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 防火墙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**管理** > **+ 显示更多** > **高级** > **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 2 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 *1:* 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

审核记录

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

防火墙管理中心的 SSO 指南

查看审核记录

在 防火墙管理中心，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**事件和日志** > **分析** > **审核日志** 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。

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 1 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。
- 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。
- 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。
- 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。

  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。
- 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。
- 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。
- 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 6 页。

相关主题

事件视图限制

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 *2:* 审核日志字段

字段	说明
时间	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，**事件和日志** > **分析** > **审核日志** 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 防火墙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

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

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**事件和日志** > **分析** > **审核日志** 。

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 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 7 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 *3:* 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 7 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 4: 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 防火墙管理中心

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	在防火墙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 防火墙管理中心 发送到外部位置，请参阅：

- 审核日志
- 审核日志证书

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。

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。

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。

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。