Cisco 安全防火墙管理中心管理指南，7.4

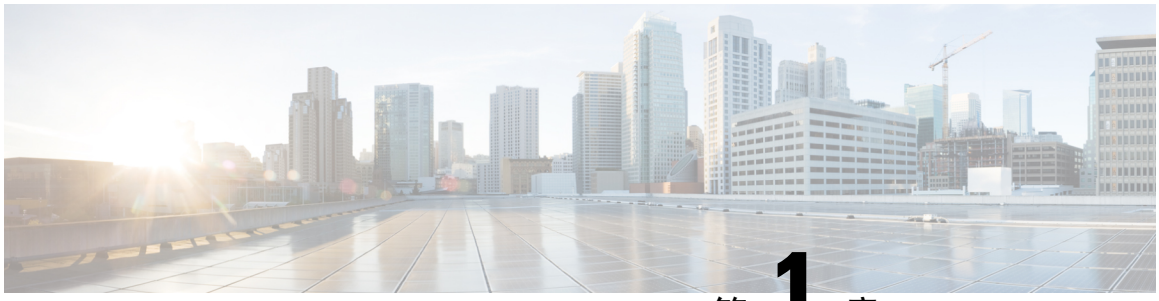
首次发布日期: 2023 年 9 月 7 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录

第 I 部分

入门



第 1 章

管理中心概述

本指南适用于作为主要管理器或仅作为分析管理器的本地设备 Cisco Secure Firewall Management Center。在将 思科防御协调器 (CDO) 云交付的 管理中心 用作主管理器时，您只能使用本地部署 管理中心 进行分析。请勿将本指南用于 CDO 管理；请参阅使用 Cisco 防御协调器中的云交付防火墙管理中心管理防火墙威胁防御。

Cisco Secure Firewall Management Center是一个功能强大的、基于 Web 的多设备管理器，它在自己的服务器硬件上运行，或者在虚拟机监控程序上作为虚拟设备运行。如果您需要多设备管理器，并且您需要 威胁防御上的所有功能，则应使用 管理中心 。管理中心 还提供强大的流量和事件的分析与监控功能。

注释 如果您有 CDO 托管设备，并且仅将本地部署 管理中心 用于分析，则本地部署 管理中心 不支持策略配置或升级。本指南中的某些相关章节和程序可能不适用于主要管理器为 CDO 的设备。

用作主用管理器的 管理中心： 管理中心 与其他管理器不兼容，因为 管理中心 拥有 威胁防御 配置，不允许绕过 管理中心直接配置 威胁防御 。

快速入门：基本设置

Cisco Secure Firewall 功能集足够强大且灵活，可以支持基本和高级配置。使用以下部分快速设置 Cisco Secure Firewall Management Center及其受管设备，以开始控制和分析流量。

在物理设备上安装和执行初始设置

过程

使用设备的文档在所有物理设备上安装和执行初始设置：

- **管理中心**
  - 您的硬件型号所对应的Cisco Secure 管理中心入门指南，可从以下网址获取

    《Cisco Secure Firewall Management Center 入门指南》
- **威胁防御 受管设备**
  - 思科 Firepower 1010 入门指南
  - Cisco Firepower 1100 入门指南
  - Cisco Firepower 2100 入门指南
  - 《Cisco Secure Firewall 3100 入门指南》
  - 思科 Firepower 4100 入门指南
  - 《Cisco Secure Firewall 4200 入门指南》
  - 思科 Firepower 9300 入门指南
  - 《适用于使用 Cisco Secure Firewall Management Center 的 ISA 3000 的 Cisco Secure Firewall Threat Defense 快速入门指南》

部署虚拟设备

如果您的部署包括虚拟设备，请按照下列步骤操作。使用文档路线图查找下列文档：浏览Cisco Secure Firewall Threat Defense 文档。

过程

步骤 1 确定将用于管理中心和设备的支持虚拟平台（可能不相同）。请参阅《*Cisco Secure Firewall* 兼容性指南》。

步骤 2 使用您的环境文档部署虚拟 Cisco Secure Firewall 管理中心：

- management center virtual 在 VMware 上运行：《思科 *Cisco Secure Firewall Management Center Virtual* 入门指南》
- management center virtual 在 AWS 上运行：《思科 *Cisco Secure Firewall Management Center Virtual* 入门指南》
- management center virtual 在 KVM 上运行：《思科 *Cisco Secure Firewall Management Center Virtual* 入门指南》

步骤 3 使用设备的文档部署虚拟设备：

- threat defense virtual 在 VMware 上运行：《*Cisco Cisco Secure Firewall Threat Defense Virtual for VMware* 入门指南》
- threat defense virtual 在 AWS 上运行：《思科 *Cisco Secure Firewall Threat Defense Virtual AWS* 入门指南》
- threat defense virtual 在 KVM 上运行：《*Cisco Cisco Secure Firewall Threat Defense Virtual for KVM* 入门指南》
- threat defense virtual 在 Azure 上运行：《*Cisco Cisco Secure Firewall Threat Defense Virtual for Azure* 入门指南》

首次登录

在首次登录新的 管理中心 之前，请按照 在物理设备上安装和执行初始设置，第 2 页 或 部署虚拟设备，第 2 页中的说明准备设备。

第一次登录到新的 管理中心（或新恢复为出厂默认设置的 管理中心 ）时，请使用 CLI 或 Web 界面的 **管理员** 帐户，并按照您的 管理中心 型号的《 思科 *Cisco Secure Firewall* 管理中心入门指南》中的说明进行操作。完成初始配置过程后，系统将配置以下方面：

- 两个**管理员**账户（一个用于 Web 接口访问，另一个用于 CLI 访问）的密码将设置为相同的值，符合 管理中心用户帐户的指南和限制，第 117 页中所述的强密码要求。系统仅在初始配置过程中同步两个 **管理员** 账户的密码。如果您在此后更改任一 **管理员** 账户的密码，两个密码将不再相同，并且强密码要求可以从 Web 接口 **管理员** 账户中删除。(请参阅 添加或编辑内部用户，第 118 页。)
- 管理中心 用于通过其管理接口 (eth0) 进行网络通信的以下网络设置将设置为默认值或您提供的值：

- 完全限定域名 (<主机名称>.<域>)
- 用于 IPv4 配置的启动协议 (DHCP 或 静态/手动)
- IPv4 地址
- 网络掩码
- 网关
- DNS 服务器
- NTP 服务器

可以通过 管理中心 Web 接口查看和更改这些设置的值；有关详细信息，请参阅 修改 管理中心 管理接口，第 76 页 和 时间同步，第 99 页 。

- 作为初始配置的一部分，系统会安排每周更新 GeoDB。我们建议您查看此任务，并在必要时进行更改，如安排 GeoDB 更新，第 216 页.
- 作为初始配置的一部分，系统会安排每周下载。我们建议您查看此任务，并在必要时进行更改，如自动执行软件下载，第 477 页.

重要事项 此任务仅下载更新。您负责安装此任务下载的任何更新。

- 作为初始配置的一部分， 系统会安排每周仅限配置的 管理中心 备份（本地存储）。我们建议您查看此任务，并在必要时进行更改，如计划 管理中心 备份，第 469 页.
- 作为初始配置的一部分，系统会下载并安装最新的VDB。为了让系统保持最新状态，我们建议您安排定期更新，如 漏洞数据库更新自动化，第 479 页.
- 作为初始配置的一部分，系统会安排每日入侵规则更新。我们建议您查看此任务，并在必要时进行更改，如计划入侵规则更新，第 219 页.

完成 管理中心 初始配置后，Web 接口将显示设备管理页面，如 《Cisco Secure Firewall Management Center 设备配置指南》中所述。

（这只是 **管理员** 用户首次登录时的默认登录页面。 **管理员** 或任何用户后续登录时，默认登录页面将按 指定主页，第 193 页中所述确定。）

完成初始配置时，通过按照设置基本策略和配置，第 4 页中的说明配置基本策略，开始控制和分析流量。

设置基本策略和配置

必须配置和部署基本策略，才能在控制面板、情景管理器和事件表中查看数据。

注释 这些并非是对策略或特性功能的全面讨论。有关其他功能和更高级配置的指南，请参阅本指南的其余部分。

开始之前

使用 Web 界面或 CLI 的**管理员**账户登录 Web 接口，并按照适用于您的硬件型号的《思科 *Cisco Secure Firewall* 管理中心入门指南》中所述执行初始配置，可从《安装和升级指南》获取。

过程

步骤 1 为此账户设置时区，如 设置默认时区，第 197 页中所述。

步骤 2 如果需要，请按照 许可证，第 239 页中的说明添加许可证。

步骤 3 如将设备添加到《Cisco Secure Firewall Management Center 设备配置指南》 中的 管理中心 中所述，将托管设备添加到部署。

步骤 4 按照以下说明配置受管设备：

- 在 《Cisco Secure Firewall Management Center 设备配置指南》中接口概述，在 威胁防御 设备上配置透明或路由模式
- 在 《Cisco Secure Firewall Management Center 设备配置指南》中接口概述，在 威胁防御 设备上配置接口

步骤 5 配置访问控制策略，如在 《Cisco Secure Firewall Management Center 设备配置指南》中 创建基本访问控制策略 中所述。

- 在大多数情况下，思科建议将**平衡的安全和连接性**入侵策略设置为默认操作。有关详细信息，请参阅 访问控制策略默认操作和 系统提供的网络分析和入侵策略。
- 在大多数情况下，思科建议启用连接日志记录，以满足组织的安全和合规性需要。在决定要记录哪些连接时，请考虑网络上的流量，以便不会干扰您的显示或系统不堪重负。有关详细信息，请参阅关于连接日志记录，第 699 页。

步骤 6 按照应用运行状况策略，第 354 页中的说明应用系统提供的默认运行状况策略。

步骤 7 自定义一些系统配置设置：

- 如果要允许服务的入站连接（例如，SNMP 或日志），请按照配置访问列表，第 41 页中的说明修改访问列表中的端口。
- 了解并考虑编辑数据库事件限制，如配置数据库事件限制，第 55 页中所述。
- 如果要更改显示语言，请按照设置 Web 接口的语言，第 68 页中的说明编辑语言设置。
- 如果您的组织限制使用代理服务器进行网络访问，请按照 修改 管理中心 管理接口，第 76 页中的说明编辑代理设置。

步骤 8 自定义网络发现策略，如在 中配置网络发现策略《Cisco Secure Firewall Management Center 设备配置指南》中所述。默认情况下，网络发现策略将分析网络上的所有流量。在大多数情况下，思科建议将发现限制在 RFC 1918 中的地址。

步骤 9 请考虑自定义如下其他常见设置：

- 如果为系统变量自定义默认值，请按照 《Cisco Secure Firewall Management Center 设备配置指南》中的说明了解 变量设置 使用方法。
- 如果要创建进行了本地身份验证的其他用户账号以访问 管理中心， 请参阅 添加或编辑内部用户，第 118 页。
- 如果要使用 LDAP 或 RADIUS 外部身份验证以允许访问 管理中心，请参阅 为管理中心配置外部身份验证，第 120 页。

步骤 10 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

下一步做什么

查看并考虑配置功能，第 7 页和本指南其余部分中描述的其他功能。

最新设备版本不支持的屏幕

虽然 管理中心 可以管理运行以前版本的设备（如 Cisco Secure Firewall Threat Defense 兼容性指南 中提供的兼容性矩阵中所述），但本指南仅包括最新版本的设备软件支持的功能。

有关仅在旧设备版本上支持的功能，请参阅与您的版本匹配的指南。

威胁防御设备

在典型的部署中，多个流量处理设备向一台 Cisco Secure Firewall Management Center报告，您可以使用它来执行管理、分析和报告任务。

威胁防御 设备是具有 NGIPS 功能的下一代防火墙 (NGFW)。NGFW 和平台功能还包括站点间和远程接入 VPN、稳健路由、NAT、集群以及应用检查和访问控制中的其他优化功能。

威胁防御 适用于各种物理和虚拟平台。

兼容性

有关管理器设备兼容性的详细信息（包括与特定设备型号兼容的软件、虚拟主机环境、操作系统等），请参阅Cisco Secure Firewall Threat Defense 版本说明、Cisco Secure Firewall Management Center 兼容性指南和Cisco Secure Firewall Threat Defense 兼容性指南。

功能

以下表列出一些常用的 功能。

设备和系统管理功能

要查找文档，请参阅浏览 Cisco Secure Firewall Threat Defense 文档。

如果要...	配置...	如以下所述...
管理登录到 Cisco Secure Firewall 设备的用户帐户	设备身份验证	管理中心 的，第 113 页和《Cisco Secure Firewall Management Center 设备配置指南》中的设备用户
监控系统硬件和软件的运行状况	运行状况监控策略	关于运行状况监控，第 341 页
备份设备上的数据	备份和恢复	备份/恢复，第 435 页
升级至新版本	系统更新	《适用于管理中心的 Cisco Secure Firewall Threat Defense 升级指南》 Cisco Secure Firewall Threat Defense 版本说明
设置物理设备基准	恢复出厂默认设置（重新映像）	适用于具备威胁防御的 Firepower 1000/2100 和 Cisco Secure Firewall 3100/4200 的思科 FXOS 故障排除指南
更新设备上的 VDB、入侵规则更新或 GeoDB	漏洞数据库 (VDB) 更新、入侵规则更新或地理定位数据库 (GeoDB) 更新	更新，第 211 页
应用许可证以利用许可证控制的功能	智能许可	关于许可证，第 239 页
确保设备运行的连续性	受管设备高可用性和/或 管理中心 高可用性	关于 《Cisco Secure Firewall Management Center 设备配置指南》 中的 *Cisco Secure Firewall* 威胁防御 “高可用性章节” 关于管理中心高可用性，第 287 页

如果要...	配置...	如以下所述...
配置设备，为两个或更多个接口之间的流量提供路由	路由	《Cisco Secure Firewall Management Center 设备配置指南》中的路由参考
在两个或多个网络之间配置数据包切换	设备切换	《Cisco Secure Firewall Management Center 设备配置指南》中的配置网桥组接口
将专用地址转换为公共地址，以进行 Internet 连接	网络地址转换 (NAT)	《Cisco Secure Firewall Management Center 设备配置指南》中的网络地址翻译
在托管 威胁防御 设备之间建立安全隧道	站点间虚拟专用网络 (VPN)	《Cisco Secure Firewall Management Center 设备配置指南》中的*VPN* 概述
在远程用户和托管 威胁防御 设备之间建立安全隧道	远程接入 VPN	《Cisco Secure Firewall Management Center 设备配置指南》中的*VPN* 概述
对受管设备、配置和事件的用户访问进行分段。	使用域的多租户	使用域的多租户简介，第 201 页
使用 REST API 客户端查看和管理设备配置	REST API 和 REST API 管理器	REST API 首选项 ，第 85 页 《*Cisco Secure Firewall* 管理中心 *REST API* 快速入门指南》
排除问题	不适用	故障排除，第 409 页

检测、防止和处理潜在威胁

要查找文档，请参阅浏览 Cisco Secure Firewall Threat Defense 文档。

如果要...	配置...	如以下所述...
检查、记录和对网络流量进行操作	访问控制策略、其他若干策略的父策略	《Cisco Secure Firewall Management Center 设备配置指南》中的访问控制简介
将指向或来自 IP 地址、URL 和/或域名的连接阻止或监控	访问控制策略中的安全情报	《Cisco Secure Firewall Management Center 设备配置指南》中的关于安全情报

如果要...	配置...	如以下所述...
控制用户在网络中可以访问的网站	策略规则中的 URL 过滤	《Cisco Secure Firewall Management Center 设备配置指南》中的*URL* 过滤
监视网络上的恶意流量和入侵	入侵策略	《Cisco Secure Firewall Management Center 设备配置指南》中的入侵策略基础知识
阻止未经检查的加密流量 检查加密或解密的流量	SSL 策略	《Cisco Secure Firewall Management Center 设备配置指南》中的*SSL* 策略概述
通过快速路径对封装的流量进行自定义深度检查并提高性能	预过滤器策略	《Cisco Secure Firewall Management Center 设备配置指南》中的关于预过滤
对访问控制允许或信任的网络流量施行速度限制	服务质量 (QoS) 策略	《Cisco Secure Firewall Management Center 设备配置指南》中的关于 *QoS* 策略
允许或阻止网络上的文件（包括恶意软件）	文件/恶意软件策略	《Cisco Secure Firewall Management Center 设备配置指南》中的网络恶意软件保护和文件策略
处理来自威胁情报源的数据	思科 Threat Intelligence Director (TID)	《Cisco Secure Firewall Management Center 设备配置指南》中的*Cisco Secure Firewall* 威胁智能导向器 概述
配置被动或主动用户身份验证以执行用户感知和用户控制	用户感知、用户身份、身份策略	《Cisco Secure Firewall Management Center 设备配置指南》中的关于用户身份源 《Cisco Secure Firewall Management Center 设备配置指南》中的关于身份策略
从网络上的流量中收集主机、应用和用户数据，以执行用户感知	网络发现策略	《Cisco Secure Firewall Management Center 设备配置指南》中的网络发现策略
使用设备以外的工具收集和分析有关网络流量和潜在威胁的数据	集成外部工具	使用外部工具的事件分析，第 597 页

如果要...	配置...	如以下所述...
执行应用检测和控制	应用检测器	《Cisco Secure Firewall Management Center 设备配置指南》中的应用检测
排除问题	不适用	故障排除，第 409 页

集成外部工具

要查找文档，请参阅浏览 Cisco Secure Firewall Threat Defense 文档。

如果要...	配置...	如以下所述...
当网络上的条件违反关联策略时自动启动补救	补救	补救简介，第 989 页 《*Firepower* 系统补救 *API* 指南》
将事件数据从 管理中心 到自定义开发的客户端应用	eStreamer 集成	eStreamer 服务器流传输，第 623 页 *Cisco Secure Firewall* 管理中心 *Event Streamer* 集成指南
使用第三方客户端在 管理中心 查询数据库表	外部数据库访问	外部数据库访问，第 58 页 *Cisco Secure Firewall* 管理中心数据库访问指南
通过从第三方源导入数据来扩充发现数据	主机输入	《Cisco Secure Firewall Management Center 设备配置指南》中的主机输入数据 《*Firepower* 系统主机输入 *API* 指南》
使用外部事件数据存储工具和其他数据资源调查事件	集成外部事件分析工具	使用外部工具的事件分析，第 597 页
排除问题	不适用	故障排除，第 409 页

搜索管理中心

您可以使用全局搜索功能快速查找并导航到 Cisco Secure Firewall Management Center 配置的元素。

注释 此功能仅在 Light 和 Dusk 主题中受支持。要更改主题，请参阅 更改 Web 接口外观，第 192 页。

您可以搜索以下实体的 管理中心 配置：

- 顶级菜单中 Web 界面页面的名称。（请参阅搜索 Web 接口菜单选项，第 14 页。）
- 对于某些策略类型：
  - 策略名称
  - 策略说明
  - 规则名称
  - 规则注释

  （请参阅搜索策略，第 14 页。）
- 对于某些对象类型：
  - 对象名称
  - 对象说明
  - 配置的值

  (请参阅 搜索对象，第 16 页 。)
- 操作方法逐步指导

  搜索将返回包含搜索词的逐步指导列表，以及指向每个逐步指导的链接。（请参阅搜索如何逐步指导，第 20 页。）

使用全局搜索时，请记住以下几点：

- 当您打开全局搜索工具时，最近十次搜索会显示在搜索文本框下方的历史记录列表中。您可以从此列表中选择一个项目来重新执行搜索。
- 当您键入搜索表达式时，界面会将搜索历史记录替换为在您键入搜索时更新的搜索结果；您不需要按 Enter 键执行搜索。
- 您可以使用鼠标或键盘箭头键和 Enter 键浏览历史记录列表或搜索结果。按 Enter 键可选择搜索结果中当前突出显示的项目。对于 Web 界面页面的结果，这会导致 管理中心 界面显示突出显示的页面。对于对象和策略，这将显示有关找到的实体的详细信息。
- 搜索不区分大小写。
- 在搜索中，可以使用以下通配符：
  - ? 匹配任意单个字符。
  - * 匹配 0 或多个字符。
  - ^ 将其前面的搜索词锚定到匹配实体的开头。

- $ 将其跟随的搜索词锚定到匹配实体的末尾

通配符无法转义。

- 为提高效率，全局搜索不返回间接搜索结果；也就是说，全局搜索不会返回引用找到搜索词的对象的策略或对象。但是，您可以通过在搜索详细信息窗格中查看找到的对象的**使用情况**选项卡来确定哪些策略或对象引用了许多找到的对象。
- 全局搜索返回搜索表达式的排名靠前的结果，具体取决于其与 管理中心中最常用的配置实体的相关性。如果全局搜索无法返回您希望找到的内容，请尝试细化搜索，尝试使用许多 GUI 页面顶部显示的搜索或过滤器工具，或者尝试 Web 界面提供的一些特定于配置的搜索功能：
  - 《Cisco Secure Firewall Management Center 设备配置指南》中的搜索规则
  - 《Cisco Secure Firewall Management Center 设备配置指南》中的搜索和过滤 *NAT* 规则表
  - 事件搜索
  - 搜索自定义表

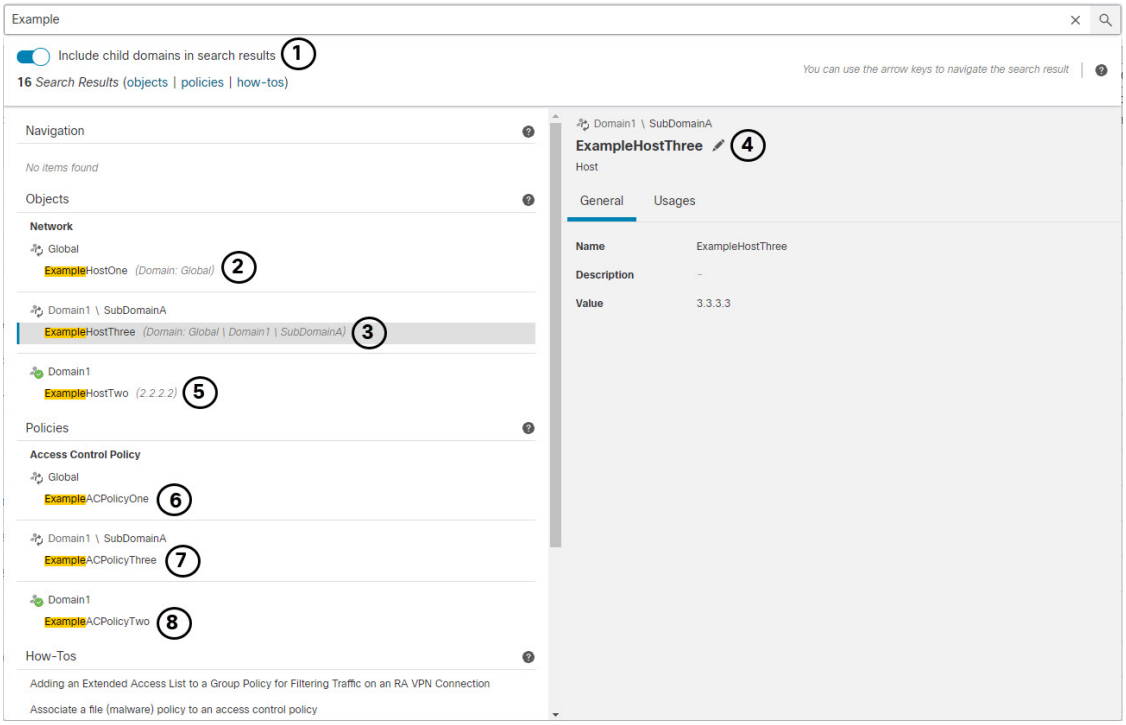
在多域部署中全局搜索

在多域部署中，默认情况下，搜索仅返回当前域及其祖先域中定义的对象和策略。您可以通过切换搜索结果对话框中的选项来查看子域中的对象和策略。

对于对象搜索，如果在当前域以外的域中定义的对象中找到搜索表达式，则搜索结果将显示这些对象所在的域的名称。如果在当前域中定义的对象中找到搜索表达式，则搜索结果会显示对象值。

在下面的示例屏幕截图中，部署包含三个级别的三个域：全局、域 1 和子域 A。当前域为 Domain1 的用户已在祖先域和子域中输入字符串“example”。

图 *1:* 多域环境中的全局搜索示例



1	用户已选择搜索子域 (SubDomainA) 以及当前域 (Domain1) 及其祖先 (Global)。	2	系统将显示父域 Global 中定义的匹配网络对象 ExampleHostOne，其中包含域名和指示用户必须切换域才能编辑详细信息的 **外部域**（）图标。
3	子域 SubDomainA 中定义的匹配网络对象 ExampleHostThree 将与域名一起显示，并且 **外部域**（）图标指示用户必须切换域才能编辑详细信息。此对象当前处于选中状态。	4	当前已选择匹配的网络对象 ExampleHostThree，并且右侧窗格中提供了相关信息。 **外部域**（）图标表示，当用户点击 **编辑**（）时，系统将提示用户确认域更改，然后才允许对对象进行编辑访问。
5	在当前域中定义的匹配网络对象 ExampleHostTwo 与对象值一起显示，并带有指示用户可以编辑此对象而无需切换域的 **当前域**（）图标。	6	系统将显示父域 Global 中定义的匹配访问控制策略 ExampleACPolicyOne，其中包含域名和指示用户必须切换域才能编辑详细信息的 **外部域**（）图标。
7	将显示子域 SubDomainA 中定义的匹配访问控制策略 ExampleACPolicyThree，其中包含域名和指示用户必须切换域才能编辑详细信息的图标。**外部域**（）	8	系统将显示当前域中定义的匹配访问控制策略 ExampleACPolicyTwo，并带有 **当前域**（）图标，指示用户无需切换域即可编辑详细信息。

搜索 Web 接口菜单选项

您可以搜索以查找 Web 界面顶级菜单中的页面位置。例如，要查看或配置服务质量设置，请搜索 **QoS**。

开始之前

此功能在经典主题中不可用。要更改主题，请参阅 更改 Web 接口外观，第 192 页。

过程

步骤 1 使用以下两种方法之一启动搜索：

- 在 Firepower 管理中心 Web 接口顶部的菜单栏中，点击 **搜索**（  ）。
- 将焦点放在文本框外，键入 / （正斜杠）。

步骤 2 输入要查找的菜单选项名称的一个或多个字母。搜索结果显示在文本框下方，并在您键入时更新；您不需要按 Enter 键执行搜索。

步骤 3 搜索结果按类别分组显示。要转到 **导航**下列出的页面，请点击搜索结果列表中的菜单路径。

搜索策略

下表指示可按名称搜索的策略类型：

适用范围	非适用范围
访问控制策略	威胁防御平台设置
预过滤器策略	Firepower 设置策略
威胁防御 NAT 策略	Firepower NAT 策略
入侵类别 • 入侵策略 • Network Analysis Policy	QoS 策略的比较 FlexConfig 策略 DNS 策略 恶意软件与文件策略 (Malware & File Policy) SSL 策略 身份策略

适用范围	非适用范围
	网络发现 应用检测器 关联策略 VPN 类别 • 动态访问策略 • 站点到站点 • 远程访问

全局搜索返回名称与搜索词匹配的策略，以及使用名称或注释与搜索词匹配的规则的访问控制策略。如果您在搜索结果列表中看到某个访问控制策略的名称与搜索结果不匹配，则表明该匹配是针对该策略中配置的规则的名称或注释进行的。

重要事项 全局搜索返回搜索表达式的排名靠前的结果，具体取决于其与 管理中心中最常用的配置实体的相关性。您的搜索词可能存在于不属于此搜索功能范围的策略类型中。有关全局搜索功能和替代搜索方法的完整说明，请参阅 搜索管理中心。

开始之前

此功能在经典主题中不可用。要更改主题，请参阅 更改 Web 接口外观，第 192 页。

过程

步骤 1 使用以下两种方法之一启动搜索：

- 在 Firepower 管理中心 Web 接口顶部的菜单栏中，点击 **搜索**（  ）。
- 将焦点放在文本框外，键入 / （正斜杠）。

步骤 2 在搜索文本框中输入搜索表达式。搜索结果显示在文本框下方，并在您键入时更新；您不需要按 Enter 键执行搜索。

步骤 3 （可选）在多域部署中，如果当前域具有后代域，则可以切换 **在搜索结果中包含子域** 以查看这些后代域中的策略。

步骤 4 搜索结果按类别分组显示。在多域部署中，在 **策略** 类别中，搜索结果按定义了找到的策略的域进行分组。在 **策略** 类别下，您可以执行以下操作：

收件人：	执行以下操作：
查看单一策略类型的搜索结果。	点击搜索结果中的策略类型，例如访问控制策略。

收件人：	执行以下操作：
查看有关策略的详细信息。	点击搜索结果列表中的策略名称以查看详细信息窗格并显示 **常规** 选项卡。
查看引用入侵和网络分析策略的访问控制策略。	点击搜索结果中的入侵或网络分析策略的名称以查看详细信息窗格并显示 **使用情况** 选项卡。
在单独的浏览器窗口中打开策略的策略配置页面。	点击搜索结果中的策略名称，然后在详细信息窗格中点击 **编辑** ( )。 在多域部署中，如果您选择编辑未在当前域中定义的策略，系统将提示您更改当前域。

搜索对象

下表指示“对象管理”页面 (**对象** > **对象管理**)上列出的对象类型在全局搜索功能范围内：

适用范围	非适用范围
AAA 服务器类别 • RADIUS 服务器组 • 单点登录服务器 访问列表类别 • 扩展访问列表 • 标准访问列表 地址池类别 • IPv4 池 • IPv6 池 AS 路径 社区列表类别 • 扩展社区 DNS 服务器组 外部属性类别 • 动态对象 • 安全组标记 地理位置 接口类别 • 安全区 • 接口组 密钥链 网络（包括网络、主机、范围、FQDN、网络组） PKI 类别 证书注册	应用过滤器 密码套件列表 社区列表类别 • 社区 可分辨名称类别 • 单独可分辨名称对象 • 可分辨名称对象组 文件列表 FlexConfig 类别 • FlexConfig 对象 • 文本对象 PKI 类别 • 外部证书组 (External Cert Groups) • 外部证书 • 内部 CA 证书 (Internal CA Groups) • 内部 CA • 内部证书组 (Internal Cert Groups) • 外部证书 • 受信任 CA 证书 (Trusted CA Groups) • 受信任 CA 安全情报类别 • DNS 列表和源 • 网络列表和源 • URL 列表和源

适用范围	非适用范围
策略列表 端口（对象和组、TCP、UDP、ICMP、ICMP6、其他） 前缀列表类别 • IPV4 前缀列表 • IPV6 前缀列表 路由映射 SLA 监控器 时间范围 时区 隧道区域 URL（对象、组） VLAN 标记（对象、组） VPN 类别 • 证书映射 • 组策略 • IKEv1 IPSec 提议 • IKEv1 策略 • IKEv2 IPsec 提议 • IKEv2 策略	Sinkhole 变量集 VPN 类别 • 安全客户端 文件 • 自定义属性

全局搜索返回名称或说明与搜索词匹配的对象，以及具有与搜索词匹配的配置值的对象。如果您在搜索结果列表中看到名称与搜索不匹配的对象，则表明该对象的说明或配置的值是匹配的。

重要事项 全局搜索返回搜索表达式的排名靠前的结果，具体取决于其与 管理中心中最常用的配置实体的相关性。您的搜索词可能不在此搜索功能范围内的对象类型中。有关全局搜索功能和替代搜索方法的完整说明，请参阅 搜索管理中心。

当您需要在部署中查找网络信息时，对象搜索尤其有用。您可以在对象名称、说明或配置的值中搜索以下内容：

- IPv4 和 IPv6 地址信息，包括以下格式：

- 完整地址（例如， `194.164.0.23`、 `2001:0db8:85a3:0000:0000:8a2e:0370:7334`。）
- 部分地址（例如， `194.164`、`2001:db8`。）
- 范围（例如， `192.164.1.1-192.168.1.5` 或 `2001:db8::0202-2001:db8::8329`。请勿在连字符前后添加空格。）全局搜索使用与指定范围内的任意地址匹配的网络地址返回对象。
- CIDR 表示法。（例如 `192.168.1.0/24`、 `2002::1234:abcd:ffff:101/64`。）全局搜索使用与指定 CIDR 块中的 any 匹配的网络地址返回对象。

- 端口信息：
  - 端口号（例如， `22` 或 `80`。）
  - 协议 (Protocols)。（例如， `https` 或 `ssh`。）
- 完全限定域名。（例如， `www.cisco.com`。)
- 列表。（例如， `http://www.cisco.com`。)
- 加密标准或散列类型。（例如， `AES-128` 或 `SHA`。）
- VLAN 标记号。（例如， `568`。）

开始之前

此功能在经典主题中不可用。要更改主题，请参阅 更改 Web 接口外观，第 192 页。

过程

步骤 1 使用以下两种方法之一启动搜索：

- 在 管理中心 Web 接口顶部的菜单栏中，点击 **搜索**（  ）。
- 将焦点放在文本框外，键入 `/`（正斜杠）。

步骤 2 在搜索文本框中输入搜索表达式。搜索结果显示在文本框下方，并在您键入时更新；您不需要按 Enter 键执行搜索。

如果在当前默认域以外的域中定义的对象中找到搜索表达式，则搜索结果将显示这些对象所在的域的名称。如果在当前域中定义的对象中找到搜索表达式，则搜索结果会显示对象值。

步骤 3 （可选）在多域部署中，如果当前域具有后代域，则可以切换 **在搜索结果中包含子域** 以查看这些后代域中的对象。

步骤 4 搜索结果按类别显示。在多域部署中，在 **对象** 类别中，搜索结果按定义找到的对象的域进行分组。在 **对象** 类别下，您可以执行以下操作：

收件人：	执行以下操作：
查看单个对象类型的搜索结果。	点击搜索结果中的对象类型，例如 **网络**。

收件人：	执行以下操作：
在搜索结果中查看有关对象的详细信息。	点击搜索结果中的对象名称可查看详细信息窗格并显示 **常规** 选项卡。
查看使用搜索结果中的对象的策略或对象的列表。	点击搜索结果中的对象名称可查看详细信息窗格并显示 **使用情况** 选项卡。 **注释** 全局搜索不提供所有对象类型的使用信息。
在单独的浏览器窗口中打开对象的对象配置页面。	点击搜索结果中的对象名称，然后在详细信息窗格中点击 **编辑** ( )。 在多域部署中，如果您选择编辑未在当前域中定义的对象，系统将提示您更改当前域。

搜索如何逐步指导

您可以搜索解决相关任务的操作方法逐步指导。例如，要查找描述设备设置程序的逐步指导，您可以搜索术语“设备”。

开始之前

此功能在经典主题中不可用。要更改主题，请参阅 更改 Web 接口外观，第 192 页。

过程

步骤 1 使用以下两种方法之一启动搜索：

- 在 Firepower 管理中心 Web 接口顶部的菜单栏中，点击 **搜索**（ ）。
- 将焦点放在文本框外，键入 /（正斜杠）。

步骤 2 输入与您想要查看逐步指导的任务相关联的搜索词。搜索结果显示在文本框下方，并在您键入时更新；您不需要按 Enter 键执行搜索。

步骤 3 搜索结果按类别分组显示。要查看 **操作方法**下列出的逐步指导，请点击搜索结果列表中的逐步指导标题。有关操作方法逐步指导的详细信息，请参阅 联机帮助、操作方法和文档，第 23 页。

切换域 Cisco Secure Firewall Management Center

在多域部署中，用户角色权限确定用户可以访问哪些域，以及用户在其中每个域内具有哪些权限。可以将单个用户帐户与多个域相关联，并在每个域中为该用户分配不同的权限。例如，可以在全局域中为用户分配只读权限，但在后代域中分配管理员权限。

与多个域关联的用户可以在同一 Web 界面会话中的域之间进行切换。

在工具栏中的用户名下，系统会显示可用域的树。树：

- 显示祖先域，但是，可以根据分配给用户帐户的权限禁用对这些域的访问。
- 隐藏用户帐户无法访问的任何其他域，包括同代域和后代域。

在切换到域时，系统会显示：

- 仅与该域相关的数据。
- 由面向该域分配给您的用户角色确定的菜单选项。

过程

在您的用户名下的下拉列表中，选择要访问的域。

情景菜单

Firepower 系统 Web 界面中的某些页面支持右键点击上下文菜单（最常见）或左键点击上下文菜单，可供您用作访问 Firepower 系统中其他功能的快捷方式。上下文菜单的内容取决于您访问菜单时所处的位置 - 不仅是页面，还可以是特定数据。

例如：

- IP 地址热点，提供有关与该地址关联的主机的信息，包括任何可用的 whois 和主机配置文件信息。
- SHA-256 散列值热点，通过其可将文件的 SHA-256 散列值添加到干净列表或自定义检测列表中，或者查看要复制的完整散列值。

在不支持 Firepower 系统上下文菜单的页面或位置上，适用于浏览器的普通上下文菜单将会显示出来。

策略编辑器

许多策略编辑器都包含基于每个规则的热点。您可以插入新规则和类别，剪切、复制和粘贴规则，设置规则状态，以及编辑规则。

入侵规则编辑器

入侵规则编辑器包含基于每个入侵规则的热点。您可以编辑规则，设置规则状态，配置阈值和抑制选项，以及查看规则文档。或者，在点击情景菜单中的**规则文档**后，可以点击文档弹出窗口中的**规则文档**以查看更具体的规则详情。

事件查看器

事件页面（“分析”菜单下的向下钻取页面和表视图）包含基于每个事件、IP地址、URL、DNS查询以及某些文件的SHA-256散列值的热点。查看大多数事件类型时，您可以执行以下操作：

- 在情景管理器中查看相关信息。
- 在新窗口中向下展开到事件信息。
- 查看事件视图中的事件字段包含过长而无法完全显示的文本（例如文件的SHA-256散列值、漏洞说明或URL）的位置的完整文本。
- 使用上下文交叉启动功能打开有关从外部至Firepower源的元素详细信息的Web浏览器窗口。有关详细信息，请参阅使用基于 Web 的资源的事件调查，第 605 页。

查看连接事件时，您可以将项目添加到默认安全情报阻止和 不阻止 名单：

- IP 地址热点中的 IP 地址。
- URL 热点中的 URL 或域名。
- DNS 查询热点中的 DNS 查询。

查看捕获的文件、文件事件和恶意软件事件时，您可以执行以下操作：

- 在干净列表或自定义检测列表中添加或删除文件。
- 下载文件的副本。
- 查看存档文件内的嵌套文件。
- 下载嵌套文件的父存档文件。
- 输入文件组成。
- 提交文件以进行本地恶意软件和动态分析。

查看入侵事件时，您可以执行与入侵规则编辑器或入侵策略中的任务类似的任务：

- 编辑触发规则。
- 设置规则状态（包括禁用规则）。
- 配置阈值和抑制选项。
- 查看规则文档。或者，在点击情景菜单中的**规则文档**后，可以点击文档弹出窗口中的**规则文档**以查看更具体的规则详情。

入侵事件数据包视图

入侵事件数据包视图包含 IP 地址热点。数据包视图使用左键点击上下文菜单。

控制面板

很多控制面板构件都包含热点，用于查看“情景管理器”(Context Explorer) 中的相关信息。控制面板构件还包含 IP 地址和 SHA-256 散列值热点。

Context Explorer

“情景管理器”(Context Explorer) 包含热点，位于其图表、表格和图形上方。如果您希望以比“情景管理器”(Context Explorer) 允许的更详细的程度来检查图形或列表中的数据，则您可以向下展开到相关数据的表视图。您还可以查看相关的主机、用户、应用、文件和入侵规则信息。

情景管理器使用左键点击上下文菜单，该菜单也包含情景管理器独有的过滤选项及其他选项。

与思科共享数据

您可以选择使用以下功能与思科共享数据：

- Cisco Success Network

  请参阅配置 Cisco Success Network 注册，第 602 页

- Web 分析

  请参阅Web 分析，第 108 页

联机帮助、操作方法和文档

可以通过以下方式从 Web 界面访问联机帮助：

- 点击各页面上的上下文帮助链接
- 通过选择**帮助 (Help)** > **页面级帮助 (Page-level Help)**

“操作方法”是一个构件，它提供导航管理中心上任务的逐步指导。逐步指导将引导您完成每个步骤，依次熟悉可能必须导航的各类陌生UI界面，引导您完成实现任务所需执行的步骤，最终完成任务。**操作方法**构件默认为启用。要禁用该构件，请从用户名下的下拉列表中选择**用户首选项**，然后取消选中 **How-To 设置**选项卡中的**启用 How-To** 复选框。要打开“操作方法”构件，请选择**帮助 (Help)** > **操作方法 (How-Tos)**。

注释 通常情况下，逐步指导对所有UI页面可用，并且不区分用户角色。但是，根据用户权限的不同，某些菜单项将不会显示在 管理中心 界面上。因此，逐步指导将不会在此类页面上执行。

管理中心 上提供了以下逐步指导：

有关 管理中心 中支持的功能逐步指导的列表，请参阅Cisco Secure Firewall Management Center 支持的功能逐步指导。

可以使用以下文档路线图查找与其他文档：

浏览 Cisco Secure Firewall Threat Defense 文档。

Cisco.com 上的用户指南

在配置 Cisco Secure Firewall Management Center部署版本 6.0+ 时，以下文档可提供帮助。

注释 有些链接的文档不适用于 Cisco Secure Firewall Management Center部署。例如， Cisco Secure Firewall Threat Defense页面上的某些链接专用于 Secure Firewall 设备管理器管理的部署，并且硬件页面上的某些链接与 管理中心无关。为避免混淆，请特别注意文档标题。此外，有些文档涵盖多个产品，因此可能会出现在多个产品页面上。

Cisco Secure Firewall Management Center

- Cisco Secure Firewall Management Center硬件设备：

  http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Cisco Secure Firewall Management Center虚拟设备：
  - http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html
  - http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

Cisco Secure Firewall Threat Defense，也称为 NGFW（下一代防火墙）设备

- Cisco Secure Firewall Threat Defense软件：

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html

- Cisco Secure Firewall Threat Defense虚拟：

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/tsd-products-support-series-home.html

- Firepower 1000 系列：

  https://www.cisco.com/c/en/us/support/security/firepower-1000-series/tsd-products-support-series-home.html

- Firepower 2100 系列：

  https://www.cisco.com/c/en/us/support/security/firepower-2100-series/tsd-products-support-series-home.html

- Cisco Secure Firewall 3100:

  https://www.cisco.com/c/en/us/support/security/secure-firewall-3100-series/series.html

- Firepower 4100 系列：

  https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html

- Cisco Secure Firewall 4200：

  https://www.cisco.com/c/en/us/support/security/secure-firewall-4200-series/series.html

- Firepower 9300：

  https://www.cisco.com/c/en/us/support/security/firepower-9000-series/tsd-products-support-series-home.html

- ISA 3000：

  https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html

文档中的许可声明

节开头的许可证声明指示必须将哪个经典或智能许可证分配到受管设备以启用该节所述的功能。

由于许可功能通常是累加的，因此许可证声明仅提供每项功能的最高要求许可证。

许可证声明中的“或”语句表明必须向受管设备分配特定许可证以启用该节所述的功能，但是附加许可证可以添加功能。例如，在文件策略中，某些文件规则操作要求向设备分配保护许可证，而其他操作则要求分配 恶意软件防御 许可证。

有关许可证的详细信息，请参阅关于许可证，第 239 页。

相关主题

关于许可证，第 239 页

文档中的受支持设备声明

章节或主题开头的“受支持设备”声明指示仅在指定的设备序列、系列或型号上才支持相应的功能。例如，许多功能仅在 Cisco Secure Firewall Threat Defense 设备上受支持。

有关此版本支持的平台的详细信息，请参阅版本说明。

文档中的访问声明

本文档中每个程序开头的“访问”声明表明执行此程序所需的预定义用户角色。所列的任何角色都可以执行此程序。

自定义角色的用户可以拥有不同于预定角色的权限。预定角色用于指示某个程序的访问要求时，具有相似权限的自定义角色也能访问。某些具有自定义角色的用户可以使用略有不同的菜单路径到达配置页面。例如，具有仅有入侵策略权限的自定义角色的用户通过入侵策略而非通过访问控制策略的标准路径来访问网络分析策略。

Firepower 系统 IP 地址约定

您可以使用 IPv4 无类域间路由选择 (CIDR) 表示法和类似的 IPv6 前缀长度表示法定义 Firepower 系统中很多位置的地址块。

使用 CIDR 或前缀长度表示法指定 IP 地址块时，Firepower 系统**只**使用掩码或前缀长度指定的那部分网络 IP 地址。例如，如果键入 10.1.2.3/8，则 Firepower 系统使用 10.0.0.0/8。

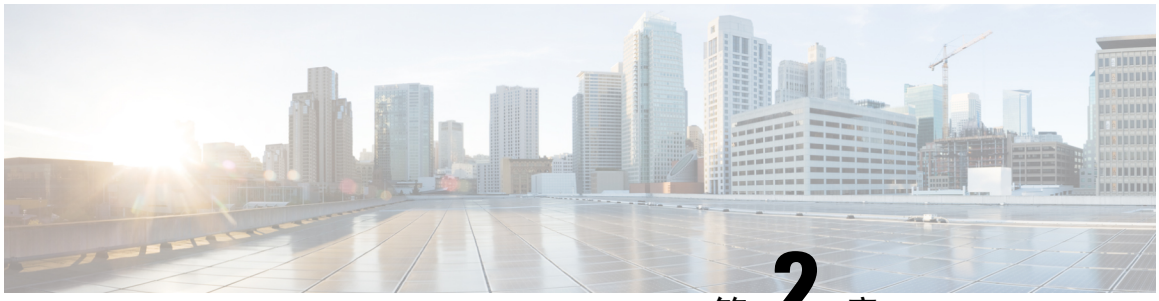
换句话说，虽然思科建议您在使用 CIDR 或前缀长度表示法时采用使用位边界上网络 IP 地址的标准方法，但是 Firepower 系统并不要求必须这么做。

其他资源

除了我们提供的大量文档外，防火墙社区也是内容丰富的参考资料库。在这里，您可以找到思科硬件的三维模型、硬件配置选择器、产品资料、配置示例、故障排除技术笔记、培训视频、实验和 Cisco Live 大会、社交媒体公众号、思科博客，以及技术出版团队发布的所有文档。

在社区网站或视频分享网站上发帖的某些个人（包括版主在内）在思科系统公司工作。这些网站上发表的观点以及任何相关评论均为原作者的个人观点，与思科无关。此处内容仅用于提供信息，不作为思科或其他各方的认可或声明。

注释 防火墙社区 上的一些视频、技术说明和参考材料指向的是旧版 管理中心。您的 管理中心 版本与视频或技术说明中引用的版本可能在用户界面上有不同之处，从而导致过程不尽相同。



第 2 章

登录到管理中心

以下主题介绍如何登录 Firepower 系统：

用户帐户

您必须提供用户名和密码才能访问 管理中心 或托管设备的 Web 接口或 CLI。在托管设备上，具有配置层级访问权限的 CLI 用户可以使用 专家 命令访问 Linux 外壳程序。在 管理中心上，所有 CLI 用户都可以使用 专家 命令。威胁防御 和 管理中心 可配置为使用外部身份验证，将用户凭证存储在外部 LDAP 或 RADIUS 服务器上；您可以保留或向外部用户提供 CLI 访问权限。 管理中心 可以配置为使用符合安全断言标记语言 (SAML) 2.0 开放式身份验证和授权标准的任何 SSO 提供程序支持单点登录 (SSO)。

管理中心CLI 提供一个有权访问所有命令的 **admin** 用户。 用户可以访问的 管理中心 Web 接口功能由管理员授予用户账户的权限控制。在托管设备上，用户可以访问 CLI 和 Web 接口的功能由管理员授予用户账号的权限控制。

注释 系统根据用户账号审核用户活动；请确保用户使用正确的账户登录系统。

注意 在托管设备上，所有 管理中心 CLI 用户和具有配置层 CLI 访问权限的用户可以在外壳程序中获取 root 权限，这可能构成安全风险。出于系统安全原因，我们强烈建议：

- 如果您建立外部身份验证，请确保对具有 CLI 访问权限的用户列表进行适当的限制。
- 在托管设备上授予 CLI 访问权限时，请显示具有配置层 CLI 访问权限的内部用户列表。
- 不建立 Linux 外壳用户；仅使用预定义的 **管理员** 用户和 **管理员** 用户在 CLI 中创建的用户。

注意 强烈建议您不要使用 Linux Shell，除非 Cisco TAC 或 Cisco Secure Firewall 用户文档明确说明需要这样做。

不同的设备支持不同类型的用户帐户，每个帐户都具有不同的功能。

Cisco Secure Firewall Management Center

Cisco Secure Firewall Management Center 支持以下用户帐户类型：

- 用于 Web 界面访问的预定义 **admin** 帐户具有管理员角色，可以通过 Web 界面进行管理。
- 自定义用户账户，**admin** 用户和具有管理员权限的用户可以创建和管理此类账户。
- 预先定义 CLI 访问的 **admin** 账户。使用此账户登录的用户可以使用 专家 命令以获得访问 Linux 外壳的权限。

  在初始配置期间，CLI **admin** 账户和 Web 接口 **admin** 账户的密码会同步，但此后您可以为两个 **admin** 账户配置单独的密码。

注意 出于系统安全原因，思科强烈建议您不要在任何设备上建立其他 Linux 外壳用户。

Cisco Secure Firewall Threat Defense 和 Cisco Secure Firewall Threat Defense Virtual 设备

Cisco Secure Firewall Threat Defense 和 Cisco Secure Firewall Threat Defense Virtual 设备支持以下用户帐户类型：

- 预先定义的 **admin** 帐户，可用于对设备进行任何形式的访问。
- 自定义用户账户，**admin** 用户和具有“配置”访问权限的用户可以创建和管理此类账户。

Cisco Secure Firewall Threat Defense支持对 SSH 用户进行外部身份验证。

系统用户界面

根据设备类型，可以使用基于 Web 的 GUI、辅助 CLI 或 Linux 外壳与设备交互。在 Cisco Secure Firewall Management Center 部署中，可从 管理中心的 GUI 执行从大多数配置任务。只有少数任务需要使用 CLI 或 Linux 外壳直接访问设备。我们强烈不鼓励您使用 Linux 外壳，除非 Cisco TAC 或用户文档明确说明需要这样做。

有关浏览器要求的信息，请参阅Cisco Secure Firewall 版本说明。

注释 在所有设备上，当用户连续三次尝试通过 SSH 登录 CLI 失败时，系统会终止 SSH 连接。

设备	基于 Web 的 GUI	辅助 CLI	Linux Shell
Cisco Secure Firewall Management Center	• 支持预定义的 **管理员** 用户和自定义用户账号。 • 可用于管理和分析任务。	• 支持预定义的 **管理员** 用户和自定义外部用户账号。 • 可通过 SSH、串行或键盘和显示器连接进行访问。 • 仅应用于思科 TAC 指导的管理和故障排除。	• 支持预定义的 **admin** 用户。 • 必须通过 Cisco Secure Firewall Management Center CLI 中的 `expert` 命令进行访问。 • 可通过 SSH、串行或键盘和显示器连接进行访问。 • 仅应用于思科 TAC 指导的管理和故障排除，或管理中心 文档中的详细指导。
Cisco Secure Firewall Threat Defense Cisco Secure Firewall Threat Defense Virtual	-	• 支持预定义的 **管理员** 用户和自定义用户账号。 • 可通过 SSH、串行或键盘和显示器连接在物理设备中进行访问。可通过 SSH 或虚拟机控制台进行访问。 • 可用于思科 TAC 指导的安装和故障排除。	• 支持预定义的 **管理员** 用户和自定义用户账号。 • 具有“配置”权限的CLI用户可使用 `expert` 命令访问。 • 仅应用于思科 TAC 指导的管理和故障排除，或管理中心 文档中的详细指导。

相关主题

添加或编辑内部用户 ， 第 118 页

Web 界面注意事项

- 如果您的组织使用通用访问卡 (CAC) 进行身份验证，通过 LDAP 进行身份验证的外部用户可以使用 CAC 凭证获得对设备 Web 接口的访问权限。
- 在默认主页顶部显示的菜单和菜单选项取决于用户帐户的权限。但是，默认主页上的链接包括适用于各种用户帐户权限范围的选项。如果点击的链接所需的权限与已授予帐户的权限不同，系统将显示警告消息并记录相关活动。
- 某些进程耗时较长，这可能会导致网络浏览器显示指明脚本无响应的消息。如果出现这种情况，请确保允许脚本继续运行，直至完成。

相关主题

指定主页，第 193 页

会话超时

默认情况下，除非您以其他方式配置为免除会话超时，否则在不活动达 1 小时之后系统会自动将您从会话中注销。

注释 对于 SSO 用户，当 管理中心 会话超时时，显示内容会短暂重定向到 IdP 接口，然后是 管理中心 登录页面。除非已从其他位置终止 SSO 会话，否则任何人只需点击登录页面上的 **单点登录** 链接即可访问 管理中心，而无需提供登录凭证。为确保 管理中心 安全并防止其他人使用您的 SSO 账户访问 管理中心，我们建议您在注销 管理中心时不要让 管理中心 登录会话处于无人参与状态，并在 IdP 上注销 SSO 联合。

具有“管理员”(Administrator) 角色的用户可以通过以下设置更改设备的会话超时间隔：

系统 > 配置 > 外壳超时

相关主题

配置会话超时，第 97 页
配置 SAML 单点登录，第 136 页

登录到 Cisco Secure Firewall Management Center Web 界面

注释 此任务适用于通过 LDAP 或 RADIUS 服务器进行身份验证的内部用户和外部用户。有关 SSO 登录，请参阅 使用 SSO 登录管理中心 Web 接口，第 31 页。

用户受限于单个活动会话。如果您尝试通过已具有活动会话的用户帐户登录，则系统会提示您终止另一会话或以另一个用户的身份登录。

在多个 管理中心共享同一 IP 地址的 NAT 环境中：

- 每次 管理中心 只能支持一个登录会话。
- 要访问不同的 管理中心，请为每次登录使用不同的浏览器（例如 Firefox 和 Chrome），或将浏览器设置为隐身或隐私模式。

开始之前

- 如果您无法访问网络界面，请联系系统管理员修改您的帐户权限，或者用具有管理员访问权限的用户身份登录并修改帐户的权限。
- 按照添加或编辑内部用户，第 118 页所述创建用户帐户。

过程

步骤 1 将浏览器定向到 **https://***ipaddress_or_hostname***/**，其中 *ipaddress* 或 *hostname* 对应您的 管理中心。

步骤 2 在**用户名 (Username)** 和**密码 (Password)** 字段中，输入用户名和密码。请注意以下准则：

- 用户名不区分大小写。
- 在多域部署中，请在用户名前面附加在其中创建用户帐户的域。无需在用户名前面附加任何祖先域。例如，如果用户帐户在 SubdomainB 中创建（其祖先域为 DomainA），则请按以下格式输入用户名：

  ```
  SubdomainB\username
  ```

- 如果您的组织在登录时使用 SecurID® 令牌，请将令牌附加到 SecurID PIN，并将其用作密码进行登录。例如，如果 PIN 为 `1111` 且 SecurID 令牌为 `222222`，请输入 `1111222222`。必须生成 SecurID PIN 后才能登录系统。

步骤 3 点击**登录 (Login)**。

相关主题

会话超时，第 30 页

使用 SSO 登录管理中心 Web 接口

管理中心可以配置为参与符合安全断言标记语言 (SAML) 2.0 开放标准的 SSO 提供程序实施的任何单点登录 (SSO) 联合。SSO 用户账户必须在身份提供程序 (IdP) 上建立，并且必须使用邮件地址作为其账户名称。如果您的用户名不是邮件地址，或者 SSO 登录失败，请联系您的系统管理员。

注释 管理中心不支持使用 SSO 账户的 CAC 凭证登录。

用户受限于单个活动会话。如果您尝试通过已具有活动会话的用户帐户登录，则系统会提示您终止另一会话或以另一个用户的身份登录。

在多个管理中心共享同一 IP 地址的 NAT 环境中：

- 每个管理中心只能支持一个登录会话。
- 要访问不同的管理中心，请为每次登录使用不同的浏览器（例如 Firefox 和 Chrome），或将浏览器设置为隐身或隐私模式。

开始之前

- 为 SSO 访问配置管理中心。请参阅配置 SAML 单点登录，第 136 页。
- 如果您无权访问 Web 界面，请联系系统管理员以在 SSO IdP 上配置您的账户。

过程

步骤 1 将浏览器定向到 **https://***ipaddress_or_hostname/*，其中 *ipaddress* 或 *hostname* 对应您的管理中心。

注释 SSO 用户必须使用专门为 SSO 访问配置的登录 URL 进行一致的访问管理中心；请向管理员咨询此信息。

步骤 2 点击**单点登录 (Single Sign-On)** 链接。

步骤 3 系统以以下两种方式之一进行响应：

- 如果您已登录 SSO 联合， 管理中心显示默认主页。
- 如果您尚未登录 SSO 联合， 管理中心 会将您的浏览器重定向到 IdP 的登录页面。在 IdP 完成登录过程后， 管理中心 显示默认主页。

相关主题

会话超时，第 30 页
配置 SAML 单点登录，第 136 页

使用 CAC 凭证登录 Cisco Secure Firewall Management Center

用户受限于单个活动会话。如果您尝试通过已具有活动会话的用户帐户登录，则系统会提示您终止另一会话或以另一个用户的身份登录。

在多个 管理中心共享同一 IP 地址的 NAT 环境中：

- 每次 管理中心 只能支持一个登录会话。
- 要访问不同的 管理中心，请为每次登录使用不同的浏览器（例如 Firefox 和 Chrome），或将浏览器设置为隐身或隐私模式。

注意 在浏览会话活动期间，**请勿**删除CAC。如果在会话期间移除或替换CAC，则网络浏览器会终止该会话，并且系统会注销 Web 界面。

开始之前

- 如果您无法访问网络界面，请联系系统管理员修改您的帐户权限，或者用具有管理员访问权限的用户身份登录并修改帐户的权限。
- 创建用户账号，如 添加或编辑内部用户，第 118 页中所述。
- 配置 CAC 身份验证和授权，如 使用 LDAP 配置通用访问卡身份验证，第 135 页中所述。

过程

步骤 1 按照您的组织的指示插入 CAC。

步骤 2 将浏览器定向到 **https://***ipaddress_or_hostname***/**，其中 *ipaddress* 或 *hostname* 对应您的 管理中心。

步骤 3 如有提示，请输入与步骤 1 中插入的 CAC 关联的 PIN。

步骤 4 如有提示，请从下拉列表中选择相应的证书。

步骤 5 点击**继续 (Continue)**。

相关主题

使用 LDAP 配置通用访问卡身份验证，第 135 页
会话超时，第 30 页
管理中心的 SSO 指南，第 137 页

登录管理中心命令行接口

管理员 CLI 用户和某些自定义外部用户可以登录 管理中心 CLI。

注意 强烈建议您不要使用 Linux 外壳，除非 Cisco TAC 或 管理中心 文档明确说明需要这样做。

注释 对于所有设备上，当用户连续三次尝试通过 SSH 登录 CLI 失败时，系统会终止 SSH 连接。

开始之前

以 **管理员** 用户身份完成初始配置过程。请参阅首次登录，第 3 页。

过程

步骤 1 使用 **管理员** 用户名和密码通过 SSH 或控制台端口连接到 管理中心 。

如果您的组织在登录时使用 SecurID® 令牌，请将令牌附加到 SecurID PIN，并将其用作密码进行登录。例如，如果 PIN 为 `1111` 且 SecurID 令牌为 `222222`，请输入 `1111222222`。必须生成 SecurID PIN 后才能登录 。

步骤 2 使用任何可用的 CLI 命令。

查看您的上次登录

如果您怀疑未经授权的用户使用您的凭证登录 Cisco Secure Firewall Management Center，您可以查看上次使用您的凭证登录的日期、时间和 IP 地址：

开始之前

如果您使用的是经典主题，则此功能不可用。您可以在“用户首选项”中选择 UI 主题。

过程

步骤 1 登录到 Cisco Secure Firewall Management Center。

步骤 2 在浏览器窗口的右上角，查找用于登录的用户 ID。

步骤 3 点击您的用户名。

步骤 4 有关上次登录的信息显示在所显示菜单的底部。

注销 Firepower 系统 Web 界面

不再使用 Firepower 系统 Web 界面时，思科建议您注销，即使只是暂时离开 Web 浏览器。注销会结束您的 Web 会话并确保没有人可以通过您的凭证使用界面。

注释 如果您要注销 管理中心上的SSO 会话，当您注销时，系统会将您的浏览器重定向到您的组织的SSO IdP。为确保 管理中心 安全并防止其他人使用您的 SSO 账户访问 管理中心 ，我们建议您在 IdP 处注销 SSO 联合。

过程

步骤 1 从用户名下的下拉列表中，选择**注销 (Logout)**。

步骤 2 如果您要注销 管理中心上的 SSO 会话，系统会将您重定向到您的组织的 SSO IdP。在 IdP 上注销以确保 管理中心 安全。

相关主题

会话超时，第 30 页

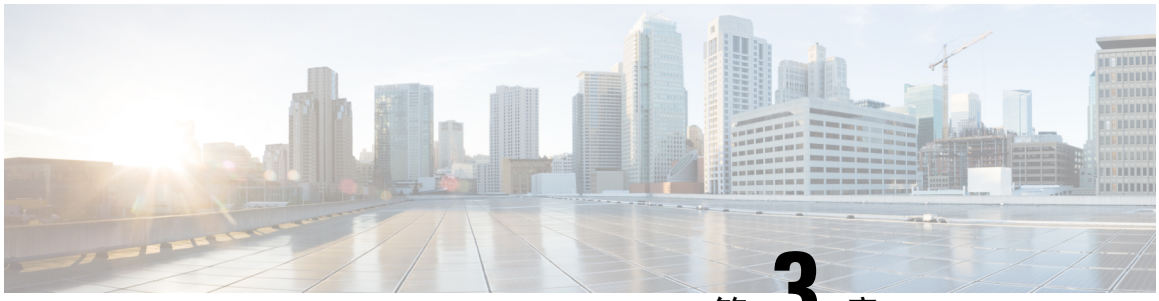
登录管理中心的历史记录

功能	最低 管理中心	最低 威胁防御	详情
添加了对使用任何符合 SAML 2.0 的 SSO 提供程序的单点登录 (SSO) 的支持。	6.7	任意	为在任何第三方 SAML 2.0 兼容身份提供程序 (IdP) 上配置的用户添加了新功能，可以使用登录页面上的新 **单点登录** 链接登录 管理中心 。 新的/修改后的屏幕： 登录屏幕
查看有关您上次登录 Cisco Secure Firewall Management Center的信息	6.5	任意	查看您上次登录的日期、时间和 IP 地址。 新增/修改的菜单： 窗口右上角的菜单，显示您用于登录的用户名。 支持的平台： 管理中心
自动CLI访问 管理中心	6.5	任意	使用 SSH 登录 管理中心时，会自动访问 CLI。虽然强烈建议不要这样做，但您可以使用 CLI 专家 命令访问 Linux 外壳程序。 **注释** 此功能弃用了为 管理中心启用和禁用 CLI 访问的版本 6.3。由于弃用此选项，虚拟 管理中心 不再显示 **系统** > **配置** > **控制台配置** 页面，该页面仍显示在物理 管理中心上。
限制SSH登录失败次数	6.3	任意	当用户通过SSH访问任何设备并连续三次尝试登录失败时，设备会终止 SSH 会话。

功能	最低 管理中心	最低 威胁防御	详情
能启用和禁用CLI访问权限 管理中心	6.3	任意	新增/修改的屏幕： 管理中心 Web 界面中对管理员可用的新复选框：在 **系统**（⚙）> **配置** > **控制台配置**页面上**启用 CLI 访问权限**。 • 选中：使用 SSH 登录 管理中心可访问 CLI。 • 取消选中：使用 SSH 登录 管理中心可访问 Linux 外壳。此为全新的 6.3 版本以及以往版本至 6.3 版本升级的默认状态。 支持的平台： 管理中心

第 II 部分

系统设置



第 3 章

系统配置

本章介绍如何在 Cisco Secure Firewall Management Center上配置系统配置设置。

系统配置的要求和前提条件

型号支持

管理中心

支持的域

全局

用户角色

管理员

管理 Cisco Secure Firewall Management Center 系统配置

系统配置可标识 管理中心 的基本设置。

过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 使用导航面板选择要更改的配置。

访问列表

您可以按 IP 地址和端口限制对 FMC 的访问。默认情况下，可为任何 IP 地址启用以下端口：

- 443 (HTTPS) 用于 Web 接口访问。
- 22 (SSH) 用于 CLI 访问。

也可以在端口 161 上添加轮询 SNMP 信息的访问权限。由于默认情况下会禁用 SNMP，因此必须先启用 SNMP，然后才能添加 SNMP 访问规则。有关详细信息，请参阅配置 SNMP 轮询，第 96 页。

注意 默认情况下，访问不受限制。要在更安全的环境中操作，请考虑为特定 IP 地址添加访问权限，然后删除默认的 **any** 选项。

配置访问列表

此访问列表不会控制外部数据库访问。请参阅启用对数据库的外部访问，第 59 页。

注意 对于您目前用来连接到 FMC 的 IP 地址，如果您删除了它的访问权限，而且无“`IP=any port=443`”这一条目，您将失去访问权限。

开始之前

默认情况下，访问列表包括 HTTPS 和 SSH 规则。要将 SNMP 规则添加到访问列表，必须先启用 SNMP。有关详细信息，请参阅配置 SNMP 轮询，第 96 页。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 （可选）如果要将 SNMP 规则添加到访问列表，请点击 **SNMP** 以配置 SNMP。默认情况下，SNMP 处于禁用状态；请参阅 配置 SNMP 轮询，第 96 页。

步骤 3 点击**访问列表 (Access List)**。

步骤 4 要添加对一个或多个 IP 地址的访问权限，请点击**添加规则 (Add Rules)**。

步骤 5 在 **IP 地址 (IP Address)** 字段中，输入 IP 地址或地址范围或 `any`。

步骤 6 选择 **SSH**、**HTTPS**、**SNMP** 或其组合，以指定要为这些 IP 地址启用哪些端口。

步骤 7 点击**添加 (Add)**。

步骤 8 点击**保存 (Save)**。

相关主题

Firepower 系统 IP 地址约定，第 26 页

访问控制首选项

在 **系统**（⚙）> **配置 (Configuration)** > **访问控制首选项 (Access Control Preferences)** 上配置访问控制首选项。

需要对规则更改添加注释

您可以通过允许（或要求）用户在保存时添加注释来跟踪对访问控制规则的更改。这使您可以快速评估为什么修改了部署中的关键策略。默认情况下，此功能处于禁用状态。

对象优化

将规则策略部署到防火墙设备时，可以配置管理中心以评估和优化在设备上创建关联网络对象组时在规则中使用的网络/主机策略对象。优化会合并相邻网络并删除冗余网络条目。这会减少运行时访问列表数据结构和配置大小，这对某些内存受限的防火墙设备有利。

例如，请考虑包含以下条目并在访问规则中使用的网络/主机对象：

```
192.168.1.0/24
192.168.1.23
10.1.1.0
10.1.1.1
10.1.1.2/31
```

启用优化后，在部署策略时，会生成生成的对象组配置：

```
object-group network test
description (Optimized by management center)
network-object 10.1.1.0 255.255.255.252
network-object 192.168.1.0 255.255.255.0
```

禁用优化时，组配置如下：

```
object-group network test
network-object 192.168.1.0 255.255.255.0
network-object 192.168.1.23 255.255.255.255
network-object 10.1.1.0 255.255.255.255
network-object 10.1.1.1 255.255.255.255
network-object 10.1.1.2 255.255.255.254
```

此优化不会更改网络/主机对象的定义，也不会创建新的网络/主机策略对象。如果网络对象组包含另一个网络、主机对象或对象组，则不会合并这些对象。相反，每个网络对象组都单独优化。此外，在部署期间，作为优化过程的一部分，仅修改网络对象组的内联值。

重要事项 在管理中心启用该功能（包括是否通过升级启用）后，在首次部署时在托管设备上进行优化。如果您有大量规则，系统可能需要几分钟到一个小时来评估您的策略并执行对象优化。在此期间，您可能还会发现设备上的CPU使用率更高。禁用该功能后，在第一次部署时会发生类似的情况。启用或禁用该功能后，建议您在影响最小的时候部署，比如维护窗口或流量较低的时段。

此功能受以下支持：

- 在版本 7.4.0 中，默认情况下为重新映像和升级的 管理中心启用此功能。要禁用它，请联系 思科 TAC。
- 在版本 7.4.1+ 中，此功能是可配置的。默认情况下，它会为重新映像的 管理中心启用，但在升级时会考虑您的当前设置。

审核日志

管理中心 以只读审核日志形式记录管理用户的活动。您可以使用多种方式查看审核日志数据：

- 使用 Web 接口： 审核和系统日志，第 389 页。

  审核日志显示在标准事件视图中，您可以依据审核视图中的任何项目查看、排序和过滤审核日志消息。您可以轻松删除和报告审核信息，也可以查看用户所做更改的详细报告。

- 将审核日志消息发送到系统日志： 将审核日志流传输到系统日志，第 43 页。。

- 将审核日志流传输到 HTTP 服务器： 将审核日志流传输到 HTTP 服务器，第 45 页。

将审核日志数据流式传输到外部系统日志或HTTP服务器，可以节省 管理中心 上的空间。 请注意，将审核信息发送到外部 URL 可能会影响系统性能。

或者，您可以确保审核日志流式传输通道安全，可以使用 TLS 证书启用 TLS 和相互身份验证；有关详细信息，请参阅 审核日志 ID证书，第 46 页。

流传输到多个系统日志服务器

您最多可以将审核日志数据传输到五个系统日志服务器。但是，如果为安全审核日志流启用了TLS，则只能将流传输到单个系统日志服务器。

将配置更改流传输到系统日志

您可以通过指定配置数据格式和主机，将配置更改作为审核日志数据的一部分传输到系统日志。管理中心支持备份和恢复审核配置日志。在高可用性的情况下，只有主用管理中心会将配置更改系统日志发送到外部系统日志服务器。日志文件在 HA 对之间同步，以便在故障转移或切换期间，新的主用管理中心将继续发送更改日志。如果 HA 对在裂脑模式下工作，则对中的两个管理中心都会将配置更改系统日志发送到外部服务器。

将审核日志流传输到系统日志

如果启用此功能，审核日志记录会按以下格式显示在系统日志中：

```
Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

其中，本地日期、时间和发起主机名称位于括号内的可选标记之前，发送设备名称在审核日志消息之前。

例如，如果为来自管理中心的审核日志消息指定 `FMC-AUDIT-LOG` 标记，则来自 管理中心 的审核日志消息示例可能如下所示：

```
Mar 01 14:45:24 localhost [FMC-AUDIT-LOG] Dev-MC7000: admin@10.1.1.2, 操作 > 监控，页面查看
```

如果你指定了严重性和设施，这些值不会出现在系统日志消息中；相反，它们会告诉接收系统日志消息的系统如何对它们进行归类。

开始之前

确保 管理中心 可以与系统日志服务器通信。保存配置时，系统使用 ICMP / ARP 和 TCP SYN 数据包验证系统日志服务器是否可访问。然后，默认情况下，系统使用端口 514 / UDP 传输审核日志。如果保护通道 （可选，请参阅 审核日志 ID证书，第 46 页），则必须为 TCP 手动配置端口 1470。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**审核日志 (Audit Log)**。

步骤 3 从**将审核日志发送到系统日志 (Send Audit Log to Syslog)** 下拉菜单中选择**已启用 (Enabled)**。

步骤 4 以下字段仅适用于发送到系统日志的审核日志：

选项	说明
发送配置更改	要在审核日志流中包含配置更改系统日志，请从下拉列表中选择相关选项： • JSON - 系统日志包括配置更改中的详细差异。 • API - 系统日志包括用于检索配置更改中详细差异的 API。 • 无 - 具有除配置更改详细信息以外的所有其他审核日志。
Host	将审核日志发送到的系统日志服务器的IP地址或完全限定名称。最多可以添加五个系统日志主机，以逗号分隔。 **注释** 仅当为审核服务器证书禁用TLS时，才能指定多个系统日志主机。
设施	创建消息的子系统。 选择 系统日志警报设施，第 535 页中所述的设施。例如，选择审核。
严重性	消息的严重性。 选择如 系统日志严重性级别，第 536 页描述的严重性。
标签	要包含在审核日志系统日志消息中的可选标记。 最佳实践：在此字段中输入值，以轻松区分审核日志消息与其他类似的系统日志消息，例如运行状况警报。 例如，如果要在发送到系统日志的所有审核日志记录之前标为 `FROMMC`，请在字段中输入 `FMC-AUDIT-LOG` 。

步骤 5 （可选）要测试系统日志服务器的IP地址是否有效，请点击 **测试系统日志服务器**。

系统发送以下数据包以验证系统日志服务器是否可访问：

1. ICMP 回应请求
2. 443 和 80 端口上的 TCP SYN

3. ICMP 时间戳查询
4. 随机端口上的 TCP SYN

注释　如果 管理中心 和系统日志服务器位于同一子网中，则使用 ARP 而不是 ICMP。

系统显示每个服务器的结果。

步骤 6 点击**保存 (Save)**。

将审核日志流传输到 HTTP 服务器

如果启用此功能，设备会按以下格式将审核日志记录发送到 HTTP 服务器：

Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action

其中，本地日期、时间和发起主机名称位于括号内的可选标记之前，发送设备名称在审核日志消息之前。

例如，如果指定标记为 FROMMC，则审核日志消息示例可能显示如下：

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring,
Page View
```

开始之前

确保设备能够与 HTTP 服务器通信。 或者，保护信道；请参阅 审核日志 ID证书，第 46 页。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**审核日志 (Audit Log)**。

步骤 3 或者，在**标记 (Tag)** 字段中，输入要与消息一起显示的标记名称。例如，如果要在所有审核日志记录之前添加 FROMMC，请在字段中输入 FROMMC。

步骤 4 从**将审核日志发送到 HTTP 服务器 (Send Audit Log to HTTP Server)** 下拉列表中选择**启用 (Enabled)**。

步骤 5 在**发送审核的 URL (URL to Post Audit)** 字段中，指定要用于发送审核信息的 URL。输入与将会监听下列 HTTP POST 变量的监听程序相对应的 URL：

- subsystem
- actor
- event_type
- message
- action_source_ip
- action_destination_ip

- `result`
- `time`
- `tag`（如果已定义；请参阅第 3 步）

注意 要允许加密的信息，请使用HTTPS URL。将审核信息发送到外部URL可能会影响系统性能。

步骤 6 点击**保存 (Save)**。

审核日志 ID证书

您可以使用传输层安全（TLS）证书保护 管理中心 和受信任审核日志服务器之间的通信。

客户端证书（需要）

生成证书签名请求（CSR），将其提交给证书颁发机构（CA）进行签名，然后将签名证书导入到管理中心 上。使用本地系统配置： 获取管理中心的已签署的审核日志客户端证书，第 47 页 和 将审核日志客户端证书导入管理中心，第 48 页。

服务器证书（可选）

为了提高安全性，我们建议您在管理中心和审核日志服务器之间进行相互身份验证。为此，请加载一个或多个证书吊销列表（CRL）。您无法将审核日志流传输到在这些CRL中列出的已吊销证书的服务器。

Cisco Secure Firewall 支持以可区别编码规则 (DER) 格式加密的 CRL。请注意，这些是系统用于验证管理中心 Web 界面的 HTTPS 客户端证书的相同 CRL。

使用本地系统配置： 需要有效的审核日志服务器证书，第 49 页。

安全地传输审核日志

如果将审核日志传输到可信的 HTTP 服务器或系统日志服务器，您可以使用传输层安全 (TLS) 证书保护 管理中心 和服务器之间的通道。您必须为要审核的每个设备生成唯一的客户端证书。

开始之前

请参阅审核日志 ID证书，第 46 页，了解所需的客户端和服务器证书信息。

过程

步骤 1 在 管理中心上获取并安装签名的客户端证书：

a) 获取管理中心的已签署的审核日志客户端证书，第 47 页：

根据系统信息和您提供的标识信息从 管理中心 生成证书签名请求 (CSR)。

将 CSR 提交至认可的可信证书颁发机构 (CA) 以请求签名的客户端证书。

如果 管理中心 和审核日志服务器之间需要相互身份验证，则签名客户端证书的 CA 必须与用于连接的服务器证书的签名 CA 相同。

b) 收到证书颁发机构签名的证书后，将其导入到 管理中心中。请参阅将审核日志客户端证书导入管理中心，第 48 页。

步骤 2 配置与服务器之间的通信通道，以使用传输层安全 (TLS) 协议并启用相互身份验证。

请参阅需要有效的审核日志服务器证书，第 49 页。

步骤 3 配置审核日志流，如果尚未执行此操作。

请参阅将审核日志流传输到系统日志，第 43 页或将审核日志流传输到 HTTP 服务器，第 45 页。

获取管理中心的已签署的审核日志客户端证书

重要事项 **审核日志证书**页在高可用性设置的备用 管理中心中不可用。无法从备用 管理中心执行此任务。

系统生成 Base-64 编码的 PEM 格式的证书请求密钥。

开始之前

记住以下几点：

- 为确保安全，请使用全球公认且可信的证书颁发机构 (CA) 签署您的证书。
- 如果您将需要在设备和审核日志服务器之间进行相互身份验证，则同一证书颁发机构必须同时签署客户端证书和服务器证书。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**审核日志证书 (Audit Log Certificate)**。

步骤 3 点击 **Generate New CSR**。

步骤 4 在**国家/地区名称（两字母代码）(Country Name [two-letter code])** 字段中输入国家/地区代码。

步骤 5 在**省/自治区/直辖市 (State or Province)** 字段中输入省/自治区/直辖市的邮编缩写。

步骤 6 输入**地区或城市 (Locality or City)**。

步骤 7 在**组织 (Organization)** 中输入组织名称。

步骤 8 输入**组织单位 (部门)** 名称。

步骤 9 在**公用名 (Common Name)** 字段中输入要为其请求证书的服务器的完全限定域名。

注释 如果公用名和 DNS 主机名不匹配，则审核日志流将失败。

步骤 10 点击**生成 (Generate)**。

步骤 11 使用文本编辑器打开新的空白文件。

步骤 12 复制证书请求中的整个文本块（包括 `BEGIN CERTIFICATE REQUEST` 和 `END CERTIFICATE REQUEST` 行），然后将其粘贴到一个空白文本文件中。

步骤 13 将该文件另存为 *`clientname`*`.csr`，其中，*`clientname`* 是计划使用证书的设备的名称。

步骤 14 点击 **Close**。

下一步做什么

- 将证书签署请求提交到您使用此程序的“开始之前”部分中的指南选择的证书颁发机构。
- 在收到已签署的证书后，请将其导入到设备；请参阅将审核日志客户端证书导入管理中心，第 48 页。

将审核日志客户端证书导入管理中心

在 管理中心 高可用性设置中， 必须 使用主用对等体。

开始之前

- 获取管理中心的已签署的审核日志客户端证书，第 47 页。
- 请确保您正在导入的是正确 管理中心的已签名证书。
- 如果生成证书的签名机构要求您信任某个中间CA，请准备好提供必要的证书链（或证书路径）。签署客户端证书的 CA 与签署证书链中任何中间证书的 CA 必须相同。

过程

步骤 1 在管理中心上，选择**系统**（⚙）>**配置**。

步骤 2 点击**审核日志证书 (Audit Log Certificate)**。

步骤 3 点击**导入审核客户端证书 (Import Audit Client Certificate)**。

步骤 4 在文本编辑器中打开客户端证书，复制整个文本块，包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行。将此文本粘贴到**客户端证书 (Client Certificate)** 字段。

步骤 5 要上传私钥，请打开私钥文件并复制整个文本块，包括 `BEGIN RSA PRIVATE KEY` 和 `END RSA PRIVATE KEY` 行。将此文本粘贴到**私钥 (Private Key)** 字段。

步骤 6 打开任何所需的中间证书，复制整个文本块，然后将其复制到**证书链 (Certificate Chain)** 字段中。

步骤 7 点击**保存 (Save)**。

需要有效的审核日志服务器证书

系统支持使用可区别编码规则 (DER) 格式的导入 CRL 来验证审核日志服务器证书。

注释 如果选择使用 CRL 验证证书，系统将使用相同的 CRL 来验证审核日志服务器证书和用于保护设备和 Web 浏览器之间的 HTTP 连接的证书。

重要事项 您无法在高可用性对中的备用 管理中心 上执行此程序。

开始之前

- 了解需要相互身份验证自己使用证书吊销列表 (CRL) 的后果，确保证书仍然有效。请参阅审核日志 ID证书，第 46 页。
- 按照安全地传输审核日志，第46页中的步骤以及该程序中引用的主题获取并导入客户端证书。

过程

步骤 1 在管理中心上，选择**系统**（⚙）>**配置**。

步骤 2 点击**审核日志证书 (Audit Log Certificate)**。

步骤 3 要使用传输层安全将审核日志安全地流式传输到外部服务器，请选择 **启用 TLS**。

启用 TLS 时，系统日志客户端 (管理中心) 验证从服务器接收的证书。仅当服务器证书验证成功时，客户端和服务器之间的连接才会成功。对于此验证过程，必须满足以下条件：

- 配置系统日志服务器以将证书发送到客户端。
- 向客户端添加（导入）CA 证书以验证服务器证书：
  - 您必须在导入客户端证书期间导入 CA 证书。
  - 如果颁发 CA 是从属 CA，则必须先添加颁发 CA，然后再从从属 CA（根 CA）添加签名 CA，依此类推。

步骤 4 如果您不希望客户端根据服务器对自身进行身份验证，但在证书由同一 CA 颁发时接受服务器证书（不推荐）：

a) 取消选择**启用相互身份验证**。

重要事项 确保服务器配置为信任客户端，而不验证任何客户端证书。

b) 点击**保存**并跳过此过程的其余部分。

步骤 5 （可选）要通过审核日志服务器启用客户端证书验证，请选择 **启用相互身份验证**。

重要事项 仅当启用 TLS 时，**启用相互身份验证** 选项才适用。

启用相互身份验证后，系统日志客户端(管理中心)会将客户端证书发送到系统日志服务器进行验证。客户端使用与系统日志服务器的服务器证书签名的 CA 相同的 CA 证书。仅当客户端证书验证成功时，连接才会成功。对于此验证过程，必须满足以下条件：

- 配置系统日志服务器以验证从客户端收到的证书。
- 添加要发送到系统日志服务器的客户端证书。该证书必须由签署系统日志服务器的服务器证书的 CA 签署。

注释 要使用相互身份验证将审核日志流式传输到系统日志服务器，请对私钥使用 PKCS#8 格式，而不是 PKCS#1 格式。使用以下命令行将 PKCS#1 密钥转换为 PKCS#8 格式：

```
openssl pkcs8 -topk8 -inform PEM -outform PEM
-nocrypt -in PKCS1 key file name -out PKCS8 key filename
```

步骤 6 （可选）要自动识别不再是有效的服务器证书，请执行以下步骤：

a) 选择**启用 CRL 提取**。

重要事项 仅当您选中 **启用相互身份验证** 复选框时，才会显示此选项。但是，仅当启用 TLS 选项时，**启用 CRL 获取** 选项才适用。CRL 用于服务器证书验证，不依赖于用于启用客户端证书验证的相互身份验证。

启用获取 CRL 会为客户端创建一个计划任务，以便定期更新（下载）CRL 或 CRL。CRL 用于服务器证书验证，其中，如果来自 CA 的 CRL 指定要验证的服务器证书已被 CA 吊销，则验证会失败。

b) 输入现有 CRL 文件的有效 URL 并点击**添加 CRL (Add CRL)**。

重复以上步骤以添加 25 个 CRL。

c) 点击**刷新 CRL (Refresh CRL)** 以从指定的 URL 加载当前 CRL。

步骤 7 验证您是否拥有由创建客户端证书的同一证书颁发机构生成的有效服务器证书。

步骤 8 点击**保存 (Save)**。

下一步做什么

（可选）设置 CRL 更新的频率。请参阅配置证书撤销列表下载，第 471 页。

查看管理中心上的审核日志客户端证书

只能查看您登录的设备的审核日志客户端证书。在管理中心高可用性对中，只能在活动对等体上查看证书。

过程

步骤 1 选择系统（⚙）> 配置。

步骤 2 点击审核日志证书 (Audit Log Certificate)。

更改调节

要监控用户进行的更改并确保它们符合您的组织的首选标准，可以将系统配置为通过邮件发送有关过去24小时内进行的更改的详细报告。每当用户保存对系统的配置更改时，就会生成更改快照。更改调节报告将汇总这些快照的信息，以提供最新系统更改的清晰摘要。

以下示例图表显示更改调节报告示例的“用户”部分，并且列出每个配置更改前和更改后的值。如果用户多次更改同一配置，报告会按时间顺序列出每次不同更改的摘要，最近的更改最先列出。

可以查看过去 24 小时内所做的更改。

配置更改调节

开始之前

- 配置邮件服务器，以接收过去 24 小时对系统进行的更改的报告邮件；有关详细信息，请参阅配置邮件中继主机和通知地址，第 58 页。

过程

步骤 1 选择系统（⚙）> 配置。

步骤 2 点击更改调节。

步骤 3 选中启用复选框。

步骤 4 从运行时间 (Time to Run) 下拉列表中选择您希望系统每天发出更改调节报告的具体时间。

步骤 5 在邮件收件人 (Email to) 字段中输入邮箱地址。

提示 添加邮箱地址后，点击重新发送上一报告 (Resend Last Report) 以向收件人发送另一个最新更改调节报告的副本。

步骤 6 如果要包含策略更改，请选中包含策略配置 (Include Policy Configuration) 复选框。

步骤 7 如果要包含过去24小时进行的所有更改，请选中显示完整更改历史记录 (Show Full Change History) 复选框。

步骤 8 点击保存 (Save)。

相关主题

使用审核日志检查更改，第 394 页

更改调节选项

包括策略配置 (Include Policy Configuration) 选项用于控制系统是否在更改调节报告中包括策略更改记录。这包括对访问控制策略、入侵策略、系统策略、运行状况策略和网络发现策略的更改。如果未选择该选项，报告将不会显示对任何策略的更改。此选项仅适用于 管理中心。

显示完整更改历史记录 (Show Full Change History) 选项用于控制系统是否在更改调节报告中包括过去24小时内发生的所有更改的记录。如果未选择该选项，报告仅包括每个类别的更改的整合视图。

注释 更改调节报告不包括对 威胁防御 接口和路由设置的更改。

变更管理

如果您的组织需要实施更加正式的配置更改流程，包括在部署更改之前进行审核跟踪和正式审批，则可以启用“更改管理”。

启用“变更管理”(Change Management) 时，系统会将 **工单**（） 快捷方式添加到菜单栏，并将**变更管理工作流程 (Change Management Workflow)** 添加到 **系统**（） 菜单。用户可以使用这些方法来管理故障单。

有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的“变更管理”一章。

在 **系统**（） > **配置** 页面上，您可以配置以下设置。点击**保存 (Save)** 保存更改。

- **启用更改管理 (Enable Change Management)** - 打开故障单和更改管理工作流程。启用后，您必须批准或放弃所有故障单才能关闭更改管理。

  要禁用该功能，请取消选择该选项。要禁用变更管理，必须批准或丢弃所有故障单。无法禁用变更管理，如果任何故障单处于“进行中”、“暂时搁置”、“已拒绝”或“待审批”状态。

- **需要审批的数量**-要批准和部署故障单，必须有多少管理员批准更改。默认值为 1，但每个故障单最多可以有 5 个审批人。用户可以在创建故障单时覆盖此编号。

注释 当更改管理启用并在使用时，无法更改审批人数量，如果至少有一个故障单处于“进行中”、“暂时搁置”、“已拒绝”或“待审批”状态。要更改所需的审批人数量，必须批准或丢弃所有故障单。

- **故障单清除持续时间**-保留已批准的故障单的天数，范围为 1-100 天。默认值为 5 天。

- **邮件通知**（可选）- 输入 **审批者列表**的 **回复地址** 和组邮件地址。您还必须配置邮件通知系统设置，邮件才能正常工作。

  对于 云交付的防火墙管理中心，不会显示对地址的回复。相反，请在邮件通知系统设置中配置此地址。

备注

有几个系统进程会阻止您启用/禁用更改管理。如果正在执行以下任何操作，则需要等待它们完成后才能更改这些设置：备份/恢复；导入/导出；域移动；升级； Flexconfig 迁移； 设备注册；高可用性注册、创建、中断或切换；集群创建、注册、中断、编辑、添加或删除节点； EPM 中断或加入。

更改这些设置时，无法锁定访问控制策略。如果策略已锁定，则必须等待锁定被释放，然后才能启用/禁用此功能。

DNS 缓存

可以将系统配置为在事件视图页面上自动解析 IP 地址。还可以为设备执行的 DNS 缓存配置基本属性。配置 DNS 缓存让您可以识别之前解析过的 IP 地址，而无需执行额外查找。这样，启用 IP 地址解析后，可以减少网络上的流量并加快事件页面的显示速度。

配置 DNS 缓存属性

DNS 解析缓存是针对整个系统的设置，它允许对以前解析过的 DNS 查找进行缓存。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **DNS 缓存 (DNS Cache)**。

步骤 3 从 **DNS 解析缓存 (DNS Resolution Caching)** 下拉列表中，选择以下选项之一：

- **已启用 (Enabled)** - 启用缓存。
- **已禁用 (Disabled)** - 禁用缓存。

步骤 4 在 **DNS 缓存超时（以分钟为单位）(DNS Cache Timeout [in minutes])** 字段中，输入 DNS 条目在因无活动而被删除前在内存中缓存的分钟数。

默认设置为 300 分钟（5 小时）。

步骤 5 点击**保存 (Save)**。

相关主题

配置事件视图设置 ， 第 193 页

控制面板

控制面板通过使用构件提供当前系统状态的概要视图；构件是一些独立的小组件，可提供有关系统不同方面的信息。系统配置了数个预定义控制面板构件。

您可以配置 管理中心，以便在控制面板上启用“自定义分析”构件。

相关主题

关于控制面板，第 321 页

启用控制面板的自定义分析构件

使用“自定义分析”(Custom Analysis) 控制面板构件，根据灵活的用户可配置查询创建事件的直观表示。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**控制面板 (Dashboard)**。

步骤 3 选中**启用自定义分析构件 (Enable Custom Analysis Widgets)** 复选框以允许用户将“自定义分析”(Custom Analysis) 构件添加到控制面板。

步骤 4 点击**保存 (Save)**。

相关主题

关于控制面板，第 321 页

数据库

为管理磁盘空间，管理中心定期删除设备数据库中的入侵事件、发现事件、审核记录、安全情报数据或 URL 过滤数据。对于每种事件类型，可以指定 管理中心 修剪后保留的记录数；从不依赖包含的任何类型记录数超过为该类型配置的保留限制的事件数据库。为提高性能，应将事件数量限制设置为您通常处理的事件数量。您可以选择在发生修剪时接收邮件通知。对于某些事件类型，可以禁用存储功能。

要手动删除单个事件，请使用事件查看器。（请注意，在版本 6.6.0+ 中，不能以这种方式手动删除连接或安全情报事件。）您还可以手动清除数据库；请参阅 数据清除和存储，第 495 页。

配置数据库事件限制

开始之前

- 如果希望在从 管理中心数据库中删除事件时收到邮件通知，则必须配置邮件服务器，请参阅配置邮件中继主机和通知地址，第 58 页。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 选择**数据库 (Database)**。

步骤 3 对于每个数据库，请输入要存储的记录的数量。

有关每个数据库可维护的记录的数量，请参阅数据库事件限制，第 55 页。

步骤 4 或者，在**数据修剪通知地址 (Data Pruning Notification Address)** 字段中，输入要接收修剪通知的邮箱地址。

步骤 5 点击**保存 (Save)**。

数据库事件限制

下表列出每个 管理中心可存储的每种事件类型记录的最小和最大数量。

表 *1:* 数据库事件限制

事件类型	上限	下限
入侵事件	1000 万（管理中心虚拟） 3000 万 (管理中心1000, 管理中心1600) 6000 万 (管理中心2500, 管理中心2600, FMCv 300) 3 亿 (管理中心4500, 管理中心4600) 4 亿 (管理中心4700)	10,000
发现事件	1000 万 (管理中心 虚拟) 2000 万 (管理中心2500, 管理中心2600, 管理中心4500, 管理中心4600, 管理中心4700, FMCv 300)	0（禁用存储）

事件类型	上限	下限
连接事件 安全情报事件	5000 万 (管理中心 虚拟) 1 亿 (管理中心1000, 管理中心1600) 3 亿 (管理中心2500, 管理中心2600, FMCv 300) 10 亿 (管理中心4500, 管理中心4600, 管理中心4700) 连接事件和安全情报事件共用数量限制。配置的最大数量总和不能超过此限制。	0（禁用存储） 如果将**最大连接事件 (Maximum Connection Events)** 值设置为零，则未与安全情报、入侵、文件和恶意软件事件关联的连接事件不会存储在 管理中心 上。 **注意** 将 **最大连接事件** 设置为零会立即清除除安全情报事件以外的现有连接事件。 有关此设置对最大流量的影响，请参阅下文。 这些设置不会影响连接摘要。
连接摘要（汇聚连接事件）	5000 万 (管理中心 虚拟) 1 亿 (管理中心1000, 管理中心1600) 3 亿 (管理中心2500, 管理中心2600, FMCv 300) 10 亿 (管理中心4500, 管理中心4600, 管理中心4700)	0（禁用存储）
关联事件和合规 allow 列表事件	100 万 (管理中心 Virtual) 200 万 (管理中心2500, 管理中心2600, 管理中心4500, 管理中心4600, 管理中心4700, FMCv 300)	一个
恶意软件事件	1000 万 (管理中心 Virtual) 200 万 (管理中心2500, 管理中心2600, 管理中心4500, 管理中心4600, 管理中心4700, FMCv 300)	10,000
文件事件	1000 万 (管理中心 虚拟) 200 万 (管理中心2500, 管理中心2600, 管理中心4500, 管理中心4600, 管理中心4700, FMCv 300)	0（禁用存储）
运行状况事件	100 万	0（禁用存储）
审核记录	100,000	一个
补救状态事件	1000 万	一个

事件类型	上限	下限
允许列表违例历史记录	30 天的违例历史记录	1 天的历史记录
用户活动（用户事件）	1000 万	一个
用户登录（用户历史记录）	1000 万	一个
入侵规则更新导入日志记录	100 万	一个
VPN 故障排除数据库	1000 万	0（禁用存储）

最大流速

管理中心 硬件型号的 **最大流量 (Maximum flow rate)**（每秒流量）值在 https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html?cachemode=refresh 的 管理中心 数据表的 **平台规格 (Platform Specifications)** 部分中指定

如果将平台设置中的**最大连接事件数**值设置为零，则不与安全情报、入侵、文件和恶意软件事件关联的连接事件不会计入 管理中心 硬件的最大流量。

此字段中的任何非零值都会导致将所有连接事件计入最大流量。

此页面上的其他事件类型不计入最大流量。

电子邮件通知

如果要执行以下操作，请配置邮件主机：

- 通过邮件发送基于事件的报告
- 通过邮件发送有关预定任务的报告
- 通过邮件发送更改调节报告
- 通过邮件发送数据删除通知
- 将邮件用于发现事件、影响标志、关联事件警报，入侵事件警报和运行状况事件警报.

配置邮件通知时，可以为系统与邮件中继主机之间的通信选择加密方法，并可根据需要为邮件服务器提供身份验证凭证。配置后，可以测试连接。

配置邮件中继主机和通知地址

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Email Notification**。

步骤 3 在**邮件中继主机 (Mail Relay Host)** 字段中，输入要使用的邮件服务器的主机名或 IP 地址。输入的邮件主机**必须**允许从设备进行访问。

步骤 4 在**端口号 (Port Number)** 字段，请输入邮件服务器上使用的端口号。

典型的端口包括：

- 25，使用加密时
- 465，使用 SSLv3 时
- 587，使用 TLS 时

步骤 5 在**加密方法 (Encryption Method)** 中选择一种加密方法。

- **TLS** - 使用传输层安全加密通信。
- **SSLv3** - 使用安全套接字层加密通信。
- **无 (None)** - 允许未加密的通信。

注释 设备和邮件服务器之间的加密通信不要求进行证书验证。

步骤 6 在**源地址 (From Address)** 字段，输入要将其用作设备发送消息的源邮箱地址的有效邮箱地址。

步骤 7 或者，要在连接到邮件服务器时提供用户名和密码，请选择**使用身份验证 (Use Authentication)**。在**用户名 (Username)** 字段中输入用户名。在**密码 (Password)** 字段中输入密码。

步骤 8 要使用已配置的邮件服务器发送测试邮件，请点击**测试邮件服务器设置 (Test Mail Server Settings)**。

系统会在按钮旁边显示一条消息，以指明测试是否成功。

步骤 9 点击**保存 (Save)**。

外部数据库访问

您可以将 管理中心配置为允许第三方客户端对其数据库进行只读访问。这样，您可以通过以下任何方式使用 SQL 来查询数据库：

- 行业标准报告工具（例如，Actuate BIRT、JasperSoft iReport 或 Crystal Reports）
- 其他任何支持 JDBC SSL 连接的报告应用（包括自定义应用）

- 思科提供的命令行 Java 应用，名为 RunQuery，可以交互方式运行或用于获取单一查询的以逗号分隔的结果

使用 管理中心的系统配置启用数据库访问，并创建允许选定主机查询数据库的访问列表。请注意，该访问列表不用于控制设备访问。

您也可以下载包含以下工具的软件包：

- RunQuery（这是思科提供的数据库查询工具）
- InstallCert 工具，可用于从要访问的 管理中心 检索和接受 SSL 证书
- 连接到数据库时必须使用的 JDBC 驱动程序

有关使用下载包中的工具来配置数据库访问的信息，请参阅《《*Firepower* 系统数据库访问指南》》。

启用对数据库的外部访问

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**外部数据库访问 (External Database Access)**。

步骤 3 选中**允许外部数据库访问 (Allow External Database Access)** 复选框。

步骤 4 在**服务器主机名 (Server Hostname)** 字段中输入相应的值。根据第三方应用要求，此值可以是 管理中心的完全限定域名 (FQDN)、IPv4 地址或 IPv6 地址。

注释 在管理中心高可用性设置中，仅输入活动对等体详细信息。我们不建议输入备用对等体的详细信息。

步骤 5 点击 **Client JDBC Driver** 旁边的 **Download** 并按照浏览器提示下载 `client.zip` 软件包。

步骤 6 要为一个或多个IP地址添加数据库访问权限，请点击**添加主机**。此时，**访问列表**字段中将会显示**IP地址**字段。

步骤 7 在 **IP 地址 (IP Address)** 字段中，输入 IP 地址或地址范围或 `any`。

步骤 8 点击**添加 (Add)**。

步骤 9 点击**保存 (Save)**。

提示 如果要恢复为上次保存的数据库设置，请点击**刷新 (Refresh)**。

相关主题

Firepower 系统 IP 地址约定 ，第 26 页

HTTPS 证书

借助安全套接字层(SSL)证书，管理中心可以在系统和Web浏览器之间建立加密通道。所有Firepower设备都随附默认证书，但其不是由任何全球知名的证书颁发机构(CA)所信任的CA生成。因此，请考虑将其替换为由全球知名或内部信任的CA签名的自定义证书。

注意 管理中心支持4096位HTTPS证书。如果管理中心使用的证书是通过大于4096位的公共服务器密钥生成的，则您将无法登录管理中心Web界面。如果出现此情况，请联系思科TAC。

注释 管理中心 REST API不支持HTTPS证书。

默认 HTTPS 服务器证书

如果使用随设备一起提供的默认服务器证书，请不要将系统配置为需要有效的HTTPS客户端证书以访问Web界面，因为默认服务器证书并非由签署客户端证书的CA签署。

默认服务器证书的生命周期取决于证书的生成时间。要查看默认服务器证书到期日期，请选择**系统**（⚙）>**配置**>**HTTPS证书**。

请注意，某些Firepower软件升级可以自动续订证书。有关详细信息，请参阅Firepower热补丁发行说明。

在管理中心上，您可以在**系统**（⚙）>**配置**>**HTTPS证书**页面上续订默认证书。

自定义 HTTPS 服务器证书

您可以使用管理中心Web界面根据系统信息和您提供的识别信息生成服务器证书请求。如果安装有受浏览器信任的内部证书颁发机构(CA)，则可以使用该请求对证书进行签署。您还可以将生成的请求发送到证书颁发机构以请求服务器证书。获得证书颁发机构(CA)的签名证书后，您可以导入该证书。

HTTPS 服务器证书要求

使用HTTPS证书保护Web浏览器和Firepower设备Web界面之间的连接时，必须使用符合互联网X.509公钥基础设施证书和证书撤销列表（CRL）配置文件（RFC 5280）的证书。当您将服务器证书导入设备时，如果该证书不符合该标准的版本3（X.509 v3），则系统会拒绝该证书。

在导入HTTPS服务器证书之前，请确保其包含以下字段：

证书字段	说明
版本	编码的证书的版本。使用版本 3。请参阅 RFC 5280，第 4.1.2.1 节。
序列号	由颁发 CA 分配给证书的正整数。颁发者和序列号唯一标识证书。请参阅 RFC 5280，第 4.1.2.2 节。
签名	CA 用于签署证书的算法的标识符。必须与 signatureAlgorithm 字段匹配。请参阅 RFC 5280，第 4.1.2.3 节。
签发实体	标明签署和签发证书的实体。请参阅 RFC 5280，第 4.1.2.4 节。
有效性	CA 保证其将维护有关证书状态的信息的间隔。请参阅 RFC 5280，第 4.1.2.5 节。
使用者	标识与存储在使用者公钥字段中的公钥关联的实体；必须是X.500可分辨名称（DN）。请参阅 RFC 5280，第4.1.2.6 节。
使用者可选名称	证书保护的域名和 IP 地址。使用者可选名称在 RFC 5280，第 4.2.1.6 节中定义。 如果证书用于多个域或IP地址，我们建议您使用此字段。
对象公钥信息	公钥及其算法的标识符。请参阅 RFC 5280，第 4.1.2.7 节。
授权密钥标识符	提供识别与用于签署证书的私钥对应的公钥的方法。请参阅 RFC 5280，第 4.2.1.1 节。
主体密钥标识符	提供一种识别包含特定公钥的证书的方法。请参阅 RFC 5280，第 4.2.1.2 节。
密钥使用	定义证书中包含的密钥的用途。请参阅 RFC 5280，第 4.2.1.3 节。
基本限制	确定证书主体是否为 CA，以及包括此证书的最大验证认证路径深度。请参阅 RFC 5280，第 4.2.1.9 节。对于 Firepower 设备中使用的服务器证书，请使用 关键 CA：FALSE。

证书字段	说明
扩展密钥使用扩展	表示除“密钥使用”扩展中指示的基本用途之外或替代其用途的已认证公钥的一个或多个用途。请参阅 RFC 5280，第 4.2.1.12 节。请确保导入可用作服务器证书的证书。
signatureAlgorithm	CA 用于对证书签名的算法的标识符。必须与签名字段匹配。请参阅 RFC 5280，第 4.1.1.2 节。
signatureValue	数字签名。请参阅 RFC 5280，第 4.1.1.3 节。

HTTPS 客户端证书

您可以使用客户端浏览器证书检查功能来限制对 Firepower 系统 Web 服务器的访问。启用用户证书时，网络服务器会检查用户的浏览器客户端是否选择了有效的用户证书。此用户证书必须由生成服务器证书的同一个可信证书颁发机构生成。浏览器无法在以下任何情况下加载 Web 界面：

- 用户在浏览器中选择的证书无效。
- 用户在浏览器中选择的证书不是由签署服务器证书的证书颁发机构生成。
- 用户在浏览器中选择的证书不是由设备上的证书链中的证书颁发机构生成。

要验证客户端浏览器证书，请将系统配置为使用在线证书状态协议 (OCSP) 或加载一个或多个证书撤销列表 (CRL)。使用 OCSP，当 Web 服务器接收到连接请求时，它会与证书颁发机构进行通信，以在建立连接之前确认客户端证书的有效性。如果将服务器配置为加载一个或多个 CRL，则 Web 服务器会将该客户端证书与 CRL 中所列的客户端证书进行比较。如果用户选择在 CRL 中列为已撤销证书的证书，则浏览器无法加载 Web 界面。

注释 如果选择使用 CRL 验证证书，则系统会使用相同的 CRL 验证客户端浏览器证书和审核日志服务器证书。

查看当前 HTTPS 服务器证书

过程

步骤 1 选择系统（⚙）> 配置。

步骤 2 点击 **HTTPS Certificate**。

生成 HTTPS 服务器证书签名请求

如果安装不是由全球知名或内部受信任的 CA 签名的证书，则当他们尝试连接 Web 界面时，浏览器会显示安全警告。

证书签名请求 (CSR) 对于生成该证书的设备是唯一的。您无法从单个设备为多个设备生成 CSR。虽然所有字段都是可选的，但我们建议输入以下值：CN、组织、组织单位、城市/区域、省/自治区、国家/地区和使用者可选名称。

为证书请求生成的密钥采用 Base-64 编码的 PEM 格式。

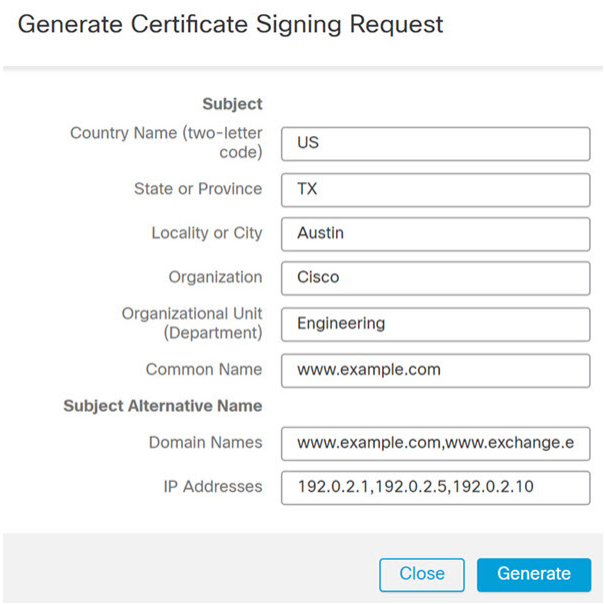
过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 点击 **HTTPS Certificate**。

步骤 3 点击 **Generate New CSR**。

下图显示了一个示例。



步骤 4 在**国家/地区名称（两字母代码）(Country Name [two-letter code])** 字段中输入国家/地区代码。

步骤 5 在**省/自治区/直辖市 (State or Province)** 字段中输入省/自治区/直辖市的邮编缩写。

步骤 6 输入**地区或城市 (Locality or City)**。

步骤 7 在**组织 (Organization)** 中输入组织名称。

步骤 8 输入**组织单位 (部门)** 名称。

步骤 9 在**公用名 (Common Name)** 字段中输入要为其请求证书的服务器的完全限定域名。

注释 在**公用名 (Common Name)** 字段中输入与在证书中所显示完全相同的服务器的完全限定域名。如果公用名与 DNS 主机名不匹配，则在连接到设备时会接收到警告。

步骤 10 要请求用于保护多个域名或 IP 地址的证书，请在“使用者可选名称”部分中输入以下信息：

a) **域名**：输入由使用者可选名称保护的完全限定域和子域（如果有）。

b) **IP 地址**：输入由使用者可选名称保护的 IP 地址。

步骤 11 点击**生成 (Generate)**。

步骤 12 打开一个文本编辑器。

步骤 13 复制证书请求中的整个文本块（包括 `BEGIN CERTIFICATE REQUEST` 和 `END CERTIFICATE REQUEST` 行），然后将其粘贴到一个空白文本文件中。

步骤 14 将该文件另存为 *`servername`*`.csr`，其中，*servername* 是计划使用证书的服务器的名称。

步骤 15 点击 **Close**。

下一步做什么

- 将证书请求提交到证书颁发机构。
- 收到签名证书后，请将其导入 管理中心；请参阅 导入 HTTPS 服务器证书，第 64 页。

导入 HTTPS 服务器证书

如果生成证书的签发机构要求您信任某个中间CA，那么您还必须提供一个证书链（即证书路径）。

如果请求了客户端证书，则当服务器证书不符合以下任一条件时，通过 Web 界面访问设备将会失败：

- 证书由签发客户端证书的同一 CA 签名。
- 证书由签发证书链中某个中间证书的 CA 签名。

注意 管理中心 支持 4096 位 HTTPS 证书。如果 管理中心 使用的证书是由大于 4096 位的公共服务器密钥生成的，则您将无法登录 Cisco Secure Firewall Management Center Web 界面。有关将 HTTPS 证书更新到版本 6.0.0 的详细信息，请参阅*Firepower* 系统发行说明，版本 *6.0*中的“将管理中心 HTTPS 证书更新到版本 6.0”。如果要生成或导入 HTTPS 证书且无法登录 管理中心 Web 界面，请联系支持部门。

开始之前

- 生成证书签名请求；请参阅生成 HTTPS 服务器证书签名请求，第 63 页。
- 将 CSR 文件上传至您想要向其请求证书的证书颁发机构，或者使用 CSR 来创建自签证书。
- 确认证书符合 HTTPS 服务器证书要求，第 60 页中所述的要求。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **HTTPS Certificate**。

步骤 3 点击**导入 HTTPS 证书**。

注释　无法导入加密的 HTTPS 证书。

步骤 4 在文本编辑器中打开服务器证书，复制整个文本块（包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行）。将此文本粘贴到**服务器证书 (Server Certificate)** 字段中。

步骤 5 是否需要提供**私钥**取决于您生成证书签名请求的方式：

- 如果使用 Cisco Secure Firewall Management Center Web 界面生成证书签名请求（如生成 HTTPS 服务器证书签名请求，第 63 页中所述），则系统已有私有密钥，您无需在此输入。
- 如果通过其他方式生成证书签名请求，则必须在此提供私有密钥。打开私有密钥文件并复制整个文本块，包括 `BEGIN RSA PRIVATE KEY` 和 `END RSA PRIVATE KEY` 行。将此文本粘贴到**私钥 (Private Key)** 字段。

步骤 6 打开任何所需的中间证书，复制整个文本块，然后将其复制到**证书链 (Certificate Chain)** 字段中。如果收到根证书，请将其粘贴到此处。如果收到中间证书，请将其粘贴到根证书下方。在两种案例下，复制整个文本块，包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行。

步骤 7 点击**保存 (Save)**。

需要有效的 HTTPS 客户端证书

使用此程序可要求连接到 管理中心 Web 界面的用户提供用户证书。系统支持使用 OCSP 或以隐私增强电子邮件 (PEM) 格式导入的 CRL 验证 HTTPS 客户端证书。

如果选择使用 CRL，要确保撤销证书列表是最新的，您可以创建计划任务来更新 CRL。系统显示 CRL 的最新刷新。

注释　要在启用客户端证书后访问 Web 界面，浏览器中**必须**有一个有效客户端证书（或您的阅读器中插入的 CAC）。

开始之前

- 导入由签署用于连接的客户端证书的同一证书颁发机构签署的服务器证书；请参阅导入 HTTPS 服务器证书，第 64 页。
- 必要时导入服务器证书链；请参阅导入 HTTPS 服务器证书，第 64 页。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **HTTPS Certificate**。

步骤 3 选择**启用客户端证书 (Enable Client Certificates)**。如有提示，请从下拉列表中选择相应的证书。

步骤 4 您会看到三个选项：

- 要用一个或多个 CRL 验证客户端证书，请选择**启用 CRL 获取 (Enable Fetching of CRL)** 并继续执行步骤 5。
- 要使用 OCSP 验证客户端证书，请选择**启用 OCSP** 并跳转至步骤 7。
- 要在不检查撤销的情况下接受客户端证书，请跳转至步骤 8。

步骤 5 输入现有 CRL 文件的有效 URL 并点击**添加 CRL (Add CRL)**。重复以上步骤以添加 25 个 CRL。

步骤 6 点击**刷新 CRL (Refresh CRL)** 以从指定的 URL 加载当前 CRL。

注释 启用 CRL 获取功能可创建定期更新 CRL 的计划任务。编辑任务以设置更新的频率。

步骤 7 验证客户端证书是否由加载到设备上的证书颁发机构签署，以及服务器证书是否由加载到浏览器证书存储区中的证书颁发机构签署。（这些证书的证书颁发机构相同。）

注意 保存已启用客户端证书的配置时，如果在您的浏览器证书存储区中无有效客户端证书，则会禁用对设备的所有 Web 服务器访问。请在保存设置之前确保已安装有效客户端证书。

步骤 8 点击**保存 (Save)**。

相关主题

配置证书撤销列表下载，第 471 页

续订默认 HTTPS 服务器证书

只能查看您登录的设备的服务器证书。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **HTTPS Certificate**。

仅当系统配置为使用默认 HTTPS 服务器证书时，才会显示此按钮。

步骤 3 点击 **续约 HTTPS 证书**。（仅当系统配置为使用默认 HTTPS 服务器证书时，此选项才会显示在证书信息下方的显示屏上。）

步骤 4 （可选）在**续订 HTTPS 证书**对话框中，选择**生成新密钥**以生成证书的新密钥。

步骤 5 在续订 **HTTPS 证书**对话框中，点击**保存**。

下一步做什么

您可以通过检查 **HTTPS 证书**页面上显示的证书有效期是否已更新，来确认证书是否已续订。

信息

Web 界面的 **系统 > 配置** 页面包含下表中列出的信息。除非另有说明，否则所有字段都为只读。

注释 另请参阅 **帮助 > 关于** 页面，其中包含类似但略有不同的信息。

字段	说明
名称	您为 管理中心 设备指定的描述性名称。尽管您可以使用主机名作为设备的名称，但在此字段中输入其他名称不会更改主机名。 此名称用于某些集成。例如，它显示在与 SecureX 和 SecureX 威胁响应集成的设备列表中。 如果更改名称，则所有已注册的设备都将被标记为过期，并且需要部署才能将新名称推送到设备。
产品型号	设备的型号名称。
序列号	设备的序列号。
软件版本	设备上当前安装的软件版本。
操作系统	当前在设备上运行的操作系统。
操作系统版本	当前设备上运行的操作系统的版本。
IPv4 地址	默认 (`eth0`) 管理接口的 IPv4 地址。如果 IPv4 管理处于禁用状态，此字段会予以指出。
IPv6 地址	默认 (`eth0`) 管理接口的 IPv6 地址。如果 IPv6 管理处于禁用状态，此字段会予以指出。
当前策略	当前部署的系统级策略。如果策略自上一次部署以来已更新，则策略的名称以斜体显示。
型号编号	存储在内部闪存驱动器上的设备特定型号。此编号可能对于故障排除非常重要。

入侵策略首选项

配置各种入侵策略首选项，以监控和跟踪部署中关键策略的更改。

设置入侵策略首选项

配置入侵策略首选项。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**入侵策略首选项 (Intrusion Policy Preferences)**。

步骤 3 您有以下选择：

- **有关策略更改的注释 (Comments on policy change)**：当用户修改入侵策略时，选中此复选框可以配置系统以使用注释功能跟踪与策略相关的更改。在启用策略更改注释的情况下，管理员可以快速评估修改部署中的关键策略的原因。

  如果对策略更改启用了注释功能，则可以将注释设置为可选或必填项。每次保存对策略所作的新更改时，管理中心 都会提示用户输入注释。

- **将入侵策略中的更改写入审核日志 (Write changes in Intrusion Policy to audit log)**：选中此复选框可将入侵策略的更改记录到审核日志中。默认情况下，此选项已启用。

- **保留已删除的 Snort 3 规则的用户覆盖 (Retain user overrides for deleted Snort 3 rules)**：选中此复选框可在 LSP 更新过程中获得任何覆盖系统定义规则的更改通知。如果启用，系统会在 LSP 更新过程中添加的新替换规则中保留规则覆盖。在管理中心菜单栏上，点击**通知 (Notifications)** > **任务 (Tasks)** 以查看通知。默认情况下，此选项已启用。

语言

可以使用 Language 页面为网络界面指定不同的语言。

设置 Web 接口的语言

在该页面上指定的语言将用于每个用户所用的网络接口。您可以选择：

- 英语
- 法语
- 中文（简体）

- 中文（繁体）
- 日语
- 韩语

过程

步骤 1 选择**系统**（⚙）> **配置**。
步骤 2 点击 **Language**。
步骤 3 选择要使用的语言。
步骤 4 点击**保存 (Save)**。

登录标识

可以使用“登录横幅”(Login Banner) 页面为安全设备或共享策略指定会话、登录或自定义消息横幅。

您可以使用 ASCII 字符和回车创建自定义登录横幅。系统不保留制表符间距。如果登录横幅过大或导致错误，则系统尝试显示横幅时 Telnet 或 SSH 会话可能会失败。

自定义登录横幅

过程

步骤 1 选择**系统**（⚙）> **配置**。
步骤 2 选择**登录横幅 (Login Banner)**。
步骤 3 在**自定义登录横幅 (Custom Login Banner)** 字段中，输入要使用的登录横幅。
步骤 4 点击**保存 (Save)**。

管理接口

安装后，您可以更改管理网络设置，包括在 管理中心上添加更多管理接口、主机名、搜索域、DNS 服务器和 HTTP 代理。

关于管理中心管理接口

默认情况下，管理中心通过单个管理接口管理所有设备。您还可以对管理接口执行初始设置，并以管理员身份通过该接口登录到管理中心 。管理接口还用于与智能许可服务器通信、下载更新以及执行其他管理功能。

关于设备管理接口的详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的关于管理设备接口 。

关于设备管理

在 管理中心 管理设备时，它会在自己和设备之间设置双向、SSL 加密的通信信道。管理中心使用此信道向设备发送有关要如何分析和管理流向设备的网络流量的信息。设备评估流量时，会生成事件并使用同一信道将其发送到管理中心。

通过使用 管理中心管理设备，您可以执行以下操作：

- 从单个位置为所有设备配置策略，从而更轻松地更改配置
- 在设备上安装各种类型的软件更新
- 向受管设备推送运行状况策略并监控其运行状态 管理中心

注释 如果您有 CDO 托管设备，并且仅将本地部署 管理中心 用于分析，则本地部署 管理中心 不支持策略配置或升级。本指南中与设备配置和其他不支持的功能有关的章节和程序不适用于主管理器为CDO 的设备。

管理中心汇总并关联入侵事件、网络发现信息和设备性能数据，从而能够监控设备报告的相互关联的信息，以及评估网络上出现的整体活动。

可以使用 管理中心来管理设备行为的几乎每个方面。

注释 尽管 管理中心 可以按照 http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html 处可用的兼容性矩阵中指定的那样管理运行之前的某些版本的设备，但需要最新版本 威胁防御 软件的新功能不适用于这些以前发布的设备。某些 管理中心 功能可能适用于早期版本。

管理连接

使用 管理中心 信息配置设备并将设备添加到 管理中心后，设备或 管理中心 可以建立管理连接。根据初始设置：

- 设备或 管理中心 都可以启动。
- 只有设备可以启动。

- 只有 管理中心 可以发起。

启动始终使用 管理中心 上的 eth0 或设备上编号最低的管理接口。如果未建立连接，则会尝试其他管理接口。管理中心 上的多个管理接口可让您连接到离散网络或隔离管理和事件流量。但是，发起方不会根据路由表选择最佳接口。

确保管理连接稳定，没有过多的丢包，吞吐量至少为 5 Mbps。

注释 管理连接是信道自身与设备之间的 TLS-1.3 加密的安全通信信道。出于安全目的，您不需要通过额外的加密隧道（例如站点间 VPN）运行此流量。例如，如果 VPN 发生故障，您将失去管理连接，因此我们建议使用简单的管理路径。

管理中心上的管理接口

管理中心使用 eth0 接口进行初始设置、对管理员的 HTTP 访问、设备管理，以及其他管理功能（如许可和更新）。

您还可以配置其他管理接口。当管理中心在不同网络上管理大量设备时，添加更多管理接口可以提高吞吐量和性能。还可以将这些接口用于所有其他管理功能。您可能希望将每个管理接口用于特定功能；例如，您可能希望将一个接口用于 HTTP 管理员访问，而将另一个接口用于设备管理。

对于设备管理，管理接口可以承载两个独立的流量隧道：管理流量隧道承载所有内部流量（如特定于管理设备的设备间流量），事件流量隧道承载所有事件流量（如 Web 事件）。可以选择在 管理中心上配置独立的仅事件接口，用于处理事件流量，可以仅配置一个事件接口。您还必须始终具有用于管理流量通道的管理接口。事件流量这能会占用大量带宽，因此将事件流量从管理流量中分离出来可以提高 管理中心的性能。例如，您可以分配一个 10 千兆以太网接口作为事件接口（如果可用），同时将多个 1 千兆以太网接口用于管理。例如，您可能希望在一个完全安全的专用网络上配置一个仅事件接口，同时在一个包括互联网访问的网络上使用常规管理接口。尽管您可以在同一网络上同时使用管理接口和事件接口，但我们建议将每个接口放在单独的网络上，以避免潜在的路由问题，包括从其他设备到 Cisco Secure Firewall Management Center 的路由问题。受管设备会将管理流量发送到管理中心的管理接口，并将事件流量发送到管理中心的仅事件接口。如果受管设备无法访问仅事件接口，则它将回退到将事件发送到管理接口。但是，无法通过仅事件接口建立管理连接。

始终首先从 eth0 尝试从 管理中心 发起管理连接，然后按顺序尝试其他接口；路由表不用于确定最佳接口。

注释 所有管理接口均支持由“访问列表”配置 (配置访问列表，第 41 页)控制的 HTTP 管理员访问。相反，您不能将某个接口限制为仅 HTTP 访问；管理接口始终支持设备管理（管理流量、事件流量或两者）。

注释 仅 eth0 接口支持 DHCP IP 寻址。其他管理接口仅支持静态 IP 地址。

每个管理中心型号的管理接口支持

有关管理接口位置，请参阅您的型号的硬件安装指南。

有关每个管理中心型号上支持的管理接口，请参阅下表。

表 *2:* 管理中心上的管理接口支持

型号	管理接口
MC1000	eth0（默认） eth1
MC2500、MC4500	eth0（默认） eth1 eth2 eth3
MC1600、MC2600、MC4600	eth0（默认） eth1 eth2 eth3 CIMC（仅支持无人值守管理。）
FMC1700、FMC2700、FMC4700	eth0（默认） eth1 eth2 eth3 CIMC（仅支持无人值守管理。）
Management Center Virtual	eth0（默认）

管理中心管理接口上的网络路由

管理接口（包括事件专用接口）仅支持通过静态路由到达远程网络。在设置 管理中心时，设置进程将为您指定的网关 IP 地址创建一个默认路由。不能删除此路由；只能修改网关地址。

在某些平台上，可以配置多个管理接口。默认路由不包括出口接口，因此选择的接口取决于您指定的网关地址以及网关属于哪个接口的网络。如果默认网络上有多个接口，设备将使用编号较低的接口作为出口接口。

如果要访问远程网络，建议为每个管理接口使用至少一个静态路由。我们建议将每个接口放在单独的网络中，以避免潜在的路由问题，包括从其他设备到 管理中心的路由问题。

注释 用于管理连接的接口不由路由表决定。始终首先使用 eth0 尝试连接，然后按顺序尝试后续接口，直到到达受管设备。

NAT 环境

网络地址转换 (NAT) 是一种通过路由器传输和接收网络流量的方法，其中涉及重新分配源或目标 IP 地址。NAT 最常见的用途是允许专用网络与互联网进行通信。静态 NAT 执行 1:1 转换，这不会引发管理中心与设备的通信问题，但端口地址转换 (PAT) 更为常用。PAT 允许您使用单一的公共 IP 地址和独特端口来访问公共网络；这些端口是根据需要动态分配的，因此您无法启动与 PAT 路由器后的设备的连接。

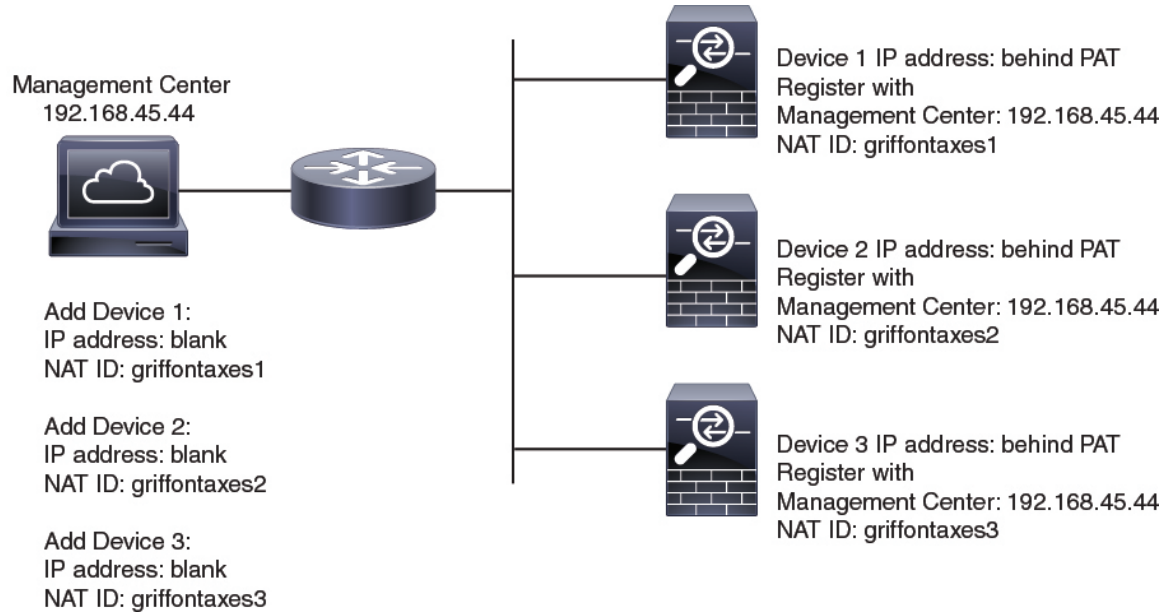
通常，无论是路由目的还是身份验证，都需要两个IP地址（连同一个注册密钥）：管理中心 当添加一个设备时，指定设备 IP 地址，设备指定 管理中心 IP 地址。但是，如果您只知道其中一个 IP 地址（这是实现路由目的的最低要求），您还必须在连接的两端指定唯一的NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。管理中心和设备使用注册密钥和 NAT ID（而不是 IP 地址）对初始注册进行身份验证和授权。

例如，您将设备添加到 管理中心，但不知道设备 IP 地址（例如，设备在 PAT 路由器后），因此只需要在 管理中心 上指定 NAT ID 和注册密钥；将 IP 地址留空。在设备上，指定 管理中心 IP 地址、相同的 NAT ID 和相同的注册密钥。设备将注册到 管理中心的 IP 地址。此时，管理中心将使用 NAT ID 而不是 IP 地址对设备进行身份验证。

尽管 NAT ID 最常用于 NAT 环境，但您可以选择使用 NAT ID 来简化向 管理中心添加多个设备的过程。在 管理中心上，在将 IP 地址留空的同时为要添加的每个设备指定唯一的 NAT ID，然后在每个设备上指定 管理中心 IP 地址和 NAT ID。注意：每个设备的 NAT ID 必须是唯一的。

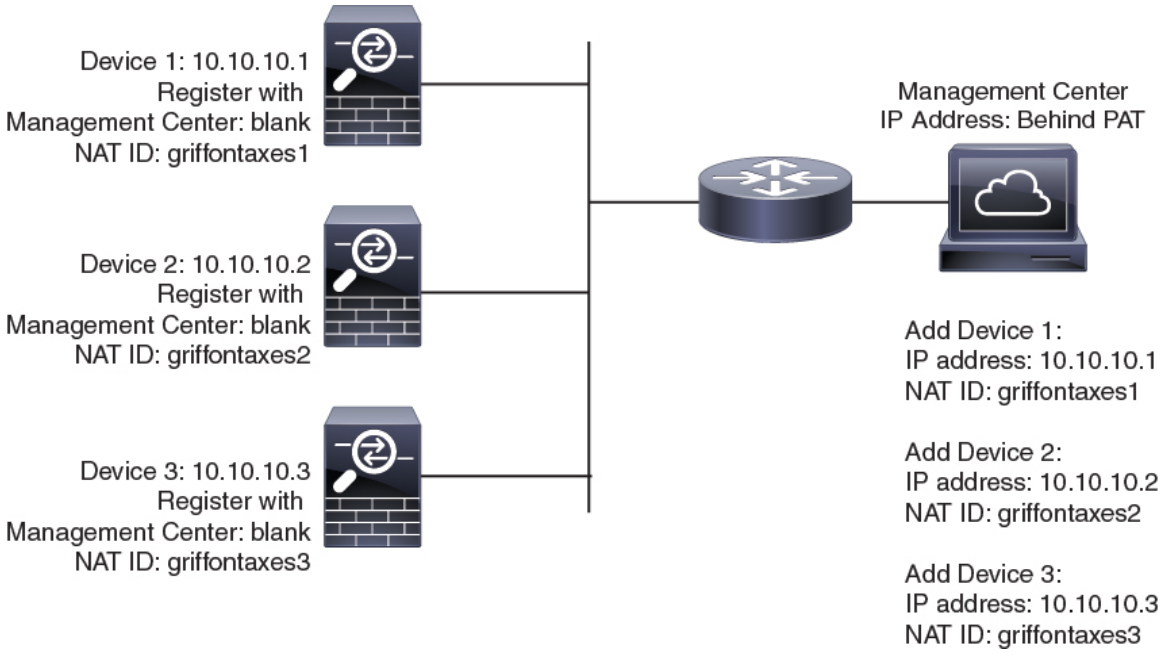
以下示例为 PAT IP 地址后的三个设备。在这种情况下，在 管理中心 和这些设备上为每个设备指定一个唯一的 NAT ID，并在这些设备上指定 管理中心 IP 地址。

图 *2: PAT* 后的受管设备 ***NAT ID***



以下示例为 PAT IP 地址后的 管理中心。在这种情况下，在 管理中心 和这些设备上为每个设备指定一个唯一的 NAT ID，并在 管理中心 上指定设备 IP 地址。

图 *3: PAT* 后的 ***FMC NAT ID***

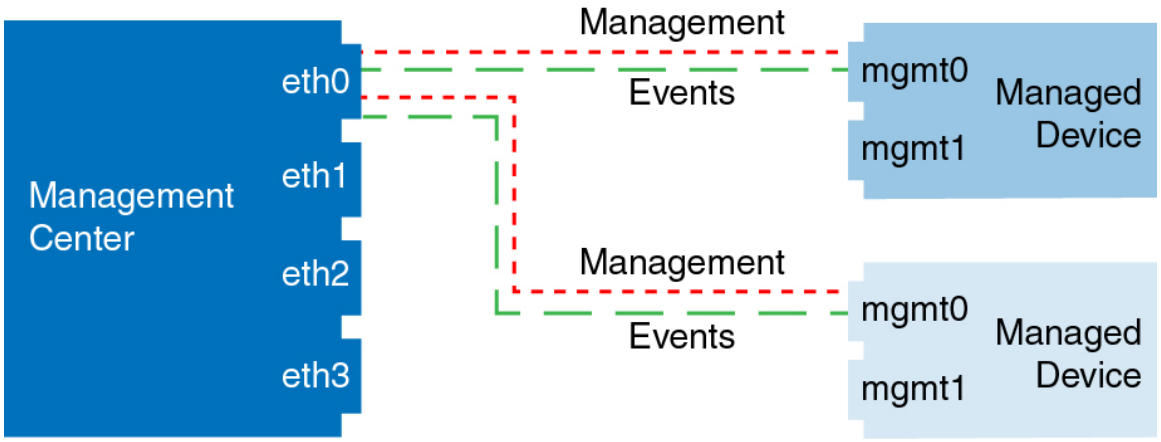


管理和事件流量通道示例

注释 如果在 威胁防御上使用数据接口进行管理，则不能对该设备使用单独的管理接口和事件接口。

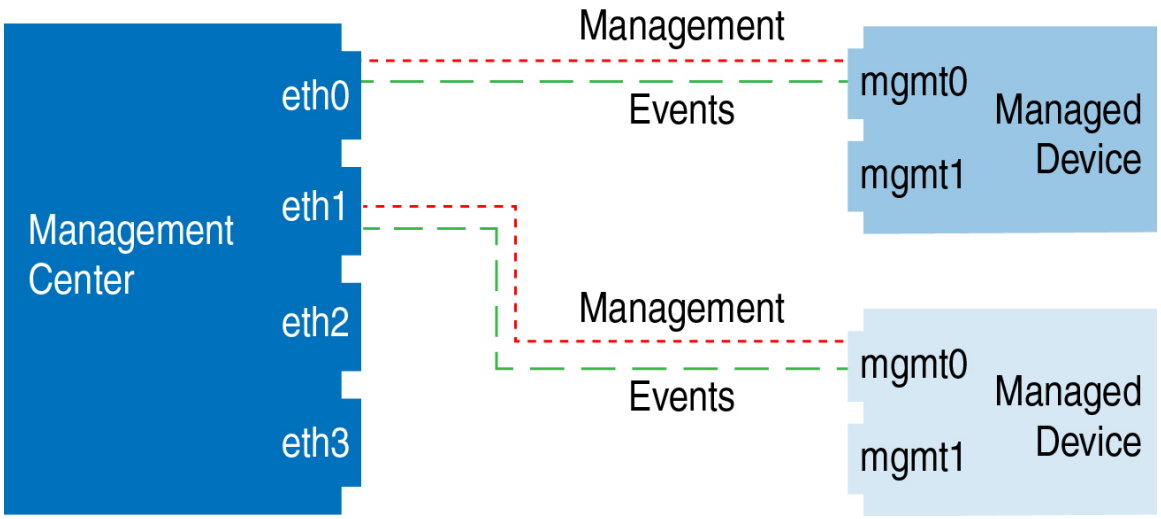
以下示例显示仅使用默认管理接口的 管理中心和受管设备。

图 *4: Cisco Secure Firewall Management Center*上的单个管理接口



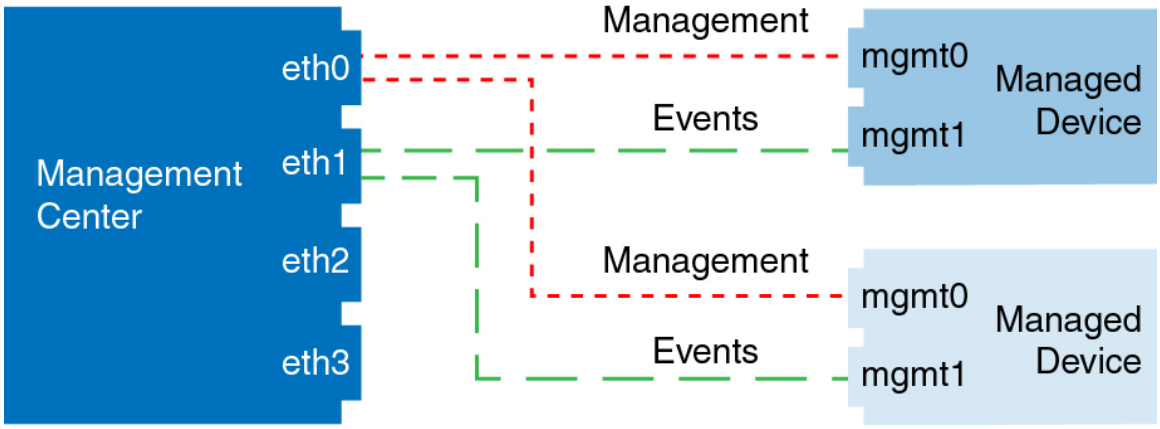
以下示例显示为设备使用单独管理接口的 管理中心；每台受管设备均使用 1 管理接口。

图 *5: Cisco Secure Firewall Management Center*上的多个管理接口



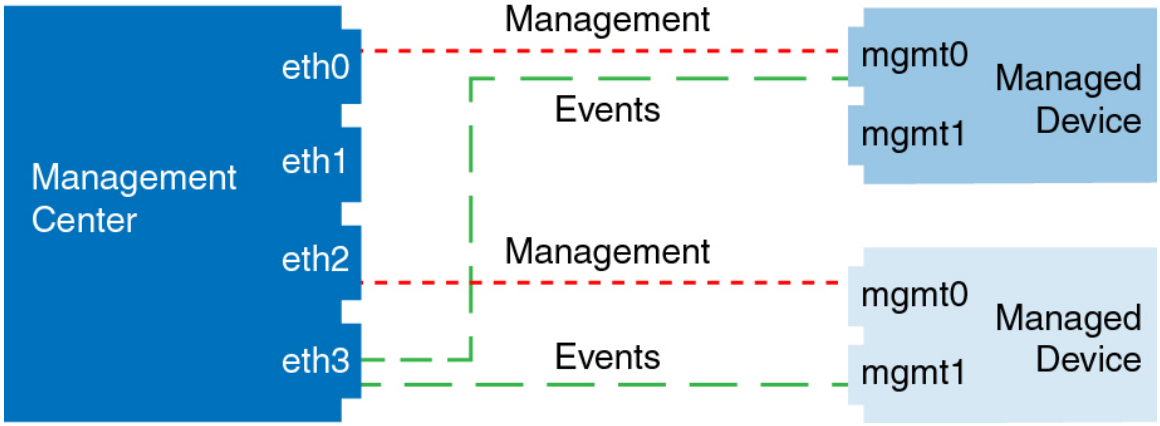
以下示例显示使用单独事件接口的 管理中心和受管设备。

图 *6: Cisco Secure Firewall Management Center*和受管设备上的单独事件接口



以下示例显示 管理中心上多个管理接口与单个事件接口的混合，以及使用单独事件接口或使用单个管理接口的受管设备的混合。

图 *7:* 混合管理和事件接口用法



修改 管理中心 管理接口

修改管理中心上的管理接口设置。您可以选择性地启用其他管理接口或配置仅限事件的接口。

⚠

注意 对所连接的管理接口进行更改时要保持谨慎；如果由于配置错误而无法重新连接，则需要访问 管理中心控制台端口以重新配置 Linux 外壳中的网络设置。您必须与思科 TAC 联系，以获取有关执行此项操作的指导。

如果更改 管理中心 IP 地址，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的编辑设备上的 管理中心 *IP* 地址或主机名 。如果更改 管理中心 IP 地址或主机名，还应在设备 CLI 中更改值，以便配置匹配。虽然在大多数情况下，无需更改设备上的管理中心IP地址或主机名即可重新建立管理连接，但在至少一种情况下，必须执行此任务才能重新建立连接：将设备添加到 管理中

心 并指定仅 NAT ID。即使在其他情况下，我们也建议保持 管理中心 IP 地址或主机名为最新状态，以实现额外的网络恢复能力。

在高可用性配置中，当您从设备 CLI 或 管理中心修改已注册设备的管理 IP 地址时，即使在 HA 同步后，辅助 管理中心 也不会反映更改。要确保辅助 管理中心 也更新，请在两个 管理中心之间切换角色，使辅助 管理中心 成为主用设备。在当前活动的 管理中心的设备管理页面上修改已注册设备的管理 IP 地址。

开始之前

- 有关多个管理接口的详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 关于管理设备接口 。
- 如果使用代理：
  - 使用 NT LAN Manager (NTLM) 身份验证的代理不受支持。
  - 如果使用或将要使用智能许可，则代理 FQDN 不能超过 64 个字符。

过程

步骤 1 选择 **系统**（⚙）> **配置**，然后选择**管理接口**。

步骤 2 在**接口**区域中，点击要配置的接口旁边的**编辑**。

本节列出了所有可用接口。不能再添加接口。

可以在每个管理接口上配置以下选项：

- **已启用** - 启用管理接口。请**不要**禁用默认的 eth0 管理接口。某些进程需要 eth0 接口。
- **信道**-必须始终至少有一个启用 **管理流量** 的接口。可选地配置一个仅事件接口。只能在 管理中心上配置一个事件接口。要执行此操作，请取消选中**管理流量**复选框，并保持**事件流量**复选框处于选中状态。对于其余管理接口，可以选择禁用 **事件流量**。无论哪种情况，设备都会尝试将事件发送到仅限事件接口；如果该接口关闭，则在管理接口上发送事件，即使已禁用事件通道。无法同时禁用接口上的事件通道和管理通道。
- **模式** - 指定链路模式。请注意，您对“自动协商”作出的所有更改将被千兆以太网接口忽略。
- **MDI/MDIX** - 设置**自动 MDIX** 设置。
- **MTU**-设置最大传输单位 (MTU)，1280-1500。默认值为 1500。
- **IPv4 配置** - 设置 IPv4 IP 地址。选择:
  - **静态** - 手动输入 **IPv4 管理 IP** 地址和 **IPv4 网络掩码**。
  - **DHCP** - 将接口设置为使用 DHCP（仅 eth0）。

    如果使用 DHCP，则必须使用 DHCP 预留，因此分配的地址不会更改。如果 DHCP 地址更改，设备注册将失败，因为 管理中心 网络配置不同步。要从 DHCP 地址更改中恢复，请连

接到 管理中心 （使用主机名或新 IP 地址）并导航至 **系统**（⚙）> **配置** > **管理接口** 以重置网络。

- **已禁用** - 禁用 IPv4。请勿同时禁用 IPv4 和 IPv6。

- **IPv6 配置** - 设置 IPv6 IP 地址。选择:
  - **静态** - 手动输入 **IPv6 管理 IP** 地址和 **IPv6 前缀长度**。
  - **DHCP** - 将接口设置为使用 DHCPv6（仅限 eth0）。
  - **已分配路由器** - 启用无状态自动配置。
  - **已禁用** - 禁用 IPv6。请勿同时禁用 IPv4 和 IPv6。
  - **IPv6 DAD** - 当您启用 IPv6 时，启用或禁用重复地址检测 (DAD)。您可能希望禁用 DAD，因为使用DAD可能会导致拒绝服务攻击。如果禁用此设置，则需要手动检查此接口是否未使用已分配的地址。

步骤 3 在 **路由** 区域中，通过点击 **编辑**（✎）编辑静态路由，或通过点击 **添加**（+）添加路由。

通过点击 👁 来查看路由表。

每个额外的接口均需要静态路由，才能访问远程网络。有关何时需要新路由的详细信息，请参阅 管理中心管理接口上的网络路由，第 72 页。

注释 对于默认路由，只能更改网关 IP 地址。通过将指定网关匹配到此接口网络，系统会自动选择出口接口。

您可以为静态路由配置以下设置：

- **目标** - 设置要创建路由的网络的目标地址。
- **网络掩码**或**前缀长度** - 设置网络的网络掩码 (IPv4) 或前缀长度 (IPv6)。
- **接口** - 设置出口管理接口。
- **网关** - 设置网关 IP 地址。

步骤 4 在**共享设置**区域中，设置所有接口共享的网络参数。

注释 如果为 eth0 接口选择了 **DHCP**，则无法手动指定从 DHCP 服务器派生的某些共享设置。

可以配置以下共享设置：

- **主机名** - 设置 管理中心主机名。主机名最多包含 64 个字符，并且必须以字母或数字开头和结尾，并且只能包含字母、数字或连字符。更改主机名后，如果您希望在系统日志消息中反映新的主机名，请重启 管理中心。在重启之后，系统日志消息才会反映新的主机名。
- **域** - 为 管理中心设置搜索域，用逗号分隔。如果没有在命令中指定完全限定域名，例如 **ping system**，则这些域将添加到主机名中。这些域仅用于管理接口，或通过管理接口的命令。

- **主 DNS 服务器、辅助 DNS 服务器、第三级 DNS 服务器** - 设置要按首选顺序使用的 DNS 服务器。
- **远程管理端口** - 设置远程管理端口用于与受管设备进行通信。管理中心和受管设备使用双向、SSL 加密的通信通道（默认情况下在端口 8305 上）进行通信。

  注释 思科强烈建议保留远程管理端口的默认设置，但如果管理端口与网络中的其他通信冲突，可以选择其他端口。如果更改管理端口，则必须在部署中需要相互通信的**所有**设备上做出该更改。

步骤 5 在 **ICMPv6** 区域中，配置 ICMPv6 设置。

- **允许发送回应应答数据包** - 启用或禁用回应应答数据包。您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。禁用回应应答数据包意味着无法使用 IPv6 ping 到管理中心管理接口，以进行测试。
- **允许发送目的地不可达数据包** - 启用或禁用目的地不可达数据包。您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。

步骤 6 在**代理**区域中，配置 HTTP 代理设置。

管理中心配置为通过端口 TCP/443 (HTTPS) 和 TCP/80 (HTTP) 直接连接到互联网。您可以使用代理服务器，以通过 HTTP 摘要对代理服务器进行身份验证。

请参阅本主题前提条件中的代理要求。

a) 选中**已启用 (Enabled)** 复选框。
b) 在 **HTTP 代理**字段中，输入代理服务器的 IP 地址或完全限定域名。

   请参阅本主题前提条件中的要求。

c) 在**端口 (Port)** 字段中，输入端口号。
d) 通过选择**使用代理身份验证**来提供身份验证凭证，然后提供**用户名**和**密码**。

步骤 7 点击**保存 (Save)**。

步骤 8 如果更改 管理中心 IP 地址，请参阅。如果更改 管理中心 IP 地址，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 编辑设备上的 管理中心 *IP* 地址或主机名 。

如果更改 管理中心 IP 地址或主机名，还应在设备 CLI 中更改值，以便配置匹配。虽然在大多数情况下，无需更改设备上的管理中心IP地址或主机名即可重新建立管理连接，但在至少一种情况下，必须执行此任务才能重新建立连接：将设备添加到管理中心 并指定仅NAT ID。即使在其他情况下，我们也建议保持 管理中心 IP 地址或主机名为最新状态，以实现额外的网络恢复能力。

更改管理中心和威胁防御 IP 地址

如果需要将 管理中心 和 威胁防御 IP 地址移至新网络，则可能需要同时更改这些地址。

过程

步骤 1 禁用管理连接。

对于高可用性对或集群，在所有设备上执行这些步骤。

a) 选择**设备** > **设备管理**。

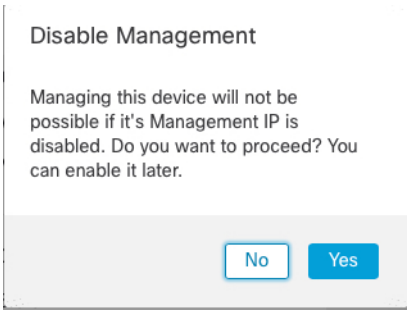
b) 点击设备旁边的 **编辑**（）。

c) 点击**设备 (Devices)**，并查看**管理 (Management)** 区域。

d) 点击滑块暂时禁用管理，使其处于禁用状态（）。

图 *8:* 禁用管理

系统将提示您继续禁用管理；点击 **是**。



步骤 2 将 管理中心 中的设备 IP 地址更改为新的设备 IP 地址。

稍后您将更改设备上的 IP 地址。

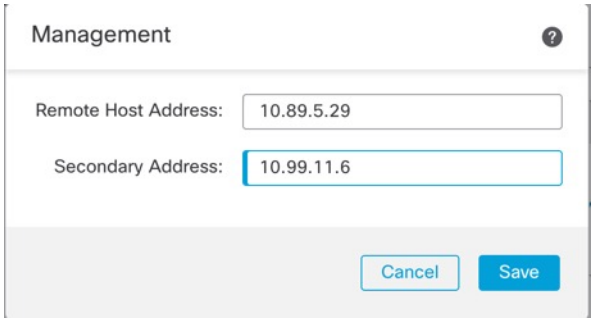
对于高可用性对或集群，在所有设备上执行这些步骤。

a) 通过点击 **编辑**（） 来编辑**远程主机地址** IP 地址和可选**辅助地址**（使用冗余数据接口时）或主机名。

图 *9:* 编辑管理地址

b) 在**管理 (Management)** 对话框中，在**远程主机地址 (Remote Host Address)** 字段和可选的**辅助地址 (Secondary Address)** 字段中修改名称或 IP 地址，然后点击**保存 (Save)**。

图 *10:* 管理 *IP* 地址



步骤 3 请更改 管理中心 IP 地址。

注意 对所连接的管理中心接口进行更改时要保持谨慎；如果由于配置错误而无法重新连接，则需要访问 管理中心 控制台端口以重新配置 Linux 外壳中的网络设置。您必须与思科 TAC 联系，以获取有关执行此项操作的指导。

a) 选择 **系统**（⚙）> **配置**，然后选择**管理接口**。
b) 在**接口**区域中，点击要配置的接口旁边的**编辑**。
c) 更改 IP 地址，然后点击**保存 (Save)**。

步骤 4 更改设备上的管理器 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

a) 在 威胁防御 CLI 中，查看 管理中心 标识符。

show managers

示例：

```
> show managers
Type                   : Manager
Host                   : 10.10.1.4
Display name           : 10.10.1.4
Identifier             : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration           : Completed
```

```
Management type           : Configuration
```

b) 编辑 管理中心 IP 地址或主机名。

configure manager edit 标识符 {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

如果 管理中心 最初由 **DONTRESOLVE** 和 NAT ID 标识，则可以使用此命令将该值更改为主机名或 IP 地址。不能将 IP 地址或主机名更改为 **DONTRESOLVE**。

示例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

步骤 5 在控制台端口更改管理器访问接口的 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

如果您使用专用管理接口：

configure network ipv4

configure network ipv6

如果您使用专用管理接口：

configure network management-data-interface disable

configure network management-data-interface

步骤 6 点击滑块重新启用管理，使其处于启用状态 （ ）。

对于高可用性对或集群，在所有设备上执行这些步骤。

图 *11:* 启用管理连接

步骤 7 （如果使用数据接口进行管理器访问）刷新 管理中心中的数据接口设置。

对于高可用性对，请在两台设备上执行此步骤。

a) 选择**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理访问权限 - 配置详细信息 (Manager Access - Configuration Details)**，然后点击**刷新 (Refresh)**。

b) 选择**设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)**，然后设置 IP 地址以便与新地址匹配。

c) 返回**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)** 以删除部署块。

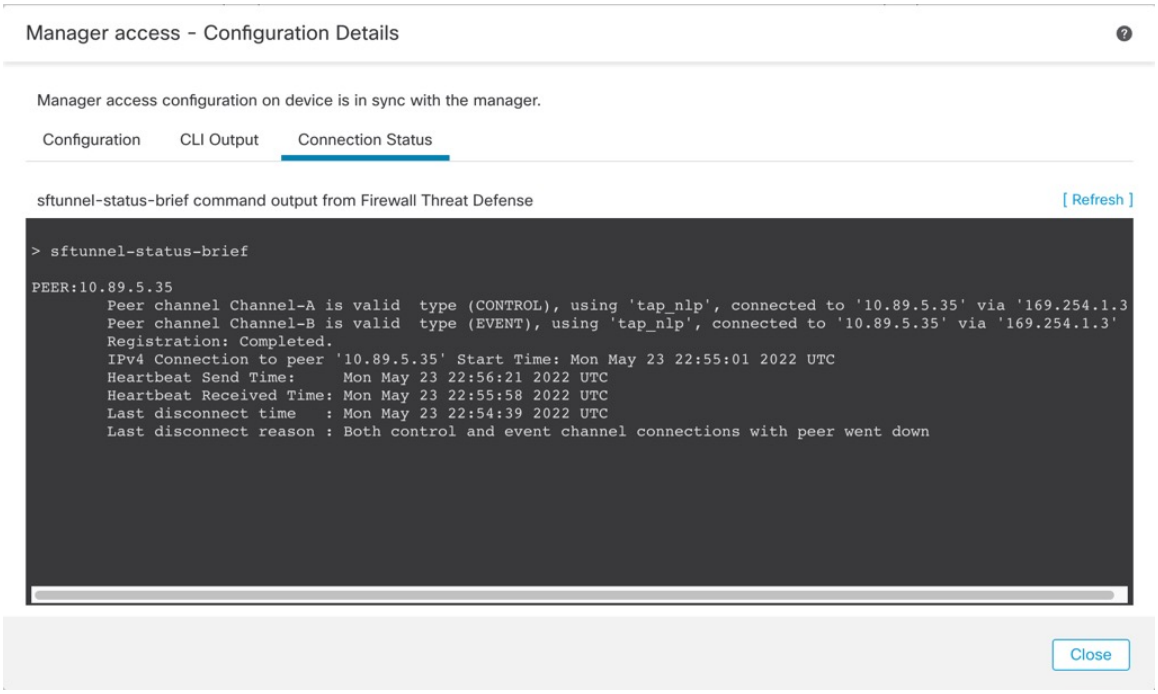
步骤 8 确保管理连接已重新建立。

在 管理中心 中，在 **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** > **连接状态 (Connection Status)** 页面上检查管理连接状态。

在 威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *12:* 连接状态



步骤 9 （对于高可用性 管理中心 对）在辅助 管理中心上重复配置更改。

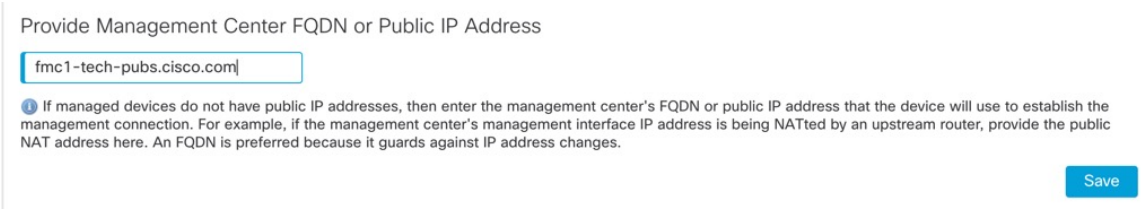
a) 更改辅助 管理中心 IP 地址。
b) 在两台设备上指定新的对等地址。
c) 将辅助设备设置为主用设备。
d) 禁用设备管理连接。
e) 更改 管理中心 中的设备 IP 地址。
f) 重新启用管理连接。

管理器远程访问

如果受管设备没有公共 IP 地址，则输入设备在建立管理连接时使用的 管理中心的 FQDN 或公共 IP 地址。例如，如果上游路由器对 管理中心的管理接口 IP 地址执行 NAT，请在此处提供 公共 NAT 地址。首选 FQDN，因为它可以防止 IP 地址更改。

如果使用序列号 (零接触调配) 方法注册设备，则此字段将自动用于管理器 IP 地址/主机名的初始配置。如果使用手动方法，则在执行设备的初始配置时，可以参考此屏幕上的值来识别公共 管理中心 IP 地址/主机名。

图 *13:* 管理器远程访问



网络分析策略首选项

当用户修改入侵策略时，可以配置系统以使用注释功能跟踪与策略相关的更改。在启用策略更改注释的情况下，管理员可以快速评估修改部署中的关键策略的原因。

如果对策略更改启用了注释功能，则可以将注释设置为可选或必填项。每次保存对策略所作的新更改时，系统都会提示用户输入注释。

或者，可以将对网络分析策略的更改写入到审核日志中。

进程

使用 Web 界面来控制 管理中心上的进程的关闭和重新启动。您可以执行以下操作：

- 关闭：启动设备的正常关闭。

注意 请**勿**使用电源按钮关闭 Firepower 设备；这样做可能导致数据丢失。通过使用 Web 界面（或 CLI），可让系统做好准备，在不丢失配置数据的情况下安全断电和重新启动。

- 重新引导：关闭并正常重启。
- 重新启动控制台：重新启动通信、数据库和 HTTP 服务器进程。这通常在故障排除过程中使用。

提示 对于虚拟设备，请参阅您的虚拟平台的文档。特别是对于 VMware，自定义电源选项是 VMware 工具的一部分。

关闭或重新启动 FMC

过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 选择**进程 (Process)**。

步骤 3 执行以下操作之一：

关闭	点击 **关闭管理中心**旁边的 **运行命令** 。
重新启动	点击 **重新引导管理中心**旁边的 **运行命令** 。 **注释** 重新启动会让您退出，系统会执行可能需要一小时才能完成的数据库检查。
重新启动控制台	点击 **重新启动管理中心**旁边的 **运行命令** 。 **注释** 重新启动可能导致已删除的主机重新显示在网络映射中。

REST API 首选项

管理中心 REST API 提供轻量级接口，以供第三方应用使用 REST 客户端和标准 HTTP 方法查看和管理设备配置。有关 管理中心 REST API 的更多信息，请参阅 Secure Firewall Management Center REST API 快速入门指南。

注释 管理中心 REST API 不支持 HTTPS 证书。

默认情况下，管理中心使用 REST API 允许来自应用的请求。可以将 管理中心配置为阻止此访问。

启用 Rest API 访问

注释 在使用 管理中心高可用性的部署中，此功能仅在主用 管理中心中可用。

过程

步骤 1 选择右上角的**齿轮**（⚙）以打开系统菜单。

步骤 2 点击 **REST API 首选项 (REST API Preferences)**。

步骤 3 要启用或禁用对 管理中心 的 REST API 访问，请选中或取消选中**启用 REST API** 复选框。

步骤 4 点击**保存 (Save)**。

步骤 5 访问 REST API Explorer，网址为：

```
https://<management_center_IP_or_name>:<https_port>/api/api-explorer
```

远程控制台访问管理

您可以通过物理设备上的 VGA 端口（默认端口）或串行端口使用 Linux 系统控制台在受支持系统上进行远程访问。使用“控制台配置”页面，选择最适合您的组织的 Firepower 部署的物理布局的选项。

在受支持的基于物理硬件的系统中，可以通过 LAN 上串行 (SOL) 连接管理接口上使用无人值守管理 (LOM) 来远程监控或管理该系统，而无需登录到该系统的管理接口。在带外管理连接上使用命令行界面可以执行有限的任务，例如查看机箱序列号或监控诸如风扇速度和温度之类的状况。支持 LOM 的电缆连接因 管理中心 型号而异：

- 对于 管理中心 MC1600、MC2600 和 MC4600 型号，使用 CIMC 端口连接以支持 LOM。有关更多信息，请参阅《*1600、2600 和 4600 型 Cisco Firepower 管理中心入门指南*》。
- 对于所有其他 管理中心 硬件型号，请使用具有默认 (eth0) 管理端口的连接来支持 LOM。有关硬件型号，请参阅 思科 *Firepower* 管理中心入门指南 。

您必须对系统和要管理系统的用户均启用 LOM。在启用系统和用户后，使用第三方智能平台管理接口 (IPMI) 实用程序访问和管理系统。

配置系统上的远程控制台设置

您必须是管理员用户才能执行此程序。

开始之前

- 禁用与设备管理接口连接的所有第三方交换设备上的生成树协议 (STP)。
- 如果计划启用无人值守管理，请参阅设备的入门指南，了解有关安装和使用智能平台管理接口 (IPMI) 实用程序的信息。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**控制台配置 (Console Configuration)**。

步骤 3 选择远程控制台访问选项：

- 选择 **VGA** 将会使用设备的 VGA 端口。
- 选择 **物理串行端口** 以使用设备的串行端口。
- 选择 **无人值守管理** 以在管理中心上使用 SOL 连接。（这可能使用默认管理端口或 CIMC 端口，具体取决于您的 管理中心 型号。有关详细信息，请参阅您的型号的 入门指南 。

步骤 4 要通过 SOL 配置 LOM，请执行以下操作：

- 选择系统的地址 **配置** （**DHCP** 或 **手动**）
- 如果选择手动配置，请输入必要的 IPv4 设置：
  - 输入要用于 LOM 的 **IP 地址 (IP Address)**。

    注释 LOM IP 地址必须不同于 管理中心 管理接口 IP 地址，并要在同一个子网中。

  - 输入系统的**网络掩码 (Netmask)**。
  - 输入系统的**默认网关 (Default Gateway)**。

步骤 5 点击**保存 (Save)**。

步骤 6 系统显示以下警告：“您必须重新启动系统才能使这些更改生效。” 点击 **确认** 立即重新启动或点击 **取消** 稍后重新启动。

下一步做什么

- 如果配置了串行访问，请确保将后面板串行端口连接到本地计算机、终端服务器或其他可支持通过以太网进行远程串行访问的设备，如适用于您的 管理中心 型号的 入门指南 中所述。
- 如果配置了无人值守管理，请启用无人值守管理用户；请参阅无人值守管理用户访问配置，第 87 页。

无人值守管理用户访问配置

必须将“无人值守管理”权限明确授予使用此功能的用户。LOM 用户还有如下限制：

- 必须为用户指定管理员角色。
- 用户名最多可包含 16 个字母数字字符。不支持将连字符和更长的用户名用作 LOM 用户名。
- 用户的 LOM 密码不得与该用户的系统密码相同。密码必须符合 用户密码，第 116 页中所述的要求。思科建议您为设备使用最大支持长度、不是基于字典的复杂密码，并且每三个月修改一次密码。
- 物理 管理中心的 最多可以有 13 个 LOM 用户。

请注意，如果在一个具有 LOM 权限的用户已登录时取消激活然后再重新激活该用户，那么该用户可能需要重新登录到 Web 界面才能重新获得对 `impitool` 命令的访问权限。

注释 高可用性同步不适用于 LOM 用户，因此它们不会在高可用性 管理中心上复制。您必须在活动 管理中心上创建启用 LOM 的不同管理员用户。

在高可用性配置中，当您为启用了 LOM 权限的本地用户创建本地用户或重置密码时，更改会从基于 UCS 的主用 管理中心同步到主用和备用 管理中心以及主用 管理中心 CIMC。新密码未与 CIMC 登录的备用管理中心同步。要确保备用管理中心也更新，请重置备用管理中心上本地用户的CIMC 登录密码。

启用无人值守管理用户访问

您必须是管理员用户才能执行此程序。

使用此任务向现有用户授予LOM访问权限。要向新用户授予LOM访问权限，请参阅添加或编辑内部用户，第 118 页。

过程

步骤 1 选择**系统**（⚙）> **用户** > **用户**。

步骤 2 要向现有用户授予 LOM 用户访问权限，请点击列表中用户名旁边的 **编辑**（✎）。

步骤 3 在**用户配置 (User Configuration)** 下，启用管理员角色。

步骤 4 选中**允许无人值守管理访问 (Allow Lights-Out Management Access)** 复选框。

步骤 5 点击**保存 (Save)**。

LAN 上串行连接配置

使用计算机上的第三方 IPMI 实用程序可通过 LAN 上串行与设备建立连接。如果您的计算机使用类似 Linux 的环境或 Mac 环境，请使用 IPMItool；对于 Windows 环境，请使用 IPMIutil 或 IPMItool，取决于您的 Windows 版本。

注释 思科建议使用 IPMItool V1.8.12 或更高版本。

Linux

IPMItool 是许多发行版的标准配置，可立即使用。

Mac

必须在 Mac 上安装 IPMItool。首先，请确认 Mac 上安装了 Apple 的 XCode 开发者工具，确保安装了用于命令行开发的可选组件（在较新版本中为 UNIX 开发和系统工具，或在较旧版本中为命令行

支持）。然后您可以安装 macports 和 IPMItool。请使用您常用的搜索引擎搜索更多信息，以下网站也可能对您帮助：

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
http://github.com/ipmitool/ipmitool/
```

Windows 的 ISE 安全评估代理

对于启用了适用于 Linux 的 Windows 子系统 (WSL) 的 Windows 版本 10 及更高版本，以及某些较早版本的 Windows Server，您可以使用 IPMItool。否则，您必须在 Windows 系统上编译 IPMIutil；您可以使用 IPMIutil 本身进行编译。请使用您常用的搜索引擎搜索更多信息，以下网站也可能对您帮助：

```
http://ipmiutil.sourceforge.net/man.html#ipmiutil
```

了解 IPMI 实用程序命令

用于 IPMI 实用程序的命令由若干段组成，如以下 Mac 上的 IPMItool 示例：

```
ipmitool -I lanplus -H IP_address -U user_name command
```

其中：

- `ipmitool` 调用实用程序。
- `-I lanplus` 指定对会话使用加密的 IPMI v2.0 RMCP+ LAN 接口。
- `-H IP_地址` 表示已配置的要访问的设备的 Lights-Out 管理 IP 地址。
- `-U 用户_名称` 是授权远程会话用户的名称。
- `命令` 是您想使用的命令的名称。

注释 思科建议使用 IPMItool V1.8.12 或更高版本。

对于 Windows 上的 IPMIutil，以上命令如下所示：

```
ipmiutil command -V 4 -J 3 -N IP_address -Uuser_name
```

使用此命令可连接到设备的命令行，就像您本人在设备旁边一样。系统会提示您输入密码。

使用 IPMItool 配置 LAN 上串行

您必须是管理员用户具有 LOM 访问权限才能执行此程序。

过程

使用 IPMItool，输入以下命令，并在提示时输入密码：

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

使用 IPMIutil 配置 LAN 上串行

您必须是管理员用户具有 LOM 访问权限才能执行此程序。

过程

使用 IPMIutil，输入以下命令，如果出现提示则输入密码：

```
ipmiutil -J 3 -N IP_address -U username sol -a
```

无人值守管理概述

通过无人值守管理 (LOM)，您可以在默认 (`eth0`) 管理接口上利用 SOL 连接执行有限的系列操作，而无需登录设备。可以使用命令创建 SOL 连接，然后使用其中一个 LOM 命令。命令执行完成后，连接将终止。

⚠

注意 在极少数情况下，如果您的计算机与系统的管理接口位于不同子网，而系统配置为使用 DHCP，则尝试访问 LOM 功能可能失败。如果发生这种情况，可以禁用然后在系统上重新启用 LOM，或者使用与系统位于同一子网的计算机来 ping 设备的管理接口。这样应该就可以使用 LOM。

⚠

注意 思科了解智能平台管理接口 (IPMI) 标准 (CVE-2013-4786) 固有的漏洞。在系统上启用无人值守管理 (LOM) 会暴露该漏洞。为了降低这种漏洞，请将您的系统部署在只有受信任用户才可以访问的安全管理网络上，并且使用最大支持长度、不是基于字典的复杂密码并且每三个月修改一次密码。为防止暴露此漏洞，请勿启用 LOM。

如果所有访问系统的尝试均失败，则可以使用 LOM 远程重新启动系统。请注意，如果在 SOL 连接处于活动状态时重新启动系统，LOM 会话可能会断开连接或超时。

⚠

注意 请**勿**重新启动系统，除非它不响应任何其他重新启动操作。远程重新启动系统不能正常重新启动系统，而且可能会丢失数据。

表 *3:* 无人值守管理命令

IPMItool	IPMIutil	说明
（不适用）	`-V 4`	启用 IPMI 会话的管理员权限
`-I lanplus`	`-J 3`	启用 IPMI 会话加密
`-H` 主机名/*IP* 地址	`-N` 节点名/*IP* 地址	表示 管理中心的 LOM IP 地址或主机名
`-U`	`-U`	表示已获授权 LOM 帐户的用户名
`sol activate`	`sol -a`	开始 SOL 会话
`sol deactivate`	`sol -d`	结束 SOL 会话
`chassis power cycle`	`power -c`	重新启动设备
`chassis power on`	`power -u`	打开设备电源
`chassis power off`	`power -d`	关闭设备电源
`sdr`	`sensor`	显示设备信息，例如风扇速度和温度

例如，显示设备信息列表的 IPMItool 命令是：

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

注释 思科建议使用 IPMItool V1.8.12 或更高版本。

对于 IPMIutil 实用程序，以上命令如下：

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

使用 IPMItool 配置无人值守管理

您必须是管理员用户具有 LOM 访问权限才能执行此程序。

过程

为 IPMItool 输入以下命令以及密码（如果提示）：

```
ipmitool -I lanplus -H IP_address -U user_name command
```

使用 IPMIutil 配置无人值守管理

您必须是管理员用户具有 LOM 访问权限才能执行此程序。

过程

为 IPMIutil 输入以下命令以及密码（如果提示）：

```
ipmiutil -J 3 -N IP_address -U username command
```

远程存储设备

在 管理中心上，您可以将本地或远程存储的以下系统用于备份和报告：

- 网络文件系统 (NFS)
- 服务器消息块 (SMB)/通用互联网文件系统 (CIFS)
- 安全外壳 (SSH)

不能将备份发送到一个远程系统而将报告发送到另一个，但是，可以选择这二者之一发送到远程系统，并将另一个存储在 管理中心。

提示 在配置并选择远程存储之后，只有在未增加连接数据库限制的情况下，才可以切换回本地存储。

管理中心远程存储 - 支持的协议和版本

管理中心版本	NFS 版本	SSH 版本	SMB 版本
6.4	V3/V4	openssh 7.3p1	V2/V3
6.5	V3/V4	ciscossh 1.6.20	V2/V3
6.6	V3/V4	ciscossh 1.6.20	V2/V3
6.7	V3/V4	ciscossh 1.6.20	V2/V3

用于启用协议版本的命令

以 root 用户身份运行以下命令以启用协议版本：

- **NFS**—`/bin/mount -t nfs '10.10.4.225':'/home/manual-check' '/mnt/remote-storage' -o 'rw,vers=4.0'`

- **SMB**—`/usr/bin/mount.cifs //10.10.0.100/pyallapp-share/testing-smb /mnt/remote-storage -o username=administrator,password=******,vers=3.0`

配置本地存储

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 选择**远程存储设备 (Remote Storage Device)**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择**本地（无远程存储）(Local [No Remote Storage])**。

步骤 4 点击**保存 (Save)**。

为远程存储配置 NFS

开始之前

- 确保外部远程存储系统可正常工作且能够从 管理中心 进行访问。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Remote Storage Device**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择 **NFS**。

步骤 4 添加连接信息：

- 在**主机 (Host)** 字段中输入存储系统的 IPv4 地址或主机名。
- 在**目录 (Directory)** 字段中输入存储区域的路径。

步骤 5 或者，选中**使用高级选项 (Use Advanced Options)** 复选框并输入任何所需命令行选项；请参阅远程存储管理高级选项，第 96 页。

步骤 6 在**系统使用 (System Usage)** 下：

- 选择**用于备份 (Use for Backups)** 以将备份存储在指定主机上。
- 选择**用于报告 (Use for Reports)** 以将报告存储在指定主机上。
- 然后，在 **Disk Space Threshold** 中输入要备份远程存储的磁盘空间阈值。默认值为 90%。

步骤 7 要测试设置，请点击**测试 (Test)**。

步骤 8 点击**保存 (Save)**。

故障排除

当与防火墙设备的 NFS 连接中存在随机延迟时，请执行以下活动，然后联系思科 TAC 进行故障排除：

- 在设备出现问题之前或之后收集故障排除文件。您可以从 Web 界面或使用 CLI 命令生成故障排除文件。有关如何生成故障排除文件的信息，请参阅 Firepower 文件生成程序故障排除。
- 收集传入和退出流量 PCAP 记录。有关程序的信息，请参阅数据包捕获概述，第 424 页。
- 在设备中使用以下命令（CLISH 模式）在 NFS 应用失败时收集系统支持跟踪数据：

