Configuratie van debug-logbestanden op proxy-horloge-parserservice

Inhoud

Inleiding

Dit document beschrijft hoe u debug-logbestanden kunt schakelen voor de Proxy Watch / Proxy Ingest Service in Secure Network Analytics (SNA) Flow Collector.

Achtergrondinformatie

Het is soms nodig om debug logs van de proxy parser van de SNA Flow Collector Proxy Ingest functie in te schakelen.

De proxy Ingest-functie is afkomstig van SNA Flow Collector en ondersteunt proxy-logopname van Cisco Web Security Appliance (WSA), McAfee, Bluecoat en Squid.

Om deze service te configureren raadpleegt u de juiste Proxy Servers-handleiding voor uw versie van Secure Network Analytics.

Configuratiedocumenten kunnen worden gevonden op de pagina voor productondersteuning: https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html

Zuiveren van proxyparser inschakelen

Toegang tot de Flow Collector console als de wortelgebruiker of open een wortelshell van het menu van de Configuratie van het Systeem toegankelijk voor sysadmin zodra ingelogd.

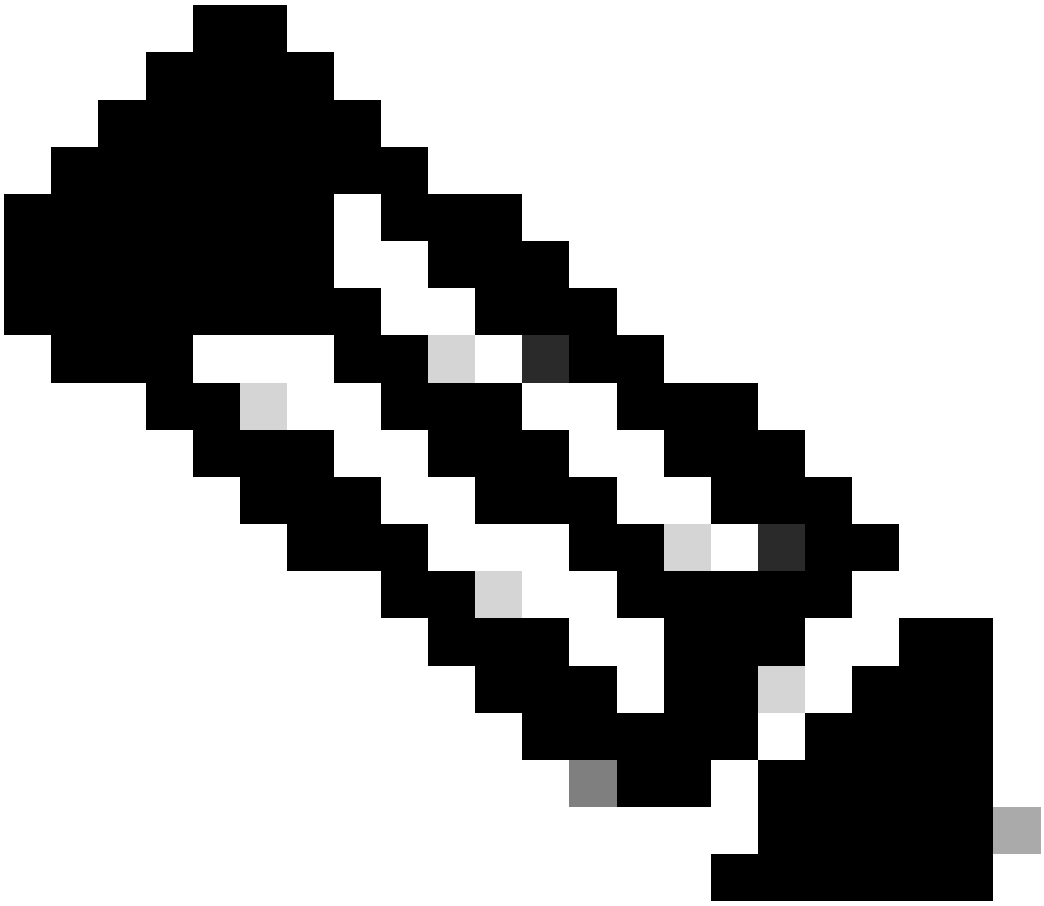
Maak het lege configuratiebestand met de opdrachttouch /lancope/var/sw-flow-proxyparser/config/a.xml.

```
<#root>

741fc:~#
```

