Configura i log di debug nel servizio parser proxy di controllo

Sommario

Introduzione

In questo documento viene descritto come attivare o disattivare i log di debug per il servizio di acquisizione proxy in SNA (Secure Network Analytics) Flow Collector.

Premesse

A volte è necessario abilitare i log di debug dal parser proxy della funzione di acquisizione proxy del raccoglitore di flussi SNA.

La funzione proxy Ingest è nativa di SNA Flow Collector e supporta l'acquisizione del log proxy da Cisco Web Security Appliance (WSA), McAfee, Bluecoat e Squid.

Per configurare questo servizio, esaminare la guida ai server proxy appropriata per la versione di Secure Network Analytics in uso.

I documenti di configurazione sono disponibili nella pagina di supporto del prodotto: https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html

Abilita debug parser proxy

Accedere alla console di Flow Collector come utente root o aprire una shell root dal menu Configurazione di sistema accessibile al sysadmin una volta effettuato l'accesso.

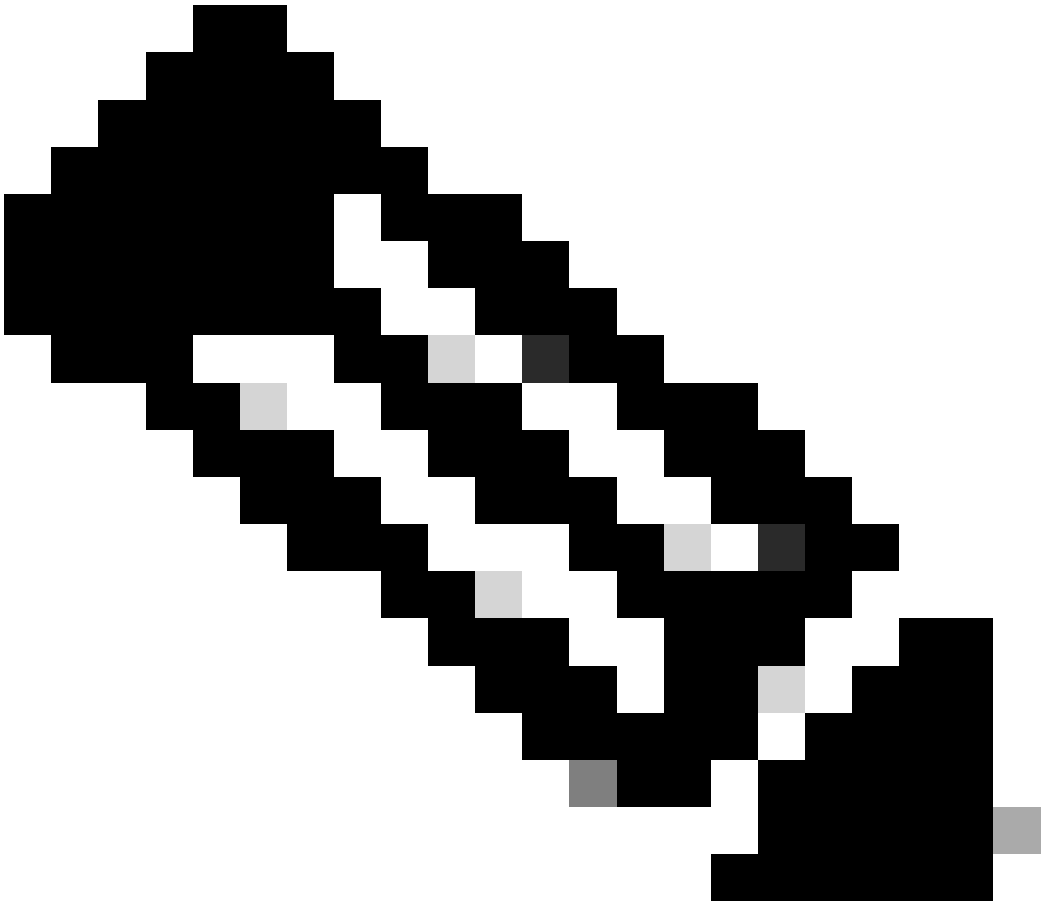
Creare il file di configurazione vuoto con il touch /lancope/var/sw-flow-proxyparser/config/a.xml comando.

```
<#root>

741fc:~#
```

