发现事件

以下主题介绍如何处理发现事件：

发现事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

发现事件中的发现和身份数据

系统会生成代表受监控网络上检测到的更改的事件表。您可以使用这些表查看网络上的用户活动，并确定如何做出响应。网络发现和身份策略指定要收集的数据类型、要监控的网段以及要使用的特定硬件接口。

您可以使用发现和身份事件表识别与网络上的主机、应用和用户相关联的威胁。系统会提供一系列可用于分析系统生成的事件的预定义工作流程。也可创建仅显示与特定需求匹配的自定义工作流程。

要收集和存储网络发现和身份数据以用于分析，您必须配置网络发现和身份策略。配置身份策略后，您必须将其调用到访问控制策略中，并将其部署到要用于监控流量的设备中。

网络发现策略提供主机、应用和非授权用户数据。身份策略提供授权用户数据。

以下发现事件表位于“分析”>“主机”和“分析”>“用户”菜单下。

发现事件表	已填充发现数据？	已填充身份数据？
主机数	是	否
主机危害表现	是	否
应用	是	否
应用详情	是	否
服务器	是	否
主机属性	是	否
发现事件	支持	支持
用户危害表现	支持	支持
活动会话	支持	支持
用户活动	支持	支持
用户	支持	支持
漏洞	是	否
第三方漏洞	是	否

查看发现事件统计信息

“发现统计信息”(Discovery Statistics) 页面显示系统检测到的主机、事件、协议、应用协议和操作系统的摘要。

此页面列出了最近一小时的统计数据和全部的累积统计数据。可选择查看特定设备或所有设备的统计信息。也可通过点击摘要内列出的事件、服务器、操作系统或操作系统供应商查看与此页面上条目匹配的事件。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**概述** > **摘要** > **发现统计信息**。

步骤 2 从**选择设备 (Select Device)** 列表中选择要查看其统计信息的设备。或者，选择**全部**查看由 管理中心 管理的所有设备的统计信息。

步骤 3 您有以下选择：

- 在“统计信息摘要”中，查看一般统计信息，如统计信息摘要部分，第 3 页中所述。
- 在“事件明细”(Event Breakdown) 中，点击要查看的事件类型。如果未显示事件，可能需要调整时间范围，如更改时间窗口中所述。
- 在“协议明细”(Protocol Breakdown) 中，查看检测到的主机当前所使用的协议。
- 在“应用协议明细”(Application Protocol Breakdown) 中，点击要查看的应用协议的名称。
- 在“操作系统明细”(OS Breakdown) 中，点击**操作系统名称 (OS Name)** 或**操作系统供应商 (OS Vendor)**。

相关主题

事件明细部分，第 4 页
协议明细部分，第 5 页
应用协议明细部分，第 5 页
操作系统明细部分，第 5 页

统计信息摘要部分

以下对统计摘要部分的各行进行了说明。

事件总数

管理中心上存储的发现事件的总数。

上一小时事件总数

最近一小时生成的发现事件的总数。

上一日事件总数

最近一日生成的发现事件的总数。

应用协议总数

检测到的主机上运行的服务器所使用的应用协议总数。

IP 主机总数

通过唯一 IP 地址识别的检测到的主机总数。

MAC 主机总数

不是通过 IP 地址识别的检测到的主机总数。

注意无论用户是否查看所有设备或特定设备的发现统计数据，Total MAC Hosts 统计数据都保持不变。这是因为受管设备是根据其 IP 地址发现主机的。此统计数据提供通过其他方式识别的独立于给定受管设备的所有主机的总数。

路由器总数

检测到的识别为路由的节点总数。

网桥总数

检测到的识别为网桥的节点总数。

主机限制使用情况

当前所使用主机上限的总百分比。主机限制根据 管理中心的型号来定义。注意只有在查看所有受管设备的统计数据时才会显示主机上限的使用情况。

注释 如果达到主机上限且已删除一台主机，则此主机不会再出现在您清除了发现数据的网络映射上。

最后一次接收的事件

最新发现事件发生的日期和时间。

最后一次接收的连接

最新连接完成的日期和时间。

事件明细部分

“事件明细”(Event Breakdown) 部分列出了最近一小时内发生的各种发现事件和主机输入事件的计数，以及数据库中存储的每种事件类型的总数的计数。

也可通过事件明细部分查看发现和主机输入事件的详细信息。

相关主题

发现和主机输入事件，第 8 页

协议明细部分

“协议明细”(Protocol Breakdown) 部分列出了检测到的主机当前所使用的协议。其中显示检测到的每个协议的名称、其在协议栈中的“协议层”和使用此协议进行通信的主机总数。

应用协议明细部分

应用协议明细部分列了检测到的主机当前所使用的应用协议。列出了协议名称、最近一个小时内运行应用协议的主机的总数和检测到的随时运行协议的主机的总数。

也可通过应用协议明细部分查看使用所检测到协议的服务器的详细信息。

相关主题

服务器数据，第 28 页

操作系统明细部分

OS 明细列部分出了当前在受监控网络中运行的操作系统，及其供应商和运行每个操作系统的主机的总数。

操作系统名称或版本的 `unknown` 值是指操作系统或其版本与系统的任何指纹都不匹配。`pending` 值表明系统尚未采集到足够的信息用于识别操作系统或其版本。

可通过 OS 明细部分查看检测到的操作系统的详细信息。

相关主题

主机数据，第 16 页

查看发现性能图表

可利用发现事件生成显示受管设备性能统计数据的图表。

新数据将进行累计，统计信息图表每五分钟更新一次。因此，如果快速重新加载图表，直到下一次五分钟更新间隔之前数据可能不会更改。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

开始之前

编辑适用的网络发现策略以包括应用、主机和用户。（这可能会影响性能。）请参阅配置网络发现规则和操作和发现的资产。

您必须是管理员或维护用户才能执行此任务。

过程

步骤 1 选择**概述** > **摘要** > **发现性能**。

步骤 2 从**选择设备**列表中，选择 管理中心或要包括的受管设备。

步骤 3 从**选择图表 (Select Graph[s])** 列表中，选择要创建的图表类型，如发现性能图表类型，第 6 页中所述。

步骤 4 从**选择时间范围 (Select Time Range)** 列表中，选择要用于图表的时间范围。

步骤 5 点击 **Graph** 生成所选统计数据的图表。

发现性能图表类型

可用图表类型的说明如下。

每秒处理的事件数

显示表示数据相关器每秒钟所处理事件数量的图表

每秒处理的连接数

显示表示数据相关器每秒钟所处理连接数量的图表

每秒生成的事件数

显示表示系统每秒钟所生成的事件数量的图表

兆位/秒

显示表示发现进程每秒钟所分析流量兆位数的图表

平均字节/数据包

显示表示发现进程分析的每个数据包中所含平均字节数的图表

千个数据包/秒

显示表示发现进程每秒钟所分析的数据包数量的图表（以千个为单位）

使用发现和身份工作流程

管理中心提供一组可用于分析为您的网络生成的发现和身份数据的事件工作流程。工作流程与网络映射是关于网络资产的关键信息来源。

管理中心为发现和身份数据、受检测主机及其主机属性、服务器、应用、应用详细信息、漏洞、用户活动和用户提供预定义工作流程。也可创建自定义工作流程。

过程

步骤 1 要访问预定义工作流程，请执行以下操作：

- 发现和主机输入数据 - 请参阅查看发现和主机输入事件， 第 14 页。
- 主机数据 - 请参阅查看主机数据， 第 16 页。
- 主机属性数据 - 请参阅查看主机属性， 第 22 页。
- 主机或用户危害表现数据 - 请参阅查看和处理感染指标数据， 第 24 页。
- 服务器数据 - 请参阅查看服务器数据， 第 28 页。
- 应用数据 - 请参阅查看应用数据， 第 32 页。
- 应用详细信息数据 - 请参阅查看应用详细信息数据， 第 34 页。
- 活动会话数据 - 请参阅查看活动会话数据， 第 49 页。
- 用户数据 - 请参阅查看用户数据， 第 52 页。
- 用户活动数据 - 请参阅查看用户活动数据， 第 54 页。
- 网络映射 - 请参阅查看网络映射。

步骤 2 要访问自定义工作流程，请选择**分析** > **高级** > **自定义工作流程**。

步骤 3 要根据自定义表访问工作流程，请选择**分析** > **高级** > **自定义表**。

步骤 4 执行以下任何操作，这些操作对于网络发现工作流程中访问的所有页面通用：

- 限制列 - 要限制显示的列，请点击要隐藏的列标题中 **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 Disabled Columns 下的列名称。

- 删除 - 要删除当前受限制视图中的部分或所有项目，请选中要删除的项目旁边的复选框，然后点击**删除 (Delete)**，或者点击**全部删除 (Delete All)**。这些项目保持删除状态，直到系统的发现功能重新启用时才可再次检测到这些项目。

  注意
  在删除**分析** > **用户标题** > **活动会话** 页面上的非 VPN (non-VPN) 会话之前，请确认会话是否已实际关闭。删除活动会话后，应用策略将无法检测设备上的会话，因此即便该策略已配置为执行这些操作，系统也不会监控或阻止会话。

  注释

有关分析 > 用户 > 活动会话页面上 VPN 会话的详细信息，请参阅“查看远程接入 VPN 当前用户”。

注释
不能删除思科（与第三方相对）漏洞；但是，可以将其标记为已审核。

- 向下展开 - 要向下展开到工作流程中的下一个页面，请参阅使用向下钻取页面。
- 导航当前页面 - 要在当前工作流程页面中导航，请参阅工作流程页面导航工具。
- 在工作流程中导航 - 要在当前工作流程中的页面之间进行导航，从而保留当前限制，请点击工作流程页面左上方的相应页面链接。
- 导航到其他工作流程 - 要导航到其他事件视图以检查关联事件，请参阅工作流程间导航。
- 对数据进行排序 - 要在工作流程中对数据进行排序，请点击列标题。再次点击列标题以反转排列顺序。
- 查看主机配置文件 - 要查看 IP 地址的主机配置文件，请点击**主机配置文件 (Host Profile)**，或者对于具有活动危害表现 (IOC) 标记的主机，点击该 IP 地址旁边显示的**受损主机 (Compromised Host)**。
- 查看用户配置文件 - 要查看用户身份信息，请点击显示在 **用户身份 (User Identity)**旁的用户图标，或对于与 IOC 相关联的用户，请点击 **红色用户 (Red User)**。

相关主题

使用工作流程
从 管理中心 数据库清除数据

发现和主机输入事件

系统可生成传达受监控网段变化详情的发现事件。为新发现的网络功能生成新的事件，并为先前识别的网络资产的任何变化生成更改事件。

在初始网络发现阶段，系统为每台主机以及已发现在每台主机上运行的每个 TCP 或 UDP 服务器生成新的事件。或者，可配置系统，以使用导出的 NetFlow 记录生成这些新主机和服务器事件。