  ```
  > system support trace
  ```

- 在故障期间，使用 **show snort counters** 命令收集 Snort 计数器两次，以查看 Snort 预处理器连接的统计信息。有关此命令的信息，请参阅 show snort counters。

为远程存储配置 SMB

开始之前

确保外部远程存储系统可正常工作且能够从 管理中心进行访问：

- 请注意，系统只能识别顶级 SMB 共享，不能识别完整文件路径。您必须使用 Windows 来共享要使用的确切目录。
- 确保您将用于从 FMC 访问 SMB 共享的 Windows 用户具有共享位置的所有权和读取/更改权限。
- 为确保安全，应安装 SMB 2.0 或更高版本。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Remote Storage Device**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择 **SMB**。

步骤 4 添加连接信息：

- 在**主机 (Host)** 字段中输入存储系统的 IPv4 地址或主机名。
- 在**共享 (Share)** 字段中输入存储区域共享。
- 或者，在**域 (Domain)** 字段中输入远程存储系统的域名。
- 在**用户名 (Username)** 字段中输入存储系统的用户名，在**密码 (Password)** 字段中输入该用户的密码。

步骤 5 或者，选中**使用高级选项 (Use Advanced Options)** 复选框并输入任何所需命令行选项；请参阅远程存储管理高级选项，第 96 页。

步骤 6 在**系统使用 (System Usage)** 下：

- 选择**用于备份 (Use for Backups)** 以将备份存储在指定主机上。
- 选择**用于报告 (Use for Reports)** 以将报告存储在指定主机上。

步骤 7 要测试设置，请点击**测试 (Test)**。

步骤 8 点击**保存 (Save)**。

为远程存储配置 SSH

开始之前

- 确保外部远程存储系统可正常工作且能够从 管理中心 进行访问。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Remote Storage Device**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择 **SSH**。

步骤 4 添加连接信息：

- 在**主机 (Host)** 字段中输入存储系统的 IP 地址或主机名。
- 在**目录 (Directory)** 字段中输入存储区域的路径。
- 在 **Username** 字段中输入存储系统的用户名，在 **Password** 字段中输入该用户的密码。要将网络域指定为连接用户名的一部分，请在用户名前面加上域后跟正斜杠 (/)。
- 要使用 SSH 密钥，请将 **SSH Public Key** 字段中的内容复制到 authorized_keys 文件中。

步骤 5 或者，选中**使用高级选项 (Use Advanced Options)** 复选框并输入任何所需命令行选项；请参阅远程存储管理高级选项，第 96 页。

步骤 6 在“系统使用”(System Usage) 下：

- 选择**用于备份 (Use for Backups)** 以将备份存储在指定主机上。
- 选择**用于报告 (Use for Reports)** 以将报告存储在指定主机上。

步骤 7 如果要测试设置，必须点击**测试 (Test)**。

步骤 8 点击**保存 (Save)**。

远程存储管理高级选项

如果选择网络文件系统 (NFS) 协议、服务器消息阻止 (SMB) 协议或 SSH 以使用文件传输协议 (SFTP) 来存储报告和备份，您可以选择**使用高级选项**复选框，以使用其中一个安装二进制选项，如 NFS、SMB 或 SSH 安装主页面所记录。

如果选择 SMB 或 NFS 存储类型，则可以使用以下格式在**命令行选项**字段中指定远程存储的版本号：

`vers=version`

其中 *版本* 是要使用的 SMB 或 NFS 远程存储的版本号。例如，要选择 NFSv4，请输入 `vers=4.0`。

如果为文件服务器启用了 SMB 加密，则仅允许 SMB 3.0 版客户端访问文件服务器。要从 管理中心 访问加密的 SMB 文件服务器，请在**命令行选项**字段中键入以下内容：

`vers=3.0`

选择加密的 SMBv3，将备份文件从 管理中心 复制或保存到加密的 SMB 文件服务器。

SNMP

您可以启用简单网络管理协议 (SNMP) 轮询。此功能支持使用 SNMP 协议第 1 版、第 2 版和第 3 版。此功能允许访问标准管理信息库 (MIB)，包括联系人、管理、位置、服务信息、IP 寻址和路由信息以及传输协议使用统计信息等系统详细信息。

注释 为 SNMP 协议选择 SNMP 版本时，请注意 SNMPv2 仅支持只读社区，SNMPv3 仅支持只读用户。此外，SNMPv3 还支持使用 AES128 加密。

启用 SNMP 轮询不会导致系统发送 SNMP 陷阱；这样做只会使 MIB 中的信息可供网络管理系统轮询。

配置 SNMP 轮询

开始之前

为计划用于轮询系统的每台计算机添加 SNMP 访问权限。请参阅配置访问列表，第 41 页。

注释 SNMP MIB 包含可用于攻击您的部署的信息。我们建议您将 SNMP 访问权限的访问列表限制为将被用于轮询 MIB 的特定主机。我们还建议您针对网络管理访问权限使用 SNMPv3 和强密码。

过程

步骤 1 选择系统（⚙）> 配置。

步骤 2 点击 **SNMP**。

步骤 3 从 **SNMP 版本** 下拉列表中，选择要使用的 SNMP 版本：

- **版本 1** 或 **版本 2**：在 **社区字符串** 字段中输入只读 SNMP 社区名称，然后跳至程序末尾。

  注释 不包含特殊字符 (< > / % # & ? ' 等）在 SNMP 社区字符串名称中。

- **版本 3**：请点击 **添加用户** 显示用户定义页面。SNMPv3 仅支持只读用户和使用 AES128 加密。

步骤 4 输入**用户名 (Username)**。

步骤 5 从**身份验证协议 (Authentication Protocol)** 下拉列表中选择要用于身份验证的协议。

步骤 6 在**身份验证密码 (Authentication Password)** 字段中输入使用 SNMP 服务器进行身份验证时所需的密码。

步骤 7 在**验证密码 (Verify Password)** 字段中重新输入身份验证密码。

步骤 8 从**隐私协议 (Privacy Protocol)** 列表中选择要使用的隐私协议，或者选择**无 (None)** 以不使用隐私协议。

步骤 9 在**隐私密码 (Privacy Password)** 字段中输入 SNMP 服务器需要的 SNMP 隐私密钥。

步骤 10 在**验证密码 (Verify Password)** 字段中重新输入隐私密码。

步骤 11 点击**添加 (Add)**。

步骤 12 点击**保存 (Save)**。

会话超时

无人参与的登录会话可能存在安全风险。可以配置用户的登录会话因无活动而超时之前允许经过的空闲时间。

请注意，对于计划长期安全地被动监控系统的场景，可以免除特定 Web 界面用户的超时。具有“管理员”(Administrator) 角色的用户拥有对菜单选项的完整访问权限，这些访问权限受损会构成额外风险，因此他们不能获得会话超时豁免。

配置会话超时

过程

步骤 1 选择系统（⚙）> 配置。

步骤 2 点击 **CLI 超时**。

步骤 3 配置会话超时：

- Web 界面（仅限于管理中心）：配置 **浏览器会话超时（分钟）**。默认值为 `60`；最大值为 `1440`（24 小时）。

  使用户免受会话超时影响的信息，请参阅 添加或编辑内部用户，第 118 页。

- CLI：配置 **CLI 超时（分钟）** 字段。默认值为 `0`；最大值为 `1440`（24 小时）。

步骤 4 点击**保存 (Save)**。

时间

时间设置在大多数页面上均使用您在“用户首选项”的“时区”页面上设置的时区（默认值是“美国/纽约”）以本地时间显示，但使用 UTC 时间存储在设备中。

限制 时区功能（在“用户首选项”中）假设，默认系统时钟设置为UTC时间。请勿尝试更改系统时间。请注意，不支持从UTC更改系统时间，而执行此操作将需要您重新映像设备以从不支持的状态中恢复。

过程

步骤 1 选择**系统**（  ）> **配置**。

步骤 2 点击 **Time**。

使用在“用户首选项”中为您的账户指定的时区显示当前时间。

如果您的设备使用 NTP 服务器：有关表条目的信息，请参阅NTP 服务器状态，第 98 页。

NTP 服务器状态

如果要从 NTP 服务器同步时间，则可以在 **时间** 页面（选择 **系统 > 配置**）上查看连接状态。

表 *4: NTP* 状态

列	Description
NTP 服务器	已配置的 NTP 服务器的 IP 地址或名称。

列	Description
状态	NTP 服务器时间同步的状态。 • **已在使用 (Being Used)** 表示设备已与 NTP 服务器同步。 • **可用 (Available)** 表示 NTP 服务器可供使用，但时间尚未同步。 • **不可用 (Not Available)** 表示 NTP 服务器在您的配置中，但 NTP 后台守护程序无法使用该服务器。 • **待定 (Pending)** 表示 NTP 服务器是新的或 NTP 后台守护程序最近重新启动过。随着时间的推移，此选项的值应更改为**已在使用 (Being Used)**、**可用 (Available)** 或**不可用 (Not Available)**。 • **未知 (Unknown)** 表示 NTP 服务器的状态未知。
身份验证	管理中心 与 NTP 服务器之间通信的身份验证状态： • **无** 表示未配置身份验证。 • **不良** 表示已配置身份验证，但失败。 • **确认** 表示身份验证成功。 如果已配置身份验证，系统会在状态值后面显示密钥编号和密钥类型（SHA-1、MD5 或 AES-128 CMAC）。例如： **bad**、**key 2**、**MD5**。
偏移 (Offset)	设备时间与已配置的 NTP 服务器上时间所相差的毫秒数。负值表示设备时间晚于 NTP 服务器，正值表示设备时间早于 NFP 服务器。
上次更新 (Last Update)	自上次与 NTP 服务器同步时间以来过去的秒数。NTP 后台守护程序会根据若干条件自动调整同步时间。例如，如果显示更长的更新时间（例如 300 秒），表示时间相对稳定，这样，NTP 后台守护程序将会确定不需要使用更小的更新增量。

时间同步

要使系统成功运行，必须在Cisco Secure Firewall Management Center (管理中心) 及其受管设备上同步系统时间。我们建议您在 管理中心 初始配置期间指定 NTP 服务器，但您可以在初始配置完成后使用此部分中的信息建立或更改时间同步设置。

请使用网络时间协议 (NTP) 服务器在 管理中心 和所有设备上同步系统时间。 管理中心 支持使用 MD5、SHA-1 或 AES-128 CMAC 对称密钥认证与 NTP 服务器进行安全通信；为了系统安全，我们建议使用此功能。

管理中心还可以将配置为仅连接经过身份验证的NTP服务器；使用此选项可提高混合身份验证环境中或将系统迁移到不同 NTP 服务器时的安全性。在对所有可访问的 NTP 服务器进行身份验证的环境中使用此设置是多余的。

注释 如果在初始配置期间为 管理中心 指定了 NTP 服务器，则与该 NTP 服务器的连接不会受到保护。您必须编辑该连接的配置，以指定 MD5、SHA-1 或 AES-128 CMAC 密钥。

注意 如果 管理中心和受管设备之间的时间不同步，会导致意外后果。

要同步 管理中心 和托管设备上的时间，请参阅：

- 推荐： 将管理中心上的时间与 NTP 服务器同步，第 100 页

  本主题提供有关将 管理中心 配置为与一台或多台 NTP 服务器同步的说明，并包含有关将受管设备配置为与同一台或多台 NTP 服务器同步的说明的链接。

- 否则： 同步时间但不访问网络 NTP 服务器，第 102 页

  本主题提供有关设置 管理中心上的时间、配置 管理中心 以用作 NTP 服务器的说明，以及有关配置受管设备以与 管理中心 NTP 服务器同步的说明的链接。

将管理中心上的时间与 NTP 服务器同步

系统的所有组件之间的时间同步至关重要。

确保 管理中心和所有受管设备之间正确同步时间的最佳方式是使用网络上的 NTP 服务器。

管理中心 支持 NTPv4。

您必须具有管理员或网络管理员权限才能执行此程序。

开始之前

请注意以下提示：

- 如果 管理中心 和托管设备无法访问网络 NTP 服务器，请不要使用此程序。参阅同步时间但不访问网络 NTP 服务器，第 102 页。
- 请勿指定不受信任的 NTP 服务器。
- 如果您计划与 NTP 服务器建立安全连接（建议用于系统安全），请获取该 NTP 服务器上配置的 SHA-1、MD5 或 AES-128 CMAC 密钥编号和值。
- 与 NTP 服务器之间的连接不使用已配置的代理设置。
- Firepower 4100 系列设备和 Firepower 9300 设备无法使用此程序设置系统时间。相反，请将这些设备配置为使用您使用此程序配置的相同 NTP 服务器。有关说明，请参阅硬件型号对应的文档。

注意 如果 管理中心已重新启动，并且 DHCP 服务器设置了不同于您在这里指定的记录的 NTP 服务器记录，则会使用 DHCP 提供的 NTP 服务器。为避免这种情况，请将 DHCP 服务器配置为会使用相同的 NTP 服务器。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Time Synchronization**。

步骤 3 如果**通过 NTP 提供时间 (Serve Time via NTP)** 处于**已启用 (Enabled)** 状态，请选择**已禁用 (Disabled)** 以禁用管理中心作为 NTP 服务器。

步骤 4 对于“**设置我的时钟**”选项，选择“**通过 NTP**”。

步骤 5 点击“**添加**”。

步骤 6 在“**添加 NTP 服务器**”对话框中，输入 NTP 服务器的主机名或 IPv4 或 IPv6 地址。

步骤 7 （可选）要保护您的 管理中心 与 NTP 服务器之间的通信，请执行以下操作：

a) 从“**密钥类型**”下拉列表中选择 **MD5**、**SHA-1** 或 **AES-128 CMAC**。

b) 输入指定的 NTP 服务器对应的 MD5、SHA-1 或 AES-128 CMAC **密钥号**和**密钥值**。

步骤 8 点击“**添加**”。

步骤 9 当仅配置两个 NTP 服务器时，它们之间的偏移量差异会很大。这将导致 管理中心 使用本地时间。因此，我们建议您配置至少三个 NTP 服务器。

要添加更多 NTP 服务器，请重复步骤 5 至 8。

步骤 10 （可选）要强制 管理中心 仅使用成功进行身份验证的NTP服务器，请选中“**仅使用经过身份验证的 NTP 服务器**”复选框。

步骤 11 点击**保存 (Save)**。

下一步做什么

将受管设备设置为与同一台 NTP 服务器或服务器同步：

- 配置设备平台设置：在 《Cisco Secure Firewall Management Center 设备配置指南》中为威胁防御配置 NTP 时间同步。

  请注意，即使您强制 管理中心 与 NTP 服务器建立安全连接（**仅使用经过身份验证的 NTP 服务器**），与该服务器的设备连接也不使用身份验证。

- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

同步时间但不访问网络 NTP 服务器

如果设备无法直接访问网络 NTP 服务器，或您的组织没有网络 NTP 服务器，可使用物理硬件管理中心来充当 NTP 服务器。

重要事项

- 除非没有其他 NTP 服务器，否则请勿使用此程序。相反，请使用 将管理中心上的时间与 NTP 服务器同步，第 100 页 中的程序。
- 不要将虚拟 管理中心 用作 NTP 服务器。

将 管理中心配置为NTP服务器**之后**，则要手动更改时间，则必须先禁用NTP选项，手动更改时间，然后重新启用 NTP 选项。

过程

步骤 1 在 管理中心上手动设置系统时间：

a) 选择**系统**（⚙）> **配置**。
b) 点击 **Time Synchronization**。
c) 如果**通过 NTP 提供时间 (Serve Time via NTP)** 处于**已启用 (Enabled)** 状态，请选择**已禁用 (Disabled)**。
d) 点击**保存 (Save)**。
e) 对于**设置我的时钟**，选择**在本地配置中手动设置**。
f) 点击**保存 (Save)**。
g) 在屏幕左侧的导航窗格中，点击**时间**。
h) 使用**设置时间 (Set Time)** 下拉列表设置时间。

注释 当您在管理中心上更改时间超过两个小时时，必须尽快重新启动设备，例如在维护窗口中，以避免任何故障。

i) 如果显示的时区不是 UTC，请点击该时区，并将时区设置为 **UTC**。
j) 点击**保存 (Save)**。
k) 点击 **Done**。
l) 点击 **Apply**。

步骤 2 设置 管理中心作为 NTP 服务器：

a) 在屏幕左侧的导航窗格中，点击**时间同步**。
b) 对于**通过 NTP 提供时间**，选择**已启用**。
c) 点击**保存 (Save)**。

步骤 3 设置受管设备，以便与 管理中心 NTP 服务器同步：

a) 在分配给托管设备的平台设置策略的“时间同步”设置中，将时钟设置为**通过管理中心的 NTP** 同步。

b) 将更改部署到托管设备。

说明：

对于 威胁防御 设备，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的为威胁防御配置 *NTP* 时间。

关于更改时间同步设置

- 管理中心 管理中心及其托管设备高度依赖准确的时间。系统时钟是维护系统时间的系统设施。系统时钟设置为协调世界时 (UTC)，它是全球规定时钟和时间的主要时间标准。

  请勿尝试更改系统时间。不支持从UTC更改系统时区，而执行此操作将需要您重新映像设备以从不支持的状态中恢复。

- 如果将管理中心配置为使用 NTP 提供时间，然后又将其禁用，受管设备上的 NTP 服务仍会尝试与管理中心同步时间。必须更新并重新部署任何适用的平台设置策略，以建立新的时间源。

- 将 管理中心配置为 NTP 服务器**之后**，则要手动更改时间，则必须先禁用 NTP 选项，手动更改时间，然后重新启用 NTP 选项。

UCAPL/CC 合规性

组织只能使用符合由美国国防部和全球认证组织制定的安全标准的设备和软件。有关此设置的详细信息，请参阅安全认证合规性模式，第 311 页。

升级配置

策略属性、对象或其他设备配置可能会在 管理中心 升级过程中发生更改。默认情况下，将 管理中心 升级到主要版本可能会启用某些功能。 **升级配置** 设置允许您在完成 管理中心的下一个主要版本升级时生成待处理的配置更改报告。此报告显示升级后待部署在受管设备上的策略和设备配置更改。管理中心 升级完成后，选择 **消息中心** > **任务** 以下载报告。

待处理的配置更改报告包括：

- **比较视图**：将待部署在受管设备上的所有升级后配置更改与当前设备配置进行比较。
- **高级视图**：使用 CLI 预览待处理的配置更改。

有关待处理配置更改报告的详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 部署预览 。

启用升级后报告

在 管理中心的下一个主要版本升级后，生成要在托管设备上部署的待定配置更改报告。

过程

步骤 1 选择 **系统**（⚙）> **配置**

步骤 2 选中 **启用升级后报告** 复选框以启用该选项。

报告在 管理中心的下一次主要版本升级后生成。此选项会在升级后为所有受管设备生成报告，生成报告所需的时间取决于配置的大小和受管设备的数量。

步骤 3 点击**保存 (Save)**。

用户配置

全局用户配置设置影响 管理中心上的所有用户。在“用户配置”(User Configuration) 页面 (**系统**（⚙）> **配置** > **用户配置**) 上配置以下设置：

- **密码重用限制**：用户最近历史记录中无法重复使用的密码数量。此限制适用于所有用户的 Web 界面访问。对于管理员用户，此限制还适用于CLI访问；系统为每种访问形式保留单独的密码列表。将限制设置为零（默认值）不会对密码重用执行任何限制。请参阅设置密码重用限制，第 105 页。
- **跟踪成功登录次数 (Track Successful Logins)**：系统会跟踪每个用户通过每种访问方法（Web 界面或CLI）成功登录到 管理中心 的天数 。用户登录后，系统会显示正在使用的接口的成功登录次数。将**跟踪成功登录次数**设置为零（默认值）时，系统不会跟踪或报告成功的登录活动。请参阅跟踪成功登录，第 105 页。
- **最大登录失败次数**：当系统在可配置时间段内临时阻止账户访问之前，用户可以连续输入错误的 Web 界面登录凭证的次数。如果用户在临时锁定生效时继续登录尝试：
  - 系统将在不通知用户临时锁定生效的情况下拒绝访问此账户（即使使用有效密码）。
  - 每次登录尝试时，系统都会继续增加此账户的失败登录次数。
  - 如果用户超过在单个“用户配置”页面上为此账户配置的**最大失败登录次数**，则在管理员用户重新激活此账户之前，此账户将处于锁定状态。
- **设置临时锁定用户的时间（分钟）： 最大失败登录次数**不为零时临时 Web 界面用户锁定的持续时间（分钟）。
- **允许的最大并发会话数 (Max Concurrent Sessions Allowed)**：可以同时打开的特定类型（只读或读/写）会话数。会话类型由分配给用户的角色决定。如果只为用户分配了只读角色，则该用户的会话会计入（**只读**）会话限制。如果用户具有任何具有写入权限的角色，则会话计入**读/写**会

话限制。例如，如果为用户分配了“管理员”(Admin) 角色，并且**具有读/写权限的用户/CLI 用户的最大会话数**设置为5，则如果已经有五个其他用户登录，则不允许该用户登录。读/写权限。

注释 出于并发会话限制的目的，系统将预定义用户角色和自定义用户角色视为只读，并在 **系统**（⚙）> **用户** > **用户** 和 **系统**（⚙）> **用户** > **用户角色** 上的角色名称中标有（**只读**）。如果用户角色的角色名称中不包含（**只读**），则系统认为该角色为读/写。系统会自动将（**只读**）应用于满足所需条件的角色。不能通过将该文本字符串手动添加到角色名称来将角色设置为只读。

对于每种类型的会话，可以设置从 1 到 1024 的最大限制。当**允许的最大并发会话数 (Max Concurrent Sessions Allowed)** 被设为零（默认值）时，并发会话数不受限制。

如果将并发会话限制更改为更严格的值，系统将不会关闭任何当前打开的会话；但是，它会阻止打开超过指定数量的新会话。

设置密码重用限制

如果启用**密码重用限制 (Password Reuse Limit)**，则系统会为 管理中心 用户保留加密的密码历史记录。用户无法重复使用其历史记录中的密码。您可以为每个用户、每种访问方法（Web接口或CLI）指定存储的密码数量。用户的当前密码会计入此数字。如果降低限制，系统将从历史记录中删除旧密码。增加限制不会恢复已删除的密码。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**用户配置**。

步骤 3 将**密码重用限制**设置为您希望在历史记录中保留的密码数量（最大值为 256）。

要禁用密码重用检查，请输入 0。

步骤 4 点击**保存 (Save)**。

跟踪成功登录

使用此程序可以在指定的天数内为每个用户跟踪成功登录次数。启用此跟踪功能后，系统会在用户登录 Web 界面或 CLI 时显示成功登录次数。

注释 如果减少天数，系统将删除较旧的登录记录。如果随后增加限制，系统不会恢复已删除天数中的登录次数。在这种情况下，报告的成功登录次数可能暂时低于实际次数。

过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 点击**用户配置**。

步骤 3 将**跟踪成功登录天数**设置为跟踪成功登录的天数（最大值为 365）。

要禁用登录跟踪，请输入 0。

步骤 4 点击**保存 (Save)**。

启用临时锁定

通过指定在锁定生效之前系统允许的连续失败登录尝试次数，来启用临时定时锁定功能。

过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 点击**用户配置**。

步骤 3 将**最大登录失败次数**设置为临时锁定用户之前最大连续失败登录尝试次数。

要禁用临时锁定，请输入 0。

步骤 4 将**临时锁定用户的时间**（**分钟**）设置为锁定已触发临时锁定的用户的分钟数。

当此值为零时，即使**最大登录失败次数**不为零，用户也不必等待重新尝试登录。

步骤 5 点击**保存 (Save)**。

设置最大并发会话数

可以指定可同时打开的特定类型（只读或读/写）会话的最大数量。会话类型由分配给用户的角色决定。如果为用户分配了只读角色，则该用户的会话计入**只读**会话限制。如果用户具有任何具有写入权限的角色，则会话计入**读/写**会话限制。

过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 点击**用户配置**。

步骤 3 对于每种类型的会话（**只读** 和 **读/写**），将 **允许的最大并发会话数** 设置为可同时打开的该类型会话的最大数量。

要按会话类型对并发用户不应用限制，请输入零。

注释 如果将并发会话限制更改为更严格的值，系统将不会关闭任何当前打开的会话；但是，它会阻止打开超过指定数量的新会话。

步骤 4 点击**保存 (Save)**。

VMware 工具

VMware 工具是专为虚拟机而设计的一套性能增强实用工具。通过这些实用工具，您可以充分利用 VMware 产品方便的功能。在 VMware 上运行的 Firepower 虚拟设备支持以下插件：

- guestInfo
- powerOps
- timeSync
- vmbackup

也可以在所有受支持的 ESXi 版本上启用 VMware 工具。有关 VMware 工具全部功能的信息，请参阅 VMware 网站 (http://www.vmware.com/)。

在面向VMware的CiscoSecureFirewallManagementCenter上启用VMware工具

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **VMware 工具 (VMware Tools)**.

步骤 3 点击**启用 VMware 工具 (Enable VMware Tools)**。

步骤 4 点击**保存 (Save)**。

漏洞映射

当服务器在发现事件数据库中拥有应用 ID 且流量的数据包报头包含供应商和版本时，系统会针对从主机 IP 地址收到或发送的所有应用协议流量自动将漏洞映射到该地址。

对于在数据包中不包含供应商或版本信息的服务器，可以将系统配置为是否针对这些无供应商和版本信息的服务器将漏洞与服务器流量关联。

例如，在某一主机提供的 SMTP 流量中，其报头不含供应商或版本号。如果在系统配置的“漏洞映射”页面上启用 SMTP 服务器，然后将该配置保存到管理检测到流量的设备的 管理中心，则所有与 SMTP 服务器关联的漏洞都将被添加到该主机的主机配置文件。

尽管检测器会收集服务器信息并将其添加到主机配置文件中，但应用协议检测器不会用于漏洞映射，因为您无法为自定义的应用协议检测器指定供应商或版本，同时也无法为漏洞映射选择服务器。

映射服务器漏洞

此程序需要任何智能许可证或保护经典许可证。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 选择**漏洞映射 (Vulnerability Mapping)**。

步骤 3 有以下选项可供选择：

- 要阻止服务器的漏洞被映射到接收不含供应商或版本信息的应用协议流量的主机上，请为相应服务器清除此复选框。
- 要使服务器的漏洞映射到接收不含供应商或版本信息的应用协议流量的主机上，请选中该服务器对应的复选框。

提示　可以使用**已启用 (Enabled)** 旁边的复选框一次性选中或清除所有复选框。

步骤 4 点击**保存 (Save)**。

Web 分析

默认情况下，为了改善Firepower产品，思科会收集非个人可识别的使用数据，包括但不限于页面交互、浏览器版本、产品版本、用户位置，以及 管理中心 设备的管理 IP 地址或主机名。

接受最终用户许可协议后开始收集数据。如果您不希望思科继续收集这些数据，可以在升级后选择退出。

过程

步骤 1 依次选择**系统 > 配置**。

步骤 2 点击 **Web 分析**。

步骤 3 进行选择，然后点击**保存**。

下一步做什么

（可选）确定是否通过 配置 Cisco Success Network 注册来共享数据。

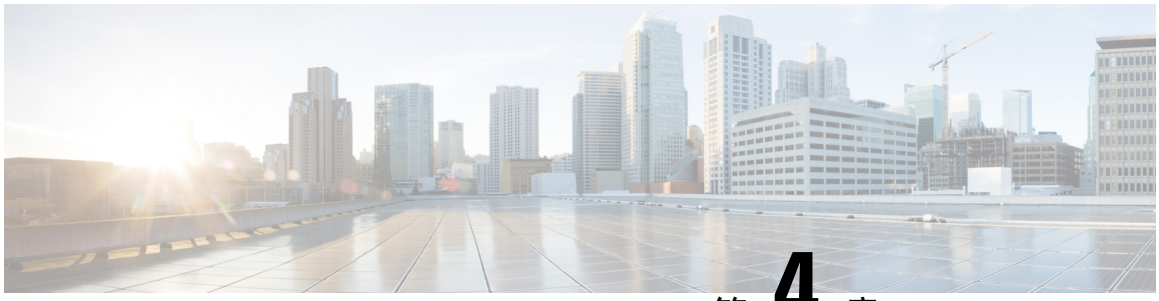
系统配置的历史记录

功能	最低 管理中心	最低 威胁防御	详情
启用升级后报告	7.4.1	任意	现在，您可以选择在 Cisco Secure Firewall Management Center 的下一个主要版本升级后，生成要在托管设备上部署的待定配置更改报告。 新增/经修改的屏幕：**系统**（⚙）> **配置 (Configuration)** > **升级配置 (Upgrade Configuration)**。 最低威胁防御版本：任意
访问控制性能改进（对象优化）。	7.2.4 7.4.0	任意	**升级影响。管理中心升级到 7.2.4 – 7.2.5 或 7.4.0 后的首次部署可能需要很长时间，并会增加托管设备上的 CPU 使用率。** 当具有重叠网络的访问控制规则时，访问控制对象优化可提高性能并消耗更少的设备资源。在管理中心启用该功能（包括是否通过升级启用）后，在首次部署时在托管设备上进行优化。如果您有大量规则，系统可能需要几分钟到一个小时来评估您的策略并执行对象优化。在此期间，您可能还会发现设备上的 CPU 使用率更高。禁用功能（包括是否通过升级禁用）后，在第一次部署时会发生类似的情况。启用或禁用该功能后，建议您在影响最小的时候部署，比如维护窗口或流量较低的时段。 新增/修改的屏幕 (需要版本 /7.4.1): **系统**（⚙）> **配置** > **f访问控制首选项** > **对象组优化**。 其他版本限制：不支持管理中心版本 7.3.x。
审核日志中的配置更改。	7.4	任意	您可以通过指定配置数据格式和主机，将配置更改作为审核日志数据的一部分传输到外部系统日志服务器。管理中心支持备份和恢复审核配置日志。管理中心高可用性设置中也支持此功能。 新增/修改的屏幕： **系统**（⚙）> **配置** > **审核日志**
法语选项。	7.2	任意	您现在可以将管理中心 Web 接口切换为法语。 新增/修改的屏幕： **系统**（⚙）> **配置** > **语言**。
对大多数连接事件免除事件速率限制。	7.0	任意	现在，将连接数据库的 **最大连接事件数** 值设置为零可免除低优先级连接事件，不计入 FMC 硬件的流量限制。以前，将此值设置为零仅适用于事件存储，不会影响流量限制。 新增/修改的屏幕： **系统**（⚙）> **配置** > **数据库** 支持的平台：硬件 FMC。

功能	最低 管理中心	最低 威胁防御	详情
支持 NTP 服务器的 AES-128 CMAC 认证。	7.0	任意	FMC 和 NTP 服务器之间的连接可以使用 AES-128 CMAC 密钥以及以前支持的 MD5 和 SHA-1 密钥进行保护。 新增/经修改的屏幕： **系统**（⚙） > **配置** > **时间同步**
Subject Alternative Name (SAN)。	6.6	任意	为 FMC 创建 HTTPS 证书时，可以指定 SAN 字段。如果证书确保多个域名或 IP 地址，我们建议您使用 SAN。有关详细信息，请参阅 RFC 5280 第 4.2.1.9 节。 新增/修改的屏幕： **系统**（⚙） > **配置** > **HTTPS 证书**
HTTPS 证书。	6.6	任意	目前，随系统一起提供的默认 HTTPS 服务器证书将在 800 天后自动到期。如果您的设备使用的是在升级到版本 6.6 之前生成的默认证书，则证书有效期因生成证书时使用的 Firepower 版本而异。有关详细信息，请参阅默认 HTTPS 服务器证书，第 60 页。 支持的平台：硬件 FMC。
安全 NTP。	6.5	任意	FMC 支持使用 SHA1 或 MD5 对称密钥身份验证与 NTP 服务器之间的安全通信。 新增/修改的屏幕： **系统**（⚙） > **配置** > **时间同步**
Web 分析。	6.5	任意	接受 EULA 后开始收集网络分析数据。和以前一样，您可以选择不继续共享数据。请参阅Web 分析，第 108 页。
适用于 FMC 的自动 CLI 访问。	6.5	任意	使用 SSH 登录 FMC 时，会自动访问 CLI。虽然强烈建议不要这样做，但您可以使用 CLI `专家` 命令访问 Linux 外壳程序。 **注释** 此功能弃用了为 FMC 启用和禁用 CLI 访问的版本 6.3。由于弃用此选项，虚拟 FMC 不再显示 **系统**（⚙） > **配置** > **控制台配置** 页面，该页面仍显示在物理 FMC 上。
只读和读/写访问的可配置会话限制。	6.5	任意	添加了 **允许的最大并发会话数** 设置。此设置允许管理员指定可同时打开的特定类型（只读或读/写）会话的最大数量。 **注释** 出于并发会话限制的目的，系统认为只读的预定义用户角色和自定义用户角色在 **系统**（⚙） > **用户** > **用户** 和 **系统**（⚙） > **用户** > **用户角色** 名称中标记为 （**只读**） 。如果用户角色的角色名称中不包含 （**只读**），则系统认为该角色为读/写。 新增/修改的屏幕： • **系统**（⚙） > **配置** > **用户配置** • **系统**（⚙） > **用户** > **用户角色**

功能	最低 管理中心	最低 威胁防御	详情
能够在管理接口上禁用重复地址检测 (DAD)。	6.4	任意	启用 IPv6 后，可以禁用 DAD。您可能希望禁用 DAD，因为使用 DAD 可能会导致拒绝服务攻击。如果禁用此设置，则需要手动检查此接口是否未使用已分配的地址。 新增/经修改的屏幕： **系统**（⚙）> **配置** > **管理接口** > **接口** > **编辑接口** > **IPv6 DAD** 支持的平台：FMC
能够在管理接口上禁用 ICMPv6 回应应答和目的地不可达消息。	6.4	任意	启用 IPv6 后，此时您可以禁用 ICMPv6 回应应答和目的地不可达消息。您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。禁用回应应答数据包意味着无法使用 IPv6 ping 到设备管理接口，以进行测试。 新增/经修改的屏幕： **系统**（⚙）> **管理接口** > **ICMPv6** 新增/修改的命令：**configure network ipv6 destination-unreachable**、**configure network ipv6 echo-reply** 支持的平台： FMC (仅限 web 接口)，FTD (仅限 CLI)
全局用户配置设置。	6.3	任意	添加了**跟踪成功登录次数**设置。系统可以跟踪每个 FMC 账户在选定天数内执行的成功登录次数。启用此功能后，用户登录后将看到一条消息，报告他们在过去所配置的天数内成功登录系统的次数。（适用于 Web 界面以及 shell/CLI 访问。） 添加了**密码重用限制**设置。系统可以跟踪每个账户的密码历史记录，以获得可配置的先前密码数量。系统会阻止所有用户重新使用此历史记录中显示的密码。（适用于 Web 界面以及 shell/CLI 访问。） 添加了**最大登录失败次数**和**设置临时锁定用户的时间**（**分钟**）设置。通过这些设置，管理员可以限制系统在可配置时间段内临时阻止账户之前用户可以连续输入错误的 Web 界面登录凭证的次数。 新增/经修改的屏幕： **系统**（⚙）> **配置** > **用户配置** 支持的平台：FMC
HTTPS 证书。	6.3	任意	目前，随系统一起提供的默认 HTTPS 服务器证书将在三年后自动到期。如果设备使用的是在升级到版本 6.3 之前生成的默认服务器证书，则此服务器证书将在首次生成之后的 20 年后到期。如果使用的是默认 HTTPS 服务器证书，则现在系统可以续订此证书。 新增/经修改的屏幕： **系统**（⚙）> **配置** > **HTTPS 证书** > **更新 HTTPS 证书** 支持的平台：FMC

功能	最低 管理中心	最低 威胁防御	详情
能启用和禁用CLI访问权限 FMC。	6.3	任意	FMC Web 接口中对管理员可用的新复选框： 在 **系统**（⚙）> **配置** > **控制台配置**上 **启用 CLI 访问** 。 • 选中：使用 SSH 登录 FMC 可访问 CLI。 • 取消选中：使用 SSH 登录 FMC 可访问 Linux 外壳。此为全新的 6.3 版本以及以往版本至 6.3 版本升级的默认状态。 在版本 6.3 之前，**控制台配置**页面上只有一项设置，它仅适用于物理设备。因此， **控制台配置** 页面在虚拟 FMC 上不可用。通过添加此新选项， **控制台配置** 页面现在显示在虚拟 FMC 和物理设备上。但是，对于虚拟 FMC，此复选框是页面上显示的唯一内容。 支持的平台：FMC



第 4 章

管理中心 的

管理中心 包括用于 Web 和 CLI 访问的默认 **管理员** 账户。本章介绍如何创建自定义用户帐户。有关使用用户帐户登录 管理中心 的详细信息，请参阅登录到管理中心，第 27 页。

关于用户

您可以在托管设备上作为内部用户添加自定义用户账号，也可以作为 LDAP 或 RADIUS 服务器上的外部用户添加自定义用户账号。每个托管设备单独维护用户账号。例如，将某个用户添加到 管理中心时，该用户只能访问管理中心；您不能使用该用户名直接登录受管设备。您必须单独在受管设备上添加用户。

内部和外部用户

托管设备支持两种用户类型：

- 内部用户 - 设备在本地数据库中检查用户。
- 外部用户 - 如果本地数据库中没有用户，则系统会查询外部 LDAP 或 RADIUS 身份验证服务器。

Web 接口和 CLI 访问

管理中心 具有 Web 接口、CLI（可从控制台（串行端口或键盘和显示器）访问或使用 SSH 访问管理界面）和 Linux 外壳。有关管理 UI 的详细信息，请参阅系统用户界面，第 29 页。

请参阅以下有关 FMC 用户类型及其可以访问的 UI 的信息：

- 管理员用户- 管理中心 支持两种不同的内部 **管理员** 用户：一种用于 Web 接口，另一种用于 CLI 访问。系统初始化过程会同步这两个 **管理员** 账户的密码，因此它们开始时相同，但由不同的内部机制跟踪，并且在初始配置后可能会出现分歧。有关系统初始化的详细信息，请参阅您的型号的 入门指南 。（要更改 Web 接口 **管理员**密码，请使用 **系统**（⚙） > **用户 (Users)** > **用户**。要更改 CLI **管理员**密码，请使用 管理中心 CLI 命令 **configure password**。）
- 内部用户 - 在 Web 界面中添加的内部用户仅具有 Web 接口访问权限。
- 外部用户 - 外部用户具有 Web 接口访问权限，您可以选择配置 CLI 访问权限。
- SSO 用户 - SSO 用户仅具有 Web 接口访问权限。

注意 CLI 用户可以使用 **expert** 命令访问 Linux 外壳。强烈建议您不要使用 Linux 外壳，除非 Cisco TAC 或 管理中心 文档明确说明需要这样做。CLI 用户可以获得 Linux 外壳中的 `sudoers` 权限，带来安全风险。出于系统安全原因，我们强烈建议：

- 限制具有 CLI 访问权限的用户列表。
- 请勿在 Linux 外壳中直接添加用户；请仅使用本章中的这些程序。

用户角色

CLI 用户角色

管理中心 上的 CLI 外部用户没有用户角色；他们可以使用所有可用命令。

Web 界面用户角色

用户权限以分配的用户角色为基础。例如，可以授予分析师预定义角色（如“安全分析师”和“发现管理员”），并为管理设备的安全管理员保留“管理员”角色。也可以创建具有根据贵组织需求定制的访问权限的自定义用户角色。

管理中心包括以下预定义的用户角色：

注释 出于并发会话限制的目的，系统将其视为只读的预定义用户角色在 **系统**（⚙） > **用户** > **用户** 和 **系统**（⚙） > **用户** > **用户角色**下的角色名称中标记为 （**只读**） 。如果用户角色的角色名称中不包含（**只读**）**(Read Only)**，则系统认为该角色为读/写。有关并发会话限制的详细信息，请参阅用户配置，第 104 页。

访问管理员

提供对**策略 (Policies)** 菜单中访问控制策略和关联功能的访问权限。“访问管理员”(Access Admin) 无法部署策略。

管理员

“管理员”有权访问所有产品信息；其会话如果受攻击会有更高安全风险，因此不能使其免于登录会话超时。

出于安全原因，应限制“管理员”(Administrator) 角色的使用。

发现管理员

提供对**策略 (Policies)** 菜单中网络发现、应用检测和关联功能的访问权限。“发现管理员”(Discovery Admin) 无法部署策略。

外部数据库用户（只有读取权限）

使用支持 JDBC SSL 连接的应用对数据库提供只读访问权限。如果第三方应用要向应用进行身份验证，必须在系统设置中启用数据库访问权限。在Web界面上，“外部数据库用户”(External Database User) 仅有权访问**帮助 (Help)** 菜单中与联机帮助相关的选项。由于此角色的功能不涉及 Web 界面，因此提供访问只是为便于支持和密码更改。

入侵管理员 **(Intrusion Admin)**

提供对**策略 (Policies)** 和**对象 (Objects)** 中所有入侵策略、入侵规则和网络分析策略功能的访问权限。“入侵管理员”(Intrusion Admin) 无法部署策略。

维护用户

提供对监控和维护功能的访问权限。“维护用户”(Maintenance User) 有权访问**运行状况 (Health)** 和**系统 (System)** 菜单中与维护相关的选项。

网络管理员

提供对**策略 (Policies)** 菜单中访问控制、SSL 检查、DNS 策略和身份策略功能以及**设备 (Devices)** 菜单中设备配置功能的访问权限。“网络管理员”(Network Admin) 可对设备部署配置更改。

安全分析师

提供对**概述 (Overview)**、**分析 (Analysis)**、**运行状况 (Health)** 和**系统 (System)** 菜单中安全事件分析功能的访问权限，以及对其中运行状况事件的只读访问权限。

Security Analyst (Read Only)

提供对**概述 (Overview)**、**分析 (Analysis)**、**运行状况 (Health)** 和**系统 (System)** 菜单中安全事件分析功能和运行状况事件的只读访问权限。

具有此角色的用户还可以：

- 从特定设备的运行状况监控页面，生成并下载故障排除文件。
- 在用户首选项下，设置文件下载首选项。
- 在用户首选项下，设置事件视图的默认时间段（**审核日志时间窗口**除外）。

安全审批人

提供对**策略 (Policies)** 菜单中访问控制和关联策略以及网络发现策略的访问权限。“安全审批人”(Security Approver) 可以查看和部署这些策略，但不能进行策略更改。

威胁情报导向器 (TID) 用户

提供对**情报**菜单中威胁情报导向器配置的访问。威胁情报导向器 (TID) 用户可以查看和配置 TID。

用户密码

以下规则适用于管理中心上启用或禁用无人值守管理(LOM)的内部用户账户的密码。不同的密码要求适用于外部身份验证的账户或启用了安全认证合规性的系统。有关详细信息，请参阅为管理中心配置外部身份验证，第 120 页和安全认证合规性，第 311 页。

在管理中心初始配置期间，系统要求**管理员**用户设置账户密码，以满足下表中所述的强密码要求。对于物理 管理中心，使用启用 LOM 的强密码要求；对于虚拟管理中心，使用未启用 LOM 的强密码要求。此时，系统会同步 Web 界面**管理员** 和 CLI 访问 **管理员**的密码。初始配置后，Web 界面**管理员**可以删除强密码要求，但 CLI 访问**管理员**必须始终遵守强密码要求，且未启用 LOM。

	未启用 LOM	已启用 LOM
密码强度检查开启	密码必须包含： • 至少八个字符，或管理员为用户配置的字符数，以较大者为准。 • 连续的重复字符数不超过两个 • 至少一个小写字母 • 至少一个大写字母 • 至少一位 • 至少一个特殊字符，例如 ！ @ # * - _ + 系统会将您的密码与密码破解词典进行比较，该词典不仅会检查许多英语词典单词，还会检查其他容易被常用密码破解技术破解的字符串。	密码必须包含： • 介于 8 到 20 个字符之间 （在 MC 1000、MC 2500 和 MC 4500 上，上限为 14 个字符，而不是 20 个字符。） • 连续的重复字符数不超过两个 • 至少一个小写字母 • 至少一个大写字母 • 至少一位 • 至少一个特殊字符，例如 ！ @ # * - _ + 不同系列的物理 管理中心 之间的特殊字符规则有所不同。我们建议您只选择上面最后一项中列出的特殊字符。 请勿在密码中包含用户名。 系统会将您的密码与密码破解词典进行比较，该词典不仅会检查许多英语词典单词，还会检查其他容易被常用密码破解技术破解的字符串。

	未启用 LOM	已启用 LOM

密码强度检查关闭	密码必须包含管理员为用户配置的最小字符数。（有关详细信息，请参阅 添加或编辑内部用户，第 118 页。）	密码必须包含：
		• 介于 8 到 20 个字符之间（在 MC 1000、MC 2500 和 MC 4500 上，上限为 14 个字符，而不是 20 个字符。）
		• 至少包含四种以下类别的字符：
		  • 大写字母
		  • 小写字母
		  • 数字
		  • 特殊字符，例如！@ # * - _ +
		不同系列的物理 管理中心 之间的特殊字符规则有所不同。我们建议您只选择上面最后一项中列出的特殊字符。
		请勿在密码中包含用户名。

管理中心用户帐户的指南和限制

- 管理中心 包括一个 **管理员** 用户用于所有形式的访问；您无法删除 **管理员** 用户。默认初始密码为 **Admin123**；系统会强制您在初始化过程中更改此设置。有关系统初始化的详细信息，请参阅您的型号的 入门指南 。
- 默认情况下，以下设置适用于 管理中心上的所有用户账户：
  - 重复使用密码方面没有限制。
  - 系统不会跟踪成功登录。
  - 系统不会为输入错误登录凭证的用户强制执行定时临时锁定。
  - 对可以同时打开的只读和读/写会话的数量没有用户定义的限制。

  您可以将所有用户的这些设置更改为系统配置。**(系统**（⚙）**> 配置 > 用户配置)** 请参阅 用户配置，第 104 页。
- 在初始设置时向用户分配默认访问角色时，请确保遵循最小权限原则。当用户首次使用其凭证登录系统时，他们的账户将被分配此默认访问角色。我们建议将默认访问角色设置为任何人登录系统所需的最低权限。例如，可以为常见用户提供“安全分析师（只读）”角色作为默认访问角色，并且可以将管理员添加到单独的管理员组以授予他们完全管理员权限。如果在分配默认访问角色时不遵循最小权限原则，则在后续登录时可能会为用户分配意外的权限级别。这可

能会导致用户拥有超出其所需访问角色的权限。请注意，此准则适用于所有用户 - 内部、外部或 CAC 用户。

如果使用默认访问角色登录的用户需要临时提升其权限，则具有管理权限的用户可以通过为其分配具有更高权限的角色来临时为其提供所需的更高级别的访问权限。此权限将在24小时不活动后撤销，并且用户将返回其默认访问角色。

如果用户需要将永久访问角色重新分配到更高权限级别（例如系统管理员），请使用“组控制访问角色”方法为用户提供管理员访问权限。此方法可确保提供的访问角色持续超过24小时，并且用户将根据组分配具有正确的权限级别。有关配置组控制访问角色的详细信息，请参阅为管理中心 步骤 15 部分。

FMC 用户帐户的前提条件和要求

型号支持

管理中心

支持的域

- SSO 配置 - 仅全局。
- 所有其他功能 - 任意。

用户角色

- SSO 配置 - 只有通过内部或通过 LDAP 或 RADIUS 进行身份验证的具有管理员角色的用户才能配置 SSO。
- 所有其他功能-具有管理员角色的任何用户。
- 使用 LDAP 配置通用访问卡身份验证 ， 第 135 页 还支持 网络管理员 角色。

添加或编辑内部用户

此程序介绍如何为 管理中心的 Web 界面中添加自定义内部用户账号。

系统 (System) > **用户 (Users)** > **用户 (Users)** 显示您手动添加的内部用户，以及用户使用 LDAP 或 RADIUS 身份验证登录时自动添加的外部用户。对于外部用户，如果分配具有较高权限的角色，可以在此屏幕上修改用户角色；不能修改密码设置。

在 管理中心上的多域部署中，用户仅在创建它们的域中可见。如果您在全局域中添加了一个用户并为其分配了分叶域的用户角色，则该用户仍显示在添加其的全局**用户**页面，尽管该用户属于分叶域。

如果在设备上启用安全认证合规性或无人值守管理 (LOM)，则适用不同的密码限制。有关安全认证合规性的详细信息，请参阅安全认证合规性 ， 第 311 页。

当您在分叶域中添加用户时，该用户在全局域中不可见。

注释 避免让多个管理员用户同时在 管理中心上创建新用户，因为这可能会因用户数据库访问冲突而导致错误。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 要创建新用户：

a) 点击**创建用户**。

b) 输入**用户名 (User Name)**。

用户名必须符合以下限制：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)。
- 字母可以是大写或小写。
- 不能包含除句号 (.) 、连字符 (-)和下划线 (_)和以外的任何标点或特殊字符。

步骤 3 要编辑现有用户，请点击要编辑的用户旁边的 **编辑**（✎） 图标。

步骤 4 **真实名称 (Real Name)**：输入描述性信息，以标识账户所属的用户或部门。

步骤 5 对于使用 LDAP 或 RADIUS 登录时自动添加的用户，**使用外部身份验证方法 (Use External Authentication Method)** 复选框已选中 。无需预配置外部用户，因此您可以忽略此字段。对于外部用户，通过取消选中此复选框，可以将此用户恢复为内部用户。

步骤 6 在**密码**和**确认密码**字段中输入值。

这些值必须符合您为此用户设置的密码选项。

步骤 7 设置**最大失败登录次数**。

输入不含空格的整数，用于指定每个用户在登录尝试失败后且帐户锁定之前可以尝试的最大次数。默认设置为五次尝试；使用 **0** 可允许无限次的登录失败。除非已启用安全认证合规性，否则**管理员**账户不会在达到最大失败登录次数后被锁定。

步骤 8 设置**最大密码长度**。

输入不含空格的整数，用于指定用户密码的最小所需长度（以字符数为单位）。默认设置为 **8**。值为 **0** 指示无需最小长度。

步骤 9 设置**密码到期前天数**。

输入用户密码到期之前经过的天数。默认设置为 **0**，指示密码永不过期。如果更改默认值，则**用户**列表的**密码生存期**列指示每个用户密码的剩余有效天数。

步骤 10 设置**密码过期前警告天数**。

输入在用户密码实际到期之前警告用户必须更改其密码的警告天数。默认设置为 0 天。

步骤 11 设置以下**选项**：

- **登录时强制密码重置 (Force Password Reset on Login)**：强制用户在下次登录时更改密码。
- **检查密码强度 (Check Password Strength)**：需要强密码。启用密码强度检查时，密码必须符合用户密码，第 116 页中所述的强密码要求。
- **免除浏览器会话超时 (Exempt from Browser Session Timeout)**：免除用户的登录会话因不活动而终止。具有管理员角色的用户无法获得豁免。

步骤 12 在**用户角色配置 (User Role Configuration)** 区域中分配用户角色。有关用户角色的详细信息，请参阅自定义 Web 界面的用户角色，第 185 页。

对于外部用户，如果通过组或列表成员身份用户角色，则无法删除最低访问权限。但是，可以分配其他权限。如果用户角色是您在设备上设置的默认用户角色，则可以在用户帐户中不受限制地修改角色。修改用户角色时，**用户**选项卡上的**身份验证方法**列提供**外部 - 本地修改**的状态。

显示的选项取决于设备是在单域还是多域部署中。

- 单域：查看要为用户分配的用户角色。
- 多域：在多域部署中，可以在已为您分配管理员访问权限的任何域中创建用户账号。用户在每个域中可拥有不同的权限。可以同时分配祖先域和后代域中的用户角色。例如，可以在全局域中为用户分配只读权限，但在后代域中分配管理员权限。请参阅以下步骤：

  1. 点击**添加域**。
  2. 从**域 (Domain)** 下拉列表中选择域。
  3. 选中要分配用户的用户角色。
  4. 点击**保存 (Save)**。

步骤 13 （可选，仅用于物理 管理中心）如果您为用户分配了管理员角色，系统将显示**管理员选项 (Administrator Options)**。您可以选择**允许无人值守管理访问 (Allow Lights-Out Management Access)** 以向用户授予无人值守管理访问权限。有关无人值守管理的详细信息，请参阅无人值守管理概述，第 90 页。

步骤 14 点击**保存 (Save)**。

为管理中心配置外部身份验证

要启用外部身份验证，您需要添加一个或多个外部身份验证对象。

关于管理中心外部身份验证

在为管理用户启用外部身份验证时，管理中心会使用外部身份验证对象中指定的LDAP或RADIUS服务器验证用户凭证。

您可以为Web界面访问配置多个外部身份验证对象。例如，如果您有5个外部身份验证对象，则其中任意对象的用户均可通过身份验证来访问Web界面。对于CLI访问，仅可使用一个外部身份验证对象。如果您启用了多个外部身份验证对象，用户仅可使用列表中的第一个对象进行身份验证。

管理中心 和 威胁防御 设备可使用外部身份验证对象。不同应用/设备可共享同一个对象，也可以为它们创建不同的对象。

注释 威胁防御 和 管理中心 的超时范围不同，因此，如果共享对象，请确保不要超过 威胁防御 的较小超时范围（对于 LDAP 为 1-30 秒，对于 RADIUS 为 1-300 秒）。如果将超时设置为更高的值，则 威胁防御 外部身份验证配置将不起作用。

对于管理中心，请直接在 **系统** > **用户** > **外部身份验证** 选项卡上启用外部身份验证对象；此设置仅会影响 管理中心 的使用情况，无需在此选项卡上为了受管设备的使用而启用此设置。对于 威胁防御 设备，必须在部署到设备的平台设置中启用外部身份验证对象。

Web界面用户由外部身份验证对象中的CLI用户单独定义。对于RADIUS上的CLI用户，您必须预配置外部身份验证对象中的RADIUS用户名列表。对于LDAP，您可以指定过滤器来匹配LDAP服务器上的CLI用户。

您无法将同时配置用于CAC身份验证的LDAP对象用于CLI访问。

注释 具有配置层级访问权限的用户可以使用CLI **expert** 命令访问Linux外壳程序。Linux外壳用户可以获得root权限，带来安全风险。确保：

- 限制具有CLI或Linux外壳访问权限的用户列表。
- 请勿创建Linux外壳用户。

关于 LDAP

通过轻量级目录访问协议(LDAP)，可以在网络上设置一个目录，用于在一个集中位置组织对象，如用户凭证。然后，多个应用可以访问这些凭证和用于描述凭证的信息。如果需要更改用户凭证，则可以在一个位置进行更改。

Microsoft 已宣布 Active Directory 服务器将在 2020 年开始实施 LDAP 绑定和 LDAP 签名。Microsoft 将这些作为一项要求，因为在使用默认设置时，Microsoft Windows 中存在一个权限提升漏洞，该漏洞可能允许中间人攻击者将身份验证请求成功转发到 Windows LDAP 服务器。有关详细信息，请参阅 Microsoft 支持站点上的 Windows 2020 LDAP 通道绑定和 LDAP 签名要求 。

如果您尚未执行此操作，我们建议您开始使用 TLS / SSL 加密对 Active Directory 服务器进行身份验证。

关于 RADIUS

远程身份验证拨入用户服务 (RADIUS) 是用于验证/授权和说明用户对网络资源的访问的一种身份验证协议。可以为符合 RFC 2865 的任何 RADIUS 服务器创建身份验证对象。

Firepower 设备支持使用 SecurID 令牌。使用 SecurID 通过服务器来配置身份验证时，利用该服务器进行身份验证的用户会将 SecurID 令牌追加到其 SecurID PIN 的末尾，并使用此代码作为其登录密码。在 Firepower 设备上无需配置任何其他信息来支持 SecurID。

添加 管理中心的 LDAP 外部身份验证对象

添加 LDAP 服务器以支持外部用户执行设备管理。

开始之前

- 您必须在设备上指定 DNS 服务器用于域名查找。即使您在此程序中为 LDAP 服务器指定了 IP 地址而非主机名，LDAP 服务器也可能返回可能包括主机名的身份验证 URI。解析主机名需要进行 DNS 查询。请参阅 修改 管理中心 管理接口，第 76 页 来添加 DNS 服务器。
- 如果是配置用于 CAC 身份验证的 LDAP 身份验证对象，请勿移除在计算机中插入的 CAC。启用用户证书后，必须一直插入 CAC。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击 **External Authentication** 选项卡。

步骤 3 点击添加图标 （+）**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 4 将**身份验证方法**设置为 **LDAP** 。

步骤 5 （可选） 如果计划将此身份验证对象用于 CAC 身份验证和授权，请勾选 **CAC** 的对应复选框。

此外，还必须遵循使用 LDAP 配置通用访问卡身份验证，第 135 页中的程序，才能完全配置 CAC 身份验证和授权。不能将此对象用于 CLI 用户。

步骤 6 在 **CAC 环境变量** 字段中，输入包含用于登录的用户名的环境变量。选中 **CAC** 复选框时，将显示此字段。启用 CAC 并使用浏览器访问设备后，可以使用包含 CAC 信息的环境变量进行登录。示例，`SSL_CLIENT_S_DN_CN = last.first.1234567890`

步骤 7 在**CAC 用户名模板**字段中，输入模板以从CAC环境变量中提取用户名部分。例如，输入`\.(\d{10})$`以提取 CAC 环境变量字符串的最后 10 位数字。

步骤 8 输入**名称**和可选**说明**。

步骤 9 从下拉列表中选择**服务器类型**。

提示 如果点击**设置默认值 (Set Defaults)**，设备将使用服务器类型的默认值填充**用户名模板 (User Name Template)**、**UI 访问属性 (UI Access Attribute)**、**CLI 访问属性 (CLI Access Attribute)**、**组成员属性 (Group Member Attribute)** 和**组成员 URL 属性 (Group Member URL Attribute)** 字段。

步骤 10 对于**主服务器**，输入**主机名/IP 地址**。

如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

步骤 11 （可选） 更改**端口**使用的默认值。

步骤 12 （可选） 输入**备份服务器**参数。

步骤 13 输入 **LDAP 特定参数**。

a) 在**基础 DN** 中为要访问的 LDAP 目录输入基础 DN。例如，要对 Example 公司的 Security 组织中的名称进行身份验证，请输入 `ou=security,dc=example,dc=com`。或者，点击**获取 DN (Fetch DNs)**，然后从下拉列表中选择相应的基本可分辨名称。

b) （可选） 输入**基本过滤器**。例如，如果目录树中的用户对象具有 `physicalDeliveryOfficeName` 属性，并且 New York 办公室中的用户对于该属性具有属性值 `NewYork`，要仅检索 New York 办公室中的用户，请输入 `(physicalDeliveryOfficeName=NewYork)`。

如果使用 CAC 身份验证，要仅过滤活动用户账号（禁用的用户账号除外），请输入 `(!(userAccountControl:1.2.840.113556.1.4.803:=2))`。此条件检索 AD 中属于 `ldpgrp` 组且 `userAccountControl` 属性值不为 `2` （已禁用）的用户账户。

c) 为有足够凭证浏览 LDAP 服务器的用户输入**用户名**。例如，如果是连接到 OpenLDAP 服务器，其中用户对象具有 `uid` 属性，并且 Example 公司 Security 部门的管理员对象的 `uid` 值为 `NetworkAdmin`，则您可以输入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。

d) 在**密码**和**确认密码**字段中输入用户密码。

e) （可选） 点击**显示高级选项**配置以下高级选项。

- **加密 (Encryption)** - 点击**无 (None)**、**TLS** 或 **SSL**。

  如果在指定端口后更改加密方法，则会将端口重置为该方法的默认值。对于**无**或 **TLS**，端口将重置为默认值 389。如果选择 SSL 加密，端口将重置为 636。

- **SSL 证书上传路径 (SSL Certificate Upload Path)** - 对于 SSL 或 TLS 加密，必须通过点击**选择文件 (Choose File)** 选择一个证书。

  要删除上传的证书，请选中**清除已加载证书 (Clear loaded certificate)** 复选框。此选项只有在上传了证书并处于外部身份验证对象的编辑模式时才会出现。

  如果之前已上传证书并要将其替换，请上传新证书并将该配置重新部署到设备，以复制转移新证书。

  注释 TLS 加密要求所有平台上均有证书。但我们建议您始终上传 SSL 证书以防中间人攻击。

- **用户名模板** - 提供与您的 **UI 访问属性**对应的模板。例如，要通过连接到 UI 访问属性为 `uid` 的 OpenLDAP 服务器来对 Example 公司的 Security 组织中工作的所有用户进行身份验证，可在**用户名模板**字段中输入 `uid=%s,ou=security,dc=example,dc=com`。对于 Microsoft Active Directory Server，可以输入 `%s@security.example.com`。

  CAC 身份验证需要使用此字段。

- **外壳用户名模板 (Shell User Name Template)** - 提供与您的 **CLI 访问属性 (CLI Access Attribute)** 对应的模板以进行 CLI 用户身份验证。例如，要通过连接到 CLI 访问属性为 `sAMAccountName` 的 OpenLDAP 服务器来对 Security 组织中工作的所有用户进行身份验证，可在**外壳用户名模板 (Shell User Name Template)** 字段中输入 `%s` 。
- **超时（秒）**-输入滚动到备份连接之前等待的秒数（1-1024 秒）。默认值为 30。

  注释 威胁防御 和 管理中心的超时范围不同，因此，如果共享对象，请确保不要超过 威胁防御的较小超时范围（1-30 秒）。如果将超时设置为更高的值，则 威胁防御 LDAP 配置将不起作用。

步骤 14 配置**属性映射 (Attribute Mapping)** 以基于属性检索用户。

- 输入 **UI 访问属性**或点击**获取属性**，以检索可用属性的列表。例如，在 Microsoft 活动目录服务器上，可能要使用 UI 访问属性检索用户，因为在 Active 目录服务器用户对象上可能没有 `uid` 属性。相反，可以通过在 **UI 访问属性 (UI Access Attribute)** 字段中输入 `userPrincipalName` 来搜索 `userPrincipalName` 属性。

  CAC 身份验证需要使用此字段。
- 如果要使用用户可分辨类型之外的外壳访问属性，请设置 **CLI 访问属性 (CLI Access Attribute)** 。例如，在 Microsoft 活动目录服务器上，通过键入 `sAMAccountName` 可使用 `sAMAccountName` CLI 访问属性来检索外壳访问用户。

步骤 15 （可选） 配置**组控制的访问角色**。

如果不使用组控制的访问角色配置用户权限，则用户仅具有外部身份验证策略默认授予的权限。

a) （可选） 在与用户角色对应的字段中，输入包含应向其分配这些角色的用户的 LDAP 组的可分辨名称。

   引用的任何组都必须存在于 LDAP 服务器上。可以引用静态 LDAP 组或动态 LDAP 组。静态 LDAP 组是成员身份由指向特定用户的组对象属性确定的组，动态 LDAP 组是通过创建根据用户对象属性检索组用户的 LDAP 搜索来确定成员身份的组。角色的组访问权限仅影响身为组成员的用户。

   如果使用动态组，则完全按照 LDAP 查询在 LDAP 服务器上的配置来使用 LDAP 查询。因此，Firepower 设备将搜索的递归数限制为 4，以防搜索语法错误导致无限循环。

   示例：

   在**管理员**字段中输入以下内容，以便对 Example 公司信息技术部门中的名称进行身份验证：

   ```
   cn=itgroup,ou=groups, dc=example,dc=com
   ```

b) 对于不属于任何指定组的用户，选择**默认用户角色**。
c) 如果使用静态组，请输入**组成员属性 (Group Member Attribute)**。

   示例：

   如果使用 `member` 属性指示默认“安全分析师”访问权限静态组中的成员身份，请输入 `member`。

d) 如果使用动态组，请输入**组成员 URL 属性 (Group Member URL Attribute)**。

示例：

如果 `memberURL` 属性包含用于检索为默认“管理员”访问权限指定的动态组成员的 LDAP 搜索，请输入 `memberURL`。

如果更改用户的角色，必须保存/部署更改的外部身份验证对象，并从**用户**屏幕中移除该用户。该用户下次登录时会自动被重新添加。

步骤 16 （可选） 设置 **CLI 访问过滤器 (Shell Access Attribute)** 以允许 CLI 用户。

为防止对 CLI 访问进行 LDAP 身份验证，请将此字段留空。要指定 CLI 用户，请选择以下方法之一：

- 要使用配置身份验证设置时指定的同一过滤器，请选中 **与基本过滤器相同**复选框。
- 要根据属性值检索管理用户条目，请输入要用作过滤器的属性名、比较运算符和属性值（用括号括起来）。例如，如果所有网络管理员都具有属性值为 `shell` 的 `manager` 属性，则可以设置基本过滤器 `(manager=shell)`。

用户名必须对 Linux 有效：

- 最多 32 个字母数字字符，外加句号 (.)、 连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含 at 符号 (@) 或斜线 (/)

注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。请确保限制具有 CLI 或 Linux 外壳访问的用户列表。

注释 请勿创建与包括在 **CLI 访问过滤器 (CLI Access Filter)** 中的用户具有相同用户名的任何内部用户。唯一的内部 管理中心 用户应为 **admin**；请勿在 **CLI 访问过滤器 (CLI Access Filter)** 中包含**管理员**用户。

步骤 17 （可选） 点击**测试**以测试与 LDAP 服务器的连接状况。

测试输出列出有效和无效的用户名。有效用户名是唯一的，并且可以包含下划线 (_)、句号 (.)、连字符 (-) 和字母数字字符。请注意，受 UI 页面大小限制，测试与具有 1000 个以上用户的服务器的连接仅会返回 1000 个用户。如果测试失败，请参阅LDAP 身份验证连接故障排除，第 190 页。

步骤 18 （可选） 此外，还可以输入**其他测试参数**来测试应可以执行身份验证的用户的用户凭证：输入**用户名** `uid` 和**密码**，然后点击**测试**。

如果是连接到 Microsoft Active Directory Server 并提供 UI 访问属性来代替 `uid`，请使用该属性的值作为用户名。还可以为用户指定完全限定的可分辨名称。

提示 如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。要验证服务器配置是否正确，请点击**测试**，而无需首先在**其他测试参数**字段中输入用户信息。如果成功，请提供要通过特定用户进行测试的用户名和密码。

示例：

要测试是否可以在 Example 公司检索到 `JSmith` 用户凭证，请输入 `JSmith` 和正确的密码。

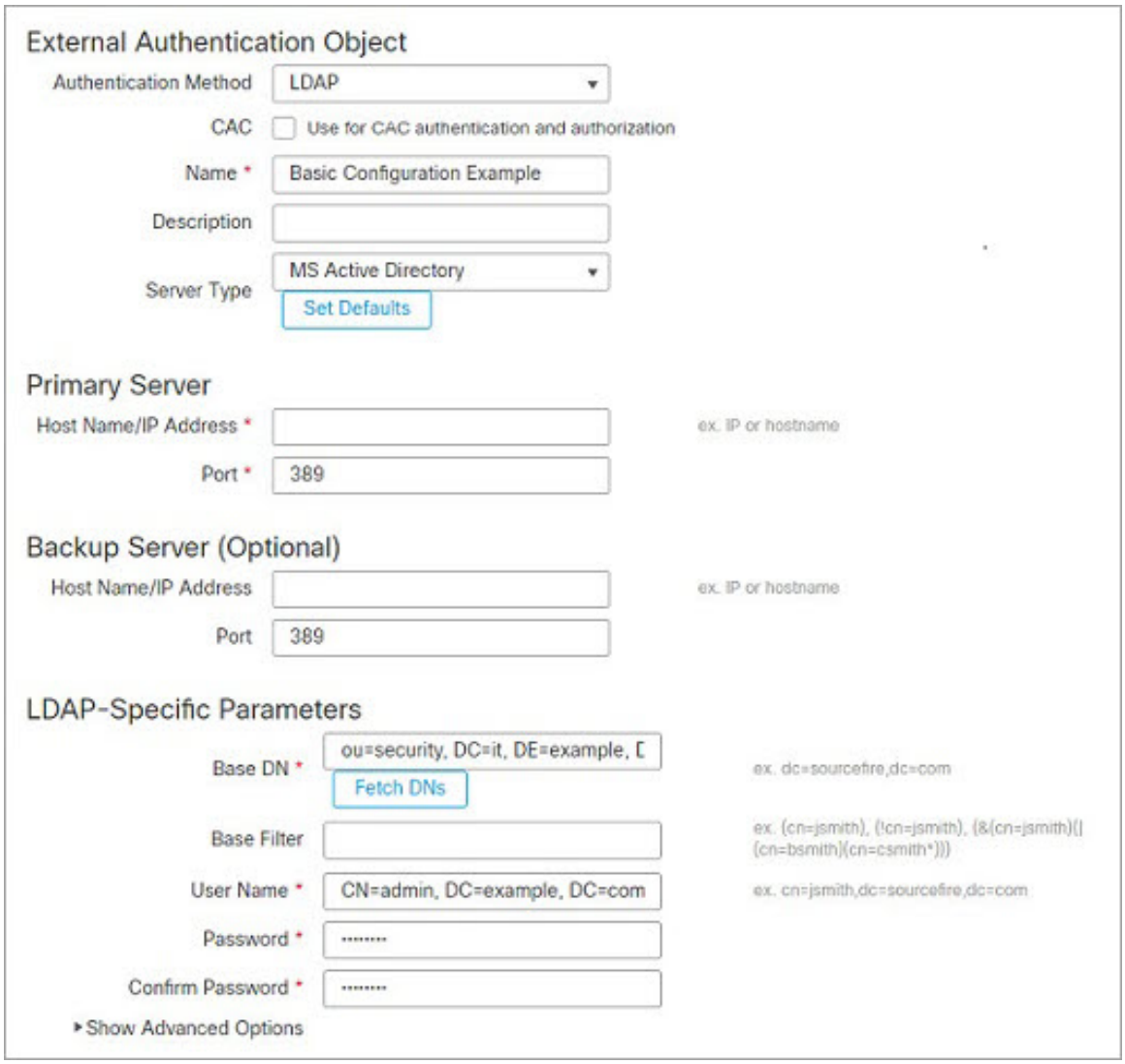
步骤 19 点击**保存 (Save)**。

步骤 20 启用此服务器。请参阅为管理中心上的用户启用外部身份验证，第 134 页。

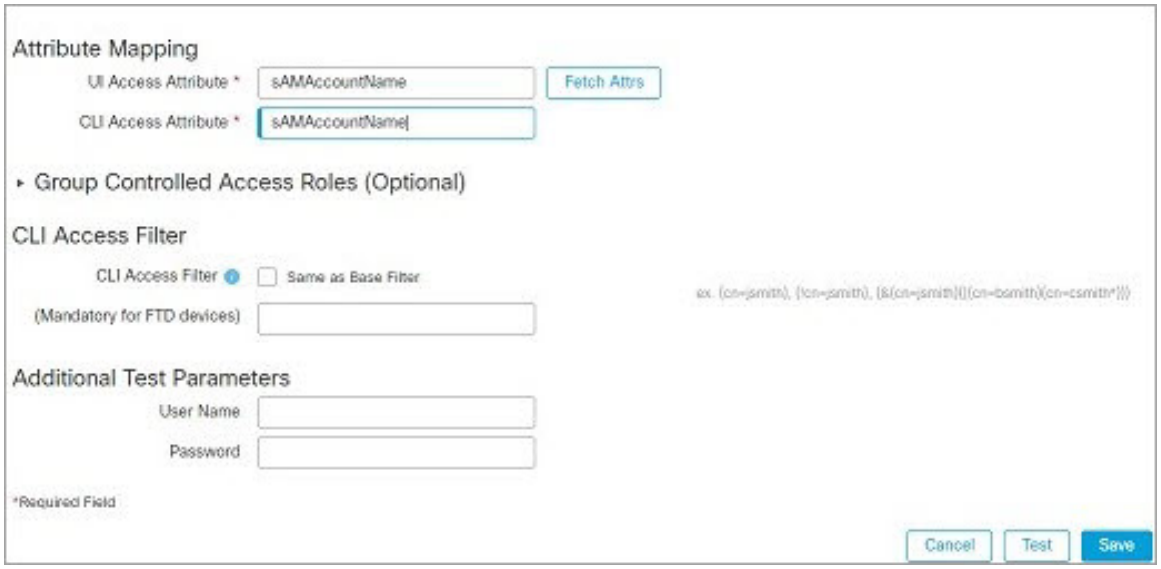
示例

基本示例

下图说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的基本配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 389 进行访问。



此示例显示对于示例公司的信息技术领域中的安全组织使用基本可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。



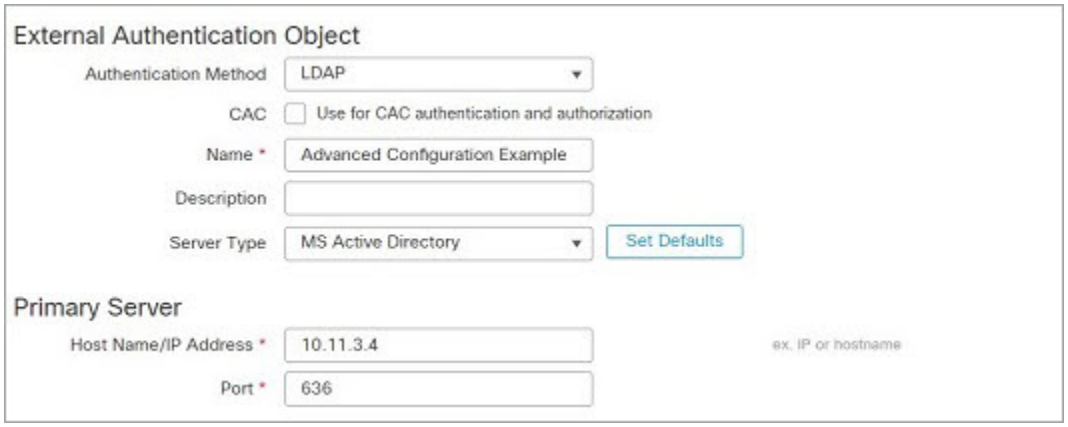
但是，由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。选择 MS Active Directory 服务器类型并点击**设置默认值 (Set Defaults)** 会将“UI 访问属性”(UI Access Attribute) 设置为 `sAMAccountName`。因此，当用户尝试登录系统时，系统会检查各对象的 `sAMAccountName` 属性以查找匹配的用户名。

此外，当用户登录到设备上的 CLI 账户中时， `sAMAccountName` 的 CLI会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

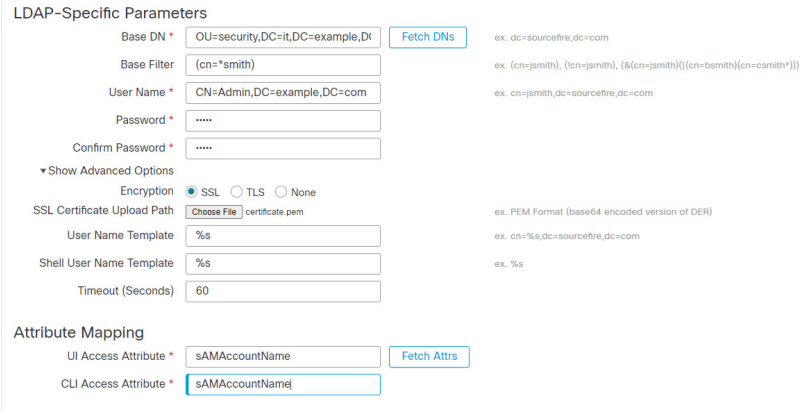
请注意，由于未对此服务器应用基本过滤器，因此系统会检查目录中基本可分辨名称所指示的所有对象的属性。经过默认时间段（或 LDAP 服务器上设置的超时期）后，与服务器的连接将超时。

高级示例

此示例说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的高级配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 636 进行访问。



此示例显示对于示例公司的信息技术领域中的安全组织使用基本可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。但请注意，此服务器具有基本过滤器 `(cn=*smith)`。该过滤器将从服务器检索到的用户限制为公用名称以 `smith` 结尾的用户。

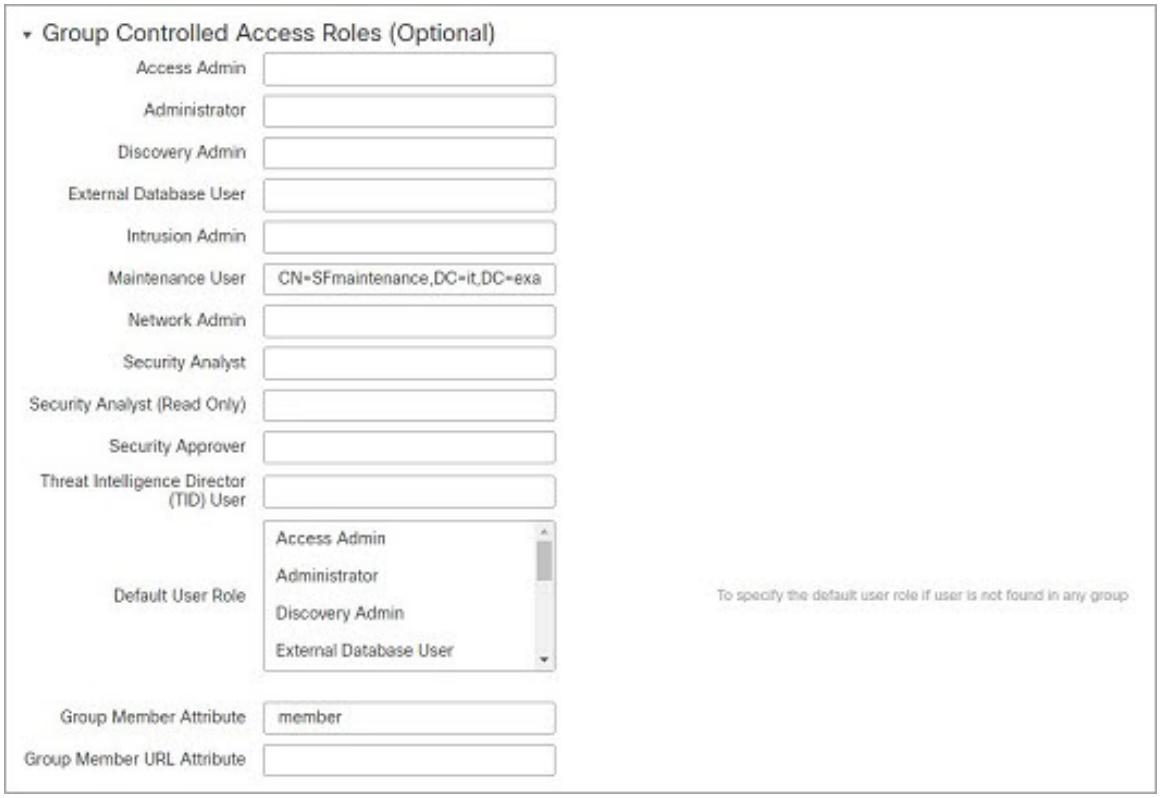


与服务器的连接使用 SSL 进行加密，并且会为该连接使用一个名为 `certificate.pem` 的证书。此外，由于 **超时（秒）** 设置，与服务器的连接在 60 秒后将超时。

由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。请注意，配置包括 `sAMAccountName`的 **UI 访问属性 (UI Access Attribute)**。因此，当用户尝试登录系统时，系统会检查各对象的 `sAMAccountName` 属性以查找匹配的用户名。

此外，当用户登录到设备上的 CLI 账户中时， `sAMAccountName` 的 **CLI 访问属性** 会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

此示例还具有相应的组设置。“维护用户”角色将被自动分配给具有成员组属性且基本域名为 `CN=SFmaintenance,DC=it,DC=example,DC=com` 的组的所有成员。



CLI 访问过滤器 设置为与基本过滤器相同，因此相同用户可以通过 CLI 访问设备，如同通过 web 接口进行访问一样。

添加管理中心的 RADIUS 外部身份验证对象

添加 RADIUS 服务器以支持外部用户执行设备管理。

在多域部署中，外部身份验证对象仅在创建对象的域中可用。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击**外部身份验证 (External Authentication)**。

步骤 3 点击 添加图标 （⊕） **添加外部身份验证对象**。

步骤 4 将**身份验证方法**设置为 **RADIUS**。

步骤 5 输入**名称**和可选**说明**。

步骤 6 对于**主服务器**，输入**主机名/IP 地址**。

步骤 7 （可选） 更改**端口**使用的默认值。

步骤 8 输入 **RADIUS 服务器密钥**。

步骤 9 （可选） 输入**备份服务器**参数。

步骤 10 （可选） 输入 **RADIUS 特定参数**。

a) 在 **超时** 中输入重试主服务器之前允许的秒数（介于 1 和 1024 之间）。默认值为 30。

注释 威胁防御 和 管理中心的超时范围不同，因此，如果共享对象，请确保不要超过 威胁防御 的较小超时范围（1-300 秒）。如果将超时设置为更高的值，则 威胁防御 RADIUS 配置将不起作用。

b) 输入滚动到备份服务器之前允许的**重试次数**。默认值为 3。

c) 在与用户角色对应的字段中，输入各用户的名称或确定应分配给这些角色的属性-值对。

将用户名和属性-值对以逗号分隔。

示例：

如果您知道所有本应为“安全分析师”的用户的 `User-Category` 属性值为 `Analyst`，则可以在**安全分析师**字段中输入 `User-Category=Analyst`，以将该角色授予这些用户。

示例：

要将“管理员”角色授予用户 `jsmith` 和 `jdoe`，请在**管理员**字段中输入 `jsmith, jdoe`。

示例：

要将“维护用户”角色授予 `User-Category` 值为 `Maintenance` 的所有用户，请在**维护用户**字段中输入 `User-Category=Maintenance`。

d) 对于不属于任何指定组的用户，请选择**默认用户角色**。

如果更改用户的角色，必须保存/部署更改的外部身份验证对象，并从**用户**屏幕中移除该用户。该用户下次登录时会自动被重新添加。

步骤 11 （可选） **定义自定义 RADIUS 属性**。

如果 RADIUS 服务器返回 `/etc/radiusclient/` 中 `dictionary` 文件内不包含的属性值，并且您计划使用这些属性来设置具有这些属性的用户的角色，则需要定义这些属性。可以通过查看 RADIUS 服务器上的用户配置文件来查找为用户返回的属性。

a) 输入**属性名称**。

定义属性时，请提供属性的名称，其中包含字母数字字符。请注意，属性名称中的单词应以破折号而不是空格进行分隔。

b) 以整数形式输入**属性 ID**。

属性 ID 应为整数且不应与 `etc/radiusclient/dictionary` 文件中的任何现有属性 ID 冲突。

c) 从下拉列表中选择**属性类型**。

还请指定属性的类型：字符串、IP 地址、整数或日期。

d) 点击**添加**以添加自定义属性。

在创建 RADIUS 身份验证对象时，系统会在设备上的 `/var/sf/userauth` 目录中创建该对象的新目录文件。添加的所有自定义属性都会添加到字典文件。

示例：

如果在含有思科路由器的网络上使用 RADIUS 服务器，则可能要使用 `Ascend-Assign-IP-Pool` 属性向从特定 IP 地址池登录的所有用户授予特定角色。`Ascend-Assign-IP-Pool` 是一个整数属性，用于定义允许用户登录的地址池，其中整数指示已分配的 IP 地址池的编号。

要声明自定义属性，请创建一个自定义属性，使其属性名称为 `Ascend-IP-Pool-Definition`，属性 ID 为 `218`，并且属性类型为 `integer`。

然后，可以在**安全分析（只读）(Security Analyst [Read Only])** 字段中输入 `Ascend-Assign-IP-Pool=2`，将只读安全分析师权限授予 `Ascend-IP-Pool-Definition` 属性值为 `2` 的所有用户。

步骤 12 （可选） 在 **CLI 访问过滤器** 区域**管理员 CLI 用户列表** 字段中，输入应具有外壳访问权限的用户名并以逗号分隔。

请确保这些用户名匹配 RADIUS 服务器上的用户名。名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加句号 (.)、连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含 at 符号 (@) 或斜线 (/)

为防止对 CLI 访问进行 RADIUS 身份验证，请将此字段留空。

注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。请确保限制具有 CLI 或 Linux 外壳访问的用户列表。

注释 删除与包括在外壳访问过滤器中的用户具有相同用户名的任何内部用户。对于 管理中心，唯一的内部 CLI 用户是 **管理员**，因此请勿同时创建 **管理员** 外部用户。

步骤 13 （可选） 点击 **测试** 以测试与 RADIUS 服务器的 管理中心 连接。

步骤 14 （可选） 此外，还可以输入**其他测试参数**来测试应可以执行身份验证的用户的用户凭证：输入**用户名**和**密码**，然后点击**测试**。

提示 如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。要验证服务器配置是否正确，请点击**测试**，而无需首先在**其他测试参数**字段中输入用户信息。如果成功，请提供要通过特定用户进行测试的用户名和密码。

示例：

要测试是否可以在 Example 公司检索到 `JSmith` 用户凭证，请输入 `JSmith` 和正确的密码。

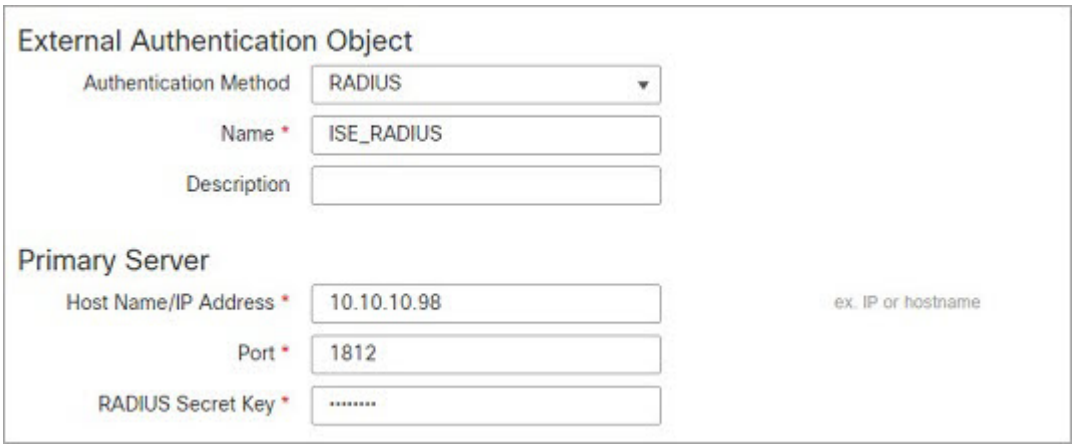
步骤 15 点击**保存 (Save)**。

步骤 16 启用此服务器。请参阅为管理中心上的用户启用外部身份验证，第 134 页。

示例

简单的用户角色指定

下图说明端口 1812 上 IP 地址为 10.10.10.98 的运行 Cisco Identity Services Engine (ISE) 的服务器的示例 RADIUS 登录身份验证对象。未定义备份服务器。



以下示例显示 RADIUS 特定参数，包括超时（30 秒）和 Firepower 系统尝试联系备份服务器（如有）之前的失败重试次数。

此示例说明 RADIUS 用户角色配置的重要方面：

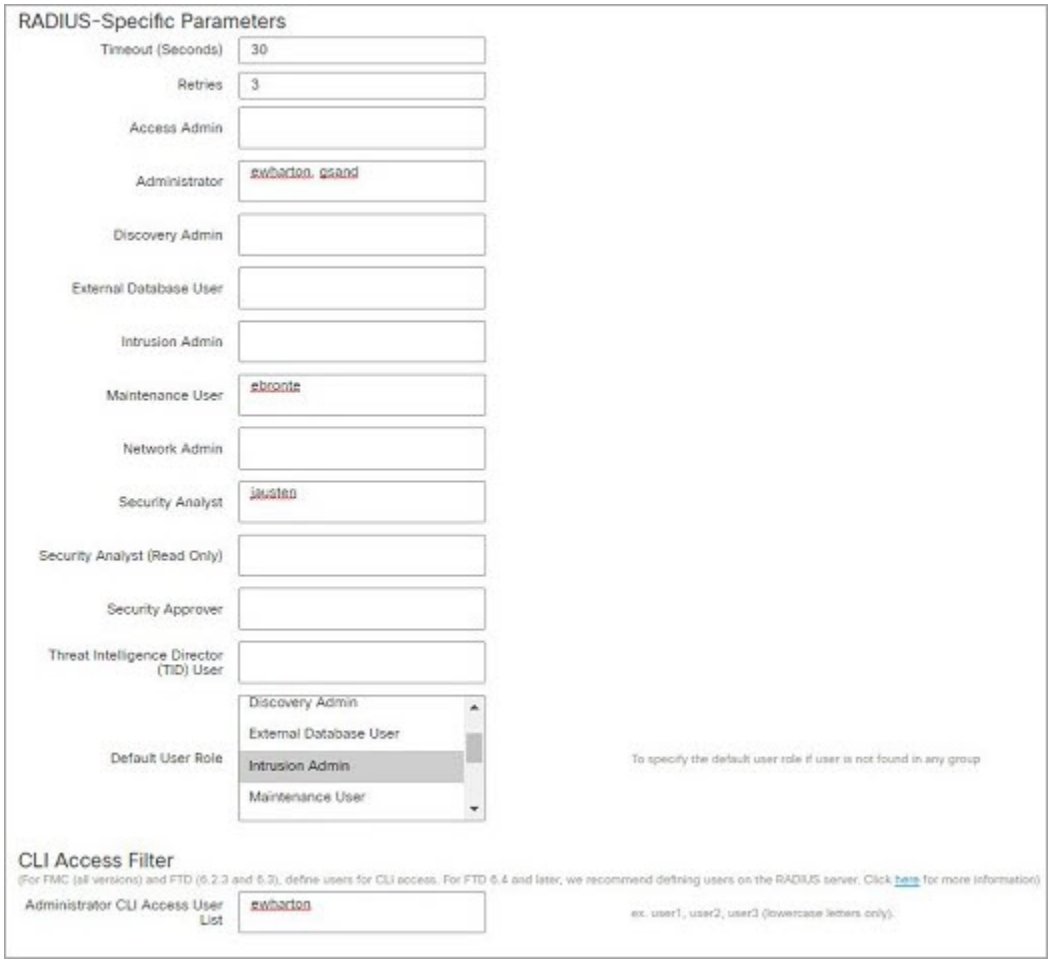
授予用户 `ewharton` 和 `gsand` Web 界面管理权限。

授予用户 `cbronte` Web 界面“维护用户”权限。

授予用户 `jausten` Web 界面“安全分析师”权限。

用户 `ewharton` 可以使用 CLI 帐户登录到设备中。

下图说明示例的角色配置：

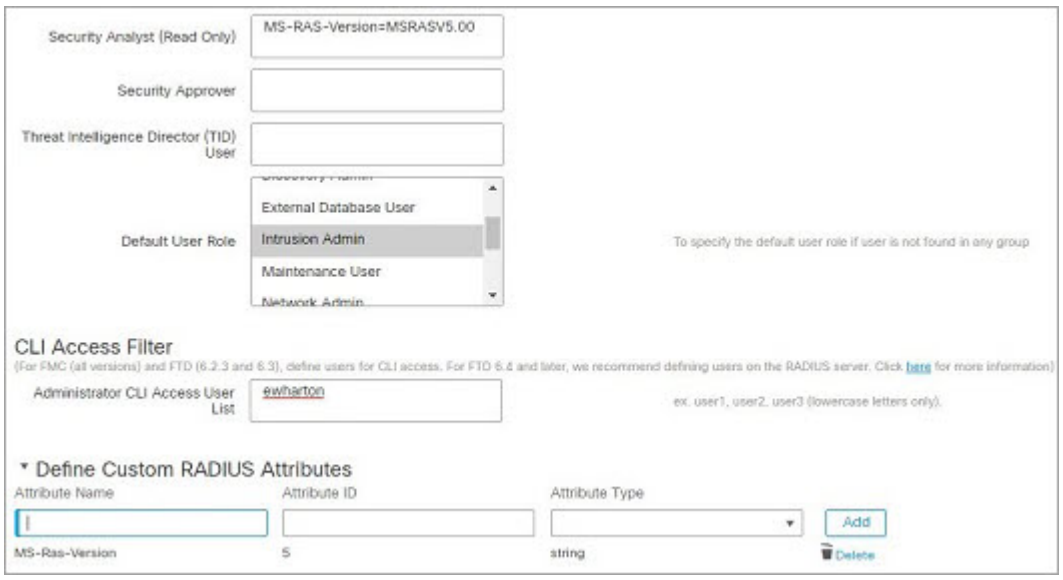


匹配属性-值对的用户角色

可以使用属性-值对识别应接收特定用户角色的用户。如果使用的属性是自定义属性，必须定义该自定义属性。

下图说明与前一示例中相同的 ISE 服务器的示例 RADIUS 登录身份验证对象中的角色配置和自定义属性定义。

但是，在此示例中，由于正在使用 Microsoft 远程访问服务器，因此为一个或多个用户返回了 `MS-RAS-Version` 自定义属性。请注意，`MS-RAS-Version` 自定义属性为字符串。在此示例中，通过 Microsoft v. 5.00 远程访问服务器登录 RADIUS 的所有用户都应得到“安全分析师（只读）”(Security Analyst [Read Only]) 角色，因此请在**安全分析师（只读）(Security Analyst [Read Only]** 字段中输入属性-值对 `MS-RAS-Version=MSRASV5.00`。



为管理中心上的用户启用外部身份验证

在为管理用户启用外部身份验证时，管理中心会使用外部身份验证对象中指定的 LDAP 或 RADIUS 服务器验证用户凭证。

开始之前

根据 添加 管理中心的 LDAP 外部身份验证对象，第 122 页 和 添加管理中心的 RADIUS 外部身份验证对象，第 129 页中所述，添加一个或多个外部身份验证对象。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击**外部身份验证 (External Authentication)**。

步骤 3 为外部 Web 界面用户设置默认用户角色。

没有角色的用户无法执行任何操作。外部身份验证对象中定义的任何用户角色将覆盖此默认用户角色。

a) 点击 **默认用户角色** 值（默认为未选定）。

a) 在**默认用户角色配置**对话框中，选中要使用的角色。

b) 点击**保存 (Save)**。

步骤 4 点击要使用的每个外部身份验证对象旁边的**滑块已启用**（🔵）。如果启用多个对象，系统会按指定顺序参照服务器比较用户。请参阅后续步骤对服务器重新排序。

如果启用外壳身份验证，则必须启用包括**CLI 访问过滤器 (CLI Access Filter)** 的外部身份验证对象。另外，CLI 访问用户只能参照其身份验证对象在列表中排在第一位的服务器进行身份验证。

步骤 5 （可选） 拖放服务器可更改出现身份验证请求时访问身份验证的顺序。

步骤 6 如果要允许外部用户执行 CLI 访问，请选择**外壳身份验证 (Shell Authentication)** > **已启用 (Enabled)**。

注释 CLI 中不支持多域功能。因此， **外壳身份验证** 选项仅在全局域中可用，在子域中不可用。

第一个外部身份验证对象名称显示在**已启用 (Enabled)** 选项旁边，提醒您只有第一个对象用于 CLI。

步骤 7 点击**保存并应用**。

使用 LDAP 配置通用访问卡身份验证

如果您的组织使用通用访问卡 (CAC)，您可以配置 LDAP 身份验证来验证登录 Web 接口的 管理中心 用户。使用 CAC 身份验证，用户可以选择直接登录，而不用为设备提供单独的用户名和密码。

CAC 身份验证用户通过其电子数据交换个人标识符 (EDIPI) 号码进行识别。

在非活动状态持续 24 小时之后，设备会删除**用户**选项卡中的 CAC 身份验证用户。每次后续登录后系统会重新添加用户，但必须重新配置对其用户角色的任何手动更改。

⚠

注意 使用 LDAP 配置 CAC 身份验证时，请确保在向用户分配默认访问角色时遵循最小权限原则。当用户首次使用其 CAC 凭证登录系统时，将为其账户分配此默认访问角色。

如果在分配默认访问角色时不遵循最小权限原则，则在后续登录时可能会为用户分配意外的权限级别。这可能会导致用户拥有超出其所需访问角色的权限。

如果使用默认访问角色登录的用户需要临时提升其权限，则具有管理权限的用户可以通过为其分配具有更高权限的角色来临时为其提供所需的更高级别的访问权限。此权限将在 24 小时不活动后撤销，并且用户将返回其默认访问角色。

如果用户需要将永久访问角色重新分配到更高权限级别（例如系统管理员），请使用 **组控制访问角色** 方法为用户提供管理员访问权限。此方法可确保提供的访问角色持续超过 24 小时，并且用户将根据组分配具有正确的权限级别。有关配置组控制访问角色的详细信息，请参阅为管理中心步骤 15 部分。

开始之前

您必须在浏览器中具有有效的用户证书（在这种情况下，即通过您的 CAC 传递至您的浏览器的证书），才能在 CAC 配置流程中启用用户证书。配置 CAC 身份验证和授权之后，网络上的用户必须在其浏览会话的持续时间内维持 CAC 连接。如果在会话期间移除或替换 CAC，则网络浏览器会终止该会话，并且系统会注销网络界面。

过程

步骤 1 按照您的组织的指示插入 CAC。

步骤 2 将浏览器定向到 **https://***ipaddress_or_hostname/*，其中 *ipaddress* 或 *hostname* 对应您的设备。

步骤 3 如有提示，请输入与步骤 1 中插入的 CAC 关联的 PIN。

步骤 4 如有提示，请从下拉列表中选择相应的证书。

步骤 5 在“登录”(Login) 页面的**用户名 (Username)** 和**密码 (Password)** 字段中，以具备管理员权限的用户身份登录。您还**不能**使用 CAC 凭证登录。

步骤 6 依次选择**系统** > **用户** > **外部身份验证**。

步骤 7 遵循添加 管理中心的 LDAP 外部身份验证对象，第 122 页中的程序，专门为 CAC 创建一个 LDAP 身份验证对象。必须配置以下内容：

- **CAC** 复选框。
- **LDAP 特定参数** > **显示高级选项** > **用户名模板**。
- **属性映射** > **UI 访问属性**。

步骤 8 点击**保存 (Save)**。

步骤 9 启用外部身份验证和 CAC 身份验证，如为管理中心上的用户启用外部身份验证，第 134 页所述。

步骤 10 选择**系统**（⚙）> **配置**，然后点击 **HTTPS 证书**。

步骤 11 如有必要，请遵循导入 HTTPS 服务器证书，第 64 页中概括的过程导入 HTTPS 服务器证书。

您计划使用的 HTTPS 服务器证书和 CAC 用户证书必须由同一个证书颁发机构 (CA) 签发。

步骤 12 在 **HTTPS 客户端证书设置 (HTTPS Client Certificate Settings)** 下，选择**启用客户端证书 (Enable Client Certificates)**。有关详细信息，请参阅需要有效的 HTTPS 客户端证书，第 65 页。

步骤 13 根据 使用 CAC 凭证登录 Cisco Secure Firewall Management Center，第 32 页登录设备。

配置 SAML 单点登录

您可以将 管理中心 配置为使用单点登录，即中央身份提供程序 (IdP) 为登录 管理中心 的用户以及组织内的其他应用提供身份验证和授权的系统。配置为参与此类 SSO 安排的应用称为联合服务提供商应用。SSO 用户只需登录一次即可访问属于同一联盟的所有服务提供商应用。

关于 SAML 单点登录

为 SSO 配置的 管理中心 在登录页面上显示单点登录链接。配置为进行 SSO 访问的用户点击此链接，将被重定向到 IdP 进行身份验证和授权，而不是在 管理中心 登录页面上提供用户名和密码。IdP 成功通过身份验证后，SSO 用户将被重定向回 管理中心 Web 界面并登录。 管理中心 与 IdP 之间的所有通信都是通过浏览器作为中介来完成的；因此， 管理中心 不需要网络连接即可直接访问身份提供程序。

管理中心 支持使用符合用于身份验证和授权的安全断言标记语言 (SAML) 2.0 开放标准的任何 SSO 提供程序。

Note 管理中心无法签署 SAML 身份验证请求消息。因此，如果 IdP 要求服务提供商对身份验证请求进行签名，则管理中心上的 SSO 将失败。

管理中心 Web 界面为以下 SSO 提供程序提供配置选项：

- Okta
- OneLogin
- Azure
- 面向客户云解决方案的 PingID 的 PingOne
- 其他

Note Cisco Secure Sign On SSO 产品不会将 管理中心 识别为预先集成的服务提供商。

管理中心的 SSO 指南

将 管理中心 配置为 SSO 联合的成员时，请记住以下几点：

- 管理中心 一次只能支持一个 SSO 提供程序，例如，您不能将 管理中心 配置为同时使用 Okta 和 OneLogin 进行 SSO。
- 高可用性配置中的管理中心可以支持 SSO，但必须牢记以下注意事项：
  - 高可用性对的成员之间未同步 SSO 配置；您必须在 SSO 对的每个成员上单独配置 SSO。
  - 高可用性对中的两个 管理中心必须使用相同的 IdP 进行 SSO。您必须在 IdP 上为每个 管理中心 配置的 SSO 配置服务提供商应用。
  - 在均配置为支持 SSO 的 管理中心高可用性对中，在用户首次使用 SSO 访问辅助 管理中心之前，该用户必须首先使用 SSO 至少登录一次主 管理中心。
  - 为高可用性对中的 管理中心配置 SSO 时：
    - 如果在主 管理中心上配置 SSO，则不需要在辅助 管理中心上配置 SSO。
    - 如果在辅助 管理中心上配置 SSO，则还需要在主 管理中心 上配置 SSO。（这是因为 SSO 用户必须在登录辅助 管理中心 之前至少登录一次主 管理中心。）
- 在使用多租户的 管理中心 中，SSO 配置只能在全局域级别应用，并且适用于全局域和所有子域。
- 只有通过内部或通过 LDAP 或 RADIUS 进行身份验证的具有管理员角色的用户才能配置 SSO。
- 管理中心 不支持从 IdP 发起的 SSO。

- 管理中心 不支持使用 SSO 账户的 CAC 凭证登录。
- 请勿使用 CC 模式在部署中配置 SSO。
- SSO 活动记录在 管理中心 审核日志中，并在子系统字段中指定登录或注销。

Related Topics

高可用性，第 287 页
域，第 201 页
使用 CAC 凭证登录 Cisco Secure Firewall Management Center，第 32 页
安全认证合规性，第 311 页
审核记录，第 391 页

SSO 用户账户

身份提供程序可以直接支持用户和组配置，也可以从其他用户管理应用（例如 Active Directory、RADIUS 或 LDAP）导入用户和组。本文档重点介绍如何配置 管理中心 与 IdP 配合使用，以支持 SSO（假设已建立 IdP 用户和组）；要配置 IdP 以支持来自其他用户管理应用的用户和组，请参阅 IdP 供应商文档。

SSO用户的大多数账户特征（包括用户名和密码）都是在IdP上建立的。在这些账户首次登录之前，这些账户不会显示在 管理中心 Web 接口用户页面上。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

可以从 管理中心 Web 接口的 **系统**（⚙）> **系统** > **编辑用户**下配置 SSO 用户的以下账户特征：

- 实际名称
- 豁免浏览器会话超时

SSO 用户的用户角色映射

默认情况下，系统会为所有被授予 SSO 访问 管理中心 权限的用户分配安全分析师（只读）角色。您可以更改此默认值，也可以为具有用户角色映射的特定SSO用户或组覆盖此默认值。建立并成功测试 管理中心 SSO 配置后，您可以配置用户角色映射，以建立 SSO 用户在登录时分配的 管理中心 用户角色。

用户角色映射需要将 管理中心 上的配置设置与 SSO IdP 应用上的设置进行协调。可以将用户角色分配给 IdP 应用中定义的用户或组。用户可能是组的成员，也可能不是，并且用户或组定义可能会或可能不会从组织内的其他用户管理系统（例如 Active Directory）导入到 IdP。因此，要有效配置 管理中心 SSO 用户角色映射，您必须熟悉 SSO 联合的组织方式，以及如何在 SSO IdP 应用中分配用

户、组及其角色。本文档重点介绍如何配置 管理中心 与 IdP 配合使用的用户角色映射；要在 IdP 中创建用户或组，或者从用户管理应用将用户或组导入 IdP，请参阅 IdP 供应商文档。

在用户角色映射中，IdP 维护 管理中心 服务提供商应用的角色属性，并且每个用户或组都配置 管理中心 有角色属性的字符串或表达式（每个 IdP 的属性值要求不同）。在 管理中心 该角色属性的名称是 SSO 配置的一部分。 管理中心 SSO 配置还包含分配给 管理中心 用户角色列表的表达式列表。当用户使用 SSO 登录 管理中心 时， 管理中心 会将该用户（或该用户的组，具体取决于配置）的角色属性值与每个 管理中心 用户角色的表达式进行比较。 管理中心 为用户分配表达式与用户提供的属性值匹配的所有角色。

Note 您可以根据个人用户权限或组权限配置要映射的 管理中心 角色，但单个 管理中心 应用不能同时支持组和个人用户的角色映射。

在 管理中心启用单点登录

Before you begin

- 在 SAML SSO 管理应用中，为 管理中心 配置服务提供商应用，并将用户或组分配给服务提供商应用：
  - 要为 Okta 配置 管理中心 服务提供商应用，请参阅为 Okta 配置管理中心服务提供商应用, on page 141。
  - 要为 OneLogin 配置管理中心服务提供商应用，请参阅为 OneLogin 配置管理中心服务提供商应用, on page 152。
  - 要为 Azure 配置管理中心服务提供商应用，请参阅为 Azure 配置管理中心服务提供商应用, on page 164。
  - 要为 PingID 的 PingOne 客户云解决方案配置 管理中心 服务提供商应用，请参阅为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 176。
  - 要为任何符合 SAML 2.0 的 SSO 提供程序配置 管理中心 服务提供程序应用，请参阅为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用, on page 180。

Procedure

步骤 1 选择**系统**（⚙）> **用户** > **单点登录**。

步骤 2 点击 **单点登录 (SSO) 配置** 滑块以启用 SSO。

步骤 3 点击 **配置 SSO (Configure SSO)** 按钮。

步骤 4 在 **选择防火墙管理中心 SAML 提供程序** 对话框中，点击所选 SSO IdP 的单选按钮，然后点击 **下一步**。

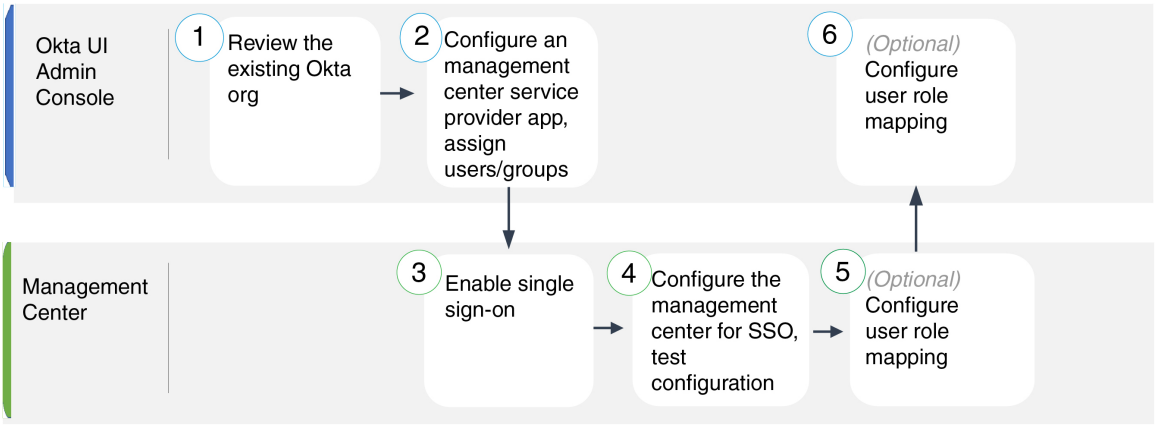
What to do next

继续执行适合您选择的 SSO 提供商的说明：

- 为 Okta SSO 配置管理中心；请参阅为 Okta SSO 配置管理中心 , on page 143。
- 使用 PingID 的 PingOne 客户云解决方案为 SSO 配置管理中心；请参阅为客户使用 PingID PingOne 为 SSO 配置管理中心 , on page 178。
- 为 Azure SSO 配置管理中心；请参阅为 Azure SSO 配置管理中心 , on page 166。
- 为 OneLogin SSO 配置管理中心；请参阅为 OneLogin SSO 配置 管理中心 , on page 154。
- 使用任何符合 SAML 2.0 的提供程序为 SSO 配置管理中心；请参阅为使用任何 SAML 2.0 兼容 SSO 提供程序的 SSO 配置 管理中心 , on page 182。

通过 Okta 配置单点登录

请参阅以下任务以使用 Okta 配置 SSO：



1	Okta UI 管理控制台	查看 Okta 组织, on page 141
2	Okta UI 管理控制台	为 Okta 配置管理中心服务提供商应用, on page 141
3	管理中心	在 管理中心启用单点登录, on page 139
4	管理中心	为 Okta SSO 配置管理中心 , on page 143
5	管理中心	在管理中心上为 Okta 配置用户角色映射, on page 144
6	Okta UI 管理控制台	在 Okta IdP 上配置用户角色映射, on page 144

查看 Okta 组织

在 Okta 中，包含用户可以使用同一 SSO 账户访问的所有联合设备和应用的实体称为 组织。在将 管理中心 添加到 Okta 组织之前，请熟悉其配置；思考以下问题：

- 有多少用户可以访问 管理中心？
- Okta 组织中的用户是否是组的成员？
- 用户和组定义是 Okta 本地的还是从用户管理应用（例如 Active Directory、RADIUS 或 LDAP）导入的？
- 您是否需要将更多用户或组添加到 Okta 组织以支持 管理中心上的 SSO？
- 您要分配哪种类型的用户角色？（如果您选择不分配用户角色， 管理中心 会自动为所有 SSO 用户分配可配置的默认用户角色。）
- 必须如何组织 Okta 组织内的用户和组，以支持所需的用户角色映射？

请记住，您可以根据个人用户权限或组权限配置要映射的 管理中心 角色，但单个 管理中心 应用不能同时支持组和个人用户的角色映射。

本文档假设您已经熟悉 Okta 经典 UI 管理控制台，并且拥有可以执行需要超级管理员权限的配置功能的账户。如果您需要更多信息，请参阅 Okta 的在线文档。

为 Okta 配置管理中心服务提供商应用

使用 Okta 经典 UI 管理控制台中的这些说明在 Okta 中创建 管理中心 服务提供商应用，并将用户或组分配给该应用。您应该熟悉 SAML SSO 概念和 Okta 管理控制台。本文档并未介绍建立功能齐全的 SSO 组织所需的所有 Okta 功能；例如，要创建用户和组，或从其他用户管理应用导入用户和组定义，请参阅 Okta 文档。

Note 如果您计划将用户组分配给 管理中心 应用，则不要将这些组中的用户作为个人进行分配。

Note 管理中心 不能支持使用多个 SSO 属性的角色映射；您必须选择用户角色映射或组角色映射，并配置单个属性以将用户角色信息从 OneLogin 传送到 管理中心。

Before you begin

- 熟悉 SSO 联合及其用户和组；请参阅 查看 Okta 组织, on page 141。
- 如有必要，在 Okta 组织中创建用户账户和/或组。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

- 确认目标 管理中心 的登录 URL (`https://ipaddress_or_hostname`)。

Note 如果可以使用多个 URL（例如，完全限定域名和 IP 地址）访问 管理中心 Web 界面，则 SSO 用户必须使用您在此任务中配置的登录 URL 一致地访问 管理中心 。

Procedure

步骤 1 在 Okta 经典 UI 管理控制台中，为 管理中心创建服务提供商应用。使用以下选项配置 管理中心 应用：

- 为 **平台**选择 `Web` 。
- 选择 `SAML 2.0` 作为 **登录方法**。
- 提供 **单点登录 URL**。

  这是浏览器代表 IdP 向其发送信息的 管理中心 URL。

  将字符串 `saml/acs` 附加到 管理中心 登录 URL。例如： `https://ExampleFMC/saml/acs`。
- 启用 **将此用于收件人 URL**”和“**目标 URL**”。
- 输入 **受众 URI**（**SP 实体 ID**）。

  这是服务提供商的全局唯一名称 (管理中心)，通常采用 URL 格式。

  将字符串 `/saml/metadata` 附加到 管理中心 登录 URL。例如：
  `https://ExampleFMC/saml/metadata`。
- 对于 **名称 ID 格式** ，选择 `未指定`。

步骤 2 （如果要向应用分配组，则可选。）将单个 Okta 用户分配给 管理中心 应用。（如果您计划将组分配给 管理中心 应用，请勿将属于这些组的成员的用户作为个人进行分配。）

步骤 3 （如果要将单个用户分配给应用，则可选。）将 Okta 组分配给 管理中心 应用。

步骤 4 （可选）为了简化 管理中心 上的 SSO 设置，您可以将 管理中心 服务提供商应用的 SAML XML 元数据文件从 Okta 下载到本地计算机。

What to do next

启用单点登录；请参阅 在 管理中心启用单点登录, on page 139。

为 Okta SSO 配置管理中心

在 管理中心 web 接口上使用这些说明。

准备工作

- 在 Okta 经典 UI 管理控制台中创建 管理中心 服务提供商应用；请参阅为 Okta 配置管理中心服务提供商应用, on page 141。
- 启用单点登录；请参阅 在 管理中心启用单点登录, on page 139。

Procedure

步骤 1 （此步骤直接从 在 管理中心启用单点登录, on page 139开始。）在 **配置 Okta 元数据** 对话框中，您有两个选择：

- 要手动输入 SSO 配置信息，请执行以下操作：
  a. 点击 **手动配置** 单选按钮。
  b. 从 Okta SSO 服务提供程序应用中输入以下值。（从 Okta 经典 UI 管理控制台检索这些值。）
     - **身份提供程序单点登录 (SSO) URL**
     - **身份提供程序颁发机构**
     - **X.509 证书**
- 如果已将 Okta 生成的 XML 元数据文件保存到本地计算机（ 为 Okta 配置管理中心服务提供商应用, on page 141中的步骤 4），则可以将文件上传到 管理中心：
  a. 点击 **上传文件** 单选按钮。
  b. 按照屏幕上的说明导航到本地计算机上的 XML 元数据文件并选择该文件。

步骤 2 点击**下一步**。

步骤 3 在 **验证元数据** 对话框中，查看配置参数，然后点击 **保存**。

步骤 4 点击 **测试配置**。如果系统显示错误消息，请查看 管理中心 的 SSO 配置以及 Okta 服务提供商应用配置，更正所有错误，然后重试。

步骤 5 当系统报告配置测试成功时，点击 **应用**。

What to do next

您可以选择为 SSO 用户配置用户角色映射；请参阅 在管理中心上为 Okta 配置用户角色映射, on page 144。如果您选择不配置角色映射，则默认情况下会为登录 管理中心 的所有 SSO 用户分配您在 在管理中心上为 Okta 配置用户角色映射, on page 144的步骤 4 中配置的用户角色。

在管理中心上为 Okta 配置用户角色映射

无论您选择哪种 SSO 提供商，在管理中心 Web 接口上为用户角色映射配置的字段都是相同的。但是，您配置的值必须考虑您使用的 SAML SSO 提供程序实施用户角色映射的方式。

Before you begin

- 查看 Okta 用户组映射信息；请参阅查看 Okta 组织, on page 141。
- 为管理中心配置 SSO 服务提供商应用；请参阅为 Okta 配置管理中心服务提供商应用, on page 141。
- 在管理中心上启用并配置单点登录；请参阅在管理中心启用单点登录, on page 139和为 Okta SSO 配置管理中心 , on page 143。

Procedure

步骤 1 选择 **系统**（⚙）> **用户**。

步骤 2 点击 **单点登录 (SSO)** 选项卡。

步骤 3 展开 **高级配置（角色映射）**。

步骤 4 从**默认用户角色 (Default User Role)** 下拉列表中选择要分配用户的 管理中心 用户角色作为默认值。

步骤 5 输入 **组成员属性**。此字符串必须与在 Okta 管理中心 提供程序应用中为用户或组的用户角色映射配置的属性名称匹配。（请参阅 在 Okta IdP 上配置角色映射的用户属性, on page 145 中的第 1 步或 在 Okta IdP 上配置角色映射的组属性, on page 146 中的第 1 步。）

步骤 6 在要分配给 SSO 用户的每个 管理中心 用户角色旁边，输入正则表达式。（ 管理中心 使用 Golang 和 Perl 支持的 Google RE2 正则表达式标准的受限版本。） 管理中心 将这些值与 IdP 发送到 管理中心的用户角色映射属性值和 SSO 用户信息进行比较。 管理中心 授予用户找到匹配项的所有角色的并集。

What to do next

- 在服务提供商应用中配置用户角色映射；请参阅 在 Okta IdP 上配置用户角色映射, on page 144。

在 Okta IdP 上配置用户角色映射

您可以在 Okta 经典 UI 管理控制台中根据个人用户权限或组权限配置 SSO 用户角色映射。

- 要基于单个用户权限进行映射，请参阅 在 Okta IdP 上配置角色映射的用户属性, on page 145。

- 要基于组权限进行映射，请参阅 在 Okta IdP 上配置角色映射的组属性, on page 146。

当 SSO 用户登录到 管理中心时，Okta 会向 管理中心 提供在 Okta IdP 配置的用户或组角色属性值。管理中心 将该属性值与分配给 SSO 配置中每个 管理中心 用户角色的正则表达式进行比较，并向用户授予找到匹配项的所有角色。（如果未找到匹配项， 管理中心 将授予用户可配置的默认用户角色。）分配给每个 管理中心 用户角色的表达式必须符合 Golang 和 Perl 支持的 受限版本的 Google RE2 正则表达式标准。 管理中心 将从 Okta 接收的属性值视为使用相同标准的正则表达式，以便与管理中心 用户角色表达式进行比较。

Note 单个 管理中心 不能同时支持组和单个用户的角色映射；您必须为 管理中心 服务提供商应用选择一种映射方法，并一致地使用它。此外， 管理中心 可以仅使用 Okta 中配置的每个 管理中心 服务提供商应用的一个组属性语句来支持组角色映射。通常，对于具有许多用户的管理中心，基于组的滚动映射更有效。您应考虑在您的 Okta 组织中建立的用户和组定义。

在 Okta IdP 上配置角色映射的用户属性

使用 Okta 经典 UI 管理控制台中的这些说明将自定义角色映射属性添加到 Okta 默认用户配置文件。

Okta 服务提供商应用可以使用两种类型的用户配置文件之一：

- Okta 用户配置文件，可以使用任何自定义属性进行扩展。
- 应用用户配置文件，只能使用 Okta 通过查询第三方应用或目录（例如 Active Directory、LDAP 或 Radius）生成的预定义列表中的属性进行扩展。

您可以在 Okta 组织中使用任一类型的用户配置文件；有关如何配置它们的信息，请参阅 Okta 文档。无论使用哪种类型的用户配置文件，要支持与管理中心的用户角色映射，都必须在配置文件中配置自定义属性，以将每个用户的角色映射表达式传达给 管理中心。

本文档介绍如何使用 Okta 用户配置文件进行角色映射；使用应用配置文件进行映射需要熟悉您的组织中使用的第三方用户管理应用来设置自定义属性。有关详细信息，请参阅 Okta 文档。

Before you begin

- 在 Okta IdP 上配置 管理中心 服务提供商应用，如为 Okta 配置管理中心服务提供商应用, on page 141中所述。
- 配置 SSO 用户角色映射 管理中心 ，如 在管理中心上为 Okta 配置用户角色映射, on page 144中所述。

Procedure

步骤 1 向默认 Okta 用户配置文件添加新属性：

- 对于 **数据类型** ，请选择 字符串。

- 提供 Okta IdP 将发送到 管理中心的 **变量名称**，其中包含要匹配用户角色映射的表达式。此变量名称必须与您在 管理中心 SSO 配置中为 **组成员属性**输入的字符串匹配。（请参阅中 在管理中心上为 Okta 配置用户角色映射, on page 144的步骤 5。）

步骤 2 对于使用此配置文件分配给管理中心服务提供商应用的每个用户，请为您刚刚创建的用户角色属性分配一个值。

使用表达式表示 管理中心 将分配给用户的一个或多个角色。 管理中心 将此字符串与您在 在管理中心上为 Okta 配置用户角色映射, on page 144的步骤 6 中分配给每个 管理中心 用户角色的表达式进行比较。（为了与 管理中心 用户角色表达式进行比较， 管理中心 将从 Okta 接收的属性值视为符合 Golang 和 Perl 支持的受限版本的 Google RE2 正则表达式标准。）

在 Okta IdP 上配置角色映射的组属性

使用 Okta 经典 UI 管理控制台中的这些说明将自定义角色映射组属性添加到 管理中心 服务提供商应用。每个 Okta 管理中心 服务提供商应用仅使用一个组属性语句 管理中心 即可支持组角色映射。

Okta 服务提供商应用可以使用以下两种类型的组之一：

- Okta 组，可以使用任何自定义属性进行扩展。
- 应用组，只能使用 Okta 通过查询第三方应用或目录（例如 Active Directory、LDAP 或 Radius）以获取受支持属性而生成的预定义列表中的属性。

您可以在 Okta 组织中使用任一类型的组；有关如何配置它们的信息，请参阅 Okta 文档。无论使用哪种类型的组，要支持与管理中心的用户角色映射，都必须为该组配置自定义属性，以将其角色映射表达式传达给 管理中心。

本文档介绍如何使用Okta组进行角色映射；与应用组进行映射需要熟悉您的组织中使用的第三方用户管理应用来设置自定义属性。有关详细信息，请参阅 Okta 文档。

Before you begin

- 在 Okta IdP 上配置 管理中心 服务提供商应用；请参阅为 Okta 配置管理中心服务提供商应用, on page 141。
- 在 管理中心配置用户角色映射； 在管理中心上为 Okta 配置用户角色映射, on page 144。

Procedure

为 管理中心 服务提供商应用创建新的 SAML 组属性：

- 对于 **名称**，请使用您在 管理中心 SSO 配置中为 **组成员属性**输入的相同字符串。（请参阅中 在管理中心上为 Okta 配置用户角色映射, on page 144的步骤 5。）
- 对于 **过滤器**，请指定一个表达式来表示 管理中心 将分配给组成员的一个或多个角色。Okta 将此值与用户所属的组的名称进行比较，然后发送匹配的组名称至 管理中心 。 管理中心 依次将

这些组名称与您 在管理中心上为 Okta 配置用户角色映射, on page 144在步骤 6 中分配给每个 管理中心 用户角色的正则表达式进行比较。

Okta 用户角色映射示例

如以下示例所示，用于支持用户角色映射的管理中心SSO配置对于单个用户和组是相同的。区别在于 Okta 中 管理中心 服务提供商应用的设置。

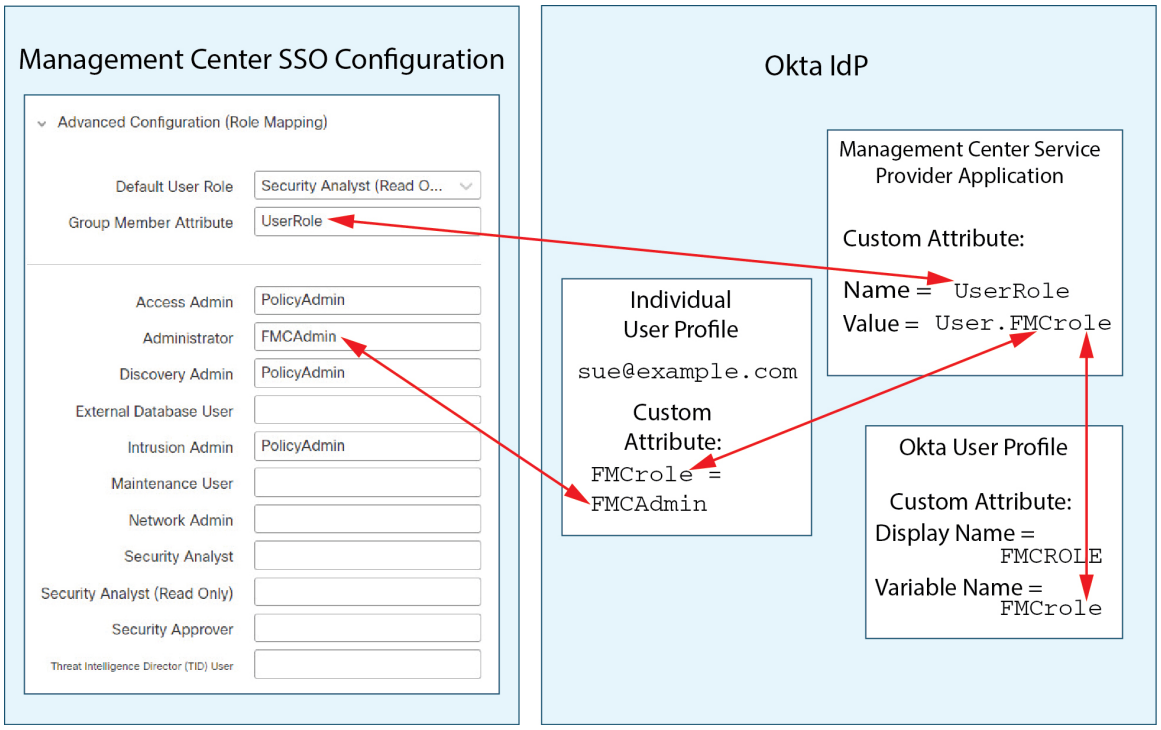
Note 您可以根据个人用户权限或组权限配置要映射的 管理中心 角色，但单个 管理中心 应用不能同时支持组和个人用户的角色映射。此外， 管理中心 可以仅使用 Okta 中配置的每个 管理中心 服务提供商应用的一个组属性语句来支持组角色映射。

个人用户账户的 Okta 角色映射示例

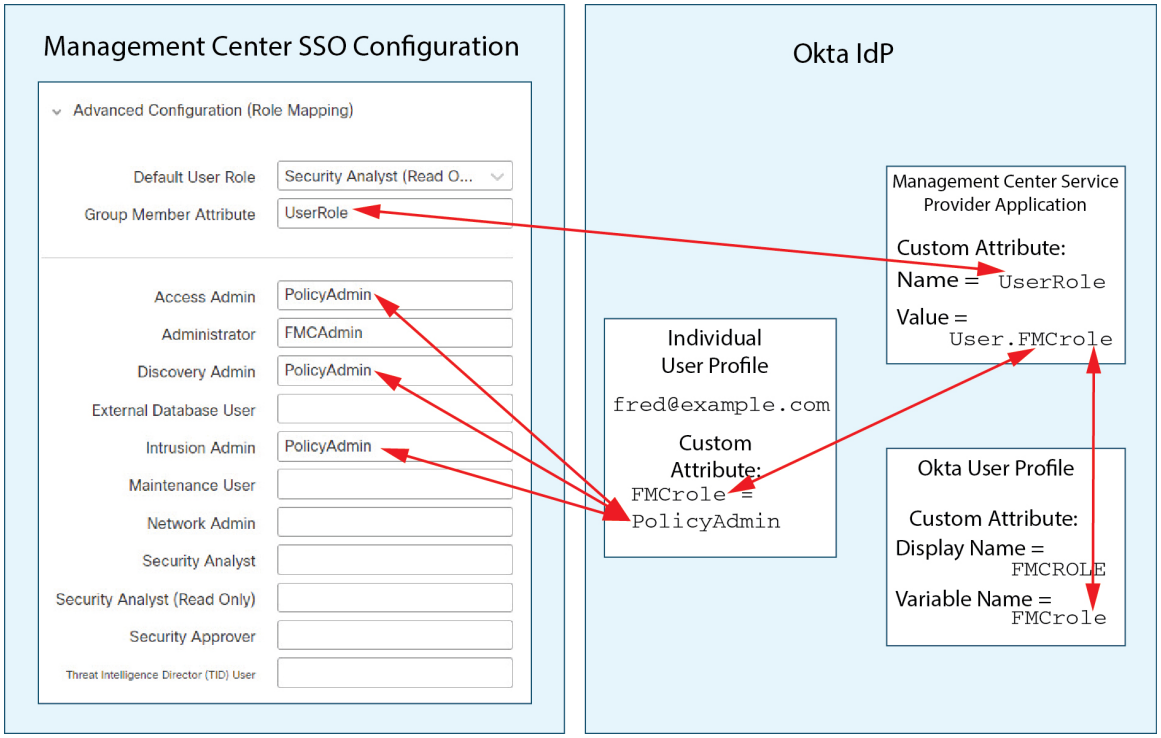
在单个用户的角色映射中，Okta管理中心服务应用具有一个自定义属性，其名称与管理中心上的组成员属性的名称匹配。（在本例中为 `UserRole`）。Okta 中的用户配置文件也有一个自定义属性（在本例中为名为 `FMCrole`的变量）。应用自定义属性 `UserRole` 的定义规定，当 Okta 将用户角色映射信息传递到 管理中心时，它将使用为相关用户分配的自定义属性值。

下图说明了 管理中心 和 Okta 配置中的相关字段和值在各个账户的用户角色映射中如何相互对应。每个图表在 管理中心 和 Okta UI 管理控制台上使用相同的 SSO 配置，但在 Okta UI 管理控制台上为每个用户分配的配置不同，以在 管理中心上为每个用户分配不同的角色。

- 在此图中，sue@example.com 使用 `FMCrole` 值 `FMCAdmin`，并且 管理中心 为她分配管理员角色。



- 在此图中，fred@example.com 使用 `FMCrole` 值 `PolicyAdmin`，并且 管理中心 分配给他角色访问管理员、发现管理员和入侵管理员。



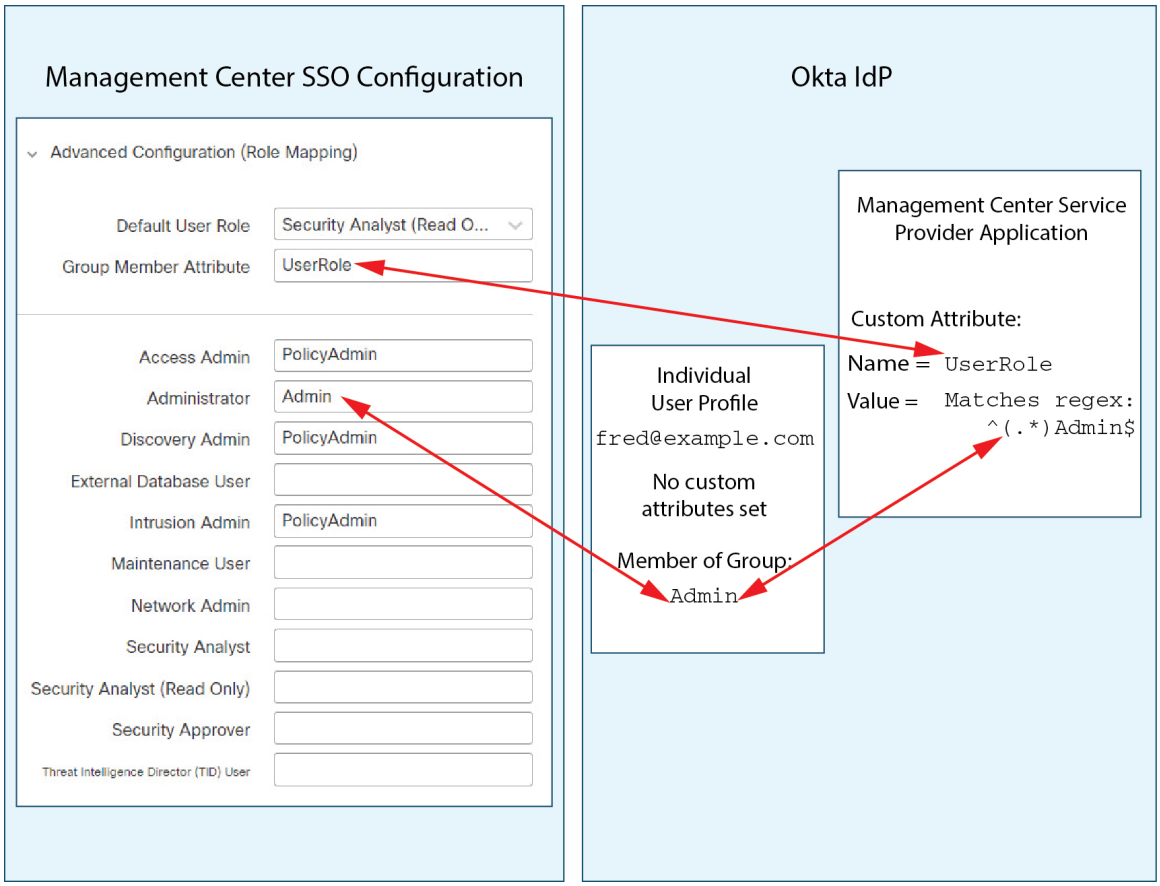
- 出于以下原因之一，为此 管理中心 分配到Okta服务应用的其他用户会被分配默认用户角色“安全分析师（只读）”：
  - 他们没有为 Okta 用户配置文件中的 `FMCole` 变量分配值。
  - 分配给其 Okta 用户配置文件中的 `FMCrole` 变量的值与为 SSO 配置 管理中心中的用户角色配置的任何表达式都不匹配。

组的 Okta 角色映射示例

在组的角色映射中，Okta服务应用具有一个自定义组属性，其名称与上的组成员属性的名称匹配（在本例中为 UserRole）。管理中心管理中心当 Okta 处理 SSO 登录请求时，它会将用户的组成员身份与分配给服务应用组属性的表达式（在本例中为^(.*)Admin$）进行比较。管理中心管理中心Okta将与组属性匹配的用户组成员身份发送给 管理中心 。 管理中心 将其接收的组名称与为每个用户角色配置的正则表达式进行比较，并相应地分配用户角色。

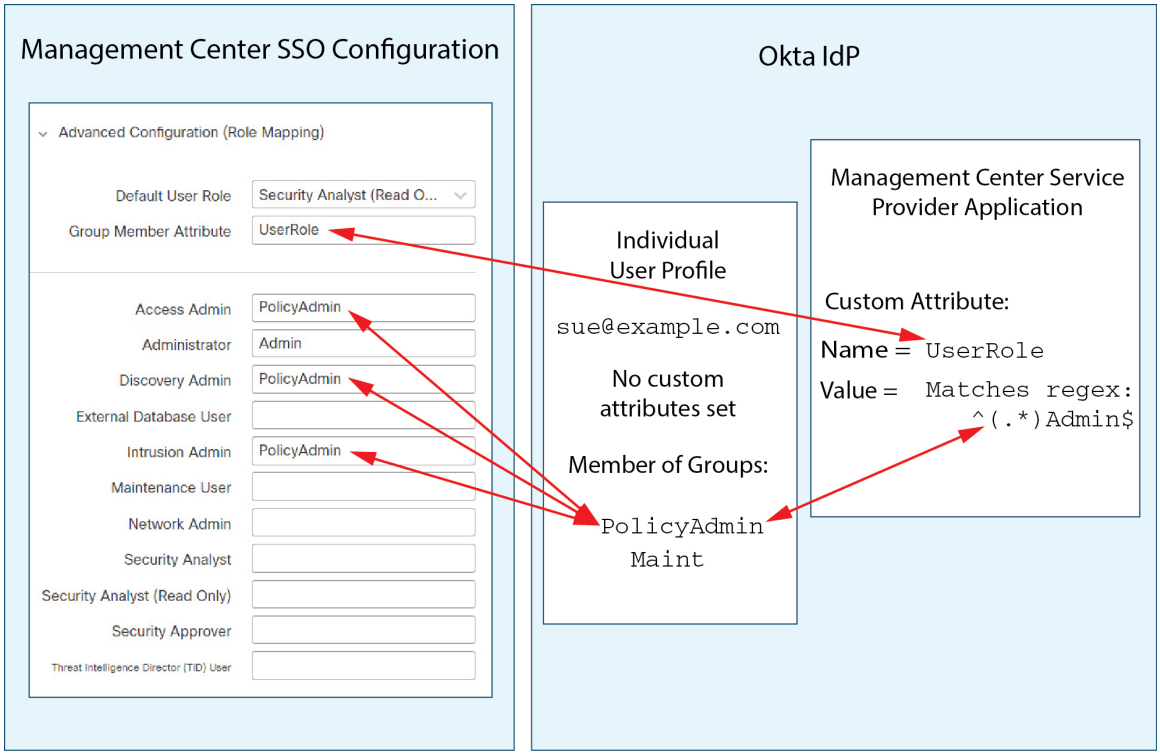
下图说明了 管理中心 和 Okta 配置中的相关字段和值在组的用户角色映射中如何相互对应。每个图表在 管理中心 和 Okta UI 管理控制台上使用相同的 SSO 配置，但在 Okta UI 管理控制台上为每个用户分配的配置不同，以在 管理中心上为每个用户分配不同的角色。

- 在此图中，fred@example.com 是 Okta IdP 组 `管理员` 的成员，与表达 `^(.*)Admin$`匹配。Okta 向管理中心 Fred 的 `管理员` 组成员发送邮件，并且 管理中心 为他分配管理员角色。

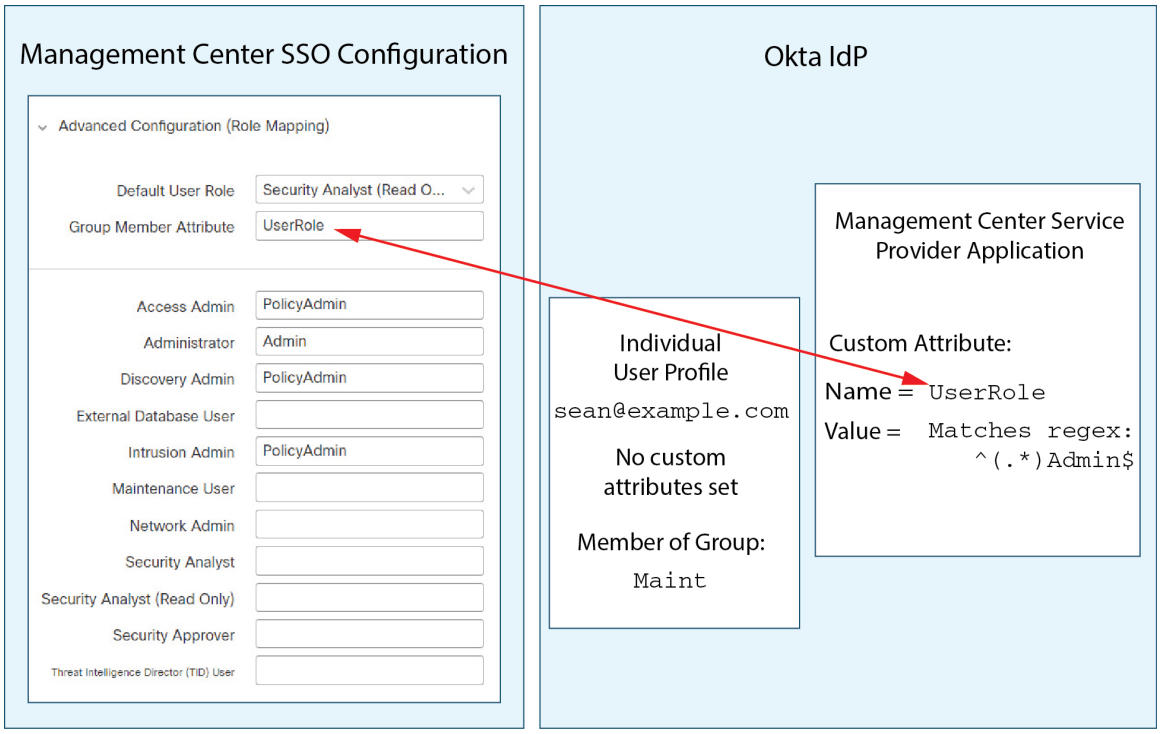


- 在此图中，sue@example.com 是 Okta IdP 组 `PolicyAdmin`的成员，它与表达式`^(.*)Admin$`匹配。Okta 发送 管理中心 Sue 的 `PolicyAdmin` 组成员身份，并且 管理中心 为她分配访问管理员、发现管理员和入侵管理员角色。

  Sue 也是 Okta 组 `Maint` 的成员，但由于此组名称与分配给 Okta 管理中心 服务应用中的组成员身份属性的表达式不匹配，因此 Okta 不会向 管理中心发送有关 Sue 的 `Maint` 组成员身份的信息，并且她在`Maint` 组不参与 管理中心 分配给她的角色。



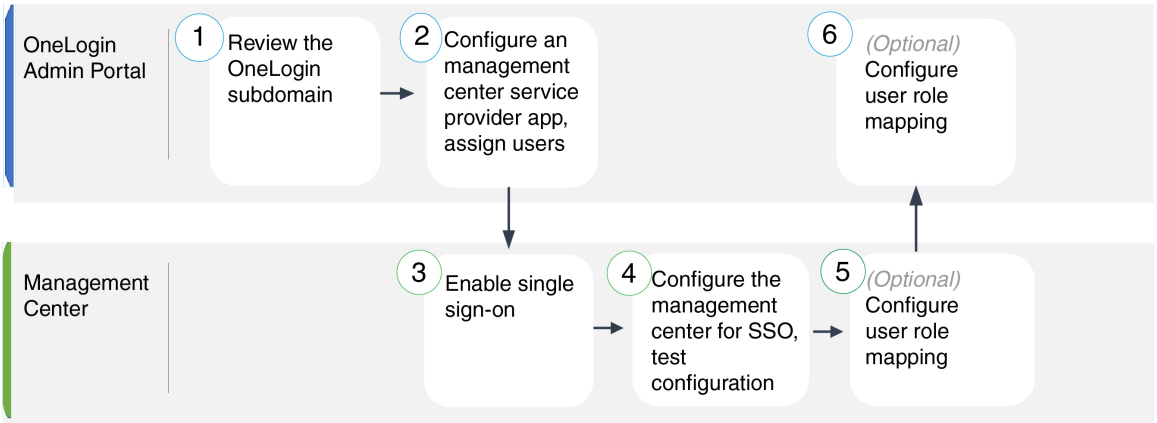
- 在此图中，sean@example.com 是 Okta IdP 组 `Maint` 的成员。此组名称与表达 `^(.*)Admin$` 不匹配，因此，当 sean@example.com 登录 管理中心时，Okta 不会将有关 Sean 的 `Maint` 组成员身份的信息发送到 管理中心，并且会为 Sean 分配默认用户角色（安全分析师（只读）），而不是“维护用户”角色。



这些图说明了在建立角色映射策略时提前规划的重要性。在本示例中，任何具有访问管理中心权限的 Okta 用户（仅为 `Maint` 组的成员）只能被分配默认用户角色。 管理中心 支持在其 Okta 服务应用配置中仅使用一个自定义组属性。分配给该属性的表达式以及建立与之匹配的组名称必须精心设计。通过在 管理中心 SSO 配置中的用户角色分配字符串中使用正则表达式，可以提高角色映射的灵活性。（分配给每个 管理中心 用户角色的表达式必须符合 Golang 和 Perl 支持的受限版本的 Google RE2 正则表达式标准。）

通过 OneLogin 配置单点登录

请参阅以下任务以使用 OneLogin 配置 SSO：



1	管理中心	查看 OneLogin 子域, on page 152
2	管理中心	为 OneLogin 配置管理中心服务提供商应用, on page 152
3	OneLogin 管理员门户	在 管理中心启用单点登录, on page 139
4	OneLogin 管理员门户	为 OneLogin SSO 配置 管理中心 , on page 154
5	OneLogin 管理员门户	在管理中心为 OneLogin 配置用户角色映射, on page 155
6	管理中心	在 OneLogin IdP 上配置用户角色映射, on page 156

查看 OneLogin 子域

在 OneLogin 中，包含用户可以使用同一 SSO 账户访问的所有联合设备和应用的实体称为子域。在将 管理中心 添加到 OneLogin 子域之前，请熟悉其配置；思考以下问题：

- 有多少用户可以访问 管理中心？
- OneLogin 子域中的用户是否是组的成员？
- 第三方目录（例如 Active Directory、Google Apps 或 LDAP）中的用户和组是否与 OneLogin 子域同步？
- 是否需要将更多用户或组添加到 OneLogin 子域以支持 管理中心上的 SSO？
- 您要分配哪种类型的 管理中心 用户角色？（如果您选择不分配用户角色， 管理中心 会自动为所有 SSO 用户分配可配置的默认用户角色。）
- 如何组织 OneLogin 子域中的用户和组，以支持所需的用户角色映射？

请记住，您可以将 管理中心 角色配置为基于单个用户或基于组进行映射，但单个 管理中心 应用不能同时支持组和单个用户的角色映射。

本文档假设您已经熟悉 OneLogin 管理员门户，并且拥有具有超级用户权限的账户。要配置用户角色映射，您还需要订用支持自定义用户字段的 OneLogin Unlimited 计划。如果您需要更多信息，请参阅在线提供的 OneLogin 文档。

为 OneLogin 配置管理中心服务提供商应用

使用 OneLogin 管理门户中的这些说明在 OneLogin 中创建 管理中心 服务提供商应用，并将用户或组分配给该应用。您应该熟悉 SAML SSO 概念和 OneLogin 管理员门户。本文档并未介绍建立功能齐全的 SSO 组织所需的所有 OneLogin 功能；例如，要创建用户和组，或从其他用户管理应用导入用户和组定义，请参阅 OneLogin 文档。

Note 如果您计划将用户组分配给 管理中心 应用，则不要将这些组中的用户作为个人进行分配。

Note 管理中心 不能支持使用多个 SSO 属性的角色映射；您必须选择用户角色映射或组角色映射，并配置单个属性以将用户角色信息从 OneLogin 传送到 管理中心。

Before you begin

- 熟悉 OneLogin 子域及其用户和组；请参阅 查看 OneLogin 子域, on page 152。
- 如有必要，在 OneLogin 子域中创建用户账户。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

- 确认目标 管理中心 的登录 URL (`https://ipaddress_or_hostname/`)。

Note 如果可以使用多个 URL 访问您的 管理中心 Web 接口。（例如，完全限定域名和 IP 地址），SSO 用户必须使用您在此任务中配置的登录 URL 一致地访问 管理中心 。

Procedure

步骤 1 使用 **SAML 测试连接器（高级）** 作为基础创建 管理中心 服务提供商应用。

步骤 2 使用以下设置配置应用：

- 对于 **受众（实体 ID）**，将字符串 `/saml/metadata` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/metadata`。
- 对于 **接收方**，将字符串 `/saml/acs` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/acs`。
- 对于 **ACS (消费者) URL 验证方**，输入 OneLogin 用于确认其使用的是正确 管理中心 URL 的表达式。您可以通过使用 ACS URL 并按如下方式修改来创建简单的验证程序：
  - 将 ^ 附加到 ACS URL 的开头。

- 在 ACS URL 末尾附加 `$`。
- 在每个 `/` 和 `?` 前面插入 `\`，在 ACS URL 中。

例如，对于 ACS URL `https://ExampleFMC/saml/acs`，适当的 URL 验证程序为 `^https:\/\/ExampleFMC\/saml\/acs$`。

- 对于 **ACS（使用者）URL**，请将字符串 `/saml/acs` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/acs`。
- 对于 **登录 URL**，请将字符串 `/saml/acs` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/acs`。
- 对于 **SAML 发起方**，请选择 服务提供商。

步骤 3 将 OneLogin 用户分配给 管理中心 服务提供商应用。

步骤 4 （可选）为了简化 管理中心 上的 SSO 设置，您可以将 管理中心 服务提供商应用的 SAML XML 元数据从 OneLogin 下载到本地计算机。

What to do next

启用单点登录；请参阅 在 管理中心启用单点登录, on page 139。

为 OneLogin SSO 配置 管理中心

在 管理中心 web 接口上使用这些说明。

Before you begin

- 在 OneLogin 管理门户上创建 管理中心 服务提供商应用；请参阅为 OneLogin 配置管理中心服务提供商应用, on page 152。
- 启用单点登录；请参阅 在 管理中心启用单点登录, on page 139。

Procedure

步骤 1 （此步骤直接从在 管理中心启用单点登录, on page 139开始。）在 **配置 OneLogin 元数据** 对话框中，您有两个选择：

- 要手动输入 SSO 配置信息，请执行以下操作：
  a. 点击 **手动配置** 单选按钮。
  b. 从 OneLogin 服务提供应用输入以下 SSO 配置值：
     - **身份提供程序单点登录 URL**：从 OneLogin 输入 **SAML 2.0 终端 (HTTP)**。
     - **身份提供程序颁发者**：输入 OneLogin 中的 **颁发者 URL**。

- **X.509 证书**：输入 OneLogin 中的 **X.509 证书** 。

- 如果已将 OneLogin 生成的 XML 元数据文件保存到本地计算机（ 为 OneLogin 配置管理中心服务提供商应用, on page 152中的步骤 4），则可以将该文件上传到 管理中心：

  a. 点击 **上传文件** 单选按钮。

  b. 按照屏幕上的说明导航到本地计算机上的 XML 元数据文件并选择该文件。

步骤 2 点击**下一步**。

步骤 3 在 **验证元数据** 对话框中，查看配置参数，然后点击 **保存**。

步骤 4 点击 **测试配置**。如果系统显示错误消息，请查看 管理中心 的 SSO 配置以及 OneLogin 服务提供程序应用配置，更正所有错误，然后重试。

步骤 5 当系统报告配置测试成功时，点击 **应用**。

What to do next

您可以选择为 SSO 用户配置用户角色映射；请参阅 在管理中心为 OneLogin 配置用户角色映射, on page 155。如果您选择不配置角色映射，则默认情况下会为登录 管理中心 的所有 SSO 用户分配您在 在管理中心为 OneLogin 配置用户角色映射, on page 155的步骤 4 中配置的用户角色。

在管理中心为 OneLogin 配置用户角色映射

无论您选择哪种 SSO 提供商，在 管理中心 web 接口上为用户角色映射配置的字段都是相同的。但是，您配置的值必须考虑您使用的 SAML SSO 提供程序实施用户角色映射的方式。

Before you begin

- 查看 OneLogin 用户和组，请参阅 查看 OneLogin 子域, on page 152。
- 为 管理中心配置 SSO 服务提供商应用；请参阅 为 OneLogin 配置管理中心服务提供商应用, on page 152。
- 在 管理中心上启用并配置单点登录；请参阅在 管理中心启用单点登录, on page 139和 为 OneLogin 配置管理中心服务提供商应用, on page 152。

Procedure

步骤 1 选择 **系统**（⚙） > **用户** > **单点登录系统** > **用户**。

步骤 2 展开 **高级配置**（**角色映射**）。

步骤 3 从**默认用户角色 (Default User Role)** 下拉列表中选择要分配给用户的 管理中心 用户角色作为默认值。

步骤 4 输入 **组成员属性**。此字符串必须与您在 OneLogin 中为 管理中心 服务提供商应用中的角色映射定义的自定义参数的字段名称匹配。（请参阅 在 OneLogin IdP 上配置单个用户的用户角色映射, on page 156 的步骤 1 或 在 OneLogin IdP 上配置组的用户角色映射, on page 157的步骤 1。）

步骤 5 在要分配给 SSO 用户的每个 管理中心 用户名旁边，输入正则表达式。 管理中心 将这些值与 IdP 发送到 管理中心 的用户角色映射属性和 SSO 用户信息进行比较。 管理中心 授予用户找到匹配项的所有角色的并集。

What to do next

在服务提供商应用中配置用户角色映射；请参阅 在 OneLogin IdP 上配置用户角色映射, on page 156。

在 OneLogin IdP 上配置用户角色映射

您可以在 Onelogin 管理员门户上根据个人权限或组权限配置 SSO 用户角色映射。

- 要基于单个用户权限进行映射，请参阅 在 OneLogin IdP 上配置单个用户的用户角色映射, on page 156。
- 要基于组权限进行映射，请参阅 在 OneLogin IdP 上配置组的用户角色映射, on page 157。

当 SSO 用户登录 管理中心时，OneLogin 会向 管理中心 提供从 OneLogin IdP 配置的自定义用户字段获取其值的用户或组角色属性值。 管理中心 将该属性值与分配给 SSO 配置中每个 管理中心 用户角色的正则表达式进行比较，并向用户授予找到匹配项的所有角色。（如果未找到匹配项， 管理中心 将授予用户可配置的默认用户角色。）分配给每个 管理中心 用户角色的表达式必须符合 Golang 和 Perl 支持的受限版本的 Google RE2 正则表达式标准。 管理中心 将从 OneLogin 接收的属性值视为使用相同标准的正则表达式，以便与 管理中心 用户角色表达式进行比较。

Note 单个 管理中心 不能同时支持组和单个用户的角色映射；您必须为 管理中心 服务提供商应用选择一种映射方法，并一致地使用它。 管理中心 只能使用 OneLogin 中配置的一个自定义用户字段来支持角色映射。通常，对于具有许多用户的 管理中心 ，基于组的角色映射更有效。您应该考虑在您的 OneLogin 子域中建立的用户和组定义。

在 OneLogin IdP 上配置单个用户的用户角色映射

使用 OneLogin 管理门户为 管理中心 服务提供商应用创建自定义参数和自定义用户字段。这些为 OneLogin 提供了在 SSO 登录过程中将用户角色信息传递到 管理中心 的方法。

Before you begin

- 查看 OneLogin 子域及其用户和组；请参阅 查看 OneLogin 子域, on page 152。
- 在 OneLogin 中创建和配置 管理中心 服务提供商应用；请参阅为 OneLogin 配置管理中心服务提供商应用, on page 152。
- 配置 SSO 用户角色映射 ， 如 在管理中心为 OneLogin 配置用户角色映射, on page 155中所述。

Procedure

步骤 1 为 管理中心 服务提供商应用创建自定义参数。

- 对于 **字段名称**，请使用您在 管理中心 SSO 配置中用于 **组成员属性** 的相同名称。（请参阅 在管理中心为 OneLogin 配置用户角色映射, on page 155中的步骤 4。）
- 对于 **值**，请提供助记符名称，例如 `FMCUserRole`。这必须与您将在此程序的步骤 2 中配置的客户用户字段的名称匹配。

步骤 2 创建自定义用户字段，以包含具有访问 管理中心权限的每个 OneLogin 用户的用户角色信息。

- 对于 **名称**字段，请提供助记符名称，例如 `FMCUserRole`。这必须与为此程序步骤 1 中所述的应用自定义参数提供的值匹配。
- 对于 **短名称**，请提供该字段的缩写备用名称。（这用于 OneLogin 编程接口。）

步骤 3 对于有权访问 管理中心 服务提供商应用的每个用户，请为此程序的步骤 2 中创建的自定义用户字段分配一个值。

当用户使用 SSO 登录 管理中心 时，您为该用户分配给此字段的值是 管理中心 与您在 SSO 配置中分配给 管理中心 用户角色的表达式进行比较的值。（请参阅中 在管理中心为 OneLogin 配置用户角色映射, on page 155的步骤 5。）

What to do next

- 通过使用 SSO 从各种账户登录 管理中心 并确认用户已按预期分配 管理中心 用户角色，测试您的角色映射方案。

在 OneLogin IdP 上配置组的用户角色映射

使用 OneLogin 管理门户为 管理中心 服务提供商应用创建自定义参数和自定义用户字段。将 OneLogin 用户分配到组。然后，在自定义用户字段和用户组之间创建一个或多个映射，以便 OneLogin 根据用户的组成员身份为自定义用户字段分配一个值。这些为 OneLogin 提供了在 SSO 登录过程中将基于组的用户角色信息传递到 管理中心 的方法。

OneLogin 服务提供程序应用可以使用以下两种组之一：

- OneLogin 的本地组。
- 从第三方应用（例如 Active Directory、Google Apps 或 LDAP）同步的组。

您可以使用任一类型的 管理中心 组进行组角色映射。本文档介绍使用 OneLogin 组进行角色映射；使用第三方应用组需要熟悉您的组织中使用的第三方用户管理应用。有关详细信息，请参阅 OneLogin 文档。

Before you begin

- 查看 OneLogin 子域及其用户和组；请参阅 查看 OneLogin 子域, on page 152。
- 在 OneLogin 中创建和配置 管理中心 服务提供商应用；请参阅为 OneLogin 配置管理中心服务提供商应用, on page 152。
- 配置 SSO 用户角色映射 ，如 在管理中心为 OneLogin 配置用户角色映射, on page 155中所述。

Procedure

步骤 1 为 管理中心 服务提供商应用创建自定义参数。

- 对于 **字段名称**，请使用您在 管理中心 SSO 配置中用于 **组成员属性** 的相同名称。（请参阅 在管理中心为 OneLogin 配置用户角色映射, on page 155中的步骤 4。）
- 对于 **值**，请提供助记符名称，例如 `FMCUserRole`。这必须与您将在此程序的步骤 2 中配置的客户用户字段的名称匹配。

步骤 2 创建自定义用户字段，以包含具有访问 管理中心权限的每个 OneLogin 用户的用户角色信息。

- 对于 **名称**字段，请提供助记符名称，例如 `FMCUserRole`。这必须与为此程序步骤 1 中所述的应用自定义参数提供的值匹配。
- 对于 **短名称**，请提供该字段的缩写备用名称。（这用于 OneLogin 编程接口。）

步骤 3 创建一个或多个用户字段映射，以将基于组的值分配给您在此程序的步骤 2 中创建的自定义用户字段。创建任意数量的映射，以便为每个 OneLogin 用户组分配正确的 管理中心 用户角色。

- 为映射创建一个或多个 **条件** ，将用户 **组** 字段与组名称进行比较。
- 如果创建多个 **条件**，请选择用户的组是否必须匹配 *任何* 或 *所有* 条件才能进行映射。
- 为映射创建 **操作** ，以将值分配给您在此程序的步骤 2 中创建的自定义用户字段。提供字段 **名称**，以及 OneLogin 为满足指定 **条件** 的所有用户分配给此自定义用户字段的字符串。

  管理中心 将此字符串与您在 在管理中心为 OneLogin 配置用户角色映射, on page 155的步骤 5 中分配给每个 管理中心 用户角色的表达式进行比较。
- 完成更改后，请 **重新应用所有映射** 。

What to do next

- 通过使用 SSO 从各种账户登录 管理中心 并确认用户已按预期分配 管理中心 用户角色，测试您的角色映射方案。

OneLogin 用户角色映射示例

如以下示例所示，用于支持用户角色映射的管理中心SSO配置对于单个用户和组是相同的。不同之处在于 OneLogin 中 管理中心 服务提供商应用的设置。

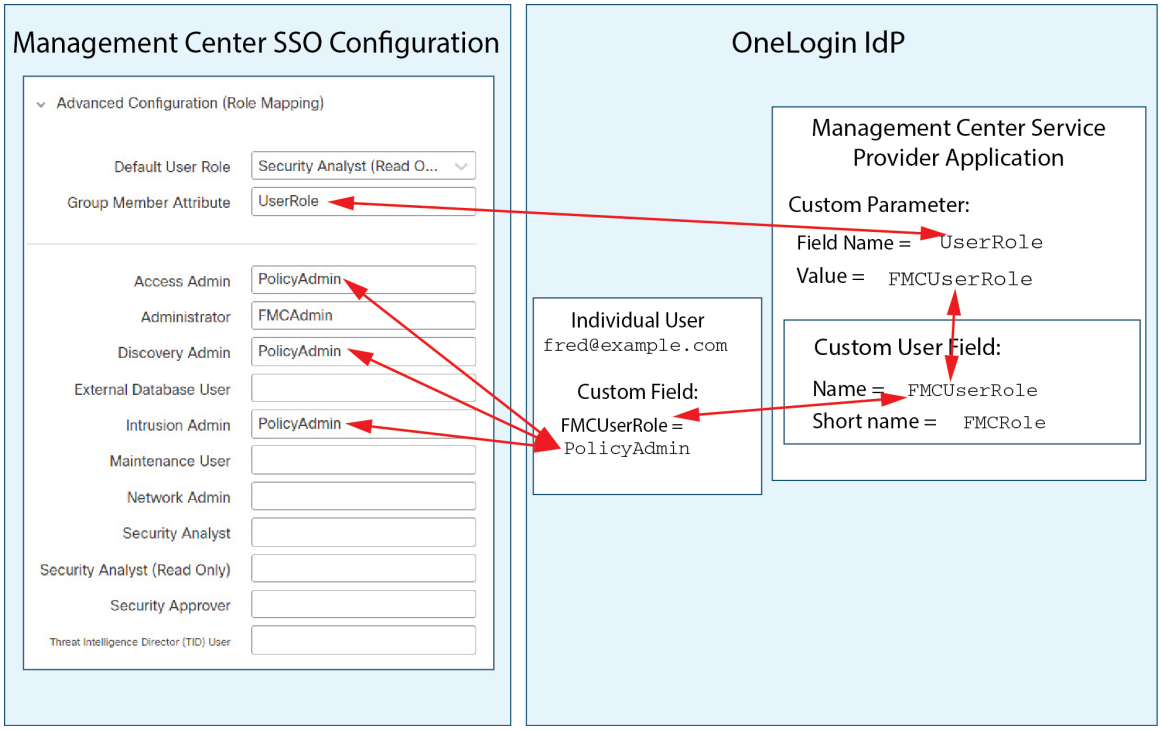
Note 单个 管理中心 不能同时支持组和单个用户的角色映射；您必须为 管理中心 服务提供商应用选择一种映射方法，并一致地使用它。 管理中心 只能使用 OneLogin 中配置的一个自定义用户字段来支持角色映射。通常，对于具有许多用户的 管理中心 ，基于组的角色映射更有效。您应该考虑在您的 OneLogin 子域中建立的用户和组定义。

单个用户账户的 OneLogin 角色映射示例

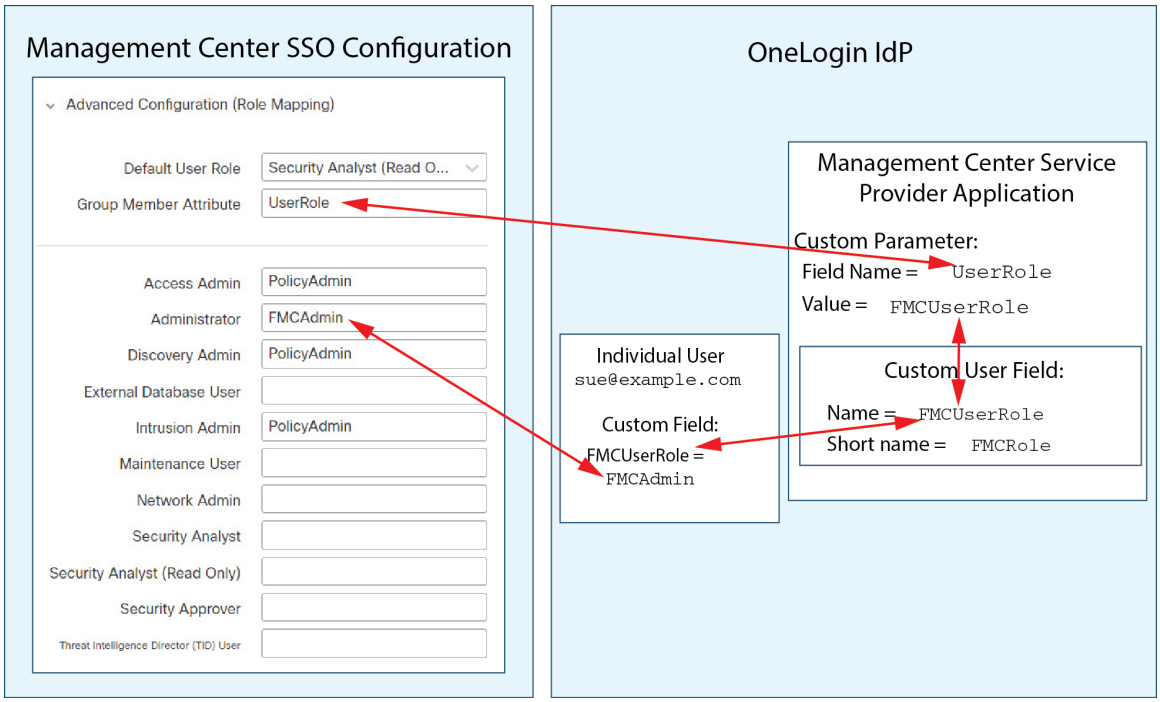
在个人用户的角色映射中，OneLogin 管理中心 服务应用具有一个自定义参数，其名称与 管理中心 上的“组成员”属性的名称匹配（在本例中为 `UserRole`）。OneLogin 还定义了一个自定义用户字段（在本例中为 `FMCUserRole`）。应用自定义参数 `UserRole` 的定义规定，当 OneLogin 将用户角色映射信息传递到 管理中心 时，它将使用相关用户的自定义用户字段 `FMCUserRole` 的值。

下图说明了 管理中心 和 OneLogin 配置中的相关字段和值在各个账户的用户角色映射中如何相互对应。每个图在 管理中心 和 OneLogin Admin 门户使用相同的 SSO 配置，但 OneLogin Admin 门户上每个用户的配置不同，在 管理中心 上为每个用户分配不同的角色。

- 在此图中，fred@example.com 使用 `FMCUserRole` 值 `PolicyAdmin` ，并且 管理中心 分配给他角色访问管理员、发现管理员和入侵管理员。



- 在此图中，sue@example.com 使用 `FMCUserRole` 值 `FMCAdmin`，并且 管理中心 为她分配管理员角色。



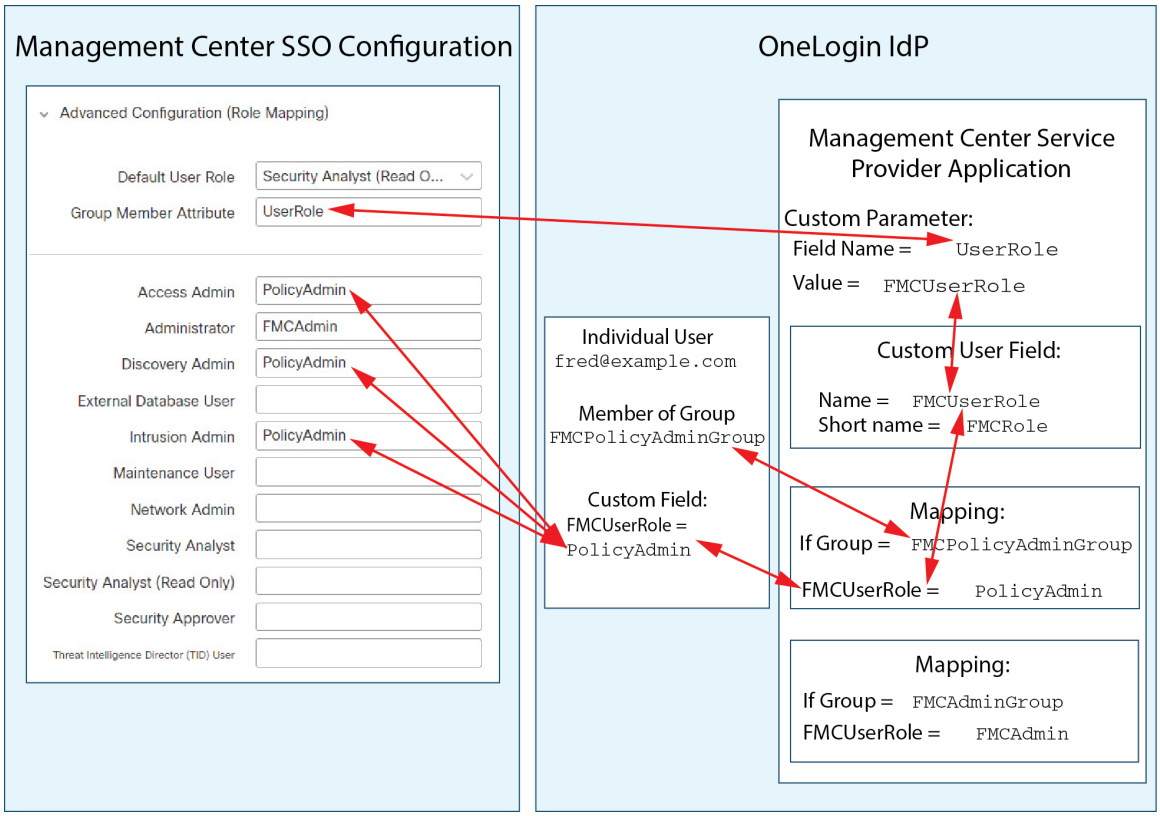
- 出于以下原因之一，为此 管理中心 分配到 OneLogin 服务应用的其他用户会被分配默认用户角色“安全分析师（只读）”：
  - 它们没有分配给 `FMCUserRole` 自定义用户字段的值。
  - 分配给 `FMCUserRole` 自定义用户字段的值与 SSO 配置 管理中心中为用户角色配置的任何表达式都不匹配。

组的 OneLogin 角色映射示例

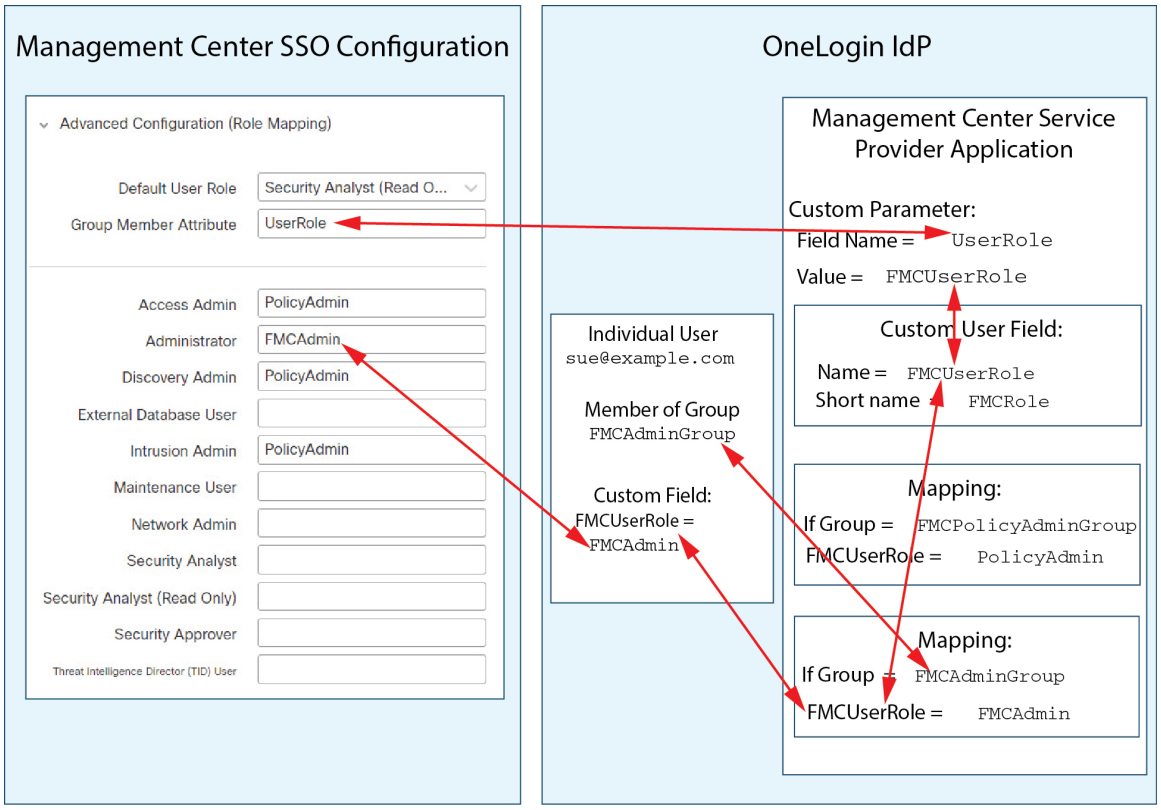
在组的角色映射中，OneLogin管理中心 服务应用具有一个自定义参数，其名称与管理中心 上的“组成员”属性的名称匹配（在本例中为 `UserRole`）。OneLogin还定义了一个自定义用户字段（在本例中为 `FMCUserRole`）。应用自定义参数 `UserRole` 的定义规定，当 OneLogin 将用户角色映射信息传递到 管理中心时，它将使用相关用户的自定义用户字段 `FMCUserRole` 的值。要支持用户组映射，必须在 OneLogin 中建立映射，以根据该用户的 OneLogin 组成员身份为每个用户的 `FMCUserRole` 字段分配值。

下图说明 管理中心 和 OneLogin 配置中的相关字段和值在组的用户角色映射中如何相互对应。每个图在 管理中心 和 OneLogin Admin 门户使用相同的 SSO 配置，但 OneLogin Admin 门户上每个用户的配置不同，在 管理中心上为每个用户分配不同的角色。

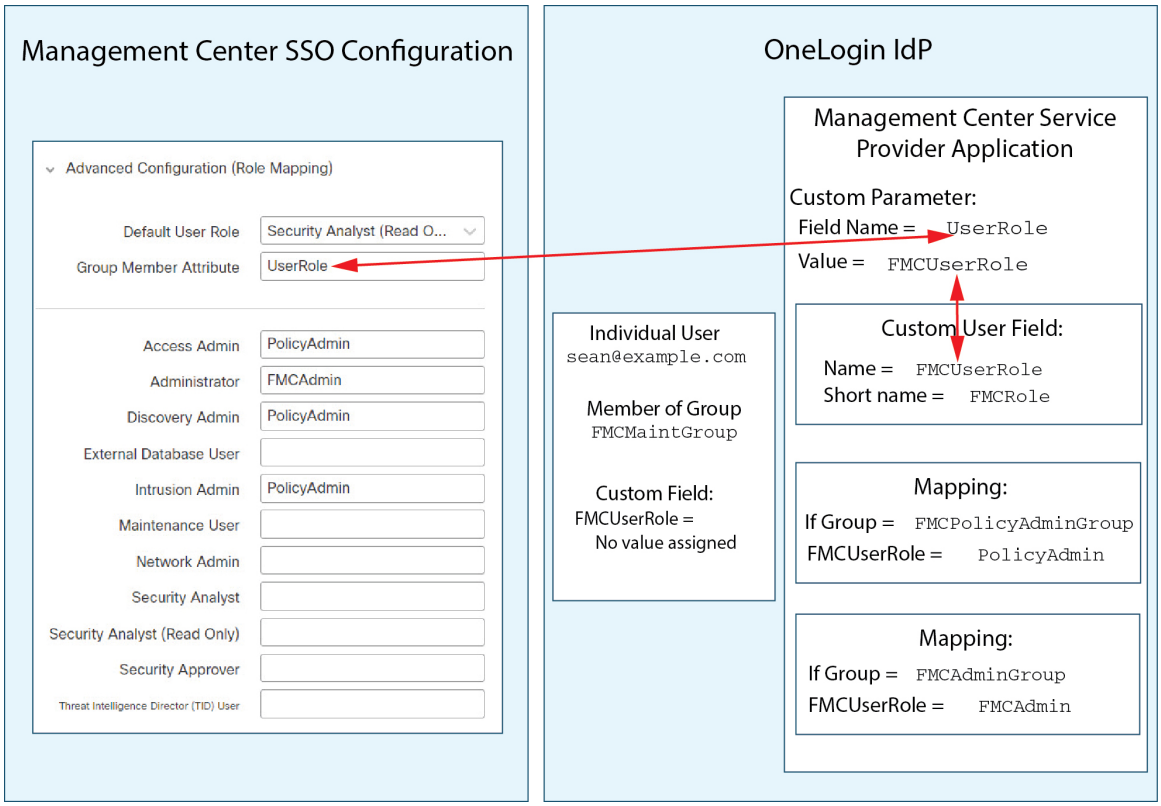
- 在此图中，fred@example.com 是 OneLogin IdP 组 `FMCPolicyAdminGroup`的成员。OneLogin 映射将值 `PolicyAdmin` 分配给 `FMCPolicyAdminGroup` 成员的自定义用户字段 `FMCUserRole` 。 管理中心为Fred 和 `FMCPolicyAdminGroup` 的其他成员分配角色访问管理员、发现管理员和入侵管理员。



- 在此图中，sue@example.com 是 OneLogin IdP 组 `FMCAdminGroup`的成员。OneLogin 映射将值 FMCAdmin 分配给 `FMCAdminGroup`成员的自定义用户字段 `FMCUserRole`。 管理中心 为 Sue 和 `FMCAdminGroup` 的其他成员分配管理员角色。

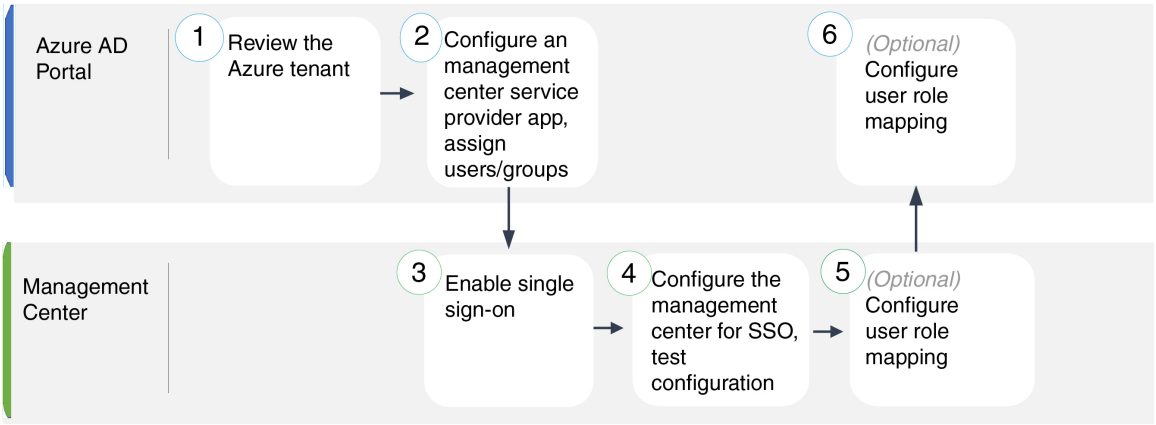


- 在此图中，sean@example.com 是 Idp 组 `FMCMaintGroup`的成员。没有与此组关联的 OneLogin 映射，因此 OneLogin 不会为 Sean 的自定义用户字段 `FMCUserRole` 分配值。 管理中心 为 Sean 分配默认用户角色（安全分析师（只读）），而不是“维护用户”角色。



通过 Azure AD 配置单点登录

请参阅以下任务以使用 Azure 配置 SSO：



1	Azure AD 门户	查看 Azure 租户, on page 164
2	Azure AD 门户	为 Azure 配置管理中心服务提供商应用, on page 164

3	管理中心	在 管理中心启用单点登录, on page 139
4	管理中心	为 Azure SSO 配置管理中心 , on page 166
5	管理中心	在管理中心上为 Azure 配置用户角色映射, on page 167
6	Azure AD 门户	在 Azure IdP 上配置用户角色映射, on page 168

查看 Azure 租户

Azure AD 是 Microsoft 基于多租户云的身份和访问管理服务。在 Azure 中，包含用户可以使用同一 SSO 账户访问的所有联合设备的实体称为 租户。在将 管理中心 添加到 Azure 租户之前，请熟悉其组织；思考以下问题：

- 有多少用户可以访问 管理中心？
- 用户是否属于组的 Azure 租户成员？
- 用户和组是否来自其他目录产品？
- 是否需要向 Azure 租户添加更多用户或组以支持 管理中心上的 SSO？
- 您要分配哪种类型的 管理中心 用户角色？（如果您选择不分配用户角色， 管理中心 会自动为所有 SSO 用户分配可配置的默认用户角色。）
- 必须如何组织 Azure 租户中的用户和组，以支持所需的用户角色映射？
- 请记住，您可以将 管理中心 角色配置为基于单个用户或基于组进行映射，但单个 管理中心 应用不能同时支持组和单个用户的角色映射。

本文档假定您已熟悉 Azure Active Directory 门户，并且拥有具有 Azure AD 租户应用管理员权限的账户。请记住， 管理中心 仅支持使用租户特定的单点登录和单点注销终端的 Azure SSO。您必须具有 Azure AD Premium P1 或更高版本的许可证和全局管理员权限；有关详细信息，请参阅 Azure 文档。

为 Azure 配置管理中心服务提供商应用

使用 Azure Active Directory 门户在 Azure Active Directory 租户中创建 管理中心 服务提供商应用并建立基本配置设置。

Note 如果您计划将用户组分配给 管理中心 应用，则不要将这些组中的用户作为个人进行分配。

Note 管理中心 不能支持使用多个 SSO 属性的角色映射；您必须选择用户角色映射或组角色映射，并配置单个属性以将用户角色信息从 OneLogin 传送到 管理中心。

Before you begin

- 熟悉 Azure 租户及其用户和组；请参阅 查看 Azure 租户, on page 164。
- 如有必要，在 Azure 租户中创建用户账号和/或组。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

- 确认目标 管理中心 的登录 URL (`https://ipaddress_or_hostname`)

Note 如果可以使用多个 URL（例如，完全限定域名和 IP 地址）访问 管理中心 Web 界面，则 SSO 用户必须使用您在此任务中配置的登录 URL 一致地访问 管理中心 。

Procedure

步骤 1 使用 Azure AD SAML 工具包作为基础创建 管理中心 服务提供商应用。

步骤 2 使用以下 **基本 SAML 配置设置**配置应用：

- 对于 **标识符（实体 ID）**，将字符串 `/saml/metadata` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/metadata`。
- 对于 **回复 URL（断言使用者服务 URL）**，将字符串 `/saml/acs` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/acs`。
- 对于 **登录 URL**，将字符串 `/saml/acs` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/acs`。

步骤 3 编辑应用的 **唯一用户标识符名称（名称 ID）**，以将登录 管理中心 的用户名强制为与用户账户关联的邮件地址：

- 对于 **源**，选择 属性。
- 对于 **源属性**：选择 `user.mail`。

步骤 4 生成证书以保护 管理中心上的 SSO。对证书使用以下选项：

- 为签名选项选择签名 SAML 响应和断言。
- 为签名算法选择 SHA-256。

步骤 5 将证书的 Base-64 版本下载到本地计算机；在 管理中心 Web 界面配置 Azure SSO 时需要用到它

步骤 6 在应用的基于 SAML 的登录信息中，请注意以下值：

- **登录 URL**
- **Azure AD 标识符**

在 管理中心 Web 界面配置 Azure SSO 时需要这些值。

步骤 7 （可选）为了简化 管理中心 的 SSO 设置，您可以将 管理中心 服务提供商应用的 SAML XML 元数据文件（在 Azure 门户中称为 **联合元数据 XML** ）下载到本地计算机。

步骤 8 将现有 Azure 用户和组分配给 管理中心 服务应用。

Note 如果您计划将用户组分配给 管理中心 应用，请勿将这些组中的用户作为个人进行分配。

Note 如果计划配置用户角色映射，则可以根据个人用户权限或组权限配置要映射的角色，但单个管理中心 应用不能同时支持组和个人用户的角色映射。

What to do next

启用单点登录；请参阅 在 管理中心启用单点登录, on page 139。

为 Azure SSO 配置管理中心

在 管理中心 web 接口上使用这些说明。

Before you begin

- 在 Azure AD 门户上创建 管理中心 服务提供商应用；请参阅为 Azure 配置管理中心服务提供商应用, on page 164。
- 启用单点登录；请参阅 在 管理中心启用单点登录, on page 139。

Procedure

步骤 1 （此步骤直接从 在 管理中心启用单点登录, on page 139开始。）在 **配置 Azure 元数据** 对话框中，您有两个选择：

- 要手动输入 SSO 配置信息，请执行以下操作：
  - **a.** 点击 **手动配置** 单选按钮。
  - **b.** 输入从 Azure SSO 服务提供程序应用检索的值：
    - 对于 **身份提供程序单点登录 URL** ，输入您在 为 Azure 配置管理中心服务提供商应用, on page 164步骤 6 中记下的 **登录 URL** 。

- 对于 **身份提供程序颁发者**，输入您在 为 Azure 配置管理中心服务提供商应用, on page 164 步骤 6 中记下的 **Azure AD 标识符**。
- 对于 **X.509 证书**，请使用您在 为 Azure 配置管理中心服务提供商应用, on page 164步骤 5 中从 Azure 下载的证书。（使用文本编辑器打开证书文件，复制内容并将其粘贴到 **X.509 证书** 字段中。）

- 如果已将 Azure 生成的 XML 元数据文件保存到本地计算机（ 为 Azure 配置管理中心服务提供商应用, on page 164的步骤 7），则可以将文件上传到 管理中心：

  a. 点击 **上传文件** 单选按钮。

  b. 按照屏幕上的说明导航到本地计算机上的 XML 元数据文件并选择该文件。

步骤 2 点击**下一步**。

步骤 3 在 **验证元数据** 对话框中，查看配置参数，然后点击 **保存**。

步骤 4 点击 **测试配置**。如果系统显示错误消息，请查看 管理中心 以及 Azure 服务提供商应用的 SSO 配置，更正所有错误，然后重试。

步骤 5 当系统报告配置测试成功时，点击 **应用**。

What to do next

您可以选择为 SSO 用户配置角色映射；请参阅 在管理中心上为 Azure 配置用户角色映射, on page 167。如果您选择不配置角色映射，则默认情况下会为登录 管理中心 的所有 SSO 用户分配您在 在管理中心上为 Azure 配置用户角色映射, on page 167的步骤 4 中配置的默认用户角色。

在管理中心上为 Azure 配置用户角色映射

无论您选择哪种 SSO 提供商，在 管理中心 web 接口上为用户角色映射配置的字段都是相同的。但是，您配置的值必须考虑您使用的 SAML SSO 提供程序实施用户角色映射的方式。

Before you begin

- 查看现有的 Azure 用户和组；请参阅 查看 Azure 租户, on page 164。
- 为 管理中心配置 SSO 服务提供商应用；请参阅 为 Azure 配置管理中心服务提供商应用, on page 164。
- 在 管理中心上启用并配置单点登录；请参阅 在 管理中心启用单点登录, on page 139和 为 Azure SSO 配置管理中心 , on page 166。

Procedure

步骤 1 选择 **系统** > **用户**。

步骤 2 点击 **单点登录** 选项卡。

步骤 3 展开 **高级配置（角色映射）**。

步骤 4 从**默认用户角色 (Default User Role)** 下拉列表中选择要分配用户的 管理中心 用户角色作为默认值。

步骤 5 输入 **组成员属性**。此字符串必须与您在 Azure 中为 管理中心 服务提供商应用创建的用户声明的名称相匹配；请参阅 在 Azure IdP 上配置个人用户的用户角色映射, on page 168 的步骤 1 或 在 Azure IdP 上配置组的用户角色映射, on page 169的步骤 1。

步骤 6 在要分配给 SSO 用户的每个 管理中心 用户角色旁边，输入正则表达式。（ 管理中心 使用 Golang 和 Perl 支持的 Google RE2 正则表达式标准的受限版本。） 管理中心 将这些值与 IdP 发送到 管理中心的用户角色映射属性值和 SSO 用户信息进行比较。 管理中心 授予用户找到匹配项的所有角色的并集。

What to do next

在服务提供商应用中配置用户角色映射；请参阅 在 Azure IdP 上配置用户角色映射, on page 168。

在 Azure IdP 上配置用户角色映射

您可以在 Azure AD 门户上根据个人用户权限或组权限配置 SSO 用户角色映射。

- 要根据个人用户权限进行映射，请参阅 在 Azure IdP 上配置个人用户的用户角色映射。
- 要基于组权限进行映射，请参阅 在 Azure IdP 上配置组的用户角色映射。

当 SSO 用户登录 管理中心时，Azure 会向 管理中心 提供用户或组角色属性值，该值从在 Azure AD 门户配置的应用角色获取。 管理中心 将该属性值与分配给 SSO 配置中每个 管理中心 用户角色的正则表达式进行比较，并向用户授予找到匹配项的所有角色。（如果未找到匹配项， 管理中心 将授予用户可配置的默认用户角色。）分配给每个 管理中心 用户角色的表达式必须符合 Golang 和 Perl 支持的受限版本的 Google RE2 正则表达式标准。 管理中心 将从 Azure 接收的属性值视为使用相同标准的正则表达式，以便与 管理中心 用户角色表达式进行比较。

Note 单个 管理中心 不能同时支持组和单个用户的角色映射；您必须为 管理中心 服务提供商应用选择一种映射方法，并一致地使用它。 管理中心 只能使用 Azure 中配置的一个声明来支持角色映射。通常，对于具有许多用户的 管理中心，基于组的角色映射更有效。应考虑在整个 Azure 租户中建立的用户和组定义。

在 Azure IdP 上配置个人用户的用户角色映射

要在 Azure 中为 管理中心 服务应用的各个用户建立角色映射，请使用 Azure AD 门户向应用添加申领，将角色添加到应用的注册清单，并将角色分配给用户。

Before you begin

- 查看 Azure 租户；请参阅 查看 Azure 租户, on page 164。
- 在 Azure 中创建和配置 管理中心 服务提供商应用；请参阅为 Azure 配置管理中心服务提供商应用, on page 164。

- 配置 SSO 用户角色映射，如 在管理中心上为 Azure 配置用户角色映射, on page 167中所述。

Procedure

步骤 1 向 管理中心 服务应用的 SSO 配置添加具有以下特征的用户申领：

- **名称**：使用您在 管理中心 SSO 配置中为 **组成员属性** 输入的相同字符串。（请参阅中 在管理中心上为 Azure 配置用户角色映射, on page 167的步骤 5。）
- **名称标识符格式**：选择 持久性。
- **源**：选择 属性。
- **源属性**：选择 `user.assignedroles`。

步骤 2 编辑 管理中心 服务应用的清单（采用 JSON 格式）并添加应用角色以表示您希望分配给 SSO 用户的 管理中心 用户角色。最简单的方法是复制现有应用角色定义并更改以下属性：

- `displayName`：将显示在 AD Azure 门户中的角色的名称。
- `说明`：有关角色的简要说明。
- `Id`：一个字母数字字符串，在清单中的 ID 属性中必须是唯一的。
- `值`：表示一个或多个 管理中心 用户角色的字符串。（注意：Azure 不允许此字符串中包含空格。）

步骤 3 对于分配给管理中心服务应用的每个用户，请分配您已添加到该应用的清单中的一个应用角色。当用户使用 SSO 登录 管理中心 时，分配给该用户的应用角色是 Azure 在服务应用的申领中发送至 管理中心 的值。 管理中心 将申领与您在 SSO 配置中分配给 管理中心 用户角色的表达式进行比较（请参阅 在管理中心上为 Azure 配置用户角色映射, on page 167的第 6 步），并为用户分配匹配的所有 管理中心 用户角色。

What to do next

- 通过使用 SSO 从各种账户登录 管理中心 并确认用户已按预期分配 管理中心 用户角色，测试您的角色映射方案。

在 Azure IdP 上配置组的用户角色映射

要为 Azure 中的 管理中心 服务应用建立角色映射，请使用 Azure AD 门户向应用添加申领，向应用的注册清单添加角色，并将角色分配给组。

Before you begin

- 查看 Azure 租户；请参阅 查看 Azure 租户, on page 164。

- 在 Azure 中创建和配置 管理中心 服务提供商应用；请参阅为 Azure 配置管理中心服务提供商应用, on page 164。
- 配置 SSO 用户角色映射 ，如 在管理中心上为 Azure 配置用户角色映射, on page 167中所述。

Procedure

步骤 1 向 管理中心 服务应用的 SSO 配置添加具有以下特征的用户申领：

- **名称**：使用您在 管理中心 SSO 配置中为 **组成员属性** 输入的相同字符串。（请参阅中 在管理中心上为 Azure 配置用户角色映射, on page 167的步骤 5。）
- **名称标识符格式**：选择 持久性。
- **源**：选择 属性。
- **源属性**：选择 `user.assignedroles`。

步骤 2 编辑 管理中心 服务应用的清单（采用 JSON 格式）并添加应用角色以表示您希望分配给 SSO 用户的 管理中心 用户角色。最简单的方法是复制现有应用角色定义并更改以下属性：

- `displayName`：将在 Ad Azure 门户中显示的角色的名称。
- `说明`：有关角色的简要说明。
- `Id`：一个字母数字字符串，在清单中的 id 属性中必须是唯一的。
- `值`：表示一个或多个 管理中心 用户角色的字符串。（Azure 不允许此字符串中包含空格。）

步骤 3 对于分配给 管理中心 服务应用的每个组，请分配您已添加到该应用的清单中的一个应用角色。当用户使用 SSO 登录 管理中心 时，您分配给该用户的组的应用角色是 Azure 在服务应用的申领中发送至 管理中心 的值。 管理中心 将申领与您在 SSO 配置中分配给 管理中心 用户角色的表达式进行比较（请参阅 在管理中心上为 Azure 配置用户角色映射, on page 167的第 6 步），并为用户分配所有匹配的 管理中心 用户角色。

What to do next

通过使用 SSO 从各种账户登录 管理中心 并确认用户已按预期分配 管理中心 用户角色，测试您的角色映射方案。

Azure 用户角色映射示例

如以下示例所示，用于支持用户角色映射的管理中心SSO配置对于单个用户和组是相同的。区别在于 Azure 中 FMC 服务提供商应用的设置。

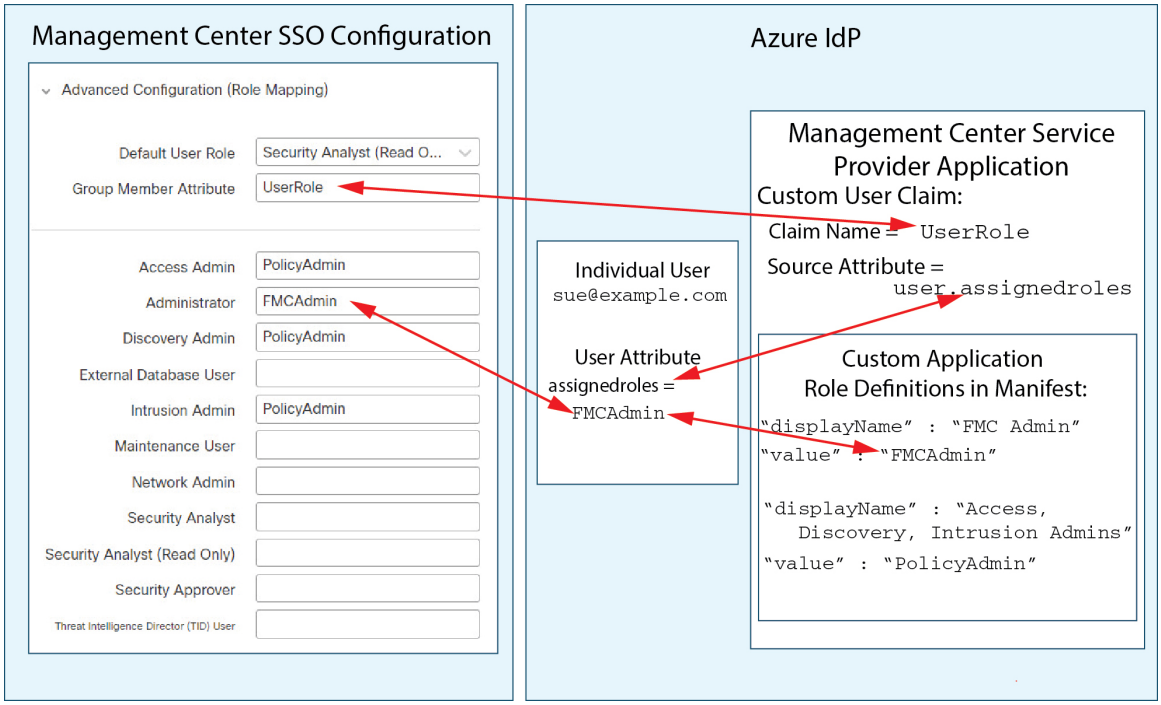
Note 您可以根据个人权限或组权限配置要映射的 管理中心 角色，但单个 FMC 应用不能同时支持组和个人用户的角色映射。 管理中心 只能使用 Azure 中配置的一个声明来支持角色映射。

个人用户账户的 Azure 角色映射示例

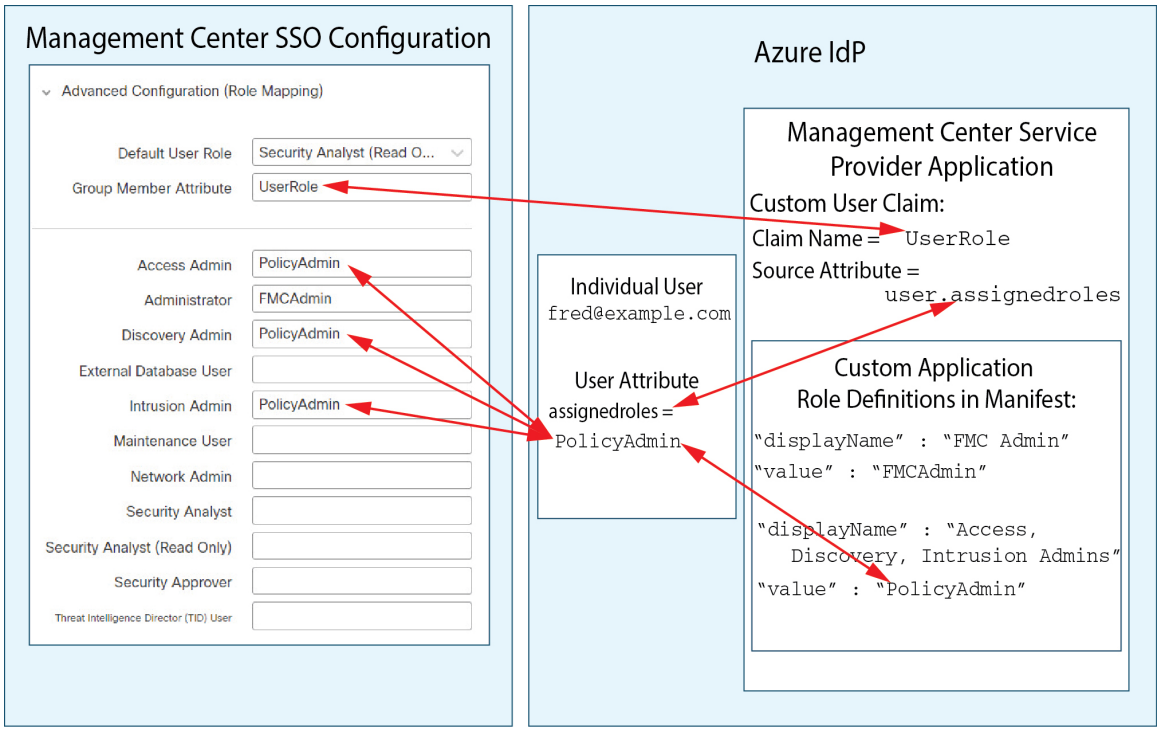
在单个用户的角色映射中，Azure 管理中心 服务应用在其清单中定义了自定义角色。（在本例中，为 FMCAdmin 和 PolicyAdmin。）这些角色可以分配给用户； Azure 将每个用户的角色分配存储在该用户的 assignedroles 属性中。该应用还定义了一个自定义用户声明，并且此声明配置为从使用 SSO 登录 FMC 的用户分配的用户角色获取其值。Azure 在 SSO 登录过程中将申领值传递给 管理中心，管理中心 将申领值与 管理中心 SSO 配置中分配给每个 管理中心 用户角色的字符串进行比较。

下图说明了 管理中心 和 Azure 配置中的相关字段和值在各个账户的用户角色映射中如何相互对应。每个图在 管理中心 和 Azure AD 门户上使用相同的 SSO 配置，但在 管理中心Azure AD 门户上为每个用户分配不同角色的配置有所不同。

- 在此图中，sue@example.com 使用 assignedroles 属性值 `FMCAdmin`，并且 管理中心 分配她的 管理中心 管理员角色。



- 在此图中，fred@example.com 使用 assignedroles 属性值 `PolicyAdmin`，并且 管理中心 分配给他角色访问管理员、发现管理员和入侵管理员。



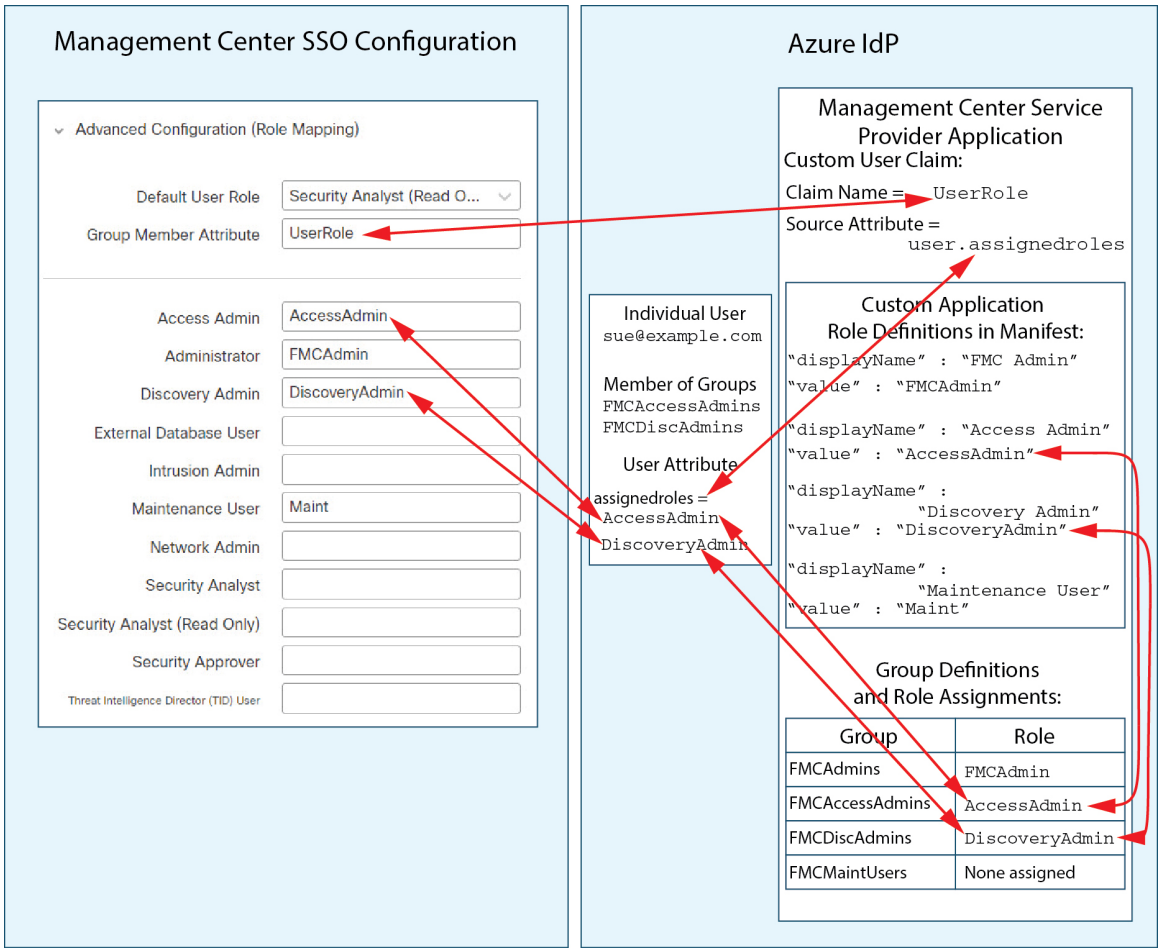
- 出于以下原因之一，为此 管理中心 分配到 Azure 服务应用的其他用户会被分配默认用户角色“安全分析师（只读）”：
  - 它们没有分配给其 assignedroles 属性的值。
  - 分配给其assignedroles 属性的值与 SSO 配置 管理中心中为用户角色配置的任何表达式都不匹配。

组的 Azure 角色映射示例

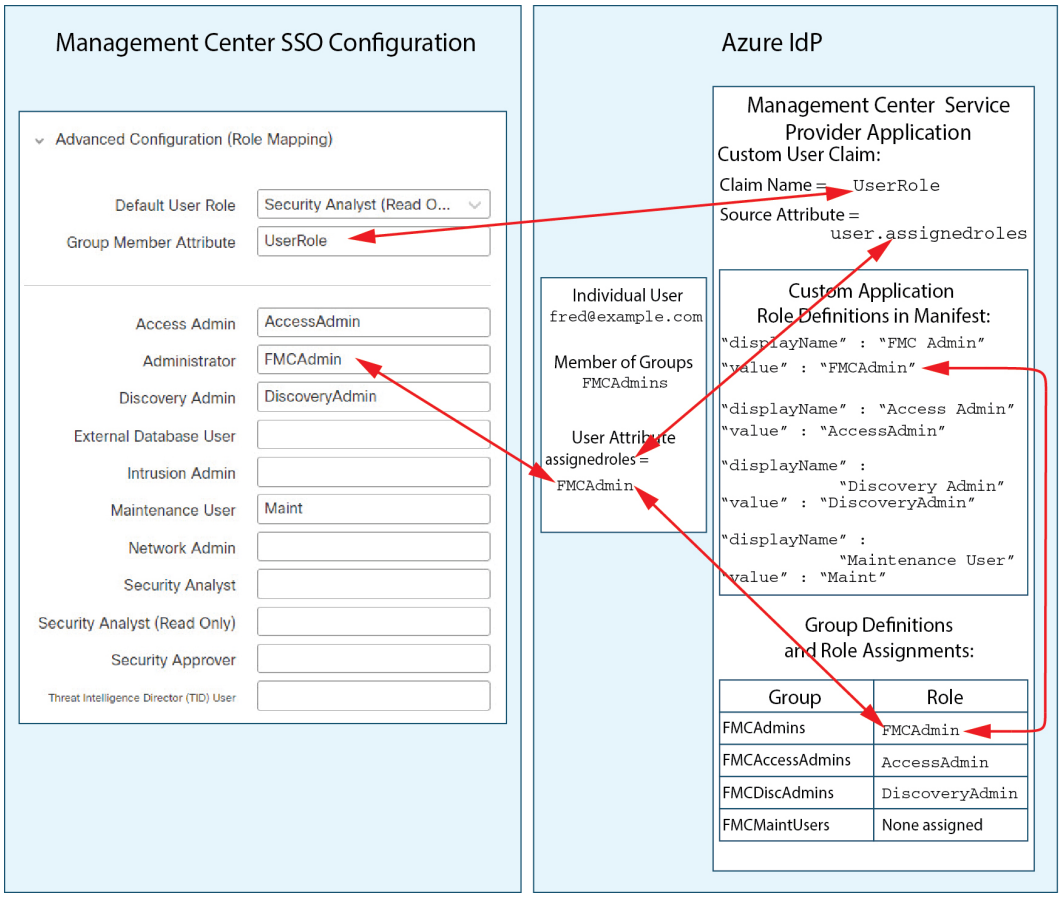
在组的角色映射中，Azure 管理中心 服务应用在其清单中定义了自定义角色。（在本例中，为 FMCAdmin、AccessAdmin、Discovery Admin 和 Maint。）这些角色可以分配给组； Azure 将每个组的角色分配传递给组成员的 assignedroles 属性。该应用还定义了一个自定义用户申领，此申领配置为从使用 SSO 登录 管理中心 的用户的已分配用户角色获取其值。Azure 在 SSO 登录过程中将申领值传递给 管理中心， 管理中心 将申领值与 管理中心 SSO 配置中分配给每个 管理中心 用户角色的字符串进行比较。

下图说明了 管理中心 和 Azure 配置中的相关字段和值在组的用户角色映射中如何相互对应。每个图在 管理中心 和 Azure AD 门户上使用相同的 SSO 配置，但在 管理中心Azure AD 门户上为每个用户分配不同角色的配置有所不同。

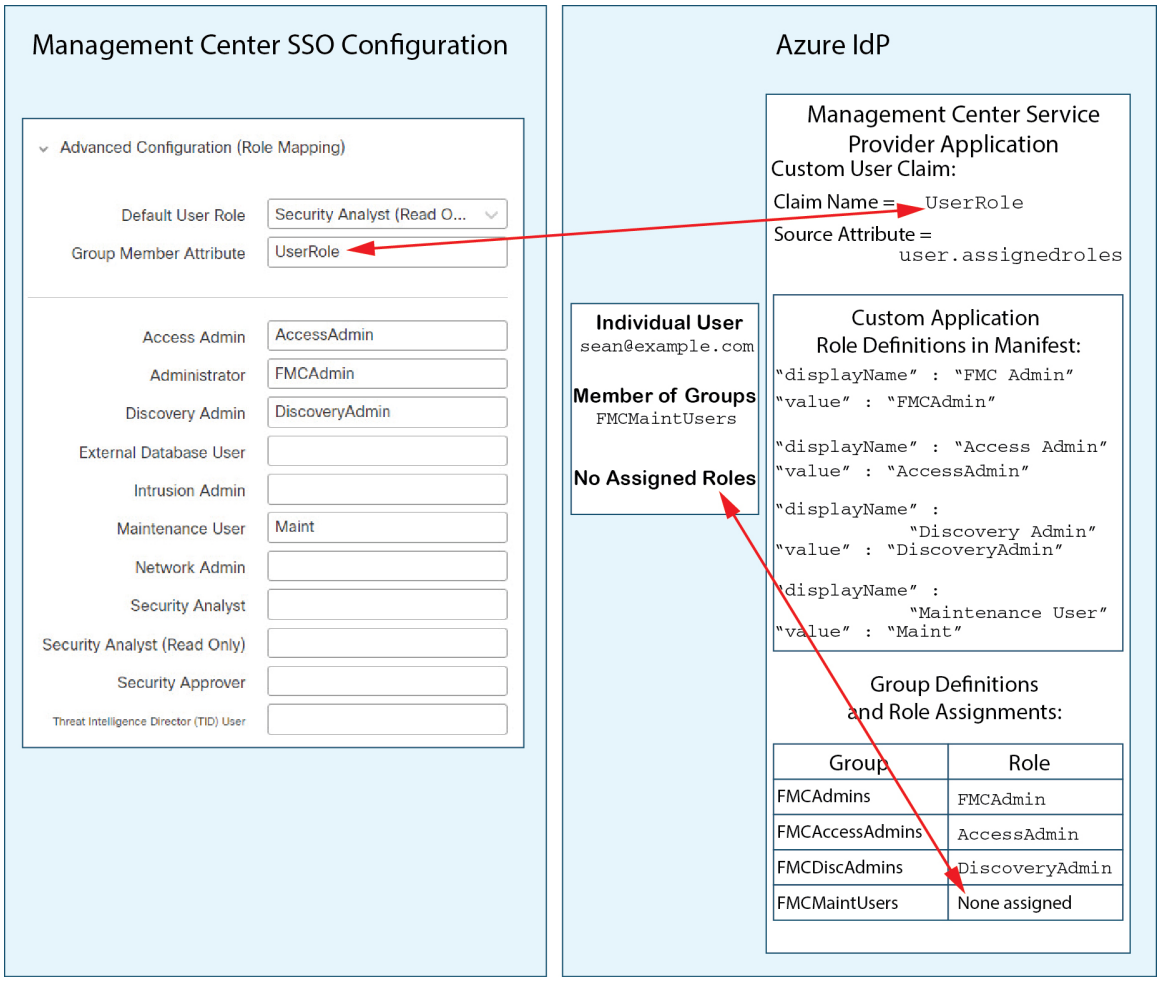
- 在此图中，sue@example.com 是组 `FMCAccessAdmins` 和 `FMCDiscoveryAdmins`的成员。她从这些组继承自定义角色 `AccessAdmin` 和 `DiscoveryAdmin`。当 Sue 使用 SSO 登录 管理中心 时， 管理中心 会为她分配访问管理员和发现管理员角色。



- 在此图中，fred@example.com 是 `FMCAdmins` 组的成员，从该组继承自定义角色 `FMCAdmin`。当Fred 使用 SSO 登录 管理中心 时， 管理中心 会为他分配管理员角色。

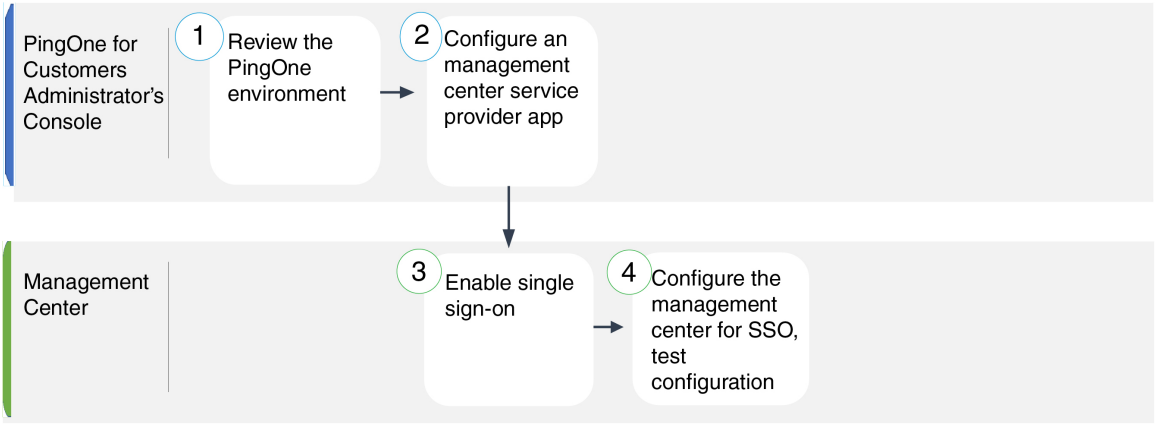


- 在此图中，sean@example.com 是 `FMCMaintUsers` 组的成员，但由于未在 Azure 管理中心 服务提供商应用中为 `FMCMaintUsers` 分配自定义角色，因此，Sean 未分配任何角色，当他使用 SSO 登录 管理中心 时， 管理中心 会为其分配默认角色“安全分析师（只读）”。



通过 PingID 配置单点登录

请参阅以下任务，以使用 PingID 的 PingOne 客户产品配置 SSO：



1	面向客户的 PingOne 管理员控制台	查看客户环境的 PingID PingOne, on page 176。
2	面向客户的 PingOne 管理员控制台	为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 176。
3	管理中心	在 管理中心启用单点登录, on page 139。
4	管理中心	为客户使用 PingID PingOne 为 SSO 配置管理中心 , on page 178。

查看客户环境的 PingID PingOne

面向客户的 PingOne 是 PingID 的云托管身份即服务 (IDaaS) 产品。在面向客户的 PingOne 中，包含用户可以使用同一 SSO 账户访问的所有联合设备的实体称为环境。在将 管理中心 添加到 PingOne 环境之前，请熟悉其组织；思考以下问题：

- 有多少用户可以访问 管理中心？
- 您是否需要添加更多用户来支持对 管理中心 的 SSO 访问？

本文档假定您已经熟悉 PingOne 客户管理员控制台，并且拥有具有组织管理员角色的账户。

为客户配置 PingID PingOne 的管理中心服务提供商应用

使用面向客户的 PingOne 管理员控制台在面向客户的 PingOne 环境中创建 管理中心 服务提供商应用，并建立基本配置设置。本文档并未介绍建立功能齐全的 SSO 环境所需的所有 PingOne 客户版功能；例如，要创建用户，请参阅 PingOne 客户文档。

Before you begin

- 熟悉面向客户的 PingOne 环境及其用户。
- 如有必要，创建更多用户。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

- 确认目标 管理中心 的登录 URL (`https://ipaddress_or_hostname`)

Note 如果可以使用多个 URL（例如，完全限定域名和 IP 地址）访问 管理中心 Web 界面，则 SSO 用户必须使用您在此任务中配置的登录 URL 一致地访问 管理中心 。

Procedure

步骤 1 使用 PingOne 客户管理员控制台使用以下设置在您的环境中创建应用：

- 选择 **Web App** 应用类型。
- 选择 **SAML** 连接类型。

步骤 2 使用 SAML 连接的以下设置配置应用：

- 对于 **ACS URL**，将字符串 `/sam/acs` 附加到登录 管理中心 URL。例如：`https://ExampleFMC/saml/acs`。
- 对于 **签名证书**，请选择签名断言和响应。
- 对于 **签名算法** ，请选择 RSA_SHA256。
- 对于 **实体 ID**，将字符串 `/saml/metadata` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/metadata`。
- 对于 **SLO 绑定** ，选择 HTTP POST。
- 对于 **断言有效期** ，输入 300。

步骤 3 在应用的 SAML 连接信息中，请注意以下值：

- **单点登录服务**
- **颁发机构 ID**

在 管理中心 Web 界面上使用 PingID 的 PingOne 客户产品配置 SSO 时，需要这些值。

步骤 4 对于 **SAML 属性**，请为单个必需属性进行以下选择：

- **PINGONE 用户属性**： 邮箱地址
- **应用属性**： `saml_subject`

步骤 5 下载 X509 PEM (`.crt`) 格式的签名证书，并将其保存到本地计算机。

步骤 6 （可选）要简化 管理中心 的 SSO 设置，您可以将 管理中心 服务提供商应用的 SAML XML 元数据文件下载到本地计算机。

步骤 7 启用应用。

What to do next

启用单点登录；请参阅 在 管理中心启用单点登录, on page 139。

为客户使用 PingID PingOne 为 SSO 配置管理中心

在 管理中心 web 接口上使用这些说明。

Before you begin

- 在 PingOne 客户管理员控制台上创建 管理中心 服务提供商应用；请参阅为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 176。
- 启用单点登录；请参阅 在 管理中心启用单点登录, on page 139。

Procedure

步骤 1 （此步骤直接从 在 管理中心启用单点登录, on page 139开始。）在 **配置 PingID 元数据** 对话框中，您有两个选择：

- 要手动输入 SSO 配置信息，请执行以下操作：
  a. 点击 **手动配置** 单选按钮。
  b. 输入您从 PingOne 客户管理员控制台检索的值：
     - 对于 **身份提供程序单点登录 URL**，输入您在 为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 176步骤 3 中记下的 **单点登录服务** 。
     - 对于 **身份提供程序颁发者**，请输入您在 为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 176步骤 3 中记下的 **颁发者 ID** 。
     - 对于 **X.509 证书**，请使用您在 为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 176步骤 5 中从 PingOne for Customer 下载的证书。（使用文本编辑器打开证书文件，复制内容并将其粘贴到 **X.509 证书** 字段中。）
- 如果已将 PingOne for Customer 生成的 XML 元数据文件保存到本地计算机（ 为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 176的步骤 6 ），则可以将文件上传到 管理中心：
  a. 点击 **上传文件** 单选按钮。
  b. 按照屏幕上的说明导航到本地计算机上的 XML 元数据文件并选择该文件。

步骤 2 点击**下一步**。

步骤 3 在 **验证元数据** 对话框中，查看配置参数，然后点击 **保存**。

步骤 4 展开 **高级配置（角色映射）**。

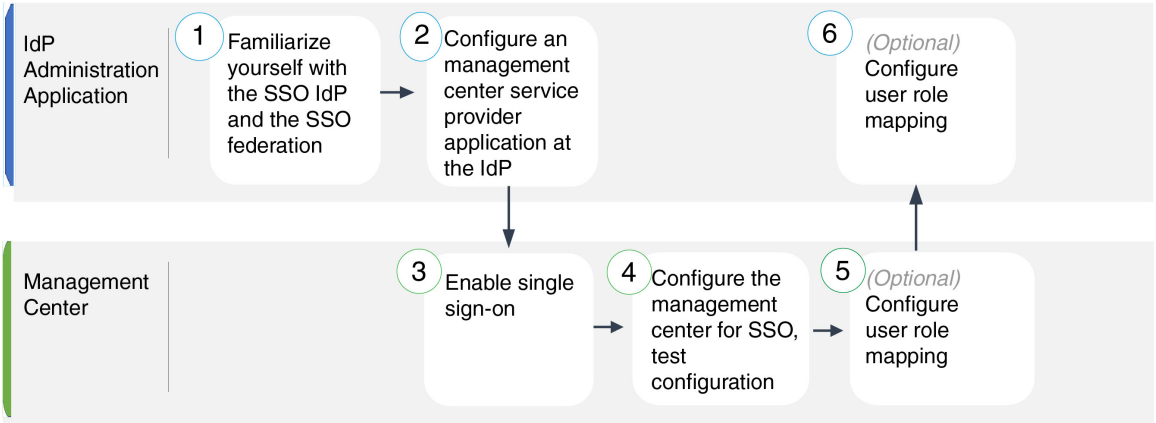
步骤 5 从**默认用户角色 (Default User Role)** 下拉列表中选择要分配用户的 管理中心 用户角色作为默认值。

步骤 6 点击 **测试配置**。如果系统显示错误消息，请查看 管理中心 的 SSO 配置以及面向客户的 PingOne 服务提供商应用，更正所有错误，然后重试。

步骤 7 当系统报告配置测试成功时，点击 **应用**。

使用任何符合 SAML 2.0 标准的 SSO 提供程序配置单点登录

管理中心 支持使用符合 SAML 2.0 SSO 协议的任何 SSO 身份提供程序 (IdP) 进行单点登录。使用各种 SSO 提供程序的通用说明必须解决要在较高级别执行的任务；使用本文档中未明确提及的提供商建立 SSO 要求您精通所选的 IdP。这些任务可帮助您确定使用任何符合 SAML 2.0 标准的 SSO 提供程序配置 管理中心 单点登录的步骤：



1	IdP 管理应用	熟悉 SSO 身份提供程序和 SSO 联合身份验证, on page 180。
2	IdP 管理应用	为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用, on page 180。
3	管理中心	在 管理中心启用单点登录, on page 139。
4	管理中心	为使用任何 SAML 2.0 兼容 SSO 提供程序的 SSO 配置 管理中心, on page 182。
5	管理中心	在 管理中心上为符合 SAML 2.0 标准的 SSO 提供程序配置用户角色映射, on page 183。
6	IdP 管理应用	在 IdP 上为符合 SAML 2.0 标准的 SSO 提供程序配置 管理中心 用户角色映射, on page 184。

熟悉 SSO 身份提供程序和 SSO 联合身份验证

阅读 IdP 供应商文档时，请记住以下注意事项：

- SSO 提供商是否要求用户在使用 IdP 之前订用或注册任何服务？
- SSO 提供程序使用哪些术语来表示常见的 SSO 概念？例如，为了指代一组联合服务提供商应用，Okta 使用 “组织”，而 Azure 使用“租户”。
- SSO 提供程序是否仅支持 SSO 或一套功能（例如，多因素身份验证或域管理）？（这可能会影响功能之间共享的某些元素的配置，尤其是用户和组。）
- IdP 用户账户需要哪些权限才能配置 SSO？
- SSO 提供商要求您为服务提供商应用建立哪些配置？例如，Okta 会自动生成 X509 证书以保护其与 管理中心的通信，而 Azure 要求您使用 Azure 门户界面生成该证书。
- 如何创建和配置用户和组？如何将用户分配到组？如何授予用户和组访问服务提供商应用的权限？
- 在测试 SSO 连接之前，SSO 提供商是否要求将至少一个用户分配给服务提供商应用？
- SSO 提供程序是否支持用户组？如何配置用户和组属性？如何将属性映射到 SSO 配置中的 管理中心 用户角色？
- 是否需要向联盟添加更多用户或组以支持 管理中心上的 SSO？
- 联盟成员中的用户是否属于组？
- 用户和组定义是 IdP 本地的，还是从 Active Directory、RADIUS 或 LDAP 等用户管理应用导入的？
- 您要分配哪种类型的用户角色？（如果您选择不分配用户角色，管理中心会自动为用户分配一个可配置的默认用户角色给所有 SSO 用户。）
- 如何组织联盟中的用户和组，以支持您的用户角色映射计划？

为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用

通常，SSO 提供商要求您在 IdP 上为每个联合应用配置服务提供商应用。支持 SAML 2.0 SSO 的所有 IdP 都需要相同的服务提供商应用配置信息，但某些 IdP 会自动为您生成一些配置设置，而其他 IdP 则要求您自己配置所有设置。

Note 如果您计划将用户组分配给 管理中心 应用，请勿将这些组中的用户作为个人进行分配。

Note 管理中心 不能支持使用多个 SSO 属性的角色映射；您必须选择用户角色映射或组角色映射，并配置单个属性以将用户角色信息从 IdP 传送到 管理中心。

Before you begin

- 熟悉 SSO 联合及其用户和组；请参阅 熟悉 SSO 身份提供程序和 SSO 联合身份验证, on page 180。
- 确认您的 IdP 账户具有执行此任务所需的权限。
- 如有必要，在 SSO 联合中创建用户账户和/或组。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

- 确认目标 管理中心 的登录 URL (`https://ipaddress_or_hostname`)

Note 如果可以使用多个 URL 访问您的 管理中心 Web 接口。（例如，完全限定域名以及 IP 地址），SSO 用户必须使用您在此任务中配置的登录 URL 一致地访问 管理中心 。

Procedure

步骤 1 在 IdP 上创建新的服务提供商应用。

步骤 2 配置 IdP 所需的值。请务必添加下面列出的字段，以通过 管理中心支持 SAML 2.0 SSO 功能。（由于不同的SSO服务提供商对SAML概念使用不同的术语，此列表提供了这些字段的备用名称，以帮助您在 IdP 应用中找到正确的设置。）：

- 服务提供商实体 ID、服务提供商标识符、受众 URI：服务提供商的全局唯一名称 (管理中心)，格式为 URL。要创建它，请将字符串 `/saml/metadata` 附加到 管理中心 登录 URL，例如 `https://ExampleFMC/saml/metadata`。
- 单点登录 URL、收件人 URL、断言使用者服务 URL：浏览器代表 IdP 向其发送信息的服务提供商 (管理中心) 地址。要创建它，请将字符串 `saml/acs` 附加到 管理中心 登录 URL，例如 `https://ExampleFMC/saml/acs`。
- X.509 证书：用于保护 管理中心 与 IdP 之间的通信的证书。某些 IdP 可能会自动生成证书，而某些 IdP 可能要求您使用 IDP 接口明确生成证书。

步骤 3 （如果要向应用分配组，则可选）将单个用户分配到 管理中心 应用。（如果您计划将组分配给 管理中心 应用，请不要将这些组的成员作为个人进行分配。）

步骤 4 （如果要将单个用户分配给应用，则可选。）将用户组分配给 管理中心 应用。

步骤 5 （可选）某些 IdP 能够生成 SAML XML 元数据文件，其中包含您在此任务中配置的信息，格式为符合 SAML 2.0 标准。如果您的 IdP 提供此功能，您可以将文件下载到本地计算机，以简化 管理中心 上的 SSO 配置过程。

What to do next

启用单点登录；请参阅 在 管理中心启用单点登录, on page 139。

为使用任何 SAML 2.0 兼容 SSO 提供程序的 SSO 配置 管理中心

在 管理中心 web 接口上使用这些说明。要使用任何符合 SAML 2.0 的 SSO 提供程序为 SSO 配置 管理中心 ， 您需要来自 IdP 的信息。

Before you begin

- 查看 SSO 联盟的组织及其用户和组。
- 在 IdP 上配置 管理中心 服务提供商应用；请参阅为使用任何 SAML 2.0 兼容 SSO 提供程序的 SSO 配置 管理中心 , on page 182。
- 从 IdP 收集服务提供商应用的以下 SSO 配置信息。由于不同的 SSO 服务提供商对 SAML 概念使用不同的术语，因此此列表提供了这些字段的备用名称，以帮助您在 IdP 应用中找到正确的值：
  - 身份提供程序单点登录 URL、登录 URL：浏览器代表 管理中心发送信息的 IdP URL。
  - 身份提供者颁发者、身份提供者颁发者 URL、颁发者 URL：IdP 的全局唯一名称，通常格式为 URL。
  - 用于保护 管理中心 和 IdP 之间通信的 X.509 数字证书。
- 启用单点登录；请参阅 在 管理中心启用单点登录, on page 139。

Procedure

步骤 1 （此步骤直接从 在 管理中心启用单点登录, on page 139开始。）在 **配置 SAML 元数据** 对话框中，您有两个选择：

- 要手动输入 SSO 配置信息，请执行以下操作：
  a. 点击 **手动配置** 单选按钮。
  b. 输入之前从 SSO 服务提供程序应用获取的以下值：
    - **身份提供程序单点登录 URL**
    - **身份提供程序颁发机构**
    - **X.509 证书**

- 如果您保存了 IdP 生成的 XML 元数据文件（ 为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用, on page 180中的步骤 5），则可以将该文件上传到 管理中心：
  a. 点击 **上传文件** 单选按钮。
  b. 按照屏幕上的说明导航到本地计算机上的 XML 元数据文件并选择该文件。

步骤 2 点击**下一步**。

步骤 3 在 **验证元数据** 对话框中，查看配置参数，然后点击 **保存**。

步骤 4 点击 **测试配置**。如果系统显示错误消息，请查看 管理中心 的 SSO 配置以及 IdP 上的服务提供商应用配置，更正所有错误，然后重试。

步骤 5 当系统报告配置测试成功时，点击 **应用**。

What to do next

您可以选择为 SSO 用户配置用户角色映射；请参阅 在 管理中心上为符合 SAML 2.0 标准的 SSO 提供程序配置用户角色映射, on page 183。如果您选择不配置角色映射，则默认情况下会为登录 管理中心 的所有 SSO 用户分配您在 在 管理中心上为符合 SAML 2.0 标准的 SSO 提供程序配置用户角色映射, on page 183的步骤 4 中配置的默认用户角色。

在 管理中心上为符合 SAML 2.0 标准的 SSO 提供程序配置用户角色映射

要实施 SAML SSO 用户角色映射，您必须在 IdP 和 管理中心上建立协调配置。

- 在 IdP 上，建立用户或组属性以传达用户角色信息并为其分配值； IdP 在对 SSO 用户进行身份验证和授权后，会将这些信息发送到 管理中心。
- 在 管理中心上，将值与要分配给用户的每个 管理中心 用户角色相关联。

当 IdP 发送与授权用户关联的 管理中心 用户或组属性时， 管理中心 会将属性值与与每个 管理中心 用户角色关联的值进行比较，并为用户分配产生匹配项的所有角色。管理中心执行此比较，将两个值视为符合 Golang 和 Perl 支持的受限版本的 Google RE2 正则表达式的正则表达式。

无论您选择哪种 SSO 提供商，在 管理中心 web 接口上为用户角色映射配置的字段都是相同的。但是，您配置的值必须考虑您使用的 SAML SSO 提供程序实施用户角色映射的方式。您的 IdP 可能会对用户或组属性实施语法限制；如果是，则必须使用符合这些要求的角色名称和正则表达式设计用户角色映射方案。

Before you begin

- 为 管理中心配置 SSO 服务提供商应用；请参阅 为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用, on page 180。
- 在 管理中心上启用和配置单点登录，请参阅 在 管理中心启用单点登录, on page 139和 为使用任何 SAML 2.0 兼容 SSO 提供程序的 SSO 配置 管理中心 , on page 182。

Procedure

步骤 1 选择 **系统** > **用户**。

步骤 2 点击 **单点登录** 选项卡。

步骤 3 展开 **高级配置（角色映射）**。

步骤 4 从**默认用户角色 (Default User Role)** 下拉列表中选择要分配用户的 管理中心 用户角色作为默认值。

步骤 5 输入 **组成员属性**。此字符串必须与 IdP 管理中心 服务提供商应用中为使用用户或组的用户角色映射配置的属性名称匹配。（请参阅 在 IdP 上为符合 SAML 2.0 标准的 SSO 提供程序配置 管理中心 用户角色映射, on page 184的第 1 步。）

步骤 6 在要分配给 SSO 用户的每个 管理中心 用户角色旁边，输入正则表达式。（ 管理中心 使用 Golang 和 Perl 支持的 Google RE2 正则表达式标准的受限版本。） 管理中心 将这些值与 IdP 发送到 管理中心的用户角色映射属性值和 SSO 用户信息进行比较。 管理中心 授予用户找到匹配项的所有角色的并集。

What to do next

在服务提供商应用中配置用户角色映射；请参阅 在 IdP 上为符合 SAML 2.0 标准的 SSO 提供程序配置 管理中心 用户角色映射, on page 184。

在 IdP 上为符合 SAML 2.0 标准的 SSO 提供程序配置 管理中心 用户角色映射

每个 IdP 配置用户角色映射的详细步骤各不相同。您必须确定如何为服务提供商应用创建自定义用户或组属性，并在 IdP 为每个用户或组分配属性值，以将用户或组权限传达给 管理中心。请注意以下事项：

- 如果您的 IdP 从第三方用户管理应用（例如 Active Directory、LDAP 或 Radius）导入用户或组配置文件，这可能会影响您如何使用属性进行角色映射。
- 考虑整个 SSO 联合中的用户和组角色定义。
- 管理中心 不能支持使用多个SSO属性的角色映射；您必须选择用户角色映射或组角色映射，并配置单个属性以将用户角色信息从 IdP 传送到 管理中心。
- 对于具有许多用户的 管理中心 ，组角色映射通常更有效。
- 如果将用户组分配给 管理中心 应用，则不要将这些组中的用户作为个人进行分配。
- 为了确定与 管理中心 用户角色的匹配， 管理中心 将从 IdP 接收的用户和组角色属性值视为符合 Golang 和 Perl 支持的 Google RE2 正则表达式标准的受限版本。您的 IdP 可能会对用户或组属性实施某些语法限制。如果是，则必须使用符合这些要求的角色名称和正则表达式设计用户角色映射方案。

Before you begin

- 确认您的 IdP 账户具有执行此任务所需的权限。

- 在 IdP 上配置 管理中心 服务提供商应用（请参阅为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用, on page 180）。

Procedure

步骤 1 在 IdP 上，创建或指定要发送到 管理中心 的属性，以包含每个用户登录的角色映射信息。这可能是用户属性、组属性或从源（例如 IdP 或第三方用户管理应用维护的用户或组定义）获取其值的其他属性。

步骤 2 配置属性获取其值的方式。将可能的值与 管理中心 SSO 配置中的用户角色关联的值进行协调。

自定义 Web 界面的用户角色

必须为每个用户帐户定义用户角色。本部分介绍如何管理用户角色，以及如何配置可进行 Web 界面访问的自定义用户角色。对于默认用户角色，请参阅用户角色，第 114 页。

创建自定义用户角色

自定义用户角色可以拥有任意一组基于菜单的权限和系统权限，它们可以是全新的用户角色，可以从预定义或其他用户角色复制而来，也可以从其他 管理中心导入。

注释 （需要版本 7.4.1+） 虽然您可以在不升级产品的情况下启用对内容更新的访问，但我们建议您采用相反的做法：没有内容的产品。也就是说，如果您在自定义用户角色中启用**产品升级**，请同时启用**内容更新**。否则，您可能无法手动上传升级包 以及升级较早的 ASA FirePOWER 和 NGIPSv 设备。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击 **User Roles**。

步骤 3 使用以下方法之一添加新用户角色：

- 点击 **Create User Role**。
- 点击要复制的用户角色旁边的 **复制**（）。
- 从其他 管理中心导入自定义用户角色：
  1. 在其他 管理中心上，点击 **导出**（）将角色保存到您的 PC。
  2. 在新 管理中心上，选择 **系统**（⚙）> **工具** > **导入/导出**。

3. 点击 **上传数据包**，然后按照说明将保存的用户角色导入到新 管理中心。

步骤 4 为新用户角色输入一个**名称**。用户角色名称区分大小写。

步骤 5 （可选） 添加**说明**。

步骤 6 为新角色选择**基于菜单的权限**。

选择权限时，会选择其所有子级，且多值权限使用第一个值。如果清除选择高级权限，则也会清除其所有子级。如果您选择权限但没有选择其所有子级，则权限以斜体文本显示。

复制要用作自定义角色基础的预定义用户角色将预先选择与该预定义角色关联的权限。

可以对自定义用户角色应用受限搜索。这些搜索将限制用户可在“分析”菜单下可用页面上的表中所看到的数据。可以配置受限搜索，方法是先创建专用的已保存搜索，然后在适当的基于菜单的权限下从**受限搜索**下拉菜单中选择该搜索。

步骤 7 （可选） 选中 **外部数据库访问（只读）** 复选框为新角色设置数据库访问权限。

此选项使用支持 JDBC SSL 连接的应用提供数据库的只读访问权限。如果第三方应用要向 管理中心进行身份验证，必须在系统设置中启用数据库访问权限。

步骤 8 （可选） 要为新用户角色设置升级权限，请参阅启用用户角色升级，第 188 页。

步骤 9 点击**保存 (Save)**。
自定义角色已保存。如果系统确定它是只读角色，则会将该角色标记为“（只读）”。这在为只读和读写用户配置并发会话数时非常重要。不能通过将“（只读）”添加到角色名称来将角色设置为只读。 有关并发会话限制的详细信息，请参阅 用户配置，第 104 页。

示例

您可以为与访问控制相关的功能创建自定义用户角色，以指定用户是否可以查看和修改访问控制和关联策略。

下表显示了如何区分应能配置访问控制策略的所有方面（入侵配置除外）的网络管理员，以及应仅能配置与入侵相关的功能的入侵管理员。 **修改威胁配置** 权限允许在规则中选择入侵策略、变量集和文件策略，配置网络分析和入侵策略的高级选项，配置安全智能策略访问控制策略，以及策略默认操作中的入侵操作。**修改剩余访问控制策略配置 (Modify Remaining Access Control Policy Configuration)** 权限涵盖策略和规则的所有其他方面，包括创建和删除策略和规则。在此示例中，策略审批人可以查看（但无法修改）访问控制和入侵策略。他们还可以将配置更改部署到设备。

表 5: 访问控制自定义角色示例

基于菜单的权限	示例角色		
	访问控制编辑器	**Intrusion & Network Analysis Editor**	策略审批人
访问控制	是	是	是

基于菜单的权限	示例角色		
	访问控制编辑器	**Intrusion & Network Analysis Editor**	策略审批人
访问控制策略	是	是	是
修改访问控制策略 (Modify Access Control Policy)	否	是	否
修改威胁配置	否	是	否
修改其余的访问控制策略配置	是	否	否
入侵策略	否	是	是
修改入侵策略	否	是	否
将配置部署到设备	否	否	是

停用用户角色

停用角色会从已分配有该角色的任何用户从移除该角色和所有相关权限。不能删除预定义用户角色，但是可以将其停用。

在多域部署中，系统会显示在当前域中创建的自定义用户角色，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义用户角色，您不可以对其进行编辑。要查看和编辑较低域中的自定义用户角色，请切换至该域。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击 **User Roles**。

步骤 3 点击要激活或停用的用户角色旁边的滑块。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

如果在具有某个角色的用户已登录时通过远端控制管理停用，然后重新启用该角色，或者在该用户的登录会话期间从备份恢复用户或用户角色，则该用户必须重新登录到Web 界面中才能重新获取对 IPMItool 命令的访问。

启用用户角色升级

可以通过密码为自定义用户角色提供权限，以除基本角色的权限以外，暂时获取其他目标用户角色的权限。通过此功能，您可以在某一用户不在场时轻松替换用户，或更密切地跟踪高级用户权限的使用。默认的用户角色不支持升级。

例如，基本角色的权限非常有限的用户可升级到管理员角色来执行管理操作。可以配置此功能，以便用户可以使用其自己的密码，或者因此使用所指定的其他用户的密码。通过第二个选项，可以轻松管理所有适用用户的一个升级密码。

要配置用户角色升级，请参阅以下工作流程。

过程

步骤 1 设置升级目标角色，第 188 页。一次只能有一个用户角色作为升级目标角色。

步骤 2 为升级配置自定义用户角色，第 188 页。

步骤 3 （对于登录的用户）升级用户角色，第 189 页。

设置升级目标角色

可以分配任何用户角色（预定义或自定义）来充当系统范围的升级目标角色。这是自定义角色可升级到的角色（如果具备这个能力）。一次只能有一个用户角色作为升级目标角色。每次升级持续时长为登录会话的持续时间，并会记录在审计日志中。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击 **User Roles**。

步骤 3 点击 **Configure Permission Escalation**。

步骤 4 从**升级目标**下拉列表中选择一个用户角色。

步骤 5 点击 **OK**，保存更改。

更改升级目标角色立即生效。已升级会话中的用户现在具有新升级目标的权限。

为升级配置自定义用户角色

要对其启用升级的用户必须属于已启用升级的自定义用户角色。以下步骤介绍如何为自定义用户角色启用升级。

为自定义角色配置升级密码时，请考虑贵组织的需求。如果要轻松管理多个升级用户，可能需要选择另一个使用密码充当升级密码的用户。如果更改该用户的密码或停用该用户，则需要该密码的所

有升级用户都会受影响。通过此操作，可以更加高效地管理用户角色升级，尤其是在选择可以集中管理的外部身份验证用户的情况下。

开始之前

根据设置升级目标角色，第 188 页设置目标用户角色。

过程

步骤 1 开始配置自定义用户角色，如创建自定义用户角色，第 185 页中所述。

步骤 2 在 **系统权限**中，选择 **设置此角色以升级至：维护用户** 复选框。

当前升级目标角色列于复选框旁边。

步骤 3 选择此角色用于升级的密码。此时您有两种选择：

- 如果希望具有此角色的用户在升级时使用其自己的密码，请选择**使用分配的用户密码进行身份验证**。
- 如果希望具有此角色的用户使用其他用户的密码，请选择**使用指定用户的密码进行身份验证**，并输入该用户名。

  注释 在使用其他用户的密码进行身份验证时，可以输入任何用户名，甚至是已停用或不存在的用户的用户名。停用其密码用于升级的用户会使具有需要该密码的角色的用户无法升级。如有必要，可以使用此功能快速移除升级能力。

步骤 4 点击**保存 (Save)**。

升级用户角色

当用户具有带升级权限的已分配自定义用户角色时，该用户可以随时升级到目标用户的权限。请注意，升级对用户首选项没有影响。

过程

步骤 1 从用户名下的下拉列表中，选择**升级权限 (Escalate Permissions)**。

如果您没有看到此选项，则您的管理员没有为您的用户角色启用升级。

步骤 2 输入身份验证密码。

步骤 3 点击**升级 (Escalate)**。除当前角色以外，您现在具有升级目标角色的所有权限。

升级持续至登录会话结束。要仅返回到基本角色的权限，必须注销，然后开始新会话。

LDAP 身份验证连接故障排除

如果创建 LDAP 身份验证对象，并且其无法成功连接到选择的服务器或无法检索所需的用户列表，则可以调整该对象中的设置。

如果在测试连接时该连接失败，请尝试以下建议对配置进行故障排除。

- 使用 Web 界面屏幕顶部和测试输出中显示的消息确定对象的哪些方面导致问题。
- 检查用于对象的用户名和密码是否有效：
  - 检查用户是否有权通过使用第三方 LDAP 浏览器连接到 LDAP 服务器来浏览至基本可分辨名称中指示的目录。
  - 检查用户名对于 LDAP 服务器的目录信息树是否唯一。
  - 如果在测试输出中显示 LDAP 绑定错误 49，则表明用户的用户绑定失败。请尝试通过第三方应用对服务器进行身份验证，以了解通过该连接进行的绑定是否也失败。
- 检查是否已正确识别服务器：
  - 检查服务器 IP 地址或主机名是否正确。
  - 检查是否有从本地设备到要连接的身份验证服务器的 TCP/IP 访问权限。
  - 检查对服务器的访问是否未被防火墙阻止，以及在对象中配置的端口是否已打开。
  - 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与用于服务器的主机名匹配。
  - 如果是对 CLI 访问进行身份验证，请检查是否未对服务器连接使用 IPv6 地址。
  - 如果使用了服务器类型默认值，请检查是否具有正确的服务器类型，并再次点击**设置默认值 (Set Defaults)** 以重置默认值。
- 如果键入了基本可分辨名称，请点击**获取 DN (Fetch DNs)** 以检索服务器上的所有可用基本可分辨名称，然后从列表中选择名称。
- 如果使用的是任意过滤器、访问属性或高级设置，请检查各项是否有效且正确键入。
- 如果使用的是任意过滤器、访问属性或高级设置，请尝试移除各设置并测试没有此设置的对象。
- 如果使用的是基本过滤器或 CLI 访问过滤器，请确保用括号将过滤器括起来，并且使用的是有效的比较运算符（包括括号在内，最大450个字符）。
- 要测试受限更多的基本过滤器，请尝试将其设置为基本可分辨名称，以使用户仅检索该用户。
- 如果使用的是加密连接：
  - 检查证书中 LDAP 服务器的名称是否与用于连接的主机名匹配。
  - 检查是否未对加密服务器连接使用 IPv6 地址。

- 如果使用的是测试用户，请确保正确键入用户名和密码。
- 如果使用的是测试用户，请移除用户凭证并测试对象。
- 通过连接到 LDAP 服务器并使用以下语法测试使用的查询：

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

例如，如果是尝试使用 `domainadmin@myrtle.example.com` 用户和基本过滤器 (`cn=*`) 连接到 `myrtle.example.com` 上的安全域，则可以使用以下语句测试连接：

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

如果可以成功测试连接，但在部署平台设置策略后身份验证不起作用，请检查在应用到设备的平台设置策略中是否已启用要使用的身份验证和对象。

如果成功连接，但要调整连接检索到的用户列表，则可以添加或更改基本过滤器或CLI访问过滤器，或者使用限制较多或较少的基本 DN。

在对与 Active Directory (AD) 服务器的连接进行身份验证时，尽管与 AD 服务器的连接成功，但连接事件日志很少指示受阻 LDAP 流量。当 AD 服务器发送重复的重置数据包时，会出现此不正确的连接日志。威胁防御 设备将第二个重置数据包识别为新连接请求的一部分，并使用“阻止”操作记录连接。

配置用户首选项

根据您的用户角色，您可以为您的用户账号指定某些首选项。

在多域部署中，用户首选项适用于您的帐户有权访问的所有域。当指定主页和控制面板首选项时，请记住某些页面和控制面板构件会受域限制。

更改密码

所有用户帐户均采用密码保护。可以随时更改密码，根据用户帐户设置，可能需要定期更改密码。

启用密码强度检查时，密码必须符合 管理中心用户帐户的指南和限制，第 117 页中所述的强密码要求。

如果是 LDAP 或 RADIUS 用户，则不能通过 Web 界面更改密码。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 点击**更改密码**。

步骤 3 （可选）选中 **显示密码** 复选框可在使用此对话时查看密码。

步骤 4 输入您的 **当前密码**。

步骤 5 此时您有两种选择：

- 输入您的新密码的 **新密码** 和 **确认密码**。
- 点击**生成密码**按钮，让系统为您创建符合所列条件的密码。（生成的密码是非助记密码；如果您选择此选项，请仔细记下密码。）

步骤 6 点击**应用 (Apply)**。

更改到期密码

根据用户帐户设置，密码可能已过期。在账户已创建时，将会设置密码到期时间段。如果密码已过期，系统会显示 Password Expiration Warning 页面。

过程

在“密码到期警告”(Password Expiration Warning) 页面上，您有两种选择：

- 点击**更改密码**，立即更改密码。如果剩余的警告天数为零，则**必须**更改密码。

  提示 启用密码强度检查时，密码必须符合 管理中心用户帐户的指南和限制，第 117 页中所述的强密码要求。

- 点击**跳过**，稍后更改密码。

更改 Web 接口外观

您可以更改 Web 接口的显示方式。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。默认情况下，系统会显示 **常规** 选项卡。

步骤 2 选择主题：

- **亮色**
- **Dusk**

- **经典** （6.6 之前版本的外观）

指定主页

可以将网络界面中的页面指定用作该设备的主页。默认主页为“默认控制面板”(**概述**>**控制面板**)，但对无权访问控制面板的用户例外，录入外部数据库用户。（请参阅 指定默认控制面板，第 198 页以设置默认控制面板。）

在多域部署中，您选择的主页适用于您的用户帐户具有访问权限的所有域。为经常访问多个域的帐户选择主页时，请记住某些页面限制为全局域。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 点击 **Home Page**。

步骤 3 从下拉列表中选择要用作主页的页面。

下拉列表中的选项基于用户帐户的访问权限。有关详细信息，请参阅用户角色，第 114 页。

步骤 4 点击**保存 (Save)**。

配置事件视图设置

使用“事件视图设置”页面配置 管理中心上事件视图的特征。请注意，一些事件视图配置仅对特定的用户角色可用。使用外部数据库用户角色的用户可以查看事件视图设置用户界面的某些部分，但是更改这些设置不会产生有意义的结果。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 点击 **Event View Settings**。

步骤 3 在 **事件首选项** 部分，配置事件视图的基本特征；请参阅 事件视图首选项，第 194 页。

步骤 4 在 **文件首选项** 部分，配置文件下载首选项；请参阅 文件下载首选项，第 195 页。

步骤 5 在 **默认时间窗口** 部分，配置默认时间窗口；请参阅 默认时间窗口，第 195 页。

步骤 6 在 **默认工作流程** 部分，配置默认工作流程；请参阅 默认工作流程，第 197 页。

步骤 7 点击**保存 (Save)**。

事件视图首选项

使用“事件视图设置”(Event View Settings) 页面的“事件首选项”(Event Preferences) 部分可在 Firepower 系统中配置事件视图的基本特征。尽管此区域对无法查看事件的用户不重要，但所有用户角色均可使用。

以下字段显示在“事件首选项”(Event Preferences) 部分：

- **确认“所有”操作**字段控制设备是否强制确认影响事件视图中所有事件的操作。

  例如，如果已启用此设置且点击事件查看上的**Delete All**，必须确认要删除的所有事件满足当前的限制条件（包括在当前页面未显示的活动），然后才可将其从数据库中删除。

- **解析 IP 地址**字段允许设备在事件视图中显示主机名（若可能）而非 IP 地址。

  请注意，如果事件查看包含大量 IP 地址，并且已启用该选项，则该视图可能缓慢显示。另请注意，为使此设置生效，必须使用管理接口配置在系统设置中建立 DNS 服务器。

- **Expand Packet View** 字段可供您配置入侵事件数据包视图的显示方式。默认情况下，设备以折叠方式显示数据包视图：
  - **None** - 折叠数据包视图的 Packet Information 部分的所有子部分
  - **Packet Text** - 仅展开 Packet Text 子部分
  - **Packet Bytes** - 仅展开 Packet Bytes 子部分
  - **All** - 展开所有部分

无论默认设置如何，您始终可以手动展开数据包视图中的部分查看有关已捕获数据包的详细信息。

- **每页行数 (Rows Per Page)** 字段控制要在向下页面和表视图中显示的每页事件行数。
- **刷新时间间隔 (Refresh Interval)** 字段设置事件查看的刷新时间间隔（以分钟为单位）。输入 0 可禁用刷新选项。请注意，此时间间隔不适用于控制面板。
- **统计信息刷新时间间隔 (Statistics Refresh Interval)** 控制事件摘要页面（例如，“入侵事件统计信息”[Intrusion Event Statistics] 和“发现统计信息”[Discovery Statistics] 页面）的刷新时间间隔。输入 0 可禁用刷新选项。请注意，此时间间隔不适用于控制面板。
- **Deactivate Rules** 字段控制哪些链接显示在标准文本规则生成的入侵事件的数据包视图上：
  - **All Policies** - 用于取消激活所有本地定义的自定义入侵规则中的标准文本规则的一个链接。
  - **当前策略 (Current Policy)** - 用于仅停用当前部署的入侵规则中的标准文本规则的一个链接。请注意，您不能停用默认策略中的规则。
  - **Ask** - 每一这些选项的链接

要在数据包视图上看到这些链接，您的用户帐户必须具有管理员或入侵管理员权限。

文件下载首选项

使用“事件视图设置”(Event View Settings) 页面的“文件首选项”(File Preferences) 部分配置本地文件下载的基本特征。此部分仅适用于具有管理员、安全分析师或安全分析师（只读）用户角色的用户。

请注意，如果设备不支持下载捕获的文件，则这些选项会被禁用。

以下字段显示在“文件首选项”(File Preferences) 部分：

- **确认“下载文件”操作 (Confirm ‘Download File’ Actions)** 复选框控制“文件下载”(File Download) 弹出窗口是否每次都显示下载文件，同时显示警告并提示继续或取消。

注意 思科强烈建议**不要**下载恶意软件，因为其可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。

请注意，在下载文件时，可随时禁用此选项。

- 当下载捕获的文件时，系统会创建一个包含该文件的有密码保护的 .zip 归档文件。**Zip 文件密码 (Zip File Password)** 字段定义要用于限制 .zip 文件的访问权限的密码。如果将此字段留空，系统会创建不需要密码的归档文件。
- **显示 Zip 文件密码 (Show Zip File Password)** 复选框会切换显示 **Zip 文件密码 (Zip File Password)** 字段中的纯文本或模糊字符。当清除此字段时，**Zip 文件密码 (Zip File Password)** 显示模糊字符。

默认时间窗口

时间段，有时称为时间范围，会对任何事件查看中的事件施加时间限制。使用“事件视图设置”页面的“默认时间段”区域控制时间段的默认行为。

此区域的用户角色访问权限列出如下：

- 管理员和维护人员可以访问完整的区域。
- 安全分析师和安全分析师（只读）可访问除**审核日志时间段**之外的所有选项。
- 访问管理员、发现管理员、外部数据库用户、入侵管理员、网络管理员和安全审批人只能访问**事件时间段**选项。

请注意，无论默认时间段设置如何，在事件分析期间，可以始终手动更改单个事件查看的时间段。另请注意，时间段设置仅对当前会话有效。在注销后重新登录时，时间段会重置为在此页面中配置的默认设置。

可为以下三种类型的事件设置默认时间段：

- **事件时间段**可为按时间限制的多数事件设置单个默认时间段。
- **审核日志时间段**可为审核日志设置默认时间段。

- **运行状况监控时间段**可为运行状况事件设置默认时间段。

仅可以为用户帐户可访问的事件类型设置时间段。所有用户类型都可设置事件时间段。管理员、维护人员和安全分析师可以设置运行状况监控时间段。管理员和维护人员可以设置审核日志时间段。

请注意，因为不是所有的事件查看都可以受时间限制，所以时间段设置对显示主机、主机属性、应用程序、客户端、漏洞、用户身份或合规 allow 名单违规的事件查看没有影响。

可以使用**多个**时间段，每种事件类型一个，也可以使用适用于所有事件的**一个**时间段。如果使用一个时间段，则不会显示三种时间段类型的设置，会显示新的**全局时间段**设置。

有以下三种类型的时间段：

- 静态，显示从特定开始时间到特定结束时间生成的所有事件。
- 扩展，显示从特定开始时间到目前生成的所有事件；随着时间的推进，时间段会进行扩展，并会有新事件添加到事件视图中。
- 滑动，显示从某个特定开始时间（例如，一天前）到当前时间生成的所有事件；随着时间向前推进，时间段会“滑动”，以便只可以查看所配置范围内的事件（在本示例中，为最后一天）

所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。

以下选项显示在**时间段设置**下拉列表：

- **显示最后时间 - 滑动式**选项允许配置指定长度的默认滑动时间窗。

  设备显示在某个特定开始时间（例如，1 小时前）和当前时间期间生成的所有事件。更改事件视图时，时间窗口会“滑动”，以便始终显示最后一小时的事件。

- 通过**显示最后时间 - 静态/扩展式**选项，可以配置指定长度的静态或扩展默认时间窗口。

  对于**静态**时间段，启用**使用结束时间**复选框。设备会显示在某个特定开始时间（例如，1 小时前）和第一次查看事件时的时间期间生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。

  对于**扩展**时间段，禁用**使用结束时间**复选框。设备显示在某个特定开始时间（例如，1 小时前）和当前时间期间生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。

- **当日 - 静态/扩展式**选项允许为当日配置静态或扩展默认时间段。当日从午夜开始，基于当前会话的时区设置。

  对于**静态**时间段，启用**使用结束时间**复选框。设备会显示从午夜到第一次查看事件时的时间期间生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。

  对于**扩展**时间段，禁用**使用结束时间**复选框。设备会显示在午夜到当前时间期间生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。请注意，如果在您注销之前，分析持续 24 小时以上，则此时间窗口可以超过 24 小时。

- **当周 - 静态/扩展式**选项允许为当周配置静态或扩展默认时间段。当周从上一周日的午夜开始，基于当前会话的时区设置。

对于**静态**时间段，启用**使用结束时间**复选框。设备会显示从午夜到第一次查看事件时的时间期间生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。

对于**扩展**时间段，禁用**使用结束时间**复选框。设备会显示在周日午夜到当前时间期间生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。请注意，如果在您注销之前，分析持续 1 周以上，则此时间窗口可以超过 1 周。

默认工作流程

工作流程是一组页面，显示分析师评估事件所使用的数据。对于每个事件类型，设备附带了至少一个预定义工作流程。例如，作为安全分析师，根据执行分析的类型，可以在十种入侵事件工作流程中选择，每种类型都会以不同的方式显示入侵事件数据。

设备会使用每种事件类型的默认工作流程进行配置。例如，按优先级和分类事件的工作流程是入侵事件的默认值。这意味着，只要查看入侵事件（包括已审阅的入侵事件），设备都会显示按优先级和分类事件的工作流程。

但是，您可以更改每种事件类型的默认工作流程。可配置的默认工作流程取决于用户角色。例如，入侵事件分析师无法设置默认发现事件工作流程。

设置默认时区

此设置仅确定您的用户账号在 Web 界面中显示的时间，例如任务计划和查看控制面板。此设置不会更改系统时间或影响任何其他用户，也不会影响系统中存储的数据（通常使用 UTC）。

警告 时区功能（在“用户首选项”中）假设系统时钟设置为UTC时间。请勿尝试更改系统时间。不支持从 UTC 更改系统，而执行此操作将需要您重新映像设备以从不支持的状态中恢复。

注释 此功能不影响用于基于时间的策略应用的时区。在 **设备 > 平台设置**中设置设备的时区。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 点击 **时区** 下拉列表。

步骤 3 选择包含要使用时区的大洲或区域。

步骤 4 选择与要使用的时区对应的国家/地区和省/自治区名称。

指定默认控制面板

当选择**概述** > **控制面板**时，系统将会显示默认控制面板。除非更改，否则所有用户的默认控制面板都是“摘要”(Summary) 控制面板。如果您的用户角色是管理员、维护人员或安全分析师，则可以更改默认控制面板。

在多域部署中，选择的默认控制面板适用于用户帐户具有访问权限的所有域。当选择频繁访问多个域的帐户的控制面板时，请记住，某些控制面板构件会受域限制。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 点击 **控制面板设置**。

步骤 3 从下拉列表中选择要用作默认的控制面板。

步骤 4 点击**保存 (Save)**。

配置操作方法设置

“操作方法”是一个构件，它提供导航管理中心上任务的逐步指导。逐步指导将引导您完成每个步骤，依次熟悉可能必须导航的各类陌生UI界面，引导您完成实现任务所需执行的步骤，最终完成任务。**操作方法**构件默认为启用。

有关 管理中心 中支持的功能逐步指导的列表，请参阅Cisco Secure Firewall Management Center 支持的功能逐步指导。

注释

- 通常情况下，逐步指导对所有 UI 页面可用，并且不区分用户角色。但是，根据用户权限的不同，某些菜单项将不会显示在 管理中心 界面上。因此，逐步指导将不会在此类页面上执行。
- 此功能在经典主题中不可用。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 **How-To 设置**。

步骤 3 选中 **启用 How-To** 复选框以启用 How-To。

步骤 4 点击**保存**。

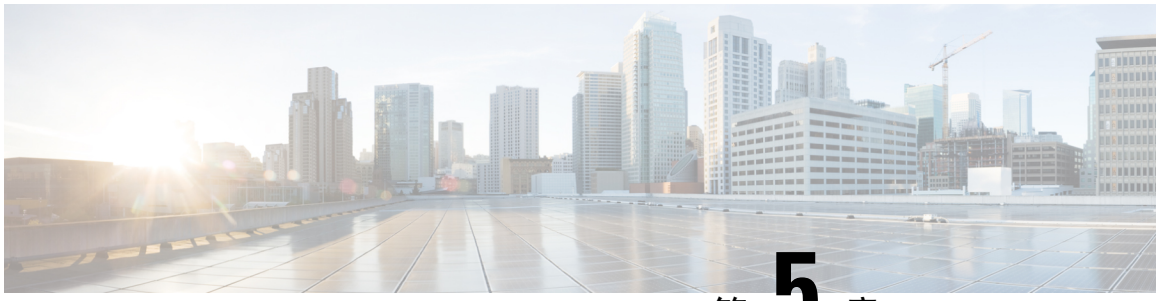
下一步做什么

要打开“操作方法”构件，请选择**帮助 (Help)** > **操作方法 (How-Tos)**。您可以搜索解决相关任务的操作方法逐步指导。有关详细信息，请参阅 搜索如何逐步指导，第 20 页。

的用户帐户历史记录

功能	最低 管理中心	最低 威胁防御	详情
用于修改访问控制策略和规则的精细权限。	7.4	任意	您可以定义自定义用户角色，以区分访问控制策略和规则中的入侵配置以及访问控制策略和规则的其余部分。使用这些权限，您可以分离网络管理团队和入侵管理团队的职责。 定义用户角色时，可以选择 **策略** > **访问控制** > **访问控制策略** > **修改访问控制策略** > **修改威胁配置** 选项，以允许在规则中选择入侵策略、变量集和文件策略，以及配置网络分析的高级选项和入侵策略、访问控制策略的安全情报策略配置以及策略默认操作中的入侵操作。您可以使用 **修改其余访问控制策略配置** 来控制编辑策略的所有其他方面的能力。包含“修改访问控制策略”权限的现有预定义用户角色继续支持所有子权限；如果要应用精细权限，则需要创建自己的自定义角色。
添加了用于分配外壳用户名模板的新字段。	7.0	任意	调配以指定用于 LDAP 外部身份验证的 CLI 访问属性模板 - 引入了 **外壳用户名模板** 。因此，CLI 属性将有自己的模板来标识 LDAP CLI 用户。 新增/修改的屏幕： **系统**（⚙）> **用户** > **外部身份验证**
添加了对使用任何符合 SAML 2.0 的 SSO 提供程序的单点登录的支持。	6.7	任意	增加了对任何第三方 SAML 2.0 兼容身份供应程序 (IdP) 上配置的外部用户的单点登录支持。这包括将用户或组角色从 IdP 映射到管理中心用户角色的能力。 只有通过内部或通过 LDAP 或 RADIUS 进行身份验证的具有管理员角色的用户才能配置 SSO。 新增/修改的屏幕： **系统**（⚙）> **用户** > **单点登录**
Web 界面的主题。	6.6	任意	您可以选择 Web 界面的外观。 选择“浅色”(Light) 或“黄昏”(Dusk) 主题，或使用以前版本中出现的经典主题。 新增/修改的屏幕： 用户名 (User Name) > **用户首选项 (User Preferences)** > **常规 (General)** > **UI 主题 (UI Theme)** 支持的平台： 管理中心

功能	最低 管理中心	最低 威胁防御	详情
为用户帐户中的名称添加了一个新字段。	6.6	任意	添加了可标识负责内部用户帐户的用户或部门的字段。 新增/修改的屏幕： **系统**（⚙）> **用户** > **用户**> **实际名称 (Real Name)** 字段
不再支持思科安全管理器单点登录。	6.5	任意	从 Firepower 6.5 开始，不再支持 管理中心 和思科安全管理器之间的单点登录。 新增/修改的屏幕： **系统**（⚙）> **用户 (Users)**> **CSM 单点登录 (CSM Single Sign-on)**
增强密码安全性。	6.5	任意	对强密码的新要求现在显示在本章中的某处，并从其他章节交叉引用。 更改密码界面中添加了新字段：**显示密码 (Show Password)** 和**生成密码 (Generate Password)**。 新增/修改的屏幕： 用户名 (User Name) > **用户首选项 (User Preferences)** > **常规 (General)** > **更改密码 (Change Password)**



第 5 章

域

以下主题介绍如何使用域管理多租户：

使用域的多租户简介

管理中心 允许您使用域实施多租户。域对受管设备、配置和事件的用户访问进行分段。您在一个顶级全球域下最多可以创建 100 个子域，分为两个或三个级别。

当您登录到 管理中心时，将会登录到单个域，称为当前域。根据您的用户帐户，您或许可以切换到其他域。

除了您的用户角色所施加的任何限制之外，您当前的域级别可能也会限制您修改各样配置的能力。管理中心 会将大多数管理任务（例如系统软件更新）限制于全局域。

管理中心会限制对枝叶域（不含子域的域）的其他任务。例如，您必须将每个受管设备与一个枝叶域相关联，并从该枝叶域的情景执行设备管理任务。请注意，每台设备只能属于一个域。

根据每个枝叶域的设备收集的发现数据，该枝叶域可构建自己的网络映射。受管设备报告的事件（连接、入侵、恶意软件等）还会与设备的枝叶域相关联。

一个域级别：全局

如果不配置多租户，则所有设备、配置和事件属于全局域，其在此情景下也是一个枝叶域。除了域管理之外，系统会隐藏特定域配置和分析选项，直到您添加子域。

两个域级别：全局和第二级

在两个级别的多域部署中，全局域只有直接的后代域。例如，托管安全运营商 (MSSP) 可以使用单一 管理中心来管理多个客户的网络安全：

- MSSP 的管理员可以登录全局域，无法查看或编辑客户的部署。他们必须登录到相应的二级命名子域，才能管理客户的部署。
- 每个客户的管理员都可以登录第二级已命名子域，以便只管理适用于其组织的设备、配置和事件。这些本地管理员无法查看或影响 MSSP 的其他客户的部署。

三个域级别：全局、第二级和第三级

在三个级别的多域部署中，全局域拥有多个子域，且至少其中一个子域又拥有其自己的子域。要扩展上述示例，请考虑这样一个场景，其中一位 MSSP 客户（已经限制在一个子域中）希望进一步对其部署进行分段。此客户希望单独管理两类设备：位于网络边缘的设备，以及位于内部的设备：

- 登录到二级子域的客户的管理员无法查看或编辑客户的边缘网络部署。他们必须登录到相应的枝叶域，才能管理部署在网络边缘的设备。
- 客户边缘网络的管理员可以登录第三级（枝叶）域，以便只管理部署在网络边缘的设备，以及适用的配置和事件。同样，客户内部网络的管理员可以登录第三级域来管理内部设备、配置和事件。边缘和内部管理员无法查看彼此的部署。

注释 在使用多租户的 管理中心 中，SSO 配置只能在全局域级别应用，并且适用于全局域和所有子域。

相关主题

配置 SAML 单点登录 ，第 136 页

域术语

本文档在介绍域和多域部署时使用以下术语：

全局域

在多域部署中，是指顶级域。如果不配置多租户，则所有设备、配置和事件都属于全局域。全局域中的管理员可以管理整个 Firepower 系统部署。

子域

第二或第三级域。

第二级域

全局域的子级。第二级域可以是枝叶域，也可以具有子域。

第三级域

第二级域的子级。第三级域始终是枝叶域。

枝叶域

没有子域的域。每台设备都必须属于枝叶域。

后代域

从层次结构中的当前域下传的域。

子域

域的直接后代。

祖先域

当前域从其下传的域。

父域

域的直接祖先。

同级域

具有相同父级的域。

当前域

您现在登录的域。在 Web 界面的右上角，系统在您的用户名之前显示当前域的名称。除非您的用户角色受限，否则可以编辑当前域中的配置。

域属性

要修改域的属性，您必须在该域的父域中具有管理员访问权限。

名称和描述

每个域在层次结构中必须拥有唯一的名称。说明是可选的。

父域

第二和第三级域有父域。在创建域后，无法更改该域的父级。

设备

仅枝叶域可包含设备。换句话说，域可以包含子域或设备，但不能同时包含两者。不能保存由非枝叶域直接控制设备的部署。

在域编辑器中，Web 界面根据可用和所选设备在域层次结构中的当前位置来显示它们。

主机限制

管理中心 可以监控并因而存储在网络映射中的主机数，具体取决于其型号。在多域部署中，枝叶域共享受监控主机的可用池，但拥有单独的网络映射。

要确保每个枝叶域都可以填充其网络映射，可以在每个子域级别设置主机限制。如果将域的主机限制设置为 0，则域在通用池中共享。

设置主机限制对每个域级别有着不同的影响：

- 枝叶 - 对于枝叶域，主机限制仅是对枝叶域可以监控的主机数量进行简单限制。

- 第二级 - 对于用于管理第三级枝叶域的第二级域，主机限制表示枝叶域可以监控的主机总数。枝叶域共享可用主机池。
- 全局 - 对于全局域，主机限制等于 管理中心 可以监控的主机总数。您无法进行更改

子域的主机限制总和加起来可超过其父域的主机限制。例如，如果全局域主机限制为 150,000，则可以配置多个子域，每个子域的主机限制为 100,000。这些域中的任一个（但并非总共）可监控 100,000 台主机。

网络发现策略控制在您达到主机限制后检测到新主机时发生的情况；您可以丢弃新主机或替代非活动时间最长的主机。由于每个枝叶域具有各自的网络发现策略，因此在系统发现新主机时，每个枝叶域会监管各自的行为。

如果您降低某个域的主机限制，且其网络映射包含比新限制更多的主机，则系统会删除处于非活动状态时间最长的主机。

相关主题

主机限制
网络发现数据存储设置

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

管理域

要修改域的属性，您必须在该域的父域中具有管理员访问权限。

过程

步骤 1 选择**系统**（⚙）> **域**。

步骤 2 管理域：

- 添加 - 点击**添加域 (Add Domain)**，或者点击父域旁边的**添加子域 (Add Subdomain)**；请参阅创建新域，第 205 页。

- 编辑 - 点击要修改的域旁边的**编辑**（ ），请参阅域属性，第 203 页。
- 删除 - 点击要删除的空白域旁边的**删除**（ ），然后确认您的选择。通过编辑设备的目标域移动要删除的域中的设备。

步骤 3 当您完成对域结构以及与枝叶域相关的所有设备的更改时，请点击**保存 (Save)** 以实施更改。

步骤 4 如有提示，请进行其他更改：

- 如果将枝叶域更改为父域，请移动或删除旧网络映射；请参阅在域之间移动数据，第 206 页。
- 如果在域之间移动设备，并且必须分配新的策略和安全区域或接口组，请参阅在域之间移动设备，第 206 页。

下一步做什么

- 为任何新域配置用户角色和策略（访问控制、网络发现等等）。根据需要更新设备属性。
- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

创建新域

您在一个顶级全球域下最多可以创建 100 个子域，分为两个或三个级别。

实施域配置之前，必须将所有设备分配到枝叶域。将某个子域到枝叶域时，该域不再是枝叶域，您必须重新分配其设备。

过程

步骤 1 在全局或第二级域中，选择**系统**（ ）> **域**。

步骤 2 点击**添加域 (Add Domain)**，或者点击父域旁边的**添加子域 (Add Subdomain)**。

步骤 3 输入**名称**和**说明**。

步骤 4 在**父域 (Parent Domain)** 中选择父域。

步骤 5 在**设备 (Devices)** 上，选择**可用设备 (Available Devices)** 以添加域，然后点击**添加到域 (Add to Domain)** 或拖放到**所选设备 (Selected Devices)** 列表中。

步骤 6 或者，点击**高级 (Advanced)** 以限制新域可以监控的主机数；请参阅域属性，第 203 页。

步骤 7 点击**保存 (Save)** 返回域管理页面。

如果任何设备被分配到非枝叶域，则系统会向您发出警告。点击**创建新域 (Create New Domain)**，为这些设备创建新域。如果计划将设备移至现有域，请点击**保持未分配 (Keep Unassigned)**。

步骤 8 当您完成对域结构以及与枝叶域相关的所有设备的更改时，请点击**保存 (Save)** 以实施更改。

步骤 9 如有提示，请进行其他更改：

- 如果将枝叶域更改为父域，请移动或删除旧网络映射；请参阅在域之间移动数据，第 206 页。

- 如果在域之间移动设备，并且必须分配新的策略和安全区域或接口组，请参阅在域之间移动设备，第 206 页。

下一步做什么

- 为任何新域配置用户角色和策略（访问控制、网络发现等等）。根据需要更新设备属性。
- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

在域之间移动数据

由于事件和网络映射与枝叶域关联，因此当您将枝叶域更改为父域时，您有两种选择：

- 将网络映射和关联事件移动到新枝叶域。
- 删除网络映射但保留事件。在这种情况下，事件仍与父域关联，直到系统根据需要或根据配置删除事件。或者，您可以手动删除旧事件。

开始之前

实施一种域配置（其中之前的枝叶域现在是父域）；请参阅管理域，第 204 页。

过程

步骤 1 对于现在为父域的每个前枝叶域：

- 选择新的**枝叶域 (Leaf Domain)** 以继承**父域 (Parent Domain)** 的事件和网络映射。
- 选择**无 (None)** 以删除父域的网络映射，但保留旧事件。

步骤 2 点击**保存 (Save)**。

下一步做什么

部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

在域之间移动设备

只要源域和目标域在移动设备的域中可见，您就可以在域之间移动设备。在域之间移动设备可能会影响应用于该设备的配置和策略。在域之间移动设备时，系统会保留以下设备配置。

- 接口
- 内联集

- 路由
- DHCP
- 关联对象
- SNMP（如果可用）

在域之间移动设备时，设备的配置可能会发生以下变化：

- 如果您希望系统在将设备移动到目标域后保留设备配置，请确保：
  - 共享访问控制策略位于全局域中。我们还建议将其他共享策略放在全局域中。
- 对于 VPN 配置，
  - 站点间 VPN 配置位于目标域中。
  - 远程访问 VPN 配置和设备证书位于全局或目标域中。
  - 如果您为某一设备分配远程访问 VPN 策略，则仅当目标域是在其中配置远程访问 VPN 的域的后代时，才可以将该设备从一个域移至另一个域。
- SNMP 的网络对象位于全局域中。
- 您可以将该设备移入任何子域，而无需删除在该设备上登记的证书。具体包括：
  - 如果应用于移动设备的运行状况策略在新域中不可访问，您可以选择新的运行状况策略。
  - 如果分配给移动设备的访问控制策略在新域中无效或不可访问，请选择新策略。每个设备都必须有一个分配的访问控制策略。
  - 如果移动设备上的接口属于在新域中不可访问的安全区域，您可以选择新区域。
  - 删除以下位置中的接口：
    - 在新域中不可访问且不在访问控制策略中使用的安全区域。
    - 所有接口组。

如果设备需要策略更新，但您不需要在区域间移动设备，则系统会显示一条消息，表明区域配置为最新配置。例如，如果设备的接口属于在公共祖先域中配置的安全区域，则您无需在将设备从一个子域移动到另一个子域时更新区域配置。

开始之前

- 创建新的域。有关详细信息，请参阅创建新域，第 205 页。
- 实施您将设备从一个域移动到另一个域的域配置，且现在必须分配新策略和安全区域；请参阅管理域，第 204 页。

过程

步骤 1 在全局域中，选择**系统 (System)** (⚙) > **域 (Domains)**。

步骤 2 编辑您计划将设备移动到的目标域。

步骤 3 在**编辑域 (Edit Domain)** 对话框中，执行以下操作之一：

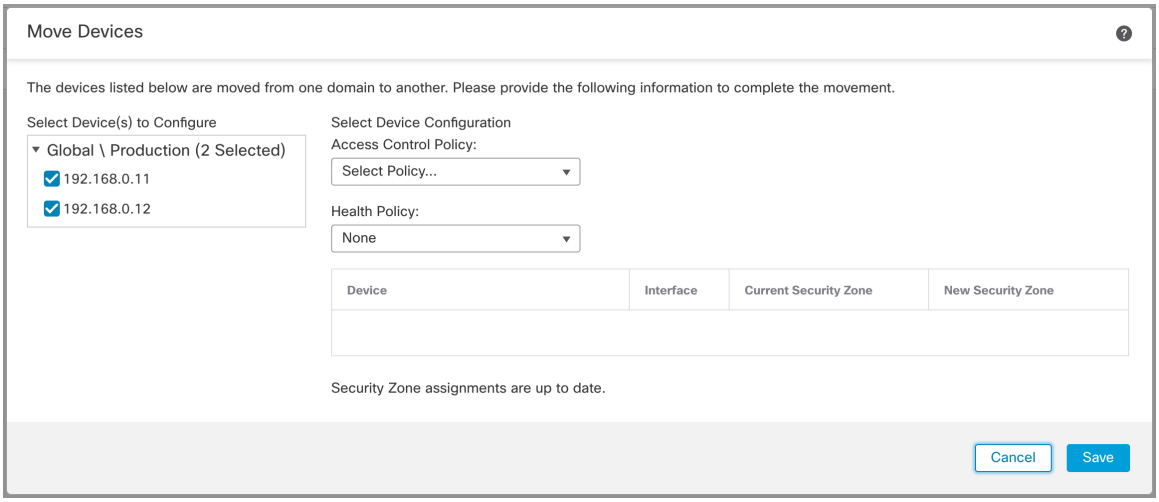
1. 选择要移动的设备，然后点击**添加到域 (Add to Domain)**。
2. 点击**保存 (Save)**。

步骤 4 在“域”(Domains) 页面上，点击**保存 (Save)**。

步骤 5 （**如果访问控制策略不在全局域中**）在**移动设备 (Move Devices)** 对话框中，执行以下操作：

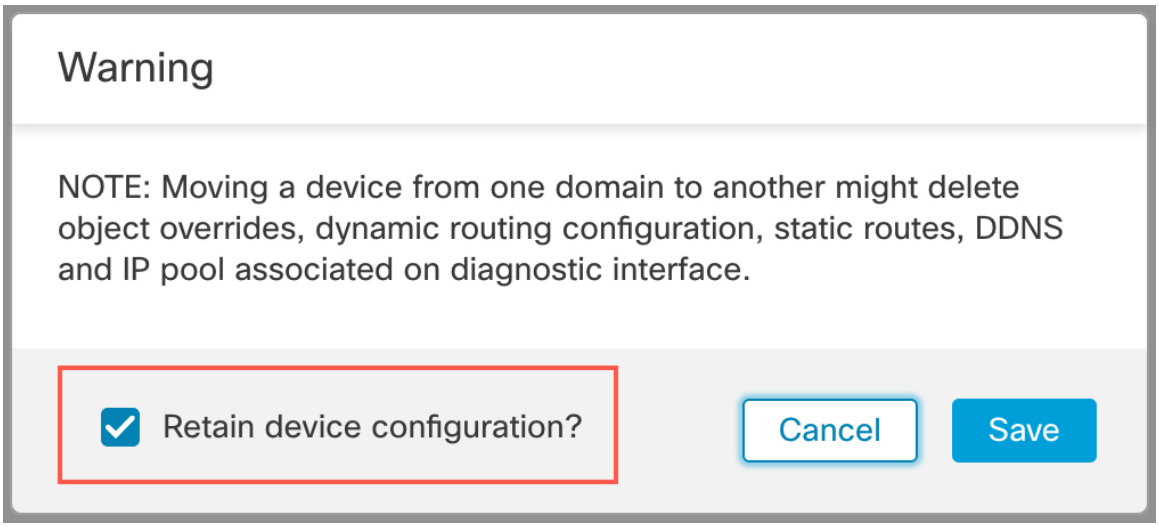
1. 在**选择要配置的设备 (Select Device(s) to Configure)** 下，选中要配置的设备。

   选中多个设备，以分配相同的运行状况和访问控制策略。



2. 在**访问控制策略 (Access Control Policy)** 中选择访问控制策略以应用于设备，或选择**新建策略 (New Policy)** 来创建新策略。
3. 在**运行状况策略 (Health Policy)** 中选择运行状况策略以应用于设备，或选择**无 (None)** 使该设备没有运行状况策略。
4. 如果系统提示将接口分配到新区域，请为列出的每个接口选择**新建安全区域 (New Security Zone)**，或选择**无 (None)** 以在稍后对其进行分配。
5. 配置完所有受影响设备后，点击**保存 (Save)**以保存策略和区域分配。

步骤 6 如果要在移动后保留设备配置，请选中**保留设备配置？(Retain device configuration?)** 复选框。



如果选择此选项，则系统会在设备被移至目标域后保留设备配置。如果不选择此选项，则您必须手动更新受移动影响的已移动设备上的设备配置。

下表显示了如何在各种场景中处理对象。

场景	系统操作
对象存在于目标域中。	重复使用对象。
目标域中存在具有相同名称和值的对象。	重复使用对象。
目标域中存在具有相同名称但值不相同的对象。	• 网络和端口 - 创建对象覆盖。 • 接口对象 - 如果类型不同，则创建新对象。 • 根据名称匹配重复使用所有其他对象类型。
对象不存在于目标域中。	创建新对象。

步骤 7 点击**保存 (Save)** 以实施域配置。

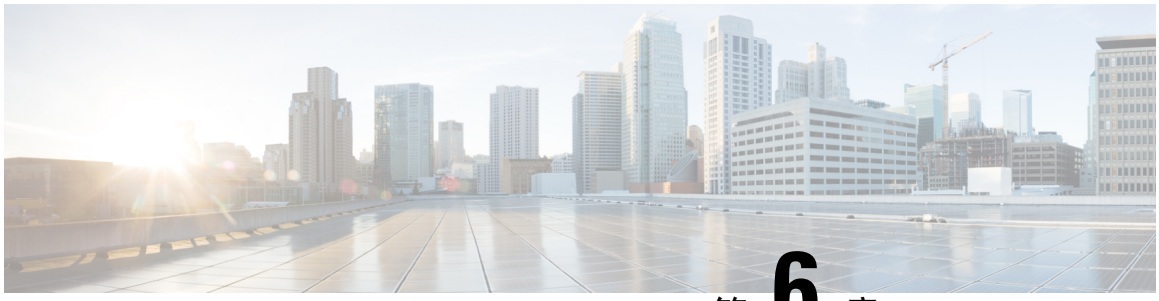
步骤 8 域配置完成后，点击**确定 (OK)**。

下一步做什么

- 在受移动影响的移动设备上更新其他配置。
- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。
- 如果在域之间移动设备后系统无法保留设备配置，则您可以手动恢复设备配置。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 中的 导出和导入设备配置 。

域管理历史记录

功能	最低 管理中心	最低 威胁防御	详情
保留与站点间 VPN 关联的设备配置	7.3	任意	将设备从一个域移动到另一个域时，只有在目标域中配置了站点间VPN时，才能保留与站点间 VPN 关联的设备配置。
保留设备配置	7.2	任意	现在，您可以在将设备从一个域移动到另一个域时保留设备配置。
增加了支持的域的最大数量	6.5	任意	您现在最多可以添加 100 个域。以前，最大值为 50 个域。 支持的平台： Cisco Secure Firewall Management Center



第 6 章

更新

本章介绍如何执行内容更新。

重要事项 要升级 管理中心 或 威胁防御 软件或机箱，请参阅管理中心当前正在运行的版本的升级指南：http://www.cisco.com/go/ftd-fmc-upgradehttp://www.cisco.com/go/ftd-fmc-upgrade-74。

要升级托管设备，请参阅云交付防火墙管理中心的 Cisco Secure Firewall Threat Defense 升级指南。

关于系统更新

使用 管理中心 为 自身及其 管理的设备升级系统软件。您还可以更新提供高级服务的各种数据库和源。

如果管理中心可以访问互联网，系统通常可以直接从思科获取更新。我们建议您尽可能安排或启用自动内容更新。某些更新在初始设置过程中或在您启用相关功能时自动启用。您必须自行安排其他更新。完成初始设置后，我们建议您查看所有自动更新，并在必要时进行调整。

表 *6:* 升级和更新

组件	说明	详细信息
系统软件	主要 软件版本包含新功能、新功能和增强功能。它们可能包括基础设施或架构更改。 维护 版本包含常规漏洞和安全相关修复。行为更改很少见，并且与这些修复相关。 补丁 是按需更新，仅限于具有紧急性的关键修复程序。 热补丁 可以解决特定的客户问题。	**直接下载：** 仅选择补丁和维护版本，通常在版本可用于手动下载后的一段时间。延迟的长度取决于版本类型、版本采用情况和其他因素。不支持按需升级和计划下载。 **注释** 在版本 7.4.1 中，我们开始支持按需直接下载所有版本（热补丁除外）。但是，不再支持按计划下载维护版本。 **计划安装：** 仅限修补程序和维护版本，作为计划任务。 **卸载：** 仅修补程序。 **恢复：** 仅限 威胁防御 主要版本和维护版本。 管理中心 或经典设备不支持恢复。 **重新映像：** 仅限主要版本和维护版本。 **请参阅：** 《适用于管理中心的 Cisco Secure Firewall Threat Defense 升级指南》
漏洞数据库 (VDB)	思科漏洞数据库 (VDB) 包含主机可能易受感染的已知漏洞，以及操作系统、客户端和应用指纹。系统借助 VDB 来确定某个特定主机是否会增加遭受危害的风险。	**直接下载：** 确认。 **计划：** 是，作为计划的任务。 **卸载：** 从 VDB 357 开始，您可以安装任何可追溯到 管理中心 的基准 VDB 的 VDB。 **请参阅：** 更新漏洞数据库 (VDB)，第 214 页
地理位置数据库 (GeoDB)	思科地理位置数据库 (GeoDB) 是一个与可路由的 IP 地址关联的地理数据数据库。	**直接下载：** 确认。 **计划：** 是，从其自己的更新页面 **卸载：** 否。 **请参阅：** 更新地理位置数据库 (GeoDB)，第 216 页
入侵规则 (SRU/LSP)	入侵规则更新提供全新和更新的入侵规则及预处理器规则、现有规则的修改状态和修改的默认入侵策略设置。 另外，规则更新还可能删除规则，提供新规则类别和默认变量，并修改默认变量值。	**直接下载：** 确认。 **计划：** 是，从其自己的更新页面。 **卸载：** 否。 **请参阅：** 更新入侵规则，第 218 页

组件	说明	详细信息
安全情报源	安全情报源是 IP 地址、域名和 URL 的集合，可用于快速过滤与条目匹配的流量。	**直接下载：** 确认。 **计划：** 是，来自对象管理器。 **卸载：** 否。 **请参阅：** 《Cisco Secure Firewall Management Center 设备配置指南》
新 URL 类别和信誉	URL过滤可以根据URL的一般分类（类别）和风险级别（信誉）控制对网站的访问。	**直接下载：** 确认。 **计划：** 是，当您配置集成/云服务时，或作为计划任务。 **卸载：** 否。 **请参阅：** 《Cisco Secure Firewall Management Center 设备配置指南》

系统更新的要求和前提条件

型号支持

任意

支持的域

全局 除非另有说明。

用户角色

管理员

系统更新的准则和限制

在更新之前

在更新部署的任何组件（包括入侵规则、VDB或GeoDB）之前，请阅读更新随附的版本说明或建议性文本。这些内容提供版本特定的关键信息，包括兼容性、前提条件、新功能、行为更改和警告。

计划的更新

系统以UTC时间安排任务（包括更新）。这意味着它们在本地发生的时间取决于日期和您的特定位置。此外，由于更新是以UTC为单位进行计划的，因此它们不会针对夏令时、夏令时或您在地点可能观察到的任何季节性调整进行调整。如果受影响，则根据当地时间，计划的更新会在夏天比冬季中的一个小时开始。

重要事项 我们 强烈 建议您查看计划任务，确保计划的更新在您预期的时间执行。

带宽准则

要升级系统软件或执行就绪性检查，升级包必须位于设备上。升级包大小不同。请确保您的带宽足以将大量数据传输到您管理的设备。请参阅将数据从Firepower管理中心下载到受管设备的准则（故障排除技术说明）。

更新漏洞数据库 (VDB)

思科漏洞数据库 (VDB) 包含主机可能易受感染的已知漏洞，以及操作系统、客户端和应用指纹。系统借助 VDB 来确定某个特定主机是否会增加遭受危害的风险。

思科定期发布 VDB 更新。在 管理中心上更新 VDB 及其关联映射所需的时间取决于网络映射中的主机数量。一般说来，将主机数除以 1000，即可估算出执行更新所需的大致时间（分钟）。

管理中心 上的初始设置会自动下载并安装思科提供的最新 VDB，作为一次性操作。它还会安排每周任务，以下载最新可用软件更新，其中包括最新 VDB。我们建议您查看此每周任务，并在必要时进行调整。或者，安排新的周期性任务，以便实际更新 VDB 和/或软件并部署配置。有关详细信息，请参阅漏洞数据库更新自动化，第 479 页。

对于 VDB 343+，所有应用检测器信息均可通过 Cisco Secure Firewall 应用检测器来获取。该站点包含一个可搜索的应用检测器数据库。版本说明提供了有关特定 VDB 版本的变更信息。

安排 VDB 更新

如果 管理中心可以访问互联网，我们建议您安排定期更新 GeoDB。请参阅漏洞数据库更新自动化，第 479 页。

手动更新 VDB

使用此程序手动更新 VDB。从 VDB 357 开始，您可以安装任何 VDB，直至 管理中心的基准 VDB。

注意 请勿执行与映射的漏洞相关的任务，直至更新完成。即使消息中心在几分钟内不显示进度或指示更新失败，也不要重启更新。相反，请联系思科 TAC。

在大多数情况下，VDB 更新后的第一次部署会重新启动 Snort 进程，从而中断流量检查。系统会在发生这种情况时向您发出警告 （更新的应用检测器和操作系统指纹需要重新启动；漏洞信息不需要）。在此中断期间，流量是被丢弃还是不经进一步检查直接通过，将取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

开始之前

如果 管理中心 无法访问 思科支持和下载站点，请从 获取更新： https://www.cisco.com/go/firepower-software。选择或搜索您的型号（或选择任何型号 - 对所有 管理中心型号使用相同的 VDB），然后浏览至 覆盖和内容更新 页面。

过程

步骤 1 转到规则更新页面。

- 版本 7.4.0：**系统**（⚙）> **更新** > **产品更新**
- 版本 7.4.1+：**系统**（⚙）> **内容更新 (Content Updates)** > **VDB 更新 (VDB Updates)**

步骤 2 选择您希望以什么方式将 VDB 上传到 管理中心。

- 直接下载：点击 **下载更新** 按钮。
- 手动上传：点击 **上传更新**，然后点击 **选择文件** 然后浏览至 VDB。选择文件后，点击 **上传**。

注释 在版本 7.4.0 中，点击**下载更新 (Download Updates)** 还会立即获取部署 的最新维护版本和最新关键修补程序。

步骤 3 安装 VDB。

a) 在要安装的漏洞和指纹数据库更新旁边，点击 **安装** 图标（适用于较新的 VDB）或 **回滚** 图标（适用于较旧的 VDB）。
b) 选择 管理中心。
c) 点击**安装**。

在消息中心监控更新进度。在更新完成后，系统将使用新的漏洞信息。但您必须先进行部署，已更新的应用检测器和操作系统指纹才会生效。

步骤 4 验证更新是否成功。

VDB 更新页面和 **帮助** （?）> **关于** 均显示当前版本。

下一步做什么

- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。
- 如果您基于漏洞、应用检测器或不再可用的指纹进行配置，请检查这些配置以确保按预期处理流量。另请记住，更新 VDB 的计划任务可以撤消回滚。要避免这种情况，请更改计划任务或删除任何较新的 VDB 软件包。

更新地理位置数据库 (GeoDB)

地理位置数据库(GeoDB)是可用于根据地理位置查看和过滤流量的数据库。我们会定期更新GeoDB，您必须定期更新 GeoDB 才能获得准确的地理位置信息。您查看 **帮助** （）> **关于** 上的当前版本。

系统随附一个将 IP 地址映射到国家/地区/大洲的 GeoDB 国家/地区代码数据包。我们还提供一个包含背景数据的 IP 数据包。该情景数据包括 其他位置详细信息，以及连接信息，例如 ISP、连接类型、代理类型、域名等。

- 在版本 7.4.0 – 7.4.1 中，当系统下载 GeoDB 更新（无论是按需下载还是按计划下载）时，它都会默认下载这两个数据包。如果背景数据对您不重要，您可以通过禁用和删除 IP 包来节省磁盘空间。
- 在版本 7.4.2+ 中，系统默认只下载国家/地区代码数据包，但如果上下文数据对您很重要且磁盘空间足够大，您也可以将其配置为下载两个数据包。

GeoDB 更新会覆盖之前的任何版本。 管理中心 会自动更新其托管设备，您不需要重新部署。更新 GeoDB 所需的时间取决于您的部署，但最多可能需要 45 分钟，具体取决于更新的大小 - 例如，如果您正在下载并处理一个完整的 IP 数据包。虽然 GeoDB 更新不会中断任何其他系统功能（包括正在进行的地理位置信息收集），但更新执行时的确会占用系统资源。

作为初始配置的一部分，系统会安排每周更新 GeoDB。我们建议您查看此任务，并在必要时进行更改，如 安排 GeoDB 更新 ， 第 216 页。

安排 GeoDB 更新

作为初始配置的一部分，系统会安排每周更新 GeoDB。我们建议您查看此任务，并在必要时进行更改，如此程序。

开始之前

确保 管理中心可以访问 思科支持和下载站点。

过程

步骤 1 转到 GeoDB 更新页面。

- 版本 7.4.0：**系统**（）> **更新** > **地理位置更新**
- 版本 7.4.1+：**系统**（）> **内容更新** > **地理位置更新**

步骤 2 在 **IP 包配置 (IP Package Configuration)**下，使用 **IP 包下载 (IP Package Download)** 选项来指定是要仅下载所需的国家/地区代码包，还是还需要 IP 包。

不使用 IP 软件包可节省磁盘空间，但也会消除 IP 地址的情景地理位置数据。如果更改此配置，请点击**保存 (Save)**。

步骤 3 在 **周期性地理位置更新**下，选择 **启用周期性每周更新...** 。

步骤 4 指定**更新开始时间**。

步骤 5 点击**保存 (Save)**。

手动更新 GeoDB

使用此程序执行按需 GeoDB 更新。

开始之前

如果 管理中心 无法访问 思科支持和下载站点，请从 获取更新： https://www.cisco.com/go/firepower-software。选择或搜索您的型号（或选择任何型号 - 对所有 管理中心型号使用相同的 GeoDB），然后浏览至 覆盖和内容更新 页面。 下载国家/地区代码包和，可选， IP 包。

过程

步骤 1 转到 GeoDB 更新页面。

- 版本 7.4.0：**系统**（⚙） > **更新** > **地理位置更新**
- 版本 7.4.1+：**系统**（⚙） > **内容更新** > **地理位置更新**

步骤 2 在 **一次性地理位置更新**下，选择要如何更新 GeoDB。

- 直接下载：选择 **下载并安装...** 。
- 手动上传：选择 **上传和安装...**， 然后点击 **选择文件** ，然后浏览到您之前下载的 国家代码 包。

步骤 3 在 **IP 包配置**下，使用 **IP 包下载** 选项指定是要仅使用国家/地区代码包，还是要使用 IP 包。

不使用 IP 软件包可节省磁盘空间，但也会消除 IP 地址的情景地理位置数据。请注意，即使您手动上传 GeoDB 数据包，如果您不需要 IP 数据包中的数据，也应禁用此选项。这是因为禁用该选项会删除任何现有/过时的 IP 软件包。

如果更改此配置，请点击**保存 (Save)**。

步骤 4 点击**导入 (Import)**。

在消息中心监控更新进度。

步骤 5 验证更新是否成功。

GeoDB 更新页面和 **帮助** （?） > **关于** 均显示当前版本。

步骤 6 （可选）如果要手动上传更新，请对 IP 软件包重复此程序。

更新入侵规则

随着新的漏洞被发现， Talos 情报小组 会发布入侵规则更新。这些更新会影响入侵规则、预处理器规则和使用这些规则的策略。入侵规则更新是累加性的，并且思科建议始终导入最新的更新。不能导入与当前安装的规则的版本匹配或早于该版本的入侵规则更新。

入侵规则更新可能提供以下内容：

- **新的和修改的规则和规则状态** - 规则更新提供新的和更新的入侵和预处理器规则。对于新的规则，每个系统提供的入侵规则中的规则状态可能不同。例如，一个新规则在 Security over Connectivity 入侵策略中可能是启用状态，在 Connectivity over Security 入侵策略中则可能是禁用状态。规则更新也可以更改现有规则的默认状态，或者完全删除现有规则。
- **新规则类别** - 规则更新可能包括始终添加的新规则类别。
- **修改的预处理器和高级设置** - 规则更新可能更改系统提供的入侵策略中的高级设置，以及系统提供的网络分析策略中的预处理器设置。它们也可以更新访问控制策略中的高级预处理和性能选项的默认值。
- **新的和修改的变量** - 规则更新可能修改现有默认变量的默认值，但不会覆盖您的更改。始终会添加新变量。

在多域部署中，可以在任何域中导入本地入侵规则，但是，只能在全局域中从 Talos 导入入侵规则更新。

了解入侵规则更新何时修改策略

入侵规则更新可以影响系统提供的和自定义网络分析策略，以及所有访问控制策略：

- **系统提供** - 对系统提供的网络分析和入侵策略的更改以及对高级访问控制设置的任何更改将在您更新后重新部署策略时自动生效。
- **自定义** - 因为每个自定义网络分析和入侵策略都使用系统提供的策略作为其基础，或作为策略链中的事件基础，所以规则更新可以影响自定义网络分析和入侵策略。但是，您可以阻止规则更新自动执行这些更改。这使您能够在独立于规则更新导入的计划中手动更新系统提供的基本策略。无论您的选择（在每个自定义策略基础上实施）如何，更新系统提供的策略**都不会**覆盖您定制的任何设置。

请注意，导入规则更新会丢弃对网络分析和入侵策略所做的所有已缓存更改。为了方便起见，Rule Updates 页面列出了包含已缓存更改的策略以及做出这些更改的用户。

部署入侵规则更新

为使入侵规则更新所做的更改生效，必须重新部署配置。在导入规则更新时，可以将系统配置为自动重新部署到受影响设备。如果允许入侵规则更新修改系统提供的基本入侵策略，则此方法尤其有用。

注意 虽然在部署时规则更新本身不会重新启动 Snort 进程，但您所做的其他更改可能会重新启动。重启 Snort 会短暂中断所有设备上的流量和检查，包括为高可用性/可扩展性配置的检查。在中断期间，接口配置会确定是丢弃流量还是在不检查的情况下允许流量通过。在不重启 Snort 进行部署时，资源需求可能会导致少量数据包未经检测而被丢弃。

周期性入侵规则更新

可以在 Rule Updates 页面上设置为按日、周或月导入规则更新。

如果部署包括管理中心的高可用性对，则仅在主防御中心上导入更新。辅助管理中心会在常规同步过程中接收规则更新。

入侵规则更新导入中的适用子任务按以下顺序出现：下载、安装、基本策略更新和策略部署。完成一个子任务后，才会开始下一个子任务。

在计划的时间，系统按照在先前步骤中所指定，安装规则更新并部署已更改的配置。在导入之前或导入过程中，可注销或使用 Web 界面执行其他任务。在导入过程中访问时，“规则更新日志”显示**红色状态**（⛔），此外，您还可以在“规则更新日志”详细视图中查看消息。根据规则更新大小和内容，可能几分钟之后才会显示状态消息。

作为初始配置的一部分，系统会安排每日入侵规则更新。我们建议您查看此任务，并在必要时进行更改，如计划入侵规则更新，第 219 页.

导入本地入侵规则

本地入侵规则是从本地计算机以采用 ASCII 或 UTF-8 编码的纯文本文件形式导入的自定义标准文本规则。可以使用 Snort 用户手册（可在 http://www.snort.org 上获取）中的说明创建本地规则。

在多域部署中，可以在任何域中导入本地入侵规则。可以查看在当前域和祖先域中导入的本地入侵规则。

计划入侵规则更新

作为初始配置的一部分，系统会安排每日入侵规则更新。我们建议您查看此任务，并在必要时进行更改，如此程序。

开始之前

- 确保更新入侵规则的流程符合您的安全策略。
- 请考虑更新因带宽约束和 Snort 重启而带给流量和检测的影响。我们建议在维护窗口执行更新。
- 确保 管理中心可以访问 思科支持和下载站点。

过程

步骤 1 转到规则更新页面。

- 版本 7.4.0：**系统**（⚙）> **更新** > **规则更新**
- 版本 7.4.1+：**系统**（⚙）> **内容更新 (Content Updates)** > **规则更新 (Rule Updates)**

步骤 2 在**重复规则更新导入 (Recurring Rule Update Imports)** 下，选中**启用重复规则更新导入 (Enable Recurring Rule Update Imports)**。

步骤 3 指定**导入频率 (Import Frequency)** 和开始时间。

步骤 4 （可选）选中**重新应用所有策略...(Reapply all policies...)** 以便在每次更新后部署。

步骤 5 点击**保存 (Save)**。

手动更新入侵规则

使用此程序执行按需入侵规则更新。

开始之前

- 确保更新入侵规则的流程符合您的安全策略。
- 请考虑更新因带宽约束和Snort重启而带给流量和检测的影响。我们建议在维护窗口执行更新。
- 如果 管理中心 无法访问 思科支持和下载站点，请从 获取更新： https://www.cisco.com/go/firepower-software。选择或搜索您的型号（或选择任何型号 - 对所有 管理中心型号使用相同的 SRU 或 LSP），然后浏览至 覆盖和内容更新 页面。

过程

步骤 1 转到规则更新页面。

- 版本 7.4.0：**系统**（⚙）> **更新** > **规则更新**
- 版本 7.4.1+：**系统**（⚙）> **内容更新 (Content Updates)** > **规则更新 (Rule Updates)**

步骤 2 在 **一次性规则更新/规则导入**下，选择要如何更新入侵规则。

- 直接下载：选择 **下载新规则更新...** 。
- 手动上传：选择 **规则更新或文本规则文件...**，然后点击 **选择文件** 并浏览到入侵规则更新。

步骤 3 （可选）选中 **重新应用所有策略...** 以在更新后部署。

步骤 4 点击**导入 (Import)**。

在消息中心监控更新进度。即使消息中心在几分钟内不显示进度或指示更新失败，也不要重启更新。相反，请联系思科 TAC。

步骤 5 验证更新是否成功。

规则更新页面和 **帮助** （） > **关于** 均显示当前版本。

下一步做什么

如果您未在更新过程中部署，请立即部署；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

导入本地入侵规则

使用以下程序导入本地入侵规则。导入的入侵规则以被禁用的状态显示在本地规则类别中。您可以在任何域中执行此任务。

开始之前

- 请确保您的本地规则文件遵循导入本地入侵规则最佳实践，第 222 页中所述的准则，
- 并确保导入本地入侵规则的过程符合您的安全策略。
- 请考虑导入因带宽约束和 Snort 重启而带给流量和检测的影响。我们建议将规则更新安排在维护窗口执行。

过程

步骤 1 转到规则更新页面。

- 版本 7.4.0：**系统**（） > **更新** > **规则更新**
- 版本 7.4.1+：**系统**（） > **内容更新 (Content Updates)** > **规则更新 (Rule Updates)**
- 任意版本：点击入侵规则编辑器页面 (**对象** > **入侵规则**) 上的**导入规则 (Import Rules)**。

