Cisco NAC Appliance (Clean Access) 4.x ：配置事件日志的系统日志设置

目录

简介

本文描述如何配置Syslog设置为了记录事件到在思科网络准入控制(美洲台)设备的一个外部服务器，以前叫作思科Clean Access (CA)。

先决条件

要求

本文假设思科Clean Access管理器(CAM)和思科Clean Access服务器(CAS)适当地安装并且工作。

使用的组件

运行软件版本4.0及以上版本的本文档中的信息根据Cisco NAC设备。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

解释事件日志

点击**事件日志**连接在**监听**模块为了查看基于系统日志的事件登陆admin控制台。有三事件日志选项卡：

- **查看日志**
- **日志设置**
- **Syslog 设置**

查看日志

图 1
视图日志选项卡包括此信息：

- Clean Access服务器的系统统计，默认情况下生成每个小时。
- 用户活动，与用户登录时间、注销时间，失败的登录尝试，等等。
- 网络配置事件，包括对媒体访问控制(MAC)的更改或IP转接列表和Clean Access服务器新增内容或者删除。
- 带外(OOB)的交换机管理事件，包括，当链路中断陷阱接收，并且，当端口变成验证或访问虚拟LAN (VLAN)。
- 更改或更新对Clean Access检查、规则和支持的防病毒/Antispyware产品列表。
- 对Clean Access服务器动态主机配置协议(DHCP)配置的更改。

默认情况下系统统计为Clean Access管理器管理的每个CAS生成每个小时。请参阅配置登陆命令的Syslog更改系统检查多频繁发生。

注意： 多数近期事件首先在事件列出现。

表1描述在视图日志显示的定位、搜索功能和实际Syslog。

表 1

	列	说明
定位	**首先/上一个/其次/为时**	这些定位链路页通过事件日志。多数近期事件首先在事件列出现。**最后**链路显示您在日志的最旧的事件。最多25个条目在页显示。
	列	点击列标题，例如类型或类别，为了由该列排序事件日志。
搜索条件	**类型**	由这些类型列标准搜索，然后单击**视图**： • 其中任一键入 • 失败 • 信息 • 成功
	类别	由这些分类列标准搜索，然后单击**视图**： • 验证[1] • 管理 • 客户端 • Clean Access 服务器 • Clean Access • SW_Management，如果OOB启用 • 其他 • DHCP

	时间	由这些时间标准的搜索，然后单击**视图**： • 在一个小时内 • 在一天之内 • 在两天内 • 在一周内 • 一个小时前 • 一天前 • 两天前 • 一周前
	在日志文本的搜索	键入希望的搜索文本并且点击**视图**。
控制	**查看**	在希望的搜索条件选择后，请点击**视图**为了显示结果。
	重置视图	如果点击**"Reset"视图**，恢复默认视图，日志在一天之内显示。
	删除	如果点击**删除**，删除事件过滤在可适用的页间数量的搜索条件。删除从Clean Access管理器存储设备删除已过滤事件。否则，事件日志通过系统关机仍然存在。请使用显示的过滤事件指示器在图1为了查看是受删除支配已过滤事件的总数。
状态显示	**类型**	• 红旗() =失败—指示一个错误或意外事件 • 绿色标志() =成功—指示一个成功或正常使用情况事件，例如成功登录和配置活动 • 黄旗() =信息—指示系统性能信息，例如负载信息和内存使用
	类别	指示起动日志事件的模块或系统组件。对于列表，参考**类别**在搜索条件下部分。注意，默认情况下，系统统计生成由Clean Access管理器管理的每个Clean Access服务器的每个小时。
	时间	显示日期和时间(hh ：mm:ss)事件，与多数近期事件首先在列表。
	事件	显示模块的事件，当多数近期事件首先列出。参见表2 - Clean Access服务器事件的示例的事件列菲尔茨。

脚注-表1

1 验证类型条目能包括项目"供应商：<provider type>，接入点：N/A，网络：N/A."为了继续为到期(EOL)传统无线客户端提供支持，若有和预先配置在管理器，"接入点：N/A，网络：N/A"字段分别为传统客户端提供接入点(AP) MAC和服务集标识(SSID)信息。

事件日志示例

表2解释典型的Clean Access服务器状况事件示例：

```
CleanAccessServer 2006-04-03 15:07:53 192.168.151.55 System Stats:
 Load factor 0 (max since reboot: 9) Mem Total: 261095424 bytes Used: 246120448
 bytes Free: 14974976 bytes Shared: 212992 bytes Buffers: 53051392 bytes Cached:
 106442752 bytes CPU User: 0% Nice: 0% System: 97% Idle: 1%
```