此外，系统为每个网络、传送和在每台已发现主机上运行的应用协议生成新的事件。您可以在配置用于监控 NetFlow 导出器的发现规则中禁用应用协议的删除，但不可以在配置用于监控系统管理的设备的发现规则中禁用应用协议的删除。如果在非 NetFlow 发现规则中启用主机或用户发现，系统则自动发现应用。

初次网络映射完成后，系统通过生成更改事件持续记录网络变化。无论先前发现的资产配置何时发生改变，系统都会生成更改事件。

生成发现事件时，系统会将它们记录到数据库。您可使用 管理中心 Web 界面查看、搜索和删除发现事件，也可以在关联规则中使用发现事件。根据生成的发现事件类型以及其他指定条件，可构建这

样的关联规则：用于关联策略时，可在网络流量符合条件时启动修复和系统日志记录、SNMP 和邮件警报响应。

可使用主机输入功能向网络映射中添加数据。可添加、修改或删除操作系统信息，这些操作会导致系统停止更新此主机的相关信息。也可手动添加，修改或删除应用协议、客户端、服务器和主机属性或修改漏洞信息。执行此操作时，系统生成主机输入事件。

发现事件类型

可以配置系统在网络发现策略中记录的发现事件的类型。查看发现事件表时，**事件 (Event)** 列中列出事件类型。以下是发现事件类型的说明。

Additional MAC Detected for Host

系统检测到先前所发现主机的新 MAC 地址时，生成此事件。

系统检测到主机经流量通过路由器时，经常生成此事件。虽然每台主机都有不同的 IP 地址，但它们似乎都有与路由器关联的 MAC 地址。系统检测到与 IP 地址关联的实际 MAC 地址时，主机配置文件中 MAC 地址显示为粗体文本且在事件视图的事件说明中 MAC 地址显示为“检测到 ARP/DHCP”消息。

Client Timeout

系统从数据库中删除一个不活跃的客户端时，生成此事件。

Client Update

系统在 HTTP 流量中检测到负载（即特定类型的内容，例如音频、视频或网页邮件）时，生成此事件。

DHCP: IP Address Changed

系统检测到主机 IP 地址因 DHCP 地址分配改变时，生成此事件。

DHCP: IP Address Reassigned

主机重新使用 IP 地址时，生成此事件；即主机因 DHCP IP 地址分配获得另一物理主机以前使用的 IP 地址时。

跳数更改 (Hops Change)

系统检测到主机与检测此主机的设备之间的网络跳数发生变化时，生成此事件。如果出现以下情况，则会发生跳数更改：

- 设备通过不同路由器看到主机流量，并能更好地确定主机的位置。
- 如果设备检测到来自该主机的 ARP 传输，这表明主机在本地网段。

Host Deleted: Host Limit Reached

在超过 管理中心上的主机限制并从网络映射删除一台受监控主机时，会发生此事件。

主机已丢弃：已达到主机限制 (Host Dropped: Host Limit Reached)

在达到 管理中心上的主机限制并丢弃一台新主机时，会发生此事件。对比此事件与达到主机上限时旧主机从网络映射中被删除的先前事件。

要在达到主机限制时丢弃新主机，请转至**策略**>**网络发现**>**高级**并将**达到主机限制时**设为**丢弃主机**。

主机 IOC 设置 (Host IOC Set)

为主机设置 IOC（危害表现）时生成此事件并生成警报。

Host Timeout

主机由于未在网络发现策略规定的区间内发生流量，因而从网络映射中丢失时生成此事件。注意个别主机IP地址和MAC地址会单独超时；主机不会从网络映射中消失除非其所有关联地址均已超时。

如果更改了网络发现策略需监控的网络，可能需要从网络映射中手动删除旧主机，以免主机限制受到影响。

Host Type Changed to Network Device

系统检测到的主机实际上是网络设备时生成此事件。

Identity Conflict

系统检测到新服务器或操作系统标识与服务器或操作系统的当前活跃标识相冲突时生成此事件。

如果要通过重新扫描主机获取更新的有效标识数据来解析标识冲突，可使用标识冲突事件触发Nmap修复。

Identity Timeout

来自主动源的服务器或操作系统身份数据超时时，生成此事件。

如果要通过重新扫描主机获取更新的有效标识数据来刷新标识冲突，可使用标识冲突事件触发Nmap修复。

MAC Information Change

系统检测到与特定 MAC 地址或 TTL 值关联的信息发生变化时，生成此事件。

系统检测到主机经流量通过路由器时，经常发生此事件。虽然每台主机都有不同的IP地址，但它们似将都有与路由器关联的 MAC 地址。系统检测到与 IP 地址关联的实际 MAC 地址时，主机配置文件中MAC地址显示为粗体文本且在事件视图的事件说明中MAC地址显示为“检测到ARP/DHCP”消息。TTL 可能会因为流量可能通过不同的路由器或者系统检测到主机的实际 MAC 地址而发生改变。

NETBIOS Name Change

系统检测到主机的NetBIOS名称改变时，生成此事件。只有有主机使用NetBIOS协议时才会生成此事件。

New Client

系统检测到新的客户端时，生成此事件。

注释 要采集和存储客户数据用于分析，请确保网络发现策略的发现规则中启用应用检测。

New Host

系统检测到新主机在网络中运行时，生成此事件。

设备处理涉及新主机的NetFlow数据时，也可生成此事件。要在此情况下生成事件，请将管理NetFlow数据的网络发现规则配置为发现主机。

New Network Protocol

系统检测到主机使用新的网络协议（IP、ARP 等）通信时，生成此事件。

New OS

系统检测到主机适用新的操作系统或者主机操作系统发生变化时，生成此事件。

New TCP Port

系统检测到主机上有活跃的新 TCP 服务器端口（例如，SMTP 或网络服务使用的端口）时，生成此事件。此事件不用于识别应用协议或与其关联的服务器；此信息在 TCP 服务器信息更新事件中传输。

设备在处理涉及网络映射中已不存在的受监控网络中服务器的 NetFlow 数据时，也会生成此事件。要在此情况下生成事件，请将管理 NetFlow 数据的网络发现规则配置为发现应用。

New Transport Protocol

系统检测到主机使用新的传输协议（例如 TCP 或 UDP）通信时生成此事件。

New UDP Port

系统检测到主机上有新的 UDP 服务器端口时，生成此事件。

设备在处理涉及网络映射中已不存在的受监控网络中服务器的 NetFlow 数据时，也会生成此事件。要在此情况下生成事件，请将管理 NetFlow 数据的网络发现规则配置为发现应用。

TCP Port Closed

系统检测到在主机上的 TCP 端口关闭时生成此事件。

TCP Port Timeout

系统在系统网络发现策略规定的区域内未检测到来自 TCP 端口的活动时，生成此事件。

TCP Server Information Update

系统检测到主机上运行的已发现 TCP 服务器发生变化时，生成此事件。

如果 TCP 服务器已升级，则生成此事件。

UDP Port Closed

系统检测到主机上 UDP 端口关闭时，生成此事件。

UDP Port Timeout

系统在网络发现策略规定的区域内未检测到来自 UDP 端口的活动时，生成此事件。

UDP Server Information Update

系统检测到主机上运行的已发现 UDP 服务器发生变化时，生成此事件。

如果 UDP 服务器已升级，则生成此事件。

VLAN Tag Information Update

系统检测到主机的 VLAN 标签发生改变时，生成此事件。

相关主题

主机输入事件类型，第 12 页

主机输入事件类型

查看发现事件表时，**Event** 列中列出事件类型。

对比用户执行特定操作（例如手动添加主机）时生成的主机输入事件与系统自身检测到受监控网络发生变化（例如来自之前未检测到主机的流量）时生成的发现事件。

可通过修改网络发现策略配置主机输入事件的类型。

如果了解了不同类型主机输入事件所提供的信息，可以更有效地确定需记录和警报的事件以及如何在关联策略中使用这些警报。此外，了解事件类型的名称有助于更有效地进行事件搜索。不同类型的主机输入事件的说明如下。

添加客户端

用户添加客户端时，生成此事件。

添加主机

用户添加主机时，生成此事件。

添加协议

用户添加协议时，生成此事件。

添加扫描结果

系统成功将 Nmap 扫描的结果添加到主机时，生成此事件。

添加端口

用户添加服务器端口时，生成此事件。

删除客户端

用户从系统中删除客户端时，生成此事件。

删除主机/网络

用户从系统中删除 IP 地址或子网时，生成此事件。

删除协议

用户从系统中删除协议时，生成此事件。

删除端口

用户从系统中删除服务器端口或服务器端口组时，生成此事件。

主机属性添加 (Host Attribute Add)

用户创建新的主机属性时，生成此事件。

主机属性删除 (Host Attribute Delete)

用户删除自定义主机属性时，生成此事件。

主机属性删除值

用户删除主机属性赋值值时，生成此事件。

主机属性设置值

用户设置为主机设置主机属性值时，生成此事件。

主机属性更新 (Host Attribute Update)

用户改变自定义主机属性的定义时，生成此事件。

设置主机重要性

用户设置或修改主机的主机重要性时，生成此事件。

设置操作系统定义

用户设置主机的操作系统时，生成此事件。

设置服务器定义

用户设置服务器的供应商和版本定义时，生成此事件。

设置漏洞影响限定条件 (Set Vulnerability Impact Qualification)

设置漏洞影响限定条件时，生成此事件。

在全局层面上禁止漏洞用于影响限制，或者在全局层面上禁用漏洞时，生成此事件。

设置的漏洞无效

用户作废（或审查）一个漏洞或多个漏洞时，生成此事件。

设置的漏洞有效

用户作废之前标记为无效的漏洞时，生成此事件。

相关主题

发现事件类型，第 9 页

查看发现和主机输入事件

通过发现事件工作流程，从发现事件和主机输入事件均可查看数据。可以根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问事件时看到的页面因所用的工作流程而有所不同。可使用预定义工作流程，包括发现事件的表视图和终止主机视图页面。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 选择**分析** > **主机标题** > **发现事件**。

步骤 2 您有以下选择：

- 调整时间范围，如更改时间窗口中所述。

  注释
  如果按时间限制事件视图，则该事件视图中可能会显示在设备的所配置时间窗口（无论是全局还是特定于事件）外部生成的事件。即使为设备配置了滑动时间窗，也可能发生这种情况。

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 6 页。
- 了解有关表中各列内容的详细信息；请参阅发现事件字段，第 15 页。