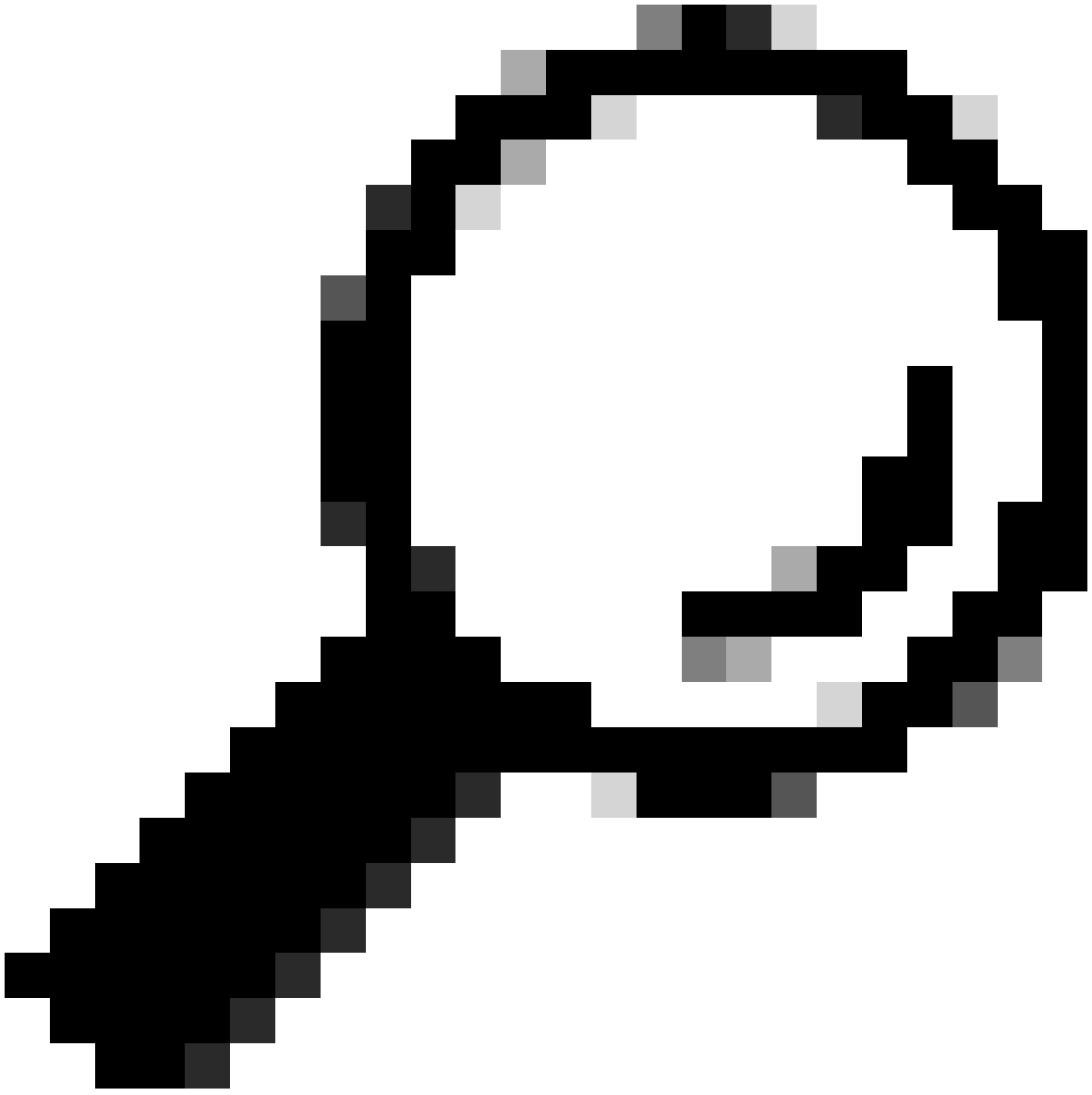
```
touch /lancope/var/sw-flow-proxyparser/config/a.xml
```

```
741fc:~#
```



Opmerking: het configuratiebestand kan elke naam hebben. De configuratiebestanden worden geladen in alfabetische volgorde, zodat een instelling die is gedefinieerd in b.xml dezelfde instellingen overschrijft die zijn geladen vanuit a.xml.

Bewerk het bestand a.xml met de opdracht **vi /lancope/var/sw-flow-proxyparser/config/a.xml** en voer het configuratievoorbeeld in.



Tip: Druk op de 'i' toets om de invoegmodus in vi te activeren. Druk op de 'Esc' toets om de invoegmodus in vi te verlaten. Typ ":wq" om op te slaan en af te sluiten in vi. Typ ":q!" om de wijzigingen in de vi te beëindigen en weg te gooien.

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

Zodra het configuratiebestand is opgeslagen, start u de proxy parser service opnieuw met de **systematische opnieuw opstarten sw-flow-proxyparser** opdracht

<#root>

```
741fc:~#
```

systemctl restart sw-flow-proxyparser.service

```
741fc:~#
```

Controleer het logbestand voor proxylogbestand parse fouten met de **staart -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.log** opdracht.

Meer beschrijvende informatie wordt toegevoegd aan het syslogprocessor.log bestand dat kan wijzen op de bron van de fout in de ontvangen proxy bericht gegevens.

Als debug berichten niet gezien worden gebruik deze alternatieve configuratie die is vereist voor oudere versies.

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

Zuiveren van proxyparser uitschakelen

Start de opdracht **rm -i /lancope/var/sw-flow-proxyparser/config/a.xml** en voer **y in** wanneer u wordt gevraagd om het configuratiebestand te

verwijderen.

<#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:~#

Start de proxy parser service opnieuw met de **systemctl start sw-flow-proxyparser** opdracht.

<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

De debug-configuratie is verwijderd.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.