프록시 감시 프록시 파서 서비스에 대한 디버그 로그 구성

목차

소개

이 문서에서는 SNA(Secure Network Analytics) 흐름 컬렉터에서 프록시 감시/프록시 수집 서비스에 대한 디버그 로그를 전환하는 방법에 대해 설명합니다.

배경 정보

SNA Flow Collector Proxy Ingest 기능의 프록시 파서에서 디버그 로그를 활성화해야 하는 경우가 있습니다.

프록시 수집 기능은 SNA Flow Collector에서 기본 제공되며 Cisco WSA(Web Security Appliance), McAfee, Bluecoat 및 Squid에서 프록시 로그 수집을 지원합니다.

이 서비스를 구성하려면 사용 중인 Secure Network Analytics 버전에 맞는 프록시 서버 가이드를 검토하십시오.

구성 문서는 제품 지원 페이지 (https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html)에서 찾을 수 있습니다.

프록시 파서 디버깅 사용

루트 사용자로 Flow Collector 콘솔에 액세스하거나, 로그인한 sysadmin에 액세스할 수 있는 시스템 구성 메뉴에서 루트 셸을 엽니다.

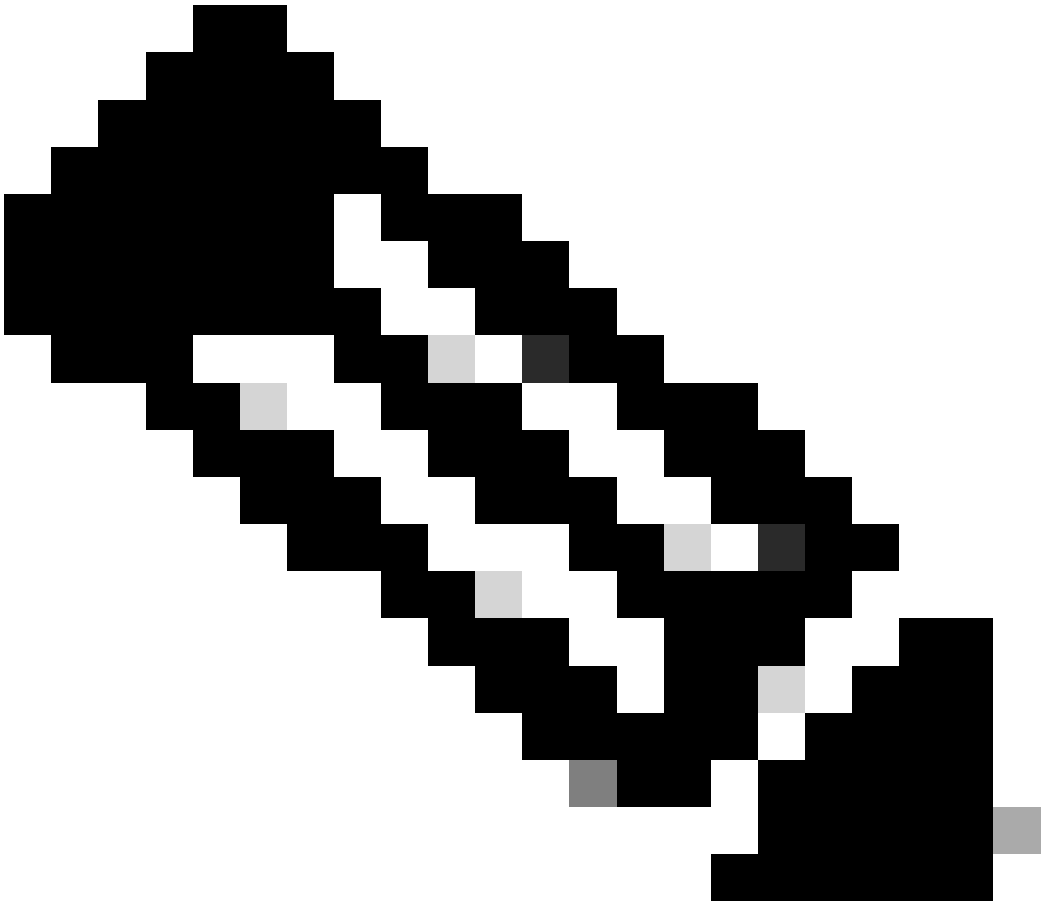
명령을 사용하여 빈 컨피그레이션 파일을 touch /lancope/var/sw-flow-proxyparser/config/a.xml 생성합니다.

```
<#root>

741fc:~#
```

