主机配置文件

以下主题介绍如何使用主机配置文件：

主机配置文件的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员

- 安全分析师

主机配置文件

主机配置文件可完整展现系统搜集到的有关单台主机的全部信息。要访问主机配置文件，请执行以下操作：

- 从任何网络映射视图进行导航。
- 从包含受监控网络上主机的 IP 地址的任何事件视图进行导航。

主机配置文件提供有关检测到的主机或设备的基本信息，例如主机名或 MAC 地址。根据许可证和系统配置，主机配置文件还可提供以下信息：

- 在主机上运行的操作系统
- 在主机上运行的服务器
- 在主机上运行的客户端和 Web 应用
- 在主机上运行的协议
- 主机上的危害表现 (IOC) 标记
- 主机上的 VLAN 标记
- 过去 24 小时网络上的用户活动
- 与主机关联的合规性 allow 违规
- 主机的最新恶意软件事件
- 与主机关联的漏洞
- 主机的 Nmap 扫描结果

配置文件中还会列出主机属性。您可以对您的网络环境而言重要的方式使用主机属性对主机进行分类例如，您可以：

- 分配表示主机所在建筑物的主机属性
- 使用主机重要性属性指定特定主机的业务重要性，并根据主机重要性定制关联策略和警报

从主机配置文件中，您可以查看应用于该主机的现有主机属性，并修改主机属性值。

如果将自适应配置文件用作被动入侵防御部署的一部分，则可以定制系统处理流量的方式，以使其最适合于主机上的操作系统的类型，以及主机正在运行的服务器和客户端。

或者，可以从主机配置文件执行Nmap扫描，以扩充主机配置文件中的服务器和操作系统信息。Nmap扫描工具主动扫描主机以获得在主机上运行的操作系统和服务器的有关信息。扫描结果会添加到主机操作系统和服务器身份列表。

相关主题

查看主机配置文件 ，第 3 页

主机配置文件限制

不可用主机

主机配置文件可能并不适用于网络上的每台主机。可能的原因包括：

- 主机由于超时而从网络映射中删除。
- 已达到主机限制。
- 主机所在的网段不受网络发现策略的监控。

不可用信息

主机配置文件中显示的信息可能根据主机类型和有关主机的可用信息而异。

例如：

- 例如，如果系统检测到使用非基于 IP 的协议（例如 STP、SNAP 或 IPX）的主机，则会将该主机作为 MAC 主机添加到网络映射中，并且该主机的可用信息远远少于 IP 主机。
- 系统可以将主机从导出的 NetFlow 记录中添加到网络映射中，但是这些主机的可用信息是有限的；请参阅NetFlow 和受管设备数据之间的差异。

（运行 VRF 的部署）单个 IP 地址可能代表多个主机

如果主机是由运行 VRF 的设备报告的，则单个 IP 地址实际上可能代表多个主机。VRF 可以监控具有重叠 IP 地址的多个网络，因此相同的 IP 地址可以存在于不同的网络中。

查看主机配置文件

过程

您有两种选择：

- 在任何网络映射上，钻取至想要浏览的配置文件的主机的 IP 地址。
- 在任何事件视图上，点击想要浏览的配置文件的主机 IP 地址旁边的 **主机配置文件** 或 **受攻击的主机** 。

主机配置文件中的基本主机信息

每个主机配置文件均可提供有关检测到的主机或其他设备的基本信息。

主机配置文件中的每个基本字段的描述如下。

域

与主机关联的域。

IP 地址

所有与主机相关的IP地址（IPv4和IPv6）。系统检测与主机相关的IP地址，并且，如果支持的话，把同一主机使用的多个 IP 地址进行分组。IPv6 主机通常至少包含两个 IPv6 地址（纯本地和全局可路由），也可能包含 IPv4 地址。纯 IPv4 主机可拥有多个 IPv4 地址。

主机配置文件列出所有检测到的与该主机相关的 IP 地址。如可用，路由主机 IP 地址还包含一个表明与地址相关的地理位置数据的旗帜图标和国家代码。

请注意，默认情况下，仅显示前三个地址。点击**全部显示 (show all)** 显示主机的所有地址。

主机名

如果已知，为主机的完全限定域名。

NetBIOS 名称

如果可用，为主机的 NetBIOS 名称。为使用 NetBIOS 而配置的 Microsoft Windows 主机，以及 Macintosh、Linux 或其他平台都可以拥有一个 NetBIOS 名称。例如，配置为 Samba 服务器的 Linux 主机可拥有多个 NetBIOS 名称。

设备（跳数)

可以为以下任意一项：

- 根据网络发现策略中的定义，主机所在网络的报告设备，或者
- 处理将主机添加至网络映射的 NetFlow 数据的设备

检测到主机的设备与设备名称后面的主机之间的网络跳数（使用括号括起）。如果多台设备可以看见主机，则报告设备将以粗体显示。

如果此字段为空，则可能出现以下情况：

- 按照网络发现策略中的规定，由未明确监控主机所在网络的设备将该主机添加到网络映射中，或
- 已使用主机输入功能成功添加该主机，但系统尚未检测到。

MAC 地址 (TTL)

主机被检测到的一个或多个 MAC 地址和相关 NIC 供应商，括号中为 NIC 硬件供应商和当前生存时间 (TTL) 值。

如果有多台设备检测到主机，不管是哪台设备报告的地址，管理中心都会显示与主机相关的所有 MAC 地址和 TTL 值。

如果 MAC 地址以粗体显示，则 MAC 地址是系统通过 ARP 和 DHCP 流量检测到的主机的实际/真实/主 MAC 地址，通过 ARP 和 DHCP 流量检测与 IP 地址确定绑定。

未以粗体显示的 MAC 地址是辅助地址，无法与主机的 IP 地址明确关联。例如，由于 防火墙 设备只能为其自身网段上的主机获取 MAC 地址，如果流量来自 防火墙 设备未直接连接的网段，则观察到的 MAC 地址（即路由器 MAC 地址）将是显示为主机的辅助 MAC 地址。

