别的操作系统的主机、有无法识别的服务器的主机，或者最近在网络上检测到的主机。请记住，Nmap 结果不能添加到不存在于网络映射中主机的网络映射。

⚠

注意

- Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。
- 如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。
- 请确保您有权限扫描您的目标。使用 Nmap 扫描不属于您或贵公司的主机可能违法。

选择适当端口进行扫描

可为已配置的每个扫描目标选择要扫描的端口。您可以指定各个端口号、端口范围或一系列端口号和端口范围，识别应当在每个目标上扫描的精确端口集。

默认情况下，Nmap 扫描 TCP 端口 1 至端口 1024。如果计划将补救用作关联政策中的响应，则可使补救仅扫描在触发关联响应的事件中指定的端口。如果按需运行补救或将补救作为预定任务加以运行，或者，如不使用来自事件的端口，则可使用其他端口选项确定哪些端口已扫描。可选择仅扫描在 `nmap-services` 文件中列出的 TCP 端口，忽略其他端口设置。除 TCP 端口外，还可扫描 UDP 端口。请注意，扫描UDP端口可能比较耗时，因此，如要快速扫描，请避免使用此选项。为选择要扫描的特定端口或端口范围，请使用 Nmap 端口规范语法识别端口。

设置主机发现选项

在开始主机的端口扫描之前，可决定是否执行主机发现，或者，可假设计划要扫描的所有主机均在线。如果选择不将所有主机视为在线，则可选择要使用的主机发现方法，如果需要，自定义在主机发现过程中扫描的端口列表。主机发现不能从已列出端口探测操作系统或服务器信息；它仅使用特殊端口上的响应确定主机是否活动且可用。如果执行主机发现且主机不可用，Nmap则不扫描该主机上的端口。

示例：使用 Nmap 解析未知操作系统

本示例介绍用于解析未知操作系统的 Nmap 配置。有关 Nmap 配置的完整介绍，请参阅 管理 Nmap 扫描 ， 第 26 页。

如果系统无法确定网络上主机的操作系统，则可使用Nmap主动扫描主机。Nmap使用其通过扫描获取的信息对可能的操作系统进行评级。然后，它使用评级最高的操作系统作为主机操作系统标识。

使用 Nmap 向新主机质询操作系统和服务器信息，会停用系统对已扫描主机的该数据进行的监控。如果使用 Nmap 发现系统标记为拥有未知操作系统的主机的主机操作系统和服务器操作系统，您也许能够识别相似的主机组。然后，可根据其中一个主机组创建自定义指纹，使系统能够根据 Nmap 扫描，将指纹与已知在主机上运行的操作系统相关联。尽可能创建自定义指纹，而不是通过第三方来源（例如，Nmap）输入静态数据，因为自定义指纹允许系统继续监控主机操作系统并按需更新。

在本例中，您将：

1. 配置扫描实例，如添加 Nmap 扫描实例 ， 第 27 页中所述。
2. 使用以下设置创建 Nmap 补救：
   - 启用 **Use Port From Event**，可扫描与新服务器相关的端口。
   - 启用**检测操作系统 (Detect Operating System)**，可检测主机的操作系统信息。
   - 启用**探测开放端口以了解厂商和版本信息 (Probe open ports for vendor and version information)**，可检测服务器厂商和版本信息。
   - 启用**将所有主机视为在线 (Treat All Hosts as Online)**，因为已知该主机存在。
3. 创建在系统检测到具有未知操作系统的主机时触发的关联规则。该规则应在**发生发现事件**并且**主机的操作系统信息已更改**且符合以下条件时触发：**操作系统名称未知**。

4. 创建包含关联规则的关联策略。
5. 在关联策略中，将第 2 步中创建的 Nmap 补救作为响应添加至第 3 步中创建的规则。
6. 激活关联策略。
7. 清除网络映射上的主机，强制网络发现重新启动，重建网络映射。
8. 一两天后，搜索关联策略生成的事件。分析在主机上检测到的操作系统的Nmap结果，弄清网络上是否有系统无法识别的特殊主机配置。
9. 如果发现未知操作系统的Nmap结果相同的主机，请为其中一台主机创建自定义指纹，并用它识别未来的类似主机。

