Firepower 系统主机输入 API 指南

思科系统公司
www.cisco.com

思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices

版本 6.0
2016 年 8 月 12 日

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上述供应商不承诺所有明示或暗示的担保，包括（但不限于）对特定用途的适销性、适用性、非侵权性以及因交易、使用或商业惯例所衍生的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

了解主机输入

Firepower 管理中心提供一种从网络上的其他源导入数据来扩充受监控主机信息的工具。

使用主机输入 API 提交网络映射信息有两种方式：一种是在管理中心上运行 nmimport 工具，另一种是使用远程客户端。在任一情况下，都需要在具有逗号分隔值（CSV 格式）的文本文件中指定网络映射详细信息。使用主机输入导入工具（第 2-1 页）提供一般说明，定义 CSV 文件格式，并介绍如何使用 nmimport 工具。配置主机输入客户端（第 3-1 页）介绍如何使用主机导入客户端。

例如，如果是设置新的 Firepower 系统，则可能要确保资产管理软件中列出的所有计算机都存在于网络映射中。您可以从资产管理应用导出主机数据，将结果格式化为适当格式化的文本文件，并使用主机输入导入工具来导入主机数据。如果资产管理系统包括每台主机的操作系统信息，则可以设置资产管理系统的第三方产品映射，并将每个第三方操作系统标签映射到对应的思科标签。可以在运行导入之前设置该映射，并且系统会将相应的思科操作系统定义与每台主机相关联。

将主机输入导入工具与 Firepower 管理中心结合使用要执行四个主要步骤：

1. 如果要使用第三方主机数据执行影响关联，则可以使用管理中心 Web 界面配置第三方产品映射，以将服务、操作系统或修复定义映射到思科产品或修复定义。
2. 如果要导入第三方漏洞，则可以使用管理中心 Web 界面配置第三方漏洞映射，以将第三方漏洞标识字符串映射到思科漏洞 ID。请注意，您也可以在导入文件中执行此映射。
3. 从第三方应用导出数据并将其格式化为 CSV 文件，如使用主机输入导入工具（第 2-1 页）中所述。
4. 使用 nmimport 工具或主机输入客户端提交 CSV 文件。

必备条件

要了解本指南中的信息，您应熟悉 Firepower 管理中心的特性和术语定义及其组件的功能（尤其是网络映射），以及系统生成的各种相关事件数据。有关这些功能连同不熟悉或产品特定的术语定义的信息，可以从《*Firepower 管理中心配置指南*》获取。有关本指南中记录的数据字段的其他信息，也可以从该《*配置指南*》获取。

产品版本兼容性

下表介绍各种主机输入功能所需的产品版本：

表 1-1　　产品版本兼容性

功能	产品版本
主机输入功能	Firepower 管理中心版本 4.9+
主机输入外部客户端功能	Firepower 管理中心版本 5.0+
主机输入移动设备识别功能	Firepower 管理中心版本 5.1+

表 1-1 产品版本兼容性（续）

功能	产品版本
IPv6 地址支持	Firepower 管理中心版本 5.2+
多域支持	Firepower 管理中心版本 6.0+

文档约定

下表列出本书中用于介绍主机输入调用中所采用的各种数据字段格式的名称。

表 1-2 密钥值数据类型约定

数据类型	说明
uint	无符号整数
uint8	无符号 8 位整数
uint32	无符号 32 位整数
string	包含字符数据的变长字节。

主机输入脚本资源

以下介绍文档中说明的某些主题以及可查找详细信息的位置。

表 3 主机输入资源

如需了解有关以下主题的更多信息...	请在以下位置查找相关信息...
主机输入导入工具	使用主机输入导入工具（第 2-1 页）
有关编写用于主机输入导入工具的导入文件的准则	编写主机输入导入文件（第 2-3 页）
要在导入文件中包含的特定主机输入函数的语法	主机输入导入语法（第 2-6 页）
运行主机输入导入工具	运行主机输入导入（第 2-25 页）
安装、配置和运行主机输入参考客户端	使用主机输入参考客户端（第 3-2 页）

使用主机输入导入工具

您可以通过创建导入文件并使用主机输入导入工具对其进行处理来将数据导入到网络映射。

有关详细信息，请参阅以下各节：

准备运行主机输入导入

某些主机导入操作取决于您使用管理中心 Web 界面将第三方产品、修复及漏洞名称和 ID 映射到思科数据库中的定义所提供的产品映射信息。根据计划导入的数据，在运行导入之前可能需要执行以下各节描述的配置步骤：

创建第三方漏洞映射

如果要导入数据（包括第三方漏洞）并将该数据用于影响关联，则在导入数据之前必须创建第三方漏洞映射集。通过第三方映射集，系统可以将第三方漏洞 ID 转换为对应的思科漏洞 ID。如果在导入之前不映射第三方漏洞，则该漏洞不会映射到思科漏洞 ID，并且无法用于影响关联。可以通过两种方式创建映射集：使用管理中心 Web 界面或使用 `AddScanResult` 命令。如果使用此命令导入扫描结果，请务必在网络发现策略中编辑输入源的源定义，以将身份源类型设置为“扫描程序”(Scanner)。

可以在任何域级别创建第三方漏洞映射。使用 `SetMap` 命令可指定要用于映射的映射名称。必须在 CSV 文件或其父级之一中使用的网络映射上定义映射。

有关通过 Web 界面映射第三方漏洞的详细信息，请参阅《*Firepower 管理中心配置指南*》。有关 `SetMap` 和 `AddScanresult` 命令的详细信息，请参阅了解导入文件格式（第 2-3 页）。

创建第三方产品映射

将操作系统或服务器数据导入到主机时，您可以将第三方产品名称详细信息映射到思科产品定义。可以通过管理中心 Web 界面创建第三方产品映射。

通过第三方产品映射集，系统可以将第三方供应商、产品和版本转换为对应的思科定义。当设置包含服务器定义或操作系统定义的第三方产品映射时，如果使用 API 添加或设置第三方服务器或操作系统，那么之后在同一脚本中为其定义显示字符串即可。

如果使用第三方产品映射将第三方修复映射到思科修复定义，设置产品映射，然后使用第三方修复名称将修复添加到主机，则系统会将修复映射到相应的思科修复定义并停用由该修复处理的漏洞。

要将第三方产品映射到思科产品定义，请执行以下操作：

访问权限：管理员

1. 依次选择**策略 (Policies) > 应用检测器 (Application Detectors)**，然后点击**用户第三方映射 (User Third-Party Mappings)**。

   系统将显示“用户第三方映射”(User Third-Party Mappings) 页面。

2. 您有两种选择：

- 要编辑现有映射集，请点击映射集旁边的**编辑 (Edit)**。
- 要创建新的映射集，请点击**创建产品映射集 (Create Product Map Set)**。

  系统将显示“编辑第三方产品映射”(Edit Third-Party Product Mappings) 页面。

3. 在**映射集名称 (Mapping Set Name)** 字段中，键入映射集的名称。
4. 在**说明 (Description)** 字段中键入说明。
5. 您有两种选择：

- 要映射第三方产品，请点击**添加产品映射 (Add Product Map)**。
- 要编辑现有第三方产品映射，请点击映射集旁边的**编辑 (Edit)**。

  系统将显示“添加产品映射”(Add Product Map) 页面。

6. 在**供应商字符串 (Vendor String)** 字段中，键入第三方产品使用的供应商字符串。
7. 在**产品字符串 (Product String)** 字段中，键入第三方产品使用的产品字符串。
8. 在**版本字符串 (Version String)** 字段中，键入第三方产品使用的版本字符串。
9. 在**产品映射 (Product Mappings)** 部分中，从以下列表中选择要用于漏洞映射的操作系统、产品和版本（如果适用）：

- 供应商
- 产品
- 主版本
- 次版本
- 修订版本
- 内部版本
- 补丁
- 扩展

  例如，如果想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 中的漏洞，请选择 **Redhat, Inc.** 作为供应商，**Redhat Linux** 作为产品以及 **9** 作为版本。

10. 点击**保存 (Save)**。

    在创建第三方产品映射后，可以使用 `SetOS`、`SetService` 或 `AddService` 命令导入数据。请注意在导入数据之前的第三方产品名称详细信息和思科产品定义。

要查找第三方和思科产品详细信息，请执行以下操作：

访问权限：管理员

1. 依次选择**策略 (Policies) > 应用检测器 (Application Detectors)**。

   系统将显示“应用检测器”(Application Detectors) 页面。

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

   系统将显示“第三方产品映射”(Third-Party Product Mappings) 页面。

3. 点击产品映射集的编辑图标 ( )。

   系统将显示“编辑第三方产品映射”(Edit Third-Party Product Mappings) 页面。

4. 点击产品映射的编辑图标 ( )。

   系统将显示“添加产品映射”(Add Product Map) 弹出窗口。请注意**供应商字符串 (Vendor String)**、**产品字符串 (Product String)** 和**版本字符串 (Version String)** 值。