主机类型

系统检测到的设备类型：主机、移动设备、越狱的移动设备、路由器、网桥、NAT 设备或负载均衡器。

系统用于区分网络设备的方法包括：

- 分析思科发现协议 (CDP) 消息，可识别网络设备及其类型（仅限思科设备）
- 检测生成树协议 (STP)，可将设备识别为交换机或网桥
- 检测多个使用相同 MAC 地址的主机，可识别属于路由器的 MAC 地址
- 检测客户端 TTL 值变化，或检测比典型启动时间变化更频繁的 TTL 值，可识别 NAT 设备和负载均衡器
- 系统用于区分移动设备的方法包括：
- 分析来自移动设备的移动浏览器的 HTTP 流量中的用户代理字符串
- 监控特定移动应用的 HTTP 流量

如果某一设备未被确定为网络设备或移动设备，则该设备将归类为主机。

上次查看时间

最后一次检测主机的 IP 地址的日期和时间。

当前用户

最近一次登录该主机的用户。

请注意，只有当现有当前用户不是授权用户时，登录主机的非授权用户才注册为当前用户。

查看

连接、发现、恶意软件和入侵事件数据视图链接，使用该事件类型的默认工作流程并仅限于显示与主机相关的事件；如果可能，这些事件包括与主机相关的所有 IP 地址。

主机配置文件中的操作系统

通过分析流量中主机生成的网络和应用堆叠或分析用户代理报告的主机数据，系统可被动检测运行在主机上的操作系统的身份。此外，系统还将核对其他来源的操作系统信息，比如通过主机输入功

能导入的 Nmap 扫描工具或应用数据。当确定将要使用的身份时，系统会考虑分配给每个身份源的优先级。默认情况下，用户输入具有最高优先级，其次是应用或扫描工具源，最后是所发现的身份。

有时候，系统会提供通用操作系统定义而非具体的定义，因为流量和其他身份源没有提供足够的信息来确定更具针对性的身份。系统将整理各种来源的信息，以尽可能利用最详细的定义。

由于操作系统会影响主机的漏洞列表以及针对主机的事件的事件影响关联，因此可能要手动提供更多具体的操作系统信息。此外，可表明已将修复（比如服务包和更新）应用到操作系统，并使修复已经解决的任何漏洞失效。

例如，如果系统确定主机的操作系统为 Microsoft Windows 2003，但主机实际上运行的是 Microsoft Windows XP Professional SP2，则可相应地设置操作系统身份。设置更具体的操作系统身份可以完善主机漏洞列表，以便该主机的影响关联更具针对性、更准确。

如果系统检测到的主机操作系统信息与由活动源提供的现有操作系统身份相冲突，则会发生身份冲突。当确实存在身份冲突时，系统将同时使用两种身份来表明漏洞和影响关联。

可以配置网络发现策略以将发现数据添加到受 NetFlow 导出器监控的主机的网络映射中。但是，除非设置主机输入功能来设置操作系统身份，否则没有可用于这些主机的操作系统数据。

如果主机运行的操作系统违反已激活的网络发现策略中的合规 allow 名单，则 管理中心 会利用 allow 名单 **违规**来标记操作系统信息。此外，如果越狱的移动设备违反有效的 allow 名单，该图标会出现在该设备的操作系统旁边。

可以为主机的操作系统身份设置自定义显示字符串。上述显示字符串随后用于主机配置文件中。

注释 更改主机的操作系统信息可能会更改其与合规 allow 名单的合规情况。

在网络设备的主机配置文件中，“操作系统”(Operating Systems) 部分的标签更改为“系统”(Systems)，并会另外显示“硬件”(Hardware) 列。如果“系统”下列出了硬件平台值，则该系统代表在网络设备后检测到的一个或多个移动设备。请注意，移动设备可能有，也可能没有硬件平台信息，但不会检测到非移动设备系统的硬件平台信息。

主机配置文件中显示的操作系统信息字段说明如下。

硬件

移动设备的硬件平台。

操作系统供应商/供应商

操作系统供应商。

操作系统产品/产品

选择以下值之一：

- 根据从所有来源收集的身份数据确定为最可能在主机上运行的操作系统
- `Pending`，如果系统尚未识别操作系统，并且没有其他身份数据可用

- unknown，如果系统无法识别操作系统，并且没有其他身份数据可用于操作系统

注释 如果主机的操作系统不是系统能够检测的系统，请参阅《Cisco Secure Firewall Management Center 设备配置指南》主机身份源 一章。

操作系统版本/版本

操作系统版本。如果主机是破解的移动设备，则版本后面的括号里会指示 Jailbroken。

来源

选择以下值之一：

- 用户：user_name
- 应用：app_name
- 扫描工具：scanner_type（Nmap 或其他扫描工具）
- FirePOWER

系统可能会从多个源协调数据，以确定操作系统的身份。

查看操作系统身份

可查看发现的或添加的主机特定操作系统的身份。系统利用来源优先分级来确定主机当前的身份。在身份列表中，当前身份以粗体突出显示。

请注意，仅当主机存在多个操作系统身份时，**查看** 才可用。

过程

步骤 1 点击主机配置文件的**操作系统 (Operating System)** 或**操作系统冲突 (Operating System Conflicts)** 部分中的**查看 (View)**。

步骤 2 查看主机配置文件中的操作系统，第 5 页中所述的信息。

步骤 3 或者，点击任何操作系统身份旁边的 **删除** ( ) 。

注释
不能删除思科检测到的操作系统身份。

此系统从“操作系统身份信息”(Operating System Identity Information) 弹出窗口中删除身份，并在适用情况下更新主机配置文件中的操作系统的当前身份。