相关主题

使用发现和身份工作流程，第 6 页

发现事件字段

可在以下发现事件表中查看和搜索的字段的说明。

时间

系统生成事件的时间。

事件

发现事件的类型或主机输入事件的类型。

IP 地址

与事件所涉及主机相关的 IP 地址。

用户

事件生成前登录到事件所涉及的主机的最后一名用户。如果授权用户登录后只有未授权用户登录，除非其他授权用户登录，否则此授权用户仍是主机的当前用户。

MAC 地址

触发发现事件的网络流量所使用NIC的MAC地址。MAC地址可以是事件所涉及的主机的实际MAC地址或者是有流量通过的网络设备的 MAC 地址。

MAC 供应商

触发发现事件的网络流量所使用 NIC 的 MAC 硬件供应商。

端口

如适用，是指触发此事件的流量所使用的端口。

说明

事件的文字说明。

域

发现主机的设备的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

设备

生成事件的受管设备的名称。对于基于 NetFlow 数据的新主机和新服务器事件，此设备是处理数据的受管设备。

相关主题

事件搜索

主机数据

系统检测到主机并采集其有关信息用于生成主机配置文件时，生成此事件。可使用管理中心 Web 界面查看，搜索和删除主机。

查看主机时，可根据所选主机创建流量量变曲线和合规 allow 名单。也可赋予主机属性，包括对于主机组的主机重要性值（它可指定业务重要性）。然后可使用这些关键性值、 allow 名单和关联规则和策略中的流量量变曲线。

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。

查看主机数据

可使用 管理中心查看列出了系统检测到的主机的表。然后，可根据要查找的信息操纵视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问主机时所看到的页面因所使用工作流程的不同而不同。两个预定义工作流程结束于主机视图中，该视图包含符合限制条件的每台主机的主机配置文件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问主机数据：

- 如果使用的是预定义工作流程，请选择**分析** > **主机标题** > **主机**。
- 如果使用的是不包含主机表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**主机 (Hosts)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程 ， 第 6 页。
- 了解有关表中各列内容的详细信息；请参阅主机数据字段 ， 第 16 页。
- 右键点击表中的项目以查看选项。（并非每个列都提供选项。）
- 为特定主机分配主机属性；请参阅为所选主机设置主机属性 ， 第 23 页。
- 为特定主机创建流量量变曲线，请参阅为所选主机创建流量量变曲线 ， 第 20 页。
- 根据特定主机创建合规 allow 名单，请参阅 根据所选主机创建合规 允许 名单 ， 第 21 页。

主机数据字段

系统发现主机时，会采集有关此主机的数据。该数据可能包括主机的 IP 地址、其运行的操作系统等等。可在主机表视图中查看部分该信息。

可以在下面的主机表中查看和搜索的字段说明。

上次查看时间

系统最后检测到的任何主机 IP 地址的日期和时间。至少应按网络发现策略中配置的更新间隔更新“上次查看时间”(Last Seen) 值，另外当系统为任何主机 IP 地址生成新的主机事件时，也要执行该更新。

对于使用主机输入功能更新操作系统数据的主机，“上次查看时间”(Last Seen) 值表示最初添加数据的日期和时间。

IP 地址

与主机关联的 IP 地址。

MAC 地址

检测到的主机 NIC 的 MAC 地址。

“MAC 地址”(MAC Address) 字段显示在主机表视图中，该视图可在主机工作流程中找到。也可将“MAC 地址”(MAC Address) 字段添加到：

- 包括来自主机表的字段的自定义表
- 基于主机表的自定义工作流程中的向下展开页面

MAC 供应商 (MAC Vendor)

检测到的主机 NIC 的 MAC 硬件供应商。

“MAC 供应商”(MAC Vendor) 字段显示在主机表视图中，该视图可在主机工作流程中找到。也可将“MAC 供应商”(MAC Vendor) 字段添加到：

- 包括来自主机表的字段的自定义表
- 基于主机表的自定义工作流程中的向下展开页面

搜索此字段时，请输入 `virtual_mac_vendor` 以匹配涉及虚拟主机的事件。

当前用户 (Current User)

主机当前登录用户的用户身份（用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则该主机的当前用户可能是非授权用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，主机的当前用户是非授权用户时，仍不能使用该用户进行用户控制。

主机重要性

分配给主机的用户指定的重要性值。

NetBIOS 名称 (NetBIOS Name)

主机的 NetBIOS 名称。只有运行 NetBIOS 协议的主机才有 NetBIOS 名称。

VLAN ID

主机使用的 VLAN ID。

跳数

逐一检测主机的设备的网络跳数。

主机类型 (Host Type)

主机的类型。可以为以下任意一种：主机、移动设备、破解移动设备、路由器、网桥、NAT 设备和负载均衡器。

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

如果设备未被识别为网络设备，则归类为主机。

搜索此字段中，请输入 `!host` 以搜索所有网络设备。

硬件

移动设备的硬件平台。

操作系统

以下项之一：

- 在主机上检测到的或使用 Nmap 或主机输入功能更新的操作系统（名称、供应商和版本）。
- 如果操作系统不匹配任何已知指纹，则为 `unknown`
- 如果系统尚未采集到足够的信息用于识别操作系统，则为 `pending`

如果系统检测到多个身份，这些身份将显示在逗号分隔列表中。

从控制面板上的“自定义分析”(Custom Analysis) 构件中调用主机事件视图时，此字段显示。它也是基于主机表的自定义表中的一个字段选项。

搜索此字段时，请输入 `n/a` 以包含操作系统尚未识别的主机。

操作系统冲突

此字段仅供搜索。

操作系统供应商

以下项之一：

- 主机上检测到的或使用 Nmap 或主机输入功能升级的操作系统的供应商。
- 如果操作系统不匹配任何已知指纹，则为 `unknown`
- 如果系统尚未采集到足够的信息用于识别操作系统，则为 `pending`

如果系统检测到多个供应商，这些供应商将显示在逗号分隔列表中。

搜索此字段时，请输入 `n/a` 以包含操作系统尚未识别的主机。

操作系统名称

以下项之一：

- 在主机上检测到的或使用 Nmap 或主机输入功能更新的操作系统。
- 如果操作系统不匹配任何已知指纹，则为 `unknown`
- 如果系统尚未采集到足够的信息用于识别操作系统，则为 `pending`

如果系统检测到多个名称，这些名称将显示在逗号分隔列表中。

搜索此字段时，请输入 `n/a` 以包含操作系统尚未识别的主机。

操作系统版本

以下项之一：

- 在主机上检测到的或使用 Nmap 或主机输入功能升级的操作系统的版本
- 如果操作系统不匹配任何已知指纹，则为 `unknown`
- 如果系统尚未采集到足够的信息用于识别操作系统，则为 `pending`

如果系统检测到多个版本，这些版本将显示在逗号分隔列表中。

搜索此字段时，请输入 `n/a` 以包含操作系统尚未识别的主机。

源类型

用于建立主机操作系统身份的源类型：

- 用户：user_name
- 应用：app_name
- 扫描工具：scanner_type（通过网络发现配置添加的 Nmap 或扫描工具）

- 对于系统检测到的操作系统，则为 `Firepower`

系统可能会从多个源协调数据，以确定操作系统的身份。

置信

以下项之一：

- 对于系统检测到的主机，指系统对在主机上运行的操作系统的身份的置信百分比
- 对于通过活跃源识别的操作系统，则为 100%，例如主机输入功能或 Nmap 扫描工具
- 对于系统不能确定操作系统身份的主机和根据 NetFlow 数据已添加到网络映射的主机，则为 `unknown`。

搜索此字段时，请输入 `n/a` 以包含根据 NetFlow 数据添加到网络映射的主机。

说明

注释主机属性的用户定义内容。

域

与主机关联的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

设备

检测到流量的受管设备或者处理 NetFlow 或主机输入数据的设备。

如果此字段为空，则以下任一条件成立：

- 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。
- 已使用主机输入功能成功添加该主机，但系统尚未检测到。

计数

与每行中所显示的信息匹配的事件数。仅在应用创建两个或多个相同行的限制后，才会显示此字段。

相关主题

事件搜索
操作系统身份冲突

为所选主机创建流量量变曲线

流量配置文件是以指定的时间跨度内收集的连接数据为基础的网络流量的配置文件。在创建流量配置文件后，可以通过对照配置文件评估新流量来检测异常网络流量，系统将假定该配置文件代表的是正常网络流量。

可使用“主机”页面为您指定的一组主机创建流量配置文件。该流量配置文件将以检测到的连接为基础，其中所指定主机之一是启动连接的主机。使用排序和搜索功能可隔离要为其创建配置文件的主机。

开始之前

您必须是管理员用户才能执行此任务。

过程

步骤 1 在主机工作流程中的表视图上，选中要为其创建白名单的主机旁边的复选框。

步骤 2 在页面底部，点击 **Create Traffic Profile**。

步骤 3 根据特定需要修改并保存流量量变曲线。

相关主题

流量量变曲线简介

根据所选主机创建合规 允许 名单

使用合规 allow 名单可以指定网络允许的操作系统、客户端和网络、传送或应用协议。

可在主机页面上根据指定的主机组的主机配置文件创建合规 allow 名单。使用排序和搜索功能隔离要用于创建 allow 列表的主机。

开始之前

您必须是管理员用户才能执行此任务。

过程

步骤 1 在主机工作流程中的表视图上，选中要为其创建 allow 列表的主机旁边的复选框。

步骤 2 在页面底部，点击**创建 (Create)允许列表**。

步骤 3 根据特定需要修改并保存 allow 名单。

相关主题

合规 允许 名单简介

主机属性数据

Firepower 系统采集有关其检测到的主机的信息，并使用该信息生成主机配置文件。但是，可能会有要提供给分析师的有关网络上主机的附加信息。可在主机配置文件中添加注释，设置主机的业务关键性或提供您所选择的任何其他信息。每个信息都称为主机属性。

可在主机配置文件限制中使用主机属性，用于生成流量量变曲线时限制所采集的数据，也可限制用于触发相关规则的条件。也可设置与相关规则对应的属性值。

相关主题

查看主机属性，第 22 页
配置设置属性补救

查看主机属性

可使用 管理中心查看系统检测到的主机表，及其主机属性。然后，可根据要查找的信息操纵视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问主机属性时所看到的页面因所使用工作流程而异。可使用预定义工作流程，此流程包括列出了所有检测到的主机及其属性的主机属性表视图，并在主机视图页面结束，此页面包含符合限制条件的每台主机的主机配置文件。

还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问主机属性数据：

- 如果使用的是预定义工作流程，请选择**分析** > **主机标题** > **主机属性**。
- 如果使用的是不包含主机属性表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**属性 (Attributes)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 6 页。
- 了解有关表中各列内容的详细信息；请参阅主机属性数据字段，第 22 页。
- 为特定主机分配主机属性；请参阅为所选主机设置主机属性，第 23 页。

主机属性数据字段

注意主机属性表不显示仅通过 MAC 地址识别的主机。

以下对主机属性表中可以查看和搜索的字段进行了说明。

IP 地址

与主机关联的 IP 地址。

当前用户 (Current User)

主机当前登录用户的用户身份（用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则该主机的当前用户可能是非授权用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，主机的当前用户是非授权用户时，仍不能使用该用户进行用户控制。

