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 13 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 1 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：

- **错误** ( ) - 指示系统上存在一个或多个错误和任意数量的警告。
- **警告**（ ） - 指示系统上存在一个或多个警告而没有错误。
- **成功** （ ） - 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 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**消除** （ ）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 5 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 7 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 7 页或管理任务消息，第 8 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

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 *1:* 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
```

联系 思科 TAC 之前

强烈建议您在联系 思科 TAC 之前收集以下项目：

- 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 12 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 *2*: 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

该选项...	报告...
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 7 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 7 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。

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。

在 Cisco Secure Firewall Management Center 查看故障排除系统日志

您可以启用 威胁防御 设备记录故障排除系统日志并将其发送到 管理中心。日志记录数据可以帮助您发现并隔离网络或设备配置问题。启用日志记录后，威胁防御 设备会将系统日志发送到管理中心进行分析和存储。

您可以通过编辑目标设备的 威胁防御 平台设置策略中的 **启用登录 Cisco Secure Firewall Management Center (Enable Logging to Secure Firewall Management Center)** 选项来管理记录和信息严重性。有关启用日志记录、配置 syslog 服务器和查看系统日志的详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 中的为威胁防御设备配置系统日志记录。

所有故障排除日志

配置 威胁防御 设备以便将所有诊断系统日志记录到管理中你想你，并将它们作为**故障排除事件**与**统一事件 (Unified Events)** 表（**分析 (Analysis)** > **统一事件 (Unified Events)**）中的其他事件一起查看。使用统一事件表实时查看故障排除日志，并将其与执行故障排除时最近的设备配置更改相关联。您可以过滤和分析同一表格中其他事件类型的日志，以深入了解情况并排除 威胁防御 设备故障。

有关查看**故障排除事件**的详细信息，请参阅使用统一事件。

您可以选择将严重性级别为“严重”、“警报”或“紧急情况”的所有故障排除系统日志发送到 管理中心。

VPN 故障排除日志

配置 威胁防御 设备，使其只向 管理中心 发送 VPN 故障排除系统日志以供分析。出现的 VPN 系统日志都具有默认严重性级别“错误”或更高严重性（除非已更改）。建议将VPN日志的记录级别设置为“错误”。将 VPN 日志级别设置为 4 或更低的严重性（“警告”、“通知”、“信息”或“调试”）可能会导致 管理中心 过载。

注释 只要您配置了具有站点间或远程访问 VPN 的设备，它就会默认自动启用将 VPN 系统日志发送至 管理中心。

查看故障排除系统日志

威胁防御 设备会捕获事件信息，以帮助您收集有关设备配置问题或 VPN 问题根源的更多信息。默认情况下，行按**时间**列排序。

开始之前

- 通过在 威胁防御 平台设置中配置**日志记录到 Cisco Secure Firewall Management Center (Logging to Secure Firewall Management Center)** (Logging to 思科防御协调器) 选项来启用日志记录。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的启用日志记录和配置基本设置。
- 您必须是枝叶域中的管理员用户才能执行此任务。

过程

步骤 1 选择**设备 (Devices)** > **故障排除 (Troubleshoot)** > **故障排除日志 (Troubleshooting Logs)**。

步骤 2 您有以下选择：

- 搜索 - 要过滤当前消息信息，请点击 **编辑搜索**。
- 查看 - 要查看与视图中所选消息关联的 VPN 详细信息，请点击 **查看**。