   有关映射第三方产品的详细信息，请参阅《*Firepower 管理中心配置指南*》。

编写主机输入导入文件

本章提供有关使用主机输入导入工具的导入命令来导入数据的语法的详细信息。当编写导入文件时，请确保按照以下各节提供的说明进行操作：

- 了解导入文件格式（第 2-3 页）
- 设置域（第 2-4 页）
- 设置源类型（第 2-4 页）
- 设置源 ID（第 2-5 页）
- 设置第三方产品映射（第 2-5 页）

了解导入文件格式

一般而言，导入文件是一个文本文件，其中每行包含一个命令，并以逗号分隔值（CSV 格式）指定命令参数。必须将几个关键命令置于文件开头（如果文件中的操作要求如此）。这些关键命令在此处进行了说明，而所有其他命令则稍后将在主机输入导入语法（第 2-6 页）中说明。

注意：系统会丢弃导入文件中其无法解释的任何数据。要在运行导入之前测试导入文件，请参阅在管理中心上测试导入（第 2-24 页）。

主机输入导入文件必须以 SetDomain（如果使用域）、SetSource 和 SetMap 命令开头，以提供应用源名称和设置已导入的数据的第三方产品名称映射。有关详细信息，请参阅了解导入文件格式（第 2-3 页）。

在 SetDomain、SetSource 和 SetMap 命令之后，可以向文件中添加其他命令行。每个命令行都包含单个命令以及该命令所需的参数，并通过硬回车结束。请注意，仅在必须提供某些字段的信息才能确保主机输入成功并将有意义的数据添加到网络映射的情况下，这些字段才是必需的。例如，可以向系统添加修复，而不提供与现有思科修复定义匹配的修复标识号或修复名称，并且不将第三方修复映射到思科修复。

有关可以包含的个别命令的语法的详细信息，请参阅以下各节：

- 主机命令（第 2-6 页）
- 服务器命令（第 2-8 页）

- 客户端应用命令（第 2-11 页）
- 协议命令（第 2-13 页）
- 软件包修复命令（第 2-14 页）
- 主机属性命令（第 2-15 页）
- 漏洞命令（第 2-16 页）
- 设置第三方产品映射（第 2-5 页）

要查看完整导入文件的示例和该文件各部分的说明，请参阅示例主机输入导入文件（第 2-19 页）。

设置域

如果系统已定义域，则您可能需要在导入文件开头指定目标域。如果客户端证书和导入文件均不指定枝叶域，则运行导入将会失败并出现错误消息。

- 系统为每个枝叶域构建单独的网络映射。在多域部署中，必须指定要添加网络映射数据的枝叶域。
- 如果您将使用主机输入客户端提交 CSV 命令，则可以为每个枝叶域创建单独的客户端证书。当使用此类证书时，所有操作都将针对该证书的域。在此情况下，没有理由在脚本中使用 SetDomain 命令。
- 如果旨在具有域的系统上使用 nmimport 工具，则导入文件必须以 SetDomain 命令开头。如果 SetDomain 命令或证书未指定任何枝叶域，则导入将立即失败并出现错误消息，而不处理任何命令。
- 域名必须通过以空格-反斜杠-空格分隔每个域级别来完全限定，例如 `Global \ Accounting` 或 `Global \ Sales \ East`。域名的大小写必须与域的定义方式完全相同。

要设置域，请执行以下操作：

对于导入文件中的第一行，请使用以下语法：

`SetDomain, DomainName`
其中 `SetDomain` 是命令的名称，*`DomainName`* 是要将已导入的数据添加到的完全限定枝叶域。

设置源类型

在导入文件的开头，您必须识别计划导入的数据的源类型。如果使用此命令导入扫描结果，请务必在网络发现策略中编辑输入源的源定义，以将身份源类型设置为“扫描程序”(Scanner)。

要设置源类型，请执行以下操作：

1. 使用以下语法向导入文件中添加一行：

   `SetSourceType, Sourcetype`
   其中 `SetSourceType` 是命令的名称，*`ourcetype`* 是要添加或用于已导入的数据的源类型。有效值为 `2`（扫描程序）或 `3`（应用）。

   如果不使用 `SetSourceType`，则默认类型为 `3`（应用）。

设置源 ID

在导入文件的开头，您必须设置计划导入的数据的源 ID。

要设置源应用名称，请执行以下操作：

1. 使用以下语法向导入文件中添加一行：

   `SetSource, SourceID`
   其中 `SetSource` 是命令的名称，*`SourceID`* 是要显示为已导入的数据的源应用的标识字符串。

   以下是 SetSource 命令的示例：

   ```
   # Set the current SOURCE_ID and Product Map to "Custom Utility"
   SetSource, Custom Utility
   ```
   要在示例文件中的情景下查看这些命令，请参阅整个示例文件（第 2-23 页）。

设置第三方产品映射

如果您计划导入第三方操作系统、服务器或修复定义，则必须创建第三方名称的用户第三方产品映射。可以使用此命令设置当前会话的当前第三方映射。您使用管理中心 Web 界面在每个第三方供应商、产品和版本组合以及对应的思科产品定义之间设置可重复使用的映射来创建第三方映射。如果设置第三方映射，然后添加或者设置主机操作系统或其中包括映射中含有的第三方应用名称的服务器数据，则系统会使用映射将思科产品定义和关联漏洞映射到发生输入的每个主机。

例如，可以创建名为“`Custom Utility`”的映射集，在其中按如下定义第三方字符串：

- 供应商字符串 - Microsoft
- 产品字符串 - Win7

可以选择该映射集中的以下思科产品映射：

- 供应商 - Microsoft, Corp.
- 产品 - Windows 7
- 补丁 - SP3

如果通过调用 `SetMap, Custom Utility` 来设置此产品映射，则其会将 `Microsoft Win7` 映射到 `Microsoft Windows 7` 产品的 VDB 条目。

要设置第三方产品映射集，请执行以下操作：

1. 使用以下语法向导入文件中添加一行：

   `SetMap, Third-PartyProductMapName`
   其中 SetMap 是命令的名称，*`Third-PartyProductMapName`* 是要用于导入的第三方产品映射集的名称。

   例如，可以将以下代码行置于 SetSource 命令后：

   ```
   SetMap, Custom Utility
   ```
   您还可以使用此命令切换到导入文件中的其他第三方产品映射。

主机输入导入语法

在设置导入文件的源 ID 和产品映射后（如设置源 ID（第 2-5 页）中所述），您可以向导入文件中添加行，以使用各种主机输入命令导入要添加到网络映射的特定数据。每个导入命令调用都必须通过硬回车结束，并导入一个导入数据集。有关完整导入文件的示例，请参阅示例主机输入导入文件（第 2-19 页）。

有关可以使用的特定命令的详细信息，请参阅以下各节：

- 主机命令（第 2-6 页）
- 服务器命令（第 2-8 页）
- 客户端应用命令（第 2-11 页）
- 协议命令（第 2-13 页）
- 软件包修复命令（第 2-14 页）
- 主机属性命令（第 2-15 页）
- 漏洞命令（第 2-16 页）
- 扫描结果命令（第 2-17 页）

主机命令

您可以使用主机输入 API 添加和删除网络映射中的主机和设置主机的操作系统定义。

有关主机命令的详细信息，请参阅以下各节：

- AddHost（第 2-6 页）
- DeleteHost（第 2-7 页）
- SetOS（第 2-7 页）
- UnsetOS（第 2-8 页）

AddHost

您可以使用 `AddHost` 命令向网络映射中添加主机。可以添加 IP 主机（具有 IP 地址和 MAC 地址 [可选] 的主机）或仅 MAC 主机（仅具有 MAC 地址的主机）。本例中添加的主机不会遭受普通主机超时。

如果网络映射已经包含具有指定 IP 地址或主 MAC 地址的主机，则 AddHost 命令将没有任何影响。如果目标是将网络映射中主机的任何现有信息替换为新信息，则必须在 AddHost 之前使用 DeleteHost 命令。

使用以下语法：

```
AddHost, ip_address, mac_address
```

表 1　AddHost 字段

字段	说明	必需	值
ip_address	指示已添加的主机的 IP 地址。	是（除非提供 MAC 地址）	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
mac_address	指示已添加的主机的 MAC 地址。	是（除非提供 IP 地址）	单个 MAC 地址。

DeleteHost

您可以使用 `DeleteHost` 命令从网络映射中删除一个或多个主机。可以通过指定主机的 IP 地址或 MAC 地址来删除 IP 主机（具有 IP 地址和 MAC 地址 [可选] 的主机）。要删除仅 MAC 主机（仅具有 MAC 地址的主机），请提供 MAC 地址：

使用以下语法：

```
DeleteHost, ip_address, mac_address
```

表 2 DeleteHost 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是（除非提供 MAC 地址）	单个 IP 地址。
mac_address	指示一个或多个受影响主机的 MAC 地址列表。	是（除非提供 IP 地址）	单个 MAC 地址。

