Configurer les journaux de débogage sur le service Proxy Watch Proxy Parser

Table des matières

Introduction

Ce document décrit comment basculer les journaux de débogage pour le service Proxy Watch / Proxy Ingest dans le collecteur de flux Secure Network Analytics (SNA).

Informations générales

Il est parfois nécessaire d'activer les journaux de débogage à partir de l'analyseur proxy de la fonctionnalité SNA Flow Collector Proxy Ingest.

La fonction d'ingestion proxy est native de SNA Flow Collector et prend en charge l'ingestion de journaux proxy depuis Cisco Web Security Appliance (WSA), McAfee, Bluecoat et Squid.

Pour configurer ce service, consultez le guide des serveurs proxy correspondant à votre version de Secure Network Analytics.

Les documents de configuration sont disponibles sur la page d'assistance produit : https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html

Activer le débogage du parseur proxy

Accédez à la console du collecteur de flux en tant qu'utilisateur racine ou ouvrez un shell racine à partir du menu Configuration du système accessible à l'administrateur système une fois connecté.

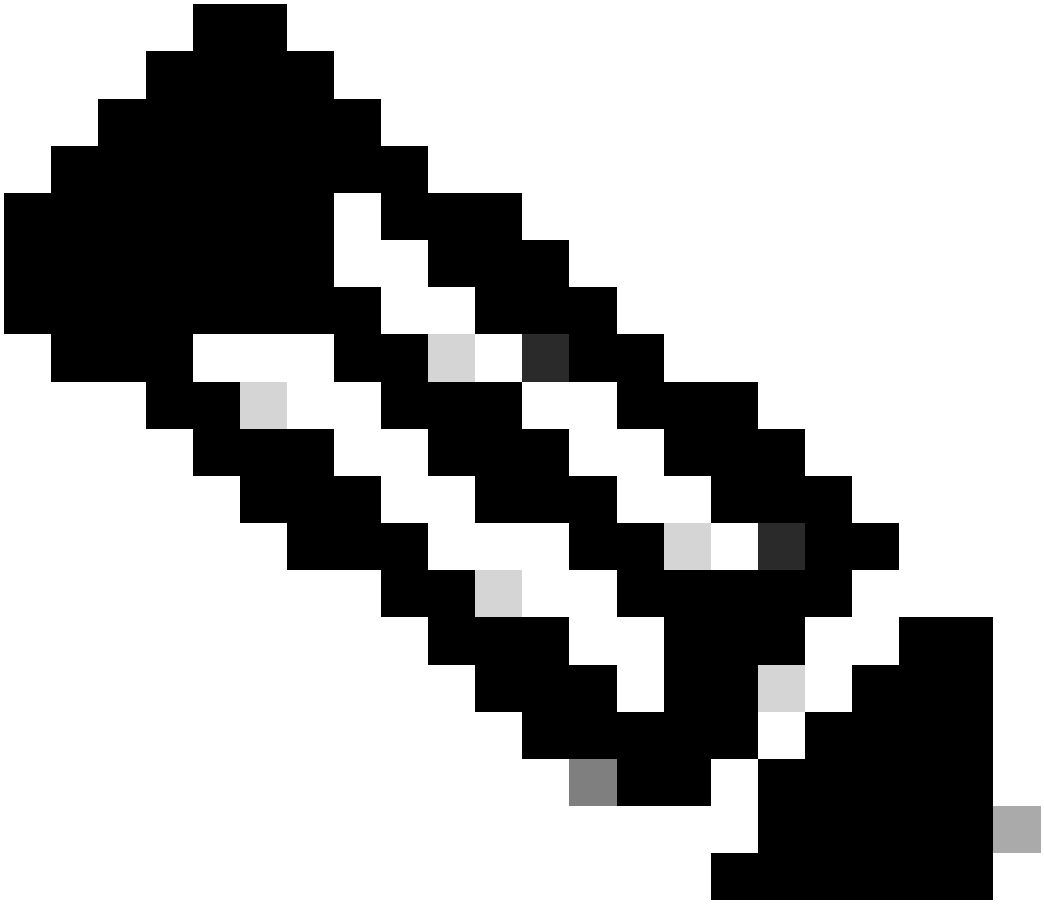
Créez le fichier de configuration vide à l'aide de la commande`touch /lancope/var/sw-flow-proxyparser/config/a.xml`.

```
<#root>

741fc:~#
```