步骤 2 （可选）删除现有的本地规则。

点击**删除所有本地规则**，然后确认是否想要将创建和导入的所有入侵规则移至删除的文件夹。

步骤 3 在 **一次性规则更新/规则导入**下，选择 **规则更新或文本规则文件以上传和安装**，然后点击 **选择文件** 并浏览到您的本地规则文件。

步骤 4 点击 **Import**。

您可以在消息中心监控导入进度。即使消息中心在几分钟内不显示进度或指示更新失败，也不要重启导入。相反，请联系思科 TAC。

下一步做什么

- 编辑入侵策略，并启用已导入的规则。
- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

导入本地入侵规则最佳实践

导入本地规则文件时，请遵循以下准则：

- 规则导入程序要求以 ASCII 或 UTF-8 编码的纯文本文件导入所有自定义规则。
- 文本文件名称可包含字母数字字符和空格，不可包含除下划线 (_)、句号 (.) 和破折号 (-) 以外的其他特殊字符。
- 系统会导入以一个井号 (#) 开头的本地规则，但它们被标记为已删除。
- 系统会导入以一个井号 (#) 开头的本地规则，但不会导入以两个井号 (##) 开头的本地规则。
- 规则不能包含任何转义字符。
- 在多域部署中，系统将为导入到“全局”域或在该域中创建的规则分配一个为 1 的 GID，并为所有其他域分配一个特定于域的 GID，数值介于 1000 与 2000 之间。
- 导入本地规则时，不必指定生成器 ID (GID)。如果指定了生成器 ID，则请仅为标准文本规则指定 GID 1。
- 首次导入规则时，请勿指定 Snort ID (SID) 或修订版本号。这可避免与其他规则的 SID 发生冲突，包括已删除的规则。系统会自动为规则分配下一个可用的自定义规则 SID（1000000 或更高） 以及版本号 1。

  如果必须导入带有 SID 的规则，则 SID 可以是 1,000,000 或以上的任何唯一数字。

  在多域部署中，如果多个管理员同时导入本地规则，则单个域中的 SID 可能不连续，因为系统已将该序列的中间编号分配给其他域。
- 导入之前已导入的本地规则的更新版本时，或者重新安装已删除的本地规则时，必须包含由系统分配的 SID 以及高于当前编号的修订版本号。您可以通过编辑规则确定当前或已删除规则的修订版本号。

注释 删除本地规则时，系统会自动增加修订版本号；这样方便恢复本地规则。所有已删除的本地规则从会从本地规则类别转移到已删除规则类别。

- 请在高可用性对中的主 管理中心 上导入本地规则，以避免 SID 编号问题。
- 如果规则包含以下任意一项，则导入失败：
  - 大于 2147483647 的 SID。
  - 长度超过 64 个字符的源或目的端口列表。

- 在多域部署中，在导入到“全局”域时，GID:SID 组合使用 GID 1 和一个已存在于其他域中的 SID；这表示该组合在版本 6.2.1 之前就已存在。可以使用 GID 1 和一个唯一的 SID 重新导入规则。

- 如果启用某个导入的本地规则，而该规则将弃用的 `threshold` 关键字与某个入侵策略中的入侵事件阈值功能结合起来使用，策略验证将会失败。
- 所有导入的本地规则都会自动保存在本地规则类别中。
- 系统始终将导入的本地规则设置为禁用状态。必须手动设置本地规则的状态后，才能将其用于入侵策略中。

查看入侵规则更新日志

系统会生成规则更新/导入日志，按时间戳、用户以及每次更新是成功还是失败列出。这些日志包含有关所有更新的规则和组件的详细导入信息；请参阅 入侵规则更新日志详情，第 223 页。使用此程序可查看规则导入日志。请注意，删除导入日志不会删除导入的对象。 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 转到规则更新页面。

- 版本 7.4.0：**系统**（⚙）> **更新** > **规则更新**
- 版本 7.4.1+：**系统**（⚙）> **内容更新 (Content Updates)** > **规则更新 (Rule Updates)**

步骤 2 点击 **Rule Update Log**。

步骤 3 （可选）点击日志文件旁边的 **视图**（👁），查看任何规则更新的详细信息。

入侵规则更新日志详情

提示 即使是通过在仅显示单个导入文件记录的“规则更新导入日志”(Rule Update Import Log) 详细视图中的工具栏上点击**搜索 (Search)** 发起搜索，也可以搜索整个规则更新导入日志数据库。确保将时间限制条件设置为包含所有搜索中要包含的对象。

表 7: 入侵规则更新日志详情

字段	说明
操作	指明对对象类型执行了以下其中一项操作： • new（对于规则而言，是指第一次把规则存储在此设备上） • changed（对于规则更新组成部分或规则而言，规则更新组成部分已被修改，或者规则的版本号更高且 GID 和 SID 相同） • collision（对于规则更新组成部分或规则而言，由于版本与设备上的现有组成部分或规则冲突，因此跳过导入） • deleted（对于规则而言，已从规则更新删除规则） • enabled（对于规则更新编辑而言，已在系统提供的默认策略中启用了预处理器、规则或其他功能） • disabled（对于规则而言，已在系统提供的默认策略中禁用规则） • drop（对于规则而言，已在系统提供的默认策略中将规则设置为“丢弃并生成事件”[Drop and Generate Events]） • error（对于规则更新或本地规则文件而言，导入失败） • apply（为导入启用了**在规则更新导入完成后重新应用所有策略 [Reapply all policies after the rule update import completes]** 选项）
默认操作	规则更新定义的默认操作。当导入对象类型是 rule 时，默认操作是 Pass、Alert 或 Drop。对于所有其他导入对象类型，没有默认操作。
详细信息	组成部分或规则独有的字符串。对于规则、GID、SID 以及已更改规则的上一个版本号，此字段显示为 previously (GID:SID:Rev)。对于未更改的规则，此字段为空白。
域	其入侵策略可使用更新规则的域。后代域中的入侵策略也可以使用该规则。此字段只存在于多域部署中。
GID	规则的生成器 ID。例如，1（标准文本规则、全局域或旧 GID）或 3（共享对象规则）。
名称	导入对象的名称（对于规则，对应的是规则“消息”[Message] 字段；对于规则更新，对应的是组成部分名称）。
策略	对于导入的规则，此字段显示所有。这表示规则导入成功，并可在所有相应的默认入侵策略中启用。对于其他导入对象类型，此字段为空白。
版本	规则的版本号。
规则更新	规则更新文件名。
SID	规则的 SID。

字段	说明
时间	导入开始的时间和日期。
类型	导入对象的类型，可以是以下类型之一： • `rule update component`（已导入的组成部分，例如规则包或策略包） • `规则` （对于规则而言，是指新的或更新后的规则） • `policy apply`（为导入启用了**在规则更新导入完成后重新应用所有策略**选项）
计数	每条记录的计数 (`1`)。当表受限时，“计数”(Count) 字段显示在表视图中，而且在默认情况下，“规则更新日志”(Rule Update Log) 详细视图受限于规则更新记录。此字段不可搜索。

维护气隙部署

如果 管理中心 未连接到互联网，则将不会自动进行必要更新。您必须手动获取并安装这些更新。

有关详情，请参阅：

- 软件升级指南： https://cisco.com/go/ftd-fmc-upgrade
- 手动更新 VDB， 第 214 页
- 手动更新入侵规则， 第 220 页
- 手动更新 GeoDB， 第 217 页

系统更新的历史记录

表 *8:* 版本 *7.4.1* 的功能

功能	最低 管理中心	最低 威胁防御	详细信息
威胁防御升级			

功能	最低 管理中心	最低 威胁防御	详细信息
包含在FXOS升级中的固件升级。	任意	任意	**机箱/FXOS 升级影响。固件升级会导致设备额外重启一次。** 对于 Firepower 4100/9300，FXOS 升级到 2.14.1 版现在包括固件升级。如果设备上的任何固件组件比 FXOS 软件包中的旧，则 FXOS 升级也会更新固件。如果固件已升级，设备会重新启动两次 - 一次是因为FXOS，另一次是因为固件。 与软件和操作系统升级一样，在固件升级期间不要进行或部署配置更改。即使系统显示为非活动状态，也不要在固件升级过程中手动重新启动或关闭。 请参阅： Cisco Firepower 4100/9300 FXOS 固件升级指南
多实例模式下 Cisco Secure Firewall 3100 的机箱升级。	7.4.1	7.4.1	对于多实例模式下的 Cisco Secure Firewall 3100，您可从容器实例（威胁防御升级）单独升级操作系统和固件（机箱升级）。 新增/修改的菜单项： • 升级机箱：**设备 (Devices)** > **机箱升级 (Chassis Upgrade)** • 升级威胁防御：**设备 (Devices)** > **威胁防御升级 (Threat Defense Upgrade)** 请参阅： 《适用于管理中心的 Cisco Secure Firewall Threat Defense 升级指南》
Management Center 升级			
在管理中心升级后自动生成配置更改报告。	任意	任意	您可以在主要升级和维护管理中心升级后自动生成配置更改报告。这样有助于您了解即将部署的更改。系统生成报告后，您可以从消息中心的“任务”(Tasks) 选项卡下载报告。 其他版本限制：仅支持从版本 7.4.1+ 升级的管理中心。不支持升级到版本 7.4.1 或更早版本。 新增/修改的屏幕：**系统**（⚙） > **配置 (Configuration)** > **升级配置 (Upgrade Configuration)** > **启用升级后报告 (Enable Post-Upgrade Report)**

表 *9:* 版本 *7.4.0* 的功能

功能	最低 管理中心	最低 威胁防御	详细信息
管理中心升级：弃用的功能			

功能	最低 管理中心	最低 威胁防御	详细信息
暂时弃用的功能。	7.4.0	因功能而异	BLAH BLAH BLAH • 改进了升级起始页面和软件包管理。 • 启用从威胁防御升级向导恢复。 • 通过威胁防御升级向导查看详细的升级状态。 • 建议的版本通知。 • 管理中心的新升级向导。 • 热补丁高可用性管理中心，无需暂停同步。 • 更新了直接下载软件升级的互联网接入要求。 升级影响。 • 计划任务仅下载补丁和 VDB 更新。 升级影响。

表 *10:* 版本 *7.3.0* 的功能

功能	最低 管理中心	最低 威胁防御	详细信息
威胁防御升级			
从思科选择并将升级包直接下载到管理中心。	7.3.0	任意	您现在可以选择要直接下载到管理中心的威胁防御升级包。使用 > **更新** > **产品更新**上的新的 **下载 更新** 子选项卡。 其他版本限制：在版本 7.2.6/7.4.1 中， 此功能被改进的软件包管理系统所取代。 请参阅： 通过管理中心FMC下载升级软件包
将升级包从威胁防御向导上传到管理中心。	7.3.0	任意	现在，您可以使用该向导上传威胁防御升级包或指定升级包位置。以前（根据版本），您使用了**系统**（⚙）> **更新 (Updates)** 或**系统**（⚙）> **产品升级 (Product Upgrades)**。 其他版本限制：在版本 7.2.6/7.4.1 中， 此功能被改进的软件包管理系统所取代。 请参阅： 威胁防御升级

功能	最低 管理中心	最低 威胁防御	详细信息
成功升级威胁防御后自动升级到 Snort 3 不再是可选操作。	7.3.0	任意	**升级影响**。 将威胁防御升级到版本 7.3+ 后，无法再禁用 **从 Snort 2 升级到 Snort 3** 选项。 在软件升级后，当您部署配置时，所有符合条件的设备将从 Snort 2 升级到 Snort 3。虽然您可以切换回单个设备，但 Snort 2 将在未来版本中被弃用，强烈建议您立即停止使用。 对于因使用自定义入侵或网络分析策略而不符合自动升级条件的设备，我们强烈建议您手动升级到 Snort 3 以提高检测和性能。有关迁移方面的帮助，请参阅适用于您的版本的 《Cisco Secure Firewall Management Center Snort 3 配置指南》 。

功能	最低 管理中心	最低 威胁防御	详细信息
Cisco Secure Firewall 3100的组合升级和安装包。	7.3.0	7.3.0	**重新映像影响**。 在版本 7.3 中，我们组合了 Cisco Secure Firewall 3100 的威胁防御安装和升级包，如下所示： • 版本 7.1 – 7.2 安装包：cisco-ftd-fp3k. *version*.SPA • 版本 7.1 – 7.2 升级包：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • 版本 7.3+ 组合软件包：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar 虽然您可以毫无问题地升级威胁防御，但不能直接从较早的威胁防御和ASA版本重新映像到威胁防御版本7.3+。这是由于新映像类型要求进行ROMMON更新。要从这些旧版本重新映像，您必须“通过”ASA9.19+，旧 ROMMON 支持此版本，但也会更新到新 ROMMON。没有单独的 ROMMON 更新程序。 要使用威胁防御版本 7.3+，您可以选择： • 从威胁防御版本 7.1 或 7.2 升级 - 使用正常升级过程。 请参阅相应的 升级指南。 • 从威胁防御版本 7.1 或 7.2 重新映像 - 首先重新映像到 ASA 9.19+，然后重新映像到威胁防御版本 7.3+。 请参阅 威胁防御→*ASA*：*Firepower 1000*、*2100*；*Cisco Secure Firewall 3100* ，然后选择 Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南中的 *ASA*→威胁防御：*Firepower 1000*、*2100* 设备模式；*Cisco Secure Firewall 3100* 。 • 从 ASA 9.17 或 9.18 重新映像 - 首先升级到 ASA 9.19+，然后重新映像到威胁防御版本 7.3+。 请参阅 Cisco Secure Firewall ASA 升级指南 ，然后选择 Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南中的 *ASA*→威胁防御：*Firepower 1000*、*2100* 设备模式；*Cisco Secure Firewall 3100*。 • 从威胁防御版本 7.3+ 重新映像 - 使用正常的重新映像过程。 请参阅 适用于具备 Firepower Threat Defense 的 Firepower 1000/2100 和 Cisco Secure Firewall 3100/4200 的思科 FXOS 故障排除指南中的使用新软件版本对系统进行重映像 。
内容更新			

功能	最低 管理中心	最低 威胁防御	详细信息
自动 VDB 下载。	7.3.0	任意	管理中心的初始设置安排了每周下载最新可用软件更新的任务，其中现在包括最新的漏洞数据库 (VDB)。我们建议您查看此每周任务，并在必要时进行调整。或者，安排新的周期性任务，以便实际更新 VDB 和/或软件并部署配置。 新增/修改的屏幕：默认情况下，系统创建的 **每周软件下载** 计划任务中的 **漏洞数据库** 复选框现在处于启用状态。
安装任何 VDB。	7.3.0	任意	从 VDB 357 开始，您现在可以安装任何 VDB，直至该管理中心的基准 VDB。 更新 VDB 后，部署配置更改。如果您基于漏洞、应用检测器或不再可用的指纹进行配置，请检查这些配置以确保按预期处理流量。另请记住，更新 VDB 的计划任务可以撤消回滚。要避免这种情况，请更改计划任务或删除任何较新的 VDB 软件包。 新增/修改的屏幕：在 **系统**（⚙）> **更新** > **产品更新** > **可用更新** 中，如果上传较旧的 VDB，系统将显示新的 **回滚** 图标，而不是 **安装** 图标。

表 *11:* 版本 *7.2.0* 的功能

功能	详细信息
威胁防御升级	

功能	详细信息
在设备之间复制升级包（“点对点同步”）。	您可以使用 威胁防御 CLI 在设备之间复制升级包，而不是从 管理中心 或内部 Web 服务器将升级包复制到每台设备（“点对点同步”）。这种安全可靠的资源共享通过管理网络进行，但不依赖于 管理中心。每个设备可容纳 5 个数据包并发传输。 此功能支持由同一版本 7.2.x-7.4.x 独立设备 管理中心 管理的版本 7.2.x-7.4.x 独立设备。不支持： • 容器实例。 • 设备高可用性对和集群。这些设备可以在正常同步流程中相互获取软件包。将升级包复制到一个组成员会自动将其同步到所有组成员。 • 由高可用性 管理中心管理的设备。 • 由 云交付的防火墙管理中心管理，但 在分析模式下添加到本地部署 管理中心 的设备。 • 不同域中的设备或由 NAT 网关分隔的设备。 • 从版本 7.1 或更早版本升级的设备，无论 管理中心 版本如何。 新增/修改的CLI 命令： **configure p2psync enable**、 **configure p2psync disable**、**show peers**、 **show peer details**、 **sync-from-peer**、 **show p2p-sync-status**
成功升级威胁防御后自动升级到 Snort 3。	当您使用版本 7.2+ 管理中心升级到威胁防御版本 7.2+ 时，您现在可以选择是否**将 Snort 2 升级到 Snort 3**。 在软件升级后，当您部署配置时，符合条件的设备将从 Snort 2 升级到 Snort 3。对于因使用自定义入侵或网络分析策略而不符合条件的设备，我们强烈建议您手动升级到 Snort 3 以提高检测和性能。如需帮助，请参阅您的版本的 《Cisco Secure Firewall Management Center Snort 3 配置指南》 。 版本限制：不支持升级到版本 7.0.x 或 7.1.x。
升级单节点集群。	现在，您可以使用设备升级页面（**设备** > **设备升级**）升级只有一个主用节点的集群。任何已停用的节点也会升级。以前，此类升级会失败。系统更新页面不支持此功能（**系统**（⚙）**更新**）。 在这种情况下，也不支持无中断升级。流量和检测的中断取决于单独的主用设备的接口配置，就像使用独立设备一样。 支持的平台：Firepower 4100/9300、Cisco Secure Firewall 3100

功能	详细信息
从 CLI 恢复威胁防御升级。	如果管理中心和设备之间的通信中断，您现在可以从设备 CLI 恢复威胁防御升级。请注意，在高可用性/可扩展性部署中，当所有设备同时恢复时，恢复更成功。使用 CLI 恢复时，打开所有设备的会话，验证每个设备是否可以恢复，然后同时启动进程。 **注意** 从 CLI 恢复可能会导致设备和管理中心之间的配置不同步，具体取决于您在升级后所做的更改。这可能会导致进一步的通信和部署问题。 新增/修改的CLI 命令： **upgrade revert**、 **show upgrade revert-info**。
Management Center 升级	
管理中心升级不会自动生成故障排除文件。	为了节省时间和磁盘空间，管理中心升级过程在升级开始前不再自动生成故障排除文件。请注意，设备升级 不受影响 ，并会继续生成故障排除文件。 要为管理中心手动生成故障排除文件，请选择 **系统**（⚙） > **运行状况** > **监控**，点击左侧面板中的 **防火墙管理中心** ，然后 **查看系统和故障排除详细信息**，然后 **生成故障排除文件**。
内容更新	
GeoDB 分为两个软件包。	在 2022 年 5 月，版本 7.2 发布前不久，我们将 GeoDB 拆分为两个包：一个将 IP 地址映射到国家/地区/大洲的国家/地区代码包，以及一个包含与可路由 IP 地址相关的上下文数据的 IP 包。此 IP 包中的情景数据可包括其他位置详细信息，以及连接信息，例如 ISP、连接类型、代理类型、域名等。 如果您的版本 7.2.0 – 7.2.5 管理中心可以访问互联网，并且您启用定期更新或从思科支持和下载站点手动启动一次性更新，则系统会自动获取这两个软件包。在版本 7.2.6+/7.4.0+ 中，您可以配置是否希望系统获取 IP 数据包。 如果手动下载更新（例如，在气隙式部署中），则必须单独导入数据包： • 国家代码包： Cisco_GEODB_Update-*date-build*.sh.REL.tar • IP 软件包： Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar **帮助** （❓） > **关于** 列出了系统当前使用的软件包版本。

表 *12:* 版本 *7.1.0* 的功能

功能	详细信息
威胁防御升级	

功能	详细信息
恢复成功的设备升级。	您现在可以将主要和维护升级恢复到 FTD。恢复可将软件恢复到上次升级前的状态，也称为 快照。如果在安装补丁后恢复升级，则会恢复补丁以及主要和/或维护升级。 **重要事项** 如果您认为可能需要恢复，则必须使用 **系统**（⚙）> **更新** 来升级 FTD。“系统更新”页面是唯一可以启用 **成功升级后启用恢复** 选项的位置，该选项会将系统配置为在启动升级时保存恢复快照。这与我们通常建议使用 **设备** > **设备升级** 页面上的向导形成鲜明对比。 容器实例不支持此功能。 最低 FTD 版本：7.1
改进了集群和高可用性设备的升级工作流程。	我们对集群和高可用性设备的升级工作流程进行了以下改进： • 升级向导现在可以将集群和高可用性设备正确显示为组，而不是单个设备。系统可以识别、报告和预先要求修复您可能遇到的组相关问题。例如，如果您在 Firepower 机箱管理器上进行了未同步的更改，则无法升级 Firepower 4100/9300 上的集群。 • 我们提高了将升级包复制到集群和高可用性对的速度和效率。以前，FMC 会按顺序将数据包复制到每个组成员。现在，组成员可以在正常同步过程中相互获取软件包。 • 您现在可以指定集群中数据设备的升级顺序。控制设备始终最后升级。

表 *13:* 版本 *7.0.0* 功能

功能	详细信息
威胁防御升级	
改进了 FTD 升级性能和状态报告。	FTD 升级现在更容易、更快、更可靠，并且占用的磁盘空间更少。消息中心的新 **升级** 选项卡进一步增强了升级状态和错误报告功能。

功能	详细信息
FTD 设备易于遵循的升级工作流程。	FMC 上的新设备升级页面（**设备 > 设备升级**）为升级版本 6.4+ FTD 设备提供了一个易于遵循的向导。它将引导您完成重要的升级前阶段，包括选择要升级的设备，将升级包复制到设备，以及兼容性和就绪性检查。 首先，请使用“设备管理”页面上的新 **升级 Firepower 软件** 操作（**设备 > 设备管理 > 选择操作**）。 继续操作时，系统会显示有关所选设备的基本信息以及当前的升级相关状态。这包括无法升级的任何原因。如果设备未在向导中“通过”某个阶段，则该阶段不会显示在下一阶段。 如果您离开向导，系统会保留您的进度，但具有管理员访问权限的其他用户可以重置、修改或继续向导。 **注释** 您仍必须使用 **系统**（⚙）> **更新** 来上传或指定 FTD 升级包的位置。您还必须使用“系统更新”页面升级 FMC 本身以及所有非 FTD 托管设备。 **注释** 在版本 7.0 中，向导无法正确显示集群或高可用性对中的设备。即使必须将这些设备作为一个单元进行选择和升级，向导也会将其显示为独立设备。设备状态和升级就绪性会逐个评估和报告。这意味着一台设备可能会“传递”到下一阶段，而另一台设备则不会。但是，这些设备仍然分组。因此，在一台设备上运行就绪性检查，所有设备上都会运行。在一台设备上启动升级，在所有设备上都会启动升级。 为避免可能的耗时升级失败，请手动确保所有组成员都已准备好继续执行向导的下一步，然后再点击 **下一步**。
一次升级更多 FTD 设备。	FTD 升级向导取消了以下限制： • 同步设备升级。 一次可以升级的设备数量现在受管理网络带宽的限制，而不是系统管理同步升级的能力。以前，我们建议不要一次升级超过五台设备。 **重要事项** 只有升级到 FTD 版本 6.7+ 才能看到此改进。如果您要将设备升级到较旧的 FTD 版本（即使您使用的是新的升级向导），我们仍建议您一次限制为五台设备。 • 按设备型号分组升级。 现在，只要系统有权访问相应的升级包，您就可以同时为所有 FTD 型号排队和调用升级。 以前，您需要选择一个升级包，然后使用该包选择要升级的设备。这意味着 只有 共享升级包时，您才能同时升级多台设备。例如，您可以同时升级两台 Firepower 2100 系列设备，但不能同时升级 Firepower 2100 系列和 Firepower 1000 系列。

表 *14:* 版本 *6.7.0* 功能

功能	详细信息
威胁防御升级	
升级会删除 PCAP 文件以节省磁盘空间。	升级现在会删除本地存储的 PCAP 文件。要升级，您必须拥有足够的可用磁盘空间，否则升级会失败。
改进了 FTD 升级状态报告和取消/重试选项。	您现在可以在“设备管理”页面上查看 FTD 设备升级和就绪性检查的状态，以及升级成功/失败的 7 天历史记录。消息中心还提供增强的状态和错误消息。 在“设备管理”和“消息中心”中点击一下即可访问新的“升级状态”弹出窗口，其中显示详细的升级信息，包括剩余百分比/时间、特定升级阶段、成功/失败数据、升级日志等。 此外，在此弹出窗口中，您可以手动取消失败或正在进行的升级（**取消升级**），或重试失败的升级（**重试升级**）。取消升级会将设备恢复到升级前的状态。 **注释** 为了能够手动取消或重试失败的升级，您必须禁用新的自动取消选项，该选项在您使用 FMC 升级 FTD 设备时显示： **在升级失败时自动取消并回滚到以前的版本**。启用选项后，设备会在升级失败时自动恢复到升级前的状态。 补丁不支持自动取消。在高可用性或集群部署中，自动取消会单独应用于每个设备。也就是说，如果一台设备上的升级失败，则仅恢复该设备。 新增/修改的屏幕： • **系统**（⚙）> **更新** > **产品更新** > **可用更新** > **安装** 图标用于 FTD 升级软件包 • **设备** > **设备管理** > **升级** • **消息中心** > **任务** 新增/修改的 CLI 命令： **show upgrade status detail**，**show upgrade status continuous**，**show upgrade status**，**upgrade cancel**，**upgrade retry**
内容更新	
规则冲突时，自定义入侵规则导入会发出警告。	现在，当您导入自定义（本地）入侵规则时，FMC 会向您发出规则冲突警告。以前，系统会以静默方式跳过导致冲突的规则 - 版本 6.6.0.1 除外，其中包含冲突的规则导入将完全失败。 在“规则更新”页面上，如果规则导入发生冲突，则“状态”列中会显示警告图标。有关详细信息，请将鼠标指针悬停在警告图标上，然后阅读工具提示。 请注意，当您尝试导入与现有规则具有相同 SID/修订号的入侵规则时，会发生冲突。您应始终确保自定义规则的更新版本具有新的修订版本号。 新增/修改的屏幕：我们在 **系统**（⚙）> **更新** > **规则更新**中添加了一个警告图标。

表 *15:* 版本 *6.6.0* 功能

功能	详细信息
威胁防御升级	
从内部 Web 服务器获取 FTD 升级包。	FTD 设备现在可以从您自己的内部 Web 服务器而不是从 FMC 获取升级包。这在 FMC 及其设备之间的带宽有限时尤其有用。它还可以节省 FMC 的空间。 **注释** 此功能仅支持运行版本 6.6+ 的 FTD 设备。它不支持升级 到 版本 6.6，也不支持 FMC 或经典设备。 新增/修改的屏幕：我们在上传升级包的页面中添加了 **指定软件更新源** 选项。
内容更新	
在初始设置期间自动更新 VDB。	设置新的或重新映像的 FMC 时，系统会自动尝试更新漏洞数据库 (VDB)。 这是一次性操作。如果 FMC 已接入互联网，我们建议您安排自动定期下载和安装 VDB 更新的任务。

表 *16:* 版本 *6.5.0* 的功能

功能	详细信息
内容更新	
自动软件下载和 GeoDB 更新。	当您设置新的或重新映像的 FMC 时，系统会自动安排： • 为 FMC 及其托管设备下载软件更新的每周任务。 • GeoDB 的每周更新。 任务是在 UTC 中安排的，这意味着它们在本地发生的时间取决于日期和您的特定位置。此外，由于任务是以 UTC 为单位进行计划的，因此它们不会针对夏令时、夏令时或您在地点可能观察到的任何季节性调整进行调整。如果您受到影响，则根据当地时间，安排的任务在夏季要比冬季“晚”一个小时。我们建议您查看自动安排的配置，并在必要时对其进行调整。

表 *17:* 版本 *6.4.0* 功能

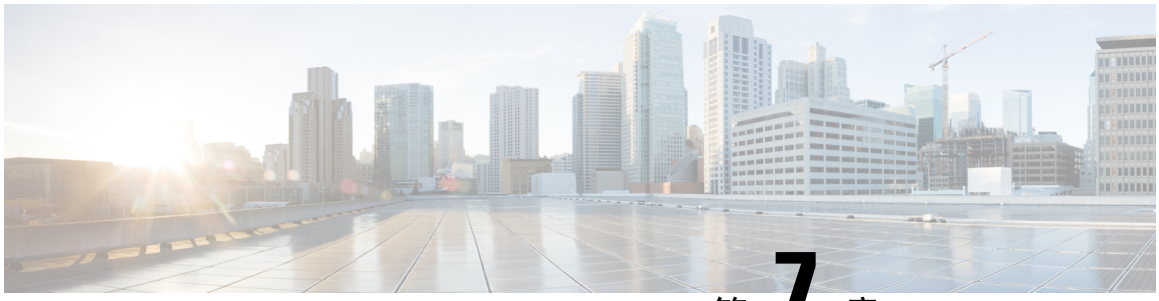
功能	详细信息
Management Center 升级	

功能	详细信息
升级会推迟计划任务。	管理中心 升级流程现在会推迟计划任务。任何计划在升级期间开始的任务都将在升级后重新启动后五分钟开始。 **注释** 在开始任何升级之前，您仍必须确保运行任务已完成。在升级开始时运行的任务会停止，成为失败的任务，且不能恢复。 请注意，从受支持的版本进行的所有升级均支持此功能。这包括 6.4.0.10 及更高版本补丁、版本 6.6.3 及更高维护版本以及版本 6.7.0+。从不支持的版本升级到支持的版本时，不支持此功能。
内容更新	
签名的 SRU、VDB 和 GeoDB 更新。	因此，系统可以验证您使用的是正确的更新文件，版本 6.4+ 使用签名的入侵规则 (SRU)、漏洞数据库 (VDB) 和地理位置数据库 (GeoDB) 更新。早期版本继续使用未签名的更新。 除非您从思科支持和下载站点手动下载更新 - 例如，在物理隔离部署中 - 否则您应该不会察觉到功能上的任何差异。但是，如果您手动下载并安装 SRU、VDB 和 GeoDB 更新，请确保为当前版本下载正确的软件包。 签名更新文件以“Cisco”（而不是“Sourcefire”）开头，以 .sh.REL.tar（而不是 .sh）结尾，如下所示： • SRU：Cisco_Firepower_SRU-日期-内部版本-vrt.sh.REL.tar • VDB：Cisco_VDB_Fingerprint_Database-4.5.0-版本.sh.REL.tar • GeoDB：Cisco_GEODB_Update-日期-内部版本.sh.REL.tar 我们将同时提供签名和未签名的更新，直到对需要未签名更新的版本的支持结束为止。不要解压签名的 (.tar) 包。如果您意外将已签名的更新上传到较早的 FMC 或 ASA FirePOWER 设备，则必须手动将其删除。离开软件包会占用磁盘空间，并且还可能导致未来升级出现问题。

表 *18:* 版本 *6.2.3* 的功能

功能	详细信息
设备升级	
升级前，将升级包复制到托管设备。	现在，您可以在运行实际升级之前，将升级包从 FMC 复制（或推送）到托管设备。这是非常有用的，因为您可以在“升级维护”窗口之外的低带宽使用时间内推送。 当您推送到高可用性、群集或可堆叠设备时，系统首先将升级包发送到活动/主要/首要设备，然后再发送到备用/数据/辅助设备。 新增/修改的屏幕： **系统**（⚙） > **更新**

功能	详细信息
内容更新	
在 VDB 更新之前， FMC 会重新启动警告。	现在 FMC 会警告您漏洞数据库 (VDB) 更新会重新启动 Snort 进程。这会中断流量检查，并且可能会中断流量，具体取决于受管设备处理流量的方式。您可以取消安装，直到更方便的时间，例如在维护窗口期间。 可能会出现以下警告： • 下载并手动安装 VDB 后。 • 当您创建计划任务来安装 VDB 时。 • VDB 在后台安装，例如，在之前安排的任务期间，或作为软件升级的一部分。



第 7 章

许可证

本章提供有关不同许可证类型、服务订用、许可要求等的深入信息。

注释 管理中心 支持智能许可证或传统 PAK（产品激活密钥）许可证作为其平台许可证。有关使用 PAK 许可证的更多信息，请参阅 配置管理中心基于 PAK 的旧版许可证，第 283 页。

关于许可证

思科智能许可是一种灵活的许可模式，为您提供一种更简便、更快速、更一致的方式来购买和管理整个思科产品组合和整个组织中的软件。此外它很安全，您可以控制用户可访问的内容。借助智能许可，您可以：

- **轻松激活：** 智能许可建立了可在整个组织中使用的软件许可证池，不再需要产品激活密钥 (PAK)。
- **统一管理：** 利用 My Cisco Entitlements (MCE)，您可以在一个易于使用的门户中全面了解您的所有 Cisco 产品和服务，始终了解您拥有以及正在使用的产品和服务。
- **许可证灵活性：** 您的软件没有与硬件节点锁定，因此您可以根据需要轻松使用和传输许可证。

要使用智能许可，您必须先在 Cisco Software Central (software.cisco.com) 上创建智能帐户。

有关思科许可的更详细概述，请访问 cisco.com/go/licensingguide

智能软件管理器和账户

当购买一个或多个许可证时，您可在智能软件管理器中对其进行管理： https://software.cisco.com/#module/SmartLicensing。通过思科智能软件管理器，您可以为组织创建一个主账户。如果您还没有账户，请点击此链接以设置新账户。通过思科智能软件管理器，您可以为组织创建一个主账户。有关说明，请参阅创建思科帐户。

默认情况下，许可证分配给主账户下的默认虚拟帐户。作为账户管理员，您可以创建其他虚拟帐户；例如，为区域、部门或子公司创建账户。使用多个虚拟账户有助于管理大量许可证和设备。

您可以通过虚拟账户管理许可证。只有该虚拟账户的设备可以使用分配给该账户的许可证。如果您需要其他许可证，则可以从另一个虚拟账户传输未使用的许可证。您还可以在虚拟账户之间迁移设备。

气隙部署的许可选项

下表比较对无互联网访问环境中的许可部署可用的选项。对于您面临的具体情况，您的销售代表可能会提供其他建议。

表 *19:* 气隙网络许可选项的比较

智能软件管理器本地版	特定许可证预留
可对大量产品进行扩展	最适合少量设备
自动化许可管理、使用情况和资产管理可视性	有限的使用情况和资产管理可视性
添加设备不会增加运营成本	添加设备的运营成本随时间推移呈线性增长
灵活、易用、开销更低	移动、添加和更改的管理和手动开销较大
允许初期和各类到期状态下存在不合规状态	不合规状态影响系统运作
有关详细信息，请参阅将管理中心注册到本地智能软件管理器，第 265 页	有关详细信息，请参阅配置特定许可证预留 (SLR)，第 273 页

管理中心和设备的许可工作原理

管理中心 向智能软件管理器注册，然后为每个受管设备分配许可证。设备不直接向智能软件管理器注册。

物理 管理中心 本身不需要许可证。 management center virtual 需要平台许可证。

与智能软件管理器的定期通信

为维护产品许可证授权，您的产品必须与智能软件管理器定期通信。

您可以使用产品实例注册令牌通过思科智能软件管理器注册 管理中心 。智能软件管理器会为 管理中心 和智能软件管理器之间的通信颁发 ID 证书。此证书有效期为 1 年，但需要每 6 个月续签一次。如果 ID 证书到期（一年后没有通信）， 管理中心 可能会从您的账户中删除。

管理中心 定期与智能软件管理器通信。如果您在智能软件管理器中进行更改，则可以刷新 管理中心 上的授权，以使更改立即生效。另外，也可以等待 管理中心 按计划通信。

您的 管理中心 必须具有对智能软件管理器的直接互联网访问权限，或使用气隙部署的许可选项，第 240 页中所述的选项之一。在 non-airgapped 部署中，常规许可证通信每 30 天进行一次，但如果具有宽限期，则 管理中心 会最多运行 90 天，而不会联系智能软件管理器。确保 管理中心 在 90 天内联系智能软件管理器，否则 管理中心 将恢复为未注册状态。

评估模式

在 管理中心 向智能软件管理器注册之前，它会在评估模式下运行 90 天。您可以将功能许可证分配给受管设备，它们将在评估模式的持续时间内保持合规。此时间段结束后， 管理中心 将取消注册。

如果您向智能软件管理器注册 管理中心 ，则评估模式将结束。如果您稍后取消注册 管理中心，则无法恢复评估模式，即使最初没有使用所有 90 天。

有关未注册状态的详细信息，请参阅已注销状态，第 241 页。

注释 您不能接收评估许可证进行强加密 (3DES/AES)；您必须向智能软件管理器注册，以接收可启用强加密 (3DES/AES) 许可证的导出合规性令牌。

不合规状态

管理中心 在以下情况下可能会处于不合规状态：

- 过度使用 - 当托管设备或 management center virtual 使用不可用的许可证时。
- 许可证到期 - 当托管设备基于时间的许可证到期时。

在不合规状态下，请参阅以下影响：

- Management Center Virtual 平台许可证 - 操作不受影响。
- 所有 托管设备许可证 - 操作不受影响。

在您解决许可问题后， 管理中心 将显示它现在符合智能软件管理器的定期计划授权。要强制授权，请点击 **系统**（⚙）> **许可证** > **智能许可证** 页面上的 **重新授权** 。

已注销状态

在以下情况下， 管理中心 可能会取消注册：

- 评估模式到期-评估模式在 90 天后到期。

- 手动注销 管理中心
- 与智能软件管理器缺少通信- 管理中心 在 1 年内不与智能软件管理器通信。注意：90 天后， 管理中心 授权将到期，但可以在一年内成功恢复通信，以自动重新授权。一年后，ID 证书到期，将从您的账户中删除 管理中心 ，因此您必须手动重新注册 管理中心。

在未注册状态下， 管理中心 无法将任何配置更改部署到 需要许可证的功能的设备。

最终用户许可证协议

http://www.cisco.com/go/softwareterms 提供了用于监管您使用此产品的思科最终用户许可证协议 (EULA) 和所有适用补充协议 (SEULA)。

许可证类型和限制

本节介绍可用的许可证类型。

表 *20*: 智能许可证

您分配的许可证	持续时间	授予的功能
基础版	永久或订用 **注释** 基础版 订用许可证仅在 Threat Defense Virtual上受支持。	除特定许可证预留和 Cisco Secure Firewall 3100/4200、基础版 永久许可证会自动分配给所有 威胁防御。 用户和应用控制 交换和路由 NAT 有关详细信息，请参阅基础版许可证 ， 第 244 页。
IPS	订用	入侵检测和预防 文件控制 安全情报过滤 有关详细信息，请参阅 IPS 许可证 ， 第 245 页

您分配的许可证	持续时间	授予的功能
恶意软件 防御	订用	恶意软件 防御 Secure Secure Malware Analytics 文件存储 （IPS 许可证是恶意软件 防御 许可证的前提条件。） 有关详细信息，请参阅中的文件和恶意软件策略的许可证要求。恶意软件防御许可证，第 244 页《Cisco Secure Firewall Management Center 设备配置指南》
运营商	Firepower 4100/9300、Cisco Secure Firewall 3100/4200 和 Threat Defense Virtual 的订用	Diameter、GTP/GPRS、M3UA 和 SCTP 检测 有关详细信息，请参阅运营商许可证，第 246 页。
URL 过滤	订用	基于类别和信誉的 URL 过滤 有关详细信息，请参阅URL 过滤许可证，第 247 页。 （IPS 许可证是 URL 过滤 许可证的前提条件。）
Management Center Virtual	• 定期智能许可-永久 • 特定许可证预留- 订用	平台许可证决定 management center virtual 可以管理的设备数量。 有关详细信息，请参阅Management Center Virtual许可证，第 244 页。
出口管制功能	永久	受国家安全、外交政策和反恐怖主义法律和法规约束的功能；请参阅出口控制功能的许可，第 248 页。
远程访问 VPN： • Secure Client Premier • Secure Client Advantage • 仅限 Secure Client VPN	订用或永久	远程访问 VPN 配置。您的账户必须允许出口控制功能，以便配置远程访问 VPN。在注册设备时，您需要选择是否满足出口要求。 威胁防御 可以使用任何有效 Secure Client 许可证。可用功能不因许可证类型不同而不同。 有关详细信息，请参阅 Secure Client许可证，第 247 页 和 《Cisco Secure Firewall Management Center 设备配置指南》中的 *VPN* 许可 。

注释 订用许可证是基于期限的许可证。

Management Center Virtual许可证

management center virtual 需要一个与其可管理的设备数量相关的平台许可证。

management center virtual 支持智能许可。

在常规智能许可中，这些许可证是永久的。

在指定许可证预留 (SLR) 中，这些许可证基于订用。

注释 对于FMCv上新设备的附加许可证要求，建议迁移到支持其他设备的更高的management center virtual型号。

基础版许可证

基础版 许可证允许您：

- 配置您的设备以执行交换和路由（包括 DHCP 中继和 NAT）
- 将设备配置为高可用性对
- 配置集群
- 通过将用户和应用条件添加到访问控制规则实施用户和应用控制
- 更新思科漏洞数据库 (VDB) 和地理位置数据库 (GeoDB)。
- 下载入侵规则，例如 SRU/LSP。但是，除非已启用 IPS 许可证，否则无法将具有入侵策略的访问控制策略或规则部署到设备。

Cisco Secure Firewall 3100/4200

您在购买 Cisco Secure Firewall 3100/4200 时获得 基础版 许可证。

其他型号

除使用特定许可证预留的部署外，对于已注册到 管理中心的每个账户， 基础版 许可证会自动添加到您的账户。对于特定许可证预留，您需要将 基础版 许可证添加到您的帐户。

恶意软件防御许可证

通过恶意软件防御许可证，您可以执行恶意软件防护和 Secure Secure Malware Analytics。通过此功能，您可以使用设备检测并阻止通过网络传输的文件中的恶意软件。要支持此功能许可证，您可以购买恶意软件 防御 (AMP) 服务订阅作为独立订阅，或与 IPS (TM) 或 IPS 和 URL 过滤 (TMC) 订用。IPS 许可证是获得恶意软件 防御 许可证的前提条件。

注释 已启用恶意软件防御许可证的受管设备会定期尝试连接到安全恶意软件分析云，即使尚未配置动态分析也如此。因此，设备的接口流量控制面板构件显示传输的流量；这是预期行为。

配置恶意软件防护作为文件策略的一部分，然后与一个或多个访问控制规则相关联。文件策略可以检测到用户通过特定应用协议上传或下载特定类型文件。恶意软件防护 支持使用本地恶意软件分析和文件预分类来检查一组受限的恶意软件文件类型。您也可以将特定文件类型下载并提交到 Secure Secure Malware Analytics 云进行动态和 Spero 分析，从而确定文件是否包含恶意软件。对于这些文件，您可以查看网络文件轨迹，其中详述文件通过网络所采用的路径。恶意软件防御许可证还可用于将特定文件添加至文件列表，并在文件策略中启用文件列表，从而在检测时自动允许或拦截这些文件。

请注意，仅在部署 恶意软件防护 和 Secure Secure Malware Analytics时，才需要恶意软件 防御 许可证。恶意软件 防御 许可证，则 管理中心 可以从安全恶意软件分析云接收 Cisco Secure Endpoint 恶意软件事件和危害表现 (IOC)。

另请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 文件和恶意软件策略的许可证要求 中的重要信息。

禁用此许可证时：

- 系统会停止查询安全恶意软件分析云，并且还会停止确认从安全恶意软件分析云发送的追溯性事件。
- 如果现有访问控制策略包含恶意软件防护 配置，则无法对其重新部署。
- 请注意，在禁用恶意软件 防御 许可证后的很短时间内，系统可以使用现有缓存文件处置情况。在时间窗口到期后，系统会向这些文件分配处置情况 `Unavailable`。

如果许可证到期，上述功能的授权将停止，而 管理中心 将进入不合规状态。

IPS 许可证

IPS 许可证可用于执行入侵检测和阻止、文件控制和安全情报过滤：

- 入侵检测和防御可用于分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。
- 文件控制 可用于检测和/或阻止用户通过特定应用协议上传（发送）或下载（接收）特定类型的文件。 恶意软件防护需要恶意软件 防御 许可证， 可用于基于某组受限文件类型的处置情况对其进行检查和阻止。
- 安全情报过滤 ， 允许您在流量接受访问控制规则的分析之前，拒绝发送到特定 IP 地址、URL 和DNS域名或从其发送的流量，即，将其阻止。动态源可用于根据最新情报立即阻止连接。或者，可将“仅监控”设置用于安全情报过滤。

您可以购买 IPS 许可证作为独立订用 (T) 或与 URL 过滤 (TC)、恶意软件 防御 (TM) 或二者的组合 (TMC)。

禁用此许可证时：

- 管理中心 会停止从受影响设备确认入侵和文件事件。因此，使用这些事件作为触发器条件的关联规则停止开启。
- 管理中心 将不会连接互联网获取思科提供的信息或第三方安全情报信息。
- 在重新启用 IPS 之前，您无法重新部署现有入侵策略。

如果许可证到期，上述功能的授权将停止，而 管理中心 将进入不合规状态。

运营商许可证

运营商许可证，可以实现以下门户检查功能：

- Diameter - Diameter是用于下一代移动和固定电信网络（例如用于 LTE（长期演进）和 IMS（多媒体子系统）的 EPS（演进的数据包系统）的身份验证、授权和记账 (AAA) 协议。在这些网络中，该协议将取代 RADIUS 和 TACACS。
- GTP/GPRS—GPRS 隧道协议 (GTP) 用于 GSM、UMTS 和 LTE 网络的通用分组无线服务 (GPRS) 流量。GTP 提供隧道控制和管理协议，通过创建、修改和删除隧道来为移动站提供 GPRS 网络接入。此外，GTP 还使用隧道机制来传送用户数据包。
- M3UA—MTP3 User Adaptation (M3UA) 是客户端/服务器协议，为基于 IP 的应用提供连接 SS7 网络的网关，以便连接信令系统 7 (SS7) 消息传递部分 3 (MTP3) 层。使用 M3UA，可以通过 IP 网络运行 SS7 用户部分（例如 ISUP）。
- SCTP - 流控制传输协议 (SCTP) 是支持基于 IP 网络的 SS7 协议的传输层协议。它支持 4G LTE 移动网络架构。SCTP 可以处理多个同步数据流、多路复用数据流，并提供更多安全功能。

注释 在设备上启用此许可证后，请使用 FlexConfig 策略启用协议检测。

运营商许可证 PID 按系列提供，而不按设备型号提供。您可以在评估模式下或使用智能许可证为每台设备启用此许可证。

Firepower 4100/9300、Cisco Secure Firewall 3100/4200 和 Threat Defense Virtual 的运营商许可证是基于期限的。此许可证还支持特定许可证预留。

支持的设备

支持运营商许可证的设备包括：

- Secure Firewall 3110
- Secure Firewall 3120
- Secure Firewall 3130
- Secure Firewall 3140
- Firepower 4112

- Firepower 4115
- Firepower 4125
- Firepower 4145
- Cisco Secure Firewall 4215
- Cisco Secure Firewall 4225
- Cisco Secure Firewall 4245
- Firepower 9300
- Threat Defense Virtual

URL 过滤许可证

URL 过滤许可证可用于编写访问控制规则，该规则可根据受监控主机请求的 URL 确定可横越网络且与那些 URL 的相关信息关联的流量。要支持此功能许可证，您可以购买 URL 过滤 服务订阅作为独立订阅，或与 IPS (TC) 或威胁和恶意软件防御 (TMC) 订用一道购买。IPS 许可证是获得该许可证的前提条件。

提示 如果没有 URL 过滤许可证，则可以指定要允许或阻止的单个 URL 或 URL 组。这个选项将对网络流量进行精细和自定义控制，但是，不允许使用 URL 类别和信誉数据来过滤网络流量。

虽然您无需 URL 过滤许可证即可将基于类别和信誉的 URL 条件添加到访问控制规则，但 管理中心 将不会下载 URL 信息。只有先将 URL 过滤许可证添加到 管理中心，然后在该策略针对的设备上进行启用，才能部署访问控制策略。

禁用此许可证时：

- 您可能会失去对 URL 过滤的访问权限。
- 具有 URL 条件的访问控制规则会立即停止过滤 URL。
- 您的 管理中心 不再可供下载 URL 数据更新。
- 如果现有访问控制策略包括的规则带有基于类别和信誉的URL条件，则不能重新部署现有的访问控制策略。

如果许可证到期，上述功能的授权将停止，而 管理中心 将进入不合规状态。

Secure Client许可证

您可以使用 Secure Client 和基于标准的 IPSec / IKEv2 配置远程访问 VPN。

要启用远程访问 VPN 功能，必须购买并启用以下许可证之一： Secure Client Advantage、 Secure Client Premier或 仅限 Secure Client VPN。如果你有 Secure Client Advantage 和 Secure Client Premier ，并想同时使用这两个许可证，则可以两个都选择。 仅限 Secure Client VPN许可证不能与 **Apex** 或 **Plus**一

起使用。 Secure Client 许可证必须与智能帐户共享。有关更多说明，请参阅http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf。

如果指定的设备不具有至少其中一个指定的Secure Client许可证类型的权利，则无法将远程访问VPN配置部署到设备。如果注册的许可证不符合规定或权利到期，系统将显示授权警报和运行状况事件。

使用远程访问 VPN 时，您的智能帐户必须已启用导出控制功能（强加密）。威胁防御需要强加密（高于 DES），才能与 Secure Client 客户端成功建立远程访问 VPN 连接。

如果以下情况属实，则无法部署远程访问 VPN：

- 管理中心上的智能许可在评估模式下运行。
- 您的智能帐户未配置为使用导出控制功能（强加密）。

出口控制功能的许可

需要出口控制功能的功能

某些软件功能受国家安全、外交政策和反恐怖主义法律和法规约束。这些出口控制功能包括：

- 安全认证合规性
- 远程访问 VPN
- 具有强加密的站点间 VPN
- 具有强加密的 SSH 平台策略
- 具有强加密的 SSL 策略
- 具有强加密的功能，例如 SNMPv3

如何确定系统当前是否启用了出口控制功能

要确定系统当前是否启用了出口控制功能：请转至**系统 > 许可证 > 智能许可证**，查看**出口控制功能**是否显示为**启用**。

关于启用出口控制功能

如果 **出口控制功能** 显示 **禁用** ，而您想要使用需要强加密的功能，有两种方式。您的组织可能有资格使用其中一种方法（或者二者皆不可使用），但不可同时使用这两种方法。

- 在智能软件管理器中生成新的产品实例注册令牌时，如果 没有 启用出口控制功能的选项：

  Cisco批准后，您可以向帐户手动添加强加密许可证，以便使用导出控制功能。有关详细信息，请参阅 对于无全局权限的账户启用出口控制功能， 第 266 页

- 如果在智能软件管理器中生成新的产品实例注册令牌时，显示选项“在使用此令牌注册的产品上允许导出控制功能”，请确保在生成令牌之前选中该选项。

  如果未为用于注册 管理中心的产品实例注册令牌启用导出控制功能，则必须使用启用了导出控制功能的新产品实例注册令牌取消注册，然后重新注册 管理中心 。

如果在评估模式下或在上 管理中心 启用强加密之前将设备注册到 管理中心，请重新启动每台受管设备以提供强加密。在高可用性部署中，主用和备用设备必须同时重启以避免出现主主状态。

授权永久有效，无需订用。

更多信息

有关出口控制的一般信息，请参阅https://www.cisco.com/c/en/us/about/legal/global-export-trade.html。

Threat Defense Virtual许可证

本部分描述可用于 threat defense virtual 的性能分级许可授权。

可以在任何受支持的 threat defense virtual vCPU/内存配置中使用任何 threat defense virtual 许可证。这可让 threat defense virtual 客户在各种各样的 VM 资源占用空间中运行。这还会增加受支持的 AWS 和 Azure 实例类型的数量。配置 threat defense virtual VM 时，支持的 vCPU 最大核数为 16（对于 VMware 和 KVM 上的 FTDv；支持的最大内存为 32GB RAM 。

Threat Defense Virtual 智能许可的性能级别

RA VPN 的会话限制由安装的 threat defense virtual 平台授权级别确定，并通过速率限制器强制执行。下表总结了基于授权层和速率限制器的会话限制。

表 *21:* 基于授权的 ***Threat Defense Virtual*** 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/32 GB	16Gbps	10,000

FTDv 性能级许可准则和限制

许可 threat defense virtual 设备时，请时刻注意以下准则和限制。

- threat defense virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。
- 可以在任何受支持的 threat defense virtual 核心/内存配置中使用任何 threat defense virtual 许可证。这可让 threat defense virtual 客户在各种各样的 VM 资源占用空间中运行。
- 无论您的设备是处于评估模式还是已注册到思科智能软件管理器，您都可以在部署 threat defense virtual时选择性能级别。

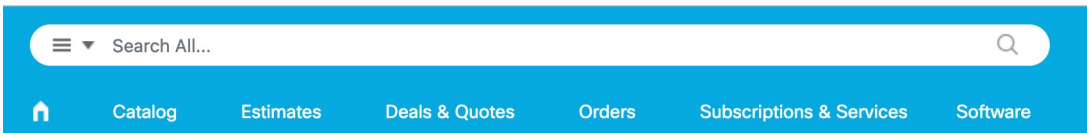
注释 确保智能许可账户包含所需的可用许可证。选择与您账户中的许可证相匹配的级别很重要。如果要将 threat defense virtual 升级到 7.0 版，可以选择 **FTDv - 变量**来保持当前的许可证合规性。threat defense virtual 会根据您的设备功能（内核数/RAM）继续执行会话限制。

- 部署新 threat defense virtual 设备或使用 REST API 调配 threat defense virtual 时，默认性能级别为 FTDv50。
- 基础版许可证以订用为基础，并映射到性能级别。您的虚拟帐户需要具有 threat defense virtual 设备的 基础版 许可证授权，以及 IPS 、恶意软件防御和 URL 过滤 许可证的授权。
- 每个 HA 对等体使用一个授权，并且每个 HA 对等体上的授权必须匹配，包括基础版许可证。
- 高可用性对的性能级别更改应应用于主对等体。
- 您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。
- 通用 PLR 许可单独应用于高可用性对中的每台设备。辅助设备不会自动镜像主设备的性能级别，而是必须手动更新。

许可证 PID

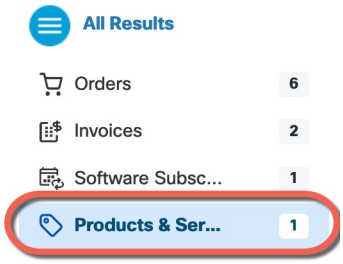
当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用思科商务工作空间上的**搜索全部 (Search All)** 字段。

图 *14:* 许可证搜索



从结果中选择**产品和服务 (Products & Services)**。

图 *15:* 成果



Management Center Virtual PID

- VMware：
  - SF-FMC-VMW-2-K9 - 2 设备
  - SF-FMC-VMW-10-K9 - 10 设备
  - SF-FMC-VMW-K9 - 25 设备
  - SF-FMC-VMW-300-K9 - 300 设备
- KVM：
  - SF-FMC-KVM-2-K9 - 2 设备
  - SF-FMC-KVM-10-K9 - 10 设备
  - SF-FMC-KVM-K9 - 25 设备
- 基于 PAK 的 VMware：
  - FS-VMW-2-SW-K9 - 2 设备
  - FS-VMW-10-SW-K9 - 10 设备
  - FS-VMW-SW-K9 - 25 设备

Threat Defense Virtual PID

订购 FTDV-SEC-SUB 时，必须选择 基础版 许可证和可选功能许可证（12 个月期限）：

- 基础版许可证：
  - FTD-V-5S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-20S-BSE-K9
  - FTD-V-30S-BSE-K9
  - FTD-V-50S-BSE-K9
  - FTD-V-100S-BSE-K9
- IPS 、恶意软件 防御和 URL 许可证组合：
  - FTD-V-5S-TMC
  - FTD-V-10S-TMC
  - FTD-V-20S-TMC
  - FTD-V-30S-TMC

- FTD-V-50S-TMC
- FTD-V-100S-TMC

- 运营商 — FTDV_CARRIER
- Cisco Secure 客户端-请参阅 思科安全客户端订购指南。

Firepower 1010 PID

- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-FPR1010T-TMC=

  当您将上述 PID 添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- Cisco Secure 客户端-请参阅 思科安全客户端订购指南。

Firepower 1100 PID

- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-FPR1120T-TMC=
  - L-FPR1140T-TMC=
  - L-FPR1150T-TMC=

  当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR1120T-TMC-1Y
  - L-FPR1120T-TMC-3Y
  - L-FPR1120T-TMC-5Y
  - L-FPR1140T-TMC-1Y
  - L-FPR1140T-TMC-3Y
  - L-FPR1140T-TMC-5Y
  - L-FPR1150T-TMC-1Y
  - L-FPR1150T-TMC-3Y
  - L-FPR1150T-TMC-5Y

- Cisco Secure 客户端-请参阅 思科安全客户端订购指南。

Firepower 2100 PID

- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-TMC=

  当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y
  - L-FPR2120T-TMC-3Y
  - L-FPR2120T-TMC-5Y
  - L-FPR2130T-TMC-1Y
  - L-FPR2130T-TMC-3Y
  - L-FPR2130T-TMC-5Y
  - L-FPR2140T-TMC-1Y
  - L-FPR2140T-TMC-3Y
  - L-FPR2140T-TMC-5Y
- Cisco Secure 客户端-请参阅 思科安全客户端订购指南。

Cisco Secure Firewall 3100 PID

- 基础版许可证：
  - L-FPR3110-BSE=
  - L-FPR3120-BSE=
  - L-FPR3130-BSE=
  - L-FPR3140-BSE=
- IPS 、恶意软件 防御和 URL 许可证组合：

- L-FPR3110T-TMC =
- L-FPR3120T-TMC =
- L-FPR3130T-TMC =
- L-FPR3140T-TMC =

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-FPR3105T-TMC-1Y
- L-FPR3105T-TMC-3Y
- L-FPR3105T-TMC-5Y
- L-FPR3110T-TMC-1Y
- L-FPR3110T-TMC-3Y
- L-FPR3110T-TMC-5Y
- L-FPR3120T-TMC-1Y
- L-FPR3120T-TMC-3Y
- L-FPR3120T-TMC-5Y
- L-FPR3130T-TMC-1Y
- L-FPR3130T-TMC-3Y
- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-TMC-5Y

- 运营商 - L-FPR3K-FTD-CAR=
- Cisco Secure 客户端-请参阅 思科安全客户端订购指南。

Firepower 4100 PID

- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-TMC=

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-FPR4112T-TMC-1Y
- L-FPR4112T-TMC-3Y
- L-FPR4112T-TMC-5Y
- L-FPR4115T-TMC-1Y
- L-FPR4115T-TMC-3Y
- L-FPR4115T-TMC-5Y
- L-FPR4125T-TMC-1Y
- L-FPR4125T-TMC-3Y
- L-FPR4125T-TMC-5Y
- L-FPR4145T-TMC-1Y
- L-FPR4145T-TMC-3Y
- L-FPR4145T-TMC-5Y

- 运营商 - L-FPR4K-FTD-CAR=
- Cisco Secure 客户端-请参阅 思科安全客户端订购指南。

Cisco Secure Firewall 4200 PID

- 基础版许可证：
  - L-FPR4215-BSE=
  - L-FPR4225-BSE=
  - L-FPR4245-BSE=
- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-FPR4215T-TMC=
  - L-FPR4225T-TMC=
  - L-FPR4245T-TMC=

  当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR4215T-TMC-1Y
  - L-FPR4215T-TMC-3Y
  - L-FPR4215T-TMC-5Y

- L-FPR4225T-TMC-1Y
- L-FPR4225T-TMC-3Y
- L-FPR4225T-TMC-5Y
- L-FPR4245T-TMC-1Y
- L-FPR4245T-TMC-3Y
- L-FPR4245T-TMC-5Y

- 运营商 - L-FPR4200K-FTD-CAR=
- Cisco Secure 客户端-请参阅 思科安全客户端订购指南。

Firepower 9300 PID

- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-FPR9K-40T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-TMC=

  当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR9K-40T-TMC-1Y
  - L-FPR9K-40T-TMC-3Y
  - L-FPR9K-40T-TMC-5Y
  - L-FPR9K-48T-TMC-1Y
  - L-FPR9K-48T-TMC-3Y
  - L-FPR9K-48T-TMC-5Y
  - L-FPR9K-56T-TMC-1Y
  - L-FPR9K-56T-TMC-3Y
  - L-FPR9K-56T-TMC-5Y
- 运营商 - L-FPR9K-FTD-CAR=
- Cisco Secure 客户端-请参阅 Cisco AnyConnect 订购指南。

ISA 3000 PID

- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-ISA3000T-TMC=

当您将上述 PID 添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-ISA3000T-TMC-1Y
- L-ISA3000T-TMC-3Y
- L-ISA3000T-TMC-5Y

- Cisco Secure 客户端-请参阅 Cisco AnyConnect 订购指南。

许可的要求和前提条件

对于特定许可证预留的要求，请参阅 特定许可证预留的要求和前提条件，第 274 页。

一般前提条件

- 确保在 管理中心 和托管设备上配置了 NTP。时间必须同步才能成功注册。

  对于 Firepower 4100/9300，必须使用与 管理中心相同的机箱 NTP 服务器在机箱上配置 NTP。

支持的域

全局，除非另有说明。

用户角色

- 管理员

高可用性、集群和多实例许可的要求和前提条件

本节介绍 高可用性（ 设备高可用性 和 management center virtual 高可用性）、集群和多实例部署的许可要求。

管理中心 高可用性许可

每台设备都需要相同的许可证，无论是由单个 管理中心 管理还是由 管理中心高可用性对（硬件或虚拟）中的管理。

示例： 如果要对由 管理中心 对管理的两个设备启用高级恶意软件保护，请购买两个 恶意软件防御许可证和两个 TM 订用，向智能软件管理器注册主要 管理中心，然后将许可证分配给主要 管理中心上的两个设备。

只有主用管理中心会向智能软件管理器注册。故障切换发生时，系统与智能软件管理器通信，以释放原始主用 管理中心 中的许可证授权，并将其分配到新的主用 管理中心。

在特定许可证预留部署中，只有主 管理中心 需要特定许可证预留。

硬件 管理中心

高可用性对中的 管理中心硬件不需要特殊许可证。

Management Center Virtual

您将需要两个相同许可的 management center virtual。

示例： 对于管理 10 台设备的 management center virtual 高可用性对，您可以使用：

- 两（2） management center virtual 10个授权
- 10 个设备许可证

如果中断高可用性对，则会释放与辅助 management center virtual 关联的 management center virtual 授权。（在本例中，您将有两个独立的 management center virtual 10。）

设备高可用性许可

高可用性配置中的两台 威胁防御 设备必须具有相同的许可证。

高可用性配置需要两种许可证权利；对中的每个设备各一个。

在建立高可用性之前，将哪些许可证分配给辅助/备用设备并不重要。进行高可用性配置期间，管理中心 会释放分配给备用设备的所有不必要的许可证，并用分配给主/主用设备的相同许可证替换它们。例如，如果主用设备具有 基础版 许可证和 IPS 许可证，而备用设备只有 基础版 许可证， 管理中心 将与智能软件管理器通信，以从您的备用设备的账户获取可用 IPS 许可证。如果您的许可证帐户不包含足够的购买权利，则您的帐户将在您购买正确数量的许可证之前变得不符合要求。

设备集群许可

每个 threat defense virtual 集群节点都需要相同的性能层许可证。我们建议为所有成员使用相同数量的 CPU 和内存，否则将限制所有节点上的性能，以匹配功能最低的成员。吞吐量级别将从控制节点复制到每个数据节点，以便它们匹配。

您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。

在将控制节点添加到 管理中心时，您可以指定要用于该集群的功能许可证。在创建集群之前，将哪些许可证分配给数据节点并不重要；控制节点的许可证设置将复制到每个数据节点。您可以在 **系统**（⚙） > **许可证** > **智能许可证 > 编辑许可证** 或**设备** > **设备管理** > **集群** > **许可证** 区域中修改集群的许可证。

注释 如果在 管理中心 获得许可（并在评估模式下运行）之前添加了集群，当您许可 管理中心 时，会在将策略更改部署到集群时遇到流量中断的情况。更改为许可模式会导致所有数据单元先退出集群，然后重新加入。

许可多实例部署

所有许可证按每个引擎/机箱（对于 Firepower 4100）或每个安全模块（对于 Firepower 9300）予以使用，而不是按每个容器实例使用。请查看以下详细信息：

- 基础版 许可证自动分配：每个 安全模块/引擎一个。
- 功能许可证手动分配到每个实例；但每个 安全模块/引擎每个功能只能使用一个许可证。例如，对于具有 3 个安全模块的 Firepower 9300，每个模块只需要一个 URL 过滤 许可证，总共需要 3 个许可证，而无须考虑正在使用的实例数。

例如：

表 *22: Firepower 9300* 上容器实例的许可证使用情况示例

Firepower 9300	实例	许可证
Security Module 1	实例 1	基础版、 URL 过滤、 恶意软件防御
	实例 2	基础版、 URL 过滤
	实例 3	基础版、 URL 过滤
安全模块 2	实例 4	基础版、 IPS
	实例 5	基础版、 URL 过滤、 恶意软件防御、 IPS
安全模块 3	实例 6	基础版、 恶意软件防御、 IPS
	实例 7	基础版、 IPS

表 *23:* 许可证总数

基础版	**URL** 过滤	恶意软件防御	**IPS**
3	2	3	2

创建思科帐户

您必须拥有思科账户才能申请智能账户并许可任何思科产品。

过程

步骤 1 打开 URL https://id.cisco.com/signin/register 以创建新账户。

步骤 2 输入所有必填字段以创建账户。

下图显示了一个示例。

步骤 3 点击**注册 (Register)**。

系统会向您发送一封包含激活码的邮件，以验证您的邮箱地址。

注释 如果您尚未收到邮件，请通过 web-help@cisco.com 向注册支持团队发送邮件。

步骤 4 在**使用您的邮箱验证 (Verify with your email)** 页面中，输入激活码以完成注册过程，然后点击**验证 (Verify)**。

注册成功后，您将被重定向到登录页面。

下一步做什么

在登录页面输入新创建的账户详细信息，以请求智能账户。请参阅创建智能账户并添加许可证，第 260 页。

创建智能账户并添加许可证

购买许可证之前，您应设置此账户。

开始之前

您的客户代表可以代表您设置智能账户。如果是这样，则无须按照本程序进行操作，而是从该客户代表处获取访问该账户所需的信息，并确认可以访问该账户。

如果您还没有思科账户，则必须创建一个新账户。有关说明，请参阅创建思科帐户。

有关智能账户的一般信息，请参阅http://www.cisco.com/go/smartaccounts。

过程

步骤 1 转到创建智能账户 (Create a Smart Account) 页面。系统将提示您使用思科账户登录。

在**创建智能账户 (Create a Smart Account)** 页面中，将显示您的基本账户信息。

步骤 2 点击右上角显示的**我的账户 (My Account)** 图标，然后点击**管理配置文件 (Manage Profile)**。

步骤 3 点击**个人 (Personal)**。

步骤 4 在**您的公司详细信息 (Your Company Details)** 部分中，点击**编辑 (Edit)**。

步骤 5 在**公司或组织 (Company or organization)** 字段中，键入您的组织名称。

步骤 6 如果您的公司信息已存在于我们的数据库中，它将显示在列表中。您可以选择您的公司。

在**地址 (Address)** 下拉列表中，选择您公司的地址。

步骤 7 如果您的公司未在我们的数据库中列出，您可以继续在**公司或组织 (Company or organization)** 字段中输入您的公司信息。

a) 在**地址 (Address)** 下拉列表中，点击下拉箭头，然后点击**添加新地址 (Add New Address)**。

b) 您可以选择以下**地址类型 (Address Type)** 选项之一：

- **公司/组织 (Company/Organization)**：提供您的组织的地址。思科会验证此地址。如果地址和公司名称无法通过国家/地区验证，您可能无法继续。因此，您必须确保提供正确的地址。
- **个人 (Personal)**：提供您的个人地址。

步骤 8 输入与您的公司相关的所有必填字段，然后点击**更新 (Update)**。

您的公司详细信息 (Your Company Details) 部分将显示您输入的公司详细信息。

如果您的公司详细信息已通过验证，系统将显示成功消息。

步骤 9 点击**更新**。

如果您的公司详细信息已通过验证，系统将显示成功消息。

步骤 10 打开在上一个选项卡中打开的**创建智能账户 (Create a Smart Account)** 页面。如果未反映更改，请刷新页面。

或者，您可以使用 https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation URL 打开此页面，然后使用您的凭证登录。

步骤 11 点击**创建帐户 (Create Account)**。

“账户摘要”(Account Summary) 页面将显示您的账户详细信息。

步骤 12 点击**完成 (Done)**。

步骤 13 等待智能账户已做好设置准备的通知邮件。在收到邮件时，按照指示点击邮件中的链接。

步骤 14 请确保智能许可帐户包含所需的可用许可证。

有关许可证 PID，请参阅 许可证 PID，第 250 页。

下一步做什么

要使用智能软件管理器配置智能许可证，请参阅配置智能许可，第 262 页。

配置智能许可

本节介绍如何通过智能软件管理器或本地智能软件管理器使用智能许可。要使用指定许可证预留，请参阅 配置特定许可证预留 (SLR)，第 273 页。

注册管理中心以进行智能许可

您可以通过互联网将管理中心直接注册到智能软件管理器，或者在使用气隙网络时，使用本地智能软件管理器注册。

将管理中心注册到智能软件管理器

将管理中心注册到智能软件管理器。

开始之前

- 请确保智能许可帐户包含所需的可用许可证。

  当您从 Cisco 或经销商那里购买设备时，您的许可证应该已链接到您的智能帐户。但是，如果您需要自己添加许可证，请参阅 Cisco 商务工作空间。有关许可证 PID，请参阅 许可证 PID，第 250 页。

- 确保 管理中心 可以在 smartreceiver.cisco.com 上到达智能软件管理器。
- 确保配置 NTP。在注册过程中，密钥交换发生在智能代理和智能软件管理器之间，因此时间必须同步才能正确注册。

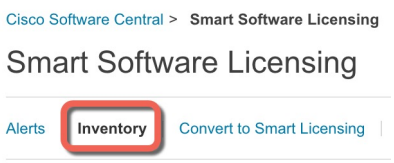
  对于 Firepower 4100/9300，必须使用与 管理中心相同的机箱 NTP 服务器在机箱上配置 NTP。

- 如果您的阻止有多个 管理中心，请确保每个 管理中心 拥有唯一的名称，以与可能注册到同一虚拟账户的其他管理中心进行区分。此名称对于管理智能许可证授权至关重要，而使用模糊名称稍后会出现问题。

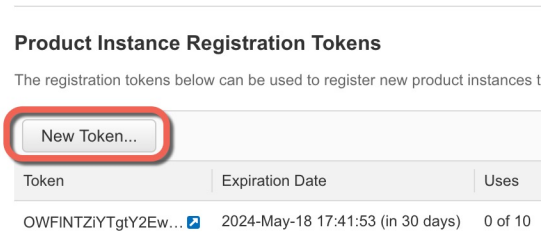
过程

步骤 1 在 智能软件管理器 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

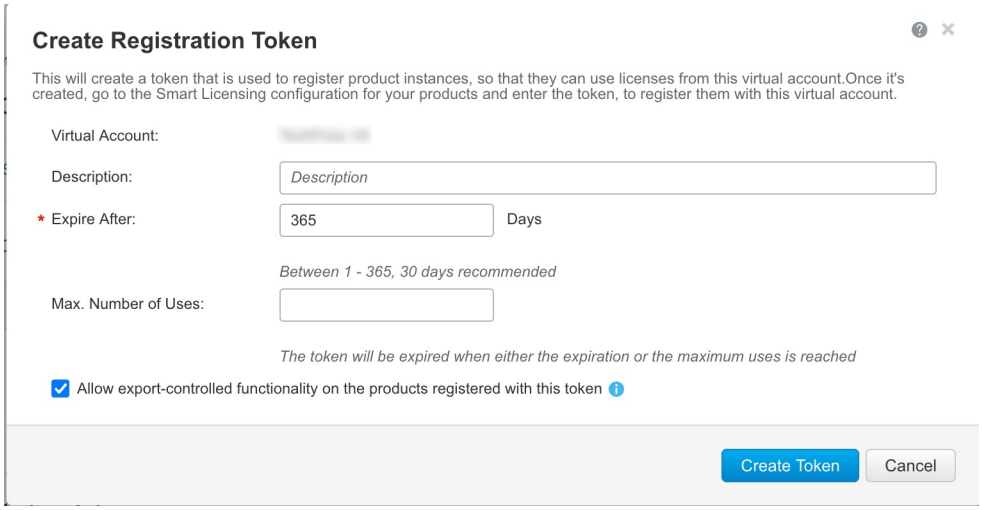
a) 点击**清单 (Inventory)**。



b) 在 **General** 选项卡上，点击 **New Token**。



c) 在 **Create Registration Token** 对话框中，输入以下设置，然后点击 **Create Token**：



- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- **最大使用次数**
- **在使用此令牌注册的产品上允许导出控制的功能 (Allow export-controlled functionaility on the products registered with this token** — 在您所在的国家/地区允许进行强加密的情况下启用导出合规性标志。如果打算使用此功能，则须立即选择该选项。如果稍后启用此功能，则需要使用新产品密钥重新注册设备并重新加载设备。如果您没有看到此选项，则您的帐户不支持出口控制功能。

系统将令牌添加到您的清单中。

d) 点击令牌右侧的箭头图标可以打开 **Token** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册威胁防御时，请准备好此令牌，以在该程序后面的部分使用。

图 *16:* 查看令牌

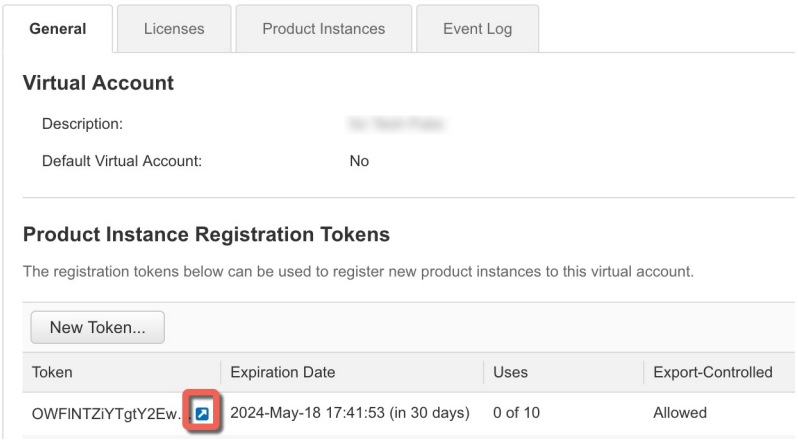
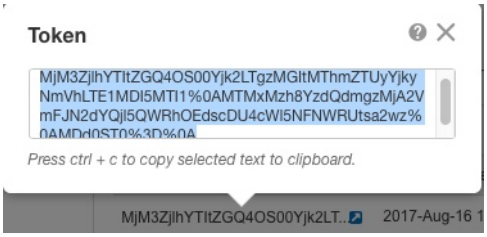


图 *17:* 复制令牌



步骤 2 在 管理中心上，选择 **系统**（⚙）> **许可证** > **智能许可证**。

步骤 3 点击**注册 (Register)**。

步骤 4 将您从 智能软件管理器 生成的令牌粘贴到 **产品实例注册令牌** 字段中。

确保文本开头和结尾处没有空格或空行。

步骤 5 如果管理中心实例已向智能许可注册，您可以选中 **覆盖现有注册管理中心实例** 复选框以覆盖智能许可中的现有注册管理中心实例。

步骤 6 决定是否向思科发送使用数据。

- **启用 Cisco Success Network** 默认处于启用状态。您可以点击**示例数据**了解思科收集的数据类型。有关详细信息，请参阅配置 Cisco Success Network 注册 ， 第 602 页。
- 默认情况下，**启用思科支持诊断** 被禁用。您可以在复选框上方提供的链接中查看 Cisco 收集的数据类型。有关详细信息，请参阅配置思科支持诊断注册 ， 第 603 页。

  注释
  - 启用后，将在下一个同步周期中在设备中启用 Cisco 支持诊断。 管理中心 与设备的同步每 30 分钟运行一次。
  - 启用后，在 管理中心注册的任何新设备都将自动启用 Cisco 支持诊断。

步骤 7 点击 **Apply Changes**（应用更改）。

下一步做什么

- 将设备添加到 管理中心；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 将设备添加到 管理中心 。
- 将许可证分配到您的设备；请参阅 将许可证分配给多个受管设备 ， 第 268 页。

将管理中心注册到本地智能软件管理器

如与智能软件管理器的定期通信 ， 第 240 页中所述，管理中心必须与 Cisco 定期通信，以维护许可证授权。如果出现以下情况之一，您便可能希望将智能软件管理器本地版（之前称为智能软件卫星服务器）用作代理服务器，以供连接到智能软件管理器：

- 管理中心为离线状态、连接受限或无连接（即部署于气隙网络中）。

  （有关气隙网络的替代解决方案，请参阅气隙部署的许可选项 ， 第 240 页。）

- 管理中心具备永久连接，但您希望通过网络中的单个连接管理智能许可证。

智能软件管理器本地版允许您安排同步或手动将智能许可证授权与智能软件管理器同步。

有关 智能软件管理器本地版 的详细信息，请参阅https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem。

过程

步骤 1 部署和设置。智能软件管理器本地版

- 请参阅智能软件管理器本地版的文档，可从https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem获取。
- 在您的智能软件管理器本地版记下 TLS/SSL 证书的 CN。
- 转至 http://www.cisco.com/security/pki/certs/clrca.cer，并将完整的 TLS/SSL 证书正文 （从“-----BEGIN CERTIFICATE-----”到“-----END CERTIFICATE-----”）复制到您在配置期间可访问的某个位置。

步骤 2 将 管理中心注册到 智能软件管理器本地版。

a) 选择**集成** > **其他集成**。
b) 点击**智能软件卫星 (Smart Software Satellite)**。
c) 选择**连接到思科智能软件卫星服务器**。
d) 使用您在此过程的前提条件中收集的CN值，按以下格式输入智能软件管理器本地版的**URL**：

   `https://FQDN_or_hostname_of_your_SSM_On-Prem/SmartTransport`

   FQDN 或主机名必须与您智能软件管理器本地版提供的证书的 CN 值匹配。

e) 添加新 **SSL 证书**，并粘贴您之前复制的证书文本。
f) 点击 **Apply**。
g) 依次选择**系统 > 许可证 > 智能许可证**，然后点击**注册**。
h) 创建新的智能软件管理器本地版令牌。
i) 复制该令牌。
j) 将该令牌粘贴到管理中心页面上的表中。
k) 点击 **Apply Changes**（**应用更改**）。

管理中心现已注册到智能软件管理器本地版。

步骤 3 将许可证分配给设备后，同步智能软件管理器本地版到智能软件管理器。

请参阅上面的智能软件管理器本地版文档。

步骤 4 安排日常同步次数。

对于无全局权限的账户启用出口控制功能

如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。

开始之前

- 确保部署尚**不**支持出口控制功能。

  如果您的部署支持出口管制功能，您将看到一个选项，您可以启用在**创建注册令牌**页中智能软件管理器出口控制功能。有关详细信息，请参阅https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html。

- 确保部署未在使用评估许可证。
- 在智能软件管理器 (Smart Software Manager) 中，转至 **清单 (Inventory)** > **许可证 (Licenses)**页面，确认拥有与 管理中心对应的许可证：

出口控制许可证	管理中心 型号
思科虚拟 FMC 系列强加密 (3DES/AES)	所有 management center virtual
思科 FMC 1K 系列强加密 (3DES/AES)	_ _
思科 FMC 2K 系列强加密 (3DES/AES)	__
思科 FMC 4K 系列强加密 (3DES/AES)	__

过程

步骤 1 选择**系统** > **许可证** > **智能许可证**。

注释 如果显示 **请求导出密钥**，则表示账户获准使用出口控制功能，您可继续使用所需功能。

步骤 2 点击**请求导出密钥**以生成导出密钥。

提示 如果出口控制密钥请求失败，则请确保虚拟账户具备有效的出口控制许可证。

通过点击 **恢复导出密钥**来禁用该出口控制许可证。

下一步做什么

您现在即可部署使用出口控制功能的配置或策略。

记住 在 威胁防御设备重启之前，由此功能启用的新出口控制许可证和所有功能将不会在这些设备上生效。在此之前，只有受以往许可证支持的功能有效。

在高可用性部署中，需要同时启动 威胁防御 设备以避免出现主主状态。

将许可证分配到设备

将设备注册到 管理中心时，可以分配大多数许可证。您还可以为每台设备或为多台设备分配许可证。

将许可证分配给单个设备

尽管有一些例外，但如果在受管设备上禁用许可证，就无法使用与该许可证关联的功能。

注释 对于同一 安全模块/引擎上的容器实例，您将对每个实例应用许可证；请注意，对于 安全模块/引擎上的所有实例，安全模块/引擎仅对每个功能占用一个许可证。

注释 对于威胁防御集群，您将对整个集群应用许可证；请注意，集群中的每个设备将对每个功能占用单独的许可证。

开始之前

您必须具有管理员或网络管理员权限才能执行此任务。使用多个域时，必须在分叶域中执行此任务。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要分配或禁用许可证的设备旁边，点击 **编辑**（）。

步骤 3 点击 **设备**。

步骤 4 点击 **许可证** 部分旁边的 **编辑**（）。

步骤 5 选中或清除相应的复选框，以便为设备分配或禁用许可证。

步骤 6 点击**保存 (Save)**。

步骤 7 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

下一步做什么

验证许可证状态：转至 **系统**（）> **许可证** > **智能许可证**，将设备的主机名或 IP 地址输入“智能许可证”表顶部的过滤器中，验证每个许可证类型是否仅对每个设备显示一个带有 **复选标记**（）的绿色圆圈 。如有任何其他图标，则将鼠标悬停在图标上查看详细信息。

将许可证分配给多个受管设备

受 管理中心 管理的设备通过 管理中心获取许可证，而非直接通过智能软件管理器获取。

使用本程序在多个设备上启用许可。

注释 对于同一 安全模块/引擎上的容器实例，您将对每个实例应用许可证；请注意，对于 安全模块/引擎上的所有实例，安全模块/引擎仅对每个功能占用一个许可证。

注释 对于威胁防御集群，您将对整个集群应用许可证；请注意，集群中的每个设备将对每个功能占用单独的许可证。

过程

步骤 1 选择**系统**（）> **许可证** > **智能许可证**或**特定许可证**。

步骤 2 点击**编辑许可证**。

步骤 3 对于想要添加到设备的每种类型的许可证：

a) 点击该类型许可证的选项卡。

b) 点击左侧列表中的设备。

c) 点击**添加**将该设备移至右侧列表。

d) 为每个设备重复此操作以接收该类型的许可证。

现在无需再担心是否拥有想要添加的所有设备的许可证。

e) 为想要添加的每种类型许可证重复此子程序。

f) 要删除许可证，请点击设备旁边的 **删除**（ ）。

g) 点击**应用**。

您可以选择集群并将任何许可证分配给集群的所有节点。

下一步做什么

验证许可证是否已正确安装。请按照监控智能许可证，第 270 页中的程序操作。

管理智能许可

本部分介绍如何管理智能软件许可。

取消注册 管理中心

从智能软件管理器中取消注册您的管理中心，以将所有许可证授权释放回您的智能帐户，以便可用于其他设备。例如，如果需要停用管理中心或重新映像，请取消注册。

有关在未注册状态下执行许可证的详细信息，请参阅已注销状态，第 241 页。

过程

步骤 1 选择**系统**（ ）> **许可证** > **智能许可证**。

步骤 2 请点击 **取消注册**（ ）。

同步或重新授权 管理中心

默认情况下，ID 证书每 6 个月自动更新，许可证授权每 30 天更新。如果您访问互联网的时间有限，或者例如在智能软件管理器中进行了任何许可更改，则可能需要为其中任一项手动续约注册。

过程

步骤 1 选择**系统**（ ）> **许可证** > **智能许可证**。

步骤 2 要更新 ID 证书，请点击 **同步**（ ）

步骤 3 要更新许可证授权，请点击 **重新授权**。

监控智能许可状态

系统 > 许可证 > 智能许可证 页面的 **智能许可证状态** 部分提供 管理中心上许可证使用情况的概览，如下所述。

使用授权

可能的状态值包括：

- **不合规** （  ） - 分配到受管设备的所有许可证均合规，并且 管理中心 与思科许可证颁发机构通信成功。
- **许可证符合规定，但与许可证授权机构的通信失败** - 设备许可证合规，但 管理中心 无法与思科许可证颁发机构通信。
- **不合规图标或无法与许可证颁发机构通信**- 一个或多个受管设备使用的许可证不合规，或 管理中心 已有超过 90 天未与思科许可证颁发机构通信。

产品注册

指定 管理中心 联系智能软件管理器并向其注册的最后日期。

分配的虚拟帐户

指定用于生成产品实例注册令牌和注册 管理中心的智能账户下的虚拟账户。如果此部署未关联智能账户内的某个特定虚拟账户，则不会显示此信息。

出口管制功能

如果启用此选项，则可部署受限制的功能。有关详细信息，请参阅出口控制功能的许可，第 248 页。

Cisco Success Network

指定是否为 管理中心启用了 Cisco Success Network。如果启用此选项，您可以向思科提供使用情况信息和统计数据，这些信息对为您提供技术支持非常重要。通过此信息，思科还可以改进产品，并使您获悉未使用的可用功能，以便您能够在网络中将产品的价值最大化。有关详细信息，请参阅配置 Cisco Success Network 注册，第 602 页。

监控智能许可证

要查看 管理中心 及其管理设备的许可证状态，请使用智能许可证页面。

对于部署中每种类型的许可证，该页面都会列出使用的许可证总数、许可证是合规还是不合规、设备类型以及设备部署所在的域和组。您还可以查看 管理中心的智能许可证状态。在同一 安全模块/引擎 上的容器实例仅会为每个 安全模块/引擎使用一个许可证。因此，即使 管理中心 在每个许可证类型下单独列出每个容器实例，功能许可证类型占用的许可证数量也将为一。

除了 **智能许可证** 页面之外，还有其他一些方法可用于查看许可证：

- **产品许可** 控制面板构件提供了许可证概览。

请参阅将构件添加到控制面板，第 335 页和按用户角色划分的控制面板构件可用性，第 323 页和产品许可构件，第 332 页。

- **设备管理** 页面 （**设备** > **设备管理**）列出应用于每个受管设备的许可证。
- **智能许可证监控** 运行状况模块在运行状况策略中使用时传达许可证状态。

过程

步骤 1 选择**系统**（⚙）> **许可证** > **智能许可证**。

步骤 2 在**智能许可证**表中，点击每个**许可证类型**文件夹左侧的箭头以展开该文件夹。

步骤 3 在每个文件夹中，验证 **许可证状态** 列中每个设备是否有具有 **复选标记**（✓） 的绿色圆圈 。

注释 如果您看到重复的 management center virtual 许可证，则每个许可证都代表一个受管设备。

如果每个设备都显示带 **复选标记**（✓）的绿色圆圈，则表示设备已正确许可并可供使用。

如果未显示带 **复选标记**（✓）的绿色圆圈，请将鼠标悬停在状态图标上以查看消息。

下一步做什么

- 如果存在不带 **复选标记**（✓）的绿色圆圈的任何设备，则可能需要购买更多许可证。

智能许可疑难解答

我的智能账户中没有显示预期许可证

如果期望看到的许可证未出现在您的智能账户中，则请尝试以下操作：

- 确保许可证不在其他虚拟账户中。您的组织的许可证管理员也许可以给予协助。
- 联系您的许可证销售者，确定许可证已转移到您的账户中。

无法连接到智能许可证服务器

首先检查明显的原因。例如，确保您的 管理中心 具有外部连接。请参阅互联网接入要求，第 1014 页。

意外出现不合规通知或其他错误

- 如果设备已向其他管理中心注册，则需要先取消注册原始管理中心，然后才能在新的管理中心下许可该设备。请参阅取消注册 管理中心，第 269 页。
- 检查订用许可证的期限是否已到期。

排除其他问题

有关其他常见问题的解决方案，请参阅 https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215838-fmc-and-ftd-smart-license-registration-a.html

转换经典许可证以在 威胁防御上使用

您可以使用许可证注册门户或智能软件管理器转换许可证，并且可以转换已分配到某个设备的未使用产品授权密钥 (PAK) 或经典许可证。

注释 您无法撤销此过程。即使某个智能许可证原为经典许可证，您也无法将其转换为经典许可证。

在 Cisco.com 上的文档中，经典许可证也称为“传统”许可证。

开始之前

- 当经典许可证仍为尚未分配到产品实例的未使用 PAK 时，将其转换为智能许可证最为简单。
- 您的硬件必须能够运行 威胁防御。请参阅 https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html 上的《思科 *Firepower* 兼容性指南。
- 您必须拥有智能账户。如果没有，请创建一个。请参阅创建智能账户并添加许可证，第 260 页。
- 智能账户中必须显示要转换的 PAK 或许可证。
- 如果使用许可证注册门户而非智能软件管理器进行转换，则必须拥有智能账户凭证才能发起转换过程。

过程

步骤 1 您将执行的转换过程取决于许可证是否已被占用：

- 如果要转换的 PAK 从未被使用，请按照说明转换 PAK。
- 如果要转换的 PAK 已分配到某个设备，请按照说明转换经典许可证。

  请确保现有的经典许可证仍向设备注册。

步骤 2 请参阅以下文档中适用于您的转换类型（PAK 或已安装的经典许可证）的说明进行操作：

- 要使用许可证注册门户转换 PAK 或许可证：
  - 要查看通过许可证注册门户进行转换的操作步骤，请点击 https://salesconnect.cisco.com/#/content-detail/7da52358-0fc1-4d85-8920-14a1b7721780。
  - 在以下文档中搜索“转换”：https://cisco.app.box.com/s/mds3ab3fctk6pzonq5meukvcpjizt7wu。

    有三个转换程序。选择适用于您的转换程序。

- 在 https://tools.cisco.com/SWIFT/LicensingUI/Home 上登录到许可证注册门户 (LRP)，然后按照上述文档中的说明进行操作。

- 要使用智能软件管理器转换 PAK 或许可证，请执行以下操作：
  - 《混合许可证转换智能软件许可证快速参考指南》：

    https://community.cisco.com/t5/licensing-enterprise-agreements/converting-hybrid-licenses-to-smart-software-licenses-qrg/ta-p/3628609?attachment-id=134907
  - 在 https://software.cisco.com/#SmartLicensing-LicenseConversion 上登录智能软件管理器，按照上述文档中适用于您的转换类型（PAK 或已安装的经典许可证）的说明进行操作。

步骤 3 在硬件上全新安装 威胁防御。

访问 https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html 查看硬件说明。

步骤 4 如果要使用 设备管理器 将此设备作为独立设备进行管理：

有关 设备管理器 配置指南中的设备许可信息，请参阅 https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html。

跳过此程序的其余步骤。

步骤 5 如果已在 管理中心上部署智能许可：

a) 在新的 威胁防御设备上设置智能许可。

请参阅将许可证分配给多个受管设备，第 268 页。

b) 验证新的智能许可证是否已成功应用到该设备。

请参阅监控智能许可证，第 270 页。

步骤 6 如果尚未在 管理中心上部署智能许可：

请参阅配置智能许可，第 262 页。（请跳过不适用或已完成的任何步骤。）

配置特定许可证预留 (SLR)

您可以使用特定许可证预留功能在气隙网络中部署智能许可。

注释 思科对特定许可证预留使用了各种名称，包括 SLR、SPLR、PLR 和永久许可证预留。思科也可能使用这些术语来指代类似但不一定相同的许可模式。

特定许可证预留启用时，管理中心会在指定的持续时间内预留来自虚拟账户的许可证，而无需访问智能软件管理器或使用 智能软件管理器本地版。

需要接入互联网的功能（例如对公共网站的 URL 查找或上下文交叉启动）将无法工作。

思科不会收集使用特定许可证预留的部署的网络分析或遥测数据。

特定许可证预留的要求和前提条件

- 如果当前使用常规智能许可，请在实施特定许可证预留之前注销管理中心。有关信息，请参阅取消注册 管理中心，第 269 页。

  当前部署到管理中心的所有智能许可证将返回账户的可用许可证池中，在实施特定许可证预留时即可重用它们。

- 特定许可证预留需要与标准智能许可相同数量和类型的许可证。
- （推荐）如果在高可用性配置中部署 管理中心 对，请注意以下事项：
  - 在分配许可证之前配置高可用性。如果您已将许可证分配给辅助 管理中心上的设备，请务必取消分配。
  - 如果将 SLR 许可证分配给主设备 管理中心，则当辅助设备 管理中心 在故障转移后变为主用设备时，您无法将 SLR 许可证添加到辅助设备 管理中心。您必须执行以下操作之一：
    - 执行故障转移，使主 管理中心 处于活动状态。
    - 取消分配并将许可证重新分配给辅助 管理中心。

验证您的智能账户是否已准备好部署特定许可证预留

为防止部署特定许可证预留时发生问题，请先完成本程序，再在 管理中心中进行任何更改。

开始之前

- 确保已满足特定许可证预留的要求和前提条件，第 274 页中的要求。
- 确保拥有智能软件管理器凭证。

过程

步骤 1 登录到智能软件管理器：

https://software.cisco.com/#SmartLicensing-Inventory

步骤 2 如果适用，请从页面右上角选择正确的账户。

步骤 3 如有必要，请点击**清单 (Inventory)**。

步骤 4 点击 **许可证**。

步骤 5 请验证以下项目：

- 显示**许可证预留**按钮。
- 对于将要部署的设备和功能，有足够的平台和功能许可证可供使用，包括设备的 management center virtual 授权（如适用）。

步骤 6 如果其中有任何项目缺失或有误，请联系您的客户代表来解决问题。

注释 在解决所有问题之前，请勿继续此过程。

启用特定许可菜单选项

本程序会将 管理中心中的“智能许可证”菜单选项更改为“特定许可证”。

过程

步骤 1 使用 USB 键盘和 VGA 显示器访问 管理中心 ，或使用 SSH 访问管理界面。

步骤 2 登录 管理中心 CLI **管理员** 账户。

步骤 3 输入 **expert** 命令以访问 Linux 外壳。

步骤 4 执行以下命令以访问特定许可证预留选项：

sudo manage_slr.pl

示例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

步骤 5 选择选项 **2**即可启用特定许可证预留。

步骤 6 选择选项 **0** 退出 manage_slr 实用程序。

步骤 7 键入 **exit** 退出 Linux 外壳。

步骤 8 输入 **exit** 退出命令行接口。

步骤 9 验证是否可以在 管理中心 Web 界面中访问**特定许可证预留**页面：

- 如果当前显示 **系统** > **许可证** > **智能许可证** 页面，则请刷新页面。

- 否则，请选择 **系统** > **许可证** > **特定许可证**。

将特定许可证预留授权码输入 管理中心

过程

步骤 1 生成预留申请代码。

a) 在 管理中心，请选择 **系统** > **许可证** > **特定许可证**。
b) 点击**生成 (Generate)**。
c) 记下**预留申请代码**。

步骤 2 生成预留授权码。

a) 转至思科智能软件管理器： https://software.cisco.com/#SmartLicensing-Inventory
b) 如有必要，请从页面右上角选择正确的账户。
c) 如有必要，请点击**清单 (Inventory)**。
d) 点击 **许可证**。
e) 点击**许可证预留 (License Reservation)**。
f) 将从 管理中心 生成的代码输入**预留申请代码**框中。
g) 点击**下一步**。
h) 选择**预留特定许可证**。
i) 向下滚动以显示整个许可证网格。
j) 在**预留数量**下，输入部署所需的每个平台和功能的许可证数量。

注释
- 您必须为每个受管设备明确包含一个 基础版 许可证，对于多实例部署，必须为每个容器明确包含一个基础许可证。
- 如果您使用 management center virtual，则必须对每个模块（多实例部署）或每个托管设备（所有其他部署）包括一个平台授权。
- 如果使用强加密功能：
  - 如果您的整个智能账户已启用出口控制功能，则无须在此进行任何操作。
  - 如果您所在组织的授权为“每管理中心 ”，则您必须选择适当的许可证。

  要为 管理中心选择正确的许可证名称，请参阅 对于无全局权限的账户启用出口控制功能 ， 第 266 页中所述的前提条件。

k) 点击**下一步**。
l) 点击**生成授权码**。

根据智能软件管理器，许可证现已处于使用状态。

m) 下载授权码，准备将其输入 管理中心。

步骤 3 在 管理中心中输入授权码。

a) 在 管理中心中，点击 **浏览** 以上传包含从智能软件管理器生成的授权码的文本文件。

b) 点击**安装 (Install)**。

c) 验证**特定许可证预留**页面上的**使用授权**是否显示为“已授权”状态。

d)

步骤 4 点击**预留许可证**选项卡以验证在生成**授权码**时所选择的许可证。

如果没有看到所需的许可证，请添加必要的许可证。有关详细信息，请参阅更新特定许可证预留。

将特定许可证分配给受管设备

使用本程序将许可证一次性地快速分配到多个受管设备。

您还可以使用本程序禁用许可证，或在设备之间移动许可证。如果您禁用设备的许可证，则不能在设备上使用与该许可证相关的功能。

过程

步骤 1 选择**系统** > **许可证** > **特定许可证**。

步骤 2 点击**编辑许可证**。

步骤 3 根据需要点击每个选项卡并将许可证分配到设备。

步骤 4 点击**应用**。

步骤 5 点击**已分配许可证**选项卡，验证许可证是否已正确安装在每个设备上。

步骤 6 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

管理特定许可证预留

本节介绍如何管理特定许可证预留。

重要提示！维护特定许可证预留部署

要更新使部署保持有效的威胁数据和软件，请参阅维护气隙部署，第 225 页。

要确保所有功能继续工作而不发生中断，请监控许可证的到期日期（位于**预留的许可证**选项卡）。如果任何许可证到期，且使用计数大于可用计数，则 管理中心 将处于不合规状态。

更新特定许可证预留

在特定许可证成功部署在 管理中心之后，即可使用本程序随时添加或删除授权。

如果您需要在许可证到期后续约，请使用此程序。如果您没有所需的许可证，则以下操作会受到限制：

- 设备注册
- 策略部署

过程

步骤 1 在 管理中心中，获取此 管理中心的唯一产品实例标识符：

a) 选择 **系统** > **许可证** > **特定许可证**。

b) 记下**产品实例**的值。

您将在此过程期间多次使用此值。

步骤 2 在智能软件管理器中，确定要升级的 管理中心 ：

a) 转至智能软件管理器：

https://software.cisco.com/#SmartLicensing-Inventory

b) 如有必要，请点击**清单**。

c) 点击 **产品实例**。

d) 在**类型**列中查找带有**FP**字样的产品实例，并在**名称**列中查找通用SKU（非主机名）。您也可以借助其他表列中的值来确定 管理中心 是正确的 管理中心。点击名称。

e) 查看 **UUID** ，看看它是否是您尝试修改的 管理中心 的 UUID。

如果不是，则必须重复这些步骤，直至找到正确的 管理中心。

步骤 3 在思科智能软件管理器中找到正确的 管理中心 后，即可更新预留许可证并生成新的授权码：

a) 在显示正确 UUID 的页面上，选择 **操作** > **更新预留许可证**。

b) 根据需要更新预留许可证。

注释

- 您必须为每个受管设备明确包含一个 基础版 许可证，对于多实例部署，必须为每个容器明确包含一个基础许可证。
- 如果您使用 management center virtual，则必须对每个模块（多实例部署）或每个托管设备（所有其他部署）包括一个平台授权。
- 如果使用强加密功能：
  - 如果您的整个智能账户已启用出口控制功能，则无须在此进行任何操作。
  - 如果您所在组织的授权为“每管理中心 ”，则您必须选择适当的许可证。

  要为 管理中心选择正确的许可证名称，请参阅 对于无全局权限的账户启用出口控制功能， 第 266 页中所述的前提条件。

c) 点击**下一步**并验证详细信息。

d) 点击**生成授权码**。
e) 下载授权码，准备将其输入 管理中心。
f) 保持 **更新预留** 页面处于打开状态。稍后您将在本程序中返回此页面。

步骤 4 更新 管理中心中的特定许可证。

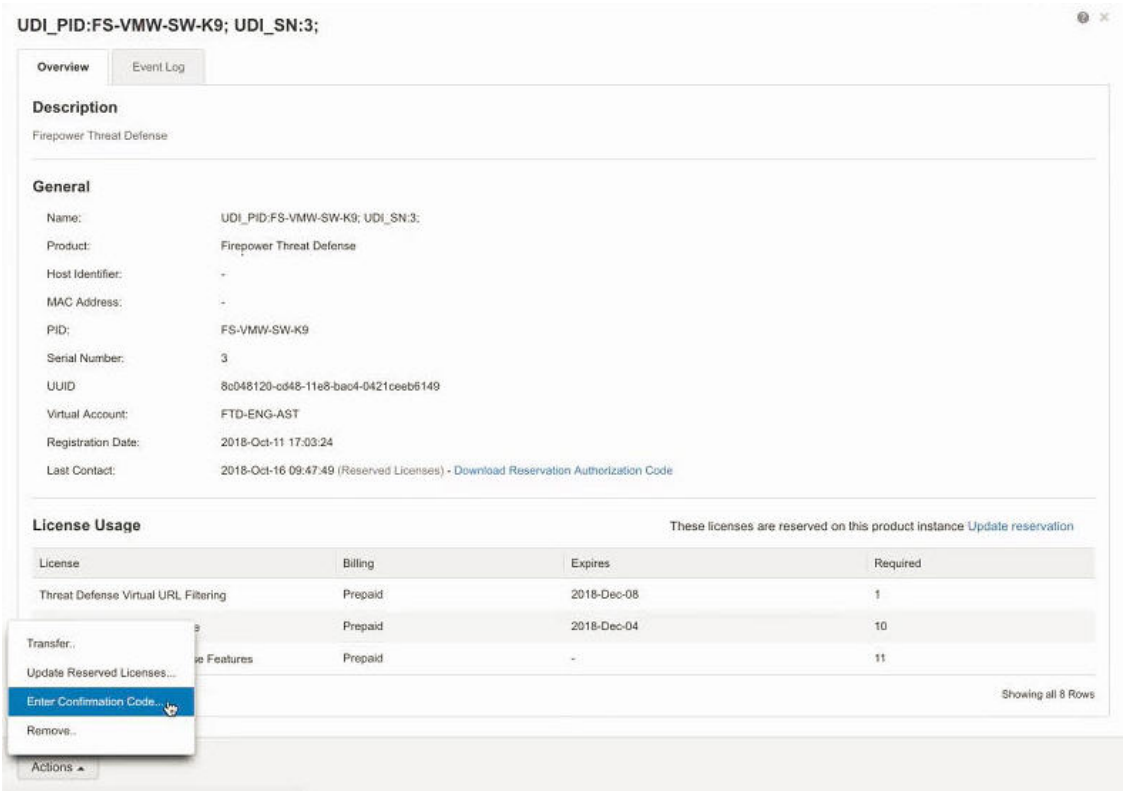
a) 选择 **系统** > **许可证** > **特定许可证**。
b) 点击**编辑 SLR**。
c) 点击**浏览**以上传新生成的授权码。
d) 点击**安装**以更新许可证。

成功安装授权码后，请确保 管理中心 **预留** 列中显示的许可证与您在思科智能软件管理器中预留的许可证相匹配。

e) 记下**确认代码**。

步骤 5 在智能软件管理器中输入确认代码：

a) 返回之前在本程序中保持打开状态的智能软件管理器页面。
b) 选择 **操作** > **输入确认代码**：



c) 输入从 管理中心生成的确认代码。

步骤 6 在 管理中心中，确认许可证已按照预期予以预留，并且每个受管设备的每个功能均显示带有选中标记 **复选标记**（ ）的绿色圆圈。

如有需要，请参阅监控特定许可证预留状态，第 282 页了解详细信息。

步骤 7 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

停用并归还特定许可证预留

如果不再需要某个特定许可证，则必须将其归还至智能账户。如果要注册智能许可帐户，必须禁用特定许可证预留（以下程序的步骤 6）。

重要事项 如果不按本程序中的步骤进行操作，则许可证仍会处于使用中的状态，无法重用。

此程序将与 管理中心关联的所有许可证授权将释放回虚拟账户。注销之后，即不允许对许可的功能进行更新或更改。

过程

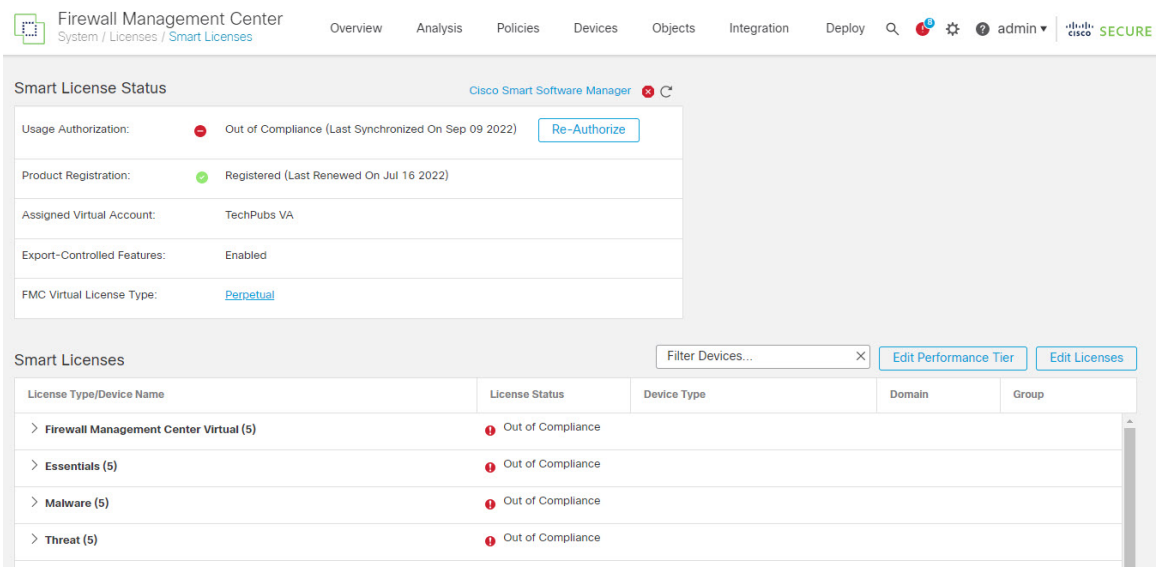
步骤 1 在 管理中心 Web 界面中，选择 **系统** > **许可证** > **特定许可证**。

步骤 2 记下此 管理中心**产品实例**的标识符。

步骤 3 从 管理中心生成返还代码，

a) 点击 **返还 SLR**。

下图显示返还 SLR。



设备变为未经许可， 管理中心 进入取消注册状态。

b) 记下**归还代码**。

步骤 4 在智能软件管理器中，确定要取消注册的 管理中心 ：

a) 转至智能软件管理器：

https://software.cisco.com/#SmartLicensing-Inventory

b) 如有必要，请点击**清单**。
c) 点击 **产品实例**。
d) 在**类型**列中查找带有**FP**字样的产品实例，并在**名称**列中查找通用SKU（非主机名）。您也可以借助其他表列中的值来确定 管理中心 是正确的 管理中心。点击名称。
e) 查看 **UUID** ，看看它是否是您尝试修改的 管理中心 的 UUID。

如果不是，则必须重复这些步骤，直至找到正确的 管理中心。

步骤 5 在确定正确的 管理中心之后，将许可证归还至智能账户：

a) 在显示正确 UUID 的页面上，选择 **操作** > **删除**。
b) 将从 管理中心 生成的预留归还代码输入 **删除产品实例** 对话框。
c) 点击 **Remove Product Instance**。

特定预留许可证会返回智能账户中的可用池中，而 管理中心 也会从智能软件管理器产品实例列表中删除。

步骤 6 在 管理中心 Linux 外壳中禁用特定许可证：

a) 使用 USB 键盘和 VGA 显示器访问 管理中心 ，或使用 SSH 访问管理界面。
b) 登录 管理中心 CLI **管理员** 账户。这使您可以访问命令行接口。
c) 输入 **expert** 命令以访问 Linux 外壳。
d) 执行以下命令：

sudo manage_slr.pl

示例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

e) 选择菜单选项 **3** 以禁用特定许可证预留。
f) 选择选项 **0** 退出 manage_slr 实用程序。
g) 输入 **exit** 以退出 Linux 外壳。
h) 输入 **exit** 退出命令行接口。

监控特定许可证预留状态

系统 > **许可证** > **特定许可证** 页面提供 管理中心上许可证使用情况的概览，如下所述。

使用授权

可能的状态值包括：

- **已授权** - 管理中心 符合许可证颁发机构的要求并成功向其注册，该机构已向设备授予许可证授权。
- **不合规** - 如果许可证到期，或者 管理中心 过度使用许可证（即使它们未被预留），则状态会显示为“不合规”。许可证授权会在特定许可证预留中予以实施，因此必须采取措施。

产品注册

指定授权码上一次在 管理中心上安装或续订时的注册状态和日期。

出口管制功能

指定是否已为 管理中心启用出口控制功能。

有关出口控制功能的详细信息，请参阅出口控制功能的许可 ， 第 248 页。

产品实例

此 管理中心的通用唯一标识符 (UUID)。此值用于在智能软件管理器中标识此设备。

确认代码

如果更新或停用并归还特定许可证，则需要**确认代码**。

“分配的许可证”选项卡

显示分配到每个设备的许可证及其状态。

“预留的许可证”选项卡

显示已使用和可分配的许可证数量，以及许可证到期日期。

特定许可证预留疑难解答

如何在智能软件管理器的产品实例列表中确认某个特定的 管理中心 ？

在智能软件管理器的产品实例页面上，如果无法基于表格其中一列中的某个值确认产品实例，则必须点击类型为 **FP** 的每个通用产品实例的名称，以查看产品实例的详细信息页面。此页面上的 **UUID** 值为某个 管理中心的唯一标识。

在 管理中心 Web 接口中，某个 管理中心 的 UUID 为 **系统** > **许可证** > **特定许可证** 页面上显示的 **产品实例** 值。

我没有在智能软件管理器中看到许可证预留按钮

如果未看到 **许可证预留** 按钮，则表示您的账户无权使用特定许可证预留。如果已在 Linux 外壳中启用特定许可证预留，并已生成请求代码，请执行以下操作：

1. 如果已在 管理中心 Web 界面中生成 **请求代码** ，请取消该请求代码。
2. 在 管理中心 Linux 外壳中禁用特定许可证预留，如 停用并归还特定许可证预留 ， 第 280 页部分所述。
3. 使用智能令牌在常规模式下通过思科智能软件管理器注册 管理中心 。
4. 请联系思科 TAC 为您的智能账户启用特定许可证。

我的许可过程被中断了。如何从中断处继续？

如果已从智能软件管理器生成授权码但尚未下载该授权码，可转至智能软件管理器中的**产品实例**页面，点击产品实例，然后点击 **下载预留授权码**。

我无法将设备注册到 management center virtual

请在智能账户中确保对想要注册的设备具有足够的 management center virtual 授权，然后更新部署以添加所需授权。

请参阅更新特定许可证预留 ， 第 277 页。

我已启用特定许可，但看不到智能许可证页面。

这是预期行为。在启用特定许可时，智能许可为禁用状态。您可以使用特定许可证页面来执行许可操作。

如果想要使用智能许可，则必须归还特定许可证。有关详细信息，请参阅停用并归还特定许可证预留 ， 第 280 页。

如果无法在 management center virtual中看到特定许可证页面怎么办？

您需要启用特定许可证才能查看特定许可证页面。有关详细信息，请参阅启用特定许可菜单选项 ， 第 275 页。

我已禁用特定许可，但忘记复制归还代码。应该怎么办？

返回代码 保存在 management center virtual中。您必须从外壳重新启用特定许可证（请参阅 启用特定许可菜单选项 ， 第 275 页），然后刷新 management center virtual Web 界面。系统将显示**归还代码**。

配置管理中心基于 PAK 的旧版许可证

管理中心 支持智能许可证或传统 PAK（产品激活密钥）许可证作为其平台许可证。此程序介绍如何应用基于 PAK 的许可证。

重新注册智能账户后，您必须为所有经典设备手动添加经典许可证。

开始之前

- 请确保您有思科在您购买许可证时提供的软件索赔证书中的产品激活秘钥(PAK)。如果有延迟，请在获取思科许可证之前联系支持部门。

过程

步骤 1 许可证密钥在智能软件管理器中唯一标识管理中心。它由管理中心的产品代码（例如66）和管理端口 (eth0) 的 MAC 地址组成；例如，66:00:00:77:FF:CC:88。

a) 选择**系统**（⚙）> **许可证** > **经典许可证**。
b) 点击 **Add New License**。
c) 请记下**添加功能许可证 (Add Feature License)** 对话框顶部的**许可证密钥 (License Key)** 字段中的值。

步骤 2 选择**系统**（⚙）> **许可证** > **经典许可证**。

步骤 3 点击 **Add New License**。

步骤 4 根据情况继续操作：

- 如果您已经获取许可证文本，请跳至步骤 8。
- 如果您仍需要获取许可证文本，请跳至下一步骤。

步骤 5 点击 **获取许可证** ，打开许可证注册门户。

注释 如果无法使用当前的计算机访问互联网，请切换至可访问互联网的计算机，并浏览至 http://cisco.com/go/license。

步骤 6 从许可证注册门户中的 PAK 生成一个许可证： https://cisco.com/go/license。

此步骤需要您在购买过程中收到的 PAK 以及 管理中心的许可证密钥。

有关使用此门户的详细信息，请参阅：

https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart

您需要账户凭证才能访问这些链接。

步骤 7 复制许可证注册门户显示或许可证注册门户发送给您的邮件中的许可证文本。

重要事项 门户或邮件中的许可文本块可能包含多个许可证。每个许可证都由一个“开始许可证”行和一个“结束许可证”行来约束。请确保一次仅复制粘贴一个许可证。

步骤 8 返回 Management Center Virtual 的 Web 界面中的**添加功能许可证 (Add Feature License)** 页面。

步骤 9 将许可证文本粘贴到**许可证 (License)** 字段。

步骤 10 点击**验证许可证 (Verify License)**。

如果许可证无效，请确保您复制的许可证文本正确无误。

步骤 11 点击**提交许可证 (Submit License)**。

有关许可的其他信息

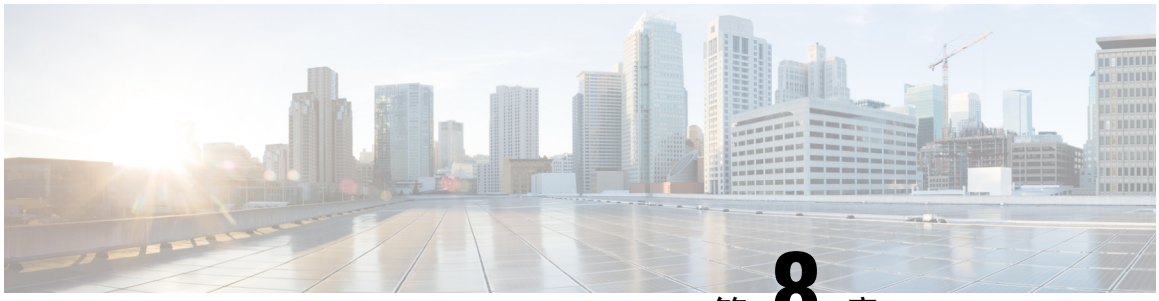
有关有助于解决许可问题的其他信息，请参阅以下文档：

- FAQ—https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-license-FAQ.html
- 许可证路线图 -https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html

许可证历史记录

功能	最低 管理中心	最低 威胁防御	详情
智能许可标准化	7.3	任意	我们在管理中心 GUI 中更改了以下许可证名称： • 基本现在更改为基础版 • 威胁现在更改为 IPS • 恶意软件现在更改为恶意软件防御 • RA VPN/AnyConnect 许可证现在是思科安全客户端 • AnyConnect Plus 现在更改为 Secure Client Advantage • AnyConnect Apex 现在更改为 Secure Client Premier • AnyConnect Apex 和 Plus 现在更改为安全客户端 Premier 和 Advantage • 仅限 AnyConnect VPN 现在更改为仅限 Secure Client VPN
支持运营商许可证	7.3	任意	运营商许可证支持对 Diameter、GTP/GPRS、SCTP 和 M3UA 协议的检测。 新增/修改的屏幕：**系统 (System)** > **智能许可证 (Smart Licenses)**
threat defense virtual智能许可的性能级别	7.0	任意	性能级许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。许可证级别映射到新 threat defense virtual 型号。

功能	最低 管理中心	最低 威胁防御	详情
Firepower 4100/9300 上威胁防御多实例功能的许可	6.3	任意	您现在可以在 Firepower 4100/9300 上部署多个 威胁防御 容器实例。每个安全模块/引擎每个功能只需要一个许可证。基础许可证会自动分配给每个实例。 新增/修改的屏幕： **系统** > **许可证** > **智能许可证** 支持的平台：Firepower 4100/9300 上的 威胁防御
气隙部署的特定许可证预留	6.3	任意	如果客户的部署无法连接互联网以与思科许可证颁发机构通信，则可以使用特定许可证预留。 新/修改后的屏幕： **系统**>**许可证**>**特定许可证**（此选项默认不可用。） 支持的平台：管理中心、威胁防御
受限客户的出口控制功能	6.3	任意	如果某些客户的智能账户没有资格使用受限功能，则在获得批准的情况下可以购买基于期限的许可证。 支持的平台：管理中心、威胁防御



第 8 章

高可用性

以下主题介绍如何配置思科 Cisco Secure Firewall Management Center的主用/备用高可用性：

关于管理中心高可用性

要确保操作的连续性，可通过高可用性功能指定冗余管理中心以管理设备。管理中心支持主用/备用高可用性，其中一个设备是主用设备并管理设备。备用设备不会主动管理设备。主用设备将配置数据写入数据存储区并复制两个设备的数据，在必要时会通过同步与备用设备共享一些信息。

主用/备用高可用性允许您配置辅助 管理中心，以便在主 管理中心发生故障时接管该设备的功能。当主 管理中心发生故障时，必须升级辅助 管理中心使其成为主用设备。

事件数据从受管设备流到高可用性对中的两个 管理中心。如果一个管理中心发生故障，可以使用另一个管理中心继续不间断地监控网络。

请注意，配置为高可用性对的管理中心既无需在同一可信管理网络上，也不必在同一地理位置中。

注意 由于系统仅对主用管理中心开放某些功能，因此如果该设备发生故障，则必须将备用管理中心升级为主用设备。

注释 在成功部署更改后立即触发 管理中心 切换可能会导致预览配置在新的主用 管理中心上不起作用。这不会影响策略部署功能。建议在完成必要的同步后在 管理中心 上触发切换。

同样，当 管理中心 HA 同步处于降级状态时，触发切换或更改角色可能会使 管理中心 HA 损坏数据库，并且可能会造成灾难性的后果。我们建议您立即联系思科技术支持中心 (TAC) 寻求进一步帮助以解决此问题。

由于各种原因，此 HA 同步最终可能处于降级状态。本章中的 更换高可用性对中的 管理中心，第 302 页 部分介绍了一些故障场景以及修复问题的后续程序。如果降级状态的原因或场景与说明的场景匹配，请按照以下步骤解决问题。对于其他原因，我们建议您联系 TAC。

关于远程接入 VPN 高可用性

如果主设备具有使用 CertEnrollment 对象注册的身份证书的远程接入 VPN 配置，则辅助设备必须具有使用同一 CertEnrollment 对象注册的身份证书。由于特定于设备的重写，CertEnrollment 对象可以具有不同的主设备值和辅助设备值。其局限是必须在高可用性形成之前在两个设备上注册相同的 CertEnrollment 对象。

管理中心高可用性中的 SNMP 行为

在 SNMP 配置的 HA 对中，当您部署警报策略时，主管理中心会发送 SNMP 陷阱。当主 管理中心发生故障时，成为主用设备的辅助 管理中心 会发送 SNMP 陷阱，而无需进行任何其他配置。

Firepower 管理中心高可用性中的角色与状态

主/辅助角色

当在高可用性对中设置 Cisco Secure Firewall Management Center时，您可以将一个 Cisco Secure Firewall Management Center配置为主，将另一个配置为辅助。配置过程中，主设备的策略将同步到辅助设备。在此同步之后，主 Cisco Secure Firewall Management Center成为主用对等体，而辅助 Cisco Secure Firewall Management Center成为备用对等体，并且这两个设备将作为受管设备和策略配置的单个设备。

主用/备用状态

高可用性对中的两个 Cisco Secure Firewall Management Center之间的主要差异与哪个对等体是主用以及哪个对等体是备用相关。主用 Cisco Secure Firewall Management Center保持完整功能，您可以从中管理设备和策略。备用 Cisco Secure Firewall Management Center的功能是隐藏的，您不能进行任何配置更改。

管理中心高可用性对上的事件处理

由于高可用性对中的两个管理中心均可接收来自受管设备的事件，因此不会共享设备的管理 IP 地址。这意味着如果一个管理中心发生故障，您不需要为了确保继续处理事件而进行干预。

AMP 云连接和恶意软件信息

尽管它们共享文件策略和相关配置，但高可用性对中的 管理中心不会共享思科 AMP 云连接和恶意软件处置。为了确保工作连续性以及受检测文件的恶意软件处置情况在两个 管理中心上均相同，主用和备用 管理中心均必须能够访问 AMP 云。

URL 过滤和安全情报

URL 过滤和安全情报配置及信息在高可用性部署中的Cisco Secure Firewall Management Center之间同步。但是，只有主 Cisco Secure Firewall Management Center会下载 URL 类别和信誉数据，以获得安全情报源的更新。

如果主 Cisco Secure Firewall Management Center发生故障，则不仅必须确保辅助 Cisco Secure Firewall Management Center可以访问互联网以更新威胁情报数据，还必须使用辅助 Cisco Secure Firewall Management Center上的 Web 界面将其升级为主用设备。

管理中心 故障切换过程中的用户数据处理

如果主 管理中心 发生故障，则辅助 管理中心 会从 TS 代理身份源传播到受管设备的用户到 IP 映射；并从 ISE/ISE-PIC 身份源传播 SGT 映射。身份源尚未发现的用户被标识为“未知”。

停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”用户。

管理中心 高可用性对上的配置管理

在高可用性部署中，只有主用 管理中心可以管理设备和应用策略。两个管理中心都处于连续同步状态。

如果主用 管理中心失败，则高可用性对进入降级状态，直到您手动将备用设备升级到主用状态。升级完成后，设备将离开维护模式。

管理中心 高可用性灾难恢复

在灾难恢复情况下，必须执行手动切换。当主 管理中心 - FMC1 失败时，访问辅助 管理中心 - FMC2 的 Web 接口并交换对等体。这也适用于辅助 (FMC2) 发生故障的情况。有关详细信息，请参阅在管理中心高可用性对中切换对等体，第 300 页。

有关恢复失败的 管理中心，请参阅更换高可用性对中的 管理中心，第 302 页。

单点登录和高可用性对

高可用性配置中的管理中心可以支持单点登录，但必须牢记以下注意事项：

- 高可用性对的成员之间未同步 SSO 配置；您必须在 SSO 对的每个成员上单独配置 SSO。
- 高可用性对中的两个 管理中心必须使用相同的 IdP 进行 SSO。您必须在 IdP 上为每个 管理中心 配置的 SSO 配置服务提供商应用。
- 在均配置为支持 SSO 的 管理中心高可用性对中，在用户首次使用 SSO 访问辅助 管理中心 之前，该用户必须首先使用 SSO 至少登录一次主 管理中心。
- 为高可用性对中的 管理中心配置 SSO 时：
  - 如果在主 管理中心上配置 SSO，则不需要在辅助 管理中心上配置 SSO。
  - 如果在辅助 管理中心上配置 SSO，则还需要在主 管理中心 上配置 SSO。（这是因为 SSO 用户必须在登录辅助 管理中心之前至少登录一次主 管理中心 。）

相关主题

配置 SAML 单点登录，第 136 页

管理中心备份期间的高可用性行为

对 管理中心高可用性对进行备份时，备份操作会暂停对等体之间的同步。在此操作过程中，您可以继续使用主用 管理中心，但不能使用备用对等体。

备份完成后，同步将继续，这将短暂地禁用主用对等体上的进程。在此暂停期间，“高可用性”页面将短暂显示一个保留页，直到所有进程都恢复为止。

管理中心 高可用性裂脑

如果高可用性对中的活动 管理中心关闭（电源问题、网络/连接问题所致），则可以将备用 管理中心提升为活动状态。当原始活动对等体出现时，两个对等体都可以假定它们处于活动状态。此状态被定义为“裂脑"。出现这种情况时，系统会提示您选择一个活动设备，这会将另一个设备降为备用状态。

如果活动管理中心关闭（或因网络故障而断开连接），您可以断开高可用性或切换角色。备用管理中心进入降级状态。

注释 当您解决裂脑时，不管将哪个设备用作辅助设备，都会丢失其所有设备注册和策略配置。例如，您将丢失对存在于辅助设备但却不在主设备上的任何策略所做的修改。如果 管理中心处于高可用性裂脑情景中，即两个设备处于活动状态，并且您在解决裂脑之前注册受管设备并部署策略，则在重新建立高可用性之前，必须从预期的备用 管理中心导出所有策略并注销所有受管设备。然后，您可以注册受管设备并将策略导入到预期的活动 管理中心。

升级高可用性对中的 管理中心

思科定期以电子形式分发多种不同类型的更新。这些更新包括对系统软件的主要和次要升级。您可能需要在高可用性设置中的 管理中心上安装这些更新。

警告 请确保在升级过程中至少有一个操作 管理中心。

开始之前

阅读升级附带的版本说明或咨询文本。版本说明提供重要信息，包括支持的平台、兼容性、先决条件、警告以及具体安装和卸载说明。

过程

步骤 1 访问主用 管理中心的 Web 界面并暂停数据同步；请参阅暂停成对管理中心之间的通信，第 300 页。

步骤 2 升级备用 管理中心。
升级完成后，备用设备将变为主用设备。当两个对等体都是主用设备时，高可用性对处于降级状态（裂脑）。

步骤 3 升级另一个 管理中心。

步骤 4 确定要用作备用设备的 管理中心。在暂停同步之后添加到备用设备的任何其他设备或策略都不会同步到主用 管理中心。仅注销其他设备并导出要保留的任何配置。

当选择新的主用管理中心时，您指定为辅助设备的管理中心将失去设备注册和部署的策略配置，这些内容不会同步。

步骤 5 通过选择具有策略和设备的所有最新所需配置的新主用 管理中心，解决裂脑问题。

管理中心高可用性故障排除

本部分列出了有关某些常见 管理中心高可用性操作错误的故障排除信息。

错误	说明	解决方案
您必须在主用 管理中心 上重置密码，然后方可登录至备用设备。	当您的账户启用强制密码重置时，您尝试登录备用 管理中心 。	由于数据库对于备用 管理中心是只读的，因此请在主用 管理中心的登录页面上重置密码。
500 内部	如果在执行关键的 管理中心高可用性操作（包括切换对等角色或暂停和恢复同步）时尝试访问 Web 界面，可能会出现该错误。	请等到操作完成后再使用 Web 界面。

错误	说明	解决方案
系统进程正在启动，请稍候 此外，Web 界面不响应。	如果在高可用性或数据同步操作期间管理中心重启（手动或从断电中恢复时），可能出现该错误。	1. 访问 管理中心外壳并使用 `manage_hadc.pl` 命令访问 管理中心高可用性配置实用程序。 **注释** 使用 `sudo` 以根用户身份运行该实用程序。 2. 使用选项 5 暂停镜像操作。 重新加载 管理中心 Web 界面。 3. 使用 Web 界面恢复同步。选择 **集成** > **其他集成**，然后点击 **高可用性** 选项卡，选择 **恢复同步**。
设备注册状态：主机 <*string*> 无法访问	在 威胁防御的初始配置期间，如果指定了 管理中心 IP 地址和 NAT ID，则 **主机** 字段可以留空。但是，在 NAT 后面 管理中心的 HA 环境中，在辅助 管理中心上添加 威胁防御 时会发生此错误。	1. 从主用 管理中心中删除 威胁防御 。请参阅 思科 Cisco Secure Firewall Management Center设备配置指南 中的从 删除设备管理中心。 2. 使用 **configure manager delete** 命令从 威胁防御 删除管理器。请参阅 Cisco Secure Firewall Threat Defense 命令参考。 3. 在 **主机** 字段中，通过 威胁防御 设备的 IP 地址或名称将 威胁防御 添加到 管理中心 。请参阅 思科 Cisco Secure Firewall Management Center 设备配置指南 中的将设备添加 到管理中心。

错误	说明	解决方案
设备注册状态：主机 <*string*> 无法访问	在辅助 管理中心 和 威胁防御 设备均位于 NAT 之后，将 威胁防御 设备添加到高可用性部署中的辅助 管理中心 中心时，会发生此错误。	在备用 管理中心 Web 界面上，点击 **集成** > **其他集成** > **高可用性**。在待处理设备注册表下，点击待处理设备的 IP 地址，然后将 IP 地址更改为 威胁防御的公共 IP 地址。 或 1. 访问 威胁防御 shell 并使用 `show manager` 命令获取备用 管理中心 条目标识符值。 2. 在 威胁防御 shell 中，将备用 管理中心 主机名编辑为公共 IP 地址。执行 `configure manager edit` <standby_uuid>主机名<standby_ip> 命令使用条目标识符值和主机 IP 地址。 有关详细信息，请参阅 使用 CLI 解决 管理中心 高可用性中的设备注册，第 299 页。
高可用性 管理中心 之间的设备配置同步已停止。	在 管理中心 高可用性同步时，设备配置历史记录文件现在与其他配置数据并行同步。如果过去 6 个小时未发生同步， 管理中心 会监控配置历史记录文件同步任务，并在HA同步超时时通知您。此运行状况警报显示在主用和备用管理中心中。	主用和备用 管理中心都将进入降级状态。请联系思科支持部门进行故障排除。

Firepower 管理中心高可用性要求

型号支持

请参阅硬件要求，第 294 页。

虚拟模型支持

请参阅虚拟平台要求，第 294 页。

支持的域

全局

用户角色

管理员

硬件要求

- 所有 管理中心 硬件支持高可用性。对等体必须为同一型号。
- 对等体可能在物理上和地理上在不同的数据中心中相互分离。
- 高可用性配置的带宽要求取决于各种因素，例如网络规模、受管设备数量、事件和日志量，以及配置更新的大小和频率。

  对于典型的 管理中心 高可用性部署，在接近100毫秒的高延迟网络的情况下，建议对等体之间的网络带宽至少为 5 Mbps。
- 不要将主要对等体的备份恢复到辅助对等体。
- 另请参阅 管理中心高可用性配置的许可证要求，第 295 页。

虚拟平台要求

以下公共云平台支持高可用性：

- Amazon Web Services (AWS)
- Oracle 云基础设施 (OCI)

以及这些内部部署/私有云平台：

- 思科 HyperFlex
- 基于内核的虚拟机 (KVM)
- Microsoft Hyper-V
- VMware vSphere/VMware ESXi

管理中心 必须具有相同的设备管理能力（FMCv2 不支持）和相同的许可。您还需要为每个托管设备提供一个 威胁防御 授权。有关详细信息，请参阅 管理中心高可用性配置的许可证要求，第 295 页。

注释 如果您仅管理版本 7.0.x Classic 设备（NGIPSv 或 ASA FirePOWER），则不需要 FMCv 授权。

软件要求

可以访问**设备信息**构件，以验证软件版本、入侵规则更新版本和漏洞数据库更新。默认情况下，该构件将显示在 **详细控制面板** 和 **摘要控制面板**的 **状态** 选项卡上。有关详细信息，请参阅设备信息构件，第 324 页

- 高可用性配置中的两个 管理中心必须具有相同的主要（第一个数字）、次要（第二个数字）和维护（第三个数字）软件版本。
- 高可用性配置中的两个 管理中心必须安装相同版本的入侵规则更新。
- 高可用性配置中的两个 管理中心必须安装相同版本的漏洞数据库更新。
- 高可用性配置中的两个 管理中心必须安装相同版本的 LSP（轻量安全安装包）。

警告 如果两个 管理中心上的软件版本、入侵规则更新版本和漏洞数据库更新版本不相同，则将无法建立高可用性。

管理中心高可用性配置的许可证要求

每台设备都需要相同的许可证，无论是由单个 管理中心 管理还是由 管理中心高可用性对（硬件或虚拟）中的管理。

示例： 如果要对由 管理中心 对管理的两个设备启用高级恶意软件保护，请购买两个 恶意软件防御许可证和两个 TM 订用，向智能软件管理器注册主要 管理中心 ，然后将许可证分配给主要 管理中心上的两个设备。

只有主用管理中心会向智能软件管理器注册。故障切换发生时，系统与智能软件管理器通信，以释放原始主用 管理中心 中的许可证授权，并将其分配到新的主用 管理中心。

在特定许可证预留部署中，只有主 管理中心 需要特定许可证预留。

硬件 管理中心

高可用性对中的 管理中心硬件不需要特殊许可证。

Management Center Virtual

您将需要两个相同许可的 management center virtual。

示例： 对于管理 10 台设备的 management center virtual 高可用性对，您可以使用：

- 两（2） management center virtual 10个授权
- 10 个设备许可证

如果中断高可用性对，则会释放与辅助 management center virtual 关联的 management center virtual 授权。（在本例中，您将有两个独立的 management center virtual 10。）

管理中心 高可用性的前提条件

在建立 管理中心 高可用性对之前：

- 从预期的辅助 管理中心向预期的主 管理中心导出所需的策略。有关详细信息，请参阅导出配置，第 489 页。
- 确保预期的辅助 管理中心没有添加任何设备。删除预期的辅助 管理中心中的设备，并将这些设备注册到预期的主 管理中心。有关详细信息，请参阅 从 管理中心删除设备 和 向 《Cisco Secure Firewall Management Center 设备配置指南》中的 管理中心 添加设备。
- 将策略导入到预期的主 管理中心。有关详细信息，请参阅导入配置，第 490 页。
- 在预期的主 管理中心上，验证导入的策略，根据需要进行编辑，并将它们部署到相应的设备。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 部署配置更改 。
- 在预期的主 管理中心上，为新添加的设备关联适当的许可证。有关详细信息，请参阅将许可证分配给单个设备，第 267 页。

现在可以继续建立高可用性。有关详细信息，请参阅 建立 管理中心 高可用性，第 296 页。

建立 管理中心 高可用性

建立高可用性可能会花费大量时间，甚至数小时，具体取决于对等体之间的带宽和策略数量。它还取决于已注册到主用 管理中心的设备数量，该数量需要同步到备用 管理中心。可以查看“高可用性”页面，以检查高可用性对等体的状态。

开始之前

- 确认两个 管理中心都符合高可用性系统要求。有关更多信息，请参阅Firepower 管理中心高可用性要求，第 293 页。
- 确认已达到建立高可用性的先决条件。有关详细信息，请参阅 管理中心 高可用性的前提条件，第 295 页。

过程

步骤 1 登录到希望指定为辅助的 管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 在此 管理中心的“角色”下，选择**辅助**。

步骤 5 在**主 Firepower 管理中心主机**文本框中，输入主 管理中心的主机名或 IP 地址。

如果主 管理中心没有可从对等 管理中心 访问的 IP 地址（可以是公共或私有 IP 地址），则可以将此字段留空。在此情况下，请同时使用**注册密钥**和**唯一 NAT ID** 字段。您需要指定至少一个 管理中心的 IP 地址才能启用 HA 连接。

步骤 6 在**注册密钥**文本框中输入一个一次性注册密钥。

该注册密钥是任何用户定义的字母数字值，最长 37 个字符。此注册表项将用于注册辅助和主 管理中心。

步骤 7 如果没有指定主 IP 地址，或者如果并未计划指定主 管理中心上的辅助 IP 地址，则请在**唯一 NAT ID** 字段中，输入一个唯一的字母数字 ID。有关详细信息，请参阅NAT 环境，第 73 页。

步骤 8 点击**注册 (Register)**。

步骤 9 使用具有管理员访问权限的帐户登录到要指定为主管理中心的防御中心。

步骤 10 选择**集成** > **其他集成**。

步骤 11 选择**高可用性**。

步骤 12 在此 管理中心的“角色”下，选择**主**。

步骤 13 在**辅助 Firepower 管理中心主机**文本框中，输入辅助 管理中心的主机名或 IP 地址。

如果辅助 管理中心 没有可从对等 管理中心 访问的 IP 地址（可以是公共或私有 IP 地址），则可以将此字段留空。在此情况下，请同时使用**注册密钥**和**唯一 NAT ID** 字段。您需要指定至少一个 管理中心 的 IP 地址才能启用 HA 连接。

步骤 14 在第 6 步中使用的**注册密钥**文本框中输入同一个一次性注册密钥。

步骤 15 如果需要，请在**唯一 NAT ID** 文本框中输入在第 7 步中使用的同一个 NAT ID。

步骤 16 点击 **Register**。

下一步做什么

建立 管理中心 高可用性时，注册到主用 管理中心的设备将自动注册到备用 管理中心。

注释 如果已注册的设备拥有 NAT IP 地址，则自动设备注册将失败，并且辅助 管理中心 的“高可用性”页面会将该设备列为本地、待处理状态。随后可在备用 管理中心的“高可用性”页面上为该设备分配另一个 NAT IP 地址。如果自动注册在备用 管理中心上因其他原因失败，但该设备显示为已注册到主用 Firepower 管理中心，则请参阅使用 CLI 解决 管理中心 高可用性中的设备注册，第 299 页。

查看 管理中心 高可用性状态

在识别主用和备用 管理中心后，可以查看关于本地 管理中心及其对等体的信息。

注释 在此上下文中，“本地对等体”是指您要查看其系统状态的设备。“远程对等体”是指其他设备，无论是处于主用还是备用状态。

过程

步骤 1 登录您使用高可用性配对的一个 管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

可以查看：

摘要信息

- 高可用性对的运行状态。当备用设备从主用设备接收配置更改时，正常运行的系统的状态将在“运行状况正常”和“正在进行同步任务”之间摆动。
- 高可用性对的当前同步状态
- 主用对等体的 IP 地址及其上次同步时间
- 备用对等体的 IP 地址及其上次同步时间

系统状态

- 两个对等体的 IP 地址
- 两个对等体的操作系统
- 两个对等体的软件版本
- 两个对等体的设备型号

注释 您只能在主用 管理中心上查看出口控制和合规性状态。

在 管理中心 高可用性对上同步的配置

在两个 管理中心之间建立高可用性时，两个设备之间将同步以下配置数据：

- 许可证授权
- 访问控制策略
- 入侵规则
- 恶意软件和文件策略
- DNS 策略
- 身份策略
- SSL 策略

- 预过滤策略
- 网络发现规则
- 应用检测器
- 关联策略规则
- 风险通告
- 扫描程序
- 响应组
- 用于调查事件的外部资源的上下文交叉启动
- 补救设置，但您必须在两个 管理中心上安装自定义模块。有关补救设置的详细信息，请参阅管理补救模块，第 999 页。

在高可用性对中配置对 管理中心 数据库的外部访问

在高可用性设置中，我们建议您仅使用活动对等体来配置对数据库的外部访问。为外部数据库访问配置备用对等体时，会导致频繁断开连接。要恢复连接，必须 暂停成对管理中心之间的通信 并 重新启动成对 管理中心之间的通信 备用对等体的同步。有关如何启用对 管理中心的外部数据库访问的信息，请参阅 启用对数据库的外部访问，第 59 页。

使用 CLI 解决 管理中心 高可用性中的设备注册

如果备用 管理中心上的自动设备注册失败，但似乎已注册到主用 管理中心，请完成以下步骤：

警告 如果执行辅助 管理中心 RMA或添加辅助 管理中心RMA，则受管设备会注销，因此会删除其配置。

过程

步骤 1 从主用 管理中心中删除设备。在 Cisco Secure Firewall Management Center 设备配置指南从 管理中心删除（注销）设备 。

步骤 2 要在备用设备 管理中心上触发设备的自动注册，请完成以下步骤：

1. 登录到受影响设备的 CLI。
2. 运行 CLI 命令： **configure manager delete**。

   此命令将会禁用并删除当前的 管理中心。
3. 运行 CLI 命令： **configure manager add**。

此命令会将设备配置为发起与 管理中心的连接。

提示 仅面向活动 管理中心在设备上配置远程管理。建立高可用性时，设备将自动注册到备用管理中心。

4. 登录主用 管理中心 并注册设备。

步骤 3 如果备用 管理中心 位于 NAT 之后，请完成以下步骤以编辑备用 管理中心的主机名：

1. 访问 威胁防御 shell 并使用 `show manager` 命令获取备用 管理中心 条目标识符值。
2. 在 威胁防御 shell 中，将备用 管理中心 主机名编辑为公共 IP 地址。执行 `configure manager edit` <standby_uuid>主机名<standby_ip>命令使用条目标识符值和主机 IP 地址。

在管理中心高可用性对中切换对等体

由于系统将某些功能限制为适用于主用管理中心，因此如果该设备发生故障，则必须将备用管理中心升级为主用设备：

过程

步骤 1 登录您使用高可用性配对的一个 管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 选择**切换角色**以将本地角色从主用更改为备用，或者从备用更改为主用。在 Primary 或 Secondary 指定保持不变的情况下，角色在两个对等体之间切换。

暂停成对管理中心之间的通信

如果要临时禁用高可用性，您可以在管理中心之间禁用通信信道。您可以从主用或备用对等体上暂停同步。

过程

步骤 1 登录您使用高可用性配对的一个管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 选择**暂停同步**。

重新启动成对 管理中心之间的通信

如果暂时禁用了高可用性，可以通过启用管理中心之间的通信通道重新启动高可用性。您可以从主用或备用对等体恢复同步。

过程

步骤 1 登录您使用高可用性配对的一个 管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 选择**恢复同步**。

在高可用性对中更改 管理中心 的 IP 地址

如果其中一个高可用性对等体的IP 地址发生更改，则高可用性将进入降级状态。要恢复高可用性，必须手动更改 IP 地址。

过程

步骤 1 登录您使用高可用性配对的一个 管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 选择**对等体管理器**。

步骤 5 选择**编辑**（ ）。

步骤 6 输入设备的显示名称，该名称仅在系统环境内使用。

输入另一个显示名称不会更改设备的主机名。

步骤 7 输入完全限定域名、通过本地 DNS 解析为有效 IP 地址的名称（即，主机名）或主机 IP 地址。

步骤 8 点击**保存 (Save)**。

禁用 管理中心 高可用性

过程

步骤 1 登录高可用性对中的其中一个管理中心。

步骤 2 选择**集成** > **其他集成**。

步骤 3 选择**高可用性**。

步骤 4 选择**破坏高可用性**。

步骤 5 选择以下选项之一来处理受管设备：

- 要使用此 管理中心控制所有受管设备，请选择**从此控制台管理注册设备**。所有设备都将从对等体注销。
- 要使用其他 管理中心控制所有受管设备，请选择**从对等体控制台管理注册设备**。所有设备都将从此管理中心注销。
- 要一起停止管理设备，请选择**从两个控制台停止管理注册设备**。所有设备都将从这两个管理中心注销。

注释 如果选择要从辅助管理中心管理注册的设备，则设备将从主要管理中心取消注册。设备现在已注册为由辅助 管理中心管理。但是，应用到这些设备的许可证会由于高可用性中断操作而取消注册。您现在必须从辅助 管理中心中的设备继续重新注册（启用）许可证。有关详细信息，请参阅将许可证分配到设备，第 267 页。

步骤 6 点击**确定 (OK)**。

更换高可用性对中的 管理中心

如果需要更换 管理中心 高可用性对中的故障设备，则必须按照下面列出的程序之一进行操作。该表列出了四种可能的故障场景，及其相对应的更换程序。

故障状态	数据备份状态	更换程序
主 管理中心发生故障	数据备份成功	更换出现故障的主 管理中心（成功备份），第 303 页
	数据备份未成功	更换发生故障的主 管理中心（成功备份），第 303 页
辅助 管理中心发生故障	数据备份成功	更换出现故障的辅助 管理中心（成功备份），第 304 页
	数据备份未成功	替换失败的辅助 管理中心（不成功的备份），第 305 页

更换出现故障的主 管理中心（成功备份）

两个 管理中心、*FMC1* 和 *FMC2* 是高可用性对的一部分。*FMC1* 是主设备， *FMC2* 是辅助设备。此任务描述在主设备数据备份成功时更换发生故障的主 管理中心、*FMC1* 的步骤。

开始之前

验证发生故障的主 管理中心的数据备份是否成功。

过程

步骤 1 请与支持部门联系，申请更换发生故障的 管理中心 - *FMC1*。

步骤 2 当主 管理中心 - *FMC1* 失败时，访问辅助 管理中心 - *FMC2* 的 Web 接口并交换对等体。有关详细信息，请参阅在管理中心高可用性对中切换对等体， 第 300 页。

这会将辅助 管理中心 - *FMC2* 升级到主用状态。

可以将 *FMC2* 用作主 管理中心，直到主 管理中心 - *FMC1* 被替换。

注意 不要破坏 *FMC2*中的 管理中心 高可用性，因为从 *FMC1* 同步到 *FMC2* 的许可证（故障之前）将从 *FMC2* 中删除，您将无法从 *FMC2*执行任何部署操作。

步骤 3 使用与 *FMC1*相同的软件版本重新映像更换的 管理中心 。

步骤 4 将从 *FMC1* 检索到的数据备份还原到新的 管理中心。

步骤 5 安装所需的 管理中心补丁、地理位置数据库 (GeoDB) 更新、漏洞数据库 (VDB) 更新和系统软件更新，以匹配 *FMC2*。

新的 管理中心和 *FMC2* 现在都是主用对等体，导致高可用性被破坏。

步骤 6 当 管理中心 Web 界面提示您选择主用设备时，请选择 *FMC2* 作为主用设备。

这会将最新的配置从 *FMC2* 同步到新的 管理中心 - *FMC1*。

步骤 7 配置成功同步后，访问辅助 管理中心 - *FMC2* 的 Web 界面并交换角色，以使主 管理中心 - *FMC1* 变成主用状态。有关详细信息，请参阅在管理中心高可用性对中切换对等体， 第 300 页。

下一步做什么

高可用性现在已重新建立，且主和辅助 管理中心现在将按预期方式工作。

更换发生故障的主 管理中心（成功备份）

两个 管理中心- *FMC1* 和 *FMC2* 是高可用性对的一部分。*FMC1* 是主设备， *FMC2* 是辅助设备。此任务介绍在从主管理中心进行数据备份不成功时，替换失败的主 管理中心 -*FMC1* 的步骤。

过程

步骤 1 请与支持部门联系，申请更换发生故障的 管理中心 - *FMC1*。

步骤 2 当主 管理中心 - *FMC1* 失败时，访问辅助 管理中心 - *FMC2* 的 Web 接口并交换对等体。有关详细信息，请参阅在管理中心高可用性对中切换对等体，第 300 页。

这会将辅助 管理中心 - *FMC2* 升级到主用状态。

可以将 *FMC2* 用作主 管理中心，直到主 管理中心 - *FMC1* 被替换。

注意 不要破坏 *FMC2*中的 管理中心 高可用性，因为从 *FMC1* 同步到 *FMC2* 的许可证（故障之前）将从 *FMC2* 中删除，您将无法从 *FMC2*执行任何部署操作。

步骤 3 使用与 *FMC1*相同的软件版本重新映像更换的 管理中心 。

步骤 4 安装所需的 管理中心补丁、地理位置数据库 (GeoDB) 更新、漏洞数据库 (VDB) 更新和系统软件更新，以匹配 *FMC2*。

步骤 5 从思科智能软件管理器取消注册 管理中心 - *FMC2*。有关详细信息，请参阅取消注册 管理中心，第 269 页。

从思科智能软件管理器取消注册管理中心可将管理中心从您的虚拟帐户中删除。与 管理中心关联的所有许可证授权将释放回虚拟账户。注销后，管理中心会进入“执行”模式，在此模式下，不允许对许可功能进行更新或更改。

步骤 6 访问辅助 管理中心 - *FMC2* 的 Web 截面，并中断 管理中心 高可用性。有关详细信息，请参阅禁用管理中心 高可用性，第 302 页。在提示选择用于处理受管设备的选项时，请选择**通过此控制台管理已注册的设备**。

因此， 同步到辅助 管理中心的证书 - *FMC2*的典型和智能许可证将被删除，您无法从 *FMC2*执行部署活动。

步骤 7 通过将 管理中心 - *FMC2* 设置为主并将 管理中心 - *FMC1* 设置为辅助，重新建立 管理中心 高可用性。有关详细信息，请参阅建立 管理中心 高可用性，第 296 页。

步骤 8 向主 管理中心 - *FMC2*注册智能许可证。有关详细信息，请参阅将管理中心注册到智能软件管理器，第 262 页。

下一步做什么

高可用性现在已重新建立，且主和辅助 管理中心现在将按预期方式工作。

更换出现故障的辅助 管理中心（成功备份）

两个 管理中心- *FMC1* 和 *FMC2* 是高可用性对的一部分。*FMC1* 是主设备， *FMC2* 是辅助设备。此任务描述当来自出现故障的辅助 管理中心 -*FMC2* 的数据备份成功时更换该设备的步骤。

开始之前

验证来自出现故障的辅助 管理中心的数据备份是否成功。

过程

步骤 1 请与支持部门联系，申请更换发生故障的 管理中心 - *FMC2*。

步骤 2 继续使用主 管理中心 - *FMC1* 作为主用 管理中心。

步骤 3 使用与 *FMC2*相同的软件版本重新映像更换的 管理中心 。

步骤 4 将从 *FMC2* 的数据备份还原到新的 管理中心。

步骤 5 安装所需的 管理中心 补丁、地理位置数据库 (GeoDB) 更新、漏洞数据库 (VDB) 更新和系统软件更新，以匹配 *FMC1*。

步骤 6 从新的 管理中心 - *FMC2*的 Web 界面恢复数据同步（如果已暂停），以同步来自主 管理中心 - *FMC1* 的最新配置。有关详细信息，请参阅重新启动成对 管理中心之间的通信 ，第 301 页。

“经典”和“智能”许可证将无缝工作。

下一步做什么

高可用性现在已重新建立，且主和辅助 管理中心现在将按预期方式工作。

替换失败的辅助 管理中心（不成功的备份）

两个 管理中心- *FMC1* 和 *FMC2* 是高可用性对的一部分。*FMC1* 是主设备， *FMC2* 是辅助设备。此任务介绍了在从辅助设备备份数据失败后，更换发生故障的辅助 管理中心 (*FMC2*) 的步骤。

过程

步骤 1 请与支持部门联系，申请更换发生故障的 管理中心 - *FMC2*。

步骤 2 继续使用主 管理中心 - *FMC1* 作为主用 管理中心。

步骤 3 使用与 *FMC2*相同的软件版本重新映像更换的 管理中心 。

步骤 4 安装所需的 管理中心 补丁、地理位置数据库 (GeoDB) 更新、漏洞数据库 (VDB) 更新和系统软件更新，以匹配 *FMC1*。

步骤 5 访问主 管理中心 - *FMC1* 的 Web 截面，并中断 管理中心 高可用性。有关详细信息，请参阅禁用 管理中心 高可用性，第 302 页。在提示选择用于处理受管设备的选项时，请选择**通过此控制台管理已注册的设备**。

步骤 6 通过将 管理中心 - *FMC1* 设置为主并将 管理中心 - *FMC2* 设置为辅助，重新建立 管理中心 高可用性。有关更多信息，请参阅建立 管理中心 高可用性，第 296 页。

- 在成功建立高可用性后，将来自主 管理中心 - *FMC1* 的最新配置同步到辅助 管理中心 - *FMC2*。

- “经典”和“智能”许可证将无缝工作。

下一步做什么

高可用性现在已重新建立，且主和辅助 管理中心现在将按预期方式工作。

管理中心 高可用性灾难恢复

在灾难恢复情况下，必须执行手动切换。当主 管理中心 - FMC1 失败时，访问辅助 管理中心 - FMC2 的 Web 接口并交换对等体。这也适用于辅助 (FMC2) 发生故障的情况。有关详细信息，请参阅在管理中心高可用性对中切换对等体，第 300 页。

有关恢复失败的 管理中心，请参阅更换高可用性对中的 管理中心，第 302 页。

恢复高可用性对中的管理中心（无硬件故障）

要在没有硬件故障的情况下恢复 管理中心 高可用性对，请执行以下程序：

- 在主要管理中心恢复备份 ，第 306 页
- 在辅助管理中心恢复备份，第 307 页

在主要管理中心恢复备份

开始之前

- 没有硬件故障和更换管理中心。
- 您熟悉备份和恢复过程。请参阅备份/恢复，第 435 页。

过程

步骤 1 验证主要 管理中心 的备份是否可用 - /var/sf/backup/ 中的本地存储或远程网络卷。

步骤 2 在主要 管理中心上暂停同步。选择 **集成** > **其他集成**，然后转到 **高可用性** 选项卡以暂停同步。

步骤 3 恢复所更换的主要 管理中心的备份。恢复完成后， 管理中心 会重新启动。

步骤 4 一旦主要管理中心处于活动状态且其用户接口可访问，则在辅助 管理中心上恢复同步。选择 **集成** > **其他集成**，然后转到 **高可用性** 选项卡以恢复同步。

在辅助管理中心恢复备份

开始之前

- 没有硬件故障和更换管理中心。
- 您熟悉备份和恢复过程。请参阅备份/恢复，第 435 页。

过程

步骤 1 验证辅助 管理中心 的备份是否可用 - /var/sf/backup/ 中的本地存储或远程网络卷。

步骤 2 在主要 管理中心上暂停同步。选择 **集成** > **其他集成**，然后转到 **高可用性** 选项卡以暂停同步。

步骤 3 在辅助 管理中心上恢复备份。恢复完成后， 管理中心 会重新启动。

步骤 4 一旦辅助管理中心处于活动状态且其用户接口可访问，则在主要 管理中心上恢复同步。选择 **集成** > **其他集成**，然后转到 **高可用性** 选项卡以恢复同步。

高可用性管理中心的统一备份

您可以在主用管理中心上执行统一备份，其中为主用和备用管理中心创建单个备份文件。统一备份仅适用于仅配置备份。如果需要事件或 TID 备份，则必须对主用和备用 管理中心进行单独的备份。当您选择仅配置备份时，默认情况下会应用统一备份。在统一备份中，如果主用设备 管理中心 无法从备用设备 管理中心获取备份 tar 文件，则会为主用设备生成可用于恢复的正常备份文件。与普通备份相比，统一备份有几个优势：

- 统一备份不要求您在主用和备用 管理中心上进行单独的备份。
- 备份中的冗余数据和存储限制在统一备份中删除。
- 在正常备份中，当主设备发生故障且辅助设备备份不可用时，您必须中断辅助 RMA 的高可用性配对。这种情况在统一备份中被根除。
- 通常，无法安排备用设备的备份。在计划的统一备份中，会同时使用主用设备和备用设备的备份。
- 执行统一备份时，不必暂停 HA 同步即可在备用设备上执行备份。

如果发生意外事件，您可以使用统一备份来恢复新的 RMA 设备。您可以通过名称识别统一备份文件。在统一备份文件名中添加前缀“Unified”。您可以选择 管理中心 进行恢复，也可以选择其状态（主用/备用）。

确保选择已恢复 管理中心 的适当状态，以防止裂脑冲突。

从统一备份恢复管理中心

使用此程序可从 备份 管理中心恢复 管理中心 （仅配置）。

过程

步骤 1 登录到要恢复的 管理中心 。

步骤 2 选择**系统**（⚙）> **工具** > **备份/恢复**。

“备份管理”页面列出所有本地和远程存储的备份文件，包括统一的备份文件（仅配置）。

如果统一备份文件不在列表中，并且您已将其保存在本地计算机上，请点击**上传备份**；请参阅管理备份和远程存储，第 462 页。

步骤 3 选择要恢复的统一备份文件并点击 **恢复**。

步骤 4 在 **恢复备份** 页面中，选择要恢复的设备。由于统一备份存储主设备和辅助设备 管理中心的备份配置，因此您需要选择要恢复的设备。

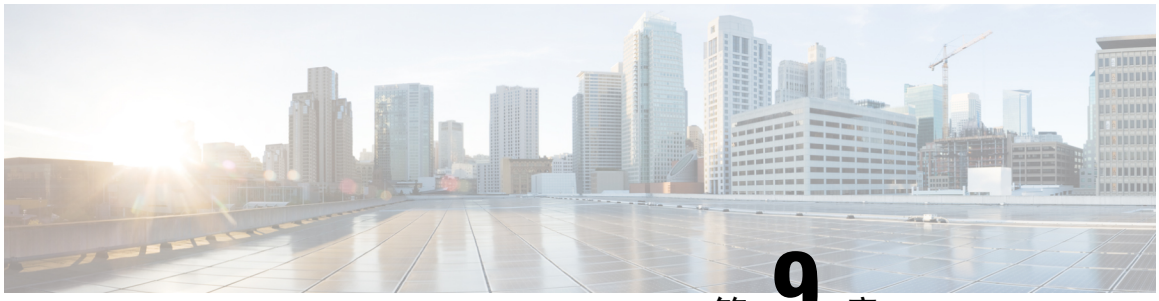
步骤 5 要选择已恢复的 管理中心的状态，请点击 **主** 用或 **备用** 单选按钮。请务必验证正在使用的管理中心的角色和状态，以免两个对等体的角色和状态配置相同。在恢复时，如果为管理中心选择的角色和状态不正确，可能会带来高可用性失败。

步骤 6 点击 **恢复**，然后点击 **确认恢复** 开始恢复。

管理中心 高可用性历史

功能	最低 管理中心	最低 威胁防御	详情
用于高可用性管理中心的单个备份文件。	7.4.1 7.2.6	任意	对高可用性对中的主用管理中心执行仅配置备份时，系统现在会创建一个备份文件，您可以使用该文件恢复任一设备。 其他版本限制：不支持管理中心版本 7.3.x 或 7.4.0。
管理中心高可用性同步增强功能。	7.4.1	任意	管理中心高可用性 (HA) 包括以下同步增强功能： • 大型配置历史记录文件可能会导致高延迟网络中的同步失败。为了防止这种情况发生，设备配置历史记录文件现在与其他配置数据并行同步。此增强功能还缩短了同步时间。 • 管理中心现在监控配置历史记录文件同步过程，并在同步超时时显示运行状况警报。 新增/修改的屏幕：您可以在以下屏幕上查看这些警报： • **通知** > **邮件中心** > **运行状况** • **集成** > **其他集成** > **高可用性** > **状态** （在 **摘要**下）
Hyper-V 上的高可用性支持。	7.4.0	任意	我们现在支持适用于 Hyper-V 的 management center virtual 高可用性。

功能	最低 管理中心	最低 威胁防御	详情
支持 KVM 上的高可用性。	7.3.0	任意	我们现在支持适用于 KVM 的 management center virtual 高可用性。
支持 AWS 和 OCI上的高可用性。	7.1.0	任意	我们现在支持适用于 AWS 和 OCI 的 management center virtual 高可用性。
HyperFlex 上的高可用性支持。	7.0.0	任意	我们现在支持适用于 HyperFlex 的 management center virtual 高可用性。
VMware 上的高可用性支持。	6.7.0	任意	我们现在支持适用于 VMware 的 management center virtual 高可用性。
单点登录。	6.7.0	任意	为单点登录配置高可用性对的一个或两个成员时，必须考虑特殊注意事项。



第 9 章

安全认证合规性

以下主题介绍如何配置系统来符合安全认证标准：

安全认证合规性模式

组织只能使用符合由美国国防部和全球认证组织制定的安全标准的设备和软件。Firepower 支持符合以下安全认证标准：

- 通用标准 (CC)：国际共同标准承认协定建立的全球标准，用于定义安全产品的属性
- 统一功能获批产品列表 (UCAPL)：符合美国国防信息系统机构 (DISA) 建立的安全要求的产品列表

注释 美国政府已将统一功能获批产品列表 (UCAPL) 的名称改为国防部信息网络获批产品列表 (DODIN APL)。本文档和 Cisco Secure Firewall Management CenterWeb 接口中对 UCAPL 的引用可以解释为对 DODIN APL 的引用。

- 联邦信息处理标准 (FIPS) 140：加密模块的要求规范

可以在 CC 模式或 UCAPL 模式下启用安全认证合规性。启用安全认证合规性不保证严格符合所选安全模式的所有要求。有关强化操作步骤的详细信息，请参阅由认证实体提供的此产品的相关准则。

注意 启用此设置后，您将无法将其禁用。如果设备需要退出 CC 或 UCAPL 模式，必须重新映像。

安全认证合规性特征

下表描述了启用 CC 或 UCAPL 模式时的行为更改。（对登录账户的限制是指命令行访问，而不是 Web 界面访问。）

系统更改	Cisco Secure Firewall Management Center		经典受管设备		Cisco Secure Firewall Threat Defense	
	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式
启用 FIPS 合规性。	兼容	兼容	兼容	兼容	兼容	兼容
系统不允许远程存储备份或报告。	兼容	兼容	—	—	—	—
系统启动额外的系统审核后台守护程序。	不兼容	是	否	是	否	不兼容
系统引导加载程序受到保护。	不兼容	是	否	是	否	不兼容
系统对登录帐户应用额外保护。	不兼容	是	否	是	否	不兼容
系统禁用重启按键序列 Ctrl+Alt+Del。	不兼容	是	否	是	否	不兼容
系统最多同时执行 10 个登录会话。	不兼容	是	否	是	否	不兼容
密码必须至少包含 15 个字符，且必须由大小写混合的字母数字字符组成，还必须至少包含一个数字字符。	不兼容	是	否	是	否	不兼容
可以使用本地设备 CLI 配置对本地 `admin` 用户要求的最低密码长度。	不兼容	不兼容	不兼容	不兼容	兼容	兼容
密码中包含的单词不能是在词典中出现过的单词或包含连续的重复字符。	不兼容	是	否	是	否	不兼容
连续三次登录尝试失败后，系统会锁定除 `admin` 以外的用户。在这种情况下，管理员必须重置密码。	不兼容	是	否	是	否	不兼容
默认情况下，系统会存储密码历史记录。	不兼容	是	否	是	否	不兼容
在失败次数超过可通过 Web 界面配置的最大失败登录尝试次数之后，`admin` 用户会被锁定。	兼容	兼容	兼容	兼容	—	—
在失败次数超过可通过本地设备 CLI 配置的最大失败登录尝试次数之后，`admin` 用户会被锁定。	不兼容	不兼容	是，无论是否启用安全认证合规性。	是，无论是否启用安全认证合规性。	兼容	兼容

系统更改	Cisco Secure Firewall Management Center		经典受管设备		Cisco Secure Firewall Threat Defense	
	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式
系统会自动为与设备进行的 SSH 会话重新生成密钥： • 某个密钥用于会话活动达一小时后 • 某个密钥用于通过连接传输 1 GB 的数据后	兼容	兼容	兼容	兼容	兼容	兼容
系统在启动时执行文件系统完整性检查(FSIC)。如果 FSIC 失败，则 Firepower 软件无法启动，远程 SSH 访问会被禁用，您只能通过本地控制台访问该设备。如果出现此问题，请联系思科 TAC。	兼容	兼容	兼容	兼容	兼容	兼容

安全认证合规性建议

在使用启用安全认证合规性的系统时，思科建议您遵循以下最佳实践：

- 要在部署中启用安全认证合规性，请首先在 Cisco Secure Firewall Management Center上将其启用，然后在所有托管设备上的同一模式下将其启用。

⚠

注意 Cisco Secure Firewall Management Center不会接受来自受管设备的事件数据，除非两者在同一安全认证合规性模式下运行。

- 对于所有用户，启用密码强度检查，并将最小密码长度设置为认证机构要求的值。
- 如果您在高可用性配置下使用 Cisco Secure Firewall Management Center，请将它们配置为使用同一安全认证合规性模式。
- 如果将 Firepower 4100/9300机箱上的 Cisco Secure Firewall Threat Defense配置为以 CC 或 UCAPL 模式运行，还应将 Firepower 4100/9300 配置为以 CC 模式运行。有关详细信息，请参阅 *Cisco Firepower 4100/9300 FXOS Firepower* 机箱管理器配置指南。
- 请勿将系统配置为使用以下任意一种功能：
  - 邮件报告、警报或数据修剪通知。
  - Nmap 扫描、思科 IOS 空路由、设置属性值或 ISE EPS 补救。
  - 备份或报告的远程存储。
  - 第三方客户端访问系统数据库。

- 通过邮件 (SMTP) 传送的外部通知或警报、SNMP 陷阱或系统日志。
- 审核未使用 SSL 证书传输到 HTTP 服务器或系统日志服务器的日志消息，以保护设备和服务器之间的通道。

- 请勿在使用 CC 模式的部署中使用 LDAP 或 RADIUS 启用外部身份验证。
- 请勿使用 CC 模式在部署中启用 CAC。
- 使用 CC 或 UCAPL 模式在部署中通过 Firepower REST API 禁用访问 Cisco Secure Firewall Management Center和受管设备。
- 使用 UCAPL 模式在部署中启用 CAC。
- 请勿使用 CC 模式在部署中配置 SSO。
- 请勿将 Cisco Secure Firewall Threat Defense设备配置为高可用性对，除非它们都使用相同的安全认证合规模式。

注释 系统对于以下各项不支持 CC 或 UCAPL 模式：

- 集群中的 Cisco Secure Firewall Threat Defense设备
- Cisco Secure Firewall Threat Defense 容器实例，位于 Firepower 4100/9300
- 使用 eStreamer 将事件数据导出到外部客户端。

设备强化

有关可用于进一步强化系统的功能的信息，请参阅最新版本的 *Cisco Firepower* 管理中心强化指南 和 *Cisco Cisco Secure Firewall Threat Defense* 强化指南，以及本文档中的以下主题：

- 许可证，第 239 页
- 管理中心 的，第 113 页
- 登录到管理中心，第 27 页
- 审核日志，第 43 页
- 审核日志 ID证书，第 46 页
- 时间同步，第 99 页
- 在 《Cisco Secure Firewall Management Center 设备配置指南》中为威胁防御配置 NTP 时间同步
- 创建邮件警报响应，第 537 页
- 配置入侵事件的邮件警报，第 546 页
- 在《Cisco Secure Firewall Management Center 设备配置指南》中配置 *SMTP*

- 关于在 《Cisco Secure Firewall Management Center 设备配置指南》中适用于 *Firepower 1000/2100* 的 *SNMP*
- 在《Cisco Secure Firewall Management Center 设备配置指南》中配置 *SMTP*
- 创建 SNMP 警报响应， 第 533 页
- 《Cisco Secure Firewall Management Center 设备配置指南》中的配置动态 *DNS*
- DNS 缓存， 第 53 页
- 审核和系统日志， 第 389 页
- 访问列表， 第 40 页
- 安全认证合规性， 第 311 页
- 为远程存储配置 SSH， 第 95 页
- 审核日志 ID证书， 第 46 页
- HTTPS 证书， 第 60 页
- 自定义 Web 界面的用户角色， 第 185 页
- 添加或编辑内部用户， 第 118 页
- 会话超时， 第 97 页
- 关于在 《Cisco Secure Firewall Management Center 设备配置指南》中配置系统日志
- 计划 管理中心 备份， 第 469 页
- 《Cisco Secure Firewall Management Center 设备配置指南》中的适用于 威胁防御的站点间 *VPN*
- 《Cisco Secure Firewall Management Center 设备配置指南》中的远程接入 *VPN*
- 《Cisco Secure Firewall Management Center 设备配置指南》中的*FlexConfig* 策略

保护您的网络

请参阅以下主题以了解可配置用于网络保护的功能：

- 访问控制策略
- 《Cisco Secure Firewall Management Center 设备配置指南》安全情报
- 《Cisco Secure Firewall Management Center 设备配置指南》侵策略使用入门
- 使用《Cisco Secure Firewall Management Center 设备配置指南》规则调整入侵策略
- 自定义《Cisco Secure Firewall Management Center 设备配置指南》入侵规则
- 更新入侵规则， 第 218 页
- 《Cisco Secure Firewall Management Center 设备配置指南》入侵事件日志记录的全局限制

- 《Cisco Secure Firewall Management Center 设备配置指南》传输层和网络层预处理器
- 《Cisco Secure Firewall Management Center 设备配置指南》具体威胁检测
- 《Cisco Secure Firewall Management Center 设备配置指南》应用层预处理器
- 审核和系统日志，第 389 页
- 入侵事件，第 749 页
- 事件搜索，第 671 页
- 工作流程，第 633 页
- 《Cisco Secure Firewall Management Center 设备配置指南》设备管理
- 登录标识，第 69 页
- 更新，第 211 页

启用安全认证合规

此配置适用于 Cisco Secure Firewall Management Center 或托管设备：

- 对于 Cisco Secure Firewall Management Center，此配置是系统配置的一部分。
- 对于托管设备，将 管理中心 中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

⚠

注意 启用此设置后，您将无法将其禁用。如果设备需要退出 CC 或 UCAPL 模式，必须重新映像。

开始之前

- 在任何设备上启用安全认证合规性之前，我们建议注册您计划让其成为部署到管理中心的一部分的所有设备。
- Cisco Secure Firewall Threat Defense 设备不能使用评估许可证；您的 智能软件管理器 账户必须启用出口管制功能。
- Cisco Secure Firewall Threat Defense 设备必须在路由模式下部署。
- 您必须是管理员用户才能执行此任务。

过程

步骤 1 根据配置的是 管理中心 还是典型托管设备，请执行以下操作：

- 管理中心： 选择 **系统**（⚙）> **配置**。
- 威胁防御 设备：选择 **设备** > **平台设置** 并创建或编辑 Cisco Secure Firewall Threat Defense 策略。

步骤 2 点击 **UCAPL/CC 合规性 (UCAPL/CC Compliance)**。

注释 在您启用UCAPL或CC合规性时设备会重启。管理中心在您保存系统配置时重启；托管设备在您部署配置更改时重启。

步骤 3 要在设备上永久启用安全认证合规性，您有两种选择：

- 要在通用条件模式中启用安全认证合规性，请从下拉列表中选择 **CC**。
- 要在统一功能获批产品列表模式中启用安全认证合规性，请从下拉列表中选择 **UCAPL**。

步骤 4 点击**保存 (Save)**。

下一步做什么

- 根据认证实体提供的本产品指南中的说明，确定其他配置更改。
- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

第 III 部分

运行状态监控

第 10 章

控制面板

以下主题介绍如何在 Firepower 系统中使用控制面板：

关于控制面板

控制面板为您提供当前系统状态的概览视图，包括有关系统收集和生成的事件的数据。您还可以使用控制面板了解有关部署中的设备的状态和整体运行状况的信息。请记住，控制面板提供的信息取决于如何许可、配置和部署系统。

注释 确保您已启用 REST API（**系统 (System)** > **配置 (Configuration)** > **REST API 首选项 (REST API Preferences)**）以在控制面板上查看相关设备指标。

提示 控制面板是一种复杂、高度可定制的监控功能，用于提供详尽的数据。要了解受监控网络的广泛、简短和多种多样的概况，请使用情景管理器。

控制面板使用选项卡显示构件：提供对系统的不同方面的见解的小型独立组件。例如，预定义的“设备信息”构件会提供有关设备名称、型号和当前运行的软件版本的信息。系统通过控制面板时间范围限制构件，可以将其更改为反映短至前一小时或长至前一年的时间段。

系统随附若干可以使用和修改的预定义控制面板。如果用户角色具有控制面板访问权限（“管理员”[Administrator]、“维护用户”[Maintenance User]、“安全分析师”[Security Analyst]、“安全分析师（只读）”[Security Analyst (Read Only)] 和具有控制面板权限的自定义角色），则默认情况下主页是预定义的“摘要控制面板”(Summary Dashboard)。但是，可以配置其他默认主页，包括非控制面板。您还可以更改默认控制面板。请注意，如果用户角色无法访问控制面板，则默认主页与角色相关；例如，发现管理员可以查看“网络发现”(Network Discovery) 页面。

您还可以使用预定义控制面板作为自定义控制面板的基础，可以将其共享或限制为专用。除非您具有管理员访问权限，否则无法查看或修改其他用户创建的专用控制面板。

注释 某些事件的深入查看页面和表视图包含一个 **Dashboard** 工具栏链接，您可以点击查看相关的预定义控制面板。如果删除预定义控制面板或选项卡，则关联的工具栏链接将不起作用。

在多域部署中，无法从祖先域查看控制面板；但是，可以创建新控制面板，这些控制面板是较高级别控制面板的副本。

Firepower 系统控制面板构件

控制面板有一个或多个选项卡，每个选项卡都会以三列布局显示一个或多个构件。Firepower 系统附有许多预定义的控制面板构件，每个构件均提供对 Firepower 系统不同方面的洞察。构件分为三类：

- 分析和报告构件：显示有关 Firepower 系统收集和生成的事件的数据。
- 其他构件：不显示事件数据和运营数据。目前，该类别中仅有的一个构件显示 RSS 源。
- 运行构件：显示有关 Firepower 系统的状态和整体运行状况的信息。

可以查看的控制面板构件取决于：

- 使用的设备类型
- 用户角色
- 当前的域（在多域部署中）

此外，每个控制面板都有一组可确定其行为的首选项。

您可以将构件最小化和最大化，在选项卡中添加和删除构件，以及在选项卡上重新排列构件。

注释 对于显示某个时间范围内的事件数的构件而言，事件的总数可能无法反映可在“分析”菜单下的页面上的表中查看其详细数据的事件数量。因为系统有时会删掉较旧的事件详情以管理磁盘空间使用情况，所以会发生这种情况。要将事件详情删除的情况降到最少，您可以微调事件日志记录，以只记录对部署最重要的事件。

构件可用性

您可以查看的控制面板构件取决于使用的设备类型、用户角色和当前域（在多域部署中）。

在多域部署中，如果看不到希望看到的构件，请切换到全局域。请参阅切换域 Cisco Secure Firewall Management Center，第 21 页。

请注意：

- 无效构件是由于使用错误类型的设备而无法查看的构件。
- 未授权构件是由于用户帐户没有必要的权限而无法查看的构件。

例如，“设备状态”构件仅在管理中心上对具有管理员、维护用户、安全分析师或安全分析师（只读）账户权限的用户可用。

虽然无法将未授权或无效的构件添加到控制面板，但是已导入的控制面板可能包含未授权或无效的构件。例如，如果已导入的控制面板满足以下条件，则此类构件可能存在：

- 由具有不同访问权限的用户创建，或者
- 属于祖先域。

不可用构件处于禁用状态，并且显示表明无法查看这些构件的原因的错误消息。

当此类构件超时或出现其他问题时，各个构件也会显示错误消息。

注释 您可以删除或最小化未授权和无效的构件，以及不显示数据的构件。请注意，在共享控制面板中对某个构件的修改会对该设备的所有用户适用。

按用户角色划分的控制面板构件可用性

下表列出了查看各个构件所需的用户帐户权限。只有具备管理员、维护用户、安全分析师或安全分析师（只读）权限的用户帐户才能使用控制面板。

具有自定义角色的用户可能可访问构件的任何组合，也可能都不能访问，具体取决于其用户角色是否许可。

表 *24:* 用户角色和控制面板构件可用性

构件	管理员	维护用户	安全分析师	安全分析师（只读
设备信息	是	是	是	是
设备状态	是	是	是	否
相关事件	是	否	是	是
当前接口状态	是	是	是	是
当前会话	是	否	否	否
自定义分析	是	否	是	是
磁盘使用率	是	是	是	是
接口流量	是	是	是	是

构件	管理员	维护用户	安全分析师	安全分析师（只读）
入侵事件	是	否	是	是
网络合规性	是	否	是	是
产品许可	是	是	否	否
产品更新	是	是	否	否
RSS 源	是	是	是	是
系统负载	是	是	是	是
系统时间	是	是	是	是
允许 列出事件	是	否	是	是

预定义控制面板构件

Firepower 系统随附若干预定义构件，当在控制面板上使用时，可以为您提供当前系统状态的概览视图。这些视图包括：

- 有关系统收集和生成的事件的数据
- 有关部署中的设备的状态和整体运行状况的信息

注释 可以查看的控制面板构件取决于使用的设备、用户角色以及在多域部署中的当前域。

设备信息构件

“设备信息”(Appliance Information) 构件可提供设备的快照。默认情况下，该构件显示在 **详细控制面板** 和 **摘要控制面板**的“状态”选项卡上。

如果在高可用性中配置了 管理中心，则 管理中心 中的设备信息构件会显示有关 管理中心 高可用性的信息。例如，它显示有关 管理中心 角色、状态、详细状态和上次联系人的信息。该构件提供：

- 设备名称、IPv4 地址、IPv6 地址和型号
- 在有控制面板的设备上安装的系统软件、操作系统、Snort、规则更新、规则包、模块包、思科漏洞数据库 (VDB) 和地理位置更新的版本信息，但 management center virtual 除外。
- 受管设备与管理设备的通信链路的名称和状态

通过修改构件首选项以显示简单或高级视图，您可以配置构件显示更多或更少信息；首选项还可控制构件的更新频率。

设备状态构件

“设备状态”(Appliance Status) 构件指示设备及其所管理的任何设备的运行状况。请注意，由于 管理中心不会自动将运行状况策略应用于受管设备，因此必须将运行状况策略手动应用于设备上，否则设备状态会显示为禁用。默认情况下，此构件显示在“详细控制面板”(Detailed Dashboard) 和“摘要控制面板”(Summary Dashboard) 的“状态”(Status) 选项卡上。

通过修改构件首选项，您可以配置构件以饼形图或表格形式显示设备状态。

首选项还可控制构件的更新频率。

您可以点击饼形图上的某个部分或设备状态表的一个数字转到Health Monitor页面，并查看设备及其所管理的任何设备的编译后的运行状况状态。

关联事件构件

“关联事件”构件按照优先级显示控制面板时间范围内每秒发生关联事件的平均次数。默认情况下，此构件显示在“详细控制面板”的“关联”选项卡上。

通过修改构件首选项，可以配置构件以显示不同优先级的关联事件，并选择线性（增量）或对数（十倍）比例。

选中一个或多个**优先级 (Priorities)** 复选框，以分别显示特定优先级事件的图形，包括不具有优先级的事件。选择**全部显示 (Show All)** 以显示所有关联事件的图形，无论其优先级如何。首选项还可控制构件的更新频率。

您可以点击某个图形查看特定优先级的关联事件，也可以点击**所有**图形查看所有关联事件。在任何一种情况下，事件均受到控制面板时间范围的限制；通过控制面板访问关联事件会更改设备的事件（或全局）时间窗口。

当前接口状态构件

Current Interface Status 构件显示设备上所有接口的状态，已启用或未使用。在 管理中心上，您可以显示管理（`eth0`、`eth1`等）接口。在受管设备上，可以选择仅显示感知（`s1p1` 等）接口或同时显示管理和感知接口。接口按类型分组：管理、内联、被动、已交换、已路由、 和未使用。

对于每个接口，该构件都会提供：

- 接口的名称
- 接口的链路状态
- 接口的链路模式（例如，100Mb 全双工或 10Mb 半双工）
- 接口类型，例如铜或光纤
- 接口接收 (Rx) 和发送 (Tx) 的数据量

代表链路状态的球的颜色指明当前状态，如下所示：

- 绿色：链路正常并且全速运行
- 黄色：链路正常，但未全速运行

- 红色：链路不正常
- 灰色：链路通过管理方式禁用
- 蓝色：链路状态信息不可用（例如，ASA）

构件首选项可控制构件的更新频率。

当前会话构件

“当前会话”(Current Sessions) 构件显示哪些用户目前已经登录设备、与发起会话的机器相关的 IP 地址，以及各用户最近一次访问设备页面的时间（基于设备的本地时间）。代表用户，也就是说，当前查看构件的用户，会以**用户图标**标记并渲染为粗体。在注销或变成不活动状态后一小时内，会话会从构件数据中删除。默认情况下，此构件显示在“详细控制面板”(Detailed Dashboard) 和“摘要控制面板”(Summary Dashboard) 的“状态”(Status) 选项卡上。

在“当前会话”(Current Sessions) 构件上，您可以：

- 点击任何用户名以管理“用户管理”(User Management) 页面上的用户帐户。
- 点击任何 IP 地址旁边的 **主机图标** 或 **受损主机图标** 以查看关联计算机的主机配置文件。
- 点击任何 IP 地址或访问时间以查看该 IP 地址以及与该 IP 地址关联的用户登录 Web 界面的时间所限制的审核日志。

构件首选项可控制构件的更新频率。

自定义分析构件

“自定义分析”构件是一款高度可自定义的构件，可用于显示系统收集和生成的事件的详细信息。

该构件随附多个预设，可用于快速访问有关部署的信息。预定义控制面板对这些预设进行广泛使用。您可以使用这些预设或创建自定义配置。至少，自定义配置可指定您感兴趣的数据（表和字段），以及该数据的汇聚方法。您还可以设置其他与显示相关的首选项，包括是否要以相对发生率（条形图）或随时间推移（曲线图）的形式显示事件。

该构件基于本地时间显示其最近更新的时间。构件的更新频率取决于控制面板的时间范围。例如，如果您将控制面板时间范围设置为 1 小时，则构件每五分钟更新一次。另一方面，如果将控制面板时间范围设置为一年，则构件每周更新一次。要确定控制面板何时进行下次更新，请将光标悬停在构件左下角的**上次更新时间**通知上方。

注释 以红色阴影显示的“自定义分析”(Custom Analysis) 构件表示其正在危害系统性能。如果构件继续保持红色，请移除该构件。也可以在系统配置中的“控制面板”(Dashboard) 设置禁用所有“自定义分析”(Custom Analysis) 构件（**系统 [System]** > **配置 [Configuration]** > **控制面板 [Dashboard]**）

显示事件的相对发生率（条形图）

对于“自定义分析”(Custom Analysis) 构件中的条形图，构件背景中的彩色条显示每个事件的相对出现次数。请从右到左阅读彩色条。

方向图标 指示和控制显示的排序顺序。向下指向的图标表示降序；向上的图标表示升序。要更改排序顺序，请点击图标。

在每个事件旁边，构件可以显示三个图标中的其中一个，以显示最近结果中的任何更改：

- 新事件图标 **添加**（＋） 表示该事件对结果而言是第一次发生。
- **向上箭头图标** 表示该事件的排名自上次构件更新以来已经上移。该图标旁边会显示指示事件上移了多少个位置的数字。
- **向下箭头图标** 表示该事件的排名自上次构件更新以来已经下移。该图标旁边会显示指示事件下移了多少个位置的数字。

显示一段时间内的事件（曲线图）

如果您想了解时间范围内的事件或其他所收集数据的信息，您可以配置 Custom Analysis 构件显示一个线形图，例如显示时间范围内配置中所生成的入侵事件总数的线形图。

“自定义分析”(Custom Analysis) 构件的限制

“自定义分析”(Custom Analysis) 构件可能会指示您无权查看配置显示的数据。例如，“维护用户”(Maintenance Users) 无权查看发现事件。又例如，构件不会显示与未许可的功能相关的信息。但是，您（以及共享控制面板的任何其他用户）可以修改构件的首选项以显示您可以看到的数据，或者甚至是删除构件。如果您希望确保不发生这种情况，请将控制面板另存为专用控制面板。

当查看用户数据时，系统只会显示授权用户。

当查看 URL 类别信息时，系统不会显示未归类的 URL。

在查看由**计数** 汇聚的入侵事件时，计数包含已审核的入侵事件；如果在“分析”菜单下的页面上的表格中查看计数，计数则不会包含已审核的事件。

注释 在多域部署中，系统会为每个枝叶域构建单独的网络映射。因此，枝叶域可以包含这样一个 IP 地址，该地址在它的网络内是唯一的，但与另一枝叶域中的 IP 地址完全相同。查看祖先域中的“自定义分析”(Custom Analysis) 构件时，可显示该重复 IP 地址的多个实例。初看上去，似乎是重复条目。但是，如果向下展开到每个 IP 地址的主机配置数据，则系统会显示它们属于不同的枝叶域。

如何为设备创建控制面板构件

任何显示设备事件的构件都可以配置为使用过滤器来限制给定设备或一组设备的事件显示。

1. 创建并保存搜索：转到 **分析** > **搜索** 并输入搜索参数以匹配特定设备名称。

注释 您必须提供精确的文本匹配，因为没有列出已部署设备名称的下拉列表。

2. 转至 **概述** > **控制面板** > **添加构件** 以创建 **自定义分析** 构件。

3. 返回 **概述** > **控制面板** 并修改新构件以使用搜索范围进行自定义。

示例：自定义分析构件的配置

通过将“自定义分析“构件配置为显示 **入侵事件** 表中的数据，可以将该构件配置为显示最近入侵事件的列表。选择 **分类** 字段并通过 **计数** 来汇聚此数据来展示生成的每种类型的事件数量。

另外，通过 **唯一事件** 合计来展示每种类型有多少个入侵事件（例如，检测到多少网络木马、可能违反公司政策的情况、试图拒绝服务攻击，等等）。

您还可以使用已保存的搜索（无论是设备随附的其中一个预定义搜索还是您创建的自定义搜索）来进一步自定义构件。例如，使用 **已丢弃事件** 搜索限制第一个示例（使用 **分类**，通过 **技术** 合计的入侵事件）来展示每一种类型中有多少个入侵事件已丢弃。

相关主题

修改控制面板时间设置，第 338 页

自定义分析构件首选项

下表介绍可以在“自定义分析”(Custom Analysis) 构件中设置的首选项。

不同的首选项根据构件的配置方式进行显示。例如，如果将构件配置为显示事件的相对发生次数（条形图）与一段时间内的图形（曲线图），则会显示一组不同的首选项。仅在选择从中显示数据的特定表时，才会显示某些首选项，例如过滤器。

表 *25:* 自定义分析构件首选项

偏好	详细信息
标题	如果不指定构件的标题，则设备使用已配置的事件类型作为标题。
预设	“自定义分析”(Custom Analysis) 预设提供有关部署的信息的快速访问。预定义控制面板对这些预设进行广泛使用。您可以使用这些预设或创建自定义配置。
表 (Table)（必要）	包含构件显示的数据的事件或资产的表。
字段 (Field)（必要）	要显示的事件类型的特定字段。要显示一段时间内的数据（曲线图），请选择**时间 (Time)**。要显示事件的相对发生次数（条形图），请选择其他选项。
汇聚 (Aggregate)（必要）	汇聚方法配置构件对显示数据的分组方法。对于大多数事件类型，默认选项为**计数 (Count)**。
过滤器	可以使用应用过滤器限制“应用统计信息”(Application Statistics) 表和“按应用划分的入侵事件统计信息”(Intrusion Event Statistics by Application) 表中的数据。

偏好	详细信息
搜索	可以使用已保存的搜索限制构件显示的数据。您必须指定搜索，不过，有些预设使用预定义搜索。 只有您才能访问另存为专用的搜索。如果在共享控制面板上配置构件，并使用专用搜索限制其事件，则构件会重置为当其他用户登录时不使用搜索。这也会影响构件的视图。如果您希望确保不发生这种情况，请将控制面板另存为专用控制面板。 只有限制连接摘要的字段才能基于连接事件限制“自定义分析”(Custom Analysis) 控制面板构件。无效的已保存搜索会灰显。 如果您使用已保存的搜索限制 Custom Analysis 构件，该构件在下一次更新之前不会反映更改。
显示	选择是要显示最频繁（**顶部**）还是最不频繁（**底部**）发生的事件。
结果	选择要显示的结果行数。
显示移动器	选择是否要显示表示最新结果中的更改的图标。
时区	选择要用于显示结果的时区。
颜色	可以更改构件的条形图中的条形颜色。

相关主题

配置构件首选项，第 336 页

从自定义分析构件查看关联事件

在自定义分析构件中，可以调用事件视图（工作流程），其中提供有关该构件中显示的事件的详细信息。事件显示在该事件类型的默认工作流程中，受到控制面板时间范围限制。根据所配置的时间窗口数量和事件类型，这还会更改 管理中心上的相应时间窗口。

例如：

- 如果配置多个时间窗口，然后从自定义分析构件访问运行状况事件，则事件会显示在默认运行状况事件工作流程中，并且运行状况监控时间窗口会更改为控制面板时间范围。
- 如果配置单个时间窗，然后从自定义分析构件访问任意类型的事件，则事件会显示在该事件类型的默认工作流程中，并且全局时间窗口会更改为控制面板时间范围。

过程

有以下选项可供选择：

- 在任意自定义分析构件上，点击构件右下角的 **视图**（ ） 以查看构件首选项限制的所有关联事件。

- 在显示事件的相对发生（条形图）的自定义分析构件上，点击任意事件以查看构件首选项以及该事件所限制的关联事件。

磁盘使用率构件

根据磁盘使用类别，“磁盘使用率”(Disk Usage) 构件显示硬盘驱动器的空间使用比例。它还会显示设备硬盘驱动器上的空间使用比例及其每个分区的容量。如果“磁盘使用量”构件安装在设备中，或者如果 管理中心管理某个包含恶意软件包的设备，则该构件会显示相同的恶意软件存储包信息。默认情况下，该构件在“默认”(Default) 控制面板和“摘要”(Summary) 控制面板的“状态”(Status) 选项卡中显示。

“按类别”(By Category) 堆积条形图显示每个磁盘使用率类别在使用的总可用磁盘空间中的比例。下表列出了可用的类别。

表 *26*: 磁盘使用率类别

磁盘使用率类别	说明
事件	系统记录的所有事件
文件 (Files)	系统存储的所有文件
备份	所有备份文件
更新 (Updates)	与更新相关的所有文件，例如规则更新和系统更新
其他	系统故障排除文件和其他文件
空闲	设备上剩余的可用空间

您可以将指针悬停在“按类别”(By Category) 堆积条形图中的磁盘使用率类别上，以查看该类别使用的可用磁盘空间的比例、磁盘上的实际存储空间，以及该类别的总可用磁盘空间。请注意，如果您安装了一个恶意软件存储包，“文件”(Files) 类别的总可用磁盘空间为恶意软件包上的可用磁盘空间。

如果您安装了恶意软件存储包，您可以通过修改构件首选项配置构件仅显示“按类别”(By Category) 堆积条形图和管理员 (`/`)、`/Volume`、`/boot` 分区使用情况，以及 `/var/storage`分区。

构件首选项还可以控制构件的更新频率，以及其显示的是当前磁盘使用情况还是在控制面板时间范围内收集的磁盘使用情况统计数据。

接口流量构件

“接口流量”(Interface Traffic) 构件显示在设备的管理接口上接收的流量速率 (Rx) 和传输的流量速率 (Tx)。默认情况下，该构件不会在任何预定义控制面板上显示。

已启用 恶意软件防御 许可证的设备会定期尝试连接到 AMP 云，即使尚未配置动态分析也如此。因此，这些设备会显示已传输流量；这也是预期行为。

构件首选项可控制构件的更新频率。

入侵事件构件

“入侵事件”(Intrusion Events)构件可显示发生在控制面板时间范围内的入侵事件（按优先级组织）。这包括有丢弃数据包和不同影响的入侵事件的统计数据。默认情况下，该构件显示在“摘要控制面板”(Summary Dashboard) 的“入侵事件”(Intrusion Events) 选项卡上。

在构件首选项中，您可以选择：

- **事件标志 (Event Flags)**，以便为包含已丢弃数据包、本应丢弃数据包或产生特定影响的事件显示单独的图表。选择**全部 (All)** 以显示所有入侵事件的额外图表，无论影响或规则状态如何。

  有关图标的说明，请参阅入侵事件，第 749 页。影响级别数字上方显示的箭头（如有）说明内联结果，定义方式如下：

  表 *27:* 工作流程和表视图中的内联结果字段内容

此图标	表明
	系统已丢弃触发规则的数据包。
	如果已启用入侵策略选项**内联时丢弃**（在内联部署中），或在系统进行修建时“丢弃并生成”规则生成了该事件，那么 IPS 应该已丢弃该数据包。
	IPS 可能已将数据包传输或传送到目的地，但包含此数据包的连接现在已被阻止。
无图标（空）	触发的规则未设置为“丢弃并生成事件”

  无论入侵策略的规则状态或内联丢弃行为如何（包括当内联接口处于分流模式的情况），系统在被动部署中都不会丢弃数据包。

- **显示**可指定**每秒平均事件数** (EPS) 或**事件总数**。
- **垂直比例 (Vertical Scale)** 以指定**线性 (Linear)**（增量）或**对数 (Logarithmic)**（十倍）比例
- 构件的更新频率。

在构件上，您可以：

- 点击与已丢弃数据包、本应丢弃数据包或特定影响相对应的图形以查看该类型的入侵事件。
- 点击对应于已丢弃事件的图形可查看已丢弃事件。
- 点击与本应丢弃事件相对应的图形可查看本应丢弃事件。
- 点击**全部 (All)** 图形可查看所有入侵事件。

所发生的事件视图受到控制面板时间范围的限制；通过控制面板访问入侵事件可能会更改设备的事件（或全球）时间段。请注意，被动部署的数据包不会丢弃，无论入侵规则状态或入侵策略的内联丢包行为如何。

网络合规性构件

“网络合规性”构件总结主机符合您配置的 allow 名单的情况。默认情况下，该构件会显示有关活跃关联策略中的所有合规 allow 名单列出的合规、不合规，以及未评估的主机数量的饼形图。默认情况下，此构件显示在“详细控制面板”(Detailed Dashboard) 的“关联”(Correlation) 选项卡上。

您可以通过修改构件首选项配置构件显示所有 allow 名单或具体 allow 名单的合规性。

如果您选择显示所有 allow 名单的网络合规性，而一旦其不符合某个有效的关联策略中的任何 allow 名单，则构件会将主机视为不合规。

您还可以使用构件首选项以指定您想使用三种不同风格中的哪一种来显示网络合规性。

网络合规性 (Network Compliance) 风格（默认）显示有关合规、不合规及尚未评估的主机数量的饼形图。您可以点击该饼形图以查看主机违规数，它会列出至少违反一个 allow 名单的主机。

一段时间内的网络合规性百分比 (Network Compliance over Time [%]) 风格显示有关控制面板时间范围内合规、不合规及尚未评估的主机相对比例的堆叠区域图。

一段时间内的网络合规性 (Network Compliance over Time) 风格显示有关控制面板时间范围内合规、不合规及尚未评估的主机数量的曲线图。

构件首选项可控制构件的更新频率。您可以选中**显示未评估 (Show Not Evaluated)** 复选框以隐藏未评估的活动。

产品许可构件

Product Licensing 构件可显示当前安装于管理中心上的设备和功能许可证。它还指示获得许可的项目数以及允许的剩余许可项目数。默认情况下，该构件不会在任何预定义控制面板上显示。

构件的顶部显示在 管理中心上安装的所有设备和功能许可证，包括临时许可证，而“过期许可证”部分则仅显示临时且已到期的许可证。

构件背景中的长条显示正在使用的各种许可证的比例；您应该从右到左阅读这些长条。已到期许可证标有一条删除线。

您可以通过修改构件首选项配置构件显示所有当前许可的功能，或者显示您可以许可的所有功能。首选项还可控制构件的更新频率。

您可以点击任何一种许可证类型发往本地配置的 License 页面并添加或删除功能许可证。

产品更新构件

“产品更新”(Product Updates) 构件为您提供当前安装在设备上的软件摘要和您已经下载但未安装的更新的信息摘要。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

由于构件使用预定任务确定最新版本，因此会显示 `Unknown`，直到您将预定任务配置为下载、推送或安装更新。

通过修改构件首选项，您可以配置构件以隐藏最新版本。首选项还可控制构件的更新频率。

构件也会为您提供可以更新软件的页面链接。您可以执行以下操作：

- 通过点击当前版本来手动更新设备。
- 通过点击最新版本来创建预定任务以下载更新。

RSS 源构件

RSS Feed 构件可向控制面板添加一个 RSS 源。默认情况下，该构件可显示思科安全新闻的信息源。默认情况下，该构件显示在 详细控制面板 和 摘要控制面板的“状态”选项卡上。

您还可以配置构件显示公司新闻的预配置摘要、Snort.org 博客，或思科威胁研究博客，或者也可以指定其在构件首选项的 URL 以创建任何其他 RSS 源的自定义连接。仅当使用由 管理中心 识别的证书颁发机构 (CA) 签名的受信任服务器证书时， 管理中心 才能显示加密的 RSS 源。如果将“RSS 源”构件配置为显示使用 管理中心 无法识别的 CA 的加密 RSS 源，或者使用自签名证书，则验证会失败，并且构件不会显示源。

信息源每 24 小时（但您可以手动更新摘要）更新一次，而且，构件会根据设备的本地时间显示最近一次更新信息源的时间。请记住，设备必须访问（两个预配置摘要的）网站或您配置的任何自定义信息源。

当您配置构件时，您还可以选择您想要在构件中显示多少个案例，以及是否想要在标题下显示案例说明；记住，并非所有的 RSS 源都会使用说明。

在“RSS 源”(RSS Feed) 构件中，您可以：

- 点击信息源中的某个案例查看案例
- 点击 **more** 链接转到信息源的网站
- 点击 **更新**（ ） 手动更新信息源

系统负载构件

“系统负载”(System Load) 构件可显示设备当前及控制面板时间范围内的（每个 CPU）CPU 使用率、内存 (RAM) 使用情况和系统负载（又称为平均负载，通过等待运行的进程数量衡量）。默认情况下，该构件显示在 详细控制面板 和 摘要控制面板的“状态”选项卡上。

您可以通过修改构件首选项来配置构件显示或隐藏平均负载。首选项还可控制构件的更新频率。

系统时间构件

“系统时间”(System Time) 构件可显示本地系统时间、正常运行时间和设备启动时间。默认情况下，该构件显示在 详细控制面板 和 摘要控制面板的“状态”选项卡上。

通过修改构件首选项，您可以配置构件以隐藏启动时间。首选项还会控制构件与设备的时钟同步的频率。

允许 名单事件构件

允许 名单事件构件按照优先级显示控制面板时间范围内每秒内事件发生的平均次数。默认情况下，此构件显示在“默认控制面板”(Default Dashboard) 的“关联”(Correlation) 选项卡上。

通过修改构件首选项，您可以配置构件以显示不同优先级的 allow 名单事件。

在构件首选项中，您可以：

- 选择一个或多个**优先级 (Priorities)** 复选框，以显示特定优先级事件的图形，包括不具备优先级的事件
- 选择 **全部显示** 以显示所有 allow 名单事件的其他图形，无论其优先级如何
- 选择**垂直刻度 (Vertical Scale)** 以选择**线性 (Linear)**（增量）或**对数 (Logarithmic)**（十倍）比例

首选项还可控制构件的更新频率。

您可以点击某个图形查看特定优先级的 allow 名单事件，或者点击 **全部** 图形查看所有 allow 名单事件。在任何一种情况下，事件均受到控制面板时间范围的限制；通过控制面板访问 allow 列表事件可更改的事件（或全局） 管理中心时间窗口。

管理控制面板

过程

步骤 1 选择**概述** > **控制面板**，然后从菜单中选择要修改的控制面板。

步骤 2 管理控制面板：

- 创建控制面板 - 创建自定义控制面板；请参阅创建自定义控制面板 ， 第 336 页。
- 删除控制面板 - 要删除控制面板，请点击要删除的控制面板旁边的 **删除**（  ） 。如果删除默认控制面板，则必须定义新的默认控制面板，否则设备会在您每次尝试查看控制面板时提示您选择控制面板。
- 编辑选项 - 编辑自定义控制面板选项；请参阅编辑控制面板选项 ， 第 338 页。
- 修改时间限制 - 修改时间显示或暂停/取消暂停控制面板，如修改控制面板时间设置 ， 第 338 页中所述。

步骤 3 添加（请参阅 添加控制面板 ， 第 335 页）、删除（点击 **关闭**（  ））和重命名（请参阅 重命名控制面板 ， 第 340 页）控制面板。

注释 不能更改控制面板的顺序。

步骤 4 管理控制面板构件：

- 添加构件 - 向控制面板中添加构件；请参阅将构件添加到控制面板 ， 第 335 页。
- 配置首选项 - 配置构件首选项；请参阅配置构件首选项 ， 第 336 页。
- 自定义显示 - 自定义构件显示；请参阅自定义构件显示 ， 第 338 页。

- 查看事件 - 查看“自定义分析”(Custom Analysis) 构件中的关联事件；请参阅从自定义分析构件查看关联事件，第 329 页。

提示 思科预定义控制面板中的“自定义分析”(Custom Analysis) 构件的每个配置都与该构件的系统预设相对应。如果您更改或删除了其中一个构件，您可以通过根据适当的预设创建一个新的 Custom Analysis 来恢复它。

添加控制面板

过程

步骤 1 查看要修改的控制面板；请参阅查看仪表板，第 340 页。

步骤 2 点击 **添加**（+）。

步骤 3 输入名称。

步骤 4 点击**确定 (OK)**。

将构件添加到控制面板

每个选项卡都可以三列布局显示一个或多个构件。向控制面板添加构件时，必须选择要向其添加构件的选项卡。系统会自动将其添加到构件最少的一列。如果所有列的构件数量均相同，新的构件会被添加到最左边的一列。您最多可以添加 15 个构件到控制面板选项卡中。

提示 在添加构件后，您可以将其移到选项卡的任何位置。但是，不能在选项卡之间移动构件。

可以查看的控制面板构件取决于正在使用的设备类型、用户角色和当前域（在多域部署中）。请记住，因为并非所有用户角色都有权访问所有控制面板构件，权限较低的用户查看权限较高的用户创建的控制面板时，可能无法使用控制面板上的部分构件。尽管未授权的构件仍将在控制面板上显示，但它们会被禁用。

过程

步骤 1 查看要添加构件的控制面板；请参阅查看仪表板，第 340 页。

步骤 2 点击要添加构件的选项卡。

步骤 3 点击 **Add Widgets**。您可以点击类别名称查看每个类别中的构件，也可以点击**所有类别 (All Categories)** 查看所有构件。

步骤 4 点击要添加的构件旁边的**添加 (Add)**。“添加构件”(Add Widgets) 页面会显示每种类型有多少个构件在选项卡上，包括您要添加的构件。

提示 要添加多个相同类型的构件（例如，您可能希望添加多个 RSS Feed 构件，或多个 Custom Analysis 构件），可再次点击 **Add**。

步骤 5 构件添加完毕后，点击**完成 (Done)** 返回到控制面板。

下一步做什么

- 如果添加的是“自定义分析”(Custom Analysis) 构件，请配置构件首选项；请参阅配置构件首选项，第 336 页。

相关主题

构件可用性，第 322 页

配置构件首选项

每个构件都有一组可确定其行为的首选项。

过程

步骤 1 在您想要更改首选项的构件标题栏上，点击 **显示首选项**（ ）。

步骤 2 根据需要进行更改。

步骤 3 在构件标题栏上，点击 **隐藏首选项**（ ） 隐藏首选项部分。

创建自定义控制面板

提示 无需创建新的控制面板，可以从其他设备中导出控制面板，然后将其导入您的设备中。随后，可以编辑所导入的控制面板以满足自身需求。

过程

步骤 1 选择**概述** > **控制面板** > **管理**。

步骤 2 点击 **Create Dashboard**。

步骤 3 修改自定义控制面板选项，如自定义控制面板选项，第 337 页中所述。

步骤 4 点击**保存 (Save)**。

自定义控制面板选项

下表介绍在创建或编辑自定义控制面板时可以使用的选项。

表 *28*: 自定义控制面板选项

选项	说明
复制控制面板 (Copy Dashboard)	创建自定义控制面板时，您可以选择是否将其基于任何现有控制面板（无论是用户创建的还是系统定义的都如此）。此选项会创建预先存在的控制面板的副本，您可以修改该副本以满足需求。或者，可以通过选择**无 (None)** 创建空白的新控制面板。仅在创建新控制面板时，此选项才可用。 在多域部署中，您可以从祖先域复制任何非专用控制面板。
名称 (Name)	自定义控制面板的唯一名称。
说明	自定义控制面板的简短说明。
选项卡更改频率 (Change Tabs Every)	指定控制面板循环使用其选项卡的频率（以分钟为单位）。除非您暂停控制面板或控制面板上只有一个选项卡，否则该设置会在您指定的时间间隔将视图转至下一个选项卡。要禁用选项卡循环，请将 0 输入**选项卡更改频率 (Change Tabs Every)** 字段中。
页面刷新频率 (Refresh Page Every)	确定整个控制面板页面自动刷新的频率。 刷新整个控制面板可以让您查看自上一次控制面板更新以来，其他用户对共享控制面板所作的，或者您对另一台计算机上的专用控制面板所作的任何首选项或布局更改。例如，在控制面板始终显示的网络运营中心 (NOC) 中，频繁刷新可能非常有用。如果在本地计算机对控制面板的进行更改，则 NOC 中的控制面板会按照指定的间隔自动刷新，并且无需手动刷新。 该“更新”不更新数据，您不需要更新整个控制面板以查看数据更新；各个构件会根据其首选项进行更新。 此值必须大于**选项卡更改频率 (Change Tabs Every)** 设置。除非您暂停控制面板，否则该设置将在您指定的时间间隔刷新整个控制面板。要禁用定期页面刷新，请将 0 输入**页面刷新频率 (Refresh Page Every)** 字段中。 **注释** 此设置与许多单个构件上的可用更新间隔分离；虽然刷新控制面板页面会重置单个构件上的更新间隔，但是构件将根据其各自的首选项进行更新，即使禁用**页面刷新间隔 (Refresh Page Every)** 设置也如此。
另存为专用 (Save As Private)	确定自定义控制面板是可由设备的所有用户查看和修改还是与您的用户帐户相关联并专门保留供自己使用。请记住，无论角色如何，具有控制面板访问权限的任何用户都可以修改共享控制面板。如果您希望确保只有您可以修改特定控制面板，请将其保存为专用控制面板。

自定义构件显示

您可以将构件最小化和最大化，以及在选项卡上重新排列构件。

过程

步骤 1 查看控制面板；请参阅查看仪表板，第 340 页。

步骤 2 自定义构件显示：

- 要在选项卡上重新排列构件，请点击要移动的构件的标题栏，然后将其拖到新位置。

  注释 不能在选项卡之间移动构件。如果您想要构件显示在不同的选项卡上，您必须将其从现有选项卡中删除，并将其添加到新的选项卡上。

- 要将控制面板上的构件最小化或最大化，请点击构件的标题栏中的 **最小化**（ ）或 **最大化**（ ）。
- 如要在选项卡上不再查看构件时删除该构件，请点击构件的标题栏中的 **关闭**（ ）。

编辑控制面板选项

过程

步骤 1 查看要编辑的控制面板；请参阅查看仪表板，第 340 页。

步骤 2 点击 **编辑**（ ）。

步骤 3 如自定义控制面板选项，第 337 页中所述更改选项。

步骤 4 点击**保存 (Save)**。

修改控制面板时间设置

您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。当您更改时间范围时，可按时间限制构件自动更新以反映新的时间范围。

任何图形中的最大数据点数为 300，时间设置确定在每个数据点内汇总的时间。以下是每个时间范围的控制面板中的数据点数量和覆盖的时间范围：

- 1 小时 = 12 个数据点，每个数据点 5 分钟
- 6 小时 = 72 个数据点，每个数据点 5 分钟
- 1 天 = 288 个数据点，每个数据点 5 分钟

- 1 周 = 300 个数据点，每个数据点 33.6 分钟
- 2 周 = 300 个数据点，每个数据点 67.2 分钟
- 30 天 = 300 个数据点，每个数据点 144 分钟
- 90 天 = 300 个数据点，每个数据点 432 分钟
- 180 天 = 300 个数据点，每个数据点 864 分钟
- 1 年 = 300 个数据点，每个数据点 1752 分钟

请注意，并非所有的构件都可受时间限制。例如，控制面板时间范围对设备信息构件无影响，该构件可提供包括设备名称、型号和当前版本的 Firepower 系统软件的信息。

请记住，对于Firepower系统的企业部署而言，将时间范围更改为长周期可能对“自定义分析”(Custom Analysis) 之类的构件无效，具体取决于新事件取代旧事件的频率。

您还可以暂停控制面板，这可以让您检查构件提供的数据，而无需更改和中断您的分析的显示。暂停控制面板具有以下影响：

- 各个构件停止更新，而不管任何**更新间隔 (Update Every)** 构件首选项设置如何。
- 控制面板选项卡停止循环，无论控制面板属性中的**循环选项卡间隔 (Cycle Tabs Every)** 设置如何。
- 控制面板页面停止刷新，无论控制面板属性中的**刷新页面间隔 (Refresh Page Every)** 设置如何。
- 更改时间范围无效。

当您完成分析时，您可以取消控制面板暂停。恢复控制面板运行会使得页面上的所有相应的构件更新以反映当前时间范围。此外，控制面板选项卡会恢复循环，控制面板页面会根据您在控制面板属性中指定的设置进行刷新。

如果出现中断控制面板系统信息流的连接问题或其他问题，控制面板会自动暂停，并显示错误通知，直至问题解决为止。

注释 您的会话一般会在 1 小时（或其他配置的时间间隔）的非活动期后注销，无论控制面板是否暂停。如果您计划长时间被动监控控制面板，您可考虑使某些用户免于会话超时，或更改系统超时设置。

过程

步骤 1 查看要添加构件的控制面板；请参阅查看仪表板 ，第 340 页。

步骤 2 或者，要更改控制面板时间范围，请从**显示最后时间 (Show the Last)** 下拉列表中选择时间范围。

步骤 3 或者，根据时间范围控制，使用 **暂停**（ ） 或 **播放**（ ）暂停或中止暂停控制面板。

重命名控制面板

过程

步骤 1 查看要修改的控制面板；请参阅查看仪表板，第 340 页。

步骤 2 点击要重命名的控制面板标题。

步骤 3 键入名称。

步骤 4 点击**确定 (OK)**。

查看仪表板

默认情况下，设备的主页会显示默认控制面板。如果您没有定义默认控制面板，主页会显示“控制面板管理”(Dashboard Management) 页面，您可以在此选择要查看的控制面板。

过程

可以随时执行以下操作之一：

- 要查看设备的默认控制面板，请选择**概述** > **控制面板**。
- 要查看特定控制面板，请选择**概述** > **控制面板**，然后从菜单中选择该控制面板。
- 要查看所有可用的控制面板，请选择**概述** > **控制面板** > **管理**。然后，您可以选择单个控制面板旁边的 **视图**（）来查看该控制面板。

第 11 章

运行状况

以下主题介绍如何在 Firepower 系统中使用运行状况监控：

运行状况监控的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

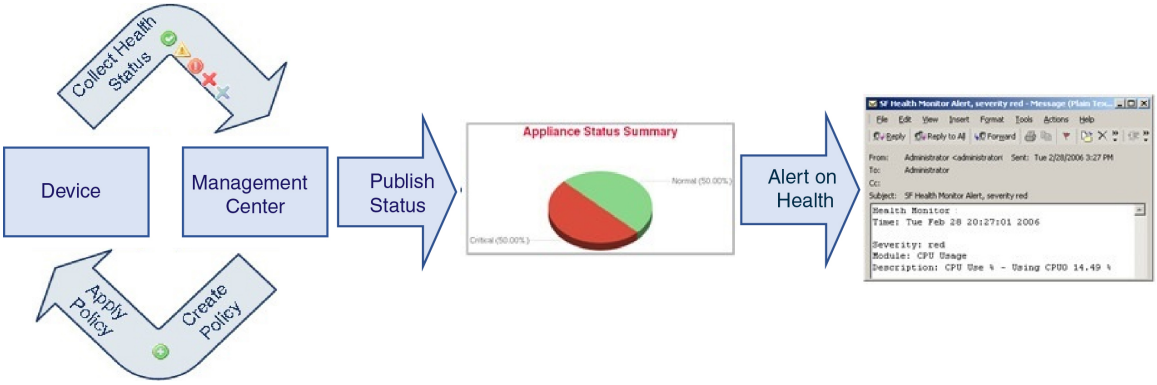
管理员

维护用户

关于运行状况监控

管理中心 上的运行状况监控器跟踪各种运行状况指标，以确保系统中的硬件和软件正常工作。您可以使用运行状况监控器检查整个系统部署中关键功能的状态。

您可以配置运行状况模块以发出警报的频率。管理中心还支持时间序列数据收集。您可以在设备及其运行状况模块上收集时间序列数据的频率。默认情况下，设备监控器会在多个预定义的运行状况监控器控制面板中报告这些指标。收集指标数据以供分析，因此没有与之关联的警报。



可以使用运行状况监控器创建一个测试集合（称为运行状况策略），并将该运行状况策略应用到一个或多个设备上。测试（称为 运行状况模块）是用来测试您指定的条件的脚本。您可以通过启用或禁用测试或者通过更改测试设置来修改运行状况策略，可以删除不再需要的运行状况策略。您还可以将来自所选设备的消息加入黑名单，从而排除这些消息。

运行状况监控系统按配置的时间间隔运行运行状况策略中的测试。您还可以按需运行所有测试或特定测试。运行状况监控器基于配置的测试条件收集运行状况事件。

运行状况模块有两种类型：基于传统的和基于电报的。

基于传统的运行状况模块监控某些系统的运行状况，例如风扇、电源和数据库完整性。当满足这些受监控系统的运行状况策略中指定的条件时，基于传统基础设施的运行状况模块会直接发出警报（绿色、红色或橙色），并显示一条短消息。

基于电报的运行状况模块监控检索受监控系统的指标信息的电报插件。您可以使用基于电报的运行状况模块的首选运行状况指标创建自定义控制面板，以便监控特定统计信息或解决特定问题。

注释 所有设备都通过“硬件警报“运行状况模块自动报告其硬件状态。管理中心还使用默认运行状况策略中配置的模块自动报告状态。某些运行状况模块（例如“设备测信号”模块）在 管理中心上运行并报告 管理中心的受管设备的状态。要使运行状况模块提供受管设备状态，必须将所有运行状况策略部署到设备。

可以使用运行状况监控器访问特定设备（在多域部署中，则是特定域）的整个系统的运行状态信息。“运行状况监控器”页面上的六边形图和状态表提供网络上所有设备（包括 管理中心）的状态的可视摘要。单个设备运行状况监视器使您可以向下钻取到特定设备的运行状况详细信息。

完全可自定义的事件视图使您可以快速轻松地分析运行状况监控器所收集的运行状况事件。这些事件视图使您可以搜索和查看事件数据，并访问可能与正调查的事件有关的其他信息。例如，如果要查看 CPU 使用率达到特定百分比的所有状况，您可以搜索 CPU 使用率模块并输入百分比值。

您还可以配置响应运行状况事件的邮件、SNMP 或者系统日志警报。运行状况警报是指标准警报和运行状况级别之间的关联。例如，如果想确保设备不会因硬件过载出现故障，您可以设置邮件警报。

然后，您可以创建运行状况警报，每当 CPU、磁盘或内存占用率达到您在该设备所应用的运行状况策略中配置的“警告”级别时，就会触发该邮件警报。您可以设置警报阈值，以最小化您收到的重复警报的数量。

注释 运行状况监控可能需要 5-6 分钟才能生成运行状况警报。

如果支持人员要求您为设备生成故障排除文件，您也可以执行此操作。

只有具有管理员用户角色权限的用户才可以访问系统运行状况数据。

高可用性对

在运行 6.7 或更高版本的 管理中心 高可用性部署中，活动 管理中心 会创建一个运行状况监控页面，该页面使用 REST API 显示基于指标的详细信息。备用 管理中心 创建运行状况监视器页面，该页面显示警报信息，并使用饼图和状态表提供网络上所有设备状态的可视化摘要。备用管理中心不显示基于指标的信息。

运行状况模块

运行状况模块或运行状况测试会测试您在运行状况策略中指定的条件。

表 *29*: 运行状况模块（所有设备）

模块	模块类型	说明
CPU 使用率（每个核心）	电报	该模块检查所有内核的 CPU 使用率是否超载，并在 CPU 使用率超过为该模块配置的阈值时发出警报。**警告阈值 %** 默认值为 `80`。**临界阈值 %** 默认值为 `90`。
磁盘状态	传统	该模块检测硬盘的性能和设备上的恶意软件存储包（如果已安装）。 当硬盘和 RAID 控制器（如果安装）存在发生故障的危险时，或者，如果安装的其他安装硬盘驱动器不是恶意软件包时，该模块生成“警告”(Warning)（黄色）运行状况警报。当无法检测到已安装恶意软件存储包时，该模块生成“警报”(Warning)（红色）运行状况警报。

模块	模块类型	说明
磁盘使用情况	电报	该模块将设备的硬盘驱动器和恶意软件存储包中的磁盘使用率与为该模块配置的限值进行对比，并在使用率超过为模块配置的阈值时发出警报。基于模块阈值，当系统删除过多的监控磁盘使用类别的文件，或者当这些类别以外的磁盘使用率达到过高级别时，该模块也发出警报。有关磁盘使用情况警报故障排除场景的信息，请参阅 磁盘使用率和事件消耗情况运行状况监控警报，第 418 页。 如果设备配置历史记录文件的大小超过允许的限制，则磁盘使用率模块会发送运行状况警报。有关磁盘使用情况警报的故障排除场景的信息，请参阅 设备配置历史记录文件的磁盘使用情况。 Cisco Secure Firewall Management Center 版本 7.2.0-7.2.5、7.3.x 和 7.4.0 不支持运行状况警报。 使用磁盘使用率运行状况模块监控设备上的 `/` 和 `/volume` 分区的磁盘使用率并跟踪耗尽频率。尽管磁盘使用率模块将 `/boot` 分区列为监控分区，但是分区的大小是静态的，因此该模块在引导分区中不发出警报。
文件系统完整性检查	传统	如果系统启用了 CC 模式或 UCAPL 模式，或者如果系统运行使用 DEV 密钥签名的映像，则此模块会执行文件系统完整性检查。默认情况下，该模块会被启用。
运行状况监视器流程	传统	该模块监控运行状况监视器本身的状态，并且如果管理中心最后收到运行状况事件后的分钟数超过“警告”或“严重”限值，则发出警报。
接口统计信息	传统	此模块确定设备当前是否收集流量并根据物理接口和汇聚接口的流量状态发出警报。对于物理接口，信息包括接口名称、链路状态和带宽。对汇聚接口，信息包括接口名称、活动链路的数量和总汇聚带宽。 **注释** 此模块还监控高可用性备用设备流量。虽然已知备用设备不会接收任何流量，但 管理中心 会发出警报，指出接口未接收任何流量。当端口通道上的某些子接口未收到流量时，应用相同的警报原则。 如果您使用 **show interface** CLI 命令来查看设备的接口统计数据，CLI 命令结果中的输入和输出速率可能会与接口模块中出现的流量速率有所不同。 此模块根据 Snort 性能监控的值显示流量速率。Snort 性能监控和管理中心接口统计信息的采样间隔不同。由于采样间隔的差异， 管理中心 GUI 中的吞吐量值可能与 威胁防御 CLI 结果中显示的吞吐量值不同。
本地恶意软件分析	传统	该模块监控本地恶意软件分析的 ClamAV 更新。

模块	模块类型	说明
内存使用率	传统	该模块将设备的内存使用率与为模块配置的限值进行对比，并在使用率超过为该模块配置的级别时发出警报。 在计算内存使用情况时， 管理中心 内存使用情况运行状况模块会监控并包括RAM、交换内存和缓存内存的使用情况。 对于内存超过4 GB的设备而言，基于一个公式来预设警报阈值，该公式计算在可能导致系统问题的可用内存中所占的比例。在内存超过4 GB的设备上，因为“警告”和“严重”阈值之间的时间间隔可能非常短，所以建议您将**警告阈值 % (Warning Threshold %)**值手动设置为50。这将进一步确保您及时收到设备的内存警报来解决问题。有关如何计算阈值的其他信息，请参阅运行状况监控器警报的内存使用阈值，第 416 页。 从版本 6.6.0 开始， management center virtual 升级到版本 6.6.0+ 所需的最低 RAM 为 28 GB， management center virtual 部署的建议 RAM 为 32 GB。我们建议您不要降低默认设置：为大多数 management center virtual 实例分配 32 GB RAM，为 management center virtual 300 分配 64 GB（仅限 VMware）。 **注意** • 当为 management center virtual 部署分配的 RAM 不足时，运行状况监控器会生成严重警报。 • 如果 管理中心 达到临界系统内存条件，则系统可能会终止使用大量内存的进程，或者如果内存使用率仍然很高，则重新启动 管理中心。 复杂的访问控制策略和规则可控制重要资源并对性能产生不利影响。
进程状态	传统	该模块确定设备上的进程是否在进程管理器外部退出或终止。 如果进程在进程管理器外部被故意退出，模块状态变更为“警告”(Warning)，并且运行状况事件消息指示哪一个进程被退出，直到该模块再次运行、该进程重新启动为止。如果进程在进程管理器外部异常终止或者崩溃，模块状态变更为“严重”(Critical)，并且运行状况事件消息指示被终止的进程，直到该模块再次运行、该进程重新启动为止。

模块	模块类型	说明
设备中威胁数据更新	传统	在 管理中心，设备用于检测威胁的某些情报数据和配置每 30 分钟会从云进行一次更新。 此模块会提醒您此信息在指定时间段内是否未在设备上更新。 监控的更新包括： • 本地 URL 类别和信誉数据 • 安全情报 URL 列表和源，包括全局阻止列表和 不阻止 列表以及来自威胁情报导向器的 URL • 安全情报网络列表和源 （IP 地址），包括全局阻止列表和 不阻止 列表以及来自威胁情报导向器的 IP 地址 • 安全情报 DNS 列表和源，包括全局阻止列表和 不阻止 列表以及来自威胁情报导向器的域。 • 本地恶意软件分析签名（来自 ClamAV） • 如**对象 > 对象管理 > 安全情报 > 网络列表和源**页面上列出的来自威胁情报导向器的 SHA 列表 • **集成 (Integration) > AMP > 动态分析连接 (Dynamic Analysis Connections)** 页面上配置的动态分析设置 • 与缓存 URL 到期相关的威胁配置设置，包括 **集成** > **其他集成** > **云服务** 页面上的缓存 URL 到期设置。（URL 缓存的更新不受此模块监控。） • 用于发送事件的 Cisco 云的通信问题。请参阅 **集成** > **其他集成 > 云服务** 页面上的 **Ciscco 云** 框。 **注释** 仅当已在系统上配置 TID 且拥有源的情况下才会包括威胁情报导向器更新。 默认情况下，此模块会在 1 小时后发送警告，在 24 小时后发送严重警报。 如果此模块显示管理中心或任何设备上发生故障，请验证管理中心是否可以访问这些设备。

表 *30:* 管理中心 运行状况模块

模块	模块类型	说明
面向终端的 AMP 状态	传统	如果 管理中心 在初始成功连接后无法连接到 AMP 云或 Cisco AMP 私有云，或者如果私有云无法联系公有 AMP 云，则该模块发出警报。如果您使用 Cisco Secure Endpoint 管理控制台撤销注册 AMP 云连接，该模块也发出警报。

模块	模块类型	说明
面向 Firepower 的 AMP 状态	传统	如果发生以下情况，则该模块发出警报： • 管理中心 无法联系 AMP 云（公有或私有） 或 Secure Secure Malware Analytics 云或设备，或 AMP 私有云无法联系公有 AMP 云。 • 用于连接的加密密钥无效。 • 设备无法联系 Secure Secure Malware Analytics 云或 Secure Secure Malware Analytics 设备以提交进行动态分析的文件。 • 根据文件策略配置，在网络流量中检测到大量文件。 如果 管理中心 丢失与互联网的连接，则系统最多可能需要 30 分钟生成一个运行状况警报。
设备心跳	传统	该模块确定设备是否正监听设备心跳并基于设备心跳状态发出警报。
数据库大小	传统	此模块检查配置数据库的大小，并在大小超过为该模块配置的值（以千兆字节为单位）时发出警报。
发现主机限制	传统	此模块确定 管理中心可以监控的主机数量是否即将达到限制，并基于为该模块配置的警告级别发出警报。有关详细信息，请参阅主机限制。
事件积压状态	传统	如果等待从设备传输到 管理中心的事件数据积压已持续增长超过 30 分钟，则该模块警报。 若要减少积压，请评估带宽并考虑减少记录的事件。
事件监控器	电报	该模块监控整体事件传入 管理中心速率。
事件流状态	传统	该模块监控管理使用 管理中心上事件流转换器的第三方客户端应用的连接。
硬件统计信息	电报	此模块监控 管理中心 硬件实体的状态，即风扇速度、温度和电源。当阈值超过配置的“警告”或“严重”限制时，此模块发出警报。
ISE 连接监控	传统	该模块监控 Cisco 身份服务引擎（ISE）和 管理中心之间的服务器连接状态。ISE 提供其他用户数据、设备类型数据、设备位置数据、SGT（安全组标记）和 SXP（安全交换协议）服务。
许可证监控	传统	该模块监控许可证到期情况。
管理中心 高可用性状态	传统	此模块会对 管理中心的高可用性状态进行监控和发出警报。如果尚未建立 管理中心高可用性，则 HA 状态为未设置高可用性。 **注释** 此模块将替换高可用性状态模块，其是之前提供的管理中心的高可用性状态。在版本 7.0 中，我们添加了受管设备的高可用性状态。
MySQL 统计信息	电报	此模块监控 MySQL 数据库的状态，包括数据库大小、活动连接数和内存使用情况。默认情况下已禁用。

模块	模块类型	说明
RadiusMQ 状态	电报	此模块收集 RabbitMQ 的各种统计信息。
RRD 服务器进程	传统	该模块确定存储时序数据的轮询数据服务器是否正常运行。如果自上次RRD服务器更新后其重新启动，则该模块将发出警报；如果在RRD服务器重新启动后连续更新的次数达到模块配置中指定的次数，则该模块将输入“严重”或“警告”状态。
领域 (Realm)	传统	允许为领域或用户不匹配设置警告阈值，包括： • 用户不匹配：系统不下载某个用户而是报告给 管理中心 。 造成用户不匹配通常是因为该用户属于不予下载至 管理中心。请回顾《Cisco Secure Firewall Management Center 设备配置指南》中介绍的信息。 • 领域不匹配：某个用户登录到某个域，而该域对应 管理中心未知的某个领域。 有关详细信息， 《Cisco Secure Firewall Management Center 设备配置指南》 。 当您尝试下载的用户数超过每个领域支持的最大下载用户数时，此模块还会显示运行状况警报。单一领域下载用户的最大数目取决于您的管理中心型号。 有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 用户限制
安全情报	传统	如果安全情报使用中且 管理中心无法更新源，或者源数据已损坏或不包含可识别的 IP 地址，该模块报警。 另请参阅设备上的威胁数据更新模块。
智能许可证监控	传统	该模块监控智能许可状态和警报，如果： • 智能许可证代理（智能代理）与智能软件管理器之间存在通信错误。 • 产品实例注册令牌已过期。 • 智能许可证使用情况不合规。 • 智能许可证授权或评估模式已过期。
Sybase 统计信息	电报	该模块监控上 管理中心Sybase 数据库的状态，包括数据库大小、活动连接数和内存使用情况。
时序数据 (RRD) 监视器	传统	该模块跟踪已损坏文件在存储时序数据（例如关联事件计数）的目录中的存在情况，并且在文件标记为已损坏和已移除时发出警报。
时间服务器状态	传统	此模块会监控 NTP 服务器的配置，并在 NTP 服务器不可用或 NTP 服务器配置无效时发出警报。 如果您收到来自此模块的严重警报，请选择 **系统**（⚙）> **配置** > **时间同步**，并检查警报中指定的 NTP 服务器的配置。

模块	模块类型	说明
时间同步状态	传统	该模块跟踪将 NTP 与 NTP 服务器上的时钟配合使用以获取时间的设备时钟的同步状态，并且在两个时钟的时间差超过十秒钟时发出警报。
未解析的组监控	传统	监控策略中使用的未解析组。
URL 过滤监视器	传统	如果 管理中心 未能成功完成以下操作，则此模块会发出警报： • 注册 Cisco 云。 • 从 Cisoc 云下载 URL 威胁数据更新。 • 完成 URL 查找。 您可以配置这些警报的时间阈值。 另请参阅设备上的威胁数据更新模块。

表 *31:* 设备运行状况模块

模块	模块类型	说明
AMP 连接状态	电报	如果 威胁防御 在初始成功连接后无法连接到 AMP 云或 Cisco AMP 私有云，或者如果私有云无法联系公有 AMP 云，则该模块发出警报。默认情况下已禁用。
AMP Threat Grid 连接	电报	在初始连接成功后，如果 威胁防御 无法连接到 AMP 威胁网格云，则模块警报。
ASP 丢弃	电报	该模块监控数据平面加速安全路径所放弃的连接。
自动应用旁路	传统	该模块监控绕过的检测应用。
机箱环境状态	传统	此模块监控机箱参数（例如风扇速度和机箱温度），并允许您设置温度的警告阈值和临界阈值。**关键机箱温度（摄氏度）**默认值为 85。**警告机箱温度（摄氏度）**默认值为 75。
集群/HA 故障转移状态	传统	该模块监控设备集群的状态。如果发生以下情况，则该模块发出警报： • 集群选举出新的主设备。 • 新的辅助设备会加入集群。 • 主设备或辅助设备会退出集群。

模块	模块类型	说明
配置资源利用率	传统	如果已部署的配置的大小使设备面临内存耗尽的风险，此模块会发出警报。 警报会显示您的配置需要多少内存，以及超出可用内存的数量。如果发生此情况，请重新评估您的配置。通常来说，您可以减少访问控制规则或入侵策略的数量或降低其复杂性。 **Snort 内存分配** • 总 *Snort* 内存表示为 威胁防御 设备上运行的 Snort 2 实例分配的内存。 • 可用内存 表示系统为 Snort 2 实例分配的内存。请注意，此值不仅是 总 *Snort* 内存 与为其他模块保留的组合内存之间的差。此值经过几次其他计算后得出，然后除以 Snort 2 进程数。 可用内存 值为负表示 Snort 2 实例没有足够的内存来部署配置。寻求支持，请联系 Cisco 技术支持中心 (TAC)。
连接统计信息	电报	此模块监控连接统计信息和 NAT 转换计数。
数据平面 CPU 使用率	电报	该模块检查设备上所有数据平面进程的平均 CPU 使用率是否超载，并在 CPU 使用率超过为该模块配置的百分比时发出警报。**警告阈值 %** 默认值为 80。**临界阈值 %** 默认值为 90。
Snort CPU 使用率	电报	该模块检查设备上所有 Snort 进程的平均 CPU 使用率是否超载，并在 CPU 使用率超过为该模块配置的百分比时发出警报。**警告阈值 %** 默认值为 80。**临界阈值 %** 默认值为 90。
系统 CPU 使用率	电报	该模块检查设备上所有系统进程的平均 CPU 使用率是否超载，并在 CPU 使用率超过为该模块配置的百分比时发出警报。**警告阈值 %** 默认值为 80。**临界阈值 %** 默认值为 90。
关键流程统计信息	电报	该模块监控关键进程的状态、资源消耗和重新启动计数。
已部署配置统计信息	电报	该模块监控有关已部署配置的统计信息，例如 ACE 数、IPS 规则数。
防火墙威胁防御平台故障	传统	此模块为 Firepower1000、2100 和 Cisco Secure Firewall 3100、4200 设备生成平台故障警报。故障是由 管理中心管理的可变对象。每个故障表示 威胁防御 实例中的一个故障或已发出的警报阈值。在一个故障的生命周期中，故障可从一个状态或一种严重性更改为另一个状态或另一种严重性。 每个故障包含有关发生故障时受影响对象的运行状态的信息。如果故障是临时性的并已得到解决，则对象会转换到正常运行状态。 有关详细信息，请参阅 *Cisco Firepower 1000/2100 FXOS* 故障和错误消息指南。
管理中心 访问配置更改	传统	该模块监控使用 **配置网络管理-数据-接口** 命令直接对 管理中心 设备执行的 FMC 访问配置更改
流分流统计信息	电报	该模块监控受管设备的硬件流分流统计信息。

模块	模块类型	说明
硬件告警	传统	该模块确定物理受管设备上的硬件是否需要更换并基于硬件状态发出警报。该模块还报告与硬件有关的守护程序的状态。
内联链路不匹配告警	传统	该模块监控与内联集相关的端口，并且如果内联对的两个接口协商不同的速度，则发出警报。
入侵和文件事件率	传统	该模块将每秒钟入侵事件的数量与为该模块配置的限值进行对比。如果超过限值，则该模块发出警报。如果入侵和文件事件速率为零，则入侵进程可能已关闭或者受管设备可能没有发送事件。选择**分析** > **入侵** > **事件**，检查是否正从该设备接收事件。 通常，网段的事件速率平均为每秒20个事件。对于具有本平均速率的网段，每秒事件（严重）数应设置为 50，每秒事件（警告）数应该设置为30。要确定系统的限值，请在设备的“统计信息”页面（**系统**（⚙） > **监控** > **统计信息**）找到“事件/秒”值，然后使用以下公式计算限值： • 每秒事件（严重）数 = “事件/秒”(Events/Sec) * 2.5 • 每秒事件（警告）数 = “事件/秒”(Events/Sec) * 1.5 您可以为每种限值设置的最大事件数是999，“严重”(Critical) 限值必须高于“警告”(Warning) 限值。
链路状态传播	传统	仅限于 ISA 3000。 该模块确定成对的内联集中链路发生故障的时间，并且触发链路状态传播模式。如果链路状态传播到该对，该模块的状态分类变更为“严重”，并且状态读作： `Module Link State Propagation: ethx_ethy is Triggered` 其中 x 和 y 为成对的接口编号。
内存使用率数据平面	电报	此模块检查数据平面进程使用的已分配内存百分比，并在内存使用率超过为该模块配置的百分比时发出警报。**警告阈值 %** 默认值为 80。**临界阈值 %** 默认值为 90。
Snort 的内存使用情况	电报	此模块检查 Snort 进程使用的已分配内存百分比，并在内存使用率超过为该模块配置的百分比时发出警报。**警告阈值 %** 默认值为 80。**临界阈值 %** 默认值为 90。
网卡重置	传统	该模块检查由于硬件故障而重新启动的网卡，并且在发生重置时发出警报。
NTP 统计信息	电报	该模块监控受管设备的 NTP 时钟同步状态。默认情况下已禁用。
电源	传统	该模块确定设备的电源是否需要更换，并基于电源状态发出警报。
路由统计信息	电报	该模块监控路由表的当前状态。
Snort3 统计信息	电报	该模块收集和监控 Snort 3 统计信息的事件，流和数据包。

模块	模块类型	说明
Snort 身份内存使用情况	传统	使您能够在内存使用率超过为模块配置的级别时为 Snort 身份处理和警报设置警告阈值。 **临界阈值 %** 默认值为 80。 此运行状况模块专门跟踪 Snort 中用于用户身份信息的总空间。它显示当前内存使用情况详细信息，用户到 IP 绑定的总数以及用户组映射详细信息。Snort 在文件中记录这些详细信息。如果内存使用情况文件不可用，则此模块的运行状况警报显示 等待数据。这可能发生在由于新安装或主要更新，从 Snort 2 切换到 Snort 3 或重新启动或主要策略部署而导致的 Snort 重启期间。根据运行状况监控周期以及当文件可用时，警告会消失，运行状况监控器会显示此模块的详细信息，其状态变为绿色。
Snort 重新配置检测	电报	如果设备重新配置失败，则该模块发出警报。此模块检测到 Snort 2 和 Snort 3 实例的重新配置失败。
Snort 统计信息	电报	该模块监控事件、流和数据包的 Snort 统计信息。
安全服务交换连接状态	电报	在初始连接成功后，如果 威胁防御 无法连接到 SSE 云，则模块警报。默认情况下已禁用。
威胁防御 HA（裂脑检查）	传统	此模块会对 威胁防御的高可用性状态进行监控和发出警报，并提供拆分情景的运行状况警报。如果尚未建立 威胁防御高可用性，则 HA 状态为未设置高可用性。
VPN 统计信息	电报	此模块监控 威胁防御 设备之间的站点到站点和 RA VPN 隧道。
XTLS 计数器	电报	该模块监控 XTLS/SSL 流、内存和缓存有效性。默认情况下已禁用。

配置运行状况监控

过程

步骤 1 确定要监控的运行状况模块，如运行状况模块，第 343 页中所述。

您可以为 Firepower 系统中的每种设备设定特定策略、仅为该设备执行适当的测试。

提示 要快速启用运行状态监控而不定义监控行为，可以应用为此目的提供的默认策略。

步骤 2 将运行状态策略应用到要跟踪运行状态的每台设备，如创建运行状况策略，第 353 页中所述。

步骤 3 （可选。）配置运行状况监控器警报，如创建运行状况监控器警报，第 365 页中所述。

您可以设置在运行状况级别达到特定运行状况模块的特定严重性级别时触发的邮件、系统日志或 SNMP 警报。

运行状况策略

运行状况策略包含可为若干模块配置的运行状况测试条件。您可以控制针对每个设备要运行的运行状况模块，并可配置每个模块运行的测试中所用的具体限值。

当配置运行状况策略时，由您决定是否为该策略启用每个运行状况模块。此外，还可以选择每个已启用模块每次评估进程运行状况时报告的运行状况的控制条件。

您可以创建在系统中每个设备上应用的一个运行状况策略、定制您计划在特定设备上应用的每个运行状况策略，或者使用为您提供的默认运行状况策略。

注释 注册设备时，管理中心 会自动为其分配默认运行状况策略。要取消运行状况策略与设备的关联，必须先将其他运行状况策略与其关联。设备必须分配至少一个运行状况策略。

默认运行状况策略

管理中心 设置过程会创建并应用初始运行状况策略，其中大多数（但不是全部）可用的运行状况模块均已启用。系统还会将此初始策略应用于添加到 管理中心的设备。

此 初始 运行状况策略基于 默认 运行状况策略，您既不能查看也不能编辑，但可以在创建自定义运行状况策略时进行复制。

升级和默认运行状况策略

升级 管理中心时，任何新的运行状况模块都将添加到所有运行状况策略，包括初始运行状况策略、默认运行状况策略和任何其他自定义运行状况策略。通常，新的运行状况模块以启用状态添加。

注释 要使新的运行状况模块开始监控和发出警报，请在升级后重新应用运行状况策略。

创建运行状况策略

如果要定制用于设备的运行状况策略，您可以创建一个新策略。策略中的设置初始填充您选定为新策略基础的运行状况策略的设置。您可以编辑策略以指定首选项，例如启用或禁用策略中的模块，根据需要更改每个模块的警报条件，并指定运行时间间隔。

过程

步骤 1 选择**系统**（⚙）> **运行状况 (Health)** > **策略 (Policy)** 。

步骤 2 点击**创建策略**。

步骤 3 输入策略的名称。

步骤 4 从 **基本策略** 下拉列表中选择要用作新策略基础的现有策略。

步骤 5 输入策略的说明。

步骤 6 选择**保存**。

下一步做什么

- 如 应用运行状况策略，第 354 页 中所述，对设备应用运行状况策略。
- 编辑策略以指定模块级策略设置，如 编辑运行状况策略，第 355 页中所述。

应用运行状况策略

当您将运行状况策略应用到设备时，您在策略中启用的所有模块的运行状况测试自动监控设备上的进程和硬件的运行状况。然后，运行状况测试继续以您在策略中配置的时间间隔运行，为设备收集运行状况数据并将该数据转发到 管理中心。

如果您在运行状况策略中启用一个模块，然后将该策略应用到不需要该运行状况测试的设备，则运行状况监控器报告该运行状况模块的状态为禁用。

如果您将启用所有模块的策略应用到设备中，它从该设备移除所有已应用的运行状况策略，以便不应用任何运行状况策略。但是，必须为设备分配至少一个运行状况策略。

当您将不同的策略应用到已应用策略的设备时，请基于新应用的测试在显示新数据时使用一些延迟。

过程

步骤 1 选择**系统**（⚙） > **运行状况 (Health)** > **策略 (Policy)** 。

步骤 2 点击要应用的策略旁边的 **部署运行策略** (🖳) 。

步骤 3 选择要应用运行状况策略的设备。

注释 必须为设备分配至少一个运行状况策略。要停止设备的运行状况监控，请创建一个所有模块都禁用的运行状况策略并将其应用到设备。要取消运行状况策略与设备的关联，必须先将其他运行状况策略与其关联。

步骤 4 点击**应用 (Apply)** 以将该策略应用到所选设备上。

下一步做什么

- 或者，监控任务状态；请参阅查看任务消息，第 415 页。

  如果成功应用该策略，设备监控便会开始。

编辑运行状况策略

您可以编辑要修改的运行状况策略。

过程

步骤 1 选择**系统**（⚙）> **运行状况 (Health)** > **策略 (Policy)** 。

步骤 2 点击要修改的策略旁边的 **编辑**（✎） 。

步骤 3 要编辑策略名称及其说明，请点击针对策略名称提供的 **编辑**（✎） 图标。

步骤 4 **运行状况模块** 选项卡显示所有设备模块及其属性。使用以下操作来配置运行状况模块：

- 点击针对模块及其属性提供的切换按钮-打开 （  ） 或关闭 （  ） 以分别启用或禁用运行状况测试。
- 要在运行状况模块上执行批量启用或禁用测试，请点击**全选 (Select All)** 切换按钮。

注释
- 模块和属性使用支持设备（威胁防御、管理中心 或两者）进行标记。
- 不能选择包含或排除 CPU 和内存模块的各个属性。

有关模块的信息，请参阅运行状况模块， 第 343 页。

步骤 5 酌情设置 **严重** 和 **警告** 阈值比例。

步骤 6 在 **设置** 选项卡中，在字段中输入相关值：

- **运行状况模块运行时间间隔**- 运行运行状况模块的频率。最小间隔为 5 分钟。
- **指标收集间隔**-在设备及其运行状况模块上收集时间序列数据的频率。默认情况下，设备监控器会在多个预定义的运行状况监控器控制面板中报告这些指标。有关控制面板的详细信息，请参阅 关于控制面板， 第 321 页。收集指标数据以供分析，因此没有与之关联的警报。
- **OpenConfig 流遥测**-配置从 威胁防御 设备到外部数据收集系统的运行状况指标遥测流，该系统使用供应商中立的 OpenConfig 模型。有关详细信息，请参阅 配置 OpenConfig 流传输遥测 。

步骤 7 要查看和修改已分配策略的设备，请执行以下操作：

a) 点击**策略分配和部署 (Policy Assignments & Deploy)**。
b) 从**可用设备 (Available Devices)** 列表中，点击要为其分配运行状况策略的设备旁边的 + 图标。
c) 点击**应用 (Apply)**。

或者，您也可以将允许状况策略应用到设备，如应用运行状况策略， 第 354 页中所述

将运行状况策略应用到要跟踪运行状况的每台设备上。当您将运行状况策略应用到设备时，您在策略中启用的所有模块的运行状况测试监控设备上的进程和硬件的运行状况，并将数据转发至 管理中心。

步骤 8 点击**保存 (Save)**。

删除运行状况策略

您可以删除不再需要的运行状况策略。但是，必须为设备分配至少一个运行状况策略。如果您删除仍然应用于设备的策略，直到您应用不同的策略，该策略设置仍然有效。此外，如果您删除应用到设备的运行状况策略，在您禁用基础的相关警报响应之前，该设备仍在生效的任何运行状况监控警报仍然处于活动状态。

提示 要停止设备的运行状况监控，请创建一个所有模块都禁用的运行状况策略并将其应用到设备。

过程

步骤 1 选择**系统**（⚙）> **运行状况 (Health)** > **策略 (Policy)** 。

步骤 2 点击要删除的策略旁边的 **删除**（🗑），然后点击**删除运行状况策略 (Delete health policy)** 将其删除。
系统将显示一则消息，指示删除是否成功。

使用 OpenConfig 发送供应商中立的遥测数据流

OpenConfig 是一个独立于供应商的软件层，它提供了一种将网络遥测数据传输到多个供应商以管理和监控网络的方式。Cisco Secure Firewall 中的 OpenConfig 流传输遥测选项使用 gNMI（gRPC 网络管理接口）协议，并允许您控制和生成从 威胁防御 设备到数据收集系统的遥测流。

防火墙威胁防御运行状况策略包含支持和启用 OpenConfig 流传输遥测功能的所有配置。在将运行状况策略部署到设备时，OpenConfig 流传输遥测配置会激活 gNMI 服务器并开始侦听来自数据收集器的远程过程调用 (RPC) 消息。

OpenConfig 流传输遥测的订用模型

OpenConfig 使用基于订用的模型，其中数据收集器会查询 威胁防御 设备，以便获取遥测数据或充当流式遥测数据的收集器。当数据收集器希望从 威胁防御 设备接收更新和指标时，它会向 威胁防御 gNMI 服务器发送 subscribeRequest RPC 消息。订用请求包括数据收集器要订用的一个或多个路径的详细信息。该消息还包括描述订用期限的订用模式。威胁防御 服务器支持以下订用模式：

- 一次订用 *(Once subscription)* - 威胁防御 设备只会向 gNMI 路径发送一次请求的数据。
- 流订用 *(Stream subscription)* - 威胁防御 会根据 `SubscribeRequest` RPC 消息中指定的触发器持续传输遥测数据。

- 采样的订用 *(Sampled subscription)* - 威胁防御 服务器会按照订用消息中指定的间隔来传输请求的数据。威胁防御支持的最小间隔为一分钟。
- 更改时订用 *(On-change subscription)* - 只要请求的值发生变化，威胁防御 就会发送数据。

威胁防御 服务器会根据所创建的订用类型以数据收集器请求的频率生成 `SubscribeResponse` RPC 消息。

OpenConfig 流传输遥测的部署模式

您可以使用以下部署模式进行 OpenConfig 流传输遥测配置：

- **拨入 (DIAL-IN)** - 在此模式下，gNMI 服务器会打开 威胁防御 上的端口并等待来自数据收集器的 `SubscribeRequest` RPC 消息。在设备运行状况策略中，可以指定 gNMI 服务器要使用的端口号，以及可与 gNMI 服务连接的数据收集器的 IP 地址。如未指定，则 gNMI 服务器将使用端口号 50051。拨入模式适用于订用遥测流的终端受信任的受信任网络。
- **拨出 (DIAL-OUT)** - gNMI 服务设计为在服务器模式下工作，在该模式下，它会接受来自 gNMI 数据收集器的订用请求并提供遥测数据。如果 gNMI 数据收集器无法访问 gNMI 服务器，则 威胁防御 会使用隧道客户端并与外部服务器建立 gRPC 隧道。该隧道允许在 gNMI 服务器和客户端之间交换 RPC 消息。当数据收集器托管在云上或受信任的网络外部时，非常适合使用拨出模式。

在拨入和拨出模式下，gNMI 服务器和 gNMI 客户端之间的所有通信都使用 TLS 加密，这需要生成一组带有私钥的证书以进行 TLS 加密。拨出模式需要额外的隧道基础设施密钥。有关详细信息，请参阅如何使用私钥生成证书。

生成新的证书和私钥

生成 OpenConfig 流传输遥测配置所需的 CA、服务器和客户端证书以及私钥集。

注释 要确保使用同一 CA 生成证书，请同时从同一终端运行以下命令。如果要重试命令，则必须重试所有命令。

开始之前

过程

步骤 1 在要运行以下命令的终端中创建一个文件夹，例如 `密钥` 。

示例：

