Cisco Secure Network Analytics

Proxy Log Configuration Guide 7.4.2



Table of Contents

Introduction	
Overview	3
Important Configuration Guidelines	3
Configuring the Blue Coat Proxy Logs	5
Creating the Format	5
Create a New Log	6
Configure the Upload Client	7
Configuring the Upload Schedule	10
Notes	
Configuration of the Visual Policy Manager	10
Configuring the McAfee Proxy Logs	
Configuring the Cisco Web Security Appliance (WSA) Proxy Logs	20
Configuring Squid Proxy Logs	
Configuring the Flow Collector	
Checking the Flows	
Contacting Support	
Change History	

Introduction

Overview

In order to gather user information from your network proxy servers for the Cisco Secure Network Analytics (formerly Stealthwatch) Proxy Log you need to configure the proxy servers logs so that the Flow Collector can receive the information and the Manager (formerly Stealthwatch Management Console) will display the information on the Flow Proxy Records page. This page provides URLs and application names of the traffic inside a network going through the proxy server.

This document describes the various procedures needed to configure the logs for different proxy servers. These servers are Blue Coat, McAfee, Cisco WSA, and Squid. This document assumes that you already have the proxy server running as part of your network. The procedures describe how to configure the proxy's logs so that the files necessary for the Flow Collector are given and the information is provided.

Complete the following steps to set up Secure Network Analytics Proxy Log:

- 1. Configure your proxy server:
 - a. Blue Coat
 - b. <u>McAfee</u>
 - c. <u>Cisco WSA</u>
 - d. <u>Squid</u>
- 2. Configure the Flow Collector
- 3. Check the Flows

Important Configuration Guidelines

When configuring the logs for any of the proxies, you must make certain to adhere to these guidelines:

- The Flow Collector and the proxy must use the same NTP server or receive time from a common source for flow and proxy records to be matched.
- When setting the IP address for Flow Collector, select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.
- There is no specific size limit on syslog proxy messages imposed by Secure Network Analytics. However, we recommend that messages be kept shorter than the shortest Maximum Transmission Unit (MTU) along the path between the proxy

and Flow Collector, usually 1500. This will eliminate packet fragmentation and increase reliability.

• Proxy Log is not supported in High Availability (HA) mode.

Configuring the Blue Coat Proxy Logs

This chapter describes the procedure for configuring the Blue Coat proxy logs to deliver to Secure Network Analytics.



Creating the Format

To create a new log format, complete the following steps:

- 1. In your browser, access your Blue Coat proxy server.
- 2. Click the **Configuration** tab.



- 3. In the main menu of the Management Console, click **Access Logging > Formats**.
- 4. Click **New** at the bottom of the page. The Create Format page opens.

Create Format	×
Format Settings:	
Format Name:	
 Custom format string (specify below) 	
W3C Extended Log File Format (ELFF) string (specify below) supplier-name rs(Content-Type) cs(User-Agent) sc-filter-result sc-filter-category x-vi	s-id s-ip s-sitename Test Format
Multiple-valued header policy: Log last header	
OK Cancel	

- 5. In the Format Name field, type a name for the new format.
- 6. Select the W3C Extended Log File Format (ELFF) option.
- 7. In the format field, type the following string:

```
timestamp duration c-ip c-port r-ip r-port s-ip s-port cs-bytes sc-bytes cs-user cs-host cs-uri
```

8. Click OK. Continue to the next section, Create a New Log

Create a New Log

To create the logs, complete the following steps:

 In the main menu, click Access Logging > Logs, and then select the new log format. The Log page opens.