- 查看全部 - 要查看视图中所有消息的事件详细信息，请点击 **查看全部**。
- 删除 - 要从数据库中删除选定的消息，请点击 **删除** 或点击 **全部删除** 以删除所有消息。

下一步做什么

如果您选择将所有故障排除系统日志发送到管理中心，请点击**分析 (Analysis)** > **统一事件 (Unified Events)** 以实时查看记录的**故障排除事件**以及其他 Cisco Secure Firewall 事件类型。

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

有关连接故障排除更多信息，请参阅 连接故障排除 ， 第 17 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 14 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 *3: 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。
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 *4:* 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。
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。

被阻止或流被阻止...	原因
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、、HTTPS 解密、 等）不支持 PCAP 重放。

对于配置了 NAT 的 威胁防御 设备，PCAP 数据包在重放时会反映转换后的地址，以便处理这些地址而不会被丢弃。但是，PCAP 重放不支持 IPv4 到 IPv6 或 IPv6 到 IPv4 的 NAT 类型。

要使数据包跟踪器捕获与身份和 TLS 解密相关的跟踪信息，必须确保在设备中将 Snort 3 配置为检测引擎。

为了实现更真实的数据包重放模拟，此工具可以模拟数据包的实际时序。它会根据 PCAP 文件中记录的时间戳重放数据包。要启用时间戳选项，请在 **packet-tracer** 命令中使用 **honor-timestamp** 关键字。

注释 当重放数据包的 威胁防御 设备处理时间高于数据包之间的延迟时，在 PCAP 中遵守时间戳的准确性会受到限制。

您可以使用 **show packet tracer** 命令中的 **export-pcapng** 关键字将 威胁防御 设备生成的数据包跟踪数据存储为 PCAP 文件的一部分。您可以使用其他外部数据包查看器工具（例如 Wireshark）来查看生成的 pcapng 文件。

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 (复制) 跟踪结果复制到剪贴板。
- 展开或折叠 (展开或折叠) 显示的结果。
- 最大化 (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 滑块已启用 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。

CPU 分析器概述

在特定时间范围内处理数据包时，CPU 分析器会收集 Snort 3 的各个模块或检查器的 CPU 使用率数据。它提供每个模块相对于 Snort 3 进程的 CPU 总使用量所消耗的 CPU 时间的信息。使用 CPU 分析器不需要重新加载配置或重新启动 Snort 3，从而最大限度地减少停机时间。分析结果显示所有模块在上次分析会话期间所用的处理时间。CPU 分析结果以 JSON 格式保存在威胁防御设备中，并在管理中心同步。

注意 CPU 分析可能会导致系统性能下降约 3%。

使用 CPU 分析器

开始之前

要使用 CPU 分析，必须有安装了 7.6 或更高版本的 Snort 3 设备。

过程

步骤 1 从管理中心，选择**设备 (Devices)** > **Snort 3 分析 (Snort 3 Profiling)**。

步骤 2 点击 **CPU 分析 (CPU Profiling)** 选项卡。

步骤 3 从**选择用于 CPU 分析的设备 (Select device for CPU Profiling)** 下拉列表中，选择用于 CPU 分析的设备。

注释
您可以在不同的设备上同时运行多个分析会话。

步骤 4 要启动 CPU 分析会话，请点击**开始 (Start)**。（会话将在 120 分钟后自动停止。）

您可以随时点击**停止 (Stop)** 来停止分析会话。但是，在计划的 120 分钟之前取消它可能无法提供精确的结果。

注释
在 CPU 分析会话期间，系统会创建一个任务。点击**通知 (Notifications)** > **任务 (Tasks)** 以查看详细信息。

最新的分析结果会自动显示在 **CPU 分析结果 (CPU Profiling Results)** 部分中。该表包含所有 Snort 3 模块或检查器在上次分析会话期间所用处理时间的统计信息。您可以以表格格式查看 CPU 分析器输出：

- **模块 (Module)**：模块或检查器的名称。
- **CPU 总时间百分比 (% Total of CPU Time)**：模块所用时间相对于 Snort 3 处理流量所用总时间的百分比。如果此值明显高于其他模块的值，则意味着该模块对 Snort 3 的性能不满意的影响更大。
- **时间（微秒）(Time [µs])**：每个模块所用的总时间（以微秒为单位）。
- **平均/检查 (Avg/Check)**：模块每次调用所用的平均时间。
- **调用方百分比 (% Caller)**：子模块（如果已配置）相对于主模块所用的时间。此值用于调试目的。

步骤 5 （可选）点击**下载快照 (Download Snapshot)** 以下载分析结果。下载的文件为 CSV 格式，包含分析结果页面中的所有字段。