相关主题

创建 Nmap 补救，第 30 页
Nmap 扫描结果，第 33 页
为客户端创建自定义指纹，第 6 页

示例：使用 Nmap 响应新主机

此示例介绍旨在对新主机作出响应的 Nmap 配置。有关 Nmap 配置的完整介绍，请参阅 管理 Nmap 扫描，第 26 页。

当系统在子网中检测到可能被入侵的新主机时，您可能想扫描该主机，确保获取该主机漏洞的准确信息。

要完成此操作，可创建和激活关联策略，当子网中出现新主机时进行检测，并启动补救以对该主机执行 Nmap 扫描。

为此，将会执行以下操作：

1. 配置扫描实例，如添加 Nmap 扫描实例，第 27 页中所述。
2. 使用以下设置创建 Nmap 补救：
   - 启用 **Use Port From Event**，可扫描与新服务器相关的端口。
   - 启用**检测操作系统 (Detect Operating System)**，可检测主机的操作系统信息。
   - 启用**探测开放端口以了解厂商和版本信息 (Probe open ports for vendor and version information)**，可检测服务器厂商和版本信息。
   - 启用**将所有主机视为在线 (Treat All Hosts as Online)**，因为已知该主机存在。
3. 创建当系统在特定子网上检测到新主机时触发的关联规则。此规则应在**发生发现事件**并**检测到新主机时**触发。
4. 创建包含关联规则的关联策略。
5. 在关联策略中，将在以前步骤中创建的 Nmap 补救作为响应添加至在第 3 步中创建的规则。
6. 激活关联策略。

7. 收到出现新主机的通知时，检查主机配置文件，以查看Nmap扫描结果并解决适用于该主机的任何漏洞。

激活策略后，可以定期检查补救状态视图（**分析** > **关联** > **状态**）以查看补救启动时间。补救的动态扫描目标应当包括因服务器检测而扫描到的主机的 IP 地址。根据 Nmap 检测到的操作系统和服务器，查看这些主机的主机配置文件，弄清主机上是否存在需要解决的漏洞。

注意 如有大型或动态网络，新主机检测可能太频繁，而无法使用扫描进行响应。为防止资源超载，请避免使用 Nmap 扫描响应频繁发生的事件。另请注意，如果使用 Nmap 向新主机质询操作系统和服务器信息，则会停用思科对已扫描主机的该数据进行的监控。

相关主题

创建 Nmap 补救，第 30 页

管理 Nmap 扫描

要使用 Nmap 扫描，至少必须配置一个 Nmap 扫描实例和一个 Nmap 补救。是否配置 Nmap 扫描目标可以选择。

过程

步骤 1 配置 Nmap 扫描：

- 如添加 Nmap 扫描实例，第 27 页中所述，添加 Nmap 扫描实例。
- 如创建 Nmap 补救，第 30 页中所述，创建 Nmap 补救。
- 或者，也可以如添加 Nmap 扫描目标，第 28 页中所述，添加 Nmap 扫描目标。

步骤 2 运行 Nmap 扫描：

- 如运行按需 Nmap 扫描，第 32 页中所述，运行按需 Nmap 扫描。
- 如《Cisco Secure Firewall Management Center 管理指南》的*Nmap* 扫描自动化中所述，配置自动 Nmap 扫描。
- 如《Cisco Secure Firewall Management Center 管理指南》的安排 *Nmap* 扫描中所述，安排自动 Nmap 扫描。

下一步做什么

- 通过查看相关任务，监控正在进行的 Nmap 扫描；请参阅《Cisco Secure Firewall Management Center 管理指南》中的查看任务消息。
- 或者，也可以优化扫描：
  - 如编辑 Nmap 扫描实例，第 28 页中所述，编辑 Nmap 扫描实例。

- 如编辑 Nmap 扫描目标，第 29 页中所述，编辑 Nmap 扫描目标。
- 如编辑 Nmap 补救，第 32 页中所述，编辑 Nmap 补救。

添加 Nmap 扫描实例

可为要用于扫描网络漏洞的每个 Nmap 模块设置独立的扫描实例。可为 Cisco Secure Firewall Management Center上的本地 Nmap 模块以及要用于远程运行扫描的任何设备设置扫描实例。每次扫描的结果始终存储在 管理中心上，可在这里配置扫描，即使是从远程设备运行扫描。为防止意外或恶意扫描关键任务主机，可创建实例黑名单，指出不应通过实例扫描的主机。

不能添加名称与任何现有扫描实例相同的扫描实例。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略** > **操作** > **实例**。
- 选择**策略** > **操作** > **扫描程序**。