Log Settings:	te Log
Log Settings:	
Log Name: Log Format: StealthWatch Description: Log file limits: The maximum size of each remote file is 0 megabytes Start an early upload if log reaches 16000 megabytes Note: The maximum allowed upload threshold is: 19999 megabyte OK Cancel	Log Settings:
Log Name: Log Format: StealthWatch Description: Log file limits: The maximum size of each remote file is 0 megabytes Start an early upload if log reaches 16000 megabytes Note: The maximum allowed upload threshold is: 19999 megabyte OK Cancel	
Log Format: StealthWatch Description: Log file limits: The maximum size of each remote file is megabytes Start an early upload if log reaches Start an early upload if log reaches Note: The maximum allowed upload threshold is: 19999 megabyte OK Cancel	Log Name:
Description: Log file limits: The maximum size of each remote file is Start an early upload if log reaches Start an early upload if log reaches Note: The maximum allowed upload threshold is: 19999 megabyte OK Cancel	Log Format: StealthWatch
Log file limits:	Description:
Log file limits:	
The maximum size of each remote file is 0 megabytes Start an early upload if log reaches 16000 megabytes Note: The maximum allowed upload threshold is: 19999 megabyte OK Cancel	Log file limits:
The maximum size of each remote file is 0 megabytes Start an early upload if log reaches 16000 megabytes Note: The maximum allowed upload threshold is: 19999 megabyte OK Cancel	
Start an early upload if log reaches 16000 megabytes Note: The maximum allowed upload threshold is: 19999 megabyte OK Cancel	The maximum size of each remote file is 0 megabytes
Note: The maximum allowed upload threshold is: 19999 megabyte	Start an early upload if log reaches 16000 megabytes
OK Cancel	Note: The maximum allowed upload threshold is: 19999 megabyte
OK Cancel	
OK Cancel	
	OK Cancel

2. Click the General Settings tab.

Logs General :	t ings Upload Client Upload Schedule	
	Log: StealthWatch	·
Log Settings:		
Log Format: StealthW	h	
Description:		
· Log file limits:		
The maximum size of e	remote file is 0 megabytes	
	reaches 16000 megabytes	
Start an early upload if	Todalos Todal Mingably cos	

- 3. From the Log Format drop-down list, select the log you created in Step 1.
- 4. In the Description field, type a description for your new log.
- Click the Apply button at the bottom of the page. Continue to the next section, Configure the Upload Client

Configure the Upload Client

To configure the upload client, complete the following steps:

1. Click the **Upload Client** tab. The Upload Client page opens.

Logs Gene	ral Settings	Upload Client	Upload Schedule
	Log: Stea	althWatch	~
Upload Client:			
Client type: Custo	m Client		✓ Settings Test Upload
Transmission Parame	ters:		
Encryption Certifica	ate: <no en<="" td=""><td>ncryption></td><td>¥</td></no>	ncryption>	¥
Signing Keyring:	<no sig<="" td=""><td>gning></td><td>~</td></no>	gning>	~
Save the log file as	: Ogzip	o file () text file	
	after: E	seconds	
Send partial buffer	anter. 5		

- 2. From the Client type drop-down list, select **Custom Client**.
- 3. Click the **Settings** button. The Custom Client settings page opens.

ustom Client settings: Log StealthWatch	
Custom server connection:	
Settings for: Primary Custom Server	
Host IP: .10.204 Port: 514	
Use secure connections (SSL)	
OK Cancel	

4. In the appropriate fields, type the IP address of the Flow Collector and listening port of the proxy parser.



5. Click OK.

Transmission Parameters:		
Encryption Certificate:	<no encryption=""></no>	~
Signing Keyring:	<no signing=""></no>	~
Save the log file as:	⊖ gzip file ● text file	
Send partial buffer after:	5 seconds	
Bandwidth Class:	<none></none>	~

- 6. For the Transmission Parameters, complete these steps:
 - a. For the Encryption Certificate, select No encryption.
 - b. From the Signing Keyring drop-down list, select no signing.
 - c. From "Save the log file as" select the Text file option.
 - d. In the "Send partial buffer after" text box, type 5.
 - e. Click the **Upload Schedule** tab, and select the continuously option for the Upload the access log.
 - f. In the Wait between connect attempts field, type 60.
 - g. In the Time between keep-alive log packets field, type 5.

7. Click the **Apply** button at the bottom of the page. Continue to the next section, **Configuring the Upload Schedule**.