设置当前操作系统身份

可以使用 Firepower 系统 Web 界面设置主机的当前操作系统身份。在网络界面设置标识来覆盖所有其他标识源，以便把标识用于漏洞评估和影响相关性。但是，如果在编辑操作系统后，系统检测到主机存在冲突的操作系统身份，则会发生操作系统冲突。在解决冲突前，这两种操作系统都被视为当前操作系统。

过程

步骤 1 点击主机配置文件的**操作系统 (Operating System)** 部分中的**编辑 (Edit)**。

步骤 2 此时有多个选择：

- 从**操作系统定义 (OS Definition)** 下拉列表中选择**当前定义 (Current Definition)**，通过主机输入确认当前的操作系统身份，然后跳转至步骤 6。
- 从**操作系统定义 (OS Definition)** 下拉列表中选择当前操作系统身份的变体，然后跳转至步骤 6。
- 从**操作系统定义 (OS Definition)** 下拉列表中选择**用户定义 (User-Defined)**，然后继续执行步骤 3。

步骤 3 或者，选择**使用自定义显示字符串 (Use Custom Display String)**，然后修改要在**供应商字符串 (Vendor String)**、**产品字符串 (Product String)** 和 **版本字符串 (Version String)** 字段中显示的自定义字符串。

步骤 4 或者，要更改为不同供应商提供的操作系统，请从**供应商 (Vendor)** 和**产品 (Product)** 下拉列表中选择。

步骤 5 或者，要配置操作系统的产品版本级别，请从**主要版本 (Major)**、**次要版本 (Minor)**、**修订版本 (Revision)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)** 下拉列表中选择。

步骤 6 或者，如果要表示已经应用操作系统的修复，请点击**配置修复 (Configure Fixes)**。

步骤 7 在下拉列表中选择适用的修复，然后点击**添加 (Add)**。

步骤 8 或者，使用 **Patch** 和 **Extension** 下拉列表添加相关补丁和扩展。

步骤 9 点击**完成**。

相关主题

操作系统身份冲突，第 8 页

操作系统身份冲突

如果当前身份是由诸如扫描程序、应用或用户之类的活动源提供，当系统检测到的新身份与当前标身份突时，会发生操作系统身份冲突。

冲突的操作系统身份列表在主机配置文件中以粗体显示。

可在系统 Web 界面解决身份冲突并设置主机当前的操作系统身份。在 Web 界面设置身份来覆盖所有其他身份源，以便把身份用于漏洞评估和影响相关性。

使冲突的操作系统身份成为当前身份

过程

步骤 1 导航至主机配置文件的**操作系统 (Operating System)** 部分。

步骤 2 您有两种选择：

- 点击要设置为主机操作系统的操作系统身份旁边的**成为当前身份 (Make Current)**。
- 如果不希望作为当前身份的身份来自活动源，请删除不需要的身份。

解决操作系统身份冲突

过程

步骤 1 在主机配置文件的**操作系统冲突 (Operating System Conflicts)** 部分点击**解决 (Resolve)**。

步骤 2 有以下选项可供选择：

- 从**操作系统定义 (OS Definition)** 下拉列表中选择**当前定义 (Current Definition)**，通过主机输入确认当前的操作系统身份，然后跳转至步骤 6。
- 从**操作系统定义 (OS Definition)** 下拉列表中选择相互冲突的操作系统身份上的一个变体，然后跳转至步骤 6。
- 从**操作系统定义 (OS Definition)** 下拉列表中选择**用户定义 (User-Defined)**，然后继续执行步骤 3。

步骤 3 或者，选择**使用自定义显示字符串 (Use Custom Display String)**，然后输入要在**供应商字符串 (Vendor String)**、**产品字符串 (Product String)** 和**版本字符串 (Version String)** 字段中显示的自定义字符串。

步骤 4 或者，要更改为不同供应商提供的操作系统，请从**供应商 (Vendor)** 和**产品 (Product)** 下拉列表中选择。

步骤 5 或者，要配置操作系统的产品版本级别，请从**主要版本**、**次要版本**、**修订版本**、**内部版本**、**补丁**和**扩展版本**下拉列表中选择。

步骤 6 或者，如果要表示已经应用操作系统的修复，请点击**配置修复 (Configure Fixes)**。

步骤 7 把已经应用的修复添加至修复列表。

步骤 8 点击**完成**。

主机配置文件中的服务器

主机配置文件的“服务器”(Servers) 部分列出在受监控网络中的主机上检测到的服务器、从导出的 NetFlow 记录添加的服务器、或者通过主动源（如扫描工具）或主机输入功能添加的服务器。

列表中每台主机最多可包含 100 台服务器。达到限制后，不管是源自活动源或被动源的新服务器信息都会被删除，直到您从主机上删除服务器或服务器超时。

如果使用 Nmap 扫描主机，Nmap 会把此前未检测到的在开放 TCP 端口运行的服务器的结果添加至服务器列表。如果进行 Nmap 扫描或导入 Nmap 结果，可展开的“扫描结果”(Scan Results) 部分内容也会出现在主机配置文件中，列出 Nmap 扫描工具在主机上检测到的服务器信息。此外，如果从网络映射中删掉主机，主机服务器的 Nmap 扫描结果会被丢弃。

注释 系统可以将主机从导出的 NetFlow 记录中添加到网络映射中，但是这些主机的可用信息是有限的；请参阅NetFlow 和受管设备数据之间的差异。

使用主机配置文件中的服务器的流程取决于访问文件的方式：

- 如果通过网络映射访问主机配置文件，会出现该服务器的详细信息，粗体高亮该服务器的名称。如果要查看主机上的任何其他服务器的详细信息，请点击服务器名称旁边的 **视图** ( ) 。
- 如果以任何其他方式访问主机配置文件，展开服务器部分并点击要查看详细信息的服务器旁边的 **视图** ( ) 。