SetOS

您可以使用 `SetOS` 命令指定所指定主机的操作系统的供应商、产品、版本和移动设备信息。当导入操作系统信息时，将会设置供应商、产品、版本和移动设备信息的显示字符串。您还可以将第三方供应商、产品和版本字符串映射到思科产品定义。有关详细信息，请参阅创建第三方产品映射（第 2-1 页）。

如果将第三方操作系统名称映射到思科定义，则思科数据库中该操作系统的漏洞对应于已导入第三方数据的主机。如果已经使用管理中心 Web 界面创建第三方产品映射集，则可以使用 `SetMap` 命令将在该映射集中指定的值用于第三方应用字符串和对应的思科定义，如设置第三方产品映射（第 2-5 页）中所述。

主机配置文件中显示的操作系统身份由最高优先级的源设置。可能的源具有以下优先级顺序：用户、扫描程序和应用（设置在网络发现策略中）、Firepower，然后是 NetFlow。请注意，如果新的优先级更高的操作系统身份具有的详细信息少于当前身份，则其不会覆盖当前操作系统身份。

如果为主机定义自定义操作系统，则管理中心 Web 界面会在事件视图的“源类型”(Source Type) 字段或主机配置文件的基本主机信息中指示更改源。

使用以下语法：

```
SetOS, ip_address, vendor_str, product_str, version_str, vendor_id,
product_id, major, minor, revision, build, patch, extension, device_string,
mobile, jailbroken
```

或者，要在设置操作系统之前设置新的产品映射，请使用以下语法：

```
SetMap, map_name
SetOS, ip_address, vendor_str, product_str, version_str, vendor_id,
product_id, major, minor, revision, build, patch, extension, device_string,
mobile, jailbroken
```

有关设置第三方产品映射的详细信息，请参阅设置第三方产品映射（第 2-5 页）。

表 3 SetOS 字段

字段	说明	必需	允许的值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
vendor_str	提供第三方应用使用的操作系统供应商显示名称。	否	字符串
product_str	提供第三方应用使用的操作系统产品显示名称。	否	字符串
version_str	提供第三方应用使用的操作系统版本显示名称。	否	字符串

表 3　SetOS 字段（续）

字段	说明	必需	允许的值
vendor_id	提供要映射到的思科供应商定义。	否	uint32
product_id	提供要映射到的思科产品定义。	否	uint32
major	提供要映射到的思科主版本定义。	否	uint32
minor	提供要映射到的思科次版本定义。	否	uint32
revision	提供要映射到的思科修订字符串。	否	uint32
build	提供要映射到的思科内部版本定义。	否	字符串
patch	提供要映射到的思科补丁定义。	否	字符串
extension	提供要映射到的思科扩展定义。	否	字符串
device_string	提供检测到的移动设备硬件信息。	否	字符串
mobile	指示操作系统是否是在移动设备上运行。	否	uint8
jailbroken	指示移动设备操作系统是否已越狱。	否	uint8

UnsetOS

您可以使用 `UnsetOS` 命令从指定主机中删除先前设置的操作系统定义。它会重置操作系统定义，以使系统能够在将来跟踪对操作系统的更改。

使用以下语法：

```
UnsetOS, ip_address
```

其中 *ip_address* 是 IP 地址、CIDR 块以及表示要重置操作系统身份的一个或多个主机的 IP 地址范围的逗号分隔列表。

服务器命令

您可以使用服务器命令更新网络映射中主机的服务器信息。

有关详细信息，请参阅以下各节：

- AddService（第 2-8 页）
- SetService（第 2-9 页）
- UnsetService（第 2-10 页）
- DeleteService（第 2-11 页）
- 客户端应用命令（第 2-11 页）

AddService

您可以使用 `AddService` 命令向网络映射中的现有主机添加服务器。

主机配置文件中显示的服务器身份由最高优先级的源设置。可能的源具有以下优先级顺序：用户、扫描程序和应用（设置在网络发现策略中）、Firepower，然后是 NetFlow。请注意，如果新的优先级更高的服务器身份具有的详细信息少于当前身份，则其不会覆盖当前操作服务器身份。

使用以下语法：

```
AddService, ip_address, port, proto, server, vendor_str, version_str,
vendor_id, product_id, major, minor, revision, build, patch, extension
```

或者，要在添加服务器之前设置新的产品映射，请使用以下语法：

```
SetMap, map_name
AddService, ip_address, port, proto, server, vendor_str, version_str,
vendor_id, product_id, major, minor, revision, build, patch, extension
```

有关设置第三方产品映射的详细信息，请参阅创建第三方产品映射（第 2-1 页）和设置第三方产品映射（第 2-5 页）。

表 4　AddService 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
port	将此字段与 `ip_address` 和 `proto` 字段结合使用，以指定要在应添加服务器的主机上添加的服务器。	是	范围在 1 到 65535 之间的整数。
proto	将此字段与 `ip_address` 和 `port` 字段结合使用，以指定要在应添加服务器的主机上添加的服务器。	是	字符串 `tcp` 或 `udp`，或者相应的协议 ID `6` (tcp) 或 `17` (udp)。
server	思科数据库中服务器的名称或 ID。	否	要识别服务器，必须包含 `service_name` 或 `service_id` 的值。如果两个字段的值均未提供，则服务器将列为 `unknown`。如果提供服务器名称，则系统会查找服务器 ID。如果服务器名称不存在任何 ID，则系统会创建 ID。
vendor_str	提供第三方应用使用的服务器供应商显示名称。	否	字符串
product_str	提供第三方应用使用的服务器产品显示名称。	否	字符串
version_str	提供第三方应用使用的服务器版本显示名称。	否	字符串
vendor_id	提供思科供应商定义。	否	uint32
product_id	提供思科产品定义。	否	uint32
major	提供思科主版本定义。	否	uint32
minor	提供思科次版本定义。	否	uint32
revision	提供思科修订字符串。	否	uint32
build	提供要映射到的思科内部版本定义。	否	字符串
patch	提供要映射到的思科补丁定义。	否	字符串
extension	提供要映射到的思科扩展定义。	否	字符串

SetService

您可以使用 `SetService` 命令指定所指定服务器的服务器协议、供应商、产品和版本。可以使用服务密钥设置服务器的显示字符串。通过在管理中心 Web 界面中映射第三方产品（请参阅创建第三方产品映射（第 2-1 页））或使用 `SetMap` 命令（请参阅设置第三方产品映射（第 2-5 页）），可以将第三方服务器数据与特定思科产品定义的漏洞信息相关联。

如果服务器协议尚不存在，则此调用会导致为字符串创建新的服务器身份。如果指定的服务器先前不存在，则系统会进行创建。

主机配置文件中显示的服务器身份由最高优先级的源设置。可能的源具有以下优先级顺序：用户、扫描程序和应用（设置在网络发现策略中）、Firepower，然后是 NetFlow。请注意，如果新的优先级更高的服务器身份具有的详细信息少于当前身份，则其不会覆盖当前服务器身份。

如果为主机定义第三方服务器定义，则 Firepower 管理中心 Web 界面会在事件的“服务器”(Servers) 表视图的“源类型”(Source Type) 字段或主机配置文件的“服务器”(Servers) 部分中指示更改源。

注：如果特定主机的网络映射中存储的服务器数量超过 100，则会忽略新的服务器信息，直至从主机中删除服务器。

使用以下语法：

```
SetService, ip_address, port, proto, server, vendor_str, version_str,
vendor_id, product_id, major, minor, revision, build, patch, extension
```

或者，要在设置服务器之前设置新的产品映射，请使用以下语法：

```
SetMap, map_name
SetService, ip_address, port, proto, server, vendor_str, version_str,
vendor_id, product_id, major, minor, revision, build, patch, extension
```

有关设置第三方产品映射的详细信息，请参阅设置第三方产品映射（第 2-5 页）。

表 5 SetService 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
port	将此字段与 `ip_address` 和 `proto` 字段结合使用，以指定要在应设置服务器的主机上设置的服务器。	是	范围在 1 到 65535 之间的整数。
proto	将此字段与 `ip_address` 和 `port` 字段结合使用，以指定要在应设置服务器的主机上设置的服务器。	是	字符串 `tcp` 或 `udp`，或者相应的协议 ID `6` (tcp) 或 `17` (udp)。
server	思科数据库中服务器的名称或 ID。	否	要识别服务器，必须包含 `service_name` 或 `service_id` 的值。如果两个字段的值均未提供，则服务器将列为 `unknown`。如果提供服务器名称，则系统会查找服务器 ID。如果服务器名称不存在任何 ID，则系统会创建 ID。
vendor_str	提供第三方应用使用的服务器供应商显示名称。	否	字符串
product_str	提供第三方应用使用的服务器产品显示名称。	否	字符串
version_str	提供第三方应用使用的服务器版本显示名称。	否	字符串
vendor_id	提供思科供应商定义。	否	uint32
product_id	提供思科产品定义。	否	uint32
major	提供思科主版本定义。	否	uint32
minor	提供思科次版本定义。	否	uint32
revision	提供思科修订字符串。	否	uint32
build	提供要映射到的思科内部版本定义。	否	字符串
patch	提供要映射到的思科补丁定义。	否	字符串
extension	提供要映射到的思科扩展定义。	否	字符串

