Configurar registros de depuración en el servicio de analizador de proxy Watch

Contenido

Introducción

Este documento describe cómo alternar los registros de depuración para Proxy Watch / Proxy Ingest Service en el Flow Collector de Secure Network Analytics (SNA).

Antecedentes

A veces es necesario habilitar los registros de depuración del analizador de proxy de la función SNA Flow Collector Proxy Ingest.

La función de ingesta de proxy es nativa de SNA Flow Collector y admite la ingestión de registros de proxy desde Cisco Web Security Appliance (WSA), McAfee, Bluecoat y Squid.

Para configurar este servicio, consulte la guía de servidores proxy correspondiente a su versión de Secure Network Analytics.

Los documentos de configuración se pueden encontrar en la página de asistencia del producto: https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html

Habilitar depuración del analizador de proxy

Acceda a la consola Flow Collector como usuario raíz o abra un shell raíz desde el menú System Configuration, al que puede acceder el administrador del sistema una vez que haya iniciado sesión.

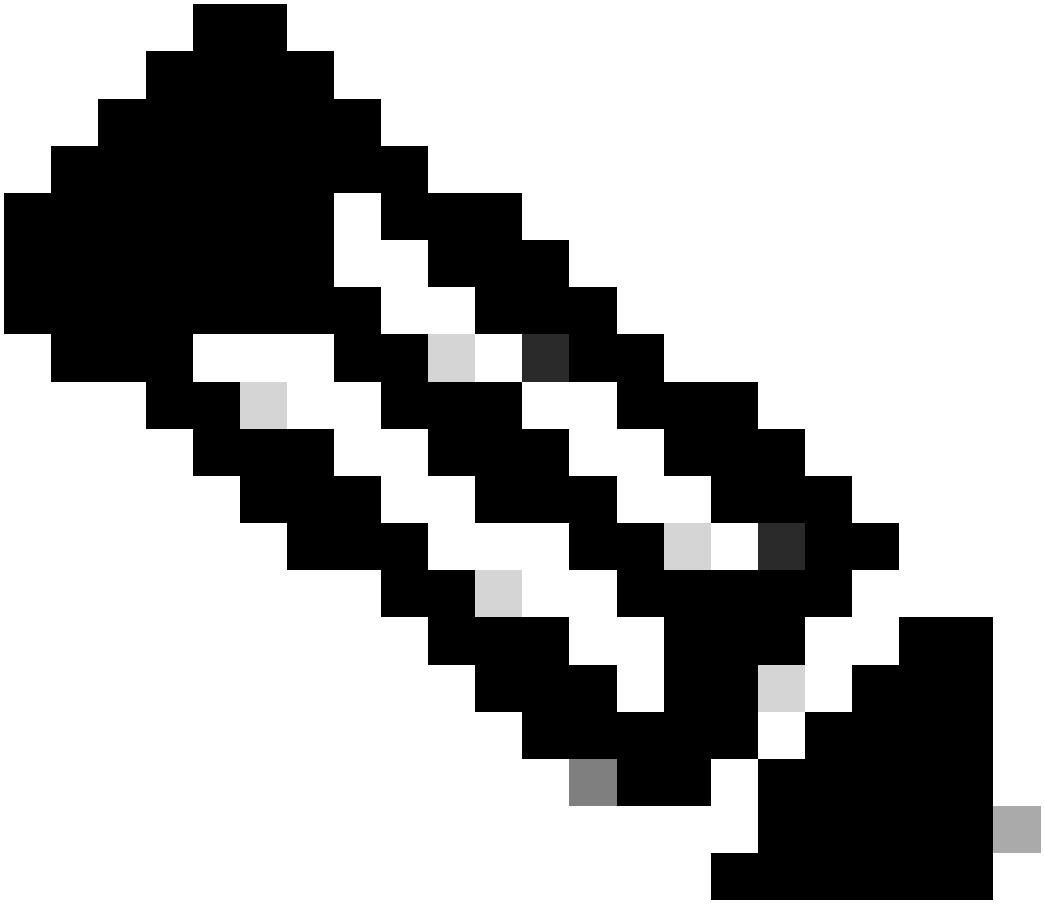
Cree el archivo de configuración vacío con el touch /lancope/var/sw-flow-proxyparser/config/a.xml comando.

```
<#root>

741fc:~#
```