主机重要性

用户赋予主机对于您所在企业的重要性。可在关联规则和策略中使用主机重要性，用于定制策略违规和对事件中所涉及主机重要性的响应。可分配低级、中级、高级或零级主机重要性。

说明

有关希望其他分析师查看的主机的信息。

所有用户定义的主机属性，包括符合 allow 名单规定的属性

用户定义的主机属性的值。主机属性表包括每个用户定义的主机属性的字段。

域

与主机关联的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

计数

与每行中所显示的信息匹配的事件数。请注意，“计数”(Count) 字段仅在应用了创建两个或多个相同行的约束后才显示。

相关主题

事件搜索

为所选主机设置主机属性

可以从主机工作流程配置预定义和用户定义的主机属性。

过程

步骤 1 在主机工作流程中，选中要向其添加主机属性的主机旁边的复选框。

提示
使用排序和搜索功能隔离要为其分配特定属性的主机。

步骤 2 在页面底部，点击**设置属性 (Set Attributes)**。

步骤 3 或者，为所选主机设置主机重要性。可以选择**无 (None)**、**低 (Low)**、**中 (Medium)** 或**高 (High)**。

步骤 4 或者，在文本框中选择的主机的主机配置文件中添加注释。

步骤 5 或者，设置已配置的任何用户定义的主机属性。

步骤 6 点击**保存 (Save)**。

危害表现数据

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。 这些主机的 IP 地址在事件视图中以 **红色的受危害主机图标**显示。

如果系统识别出主机可能受到危害，则与该危害关联的用户也会被标记出来。这些用户在事件视图中以**红色用户图标**显示。

如果某个文件在标记为 IOC 的 300 秒内再次被检测到包含恶意软件，则不会生成另一个 IOC。如果在 300 秒之后再次检测到同一文件，则系统会生成新的 IOC。

要配置系统将事件标记为危害表现，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 。

相关主题

编辑服务器身份

查看和处理感染指标数据

可以使用 管理中心查看显示感染指标 (IOC) 的表。可以根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

所看到的页面因所使用的工作流程而异。预定义 IOC 工作流程会在配置文件视图中终止，此视图包含符合限制条件的每台主机或每个用户的主机或用户配置文件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

开始之前

- 为使系统能够检测和标记危害表现 (IOC)，必须激活网络发现策略中的 IOC 功能并至少启用一个 IOC 规则。请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 启用危害表现规则 。
- 必须在有效身份策略中识别用户身份。

过程

步骤 1 确定 Web 界面中的哪个位置具有满足您需求的信息。

您可以在以下位置查看或处理感染指标数据：

- 事件查看器（“分析”(Analysis) 菜单下）- 连接、安全情报、入侵、恶意软件和 IOC 发现事件的视图指示事件是否触发了 IOC。请注意，触发 IOC 规则的 Cisco Secure Endpoint 生成的恶意软件事件的事件类型为 `AMP IOC`，并同时显示指明危害的事件子类型。

- 控制面板 - 在控制面板中，“威胁摘要控制面板”(Threats of the Summary Dashboard) 会默认按主机和用户来显示 IOC 标记。Custom Analysis 构件根据 IOC 数据提供预设。
- 情景管理器 - 情景管理器的“危害表现”(Indications of Compromise) 部分按 IOC 类别显示主机图，按主机显示 IOC 类别。
- “网络映射”(Network Map) 页面 -“分析”(Analysis) >“主机”(Hosts) >“网络映射”(Network Map) 下的“危害表现”(Indications of Compromise) 会按危害类型和 IP 地址对您网络上可能受到危害的主机进行分组。
- “网络文件轨迹详细信息”(Network File Trajectory Detailss) 页面 -“分析”(Analysis) >“文件”(Files) >“网络文件轨迹”(Network File Trajectory) 下列出的文件的详细信息页面允许您跟踪您网络中的危害表现。
- “主机危害表现”(Host Indications of Compromise) 页面 -“分析”(Analysis) >“主机”(Hosts) 菜单下的“主机危害表现”(Indications of Compromise) 页面列出按 IOC 标记分组的受监控主机。使用本页面上的工作流程深入了解您的数据。
- “用户危害表现”(User Indications of Compromise) 页面 -“分析”(Analysis) >“用户”(Users) 菜单下的“用户危害表现”(User Indications of Compromise) 页面列出与潜在 IOC 事件相关联并按 IOC 标记分组的用户。使用本页面上的工作流程深入了解您的数据。
- “主机配置文件”(Host Profile) 页面 - 可能受到危害的主机的主机配置文件会显示与该主机相关联的所有 IOC 标记，并允许您解决 IOC 标记及配置 IOC 规则状态。
- “用户配置文件”(User Profile) 页面 - 与潜在 IOC 事件相关联的用户的用户配置文件会显示与该用户相关联的所有 IOC 标记，并允许您解决 IOC 标记及配置 IOC 规则状态。（用户配置文件在 管理中心 Web 界面中被标记为“用户身份”。）

步骤 2 如果适用，请执行以下选项之一并执行此过程中的其余步骤：

选项	描述
要研究与主机相关的 IOC，请执行以下操作：	• 如果使用的是预定义工作流程，请选择**分析 > 主机标题 > 感染指标**。 • 如果使用的是不包含主机 IOC 表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**主机危害表现 (Host Indications of Compromise)**。
要研究与用户关联的 IOC，请执行以下操作：	• 如果使用的是预定义工作流程，请选择**分析 (Analysis) > 用户 (Users) > 危害表现 (Indications of Compromise)**。 • 如果使用的是不包含用户 IOC 表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**用户危害表现 (User Indications of Compromise)**。

步骤 3 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。

- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 6 页。
- 了解有关表中各列内容的详细信息；请参阅危害表现数据字段，第 26 页。
- 在“主机危害表现”(Host Indications of Compromise) 页面上：点击 **IP 地址 (IP Address)** 列中的**受损主机 (Compromised Host)**，查看受损主机的主机配置文件。
- 在“用户危害表现”(User Indications of Compromise) 页面上：通过点击**用户 (User)** 列中的**红色用户 (Red User)** 来查看与危害关联的用户配置文件。
- 将 IOC 事件标记为“已解决”，这样它们就不会再显示在此列表中。为此，请选中要修改的 IOC 事件旁边的复选框，然后点击**标记为已解决 (Mark Resolved)**。
- 通过点击**首次查看时间 (First Seen)** 或**上次查看时间 (Last Seen)** 列中的 **视图** (👁) 来查看触发 IOC 的事件的详细信息。
- 查看更多选项：右键点击表中的值。

危害表现数据字段

以下是主机或用户 IOC（危害表现）表中的字段。并非每个与 IOC 相关的表都包含所有字段。

IP 地址（查看主机 IOC 数据时）

与触发 IOC 的主机关联的 IP 地址。

用户（查看用户 IOC 数据时）

与触发 IOC 的事件关联的用户的用户名、领域和身份验证源。

类别

所指示危害类型的简要说明，例如 `Malware Executed` 或 `Impact 1 Attack`。

事件类型

与特定 IOC 关联的标识符，指触发该 IOC 的事件。

说明

对可能受到危害的主机的影响的说明，例如此主机可能受到远程控制 (`This host may be under remote control`) 或已针对此主机执行了恶意软件 (`Malware has been executed on this host`)。

首次查看时间/上次查看时间

触发 IOC 的事件首次/最近出现的日期与时间。

域

触发 IOC 的主机的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

相关主题

事件搜索

编辑单台主机或单个用户的危害表现规则状态

如果在网络发现策略中启用，危害表现规则适用于监控网络中的所有主机以及与此网络中的 IOC 事件关联的授权用户。您可以禁用单台主机或单个用户的规则，以避免无用的 IOC 标记（例如，您可能不希望看到 DNS 服务器的 IOC 标记）。如果在适用的网络发现策略中禁用规则，则无法针对特定的主机或用户启用该规则。禁用特定主机的规则不会影响对同一事件中涉及的用户的标记，反之亦然。

过程

步骤 1 导航至主机或用户配置文件的**危害表现 (Indications of Compromise)** 部分。

步骤 2 点击**编辑规则状态 (Edit Rule States)**。

步骤 3 在规则的**已启用**列中，点击滑块启用或禁用规则。

步骤 4 点击**保存 (Save)**。

查看危害表现标记的源事件

您可利用主机配置文件和用户配置文件的“危害表现”(Indications of Compromise) 部分快速导航至触发了 IOC 标记的事件。通过分析这些事件，可获得所需信息，以确定是否需要采取措施处理危害威胁以及采取什么措施。

点击 IOC 标记时间戳旁边的 **视图** (👁) 可导航至相关事件类型的事件表视图，仅显示触发 IOC 标记的事件。

管理中心中仅显示用户 IOC 的第一个实例。后续实例由 DNS 服务器捕获。

过程

步骤 1 在主机或用户 配置文件中，导航至**危害表现 (Indications of Compromise)** 部分。

步骤 2 点击要调查的 IOC 标记的 **首次发现** 或 **最后发现** 列中的 **视图** (👁)。

解决危害表现标记

在分析和处理完危害表现 (IOC) 标记指示的威胁后，或者如果确定 IOC 标记代表误报，可将事件标记为已解决。将事件标记为已解决会将其从主机配置文件 和用户配置文件中删除；如果配置文件上的所有活动 IOC 标记均已解决，则 **受到危害的主机** 或显示用户与受到危害表现 **红色用户图标** 将不再显示。对于已经解决的 IOC，仍然可查看 IOC 触发事件。

如果触发 IOC 标记的事件再次出现，系统会重新设置此标记，除非您已为主机或用户禁用 IOC 规则。

过程

步骤 1 在主机或用户配置文件中，导航至**危害表现 (Indications of Compromise)** 部分。

步骤 2 您有两种选择：

- 要将单个 IOC 标记标记为已解决，请点击要解决的标记右侧的 **删除** ( ) 。
- 要将配置文件上所有的IOC标记标记为已解决，请点击**将所有标记为已解决 (Mark All Resolved)**。

服务器数据

系统收集有关在受监控网段中的主机上运行的所有服务器的信息。此信息包括：

- 服务器的名称
- 服务器使用的应用和网络协议
- 服务器的供应商和版本
- 与运行服务器的主机关联的 IP 地址
- 服务器进行通信的端口

系统检测到服务器时，生成发现事件，除非关联的主机已达到其最大服务器数量。可使用管理中心 Web 界面查看、搜索和删除服务器事件。

关联规则也可基于服务器事件。例如，可在系统检测到其中一台主机上有聊天服务器运行时触发关联规则，例如 ircd。

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。

查看服务器数据

可使用 管理中心查看检测到的服务器表。然后，可根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问服务器时看到的页面因所用的工作流程而有所不同。所有预定义工作流程会产生主机视图，该视图包含符合限制条件的每台主机的配置文件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问数据库数据：

