設定Proxy Watch Proxy剖析器服務的偵錯日誌

目錄

簡介

本檔案介紹如何在安全網路分析(SNA)流量收集器中切換Proxy Watch/Proxy Ingest服務的偵錯日誌。

背景資訊

有時需要從SNA流量收集器代理接收功能的代理分析程式啟用調試日誌。

代理接收功能是SNA流量收集器的本地功能，支援從思科網路安全裝置(WSA)、McAfee、Bluecoat和Squid接收代理日誌。

要配置此服務，請查閱適用於您的Secure Network Analytics版本的相應代理伺服器指南。

配置文檔位於產品支援頁面：https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html

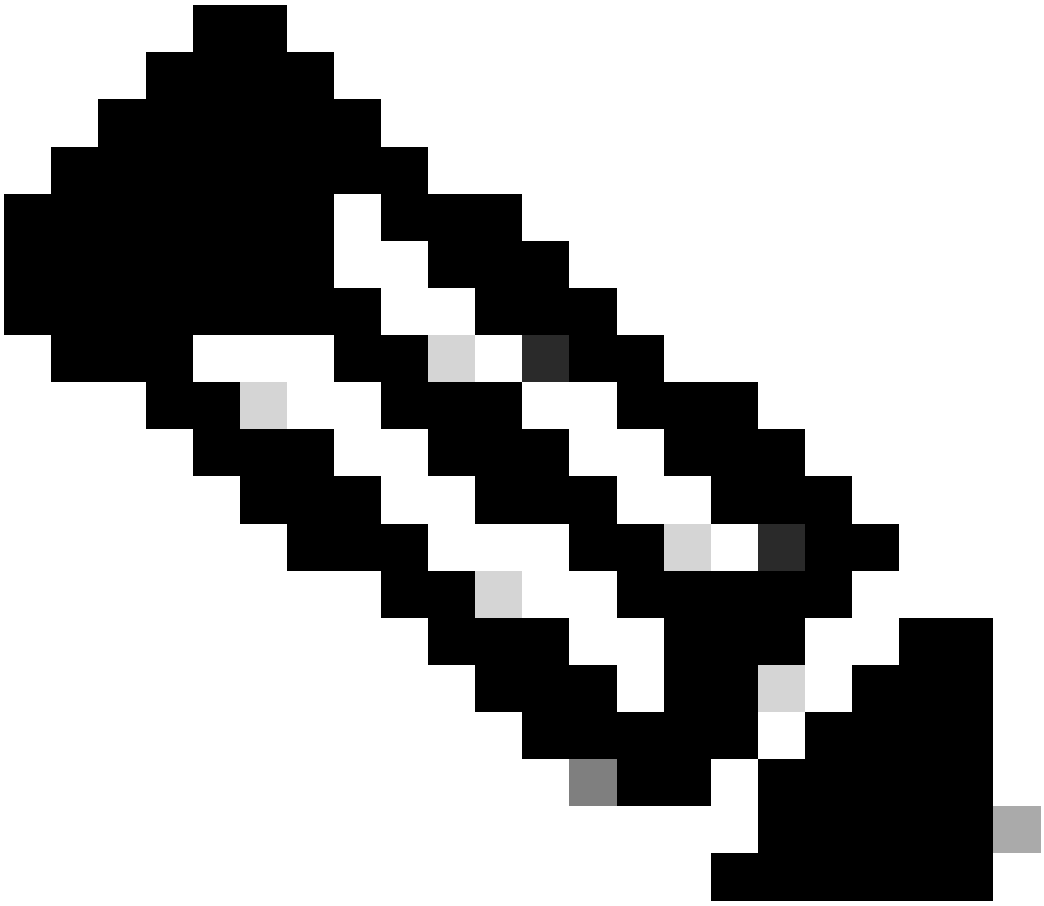
啟用代理剖析器偵錯

以root使用者身份訪問流量收集器控制檯，或者從系統管理員登入後可訪問的System Configuration選單中打開一個根shell。

使用touch /lancope/var/sw-flow-proxyparser/config/a.xml命令建立空配置檔案。

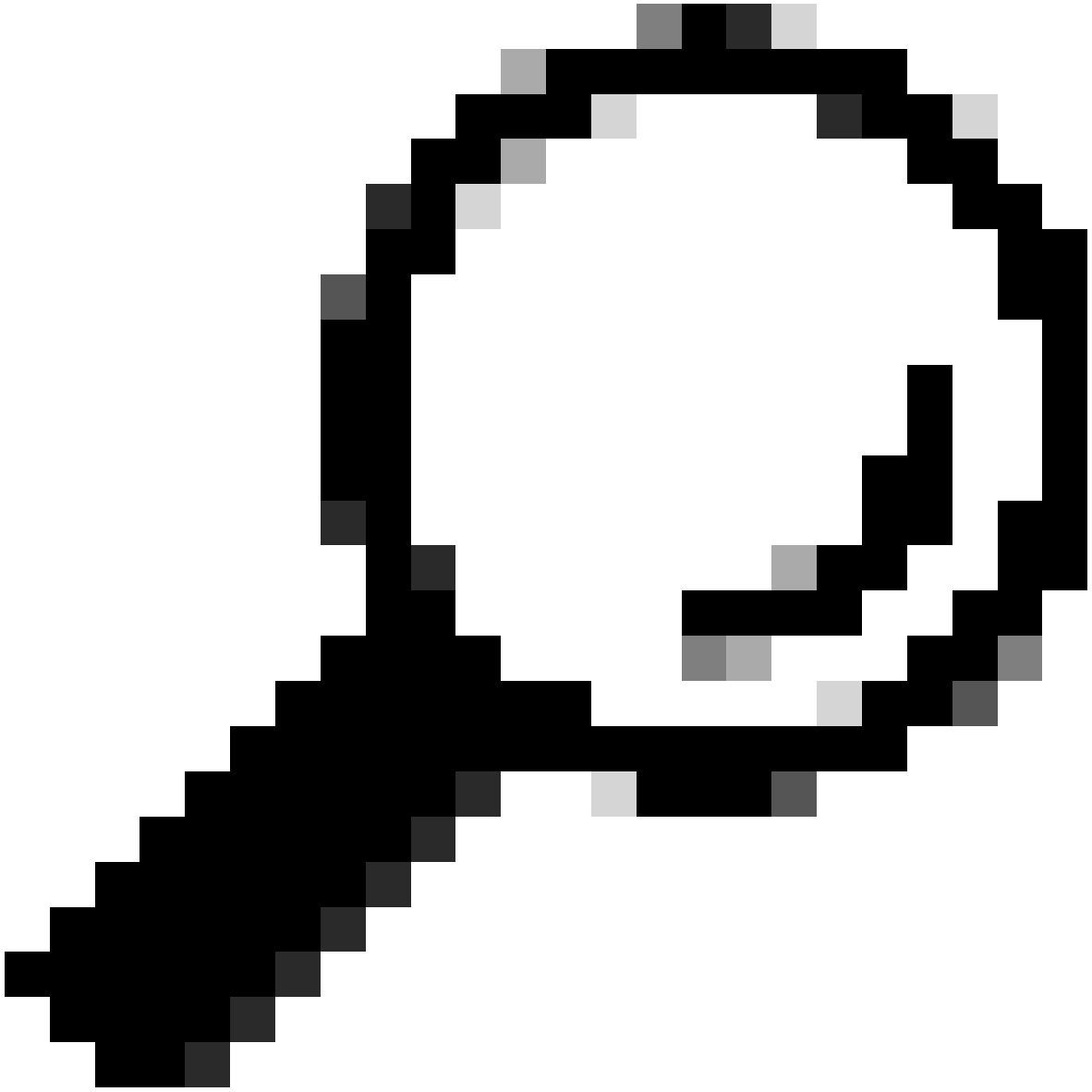
```
<#root>

741fc:~#

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

```
741fc:~#
```



注意：組態檔案可以有任何名稱。組態檔案會依照字母順序載入，因此在b.xml中定義的設定會覆寫從a.xml載入的相同設定。

使用**vi /lancope/var/sw-flow-proxyparser/config/a.xml**命令編輯a.xml檔案並輸入配置示例。



提示：按「i」鍵進入vi中的插入模式。按Esc鍵退出vi中的插入模式。鍵入「：wq」以儲存並退出vi。鍵入「：q！」退出並放棄在vi中進行的更改。

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

儲存配置檔案後，使用**systemctl restart sw-flow-proxyparser**命令重新啟動代理解析器服務

<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

使用**tail -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.log**命令監視代理日誌解析錯誤的日誌檔案。

更多描述性資訊被增加到syslogprocessor.log日誌檔案中，這些資訊可以指示接收到的代理消息資料中的錯誤來源。

如果未看到調試消息，則使用此替代配置，這是舊版本所必需的。

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

停用代理剖析器偵錯

運行**rm -i /lancope/var/sw-flow-proxyparser/config/a.xml** 命令，並在系統提示刪除配置檔案時輸入**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**命令重新啟動代理分析程式服務。

<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

已移除偵錯組態。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。