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 *1:* 主机统计信息

类别	说明
时间	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 (Load Average)	过去 1 分钟、5 分钟和 15 分钟内 CPU 队列的平均进程数。

类别	说明
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。
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 Cisco Secure Firewall Management Center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 *2:* 进程列表列

列	说明
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）

列	说明
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
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 4 页
可执行文件和系统实用程序，第 6 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 *3:* 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

后台守护程序	说明
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 和有效的证书身份验证；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 Firepower 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
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，并向文件中记录运行时信息
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服务。目前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 Cisco Secure Firewall Management Center。
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 sfmb）处理请求

后台守护程序	说明
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 *4:* 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
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

可执行程序	说明
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
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 Cisco Secure Firewall Management Center之间的联络
sfmb	表示消息代理进程；处理 Cisco Secure Firewall Management Center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

可执行程序	说明
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

SFDataCorrelator 进程统计信息部分

在 Cisco Secure Firewall Management Center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Cisco Secure Firewall Management Center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 *5:* 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 Cisco Secure Firewall Management Center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Cisco Secure Firewall Management Center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 *6:* 入侵事件信息

统计信息	说明
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
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 Cisco Secure Firewall Management Center 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 10 页中所述的信息。

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。