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

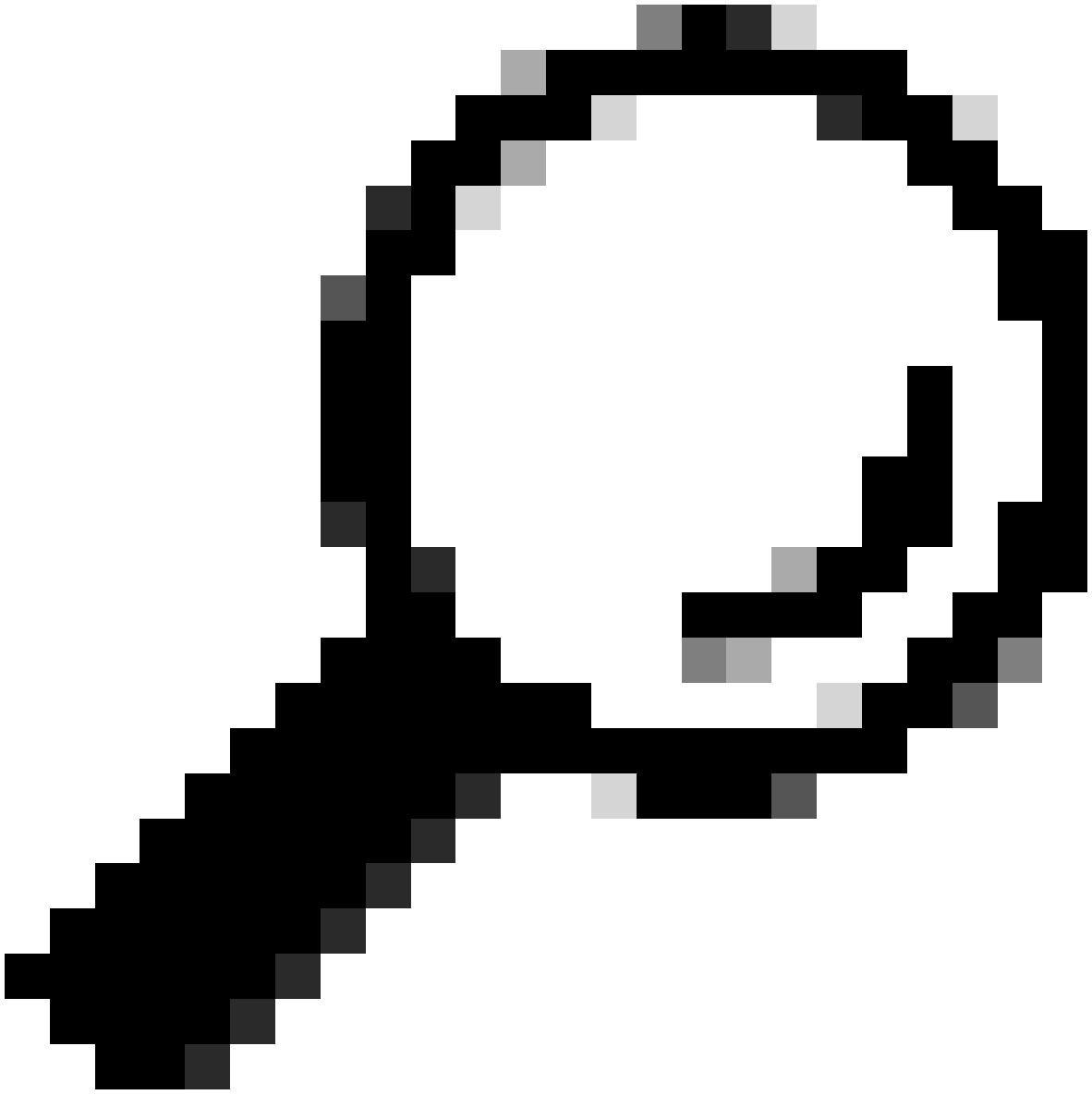
```
741fc:~#
```



참고: 컨피그레이션 파일의 이름은 무엇이든 지정할 수 있습니다. 컨피그레이션 파일은 알파벳 순서로 로드되므로 b.xml에 정의된 설정이 a.xml에서 로드된 동일한 설정을 덮어씁니다.

---

vi /lancope/var/sw-flow-proxyparser/config/a.xml 명령을 사용하여 a.xml **파일**을 편집하고 컨피그레이션 예를 입력합니다.



팁: vi에서 삽입 모드로 들어가려면 'i' 키를 누르십시오. vi에서 삽입 모드를 종료하려면 'Esc' 키를 누릅니다. vi에서 저장하고 종료하려면 ":wq"를 입력합니다. vi에서 변경 사항을 종료하고 취소하려면 ":q!"를 입력합니다.

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

컨피그레이션 파일이 저장되면 systemctl restart sw-flow-proxyparser 명령을 사용하여 프록시 **파서 서비스**를 재시작합니다

<**#root**>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

tail -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.log 명령을 사용하여 로그 파일에서 프록시 로그 구문 분석 **오류**를 모니터링합니다.

수신된 프록시 메시지 데이터에서 오류의 원인을 나타낼 수 있는 syslogprocessor.log 로그 파일에 자세한 설명 정보가 추가됩니다.

디버그 메시지가 표시되지 않으면 이전 버전에 필요한 이 대체 컨피그레이션을 사용합니다.

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

프록시 파서 디버깅 사용 안 함

rm -i /lancope/var/sw-flow-proxyparser/config/a.xml 명령을 실행하고 컨피그레이션 파일을 삭제하라는 프롬프트가 표시되면 **y**를 입력합니다.

<#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 명령을 **사용하여 프록시 파서 서비스를** 다시 시작합니다.

<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

디버그 컨피그레이션이 제거되었습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.