Debug-Protokolle für Proxy Watch Proxy Parser Service konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Debug-Protokolle für den Proxy Watch/Proxy Ingest Service in Secure Network Analytics (SNA) Flow Collector umgeschaltet werden.

Hintergrundinformationen

Manchmal ist es erforderlich, Debug-Protokolle vom Proxy-Parser der SNA Flow Collector Proxy Ingest-Funktion zu aktivieren.

Die Proxy Ingest-Funktion ist nativ für SNA Flow Collector und unterstützt die Protokollierung über die Cisco Web Security Appliance (WSA), McAfee, Bluecoat und Squid.

Um diesen Service zu konfigurieren, lesen Sie das entsprechende Proxy-Server-Handbuch für Ihre Version von Secure Network Analytics.

Konfigurationsdokumente finden Sie auf der Seite für den Produktsupport unter: https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html

Proxyparser-Debugging aktivieren

Greifen Sie als Root-Benutzer auf die FlowCollector-Konsole zu, oder öffnen Sie eine Root-Shell über das Menü "System Configuration", auf das der Systemadministrator nach der Anmeldung zugreifen kann.

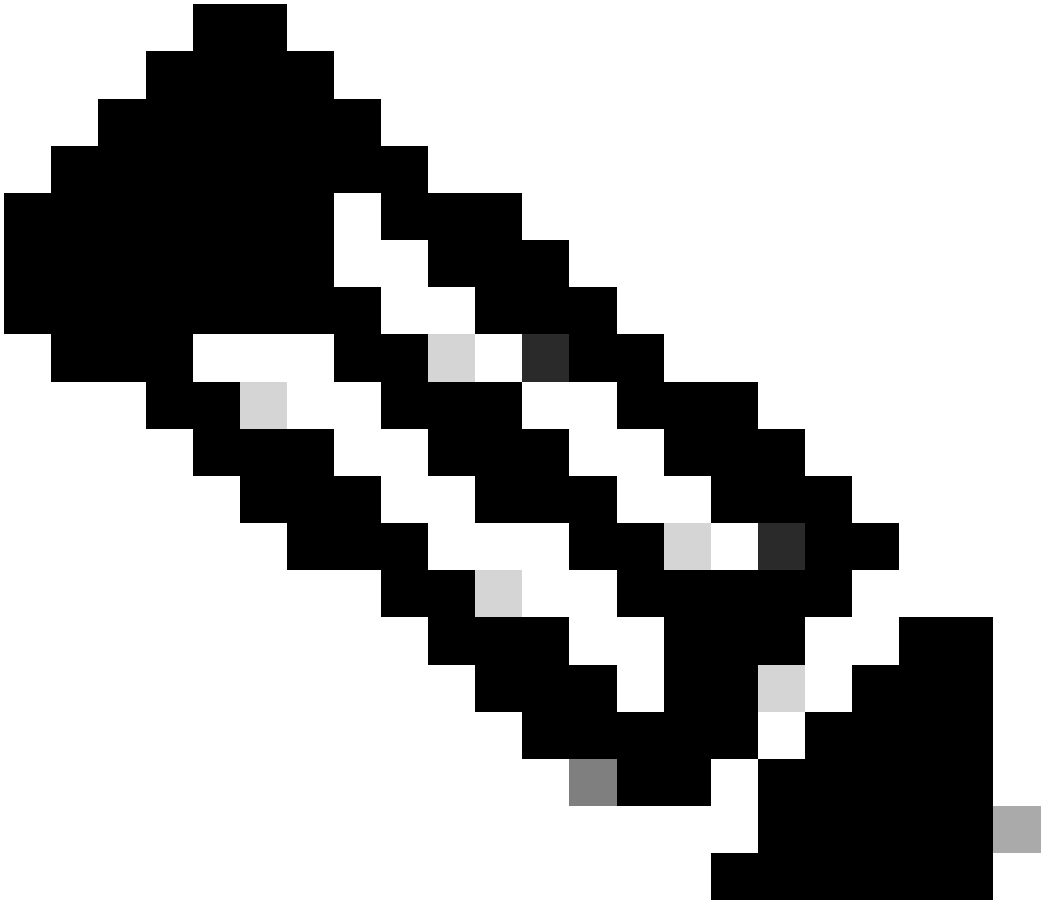
Erstellen Sie die leere Konfigurationsdatei mit dem touch /lancope/var/sw-flow-proxyparser/config/a.xml Befehl.

```
<#root>

741fc:~#
```