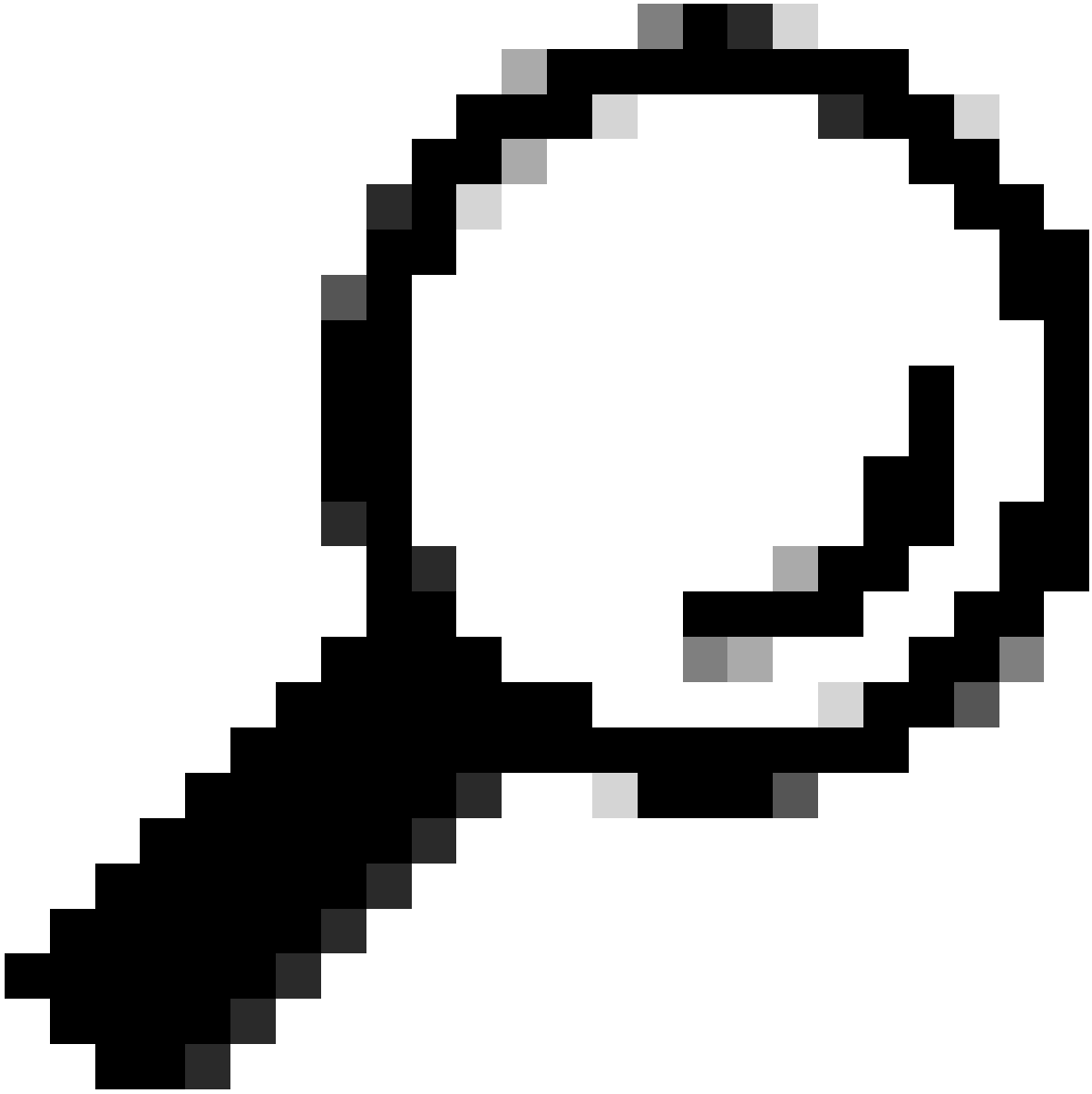
```
touch /lancope/var/sw-flow-proxyparser/config/a.xml
```

```
741fc:~#
```



Nota: El archivo de configuración puede tener cualquier nombre. Los archivos de configuración se cargan en orden alfabético, por lo que una configuración definida en b.xml sobrescribe la misma configuración cargada desde a.xml.

Edite el archivo a.xml con el comando **vi /lancope/var/sw-flow-proxyparser/config/a.xml** e ingrese el ejemplo de configuración.



Sugerencia: presione la tecla 'i' para ingresar al modo de inserción en vi. Pulse la tecla "Esc" para salir del modo de inserción en vi. Escriba ":wq" para guardar y salir en vi. Escriba ":q!" para salir y descartar los cambios en vi.

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

Una vez guardado el archivo de configuración, reinicie el servicio de analizador de proxy con el comando **systemctl restart sw-flow-proxyparser**

<#root>

```
741fc:~#
```

systemctl restart sw-flow-proxyparser.service

```
741fc:~#
```

Supervise el archivo de registro para detectar errores de análisis de registro de proxy con el comando **tail -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.log**.

Se agrega información más descriptiva al archivo de registro syslogprocessor.log que puede indicar el origen del error en los datos de mensajes proxy recibidos.

Si no se ven mensajes de depuración, utilice esta configuración alternativa, que es necesaria para las versiones anteriores.

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

Deshabilitar depuración del analizador proxy

Ejecute el comando **rm -i /lancope/var/sw-flow-proxyparser/config/a.xml** e ingrese **y** cuando se le solicite eliminar el archivo de configuración.

```
<#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 el servicio de analizador de proxy con el comando **systemctl restart sw-flow-proxyparser**.

```
<#root>

741fc:~#

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

```
741fc:~#
```

Se ha eliminado la configuración de depuración.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).