表2 -事件列菲尔茨

值	说明
CleanAccessServer	Clean Access服务器报告事件
2006-04-03 15:07:53	事件的日期和时间
192.168.151.55	报告Clean Access服务器的IP地址
0	负荷系数指示等待由Clean Access服务器处理，即，当前负载由CAS处理数据包的数量。当负荷系数增长时，它是数据包在将处理的队列等待的征兆。如果负荷系数超过500在任何一致时期，例如五分钟，这表明Clean Access服务器有入站数据流/数据包平稳的高负载。如果此编号增加到500或更加高，请关系到。
(<n>)	在随时队列的最大信息包的数量。换句话说，最大载荷由Clean Access服务器处理了。
Mem 261095424	这些是内存使用统计信息。有显示的六个编号此处： • 总内存 • 占用的内存 • 空闲存储器 • 共享内存 • 缓冲内存 • 缓存存储器
246120448	
14974976	
212992	
53051392	
106442752	
CPU	这些编号指示CPU在硬件的处理器负载，在百分比。

0% 0% System:97% 1%	这四个编号由在用户，好，系统和空闲进程的系统指示中花费的时间。 **注意：** 由CPU的中花费的时间在系统进程比在Clean Access服务器的90百分比典型地极大。这指示一个健康系统。

限制已登录事件数量

事件日志阈值是在Clean Access管理器数据库将存储的事件数量。日志事件最大在CAM保持的，默认情况下，是100,000。您能指定在CAM数据库每次将存储的200,000个条目事件日志阈值。事件日志是一本圆的日志。当日志通过事件日志阈值时，最旧的条目覆盖。

为了更改事件最大：

1. 点击**日志setting选项**在**Monitoring>事件日志**页。
2. 在**最大事件日志**字段进入新号码。
3. 单击**更新**。

配置Syslog记录日志

系统统计生成每个小时，默认情况下，由Clean Access管理器管理的每个Clean Access服务器的。默认情况下，事件日志写入对CAM。您能重定向CAM事件日志到另一个服务器，例如您自己的系统日志服务器。

另外，您能配置您多频繁希望CAM记录系统状态信息。为了执行此，在**Syslog健康日志间隔**字段设置值。默认时间为 60 分钟。

为了配置Syslog记录日志：

1. 选择**Monitoring>事件日志> Syslog设置**。
2. 在**系统日志服务器地址**地址字段输入系统日志服务器的IP地址。默认是**127.0.0.1**。
3. 在**系统日志服务器端口字段**输入系统日志服务器的端口。默认是**514**。
4. 回车您多频繁在**系统工作状况日志间隔**字段希望CAM记录系统状态信息，以分钟。默认时间为60 分钟。此设置确定多么CAS统计信息频繁地登陆事件日志。
5. 点击**更新**为了保存您的更改。**注意：** 在您设置您的在CAM后的系统日志服务器，您能测试您的配置。为了执行此，注销和日志回到CAM admin控制。这生成系统日志事件。如果CAM事件在您的系统日志服务器看不到，请确保系统日志服务器接收用户数据报协议(UDP) 514数据包，并且他们在您的网络在别处没有阻塞。**注意：** 因为不支持，配置多个SYSLOG服务器不是可能的。您能只转发到一个系统日志服务器。

日志文件

事件日志在Clean Access管理器数据库表里查找和被命名log_info表。列出其他登录Clean Access管理器。

表 3

文件	说明
/var/log/messages	启动

/var/log/dhcplog	DHCP中继， DHCP日志
/tmp/perfigo-log0.log.*	Perfigo 3.5(4)的服务日志和及早[1]
/perfigo/logs/perfigo-log0.log.*	Perfigo 3.5(5)的服务日志及以后[1,2]
/perfigo/logs/perfigo-redirect-log0.log.0	证书相关的CAM/CAS连接错误
/var/nessus/logs/nessusd.messages	Nessus插件测验日志
/perfigo/control/apache/logs/ *	安全套接字协议层(SSL)证书， Apache错误日志
/perfigo/control/tomcat/logs/localhost *	Tomcat，重定向，JavaServer页(JSP)日志
/var/log/ha-log	CAM和CAS的高性能的日志

脚注-表3

1. 0而不是*显示最最近的日志。

2. 事件为从交换机的CAM接收的通知仅写入对的交换机管理注册文件系统(/perfigo/logs/perfigo-log0.log.0)。此外，只有当日志级别设置为INFO或更加细致时，这些事件写入到磁盘。

相关信息

- Cisco NAC设备支持页面
- 技术支持和文档 - Cisco Systems