步骤 6 （可选）点击**按 Snort 时间百分比过滤 (Filter by % of Snort time)** 切换按钮，以过滤掉执行时间超过 *n*% 的分析时间的模块。

步骤 7 （可选）使用**搜索 (Search)** 字段搜索 **CPU 分析结果 (CPU Profiling Results)** 表中的字段。

注释
除**模块 (Module)** 外，您可以点击任何其他列标题对数据进行排序。

步骤 8 （可选）点击**分析历史记录 (Profiling History)** 部分（左侧的可折叠面板）将其展开，并查看代表所选设备的先前分析会话的一组卡片。当您点击历史记录中的卡片时，详细信息将显示在**CPU 分析结果**部分中。

注释 如果在CPU分析运行时启动部署，分析会话将自动终止以适应部署，但因访问控制策略规则和安全情报更改而导致的部署除外。您必须再次为设备运行 CPU 分析。

规则分析器概述

Snort 3 规则分析器收集有关处理一组 Snort 3 入侵规则所用时间的数据，突出显示潜在问题，并显示性能不理想的规则。在 Snort 3 引擎中，规则分析器会使用 Snort 3 入侵检测机制来检查流量。规则分析器会显示需要最长时间检查的前 100 条 IPS 规则。触发规则分析器不需要重新加载或重新启动 Snort 3。规则分析结果以 JSON 格式保存在威胁防御设备中，并在管理中心同步。

使用规则分析器

开始之前

要使用规则分析，必须有安装了 7.6 或更高版本的 Snort 3 设备。

过程

步骤 1 从管理中心，选择**设备 (Devices)** > **Snort 3 分析 (Snort 3 Profiling)**。

步骤 2 点击**规则分析 (Rule Profiling)** 选项卡。

步骤 3 从**选择用于规则分析的设备 (Select device for Rule Profiling)** 下拉列表中，选择用于规则分析的设备。

注释
您可以在不同的设备上同时运行多个分析会话。

步骤 4 要启动规则分析会话，请点击**开始 (Start)**。（会话将在 120 分钟后自动停止。）

您可以随时点击**停止 (Stop)** 来停止分析会话。但是，在计划的 120 分钟之前取消它可能无法提供精确的结果。

注释
在进行规则分析会话时，系统会创建一个任务。点击**通知 (Notifications)** > **任务 (Tasks)** 以查看详细信息。

最新的分析结果会自动显示在**规则分析结果 (Rule Profiling Results)** 部分中。该表包含按总时间（以微秒 [µs] 为单位）处理时间最长的规则的统计信息（按降序排序）。您可以以表格格式查看 IPS 规则分析器输出：

- **Snort 时间百分比 (% of Snort Time)**：处理规则所花费的时间，相对于 Snort 3 操作的总时间。
- **修订版 (Rev)**：规则的修订号。
- **检查 (Checks)**：执行 IPS 规则的次数。
- **匹配数 (Matches)**：IPS 规则在流量中完全匹配的次数。
- **警报 (Alerts)**：IPS 规则触发 IPS 警报的次数。
- **时间 (Time)**：Snort 检查 IPS 规则所用的时间（以微秒为单位）。
- **平均/检查 (Avg/Check)**：Snort 在单次规则检查上花费的平均时间。
- **平均/匹配 (Avg/Match)**：Snort 在找到匹配的单次检查上花费的平均时间。
- **平均/不匹配 (Avg/Non-Match)**：Snort 在没有找到匹配的单次检查上花费的平均时间。
- **超时 (Timeouts)**：规则超出访问控制策略的“基于延迟的性能设置”中配置的规则处理阈值的次数。
- **暂停 (Suspends)**：由于连续违反阈值而暂停规则的次数。

步骤 5 （可选）点击**下载快照 (Download Snapshot)** 以下载分析结果。下载的文件为 CSV 格式，包含分析结果页面中的所有字段。

步骤 6 （可选）点击按 **Snort 时间百分比过滤 (Filter by % of Snort time)** 切换按钮，过滤掉执行时间超过 *n*% 的分析时间的规则。一般来说，如果一条规则花费了 Snort 整体处理时间的 0.2% 或更多，就会被认为执行得不尽人意。

步骤 7 （可选）使用**搜索 (Search)** 字段搜索**规则分析结果 (Rule Profiling Results)** 表中的字段。

步骤 8 （可选）点击**规则分析历史记录 (Rule Profiling History)** 部分（左侧的可折叠面板）将其展开，并查看代表所选设备的先前分析会话的一组卡片。当您点击历史记录中的卡片时，详细信息将显示在**规则分析结果 (Rule Profiling Results)** 部分。

注释 如果在规则分析运行时启动部署，分析会话将自动终止以适应部署，但因访问控制策略规则和安全情报更改而导致的部署除外。您必须再次为设备运行规则分析。

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 5: 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
许可	智能许可疑难解答 特定许可证预留疑难解答
管理中心 高可用性	管理中心高可用性故障排除
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
URL 筛选	在 《Cisco Secure Firewall Management Center 设备配置指南》中的*URL* 过滤故障排除
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 17 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。