注释 如果主机正在运行的是违反经激活的关联策略中的合规 allow 名单的服务器，则 管理中心 会利用 allow 名单 **违规**来标记不合规的服务器。

服务器列表中的列说明如下。

协议

服务器所用协议名称。

端口

运行服务器的端口。

应用协议

以下任一项：

- 应用协议的名称
- 如果系统由于多个原因之一无法肯定或否定地识别应用协议，则为 `pending`

- 如果系统无法根据已知应用协议指纹识别应用协议或如果在没有添加相应服务器的情况下，通过主机输入功能添加具有端口信息的漏洞来添加服务器，则为 unknown

将鼠标悬停在应用协议名称上，会显示标记。

供应商和版本 (Vendor and Version)

由系统、Nmap或其他主动源识别的或通过主机输入功能获得的供应商和版本。如果没有可用源提供任何识别信息，字段为空。

主机配置文件中的服务器详细信息

管理中心列出的每个服务器的被动检测到的身份最多可达 16 个。被动检测源包括网络发现数据和 NetFlow 记录。如果系统检测到多个供应商或服务器版本，该服务器可拥有多个被动标识。例如，如果网络服务器运行不同版本的服务器软件，受管设备和网络服务器场之间的负载均衡器会让系统识别多种 HTTP 被动标识。请注意，管理中心对源自活动源的服务器标识数量没有限制，例如，用户输入、扫描工具或其他应用。

管理中心将以粗体显示当前的标识。系统可将服务器当前的标识用于各种用途，包括将漏洞分配给主机、影响评估、根据主机配置文件限制性条件和合规 allow 名单编写评估相关性规则等。

服务器详细信息可显示与所选服务器相关的更新后的子服务器信息。

查看主机配置文件中的服务器时，服务器详细信息也可在服务器详细信息下方显示服务器横幅。服务器横幅提供关于服务器的额外信息，以帮助您识别服务器。当攻击者有意修改服务器横幅字符串时，系统无法识别或检测被错误识别的服务器。服务器横幅显示服务器检测到的第一个数据包的前 256 个字节。这类信息仅在系统第一次检测到服务器的时候收集，而且仅收集一次。横幅内容分两列列出，左侧以十六进制表示，右侧以相应的 ASCII 表示。

注释 要查看服务器横幅，您必须启用网络发现策略中的**捕获横幅 (Capture Banners)** 复选框。默认情况下该选项处于禁用状态。

主机配置文件的服务器详细信息部分显示以下信息：

协议

服务器所用协议名称。

端口

运行服务器的端口。

点击数

由系统受管设备或 Nmap 扫描工具检测到的服务器的次数。除非系统检测到该服务器的流量，否则通过主机输入导入的服务器的命中次数为 0。

上次使用时间 (Last Used)

上次检测到服务器的时间和日期。除非系统检测到该服务器有新的流量，否则主机输入数据的上次使用时间反映了初始数据导入时间。根据 管理中心配置中的设置，通过主机输入功能导入的扫描工具和应用数据会超时，但通过 管理中心 Web 界面的用户输入不会超时。

应用协议

如果已知，服务器所用的应用协议的名称。

供应商

服务器供应商。如果供应商未知，不显示该字段。

版本

服务器版本。如果版本未知，不显示该字段。

来源

选择以下值之一：

- 用户：user_name
- 应用：app_name
- 扫描工具：scanner_type（Nmap 或其他扫描工具）
- 对于系统检测到的应用，为 `Firepower`、`Firepower Port Match` 或 `Firepower Pattern Match`
- 对于从 NetFlow 记录添加到网络映射的服务器，为 `NetFlow`

系统可能会从多个源协调数据，以确定服务器的身份。

查看服务器详细信息

过程

在主机配置文件中，点击 **服务器** 部分的服务器旁边的 **视图** () 。

编辑服务器身份

可手动更新主机上服务器的身份设置和配置已经应用到主机的任何修复，以删除经修复解决的漏洞。此外，还可以删除服务器身份。

删除身份不会删除服务器，即使删除唯一身份也如此。删除标识会将标识从 Server Detail 弹出窗口移除，而且如果适用，更新主机配置文件中的服务器当前的标识。

不能编辑或删除由思科管理的设备添加的服务器身份。

过程

步骤 1 导航至主机配置文件的**服务器 (Servers)** 部分。

步骤 2 点击**查看 (View)** 以打开“服务器详细信息”(Server Detail) 弹出窗口。

步骤 3 要删除服务器身份，请点击要移除的服务器身份旁边的 **删除** ( ) 。

步骤 4 要修改服务器身份，请点击服务器列表中的服务器旁边的 **编辑** ( ) 。

步骤 5 您有两种选择：

- 从**选择服务器类型 (Select Server Type)** 下拉列表中选择当前定义。
- 从**选择服务器类型 (Select Server Type)** 下拉列表中选择服务器类型。

步骤 6 或者，要仅列出该服务器类型的供应商和产品，请选中**按服务器类型限制 (Restrict by Server Type)** 复选框。

步骤 7 或者，要自定义服务器的名称和版本，请选择**使用自定义显示字符串 (Use Custom Display String)**，然后输入**供应商字符串 (Vendor String)** 和**版本字符串 (Version String)**。

步骤 8 在**产品映射 (Product Mappings)** 部分中，选择要使用的操作系统、产品和版本。

示例：

例如，如果希望服务器映射到 Red Hat Linux 9，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 如果要指示已应用服务器的修复，请点击**配置修复 (Configure Fixes)**，并将要为该服务器应用的补丁添加到修复列表。

步骤 10 点击**完成**。

解决服务器身份冲突

当应用或扫描仪等活动源将服务器身份数据添加到主机上时，如果系统随后检测到该端口上出现表明冲突服务器身份的流量，则会出现服务器身份冲突。

过程

步骤 1 在主机配置文件中，导航至**服务器 (Servers)** 部分。

步骤 2 点击服务器旁边的解决。

步骤 3 从**选择服务器类型 (Select Server Type)** 下拉列表中选择服务器类型。

步骤 4 或者，要仅列出该服务器类型的供应商和产品，请选中**按服务器类型限制 (Restrict by Server Type)** 复选框。

步骤 5 或者，要自定义服务器的名称和版本，请选择**用户自定义显示字符串 (Use Custom Display String)**，然后输入**供应商字符串 (Vendor String)** 和**版本字符串 (Version String)**。