Configuring the Upload Schedule

To configure the upload schedule, complete the following steps:

1. Click the **Upload Schedule** tab.

Logs General Settings	Upload Client Upload Schedule	1
	Log: StealthWatch	
Г Upload type: —————		4
Upload the access log		4
\odot continuously \odot periodically		1
Wait between connect attempts:	60 seconds	
Time between keep-alive log packets:	5 seconds	
	ىسى مەربىيىنى بىيى يەرىمىدىن بىرى بىيى بىيى بىيى بىيى بىيى بىيى بىيى	

- 2. For the "Upload the access log," select **continuously**.
- 3. Wait between correct attempts is 60 seconds.
- 4. Time between keep-alive log packet **5** seconds.
- 5. Click the **Apply** button at the bottom of the page.

This completes the configuration for the Blue Coat proxy logs for the Flow Collector.

Notes

Further notes on configuration:

- The Flow Collector and Proxy must be on the same NTP server or receive time from a common source for flow and proxy records to be matched.
- Only one log output mechanism for the proxy is supported. If you are already exporting logs for some particular reason we will not be able to capture and parse proxy records.
- UDP is not supported.

Configuration of the Visual Policy Manager

Configuration of the Visual Policy Manager enables you to check that the proxy log is being sent to the Flow Collector.



1. In the Configuration tab page in the main menu, click **Policy > Visual Policy Manager**. The Visual Policy Manager opens.



2. Click the Launch button at the bottom for your configured log. The Visual Policy Manager for the log window opens.



3. Click **Policy > Add Web Access Layer**. The Add New layer screen opens.

Add New Layer		×
Layer Name:		
Web Access Layer (1)		
ОК	Cancel	
	N	

4. Type a name for the new layer, and then click **OK**.



5. Right-click **Deny** in the Action column and then click **Set**. The Set Action Object dialog opens.

🔅 Set Action Object 🛛 🔀
Existing Action Objects
Show: All (sort by object-name)
AccessLog1
🕗 Allow
🚰 Always Verify
Block IM Message Encryption
Block Popup Ads
🖀 Bypass Cache
🚰 Check Authorization
S Deny
🖉 Deny (Content Filter)
Enicable East, Cachina in Windows Madia Class
New 😓 Remove Edit
OK Cancel Help

6. Click **New** and select **Modify Access Logging**. The Edit Access Logging Object dialog opens.

🕃 Edit Acc	ess Logging Object		X
Name:	btealthWatch_Log	gging]
O Disable	all access logging:		
C Reset t	o default access loggir	ng	
Enable	logging to:	StealthWatch	Y
O Disable	logging to	StealthWatch	v
	ОК	Cancel	Help

- 7. Click Enable logging to.
- 8. Type a name for your log and then select your log.
- 9. Click **OK**. The object is added.
- 10. In the Set Action Object dialog, click **OK**.

File Edit Policy Co	nfiguration View Help			
Add rule	Delete rule(s)	🛧 Move up	Moverau	🔁 Install policy
Worth the man war				

- 11. Click the **Install policy** button at the top right.
- 12. Click **No** and then **OK** for the following windows.

Statistics Configu	ration Maintenance	
Summary Traffic Details Application Details	1 Log Size Upload Status 2 Log: Sized/Watch	
Bandwidth Mgmt.		

