プロキシウォッチプロキシパーサーサービスのデバッグログの設定

内容

はじめに

このドキュメントでは、Secure Network Analytics(SNA)フローコレクタのプロキシウォッチ/プロキシ取り込みサービス(PWINS)のデバッグログを切り替える方法について説明します。

背景説明

SNA Flow Collector Proxy Ingest機能のプロキシパーサーからのデバッグログを有効にすることが必要な場合があります。

プロキシ取り込み機能はSNA Flow Collectorにネイティブで、Cisco Webセキュリティアプライアンス(WSA)、McAfee、Bluecoat、およびSquidからのプロキシログ取り込みをサポートします。

このサービスを設定するには、使用しているSecure Network Analyticsのバージョンに適した『Proxy Servers』ガイドを確認してください。

設定に関するドキュメントは、製品サポートページ(https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html)から入手できます。

プロキシパーサーデバッグを有効にする

ルートユーザとしてフローコレクタコンソールにアクセスするか、ログイン後にsysadminがアクセスできるシステム設定メニューからルートシェルを開きます。

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

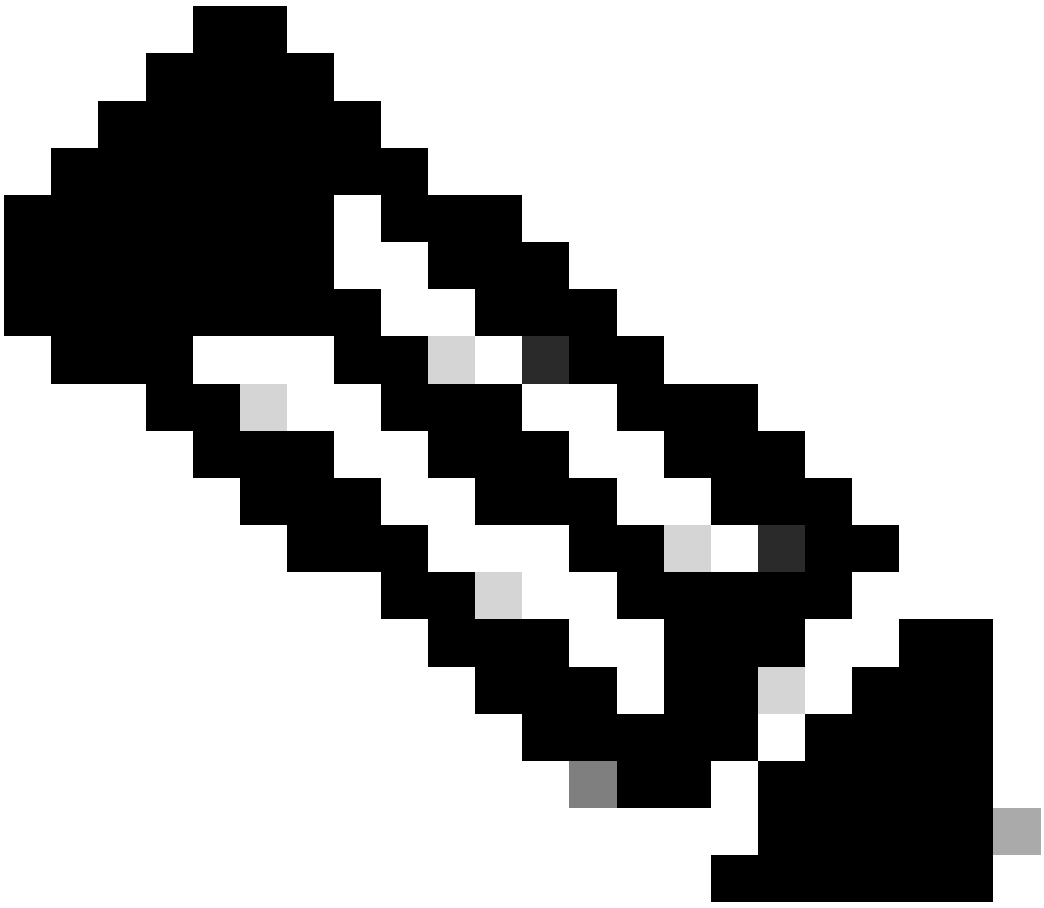
コマンドを使用して、空のコンフィギュレーションファイルを作成します。

<#root>

741fc:~#

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

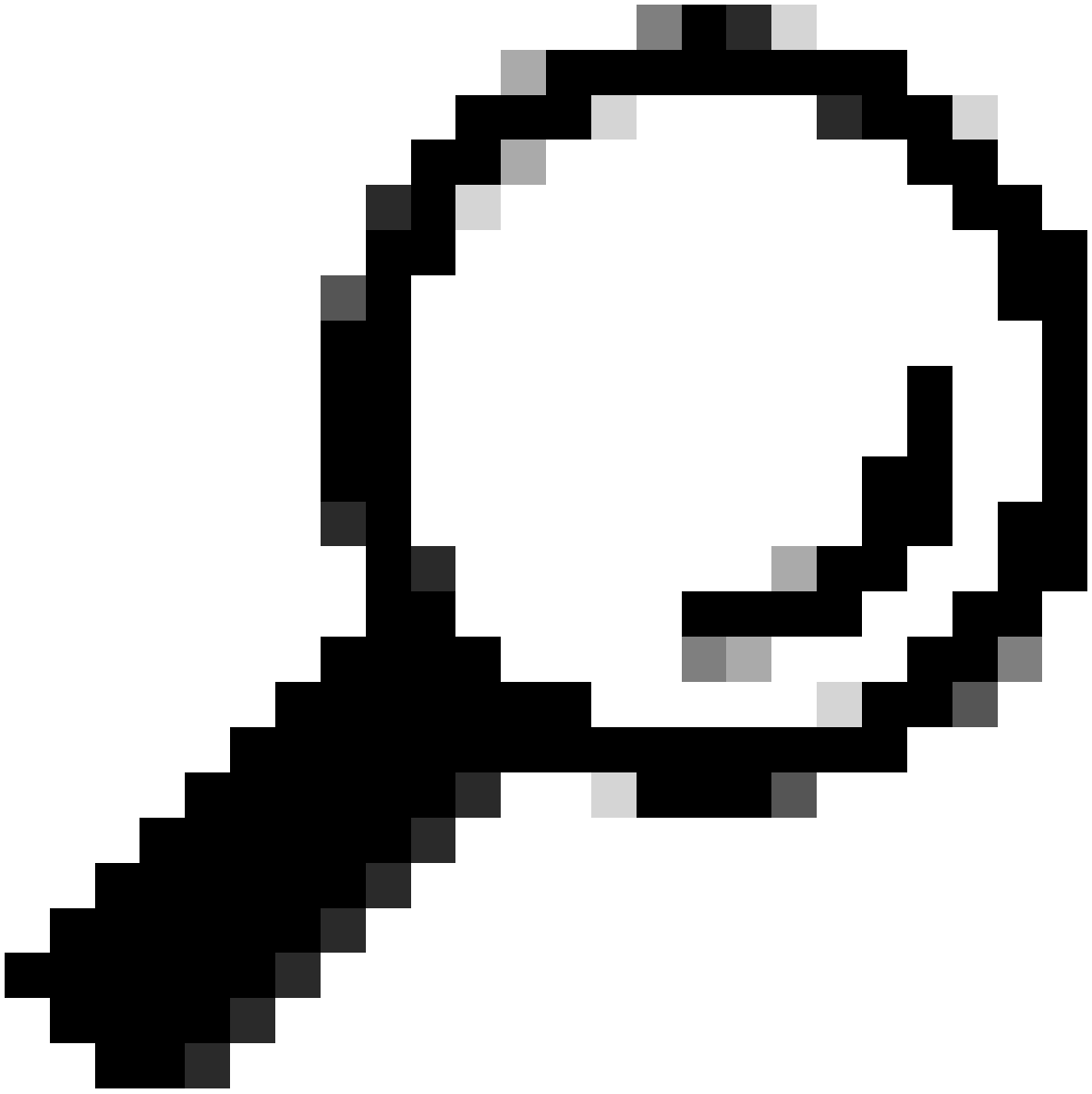
```
741fc:~#
```



注：コンフィギュレーションファイルには任意の名前を付けることができます。コンフィギュレーションファイルはアルファベット順にロードされるため、b.xmlで定義された設定は、a.xmlからロードされた同じ設定を上書きします。

---

vi /lancope/var/sw-flow-proxyparser/config/a.xmlコマンドを使用してa.xmlファイルを編集し、設定例を入力します。



ヒント:viで挿入モードに入るには「i」キーを押します。viで挿入モードを終了するには、'Esc'キーを押します。viで保存して終了するには「:wq」と入力します。終了してviの変更を破棄するには、「:q!」と入力します。

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

コンフィギュレーションファイルを保存したら、**systemctl restart sw-flow-proxyparser**コマンドを使用して、プロキシパーサーサービスを再起動します

<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

tail -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.logコマンドを使用して、プロキシログ解析エラーがないかログファイルを監視します。

syslogprocessor.logログファイルに、受信したプロキシメッセージデータのエラーの原因を示すより詳細な情報が追加されます。

デバッグメッセージが表示されない場合は、古いバージョンに必要なこの代替設定を使用します。

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

プロキシパーサーデバッグを無効にする

rm -i /lancope/var/sw-flow-proxyparser/config/a.xmlコマンドを実行し、コンフィギュレーションファイルを削除するように求められたら、**y**と入力します。

<**#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:~#

systemctl restart sw-flow-proxyparserコマンドを使用して、プロキシパーサーサービスを再起動します。

<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

デバッグ設定が削除されました。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。