步骤 6 在**产品映射 (Product Mappings)** 部分中，选择要使用的操作系统、产品和版本。

示例：

例如，如果希望服务器映射到 Red Hat Linux 9，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 7 如果要指示已应用服务器的修复，请点击**配置修复 (Configure Fixes)**，并将要为该服务器应用的补丁添加到修复列表。

步骤 8 点击**完成**。

主机配置文件中的 Web 应用

主机配置文件的“Web 应用”(Web Application) 部分显示系统识别为在您的网络主机上运行的客户端和 Web 应用。系统可同时从被动和主动检测源识别客户端和 Web 应用信息，但是从 NetFlow 记录添加的主机信息有限。

此部分的详细信息包含在主机上检测到的应用的产品和版本、任何可用客户端或 Web 应用信息，以及上一次检测到使用应用的时间。

此部分最多列出16个在主机上运行的客户端。在达到限制后，会丢弃来自主动或被动来源的新客户端信息，直到您从主机上删除客户端应用，或系统由于客户端闲置把客户端从主机配置文件中删除（客户端超时）。

此外，对于每个检测到的网络浏览器，系统会显示浏览器访问的前 100 个 Web 应用。在达到限制后，会丢弃来自主动或被动来源的与该浏览器相关的新 Web 应用，直到出现下列任何一种情况：

- 网络浏览器客户端应用超时，或
- 从主机配置文件删除与 Web 应用相关的应用信息

如果主机正在运行的是违反经激活的关联策略中的合规 allow 名单的应用，则 Firepower 管理中心会利用 allow 名单 **违规**来标记不合规的应用。

提示 要分析与主机上特定应用相关的连接事件，请点击该应用旁边的 **日志记录**（ ）。系统将显示连接事件首选工作流程的首页，该页面显示受应用的类型、产品和版本，以及主机的 IP 地址限制的连接事件。如果连接事件没有首选工作流程，必须选择一个首选工作流程。

下面介绍主机配置文件中显示的应用信息。

应用协议

显示应用（HTTP 浏览器、DNS 客户端等等）所使用的应用协议。

客户端

来源于负载的客户端信息，由 Firepower 系统识别、由 Nmap 捕获、或通过主机输入功能获得。如果没有可用源提供任何识别信息，字段为空。

版本

显示客户端版本。

Web 应用

对于网络浏览器，为系统在 http 流量中检测到的内容。Web 应用信息表示由 Firepower 系统识别、由 Nmap 捕获、或通过主机输入功能获得的特定类型的内容（例如，WMV 或 QuickTime）。如果没有可用源提供任何识别信息，字段为空。

从主机配置文件中删除 Web 应用

要移除已知的未在主机上运行的应用，您可从主机配置文件删除该应用。请注意，删除主机上的应用可让主机符合合规 allow 名单。

注释 如果系统再次检测到应用，系统会将该应用重新添加至网络映射和主机配置文件。

过程

步骤 1 在主机配置文件中，导航至**应用 (Applications)** 部分。

步骤 2 点击要删除的应用旁边的 **删除** ( ) 。

主机配置文件中的主机协议

每个主机配置文件都包含在网络流量中检测到的与主机关联的协议有关的信息。此信息包括：

协议

指主机使用的协议的名称。

层

指协议运行的网络层（`Network` 或 `Transport`）。

如果主机配置文件中显示的协议违反经激活的关联策略中的合规 allow 名单，则 管理中心 会利用 allow 名单 **违规**来标记不符合规定的协议。

如果主机配置文件列出您已知不在该主机上运行的协议，则可以删除那些协议。从主机上删除协议可让主机符合合规 allow 名单。

注释 如果系统再次检测到协议，系统会将该协议重新添加至网络映射和主机配置文件。

从主机配置文件中删除协议

过程

步骤 1 导航至主机配置文件的**协议 (Protocols)** 部分。

步骤 2 点击要删除的协议旁边的 **删除** ( ) 。

主机配置文件中的危害表现

系统将各种类型的数据（入侵事件、安全智能、连接事件及文件或恶意软件事件）进行关联，以确定受监控网络上的主机是否可能受到恶意手段的危害。事件数据的某些组合和频率触发了受影响主机上的危害表现 (IOC) 标记。

主机配置文件中的“危害表现”部分将显示主机的所有危害表现标记。

要配置系统以标记危害表现，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的妥协规则的启用指示 。

有关使用危害表现的详细信息，请参阅危害表现数据和相应主题下的子主题。

主机配置文件中的 VLAN 标记

如果主机构成虚拟局域网 (VLAN) 的一部分，系统会显示主机配置文件的 VLAN Tag 部分。

物理网络设备通常使用 VLAN 从各种网络块创建逻辑网段。系统检测到 802.1q VLAN 标记并显示每个标记的下列信息：

- **VLAN ID** 标识主机所属的 VLAN。对于 802.1q VLAN，它可以是介于 0 至 4095 之间的任何整数。
- **类型 (Type)** 标识包含 VLAN 标记的封装包，可以是以太网或令牌环。
- **优先级 (Priority)** 标识在 VLAN 标记中的优先级，可以是 0 至 7 之间的任何一个整数，其中 7 表示最高优先级。

如果VLAN标记嵌套在数据包中，系统进行处理，且管理中心显示最里面的VLAN标记。系统仅收集并显示其通过 ARP 和 DHCP 流量识别的 MAC 地址的 VLAN 标记信息。

例如，在一个全部由打印机构成的VLAN中，并且系统在该VLAN中检测到Microsoft Windows 2000操作系统，VLAN 标记信息是有用的。此外，VLAN 信息帮助系统生成更准确的网络映射。