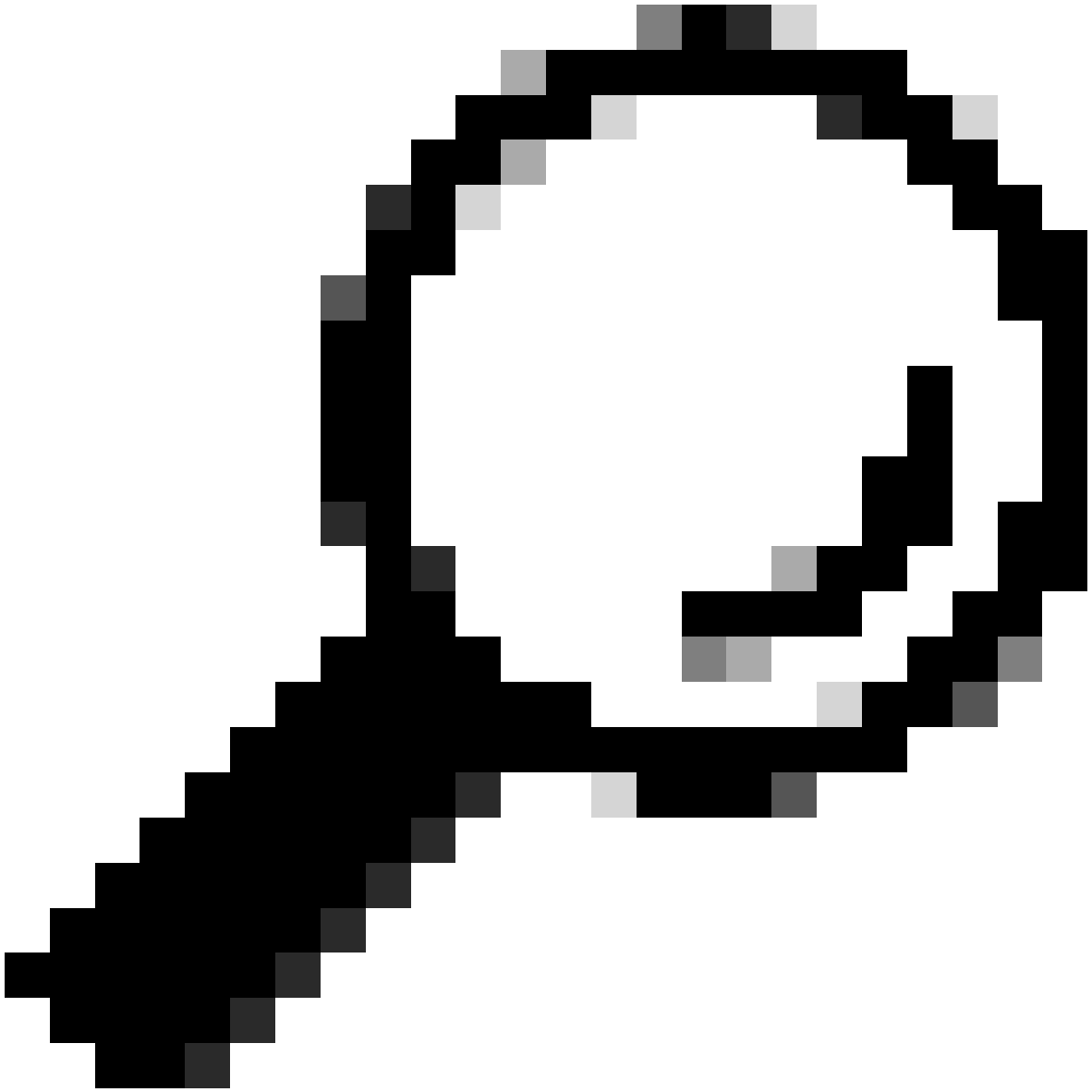
```
touch /lancope/var/sw-flow-proxyparser/config/a.xml
```

```
741fc:~#
```



Hinweis: Die Konfigurationsdatei kann einen beliebigen Namen haben. Konfigurationsdateien werden in alphabetischer Reihenfolge geladen, sodass eine in b.xml definierte Einstellung dieselben Einstellungen überschreibt, die aus a.xml geladen wurden.

Bearbeiten Sie die XML-Datei mit dem Befehl **vi /lancope/var/sw-flow-proxyparser/config/a.xml**, und geben Sie das Konfigurationsbeispiel ein.



Tipp: Drücken Sie die i-Taste, um in vi in den Einfügemodus zu wechseln. Drücken Sie die Esc-Taste, um den Einfügemodus in vi zu beenden. Geben Sie ":wq" ein, um zu speichern, und beenden Sie vi. Geben Sie ":q!" ein, um Änderungen in vi zu beenden und zu verwerfen.

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

Starten Sie nach dem Speichern der Konfigurationsdatei den Proxy-Parserdienst mit dem Befehl **systemctl restart sw-flow-proxyparser** neu.

<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

Überwachen Sie die Protokolldatei mit dem Befehl **tail -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.log auf** Fehler beim Analysieren des Proxyprotokolls.

Der Protokolldatei syslogprocessor.log werden weitere beschreibende Informationen hinzugefügt, die die Fehlerquelle in den empfangenen Proxy-Nachrichtendaten angeben können.

Wenn keine Debug-Meldungen angezeigt werden, verwenden Sie diese alternative Konfiguration, die für ältere Versionen erforderlich ist.

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

Proxyparser-Debugging deaktivieren

Führen Sie den Befehl **rm -i /lancope/var/sw-flow-proxyparser/config/a.xml aus**, und geben Sie **y ein**, wenn Sie aufgefordert werden, die Konfigurationsdatei zu löschen.

```
<#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:~#
```

Starten Sie den Proxy-Parserdienst mit dem Befehl **systemctl restart sw-flow-proxyparser** neu.

```
<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service
```

```
741fc:~#
```

Die Debugkonfiguration wurde entfernt.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.