UnsetService

您可以使用 `UnsetService` 命令从指定主机中删除用户添加的服务器定义。`UnsetService` 不删除通过 Firepower 检测到的任何服务器定义。

注：如果特定主机的网络映射中存储的服务器数量超过 100，则会忽略新的服务器信息，直至从主机中删除服务器。

使用以下语法：

```
UnsetService, ip_address, port, proto
```

表 6 UnsetService 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
port	将此字段与 `ip_address` 和 `proto` 字段结合使用，以指定要在应删除服务器的主机上删除的服务器。	是	范围在 1 到 65535 之间的整数。
proto	将此字段与 `ip_address` 和 `port` 结合使用，以指定要在应删除服务器的主机上删除的服务器。	是	字符串 `tcp` 或 `udp`，或者相应的协议 ID `6` (tcp) 或 `17` (udp)。

DeleteService

您可以使用 `DeleteService` 命令从指定主机中删除服务器。您还必须指定要删除的服务器的端口和协议。

使用以下语法：

```
DeleteService, ip_address, port, proto
```

表 7 DeleteService 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
port	将此字段与 `ip_address` 和 `proto` 结合使用，以指定要在应删除服务器的主机上删除的服务器。	是	范围在 1 到 65535 之间的整数。
proto	将此字段与 `ip_address` 和 `port` 字段结合使用，以指定要在应删除服务器的主机上删除的服务器。	是	字符串 `tcp` 或 `udp`，或者相应的协议 ID `6` (tcp) 或 `17` (udp)。

客户端应用命令

您可以使用客户端应用命令修改网络映射中主机的客户端应用数据。

有关详细信息，请参阅以下各节：

- AddClientApp（第 2-11 页）
- DeleteClientApp（第 2-12 页）
- DeleteClientAppPayload（第 2-12 页）

AddClientApp

您可以使用 `AddClientApp` 命令将客户端应用添加到网络映射中的现有主机。如果客户端应用名称在思科数据库中尚不存在，则系统会为客户端应用创建新条目。

主机配置文件中显示的客户端应用身份由最高优先级的源设置。可能的源具有以下优先级顺序：用户、扫描程序和应用（设置在网络发现策略中）、Firepower，然后是 NetFlow。请注意，如果新的优先级更高的客户端应用身份具有的详细信息少于当前身份，则其不会覆盖当前客户端应用身份。

使用以下语法：

```
AddClientApp, ip_address, app_name, app_type, version
```

表 8 AddClientApp 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
app_name	指示客户端应用名称。	是	包含字母数字字符或空格的字符串。 对于现有应用，对应于数据库中的 ID 值。系统会查找 ID 以确认其是否与现有客户端应用 ID 匹配。如果不匹配，则创建新 ID。
app_type	不建议使用此字段。	否	空值。
version	指示应用版本。	否	包含字母数字字符或空格的字符串。

DeleteClientApp

您可以使用 `DeleteClientApp` 命令从指定主机中删除客户端应用。

使用以下语法：

`DeleteClientApp, ip_address, app_name, app_type, version`

表 9 DeleteClientApp 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
app_name	指示客户端应用名称。	是	包含字母数字字符或空格的字符串。 对于现有应用，对应于数据库中的 ID 值。系统会查找 ID 以确认其是否与现有客户端应用 ID 匹配。如果不匹配，则创建新 ID。
app_type	不建议使用此字段。	否	空值。
version	指示应用版本。	否	包含字母数字字符或空格的字符串。

DeleteClientAppPayload

您可以使用 `DeleteClientAppPayload` 命令从指定主机中删除 Web 应用。

使用以下语法：

`DeleteClientAppPayload, ip_address, app_name, app_type, version, payload_type, payload_id`

表 10 DeleteClientAppPayload 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
app_name	指示客户端应用名称。	是	包含字母数字字符或空格的字符串。 对于现有应用，对应于数据库中的 ID 值。系统会查找 ID 以确认其是否与现有客户端应用 ID 匹配。如果不匹配，则创建新 ID。
app_type	不建议使用此字段。	否	空值。
version	指示应用版本。	否	包含字母数字字符或空格的字符串。

表 10 DeleteClientAppPayload 字段（续）

字段	说明	必需	值
payload_type	指示 Web 应用类别。	是	数字 0。 对于现有应用，对应于数据库中的 ID 值。系统会查找类型，以确认其是否与现有 Web 应用类型匹配。如果不匹配，则创建新类型。
payload_id	指示 Web 应用名称。	是	包含字母数字字符或空格的字符串。 对于现有应用，对应于数据库中的 ID 值。系统会查找 ID，以确认其是否与现有 Web 应用 ID 匹配。如果不匹配，则创建新 ID。

协议命令

您可以使用协议命令更新网络映射中主机的协议信息。

有关详细信息，请参阅以下各节：

- DeleteProtocol（第 2-13 页）
- AddProtocol（第 2-13 页）

DeleteProtocol

您可以使用 `DeleteProtocol` 命令从指定的 IP 或 MAC 主机中删除协议。

使用以下语法：

```
DeleteProtocol, ip_address, mac_address, proto, type
```

表 11 DeleteProtocol 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是（除非提供 MAC 地址）	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
mac_address	指示一个或多个受影响主机的 MAC 地址列表。	是（除非提供 IP 地址）	带有或不带分隔冒号的 MAC 地址字符串列表。
proto	指示要删除的协议的标识字符串或名称。	是	包含字母数字字符或空格的有效协议名称。对于传输协议（“xport”），/etc/protocols 文件中所列的协议可接受。对于网络协议（“net”），请参阅网络协议值（第 A-1 页）。
type	指示要删除的协议的类型。	是	“xport”或“net”

AddProtocol

您可以使用 `AddProtocol` 命令将网络协议或传输协议添加到网络映射中的现有主机。您可以提供协议 ID、存在于管理中心上 /etc/protocols 文件中的传输协议名称或网络协议值（第 A-1 页）中的网络协议名称。

注：不能将传输协议添加到仅 MAC 主机。

使用以下语法：

```
AddProtocol, ip_address, mac_address, proto, type
```

表 12 AddProtocol 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是（除非提供 MAC 地址）	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
mac_address	指示一个或多个受影响主机的 MAC 地址列表。	是（除非提供 IP 地址）	带有或不带分隔冒号的 MAC 地址字符串列表。
proto	指示要添加的协议的标识字符串或名称。	是	包含字母数字字符或空格的有效协议名称。对于传输协议（"xport"），/etc/protocols 文件中所列的协议可接受。对于网络协议（"net"），请参阅网络协议值（第 A-1 页）。
type	指示要添加的协议的类型。	是	"xport"或"net"

软件包修复命令

您可以使用软件包修复命令应用或删除进行导入的枝叶域的网络映射中主机的修复。

有关详细信息，请参阅以下各节：

- AddFix（第 2-14 页）
- RemoveFix（第 2-15 页）

AddFix

您可以使用 AddFix 命令将修复映射到指定的主机或服务器。可以使用思科漏洞数据库 (VDB) 中的修复 ID 或者使用通过管理中心 Web 界面映射到 VDB 中的修复的第三方修复来映射修复。

将修复应用到主机或服务器时，将会调整系统的漏洞映射，并且已修复的漏洞在 Web 界面中标记为“无效”(Invalid) 且不会用于影响评估。但请注意，如果所应用的修复不适用于操作系统或服务器身份，则该修复没有任何作用。

使用以下语法：

```
AddFix, ip_address, port, proto, fix_id
```

表 13 AddFix 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
port	通过 proto 字段，识别发生导入的主机上的修复所影响的服务器。	是（如果修复适用于服务器）	范围在 1 到 65535 之间的整数。
proto	通过 port 字段，识别发生导入的主机上的修复所影响的服务器。	否	字符串 tcp 或 udp，或者相应的协议 ID 6 (tcp) 或 17 (udp)。
fix_id	指示修复的标识字符串。	是	思科修复标识号，或者通过在调用 AddFix 命令之前调用 SetMap 命令来使用的第三方产品映射中定义的修复名称。有关详细信息，请参阅设置第三方产品映射（第 2-5 页）。