13. Launch the Blue Coat Visual Policy Manager again.

🗱 В	lue Co	at Visu	al Po	olicy Mana	ager (.10.2	24 - Blue	Coat S	G210
File	Edit	Policy	Соп	figuration	View	Help				1
	o Ac	dd rule		T Dele	ete ruk	e(s)		🛧 Move	e up	
Stea	lthWa	tch Lorr	ina İ	able Laurer		1				
No		5	En	able Layer		tination	٦		Service	
	1 Any		Re	name Laye	r			Any		1
			De	lete Layer						
			Ad	d Layer Gu	ard					
	~~~~		~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	-					ĺ

- 14. Right-click the logging tab and then select **Enable Layer**.
- 15. Click the Install Policy button. The Policy Installed opens.
- 16. Click **OK.**



17. Click the **Statistics** tab, and in the log menu, select your log.



18. In the main menu, click **Access Logging**, and then click the Log Tail tab. The Log Tail window opens.

Log Tail Log Size Upload Status	
Log: StealthWa	tch 🔻
,	-
1458669295.851 0 .10.118 424	63 66.235.139.205 80 192.168.10.24 80 730 508 - shutterfly.112.207.net http:/
1458669295.861 0 .10.110 651	22 23.195.245.198 80 192.168.10.24 80 149 345 - go.microsoft.com http://go.mi
1458669295.916 0 .10.118 424	63 66.235.139.205 80 192.168.10.24 80 817 507 - shutterfly.112.207.net http:/
1458669300.396 0 .10.110 651	23 184.51.126.75 80 192.168.10.24 80 264 450 - crl.microsoft.com http://crl.m
1458669300.892 0 10.10.110 651	22 23.195.245.198 80 192.168.10.24 80 149 344 - go.microsoft.com http://go.mi
1458669305.022 0 .10.110 651	23 184.51.126.75 80 192.168.10.24 80 278 448 - crl.microsoft.com http://crl.m ⁻¹
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	allow the assessment a second consistence on a statement of the second and the second second assessment of the second

- 19. Click **Start Tail** button at the bottom of the page.
- 20. On the Statistics main menu, click **System > Event Logging**. This page will show if the log file is uploaded to the Flow Collector and the changes made. It shows whether the proxy is connected to the Flow Collector.

Statistics Configu	ration Maintenance		Health: 0
Summary	Event log: END OF LOG		
Traffic Details			
Application Details	2015-09-17 13:56:23-04:00EDT	"Access Log Custom (StealthWatch): Couldn't connect to server" 6F E000A:1 alog_stream_custom.cp	p:317
ADN History	2015-09-17 13:56:23-04:00EDT	"Access Log (StealthWatch): Unable to connect to remote server for log uploading" 0 E0008:1 alo	g_facility_i
Bandwidth Mgmt.	2015-09-17 13:57:23-04:00EDT	"Access Log (StealthWatch): Unable to connect to remote server for log uploading" 0 E0008:1 alo	g_facility_i
ProxyClient	2015-09-17 13:58:19-04:00EDT	"Config admin at 10.89 'admin', access log custom client primary IP address set to "192.16	8.10.204:851
Network	2015-09-17 13:58:23-04:00EDT	"Access Log Custom (StealthWatch): Connecting to primary server 10.204:8514." 0 E0000:96	alog_strea
ICAP	2015-09-17 14:00:03-04:00EDT	"Snapshot sysinfo_stats has fetched /sysinfo-stats" 0 2C0006:96 snapshot_worker.cpp:236	_ 1
Protocol details	2015-09-17 14:15:03-04:00EDT	"NTP: Periodic query of server .10.10, system clock is 0 seconds 367 ms slow compared to NT	P time. Upde
System	2015-09-17 14:25:47-04:00EDT	"Config admin at .10.89 'admin', installed new VPM Policy File and VPM XML File" 0 140002:	7D cli_pas
Resources	2015-09-17 14:28:21-04:00EDT	"Config admin at10.89 'admin', installed new VPM Policy File and VPM XML File" 0 140002:	7D cli_par
Contents	2015-09-17 14:33:14-04:00EDT	"Access Log (Stealthwatch2): Configure upload site for uploads to work" O E0006:7D alog facilit	y impl.cpp:3
Event Logging	2015-09-17 14:33:14-04:00EDT	"Access Log (Stealthwatch2): New Log Manager Object created. Max log size is 20000NB, upload thre	shold is 160
Failover	2015-09-17 14:33:14-04:00EDT	"Access Log (Stealthwatch2) has been initialized." 0 E0000:96 alog facility impl.cpp:269	
man man and and and and and and and and and a	20+5-02-17 14-33-00-04:00507-	-"Config-admin_at_19>-168-40-06-Ledwiniu prosted a new lost"Stoelthratch?""	C. (MAN 42.63

21. Continue to the <u>Configuring the Flow Collector</u> chapter to set up your Flow Collector to receive syslog information.

Configuring the McAfee Proxy Logs

This chapter describes the procedure for configuring the McAfee proxy logs from the McAfee Web Gateway to deliver to Secure Network Analytics.

- Make sure that you have downloaded the XML configuration file for the McAfee proxy. Go to Cisco Software Central to download the readme and Proxy Log XML configuration files.
- Log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator.
 - The McAfee proxy version used for testing was 7.4.2.6.0 18721.

To set up the McAfee proxy log, complete the following steps:

1. Download the XML file, FlowCollector_[date]_McAfee_Log_XML_Config_[v].xml, and then save it to your preferred location.

"Date" indicates the date of the XML file, and "v" indicates the version of the
McAfee proxy version. Be sure to select the XML file with the same version number as your McAfee proxy.