```
mkdir keys
```

步骤 2 使用相应的私钥创建自签名 CA 证书。

示例：

以下示例命令会生成新的 RSA 私钥，并使用它创建具有提供的主题信息的自签名 X.509 证书：

```
openssl req -x509 -newkey rsa:4096 -days 365 -nodes -keyout keys/ca-key.pem -out
keys/ca-cert.pem -subj "/C=XX
/ST=YY/L=ZZZ/O=Example/OU=EN/CN=gnmi-ca/emailAddress=abc@example.com"
```

主题信息包括提供的国家/地区 (C)、省/自治区 (ST)、地区 (L)、组织 (O)、组织单位 (OU)、通用名称 (CN) 和邮件地址。

私钥保存为 `ca-key.pem` 文件，证书保存为 `keys` 文件夹中的 `ca-cert.pem` 文件。

步骤 3 使用指定的通用名称 (CN) 和使用者备用名称 (SAN) 创建自签名服务器证书：

示例：

以下示例命令会生成新的 RSA 私钥，并使用它创建具有提供的主题信息的自签名 X.509 证书。在本例中，192.168.0.200 是 威胁防御 设备的 IP 地址，192.168.0.202 是客户端的 IP 地址。

注释 如果要在拨入模式下使用此证书和密钥集，则不需要客户端 IP。

```
CN="192.168.0.200"
SAN="IP:192.168.0.200,IP:192.168.0.202"
openssl req -newkey rsa:4096 -nodes -keyout keys/server-key.pem -out keys/server-req.pem
-subj "/C=XX/ST=YY/L=ZZZ/O=Example/OU=EN/CN=${CN}/emailAddress=abc@example.com}"
openssl x509 -req -extfile <(printf "subjectAltName=${SAN}") -in keys/server-req.pem -days
 60 -CA keys/ca-cert.pem -CAkey keys/ca-key.pem -CAcreateserial -out keys/server-cert.pem
cat keys/server-key.pem keys/server-cert.pem keys/ca-cert.pem > keys/server-combined.pem
```

`openssl req` 命令会生成新的 RSA 私钥和证书签名请求 (CSR)。私钥保存为 `server-key.pem` 文件，CSR 保存为 `keys` 文件夹中的 `server-req.pem` 文件。

`openssl x509` 命令处理 CSR 并生成服务器证书。服务器证书在 `keys` 文件夹中另存为 `server-cert.pem` 文件。

`cat` 命令将服务器密钥、服务器证书和 CA 证书合并到一个名为 `server-combined.pem` 的文件中，并将该文件保存在 keys 文件夹中。

从 管理中心配置 **OpenConfig Streaming** 遥测时，必须上传 `server-combined.pem` 。在 威胁防御 和隧道服务器（拨出模式）上运行的 gNMI 服务器使用此证书进行 TLS 通信。如果使用密码加密私钥，请确保在将证书上传到 管理中心时指定密码。

步骤 4 使用指定的通用名称 (CN) 和使用者备用名称 (SAN) 创建客户端证书。

示例：

以下示例命令会生成新的 RSA 私钥，并使用它创建具有提供的主题信息的自签名 X.509 证书。在本例中，192.168.0.202 是客户端的 IP 地址。

```
CN="192.168.0.202"
SAN="IP:192.168.0.202"
openssl req -newkey rsa:4096 -nodes -keyout keys/client-key.pem -out keys/client-req.pem
-subj "/C=XX/ST=YY/L=ZZZ/O=example/OU=EN/CN=${CN}/emailAddress=abc@example.com"
openssl x509 -req -extfile <(printf "subjectAltName=${SAN}") -in keys/client-req.pem -days
 60 -CA keys/ca-cert.pem -CAkey keys/ca-key.pem -CAcreateserial -out keys/client-cert.pem
```

gNMI 客户端使用客户端证书 `client-cert.pem` 和私钥进行 TLS 通信。

步骤 5 （可选）对于拨出模式，请使用指定的通用名称 (CN) 和使用者备用名称 (SAN) 创建隧道服务器证书。

示例：

以下示例命令会生成新的 RSA 私钥，并使用它创建具有提供的主题信息的自签名 X.509 证书。在本例中，192.168.0.202 是客户端的 IP 地址。

```
CN="192.168.0.202"
SAN="IP:192.168.0.202"
openssl req -newkey rsa:4096 -nodes -keyout keys/tunnel-server-key.pem -out
keys/tunnel-server-req.pem -subj "
/C=XX/ST=YY/L=ZZZ/O=Example/OU=EN/CN=${CN}/emailAddress=abc@example.com}"
openssl x509 -req -extfile <(printf "subjectAltName=${SAN}") -in keys/tunnel-server-req.pem
 -days 60 -CA keys/ca-cert.pem -CAkey keys/ca-key.pem -CAcreateserial -out
keys/tunnel-server-cert.pem
```

配置 OpenConfig 流传输遥测

开始之前

- 确保要部署运行状况策略配置的 威胁防御 设备允许安装 SSL 证书和私钥。
- 确保配置支持 OpenConfig 流遥测实施的 gNMI 客户端，您可以从中向 威胁防御上的 gNMI 服务器发出 gRPC 请求。
- 要使用拨出模式并配置 OpenConfig 流遥测，请确保在管理系统上配置 gRPC 隧道服务器和客户端。此隧道配置启用 gNMI 客户端和 威胁防御 设备之间的通信。
- 要执行以下任务，您必须是管理员用户。

过程

步骤 1 选择 **系统** > **策略**。

步骤 2 点击要修改的威胁防御运行状况策略旁边的 **编辑运行状况策略** 图标。

步骤 3 转到 **设置** 选项卡。

步骤 4 移动 **OpenConfig 流遥测** 滑块以启用配置。默认情况下配置会被禁用。

步骤 5 上传 **SSL 证书**。gNMI 服务器使用此证书为 TLS 连接启用服务器身份验证，并加密通过通道的所有通信。

OpenConfig 流遥测配置仅支持 PEM 格式的证书。管理中心 执行以下证书验证，以确保设备和 gNMI 收集器之间的通信加密，而不会出现连接故障：

- 验证 ASCII 文本是否为有效的证书文件。
- 检查上传的证书的到期日期。
- 验证上传的 PEM 文件中的预期证书和私钥的数量。文件必须至少有一个证书，并且证书中的私钥数量必须始终为 1。
- 验证并接受密钥块类型 PRIVATE KEY、 RSA PRIVATE KEY、 ENCRYPTED PRIVATE KEY或 RSA ENCRYPTED PRIVATE KEY。

- 对于加密的 PEM 文件，验证 Proc-Type: 4,ENCRYPTED? 存在关键字。
- 验证密码对加密的 PEM 文件是否有效。

步骤 6 （可选）如果私钥文件已加密，请指定密码。

步骤 7 选择用于通过 gNMI 协议进行流传输遥测的部署模式。

对于 **拨入** 模式：

1. 为 gNMI 服务分配端口号。

   gNMI 服务器打开端口并等待来自收集器的 gRPC 请求。

2. 指定连接到 威胁防御 设备的 gNMI 收集器的 IPv4/IPv6 地址。
3. 点击 **添加收集器** 以添加更多 gNMI 收集器。您最多可以添加五个收集器。

对于 **拨出** 模式：

1. 指定 gNMI 收集器的主机名和端口号，该收集器可以从 威胁防御 设备订阅数据流遥测。
2. 点击 **添加收集器** 以添加更多 gNMI 收集器。您最多可以添加五个收集器。

步骤 8 指定用于验证 gNMI 收集器的用户名和密码。

收到 `SubscribeRequest` RPC 消息时， 威胁防御 服务器使用此凭证对 gNMI 收集器进行身份验证。每条遥测消息都不会使用用户名和密码进行身份验证。系统使用先前经过身份验证的加密流传输通道传输遥测消息。

步骤 9 点击**保存 (Save)**。

下一步做什么

将运行状况策略部署到 威胁防御 设备，以使配置更改生效。

OpenConfig 流传输遥测故障排除

由未知机构签名的证书

- 确保您已将正确的证书上传到 管理中心。
- 验证证书和密钥生成步骤。确保正确指定了 IP 使用者备用名称 (SAN)。

证书无效

如果 管理中心 显示错误“已请求 (IP)，但证书对 (IP) 无效”，请验证服务器证书和密钥生成步骤。

- 确保在服务器证书中正确指定 IP SAN。如果配置适用于多个 威胁防御 设备，则必须在 IP SAN 字段中指定所有设备。
- 如果使用的是拨出模式，请确保在服务器证书中指定客户端 IP。

未能生成响应对象

如果收到“未能生成响应对象，未收到任何数据”错误，则表示gNMI输入插件正在等待指标导出。以下是电报重新启动时显示的示例响应：

```
root@cronserver:/home/secanup/openconfig-test# gnmic -a $ADDRESS:$PORT --tls-cert $CLIENTCERT
 --tls-ca $CACERT --tls-key $CLIENTKEY -u $USER -p $PASS sub --mode once --path
"openconfig-system/system/memory"
rpc error: code = Aborted desc = Error in gnmi_server: failed to generate response object.did
 not receive any data
Error: one or more requests failed
```

等待 gNMI 输入插件重新启动，然后重试您的请求。

重启电报

当电报没有响应时，在 威胁防御 CLI 控制台上使用以下命令重新启动进程：

```
pmtool restartbyid hmdaemon
```

获取 gNMI 服务器的当前状态

启用 OpenConfig 流遥测后，要了解 gNMI 服务器的状态，请使用 威胁防御 CLI 控制台运行以下命令：

```
curl localhost:9275/OpenConfig/status
```

以下是对该命令的响应示例：

```
root@firepower:/home/admin# curl localhost:9275/openconfig/status
Mode (Dialin/Dialout): DialIn
Subscription Details:
    Active Subscription Details:
        Stream Mode Subscription Details:
            Total Stream Subscription Request Count: 1
            'Ip of Collector- Subscribe paths:'
                172.16.0.101:45826:
                - /openconfig-system/system/state/hostname
            Sample Subscription Count: 1
            On Change Subscription Count: 0
        Once Mode Subscription Details:
            Total Subscription Request Count: 0
            Total Subscription Count: 0
            'Ip of Collector- Subscribe paths:' : {}
    Total Subscription Details:
        Stream Mode Subscription Details:
            Total Stream Subscription Request Count: 1
            'Ip of Collector- Subscribe paths:' :
                 172.16.0.101:45826:
                 - /openconfig-system/system/state/hostname
        Sample Subscription Count: 1
        On Change Subscription Count: 0
    Once Mode Subscription Details:
        Total Subscription Request Count: 0
        Total Subscription Count: 0
        'Ip of Collector- Subscribe paths:': {}
```

运行状况监控中的设备排除

在正常的网络维护过程中，您禁用设备或使其暂时不可用。由于此类停运是有意而为，因此您不希望这些设备的运行状态影响 管理中心上的摘要运行状态。

您可以使用运行状况监视器排除功能禁用对设备或模块的运行状况监控状态报告。例如，如果您知道一个网段将不可用，因为到该网段上受管设备的连接失效，所以您可以临时禁用对该设备的运行状况监控，以禁止管理中心上的运行状况显示警告或严重状态。

当您禁用运行状况监控状态时，仍会生成运行状况事件，但是它们处于禁用状态，不会影响运行状况监视器的运行状况。如果您从排除名单移除设备或模块，排除过程中生成的事件继续显示禁用的状态。

要在设备上临时禁用运行状况事件，请转到排除配置页面并将设备添加至设备排除名单。在设置生效后，系统在计算整体运行状况时，不再考虑列入排除名单的设备。“运行状况监控设备状态摘要”(Health Monitor Appliance Status Summary) 列出处于禁用状态的设备。

您还可以禁用单个运行状况模块。例如，当在管理中心上达到主机限制时，可以将 主机限制状态消息禁用。

请注意，在“运行状况监控”主页面，如果您通过点击该状态行上的箭头来展开以查看具有特定状态的设备列表，就可以区分被排除的设备。

注释 在管理中心上，运行状况监视器排除设置是本地配置设置。因此，如果您将设备排除，接着将其删除，然后使用 管理中心重新注册，排除设置保持不变。最近重新注册的设备仍旧被排除。

从运行状况监控中排除设备

您可以单独或按组、型号或关联运行状况策略将设备排除。

如果需要将单个设备的事件和运行状况设置为禁用，您可以将该设备排除。在排除设置生效后，该设备在“运行状况监控设备模块摘要”中显示为已禁用，并且该设备的运行状况事件的状态为已禁用。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **排除**。

步骤 2 点击**添加设备**。

步骤 3 在 **设备排除** 对话框中的 **可用设备**下，点击 **添加**（⊕） 要从运行状况监控中排除的设备。

步骤 4 点击 **排除**。所选设备显示在排除项主页中。

步骤 5 要从排除项列表中删除设备，请点击 **删除**（🗑）。

步骤 6 点击**应用**。

下一步做什么

要排除设备上的单个运行状况策略模块，请参阅 排除运行状况策略模块，第 363 页。

排除运行状况策略模块

您可以将设备上的单个运行状况策略模块排除。您可能想要执行此操作以禁止来自模块的事件将设备的状态变更为警告或严重。

排除项设置生效后，设备会显示设备中从运行状况监控中排除的模块数量。

提示 确保您跟踪单独排除的模块，以便您可以在需要时重新激活它们。如果您意外地禁用模块，则可能漏掉所需的警告或严重消息。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **排除**。

步骤 2 点击要修改的设备旁边的 **编辑**（✎）。

步骤 3 在 **排除运行状况** 模块对话框中，默认情况下，设备的所有模块都从运行状况监控中排除。某些模块仅适用于特定设备；有关详细信息，请参阅运行状况模块，第 343 页。

步骤 4 要指定设备的排除持续时间，请从 **排除周期** 下拉列表中选择持续时间。

步骤 5 要选择要从运行状况监控中排除的模块，请点击 **启用模块级别排除** 链接。 **排除运行状况模块** 对话框显示设备的所有模块。默认情况下，禁用不适用于关联运行状况策略的模块。要排除模块，请执行以下操作：

1. 点击所需模块旁边的 **滑块**（  ）按钮。
2. 要指定所选模块的排除持续时间，请从 **排除周期** 下拉列表中选择持续时间。

步骤 6 如果为排除项配置选择 **排除周期** 而不是 **永久**，则可以选择在配置到期时自动将其删除。要启用此设置，请选中 **自动删除过期配置** 复选框。

步骤 7 点击**确定**。

步骤 8 在设备排除主页中，点击 **应用**。

过期的运行状况监控器排除项

当设备或模块的排除期限到期时，您可以选择清除或更新排除项。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **排除**。

设备上会显示 **警告**（⚠） 图标，指示从警报中排除设备或模块的持续时间到期。

步骤 2 要更新设备排除项，请点击设备旁边的 **编辑**（✎）。在 **排除运行状况模块** 对话框中，点击 **续约** 链接。使用当前值扩展排除期。

步骤 3 要清除排除设备，请点击设备旁边的 **删除**（🗑），点击 **从排除项中删除设备**，然后点击 **应用**。

步骤 4 要更新或清除模块排除项，请点击设备旁边的 **编辑**（✎）。在 **排除运行状况模块** 对话框中，点击 **启用模块级别排除** 链接，然后针对模块点击 **续约** 或 **清除** 链接。当您点击 **续约**时，模块上的排除期限将使用当前值延长。

运行状况监控器警报

您可以设置警报以在运行状况策略中的模块状态变更时，通过邮件、SNMP 或系统日志通知您。您可以将现有警报响应与运行状况事件级别相关联，以在特定级别的运行状况事件发生时触发和发出警报。

例如，如果您担心设备可能用尽硬盘空间，可以在剩余磁盘空间达到警告级别时自动向系统管理员发送一封邮件。如果硬盘驱动器继续加载，您可以在硬盘驱动器达到严重性级别时发送第二封邮件。

运行状况监控器警报信息

运行状况监视器生成的警报包含以下信息：

- 严重程度，指明警报的严重性级别。
- 模块，指定其测试结果触发警报的运行状况模块。
- 说明，包括触发警报的运行状况测试结果。

下表介绍了这些严重级别。

表 *32:* 警报严重性

严重性	说明
严重	运行状况测试结果符合触发“严重”(Critical) 警报状态的条件。
警告	运行状况测试结果符合触发“警告”(Warning) 警报状态的条件。
正常状态	运行状况测试结果符合触发“正常”(Normal) 警报状态的条件。
错误	运行状况测试未运行。

严重性	说明
已恢复	运行状况测试结果符合在“严重”(Critical) 或“警告”(Warning) 警报状态之后返回到正常警报状态的条件。

创建运行状况监控器警报

您必须是管理员用户才能执行此程序。

当您创建运行状况监控器警报时，您可以在严重性级别、运行状况模块和警报响应之间建立关联。您可以使用现有警报或特别配置新的警报以报告系统运行状况。当选定的模块发生严重性级别时，警报触发。

如果您以复制现有阈值的方式创建或更新阈值，将会收到冲突通知。当存在重复的阈值时，运行状况监控器使用生成最少警报的阈值并忽略其他阈值。该阈值的超时值必须介于 5 和 4,294,967,295 分钟之间。

开始之前

- 配置用于管理 管理中心与 SNMP、系统日志或邮件服务器（用于发送运行状况警报）通信的警报响应；请参阅Cisco Secure Firewall Management Center 警报响应，第 531 页。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控警报**。

步骤 2 点击 **Add**。

步骤 3 在 **添加运行状况警报** 对话框，在 **运行状况警报名称** 字段输入运行状况警报的名称。

步骤 4 从 **严重性** 下拉列表中，选择要用于触发警报的严重性级别。

步骤 5 从 **警报** 下拉列表中，选择在达到指定的严重性级别时要触发的警报响应。如果尚未 Cisco Secure Firewall Management Center 警报响应，请点击 **警报** 以访问 **警报** 页面并进行设置。

步骤 6 从 **运行状况模块** 列表中选择要为其应用警报的运行状况策略模块。

步骤 7 或者，在**阈值超时 (Threshold Timeout)** 字段中，输入在每个阈值期间结束和阈值计数重置之前应经过的分钟数。

即使策略运行时间间隔值小于阈值超时值，给定模块中报告的两个运行状况事件之间的间隔始终较大。例如，如果将阈值超时更改为 8 分钟，并且策略运行时间间隔为 5 分钟，则报告的事件之间的时间间隔为 10 (5 x 2) 分钟。

步骤 8 点击**保存 (Save)** 保存运行状况警报。

编辑运行状况监控器警报

您必须是管理员用户才能执行此程序。

您可以编辑现有运行状况监视器警报以更改与运行状况监控器警报相关的严重性级别、运行状况模块或警报响应。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控警报**。

步骤 2 点击针对您要修改的所需运行状况警报提供的 **编辑**（✎） 图标。

步骤 3 在 **编辑运行状况警报** 对话框中，从 **警报** 下拉列表中选择所需的警报条目，或点击 **警报** 链接以配置新的警报条目。

步骤 4 点击**保存 (Save)**。

删除运行状况监控器警报

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控警报**。

步骤 2 点击要删除的运行状况警报旁边的 **删除**（🗑） ，然后点击 **删除运行状况警报** 将其删除。

下一步做什么

- 禁用或删除基础警报响应，以确保不会继续发出警报；请参阅Cisco Secure Firewall Management Center 警报响应 ， 第 531 页。

关于运行状况监控器

您必须是管理员、运维或安全分析师用户才能执行此程序。

运行状况监控器为管理中心管理的所有设备以及管理中心提供已编译的运行状况。运行状况监控器由以下部分组成：

- 运行状况摘要页面 - 提供 管理中心 和 管理中心 管理的所有设备的运行状况概览视图。设备将单独列出，或根据其地理位置、高可用性或集群状态（如果适用）进行分组。
  - 将鼠标悬停在表示设备运行状况的六边形上时，可查看管理中心和任何设备的运行状况摘要。

- 设备左侧的点表示其运行状况：
  - 绿色 — 无警报。
  - 橙色 — 至少一个运行状况警告。
  - 红色 — 至少一个严重运行状况警报。

- 监控导航窗格 — 允许您导航设备层次结构。您可以从导航窗格查看各个设备的运行状况监控器。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控**。

步骤 2 在 **运行状况** 登录页面中查看 管理中心 及其受管设备的状态。

a) 将鼠标指针悬停在六边形上可查看设备的运行状况摘要。弹出窗口显示前五个运行状况警报的截断摘要。点击弹出窗口可打开运行状况警报摘要的详细视图。

b) 在设备列表中，点击 **展开**（>）和 **折叠**（⌄）以展开和折叠设备的运行状况警报列表。

展开该行时，系统将列出所有运行状况警报，包括状态、标题和详细信息。

注释 运行状况警报按严重性级别排序。

步骤 3 使用监控导航窗格访问设备特定的运行状况监控器。使用监控导航窗格时：

a) 点击 **主页** 返回运行状况摘要页面。

b) 点击**防火墙管理中心 (Firewall Management Center)** 以查看 Cisco Secure Firewall Management Center 本身的运行状况监控器。

c) 在设备列表中，点击 **展开**（>）和 **折叠**（⌄）以展开和折叠受管设备列表。

展开该行时，系统会列出所有设备。

d) 点击设备可查看设备特定的运行状况监控器。

下一步做什么

- 有关由管理中心管理的任何设备的已编译运行状况和指标的信息，请参阅设备运行状况监控器，第 371 页。
- 有关 管理中心运行状况的信息，请参阅使用 管理中心 运行状况监控器，第 368 页。

要随时返回运行状况登录页面，请点击 **主页**。

使用 管理中心 运行状况监控器

您必须是管理员、运维或安全分析师用户才能执行此程序。

管理中心 监控器提供 管理中心的运行状态的详细视图。运行状况监控器由以下部分组成：

- 高可用性（如果已配置）－高可用性 (HA) 面板显示当前 HA 状态，包括主用和备用设备的状态、上次同步时间和整体设备运行状况。
- 事件速率－“事件速率”面板将最大事件速率显示为基准，以及 管理中心接收的整体事件速率。
- 事件容量－“事件容量”面板按事件类别显示当前消耗量，包括事件的保留时间、当前事件容量与最大事件容量，以及容量溢出机制，其中 管理中心在存储的事件超出配置的最大容量时向您发出警报。
- 进程运行状况－“进程运行状况”面板提供关键进程的概览视图，以及一个选项卡，可让您查看所有已处理进程的状态，包括每个进程的 CPU 和内存使用情况。
- CPU－“CPU” 面板允许您在平均 CPU 使用率（默认）和所有核心的 CPU 使用率之间切换。
- 内存－“内存”面板显示 管理中心上的整体内存使用情况。
- 接口－“接口”面板显示所有接口的平均输入和输出速率。
- 磁盘使用－“磁盘”使用面板显示整个磁盘的使用情况，以及存储 管理中心 数据的关键分区的使用情况。
- 硬件统计信息－硬件统计信息显示管理中心机箱的风扇速度、电源和温度。有关详细信息，请参阅管理中心的硬件统计信息，第 370 页。

提示 在会话处于不活动状态达到 1 小时（或配置的其他时间间隔）之后，会话通常注销。如果计划长时间被动监控运行状态，请考虑免除某些用户发生会话超时，或者更改系统超时设置。有关详细信息，请参阅 添加或编辑内部用户，第 118 页 和 配置会话超时，第 97 页 。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控**。

步骤 2 使用 **监控** 导航窗格访问 管理中心 和设备特定的运行状况监控器。

- 独立 管理中心 显示为单个节点；高可用性 管理中心 显示为一对节点。
- 运行状况监控器可用于 HA 对中的主用设备和备用 管理中心 。

步骤 3 了解 管理中心 控制面板。

管理中心 控制面板包括 管理中心 的 HA 状态摘要视图（如果已配置），以及 管理中心 进程和设备指标（例如 CPU、内存和磁盘使用情况）的概览视图。

运行设备的所有模块

您必须是管理员、运维或安全分析师用户才能执行此程序。

在您创建运行状况策略时配置的策略运行时间间隔内，运行状况模块测试自动运行。但是，您也可以按需运行所有运行状况模块测试，以收集该设备的最新运行状况信息。

过程

步骤 1 查看设备的运行状况监控器。

步骤 2 点击**运行所有模块 (Run All Modules)**。状态栏指示测试进程，然后“运行状况监控设备”(Health Monitor Appliance) 页面刷新。

注释 当您手动运行运行状况模块时，第一次自动发生的刷新可能不会影响自动运行测试的数据。如果没有为您手动运行的模块更改该值，请等待几秒钟，然后点击设备名称来刷新该页面。您还可以等待页面再次自动刷新。

运行特定运行状况模块

您必须是管理员、运维或安全分析师用户才能执行此程序。

在您创建运行状况策略时配置的策略运行时间间隔内，运行状况模块测试自动运行。但是，您也可以按需运行一个运行状况模块测试以收集该模块的最新运行状况信息。

过程

步骤 1 查看设备的运行状况监控器。

步骤 2 在**模块状态摘要 (Module Status Summary)** 图形中，点击要查看的运行状况警报状态类别的颜色。

步骤 3 在要查看其事件列表的警报的**警报详细信息 (Alert Detail)** 行，请点击**运行 (Run)**。

状态栏指示测试进程，然后“运行状况监控设备”(Health Monitor Appliance) 页面刷新。

注释 当您手动运行运行状况模块时，第一次自动发生的刷新可能不会影响自动运行测试的数据。如果没有为您刚才手动运行的模块更改该值，请等待几秒钟，然后点击设备名称来刷新该页面。您还可以等待页面再次自动刷新。

生成运行状况模块警报图形

您必须是管理员、运维或安全分析师用户才能执行此程序。

您可以图表表示特定设备的特定运行状况测试的一段时间内的结果。

过程

步骤 1 查看设备的运行状况监控器。

步骤 2 在“运行状况监控设备”(Health Monitor Appliance) 页面的**模块状态摘要 (Module Status Summary)** 图形中，点击要查看的运行状况警报状态类别的颜色。

步骤 3 在要查看其事件列表的警报的 **Alert Detail** 行，请点击 **Graph**。

提示 如果未显示事件，您可能需要调整时间范围。

管理中心的硬件统计信息

管理中心设备（仅限物理）上的硬件统计信息包括有关其硬件实体的信息，例如风扇速度、电源和温度。要使 SNMP 轮询并发送陷阱以监控管理中心的运行状况，请执行以下操作：

1. 在管理中心启用 SNMP 以轮询 MIB。默认情况下，管理中心上的 SNMP 处于禁用状态。请参阅配置 SNMP 轮询，第 96 页。
2. 为每个启用陷阱所需的 SNMP 主机添加 ACL 条目。确保指定主机的 IP 地址，并将端口选择为 SNMP。请参阅配置访问列表，第 41 页。

要在 **运行状况** > **监控器** 页面上查看硬件统计信息，请执行以下操作：

1. 在 **运行状况** > **策略** 页面上，确保已启用硬件统计信息模块。您可以更改阈值默认值。
2. 将 Portlet 添加到管理中心运行状况监控控制面板 - 选择硬件统计信息指标组，然后选择风扇速度和温度指标。

您可以在 **运行状况监控** > **主页** 页面的防火墙管理中心下查看电源状态。

注释

- 风扇速度以 RPM 为单位显示。
- 温度以 °C （摄氏度）为单位显示。
- 当电源的一个插槽处于活动状态时，控制面板将其显示为 在线 ，另一个插槽显示为 无电源。
- 图中的每条水平线分别显示每个 PSU 和风扇的状态。
- 将鼠标悬停在图形上可查看该单个统计信息的数据。

设备运行状况监控器

设备运行状况监控器为 管理中心管理的任何设备提供已编译的运行状况。设备运行状况监控器收集 Firepower 设备的运行状况指标，以便预测和响应系统事件。设备运行状况监控器由以下组件组成：

- 系统详细信息 - 显示有关受管设备的信息，包括已安装的 Firepower 版本和其他部署详细信息。
- 故障排除和链接 - 提供常用故障排除主题和程序的便捷链接。
- 运行状况警报 - 运行状况警报监控器提供设备运行状况的概览视图。
- 时间范围 - 用于限制各种设备指标窗口中显示的信息的可调时间窗口。
- 设备指标 - 跨预定义控制面板分类的一系列关键 Firepower 设备运行状况指标，包括：
  - CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
  - 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。
  - 接口 - 接口状态和汇聚流量统计信息。
  - 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
  - Snort - 与 Snort 进程相关的统计信息。
  - 磁盘使用率 - 设备磁盘使用率，包括磁盘大小和每个分区的磁盘使用率。
  - 关键进程 - 与托管进程相关的统计信息，包括进程重新启动和其他选定的运行状况监控器，例如 CPU 和内存使用率。

有关受支持设备指标的完整列表，请参阅 Cisco Secure Firewall Threat Defense 运行状况指标。

查看系统详细信息和故障排除

您必须是管理员、运维或安全分析师用户才能执行此程序。

“系统详细信息”部分提供所选设备的常规系统信息。您还可以启动该设备的故障排除任务。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控**。

使用监控导航窗格访问设备特定的运行状况监控器。

步骤 2 在设备列表中，点击 **展开**（>）和 **折叠**（⌄）以展开和折叠受管设备列表。

步骤 3 点击设备可查看设备特定的运行状况监控器。

步骤 4 点击 **查看系统和故障排除详细信息...**的链接

默认情况下，此面板处于折叠状态。点击链接可展开折叠部分，以查看设备的 **系统详细信息** 和 **故障排除和链接** 。系统详细信息包括：

- **版本：** FirePOWER 软件版本。

- **型号：** 设备型号。
- **模式：** 防火墙模式。Firepower Threat Defense 设备面向普通防火墙接口支持两种防火墙模式：路由模式和透明模式。
- **VDB：** 思科漏洞数据库 (VDB) 版本。
- **SRU：** 入侵规则集版本。
- **Snort：** Snort 版本。

步骤 5 有以下故障排除选项可供选择：

- 生成故障排除文件；请参阅 为特定系统功能生成故障排除文件，第 421 页
- 生成和下载高级故障排除文件；请参阅 下载高级故障排除文件，第 422 页。
- 创建和修改运行状况策略；请参阅 创建运行状况策略，第 353 页。
- 创建和修改运行状况监控器警报；请参阅 创建运行状况监控器警报，第 365 页。

查看设备运行状况监控器

您必须是管理员、运维或安全分析师用户才能执行此程序。

设备运行状况监控器提供防火墙设备的运行状态的详细视图。设备运行状况监控器会编译设备指标，并在一系列控制面板中提供设备的运行状况和趋势。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控**。

使用监控导航窗格访问设备特定的运行状况监控器。

步骤 2 在设备列表中，点击 **展开**（>）和 **折叠**（⌄）以展开和折叠受管设备列表。

步骤 3 在设备名称右侧的页面顶部的警报通知中查看设备的**运行状况警报 (Health Alerts)**。

将鼠标指针悬停在**运行状况警报 (Health Alerts)** 上可查看设备的运行状况摘要。弹出窗口显示前五个运行状况警报的截断摘要。点击弹出窗口可打开运行状况警报摘要的详细视图。

步骤 4 您可以从右上角的下拉列表中配置时间范围。您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。从下拉列表中选择**自定义 (Custom)** 以配置自定义开始和结束日期。

点击刷新图标可将自动刷新设置为 5 分钟或关闭自动刷新。

步骤 5 点击 **在图顶部显示部署细节** () 图标，在趋势图上根据所选时间范围显示部署重叠。

在图顶部显示部署细节 () 图标指示所选时间范围内的部署数量。垂直条带表示部署开始和结束时间。在多个部署的情况下，可显示多个频段/行。点击虚线顶部的图标可查看部署详细信息。

步骤 6 默认情况下，设备监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括CPU、内存、接口、连接统计信息；以及磁盘使用情况和关键进程信息。
- CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
- 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。
- 接口 - 接口状态和汇聚流量统计信息。
- 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
- Snort - 与 Snort 进程相关的统计信息。
- ASP 丢包 - 与加速安全路径 (ASP) 性能和行为相关的统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持设备指标的完整列表，请参阅 Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 7 点击 **添加新控制面板** (+)，通过从可用指标组构建您自己的变量集来创建自定义关联控制面板；请参阅 关联设备指标 ， 第 373 页。

关联设备指标

设备运行状况监控器包括一系列用于预测和响应系统事件的关键 威胁防御 设备指标。任何 威胁防御 设备的运行状况都可以通过这些报告的指标来确定。

默认情况下，设备监控器会在多个预定义的控制面板中报告这些指标。这些控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括CPU、内存、接口、连接统计信息；以及磁盘使用情况和关键进程信息。
- CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
- 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。
- 接口 - 接口状态和汇聚流量统计信息。
- 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
- Snort - 与 Snort 进程相关的统计信息。
- ASP 丢包 - 与加速安全路径 (ASP) 性能和行为相关的统计信息。

您可以添加自定义控制面板来关联相互关联的指标。从预定义的关联组中选择，例如CPU和Snort；或通过从可用指标组构建您自己的变量集来创建自定义关联控制面板。有关受支持设备指标的完整列表，请参阅 Cisco Secure Firewall Threat Defense 运行状况指标。

开始之前

- 要在运行状况监控控制面板中查看和关联时间序列数据（设备指标），请启用 REST API（**设置** > **配置** > **REST API 首选项**）。
- 您必须是管理员、运维或安全分析师用户才能执行此程序。

注释 关联设备指标仅适用于 威胁防御 6.7 及更高版本。因此，对于 6.7 之前的 威胁防御 版本，即使启用 REST API，运行状况监控控制面板也不会显示这些指标。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控**。

使用监控导航窗格访问设备特定的运行状况监控器。

步骤 2 在**设备 (Devices)** 列表中，点击 **展开**（>）和 **折叠**（∨）以展开和折叠受管设备列表。

步骤 3 选择要为其修改控制面板的设备。

步骤 4 点击**添加新控制面板 (Add New Dashboard)** (+) 图标以添加新控制面板。

步骤 5 指定用于标识控制面板的名称。

步骤 6 要从预定义关联组创建控制面板，请点击**从预定义关联 (Add from Predefined Correlations)** 下拉列表中添加，选择组，然后点击**添加控制面板 (Add Dashboard)**。

步骤 7 要创建自定义关联控制面板，请从**选择指标组 (Select Metric Group)** 下拉列表中选择一个组，然后从**选择指标 (Select Metrics)** 下拉列表中选择相应的指标。

有关受支持设备指标的完整列表，请参阅 Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 8 点击**添加指标 (Add Metrics)** 以从另一个组中添加和选择指标。

步骤 9 要删除单个指标，请点击项目右侧的 **x** 图标。点击删除图标可删除该组。

步骤 10 点击**添加控制面板 (Add Dashboard)** 以完成工作流程并将控制面板添加到运行状况监控器。

步骤 11 您可以**编辑**或**删除**预定义的控制面板和自定义关联控制面板。

集群运行状况监控器

当 威胁防御 是集群的控制节点时， 管理中心 会定期从设备指标数据收集器收集各种指标。集群运行状况监控器由以下组件组成：

- 概述控制面板 - 显示有关集群拓扑、集群统计信息和指标图表的信息：
  - 拓扑部分显示集群的实时状态、单个威胁防御的运行状况、威胁防御节点类型（控制节点或数据节点）以及设备的状态。设备的状态可以是 已禁用 （当设备离开集群时）、 已添加 （在公共云集群中，不属于 管理中心的其他节点）或 正常 （节点的理想状态）。

- 集群统计信息部分显示集群的当前指标，包括CPU使用率、内存使用率、输入速率、输出速率、活动连接和NAT转换。

注释 CPU 和内存指标显示数据平面和 snort 使用情况的单个平均值。

- 指标图表（即CPU使用情况、内存使用情况、吞吐量和连接）以图形方式显示指定时间段内的集群统计信息。

- 负载分布控制面板 - 在两个构件中显示集群节点的负载分布：
  - “分布”构件显示整个集群节点在整个时间范围内的平均数据包和连接分布情况。此数据描述节点如何分配负载。使用此构件，您可以轻松识别负载分布中的任何异常并进行纠正。
  - “节点统计信息”构件以表格格式显示节点级别指标。它显示有关CPU使用率、内存使用率、输入速率、输出速率、活动连接以及跨集群节点的NAT转换的指标数据。此表视图使您能够关联数据并轻松识别任何差异。
- 成员性能控制面板 - 显示集群节点的当前指标。您可以使用选择器来过滤节点并查看特定节点的详细信息。指标数据包括CPU使用率、内存使用率、输入速率、输出速率、活动连接和NAT转换。
- CCL 控制面板 - 以图形方式显示集群控制链路数据，即输入和输出速率。
- 故障排除和链接 - 提供常用故障排除主题和程序的便捷链接。
- 时间范围 - 用于限制各种设备指标窗口中显示的信息的可调时间窗口。
- 自定义控制面板 - 显示有关集群范围指标和节点级指标的数据。但是，节点选择仅适用于威胁防御指标，不适用于节点所属的整个集群。

查看集群运行状况监控器

您必须是管理员、运维或安全分析师用户才能执行此程序。

集群运行状况监控器提供集群和其节点的运行状态的详细视图。此集群运行状况监控器在一系列控制面板中提供集群的运行状况和趋势。

开始之前

- 确保您已从管理中心中的一个或多个设备创建集群。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控**。

使用监控导航窗格访问节点特定的运行状况监控器。

步骤 2 在设备列表中，点击 **展开**（ ） 和 **折叠**（ ） 以展开和折叠受管集群设备列表。

步骤 3 要查看集群运行状况统计信息，请点击集群名称。默认情况下，集群监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括其节点、CPU、内存、输入和输出速率、连接统计信息；以及 NAT 转换信息。
- 负载分布 — 跨集群节点的流量和数据包分布。
- 成员性能 - 有关 CPU 使用率、内存使用率、输入吞吐量、输出吞吐量、活动连接和 NAT 转换的节点级统计信息。
- CCL - 接口状态和汇聚流量统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持的集群指标的完整列表，请参阅Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 4 您可以从右上角的下拉列表中配置时间范围。您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。从下拉列表中选择**自定义 (Custom)** 以配置自定义开始和结束日期。

点击刷新图标可将自动刷新设置为 5 分钟或关闭自动刷新。

步骤 5 点击“部署”图标，在趋势图上根据所选时间范围显示部署重叠。

部署图标指示所选时间范围内的部署数量。垂直条带表示部署开始和结束时间。对于多个部署，将显示多个频段/行。点击虚线顶部的图标可查看部署详细信息。

步骤 6 （对于特定节点运行状况监控器）在设备名称右侧的页面顶部的警报通知中查看节点的 **运行状况警报** 。

将鼠标指针悬停在**运行状况警报**上可查看节点的运行状况摘要。弹出窗口显示前五个运行状况警报的截断摘要。点击弹出窗口可打开运行状况警报摘要的详细视图。

步骤 7 （对于特定节点运行状况监控器）默认情况下，设备监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括CPU、内存、接口、连接统计信息；以及磁盘使用情况和关键进程信息。
- CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
- 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。
- 接口 - 接口状态和汇聚流量统计信息。
- 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
- Snort - 与 Snort 进程相关的统计信息。
- ASP 丢弃 — 与因各种原因而丢弃的数据包相关的统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持设备指标的完整列表，请参阅Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 8 点击运行状况监控器右上角的加号 (+)，通过从可用指标组构建您自己的变量集来创建自定义控制面板。

对于集群范围的控制面板，选择集群指标组，然后选择指标。

运行状况监控器状态类别

可用状态类别按严重性在下表中列出。

表 *33*: 运行状况指示灯

状态级别	状态图标	饼形图中的状态颜色	说明
错误	**错误**（）	黑色	表示设备中的至少一个运行状况监控模块出现故障，并且自故障发生后未能成功重新运行。请与您的技术支持代表联系以获得对运行状况监控模块的更新。
严重	**严重**（  ）	红色	表示对于设备中的至少一个运行状况模块而言，已超过严重限值，并且该问题尚未解决。
警告	**警告**（  ）	黄色	表示对于设备中的至少一个运行状况模块而言，已超过警告限值，并且该问题尚未解决。 此状态还表示一种过渡状态，在这种状态下，由于设备配置发生更改，所需数据暂时不可用或无法处理。根据监控周期，此过渡状态会自动更正。
正常	**正常**（  ）	绿色	表示设备中的所有运行状况模块都在应用于该设备的健康策略中配置的限值内运行。
已恢复	**已恢复**（  ）	绿色	表示设备中的所有运行状况模块（包括处于“严重”或“警告”状态的模块）都在应用于该设备的运行状况策略中配置的限值内运行。
Disabled	**已禁用**（  ）	蓝色	表示设备被禁用或排除，设备没有应用运行状况策略，或者设备当前无法访问。

运行状况事件视图

通过“运行状况事件视图”页面，您可以查看由运行状况监控器在 管理中心日志运行状况事件中记录的运行状况事件。完全可自定义的事件视图使您可以快速轻松地分析运行状况监控器所收集的运

行状况事件。可以搜索事件数据，以便轻松访问可能与正调查的事件有关的其他信息。如果您了解每个运行状况模块测试的条件，就可以更有效地配置运行状况事件的警报。

可以在运行状况事件视图页面执行许多标准事件视图功能。

查看运行状况事件

您必须是管理员、运维或安全分析师用户才能执行此程序。

“运行状况事件表视图”(Table View of Health Events) 页面提供指定设备上所有运行状况事件的列表。

当您在管理中心中从Health Monitor页面访问运行状况事件时，您可以检索所有受管设备的所有运行状况事件。

提示 您可以为该视图添加书签，使您可以返回到其中包含事件的运行状况事件表的运行状况事件工作流程页面。加入书签的视图检索您当前正查看的时间范围内的事件，但是如果需要，您可以稍后修改时间范围以使用较新的信息更新该表。

过程

选择**系统**（⚙）> **运行状况** > **事件**。

提示 如果您使用的自定义工作流程不包括运行状况事件表视图，请点击（**切换工作流程**）**([switch workflow])**。在“选择工作流程”(Select Workflow) 页面上，点击**运行状况事件 (Health Events)**。

注释 如果未显示事件，您可能需要调整时间范围。

按模块和设备查看运行状况事件

过程

步骤 1 查看设备的运行状况监控器；请参阅查看设备运行状况监控器，第 372 页。

步骤 2 在**模块状态摘要 (Module Status Summary)** 图形中，点击要查看的事件状态类别的颜色。

警报详细信息列表切换显示内容以显示或隐藏事件。

步骤 3 在要查看其事件列表的警报的 **Alert Detail** 行，请点击 **Events**。

系统将显示“运行状况事件”(Health Events) 页面，其中包含以设备名称和指定运行状况警报模块名称为限制的查询的结果。如果未显示事件，您可能需要调整时间范围。

步骤 4 如果要查看指定设备的所有运行状况事件，请展开**搜索限制 (Search Constraints)**，然后点击**模块名称 (Module Name)** 限制将其删除。

查看运行状况事件表

您可以查看和修改运行状况事件表。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **事件**。

步骤 2 有以下选项可供选择：

- 书签 - 要将当前页面加入书签，以便可以快速返回到该页面，请点击**将此页面加入书签 (Bookmark This Page)**，提供书签的名称，然后点击**保存 (Save)**。
- 更改工作流程 - 要选择其他运行状况事件工作流程，请点击（**切换工作流程**）**([switch workflows])**。
- 删除事件 - 要删除运行状况事件，请选中要删除的事件旁边的复选框，然后点击**删除 (Delete)**。要删除当前受限制视图中的所有事件，请点击 **Delete All**，然后确认要删除所有事件。
- 生成报告 - 根据表视图中的数据生成报告 - 点击**报告设计器 (Report Designer)**。
- 修改 - 修改在“运行状况”(Health) 表视图中列出的事件的时间和日期范围。请注意，如果按时间限制事件视图，则在设备配置的时间窗口外生成的事件（无论是全局还是特定事件）可能显示在事件视图中。即使为设备配置了滑动时间窗口，也可能发生这种情况。
- 导航 - 浏览事件视图页面。
- 导航书签 - 要导航至书签管理页面，请点击任何事件视图中的**查看书签**。
- 导航其他 - 导航至其他事件表以查看关联事件。
- 排序 - 对显示的事件进行排序，更改事件表中显示的列，或者限制显示的事件
- 查看全部 - 要查看视图中所有事件的事件详细信息，请点击**查看全部 (View All)**。
- 查看详细信息 - 要查看与单个运行状况事件关联的详细信息，请点击事件左侧的向下箭头链接。
- 查看多个 - 要查看多个运行状况事件的事件详细信息，请选中与要查看其详细信息的事件对应的行旁边的复选框，然后点击**查看 (View)**。
- 查看状态 - 要查看特定状态的所有事件，请点击“状态”列中的“状态”以获取具有该状态的事件。

运行状况事件表

您在运行状况策略中选择启用的“运行状况监控”模块会运行各种测试，以确定设备运行状况。当运行状况满足您指定的条件时，系统将生成一个运行状况事件。

下表介绍在运行状况事件表中可以查看和搜索的字段。

表 *34:* 运行状况事件字段

字段	说明
模块名称	指定生成要查看的运行状况事件的模块的名称。例如，要查看衡量 CPU 性能的事件，请键入 `CPU`。搜索应检索适用的 CPU 使用率和 CPU 温度事件。
测试名称 （仅限搜索）	生成事件的运行状况模块的名称。
时间 （仅限搜索）	运行状况事件的时间戳。
说明	生成事件的运行状况模块的描述。例如，当无法执行进程时生成的运行状况事件被标记为 `Unable to Execute`。
值	生成事件的运行状况测试所获得的结果值（单位数量）。 例如，如果只要其正在监控的设备使用的 CPU 资源达到 80% 或以上，管理中心就会生成运行状况事件，则该值可以是介于 80 到 100 之间的一个数字。
单位	结果的单位描述符。您可以使用星号 (*) 创建通配符搜索。 例如，如果其正在监控的设备使用的 CPU 资源达到 80% 或以上时，管理中心会生成运行状况事件，则单位描述符为百分号 (%)。
状态	为设备报告的状态（严重、黄色、绿色或已禁用）。
设备	报告运行状况事件的设备。

运行状况监控历史

表 *35:*

功能	最低 管理中心	最低 威胁防御	详情
更新了 管理中心 内存使用模块默认阈值。	7.4.1	任意	管理中心内存使用警告和严重警告的默认阈值现在分别被设置为 88% 和 90%。 新增/修改的屏幕：**系统**（⚙）> **运行状况 (Health)** > **策略 (Policy)** > 编辑**防火墙管理中心运行状况策略 (Firewall Management Center Health Policy)** > **运行状况模块 (Health Modules)** > **内存使用情况 (Memory Usage)**。

功能	最低 管理中心	最低 威胁防御	详情
改进了 管理中心 的内存使用量计算。	7.4.1	任意	管理中心内存使用模块在计算内存使用量时，将考虑可用交换内存和高速缓冲存储器的数量，以准确确定内存使用量并发送使用状况警报。 新增/修改的屏幕：**系统**（⚙）> **运行状况 (Health)** > **监控器 (Monitor)** > **防火墙管理中心 (Firewall Management Center)** > **添加新控制面板 (Add New Dashboard)**。
NTP 服务器同步问题的运行状况警报。	7.4.1	任意	在 Cisco Secure Firewall Management Center 运行状况策略中引入了**时间服务器状态**模块。启用后，此模块会监控 NTP 服务器的配置，并在 NTP 服务器不可用或 NTP 服务器配置无效时发出警报。 新增/修改的屏幕：**系统**（⚙）> **运行状况 (Health)** > **策略 (Policy)** > **防火墙管理中心运行状况策略 (Firewall Management Center Health Policy)** > **运行状况模块 (Health Modules)** > **时间同步 (Time Synchronization)**。
使用 OpenConfig 将遥测数据流传输到外部服务器。	7.4	7.4	您现在可以从威胁防御设备使用 OpenConfig 将指标和运行状况监控信息发送到外部服务器（gNMI 收集器）。您可以配置威胁防御或收集器来发起连接（通过 TLS 加密）。 新增/修改的屏幕：**系统**（⚙）> **运行状况 (Health)** > **策略 (Policy)** > **防火墙威胁防御策略 (Firewall Threat Defense Policies)** > **设置 (Settings)** > **OpenConfig 流传输遥测 (OpenConfig Streaming Telemetry)**。
运行状况监控使用性增强。	7.4	任意	改进了 **添加新控制面板** 对话框，有助于轻松创建自定义控制面板。包含用于编辑或删除预定义设备运行状况监控控制面板的选项。 新增/修改的屏幕：**系统**（⚙）> **运行状况** > **监控器** > **设备** > **添加新控制面板**。
新的集群运行状况监控控制面板。	7.3	任意	引入了一个用于查看集群运行状况监控器指标的新控制面板，其中包含以下组件： • 概述 - 显示有关集群拓扑、集群统计信息和指标图表的信息。 • 负载分布 - 显示跨集群节点的负载分布。 • 成员性能 - 显示集群的所有成员节点的当前指标。 • CCL - 以图形方式显示集群控制链路数据，即输入和输出速率。 **注释** 这些功能仅适用于集群。因此，您必须在 **监控** 窗格的 **设备** 列表下选择集群，才能查看和使用集群控制面板。 新增/修改的屏幕：**系统**（⚙）> **运行状况** > **监控器**。

功能	最低 管理中心	最低 威胁防御	详情
新的硬件统计模块。	7.3	任意	管理中心 硬件和环境状态统计信息已添加到运行状况监控控制面板： • 引入了新的策略模块 **硬件统计信息**，以启用对管理中心硬件上的硬件后台守护程序的监控。 指标包括风扇速度、温度和电源。 • 还添加了自定义指标组 **硬件统计信息**，以在监控控制面板上查看硬件运行状况指标的图形表示。 • 电源状态在管理中心的 **运行状况警报** 中捕获。 **注释** 这些功能仅适用于管理中心。因此，它们仅在管理中心控制面板上可用。 新增/修改的菜单项： • **系统**（⚙） > **运行状况** > **监控** • **系统**（⚙） > **运行状况** > **策略**
新的硬件和环境状态指标组，	7.3	任意	威胁防御硬件和环境状态统计信息已添加到运行状况监控控制面板： • 引入了自定义指标组 **硬件/环境状态**，用于查看有关威胁防御的硬件相关统计信息。指标包括风扇速度、机箱温度、SSD 状态和电源。 • 设备 **运行状况警报** 已增强，包括威胁防御硬件的电源状态 - 异常热状态显示严重警报 ，正常热状态显示 正常 警报。 **注释** 这些功能仅适用于威胁防御硬件。因此，您必须在 **监控** 窗格的 **设备** 列表下选择适当的设备。 新增/修改的屏幕： **系统**（⚙） > **运行状况** > **监控器**。
运行状况监控使用性增强。	7.1	任意	以下 UI 页面经过临时改进，以提高数据的可用性和显示效果： • 策略 • 排除 • 监控警报 新增/修改的屏幕： • **系统**（⚙） > **运行状况** > **策略** • **系统**（⚙） > **运行状况** > **排除** • **系统**（⚙） > **运行状况** > **监控警报**

功能	最低 管理中心	最低 威胁防御	详情
大象流检测。	7.1	任意	运行状况警报包含以下增强功能： • 连接统计信息包括活动的象流。 • 连接组指标包括活动的象流数。 思科 Firepower 2100 系列不支持象流检测功能。
已停用非托管磁盘使用率高 (high unmanaged disk usage) 警报。	7.0.6	任意	“磁盘使用情况”(Disk Usage) 运行状况模块不再针对非托管磁盘使用率过高 (high unmanaged disk usage) 发出警报。升级后，您可能会继续看到这些警报，直到将运行状况策略部署到托管设备（停止显示警报）或升级设备（停止发送警报）。 **注释** 版本 7.0 – 7.0.5、7.1.x、7.2.0 – 7.2.3 和 7.3.x 继续支持这些警报。如果您的 管理中心 正在运行这些版本中的任何一个，您也可能会继续看到警报。

功能	最低 管理中心	最低 威胁防御	详情
新的运行状况模块。	7.0	任意	我们添加了以下运行状况模块： • AMP 连接状态：从 威胁防御监控 AMP 云连接。 • AMP Threat Grid 状态：从 威胁防御监控 AMP Threat Grid 云连接。 • ASP 丢弃：监控数据平面加速安全路径所放弃的连接。 • 高级 Snort 统计信息：监控与数据包性能、流计数器和流事件相关的 Snort 统计信息。 • 事件流状态：监控使用事件流转换器的第三方客户端应用的连接 • FMC访问配置更改：监控直接在管理中心上进行的访问配置更改。 • FMC HA 状态：监控主用和备用 管理中心 以及设备之间的同步状态。替换高可用性状态模块。 • FTD HA 状态：监控主用和备用 威胁防御 HA 对以及设备之间的同步状态。 • 文件系统完整性检查：如果系统启用了 CC 模式或 UCAPL 模式，则执行文件系统完整性检查。 • 流量分流：监控 Firepower 9300 和 4100 平台上的硬件流量分流统计信息。 • 命中计数：监控访问控制策略中特定规则的命中次数。 • MySQL 状态：监控 MySQL 数据库的状态。 • NTP 状态：监控托管设备的 NTP 时钟同步状态。 • RabbitMQ 状态：监控 RabbitMQ 消息传递代理的状态。 • 路由统计信息：监控来自 威胁防御的 IPv4 和 IPv6 路由信息。 • 安全服务交换连接状态：监控来自 威胁防御 的安全服务交换云连接。 • Sybase 状态：监控 Sybase 数据库的状态。 • 未解析组监控器：监控访问控制策略中使用的未解析组。 • VPN 统计信息：监控站点间和远程访问 VPN 隧道统计信息。 • xTLS 计数器：监控 xTLS/SSL 流、内存和缓存有效性

功能	最低 管理中心	最低 威胁防御	详情

运行状况监控增强功能。	7.0	任意	运行状况监控器添加了以下增强功能：
			• 增强的 管理中心 控制面板，提供以下内容的摘要视图：
			  • 高可用性
			  • 事件速率和容量
			  • 流程运行状况
			  • CPU 阈值
			  • Memory
			  • 接口速率
			  • 磁盘使用情况
			• 增强型 威胁防御 控制面板：
			  • 裂脑情景的运行状况警报
			  • 新运行状况模块提供的其他运行状况指标

功能	最低 管理中心	最低 威胁防御	详情
新的运行状况模块。	6.7	任意	不再使用CPU使用率模块。相反，请参阅以下模块了解CPU使用情况： • CPU 使用情况（每个核心）：监控所有核心上的 CPU 使用情况。 • CPU 使用率数据平面：监控设备上所有数据平面进程的平均 CPU 使用率。 • CPU 使用率 Snort：监控设备上 Snort 进程的平均 CPU 使用率。 • CPU 使用率系统：监控设备上所有系统进程的平均 CPU 使用率。 添加了以下模块以跟踪统计信息： • 连接统计信息：监控连接统计信息和 NAT 转换计数。 • 关键进程统计信息：监控关键进程的状态、资源消耗和重新启动计数。 • 部署的配置统计信息：监控有关已部署配置的统计信息，例如ACE数、IPS 规则数。 • Snort 统计信息：监控事件、流和数据包的 Snort 统计信息。 添加了以下模块以跟踪内存使用情况： • 内存使用率数据平面：监控数据平面进程使用的已分配内存的百分比。 • 内存使用情况 Snort：监控 Snort 进程使用的已分配内存的百分比。
运行状况监控增强功能。	6.7	任意	运行状况监控器添加了以下增强功能： • 运行状况摘要页面，提供 Firepower 管理中心和 管理中心 管理的所有设备的运行状况概览视图。 • 监控导航窗格允许您导航设备层次结构。 • 受管设备单独列出，或根据其地理位置、高可用性或集群状态（如果适用）分组。 • 您可以从导航窗格查看各个设备的运行状况监控器。 • 用于关联相关指标的自定义控制面板。从预定义的关联组中选择，例如 CPU 和 Snort；或通过从可用指标组构建您自己的变量集来创建自定义关联控制面板。

功能	最低 管理中心	最低 威胁防御	详情
功能移动至设备模块上的威胁数据更新	6.7	任意	不再使用本地恶意软件分析模块。有关此信息，请参阅设备上的威胁数据更新。 以前由安全情报模块和 URL 过滤模块提供的一些信息现在由设备上的威胁数据更新模块提供。
新增运行状况模块：配置内存分配。	7.0 6.6.3	任意	版本 6.6.3 改进了设备内存管理，并引入了新的运行状况模块：配置内存分配。 当已部署的配置的大小使设备面临内存耗尽的风险，此模块会发出警报。警报会显示您的配置需要多少内存，以及超出可用内存的数量。如果发生此情况，请重新评估您的配置。通常来说，您可以减少访问控制规则或入侵策略的数量或降低其复杂性。
URL过滤监控器改进。	6.5	任意	如果管理中心无法注册到思科云，URL过滤监控模块现在会发出警报。
URL过滤监控器改进。	6.4	任意	您可以配置 URL 过滤监控器警报的时间阈值。
新增运行状况模块：设备中威胁数据更新。	6.3	任意	新增模块**设备中威胁数据更新**。 如果设备用于检测威胁的某些情报数据和配置未在您指定的时间段内于设备上更新，则此模块会提醒您。

第 12 章

审核和系统日志

以下主题介绍如何审核系统上的活动：

系统日志

“系统日志”(System Log) (syslog) 页面上提供设备的系统日志信息。

您可以用两种方式审核系统中的活动。隶属 Firepower 系统的设备会为用户每次与 Web 界面的交互生成审核记录，同时也在系统日志中记录系统状态消息。

系统日志显示系统生成的每条消息。以下项目会按顺序列出：

- 生成消息的日期
- 生成消息的时间
- 生成消息的主机
- 消息本身

查看系统日志

系统日志信息是本地消息。例如，您**不能**使用 管理中心查看受管设备上系统日志中的系统状态消息。

您可以使用 UNIX 文件搜索实用程序 Grep 接受的大多数语法来过滤消息。这包括使用与 Grep 兼容的正则表达式实现模式匹配。

开始之前

您必须是“管理员”或“维护”用户并位于“全局”域中才能查看系统统计信息。

过程

步骤 1 选择**系统**（⚙）> **监控** > **系统日志**。

步骤 2 要在系统日志中搜索特定消息内容，请执行以下操作：

a) 在过滤器字段中输入单词或查询，如系统日志过滤器的语法，第 390 页中所述。

支持仅与 Grep 兼容的搜索语法。

示例：

要搜索包含用户名“Admin”的所有日志条目，请使用 `Admin`。

要搜索 11 月 27 日生成的所有日志条目，请使用 `Nov[[:space:]]*27` 或 `Nov.*27`（而不是 `Nov 27` 或 `Nov*27` ）。

要搜索包含 11 月 5 日的授权调试信息的所有日志条目，请使用 `Nov[[:space:]]*5.*AUTH.*DEBUG`。

b) 要使搜索区分大小写，请选择**区分大小写**。（默认情况下，过滤器不区分大小写。）

c) 要搜索**不**符合所输入条件的所有系统日志消息，请选择**排除**。

d) 点击**前往 (Go)**。

系统日志过滤器的语法

下表显示了在系统日志过滤器中可以使用的正则表达式语法：

表 *36:* 系统日志过滤器语法

语法构成	说明	示例
.	匹配任意字符或空格	`Admi.` 匹配 `Admin`、`AdmiN`、`Admi1` 和 `Admi&`
`[[:alpha:]]`	匹配任意字母字符	`[[:alpha:]]dmin` 匹配 `Admin`、`bdmin` 和 `Cdmi`
`[[:upper:]]`	匹配任意大写字母字符	`[[:Upper:]]dmin` 匹配 `Admin`、`Bdmin` 和 `Cdmi`
`[[:lower:]]`	匹配任意小写字母字符	`[[:Lower:]]dmin` 匹配 `admin`、`bdmin` 和 `cdmi`
`[[:digit:]]`	匹配任意数字字符	`[[:Digit:]]dmin` 匹配 `0dmin`、`1dmin` 和 `2dmi`
`[[:alnum:]]`	匹配任意字母数字字符	`[[:Alnum:]]dmin` 匹配 `1dmin`、`admin`、`2dmin`
`[[:space:]]`	匹配任意空格，包括制表符	`Feb[[:space:]]29` 匹配从 2 月 29 日起的日
*	匹配其符合的字符或表达式的零个或更多实例	`Ab*` 匹配 `a`、`ab`、`abb`、`ca`、`cab` 和 `cabb` `[ab]*` 匹配所有字符
?	匹配零个或一个实例	`ab?` 匹配 `a` 或 `ab`

语法构成	说明	示例
\	允许您搜索一般会被解释为正则表达式语法的字符	`alert\?` 匹配 `alert?`

关于系统审核

隶属 Firepower 系统的设备会为用户每次与 Web 界面的交互生成审核记录。

相关主题

标准报告，第 505 页

审核记录

Cisco Secure Firewall Management Center 记录用户活动的只读审核信息。审核日志显示在标准事件视图中，您可以依据审核视图中的任何项目查看、排序和过滤审核日志消息。您可以轻松删除和报告审核信息，也可以查看用户所作更改的详细报告。

审核日志中最多可以存储 100000 个条目。当审核日志中条目的数量超过 100000 时，设备会从数据库中删除最旧的记录，保持数据库中条目的数量为 100000。

审核日志不会显示登录错误的用户或源 IP：

- 输入错误的密码时不显示源 IP。
- 当用户帐户不存在时，系统不会同时显示源 IP 和用户。
- 如果对 LDAP 用户的尝试失败，则不会触发审核日志。

相关主题

管理中心的 SSO 指南，第 137 页

查看审核记录

在 管理中心，您可以查看审核记录表。预定义的审计工作流程包括一个事件表视图。可以根据要查找的信息操纵表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

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

您必须是管理员用户才能执行此程序。

过程

步骤 1 使用**系统**（⚙）> **监控** > **审核**访问审核日志工作流程。

步骤 2 如果未显示事件，您可能需要调整时间范围。有关详细信息，请参阅事件时间限制，第 658 页。

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。

步骤 3 有以下选项可供选择：

选择仅适用于搜索限制的结果。例如，当您搜索运行**状况事件**时，生成的视图页面会显示**工作流程**选项。同样，仅当您处于 **漏洞** 表视图中时，才会显示查看 **(视图**（  ）) 特定漏洞的选项。

- 要了解有关表中各列内容的详细信息，请参阅系统日志，第 389 页。
- 要对当前工作流程页面上的事件进行排序和限制，请参阅使用表视图页面，第 650 页。
- 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。有关详细信息，请参阅使用工作流程，第 642 页。
- 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，第 650 页。
- 要限制特定值，请点击行中的值。如果在详细浏览页面中点击一个值，您将进入下一个页面并限制该值。请注意，在表视图中点击某一行中的一个值时，会限制该表视图，并使系统**不会**向下展开到下一页。有关详细信息，请参阅事件视图限制，第 664 页。

  提示 表视图的页面名称中始终包含“Table View”。

- 要删除审核记录，请选中要删除的事件旁边的复选框，然后点击**删除**，或点击**全部删除**以删除当前受限制视图中的所有事件。
- 要将当前页面加入书签，以便您可以快速返回到该页面，请点击**将此页面加入书签 (Bookmark This Page)**。有关详细信息，请参阅书签，第 667 页。
- 要导航至书签管理页面，请点击**查看书签 (View Bookmarks)**。有关详细信息，请参阅书签，第 667 页。
- 要根据当前视图中的数据生成报告，请点击 **报告 (Reporting)**。有关详细信息，请参阅 从事件视图创建报告模板，第 509 页。
- 要查看审核日志中记录的系统更改摘要，请点击 **消息** 列中的适用事件旁边的 **比较** 。有关详细信息，请参阅 使用审核日志检查更改，第 394 页。

相关主题

事件视图限制，第 664 页

审核日志工作流程字段

下表介绍了可以查看和搜索的审核日志字段。

表 *37:* 审核日志字段

字段	说明
Time	设备生成审核记录的时间和日期。
用户	触发审核事件的用户的用户名。

字段	说明
子系统	用户生成审核记录所遵循的完整菜单路径。例如，**系统**（⚙）>**监控**>**审核**是查看审核日志的菜单路径。 对于菜单路径不相关的少数情况，“子系统”(Subsystem) 字段仅显示事件类型。例如，**登录 (Login)** 对用户登录尝试进行分类。
消息	用户执行的操作或用户在页面上点击的按钮。 例如，`Page View` 表示用户简单查看了子系统中显示的页面，而 `Save` 意味着用户点击了页面上的 **Save** 按钮。 对系统的更改会以一个 **比较图标** 显示，您可以点击以查看更改摘要。
源 IP	与用户使用的主机相关联的 IP 地址。 注意：搜索此字段时，必须输入特定的 IP 地址；搜索审核日志时不可以使用 IP 范围。
域	触发审核事件时用户的当前域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
配置更改 （仅限搜索）	指定是否查看搜索结果中配置更改的审核记录。（`yes` 或 `no`）
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。此字段不可搜索。

相关主题

事件搜索，第 671 页

审核事件表视图

您可以更改事件视图的布局或按字段值限制视图中的事件。当禁用某列时，在点击想要隐藏的列标题中的 **关闭**（✕） 后，系统会显示弹出窗口，在窗口中点击 **应用**。禁用列时，该列在会话持续时间内处于禁用状态（除非稍后重新添加该列）。请注意，禁用第一列时，会添加“计数”列。

要隐藏或显示其他列，或将已禁用列添加回视图中，选择或清除相应的复选框，然后点击**应用 (Apply)**。

请注意，在表视图中点击某一行中的一个值时，会限制该表视图，且不会向下展开到工作流程中的下一个页面。

提示 表视图的页面名称中始终包括“Table View”。

相关主题

使用工作流程，第 642 页

使用审核日志检查更改

您可以使用审核日志来查看详细的一些系统更改报告。这些报告会比较系统当前配置与执行受支持的更改之前的最近配置。

“比较配置”(Compare Configurations) 页面显示更改前的系统配置和采用并行格式的运行配置之间的差异。每个配置上方的标题栏中将显示审核事件类型、上次修改时间，以及进行更改的用户的名称。

两个配置之间的差异将突出显示：

- 蓝色表示此突出显示的设置在两个配置中不同，并用红色文本注明其不同之处。
- 绿色表示此突出显示的设置在一个配置中出现，而在另一个配置中却没有出现。

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

您必须是管理员用户才能执行此程序。

过程

步骤 1 选择**系统**（⚙）> **监控** > **审核**。

步骤 2 点击 **比较**，其位于 **消息** 列的适用审计日志事件旁边。

提示 可以点击标题栏上方的**上一个 (Previous)** 或**下一个 (Next)** 在不同更改间切换。如果更改摘要长度超过一个页面，您也可以使用右侧的滚动条查看其他的更改。

抑制审核记录

如果审核策略不要求您审核特定类型的用户与 Firepower 系统之间的交互，则可以防止这些交互在 Cisco Secure Firewall Management Center 或 。例如，默认情况下，每次用户查看联机帮助时，Firepower 系统都会生成一个审核记录。如果您不需要保留这些交互记录，可以自动屏蔽它们。

要配置审计事件屏蔽，您必须具备设备的管理员用户帐户权限，且必须能够访问设备的控制台或打开一个安全外壳。

⚠

注意 确保仅授权人员可以访问设备及其管理员帐户。

开始之前

您必须是管理员用户才能执行此程序。

过程

在 /etc/sf 目录中，创建以下形式的一个或多个 AuditBlock 文件，其中 type 是审核块类型，第 395 页中所述的类型之一：

AuditBlock.*type*

注释 如果为特定类型的审核消息创建 AuditBlock.*type* 文件，但之后确定不想再抑制它们，则必须删除 AuditBlock.*type* 文件的内容，但在 Firepower 系统上保留该文件本身。

审核块类型

每种审核块类型的内容都必须为特定格式，如下表所述。确保您使用的是正确的文件名大写字母。另请注意，文件的内容区分大小写。

请注意，当您添加 AuditBlock 文件时，带审核子系统和审核过滤器类型已更改消息的审核记录会被添加到审核事件中。出于安全原因，该审计记录**不能**被屏蔽。

表 *38:* 审核块类型

类型	说明
地址	创建一个以 AuditBlock.address 命名的文件，并包括您想要从审核日志中屏蔽的各 IP 地址，每行一个。您可以使用部分 IP 地址，前提是它们从地址开始处映射。例如，部分地址 10.1.1 匹配从 10.1.1.0 到 10.1.1.255 的地址。
消息	创建一个以 AuditBlock.message 命名的文件，并包括您想要屏蔽的消息子字符串，每行一个。 请注意，子字符串会进行匹配，因此如果您的文件中包括 backup，则包括文字 backup 的所有消息都将被屏蔽。
子系统	创建一个以 AuditBlock.subsystem 命名的文件，并包括您想要屏蔽的各子系统，每行一个。 请注意，子字符串**不**进行匹配。您必须使用准确的字符串。有关所审核的子系统列表，请参阅已审核的子系统，第 395 页。
用户	创建一个以 AuditBlock.user 命名的文件，并包括您想要屏蔽的各用户帐号，每行一个。可以使用部分字符串进行匹配，前提是它们从用户名开始处映射。例如，部分用户名 IPSAnalyst 匹配用户名 IPSAnalyst1 和 IPSAnalyst2。

已审核的子系统

下表列出了经审计的子系统。

表 *39:* 子系统名称

名称	包括与下列各项的用户交互.....
管理	管理功能，例如系统和访问配置、时间同步、备份和恢复、设备管理、用户帐户管理和调度
警报	警报功能，例如邮件、SNMP 和系统日志警报
审核日志	审核事件视图
审计日志搜索	审计事件搜索
命令行	命令行界面
配置	邮件警报
上下文交叉启动	添加到系统或从控制面板和事件视图访问的外部资源
COOP	操作功能连续性
日期	事件视图的日期和时间范围
默认子系统 (Default Subsystem)	没有已分配子系统的选项
检测和防御策略 (Detection & Prevention Policy)	入侵策略的菜单选项
错误	系统级错误
eStreamer	eStreamer 配置
EULA	审核最终用户许可协议
事件	入侵和发现事件视图
已审核的事件 (Events Reviewed)	已审核的入侵事件
事件搜索 (Events Search)	任何事件搜索
未能安装规则更新 (Failed to install rule update) `rule_update_id`	安装规则更新
标头	用户登录后用户界面的初次展示
运行状况	运行状况监控
运行状况事件	运行状况监控事件视图
帮助	在线帮助
高可用性	建立和处理高可用性对中的 管理中心

名称	包括与下列各项的用户交互.....
IDS 影响标记 (IDS Impact Flag)	入侵事件的影响标志配置
IDS 策略 (IDS Policy)	入侵策略
IDSRule sid:`sig_id` rev:`rev_num`	按 SID 划分的入侵规则
执行安装	安装更新
入侵事件	入侵事件
登录	Web 界面登录和注销功能
注销	Web 界面注销功能
菜单	任何菜单选项
配置输出 (Configuration export) > `config_type` > `config_name`	导入特定类型和名称的配置
权限升级 (Permission Escalation)	用户角色升级
偏好设置	用户首选项，例如用户帐户时区和单个事件的首选项
策略	任何策略，包括入侵策略
注册	在管理中心上注册设备
RemoteStorageDevice	配置远程存储设备
报告	报告列表和报告设计者功能
规则	入侵规则，包括入侵规则编辑器和规则导入进程
规则更新导入日志 (Rule Update Import Log)	查看规则更新导入日志
规则更新安装 (Rule Update Install)	安装规则更新
会话终止	Web 界面会话超时session timeouts
状态	系统日志以及主机和性能统计数据
系统	各种系统范围设置
任务队列	查看后台进程状态
用户	创建和修改用户帐户和角色

关于将审核日志发送至外部位置

要将审核日志从 FMC 发送到外部位置，请参阅：

- 审核日志，第 43 页
- 审核日志 ID证书，第 46 页

第 13 章

统计信息

以下主题介绍如何监控 Firepower 系统：

关于系统统计信息

“统计信息”页面列出常规设备统计信息的当前状态，包括磁盘使用率和系统进程、数据相关器统计信息和入侵事件信息。

主机统计信息部分

下表介绍了 Statistics 页面列出的主机统计信息。

表 *40:* 主机统计信息

类别	说明
Time	系统当前时间。
正常运行时间 (Uptime)	系统上次启动后持续的天数（如果适用）、小时数和分钟数。
内存使用率	正使用的系统内存的百分比。
平均负载	过去 1 分钟、5 分钟和 15 分钟内 CPU 队列的平均进程数。
磁盘使用情况	正使用的磁盘空间的百分比。点击箭头查看更详细的主机统计信息。

类别	说明
流程	系统中运行的进程摘要。

磁盘使用率部分

“统计信息”(Statistics) 页面的“磁盘使用率”(Disk Usage) 部分提供磁盘使用率快览，可以按类别和分区状态进行查看。如果您在设备上安装了一个恶意软件存储包，您还可以查看分区状态。您可以随时监控此页面，确保系统进程和数据库有充足的磁盘空间可用。

提示 您也可以在 使用运行状况监控器在磁盘空间较低的情况下监控磁盘使用量和警报。

进程部分

在“统计信息”(Statistics) 页面的“进程”(Processes) 部分，可以查看一台设备上正在运行的进程。它为每个运行的进程提供常规进程信息和特定信息。您可以使用 管理中心的Web 界面查看任何受管设备的进程状态。

请注意，设备上运行有两个不同类型的进程：后台守护程序和可执行文件。后台守护程序始终运行，可执行文件在需要时运行。

进程状态字段

展开“统计信息”(Statistics) 页面的“进程”(Processes) 部分时，也可以查看以下内容：

Cpu(s)

列出以下 CPU 使用信息：

- 用户进程使用百分比
- 系统进程使用百分比
- 优先使用情况百分比（拥有负优先值进程的CPU 使用情况，表示更高优先级）。优先值是指系统进程的计划优先级，范围为 -20（最高优先级）到 19（最低优先级）。
- 空闲使用百分比

Mem

列出以下内存使用信息：

- 内存中千字节总数
- 内存中已使用千字节总数

- 内存中空闲的千字节总数
- 内存中缓存的千字节总数

交换

列出以下交换使用信息：

- 交换空间中千字节总数
- 交换空间中已使用千字节总数
- 交换空间中空闲的千字节总数
- 交换空间中缓存的千字节总数

下表介绍了显示在“进程”(Processes) 部分中的各列。

表 *41:* 进程列表列

列	**Description**
Pid	进程 ID 编号
用户名	运行进程的用户或组的名称
Pri	进程优先级
Nice	优先值是表示一个进程计划优先级的值。值范围为 -20（最高优先级）到 19（最低优先级）
Size	进程使用的内存大小（以千字节计，除非数值后是 m，即表示兆字节）
Res	内存中常驻页面文件的数量（以千字节计，除非数值后是 m，即表示兆字节）
省/自治区	进程状态： • D - 进程处于不可中断休眠（通常为“输入/输出”） • N - 进程有一个正优先值 • R - 进程可运行（在运行队列中） • S - 进程处于休眠模式 • T - 进程被跟踪或停止 • W - 进程在分页 • X - 进程已废弃 • Z - 进程已失效 • < - 进程有一个负优先值

列	Description
时间	进程运行的时间（格式为小时:分钟:秒）
Cpu	进程正在占用 CPU 的百分比
命令	进程的可执行名称

相关主题

系统后台守护程序，第 402 页
可执行文件和系统实用程序，第 403 页

系统后台守护程序

后台守护程序在设备上持续运行。它们确保服务可用，并在需要时产生进程。下表列出了“进程状态”(Process Status) 页面可以看到的后台守护程序，并对其功能进行简要说明。

注释 下表并非一台设备上可运行的所有进程的详尽列表。

表 42: 系统后台守护程序

后台守护程序	说明
crond	管理计划命令的实施（cron 作业）
dhclient	管理动态主机 IP 寻址
fpcollect	管理客户端和服务器指纹的收集
httpd	管理 HTTP（Apache Web 服务器）进程
httpsd	管理 HTTPS （使用 SSL 的 Apache Web 服务器）服务，检查正在运行的 SSL 和有 身份验证；在后台运行，为设备提供安全的网络接入
keventd	管理 Linux 内核事件通知消息
klogd	管理 Linux 内核消息监听和记录
kswapd	管理 Linux 内核交换内存
kupdated	管理 Linux 内核更新进程，执行磁盘同步
mysqld	管理数据库进程
ntpd	管理网络时间协议 (NTP) 进程
pm	管理所有系统进程，启动所需进程，重新启动所有意外发生故障的进程

后台守护程序	说明
reportd	管理报告
safe_mysqld	管理数据库的安全模式运行；如果出现错误，重新启动数据库后台守护程序，并 录运行时信息
SFDataCorrelator	管理数据传输
sfestreamer（仅限 管理中心）	管理使用事件流转换器的第三方客户端应用的连接
sfmgr	使用到一台设备的 sftunnel 连接，为远程管理和配置该设备提供 RPC 服务
SFRemediateD（仅限 管理中心）	管理补救响应
sftimeserviced（仅限 管理中心）	将时间同步消息转发到受管设备
sfmbservice	使用到设备的 sftunnel 连接，为在远程设备上运行的 sfmb 消息代理进程提供接入 仅由运行状况监控用于将运行状况事件和警报从受管设备发送到 管理中心。
sftroughd	侦听进入套接字的连接，然后调用正确的可执行程序（通常是思科消息代理 sfm
sftunnel	为需要与远程设备通信的所有进程提供安全的通信通道
sshd	管理安全外壳 (SSH) 进程；在后台运行，为设备提供 SSH 接入
syslogd	管理系统日志记录（系统日志）进程

可执行文件和系统实用程序

系统会有许多可执行文件，它们在其他进程或用户操作执行时开始运行。下表介绍了在“进程状态”(Process Status) 页面可能会看到的可执行程序。

表 *43:* 系统可执行程序和实用程序

可执行程序	说明
awk	执行用 `awk` 编程语言编写的程序的实用程序
Bash	GNU Bourne-Again 外壳
cat	读取文件并将内容写入标准输出的实用程序
chown	更改用户和组文件权限的实用程序
chsh	更改默认登录外壳的实用程序

可执行程序	说明
SFDataCorrelator（仅限管理中心）	分析由系统创建的二进制文件，从而生成事件、连接数据和网络映射
cp	复制文件的实用程序
df	列出设备可用空间量的实用程序
echo	将内容写入标准输出的实用程序
egrep	按特定输入搜索文件和文件夹、支持标准 grep 不支持的正则表达式扩展集的实用程序
find	按特定输入循环搜索目录的实用程序
grep	按特定输入搜索文件和目录的实用程序
halt	停用服务器的实用程序
httpsdctl	处理安全 Apache 网络进程
hwclock	允许访问硬件时钟的实用程序
ifconfig	表示网络配置可执行程序。确保 MAC 地址保持不变
iptables	根据“访问配置”(Access Configuration) 页面所做的更改处理访问限制。
iptables-restore	处理 iptables 文件恢复
iptables-save	处理对 iptables 保存的更改
kill	可用来结束会话和进程的实用程序
killall	可用来结束所有会话和进程的实用程序
ksh	Korn 外壳的公共域版本
logger	提供通过命令行访问系统日志后台守护程序方法的实用程序
md5sum	为指定文件打印校验和以及块数量的实用程序
mv	移动（重命名）文件的实用程序
myisamchk	表示数据库表校验和修复
mysql	表示数据库进程；可能出现多个实例
openssl	表示创建身份验证证书
perl	表示一个 perl 进程

可执行程序	说明
ps	将进程信息写入标准输出的实用程序
sed	用来编辑一个或多个文本文件的实用程序
sfheartbeat	识别检测信号广播，表示设备处于活动状态；检测信号用来保持设备和管理中心之间的联络
sfmb	表示消息代理进程；处理 管理中心和设备之间的通信。
sh	Korn 外壳的公共域版本
shutdown	关闭设备的实用程序
sleep	在指定秒数内暂停进程的实用程序
smtpclient	启用邮件事件通知功能后，处理邮件传输的邮件客户端
snmptrap	将 SNMP 陷阱数据转发到启用 SNMP 通知功能后指定的 SNMP 陷阱服务器
snort	表示 Snort 正在运行
ssh	表示与设备连接的安全外壳 (SSH)
sudo	表示 sudo 进程，其允许管理员以外的用户运行可执行程序
top	显示最高 CPU 进程信息的实用程序 **注释** 此实用程序的 CPU 使用情况输出是 CPU 核心的不同使用类型的拆分。您必须添加用户和系统进程的使用情况，才能了解实际的总 CPU 使用情况。 例如，如果 top 命令的输出为：`%Cpu(s): 76.6 us, 22.1 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 1.3 si, 0.0 st` 在这里，76.6% 的 CPU 时间由用户进程使用，22.1% 的 CPU 时间由系统（内核）进程使用。总 CPU 使用率为 98.7%。 因此，此实用程序中报告的 CPU 使用情况似乎与“运行状况监控”控制面板不同。此外，此实用程序使用三秒的时间间隔来计算 CPU 使用率。而管理中心运行状况监控器使用一秒间隔。
touch	用来更改指定文件的访问和修改时间的实用程序
vim	用来编辑文本文件的实用程序
wc	执行指定文件行、字和字节计数的实用程序

相关主题

配置访问列表，第 41 页

SFDataCorrelator 进程统计信息部分

在 管理中心上，可以查看有关当日数据相关器和网络发现进程的统计信息。当受管设备执行数据收集、解码和分析时，网络发现进程将数据与指纹和漏洞数据库相关联，然后由管理中心上运行的Data Correlator处理成二进制文件。数据相关器分析二进制文件的信息后生成事件，然后创建网络映射。

网络发现和数据相关器中显示的统计信息为当日的平均值，使用每台设备从 12:00 AM 到 11:59 PM 之间搜集的统计信息。

下表介绍数据相关器进程显示的统计信息。

表 *44:* 数据相关器进程统计信息

类别	说明
Events/Sec	Data Correlator 每秒钟接收和处理的发现事件的数量
连接数/秒	Data Correlator 每秒钟接收和处理的连接的数量
CPU Usage - User (%)	当日用户进程占 CPU 时间的平均百分比
CPU Usage - System (%)	当日系统进程占 CPU 时间的平均百分比
VmSize (KB)	当日分配给 Data Correlator 的平均内存大小，单位为千字节
VmRSS (KB)	当日 Data Correlator 使用的平均内存使用量，单位为千字节

入侵事件信息部分

在 管理中心和受管设备上，可以查看“统计信息”页面上有关入侵事件的摘要信息。此信息包括上次入侵事件的日期和时间、过去一小时和昨天发生的事件总数，以及数据库的事件总数。

注释 Statistics 页面 Intrusion Event Information 部分的信息依据是受管设备上存储的入侵事件，而不是发送到管理中心的信息。如果受管设备无法在本地存储（或配置为不存储）入侵事件，则此页面上不会列出入侵事件信息。

下表介绍了 Statistics 页面 Intrusion Event Information 部分显示的统计信息。

表 *45:* 入侵事件信息

统计信息	**Description**
上次警报时间	上次事件发生的日期和时间
上一小时事件总数	过去一个小时内发生的事件总数

统计信息	Description
上一日事件总数	过去 24 小时内发生的事件总数
数据库中的事件总数	事件数据库中的事件总数

查看系统统计信息

显示内容包括 管理中心 及其受管设备的统计信息。

开始之前

您必须是“管理员”或“维护”用户并位于“全局”域中才能查看系统统计信息。

过程

步骤 1 选择**系统**（⚙）> **监控** > **统计信息**。

步骤 2 从 **选择设备** 列表中选择设备，然后点击 **选择设备**。

步骤 3 查看可用统计信息。

步骤 4 在“磁盘使用率”(Disk Usage) 部分，您可以执行以下操作：

- 在**按类别 (By Category)** 层叠图中将指针悬停在一个磁盘使用类别上以（按顺序）查看：
  - 该类别使用的可用磁盘空间百分比
  - 该磁盘的实际存储空间
  - 该类别的总可用磁盘空间
- 点击**按分区**旁边的向下箭头将其展开。如果安装有恶意软件存储包，则系统会显示 `/var/storage` 分区使用情况。

步骤 5 （或者）点击 **进程** 旁边的箭头以查看 查看系统统计信息，第 407 页中所述的信息。

第 14 章

故障排除

以下主题描述如何诊断您可能在 Firepower 系统中遇到的问题：

故障排除最佳做法

- 在您进行更改以尝试修复问题之前，请生成故障排除文件以捕获原始问题。请参阅用于故障排除的运行状况监控器报告， 第 421 页及其子节。

  如果您需要联系思科 TAC 以获得支持，则您可能需要此故障排除文件。

- 可以通过查看“消息中心”中的错误和警告消息开始调查。请参阅 系统消息， 第 409 页

- 可以在您的产品的产品文档页面上的“故障排除和警报”标题下，查找适用的技术说明和其他故障排除资源。

系统消息

当需要跟踪发生在 Firepower 系统中的问题时，请从消息中心开始调查。通过此功能，可以查看 Firepower 系统持续生成的有关系统活动和状态的消息。

要打开消息中心，请点击位于主菜单中“部署”菜单旁边的“系统状态”图标。根据系统状态，此图标可采用以下形式之一：

- - 指示系统上存在一个或多个错误和任意数量的警告。
- - 指示系统上存在一个或多个警告而没有错误。
- - 指示系统上不存在任何警告或错误。

如果随该图标显示数字，则其指示错误或警告消息的当前总数。

要关闭消息中心，请点击 Firepower 系统 Web 界面内其外部的任意位置。

除消息中心以外，Web 界面也会显示对您的活动和日常系统活动的立即响应中的弹出通知。某些弹出通知在五秒后自动消失，而其他通知则“粘滞”，意味着它们会显示直至您通过点击**解除**（×）明确将其消除为止。点击通知列表顶部的**消除 (Dismiss)** 链接以一次性解除所有通知。

提示 将光标悬停在非粘滞弹出通知的上方会导致其粘滞。

系统根据用户的许可证、域和访问角色确定在弹出通知和消息中心内向其显示哪些消息。

消息类型

消息中心显示消息报告系统活动和状态，分为三个不同选项卡：

部署

此选项卡显示与系统中的每个设备的配置部署相关的当前状态，按域分组。系统在此选项卡上报告以下部署状态值。通过点击**显示历史记录**，可以获得有关部署作业的其他详细信息。

- 运行（**旋转**）- 该配置处于部署过程中。
- **成功** - 该配置已成功部署。
- **警告**（） - 警告部署状态利用 **警告系统状态图标**为所显示的消息计数提供帮助。
- **失败** - 该配置未能部署；请参阅 需要部署的配置更改。失败的部署利用 **错误系统状态图标**为所显示的消息计数提供帮助。

升级

此选项卡显示与托管设备的软件升级任务相关的当前状态。系统在此选项卡上报告以下升级状态值：

- **正在进行 (In progress)** - 表示升级任务正在进行。
- **已完成 (Completed)** - 表示软件升级任务已成功完成。
- **失败 (Failed)** - 表示软件升级任务未能完成。

运行状况

此选项卡显示系统中每个设备的当前运行状况信息，按域分组。运行状况由运行状况模块生成，如关于运行状况监控，第 341 页中所述。系统在此选项卡上报告以下运行状况状态值：

- **警告**（  ） - 表示对于设备中的运行状况模块而言，已超过警告限值，并且该问题尚未解决。“运行状况监控”页面利用**黄色三角形**（  ）来指示这些状况。警告状态利用**警告系统状态图标**为所显示的消息计数提供帮助。
- **严重**（  ） - 表示对于设备中的运行状况模块而言，已超过严重限值，并且该问题尚未解决。“运行状况监控”(Health Monitor) 页面利用 **严重**（  ） 图标来指示这些状况。严重状态利用 **错误系统状态图标**为所显示的消息计数提供帮助。
- **错误**（  ） - 表示设备中的运行状况监控模块出现故障，并且自故障发生后未能成功重新运行。“运行状况监控”页面利用**错误图标**来指示这些状况。错误状态利用**错误系统状态图标**为所显示的消息计数提供帮助。

可以点击“运行状况”(Health) 选项卡中的链接来查看有关“运行状况监控”(Health Monitor) 页面的详细信息。如果没有当前运行状况条件，“运行状况”(Health) 选项卡不显示消息。

任务

某些任务（例如配置备份或更新安装）需要一些时间来完成。此选项卡显示这些长时间运行任务的状态，并且可以包括由您或系统中的其他用户（如果您有适合的访问权限）发起的任务。此选项卡根据每条消息的最新更新时间，按时间倒序显示消息。某些任务状态消息包括有关所述任务的更详细信息的链接。系统在此选项卡上报告以下任务状态值：

- **等待()** - 表示等待另一个正在进行的任务完成后再运行的任务。此消息类型显示更新进度条。
- **运行** - 表示正在进行的任务。此消息类型显示更新进度条。
- **重试** - 表示自动重试的任务。请注意，并非所有的任务都可以重试。此消息类型显示更新进度条。
- **成功** - 表示已成功完成的任务。
- **失败** - 表示未成功完成的任务。失败的任务利用 **错误系统状态图标**为所显示的消息计数提供帮助。
- **停止或暂停** - 表示由于系统更新而中断的任务。停止的任务不能恢复。恢复正常操作后，再次启动任务。
- 已跳过 - 正在进行的进程阻止了任务的启动。重试以启动任务。

当新任务开始时，此选项卡中显示新消息。随着任务完成（状态成功、失败或停止），此选项卡继续以指示的最终状态显示消息，直至删除它们。思科建议您删除消息以减少“任务”(Tasks) 选项卡和消息数据库的混乱。

消息管理

从“消息中心”(Message Center) 可以执行以下操作：

- 选择以显示弹出通知。
- 显示系统数据库中的更多任务状态消息（如有任何尚未移除的此类消息）。
- 下载所有任务管理器通知的报告。
- 移除单个任务状态消息。（此操作会影响到可以查看已移除消息的所有用户。）
- 批量移除任务状态消息。（此操作会影响到可以查看已移除消息的所有用户。）

提示 思科建议您定期在“任务”(Task) 选项卡中移除积累的任务状态消息，使显示画面和数据库减少凌乱感。当数据库中的消息数接近 100,000 条时，系统会自动删除您已移除的任务状态消息。

查看基本系统信息

“关于”页面显示有关设备的信息，包括型号、序列号和系统各组件的版本信息。此页面还包含思科的版权信息。

过程

步骤 1 点击页面顶部工具栏中的 **帮助** （  ）。

步骤 2 选择**关于 (About)**。

查看设备信息

过程

选择**系统**（）> **配置**。

管理系统消息

过程

步骤 1 点击**通知 (Notifications)** 以显示消息中心。

步骤 2 有以下选项可供选择：

- 点击 **部署** 以查看与配置部署相关的消息。请参阅查看部署消息，第 413 页。您必须是 Admin 用户或者拥有**将配置部署到设备**的权限才能查看这些消息。
- 点击**升级 (Upgrades)** 以查看与设备升级任务相关的消息。请参阅“查看升级消息”。请参阅查看升级消息。您必须是管理员用户或者拥有**更新**权限才能查看这些消息。

  系统将显示新的建议升级版本。您可以选择分别使用“ **提醒我** ”或“ **详细信息** ”选项设置提醒或查看更多信息。

- 点击 **运行状况** 以查看与您的 管理中心 和在其中注册的设备相关的消息。请参阅查看运行状况消息，第 415 页。您必须是管理员用户或者拥有 **运行状况** 的权限才能查看这些消息。

  您可以通过点击 **运行状况监控器** 链接导航到“运行状况监控器”页面。

- 点击 **任务** 以查看或管理与长期运行任务相关的消息。请参阅查看任务消息，第 415 页或管理任务消息，第 416 页。每个人都可以看到自己的任务。要查看其他用户的任务，您必须是 Admin 用户或拥有**查看其他用户的任务**权限。您可以通过点击**删除已完成的任务**链接从通知中删除已完成的任务。
- 点击**下载报告 (Download Report)** 图标可生成任务管理器中所有通知的报告。选择**下载 CSV (Download CSV)** 或**下载 PDF (Download PDF)** 以下载报告。
- 点击**显示通知 (Show notifications)** 滑块以启用或禁用弹出通知显示。

查看部署消息

您必须是 Admin 用户或者拥有**将配置部署到设备**的权限才能查看这些消息。

过程

步骤 1 点击**通知 (Notifications)** 以显示消息中心。

步骤 2 点击**部署 (Deployments)**。

步骤 3 有以下选项可供选择：

- 点击**总计 (total)** 以查看所有当前部署状态。
- 点击状态值以只查看具有该部署状态的消息。

- 将光标悬停在消息的已逝时间指标上（例如，**1m 5s**）可查看已逝时间，以及部署的开始和停止时间。

步骤 4 点击**显示部署历史 (show deployment history)** 查看有关部署作业的更多详细信息。

Deployment History 表在左侧列中以时间倒序列出部署作业。

a) 选择部署作业。

右侧列中的表显示该作业中包含的各个设备，以及每个设备的部署状态。

b) 要查看设备的响应以及部署期间发送到设备的命令，请点击设备的**脚本 (Transcript)** 列中的下载图标。

该脚本包含以下各节：

- **Snort Apply** - 如果 Snort 相关的策略中有任何故障或响应，此部分中会显示消息。通常，该部分为空。
- **CLI Apply** - 此部分涵盖使用发送到 Lina 进程的命令配置的功能。
- **Infrastructure Messages** - 此部分显示不同部署模块的状态。

在 **CLI Apply** 部分中，部署脚本包括发送到设备的命令以及从该设备返回的任何响应。这些响应可以是信息性消息或错误消息。对于失败的部署，请查找指示命令错误的消息。如果您正在使用 FlexConfig 策略配置自定义的功能，则检查这些错误特别有用。这些错误可帮助您纠正尝试配置这些命令的 FlexConfig 对象中的脚本。

注释 为托管功能发送的命令与从 FlexConfig 策略生成的命令之间没有显著差异。

例如，以下序列显示 管理中心 发送了命令来为 GigabitEthernet0/0 配置外部逻辑名。设备的响应是自动将安全级别设置为 0。威胁防御 不使用任何安全级别。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

查看升级消息

您必须是管理员用户或者拥有**更新**权限才能查看这些消息。

过程

步骤 1 点击**通知 (Notifications)** 以显示消息中心。

步骤 2 点击**升级 (Upgrades)**。

步骤 3 可以执行以下操作：

- 点击**总计**以查看所有当前升级任务。
- 点击状态值以只查看具有该状态的消息。
- 点击**设备管理 (Device Management)**，了解有关升级任务的更多详细信息。

查看运行状况消息

您必须是管理员用户或者拥有 **运行状况** 的权限才能查看这些消息。

过程

步骤 1 点击**通知 (Notifications)** 以显示消息中心。

步骤 2 点击 **运行状况**。

步骤 3 有以下选项可供选择：

- 点击 **总计** 以查看所有当前运行状态。还显示严重性的细分，即警告、严重和错误。
- 点击状态值以只查看具有该状态的消息。
- 将光标悬停在消息的相对时间指标上（例如，**3 天前**）可查看该消息最新更新的时间。
- 要查看特殊信息的详细运行状态信息，请点击该消息。
- 要查看“运行状况监控器”(Health Monitor) 页面上的完整运行状态，请点击 **运行状况监控器**。

相关主题

关于运行状况监控，第 341 页

查看任务消息

每个人都可以看到自己的任务。要查看其他用户的任务，您必须是 Admin 用户或拥有**查看其他用户的任务**权限。

过程

步骤 1 点击**通知 (Notifications)** 以显示消息中心。

步骤 2 点击**任务 (Tasks)**。

步骤 3 有以下选项可供选择：

- 点击**总计 (total)**以查看所有当前任务状态。要根据状态（即等待、正在运行、正在重试、成功和失败）查看任务，请点击它们。
- 点击状态值以只查看具有该状态的任务的消息。

注释　已停止任务的消息仅显示在任务状态消息总列表中。您无法过滤已停止任务。

- 将光标悬停在消息的相对时间指标上（例如，**3 天前**）可查看该消息最新更新的时间。
- 点击消息中的任何链接，查看有关该任务的详细信息。
- 如果可显示更多任务状态消息，请点击消息列表底部的**获取更多消息 (Fetch more messages)** 以对其进行检索。

管理任务消息

每个人都可以看到自己的任务。要查看其他用户的任务，您必须是 Admin 用户或拥有**查看其他用户的任务**权限。

过程

步骤 1 点击“系统状态”(System Status) 以显示消息中心。

步骤 2 点击“任务”(Tasks)。

步骤 3 有以下选项可供选择：

- 如果可显示更多任务状态消息，请点击消息列表底部的**获取更多消息 (Fetch more messages)** 以对其进行检索。
- 要移除一条已完成的任务的消息（状态为已停止、成功或失败），请点击该消息旁边的 **删除**（ ）。
- 要移除已完成的所有任务的全部消息（状态为已停止、成功或失败），请使用**总数 (total)** 过滤消息，然后点击**移除所有已完成的任务 (Remove all completed tasks)**。
- 要移除已成功完成的所有任务的全部消息，请使用**成功 (success)** 过滤消息，然后点击**移除所有成功的任务 (Remove all successful tasks)**。
- 要移除已失败的所有任务的全部消息，请使用**失败 (failure)** 过滤消息，然后点击**移除所有失败的任务 (Remove all failed tasks)**。

运行状况监控器警报的内存使用阈值

内存使用率情况模块将设备的内存使用率与为模块配置的限值进行对比，并在使用率超过该级别时发出警报。模块监控来自受管设备和 管理中心 本身的数据。

内存使用率的两个可配置阈值（严重和警告）可设置为已用内存的百分比。当超过这些阈值时，系统将生成具有指定严重性级别的运行状况警报。但是，运行状况警报系统不会以准确的方式计算这些阈值。

使用高内存设备时，某些进程预计会使用比低内存占用的设备更大的总系统内存百分比。设计的目的是尽可能多地使用物理内存，同时为辅助进程留出少量可用内存。

比较两台设备，一台有 32 GB 内存，一台有 4 GB 内存。在具有 32 GB 内存的设备中，5% 内存 (1.6GB) 是比具有 4 GB 内存的设备（4GB 的 5% = 200MB）留给辅助进程更大的内存值。

为了说明某些进程使用系统内存的百分比较高，管理中心 会计算总内存以包括总物理内存和总交换内存。因此，用户配置的阈值输入的强制内存阈值可能会导致运行状况事件，其中事件的“值”列与为确定超出阈值而输入的值不匹配。

从版本 7.4.1 开始，内存使用情况运行状况模块通过考虑可用内存、可用交换内存和缓冲区缓存来计算内存使用情况。为避免过早的内存使用状况警报，建议不要分别超过警告和严重警报阈值 88% 和 90%。

下表显示用户输入阈值和强制阈值的示例，具体取决于安装的系统内存。

注释 此表中的值为示例。您可以使用此信息外推与此处显示的已安装 RAM 不匹配的设备的阈值，也可以联系 Cisco TAC 进行更精确的阈值计算。

表 *46:* 基于已安装 ***RAM*** 的内存使用率阈值

用户输入阈值	每个安装的内存 (RAM) 的实施阈值			
	4 GB	**6 GB**	**32 GB**	**48 GB**
10%	10%	34%	72%	81%
20%	20%	41%	75%	83%
30%	30%	48%	78%	85%
40%	40%	56%	81%	88%
50%	50%	63%	84%	90%
60%	60%	70%	88%	92%
70%	70%	78%	91%	94%
80%	80%	85%	94%	96%
90%	90%	93%	97%	98%
100%	100%	100%	100%	100%

注意 如果管理中心达到临界系统内存条件，则系统可能会终止使用大量内存的进程，或者如果内存使用率仍然很高，则重新启动 管理中心 。

磁盘使用率和事件消耗情况运行状况监控警报

硬盘使用状况模块将受管设备的硬盘驱动器和恶意软件存储包中的磁盘使用率与为该模块配置的限值进行对比，并在使用率超过为模块配置的百分比时发出警报。基于模块阈值，当系统删除过多的监控磁盘使用类别的文件，或者当这些类别以外的磁盘使用率达到过高级别时，该模块也发出警报。

本主题介绍磁盘使用情况运行状况模块生成的“耗尽未处理事件”运行状况警报的症状和故障排除指南。

磁盘管理器进程管理设备的磁盘使用情况。磁盘管理器监控的每种文件类型都分配有一个孤岛。根据系统上可用的磁盘空间量，磁盘管理器会为每个孤岛计算高水位线（HWM）和低水位线（LWM）。

要显示系统每个部分（包括孤岛、低水位线和高水位线）的磁盘使用情况详细信息，使用 **show disk-manager** 命令。

示例

以下是磁盘管理器信息的示例。

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        499.197 MB  1.950 GB
Action Queue Results                0 KB        499.197 MB  1.950 GB
User Identity Events                0 KB        499.197 MB  1.950 GB
UI Caches                           4 KB        1.462 GB    2.925 GB
Backups                             0 KB        3.900 GB    9.750 GB
Updates                             0 KB        5.850 GB    14.625 GB
Other Detection Engine              0 KB        2.925 GB    5.850 GB
Performance Statistics              33 KB       998.395 MB  11.700 GB
Other Events                        0 KB        1.950 GB    3.900 GB
IP Reputation & URL Filtering       0 KB        2.437 GB    4.875 GB
Archives & Cores & File Logs        0 KB        3.900 GB    19.500 GB
Unified Low Priority Events         1.329 MB    4.875 GB    24.375 GB
RNA Events                          0 KB        3.900 GB    15.600 GB
File Capture                        0 KB        9.750 GB    19.500 GB
Unified High Priority Events        0 KB        14.625 GB   34.125 GB
IPS Events                          0 KB        11.700 GB   29.250 GB
```

运行状况警报格式

当 管理中心 上的运行状况监控进程运行时（每 5 分钟一次或触发手动运行）时，磁盘使用情况模块会查看diskmanager.log文件，如果满足正确的条件，则会触发运行状况警报。

运行状况警报的结构为 - Drain of unprocessed events from <*SILO NAME*>。

例如，来自低优先级事件中的未处理事件的消耗。

重要事项 只有事件孤岛会生成 来自 <*SILO NAME*>的未处理事件的消耗 运行状况警报。此警报的严重性级别始终为 **严重** 。

除警报外，其他症状还包括：

- 管理中心 用户界面上的速度缓慢
- 事件丢失

常见故障排除场景

在 来自 <*SILO NAME*>的未处理事件的消耗 运行状况警报，这也可能是事件处理路径中的瓶颈导致的。

这些磁盘使用率警报存在三个潜在瓶颈：

- 日志记录过多 - 威胁防御 上的事件处理程序进程超额订用（其读取速度比 Snort 写入的速度慢）。
- Sftunnel 瓶颈-事件接口不稳定或超订用。
- SFDataCorrelator 瓶颈 - 管理中心 和托管设备之间的数据传输通道超订用。

过多日志记录

此类运行状况警报的最常见原因之一是输入过多。从 **show disk-manager** 命令中收集的低水位线（LWM）和高水位线（HWM）之间的差异显示，该筒仓中有多少空间可用于从LWM（刚耗尽）到HWM值。如果有未处理的事件，请查看日志记录配置。

- 检查重复日志记录-如果您查看 管理中心上的相关器 *perfstats*，则可以识别重复日志记录场景：

  ```
  admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
  ```

- 检查 ACP 的日志记录设置-检查访问控制策略（ACP）的日志记录设置。如果日志记录设置包括连接的“开始”和“结束”，请修改设置以仅记录结束，以减少事件数量。

  确保按照 连接日志记录最佳实践，第 707 页中所述的最佳实践。

通信瓶颈-Sftunnel

Sftunnel 负责 管理中心 和托管设备之间的加密通信。事件通过隧道发送到 管理中心。托管设备和 管理中心 之间的通信信道 (sftunnel) 中的连接问题和/或不稳定可能是由于：

- Sftunnel 关闭或不稳定（振荡）。

  确保 管理中心 和托管设备在其 TCP 端口 8305 上的管理接口之间具有可访问性。

  sftunnel 进程应稳定且不应意外重启。通过检查 **/var/log/message** 文件并搜索包含 ***sftunneld*** 字符串的消息来验证此项。

- Sftunnel 已超额订用。

  查看来自健康监控器的趋势数据，并查找 管理中心管理接口超订用的迹象，这可能是管理流量激增或持续超订用。

  作为 eventing 的辅助管理接口使用。要使用此接口，您必须在 威胁防御 CLI 上使用 **configure network management-interface** 命令来配置其 IP 地址和其他参数。

通信瓶颈 - SFDataCorrelator

SFDataCorrelator 管理 管理中心 和托管设备之间的数据传输；在 管理中心上，它会分析系统创建的二进制文件以生成事件，连接数据和网络映射。第一步是查看 **diskmanager.log** 文件，了解要收集的重要信息，例如：

- 消耗的频率。
- 耗尽未处理事件的文件数。
- 发生未处理事件的情况。

每次磁盘管理器进程运行时，都会在其自己的日志文件（位于 **[/ngfw]/var/log/diskmanager.log**下）为每个不同的孤岛生成一个条目。从 diskmanager.log（CSV 格式）收集的信息可用于帮助缩小搜索范围。

额外故障排除步骤：

- 该 **stats_unified.pl** 命令可帮助您确定托管设备是否确实有一些数据必须发送到 管理中心。当托管设备和管理中心 遇到连接问题时，可能会发生这种情况。受管设备将日志数据存储到硬盘驱动器上。

  ```
  admin@FMC:~$ sudo stats_unified.pl
  ```

- **manage_proc.pl** 命令可以在 管理中心 端重新配置相关器。

  ```
  root@FMC:~# manage_procs.pl
  ```

在联系 Cisco 技术支持中心 (TAC) 之前 。

强烈建议您在联系 Cisco TAC之前收集以下物品：

- 看到的运行状况警报的截图。
- 对从 管理中心生成的文件进行故障排除。
- 对从受影响的受管设备生成的文件进行故障排除。

  首次发现问题的日期和时间。

- 有关最近对策略所做的任何更改的信息（如果适用）。

  stats_unified.pl 命令的输出，如 通信瓶颈 - SFDataCorrelator ， 第 420 页中所述。

设备配置历史记录文件的磁盘使用情况

磁盘使用情况运行状况模块监控管理中心上的设备配置历史记录文件的大小，并在大小超过允许的限制时发送运行状况警报。用于存储设备配置历史记录文件的最大磁盘大小为 20 GB。在 管理中心高可用性部署中，仅当 HA 同步暂停时，此运行状况警报才会显示在备用 管理中心 上。

设备配置历史记录文件的大小超过允许的限制可能会导致升级 管理中心就绪性失败。在 管理中心高可用性部署中，超过设备配置历史记录文件大小限制可能会降低 HA 同步速度。

要解决设备配置历史记录文件大小运行状况警报，请依次选择 **部署** > **部署历史记录** > **部署设置** > **配置版本设置**，并减少 **要保留的版本数**。减少版本数量会删除最早的配置版本，以匹配您选择的版本大小。 **估计配置版本大小** 根据您选择保留的版本数提供 管理中心上的配置历史记录文件的大致大小。使用估计值更改版本数，以将配置版本的大小降低到允许的限制以下。

有关详细信息，请参阅 Cisco Secure Firewall Management Center Snort 3 配置指南中的 设备配置版本的序号 。

用于故障排除的运行状况监控器报告

某些情况下，如果您的设备有问题，支持人员可能要求您提供故障排除文件以帮助诊断该问题。系统可以使用以特定功能区域为目标的信息生成故障排除文件，以及您可与支持人员合作检索的高级故障排除文件。您可以选择下表中列出的任何选项，为特定功能定制故障排除文件的内容。

请注意，在所报告的数据方面，某些选项重叠，但是无论您选择什么选项，故障排除文件都不会包含冗余备份。

表 *47*: 可选择的故障排除选项

该选项...	报告...
Snort 性能和配置 (Snort Performance and Configuration)	与设备上的 Snort 相关的数据和配置设置
硬件性能和日志 (Hardware Performance and Logs)	与设备硬件性能相关的数据和日志
系统配置、策略和日志	与设备的当前系统配置相关的配置设置、数据和日志
检测配置、策略和日志	与对设备的检测相关的配置设置、数据和日志
接口和网络相关数据 (Interface and Network Related Data)	与设备的内联集和网络配置相关的配置设置、数据和日志
发现、感知、VDB 数据和日志	与设备上当前的发现和感知配置相关的配置设置、数据和日志
升级数据和日志 (Upgrade Data and Logs)	与设备的前期升级相关的数据和日志
所有数据库数据 (All Database Data)	包含在故障排除报告中的所有数据库相关数据
所有日志数据 (All Log Data)	设备数据库收集的所有日志
网络映射信息 (Network Map Information)	当前网络拓扑数据

为特定系统功能生成故障排除文件

可以生成和下载可发送给支持人员的自定义故障排除文件。

开始之前

您必须是管理员、维护人员、安全分析师或安全分析师（只读）用户才能执行此任务。

过程

步骤 1 执行 查看设备运行状况监控器，第 372 页中的步骤。

步骤 2 依次选择 **系统**（⚙）> **运行状况** > **监控**，点击左侧面板中的设备，然后点击 **查看系统和故障排除详细信息**，然后点击 **生成故障排除文件**。

注释
- 当您从 管理中心 Web 接口生成 管理中心 故障排除文件时，该文件存储在 管理中心中。请注意，只有最新的故障排除文件会存储在 管理中心中。
- 当您从 管理中心 Web 接口生成 威胁防御 故障排除文件时，该文件将在 威胁防御 中生成并复制到 管理中心。请注意，只有最新的 威胁防御 故障排除文件会存储在管理中心中。
- 当从 CLI 生成 管理中心 和 威胁防御 的故障排除文件时，所有版本的故障排除文件都分别在 管理中心 和 威胁防御 中进行维护。

步骤 3 选择“所有数据”生成所有可能的故障排除数据或选中单个复选框，如 查看任务消息，第 415 页中所述。

步骤 4 点击**生成**。

步骤 5 在消息中心查看任务消息；请参阅查看任务消息，第 415 页。

步骤 6 找出对应所生成的故障排除文件的任务。

步骤 7 在设备生成故障排除文件并且任务状态变更为已完成之后，点击**点击检索生成的文件**。

步骤 8 按照浏览器的提示下载文件。（故障排除文件将下载到一个 `.tar.gz` 文件中。）

步骤 9 按照支持部门的指示将故障排除文件发送给思科。

下载高级故障排除文件

您可以下载故障排除文件。

开始之前

您必须是管理员、维护人员、安全分析师或安全分析师（只读）用户才能执行此任务。

过程

步骤 1 查看设备的运行状况监控器；请参阅 查看设备运行状况监控器，第 372 页。

步骤 2 依次选择 **系统**（⚙）> **运行状况** > **监控**，点击左侧面板中的设备，然后点击 **查看系统和故障排除详细信息**，然后点击 **高级故障排除**。

步骤 3 在 **文件下载**，输入支持部门提供的文件名。

步骤 4 点击**下载 (Download)**。

步骤 5 按照浏览器的提示下载文件。

注释　对于受管设备，系统通过将设备名称置于文件名前面来重命名文件。

步骤 6 按照支持部门的指示将故障排除文件发送给思科。

一般故障排除

内部电源故障(硬件故障、电涌等)或外部电源故障(未插线)可能导致系统不正常关闭或重新启动。这些情况可能导致数据损坏。

基于连接的故障排除

基于连接的故障排除或调试可跨模块提供统一调试，以收集特定连接的相应日志。它还支持最多七级的基于级别的调试，并为 lina 和 Snort 日志启用统一的日志收集机制。基于连接的调试支持以下功能：

- 一种常见的基于连接的调试子系统，用于对 威胁防御中的问题进行故障排除
- 跨模块的调试消息的统一格式
- 重新启动后的持续调试消息
- 基于现有连接的跨模块端到端调试
- 调试正在进行的连接

注释　Firepower 2100 系列设备不支持基于连接的调试。

有关连接故障排除更多信息，请参阅 连接故障排除 ， 第 423 页。

连接故障排除

过程

步骤 1 使用 **调试数据包-条件** 命令配置过滤器以识别连接。

示例：

```
Debug packet-condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177
255.255.255.255
```

步骤 2 为感兴趣的模块和相应级别启用调试。输入 **调试数据包** 命令。

示例：

```
Debug packet acl 5
```

步骤 3 使用以下命令开始调试数据包：

```
debug packet-start
```

步骤 4 使用以下命令从数据库获取调试消息以分析调试消息：

```
show packet-debugs
```

步骤 5 使用以下命令停止调试数据包：

```
debug packet-stop
```

Cisco Secure Firewall Threat Defense 设备的高级故障排除

可以使用数据包跟踪器和数据包捕获功能在 Cisco Secure Firewall Threat Defense设备上执行深度故障排除分析。数据包跟踪器允许防火墙管理员向安全装置中注入虚拟数据包，跟踪从入口到出口的流量。在跟踪过程中，根据流量和路由查找、ACL、协议检查、NAT 和入侵检测。此实用程序非常有效，因为它能通过使用协议和端口信息指定源和目标地址来模拟实际流量的功能。跟踪选项可捕获数据包，从而判断出数据包是否已删除或是否成功。

有关故障排除文件的详细信息，请参阅 下载高级故障排除文件，第 422 页。

数据包捕获概述

带有跟踪选项的数据包捕获功能允许通过系统跟踪在入口接口上捕获的真实数据包。跟踪信息将在以后阶段显示。这些数据包不会在出口接口上被丢弃，因为它们是真正的数据路径流量。针对 威胁防御 设备的数据包捕获支持对数据包进行故障排除和分析。

获取数据包后，Snort 将检测在数据包中启用的跟踪标志。Snort 会写入跟踪器元素，数据包通过它进行遍历。由于捕获数据包而导致的 Snort 断言可以是以下：之一。

表 *48: Snort* 判定

裁定	说明
通过	允许分析的数据包。
阻止	数据包未转发。
更换	数据包已修改。
AllowFlow	流直接通过，不经过检查。
BlockFlow	流被阻止。

裁定	说明
忽略	流被阻止；仅当流在被动接口上受阻时才会发生。
重试	流停滞，正在等待 enamelware 或 URL 类别/信誉查询。在超时的情况下，处理继续进行，但结果未知：如果是漆包，则允许该文件；在 URL 类别/信誉的情况下，AC 规则查找将继续使用未分类和未知的信誉。

根据 Snort 判定，丢弃或允许数据包。例如，如果 Snort 判定为 **BlockFlow**，数据包将被丢弃，并且会话中的后续数据包在到达 Snort 之前会被丢弃。当 Snort 判定为 **阻止** 或 **BlockFlow**时， **丢弃原因** 可以是以下其中一项：

表 *49:* 丢弃原因

被阻止或流被阻止...	原因
Snort	Snort无法处理数据包，例如，由于数据包已损坏或格式无效，snort 无法解码。
预处理的应用 ID	应用 ID 模块/预处理本身不会阻止数据包；但这可能表示应用 ID 检测导致其他模块（例如，防火墙）匹配阻止规则。
SSL 预处理	SSL 策略中存在与流量匹配的阻止/重置规则。
防火墙	防火墙策略中有一个阻止/重置规则来匹配流量。
已预处理的强制网络门户	存在使用身份策略匹配流量的阻止/重置规则。
安全搜索预处理	有使用防火墙策略中的安全搜索功能来匹配流量的阻止/重置规则。
SI 预处理	AC 策略的“安全情报”选项卡中有一个阻止/重置规则，用于阻止流量、例如 DNS 或 URL SI 规则。
过滤器预处理	AC 策略的过滤器选项卡中有一个阻止/重置规则来匹配流量。
已预处理的数据流	存在入侵规则阻止/重置流连接，例如，当 TCP 规范化错误时阻止。
会话预处理	此会话之前已被某个其他模块阻止，因此会话预处理将阻止同一会话的更多数据包。
分片预处理	阻塞，因为数据的较早分片被阻止。

被阻止或流被阻止...	原因
预处理的 Snort 响应	有一个 react snort 规则，例如，发送有关特定 HTTP 流量的响应页面。
预处理的 Snort 响应	有一个 snort 规则，用于在数据包匹配条件时发送自定义响应。
信誉预处理	数据包匹配信誉规则，例如阻止给定 IP 地址。
预处理后的 x-Link2State	由于在 SMTP 中检测到缓冲区溢出漏洞而被阻止。
后孔预处理	由于检测到 backorifice 数据而阻塞。
SMB 预处理	有一条 snort 规则可阻止 SMB 流量。
已预处理的文件进程	有阻止文件的文件策略，例如，阻止程序。
IPS 预处理	有一个使用 IPS 的 snort 规则，例如，速率过滤。

数据包捕获功能支持捕获和下载存储在系统内存中的数据包。但是，由于内存限制，缓冲区大小限制为 32 MB。能够处理大量数据包捕获的系统会快速超出最大缓冲区大小，从而有必要提高数据包捕获限制。使用辅助内存（通过创建文件写入捕获数据）可达到此目的。支持的最大文件大小为 10 GB。

配置了 **file-size** 时，捕获的数据会存储到该文件，系统则会基于捕获名称 **recapture** 分配文件名称。

当需要捕获大小限制超过 32 MB 的数据包时，就会使用该 **file-size** 选项。

有关更多信息，请参阅Cisco Secure Firewall Threat Defense 命令参考。

使用捕获跟踪

数据包捕获是一种实用程序，可根据定义的条件提供通过设备的指定接口的网络流量的实时快照。只要此过程未暂停或分配的内存未耗尽，它就会继续捕获数据包。

数据包捕获信息包括来自 Snort 和预处理器的关于裁定以及系统在处理数据包时所采取的操作的信息。同时可以进行多个数据包捕获。可将系统配置为修改、删除、清除和保存捕获。

注释 捕获数据包数据需要数据包复制。此操作可能会导致处理数据保持出现延迟，并有可能降低数据包吞吐量。我们建议使用数据包过滤器来捕获特定的流量数据。

开始之前

要在 Cisco Secure Firewall Threat Defense 设备上使用数据包捕获工具，您必须是管理员或维护用户。

过程

步骤 1 在管理中心上，选择**设备** > **数据包捕获**。

步骤 2 选择设备。

步骤 3 点击**添加捕获**。

步骤 4 为捕获跟踪输入**名称**。

步骤 5 为捕获跟踪选择**接口**。

步骤 6 指定**匹配条件**详细信息：

a) 选择**协议**。

b) 为**源主机**输入 IP 地址。

c) 为**目标主机**输入 IP 地址。

d) （可选）选中 **SGT 编号**复选框，然后输入安全组标记 (SGT)。

步骤 7 指定**缓冲区**详细信息：

a) （可选）输入最大**数据包大小**。

b) （可选）输入最小**缓冲区大小**。

c) 如果希望捕获的流量没有中断，请选择**连续捕获**；如果希望捕获在达到最大缓冲区大小时停止，则请选择**在已满时停止**。

注释 如果启用了 **继续捕获** ，则当分配的内存已满时，内存中最早捕获的数据包将被新捕获的数据包覆盖。

d) 如果希望捕获每个数据包的详细信息，请选中 **跟踪**复选框。

e) 在 **跟踪计数** 字段中输入值。默认值为 128。可以输入介于 1-1000 范围内的值。

步骤 8 点击**保存**。

数据包捕获屏幕显示数据包捕获详细信息及其状态。要自动刷新数据包捕获页面，请选中 **启用自动刷新** 复选框，然后输入自动刷新间隔（以秒为单位）。

您可以对数据包执行以下操作：

- **编辑**（ ） 修改捕获条件。
- **删除**（ ） 以删除数据包捕获和捕获的数据包。
- **清除**（ ）清除数据包捕获中捕获的所有数据包。要从所有现有数据包捕获中清除捕获的数据包，请点击 **清除所有数据包**。
- **暂停**（ ） 暂时停止捕获数据包。
- **保存**（ ） 在本地计算机上以 ASCII 或 PCAP 格式保存捕获的数据包的副本。选择所需的格式选项，然后点击 **保存**。保存的数据包捕获将下载到您的本地计算机。
- 要查看正在捕获的数据包的详细信息，请点击所需的捕获行。

数据包跟踪器概览

通过数据包跟踪工具，您可以对具有源地址、目标地址和协议特征的数据包进行建模，从而测试策略配置。跟踪会根据配置的访问规则、NAT、路由、访问策略和速率限制策略进行策略查询，以验证数据包是允许访问还是拒绝访问。数据包流基于接口、源地址、目标地址、端口和协议进行模拟。通过这种测试数据包的方法，您可以验证策略的有效性，并测试是否按要求处理了您希望允许或拒绝的流量类型。

除了验证配置之外，您还可以使用跟踪器调试意外行为，例如数据包本应被允许，但却被拒绝访问的情况。为全面模拟数据包，数据包跟踪器会跟踪数据路径 - 慢速路径和快速路径模块。初始，处理会根据每个会话和每个数据包进行。当防火墙按会话或按数据包处理数据包时，数据包跟踪工具和捕获与跟踪功能按数据包记录跟踪数据。

PCAP 文件

您可以使用具有完整的数据流的 PCAP 文件来启动数据包跟踪器。目前，仅支持具有最多 100 个数据包的单个基于 TCP/UDP 的流的 PCAP。数据包跟踪器工具读取 PCAP 文件，初始化客户端和服务器重放实体的状态。该工具开始以同步方式重放数据包，方法是在 PCAP 中收集和存储每个数据包的跟踪输出，以便进行后续处理和显示。

PCAP 重放

数据包重放按 PCAP 文件中的数据包顺序执行，对重放活动的干扰（如有）都会终止重放活动并结束重放。系统将为指定入口接口和出口接口上的 PCAP 中的所有数据包生成跟踪输出，从而提供流评估的完整情景。

在重放期间动态修改数据包的一些功能（例如 IPsec、VPN、SSL 、HTTPS 解密、NAT 等）不支持 PCAP 重放。

使用数据包跟踪器

要在 Cisco Secure Firewall Threat Defense 设备上使用数据包跟踪器，您必须是管理员或维护用户。

过程

步骤 1 在管理中心上，选择**设备** > **Packet Tracer**。

步骤 2 从 **选择设备** 下拉列表中，选择要为其运行跟踪的设备。

步骤 3 从 **接口** 下拉列表中，选择数据包跟踪的入口接口。

注释 请勿选择 VTI。数据包跟踪器不支持 VTI 作为入口接口。

步骤 4 要在数据包跟踪器中使用 PCAP 重放，请执行以下操作：

a) 点击 **选择 PCAP 文件**。

b) 要上传新的 PCAP 文件，请点击 **上传 PCAP 文件**。要重新使用最近上传的文件，请点击列表中的文件。

注释 仅支持 .pcap 和 .pcapng 文件格式。PCAP 文件只能包含一个基于 TCP/UDP 的流，最多 100 个数据包。PCAP 文件名（包括文件格式）的最大字符数限制为 64。

c) 在 **上传 PCAP** 框中，您可以拖动 PCAP 文件，也可以在框中点击以浏览并上传文件。选择文件后，上传过程会自动启动。

d) 转至此 步骤 13.