RemoveFix

您可以使用 RemoveFix 命令从指定的主机或服务器中删除修复映射。当删除修复时，将会相应地更新漏洞映射。

使用以下语法：

RemoveFix, *ip_address*, *port*, *proto*, *fix_id*

表 14 RemoveFix 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
port	通过 proto 字段，识别发生导入的主机上的修复所影响的服务器。	是（如果修复适用于服务器）	范围在 1 到 65535 之间的整数。
proto	通过 port 字段，识别发生导入的主机上的修复所影响的服务器。	否	字符串 tcp 或 udp，或者相应的协议 ID 6 (tcp) 或 17 (udp)。
fix	指示修复的标识字符串。	是	思科修复名称，或者通过在调用 AddFix 命令之前调用 SetMap 命令来使用的第三方产品映射中定义的修复名称。有关详细信息，请参阅设置第三方产品映射（第 2-5 页）。

主机属性命令

您可以使用主机输入导入工具设置进行导入的枝叶域的网络映射的属性值。有关详细信息，请参阅以下各节：

- AddHostAttribute（第 2-15 页）
- DeleteHostAttribute（第 2-15 页）
- SetAttributeValue（第 2-15 页）
- DeleteAttributeValue（第 2-16 页）

AddHostAttribute

您可以使用 AddHostAttribute 命令添加文本或 URL 属性。请注意，添加主机属性不会添加该属性的值。有关设置属性值的详细信息，请参阅下面 SetAttributeValue（第 2-15 页）。

使用以下语法：

AddHostAttribute, *attributename*, *attributetype*

其中 *attributename* 是属性的名称（包含字母数字字符和空格），*attributetype* 是属性的类型（text 或 URL）。

DeleteHostAttribute

您可以使用 DeleteHostAttribute 命令删除属性。

使用以下语法：

DeleteHostAttribute, *attributename*

其中 *attributename* 是属性的名称。（有效名称包含字母数字字符和空格。）

SetAttributeValue

您可以使用 SetAttributeValue 命令将现有属性的值设置为指定主机的指定值。此命令可以设置用户定义的主机属性和 Criticality 属性的值。可以使用此命令通过将"criticality"用作属性 ID 来设置主机临界性。

使用以下语法：

```
SetAttributeValue, ip_address, attribute, value
```

表 15 SetAttributeValue 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
attribute	指示主机属性名称。	是	包含字母数字字符或空格的有效属性名称。
value	指示主机属性值。	是	包含字母数字字符或空格的命名属性的有效属性值。如果为列表属性传入值，则该值必须是该列表属性的现有命名值。

DeleteAttributeValue

您可以使用 `DeleteAttributeValue` 命令删除主机的属性值。

使用以下语法：

```
DeleteAttributeValue, ip_address, attribute, value
```

表 16 DeleteAttributeValue 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
id	指示主机属性名称。	是	包含字母数字字符或空格的有效属性名称。
value	指示主机属性值。	是	包含字母数字字符或空格的命名属性的有效属性值。如果为列表属性传入值，则该值必须是该列表属性的现有命名值。

漏洞命令

您可以使用漏洞命令更新主机上漏洞的状态。

有关详细信息，请参阅以下各节：

- SetInvalidVulns（第 2-16 页）
- SetValidVulns（第 2-17 页）

SetInvalidVulns

您可以使用 `SetInvalidVulns` 命令停用主机或主机组上的漏洞。为使命令调用生效，漏洞必须在主机上存在并设置为有效。

使用以下语法：

```
SetInvalidVulns, ip_address, port, proto, type, vuln_id
```

表 17 SetInvalidVulns 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
port	通过 `proto` 字段，识别发生导入的主机上的漏洞所影响的服务器。	是（如果修复适用于服务器）	范围在 1 到 65535 之间的整数。

表 17 SetInvalidVulns 字段（续）

字段	说明	必需	值
proto	通过 port 字段，识别发生导入的主机上的漏洞所影响的服务器。	是（如果修复适用于服务器）	字符串 tcp 或 udp，或者相应的协议 ID 6 (tcp) 或 17 (udp)。
vuln_id	指示漏洞的漏洞 ID。	是	有效的思科漏洞 ID 或映射的第三方漏洞 ID。 对于第三方漏洞，请注意必须映射第三方漏洞 ID 并引用 vuln_type 字段中设置的漏洞映射集。有关详细信息，请参阅创建第三方漏洞映射（第 2-1 页）。

SetValidVulns

您可以使用 SetValidVulns 命令激活主机或主机组上的漏洞。将漏洞设置为对于主机有效后，管理中心就会向事件分配红色影响，即使事件中的 SID 映射到有效漏洞也如此。为使命令调用生效，漏洞必须在主机上存在并设置为无效。

使用以下语法：

```
SetValidVulns, ip_address, port, proto, type, vuln_id
```

表 18 SetValidVulns 字段

字段	说明	必需	值
ip_address	指示包含一个或多个受影响主机的一个或多个 IP 地址的字符串。	是	IP 地址、CIDR 掩码范围、IP-IP 范围或此类值的带引号的逗号分隔列表。
port	通过 proto 字段，识别发生导入的主机上的漏洞所影响的服务器。	是（如果修复适用于服务器）	范围在 1 到 65535 之间的整数。
proto	通过 port 字段，识别发生导入的主机上的漏洞所影响的服务器。	是（如果修复适用于服务器）	字符串 tcp 或 udp，或者相应的协议 ID 6 (tcp) 或 17 (udp)。
vuln_id	指示漏洞的漏洞 ID。	是	有效的思科漏洞 ID 或映射的第三方漏洞 ID。 对于第三方漏洞，请注意必须映射第三方漏洞 ID 并引用 vuln_type 字段中设置的漏洞映射集。有关详细信息，请参阅创建第三方漏洞映射（第 2-1 页）。

扫描结果命令

您可以使用主机输入导入工具将扫描结果添加到管理中心以及将添加的结果刷新到数据库。在添加扫描结果时，可以将结果中的第三方漏洞映射到 CVE 或 BugTraq 漏洞。

有关详细信息，请参阅以下各节：

AddScanResult 命令

您可以使用 AddScanResult 命令从第三方漏洞扫描程序添加扫描结果，并将每个漏洞映射到 BugTraq 或 CVE ID。如果使用此命令导入扫描结果，请务必在网络发现策略中编辑输入源的源定义，以将身份源类型设置为“扫描程序”(Scanner)。

使用以下语法：

```
AddScanResult, ipaddr, scanner_id, vuln_id, port, protocol, name,
description, cve_ids, bugtraq_ids
```

注：结果的添加方式取决于使用 ScanUpdate 还是 ScanFlush 命令。有关详细信息，请参阅 ScanFlush 命令（第 2-18 页）和 ScanUpdate 命令（第 2-19 页）。

表 19 AddScanResult 字段

字段	说明	必需	允许的值
ipaddr	指示已扫描的一个或多个主机的 IP 地址。	是	单个 IP 地址。
scanner_id	指示已获取扫描结果的扫描程序的扫描程序 ID。	是	'scanner_id' 其中 `scanner_id` 是指示扫描程序（即添加的漏洞数据源）的名称的字符串。 要从先前使用的扫描程序添加扫描结果，请指示已添加结果的管理中心上系统策略中所列的特定扫描程序名称。 从新的扫描程序 ID 添加结果会将该扫描程序添加到系统策略。默认情况下，新的扫描程序添加为最低优先级。如果要更改扫描程序的优先级，则可以在系统策略中执行此操作。有关详细信息，请参阅《*Firepower 管理中心配置指南*》。
vuln_id	指示漏洞的漏洞 ID。	是	有效的思科漏洞 ID 或映射的第三方漏洞 ID。 如果此字段、端口、协议、bugtraq_ids 和 cve_ids 为空，则这是通用扫描结果。
port	通过 `proto` 字段，识别发生导入的主机上的漏洞所影响的服务器。	是（如果漏洞适用于服务器）	范围在 1 到 65535 之间的整数。
proto	通过 `port` 字段，识别发生导入的主机上的漏洞所影响的服务器。	是（如果漏洞适用于服务器）	字符串 `tcp` 或 `udp`，或者相应的协议 ID `6` (tcp) 或 `17` (udp)。
name	正在导入的漏洞的名称。	否	用单引号引起来的字符串；例如： 'Using NetBIOS to retrieve info from a Windows host'
description	正在导入的漏洞的说明。	否	用单引号引起来的字符串；例如： `'The following 2 NetBIOS names have been gathered...'`
cve_ids	CVE 漏洞 ID 的空格分隔列表	否	有效的 CVE 漏洞 ID；例如，`'cve_ids: CVE2003-0988'`。 如果此字段、端口、协议、vuln_id 和 bugtraq_ids 为空，则这是通用扫描结果。
bugtraq_ids	BugTraq 漏洞 ID 的空格分隔列表	否	有效的 BugTraq 漏洞 ID；例如，`'bugtraq_ids: 9506'`。 如果此字段、端口、协议、vuln_id 和 cve_ids 为空，则这是通用扫描结果。

ScanFlush 命令

使用 `AddScanResult` 将扫描结果添加到管理中心后，必须使用 `ScanUpdate` 或 `ScanFlush` 命令来使 `AddScanResult` 命令在管理中心上运行，从而将扫描结果上传到数据库。