步骤 2 添加补救：

- 如果通过上述第一种方法访问列表，请找到“添加新实例”(Add a New Instance) 部分，从下拉列表中选择“Nmap 补救”(Nmap Remediation) 模块，然后点击**添加 (Add)**。
- 如果通过上述第二种方法访问该列表，请点击**添加 Nmap 实例 (Add Nmap Instance)**。

步骤 3 输入**实例名称 (Instance Name)**。

步骤 4 输入**说明**。

步骤 5 或者，在**豁免的主机 (Exempted hosts)** 字段中，使用以下语法指定任何 绝不应使用此扫描实例扫描的主机或网络：

- 对于 IPv6 主机，精确的 IP 地址（例如，`2001:DB8::fedd:eeff`）
- 对于 IPv4 主机，精确的 IP 地址（例如，`192.168.1.101`）或使用 CIDR 表示法的 IP 地址块（例如，`192.168.1.0/24` 扫描 `192.168.1.1` 和 `192.168.1.254` [含] 之间的 254 台主机）
- 请注意，不能使用感叹号 (!) 否定地址值。

注释 如果明确将黑名单网络中的主机作为扫描目标，该扫描将不运行。

步骤 6 或者，要从远程设备而非管理中心运行扫描，请在**远程设备名称 (Remote Device Name)** 字段中指定设备的 IP 地址或名称，因为它会显示在 管理中心 Web 界面中的设备“信息”(Information) 页面中。

步骤 7 点击**创建**。
系统创建完实例后，以编辑模式显示实例。

步骤 8 或者，将 Nmap 补救添加到实例。为此，请找到实例的“已配置补救”(Configured Remediations) 部分，点击**添加 (Add)**，然后创建补救，如创建 Nmap 补救，第 30 页中所述。

步骤 9 点击**取消 (Cancel)**，返回实例列表。

注释　如果您通过**扫描程序 (Scanners)** 访问 Nmap 扫描实例列表，系统不会显示您添加的实例，除非您也将补救添加到该实例。要查看尚未添加补救的实例，请使用**实例 (Instances)** 菜单选项访问列表。

编辑 Nmap 扫描实例

当编辑扫描实例时，可以查看、添加和删除与实例关联的补救。不再想使用 Nmap 扫描实例中描述的 Nmap 模块时，请删除该 Nmap 扫描实例。请注意，如果删除扫描实例，也将删除使用该实例的任何补救。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略** > **操作** > **实例**。
- 选择**策略** > **操作** > **扫描程序**。

步骤 2 在要编辑的实例旁，点击 **视图**（）。

步骤 3 对扫描实例设置进行更改，如添加 Nmap 扫描实例，第 27 页中所述。

步骤 4 点击**保存 (Save)**。

步骤 5 点击 **Done**。

下一步做什么

- 或者，将新补救添加到扫描实例；请参阅 创建 Nmap 补救，第 30 页
- 或者，编辑与实例关联的补救；请参阅编辑 Nmap 补救，第 32 页。
- 或者，删除与实例关联的补救；请参阅运行按需 Nmap 扫描，第 32 页。
- 或者，通过点击扫描目标旁边的 **删除**（） 来删除扫描实例。

添加 Nmap 扫描目标

配置 Nmap 模块时，可创建和保存扫描目标，识别想在执行按需或预定扫描时作为扫描目标的主机和端口，从而避免每次构建新扫描目标。扫描目标包括一个或一组要扫描的 IP 地址，以及一台或多台主机上的端口。对于 Nmap 目标，也可使用 Nmap 八位字节范围寻址或 IP 地址范围。有关 Nmap 八位组范围寻址的详细信息，请参阅 http://insecure.org 上的 Nmap 文档。