主机配置文件中的用户历史记录

主机配置文件的用户历史记录部分将为过去二十四小时的用户活动提供图形表示。典型的用户会在晚上注销，并有可能与其他用户共享主机资源。用正常的短条形表示定期登录请求，例如要查看邮件的登录请求。用户标识列表附带有条形图，表明检测到用户登录的时间。请注意，对于未授权的登录，条形图将灰显。

请注意，系统的确会将主机上未授权的用户登录与该主机的IP地址关联，因此，用户会显示在该主机的用户历史中。然而，如果检测到同一台主机的授权用户登录，则与授权用户登录相关的用户将沿用与主机 IP 地址的关联，而新的未授权用户登录不会破坏用户与主机 IP 地址的关联。如果在网络发现策略中配置捕获失败的登录，列表包括登录主机失败的用户。

主机配置文件中的主机属性

可利用主机属性按照对网络环境而言重要的方式来对主机进行分门别类。Firepower系统中有三种类型的属性：

- 预定义主机属性
- 合规 *allow* 名单主机属性
- 用户定义的主机属性

在设置预定义主机属性或创建用户定义的主机属性后，必须分配主机属性值。

注释 主机属性可在任意域级别定义。可以分配在当前和祖先域中创建的主机属性。

预定义主机属性

管理中心提供两个预定义的主机属性：

主机重要性

此属性用于指定特定主机的业务重要性，并根据主机重要性定制关联响应。例如，如果您认为组织的邮件服务器比一般用户工作站对业务更重要，可以将“高”(High) 值分配给邮件服务器和其他业务关键设备，将“中”(Medium) 或“低”(Low) 值分配给其他主机。然后，根据受影响的主机重要性创建可发出不同警报的关联策略。

说明

此特定主机属性用于记录需要其他分析师查看的主机的信息。例如，如果网络上有使用测试用旧版未打补丁操作系统的计算机，可使用注释功能注明此系统特意未打补丁。

允许 列表主机属性

所创建的每个合规 allow 名单会创建与 allow 名单具有相同名称的主机属性。 allow 名单主机属性的可能值包括：

- 合规 - 识别符合 allow 名单的主机。
- 不合规 - 识别违反 allow 名单的主机。
- 未评估 - 识别不是 allow 名单的有效目标或因任何原因尚未评估的主机。

不能编辑 an allow 名单主机属性值或删除 an allow 名单主机属性。

用户定义的主机属性

如果要使用与那些预定义主机属性或合规 allow 名单主机属性中所用的不同的条件识别主机，您可以创建用户定义的主机属性。例如，您可以：

- 向主机分配物理位置标识符，比如设施代码、城市或房间号码。
- 分配表明特定主机的系统管理员的责任方标识符。然后，制定相关性规则和策略，当检测到与主机相关的问题时，把警报发送给适当的系统管理员。
- 根据主机的IP地址自动将预先定义的列表值分配给主机。当新主机第一次出现在网络上时，可使用此功能将值分配给新主机。

用户定义的主机属性显示在主机配置文件页面中，可在此页面为每台主机分配值。您还可以：

- 在关联策略和搜索中使用这些属性。
- 在事件的主机属性表视图中查看属性并据此生成报告。

用户定义的主机属性可以是以下类型之一：

文本

允许您手动将文本字符串分配给主机。

整数

允许用户指定一系列正整数中的第一个和最后一个数字，然后手动把这些数字中的一个数字分配给主机。

名单

允许您创建字符串值列表，然后手动将这些值中的其中一个分配给主机。此外，还可根据主机的 IP 地址自动把值分配给主机。

如果根据具有多个 IP 地址的主机的一个 IP 地址自动分配值，那些值将应用到与该主机相关的所有地址。当查看 Host Attributes 表时，请记住此点。

自动分配列表值时，请考虑使用网络对象而不是文字 IP 地址。此方法可提高可维护性，尤其是在多域部署中。在这种部署中，通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义祖先配置。在多域部署中，在祖先域级别定义自动分配的列表时务必要小心谨慎，以避免在后代域使用重叠 IP 地址时与非预定主机匹配。

URL

允许您手动将 URL 值分配给主机。

删除用户定义的主机属性可将用户定义的主机属性从所有使用该主机属性的主机配置文件中删除。

创建基于文本或 URL 的主机属性

过程

步骤 1 选择**分析** > **主机标题** > **主机属性**。
步骤 2 点击 **Host Attribute Management**。
步骤 3 点击 **Create Attribute**。
步骤 4 输入 **Name**。
步骤 5 在**类型**中选择要创建的属性的类型，如用户定义的主机属性，第 18 页中所述
步骤 6 点击**保存 (Save)**。

创建基于整数的主机属性

当定义基于整数的主机属性时，必须指定属性接受的数字范围。

过程

步骤 1 选择**分析** > **主机标题** > **主机属性**。
步骤 2 点击 **Host Attribute Management**。
步骤 3 点击 **Create Attribute**。
步骤 4 输入 **Name**。
步骤 5 在**类型 (Type)** 中选择要创建的属性的类型，如用户定义的主机属性，第 18 页中所述。
步骤 6 在**最小值 (Min)** 字段中，输入可分配给主机的最小整数值。
步骤 7 在**最大值 (Max)** 字段，输入可分配给主机的最大整数值。

