Configurar Logs de Depuração no Serviço de Analisador de Proxy de Observação de Proxy

Contents

Introdução

Este documento descreve como alternar logs de depuração para o serviço de observação de proxy/ingestão de proxy no coletor de fluxo do Secure Network Analytics (SNA).

Informações de Apoio

Às vezes, é necessário habilitar logs de depuração do analisador de proxy do recurso SNA Flow Collector Proxy Ingest.

O recurso Ingestão de proxy é nativo do SNA Flow Collector e suporta a inclusão de registro de proxy do Cisco Web Security Appliance (WSA), McAfee, Bluecoat e Squid.

Para configurar esse serviço, consulte o guia apropriado de servidores proxy para a sua versão do Secure Network Analytics.

Os documentos de configuração podem ser encontrados na página de suporte do produto: https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html

Habilitar depuração do analisador de proxy

Acesse o console do Flow Collector como o usuário raiz ou abra um shell raiz no menu System Configuration (Configuração do sistema) acessível ao administrador do sistema depois de fazer login.

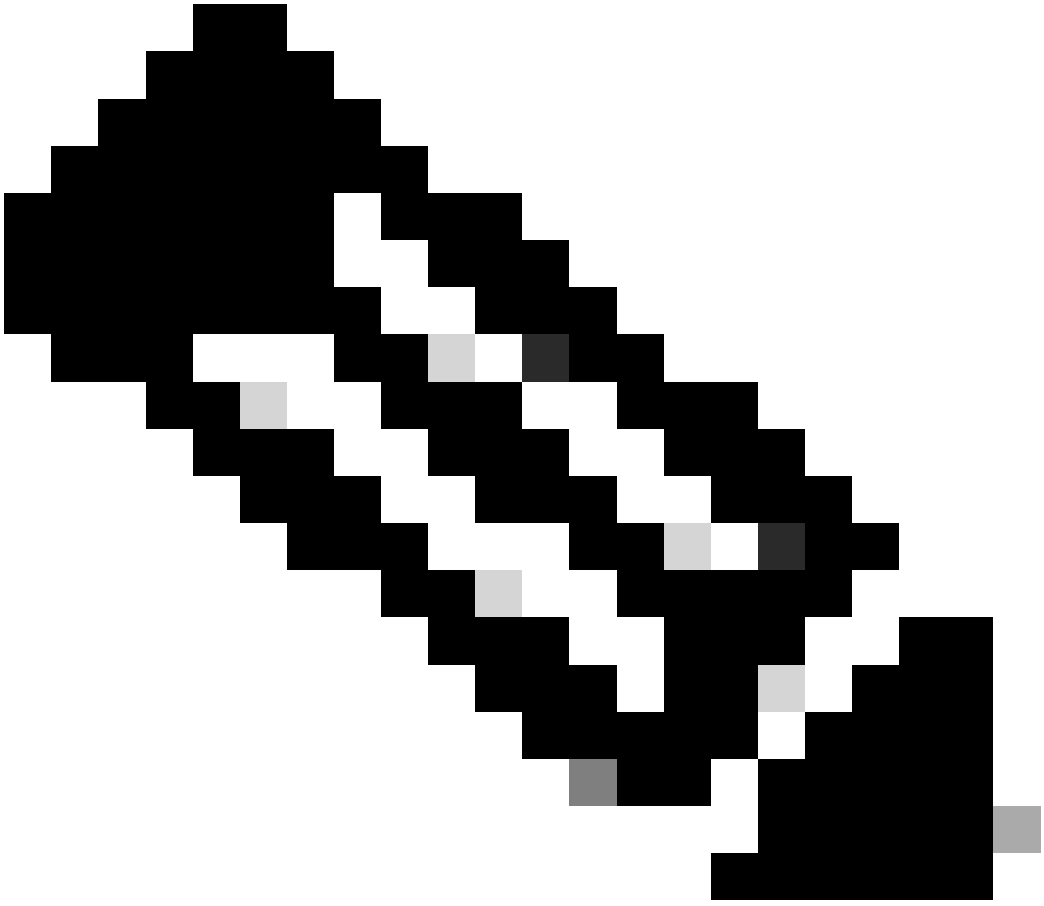
Crie o arquivo de configuração vazio com o comando`touch /lancope/var/sw-flow-proxyparser/config/a.xml`.

```
<#root>

741fc:~#
```

