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

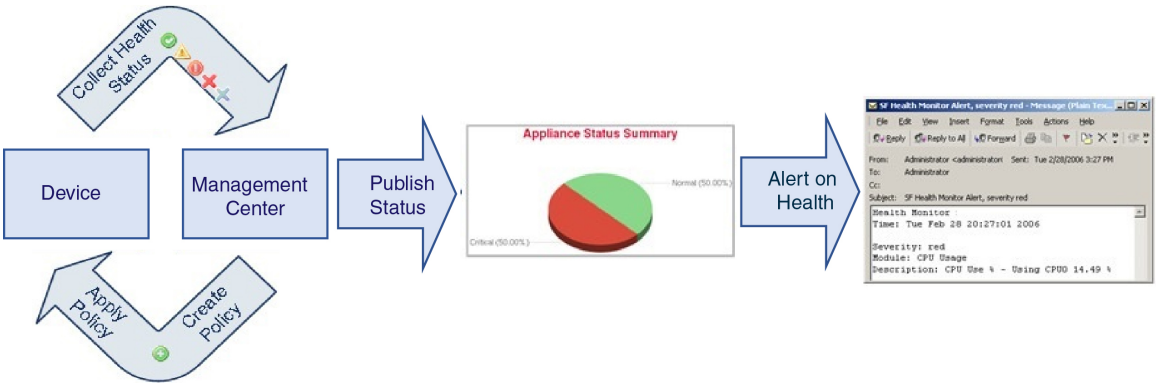
管理员

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 *1:* 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 。 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运行状况监控警报的磁盘使用情况 。 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 。 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 *2:* 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 *3:* 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 3 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 13 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 25 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 14 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 15 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。

  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 3 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。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 14 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 23 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 3 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 *4:* 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。

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 配置警报响应，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。

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 31 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 28 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 30 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 和 配置会话超时 。

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。
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。

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
- 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。
- 创建和修改运行状况策略；请参阅 创建运行状况策略，第 13 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 25 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 33 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 5: 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 32 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 *6:* 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 *7:*

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。

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。