Follow these steps to acquire it:

- a. Go to https://software.cisco.com, Cisco Software Central.
- b. In the Download and manage > Download and Upgrade section, select Access downloads.
- c. Scroll down to the select a **Product field**.
- d. Type Secure Network Analytics in the Select a Product field. Press Enter.
- e. Select **Secure Network Analytics Virtual Flow Collector** or another Flow Collector.
- f. Select Secure Network Analytics System Software > Configuration Files.
- 2. Log in to the McAfee proxy server.



3. Click the Policy icon, and then click the **Rule Sets** tab.



4. Select Log Handler, and then select Default.



5. Click Add > Rule Set from the Library.



- 6. Click Import from file, and then select the XML file.
- 7. Select mcafeelancopelog in the log handler that was just imported.

Make sure the rule set and the rule "create access logline" and "send to syslog" is enabled.

- 8. Click the Configuration icon at the top of the page.
- 9. At the left of the page, click the **File Editor** tab, and then select the rsyslog.conf file.

Appliances	File Editor
Files	
🖃 🖆 mcafee	
host	s
mwg	
ospf	6d.conf
ospf	d.conf
reso	lv.conf
mipd.	conf
···· 📄 ripng	d.conf
rsys	log.conf
snmp	od.conf
Sock	d.conf
📑 sshd	config
sysc	tl.conf
zebr	a.conf

10. At the bottom of the text box (beside the list of files), type the following text:

daemon.info @[FlowCollector IP Address:514]



Make sure to select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.

- 11. Comment out this line: *.info; mail.none; authpriv.none; cron.none.
- 12. Add this line:

*.info;daemon.!=info;mail.none;authpriv.none;cron.none /var/log/messages.

13. Click the **Save Changes** button at the top right of the page.

14. Continue to the <u>Configuring the Flow Collector</u> chapter to set up your Flow Collector to receive syslog information.

Configuring the Cisco Web Security Appliance (WSA) Proxy Logs

This chapter describes the procedure for configuring the Cisco proxy logs to deliver to Secure Network Analytics.

Cisco WSA proxy does not support Virtual IPs for adding the proxy device.

To set up the Cisco proxy log, complete the following steps:



1. Log in to the Cisco proxy server.

A	Reporting	Web Security Manager	Security Services	Network	System Administration	
					Policy Trace	
					Alerts	
					Log Subscriptions	
					Return Addresses	

2. On the main menu, click **System Administration > Log Subscriptions**. The Log Subscriptions page opens.

Log Subsc	riptions	
Configured Log Add Log Subsc	Subscriptions	
Log Name	Туре	Log Files
access-w3c	W3C Logs	Syslog Push - Host 10.205.14.30

3. Click the Add Log Subscriptions button. The New Log Subscriptions page opens.

Log Type:	Select a log type	•
	Feedback Logs	*
	FIPS Logs	j
	FTP Server Logs	
	GUI Logs	
	Haystack Logs	-
	Logging Logs	
	NTP Logs	
	OCSP Logs	
	PAC File Hosting Daemon Logs	i
	Reporting Logs	
	Reporting Query Logs	
	SaaS Auth Logs	
	SHD Logs	
	SNMP Logs	
	Status Logs	
	System Logs	
	UDS Logs	
	Updater Logs	
	W3C Logs	
	Welcome Page Acknowledgement Logs	Ť

4. From the Log Type drop-down list, select W3C Logs. The available W3C Log fields appear.

Subscriptio		
Log Type:	W3C Logs	
Log Name:	(will be used to name the log directory)	
Log Fields:	Available Log Fields CMF CMF CMF Science Control Coport Co	

- 5. In the Log Name field, type a name for the log that you will use.
- 6. From the Available Log Fields list, select **Timestamp**, and then click **Add** to move it the Select Log Fields list.



- 7. Repeat the previous step for the each of the following log fields in order:
 - a. timestamp
 - b. x-elapsed-time
 - c. c-ip
 - d. c-port
 - e. cs-bytes
 - f. s-ip
 - g. s-port
 - h. sc-bytes
 - i. cs-usernames
 - j. s-computerName
 - k. cs-url

The Selected Log Fields list should contain these fields as illustrated:



The Selected Log Fields list must be in the order above, with no other fields present.

8. Scroll to the bottom of the page, and then select the **Syslog Push** option.

Syslog Push	
Hostname:	.22.12
Protocol:	● UDP □ TCP
Facility:	user T
	Submit

9. In the Hostname field, type the Flow Collector IP address or its host name that the proxy sends logs to.

Make sure to select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.

- 10. Click **Submit**. The new log is added to the Log Subscription list.
- 11. Continue to the **Configuring the Flow Collector** chapter to set up your Flow Collector to receive syslog information.

Configuring Squid Proxy Logs

This chapter describes the procedure for configuring the Squid proxy logs to deliver to Secure Network Analytics. To configure the logs requires using SSH to edit files on the proxy server.

To configure the Squid proxy logs, complete the following steps:

- 1. Log into a shell for the machine running Squid
- 2. Go to the directory containing squid.conf (typically /etc/squid) and open it in an editor.
- 3. Add the following lines to squid.conf to configure logging:

