在代理监视代理解析器服务上配置调试日志

目录

简介

本文档介绍如何在安全网络分析(SNA)流量收集器中切换代理监视/代理接收服务的调试日志。

背景信息

有时需要从SNA流量收集器代理接收功能的代理解析器启用调试日志。

代理接收功能是SNA流量收集器的固有功能，支持从思科网络安全设备(WSA)、McAfee、Bluecoat和Squid接收代理日志。

要配置此服务，请查看与您的Secure Network Analytics版本对应的代理服务器指南。

配置文档位于产品支持页面：https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html

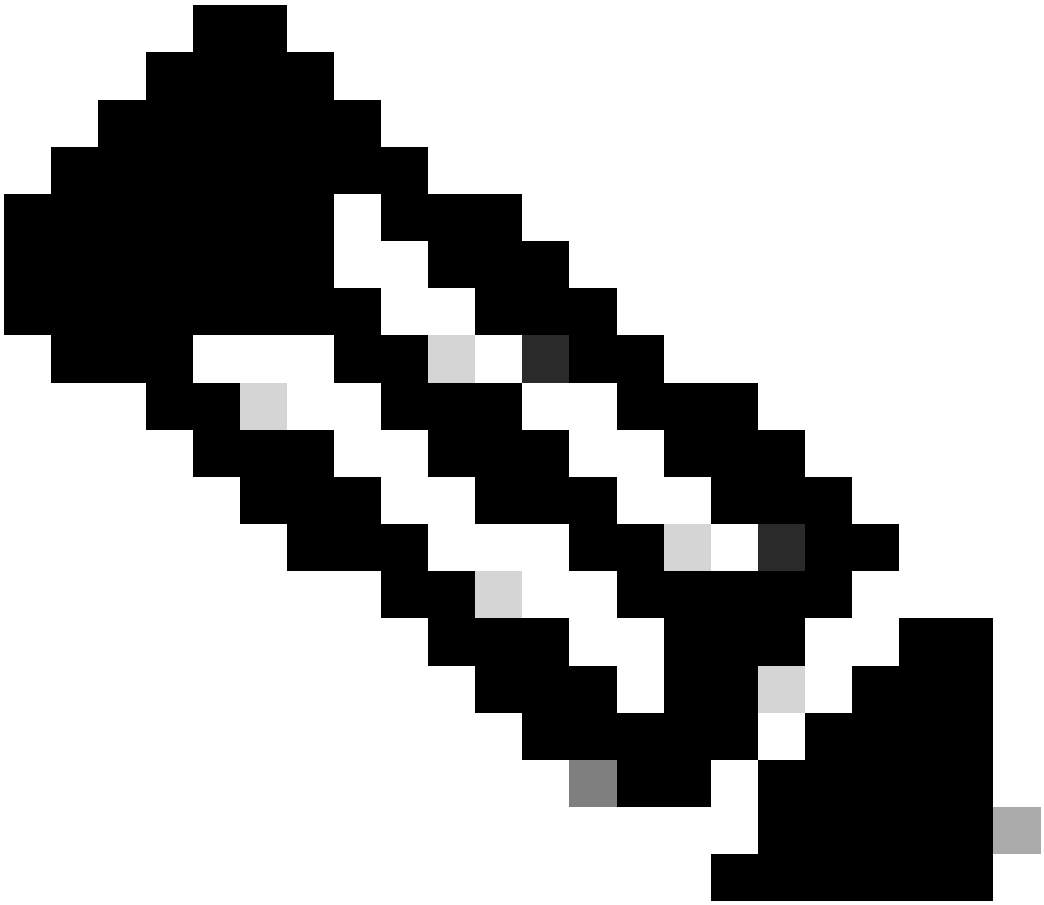
启用代理解析器调试

以root用户身份访问流量收集器控制台，或从sysadmin登录后可访问的System Configuration菜单打开根shell。

使用touch /lancope/var/sw-flow-proxyparser/config/a.xml命令创建空配置文件。

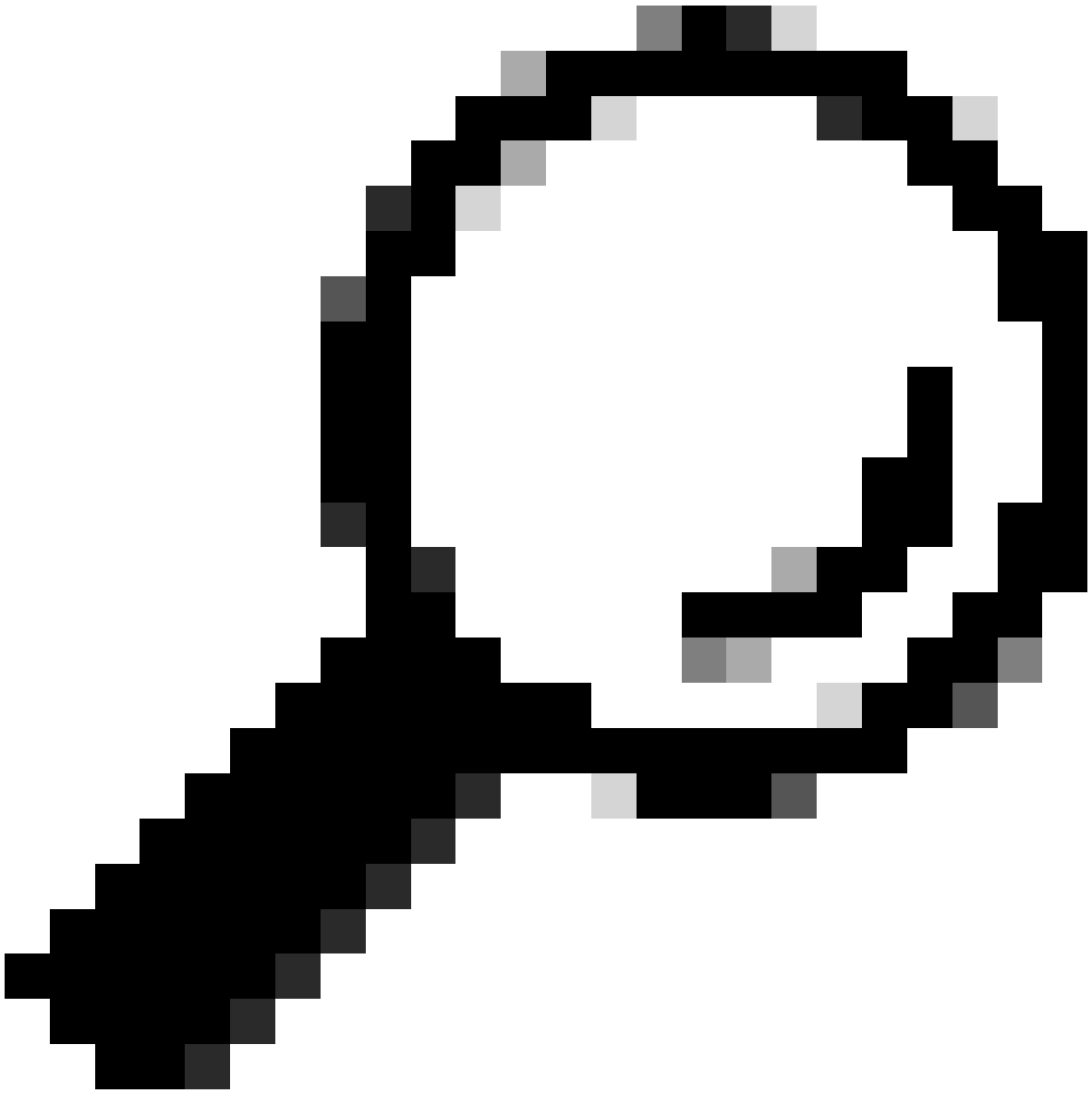
```
<#root>

741fc:~#

touch /lancope/var/sw-flow-proxyparser/config/a.xml
```

```
741fc:~#
```



注意：配置文件可以具有任何名称。配置文件按字母顺序加载，因此b.xml中定义的设置会覆盖从a.xml加载的相同设置。

使用**vi /lancope/var/sw-flow-proxyparser/config/a.xml**命令编辑a.xml文件并输入配置示例。



提示：按“i”键进入vi中的插入模式。按Esc键退出vi中的插入模式。键入“：wq”以在vi中保存和退出。键入“：q！”退出vi并放弃更改。

```
<command-line>
<param>--loglevel</param>
<param>com.lancope.sws.syslogprocess.handlers=DEBUG</param>
</command-line>
```

保存配置文件后，使用**systemctl restart sw-flow-proxyparser**命令重新启动代理解析器服务

<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

使用**tail -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.log**命令监视日志文件以查找代理日志解析错误。

更多描述性信息被添加到syslogprocessor.log日志文件中，这些信息可以指示接收到的代理消息数据中错误的来源。

如果未看到调试消息，则使用此替代配置，这是早期版本所必需的。

```
<command-line>
<param>--loglevels</param>
<param>com.lancope.sws.syslogprocess.handlers=DEBUG</param>
</command-line>
```

禁用代理解析器调试

运行**rm -i /lancope/var/sw-flow-proxyparser/config/a.xml** 命令，并在提示删除配置文件时输入y。

<#root>

741fc:~#

rm -i /lancope/var/sw-flow-proxyparser/config/a.xml

rm: remove regular file '/lancope/var/sw-flow-proxyparser/config/a.xml'?

y

741fc:~#

使用**systemctl restart sw-flow-proxyparser**命令重新启动代理解析器服务。

<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

调试配置已删除。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。