步骤 5 要定义跟踪参数，请从 **协议** 下拉菜单中选择跟踪的数据包类型，并指定协议特征：

- **ICMP** - 输入 ICMP 类型、ICMP 代码 (0-255)，并且可以选择键入 ICMP 标识符。
- **TCP/UDP/SCTP** - 输入源和目标端口号。
- **GRE/IPIP**-输入协议编号 0-255。
- **ESP**-输入源的 SPI 值 0-4294967295。
- **RAWIP**-输入端口号 0-255。

步骤 6 选择数据包跟踪的 **源类型** ，然后输入源 IP 地址。

源和目标类型包括 IPv4、IPv6 和完全限定域名 (FQDN)。如果使用思科 TrustSec，则可以指定 IPv4 或 IPv6 地址和 FQDN。

步骤 7 选择数据包跟踪的**源端口**。

步骤 8 选择数据包跟踪的**目标**类型，然后输入目标 IP 地址。

目标类型选项因您选择的源类型而异。

步骤 9 选择数据包跟踪的**目标端口**。

步骤 10 （可选）如果要跟踪安全组标记 (SGT) 值嵌入到层 2 CMD 标头 (TrustSec) 中的数据包，请输入有效的 **SGT 编号**。

步骤 11 如果希望数据包跟踪器进入父接口（稍后重定向到子接口），请输入 **VLAN ID**。

此值仅对非子接口可选，因为可以在子接口上配置所有接口类型。

步骤 12 为数据包跟踪指定**目标 MAC 地址**。

如果 Cisco Secure Firewall Threat Defense设备在透明防火墙模式下运行，并且入口接口为 VTEP，那么如果您在 **VLAN ID**中输入值，需要填写**目标 MAC 地址**。如果接口是桥接组成员，输入 **VLAN ID** 值时，**目标 MAC 地址**可选，不输入 **VLAN ID** 值时该值必填。

如果 Cisco Secure Firewall Threat Defense 在路由防火墙模式下运行时，如果输入接口是桥接组成员，**VLAN ID** 和 **目标 MAC 地址** 可选。

步骤 13 （可选）如果您希望 Packet Tracer 忽略对模拟数据包的安全检查，请点击 **绕过模拟数据包的所有安全检查**。这使得数据包跟踪器能够通过系统继续跟踪数据包，否则这些数据包将被丢弃。

步骤 14 （可选）要允许通过出口接口从设备发出数据包，请点击 **允许从设备传输模拟数据包**。

步骤 15 （可选）如果您希望 Packet Tracer 将注入的数据包视为 IPsec/SSL VPN 解密的数据包，请点击 **将模拟数据包视为 IPsec/SSL VPN 解密**。

步骤 16 点击 **Trace**（跟踪）。

跟踪结果 显示 PCAP 数据包通过系统的每个阶段的结果。点击单个数据包可查看数据包的跟踪结果。可以执行以下操作：

- 将 () 跟踪结果复制到剪贴板。
- 展开或折叠 () 显示的结果。
- 最大化 () 跟踪结果屏幕。

系统将显示每个阶段的已用时间信息，这些信息有助于衡量处理工作量。结果部分还会显示从入口接口流向出口接口的整个数据包流所花费的总时间。

跟踪历史记录 窗格显示每个 PCAP 跟踪的已存储跟踪详细信息。它最多可以存储 100 个数据包跟踪。您可以选择已保存的跟踪并再次运行数据包跟踪活动。可以执行以下操作：

- 使用任何跟踪参数搜索跟踪。
- 禁用使用 按钮将跟踪保存到历史记录。
- 删除特定跟踪结果。
- 清除所有痕迹。

如何从 Web 接口使用 威胁防御 诊断 CLI

您可以从 管理中心 执行所选的 威胁防御 诊断 CLI 命令。命令 **ping**（**ping system** 除外）、**traceroute** 和选择 **show** 命令在诊断 CLI 中运行，而不是在常规 CLI 中运行。

在运行 **show** 命令时，如果收到消息无法正确执行命令。请查看日志以了解更多详细信息，这意味着该命令在诊断 CLI 中无效。例如，**show access-list** 有效，但如果输入 **show access-control-policy**，则会显示此消息。要使用非诊断命令，请使用 SSH 登录到管理中心外部的设备。

有关 威胁防御 CLI 的详细信息，请参阅 Cisco Secure Firewall Threat Defense 命令参考。

开始之前

- 您必须是管理员、维护人员或安全分析师才能使用诊断 CLI。
- 诊断 CLI 的目的是使您能够快速使用一些命令，这些命令可用于对设备进行故障排除。要访问全部命令，请直接与设备打开 SSH 会话。
- 在使用 管理中心 高可用性的部署中，诊断 CLI 仅在主用 管理中心 中可用。

过程

步骤 1 选择**设备** > **威胁防御 CLI**。

您还可以通过设备的运行状况监控器访问 CLI 工具（**系统**（⚙） > **运行状况** > **监控**）。在这里，您可以选择设备，点击 **查看系统和故障排除详细信息** 链接，点击 **高级故障排除**，然后点击该页面上的 **威胁防御 CLI** 。

步骤 2 从**设备 (Device)** 下拉列表中，选择要在其上执行诊断命令的设备。

步骤 3 从**命令 (Command)** 列表中，选择要执行的命令。

步骤 4 在**参数 (Parameters)** 字段中输入命令参数。

有关有效参数，请参阅Cisco Secure Firewall Threat Defense 命令参考。

例如，要执行 **show access-list** 命令，请从**命令 (Command)** 下拉列表中选择 **show**，然后在**参数 (Parameters)** 字段中输入 **access-list** 。

注释 请勿在**参数 (Parameters)** 字段中键入完整命令。仅键入相关关键字。

步骤 5 点击**执行 (Execute)** 以查看命令输出。

如果显示消息无法正确执行命令。请查看日志以了解更多详细信息，请仔细检查参数。可能存在语法错误。

此消息还可能意味着您尝试执行的命令不是诊断CLI环境中的有效命令（您可以使用 **system support diagnostic-cli** 命令从设备访问）。使用 SSH 登录设备以使用这些命令。

功能特定的故障排除

有关功能特定的故障排除技巧和技术，请参阅下表。

表 *50*: 功能特定的故障排除主题

功能	相关故障排除信息
应用控制	在 《Cisco Secure Firewall Management Center 设备配置指南》中应用控制的最佳实践
LDAP 外部身份验证	LDAP 身份验证连接故障排除， 第 190 页
许可	智能许可疑难解答， 第 271 页 特定许可证预留疑难解答， 第 282 页
管理中心 高可用性	管理中心高可用性故障排除， 第 291 页
用户规则条件	在 《Cisco Secure Firewall Management Center 设备配置指南》中的用户控制故障排除
用户身份源	有关 ISE/ISE-PIC、TS 代理身份源、强制网络门户身份源和远程接入 VPN 身份源的故障排除信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的相应部分 LDAP 身份验证连接故障排除， 第 190 页
URL 筛选	在 《Cisco Secure Firewall Management Center 设备配置指南》中的*URL* 过滤故障排除

功能	相关故障排除信息
领域和用户数据下载	在 《Cisco Secure Firewall Management Center 设备配置指南》中的领域和用户下载故障排除
网络发现	在 《Cisco Secure Firewall Management Center 设备配置指南》中的对网络发现策略进行故障排除
自定义安全组标记 (SGT) 规则条件	中的自定义 SGT 规则条件 《Cisco Secure Firewall Management Center 设备配置指南》
SSL 规则	在 《Cisco Secure Firewall 设备管理器配置指南》中的 SSL 规则一章
思科 Threat Intelligence Director (TID)	在 《Cisco Secure Firewall Management Center 设备配置指南》中的故障排除 *Cisco Secure Firewall* 威胁智能导向器
Cisco Secure Firewall Threat Defense系统日志	在 《Cisco Secure Firewall Management Center 设备配置指南》中的关于配置系统日志
入侵性能统计数据	在 《Cisco Secure Firewall Management Center 设备配置指南》中的入侵性能统计信息日志记录配置
基于连接的故障排除	基于连接的故障排除， 第 423 页

第 IV 部分

工具

第 15 章

备份/恢复

关于备份和恢复

灾难恢复能力是任何系统维护计划的重要组成部分。作为灾难恢复计划的一部分，我们建议您定期备份到安全的远程位置。

按需备份

您可以从 管理中心 对 管理中心以及许多 威胁防御 设备执行按需备份。

有关详细信息，请参阅备份 管理中心FMC 或受管设备， 第 443 页。

计划的备份

您可以在 管理中心上使用调度程序来自动执行备份。您还可以从 管理中心 安排远程设备备份。

管理中心 设置过程安排每周仅配置备份，以存储在本地。 这不能替代完整的异地备份-在初始设置完成后，您应查看已安排的任务并进行调整，以满足组织的需求。

有关详细信息，请参阅计划的备份， 第 469 页。

存储备份文件

您可以在本地存储备份。但是，我们建议您通过将 NFS、SMB 或 SSHFS 网络卷安装为远程存储，将 管理中心和托管设备备份到安全的远程位置。执行此操作后，所有后续备份都将复制到该卷，但您仍可以使用 管理中心 对其进行管理。

有关详细信息，请参阅远程存储设备，第 92 页 和 管理备份和远程存储，第 462 页。

恢复 管理中心 和受管设备

您可以从备份管理页面恢复 管理中心 。 您必须使用 威胁防御 CLI 来恢复 威胁防御 设备，但 ISA 3000 零接触恢复除外，该恢复使用 SD 卡和重置按钮。

有关详细信息，请参阅恢复 管理中心 和托管设备，第 448 页。

备份的内容是什么？

管理中心 备份可以包括：

- (Recommended Configurations)。

  可以在 管理中心 Web 界面上设置的所有配置都包含在配置备份中，远程存储和审核日志服务器证书设置除外。在多域部署中，必须备份配置。不能仅备份事件或 TID 数据 。

- 事件。

  事件备份包括 管理中心 数据库中的所有事件。但是，管理中心 事件备份不包括入侵事件审核状态。已恢复的入侵事件不会显示在“已审核事件”页面上。

- 威胁智能导向器 (TID) 数据。

  关于更多信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 有关备份和恢复威胁智能导向器 数据 。

设备备份始终仅用于配置。

恢复的内容是什么？

恢复配置会覆盖 所有 备份配置，只有极少数例外。在 管理中心 上，恢复事件和 TID 数据会覆盖所有现有事件和 TID 数据，但入侵事件除外。

确保您了解并计划以下事项：

- 您无法恢复未备份的内容。

  管理中心 配置备份不包括远程存储和审核日志服务器证书设置，因此您必须在恢复后重新配置这些设置。此外，由于管理中心 事件备份不包括入侵事件审核状态，因此已恢复的入侵事件不会显示在“已审核事件”页面上。

- 恢复失败 VPN 证书。

  威胁防御 恢复过程会从 威胁防御 设备中删除 VPN 证书和所有 VPN 配置，包括在执行备份后添加的证书。恢复 威胁防御 设备后，必须重新添加/重新注册所有 VPN 证书，并重新部署设备。

- 恢复到已配置的 管理中心（而不是恢复出厂或重新映像）会合并入侵事件和文件列表。

  管理中心 事件恢复过程不会覆盖入侵事件。相反，备份中的入侵事件会添加到数据库中。要避免重复，请在恢复之前删除现有入侵事件。

管理中心 配置恢复过程不会覆盖 恶意软件防护 使用的干净和自定义检测文件列表。相反，它会将现有文件列表与备份中的文件列表合并。要替换文件列表，请在恢复之前删除现有文件列表。

备份和还原要求

Backup and Restore具有以下要求。

型号要求：备份

您可以备份：

- 管理中心。
- 硬件上运行的威胁防御，包括容器实例。
- 用于私有云的 Threat Defense Virtual，但集群设备和用于 KVM 的 threat defense virtual 除外。
- 用于私有云的 Threat Defense Virtual，但用于 KVM 的 threat defense virtual 除外。
- 用于 AWS 的 Threat Defense Virtual，但集群设备除外。不支持任何其他公共云部署的备份。
- 用于 AWS 的 Threat Defense Virtual，但集群设备除外。不支持任何其他公共云部署的备份。

如果需要更换不支持备份和恢复的设备，则必须手动重新创建设备特定的配置。但是，备份 管理中心 会备份部署到受管设备的策略和其他配置，以及已从设备传输到 管理中心的事件。

型号要求：恢复

替换受管设备必须与您要替换的设备具有相同的型号，具有相同数量的网络模块和相同类型和数量的物理接口。

对于 管理中心，不仅可以在 RMA 场景中使用Backup and Restore，还可以在 管理中心之间迁移配置和事件。关于详细信息，包括支持的目标和目的模型，请参阅 Cisco Secure Firewall Management Center 型号迁移指南。

版本要求

作为任何备份的第一步，请注意补丁级别。要恢复备份，旧设备和新设备必须运行相同的软件版本，包括补丁。要恢复 Firepower 4100/9300 机箱，您必须运行兼容的 FXOS。

对于 管理中心 备份，不需要具有相同的 VDB 或 SRU。但请注意，恢复备份会将现有 VDB 替换为备份文件中的 VDB。如果已恢复的 SRU 或 VDB 版本早于 思科支持和下载站点 上的可用版本，我们建议您安装较新的版本。

许可证要求

解决最佳实践和程序中所述的许可或孤立权利问题。如果您发现许可冲突，请联系 思科 TAC。

域要求

到：

- 备份或恢复 管理中心：仅限全局。
- 从 管理中心备份设备：仅全局。
- 恢复设备：无。在 CLI 本地恢复设备。

在多域部署中，不能仅备份事件/ TID 数据。您还必须备份配置。

备份和恢复的指南和限制

备份和恢复有以下指南和限制。

备份和恢复适用于灾难恢复/ RMA

备份和恢复主要用于 RMA 场景。在开始故障或发生故障的物理设备的恢复过程之前，请联系 思科 TAC 更换硬件。

您还可以使用Backup and Restore在 管理中心之间迁移配置和事件。这使得更换 管理中心（由于不断增长的组织、从物理实施迁移到虚拟实施、硬件更新等技术或业务等方面的原因）变得更容易。

备份和恢复不是配置导入/导出

备份文件包含唯一识别设备的信息，并且不能共享。不要使用备份和恢复过程在设备或装置之间复制配置，或作为测试新配置时保存配置的一种方式。相反，请使用导入/导出功能。

例如， 威胁防御 设备备份包括设备的管理IP地址以及设备连接到其管理 管理中心所需的所有信息。请勿将 威胁防御 备份恢复到由其他 管理中心管理的设备；恢复的设备将尝试连接到备份中指定的 管理中心 。

恢复为单个和本地恢复

您可以单独和本地恢复到 管理中心和受管设备。这意味着：

- 您无法批量恢复到高可用性 或集群的 管理中心或设备。
- 您无法使用 管理中心 恢复设备。对于 管理中心，可以使用 Web 接口进行恢复。 对于 威胁防御 设备，必须使用 威胁防御 CLI，但 ISA 3000 零接触恢复除外，该恢复使用 SD 卡和重置按钮。
- 您不能使用 管理中心 用户账号登录并从其受管设备之一恢复。管理中心 和设备会维护自己的用户账号。

Firepower 4100/9300 的配置导入/导出准则

使用配置导出功能将包含 Firepower 4100/9300 机箱的逻辑设备和平台配置设置的 XML 文件导出到远程服务器或本地计算机。之后，您便可以导入此配置文件，快速将配置设置应用于 Firepower 4100/9300 机箱，以返回到已知的正确配置，或从系统故障中恢复。

准则和限制

- 请勿修改配置文件的内容。如果配置文件被修改，使用该文件进行配置导入可能会失败。
- 特定应用的配置设置不包含在配置文件内。您必须使用应用提供的配置备份工具来管理特定应用的设置和配置。
- 将配置导入到 Firepower 4100/9300 机箱 时，Firepower 4100/9300 机箱 上的所有现有配置（包括任何逻辑设备）会被删除并完全替换为导入文件中包含的配置。
- 除了在 RMA 场景中，我们建议您只将配置文件导入当初从中导出该配置的同一个 Firepower 4100/9300 机箱。
- 进行导入的 Firepower 4100/9300 机箱 的平台软件版本应与执行导出时的版本相同。否则，导入操作将无法确保会成功。我们建议您在升级或降级 Firepower 4100/9300 机箱 时导出备份配置。
- 进行导入的 Firepower 4100/9300 机箱 必须在与执行导出时所用的相同插槽中安装相同的网络模块。
- 进行导入的 Firepower 4100/9300 机箱 必须为您正在导入的导出文件中定义的任意逻辑设备安装了正确的软件应用映像。
- 要避免覆盖现有的备份文件，请更改备份操作中的文件名或将现有文件复制到其他位置。

注释 您必须单独备份逻辑应用，因为 FXOS 导入/导出将仅备份 FXOS 配置。FXOS 配置导入将导致逻辑设备重新启动，并使用出厂默认配置重建设备。

备份和还原的最佳实践

备份和恢复具有以下最佳实践。

何时备份

我们建议在维护时段或其他使用率较低的时间进行备份。

当系统收集备份数据时，数据的关联性可能会暂时停顿（仅限管理中心），而且你可能无法改变与备份有关的配置。如果包含事件数据，则 eStreamer 等事件相关功能不可用。

您应在以下情况下进行备份：

- 常规 计划的或 按需备份。

作为灾难恢复计划的一部分，我们建议您定期执行备份。

管理中心 设置过程安排每周仅配置备份，以存储在本地。 这不能替代完整的异地备份-在初始设置完成后，您应查看已安排的任务并进行调整，以满足组织的需求。有关详细信息，请参阅计划的备份，第 469 页。

- 在 SLR 更改之后。

  对特定许可预留（SLR）进行更改后，备份 管理中心 。如果您进行更改并恢复较旧的备份，则您的特定许可返回代码会出现问题，并且可能会产生孤立授权。

- 在升级或重新映像之前。

  如果升级失败是灾难性的，您可能必须重新映像并恢复。重新映像会将大多数设置恢复为出厂默认设置，包括系统密码。如果您有最近的备份，可以更快地恢复正常操作。

- 升级后。

  在升级后进行备份，以便获得新升级的部署的快照。我们建议您在升级其托管设备后 备份管理中心 ，以便新的 管理中心 备份文件“知道”其设备已升级。

维护备份文件安全

备份存储为未加密的存档（.tar）文件。

PKI 对象中的私钥--代表支持你的部署所需的公钥证书和成对的私钥--在被备份之前被解密在恢复备份时，将使用随机生成的密钥重新加密密钥。

注释 我们建议您将 管理中心和设备备份到安全的远程位置并验证传输是否成功。本地删除的备份可以手动删除，也可以通过升级过程删除，从而清除本地存储的备份。

尤其是由于备份文件未加密的情况，因此不允许未经授权的访问。如果修改备份文件，恢复过程将失败。请记住，具有 管理员/维护角色 的任何人都可以访问“备份管理”页面，他们可以在其中移动和删除远程存储中的文件。

在 管理中心的系统配置中，您可以安装NFS、SMB或SSHFS网络卷作为远程存储。执行此操作后，所有后续备份都将复制到该卷，但您仍可以使用 管理中心对其进行管理。有关详细信息，请参阅远程存储设备，第 92 页 和 管理备份和远程存储，第 462 页。

请注意，只有 管理中心 安装网络卷。 受管设备备份文件通过 管理中心路由。确保你有足够的带宽在 管理中心 和其设备之间进行大量的数据传输。有关详细信息，请参阅将数据从 Firepower 管理中心下载到受管设备的准则（故障排除技术说明）。

管理中心 高可用性部署中的 Backup and Restore

在 管理中心 高可用性部署中，备份一个 管理中心 不会备份另一个。您应定期备份两个对等体。请勿使用来自另一个 HA 的备份文件恢复一个 HA 对等体。备份文件包含唯一识别设备的信息，并且不能共享。

请注意，您可以在没有成功备份的情况下替换 HA 管理中心 。有关更换 HA 管理中心（无论是否成功备份）的详细信息，请参阅 更换高可用性对中的 管理中心 ，第 302 页。

威胁防御 高可用性部署中的 Backup and Restore

在 威胁防御 高可用性部署中，您应该：

- 从 管理中心备份设备对，但从 威胁防御 CLI 单独和本地恢复。

  备份过程会为 威胁防御 高可用性设备生成唯一的备份文件。请勿使用来自另一个高可用性的备份文件恢复一个高可用性对等体。备份文件包含唯一识别设备的信息，并且不能共享。

  威胁防御 高可用性设备的角色记录在其备份文件名中。还原时，请确保选择适当的备份文件：主要与辅助。

- 在恢复之前， 请勿 暂停或中断高可用性。

  保持高可用性配置可确保替换设备在恢复后可以轻松重新连接。请注意，您必须恢复高可用性同步才能执行此操作。

- 请勿 同时在两个对等体上运行 **恢复** CLI 命令。

  假设您已成功备份，您可以替换高可用性对中的一个或两个对等体。您可以同时执行的任何物理更换任务：取消安装，重新安装等。 但是， 请勿 在第二台设备上运行 **恢复** 命令，直到第一台设备的恢复过程完成，包括重新启动。

请注意，您可以在没有成功备份的情况下更换 威胁防御 高可用性设备。

集群部署 威胁防御 中的备份和恢复

在 威胁防御 集群部署中，您应该：

- 从 管理中心备份完整集群，但从 威胁防御 CLI 单独和本地恢复节点。

  备份过程会生成一个捆绑的tar文件，其中包含每个集群节点的唯一备份文件。请勿使用另一个节点的备份文件恢复另一个节点。备份文件包含唯一识别设备的信息，并且不能共享。

  节点的角色记录在其备份文件名中。还原时，请确保选择适当的备份文件：控制或数据。

  您无法备份单个节点。如果数据节点无法备份，管理中心仍将备份所有其他节点。如果控制节点备份失败，则取消备份。

- 在恢复之前， 请勿 暂停或中断集群。

  保持集群配置可确保替换设备在恢复后可以轻松重新连接。

- 请勿 同时在多个节点上运行 **恢复** CLI 命令。我们建议您先恢复控制节点，等待其重新加入集群，然后再恢复任何数据节点。

  假设您有成功的备份，则可以替换集群中的多个节点。您可以同时执行的任何物理更换任务：取消安装，重新安装等。但是， 请勿 在其他节点上运行 **恢复** 命令，直到之前节点的恢复过程完成，包括重新启动。

Firepower 4100/9300 机箱的备份和恢复

要在 Firepower 4100/9300 机箱上恢复 威胁防御 软件，机箱必须运行兼容的 FXOS 版本。

当您备份 Firepower 4100/9300 机箱时，我们强烈建议您也备份 FXOS 配置。有关其他最佳实践，请参阅 Firepower 4100/9300 的配置导入/导出准则，第 439 页。

备份前

在备份之前，您应该：

- 更新 管理中心上的 VDB 和 SRU。

  我们始终建议您使用最新的漏洞数据库（VDB）和入侵规则（SRU）。在备份 管理中心之前，请检查 思科支持和下载站点 是否有较新版本。

- 检查磁盘空间。

  在开始备份之前，请确保设备或远程存储服务器上有足够的磁盘空间。可用空间显示在“备份管理”页面上。

  如果没有足够的空间，备份可能会失败。尤其是在安排备份时，请确保定期删除备份文件或为远程存储位置分配更多磁盘空间。

还原前

在恢复之前，您应：

- 恢复许可更改。

  请恢复自备份以来所做的任何许可更改。

  否则，恢复后您可能会遇到许可证冲突 或孤立的权利问题 。 但是， 请勿 从 Cisco 智能软件管理器（CSSM）注销。如果从 CSSM 注销，则必须在恢复后再次注销，然后重新注册。

  恢复完成后，重新配置许可。如果您发现许可冲突 或孤立的权利，请联系 思科 TAC 。

- 断开故障设备。

  断开管理接口，对于设备，断开数据接口。

  恢复 威胁防御 设备会将替换设备的管理 IP 地址设置为旧设备的管理 IP 地址。为避免 IP 冲突，请先断开旧设备与管理网络的连接，然后再更换备份。

  请注意，恢复 管理中心 不 会更改管理 IP 地址。您必须在更换时手动设置该设置-只需确保先断开旧设备与网络的连接，然后再执行此操作。

- 请勿 取消注册受管设备。

  无论您是恢复 管理中心 或托管设备，都不要从 管理中心注销设备，即使您从网络上物理断开设备。

  如果取消注册，则需要重做一些设备配置，例如安全区域到接口的映射。恢复后，管理中心和设备应开始正常通信。

- 重新映像。

在 RMA 场景中，替换设备将配置为出厂默认设置。但是，如果已配置替换设备，我们建议您重新映像。重新映像会将大多数设置恢复为出厂默认设置，包括系统密码。您只能重新映像到主要版本，因此您可能需要在重新映像后进行修补。

如果不重新映像，请记住， 管理中心 入侵事件和文件列表会合并而不是覆盖。

还原后

还原后，您应：

- 重新配置未恢复的任何内容。

  这可能包括重新配置许可，远程存储和审核日志服务器证书设置。 您还必须重新添加/重新注册失败的 威胁防御 VPN 证书。

- 更新 管理中心上的 VDB 和 SRU。

  我们始终建议您使用最新的漏洞数据库（VDB）和入侵规则（SRU）。 这对于VDB 尤其重要，因为备份中的 VDB 将覆盖替换 管理中心上的 VDB。

- 部署。

  恢复管理中心后，部署到所有托管设备。恢复设备后，必须从“设备管理”页面强制部署：请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 将现有配置重新部署到设备 。无论是恢复 管理中心 还是 必须 部署的设备。

备份 管理中心FMC 或受管设备

您可以对支持的设备执行按需或计划备份。

从 管理中心备份 设备不需要备份配置文件。但是， 管理中心 会备份需要备份配置文件。按需备份过程允许您创建新的备份配置文件。

备份 管理中心

使用此程序执行按需 管理中心 备份。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 437 页
- 备份和恢复的指南和限制， 第 438 页
- 备份和还原的最佳实践， 第 439 页

过程

步骤 1 选择**系统**（⚙）> **工具** > **备份/恢复**。

“备份管理”页面列出所有本地和远程存储的备份。它还列出了可用于存储备份的磁盘空间。如果没有足够的空间，备份可能会失败。

步骤 2 选择是使用现有备份配置文件还是全新启动。

管理中心 备份要求您使用或创建备份配置文件。

- 点击 **备份配置文件** 以使用现有备份配置文件。

  在要使用的配置文件旁边，点击编辑图标。然后，您可以点击 **开始备份** 立即开始备份。或者，如果要编辑配置文件，请继续执行下一步。

- 点击 **Firepower 管理备份** 以开始全新的备份并创建新的备份配置文件。

  输入配置文件的 **名称** 。

步骤 3 选择要备份的内容：

- **备份配置**。在管理中心的高可用性中，如果您选择仅在主用管理中心上备份配置，则默认情况下，主用 [] 和备用 管理中心都备份到单个统一备份文件中。有关高可用性中 管理中心 的统一备份的信息，请参阅 高可用性管理中心的统一备份，第 307 页。
- **备份事件**
- **备份威胁情报导向器**

在多域部署中，必须备份配置。不能仅备份事件或 TID 数据 。有关为每个选项备份的内容的详细信息，请参阅 关于备份和恢复，第 435 页。

步骤 4 请注意 管理中心 备份文件的 **存储位置** 。

这将是 `/var/sf/backup/`中的本地存储或远程网络卷。有关详细信息，请参阅管理备份和远程存储，第 462 页。

步骤 5 （可选）启用 **完成时复制** 以将已完成的 管理中心 备份复制到远程服务器。

提供主机名或 IP 地址，远程目录的路径以及用户名和密码。要使用 SSH 公共密钥而不是密码，则将 **SSH 公共密钥** 字段中的内容到该机器上指定用户的 `授权的_密钥` 文件中。

注释 如果要在本地存储备份并将其存储到远程位置，此选项非常有用。如果配置了 SSH 远程存储，请 不 要在完成后使用 **复制将备份文件复制到同一目录**。

步骤 6 （可选）启用 **邮件** 并输入在备份完成时收到通知的邮件地址。

要接收邮件通知，必须将 管理中心 配置为连接到邮件服务器： 配置邮件中继主机和通知地址，第 58 页。

步骤 7 点击 **开始备份** 开始按需备份。

如果您不使用现有备份配置文件，则系统会自动创建并使用该配置文件。如果决定不立即运行备份，可以点击 **保存** 或 **另存为** 保存配置文件。无论是哪种情况，都可以使用新创建的配置文件来配置计划备份。

步骤 8 在消息中心监控进度。

当系统收集备份数据时，数据的关联性可能会暂时停顿，而且你可能无法改变与备份有关的配置。如果配置了远程存储或启用 **完成时复制**，则 管理中心 可能会将临时文件写入远程服务器。这些文件在备份过程结束时进行清理。

下一步做什么

如果配置了远程存储或启用 **完成时复制**，请验证备份文件的传输是否成功。

从 管理中心备份设备

使用此程序对以下任何设备执行按需备份：

- 威胁防御：物理设备、独立、高可用性、集群
- threat defense virtual：私有云、独立、高可用性、集群

备份和恢复不支持任何其他平台或配置。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 437 页
- 备份和恢复的指南和限制， 第 438 页
- 备份和还原的最佳实践， 第 439 页

如果您要备份 Firepower 4100/9300 机箱，则还必须备份 FXOS 配置： 导出 FXOS 配置文件， 第 446 页

过程

步骤 1 选择 **系统**（⚙） > **工具** > **备份/恢复**，然后点击 **受管设备备份**。

步骤 2 选择一个或多个 **受管设备**。

对于集群，请选择集群。不能在单个节点上执行备份。

步骤 3 请注意设备备份文件的 **存储位置** 。

这将是 /var/sf/remote-backup/中的本地存储或远程网络卷。对于 ISA 3000，如果您安装了 SD 卡，也会在 /mnt/disk3/backup的 SD 卡上创建备份副本。有关详细信息，请参阅管理备份和远程存储，第 462 页。

步骤 4 如果未配置远程存储，请选择是否要 **检索到管理中心**。

- 已启用（默认）：将备份保存到 /var/sf/remote-backup/ 中的 管理中心。

  对于集群，此选项始终处于选中状态。单个节点备份文件将复制到管理中心，然后捆绑为单个压缩 tar 文件，然后再复制到任何远程存储。

- 已禁用：将备份保存到 /var/sf/backup 中的设备。

步骤 5 点击 **开始备份** 开始按需备份。

步骤 6 在消息中心监控进度。

下一步做什么

如果配置了远程存储，请验证备份文件的传输是否成功。

导出 FXOS 配置文件

使用配置导出功能将包含 Firepower 4100/9300 机箱逻辑设备和平台配置设置的 XML 文件导出到远程服务器或本地计算机。

注释 此程序介绍在备份 威胁防御时如何使用 Cisco Secure Firewall 机箱管理器 来导出 FXOS 配置。有关 CLI 程序，请参阅相应版本的《思科 Firepower 4100/9300 FXOS CLI 配置指南》。

开始之前

查看 Firepower 4100/9300 的配置导入/导出准则。

过程

步骤 1 在 Cisco Secure Firewall 机箱管理器 上依次选择**系统 (System)** > **配置 (Configuration)** > **导出 (Export)**。

步骤 2 要将配置文件导出到本地计算机：

a) 点击**本地 (Local)**。

b) 点击**导出 (Export)**。
配置文件已创建，然后根据您的浏览器，该文件可能会自动下载到默认下载位置，或者系统会提示您保存文件。

步骤 3 要将配置文件导出到远程服务器：

a) 点击**远程 (Remote)**。

b) 选择与远程服务器通信时要使用的协议。它可以是以下协议之一：FTP、TFTP、SCP 或 SFTP。
c) 输入备份文件应存储位置的主机名或 IP 地址。这可以是 Firepower 4100/9300 机箱可通过网络访问的服务器、存储阵列、本地驱动器或任何读/写介质。

   如果使用主机名而不使用 IP 地址，则必须配置 DNS 服务器。

d) 如果您使用非默认端口，请在**端口 (Port)** 字段中输入端口号。
e) 输入系统在登录远程服务器时应使用的用户名。如果协议是 TFTP，将无法应用该字段。
f) 输入远程服务器用户名的密码。如果协议是 TFTP，将无法应用该字段。

   注释 密码不得超过 64 个字符。如果输入的密码超过 64 个字符， 机箱管理器 将显示错误，指出 `org-root/cfg-exp-policy-default 的属性 pwd 超出范围。`

g) 在**位置 (Location)** 字段中，输入配置文件导出位置的完整路径，包括文件名。
h) 点击的**导出 (Export)** 按钮。
   配置文件已创建，并已被导出到指定位置。

创建备份配置文件

备份配置文件是一组已保存的首选项-要备份的内容，备份文件的存储位置等。

FMC 备份 需要备份配置文件。从 FMC 备份设备不需要备份配置文件。

当您执行按需FMC备份时，如果不选择现有备份配置文件，系统会自动创建一个并使用它。然后，您可以使用新创建的配置文件配置计划备份。

以下程序介绍如何在不执行按需备份的情况下创建备份配置文件。

过程

步骤 1 选择 **系统**（⚙） > **工具** > **备份/恢复**，然后点击 **备份配置文件**。
步骤 2 点击 **创建配置文件** 并输入 **名称**。
步骤 3 选择要备份的内容。

- **备份配置**
- **备份事件**
- **备份威胁情报导向器**

在多域部署中，必须备份配置。不能仅备份事件或 TID 数据 。有关为每个选项备份的内容的详细信息，请参阅 关于备份和恢复 ， 第 435 页。

步骤 4 请注意备份文件的 **存储位置** 。

这将是 /var/sf/backup/中的本地存储或远程网络卷。对于 ISA 3000，如果您安装了 SD 卡，也会在 /mnt/disk3/backup的 SD 卡上创建备份副本。有关详细信息，请参阅管理备份和远程存储，第 462 页。

步骤 5 （可选） **启用完成时复制** 以将已完成的 FMC 备份复制到远程服务器。

提供主机名或 IP 地址，远程目录的路径以及用户名和密码。要使用 SSH 公共密钥而不是密码，则将 **SSH 公共密钥** 字段中的内容到该机器上指定用户的 授权的_密钥 文件中。

注释 如果要在本地存储备份并将其存储到远程位置，此选项非常有用。如果配置了 SSHFS 远程存储，请 勿 在完成后使用 **复制将备份文件复制到同一目录**。

步骤 6 （可选）启用 **邮件** 并输入在备份完成时收到通知的邮件地址。

要接收邮件通知，必须将 FMC 配置为连接到邮件服务器： 配置邮件中继主机和通知地址，第 58 页。

步骤 7 点击**保存 (Save)**。

恢复 管理中心 和托管设备

对于 管理中心，可使用 Web 接口从备份恢复。 对于 威胁防御 设备，必须使用 威胁防御 CLI。您无法使用 管理中心 恢复设备。

以下各节介绍如何恢复 管理中心 和托管设备。

从备份恢复 管理中心

当恢复 管理中心 备份时，可以选择恢复备份文件中包含的任何或所有组件（事件、配置、TID 数据）。

注释 恢复配置会覆盖 所有 配置，只有极少数例外。它还会重新启动 管理中心。恢复事件 和 TID 数据 会覆盖 所有 现有事件 和 TID 数据，但入侵事件除外。确保您已准备就绪。

使用此程序从备份恢复 管理中心 。 有关 管理中心 HA 部署中的备份和恢复的详细信息，请参阅 更换高可用性对中的 管理中心，第 302 页。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求，第 437 页
- 备份和恢复的指南和限制，第 438 页

- 备份和还原的最佳实践， 第 439 页

过程

步骤 1 登录到要恢复的 管理中心 。

步骤 2 选择**系统**（⚙）> **工具** > **备份/恢复**。

“备份管理”页面列出所有本地和远程存储的备份文件。您可以点击备份文件以查看其内容。

如果备份文件不在列表中，并且您已将其保存在本地计算机上，请点击**上传备份**；请参阅管理备份和远程存储， 第 462 页。

步骤 3 选择要恢复的备份文件并点击 **恢复**。

步骤 4 从可用组件中选择要恢复的组件，然后再次点击 **恢复** 以开始。

步骤 5 在消息中心监控进度。

如果要恢复配置，可以在 管理中心 重启后重新登录。

下一步做什么

- 如有必要，请重新配置在还原之前恢复的任何许可设置。如果您发现许可冲突 或孤立的权利，请联系 思科 TAC 。
- 如有必要，请重新配置远程存储和审核日志服务器证书设置。这些设置不包括在备份中。
- （可选）更新 SRU 和 VDB。如果已恢复的 SRU 或 VDB 版本早于 思科支持和下载站点 上的可用版本，我们建议您安装较新的版本。
- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

从备份恢复威胁防御： Firepower1000/2100,CiscoSecureFirewall3100/4200, ISA 3000 (非零触摸)

设备备份和恢复适用于 RMA。恢复配置会覆盖设备上的 所有 配置，包括管理 IP 地址。也重启设备。

如果发生硬件故障，此程序概述了如何更换 Firepower 1000/2100、Secure Firewall 3100/4200 或 ISA 3000 威胁防御 设备、独立或高可用性对或作为集群。它假定您有权访问要替换的设备的成功备份；请参阅 从 管理中心备份设备， 第 445 页。有关使用 SD 卡在 ISA 3000 上进行零接触恢复的信息，请参阅 从备份的零接触恢复 威胁防御： ISA 3000， 第 452 页。

对于高可用性和集群 设备，您可以使用此程序替换所有对等体。要同时替换所有，请同时在所有设备上执行所有步骤，但 **恢复** CLI 命令本身除外。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。对于 威胁防御 高可用性和集群设备，请不要暂停或中断高可用性或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 437 页
- 备份和恢复的指南和限制， 第 438 页
- 备份和还原的最佳实践， 第 439 页

过程

步骤 1 联系 思科 TAC 更换硬件。

获取相同的型号，具有相同数量的网络模块和相同类型和数量的物理接口。您可以从 思科退货门户 开始 RMA 进程。

步骤 2 找到故障设备的成功备份。

根据备份配置，可以存储设备备份：

- 在故障设备本身的 `/var/sf/backup` 中。
- 在 管理中心 中的 `/var/sf/remote-backup`。
- 在远程存储位置。

对于 威胁防御 高可用性和集群 设备，您可以将组作为一个单元进行备份。对于高可用性设备，备份过程会生成唯一的备份文件，并在备份文件名称中标明每个设备的角色。 对于群集，控制节点和数据节点备份文件捆绑在一个压缩文件中。您必须提取文件，这些文件也会显示设备角色。

如果备份的唯一副本位于故障设备上，请立即将其复制到其他位置。如果重新映像设备，备份将被清除。如果出现其他问题，您可能无法恢复备份。有关详细信息，请参阅管理备份和远程存储， 第 462 页。

替换设备需要备份，但可以在恢复过程中使用 SCP 进行检索。我们建议您将备用设备放在 SCP 可访问的位置，以供替换设备使用。或者，您可以将备份复制到替换设备本身。

步骤 3 移除（拆开）故障设备。

断开所有接口。在 威胁防御 高可用性部署中，这包括故障切换链路。 对于集群，这包括集群控制链路。

请参阅您的型号的硬件安装和入门指南： http://www.cisco.com/go/ftd-quick。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。对于 威胁防御 高可用性和集群 设备，请不要暂停或中断高可用性或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

步骤 4 安装替换设备并将其连接到管理网络。

将设备连接至电源并将管理接口连接至管理网络。在 威胁防御 高可用性部署中，连接故障切换链路。 对于集群，请连接集群控制链路。但是， 请勿 连接数据接口。

请参阅您的型号的硬件安装指南： http://www.cisco.com/go/ftd-quick。

步骤 5 （可选）重新映像替换 设备。

在 RMA 场景中，替换设备将配置为出厂默认设置。如果替换设备运行的主版本与故障设备不同，我们建议您重新映像。

请参阅 Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南。

步骤 6 在替换设备上执行初始配置。

以 `admin` 用户身份访问 威胁防御 CLI。安装向导会提示您配置管理 IP 地址，网关和其他基本网络设置。

请勿设置与故障设备相同的管理 IP 地址。如果您需要注册设备以进行修补，这可能会导致问题。恢复过程将正确重置管理 IP 地址。

请参阅您的型号的入门指南中的初始配置主题： http://www.cisco.com/go/ftd-quick。

注释 如果需要修补替换设备，请按照入门指南中的说明启动 管理中心 注册过程。如果不需要修补， 请勿 注册。

步骤 7 确保替换设备运行与故障设备相同的软件版本， 包括补丁。

确保不应从管理中心中删除现有设备。替换设备应不受物理网络的管理，新硬件以及替换的威胁防御 补丁应具有相同的版本。 威胁防御 CLI 没有升级命令。要修补，请执行以下操作：

a) 从 管理中心 Web 界面，完成设备注册过程。

创建新的AC策略并使用默认操作“网络发现”。保持此策略不变；请勿添加任何功能或修改。这用于注册设备和部署无功能的策略，以便您不需要许可证，然后便可以修补设备。备份恢复后，应将许可和策略恢复到预期状态。

b) 修补设备：https://www.cisco.com/go/ftd-upgrade。

c) 从 管理中心。

如果不注销，则在恢复过程将“旧”设备恢复后，您将有一个 Ghost 设备注册到 管理中心 。

步骤 8 确保替换设备有权访问备份文件。

恢复过程可以使用 SCP 检索备份，因此我们建议您将备份放在可访问的位置。或者，您可以手动将备份复制到替换设备本身，复制到 `/var/sf/backup`。 对于群集设备，从备份捆绑包中提取相应的备份文件。

步骤 9 从 威胁防御 CLI 恢复备份。

以 admin 用户身份访问 威胁防御 CLI。您可以使用控制台，也可以通过 SSH 连接到新配置的管理接口（IP 地址或主机名）。请记住，恢复过程将更改此 IP 地址。

要恢复，请执行以下操作：

- 使用 SCP： **restore remote-manager-backup location** *scp-主机名称 用户名 文件路径 备份 tar-文件*
- 从本地设备： **restore remote-manager-backup** 备份 *tar-文件*

在 威胁防御 高可用性 和集群 部署中，请确保选择适当的备份文件：主要与辅助，或控制与数据。该角色在备份文件名中注明。如果要恢复所有设备，请依次执行此操作。在第一台设备的恢复过程完成（包括重新启动）之前，请勿在下一台设备上运行 **恢复** 命令。

步骤 10 登录 管理中心 并等待替换设备连接。

还原完成后，设备会退出 CLI，重新启动并自动连接到 管理中心。此时，设备应显示为过时。

步骤 11 在部署之前，请执行任何恢复后任务并解决任何恢复后问题：

- 解决许可冲突或孤立授权问题。联系思科 TAC。
- 恢复高可用性同步。从 威胁防御 CLI， 输入 配置高可用性恢复。 请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的暂停和恢复高可用性。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 威胁防御 设备中删除 VPN 证书，包括在执行备份后添加的证书。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 管理 *VPN* 证书 。

步骤 12 部署配置。

您 必须 部署。恢复设备后，必须从“设备管理”页面强制部署。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 将现有配置重新部署到设备 。

步骤 13 连接设备的数据接口。

请参阅您的型号的硬件安装指南： http://www.cisco.com/go/ftd-quick。

下一步做什么

验证恢复是否成功以及替换设备是否按预期传递流量。

从备份的零接触恢复 威胁防御： ISA 3000

设备备份和恢复适用于 RMA。恢复配置会覆盖设备上的 所有 配置，包括管理 IP 地址。也重启设备。

万一发生硬件故障，此程序概述了如何更换 ISA 3000 威胁防御 设备（独立或 HA 对）。它假设您在 SD 卡上备份了发生故障的设备；请参阅 从 管理中心备份设备 ， 第 445 页。

对于高可用性和集群 设备，您可以使用此程序替换所有对等体。要同时替换所有，请同时在所有设备上执行所有步骤，但 **恢复** CLI 命令本身除外。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。对于 威胁防御 高可用性和集群设备，请不要暂停或中断高可用性或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 437 页
- 备份和恢复的指南和限制， 第 438 页
- 备份和还原的最佳实践， 第 439 页

过程

步骤 1 联系 思科 TAC 更换硬件。

获取相同的型号，具有相同数量的网络模块和相同类型和数量的物理接口。您可以从 思科退货门户 开始 RMA 进程。

步骤 2 从故障设备中取出 SD 卡，然后拆开设备。

断开所有接口。在 威胁防御 HA 部署中，这包括故障切换链路。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。对于 威胁防御 高可用性和集群 设备，请不要暂停或中断高可用性或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

步骤 3 重新安装替换设备，并将其连接到管理网络。在 威胁防御 HA 部署中，连接故障切换链路。但是，请勿 连接数据接口。

如果需要重新映像设备或应用软件补丁，请连接电源接头。

步骤 4 （可能需要）重新映像更换设备。

在RMA场景中，替换设备将配置为出厂默认设置。如果替换设备未运行与故障设备相同的主版本，则需要重新映像。从 https://www.cisco.com/go/isa3000-software 获取安装程序。

请参阅 Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南 以重新映像。

步骤 5 （可能需要）确保替换设备运行与故障设备相同的 Firepower 软件版本， 包括相同的补丁版本。如果需要修补设备，可以连接到 Secure Firewall 设备管理器 （设备管理器）以安装补丁。

以下程序假设您具有出厂默认配置。如果已配置设备，则可以登录 设备管理器 并直接转到 **设备** > **升级** 页面以安装补丁。

无论是哪种情况，都应从 https://www.cisco.com/go/isa3000-software获取补丁包。

a) 将您的计算机直接连接到内部（以太网 1/2）接口，并通过默认 IP 地址访问 设备管理器：**https://192.168.95.1**。
b) 输入 **admin** 用户名和默认密码 **Admin123**，然后点击 **登录**。
c) 完成设置向导。请记住，您不会保留在 设备管理器 中配置的任何内容；您只需跳过任何初始配置，即可应用补丁，因此在设置向导中输入的内容并不重要。
d) 转到 **设备** > **升级** 页面。

   系统升级 部分将显示当前运行的软件版本。

e) 点击 **浏览**上传上传补丁文件。
f) 点击**安装**开始安装过程。

   图标旁的信息表示设备是否会在安装期间重新启动。您将从系统中自动注销。安装可能需要 30 分钟或更长时间。

   请耐心等候，然后重新登录系统。“设备摘要”（或“系统监控”控制面板）应该显示新版本。

   注释 不要只刷新浏览器窗口，而要从 URL 中删除所有路径，然后重新连接到主页。这可确保使用最新代码刷新缓存的信息。

步骤 6 将 SD 卡插入替换设备。

步骤 7 启动或重新启动设备，并在设备启动后不久，按住“重置”按钮不小于 3 秒且不超过 15 秒。

如果您使用 设备管理器 安装过补丁，则可以从 **设备** > **系统设置** > **重启/关机** 页面重启。从 威胁防御 CLI 中，使用 **reboot** 命令。如果尚未连接电源，请立即连接。

使用线规为 0.033 英寸或更小的标准 #1 回形针按下“重置”按钮。恢复过程在启动期间触发。设备将恢复配置，然后重新启动。然后，设备将自动向 管理中心 注册。

如果要恢复高可用性对中的两台设备，请依次执行此操作。在第一台设备的恢复过程完成（包括重新启动）之前，请勿恢复第二台设备。

步骤 8 登录 管理中心 并等待替换设备连接。

此时，设备应显示为过时。

步骤 9 在部署之前，请执行任何恢复后任务并解决任何恢复后问题：

- 解决许可冲突或孤立授权问题。联系思科 TAC。
- 恢复高可用性同步。从 威胁防御 CLI， 输入 `configure high-availability resume`。 请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的暂停和恢复高可用性。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 威胁防御 设备中删除 VPN 证书，包括在执行备份后添加的证书。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的管理 *VPN* 证书 。

步骤 10 部署配置。

您 必须 部署。恢复设备后，必须从“设备管理”页面强制部署。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 将现有配置重新部署到设备 。

步骤 11 连接设备的数据接口。

请参阅您的型号的硬件安装指南： http://www.cisco.com/go/ftd-quick。

下一步做什么

验证恢复是否成功以及替换设备是否按预期传递流量。

从备份恢复 威胁防御： Firepower 4100/9300 机箱

设备备份和恢复适用于 RMA。恢复配置会覆盖设备上的 所有 配置，包括管理 IP 地址。也重启设备。

在发生硬件故障的情况下，此程序概述了如何替换 Firepower 4100/9300、独立、高可用性对 或作为集群。它假设您有权访问以下项的成功备份：

- 要替换的逻辑设备；请参阅 从 管理中心备份设备 ， 第 445 页。
- FXOS 配置，请参阅 导出 FXOS 配置文件 ， 第 446 页。

对于高可用性和集群 设备，您可以使用此程序替换所有对等体。要同时替换所有，请同时在所有设备上执行所有步骤，但 **恢复** CLI 命令本身除外。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。对于 威胁防御 高可用性和集群设备，请不要暂停或中断高可用性或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求 ， 第 437 页
- 备份和恢复的指南和限制 ， 第 438 页
- 备份和还原的最佳实践 ， 第 439 页

过程

步骤 1 联系 思科 TAC 更换硬件。

获取相同的型号，具有相同数量的网络模块和相同类型和数量的物理接口。您可以从 思科退货门户 开始 RMA 进程。

步骤 2 找到故障设备的成功备份。

根据备份配置，可以存储设备备份：

- 在故障设备本身的 `/var/sf/backup` 中。
- 在 管理中心 中的 `/var/sf/remote-backup`。
- 在远程存储位置。

对于 威胁防御 高可用性和集群 设备，您可以将组作为一个单元进行备份。对于高可用性设备，备份过程会生成唯一的备份文件，并在备份文件名称中标明每个设备的角色。 对于群集，控制节点和数据节点备份文件捆绑在一个压缩文件中。您必须提取文件，这些文件也会显示设备角色。

如果备份的唯一副本位于故障设备上，请立即将其复制到其他位置。如果重新映像设备，备份将被清除。如果出现其他问题，您可能无法恢复备份。有关详细信息，请参阅管理备份和远程存储，第 462 页。

替换设备需要备份，但可以在恢复过程中使用 SCP 进行检索。我们建议您将备用设备放在 SCP 可访问的位置，以供替换设备使用。或者，您可以将备份复制到替换设备本身。

步骤 3 找到 FXOS 配置的成功备份。

步骤 4 移除（拆开）故障设备。

断开所有接口。在 威胁防御 高可用性部署中，这包括故障切换链路。 对于集群，这包括集群控制链路。

请参阅您的型号的硬件安装和入门指南： http://www.cisco.com/go/ftd-quick。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。对于 威胁防御 高可用性和集群 设备，请不要暂停或中断高可用性或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

步骤 5 安装替换设备并将其连接到管理网络。

将设备连接至电源并将管理接口连接至管理网络。在 威胁防御 高可用性部署中，连接故障切换链路。 对于集群，请连接集群控制链路。但是， 请勿 连接数据接口。

请参阅您的型号的硬件安装指南： http://www.cisco.com/go/ftd-quick。

步骤 6 （可选）重新映像替换 设备。

在 RMA 场景中，替换设备将配置为出厂默认设置。如果替换设备运行的主版本与故障设备不同，我们建议您重新映像。

请参阅相应的 《Cisco Firepower 4100/9300 FXOS Firepower 机箱管理器配置指南》中有关恢复出厂默认配置的说明。

步骤 7 确保 FXOS 运行的是兼容版本。

在重新添加逻辑设备之前，您必须运行兼容的FXOS版本。您可以使用 机箱管理器 导入备份的FXOS配置： 导入配置文件 ， 第 458 页。

步骤 8 使用 机箱管理器 添加逻辑设备并执行初始配置。

请勿设置与故障机箱上的逻辑设备相同的管理IP地址。如果您需要注册逻辑设备以进行修补，这可能会导致问题。恢复过程将正确重置管理 IP 地址。

请参阅 管理中心 适用于您的型号的入门指南中的FMC 部署章节： http://www.cisco.com/go/ftd-quick。

注释 如果需要修补逻辑设备，请按照入门指南中的说明注册到 管理中心 。如果不需要修补， 请勿 注册。

步骤 9 确保替换设备运行与故障设备相同的软件版本， 包括补丁。

确保不应从管理中心中删除现有设备。替换设备应不受物理网络的管理，新硬件以及替换的 威胁防御 补丁应具有相同的版本。 威胁防御 CLI 没有升级命令。要修补，请执行以下操作：

a) 从 管理中心 Web 界面，完成设备注册过程。

创建新的AC策略并使用默认操作“网络发现”。保持此策略不变；请勿添加任何功能或修改。这用于注册设备和部署无功能的策略，以便您不需要许可证，然后便可以修补设备。备份恢复后，应将许可和策略恢复到预期状态。

b) 修补设备：https://www.cisco.com/go/ftd-upgrade。

c) 从 管理中心。

如果不注销，则在恢复过程将“旧”设备恢复后，您将有一个 Ghost 设备注册到 管理中心 。

步骤 10 确保替换设备有权访问备份文件。

恢复过程可以使用 SCP 检索备份，因此我们建议您将备份放在可访问的位置。或者，您可以手动将备份复制到替换设备本身，复制到 `/var/sf/backup`。 对于群集设备，从备份捆绑包中提取相应的备份文件。

步骤 11 从 威胁防御 CLI 恢复备份。

以 `admin` 用户身份访问 威胁防御 CLI。您可以使用控制台，也可以通过 SSH 连接到新配置的管理接口（IP 地址或主机名）。请记住，恢复过程将更改此 IP 地址。

要恢复，请执行以下操作：

- 使用 SCP： **restore remote-manager-backup location** *scp-主机名称 用户名 文件路径 备份 tar-文件*
- 从本地设备： **restore remote-manager-backup** 备份 *tar-文件*

在 威胁防御 高可用性 和集群 部署中，请确保选择适当的备份文件：主要与辅助，或控制与数据。该角色在备份文件名中注明。如果要恢复所有设备，请依次执行此操作。在第一台设备的恢复过程完成（包括重新启动）之前，请勿在下一台设备上运行 **恢复** 命令。

步骤 12 登录 管理中心 并等待替换设备连接。

还原完成后，设备会退出 CLI，重新启动并自动连接到 管理中心。此时，设备应显示为过时。

步骤 13 在部署之前，请执行任何恢复后任务并解决任何恢复后问题：

- 解决许可冲突或孤立授权问题。联系思科 TAC。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 威胁防御 设备中删除 VPN 证书，包括在执行备份后添加的证书。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 管理 *VPN* 证书 。

步骤 14 部署配置。

您 必须 部署。恢复设备后，必须从“设备管理”页面强制部署。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 将现有配置重新部署到设备 。

步骤 15 连接设备的数据接口。

请参阅您的型号的硬件安装指南： http://www.cisco.com/go/ftd-quick。

下一步做什么

验证恢复是否成功以及替换设备是否按预期传递流量。

导入配置文件

您可以使用配置导入功能应用之前已从 Firepower 4100/9300 机箱导出的配置设置。此功能允许您返回已知的良好配置或从系统故障中进行恢复。

注释 此程序介绍如何在恢复 Firepower 软件之前使用 机箱管理器 来导入 FXOS 配置。有关 CLI 程序，请参阅相应版本的《思科 Firepower 4100/9300 FXOS CLI 配置指南》。

开始之前

查看 Firepower 4100/9300 的配置导入/导出准则。

过程

步骤 1 在 机箱管理器上选择 **系统 (System)** > **工具 (Tools)** > **导入/导出 (Import/Export)**。

步骤 2 要从本地配置文件导入：

a) 点击**本地 (Local)**。
b) 点击**选择文件 (Choose File)** 以导航到要导入的配置文件并将其选定。
c) 点击**导入 (Import)**。
系统将打开确认对话框，请求您确认是否要继续，并警告您可能需要重新启动机箱。
d) 点击**是 (Yes)** 以确认要导入指定的配置文件。
现有配置被删除，导入文件中指定的配置应用到 Firepower 4100/9300 机箱。在导入过程中，如果有分支端口配置更改，Firepower 4100/9300 机箱将需要重新启动。

步骤 3 要从远程服务器上的配置文件导入：

a) 点击**远程 (Remote)**。
b) 选择与远程服务器通信时要使用的协议。它可以是以下协议之一：FTP、TFTP、SCP 或 SFTP。
c) 如果您使用非默认端口，请在**端口 (Port)** 字段中输入端口号。
d) 输入备份文件存储位置的主机名或 IP 地址。这可以是 Firepower 4100/9300 机箱可通过网络访问的服务器、存储阵列、本地驱动器或任何读/写介质。

如果使用主机名而不使用 IP 地址，则必须配置 DNS 服务器。

e) 输入系统在登录远程服务器时应使用的用户名。如果协议是 TFTP，将无法应用该字段。
f) 输入远程服务器用户名的密码。如果协议是 TFTP，将无法应用该字段。

注释 密码不得超过 64 个字符。如果输入的密码超过 64 个字符， 机箱管理器 将显示错误，指出 `org-root/cfg-exp-policy-default 的属性 pwd 超出范围`。

g) 在**文件路径 (File Path)** 字段中，输入配置文件的完整路径，包括文件名。
h) 点击的**导入 (Import)** 按钮。
系统将打开确认对话框，请求您确认是否要继续，并警告您可能需要重新启动机箱。
i) 点击**是 (Yes)** 以确认要导入指定的配置文件。
现有配置被删除，导入文件中指定的配置应用到 Firepower 4100/9300 机箱。在导入过程中，如果有分支端口配置更改，Firepower 4100/9300 机箱将需要重新启动。

从备份恢复 Threat Defense Virtual

使用此程序可更换故障或发生故障的 threat defense virtual 设备。

对于高可用性和集群 设备，您可以使用此程序替换所有对等体。要同时替换所有，请同时在所有设备上执行所有步骤，但 **恢复** CLI 命令本身除外。

注释 请勿 从 管理中心注销，即使在断开设备与网络的连接时也是如此。对于 威胁防御 高可用性和集群设备，请不要暂停或中断高可用性或集群 。维护这些链路可确保替换设备在恢复后可以自动重新连接。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。 您不想跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 437 页
- 备份和恢复的指南和限制， 第 438 页
- 备份和还原的最佳实践， 第 439 页

过程

步骤 1 找到故障设备的成功备份。

根据备份配置，可以存储设备备份：

- 在故障设备本身的 `/var/sf/backup` 中。
- 在 管理中心 中的 `/var/sf/remote-backup`。
- 在远程存储位置。

对于 威胁防御 高可用性和集群 设备，您可以将组作为一个单元进行备份。对于高可用性设备，备份过程会生成唯一的备份文件，并在备份文件名称中标明每个设备的角色。 对于群集，控制节点和数据节点备份文件捆绑在一个压缩文件中。您必须提取文件，这些文件也会显示设备角色。

如果备份的唯一副本位于故障设备上，请立即将其复制到其他位置。如果重新映像设备，备份将被清除。如果出现其他问题，您可能无法恢复备份。有关详细信息，请参阅管理备份和远程存储， 第 462 页。

替换设备需要备份，但可以在恢复过程中使用 SCP 进行检索。我们建议您将备用设备放在 SCP 可访问的位置，以供替换设备使用。或者，您可以将备份复制到替换设备本身。

步骤 2 删除故障设备。

关机、关闭电源并删除虚拟机。对于程序，请参阅您的虚拟托管环境的相关文档。

步骤 3 部署替换设备。

请参阅https://www.cisco.com/go/ftdv-quick。

步骤 4 在替换设备上执行初始配置。

使用控制台以 `admin` 用户身份访问 威胁防御 CLI。安装向导会提示您配置管理 IP 地址，网关和其他基本网络设置。

请勿设置与故障设备相同的管理 IP 地址。如果您需要注册设备以进行修补，这可能会导致问题。恢复过程将正确重置管理 IP 地址。

请参阅入门指南中的 CLI 设置主题： https://www.cisco.com/go/ftdv-quick。

注释 如果需要修补替换设备，请按照入门指南中的说明启动 管理中心 注册过程。如果不需要修补， 请勿 注册。

步骤 5 确保替换设备运行与故障设备相同的软件版本， 包括补丁。

确保不应从管理中心中删除现有设备。替换设备应不受物理网络的管理，新硬件以及替换的 威胁防御 补丁应具有相同的版本。 威胁防御 CLI 没有升级命令。要修补，请执行以下操作：

a) 从 管理中心 Web 界面，完成设备注册过程。

创建新的AC策略并使用默认操作“网络发现”。保持此策略不变；请勿添加任何功能或修改。这用于注册设备和部署无功能的策略，以便您不需要许可证，然后便可以修补设备。备份恢复后，应将许可和策略恢复到预期状态。

b) 修补设备：https://www.cisco.com/go/ftd-upgrade。

c) 从 管理中心。

如果不注销，则在恢复过程将“旧”设备恢复后，您将有一个 Ghost 设备注册到 管理中心 。

步骤 6 确保替换设备有权访问备份文件。

恢复过程可以使用 SCP 检索备份，因此我们建议您将备份放在可访问的位置。或者，您可以手动将备份复制到替换设备本身，复制到 `/var/sf/backup`。 对于群集设备，从备份捆绑包中提取相应的备份文件。

步骤 7 从 威胁防御 CLI 恢复备份。

以 `admin` 用户身份访问 威胁防御 CLI。您可以使用控制台，也可以通过 SSH 连接到新配置的管理接口（IP 地址或主机名）。请记住，恢复过程将更改此 IP 地址。

要恢复，请执行以下操作：

- 使用 SCP： **restore remote-manager-backup location** *scp-主机名称 用户名 文件路径 备份 tar-文件*
- 从本地设备： **restore remote-manager-backup** 备份 *tar-文件*

在 威胁防御 高可用性 和集群 部署中，请确保选择适当的备份文件：主要与辅助，或控制与数据。该角色在备份文件名中注明。如果要恢复所有设备，请依次执行此操作。在第一台设备的恢复过程完成（包括重新启动）之前，请勿在下一台设备上运行 **恢复** 命令。

步骤 8 登录 管理中心 并等待替换设备连接。

还原完成后，设备会退出 CLI，重新启动并自动连接到 管理中心。此时，设备应显示为过时。

步骤 9 在部署之前，请执行任何恢复后任务并解决任何恢复后问题：

- 解决许可冲突或孤立授权问题。联系思科 TAC。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 威胁防御 设备中删除 VPN 证书，包括在执行备份后添加的证书。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 管理 *VPN* 证书 。

步骤 10 部署配置。

您 必须 部署。恢复设备后，必须从“设备管理”页面强制部署。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 将现有配置重新部署到设备 。

步骤 11 添加和配置数据接口。

请参阅入门指南：https://www.cisco.com/go/ftdv-quick。

下一步做什么

验证恢复是否成功以及替换设备是否按预期传递流量。

管理备份和远程存储

备份存储为未加密的存档（.tar）文件。文件名包括标识信息，包括：

- 与备份关联的备份配置文件或计划任务的名称。
- 备份设备的显示名称或 IP 地址。
- 设备的角色，例如 HA 对的成员。

我们建议备份到安全的远程位置并验证传输是否成功。设备上的备份可以手动或通过升级过程删除；升级会清除本地存储的备份。有关您的选项的详细信息，请参阅 备份存储位置 ，第 463 页。

注意 尤其是由于备份文件未加密的情况，因此不 允许未经授权的访问。如果修改备份文件，恢复过程将失败。请记住，具有 管理员/维护角色 的任何人都可以访问“备份管理”页面，他们可以在其中移动和删除远程存储中的文件。

以下程序介绍如何管理备份文件。

过程

步骤 1 选择**系统**（⚙）> **工具** > **备份/恢复**。

“备份管理”页面列出了可用的备份。它还列出了可用于存储备份的磁盘空间。如果没有足够的空间，备份可能会失败。

步骤 2 执行以下操作之一：

表 *51:* 远程存储和 备份文件管理

要想	相应操作
为备份启用或禁用远程存储，而无需编辑 管理中心 系统配置。	点击 **启用备份的远程存储**。 此选项仅在配置远程存储后显示。在此处切换也会在系统配置（**系统 > 配置 > 远程存储设备**）中切换它。 **提示** 要快速访问远程存储配置，请点击 **备份管理** 页面右上角的远程存储。 **注释** 要将备份存储在远程存储位置，还必须启用**检索到管理中心 (Retrieve to Management Center)** 选项（请参阅从 管理中心备份设备 ， 第 445 页）。
在 管理中心 和远程存储位置之间移动文件。	点击 **移动**。 您可以根据需要来回移动文件多次。这将从当前位置删除（而不是复制）文件。 将备份文件从远程存储移动到 管理中心时，其存储在 管理中心 上的位置取决于备份的类型： • 管理中心 备份： `/var/sf/backup` • 设备备份： `/var/sf/remote-backup`
查看备份的内容。	点击备份文件。
删除备份文件。	选择文件，并点击 **删除**。 您可以删除本地和远程存储的备份文件。
从您的计算机上传备份文件。	点击 **上传备份**，选择一个备份文件，然后再次点击 **上传备份** 。
将备份下载到您的计算机。	选择备份文件，然后点击 **下载**。 与移动备份文件不同，此操作不会从 管理中心 中删除备份。将下载的备份存储在安全的位置。

备份存储位置

下表介绍 管理中心 和受管设备的备份存储选项。

表 *52:* 备份存储位置

位置	详细信息
远程，通过安装网络卷（NFS、SMB、SSHFS）。	**注释** 仅当您已配置远程存储并启用检索到管理中心选项时，备份才会存储在远程存储位置（请参阅）。从 管理中心备份设备，第 445 页 在 管理中心的系统配置中，您可以将 NFS、SMB 或 SSHFS 网络卷安装为 管理中心 和设备备份的远程存储；请参阅 远程存储设备，第 92 页。） 执行此操作后，所有后续 管理中心 备份 和 管理中心发起的设备备份都将复制到该卷，但您仍可以使用 管理中心 来管理它们（恢复、下载、上传、删除、移动）。 请注意，只有 管理中心 安装网络卷。 受管设备备份文件通过 管理中心路由。确保你有足够的带宽在管理中心和其设备之间进行大量的数据传输。有关详细信息，请参阅将数据从 Firepower 管理中心下载到受管设备的准则（故障排除技术说明）。
远程，通过复制（SCP）。	**注释** 仅当您已配置远程存储并启用**检索到管理中心 (Retrieve to Management Center)** 选项时，备份才会存储在远程存储位置（请参阅 从 管理中心备份设备，第 445 页）。 对于 管理中心，可以使用**完成时复制 (Copy when complete)** 选项将已完成（SCP）的备份安全复制到远程服务器。 与通过安装网络卷的远程存储相比，**完成时复制** 无法复制到 NFS 或 SMB 卷。您无法提供 CLI 选项或设置磁盘空间阈值，并且它不会影响报告的远程存储。您也无法在备份文件复制后对其进行管理。 如果要在本地存储备份 并 将其 SCP 放置到远程位置，此选项非常有用。 **注释** 如果在 管理中心 系统配种中配置 SSHFS 远程存储，请勿在完成后使用**复制将备份文件复制到同一目录**。
本地，在 管理中心上。	如果未通过安装网络卷配置远程存储，则可以在 管理中心上保存备份文件： • 管理中心 备份保存到 `/var/sf/backup`。 • 如果在执行备份时启用**检索到管理中心 (Retrieve to Management Center)** 选项，设备备份将保存到 管理中心 上的 `/var/sf/remote-backup` 。

位置	详细信息
本地，位于设备内部闪存上。	如果您执行以下操作，设备备份文件将保存到设备上的 `/var/sf/backup`： • 请勿通过安装网络卷配置远程存储。 • 请勿启用 **向管理中心检索**。
本地，位于设备 SD 卡上。	对于 ISA 3000，当您将设备备份到本地 `/var/sf/backup` 内部闪存位置时，如果您安装了 SD 卡，备份将自动复制到 SD 卡，位于 `/mnt/disk3/backup/` 用于零接触恢复。

备份和恢复历史记录

功能	最低 管理中心	最低 威胁防御	详细信息
用于高可用性管理中心的单个备份文件。	7.4.1 7.2.6	任意	对高可用性对中的主用管理中心执行仅配置备份时，系统现在会创建一个备份文件，您可以使用该文件恢复任一设备。 其他版本限制：不支持管理中心版本 7.3.x 或 7.4.0。
对集群设备备份和恢复。	7.3.0	任意	您现在可以使用管理中心备份设备集群，但在公共云中除外（AWS的 Threat Defense Virtual）。要恢复，请使用设备 CLI。 新增/修改的屏幕：**系统 (System)** > **工具 (Tools)** > **备份/恢复 (Backup/Restore)** > **托管设备备份 (Managed Device Backup)** 新增/经修改的命令： **restore remote-manager-backup**
备份和恢复 AWS 的 Threat Defense Virtual。	7.2.0	任意	您现在可以使用管理中心备份 AWS 的 Threat Defense Virtual，但设备集群除外。要恢复，请使用设备 CLI。
使用 SD 卡在 ISA 3000 上进行零接触恢复	7.0.0	7.0.0	执行本地备份时，备份文件将复制到 SD 卡（如果有）。要恢复替换设备上的配置，只需在新设备中安装 SD 卡，并在设备启动期间按住重置按钮 3 到 15 秒。
FTD 容器实例备份和恢复。	6.7.0	6.7.0	您现在可以使用 FMC 在 Firepower 4100/9300 上对 FTD 容器实例执行按需远程备份。
不再需要匹配 VDB 即可恢复。	6.6.0	任意	从备份恢复 FMC 会将现有 VDB 替换为备份文件中的 VDB。在恢复之前，您不再需要匹配 VDB 版本。
自动安排的备份。	6.5.0	任意	对于新的或重映的FMC，设置流程会创建每周计划的任务，以备份FMC配置并将其存储在本地。

功能	最低 管理中心	最低 威胁防御	详细信息
托管设备的按需远程备份。	6.3.0	6.3.0	您现在可以使用 FMC 来预定某些受管设备的按需远程备份。 有关支持的平台，请参阅 备份和还原要求，第 437 页。 新增/修改的屏幕： **系统 > 工具 > 备份/恢复 > 受管设备备份** 新增/修改的 FTD CLI 命令： **restore**

第 16 章

计划

以下主题介绍如何安排任务：

关于任务安排

可安排各种任务在指定时间运行一次或反复运行。

任务在后端UTC中安排的，这意味着它们在本地发生的时间取决于日期和您的特定位置。此外，由于任务是以UTC为单位进行计划的，因此它们不会针对夏令时、夏令时或您在地点可能观察到的任何季节性调整进行调整。如果受影响，则根据当地时间，计划任务会在夏天比冬季中的一个小时开始。

某些任务由初始设置过程自动安排或执行：

- 下载并安装最新 VDB 的一次性任务。
- 用于下载最新可用软件更新和 VDB的每周计划任务，其中包括最新 VDB。
- 执行 管理中心 本地存储的仅配置备份的每周计划任务。

您应查看每周任务并在必要时进行调整。或者，安排新的周期性任务以实际更新 VDB 和/或软件，并部署配置。

重要事项 我们强烈建议您查看计划任务，确保这些任务在您预期的时间执行。有些任务（例如，那些涉及自动化软件更新的任务，或者要求将更新推送到受管设备的任务）可能会显著增加低带宽网络的负载。应安排此类任务在网络使用量较低的时段运行。其他任务（例如部署配置）可能会导致流量中断。您应在维护窗口期间安排此类任务。

任务安排的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 维护用户

配置周期性任务

使用相同流程为所有类型的任务设置周期性任务的频率。

请注意，Web 界面上大多数页面中显示的时间为本地时间，由您在本地配置中指定的时区决定。而且，管理中心将在适当时自动调整本地显示的夏令时 (DST) 时间。但是，从 DST 到标准时以及从标准时到 DST 跨越转换日期的周期性任务不会调整转换。即，如果创建的某项任务安排在标准时上午 2:00 执行，则它将于 DST 上午 3:00 运行。同理，如果创建的某项任务安排在 DST 上午 2:00 执行，则它将于标准时上午 1:00 运行。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从**作业类型 (Job Type)** 列表中，选择要安排的任务类型。

步骤 4 点击 **安排要运行的任务** 选项旁边的 **周期性** 。

步骤 5 在 **Start On** 字段中，指定想要开始周期性任务的日期。

步骤 6 在 **Repeat Every** 字段中，指定想要任务重复的频率。

可键入数字，或者点击 **向上**（▲） 和 **向下**（▼） 指定时间间隔。例如，键入 2 并点击 **天数** 让任务每两天运行一次。

步骤 7 在 **Run At** 字段中，指定想要开始周期性任务的时间。

步骤 8 如需每周或每月运行一次任务，请在**重复日期 (Repeat On)** 字段中选择要运行任务的天数。

步骤 9 为工作命名。

步骤 10 为正在创建的任务类型选择其余选项：

- “备份”(Backup) - 安排备份作业，如 计划 管理中心 备份， 第 469 页 中所述。
- “下载 CRL”(Download CRL) - 安排证书撤销列表下载，如配置证书撤销列表下载， 第 471 页中所述。
- “部署策略”(Deploy Policies) - 安排策略部署，如自动执行策略部署， 第 472 页中所述。
- “Nmap 扫描”(Nmap Scan) - 安排 Nmap 扫描，如安排 Nmap 扫描， 第 473 页中所述。
- “报告”(Report) - 安排报告生成，如 自动执行报告生成， 第 474 页中所述 。
- Cisco 建议规则 - 安排自动更新，如 自动生成 思科 建议， 第 476 页中所述。
- “下载最新更新”(Download Latest Update) - 安排软件或 VDB 更新下载，如自动执行软件下载， 第 477 页或自动执行 VDB 更新下载， 第 480 页中所述。
- “安装最新更新” - 安排在 管理中心 或受管设备上安装软件或 VDB 更新，如 自动执行软件安装， 第 479 页 或 自动执行 VDB 更新安装， 第 480 页中所述
- “推送最新更新”(Push Latest Update) - 安排将软件更新推送到受管设备，如自动执行软件推送， 第 478 页中所述。
- “更新 URL 过滤数据库”(Update URL Filtering Database) - 安排 URL 过滤数据的自动更新，如使用已安排任务自动执行 URL 过滤更新， 第 481 页中所述 。

步骤 11 点击**保存 (Save)**。

计划的备份

您可以在 Cisco Secure Firewall Management Center 上使用调度程序自动执行自己的备份。您还可以从管理中心安排远程设备备份。 有关备份的信息，请参阅 备份/恢复， 第 435 页。

请注意，并非所有设备都支持远程备份。

计划 管理中心 备份

您可以使用 管理中心 上的调度程序来自动执行 管理中心 和 设备备份。请注意，并非所有设备都支持远程备份。有关详细信息，请参阅备份/恢复， 第 435 页。

注释 作为初始配置的一部分， 系统会安排每周仅限配置的 管理中心 备份（本地存储）。我们建议您查看此任务，并在必要时进行更改，如 此主题。

开始之前

创建指定您的备份首选项的备份配置文件。请参阅创建备份配置文件， 第 447 页。

您必须在全局域中才能执行此任务。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 从 **Job Type** 列表中，选择 **Backup**。

步骤 3 指定要备份 **一次** 还是 **定期**备份。

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 对于定期任务，请参阅 配置周期性任务，第 468 页。

步骤 4 输入 **作业名称**。

步骤 5 对于 **备份类型**，点击 **管理中心**。

步骤 6 选择 **备份配置文件**。

步骤 7 （可选）输入 **注释**。

请保持注释简短。他们将显示在计划日历页面的“任务详细信息”部分中。

步骤 8 （可选）在 **邮件发送状态：** 字段中输入邮件地址或邮件地址的逗号分隔列表。

有关设置邮件中继服务器以发送任务状态消息的信息，请参阅 配置邮件中继主机和通知地址，第 58 页。

步骤 9 点击**保存 (Save)**。

安排远程设备备份

您可以使用 管理中心 上的调度程序来自动执行 管理中心 和设备备份。请注意，并非所有设备都支持远程备份。有关详细信息，请参阅备份/恢复，第 435 页。

您必须在全局域中才能执行此任务。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 从 **Job Type** 列表中，选择 **Backup**。

步骤 3 指定要备份 **一次** 还是 **定期**备份。

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 对于定期任务，请参阅 配置周期性任务，第 468 页。

步骤 4 输入 **作业名称**。

步骤 5 对于**备份类型**，请点击**设备**。

步骤 6 选择一个或多个设备。

如果您的设备未列出，则表示它不支持远程备份。

步骤 7 如果未配置远程备份存储，请选择是否要 **检索到管理中心**。

- 已启用（默认）：将备份保存到 `/var/sf/remote-backup/` 中的 管理中心。
- 已禁用：将备份保存到 `/var/sf/backup/`中的设备。

如果配置了远程备份存储，则远程保存备份文件，并且此选项无效。有关详细信息，请参阅管理备份和远程存储，第 462 页。

步骤 8 （可选）输入 **注释**。

请保持注释简短。他们将显示在计划日历页面的“任务详细信息”部分中。

步骤 9 （可选）在 **邮件发送状态：** 字段中输入邮件地址或邮件地址的逗号分隔列表。

有关设置邮件中继服务器以发送任务状态消息的信息，请参阅 配置邮件中继主机和通知地址，第 58 页。

步骤 10 点击**保存 (Save)**。

配置证书撤销列表下载

必须使用 管理中心。

当支持在启用用户证书或审核日志证书的设备上的本地配置中下载证书吊销列表 (CRL) 时，系统会自动创建下载 CRL 任务。可以使用计划程序来编辑任务以设置更新频率。

开始之前

- 启用并配置用户证书，或者审核日志证书并设置一个或多个CRL下载URL。有关详细信息，请参阅 需要有效的 HTTPS 客户端证书，第 65 页 和 需要有效的审核日志服务器证书，第 49 页。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **作业类型**中，选择 **下载 CRL**。

步骤 4 指定要如何安排 CRL 下载，**一次 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 468 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 7 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须在管理中心上配置一台有效的邮件中继服务器，以发送状态消息。

步骤 8 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址 ， 第 58 页

自动执行策略部署

在 管理中心 中修改配置设置后，必须将这些更改部署到受影响的设备。

⚠

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为和部署或激活时重启 Snort 进程的配置。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **作业类型**，选择 **部署策略**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务 ， 第 468 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在**设备 (Device)** 字段中，选择要部署策略的设备。

步骤 7 根据需要选中或取消选中 **跳过最新设备的部署** 复选框。

默认情况下，系统会启用**跳过最新设备的部署**以提高策略部署过程中的性能。

注释 如果从 管理中心 Web 界面发起的策略部署正在进行，则系统不会执行已安排的部署策略任务。相应地，如果已安排的策略部署任务正在进行，则系统不允许从 Web 界面发起策略部署。

步骤 8 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Tasks Details) 部分中；请保持注释简短。

步骤 9 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 10 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 58 页
需要部署的配置更改

Nmap 扫描自动化

您可在网络上安排定期 Nmap 目标扫描。自动化扫描允许您刷新 Nmap 扫描之前提供的信息。由于 Firepower 系统无法更新 Nmap 提供的数据，因此需要定期重新扫描以保持数据为最新。还可安排扫描，使其自动在网络主机上测试未识别的应用或服务器。

请注意，发现管理员也可使用 Nmap 扫描作为补救。例如，主机上发生的操作系统冲突可能会触发 Nmap 扫描。运行扫描可以获取主机的最新操作系统信息，这样可以解决冲突。

如果之前未曾使用 Nmap 扫描功能，则在定义计划扫描之前，需要配置 Nmap 扫描。

相关主题

Nmap 扫描

安排 Nmap 扫描

Nmap 使用 Nmap 扫描结果替换系统检测到的主机操作系统、应用或服务器之后，系统不再更新 Nmap 替换的主机信息。Nmap 提供的服务和操作系统数据将保持不变，直到您运行另一个 Nmap 扫描为止。如果计划使用 Nmap 扫描主机，则可能要设置定期安排的扫描，以使 Nmap 提供的操作系统、应用或服务器保持最新。如从网络删除主机并重新添加，则将丢弃任何 Nmap 扫描结果，系统假设监控主机的所有操作系统和服务数据。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type**，选择 **Nmap Scan**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 468 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在 **Nmap 补救**字段中，选择 Nmap 补救。

步骤 7 在 **Nmap 目标 (Nmap Target)** 字段中，选择扫描目标。

步骤 8 在**域 (Domain)** 字段中，选择要扩充其网络映射的域。

步骤 9 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

提示 注释字段显示在日历计划页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 10 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 11 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 58 页

自动执行报告生成

可自动生成报告，以使它们按固定间隔运行。

开始之前

- 对于风险报告以外的报告：创建报告模板。有关详细信息，请参阅报告模板，第 506 页。
- 如果要使用调度程序分发邮件报告，请配置邮件中继主机并指定报告收件人和消息信息。请参阅配置邮件中继主机和通知地址，第 58 页和（对于风险报告以外的报告）在生成时通过邮件分发报告，第 525 页或（对于风险报告）生成、查看和打印风险报告，第 504 页。
- （可选）设置或更改计划报告的文件名、输出格式、时间窗口或邮件分发设置。请参阅指定计划报告的报告生成设置，第 475 页。
- 如果您选择 PDF 作为报告输出格式，请查看报告模板并确认模板每个部分中的结果数量不超过 PDF 的相关限制。有关信息，请参阅报告模板字段，第 506 页。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从**作业类型 (Job Type)** 列表，选择一个作业。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 468 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在**报告模板 (Report Template)** 字段中，选择风险报告或报告模板。

步骤 7 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Tasks Details) 部分中；请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

注释 配置此选项**不会**分发报告。

步骤 9 如果不想在报告没有数据时（例如，当报告期间未发生特定类型的事件时）接收报告邮件附件，请选中**如果报告为空，仍附加到邮件中 (If report is empty, still attach to email)** 复选框。

步骤 10 点击**保存 (Save)**。

指定计划报告的报告生成设置

您必须具有管理员或安全分析师权限才能执行此任务。

要指定或更改计划报告的文件名、输出格式、时间窗口或邮件分发设置，请执行以下操作：

过程

步骤 1 选择**概述 > 报告 > 报表模板**。

步骤 2 针对要更改的报告模板，点击**编辑**。

步骤 3 如果您将选择 PDF 输出：

a) 查看报告中是否有任何部分在结果数量旁边显示一个黄色三角形。
b) 如果您看到任何黄色三角形，请将光标悬停在该三角形上，以查看该部分 PDF 输出允许的最大结果数。
c) 对于带有黄色三角形的每个部分，将结果数量减少到低于该限制的数量。
d) 如果没有其他黄色三角形，请点击**保存**。

步骤 4 点击**生成 (Generate)**。

注释 如果要更改报告生成设置而不立即生成报告，则必须从模板配置页中点击**生成**。如果从模板列表视图中点击**生成**，系统不会保存更改，除非您生成报表。

步骤 5 修改设置。

步骤 6 要保存新设置而不生成报告，请点击**取消**。

要保存新设置并生成报告，请点击**生成**，然后跳过此过程中的其余步骤。

步骤 7 点击**保存 (Save)**。

步骤 8 如果您看到有关保存的提示，即使您未进行更改，请点击**确定**。

自动生成 思科 建议

可使用自定义入侵策略中最近保存的配置设置，根据网络发现数据，自动生成规则状态建议。

注释 如果系统自动为入侵策略生成预定建议并且不保存更改，则必须丢弃在入侵策略中所做出的更改，而且如果想要策略反映自动生成的建议，还必须执行此策略。

当任务运行时，系统自动生成建议规则状态，并且根据策略的配置修改入侵规则的状态。已修改的规则状态在下次部署入侵策略时生效。

开始之前

- 在入侵策略中配置 思科 建议的规则，如 《Cisco Secure Firewall Management Center 设备配置指南》中所述。
- 如果要通过邮件发送任务状态消息，请配置有效的邮件中继服务器。
- 您必须具有 IPS 智能许可证或保护经典许可证才能生成建议。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **作业类型**中，选择 **Firepower 建议规则**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 468 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中输入名称。

步骤 6 在**策略 (Policies)** 旁边，选择要在其中生成建议的一个或多个入侵策略。选中 **所有策略** 复选框以选择所有策略。

步骤 7 （可选）在**注释 (Comment)** 字段中输入备注。

请保持注释简短。注释显示在计划日历页面的“任务详细信息”(Task Details) 部分中。

步骤 8 （可选）要通过邮件发送任务状态消息，请在**邮件状态收件人：(Email Status To:)** 字段中输入邮件地址（或以逗号分隔的多个邮件地址）。

步骤 9 点击**保存 (Save)**。

相关主题

冲突和更改：网络分析和入侵策略

关于 Cisco 建议的规则
配置邮件中继主机和通知地址，第 58 页

软件升级自动化

您可以自动下载 修补程序， 并应用维护版本和修补程序。

要升级 管理中心，请安排下载和安装任务。要升级受管设备，请安排下载、推送和安装任务。确保在任务之间留出足够的时间；例如，计划在推送仍在运行时进行的安装将失败。

主要版本不支持此功能。 需要访问互联网才能下载升级包。计划对设备组进行升级时，升级将同时在所有分组设备上运行。

注释 作为初始配置的一部分，系统会安排每周下载。我们建议您查看此任务，并在必要时进行更改，如自动执行软件下载，第 477 页。 此任务仅下载更新。您负责安装此任务下载的任何更新。

相关主题

管理接口，第 69 页
更新，第 211 页

自动执行软件下载

使用此程序可安排 和选定补丁和维护版本的下载。您必须在全局域中。

注释 在版本 7.4.1+ 中，此任务不再下载维护版本。要将维护（和主要）版本直接下载到 管理中心，请使用 **系统**（⚙）> **产品升级**。

开始之前

确保 管理中心可以访问互联网。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Download Latest Update**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 468 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 选中 **更新项目**旁边的 **软件** 复选框。

步骤 7 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 58 页

自动执行软件推送

如果想要在受管设备上自动安装软件更新，必须先将更新推送至设备，然后再安装。

创建向受管设备推送软件更新的任务时，确保在推送任务与预定安装任务之间预留充分时间，以便将更新复制至设备。

您必须在全局域中才能执行此任务。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Push Latest Update**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 468 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 从**设备 (Device)** 下拉列表中，选择要更新的设备。

步骤 7 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 58 页

自动执行软件安装

请确保在向受管设备推送更新的任务与安装更新的任务之间预留充分的时间。

您必须在全局域中才能执行此任务。

注意 视乎正在安装的更新，设备可能在安装软件之后重新启动。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从**作业类型 (Job Type)** 列表中，选择**安装最新更新 (Install Latest Update)**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 468 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在 **设备** 下拉列表中，选择要在其上安装更新的设备 （包括 管理中心） 。

步骤 7 选中**更新项目 (Update Items)** 旁边的**软件 (Software)** 复选框。

步骤 8 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 9 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 10 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 58 页

漏洞数据库更新自动化

可以使用安排功能更新思科漏洞数据库 (VDB)，从而确保正在使用最新信息评估网络主机。您必须将下载、安装和后续部署安排为单独的任务，以便在任务之间留出足够的时间。

注释 管理中心上的初始设置会自动下载并安装思科提供的最新VDB，作为一次性操作。它还会安排每周任务，以下载最新可用软件更新，其中包括最新VDB。我们建议您查看此每周任务，并在必要时进行调整。或者，安排新的周期性任务，以便实际更新 VDB 和/或软件并部署配置。

相关主题

管理接口，第 69 页

自动执行 VDB 更新下载

您必须在全局域中才能执行此任务。

开始之前

请确保 管理中心能够访问互联网。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Download Latest Update**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 468 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在**更新项目 (Update Items)** 旁边，选中**漏洞数据库 (Vulnerability Database)** 复选框。

步骤 7 （可选）在 **注释** 字段中输入简要注释。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 58 页

自动执行 VDB 更新安装

在 VDB 更新下载任务与更新安装任务之间预留足够的时间。

您必须在全局域中才能执行此任务。

⚠

注意 在大多数情况下，VDB 更新后的第一次部署会重新启动 Snort 进程，从而中断流量检查。系统会在发生这种情况时向您发出警告 （更新的应用检测器和操作系统指纹需要重新启动；漏洞信息不需要）。在此中断期间，流量是被丢弃还是不经进一步检查直接通过，将取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

过程

步骤 1 选择系统（⚙）> 工具 > 计划。

步骤 2 点击 **Add Task**。

步骤 3 从作业类型 **(Job Type)** 列表中，选择安装最新更新 **(Install Latest Update)**。

步骤 4 指定要如何安排任务，一次性 **(Once)** 或周期性 **(Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 468 页以了解详细信息。

步骤 5 在作业名称 **(Job Name)** 字段中键入名称。

步骤 6 从设备下拉列表中，选择 管理中心。

步骤 7 在更新项目 **(Update Items)** 旁边，选中漏洞数据库 **(Vulnerability Database)** 复选框。

步骤 8 （可选）在 注释 字段中输入简要注释。

步骤 9 如果要通过邮件发送任务状态消息，请在状态收件人：**(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 10 点击保存 **(Save)**。

相关主题

配置邮件中继主机和通知地址，第 58 页

使用已安排任务自动执行 URL 过滤更新

为了确保 URL 过滤的威胁数据为最新，系统必须从思科综合安全情报 (CSI) 云获取数据更新。

默认情况下，在启用URL过滤时，也会启用自动更新。但是，如果需要控制这些更新的发生时间，请使用本主题中所述的程序，而不要使用默认更新机制。

尽管每日更新往往较小，如果距离上次更新已超过五天，新 URL 过滤数据可能需要 20 分钟才能下载完成，具体情况视带宽而定。然后，执行更新也可能最多需要 30 分钟。

开始之前

- 确保 管理中心能够访问互联网；请参阅安全、互联网接入和通信端口，第 1013 页。
- 确保 URL 过滤已启用。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 使用类别和信誉启用 *URL* 过滤。
- 验证未选中 集成 > 其他集成 菜单下 云服务 上的 启用自动更新 。
- 您必须在全局域中才能执行此任务。您必须具有 URL 过滤许可证。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Update URL Filtering Database**。

步骤 4 指定要如何安排更新，**一次性 (Once)** 或者**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 468 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 7 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 8 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 58 页

预定任务审核

添加预定任务后，即可查看这些任务，评估它们的状态。在页面的“查看选项”(View Options) 部分，查使用日历和预定任务列表查看预定任务。

Calendar 视图选项可用于查看哪些预定任务在哪天发生。

“任务列表”(Task List) 显示一列任务及其状态。打开日历时，任务列表出现在日历下方。此外，也可通过从日历中选择日期或任务来查看它。

可编辑先前创建的预定任务。如果想要测试一次预定任务，确保参数正确，此功能特别有用。稍后，任务成功完成后，即可将其更改为周期性任务。

可从“计划视图”(Schedule View) 页面执行两类删除。可删除尚未运行的特定一次性任务，也可删除周期性任务的每个实例。如果删除周期性任务的一个实例，该任务的所有实例均将删除。如果删除预定运行一次的任务，则仅删除该任务。

任务列表详细信息

表 *53:* 任务列表列

列	说明
名称 (Name)	显示预定任务的名称及与其关联的注释。
类型	显示预定任务的类型。
开始时间 (Start Time)	显示预定任务的开始日期和时间。
频率 (Frequency）	显示任务的运行频率。
上次运行时间	显示实际开始日期和时间。 对于周期性任务，这适用于最近执行。
上次运行状态	描述预定任务的当前状态。 • **复选标记** （ ） 指明任务已成功运行。 • 问号图标 (**问号** （ ）) 指明任务处于未知状态。 • 感叹号图标 ( ) 指明任务已失败。 对于周期性任务，这适用于最近执行。
下次运行时间	显示周期性任务的下次执行时间。 为一次性任务显示“不适用”(N/A)。
创建者	显示创建预定任务的用户的名称。
编辑	编辑预定任务。
删除	删除预定任务。

在日历中查看预定任务

您可以在日历上查看计划任务。

过程

步骤 1 选择**系统**（ ） > **工具** > **计划**。

步骤 2 可使用日历视图执行以下任务：

- 点击 **双左箭头**（«） 可后退一年。
- 点击 **单左箭头**（<） 可后退一个月。
- 点击 **单右箭头**（>） 可向前移动一个月。
- 点击 **双右箭头**（»） 可向前移动一年。
- 点击**今天 (Today)**，返回当前月份和年份。
- 点击**添加任务 (Add Task)**，安排新任务。
- 点击一个日期，在日历下方的任务列表中查看所有预定任务的特定日期。
- 点击在某个日期发生的特定任务，在日历下方的任务列表中查看此任务。

编辑预定任务

您可以编辑计划任务。

过程

步骤 1 选择**系统**（⚙） > **工具** > **计划**。
步骤 2 在日历上，点击要编辑的任务，或者任务出现的日期。
步骤 3 在 **任务详细信息** 表中，点击要编辑的任务旁边的 **编辑**（✎） 。
步骤 4 编辑任务。
步骤 5 点击**保存 (Save)**。

删除预定任务

您可以删除计划任务。

过程

步骤 1 选择**系统**（⚙） > **工具** > **计划**。
步骤 2 在日历中，点击要删除的任务。对于周期性任务，请点击任务的实例。
步骤 3 在 **任务详情** 表中，点击 **删除**（🗑），然后确认您的选择。

计划任务的历史记录

功能	最低 管理中心	最低 威胁防御	详情
计划任务仅下载补丁和 VDB 更新。	7.4.1	任意	**升级影响。计划的下载任务停止检索维护版本。** **下载最新更新** 计划任务不再下载维护版本；现在，它仅下载最新的适用补丁和 VDB 更新。要将维护（和主要）版本直接下载到管理中心，请使用 **系统**（⚙）> **产品升级**。 其他版本限制：不支持管理中心版本 7.3.x 或 7.4.0。
自动 VDB 下载。	7.3.0	任意	初始设置计划每周执行一次任务，以下载最新的可用软件更新，现在包括最新的VDB。我们建议您查看此每周任务并在必要时进行调整，同时安排新的每周任务来实际更新VDB。您必须部署配置，新的应用检测器和操作系统指纹才会生效。 新增/修改的屏幕：默认情况下，系统创建的 **每周软件下载** 计划任务中的 **漏洞数据库** 复选框现在处于启用状态。
自动入侵规则更新。	6.6	任意	初始设置现在会启用每日入侵规则更新。我们建议您查看此任务，并在必要时进行调整。要让更新后的规则生效，您必须部署配置。
自动软件下载和配置备份。	6.5	任意	初始设置现在会安排每周任务以便： • 为 FMC 及其托管设备下载最新的可用软件更新。 • 执行本地存储的仅配置备份。 我们建议您查看这些任务，并在必要时进行调整。
为许多托管设备安排远程备份。	6.4	任意	安排设备备份。 新增/修改的屏幕：配置定期备份时，您现在可以选择**备份类型 (Backup Type)**：管理中心与设备。 平台限制：设备必须支持按需备份；请参阅 备份和还原要求，第 437 页。

第 17 章

导入/导出

以下主题介绍如何使用导入/导出功能：

关于配置导入/导出

可以使用导入/导出功能在设备之间复制配置。导入/导出不是备份工具，但可简化将新设备添加到部署的过程。

既可导出单项配置，也可通过单次操作导出一组（相同类型或不同类型的）配置。当您稍后将软件包导入另一台设备时，您可选择要导入软件包中的哪些配置。

导出的数据包包含该配置的版本信息，从而确定是否可以将该配置导入到另一设备上。当设备兼容但数据包包含重复配置时，系统会提供解决方法选项。

注释 导入和导出设备必须运行相同版本的Firepower系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。如果版本不匹配，导入将失败。您可以使用导入/导出功能更新入侵规则。相反，请下载并应用最新的规则更新版本。

支持导入/导出的配置

以下配置支持导入/导出：

- 访问控制策略及其调用的策略：预过滤器、网络分析、入侵、SSL、文件、威胁防御服务策略
- 入侵策略，与访问控制无关
- NAT 策略（仅限 Cisco Secure Firewall Threat Defense）

- FlexConfig 策略。但在导出该策略时，将会清除任何密钥变量的内容。在导入使用密钥的 FlexConfig 策略后，必须手动编辑所有密钥的值。
- 平台设置
- 运行状况策略
- 警报响应
- 应用检测器（用户定义的检测器以及那些由思科专业服务提供的检测器）
- 控制面板
- 自定义表
- 自定义工作流程
- 保存的搜索
- 自定义用户角色
- 报告模板
- 第三方产品和漏洞映射
- 用于用户控制的用户和组

配置导入/导出的特殊注意事项

当导出配置时，系统也会导出其他所需的配置。例如，导出访问控制策略也会导出该策略调用的任何子策略、该策略使用的对象和对象组、祖先策略等等。又例如，如果导出启用了外部身份验证的平台设置策略，则也会导出身份验证对象。但是，也有一些例外：

- 系统提供的数据库和源 - 系统不会导出 URL 过滤类别和信誉数据、思科情报源数据或地理位置数据库 (GeoDB)。确保部署中的所有设备可从思科获取最新信息。
- 全局安全情报列表 - 系统会导出与导出的配置关联的全局安全情报阻止和 不阻止 名单。导入过程将这些名单转换为用户创建的列表，然后将这些新列表用于导入的配置中。这可确保导入的列表不会与现有全局阻止和 不阻止 名单发生冲突。要在导入 管理中心 时使用全局列表，请将这些列表手动添加到导入的配置中。
- 入侵策略共享层 - 导出过程会中断入侵策略共享层。以前共享的层包含在数据包中，而导入的入侵策略不包含共享层。
- 入侵策略默认变量集 - 导出数据包包含一个默认变量集，此变量集包含自定义变量及带用户定义值的系统提供的变量。导入过程会使用导入的值更新导入 管理中心上的默认变量集。但是，导入过程**不**会删除不存在于导出数据包中的自定义变量。对于在导出数据包中未设置的值，导入过程也不会恢复导入 管理中心上的用户定义值。因此，如果导入管理中心具有配置不同的默认变量，则导入的入侵策略的行为可能会与预期大不相同。
- 自定义用户对象 - 如果您在 管理中心中创建了自定义用户组或对象，并且此类自定义用户对象是访问控制策略中任何规则的一部分，那么请注意，导出文件 (.sfo) 不会包含用户对象信息，因

此在导入此类策略时，对此类自定义用户对象的任何引用都将被删除，不会导入到目标 管理中心。为了避免由于缺少用户组而引起的检测问题，请手动将自定义的用户对象添加到新的 管理中心，并在导入后重新配置访问控制策略。

导入对象和对象组时：

- 通常，导入过程将对象和对象组作为新对象和对象组导入，您不能替换现有的对象和对象组。但是，如果采用导入的配置的网络和端口对象或对象组与现有对象或对象组匹配，则导入的配置将重用现有对象/对象组，而不是创建新的对象/对象组。系统通过比较每个网络和端口对象/对象组的名称（不包括任何自动生成的编号）和内容来确定匹配。
- 如果在导入 管理中心时导入对象的名称与现有对象匹配，系统会将自动生成的编号附加到导入的对象和对象组的名称，以使其唯一。
- 您必须将导入的配置中使用的任何安全区域和接口组映射到导入 管理中心管理的匹配类型区域和组。
- 如果导出使用包含私钥的 PKI 对象的配置，系统会在导出之前解密私钥。导入时，系统会使用随机生成的密钥加密密钥。

配置导入/导出的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员

导出配置

导出过程可能需要几分钟，取决于正在导出的配置数量以及这些配置引用的对象数量。

提示

Firepower 系统中的许多列表页面的列表项旁均包括 **YouTube EDU**（） 。如果该图标存在，您可将其作为下列导出步骤的快速替代项。

开始之前

- 确认导入和导出设备运行的是同一版本的Firepower系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。

过程

步骤 1 选择**系统**（⚙）> **工具** > **导入/导出**。

步骤 2 点击 **折叠**（⌄）和 **展开**（>）图标以折叠和展开可用配置列表。

步骤 3 选中要导出的配置并点击**导出 (Export)**。

步骤 4 按照网页浏览器提示将已导出软件包保存至计算机。

导入配置

视乎正在导入的配置数量以及这些配置所引用的对象数量，导入过程可能需要几分钟。

注释 如果您注销系统、如果您更改到其他域，或者点击**导入**后用户会话到期，导入过程将在后台继续进行，直到完成为止。我们建议您等待导入过程完成，然后再创建任何新的对象或策略。在导入过程中尝试创建它们可能会导致失败。

开始之前

- 确认导入和导出设备运行的是同一版本的软件系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。

过程

步骤 1 在导入设备上，选择**系统**（⚙）> **工具** > **导入/导出**。

步骤 2 点击**上传软件包**。

步骤 3 输入已导出的软件包的路径或浏览到其位置，然后点击**上传 (Upload)**。

步骤 4 如果没有版本不匹配情况或其他问题，请选择要导入的配置，然后点击**导入 (Import)**。
如果无需执行任何冲突解决方案或接口对象映射，则表明导入完成，并会显示成功消息。跳过此程序的其余步骤。

步骤 5 如果提示，请在导入冲突解决方案页面上，将已导入的配置中使用的接口对象映射到具有由导入 管理中心管理的匹配接口类型的区域和组。

源和目标接口对象的接口对象类型（安全区域或接口组）以及接口类型（被动，内联，路由等等）必须匹配。有关信息，请参阅接口。

如果您正在导入的配置引用尚不存在的安全区域或接口组，则可以将其映射到现有接口对象或创建新接口对象。

注释　对于单个访问控制策略，您可以选择将现有策略替换为导入的策略。但是，对于嵌套访问控制策略，只能将其作为新策略导入。

步骤 6　点击 **Import**。

步骤 7　如果提示，请在“导入解决方案”(Import Resolution) 页面上，展开每项配置并选择相应的选项，如解决导入冲突，第 491 页中所述。

步骤 8　点击 **Import**。

步骤 9　更新所有源。

例如，转到 **对象 > 对象管理 > 安全情报**，然后点击 URL、网络和 DNS 列表和源页面上的 **更新源** 按钮。

导入的策略不包括源内容。

步骤 10　等待所有源更新完成，然后再将策略部署到设备。

下一步做什么

注释　如果导入包含 Microsoft Active Directory 用户和组的配置 我们强烈建议您在导入后下载所有用户和组，以避免出现访问控制策略和其他策略 解密策略中的问题。（**集成 > 其他集成 > 领域**，然后点击 ⬇（**立即下载**）。

- 或者，查看总结已导入的配置的报告；请参阅查看任务消息，第 415 页。

解决导入冲突

当您尝试导入配置时，系统会确定设备上是否已存在同一名称和类型的配置。当导入包含重复配置时，系统会提供适合于您的部署的解决方法选项，其中包括：

- **保持现有配置 (Keep existing)**

  系统不导入该配置。

- **替换现有配置 (Replace existing)**

  系统使用选择用于导入的配置覆盖当前配置。

- **保留最新配置 (Keep newest)**

  仅在所选配置的时间戳比设备上的当前配置中的时间戳更新时，系统才会导入所选配置。

注释 如果导入包含 Microsoft Active Directory 用户和组的配置 我们强烈建议您在导入后下载所有用户和组，以避免出现访问控制策略和其他策略解密策略中的问题。（**集成** > **其他集成** > **领域**，然后点击 （**立即下载**）。

- **导入为新配置 (Import as new)**

  系统导入所选重复配置，将系统生成的编号附加到名称以使其唯一。（可以在完成导入过程之前更改此名称。）设备上的原始配置保持不变。

系统提供的解决方法选项取决于部署是否使用域，以及导入的配置是在当前域中定义的配置的重复，还是在当前域的祖先或后代中定义的配置的重复。下表列出系统何时提供或不提供解决方法选项。

解决方法选项	Cisco Secure Firewall Management Center		受管设备
	在当前域中重复	在祖先域或后代域中重复	
保持现有配置 (Keep existing)	兼容	兼容	兼容
替换现有配置 (Replace existing)	是	否	兼容
保留最新配置 (Keep newest)	是	否	兼容
导入为新配置 (Import as new)	兼容	兼容	兼容

当导入包含使用干净或自定义检测文件列表的文件策略的访问控制策略，并且文件列表出现重复名称冲突时，系统会提供上表中所述的冲突解决方法选项，但是系统对策略和文件列表执行的操作会有所差异，如下表所述：

解决方法选项	系统操作	
	访问控制策略及其关联的文件策略导入为新策略，并且合并文件列表	现有访问控制策略及其关联的文件策略和文件列表保持不变
保持现有配置 (Keep existing)	不兼容	兼容
替换现有配置 (Replace existing)	是	否
导入为新配置 (Import as new)	是	否

解决方法选项	系统操作	
	访问控制策略及其关联的文件策略导入为新策略，并且合并文件列表	现有访问控制策略及其关联的文件策略和文件列表保持不变
保持最新配置 (Keep newest)，并且导入的访问控制策略为最新策略	是	否
保持最新配置 (Keep newest)，并且现有访问控制策略为最新策略	不兼容	兼容

如果修改设备上的已导入配置，然后将该配置重新导入到同一设备，则必须选择要保留的配置版本。

第 18 章

数据清除和存储

存储在 FMC 上的数据

对象	请参阅
有关 FMC 上数据存储的一般信息	磁盘使用率构件， 第 330 页
清除旧数据	从 管理中心 数据库清除数据， 第 496 页
允许外部访问 FMC 上的数据（这是一项高级功能）	外部数据库访问， 第 58 页
备份	管理备份和远程存储， 第 462 页 和子主题
报告	配置本地存储， 第 93 页
事件	连接日志记录， 第 699 页 数据库， 第 54 页 和子主题
网络发现数据	网络发现数据存储设置 和 《Cisco Secure Firewall Management Center 设备配置指南》中的后续主题
文件	《Cisco Secure Firewall Management Center 设备配置指南》的 网络恶意软件保护和文件策略 一章中有关存储文件的信息，包括最佳实践。 调整文件和恶意软件检测性能和存储 《Cisco Secure Firewall Management Center 设备配置指南》
数据包数据	《Cisco Secure Firewall Management Center 设备配置指南》中的编辑常规设置

对象	请参阅
用户和用户活动	《Cisco Secure Firewall Management Center 设备配置指南》中的用户数据库 《Cisco Secure Firewall Management Center 设备配置指南》中的用户活动数据库

从 管理中心 数据库清除数据

您可以使用数据库清除页面从 管理中心 数据库清除发现、身份、连接和安全情报数据文件。请注意，清除数据库时，会重新启动相应的进程。

⚠

注意 清除数据库会从 管理中心中移除指定的数据。删除数据后，该数据无法恢复。

开始之前

您必须具有管理员或安全分析师权限才能清除数据。您只能在全局域中。

过程

步骤 1 选择**系统**（⚙）> **工具** > **数据清楚**。

步骤 2 在 **发现和身份**下，执行以下任何或所有操作：

- 选中**网络发现事件 (Network Discovery Events)** 复选框以从数据库删除所有网络发现事件。
- 选中**主机 (Hosts)** 复选框以从数据库删除所有主机和主机 危害表现标志。
- 选中**用户活动 (User Activity)** 复选框以从数据库删除所有用户活动事件。
- 选中**用户身份 (User Identities)** 复选框以从数据库删除所有用户登录信息和用户历史记录数据，以及用户危害表现标志。

  注释 不会 删除 Microsoft Azure AD 领域的用户活动事件、用户登录和用户历史记录数据。

步骤 3 在 **Connections** 下，执行以下任一或所有步骤：

- 选中**连接事件 (Connection Events)** 复选框以从数据库删除所有连接数据。
- 选中**连接摘要事件 (Connection Summary Events)** 复选框以从数据库删除所有连接摘要数据。
- 选中**安全情报事件 (Security Intelligence Events)** 复选框以从数据库删除所有安全情报数据。

注释 选中**连接事件**复选框不会删除安全情报事件。带有安全情报数据的连接仍将显示在“安全情报事件”页面上（位于“分析”>“连接”菜单下）。同样，选中**安全情报事件 (Security Intelligence Events)** 复选框不会删除具有关联安全情报数据的连接事件。

步骤 4 点击**清除所选事件 (Purge Selected Events)**。
项目会被清除，且相应进程会重启。

外部数据存储

您可以选择使用远程数据存储来存储某些类型的数据。

对象	请参阅
备份	管理备份和远程存储， 第 462 页 和子主题 远程存储设备， 第 92 页 和子主题
报告	远程存储设备， 第 92 页 和子主题 将报告移至远程存储器， 第 528 页
事件	有关 使用外部工具的事件分析， 第 597 页中的系统日志和其他资源的信息 在思科 Cisco Secure Cloud Analytics中的远程数据存储， 第 498 页 Secure Network Analytics 设备上的远程数据存储， 第 498 页 如果您远程存储连接事件，请考虑在FMC上禁用连接事件的存储。有关信息，请参阅 数据库， 第 54 页 以及子主题。

重要事项 如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。

安全分析和日志记录 远程事件存储选项的比较

将事件数据存储到 管理中心外部的类似但不同的选项：

本地	SaaS
您购买、许可并设置防火墙后的存储系统。	您购买许可证和数据存储计划，并将数据发送到思科云。

本地	SaaS
支持的事件类型： • 连接 • 安全情报 • 入侵 • 文件和恶意软件 • LINA	支持的事件类型： • 连接 • 安全情报 • 入侵 • 文件和恶意软件
支持系统日志和直接集成。	支持系统日志和直接集成。
• 查看 Cisco Secure Network Analytics 管理器上的所有事件。 • 从 FMC 事件查看器交叉启动，以查看 Cisco Secure Network Analytics 管理器上的事件。 • 在 FMC 中查看远程存储的连接和安全情报事件	在 CDO 中查看事件，或者 Secure Network Analytics，具体取决于您的许可证。从 FMC 事件查看器交叉启动。
有关更多信息，请参阅 Secure Network Analytics 设备上的远程数据存储，第 498 页中的链接。	有关更多信息，请参阅 在思科 Cisco Secure Cloud Analytics中的远程数据存储，第 498 页中的链接。

在思科 Cisco Secure Cloud Analytics中的远程数据存储

使用 安全分析和日志记录 (SaaS)将选定的 Firepower 事件数据发送到 Cisco Secure Cloud Analytics 。支持的事件：连接、安全情报、入侵、文件和恶意软件。

关于详细信息，请参阅 https://cisco.com/go/firepower-sal-saas-integration-docs中的 *Firepower* 管理中心和思科安全分析与日志记录 *(SaaS)* 集成指南 。

您可以直接或通过系统日志发送事件。

重要事项 如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。

Secure Network Analytics 设备上的远程数据存储

如果您需要比 Firepower 设备更多的数据存储，可以使用 安全分析和日志记录（本地部署） 在 Secure Network Analytics 设备上存储 Firepower 数据。有关完整信息，请参阅 https://cisco.com/go/sal-on-prem-docs提供的文档。

您可以在 管理中心 中查看连接事件，即使它们存储在 Secure Network Analytics设备上。请参阅在 Cisco Secure Firewall Management Center 和使用存储在 Secure Network Analytics 设备上的连接事件上工作，第 651 页。

重要事项 如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。

数据存储历史记录

功能	最低 管理中心	最低 威胁防御	详情
免除低优先级连接事件的事件速率限制	7.0	任意	如果您选择不在 管理中心 上存储连接事件，因为您将它们存储在远程卷上，则这些事件不会计入 管理中心 硬件设备的流量限制。 如果使用新的 7.0 配置将事件发送到 安全分析和日志记录（本地部署），则将此设置配置为该集成的一部分。 否则，请参阅 数据库事件限制，第 55 页中的有关连接数据库的信息。 新增/修改的页面：无。仅行为更改。
改进了将事件发送到 Secure Network Analytics 设备的流程	7.0	任意	新向导简化了使用 安全分析和日志记录（本地部署）将事件直接发送到 Secure Network Analytics 设备的过程。 该向导还允许您在查看 管理中心上的事件页面时查看远程存储的连接事件，并从 管理中心 交叉启动以查看 Secure Network Analytics 设备上的事件。 如果您已将系统配置为使用系统日志发送事件，则将继续使用系统日志发送事件，除非您禁用这些配置。 有关详细信息，请参阅 Secure Network Analytics 设备上的远程数据存储，第 498 页中引用的文档。 新增/修改的页面： **系统 > 日志记录 > 安全分析和日志记录** 页面现在显示用于创建交叉启动选项的向导，而不是配置。

功能	最低 管理中心	最低 威胁防御	详情
Secure Network Analytics 设备上的远程数据存储	6.7	任意	您现在可以使用 安全分析和日志记录（本地部署）远程存储大量 Firepower 事件数据。在 管理中心中查看事件时，您可以快速交叉启动以查看远程数据存储位置中的事件。 支持的事件：连接、安全情报、入侵、文件和恶意软件。使用系统日志发送事件。 此解决方案取决于运行 Stealthwatch Enterprise (SWE) 版本 7.3 的 Stealthwatch 管理控制台 (SMC) 虚拟版的可用性。 请参阅 Secure Network Analytics 设备上的远程数据存储 ，第 498 页。
在思科 Cisco Secure Cloud Analytics中的远程数据存储	6.4	任意	使用系统日志发送选定的 Firepower 数据使用 安全分析和日志记录 (SaaS)。支持的事件：连接、安全情报、入侵、文件和恶意软件。 关于详细信息，请参阅 https://cisco.com/go/firepower-sal-saas-integration-docs中的 *Firepower* 管理中心和思科安全分析与日志记录 *(SaaS)* 集成指南 。

第 V 部分

报告和警报

第 19 章

报告

以下主题介绍如何在 Firepower 系统中使用报告：

报告的要求和前提条件

型号支持

任何。

支持的域

任意

用户角色

- 管理员
- 维护用户 （仅风险报告）
- 安全分析师

报告简介

Firepower 系统提供两种类型的报告：

- 风险报告， 第 504 页 — 在您的网络上发现的风险的高级摘要。

- 标准报告，第 505 页 — 关于您的 Firepower 系统的所有方面的详细可自定义报告。

风险报告

风险报告是对组织中发现的风险的可移植、高级别、易于解释的摘要。您可以使用这些报告与无权访问您的系统以及可能不是网络安全专家的人员共享有关风险区域的信息以及处理这些风险的建议。这些报告旨在促进对网络安全投资领域的讨论。

风险报告模板

- **高级恶意软件风险报告**
- **攻击风险报告**。以下是此报告中的字段：
  - **攻击总数**-IPS 事件总数。
  - **相关攻击**-影响标志等于 1 的 IPS 事件的数量。
  - **目标主机**-IPS 事件中影响标志等于 1 的唯一目标 IP 地址的数量。
  - **无关攻击**-影响标志不等于 1 的 IPS 事件的百分比。
  - **需要注意的事件**-影响标志为 1 的 IPS 事件的百分比。
  - **连接到 CnC 服务器的主机**-IOC 类别为 “已连接 CnC”的唯一主机的总数。
- **网络风险报告**

生成、查看和打印风险报告

标准报告模板不适用于风险报告。

报告与当前域相关。

每个风险报告生成为 HTML 文件。

要安排风险报告生成，请参阅自动执行报告生成，第 474 页。

开始之前

- 确保将您的系统配置为检测要总结的风险。
- 如果要通过邮件传送报告且尚未配置中继主机，则可以立即执行此操作。有关信息，请参阅配置邮件中继主机和通知地址，第 58 页。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板**。

步骤 3 点击所需报告的 **生成报告** 。

步骤 4 输入信息。

- 在“输入参数”(Input Parameters) 部分中输入的信息将显示在报告的标题页面上。您可以将这些字段留空。

步骤 5 点击**生成 (Generate)**。

步骤 6 点击 **OK**。

下一步做什么

- 要查看、下载、移动或删除风险报告，请参阅关于使用生成的报告 ， 第 526 页。
- 可以从大多数受支持的浏览器将任何风险报告打印为 PDF。要获得最佳效果，请在浏览器的打印或打印预览设置中启用背景色、图像以及页眉和页脚（可选）。支持的页面大小为 A4 和美国信纸大小。

标准报告

系统提供一个灵活的报告系统，能够利用 管理中心上显示的事件视图或控制面板快速而轻松地生成多部分报告。还可以从头设计自定义报告。

报告是一种采用 PDF、HTML 或 CSV 格式的文档文件，其包含要传达的内容。报告模板指定报告及其各部分的数据搜索和格式。系统内有一个功能强大的报告设计器，用于自动执行报告模板的设计。可以复制 Web 界面中显示的任何活动视图表或控制面板图形的内容。

可以根据需要的数量创建报告模板。每个报告模板均可定义报告中的各个部分，并指定创建报告内容的数据库搜索，以及演示文稿格式（表、图表，详细视图等等）和时间范围。模板还指定文档属性，例如封面和目录以及文档页面是否有页眉和页脚（仅适用于 PDF 格式的报告）。可以将报告模板导出到单个的配置包文件中，然后再导入，以便在其他 管理中心上重复使用。

在模板中可以加入输入参数，以扩展其实用性。使用输入参数，可以对相同报告进行定制化变动。当使用输入参数生成报告时，生成过程会提示输入每个输入参数的值。键入的值对报告内容的限制是一次性的。例如，在生成入侵事件报告的搜索“目标 IP”字段可以放入一个输入参数；在报告生成时，可以在系统提示输入目标 IP 地址时指定部门的网段。生成的报告随后只包含该特定部门的相关信息。

关于设计报告

报告模板

使用报告模板定义报告每部分数据的内容和格式，以及报告文件的文档属性（封面、目录以及页眉和页脚）。在生成报告之后，模板仍可重复使用，直到将其删除为止。

报告包含一个或多个信息部分。为每个部分分别选择格式（文本、表或图表）。针对某部分所选的格式可能会限制其可包含的数据。例如，使用饼图格式，无法显示某些表中基于时间的信息。可以随时更改部分的数据条件或格式，以获得最佳演示效果。

可以在预定义的事件视图基础上完成报告的初始设计，也可以通过从任何定义的控制面板、工作流程或摘要导入内容开始设计。还可以从空的模板开始添加部分并逐一定义其属性。

注释 在多域部署中，可以查看但无法编辑属于祖先域的报告模板。要从这些模板生成报告，必须将它们复制到当前的域。

报告模板字段

下表列出可以用来构建报告模板组成部分的字段。并非所有字段都会在所有类型的部分中使用；选择一个部分所采用的格式后，系统会显示相应的字段。

字段名称	部分类型	定义
格式	n/a	选择部分数据所采用的格式： **条形图**（）：比较所选变量的数量。 **折线图**（）：显示所选变量随时间推移的趋势/更改。仅适用于基于时间的表。 **饼图**（）：将每个所选变量显示为总体的百分比。数量为零的变量不在图表中显示。极少的数量归到标记为 **Other** 的类别。 **表视图**（）：显示每个记录的属性值。不适用于摘要或统计数据。 **详细信息视图**（）：显示与特定事件相关联的复杂对象数据，例如数据包（用于入侵事件）和主机配置文件（用于主机事件）。此格式仅适用于涉及此类对象的事件类型。如果请求的数量很大，输出可能会降低性能。
表	全部	选择从其提取部分数据的表。
预设	全部	预定义的搜索。在定义新的搜索时，请选择合适的预设初始化搜索条件。
Search 或 Filter	全部	对于大多数表，可使用预定义的或保存的 **Search** 限制报告。您还可以通过点击 **编辑**（） 来创建新搜索。 对于“应用统计信息”(Application Statistics) 表，使用用户定义的应用**过滤器**限制报告。

字段名称	部分类型	定义
X 轴	条形图 折线图 饼图	所选图表的 X 轴的可用数据。 对于折线图，X 轴值始终是 **Time**。对于条形图和饼图，则不能选择 **Time** 为 X 轴值。
Y 轴	条形图 折线图 饼图	所选图表的 Y 轴的可用数据。
部分说明	全部	位于部分中的搜索数据前面的描述性文本。 输入文本和输入参数组合。新部分的默认设置是 `$<Time Window>` 和 `$<Constraints>`。
时间窗口	全部	部分中显示的数据的时间窗口。 如果部分搜索基于时间的表，可以选择复选框以继承报告的全局时间窗口。或者，可以为部分设置特定时间窗口。
数据源	所有 (All)	如果使用向导配置 安全分析和日志记录（本地部署）使用的远程（外部）数据存储，则可以选择用于连接和安全情报事件的数据源。 选项如下： • **自动**：显示 FMC 上存储的数据（如果可用）。如果 FMC 上的数据在整个所选时间段内不可用，则仅显示远程存储的数据。 • **本地**：仅显示存储在 FMC 上的数据，无论选择的时间段如何。 选择此选项以包括远程卷上不可用的数据，例如从未配置为将事件发送到远程卷的设备生成的事件。 • **扩展**：仅显示存储在远程卷上的数据。
最大结果数	表格视图 详细信息视图	要包括的匹配记录最大数。 与 CSV 或 HTML 报告相比，PDF 报告可以包括更少的记录。如果数量太大，Web 界面将通过警告和错误图标加以指示。将鼠标指针悬停在图标上可查看限制。
结果	条形图 饼图	选择**顶部**或**底部**并输入构建图表所用的匹配记录数。
颜色	条形图 折线图	部分中绘制数据的颜色。

报告模板创建

报告模板是各部分的框架，每个部分通过自己的数据库查询独立构建。

您可以通过创建新模板，使用现有模板，将模板基于事件视图，或者导入控制面板或工作流程来构建新的报告模板。

如果不想复制现有报告模板，可以创建一个全新模板。创建模板的第一步是生成用于添加和格式化各部分的框架。然后，按照希望的顺序设计各个模板部分并设置报告文档的属性。

每个模板部分均包括由搜索或过滤器生成的数据集，且具有确定展现方式的格式规格（表、饼图等）。通过选择要在输出中包含的数据记录中的字段，以及要显示的时间范围和记录数量，进一步确定部分内容。

注释　使用部分预览实用程序可检查列选择和饼图颜色等输出特性。但这并不能可靠地表明配置的搜索是否正确。

从模板生成的报告具有多个覆盖所有部分和控制功能的文档属性，例如封面、页眉和页脚、页码等。

请注意，如果选择 CSV 作为文档格式，则无需设置文档属性。

如果在现有模板中找到理想模型，则可以复制模板并编辑其属性以创建新报告模板。思科还提供一组在模板列表中的**报告 (Reports)** 选项卡上可视的预定义报告模板。

从事件视图中，可以创建报告模板并将其修改为满足您的需求。可以添加更多部分、修改自动包含的部分和删除各部分。

通过导入控制面板、工作流程和统计摘要，可以快速创建新的报告。导入会为控制面板中的每个构件图形以及工作流程中的每个事件视图都创建一个部分。为重点显示最重要的信息，可以删除任何不必要的部分。

创建自定义报告模板

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板**。

步骤 3 点击 **Create Report Template**。

步骤 4 在**报告标题**字段中输入新模板的名称。

步骤 5 要向报告标题添加输入参数，请将光标置于应显示参数值的标题中，然后点击插入**输入参数**（＋）。

步骤 6 根据需要，使用“报告部分”标题栏下的一组添加来插入部分。

步骤 7 配置部分内容，如报告模板配置，第 511 页中所述。

提示　可以点击部分窗口底部的**预览 (Preview)**，查看所选择的列布局或图形格式。

步骤 8 点击**高级 (Advanced)**，设置 PDF 和 HTML 报告的属性，如报告模板中的文档属性，第 519 页中所述。

步骤 9 点击**保存 (Save)**。

如果看到一条错误，请查找每部分中结果值旁边的黄色三角形。如果看到任何此类三角形，请执行以下任一操作：

- 对于显示黄色三角形的每个字段，将鼠标指针悬停在三角形上方，并将结果数量减少到指示的数字。
- 点击**生成**，并包括 PDF 之外的输出格式。

从现有模板创建报告模板

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板**。

步骤 3 点击要复制的报告模板旁边的 **复制**（  ）。

步骤 4 在**报告标题 (Report Title)** 字段中，输入名称。

步骤 5 根据需要对模板进行更改。

步骤 6 点击**保存 (Save)**。

从事件视图创建报告模板

过程

步骤 1 在事件视图中填入要在报告中显示的事件：

- 使用事件搜索定义要查看的事件。
- 深入查找工作流程，直到在事件视图中获得相应的事件。

步骤 2 从事件视图页面中，点击 **Report Designer**。

“报告部分”(Report Sections) 页面为已捕获工作流程中的每个视图显示一个部分。

步骤 3 或者，在**报告标题 (Report Title)** 字段中输入新名称并点击**保存 (Save)**。

步骤 4 您可以执行以下操作：

- 添加封面、目录、开始页码或页眉和页脚文本 - 点击 **高级** 设置。
- 添加分页符 - 点击 **添加分页符**（  ），并将新分页符对象从模板底部拖动到应该开始新页面的那个部分的前面。
- 添加文本部分 - 点击 **添加文本部分**（  ），并将新文本部分从模板底部拖动到要在报告模板中显示的位置。
- 更改某个部分的标题 - 点击标题栏中该部分的标题，输入部分标题，然后点击**确定 (OK)**。

- 配置报告部分 - 调整每个部分中的字段设置。

  提示 要查看某一部分的当前列布局或图表格式，请点击该部分的 **Preview** 链接。

- 从报告中排除模板部分 - 点击该部分标题栏中的 **删除**（×） 并确认删除。

  注释 有些工作流程中，报告的最后部分包含显示数据包、主机配置文件或漏洞的详细视图，具体视工作流程而定。生成报告时使用这些详细视图检索大量事件，可能会影响 管理中心的性能。

步骤 5 点击**保存 (Save)**。

通过导入控制面板或工作流程创建报告模板

过程

步骤 1 确定要在报告中复制的控制面板、工作流程或摘要。

步骤 2 选择**概述** > **报告**。

步骤 3 点击 **报告模板**。

步骤 4 点击 **Create Report Template**。

步骤 5 在**报告标题 (Report Title)** 字段中输入新报告模板的名称。

步骤 6 点击**保存 (Save)**。

步骤 7 点击 **导入部分**（）。可以选择导入报告部分的数据源选项，第 511 页中所述的任何数据源。

步骤 8 从下拉菜单中选择控制面板、工作流程或摘要。

步骤 9 对要添加的数据源，点击 **Import**。

对于控制面板，每个构件图形都有自己的部分；对于工作流程，每个事件视图都有自己的部分。

步骤 10 根据需要更改各部分的内容。

注释 有些工作流程中，报告的最后部分包含显示数据包、主机配置文件或漏洞的详细视图，具体视工作流程而定。生成报告时使用这些详细视图检索大量事件，可能会影响 管理中心的性能。

步骤 11 点击**保存 (Save)**。

导入报告部分的数据源选项

表 *54:* 导入报告部分窗口上的数据源选项

选择的选项	导入内容
导入控制面板 (Import Dashboard)	所选控制面板上的任何自定义分析构件。
导入工作流程 (Import Workflow)	任何预定义或自定义的工作流程。 选项具有以下格式： `Table - Workflow name` 例如，`Connection Events - Traffic by Port` 可导入从“连接事件”(Connection Events) 表生成的“按端口划分的流量”(Traffic by Port) 工作流程中的视图。
导入摘要部分 (Import Summary Sections)	以下任意一种通用摘要： • 入侵详细摘要 • 入侵简要摘要 • 发现详细摘要 • 发现简要摘要

报告模板配置

创建报告模板后，可以进行修改和自定义。可以通过修改各种报告部分属性调整部分的内容及其数据展示。

报告模板中的各部分通过查询数据库表生成该部分的内容。更改部分的数据格式使用相同的数据查询，但会根据格式类型的分析用途修改部分中显示的字段。例如，入侵事件的表视图在部分中填入每个事件记录的大量数据字段，而饼图部分则显示各个选定属性代表的所有匹配记录的比例，不显示单个事件的详细信息。条形图部分比较具有特定属性的匹配记录总数。折线图就单个属性总结匹配记录随时间推移的变化。折线图仅适用于基于时间的数据，不适用于有关主机、用户和第三方漏洞等信息。

报告部分中的搜索或过滤器指定部分内容所基于的数据库查询。对于大多数表，可以使用预定义或保存的搜索来限定报告，也可以即时创建新的搜索：

- 预定义的搜索作为示例用于搜索特定事件表，并可以对可能想要在报告中包含的重要网络信息提供快速访问。
- 保存的事件搜索包括您或他人已创建的全部公共事件搜索，以及所有保存的私密事件搜索。
- 只有在报告模板本身中才能实现当前报告模板的保存搜索。已保存报告模板搜索的搜索名称以字符串“Custom Search”结尾。用户在设计报告时创建这些搜索。

对于“应用统计信息”(Application Statistics) 表，使用用户定义的应用过滤器限制报告。

如果在部分中包括表数据，则可以选择要显示数据记录中的哪些字段。表中所有字段都可以包括或排除。选择实现报告用途的字段，然后进行相应的排列和排序。

可以向模板添加文本部分以提供自定义文本，例如，整个报告或各部分的简介。

在模板中，可以在任何部分的前面或后面添加分页符。此功能尤其适用于多部分报告，其具有介绍各个部分的文本页面。

报告模板的时间段定义模板的报告周期。

注释 安全分析人员仅可以编辑由其创建的报告模板。在多域配置中，无法从祖先域编辑报告模板，但是可以复制以创建后代版本。

设置报告模板部分的表和数据格式

过程

步骤 1 点击**概述 (Overview)** > **报告 (Reporting)** > **报告模板 (Report Templates)** > **创建报告模板 (Create Report Template)**。

步骤 2 在报告模板部分，使用**表 (Table)** 下拉菜单选择要查询的表。

格式 字段显示适用于所选表的每个输出格式。

步骤 3 选择相关部分适用的输出格式。

步骤 4 要更改搜索限制，请点击 **搜索** 或 **过滤器** 字段旁边的 **编辑**（ ）。

步骤 5 对于图形输出格式（饼图、条形图等），请使用下拉菜单调整 **X-Axis** 和 **Y-Axis** 参数。

当为 X 轴选择值时，只有相对应的值才显示在 Y 轴下拉菜单中，反之亦然。

步骤 6 对于表输出，请在输出中选择列、显示顺序和排序顺序。

步骤 7 点击**保存 (Save)**。

相关主题

报告模板字段，第 506 页

为报告模板部分指定搜索或过滤器

过程

步骤 1 在报告模板部分中，从**表 (Table)** 下拉菜单中选择要查询的数据库表：

- 对于大多数表，显示**搜索 (Search)** 下拉列表。
- 对于“应用统计信息”(Application Statistics) 表，显示**过滤器 (Filter)** 下拉列表。

步骤 2 选择要用于限制报告的搜索或过滤器。

点击 **编辑**（）可查看搜索条件或创建新的搜索。

修改报告模板表格式部分中的字段

过程

步骤 1 对于表格式报告部分，请点击 **字段** 参数旁边的 **编辑**（） 图标。

步骤 2 如果要修改该部分，必须添加和删除字段，并将字段拖入到所需的列顺序中。

步骤 3 如果要更改任何列的排序顺序，必须使用每个行旁边的下拉列表设置排序顺序和优先级。

步骤 4 点击**确定 (OK)**。

向报告模板添加文本部分

文本部分可包含使用多种字体大小和样式（如粗体、斜体等）的富文本，以及输入参数和导入的图像。

提示 文本部分对于介绍报告或报告各部分非常有用。

过程

步骤 1 在报告模板编辑器中，点击 **添加文本部分**（）。

步骤 2 将新文本部分拖放到其在报告模板的指定位置。

步骤 3 如果要将文本部分放在页面开始或末尾，请在文本部分之前或之后添加分页符。

步骤 4 如果要更改文本部分的通用名称，请点击标题栏中的部分名称并输入新名称。

步骤 5 在文本部分的正文中添加带格式的文本和图像。

可以包括在生成报告时动态更新的输入参数。

步骤 6 点击**保存 (Save)**。

相关主题

输入参数，第 516 页

向报告模板添加分页符

过程

步骤 1 在报告模板编辑器中，点击 **添加分页符**（  ）。

分页符显示在模板的底部。

步骤 2 将分页符拖放到部分前面或后面的指定位置。

步骤 3 点击**保存 (Save)**。

全局时间窗口与报告模板部分

包含基于时间的数据的报告模板（例如，入侵或发现事件）具有全局时间窗口，默认情况下，模板中基于时间的部分创建时会继承该时间窗口。更改全局时间窗口会更改配置为继承全局时间窗口的部分的本地时间窗口。您可以通过清除**继承时间窗口 (Inherit Time Window)** 复选框来禁用单个部分的时间窗口继承。然后，您可以编辑本地时间窗口。

注释 全局时间窗口继承仅适用于具有基于时间的表数据的报告部分，例如入侵事件和发现事件。对于报告网络资产（主机和设备）和相关信息（如漏洞）的部分，必须分别设置每个时间窗口。

为报告模板及其部分设置全局时间窗口

提示 报告的每个部分可以有不同的时间范围。例如，第一部分可能是一个月度摘要，而剩余部分则可深入提供周级别的详细信息。在这些情况下，单独设置部分级别的时间窗口。

过程

步骤 1 在报告模板编辑器中，点击**生成 (Generate)**。

步骤 2 要修改全局时间段，请点击 **时间窗口** （  ）。

步骤 3 在 **事件时间窗口**中修改时间设置。

步骤 4 点击 **Apply**。

步骤 5 点击**生成 (Generate)** 以生成报告并点击**是 (Yes)** 进行确认。

为报告模板部分设置本地时间窗口

过程

步骤 1 在模板的“报告部分”页面上，清除该部分的**继承时间窗口**复选框（若有）。

步骤 2 要更改部分的本地时间段，请点击 **时间窗口** （ ）。

注释　包含统计表的数据的部分只能有滑动时间窗。

步骤 3 点击“事件时间窗口”(Events Time Window) 上的**应用 (Apply)**。

步骤 4 点击**保存 (Save)**。

重命名报告模板部分

过程

步骤 1 在报告模板编辑器中，点击部分页眉中的当前部分名称。

步骤 2 为该部分输入新名称。

步骤 3 点击**确定 (OK)**。

预览报告模板部分

预览功能显示表视图的字段布局和排序顺序以及图形的重要易读特征，如饼图颜色。

过程

步骤 1 在编辑报告模板部分时，可随时点击**预览 (Preview)** 预览该部分。

步骤 2 点击**确定 (OK)** 关闭预览。

报告模板部分中的搜索

生成成功报告的关键在于定义填入报告部分的搜索。Firepower 系统提供搜索编辑器，可查看报告模板中可用的搜索以及定义新的自定义搜索。

在报告模板部分搜索

过程

步骤 1 在报告模板的相关部分中，点击 **搜索** 字段旁边的 **编辑**（ ）。

步骤 2 如果要根据预定义搜索进行自定义搜索，必须从**已保存搜索 (Saved Searches)** 下拉列表中选择预定义搜索。

此列表包含此表格的所有可用预定义搜索，包括系统范围和报告特定的预定义搜索。

步骤 3 在相应的字段中编辑搜索条件。

对于某些字段，限制可以包含与事件搜索相同的运算符（<、<>等）。如果输入多个条件，则搜索只返回与所有条件匹配的记录。

步骤 4 如果要从下拉菜单插入输入参数，而不是输入限制值，则必须点击 **输入参数**（ ）。

注释 在编辑报告搜索的限制时，系统会使用以下名称保存已编辑的搜索：*section* custom search，其中 *section* 是部分标题栏中的名称，后跟字符串 custom search。要使保存的自定义搜索具有有意义的名称，请确保更改部分名称后再保存编辑的搜索。无法重命名已保存的报告搜索。

步骤 5 点击 **OK**。

输入参数

在报告模板中可以使用输入参数，使报告可以在生成时自动更新。 **输入参数**（ ） 指示可处理它们的字段。有两种输入参数：

- 预定义的输入参数由内部系统功能或配置信息解析。例如，在生成报告时，系统用当前日期和时间替换 $<Time> 参数。
- 用户定义的输入参数提供部分搜索限制。使用输入参数限制搜索，会指示系统在生成时从请求报告的人员那里收集值。这样，可以在生成时动态地定制报告显示特定数据子集，而无需更改模板。例如，可以为报告部分搜索的**目标 IP (Destination IP)** 字段提供输入参数。然后，当生成报告时，可以输入特定部门的 IP 网段，以仅获得该部门的数据。

  还可以定义字符串类型输入参数，在报告的以下特定区域中添加动态文本，例如，邮件（主题或正文）、报告文件名和文本部分。可以为不同部门个性化设置报告，具有自定义的报告文件名、邮件地址和邮件消息，使同一模板适用一切。

预定义输入参数

表 *55:* 预定义输入参数

插入此参数.....	.....在模板中包括此信息：
$<Logo>	所选的上传徽标

插入此参数.....	.....在模板中包括此信息：
$<Report Title>	报告标题
$<Time>	运行报告的日期和时间，精细度为一秒
$<Month>	当前月份
$<Year>	当前年份
$<System Name>	管理中心的名称
$<Model Number>	管理中心的型号
$<Time Window>	当前应用于报告部分的时间窗口
$<Constraints>	当前应用于报告部分的搜索限制

表 *56*: 预定义输入参数的使用

参数	报告模板封面	报告模板报告标题	报告模板部分说明	报告模板文本部分	生成报告文件名	生成报告邮件主题、正文
$<Logo>	是	否	否	否	否	否
$<Report Title>	是	否	是	是	是	是
$<Time>	是	是	是	是	是	是
$<Month>	是	是	是	是	是	是
$<Year>	是	是	是	是	是	是
$<System Name>	是	是	是	是	是	是
$<Model Number>	是	是	是	是	是	是
$<Time Window>	否	否	是	否	否	否
$<Constraints>	否	否	是	否	否	否

用户定义的输入参数

使用输入参数可扩展搜索的实用性。输入参数指示系统在生成时从请求报告的人员那里收集值。这样，可以在生成时动态地限制报告显示特定数据子集，而无需更改搜索。例如，可以为深度提供部门级安全事件的报告部分的**目标 IP (Destination IP)** 字段提供输入参数。当生成报告时，可以输入特定部门的 IP 网段，以仅获得该部门的数据。

输入参数的类型确定可以使用其的搜索字段。只能在相应的字段中使用指定类型。例如，定义为字符串类型的用户参数可插入文本字段，但不可插入接受 IP 地址的字段。

定义的每个输入参数均具有名称和类型。

表 57: 用户定义的输入参数类型

将此参数类型.....	用于包含此数据的字段.....
网络/IP (Network/IP)	CIDR 格式的任何 IP 地址或网段
应用	应用协议、客户端应用或 Web 应用的名称
事件消息 (Event Message)	任何事件视图消息
设备	管理中心 或受管设备
用户名	用户身份，比如发起方用户和响应方用户
编号 (Number)（VLAN ID、Snort ID、Vuln ID）	任何 VLAN ID、Snort ID 或漏洞 ID
字符串	文本字段（如应用或操作系统版本、注释或说明）

创建用户定义的输入参数

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击 **添加输入参数**（＋）。

步骤 3 输入参数**名称 (Name)**。

步骤 4 从**类型 (Type)** 下拉列表中选择值。

步骤 5 点击**确定 (OK)** 添加参数。

步骤 6 点击**确定 (OK)** 返回到编辑器。

编辑用户定义的输入参数

报告模板的**输入参数 (Input Parameters)** 部分列出模板的所有可用用户定义参数。

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击要修改的参数旁边的 **编辑**（✎） 。

步骤 3 在**名称 (Name)** 中输入新名称。

步骤 4 使用**类型 (Type)** 下拉列表来更改参数类型。

步骤 5 点击 **OK**，保存更改。

步骤 6 如果要删除输入参数，请点击输入参数旁边的 **删除**（ ） 并确认。

步骤 7 点击**确定 (OK)** 返回到报告模板编辑器。

使用用户定义的输入参数限制搜索

定义的输入参数仅适用于与其参数类型匹配的搜索字段。例如，**网络/IP (Network/IP)** 类型的参数仅适用于接受 CIDR 格式的 IP 地址或网段的字段。

过程

步骤 1 在报告模板编辑器中，点击该部分中 **搜索** 字段旁边 **编辑**（ ）。

可接受输入参数的字段标有 **输入参数**（ ）。

步骤 2 点击字段旁边的 **输入参数**（ ），然后从下拉菜单中选择输入参数。

用户定义的输入参数标有 ( )。

步骤 3 点击**确定 (OK)**。

报告模板中的文档属性

在生成报告之前，可以设置影响报告外观的文档属性。这些属性包括可选封面和目录。对一些属性是否支持取决于所选的报告格式：PDF、HTML 或 CSV。

表 *58:* 文档属性支持

属性	是否支持 **PDF**?	是否支持 **HTML**?	是否支持 **CSV**?
封面页	是，具有可选徽标和自定义外观	是，具有可选徽标和自定义外观	否
目录	是	是	否
页眉和页脚	是，在任意字段中均具有可选文本或徽标	否	否
自定义开始页码	是	否	否
不显示首页页码的选项	是	否	否

编辑报告模板中的文档属性

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 有以下选项可供选择：

- 添加封面 - 要添加封面，请选中**包含封面 (Include Cover Page)** 复选框。
- 自定义封面 - 要编辑封面设计，请参阅自定义封面，第 520 页。
- 添加目录 - 要添加目录，请选中**包含目录 (Include Table of Contents)** 复选框。
- 管理徽标 - 要管理与模板关联的徽标图像，请参阅管理报告模板徽标，第 520 页。
- 配置页眉和页脚 - 要指定此模板的页眉和页脚的元素，请使用**页眉 (Header)** 和**页脚 (Footer)** 字段中的下拉列表。
- 设置首页码 - 要指定报告首页的页码，请输入**页码开始 (Page Number Start)** 值。
- 显示首页码 - 要显示报告首页的页码，请选中**对首页编号？(Number First Page?)** 复选框。如果选择此选项，则封面未编号。

步骤 3 点击**确定 (OK)**，保存更改。

自定义封面

可以自定义报告模板的封面。封面可包含使用多种字体大小和样式（如粗体、斜体等）的富文本，以及输入参数和导入的图像。

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击 **覆盖页面设计**旁边的 **编辑**（ ）。

步骤 3 在富文本编辑器中编辑封面设计。

步骤 4 点击**确定 (OK)**。

管理报告模板徽标

可以在 管理中心上存储多个徽标，并将其与其他报告模板关联。在设计模板时设置徽标关联。如果导出模板，导出包会包含徽标。

将徽标上传到 管理中心时，该徽标可用于：

- 管理中心上的所有报告模板，或
- 在多域部署中，当前域中的所有报告模板

徽标图像可为 GIF、JPG 或 PNG 格式。

可以将报告中的徽标更改为上传到 管理中心的任何 JPG 图像。例如，如果重复使用模板，可以将另一个公司的徽标与报告关联。

可以删除任何已上传的徽标。删除徽标会将其从使用它的所有模板中都删除。删除操作无法撤消。请注意，不能删除预定义思科徽标。

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

当前与模板相关联的徽标显示在 **General Settings** 中的 **Logo** 下。

步骤 2 点击徽标旁边的 **编辑**（ ）。

步骤 3 有以下选项可供选择：

- 添加 - 添加新徽标，如添加新徽标，第 521 页中所述。
- 更改 - 更改报告模板的徽标，如更改报告模板的徽标，第 521 页中所述。
- 删除 - 删除徽标，如删除徽标，第 522 页中所述。

添加新徽标

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击 **徽标** 字段旁边的 **编辑**（ ）。

步骤 3 点击 **Upload Logo**。

步骤 4 点击 **浏览**，浏览至文件的位置，然后点击 **打开**。

步骤 5 点击**上传**。

步骤 6 如果要将新徽标与当前模板关联，请选择当前模板，然后点击**确定 (OK)**。

更改报告模板的徽标

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击 **徽标** 字段旁边的 **编辑**（ ）。

步骤 3 从“选择徽标”(Select Logo) 对话框中，选择要与报告模板关联的徽标。

步骤 4 点击**确定 (OK)**。

删除徽标

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击 **徽标** 字段旁边的 **编辑**（ ）。

步骤 3 从“选择徽标”(Select Logo) 对话框中，选择要删除的徽标。

步骤 4 点击 **Delete Logo**。

步骤 5 点击**确定 (OK)**。

管理报告模板

在多域部署中，系统会显示在当前域中创建的报告模板，您可以对其进行编辑。系统还会显示在祖先域中创建的报告模板，您不可以对其进行编辑。要查看和编辑在较低域中创建的报告模板，请切换至该域。系统仅显示在当前域中创建的报告。

您必须是管理员用户才能执行此任务。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板**。

步骤 3 有以下选项可供选择：

- 删除 - 在要删除的模板旁边，点击 **删除**（ ） 并确认。

  不能删除系统提供的报告模板。安全分析人员仅可删除由其创建的报告模板。在多域部署中，仅可以删除属于当前域的报告模板。

- 编辑 - 要编辑报告模板，请参阅编辑报告模板， 第 522 页。
- 导出 - 要导出报告模板，请参阅导出报告模板， 第 523 页。

  提示 也可以使用标准配置导出过程导出报告模板；请参阅导出配置， 第 489 页。

- 导入 - 要导入报告模板，请参阅导入配置， 第 490 页。

编辑报告模板

在多域部署中，系统会显示在当前域中创建的报告模板，您可以对其进行编辑。系统还会显示在祖先域中创建的报告模板，您不可以对其进行编辑。要查看和编辑在较低域中创建的报告模板，请切换至该域。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板**。

步骤 3 点击要编辑的模板的 **编辑**（ ）。

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

步骤 4 有以下选项可供选择：

- 添加分页符；请参阅向报告模板添加分页符，第 514 页。
- 添加文本部分；请参阅向报告模板添加文本部分，第 513 页。
- 配置部分内容，如报告模板配置，第 511 页中所述。
- 创建输入参数；请参阅创建用户定义的输入参数，第 518 页。
- 编辑输入参数；请参阅编辑用户定义的输入参数，第 518 页。
- 编辑文档属性；请参阅编辑报告模板中的文档属性，第 520 页。
- 搜索模板部分；请参阅在报告模板部分搜索，第 516 页。
- 通过点击**高级 (Advanced)** 来设置文档属性，如报告模板中的文档属性，第 519 页中所述。
- 设置全局时间窗口；请参阅为报告模板及其部分设置全局时间窗口，第 514 页。
- 设置本地时间窗口；请参阅为报告模板部分设置本地时间窗口，第 515 页。
- 设置搜索字段；请参阅修改报告模板表格式部分中的字段，第 513 页。
- 设置表和数据格式；请参阅设置报告模板部分的表和数据格式，第 512 页。
- 指定搜索和过滤器；请参阅为报告模板部分指定搜索或过滤器，第 512 页。

导出报告模板

您必须是管理员用户才能执行此任务。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 选择 **报告模板**。

步骤 3 点击要导出的模板的 **导出** 图标。

关于生成报告

生成报告

创建并自定义报告模板后，便可生成报告了。在生成过程中，可以选择报告格式（HTML、PDF 或 CSV）。还可以调整报告的全局时间段，它对所有部分应用一致的时间范围，但您排除的时间范围除外。

PDF 报告：

- 不支持使用 Unicode (UTF-8) 字符的文件名。
- 包含特殊 Unicode 文件名（例如，文件或恶意活动中显示的那些文件名）的任何报告部分将以转换形式显示这些文件名。
- 在每个报告部分配置的结果数必须接受某些限制。要查看这些限制，请将鼠标指针移至报告模板中显示的任意黄色三角形上。

如果报告模板的搜索规格中包括用户输入参数，生成过程会提示输入值，将报告的这次运行定制为数据的一个子集。

如已配置 DNS 服务器且启用 IP 地址解析，则当解析成功时，报告包含主机名。

在多域部署中，如果在祖先域中生成报告，该报告可包括来自所有后代域的结果。要为特定叶域生成报告，请切换至该域。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板**。

步骤 3 点击要用于生成报告的模板旁边的 **报告**（ ）。

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。

提示 要从祖先模板生成报告，请将该模板复制到当前域。

步骤 4 或者，也可以配置报告名称：

- 输入新的**文件名 (File Name)**。如果不输入新名称，系统将使用报告模板中指定的名称。
- 使用 **输入参数**（ ）向文件名添加一个或多个输入参数。

步骤 5 通过点击，选择报告的输出格式：HTML、PDF 或 CSV。

如果 PDF 选项显示为灰色，说明在一个或多个报告部分中配置的结果数量可能太高。有关特定限制，请查找报告模板中的黄色三角形并将鼠标指针悬停在所查找的任意黄色三角形上。

步骤 6 如果要更改全局时间段，请点击 **时间窗口** （ ）。

注释 只有当单个报告部分配置为继承全局设置时，设置全局时间段才会影响单个报告的内容。

步骤 7 为**输入参数 (Input Parameters)** 部分中显示的任何字段输入值。

提示 通过在字段中键入 * 通配符，可以忽略用户参数。这会消除对搜索的用户参数限制。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址或 VLAN 标记限制报告结果可能会出现意外结果。

步骤 8 如果在 管理中心配置中启用了邮件中继主机，点击**邮件**可在报告生成时自动通过邮件传送报告。

步骤 9 点击**生成**，并在显示提示时进行确认。

点击**生成**会保存报告模板的“生成”设置。

如果点击**关闭**，仅会在会话持续期间保存您所做的选择。

步骤 10 有以下选项可供选择：

- 点击报告链接以在新窗口中显示该报告。
- 点击**确定 (OK)** 返回到报告模板编辑器。

报告生成选项

可以配置报告生成选项来执行以下操作：

- 安排生成未来报告，可以是一次报告也可以是循环报告。请参阅自动执行报告生成，第 474 页。可以在每日、每周和每月等全程时间范围上自定义计划。
- 使用调度程序分发邮件报告。必须在计划任务**之前**配置报告模板和邮件中继主机。
- 当生成报告时，将报告作为邮件附件自动发送到收件人列表。必须具有适当配置的邮件中继主机，才能通过邮件传送报告。
- 将新生成的报告文件保存到所配置的远程存储位置。要使用远程存储，必须先配置远程存储位置。

注释 如果在远程存储后又切换回本地存储，则远程存储中的报告不在“报告”(Reports) 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

在生成时通过邮件分发报告

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板**。

步骤 3 点击要用于生成报告的模板旁边的 **报告**（ ）。

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。

提示 要从祖先模板生成报告，请将该模板复制到当前域。

步骤 4 展开窗口的**邮件 (Email)** 部分。

步骤 5 在**邮件选项 (Email Options)** 字段中，选择**发送邮件 (Send Email)**。

步骤 6 在**收件人列表 (Recipient List)**、**CC** 和 **BCC** 字段中，输入逗号分隔列表形式的收件人邮箱地址。

步骤 7 在**主题 (Subject)**字段中，输入邮件主题。

提示 可以在**主题 (Subject)** 和邮件正文中提供输入参数，以动态生成邮件中的信息，例如时间戳或管理中心名称。

步骤 8 根据需要在邮件正文中输入附函。

步骤 9 点击**确定 (OK)** 并确认。

相关主题

配置邮件中继主机和通知地址，第 58 页

安排未来报告

请参阅自动执行报告生成，第 474 页。

关于使用生成的报告

在“报告”(Reports) 选项卡页面上访问和使用之前生成的报告。

查看报告

“报告”列出所有以前生成的报告，提供报告名称、生成日期和时间、生成用户以及报告是在本地还是远程存储的信息。状态栏指示报告是已生成，处于生成队列中（例如，对于计划任务）还是无法生成（例如，由于磁盘空间不足）。

请注意，具有管理员访问权限的用户可以查看所有报告；其他用户只能查看自己所生成的报告。

在多域部署中，只能查看在当前域中生成的报告。

“报告”页面显示所有本地存储的报告。如果当前配置了远程存储，该页面也显示远程存储的报告。远程存储的报告的**位置 (Location)** 列数据为 `Remote`。

注释 如果在远程存储后又切换回本地存储，则远程存储中的报告不在“报告”(Reports) 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

过程

步骤 1 选择概述 > 报告。

步骤 2 点击 报告。

步骤 3 点击要查看的报告。

下载报告

可以将任何报告文件下载到本地计算机。由此，可以通过邮件发送报告，或者通过其他可用的手段以电子方式分发。

在多域部署中，只能下载在当前域中生成的报告。

过程

步骤 1 选择概述 > 报告。

步骤 2 点击 报告。

步骤 3 选中要下载的报告旁边的复选框，然后点击下载 **(Download)**。

提示 点击页面左上方的复选框以下载页面上的所有报告。如果有多个报告页面，则系统会再显示一个复选框，可以点击该复选框以下载所有页面上的所有报告。

步骤 4 根据浏览器提示下载报告。如果选择多个报告，则以单个 `.zip` 文件形式对其进行下载。

远程存储报告

当前配置的报告存储位置显示在“概述”(Overview) >“报告”(Reporting) >“报告”(Reports) 页面的底部，提供本地、NFS 和 SMB 存储的磁盘使用率。如果使用 SSH 访问远程存储，则不提供磁盘使用量的数据。

注释 如果在远程存储后又切换回本地存储，则远程存储中的报告不在“报告”(Reports) 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

开始之前

- 配置远程存储位置，如 远程存储设备，第 92 页中所述。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 选择 **报告**。

步骤 3 选中页面底部的**启用报告的远程存储 (Enable Remote Storage of Reports)** 复选框。

下一步做什么

- 将报告从本地存储移至远程存储；请参阅将报告移至远程存储器，第 528 页。

相关主题

远程存储设备，第 92 页
将报告移至远程存储器，第 528 页

将报告移至远程存储器

可以按批量处理模式或单个地将本地存储的报告转移到远程存储位置。

注释 如果在远程存储后又切换回本地存储，则远程存储中的报告不在“报告”(Reports) 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

开始之前

- 配置远程存储位置，如远程存储设备，第 92 页中所述。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 选择 **报告**。

步骤 3 选中要移动的报告旁边的复选框，然后点击**移动 (Move)**。

提示 选中页面左上方的复选框以移动页面上的所有报告。如果报告有多页，则会再显示一个复选框，可以选中该复选框来移动所有页面上的全部报告。

步骤 4 确认要转移报告。

删除报告

可以随时删除报告文件。此步骤会完全删除文件，并且无法恢复。尽管仍然有生成了报告的报告模板，但如果时间段已扩展或滑动，就可能难以重新生成特定报告文件。如果模板使用输入参数，重新生成可能也很困难。

在多域部署中，只能删除在当前域中生成的报告。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告**。

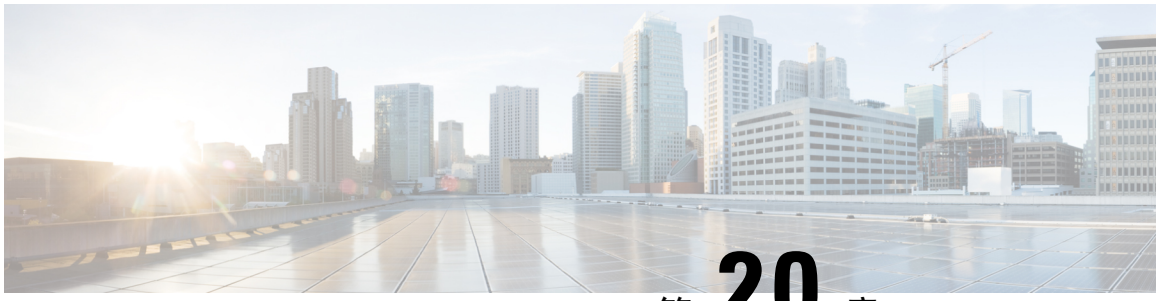
步骤 3 有以下选项可供选择：

- 删除所选项 - 选中要删除的报告旁边的复选框，然后点击**删除 (Delete)**。
- 删除所有 - 选中页面左上方的复选框以删除页面上的所有报告。如果报告有多页，则会再显示一个复选框，可以选中该复选框来删除所有页面上的全部报告。

步骤 4 确认删除。

报告历史记录

功能	最低 管理中心	最低 威胁防御	详情
在报告模板中选择连接事件的数据源	7.0	任意	如果使用向导配置远程数据存储时使用 安全分析和日志记录（本地部署），则可以选择在报告中包含存储在该卷上的数据。 修改的页面：报告模板
漏洞报告的更改	6.7	任意	报告输出已根据 Bugtraq 数据的可用性进行了调整。



第 20 章

含警报响应的外部警报

以下主题介绍如何使用警报响应从 Cisco Secure Firewall Management Center发送外部事件警报：

Cisco Secure Firewall Management Center 警报响应

通过 SNMP、系统日志或邮件发送外部事件通知有助于重要系统监控。Cisco Secure Firewall Management Center使用可配置的警报响应与外部服务器交互。警报响应是一种配置，用于表示与电子邮件、SNMP 或系统日志服务器的连接。它们称为响应的原因在于，可将它们用于发送警报，以响应由 Firepower 检测到的事件。可以配置多个警报响应，以便向不同的监控服务器和/或人员发送不同类型的警报。

注释 根据您的设备和 Firepower 版本，警报响应可能不是发送系统日志消息的最佳方式。请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 关于系统日志和 配置安全事件系统日志消息的最佳实践， 第 610 页。。

注释 使用警报响应的警报是由 Cisco Secure Firewall Management Center发送的。不使用警报响应的入侵电子邮件警报也是由 Cisco Secure Firewall Management Center发送的。相比之下，基于单个入侵规则触发的 SNMP 和 系统日志警报是由受管设备直接发送的。有关详细信息，请参阅入侵事件的外部警报， 第 541 页。

在大多数情况下，外部警报中的信息与您记录到数据库中的任何相关联事件中的信息相同。但是，无论是何种基础事件类型，对于关联规则中包含连接跟踪器的关联事件警报，您收到的信息都与流量量变曲线更改警报相同。

可在“警报”页面（**策略** > **操作** > **警报**）上创建和管理警报响应。新的警报响应自动启用。要暂停警报生成，可以禁用警报响应，而非将它们删除。

对警报响应所做的更改会立即生效，但将连接日志发送到 SNMP 陷阱或系统日志服务器时除外。

支持警报响应的配置

创建警报响应后，可以使用它从 Cisco Secure Firewall Management Center发送以下外部警报。

警报/事件类型	有关详细信息，请参阅
按影响标志划分的入侵事件	配置影响标志警报， 第 537 页
按类型划分的发现事件	配置发现事件警报， 第 538 页
由 恶意软件防护 检测到的恶意软件和追溯性恶意软件事件（“基于网络”）	配置 恶意软件防护警报， 第 539 页
按关联策略违规划分的关联事件	将响应添加到规则和允许名单， 第 941 页
按日志记录规则或默认操作（不支持邮件警报）划分的连接事件	您可以记录的其他连接， 第 700 页
按运行状况模块和严重性级别划分的运行状况事件	创建运行状况监控器警报， 第 365 页

警报报告的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员

创建 SNMP 警报响应

对于除了 威胁防御的设备类型，可使用 SNMPv1、SNMPv2 或 SNMPv3 创建 SNMP 警报响应。

注释 为 SNMP 协议选择 SNMP 版本时，请注意 SNMPv2 仅支持只读社区，SNMPv3 仅支持只读用户。此外，SNMPv3 还支持使用 AES128 加密。

如果想要使用 SNMP 监控 64 位值，则必须使用 SNMPv2 或 SNMPv3。SNMPv1 不支持 64 位监控。

开始之前

- 如果网络管理系统需要 Cisco Secure Firewall Management Center的管理信息库 (MIB) 文件，则可在 `/etc/sf/DCEALERT.MIB` 处获取该文件。

过程

步骤 1 选择**策略** > **操作** > **警报**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建 SNMP 警报 (Create SNMP Alert)**。

步骤 3 编辑 SNMP 警报配置字段：

a) **名称**-输入名称以指定 SNMP 响应。

b) **陷阱服务器**-输入 SNMP 陷阱服务器的主机名或 IP 地址。

注释 如果在此字段中输入了无效的 IPv4 地址（例如 192.169.1.456），则系统**不会**发出警告。相反，无效地址会被视为主机名。

c) **版本**-从下拉列表中，选择要使用的 SNMP 版本。SNMPv3 是默认设置。

选项包括：

- **SNMPv1** 或 **SNMPv2**：在 **社区字符串** 字段中输入只读 SNMP 社区名称，然后跳至程序末尾。

  注释 不包含特殊字符 (< > / % # & ? ' 等）在 SNMP 社区字符串名称中。

- 对于 **SNMP v3**：在 **用户名** 字段中，输入要使用 SNMP 服务器对其进行身份验证的用户的名称并继续下一步。

d) **身份验证协议**-从下拉列表中选择要用于身份验证的协议。

选项包括：

- **MD5**- 消息摘要 5 (MD5) 散列功能。
- **SHA**—安全散列算法 (SHA) 散列函数。

e) **身份验证密码**-输入用于身份验证的密码。

f) **隐私协议**－从下拉列表中选择要用于加密私有密码的协议。

选项包括：

- **DES**-在对称密钥块算法中使用 56 位密钥的数据加密标准 (DES)。
- **AES**-在对称密码算法中使用 56 位密钥的高级加密标准 (AES)。
- **AES128**-在对称密码算法中使用 128 位密钥的 AES。密钥越长，其提供的安全性就越高，但性能会随之降低。

g) **隐私密码**-输入 SNMP 服务器所需的隐私密码。如果指定私有密码，则隐私被启用，且还必须指定身份验证密码。

h) **引擎 ID**-使用偶数数字（十六进制表示法）输入 SNMP 引擎的标识符。

使用 SNMPv3 时，系统使用引擎 ID 值对消息进行编码。SNMP 服务器需要使用该值对消息进行解码。

思科建议您使用十六进制版本的 Cisco Secure Firewall Management Center的 IP 地址。例如，如果 Cisco Secure Firewall Management Center 的 IP 地址为 10.1.1.77，请使用 0a01014D0。

步骤 4 点击**保存 (Save)**。

下一步做什么

更改会立即生效，但以下情况除外：

如果你使用警报响应来发送连接日志，你必须在编辑这些警报响应后部署配置更改。

创建系统日志警报响应

配置系统警报响应时，可指定与系统日志消息相关联的严重性和消息来源，以确保它们得到系统日志服务器的正确处理。消息来源指明创建消息的子系统，严重性界定消息的严重性。消息来源和严重性不显示在系统日志中的实际消息中，而是告知接收系统日志消息的系统如何对消息进行归类。

提示 有关系统日志如何运行及如何对其进行配置的更多详细信息，请参阅系统文档。在 UNIX 系统上，`syslog` 和 `syslog.conf` 的 `man` 页面提供了概念信息和配置说明。

虽然在创建系统日志警报响应时可选择任何类型的设施，但是应根据系统日志服务器选择合适的设施；并非所有系统日志服务器都支持所有设施。对于 UNIX 系统日志服务器，`syslog.conf` 文件应指示哪些设备保存到了服务器的哪些日志文件上。

开始之前

- 在许多情况下，不建议使用此程序发送系统日志消息。

- 确认系统日志服务器可接受远程消息。

过程

步骤 1 选择**策略** > **操作** > **警报**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建系统日志警报 (Create Syslog Alert)**。

步骤 3 输入警报的**名称 (Name)**。

步骤 4 在**主机 (Host)** 字段中，输入系统日志服务器的主机名或 IP 地址。

注释 如在此字段中输入了无效的 IPv4 地址（例如 192.168.1.456），则系统**不会**发出警告。相反，无效地址会被视为主机名。

步骤 5 在**端口 (Port)** 字段中，输入服务器用于系统日志消息的端口。默认情况下，此值为 514。

步骤 6 从**设施 (Facility)** 列表中，选择系统日志警报设施，第 535 页中所述的设施。

步骤 7 从**严重性 (Severity)** 列表中，选择系统日志严重性级别，第 536 页中所述的严重性。

步骤 8 在**标记 (Tag)** 字段中，输入要与系统日志消息一起显示的标记名称。

例如，如果要在发送到系统日志的所有消息前加上 `FromMC`，请在字段中输入 `FromMC`。

步骤 9 点击**保存 (Save)**。

下一步做什么

更改会立即生效，但以下情况除外：

如果你使用警报响应来发送连接日志到系统日志服务器，你必须在编辑这些警报响应后部署配置更改。

如果您将此警报响应用于安全事件，则必须在策略中指定此警报响应。请参阅安全事件系统日志的配置位置，第 615 页。

系统日志警报设施

下表列出了可选择的系统日志设施。

表 *59:* 可用的系统日志设施

设施	说明
AUTH	与安全和授权关联的消息。
AUTHPRIV	与安全和授权关联的访问受限的消息。在很多系统上，这些消息会转发至一个安全文件。
控制台	警报消息。

设施	说明
CRON	时钟守护程序生成的消息。 请注意，运行 Linux 操作系统的系统日志服务器将使用 CRON 消息来源。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
邮件	邮件系统生成的消息。
NEWS	网络新闻子系统生成的消息。
NTP	NTP 守护程序生成的消息。
安全	审核子系统生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
SOLARIS-CRON	时钟后台守护程序生成的消息。 请注意，运行 Windows 操作系统的系统日志服务器将使用 CLOCK 消息来源。
USER	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

系统日志严重性级别

下表列出可选择的标准系统日志严重性级别。

表 *60:* 系统日志严重性级别

级别	说明
ALERT	应立即更正的状况。
CRIT	临界状况。
DEBUG	包含调试信息的消息。
EMERG	向所有用户广播的紧急状况。
ERR	错误状况。

级别	说明
INFO	参考性消息。
通知	需要注意但非错误的状况。
警告	警告消息。

创建邮件警报响应

开始之前

- 确认 Cisco Secure Firewall Management Center可反向解析其自身的 IP 地址。
- 配置邮件中继主机，如配置邮件中继主机和通知地址，第 58 页中所述。

注释 不可以使用邮件警报记录连接。

过程

步骤 1 选择**策略 > 操作 > 警报**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建邮件警报 (Create Email Alert)**。

步骤 3 为警报响应输入**名称 (Name)**。

步骤 4 在**收件人 (To)** 字段中，输入要将警报发送到其中的邮箱地址（用逗号分隔）。

步骤 5 在**发件人 (From)** 字段中，输入要显示为警报发件人的邮箱地址。

步骤 6 在 **Relay Host** 旁，验证列出的邮件服务器是要用于发送警报的服务器。

提示 要更改电邮服务器，请点击 **编辑**（）。

步骤 7 点击**保存 (Save)**。

配置影响标志警报

可将系统配置为只要出现带有特定影响标志的入侵事件就会发出警报。影响标志可通过将入侵数据、网络发现数据和漏洞信息相关联来帮助评估入侵对网络的影响。

您必须具有 IPS 智能许可证或保护经典许可证才能配置这些警报。

过程

步骤 1 选择策略 > 操作 > 警报。

步骤 2 点击 影响标志警报。

步骤 3 在警报 (Alerts) 部分中，选择要用于每种警报类型的警报响应。

提示 要创建新警报响应，请从任何下拉列表中选择新建 (New)。

步骤 4 在影响配置 (Impact Configuration) 部分中，选中相应复选框为每个影响标志指定要接收的警报。

有关影响标志的定义，请参阅入侵事件影响级别，第 763 页。

步骤 5 点击保存 (Save)。

配置发现事件警报

可将系统配置为只要出现特定类型的发现事件就会发出警报。

开始之前

- 将网络发现策略配置为记录要为其配置警报的发现事件类型，如《Cisco Secure Firewall Management Center 设备配置指南》中 网络发现策略 中所述

过程

步骤 1 选择策略 > 操作 > 警报。

步骤 2 点击 发现事件警报 (Discovery Event Alerts)。

步骤 3 在警报 (Alerts) 部分中，选择要用于每种警报类型的警报响应。

提示 要创建新警报响应，请从任何下拉列表中选择新建 (New)。

步骤 4 在事件配置 (Events Configuration) 部分中，选中与要为每种发现事件类型接收的警报对应的复选框。

步骤 5 点击保存 (Save)。

配置 恶意软件防护警报

可将系统配置为只要 恶意软件防护 生成任何恶意软件事件（包括回溯性事件）（即，生成“基于网络的恶意软件事件”），就向您发出警报。不能对面向终端的AMP生成的恶意软件事件（“基于终端的恶意软件事件”）发出警报。

开始之前

- 配置文件策略以执行恶意软件云查找并将该策略与访问控制规则相关联，。 有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的访问控制概述。
- 您必须具有 恶意软件防御 许可证才能配置这些警报。

过程

步骤 1 选择**策略 > 操作 > 警报**。

步骤 2 点击 **高级恶意软件防护警报**。

步骤 3 在**警报 (Alerts)** 部分中，选择要用于每种警报类型的警报响应。

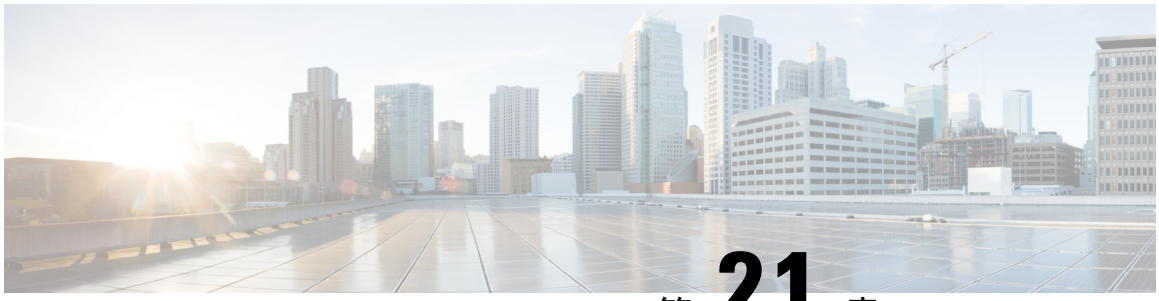
提示 要创建新警报响应，请从任何下拉列表中选择**新建 (New)**。

步骤 4 在**事件配置 (Event Configuration)** 部分中，选中与要为每种恶意软件事件类型接收的警报对应的复选框。

请注意，**所有基于网络的恶意软件事件 (All network-based malware events)** 包括**追溯性事件 (Retrospective Events)**。

（根据定义，基于网络的恶意软件事件不包括由面向终端的 AMP 生成的事件。）

步骤 5 点击**保存 (Save)**。



第 21 章

入侵事件的外部警报

以下主题介绍如何配置入侵事件的外部警报：

关于入侵规则的外部警报

外部入侵事件通知可帮助进行关键系统监控：

- SNMP - 按照入侵策略配置并从受管设备发送。您可以按照入侵规则启用 SNMP 警报。
- 系统日志 - 按照入侵策略配置并从受管设备发送。当您在入侵策略中启用系统日志警报时，可以为该策略中的每个规则将其打开。
- 邮件 - 跨所有入侵策略配置并从 Cisco Secure Firewall Management Center发送。您可以按照入侵规则启用邮件警报，并限制警报的长度和频率。

请记住，如果您配置了入侵事件抑制或阈值，系统可能不会每次在规则触发时都生成入侵事件（因此可能不会发送警报）。

注释 Cisco Secure Firewall Management Center还使用 SNMP、系统日志和邮件警报响应来发送不同类型的外部警报；请参阅Cisco Secure Firewall Management Center 警报响应，第 531 页。系统不使用警报响应来根据单个入侵事件发送警报。

相关主题

入侵策略中的入侵事件通知过滤器

入侵事件外部警报的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵事件外部警报的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

配置入侵事件的 SNMP 警报

在入侵策略中启用外部 SNMP 警报后，可以配置各个规则以便在触发规则时发送 SNMP 警报。这些警报是从受管设备发送的。

过程

步骤 1 在入侵策略编辑器的导航窗格中，点击**高级设置**。

步骤 2 确保 **SNMP 警报**是**已启用**状态，然后点击**编辑**。
页面底部消息会识别包含配置的入侵策略层。

步骤 3 选择 **SNMP 版本**，然后按入侵 SNMP 警报选项，第 543 页中所述指定配置选项。

步骤 4 在导航窗格中，点击**规则**。

步骤 5 在规则窗格中，选择要设置 SNMP 警报的规则，然后选择**警报** > **添加 SNMP 警报**。

步骤 6 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

入侵 SNMP 警报选项

如果网络管理系统要求使用管理信息库文件 (MIB)，您可以从Cisco Secure Firewall Management Center 中获取，具体位置为 `/etc/sf/DCEALERT.MIB`。

SNMP v2 选项

选项	说明
陷阱类型	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则选择**二进制形式**选项。否则，应选择**字符串形式**。例如，HP Openview 需要选择**字符串形式**。
陷阱服务器 (Trap Server)	收到 SNMP 陷阱通知的服务器。 可指定单一 IP 地址或主机名。
社区字符串 (Community String)	群体名称。

SNMP v3 选项

受管设备使用引擎 ID 值对 SNMPv3 警报进行编码。要解码警报，您的 SNMP 服务器需要此值，即发送设备的管理接口 IP 地址的十六进制版本，并附加“01”。

例如，如果发送 SNMP 警报的设备的管理接口 IP 地址是 172.16.1.50，则引擎 ID 值为 0xAC10013201。

选项	说明
陷阱类型	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则选择**二进制形式**选项。否则，应选择**字符串形式**。例如，HP Openview 需要选择**字符串形式**。
陷阱服务器 (Trap Server)	收到 SNMP 陷阱通知的服务器。 可指定单一 IP 地址或主机名。

选项	说明
身份验证密码 (Authentication Password)	身份验证所需的密码。SNMP v3 使用消息摘要 5 (MD5) 散列函数或安全散列算法 (SHA) 散列函数进行密码加密，具体取决于配置。 一旦指定身份验证密码，身份验证即可启用。
私有密码 (Private Password)	用于保护隐私的 SNMP 密钥。SNMP v3 采用数据加密标准 (DES) 分组密码对密码进行加密。输入 SNMP v3 密码后，初始配置期间的密码会以明文显示，但以加密格式保存。 如果指定私有密码，则隐私被启用，且还必须指定身份验证密码。
用户名	SNMP 用户名。

为入侵事件配置系统日志警报

在入侵策略中启用系统日志警报后，系统将在受管设备自身或者一台或多台外部主机上向系统日志发送所有入侵事件。如果指定了外部主机，系统将从受管设备发送系统日志警报。

过程

步骤 1 在入侵策略编辑器的导航窗格中，点击**高级设置 (Advanced Settings)**。

步骤 2 请确保**系统日志警报 (Syslog Alerting)** 为**已启用 (Enabled)**，然后点击**编辑 (Edit)**。
页面底部消息会识别包含配置的入侵策略层。**系统日志警报**页面添加在**高级设置**下。

步骤 3 输入您要发送系统日志警报的**日志记录主机**的 IP 地址。

如果您将**日志记录主机**字段留空，则系统将从关联访问控制策略中的“日志记录”获取日志记录主机详细信息。

步骤 4 选择**设施**和**严重性**级别，如入侵系统日志警报的设施和严重性，第 545 页中所述。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

入侵系统日志警报的设施和严重性

受管设备可以使用特定的设施和**严重性**将入侵事件作为系统日志警报发送，以便日志主机可以对警报进行分类。设施指定生成警报的子系统。这些设施和**严重性**值不会出现在实际的系统日志消息中。

根据您的环境选择有意义的值。本地配置文件（如基于 UNIX 的日志记录主机上的 syslog.conf）可能指示将哪些设施保存到哪些日志文件中。

系统日志警报设施

设施	说明
AUTH	与安全和授权关联的消息。
AUTHPRIV	与安全和授权关联的访问受限的消息。在很多系统上，这些消息会转发至一个安全文件。
控制台	警报消息。
CRON	时钟守护程序生成的消息。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
邮件	邮件系统生成的消息。
NEWS	网络新闻子系统生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
USER	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

系统日志警报严重性

级别	说明
EMERG	紧急状况，向所有用户广播
ALERT	需要立即更正的状况
CRIT	严重的状况

级别	说明
ERR	错误状况
WARNING	警告消息
通知	并未出现错误，但需引起注意的状况
INFO	参考性消息
DEBUG	包含调试信息的消息

配置入侵事件的邮件警报

如果启用了入侵邮件警报，无论哪个受管设备或入侵策略检测到入侵，系统都可以在生成入侵事件时发送邮件。这些警报从 Cisco Secure Firewall Management Center发送。

开始之前

- 配置邮件主机以接收邮件警报；请参阅配置邮件中继主机和通知地址，第 58 页。
- 确保 Cisco Secure Firewall Management Center可以反转解析自己的 IP 地址。

过程

步骤 1 选择**策略 > 操作 > 警报**。

步骤 2 点击 **入侵邮件**。

步骤 3 如入侵邮件警报选项，第 546 页中所述，选择警报选项，包括要警报的入侵规则或规则组。

步骤 4 点击**保存 (Save)**。

入侵邮件警报选项

On/Off

启用或禁用入侵邮件警报。

注释 启用它将为所有规则启用警报，除非选择单个规则。

发件人/收件人地址

邮件发件人和收件人。您可以指定一个以逗号分隔的收件人列表。

最大警报数和频率

Cisco Secure Firewall Management Center将按时间间隔发送（**频率**）的邮件警报最大数（**最大警报数**）。

Coalesce Alerts

通过将具有相同源 IP 和规则 ID 的警报分组来减少发送的警报数。

Summary Output

启用简要警报，适用于文本受限的设备。简要警报包含以下内容：

- 时间戳
- 协议
- 源和目标 IP 和端口
- 消息
- 同一个源 IP 生成的入侵事件数量

例如：`2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0 snort_decoder: Unknown Datagram decoding problem! (116:108)`

如果启用**摘要输出**，还应考虑启用**组合警报**。您可能还希望降低**最大警报数**，以避免超过文本消息限制。

时区

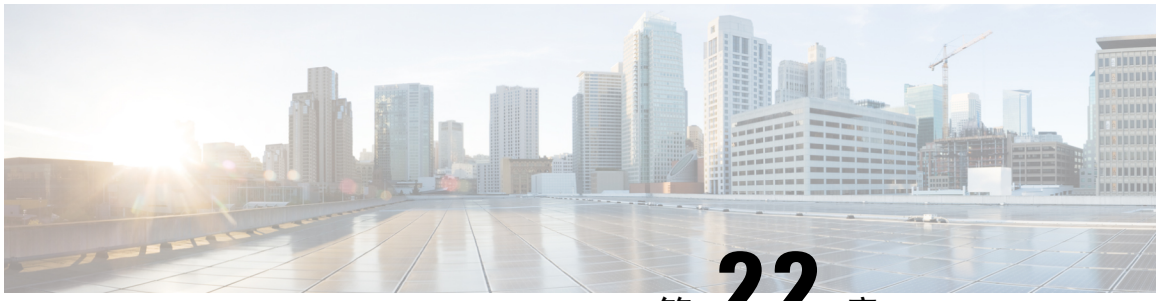
警报时间戳的时区。

Email Alerting on Specific Rules Configuration

允许您选择要在其中设置邮件警报的规则。

第 VI 部分

事件和资产分析工具



第 22 章

Context Explorer

以下主题介绍如何在 Firepower 系统中使用情景管理器：

关于情景管理器

Firepower 系统情景管理器在情景中显示有关受监控网络状态的详细、交互图形信息，包括有关应用、应用统计、连接、地理位置、危害表现、入侵事件、主机、服务器、安全情报、用户、文件（包括恶意软件文件）和相关URL的数据。不同部分以生动的曲线图、条形图、饼状图和环状图方式显示这些数据，附有详细列表。第一部分是随着时间推移的流量和事件计数曲线图，提供网络活动的最新趋势一览图。

可轻松创建和应用自定义过滤器以微调分析；此外，点击图形区域或将光标悬停在图形区域，还可更详细地查看各数据部分。还可配置情景管理器的时间范围，以反映短至前一小时或长至上一年的时间段。只有具备管理员、安全分析师或安全分析师（只读）用户角色的用户才能访问情景管理器。

Firepower 系统控制面板可自定义、分区且可实时更新。相反，情景管理器需手动更新，以便为其数据提供更广泛的上下文，而且拥有单一且一致的布局，以供活跃用户浏览。

可根据自己的特定需求使用控制面板监控网络和设备上的实时活动。相反，可用情景管理器在特别详细和清晰的情景中调查一组预定义的最新数据：例如，如果注意到网络中只有 15% 的主机在使用 Linux，但却占据了几乎所有的 YouTube 流量，则可快速应用过滤器查看仅适合 Linux 主机的数据和/或 YouTube 关联的应用数据。与紧凑、狭小的控制面板构件不同，情景管理器部分旨在以对 Firepower 系统的专家和普通用户均有效的格式醒目再现的系统活动。

显示的数据取决于您如何许可和部署受管设备以及是否配置提供数据的功能等因素。也可以应用过滤器限制所有情景管理器部分中显示的数据。

在多域部署中，在祖先域中查看数据时，情景管理器会显示所有子域的汇聚数据。在枝叶域中，只能查看特定于该域的数据。

控制面板和情景管理器之间的区别

下表概述控制面板与情景管理器之间的一些主要区别。

表 *61:* 比较：控制面板与情景管理器

功能	控制面板	Context Explorer
可显示数据	Firepower 系统监控的任何内容	应用、应用统计、地理定位、主机危害表现、入侵事件、文件（包括恶意软件文件）、主机、安全情报事件、服务器、用户和 URL
可自定义性	• 控制面板构件的选择可自定义 • 可按不同程度自定义各个构件	• 不能改变基本布局 • 应用的过滤器显示在情景管理器 URL 中且可标上书签供以后使用
数据更新频率	自动（默认）；用户配置的频率	手动
数据过滤	可用于某些构件（必须编辑构件首选项）	可用于情景管理器的所有部分，可支持多个过滤器
图形上下文	某些构件（特别是“自定义分析”[Custom Analysis]）可以图形方式显示数据	所有数据的广泛图形上下文，包括特别详细的环状图
链接到相关 Web 界面页面	在某些构件中	在每个部分
已显示数据的时间范围	用户配置	用户配置

相关主题

关于控制面板，第 321 页

“流量和入侵事件计数时间”图形

情景管理器顶部有一个随时间推移的流量和入侵事件曲线图。X 轴标绘时间间隔（从五分钟到一个月不等，取决于选定的时窗）。Y 轴以千字节标绘流量（蓝线）和入侵事件计数（红线）。

请注意，最小的 X 轴间隔为五分钟。为满足此要求，系统将在选定的时间范围内将起点和终点四舍五入至最近的五分钟间隔。

在默认情况下，此部分显示选定时间范围内的所有网络流量和生成的所有入侵事件。如果应用过滤器，该图表会改为仅显示与过滤器中指定条件相关联的流量和入侵事件。例如，过滤 `Windows` 的**操作系统名称 (OS Name)** 导致时间图形仅显示与使用 Windows 操作系统的主机相关联的流量和事件。

如果过滤情景管理器上的入侵事件数据（例如**优先级 (Priority)** 为 `High`），蓝色流量曲线将隐藏，以便单独突出入侵事件。

将鼠标指针悬停在图形线条的任何点上方，即可查看有关流量和事件计数的确切信息。将鼠标指针悬停在其中一个彩色线条上方，也可将该线条拖至图形前沿，提供更清晰的上下文。

此部分主要从“入侵事件”和“连接事件”表提取数据。

危害表现部分

Context Explorer 的 Indications of Compromise（危害表现）部分包含两个交互部分，提供受监控网络上可能受损主机的全局视图：已触发最常用 IOC 类型的比例视图，以及按已触发指示数量显示的主机视图。

有关 IOC 的详细信息，请参阅危害表现数据，第 877 页。

“按表现划分的主机”图形

“按表现划分的主机”图形以环状图形式显示受监控网络中主机触发的危害表现 (IOC) 的比例视图。内环按 IOC 类别划分的（例如，`CnC Connected` 或 `Malware Detected`），同时，外环进一步按特定事件类型划分数据（例如，`Impact 2 Intrusion Event - attempted-admin` 或 `Threat Detected in File Transfer`）。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”(Hosts) 和“主机危害表现”(Host Indications of Compromise) 表中提取数据。

“按主机划分的表现”图形

“按主机划分的指示”图形以条形图形式显示受监控网络中 15 个 IOC 最活跃的主机触发的独特危害表现 (IOC) 的计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”(Hosts) 和“主机危害表现”(Host Indications of Compromise) 表中提取数据。

网络信息部分

情景管理器的“网络信息”(Network Information) 部分包含六个交互图形，这六个交互图显示受监控网络中连接流量的全局视图：源、目标、用户、与流量关联的安全区域、网络主机使用的操作系统故障细分，以及 Firepower 系统对网络流量执行的访问控制措施的比例视图。

“操作系统”图形

“操作系统”图形以环状图形式显示在受监控网络中主机上检测到的操作系统的比例再现。内环按操作系统名称划分（例如，`Windows` 或 `Linux`），而外环按特定操作系统版本进一步划分该数据（例如，`Windows Server 2008` 或 `Linux 11.x`）。一些密切相关的操作系统（例如，Windows 2000、Windows XP 和 Windows Server 2003）组合在一起。非常罕见或无法识别的操作系统在**其他 (Other)** 下分组。

请注意，无论日期和时间限制如何，此图形均反映所有可用数据。如果更改情景管理器的时间范围，图形不变。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”表提取数据。

“按源 IP 划分的流量”图形

“按源 IP 划分的流量”图形以条形图形式显示受监控网络中前 15 个最活跃源 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个源 IP 地址，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按源 IP 划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

“按源用户划分的流量”图形

“按源用户划分的流量”图形以条形图形式显示受监控网络中前15个最活跃源用户的网络流量（千字节每秒）和独特连接的计数。对于列出的每个源 IP 地址，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按源用户划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。它显示授权的用户数据。

“按访问控制操作划分的连接”图形

“按访问控制操作划分的连接”图形以饼图形式显示Firepower系统部署已对受监控流量采取的访问控制操作（例如阻止 [Block] 或允许 [Allow]）的比例视图。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按源用户划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

“按目标 IP 划分的流量”图形

“按目标 IP 划分的流量”图形以条形图形式显示受监控网络中前 15 个最活跃目标 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个目标 IP 地址，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按目标 IP 划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

“按入口/出口安全区域划分的流量”图形

“按入口/出口安全区域划分的流量”图形以条形图形式显示受监控网络上配置的每个安全区域的传入或传出网络流量（千字节每秒）和独特连接的计数。您可配置此图形，根据自己的需求显示入口（默认）或出口安全区域的信息。

对于列出的每个安全区域，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息

提示 要限制此图形，使其仅按出口安全区域显示流量，将鼠标指针悬停在图形上方，然后在显示的切换按钮上点击**出口 (Egress)**。点击**入口 (Ingress)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“入口”(Ingress) 视图。

注释 如果过滤入侵事件信息，“按入口/出口安全区域划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

应用信息部分

情景管理器的“应用信息”(Application Information) 部分包含三个交互图形和一个表格式列表，它们显示受监控网络中应用活动的全局视图：流量、入侵事件以及与应用相关联且进一步按分配给每个应用的预估风险或业务关联性排列的主机。“应用详细信息”(Application Details) 列表列出了每个应用及其风险、业务关联性、类别和主机计数的交互列表。

对于此部分的所有“应用”实例，“应用信息”(Application Information) 图形集默认对应用协议（例如 DNS 或 SSH）进行具体检查。您还可配置“应用信息”(Application Information) 部分，具体检查客户端应用（例如 PuTTY 或 Firefox）或 Web 应用（例如 Facebook 或 Pandora）。

关注应用信息部分

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**分析** > **情景管理器**。

步骤 2 将鼠标指针悬停在 **Application Protocol Information** 部分的上方。

注释 如果之前在同一个情景管理器会话中更改了此设置，该部分标题可能改为显示**客户端应用信息 (Client Application Information)** 或 **Web 应用信息 (Web Application Information)**。

步骤 3 点击 **Application Protocol**、**Client Application** 或 **Web Application**。

“按风险/业务关联性和应用划分的流量”图形

“按风险/业务关联性和应用划分的流量”图形以环状图形式显示在受监控网络上检测到的应用流量的比例再现，这些受监控网络按应用的预估风险（默认值）或预估业务关联性进行排列。内环按预估的风险/业务关联性水平（例如，`Medium`或`High`）划分，而外环按特定应用对数据进行进一步的划分（例如，`SSH` 或 `NetBIOS`）。很少检测到的应用在**其他 (Other)** 下分组。

请注意，无论日期和时间限制如何，此图形均反映所有可用数据。如果更改情景管理器的时间范围，图形不变。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其按业务相关性和应用显示流量，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**业务相关性 (Business Relevance)**。点击**风险 (Risk)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“风险”(Risk) 视图。

注释 如果过滤入侵事件信息，“按风险/业务和应用划分的流量”图形将隐藏。

此图形主要从“连接事件”和“应用统计信息”表提取数据。

“按风险/业务关联性和应用划分的入侵事件”图形

“按风险/业务关联性和应用划分的入侵事件”图形以环状图形式显示受监控网络上检测到的入侵事件以及与这些入侵事件相关联的应用的比例再现，这些事件按应用的预估风险（默认值）或预估业务关联性进行排列。内环按预估的风险/业务关联性水平（例如，`Medium`或`High`）划分，而外环按特定应用对数据进行进一步的划分（例如，`SSH` 或 `NetBIOS`）。很少检测到的应用在**其他 (Other)** 下分组。

将鼠标指针悬停在环状图形任何部分的上方，即可查看更详细的信息。点击图形中的任何部分，可过滤或向下展开该信息或（如适用）查看应用信息。

提示 要限制此图形，使其按业务相关性和应用显示入侵事件，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**业务相关性 (Business Relevance)**。点击**风险 (Risk)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“风险”(Risk) 视图。

此图形主要从“入侵事件”和“应用统计数据”表提取数据。

“按风险/业务关联性和应用划分的主机”图形

“按风险/业务关联性和应用划分的主机”图形以环状图形式显示受监控网络上检测到的主机以及与这些主机相关联的应用的比例化再现，这些主机按应用的预估风险（默认值）或预估业务关联性进行排列。内环按预估的风险/业务关联性水平（例如，`Medium` 或 `High`）划分，而外环按特定应用对数据进行进一步的划分（例如，`SSH` 或 `NetBIOS`）。非常罕见的应用在**其他 (Other)** 下分组。

将鼠标指针悬停在环状图形任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其按业务相关性和应用显示主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**业务相关性 (Business Relevance)**。点击**风险 (Risk)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“风险”(Risk) 视图。

此图形主要从“应用”表提取数据。

应用详细信息列表

“应用信息”(Application Information) 部分底端为“应用详细信息列表”(Application Details List)，该表格提供受监控网络上检测到的每个应用的预估风险、预估业务关联性、类别和主机计数信息。应用按关联主机计数的降序列出。

“应用详细信息列表”(Application Details List) 不能排序，但是，可以点击任何表条目过滤或向下展开该信息或（如适用）查看应用信息。此表主要从“应用”(Applications) 表提取数据。

请注意，无论日期和时间限制如何，此列表均反映所有可用数据。如果更改资源管理器的时间范围，列表不变。

安全情报部分

Context Explorer 的“安全情报”部分包含三个交互条形图，这些图显示被安全情报阻止或监控的受监控网络上流量的全局视图。这些图分别按类别、源 IP 地址和目标 IP 地址对相关流量排序；显示流量（每秒千字节数）和适用连接数。

“按类别划分的安全情报流量”图形

“按类别划分的安全情报流量”图形以条形图形式显示受监控网络上的网络流量（千字节每秒）和顶级安全情报类别流量的独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按类别划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

“按源 IP 划分的安全情报流量”图形

“按源 IP 划分的安全情报流量”视图以条形图形式显示受监控网络中安全情报监控流量的顶级源 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按源 IP 划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

“按目标 IP 划分的安全情报流量”图形

“按目标 IP 划分的安全情报流量”图形以条形图形式显示受监控网络中安全情报监控流量的顶级源 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按目标 IP 划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

入侵信息部分

Context Explorer 的 Intrusion Information 部分包含六个交互图形和一个表格式列表，它们显示受监控网络中入侵事件的全局视图：影响级别、攻击源、目标、用户、优先级、与入侵事件关联的安全区域，以及入侵事件分类、优先级和计数的详细列表。

“按影响划分的入侵事件”图形

“按影响划分的入侵事件”图形以饼状图形式显示受监控网络上入侵事件的比例视图，按预估的影响级别（从 0 - 4）分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵检测 (IDS 数据)”和“入侵事件”表提取数据。

“主要攻击者”图形

“主要攻击者”图形以条形图形式显示受监控网络中主要攻击性主机 IP 地址（导致这些事件的地址）的入侵事件的计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

“主要用户”图形

“主要用户”图形以条形图形式按事件计数显示与最高入侵事件计数关联的受监控网络上的用户。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵检测 (IDS) 用户数据”和“入侵事件”表提取数据。它显示授权的用户数据。

“按优先级划分的入侵事件”图形

“按优先级划分的入侵事件”图形以饼状图形式显示受监控网络中入侵事件的比例视图，按预估的优先级（例如，高 (High)、中 (Medium) 或低 (Low)）分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

“主要目标”图形

“主要目标”图形以条形图形式显示受监控网络中主要目标主机 IP 地址（导致这些事件的连接中的目标）的入侵事件计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

“主要入口/出口安全区域”图形

“主要入口/出口安全区域”图形以条形图形式显示与受监控网络上配置的每个安全区域（入口或出口，取决于图形设置）关联的入侵事件计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅按出口安全区域显示流量，将鼠标指针悬停在图形上方，然后在显示的切换按钮上点击**出口 (Egress)**。点击**入口 (Ingress)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“入口”(Ingress) 视图。

此图形主要从“入侵事件”表提取数据。

您可配置此图形，根据自己的需求显示入口（默认）或出口安全区域的信息。

入侵事件详细信息列表

“入侵信息”(Intrusion Information) 部分的底端为“入侵事件详细信息”列表，该表格提供了受监控网络上检测到的每个入侵事件的分类、预估优先级和事件计数信息。这些事件按事件计数降序列出。

“入侵事件详细信息”列表不能排序，但是，可点击任何表条目过滤或向下展开该信息。此表主要从“入侵事件”表提取数据。

文件信息部分

Context Explorer 的 Files Information 部分包含六个交互图形，它们显示受监控网络上的文件和恶意事件的全局视图。

五个图形显示恶意软件防护（以前称为面向 Firepower 的 AMP）相关的数据：网络流量中检测到的文件的文件类型、文件名和恶意软件处置情况，以及发送（上传）和接收（下载）这些文件的主机。最终图形显示在您的组织中检测到的所有恶意软件威胁，无论是由恶意软件防护 还是面向终端的 AMP 检测到。

注释 如果过滤入侵信息，整个 Files Information 部分将隐藏。

“主要文件类型”图形

“主要文件类型”图形以饼状图形式显示网络流量中检测到的文件类型的比例视图（外环），按文件类别（内环）分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”表提取数据。

“主要文件名”图形

“主要文件名”图形以条形图形式显示网络流量中检测到的主要独特文件名的计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”表提取数据。

“按处置情况划分的文件”图形

“主要文件类型”图形以饼状图形式显示恶意软件防护 功能检测到的文件恶意软件处置情况的比例视图。请注意，只有 Cisco Secure Firewall Management Center对其执行恶意软件云查找的文件才具有处置情况。未触发云查找的文件性质为 `N/A`。`Unavailable` 性质表示Cisco Secure Firewall Management Center无法执行恶意软件云查找。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”表提取数据。

“发送文件的主要主机”图形

“发送文件的主要主机”图形以条形图形式显示网络流量中检测到的主要文件发送主机 IP 地址的文件数量计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示发送恶意软件的主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**恶意软件 (Malware)**。点击**文件 (Files)** 以返回默认文件视图。请注意，离开情景管理器也会使此图形返回默认文件视图。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”表提取数据。

“接收文件的主要主机”图形

“接收文件的主要主机”图形以条形图形式显示网络流量中检测到的主要文件接收主机 IP 地址的文件数量计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示接收恶意软件的主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**恶意软件 (Malware)**。点击**文件 (Files)** 以返回默认文件视图。请注意，离开情景管理器也会使此图形返回默认文件视图。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”表提取数据。

“主要恶意软件检测”图形

“主要恶意软件检测”图形以条形图形式显示在您的组织中检测到的主要恶意软件威胁的计数，无论是由 恶意软件防护 还是由 Cisco Secure Endpoint进行检测。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”和“恶意软件事件”表提取数据。

地理位置信息部分

Context Explorer 的 Geolocation Information 部分包含三个交互环状图形，它们显示与受监控网络上主机交换数据的国家/地区的全局视图：发起方或响应方国家/地区的独特连接、按源或目标国家/地区划分的入侵事件以及按发送或接收国家/地区划分的文件事件。

“按发起方/响应方国家/地区划分的连接”图形

甜甜圈形的“按发起方/响应方国家/地区划分的连接”图形显示了一幅作为发起方（默认值）或响应方参与您网络上的连接的国家/地区的比例视图。内环将这些国家/地区按大陆组合。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示作为连接响应方的国家/地区，将鼠标指针悬停在图形上方，然后在显示的切换按钮上，点击**响应方 (Responder)**。点击**发起方 (Initiator)** 返回默认视图。请注意，离开 Context Explorer 也会使此图形返回默认“发起方”(Initiator) 视图。

此图形主要从“连接摘要数据”表提取数据。

“按源/目标国家/地区划分的入侵事件”图形

“按源/目标国家/地区划分的入侵事件”图形以环状图形式显示作为事件（默认值）或目标来源的网络上入侵事件涉及的国家/地区的比例视图。内环将这些国家/地区按大陆组合。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示作为入侵事件目标的国家/地区，将鼠标指针悬停在图形上方，然后在显示的切换按钮上，点击**目标 (Destination)**。点击**源 (Source)** 以返回默认视图。请注意，离开情景管理器也会使此图形返回默认“源”(Source) 视图。

此图形主要从“入侵事件”表提取数据。

“按发送/接收国家/地区划分的文件事件”图形

“按发送/接收国家/地区划分的文件事件”图形以环状图形式显示网络上文件事件中检测到作为发送（默认值）或接收文件的国家/地区的比例视图。内环将这些国家/地区按大陆组合。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示接收文件的国家/地区，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**接收方 (Receiver)**。点击**发送方 (Sender)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“发送方”(Sender) 视图。

此图形主要从“文件事件”表提取数据。

URL 信息部分

Context Explorer 的“URL 信息”(URL Information) 部分包含三个交互条形图形，它们显示与受监控网络上主机交换数据的 URL 的全局视图：与 URL 相关联、按单个 URL、 URL 类别和 URL 声誉排序的流量和独特连接。不能过滤 URL 信息。

注释 如果过滤入侵事件信息，整个“URL 信息”(URL Information) 部分将隐藏。

请注意，您必须具有 URL 过滤 可证才能使此图形包含 URL 类别和信誉数据。

“按 URL 划分的流量”图形

“按 URL 划分的流量”图形以条形图形式显示受监控网络中请求最频繁的 15 个 URL 的网络流量（千字节每秒）和独特连接的计数。对于列出的每个 URL，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按 URL 划分的流量”图形将隐藏。

请注意，您必须具有 URL 过滤 可证才能使此图形包含 URL 类别和信誉数据。

此图形主要从“连接事件”表提取数据。

“按 URL 类别划分的流量”图形

“按 URL 类别划分的流量”图形以条形图形式显示受监控网络中请求最频繁的 URL 类别 （例如，搜索引擎 [Search Engines] 和流媒体 [Streaming Media]）的网络流量（千字节每秒）和独特连接的计数。对于列出的每个 URL 类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按 URL 类别划分的流量”图形将隐藏。

请注意，您必须具有 URL 过滤 可证才能使此图形包含 URL 类别和信誉数据。

此图形主要从“URL 统计数据”和“连接事件”表提取数据。

“按 URL 信誉划分的流量”图形

“按URL信誉划分的流量”图形以条形图形式显示受监控网络中请求最频繁的URL信誉组（例如，受信任的 或 中立）的网络流量（千字节每秒）和独特连接的计数。对于列出的每个 URL 声誉组，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按 URL 声誉划分的流量”图形将隐藏。

请注意，您必须具有 URL 过滤 可证才能使此图形包含 URL 类别和信誉数据。

此图形主要从“URL 统计数据”和“连接事件”表提取数据。

情景管理器的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 安全分析师

刷新情景管理器

情景管理器不会自动更新显示的信息。要更新数据，必须手动刷新情景管理器。

请注意，虽然重新加载情景管理器（通过刷新资源管理器程序或离开，然后返回情景管理器）可刷新所有显示的信息，但此操作不会保留对部分配置做出的任何更改（例如“入口/出口”图形和“应用信息”[Application Information] 部分）且可能导致加载延迟。

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**分析** > **情景管理器**。

步骤 2 点击右上角的**重新加载 (Reload)**。

在刷新完成之前，**重新加载** 按钮呈灰色显示。

设置情景管理器时间范围

可配置情景管理器的时间范围，以反映短至前一小时或长至上一年的时间段。请注意，如果更改时间范围，情景管理器无法自动更新反映所做的更改。要应用新的时间范围，必须手动刷新情景管理器。

即使离开情景管理器或终止登录会话，对时间范围所做的更改也会持续。

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**分析** > **情景管理器**。

步骤 2 从**显示最后时间 (Show the last)** 下拉列表，选择时间范围。

步骤 3 或者，要从新时间范围查看数据，请点击 **Reload**。

提示 点击 **Apply Filters** 也可应用任何时间范围更新。

最小化和最大化情景管理器部分

可最小化和隐藏情景管理器的一个或多个部分。如要仅重点关注某些部分，或如果想要更简单的视图，此操作很有用。不能最小化“流量和入侵事件计数时间”图形。

即使刷新页面或注销设备，情景管理器部分仍会保持处于配置的最小化或最大化状态。

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**分析** > **情景管理器**。

步骤 2 要最小化某个部分，请点击部分的标题栏中的 **折叠箭头** （ ） 。

步骤 3 要最大化某个部分，请点击最小化部分的标题栏中的最大化 **展开箭头** （ ） 。

向下展开情景管理器数据

如果想要超出 Context Explorer 允许的范围，更详细地检查图形和列表数据，可向下展开相关数据的表视图。（请注意，不能向下展开“随时间推移的流量和入侵事件”[Traffic and Intrusion Events over Time] 图形。）例如，向下展开“按源 IP 划分的流量”(Traffic by Source IP) 图形中的 IP 地址可显示“连接事件”(Connection Events) 表的“具有应用详细信息的连接”(Connections with Application Details) 视图，仅包括与所选源 IP 地址关联的数据。