`ScanFlush` 命令无需任何参数，并且只要要在导入文件中将数据上传到数据库，即可使用该命令。

如果使用 `ScanFlush` 命令，则其会从主机中删除任何现有扫描结果并仅添加新结果。

ScanUpdate 命令

使用 AddScanResult 将扫描结果添加到管理中心后，必须使用 ScanUpdate 或 ScanFlush 命令来使 AddScanResult 命令在管理中心上运行，从而将扫描结果上传到数据库。

ScanUpdate 命令无需任何参数，并且只要要在导入文件中将数据上传到数据库，即可使用该命令。

如果使用 ScanUpdate 命令，则其不会从主机中删除现有扫描结果。它将新扫描结果与现有扫描结果合并。

如果将 ScanUpdate 命令与 DeleteScanResult 命令结合使用，则会删除特定结果。

请注意，当导入完成时，即使 ScanUpdate 未显式包含在导入文件中，也会自动执行该命令，因为客户端连接关闭。

DeleteScanResult 命令

您可以将 DeleteScanResult 命令与 ScanUpdate 命令结合使用，以从特定主机中删除特定扫描结果。

如果提供可选参数的值，则会将结果限于与这些参数匹配的结果。如果不提供可选参数的值，则会删除指定 IP 地址上的所有结果。

使用以下语法：

```
DeleteScanResult, ipaddr, 'scanner_id', vuln_id, port, protocol
```

表 20　DeleteScanResult 字段

字段	说明	必需	允许的值
ipaddr	指示已扫描的一个或多个主机的 IP 地址。	是	单个 IP 地址。
scanner_id	指示已获取扫描结果的扫描程序的扫描程序 ID。	否	'scanner_id' 其中 scanner_id 是指示扫描程序（即添加的漏洞数据源）的名称的字符串。 要从先前使用的扫描程序添加扫描结果，请指示已添加结果的管理中心上系统策略中所列的特定扫描程序名称。 从新的扫描程序 ID 添加结果会将该扫描程序添加到系统策略。默认情况下，新的扫描程序添加为最低优先级。如果要更改扫描程序的优先级，则可以在系统策略中执行此操作。有关详细信息，请参阅《*Firepower 管理中心配置指南*》。
vuln_id	指示漏洞的漏洞 ID。	否	有效的第三方漏洞 ID。
port	通过 proto 字段，识别发生导入的主机上的漏洞所影响的服务器。	否	范围在 1 到 65535 之间的整数。
proto	通过 port 字段，识别发生导入的主机上的漏洞所影响的服务器。	否	字符串 tcp 或 udp，或者相应的协议 ID 6 (tcp) 或 17 (udp)。

示例主机输入导入文件

以下各节说明您可能如何构造导入文件以使用主机输入导入工具来导入数据。

以下各节按顺序显示文件的每个部分：

- 示例：设置源域、源 ID 和产品映射（第 2-20 页）
- 示例：添加主机（第 2-20 页）
- 示例：向主机中添加协议（第 2-20 页）

示例：设置源域、源 ID 和产品映射

示例脚本首先将执行调用，以设置要在导入中使用的域、源应用名称和产品映射：

```
# Set the current DOMAIN to Global \ Sales \ East
#
SetDomain, Global \ Sales \ East
# Set the current SOURCE_ID and Product Map to "Asset Management App"
SetSource, Asset Management App
SetMap, Asset Management App
```

此源域提供其中将添加主机信息的域。源 ID 值提供应用名称以供系统在由此导入造成的主机输入事件中使用。如果您已查看使用此导入修改的主机的主机输入事件或主机配置文件，则“源类型”(Source Type) 值将是 `Application: Asset Management App`。

请注意，SetMap 命令使用的名为“Asset Management App”的产品映射是使用管理中心 Web 界面创建的。

由于第三方产品映射是 Asset Management App 映射集，因此系统会使用该映射集中定义的产品映射或修复映射将导入文件中包含的命令中的任何第三方操作名称或服务器名称映射到思科定义，如示例：设置操作系统（第 2-21 页）中所示。

示例：添加主机

在文件设置源应用名称和第三方产品映射后，将会执行用于导入数据的命令。数据将添加到使用 SetDomain 命令或证书指定的枝叶域的网络映射中。第一个导入命令是 `AddHost` 命令。

```
# Add an IP host with no Primary MAC
#
AddHost,1.2.3.4
```

请注意，所添加的主机的 IP 地址是`1.2.3.4`，并且没有为主机设置任何主 MAC 地址。

示例：向主机中添加协议

导入文件中的下一个命令会将 `ospf` 协议添加到 `1.2.3.4` 主机：

```
# Add the ospf protocol to the host
#
AddProtocol, 1.2.3.4,,ospf,xport
```

请注意，该协议的协议类型为 `xport`。

示例：向主机中添加服务器

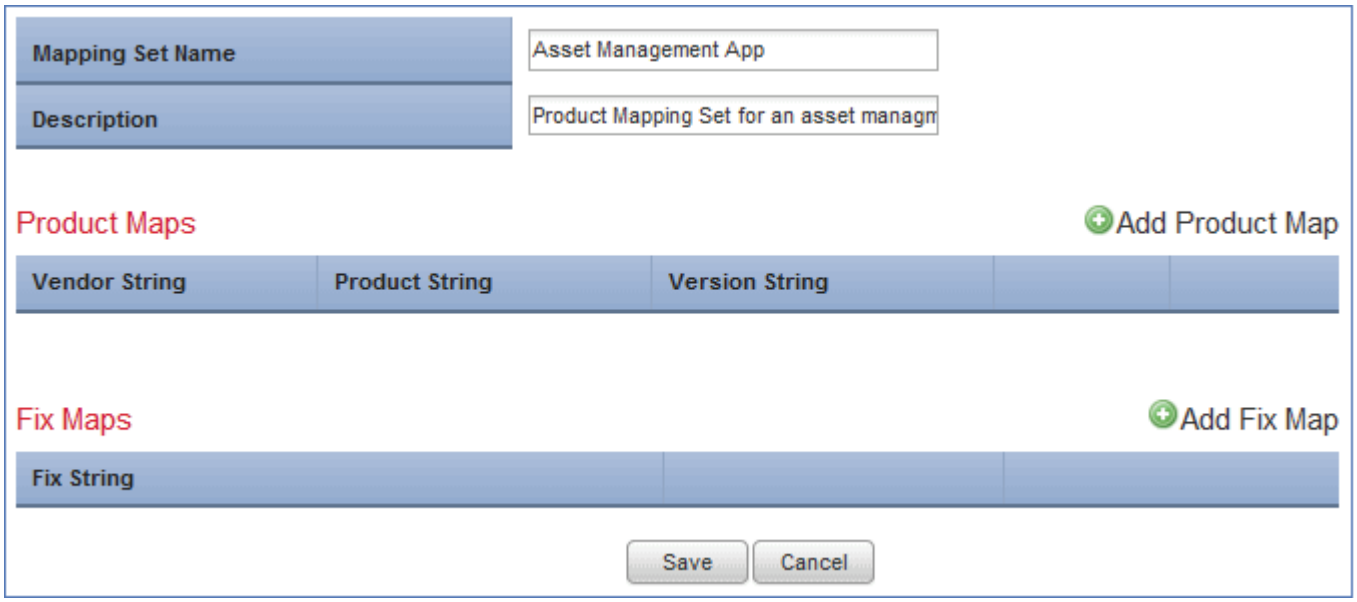
导入文件的下一个命令使用 AddService 命令将 OpenSSH 服务器添加到 1.2.3.4 主机：

```
# Add a server for the host
#
AddService,1.2.3.4, 22, tcp, ssh, OpenSSH, 4.1
```

请注意，该命令将端口设置为 22，将协议设置为 tcp，将服务器类型设置为 ssh，将供应商显示字符串设置为 OpenSSH，并将版本显示字符串设置为 4.1。

示例：设置操作系统

接下来，导入文件使用 SetOS 命令设置主机的操作系统值。Asset Management App 映射集包含产品映射，用于将第三方产品名称 Microsoft Win2K 映射到 Microsoft Windows 2000 SP3 的思科产品定义：