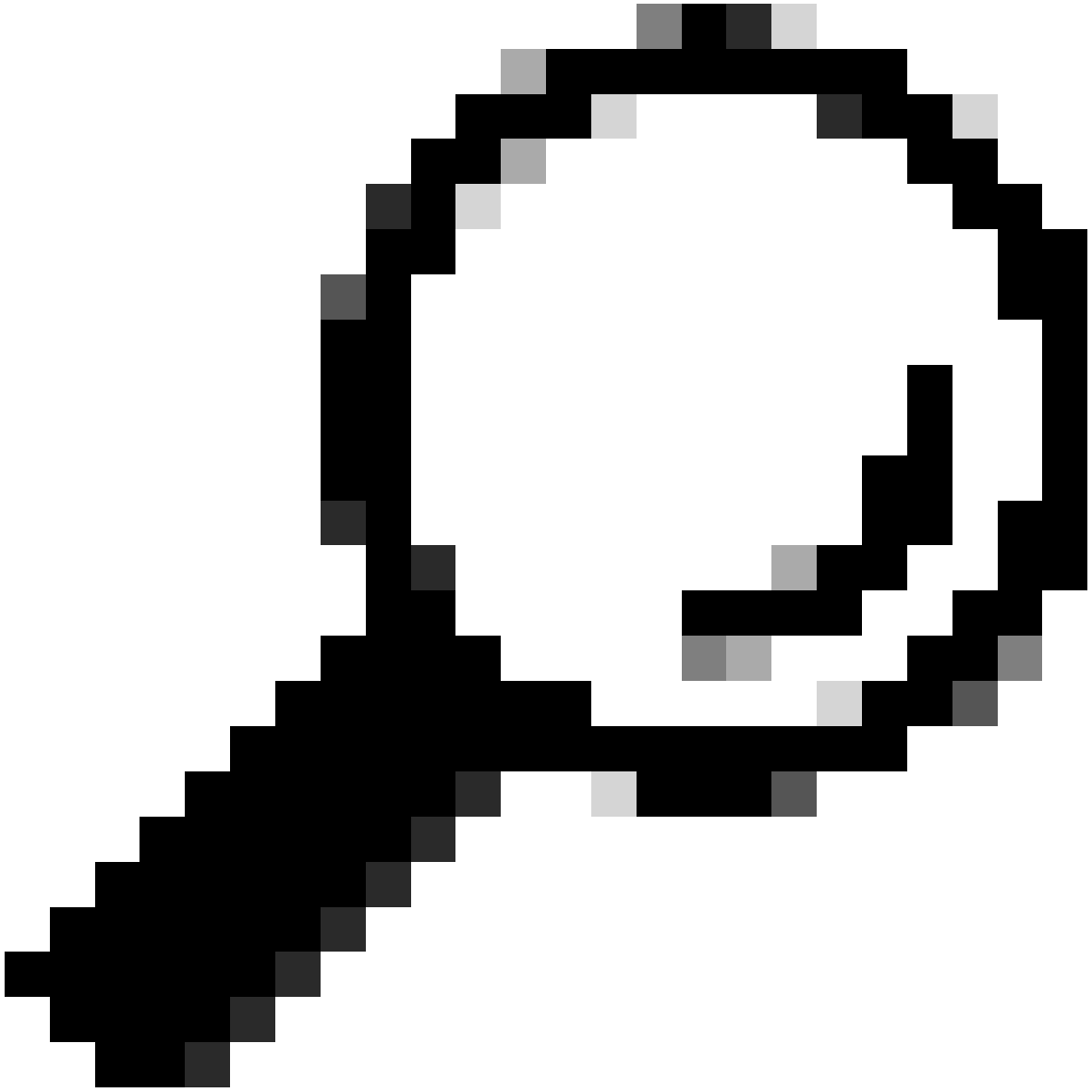
```
touch /lancope/var/sw-flow-proxyparser/config/a.xml
```

```
741fc:~#
```



Observação: o arquivo de configuração pode ter qualquer nome. Os arquivos de configuração são carregados em ordem alfabética, portanto uma configuração definida em b.xml substitui as mesmas configurações carregadas de a.xml.

Edite o arquivo a.xml com o comando **vi /lancope/var/sw-flow-proxyparser/config/a.xml** e insira o exemplo de configuração.



Dica: pressione a tecla 'i' para entrar no modo de inserção no vi. Pressione a tecla 'Esc' para sair do modo de inserção no vi. Digite ":wq" para salvar e sair em vi. Digite ":q!" para sair e descartar as alterações no vi.

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

Quando o arquivo de configuração for salvo, reinicie o serviço de analisador de proxy com o comando **systemctl restart sw-flow-proxyparser**

```
<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#
```

Monitore o arquivo de log para erros de análise de log de proxy com o comando **tail -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.log**.

Informações mais descritivas são adicionadas ao arquivo de log syslogprocessor.log, que pode indicar a origem do erro nos dados da mensagem de proxy recebida.

Se as mensagens de depuração não forem vistas, use esta configuração alternativa, que é necessária para versões mais antigas.

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

Desabilitar depuração do analisador de proxy

Execute o comando **rm -i /lancope/var/sw-flow-proxyparser/config/a.xml** e insira **y** quando solicitado a excluir o arquivo de configuração.

<#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:~#

Reinicie o serviço de analisador de proxy com o comando **systemctl restart sw-flow-proxyparser**.

<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

A configuração de depuração foi removida.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.