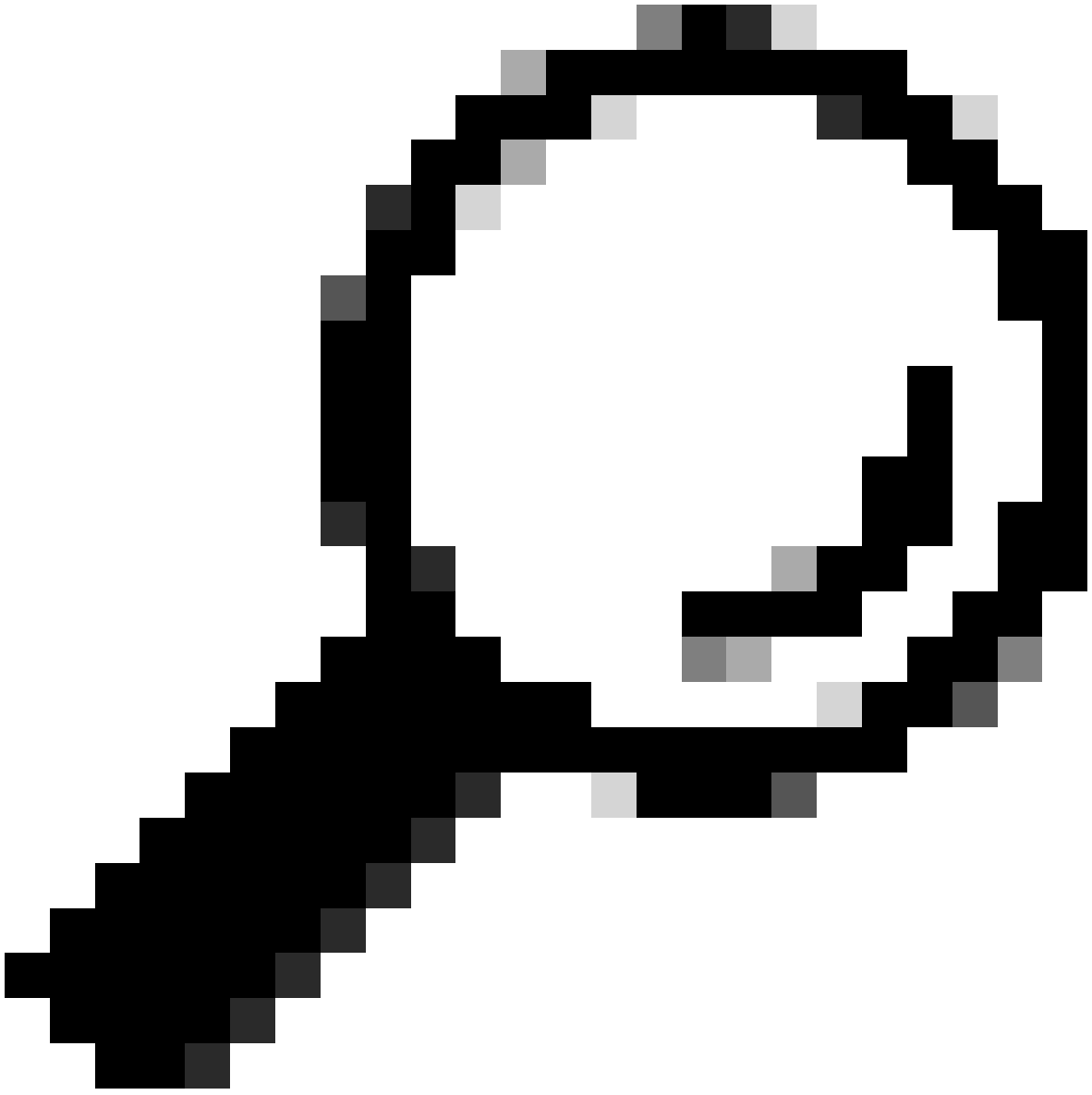
```
touch /lancope/var/sw-flow-proxyparser/config/a.xml
```

```
741fc:~#
```



Nota: il file di configurazione può avere qualsiasi nome. Poiché i file di configurazione vengono caricati in ordine alfabetico, un'impostazione definita in b.xml sovrascrive le stesse impostazioni caricate da a.xml.

Modificare il file a.xml con il comando **vi /lancope/var/sw-flow-proxyparser/config/a.xml** e immettere l'esempio di configurazione.



Suggerimento: premere 'i' per accedere alla modalità di inserimento in vi. Premere 'Esc' per uscire dalla modalità di inserimento in vi. Digitare ":wq" per salvare e uscire in vi. Digitate ":q!" per uscire ed eliminare le modifiche in vi.

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

Dopo aver salvato il file di configurazione, riavviare il servizio parser proxy con il comando **systemctl restart sw-flow-proxyparser**

<#root>

```
741fc:~#
```

systemctl restart sw-flow-proxyparser.service

```
741fc:~#
```

Monitorare il file di log per individuare eventuali errori di analisi del log proxy con il comando **tail -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.log**.

Nel file di log syslogprocessor.log vengono aggiunte informazioni più descrittive che possono indicare l'origine dell'errore nei dati del messaggio proxy ricevuto.

Se i messaggi di debug non vengono visualizzati, utilizzare questa configurazione alternativa richiesta per le versioni precedenti.

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

Disabilita debug parser proxy

Eseguire il comando **rm -i /lancope/var/sw-flow-proxyparser/config/a.xml** e immettere **y** quando richiesto per eliminare il file di configurazione.

<#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:~#

Riavviare il servizio parser proxy con il comando **systemctl restart sw-flow-proxyparser**.

<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#

La configurazione di debug è stata rimossa.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).