注意：

- 扫描包含大量主机的扫描目标可能需要延长的时间。作为一种解决方法，每次仅扫描几台主机。

- Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。

过程

步骤 1 选择**策略** > **操作** > **扫描程序**。

步骤 2 在工具栏上，点击 **Targets**。

步骤 3 点击 **Create Scan Target**。

步骤 4 在**名称 (Name)** 字段中，输入要用于此扫描目标的名称。

步骤 5 在 **IP 范围 (IP Range)** 文本框中，使用Nmap 扫描准则，第 23 页中所述的语法指定要扫描的一个或多个主机。

注释 如果在扫描目标中的 IP 地址或范围列表中使用逗号，则保存目标时，逗号将转换为空格。

步骤 6 在**端口 (Ports)** 字段中，指定要扫描的端口。

可使用从 1 到 65535 的值输入以下任意项：

- 端口号
- 用逗号分隔的端口列表
- 用连接号分隔的端口号范围
- 多个用连接号分隔的端口号范围，用逗号分隔

步骤 7 点击**保存 (Save)**。

编辑 Nmap 扫描目标

提示 如果不想使用补救扫描特定 IP 地址，但是该 IP 地址已添加至目标，则可能想编辑补救的动态扫描目标，因为主机参与了启动补救的关联策略违反事件。

如果不再想扫描已在扫描目标中列出的主机，请删除扫描目标。

过程

步骤 1 选择**策略** > **操作** > **扫描程序**。

步骤 2 在工具栏上，点击 **Targets**。

步骤 3 点击要编辑的扫描目标旁边的 **编辑**（）。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 按需进行修改。有关详细信息，请参阅添加 Nmap 扫描目标，第 28 页。

步骤 5 点击**保存 (Save)**。

步骤 6 或者，通过点击扫描目标旁边的 **删除**（  ） 来删除扫描目标。

创建 Nmap 补救

Nmap补救只可以通过将它添加到现有Nmap扫描实例来创建。补救定义了扫描的设置。它可用作关联策略中的响应、按需运行或在指定时间作为预定任务运行。

Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。

有关 Nmap 功能的一般信息，请参阅 http://insecure.org 上的 Nmap 文档。

开始之前

- 如添加 Nmap 扫描实例，第 27 页中所述，添加 Nmap 扫描实例。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 点击要添加补救的实例旁边的 **视图**（）。

步骤 3 在“已配置补救”(Configured Remediations) 部分，点击**添加 (Add)**。

步骤 4 输入**补救名称 (Remediation Name)**。

步骤 5 输入**说明**。

步骤 6 如果计划使用此补救响应在发生入侵事件、连接事件或用户事件时触发的关联规则，请配置**扫描事件中的哪个地址？(Scan Which Address(es) From Event?)** 选项。

提示 如果计划使用此补救响应在发生发现事件或主机输入事件时触发的关联规则，默认情况下，补救将扫描事件涉及到的主机的 IP 地址；无需配置此选项。

注释 请**勿**为了响应在流量配置文件发生变化时触发的关联规则而分配 Nmap 补救。

步骤 7 配置**扫描类型 (Scan Type)** 选项。

步骤 8 或者，除了 TCP 端口，还要扫描 UDP 端口，请为**扫描 UDP 端口 (Scan for UDP ports)** 选项选择**开启 (On)**。

提示 UDP 端口扫描比 TCP 端口扫描需要更多的时间。要加速扫描，请禁用此选项。

步骤 9 如果计划使用此补救响应关联策略违反事件，请配置**使用事件中的端口 (Use Port From Event)** 选项。

步骤 10 如果计划使用此补救响应关联策略违反事件，并希望使用运行检测引擎来检测事件的设备运行扫描，请配置**从报告检测引擎扫描 (Scan from reporting detection engine)** 选项。

步骤 11 配置**快速端口扫描 (Fast Port Scan)** 选项。

步骤 12 在**端口范围和扫描顺序 (Port Ranges and Scan Order)** 字段中，输入要在默认情况下使用 Nmap 端口规范语法按自己想要的顺序扫描的端口。

使用以下格式：

- 指定从 1 到 65535 的值。
- 使用逗号或空格分隔端口。
- 使用连字符指明端口范围。
- 扫描 TCP 和 UDP 端口时，以 T 作为要扫描的 TCP 端口列表的开端，以 U 作为 UDP 端口列表的开端。

注释 启动补救以响应关联策略违反事件时，**使用事件中的端口 (Use Port From Event)** 选项将覆盖此设置，如第 8 步中所述。

示例：

要扫描 UDP 流量的端口 53 和 111，然后扫描 TCP 流量的端口 21-25，请输入 `U:53,111,T:21-25`。

步骤 13 要探测开放端口以了解服务器厂商和版本信息，请配置**探测开放端口以获取供应商和版本信息 (Probe open ports for vendor and version information)**。

步骤 14 如果选择探测开放端口，请从**服务版本强度 (Service Version Intensity)** 下拉列表中选择一个数字，设置使用的探针数量。

步骤 15 要扫描操作系统信息，请配置**检测操作系统 (Detect Operating System)** 设置。

步骤 16 要确定主机发现是否发生，是否仅针对可用端口运行端口扫描，请配置**将所有主机视为在线 (Treat All Hosts As Online)**。

步骤 17 要设置希望 Nmap 在测试主机可用性时使用的方法，请从**主机发现方法 (Host Discovery Method)** 下拉列表中选择一种方法。