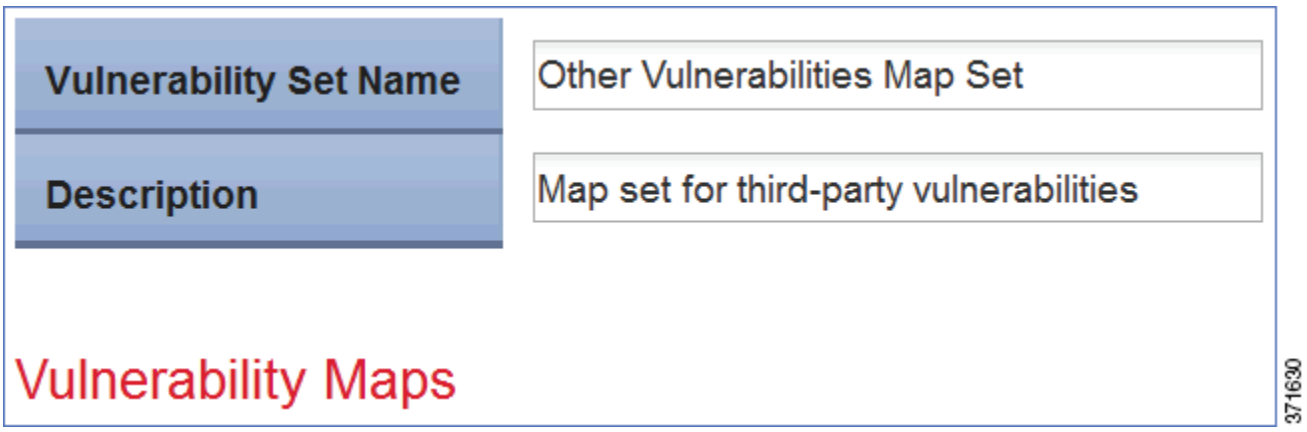
导入文件中的命令如下：

```
# Set the OS.Because the Map is set to "Asset Management App" these values
resolve to the Windows 2000 SP3 definition
#
SetOS, 1.2.3.4, Microsoft, Win2k
```

请注意，SetOS 命令行包含 vendor_str 和 product_str 字段的值，用于将操作系统显示名称设置为 Microsoft Win2K。由于这些字段值与 Asset Management App 产品映射集中定义的**供应商字符串 (Vendor String)** 和**产品字符串 (Product String)** 设置匹配，因此系统会将第三方操作系统名称映射到思科 Microsoft Windows 2000 SP3 产品定义。

示例：添加第三方漏洞

接下来，导入文件将第三方漏洞导入到 1.2.3.4 主机。此示例取决于使用管理中心 Web 界面创建的第三方漏洞映射集：



导入文件中的命令将 Vuln003 漏洞设置为有效：

```
# Add a third-party vulnerability (from third-party vulnerability map "Other
Vulnerabilities Map Set") to the host
#
SetValidVuln, 1.2.3.4,,, Other Vulnerabilities Map Set, Vuln0003
```

示例：设置主机临界性

导入文件中的下一个命令使用 SetAttributeValue 命令将 1.2.3.4 主机的临界性设置为“高”(High)。

```
# Set the criticality of the host to "High"
#
SetAttributeValue, 1.2.3.4,criticality,high
```

请注意，属性名称设置为 criticality，并且属性值设置为“high”。

示例：添加扫描结果

导入文件中的下一个命令集使用 AddHost 命令添加主机，然后使用 AddScanResult 命令从第三方扫描程序添加该主机的数据。

```
# Add IP host for scan results to follow
#
AddHost,1.2.3.5
#
# Add the scan result from a Qualys scanner to the network map
#
AddScanResult,1.2.3.5,"Qualys",82003,,,"ICMP Timestamp Request","ICMP
(Internet Control and Error Message Protocol) is a protocol encapsulated in
IP packets.Its principal purpose is to provide a protocol layer able to
inform gateways of the inter-connectivity and accessibility of other
gateways or hosts. ping is a well-known program for determining if a host is
up or down.It uses ICMP echo packets.ICMP timestamp packets are used to
synchronize clocks between hosts.","cve_ids: CVE-1999-0524","bugtraq_ids:"
```

示例：在管理中心上运行命令

`ScanFlush` 命令向管理中心表明其可以在 ScanFlush 行上运行已加入队列的命令。

ScanFlush

示例：向主机中添加客户端应用

然后，导入文件使用 `AddClientApp` 命令将名为 `BMC Remedy` 的客户端应用添加到 `1.2.3.4` 主机。

```
# Add a Client App
#
AddClientApp, 1.2.3.4, “BMC Remedy”, "Asset Manager", "0.0"
```

请注意，客户端应用 ID 设置为 `BMC Remedy`，客户端应用类型设置为 `Asset Manager`，并且版本设置为 `0.0`。

示例：添加仅 MAC 主机

最后，导入文件使用 `AddHost` 命令添加仅 MAC 主机。

```
# Add a MAC-only host
#
AddHost,,01:02:03:04:05:06
```

请注意，`ip_address` 字段留空并改为提供 MAC 地址。

另请注意，虽然文件结尾没有 `ScanFlush` 命令，但在导入文件完成时，脚本中的剩余数据会发送到网络映射，因为会话断开连接。

整个示例文件

以上各节中说明的完整导入文件如下所示：

```
# Example import file for Host Input Import Tool
#
# Set the DOMAIN to “Global \ Sales \ East”
#
# Set the current SOURCE_ID and Product Map to "Asset Management App"
#
SetDomain, Global \ Sales \ East
SetSource, Asset Management App
SetMap, Asset Management App
#
# Add an IP host with no Primary MAC
#
AddHost,1.2.3.4
#
# Add the ospf protocol to the host
#
AddProtocol, 1.2.3.4,,ospf,xport
#
# Add a server for the host
#
AddService,1.2.3.4, 22, tcp, ssh, OpenSSH, 4.1
#
# Set the OS.Because the Map is set to "Asset Management App" these values
resolve to the Windows 2000 SP3 definition
#
SetOS, 1.2.3.4, Microsoft, Win2k
#
```

```
# Add a third-party vulnerability (from third-party map "Other
Vulnerabilities Set") to the host
#
SetValidVuln, 1.2.3.4,,, Other Vulnerabilities Set, Vuln0003
#
# Set the criticality of the host to "High"
#
SetAttributeValue, 1.2.3.4,criticality,high
#
# Add IP host for scan results to follow
#
AddHost,1.2.3.5
#
# Add the scan result from a Qualys scanner to the network map
#
AddScanResult,1.2.3.5,"Qualys",82003,,,"ICMP Timestamp Request","ICMP
(Internet Control and Error Message Protocol) is a protocol encapsulated in
IP packets.Its principal purpose is to provide a protocol layer able to
inform gateways of the inter-connectivity and accessibility of other
gateways or hosts. ping is a well-known program for determining if a host is
up or down.It uses ICMP echo packets.ICMP timestamp packets are used to
synchronize clocks between hosts.","cve_ids: CVE-1999-0524","bugtraq_ids:"
#
#Send the commands above to the host input service for processing
#
ScanFlush
#
# Add a Client App
#
AddClientApp, 1.2.3.4, "BMC Remedy", "Asset Manager", "0.0"
#
# Add a MAC only host
#
AddHost,,01:02:03:04:05:06
```

在管理中心上测试导入

您可以使用导入文件来模拟导入，以确保其行为符合预期。由于许多命令都允许将重复数据导入到网络映射中，因此要避免多次运行同一导入。运行测试导入可避免该问题。此外，系统会丢弃导入文件中其无法解释的任何数据，因此要确保导入文件将完全导入。测试将结果报告到屏幕（或者可以将其重定向到文件），因此之后可以更正文件的任何问题，然后再运行实际导入。

要测试导入文件，请执行以下操作：

1. 将所创建的导入文件复制到要运行导入的管理中心。
2. 使用 `admin` 帐户登录到管理中心中。
3. 在命令行中，键入 `nmimport.pl -t` *filename*。

   要将测试导入的结果重定向到日志文件，请将 `>` *logfilename* 添加到命令结尾。

   系统将已导入的数据添加到网络映射，并在屏幕上显示结果消息或将其重定向到指定的文件。

运行主机输入导入

您可以从命令行运行主机输入导入工具，以处理所创建的导入文件。

注意：系统会丢弃导入文件中其无法解释的任何数据。此外，如果多次运行同一导入，则可能会在网络映射中找到某些项目的重复数据。为避免这些问题，可能要在运行实际导入之前测试导入文件的导入。有关详细信息，请参阅在管理中心上测试导入（第 2-24 页）。

请注意，如果在有权访问管理中心的远程主机上设置主机输入参考客户端，则可以使用 `sf_host_input_agent.pl` 脚本从客户端处理导入文件。有关设置参考客户端的详细信息，请参阅运行主机输入参考客户端（第 3-4 页）。

要运行导入，请执行以下操作：

1. 将所创建的导入文件复制到要运行导入的管理中心。
2. 使用 `root` 帐户登录到管理中心中。
3. 在命令行中，键入 `nmimport.pl` *`filename`*。

   要将测试导入的结果重定向到日志文件，请将 `>` *`logfilename`* 添加到命令结尾。

   系统将已导入的数据添加到网络映射，并在屏幕上显示结果消息或将其重定向到指定的文件。

配置主机输入客户端

除接受来自管理中心上的用户的主机输入命令以外，管理中心的主机输入服务还接受来自外部主机上经过身份验证的主机输入客户端的批量导入文件。您可以使用主机输入客户端处理为主机输入导入工具创建的导入文件，然后将数据发送到管理中心，从而将信息添加到网络映射。