- 如果使用的是预定义工作流程，请选择**分析** > **主机标题** > **服务器**。
- 如果使用的是不包含服务器表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**服务器 (Servers)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 6 页。
- 了解有关表中各列内容的详细信息；请参阅服务器数据字段，第 29 页。
- 通过选中要编辑的服务器事件旁边的复选框，然后点击**设置服务器身份 (Set Server Identity)** 来编辑服务器身份。
- 右键点击表中的项目以查看选项。（并非每个列都提供选项。）

服务器数据字段

可以在下面的服务器表中查看和搜索的字段的说明。

上次使用时间

上次在网络上使用服务器的日期和时间或原先使用主机输入功能更新服务器的日期和时间。至少按网络发现策略中配置的更新间隔更新 Last Used 值，当系统检测到服务器信息更新时也更新该值。

IP 地址

与运行服务器的主机关联的 IP 地址。

端口

服务器运行所在端口。

协议

服务器使用的网络或传输协议。

应用协议

以下项之一：

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

- 如果系统无法根据已知服务器指纹识别服务器或者服务器通过主机输入进行添加但不包含应用协议，则为 unknown。

应用协议的类别、标记、风险或业务关联性 (Category、Tags、Risk or Business Relevance for Application Protocols)

已分配给应用协议的类别、标记、风险级别和业务关联性。这些过滤器可用于集中过滤特定数据集。

供应商

以下项之一：

- 系统、Nmap 或其他活跃源识别的服务器供应商或者使用主机输入功能指定的服务器供应商
- 如果系统无法根据已知服务器指纹识别其供应商或者服务器是使用 NetFlow 数据添加到网络映射的，则为空白。

Version

以下项之一：

- 系统、Nmap 或其他活跃源识别的服务器版本或者使用主机输入功能指定的服务器版本
- 如果系统无法根据已知服务器指纹识别其版本或者服务器是使用 NetFlow 数据添加至网络映射的，则为 blank。

Web 应用程序

基于系统在 HTTP 流量中检测到的负载内容的 Web 应用。注意，如果系统检测到 HTTP 应用协议，但无法检测到特定网络应用，则系统提供通用网络浏览名称。

Web 应用的类别、标记、风险或业务关联性 (Category、Tags、Risk or Business Relevance for Web Applications)

分配给 Web 应用的类别、标记、风险级别和业务关联性。这些过滤器可用于集中过滤特定数据集。

点击数

服务器被访问的次数。对于使用主机输入功能添加的服务器，此值始终为 0。

源类型

选择以下值之一：

- 用户：user_name
- 应用：app_name
- 扫描工具：scanner_type（通过网络发现配置添加的 Nmap 或扫描工具）

- 对于 Firepower 系统检测到的服务器，为 `Firepower`、`Firepower Port Match` 或 `Firepower Pattern Match`
- 对于使用 NetFlow 数据添加的服务器，为 `NetFlow`

域

运行服务器的主机的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

设备

检测到流量的受管设备或者处理 NetFlow 或主机输入数据的设备。

当前用户 (Current User)

主机当前登录用户的用户身份（用户名）。

当非授权用户登录主机中时，该登录会记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则该主机的当前用户可能是非授权用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，主机的当前用户是非授权用户时，仍不能使用该用户进行用户控制。

计数

与每行中所显示的信息匹配的事件数。仅在应用创建两个或多个相同行的限制后，才会显示此字段。

相关主题

事件搜索

应用和应用详细信息数据

当受监控主机连接到另一台主机时，在许多情况下，系统可以确定所使用的应用。Firepower 系统检测许多邮件、即时消息、对等设备、Web 应用以及其他类型应用的使用情况。

对于检测到的每款应用，系统会记录使用该应用的 IP 地址、产品、版本和检测到的使用次数。可使用 Web 界面查看、搜索和删除应用事件。此外，也可以使用主机输入功能更新一台或多台主机上的应用数据。

如果您知道每台主机上所运行的应用，可以根据该信息创建主机配置文件资格条件，用其约束构建流量配置文件时可收集的数据，也可以用其限制希望触发关联规则的条件。此外，也可以将关联规则设为基于应用检测而触发。例如，如果您希望员工使用特定的邮件客户端，可以设置在系统检测到您的任意一台主机上运行不同的邮件客户端时触发关联规则。

您可以通过仔细阅读每个 Firepower 系统更新的版本说明和每个 VDB 更新的公告来获取有关 Firepower 的应用检测器的最新信息。

要采集和存储应用数据用于分析，请确保在网络发现策略中启用应用检测。

查看应用数据

可使用 管理中心查看检测到的应用表。然后，可根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问应用时所看到的页面因所使用的工作流程而异。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问应用数据：

- 如果使用的是预定义工作流程，请选择**分析** > **主机标题** > **应用详细信息**。
- 如果使用的是不包含应用详细信息的表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择 **客户端 (Clients)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 6 页。
- 了解有关表中各列内容的详细信息；请参阅应用数据字段，第 32 页。
- 通过点击客户端、应用协议或 Web 应用旁边的 **应用详细信息视图** ，打开特定应用的“应用详细信息视图”。
- 右键点击事件值，查看系统外部源中的数据。您看到的选项取决于数据类型，包括公共源；其他来源取决于您配置的资源。有关信息，请参阅使用基于 Web 的资源的事件调查
- 可右键点击表中的事件值，然后从思科或第三方情报源中进行选择，来收集有关事件的情报。例如，您可以从思科 Talos 获取有关可疑 IP 地址的详细信息。您看到的选项将取决于数据类型以及系统上配置的集成。有关详细信息，请参阅 使用基于 Web 的资源的事件调查。

应用数据字段

系统检测已知客户端流量、应用协议或网络应用时，会记录有关该应用及运行该应用的主机的信息。

可在以下应用表中查看和搜索的字段说明。

应用

检测到的应用的名称。

IP 地址

与使用应用的主机关联的 IP 地址。

类型

应用类型：

应用协议

代表主机之间的通信。

客户端应用

代表主机上运行的软件。

Web 应用

代表 HTTP 流量的内容或所请求的 URL。

类别

说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。

标签

有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。

风险

应用被用于可能违反组织安全策略之目的的可能性。应用风险的取值范围为“极低”(Very Low) 到“极高”(Very High)。

在应用协议风险、客户端风险和网络应用风险中，如适用，则是触发入侵事件的流量中检测到的三个风险中级别最高的风险。

业务相关性

应用被用于组织的企业运营中（而不是被用于娱乐目的）的可能性。应用的业务关联性的取值范围为“极低”(Very Low) 到“极高”(Very High)。

在应用协议业务相关性、客户端业务相关性和网络应用业务相关性中，如适用，则是触发入侵事件的流量中检测到的三个业务关联性中关联性最低的一个。

当前用户 (Current User)

主机当前登录用户的用户身份（用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则该主机的当前用户可能是非授权用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，主机的当前用户是非授权用户时，仍不能使用该用户进行用户控制。

域

使用应用的主机的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

计数

与每行中所显示的信息匹配的事件数。请注意，“计数”(Count) 字段仅在应用了创建两个或多个相同行的约束后才显示。

相关主题

事件搜索

查看应用详细信息数据

可使用 管理中心查看检测到的应用详细信息表格。然后，可根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问应用详细信息时看到的页面因所用的工作流程而有所不同。预定义的工作流程有两种。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问应用详细信息数据

- 如果使用的是预定义工作流程，请选择**分析** > **主机标题** > **应用详细信息**。
- 如在使用的自定义工作流程不包括应用详情表视图，请点击**(switch workflow)**，然后选择**Clients**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 6 页。
- 了解有关表中各列内容的详细信息；请参阅应用详细信息数据字段，第 34 页。
- 通过点击客户端旁边的**应用详细信息视图 (Application Detail View)**，打开特定应用的“应用详细信息视图”。
- 右键点击事件值，查看系统外部可用源中的数据。您看到的选项取决于数据类型，包括公共源；其他来源取决于您配置的资源。有关信息，请参阅使用基于 Web 的资源的事件调查
- 可右键点击表中的事件值，然后从思科或第三方情报源中进行选择，来收集有关事件的情报。例如，您可以从思科 Talos 获取有关可疑 IP 地址的详细信息。您看到的选项将取决于数据类型以及系统上配置的集成。有关详细信息，请参阅 使用基于 Web 的资源的事件调查。

应用详细信息数据字段

系统检测已知客户端流量、应用协议或网络应用时，会记录有关该应用及运行该应用的主机的信息。

可在以下应用详细信息表中查看和搜索的字段的说明。

上次使用时间 (Last Used)

最后一次使用该应用的时间或使用主机输入功能更新该应用数据的时间。至少按网络发现策略中配置的更新间隔更新“上次使用时间”(Last Used) 的值，当系统检测到应用信息更新时也更新该值。

IP 地址

与使用应用的主机关联的 IP 地址。

客户端

应用的名称。请注意，如果系统检测到应用协议但检测不到特定客户端，则会向应用协议名称中附加 `client` 以提供通用名称。

Version

应用的版本。

客户端、应用协议以及 Web 应用的类别、标记、风险或业务关联性

分配给应用的分类、标记、风险级别和业务相关性。这些过滤器可用于集中过滤特定数据集。

应用协议

应用所使用的应用协议。请注意，如果系统检测到应用协议但检测不到特定客户端，则会向应用协议名称中附加 `client` 以提供通用名称。

Web 应用程序

基于系统在 HTTP 流量中检测到的负载内容或 URL 的 Web 应用。请注意，如果系统检测到 HTTP 应用协议，但无法检测到特定网络应用，系统会在此处提供通用的 网络浏览应用。

点击数

系统检测到在使用的应用的次数。对于使用主机输入功能添加的应用，此值始终为 `0`。

域

使用应用的主机的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

设备

生成发现事件的设备，包括应用详细信息。

当前用户 (Current User)

主机当前登录用户的用户身份（用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则该主机的当前用户可能是非授权用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，主机的当前用户是非授权用户时，仍不能使用该用户进行用户控制。

计数

与每行中所显示的信息匹配的事件数。请注意，“计数”(Count) 字段仅在应用了创建两个或多个相同行的约束后才显示。

相关主题

事件搜索

漏洞数据

系统有自己的漏洞跟踪数据库，该数据库与系统的指纹识别功能相结合，用于识别与网络中主机关联的漏洞。主机上运行的操作系统、服务器和客户端有不同组关联漏洞。

您可以使用 管理中心来：

- 跟踪和审查每个主机的漏洞。
- 在修复主机或者以其他方式将其判断为对漏洞免疫后，停用该主机的漏洞。

除非在 管理中心配置中映射服务器所使用的应用协议，否则不会映射无供应商和无版本服务器的漏洞。无法映射无供应商和无版本客户端的漏洞。

相关主题

映射服务器漏洞

漏洞数据字段

除非另有说明，否则这些字段显示在 **分析 > 主机 > 漏洞**下的所有页面上。

计数

与每行中所显示的信息匹配的事件数。请注意，“计数”(Count) 字段仅在应用了创建两个或多个相同行的约束后才显示。

CVE ID

与 MITRE 常见漏洞和披露 (CVE) 数据库 (https://cve.mitre.org/) 中的漏洞相关联的标识号。

要在国家漏洞数据库 (NVD) 中查看有关此漏洞的详细信息，请右键点击 CVE ID，然后选择 **在 NVD 中查看说明**。

发布日期

发布漏洞的日期。

说明

国家漏洞数据库 (NVD) 中漏洞的简要说明。

有关完整说明，请右键点击 CVE ID，然后选择**在 NVD 中查看说明 (View description in NVD)** 以查看国家漏洞数据库 (NVD) 中的详细信息。