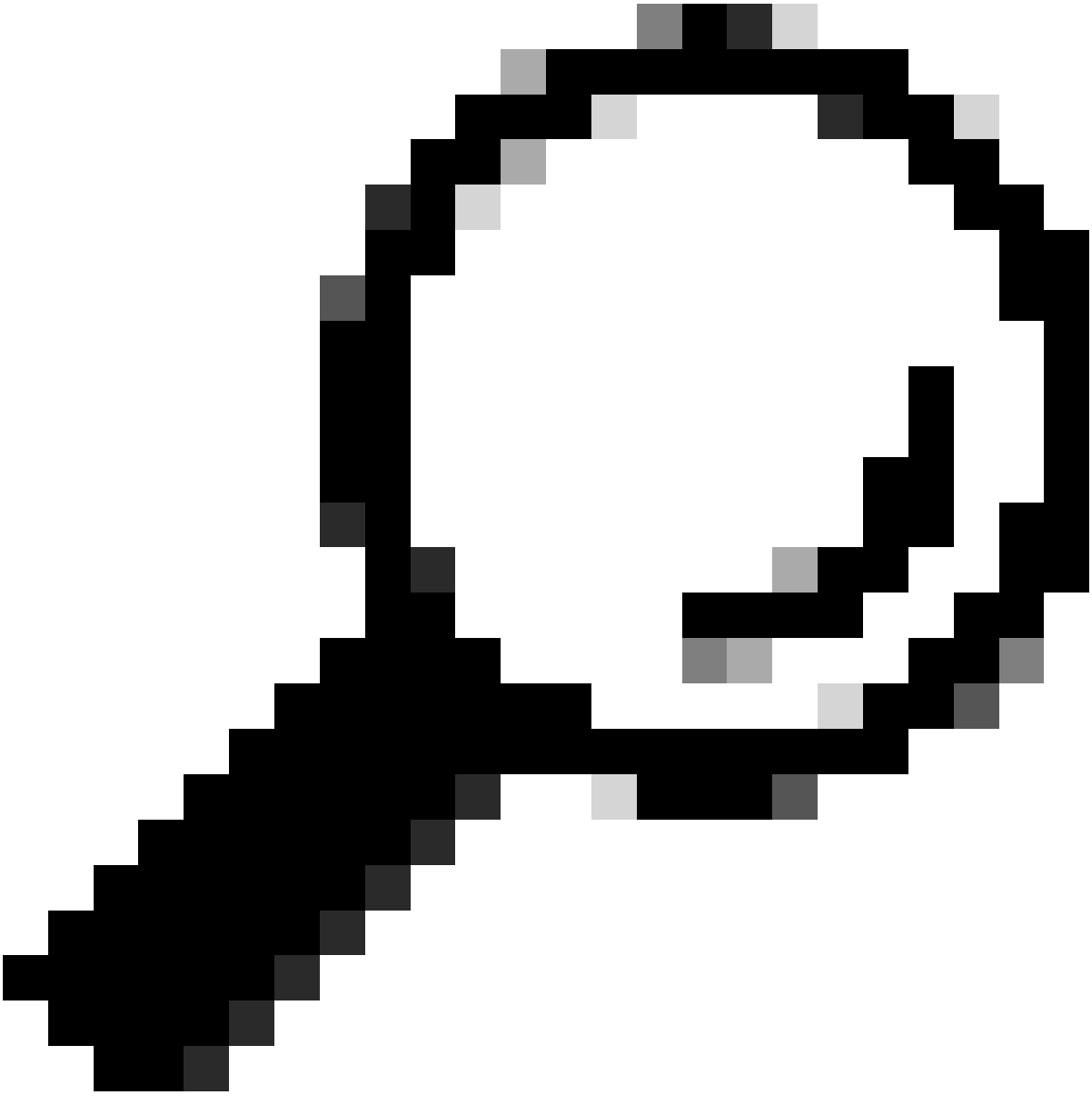
```
touch /lancope/var/sw-flow-proxyparser/config/a.xml
```

```
741fc:~#
```



Remarque : le fichier de configuration peut porter n'importe quel nom. Les fichiers de configuration sont chargés par ordre alphabétique, de sorte qu'un paramètre défini dans b.xml remplace les mêmes paramètres chargés à partir du fichier a.xml.

Modifiez le fichier a.xml à l'aide de la commande **vi /lancope/var/sw-flow-proxyparser/config/a.xml** et entrez l'exemple de configuration.



Conseil : appuyez sur la touche 'i' pour passer en mode insertion dans vi. Appuyez sur la touche Échap pour quitter le mode insertion dans vi. Entrez « : wq » pour enregistrer et quitter dans vi. Tapez « : q ! » pour quitter et annuler les modifications dans vi.

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

Une fois le fichier de configuration enregistré, redémarrez le service d'analyse proxy avec la commande **systemctl restart sw-flow-proxyparser**

```
<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#
```

Surveillez les erreurs d'analyse du journal du proxy dans le fichier journal à l'aide de la commande **tail -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.log**.

Des informations plus descriptives sont ajoutées au fichier journal syslogprocessor.log qui peut indiquer la source de l'erreur dans les données de message proxy reçues.

Si les messages de débogage ne sont pas visibles, utilisez cette configuration alternative qui est requise pour les versions antérieures.

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

Désactiver le débogage de proxy parser

Exécutez la commande **rm -i /lancope/var/sw-flow-proxyparser/config/a.xml** et entrez **y** lorsque vous y êtes invité pour supprimer le fichier de configuration.

```
<#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:~#
```

Redémarrez le service d'analyse proxy à l'aide de la commande **systemctl restart sw-flow-proxyparser**.

```
<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#
```

La configuration de débogage a été supprimée.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.