步骤 8 点击**保存 (Save)**。

创建基于列表的主机属性

当定义基于列表的主机属性时，必须为列表提供所有的值。这些值可包含字母数字字符、空格和符号。

过程

步骤 1 选择**分析** > **主机标题** > **主机属性**。
步骤 2 点击 **Host Attribute Management**。
步骤 3 点击 **Create Attribute**。
步骤 4 输入 **Name**。
步骤 5 在**类型 (Type)** 中选择要创建的属性的类型，如用户定义的主机属性，第 18 页中所述。
步骤 6 要将值添加到列表，请点击**添加值 (Add Value)**。
步骤 7 在**名称 (Name)** 字段中，输入要添加的第一个值。
步骤 8 或者，要自动分配刚刚添加到主机属性值，请点击**添加网络 (Add Networks)**。
步骤 9 从**值 (Value)** 下拉列表中选择已添加的值。
步骤 10 在 **IP 地址 (IP Address)** 和 **网络掩码 (Netmask)** 字段中，输入代表要自动分配该值的 IP 地址块的 IP 地址和网络掩码 (IPv4)。
步骤 11 重复第 6 步至第 10 步，在列表中添加更多值，并自动将其分配给 IP 地址块中的新主机。
步骤 12 点击**保存 (Save)**。

设置主机属性值

可以设置预定义和自定义主机属性的值。不过，无法为系统生成的合规 allow 名单主机属性设置值。

过程

步骤 1 打开要修改的主机配置文件。
步骤 2 在**属性 (Attributes)** 部分中，点击 **编辑属性 (Edit Attributes)**。
步骤 3 根据需要更新属性。
步骤 4 点击**保存 (Save)**。

主机配置文件中的允许 列表违规事件

合规 *allow* 名单（或 *allow* 名单）指允许用户指定可在特定子网上运行的操作系统、应用协议、客户端、网络应用和协议的一系列条件。

如果在活动关联策略中添加 an allow 名单，系统检测到主机违反 allow 名单时， 管理中心 会将 an allow 名单事件（一种特殊类型的关联活动）记入数据库。这些 allow 名单事件中的任何一个事件都对应一种 an *allow* 名单违规，表明特定主机违反 allow 名单的原因和方式。如果主机违反一个或多个 allow 名单，可以两种方式查看其主机配置文件中的这些违规情况。

首先，主机配置文件列出与主机相关的单个 allow 名单违规事项。

主机配置文件中的 allow 名单违规信息的说明如下。

类型

违规类型，即违规是由于操作系统、应用、服务器还是协议不符合规定造成的。

原因

出现违规的具体原因。例如，如果 an allow 名单仅容许 Microsoft Windows 主机，主机配置文件会显示当前运行在主机上的操作系统（比如，`Linux Linux 2.4、2.6`）

允许 名单

与违规关联的 allow 名单的名称。

其次，在与操作系统、应用、协议和服务器有关的部分中， 管理中心 将为不合规元素标记 allow 名单 **违规**。例如，对于仅容许 Microsoft Windows 主机的 an allow 名单，主机配置文件会在该主机操作系统信息旁边显示 allow 名单违规图标。

注释 您可以利用主机的配置文件为合规 allow 名单创建共享主机配置文件。

创建共享 允许 名单主机配置文件

合规 allow 名单共享主机配置文件明确规定操作系统、应用协议、客户端、网络应用和允许在多个 allow 名单的目标主机上运行的协议。即，如果创建了多个 allow 名单，但要使用相同的主机配置文件来评估运行 allow 名单中规定的特定操作系统的主机，可使用共享主机配置文件。

可使用任何 IP 地址已知的主机的主机配置文件创建可供合规 allow 名单使用的共享主机配置文件。但请注意，如果系统尚未识别主机的操作系统，则无法根据单个主机的主机配置文件创建共享主机配置文件。

过程

步骤 1 在主机配置文件中，点击**生成 允许列表 配置文件**。

步骤 2 根据特定需要修改并保存共享主机配置文件。

相关主题

构建 允许 列表主机配置文件

主机配置文件中的恶意软件检测

Most Recent Malware Detections 部分列出主机发送或接收恶意软件文件的最新恶意软件事件，最多 100 个。主机配置文件列出基于网络的恶意软件事件（恶意软件防护 生成的恶意软件事件）和基于终端的恶意软件事件（面向终端的 AMP 生成的恶意软件事件）。

如果主机涉及文件事件，且文件在回溯时被确定为恶意软件，在识别恶意软件开始后，恶意软件检测列表会显示传输文件的原始事件。当确定为恶意软件的文件在回溯时被确定为非恶意软件时，该列表不会再显示与该文件相关的恶意软件事件。例如，如果文件性质为 `Malware`，并且该性质更改为 `Clean`，则从主机配置文件中的恶意软件检测列表中移除针对该文件的事件。

在主机配置文件中查看恶意软件检测情况时，可通过点击 **恶意软件**以查看该主机的恶意软件事件。

对主机配置文件中“最新恶意软件检测”(Most Recent Malware Detections) 部分中各列的描述如下。

时间

事件生成的日期和时间。

对于文件在回溯时被确定为恶意软件的事件，请注意，这是指原始事件的时间而非确定恶意软件的时间。

主机角色 (Host Role)

主机在传输检测到的恶意软件中的角色，为发送方或接收方。请注意，对于面向终端的AMP生成的恶意软件事件（“基于终端的恶意软件事件”），主机扮演的角色始终是接收者。

威胁名称

被测恶意软件名称。

文件名

恶意软件文件的名称。

文件类型

文件类型，例如 `PDF` 或 `MSEXE`。

主机配置文件中的漏洞

主机配置文件 Vulnerabilities 部分显示影响该主机的漏洞。这些漏洞基于系统在主机上检测到的操作系统、服务器和应用。

如果主机操作系统标识或主机上的一种应用协议存在标识冲突，系统会在冲突解决前显示这两种标识的漏洞。

对于从 NetFlow 数据添加到网络映射的主机，没有任何操作系统信息可用，因此，系统无法为涉及这些主机的入侵事件分配“易受攻击”（影响级别 1：红色）影响级别。在此情况下，请使用主机输入功能手动设置主机的操作系统身份。

流量通常不包括有关服务器供应商和版本的信息。默认情况下，系统并不映射此类流量的发送和接收主机的关联漏洞。但可配置系统以映射没有供应商或版本信息的特定应用协议的漏洞。