影响

请参阅“漏洞影响”（下文）。

影响质量

此字段仅在“漏洞详细信息”页面上可用。

使用下拉列表启用或禁用漏洞。管理中心忽略其影响相关性中的禁用漏洞。

此处指定的设置确定如何在整个系统范围内处理漏洞，而且该设置不限于从中选择该值的主机配置文件。

远程

指示漏洞是否可以远程利用 (TRUE/FALSE)。

严重性

国家漏洞数据库 (NVD) 中的基本分数和通用漏洞评分系统 (CVSS) 分数。

Snort ID

与 Snort ID (SID) 数据库中的漏洞相关联的标识号。也就是说，如果入侵规则能检测到利用特殊漏洞的网络流量，则此漏洞与入侵规则的 SID 关联。

请注意，一个漏洞可能与多个 SID（或根本不与 SID）关联。如果一个漏洞与多个 SID 关联，则每个 SID 在漏洞表中各占一行。

SVID

系统用于跟踪漏洞的漏洞标识号。

要查看此漏洞的详细信息，请点击 **视图** ( )。

漏洞影响/影响

漏洞的严重性，等级从 0 级至 10 级，10 级最严重。

相关主题

事件搜索

漏洞停用

停用漏洞可防止系统使用该漏洞评估入侵影响关联。您可以在修复网络上的主机或者以其他方式将其判断为免疫后停用漏洞。注意，如果系统发现一台新主机受该漏洞影响，可视为该漏洞对此主机有效（不会自动停用）。

停用**不**受 IP 地址限制的漏洞工作流程中的漏洞会停用网络上所有受检测主机的漏洞。您只能在以下位置停用漏洞工作流程中的漏洞：

- 默认漏洞工作流程的第二页，**网络上的漏洞 (Vulnerabilities on the Network)**，该页面仅显示适用于网络上的主机的漏洞

- 使用搜索根据 IP 地址限制的自定义或预定义漏洞工作流程中的页面。

您可以使用网络映射，使用主机的主机配置文件，或通过根据要停用漏洞的一个或多个主机的 IP 地址限制漏洞工作流程来停用单个主机的漏洞。对有多个关联 IP 地址的主机，此功能仅适用于该主机的单一选定 IP 地址。

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。

相关主题

停用单个主机的漏洞
停用单个漏洞
停用多个漏洞，第 39 页

查看漏洞数据

可使用 管理中心查看漏洞表。然后，可根据要查找的信息操纵事件视图。

访问漏洞时看到的页面因使用的工作流程而异。可使用预定义的工作流程，其中包括漏洞的表视图。数据库中的每个漏洞在表视图中都各占一行，无论任何检测到的主机是否显示这些漏洞。适用于网络中所检测到主机的每个漏洞（未停用）在预定义工作流程的第二页都各占一行。预定义工作流程在漏洞详情视图中终止，该视图包含符合限制条件的每个漏洞的详细说明。

提示 如要查看适用于单台主机或一组主机的漏洞，应通过指定主机 IP 地址或 IP 地址范围的方式执行漏洞搜索。

还可创建自定义工作流程，仅显示匹配特定需求的信息。

漏洞表不受多域部署中的域限制。

过程

步骤 1 访问漏洞表：

- 如果使用的是预定义漏洞工作流程，请选择**分析** > **主机** > **漏洞**。
- 如果使用的是不包含漏洞表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**漏洞 (Vulnerabilities)**。

步骤 2 您有以下选择：

- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 6 页。
- 停用漏洞，以使这些漏洞不再用于当前易受攻击主机的入侵影响关联；请参阅停用多个漏洞，第 39 页。
- 通过点击 SVID 列中的 **视图** () 来查看漏洞的详细信息。或者，限制漏洞 ID 并向下钻取至漏洞详情页面。有关查看其他详细信息的选项，请访问 查看漏洞详细信息，第 39 页。

- 通过右键点击标题并选择**显示全文 (Show Full Text)** 来查看漏洞标题的全文。

查看漏洞详细信息

过程

可以通过下列任意方法查看漏洞详细信息：

- 选择 **分析** > **主机** > **漏洞**，然后点击 SVID 旁边的 **视图** ( ) 。
- 选择 **分析** > **主机** > **第三方漏洞**，然后点击 SVID 旁边的 **视图** ( ) 。
- 选择 **分析** > **主机标题** > **网络映射**，然后点击 **漏洞**。
- 查看受漏洞影响的主机配置文件（**分析** > **主机标题** > **网络映射**，点击**主机 (Hosts)**，然后向下展开并点击您正在调查的主机），并展开配置文件的**漏洞 (Vulnerabilities)** 部分。
- 在 **分析 (Analysis)** > **主机 (Hosts)** > **漏洞 (Vulnerabilities)** 下的任何表中，右键点击 **CVE ID** 列中的值，然后选择**在 NVD 中查看说明 (View description in NVD)** 以在 NVD（国家漏洞数据库）网站上查看该 CVE。

停用多个漏洞

停用**不**受 IP 地址限制的漏洞工作流程中的漏洞会停用网络上所有受检测主机的漏洞。

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。只要在祖先域中激活了漏洞，枝叶域即可激活或停用其设备的该漏洞。

过程

步骤 1 访问漏洞表：

- 如果使用的是预定义漏洞工作流程，请选择**分析** > **主机** > **漏洞**。
- 如果使用的是不包含漏洞表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**漏洞 (Vulnerabilities)**。

步骤 2 点击**网络上的漏洞 (Vulnerabilities on the Network)**。

步骤 3 选中要停用的漏洞旁边的复选框。

步骤 4 点击页面底部的**审核 (Review)**。

相关主题

停用单个主机的漏洞

停用单个漏洞

第三方漏洞数据

Firepower 系统有自己的漏洞跟踪数据库，该数据库与系统的指纹识别功能相结合，用于识别与网络中主机关联的漏洞。

可以使用从第三方应用导入的网络映射数据来扩充系统的漏洞数据。为此，组织必须能够编写脚本或创建命令行导入文件来导入该数据。有关详细信息，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，必须将第三方漏洞信息映射至数据库中的操作系统和应用定义。不能将第三方漏洞信息映射至客户端定义。

查看第三方漏洞数据

使用主机输入功能导入第三方漏洞数据后，可使用管理中心查看第三方漏洞表。然后，可根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问第三方漏洞时所看到的页面因所使用的工作流程而异。预定义的工作流程有两种。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问第三方漏洞数据：

- 如果使用的是预定义工作流程，请选择**分析** > **主机** > **第三方漏洞**。
- 如果使用的是不包含第三方漏洞的表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**按源划分的漏洞 (Vulnerabilities by Source)** 或**按 IP 地址划分的漏洞 (Vulnerabilities by IP Address)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 6 页。
- 了解有关表中各列内容的详细信息；请参阅第三方漏洞数据字段，第 40 页。
- 通过点击 SVID 列中的 **视图** () 来查看第三方漏洞的漏洞详细信息。或者，限制漏洞 ID 并向下钻取至漏洞详情页面。

第三方漏洞数据字段

可以在第三方漏洞表中查看和搜索的字段说明如下。

漏洞来源 (Vulnerability Source)

第三方漏洞的来源，例如，QualysGuard 或 NeXpose。

漏洞 ID (Vulnerability ID)

与其源漏洞关联的 ID 编码。

IP 地址

与受漏洞影响主机关联的 IP 地址。

端口

如果漏洞与特定端口上运行的服务器关联，则为端口号。

Bugtraq ID

与 Bugtraq 数据库中漏洞关联的标别号。

CVE ID

与 MITRE 常见漏洞和披露 (CVE) 数据库 (https://cve.mitre.org/) 中的漏洞相关联的标识号。

SVID

系统用于跟踪漏洞的旧版漏洞标识号

点击 **视图** () 以访问 SVID 的漏洞详情。

Snort ID

与 Snort ID (SID) 数据库中的漏洞相关联的标识号。也就是说，如果入侵规则能检测到利用特殊漏洞的网络流量，则此漏洞与入侵规则的 SID 关联。

请注意，一个漏洞可能与多个 SID（或根本不与 SID）关联。如果一个漏洞与多个 SID 关联，则每个 SID 在漏洞表中各占一行。

标题

漏洞的标题。

说明

漏洞的简要说明。

域

具有漏洞的主机的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

计数

与每行中所显示的信息匹配的事件数。请注意，“计数”(Count) 字段仅在应用了创建两个或多个相同行的约束后才显示。

相关主题

事件搜索

活动会话、用户和用户活动数据

身份源会收集活动会话数据、用户数据和用户活动数据。这些数据显示在与用户相关的各个工作流程中：

- 活动会话 - 此工作流程显示网络上的所有当前用户会话。运行多个同时活动会话的单个用户将在该表中占用多个行。有关此工作流程中显示的用户数据类型的详细信息，请参阅活动会话数据，第 48 页。
- 用户 - 此工作流程显示网络上可见的所有用户。单个用户在该表中占用一行。有关此工作流程中显示的用户数据类型的详细信息，请参阅用户数据，第 49 页。
- 用户活动 - 此工作流程显示网络上可见的所有用户活动。具有多个用户活动实例的单个用户将在该表中占用多个行。有关此工作流程中显示的用户活动类型的详细信息，请参阅用户活动数据，第 52 页。

有关填充这些工作流程的用户身份来源的详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。

用户相关字段

与用户相关的数据显示在活动会话表、用户表和用户活动表中。

注释 Azure AD 领域用户 和被动身份代理发现的用户的活动会话仅显示在 **活动会话** 新 UI 布局中，而不显示在旧版 UI 中。

表 *1:* 活动会话、用户和用户活动字段说明

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
活动会话计数	与用户相关的活动会话数。	不支持	支持	否
身份验证类型	身份验证类型：不进行身份验证、被动身份验证、主动身份验证、访客身份验证、失败身份验证或 VPN 身份验证。 有关每种身份验证类型所支持的身份源的详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。	是	不支持	支持