视乎要检查的数据类型，情景菜单中会显示其他选项。与特定 IP 地址相关联的数据点提供的选项可用于查看有关所选 IP 地址的主机或域名信息。与特定应用相关联的数据点提供的选项可用于查看有关所选应用的应用信息。与特定用户相关联的数据点提供的选项可用于查看该用户的用户配置文件页。与入侵事件消息相关联的数据点提供了查看与该事件相关联的入侵规则的规则文档的选项，与特定IP地址相关联的数据点提供了将该地址添加到阻止或不阻止列表的选项。有关这些列表的详细信息，请参阅 全局和域安全情报列表 。

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**分析** > **情景管理器**。

步骤 2 在除 **随时间推移的流量和入侵事件**以外的任何部分中，点击要调查的数据点。

步骤 3 视乎所选数据点，系统提供多个选项：

- 要在表视图中查看此数据的更多详细信息，请选择**深入分析 (Drill into Analysis)**。
- 如果选择了与特定 IP 地址相关联的数据点并要查看有关关联主机的详细信息，请选择**查看主机信息 (View Host Information)**。
- 如果选择了具有特定 IP 地址的数据点并要对该地址执行 whois 搜索，请选择 **Whois**。
- 如果选择了与特定应用相关联的数据点并要查看有关该应用的详细信息，请选择**查看应用信息 (View Application Information)**。
- 如果选择了与特定用户相关联的数据点并要查看有关该用户的详细信息，请选择**查看用户信息 (View User Information)**。
- 如果选择了与特定入侵事件消息相关联的数据点并要查看有关关联入侵规则的详细信息，请选择**查看规则文档**；或者，然后点击**规则文档**，以查看更具体的规则详细信息
- 如果您选择了与特定IP地址关联的数据点，并希望将该IP地址添加到安全情报全局阻止或不阻止列表，请选择适当的选项。

情景管理器中的过滤器

除了 Context Explorer 初始显示的基本、广泛数据外，可选择为网络中活动的更精细的上下文照片过滤该数据。过滤器包含除 URL 信息外的所有类型 Firepower 系统数据，支持排除和纳入，点击情景管理器图形数据点即可快速应用，并影响整个管理器。可以一次应用最多 20 个过滤器。

过滤器可以通过多种方式添加至 Context Explorer 数据：

- 从“添加过滤器”(Add Filter) 对话框添加
- 在管理器中选择一个数据点时，从情景菜单添加
- 从特定详细信息视图页面（“应用详细信息”[Application Detail]、“主机配置文件”[Host Profile]、“规则详细信息”[Rule Detail] 和“用户配置文件”[User Profile]）显示的文本链接添加。点击这些链接，根据详细信息视图页面的相关数据自动打开并过滤情景管理器。例如，点击一个用户详细信息页面上的情景管理器以便用户 `jenkins` 限制管理器仅显示与该用户相关的数据。

某些过滤器类型与其他类型不兼容：例如，与入侵事件相关的过滤器（例如，**设备 [Device]** 和**内联结果 [Inline Result]**）无法与连接事件相关的过滤器（例如，**访问控制操作 (Access Control Action)**）同时应用，因为系统无法按入侵事件数据对连接事件数据进行排序。系统将自动阻止同时应用不兼容过滤器；只要存在不兼容性，当一个过滤器类型最近被激活时，不兼容的过滤器会被隐藏。

当多个过滤器活跃时，同一种数据类型的值被视为 OR 搜索条件：将出现至少与其中一个值相匹配的所有数据。不同数据类型的值被视为 AND 搜索条件：显示至少与每种过滤数据类型相匹配的数

据。例如，为 `Application: 2channel`、`Application: Reddit` 和 `User: edickinson` 的过滤器集显示的数据必须与用户 `edickinson` **和** 应用`2channel` **或**应用 `Reddit` 相关联。

在多域部署中，当查看祖先域中的情景管理器时，可以通过多个后代域来过滤。在这种情况下，还添加 **IP 地址 (IP Address)** 过滤器时，要特别注意。系统会为每个枝叶域构建单独的网络映射。使用文字 IP 地址限制此配置可能会出现意外结果。

请注意，显示的数据取决于您如何许可和部署受管设备以及是否配置提供数据的功能等因素。

注释 过滤器用作一种简单、灵活的工具，可在任何指定时间获取准确的Firepower数据情景。过滤器不用作永久性配置设置，在离开 Context Explorer 或结束会话时会消失。要保留过滤器设置以备以后使用，请参阅保存过滤的情景管理器视图，第 571 页。

数据类型字段选项

下表列出可用作过滤器的数据类型，并带有每种类型的示例和简要定义。

表 *62:* 过滤器数据类型

类型	示例值	定义
访问控制操作 (Access Control Action)	`Allow`、`Block`	访问控制策略为允许或阻止流量而采取的操作。
应用类别 (Application Category)	`web browser`、`email`	应用的最基本功能的一般分类。
应用名称	`Facebook`、`HTTP`	应用的名称。
应用风险	`Very High`、`Medium`	应用的预计安全风险
应用标记 (Application Tag)	`encrypts communications`、`sends mail`	有关应用的其他信息；应用可以具有任意数量的标记，包括无任何标记。
应用类型	`Client`、`Web Application`	应用的类型：应用协议、客户端或 Web 应用。
业务相关性	`Very Low`、`High`	应用与业务活动的预计关联性（与娱乐相对）。
大陆 (Continent)	`North America`、`Asia`	与受监控网络上检测到的可路由IP地址相关联的大陆。
国家/地区	`Canada`、`Japan`	与受监控网络上检测到的可路由 IP 地址相关联的国家/地区。
设备	`device1.example.com`, `192.168.1.3`	受监控网络上的设备的名称或 IP 地址。
域	`Asia Division`、`Europe Division`	要绘制网络活动图表的设备的域。此数据类型只存在于多域部署中。

类型	示例值	定义
事件分类 (Event Classification)	`Potential Corporate Policy Violation`、`Attempted Denial of Service`	入侵事件的概要说明，由触发该事件的规则、解码器或预处理器的分类确定。
事件消息 (Event Message)	`dns response`、`P2P`	事件生成的消息，由触发该事件的规则、解码器或预处理器确定。
文件性质 (File Disposition)	`Malware`、`Clean`	Cisco Secure Firewall Management Center对其执行了恶意软件云查找的文件的处置情况。
文件名	`Packages.bz2`	网络流量中检测到的文件的名称。
文件 SHA256	任何 32 位字符串	Cisco Secure Firewall Management Center对其执行了恶意软件云查找的文件的 SHA-256 散列值。
文件类型	`GZ`、`SWF`、`MOV`	网络流量中检测到的文件类型。
文件类型类别 (File Type Category)	`Archive`、`Multimedia`、`Executables`	网络流量中检测到的文件类型的一般类别。
IP 地址	`192.168.1.3`、`2001:0db8:85a3::0000/24`	IPv4 或 IPv6 地址、地址范围或地址块。 请注意，搜索 IP 地址时可返回事件，其中，该地址是事件的源或目标。
影响级别 (Impact Level)	`Impact Level 1`、`Impact Level 2`	受监控网络上的事件的预计影响。
内联结果	`dropped`、`would have dropped`	流量是已丢弃、应已丢弃还是未由系统处理
IOC 类别 (IOC Category)	`High Impact Attack`、`Malware Detected`	已触发的危害表现 (IOC) 事件的类别。
IOC 事件类型 (IOC Event Type)	`exploit-kit`, `malware-backdoor`	与特定危害表现 (IOC) 相关联的标识符，指代触发该标识符的事件。
恶意软件威胁名称 (Malware Threat Name)	`W32.Trojan.a6b1`	恶意软件威胁的名称。
OS 名称 (OS Name)	`Windows`、`Linux`	操作系统的名称。
OS 版本	`XP`, `2.6`	操作系统的特定版本。
优先级	`high`、`low`	事件的预计紧急程度。
安全情报类别 (Security Intelligence Category)	`Malware`、`Spam`	危险流量的类别，由安全情报确定。
安全区	`My Security Zone`、`Security Zone X`	接口集，流量通过其进行分析，并在内联部署中传递

类型	示例值	定义
SSL	yes、no	SSL 或 TLS 加密流量。
用户	wsmith、mtwain	登录到受监控网络上的主机的用户的身份。

从“添加过滤器”(Add Filter) 窗口新建过滤器

使用此程序，通过“添加过滤器”(Add Filter) 窗口从头开始创建过滤器。（也可以使用情景菜单创建快速过滤器。）

点击情景管理器左上方的 **过滤器** 下的 **加号**（+）即可访问的“添加过滤器”窗口，该窗口仅包含两个字段：

- **数据类型 (Data Type)** 下拉列表包含许多可用于限制情景管理器的不同类型的 Firepower 系统数据。选择一个数据类型后，在**过滤器 (Filter)** 字段为该类型输入一个特定的值（例如，为类型**大洲 [Continent]** 输入一个值亚洲 [Asia]）。为了便于操作，“过滤器”(Filter) 字段将所选数据类型提供多个灰显示例值。（在该字段中输入数据时，这些示例值将被擦除。）
- 在**过滤器 (Filter)** 字段中，可以输入特殊搜索参数，例如，* 和 !，本质上与事件搜索中一致。可以通过为过滤器参数加上 ! 符号作为前缀来创建排斥过滤器。

注释 添加的过滤器不会自动应用；必须点击**应用过滤器 (Apply Filters)** 才能查看情景管理器中的过滤内容。

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**分析** > **情景管理器**。

步骤 2 在左上角的 **过滤器** 下，点击 **加号**（+）。

步骤 3 从**数据类型 (Data Type)** 下拉列表中，选择要过滤的数据类型。

步骤 4 在**过滤器 (Filter)** 字段中，输入要过滤的数据类型值。

步骤 5 点击 **OK**。

步骤 6 或者，请重复以上步骤添加更多的过滤器，直至添加完所需的过滤器集。

步骤 7 点击 **Apply Filters**。

相关主题

数据类型字段选项，第 568 页
搜索限制，第 671 页

从情景菜单创建快速过滤器

浏览情景管理器图形和列表数据时，可点击数据点，然后使用上下文菜单根据该数据快速创建一个过滤器（包容性或排除性）。如用上下文菜单过滤“应用”、“用户”或“入侵事件消息”数据类型的信息，或任何单个主机，则过滤器构件包括一个构件信息，该图标链接至该数据类型（例如应用数据的“应用详细信息”）的相关详细信息页面。请注意，不能过滤 URL 数据。

上下文菜单还可用于更详细地调查特定图形或列表数据。

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。

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 在资源管理器的任何部分（“随时间推移的流量和入侵事件”部分或包含URL数据的部分除外），点击要过滤的数据点。

步骤 3 此时您有两种选择：

- 要为该数据添加一个过滤器，请点击**添加过滤器 (Add Filter)**。
- 要为该数据添加一个排除过滤器，请点击**添加排除过滤器 (Add Exclude Filter)**。应用后，该过滤器显示与排除值**不**关联的所有数据。排除过滤器的过滤器值之前显示一个感叹号 (!)。

保存过滤的情景管理器视图

要在离开情景管理器或结束会话后在情景管理器中保留过滤设置，请使用所应用的首选过滤器创建情景管理器的浏览器书签。由于已应用的过滤器已纳入Context Explorer页面URL，加载该页面的书签也会加载相应的过滤器。

过程

使用所应用的首选过滤器创建情景管理器的浏览器书签。

查看过滤器数据

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。

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 在任何符合条件的过滤器构件上，点击 **信息** 。

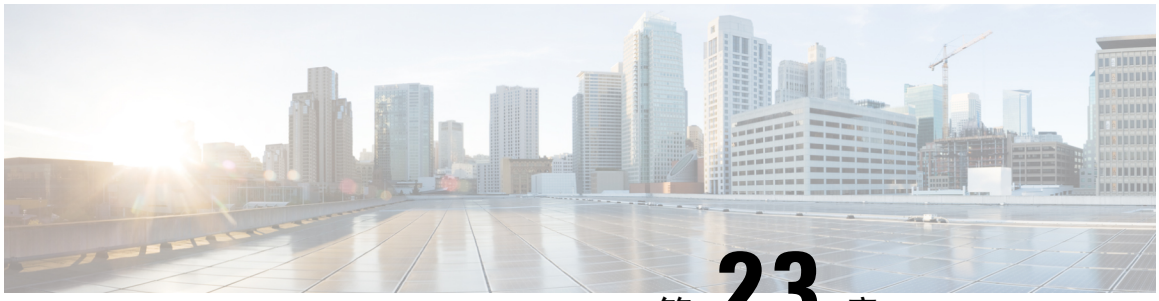
删除过滤器

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 在左上方的 **过滤器** 下，单独点击 **关闭**（×） 以删除过滤器构件。

提示 如果要一次性删除所有过滤器，可点击 **清除**按钮。



第 23 章

统一事件

以下主题介绍如何使用统一事件：

关于统一事件

统一事件为您提供多种类型（连接、入侵、文件、恶意软件和一些安全相关的连接事件）的单一屏幕视图。相互关联的事件在表中堆叠在一起，以提供有关安全事件的统一视图和更多上下文。如果“统一事件”表中有入侵事件，请点击入侵事件以突出显示关联的连接事件。现在，您可以将连接事件与入侵事件关联，以便更好地了解和解决网络问题，而无需在多个事件查看器之间切换。

统一事件表可高度自定义。您可以创建和应用自定义过滤器，以微调事件查看器上显示的信息。统一事件查看器还可以选择保存您经常用于特定需求的自定义过滤器，然后快速加载已保存的过滤器。此外，您还可以通过添加或删除列、固定列或拖动列并重新排序来创建定制的事件查看器表。

通过“统一事件”表中的**实时视图**选项，您可以实时查看防火墙事件并监控网络上的活动。例如，如果您是防火墙管理员，在进行策略更改后实时查看事件更新可以帮助您确保在网络上正确实施策略更改。

统一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

使用统一事件查看器操作

在单个表中查看和处理各种防火墙事件，而无需在多个事件查看器之间切换。

使用此视图：

- 在统一视图中查找不同类型事件之间的关系。
- 实时查看策略更改的影响。

开始之前

您必须具有 管理员 或 安全分析师 权限才能执行此任务。

过程

步骤 1 选择 **分析** > **统一事件**。

步骤 2 选择时间范围（固定或滑动）。有关详细信息，请参阅 在统一事件查看器中设置时间范围。

步骤 3 如果要在 Secure Network Analytics 设备上远程存储事件，并且有充分的理由更改数据源，请选择数据源。请查看 在 Cisco Secure Firewall Management Center 和使用存储在 Secure Network Analytics 设备上的连接事件上工作中的重要信息。

步骤 4 您可以过滤统一事件查看器最初显示的大量防火墙事件，以了解网络中事件的更精细情景。有关详细信息，请参阅 统一事件查看器中的过滤器。

步骤 5 选择更多选项：

要执行此操作...	相应操作
自定义列	• 添加或删除列： 点击列选择器 () 并选择列。某些字段中的值取决于事件类型。每个字段旁边显示的以下图标表示事件类型对应关系： • 连接事件 () • 安全相关的连接事件 () • 入侵事件 () • 文件事件 () • 恶意软件事件 () 点击列集过滤选项旁边的事件图标，可根据所选事件类型过滤事件字段列表。 **注释** 包含许多列可能会降低性能。您可以通过展开事件行查看事件详细信息来查看隐藏列的数据。 • 对列重新排序： 拖放列标题。 • 将列固定（冻结）到表的左侧或右侧，使它们不会滚动： 将列拖至表的左侧或右侧。 或者，将列标题拖放到固定区域。 要取消固定列，请将该列拖出固定区域。 • 调整列大小。 • 将列恢复为默认设置。 • 保存列集。有关详细信息，请参阅 在统一事件查看器中保存列集 主题。 数据始终按时间排序，最新事件排在最前面。
识别相关事件	点击一行可突出显示与此事件相关的其他事件。 如果需要，过滤事件以显示足够小的事件集。 **注释** 连接的发起方不一定与恶意软件文件的发送方相同。通过使用 **源或目标IP** 过滤器过滤统一事件查看器，搜索与连接事件关联的文件或恶意软件事件。

要执行此操作...	相应操作
查看事件详情	点击行左端的 >（拓展）图标。事件详细信息不包括没有要显示的数据的字段。 **提示** 或者，双击事件行可查看 **事件详细信息** 窗格。当 **事件详细信息** 窗格打开时，点击表中的任何事件行以加载该事件的详细信息。
使用 Packet Tracer 对事件进行故障排除	1. 点击要运行数据包跟踪的行旁边的省略号图标 (⋮)。 2. 选择 **打开 Packet Tracer**，根据事件的源和目标寻址以及协议特征，在 Packet Tracer 工具中为数据包建模。跟踪模拟数据包并使用跟踪结果对安全事件进行故障排除。有关如何使用数据包跟踪器工具的详细信息，请参阅 使用数据包跟踪器，第 428 页。
实时查看事件	点击 **上线**。有关详细信息，请参阅 统一事件查看器中的事件实时视图。 如果事件流过快，请输入过滤条件。
交叉启动到外部资源	点击表格单元格中的省略号 (⋮)，查看可用于该单元格值的选项（如果有）。 有关详细信息，请参阅使用基于 Web 的资源的事件调查，第 605 页。
打开多个统一事件查看器选项卡/窗口	• 您可以使用多个浏览器选项卡或窗口显示统一事件查看器的不同视图。 • 每个新选项卡或窗口都具有最近修改的选项卡/窗口的特征。 • 要将任何打开的选项卡/窗口设置为模板，请对其进行细微更改。 • 多个选项卡中的查询按顺序处理。 • 根据视图（例如，复杂查询或传入事件速率较高时在实时视图模式的查看），如果同时打开超过 4 个选项卡，性能可能会降低。
保存搜索	将自定义搜索保存为您的收藏，并在以后快速加载。有关详细信息，请参阅 在统一事件查看器中保存搜索。
为查询结果添加书签或共享	将 URL 加入书签或复制粘贴到浏览器窗口中。 • 如果 URL 使用滑动时间范围，则稍后将检索不同的事件。 • 列可视性、大小和顺序以及实时流设置不会在 URL 中捕获。

在统一事件查看器中设置时间范围

在统一事件查看器中配置时间范围，以查看特定时间段的防火墙事件。当您更改时间范围时，统一事件查看器会自动刷新以反映您的更改。

您选择的时间范围不适用于事件查看器中的其他表。例如，您在查看连接事件时选择的时间范围不适用于统一事件查看器，反之亦然。

重要事项 如果您的时间段延长到超出连接事件的保留期，请在 **分析** > **连接** > **安全情报事件**下的表中查找安全情报事件。

开始之前

您必须具有 管理员 或 安全分析师 权限才能执行此任务。

过程

步骤 1 选择 **分析** > **统一事件**。

默认情况下，统一事件查看器显示过去一小时的事件。

步骤 2 点击当前时间范围。

步骤 3 选择以下其中一个选项：

- 如果要查看固定时间范围内的事件，请点击 **固定时间范围** 并选择 **开始时间** 和 **结束时间**。

  提示 点击 **现在** 快速将当前时间设置为 **结束时间**。

- 如果您想配置指定长度的滑动式默认时间窗口，点击 **滑动式时间范围**。

  设备显示在某个特定开始时间（例如，1 小时前）和当前时间期间生成的所有事件。刷新事件视图时，时间窗口会“滑动”，以便始终显示最后一小时的事件。

步骤 4 点击**应用 (Apply)**。

统一事件查看器中的事件实时视图

将统一事件查看器配置为实时显示防火墙事件，而无需手动刷新事件查看器。在 **实时视图** 模式下，当网络中发生安全事件时，会实时显示事件日志，这有助于您更好地解决问题。

开始之前

您必须具有 管理员 或 安全分析师 权限才能执行此任务。

过程

步骤 1 选择 **分析** > **统一事件**。

默认情况下，统一事件查看器显示最近一小时的事件。

步骤 2 要查看实时事件更新，请点击 **上线**。

新事件将填充在事件表的顶部。时间范围部分显示一个计时器，通知您统一事件查看器的运行时间。

下一步做什么

要退出实时视图模式，请点击 **实时**。

统一事件查看器中的过滤器

统一事件查看器最初显示过去一小时内的多种类型的防火墙事件。您可以过滤统一事件的默认视图，以获取更精细的网络活动情景图片。过滤器支持排除和包含过滤条件。

过滤器可帮助您快速访问关键信息。例如，如果您是防火墙管理员，并且要允许或拒绝某些用户访问特定应用，则可以设置用户搜索条件以扫描防火墙日志。事件查看器显示与搜索条件匹配的事件日志。

开始之前

您必须具有 管理员 或 安全分析师 权限才能执行以下任务。

过程

步骤 1 选择 **分析** > **统一事件**。

步骤 2 输入过滤器条件：

- 要手动输入过滤条件，请在搜索文本字段中键入确切的条件，或从下拉列表中选择条件。然后，提供过滤条件值。输入值时，系统会尽可能在下拉列表中提示您建议。
- 点击表中事件的单元格中的点，然后选择一个选项以在过滤条件中包括或排除该值。

  提示
  - 使用 **Ctrl+点击** (Windows) 或 **Command-点击** (Mac) 键快速添加包含过滤条件。
  - 使用 **Alt+点击** (Windows) 或 **Option 点击** (Mac) 键快速添加排除过滤条件。

- 请细化您的过滤条件。有关通配符和搜索行为的重要信息，请参阅 事件搜索，第 671 页。
- 在值字段中，在值前面添加运算符（例如 <、>、！等）。例如，在 **操作** 字段中输入 `!Allow` 可查找操作不是“允许”的所有事件。

步骤 3 执行搜索。

提示 您可以使用 **Ctrl+Enter** (Windows) 或 **Command-Enter** (Mac) 键盘命令启动搜索。

当显示的列都具有相同的值时，统一事件查看器中的事件不会聚合。与过滤条件匹配的每个事件都单独列出。

下一步做什么

要保存自定义过滤器，请参阅 在统一事件查看器中保存搜索 主题。

在统一事件查看器中保存搜索

开始之前

您必须具有 管理员 或 安全分析师 权限才能保存列集。

过程

步骤 1 选择 **分析** > **统一事件**。

步骤 2 按照 统一事件查看器中的过滤器 主题的过滤器中的说明建立搜索条件。

步骤 3 点击搜索文本框中的 **收藏夹搜索** (☆) 图标。

步骤 4 执行以下操作之一：

- 要保存新搜索，请指定搜索名称，然后点击 **另存为**。
- 要覆盖已保存的搜索，请在已保存的搜索上点击 **编辑** ，然后点击 **覆盖**。

下一步做什么

要加载已保存的搜索，请参阅 在统一事件查看器中加载保存的搜索 主题。

在统一事件查看器中加载保存的搜索

开始之前

- 您必须具有 管理员 或 安全分析师 权限才能执行此任务。
- 按照 在统一事件查看器中保存搜索 主题的说明建立已保存搜索。

过程

步骤 1 选择 **分析** > **统一事件**。

步骤 2 点击搜索文本框中的 **收藏夹搜索** (☆) 图标。

步骤 3 点击要加载的已保存搜索。

在统一事件查看器中保存列集

开始之前

您必须具有 管理员 或 安全分析师 权限才能保存列集。

过程

步骤 1 选择 **分析** > **统一事件**。

步骤 2 点击列选择器图标 ()，然后选择要保存的列集。

步骤 3 点击 **收藏的列集** (☆) 图标。

步骤 4 执行以下操作之一：

- 要保存新列集，请指定列集名称，然后点击 **另存为**。
- 要覆盖收藏夹列集，请在要覆盖的列集上点击 **编辑** ()，然后点击 **覆盖**。

下一步做什么

要加载已保存的列集，请参阅 在统一事件查看器中加载已保存的列集 主题。

在统一事件查看器中加载已保存的列集

开始之前

- 您必须具有 管理员 或 安全分析师 权限才能执行此任务。
- 保存收藏夹列集，如 在统一事件查看器中保存列集 主题中所述。

过程

步骤 1 选择 **分析** > **统一事件**。

步骤 2 点击列选择器图标 ()。

步骤 3 点击 **收藏的列集** (☆) 。

步骤 4 点击要加载的列集。

统一事件查看器列说明

某些字段中的值取决于事件类型。默认情况下，字段对应关系如下：

统一事件查看器字段名称	连接或安全情报事件字段名称	入侵事件字段名称	文件事件字段名称	恶意软件事件字段名称
时间	首个数据包 参见下文注意事项。	时间	时间	时间
活动类型	--	--	--	--
操作	操作	内联结果	操作	操作
原因	原因	原因	（不适用）	（不适用）
源 IP	发起方 IP	源 IP	发送 IP	发送 IP
目标 IP	响应方 IP	目标 IP	接收 IP	接收 IP
源端口/ICMP 类型	源端口	源端口	发送端口	发送端口
目标地端口/ICMP 代码	目的端口	目的端口	接收端口	接收端口
Web 应用程序	Web 应用程序	Web 应用程序	Web 应用程序	Web 应用程序
规则	访问控制规则	访问控制规则	（不适用）	（不适用）
策略	访问控制策略	入侵策略	文件策略	文件策略
设备	设备	设备	设备	设备

点击列选择器 () 图标可查看所有事件字段及其对应关系。

有关字段说明，请参阅以下主题：

- 连接和 安全相关连接 事件字段 ， 第 717 页

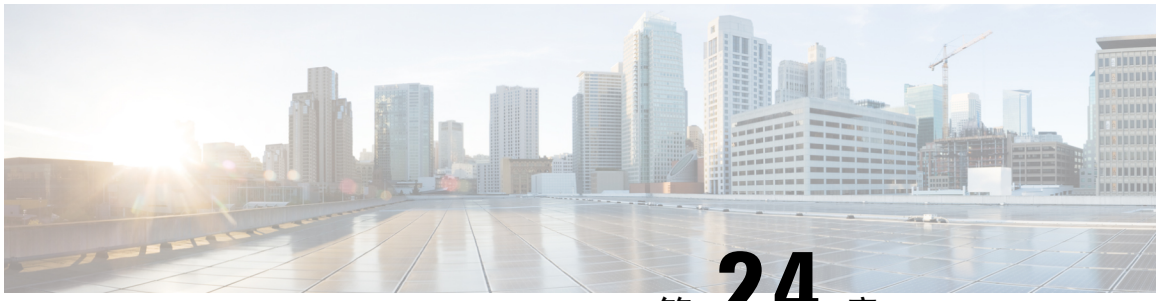
- 入侵事件字段，第 752 页
- 文件和恶意软件事件字段，第 800 页

另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明，第 733 页。

注释 即使您在连接开始时未启用日志记录，系统也会将此值用作统一事件查看器中的时间字段。要确定是否在连接开始和结束时记录了连接事件，请展开事件的行以查看详细信息。如果连接的两端均已记录，您会看到 **最后一个数据包** 字段。

统一事件的历史记录

功能	最低 管理中心	最低 威胁防御	详情
用于统一事件查看器的数据包跟踪器	7.4.1	任意	现在，您可以从“统一事件查看器”页面打开数据包跟踪器，以对安全事件进行故障排除。 点击要运行数据包跟踪的事件旁边的省略号图标 (⋮)（展开），然后点击 **在数据包跟踪器中打开 (Open in Packet Tracer)**。
统一事件查看器改进	7.4	任意	改进了保存收藏列集和搜索功能。
保存常用搜索	7.3	任意	将列集和搜索保存为收藏项，稍后快速启动它们。
统一事件查看器	7.0	任意	查看和处理具有多种事件类型的单个表：连接（包括安全情报）、入侵、文件和恶意软件。 新增/修改的页面： **分析** > **统一事件**下面的新页面。 支持的平台： 管理中心



第 24 章

网络映射

以下主题介绍如何使用网络映射：

网络映射的要求和前提条件

型号支持

任意。

支持的域

枝叶

用户角色

- 管理员
- 发现管理员

网络映射

Firepower 系统监控通过网络传输的流量，解码流量数据，然后将该数据与既有的操作系统和指纹进行比较。系统之后会使用该数据构建网络的详细表示，称为网络映射。在多域部署中，系统为每个枝叶域都创建单个网络映射。

系统从标识用于在网络发现策略中监控的受管设备收集数据。受管设备直接从受监控流量和间接从已处理的 NetFlow 记录检测网络资产。如果多台设备检测到同一网络资产，则系统会将信息合并成资产的复合表示。

要通过被动检测扩充数据，请执行以下操作：

- 使用开源扫描工具 Nmap™ 主动扫描主机，并将扫描结果添加到网络映射。
- 使用主机输入功能从第三方应用手动添加主机数据。

网络映射显示根据检测到的主机和网络设备显示网络拓扑。

网络映射可用于：

- 获取网络的快速整体视图。
- 选择不同的视图，以适应要执行的分析。网络映射的每个视图都有相同的格式：具有可扩展的类别和子类别的分层树。点击某个类别时，该类别将展开显示其下属的子类别。
- 通过自定义拓扑功能组织并识别子网。例如，如果贵公司中的每个部门使用不同的子网，则可使用自定义拓扑功能将熟悉的标签分配到这些子网。
- 通过深入了解任何受监控主机的主机配置文件查看详细信息。
- 如果对于调查资产不再感兴趣，请将其删除。

注释 如果系统检测到与已从网络映射中删除的主机关联的活动，则其会将该主机重新添加到网络映射。同样，如果系统检测到应用发生更改（例如，如果 Apache Web 服务器升级到新版本），则会将已删除的应用重新添加到网络映射。如果系统检测到使主机易受攻击的更改，则表明在特定主机上重新激活了漏洞。

提示 如果要从网络映射永久排除主机或子网，请修改网络发现策略。如果您发现负载均衡器和 NAT 设备生成额外或不相关的事件，则可能希望从监控中将其排除。

主机网络映射

“主机”选项卡上的网络映射将显示主机计数以及主机 IP 地址和主 MAC 地址的列表。每个地址或部分地址都是一条指向下一级的链接。此网络映射视图提供系统检测到的所有唯一主机的计数，无论主机有一个 IP 地址还是多个 IP 地址。

使用主机网络映射查看网络上按分层树中子网排列的主机，以及向下钻取到特定主机的主机配置文件。

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。

通过为网络创建自定义拓扑，可向主机网络映射中显示的子网分配有意义的标签，例如，部门名称。也可根据在自定义拓扑中指定的公司查看主机网络映射。

可从主机网络映射中删除整个网络、子网或个别主机。例如，如果知道主机不再连接到网络，则可将其删除以简化分析。如果系统此后检测到与已删除主机关联的活动，则会将该主机重新添加至网络映射。如果要从网络映射永久排除主机或子网，请修改网络发现策略。

注意 请勿从网络映射删除网络设备。系统会使用它们来确定网络拓扑。

在主机网络映射页面上，只能搜索主 MAC 地址，而主机 [MAC] 计数器仅包括主 MAC 地址。有关主 MAC 地址和辅助 MAC 地址的说明，请参阅 主机配置文件中的基本主机信息，第 831 页。

网络设备网络映射

“网络设备”(Network Devices) 选项卡上的网络映射显示将一个网段连接到另一个网段的网络设备（网桥、路由器、NAT 设备和负载平衡器）。该映射包含两个部分，分别列出按 IP 地址识别的设备和按 MAC 地址识别的设备。

该映射还提供系统检测到的所有唯一网络设备的计数，无论设备具有一个 IP 地址还是多个 IP 地址。

如为网络创建自定义拓扑，则网络设备网络映射中会显示分配给子网的标签。

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

如果网络设备使用 CDP 进行通信，则其可能有一个或多个 IP 地址。如果它使用 STP 进行通信，则可能仅有 MAC 地址。

由于系统使用其位置来确定网络拓扑，因此不能从网络映射中删除网络设备。

网络设备的主机配置文件具有“系统”(System) 部分而不是“操作系统”(Operating Systems) 部分，其中包括反映网络设备后检测到的任何移动设备的硬件平台的“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。

移动设备网络映射

“移动设备”(Mobile Devices) 选项卡上的网络映射显示连接到网络的移动设备。此网络映射视还提供系统检测到的所有唯一移动设备的计数，无论设备有一个 IP 地址还是多个 IP 地址。

每个地址或部分地址都是一条指向下一级的链接。您也可以删除子网或 IP 地址；如果系统重新发现设备，则会将该设备重新添加到网络映射。

您还可以向下展开以查看移动设备的主机配置文件。

要识别移动设备，系统应执行以下操作：

- 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

如为网络创建自定义拓扑，则移动设备网络映射中会显示分配给子网的标签。

危害表现网络映射

“危害表现”(Indications of Compromise) 选项卡上的网络映射显示网络上按 IOC 类别组织的受损主机。受影响主机列在每个类别下方。每个地址或部分地址都是一条指向下一级的链接。

从危害表现网络映射中，可查看通过特定方式确定为已受损的每个主机的主机配置文件。也可删除（标记为已解析）任何 IOC 类别或任何特定主机，这会从相关主机中移除 IOC 标记。例如，如已确定问题得到解决且不可能复发，即可从网络映射中删除 IOC 类别。

标记从网络映射解析的主机或 IOC 类别不会将其从网络中移除。如果系统最近检测到触发该 IOC 的信息，则网络映射中会重新显示已解析的主机或 IOC 类别。

有关系统如何确定感染指标的详细信息，请参阅危害表现数据，第 877 页和子主题。

应用协议网络映射

“应用协议”(Application Protocols) 选项卡上的网络映射显示您的网络上运行的应用，按应用名称、供应商、版本并最终按运行每个应用的主机在分层树中排列。

系统检测到的应用可能随系统软件和 VDB 更新而变化，并且在导入任何附加探测器的情况下也会变化。每个系统或 VDB 更新的版本说明或咨询文本均包含有关任何新的和已更新的探测器的信息。有关探测器的全面最新列表，请参阅思科支持网站 (http://www.cisco.com/cisco/web/support/index.html)。

在此网络映射中，您可查看运行特定应用的每台主机的主机配置文件。

还可以删除任何应用类别、在所有主机上运行的任何应用或在特定主机上运行的任何应用。例如，如果知道应用在主机上已禁用并要确保系统不使用它进行影响级别限定，即可从网络映射中删除该应用。

从网络映射中删除应用不会将其从网络中移除。如果系统检测到应用发生变化（例如，如果 Apache 网络服务器升级到新版本），或者如果重新启动系统的发现功能，则网络映射中会重新显示已删除的应用。

视乎删除的内容，行为有所不同：

- 应用类别 - 删除应用类别会将其从网络映射中移除。驻留在该类别下的所有应用都会从包含应用的任何主机配置文件中移除。

  例如，如果删除 **http**，则会从所有主机配置文件中移除标识为 **http** 的所有应用，并且网络映射的应用视图中不再显示 **http**。

- 特定应用、供应商或版本 - 删除特定应用、供应商或版本会从网络映射中以及从包含该网络映射的任何主机配置文件中移除受影响的应用。

  例如，如果展开 **http** 类别并删除 **Apache**，则会从包含列为 Apache 的所有应用（具有 Apache 下列出的任何版本）的任何主机配置文件中移除这些应用。同样，如果删除特定版本（例如 **1.3.17**）而不是删除 **Apache**，则仅会将所选版本从受影响主机配置文件中删除。

- 特定 IP 地址 - 删除 IP 地址会将其从应用列表中移除，并从所选 IP 地址的主机配置文件中移除应用本身。

  例如，如果展开 **http**、**Apache**、**1.3.17 (Win32)**，然后删除 **172.16.1.50:80/tcp**，则会从 IP 地址 172.16.1.50 的主机配置文件中删除 Apache 1.3.17 (Win32) 应用。

漏洞网络映射

“漏洞”选项卡上的网络映射显示系统在网络中检测到的漏洞，按旧版漏洞 ID (SVID)、 CVE ID 或 Snort ID排列。

从此网络映射中，可查看特定漏洞的详细信息；还可查看受特定漏洞影响的任何主机的主机配置文件。此信息有助于评估该漏洞对特定受影响主机造成的威胁。

如果确定特定漏洞不适用于网络上的主机（例如，已应用补丁），则可停用漏洞。已停用的漏洞仍显示在网络映射中，但是其先前受影响主机的 IP 地址以灰色斜体显示。那些主机的主机配置文件将已停用的漏洞显示为无效，不过可以手动将其标记为对于个别主机有效。

如果主机上的应用或操作系统存在身份冲突，则系统会列出两种潜在身份的漏洞。解决身份冲突后，漏洞保持与当前身份关联。

默认情况下，仅当数据包包含应用的供应商和版本时，网络映射才会显示检测到的应用的漏洞。但是，可将系统配置为列出缺少供应商和版本数据的应用的漏洞，只需在 管理中心配置中为应用启用漏洞映射设置。

漏洞 ID（或漏洞 ID 的范围）旁边的数字表示两个计数：

受影响的主机

第一个数字是受漏洞影响的非唯一主机的计数。如果主机受多个漏洞影响，则会多次对其进行计数。因此，计数可能高于网络上的主机数。停用漏洞会按可能受该漏洞影响的主机数减小此计数。如果尚未面向漏洞或漏洞范围停用任何潜在受影响主机的任何漏洞，则不显示此计数。

可能受影响的主机

第二个数字是系统已确定为潜在受漏洞影响的非唯一主机的总数的计数。

停用漏洞致使其仅对指定的主机处于非活动状态。可停用已判定为易受攻击的所有主机或指定的个别易受攻击主机的漏洞。漏洞停用之后，适用的主机 IP 地址以灰色斜体显示在网络映射中。此外，这些主机的主机配置文件将已停用的漏洞显示为无效。

如果系统随后在主机上检测到未尚未停用的漏洞（例如，在网络映射中的新主机上），则系统会激活该主机的漏洞。必须明确停用最近发现的漏洞。此外，如果系统检测到主机的操作系统或应用变化，则可能重新激活关联的已停用漏洞。

主机属性网络映射

“主机属性”选项卡上的网络映射显示按用户定义的主机属性或合规 allow 名单主机属性组织的主机。您不能使用此显示中的预定义主机属性组织主机。

选择要用于组织主机的主机属性时，管理中心列出该属性在网络映射中的可能值并根据其分配值将主机分组。例如，如果选择按allow名单主机属性组织主机，则系统会在类别“合规”、“不合规”和“未评估”中显示这些主机。

还可查看为其分配了特定主机属性值的任何主机的主机配置文件。

相关主题

主机配置文件中的主机属性，第 845 页

查看网络映射

您必须是 管理员 或 安全分析师 用户才能查看网络映射。

过程

步骤 1 选择**分析** > **主机** > **网络映射**。

步骤 2 点击要查看的网络映射。

步骤 3 根据情况继续操作：

- 选择域 - 在多域部署中，从**域 (Domain)** 下拉列表中选择分叶域。
- 过滤主机 - 如果要按 IP 或 MAC 地址过滤，请在搜索字段中输入地址。要清除搜索，请点击 **清除**（✕）。
- 向下展开 - 如果要调查类别或主机配置文件，请向下展开映射中的类别或子网。如果已定义自定义拓扑，请点击 **主机** 中的 （**拓扑**） 以查看它，然后在要切换回默认视图时点击 （**主机**） 。
- 删除 - 点击相应元素旁边的 **删除**（🗑） 以执行下列操作：
  - 从**主机 (Hosts)**、**网络设备 (Network Devices)**、**移动设备 (Mobile Devices)** 或**应用协议 (Application Protocols)** 选项卡上的映射中删除元素。
  - 标记**危害表现 (Indications of Compromise)** 上解析的 IOC 类别、受损主机或受损主机组。
  - 停用**漏洞 (Vulnerabilities)** 上所有主机或单个主机的漏洞。
- 指定漏洞类 - 在 **漏洞**上，从 **类型** 下拉列表中选择要查看的漏洞的类。
- 指定组织属性 - 在**主机属性 (Host Attributes)** 上，从**属性 (Attribute)** 下拉列表中选择属性。

相关主题

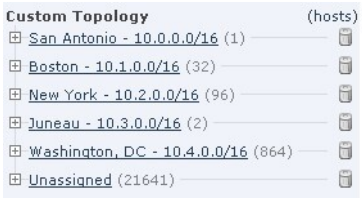
自定义网络拓扑，第 588 页
主机配置文件，第 830 页

自定义网络拓扑

使用自定义拓扑功能帮助排列和识别主机及网络设备网络映射中的子网。

例如，如果贵公司中的每个部门使用不同的子网，则可使用自定义拓扑功能标示这些子网。

也可根据在自定义拓扑中指定的公司查看主机网络映射。



您可以使用以下任何或所有策略指定自定义拓扑的网络：

- 您可以从网络发现策略导入网络，以添加您将系统配置为要监控的网络。
- 您可以手动向拓扑中添加网络。

“自定义拓扑”(Custom Topology) 页面列出自定义拓扑及其状态。如果策略名称旁边的灯泡图标亮起，表明拓扑处于活动状态并影响网络映射。如果该图标呈灰色显示，则表明拓扑处于不活动状态。

相关主题

主机网络映射，第 584 页
网络设备网络映射，第 585 页

创建自定义拓扑

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击工具栏中的**自定义拓扑 (Custom Topology)**。

步骤 3 点击 **Create Topology**。

步骤 4 输入 **Name**。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 向拓扑添加网络。可使用以下任何或所有策略：

- 从网络发现策略导入网络，如从网络发现策略导入网络，第 590 页中所述。
- 手动添加网络，如手动向自定义拓扑添加网络，第 590 页中所述。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 激活拓扑，如激活和停用自定义拓扑，第 591 页中所述。

从网络发现策略导入网络

过程

步骤 1 访问要将网络导入到的自定义拓扑：

- 创建自定义拓扑；请参阅创建自定义拓扑，第 589 页。
- 编辑现有自定义拓扑；请参阅编辑自定义拓扑，第 591 页。

步骤 2 点击**导入策略网络 (Import Policy Networks)**。

步骤 3 点击**加载 (Load)**。系统显示网络发现策略的拓扑信息。

步骤 4 优化拓扑：

- 通过点击网络旁边的 **编辑**（ ），键入名称并点击 **重命名**来对拓扑中的网络进行重命名。
- 通过点击 **删除**（ ），然后点击 **确定** 以确认来从拓扑中删除网络。

步骤 5 点击**保存 (Save)**。

下一步做什么

- 激活拓扑，如激活和停用自定义拓扑，第 591 页中所述。

手动向自定义拓扑添加网络

过程

步骤 1 访问您要添加网络的自定义拓扑：

- 创建自定义拓扑；请参阅创建自定义拓扑，第 589 页。
- 编辑现有自定义拓扑；请参阅编辑自定义拓扑，第 591 页。

步骤 2 点击 **Add Network**。

步骤 3 如果要将网络的自定义标签添加到主机和网络设备网络映射中，请键入**名称 (Name)**。

步骤 4 输入用于表示待添加网络的 **IP 地址**和**网络掩码** (IPv4)。

步骤 5 点击**添加 (Add)**。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 激活拓扑，如激活和停用自定义拓扑，第 591 页中所述。

相关主题

Firepower 系统 IP 地址约定，第 26 页

激活和停用自定义拓扑

注释 只有一个自定义拓扑可以随时处于活动状态。如已创建多个拓扑，则激活一个拓扑会自动停用当前活动的拓扑。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 选择**自定义拓扑 (Custom Topology)**。

步骤 3 点击拓扑旁边的滑块以激活或停用该拓扑。

编辑自定义拓扑

对活动拓扑进行的更改会立即生效。

过程

步骤 1 选择**策略** > **网络发现**。

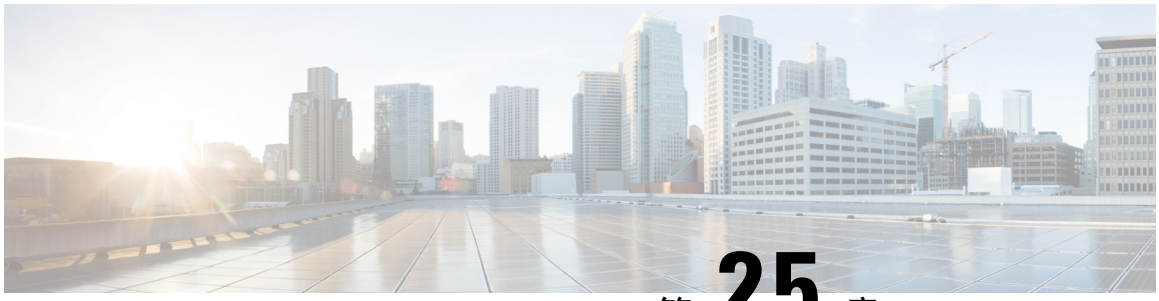
在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击**自定义拓扑 (Custom Topology)**。

步骤 3 点击要编辑的拓扑旁边的 **编辑**（ ）。

步骤 4 编辑拓扑，如创建自定义拓扑，第 589 页中所述。

步骤 5 点击**保存 (Save)**。



第 25 章

查找

以下主题介绍如何查找关于 Firepower 系统可能了解或可能不了解的实体的信息：

介绍查找

如果您的 管理中心已连接到互联网，则可以使用手动查找功能查找以下信息：

- 任何 IP 地址的区域信息注册表 (RIR) 信息 (whois)。
- URL 类别和信誉通过 URL 过滤功能分类。
- 任何 IP 地址的地理位置信息：国家/地区名称、国家/地区代码和大洲名称。（为了确保您使用的是最新的地理位置信息，思科强烈建议您定期更新 管理中心上的地理位置数据库 (GeoDB)。

执行 Whois 查找

开始之前

- 确保 管理中心能够访问互联网；请参阅安全、互联网接入和通信端口，第 1013 页。

过程

步骤 1 选择**分析** > **高级** > **Whois**。

步骤 2 输入 IP 地址，然后点击**搜索**。

查找 URL 类别和信誉

您可以手动查找 URL 的类别和信誉。使用此功能可以了解如何评估特定的 URL，以便计划、调整或解决策略处理问题，或者调查通过思科解决方案之外的源引起您注意的可能有问题的URL。这些结果中的类别和声望与 URL 过滤功能使用的类型和信誉相同。

开始之前

- 管理中心必须具有 Internet 访问权限；请参阅安全、互联网接入和通信端口，第 1013 页。
- 必须启用 URL 过滤和**向思科云查询未知 URL** 选项。请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 *URL* 过滤一章。
- 必须至少有一个设备注册到 管理中心，并且为其分配了有效的 URL 过滤 许可证。
- 您必须是管理员或安全分析师用户才能执行此任务。

过程

步骤 1 选择**分析** > **高级** > **URL**。

步骤 2 以任何通用格式输入多达 250 个 URL 和公共可路由的 IP 地址（例如，URL 可以包含或不包含“http”、“www”，可以是子域，也可以缩短)。用空格或回车分隔每个输入项。

不支持星号 (*) 这类通配符。

步骤 3 点击 **Search**。

如果输入了很多 URL，并且网络速度很慢，处理可能需要几分钟的时间。

如果看到 URL 无效的错误信息，请检查拼写或尝试不同的 URL 形式。例如，添加或省略“www”或“http(s)”前缀。

一个 URL 可能属于多达六类别，但只有一个声誉。

步骤 4 （可选）通过点击列标题对结果进行排序。

步骤 5 （可选）要将结果保存为 CSV 文件，请点击**导出 CSV**。

CSV 文件中包含一个用于名誉级别的附加列，因此您可以按风险排序。对于系统风险数据不足的 URL，零 (0) 表示未知风险。

下一步做什么

如果要查看可能的类别和信誉列表，请转到**策略 (Policies)** > **访问控制 (Access Control)** > **访问控制 (Access Control)**，点击策略或添加新的策略，点击**添加规则 (Add Rule)**，然后点击 **URL**。

查找 IP 地址的地理位置信息

可以使用地理位置查找功能来查找国家/地区名称、ISO 3166-1 三位数字的国家/地区代码，以及与任何 IP 地址相关联的大陆名称。

过程

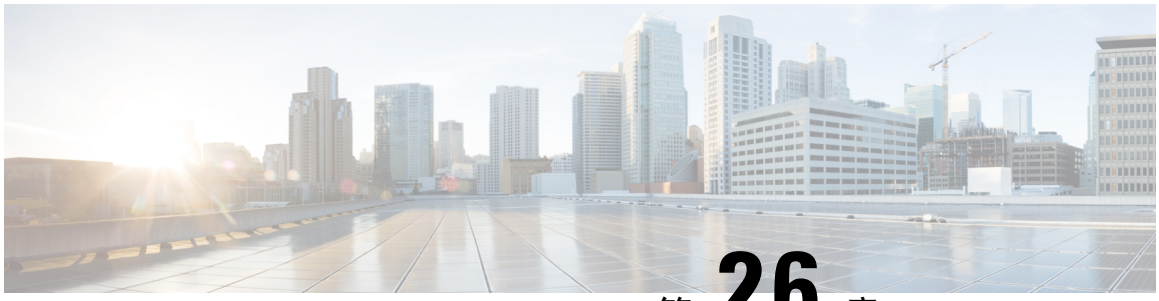
步骤 1 选择**分析** > **高级** > **地理位置**。

步骤 2 要查看一个或多个 IP 地址的地理位置信息，请输入该地址或这些地址，然后点击**搜索**。可以指定 IPv4 地址、IPv6 地址，或者二者。使用逗号、分号、回车或任何空格字符来分隔多个地址。

提示 点击**清除**以清除文本框。

步骤 3 或者，可以点击列标题对数据进行排序。可按除“IP 地址”外的任何字段进行排序。

步骤 4 （可选）要将结果另存为 CSV 文件，请点击**导出 CSV**。



第 26 章

使用外部工具的事件分析

与思科 SecureX集成

通过单一管理平台（SecureX 云门户）查看和处理所有思科安全产品及其他产品的数据。使用SecureX可用的工具来丰富您的威胁追踪和调查。 SecureX 还可以提供有用的设备和设备信息，例如每个设备和设备是否正在运行最佳软件版本。

有关 SecureX的详细信息，请参阅思科 SecureX 页面。

启用 SecureX 集成

思科 SecureX 结合了思科的集成安全产品组合以及您的基础设施的优势，旨在提供可统一可视性、实现自动化并增强网络、终端、云和应用安全性的一致体验。有关 SecureX 的详细信息，请参阅思科 SecureX 产品页面。

通过将 SecureX 与 管理中心 集成，您可以全面了解 管理中心 中的所有数据。有关将 管理中心 与SecureX集成的更多信息，请参阅 Cisco Secure Firewall Management Center (版本 7.2 或更高) 和 SecureX 集成指南。

开始之前

您需要一个属于组织的 SecureX 账户。如果没有 SecureX 帐户，请使用 CDO 租户创建 SecureX 帐户。有关详细信息，请参阅使用 CDO 创建 SecureX 帐户。

过程

步骤 1 在 管理中心 中，选择**集成 (Integration)** > **SecureX**。

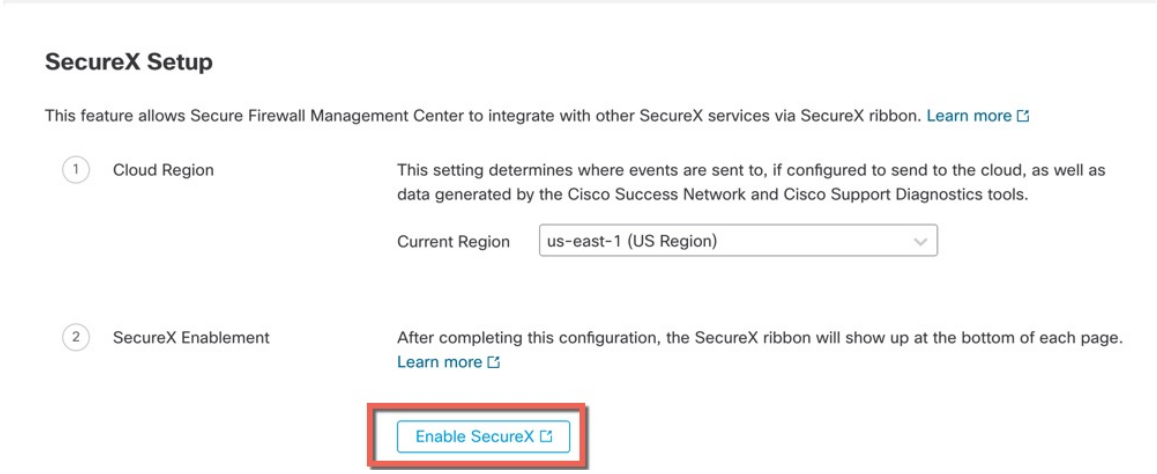
步骤 2 （可选） 对于**云区域 (Cloud Region)**，请选择您的**当前区域 (Current Region)**。

默认情况下，选择的区域与您的智能许可区域匹配，因此您可能不需要更改区域。

步骤 3 在 **SecureX 启用 (SecureX Enablement)** 中，执行以下步骤。

a) 点击**启用 SecureX (Enable SecureX)**。

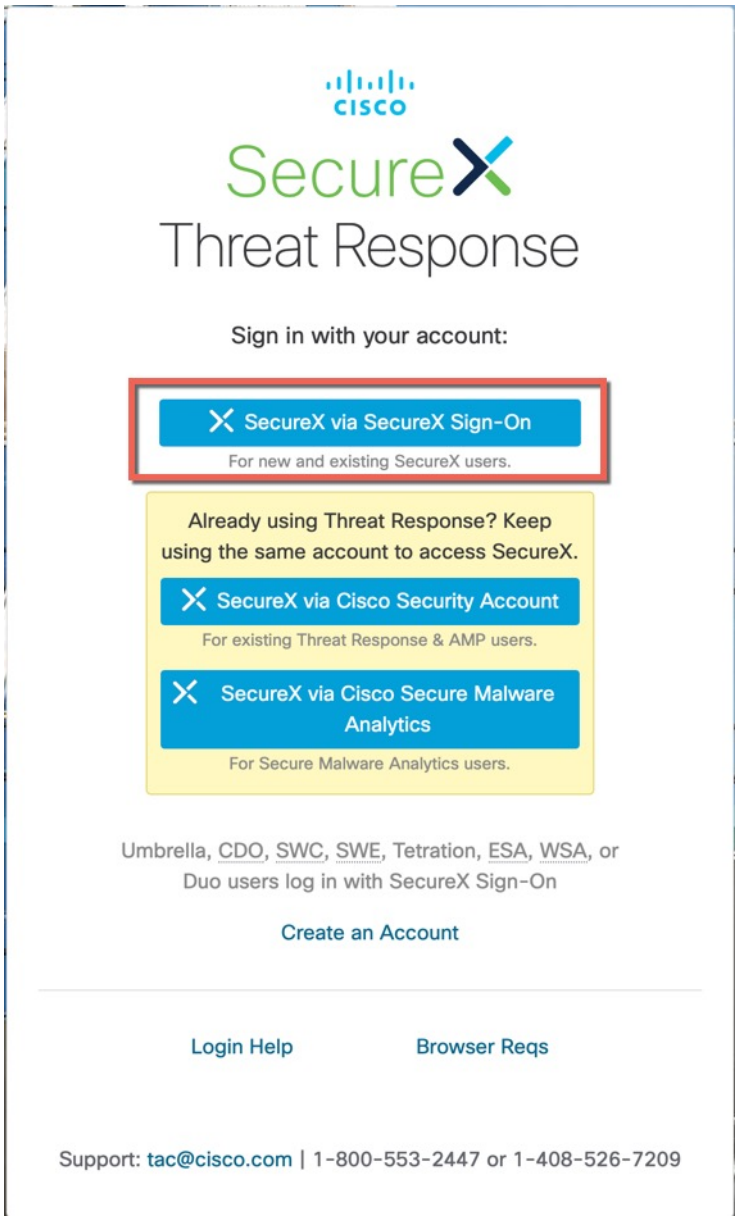
图 *18:* 启用 *SecureX*



b) 登录 SecureX。

系统将打开一个单独的浏览器选项卡或窗口，供您登录SecureX账户。确保此页面未被弹出窗口阻止程序阻止。

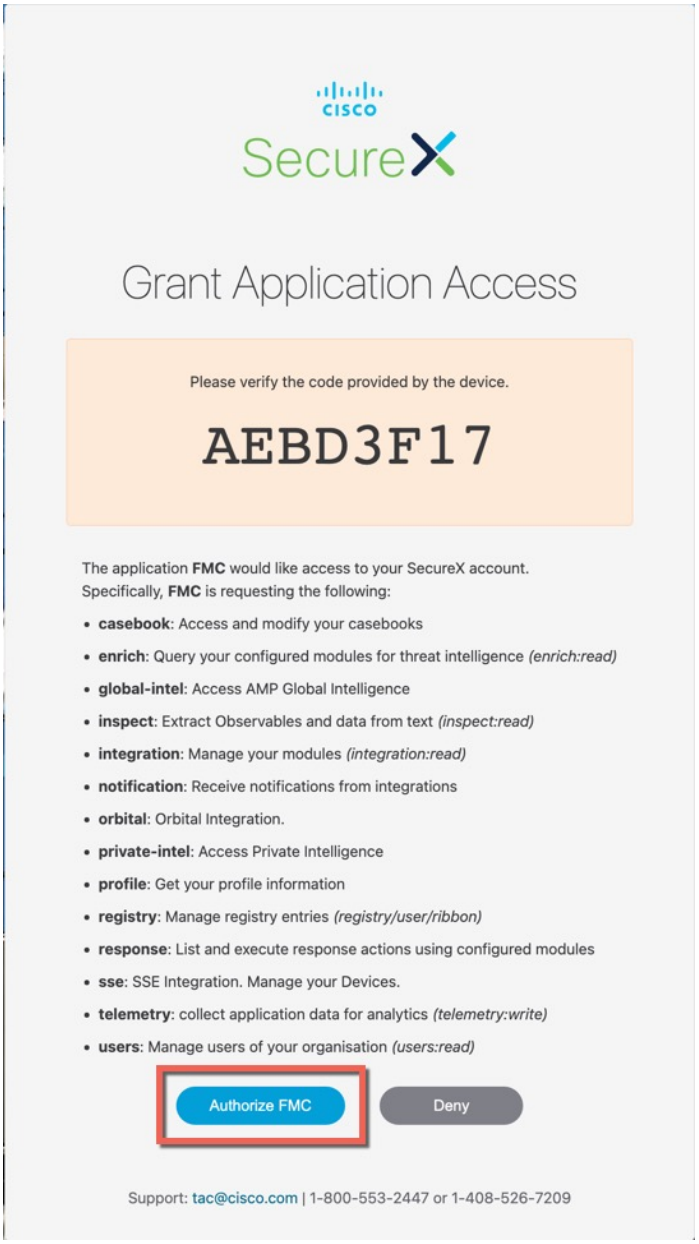
图 *19: SecureX* 登录



c) 点击**授权 FMC (Authorize FMC)**。

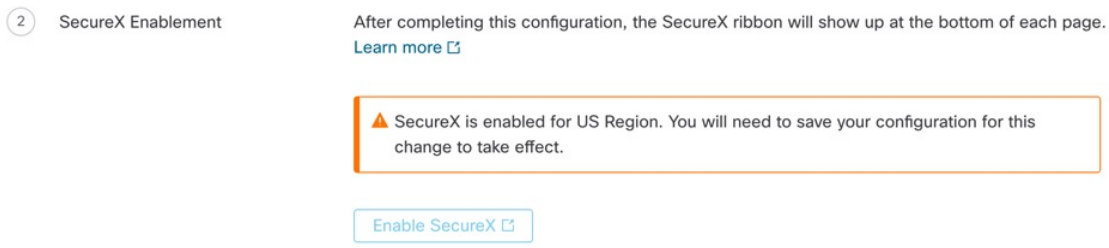
您将看到一个代码，该代码应与 管理中心中显示的代码匹配。

图 *20:* 授予应用访问权限



d) 管理中心 与 SecureX 集成后，您会看到一条成功消息。点击**保存 (Save)**。

图 *21:* 成功消息



配置 管理中心 以便将事件发送到 思科安全云

将 管理中心 配置为托管 威胁防御 设备直接将事件发送至 思科安全云。在适用和启用的情况下，您在此页面中配置的云区域和事件类型可用于多个集成。

开始之前

- 确保使用智能许可证（**系统**（⚙）>**智能许可证**）注册管理中心或启用 思科安全云 集成，以便让设备能够将防火墙事件发送到思科云。
- 在 管理中心 中：
  - 转至**系统 (System)** > **配置 (Configuration)** 页面并为 管理中心 提供唯一名称，以便其可在云中的**设备 (Devices)** 列表中明确识别。
  - 将您的 威胁防御 设备添加到 管理中心，向其分配许可证，并确保系统正常运行。确保您已创建必要的策略，生成的事件如在 管理中心 UI 中的**分析 (Analysis)** 菜单下如预期那样显示。
- 请确保您拥有思科安全云登录凭证，并且可以登录到创建您的账户的 SecureX 区域云。

  有关 SecureX 区域云 URL 和支持的设备版本的详细信息，请参阅 思科 Cisco Secure Firewall Management Center 和 SecureX集成指南。
- 如果您当前使用系统日志将事件发送到云，请禁用这以避免重复。

过程

步骤 1 确定要用于发送防火墙事件的思科区域云。有关选择区域云的详细信息，请参阅 思科 Cisco Secure Firewall Management Center 和 SecureX 集成指南。

注释 如果 SecureX 已启用，并且 管理中心 已注册到所选区域云，则更改区域云会禁用 SecureX。您可以在更改区域云后再次启用 SecureX 。

步骤 2 在 管理中心 中，点击**集成 (Integration)** > **SecureX**。

步骤 3 从**当前区域 (Current Region)** 下拉列表中选择区域云。

步骤 4 选中**将事件发送到云 (Send events to the cloud)** 复选框以启用云事件配置。

步骤 5 选择要发送至云的事件类型。

注释 您发送到云端的事件可用于多个集成，如下表所示。

集成	受支持的事件选项	备注
思科安全分析和日志记录 (SaaS)	全部	高优先级连接事件包括： • 安全相关 连接事件 • 与文件和恶意软件事件相关的连接事件 • 与入侵事件相关的连接事件
思科 SecureX 和 思科 SecureX 威胁响应	取决于您的版本： • 安全相关的连接事件。 • 入侵事件。 • 文件和恶意软件事件。	即使您发送所有连接事件，思科 SecureX 和 思科 SecureX 威胁响应 仅支持安全相关的连接事件。

注释
- 如果 **启用入侵事件**， 管理中心 会随影响标志一起发送事件。
- 如果启用**文件和恶意软件事件 (File and Malware Events)**，除了从 威胁防御 设备发送的事件外，管理中心 还会发送追溯性事件。

步骤 6 点击**保存 (Save)**。

配置 Cisco Success Network 注册

Cisco Success Network 是一项云服务，使 管理中心 能够与思科云建立安全连接，并流式传输使用信息和统计信息。此数据流遥测提供一种机制，可从 威胁防御 设备选择相关数据，并出于以下原因以结构化的格式将其发送至远程管理站：

- 通知您在网络中可用来改进产品效果但尚未使用的功能。
- 通知您适用于您产品的其他技术支持服务和监控。
- （如果与SecureX集成）在SecureX磁贴中汇总设备和设备状态，并了解所有设备是否都在运行最佳软件版本。
- 帮助思科改善产品。

要了解有关思科收集的遥测数据的更多信息，请参阅 从 Cisco Secure Firewall Management Center 设备收集的 Cisco Success Network 遥测数据。

当您启用思科支持诊断或 Cisco Success Network 时， 管理中心 会始终建立并维护与思科云的安全连接。但是，当您启用思科支持诊断时，管理中心 和 威胁防御 设备都会建立并维护与思科云的安全连接。您可以随时通过禁用 Cisco Success Network 和思科支持诊断功能来关闭该连接，这样会将 管理中心 与思科云断开。

将管理中心注册到智能软件管理器时，可启用 Cisco Success Network。

注释

- Cisco Success Network 在评估模式下不支持。
-
- 如果管理中心具有有效的智能软件管理器本地版（之前称为“智能软件卫星服务器”）配置或使用特定许可证预留，Cisco Success Network 将被禁用。

开始之前

启用 SecureX集成或使用智能许可证注册您的管理中心，以执行此任务。

过程

步骤 1 点击 **集成** > **SecureX**。

步骤 2 在 **思科云支持**下，选中 **启用 Cisco Success Network (Enable Cisco Success Network)** 复选框以启用此服务。

注释 在继续之前，请阅读**启用 Cisco Success Network (Enable Cisco Success Network)** 复选框旁边提供的信息。

步骤 3 点击**保存 (Save)**。

配置思科支持诊断注册

思科支持诊断是一项用户启用的基于云的 TAC 支持服务。启用后， 管理中心 和托管设备会与思科云建立安全连接，以传输与系统运行状况相关的信息。

思科支持诊断通过允许思科 TAC 在解决 TAC 案例期间从您的设备安全地收集重要数据，在故障排除期间提供增强的用户体验。此外，思科会定期收集运行状况数据，并使用自动问题检测系统处理这些数据，以便在出现问题时通知您。虽然解决 TAC 案例期间的数据收集服务适用于拥有支持合同的所有用户，但通知服务仅适用于拥有特定服务合同的用户。

思科支持诊断功能允许 威胁防御 设备和 管理中心 建立并维护与思科云的安全连接。管理中心 会将收集的数据发送到 **SecureX 集成 (SecureX Integration)** 页面上选定的区域。

您可以随时通过禁用 Cisco Success Network 和思科支持诊断功能来关闭该连接，这样会将这些功能与思科云断开。

管理员可以按照 为特定系统功能生成故障排除文件中的步骤来查看从管理中心收集的简单数据集。

开始之前

启用 SecureX集成或使用智能许可证注册您的管理中心，以执行此任务。

过程

步骤 1 点击 **集成** > **SecureX**。

步骤 2 在 **思科云支持**下，选中 **启用思科支持诊断** 复选框以启用此服务。

注释 在继续之前，请参阅 **启用思科支持诊断** 复选框旁边提供的信息。

步骤 3 点击**保存 (Save)**。

使用 Ribbon 访问 SecureX

功能区显示在管理中心 Web 界面中每个页面的底部。您可以使用功能区快速跳转到其他思科安全产品，并处理来自多个来源的威胁数据。

开始之前

- 如果在 管理中心 Web 界面页面的底部没有看到 SecureX 功能区，请不要使用此程序。

  相反，请参阅 Cisco Secure Firewall Threat Defense 和 SecureX 集成指南。

- 如果您还没有 SecureX 账户，请从您的 IT 部门获取一个。

过程

步骤 1 在 管理中心中，点击任何 管理中心 页面底部的功能区。

步骤 2 点击 **获取 SecureX**。

步骤 3 登录到 SecureX。

步骤 4 点击链接以授权访问。

步骤 5 点击功能区以展开并使用它。

下一步做什么

有关功能区功能及其使用方法的信息，请参阅 SecureX 中的在线帮助。

使用的事件分析 SecureX 威胁响应

SecureX 威胁响应 以前称为思科威胁响应 (CTR)。

使用思科云中的集成平台 SecureX 威胁响应可快速检测、调查和响应威胁，让您可以使用从多个产品汇聚的数据分析事件，包括 Cisco Secure Firewall。

- 有关 SecureX 威胁响应的一般信息，请参阅：

  思科 SecureX 威胁响应产品页面。

- 有关将 SecureX 威胁响应到集成 Firepower 的详细说明，请参阅：
- 请参阅 Cisco Secure Firewall Threat Defense 和思科 SecureX 集成指南。

查看 SecureX 威胁响应中的事件数据

开始之前

- 按照 Cisco Secure Firewall Threat Defense 和思科 SecureX 威胁响应集成指南中的说明设置集成。
- 查看 SecureX 威胁响应 中的联机帮助，了解如何查找、调查威胁并对其采取措施。
- 您将需要您的凭证才能访问 SecureX 威胁响应。

过程

步骤 1 在 Cisco Secure Firewall Management Center中，执行以下操作：

- 要从特定事件跳转到 SecureX 威胁响应，请执行以下操作：

  a. 导航到**分析 > 入侵**菜单下列出受支持事件的页面。

  b. 右键点击源或目标 IP 地址，然后选择**威胁响应 IP (Thereat Response IP)**。

步骤 2 按提示登录到 SecureX 威胁响应。

使用基于 Web 的资源的事件调查

使用上下文交叉启动功能可在 Cisco Secure Firewall Management Center以外快速查找有关基于 Web 的资源中的潜在威胁的更多信息。例如，您可以：

- 在思科或第三方云托管服务中查找可疑源 IP 地址，所述服务发布有关已知和可疑威胁的信息；或

- 在您组织的历史日志中查找特定威胁的以往实例，前提是您的组织将这些数据存储在安全信息和事件管理 (SIEM) 应用中。
- 查找有关特定文件的信息（包括文件轨迹信息），前提是您的组织已部署思科 Cisco Secure Endpoint。

调查事件时，您可以直接从 Cisco Secure Firewall Management Center中的事件查看器或控制面板中点击某个事件以转到外部资源中的相关信息。这样，您可以根据 IP 地址、端口、协议、域和/或 SHA 256 散列值快速收集有关特定事件的背景信息。

例如，假设您正在查看“排名靠前的攻击者”控制面板构件，并希望查找有关其中一个所列源 IP 地址的更多信息。您想要查看 Talos 发布了哪些有关此 IP 地址的信息，因此您选择“Talos IP”资源。Talos 网站将打开一个页面，其中包含有关此特定 IP 地址的信息。

您可以从一组预定义的常用思科和第三方威胁情报服务的链接中进行选择，并可以添加指向其他基于 Web 的服务的自定义链接，以及指向 SIEM 或其他具有 Web 界面的产品的自定义链接。请注意，某些资源可能需要拥有账户或购买产品。

关于管理上下文交叉启动资源

使用**分析 > 高级 > 上下文交叉启动**页面管理基于 Web 的外部资源。

例外：按照 配置交叉启动链接 Secure Network Analytics，第 608 页中的程序管理 Secure Network Analytics 设备的交叉启动链路。

思科提供的预定义资源标注有思科徽标。其余链接是第三方资源。

您可以禁用或删除任何不需要的资源，也可以重命名这些资源，例如通过在名称前面加上小写“z”，这样这些资源便排序在列表底部。禁用交叉启动资源将对所有用户禁用。您无法恢复已删除的资源，但可以重新创建这些资源。

要添加资源，请参阅添加上下文交叉启动资源，第 607 页。

自定义上下文交叉启动资源的要求

添加自定义上下文交叉启动资源时：

- 资源必须可通过网络浏览器访问。
- 仅支持 http 和 https 协议。
- 仅支持 GET 请求；不支持 POST 请求。
- 不支持在 URL 中编码变量。虽然 IPv6 地址可能需要编码冒号分隔符，但大多数服务都不需要这种编码。
- 最多可以配置 100 个资源，包括预定义的资源。
- 您必须是 管理员 或 安全分析师 用户才能创建交叉启动，但也可以是只读 安全分析师 才能使用它们。

添加上下文交叉启动资源

您可以添加上下文交叉启动资源，例如威胁情报服务以及安全信息和事件管理 (SIEM) 工具。

在多域部署中，您可以在父域中查看和使用资源，但您只能在当前域中创建和编辑资源。 所有域中的资源总数限制为 100。

开始之前

- 如果要向 Secure Network Analytics 设备添加链路， 请检查所需的链路是否已存在；配置 安全分析和日志记录（本地部署）时，系统会自动为您创建大多数链路，。
- 请参阅自定义上下文交叉启动资源的要求，第 606 页。
- 如果将链接到的资源需要，请创建或获取账户以及访问所需的凭证。或者，为每个需要访问权限的用户分配和分发凭证。
- 确定您将链接到的资源的查询链接的语法：

  通过浏览器访问资源，并根据需要使用该资源的文档来编制查询链接，搜索您希望查询链接查找的信息类型的特定示例需要此查询链接，例如 IP 地址。

  运行查询，然后从浏览器的位置栏复制生成的 URL。

  例如，查询的 URL 可能为：
  `https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10`。

过程

步骤 1 选择**分析 > 高级 > 上下文交叉启动**。

步骤 2 点击**新建交叉启动 (New Cross-Launch)**。

在显示的表单中，所有标记星号的字段必须填写值。

步骤 3 输入唯一的资源名称。

步骤 4 将资源中的有效 URL 字符串粘贴到 **URL 模板**字段中。

步骤 5 使用适当的变量替换查询字符串中的特定数据（例如 IP 地址）：将光标置于相应位置，然后点击变量（例如， **ip**）一次以插入变量。

在上方“开始之前”部分中的示例中，生成的 URL 可能是：
`https://www.talosintelligence.com/reputation_center/lookup?search={ip}`。
使用上下文交叉启动链接时，URL 中的 {ip} 变量将替换为用户在事件查看器或控制面板中右键点击的 IP 地址。

要查看每个变量的说明，请将鼠标悬停在变量上。

您可以为单个工具或服务创建多个上下文交叉启动链接，为每个链接使用不同的变量。

步骤 6 点击 **使用示例数据测试** （） 以使用示例数据测试您的链接。

步骤 7 修复任何问题。

步骤 8 点击**保存 (Save)**。

使用上下文交叉启动调查事件

开始之前

如果您将访问的资源需要凭证，请确保您具有这些凭证。

过程

步骤 1 导航到 Cisco Secure Firewall Management Center中显示事件的以下其中一个页面：

- 控制面板（**概述 > 控制面板**），或
- 事件查看器页面（**分析**菜单下包括事件表的任何菜单选项。）

步骤 2 右键点击感兴趣的事件，然后选择要使用的上下文交叉启动资源。

如有必要，在上下文菜单中向下滚动以查看所有可用选项。

右键点击的数据类型决定了您可看到的选项；例如，如果您右键点击 IP 地址，则只能看到与 IP 地址相关的上下文交叉启动选项。

例如，要从思科 Talos 获取有关入侵事件中的源 IP 地址的威胁情报，请选择 **Talos SrcIP** 或 **Talos IP**。

如果资源包括多个变量，则用于选择该资源的选项仅适用于对于每个包含的变量只有单个可能值的事件。

上下文交叉启动资源将在单独的浏览器窗口中打开。

处理查询可能需要一些时间，具体取决于待查询的数据量、资源的速度和需求等。

步骤 3 必要时登录资源。

配置交叉启动链接 Secure Network Analytics

您还可以从 Cisco Secure Firewall Threat Defense 中的事件交叉启动，以查看 Secure Network Analytics 设备上的相关数据。有关 Secure Network Analytics 产品的详细信息，请参阅思科安全分析和日志记录产品页面。

有关上下文交叉启动的一般信息，请参阅 使用上下文交叉启动调查事件，第 608 页。

使用此程序可配置一组指向 Secure Network Analytics 设备的交叉启动链路。

注释

- 如果稍后要对这些链接进行更改，请返回到此程序；您无法直接在上下文交叉启动列表页面上进行更改。
- 您可以使用添加上下文交叉启动资源，第607页中的程序手动创建其他链接以交叉启动到Secure Network Analytics 设备中，但这些链接仍独立于自动创建的资源，您必须手动管理它们。

开始之前

- 您必须部署并运行 Secure Network Analytics 设备。
- 如果您当前使用系统日志将事件从支持直接发送事件的设备版本发送到Secure Network Analytics，请禁用这些设备的系统日志（或为这些设备分配不包含系统日志配置的访问控制策略），以避免在远程卷上复制事件。
- 您必须具备以下条件：
  - 管理器的主机名或 IP 地址。
  - Secure Network Analytics 设备上具有管理员权限的帐户的凭证。

如果要使用 安全分析和日志记录（本地部署） 将 Cisco Secure Firewall Threat Defense 数据发送到 Secure Network Analytics 设备，请参阅 Secure Network Analytics 设备上的远程数据存储，第 498 页。

过程

步骤 1 依次选择 。

步骤 2 您的 Secure Network Analytics 部署有两个选项：

- 仅限管理器 - 部署独立管理器以接收和存储事件，您可以从中查看和查询事件。
- 数据存储 - 部署用于接收事件的思科 Secure Network Analytics 流量收集器、用于存储事件的 Secure Network Analytics 数据存储以及用于查看和查询事件的管理器。

选择部署选项，然后点击**开始 (Start)**。

步骤 3 完成向导。有关详细信息，请参阅《思科安全分析和日志记录防火墙集成指南》中的 Cisco Secure Firewall Management Center 配置部分。

步骤 4 验证新的交叉启动链接：选择 **分析 > 高级 > 上下文交叉启动**。

如果要进行更改，请返回此程序；您无法直接在上下文交叉启动列表页面上进行更改。

下一步做什么

使用 Secure Network Analytics 凭证从事件交叉启动到 Secure Network Analytics 事件查看器。

要从管理中心事件查看器或控制面板中的事件交叉启动，请右键点击相关事件的表格单元格，然后选择相应的选项。

处理查询可能需要一些时间，具体取决于需要处理的数据量、Cisco Secure Network Analytics 管理器上的速度和需求等。

关于发送 安全事件的系统日志消息

您可以通过系统日志将与连接、 安全情报、入侵以及文件和恶意软件事件 相关的数据发送到安全信息和事件管理 (SIEM) 工具或其他外部事件存储和管理解决方案，例如。

这些事件有时也称为 Snort® 事件。

关于配置系统以向系统日志发送安全事件数据

为了配置系统以发送安全事件系统日志，您需要了解以下内容：

- 配置安全事件系统日志消息的最佳实践，第 610 页
- 安全事件系统日志的配置位置，第 615 页
- 在《Cisco Secure Firewall Management Center 设备配置指南》中的适用于安全事件系统日志消息的 *FTD* 平台设置
- 如果在任何策略中更改系统日志设置，则必须重新部署才能使更改生效。

配置安全事件系统日志消息的最佳实践

设备和版本	配置位置
所有 (All)	如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。

设备和版本	配置位置
Cisco Secure Firewall Threat Defense	1. 完成下列事项来配置 威胁防御 平台设置：（**设备 > 平台设置 > 威胁防御设置 > 系统日志**。） 1. 点击 **设备** > **平台设置**。 2. 编辑威胁防御设置策略。 3. 在左侧导航窗格中，点击 **系统日志**。 也请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 适用于安全事件系统日志消息的威胁防御平台设置 。 2. 在访问控制策略“日志记录”选项卡中，选择使用 威胁防御 平台设置。 3. （对于入侵事件）将入侵策略配置为使用访问控制策略“日志记录”选项卡中的设置。（这是默认。） 不建议覆盖其中任何设置。 有关基本信息，请参阅 从 威胁防御 设备发送安全事件系统日志消息，第 611 页。
所有其他设备	1. 创建警报响应 2. 配置访问控制策略日志记录以使用警报响应。 3. （对于入侵事件）在入侵策略中配置系统日志设置。 有关完整的详细信息，请参阅 从经典设备发送安全事件系统日志消息，第 614 页。

从 威胁防御 设备发送安全事件系统日志消息

此程序记录从 威胁防御 管理的 Cisco Secure Firewall Management Center设备。

注释 许多 威胁防御 系统日志设置不适用于安全事件。仅配置此程序中所述的选项。

开始之前

- 在 Cisco Secure Firewall Management Center中，配置策略以生成安全事件，并验证您希望看到的事件显示在“分析”菜单下的适用表中。
- 收集系统日志服务器 IP 地址，端口和协议（UDP 或 TCP）：
- 确保您的设备可以访问系统日志服务器。

- 确认系统日志服务器可接受远程消息。
- 有关连接日志的重要信息，请参阅 连接日志记录， 第 699 页的章节。

过程

步骤 1 为 威胁防御 设备配置系统日志设置：

a) 点击 **设备 > 平台设置**。
b) **编辑** 与 威胁防御 设备关联的平台设置策略。
c) 在左侧导航窗格中，点击 **系统日志**。
d) 点击**系统日志服务器 (Syslog Servers)**，然后点击 **添加**（+） 以输入服务器、协议、接口和相关信息。

如果您对此页面上的选项有任何疑问，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

e) 点击 **系统日志设置** 并配置以下设置：
   - **在系统日志消息中启用时间戳**
   - **时间戳格式**
   - **启用系统日志设备 ID**
f) 点击 **日志记录设置**。
g) 在**基本日志记录设置 (Basic Logging Settings)** 中，选择是否要**以 EMBLEM 格式发送系统日志 (Send syslogs in EMBLEM format)**。
h) 点击**保存 (Save)** 以保存您的设置。

步骤 2 配置访问控制策略的常规日志记录设置（包括文件和恶意软件日志记录）：

a) 点击 **策略 (Policies) > 访问控制 (Access Control)**。
b) 编辑适用的访问控制策略。
c) 点击**更多 (More)** > **日志记录 (Logging)**。
d) 威胁防御 6.3 及更高版本：选择**使用在设备上部署的威胁防御平台设置策略中配置的系统日志设置**。
e) （可选）选择 **系统日志严重性**。
f) 如果要发送文件和恶意软件事件，选择**为文件和恶意软件事件发送系统日志消息 (Send Syslog messages for File and Malware events)**。
g) 点击**保存 (Save)**。

步骤 3 为访问控制策略启用安全情报事件日志记录：

a) 在同一访问控制策略中，点击 **安全情报** 选项卡。
b) 在以下每个位置，点击 **日志记录**（ ） 并启用连接的开始和结束和 **系统日志服务器**：
   - 在 **DNS 策略** 旁边。

- 在 **阻止列表** 框中，对于 **网络** 和对于 **URL**。

c) 点击**保存 (Save)**。

步骤 4 为访问控制策略中的每个规则启用系统日志记录：

a) 在同一访问控制策略中，点击**访问控制 (Access Control)** > **添加规则 (Add Rule)**。
b) 选择一条规则进行编辑。
c) 点击规则中的**日志记录 (Logging)** 选项卡。
d) 选择是记录连接的开始还是结束，或者同时选择两者。

（连接日志记录会生成大量数据；记录开始和结束时会生成大约两倍的数据。并非在开始和结束时都可以记录每个连接。）

e) 如果要记录文件事件，请选择 **日志文件**。
f) 启用 **系统日志服务器**。
g) 验证规则是“**在访问控制日志记录中使用默认系统日志配置**”。
h) 点击 **Confirm**。
i) 对策略中的每个规则重复上述步骤。

步骤 5 如果发送入侵事件：

a) 导航至与访问控制策略关联的入侵策略。
b) 在入侵策略中，点击 **高级设置** > **系统日志警报** > **已启用**。
c) 如有必要，请点击 **编辑**
d) 输入选项：

选项	值
日志记录主机	除非将入侵事件系统日志消息发送到与其他系统日志消息不同的系统日志服务器，否则将此字段留空以使用您在上面配置的设置。
设施	仅当您在此页面上指定日志记录主机时，此设置才适用。 有关说明，请参阅系统日志警报设施，第 535 页。
严重性	仅当您在此页面上指定日志记录主机时，此设置才适用。 有关说明，请参阅系统日志严重性级别，第 536 页。

e) 点击 **Back**（返回）。
f) 点击左侧导航窗格中 **策略信息** 。
g) 点击**确认更改 (Commit Changes)**。

下一步做什么

- （可选）为单个策略和规则配置不同的日志记录设置。

请参阅 管理中心 联机帮助中 连接和安全情报事件系统日志的配置位置（所有设备），第 615 页。

这些设置需要系统日志警报响应，其配置如 创建系统日志警报响应，第 534 页中所述。它们不使用您在此程序中配置的平台设置。

- 要配置典型设备的安全事件系统日志记录，请参阅 从经典设备发送安全事件系统日志消息，第 614 页。
- 如果完成更改，请将更改部署到受管设备。

从经典设备发送安全事件系统日志消息

开始之前

- 配置策略以生成安全事件。
- 确保您的设备可以访问系统日志服务器。
- 确认系统日志服务器可接受远程消息。
- 有关连接日志的重要信息，请参阅 连接日志记录，第 699 页的章节。

过程

步骤 1 为经典设备配置警报响应：

请参阅创建系统日志警报响应，第 534 页。

步骤 2 在访问控制策略中配置系统日志设置：

a) 点击 **策略 (Policies) > 访问控制 (Access Control)**。
b) 编辑适用的访问控制策略。
c) 点击 **日志记录 (Logging)**。
d) 选择 **使用特定系统日志警报发送**。
e) 选择您在上面创建的 **系统日志警报** 。
f) 点击**保存 (Save)**。

步骤 3 如果您将发送文件和恶意软件事件：

a) 选择 **发送文件和恶意软件事件的系统日志消息**。
b) 点击**保存 (Save)**。

步骤 4 如果您将发送入侵事件：

a) 导航至与访问控制策略关联的入侵策略。
b) 在入侵策略中，点击 **高级设置 > 系统日志警报 > 已启用**。
c) 如有必要，请点击 **编辑**
d) 输入选项：

选项	值
日志记录主机	除非将入侵事件系统日志消息发送到与其他系统日志消息不同的系统日志服务器，否则将此字段留空以使用您在上面配置的设置。
设施	仅当您在此页面上指定日志记录主机时，此设置才适用。 请参阅系统日志警报设施，第 535 页。
严重性	仅当您在此页面上指定日志记录主机时，此设置才适用。 请参阅系统日志严重性级别，第 536 页。

e) 点击 **Back**（返回）。
f) 点击左侧导航窗格中 **策略信息** 。
g) 点击**确认更改 (Commit Changes)**。

下一步做什么

- （可选）为各个访问控制规则配置不同的日志记录设置。请参阅 连接和安全情报事件系统日志的配置位置（所有设备），第 615 页中适用的表行。这些设置需要系统日志警报响应，其配置如 创建系统日志警报响应，第 534 页中所述。它们不使用您上面配置的设置。
- 要为 FTD 设备配置安全事件系统日志记录，请参阅 从 威胁防御 设备发送安全事件系统日志消息，第 611 页。

安全事件系统日志的配置位置

- 连接和安全情报事件系统日志的配置位置（所有设备），第 615 页
- 入侵事件系统日志的配置位置（FTD 设备），第 617 页
- 入侵事件系统日志的配置位置（非 FTD 设备），第 618 页
- 文件和恶意软件事件系统日志的配置位置，第 618 页

连接和安全情报事件系统日志的配置位置（所有设备）

有许多位置可配置日志记录设置。使用下表来确保设置所需的选项。

重要事项

- 配置系统日志设置时，尤其是在使用其他配置的继承默认设置时要特别注意。某些选项可能无法用于所有受管设备型号和软件版本，如下表所示。
- 有关配置连接日志记录的重要信息，请参阅连接日志记录，第 699 页一章。

配置位置	说明和更多信息
设备 > 平台设置，威胁防御设置策略，**系统日志**	此选项仅适用于 威胁防御 设备。 您在此处配置的设置可以在访问控制策略的日志记录设置中指定，然后在此表的其余策略和规则中使用或覆盖。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。
策略 > 访问控制，<每个策略>，**日志记录**	您在此处配置的设置是所有连接和安全情报事件的系统日志的默认设置，除非您在此表的其余行中指定的位置处覆盖后代策略和规则中的默认设置。 威胁防御 设备的建议设置：使用威胁防御平台设置。有关信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。 所有其他设备的必需设置：使用系统日志警报。 如果您指定系统日志警报，请参阅创建系统日志警报响应，第 534 页。 有关“日志记录”选项卡上的设置的详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》 。
策略> 访问控制，<每个策略>，**规则**， **默认操作** 行， **日志记录**（ ）	与访问控制策略关联的默认操作的日志记录设置。 请参阅有关登录 《Cisco Secure Firewall Management Center 设备配置指南》 和 使用策略默认操作记录连接，第 713 页 的信息。
策略 > 访问控制，<每个策略>，**规则**，<每个规则>， **登录**	访问控制策略中特定规则的日志记录设置。 请参阅有关登录到 《Cisco Secure Firewall Management Center 设备配置指南》 的信息。
策略 > 访问控制，<每个策略>，**安全情报**， **日志记录**（ ）	安全情报阻止列表的日志记录设置。 点击这些按钮可配置： • DNS 阻止列表日志记录选项 • URL 阻止列表日志记录选项 • 网络阻止列表日志记录选项（对于受阻列表中的 IP 地址） 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》
策略 > 访问控制，<每个策略>，**默认操作** 行， **日志记录**（ ）	与 SSL 策略关联的默认操作的日志记录设置。 请参阅使用策略默认操作记录连接，第 713 页。

配置位置	说明和更多信息
策略 > SSL，<每个策略>，<每个规则>， **日志记录**	SSL 规则的日志记录设置。 请参阅《Cisco Secure Firewall Management Center 设备配置指南》。
策略 > 预过滤器，<每个策略>，**默认操作** 行， **日志记录**（ ）	与预过滤器策略关联的默认操作的日志记录设置。 请参阅使用策略默认操作记录连接，第 713 页。
策略 > 预过滤器，<每个策略>，<每个预过滤器规则>， **日志记录**	预过滤器策略中每个预过滤器规则的日志记录设置。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》
策略 > 预过滤器，<每个策略>，<每个隧道规则>， **日志记录**	预过滤器策略中每个隧道规则的日志记录设置。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》
威胁防御 集群配置的其他系统日志设置：	《Cisco Secure Firewall Management Center 设备配置指南》 多次提到了系统日志；在该章中搜索“系统日志。”

入侵事件系统日志的配置位置（FTD 设备）

您可以在各个位置指定入侵策略的系统日志设置，也可以从访问控制策略或FTD平台设置或者从这两者继承设置。

配置位置	说明和更多信息
设备 > 平台设置，威胁防御设置策略，**系统日志**	您在此处配置的系统日志目标可以在访问控制策略的“日志记录”选项卡中指定，该策略可以是入侵策略的默认策略。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。
策略 > 访问控制，<每个策略>， **日志记录**	入侵事件的系统日志目标的默认设置（在入侵策略未指定其他日志记录主机的情况下）。 请参阅《Cisco Secure Firewall Management Center 设备配置指南》。

配置位置	说明和更多信息
策略 > 入侵，<每个策略>，**高级设置**，启用**系统日志警报**，点击**编辑**	要指定访问控制策略“日志记录”选项卡中指定的目标之外的系统日志收集器，并指定设施和严重性，请参阅为入侵事件配置系统日志警报，第 544 页。 如果您要使用入侵策略中配置的**严重性**或**设施**或两者，则还必须在策略中配置日志记录主机。如果您使用访问控制策略中指定的日志记录主机，则不会使用入侵策略中指定的严重性和设施。
策略 > 访问控制 > 日志记录 > IPS 设置	如果您想要发送 IPS 事件的系统日志消息。配置的默认系统日志设置用于 IPS 事件的系统日志目标

入侵事件系统日志的配置位置（非 FTD 设备）

- （默认）访问控制策略《Cisco Secure Firewall Management Center 设备配置指南》，如果您指定系统日志警报（请参阅创建系统日志警报响应，第 534 页。）
- 或者参阅为入侵事件配置系统日志警报，第 544 页。

默认情况下，入侵策略使用访问控制策略的“日志记录”选项卡中的设置。如果未在此处配置适用于 FTD 以外设备的设置，则不会为 FTD 以外的设备发送系统日志，也不会显示警告。

文件和恶意软件事件系统日志的配置位置

配置位置	说明和更多信息
在访问控制策略中： **策略 > 访问控制**，<每个策略>， **日志记录**	这是将系统配置为发送文件和恶意软件事件系统日志的主要位置。 如果您不使用 FTD 平台设置中的系统日志设置，则还必须创建警报响应。请参阅创建系统日志警报响应，第 534 页。
在 Firepower Threat Defense 平台设置中： **设备 > 平台设置**，威胁防御设置策略，**系统日志**	这些设置仅适用于运行受支持版本的 Firepower Threat Defense 设备，并且仅当您将访问控制策略中的“日志记录”选项卡配置为使用 FTD 平台设置时才适用。 请参阅《Cisco Secure Firewall Management Center 设备配置指南》。
在访问控制规则中： **策略 > 访问控制**，<每个策略>， 规则，<每个规则>， **日志记录**	如果您不使用 FTD 平台设置中的系统日志设置，则还必须创建警报响应。请参阅创建系统日志警报响应，第 534 页。

安全事件系统日志消息剖析

FTD 中的示例安全事件消息（入侵事件）

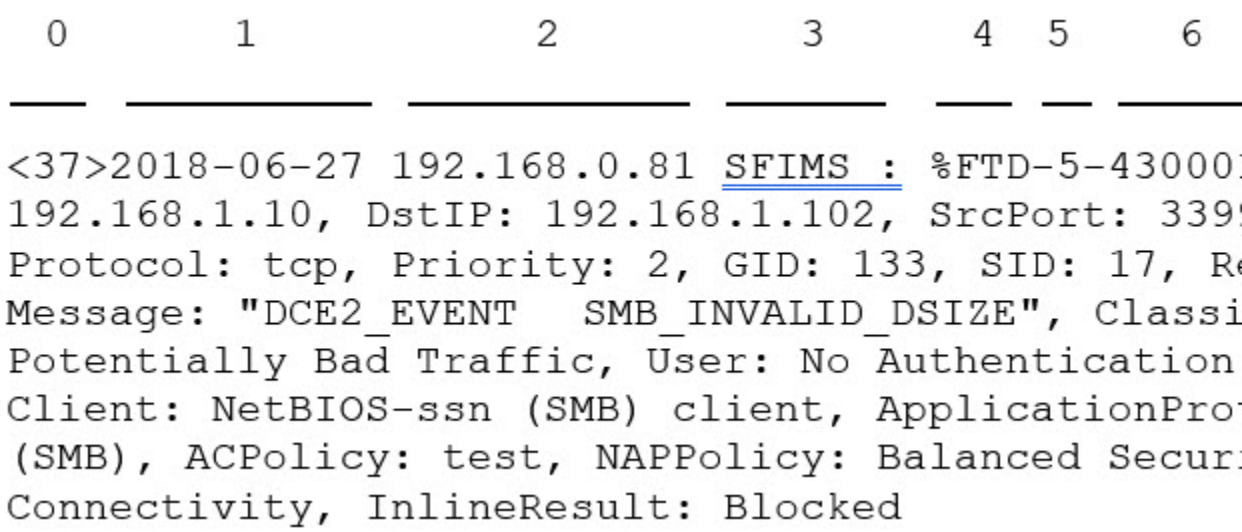


表 *63:* 安全事件系统日志消息的组件

示例消息中的项目编号	报头元素	说明
0	PRI	优先级值代表警报的设施和严重性。仅当您使用 FMC 平台设置以 EMBLEM 格式启用日志记录时，系统日志消息中才会显示该值。如果通过访问控制策略的日志记录选项卡启用入侵事件日志记录，则系统日志消息中会自动显示 PRI 值。有关如何启用 EMBLEM 格式的信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。有关 PRI 的详细信息，请参阅 RFC5424。

示例消息中的项目编号	报头元素	说明
1	时间戳	从设备发送系统日志消息的日期和时间。 • （从FTD设备发送的系统日志）对于使用访问控制策略及其后代中的设置发送的系统日志，或者如果在FTD平台设置中指定使用此格式，日期格式是 ISO 8601 中定义的格式，时间戳是 RFC 5424 中指定的格式 (yyyy-MM-ddTHH:mm:ssZ)，其中字母 Z 表示 UTC 时区。 • （从所有其他设备发送的系统日志）对于使用访问控制策略及其后代中的设置发送的系统日志，日期格式是 ISO 8601 中定义的格式，时间戳是 RFC 5424 中指定的格式 (yyyy-MM-ddTHH:mm:ssZ)，其中字母 Z 表示 UTC 时区。 • 否则，即使未指示时区，仍采用 UTC 时区格式的月、日和时间。 要在 FTD 平台设置中配置时间戳设置，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。
2	发送消息的设备或接口。 该字段可以是： • 接口的 IP 地址 • 设备主机名 • 自定义设备标识符	（对于从 FTD 设备发送的系统日志） 如果使用 FTD 平台设置发送了系统日志消息，则这是在 **系统日志设置** 中为 **启用系统日志设备 ID** 选项配置的值（如果已指定）。 否则，报头中不存在此元素。 要在FTD平台设置中配置此设置，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。
3	自定义值	如果使用警报响应发送了消息，则这是在发送消息的警报响应中配置的**标记**值（如果已配置）。（请参阅创建系统日志警报响应，第 534 页。） 否则，报头中不存在此元素。
4	%FTD	发送消息的设备的类型。%FTD 是 Firepower Threat Defense
5	严重性	在系统日志设置中为触发消息的策略指定的严重性。 有关严重性的说明，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的 严重性级别 或 系统日志严重性级别，第 536 页。

示例消息中的项目编号	报头元素	说明
6	事件类型标识符	• 430001：入侵事件 • 430002：连接开始时记录的连接事件 • 430003：连接结束时记录的连接事件 • 430004：文件事件 • 430005：文件恶意软件事件
--	设施	请参阅安全事件系统日志消息中的设施，第 621 页。
--	消息的其余部分	用冒号分隔的字段和值。 具有空值或未知值的字段在消息中会被省略。 有关字段说明，请参阅： • 连接和 安全相关连接 事件字段，第 717 页。 • 入侵事件字段，第 752 页 • 文件和恶意软件事件字段，第 800 页 **注释** 字段说明列表包括系统日志字段和事件查看器中显示的字段（Firepower 管理中心 Web 界面中“分析”菜单下的菜单选项。）通过系统日志提供的字段这样标记。 在事件查看器中显示的某些字段无法通过系统日志获得。此外，某些系统日志字段不包括在事件查看器中（但可以通过搜索获得），某些字段被组合在一起或被分开。

安全事件系统日志消息中的设施

设施值通常在安全事件系统日志消息中不相关。但是，如果您需要设施，请使用下表：

设备	要在连接事件中包括设施	要在入侵事件中包括设施	在系统日志消息中的位置
FTD	在 FTD 平台设置中使用 EMBLEM 选项。 使用 FTD 平台设置发送系统日志消息时，连接事件的设施值始终为 **ALERT**。	在 FTD 平台设置中使用 EMBLEM 选项或使用入侵策略中的系统日志设置配置日志记录。如果您使用入侵策略，则还必须在入侵策略设置中指定日志记录主机。 启用系统日志警报并配置入侵策略的设施和严重性。请参阅为入侵事件配置系统日志警报，第 544 页。	虽然设施不会出现在消息报头中，但是系统日志收集器可以根据 RFC 5424 的第 6.2.1 节导出该值。
FTD 以外的设备	使用警报响应。	使用入侵策略高级设置中的系统日志设置或访问控制策略“日志记录”选项卡中标识的警报响应。	

有关详细信息，请参阅入侵系统日志警报的设施和严重性，第 545 页和创建系统日志警报响应，第 534 页。

Firepower 系统日志消息类型

Firepower 可以发送多种系统日志数据类型，如下表所述：

系统日志数据类型	请参阅
来自 FMC 的审核日志	将审核日志流传输到系统日志，第 43 页和审核和系统日志，第 389 页一章
来自 FTD 设备的设备运行状况和网络相关日志	《Cisco Secure Firewall Management Center 设备配置指南》
来自 FTD 设备的连接、 安全情报和入侵事件日志	关于配置系统以向系统日志发送安全事件数据，第 610 页。
来自经典设备的连接、安全情报和入侵事件日志	关于配置系统以向系统日志发送安全事件数据，第 610 页
文件和恶意软件事件日志	关于配置系统以向系统日志发送安全事件数据，第 610 页
IPS 设置	发送 IPS 事件的系统日志消息。 入侵事件系统日志的配置位置（FTD 设备），第 617 页

安全事件的系统日志限制

- 如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。
- 可能需要 15 分钟事件才能显示在系统日志收集器上。
- 以下文件和恶意软件事件的数据不可通过系统日志获得：
  - 追溯性事件
  - 由面向终端的 AMP 生成的事件

eStreamer 服务器流传输

通过 Event Streamer (eStreamer)，您可以将几种事件数据从 Cisco Secure Firewall Management Center 传输到自定义开发的客户端应用。有关详细信息，请参阅 *Firepower* 系统 *Event Streamer* 集成指南。

您必须将 eStreamer 服务器配置为向客户端发送 eStreamer 事件，提供关于客户端的信息并生成建立通信时要使用的身份验证凭据集，然后，要用作 eStreamer 服务器的设备才能开始向外部客户端流传输 eStreamer 事件。可从设备的用户界面执行所有这些任务。一旦保存设置，收到请求时，您选择的事件将转发至 eStreamer 客户端。

您可以控制 eStreamer 服务器能够向发出请求的客户端传输的事件类型。

表 *64: eStreamer* 服务器可传输的事件类型

事件类型	说明
入侵事件	受管设备生成的入侵事件
入侵事件数据包数据	与入侵事件关联的数据包
入侵事件额外数据	与入侵事件关联的额外数据，如通过 HTTP 代理或负载均衡器连接至 Web 服务器的客户端的源 IP 地址
发现事件	网络发现事件
关联和 允许列表 事件	关联和合规性 allow 名单事件
影响标志警报	生成的影响警报 管理中心
用户事件	用户事件
恶意软件事件	恶意软件事件
文件事件	文件事件
连接事件	有关被监控主机与所有其他主机之间的会话流量的信息。

系统日志与 eStreamer 在安全事件方面的比较

通常，目前没有对 eStreamer 进行重大投资的组织应使用系统日志而不是 eStreamer 来在外部管理安全事件数据。

系统日志	eStreamer
无需任何自定义	需要执行大量自定义和持续维护来适应每个版本的更改
标准	受限于专有环境
系统日志标准不能防范数据丢失，尤其是在使用 UDP 时	防范数据丢失
直接从设备发送	从 FMC 发送，增加处理开销
仅支持 文件和恶意软件事件、 连接事件（包括安全情报事件）和入侵事件。	支持 eStreamer 服务器流传输，第 623 页中所列的所有事件类型。
某些事件数据只能从 FMC 发送。请参阅仅通过 eStreamer 发送的数据，不通过系统日志发送，第 624 页。	包括无法直接从设备通过系统日志发送的数据。请参阅仅通过 eStreamer 发送的数据，不通过系统日志发送，第 624 页。

仅通过 eStreamer 发送的数据，不通过系统日志发送

以下数据仅可从 Cisco Secure Firewall Management Center 获取，因此无法从设备通过系统日志发送：

- 数据包日志
- 入侵事件额外数据事件

  有关说明，请参阅 eStreamer 服务器流传输，第 623 页。
- 统计信息和汇聚事件
- 网络发现事件
- 用户活动和登录事件
- 相关事件
- 对于恶意软件事件：
  - 追溯性判定
  - ThreatName 和 Disposition，除非有关相关 SHA 的信息已同步到设备
- 以下字段：
  - Impact 和 ImpactFlag 字段

    有关说明，请参阅 eStreamer 服务器流传输，第 623 页。

- IOC_Count 字段

- 大多数原始 ID 和 UUID。

  例外情况：

  - 连接事件的系统日志包括以下内容：FirewallPolicyUUID、FirewallRuleID、TunnelRuleID、MonitorRuleID、SI_CategoryID、SSL_PolicyUUID 和 SSL_RuleID
  - 入侵事件的系统日志包括 IntrusionPolicyUUID、GeneratorID 和 SignatureID

- 拓展元数据包括但不限于：

  - LDAP 提供的用户详细信息，例如全名、部门、电话号码等。

    系统日志仅在事件中提供用户名。

  - 基于状态的信息的详细信息，例如 SSL 证书详细信息。

    系统日志提供证书指纹等基本信息，但不会提供证书 CN 等其他证书详细信息。

  - 详细的应用信息，例如应用标签和类别。

    系统日志仅提供应用名称。

  某些元数据消息还包括有关对象的额外信息。

- 地理位置信息

选择 eStreamer 事件类型

eStreamer 事件配置 (eStreamer Event Configuration) 复选框控制 eStreamer 服务器可传输的事件。您的客户端仍必须在发送到 eStreamer 服务器的请求消息中，特别请求您要其接收的事件类型。有关详细信息，请参阅 *Firepower 系统 Event Streamer* 集成指南。

在多域部署中，您可以在任何域级别配置 eStreamer 事件配置。但是，如果祖先域已启用特定事件类型，则无法禁用后代域中的事件类型。

为 管理中心，您必须是管理员用户才能执行此任务。

过程

步骤 1 选择**集成** > **其他集成**。

步骤 2 点击 **eStreamer**。

步骤 3 在 **eStreamer 事件配置 (eStreamer Event Configuration)** 下，选中或清除想要 eStreamer 转发到请求客户端的事件类型旁边的复选框（在eStreamer 服务器流传输 ， 第 623 页中进行了介绍）。

步骤 4 点击**保存 (Save)**。

配置 eStreamer 客户端通信

必须先从 eStreamer 页面将客户端添加到 eStreamer 服务器的对等体数据库，然后 eStreamer 才能向该客户端发送 eStreamer 事件。您还必须将 eStreamer 服务器生成的身份验证证书复制到该客户端。完成这些步骤后，无需重新启动 eStreamer 服务即可使客户端能够连接到 eStreamer 服务器。

在多域部署中，可以在任何域中创建 eStreamer 客户端。通过身份验证证书，可以仅从客户端证书的域和任何后代域请求事件。eStreamer 配置页面仅显示与当前域相关联的客户端，因此，如果要下载或吊销证书，请切换到创建了客户端的域。

您必须是管理员或发现管理员用户，才能对 管理中心执行此任务。

过程

步骤 1 选择**集成** > **其他集成**。

步骤 2 点击 **eStreamer**。

步骤 3 点击 **Create Client**。

步骤 4 在**主机名 (Hostname)** 字段中，输入运行 eStreamer 客户端的主机的主机名或 IP 地址。

注释 如果尚未配置 DNS 解析，请使用 IP 地址。

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

步骤 6 点击**保存 (Save)**。
eStreamer 服务器现在允许主机访问 eStreamer 服务器上的端口 8302，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。

步骤 7 点击客户端主机名称旁边的 **下载**（ ） 以下载证书文件。

步骤 8 将证书文件保存至客户端用于 SSL 身份验证的适当目录。

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

请注意，无需重新启动 eStreamer 服务；系统将立即撤销访问权限。

Splunk 中的事件分析

您可以使用 Cisco Secure Firewall (f.k.a. 面向 Splunk （以前称为适用于 Splunk 的思科 Firepower 应用）作为显示和处理 Firepower 事件数据的外部工具，以追踪和调查网络上的威胁。

eStreamer 为必填项。这个是高级功能。请参阅eStreamer 服务器流传输 ， 第 623 页。

有关详细信息，请参阅 https://cisco.com/go/firepower-for-splunk。

IBM QRadar 中的事件分析

您可以使用适用于 IBM QRadar 的思科 Firepower 应用作为显示事件数据并帮助您分析、寻找和调查网络威胁的替代方法。

eStreamer 为必填项。这个是高级功能。请参阅eStreamer 服务器流传输 ， 第 623 页。

有关详细信息，请参阅 https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/QRadar/integration-guide-for-the-cisco-firepower-app-for-ibm-qradar.html。

使用外部工具分析事件数据的历史记录

特性	最低 管理中心	最低 威胁防御	详细信息
SecureX 功能区	7.0	任意	SecureX 功能区将转换为 SecureX，可即时了解思科安全产品中的威胁形势。 要在 管理中心中显示 SecureX 功能区，请参阅 *Firepower* 和 *SecureX* 集成指南 ，网址为 https://cisco.com/go/firepower-securex-documentation。 新增/修改的屏幕：新页面：系统 > SecureX
将所有连接事件发送至思科云	7.0	任意	您现在可以将所有连接事件发送到思科云，而不仅仅是发送高优先级连接事件。 新增/经修改的屏幕：系统 > 集成 > 云服务页面上的新选项
交叉启动以查看 Secure Network Analytics中的数据	6.7	任意	此功能引入了一种在“分析”>“上下文交叉启动”页面上为 Secure Network Analytics 设备创建多个条目的快速方法。 这些条目允许您右键点击相关事件，以交叉启动 Secure Network Analytics 并显示与您交叉启动的数据点相关的信息。 新菜单项：系统 > 日志记录 > 安全分析和日志记录 配置事件发送至 Secure Network Analytics的新页面。

特性	最低 管理中心	最低 威胁防御	详细信息
从其他字段类型进行上下文交叉启动	6.7	任意	现在，您可以使用以下其他类型的事件数据交叉启动外部应用： • 访问控制策略 • 入侵策略 • 应用协议 • 客户端应用 • Web 应用 • 用户名（包括领域） 新菜单选项：右键点击“分析”菜单下页面上的“控制面板”构件和事件表中的事件的上述数据类型时，可以使用上下文交叉启动选项。 支持的平台： Cisco Secure Firewall Management Center
与 IBM QRadar 集成	6.0 及更高版本	任意	IBM QRadar 用户可以使用新的 Firepower 特定应用来分析其事件数据。 可用功能受 Firepower 版本的影响。 请参阅IBM QRadar 中的事件分析，第 627 页。

与 SecureX 威胁响应集成的增强功能	6.5	任意	• 支持区域云：
			  • 美国（北美）
			  • 欧洲
			• 支持其他事件类型：
			  • 文件和恶意软件事件
			  • 高优先级连接事件
			  这些是与以下内容相关的连接事件：
			  • 入侵事件
			  • 安全情报事件
			  • 文件和恶意软件事件
			经修改的屏幕：**系统 > 集成 > 云服务**中新的选项。
			支持的平台：此版本中通过直接集成或系统日志支持的所有设备。

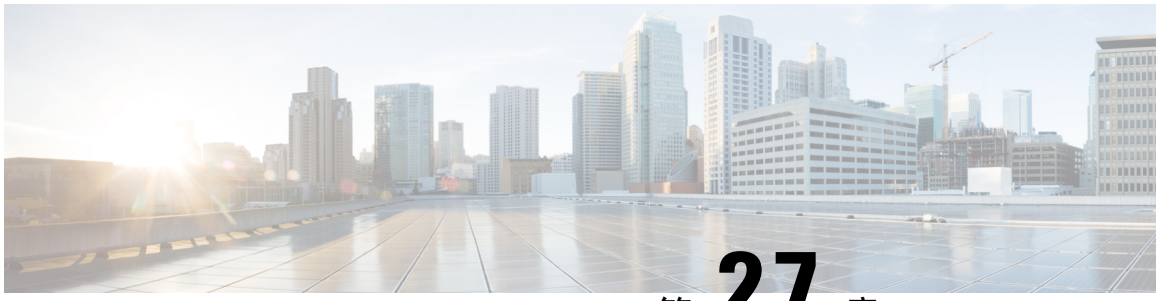
Syslog	6.5	任意	AccessControlRuleName 字段现在在入侵事件系统日志消息中可用。

特性	最低 管理中心	最低 威胁防御	详细信息
集成思科安全数据包分析器	6.5	任意	已删除对此功能的支持。
集成 SecureX 威胁响应	6.3（通过系统日志，使用代理收集器） 6.4（直接）	任意	使用 SecureX 威胁响应中功能强大的分析工具，将 Firepower 入侵事件数据与来自其他来源的数据集成，以便统一查看网络上的威胁。 经修改的屏幕（版本 6.4）：**系统 > 集成 > 云服务**中新的选项。 支持的平台：运行 6.3 版（通过系统日志）或 6.4 版的 Cisco Secure Firewall Threat Defense 设备。
文件和恶意软件事件的系统日志支持	6.4	任意	现在可以通过系统日志从受管设备发送完全限定的文件和恶意软件事件数据。 修改的屏幕： **策略 > 访问控制 > 访问控制 > “日志记录**。 支持的平台：运行 6.4 版的所有受管设备。
与 Splunk 集成	支持所有 6.x 版本	任意	Splunk 用户可以使用新的独立 Splunk 应用程序 Cisco Secure Firewall (f.k.a. 面向 Splunk分析事件。 可用功能受 Firepower 版本的影响。 请参阅Splunk 中的事件分析，第 626 页。
集成思科安全数据包分析器	6.3	任意	引入的功能：立即向思科安全数据包分析器查询与事件相关的数据包，然后点击以检查思科安全数据包分析器中的结果或下载结果以便在另一种外部工具中进行分析。 新屏幕： **系统 > 集成 > 数据包分析器** **分析 > 高级 > 数据包分析器查询** 新菜单选项：**查询数据包分析器**菜单项，在右键点击“控制面板”页面上的事件和“分析”菜单下页面上的事件表时会出现此菜单项。 支持的平台： Cisco Secure Firewall Management Center
上下文交叉启动	6.3	任意	引入的功能：右键点击事件以在基于 URL 的预定义或自定义外部资源中查找相关信息。 新增屏幕： **分析 > 高级 > 上下文交叉启动** 新菜单选项：多个选项，在右键点击“控制面板”页面上的事件和“分析”菜单下页面上的事件表时会出现这些选项。 支持的平台： Cisco Secure Firewall Management Center

特性	最低 管理中心	最低 威胁防御	详细信息
连接和入侵事件系统日志消息	6.3	任意	能够使用新的统一、简化配置，通过系统日志将完全限定的连接和入侵事件发送到外部存储和工具。现在消息报头进行了标准化，包括事件类型标识符，消息变得更小，因为省略了具有未知值和空值的字段。 支持的平台： • 所有新功能：运行 6.3 版的 威胁防御 设备。 • 部分新功能：运行 6.3 版的非威胁防御 设备。 • 更少的新功能：运行 6.3 以下版本的所有设备。 有关更多信息，请参阅关于发送 安全事件的系统日志消息，第610页下的主题以及子主题。
eStreamer	6.3	任意	将 eStreamer 内容从“主机身份源”一章移至本章，并添加了将 eStreamer 与系统日志进行比较的摘要。

第 VII 部分

工作流程和表格



第 27 章

工作流程

以下主题介绍如何使用工作流程：

概述：工作流程

工作流程是管理中心网络界面中可供分析师用于评估系统生成的事件的定制系列的数据页面。

管理中心提供以下类型的工作流程：

预定义工作流程

随系统交付的预设工作流程。您无法编辑或删除预定义工作流程。但是，可以复制预定义工作流程，将其用作自定义工作流程的基础。

已保存的自定义工作流程

基于随 管理中心交付的已保存自定义表的自定义工作流程。您可以编辑、删除和复制这些工作流程。

自定义工作流程

您为特定需求创建和自定义的工作流程，或者在您创建自定义表时系统自动生成的工作流程。您可以编辑、删除和复制这些工作流程。

工作流程中显示的数据通常取决于您如何许可和部署受管设备以及是否配置提供数据的功能等因素。

预定义工作流程

以下部分介绍的预定义工作流程随系统一同交付。您无法编辑或删除预定义工作流程，但是您可以复制预定义工作流程，并将其用作自定义工作流程的基础。

预定义入侵事件工作流程

下表描述 Firepower 系统随附的预定义入侵事件工作流程。

表 *65:* 预定义入侵事件工作流程

工作流程名称	说明
目标端口	由于目标端口通常绑定到应用，因此该工作流程可以帮助检测警报量异常高的应用。“目标端口”列还可以帮助识别不应存在于网络上的应用。
事件特定	此工作流程提供两个有用的功能。频繁发生的事件可能指示： • 误报 • 蠕虫 • 配置严重错误的网络 偶尔发生的事件很可能指示针对性攻击和特别关注事项。
按照优先级和分类显示事件	此工作流程按事件优先级列出事件及其类型，随之还列出一个表明每个事件已发生的次数的计数。
到目标的事件	此工作流程提供受攻击主机IP地址和攻击性质的高级视图；在适用情况下，还可查看有关攻击中涉及的国家/地区的信息。
IP 特定	此工作流程显示哪些主机IP地址生成最多警报。事件数最多的主机面向公众并接收蠕虫类型流量（指示适合进行调整的位置），或者需要进一步调查以确定警报原因。具有最低计数的主机也有必要进行调查，因为它们可能是针对性攻击的对象。低计数还可指示主机可能不属于该网络。
影响和优先级	通过此工作流程，可以快速查找影响重大的复发事件。报告的影响级别通过事件已发生的次数进行显示。使用此信息，可以识别复发最频繁的重大影响事件，此类事件可能指示网络上的大范围攻击。
影响和源	此工作流程可帮助识别正在进行攻击的源。报告的影响级别通过事件的关联源IP地址进行显示。例如，如果反复出现来自同一源IP地址的1级影响事件，则可能表示攻击者已识别易受攻击的系统并在针对它们进行攻击。
对目标的影响	可以使用此工作流程识别在易受攻击计算机上重复发生的事件，以便解决这些系统上的漏洞并停止进行的任何攻击。

工作流程名称	说明
源端口	此工作流程指示哪些服务器生成的警报最多。可以使用此信息标识需要调整的方面，并确定需要注意的服务器。
源和目标	此工作流程识别共享高级警报的主机 IP 地址。列表顶部的对可能是误报，也可能标识需要调整的方面。可以检查列表底部的对来查找针对性攻击、访问其不应访问的资源的用户或不属于该网络的主机。

预定义恶意软件工作流程

下表介绍了 管理中心中包含的预定义恶意软件工作流程。所有预定义恶意软件工作流程都使用恶意软件事件表视图。

表 *66:* 预定义恶意软件工作流程

工作流程名称	说明
恶意软件摘要	此工作流程提供在网络流量中或由面向终端的 AMP 连接器检测到的恶意软件列表，按个别威胁分组。
恶意软件事件摘要 (Malware Event Summary)	此工作流程提供不同恶意软件事件类型和子类型的快速细分。
接收恶意软件的主机 (Hosts Receiving Malware)	此工作流程提供已接收恶意软件的主机 IP 地址列表，按恶意软件文件的关联性质分组。
发送恶意软件的主机 (Hosts Sending Malware)	此工作流程提供已发送恶意软件的主机 IP 地址列表，按恶意软件文件的关联性质分组。
引入恶意软件的应用 (Applications Introducing Malware)	此工作流程提供已接收文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。

预定义文件工作流程

下表描述管理中心中包含的预定义文件事件工作流程。所有预定义文件事件工作流程都使用文件事件表视图。

表 *67:* 预定义文件工作流程

工作流程名称	说明
文件摘要	此工作流程提供不同文件事件类别和类型以及任何关联恶意软件性质的快速细分。
接收文件的主机	此工作流程提供已接收文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。

工作流程名称	说明
发送文件的主机	此工作流程提供已发送文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。

预定义捕获文件工作流程

下表描述 管理中心中包含的预定义捕获文件工作流程。所有预定义捕获文件工作流程都使用捕获文件表视图。

表 *68:* 预定义捕获文件工作流程

工作流程名称	说明
捕获的文件摘要	此工作流程根据类型、类别和威胁评分提供捕获文件的细分。
动态分析状态	此工作流程根据是否已提交捕获文件进行动态分析来提供此类文件的计数。

预定义连接数据工作流程

下表描述管理中心中包含的预定义连接数据工作流程。所有预定义连接数据工作流程都使用连接数据表视图。

表 *69:* 预定义连接数据工作流程

工作流程名称	说明
连接事件	此工作流程提供基本连接和检测到的应用信息的摘要视图，然后可以使用该视图向下展开至事件表视图。
按应用分类的连接	此工作流程包含从检测到的连接数来看监控网段上 10 个最活跃应用的图形。
按发起方分类的连接	此工作流程包含从连接数来看监控网段上 10 个最活跃的发起了连接事务的主机 IP 地址的图形。
按端口分类的连接	此工作流程包含从检测到的连接数来看监控网段上 10 个最活跃端口的图形。
按响应方分类的连接	此工作流程包含从连接数来看监控网段上 10 个最活跃的主机 IP 地址（主机 IP 是连接事务中的响应方）的图形。
Connections over Time	此工作流程包含某个时间跨度的监控网段上的连接总数的图形。

工作流程名称	说明
按应用分类的流量	此工作流程包含从传输的字节数来看监控网段上 10 个最活跃应用的图形。 应用计数反映与应用连接匹配的每个检测器。根据应用协议、Web 应用、客户端检测器或内部检测器是否与流量匹配，以及流量是来源于移动设备还是属于加密会话的一部分，同一应用会话可能在列表中出现多次。如果在客户端流中看到了该应用，并且不存在特定客户端检测器，则可以报告通用客户端。 例如，您可能会看到同一 YouTube 流量会话既报告为 **YouTube**（因为它与 YouTube Web 应用检测器匹配），又报告为 **YouTube 客户端**（因为内部 YouTube 检测器与客户端会话中常见的特征相匹配）。 使用连接事件中的信息和网络的网络映射确定特定应用连接的更多上下文。
按发起方分类的流量	此工作流程包含从每个地址传输的总数据量来看监控网段上 10 个最活跃主机 IP 地址的图形。
按端口分类的流量	此工作流程包含从传输的字节数来看监控网段上 10 个最活跃端口的图形。
按响应方分类的流量	此工作流程包含从每个地址接收的总字节数来看监控网段上 10 个最活跃主机 IP 地址的图形。
一段时间内的流量	此工作流程包含某个时间跨度的监控网段上传输的总数据量的图形。
按响应方分类的唯一发起方	此工作流程包含从已联系每个地址的唯一发起方数量来看监控网段上 10 个最活跃响应主机 IP 地址的图形。
按发起方分类的唯一响应方	此工作流程包含从已联系地址的唯一响应方数量来看监控网段上 10 个最活跃发起主机 IP 地址的图形。

预定义安全情报工作流程

下表描述 管理中心中包含的预定义安全情报工作流程。所有预定义安全情报工作流程均采用安全情报事件表格视图。

表 *70*: 预定义安全情报工作流程

工作流程名称	说明
安全情报事件	此工作流程提供基本安全情报和检测到的应用信息的摘要视图，然后可以使用该视图向下展开至事件表视图。
安全情报摘要 (Security Intelligence Summary)	此工作流程与“安全情报事件”(Security Intelligence Events) 工作流程相同，但是从其中仅按类别和计数列出了安全情报事件的“安全情报摘要”(Security Intelligence Summary) 页面开始。

工作流程名称	说明
具有 DNS 详细信息的安全情报 (Security Intelligence with DNS Details)	此工作流程与“安全情报事件”(Security Intelligence Events) 工作流程相同，但是从其中仅按类别和 DNS 相关特性列出安全情报事件的“具有 DNS 详细信息的安全情报”(Security Intelligence with DNS Details) 页面开始。

预定义主机工作流程

下表描述可与主机数据配合使用的预定义工作流程。

表 *71:* 预定义主机工作流程

工作流程名称	说明
主机数	此工作流程包含主机表视图，后跟主机视图。通过基于“主机”(Hosts) 表的工作流程视图可轻松查看与主机关联的所有 IP 地址上的数据。
操作系统摘要 (Operating System Summary)	可以使用此工作流程分析网络上正在使用中的操作系统。

预定义危害表现工作流程

下表描述可与 IOC（危害表现）数据配合使用的预定义工作流程。

表 *72:* 预定义危害表现工作流程

工作流程名称	说明
主机危害表现	此工作流程以按计数和类别分组的 IOC 数据的摘要视图开头，提供按事件类型进一步细分摘要数据的详细视图。 通过**分析 (Analysis) > 主机 (Hosts)** 菜单访问此工作流程。
按主机划分的危害表现 (Indications of Compromise by Host)	可以使用此工作流程衡量网络上哪些主机最可能受损（基于 IOC 数据）。 通过**分析 (Analysis) > 主机 (Hosts)** 菜单访问此工作流程。
用户危害表现	此工作流程以按计数和类别分组的 IOC 数据的摘要视图开头，提供按事件类型进一步细分摘要数据的详细视图。 通过**分析 (Analysis) > 用户 (Users)** 菜单访问此工作流程。
按用户划分的危害表现	使用此工作流程衡量网络上哪些用户最可能受到潜在危害的影响（基于 IOC 数据）。 通过**分析 (Analysis) > 用户 (Users)** 菜单访问此工作流程。

预定义应用工作流程

下表描述可与应用数据配合使用的预定义工作流程。

表 *73:* 预定义应用工作流程

工作流程名称	说明
应用业务相关性	可以使用此工作流程分析网络上正在运行的各估算业务关联性级别的应用，从而能够监控网络资源的相应使用。
应用类别 (Application Category)	可以使用此工作流程分析网络上正在运行的各类别的应用（如邮件、搜索引擎或社交网络），从而能够监控网络资源的相应使用。
Application Risk	可以使用此工作流程分析网络上正在运行的各估算安全风险级别的应用，从而能够估算用户活动的潜在风险并采取相应措施。
应用摘要 (Application Summary)	可以使用此工作流程获取有关网络上的应用和关联主机的详细信息，从而能够仔细检查主机应用活动。
应用	可以使用此工作流程分析网络上正在运行的应用，从而能够大致了解网络的使用方式。

预定义应用详细信息工作流程

下表描述可与应用详情和客户端数据配合使用的预定义工作流程。

表 *74:* 预定义应用详细信息工作流程

工作流程名称	说明
应用详情	可以使用此工作流程更详细地分析网络上的客户端应用。然后，工作流程提供客户端应用表视图，后跟主机视图。
客户端	此工作流程包含客户端应用表视图，后跟主机视图。

预定义服务器工作流程

下表描述可与服务器数据配合使用的预定义工作流程。

表 *75:* 预定义服务器工作流程

工作流程名称	说明
按计数划分的网络应用 (Network Applications by Count)	可以使用此工作流程分析网络上最频繁使用的应用。

工作流程名称	说明
按命中数划分的网络应用”(Network Applications by Hit)	可以使用此工作流程分析网络上最活跃的应用。
服务器详细信息	可以使用此工作流程详细分析检测到的服务器应用协议的供应商和版本。
服务器	此工作流程包含应用表视图，后跟主机视图。

预定义主机属性工作流程

下表描述可与主机属性数据配合使用的预定义工作流程。

表 *76:* 预定义主机属性工作流程

工作流程名称	说明
属性	可以使用此工作流程监控网络上主机的 IP 地址和主机状态。

预定义发现事件工作流程

下表介绍可用于查看发现和身份数据的预定义工作流程。

表 *77:* 预定义发现事件工作流程

工作流程名称	说明
发现事件 (Discovery Events)	此工作流程以表视图形式提供发现事件的详细列表，后跟主机视图。

预定义用户工作流程

下表介绍可用于查看用户发现和用户身份数据的预定义工作流程。

表 *78:* 预定义用户工作流程

工作流程名称	说明
活动会话	此工作流程提供用户身份源收集的活动会话列表。
用户	此工作流程提供用户身份源收集的用户信息列表。

预定义漏洞工作流程

下表描述管理中心中包含的预定义漏洞工作流程。

表 *79*: 预定义漏洞工作流程

工作流程名称	说明
漏洞	可以使用此工作流程审查数据库中的漏洞，包括仅含应用于网络上检测到的主机的活动漏洞的表视图。工作流程提供漏洞详情视图，该视图包含符合限制条件的每个漏洞的详细说明。

预定义第三方漏洞工作流程

下表描述管理中心中包含的预定义第三方漏洞工作流程。

表 *80*: 预定义第三方漏洞工作流程

工作流程名称	说明
按 IP 地址分组的漏洞 (Vulnerabilities by IP Address)	可以使用此工作流程快速了解监控网络上每个主机 IP 地址检测到的第三方漏洞数量。
Vulnerabilities by Source	可以使用此工作流程快速了解每个第三方漏洞源（如 QualysGuard 扫描程序）检测到的第三方漏洞数量。

预定义关联和 允许 列表工作流程

各类型的相关性数据、 allow 名单事件、 allow 名单违例和修复状态事件具有对应的预定义工作流程。

表 *81*: 预定义关联工作流程

工作流程名称	说明
相关事件	此工作流程包含关联事件表视图。
允许 列出事件	此工作流程包含 allow 名单事件表视图。
主机违规计数 (Host Violation Count)	此工作流程提供列出了违反至少一个 allow 名单的所有主机 IP 地址的一系列页面。
允许 名单违规事件	此工作流程包含列出了所有违例的 allow 名单违例表视图，其中最新检测到的违例位于列表顶部。该表中的每一行都包含一个检测到的违规事件。
状态	此工作流程包含修复状态表视图，其中包括所违反策略的名称以及应用的修复的名称和状态。

预定义系统工作流程

Firepower 系统随附一些其他工作流程，包括系统事件（例如审核事件和运行状况事件），以及列出了规则更新导入和活动扫描的结果的工作流程。

表 *82:* 其他预定义工作流程

工作流程名称	说明
审核日志 (Audit Log)	此工作流程包含列出了审核事件的审核日志表视图。
运行状况事件	此工作流程显示运行状况监控策略所触发的事件。
规则更新导入日志 (Rule Update Import Log)	此工作流程包含一个表视图，其中列出了有关成功和失败规则更新导入的信息。
扫描结果 (Scan Results)	此工作流程包含列出了已完成的各项扫描的表视图。

自定义表工作流程

可以使用自定义表功能创建使用来自两种或多种类型事件的数据的表。这一点非常有用，例如可以创建将入侵事件数据与发现数据关联的表和工作流程，从而能够简单地搜索影响关键系统的事件。

创建自定义表时，系统会自动创建可用于查看与表关联的事件的工作流程。工作流程中的功能根据所使用的表类型而异。例如，基于入侵事件表的自定义表工作流程始终以数据包视图结尾。但是，基于发现事件的自定义表工作流程以主机视图结尾。

与基于预定义事件表的工作流程不同，基于自定义表的工作流程没有指向其他类型工作流程的链接。

使用工作流程

过程

步骤 1 选择适当的菜单路径和选项，如工作流程选择，第 644 页表中所述。

步骤 2 在当前工作流程中导航：

- 要查看已选事件数据类型中的所有可用列，请使用表视图页面；请参阅使用表视图页面，第650页。
- 要查看已选事件数据类型中的一部分可用列，请使用向下钻取页面；请参阅使用向下钻取页面，第 650 页。
- 要显示工作流程下一页中的相应行，请点击 **向下箭头**（ ）。

- 要在多页工作流程的页面之间移动，请使用每页底部的工具；请参阅工作流程页面遍历工具，第 647 页。
- 要查看不同类型的事件的工作流程中应用的相同限制，请点击**跳转至 (Jump to)** 并从下拉列表中选择事件视图。

步骤 3 修改当前工作流程的显示：

- 选中页面上一行或多行的复选框以指示要影响的行，然后点击该页面底部的按钮之一（例如，**查看**），以对所有选中行执行该操作。
- 选中行顶部的复选框以选择该页面上的所有行，然后点击该页面底部的按钮之一（例如，**查看**），以对页面上的所有行执行该操作。
- 通过在要隐藏的列标题中点击**关闭**（×）来限制显示的列。在显示的弹出窗口中，点击**应用**。

  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。

- 通过所选字段的选定值限制数据视图。有关信息，请参阅事件视图限制，第 664 页和复合事件视图限制，第 665 页。
- 更改事件视图上的时间限制。位于页面右上角的日期范围为工作流程中要包含的事件设置时间范围；有关详细信息，请参阅事件时间限制，第 658 页。

  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。

- 要按列对数据进行排序，请点击该列的名称。要反向排序，请再次点击该列的名称。方向指示数据按哪一列排序，以及排序是 **升序** 或 **降序**。
- 点击工作流程页面链接，以使用任何活动限制显示该页面。工作流程页面链接显示在预定义工作流程表视图和向下展开页面左上角，位于事件上方和工作流程名称下方。

步骤 4 查看当前工作流程中的其他数据：

- 要在新窗口中查看文件的轨迹映射，请点击文件名和 SHA-256 散列值列中的网络文件轨迹。该图标因文件状态而异；请参阅文件轨迹图标，第 647 页。
- 要显示与 IP 地址相关的主机配置文件的弹出窗口，请点击任何 IP 地址列中的主机配置文件。该图标因文件状态而异；请参阅主机配置文件图标，第 648 页。
- 要查看与文件相关的最高威胁评分的动态分析摘要报告，请点击任何威胁评分列中的威胁评分。该图标因文件的最高威胁评分而异；请参阅威胁评分图标，第 648 页。
- 要查看用户配置文件信息，点击**用户** 或者，对于与危害迹象有关的用户，在任何用户身份栏中点击 **红色用户** 。如果用户无法在数据库中（即，是面向终端的 AMP 连接器用户），则用户图标呈灰色显示。

- 要查看第三方漏洞的漏洞详细信息，请点击任何第三方漏洞 ID 列中的 **漏洞** 。
- 查看汇聚的数据点时，将指针悬停在标志上方可查看国家/地区名称。
- 查看个别数据点时，可以点击标志以进一步查看地理定位，第 652 页中所述的地理位置详细信息。

步骤 5 导航到不同的工作流程：

要使用不同的工作流程查看同一事件类型，请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])**，然后选择要使用的工作流程。请注意，**不能**将不同的工作流程用于扫描结果。

按用户角色划分的工作流程访问

对工作流程的访问由用户角色确定。有关详细信息，请参阅下表。

用户角色	可访问的工作流程
管理员	可以访问任何工作流程，并且是仅有的可访问审核日志、扫描结果和规则更新导入日志的用户。
维护用户	可以访问运行状况事件。
“安全分析师”(Security Analyst) 和“安全分析师 [只读]”(Security Analyst [Read Only])	可以访问入侵、恶意软件、文件、连接、发现、漏洞、相关性和运行状况工作流程。

工作流程选择

系统提供下表中所列数据类型的预定义工作流程。

表 *83:* 使用工作流程的功能

功能	菜单路径	选项
连接事件	分析 (Analysis) > 连接 (Connections)	事件
安全情报事件	分析 (Analysis) > 连接 (Connections)	安全情报事件
相关事件	分析 (Analysis) > 关联 (Correlation)	相关事件 允许 列出事件 允许 名单违规事件 状态
恶意软件事件	分析 (Analysis) > 文件 (Files)	恶意软件事件

功能	菜单路径	选项
文件事件	分析 (Analysis) > 文件 (Files)	文件事件
捕获的文件	分析 (Analysis) > 文件 (Files)	捕获的文件
主机事件	分析 (Analysis) > 主机 (Hosts)	网络映射 (Network Map) 主机数 感染指标 应用 应用详情 服务器 主机属性 (Host Attributes) 发现事件 (Discovery Events)
入侵事件	分析 (Analysis) > 入侵 (Intrusions)	事件 已审核事件 (Reviewed Events)
用户事件	分析 (Analysis) > 用户 (Users)	活动会话 用户活动 用户 感染指标
漏洞事件	分析 (Analysis) > 主机 (Hosts)	漏洞 第三方漏洞 (Third-Party Vulnerabilities)
扫描结果	策略 (Policies) > 操作 (Actions) > 扫描工具 (Scanners)	—
运行状况事件	系统> 运行状况 > 事件	—
审核事件	系统 (System) > 监控 (Monitoring)	审核
规则更新导入日志 (Rule Update Import Log)	系统 (System) > 更新 (Updates) 版本 7.2.0 – 7.2.5：系统 > 更新 版本 7.4.1+：系统 > 内容更新	规则更新

查看上表中描述的任何种类的数据时，事件显示在该数据的默认工作流程的第一页上。您可通过配置事件视图设置来指定不同的默认工作流程。请注意，工作流程访问取决于用户角色。

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。

相关主题

配置事件视图设置，第 193 页

工作流程页面

虽然各类型的工作流程中的数据不同，但是所有工作流程都共享公共的功能集。工作流程可以包含若干类型的页面。可以在工作流程页面上执行的操作取决于页面类型。

通过工作流程中的向下钻取页面和表视图页面，您可以快速缩小数据视图的范围，从而能够专注于对分析至关重要的事件。表视图页面和向下钻取页面都支持许多可用于限制要查看的事件集或浏览工作流程的功能。当查看工作流程中的向下钻取页面或表视图中的数据时，可以基于任何可用列对数据进行升序或降序排序。如果数据库包含的事件数超过单个工作流程页面上可显示的事件数，则可点击页面底部的链接以显示更多事件。点击其中一个链接时，时间窗口自动暂停，以便不会重复显示相同事件；当您准备就绪时，可以取消暂停时间窗口。

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。

表视图

表视图对应于工作流程所基于的数据库中的每个字段包含一列（如果默认情况下启用了该页面）。

为获得最佳性能，请仅显示所需的列。显示的列越多，显示数据所需的资源就越多。

请注意，禁用表视图中的列时，如果禁用该列会创建两个或多个相同的行，则Firepower系统将向事件视图中添加“计数”列，如果超过 6 列则显示（排除“计数”列）。

点击表视图页面中的某个值时，即受该值限制。

创建自定义工作流程时，通过点击**添加表视图**向其中添加表视图。

向下钻取页面

通常，向下钻取页面是在移至表视图页面之前用于将调查范围缩小到若干事件的中间页面。向下钻取页面包含数据库中可用的列的子集。

例如，发现事件的向下钻取页面可能仅包含“IP地址”、“MAC地址”和“时间”列。另一方面，入侵事件的向下钻取页面可能包含“优先级”、“影响标志”、“内联结果”和“消息”列。

通过向下钻取页面，可以缩小所查看的事件范围并在工作流程中前进。例如，如果点击向下钻取页面中的某个值，即受该值限制并会移至工作流程中的下一页，从而更密切关注与所选值匹配的事件。点击向下钻取页面中的值并不会禁用该值所在的列，即使前进到的页面是表视图也如此。请注意，预定义工作流程的向下钻取页面始终具有Count列。创建自定义工作流程时，通过点击**Add Page**向其中添加向下钻取页面。

图形

基于连接数据的工作流程可以包含图页面，也称为连接图。

例如，连接图可能会显示列出了随时间推移系统检测到的连接数的曲线图。通常，连接图是类似于向下钻取页面的中间页面，用于缩小调查范围。

最终页面

工作流程的最终页面取决于工作流程所基于的事件的类型。

- 主机视图是基于应用、应用详细信息、发现事件、主机、危害表现 (IOC)、服务器、allow 名单违规事件、主机属性或第三方漏洞的工作流程的最终页面。通过从此页面查看主机配置文件，可以轻松查看与具有多个地址的主机关联的所有 IP 地址上的数据。
- 用户详细信息视图是基于用户、用户活动和用户危害表现的工作流程的最终页面。
- 漏洞详细视图是基于思科漏洞的工作流程的最终页面。
- 数据包视图是基于入侵事件的工作流程的最终页面。

基于其他类型的事件（例如，审核日志事件和恶意软件事件）的工作流程没有最终页面。

在工作流程的最终页面上，可以展开详细信息部分以查看有关该工作流程期间所关注的集合中各对象的特定信息。尽管 Web 界面没有在工作流程的最终页面上列出限制，但是先前设置的限制会保留并应用到数据集。

工作流程页面导航工具

工作流程页面提供视觉提示，以方便在各页面之间导航并选择要在事件分析过程中显示的信息。

工作流程页面遍历工具

如果工作流程包含多个页面的数据，则每个页面的底部会显示工作流程中的页数，以及下表中所列的可用于在页面间导航的工具：

表 *84:* 工作流程页面遍历工具

页面遍历工具	操作
页码 （要查看其他页面，请输入希望查看的页码，然后按 Enter 键。）	查看其他页面
>	查看下一页
<	查看上一页
>|	跳至最后一页
|<	跳至第一页

文件轨迹图标

当工作流程页面提供机会在新窗口中查看文件的轨迹映射时，将会显示网络轨迹图标。此图标根据文件状态而异。

表 *85:* 文件轨迹图标

文件轨迹图标	文件状态
正常	正常
恶意软件	恶意软件
自定义检测	自定义检测
未知	未知
不可用	不可用

主机配置文件图标

当工作流程页面为您提供机会在弹出式窗口中查看与某个 IP 地址关联的主机配置文件时，将会显示主机配置文件图标。如果主机配置文件图标呈灰色显示，则无法查看主机配置文件，因为该主机不能位于网络映射中（例如，0.0.0.0）。根据主机的状态，此图标看起来会有所不同。

表 *86:* 主机配置文件图标

主机配置文件图标	主机状态
	主机未被标记为可能受到危害。
	通过已触发的危害表现 (IOC) 规则，主机被标记为可能受到危害。
	列入阻止列表（仅当根据安全情报数据执行流量过滤时才会显示。）
	列入阻止列表，设置为监控（仅当根据安全情报数据执行流量过滤时才会显示。）

威胁评分图标

在工作流程页面为您提供机会查看与文件的最高威胁评分关联的动态分析摘要报告时，会显示威胁评分图标。该图标因文件的最高威胁评分而异。

表 *87:* 威胁评分图标

威胁评分图标	威胁评分级别
低	低
中等	中
高	高
很高	很高

用户图标

当工作流程页面为您提供机会在弹出窗口中查看与某个用户名关联的用户身份时，会显示用户图标。

表 *88:* 用户图标

用户图标	用户状态
用户	用户未与任何危害表现关联。
红色用户	用户与一个或多个危害表现关联。

工作流程工具栏

工作流程中的每个页面包含用于提供对相关功能的快速访问的工具栏。下表描述工具栏上的每个链接

表 *89:* 工作流程工具栏链接

特性	说明
为此页添加书签	将当前页面加入书签，以便稍后可以返回到该页面。加入书签可捕获所查看的页面上已生效的限制，以便稍后能够返回到同一数据（假设数据仍然存在）。
报告设计器	以当前受限工作流程作为选择条件打开报告设计器。
控制面板	打开与当前工作流程相关的控制面板。例如，连接事件工作流程链接到“连接摘要”控制面板。
查看书签	显示可从中进行选择的已保存书签列表。
搜索	显示可在其中对工作流程中的数据执行高级搜索的搜索页面。也可以点击向下箭头图标以选择并使用已保存的搜索。

相关主题

从事件视图创建报告模板，第 509 页
关于控制面板，第 321 页
事件搜索，第 671 页
书签，第 667 页
创建书签，第 668 页
查看书签，第 668 页

使用向下钻取页面

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如使用工作流程的功能中所述。

步骤 2 在任何工作流程中，您有以下选择：

- 要向下展开到限制某个特定值的下一个工作流程页面，请点击某一行中的一个值。请注意，此操作仅适用于向下钻取页面。在表视图中点击一行中的一个值仅限于表视图，不能钻取到下一页面。
- 要向下展开到限制某些事件的下一个工作流程页面，请选中要在下一个工作流程页面上查看的事件旁边的复选框，然后点击**查看 (View)**。
- 要向下展开到保留当前限制的下一个工作流程页面，请点击**查看全部 (View All)**。

提示 表视图的页面名称中始终包括“Table View”。

使用表视图页面

表视图页面提供在向下钻取、主机视图、数据包视图或漏洞详细信息页面上不可用的某些功能。按如下所述使用这些功能：

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如工作流程选择，第 644 页中所述。

步骤 2 从工作流程名称下方显示的工作流程路径中选择表视图。

步骤 3 如果事件数据是远程存储的，您可能会看到一个选项，用于选择显示本地数据还是远程数据。

请参阅在 Cisco Secure Firewall Management Center 和使用存储在 Secure Network Analytics 设备上的连接事件上工作，第 651 页。

步骤 4 根据需要使用下列功能在表视图中排列和导航：

- 要显示已禁用列的列表，请点击“搜索限制” **展开箭头**（）。
- 要隐藏已禁用列的列表，请点击“搜索限制” **折叠箭头**（）。
- 要将已禁用列重新添加到事件视图中，请点击“搜索限制” **展开箭头**（）以展开搜索限制，然后点击禁用列下的列名。

- 要显示或隐藏（禁用）列，请点击任何列名称旁边的**清除**（✕）。在显示的弹出窗口中，选中或清除相应的复选框以指示要显示哪些列，然后点击**应用 (Apply)**。

在 Cisco Secure Firewall Management Center 和使用存储在 Secure Network Analytics 设备上的连接事件上工作

如果您的设备正在使用 安全分析和日志记录（本地部署）向 Secure Network Analytics 设备发送连接事件，您可以在 管理中心的事件查看器和情景管理器中查看和使用这些远程存储的事件，并在生成报告时包括这些事件。 您还可以从 管理中心 中的事件交叉启动，以查看 Secure Network Analytics 设备上的相关数据。

默认情况下，系统会根据您指定的时间范围自动选择适当的数据源。如果要覆盖数据源，请使用此程序。

重要事项 当您更改数据源时，您的选择会在依赖于事件数据源的所有相关分析功能（包括报告）中保持不变，直到您对其进行更改（即使在您注销后）。您的选择不适用于其他 管理中心 用户。

所选数据源仅用于低优先级连接事件。所有其他事件类型（入侵，文件和恶意软件事件；与这些事件关联的连接事件；以及安全情报事件）都会显示，无论数据源如何。

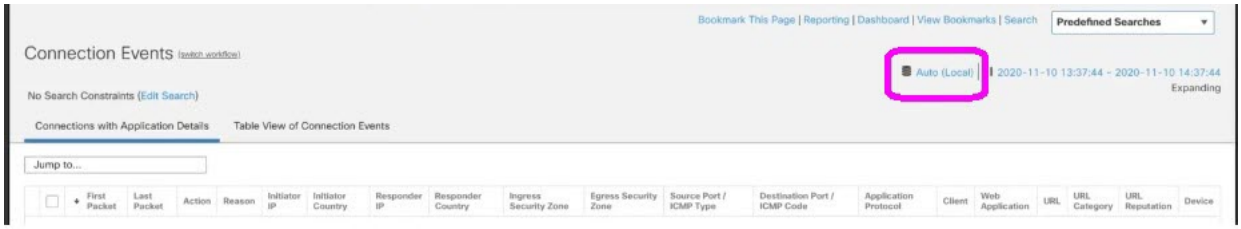
开始之前

您已使用向导向 安全分析和日志记录（本地部署）发送连接事件。

过程

步骤 1 在 管理中心 Web 界面中，导航至显示连接事件数据的页面，例如 **分析 >连接 > 事件**。

步骤 2 点击此处显示的数据源并选择一个选项：



注意 如果选择**本地**，则系统仅显示管理中心上的可用数据，即使本地数据在所选的整个时间范围内不可用。您不会收到此情况的通知。

步骤 3 （可选）要直接在 Secure Network Analytics 设备中查看相关数据，请右键点击（在统一事件查看器中，点击）IP 地址或域等值，然后选择交叉启动选项。

地理定位

您可以利用地理位置数据库 (GeoDB) 根据国家/地区和大洲查看和过滤流量。请注意，对于检测到在不同国家/地区之间移动的移动设备和其他主机，系统可能会报告大洲而不是具体的国家/地区。

系统随附一个将 IP 地址映射到国家/地区/大洲的初始 GeoDB 国家/地区代码包，因此信息应始终可用。系统还可以下载包含上下文数据的 IP 包。这可能包括：

- 地区（州、省或其他国家/地区）、城市和邮政编码。
- 纬度/经度、时区和可点击地图。
- 自治系统编号 (ASN)，以及与该 ASN 有关的其他信息。
- 互联网服务提供商 (ISP)、连接类型和代理类型。
- 家庭/企业、组织和域名信息。

要查看此信息，请点击事件、资产配置文件、情景管理器、控制面板和其他分析工具中出现的小国家/地区标志图标和 ISO 国家/地区代码。无法在“连接摘要”(Connection Summary) 之类的控制面板上查看地理定位详细信息来获取汇聚的地理定位信息。

我们定期发布 GeoDB 更新。您必须定期更新 GeoDB 以获取准确的地理位置信息；请参阅 更新地理位置数据库 (GeoDB)，第 216 页。

相关主题

网络条件
地理定位
关联策略和规则简介，第 939 页
流量量变曲线条件，第 979 页
更新地理位置数据库 (GeoDB)，第 216 页

连接事件图形

除使用表格向下钻取页面的工作流程和事件的最终表格视图之外，系统可以用在五分钟间隔内汇聚的数据以图形方式展示某些连接数据。请注意，您只可以用图形显示用于汇聚数据的信息：源和目标 IP 地址（以及那些主机的关联用户）、目标端口、传输协议以及应用协议。

提示 您无法将安全情报事件与其关联连接事件分开单独用图形展示。有关安全情报过滤活动的图形概述，请使用控制面板和情景管理器。

有三种不同类型的连接图形：

- 饼形图，显示按各种类别分组的一个数据集中的数据。
- 条形图，显示按各种类别分组的一个或多个数据集中的数据。
- 曲线图，用标准或速度（更改速率）视图图示一个或多个数据集随着时间推移的数据。

注释 系统用曲线图显示流量量变曲线，您可以操作其他任何连接图的方式操作这些图形，但会有一些限制。要查看流量量变曲线，您必须具有管理员访问权限。

与工作流程表一样，您可以向下钻取并限制工作流程图，以重点关注您的分析。

条形图和曲线图可以显示多个数据集；也就是说，它们可以在 y 轴为每个 x 轴数据点显示几个值。例如，您可以显示独立发起方和响应方的总数。饼形图只能显示一个数据集。

通过改变 x 轴、y 轴或者 x 轴和 y 轴，可以在连接图上显示不同的数据和数据集。在饼形图上改变 x 轴可以改变自变量，改变 y 轴可以改变因变量。

相关主题

连接摘要（图形的汇聚数据），第 716 页

使用连接事件图形

在 管理中心上，可以查看连接事件图形并根据要查找的信息操纵这些图形。

访问连接图时看到的页面因所用的工作流程而有所不同。可以使用预定义的工作流程，最终会产生连接事件表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

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**分析** > **连接** > **事件**。

注释 如果显示的是连接事件表而非图形，或者要查看不同图形，请按工作流程标题点击（**切换工作流程**）**([switch workflow])**，然后选择包括图形的预定义工作流程或选择自定义工作流程。请注意，所有预定义连接事件工作流程（包括连接图）最终都会产生连接的表视图。

步骤 2 您有以下选择：

- 时间范围 - 要调整时间范围（如果是空图形会非常有用），请参阅更改时间窗口，第 661 页。
- 字段名称 - 要详细了解可以用图形表示的数据，请参阅连接和 安全相关连接 事件字段，第 717 页。
- 主机配置文件 - 要查看某个 IP 地址的主机配置文件，请在按发起方或响应方显示连接数据的图形上，点击条形图的某一条或饼形图的某一块，然后选择**查看主机配置文件 (View Host Profile)**。
- 用户配置文件 - 要查看用户配置文件信息，请在按发起方用户显示连接数据的图形上，点击条形图的某一条或饼形图的某一块，然后选择**查看用户配置文件 (View User Profile)**。

- 其他信息 - 要了解有关绘图数据的详细信息，请将光标移动至曲线图的某一点上、条形图的某一条上或饼形图的某一块上。
- 限制 - 要按任意 x 轴（自变量）条件限制连接图形而不前进到工作流程中的下一页，请点击曲线图的某一点、条形图的某一条或饼形图的某一块，然后选择**查看依据...** 选项，允许或拒绝 VPN 核心模块和其他可选模块的软件更新。
- 数据选择 - 要更改图形中显示的数据，请点击 **X 轴 (X-Axis)** 或 **Y 轴 (Y-Axis)**，然后选择要用图形表示的新数据。请注意，将 x 轴更改为**时间 (Time)** 或反之，还会更改图形类型；改变 y 轴会影响显示的数据集。
- 数据集 - 要更改图形的数据集，请点击**数据集 (Datasets)**，然后选择新的数据集。
- 分离 - 要分离连接图形以便在不影响默认时间范围的情况下执行进一步分析，请点击**分离 (Detach)**。

  提示 在分离图中点击**新建窗口 (New Window)** 可创建副本。然后，您可以在每个分离图上进行不同分析。请注意，流量剖面图是分离图形。

- 向下展开 - 要向下展开到工作流程中的下一页，请点击曲线图上的某一点、条形图上的某一条或饼形图上的某一块，然后选择**向下展开 (Drill-down)**。点击曲线图上的某个点可将下一个页面的时间范围更改为以所点击点为中心的10分钟时间区间。点击条形图上的某一条或饼形图上的某一块，可基于该条或该块表示的标准限制下一个页面。
- 导出 - 要将图形的连接数据导出为 CSV（逗号分隔值）文件，请点击**导出数据 (Export Data)**。然后，点击**下载 CSV 文件 (Download CSV File)**，并保存文件。
- 图形类型：曲线图 - 要在标准曲线图与速度（变化率）曲线图之间切换，请点击**速度 (Velocity)**，然后选择**标准 (Standard)** 或**速度 (Velocity)**。
- 图表类型：条形图和饼形图 - 要在条形图与饼形图之间切换，请点击**切换为条形图 (Switch to Bar)** 或**切换为饼形图 (Switch to Pie)**。因为不能在饼形图上显示多个数据集，如果将具有多个数据集的条形图切换到饼形图，该饼形图只显示一个自动选择的数据集。当选择要显示的数据集时，管理中心会首选显示总统计信息，而不是发起方和响应方的统计信息；在显示发起方统计信息和响应方统计信息时，会首选显示发起方统计数据。
- “在页面之间导航”(Navigate Between Pages) - 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- “在事件视图之间导航”(Navigate Between Event Views) - 要导航至其他事件视图以查看关联事件，请点击**跳转至 (Jump to)** 并从下拉列表中选择事件视图。
- “重定中心”(Recenter) - 要围绕某个时间点重定曲线图的中心而不更改时间范围的长度，请点击该点，然后选择**重定中心 (Recenter)**。
- “缩放”(Zoom) - 要围绕某个时间点重定曲线图的中心，同时进行放大或缩小，请点击该点，选择**缩放 (Zoom)**，然后选择新的时间区间。

注释 除非使用分离图，否则限制、重定中心和缩放会改变 管理中心的默认时间范围。

示例

示例：限制连接图形

思考一个长时间区间连接的图形。如果在按端口图形上应用时间点限制，系统会显示一个条形图，列出基于检测到的连接事件数目、同时受以所点击点为中心的 10 分钟时间区间限制的 10 个最活跃的端口。

如果通过点击条形图中的一条并选择**按发起方 IP 查看 (View by Initiator IP)** 进一步限制该图形，系统将显示一个新的条形图。该条形图不仅受到与之前相同的 10 分钟时间区间的限制，还受到所点击条柱表示的端口的限制。

示例：更改饼形图上的 X 轴和 Y 轴

考虑一个图形化显示各端口数据量的饼形图。在这种情形下，x 轴是**响应方端口 (Responder Port)**，y 轴是 **KBytes**。该饼图表示在一定时间区间内由监控网络发送的总数据量。该饼图的楔块表示在每端口上检测到的数据百分比。

- 如果将该饼图 x 轴变更为**应用协议 (Application Protocol)**，该饼图仍然表示已传输的总数据量，但该饼图的楔块表示为每个已检测到应用协议传输的数据百分比。
- 如果将该图形的 y 轴改为**数据包数 (Packets)**，该饼形图表示在一定时间区间内监控网络传输的数据包总数，而形饼图的楔块表示每个端口上检测到的数据包在数据包总数中所占的百分比。

相关主题

使用工作流程，第 642 页
配置事件视图设置，第 193 页

连接图形数据选项

通过改变 x 轴、y 轴或者 x 轴和 y 轴，可以在连接图上显示不同的数据。在饼形图上改变 x 轴可以改变自变量，改变 y 轴可以改变因变量。

表 *90: X* 轴选项

X 轴选项	图表类型	绘制此数据的方式
应用协议	条形图或饼形图	通过 10 个最活跃的应用协议
设备	条形图或饼形图	通过 10 个最活跃的受管设备
发起方 IP	条形图或饼形图	通过 10 个最活跃的发起方主机 IP 地址

X 轴选项	图表类型	绘制此数据的方式
发起方用户	条形图或饼形图	通过 10 个最活跃的发起方用户
响应方 IP	条形图或饼形图	通过 10 个最活跃的响应方主机 IP 地址
响应方端口 (Responder Port)	条形图或饼形图	通过 10 个最活跃的响应方端口
源设备	条形图或饼形图	通过 10 个最活跃的 NetFlow 数据导出器，以及 Firepower 系统受管设备检测到的所有连接的名为 `Firepower` 的源设备。
时间	折线图	在一段时间内 在**时间 (Time)** 中更改 y 轴的结束和起始时间也会更改图形类型，并可能更改数据集。

表 *91: Y* 轴选项

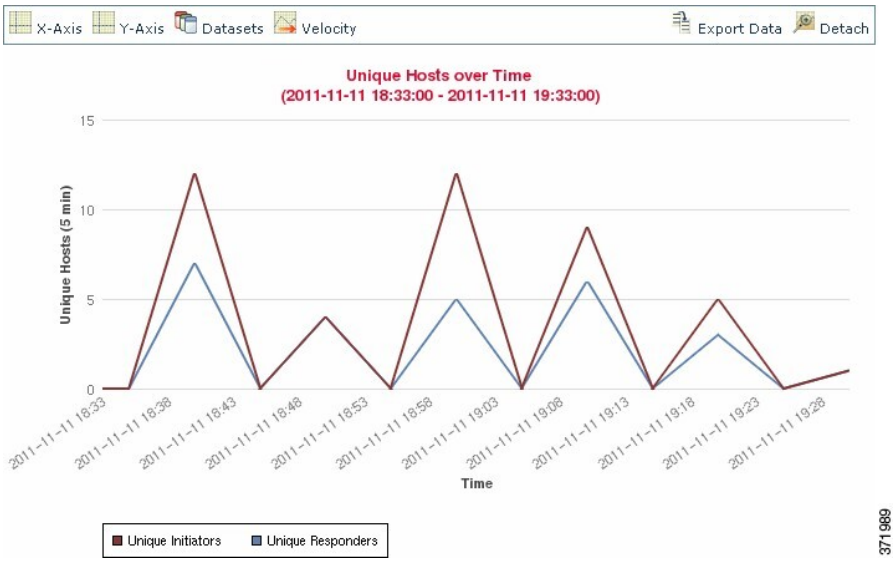
Y 轴选项	使用 X 轴标准绘制此数据
字节	传输的字节数
连接	连接数量
KBytes	传输的千字节数
KBytes Per Second	每秒的千字节数
数据包	传输的数据包数量
独立主机	检测到的独立主机数量
独立应用协议	独立应用协议数量
唯一用户	独立用户数量

具有多个数据集的连接图形

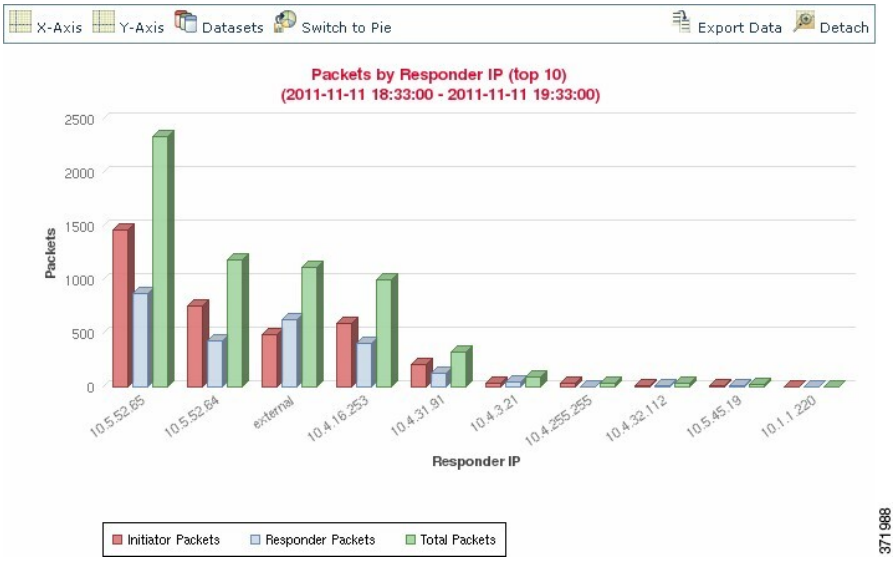
条形图和曲线图可以显示多个数据集；也就是说，它们可以在 y 轴为每个 x 轴数据点显示几个值。例如，您可以显示独立发起方和响应方的总数。

注释 饼形图上**不能**显示多个数据集。如果将具有多个数据集的条形图切换到饼形图，该饼形图只显示一个自动选择的数据集。当选择要显示的数据集时，管理中心会首选显示总统计信息，而不是发起方和响应方的统计信息；在显示发起方统计信息和响应方统计信息时，会首选显示发起方统计数据。

在曲线图上，多个数据集显示为多条线，每条线颜色不同。例如，下面的图形显示了在一个小时的时间区间内监控网络上检测到的独立发起方总数和独立响应方总数。



在条形图上，与 x 轴的各个数据点对应的多个数据集显示为一组彩色条形柱。例如，下面的条形图显示监控网络上传输的数据包总数、发起方传输的数据包总数以及响应方传输的数据包总数。



连接图形数据集选项

下表介绍了在连接图 x 轴上可以显示的数据集。

表 *92:* 数据集选项

如果 y 轴显示...	可以选为数据集的对象为...
连接	仅默认数量，即在受监控网络上检测到的连接数（**连接数 [Connections]**）这是流量配置文件图的唯一选项。
千字节数 (KBytes)	组合： • 监控网络上传输的总数据量（**总千字节数 [Total KBytes]**） • 监控网络上的主机 IP 地址传输的数据量（**发起方千字节数 [Initiator KBytes]**） • 监控网络上的主机IP地址收到的数据量（**响应方千字节数 [Responder KBytes]**）
每秒千字节数 (KBytes Per Second)	仅默认数量，指在监控网络上每秒传输的总数据量（**每秒总千字节数 [Total KBytes Per Second]**）
数据包	组合： • 在监控网络上传输的数据包总数（**数据包总数 [Total Packets]**） • 在监控网络上从主机 IP 地址传输的数据包总数（**发起方数据包数 [Initiator Packets]**） • 在监控网络上主机 IP 地址收到的数据包总数（**响应方数据包数 [Responder Packets]**）
独立主机数 (Unique Hosts)	组合： • 在监控网络上独立会话发起方的数量（**独立发起方数 [Unique Initiators]**） • 在监控网络上独立会话响应方的数量（**独立响应方数 [Unique Responders]**）
独立应用协议数 (Unique Application Protocols)	仅默认数量，指监控网络上的独立应用协议的数量（**独立应用协议数 [Unique Application Protocols]**）
唯一用户	仅默认数量，指登录到监控网络上会话发起方的独立用户的数量（**独立发起方用户数 [Unique Initiator Users]**）

事件时间限制

每个事件具有指示事件发生时间的时间戳。可以通过设置时间窗口（有时称为时间范围）限制某些工作流程中显示的信息。

基于可按时间限制的事件的工作流程在页面顶部具有一条时间范围线。

默认情况下，工作流程使用设置为前一小时的扩展式时间窗口。例如，如果您在上午 11:30 登录，将会看到发生在上午 10:30 和上午 11:30 之间的事件。随着时间的推进，时间窗口进行扩展。在中午 12:30，您将会看到发生在上午 10:30 和中午 12:30 之间的事件。

可以通过在事件视图设置中设置自己的默认时间窗口来更改此行为：该时间窗口管理三个属性：

- 时间窗口类型（静态、扩展式或滑动式）
- 时间窗口长度
- 时间窗口数量（多个时间窗口或单个全局时间窗口）

无论默认时间窗口设置如何，都可以在事件分析期间手动更改时间窗口，方法是点击页面顶部的时间范围，该页面会显示“日期/时间”(Date/Time) 弹出窗口。根据配置的时间窗口数量和使用的设备类型，还可以使用“日期/时间”(Date/Time) 窗口更改所查看的事件类型的默认时间窗口。

最后，您可以在查看滑动式或扩展式工作流程时暂停时间窗口。请参阅暂停时间窗口以暂时冻结数据集，第 661 页。

相关主题

配置事件视图设置，第 193 页
使用连接和 安全相关连接 事件表，第 741 页

事件的每次会话时间窗口自定义

无论默认时间窗口设置如何，都可以在事件分析期间手动更改时间窗口。

注释 手动时间窗口设置仅对当前会话有效。在注销然后重新登录时，时间窗口会重置为默认值。

根据配置的时间窗口数量，更改一个工作流程的时间窗口可能会影响设备上的其他工作流程。例如，如果具有单个全局时间窗口，则更改一个工作流程的时间窗口会更改设备上所有其他工作流程的时间窗口。另一方面，如果使用的是多个时间窗口，则更改审核日志或运行状况事件工作流程时间窗口对于任何其他时间窗口没有影响，而更改其他种类的事件的时间窗口则会影响可按时间限制的所有事件（审核事件和运行状况事件除外）。

请注意，由于并非所有工作流程都可按时间限制，因此时间窗口设置对基于主机、主机属性、应用、应用详情、漏洞、用户或 allow 名单违例的工作流程没有影响。

使用“日期/时间”窗口上的“时间窗口”选项卡可手动配置时间窗口。根据在默认时间窗口设置中配置的时间窗口数量，选项卡的标题为以下之一：

- **事件时间窗口** - 如果配置了多个时间窗口，并且是为除审核日志和运行状况事件工作流程以外的工作流程设置的时间窗口
- **运行状况监控时间窗口** - 如果配置了多个时间窗口，并且是为运行状况事件工作流程设置的时间窗口
- **审核日志时间窗口** - 如果配置了多个时间窗口，并且是为审核日志设置的时间窗口

- **全局时间窗口** - 如果配置了单个时间窗口

配置时间窗口时必须首先决定要使用的时间窗口的类型。

- 静态时间窗口显示从特定开始时间到特定结束时间生成的所有事件。
- 扩展式时间窗口显示从特定开始时间到目前生成的所有事件；随着时间的推进，时间窗口会进行扩展，并会有新事件添加到事件视图中。
- 滑动式时间窗口显示从特定开始时间（例如，一周前）到目前生成的所有事件；刷新页面时，时间窗口会“滑动”，以便仅显示您配置的时间范围（在此示例中是上周）内的事件。要在检查数据集时暂时阻止更新数据集，请参阅暂停时间窗口以暂时冻结数据集，第 661 页。

根据选择的类型，“日期/时间”窗口会更改以提供不同的配置选项。

注释 Firepower 系统根据在时区首选项中指定的时间使用 24 小时制时钟。

时间窗口设置

下表说明可在 Time Window 选项卡上配置的各种设置。

表 *93:* 时间窗口设置

设置	时间段类型	说明
时间段类型下拉列表	n/a	选择要使用的时间段类型：静态、扩展式或滑动式。 请注意，如果按时间限制事件视图，则在设备配置的时间窗口外生成的事件（无论是全局还是特定事件）可能显示在事件视图中。即使为设备配置了滑动时间窗口，也可能发生这种情况。
“开始时间”(Start Time) 日历	静态和扩展式	指定时间段的开始日期和时间。所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。 可以使用“预设”(Presets) 选项而不是使用日历，如下所述。
“结束时间”(End Time) 日历	静态	指定时间段的结束日期和时间。所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。 请注意，如果使用的是扩展式时间段，则“结束时间”(End Time) 日历会灰显并指定结束时间为“现在”(Now)。 可以使用“预设”(Presets) 选项而不是使用日历，如下所述。
显示“最后”(Last) 字段和下拉列表	滑动式	配置滑动式时间段的长度。
预设：最后 (Presets: Last)	all	根据设备的本地时间，点击列表中的其中一个时间范围以更改时间段。例如，点击 **1 周 (1 week)** 会将时间段更改为反映上周。点击预设会将日历更改为反映选择的预设。

设置	时间段类型	说明
预设：当前 (Presets: Current)	静态和扩展式	根据设备的本地时间和日期，点击列表中的其中一个时间范围以更改时间段。点击预设会将日历更改为反映选择的预设。 请注意： • 当日在午夜开始 • 当周在星期天午夜开始 • 当月在月份第一日午夜开始
预设：同步 (Presets: Synchronize with)	所有（如果使用的是全局时间段则不适用）	点击其中一项： • **事件时间段 (Events Time Window)** 将当前时间段与事件时间段同步 • **运行状况监控时间段 (Health Monitoring Time Window)** 将当前时间段与运行状况监控时间段同步 • **审核日志时间段 (Audit Log Time Window)** 将当前时间段与审核日志时间段同步

更改时间窗口

过程

步骤 1 在按时间限制的工作流程中，点击 **时间范围**（ ） 以转至“日期/时间”(Date/Time) 窗口。

步骤 2 在**事件时间窗口 (Events Time Window)** 上，设置时间窗口，如时间窗口设置，第 660 页中所述。

提示 点击**重置 (Reset)** 以将时间窗口重新更改为默认设置。

步骤 3 点击**应用 (Apply)**。

暂停时间窗口以暂时冻结数据集

如果您正在使用滑动式或扩展式时间窗口，您可以暂停时间窗口来检查工作流程提供的数据快照。这样会有所帮助，因为未暂停的工作流程在更新时，可能会移除要检查的事件，或者添加无关的事件。

当您点击页面底部的链接以显示另一事件页面时，时间窗口会自动暂停；您可以在准备好时取消暂停时间窗口。

完成分析后，可以取消暂停时间窗口。取消暂停时间窗口将根据您的喜好对其进行更新，并且还更新事件视图以反映已取消暂停的时间窗口。

暂停事件时间窗口对控制面板没有影响，而暂停控制面板对暂停事件时间窗口也没有任何影响。

过程

在受时间限制的工作流程上，选择所需的时间范围控件：

- 要暂停时间窗口，请点击时间范围控件 **暂停**（ ）。
- 要取消暂停时间窗口，请点击时间范围控件 **播放**（ ）。

事件的默认时间窗口

在事件分析期间，可以使用“日期/时间”(Date/Time) 窗口上的“首选项”(Preferences) 选项卡更改所查看的事件类型的默认时间窗口，而不必使用事件视图设置。

请记住，以此方式更改默认时间窗口仅会更改所查看的事件类型的默认时间窗口。例如，如果配置了多个时间窗口，则更改“首选项”(Preferences) 选项卡上的默认时间窗口会更改事件、运行状况监控或审核日志窗口的设置，换句话说，以第一个选项卡指示的时间窗口为准。如果配置了单个时间窗口，则更改“首选项”(Preferences) 选项卡上的默认时间窗口会更改所有事件类型的默认时间窗口。

相关主题

默认时间窗口，第 195 页

事件类型的默认时间窗口选项

下表说明可在 Preferences 选项卡上配置的各种设置。

表 *94:* 时间窗口首选项

偏好	说明
刷新间隔	设置事件视图的刷新间隔（以分钟为单位）。输入零会禁用刷新选项。
时间窗口数	指定要使用的时间窗口数量： • 选择**多个 (Multiple)** 以根据可按时间限制的事件为审核日志、运行状况事件和工作流程配置单独的默认时间窗口。 • 选择**单个 (Single)** 以使用适用于所有事件的全局时间窗口。
默认时间窗口：显示最后时间 - 滑动式	此设置允许配置指定长度的滑动式默认时间窗口。 设备显示在某个特定开始时间（例如，1 小时前）和当前时间期间生成的所有事件。更改事件视图时，时间窗口会“滑动”，以便始终显示最后一小时的事件。

偏好	说明
默认时间窗口：显示最后时间 - 静态/扩展式	此设置允许配置指定长度的静态或扩展式默认时间窗口。 对于**静态**时间窗口（启用**使用结束时间 [Use End Time]** 复选框），设备显示从特定开始时间（例如，1 小时前）到首次查看事件时生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。 对于**扩展式**时间窗口（禁用**使用结束时间 [Use End Time]** 复选框），设备显示从特定开始时间（例如，1 小时前）到目前生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。
默认时间窗口：当日 - 静态/扩展式	此设置允许配置当日的静态或扩展式默认时间窗口。当日从午夜开始，基于当前会话的时区设置。 对于**静态**时间窗口（启用**使用结束时间 [Use End Time]** 复选框），设备显示从午夜到首次查看事件时生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。 对于**扩展式**时间窗口（禁用**使用结束时间 [Use End Time]** 复选框），设备显示从午夜到目前生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。请注意，如果在您注销之前，分析持续 24 小时以上，则此时间窗口可以超过 24 小时。
默认时间窗口：当周 - 静态/扩展式	此设置允许配置当周的静态或扩展式默认时间窗口。当周从上一周日的午夜开始，基于当前会话的时区设置。 对于**静态**时间窗口（启用**使用结束时间 [Use End Time]** 复选框），设备显示从午夜到首次查看事件时生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。 对于**扩展式**时间窗口（禁用**使用结束时间 [Use End Time]** 复选框），设备显示从星期天午夜到目前生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。请注意，如果在您注销之前，分析持续 1 周以上，则此时间窗口可以超过 1 周。

更改事件类型的默认时间窗口

过程

步骤 1 在按时间限制的工作流程中，点击 **时间范围**（ ） 以转至“日期/时间”窗口。

步骤 2 点击 **首选项** 选项卡并更改您的首选项，如 事件类型的默认时间窗口选项，第 662 页表中所述。

步骤 3 点击**保存首选项**。

步骤 4 此时您有两种选择：

- 要将新的默认时间窗口设置应用于所使用的事件视图，请点击**应用**以关闭“日期/时间”窗口并刷新事件视图。

- 要继续分析而不应用默认时间窗口设置，请关闭“日期/时间”窗口而不点击**应用**。

事件视图限制

工作流程页面上显示的信息由实施的限制来确定。例如，最初打开事件工作流程时，信息限制为前一小时生成的事件。

要前进到工作流程中的下一页并通过特定值限制所查看的数据，请选择页面上具有这些值的行，然后点击**查看 (View)**。要前进到工作流程中的下一页并保留当前限制和传递所有事件，请选择**查看全部 (View All)**。

注释 如果选择含有多个非计数值的行并点击**查看 (View)**，则会创建复合限制。

限制工作流程中的数据有第三种方法。要将页面限制为含有选定值的行，并且还将选定值添加到页面顶部的限制列表中，请点击页面上某一行中的值。例如，如果查看的是已记录连接的列表，并要使用访问控制将该列表仅限于允许的连接，请点击**操作 (Action)** 列中的**允许 (Allow)**。又例如，如果查看的是入侵事件，并要将列表仅限于目标端口为 80 的事件，请点击**目标端口/ICMP 代码 (Destination Port/ICMP Code)** 列中的 **80 (http)/tcp**。

提示 根据监控规则条件来限制连接事件的程序略有不同，可能需要采取一些额外步骤。此外，不能按关联文件或入侵信息来限制连接事件。

还可以使用搜索来限制工作流程中的信息。要根据一列中的多个值进行限制时，请使用此功能。例如，如果要查看与两个 IP 地址相关的事件，请点击**编辑搜索 (Edit Search)**，然后修改“搜索”(Search) 页面上相应的 IP 地址字段以将两个地址均包含在内，然后点击**搜索 (Search)**。

在搜索页面上输入的搜索条件会列为页面顶部的限制，并且产生的事件相应地受限制。在 管理中心 中，除非当前限制是复合限制，否则导航到其他工作流程时也会应用这些限制。

在搜索时，必须特别注意搜索限制是否适用于所搜索的表。例如，客户端数据在连接摘要中不可用。如果根据连接中检测到的客户端搜索连接事件，然后在连接摘要事件视图中查看结果，则 管理中心 会显示连接数据，如同其完全未受限制一样。无效限制会标示为不适用 (N/A)，并带有删除线标记。

限制事件

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如工作流程选择，第 644 页中所述。

步骤 2 在任何工作流程中，您有以下选择：

- 要将视图限于与单个值相匹配的事件，请点击页面上行中的所需值。

- 要将视图限于与多个值相匹配的事件，请选中具有这些值的事件的对应复选框，然后点击**视图 (View)**。

  注释 如果行包含多个非计数值，则会添加复合限制。

- 要删除限制，请点击“搜索限制” **展开箭头**（ ），然后点击展开的“搜索限制”(Search Constraints) 列表中的限制名称。
- 要使用“搜索”(Search) 页面编辑限制，请点击**编辑搜索 (Edit Search)**。
- 要将限制另存为已保存的搜索，请点击**保存搜索 (Save Search)** 并指定查询名称。

  注释 不能保存包含复合限制的查询。

- 要对其他事件视图使用相同限制，请点击**跳至 (Jump to)** 并选择事件视图。

  注释 当切换到其他工作流程时，不会保留复合限制。

- 要切换限制的显示，请点击“搜索限制”**展开箭头**（ ）或“搜索限制” **折叠箭头**（ ）。这在限制列表较大并占据大部分屏幕时有用。

复合事件视图限制

复合限制基于特定事件的所有非计数值。选择含有多个非计数值的行时，需要设置复合限制，该限制仅检索与该页面上的该行中所有非计数值都匹配的事件。例如，如果选择源 IP 地址为 `10.10.31.17` 且目标 IP 地址为 `10.10.31.15` 的行以及源 IP 地址为 `172.10.10.17` 且目标 IP 地址为 `172.10.10.15` 的行，则会检索下列所有内容：

- 源 IP 地址为 10.10.31.17 且目标 IP 地址为 10.10.31.15 的事件

  或

- 源 IP 地址为 172.10.31.17 且目标 IP 地址为 172.10.31.15 的事件

将复合限制与简单限制组合时，简单限制分布在各复合限制集合中。例如，如果在以上所列的复合限制中为协议值 `tcp` 添加了一条简单限制，则会检索下列所有内容：

- 源 IP 地址为 10.10.31.17 且目标 IP 地址为 10.10.31.15 且协议为 tcp 的事件

  或

- 源 IP 地址为 172.10.31.17 且目标 IP 地址为 172.10.31.15 且协议为 tcp 的事件

不能对复合限制执行搜索或保存搜索操作。您也不能在使用事件视图链接或点击（**切换工作流程**）以切换到其他工作流程时保留复合限制。如果将应用了复合限制的事件视图加入书签，则不使用书签保存限制。

使用复合事件视图限制

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如工作流程选择，第 644 页中所述。

步骤 2 要管理复合限制，您有以下选择：

- 要创建复合限制，请选择一个或多个具有多个非计数值的行，然后点击**查看 (View)**。
- 要清除复合限制，请点击“搜索限制” **展开箭头** （ ） 并点击 **复合限制**。

工作流程间导航

您可以使用工作流程页面上的**跳至...(Jump to...)**）下拉列表中的链接导航到其他工作流程。选择下拉列表以查看并选择其他工作流程。

选择新工作流程时，所选行共享的属性和所设置的限制用于新工作流程中（如果其适用）。如果配置的限制或事件属性没有映射到新工作流程中的字段，则表明其已丢弃。此外，从一个工作流程切换到另一个工作流程时未保留复合限制。而且，捕获的文件工作流程中的限制仅传输到文件和恶意软件事件工作流程。

注释 查看某个时间范围的事件计数时，事件的总数可能无法反映为其提供了更详细数据的事件的数量。因为系统有时会删掉较旧的事件详情以管理磁盘空间使用情况，所以会发生这种情况。要将事件详情删除的情况降到最少，您可以微调事件日志记录，以只记录对部署最重要的事件。

请注意，除非已暂停时间段或已配置静态时间段，否则在更改工作流程时时间段会更改。

此功能可增强您调查可疑活动的能力。例如，如果查看的是连接数据并发现内部主机在向外部站点传送异常大量的数据，则可以选择响应方 IP 地址和端口作为限制，然后跳至**应用 (Applications)** 工作流程。应用工作流程将使用响应方 IP 地址和端口作为 IP 地址和端口限制，并显示有关应用的其他信息，如应用的种类。也可以点击页面顶部的**主机 (Hosts)** 以查看远程主机的主机配置文件。

在找到有关应用的详细信息后，可以选择**关联事件**以返回到连接数据工作流程，从限制中删除响应方 IP，向限制中添加发起方 IP，然后选择**应用详细信息**以了解发起主机上的用户在将数据传输到远程主机时使用了哪个客户端。请注意，端口限制未转移到“应用详细信息”(Application Details) 页面。保持本地主机作为限制时，也可以使用其他导航按钮查找其他信息。

- 要发现本地主机是否已违反任何策略，请保持 IP 地址作为限制并从**跳至 (Jump to)** 下拉列表中选择**关联事件 (Correlation Events)**。
- 要了解是否对主机触发了指示危害的入侵规则，请从**跳至 (Jump to)** 下拉列表中选择**入侵事件 (Intrusion Events)**。

- 要查看本地主机的主机配置文件并确定主机是否易受可能已被利用的任何漏洞的攻击，请从**跳至 (Jump to)** 下拉列表中选择**主机 (Hosts)**。

使用统一事件查看器操作

统一事件为您提供多种类型（连接、入侵、文件、恶意软件和一些安全相关的连接事件）的单一屏幕视图。统一事件表可高度自定义。您可以创建和应用自定义过滤器，以微调事件查看器上显示的信息。通过“统一事件”表中的**实时视图**选项，您可以实时查看防火墙事件并监控网络上的活动。

使用统一事件查看器执行以下操作：

- 查找不同类型事件之间的关系
- 实时查看策略更改的影响

过程

步骤 1 选择**分析** > **统一事件**。

步骤 2 选择时间范围（固定或滑动）以查看特定时间段的防火墙事件。默认情况下，统一事件查看器表显示前一小时的事件。您可以过滤该表以获取更精细的安全事件上下文，自定义表列，或启用实时视图并实时查看事件更新。

有关统一事件的详细信息，请参阅 关于统一事件。

书签

如果要在事件分析中快速返回到特定位置和时间，请创建书签。书签保留以下有关信息：

- 使用的工作流程
- 查看的工作流程部分
- 工作流程中的页码
- 任何搜索限制
- 任何已禁用列
- 使用的时间范围

创建的书签可供具有书签访问权限的所有用户帐户使用。这意味着，如果发现需要深入分析的事件集，则可以轻松创建书签并将调查移交给具有相应特权的其他用户。

注释 如果删除书签中显示的事件（直接由用户删除或通过自动数据库清除），则书签不再显示原始事件集。

创建书签

在多域部署中，只能查看在当前域中创建的书签。

过程

步骤 1 在事件分析期间，显示了有关事件的情况下，点击 **Bookmark This Page**。

步骤 2 在**书签名称 (Bookmark Name)** 字段中，输入名称。

步骤 3 点击**保存书签 (Save Bookmark)**。

查看书签

在多域部署中，只能查看在当前域中创建的书签。

过程

从任何事件视图中，您有两个选项：

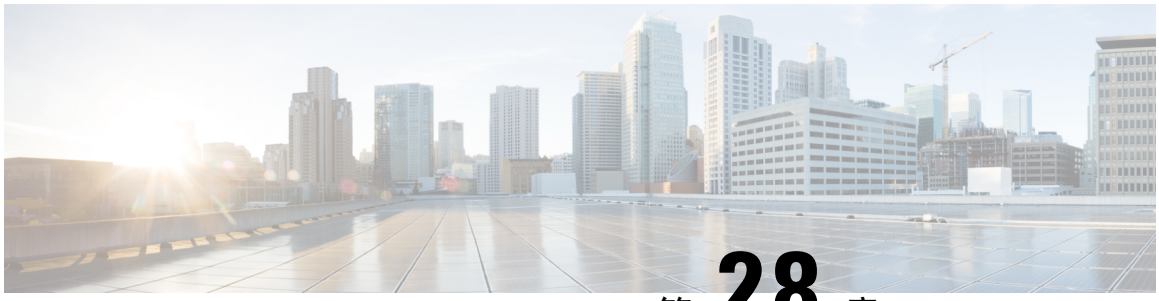
- 将指针悬停在**查看书签 (View Bookmarks)** 上方，然后点击下拉菜单中的所需书签。
- 点击 **查看书签**，然后在“查看书签”页面上，点击所需的书签名称或其旁边的 **视图**（  ）。

  注释 如果删除书签中最初显示的事件（直接由用户删除或通过自动数据库清除），则书签不再显示原始事件集。

工作流程历史记录

表 *95:*

功能	最低 管理中心	最低 威胁防御	详细信息
已弃用：入侵事件和事件剪贴板。	7.1	任意	入侵事件和事件剪贴板已弃用。 弃用的屏幕： • **分析 > 入侵 > 事故** • **分析 > 入侵 > 事故**
统一事件查看器。	7.0	任意	在单个表中查看和处理多种事件类型：连接（包括安全情报）、入侵、文件和恶意软件。 新增/修改的屏幕： **分析 > 统一事件**
处理远程存储的事件。	7.0	任意	您可以使用 FMC 处理存储在 Secure Network Analytics 设备上的连接事件。系统会自动使用最合适的数据源，您也可以明确选择数据源。仅当您已完成 安全分析和日志记录（本地部署） 向导时，才会显示此选项。 新增/修改的屏幕：显示连接事件的页面，例如事件查看器、控制面板、上下文资源管理器和报告。
在某些情况下提高了工作流程表的加载速度。	6.6	任意	工作流程页面上的表现在仅在不超过六列时显示相同行的计数列。这可以最大限度地减少所需的计算量，从而提高表加载速度。 新增/修改的屏幕：事件查看器。



第 28 章

事件搜索

以下主题介绍如何在工作流程中搜索事件：

事件搜索

Firepower 系统生成的信息作为事件存储在数据库表中。事件包含多个字段，描述导致设备生成事件的活动。您可以创建并保存面向您的环境为任何不同事件类型自定义的搜索，并将其保存以供今后重复使用。

保存搜索时，请为其命名，并指定此搜索仅供您自己使用还是供设备的所有用户使用。如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。如果先前保存了一个搜索，则可加载该搜索，做出任何必要更改，然后开始搜索。自定义分析控制面板构件、报告模板和自定义角色也可以使用保存的搜索。如有已保存的搜索，可从 Search 页面删除这些搜索。

对于某些事件类型，Firepower 系统会提供预定义搜索，既可将其用作示例，又可借助其快速访问有关网络的重要信息。可针对网络环境修改预定义搜索中的字段，然后保存搜索，以供日后重复使用。

可使用的搜索条件取决于搜索类型，但搜索技巧相同。搜索仅返回与所有字段的指定搜索条件匹配的记录。

注释 搜索自定义表所需的程序略有不同。

相关主题

搜索自定义表，第 694 页

搜索限制

每个数据库表都有自己的搜索页面，您可以在此页面中输入搜索限制值以应用于为该表定义的字段。根据字段的类型，可使用专用语法来指定条件，例如通配符或数值范围。

搜索结果显示在工作流程页面，以柱状布局显示每个表字段。某些数据库表还可使用未在工作流程页面显示为列的字段进行搜索。查看工作流程页面中的结果时，要确定此类限制是否适用于搜索结果，请点击 **展开箭头** （ ） 以查看活动的搜索限制。

通用搜索限制

搜索事件时，请遵循以下通用准则：

- 许多字段需要通配符才能进行部分匹配搜索。所有字段都接受这些搜索的通配符。

  请参阅搜索中的通配符和符号 ， 第 672 页。

- 所有字段接受协商 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A、B、"C、D、E" (A, B, "C, D, E")` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C、D、E" ("C, D, E")` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 在任何字段中指定 `n/a` 表示无字段相关信息的事件；使用 `!n/a` 表示该字段已填充的事件。
- 您可以在众多数字字段前面加上大于 (>)、大于或等于 (>=)、小于 (<)、小于或等于 (<=) 、等于 (=) 或不等于 (<>) 运算符。

提示 当搜索具有较长复杂值的字段（例如 SHA-256 散列值）时，可以从原材料复制搜索条件值，并将其粘贴到搜索页面上的合适字段中。

搜索中的通配符和符号

在连接和安全情报事件的所有文本字段以及其他事件类型的大多数文本字段中搜索时，搜索文本字段中的部分匹配项需要使用星号 (*) 来表示字符串中的未指定字符。不带星号的搜索是这些字段中的完全匹配搜索。即使在不需要通配符的字段中，我们也建议始终使用通配符进行部分匹配搜索。

例如，要查找 `example.com`、`www.example.com` 或 `Department.example.com`，请搜索 `*.example.com`。在大多数情况下，搜索 `example.com` 只会返回 `example.com`。

如果想要搜索非字母数字字符（包括星号字符），请用引号将搜索字符串引起来。例如，要搜索字符串：

```
Find an asterisk (*)
```

输入：

```
"Find an asterisk (*)"
```

搜索中的对象和应用过滤器

Firepower 系统可用于创建可用作网络配置一部分的已命名对象、对象组和应用过滤器。执行或保存搜索时，可使用这些对象、组和过滤器作为搜索条件。

执行搜索时，对象、对象组和应用过滤器以 `${object_name}` 格式显示。例如，对象名称为 `ten_ten_network` 的网络对象在搜索中显示为 `${ten_ten_network}`。

在可使用对象作为搜索条件的搜索字段旁边，可点击 **对象** （+） 。

相关主题

对象管理器

搜索中的时间限制

下表显示了采用时间值的搜索条件字段接受的格式。

表 *96:* 搜索字段中的时间规范

时间格式	示例
`today [at HH:MMam|pm]`	`today` `today at 12:45pm`
`YYYY-DDMM- HH:MM:SS`	`2006-03-22 14:22:59`

可在时间值前输入下列运算符之一。

表 *97:* 时间规范运算符

运算符	示例	说明
<	`< 2006-03-22 14:22:59`	返回时间戳早于 2006 年 3 月 22 日下午 2:23 的事件。
>	`> today at 2:45pm`	返回时间戳晚于今天下午 2:45 的事件。

搜索中的 IP 地址

在搜索中指定 IP 地址时，可输入单个 IP 地址、用逗号隔开的地址列表、地址块或者一系列用连字符 (-) 隔开的 IP 地址。也可使用求反。

对于支持 IPv6 的搜索（例如，入侵事件、连接数据和关联事件搜索），可输入 IPv4 和 IPv6 地址与 CIDR/前缀长度地址块的任意组合。按 IP 地址搜索主机时，结果包括至少有一个 IP 地址与搜索条件匹配的所有主机，即搜索 IPv6 地址可能会返回原地址是 IPv4 的主机。

使用 CIDR 或前缀长度表示法指定 IP 地址块时，系统 **只** 使用掩码或前缀长度指定的那部分网络 IP 地址。例如，如果键入 `10.1.2.3/8`，则系统使用 `10.0.0.0/8`。

因为 IP 地址可以用网络对象表示，所以，也可点击 IP 地址搜索字段旁边的添加网络 **对象** （+） 使用网络对象作为 IP 地址搜索条件。

表 *98:* 可接受的 *IP* 地址语法

要指定的内容...	键入的内容...	示例
单个 IP 地址	IP 地址。	`192.168.1.1` `2001:db8::abcd`
多个 IP 地址，使用列表	用逗号隔开的 IP 地址列表。请**不要**在逗号前后添加空格。	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
可以使用 CIDR 块或前缀长度指定的一系列 IP 地址	采用 IPv4 CIDR 或 IPv6 前缀长度表示法的 IP 地址块。	`192.168.1.0/24` 这可在子网掩码为 255.255.255.0 的 192.168.1.0 网络中指定任意 IP，即 192.168.1.0 至 192.168.1.255。
不可使用 CIDR 块或前缀长度指定的一系列 IP 地址	使用连字符的 IP 地址范围。请**勿**在连字符前后添加空格。	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

用于指定 IP 地址或 IP 地址范围的任何其他方法的求反	在 IP 地址、块或范围前面输入感叹号。	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

被阻止或受监控（但本应被阻止）的主机 请参阅主机配置文件图标，第 648 页。	在连接和安全情报事件中，在“发起方 IP”和“响应方 IP”字段中： • block • 监控	--

相关主题

Firepower 系统 IP 地址约定，第 26 页

搜索中的 URL

搜索 URL 时，请包含通配符。例如，使用 **`*example.com*`** 查找域的所有变体，例如 **`https://example.com`** 和 **`division.example.com`** 以及 **`example.com/division/`**。

搜索中的受管设备

如果您对设备进行分组（无论是仅在FMC上，还是作为实际的高可用性或可扩展性配置），则搜索组的名称会正确返回组中所有设备的结果。

如果系统找到组、则系统会用用于执行搜索的相应成员设备名称替换组名称。在设备字段保存使用了设备组 的搜索时，系统会保存设备字段中指定的名称，并且每次执行搜索时都会再次执行设备名称替换。

搜索中的端口

Firepower 系统接受搜索中端口号的特定语法。可输入：

- 单个端口号
- 用逗号隔开的端口号列表。
- 两个用连字号隔开的端口号，代表端口号范围
- 后接协议缩写、并用正斜杠隔开的端口号（仅限搜索入侵事件时）
- 一个端口号或端口号范围，前面带有感叹号，表示指定端口的求反

注释 指定端口号或范围时，请**不要**使用空格。

表 *99:* 端口语法示例

示例	说明
`21`	返回端口 21 上的所有事件，包括 TCP 和 UDP 事件。
`!23`	返回除端口 23 上的事件以外的所有事件。
`25/tcp`	返回端口 25 上的所有与 TCP 相关的入侵事件。
`21/tcp,25/tcp`	返回端口 21 和 25 上所有与 TCP 相关的入侵事件。
`21-25`	返回端口 21 到 25 上的所有事件。

搜索中的事件字段

当搜索事件时，可以使用以下字段作为搜索条件：

- 审核日志工作流程字段 ， 第 392 页
- 应用数据字段 ， 第 886 页
- 应用详细信息数据字段 ， 第 888 页
- 捕获文件字段 ， 第 818 页

- 允许 名单事件字段， 第 916 页
- 连接和 安全相关连接 事件字段， 第 717 页
- 关联事件字段， 第 912 页
- 发现事件字段， 第 868 页
- 运行状况事件表， 第 379 页
- 主机属性数据字段， 第 876 页
- 主机数据字段， 第 870 页
- 文件和恶意软件事件字段， 第 800 页
- 入侵事件字段， 第 752 页
- 入侵规则更新日志详情， 第 223 页
- 补救状态表字段， 第 920 页
- 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 *Nmap* 扫描结果字段
- 服务器数据字段， 第 883 页
- 第三方漏洞数据字段， 第 894 页
- 用户相关字段， 第 896 页
- 漏洞数据字段， 第 890 页
- 允许 列表违规事件字段， 第 918 页

执行搜索

您必须具有管理员或安全分析师权限才能执行搜索。

过程

步骤 1 选择 **分析** > **搜索**。

提示 也可以点击工作流程中任何页面上的**搜索 (Search)**。

步骤 2 从表下拉列表中，选择想搜索的事件或数据的类型。

步骤 3 在相应的字段中输入搜索条件。请参阅以下各节，了解有关可使用的搜索条件的详细信息：

- 搜索限制， 第 671 页
- 审核日志工作流程字段， 第 392 页
- 应用数据字段， 第 886 页

- 应用详细信息数据字段， 第 888 页
- 捕获文件字段， 第 818 页
- 允许 名单事件字段， 第 916 页
- 连接和 安全相关连接 事件字段， 第 717 页
- 关联事件字段， 第 912 页
- 发现事件字段， 第 868 页
- 运行状况事件表， 第 379 页
- 主机属性数据字段， 第 876 页
- 主机数据字段， 第 870 页
- 文件和恶意软件事件字段， 第 800 页
- 入侵事件字段， 第 752 页
- 入侵规则更新日志详情， 第 223 页
- 补救状态表字段， 第 920 页
- 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 *Nmap* 扫描结果字段
- 服务器数据字段， 第 883 页
- 第三方漏洞数据字段， 第 894 页
- 用户数据字段
- 用户活动数据字段
- 漏洞数据字段， 第 890 页
- 允许 列表违规事件字段， 第 918 页

步骤 4 如果要在以后再次使用搜索，请保存搜索，如保存搜索， 第 678 页中所述。

步骤 5 点击**搜索 (Search)** 开始搜索。搜索结果出现在正在搜索的表的默认工作流程中，受时间约束（如适用）。

下一步做什么

- 要使用工作流程分析搜索结果，请参阅使用工作流程， 第 642 页。

相关主题

配置事件视图设置， 第 193 页

保存搜索

您必须具有管理员或安全分析师权限才能保存搜索。

在多域部署中，系统会显示在当前域中创建的已保存搜索，您可以对其进行编辑。系统还会显示在祖先域中创建的已保存搜索，您不可以对其进行编辑。要查看和编辑在较低域中创建的搜索，请切换至该域。

开始之前

- 建立搜索条件（如执行搜索，第 676 页中所述）或加载已保存的搜索（如加载已保存的搜索，第 678 页中所述）。

过程

步骤 1 从“搜索”(Search) 页面中，如果要将搜索另存为专用，以便只有您才能对搜索进行访问，请选中**专用 (Private)** 复选框。

提示 如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 2 此时您有两种选择：

- 如果要保存已加载搜索的新版本，请点击**另存为新项目 (Save As New)**。
- 如果要保存新搜索或使用同一名称覆盖自定义搜索，请点击**保存 (Save)**。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。

加载已保存的搜索

您必须具有管理员或安全分析师权限才能载入已保存的搜索。

在多域部署中，系统会显示在当前域中创建的已保存搜索，您可以对其进行编辑。系统还会显示在祖先域中创建的已保存搜索，您不可以对其进行编辑。要查看和编辑在较低域中创建的搜索，请切换至该域。

过程

步骤 1 选择**分析** > **搜索**。

提示 也可以点击工作流程中任何页面上的**搜索 (Search)**。

步骤 2 从表下拉列表中，选择要搜索的事件或数据的类型。

步骤 3 从**自定义搜索 (Custom Searches)** 列表或**预定义搜索 (Predefined Searches)** 列表中选择要加载的搜索。

步骤 4 如果要使用其他搜索条件，请更改搜索限制。

步骤 5 如果要在以后再次使用更改的搜索，请保存搜索，如保存搜索，第 678 页中所述。

步骤 6 点击**搜索 (Search)**。

通过外壳查询覆盖

系统管理员可以使用 Linux 基于外壳的查询管理工具找到和停止长期查询。

借助于查询管理工具，可找到并停止运行时间超过指定分钟数的查询。停止查询时，此工具会将事件记入审计日志和系统日志。

请注意， 管理员 内部用户可以访问 FMC CLI。如果使用授予 CLI 访问权限的外部身份验证对象，匹配外壳访问过滤器的用户也可以登录 CLI。

注释 退出 Web 界面的搜索页面不会停止查询。需要很长时间才返回结果的查询在运行时会影响总体系统性能。

基于外壳的查询管理语法

使用以下语法管理长期运行的查询：

```
query_manager [-v] [-l [minutes]] [-k query_id [...]] [--kill-all minutes]
```

表 *100: query_manager* 选项

选项	说明
`-h, --help`	打印简短的帮助消息。
`-l, --list [minutes]`	列出所有运行时间超过已用分钟数的查询。默认情况下，将显示所有运行时间超过 1 分钟的查询。
`-k, --kill query_id [...]`	通过传入 ID 终止查询。该选项可使用多个 ID。
`--kill-all minutes`	终止所有运行时间超过已用分钟数的查询。
`-v, --verbose`	包含完整 SQL 查询的详细输出。

注意 出于系统安全原因，思科强烈建议您不要在任何设备上建立其他 Linux 外壳用户。

停止长期查询

您必须是 **管理员** 用户或具有 CLI 访问权限的外部身份验证用户

过程

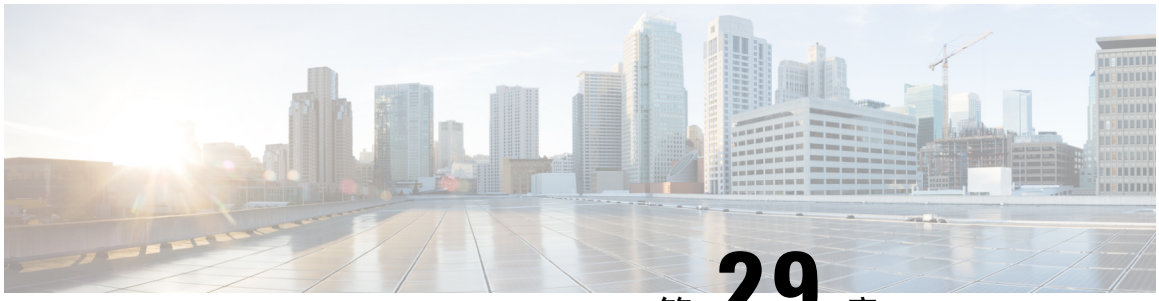
步骤 1 通过 `ssh` 连接至Cisco Secure Firewall Management Center。

步骤 2 发出命令 `专家` 以访问 Linux 外壳。

步骤 3 使用基于外壳的查询管理语法，第 679 页中所述的语法在 `sudo` 下运行 `query_manager`。

搜索事件的历史记录

功能	最低 管理中心	最低 威胁防御	详情
许多字段中的部分匹配搜索现在需要通配符	6.6	任意	例如，搜索 URL 时，请使用 **`*example.com*`** 查找 **`example.com`** 的所有变量。 在搜索连接或安全情报事件时，此行为更改适用于 **分析 > 搜索** 页面上的搜索。也可以通过其他页面上的链接访问此搜索页面。 在不需要使用通配符进行部分匹配搜索的字段中，可以选择使用通配符。 受影响的平台： 管理中心



第 29 章

自定义工作流程

以下主题介绍如何使用自定义工作流程：

自定义工作流程简介

如果预定义工作流程和思科提供的自定义工作流无法满足需求，则可以创建并管理自定义工作流程。

自定义工作流程是为满足贵组织的特有需求而创建的工作流程。创建自定义工作流程时，请选择工作流程所基于的事件（或数据库表）类型。在 管理中心中，可以将自定义工作流程基于自定义表。还可以选择自定义工作流程包含的页面；自定义工作流程可以包含向下展开页面、表视图页面和主机页面或数据包视图页面。

如果事件评估过程更改，则可以编辑自定义工作流程来满足新的需求。请注意，不能编辑任何预定义工作流程。

提示 可以将自定义工作流程设置为任何事件类型的默认工作流程。

已保存的自定义工作流程

除无法修改的预定义工作流程以外，管理中心还包含若干已保存的自定义工作流程。其中每个工作流程基于自定义表，并且可以修改。

在多域部署中，这些已保存的工作流程属于全球域，并且不能在较低的域中进行修改。

表 *101:* 已保存的自定义工作流程

工作流程名称	说明
按照优先级和分类显示事件	此工作流程按事件优先级列出事件及其类型，随之还列出一个表明每个事件已发生的次数的计数。 此工作流程基于 Intrusion Events 自定义表。
具有服务器的主机默认工作流程	可以使用此工作流程快速查看“具有服务器的主机”自定义表中的基本信息。 此工作流程基于 Hosts with Servers 自定义表。
服务器和主机详细信息	可以使用此工作流程确定哪些服务器在网络上使用最频繁以及哪些主机在运行这些服务器。 此工作流程基于 Hosts with Servers 自定义表。

自定义工作流程的创建

如果预定义工作流程和思科提供的自定义工作流程无法满足需求，则您可以创建自定义工作流程。

提示 可以从其他设备导出自定义工作流程，然后将其导入到设备上，而不是创建新的自定义工作流程。然后，可以编辑导入的工作流程来满足需求。

创建自定义工作流程时，请执行以下操作：

- 选择要作为工作流程源的表
- 提供工作流程名称
- 向工作流程中添加向下钻取页面和表视图页面

对于工作流程中的各向下钻取页面，可以：

- 提供显示在 Web 界面中页面顶部的名称
- 每页包含最多五列
- 指定默认排序顺序（升序或降序）

可以在一系列工作流程页面的任何位置添加表视图页面。它们不具有任何可编辑属性，如页面名称、排序顺序或用户可定义的列位置。

注释 必须向自定义工作流程中添加至少一个向下钻取页面或事件表视图。

注释 如果您选择**漏洞 (Vulnerabilities)** 作为表类型，然后添加 **IP 地址 (IP Address)** 作为表列，则除非使用搜索功能限制工作流程以查看特定 IP 地址或地址块，否则在使用自定义工作流程查看漏洞时不会显示 IP 地址列。

自定义工作流程的最终页面取决于工作流程所基于的表，如下表所述。创建工作流程时，系统会默认添加这些最终页面。

表 *102:* 自定义工作流程最终页面

事件/资产类型	最终页面
发现事件	主机数
漏洞	漏洞详细信息
第三方漏洞	主机数
用户	用户
感染指标	主机或用户
入侵事件	数据包

系统不是根据其他种类的事件（例如，审核日志或恶意软件事件）向自定义工作流程中添加最终页面。

基于连接数据的自定义工作流程与其他自定义工作流程类似，不同之处在于其中可包括具备连接摘要数据的向下钻取页面、连接数据图形页面、具备单独连接数据的向下钻取页面和表视图页面。

根据非连接数据创建自定义工作流程

您必须具有管理员或安全分析师权限，才能根据非连接数据创建自定义工作流程。

过程

步骤 1 选择**分析** > **高级** > **自定义工作流程**。

步骤 2 点击**创建自定义工作流程 (Create Custom Workflow)**。

步骤 3 在**名称 (Name)** 字段中输入工作流程的名称。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 从**表 (Table)** 下拉列表中选择要包含的表。

步骤 6 如果要向工作流程中添加一个或多个向下展开页面，请点击**添加页面 (Add Page)**。

步骤 7 在**页面名称 (Page Name)** 字段中输入页面的名称。

步骤 8 在“列 1”(Column 1) 下，选择排序优先级和表列。此列将显示在页面最左侧的列中。

示例：

例如，要创建显示所针对的目标端口的页面，并要按计数对页面进行排序，请从**排序优先级 (Sort Priority)** 下拉列表中选择 **2**，并从**字段 (Field)** 下拉列表中选择**目标端口/ICMP 代码 (Destination Port/ICMP Code)**。

步骤 9 继续选择要包含的字段并设置其排序优先级，直至指定要在页面上显示的所有字段。

步骤 10 如果要向工作流程中添加表视图页面，请点击**添加表视图 (Add Table View)**。

步骤 11 点击**保存 (Save)**。

创建自定义连接数据工作流程

基于连接数据的自定义工作流程与其他自定义工作流程类似，不同在于可以包含连接数据图形页面以及向下展开页面和表视图页面。可以按任意顺序在工作流程中包含尽可能多的各类型的页面。每个连接数据图形页面包含单个图形，可以是曲线图、条形图或饼形图。在曲线图和条形图中，可以包含多个数据集。

您必须具有管理员权限，才能根据连接数据创建自定义工作流程。

过程

步骤 1 选择**分析** > **高级** > **自定义工作流程**。

步骤 2 点击**创建自定义工作流程 (Create Custom Workflow)**。

步骤 3 在**名称 (Name)** 字段中输入工作流程的名称。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 从**表 (Table)** 下拉列表中，选择**连接事件 (Connection Events)**。

步骤 6 如果要向工作流程中添加一个或多个向下钻取页面，您有两个选择：

- 点击**添加页面 (Add Page)** 以添加包含有关个别连接的数据的向下钻取页面。
- 点击**添加摘要页面 (Add Summary Page)** 以添加包含连接摘要数据的向下钻取页面。

步骤 7 在**页面名称 (Page Name)** 字段中输入页面的名称。

步骤 8 在**列 1 (Column 1)** 下，选择排序优先级和表列。此列将显示在页面最左侧的列中。

步骤 9 继续选择要包含的字段并设置其排序优先级，直至指定要在页面上显示的所有字段。

示例：

例如，要创建显示通过受监控网络传输的流量的页面，并要按传输最多流量的响应方对页面进行排序，请从**排序优先级 (Sort Priority)** 下拉列表中选择 **1**，并从**字段 (Field)** 下拉列表中选择**响应方字节数 (Responder Bytes)**。

步骤 10 如果要向工作流程中添加一个或多个图形页面，请点击**添加图形 (Add Graph)**。

步骤 11 在**图形名称 (Graph Name)** 字段中输入页面的名称。

步骤 12 选择要包含在页面上的图形的类型：

- 曲线图 (**折线图**（  ）)
- 条形图 (**条形图**（  ）)
- 饼形图 (**饼图**（  ）)

步骤 13 通过选择图形的 x 轴和 y 轴指定要图形化的数据种类。

在饼图中，x 轴表示独立变量，y 轴表示因变量。

步骤 14 选择要包含在图形中的数据集。

请注意，饼形图只能包含一个数据集。

步骤 15 如果要添加连接数据的表视图，请点击**添加表视图 (Add Table View)**。

表视图不可配置。

步骤 16 点击**保存 (Save)**。

自定义工作流程使用和管理

用于查看工作流程的方法取决于工作流程是基于其中一个预定义事件表还是基于自定义表。

如果自定义工作流程基于预定义事件表，请以与访问设备随附的工作流程相同的方式对其进行访问。例如，要根据“主机”表访问自定义工作流程，请选择**分析** > **主机** > **主机**。另一方面，如果自定义工作流程基于自定义表，则必须从 Custom Tables 页面对其进行访问。

如果事件评估过程更改，则可以编辑自定义工作流程来满足新的需求。请注意，不能编辑任何预定义工作流程。

提示 可以将自定义工作流程设置为任何事件类型的默认工作流程。

根据预定义表查看自定义工作流程

您必须具有管理员、维护或安全分析师权限才能查看自定义工作流程。

过程

步骤 1 为自定义工作流程所基于的表选择适当的菜单路径和选项，如工作流程选择，第 644 页中所述。

步骤 2 要使用其他工作流程，包括自定义工作流程，请点击当前工作流程标题旁边的**切换工作流程 (switch workflow)**。

步骤 3 如果未显示事件并且可按时间限制工作流程，则可能需要调整时间范围；请参阅事件时间限制，第 658 页。

根据自定义表查看自定义工作流程

您必须具有管理员或安全分析师权限，才能查看基于自定义表的自定义工作流程。

在多域部署中，系统会显示在当前域中创建的自定义工作流程，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义工作流程，您不可以对其进行编辑。要查看和编辑较低域中的自定义工作流程，请切换至该域。

过程

步骤 1 选择**分析** > **高级** > **自定义表**。

步骤 2 点击要查看的自定义表旁边的 **视图**（）， 或者点击自定义表的名称。

步骤 3 要使用其他工作流程，包括自定义工作流程，请点击当前工作流程标题旁边的 **(switch workflow)**。

步骤 4 如果未显示事件并且可按时间限制工作流程，则可能需要调整时间范围；请参阅事件时间限制，第 658 页。

编辑自定义工作流程

您必须具有管理员或安全分析师权限才能编辑自定义工作流程。

在多域部署中，系统会显示在当前域中创建的自定义工作流程，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义工作流程，您不可以对其进行编辑。要查看和编辑较低域中的自定义工作流程，请切换至该域。