步骤 18 如果要在主机发现过程中扫描自定义端口列表，请在**主机发现端口列表 (Host Discovery Port List)** 字段中输入适合所选主机发现方法的端口列表，用逗号隔开。

步骤 19 配置**默认 NSE 脚本 (Default NSE Scripts)** 选项，控制是否使用默认 Nmap 脚本集进行主机发现以及服务器、操作系统和漏洞发现。

提示 请参阅 http://nmap.org/nsedoc/categories/default.html，获取默认脚本列表。

步骤 20 要设置扫描过程的时间选择，请从**计时模板 (Timing Template)** 下拉列表中选择计时模板编号。

选择的编号越大，速度越快，扫描越不全面；而选择的编号越小，速度越慢，扫描越全面。

步骤 21 点击**创建**。
系统创建完补救后，在编辑模式中显示它。

步骤 22 点击**完成 (Done)** 以返回相关实例。

步骤 23 点击**确定 (OK)** 以返回实例列表。

相关主题

Nmap 补救选项，第 18 页

编辑 Nmap 补救

对 Nmap 补救所做的更改不会影响正在进行的扫描。新设置将在下一次扫描开始时生效。删除不再需要的 Nmap 补救。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略** > **操作** > **实例**。
- 选择**策略** > **操作** > **扫描程序**。

步骤 2 访问要编辑的补救：

- 如果通过上述第一种方法访问列表，请点击相关实例旁的**视图**（）），然后在要在“已配置补救”部分中编辑的补救旁边再次点击该补救。
- 如果通过上述第二种方法访问列表，请点击要编辑的补救边的 **视图**（）。

步骤 3 根据需要进行修改，如创建 Nmap 补救，第 30 页中所述。

步骤 4 如果要保存更改，请点击**保存 (Save)**，或者如果要不保存而直接退出，请点击**完成 (Done)**。

步骤 5 或者，通过点击补救旁边的 **删除**（） 来删除补救。

运行按需 Nmap 扫描

可在需要时启动按需 Namp 扫描。可以通过输入要扫描的 IP 地址和端口或者通过选择现有扫描目标，指定按需扫描目标。

Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。

开始之前

- 或者，添加 Nmap 扫描目标；请参阅添加 Nmap 扫描目标，第 28 页。

过程

步骤 1 选择**策略** > **操作** > **扫描程序**。

步骤 2 在要用于执行扫描的 Nmap 补救旁，点击 **扫描** （）。

步骤 3 或者，要使用已保存的扫描目标进行扫描，请从**已保存的目标 (Saved Targets)** 下拉列表中选择目标，然后点击**加载 (Load)**。

步骤 4 在 **IP 范围 (IP Range[s])** 字段中，指定要扫描或修改已加载列表的主机的 IP 地址。

注意：

- 对于带 IPv4 地址的主机，可指定多个 IP 地址，用逗号隔开，或者使用 CIDR 表示法。也可在 IP 地址前面添加感叹号 (!)，否定 IP 地址。
- 对于带 IPv6 地址的主机，请使用精确的 IP 地址。不支持地址范围。

步骤 5 在**端口 (Ports)** 字段中，指定要扫描的端口或修改已加载的列表。

可输入一个端口号、用逗号隔开的端口列表或者用连接号隔开的端口号范围。

步骤 6 点击 **Scan Now**。

下一步做什么

- 或者，监控任务状态；请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 查看任务消息 。

Nmap 扫描结果

您可以监控正在进行的Nmap扫描，导入先前通过Firepower系统执行的扫描中的结果或在Firepower系统外执行的结果，以及查看和分析扫描结果。

您可查看作为弹出窗口中渲染页面的扫描结果（使用本地Nmap模块创建），也可下载原始XML格式的 Nmap 结果文件。

您还可在主机配置文件和网络映射中查看由 Nmap 检测到的操作系统和服务器信息。如果主机扫描为已过滤或已关闭端口上的服务器生成服务器信息，或者如果扫描收集无法包含在操作系统信息或服务器部分中的信息，主机配置文件会将这些结果纳入“Nmap 扫描结果”(Nmap Scan Results) 部分。