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
是否可用于策略	值 **Yes** 表示用户是从用户存储区（例如，Active Directory）中检索的。（ 被动身份代理 不会下载临时用户。) 值 **No** 表示虽然 管理中心 收到了该用户的登录报告，但该用户不在用户存储区中。当排除组中的用户登录到用户存储区时，可能会发生这种情况。配置领域时，您可以排除组以阻止下载这些组。 虽然不可用于策略的用户（例如临时用户）会记录在 管理中心中，但是这些用户不会发送到受管设备。	不支持	支持	否
计数	注释 **计数**字段仅在应用了创建两个或多个相同行的限制条件后才会显示。 取决于与特定行中显示的信息匹配的表、会话数、用户或活动事件。	支持	支持	支持
当前 IP	（另请参阅当前 IP/域名和 IP 地址。） 与用户登录到的主机相关联的 IP 地址。 如果用户没有活动会话，此字段在用户表中为空。	是	否	不兼容
部门	由领域获取的用户所在部门。如果没有明确地与您的服务器上用户关联的部门，则该部门列为服务器分配的任何默认组。例如，在 Active Directory 中，此项为 `Users (ad)`。如果符合以下条件，则此字段为空： • 您尚未配置领域。 • 管理中心无法将 管理中心 数据库中的用户与 LDAP 记录关联（例如，对于通过 AIM、Oracle 或 SIP 登录添加到数据库的用户）。	支持	支持	否
说明	有关会话、用户或用户活动的详细信息（如有）。	否	不兼容	支持

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
设备	对于由基于流量的检测或主动身份验证身份源检测到的用户活动，为用户识别了用户的设备的名称。 对于其他用户活动类型，是管理管理中心。 注释 如果已在高可用性部署中配置 VPN，则针对活动 VPN 会话显示的设备名称可以是识别用户会话的主要或辅助设备。	是	不支持	支持
发现应用	用于检测用户的应用或协议。 • 对于基于流量的检测检测到的用户活动，为以下项目之一：ldap、pop3、imap、oracle、sip、http、ftp、mdns 或 aim。 注释 不会根据 SMTP 登录将用户添加到数据库中。 • 对于所有其他用户活动：ldap。	支持	支持	支持
当前 IP 域/域	在活跃会话表中，为在其中检测到了用户活动的多租户域。 在用户表中，为与用户的领域相关联的多租户域。 在用户活动表中，为在其中检测到了用户活动的多租户域。 仅当曾经配置管理中心以实现多租户时，此字段才存在。	支持	支持	支持
邮件	用户的邮件地址。如果符合以下条件，则此字段为空： • 用户已通过 AIM 登录添加到数据库。 • 用户已通过 LDAP 登录添加到数据库且没有与 LDAP 服务器用户关联的邮箱地址。	是	是（作为电子邮件）	否
结束端口	如果用户由 TS 代理报告且用户会话当前处于活动状态，则此字段标识分配给用户的端口范围的结束值。如果用户的 TS 代理会话处于非活动状态，或者如果用户由其他身份源报告，则此字段为空。	支持	不支持	支持
终端位置	使用 ISE 对用户进行身份验证的网络设备的 IP 地址，如 ISE 所识别。如果未配置 ISE，此字段留空。	否	不兼容	支持

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
终端配置文件	用户终端设备类型，如思科 ISE 所识别。如果未配置 ISE，此字段留空。	否	不兼容	支持
事件	用户活动事件类型。	否	不兼容	支持
名字	由领域获取的用户名字。如果符合以下条件，则此字段为空： • 您尚未配置领域。 • 管理中心无法将 管理中心 数据库中的用户与 LDAP 记录关联（例如，对于通过 AIM、Oracle 或 SIP 登录添加到数据库的用户）。 • 没有与 LDAP 服务器上的用户关联的名字。	支持	支持	否
IP 地址	对于**用户登录**用户活动，为登录中涉及的 IP 地址或内部 IP 地址： • LDAP、POP3、IMAP、FTP、HTTP、MDNS 和 AIM 登录 - 用户主机的地址 • SMTP 和 Oracle 登录 - 服务器的地址 • SIP 登录 - 会话发起人的地址 （(另请参阅当前 IP 和当前 IP/域名。） 关联 IP 地址并不意味着该用户为此 IP 地址的当前用户；当非授权用户登录主机时，登录信息将会记录到用户和主机历史记录中。如果没有授权用户与该主机相关联，则该主机的当前用户可能是非授权用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。 对于其他类型的用户活动，此字段留空。	否	不兼容	支持
姓氏	由领域获取的用户姓氏。如果符合以下条件，则此字段为空： • 您尚未配置领域。 • 管理中心无法将 管理中心 数据库中的用户与 LDAP 记录关联（例如，对于通过 AIM、Oracle 或 SIP 登录添加到数据库的用户）。 • 没有与 LDAP 服务器上的用户关联的姓氏。	支持	支持	否

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
上次查看时间	用户上次发起会话（或用户数据更新）的日期和时间。	支持	支持	否
登录时间	用户发起会话的日期和时间。	是	否	不兼容
PAT 范围起始值	TS 代理用户的起始端口地址转换范围。	是	否	不兼容
电话号码	由领域获取的用户电话号码。如果符合以下条件，则此字段为空： • 您尚未配置领域。 • 管理中心无法将 管理中心 数据库中的用户与 LDAP 记录关联（例如，对于通过 AIM、Oracle 或 SIP 登录添加到数据库的用户）。 • 没有与您的服务器上用户关联的电话号码。	是（作为电话）	是	否
领域	与用户关联的身份领域。	支持	支持	支持
安全组标签	当数据包进入受信任的 TrustSec 网络时思科 TrustSec 应用的安全组标记 (SGT) 属性。如果未配置 ISE，此字段留空。	否	不兼容	支持
会话持续时间	用户会话的持续时间，根据**登录时间**和当前时间计算。	是	否	不兼容
起始端口	如果用户由 TS 代理报告且用户会话当前处于活动状态，则此字段标识分配给用户的端口范围的开始值。如果用户的 TS 代理会话处于非活动状态，或者如果用户由其他身份源报告，则此字段为空。	支持	不支持	支持
时间	系统检测到用户活动的时间。	否	不兼容	支持

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
用户	至少，此字段会显示用户的领域和用户名。例如，`Lobby\jsmith`，其中 Lobby 为领域，jsmith 为用户名。 如果领域从 LDAP 服务器下载其他用户数据，且系统将其与一名用户相关联，则此字段也会显示用户的姓氏、名字和类型。例如，`John Smith (Lobby\jsmith, LDAP)`，其中 John Smith 为用户的姓名，LDAP 为类型。 **注释** 由于基于流量的检测可记录失败的 AIM 登录尝试，因此 管理中心可存储无效 AIM 用户（例如，用户名拼写错误的用户）。	支持	支持	否
用户名	与用户关联的用户名。	支持	支持	支持
流入的 VPN 字节数	对于远程接入 VPN 报告的用户活动，为 威胁防御接收的来自远程对等体或客户端的总字节数。 **注释** 在用户的 VPN 会话终止后，您可以查看接收的总字节数。对于正在进行的 VPN 会话，此项不是动态计数器。 对于其他类型的用户活动，此字段留空。	是	不支持	支持
流出的 VPN 字节数	对于远程接入 VPN 报告的用户活动，为 威胁防御传输到远程对等体或客户端的总字节数。 **注释** 在用户的 VPN 会话终止后，您可以查看传输的总字节数。对于正在进行的 VPN 会话，此项不是动态计数器。 对于其他类型的用户活动，此字段留空。	否	不兼容	支持
VPN 客户端应用	对于远程接入 VPN 报告的用户活动，为远程用户的 Cisco Secure 客户端 AnyConnect VPN 模块 应用。 对于其他类型的用户活动，此字段留空。	是	不支持	支持
VPN 客户端国家/地区	对于远程接入 VPN 报告的用户活动，为 Secure Client VPN 报告的国家/地区名称。 对于其他类型的用户活动，此字段留空。	否	不兼容	支持

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
VPN 客户端操作系统	对于远程接入 VPN 报告的用户活动，为 Secure Client VPN 报告的远程用户的终端操作系统。 对于其他类型的用户活动，此字段留空。	是	不支持	支持
VPN 客户端公共 IP	对于远程接入 VPN 报告的用户活动，为 Secure Client VPN 设备的公开可路由 IP 地址。 对于其他类型的用户活动，此字段留空。	是	不支持	支持
VPN 连接持续时间	对于远程接入 VPN 报告的用户活动，为会话处于活动状态的总时间 (HH:MM:SS)。 对于其他类型的用户活动，此字段留空。	否	不兼容	支持
VPN 连接配置文件	对于远程接入 VPN 报告的用户活动，为 VPN 会话使用的连接配置文件（隧道组）的名称。连接配置文件是远程接入 VPN 策略的一部分。 对于其他类型的用户活动，此字段留空。	是	不支持	支持
VPN 组策略	对于远程接入 VPN 报告的用户活动，为建立 VPN 会话时分配给客户端的组策略的名称；可能是静态分配的与 VPN 连接配置文件关联的组策略，或者是使用 RADIUS 进行身份验证时为动态分配的组策略。如果由 RADIUS 服务器分配，此组策略将覆盖为 VPN 连接配置文件配置的静态策略。组策略可配置适用于远程接入 VPN 策略中用户组的公用属性。 对于其他类型的用户活动，此字段留空。	是	不支持	支持
VPN 会话类型	对于远程接入 VPN 报告的用户活动，为会话类型：局域网到局域网或远程。 对于其他类型的用户活动，此字段留空。	是	不支持	支持

活动会话数据

分析 > **用户** > **活动会话**工作流显示有关当前用户会话的特定信息。当您网络上的用户同时运行多个会话时，Firepower 系统可以唯一地标识符合以下条件的会话：

- 它们具有唯一的 **IP 地址**值。
- 根据思科终端服务 (TS) 代理提供的信息，它们具有唯一的**起始端口**和**结束端口**值。
- 它们具有唯一的**当前 IP 域**值。

- 它们通过不同的身份源进行身份验证。
- 它们与不同的身份领域相关联。

有关系统存储的用户和用户活动数据的详细信息，请参阅用户数据，第 49 页和用户活动数据，第 52 页。

有关常规用户相关事件故障排除和远程接入VPN故障排除的信息，请参阅领域和用户下载故障排除和 *VPN* 故障排除。

查看活动会话数据

您可以查看活动会话表，然后根据要查找的信息管理事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问用户时所看到的页面因所使用的工作流程而异。可使用预定义工作流程并在用户详情页面终止，此工作流程包括列出了检测到的所有用户的用户表视图。用户详情页面提供有关符合限制条件的所有用户的信息。

过程

步骤 1 访问用户数据：

- 如果使用的是预定义工作流程，请点击 **分析** > **用户标题** > **活动会话**。
- 如果使用的是不包含活动会话表视图的自定义工作流，请点击（**切换工作流程**），然后选择**活动会话**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 6 页。
- 有关表中各列内容的详细信息，请参阅活动会话数据，第 48 页和用户相关字段，第 42 页。