过程

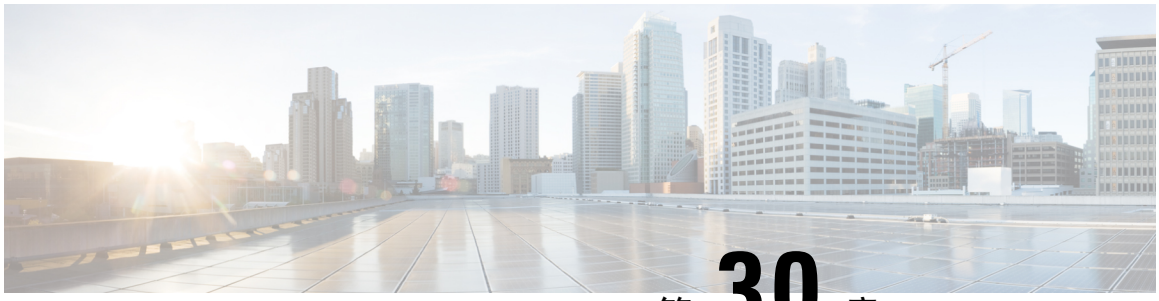
步骤 1 选择**分析** > **高级** > **自定义工作流程**。

步骤 2 点击要编辑的工作流程名称旁边的 **编辑**（） 。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 对工作流程进行所需的任何更改。

步骤 4 点击**保存 (Save)**。



第 30 章

自定义表格

以下主题介绍如何使用自定义表：

自定义表简介

Firepower 系统收集有关网络的信息时， 管理中心 会将这些信息存储在一系列数据库表中。当您使用工作流程查看生成的信息时，管理中心会从其中一个表提取数据。例如，“按计数统计的网络应用”工作流程的每个页面的列取自“应用”表中的字段。

如果您确定通过组合不同表中的字段会增强对网络上活动的分析，则可创建自定义表。

请注意，您可以为预定义表或自定义表创建自定义工作流程。

预定义的自定义表

自定义表包含两个或多个预定义表中的字段。Firepower 系统随附多个系统定义的自定义表，但是，您可以创建其他仅包含符合自身特定需求的信息的自定义表。

例如，Firepower 系统随附用于将入侵事件数据与主机数据相关联的系统定义的自定义表，因此，您可以搜索会影响关键系统的事件并在一个工作流程中查看搜索结果。

在多域部署中，预定义的自定义表属于全局域，不能在低层域中进行修改。

下表介绍系统随附的自定义表。

表 *103:* 系统定义的自定义表

表	说明
主机及服务器 (Hosts with Servers)	包含“主机”(Hosts) 和服务器 (Servers) 表中的字段，提供有关检测到的在网络上运行的应用的信息，以及有关运行这些应用的主机的基本操作系统信息。

可能的表组合

创建自定义表时，可以组合具有相关数据的预定义表中的字段。下表列出了可用来组合创建新自定义表的预定义表。请记住，创建的自定义表也可以组合两个以上预定义自定义表中的字段。

表 *104:* 自定义表组合

可以将这些表中的字段...	与这些表中的字段进行组合...
应用	• 相关事件 • 入侵事件 • 连接摘要数据 (Connection Summary Data) • 主机属性 (Host Attributes) • 应用详情 • 发现事件 (Discovery Events) • 主机数 • 服务器 • 允许 列出事件
相关事件	• 应用 • 主机属性 (Host Attributes) • 主机数
入侵事件	• 应用 • 主机属性 (Host Attributes) • 主机数 • 服务器

可以将这些表中的字段...	与这些表中的字段进行组合...
连接摘要数据 (Connection Summary Data)	• 应用 • 主机属性 (Host Attributes) • 主机数 • 服务器
主机危害表现	• 应用 • 应用详情 • 捕获的文件 • 连接摘要数据 (Connection Summary Data) • 相关事件 • 发现事件 (Discovery Events) • 主机属性 (Host Attributes) • 主机数 • 入侵事件 • 安全情报事件 • 服务器 • 允许 列出事件
主机属性 (Host Attributes)	• 应用 • 相关事件 • 入侵事件 • 连接摘要数据 (Connection Summary Data) • 应用详情 • 发现事件 (Discovery Events) • 主机数 • 服务器 • 允许 列出事件

可以将这些表中的字段...	与这些表中的字段进行组合...
应用详情	• 应用 • 主机属性 (Host Attributes) • 主机数
发现事件 (Discovery Events)	• 应用 • 主机属性 (Host Attributes) • 主机数
安全情报事件	• 应用 • 主机属性 (Host Attributes) • 主机数 • 服务器
主机数	• 应用 • 相关事件 • 入侵事件 • 连接摘要数据 (Connection Summary Data) • 主机属性 (Host Attributes) • 应用详情 • 发现事件 (Discovery Events) • 服务器 • 允许 列出事件
服务器	• 应用 • 入侵事件 • 连接摘要数据 (Connection Summary Data) • 主机属性 (Host Attributes) • 主机数

可以将这些表中的字段...	与这些表中的字段进行组合...
允许 列出事件	• 应用 • 主机属性 (Host Attributes) • 主机数

有时，一个表中的字段会映射到另一个表中的多个字段。

创建新的自定义表时，系统会自动创建显示表中所有列的默认工作流程。此外，如同预定义表一样，您可以搜索自定义表来获取要在网络分析中使用的数据。您还可以根据自定义表生成报告，就像使用预定义表时一样。

用户定义的自定义表

提示 可以从另一个管理中心导出自定义表，然后将其导入到您的管理中心，而不是创建新的自定义表。

要创建自定义表，请确定哪些预定义表含有要在自定义表中包含的字段。然后，可以选择要包含的字段，如有必要，请为所有公共字段配置字段映射。

提示 借助涉及“主机”(Hosts) 表的数据，可以查看与来自一台主机的所有 IP 地址而不是一个特定 IP 地址相关的数据。

例如，不妨考虑将“关联事件”(Correlation Events) 表和“主机”(Hosts) 表中的字段组合起来以创建自定义表。通过这样的自定义表，您可以获取有关涉及任何关联策略违例的主机的详细信息。请注意，您必须决定从“主机”(Hosts) 表显示与“关联事件”(Correlation Events) 表中的源 IP 地址还是目标 IP 地址匹配的数据。

如果查看此自定义表的事件表视图，则它会显示相关性事件（每行一个）。可以将自定义表配置为包含以下信息：

- 事件的生成日期和时间
- 违例的关联策略的名称
- 触发违例的规则的名称
- 与相关性事件中涉及的源主机（又称为发起主机）相关的 IP 地址
- 源主机的 NetBIOS 名称
- 源主机运行的操作系统和版本
- 源主机的关键性

提示　可以创建类似的自定义表来显示目标主机（又称为响应主机）的以上信息。

创建自定义表

过程

步骤 1　选择**分析** > **高级** > **自定义表**。

步骤 2　点击 **Create Custom Table**。

步骤 3　在**名称 (Name)** 字段中，输入自定义表的名称。

示例：

例如，您可输入 `Correlation Events with Host Information (Src IP)`。

步骤 4　从**表 (Tables)** 下拉列表中，选择**关联事件 (Correlation Events)**。

步骤 5　在 **字段 (Fields)** 下，选择 **时间 (Time)** 并点击 **添加 (Add)** 以添加生成关联事件的日期和时间。

步骤 6　重复第 5 步以添加**策略 (Policy)** 和**规则 (Rule)** 字段。

提示　按住 Ctrl 或 Shift 键并点击可选择多个字段。也可以点击并拖动以选择多个相邻值。但是，如果要指定字段在与表关联的事件表视图中的出现顺序，请一次添加一个字段。

步骤 7　从**表 (Tables)** 下拉列表中，选择**主机 (Hosts)**。

步骤 8　向自定义表添加 **IP 地址 (IP Address)**、**NetBIOS 名称 (NetBIOS Name)**、**OS 名称 (OS Name)**、**OS 版本 (OS Version)** 和**主机重要性 (Host Criticality)** 字段。

步骤 9　在**通用字段 (Common Fields)** 下的**关联事件 (Correlation Events)** 旁边，选择**源 IP (Source IP)**。

这样，自定义表即配置为显示在第8步中选择的有关相关性事件中涉及的源主机（又称为发起主机）的主机信息。

提示　可以按照以上步骤创建显示有关相关性事件中涉及的目标主机（又称为响应主机）的主机详细信息的自定义表，但在操作过程中应选择**目标 IP (Destination IP)** 而不是**源 IP (Source IP)**。

步骤 10　点击**保存 (Save)**。

修改自定义表

在多域部署中，系统会显示在当前域中创建的自定义表，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义表，您不可以对其进行编辑。要查看和编辑较低域中的自定义表，请切换至该域。

过程

步骤 1 选择**分析** > **高级** > **自定义表**。

步骤 2 点击要编辑的表旁边 **编辑**（ ）。

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

步骤 3 或者，点击要删除的字段旁边的 **删除**（ ），从表中删除字段。

注释 如果删除报告中当前正在使用的字段，则系统将提示您确认是否要删除使用这些报告中的这些字段的部分。

步骤 4 根据需要进行其他更改。

步骤 5 点击**保存 (Save)**。

删除自定义表

在多域部署中，系统会显示在当前域中创建的自定义表，您可以对其进行删除。系统还会显示在祖先域中创建的自定义表，您不可以对其进行删除。要删除较低域中的自定义表，请切换至该域。

过程

步骤 1 选择**分析** > **高级** > **自定义表**。

步骤 2 点击要删除的自定义表旁边的 **删除**（ ）。

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。

根据自定义表查看工作流程

创建自定义表时，系统会自动为其创建默认工作流程。默认工作流程的第一页显示事件表视图。如果在自定义表中包含入侵事件，则工作流程的第二页是数据包视图。否则，工作流程的第二页是主机页面。您也可以根据自定义表创建自己的自定义工作流程。

提示 根据某个自定义表创建自定义工作流程后，可以将创建的自定义工作流程指定为该自定义表的默认工作流程。

您可以使用相同方法查看自定义表中根据预定义表用于事件视图的事件。

在多域部署中，系统会显示在当前域中创建的自定义表，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义表，您不可以对其进行编辑。要查看和编辑较低域中的自定义表，请切换至该域。

过程

步骤 1 选择**分析** > **高级** > **自定义表**。

步骤 2 点击与要查看的工作流程有关的自定义表旁边的 **视图**（  ）。

搜索自定义表

在多域部署中，系统会显示在当前域中创建的自定义表，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义表，您不可以对其进行编辑。要查看和编辑较低域中的自定义表，请切换至该域。

过程

步骤 1 选择**分析** > **高级** > **自定义表**。

步骤 2 点击要搜索的自定义表旁边的 **视图**（  ）。

提示 要使用不同的工作流程（包括自定义工作流程），请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])**。

步骤 3 点击 **Search**。

提示 要在数据库中搜索不同类型的事件或数据，请从表下拉列表中进行选择。

步骤 4 在相应的字段中输入搜索条件。

如果您输入多个字段的条件，搜索只返回符合所有字段指定搜索条件的记录。

提示 点击搜索字段旁边的 **对象**（+）可将对象用作搜索条件。

步骤 5 如果您计划保存搜索，也可以选中**私有 (Private)** 复选框将搜索另存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示 如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 6 或者，您可以保存搜索，以备以后使用。您有以下选择：

- 点击 **Save**，保存搜索条件。如果选中**私有 (Private)** 复选框，则该搜索只对您的帐户显示。
- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。如果选中**私有 (Private)** 复选框，则该搜索保存成功并只对您的帐户显示。

步骤 7 点击**搜索 (Search)** 开始搜索。

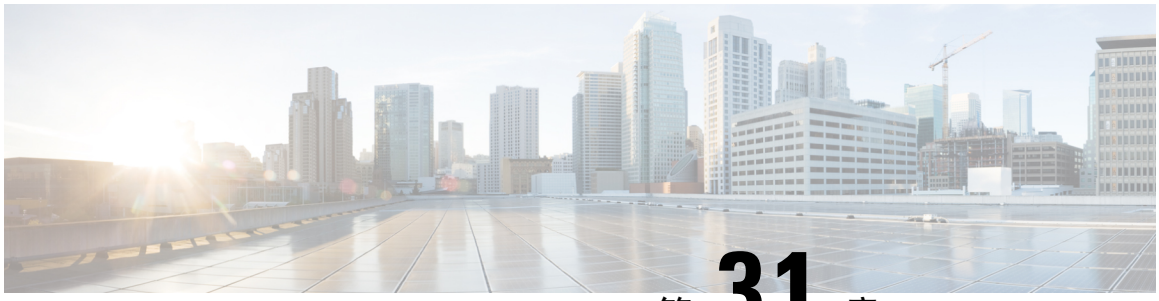
搜索结果显示在自定义表的默认工作流程中，通过当前时间范围（如适用）进行约束。

自定义表的历史记录

特性	最低 管理中心	最低 威胁防御	详细信息
删除了对自定义表中连接事件的支持	6.6	任意	您无法再创建包含连接事件的自定义表。 如果您升级到版本 6.6：包含连接事件的现有表将被列为已弃用，并且不会显示任何数据，并且您无法导出或编辑这些表。现有报告、自定义工作流程和控制面板可能包括已弃用的表；您可能需要查看这些内容。 修改了屏幕： **分析 > 高级 > 自定义表** 以及用于添加或编辑自定义表的页面。 受影响的平台： 管理中心

第 VIII 部分

事件和资产



第 31 章

连接日志记录

以下主题介绍如何配置 Firepower 系统以记录由受监控网络上的主机进行的连接：

关于连接日志记录

系统可以生成其受管设备检测到的连接的日志。这些日志称为连接事件。规则和策略中的设置可供您精细控制记录的连接、记录连接的时间以及存储数据的位置。特殊连接事件称为 安全相关的连接事件，代表被基于信誉的安全情报功能阻止的连接。

连接事件包含关于检测到的会话的数据。任何单个连接事件的可用信息都取决于多种因素，但通常包括：

- 基本连接属性：时间戳、源和目标 IP 地址、入口和出口区域，处理连接的设备等
- 系统发现或推断的其他连接属性：应用、请求的 URL 或与连接关联的用户等
- 有关连接记录原因的元数据：哪个配置处理流量，连接是被允许还是被阻止，以及有关已加密和已解密连接的详细信息等

根据您的组织的安全和合规性需求记录连接。设置连接日志记录时，请记住：系统可能会因为多种原因记录连接，禁用某一处的日志记录并不意味着不会记录匹配连接。

连接事件中的信息取决于多种因素，包括流量特征、最终处理连接的配置等。

注释 您可以用导出的 NetFlow 记录生成的连接数据补充您的受管设备收集的连接日志。这在受管设备无法监控的网络上部署支持 NetFlow 的路由器或其他设备时尤为有用。

始终记录的连接

除非禁用连接事件存储，否则系统会将以下连接结束事件自动保存到 管理中心数据库，不考虑任何其他日志记录配置。

与入侵关联的连接

除非通过访问控制策略的默认操作来处理连接，否则系统会自动记录与入侵事件关联的连接。

当与访问控制默认操作关联的入侵策略生成入侵事件时，系统不会自动记录相关连接终止事件。相反，您必须明确启用默认操作连接日志记录。对于不想记录任何连接数据的仅入侵防御部署，这十分有用。

不过，如果您为默认操作启用连接开始日志记录，除了记录连接开始事件，系统会在关联的入侵策略触发时记录连接结束事件。

与文件和恶意软件事件关联的连接

系统会自动记录与文件和恶意软件事件关联的连接。

注释 检查 NetBIOS-SSN (SMB) 流量所生成的文件事件不会立即生成连接事件，因为客户端和服务器构建一个持久连接。系统在客户端或服务器结束会话之后生成连接事件。

与智能应用绕行关联的连接

系统会自动记录与 IAB 关联的已绕行和将绕行的连接。

受监控连接

系统始终记录受监控流量的连接结束事件，即使流量与其他规则都不匹配且您没有启用默认操作日志记录。有关详细信息，请参阅 受监控连接的日志记录，第 702 页。

您可以记录的其他连接

要仅记录关键连接，可以逐条规则启用连接日志记录。如果为某条规则启用连接日志记录，则系统会记录该规则处理的所有连接。

您还可以记录策略默认操作处理的连接。根据规则或默认策略操作（以及针对访问控制的规则检查配置），您的日志记录选项可能有所不同。

预过滤器策略：规则和默认操作

您可以记录您通过预过滤器策略使用快速路径或进行阻止的连接（包括整个明文、传递隧道）。

预过滤使用外部报头条件处理流量。对于您记录的隧道，生成的连接事件包含来自外部封装报头的信息。

对于需要接受进一步分析的流量，预缩率策略中的日志记录功能已禁用，但匹配连接可能仍然被其他配置记录下来。系统会使用内部报头执行所有进一步的分析，也就是说，系统单独处理并记录允许隧道内的每个连接。

解密策略：规则和默认操作

您可以记录匹配 解密规则或解密策略 默认操作的连接。

对于受阻连接，系统会立即结束会话并生成事件。对于受监控连接以及您将其传递到访问控制规则的连接，系统会在会话结束时生成事件。

访问控制策略：安全情报决策

只要基于信誉的安全情报功能阻止连接，您就可以对该连接进行日志记录。

或者，您可以像被动部署中建议的那样，使用仅监控设置进行安全情报过滤。这使得系统可以进一步分析本应被安全情报组织的连接，并仍将记录匹配项。安全情报监控还允许您使用安全情报信息创建流量配置文件。

当系统由于安全情报过滤而记录连接事件时，它也会记录匹配的安全情报事件，这是一种您可以单独查看和分析的特殊类型连接事件，而且可以单独存储和删除。因此，您可以确定连接中匹配的 IP 地址，列入受阻止和受监控的 IP 地址旁边的主机图标在 **分析** > **连接** 菜单下的页面上的表格中看上去稍有不同。

访问控制策略：规则和默认操作

您可以记录匹配访问控制规则或访问控制策略默认操作的连接。

相关主题

规则和策略操作如何影响日志记录 ，第 701 页

规则和策略操作如何影响日志记录

连接事件包含有关连接记录原因的元数据，包括哪些配置处理流量。配置连接日志记录时，规则操作和策略默认操作不仅可以确定系统如何检查和处理匹配流量，而且可以确定您何时及如何记录匹配流量的相关详细信息。

相关主题

连接和 安全相关连接 事件字段 ，第 717 页

快速路径连接的日志记录

您可以记录快速路径连接和非加密隧道，其包括与预过滤器策略中的以下规则和操作匹配的流量：

- 隧道规则 - **快速路径 (Fastpath)** 操作（记录外部会话）
- 预过滤器规则 - **快速路径 (Fastpath)** 操作

快速路径流量会绕过其余访问控制和 QoS，因此快速路径连接的连接事件包含的信息是有限的。

受监控连接的日志记录

系统始终记录与以下配置匹配的流量的连接结束事件，即使流量与其他规则都不匹配且您没有启用默认操作日志记录：

- 安全情报 - 阻止列表设为监控（也生成安全情报事件）
- SSL 规则 - **监控 (Monitor)** 操作
- 访问控制规则 - **监控 (Monitor)** 操作

系统不会在每次单个连接匹配“监控”(Monitor) 规则时都成一个单独的事件。由于单一连接可能与多条“监控”(Monitor) 规则相匹配，每个连接事件均可能包含和显示关于该连接匹配的前八条监控访问控制规则，以及第一条匹配的 SSL 监控规则的信息。

同样，如果您将连接事件发送至外部系统日志或 SNMP 陷阱服务器，则每当单一连接与监控规则相匹配时，系统均不会发送单独的警报。相反，系统在连接终止时发送的警报包含有关连接匹配的监控规则的信息。

受信任连接的日志记录

您可以记录受信任连接的开始和结束，包括匹配以下规则和操作的流量：

- 访问控制规则 - **信任 (Trust)** 操作
- 访问控制默认操作 - **信任所有流量 (Trust All Traffic)**

注释 虽然您可以记录受信任的连接，但是建议不要这样做，因为受信任的连接不会受到深入检查或发现，因此受信任连接的连接事件包含的信息有限。

信任规则在第一个数据包上检测到的 TCP 连接仅生成连接结束事件。系统将在最终会话数据包发送完毕 1 小时后生成事件。

受阻连接的日志记录

您可以记录受阻连接，这包括与以下规则和操作匹配的流量：

- 隧道规则 - **阻止 (Block)**
- 预过滤器规则 - **阻止 (Block)**
- 预过滤器默认操作 - **阻止所有隧道流量 (Block all tunnel traffic)**
- 安全情报 - 阻止列表勿设为监控（也生成安全情报事件）
- 解密规则—**阻止** 和 **阻止并重置**
- SSL 默认操作 - **阻止 (Block)** 和**阻止并重置 (Block with reset)**
- 访问控制规则 - **阻止 (Block)**、**阻止并重置 (Block with reset)** 和**交互式阻止 (Interactive Block)**

- 访问控制默认操作 - **阻止所有流量 (Block All Traffic)**

仅内联部署的设备（即使用已路由、已交换或透明接口或内联接口对）可以阻止流量。因为阻止的连接实际上在被动部署中并未被阻止，所以系统可能针对每个被阻止的连接报告多个连接开始事件。

注意 在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。对 Block 规则启用日志记录之前，考虑此规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口的流量。

受阻连接的连接开始和连接结束的日志记录

当您记录受阻连接时，系统如何进行记录该连接取决于其受阻原因；当根据连接日志配置关联规则时，必须记住这一点：

- 对于阻止已加密流量的 SSL 规则和 SSL 策略 默认操作，系统记录连接 **结束**事件。这是因为系统无法确定连接是否使用会话中的第一个数据包加密。
- 对于其他阻止操作，系统会记录连接**开始**的事件。匹配流量会被拒绝，无需进一步检测。

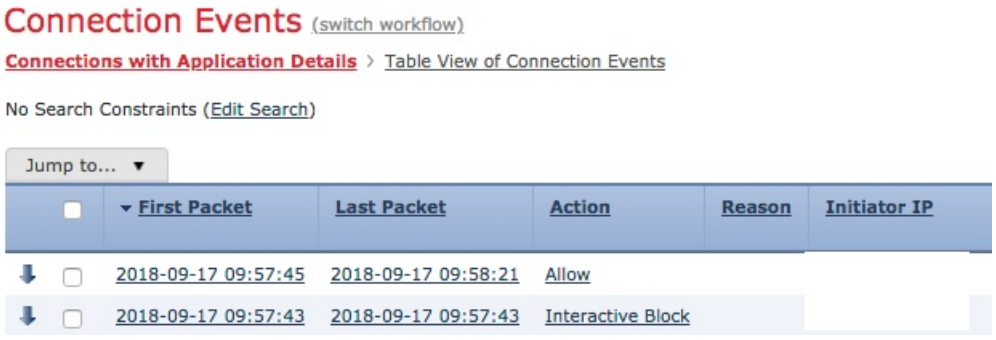
绕行交互式阻止的日志记录

当用户浏览受禁网站时，交互式阻止访问控制规则导致系统显示警告页面，该等规则可供您配置连接结束日志记录。这是因为，如果用户点击浏览警告页面，该连接会被视为系统可以监控和记录并且允许访问的新连接。

因此，对于与“交互式阻止”或“交互式阻止并重置”规则匹配的数据包而言，系统可以生成以下连接事件：

- 用户的请求最初被阻止且显示警告页面时的连接开始事件；该事件的关联操作为交互式阻止或交互式阻止并重置
- 当用户点击警告页面并加载最初请求的页面时生成的多个连接开始或连接结束事件；这些事件的关联操作为允许，原因为用户绕行

  下图显示交互式阻止以及允许操作的示例。



允许连接的日志记录

您可以记录允许连接，这包括与以下规则和操作匹配的流量：

- SSL 规则 - **解密 (Decrypt)** 操作
- SSL 规则 - **不解密 (Do not Decrypt)** 操作
- SSL 默认操作 - **不解密 (Do not Decrypt)**
- 访问控制规则 - **允许 (Allow)** 操作
- 访问控制默认操作 - **仅限网络发现 (Network Discovery Only)** 以及任何入侵防御选项

为这些配置启用日志记录可确保连接已记录，同时也允许（或指定）下一阶段的检查和流量处理。SSL 日志记录始终在连接结束时进行；访问控制配置也允许在连接开始时进行日志记录。

虽然隧道和预过滤器规则中的**分析 (Analyze)** 操作也允许连接继续进行访问控制，但禁用进行此操作的规则的日志记录。匹配连接仍然可由其他配置进行记录。允许的隧道可能会对封装会话进行单独评估和记录。

当您通过访问控制规则或默认操作允许流量时，可以使用相关入侵策略进一步检查流量和阻止入侵。对于访问控制规则，您也可以使用文件策略检测和阻止被禁止的文件，包括恶意软件。除非禁用连接事件存储，否则系统将自动记录大多数与入侵、文件和恶意软件事件关联的允许连接。有关详细信息，请参阅始终记录的连接，第 700 页。

具有加密负载的连接不进行深度检查，因此加密连接的连接事件包含的信息有限。

允许连接的文件和恶意软件事件日志记录

当文件策略检测或阻止文件时，它会将以下事件之一记录到 管理中心数据库：

- 文件事件，代表检测到的或被阻止的文件，包括恶意软件文件
- 恶意软件事件，仅代表检测到的或被阻止的恶意软件文件
- 可追溯的恶意软件事件，其在之前检测到的文件的恶意软件性质变更时生成

您可以以每个访问控制规则为基础禁用此日志记录。您还可以完全禁用文件和恶意软件事件存储。

注释 建议您将文件和恶意软件事件日志记录保持启用状态。

连接开始和连接结束日志记录

您可以在连接开始或结束时记录该连接，对于受阻流量，下列情况除外：

- 受阻流量 - 由于会立即拒绝受阻流量而不进一步检查，因此通常您只能记录受阻流量的连接开始事件。没有要记录的唯一连接结束。

- 受阻加密流量 - 当在 解密策略中启用连接日志记录时，系统会记录连接结束而不是连接开始事件。这是因为，系统无法确定连接是否使用会话中第一个数据包加密，因此无法立即阻止已加密会话。

要优化性能，请记录所有连接的开始或终止，而不是同时记录两者。出于任何原因监控连接都会强制执行连接结束日志记录。对于单个未被阻止的连接，连接终止事件包含连接开始事件中的所有信息，以及在会话期间收集到的信息。

下表详细列出了连接开始和连接终止事件之间的差异，包括相比于记录每种事件的优势。

表 *105:* 比较连接开始和连接结束事件

	连接开始事件	连接结束事件
生成时间…	当系统检测到连接开始（或者在前几个数据包之后，如果事件生成取决于应用或 URL 识别）。	当系统： • 检测到连接关闭。 • 在一段时间后未检测到连接结束。 • 由于内存限制，无法再跟踪会话。
记录对象...	除受到 解密策略阻止以外的所有连接。	大部分连接。
包含...	仅在第一个数据包中可以确定的信息（或者前几个数据包，如果事件生成取决于应用或 URL 识别）。	连接开始事件中的所有信息，以及通过在会话期间检查流量确定的信息；例如，传输的数据总量或连接中最后一个数据包的时间戳。 **注释** 如果威胁防御系统对连接返回 snort 判定，或者您对连接进行了快速路径连接，则连接事件不会计算传输的数据量。
十分有用…	如果您要记录： • 阻止的连接。 • 仅连接的开始，因为连接结束信息对您无关紧要。	如果要： • 被 解密策略处理的日志加密连接。 • 使用在会话期间收集的信息执行任何类型的详细分析或者触发关联规则。 • 查看自定义工作流程中的连接摘要（汇聚连接数据），查看图形格式的连接数据，或者创建并使用流量量变曲线。

Cisco Secure Firewall Management Center 与外部日志记录

如果您在 管理中心上存储连接和安全情报事件日志，则可以使用 Firepower 系统的报告、分析和数据关联功能。例如：

- 控制面板和情景管理器为您提供由系统记录的连接的图形化概览视图。
- 事件视图（大多数选项在“分析”菜单下提供）显示有关系统记录的连接的详细信息，您可以用图形或表格格式显示这些信息，也可以在报告中将其汇总。
- 流量分析使用连接数据创建正常网络流量的配置文件，然后您可以将其用作检测和跟踪异常行为的基准。
- 通过关联策略，您可以生成事件并触发对特定类型的连接或流量量变曲线更改的响应（例如警报或外部补救）。

管理中心可以存储的事件数取决于其型号。

注释 要使用这些功能，**必须**记录连接（而且在大多数情况下，必须记录连接结束而非开始事件）。这就是为什么系统自动记录关键连接，即与记录的入侵、受禁文件和恶意软件关联的那些链接。

您还可以使用以下工具将事件记录到外部系统日志或 SNMP 陷阱服务器或其他外部工具：

- 对于任何设备上的外部日志记录：

  您配置的连接称为 警报响应。

- 对于 威胁防御 设备上的外部日志记录：

  请参阅了解配置系统日志和在《Cisco Secure Firewall Management Center 设备配置指南》中配置 *SNMP* 陷阱的相关信息。

- 有关与外部日志记录相关的其他选项：

  请参阅使用外部工具的事件分析，第 597 页。

相关主题

Cisco Secure Firewall Management Center 警报响应，第 531 页

连接日志记录的限制

无法记录：

- 其封装连接由访问控制检查的明文、传递隧道的外部会话
- 三次握手尚未完成的 TCP 连接。

  不会记录这些连接，因为这样做可能会导致您的 Firepower 部署遭受拒绝服务攻击。

  但是，您可以使用以下解决方法来监控或调试失败的连接：

  - 在命令行界面使用 **show asp drops** 命令。
  - 使用数据包捕获功能来获取有关这些连接的更多详细信息。请参阅数据包捕获概述，第 424 页及其子主题。

如果某个连接事件不包含您认为其应包含的信息，请参阅填充连接事件字段的要求，第 735 页和连接事件字段中的可用信息，第 737 页。

当事件显示在事件查看器中时

以下几点适用于所有类型的事件：

- 如果您正在查看“分析”菜单下的页面，则必须刷新页面以显示新事件。
- 事件通常在检测到流量后几秒钟内即可查看。但是，在以下情况下可能会出现任意延迟：FMC 正在管理低带宽网络上的许多设备；或在暂停事件处理的操作（例如事件备份）期间。
- 根据定义的规则记录的所有连接事件都显示在事件查看器中。用于过滤事件的选项不适用于连接事件的统一日志记录。

连接日志记录最佳实践

使用以下最佳实践确保仅记录要记录的连接。

因此，仅记录关键连接，在每个访问控制规则的基础上启用连接日志记录。

始终记录的连接

系统将自动记录以下连接：

- 一些与检测到的文件、恶意软件、入侵和智能应用绕行 (IAB) 关联的连接。

  有关详细信息，请参阅始终记录的连接，第 700 页。

- 受监控连接。

  有关详细信息，请参阅受监控连接的日志记录，第 702 页。

永远不会记录的连接

请勿启用以下各项的日志记录：

- 访问控制规则与信任操作。

  受信任的连接不会受到深入检查或发现，因此受信任连接的连接事件包含的信息有限。

- 请勿在被动部署中启用“阻止”规则的日志记录。要记录在内联部署设备时系统将阻止的连接，请使用“监控”规则而不是“阻止”规则。

  仅内联部署的设备（即使用已路由、已交换或透明接口或内联接口对）可以阻止流量。因为阻止的连接实际上在被动部署中并未被阻止，所以系统可能针对每个被阻止的连接报告多个连接开始事件。

- 不感兴趣的流量。示例如下：
  - 特定的允许流量，例如对可信 DNS 主机的 DNS 请求。

- 与服务产品无关的基础设施流量。

（如前所述，您仍然可以监控此流量是否存在威胁。）

如始终记录的连接，第 700 页中所讨论的，即使禁用了上述各项的日志记录，仍然会记录入侵事件、恶意软件和 IAB。

避免记录将在其他位置记录的内容

如果其他设备或服务正在记录网段的连接数据，请在 管理中心中禁用该网段数据的日志记录。示例如下：

- 如果路由器在与 管理中心相同的网段上记录连接事件，请避免记录 管理中心 上的相同连接，除非您需要将连接事件用于其他用途，例如关联策略或流量配置文件。

  有关关联策略的详细信息，请参阅关联策略和规则简介，第 939 页。有关流量配置文件的详细信息，请参阅流量量变曲线简介，第 977 页。

- 如果使用 Secure Network Analytics 以利用交换机和路由器报告的 NetFlow 记录来识别潜在的行为异常和可疑流量模式，则可以禁用监控这些网段的规则的连接日志记录，依靠 Secure Network Analytics 对网络的这些部分进行行为分析。

  有关详细信息，请参阅 Secure Network Analytics 文档。

记录连接的开始或结束（并非两者）

如果可以在连接开始或结束日志记录之间进行选择，请启用连接结束日志记录。这是因为连接结束记录连接开始事件的信息以及在会话期间收集的信息。

仅当要记录被阻止的连接或连接结束信息对您无关紧要时，才记录连接开始。

有关详细信息，请参阅连接开始和连接结束日志记录，第 704 页。

受阻流量的日志记录

因为受阻流量会被立即拒绝，无需进一步检查，因此您可以仅记录连接开始事件。

有关详细信息，请参阅受阻连接的日志记录，第 702 页。

将事件记录到外部位置

如果您的公司的安全策略允许，您可以使用以下任意一项将日志传输到外部源，从而节省 管理中心的磁盘空间：

- eStreamer，可以让您将日志从 管理中心 传输到自定义开发的客户端应用。有关详细信息，请参阅 *Firepower eStreamer* 集成指南。

- 系统日志或 SNMP 陷阱，称为警报响应。有关详细信息，请参阅Cisco Secure Firewall Management Center 警报响应，第 531 页。

指定事件记录的最大数量

考虑可以存储在数据库中的最小和最大记录数量。例如，默认情况下，虚拟 管理中心 可以存储 1000 万个事件，但最大事件数量为 5000 万个。转至**系统 (System)** > **配置 (Configuration)** > **数据库 (Database)** 以调整为满足需求的大小。

有关所有 管理中心 型号及其事件数据库大小的列表，请参阅数据库事件限制，第 55 页。

控制连接事件中显示的内容

要指定连接事件中显示的行数，请点击 管理中心 右上角的用户名，然后点击**用户首选项 (User Preferences)** > **事件视图设置 (Event View Settings)**。 可以设置的最大值是每页 1000 个事件。

设置连接事件报告

为确保不会错过连接事件，可以设置 .csv 格式的自动报告，并可选择安排以固定的时间间隔生成报告。有关详情，请参阅：

- 使用报告设计器（**分析 (Analysis)** > **连接 (Connection)** > **事件 (Events)** > **报告设计器 (Report Designer)**）：关于设计报告，第 506 页。
- 安排任务（**系统** > **工具** > **安排**）：关于任务安排，第 467 页。

连接日志记录的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

配置连接日志记录

以下各部分介绍如何设置连接日志记录以匹配各种规则和条件。

使用隧道和预过滤器规则记录连接

预过滤器策略仅适用于 Cisco Secure Firewall Threat Defense 设备。

开始之前

- 将规则操作设置为**阻止 (Block)** 或**快速路径** （**Fastpath**）。对于**分析 (Analyze)** 操作，记录已被禁用，这可以让连接继续接受访问控制的检查，由其他配置来确定其处理和记录。
- 日志记录在内部流上执行，而不是在封装流上执行。

过程

步骤 1 在预过滤策略编辑器中，点击要在其中配置记录的规则旁边的 **编辑**（ ）。

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

步骤 2 点击 **日志记录**。

步骤 3 指定您是否想要选择 **Log at Beginning of Connection** 还是选择 **Log at End of Connection**。

要优化性能，请记录所有连接的开始或终止，而不是同时记录两者。因为阻止的流量会被立即拒绝而无需进一步检查，所以只能记录“阻止”(Block) 规则的连接结束事件。

步骤 4 指定将连接事件发送至何处：

步骤 5 点击**保存 (Save)** 保存规则。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

使用 TLS/SSL 规则记录可解密连接

过程

步骤 1 在 解密策略 编辑器中，点击要在其中配置记录的规则旁边的 **编辑**（ ）。

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

步骤 2 点击 **日志记录**。

步骤 3 选中**在连接结束时记录 (Log at End of Connection)**。

对于受监控流量，需要连接结束日志记录。

步骤 4 指定将连接事件发送至何处。

如果要对这些连接事件执行基于 管理中心的分析，请将事件发送到事件查看器。对于受监控流量，需要执行此操作。

步骤 5 点击**保存 (Save)** 保存规则。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

使用安全情报记录连接

安全情报策略需要威胁智能许可证或保护经典许可证。

过程

步骤 1 在访问控制策略编辑器中，点击 **安全情报**。

步骤 2 点击 **日志记录**（ ） 以使用以下条件启用安全情报日志记录：

- 按 IP 地址 - 点击 **网络**旁边的日志记录。
- 按 URL - 点击 **URL**旁边的日志记录。
- 按域名 - 点击 **DNS 策略** 下拉列表旁边的日志记录。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 选中**记录连接 (Log Connections)** 复选框。

步骤 4 指定要将连接和 安全相关的连接事件发送到何处。

如果要执行基于 管理中心的分析，或者如果要将列入阻止名单为仅监控，请将事件发送到事件查看器。

步骤 5 点击**确定 (OK)** 以设置日志记录选项。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

使用访问控制规则记录连接

根据您选择的规则操作和深度检查选项，您的日志记录选项会有所不同；请参阅规则和策略操作如何影响日志记录，第 701 页。

过程

步骤 1 在访问控制策略编辑器中，点击要配置日志记录的规则旁边的 **编辑**（ ）。

如果显示**视图**（ ），则表明配置继承自祖先策略或属于祖先域，或者您没有修改配置的权限。

步骤 2 点击**日志记录**选项卡。

步骤 3 指定您是否想要选择 **Log at Beginning of Connection** 还是选择 **Log at End of Connection**。

要优化性能，请记录所有连接的开始或终止，而不是同时记录两者。

步骤 4 （可选）选中**记录文件 (Log Files)** 复选框以记录与连接关联的文件和恶意软件事件。

思科建议您将此选项保留为已启用。

步骤 5 指定将连接事件发送至何处：

- **事件查看器**：将事件发送到 管理中心。使用云管理时，将事件发送到云交付 管理中心 和本地管理中心（如果已将其配置为仅执行事件分析）。您可以在任一产品的事件查看器中查看事件。
- **系统日志服务器**：将连接事件发送到访问控制策略的“日志记录”选项卡中配置的系统日志服务器，除非被覆盖。

  显示覆盖：显示可覆盖访问控制策略中配置的设置的选项。

  - **覆盖严重性**：选择此选项并为规则选择严重性时，此规则的连接事件将具有所选择的严重性，而与在访问控制策略的“日志记录”选项卡中配置的严重性无关。
  - **覆盖默认系统日志目标**：将为此规则的连接事件生成的系统日志发送到此警报中指定的目标。

- **SNMP 陷阱**：连接事件发送到所选的 SNMP 陷阱。

步骤 6 点击 **Save** 保存规则。

下一步做什么

- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

使用策略默认操作记录连接

策略的默认操作确定系统如何处理与策略中所有规则均不匹配的流量（访问控制和 解密策略中的“监控”规则除外，这些规则匹配和记录流量，但不处理或检测流量）。

解密策略 默认操作的记录设置还监管系统如何记录无法解密的会话。

开始之前

- 对于预过滤器默认操作日志记录，请将默认操作设置为**阻止所有隧道流量 (Block all tunnel traffic)**。对于**允许所有隧道流量 (Allow all tunnel traffic)** 操作，日志记录已被禁用，这可以让连接继续接受访问控制的检查，由其他配置来确定其处理和记录。

过程

步骤 1 在策略编辑器中，点击**默认操作 (Default Action)** 下拉列表旁边的 **日志记录**（ ） 。

步骤 2 指定要记录匹配连接的时间：

- “在连接开始时记录”(Log at Beginning of Connection) - SSL 默认操作不支持。
- “在连接结束时记录”(Log at End of Connection) - 如果选择访问控制**阻止所有流量 (Block All Traffic)** 默认操作或预过滤**阻止所有隧道流量 (Block all tunnel traffic)** 默认操作，则不受支持。

要优化性能，请记录所有连接的开始或终止，而不是同时记录两者。

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。 在访问控制策略中，也可从祖先策略继承配置。

步骤 3 指定将连接事件发送至何处。

如果要对这些连接事件执行基于 管理中心的分析，请将事件发送到事件查看器。

步骤 4 点击**确定 (OK)**。

步骤 5 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

限制长 URL 的日志记录

HTTP 流量的连接结束事件会记录受监控主机所请求的 URL。禁用或限制存储的 URL 字符数可提高系统性能。禁用 URL 日志记录（存储零字符）不会影响 URL 过滤。尽管系统不会记录流量，但会根据请求的 URL 过滤流量。

过程

步骤 1 在访问控制策略编辑器中，点击 **高级 (Advanced)**，然后点击 **常规设置 (General Settings)** 旁边的 **编辑**（）。

如果显示**视图**（），则表明配置继承自祖先策略或属于祖先域，或者您没有修改配置的权限。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

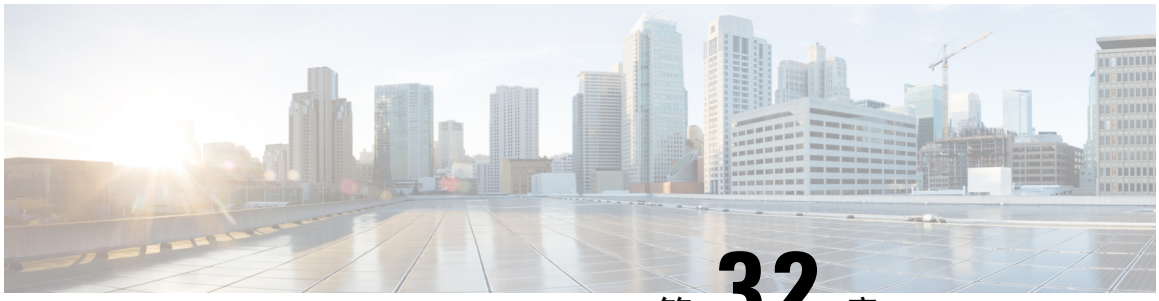
步骤 2 输入**要在连接事件中存储的最大 URL 字符数 (Maximum URL characters to store in connection events)**。

步骤 3 点击**确定 (OK)**。

步骤 4 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。



第 32 章

连接和安全相关的连接事件

以下主题介绍如何使用连接事件和安全事件表。

关于连接事件

系统可以生成其受管设备检测到的连接的日志。这些日志称为连接事件。连接事件包括 安全相关连接事件 （被基于信誉的安全情报功能被阻止的连接。）

连接事件通常包括由以下项检测到的事务：

- 访问控制策略
- 解密策略
- 预过滤器策略（由预过滤器或隧道规则捕获）
- DNS 阻止列表
- URL 阻止列表
- 网络（IP 地址）阻止列表

规则和策略中的设置可供您精细控制记录的连接、记录连接的时间以及存储数据的位置。

有关详细信息，请参阅连接日志记录， 第 699 页。

相关主题

关于安全情报

连接与安全相关连接事件

安全相关连接事件 是一个当会话被阻止或被基于信誉的安全情报功能监控时生成的连接事件。

但是，对于每个 安全相关连接事件，都有相同的连接事件。您可以单独查看和分析 安全相关连接事件 。系统还会单独地存储和删除 安全相关连接事件 。

请注意，在进行更多资源密集型评估之前，系统会强制实施安全智能。当连接被安全智能阻止时，生成的事件不包含系统从后续评估（例如用户身份）收集的信息。

注释 在本指南中，除非另行说明，否则有关连接事件的也与 安全相关连接事件有关。

NetFlow 连接

要补充受管设备收集到的连接数据，可以使用 NetFlow 导出器广播的记录来生成连接事件。这在 NetFlow 导出器监控的网络不同于受管设备监控的网络时尤为有用。

系统会将 NetFlow 记录记录为 Cisco Secure Firewall Management Center数据库中的单向连接结束事件。这些连接的可用信息与访问控制策略检测到的连接略有不同；请参阅NetFlow 和受管设备数据之间的差异。

相关主题

NetFlow 数据

连接摘要（图形的汇聚数据）

系统会将在五分钟间隔内收集到的数据汇聚为连接摘要，供系统用于生成连接图形和流量量变曲线。或者，您可以基于连接摘要数据创建自定义工作流程，并以与基于单个连接事件的工作流程相同的方式来使用此类工作流程。

请注意，尽管相应的连接结束事件可以汇总到连接摘要数据中，但 安全相关连接事件无任何特定的连接摘要。

多个连接必须满足以下条件才能汇总到连接摘要：

- 代表连接结束
- 具有相同的源 IP 地址和目标 IP 地址，并在响应方（目标）主机上使用相同的端口
- 使用相同的协议（TCP 或 UDP）
- 使用相同的应用协议
- 由同一受管设备或由同一 NetFlow 导出器检测

每份连接摘要都包括总流量统计信息，以及摘要中连接的数量。由于NetFlow导出器生成单向连接，因此对于基于 NetFlow 数据的每个连接而言，摘要的连接计数按 2 递增。

请注意，连接摘要中并未包含与摘要中汇总的连接相关联的所有信息。例如，在汇总连接以形成连接摘要时没有使用客户端信息，因此摘要中不包含客户端信息。

长期运行连接

如果汇总连接数据的受控会话跨越两个或多个 5 分钟时间间隔，那么该连接可视为长期运行连接。当计算连接摘要中的连接数时，系统仅累加启动长期运行连接的 5 分钟间隔内的连接数。

此外，当计算由长期运行连接中的发起方和响应方传输的数据包和字节数时，系统并不会报告每 5 分钟间隔中实际传输的数据包和字节数。相反，系统会假定一个固定传输比率，并基于传输的数据包和字节总数、连接长度及每 5 分钟间隔内发生的连接部分计算预估数字。

源于外部响应方的组合连接摘要

要减少存储连接数据所需的空间并加快连接图的绘制，系统将在下列情况下合并连接摘要：

- 连接中涉及的其中一台主机并不在监控网络中
- 除外部主机的 IP 地址以外，摘要中的连接还满足摘要汇聚条件

当在“分析”>“连接”子菜单页面中查看连接摘要并使用连接图时，系统将显示`external`，而非未监控主机的 IP 地址。

由于执行汇总的缘故，如果您尝试从涉及外部响应方的连接摘要或连接图深入了解连接数据的表视图（即，访问单个连接的数据），该表视图将不包含任何信息。

连接和 安全相关连接 事件字段

注释 您不能使用连接/安全相关的连接事件“搜索”页面搜索与连接关联的事件。

访问控制策略（系统日志：ACPolicy）

监控连接的访问控制策略。

访问控制规则 (系统日志：AccessControlRuleName)

处理连接的访问控制规则或默认操作，以及最多 8 条该连接匹配的监控规则。

如果连接匹配一个监控规则，则 Cisco Secure Firewall Management Center会显示处理连接的规则的名称，后跟监控规则名称。如果连接匹配多个监控规则，则会显示匹配的监控规则数量，例如，默认操作 + 2 个监控规则。

要显示包含与连接匹配的前 8 个监控规则的列表的弹出窗口，请点击***N* 个监控规则**。

操作（系统日志：AccessControlRuleAction）

与已记录连接的配置关联的操作。

对于受安全情报监控的连接，该项操作即为由连接触发的第一个非监控访问控制规则的操作，或者为默认操作。同样，由于与监控规则匹配的流量始终由后续规则或通过默认操作进行处理，因此与因监控规则而记录的连接相关联的操作绝不会是“监控”(Monitor)。不过，您仍然可以在与监控规则匹配的连接上触发关联策略违规。

操作	说明
允许	通过访问控制明确允许的或者由于用户绕过交互式阻止而允许的连接。
阻止、阻止并重置	受阻连接，包括： • 按预过滤器策略阻止的隧道及其他连接 • 被安全情报阻止的连接。 • 按 SSL 策略阻止的加密连接。 • 漏洞按入侵策略阻止的连接。 • 文件（包括恶意软件）按文件策略阻止的连接。 对于系统阻止入侵或文件的连接，即使使用访问控制“允许”(Allow)规则调用深度检查，系统也将显示 `Block`。
快速路径	按预过滤器策略使用快速路径的非加密隧道及其他连接
交互式阻止、交互式阻止并重置	在系统最初使用“交互式阻止”(Interactive Block) 规则阻止用户的 HTTP 请求时记录的连接。如果用户点击浏览系统显示的警告页面，则为会话记录的其他连接会执行操作“允许”(Allow)。
信任	访问控制信任的连接。系统根据设备型号以不同方式记录受信任的TCP连接。
默认操作	访问控制策略的默认操作处理的连接。
（空白/空）	在传递足够的数据包以匹配规则之前，连接已关闭。 只有在访问控制以外的其他设备（例如入侵防御）导致记录连接时，才会发生这种情况。

应用协议（系统日志：ApplicationProtocol）

在 Cisco Secure Firewall Management Center Web 界面中，此值限制摘要和图形。

连接中检测到的表示主机之间通信的应用协议。

应用协议类别和标记 (Application Protocol Category and Tag)

展示了应用特征的条件条件，协助您了解应用功能。

应用风险

与连接中检测到的应用流量关联的风险：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。

业务相关性

与连接中检测到的应用流量关联的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。

客户端和客户端版本（系统日志：Client、ClientVersion）

在连接中检测到的客户端应用及版本。

如果系统无法识别连接中使用的特定客户端，则该字段会显示附加到应用协议名称的术语“client”，以提供通用名称，例如，FTP client。

客户端类别和标记 (Client Category and Tag)

展示了应用特征的条件，协助您了解应用功能。

连接计数器 （仅限系统日志）

区分一个连接与另一个同时连接的计数器。此字段本身没有意义。

以下字段共同唯一标识连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

连接实例 ID （仅限系统日志）

处理连接事件的 Snort 实例。此字段本身没有意义。

以下字段共同唯一标识连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

ConnectionDuration（仅限系统日志）

此字段仅作为系统日志字段存在；不会出现在 Cisco Secure Firewall Management Center Web 界面中。（Web 界面使用“第一个数据包”列和“最后一个数据包”列来传达此信息。）

仅当在连接结束后发生日志记录时，此字段才具有值。对于 start-of-connection 系统日志消息，由于此字段在当时未知，因此不是输出。

对于 end-of-connection 系统日志消息，此字段指示第一个数据包到最后一个数据包之间经过的秒数，短连接的秒数可为零。例如，如果系统日志的时间戳为 12:34:56，ConnectionDuration 为 5，则第一个数据包出现于 12:34:51。

连接

连接摘要中的连接数。对于长期运行连接，即跨越多个连接摘要间隔的连接，只有第一个连接摘要间隔可递增。要使用**连接 (Connections)** 条件查看有意义的搜索结果，请使用具有连接摘要页面的自定义工作流程。

计数

与每行显示的信息相匹配的连接数。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。如果创建了自定义工作流程，但未在向下钻取页面中添加**计数 (Count)** 列，则每个连接都将单独列出，且数据包和字节并不汇总。

解密对等体

为关联连接解密数据包的 VPN 对等体的 IP 地址（对等体的 IKE 地址）。

您必须启用访问控制策略规则的日志记录设置，以便在连接开始和结束时进行记录，以查看 VPN 对等体 IP 地址。如果启用绕过已解密流量的访问控制策略 (sysopt connection permit-vpn) 选项，则无法查看已解密流量的详细信息。

检测类型（系统日志：DetectionType）

此字段显示客户端应用的检测来源。它可以是 **AppID** 或 **加密可视性**。

目标端口/ICMP 代码（系统日志：单独字段 - DstPort、ICMPCode）

在 Cisco Secure Firewall Management Center Web 界面中，这些值限制摘要和图形。

会话 响应方使用的端口或 ICMP 代码。

DestinationSecurityGroup （仅限系统日志）

此字段包含与 **DestinationSecurityGroupTag**中的数字值关联的文本值（如果可用）。如果组名不可用作文本值，则此字段包含与 DestinationSecurityGroupTag 字段相同的整数值。

DestinationSecurityGroupType （仅限系统日志）

此字段显示从中获取安全组标记的源。

值	说明
内联	目标 SGT 值来自数据包
会话目录	目标 SGT 值通过会话目录主题来自 ISE
SXP	目标 SGT 值来自 ISE 通过 SXP 主题

目标 SGT（系统日志： DestinationSecurityGroupTag）

连接中涉及的目标的数值安全组标记 (SGT) 属性。

目标 SGT 值从 **DestinationSecurityGroupType** 字段中指定的 源获取。

检测类型

此字段显示客户端的检测来源。

设备

在 Cisco Secure Firewall Management Center Web 界面中，此值限制摘要和图形。

检测到连接的受管设备，或者对于从 NetFlow 数据生成的连接，是指处理数据的受管设备。

DeviceUUID （仅限系统日志）

生成事件的 Firepower 设备的唯一标识符。

以下字段共同唯一标识连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

DNS 查询（系统日志：DNSQuery）

在与名称服务器的连接中提交的用于查找域名的 DNS 查询。

当启用 DNS 过滤时，此字段还可以保存 URL 过滤匹配的域名。在这种情况下，URL 字段将为空，URL 类别和 URL 信誉字段包含与域关联的值。

有关 DNS 过滤的详细信息，请参阅 DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别。

DNS 记录类型（系统日志：DNSRecordType）

用于解析连接中提交的 DNS 查询的 DNS 资源记录的类型。

DNS 响应（系统日志：DNSResponseType）

查询时在与名称服务器的连接中返回的 DNS 响应。

DNS Sinkhole 名称（系统日志：DNS_Sinkhole）

系统将连接重定向的 Sinkhole 服务器的名称。

DNS TTL（系统日志：DNS_TTL）

DNS 服务器缓存 DNS 资源记录的秒数。

域

检测到连接的受管设备的域，或者对于从 NetFlow 数据生成的连接，是指处理数据的受管设备的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

加密对等体

为关联连接加密数据包的 VPN 对等体的 IP 地址（对等体的 IKE 地址）。

您必须启用访问控制策略规则的日志记录设置，以便在连接开始和结束时进行记录，以查看 VPN 对等体 IP 地址。

加密可视性指纹（系统日志： EncryptedVisibilityFingerprint）

加密可视性引擎 (EVE) 为会话检测到的 TLS 指纹。

加密可视性进程名称（系统日志： EncryptedVisibilityProcessName）

由加密可视性引擎（EVE）分析的 TLS 客户端呼叫数据包中的进程或客户端。

加密可视性置信度得分（系统日志： EncryptedVisibilityConfidenceScore）

加密可视性引擎检测到正确进程的置信度值范围为 0-100%。例如，如果进程名称为 Firefox，并且置信度分数为 80%，则意味着引擎 80% 的置信度表示其检测到的进程是 Firefox。

加密可视性威胁置信度（系统日志： EncryptedVisibilityThreatConfidence）

加密可视性引擎（EVE）检测到的进程包含威胁的概率级别。此字段根据威胁置信度分数中的值指示频段（非常高，高，中，低或非常低）。

加密可视性威胁置信度评分（系统日志： EncryptedVisibilityThreatConfidenceScore）

加密可视性引擎检测到的进程包含威胁的置信度值范围为 0-100%。如果威胁置信度分数非常高，例如 90%，则加密可视性进程名称字段显示“恶意软件”。

终端位置 (Endpoint Location)

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。

终端配置文件（系统日志：Endpoint Profile）

用户的终端设备类型，如 ISE 所识别。

事件优先级 （仅限系统日志）

连接事件是否为高优先级事件。高 优先级事件是与入侵、安全情报、文件或恶意软件事件关联的连接事件。所有其他事件均为 低 优先级。

文件（系统日志：FileCount）

在与一个或多个文件事件关联的连接中检测到或阻止的文件（包括恶意软件文件）数量。

在 Cisco Secure Firewall Management Center Web 界面中， **查看文件图标** 指向文件列表。图标上的数字表示连接中检测到或阻止的文件数量（包括恶意软件文件）。

第一个数据包或最后一个数据包（系统日志：ConnectionDuration 字段）

查看了会话的第一个或最后一个数据包的日期和时间。

第一个数据包时间 （仅限系统日志）

系统遇到第一个数据包的时间。

以下字段共同唯一标识连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

HTTP 引用站点（系统日志：HTTPReferer）

HTTP 来源地址，表示在连接中检测到的 HTTP 流量的请求 URL 来源地址（例如提供到另一个 URL 的链接或从其导入链接的网站）。

HTTP 响应代码（系统日志：HTTPResponse）

发送的 HTTP 状态代码用于响应客户端通过连接的 HTTP 请求。

入口/出口接口（系统日志：IngressInterface、EgressInterface）

与连接相关的入口或出口接口。如果部署包括异步路由配置，则入口和出口接口可能属于同一内联集。

入口/出口安全区域（系统日志：IngressZone、EgressZone）

与连接相关的入口或出口安全区。

对于重新分区的封装连接，“入口”(Ingress) 字段显示您分配的隧道区域，而不是原始入口安全区域。“出口”(Engress) 字段为空。

入口虚拟路由器/出口虚拟路由器（系统日志： IngressVRF、 EgressVRF）

在使用虚拟路由的网络中，用于流量进出网络的虚拟路由器的名称。

发起方/响应方字节数（系统日志：InitiatorBytes、ResponderBytes）

会话发起方传输的总字节数或会话响应方接收的总字节数。

Initiator/Responder Continent

当检测到可路由 IP 时，与会话发起方或响应方的 IP 地址关联的大洲。

Initiator/Responder Country

当检测到可路由 IP 时，与会话发起方或响应方的 IP 地址关联的国家/地区。系统显示国家/地区的旗帜图标和国家/地区的 ISO 3166-1 alpha-3 国家/地区代码。将鼠标指针悬停在旗帜图标上可以查看该国家/地区的全名。

发起方/响应方 IP（系统日志：SrcIP、DstIP）

在 Cisco Secure Firewall Management Center Web 界面中，这些值限制摘要和图形。

会话发起方或响应方的 IP 地址（如果启用 DNS 解析，则还包括主机名）。

另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明，第 733 页。

在 Cisco Secure Firewall Management Center Web 界面中，主机图标标识导致连接被阻止的 IP 地址。

对于被预过滤器策略阻止或使用快速路径的明文、传递隧道，启动器和响应器 IP 地址不表示隧道终端（隧道任一端的网络设备的路由接口）。

发起方/响应方数据包数 (系统日志： InitiatorPackets、ResponderPackets)

会话发起方传输的总数据包数或会话响应方接收的总数据包数。

发起方用户（系统日志：User）

在 Cisco Secure Firewall Management Center Web 界面中，此值限制摘要和图形。

登录到会话发起方的用户。如果使用**无身份验证**填充此字段，则用户流量：

- 匹配没有关联身份策略的访问控制策略
- 与身份策略中的任何规则都不匹配

如果适用，用户名前面会附加 <区域>\。

另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明，第 733 页。

入侵事件（系统日志：IPSCount）

与连接相关的入侵事件数量（如有）。

在 Cisco Secure Firewall Management Center Web 界面中， **查看入侵事件图标** 指向事件列表。

IOC

事件是否针对连接中涉及的主机触发了危害表现 (IOC)。

NAT 源/目标 IP （系统日志： NAT_InitiatorIP，NAT_ResponderIP）

会话发起方或响应方的 NAT 转换 IP 地址。

NAT 源/目标端口（系统日志： NAT_InitiatorPort，NAT_ResponderPort）

会话发起方或响应方的 NAT 转换端口。

NetBIOS 域（系统日志：NetBIOSDomain）

会话中使用的 NetBIOS 域。

NetFlow SNMP Input/Output

对于从NetFlow数据生成的连接，是指连接流量进入或退出NetFlow导出器时接口的接口索引。

NetFlow 源/目标自治系统 (NetFlow Source/Destination Autonomous System)

对于从 NetFlow 数据生成的连接，是指连接中的流量源或目标的边界网关协议自治系统编号。

NetFlow 源/目标前缀 (NetFlow Source/Destination Prefix)

对于从 NetFlow 数据生成的连接，是指与源或目标前缀掩码用 AND 连接的源或目标 IP 地址。

NetFlow 源/目标 TOS (NetFlow Source/Destination TOS)

对于从 NetFlow 数据生成的连接，是指连接流量进入或退出 NetFlow 导出器时服务类型 (TOS) 字节的设置。

网络分析策略（系统日志：NAPPolicy）

与事件生成相关的网络分析策略 (NAP)（如果有）。

原始客户端国家/地区 (Original Client Country)

原始客户端IP地址所属的国家/地区。为获取该值，系统从X-Forwarded-For (XFF)、True-Client-IP或自定义的HTTP报头提取原始客户端IP地址，然后使用地理位置数据库 (GeoDB) 将其映射到国家/地区。要填充此字段，必须启用根据原始客户端处理代理流量的访问控制规则。

原始客户端 IP（系统日志：originalClientSrcIP）

来自 X-Forwarded-For (XFF)、True-Client-IP 或自定义的 HTTP 报头的原始客户端 IP 地址。要填充此字段，必须启用根据原始客户端处理代理流量的访问控制规则。

预过滤器策略（系统日志：Prefilter Policy）

处理连接的预过滤器策略。

协议（系统日志：Protocol）

在 Cisco Secure Firewall Management Center Web 界面中：

- 此值限制摘要和图形。
- 此字段仅用作搜索字段。

连接中使用的传输协议。要搜索特定协议，请使用 http://www.iana.org/assignments/protocol-numbers 中所列的名称或编号协议。

QoS 应用的接口 (QoS-Applied Interface)

对于速率受限的连接，是指应用了速率限制的接口的名称。

QoS 丢弃的发起方/响应方字节数 (QoS-Dropped Initiator/Responder Bytes)

由于速率限制而从会话发起方或会话响应方丢弃的字节数。

QoS 丢弃的发起方/响应方数据包数 (QoS-Dropped Initiator/Responder Packets)

由于速率限制而从会话发起方或会话响应方丢弃的数据包的数量。

QoS 策略的比较

对连接进行了速率限制的 QoS 策略。

QoS 规则 (QoS Rule)

对连接进行了速率限制的 QoS 规则。

原因（系统日志：AccessControlRuleReason）

在许多情况下记录连接的一个或多个原因。有关完整列表，请参阅连接事件原因，第 734 页。

原因为“IP 阻止”(IP Block)、“DNS 阻止”(DNS Block) 和“URL 阻止”(URL Block) 的连接在每个唯一发起方-响应方对中的阈值都为 15 秒。系统在阻止其中一个连接后，无论端口或协议如何，在接下来的 15 秒内都不会为这两个主机之间的其他受阻连接生成连接事件。

引用的主机（系统日志：ReferencedHost）

如果连接中的协议是 HTTP 或 HTTPS，则此字段显示各协议使用的主机名。

SecIntMatchingIP（仅限系统日志）

哪些 IP 地址匹配。

可能的值：`None`、`Destination` 或 `Source`。

安全情景（系统日志：Context）

对于在多情景模式下由 ASA FirePOWER 处理的连接，是指识别流量通过的虚拟防火墙组的元数据。

安全情报类别（系统日志： URLSICategory、 DNSSICategory 、IPReputationSICategory）

代表或包含连接中被受阻的URL、域名或IP地址的对象的名称。安全情报类别可以是网络对象或组、阻止列表、自定义安全情报列表或源、与观察关联的 TID 类别或者情报源中一个类别的名称。

在 Cisco Secure Firewall Management Center Web 界面中，DNS、网络（IP 地址）和 URL 安全情报连接事件会合并为单个类别字段。在系统日志消息中，这些事件具有特定的类型。

与安全相关的连接事件包括安全情报事件和其他连接事件，例如触发入侵或恶意软件事件的连接事件。**安全情报摘要** 工作流程按类别和计数显示所有安全情报事件。没有安全情报类别的事件将分组并仅显示计数。

有关智能情报源中的类别详细信息，请参阅安全情报类别。

源设备

在 Cisco Secure Firewall Management Center Web 界面中，此值限制摘要和图形。

广播用于为连接生成的数据的 NetFlow 导出器的 IP 地址。如果受管设备检测到连接，则此字段显示 `Firepower`。

源端口/ICMP 类型（系统日志：SrcPort、ICMPType）

在 Cisco Secure Firewall Management Center Web 界面中，这些值限制摘要和图形。

会话发起方使用的端口或 ICMP 类型。

SourceSecurityGroup （仅限系统日志）

此字段包含与 **SourceSecurityGroupTag** 中的数字值关联的文本值（如果可用）。如果组名不可用作文本值，则此字段包含与 SourceSecurityGroupTag 字段相同的整数值。可以从内联设备（未指定源 SGT 名称）或从 ISE（指定源）获取标签。

SourceSecurityGroupType （仅限系统日志）

此字段显示从中获取安全组标记的源。

值	说明
内联	源 SGT 值来自数据包
会话目录	源 SGT 值通过会话目录主题来自 ISE
SXP	源 SGT 值来自 ISE 通过 SXP 主题

源 SGT（系统日志： SourceSecurityGroupTag）

连接中涉及的数据包的安全组标记 (SGT) 的数值呈现的属性。SGT 指定受信任网络中的流量源的权限。安全组访问（思科 TrustSec 和思科 ISE 的功能）在数据包进入网络时应用该属性。

SSL 实际操作（系统日志：SSLActualAction）

在 Cisco Secure Firewall Management Center Web 界面中，此字段仅为搜索字段。

系统显示搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中的字段值。

系统应用于 SSL 策略中的加密流量的操作。

操作	说明
阻止/阻止并重置	表示阻止的加密连接。
解密（重新签名）	表示使用重新签名的服务器证书解密的传出连接。
解密（替换密钥）	表示使用具有替代公钥的自签名服务器证书解密的传出连接。
解密（已知密钥）	表示使用已知私钥解密的传入连接。
默认操作	表示连接采用默认操作处理。
不解密	表示系统未解密的连接。

SSL 证书信息（系统日志：SSLCertificate）

在 Cisco Secure Firewall Management Center Web 界面中，此字段仅为搜索字段。

用于加密流量的公钥证书上存储的信息，包括：

- 使用者/颁发者公用名称
- 使用者/颁发者组织
- 使用者/颁发者单位
- 无效时间
- 序列号
- 证书指纹
- 公钥指纹

SSL 证书状态（系统日志：SSLServerCertStatus）

仅在配置了证书状态规则条件时，此字段才适用。如果加密流量与 SSL 规则匹配，则此字段显示以下一个或多个服务器证书状态值：

- 自签名
- 有效
- 无效签名
- 无效颁发者
- 已到期
- 未知
- 无效
- 已撤销

如果无法解密的流量与 SSL 规则相匹配，则此字段显示未检查 `(Not Checked)`。

SSL 密码套件（系统日志：SSSLCipherSuite）

表示用于加密连接的密码套件的宏值。有关密码套件值的指定，请参阅https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。

应用于连接的 SSL 加密

此字段在 Firepower 管理中心 Web 界面中仅用作搜索字段。

在 **SSL** 搜索字段中输入 **`yes`** 或 **`no`** 以查看 TLS/SSL 加密或非加密连接。

SSL 预期操作（系统日志：SSLExpectedAction）

在 Cisco Secure Firewall Management Center Web 界面中，此字段仅为搜索字段。

在 SSL 规则生效的情况下，系统预期会应用于加密流量的操作。

输入为 **SSL 实际操作 (SSL Actual Action)** 列出的任何值。

SSL 失败原因（系统日志：SSLFlowStatus）

系统无法解密已加密流量的原因：

- 未知
- 不匹配
- 成功
- 未缓存的会话
- 未知加密套件
- 不受支持的加密套件
- 不支持的 SSL 版本
- 使用了 SSL 压缩
- 会话在被动模式下无法解密
- 握手错误
- 解密错误
- 挂起的服务器名称类别查找
- 挂起的公用名类别查找
- 内部错误 (Internal Error)
- 不完全握手
- 网络参数不可用
- 服务器证书处理无效
- 服务器证书指纹不可用
- 无法缓存使用者 DN
- 无法缓存颁发者 DN
- 未知的 SSL 版本
- 外部证书列表不可用
- 外部证书指纹不可用
- 内部证书列表无效
- 内部证书列表不可用
- 内部证书不可用
- 内部证书指纹不可用

- 服务器证书验证不可用
- 服务器证书验证失败
- 无效操作

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL 流错误

当在 TLS/SSL 会话期间发生错误时，为错误名称和十六进制代码，如果未发生错误，则为 `Success`。

SSL 流标志

已加密连接的前十大调试级别标记。在工作流程页面上，要查看所有标记，请点击省略号 (**...**)。

如果您的受管设备过载，则将显示消息OVER_SUBSCRIBED。有关详细信息，请参阅对 TLS/SSL 超订用进行故障排除。

SSL 流消息

下面的关键字表示加密流量与在 TLS/SSL 握手期间客户端和服务器之间交换的指定消息类型相关联。有关详细信息，请参阅http://tools.ietf.org/html/rfc5246。

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED

- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER
- 服务器_名称_不匹配

  在会话中看到的服务器证书具有不对应于指定域名的公用名或 SAN 值。

- 证书_缓存_HIT

  在缓存中找到与目标域名匹配的证书。

- 证书_缓存_MISS

  在缓存中未找到与目标域名匹配的证书。

如果应用使用 TLS/SSL 心跳扩展，则将显示消息 HEARTBEAT。有关详细信息，请参阅关于 TLS 心跳。

SSL 策略（系统日志：SSLPolicy）

处理连接的 SSL 策略。

如果在访问控制策略高级设置中启用了 TLS 服务器身份发现，并且没有与访问控制策略关联的 SSL 策略，则此字段 不 对所有 SSL 事件保留任何内容。

SSL 规则（系统日志：SSLRuleName）

处理连接的 SSL 规则或默认操作，以及与连接匹配的第一个监控规则。如果连接匹配某个监控规则，则该字段会显示处理连接的规则的名称，后跟监控规则名称。

SSLServerName（仅限系统日志）

此字段仅作为系统日志字段存在；不会出现在 Cisco Secure Firewall Management Center Web 界面中。

客户端用于建立加密连接的服务器主机名。

SSL 会话 ID（系统日志：SSLSessionID）

在 TLS/SSL 握手期间，在客户端与服务器之间协商的十六进制会话 ID。

SSL 状态

与记录加密连接的 **SSL 实际操作 (SSL Actual Action)**（SSL 规则、默认操作或无法解密的流量操作）关联的操作。**锁定图标** 指向SSL证书详细信息。如果证书不可用（例如，对于因TLS/SSL握手错误而受阻的连接），锁定图标会显示为灰色。

如果系统无法解密已加密连接，则其会显示所采取的 **SSL 实际操作 (SSL Actual Action)**（无法解密的流量操作）以及 **SSL 失败原因 (SSL Failure Reason)**。例如，如果系统检测到使用未知密码套件加密的流量并且未做进一步检查即允许了该流量，则此字段显示 `Do Not Decrypt (Unknown Cipher Suite)`。

如果加密连接的 SSL 握手不完整，并且系统无法解密流量，则 **SSL 状态** 字段显示 未知（不完整握手）。

当搜索该字段时，请输入一个或多个 **SSL 实际操作 (SSL Actual Action)** 和 **SSL 失败原因 (SSL Failure Reason)** 值以查看系统处理或无法解密的已加密流量。

SSL 使用者/颁发者所在国家/地区

此字段仅在 Cisco Secure Firewall Management Center Web 界面中可用，且仅作为搜索字段。

与加密证书关联的使用者或颁发者所在国家/地区的双字符 ISO 3166-1 alpha-2 国家/地区代码。

SSL 票证 ID（系统日志：SSLTicketID）

在 TLS/SSL 握手期间发送的会话单信息的一个十六进制哈希值。

SSLURLCategory（仅限系统日志）

加密连接中受访 URL 的 URL 类别。

此字段仅作为系统日志字段存在；在 Cisco Secure Firewall Management Center Web 界面中，此字段中的值包含在“URL 类别”列中。

另请参阅 **URL**。

SSL 版本（系统日志：SSLVersion）

用来加密连接的 TLS/SSL 协议版本。

- 未知
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TLSv1.2
- TLSv1.3

TCP 标志（系统日志：TCPFlags）

对于从 NetFlow 数据生成的连接，是指在连接中检测到的 TCP 标志。

当搜索此字段时，输入逗号分隔的 TCP 标志列表以查看 至少 具有其中一个标志的所有连接。

时间

系统用来在连接摘要中汇总连接的 5 分钟时间间隔的结束时间。此字段不可搜索。

数据包总数

此字段仅用作搜索字段。

在连接中传输的数据包的总数。

流量 (KB)

此字段仅用作搜索字段。

在连接中传输的总数据量（以千字节为单位）。

隧道/预过滤器规则（系统日志：Tunnel or Prefilter Rule）

处理连接的隧道规则、预过滤器规则或预过滤器策略默认操作。

URL、URL 类别和 URL 信誉（系统日志： URL、 URL 类别 和 SSLURLCategory， URL 类别）

会话期间受控主机请求的 URL 以及该 URL 的类别和信誉（如有）。

要使事件显示 URL 类别和信誉，必须在访问控制策略中包含适用的 URL 规则，并在 **URL** 选项卡下为该规则配置 URL 类别和 URL 信誉。

如果连接在与 URL 规则匹配之前得到处理，则 URL 类别和信誉不会显示在事件中。

如果 URL 列为空且 DNS 过滤已启用，则 DNS 查询字段显示域，并且 URL 类别和 URL 信誉值适用于该域。

如果系统识别或阻止 TLS/SSL 应用，而请求的 URL 位于加密流量中，系统会基于 SSL 证书识别流量。因此，对于 TLS/SSL 应用，此字段表示包含在证书中的通用名称。

另请参阅上述 **SSLURLCategory**。

用户代理（系统日志：UserAgent）

从连接中检测到的 HTTP 流量提取的用户代理字符串应用信息。

VLAN ID（系统日志：VLAN_ID）

与触发连接的数据包关联的最内部的 VLAN ID。

VPN 操作

与连接关联的 VPN 操作。

可能的值包括：

- **加密**：VPN 对已记录连接的流量进行加密。请参阅 **加密对等体** 列，了解加密连接的 VPN 对等体的 IP 地址。
- **解密**：VPN 解密已记录连接的流量。请参阅 **加密对等体** 列，了解解密连接的 VPN 对等体的 IP 地址。
- **VPN 路由**：流量通过 VPN 隧道转换。VPN 在连接开始时执行解密，在连接结束时执行加密。请参阅 **加密对等体** 和 **解密对等体列**，了解加密和解密连接的 VPN 对等体的 IP 地址。

Web 应用（系统日志：WebApplication）

表示连接中检测到的 HTTP 流量内容或请求的 URL 的 Web 应用。

如果 Web 应用不匹配事件的 URL，该流量大概是推荐流量，例如广告流量。如果系统检测到推荐流量，则会存储该推荐应用（如有），并将该应用列为 Web 应用。

如果系统不能在 HTTP 流量中识别特定的网络应用，该字段显示网络浏览 (`Web Browsing`)。

Web 应用类别和标记 (Web Application Category and Tag)

展示了应用特征的条件，以帮助您了解应用功能。

关于连接和 安全相关连接事件 字段

在 Cisco Secure Firewall Management Center Web 界面中，您可以使用 **分析 > 连接** 子菜单下的表格和图形工作流程查看和搜索连接和 安全相关连接 事件。

注释 对于每个 安全相关连接事件，都有相同、独立存储的连接事件。所有 安全相关连接事件 都有一个由系统填充的 **安全情报类别** 字段。

任何单独事件的可用信息视系统记录连接的方式、原因和时间而异。

搜索限制

搜索页面上标有星号 **(*)** 的字段会限制连接图形和连接摘要。由于连接图基于连接摘要，因此，约束连接摘要的相同条件也约束连接图。如果使用无效搜索限制来搜索连接摘要，并在自定义工作流程中使用连接摘要页面查看结果，则无效限制会标记为不适用 (N/A)，并标有删除线。

系统日志字段

大多数字段会同时显示在 Cisco Secure Firewall Management Center Web 界面和系统日志消息中。没有所列的系统日志等同项的字段在系统日志消息中不可用。如前所述，一些字段仅在系统日志中提供，并且其他一些字段在系统日志消息中为分开字段，而在 Web 界面中为合并字段，反之亦然。

有关发起方/响应方，源/目标和发件人/接收方字段的说明

表 *106:* 术语比较

字段	事件类型	说明
发起方/响应方	连接	连接的发起方/响应方。 连接的发起方不一定与入侵源或恶意软件文件的发送方相同。
源/目标	入侵	攻击的源/目标。 入侵事件的源可以是连接的发起方或响应方。
发件人/收件人 （正在发送...，正在接收...）	文件，恶意软件	文件或恶意软件的发件人/收件人。 文件的发送方不一定是连接的发起方，因为可以上传或下载文件。

连接事件原因

在以下情况下，连接事件中的“原因”(Reason) 字段显示记录连接的原因：

原因	说明
内容限制	系统修改数据包以实施与安全搜索功能相关的内容限制。
DNS 阻止	系统未经检查就根据域名和安全情报数据拒绝连接。“DNS 阻止”原因与“阻止”、“找不到域”或 Sinkhole 操作匹配，具体取决于 DNS 规则操作。
DNS 监控	系统将根据域名和安全情报数据拒绝连接，但您将系统配置为监控而不是拒绝连接。
大象流	连接速率大到足以被认为是大象流，这种流的大小足以影响整体系统性能。默认情况下，大象流是速率大于每 10 秒 1GB 的流。您可以使用 **系统支持大象流检测** 命令调整字节和时间阈值，以在 威胁防御 CLI 中识别大象流。有关详细信息，请参阅Cisco Secure Firewall Threat Defense 命令参考。 **注释** 仅当超过字节和时间阈值时，流才被视为大象流。 您可以创建自定义控制面板来关联象流和其他相互关联的指标，例如Snort、系统和物理核心等CPU指标。有关详细信息，请参阅“测试和故障排除”章节。
已豁免大象流	如果检测到大型流，并且该流与为必须免于补救的流定义的L4 ACL规则匹配。
文件阻止	连接中包含系统禁止传输的文件或恶意软件文件。“文件阻止”原因始终与“阻止”操作匹配。
文件自定义检测	连接中包含自定义检测列表上系统禁止传输的文件。
文件监控	系统在连接中检测到特定类型的文件。
允许继续传输文件	文件传输最初被“阻止文件”或“阻止恶意软件”文件规则阻止。在部署允许该文件的新访问控制策略之后，将自动继续 HTTP 会话。此原因只出现在内联部署中。
阻止继续传输文件	“检测文件”或“恶意软件云查找”文件规则最初允许文件传输。在新访问控制策略阻止文件部署之后，会自动停止 HTTP 会话。此原因只出现在内联部署中。
智能应用绕行 (Intelligent App Bypass)	智能应用绕行 (IAB) 模式： • 如果操作是“信任”(Trust)，则 IAB 处于绕行模式。匹配的流量通过，无需进一步检查。 • 如果操作是“允许”(Allow)，则 IAB 处于测试模式。匹配流量可供进一步检查。

原因	说明
入侵阻止	Snort2 引擎-系统阻止或本可阻止在连接中检测到的漏洞（入侵策略违规）。“入侵阻止”原因与用于阻止漏洞的“阻止”操作和用于本可阻止漏洞的“允许”操作匹配。 Snort3引擎-当出现“将被丢弃”结果时，连接事件原因为空，而不是“入侵阻止”。对于“已丢弃”事件，在填充连接事件原因方面将其视为“允许”。
入侵监控	系统检测到但并未阻止连接中检测到的漏洞。当触发的入侵规则状态设置为“生成事件”时，即会发生这种情况。
IP 阻止	系统未经检查就根据 IP 地址和安全情报数据拒绝连接。“IP 阻止”原因始终与“阻止”操作匹配。
IP 监控	系统将根据 IP 地址和安全情报数据拒绝连接，但您将系统配置为监控而不是拒绝连接。
SSL 阻止	系统基于 TLS/SSL 检查配置阻止加密连接。“SSL 阻止”(SSL Block) 原因始终与“阻止”(Block) 操作匹配。
URL 阻止	系统未经检查就根据 URL 和安全情报数据拒绝连接。“URL 阻止”原因始终与“阻止”操作匹配。
URL 监控	系统将根据 URL 和安全情报数据拒绝连接，但您将系统配置为监控而不是拒绝连接。
用户绕行	系统最初阻止用户的 HTTP 请求，但用户点击浏览警告页面以查看网站。“用户绕行”(User Bypass) 原因始终与“允许”(Allow) 操作匹配。

填充连接事件字段的要求

可用于连接事件、 安全相关的连接事件或连接摘要的信息取决于多种因素。

设备型号和许可证

许多功能要求您启用目标设备上的特定许可功能，并且许多功能仅在部分型号上可用。

流量特征

系统仅报告在网络流量中展示（并且可检测）的信息。例如，可能没有与发起人主机相关联的用户，或者在协议不是 DNS、HTTP 或 HTTPS 的连接中未检测到引用的主机。

源/检测方法：基于流量的检测与 NetFlow

除纯 NetFlow 字段以外，NetFlow 记录中可用的信息比由基于流量的检测生成的信息更有限；请参阅NetFlow 和受管设备数据之间的差异。

评估阶段

每种类型的流量检查和控制都以提供最大灵活性和性能的方式进行。

例如，在进行更多资源密集型评估之前，系统会强制实施安全情报。当连接被安全情报阻止时，生成的事件不包含系统本该从后续评估中收集的信息（例如用户身份）。

记录方法：连接的开始或结束

当系统检测到连接时，您可以在其开始还是结束（或两者）时记录该连接取决于如何将系统配置为检测和处理该连接。

开始连接事件不具有必须通过检查会话持续时间内的流量来确定的信息（例如，连接中传输数据的总量或最终数据包的时间戳）。也不保证开始连接事件拥有关于会话中应用或URL流量的信息，且该等事件不包含有关会话加密的任何详细信息。连接开始日志记录通常是受阻连接的唯一选项。

连接事件类型：个别与摘要

连接摘要不包含与其汇聚连接相关联的所有信息。例如，在汇总连接以形成连接摘要时没有使用客户端信息，因此摘要中不包含客户端信息。

请记住，连接图基于连接摘要数据，这些数据仅使用连接结束日志。如果系统配置为仅记录连接开始数据，则连接图和连接摘要事件视图不包含任何数据。

注释 与安全相关的连接事件包括安全情报事件和其他连接事件，例如触发入侵或恶意软件事件的连接事件。**安全情报摘要 (Security Intelligence Summary)** 工作流程将没有安全情报类别的安全相关连接事件分组，并显示没有 **安全情报类别 (Security Intelligence Category)** 值的计数。

其他配置

影响连接日志记录的其他配置包括但不限制：

- 仅当在与通过 Active Directory 域控制器进行身份验证的用户关联的连接中配置 ISE 时，才填充 ISE 相关字段。连接事件不包含通过 LDAP、RADIUS 或 RSA 域控制器进行身份验证的用户的 ISE 数据。
- 仅当将 ISE 配置为身份源或添加自定义 SGT 规则条件时，才会填充“安全组标记” (SGT) 字段。
- 仅在由预过滤器策略处理的连接中，才会填充预过滤器相关字段（包括安全区域字段中的隧道区域信息）。
- 仅在由 解密策略处理的加密连接中，才会填充TLS/SSL相关字段。如果不需要解密流量，则可以使用“不解密”规则操作查看这些字段的值。
- 仅在由与文件策略关联的访问控制规则记录的连接中，才会填充文件信息字段。
- 仅在由与入侵策略关联或使用默认操作的访问控制规则记录的连接中，才会填充入侵信息字段。
- 仅在速率受限的连接中，才会填充 QoS 相关字段。

- 仅在特定情况下（例如，当用户绕过交互式阻止配置时），才会填充“原因”(Reason) 字段。
- 仅当曾经配置 Cisco Secure Firewall Management Center以实现多租户时，才存在“域”字段。
- 访问控制策略中的一项高级设置控制系统为 HTTP 会话中的受监控主机请求的每个 URL 存储在连接日志中的字符数。如果您使用此设置来禁用URL 日志记录，则虽然您仍可查看类别和信誉数据（如果存在），但系统不会在连接日志中显示单个 URL。
- 要使连接事件显示 URL 类别和信誉，必须在访问控制策略中包含适用的 URL 规则，并在 **URL** 选项卡下配置具有 URL 类别和 URL 信誉的规则。如果连接在与 URL 规则匹配之前得到处理，则 URL 类别和信誉不会显示在事件中。

相关主题

NetFlow 和受管设备数据之间的差异

连接事件字段中的可用信息

本主题中的表指示系统何时可以填充连接和安全情报字段。表中的列表示以下事件类型：

- 源：直接 - 代表由系统受管设备检测和处理的连接的事件。
- 源：NetFlow - 代表由 NetFlow 导出器导出的连接的事件。
- 记录：开始 - 代表在开始时记录的连接的事件。
- 记录：结束 - 代表在结束时记录的连接的事件。

表中的“是”并不意味着系统必须填充连接事件字段，而表示它可以填充。系统仅报告在网络流量中展示（并且可检测）的信息。例如，只有由 解密策略处理的加密连接的记录，才会填充 TLS/SSL 相关字段。

连接事件字段	源：直接	源：NetFlow	记录：开始	记录：结束
访问控制策略	是	否	是	是
访问控制规则	是	否	是	是
操作	是	否	是	是
应用协议	是	是	如果有	是
应用协议类别和标记	是	否	如果有	是
应用风险	是	否	如果有	是
业务相关性	是	否	如果有	是
客户端	是	否	如果有	是
客户端类别和标记	是	否	如果有	是

连接事件字段	源：直接	源：NetFlow	记录：开始	记录：结束
客户端版本	是	否	如果有	是
连接	是	是	否	是
计数	是	是	是	是
目标端口/ICMP 类型	是	是	是	是
目标 SGT	是	否	是	是
设备	是	是	是	是
域	是	是	是	是
DNS 查询	是	否	是	是
DNS 记录类型	是	否	是	是
DNS 响应	是	否	是	是
DNS Sinkhole 名称	是	否	是	是
DNS TTL	是	否	是	是
出口接口	是	否	是	是
出口安全区域	是	否	是	是
终端位置	是	否	是	是
终端配置文件	是	否	是	是
文件	是	否	否	是
首个数据包	是	是	是	是
HTTP 引用站点	是	否	否	是
HTTP 响应代码	是	否	是	是
入口接口	是	否	是	是
入口安全区域	是	否	是	是
发起方字节数	是	是	不实用	是
发起方所在国家/地区	是	否	是	是
发起方 IP	是	是	是	是
发起方数据包数	是	是	不实用	是

连接事件字段	源：直接	源：NetFlow	记录：开始	记录：结束
发起方用户	是	是	是	是
入侵事件	是	否	否	是
入侵策略	是	否	是	是
IOC（危害表现）	是	否	是	是
最后数据包	是	是	否	是
NetBIOS 域	是	否	是	是
NetFlow 源/目标自治系统	否	是	否	是
NetFlow 源/目标前缀	否	是	否	是
NetFlow 源/目标 TOS	否	是	否	是
NetFlow SNMP 输入/输出	否	是	否	是
Network Analysis Policy	是	否	是	是
原始客户端国家/地区	是	否	是	是
原始客户端 IP	是	否	是	是
预过滤器策略	是	否	是	是
QoS 适用接口	是	否	否	是
QoS 丢弃的发起方字节数	是	否	否	是
QoS 丢弃的发起方数据包数	是	否	否	是
QoS 丢弃的响应方字节数	是	否	否	是
QoS 丢弃的响应方数据包数	是	否	否	是
QoS 策略的比较	是	否	否	是
QoS 规则	是	否	否	是
原因	是	否	是	是
引用的主机	是	否	否	是
响应方字节数	是	是	不实用	是
响应方所在国家/地区	是	否	是	是
响应方 IP	是	是	是	是

连接事件字段	源：直接	源：NetFlow	记录：开始	记录：结束
响应方数据包数	是	是	不实用	是
安全情景（仅 ASA）	是	否	是	是
安全情报类别	是	否	是	是
源设备	是	是	是	是
源端口/ICMP 类型	是	是	是	是
源 SGT	是	否	是	是
SSL 证书状态	是	否	否	是
SSL 密码套件	是	否	否	是
SSL 流错误	是	否	否	是
SSL 流量标志	是	否	否	是
SSL 流量消息	是	否	否	是
解密策略	是	否	否	是
解密规则	是	否	否	是
SSL 会话 ID	是	否	否	是
SSL 状态	是	否	否	是
SSL 版本	是	否	否	是
TCP 标志	否	是	否	是
时间	是	是	否	是
隧道/预过滤器规则	是	否	是	是
URL	是	否	如果有	是
URL 类别	是	否	如果有	是
URL 信誉	是	否	如果有	是
用户代理	是	否	否	是
VLAN ID	是	否	是	是
Web 应用程序	是	否	如果有	是
Web 应用类别和标记	是	否	如果有	是

使用连接和 安全相关连接 事件表

可以使用 Cisco Secure Firewall Management Center 查看连接或 安全相关连接事件表。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。

访问连接图时看到的页面因所用的工作流程而有所不同。可以使用预定义的工作流程，最终会产生事件的表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

使用连接或安全情报工作流程表时，可以执行许多常见操作。

请注意，当您在向下展开解页面上约束连接事件时，来自相同事件的数据包和字节数将累加。然而，如果您正使用自定义工作流程，且没有将**计数 (Count)** 列添加到向下钻取页面，则会单独列出事件，数据包和字节将不会累加。

请注意，如果系统生成的连接事件数超过 25，则**连接事件 (Connection Events)** 表视图会显示**众多事件中的 1 个 (1 of Many)**，而不是可用的事件页面数。

开始之前

您必须是管理员或安全分析师用户才能执行此任务。

过程

步骤 1 选择以下其中一个选项：

- **分析** > **连接** > **事件** （适用于连接事件）
- **分析 (Analysis)** > **连接 (Connections)** > **安全相关事件 (Security-Related Events)**

注释 如果系统显示连接图而不是表，请按工作流程标题点击**切换工作流程 (switch workflow)**，然后选择预定义**连接事件 (Connection Events)** 工作流程，或自定义工作流程。请注意，所有预定义连接事件工作流程（包括连接图）最终都会产生连接的表视图。

步骤 2 有以下选项可供选择：

- “时间范围”(Time Range) - 要调整时间范围（如果未显示事件，则非常有用），请参阅更改时间窗口，第 661 页。
- 数据源 - 如果使用 安全分析和日志记录（本地部署）远程存储数据，并且您有充分的理由更改数据源，请选择数据源。有关此选项的重要信息，请参阅在 Cisco Secure Firewall Management Center 和使用存储在 Secure Network Analytics 设备上的连接事件上工作，第 651 页。
- “字段名称”(Field Names) - 要了解有关表中各列内容的详细信息，请参阅连接和 安全相关连接 事件字段，第 717 页。

  提示 事件表视图中的多个字段在默认情况下处于隐藏状态。要更改显示的字段，请点击任何列名称中的 **x** 以显示字段选择器。

- 其他信息 - 要查看系统外部可用源中的数据，请右键点击事件值。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，第 605 页
- 外部情报 - 要收集有关事件的情报，请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。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，第 605 页。
- 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)**。
- 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)**。
- 文件和恶意软件 - 要查看在连接中检测到或阻止的文件（包括恶意软件），请点击**查看文件 (View Files)**，然后如查看连接中检测到的文件和恶意软件，第 743 页中所述继续操作。
- 入侵事件 - 要查看与某个连接关联的入侵事件，及其优先级和影响，请点击 **入侵事件 (Intrusion Events)** 列中的 **入侵事件 (Intrusion Events)** 列，然后如查看与连接关联的入侵事件，第 744 页中所述继续操作。

  提示 要快速查看与一个或多个连接关联的入侵、文件或恶意软件事件，请使用表中的复选框选中连接，然后从**跳转至**下拉列表中选择合适的选项。请注意，由于它们在访问控制规则评估之前已被阻止，因此可能没有与列入安全情报阻止名单的连接关联的文件或入侵。如果已配置安全情报来监控连接（而非将其阻止），则只可以看到安全情报事件的这一信息。

- 证书 - 要查看有关用于解密连接的可用证书的详细信息，请在 **SSL 状态 (SSL Status)** 列中点击**已启用的锁定 (Enabled Lock)**。
- 限制 - 要限制显示的列，请在要隐藏的列标题中点击 **关闭**（×） 在显示的弹出窗口中，点击 **Apply**。

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

- 删除事件 -（仅限安全相关连接事件 表）要删除当前限制视图中的部分或全部项目，请选中要删除的项目旁边的复选框，然后点击 **删除** 或点击 **全部删除**。
- 向下展开 - 请参阅使用向下钻取页面，第 650 页。

  提示 要使用匹配已记录连接的多个监控规则之一向下展开，请点击一个 *N* **监控规则**值。在出现的弹出窗口中，点击要用于限制连接事件的监控规则。

- “导航此页面”(Navigate This Page) - 请参阅工作流程页面遍历工具，第 647 页。

- “在页面之间导航”(Navigate Between Pages) - 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- “在事件视图之间导航”(Navigate Between Event Views) - 要导航至其他事件视图以查看关联事件，请点击**跳转至 (Jump to)** 并从下拉列表中选择事件视图。
- “排序”(Sort) - 要对工作流程中的数据排序，请点击列标题。再次点击列标题以反转排列顺序。

相关主题

概述：工作流程，第 633 页
配置事件视图设置，第 193 页

查看连接中检测到的文件和恶意软件

如果将一个文件策略与一个或多个访问控制规则相关联，系统可以在匹配的流量中检测文件（包括恶意软件）。使用“分析”>“连接”菜单选项可查看与这些规则记录的连接关联的文件事件（如有）。 Cisco Secure Firewall Management Center 不显示文件列表，而是在**文件 (Files)** 列中显示视图文件 ()。“查看文件”上的数字表示连接中检测到或阻止的文件数量（包括恶意软件文件）。

并非所有文件和恶意软件事件都与连接有关。具体包括：

- 面向终端的AMP检测到的恶意软件事件（“基于终端的恶意软件事件”）与连接不相关。这些事件是从面向终端的 AMP 导入。
- 许多启用 IMAP 的邮件客户端使用单个 IMAP 会话，仅当用户退出应用时才结束。尽管长期运行的连接是由系统进行记录，但是在会话结束之前，会话中下载的文件不会与连接关联。

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

您必须是管理员或安全分析师用户才能执行此任务。

过程

步骤 1 转到**分析 > 连接**并选择相关选项。

步骤 2 使用连接事件表时，点击**查看文件 (View Files)**。
系统会显示弹出窗口，其中显示连接中检测到的文件列表及其类型和恶意软件处置情况（如适用）。

步骤 3 有以下选项可供选择：

- 查看 - 要查看文件事件表视图，请点击**文件的查看 (Malware File’s View)**。
- 查看 - 要查看恶意软件事件表视图的详细信息，请点击**恶意软件的查看 (Malware File’s View)**。
- 跟踪 - 要跟踪通过您的网络传输的文件，请点击**文件的轨迹 (File’s Trajectory)**。

- 查看 - 要查看连接的所有检测到的文件或面向网络的 AMP 检测到的恶意软件事件（“基于网络的恶意软件事件”），请点击**查看文件事件**或**查看恶意软件事件**。

相关主题

概述：工作流程，第 633 页
配置事件视图设置，第 193 页

查看与连接关联的入侵事件

如果您将入侵策略与访问控制规则或默认操作相关联，系统可以检测匹配流量中的漏洞。使用“分析”>“连接”菜单选项可查看与已记录连接相关联的入侵事件（如有），及其优先级和影响。

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

您必须是管理员或安全分析师用户才能执行此任务。

过程

步骤 1 转到**分析 > 连接**并选择相关选项。

步骤 2 使用连接事件表时，点击**入侵事件 (Intrusion Events)** 列中的**入侵事件 (Intrusion Events)** 。

步骤 3 在显示的弹出窗口中，您有以下选择：

- 点击 **所列事件的视图 (Listed Event’s View)** 以查看数据包视图中的详细信息。
- 点击**查看入侵事件 (View Intrusion Events)**，查看与连接关联的所有入侵事件的详细信息。

相关主题

概述：工作流程，第 633 页
配置事件视图设置，第 193 页

已加密连接的证书详细信息

可以使用“分析”>“连接”菜单下的选项来显示用于加密系统处理的连接的公钥证书（如有）。该证书包含以下信息。

表 ***107:*** 已加密连接的证书详细信息

属性	说明
使用者/颁发者公用名 (Subject/Issuer Common Name)	证书使用者或证书颁发者的主机名和域名。

属性	说明
使用者/颁发者组织 (Subject/Issuer Organization)	证书使用者或证书颁发者的组织。
使用者/颁发者组织单位 (Subject/Issuer Organization Unit)	证书使用者或证书颁发者的组织单位。
无效时间	证书有效日期。
序列号	由发行 CA 分配的序列号。
证书指纹	用于验证证书的 SHA 散列值。
公钥指纹	用于对证书内所含公钥进行身份验证的 SHA 哈希值。

相关主题

概述：工作流程，第 633 页
配置事件视图设置，第 193 页

查看连接摘要页面

“连接摘要”(Connection Summary) 页面仅对于满足以下条件的用户才可视：具有受连接事件搜索限制的自定义角色，已被授予对“连接摘要”(Connection Summary) 页面的基于菜单的显式访问权限。此页面提供按不同条件组织的受监控网络上的活动的图形。例如，“随时间推移的连接”(Connections over Time) 图形显示在选择的间隔内受监控网络上的连接总数。

如同连接图，您几乎可以在连接摘要图上执行完全一样的操作。然而，由于“连接摘要”(Connection Summary) 页面上的图形基于汇总数据，因此，您无法检查图形依赖的单个连接事件。换句话说，您无法从连接摘要图展开到连接数据表视图。

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。

过程

步骤 1 选择**概述** > **摘要** > **连接摘要**。

步骤 2 从**选择设备 (Select Device)** 列表中，选择要查看其摘要的设备，或者选择**所有 (All)** 以查看所有设备的摘要。

步骤 3 要操纵和分析连接图，请如使用连接事件图形，第 653 页中所述继续操作。

提示 要将连接图分离，以便可以执行进一步分析而不影响默认时间范围，请点击**查看 (View)**。

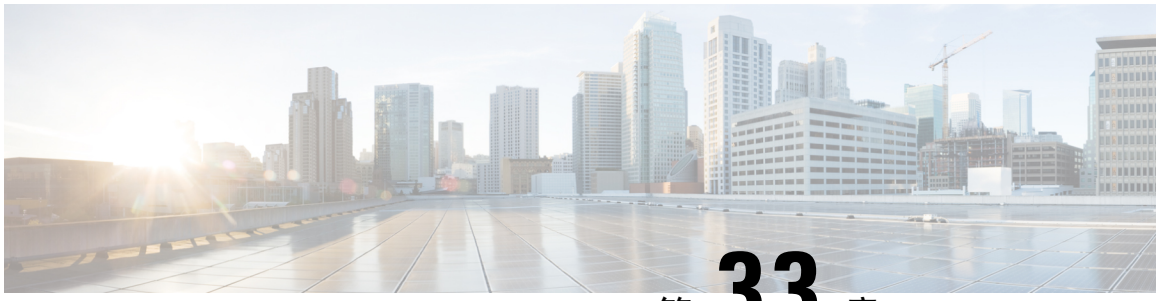
相关主题

启用用户角色升级，第 188 页

连接和安全情报事件历史记录

功能	最低 管理中心	最低 威胁防御	详情
新建连接事件原因 - 象流。	7.1	任意	请参阅连接事件原因，第 734 页。
NAT 转换后的 IP 地址和端口	7.1	任意	连接和安全情报事件表中添加了四个新字段： • NAT 源 IP • NAT 目标 IP • NAT 源端口 • NAT 目标端口
能够在处理远程存储的某些事件时选择数据源	7.0	任意	请参阅工作流程历史记录，第 669 页。
DNS 过滤	7.0 6.7（测试版功能）	任意	启用 DNS 过滤时： • DNS 查询字段可能包含与 DNS 过滤匹配项关联的域。 • 如果 URL 字段为空，但 DNS 查询、URL 类别和 URL 信誉有值，则事件由 DNS 过滤功能生成，类别和信誉适用于 DNS 查询中指定的域。 • 另请参阅中 《Cisco Secure Firewall Management Center 设备配置指南》的 *DNS* 过滤和事件 。
删除对连接事件的自定义表的支持	6.6	任意	您无法再为连接事件创建自定义表。如果升级，则连接事件的任何预先存在的自定义表仍然可用，但始终不返回结果。 其他类型的自定义表没有变化。 新增/修改的屏幕： **分析 > 高级 > 自定义表**上的“表”选项 平台： 管理中心
删除和删除所有连接事件的功能	6.6	任意	删除和全部删除按钮已从连接事件表页面中删除。 要清除所有连接事件，请参阅 数据清除和存储，第 495 页。 新增/修改的屏幕： **分析 > 连接 > 事件** 平台： 管理中心

功能	最低 管理中心	最低 威胁防御	详情
VRF 和 SGT 的新字段	6.6	任意	• 入口虚拟路由器（系统日志：IngressVRF） • 出口虚拟路由器（系统日志：EgressVRF） • DestinationSecurityGroupType （仅限系统日志） • SourceSecurityGroupType （仅限系统日志）
新增和更改的安全组标记字段	6.5	任意	管理中心 Web 界面中的字段更改： • 更改的字段：安全组标记现在是源 SGT • 新字段：目标 SGT 对系统日志字段的更改： • 更改的字段： SecurityGroup 现在是 SourceSecurityGroupTag • 新字段： • SourceSecurityGroup • DestinationSecurityGroup • DestinationSecurityGroupTag 支持的平台： 管理中心、托管设备
新系统日志字段：事件优先级	6.5	任意	当连接事件与入侵、文件、恶意软件或安全情报事件相关联时，该字段将它们标识为高优先级。
系统日志中连接事件的唯一标识符	6.4.0.4	任意	以下系统日志字段共同唯一标识连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。



第 33 章

入侵事件

以下主题介绍如何处理入侵事件。

关于入侵事件

Firepower 系统可以帮助监控网络中可能影响主机及其数据的可用性、完整性和机密性的流量。通过将受管设备放在关键网段，可以检查流经网络的数据包是否包含恶意活动。系统通过使用多种机制查找攻击者开发的众多漏洞。

如果系统识别出潜在的入侵，会生成入侵事件（有时以传统术语称为“IPS 事件”）；入侵事件是有关攻击源和攻击目标的日期、时间、漏洞类型以及情境信息的记录。对于基于数据包的事件，还会记录触发事件的一个或多个数据包的副本。受管设备将其事件传输到Cisco Secure Firewall Management Center，在其中可以查看汇聚数据并更好地了解针对网络资产的攻击。

还可以将受管设备部署为内联式、交换式或路由式入侵系统，以便将设备配置为会丢弃或替换已知有害的数据包。

用于查看和评估入侵事件的工具

您可以使用以下工具复审入侵事件和评估其在网络环境与安全策略情境中是否重要所需的工具。

- 事件摘要页面，提供受管设备上当前活动的概览。

- 基于文本的报告和图表报告，可以针对所选的任何时间段生成此类报告；还可以自行设计报告并将其配置为按预定的时间间隔运行
- 事故处理工具，可用于收集与攻击相关的事件数据；还可以添加备注来帮助跟踪调查和响应
- 自动报警，可用于配置 SNMP、邮件和系统日志
- 可用于响应和处理特定入侵事件的自动关联策略
- 预定义和自定义工作流程，可用于向下钻取数据以识别要进一步调查的事件
- 用于管理和分析数据的外部工具。您可以使用系统日志或 eStreamer将数据发送到这些工具。有关详细信息，请参阅 使用外部工具的事件分析，第 597 页

此外，您还可以使用 **分析 > 高级 > 上下文交叉启动** 页面上的预定义资源等公开信息来了解有关恶意实体的详细信息。

要搜索特定消息字符串并检索生成事件的规则的文档，请参阅 https://www.snort.org/rule_docs/。

入侵事件的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵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
- 入侵管理员 (Intrusion Admin)

查看入侵事件

可以查看入侵事件来确定其是否会对网络安全构成威胁。

初始入侵事件视图因用于访问页面的工作流程而异。可以使用其中一个预定义工作流程（其中包括一个或更多向下展开页面、入侵事件表视图和一个终止数据包视图），或者也可以创建自己的工作流程。还可以查看基于自定义表的工作流程，该表可能包括入侵事件。

如果事件视图包含大量 IP 地址且已启用**解析 IP 地址 (Resolve IP Addresses)** 事件视图设置，事件视图可能显示得很慢。

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**分析** > **入侵** > **事件**。

步骤 2 有以下选项可供选择：

- 调整时间范围 - 如更改时间窗口，第 661 页中所述，调整事件视图的时间范围。
- 更改工作流程 - 如果使用的是不包含入侵事件表视图的自定义工作流程，请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])** 以选择系统提供的任意工作流程。
- 限制 - 要将视图缩小至对分析非常重要的入侵事件，请参阅使用入侵事件工作流程，第 769 页。
- 删除事件 - 要从数据库删除事件，请点击**删除 (Delete)** 删除您正查看其数据包的事件，或点击**全部删除 (Delete All)** 删除您之前已选择其数据包的所有事件。
- 标记为“已审核” - 要将入侵事件标记为“已审核”，请参阅将入侵事件标记为“已审核”，第 765 页。
- 查看连接数据 - 要查看与入侵事件关联的连接数据，请参阅查看与入侵事件关联的连接数据，第 764 页。
- 查看内容 - 如入侵事件字段，第 752 页中所述，查看表中各列的内容。

相关主题

使用入侵事件数据包视图，第 772 页

关于入侵事件字段

如果系统识别出潜在的入侵，会生成入侵事件；入侵事件是有关攻击源和攻击目标的日期、时间、漏洞类型以及情境信息的记录。对于基于数据包的事件，还会记录触发事件的一个或多个数据包的副本。

您可以在 Cisco Secure Firewall Management Center Web 界面中通过路径**分析** > **入侵** > **事件**来查看入侵事件数据，或者将某些字段中的数据作为系统日志消息发出以供外部工具使用。系统日志字段如下方列表所示；没有所列的系统日志等同项的字段在系统日志消息中不可用。

搜索入侵事件时，请记住任何单独事件的可用信息视系统记录事件的方式、原因和时间而异。例如，只有加密流量上触发的入侵事件才包含 TLS/SSL 信息。

注释 在 Cisco Secure Firewall Management Center Web 界面中，入侵事件表视图内的一些字段默认被禁用。要在会话期间启用某个字段，请展开搜索限制条件，然后点击**已禁用列 (Disabled Columns)** 下的列名。

入侵事件字段

访问控制策略（系统日志：**ACPolicy**）

与启用了生成事件的入侵规则、预处理器规则或解码器规则的入侵策略相关联的访问控制策略。

访问控制规则 (系统日志： **AccessControlRuleName)**

调用生成事件的入侵策略的访问控制规则。`Default Action` 指示启用了规则的入侵政策未与特定访问控制规则相关联，而是配置为访问控制策略的默认操作。

如果存在以下情况，则此字段为空 （对于系统日志消息，则为省略）：

- 无关联规则/默认操作：如果入侵检测未关联访问控制规则或默认操作，例如，例如数据包已经过默认入侵策略检查的情况，系统才会决定应用哪条入侵检测规则。（此策略在访问控制策略的“高级”选项卡中指定。）
- 无关联的连接事件：如果对会话记录的连接事件已从数据库中清除，例如连接事件的周转高于入侵事件的情况。

应用协议（系统日志：**ApplicationProtocol**）

表示在触发入侵事件的流量中检测到的主机之间的通信的应用协议（如果可用）。

应用协议类别和标记 (Application Protocol Category and Tag)

展示了应用特征的条件条件，协助您了解应用功能。

应用风险

与在触发入侵事件的流量中检测到的应用相关联的风险：“非常高”(Very High)、“高”(High)、“中”(Medium)、“低”(Low) 或“非常低”(Very Low)。在连接中检测的各种类型的应用都有相关的风险；此字段显示当中的最高风险。

业务相关性

与在触发入侵事件的流量中检测到的应用相关联的业务关联性：“非常高”(Very High)、“高”(High)、“中”(Medium)、“低”(Low) 或“非常低”(Very Low)。连接中检测的各类应用都有相关业务；此字段显示当中最低（相关性最小）的业务相关性。

分类 (系统日志：Classification)

生成事件的规则所属的分类。

请参阅 入侵事件详细信息中的可能分类值列表。

当搜索此字段时，请为生成要查看的事件的规则输入分类编号，或者全部或部分分类名称或说明。也可以输入编号、名称或描述的以逗号分隔列表。最后，如果添加自定义分类，还可以使用其完整或部分名称或描述进行搜索。

客户端（系统日志：Client）

客户端应用（如果有），代表在触发入侵事件的流量中检测到的受监控主机上运行的软件。

客户端类别和标记 (Client Category and Tag)

展示了应用特征的条件，协助您了解应用功能。

连接计数器 （仅限系统日志）

区分一个连接与另一个同时连接的计数器。此字段本身没有意义。

以下字段共同唯一地标识与特定入侵件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

连接实例 ID （仅限系统日志）

处理连接事件的 Snort 实例。此字段本身没有意义。

以下字段共同唯一地标识与特定入侵件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

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。此字段不可搜索。

CVE ID

此字段仅为搜索字段。

按与 MITRE 常见漏洞和披露 (CVE) 数据库 (https://cve.mitre.org/) 中漏洞相关联的标识号进行搜索。

目的地所在的大洲

入侵事件中涉及的接收主机所在的大洲。

目的地国家/地区

入侵事件中涉及的接收主机所在的国家/地区。

目标主机重要性

生成事件时的目标主机重要性（相应主机的“主机重要性”属性的值）。

请记住，当主机的重要性发生变化时，此字段不会更新。但是，新事件将具有新的重要性值。

目标 IP（系统日志：DstIP）

入侵事件中涉及的接收主机使用的 IP 地址。

另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明，第 733 页。

目标端口/ICMP 代码（系统日志：DstPort、ICMPCode）

接收流量的主机的端口号。对于 ICMP 流量，在没有端口号的情况下，此字段显示 ICMP 代码。

目标用户

与连接事件的响应方 IP 关联的用户名。此主机可能是也可能不是接收漏洞攻击的主机。此值通常仅为您的网络中的用户所知。

。

另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明，第 733 页。

设备

已部署访问控制策略的受管设备。

DeviceUUID （仅限系统日志）

生成事件的 Firepower 设备的唯一标识符。

以下字段共同唯一地标识与特定入侵件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

域

检测到入侵的设备的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

出口接口（系统日志：EgressInterface）

触发事件的数据包的出口接口。对于被动接口，不填充此接口列。

出口安全区域（系统日志：EgressZone）

触发事件的数据包的出口安全区域。在被动部署中不填充此安全区域字段。

出口虚拟路由器

在使用虚拟路由的网络中，用于流量离开网络的虚拟路由器的名称。

电子邮件附件

提取自“MIME 内容性质”报头的 MIME 附件文件名。要显示附件文件名，必须启用 SMTP 预处理器的**记录 MIME 附件名称 (Log MIME Attachment Names)** 选项。支持多个附件文件名。

邮件报头

此字段仅为搜索字段。

提取自邮件报头的数据。

要将邮件报头与 SMTP 流量的入侵事件相关联，必须启用 SMTP 预处理器 **Log Headers** 选项。

邮件收件人 (Email Recipient)

提取自 SMTP RCPT TO 命令的邮件收件人的地址。要显示此字段的值，必须启用 SMTP 预处理器的**记录收件人地址 (Log To Addresses)** 选项。支持多个收件人地址。

邮件发件人 (Email Sender)

提取自 SMTP MAIL FROM 命令的邮件发件人的地址。要显示此字段的值，必须启用 SMTP 预处理器的**记录发件人地址 (Log From Addresses)** 选项。支持多个发件人地址。

第一个数据包时间 （仅限系统日志）

系统遇到第一个数据包的时间。

以下字段共同唯一地标识与特定入侵件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

发电机

生成事件的组件。

另请参阅有关以下入侵事件字段的信息：GID、消息和 Snort ID。

GID（仅限系统日志）

生成器 ID；生成事件的组件 ID。

另请参阅有关以下入侵事件字段的信息：生成器、消息和 Snort ID。

HTTP 主机名 (HTTP Hostname)

提取自 HTTP 请求主机报头的主机名（如果有）。请注意，请求数据包并非总是包含主机名。

要将主机名与 HTTP 客户端流量的入侵事件相关联，必须启用 HTTP 检查预处理器 **Log Hostname** 选项。

在表视图中，此列显示提取的主机名的前50个字符。将光标悬停在缩写主机名的显示部分上可显示完整名称（最多包含 256 个字节）。还可以在数据包视图中显示完整主机名（最多包含 256 个字节）。

HTTP 响应代码（系统日志：HTTPResponse）

在对客户端的 HTTP 请求的响应中通过触发事件的连接发送的 HTTP 状态代码。

HTTP URI

与触发入侵事件的 HTTP 请求数据包相关的原始 URI（如果有）。请注意，请求数据包并非总是包含 URI。

要将 URI 与 HTTP 客户端流量的入侵事件相关联，必须启用 HTTP 检查预处理器 **Log URI** 选项。

要查看与 HTTP 响应触发的入侵事件相关的 HTTP URI，应配置 **Perform Stream Reassembly on Both Ports** 选项中的 HTTP 服务器端口；但请注意，这样会增加流量重组的资源需求。

此列显示提取的 URI 的前五十个字符。将光标悬停在缩写 URI 的显示部分上可显示完整 URI（最多包含 2048 个字节）。还可以在数据包视图中显示完整 URI（最多包含 2048 个字节）。

影响

此字段中的影响级别指示入侵数据、网络发现数据和漏洞信息之间的相关性。

当搜索此字段时，请勿指定影响图标颜色或部分字符串。例如，请勿使用 **blue**、**level 1** 或 **0**。不区分大小写的有效值为：

- 影响 0，影响级别 0
- 影响 1，影响级别 1
- 影响 2，影响级别 2
- 影响 3，影响级别 3
- 影响 4，影响级别 4

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。

入口接口（系统日志：IngressInterface）

触发事件的数据包的入口接口。对于被动接口，仅填充此接口列。

入口安全区域（系统日志：IngressZone）

触发事件的数据包的入口安全区域或隧道区域。在被动部署中仅填充此安全区域字段。

入口虚拟路由器

在使用虚拟路由的网络中，用于流量进入网络的虚拟路由器的名称。

内联结果（系统日志：InlineResult）

在工作流程和表视图中，此字段显示以下其中一项：

表 *108:* 工作流程和表视图中的内联结果字段内容

此图标	表明
	系统已丢弃触发规则的数据包。
	如果已启用入侵策略选项 **内联时丢弃** （在内联部署中），或在系统进行修建时“丢弃并生成”规则生成了该事件，那么 IPS 应该已丢弃该数据包。
	IPS 可能已将数据包传输或传送到目的地，但包含此数据包的连接现在已被阻止。
无图标（空）	触发的规则未设置为“丢弃并生成事件”

下表列出了内联结果的可能原因 - 已丢弃和部分丢弃。

内联结果	原因	详细原因
会丢弃	被动或分流模式下的接口	您已将接口配置为内联分流或被动模式。
	“检测”检测模式下的入侵策略	您已将入侵策略中的检测模式设置为检测。
	连接超时	由于 TCP/IP 连接超时，Snort 检测引擎已暂停检测。
部分丢弃	已关闭连接 (0x01)	在创建新流时，如果分配的流数超过允许的流数，Snort 检测引擎会删除最近最少使用的流。
	已关闭连接 (0x02)	当重新加载 Snort 检测引擎导致内存调整时，引擎会删除最近最少使用的数据流。
	连接已关闭 (0x04)	当 Snort 检测引擎正常关闭时，引擎会清除所有活动数据流。

无论入侵策略的规则状态或内联丢弃行为如何（包括当内联接口处于分流模式的情况），系统在被动部署中都不会丢弃数据包。

当搜索此字段时，请输入以下任一项：

- **已丢弃** 用于指定在内联部署中是否丢弃数据包。
- **会丢弃** 用于指定当入侵策略设置为在内联部署中丢弃数据包时是否已丢弃数据包。
- **部分丢弃** 用于指定数据包是否已传输或传送到目的地，但包含此数据包的连接现在已被阻止。

入侵策略 （系统日志： **IntrusionPolicy**）

启用了生成事件的入侵规则、预处理器规则或解码器规则的入侵策略。可以选择入侵策略作为访问控制策略的默认操作，也可以将入侵策略与访问控制规则相关联。

IOC（系统日志：**NumIOC**）

触发入侵事件的流量是否也触发了危害表现 (IOC)。

当搜索此字段时，请指定 **`triggered`** 或 **`n/a`**。

消息（系统日志：**Message**）

事件的说明文本。对于基于规则的入侵事件，事件消息提取自规则。对于基于解码器和预处理器的事件，事件消息采用硬编码。

生成器和 Snort ID（GID 和 SID）与 SID 版本（修订版本）以冒号分隔的数字格式括于括号中（GID:SID:版本）附于其后。例如，**`(1:36330:2)`**。

MITRE

您可以点击以显示 MITRE 战术和层次结构中的技术的完整列表的模式计数。

MPLS 标签（系统日志：**MPLS_Label**）

与触发入侵事件的数据包相关联的多协议标签交换标签。

网络分析策略（系统日志：**NAPPolicy**）

与事件生成相关联的网络分析策略（如果有）。

此字段显示提取的 URI 的前五十个字符。将光标悬停在缩写 URI 的显示部分上可显示完整 URI（最多包含 2048 个字节）。还可以在数据包视图中显示完整 URI（最多包含 2048 个字节）。

原始客户端 IP

提取自 X-Forwarded-For (XFF)、True-Client-IP 或自定义的 HTTP 报头的原始客户端 IP 地址。

要显示此字段的值，必须在网络分析策略中启用 HTTP 预处理器的**提取原始客户端 IP 地址 (Extract Original Client IP Address)** 选项。或者，在网络分析策略的同一区域，还可以指定最多六个自定义客户端 IP 报头，并设置系统选择“原始客户端 IP 事件”(Original Client IP event) 字段值的优先顺序。

优先级（系统日志：**Priority**）

事件优先级由Talos 情报小组 确定。优先级对应于 `priority` 关键字的值或 `classtype` 关键字的值。对于其他入侵事件，优先级由解码器或预处理器决定。有效值为“高”(high)、“中”(medium) 和“低”(low)。

协议（系统日志：**Protocol**）

在 Cisco Secure Firewall Management Center Web 界面中，此字段仅为搜索字段。

连接中使用的传输协议的名称或编号，如 http://www.iana.org/assignments/protocol-numbers 中所列。这是与源端口和目标端口/ICMP 列相关的协议。

审核者 (Reviewed By)

审核事件的用户的名称。当搜索此字段时，可以输入 **unreviewed** 以搜索尚未审核的事件。

修订版本（仅限系统日志）

用于生成事件的签名的版本。

另请参阅有关以下入侵事件字段的信息：生成器、GID、消息、SID 和 Snort ID。

规则组

非 MITRE 规则组的计数，您可以点击该计数以调出模式，其中显示规则组的完整列表。

安全情景（系统日志：Context）

识别流量通过的虚拟防火墙组的元数据。系统仅对多情景模式下的 ASA FirePOWER 填充此字段。

SID（仅限系统日志）

生成事件的规则的签名 ID（亦称 Snort ID）。

另请参阅有关以下入侵事件字段的信息：生成器、GID、消息、修订版本和 Snort ID。

Snort ID

此字段仅为搜索字段。

（对于系统日志字段，请参阅 SID。）

在执行搜索时：指定生成事件的规则的 Snort ID (SID)，或者指定规则的生成器 ID (GID) 和 SID 组合，其中 GID 和 SID 使用冒号 (:) 隔开，格式为 GID:SID。可指定下表中的任何值：

表 *109: Snort ID* 搜索值

值	示例
单个 SID	10000
SID 范围	10000-11000
大于某个 SID	>10000
大于或等于某个 SID	>=10000
小于某个 SID	<10000
小于或等于某个 SID	<=10000
以逗号分隔的 SID 值列表	10000,11000,12000

值	示例
单个 GID:SID 组合	1:10000
以逗号分隔的 GID:SID 组合列表	1:10000,1:11000,1:12000
以逗号分隔的 SID 和 GID:SID 组合列表	10000,1:11000,12000

您查看的事件的SID在“消息”(Message)列中列出。有关详细信息，请参阅此部分中有关“消息”字段的说明。

源大洲

入侵事件中涉及的发送主机所在的大洲。

源国家/地区

入侵事件中涉及的发送主机所在的国家/地区。

源主机重要性

生成事件时的源主机重要性（相应主机的“主机重要性”属性的值）。

请记住，当主机的重要性发生变化时，此字段不会更新。但是，新事件将具有新的重要性值。

源 IP（系统日志：SrcIP）

入侵事件中涉及的发送主机使用的 IP 地址。

另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明，第 733 页。

源端口/ICMP 类型（系统日志：SrcPort、ICMPType）

发送主机上的端口号。对于 ICMP 流量，在没有端口号的情况下，此字段显示 ICMP 类型。

源用户（系统日志：User）

与发起连接的主机（可能是也可能不是漏洞攻击的源主机）的IP地址相关联的用户名。此用户值通常只有您的网络上的用户知道。

如果适用，用户名前面会附加 <区域>\。

SSL 实际操作（系统日志：SSLActualAction）

在 Cisco Secure Firewall Management Center Web 界面中，此字段仅为搜索字段。

系统应用于已加密流量的操作：

阻止/阻止并重置

表示阻止的加密连接。

解密（重新签名）

表示使用重新签名的服务器证书解密的传出连接。

解密（替换密钥）

表示使用具有替代公钥的自签名服务器证书解密的传出连接。

解密（已知密钥）

表示使用已知私钥解密的传入连接。

默认操作

表示连接采用默认操作处理。

不解密

表示系统未解密的连接。

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL 证书信息

此字段仅为搜索字段。

用于加密流量的公钥证书上存储的信息，包括：

- 使用者/颁发者公用名称
- 使用者/颁发者组织
- 使用者/颁发者单位
- 无效时间
- 序列号
- 证书指纹
- 公钥指纹

SSL 失败原因

此字段仅为搜索字段。

系统无法解密已加密流量的原因：

- 未知
- 不匹配
- 成功
- 未缓存的会话
- 未知加密套件

- 不受支持的加密套件
- 不支持的 SSL 版本
- 使用了 SSL 压缩
- 会话在被动模式下无法解密
- 握手错误
- 解密错误
- 挂起的服务器名称类别查找
- 挂起的公用名类别查找
- 内部错误 (Internal Error)
- 网络参数不可用
- 服务器证书处理无效
- 服务器证书指纹不可用
- 无法缓存使用者 DN
- 无法缓存颁发者 DN
- 未知的 SSL 版本
- 外部证书列表不可用
- 外部证书指纹不可用
- 内部证书列表无效
- 内部证书列表不可用
- 内部证书不可用
- 内部证书指纹不可用
- 服务器证书验证不可用
- 服务器证书验证失败
- 无效操作

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL 状态

与记录加密连接的 **SSL 实际操作** （解密规则、默认操作或无法解密的流量操作）关联的操作。

如果系统无法解密已加密连接，则其会显示所采取的 **SSL 实际操作 (SSL Actual Action)**（无法解密的流量操作）以及 **SSL 失败原因 (SSL Failure Reason)**。例如，如果系统检测到使用未知密码套件加

密的流量并且未做进一步检查即允许了该流量，则此字段显示 `Do Not Decrypt (Unknown Cipher Suite)`。

点击 **锁图标** 可查看证书详细信息。

当搜索该字段时，请输入一个或多个 **SSL 实际操作 (SSL Actual Action)** 和 **SSL 失败原因 (SSL Failure Reason)** 值以查看系统处理或无法解密的已加密流量。

SSL 使用者/颁发者所在国家/地区

此字段仅为搜索字段。

与加密证书关联的使用者或颁发者所在国家/地区的双字符 ISO 3166-1 alpha-2 国家/地区代码。

时间

事件的日期和时间。此字段不可搜索。

VLAN ID（系统日志：VLAN_ID）

与触发入侵事件的数据包相关的最内部的 VLAN ID。

Web 应用（系统日志：WebApplication）

Web 应用，代表在触发入侵事件流量中检测到的 HTTP 流量的内容或请求的 URL。

如果系统检测到 HTTP 应用协议，但无法检测特定 Web 应用，则系统会另行提供通用 Web 浏览名称。

Web 应用类别和标记 (Web Application Category and Tag)

展示了应用特征的条件，以帮助您了解应用功能。

相关主题

事件搜索，第 671 页

入侵事件影响级别

为了帮助评估事件对网络的影响，Cisco Secure Firewall Management Center在入侵事件的表视图中显示影响级别。对于每一个事件，系统都会添加影响级别图标，其颜色表示入侵数据、网络发现数据和漏洞信息之间的相关性。

注释 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。

下表介绍了影响级别的可能值。

表 *110:* 影响级别

影响级别 (Impact Level)	漏洞	颜色	说明
未知 （0）	未知	灰色	源主机和目标主机都不在由网络发现监控的网络上。
易受攻击 （1）	较弱	红色	可以为以下任意一项： • 源主机或目标主机在网络映射中，并且漏洞已映射到主机 • 源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。
可能易受攻击 （2）	可能易受攻击	橙色	源主机或目标主机在网络映射中，并且下列情况之一属实： • 对于面向端口的流量，端口正在运行服务器应用协议 • 对于非面向端口的流量，主机使用此协议
当前不易受攻击 （3）	当前不易受攻击	黄色	源主机或目标主机在网络映射中，并且下列情况之一属实： • 对于面向端口的流量（例如 TCP 或 UDP），端口不处于打开状态 • 对于非面向端口的流量（例如 ICMP），主机不使用此协议
未知目标 （4）	未知目标	蓝色	源主机或目标主机在受监控网络上，但网络映射中没有该主机的条目。

查看与入侵事件关联的连接数据

系统可以记录在其中检测到入侵事件的连接。虽然会对与访问控制规则关联的入侵策略自动执行这种记录，但必须手动启用连接记录才能查看与默认操作关联的连接数据。

在事件的表视图之间导航时，查看相关数据最有用。

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**分析** > **入侵** > **事件**。

步骤 2 使用表中的复选框选择入侵事件，然后从**跳转至**下拉列表中选择**连接**。

提示 可以使用类似方法查看与特定连接相关的入侵事件。有关详细信息，请参阅 工作流程间导航，第 666 页。

相关主题

允许连接的日志记录，第 704 页
使用入侵事件工作流程，第 769 页
使用连接和 安全相关连接 事件表，第 741 页

将入侵事件标记为“已审核”

如果确信入侵事件不是恶意的，可以将其标记为“已审核”。

如果检查了某个入侵事件并确信其不对网络安全构成威胁（例如，因为您知道网络中的所有主机均不易受检测到的漏洞攻击），那么可以将事件标记为“已审核”。已审核事件存储在数据库中并包括在事件摘要统计信息中，但不再显示在默认入侵事件页面中。您的姓名会作为审核者显示。

在多域部署中，如果将事件标记为“已审核”，则系统会在可以查看该事件的所有域中将其标记为“已审核”。

如果执行备份然后删除已审核的入侵事件，恢复备份会恢复已删除的入侵事件，但不能恢复其“已审核”状态。应在**入侵事件 (Intrusion Events)** 下，而不是在**已审核事件 (Reviewed Events)** 下查看这些恢复的入侵事件。

过程

在显示入侵事件的页面上，您有两个选择：

- 要标记事件列表中的一个或多个入侵事件，请选择事件旁边的复选框并点击**审核 (Review)**。
- 要标记事件列表中的所有入侵事件，请点击 **Review All**。

相关主题

使用入侵事件工作流程，第 769 页

查看之前已审核的入侵事件

在多域部署中，如果将事件标记为“已审核”，则系统会在可以查看该事件的所有域中将其标记为“已审核”。

过程

步骤 1 选择**分析** > **入侵** > **已审核事件**。

步骤 2 有以下选项可供选择：

- 调整时间范围，如更改时间窗口，第 661 页中所述。
- 如果使用的是不包含入侵事件表视图的自定义工作流程，请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])** 以选择系统提供的任意预定义工作流程。
- 要了解有关显示的事件的详细信息，请参阅入侵事件字段，第 752 页。

相关主题

使用入侵事件工作流程，第 769 页

将已审核的入侵事件标记为“未审核”

可以将已审核的事件返回到默认入侵事件视图，方法是将该事件标记为“未审核”。

在多域部署中，如果将事件标记为“已审核”，则系统会在可以查看该事件的所有域中将其标记为“已审核”。

过程

在显示已审核事件的页面上，您有两个选择：

- 要删除已审核事件列表中的单个入侵事件，请选中特定事件旁边的复选框并点击**取消审核 (Unreview)**。
- 要从已审核事件列表移除所有入侵事件，请点击 **Unreview All**。

预处理器事件

预处理器提供两项功能：对数据包执行指定操作（例如解码和规范化 HTTP 流量）；一旦数据包触发某个预处理器选项且相关预处理器规则处于启用状态，就会通过生成事件来报告指定预处理器选项的执行情况。例如，您可以用 HTTP 检查生成器 (GID) 119 和 Snort ID (SID) 2 来启用 `Double Encoding` HIIP 检查选项及相关的预处理器规则，以在预处理器遇到 IIS 双编码流量时生成事件。

生成事件来报告预处理器的执行情况有助于检测异常协议漏洞攻击。例如，攻击者可以制造重叠的 IP 片段来对主机进行 DoS 攻击。IP 分片重组预处理器可以检测此类攻击并为之生成入侵事件。

预处理器事件与规则事件的不同之处在于，数据包显示不包含对事件的详细规则说明。相反，数据包显示的是事件消息、GID、SID、数据包报头数据和数据包负载。这让您可以分析数据包的报头信息，确定数据包的报头选项是否正在使用以及它们是否会令系统出现漏洞，并检查数据包负载。预

处理器分析每个数据包后，规则引擎对其执行适当的规则（如果预处理器能够整理数据包并将其作为有效会话的一部分），进一步分析潜在内容级别的威胁并提供相关报告。

预处理器生成器 ID

每个预处理器都有自己的生成器 ID（即 GID），用以指明数据包触发的是哪个预处理器。某些预处理器还具有相关 SID，这是用于对潜在攻击进行分类的 ID 编号。这有助于通过对事件类型进行分类来更有效地分析事件，就像规则的 Snort ID (SID) 可以提供数据包触发规则的情景一样。可以在入侵策略“规则”页面的“预处理器”筛选组中按预处理器列出预处理器规则；还可以在“类别”筛选组的预处理器和数据包解码器子组中列出预处理器规则。

注释 由标准文本规则生成的事件的生成器 ID 为 1（全局域或旧式 GID）或 1000-2000（子代域）。对于共享对象规则，事件的生成器 ID 为 3。对于二者，事件的 SID 指明触发的是哪条具体规则。

下表介绍了生成每个 GID 的事件的类型。

表 *111:* 生成器 *ID*

ID	组件	说明
1	标准文本规则	该事件是在数据包触发标准文本规则 （全局域或旧式 GID）时生成的。
2	标记的数据包	事件由标记生成器生成（标记生成器会根据带标记会话生成数据包）。使用 `tag` 规则选项时会出现这种情况。
3	共享对象规则	在数据包共享对象规则时生成事件。
102	HTTP 解码器	解码器引擎解码数据包中的 HTTP 数据。
105	Back Orifice 检测器	Back Orifice 检测器识别与数据包关联的 Back Orifice 攻击。
106	RPC 解码器	RPC 解码器解码数据包。
116	数据包解码器	事件由数据包解码器生成。
119、120	HTTP 检查预处理器	事件由 HTTP 检查预处理器生成。GID 120 规则与服务器特定 HTTP 流量相关。
122	端口扫描检测器	事件由端口扫描流量检测器生成。
123	IP 分片重组器	分片的 IP 数据报不能正确重组时生成事件。
124	SMTP 解码器	SMTP 预处理器检测到针对 SMTP 谓词的漏洞时生成事件。
125	FTP 解码器	FTP/Telnet 解码器检测到 FTP 流量中有漏洞时生成事件。
126	Telnet 解码器	FTP/Telnet 解码器检测到 Telnet 流量中有漏洞时生成事件。
128	SSH 预处理器	SSH 预处理器检测到 SSH 流量中的漏洞时生成事件。

ID	组件	说明
129	流预处理器	在数据流预处理器对数据流进行预处理期间生成事件。
131	DNS 预处理器	事件由 DNS 预处理器生成。
133	DCE/RPC 预处理器	事件由 DCE/RPC 预处理器生成。
134	规则延迟 数据包延迟	规则延迟暂停 (134:1) 或重新启用 (134:2) 一组入侵规则时，或者由于超出数据包延迟阈值而使系统停止检查数据包 (134:3) 时，生成事件。
135	基于速率的攻击检测器	基于速率的攻击检测器识别到网络上的主机存在过多连接时生成事件。
137	SSL 预处理器	事件由 TLS/SSL 预处理器生成。
138、139	敏感数据预处理器	事件由敏感数据预处理器生成。
140	SIP 预处理器	事件由 SIP 预处理器生成。
141	IMAP 预处理器	事件由 IMAP 预处理器生成。
142	POP 预处理器	事件由 POP 预处理器生成。
143	GTP 预处理器	事件由 GTP 预处理器生成。
144 个	Modbus 预处理器	事件由 Modbus SCADA 预处理器生成。
145	DNP3 预处理器	事件由 DNP3 SCADA 预处理器生成。
148	CIP 预处理器	事件由 CIP SCADA 预处理器生成。
149	S7Commplus 预处理器	事件由 S7Commplus SCADA 预处理器生成。
1000 - 2000	标准文本规则	在数据包触发标准文本规则（子代域）时生成事件。

入侵事件工作流程页面

如果监控的流量违反策略，当前入侵策略中启用的预处理器规则、解码器规则和入侵规则就会生成入侵事件。

Firepower 系统提供使用事件数据填充的一组预定义工作流程，可用于查看和分析入侵事件。这些工作流程中，每个都会引导您浏览一系列页面，从而帮助您确定要评估的入侵事件。

预定义的入侵事件工作流程包含三种不同类型的页面（又称为事件视图）：

- 一个或多个向下钻取页面
- 入侵事件的表视图

- 数据包视图

向下钻取页面通常在一个表中包含两列或更多列（对于某些向下钻取视图，有多个表），通过其可查看一种特定类型的信息。

“向下钻取”以查找有关一个或多个目标端口的详细信息时，将会自动选择这些事件，然后显示工作流程中的下一页。这样，向下展开表就能够帮助减少一次分析的事件数。

入侵事件的初始表视图在其各自的行中列出每个入侵事件。表中的各列列出各种信息，例如时间、源 IP 地址、源端口、目标 IP 地址、目标端口、事件优先级和事件消息，等等。

在表视图中选择事件时，可以先不选择事件并显示工作流程中的下一页，而是为事件添加限制条件。限制条件是对要分析的事件类型施加的限制。

例如，如果点击任何列中的 **关闭**（×） 并从下拉列表清除 **时间** ，可以将“时间”作为一列移除。要减少分析中事件列表的事件数，可以点击表视图任一行中某个值的链接。例如，要将分析范围缩小为从其中一个源 IP 地址（假设是潜在攻击者）生成的事件，请点击**源 IP 地址 (Source IP Address)** 列中的 IP 地址。

如果选择表中的一行或多行，然后点击**视图 (View)**，将会显示数据包视图。数据包视图提供有关触发生成事件的规则或预处理器的数据包的信息。数据包视图的每个部分都包含有关数据包中特定层的信息。您可以展开折叠的部分以了解详细信息。

注释 由于每个端口扫描事件均由多个数据包触发，因此端口扫描事件会使用特殊版本的数据包视图。

如果预定义工作流程无法满足您的特定需求，则您可以创建仅显示您感兴趣的信息的自定义工作流程。自定义入侵事件工作流程可以包含向下钻取页面和/或事件表视图；系统自动将数据包视图包含作为最后一页。根据调查事件的需要，您可以轻松地在预定义工作流程和自定义工作流程之间切换。

使用入侵事件工作流程

事件的下钻式视图和表视图共享一些常见功能，这些功能可用于缩小事件列表，以便将分析焦点集中到一组相关事件上。

为了避免在不同的工作流程页面上显示相同的入侵事件，当您点击位于页面底部的链接显示另一页事件时，事件范围会暂停；当您在后续页面上点击以执行任何其他操作时，事件范围将会继续。

提示 在操作过程中，可以随时将限制条件保存为一组搜索条件。例如，如果您发现几天内您的网络被来自某个 IP 地址的攻击者探测，您可以在调查期间保存限制条件，以供日后再次使用。但是，不能将复合限制条件保存为一组搜索条件。

过程

步骤 1 使用**分析** > **入侵** > **事件**访问入侵事件工作流程。

步骤 2 或者，限制事件视图中显示的入侵事件数，如入侵事件向下钻取页面限制，第 771 页或入侵事件表视图限制，第 771 页中所述。

步骤 3 有以下选项可供选择：

- 要了解有关显示的列的详细信息，请参阅入侵事件字段，第 752 页。
- 要查看主机的配置文件，请点击显示在主机 IP 地址旁边的 **主机配置文件** 。
- 要查看地理位置详细信息，请点击“源国家/地区”或“目标国家/地区”列中显示的旗帜。
- 要查看 Firepower 系统外部可用源中的数据，请右键点击事件值。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，第 605 页
- 要收集有关事件的一般情报，请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。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，第 605 页。
- 要修改所显示事件的时间和日期范围，请参阅更改时间窗口，第 661 页。

  提示 如果入侵事件未显示在事件视图中，调整指定的时间范围可能会返回结果。建议不要指定旧的时间范围，因为旧时间范围内的事件可能已被删除。调整规则阈值配置可能生成事件。

  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段（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。

- 要在当前工作流程页面排序事件或在当前工作流程页面内导航，请参阅使用工作流程，第 642 页。
- 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- 要从事件数据库中删除事件，选中要删除的事件旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**。
- 要将事件标记为“已审核”以将其从入侵事件页面上移除，但不将其从事件数据库中移除，请参阅将入侵事件标记为“已审核”，第 765 页。
- 要下载触发每个所选事件的数据包的本地副本（libpcap 格式的数据包捕获文件），请选中由要下载的数据包触发的事件旁边的复选框，然后点击**下载数据包 (Download Packets)** 或点击**下载所有数据包 (Download All Packets)**。捕获的数据包以 libpcap 格式保存。多个常用的协议分析器均使用此格式。
- 要导航至其他事件视图以查看关联事件，请参阅工作流程间导航，第 666 页。
- 要暂时使用另一个工作流程，请点击**切换工作流 (switch workflow)**。
- 要为当前页面添加书签以便快速返回该页面，请点击**将此页面加入书签 (Bookmark This Page)**。

- 要查看“摘要”(Summary) 控制面板的“入侵事件”(Intrusion Events) 部分，请点击**控制面板 (Dashboards)**。
- 要导航至书签管理页面，请点击**查看书签 (View Bookmarks)**。
- 要根据当前视图中的数据生成报告，请参阅从事件视图创建报告模板，第 509 页。

相关主题

事件搜索，第 671 页
书签，第 667 页

入侵事件向下钻取页面限制

下表介绍如何使用向下钻取页面。

表 *112:* 限制向下钻取页面上的事件

所需的操作…	可执行的操作
向下展开到下一个工作流程页面，约束特定值	点击该值。 例如，在“目标端口”(Destination Port) 工作流程中，要将事件限制为目标端口为 80 端口的事件，请点击 **DST 端口/ICMP 代码 (DST Port/ICMP Code)** 列中的 **80/tcp**。屏幕上将会显示工作流程的下一页（“事件”[Events] 页面），其中仅包含 80/tcp 端口事件。
向下展开到下一个工作流程页面，约束选定事件	选择要在下一个工作流程页面上查看的事件旁边的复选框，然后点击**查看 (View)**。 例如，在“目标端口”(Destination Port) 工作流程中，要将事件限制为目标端口为 20/tcp 和 21/tcp 端口的事件，请选择这些端口对应行旁边的复选框，然后点击**查看 (View)**。屏幕上将会显示工作流程的下一页（“事件”[Events] 页面），其中仅包含 20/tcp 和 21/tcp 端口事件。 请注意，如果对多行施加限制，并且表具有多列（不包括“计数”[Count] 列），则会构建复合限制。复合限制可确保您限制中的事件数不会超过意欲包含的数量。例如，如果使用“事件和目标”(Event and Destination) 工作流程，在第一个向下钻取页面上选择的每一行都会创建一个复合限制条件。如果您选择的是目标 IP 地址为 10.10.10.100 的事件 1:100，同时也选择了目标 IP 地址为 192.168.10.100 的事件 1:200，则复合限制可确保您不会同时也选择事件类型为 1:100、目标 IP 地址为 192.168.10.100 的事件，或者事件类型为 1:200、目标 IP 地址为 10.10.10.100 的事件。
向下展开到下一个工作流程页面，保留当前限制	点击**查看全部 (View All)**。

入侵事件表视图限制

下表介绍如何使用表视图。

表 *113:* 限制事件表视图中的事件

所需的操作…	可执行的操作
将视图限制为仅显示具有单个属性的事件	点击该属性。 例如，要将视图限制为仅显示目标端口为 80 端口的事件，请点击 **DST 端口/ICMP 编码 (DST Port/ICMP Code)** 列中的 **80/tcp**。
从表中移除列	在要隐藏的列标题中点击 **关闭**（×）。在显示的弹出窗口中，点击 **Apply**。 如果要隐藏或显示其他列，请选择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** 以展开搜索限制条件，然后点击 **禁用列**下的列名称。
查看与一个或多个事件相关的数据包	执行以下其中一种操作： • 点击要查看的数据包的事件旁边的向下 **箭头图标** 。 • 选择要查看的一个或多个数据包，然后点击页面底部的 **View**。 • 在页面底部，点击**查看全部**以查看与当前限制条件匹配的所有事件的数据包。

使用入侵事件数据包视图

数据包视图提供有关触发生成入侵事件的规则的数据包的信息。

提示 如果用于检测事件的设备的**传输数据包**选项已禁用，则 Cisco Secure Firewall Management Center上的数据包视图不包含数据包信息。

数据包视图通过提供有关数据包触发的入侵事件的信息来指示捕获特定数据包的原因，这些信息包括事件的时间戳、消息、分类和优先级（如果事件由标准文本规则生成，则还包括生成事件的规则）。数据包视图还提供有关数据包的一般信息（例如大小）。

此外，数据包视图有一部分是介绍数据包中的每一层（数据链路层、网络层和传输层），还有一部分介绍组成数据包的字节。如果系统已解密数据包，可以查看解密的字节。可以展开折叠的部分以显示详细信息。

注释 由于每个端口扫描事件均由多个数据包触发，因此端口扫描事件会使用特殊版本的数据包视图。

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。

过程

步骤 1 在入侵事件的表视图中，选择要查看的数据包，如入侵事件表视图限制，第 771 页中所述。

步骤 2 或者，如果选择多个事件，可以使用页面底部的页码来浏览数据包视图中的数据包。

步骤 3 此时，您还有以下选择：

- 调整 - 要修改数据包视图中的日期和时间范围，请参阅更改时间窗口，第 661 页。
- 配置 - 要配置触发事件的入侵规则，请点击“操作”(Actions) 旁边的箭头，然后如在数据包视图中配置入侵规则，第 776 页中所述继续操作。
- 删除 - 要从数据库删除事件，请点击**删除 (Delete)** 以删除您正在查看其数据包的事件，或点击**全部删除 (Delete All)** 以删除您之前已选择其数据包的所有事件。
- 下载 - 要下载触发事件的数据包的本地副本（libpcap 格式的数据包捕获文件），请点击**下载数据包** 保存您正在查看的事件的已捕获数据包副本，或点击**下载所有数据包**保存您之前已选择其数据包的所有事件的已捕获数据包副本。捕获的数据包以 libpcap 格式保存。多个常用的协议分析器均使用此格式。

  注释 不能下载端口扫描数据包，因为单个端口扫描事件基于多个数据包；但端口扫描视图提供所有可用的数据包信息。要下载，必须至少有 15% 的可用磁盘空间。

- 标记为已审核 - 要将事件标记为“已审核”以从事件视图中将其移除，但不从事件数据库中移除，请点击**审核 (Review)** 以标记您正在查看其数据包的事件，或点击**全部审核 (Review All)** 以标记您之前已选择其数据包的所有事件。有关详细信息，请参阅将入侵事件标记为“已审核”，第 765 页。
- 查看其他信息 - 要展开或折叠页面部分，请点击该部分旁边的箭头。有关详细信息，请参阅事件信息字段，第 773 页、帧信息字段，第 779 页和数据链路层信息字段，第 780 页。
- 查看网络层信息 - 请参阅查看网络层信息，第 781 页。
- 查看数据包字节信息 - 请参阅查看数据包字节信息，第 786 页。
- 查看传输层信息 - 请参阅 查看传输层信息，第 783 页

相关主题

端口扫描检测

事件信息字段

在数据包视图上，可以查看有关“事件信息”部分数据包的信息。

事件

事件消息。对于基于规则的事件，这相当于规则消息。对于其他事件，这取决于解码器或预处理器。

事件 ID 以 (GID:SID:Rev) 格式附加到消息后面。GID 是生成事件的规则引擎、解码器或预处理器的生成器 ID。SID 是规则、解码器消息或预处理器消息的标识符。Rev 是规则的修订号。

时间戳

捕获数据包的时间，采用 UTC 时区。

分类

事件分类。对于基于规则的事件，这相当于规则分类。对于其他事件，这取决于解码器或预处理器。

优先级

事件优先级。对于基于规则的事件，这相当于 `priority` 关键字的值或 `classtype` 关键字的值。对于其他事件，这取决于解码器或预处理器。

入口安全区域

触发事件的数据包的入口安全区域。在被动部署中仅填充此安全区域字段。

出口安全区域

触发事件的数据包的出口安全区域。在被动部署中未填充此字段。

域

受管设备所属的域。 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

已部署访问控制策略的受管设备。

安全情景

识别流量通过的虚拟防火墙组的元数据。请注意，系统仅对多情景模式下的 ASA FirePOWER 填充此字段。

入口接口

触发事件的数据包的入口接口。对于被动接口，仅填充此接口列。

出口接口

对于内联部署，指触发事件的数据包的出口接口。

源/目标 IP

触发事件的数据包源自的（源）主机 IP 地址或域名，或触发事件的流量的目标主机（目的地）。

源端口/ICMP 类型 (Source Port/ICMP Type)

触发事件的数据包的源端口。对于 ICMP 流量，在没有端口号的情况下，系统将显示 ICMP 类型。

目标端口/ICMP 代码 (Destination Port/ICMP Code)

接收流量的主机的端口号。对于 ICMP 流量，在没有端口号的情况下，系统将显示 ICMP 代码。

邮件报头

提取自邮件报头的数据。请注意，邮件报头不显示在入侵事件表视图中，但可以将邮件报头数据作为搜索条件。

要将邮件报头与 SMTP 流量的入侵事件相关联，必须启用 SMTP 预处理器的**记录报头 (Log Headers)** 选项。对于基于规则的事件，提取邮件数据时会显示此行。

HTTP 主机名 (HTTP Hostname)

提取自 HTTP 请求主机报头的主机名（如果有）。此行显示完整的主机名（最多包含 256 个字节）。如果完整主机名不再是单行，则可以将其展开。

要显示主机名，必须启用 HTTP 检查预处理器 **Log Hostname** 选项。

请注意，HTTP 请求数据包并非总是包含主机名。对于基于规则的事件，当数据包包含 HTTP 主机名或 HTTP URI 时，会显示此行。

HTTP URI

与触发入侵事件的 HTTP 请求数据包相关的原始 URI（如果有）。此行显示完整 URI（最多包含 2048 个字节）。如果完整 URL 不再是单行，则可以将其展开。

要显示 URI，必须启用 HTTP 检查预处理器 **Log URI** 选项。

请注意，HTTP 请求数据包并非总是包含 URI。对于基于规则的事件，当数据包包含 HTTP 主机名或 HTTP URI 时，会显示此行。

要查看与 HTTP 响应触发的入侵事件相关的 HTTP URI，应配置 **Perform Stream Reassembly on Both Ports** 选项中的 HTTP 服务器端口；但请注意，这样会增加流量重组的资源需求。

入侵策略

启用了生成入侵事件的入侵规则、预处理器规则或解码器规则的入侵策略。可以选择入侵策略作为访问控制策略的默认操作，也可以将入侵策略与访问控制规则相关联。

访问控制策略

包含入侵策略（启用了生成事件的入侵规则、预处理器规则或解码器规则）的访问控制策略。

访问控制规则

与生成事件的入侵规则关联的访问控制规则。默认操作指示启用了规则的入侵策略未与访问控制规则关联，而是配置为访问控制策略的默认操作。

规则

对于标准文本规则事件，是指生成事件的规则。

请注意，如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

由于规则数据可能包含有关网络的敏感信息，管理员可以使用用户角色编辑器中的 View Local Rules 权限来设置用户查看数据包视图中的规则信息的权限。

操作

对于标准文本和自定义规则事件，展开**操作**以对触发事件的规则执行以下任何操作：

- 编辑规则
- 查看规则修订文档；仅对于标准文本规则，在“操作”下点击**查看文档**后，您可以点击文档弹出窗口中的**规则文档**以查看更具体的规则详情。
- 向规则添加注释
- 更改规则的状态
- 设置规则的阈值
- 抑制规则

请注意，如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

在数据包视图中配置入侵规则

在入侵事件的数据包视图中，可以对触发事件的规则执行几项操作。请注意，如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

过程

步骤 1 在入侵规则生成的入侵事件的数据包视图中，展开“事件信息”(Event Information) 部分的**操作 (Actions)**。

步骤 2 有以下选项可供选择：

- 注释 - 对于标准文本规则事件，点击**规则注释 (Rule Comment)** 可以向生成事件的规则添加文本注释。这样做可以提供有关规则以及其识别出的漏洞或策略违规的额外上下文和信息。还可以在入侵规则编辑器中添加和查看规则注释。
- 禁用 - 要禁用此规则，请点击以下选项之一：
  - **在当前 Snort 2 策略 (<policy_name>) 中禁用此规则**
  - **在所有本地创建的 Snort 2 策略中禁用此规则**

  如果此事件由标准文本规则生成，必要时可以禁用此规则。可以在能够在本地编辑的所有策略中设置此规则。或者，如果您能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置此规则。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认策略。

  注释 不能从数据包视图禁用共享对象规则，也不能禁用默认策略中的规则。

- 丢弃数据包并生成事件 - 要将规则设置为丢弃触发该规则的数据包并生成事件，请点击以下选项之一：
  - **设置此规则可丢弃触发数据包并在当前 Snort 2 策略 (<policy_name>) 中生成事件**
  - **设置此规则可丢弃触发数据包并在所有本地创建的 Snort 2 内联策略中生成事件**

如果受管设备在网络中以内联方式部署，可以在能够在本地编辑的所有策略中将触发事件的规则设置为丢弃触发该规则的数据包。或者，如果您能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置此规则。

请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认策略。请注意，仅在当前策略中启用了 **Drop when Inline** 的情况下，才会显示此选项。

- 编辑 - 对于标准文本规则事件，点击 **编辑** （以编辑 Snort 2 规则）或 **编辑 Snort 3 规则** 可修改生成事件的规则。如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

  注释 如果编辑由系统提供的规则（而不是自定义的标准文本规则），则实际上会创建新的本地规则。请确保将本地规则设置为生成事件，并禁用当前入侵策略中的原始规则。但请注意，不能启用默认策略中的本地规则。

- 生成事件 - 点击 **设置此规则以在所有本地创建的 Snort 2 策略中生成事件** 可将规则设置为生成事件。

  如果此事件由标准文本规则生成，则可以将规则设置为在可本地编辑的所有策略中生成事件。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认策略。

  注释 不能将共享对象规则设置为从数据包视图生成事件，也不能禁用默认策略中的规则。

- 设置抑制选项 - 展开**设置抑制选项 (Set Suppression Options)**，然后如在数据包视图中设置抑制选项，第 778 页中所述继续操作。

  可以使用此选项以在能够在本地编辑的所有策略中抑制触发此事件的规则。或者，如果能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中抑制此规则。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。

- 设置阈值选项 - 展开**设置抑制选项 (Set Thresholding Options)**，然后如在数据包视图中设置阈值选项，第 778 页中所述继续操作。

  可以使用此选项在能够在本地编辑的所有策略中为触发此事件的规则创建阈值。或者，如果能够在本地编辑当前策略，可以仅为当前策略（即，生成事件的策略）创建阈值。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认入侵策略。

- 查看文档 - 点击**查看文档**可了解有关生成事件的规则的详细信息。或者，然后点击**规则文档**来查看更具体的规则详细信息。

在数据包视图中设置阈值选项

通过在入侵事件的数据包视图中设置阈值选项，可以控制每个规则随时间推移生成的事件数。可以在能够在本地编辑的所有策略中设置阈值选项；或者，如果能够在本地编辑策略，可以仅在当前策略（即，导致事件生成的策略）中设置阈值选项。

过程

步骤 1 在入侵规则生成的入侵事件的数据包视图中，展开“事件信息”(Event Information) 部分的**操作 (Actions)**。

步骤 2 展开**设置阈值选项 (Set Thresholding Options)**，并在两个选项中选择一个：

- **在当前 Snort 2 策略 (<policy_name>)**
- **在所有本地创建的 Snort 2 策略中**

步骤 3 选择要设置的阈值的类型：

- 点击**限制 (limit)** 以将通知限制为每个时间段内仅为指定数目的事件实例提供通知。
- 点击**阈值 (threshold)** 为每个时间段内每发生指定数目的事件实例提供通知。
- 点击**两者 (both)** 则在每个时间段内事件实例数达到指定数量后提供一次通知。

步骤 4 点击相应的阈值，以指明是要按**源 (Source)** 或**目标 (Destination)** IP 地址跟踪事件实例。

步骤 5 在**计数 (Count)** 字段中，输入要用作阈值的事件实例数。

步骤 6 在**秒 (Seconds)** 字段中，输入一个 1 和 86400 之间的数字来指定跟踪事件实例的时间段。

步骤 7 如果要覆盖现有入侵策略中的规则的所有当前阈值，请选中**覆盖此规则的任何现有设置 (Override any existing settings for this rule)** 复选框。

步骤 8 点击 **Save Thresholding**。

在数据包视图中设置抑制选项

可以使用抑制选项抑制全部入侵事件，或者基于源或目标 IP 地址抑制入侵事件。可在能够在本地编辑的所有策略中设置抑制选项。或者，如果能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置抑制选项。

过程

步骤 1 在入侵规则生成的入侵事件的数据包视图中，展开“事件信息”(Event Information) 部分的**操作 (Actions)**。

步骤 2 展开**设置抑制选项 (Set Suppression Options)**，并在两个可能的选项中选择一个：

- **在当前 Snort 2 策略 (<policy_name>)**

- 在所有本地创建的 **Snort 2** 策略中

注释　仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。

步骤 3　选择以下其中一个**跟踪方式 (Track By)** 选项：

- 点击**源 (Source)** 可抑制由指定源 IP 地址发出的数据包生成的事件。
- 点击**目标 (Destination)** 可抑制由发往指定目标 IP 地址的数据包生成的事件。
- 点击**规则 (Rule)** 可完全抑制触发此事件的规则的事件。

步骤 4　在 **IP address or CIDR block** 字段中，输入要指定为源或目标 IP 地址的 IP 地址或 CIDR 块/前缀长度。

步骤 5　点击 **Save Suppression**。

相关主题

Firepower 系统 IP 地址约定，第 26 页

帧信息字段

在数据包视图中，点击**帧 (Frame)** 旁边的箭头可查看捕获的帧的信息。数据包视图可以显示单个帧或多个帧。每个帧提供有关单个网络数据包的信息。您会看到多个帧，例如，对于已标记的数据包或重组的 TCP 数据流中的数据包。

帧 n (Frame n)

捕获的帧，其中，*n* 为 1（对于单帧数据包）或递增帧编号（对于多帧数据包）。帧中捕获的字节数将附加到帧编号后面。

到达时间 (Arrival Time)

捕获帧的日期和时间。

与捕获上一个帧的时间间隔 (Time delta from previous captured frame)

对于多帧数据包，表示自捕获上一个帧以来经过的时间。

与显示上一个帧的时间间隔 (Time delta from previous displayed frame)

对于多帧数据包，表示自显示上一个帧以来经过的时间。

自引用或第一个帧以来经过的时间 (Time since reference or first frame)

对于多帧数据包，表示自捕获第一个帧以来经过的时间。

帧编号 (Frame Number)

递增的帧编号。

帧长度 (Frame Length)

帧的长度，以字节为单位。

捕获长度 (Capture Length)

捕获的帧的长度，以字节为单位。

帧标记 (Frame is marked)

帧是否被标记（true 或 false）。

帧中的协议 (Protocols in frame)

帧中包括的协议。

相关主题

tag 关键字
TCP 数据流重组

数据链路层信息字段

在数据包视图中，点击数据链路层协议（例如，**以太网 II [Ethernet II]**）旁边的箭头可查看有关数据包的数据链路层信息，这些信息包括源主机和目标主机的 48 位介质访问控制 (MAC) 地址。它还可能根据硬件协议，显示有关数据包的其他信息。

注释 请注意，本示例介绍以太网链路层信息，也可能出现其他协议。

数据包视图反映数据链路层使用的协议。以下列表说明在数据包视图中可能会看到的以太网 II 或 IEEE 802.3 以太网数据包的信息。

目标

目标主机的 MAC 地址。

注释 以太网还可以使用组播地址和广播地址作为目标地址。

来源

源主机的 MAC 地址。

类型

对于以太网 II 数据包，代表在以太网帧中封装的数据包的类型，例如 IPv6 或 ARP 数据报。请注意，此项目仅对以太网 II 数据包显示。

长度

对于 IEEE 802.3 以太网数据包，代表数据包的总长度（以字节为单位，不包括校验和）。请注意，此项目仅对 IEEE 802.3 以太网数据包显示。

查看网络层信息

过程

在数据包视图中，点击网络层协议（例如，**互联网协议**）旁边的箭头可查看有关与数据包相关的网络层的更多详细信息。

注释 请注意，本示例介绍的是 IP 数据包；也可能出现其他协议。

IPv4 网络层信息字段

以下列表介绍在 IPv4 数据包中可能显示的协议特定信息。

版本

互联网协议的版本号。

报头长度

报头（包括任何 IP 选项）中的字节数。不带选项的 IP 报头的长度为 20 字节。

差分服务字段

差分服务的值，用以指明发送主机如何支持显式堵塞通知 (ECN)：

- `0x0` - 不支持具有 ECN 功能的传输 (ECT)
- `0x1` 和 `0x2` - 支持 ECT
- `0x3` - 堵塞情况 (CE)

总长度

IP 数据包的长度（以字节为单位，不包括 IP 报头在内）。

标识

唯一标识源主机发送的 IP 数据报的值。此值用于跟踪同一数据报的数据分片。

标志

控制 IP 分片的值，其中：

“最后一个分片”(Last Fragment) 标志的值指明是否有更多与数据报相关的分片。

- 0 - 没有更多与数据报相关的分片
- 1 - 有更多与数据报相关的分片

“不分片”(Don’t Fragment) 标志的值控制数据报是否可以分片：

- 0 - 数据报可以分片
- 1 - 数据报不可分片

分片偏移量

自数据报开始以来分片偏移量的值。

生存时间 (ttl)

数据包在过期之前可以在路由器之间跳转的剩余跳数。

协议

封装在 IP 数据报中的传输协议；例如，ICMP、IGMP、TCP 或 UDP。

报头校验和

指明 IP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏或可能正被用于躲避入侵。

源/目标

源（或目标）主机的 IP 地址或域名。

请注意，要显示域名，必须启用 IP 地址解析。

点击地址或域名查看上下文菜单，然后选择 **Whois** 可在主机上执行 whois 搜索，选择 **查看主机配置文件** 可查看主机信息，或选择可将地址添加到全局黑名单或白名单。

IPv6 网络层信息字段

以下列表介绍在 IPv6 数据包中可能显示的协议特定信息。

流量类别

IPv6 报头中的试验性 8 位字段，用于识别 IPv6 数据包类别或优先级，类似于 IPv4 提供的差分服务功能。未使用时，此字段设为零。

流标签

可选的 20 位 IPv6 十六进制值（从 1 到 FFFFF），用于识别特殊流（例如，非默认服务质量或实时服务）。未使用时，此字段设为零。

负载长度

表示 IPv6 负载中八位组数的 16 位字段，负载由 IPv6 报头后面的所有数据包组成，包括任何扩展报头。

下一报头

表示紧随 IPv6 报头之后的报头类型的 8 位字段，使用与 IPv4 协议字段相同的值。

跳数限制

一个 8 位十进制整数，其中用于转发数据包的每个节点每次减 1。如果递减的值达到零，则丢弃数据包。

来源

源主机的 128 位 IPv6 地址。

目标

目标主机的 128 位 IPv6 地址。

查看传输层信息

过程

步骤 1 在数据包视图中，点击传输层协议（例如，**TCP**、**UDP** 或 **ICMP**）旁边的箭头。

步骤 2 或者，点击**数据 (Data)**（如果显示）可在紧接其上方的数据包视图的“数据包信息”(Packet Information) 部分中查看协议负载的前二十四个字节。

步骤 3 查看 TCP、UDP 和 ICMP 协议的传输层内容，如TCP 数据包视图字段，第 783 页、UDP 数据包视图字段，第 784 页或ICMP 数据包视图字段，第 785 页中所述。

注释 请注意，这些示例讨论 TCP、UDP 和 ICMP 数据包；也可能出现其他协议。

TCP 数据包视图字段

本节介绍 TCP 数据包的特定于协议的信息。

源端口

用于识别发起应用协议的编号。

目标端口

用于识别接收应用协议的编号。

序列号

当前 TCP 分段中第一个字节的值，包含在 TCP 数据流中的初始序列号中。

下一个序列号

在响应数据包中，要发送的下一个数据包的序列号。

确认号

TCP 确认，包含在之前接受的数据的序列号中。

报头长度

报头中的字节数。

标志

六位，表示 TCP 分段的传输状态：

- `U` - 紧急指针有效
- `A` - 确认号有效
- `P` - 接收方应推送数据
- `R` - 重置连接
- `S` - 同步序列号以开始新连接
- `F` - 发送方完成发送数据

窗口大小

接收主机将接受的未确认数据数量（以字节为单位）。

校验和

指明 TCP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏或可能正被用于躲避入侵。

紧急指针

TCP 分段中发送紧急数据的位置（如果存在）。与 `U` 标记一起使用。

选项

TCP 选项的值（如果有）。

UDP 数据包视图字段

本节介绍 UDP 数据包的特定于协议的信息。

源端口

用于识别发起应用协议的编号。

目标端口

用于识别接收应用协议的编号。

长度

UDP 报头和数据的总长度。

校验和

指明 UDP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏。

ICMP 数据包视图字段

本节介绍 ICMP 数据包的协议特定信息。

类型

ICMP 消息的类型：

- 0 - 回应应答
- 3 - 目的地不可达
- 4 - 源抑制
- 5 - 重定向
- 8 - 回应请求
- 9 - 路由器通告
- 10 - 路由器请求
- 11 - 超时
- 12 - 参数问题
- 13 - 时间戳请求
- 14 - 时间戳应答
- 15 - 信息请求（过时）
- 16 - 信息应答（过时）
- 17 - 地址掩码请求
- 18 - 地址掩码应答

代码

ICMP 消息类型随附的代码。ICMP 消息类型 3、5、11 和 12 都有一个相应的代码，如 RFC 792 中所述。

校验和

指明 ICMP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏。

查看数据包字节信息

过程

在数据包视图中，点击**数据包字节数 (Packet Bytes)** 旁边的箭头可查看构成数据包的字节的十六进制和 ASCII 版本。如果系统已解密流量，可以查看解密的数据包字节。

内部来源的入侵事件

来自内部源的入侵事件表示网络上的主机受到攻击。如果源 IP 地址在您的网络上，则表明您应该调查此主机。

查看入侵事件统计信息

Intrusion Event Statistics 页面提供设备当前状态和网络生成的所有入侵事件的简要摘要。

页面上显示的每个 IP 地址、端口、协议和事件消息等均为链接。点击任意链接可查看相关的事件信息。例如，如果前 10 大目标端口之一是 `80 (http)/tcp`，点击该链接会显示默认入侵事件工作流程的第一个页面，并列出以该端口为目标的事件。请注意，只会显示当前时间范围内的事件（以及生成事件的受管设备）。此外，标记为“已审核”的入侵事件会继续显示在统计信息中。例如，如果当前时间范围是过去一小时，但第一个事件是在五小时前生成的，当点击 **First Event** 链接时，打开的事件页面将不会显示事件，直至时间范围被更改。

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。

过程

步骤 1 选择**概述** > **摘要** > **入侵事件统计信息**。

步骤 2 从页面顶部的两个选择框选择要查看其统计信息的区域和设备，或者选择**所有安全区域 (All Security Zones)** 和**所有设备 (All Devices)** 以查看收集入侵事件的所有设备的统计信息。

步骤 3 点击 **Get Statistics**。

提示 要查看自定义时间范围内的数据，请点击页面右上角区域的链接并按照更改时间窗口，第 661 页中的指示操作。

主机统计信息

“入侵事件统计信息”(Intrusion Event Statistics) 页面的“主机统计信息”(Host Statistics) 部分提供有关设备本身的信息。在 Cisco Secure Firewall Management Center上，此部分还提供有关所有受管设备的信息。

这些信息包括以下内容：

时间

设备的当前时间。

正常运行时间

设备本身重新启动以来的天数、小时数和分钟数。在Cisco Secure Firewall Management Center上，Uptime 还显示每个受管设备上一次重新启动的时间、已登录用户数和平均负载。

磁盘使用情况

正使用的磁盘空间的百分比。

内存使用率

正使用的系统内存的百分比。

平均负载

过去 1 分钟、5 分钟和 15 分钟内 CPU 队列的平均进程数。

事件概述

“入侵事件统计信息”(Intrusion Event Statistics) 页面的“事件概述”(Event Overview) 部分提供入侵事件数据库中信息的概述。

这些统计信息包括以下内容：

事件

入侵事件数据库中的事件数。

时间范围内的事件 (Events in Time Range)

当前选定的时间范围以及数据库中属于该时间范围的事件数量和所占百分比。

第一个事件 (First Event)

事件数据库中第一个事件的事件消息。

上一事件

事件数据库中最后一个事件的事件消息。

注释 如果在 Cisco Secure Firewall Management Center上查看入侵事件数据时选择受管设备，将会转而显示该设备的“事件概述”部分。

事件统计信息

“入侵事件统计信息”页面的“事件统计信息”部分提供有关入侵事件数据库中信息的更具体信息。

这些信息包括以下方面的详细信息：

- 前 10 大事件类型
- 前 10 大源 IP 地址
- 前 10 大目标 IP 地址
- 前 10 大目标端口
- 具有最大数量事件的协议、入口安全区域、出口安全区域和设备

注释 在多域部署中，系统会为每个枝叶域构建单独的网络映射。因此，枝叶域可以包含这样一个 IP 地址，该地址在它的网络内是唯一的，但与另一枝叶域中的IP地址完全相同。在祖先域中查看事件统计信息时，系统可以展示该重复IP地址的多个实例。初看上去，似乎是重复条目。但是，如果向下展开到每个 IP 地址的主机配置数据，则系统会显示它们属于不同的枝叶域。

查看入侵事件性能图表

在入侵事件性能页面上，可生成用于说明 Cisco Secure Firewall Management Center或受管设备的入侵事件在特定时间段内的性能统计信息的图表。可以生成图表来反映每秒入侵事件数、每秒兆位数、每个数据包的平均字节数、Snort未检查的数据包百分比以及因TCP规范化而被阻止的数据包数量。这些图表可以显示过去一小时、前一天、上一周或上个月的运行统计信息。

注释 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。每个图表显示所选时间段（上个月、上周、前一天或前一小时）内所示时间间隔（每天、每小时或每五分钟）的平均 值。如果平均值小于 1，则以十进制形式显示值。

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** > **入侵事件性能**。

步骤 2 从**选择设备 (Select Device)** 列表中，选择要查看其数据的设备。

步骤 3 从**选择图表 (Select Graph[s])** 列表中，选择要创建的图表类型，如入侵事件性能统计信息图表类型，第 789 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**。

步骤 6 要保存图表，请右键点击它并按照浏览器的指示保存图像。

入侵事件性能统计信息图表类型

下表列出了可用的图表类型。请注意，如果图表类型填充的数据受网络分析策略 **Inline Mode** 设置影响，则图表类型显示会有所不同。如果禁用**内联模式**，Web 界面上标有星号 (*) 的图表类型（在下方列中列出 `yes`）会使用有关流量的数据进行填充；如果启用**内联模式**，则系统会修改或丢弃数据。

表 *114:* 入侵事件性能图表类型

要为以下项生成数据：	您必须.....	代表含义.....	是否受“内联模式”(Inline Mode) 影响？
平均字节/数据包	n/a	每个数据包中包含的平均字节数。	否
在 TCP 流量/数据包中规范化的 ECN 标志	启用 **Explicit Congestion Notification** 并选择 **Packet**	无论是否协商，以数据包为单位，已为其清除 ECN 标记的数据包的数量。	是
在 TCP 流量/会话中规范化的 ECN 标记	启用 **Explicit Congestion Notification** 并选择 **Stream**	未协商使用 ECN 使用时，以数据流为单位，ECN 标记被清除的次数。	是
事件/秒	n/a	设备上每秒生成的事件数。	否
ICMPv4 回应规范化	启用 **Normalize ICMPv4**	回显（请求）或回显回复消息中 8 位 Code 字段被清除的 ICMPv4 数据包的数量。	是
ICMPv6 回应规范化	启用 **Normalize ICMPv6**	回显（请求）或回显回复消息中 8 位 Code 字段被清除的 ICMPv6 数据包的数量。	是
IPv4 DF 标记规范化	启用 **Normalize IPv4** 和 **Normalize Don’t Fragment Bit**	IPv4 Flags 报头字段的一位 Don’t Fragment 子字段被清除的 IPv4 数据包的数量。	是
IPv4 选项规范化	启用**规范化 IPv4 (Normalize IPv4)**	选项八位字节被设置为 1（“无操作”[No Operation]）的 IPv4 数据包的数量。	是

要为以下项生成数据：	您必须.....	代表含义.....	是否受“内联模式”(Inline Mode)影响？
IPv4 保留标记规范化	启用 **Normalize IPv4** 和 **Normalize Reserved Bit**	IPv4 Flags 报头字段的一位 Reserved 子字段被清除的 IPv4 数据包的数量。	是
IPv4 调整大小规范化	启用 **Normalize IPv4**	已按照IP报头中指定数据报长度截断多余长度负载的 IPv4 数据包的数量。	是
IPv4 TOS 规范化	启用 **Normalize IPv4** 和 **Normalize TOS Bit**	单字节 Differentiated Services (DS) 字段（之前叫做 Type of Service (TOS) 字段）被清除的 IPv4 数据包的数量。	是
IPv4 TTL 规范化	启用**规范化 IPv4 (Normalize IPv4)**、**最大 TTL (Maximum TTL)** 和**重置 TTL (Reset TTL)**	IPv4 生存时间规范化的数量。	是
IPv6 选项规范化	启用 **Normalize IPv6**	Hop-by-Hop Options 或 Destination Options 扩展报头中 Option Type 字段设置为 00（跳过并继续处理）的 IPv6 数据包的数量。	是
IPv6 TTL 规范化	启用**规范化 IPv6 (Normalize IPv6)**、**最小 TTL (Minimum TTL)** 和**重置 TTL (Reset TTL)**	IPv6 跳数限制 (TTL) 规范化的数量。	是
兆位/秒	n/a	每秒通过设备的流量兆位数。	否
调整大小以适应MSS的数据包规范化	启用**调整数据以适应 MSS (Trim Data to MSS)**	负载长于“TCP 数据”(TCP Data) 字段，因而被调整至“最大分片大小”(Maximum Segment Size) 的数据包的数量。	是
调整大小以适应TCP窗口的数据包规范化	启用**调整数据以适应窗口 (Trim Data to Window)**	“TCP 数据”(TCP Data) 字段被调整以适应接收主机的 TCP 窗口的数据包的数量。	是
丢包率	n/a	所有选定设备上未经检查的数据包的平均百分比。例如，如果选择两个设备，那么平均百分比 50% 可能表示一个设备的丢包率为 90%，另一个的丢包率为 10%。也可能表示这两个设备的丢包率均为 50%。当选择一个设备时，此图表仅表示总丢包率。	否
数据条带化的RST数据包规范化	启用 **RST 时删除数据 (Remove Data on RST)**	数据被从 TCP 重置 (RST) 数据包移除的数据包的数量。	是

要为以下项生成数据：	您必须.....	代表含义.....	是否受“内联模式”**(Inline Mode)** 影响？
数据条带化的SYN数据包规范化	启用 **SYN 时删除数据 (Remove Data on SYN)**	当 TCP 操作系统不是 Mac OS 时数据被从 SYN 数据包移除的数据包的数量。	是
TCP 报头填充规范化	启用**规范化/清除选项填充字节 (Normalize/Clear Option Padding Bytes)**	选项填充字节设置为 0 的 TCP 数据包的数量。	是
无选项 TCP 规范化	启用**允许这些 TCP 选项 (Allow These TCP Options)** 并设置为 `any` 之外的任意选项	“时间戳”(Time Stamp) 选项条带化的数据包的数量。	是
TCP NS 标记规范化	启用**显式堵塞通知**并选择**数据包**	“ECN 随机数总和 (NS)”(ECN Nonce Sum [NS]) 选项规范化的数量。	是
TCP 选项规范化	启用**允许这些 TCP 选项 (Allow These TCP Options)** 并设置为 `any` 之外的任意选项	选项字段设置为“无操作（TCP 选项 1）”(No Operation [TCP Option 1]) 的选项的数量（MSS、“窗口比例”[Window Scale]、“时间戳”[Time Stamp] 以及明确允许的选项除外）。	是
TCP 数据包阻止条件规范化	启用**规范化 TCP 负载 (Normalize TCP Payload)**（分片重组必须失败）	因为 TCP 分段无法正确重组而被丢弃的数据包的数量。	是
TCP 保留标记规范化	启用**规范化/清除保留位 (Normalize/Clear Reserved Bits)**	“保留”(Reserved) 位被清除的 TCP 数据包的数量。	是
TCP 分段重组规范化	启用**规范化 TCP 负载 (Normalize TCP Payload)**（分片重组必须成功）	“TCP 数据”(TCP Data) 字段已规范化以确保重传数据一致性的数据包数量（无法正确重组的所有分段都被丢弃）。	是
TCP SYN 选项规范化	启用**允许这些 TCP 选项 (Allow These TCP Options)** 并设置为 `any` 之外的任意选项	由于未设置 SYN 控制位，“最大分片大小”(Maximum Segment Size) 或“窗口比例”(Window Scale) 选项被设置为“无操作（TCP 选项 1）”(No Operation [TCP Option 1]) 的选项的数量。	是
TCP 时间戳 ECR 规范化	启用**允许这些 TCP 选项 (Allow These TCP Options)** 并设置为 `any` 之外的任意选项	“时间戳回应答复 (TSecr)”(Time Stamp Echo Reply [TSecr]) 选项字段由于未设置确认 (ACK) 控制位而被清除的数据包的数量。	是

要为以下项生成数据：	您必须.....	代表含义.....	是否受“内联模式”(Inline Mode)影响？
TCP 紧急指针规范化	启用 **Normalize Urgent Pointer**	双字节 TCP 报头 Urgent Pointer 字段大于负载长度，因而被设置成负载长度的数据包的数量。	是
被阻止的地址块总数	配置**内联模式 (Inline Mode)**或**内联时丢弃 (Drop when Inline)**	丢弃的数据包总数，包括规则、解码器和预处理器丢弃。	否
总计注入的数据包	配置**内联模式 (Inline Mode)**	在重新传输前调整大小的数据包的数量。	否
总 TCP 过滤的数据包	配置“TCP 数据流预处理”(TCP Stream Preprocessing)	由于 TCP 端口过滤而被数据流跳过的数据包的数量。	否
总 UDP 过滤的数据包	配置“UDP 数据流预处理”(UDP Stream Preprocessing)	由于 UDP 端口过滤而被数据流跳过的数据包的数量。	否
紧急标记清除规范化	启用**如果未设置紧急指针则清除 URG (Clear URG if Urgent Pointer is Not Set)**	因为未设置紧急指针，TCP 报头 URG 控制位被清除的数据包的数量。	是
紧急指针和紧急标记清除规范化	启用**空负载时清除紧急指针/URG (Clear Urgent Pointer/URG on Empty Payload)**	TCP 报头“紧急指针”(Urgent Pointer) 字段和 URG 控制位由于没有负载而被清除的数据包的数量。	是
紧急指针清除规范化	启用 **Clear Urgent Pointer if URG=0**	16 位 TCP 报头 Urgent Pointer 字段由于未设置紧急 (URG) 控制位而被清除的数据包的数量。	是

相关主题

内联规范化预处理器
内联部署中预处理器流量的修改
内联部署中的丢弃行为

查看入侵事件图表

Firepower 系统提供显示入侵事件随时间推移变化趋势的图表。可为一个或所有受管设备生成时间变化范围为过去一小时至上个月的入侵事件图表。

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** > **入侵事件图表**。

步骤 2 在**选择设备 (Select Device)** 下，选择**全部 (all)** 以包括所有设备，或选择要包括在图表中的特定设备。

步骤 3 在**选择图表 (Select Graph[s])** 下，选择要生成的图表类型：

- 前 10 个目标端口
- 前 10 个源 IP 地址
- 前 10 个事件消息

步骤 4 在**选择时间范围 (Select Time Range)** 下，选择图表的时间范围：

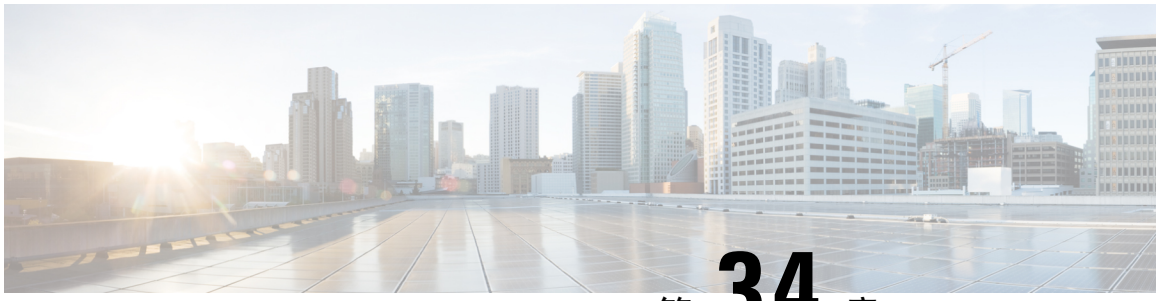
- 过去一小时
- 最近一天
- 上周
- 上个月

步骤 5 点击 **Graph**。

入侵事件历史记录

功能	最低 管理中心	最低 威胁防御	详情
IPS 事件数据存储库替换	7.1	任意	• 入侵事件、入侵事件剪贴板和默认自定义表（使用入侵事件列 - **具有源重要性的入侵事件** 和 **具有目标重要性的入侵事件**）已弃用。 您无法再使用 **复制** 和 **全部复制** 按钮将事件添加到剪贴板。 弃用的页面： • **分析** > **入侵** > **事故** • **分析** > **入侵** > **事故** • 主入侵事件表中添加了两个新字段 - **源主机重要性** 和 **目标主机重要性**。 支持的平台： Cisco Secure Firewall Management Center
系统日志中连接事件的唯一标识符	6.4.0.4	任意	以下系统日志字段共同唯一标识连接事件并在入侵事件的系统日志中显示：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。
系统日志中现包括 IntrusionPolicy 字段	6.4	任意	入侵事件系统日志现在指定触发事件的入侵策略。

功能	最低 管理中心	最低 威胁防御	详情
新入侵事件搜索字段：CVE ID	6.4	任意	您现在可以按 MITRE 的常见漏洞和风险标识号进行搜索 修改的屏幕： **分析 > 入侵 > 事件 > 编辑搜索** 支持的平台：所有。



第 34 章

文件/恶意软件事件和网络文件轨迹

以下主题提供文件和恶意软件事件的概述、本地恶意软件分析、动态分析、捕获文件和网络文件轨迹。

关于文件/恶意软件事件和网络文件轨迹

文件策略会自动为匹配的流量生成文件和恶意软件事件，并记录捕获的文件信息。当文件策略生成文件或恶意软件事件或者捕获文件时，系统还会自动将关联连接的结尾记录到 Cisco Secure Firewall Management Center数据库。您可分析此数据以解决任何不利影响及阻止未来攻击的事件。

根据文件分析结果，您可以使用“分析”>“文件”菜单下提供的页面上的表格查看捕获的文件以及生成的恶意软件和文件事件。您可以仔细查阅文件的构成、处置情况、威胁评分和动态分析摘要报告（如果有这些信息），从而进一步了解恶意软件分析。

要使分析更具针对性，您可以使用恶意软件文件的网络文件轨迹（显示该文件如何遍历您的网络、如何在主机之间传输以及各种文件属性的图）来跟踪个别威胁随时间推移跨主机进行的传播，从而在最有用的方面集中开展爆发控制和防御工作。

如果您在文件规则中配置本地恶意软件分析或动态分析，则系统会对与规则匹配的文件进行预分类并生成文件处置情况报告。

如果您的组织已部署面向终端的 *AMP* 并将该部署与 Cisco Secure Firewall Management Center进行了集成，您还可以导入扫描记录、恶意软件检测和隔离，以及该产品识别的感染指标(IOC)。此数据与 Firepower 收集的事件数据一起显示，以便更全面地了解网络上的恶意软件。

情景管理器、控制面板和报告功能也有助于更深入地了解检测、捕获和阻止的文件及恶意软件。您也可以使用事件触发关联策略违规或者通过邮件、SMTP 或系统日志向您发出警报。

注释 要配置系统以检测恶意软件并生成文件和恶意软件事件，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的 网络恶意软件保护和文件策略 。

文件和恶意软件事件

Cisco Secure Firewall Management Center可以记录各种类型的文件和恶意软件事件。可用于任何单个事件的信息可能会根据该事件的生成方式和原因而异：

- 文件事件表示文件，包括Firepower系统（恶意软件防护）检测到的恶意软件。文件事件不包含面向终端的 AMP 相关字段。
- 恶意软件事件表示恶意软件防护 或面向终端的 AMP 检测到的恶意软件；恶意软件事件还可以记录除来自面向终端的 AMP 部署的威胁以外的数据，例如扫描和隔离。
- 追溯性恶意软件事件表示恶意软件防护 检测到的其处置情况（文件是否为恶意软件）已更改的文件。

注释
- 由恶意软件防护 识别为恶意软件的文件同时生成文件事件和恶意软件事件。由面向终端的AMP生成的恶意软件事件没有对应的文件事件。
- 检查 NetBIOS-ssn (SMB) 流量所生成的文件事件不会立即生成连接事件，因为客户端和服务器构建一个持久连接。系统在客户端或服务器结束会话之后生成连接事件。
- Firepower 系统支持显示和输入使用 Unicode (UTF-8) 字符的文件名。但是，Unicode 文件名在 PDF 报告中以转译形式显示。此外，SMB 协议将文件名中不可打印的字符替换为英文句号。

文件和恶意软件事件类型

文件事件

系统将按照当前部署的文件策略记录当受管设备在网络流量中检测或阻止文件时生成的文件事件。

系统生成文件事件时，无论调用访问控制规则采用何种日志记录配置，系统都会将关联连接的结束事件记录到 Cisco Secure Firewall Management Center数据库中。

恶意软件事件

Firepower系统（特别是恶意软件防护 功能）在网络流量中检测到恶意软件时会生成恶意软件事件，这是整个访问控制配置的一部分。恶意软件事件包含生成事件的处置情况，以及有关检测该恶意软件的方式、位置和时间的情景数据。

表 *115:* 恶意软件事件生成情景

当系统检测到文件并且...	处理结果
成功查询 AMP 云（执行恶意软件云查找）以了解文件的处置情况	恶意软件、干净或未知
查询 AMP 云，但无法建立连接或云因其他原因而不可用	不可用 您可能看到很少一部分事件为此处置；这是预期行为。
与文件关联的威胁评分超过检测到该文件的文件策略中定义的恶意软件威胁评分阈值，或者本地恶意软件分析识别恶意软件	恶意软件
它包含在自定义检测列表中（手动标记为恶意软件）	自定义检测
它包含在干净的列表中（手动标记为干净）	正常

恶意软件事件中的文件处置和文件操作

每个文件规则都有用于确定系统如何处理与规则条件匹配的流量的关联操作。如果选择 阻止恶意软件 或 恶意软件云查询 作为文件规则操作，系统将查询 AMP 云以确定通过网络传输的文件是否包含恶意软件，然后阻止存在威胁的文件。云查找允许您根据文件的 SHA-256 散列值获取并记录文件的处置情况。

下表介绍与 AMP 云返回的文件处置情况相关联的文件操作：

表 *116:* 恶意软件事件中的文件处置和文件操作

已选的文件规则操作	文件处置	恶意软件事件中的文件操作
• 阻止恶意软件 • 恶意软件云查找	恶意软件	阻止
	• 正常 • 未知 • 不可用 • 不适用	云查找 **注释** 在文件策略编辑器高级设置下，您可以为 **如果 AMP 云处置情况为未知，根据威胁评分覆盖处置情况** 选项设置阈值威胁评分。如果设置了阈值威胁评分，则 AMP 云判定为“未知”的文件如果其动态分析评分等于或低于阈值，则会被视为恶意软件。

追溯性恶意软件事件

对于在网络流量中检测到的恶意软件文件，处置情况可以更改。例如，AMP 云可以确定先前被视为干净的文件现在被识别为恶意软件，或者正好相反，以前被识别为恶意软件的文件实际上是干净的。当上周查询的文件的处置情况发生更改时，AMP 云会通知系统。然后将发生两件事情：

- Cisco Secure Firewall Management Center产生新追溯性恶意软件事件。

  新追溯性恶意软件事件代表上一周检测到的具备相同 SHA-256 哈希值的所有文件的性质发生变更。因此，这些事件包含限定信息：Cisco Secure Firewall Management Center接到性质变更通知的日期和时间、新性质、文件 SHA-256 哈希值以及威胁名称。它们不包含 IP 地址或其他上下文信息。

- Cisco Secure Firewall Management Center变更此前检测到的具有追溯事件相关 SHA-256 哈希值的文件的文件性质。

  如果文件性质变更为 Malware，Cisco Secure Firewall Management Center在其数据库内记录新恶意软件事件。除了新性质，新恶意软件事件信息与最初检测到文件时生成的文件事件中的信息都相同。

  如果文件的处置情况更改为“安全”，则 Cisco Secure Firewall Management Center不会删除恶意软件事件。相反，该事件反映处置情况更改。这表示文件性质为安全的文件能够出现在恶意软件表中，前提是它们最初被视为恶意软件。从未识别为恶意软件的文件只会出现在文件表中。

由面向终端的 AMP 生成的恶意软件事件

如果您的组织使用面向终端的AMP，则个人用户可以在终端（计算机和移动设备）上安装轻量级连接器。连接器可在进行上传、下载、执行、打开、复制、移动等操作后检查文件。这些连接器与 AMP 云进行通信，以确定检查的文件是否包含恶意软件。

文件被确定为恶意软件后，AMP 云会向 Cisco Secure Firewall Management Center发送威胁识别。AMP 云还可以向 Cisco Secure Firewall Management Center发送其他类型的信息，包括有关扫描、隔离、受阻执行和云召回的数据。Cisco Secure Firewall Management Center将这些信息记录为恶意软件事件。

注释 面向终端的 AMP 生成的恶意软件事件中所报告的 IP 地址可能不在网络映射中 - 甚至可能根本不在监控的网络中。根据部署、合规级别以及其他因素，您的组织中由面向终端的AMP监控的终端可能与恶意软件防护 监控的终端不是相同的主机。

使用 Cisco Secure Endpoint 的恶意软件事件分析

如果您的组织已部署 Cisco Cisco Secure Endpoint：

- 您可以将系统配置以在 管理中心 事件页面上显示由Cisco Secure Endpoint检测的恶意软件事件，旁边显示 恶意软件防护检测到的事件。
- 如果您使用 AMP 公共云，可以在 Cisco Secure Endpoint中查看文件轨迹和有关特定 SHA 的其他信息。

要配置上述功能，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的 集成 *Firepower* 和 *Cisco Secure Endpoint*。

来自 Cisco Secure Endpoint 的事件数据

如果您的组织已部署 Cisco Secure Endpoint 以进行恶意软件防护，则您可以将系统配置为允许在 管理中心 中处理来自 Cisco Secure Endpoint的文件和恶意软件数据。

但是，您应了解来自 Cisco Secure Endpoint 的文件和恶意软件数据与来自系统的 恶意软件防护 功能的文件和恶意软件数据之间的差异。

由于Cisco Secure Endpoint 恶意软件检测是在下载或执行时于终端处执行，而受管设备在网络流量中检测恶意软件，因此两种类型的恶意软件事件中的信息不同。例如，Cisco Secure Endpoint 检测到的恶意软件事件（“基于终端的恶意软件”）包含有关文件路径、调用客户端应用等等的信息，而网络流量中的恶意软件检测则包含有关用于传输文件的连接的端口、应用协议和始发 IP 地址信息。

再例如，恶意软件防护检测到的恶意软件事件（“基于网络的恶意软件事件”）中，用户信息向用户展示此用户最近登录的主机是恶意软件的攻击目标，并且恶意软件是由网络发现功能确定的。但是， Cisco Secure Endpoint-报告的用户是指当前登录其中检测到恶意软件的终端的用户。

注释 根据您的部署，由 Cisco Secure Endpoint 监控的终端可能不是与由 恶意软件防护监控的终端相同的主机。因此， Cisco Secure Endpoint 生成的恶意软件事件不将主机添加到网络映射。但是，系统会使用 IP 和 MAC 地址数据标记具有从 Cisco Secure Endpoint 部署获取的危害表现的受监控主机。如果不同恶意软件解决方案监控的两个不同主机具有相同的 IP 和 MAC 地址，则系统可能会错误地标记具有 Cisco Secure Endpoint IOC 的受监控主机。

下表汇总了 Firepower 使用 恶意软件防御 许可证时生成的事件数据与 Cisco Secure Endpoint生成的事件数据之间的差异。

表 *117: AMP* 产品之间的数据差异汇总

功能	恶意软件防护	Cisco Secure Endpoint
生成的事件	文件事件、捕获文件、恶意软件事件及追溯性恶意软件事件	恶意软件事件
恶意软件事件中的信息	基本的恶意软件事件信息，以及连接数据（IP 地址、端口和应用协议）	深入的恶意软件事件信息；无连接数据
网络文件轨迹	基于管理中心	管理中心 和 Cisco Secure Endpoint 管理控制台均具有网络文件轨迹。两者均很有用。

相关主题

在 《Cisco Secure Firewall Management Center 设备配置指南》中集成 *Firepower* 和 *Cisco Secure Endpoint*

使用文件和恶意软件事件工作流程

通过此过程可查看表中的文件和恶意软件事件，并根据与分析相关的信息操作事件视图。在访问事件时看到的页面因工作流程有所不同。工作流程只是一系列页面，您可以从广泛视图移动到更加突出重点的视图，使用这些页面评估事件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

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。

您必须是管理员或安全分析师用户才能执行此任务。

过程

选择以下其中一个选项：

- **分析** > **文件** > **文件事件**
- **分析** > **文件** > **恶意软件事件**

提示 事件表视图中的一些字段在默认情况下处于隐藏状态。要显示事件视图的隐藏字段，请展开搜索限制，然后点击 **Disabled Columns** 下的字段名称。

提示 要快速查看检测到特定文件的连接，请使用表中的复选框选择文件，然后从**跳转至**下拉列表中选择**连接事件**。

提示 右键点击表中的项目以查看选项。（并非每个列都提供选项。）

相关主题

文件和恶意软件事件字段，第 800 页
预定义文件工作流程，第 635 页
预定义恶意软件工作流程，第 635 页
配置事件视图设置，第 193 页

文件和恶意软件事件字段

文件和恶意软件事件（您可以通过工作流程查看和搜索文件和恶意软件事件）包含此部分中列出的字段。请记住，可用于任何单个事件的信息可能会根据该事件的生成方式和原因而异。

注释 由恶意软件防护 识别为恶意软件的文件同时生成文件事件和恶意软件事件。由 Cisco Secure Endpoint 生成的恶意软件事件没有对应的文件事件，并且文件事件没有与 Cisco Secure Endpoint相关的字段。

系统日志消息使用初始值填充并且不会更新。即使 管理中心 Web 接口中的等效字段使用追溯性判定等进行了更新，系统日志消息也不会更新。

操作（系统日志： **FileAction**）

检测文件的文件策略规则的相关操作以及任何相关文件规则操作选项。

AMP 云

产生面向终端的 AMP 事件的 AMP 云名称。

应用文件名

检测面向终端的 AMP 期间访问恶意软件文件的客户端应用。这些应用与网络发现或应用控制**无**关联。

应用文件 **SHA256**

检测面向终端的 AMP 期间访问被检测或隔离文件的父文件的 SHA-256 散列值。

在统一事件查看器中，此字段显示为 **应用文件 SHA-256**。

应用协议（系统日志：**ApplicationProtocol**）

受管设备检测到文件的流量所用应用协议。

应用协议类别或标记

展示应用特征的条件，协助您了解应用功能。

应用风险

与连接中检测到的应用流量关联的风险：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。

存档深度（系统日志： **ArchiveDepth**）

文件嵌入存档文件的层级（如有）。

存档名称（系统日志： **ArchiveFileName**）

包含恶意软件文件的存档文件名称（如有）。

要查看存档文件的内容，请在**分析 (Analysis) > 文件 (Files)**下打开列出该存档文件的任意表，右键点击该存档文件的表行来打开情景菜单，然后点击**查看存档内容 (View Archive Contents)**。

存档 **SHA256**（系统日志： **ArchiveSHA256**）

包含恶意软件文件的存档文件的 SHA-256 散列值（如有）。

要查看存档文件的内容，请在“分析”(Analysis)>“文件”(Files) 下打开列出该存档文件的任意表，右键点击该文档文件的表行来打开情景菜单，然后点击**查看存档内容 (View Archive Contents)**。

ArchiveFileStatus（仅限系统日志）

正在被检测的存档的状态。可能会有以下值：

- 待处理 - 正在检测存档
- 已提取 - 已成功检测，且无任何问题
- 失败 - 检测失败，系统资源不足
- 超出深度 - 检测成功，但存档超出嵌套检测深度
- 已加密 - 部分检测成功，存档已加密或包含加密存档
- 不可检测 - 部分检测成功，文件可能格式有误或损坏

业务相关性

与连接中检测到的应用流量关联的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。

类别/文件类型类别

一般类别文件类型，例如：Office 文档、存档、多媒体、可执行文件、PDF 文件、编码文件、图形或系统文件。

客户端（系统日志：**Client**）

在一台主机上运行并依靠服务器发送文件的客户端应用。

客户端类别或标记

展示应用特征的条件，协助您了解应用功能。

连接计数器 （仅限系统日志）

区分一个连接与另一个同时连接的计数器。此字段本身没有意义。

以下字段共同唯一地标识与特定文件或恶意软件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

连接实例 ID （仅限系统日志）

处理连接事件的 Snort 实例。此字段本身没有意义。

以下字段共同唯一地标识与特定文件或恶意软件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

计数

应用创建两个或多个相同行的限制条件后，与每行中的信息匹配的事件数。

检测名称

被测恶意软件名称。

检测器

识别恶意软件的面向终端的 AMP 检测器，例如 ClamAV、Spero 或 SHA。

设备

对于文件事件和 Firepower 设备生成的恶意软件事件，显示检测到文件的设备的名称。

对于面向终端的 AMP 生成的恶意软件事件和 AMP 云生成的追溯性恶意软件事件，显示 管理中心的名称。

DeviceUUID （仅限系统日志）

生成事件的 Firepower 设备的唯一标识符。

以下字段共同唯一地标识与特定文件或恶意软件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

处置情况/文件处置情况（系统日志： SHA_Disposition）

文件的处置情况：

恶意软件

表示 AMP 云将文件归类为恶意软件，本地恶意软件分析识别的恶意软件或文件威胁评分超过文件策略中定义的恶意软件阈值。

干净

表示 AMP 云将文件分类为干净，或用户将文件添加到干净列表。干净的文件仅在变更为干净后才会显示在恶意软件表中。

未知

表示系统已查询 AMP 云，但文件尚未被分配处置情况；换句话说，AMP 云尚未对文件进行分类。

自定义检测

表示用户将文件添加到自定义检测列表。

不可用

表示系统无法查询 AMP 云。您可能看到很少一部分事件为此处置；这是预期行为。

不适用

表示“检测文件”或“阻止文件”规则已处理文件，Cisco Secure Firewall Management Center未查询 AMP 云。

只有系统为之查询 AMP 云的文件才会显示文件处置情况。

系统日志字段仅反映初始处置情况；它们不会进行更新以反映追溯裁定。

域

对于文件事件和Firepower设备生成的恶意软件事件，显示检测到文件的设备的域。对于面向终端的AMP生成的恶意软件事件和AMP云生成的追溯性恶意软件事件，显示与报告事件的AMP云连接关联的域。

仅当曾经配置 管理中心以实现多租户时，此字段才存在。

DstIP（仅限系统日志）

对连接作出响应的主机的IP地址。这可能是文件发送方或接收方的IP地址，具体取决于FileDirection字段中的值：

如果 FileDirection 字段中的值为 **`Upload`**，则为文件接收方的 IP 地址。

如果 FileDirection 字段中的值为 **`Download`**，则为文件发送方的 IP 地址。

另请参阅 **SrcIP**。

另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明，第 733 页。

DstPort（仅限系统日志）

DstIP 所述在连接中使用的端口。

出口虚拟路由器

在使用虚拟路由的网络中，用于流量离开网络的虚拟路由器的名称。

事件子类型

导致恶意软件检测的面向终端的 AMP 操作，例如，“创建”(Create)、“执行”(Execute)、“移动”(Move) 或“扫描”(Scan)。

事件类型

恶意软件事件的子类型。

文件名（系统日志： FileName）

文件名称。

文件路径

面向终端的 AMP 检测到的恶意软件文件的文件路径，不包括文件名。

文件策略（系统日志： FilePolicy）

检测文件的文件策略。

文件存储/已存储（系统日志： FileStorageStatus）

与事件关联的文件的存储状态：

已存储

返回当前存储相关文件的所有事件。

已在连接中存储 (Stored in connection)

返回系统捕获并存储相关文件的所有事件，无论当前是否已存储相关文件。

失败

返回系统无法存储相关文件的所有事件。

系统日志字段仅包含初始状态；它们不会进行更新以反映更改的状态。

文件时间戳

面向终端的 AMP 检测到恶意软件文件创建的时间和日期。

FileDirection（仅限系统日志）

文件在连接期间是否进行过下载或上传。可能的值包括：

- 下载 - 文件由 DstIP 传输至 SrcIP。
- 上传 - 文件由 SrcIP 传输至 DstIP。

FileSandboxStatus（仅限系统日志）

表示是否已发送文件以进行动态分析，若已发送则表示状态。

第一个数据包时间 （仅限系统日志）

系统遇到第一个数据包的时间。

以下字段共同唯一地标识与特定文件或恶意软件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

FirstPacketSecond（仅限系统日志）

文件下载或上传流程开始的时间。

消息报头时间戳中捕获有事件发生的时间。

HTTP 响应代码

传输文件时，系统响应客户端的 HTTP 请求发送的 HTTP 状态代码。

入口虚拟路由器

在使用虚拟路由的网络中，用于流量进入网络的虚拟路由器的名称。

IOC

对于连接涉及的主机，恶意软件事件是否触发危害表现 (IOC)。当面向终端的 AMP 数据触发 IOC 规则时，将生成 AMP IOC 类型的完整恶意软件事件。

消息

恶意软件事件相关的其他信息。对于文件事件和 Firepower 设备生成的恶意软件事件，系统仅对处置情况发生变更的文件（即具有关联追溯性事件的文件）填充此字段。

MITRE

您可以点击以显示 MITRE 战术和层次结构中的技术的完整列表的模式计数。

协议（仅限系统日志）

用于连接的协议，例如 TCP 或 UDP。

接收大洲

接收文件的主机所在大洲。

接收国家/地区

接收文件的主机所在国家/地区。

接收 IP

在 管理中心 web 接口，对于文件事件和 Firepower 设备生成的恶意软件事件，显示接收文件的主机的 IP 地址。另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明，第 733 页。

对于面向终端的 AMP 生成的恶意软件事件，显示连接器报告事件的终端的 IP 地址。

有关系统日志等效项（仅 Firepower 设备生成的事件），请参阅 **DstIP** 和 **SrcIP**。

接收端口

在 管理中心 web 接口，检测到文件的流量所用目标端口。

对于系统日志等效项，请参阅 **DstIP** 和 **SrcIP** 以及 **DstPort** 和 **SrcPort**。

安全情景（系统日志：Context）

识别流量通过的虚拟防火墙组的元数据。请注意，仅当系统管理至少一个在多情景模式下运行的 ASA FirePOWER 设备时才会显示此字段。

发送大洲

发送文件的主机所在大洲。

发送国家/地区

发送文件的主机所在国家/地区。

发送 IP

在 管理中心 Web 接口，发送文件的主机的 IP 地址。另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明，第 733 页。

对于系统日志等效项，请参阅 **DstIP** 和 **SrcIP**。

发送端口

在 管理中心 web 接口，检测到文件的流量所用源端口。

对于系统日志等效项，请参阅 **DstIP** 和 **SrcIP** 以及 **DstPort** 和 **SrcPort**。

SHA256/文件 SHA256 （系统日志： FileSHA256）

文件的 SHA-256 散列值。

要具有 SHA256 值，文件必须已经过以下任一文件规则处理：

- 启用了**存储文件**的“检测文件”文件规则
- 启用了**存储文件**的“阻止文件”文件规则
- “恶意软件云查找”(Malware Cloud Lookup) 文件规则
- “阻止恶意软件”(Block Malware) 文件规则
- 面向终端的 AMP

此列还会显示代表最近检测到的文件事件和文件处置情况且链接到网络文件轨迹的网络文件轨迹图标。

大小 (KB)/文件大小 (KB) （系统日志： FileSize）

在 管理中心 Web 接口，文件大小（千字节）。

在系统日志消息中：文件大小（字节）。

请注意，如果系统在完全接收某个文件前确定了该文件的文件类型，则可能不会计算该文件的大小。在这种情况下，此字段为空。

SperoDisposition（仅限系统日志）

表示文件分析中是否使用了 SPERO 签名。可能的值：

- 已对文件执行 Spero 检测
- 未对文件执行 Spero 检测

SrcIP（仅限系统日志）

发起连接的主机的 IP 地址。这可能是文件发送方或接收方的 IP 地址，具体取决于 FileDirection 字段中的值：

如果 FileDirection 字段中的值为 **Upload**，此为文件发送方的 IP 地址。

如果 FileDirection 字段中的值为 **Download**，此为文件接收方的 IP 地址。

另请参阅 **DstIP**。

另请参阅有关发起方/响应方，源/目标和发件人/接收方字段的说明，第 733 页。

SrcPort（仅限系统日志）

SrcIP 所述在连接中使用的端口。

SSL 实际操作（系统日志：SSLActualAction）

系统应用于已加密流量的操作：

阻止或通过重置阻止

表示阻止的加密连接。

解密（重新签名）

表示使用重新签名的服务器证书解密的传出连接。

解密（替换密钥）

表示使用具有替代公钥的自签名服务器证书解密的传出连接。

解密（已知密钥）

表示使用已知私钥解密的传入连接。

默认操作

表示连接采用默认操作处理。

不解密

表示系统未解密的连接。

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL 证书信息

用于加密流量的公钥证书上存储的信息，包括：

- 使用者/颁发者公用名称
- 使用者/颁发者组织
- 使用者/颁发者单位
- 无效时间

- 序列号、证书指纹
- 公钥指纹

有关系统日志，请参阅 **SSLCertificate**。

SSL 失败原因（系统日志： SSLFlowStatus）

系统无法解密已加密流量的原因：

- 未知
- 不匹配
- 成功
- 未缓存的会话
- 未知加密套件
- 不受支持的加密套件
- 不支持的 SSL 版本
- 使用了 SSL 压缩
- 会话在被动模式下无法解密
- 握手错误
- 解密错误
- 挂起的服务器名称类别查找
- 挂起的公用名类别查找
- 内部错误 (Internal Error)
- 网络参数不可用
- 服务器证书处理无效
- 服务器证书指纹不可用
- 无法缓存使用者 DN
- 无法缓存颁发者 DN
- 未知的 SSL 版本
- 外部证书列表不可用
- 外部证书指纹不可用
- 内部证书列表无效
- 内部证书列表不可用

- 内部证书不可用
- 内部证书指纹不可用
- 服务器证书验证不可用
- 服务器证书验证失败
- 无效操作

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL 状态

与记录加密连接的 **SSL 实际操作** （解密规则、默认操作或无法解密的流量操作）关联的操作。 **锁定图标** 指向 TLS/SSL 证书详细信息。如果证书不可用（例如，对于因 TLS/SSL 握手错误而受阻的连接），锁定图标会灰显。

如果系统无法解密已加密连接，则其会显示所采取的 **SSL 实际操作 (SSL Actual Action)**（无法解密的流量操作）以及 **SSL 失败原因 (SSL Failure Reason)**。例如，如果系统检测到使用未知密码套件加密的流量并且未做进一步检查即允许了该流量，则此字段显示 `Do Not Decrypt (Unknown Cipher Suite)`。

当搜索该字段时，请键入一个或多个 **SSL 实际操作 (SSL Actual Action)** 和 **SSL 失败原因 (SSL Failure Reason)** 值以查看系统处理或无法解密的已加密流量。

SSL 使用者/颁发者所在国家/地区

与加密证书关联的使用者或颁发者所在国家/地区的双字符 ISO 3166-1 alpha-2 国家/地区代码。

SSLCertificate（仅限系统日志）

TLS/SSL 服务器的证书指纹。

威胁名称（系统日志： ThreatName）

被测恶意软件名称。

威胁评分（系统日志： ThreatScore）

与此文件相关的最新威胁评分。此为 0 至 100 之间的数值，该数值基于动态分析期间观察到的潜在恶意行为。

威胁评分图标可连接到“动态分析摘要”(Dynamic Analysis Summary) 报告。

时间

事件生成的日期和时间。此字段不可搜索。

在系统日志消息中，请参阅 **FirstPacketSecond**。

类型/文件类型（系统日志： FileType）

文件类型，例如 HTML 或 MSEXE。

URI/文件 URI（系统日志： URI）

与文件事务关联的连接的 URI，例如，用户下载文件所使用的 URL。

用户（系统日志： User）

发起连接的主机的 IP 地址相关的用户名。如果此 IP 地址在您的网络外部，则关联的用户名通常是未知的。

如果适用，用户名前面会附加 <区域>\。

对于文件事件和Firepower设备生成的恶意软件事件，此字段显示由身份策略或授权登录确定的用户名。如果没有身份策略，则显示“无需身份验证”。

对于面向终端的 AMP 生成的恶意软件事件，用户名由面向终端的 AMP 确定。这些用户不受用户发现或控制束缚。他们不会出现在用户表中，您也无法查看这些用户详细信息。

Web 应用（系统日志：WebApplication）

代表连接内被检测 HTTP 流量内容或所请求 URL 的应用。

Web 应用类别或标记

展示了应用特征的条件，以帮助您了解应用功能。

恶意软件事件子类型

下表列出了恶意软件事件子类型、是面向网络的AMP生成的恶意软件事件（“基于网络的恶意软件事件”）还是面向终端的AMP生成的恶意软件事件（“基于终端的恶意软件事件”）可具有该子类型，以及系统是否使用该子类型来建立网络文件轨迹。

表 *118:* 恶意软件事件类型

恶意软件事件子类型/搜索值	恶意软件防护	面向终端的 AMP	文件轨迹
网络文件传送中检出威胁	是	否	是
网络文件传送（回溯）中检出威胁	是	否	是
检测出威胁	否	是	是
排除部分检出威胁	否	是	是
隔离威胁	否	是	是
AMP IOC（危害表现）	否	是	否
执行受阻	否	是	否

恶意软件事件子类型/搜索值	恶意软件防护	面向终端的 AMP	文件轨迹
云召回隔离	否	是	否
云召回隔离尝试失败	否	是	否
开始云召回隔离	否	是	否
从隔离中恢复云召回	否	是	否
从隔离中恢复云召回失败	否	是	否
从隔离中恢复云召回启动	否	是	否
隔离失败	否	是	否
恢复隔离项目	否	是	否
恢复隔离失败	否	是	否
开始恢复隔离	否	是	否
扫描完成，未检出	否	是	否
扫描完成，检出	否	是	否
扫描失败	否	是	否
开始扫描	否	是	否

