Configure Debug Logs on Proxy Watch Proxy Parser Service

Contents

Introduction
Background Information
Enable proxy parser debugging
Disable proxy parser debugging

Introduction

This document describes how to toggle debug logs for the Proxy Watch / Proxy Ingest Service in Secure Network Analytics (SNA) Flow Collector.

Background Information

It is sometimes necessary to enable debug logs from the proxy parser of the SNA Flow Collector Proxy Ingest feature.

The proxy Ingest feature is native to SNA Flow Collector and supports proxy log ingestion from Cisco Web Security Appliance (WSA), McAfee, Bluecoat, and Squid.

To configure this service review the appropriate Proxy Servers guide for your version of Secure Network Analytics.

Configuration documents can be located on the product support page: https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html

Enable proxy parser debugging

Access the Flow Collector console as the root user or open a root shell from the System Configuration menu accessible to the sysadmin once logged in.

Create the empty configuration file with the `touch /lancope/var/sw-flow-proxyparser/config/a.xml` command.

```
<#root>

741fc:~#

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


741fc:~#
```

Note: The configuration file can have any name. Configuration files are loaded in alphabetical order, so a setting defined in b.xml overwrites the same settings loaded from a.xml.

Edit the a.xml file with the **vi /lancope/var/sw-flow-proxyparser/config/a.xml** command and enter the configuration example.

> **Tip**: Press the 'i' key to enter insert mode in vi. Press the 'Esc' key to exit insert mode in vi. Type ":wq" to save and quit in vi. Type ":q!" to quit and discard changes in vi.

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

Once the configuration file is saved, retart the proxy parser service with the **systemctl restart sw-flow-proxyparser** command

<#root>

```
741fc:~#

systemctl restart sw-flow-proxyparser.service


741fc:~#
```

Monitor the log file for proxy log parse errors with the **tail -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.log** command.

More descriptive information is added to the syslogprocessor.log log file that can indicate the source of the error in the received proxy message data.

If debug messages are not seen use this alternate configuration which is required for older versions.

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

Disable proxy parser debugging

Run the **rm -i /lancope/var/sw-flow-proxyparser/config/a.xml** command and enter **y** when promted to delete the configuration file.

<#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:~#
```

Restart the proxy parser service with the **systemctl restart sw-flow-proxyparser** command.

<#root>

```
741fc:~#
systemctl restart sw-flow-proxyparser.service

741fc:~#
```

The debug configuration has been removed.