用户数据

当身份源报告尚未包含在数据库中的用户的用户登录时，除非专门限制该登录类型，否则会将该用户添加到数据库中。

当出现以下情况之一时，系统会更新用户数据库：

- 管理中心 上的用户从用户表中手动删除非授权用户。
- 某个身份源报告该用户已注销。
- 某个领域结束其**用户会话超时：通过验证的用户**、**用户会话超时：未通过验证的用户**或**用户会话超时：访客用户**设置指定的用户会话。

注释 如果已配置 ISE/ISE-PIC，则您可能会在用户表中看到主机数据。由于并不完全支持由 ISE/ISE-PIC 进行的主机检测，所以不能使用 ISE 报告的主机数据执行用户控制。

系统检测到的用户登录类型确定存储的有关新用户的信息内容。

身份源	登录类型	存储的用户数据
ISE/ISE-PIC	Active Directory LDAP RADIUS RSA	• username • 当前 IP 地址 • 安全组标记 (SGT) - 不受 ISE-PIC 支持 • 终端配置文件/设备类型 - 不受 ISE-PIC 支持 • 终端位置/位置 IP - 不受 ISE-PIC 支持 • 类型 (LDAP)
TS 代理	Active Directory	• username • 当前 IP 地址 • 开始端口 • 结束端口 • 类型 (LDAP)
强制网络门户	Active Directory LDAP	• username • 当前 IP 地址 • 类型 (LDAP)

身份源	登录类型	存储的用户数据
基于流量的检测	LDAP AIM Oracle SIP HTTP FTP MDNS	• username • 当前 IP 地址 • 类型 (AD)
	POP3 IMAP	• username • 当前 IP 地址 • 邮箱地址 • 类型（`pop3` 或 `imap`）

注释 此表中不显示有关 Microsoft Azure Active Directory 用户的数据。

如果将领域配置为自动下载用户，则 管理中心会根据指定的间隔查询服务器。系统检测到新用户登录后，管理中心数据库可能需要五到十分钟的时间来使用用户元数据更新。管理中心获取关于每个用户的以下信息和元数据：

- username
- 名字和姓氏
- 邮箱地址
- department
- telephone number
- 当前 IP 地址
- 安全组标记 (SGT)（如果可用）
- 终端配置文件（如果可用）
- 终端位置（如果可用）
- 开始端口（如果可用）
- 结束端口（如果可用）

管理中心可在其数据库中存储的用户数取决于 管理中心型号。当检测到未授权用户登录主机时，会在用户和主机历史记录中记录该登录。如果没有授权用户与该主机相关联，则该主机的当前用户可能是非授权用户。但是，检测至一个授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。

请注意，对 AIM、Oracle 和 SIP 登录进行基于流量的检测会创建重复用户记录，因为它们不与系统从 LDAP 服务器获取的任何用户元数据关联。要防止由于这些协议中的用户记录重复而过度使用用户计数，请配置基于流量的检测以忽略这些协议。

可从数据库中搜索、查看和删除用户；也可从数据库中清除所有用户。

有关一般用户相关事件的故障排除信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。

查看用户数据

可查看用户表，然后根据所查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问用户时所看到的页面因所使用的工作流程而异。可使用预定义工作流程并在用户详情页面终止，此工作流程包括列出了检测到的所有用户的用户表视图。用户详情页面提供有关符合限制条件的所有用户的信息。

过程

步骤 1 访问用户数据：

- 如果使用的是预定义工作流，请选择 **分析** > **用户** > **用户**。
- 如果使用的是不包含用户表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**用户 (Users)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 6 页。
- 了解有关表中各列内容的详细信息；请参阅用户相关字段，第 42 页。

用户活动数据

系统生成在网络上传达用户活动详细信息的事件。当系统检测到用户活动时，会将用户活动数据记录到数据库中。可查看、搜索和删除用户活动；也可从数据库中清除所有用户活动。

当某用户首次出现在您的网络上时，系统会记录该用户的活动事件。当该用户再次出现时，不会记录新的用户活动事件。但是，如果该用户的 IP 地址发生更改，则系统会记录新的用户活动事件。

系统也会将用户活动与其他类型的事件相关联。例如，入侵事件可以指出在事件发生时登录源主机和目标主机的用户。这种关联可让您了解哪个用户已登录作为攻击目标的主机，或者了解内部攻击或端口扫描的发起者。

也可在关联规则中使用用户活动。根据用户活动的类型和指定的其他条件，可构建这样的关联规则：在用于关联策略时，可在网络流量符合条件的情况下启动补救和警报响应。

注释 如果已配置 ISE/ISE-PIC，则您可能会在用户表中看到主机数据。由于并不完全支持由 ISE/ISE-PIC 进行的主机检测，所以不能使用 ISE 报告的主机数据执行用户控制。

以下对四种类型的用户活动数据进行了说明。

新用户身份

当系统检测到数据库中不存在的未知用户登录时，将生成此类事件。

当某用户首次出现在您的网络上时，系统会记录该用户的活动事件。当该用户再次出现时，不会记录新的用户活动事件。但是，如果该用户的 IP 地址发生更改，则系统会记录新的用户活动事件。

用户登录

出现以下任一情况时，将生成此类型事件：

- 强制网络门户执行成功或失败的用户身份验证。
- 基于流量的检测检测到成功或失败的用户登录。

注释 系统将不记录由基于流量的检测发现的 SMTP 登录，除非数据库中已有匹配邮件地址的用户。

当非授权用户登录主机中时，该登录会记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则该主机的当前用户可能是非授权用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。

如果使用的是强制网络门户或基于流量的检测，请注意以下有关失败用户登录和失败用户身份验证数据的内容：

- 基于流量的检测（LDAP、IMAP、FTP 和 POP3 流量）报告的失败登录显示在用户活动表视图中，但不显示在用户表视图中。如果已知用户登录失败，则系统将通过其用户名来识别用户。如果未知用户登录失败，则系统将使用 **Failed Authentication** 作为其用户名。
- 强制网络门户报告的失败身份验证失败情况既显示在用户事件表视图中，又显示在用户表视图中。如果已知用户身份验证失败，则系统将通过其用户名来识别用户。如果未知用户身份验证失败，则系统将通过其输入的用户名来识别用户。

删除用户身份

手动删除数据库中用户时，将生成此类型事件。

已丢弃用户身份：已达到用户限制

当系统检测到数据库中不存在的用户但是无法添加该用户（因为数据库中用户数已经达到 管理中心型号规定的最大数量）时，将生成此类型事件。

在达到用户限制后，系统在多数情况下会停止向数据库添加新用户。要添加新用户，必须手动从数据库中删除旧的或非活动用户，或者清除数据库中的所有用户。

但是，系统支持授权用户。如果已达到极限且系统检测到先前未检测到的授权用户登录，则系统会删除保持非活动状态时间最长的非授权用户，并将其替换为新授权用户。

用户危害表现事件

系统将以下用户 IOC 更改记录在用户活动数据库中：

- 危害表现已解决。
- 为用户启用或禁用危害表现规则。

有关一般用户相关事件的故障排除信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

查看用户活动数据

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

可查看用户活动表，然后根据所需查找的信息操纵事件视图。访问用户活动时看到的页面因所使用的工作流程而异。可使用预定义工作流程（该工作流程包括用户活动表视图）并在用户详细信息页面（该页面包括符合限制条件的每个用户的详细信息）中终止。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问用户活动数据：

- 如果使用的是预定义工作流程，请选择**分析** > **用户标题** > **用户活动**。
- 如果使用的是不包含用户活动的表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**用户活动 (User Activity)**。

提示
如未显示事件，可能需要调整时间范围；请参阅更改时间窗口。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 6 页。
- 了解有关表中各列内容的详细信息；请参阅用户相关字段，第 42 页。

用户配置文件和主机历史记录

您可以通过查看“用户”(User) 弹出窗口了解有关特定用户的详细信息。出现的页面在本文档中称为“用户配置文件”，在 Web 界面中的标题为“用户身份”。

可以通过以下方式显示该窗口：

- 将用户数据与其他类型的事件相关联的任何事件视图
- 活动会话的表格视图
- 用户的表视图

用户信息也可在用户工作流程终止页面上显示。

所看到的用户数据与将在用户的表视图中看到的数据相同。

“危害表现”部分

有关此部分的信息，请参阅：

- 《Cisco Secure Firewall Management Center 设备配置指南》中的危害指标
- 危害表现数据字段，第 26 页
- 编辑单台主机或单个用户的危害表现规则状态，第 27 页
- 解决危害表现标记，第 27 页
- 查看危害表现标记的源事件，第 27 页

“主机历史记录”部分

主机历史记录以图表再现了最后二十四个小时的用户活动。用户所登录和所注销主机的 IP 地址的列表以条形图大约显示登录和注销次数。典型用户在一天中可能登录和注销多台主机。例如，如果定期自动登录邮件服务器，则将显示多个短期会话，而如果长时间登录（例如在工作时间），则将显示长时间会话。

如果使用基于流量的检测或强制网络门户捕获失败的登录，则主机历史记录还包含用户无法登录的主机。

用于生成主机历史记录的数据存储在用户历史记录数据库中，默认情况下可存储 10 百万次用户登录事件。如果在主机历史记录中未看到特殊用户的任何数据，则该用户为非活动用户，或者可能需要增加数据库限制。

相关主题

用户数据字段

查看用户详细信息和主机历史记录

过程

此时您有两种选择：

- 在列出用户的任何事件视图中，点击用户身份旁边显示的 **用户图标**，或者，对于与危害表现关联的用户， **红色用户图标**。
- 在任何用户工作流程中，点击 Users terminating 页面。

处理发现事件的历史记录

表 2:

功能	管理中心最低版本	威胁防御最低版本	详情
漏洞页面更改	6.7	任意	Bugtraq 及其漏洞数据不再可用。已进行以下更改： • 大多数漏洞数据现在来自国家漏洞数据库 (NVD)。 • 已删除过时和冗余字段。 • 表视图中添加了新的 CVE ID 列，表和详细信息页面中添加了新的“严重性”字段。 • 现在，您可以右键点击表中的 CVE ID，在 NVD 中查看有关该漏洞的详细信息。 • 表中的漏洞影响列已重命名为影响。（详细信息视图中的字段名称未更改。） • 在分析 > 主机 > 网络映射 > 主机下查看主机配置文件中的漏洞时，漏洞（不包括第三方漏洞）的详细信息使用新的字段集。 • 已从“分析”>“主机”>“网络映射”>“漏洞”页面上的“漏洞”选项中删除 Bugtraq 选项。 经修改的屏幕： • ”分析 > 主机 > 漏洞“下的所有页面 • “分析”>“主机”>“网络映射”页面上的“主机和漏洞”选项卡 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。