查看 Nmap 扫描结果

当 Nmap 扫描完成后，可以查看扫描结果表。

可以根据所查找的信息操作结果视图。您在访问扫描结果时看到的页面将随您所使用的工作流程而变化。可使用预定义的工作流程，其中包括扫描结果表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

可在 http://insecure.org 上下载 Nmap 结果，并使用 Nmap 1.01 DTD 查看。

还可清除扫描结果。

过程

步骤 1 选择策略 > 操作 > 扫描程序。

步骤 2 在工具栏上，点击扫描结果 (Scan Results)。

步骤 3 有以下选项可供选择：

- 调整时间范围，如《Cisco Secure Firewall Management Center 管理指南》中的事件时间限制所述。
- 要使用不同的工作流程，包括自定义工作流程，请按工作流程标题点击 **(switch workflows)** 。
- 要查看作为弹出窗口中页面已渲染的扫描结果，请点击扫描作业旁的查看。
- 要保存扫描结果文件的副本，以便在任何文本编辑器中查看原始 XML 代码，请在扫描作业旁点击下载 (Download)。
- 要对扫描结果排序，请点击列标题。再次点击列标题以反转排列顺序。
- 要限制显示的列，请在要隐藏的列标题中点击关闭（×）。在显示的弹出窗口中，点击**Apply**。

  提示 要隐藏或显示其他列，请选中或清除相应的复选框，然后点击应用 (Apply)。要将已禁用列添加回视图中，请点击展开箭头展开搜索限制条件，然后点击已禁用列 (Disabled Columns) 下的列名称。

- 要向下展开到工作流程中的下一个页面，请参阅《Cisco Secure Firewall Management Center 管理指南》中的使用向下钻取页面。
- 要配置扫描实例和补救，请点击工具栏中的扫描工具 并参阅管理 Nmap 扫描 ， 第 26 页。
- 要在工作流程页面之内及在各工作流程页面之间导航，请参阅《Cisco Secure Firewall Management Center 管理指南》中的工作流程页面导航工具。
- 要导航至其他事件视图以查看关联的事件，请从跳至 (Jump to) 下拉列表中选择要查看的事件视图的名称。
- 要搜索扫描结果，请在相应字段中输入搜索条件。

相关主题

Nmap 扫描结果字段 ， 第 34 页

Nmap 扫描结果字段

运行 Nmap 扫描时，管理中心 在数据库中收集扫描结果。下表介绍了扫描结果表中可以查看和搜索的字段。

表 2: 扫描结果字段

字段	说明
开始时间	生成结果的扫描的开始日期和时间。
结束时间	生成结果的扫描的结束日期和时间。

字段	说明
目标	生成结果的扫描的扫描目标的 IP 地址（或主机名，如果 DNS 解析已启用）。
扫描类型 (Scan Type)	要么是 Nmap，要么是第三方扫描工具的名称，指明生成结果的扫描的类型。
扫描模式 (Scan Mode)	生成结果的扫描的模式： • On Demand - 来自按需扫描的结果。 • 导入 - 来自不同系统上扫描的结果，和已导入 管理中心的结果。 • 预定 (Scheduled) - 来自作为预定任务运行的扫描的结果。
结果	扫描的结果。
域	扫描目标的域。此字段只存在于多域部署中。

导入 Nmap 扫描结果

您可以导入在系统外执行的 Nmap 扫描所创建的 XML 结果文件。您还可以导入先前从系统下载的 XML 结果文件。要导入 Nmap 扫描结果，结果文件必须采用 XML 格式，且兼容于 Nmap 1.01 DTD。有关创建 Nmap 结果的详细信息以及 Nmap DTD 的详细信息，请参阅 http://insecure.org 上的 Nmap 文档。

主机必须已存在于网络映射中，然后 Nmap 才能将其结果附加到主机配置文件。

过程

步骤 1 选择**策略** > **操作** > **扫描程序**。

步骤 2 在工具栏上，点击 **Import Results**。

步骤 3 点击**浏览 (Browse)**，导航至结果文件。

步骤 4 返回“导入结果”(Import Results) 页面后，点击**导入 (Import)**，导入结果。

主机身份源的历史记录

功能	最低 管理中心	最低 威胁防御	详情
主机输入数据功能的安全性改进	6.5	任意	TLS 1.2 现在被用于 管理中心 和主机输入客户端之间的通信。该主题配置主机输入客户端， 第 17 页已使用此信息进行更新。

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。