文件和恶意软件事件字段中的可用信息

下表列出系统是否显示每个文件和恶意软件事件字段的信息。

如果您的组织已部署面向终端的 AMP，您可以选择将该产品与 Firepower 部署进行集成。

- 从面向终端的 AMP 部署导入的恶意软件事件和危害表现 (IOC) 不包含情景连接信息，但其确实包含在下载或执行时获取的信息，例如文件路径、调用客户端应用等等。
- 文件事件表视图不显示与面向终端的 AMP 相关的字段。

表 *119*: 文件和恶意软件事件字段中的可用信息

字段	文件事件	Firepower 系统检测到的恶意软件事件	Firepower 系统检测到的追溯性事件	由面向终端的 AMP 检测到的恶意软件事件
操作	是	是	是	否
AMP 云	否	否	否	是

字段	文件事件	Firepower 系统检测到的恶意软件事件	Firepower 系统检测到的追溯性事件	由面向终端的 AMP 检测到的恶意软件事件
应用文件名	否	否	否	是
应用文件 SHA256	否	否	否	是
应用协议	是	是	否	否
应用协议类别或标记	是	是	是	否
应用风险	是	是	是	否
存档深度	是	是	否	是
存档名称	是	是	否	是
存档 SHA256	是	是	否	是
业务相关性	是	是	是	否
类别/文件类型类别	是	是	否	是
客户端	是	是	是	否
客户端类别或标记	是	是	是	否
计数	是	是	是	是
检测名称	否	是	否	否
检测器	否	否	否	是
设备	是	是	是	是
处置情况/文件处置情况	是	是	是	否
域	是	是	是	是
事件子类型	否	否	否	是
事件类型	否	是	是	是
文件名	是	是	否	是
文件路径	否	否	否	是
文件策略	是	否	否	否
文件时间戳	否	否	否	是

字段	文件事件	Firepower 系统检测到的恶意软件事件	Firepower 系统检测到的追溯性事件	由面向终端的 AMP 检测到的恶意软件事件
HTTP 响应代码	是	是	否	否
IOC（危害表现）	否	是	是	是
消息	是	是	否	是
接收大洲	是	是	是	否
接收国家/地区	是	是	否	否
接收 IP	是	是	否	是
接收端口	是	是	否	否
安全情景	是	是	是	是
发送大洲	是	是	是	否
发送国家/地区	是	是	否	否
发送 IP	是	是	否	否
发送端口	是	是	否	否
SHA256/文件 SHA256	是	是	是	是
大小 (KB)/文件大小 (KB)	是	是	否	是
SSL 实际操作（仅限搜索）	是	是	否	否
SSL 证书信息 (SSL Certificate Information)（仅限搜索）	是	是	否	否
SSL 失败原因 （仅限搜索）	是	是	否	否
SSL 状态	是	是	否	否
SSL 使用者/颁发者所在国家/地区（仅限搜索）	是	是	否	否
文件存储/已存储（仅限搜索）	是	是	否	否
威胁名称	否	是	是	是
威胁评分	是	是	否	否
时间	是	是	是	是

字段	文件事件	Firepower 系统检测到的恶意软件事件	Firepower 系统检测到的追溯性事件	由面向终端的 AMP 检测到的恶意软件事件
类型/文件类型	是	是	否	是
URI/文件 URI	是	是	否	否
用户	是	是	否	是
Web 应用程序	是	是	是	否
Web 应用类别或标记	是	是	是	否

查看有关已分析文件的详细信息

提示 要查看其他选项，请右键点击事件页面上的表中的文件 SHA。有关信息，请参阅使用基于 Web 的资源的事件调查，第 605 页。

文件构成报告

如果配置本地恶意软件分析或动态分析，则系统会在分析文件后会生成文件构成报告。您可以通过此报告进一步分析文件，并确定它们是否可能携带嵌入式恶意软件。

文件构成报告列出文件属性、文件中嵌入的任何对象以及任何检测到的病毒。文件构成报告还可能列出特定于该文件类型的其他信息。当系统删除存储的文件时，也会删除相关联的文件构成报告。

要查看文件组成信息，请参阅使用网络文件轨迹，第 826 页。

在 AMP 私有云中查看文件详细信息

如果您已部署 AMP 私有云，则可以查看有关私有云中已分析文件的其他详细信息。

有关详细信息，请参阅私有云的文档。

过程

直接登录 AMP 私有云控制台。

威胁评分和动态分析摘要报告

威胁评分

表 *120:* 威胁评分等级

威胁评分	数字分数	图标
Low	0-24	低
Medium	25-69	中等
High	70-94	高
Very High	95-100	很高

Cisco Secure Firewall Management Center对文件威胁评分进行缓存的时间与对文件处置情况进行缓存的时间相同。如果系统之后检测到这些文件，则会显示缓存威胁评分而不是重新查询 Secure Secure Malware Analytics 云或 Secure Secure Malware Analytics 设备。您可以自动向威胁评分超过已定义的恶意软件阈值威胁评分的文件分配恶意软件文件处置情况。

动态分析总结

如有动态分析总结，您可以点击威胁评分图标进行查看。如果存在多份报告，该总结应当基于与精确威胁评分匹配的最新报告。如果没有报告与精确威胁评分匹配，则会显示威胁评分最高的报告。如果存在多份报告，您可以选择一个威胁评分查看各份报告。

总结将列明构成威胁评分的各部分威胁。每个组件威胁都可以扩展至列出 AMP 云查找结果，以及与此组件威胁相关的任何进程。

进程树显示 Secure Secure Malware Analytics 云尝试运行该文件时启动的进程。这有助于识别包含恶意软件的文件是否在尝试访问超出预期的进程和系统资源（例如，运行 Word 文档打开 Microsoft Word，接着启动 Internet Explorer，然后运行 Java 运行时环境）。

列出的每个进程都包含可用于验证实际进程的进程标识符。进程树中的子节点表示由于父进程而启动的进程。

从动态分析摘要中，您可以点击**查看完整报告 (View Full Report)** 以查看完整分析报告，其中详述 AMP 云的完整分析，包括常规文件信息、对检测到的所有进程的更深入审核、文件分析明细以及其他相关信息。

查看思科 **Secure Secure Malware Analytics** 云中的动态分析结果

Secure Secure Malware Analytics 提供的有关已分析文件的报告比 管理中心提供的要详细。如果您的组织有 Secure Secure Malware Analytics 云账户，则您可以直接访问 Secure Secure Malware Analytics 门户，查看有关从受管设备发出的进行分析的文件的其他详细信息。

开始之前

- 将您的 管理中心 与您的 Secure Secure Malware Analytics 云账户关联。请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 启用对公共云中动态分析结果的访问权限
- 许可证要求：恶意软件
- 您必须在全局域中才能执行此任务。
- 您必须具有以下用户角色之一：管理员、访问管理员、网络管理员

过程

步骤 1 通过 Secure Secure Malware Analytics 文档中提供的地址访问 Secure Secure Malware Analytics 云门户。

步骤 2 使用您在此任务的前提条件中创建关联时使用的帐户凭证登录。

步骤 3 查看组织提交的文件，或使用其 SHA 搜索特定文件。

如有问题，请参阅 Secure Secure Malware Analytics 文档。

使用已捕获文件工作流程

当受管设备捕获在网络流量中检测到的文件时，它会记录一个事件。

注释 如果设备捕获包含恶意软件的文件，设备会生成两个事件：其检测文件时的文件事件，以及其识别恶意软件时的恶意软件事件。

通过此过程可查看表中已捕获文件的列表，并根据与分析相关的信息操作事件视图。在访问捕获的文件时看到的页面因工作流程有所不同。工作流程只是一系列页面，您可以使用这些页面从较宽泛的视图移动至更精细化的视图来评估事件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

如果系统在配置更改后重新捕获文件（如更新的文件策略），则会更新该文件的现有信息。

例如，如果您将文件策略配制为通过**恶意软件云查找 (Malware Cloud Lookup)** 操作捕获文件，则系统会连同文件一起存储文件处置情况和威胁评分。然后，如果您更新文件策略，且系统因新的**检测文件 (Detect Files)** 操作重新捕获同一文件，则系统会更新该文件的**上次更改时间 (Last Changed)** 值。但系统不会删除现有处置情况和威胁评分，即使您没有再次执行恶意软件云查找。

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

您必须是管理员或安全分析师用户才能执行此任务。

过程

选择**分析** > **文件** > **捕获的文件**。

提示 事件表视图中的一些字段在默认情况下处于隐藏状态。要显示事件视图的隐藏字段，请展开搜索限制，然后点击 **Disabled Columns** 下的字段名称。

相关主题

捕获文件字段，第 818 页
预定义捕获文件工作流程，第 636 页
配置事件视图设置，第 193 页

捕获文件字段

捕获文件表视图是预定义捕获文件工作流程的最终页面，也可以添加到自定义工作流程中，且该视图为捕获文件表中的每个字段都准备了对应的列。

搜索此表时，请记住搜索结果取决于所搜索事件的可用数据；根据可用数据，搜索限制可能并不适用。例如，如果文件从未被提交用于动态分析，可能没有与其关联的威胁评分。

表 *121:* 捕获文件字段

字段	说明
存档检查状态	对于存档文件，存档检查状态如下： • “待定”(Pending) 表示系统仍在检查存档文件及其内容。如果文件再次通过您的系统，就可以提供完整的信息。 • “已提取”(Extracted) 表示系统能够提取和检查存档内容。 • 在极少数情况下，如果系统无法处理提取内容，会出现“失败”(Failed) 状态。 • “超出深度”(Depth Exceeded) 表示存档包含超出最大允许深度的进一步嵌套存档文件。 • “已加密”(Encrypted) 表示存档文件内容已加密，无法进行检查。 • “不可检查”(Not Inspectable) 表示系统未提取和检查存档内容。策略规则操作、策略配置和损坏文件是出现此状态的三个主要原因。 要查看某个存档文件的内容，请右键点击其在表中所在的行，打开上下文菜单，然后选择**查看存档内容 (View Archive Contents)**。
类别	一般类别文件类型，例如：Office 文档、存档、多媒体、可执行文件、PDF 文件、编码文件、图形或系统文件。
检测名称	被测恶意软件名称。

字段	说明
处理结果	文件的 恶意软件防护处置情况： • “恶意软件”(Malware) 表示本地恶意软件分析识别出恶意软件，AMP 云将文件归类为恶意软件，或文件威胁评分超过文件策略中定义的恶意软件阈值。 • “干净”(Clean) 表示 AMP 云将文件归类为干净，或者用户将该文件添加到干净列表。 • “未知”(Unknown) 表示系统查询了 AMP 云，但是尚未为文件分配处置情况；换句话说，AMP 云尚未将文件分类。 • “自定义检测”(Custom Detection) 表示用户将文件添加到自定义检测列表。 • “不可用”(Unavailable) 表示系统无法查询 AMP 云。您可能看到很少一部分事件为此处置；这是预期行为。 • “不适用”表示“检测文件”或“阻止文件”规则处理了文件，Cisco Secure Firewall Management Center未查询 AMP 云。
域	检测到捕获文件的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

字段	说明
动态分析状态	以下一个或多个值表示是否已提交文件以供动态分析： • “分析完成”(Analysis Complete) - 已提交文件以供动态分析且收到威胁评分和动态分析摘要报告 • “容量已处理”(Capacity Handled) - 已存储文件，因为当前无法提交文件 • “容量已处理（网络问题）”(Capacity Handled [Network Issue]) - 已存储文件，因为由于网络连接问题而无法提交文件 • “容量已处理（速率限制）”(Capacity Handled [Rate Limit]) - 已存储文件，因为已达到最大提交数量而无法提交文件 • 设备未激活 - 未提交文件，因为未在内部 Secure Secure Malware Analytics 设备上激活设备。如果看到此状态，请联系支持部门。 • “失败（分析超时）”(Failure [Analysis Timeout]) - 文件已提交，但 AMP 云尚未为其返回结果 • “失败（无法运行文件）”(Failure [Cannot Run File]) - 文件已提交，但 AMP 无法在测试环境中运行文件 • “失败（网络问题）”(Failure [Network Issue]) - 文件由于网络连接失败而未提交 • “未发送以供分析”(Not Sent for Analysis) - 文件未提交 • “不可疑（未发送以供分析）”(Not Suspicious [Not Sent For Analysis]) - 文件预先分类为非恶意软件 • 之前已分析 - 具有缓存威胁评分的文件，表示之前已发送 • 拒绝分析 - 根据静态分析，文件不太可能构成风险，例如，因为它不包含动态元素。 • “已发送以供分析”(Sent for Analysis) - 文件被预先分类为恶意软件，并排队等待动态分析
动态分析状态已更改	上一次文件分析状态发生变化的时间。
文件名	最近检测到的与文件 SHA-256 散列值相关的文件名。
上次更改时间	上一次更新与该文件有关信息的时间。
上次发送时间	最近一次向 AMP 云提交文件以供动态分析的时间。

字段	说明
本地恶意软件分析状态	下列值之一表示系统是否对文件执行本地恶意软件分析： • “分析完成”(Analysis Complete) - 系统使用本地恶意软件分析检查文件，并对文件预先分类。 • “分析失败”(Analysis Failed) - 系统尝试使用本地恶意软件分析检查文件但已失败。 • “手动请求已提交”(Manual Request Submitted) - 用户提交文件以供本地恶意软件分析 • “未分析”(Not Analyzed) - 系统未使用本地恶意软件分析检查文件
SHA256	文件的SHA-256散列值以及显示最近检测文件事件和文件处置情况的网络文件轨迹图标。要查看网络文件轨迹，请点击轨迹图标。
存储状态	表示文件是否存储于受管设备： • 已存储文件 • 未存储（处置情况待定）(Not Stored [Disposition Was Pending])
威胁评分	与此文件相关的最新威胁评分。 要查看动态分析总结报告，请点击威胁评分图标。
类型	文件类型；例如 HTML 或 MSEXE。

存储的文件下载

设备存储文件后，只要 Cisco Secure Firewall Management Center可以与该设备保持通信并且未删除文件，就可以将文件下载本地主机以供长期存储和分析，并手动分析文件。您可以从相关文件事件、恶意软件事件、捕获文件视图或文件轨迹中下载文件。

由于恶意软件有害，默认情况下，您必须在每次下载文件时进行确认。但是，可以在“用户首选项”(User Preferences) 中禁用确认。

因为性质为Unknown的文件可能包含恶意软件，当您下载文件时，系统会首先将该文件存档至 `.zip` 压缩包。`.zip` 文件名包含文件处置情况和文件类型（如有）以及 SHA-256 散列值。您可以对 `.zip` 文件采用密码保护以防意外解压缩。可以在“用户首选项”(User Preferences) 中编辑或删除默认 `.zip` 文件密码。

注意 思科强烈建议**不要**下载恶意软件，因为其可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。

手动提交文件以供分析

手动提交文件以进行分析时，系统会运行本地分析，然后将这些文件提交到云以进行动态分析。但是，如果文件策略中未启用本地分析，您需要手动提交文件进行分析，则系统仅发送文件进行动态分析。

除了可执行文件，您也可以提交不适合自动提交的文件类型，例如 .swf、.jar 和其他类型。这样，您可以更快速地分析多种文件（而不管处置情况为何），并准确确定事故具体成因。

注释 系统会检查 AMP 云，确定动态分析合格文件类型列表是否更新（不超过一日一次）以及可提交的最小和最大文件大小。

根据具体情况，有两种方法可以提交文件进行分析：

开始之前

为了手动提交捕获的文件以进行分析，必须配置一个或多个文件规则来存储文件。有关信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 网络恶意软件保护和文件策略 一章。

过程

步骤 1 要提交单个文件进行分析，请执行以下操作：

a) 选择以下一个选项：

- **分析 > 文件 > 文件事件**
- **分析 > 文件 > 恶意软件事件**
- **Analysis（分析）> Files（文件）> Captured Files（捕获的文件）**

b) 点击 **<事件类型或文件> 的表视图**。

c) 右键点击表中的文件，然后选择**分析文件 (Analyze File)**。

步骤 2 要提交多个捕获的文件以进行分析（一次最多 25 个），请执行以下操作：

a) 选择**分析 > 文件 > 捕获的文件**。

b) 选中每个要分析的文件旁边的复选框。

c) 点击**分析**。

网络文件轨迹

网络文件轨迹功能映射出主机怎样在网络中传送文件，包括恶意软件文件。轨迹以图表形式展示文件传输数据、文件处置情况以及是否阻止文件传送或是否隔离文件。您可以确定哪些主机和用户可能已传送恶意软件、哪些主机存在风险，并观察文件传送趋势。

您可以跟踪具有 AMP 云分配处置情况的所有文件。系统可以使用与检测和阻止来自恶意软件防护和面向终端的 AMP 的恶意软件相关的信息来建立轨迹。

最近检测到的恶意软件和分析的轨迹

“网络文件轨迹列表”(Network File Trajectory List) 页面显示网络上最近检测到的恶意软件，以及最近查看过轨迹映射的文件。从这些列表中，可以查看最近在网络上查看每个文件的时间，该文件的 SHA-256 散列值、名称、类型、当前文件处置情况、内容（对于存档文件），以及与该文件相关联的事件的数量。

该页面还包含一个可让您定位文件的搜索框，可基于 SHA-256 哈希值、文件名或传送或接收文件主机的 IP 地址进行查找。定位一个文件后，您可以点击**文件 SHA256** 值，查看详细轨迹映射。

网络文件轨迹详细视图

您可以通过查看网络文件详细轨迹在网络中跟踪文件。搜索文件的 SHA 256 值或点击网络文件轨迹列表中的**文件 SHA 256 (File SHA 256)** 链接可查看该文件的详细信息。

“网络文件轨迹详细信息”(Network File Trajectory Details) 页面包含三个部分：

- 摘要信息 - 文件的轨迹页面显示文件的相关摘要信息，包括文件识别信息、首次及最近一次在网络上查看该文件的时间及查看该文件的用户、与该文件相关的事件和主机数量以及该文件的当前处置情况。从本节开始，如果受管设备已存储文件，您可以进行本地下载、提交文件进行动态分析或将文件添加至文件列表。
- 轨迹映射 - 文件的轨迹映射直观地跟踪从网络上第一次检测到文件至最近一次检测到该文件的情况。该映射显示出主机传送或接收文件的时间、传送文件频率和阻止或隔断文件的时间。数据点之间的垂直线代表文件在主机之间传送。连接数据点的水平线表示随时间推移的主机文件活动。

  该映射同时显示该文件生成文件事件的频率，以及系统为文件分配性质或回溯性质的时间。您可以在映射中选择数据点，并突出显示追溯至主机第一次传输该文件的实例的路径；此路径还将贯穿每次主机作为该文件接收方或发送方的事例，并识别所涉及的用户。
- 相关事件 -“事件”(Events) 表列出映射中各数据点的事件信息。使用该表和映射，您可以准确定位特定文件事件、网络上传送或接收该文件的主机和用户、映射中的相关事件以及表中受选定值限制的其他关联事件。

网络文件轨迹摘要信息

对于“网络文件轨迹”(Network File Trajectory) 列表中显示的文件，“详细信息”(Details) 页面顶部会显示以下摘要信息。

提示 要查看相关文件事件，请点击字段值链接。在新窗口中打开文件事件默认工作流程首页，显示包含选定值的所有文件事件。

表 *122:* 网络文件轨迹摘要信息字段

名称	说明
存档内容	对已检查存档文件，指存档文件包含的文件数量。
当前处置	可以为下列恶意软件防护 文件安全状态之一： • 恶意软件 (Malware) 表示 AMP 云将文件分类为恶意软件，本地恶意软件分析识别恶意软件，或者文件的威胁评分超过文件策略中定义的恶意软件阈值。 • 干净 (Clean) 表示 AMP 云将文件归类为干净，或者用户将该文件添加到干净列表。 • 未知 (Unknown) 表示系统查询了 AMP 云，但是尚未为文件分配处置情况；换句话说，AMP 云尚未将文件分类。 • Custom Detection 表示用户将文件添加到自定义检测列表。 • 不可用 (Unavailable) 表示系统无法查询 AMP 云。您可能看到很少一部分事件为此处置；这是预期行为。 • 不适用表示“检测文件”或“阻止文件”规则处理了文件，Cisco Secure Firewall Management Center未查询 AMP 云。
检测名称	本地恶意软件分析检测到的恶意软件的名称。
事件计数	网络上看到的与该文件相关事件的数量，以及如检测到超过250个事件时映射中显示的事件数量。
文件类别	文件类型的一般类别，例如 Office Documents 或 System Files。
文件名	事件关联文件的名称，如网络上所示。 如果一个SHA-256哈希值与多个文件名关联，列出最近检测到的文件名。您还可通过点击more将其展开以查看其余文件名。
文件 SHA256	文件的 SHA-256 散列值。 默认情况下以压缩格式显示哈希值。要查看完整哈希值，请将指针悬停在上方。如果一个文件名与多个 SHA-256 哈希值关联，将指针悬停在链接上方查看全部哈希值。
文件大小 (KB)	文件大小（千字节）。

名称	说明
文件类型	文件类型，例如 HTML 或 MSEXE。
首次查看时间	恶意软件防护 或面向终端的 AMP 首次检测到文件以及主机（第一个上传该文件和相关用户的身份信息的主机）的 IP 地址的时间。
上次查看时间	恶意软件防护 或面向终端的 AMP 最近一次检测到文件以及主机（最后一个下载该文件和相关用户的身份信息的主机）的 IP 地址的时间。
父应用	在面向终端的 AMP 执行检测时访问恶意软件文件的客户端应用。这些应用与网络发现或应用控制无关联。
出现时间	发送或接收文件的主机数量。因为一台主机可以在不同时间上传和下载文件，在 Seen On Breakdown 字段中的主机总数可能与发送方总数加上接收方总数之和并不匹配。
中断时出现	发送文件的主机数量，然后紧接接收文件的主机数量。
威胁名称	通过面向终端的 AMP 与检测到的恶意软件相关联的威胁的名称。
威胁评分	文件的威胁评分。

网络文件轨迹映射和相关事件列表

文件轨迹映射的 y 轴包含与该文件交互的所有主机 IP 地址的列表。IP 地址按照系统在主机上首次检测到该文件的时间降序排列。每行都包含与该 IP 地址相关的所有事件，无论是单一文件事件、文件传送还是回溯事件。x 轴包含系统检测到各个事件的日期和时间。时间戳按时间顺序排列。如果一分钟内发生了多个事件，则在同一栏中列出所有事件。您可以水平或垂直滚动映射，以查看其他事件和 IP 地址。

映射中显示多达 250 个与文件 SHA-256 散列值有关的事件。如有超过 250 个事件，则映射上只显示前十个，并用 **箭头**截略其他事件。然后映射再显示剩下的 240 个事件。

系统将在新窗口中显示“文件事件”默认工作流程的首页，同时显示基于文件类型受限的所有其他事件。如果未显示面向终端的 AMP 生成的恶意软件事件，您必须切换到“恶意软件事件”表进行查看。

每个数据点都表示一个事件及其文件处置情况，如映射下方图例中所述。例如，“恶意软件阻止”(Malware Block) 事件图标结合了“恶意处置情况”(Malicious Disposition) 图标和“阻止事件”(Block Event) 图标。

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”）包括一个图标。回溯事件在栏中为检测到文件的各个主机显示一个图标。文件传送事件始终包括两个图标，一个文件发送图标和一个文件接收图标，两者之间用垂直线连接。箭头表示从发送方到接收方的文件传送方向。

要跟踪文件在网络中的历程，可以点击任意数据点突出显示一个轨迹，其中包括与选定数据点相关的所有数据点。这其中包括与下列类型的事件相关的数据点：

- 无论关联 IP 地址作为发送方还是接收方的任何文件传送
- 涉及关联 IP 地址的任何面向终端的 AMP 生成的恶意软件事件（“基于终端的恶意软件事件”）

- 如果涉及另一个 IP 地址，无论该关联 IP 地址作为发送方还是接收方的所有文件传送
- 如果涉及另一个 IP 地址，涉及该 IP 地址的任何面向终端的 AMP 生成的恶意软件事件（“基于终端的恶意软件事件”）

同时突出显示与任何突出显示的数据点相关的所有 IP 地址和时间戳。同时突出显示事件表中的相应事件。如果一条轨迹中包含截略事件，则用虚线突出显示轨迹本身。可能有截略事件与轨迹相交，但并不在映射中进行显示。

使用网络文件轨迹

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。

提示 如果您的组织已部署 Cisco Secure Endpoint，则该产品还具有网络文件轨迹功能。要从 管理中心 跳转至 Cisco Secure Endpoint，请参阅 使用 Cisco Secure Endpoint 控制台中的事件数据，第 827 页。有关 Cisco Secure Endpoint中的文件轨迹功能的详细信息，请参阅 Cisco Secure Endpoint 文档。

开始之前

如果您正在使用 恶意软件防护，则需要 恶意软件防御 许可证。

您必须是管理员或安全分析师用户才能执行此任务。

过程

步骤 1 选择**分析** > **文件** > **网络文件轨迹**。

提示 您还可以从情景管理器、控制面板或具有文件信息的事件视图来访问文件轨迹。

步骤 2 点击列表中的**文件 SHA 256 (File SHA 256)** 链接。

步骤 3 或者，在搜索字段输入完整的 SHA-256 散列值、主机 IP 地址或要跟踪的文件的名称，然后按 Enter 键。

提示 如果只有一个结果匹配，系统将显示该文件的 Network File Trajectory 页面。

步骤 4 在“摘要信息”(Summary Information) 部分中，可以执行以下操作：

- 将文件添加到文件列表 - 要在干净的列表或自定义检测列表中添加或删除文件，请点击 **编辑**（）。
- 下载文件 - 要下载文件，请点击下 **下载**（），并在出现提示时，确认要下载该文件。如果该文件无法下载，则此下载文件呈灰色显示。
- 报告 - 点击威胁评分，查看“动态分析摘要”报告。
- 提交动态分析 - 点击 **AMP 云** 以提交文件进行动态分析。如果该文件无法提交或您无法连接到 AMP 云，则此 AMP 云呈灰色显示。

- 查看存档内容 - 要查看有关存档文件内容的信息，请点击 **视图**（  ）。
- 查看文件组成 - 要查看文件的组成，请点击 **文件列表**。如果系统未生成文件组成报告，则此文件列表呈灰色显示。
- 查看威胁评分相同的捕获文件 - 点击威胁评分链接，查看具有该威胁评分的所有捕获文件。

注释 思科强烈建议**不要**下载恶意软件，因为其可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。

步骤 5 在轨迹映射上，可以执行以下操作：

- 确定第一个实例 - 点击一个 IP 地址，确定第一次发生涉及 IP 地址的文件事件的位置。突出显示连至该数据点的路径，以及与第一个文件事件相关的任何介于其间的文件事件和 IP 地址。同时突出显示事件表中的相应事件。如当前不可见，映射会滚动至该数据点。
- 跟踪 - 点击任意数据点，突出显示包含与所选数据点相关的所有数据点的轨迹，从而通过网络跟踪文件的进度。
- 查看隐藏事件 - 点击箭头，查看“文件摘要”事件视图中未显示的所有事件。
- 查看匹配文件事件 - 将指针悬停在 **匹配文件事件** 上方，查看事件的摘要信息。如果点击任何事件摘要信息链接，则会在新窗口中显示“文件事件”(File Events) 默认工作流程的首页，其中包含基于文件类型限制的所有其他事件。“文件摘要”(File Summary) 事件视图在新窗口中打开，显示与所点击的条件值相匹配的所有文件事件。

步骤 6 在“事件”(Events) 表中，可以执行以下操作：

- 突出显示 - 选择表行，突出显示映射中的数据点。如当前不可见，映射会滚动至选定文件事件并显示该事件。
- 排序 - 点击列标题以按升序或降序对事件进行排序。

使用 Cisco Secure Endpoint 控制台中的事件数据

如果您的组织已部署 Cisco Secure Endpoint，则您可以在 Cisco Secure Endpoint 控制台中查看 恶意软件事件数据，并可以使用该应用的全局网络文件轨迹工具。

提示 有关使用 Cisco Secure Endpoint 及其控制台的信息，请参阅控制台中的在线帮助或 https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html中提供的其他文档

要从 Cisco Secure Firewall Management Center访问 Cisco Secure Endpoint 控制台，请执行以下操作之一：

开始之前

- 必须配置与 Cisco Secure Endpoint 的连接（请参阅 集成 *Firepower* 和 *Cisco Secure Endpoint* 中的《Cisco Secure Firewall Management Center 设备配置指南》）并且 Cisco Secure Firewall Management Center 必须能够连接到 AMP 云。
- 您将需要您的 Cisco Secure Endpoint 凭证。
- 您必须是管理员用户才能执行此任务。
- 如果要从 管理中心中的恶意软件事件转向别处的恶意软件事件，请确保正确启用了 Cisco Secure Endpoint 上下文交叉启动选项。请参阅使用基于 Web 的资源的事件调查，第 605 页下的主题。

过程

步骤 1 方法 1：

a) 选择**集成 (Integration)** > **AMP** > **AMP 管理 (AMP Management)**。

b) 点击表中的云名称。

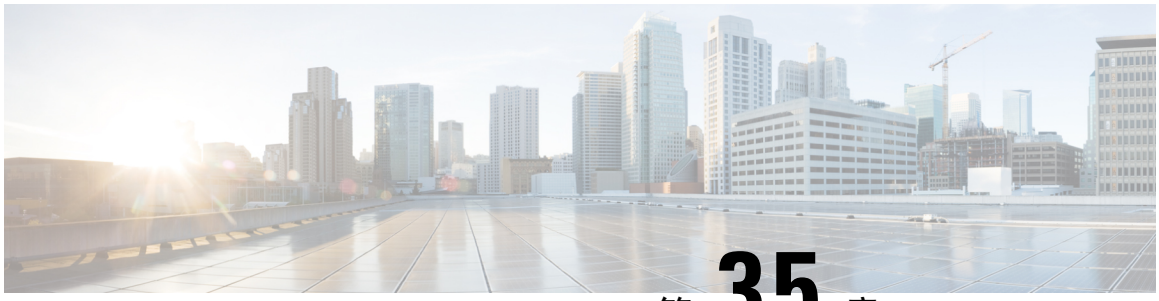
步骤 2 方法 2：

a) 导航到**分析** > **文件**下的表中的恶意软件事件。

b) 右键点击文件 SHA，然后选择 Cisco Secure Endpoint 选项。

文件/恶意软件事件和网络文件轨迹的历史记录

功能	最低 管理中心	最低 威胁防御	详情
文件和恶意软件事件中的 MITRE 信息。	7.4	7.4	系统现在在文件和恶意软件事件中包含 MITRE 信息（来自本地恶意软件分析）。您可以在经典和统一事件视图中查看MITRE信息。请注意，默认情况下，MITRE 列在两个事件视图中都是隐藏的。
用于动态分析的改进的预分类文件。	6.7	任意	额外的评估可避免发送不必要的文件以进行动态分析。未根据此评估发送到云的文件的新动态分析状态为 **已拒绝分析**。 新增/修改后的屏幕： **分析** > **捕获的文件** > **捕获文件的表视图**
系统日志中连接事件的唯一标识符。	6.4.0.4	任意	以下系统日志字段共同唯一标识连接事件并在文件和恶意软件事件的系统日志中显示：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。
通过系统日志发送文件和恶意软件事件	6.4	任意	本章中的字段说明指定了系统日志消息中包含的字段。 有关配置信息，请参阅 文件和恶意软件事件系统日志的配置位置，第 618 页。



第 35 章

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 831 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 Firepower 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 Firepower 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 833 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 836 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、安全情报、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， 第 877 页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** > **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 846 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** > **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 846 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** > **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 846 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 ，第 932 页

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，第 890 页
漏洞停用，第 891 页

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 852 页
停用多个漏洞，第 893 页

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 852 页
停用多个漏洞，第 893 页
操作系统身份冲突，第 836 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**。

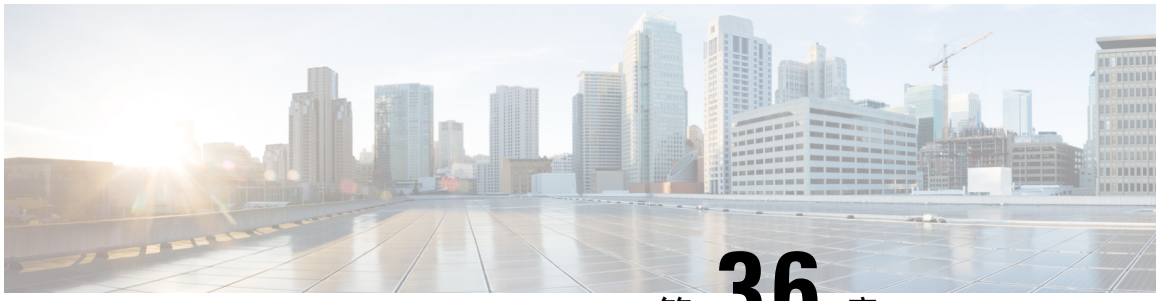
系统扫描主机并将结果添加到主机配置文件中。

相关主题

Nmap 扫描自动化 ，第 473 页

主机配置文件的历史记录

功能	最低 管理中心	最低 威胁防御	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



第 36 章

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	兼容	兼容
用户危害表现	兼容	兼容
活动会话	兼容	兼容
用户活动	兼容	兼容
用户	兼容	兼容
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 857 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，第 661 页中所述。
- 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 858 页
协议明细部分，第 859 页
应用协议明细部分，第 859 页
操作系统明细部分，第 859 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 862 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 882 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 869 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 860 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 868 页。
- 主机数据 - 请参阅查看主机数据， 第 870 页。
- 主机属性数据 - 请参阅查看主机属性， 第 875 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 878 页。
- 服务器数据 - 请参阅查看服务器数据， 第 882 页。
- 应用数据 - 请参阅查看应用数据， 第 885 页。
- 应用详细信息数据 - 请参阅查看应用详细信息数据， 第 887 页。
- 活动会话数据 - 请参阅查看活动会话数据， 第 902 页。
- 用户数据 - 请参阅查看用户数据， 第 905 页。
- 用户活动数据 - 请参阅查看用户活动数据， 第 907 页。
- 网络映射 - 请参阅查看网络映射， 第 588 页。

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 (Analysis)** > **用户 (Users)** > **活动会话 (Active Sessions)** 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，第 650 页。
- 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，第 647 页。
- 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，第 666 页。
- 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，第 642 页
从 管理中心 数据库清除数据，第 496 页

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 866 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 863 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** > **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，第 661 页中所述。

  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 860 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 868 页。

相关主题

使用发现和身份工作流程，第 860 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，第 671 页

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** > **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 860 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 870 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 877 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 874 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 875 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，第 671 页
操作系统身份冲突，第 836 页

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，第 977 页

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，第 925 页

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 875 页
配置设置属性补救，第 998 页

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** > **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 860 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 876 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 877 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，第 671 页

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、安全情报、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，第 840 页

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 > 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 860 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 880 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，第 671 页

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** > **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 860 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 883 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，第 671 页

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** > **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 860 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 886 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，第 605 页
- 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，第 605 页。

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，第 671 页

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** > **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 860 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 888 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，第 605 页
- 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，第 605 页。

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，第 671 页

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，第 108 页

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，第 671 页

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，第 852 页
停用单个漏洞，第 852 页
停用多个漏洞，第 893 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 860 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 893 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 892 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** > **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** > **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，第 852 页
停用单个漏洞，第 852 页

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 860 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 894 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。(http://www.securityfocus.com/bid/)

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，第 671 页

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 902 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 903 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 906 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。

表 *123:* 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。	不兼容	是	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	否	兼容
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。 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。	不兼容	是	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。	兼容	兼容	兼容
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

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
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）。	兼容	是	否
说明	有关会话、用户或用户活动的详细信息（如有）。	不兼容	不兼容	兼容
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	否	兼容
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。	兼容	兼容	兼容
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。	兼容	兼容	兼容

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
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。	不兼容	否	兼容
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。	不兼容	不兼容	兼容
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。	不兼容	不兼容	兼容
事件	用户活动事件类型。	不兼容	不兼容	兼容
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。	兼容	是	否

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
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。	不兼容	不兼容	兼容
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。	兼容	是	否
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。	兼容	是	否
登录时间	用户发起会话的日期和时间。	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

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
领域	与用户关联的身份领域。 注释 Azure AD 领域用户的活动会话仅显示在**活动会话 (Active Sessions)** 新 UI 布局中，而不显示在旧版 UI 中。	兼容	兼容	兼容
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。	不兼容	不兼容	兼容
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。	不兼容	否	兼容
时间	系统检测到用户活动的时间。	不兼容	不兼容	兼容
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）。	兼容	是	否
用户名	与用户关联的用户名。	兼容	兼容	兼容
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	否	兼容

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
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。	不兼容	不兼容	兼容
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	否	兼容
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。	不兼容	不兼容	兼容
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	否	兼容
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	否	兼容
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。	不兼容	不兼容	兼容
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	否	兼容

字段	说明	活动会话表	用户表 (Users Table)	用户活动表
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	否	兼容
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	否	兼容

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 903 页和用户活动数据，第 906 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 (Analysis)** > **用户 (Users)** > **活动会话 (Active Sessions)**。
- 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 860 页。
- 有关表中各列内容的详细信息，请参阅活动会话数据，第 902 页和用户相关字段，第 896 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)

身份源	登录类型	存储的用户数据
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)
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 860 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 896 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 (Analysis)** > **用户 (Users)** > **用户活动 (User Activity)**。
- 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，第 661 页。

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 860 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 896 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 880 页
- 编辑单台主机或单个用户的危害表现规则状态，第 880 页
- 解决危害表现标记，第 881 页
- 查看危害表现标记的源事件，第 881 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

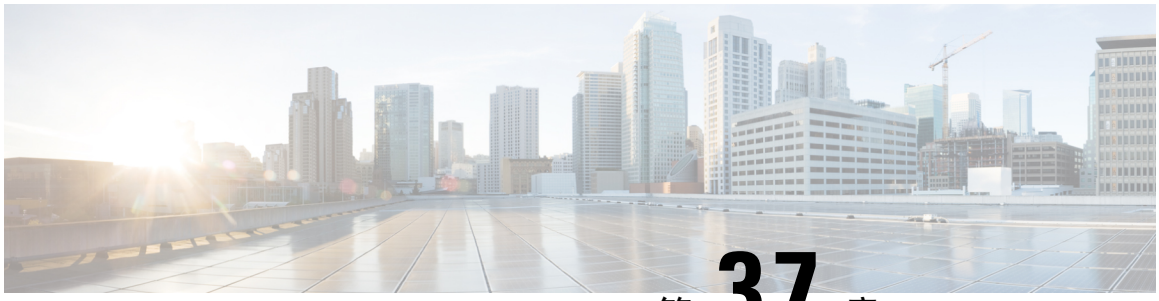
此时您有两种选择：

- 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 *124:*

功能	最低 管理中心	最低 威胁防御	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



第 37 章

关联事件和合规性事件

以下主题介绍如何查看关联事件和合规性事件。

查看关联事件

当活动的关联策略中的关联规则触发时，系统生成关联事件并将其记录至数据库。

注释 当活动的关联策略中的合规 allow 名单触发时，系统生成 an allow 名单事件。

您可以查看关联事件表，然后根据查找的信息操作事件视图。

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。

您在访问关联事件时看到的页面将随您所使用的工作流程而变化。您可以使用预定义的工作流程，其中包括关联事件的表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

开始之前

您必须是 管理员 或 安全分析师 用户才能执行此任务。

过程

步骤 1 选择**分析** > **关联** > **关联事件** 。

或者，要使用不同的工作流程，包括自定义工作流程，请按工作流程标题点击（**切换工作流程**）**([switch workflow])**。

提示 如果使用的是不包含关联事件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**关联事件 (Correlation Events)**。

步骤 2 或者，调整时间范围，如更改时间窗口，第 661 页中所述。

步骤 3 执行下列操作之一：

- 要了解有关显示的列的详细信息，请参阅关联事件字段，第 912 页。
- 要查看 IP 地址的主机配置文件，请点击显示在 IP 地址旁边的主机配置文件。
- 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)**。
- 要对事件进行排序和限制，或者要在当前工作流程页面中导航，请参阅使用工作流程，第 642 页。
- 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- 要向下展开到工作流程中的下一个页面，限制具体值，请参阅使用向下钻取页面，第 650 页。
- 要删除部分或全部关联事件，请选中要删除的事件旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**，并确认要删除当前限制视图中的所有事件。
- 要导航至其他事件视图以查看关联事件，请参阅工作流程间导航，第 666 页。
- 要查看 Firepower 系统外部可用源中的数据，请右键点击事件值。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，第 605 页
- 要收集有关事件的情报，请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。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，第 605 页。

相关主题

数据库事件限制，第 55 页
工作流程页面，第 646 页

关联事件字段

当关联规则触发时，系统会生成关联事件。下表介绍关联事件表中可以查看和搜索的字段。

表 *125:* 关联事件字段

字段	说明
说明	关联事件的说明。说明中的信息取决于规则触发方式。 例如，如果操作系统的信息更新事件触发规则，则系统显示新的操作系统名称和可信度。
设备	生成触发策略违规的事件的设备的名称。

字段	说明
域	其受监控流量触发了策略违规的设备的域。仅当曾经配置管理中心以实现多租户时，此字段才存在。
影响	基于入侵数据、发现数据和漏洞信息之间的关联分配给关联事件的影响级别。 搜索此字段时，有效值（不区分大小写）包括 `Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、`Impact 3`、`Impact Level 3`、`Impact 4` 和 `Impact Level 4`。请勿使用影响图标颜色或部分字符串（例如，请勿使用 `blue`、`level 1` 或 `0`）。
“入口接口”(Ingress Interface) 或“出口接口”(Egress Interface)	触发策略违规的入侵或连接事件的入口或出口界面。
“入口安全区域”(Ingress Security Zone) 或“出口安全区域”(Egress Security Zone)	触发策略违规的入侵或连接事件的入口或出口安全区域。
内联结果	以下任一项： • 一个黑色向下箭头，表示系统丢弃触发入侵规则的数据包 • 一个灰色向下箭头，表示如果启用**内联时丢弃 (Drop when Inline)** 入侵策略选项，则系统已经丢弃内联中的数据包、交换或路由部署 • 空白，表示触发的入侵规则未设置为“丢弃并生成事件”(Drop and Generate Events) 使用此字段搜索入侵事件触发的策略违规时，请输入： • `dropped`，用来指定是否已经在内联、交换的或路由的部署中丢弃数据包 • `would have dropped`，用于指定当入侵策略设置为在内联、交换的或路由的部署中丢弃数据包时是否已丢弃数据包 请注意，不管规则状态或入侵策略的丢弃行为如何（包括当内联集处于分流模式下），系统都无法在被动部署情况下丢失数据包。
策略	违反的策略的名称。
优先级	关联事件的优先级，由触发的规则或违规的关联策略的优先级确定。搜索此字段时，请输入 `none` 表示无优先级。
规则	触发策略违规的规则的名称。
安全情报类别 (Security Intelligence Category)	代表或包含触发策略违规的事件中的被受阻的 IP 地址的对象的名称。 搜索此字段时，请指定与触发策略违规的关联事件相关联的安全情报类别。安全情报类别可能是安全情报对象的名称、全局阻止列表、自定义安全情报列表或源，或者情报源中的其中一个类别。

字段	说明
“源大洲”(Source Continent) 或“目标大洲”(Destination Continent)	与触发策略违规的事件中的源或目标主机 IP 地址相关联的大洲。
“源国家/地区”(Source Country) 或“目标国家/地区”(Destination Country)	与触发策略违规的事件中的源或目标主机 IP 地址相关的国家/地区。
“源主机重要性”(Source Host Criticality) 或“目标主机重要性”(Destination Host Criticality)	涉及关联事件的源主机或目标主机的用户分配的主机重要性：无 (None)、低 (Low)、中 (Medium) 或高 (High)。 请注意，只有基于发现事件、主机输入事件或连接事件按规则生成的关联事件才包含源主机重要性。
“源 IP”(Source IP) 或“目标 IP”(Destination IP)	触发策略违规的事件中的源主机或目标主机的 IP 地址。
“源端口/ICMP 类型”(Source Port/ICMP Type) 或“目标端口/ICMP 代码”(Destination Port/ICMP Code)	与触发策略违规的事件有关的源流量的源端口或 ICMP 类型或者目标流量的目标端口或 ICMP 代码。
“源用户”(Source User) 或“目标用户”(Destination User)	登录触发策略违规的事件中的源主机或目标主机的用户的姓名。
时间	生成关联事件的日期和时间。此字段不可搜索。
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。此字段不可搜索

相关主题

事件搜索，第 671 页

使用合规 允许 名单工作流程

管理中心 提供了一组工作流程，可用于分析为您的网络生成的 allow 名单事件和违规。工作流程与网络映射和控制面板一起构成关于网络资产合规性的关键信息的来源。

系统为 allow 名单事件和违规提供预定义工作流程。也可创建自定义工作流程。在使用合规 allow 名单工作流程时，可以执行许多常见操作。

开始之前

您必须是 管理员、 安全分析师或 发现管理员 用户才能执行此任务。

过程

步骤 1 使用 **分析** > **关联** 菜单访问 an allow 名单工作流程。

步骤 2 您有以下选择：

- “切换工作流程”(Switch Workflow) - 要使用不同的工作流程（包括自定义工作流程），请点击（**切换工作流程**）**([switch workflow])**。
- “时间范围”(Time Range) - 要调整时间范围（如果未显示事件，则非常有用），请参阅更改时间窗口，第 661 页。
- 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**()，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** 。
- “用户配置文件”（仅事件）- 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)**。
- 限制 - 要限制显示的列，请在要隐藏的列标题中点击 **关闭**（×） 在显示的弹出窗口中，点击 **Apply**。

  提示 要隐藏或显示其他列，请先选择或清除相应的复选框，然后点击**应用 (Apply)**。要将已禁用列添加回视图中，请展开搜索限制条件，然后点击“已禁用列”(Disabled Columns) 下的列名称。

- 向下展开 - 请参阅使用向下钻取页面，第 650 页。
- “排序”(Sort) - 要对工作流程中的数据排序，请点击列标题。再次点击列标题以反转排列顺序。
- “导航此页面”(Navigate This Page) - 请参阅工作流程页面遍历工具，第 647 页。
- “在页面之间导航”(Navigate Between Pages) - 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- “在事件视图之间导航”(Navigate Between Event Views) - 要导航至其他事件视图以查看关联事件，请点击**跳转至 (Jump to)** 并从下拉列表中选择事件视图。
- “删除事件”(Delete Events)（仅事件）- 要删除当前限制视图中的部分或全部项目，请选中要删除的项目旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**。

相关主题

工作流程页面，第 646 页
配置事件视图设置，第 193 页

查看 允许 列表事件

完成初始评估后，每当受监控的主机违反有效的 allow 名单，系统会生成 an *allow* 名单事件 。 名单事件是特殊类型的关联事件，会被记录到 管理中心 关联事件数据库中。

您可以使用 管理中心查看合规 allow 名单事件表。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 allow 名单事件时系统显示的页面取决于您使用的工作流程。可以使用预定义的工作流程，最终会产生事件的表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

开始之前

您必须是 管理员、 安全分析师或 发现管理员 用户才能执行此任务。

过程

步骤 1 选择**分析** > **关联** > **允许列表事件**。

步骤 2 您有以下选择：

- 要执行基本工作流程操作，请参阅使用合规 允许 名单工作流程，第 914 页。
- 要了解有关表中各列内容的详细信息，请参阅允许 名单事件字段，第 916 页。
- 要查看更多选项，请右键点击表中的值。

允许 名单事件字段

允许 名单事件（您可以通过工作流程查看和搜索白名单事件）包含以下字段。

设备

检测到 allow 名单违规行为的受管设备的名称。

说明

说明 allow 名单是如何被违反的。例如：

```
Client “AOL Instant Messenger” is not allowed.
```

涉及应用协议的违规指明应用协议的名称和版本，以及所使用的端口和协议（TCP 或 UDP）。如果限制禁止某个特定的操作系统，描述中会包含操作系统的名称。例如：

```
Server "ssh / 22 TCP (OpenSSH 3.6.1p2)" is not allowed on Operating System
“Linux Linux 2.4 or 2.6”.
```

域

已变为不符合 allow 名单的主机的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

主机重要性

用户向不符合 allow 名单的源主机所分配的主机重要性：“无”、“低”、“中” 或“高”。

IP 地址

已变为不符合 allow 名单的主机的 IP 地址。

策略

被违反的关联策略的名称，即包含该 allow 名单的关联策略。

端口

与触发应用协议 allow 名单违规（违规应用协议造成的违规）的发现事件关联的端口（如有）。对于其他类型的 allow 名单违规活动，该字段为空白。

优先级

策略或触发策略违规的 allow 名单所指定的优先级。根据关联策略中 allow 名单的优先级或关联策略自身的优先级来确定。请注意， allow 名单的优先级优先于策略的优先级。搜索此字段时，请输入 `none` 表示无优先级。

时间

allow 名单事件生成时的日期和时间。此字段不可搜索。

用户

登录已变为不符合 allow 名单的主机的任何已知用户的身份。

允许 名单

allow 名单的名称。

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。此字段不可搜索。

查看 允许 列表违规事件

系统会记录您的网络上的当前 *allow* 名单违规事件 。每个违规事件代表一个禁止在您的其中一台主机上运行的事件。如果主机变为合规，则系统将从数据库移除现已纠正的违规。

您可以使用 管理中心 查看所有活动 allow 名单的 allow 名单违规事件表。然后，可根据要查找的信息操纵事件视图。

访问 allow 名单违规事件时显示的页面因使用的工作流程而异。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。

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**分析** > **关联** > **允许列表违规**。

步骤 2 您有以下选择：

- 要执行基本工作流程操作，请参阅使用合规 允许 名单工作流程，第 914 页。
- 要了解有关表中各列内容的详细信息，请参阅允许 列表违规事件字段，第 918 页。
- 要查看更多选项，请右键点击表中的值。

允许 列表违规事件字段

可使用工作流程查看和搜索的允许 名单违规事件包含以下字段。

域

违规主机所在的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

信息

与该 allow 名单违规事件相关的任何可用的供应商、产品或版本信息。对于违反 an allow 名单的协议，此字段还指出违规是由网络协议还是传输协议造成的。

IP 地址

违规主机的 IP 地址。

端口

与触发应用协议 allow 名单违规（违规应用协议造成的违规）的事件关联的端口（如有）。对于其他类型的 allow 名单违规活动，该字段为空白。

协议

与触发应用协 allow 名单违规（违规应用协议造成的违规）的事件关联的协议（如有）。对于其他类型的 allow 名单违规活动，该字段为空白。

时间

该 allow 名单违规事件被检测到的日期和时间。

类型

allow 名单违规事件的类型，即该违规事件是否由于下列内容不合规而导致：

- 操作系统 (os)（搜索此字段时，请输入 **os** 或 **operating system**。）
- 应用协议（服务器）
- 客户端
- 协议
- Web 应用 (web)（搜索此字段时，请输入 **web application**。）

允许 名单

被违反的 allow 名单的名称。

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。此字段不可搜索。

补救状态事件

当补救触发时，系统会将补救状态事件记录到数据库。可在“补救状态”(Remediation Status) 页面中查看这些事件。可搜索、查看和删除补救状态事件。

相关主题

补救状态表字段，第 920 页

查看补救状态事件

您在访问补救状态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，其中包括补救的表视图。在表视图中，每个补救状态事件占一行。还可创建自定义工作流程，仅显示匹配特定需求的信息。

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

您必须是 管理员 用户才能执行此任务。

过程

步骤 1 选择**分析** > **关联** > **状态**。

步骤 2 或者，调整时间范围，如更改时间窗口，第 661 页中所述。

步骤 3 或者，要使用不同的工作流程，包括自定义工作流程，请按工作流程标题点击（**切换工作流程**）**([switch workflow])**。

提示 如果使用的是不包含补救表视图的自定义工作流程，则按工作流程标题点击（**切换工作流程**）**([switch workflow])** 菜单，然后选择**补救状态 (Remediation Status)**。

步骤 4 您有以下选择：

- 要了解有关显示的列的详细信息，请参阅补救状态表字段，第 920 页。
- 要对事件进行排序和限制，请参阅使用工作流程，第 642 页。
- 要导航至关联事件视图查看相关事件，请点击**关联事件 (Correlation Events)**。
- 要为当前页面添加书签以便快速返回该页面，请点击**将此页面加入书签 (Bookmark This Page)**。要导航至书签管理页面，请点击**查看书签 (View Bookmarks)**。
- 要根据表视图中的数据生成报告，请点击**报告设计器**，如从事件视图创建报告模板，第 509 页中所述。
- 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，第 650 页。
- 要从系统删除补救状态事件，请选中要删除的事件旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**，并确认要删除当前限制视图中的所有事件。
- 要搜索补救状态事件，请点击**搜索 (Search)**。

相关主题

使用工作流程，第 642 页

补救状态表字段

下表介绍补救状态表中可以查看和搜索的字段。

表 *126*: 补救状态字段

字段	说明
域	其受监控流量触发了策略违规（反过来又触发了补救）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。
策略	已违反并触发补救的关联策略的名称。
补救名称	已发起的补救的名称。

字段	说明
结果消息	描述在发起补救后所发生情况的消息。状态消息包括： • 补救成功完成 • 提供给补救模块的输入出错 • 补救模块配置出错 • 登录远程设备或服务器时出错 • 无法在远程设备或服务器上获得所需权限 • 登录远程设备或服务器时超时 • 执行远程命令或服务器时超时 • 远程设备或服务器不可达 • 已尝试补救，但是失败 • 未能执行补救程序 • 未知/意外错误 如已安装自定义补救模块，则可能出现自定义模块实现的其他状态消息。
规则	触发了补救的关联规则的名称。
时间	管理中心发起补救的日期和时间。
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。此字段不可搜索。

相关主题

事件搜索，第 671 页

使用补救状态事件表

您可以更改事件视图的布局或按字段值限制视图中的事件。

当禁用列时，除非稍后重新添加该列，否则该列在会话持续时间内处于禁用状态。如果禁用第一列，则会添加“计数”(Count) 列。

请注意，在表视图中点击某一行中的一个值时，会限制该表视图，且不会向下展开到下一个页面。

提示 表视图的页面名称中始终包含“Table View”。

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

您必须是 管理员 用户才能执行此任务。

过程

步骤 1 选择**分析** > **关联** > **状态**。

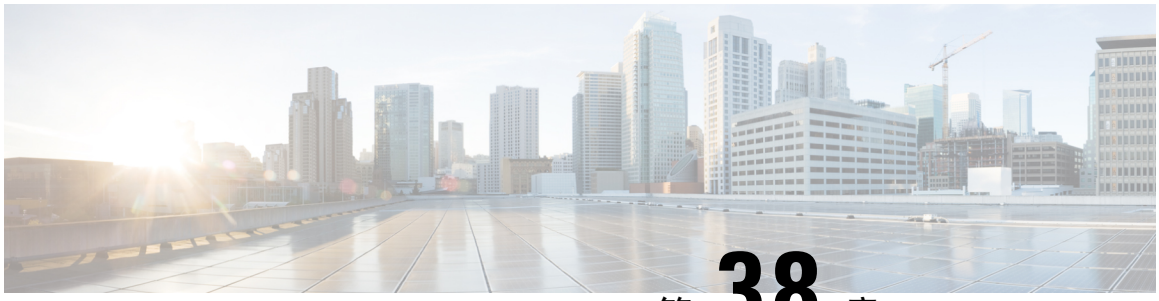
提示 如果使用的是不包含补救表视图的自定义工作流程，则按工作流程标题点击（**切换工作流程**）**([switch workflow])** 菜单，然后选择**补救状态 (Remediation Status)**。

步骤 2 您有以下选择：

- 要了解有关显示的列的详细信息，请参阅补救状态表字段，第 920 页。
- 要对事件进行排序和限制，请参阅使用工作流程，第 642 页。

第 IX 部分

关联和合规性



第 38 章

合规名单

以下主题介绍如何在将合规 allow 名单添加到关联策略之前对其进行配置。

合规 允许 名单简介

合规 *allow* 名单，有时缩写为 an *allow* 名单，是指定允许在网络上的主机上运行的操作系统、应用（Web 和客户端）以及协议的一系列条件。如果主机不在名单，系统也会生成一个事件（违反）。

合规 allow 名单有两个主要组件：

- 目标 是您选择用于合规评估的主机。您可以评估所有或部分受监控的主机，按照子网、VLAN 和主机属性进行限制。在多域部署中，您可以将域以及域内或跨域的子网作为目标。
- 主机配置文件指定面向目标的合规条件。全局主机配置文件与操作系统无关。您也可以配置操作系统特定的主机配置文件，主机配置文件为一个 allow 名单独有或跨 allow 名单共享。

Talos 情报小组 提供配有建议设置的默认 allow 名单。您也可以创建自定义 allow 名单。简单的自定义名单可能只允许主机运行某一操作系统。较复杂的名单可能允许所有操作系统，但指定主机在特定端口上运行某一应用协议必须使用的操作系统。

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。 此限制可能会影响创建合规 allow 名单的方式。

实施合规 允许 名单

要实施 allow 名单，请将该名单添加到活动关联策略。系统评估目标并给每个主机分配对应的属性：

- 合规 - 主机没有违反名单。

- 不合规 - 主机违反名单。
- 未评估 - 主机不是名单的目标，主机现在正在接受评估，或者系统没有足够的信息来确定主机是否合规。

注释 要删除主机属性，请删除其对应的 allow 名单。停用、删除或删除关联策略中的 an allow 名单 **不** 会删除主机属性，也不会更改每个主机的属性值。

完成初始评估后，当受监控的主机不再符合活动 allow 名单时，系统会生成 an *allow* 名单事件；它会还记录 an *allow* 名单违规。

您可以使用工作流程、控制面板以及网络映射来监控整个系统的合规活动，并确定个别主机何时、以何种方式违反了您的 allow 名单。您也可以通过补救和警报自动对如违规做出响应。

示例：将 HTTP 限制为 Web 服务器

您的安全策略规定只有 Web 服务器可以运行 HTTP。您可以创建一份评估整个网络（不包括 Web 场）的 an allow 名单，以确定哪些主机正在运行 HTTP。

通过使用网络映射和控制面板，您可以获取您的网络合规性的概览摘要。只需几秒钟，便可以确定组织内的哪些主机违反了策略正在运行 HTTP，并采取相应的行动。

然后，使用关联功能配置系统，使系统在 Web 场之外的主机开始运行 HTTP 时发出警报。

相关主题

配置关联策略，第 941 页

合规 允许 名单目标网络

目标网络 指定要用于合规性评估的主机。An allow 名单可具有多个目标网络，并且会评估与其任何目标的条件相符的主机。

最初，您可通过 IP 地址或范围限制目标网络。在多域部署中，初始限制还包括一个域。

系统提供的默认 allow 名单针对所有受监控主机：0.0.0.0/0 和 ::/0。在多域部署中，默认 allow 名单限用于（且仅适用于）全局域。

如果修改目标网络或主机，致使该主机不再是 allow 名单的有效目标，则该主机不再通过名单进行评估，并且既不视为合规，也不视为不合规。

调查和优化目标网络

将目标网络添加到 an allow 名单中时，系统会提示您调查网络映射以帮助确定合规主机的特征。调查会将目标添加到表示已调查的主机的 allow 名单中。

您可以调查子网或单个主机。在多域部署中，您可以调查整个域，也可以跨域调查。调查祖先域会导致系统调查该域的后代。

除已添加的目标之外，调查还会对在该调查中检测到的每个操作系统都使用一个主机配置文件填充 allow 名单。这些主机配置文件允许系统在适用操作系统上检测到的所有客户端、应用协议、Web 应用和协议。

在调查目标网络（或跳过调查）后，请优化目标。您可以按 IP 地址排除主机，或者按主机属性或 VLAN 限制目标网络。

使用合规 允许 名单设定目标域

在多域部署中，域和目标网络紧密相连。

- 枝叶域管理员可以创建对其枝叶域内的主机进行评估的 allow 名单。
- 更高级别的域管理员可以创建跨域评估主机的 allow 名单。您可以在同一个 allow 名单中以不同域中的不同子网作为目标。

假设您是全局域管理员，并且要将同一合规性条件应用于整个部署中的 Web 服务器。您可以在全局域中创建用于定义合规性条件的 allow 名单。然后，使用指定各枝叶域中 Web 服务器的 IP 空间（或单个 IP 地址）的目标网络来限制 allow 名单。

注释 除将枝叶域中的 IP 地址和范围设定为目标之外，您还可以使用更高级别的域来限制目标网络。将更高级别的域中的子网设定为目标即会以**每个**后代枝叶域中的**同一**子网为目标。 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

合规 允许 名单主机配置文件

在合规 allow 名单中，主机配置文件指定允许在目标主机上运行的操作系统、客户端、应用协议、Web 应用和协议。有三种类型的主机配置文件可在合规 allow 名单中使用；每个类型在合规名单编辑器中以不同方式显示。

表 *127:* 合规 允许 名单主机配置文件类型

主机配置文件类型	外观	说明
全局	任何操作系统	指定允许在目标主机上运行的内容，而不考虑操作系统
特定于操作系统	以纯文本列示	指定允许在特定操作系统的目标主机上运行的内容
共享	以斜体形式列示	指定可以在多个 allow 名单中使用的操作系统条件

操作系统特定主机配置文件

在合规 allow 名单中， 特定操作系统主机配置文件 不仅指定了允许在网络上运行的操作系统，还指定了允许在这些操作系统上运行的应用协议、客户端、Web 应用及通信协议。

例如，可以要求合规主机运行特定版本的 Microsoft Windows。再例如，可以允许 SSH 于端口 22 在 Linux 主机上运行，并进一步限制 SSH 客户端的供应商和版本。

请为允许在网络上运行的各个操作系统创建一个主机配置文件。要禁止网络上的某个操作系统，则不要创建该操作系统的主机配置文件。例如，为了确保网络上的所有主机均运行 Windows，请将 allow 名单配置为只包含该操作系统的主机配置文件。

注释 未识别的主机在被识别之前，一直处于符合所有 allow 名单条件的状态。但是，可以为未知主机创建一份 an allow 名单主机配置文件。未识别的主机是指系统尚未收集足够的信息识别其操作系统的主机。未知主机是指其操作系统与已知指纹不匹配的主机。

共享主机配置文件

在合规 allow 名单中，共享主机配置文件绑定到特定操作系统，但是您可以在多个 allow 名单中使用每个共享主机配置文件。

例如，您可能在全球具有多个办事处，其中每个位置对应单独的 allow 名单，但是要对运行 Apple Mac OS X 的所有主机都使用同一配置文件。您可以为该操作系统创建共享配置文件，并将其用于所有 allow 名单中。

默认 allow 名单使用共享主机配置文件的一个特殊类别，即 内置主机配置文件。这些配置文件使用内置应用协议、Web 应用、协议和客户端。在合规 allow 名单编辑器中，系统使用 **内置主机配置文件图标**标记这些配置文件。

在多域部署中，系统会显示在当前域中创建的共享主机配置文件，您可以对其进行编辑。系统还会显示祖先域中的共享主机配置文件，您不可以对其进行编辑。要查看和编辑在较低域中创建的共享主机配置文件，请切换至该域。

注释 如果修改共享主机配置文件（包括内置主机配置文件），或者修改内置应用协议、协议或客户端，则更改会影响使用它的每个 allow 名单。如果无意中更改或删除了这些内置元素，则可以重置为出厂默认设置。

允许 违规触发器

当系统出现以下情况时，主机的 allow 名单合规情况会发生变化：

- 检测到主机的操作系统发生变化
- 检测到主机的操作系统或主机上的应用协议存在身份冲突
- 检测到主机上有新的 TCP 服务器端口（例如，SMTP 或网络服务器使用的端口）处于活动状态，或主机上有新的 UDP 服务器正在运行
- 检测到主机上运行的 TCP 或 UDP 服务器发生变化，例如由于升级导致版本发生变化
- 检测主机上有新的客户端或 Web 应用正在运行

- 从其数据库中丢弃不活动的客户端或 Web 应用
- 检测到主机正使用新的网络或传输协议进行通信
- 检测到新的破解移动设备
- 检测到主机上的某个 TCP 或 UDP 端口已关闭或超时

此外，您还可以使用主机输入功能或主机配置文件执行以下操作来触发主机合规性的改变：

- 向主机添加客户端、协议或服务器
- 从主机中删除客户端、协议或服务器
- 设置主机的操作系统定义
- 更改主机的主机属性，这样该主机便不再是一个有效目标

注释 为避免事件数量过多而使系统不堪重负，系统在初始评估时不会为违规主机生成 allow 名单事件，也不会对由于修改了有效 allow 名单或共享主机配置文件而导致违规的主机生成不合规名单事件。但是，仍会记录违规情况。如果要为所有违规目标生成 allow 名单事件，请清除发现数据。重新发现网络资产可能会触发 allow 名单事件。

操作系统合规性

如果 allow 名单指定只允许在网络上运行 Microsoft Windows 主机，但系统检测到主机正在运行 Mac OS X，则系统会生成 an allow 名单事件。此外，该主机与 allow 名单关联的主机属性从“合规”更改为“违规”。

要将本示例中主机的合规属性恢复为合规，必须发生下列任一情况：

- 您编辑 allow 名单，以允许 Mac OS X 操作系统的运行
- 您手动将主机的操作系统定义更改为 Microsoft Windows
- 系统检测到操作系统已更改回 Microsoft Windows

从网络映射中删除违规资产

如果 allow 名单禁止使用 FTP，并且您从应用协议网络映射或事件视图中删除了 FTP，则运行 FTP 的主机的属性变为合规。但如果系统再次检测到该应用协议，则会生成 an allow 名单事件，且该主机的属性变为违规。

仅对完整信息触发

如果 allow 名单仅在端口 21 上允许 TCP FTP 流量，且系统检测到端口 21/TCP 上存在不确定的活动，则 allow 名单不会触发。仅当系统将该流量识别为除 FTP 流量以外的其他流量，

或者您使用主机输入功能将该流量指定为非 FTP 流量时， allow 名单才会触发。系统不会记录仅含部分信息的违规。

合规的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员

创建合规 允许 名单

当创建合规 allow 名单时，系统会提示您调查网络，创建初始目标并帮助确定合规主机的特征。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **允许列表**。

步骤 2 点击 **New允许列表**。

步骤 3 或者，输入初始目标网络的 **IP 地址 (IP Address)** 和**网络掩码 (Netmask)**。在多域部署中，在**域 (Domain)** 中选择目标网络所在的域。

提示 要调查整个受监控网络，请使用默认值 0.0.0.0/0 和 ::/0。

注释 在为目标网络选择域之后，不能更改该域。将更高级别的域中的子网设定为目标即会以**每个**后代枝叶域中的**同一**子网为目标。 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 添加目标网络：

- 添加 - 要添加目标网络而无需调查，请点击**添加 (Add)**。
- 添加并调查网络 - 要添加并调查目标网络，请点击**添加并调查网络 (Add and Survey Network)**。
- 跳过 - 要创建 an allow 名单而不调查网络，请点击 **跳过**。

步骤 5 或者，为 allow 名单输入新的 **名称** 和 **说明** 。

步骤 6 或者，在网络上**允许破解的移动设备 (Allow Jailbroken Mobile Devices)**。禁用此选项会导致破解设备生成 allow 名单违规。

步骤 7 向 allow 名单中至少添加一个 **目标网络**，如 为合规 允许 名单创建目标网络，第 931 页中所述。

步骤 8 使用**允许的主机配置文件 (Allowed Host Profiles)** 确定合规主机的特征：

- 全局主机配置文件 - 要编辑 allow 名单的全局主机配置文件，请点击 **任何操作系统**，然后如 构建 允许 列表主机配置文件，第 932 页中所述继续操作。
- 编辑已调查的配置文件 - 要编辑由网络调查创建的现有操作系统特定主机配置文件，请点击其名称，然后如构建 允许 列表主机配置文件，第 932 页中所述继续操作。
- 创建新配置文件 - 要为此 allow 名单创建新的操作系统特定主机配置文件，请点击 **允许的主机配置文件**旁边的 **添加**（+），然后如 构建 允许 列表主机配置文件，第 932 页中所述继续操作。
- 添加共享主机配置文件 - 要向 allow 名单中添加现有共享主机配置文件，请点击 **添加共享主机配置文件**，选择要添加的共享主机配置文件，然后点击 **确定**。共享主机配置文件以斜体显示。

步骤 9 点击**保存 (Save)允许列表**。

下一步做什么

- 将 allow 名单添加到活动关联策略中，如 配置关联策略，第 941 页中所述。系统立即开始评估 allow 名单并生成违规。

相关主题

合规 允许 名单目标网络，第 926 页
根据所选主机创建合规 允许 名单，第 875 页
Firepower 系统 IP 地址约定，第 26 页

为合规 允许 名单创建目标网络

添加目标网络时，可以对其进行调查以确定合规主机的特征。此调查会对调查中检测到的每个操作系统都使用一个主机配置文件来填充 allow 名单。这些主机配置文件允许系统在适用操作系统上检测到的所有客户端、应用协议、Web 应用和协议。

过程

步骤 1 在合规 allow 名单编辑器中，点击 **添加目标网络**。

步骤 2 为目标网络输入 **IP 地址 (IP Address)** 和**网络掩码 (Netmask)**。

步骤 3 在多域部署中，在**域 (Domain)** 中选择目标网络所在的域。

注释 在为目标网络选择域之后，不能更改该域。将更高级别的域中的子网设定为目标即会以**每个**后代枝叶域中的**同一**子网为目标。 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 添加目标网络：

- 添加 - 要在不调查的情况下添加目标网络，请点击**添加 (Add)**。
- 添加并调查网络 - 要添加并调查目标网络，请点击**添加并调查网络 (Add and Survey Network)**。

步骤 5 或者，点击新目标以进一步对其进行配置：

- 名称 - 在**名称 (Name)** 中输入新名称。
- 添加网络 - 要以其他主机为目标，请点击 **添加**（+），然后输入 **IP 地址** 和 **网络掩码**。要从 allow 名单合规性中排除网络，请选择 **排除**。
- 添加主机属性 - 要以具有特定主机属性的主机为目标，请点击 **添加**（+），然后指定 **属性** 及其 **值** 。
- 添加 VLAN - 要以 VLAN 为目标，请点击 **添加**（+），然后键入 VLAN 编号（对于 802.1q VLAN）。
- 删除 - 要删除目标限制，请点击 **删除**（🗑）。

步骤 6 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

相关主题

合规 允许 名单目标网络 ， 第 926 页
Firepower 系统 IP 地址约定 ， 第 26 页

构建 允许 列表主机配置文件

主机配置文件 指定 allow 名单的合规性条件，即允许在目标主机上运行的操作系统、客户端、应用协议、Web 应用和协议。

每个 allow 名单都有一个与操作系统无关的全局主机配置文件。例如，无需编辑多个 Microsoft Windows 和 Linux 主机配置文件以允许 Mozilla Firefox，可以将全局主机配置文件配置为允许 Firefox，无论检测到该主机使用的是什么操作系统。

您也可以配置操作系统特定的主机配置文件，主机配置文件为一个 allow 名单独有或跨 allow 名单共享。

注释 如果修改共享主机配置文件（包括内置主机配置文件），或者修改内置应用协议、协议或客户端，则更改会影响使用它的每个 allow 名单。如果无意中更改或删除了这些内置元素，则可以重置为出厂默认设置。

开始之前

- 如 编辑合规 允许 名单， 第 936 页中所述在 an allow名单内创建或编辑主机配置文件，或者如 管理共享主机配置文件， 第 937 页中所述创建或编辑共享主机配置文件。

过程

步骤 1 在合规 allow 名单主机配置文件编辑器中，配置主机配置文件：

- 名称 - 输入**名称 (Name)**。
- 操作系统 - 要将主机配置文件限制为特定的操作系统，请使用**操作系统供应商 (OS Vendor)**、**操作系统名称 (OS Name)** 和**版本 (Version)** 下拉列表。由于其目的是应用到运行任何操作系统的主机，因此无法限制全局主机配置文件。
- 应用协议 - 要允许应用协议，请点击 **添加**（+），并如 将应用协议添加到合规 允许 列表， 第 933 页中所述继续操作。
- 客户端 - 要允许客户端，请点击 **添加**（+），并如 将客户端添加到合规 允许 列表， 第 934 页中所述继续操作。
- Web 应用 - 要允许 Web 应用，请点击 **添加**（+），并如 将 Web 应用添加到合规 允许 列表， 第 935 页中所述继续操作。
- 协议 - 要允许协议，请点击 **添加**（+），并如 将协议添加到合规 允许 列表， 第 935 页中所述继续操作。
- 删除 - 要禁止之前允许的项目，请点击 **删除**（🗑）。
- 编辑属性 - 要编辑允许的应用协议、客户端或协议的属性，请点击其名称。进行的更改反映在使用该元素的所有主机配置文件中。

提示 选中相应的**全部允许...(Allow all...)**复选框，以允许与此配置文件匹配的主机的所有应用协议、客户端或 Web 应用。

步骤 2 要立即实施自上次保存后进行的所有更改，请点击**保存允许列表**（或如果您编辑的是共享主机配置文件，则点击 **保存所有配置文件** ）。

将应用协议添加到合规 允许 列表

使用 allow 名单主机配置文件，您可以在全局范围或在特定操作系统上将应用协议允许。或者，可以按端口、供应商或版本限制应用协议。例如，可以允许特定版本的 SSH 在 Linux 主机的端口 22/TCP 上运行。

过程

步骤 1 创建或修改合规 allow 列表主机配置文件时，点击 **允许的应用协议** 旁边的 **添加**（+）（或者，如果修改的是全局主机配置文件，则点击 **全局允许的应用协议** 旁边的添加图标）。

步骤 2 此时您有两种选择：

- 如果列出了要允许的应用协议，请选择这些协议。Web 界面列出 allow 名单已允许或当前允许的应用协议。
- 要允许列表中未包含的应用协议，请选择**<新应用协议> (<New Application Protocol>)**，然后点击**确定 (OK)** 显示应用协议编辑器。选择要允许的应用协议**类型 (Type)** 和**协议 (Protocol)**。或者，按**端口 (port)**、**供应商 (Vendor)** 和**版本 (Version)** 限制应用协议。

  注释 必须完全按照供应商和版本在应用的表视图中的显示键入该供应商和版本。如果不指定供应商或版本，则只要类型与协议匹配， allow 名单便允许所有供应商和版本。

步骤 3 点击 **OK**。

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

将客户端添加到合规 允许 列表

使用 allow 名单主机配置文件时，可以在全局或在特定操作系统上将客户端允许。或者，要求客户端的特定版本。例如，可以只允许 Microsoft Internet Explorer 10 在 Microsoft Windows 主机上运行。

过程

步骤 1 创建或修改合规 allow 名单主机配置文件时，点击 **允许的客户端** 旁边的 **添加**（+） 或者，如果修改的是全局主机配置文件，则点击 **全局允许的客户端** 旁边的图标）。

步骤 2 此时您有两种选择：

- 如果要允许的客户端已列出，请选择这些客户端。Web 界面列出已被 allow 名单允许或当前允许的客户端。
- 要允许不在列表中的客户端，请选择**<新建客户端> (<New Client>)** 并点击**确定 (OK)** 以显示客户端编辑器。从下拉列表中选择要允许的**客户端 (Client)**，或者将客户端限制为允许的**版本 (Version)**。

  注释 必须准确地输入版本，因为它会显示在客户端表视图中。如果不指定版本，则允许所有版本。

步骤 3 点击 **OK**。

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

将 Web 应用添加到合规 允许 列表

使用 allow 名单主机配置文件，您可以在全局范围或在特定操作系统上将 web 应用允许。

过程

步骤 1 创建或修改合规 allow 名单主机配置文件时，点击 **允许的 Web 应用** 旁边的 **添加**（+）（或者，如果修改的是全局主机配置文件，则点击 **全局允许的 Web 应用** 旁边的图标）。

步骤 2 选择要允许的 Web 应用。

步骤 3 点击 **OK**

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

将协议添加到合规 允许 列表

使用 allow 名单主机配置文件，您可以在全局范围或在特定操作系统上将协议允许。始终允许在任何主机上运行 ARP、IP、TCP 和 UDP；不能禁用这些协议。

过程

步骤 1 创建或修改合规 allow 列表主机配置文件时，点击 **允许的协议** 旁边的 **添加**（+）（或者，如果修改的是全局主机配置文件，则点击 **全局允许的协议** 旁边的添加图标）。

步骤 2 此时您有两种选择：

- 如果列出了要允许的协议，请选择这些协议。Web 界面列出 allow 名单已允许或当前允许的协议。
- 要允许列表中未包含的协议，请选择**<新协议> (<New Protocol>)**，然后点击**确定 (OK)** 显示协议编辑器。从**类型 (Type)** 下拉列表中，选择协议类型（**网络 [Network]** 或**传输 [Transfer]**），然后从下拉列表中选择**协议 (Protocol)**。

  提示 选择 **Other (manual entry)** 以指定不在列表中的通信协议。对于网络协议，请键入 http://www.iana.org/assignments/ethernet-numbers/ 中所列的相应编号。对于传输协议，请键入 http://www.iana.org/assignments/protocol-numbers/ 中所列的相应编号。

步骤 3 点击 **OK**。

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

管理合规 允许 名单

可以使用 允许 名单页面管理合规allow名单和共享主机配置文件。默认allow名单表示建议的设置，并使用共享主机配置文件的一个特殊类别，即 内置主机配置文件。

在多域部署中，系统会显示在当前域中创建的合规 allow 名单，您可以对其进行编辑。系统还会显示祖先域中的选定 allow 名单，您不可以对其进行编辑。要查看和编辑在较低域中创建的 allow 名单，请切换至该域。

注释 如果配置暴露有关不相关域的信息（包括名称、受管设备等），则系统不会显示祖先域的配置。 默认 allow 名单仅在全局域中可用。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **允许列表**。

步骤 2 管理合规 allow 名单：

- 创建 - 要创建新的 allow 名单，请点击 **新建允许列表**，然后如 创建合规 允许 名单，第 930 页中所述继续操作。
- 删除 - 要删除未使用的 an allow 名单，请点击 **删除**（）），然后确认要删除该 allow 名单。删除 an allow 名单还会从网络上所有主机中删除其关联的主机属性。 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。
- 编辑 - 要修改现有 allow 名单，请点击 **编辑**（），然后如 编辑合规 允许 名单，第 936 页中所述继续操作。如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。
- 共享主机配置文件 - 要管理 allow 名单的共享主机配置文件，请点击 **编辑共享配置文件**，然后如 管理共享主机配置文件，第 937 页中所述继续操作。

编辑合规 允许 名单

当修改并保存活动关联策略中包含的合规 allow 名单时，系统会立即重新评估 allow 名单的目标网络中主机的合规性。尽管此重新评估可能会使某些主机合规或不合规，但是系统不会生成任何 allow 名单事件。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **允许列表**。

步骤 2 在要修改的 allow 名单旁，点击 **编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 编辑合规 allow 名单：

- 名称和说明 - 要更改名称或说明，请点击左侧面板中的 allow 名单名称以显示基本 allow 名单信息，然后键入新信息。
- 允许破解的设备 - 要在网络上允许破解的移动设备，请点击左侧面板中的 allow 名单名称以显示基本 allow 名单信息，然后启用 **允许破解的移动设备**。禁用此选项会导致破解设备生成 allow 名单违规。
- 添加允许的主机配置文件 - 要为此 allow 名单创建操作系统特定主机配置文件，请点击“允许的主机配置文件”旁边的 **添加**（），然后如 构建 允许 列表主机配置文件，第 932 页中所述继续操作。
- 添加共享主机配置文件 - 要向 allow 名单中添加现有共享主机配置文件，请点击 **添加共享主机配置文件**，选择要添加的共享主机配置文件，然后点击 **确定**。共享主机配置文件以斜体显示。
- 添加目标网络 - 要添加新的目标网络而不调查其主机，请点击“目标网络”旁边的 **添加**（），然后如 为合规 允许 名单创建目标网络，第 931 页中所述继续操作。
- 删除主机配置文件 - 要从 allow 名单中删除共享主机配置文件或操作系统特定主机配置文件，请点击主机配置文件旁边的 **删除**（），然后确认选择。删除共享主机配置文件会从 allow 名单中将其移除，但是不会删除该配置文件，也不会从使用它的任何其他 allow 名单中将其移除。您无法删除 an allow 名单的全局主机配置文件。
- 删除目标网络 - 要从 allow 名单中移除目标网络，请点击网络旁边的 **删除**（），然后确认选择。
- 编辑全局主机配置文件 - 要编辑 allow 名单的全局主机配置文件，请点击 **任何操作系统**，然后如 构建 允许 列表主机配置文件，第 932 页中所述继续操作。
- 编辑其他主机配置文件 - 要编辑共享主机配置文件或操作系统特定主机配置文件，请点击该主机配置文件的名称，然后如构建 允许 列表主机配置文件，第 932 页中所述继续操作。
- 编辑目标网络 - 要编辑目标网络，请点击网络的名称，然后如为合规 允许 名单创建目标网络，第 931 页中所述继续操作。

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击 **保存允许列表**。

管理共享主机配置文件

在合规 allow 名单中，共享主机配置文件绑定到特定操作系统，但是您可以在多个 allow 名单中使用每个共享主机配置文件。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。

在多域部署中，系统会显示在当前域中创建的共享主机配置文件，您可以对其进行编辑。系统还会显示祖先域中的共享主机配置文件，您不可以对其进行编辑。要查看和编辑在较低域中创建的共享主机配置文件，请切换至该域。

注释 如果修改共享主机配置文件（包括内置主机配置文件），或者修改内置应用协议、协议或客户端，则更改会影响使用它的每个 allow 名单。如果无意中更改或删除了这些内置元素，则可以重置为出厂默认设置。

过程

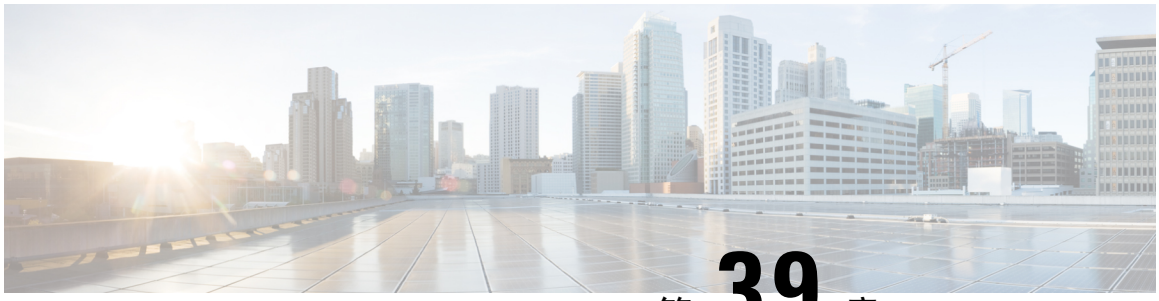
步骤 1 选择 **策略** > **关联**，然后点击 **允许列表**。

步骤 2 点击 **Edit Shared Profiles**。

步骤 3 管理共享主机配置文件：

- 创建共享主机配置文件 - 要创建新的共享主机配置文件而不调查主机，请点击共享主机配置文件旁边的 **添加**（），然后如 构建 允许 列表主机配置文件，第 932 页中所述继续操作。
- 通过调查创建共享主机配置文件 - 要通过调查网络创建多个新的共享主机配置文件，请点击**添加目标网络 (Add Target Network)**，然后如为合规 允许 名单创建目标网络，第 931 页中所述继续操作。
- 删除 - 要删除共享主机配置文件，请点击 **删除**（  ），然后确认您的选择。
- 编辑 - 要修改现有的共享主机配置文件（包括内置共享主机配置文件），请点击其名称，然后如构建 允许 列表主机配置文件，第 932 页中所述继续操作。
- 重置内置主机配置文件 - 要将所有内置主机配置文件重置为出厂默认设置，请点击**内置主机配置 (Built-in Host Profiles)**，然后点击**重置为出厂默认设置 (Reset to Factory Defaults)** 并确认您的选择。

步骤 4 要立即实施自上次保存后做出的所有更改，请点击**保存所有配置文件 (Save All Profiles)**。



第 39 章

关联策略

以下主题介绍如何配置关联策略和规则。

关联策略和规则简介

您可以通过关联功能，使用关联策略实时应对网络威胁。

当网络活动触发某个活动的关联策略中的 关联规则 或 合规 *allow* 名单 时，会导致关联 策略违规 的发生。

关联规则

当活动的关联策略中的关联规则触发时，系统会生成关联事件。关联规则可在以下情况下触发：

- 系统生成特定类型的事件（连接、入侵、恶意软件、发现、用户活动等）。
- 网络流量偏离其正常的量变曲线。

可以通过下列方式限制关联规则：

- 添加主机配置文件限定条件以使用涉及触发事件的主机的主机配置文件中的信息限制该规则。
- 向关联规则中添加连接跟踪器，以便在满足规则的初始条件后，系统开始跟踪某些连接。然后，只有在跟踪的连接满足其他条件时，才可生成关联事件。
- 向关联规则中添加用户资格，以跟踪某些用户或用户群。例如，您可以限制关联规则，以便只有特定用户的流量或来自特定部门的流量才会触发该关联规则。
- 添加暂停周期。当关联规则触发后，暂停周期会导致该规则在指定时间间隔内不会再次触发。暂停周期过后，该规则可再次触发并开始新的暂停周期。

- 添加非活动周期在非活动周期，关联规则不会触发。

虽然您可以配置关联规则而不对您的部署授予许可，但使用未经许可组件的规则不会触发。

合规 允许 名单

合规 allow 名单指定允许在网络中的主机上运行的操作系统、应用（Web 和客户端）及协议。当主机违反用于活动关联策略使用的 an allow 名单时，系统生成 an *allow* 名单事件。

关联响应

对关联策略违规的响应包括简单的警报以及各种补救（例如扫描主机）。您可以将每个关联规则或allow名单与单个响应或一组响应相关联。

如果网络流量触发多个规则或allow名单，系统将发起与每个规则和allow名单相关的所有响应。

关联和多租户

在多域部署中，可以在任意域级别创建关联策略，只要使用的是该级别可用的规则、 allow 名单和响应。高层域管理员可以在域中或跨域执行关联：

- 按域限制关联规则将匹配该域的后代所报告的事件。
- 高层域管理员可以跨域创建评估主机的合规 allow 名单。您可以在同一个 allow 名单中以不同域中的不同子网作为目标。

注释 系统会为每个分叶域构建单独的网络映射。使用文字配置（例如 IP 地址、VLAN 标记和用户名）限制跨域关联规则可能会出现意外结果。

相关主题

合规 允许 名单简介，第 925 页
Cisco Secure Firewall Management Center 警报响应，第 531 页
补救简介，第 989 页

合规的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员

配置关联策略

使用关联规则、合规 allow 名单、警报响应和补救来构建关联策略。

在多域部署中，可以在任何域级别使用该级别可用的任何构成配置来创建关联策略。

可为每个关联策略以及该策略中使用的每条规则和 allow 名单分配优先级。规则和 allow 名单优先级会覆盖关联策略优先级。如果网络流量违反关联策略，则产生的关联事件会显示策略优先级值，除非违反的规则或 allow 名单有自己的优先级。

过程

步骤 1 选择**策略** > **关联**。

步骤 2 点击**创建策略**。

步骤 3 输入 **策略名称** 和 **策略说明**。

步骤 4 从**默认优先级 (Default Priority)** 下拉列表中选择策略的优先级。选择**无 (None)** 以便仅使用规则的优先级。

步骤 5 点击**添加规则 (Add Rules)**，选择要在策略中使用的规则和 allow 名单，然后点击**添加 (Add)**。

步骤 6 从每个规则或 allow 名单的**优先级 (Priority)** 列表中选择优先级：

- 优先级值介于 1 到 5 之间。
- **无**
- **默认 (Default)**，以使用策略的默认优先级

步骤 7 将响应添加到规则和 allow 名单中，如 将响应添加到规则和允许名单 ， 第 941 页中所述。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 通过点击滑块来激活策略。

将响应添加到规则和允许名单

您可以将每个关联规则或allow名单与单个响应或一组响应相关联。如果网络流量触发多个规则或allow名单，系统将发起与每个规则和allow名单相关的所有响应。请注意，Nmap 补救在用作对流量量变曲线更改的响应时不会启动。

在多域部署中，可以使用在当前域或祖先域中创建的或响应。

过程

步骤 1 在关联策略编辑器中要添加响应的规则或 allow 名单旁边，点击**响应** （  ）。

步骤 2 在“未分配的响应”(Unassigned Responses) 下，选择在规则或allow名单触发时要启动的响应，然后点击向上箭头 (^)。

步骤 3 点击**更新**。

相关主题

Cisco Secure Firewall Management Center 警报响应 ，第 531 页
补救简介 ，第 989 页

管理关联策略

对活动关联策略进行的更改会立即生效。

激活关联策略时，系统会立即开始处理事件并触发响应。请注意，系统不会在初次、激活后的评估中为不合规主机生成 allow 名单事件。

在多域部署中，系统会显示在当前域中创建的关联策略，您可以对其进行编辑。系统还会显示来自祖先域中的选定关联策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的关联策略，请切换至该域。

注释 如果配置暴露有关不相关域的信息（包括名称、受管设备等），则系统不会显示祖先域的配置。

过程

步骤 1 选择**策略** > **关联**。

步骤 2 管理关联策略：

- 激活或停用 - 点击滑块。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 创建 - 点击**创建策略 (Create Policy)**；请参阅配置关联策略 ，第 941 页。
- 编辑 - 点击 **编辑**（）；请参阅 配置关联策略 ，第 941 页。 如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除 - 点击 **删除**（）。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

配置关联规则

简单的关联规则仅要求发生特定类型的事件。您不需要提供更具体的条件。例如，基于流量量变曲线变更的关联规则不需要条件。您也可以使用多个条件和添加的限制来创建复杂的关联规则。

当创建关联规则触发条件、主机配置文件限定条件、用户资格或连接跟踪器时，语法发生变化但结构保持不变。

注释 在多域部署中，按祖先域限制关联规则将匹配该域的后代所报告的事件。

开始之前

- 确认您的部署正在收集您要用来触发关联事件的信息类型。例如，任意单个连接或连接摘要事件的可用信息取决于几个因素，包括检测方法、日志记录方法和事件类型。 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。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **规则管理**。

步骤 2 点击 **Create Rule**。

步骤 3 输入**规则名称 (Rule Name)** 和**规则说明 (Rule Description)**。

步骤 4 或者，也可为规则选择**规则组 (Rule Group)**。

步骤 5 选择基础事件类型，并为关联规则指定其他触发条件（后者为可选项）。您可以选择以下基础事件类型：

- **发生 VPN 故障排除事件** - 请参阅VPN 故障排除事件触发条件的语法，第 944 页。
- **发生入侵事件 (an intrusion event occurs)** - 请参阅入侵事件触发条件的语法，第 945 页。
- **发生恶意软件事件 (a malware event occurs)** - 请参阅恶意软件事件触发条件的语法，第 947 页。
- **发生发现事件 (a discovery event occurs)** - 请参阅发现事件触发条件的语法，第 948 页。
- **检测到用户活动 (user activity is detected)** - 请参阅用户活动事件触发条件的语法，第 951 页。
- **发生主机输入事件 (a host input event occurs)** - 请参阅主机输入事件触发条件的语法，第 952 页。
- **发生连接事件 (a connection event occurs)** - 请参阅连接事件触发条件的语法，第 953 页。
- **流量量变曲线更改 (a traffic profile changes)** - 请参阅流量量变曲线更改的语法，第 956 页。

步骤 6 或者，也可以通过添加以下任一项或全部条件来进一步限制关联规则：

- 主机配置文件限定条件 - 点击**添加主机配置文件限定条件 (Add Host Profile Qualification)**；请参阅关联主机配置文件限定条件的语法，第 958 页。
- 连接跟踪器 - 点击**添加连接跟踪器 (Add Connection Tracker)**；请参阅连接跟踪器，第 962 页。

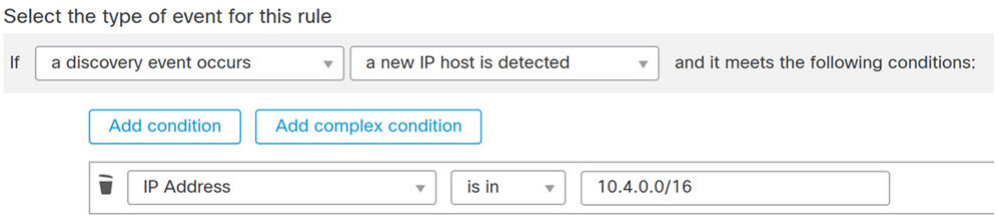
- 用户资格 - 点击**添加用户资格 (Add User Qualification)**；请参阅用户资格的语法，第 961 页。
- 暂停周期 - 在“规则选项”(Rule Options) 下，使用**暂停 (Snooze)** 文本字段和下拉列表指定在关联规则触发后系统要再次触发该规则应等待的时间间隔。
- 非活动周期 - 在“规则选项”(Rule Options) 下，点击**添加非活动周期 (Add Inactive Period)**。使用文本字段和下拉列表，指定您希望系统停止根据关联规则评估网络流量的时间和频率。

提示 要移除暂停周期，请将时间间隔指定为 0（秒、分钟或小时）。

步骤 7 点击**保存规则 (Save Rule)**。

简单的关联规则示例

如果在特定子网中检测到新的主机，则会触发以下简单的关联规则。请注意，当类别为 IP 地址时，选择 **is in** 或 **is not in** 作为运算符使您可以指定 IP 地址是还是不是在 IP 地址块中，如特殊表示法（例如 CIDR）所述。



下一步做什么

- 使用关联策略中的规则，如配置关联策略，第 941 页中所述。

相关主题

管理关联规则，第 973 页
关联规则构建机制，第 970 页
暂停和非活动周期，第 970 页
NetFlow 和受管设备数据之间的差异

VPN 故障排除事件触发条件的语法

下表介绍将 VPN 故障排除事件选定为基础事件时如何构建关联规则条件。

表 *128: VPN* 故障排除事件数的语法

如果您指定.....	选择运算符，然后输入.....
设备	选择一个或多个启用了 VPN 故障排除系统日志的设备。

如果您指定.....	选择运算符，然后输入.....
系统日志消息类	选择 VPN 系统日志消息类。生成具有所选消息类的系统日志时，它会满足关联规则条件并生成关联事件。
系统日志消息 ID	为关联规则指定 VPN 系统日志消息 ID。
系统日志消息文本	为关联规则指定 VPN 系统日志消息文本。
系统日志严重性	指定 VPN 系统日志严重性。为所选严重性生成的 VPN 故障排除系统日志会触发关联事件。
用户名	提及需要为其生成关联事件的流量的 VPN 用户名。

入侵事件触发条件的语法

下表介绍将入侵事件选定为基础事件时如何构建关联规则条件。

表 *129:* 入侵事件的语法

如果您指定.....	选择运算符，然后.....
访问控制策略	选择使用生成入侵事件的入侵策略的一个或多个访问控制策略。
访问控制规则名称	输入使用生成入侵事件的入侵策略的访问控制规则的全部或部分名称。
应用协议	选择一个或多个与入侵事件关联的应用协议。
应用协议类别	选择一个或多个应用协议类别。
分类	选择一个或多个分类。
客户端	选择一个或多个与入侵事件关联的客户端。
客户端类别	选择一个或多个客户端类别。
目标国家/地区或源国家/地区	选择一个或多个与入侵事件中的源或目标 IP 地址关联的国家/地区。
目标 IP、源 IP、源 IP 和目标 IP，或者源 IP 或目标 IP	输入单个 IP 地址或地址块。
目标端口/ICMP 代码或源端口/ICMP 类型	输入源流量的端口号或 ICMP 类型或目标流量的端口号或 ICMP 代码。
设备	选择一个或多个可能生成事件的设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
出口接口或入口接口	选择一个或多个接口。

如果您指定.....	选择运算符，然后.....
出口安全区域或入口安全区域	选择一个或多个安全区域或隧道区域。
生成器 ID	选择一个或多个预处理器。
影响标志	选择分配给入侵事件的影响级别。 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。
内联结果	选择系统**已丢弃 (dropped)** 还是**应该已丢弃 (would have dropped)** 违反入侵策略的数据包。 在内联、交换或路由部署中，系统可以丢弃数据包。但是在被动部署中，包括当内联集处于分路模式下时，不管入侵规则状态或入侵策略的丢弃行为如何，系统都无法丢弃数据包。
入侵策略	选择一个或多个生成入侵事件的入侵策略。
IOC 标记	选择危害表现标记是不是因为入侵事件而设置。
优先级	选择规则优先级。 对于基于规则的入侵事件，优先级对应于 `priority` 关键字的值或 `classtype` 关键字的值。对于其他入侵事件，优先级由解码器或预处理器决定。
协议	输入 http://www.iana.org/assignments/protocol-numbers 中所列的传输协议的名称或编号。
规则消息	输入全部或部分规则消息。
规则 SID	输入由逗号分隔的单个 Snort ID (SID) 或多个 SID。 如果将 **is in** 或 **is not in** 选定为运算符，则无法使用具有多项选择的弹出窗口。必须输入由逗号分隔的 SID 列表。
规则类型	指定规则是否本地规则。 本地规则包括自定义的标准文本入侵规则、经您修改的标准文本规则，以及您在保存包含已修改报头信息时创建的共享对象规则的任何新实例。
SSL 实际操作	选择指示系统如何处理加密连接的 SSL 规则操作。
SSL 证书指纹	输入用来加密流量的证书的指纹或选择与指纹相关的使用者公用名。
SSL 证书使用者公用名 (CN)	输入用于加密会话的证书的全部或部分使用者公用名。
SSL 证书使用者国家/地区 (C)	选择一个或多个用于加密会话的证书使用者国家/地区代码。
SSL 证书使用者组织 (O)	输入用于加密会话的证书的全部或部分使用者组织名称。
SSL 证书使用者组织单位 (OU)	输入用于加密会话的证书的全部或部分使用者组织单位名称。

如果您指定.....	选择运算符，然后.....
SSL 流状态	基于系统尝试解密流量的结果选择一种或多种状态。
用户名	输入登录入侵事件中的源主机的用户的用户名。
VLAN ID	输入与触发入侵事件的数据包关联的最内部的 VLAN ID
Web 应用程序	选择与入侵事件关联的一个或多个 Web 应用。
Web 应用类别	选择一种或多种 Web 应用类别。

相关主题

入侵事件字段，第 752 页
Firepower 系统 IP 地址约定，第 26 页

恶意软件事件触发条件的语法

要使关联规则基于恶意软件事件，首先得指定要使用的恶意软件事件类型。您的选择决定您可以使用的一组触发条件。您可以选择：

- **通过基于终端的恶意软件检测**（由面向终端的 AMP 检测）
- **通过基于网络的恶意软件检测**（由面向网络的 AMP 检测）
- **通过基于网络的追溯性恶意软件检测**（由面向网络的 AMP 进行追溯性检测）

下表介绍将恶意软件事件选定为基础事件时如何构建关联规则条件。

表 *130:* 恶意软件事件的语法

如果您指定.....	选择运算符，然后.....
应用协议	选择一个或多个与恶意软件事件相关的应用协议。
应用协议类别	选择一个或多个应用协议类别。
客户端	选择一个或多个与恶意软件事件相关的客户端。
客户端类别	选择一个或多个客户端类别。
目标国家/地区或源国家/地区	选择一个或多个与恶意软件事件中的源或目标 IP 地址相关的国家/地区。
“目标 IP”、“主机 IP”或“源 IP”	输入单个 IP 地址或地址块。
目标端口/ICMP 代码	输入目标流量的端口号或 ICMP 代码。
处理结果	选择**恶意软件 (Malware)** 或 **自定义检测 (Custom Detection)** 或选择两者。

如果您指定.....	选择运算符，然后.....
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
事件类型	选择一个或多个与由面向终端的 AMP 检测的恶意软件事件关联的事件类型。
文件名	输入文件的名称。
文件类型	选择文件类型。
文件类型类别	选择一个或多个文件类型类别。
IOC Tag	选择危害表现标记**是 (is**） 还是**不是 (is not)** 因为恶意软件事件而设置。
SHA-256	输入或粘贴文件的 SHA-256 散列值。
SSL 实际操作	选择指示系统如何处理加密连接的 SSL 规则操作。
SSL 证书指纹	输入用来加密流量的证书的指纹或选择与指纹相关的使用者公用名。
SSL 证书使用者公用名 (CN)	输入用于加密会话的证书的全部或部分使用者公用名。
SSL 证书使用者国家/地区 (C)	选择一个或多个用于加密会话的证书使用者国家/地区代码。
SSL 证书使用者组织 (O)	输入用于加密会话的证书的全部或部分使用者组织名称。
SSL 证书使用者组织单位 (OU)	输入用于加密会话的证书的全部或部分使用者组织单位名称。
SSL 流状态	基于系统尝试解密流量的结果选择一种或多种状态。
源端口/ICMP 类型	输入源流量的端口号或 ICMP 类型。
Web 应用程序	选择一个或多个与恶意软件事件相关的 Web 应用。
Web 应用类别	选择一种或多种 Web 应用类别。

相关主题

文件和恶意软件事件字段，第 800 页
Firepower 系统 IP 地址约定，第 26 页

发现事件触发条件的语法

要使关联规则基于发现事件，首先得指定要使用的发现事件类型。您的选择决定您可以使用的一组触发条件。下表列出可以选择的发现事件类型。

在跃点变更上或由于达到主机限制而使系统丢弃新的主机时，不能触发关联规则。然而，当任何类型的发现事件发生时，可选择 **there is any type of event** 来触发该规则。

表 *131:* 关联规则触发条件对比发现事件类型

选择的选项	要使用的发现事件类型
a client has changed	客户端更新
a client timed out	客户端超时
a host IP address is reused	DHCP：IP 地址已重新分配
a host is deleted because the host limit was reached	已删除主机:已达主机限制
a host is identified as a network device	主机类型已更改为网络设备
a host timed out	主机超时
a host’s IP address has changed	DHCP：IP 地址已更改
a NETBIOS name change is detected	NETBIOS 名称更改
a new client is detected	新客户端
a new IP host is detected	新主机
a new MAC address is detected	为主机检测的其他 MAC
a new MAC host is detected	新主机
a new network protocol is detected	新网络协议
a new transport protocol is detected	新传输协议
a TCP port closed	TCP 端口已关闭
a TCP port timed out	TCP 端口超时
a UDP port closed	UDP 端口已关闭
a UDP port timed out	UDP 端口超时
a VLAN tag was updated	VLAN 标记信息更新
an IOC was set	危害表现
an open TCP port is detected	新 TCP 端口
an open UDP port is detected	新 UDP 端口
the OS information for a host has changed	新操作系统

选择的选项	要使用的发现事件类型
the OS or server identity for a host has a conflict	身份冲突
the OS or server identity for a host has timed out	身份超时
there is any kind of event	any event type
there is new information about a MAC address	MAC 信息更改
there is new information about a TCP server	TCP 服务器信息更新
there is new information about a UDP server	UDP 服务器信息更新

下表介绍将发现事件选定为基础事件时如何构建关联规则条件。

表 *132:* 发现事件的语法

如果您指定.....	选择运算符，然后.....
应用协议	选择一个或多个应用协议。
应用协议类别	选择一个或多个应用协议类别。
应用端口	输入应用协议端口号。
客户端	选择一个或多个客户端。
客户端类别	选择一个或多个客户端类别。
客户端版本	输入客户端的版本号。
设备	选择一个或多个可能生成发现事件的设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
硬件	输入移动设备的硬件型号。例如，要与所有 Apple iPhone 都匹配，请输入 **`iPhone`**。
主机类型	选择一个或多个主机类型。可以在一个主机或多种网络设备中的一种之间选择。
“IP 地址”(IP Address) 或“新建 IP 地址”(New IP Address)	输入单个 IP 地址或地址块。
Jailbroken	选择**是 (Yes)** 表示事件中的主机是破解移动设备，选择**否 (No)** 表示其不是破解移动设备。
MAC 地址	输入主机的全部或部分 MAC 地址。 例如，如果知道特定硬件制造商的设备拥有的 MAC 地址以 0A:12:34 开头，则可选择**开头为 (begins with)** 作为运算符，然后输入 **`0A:12:34`** 作为值。

如果您指定.....	选择运算符，然后.....
MAC 类型	选择 MAC 地址是否是**按 ARP/DHCP 检测 (ARP/DHCP Detected)**。 例如，选择系统是否将 MAC 地址明确识别为属于主机（**按 ARP/DHCP 检测 [is ARP/DHCP Detected]**），或者因为，打个比方，受管设备和主机之间有路由器，因此系统是否可以看见许多具有该 MAC 地址的主机（**不是按 ARP/DHCP 检测 [is not ARP/DHCP Detected}**）。
MAC 供应商	输入触发发现事件的网络流量使用的 NIC 的 MAC 硬件供应商的全部或部分名称。
移动	选择**是 (Yes)** 表示事件中的主机是移动设备，选择**否 (No)** 表示其不是移动设备。
NETBIOS 名称	输入主机的 NetBIOS 名称。
网络协议	输入 http://www.iana.org/assignments/ethernet-numbers 中所列的网络协议编号。
操作系统名称	选择一个或多个操作系统名称。
操作系统供应商	选择一个或多个操作系统供应商。
操作系统版本	选择一个或多个操作系统版本。
“协议”(Protocol) 或“传输协议”(Transport Protocol)	输入 http://www.iana.org/assignments/protocol-numbers 中所列的传输协议的名称或编号。
来源	选择主机输入数据的源（用于操作系统和服务器标识更改与超时）。
源类型	选择主机输入数据的源的类型（用于操作系统和服务器标识更改与超时）。
VLAN ID	输入涉及事件的主机的 VLAN ID。
Web 应用程序	选择 Web 应用。

相关主题

发现事件类型，第 863 页
发现事件字段，第 868 页
Firepower 系统 IP 地址约定，第 26 页

用户活动事件触发条件的语法

要将关联规则以用户活动为基础，请首先选择要使用的用户活动的类型。您的选择决定您可以使用的一组触发条件。您可以选择：

- **检测到的新用户身份**
- **登录到主机的用户**

下表介绍将用户活动选定为基础事件时如何构建关联规则条件。

表 133: 用户活动的语法

如果您指定.....	选择运算符，然后.....
设备	选择可能检测到用户活动的一个或多个设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
IP 地址	输入单个 IP 地址或地址块。
用户名	输入用户名。

相关主题

用户活动数据字段

Firepower 系统 IP 地址约定 ，第 26 页

主机输入事件触发条件的语法

要使关联规则基于主机输入事件，首先得指定要使用的主机输入事件类型。您的选择决定您可以使用的一组触发条件。下表列出可以选择的主机输入事件类型。

当添加、删除或更改用户定义的主机属性的定义，或设置漏洞影响限定条件时，不能触发关联规则。

表 134: 关联规则触发条件与主机输入事件类型

选择的选项	触发该事件类型的规则...
添加客户端	添加客户端
删除客户端	删除客户端
添加主机	添加主机
添加协议	添加协议
删除协议	删除协议
添加扫描结果	添加扫描结果
设置服务器定义	设置服务器定义
添加服务器	添加端口
删除服务器	删除端口
漏洞标记为无效	漏洞设置为无效
漏洞标记为有效	漏洞标记为有效
删除地址	删除主机/网络

选择的选项	触发该事件类型的规则...
删除属性值	主机属性删除值
设置属性值	主机属性设置值
设置操作系统定义	设置操作系统定义
设置主机严重性	设置主机严重性

下表介绍将主机输入事件选定为基础事件时如何构建关联规则条件。

表 *135:* 主机输入事件的语法

如果您指定.....	选择运算符，然后.....
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
IP 地址	输入单个 IP 地址或地址块。
来源	选择主机输入数据的源。
源类型	选择主机输入数据的源类型。

相关主题

主机输入事件类型，第 866 页
发现事件字段，第 868 页
Firepower 系统 IP 地址约定，第 26 页

连接事件触发条件的语法

要使关联规则基于连接事件，首先指定要使用的连接事件类型。请注意，可用于连接事件的信息可能会根据系统记录连接的方式、原因和时间而异。您可以选择：

- 位于连接开头或末尾
- 位于连接开头
- 位于连接末尾

下表介绍将连接事件选定为基础事件时如何构建关联规则条件。

表 *136:* 连接事件的语法

如果您指定.....	选择运算符，然后.....
访问控制策略	选择记录连接的一个或多个访问控制策略。

如果您指定.....	选择运算符，然后.....
Access Control Rule Action	选择与记录连接的访问控制规则相关的一个或多个操作。 当网络流量与任何监控规则的条件匹配时，不管随后处理连接的规则或默认操作如何，都选择**监控 (Monitor)** 以触发关联事件。
访问控制规则	输入记录连接的访问控制规则的全部或部分名称。 不管随后处理连接的规则或默认操作如何，您都可以输入其条件与连接匹配的任何监控规则的名称。
应用协议	选择一个或多个与连接相关的应用协议。
应用协议类别	选择一个或多个应用协议类别。
客户端	选择一个或多个客户端。
客户端类别	选择一个或多个客户端类别。
客户端版本	输入客户端的版本号。
连接持续时间	输入连接事件的持续时间，单位为秒。
连接类型	指定是否要根据获取连接信息的方式触发关联规则： • 为已导出 NetFlow 数据生成的连接事件选择**是 (is)** 和 **Netflow**。 • 为 Firepower 系统受管设备检测到的连接事件选择**不是 (is not)** 和 **Netflow**。
目标国家/地区或源国家/地区	选择一个或多个与连接事件中的源或目标 IP 地址相关的国家/地区。
设备	选择一个或多个检测到连接或处理连接（对于已导出 NetFlow 记录的连接数据）的设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
出口接口或入口接口	选择一个或多个接口。
出口安全区域或入口安全区域	选择一个或多个安全区域或隧道区域。
“发起方字节数”(Initiator Bytes)、“响应方字节数”(Responder Bytes) 或“总字节数”(Total Bytes)	输入以下其中一项： • 发送的字节数（**发起方字节数 [Initiator Bytes]**）。 • 接收的字节数（**响应方字节数 [Responder Bytes]**）。 • 发送和接收的字节数（**总字节数 [Total Bytes]**）。
“发起方 IP”、“响应方 IP”、“发起方和响应方 IP”或“发起方 IP 或响应方 IP”	指定单个 IP 地址或地址块。

如果您指定.....	选择运算符，然后.....
“发起方数据包数”(Initiator Packets)、“响应方数据包数”(Responder Packets) 或“数据包总数”(Total Packets)	输入以下其中一项： • 发送的数据包数量（**发起方数据包数 [Initiator Packets]**）。 • 接收的数据包数量（**响应方数据包数 [Responder Packets]**）。 • 发送和接收的数据包数量（**数据包总数 [Total Packets]**）
“发起方端口/ICMP 类型”(Initiator Port/ICMP Type) 或“响应方端口/ICMP 代码”(Responder Port/ICMP Code)	输入发起方流量的端口号或 ICMP 类型或接收方流量的端口号或 ICMP 类型。
IOC 标记	指定危害表现标记**是 (is)** 还是**不是 (is not)** 因为连接事件而设置。
NetBIOS 名称	输入连接中受监控主机的 NetBIOS 名称。
NetFlow 设备	选择要用于触发关联规则的 NetFlow 导出器的 IP 地址。如果没有将任何 NetFlow 导出器添加到网络发现策略，则 **NetFlow 设备 (NetFlow Device)** 下拉列表为空。
预过滤器策略 (Prefilter Policy)	选择一个或多个处理连接的预过滤器策略。
原因	选择一个或多个与连接事件关联的原因。
安全情报类别	选择一个或多个与连接事件关联的安全情报类别。 要将安全情报类别用作连接结束事件的条件，请在访问控制策略中该类别设置到**监控 (Monitor)** 而非**阻止 (Block)** 中。
SSL 实际操作	指定指示系统如何处理加密连接的 SSL 规则操作。
SSL 证书指纹	输入用来加密流量的证书的指纹或选择与指纹相关的使用者公用名。
SSL 证书状态	选择一个或多个与用于加密会话的证书关联的状态。
SSL 证书使用者公用名 (CN)	输入用于加密会话的证书的全部或部分使用者公用名。
SSL 证书使用者国家/地区 (C)	选择一个或多个用于加密会话的证书使用者国家/地区代码。
SSL 证书使用者组织 (O)	输入用于加密会话的证书的全部或部分使用者组织名称。
SSL 证书使用者组织单位 (OU)	输入用于加密会话的证书的全部或部分使用者组织单位名称。
SSL 密码套件	选择一个或多个用于加密会话的加密套件。
SSL 加密会话	选择**已成功解密 (Successfully Decrypted)**。
SSL 流状态	基于系统尝试解密流量的结果选择一种或多种状态。

如果您指定.....	选择运算符，然后.....
SSL 策略	选择一个或多个记录加密连接的 SSL 策略。
SSL 规则名称	输入记录加密连接的 SSL 规则的全部或部分名称。
SSL 服务器名称	输入客户端用来建立加密连接的服务器的全部或部分名称。
SSL URL 类别	选择一个或多个在加密连接中受访的 URL 的 URL 类别。
SSL 版本	选择一个或多个用于加密会话的 SSL 或 TLS 版本。
TCP 标志	选择为了触发关联规则，连接事件必须包含的 TCP 标志。只有 NetFlow 记录生成的连接数据包含 TCP 标志。
传输协议	输入连接使用的传输协议：**TCP** 或 **UDP**。
隧道/预过滤器规则 (Tunnel/Prefilter Rule)	输入处理连接的隧道或预过滤器规则的全部或部分名称。
URL	输入在连接中受访的全部或部分 URL。
URL 类别	选择一个或多个在连接中受访的 URL 的 URL 类别。
URL 信誉	选择一个或多个在连接中受访的 URL 的 URL 信誉值。
用户名	输入登录连接中的任一主机的用户的用户名。
Web 应用程序	选择一个或多个与连接关联的 Web 应用。
Web 应用类别	选择一种或多种 Web 应用类别。

相关主题

连接和 安全相关连接 事件字段，第 717 页
Firepower 系统 IP 地址约定，第 26 页

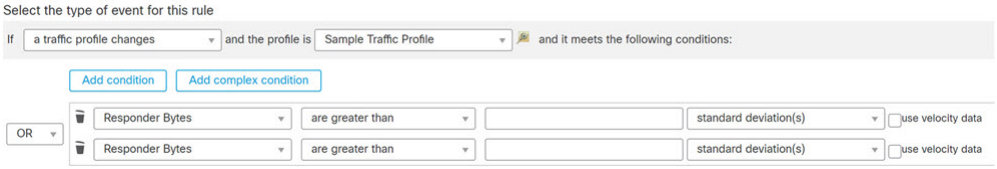
流量量变曲线更改的语法

要使关联规则基于流量量变曲线更改，首先选择要使用的流量量变曲线。当网络流量偏离以您所选量变曲线为特征的模式时，触发此规则。

可以基于原始数据或从计算数据得出的统计结果触发该规则。例如，您可以编写如果通过网络的数据量（单位：字节）突然达到高峰时触发的规则，该高峰可能是由于攻击或其他安全策略违规造成的。如果出现下列两种情况中的一种，可以指定规则触发：

- 通过网络的字节数量激增，超过一定数量的字节
- 通过网络的字节数激增，超过流量平均值上下的一定数量的标准偏差

  请注意，要创建在通过网络的字节数超出一定数量的标准偏差（高于或低于）时触发的规则，必须指定上下限，如下图所示。



要创建在通过网络的字节数超过一定数量的高于平均值的标准偏差时触发的规则，请仅使用图中所示的第一个条件。

要创建在通过网络的字节数超过一定数量的低于平均值的标准偏差时触发的规则，请仅使用第二个条件。

选中**使用速度数据 (use velocity data)** 复选框，以基于数据点之间的变化率触发关联规则。如果要使用上例中的速度数据，则可以指定在出现下列任何一种情况时触发规则：

- 通过网络的字节数量变化幅度非常大，高于或低于一定数量的高于平均变化率的标准偏差
- 通过网络的字节数激增，高于一定数量的字节

下表介绍在将流量量变曲线变更选定为基础事件时如何构建关联规则中的条件。

表 *137:* 流量量变曲线更改的语法

如果您指定.....	选择运算符，然后输入.....	然后选择以下之一.....
连接数	检测到的连接总数 **或** 高于或低于平均值的标准偏差的数量，检测到的连接数量必须在此范围内以触发该规则	连接 标准偏差
总字节数、发起方字节数或响应方字节数	以下任一项： • 发送的总字节数（**字节总数**） • 发送的字节数（**发起方字节数 [Initiator Bytes]**） • 接收的字节数（**响应方字节数 [Responder Bytes]**） **或** 高于或低于平均值的标准偏差的数量，上述条件之一必须在此范围内以触发该规则	字节 标准偏差

如果您指定.....	选择运算符，然后输入.....	然后选择以下之一.....
数据包总数、发起方数据包数或响应方数据包数	以下任一项： • 发送的数据包总数（**数据包总数**） • 发送的数据包数量（**发起方数据包数 [Initiator Packets]**） • 接收的数据包数量（**响应方数据包数 [Responder Packets]**） **或** 高于或低于平均值的标准偏差的数量，上述条件之一必须在此范围内以触发该规则	数据包 标准偏差
独立发起方	发起会话的独立主机的数量 **或** 高于或低于平均值的标准偏差的数量，检测到的独立发起方的数量必须为该平均值以触发该规则	发起方 标准偏差
独立响应方	响应会话的独立主机的数量 **或** 高于或低于平均值的标准偏差的数量，检测到的唯一响应方的数量必须为该平均值以触发该规则	响应方 标准偏差

关联主机配置文件限定条件的语法

要根据事件中所涉及的主机的主机配置文件来限制关联规则，请添加主机配置文件限定条件。不能将主机配置文件限定条件添加到在恶意软件事件、流量量变曲线更改或新的 IP 主机的检测上触发的关联规则。

当构建主机配置文件限定条件时，先指定要用于限制关联规则的主机。可选择的主机取决于规则的基础事件类型：

- 连接事件 - 选择**响应方主机 (Responder Host)** 或**发起方主机 (Initiator Host)**。
- 入侵事件 - 选择**目标主机 (Destination Host)** 或**源主机 (Source Host)**。
- 发现事件、主机输入事件或用户活动 - 选择**主机 (Host)**。

下表介绍如何构建关联规则的主机配置文件限定条件。

表 *138:* 主机配置文件限定条件的语法

如果您指定.....	选择运算符，然后.....
应用协议 (Application Protocol) > 应用协议 (Application Protocol)	选择应用协议。
应用协议 (Application Protocol) > 应用端口 (Application Port)	输入应用协议端口号。
应用协议 (Application Protocol) > 协议 (Protocol)	选择一个协议。
Application Protocol Category	选择类别。
客户端 > 客户端	选择客户端。
客户端 > 客户端版本	输入客户端版本。
客户端类别	选择类别。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾经配置 管理中心以实现多租户时，此字段才存在。
硬件	输入移动设备的硬件型号。例如，要与所有 Apple iPhone 都匹配，请输入 **`iPhone`**。
主机重要性	选择主机重要性。
主机类型	选择一个或多个主机类型。您可以在一个常规主机或多种网络设备中的一种之间选择。
IOC 标记	选择一个或多个危害表现标记。
Jailbroken	选择**是 (Yes)** 表示事件中的主机是破解移动设备，选择**否 (No)** 表示其不是破解移动设备。
MAC 地址 > MAC 地址	输入主机的全部或部分 MAC 地址。
MAC 地址 > MAC 类型	选择 MAC 类型是否为“按 ARP/DHCP 检测”(ARP/DHCP detected)： • 系统是否明确地将 MAC 地址识别为属于主机（**按 ARP/DHCP 检测 [ARP/DHCP Detected]**） • 打个比方，因为设备和主机之间有路由器，所以系统看到许多主机具有该 MAC 地址（**不按 ARP/DHCP 检测 [is not ARP/DHCP Detected]**） • MAC 类型不相关（**为任意 [is any]**）
MAC 供应商	输入主机使用的硬件的全部或部分 MAC 供应商。
移动	选择**是 (Yes)** 表示事件中的主机是移动设备，选择**否 (No)** 表示其不是移动设备。

如果您指定.....	选择运算符，然后.....
NetBIOS 名称	输入主机的 NetBIOS 名称。
网络协议	输入 http://www.iana.org/assignments/ethernet-numbers 中所列的网络协议编号。
操作系统 > 操作系统供应商	选择一个或多个操作系统供应商名称。
操作系统 > 操作系统名称	选择一个或多个操作系统名称。
操作系统 > 操作系统版本	选择一个或多个操作系统版本。
传输协议	输入 http://www.iana.org/assignments/protocol-numbers 中所列的传输协议的名称或编号。
VLAN ID	输入主机的 VLAN ID 号。
Web 应用程序	选择 Web 应用。
Web 应用类别	选择类别。
任何可用的主机属性，包括默认合规性 allow 名单主机属性	根据主机属性类型输入或选择适合的值。

使用隐含或通用客户端来构建主机配置文件限定条件

如果系统报告检测到的客户端使用的应用协议名称后跟 `client`（例如，`HTTPS client`），则该客户端是隐含或通用客户端。在这些情况下，系统未检测到特定客户端，但根据服务器响应流量推断客户端的存在。

要使用隐含或通用客户端创建主机配置文件限定条件，应限制使用在响应方主机上而不是客户端上运行的应用协议。

使用事件数据来构建主机配置文件限定条件

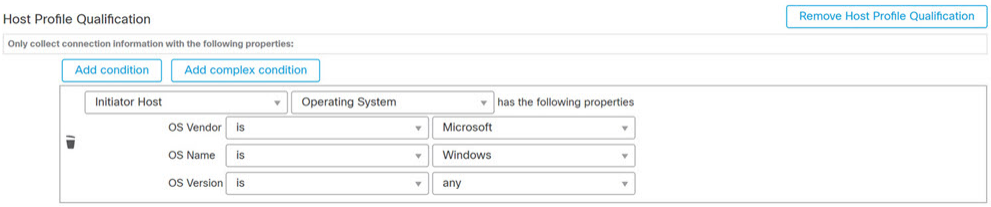
在构建主机配置文件限定条件时，通常可以使用关联规则的基础事件中的数据。

例如，当系统检测到受监控主机之一使用了特定浏览器时，假设触发关联规则。进一步假设，当检测此使用时，如果浏览器版本不是最新版本，则您要生成事件。

您可将主机配置文件限定条件添加到此关联规则，以便只有在**客户端 (Client)** 是**事件客户端 (Event Client)**，但**客户端版本 (Client Version)** 不是最新版本的情况下才会触发规则。

主机配置文件限定条件示例

下列主机配置文件限定条件会限制关联规则，以便该规则仅在涉及作为其基础的发现事件的主机运行一个 Microsoft Windows 版本时才触发。



相关主题

主机数据字段，第 870 页

用户资格的语法

如果您使用连接事件、入侵事件、发现事件或主机输入事件触发关联规则，则您可以基于涉及事件的用户的标识限制该规则。此限制称为用户资格。例如，您可以限制关联规则，以便仅当源用户或目标用户源自销售部门时才会触发关联规则。

不能将用户资格添加到在流量量变曲线发生更改或检测到用户活动时触发的关联规则中。此外，系统还通过在身份领域中建立的管理中心-服务器连接获取用户详细信息。该信息不能提供给数据库中的所有用户。

当构建用户资格时，先指定要用于限制关联规则的身份。可选择的身份取决于规则的基础事件类型：

- 连接事件 - 选择**发起方身份**或**响应方身份**。
- 入侵事件 - 选择**目标身份**或**源身份**。
- 发现事件 - 选择**主机身份 (Identity on Host)**。
- 主机输入事件 - 选择**主机身份 (Identity on Host)**。

下表介绍如何构建关联规则的用户资格。

表 *139:* 用户资格的语法

如果您指定.....	选择运算符，然后.....
身份验证协议	选择用于检测用户的身份验证协议（或用户类型协议）。
部门	输入部门。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾经配置 管理中心以实现多租户时，此字段才存在。
电子邮件	输入邮箱地址。
名字	输入名字。
姓氏	输入姓氏。
电话	输入电话号码。

如果您指定.....	选择运算符，然后.....
用户名	输入用户名。

相关主题

用户数据字段

连接跟踪器

连接跟踪器限制关联规则，以便在满足规则的初始条件后（包括主机配置文件和用户资格），系统开始跟踪某些连接。如果跟踪的连接满足在指定的时间段内收集到的其他条件，则系统会为规则生成关联事件。

提示 通常，连接跟踪器监控非常具体的流量，而且当被触发时，仅运行指定的一段时间。将连接跟踪器与流量量变曲线进行对比，发现后者一般监控的网络流量范围比较广并且持续运行。

连接跟踪器可以通过两种方法生成事件。

满足条件时，立即触发的连接跟踪器

可以配置连接跟踪器，以便在网络流量满足跟踪器的条件时，立即触发关联规则。如果出现这种情况，即使还没有超过超时周期，系统也为该连接跟踪器实例停止跟踪连接。如果此前触发关联规则的相同类型的策略违规再次发生，则系统可创建新的连接跟踪器。

但是，如果在网络流量满足连接跟踪器中的条件之前时间到期，则系统不会生成关联事件，并且还会停止跟踪该规则实例的连接。

例如，只有在特定类型的连接发生的次数超过一定时间周期内的具体次数时，连接跟踪器才可以通过生成关联事件作为一种事件阈值。或者，只有在初始连接之后，系统检测到过多数据传输时，才可以生成关联事件。

在超时期结束时触发的连接跟踪器

可以配置连接跟踪器，以便连接跟踪器可依靠在整个超时周期内搜集到的数据，因此在超时期结束前，您不能触发该连接跟踪器。

例如，如果将连接跟踪器配置为在特定时间段内检测到的字节数少于特定的传输字节数时触发，则系统在那段时间终止前处于等待状态，然后再在网络流量满足该条件时生成事件。

添加连接跟踪器

开始之前

- 根据连接、入侵、发现、用户身份或主机输入事件创建关联策略。不能将连接跟踪器添加到基于恶意软件事件或流量量变曲线更改的规则。

过程

步骤 1 在关联规则编辑器（**策略** > **关联** > **规则管理**）中，点击编辑，然后点击 **添加连接跟踪器**。

步骤 2 指定要跟踪的连接；请参阅连接跟踪器的语法，第 963 页。

步骤 3 根据跟踪的连接，指定要生成关联事件的时间；请参阅连接跟踪器事件的语法，第 965 页。

步骤 4 指定在此期间必须满足跟踪器的条件的时间间隔（单位：秒、分或小时）。

连接跟踪器的语法

下表介绍如何构建指定要跟踪的连接种类的连接跟踪器条件。

表 *140:* 连接跟踪器的语法

如果您指定.....	选择运算符，然后.....
访问控制策略	选择一个或多个处理要跟踪的连接的访问控制策略。
访问控制规则操作	选择一个或多个与记录要跟踪的连接的访问控制规则关联的访问控制规则操作。 不管随后处理连接的规则或默认操作如何，请选择**监控 (Monitor)** 以跟踪与任何监控规则的条件匹配的连接。
访问控制规则名称	输入记录要跟踪的连接的访问控制规则的全部或部分名称。 要跟踪匹配监控规则的连接，请输入监控规则的名称。不管随后处理连接的规则或默认操作如何，系统都对连接进行跟踪。
应用协议	选择一个或多个应用协议。
应用协议类别	选择一个或多个应用协议类别。
客户端	选择一个或多个客户端。
客户端类别	选择一个或多个客户端类别。
客户端版本	输入客户端的版本。
连接持续时间	输入连接持续时间，以秒为单位。
连接类型	指定是否要根据获取连接信息的方式触发关联规则： • 为已导出 NetFlow 记录生成的连接事件选择**是 (is)** 和 **Netflow**。 • 为 Firepower 系统受管设备检测到的连接事件选择**不是 (is not)** 和 **Netflow**。
目标国家/地区或源国家/地区	选择一个或多个国家/地区。
设备	选择一个或多个要跟踪其已检测连接的设备。如果要跟踪 NetFlow 连接，请选择处理来自已导出 NetFlow 记录的连接数据的设备。

如果您指定.....	选择运算符，然后.....
入口接口或出口接口	选择一个或多个接口。
“入口安全区域”(Ingress Security Zone) 或“出口安全区域”(Egress Security Zone)	选择一个或多个安全区域或隧道区域。
“发起方 IP”(Initiator IP)、“响应方 IP”(Responder IP)、或“发起方/响应方 IP”(Initiator/Responder IP)	输入单个 IP 地址或地址块。
“发起方字节数”(Initiator Bytes)、“响应方字节数”(Responder Bytes) 或“总字节数”(Total Bytes)	输入以下其中一项： • 发送的字节数（**发起方字节数 [Initiator Bytes]**） • 接收的字节数（**响应方字节数 [Responder Bytes]**） • 发送和接收的字节数（**总字节数 [Total Bytes]**）
“发起方数据包数”(Initiator Packets)、“响应方数据包数”(Responder Packets) 或“数据包总数”(Total Packets)	输入以下其中一项： • 发送的数据包数量（**发起方数据包数 [Initiator Packets]**） • 接收的数据包数量（**响应方数据包数 [Responder Packets]**） • 发送和接收的数据包数量（**数据包总数 [Total Packets]**）
“发起方端口/ICMP 类型”(Initiator Port/ICMP Type) 或“响应方端口/ICMP 代码”(Responder Port/ICMP Code)	输入发起方流量的端口号或 ICMP 类型或接收方流量的端口号或 ICMP 类型。
IOC 标记	选择危害表现标记是**已设置 (is)** 还是**未设置 (is not)**。
NETBIOS 名称	输入连接中受监控主机的 NetBIOS 名称。
NetFlow 设备	选择要跟踪的 NetFlow 导出器的 IP 地址。如果没有将任何 NetFlow 导出器添加到网络发现策略，则“NetFlow 设备”(NetFlow Device) 下拉列表为空。
预过滤器策略 (Prefilter Policy)	选择一个或多个处理要跟踪的连接的预过滤器策略。
原因	选择一个或多个与要跟踪的连接关联的原因。
安全情报类别	选择一个或多个与要跟踪的连接关联的安全情报类别。
TCP 标志	选择为了跟踪连接在连接中必须包含的 TCP 标志。只有导出的 NetFlow 记录生成的连接包含 TCP 标志数据。
传输协议	选择连接使用的传输协议。

如果您指定.....	选择运算符，然后.....
URL	输入要跟踪的连接中受访的全部或部分 URL。
URL 类别	选择要跟踪的连接中受访的 URL 的一个或多个 URL 类别。
URL 信誉	选择要跟踪的连接中受访的 URL 的一个或多个 URL 信誉值。
用户名	输入登录要跟踪的连接中的任一主机的用户的用户名。
Web 应用程序	选择一个或多个 Web 应用。
Web 应用类别	选择一个或多个 Web 应用类别。

使用事件数据构建连接跟踪器

在构建连接跟踪器时，通常可以使用关联规则的基础事件中的数据。

例如，假设系统检测到新客户端时会触发关联规则。将连接跟踪器添加到此类型的关联规则时，系统会自动向跟踪器填充指向基础事件的限制：

- **发起方/响应方 IP (Initiator/Responder IP)** 设置为**事件 IP 地址 (Event IP Address)**。
- **客户端 (Client)** 设置为**事件客户端 (Event Client)**。

提示 要跟踪特定 IP 地址或 IP 地址块的连接，请点击**切换至手动输入 (switch to manual entry)** 以手动指定 IP。点击 **switch to event fields** 返回以使用事件中的 IP 地址。

相关主题

连接和 安全相关连接 事件字段，第 717 页
Firepower 系统 IP 地址约定，第 26 页

连接跟踪器事件的语法

下表介绍如何构建指定何时基于正在跟踪的连接生成关联事件的连接跟踪器条件。

表 *141:* 连接跟踪器事件的语法

如果您指定.....	选择运算符，然后输入.....
连接数	检测到的连接总数
SSL 加密会话数	检测到的 SSL 或 TLS 加密会话的总数

如果您指定.....	选择运算符，然后输入.....
总字节数、发起方字节数或响应方字节数	以下任一项： • 发送的总字节数（**字节总数**） • 发送的字节数（**发起方字节数 [Initiator Bytes]**） • 接收的字节数（**响应方字节数 [Responder Bytes]**）
数据包总数、发起方数据包数或响应方数据包数	以下任一项： • 发送的数据包总数（**数据包总数**） • 发送的数据包数量（**发起方数据包数 [Initiator Packets]**） • 接收的数据包数量（**响应方数据包数 [Responder Packets]**）
独立发起方或 独立响应方	以下任一项： • 检测到的发起会话的独立主机的数量 (**Unique Initiators**) • 响应检测到的连接的独立主机的数量 (**Unique Responders**)

外部主机连接过多的配置示例

考虑这样一个场景：您将敏感文件存档到网络 10.1.0.0/16 上，而且该网络外的主机通常不向网络内的主机发起连接。网络外的主机偶尔会发起连接，但您已确定如果在两分钟内发起四次或更多次的连接，则说明有令人担心的问题。

下图所示规则规定当 10.1.0.0/16 网络外的主机向网络内的主机发起连接时，系统将开始跟踪符合该标准的连接。然后，如果系统在两分钟内检测到匹配该签名的四次连接（包括原始连接），系统会生成关联事件。

Rule Information

Add User

Rule Name: Archive Connections - Outside

Rule Description: Trigger on 4 ouside connections tc

Rule Group: Ungrouped

Select the type of event for this rule

If: a connection event occurs | at either the beginning or the en | and it meets the following conditions:

Add condition | Add complex condition

OR

Initiator IP | is not in | 10.1.0.0/16

Responder IP | is in | 10.1.0.0/16

Connection Tracker

... start tracking connections that meet the following conditions:

Add condition | Add complex condition

AND

Initiator IP | is not in | 10.1.0.0/16

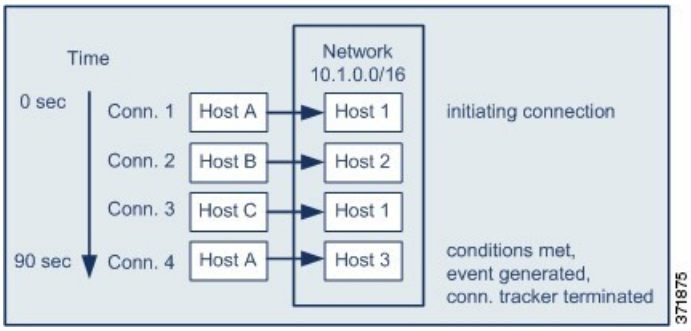
Responder IP | is in | 10.1.0.0/16

... and generate an event if:

Add condition | Add complex condition

total | Number of Connections | are greater than or equal to | 4

下图显示网络流量如何触发上述关联规则。



在本示例中，系统检测到满足关联规则基本条件的连接，即系统检测到从 10.1.0.0/16 网络外的主机到该网络内主机的连接。这样创建连接跟踪器。

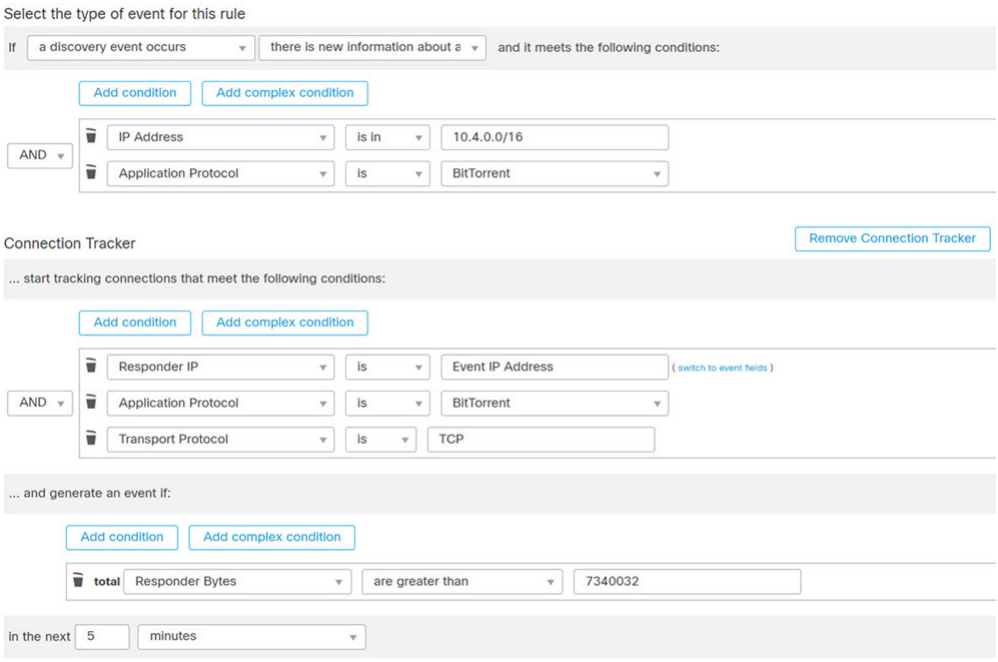
处理连接跟踪器的阶段如下：

- 首先，当系统检测到从网络外的主机 A 向网络内的主机 1 进行的连接时，系统开始跟踪连接。
- 系统又检测到符合连接跟踪器特征的两次连接：Host B 至 Host 2 和 Host C 至 Host 1。
- 当在两分钟的时间限制内 Host A 连接到 Host 3 时，系统检测到第四次符合特征的连接。满足规则条件。
- 最后，系统生成关联事件，且系统停止跟踪连接。

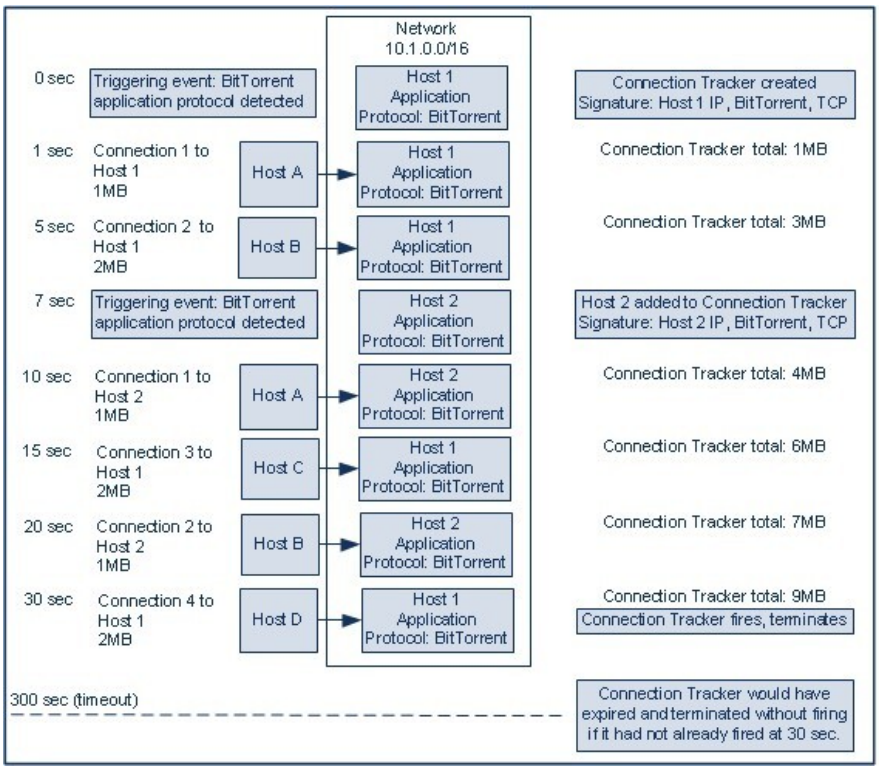
BitTorrent 数据传输过多的配置示例

考虑这样一个场景：您希望在初始连接受监控网络的任何主机后，如果系统检测到 BitTorrent 数据传输量过多，则生成一个关联事件。

下图显示当系统检测到受监控网络上的 BitTorrent 应用协议时触发的关联规则。该规则具有限制规则的连接跟踪器，以便仅当受监控网络（在本例中为 10.1.0.0/16）上的主机在出现初始策略违规后的五分钟内通过 BitTorrent 传输的总数据超过 7 MB（7340032 字节）时触发该规则。



下图显示网络流量如何触发上述关联规则。



在本示例中，系统在两个不同的主机上检测到 BitTorrent TCP 应用协议：Host 1 和 Host 2。这两台主机通过 BitTorrent 将数据传输到其他四台主机：Host A、Host B、Host C 和 Host D。

处理该连接跟踪器的阶段如下：

- 首先，当系统检测到 Host 1 上的 BitTorrent 应用协议时，系统开始跟踪 0 秒标记处的连接。请注意，如果系统在接下来的 5 分钟（到 300 秒标记）内未检测到 7 MB 的 BitTorrent TCP 传输数据，则连接跟踪器将过期。
- 5 秒钟时，Host 1 已经传输符合特征的 3 MB 数据：
  - 在 1 秒标记处时，从 Host 1 传输至 Host A 的 1 MB 的数据量 （1MB 符合连接跟踪器条件的 BitTorrent 总流量）
  - 在 5 秒标记处时，从 Host 1 传输至 Host B 的 2MB 的数据量（总共 3MB）
- 在 7 秒种时，系统在 Host 2 上检测到 BitTorrent 应用协议，同时也开始跟踪该主机的 BitTorrent 连接。
- 在 20 秒种时，系统已经检测到从 Host 1 和 Host 2 传输的符合特征的其他数据：
  - 在 10 秒标记处时，从 Host 2 传输至 Host A 的 1MB 的数据量（总共 4MB）
  - 在 15 秒标记处时，从 Host 1 传输至 Host C 的 2 MB 的数据量（总共 6 MB）
  - 在 20 秒标记处时，从 Host 2 传输至 Host B 的 1MB 的数据量（总共 7MB）

- 尽管 Host 1 和 Host 2 目前已经传输 7 MB 的 BitTorrent 综合数据，但因为传输字节总数必须**超过** 7 MB，所以规则不会触发（**响应方字节数超过 7340032 [Responder Bytes are greater than 7340032]**）。此时，如果系统在跟踪器超时期间余下的 280 秒内没有检测到其他 BitTorrent 数据传输，则跟踪器过期且系统不会生成关联事件。
- 但是，在 30 秒钟时，系统检测到其他 BitTorrent 传输，且满足规则条件：
  - 在 30 秒标记处时，2 MB 数据从 Host 1 传输至 Host D（总共 9 MB）
- 最后，系统会生成关联事件。此外，尽管 5 分钟的周期尚未过期，但是在该连接跟踪器示例中，系统也停止跟踪连接。如果此时系统检测到使用 BitTorrent TCP 应用协议的新连接，则系统会创建新的连接跟踪器。请注意，在 Host 1 向 Host D 传输总计 2 MB 的数据后，系统生成关联事件，因为其在会话终止后才会计算连接数据。

暂停和非活动周期

您可以在关联规则中配置暂停周期。当关联规则触发时，即使在指定间隔期间违反该规则，暂停周期也会指示系统在该间隔内停止触发该规则。在暂停周期过后，规则可以再次触发（并开始进入新的暂停周期）。

例如，您网络上的某个主机可能不应产生流量。每当系统检测到涉及该主机的连接时都会触发一个的简单关联规则，致使可能在短时间内创建多个关联事件，具体取决于发往和来自该主机的网络流量。要限制披露策略违规的关联事件数量，可以添加暂停周期，以便仅为系统检测到的涉及该主机的第一个连接（在指定的时间周期内）生成关联事件。

此外，还可以在关联规则中设置非活动周期。在非活动周期，关联规则将不会触发。您可以将非活动周期设置为每日、每周或每月循环。例如，您每天可能会对内部网络执行夜间 Nmap 扫描，以查找主机操作系统的变化情况。在这种情况下，可以对扫描时间和期间影响到的关联规则设置一个每天非活动周期，以便那些规则不会被错误地触发。

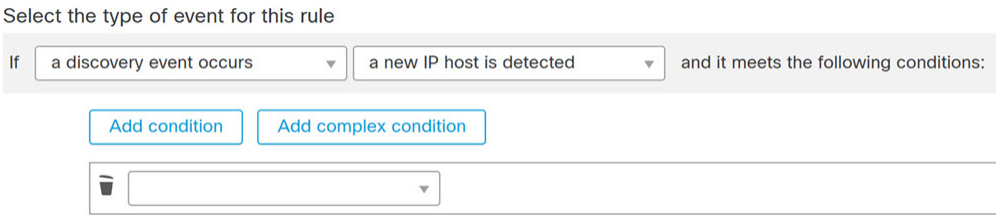
关联规则构建机制

您可通过指定触发条件来构建关联规则。您可以在条件中使用的语法会根据您正在创建的元素而变化，但是机制相同。

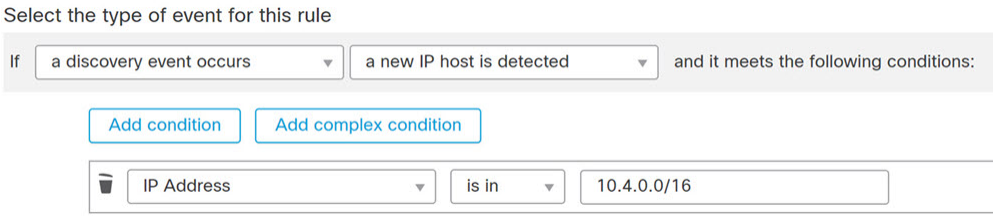
大多数条件有三部分：类别、运算符和值。

- 可选择的类别取决于您是在构建关联规则触发器、主机配置文件限定条件、连接跟踪器还是用户资格。在关联规则触发器中，类别的划分进一步取决于规则的基础事件类型。某些条件可能包含多个类别，每个类别都可能有自己的运算符和值。
- 条件的可用运算符取决于类别。
- 可用于指定条件值的语法取决于类别和运算符。有时侯，您可以在文本字段键入值。有时候，您可以从下拉列表中选择一个值（或多个值）。

例如，如果要在每次检测到新主机时都生成关联事件，则可以创建无条件的简单规则。



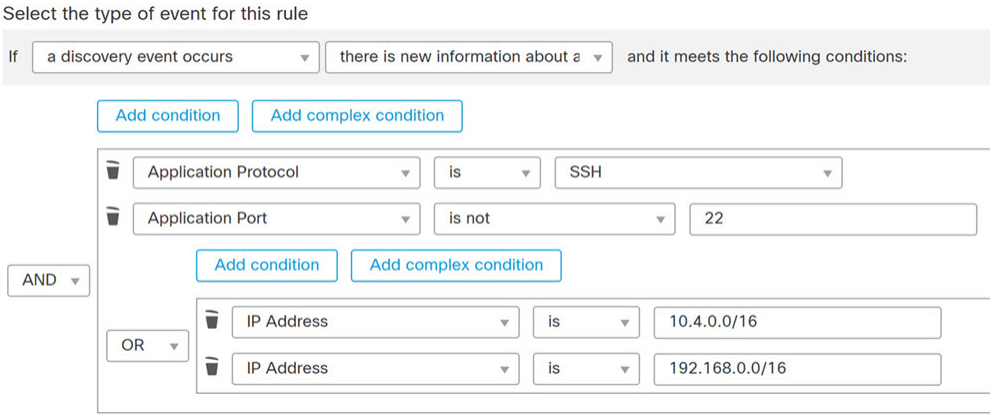
如果要在仅当 10.4.x.x 网络中检测到该新的主机时进一步限制规则并生成事件，则可以添加一个条件。



当构建的结构不止一个条件时，必须使用 **AND** 或 **OR** 运算符将这些条件结合起来。相同级别的条件会被放在一起评估：

- **AND** 运算符要求必须满足其控制的级别上的所有条件。
- **OR** 运算符要求必须满足其控制的级别上的至少一个条件。

检测 10.4.x.x 网络和 192.168.x.x 网络上的非标准端口的 SSH 活动的以下规则具有四个条件，底部的两个的条件较复杂。



从逻辑上讲，该规则被评估如下：

```
(A and B and (C or D))
```

表 *142:* 规则评估

关键字	为陈述以下情况的条件.....
A	应用协议为 SSH

关键字	为陈述以下情况的条件.....
B	应用端口不是 22
选	IP 地址为 10.0.0.0/8
D	IP 地址为 196.168.0.0/16

注意 评估触发常见事件的复杂关联规则可降低系统的性能。例如，系统必须根据每个已记录的连接评估的多条件规则可能会导致资源超载。

关联规则中的添加和连接条件

过程

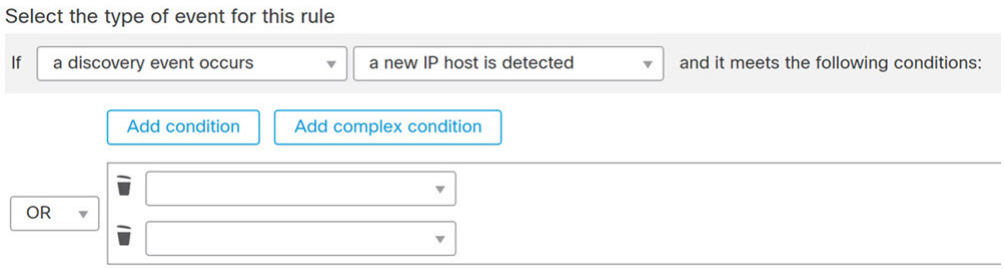
步骤 1 在关联规则编辑器中 (**策略** > **关联** > **规则管理**)，添加简单或复杂条件：

- 简单 - 点击**添加条件 (Add condition)**。
- 复杂 - 点击**添加复杂条件 (Add complex condition)**。

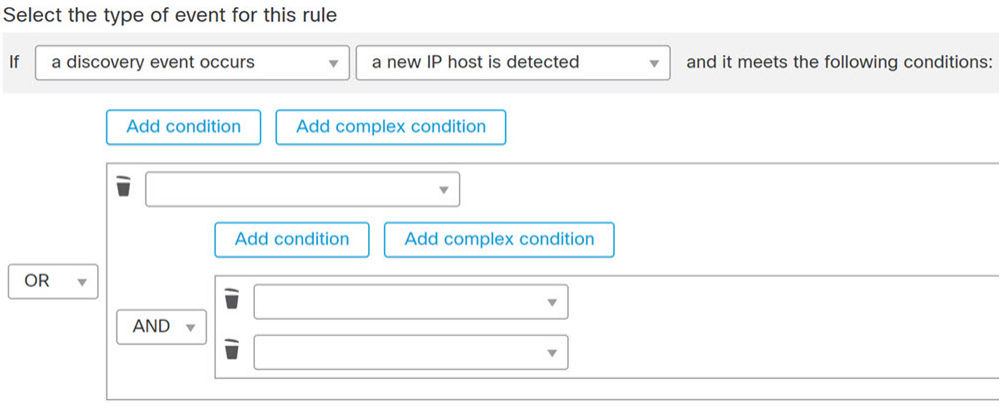
步骤 2 通过从条件左侧的下拉列表中选择 **AND** 或 **OR** 运算符来连接条件。

示例：简单和复杂条件

下图显示具有使用 **OR** 运算符结合的两个简单条件的关联规则。



下图显示具有使用**OR**运算符结合的一个简单条件和一个复杂条件的关联规则。复杂条件包括使用 **AND** 运算符结合的两个简单条件。



在关联规则条件中使用多个值

在构建关联条件且条件语法允许您从下拉列表中选择值时，通常可以从列表中选择多个值。

过程

步骤 1 在关联条件编辑器中，构建条件，选择 **is in** 或 **is not in** 作为运算符。

步骤 2 点击文本字段或**编辑 (Edit)** 链接的任意位置。

步骤 3 在**可用 (Available)** 下，选择多个值。也可以点击并拖动以选择多个相邻值。

步骤 4 点击右箭头 (>) 将选定条目移动到**选定项 (Selected)** 中。

步骤 5 点击**确定 (OK)**。

管理关联规则

在多域部署中，系统会显示在当前域中创建的关联规则和组，您可以对这些关联规则和组进行编辑。它还显示祖先域中的所选关联规则和组，您无法对这些关联规则和组进行编辑。要查看和编辑在较低域中创建的关联规则和组，请切换至该域。

注释 如果配置暴露有关不相关域的信息（包括名称、受管设备等），则系统不会显示祖先域的配置。

对活动关联策略中的规则进行的更改会立即生效。

开始之前

- 如果要删除规则，请从所有关联策略中将其删除，如管理关联策略，第 942 页中所述。

过程

步骤 1 选择 策略 > 关联，然后点击 规则管理。

步骤 2 管理规则：

- 创建 - 点击**创建规则 (Create Rule)**；请参阅配置关联规则，第 943 页。
- 创建组 - 点击**创建组 (Create Group)**，输入组的名称，然后点击**保存 (Save)**。要向组中添加规则，请编辑该规则。
- 编辑 - 点击 **编辑**（）；请参阅 配置关联规则，第 943 页。 如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除规则或规则组 - 点击 **删除**（）。删除规则组会对规则取消分组。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

配置关联响应组

您可以创建警报和补救的关联响应组，然后将该组激活并分配到活动关联策略中的关联规则。当网络流量与关联规则相匹配时，系统会启动所有分组的响应。

在活动关联策略中使用时，对活动组或其任何分组响应的更改会立即生效。

过程

步骤 1 选择**策略** > **关联**，然后点击**组**。

步骤 2 点击 **Create Group**。

步骤 3 输入 **Name**。

步骤 4 如果在创建后激活组，请选中**活动 (Active)** 复选框。

已停用的组不会启动响应。

步骤 5 选择对组的**可用响应 (Available Responses)**，然后点击向右箭头 (>) 以将其移至**组中的响应 (Responses in Group)**。要向另一边移动响应，请使用向左箭头 (<)。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 如果在创建后未激活组并要立即将其激活，请点击滑块。

相关主题

Cisco Secure Firewall Management Center 警报响应，第 531 页
补救简介，第 989 页

管理关联响应组

如果关联策略中没有使用响应组，可以删除该组。删除响应组将取消对响应的分组。您也可以在不删除响应组的情况下，暂时停用响应组。这样可以在系统中保留响应组，但在违反策略时不会启动响应组。

在多域部署中，系统会显示在当前域中创建的组，您可以对其进行编辑。系统还会显示在祖先域中创建的组，您不可以对其进行编辑。要查看和编辑在较低域中创建的组，请切换至该域。

对活动的、正在使用的相应组进行的更改会立即生效。

过程

步骤 1 选择**策略** > **关联**，然后点击**组**。

步骤 2 管理响应组：

- 激活或停用 - 点击滑块。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 创建 - 点击**创建组 (Create Group)**；请参阅配置关联响应组，第 974 页。
- 编辑 - 点击 **编辑**（ ）；请参阅 配置关联响应组，第 974 页。 如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除 - 点击 **删除**（ ）。 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。

第 40 章

流量分析

以下主题介绍如何配置流量量变曲线：

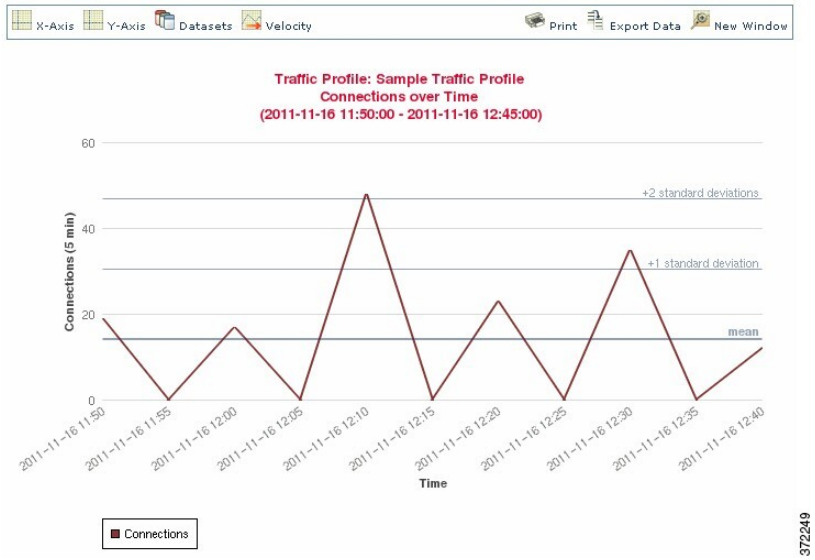
流量量变曲线简介

流量量变曲线是基于在分析时间窗口 (PTW) 收集的连接数据的网络流量图形。此测量可能表示正常网络流量。在学习期后，可以通过对照量变曲线评估新的流量来检测异常网络流量。

默认 PTW 是一周，但是，您可以将其更改为短至 1 小时或长至几周。默认情况下，流量量变曲线会生成系统在五分钟时间区间内生成的连接事件的统计数据。但是，可以将此采样率增加到长达 1 小时。

提示 思科建议 PTW 至少包含 100 个数据点。配置 PTW 和采样率，以便流量量变曲线包含足够的数据以具备统计意义。

下图显示了 PTW 为一天及采样率为五分钟的流量量变曲线。



您也可以在流量量变曲线中设置非活动周期。流量量变曲线在非活动周期内收集数据，但在计算量变曲线统计数据不使用该数据。一段时间内划分的流量量变曲线图可显示非活动周期为阴影区域。

例如，可以考虑所有工作站均在每晚午夜时备份的网络基础设施。备份大约需要30分钟，并将使网络流量达到峰值。可以为流量量变曲线配置周期性非活动周期，以与计划备份相符。

注释 系统使用连接结束数据创建连接图和流量量变曲线。要使用流量量变曲线，请确保将连接结束事件记录到 管理中心数据库。

实施流量量变曲线

当激活流量量变曲线时，系统会收集并评估所配置的学习期 (PTW) 的连接数据。在学习期后，系统评估根据流量量变曲线编写的关联规则。

例如，您可写入当通过网络的数据量（单位为数据包、KB或连接数）突然达到平均流量以上三个标准差的峰值时触发的规则，这可能表示出现攻击或其他安全策略违规。然后，您可以包括关联策略中的规则以警告您流量达到峰值或执行补救措施作为响应措施。

以流量量变曲线为目标

量变曲线条件和主机配置文件限定条件限制流量量变曲线。

使用量变曲线条件，可以分析所有网络流量，也可以将流量量变曲线限用于监控域、域内或跨域的子网或者单个主机。在多域部署中：

- 分叶域管理员可以分析其分叶域内的网络流量。
- 较高级别的域管理员可以在域内或跨域分析流量。

量变曲线条件还可以使用基于连接数据的条件来限制流量量变曲线。例如，可以设置量变曲线条件，以便流量量变曲线仅使用特定端口、协议或应用来分析会话。

最后，还可以使用有关被跟踪主机的信息来限制流量量变曲线。此类限制被称为主机配置条件限定条件。例如，可以仅收集具有高重要性的主机的连接数据。

注释 将流量量变曲线限于较高级别的域可汇聚并分析**每个**后代分叶域中**相同**类型的流量。系统会为每个分叶域构建单独的网络映射。在多域部署中，跨域分析流量可能会出现意外结果。

相关主题

关联策略和规则简介，第 939 页

流量量变曲线条件

您可以创建简单的流量量变曲线条件和主机配置文件限定条件，也可以通过结合和嵌套条件创建较复杂的结构。

条件有三部分：类别、运算符和值。

- 可以使用的类别取决于是构建流量量变曲线条件还是主机配置文件限定条件。
- 可以使用的运算符取决于选择的类别。
- 可用于指定条件值的语法取决于类别和运算符。有时侯，必须在文本字段键入值。有时候，可以从下拉列表中选择一个或多个值。

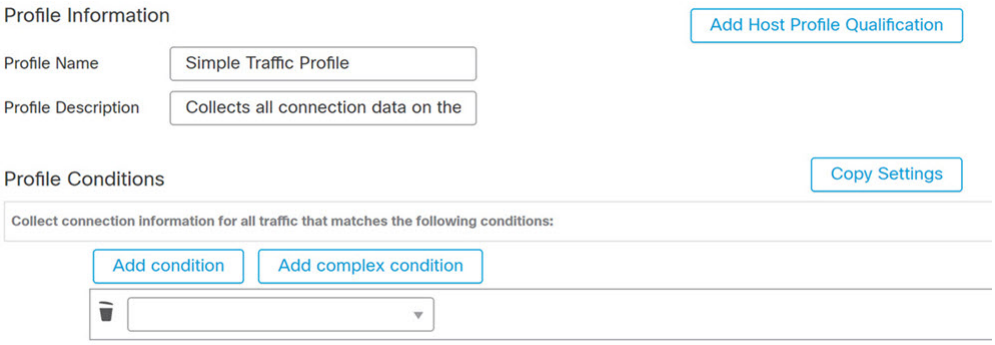
对于主机配置文件限定条件，还必须指定是否使用有关发起或响应主机的信息数据限制流量量变曲线。

当构建的结构不止一个条件时，必须使用 **AND** 或 **OR** 运算符将这些条件结合起来。相同级别的条件会被放在一起评估：

- **AND** 运算符要求必须满足其控制的级别上的所有条件。
- **OR** 运算符要求必须满足其控制的级别上的至少一个条件。

受限制的流量量变曲线

如果要创建为整个监控网段收集数据的流量量变曲线，可以创建一个非常简单的不带条件的流量量变曲线，如下图所示。



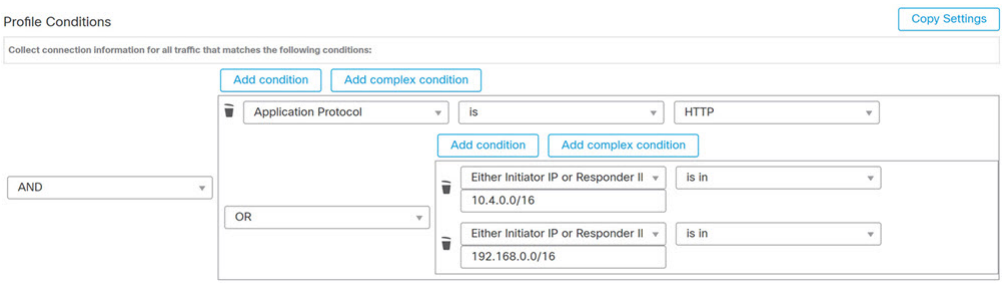
简单流量量变曲线

如果要仅为子网限制流量量变曲线和收集数据，可以添加单个条件，如下图所示。

复杂流量量变曲线

以下流量量变曲线包含以 **AND** 连接的两个条件。这意味着流量量变曲线仅会在两种条件均为真时收集连接数据。在本示例中，它会收集所有 IP 地址在特定子网中的主机的 HTTP 连接。

相反，在任意一个子网中收集HTTP活动连接数据的以下流量量变曲线有三个条件，最后一个构成复杂条件。



从逻辑上讲，上述流量量变曲线应如下进行评估：

```
(A and (B or C))
```

关键字	为陈述以下情况的条件.....
A	应用协议名称是 HTTP
B	IP 地址为 10.4.0.0/16
C	IP 地址为 192.168.0.0/16

流量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
- 发现管理员

管理流量量变曲线

只有对处于活动状态的完整流量量变曲线写入的规则才可触发关联策略违规。每个流量量变曲线旁边的滑块表示该配置文件是否处于活动状态并正在收集数据。进度条显示流量量变曲线学习期的状态。

在多域部署中，系统会显示在当前域中创建的流量量变曲线，您可以对其进行编辑。系统还会显示祖先域中的选定流量量变曲线，您不可以对其进行编辑。要查看和编辑在较低域中创建的流量量变曲线，请切换至该域。

注释 如果祖先域中的流量量变曲线的条件可透露无关域的信息（包括名称、受管设备等），则系统不会显示该配置文件。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **流量量变曲线**。

步骤 2 管理流量量变曲线：

- 激活/停用 - 要激活或停用流量量变曲线，请点击滑块。停用流量量变曲线会删除其关联的数据。如果重新激活该配置文件，必须等待 PTW 时长后，对其写入的规则才会触发。
- 创建 - 要创建新的流量量变曲线，请点击**新建配置文件**，然后如配置流量量变曲线，第 982 页中所述继续操作。您也可以点击 **复制**（）编辑现有流量量变曲线的副本。
- 删除 - 要删除流量量变曲线，请点击 **删除**（），然后确认您的选择。
- 编辑 - 要修改现有流量量变曲线，请点击 **编辑**（），然后如配置流量量变曲线，第 982 页中所述继续操作。如果流量量变曲线处于活动状态，则只能更改其名称和说明。
- 图表 - 要查看图表形式的流量量变曲线，请点击 **图形**（）。在多域部署中，如果属于祖先域的流量量变曲线的图表可透露无关域的信息，则无法查看该图表。

配置流量量变曲线

将流量量变曲线限于较高级别的域可汇聚并分析**每个**后代分叶域中**相同**类型的流量。系统会为每个分叶域构建单独的网络映射。在多域部署中，跨域分析流量可能会出现意外结果。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **流量量变曲线**。

步骤 2 点击 **New Profile**。

步骤 3 输入**配置文件名称 (Profile Name)** 和输入**配置文件说明 (Profile Description)**（可选）。

步骤 4 或者，限制流量量变曲线：

- “复制设置”(Copy Settings) - 要复制某个现有流量量变曲线的设置，请点击**复制设置 (Copy Settings)**，选择要使用的流量量变曲线，然后点击**加载 (Load)**。
- “配置文件条件”(Profile Conditions) - 要使用被跟踪连接的信息限制流量量变曲线，请按添加流量量变曲线条件，第 983 页中所述进行操作。
- “主机配置文件限定条件”(Host Profile Qualification) - 要使用被跟踪主机的信息限制流量量变曲线，请按将主机配置文件限定条件添加到流量量变曲线中，第 984 页中所述进行操作。
- “分析时间窗口 (PTW)”(Profiling Time Window [PTW]) - 要更改**分析时间窗口 (Profiling Time Window)**，请输入时间单位，然后选择**小时数 (hour[s])**、**天数 (day[s])** 或**周数 (week[s])**。
- “采样率”(Sampling Rate) - 选择**采样率 (Sampling Rate)**（以分钟为单位）。
- “非活动周期”(Inactive Period) - 点击**添加非活动周期 (Add Inactive Period)**，然后使用下拉列表指定希望流量量变曲线保持非活动的时间和频率。非活动流量量变曲线不会触发关联规则。流量量变曲线不包含配置文件统计信息中非活动时期的数据。

步骤 5 保存流量量变曲线：

- 要保存量变曲线并立即开始收集数据，请点击 **Save & Activate**。
- 要保存量变曲线而不激活它，请点击 **Save**。

添加流量量变曲线条件

过程

步骤 1 在流量量变曲线编辑器中的“量变曲线条件”下，为要添加的每个条件点击**添加条件**或**添加复杂条件**。相同级别的条件会被放在一起评估。

- 如果需要所有条件都位于满足操作符控制的级别上，选择 **AND**。
- 如果需要只有一个条件位于满足操作符控制的级别上，请选择 **OR**。

步骤 2 为每个条件指定类别、运算符和值，如流量量变曲线条件的语法，第 984 页和流量量变曲线条件，第 979 页中所述。

如果选择 **is in** 或 **is not in** 作为运算符，则可以在单个条件中选择多个值，如在流量量变曲线条件中使用多个值，第 988 页中所述。

当类别为某个 IP 地址时，选择 **is in** 或 **is not in** 作为操作符使您可以指定 IP 地址是还是不是在某个 IP 地址范围中。

示例

以下流量量变曲线收集有关特定子网的信息。条件的类别是 **Initiator/Responder IP**，操作符是 **is in**，值为 `10.4.0.0/16`。

相关主题

Firepower 系统 IP 地址约定，第 26 页

将主机配置文件限定条件添加到流量量变曲线中

过程

步骤 1 在流量量变曲线编辑器上，点击**添加主机配置文件限定条件 (Add Host Profile Qualification)**。

步骤 2 在“主机配置文件限定条件”下，为要添加的每个条件点击**添加条件** 或**添加复杂条件**。相同级别的条件会被放在一起评估。

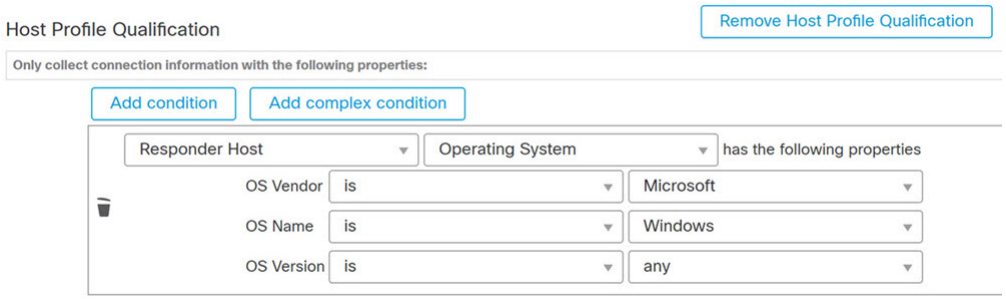
- 如果需要所有条件都位于满足操作符控制的级别上，选择 **AND**。
- 如果需要只有一个条件位于满足操作符控制的级别上，请选择 **OR**。

步骤 3 为每个条件指定主机类型、类别、运算符和值，如流量量变曲线中主机配置文件限定条件的语法，第 985 页和流量量变曲线条件，第 979 页中所述。

如果选择 **is in** 或 **is not in** 作为运算符，则可以在单个条件中选择多个值，如在流量量变曲线条件中使用多个值，第 988 页中所述。

示例

以下主机配置文件限定条件则限制了流量量变曲线以便其只在检测到的连接中的响应主机运行 Microsoft Windows 版本时才会收集连接数据。



流量量变曲线条件的语法

下表介绍了如何构建流量量变曲线条件。请记住，可用于构建流量量变曲线的连接数据取决于多个因素，包括流量特征和检测方法。

表 *143:* 流量量变曲线条件的语法

如果选择.....	选择运算符，然后.....
应用协议	选择一个或多个应用协议。
应用协议类别	选择一个或多个应用协议类别。

如果选择.....	选择运算符，然后.....
客户端	选择一个或多个客户端。
客户端类别	选择一个或多个客户端类别。
连接类型	选择配置文件是使用来自 Firepower 系统受管设备监控的流量还是来自已导出的 NetFlow 记录的连接数据。 如果您不指定连接类型，则流量量变曲线会同时包括两者。
目标国家/地区或源国家/地区	选择一个或多个国家/地区。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。
“发起方 IP”(Initiator IP)、“响应方 IP”(Responder IP) 或“发起方/响应方 IP”(Initiator/Responder IP)	输入 IP 地址或 IP 地址范围。 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。
NetFlow 设备	选择要使用其数据创建流量量变曲线的 NetFlow 导出器。
响应器端口/ICMP 代码	输入端口号或 ICMP 代码。
安全情报类别	选择一个或多个安全情报类别。 要将安全情报类别用于流量量变曲线条件，该类别必须在访问控制策略中设置为**监控(Monitor)**而不是**阻止 (Block)**。
SSL 加密会话	选择**已成功解密 (Successfully Decrypted)**。
传输协议	输入 **TCP** 或 **UDP** 作为传输协议。
Web 应用程序	选择一个或多个 Web 应用。
Web 应用类别	选择一个或多个 Web 应用类别。

相关主题

填充连接事件字段的要求，第 735 页
Firepower 系统 IP 地址约定，第 26 页

流量量变曲线中主机配置文件限定条件的语法

当构建主机配置文件限定条件时，必须首先选择要用于限制流量量变曲线的主机。您可以选择**响应方主机 (Responder Host)** 或**发起方主机 (Initiator Host)**。在选择主机角色之后，请继续构建主机配置文件限定条件。

虽然可以使用 NetFlow 记录将主机添加到网络映射中，但是有关这些主机的可用信息有限。例如，这些主机没有可用的操作系统数据，除非您使用主机输入功能提供这些数据。此外，如果流量量变曲线使用已导出的 NetFlow 记录中的连接数据，请记住，NetFlow 记录不包含有关连接中的哪台主机是发起方和哪台主机是响应方的信息。当系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息。

要匹配隐含或一般客户端，请根据响应客户端的服务器所用的应用协议创建主机配置文件限定条件。当作为连接发起方或源的主机上的客户端列表包含**客户端**遵循的应用协议名称时，该客户端可能实际上就是一种隐含客户端。换句话说，系统会根据使用该客户端的应用协议的服务器响应流量，而非检测到的客户端流量来报告该客户端。

例如，如果系统将 **HTTPS 客户端**作为主机上的一个客户端进行报告，请为**响应方主机**创建主机配置限定条件，其中**应用协议 (Application Protocol)** 被设置为 **HTTPS**，因为 HTTPS 客户端会根据响应方或目标主机发送的 HTTPS 服务器响应流量被报告为一种一般客户端。

表 *144:* 主机配置文件限定条件的语法

如果选择.....	选择运算符，然后.....
应用协议 (Application Protocol) > 应用协议 (Application Protocol)	选择一个或多个应用协议。
应用协议 (Application Protocol) > 应用端口 (Application Port)	输入应用协议端口号。
应用协议 (Application Protocol) > 协议 (Protocol)	选择协议。
应用协议类别	选择一个或多个应用协议类别。
客户端 > 客户端	选择一个或多个客户端。
客户端 > 客户端版本	输入客户端版本。
客户端类别	选择一个或多个客户端类别。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。
硬件	输入移动设备硬件型号。例如，要与所有 Apple iPhone 都匹配，请输入 `iPhone`。
主机重要性	选择主机重要性。
主机类型	选择一个或多个主机类型。您可以在一个常规主机或多种网络设备中的一种之间选择。
IOC 标记	选择一个或多个 IOC 标记。
Jailbroken	选择**是 (Yes)** 表示事件中的主机是破解移动设备，选择**否 (No)** 表示其不是破解移动设备。

如果选择.....	选择运算符，然后.....
MAC 地址 > MAC 地址	输入主机的全部或部分 MAC 地址。
MAC 地址 > MAC 类型	选择 MAC 类型是否是**按 ARP/DHCP 检测 (ARP/DHCP Detected)**，即， • 系统是否明确地将 MAC 地址识别为属于主机（**按 ARP/DHCP 检测 [ARP/DHCP Detected]**） • 打个比方，因为设备和主机之间有路由器，所以系统看到许多主机具有该 MAC 地址（**不按 ARP/DHCP 检测 [is not ARP/DHCP Detected]**） • MAC 类型不相关（**为任意 [is any]**）
MAC 供应商	输入主机使用的硬件的全部或部分 MAC 供应商。
移动	选择**是 (Yes)** 表示事件中的主机是移动设备，选择**否 (No)** 表示其不是移动设备。
NETBIOS 名称	输入主机的 NetBIOS 名称。
网络协议	输入 http://www.iana.org/assignments/ethernet-numbers 中所列的网络协议编号。
操作系统 > 操作系统供应商	选择一个或多个操作系统供应商名称。
操作系统 > 操作系统名称	选择一个或多个操作系统名称。
操作系统 > 操作系统版本	选择一个或多个操作系统版本。
传输协议	输入 http://www.iana.org/assignments/protocol-numbers 中所列的传输协议的名称或编号。
VLAN ID	输入主机的 VLAN ID 号。 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。
Web 应用程序	选择一个或多个 Web 应用。
Web 应用类别	选择一个或多个 Web 应用类别。
任何可用的主机属性，包括默认合规性 allow 名单主机属性	指定适当的值，这取决于您选择的主机属性类型： • 如果主机属性类型为 Integer，请在针对该属性确定的范围中输入一个整数值。 • 如果主机属性类型为“文本”(Text)，请输入文本值。 • 如果主机属性类型为“列表”(List)，请选择有效的列表字符串。 • 如果主机属性类型是 URL，请输入 URL 值。

在流量量变曲线条件中使用多个值

在构建条件，且条件语法允许您从下拉列表中选择值时，您通常可以从列表中选择多个值。

例如，如果想要将主机配置文件限定条件添加到需要主机运行 UNIX 的流量量变曲线，而非构建使用 OR 操作符连接的多个条件，请使用以下步骤。

过程

步骤 1 在构建流量量变曲线或主机配置文件限定条件时，选择 **is in** 或 **is not in** 作为运算符。
下拉列表会更改至文本字段。

步骤 2 点击文本字段或**编辑 (Edit)** 链接的任意位置。

步骤 3 在**可用 (Available)** 下，选择多个值。

步骤 4 点击右箭头将选定条目移动到**选定项 (Selected)** 中。

步骤 5 点击**确定 (OK)**。

第 41 章

补救

以下主题包含有关配置补救的信息：

补救措施的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 发现管理员

补救简介

补救是一种 Firepower 系统为响应关联策略违规而启动的程序。

当补救程序运行时，系统会生成补救状态事件。补救状态事件包括详细信息，如补救名称、触发补救的关联策略和规则及退出状态消息。

系统支持多种补救模块：

- 思科 ISE 自适应网络控制 (ANC) - 应用或清除关联策略违规中涉及的 ISE 配置的 ANC 策略
- 思科 IOS 空路由 - 在出现关联策略违规的情况下，阻止发送到主机或网络的流量（需要思科 IOS 版本 12.0 或更高版本）
- Nmap 扫描 - 扫描主机以确定运行的操作系统和服务器
- 设置属性值 - 在出现关联策略违规的情况下，设置一台主机的属性。

提示 您可以安装执行其他任务的自定义模块；请参阅《《*Firepower* 系统补救 *API* 指南》》。

实施补救

要实施补救，请先为所选模块创建至少一个实例。您可为每个模块创建多个实例，其中每个实例的配置各不相同。例如，要使用思科 IOS 空路由补救模块与多个路由器通信，请为该模块配置多个实例。

然后，您可以为每个实例添加多个补救，这些补救介绍了违反策略时要执行的操作。

最后，将补救与关联策略中的规则相关联，以便系统启动补救以响应关联策略违规。

补救和多租户

在多域部署中，您可以在任何域级别安装自定义补救模块。系统提供的模块属于全局域。

虽然您无法将补救添加到祖先域中创建的实例，但可以在当前域中创建类似配置的实例，并将补救添加到该实例。您也可以使用祖先域中创建的补救作为关联响应。

相关主题

Cisco Secure Firewall Management Center 警报响应，第 531 页
Nmap 扫描
将响应添加到规则和允许名单，第 941 页

思科 ISE EPS 补救

如果已在 ISE 部署中启用并配置终端保护服务 (EPS)，则可以配置 管理中心以启动使用 ISE 的补救。完全配置时，ISE EPS 补救在涉及关联策略违规的源或目标主机上运行以下**缓解操作 (Mitigation Actions)**：

- **隔离** - 限制或拒绝终端访问网络
- **取消隔离** - 取消终端的隔离状态，允许对网络进行完全访问
- **关闭** - 停用终端的网络附加系统 (NAS) 端口，以将其与网络断开

您还可以免除特定 IP 地址的 ISE EPS 补救。

注释 您的 ISE 版本和配置会影响您使用 ISE 的方式。例如，您不能使用 ISE-PIC 执行 SE EPS 补救。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 使用 *ISE/ISE-PIC* 进行用户控制 一章。

有关 ISE EPS 操作的详细信息，请参阅《思科身份服务引擎用户指南》。

配置 ISE EPS 补救

您可以通过在源或目标主机上运行 ISE EPS 补救对关联策略违规做出响应。

注释 ISE-PIC 无法执行 ISE EPS 补救。

开始之前

- 在 ISE 服务器上配置 EPS 操作。
- 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中有关配置 ISE/PIC 的章节。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 添加 pxGrid 缓解实例，如添加 ISE EPS 实例，第 991 页中所述。

步骤 3 添加一个或多个 ISE EPS 补救，如添加 ISE EPS 补救，第 992 页中所述。

下一步做什么

- 将补救作为对关联策略违规的响应进行分配，如将响应添加到规则和允许名单，第 941 页中所述。

添加 ISE EPS 实例

创建 ISE EPS 实例以按日志记录类型将单个补救分组。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 从**添加新实例 (Add a New Instance)** 列表中，选择 **pxGrid Mitigation(v1.0)** 作为模块类型，然后点击**添加 (Add)**。

步骤 3 输入**实例名称 (Instance Name)** 和**说明 (Description)**。

步骤 4 设置 **启用日志记录** 选项以启用或禁用系统日志记录。

步骤 5 点击**创建**。

下一步做什么

- 创建 ISE EPS 补救，如添加设置属性值补救，第 998 页中所述。

相关主题

Firepower 系统 IP 地址约定，第 26 页

添加 ISE EPS 补救

在实例中创建一个或多个 ISE EPS 补救，以在关联策略违反涉及的源或目标主机上运行**缓解操作 (Mitigation Actions)**。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 创建 ISE EPS 实例，如添加 ISE EPS 实例，第 991 页中所述。

过程

步骤 1 选择**策略 > 操作 > 实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（  ）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**缓解目标 (Mitigate Destination)** 或**缓解源 (Mitigate Source)**并点击**添加 (Add)**。

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 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 选择**缓解操作 (Mitigation Action)**：**隔离 (quarantine)**、**取消隔离 (unquarantine)** 或**关闭 (shutdown)**。

步骤 6 （可选）要免除 IP 地址或范围的补救，请将其输入到 **允许列表** 框中。

步骤 7 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单，第 941 页。

思科 IOS 空路由补救

借助思科 IOS 空路由补救模块，您可以使用思科的“null route”命令阻止某个 IP 地址或地址范围。这会将发送到某主机或网络的所有流量路由到路由器的 NULL 接口，从而丢弃这些流量。不过，这不会阻止从违规主机或网络发送的流量。

注释 不要使用基于目标的补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

注意 思科 IOS 补救激活后，就不再有超时期限。要解除阻止 IP 地址或网络，必须从路由器手动清除路由更改。

为思科 IOS 路由器配置补救

注释 不要使用基于目标的补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

注意 思科 IOS 补救激活后，就不再有超时期限。要解除阻止 IP 地址或网络，必须从路由器手动清除路由更改。

开始之前

- 确认思科路由器运行的是思科 IOS 12.0 或更高版本。
- 确认您对路由器具有 15 级管理访问权限。

过程

步骤 1 在思科路由器上启用 Telnet，如思科路由器或 IOS 软件随附的文档中所述。

步骤 2 在 管理中心上，为计划使用的每个思科 IOS 路由器添加思科 IOS 空路由实例；请参阅添加思科 IOS 实例，第 994 页。

步骤 3 根据在违反关联策略时要在路由器上引发的响应类型，为每个实例创建补救。

- 添加思科 IOS 阻止目标补救，第 995 页
- 添加思科 IOS 阻止目标网络补救，第 995 页
- 添加思科 IOS 阻止源补救，第 996 页

- 添加思科 IOS 阻止源网络补救，第 997 页

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单，第 941 页。

添加思科 IOS 实例

如果具有多个要发送补救的路由器，请为每个路由器创建单独的实例。

开始之前

- 在思科 IOS 路由器上配置 Telnet 访问，如路由器或 IOS 软件随附的文档中所述。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 从**添加新实例**列表中，选择**思科 IOS 空路由**并点击**添加**。

步骤 3 输入**实例名称 (Instance Name)** 和**说明 (Description)**。

步骤 4 在**路由器 IP (Router IP)** 字段中，输入要用于补救的思科 IOS 路由器的 IP 地址。

步骤 5 在**用户名 (Username)** 字段中，输入路由器的 Telnet 用户名。该用户必须对路由器拥有 15 级管理访问权限。

步骤 6 在**连接密码 (Connection Password)** 字段中，输入 Telnet 用户的用户密码。

步骤 7 在**启用密码 (Enable Password)** 字段中，输入 Telnet 用户的启用密码。该密码用于进入路由器的特权模式。

步骤 8 在**允许名单** 字段中，输入要免除补救的 IP 地址或范围（每行一个）。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 9 点击**创建**。

下一步做什么

- 添加要供关联策略使用的特定补救，如添加思科 IOS 阻止目标补救，第 995 页、添加思科 IOS 阻止目标网络补救，第 995 页、添加思科 IOS 阻止源补救，第 996 页和添加思科 IOS 阻止源网络补救，第 997 页中所述。

相关主题

Firepower 系统 IP 地址约定，第 26 页

添加思科 IOS 阻止目标补救

思科 IOS 阻止目标补救可阻止从路由器发送到关联事件违规中涉及的目标主机的流量。不要使用此补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 994 页中所述。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**阻止目标 (Block Destination)** 并点击**添加 (Add)**。

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 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单，第 941 页。

添加思科 IOS 阻止目标网络补救

思科 IOS 阻止目标网络补救可阻止从路由器发送到关联事件违规中涉及的目标主机网络的流量。不要使用此补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 994 页中所述。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（）。

步骤 3 在**已配置补救**部分，选择**阻止目标网络**并点击**添加**。

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 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 在 **Netmask** 字段中，输入子网掩码或使用 CIDR 表示法说明要阻止流量进入的网络。

例如，要在单个主机触发规则时阻止流量进入整个 Class C 网络（不推荐），请使用 `255.255.255.0` 或 `24` 作为子网掩码。

又例如，要阻止流量进入包括触发 IP 地址的 30 条地址，请指定 `255.255.255.224` 或 `27` 作为子网掩码。在这种情况下，如果 IP 地址 `10.1.1.15` 触发补救，则将阻止 `10.1.1.1` 与 `10.1.1.30` 之间的所有 IP 地址。要阻止触发 IP 地址，请将该字段留空，输入 `32` 或 `255.255.255.255`。

步骤 6 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单，第 941 页。

相关主题

Firepower 系统 IP 地址约定，第 26 页

添加思科 IOS 阻止源补救

思科 IOS 阻止源补救可阻止从路由器发送到关联策略违规中涉及的源主机的流量。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 994 页中所述。

过程

步骤 1 选择**策略 > 操作 > 实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（  ）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**阻止源 (Block Source)**，然后点击**添加 (Add)**。

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 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单，第 941 页。

添加思科 IOS 阻止源网络补救

思科 IOS 阻止源网络补救可阻止从路由器发送到关联事件违规中涉及的源主机网络的流量。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 994 页中所述。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（  ）。

步骤 3 在**已配置补救**部分，选择**阻止源网络**并点击**添加**。

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 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 在 **Netmask** 字段中，输入子网掩码或描述要阻止流量进入的网络 CIDR 表示法。

例如，要在单个主机触发规则时阻止流量进入整个 Class C 网络（不推荐），请使用 `255.255.255.0` 或 `24` 作为子网掩码。

又例如，要阻止流量进入包括触发 IP 地址的 30 条地址，请指定 `255.255.255.224` 或 `27` 作为子网掩码。在这种情况下，如果 IP 地址 `10.1.1.15` 触发补救，则将阻止 `10.1.1.1` 与 `10.1.1.30` 之间的所有 IP 地址。要阻止触发 IP 地址，请将该字段留空，输入 `32` 或 `255.255.255.255`。

步骤 6 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单，第 941 页。

相关主题

Firepower 系统 IP 地址约定，第 26 页

Nmap 扫描补救

Firepower 系统与用于网络探索和安全审核的开源主动扫描程序 Nmap™ 集成。您可以通过 Nmap 补救对关联策略违规做出响应，Nmap 补救会触发 Nmap 扫描补救。

有关 Nmap 扫描的详细信息，请参阅Nmap 扫描。

设置属性值补救

可以响应关联策略违规，只需在触发事件发生的主机上设置主机属性值。对于文本主机属性，可以使用事件说明作为属性值。

配置设置属性补救

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 创建设置属性实例，如添加设置属性值实例，第 998 页中所述。

步骤 3 添加设置属性补救，如添加设置属性值补救，第 998 页中所述。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单，第 941 页。

相关主题

预定义主机属性，第 845 页
用户定义的主机属性，第 846 页

添加设置属性值实例

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 从**添加新实例 (Add a New Instance)** 列表中选择**设定的属性值 (Set Attribute Value)**，然后点击**添加 (Add)**。

步骤 3 输入**实例名称 (Instance Name)** 和**说明 (Description)**。

步骤 4 点击**创建**。

下一步做什么

- 如添加设置属性值补救，第 998 页中所述，创建设定的属性补救。

添加设置属性值补救

设置属性值补救在关联策略违规所涉及的主机上设置主机属性。为要设置的每个属性值创建补救。对于文本属性，可以使用触发事件的说明作为属性值。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 创建设置属性实例，如添加设置属性值实例，第 998 页中所述。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 在要向其添加补救的实例旁，点击 **视图**（）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**设置属性值 (Set Attribute Value)**，然后点击**添加 (Add)**。

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 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 要使用此补救响应带有源和目标数据的事件，请选择**从事件更新哪些主机 (Update Which Host(s) From Event)** 选项。

步骤 6 对于文本属性，请指定是否要**将事件说明用于属性值 (Use Description From Event For Attribute Value)**：

- 要使用事件说明作为属性值，请点击**打开 (On)** 并在**属性值 (Attribute Value)** 中输入要设置的属性值。
- 要使用补救的**属性值 (Attribute Value)** 设置作为属性值，请点击**关闭 (Off)**。

步骤 7 依次点击 **Create** 和 **Done**。

下一步做什么

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和允许名单，第 941 页。

管理补救模块

在多域部署中，自定义表会显示在当前域中安装的补救模块，您可以对其进行删除。系统还会显示在祖先域中安装的模块，您不可以对其进行删除。要管理较低域中的补救模块，请切换至该域。

过程

步骤 1 选择**策略** > **操作** > **模块**。

步骤 2 管理补救模块：

- 配置 - 要查看模块的“模块详细信息”页面并配置其实例和补救，请点击 **视图**（）。在多域部署中，对于安装在祖先域中的模块，无法在当前域中使用“模块详细信息”(Module Detail) 页

面为其添加、删除或编辑实例。相反，请使用“实例”页面（**策略** > **操作** > **实例**）；请参阅管理补救实例，第 1000 页。

- 删除 - 要删除未在使用的自定义模块，请点击 **删除**（）。无法删除系统提供的模块。
- 安装 - 要安装自定义模块，请点击**选择文件 (Choose File)**，浏览至模块，然后点击**安装 (Install)**。有关详细信息，请参阅《*Firepower* 系统补救 *API* 指南》。

管理补救实例

“实例”(Instances) 页面列出了所有补救模块的所有已配置实例。

在多域部署中，系统会显示在当前域中创建的补救实例，您可以对其进行编辑。系统还会显示在祖先域中创建的实例，您不可以对其进行编辑。要管理较低域中的补救实例，请切换至该域。

虽然您无法将补救添加到祖先域中创建的实例，但可以在当前域中创建类似配置的实例，并将补救添加到该实例。您也可以使用祖先域中创建的补救作为关联响应。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 管理补救实例：

- 添加 - 要添加实例，请选择要为其添加实例的补救模块，然后点击**添加 (Add)**。对于系统提供的模块，请参阅：
  - 添加 ISE EPS 实例，第 991 页
  - 添加思科 IOS 实例，第 994 页
  - 《Cisco Secure Firewall Management Center 设备配置指南》
  - 添加设置属性值实例，第 998 页

  如需获取添加自定义模块的帮助，请参阅该模块的文档（如有）。
- 配置 - 要配置实例详细信息并添加对实例的补救，请点击 **视图**（）。
- 删除 - 要删除未在使用的实例，请点击 **删除**（）。

管理单个补救模块的实例

“模块详细信息”(Module Detail) 页面显示为特定补救模块配置的所有实例和补救。

在多域部署中，可以访问当前域和祖先域中安装的补救模块的“模块详细信息”(Module Detail) 页面。但是，不能使用“模块详细信息”(Module Detail) 页面为祖先域中安装的模块添加、删除或编辑当前域中的实例。相反，请使用“实例”页面（**策略** > **操作** > **实例**）；请参阅管理补救实例，第 1000 页。

过程

步骤 1 选择**策略** > **操作** > **模块**。

步骤 2 在要管理其实例的补救模块的旁边，点击 **视图**（）。

步骤 3 管理补救实例：

- 添加 - 要添加实例，请点击**添加 (Add)**。对于系统提供的模块，请参阅：
  - 添加 ISE EPS 实例，第 991 页
  - 添加思科 IOS 实例，第 994 页
  - 《Cisco Secure Firewall Management Center 设备配置指南》
  - 添加设置属性值实例，第 998 页

  要帮助为自定义模块添加实例，该参阅该模块的文档（如果可用）。
- 配置 - 要配置实例详细信息并添加对实例的补救，请点击 **视图**（）。
- 删除 - 要删除未在使用的实例，请点击 **删除**（）。

第 X 部分

参考

第 42 章

Cisco Secure Firewall Management Center 命令行参考

本参考介绍 Cisco Secure Firewall Management Center的命令行界面 (CLI)。

注释 有关 Cisco Secure Firewall Threat Defense，请参阅Cisco Secure Firewall Threat Defense 命令参考。

关于 Cisco Secure Firewall Management Center CLI

使用 SSH 登录 管理中心时，可以访问 CLI。虽然我们强烈建议不要这样做，但您可以使用 专家 命令访问 Linux 外壳。

注意 强烈建议您不要访问 Linux 外壳，除非 Cisco TAC 或 Firepower 用户文档明确说明需要这样做。

注意 具有 Linux 外壳访问权限的用户可以获得 root 权限，这将带来安全风险。出于系统安全原因，我们强烈建议：

- 如果您建立外部身份验证，请确保相应地限制具有 Linux 外壳访问权限的用户列表。
- 除了预定义 管理员 用户外，不要建立 Linux 外壳用户。

您 可以使用本附录中所述的命令查看 、对 Cisco Secure Firewall Management Center进行故障排除，以及执行有限的配置操作。

Cisco Secure Firewall Management Center CLI 模式

CLI 包含四种模式。默认模式“CLI 管理”包括用于在 CLI 本身内导航的命令。其余模式包含处理三个不同方面的 Cisco Secure Firewall Management Center功能的命令；这些模式中的命令以模式名称开头：`system`、`show` 或 `configure`。

进入某个模式时，CLI提示符会发生更改以反映当前模式。例如，要显示有关系统组件的版本信息，可在标准 CLI 提示符下输入完整命令：

```
> show version
```

如果您之前进入了 `show` 模式，则可以在显示模式 CLI 提示符下输入不含 `show` 关键字的命令：

```
show> version
```

Cisco Secure Firewall Management Center CLI 管理命令

CLI 管理命令可用于与 CLI 进行交互。这些命令不影响设备的运行。

exit

将 CLI 上下文上移至下一个最高级别的 CLI 上下文。从默认模式发出此命令会使用户注销当前 CLI 会话。

语法

```
exit
```

示例

```
system> exit
>
```

expert

调用 Linux 外壳。

语法

```
expert
```

示例

```
> expert
```

?（问号）

为 CLI 命令和参数显示上下文相关帮助。按照以下说明使用问号 (?) 命令：

- 要为当前 CLI 上下文中可用的命令显示帮助，请在命令提示符处输入问号 (?)。
- 要显示以特定字符集开头的可用命令的列表，请输入缩写命令，再紧接着输入问号 (?)。
- 要为命令的合法参数显示帮助，请在命令提示符处输入问号 (?) 代替参数。

请注意，问号 (?) 不会回送到控制台。

语法

```
?
abbreviated_command ?
command [arguments] ?
```

示例

```
> ?
```

Cisco Secure Firewall Management Center CLI Show 命令

Show 命令提供有关设备状态的信息。这些命令不会更改设备的运行模式，并且运行它们对系统运行的影响极小。

version

显示产品版本和内部版本以及 UUID 和其他信息。

语法

```
show version
```

示例

```
> show version
-------------------[ fmc-austin ]--------------------
Model                     : Cisco Secure Firewall Management Center for VMware (66) Version
```

```
 7.6.0 (Build 1385)
UUID                        : a904b8b2-ca9a-11ee-a583-5e804c16b2fd
Rules update version        : 2024-05-13-001-vrt
LSP version                 : lsp-rel-20240513-1955
VDB version                 : 380
----------------------------------------------------
```

Cisco Secure Firewall Management Center CLI 配置命令

配置命令可供用户配置和管理系统。这些命令会影响系统的运行。

password

允许当前 CLI 用户更改其密码。

注意 出于系统安全原因，我们强烈建议：除了任何设备上的预定义 **管理** 外，不要建立 Linux 外壳用户。

注释 导出模式不支持 密码 命令。要 Cisco Secure Firewall 系统上重置管理员用户的密码，请参阅 了解更多信息。如果您在专家模式下使用 密码 命令重置管理员密码，我们建议您使用 配置用户管理员密码 命令重新配置密码。重新配置密码后，切换到专家模式，并确保 /opt/cisco/config/db/sam.config 和 /etc/shadow 文件中的 admin 用户的密码散列相同。

发出命令后，CLI 会提示用户其当前（或旧）密码，然后提示用户输入新密码两次。

语法

```
configure password
```

示例

```
> configure password
Changing password for admin.
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Cisco Secure Firewall Management Center CLI 系统命令

系统命令可供用户管理整个系统的文件以及访问控制设置。

generate-troubleshoot

生成供思科进行分析的故障排除数据。

语法

```
system generate-troubleshoot option1 optionN
```

其中，选项是用空格分隔的以下一项或多项：

- ALL：运行以下所有选项。
- SNT：Snort 性能和配置
- PER：硬件性能和日志
- SYS：系统配置、策略和日志
- DES：检测配置、策略和日志
- NET：接口和网络相关数据
- VDB：发现、感知、VDB 数据和日志
- UPG：升级数据和日志
- DBO：所有数据库数据
- LOG：所有日志数据
- NMP：网络映射信息

示例

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl…
Please, be patient. This may take several minutes.
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
Troubleshooting information successfully created at
/var/common/results-06-14-2018—222027.tar.gz
```

lockdown

移除 专家 命令并访问设备上的 bash shell。

⚠

注意 没有支持部门提供的修复程序，此命令将无法撤销。请谨慎使用。

语法

```
system lockdown
```

示例

```
> system lockdown
```

reboot

重新启动设备。

语法

```
system reboot
```

示例

```
> system reboot
```

restart

重新启动设备应用。

语法

```
system restart
```

示例

```
> system restart
```

shutdown

关闭设备。

语法

```
system shutdown
```

示例

```
> system shutdown
```

安全清除

永久擦除硬盘驱动器数据。

在使用此命令之前，必须使用串行端口连接到管理中心。执行此命令时，设备会重新启动并永久删除所有数据。该过程可能需要几个小时才能完成；驱动器越大，需要的时间越长。确保您有电源，以防止在安全擦除过程中出现中断。擦除完成后，您可以安装新的软件映像。

⚠

注意 擦除硬盘驱动器会导致丢失设备上的所有数据，包括 ISO 图像。

支持的设备

- Firepower 管理中心 1600、2600、4600
- Firewall 管理中心 1700、2700、4700

语法

```
secure-erase
```

示例

```
> secure-erase
***************************** Caution *******************************

 If you run this command:
     - The management center hard drive data, including configurations
       and bootable images, will be permanently erased.
     - The device will reboot and reinitialize.

Note: Do not power off your device during this procedure.

*********************************************************************

Do you want to proceed? (Yes/No)
```

Cisco Secure Firewall Management Center CLI 的历史记录

功能	最低 管理中心	最低 威胁防御	详情
自动CLI访问 管理中心	6.5	任意	使用 SSH 登录 管理中心时，会自动访问 CLI。虽然强烈建议不要这样做，但您可以使用 CLI 专家 命令访问 Linux 外壳程序。 注释 此功能弃用了为 管理中心启用和禁用 CLI 访问的版本 6.3。由于弃用此选项，虚拟 管理中心 不再显示 **系统** > **配置** > **控制台配置** 页面，该页面仍显示在物理 管理中心上。
能启用和禁用CLI访问权限 管理中心	6.3	任意	新增/修改的屏幕： 管理中心 Web 界面中对管理员可用的新复选框：在 **系统**（⚙）> **配置** > **控制台配置**页面上**启用 CLI 访问权限**。 • 选中：使用 SSH 登录 管理中心可访问 CLI。 • 取消选中：使用 SSH 登录 管理中心可访问 Linux 外壳。此为全新的 6.3 版本以及以往版本至 6.3 版本升级的默认状态。 支持的平台： 管理中心
管理中心 CLI	6.3	任意	引入的功能。 最初支持以下命令： • `exit` • `expert` • `?` • `show version` • `configure password` • `system generate-troubleshoot` • `system lockdown` • `system reboot` • `system restart` • `system shutdown` 支持的平台： 管理中心

第 43 章

安全、互联网接入和通信端口

以下主题提供有关系统安全、互联网接入和通信端口的信息：

安全要求

为了保护Cisco Secure Firewall Management Center，应将其安装在受保护的内部网络中。虽然 管理中心已配置为仅拥有必需的服务和可用端口，但必须确保无法从防火墙外部攻击它（或任何受管设备）。

如果管理中心及其受管设备位于同一个网络，可以将设备的管理接口连接到与管理中心相同的受保护内部网络。这样，就可以安全地从管理中心控制设备。您还可以配置多个管理接口，使管理中心能够管理和隔离来自其他网络上设备的流量。

无论如何部署设备，内部设备通信将始终加密。但是，您仍需采取措施，确保设备之间的通信不会出现中断、阻塞或受到篡改；例如，遭受分布式拒绝服务 (DDoS) 或中间人攻击。

思科云

管理中心 与思科云中的资源进行通信，用于实现以下功能：

- **高级恶意软件防护**

  默认配置的是公共云；要进行更改，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 更改 *AMP* 选项 。

- **URL 筛选**

  有关详细信息，请参阅 *URL* 过滤 一章。

- **集成 安全分析和日志记录 (SaaS)**

请参阅在思科 Cisco Secure Cloud Analytics中的远程数据存储， 第 498 页。

- 有关详细信息，请参阅以下链接的集成文档：
  - 与思科 SecureX集成， 第 597 页
  - 使用的事件分析 SecureX 威胁响应， 第 605 页
- **主动支持功能**

  有关信息，请参阅配置思科支持诊断注册。
- **Cisco Success Network**

  有关信息，请参阅配置 Cisco Success Network 注册， 第 602 页。
- **Cisco Umbrella 连接**

  有关信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的 *DNS* 策略。

互联网接入要求

默认情况下，系统配置为通过 443/tcp (HTTPS) 端口和 80/tcp (HTTP) 端口连接到互联网。如果您不希望设备直接接入互联网，则可以配置代理服务器。对于许多功能，您的位置可以确定系统可以访问哪些资源。

大多数情况下，它是可接入互联网的 管理中心。高可用性对中的两个 管理中心 均应可以接入互联网。根据功能，有时两个对等体均可以接入互联网，而有时只有活动对等体才可以接入互联网。

有时受管设备也可以接入互联网。例如，如果恶意软件防护配置使用动态分析，则受管设备会将文件直接提交到 Secure Secure Malware Analytics 云。或者，您也可以将设备同步到外部 NTP 服务器。

此外，除非您禁用 Web 分析跟踪，否则浏览器可能会与 Google (google.com) 或 Amplitude (amplitude.com) Web 分析服务器通信，以向 Cisco 发送非个人可识别的使用数据。

表 *145:* 互联网接入要求

功能	原因	管理中心 高可用性	Resource
恶意软件	恶意软件云查找。	两个对等体均执行查找。	请参阅正确的 Cisco Secure Endpoint 和恶意软件分析操作所需的服务器地址。
	下载签名更新以进行文件预分类和本地恶意软件分析。	活动对等体执行下载，并同步到备用对等体。	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	提交文件以进行动态分析（受管设备）。 查询动态分析结果 (管理中心)。	两个对等体均查询动态分析报告。	fmc.api.threatgrid.com fmc.api.threatgrid.eu

功能	原因	管理中心 高可用性	Resource
面向终端的 AMP	从 AMP 云接收由面向终端的 AMP 检测到的恶意软件事件。 显示由面向终端的 AMP 中的系统检测到的恶意软件事件。 使用在面向终端的 AMP 中创建的集中式文件阻止名单和允许名单覆盖 AMP 云中的处置情况。	两个对等体均接收事件。 您还必须在两个对等体上配置云连接（配置不会同步）。	请参阅正确的 Cisco Secure Endpoint 和恶意软件分析操作所需的服务器地址。
安全情报	下载安全情报源。	活动对等体执行下载，并同步到备用对等体。	intelligence.sourcefire.com
URL 过滤	下载 URL 类别和信誉数据。 手动查询（查找）URL 类别和信誉数据。 查询未分类的 URL。	活动对等体执行下载，并同步到备用对等体。	URL： • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates.ironport.com IPv4 块： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPV6 块： • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Cisco Secure Dynamic Attributes Connector	从 Amazon Elastic Container Registry (Amazon ECR) 获取软件包	获取主用对等体上的字段映像，然后将其同步到备用对等体。	https://public.ecr.aws https://csdac-cosign.s3.us-west-1.amazonaws.com
思科智能许可	与思科智能软件管理器通信。	活动对等体执行通信。	smartreceiver.cisco.com www.cisco.com
Cisco Success Network	传输使用信息和统计信息。	活动对等体执行通信。	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com

功能	原因	管理中心 高可用性	Resource
思科支持诊断结果	接受授权请求并传输使用信息和统计信息。	活动对等体执行通信。	api-sse.cisco.com:8989
系统更新	直接将更新从思科下载到管理中心： • 系统软件 • 入侵规则 (SRU/LSP) • 漏洞数据库 (VDB) • 地理位置数据库 (GeoDB)	更新活动对等体上的入侵规则、VDB 和 GeoDB，然后再同步到备用对等体。 在每个对等体上单独升级系统软件。	amazonaws.com cisco.com
SecureX 威胁响应集成	请参阅相应的 集成指南。		
时间同步	同步部署中的时间。 代理服务器不支持。	使用外部 NTP 服务器的任何设备均必须接入互联网。	time.cisco.com
RSS 源	在控制面板上显示思科威胁研究博客。	显示RSS源的任何设备均必须接入互联网。	blog.talosintelligence.com
Whois	请求外部主机的 whois 信息。 代理服务器不支持。	请求 whois 信息的任何设备均必须接入互联网。	whois 客户端会尝试猜出要查询的正确服务器。如果猜不出，则使用： • NIC 句柄：whois.networksolutions.com • IPv4 地址和网络名称：whois.arin.net

通信端口要求

管理中心 和托管设备在 8305/tcp 端口上使用双向、SSL 加密的通信通道进行通信。此端口 必须 保持开放，以进行基本通信。

其他端口允许安全管理，并访问特定功能所需的外部资源。一般来说，除非启用或配置相关功能，否则，功能相关的端口会保持关闭。在了解此操作对部署的影响之前，请勿更改或关闭已打开的端口。

表 *146:* 通信端口要求

端口	协议/功能	平台	方向	详细信息
22/tcp	SSH	管理中心 威胁防御	入站	与设备的安全远程连接。
53/tcp 53/udp	DNS		出站	DNS
67/udp 68/udp	DHCP		发送	DHCP
123/udp	NTP		发送	同步时间。
161/udp	SNMP	管理中心 威胁防御	入站	允许通过 SNMP 轮询访问 MIB。
162/udp	SNMP		发送	发送 SNMP 警报至远程陷阱服务器。
389/tcp 636/tcp	LDAP		发送	与 LDAP 服务器通信以进行外部身份验证。 获取检测到的 LDAP 用户元数据（仅限管理中心）。 可配置。
443/tcp	HTTPS	管理中心	接收	访问 Web 界面。
443/tcp	远程接入 VPN (SSL/IPSec)	威胁防御	入站	允许远程用户与您的网络建立安全的VPN连接。
500/udp 4500/udp	远程接入 VPN (IKEv2)	威胁防御	入站	允许远程用户与您的网络建立安全的VPN连接。
443/tcp	HTTPS	管理中心 威胁防御	接收	使用 Firepower REST API（包括思科终端服务 (TS) 代理）与第三方集成产品通信。
443/tcp	HTTPS		发送	发送和接收来自互联网的数据。 有关详细信息，请参阅互联网接入要求，第 1014 页。
443	HTTPS	管理中心	both	与面向终端的 AMP 集成
514/udp	系统日志（警报）		发送	向远程系统日志服务器发送警报。
623/udp	SOL/LOM	管理中心	入站	使用 LAN 上串行 (SOL) 连接执行无人值守管理 (LOM)。

端口	协议/功能	平台	方向	详细信息
885/tcp	强制网络门户	威胁防御	入站	与强制网络门户身份源通信。
1500/tcp 2000/tcp	数据库访问	管理中心	入站	允许第三方客户端对事件数据库进行只读访问。
1812/udp 1813/udp	RADIUS		发送	与 RADIUS 服务器通信以进行外部身份验证和记账。 可配置。
8302/tcp	eStreamer	管理中心	入站	与 eStreamer 客户端通信。
8305/tcp	设备通信		双向	在同一部署中的设备之间安全地进行通信。 可配置。如果更改此端口，必须为部署中的所有设备更改此端口。建议保留默认值。
8307/tcp	主机输入客户端	管理中心	入站	与主机输入客户端通信。
8989/tcp	思科支持诊断结果		两者	接受授权请求并传输使用信息和统计信息。

相关主题

添加 管理中心的 LDAP 外部身份验证对象，第 122 页
添加管理中心的 RADIUS 外部身份验证对象，第 129 页

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。