可以使用所提供的主机输入 API 参考客户端处理和发送 CSV 数据，或者测试主机输入客户端与管理中心的连接。

请执行以下任务来管理管理中心与输入客户端的交互：

1. 建立经过身份验证的管理中心连接。

   有关生成身份验证凭证以建立经过身份验证的管理中心连接的信息，请参阅向管理中心注册主机输入客户端（第 3-1 页）。

2. 在计划运行参考客户端的计算机上设置该参考客户端。有关详细信息，请参阅使用主机输入参考客户端（第 3-2 页）。

   有关创建将使用参考客户端处理的导入文件（也称为命令文件）的信息，请参阅编写主机输入导入文件（第 2-3 页）。

向管理中心注册主机输入客户端

许可证：任意

您必须先向管理中心注册运行客户端的计算机，然后才能使用主机输入客户端。管理中心之后将生成会下载到客户端计算机的身份验证证书。

要添加主机输入客户端，请执行以下操作：

访问权限：管理员

1. 如果已在系统中创建域，请在域切换程序中选择所需的域。使用为全局域或其他父域创建的证书的客户端将有权修改该范围内的任何枝叶域，但是导入文件必须指定具体的域。使用为枝叶域创建的证书的客户端仅有权修改该枝叶域。

2. 依次选择**系统 (System) > 集成 (Integration) > 主机输入客户端 (Host Input Client)**。

   系统将显示“主机输入客户端”(Host Input Client) 页面。

3. 点击**创建客户端 (Create Client)**。

   系统将显示“创建客户端”(Create Client) 页面。

4. 在**主机名 (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。

注意：如果使用主机名，则主机输入服务器**必须**能够将主机解析为 IP 地址。如果尚未配置 DNS 解析，应先配置解析或使用 IP 地址。

5. 如果想要对证书文件进行加密，请在**密码 (Password)** 字段中输入密码。
6. 点击**保存 (Save)**。

   主机输入服务允许客户端计算机在管理中心上访问端口 8307，并创建要在客户端-服务器身份验证期间使用的身份验证证书。系统将再次显示“主机输入客户端”(Host Input Client) 页面，其中会在**主机输入客户端 (Host Input Clients)** 下列出新的客户端。
7. 点击证书文件旁边的下载图标 ()。
8. 将证书文件保存到供客户端计算机用于 SSL 身份验证的目录。

   客户端现在可以连接到管理中心。

注意：要撤消客户端的访问权限，请点击要删除的主机旁边的删除图标 ()。请注意，无需重新启动管理中心上的主机输入服务；系统会立即撤销访问权限。

将客户端连接到管理中心

当客户端连接时，管理中心上的主机输入服务从客户端读取版本。如果客户端发送比服务器的版本更新的版本，则服务会拒绝连接。

此外，在初次交换期间，主机输入服务会将每个事务的最大允许数据大小传达到客户端。如果客户端尝试发送大于最大大小的数据块，则服务器会关闭连接。

使用主机输入参考客户端

主机输入 SKD 随附的参考客户端是说明如何使用主机输入 API 的一系列示例客户端脚本和 Perl 模块。您可以运行这些脚本和模块来自行熟悉主机输入导入，也可以将其用于调试定制客户端的安装问题。您还可以使用其中一个脚本处理来自客户端的主机输入命令文件。

有关设置参考客户端的详细信息，请参阅以下各节：

- 设置主机输入参考客户端（第 3-2 页）
- 运行主机输入参考客户端（第 3-4 页）

设置主机输入参考客户端

要使用主机输入参考客户端，您必须先安装样本脚本并将客户端配置为符合脚本要求。

有关详细信息，请参阅以下各节：

- 了解主机输入参考客户端（第 3-3 页）
- 配置主机输入配置参考客户端的通信（第 3-3 页）
- 加载主机输入参考客户端的常规必备软件（第 3-3 页）
- 下载并解压缩主机输入参考客户端（第 3-3 页）
- 创建主机输入参考客户端的证书（第 3-3 页）

了解主机输入参考客户端

您可以下载 HostInputClientSDK.zip 软件包，其中包含来自思科支持站点的主机输入参考客户端。表 3-1 主机输入参考客户端文件（第 3-3 页）列出 HostInputClientSDK.zip 软件包中包含的文件。

表 3-1 主机输入参考客户端文件

文件名	说明
SFHIClient.pm	此 Perl 模块包含由 Perl 客户端调用的命令。
SFPkcs12.pm	此 Perl 模块解析客户端证书并允许客户端连接到管理中心。
sf_host_input_agent.pl	可以使用此 Perl 脚本通过指定相应的输入插件和命令文件来导入 CSV 数据。
InputPlugins/csv.pm	可以调用此 Perl 模块运行用于导入 CSV 数据的命令文件。

配置主机输入配置参考客户端的通信

参考客户端使用安全套接字层 (SSL) 协议进行数据通信。您必须在计划用作客户端的计算机上安装 OpenSSL，并且针对您的环境适当对其进行配置。

要在客户端上设置 SSL，请执行以下操作：

1. 从 http://openssl.org/source/ 下载 OpenSSL。
2. 将源解压缩到 /usr/local/src。
3. 通过运行配置脚本来配置源。
4. 创建并安装已编译的源。

加载主机输入参考客户端的常规必备软件

您必须先在客户端计算机上安装 IO::Socket::SSL Perl 模块，然后才能运行主机输入参考客户端。可以手动安装该模块，也可以使用 cpan 进行安装。

注意：如果未在客户端计算机上安装 Net::SSLeay 模块，请也安装该模块。Net::SSLeay 对于与 OpenSSL 通信是必需的。

您还需要安装并配置 OpenSSL 以支持与管理中心的 SSL 连接。有关详细信息，请参阅配置主机输入配置参考客户端的通信（第 3-3 页）。

此外，如果计划将 Qualys 插件用于主机输入客户端，则必须安装 XML::Smart Perl 模块及其必备软件。如果计划使用 IPv6 在客户端与管理中心之间进行通信，还必须安装 IO::Socket::INET6 Perl 模块。

下载并解压缩主机输入参考客户端

您可以下载包含来自支持站点的主机输入参考客户端的 HostInputClientSDK.zip 文件。

将 zip 文件解压缩到运行 Linux 操作系统的计算机（计划运行客户端）。

创建主机输入参考客户端的证书

许可证：任意

您需要先按照向管理中心注册主机输入客户端（第 3-1 页）中所述创建客户端证书，然后才能使用主机输入参考客户端。必须将证书文件保存到放置参考客户端的目录。

要创建参考客户端的证书，请执行以下操作：

访问权限：管理员

1. 按照向管理中心注册主机输入客户端（第 3-1 页）中所述创建客户端。
2. 将证书文件保存到放置参考客户端的目录。

运行主机输入参考客户端

主机输入 Perl 参考客户端脚本设计为在具有 Linux 内核的操作系统上使用，但是应在任何基于 POSIX 的操作系统上适用，只要客户端计算机满足设置主机输入参考客户端（第 3-2 页）中定义的必备条件即可。

您可以在管理中心上使用参考客户端将 CSV 数据从远程客户端导入到网络映射。

使用以下语法运行 `sf_host_input_agent.pl` 脚本：

```
./sf_host_input_agent.pl -server=ManagementCenterIPAddress -level=DebugLevel
-logfile=LogFile -pluginfo=CSVCommandFile.csv
```

例如，使用名为 `csv_file.txt` 的 CSV 文件导入到 IP 地址为 10.10.0.4 且向 HostInput.log 日志文件记录调试日志的管理中心：

```
./sf_host_input_agent.pl -server=10.10.0.4 -level=3 -logfile=HostInput.log
-pluginfo=cvs_file.txt csv
```

网络协议值

使用 `AddProtocol` 和 `DeleteProtocol` 命令，您可以向主机中添加协议或从主机中删除协议。下表详述可用的网络协议值。

表 A-1　　网络协议值

值	说明
IP	Internet 协议版本 4
ARP	地址解析协议
BPDU(STP)	网桥协议数据单元（生成树协议）
RARP	反向地址解析协议
OldIPX	网间数据包交换，早期版本
IP Version 6	Internet 协议版本 6
Loopback	环回
SNAP	子网访问协议
Novell NetWare	Novell NetWare
NetBIOS	网络基本输入/输出系统
NetBIOS (Response)	网络基本输入/输出系统响应
IPX	网间数据包交换
Intel ANS	Intel 高级网络服务
DEC MOP Dump/Load Assistance	Digital Equipment Corporation 维护操作协议转储/负载帮助
DEC MOP Remote Console	Digital Equipment Corporation 维护操作协议远程控制台
PPPoE Discovery	以太网上的点对点发现阶段
PPPoE Session	以太网上的点对点会话阶段