如果使用主机输入功能添加网络中主机的第三方漏洞信息，系统会额外显示“漏洞”部分。例如，如果导入从 QualysGuard 扫描工具获得的漏洞，系统上的主机配置文件将包含 QualysGuard Vulnerabilities 部分。对于第三方漏洞，主机配置文件中相应的“漏洞”(Vulnerabilities) 部分包含的信息仅限于用户使用主机输入功能导入漏洞数据时提供的信息。

您可把第三方漏洞与操作系统和应用协议关联起来，但不得关联客户端。有关导入第三方漏洞的信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

主机配置文件中“漏洞”(Vulnerabilities) 部分中各列的说明如下。

名称

漏洞名称。

远程

表明漏洞是否可以远程利用。如果该列为空，漏洞定义不包含此信息。

组件

与漏洞有关的操作系统、应用协议或客户端的名称。

端口

端口号，如果漏洞与在特定端口运行的应用协议相关。

相关主题

漏洞数据字段
漏洞停用

下载漏洞补丁

可以下载补丁以减少在网络中主机上发现的漏洞。

过程

步骤 1 访问要下载补丁的主机的主机配置文件。

步骤 2 展开**漏洞 (Vulnerabilities)** 部分。

步骤 3 点击要修补漏洞的名称。

步骤 4 展开**修复 (Fixes)** 部分以显示漏洞的补丁列表。

步骤 5 点击要下载的补丁旁边的 **Download**。

步骤 6 下载补丁并应用到受影响的系统上。

停用单个主机的漏洞

可以使用主机漏洞编辑器逐台主机停用漏洞。当停用主机漏洞时，该主机的影响相关性依然在使用该漏洞，但其影响级别自动降低一个级别。

过程

步骤 1 导航至主机配置文件的**漏洞 (Vulnerabilities)** 部分。

步骤 2 点击**编辑漏洞 (Edit Vulnerabilities)**。

步骤 3 从**有效漏洞 (Valid Vulnerabilities)** 列表中选择漏洞，然后点击向下箭头将其移至**无效漏洞 (Invalid Vulnerabilities)** 列表。

提示
可以点击并拖动以选择多个相邻漏洞；也可以双击任何漏洞以在列表间将其移动。

步骤 4 点击**保存 (Save)**。

下一步做什么

- 或者，通过将主机的漏洞从**无效漏洞 (Invalid Vulnerabilities)** 列表移至**有效漏洞 (Valid Vulnerabilities)** 列表来停用该漏洞。

相关主题

停用单个漏洞，第 24 页
停用多个漏洞

停用单个漏洞

如果停用主机配置文件中的漏洞，则网络中的所有主机都会停用该漏洞。但是，可随时重新激活。

在多域部署中，停用祖先域中的某个漏洞将会使其在所有后代域中都停用。如果在祖先域中激活漏洞，则分叶域可以为其设备激活或停用该漏洞。

过程

步骤 1 访问漏洞详细信息：

- 在受影响的主机配置文件，展开**漏洞 (Vulnerabilities)** 部分，点击要启用或禁用的漏洞的名称。
- 在预定义工作流程中，选择 **分析** > **主机** > **漏洞**，然后点击要启用或禁用的漏洞旁边的 **视图** ( ) 。

步骤 2 从**影响限定条件 (Impact Qualification)** 下拉列表中选择**已禁用 (Disabled)**。

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。

步骤 3 确认要更改网络映射上所有主机的**影响限定条件 (Impact Qualification)** 值。

步骤 4 点击 **Done**。

下一步做什么

- 或者，通过在执行上述步骤时从**影响限定条件 (Impact Qualification)**下拉列表中选择**已启用 (Enabled)** 激活漏洞。

相关主题

停用单个主机的漏洞 ，第 24 页
停用多个漏洞
操作系统身份冲突 ，第 8 页

主机配置文件中的扫描结果

当您使用 Nmap 扫描主机时，或者导入 Nmap 的扫描结果时，这些结果出现在所有被扫描的主机的主机配置文件中。

直接把 Nmap 搜集到的有关主机操作系统和运行在开放式未经过滤的端口的服务器的信息分别添加到主机配置文件的“文件系统”(Operating System) 和“服务器”(Servers) 部分。此外，Nmap 在“扫描结果”(Scan Results) 部分添加该主机的扫描结果列表。请注意，扫描必须找到主机上的开放端口，以便“扫描结果”(Scan Results) 部分出现在配置文件中。

结果代表的是信息源、扫描的端口的数量和类型、运行在端口的服务器的名称和任何 Nmap 检测到的其他信息，比如端口状态或服务器的供应商名称。如果扫描UDP端口，在这些端口上检测到的服务器仅出现在“扫描结果”(Scan Results) 部分。

请注意，可从主机配置文件运行 Nmap 扫描。

扫描主机配置文件中的主机

可对主机配置文件中的主机进行 Nmap 扫描。在扫描完后，更新主机配置文件中的该主机的服务器和操作系统信息。所有其他扫描结果可添加至主机配置文件中的“扫描结果”部分。

注意 在再一次运行Nmap扫描或用更高优先级的主机输入覆盖之前，Nmap提供的服务器和操作系统数据保持不变。如果计划使用 Nmap 来扫描主机，请定期安排扫描。

开始之前

- 添加 Nmap 扫描实例；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的主机身份源 一章。

过程

步骤 1 在主机配置文件中，点击 **Scan Host**。

步骤 2 点击要用来扫描主机的扫描更正旁边的 **Scan**。

系统扫描主机并将结果添加到主机配置文件中。

相关主题

Nmap 扫描自动化

主机配置文件的历史记录

功能	管理中心最低版本	威胁防御最低版本	详情
使用 VRF 时的限制	6.6	任意	如果在您的环境中使用虚拟路由和转发，则单个IP地址可能代表多个主机，因为 VRF 可能包含重叠的网络空间。 支持的平台： 管理中心

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。