```
logformat access_format %ts%03tu %<tt %>a %>p %>st %<A %<st %<la
%<lp %la %lp %un %ru
access log syslog:user.6 access format</pre>
```

4. Restart squid using the following:

/etc/init.d/squid3 restart

 Configure the syslog service on the Squid server to forward logs to the Flow Collector. This is dependent on the Linux distribution, but for syslog-ng you would add the following to /etc/syslog-ng:

```
# Audit Log Facility BEGIN
filter bs_filter { filter(f_user) and level(info) };
destination udp_proxy { udp("10.205.14.15" port(514)); };
log {
source(s_all);
filter(bs_filter);
destination(udp_proxy);
};
# Audit Log Facility END
```

Make sure to select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.

- 6. Then restart syslog-ng with /etc/init.d/syslog-ng restart.
- 7. Continue to the <u>Configuring the Flow Collector</u> to receive syslog information.

Configuring the Flow Collector

After you have configured the proxy server, you need to configure the Flow Collector to accept the data.

To configure the Flow Collector to receive syslog information, complete the following steps:

- 1. Log in to your Manager.
- 2. Select Configure > GLOBAL Central Management.
- 3. Click the *** (Ellipsis) icon for your Flow Collector, then click View Appliance Statistics. The Flow Collector interface opens.
- 4. Click **Configuration > Proxy Ingest**. The Proxy Servers page opens.
- 5. Type the IP address of proxy server.
- 6. From the Proxy Type drop-down list, select your proxy server.

If your type of proxy server is not listed, you will not be able to use proxy logs at this time.

- 7. In the Proxy ID field, type the IP address of the proxy server.
- 8. In the Proxy Service Port field, type the port number of the proxy server.
- 9. If you want the proxy server to trigger alarms, clear the Exclude from Alarming check box.
- 10. Click Add.
- 11. Click **Apply**. The proxy server appears in the Proxy Ingest table at the top of the page.
- 12. Continue to the next chapter, **Checking the Flows**.

Checking the Flows

To check that you are receiving the flows, complete the following steps:

J	Support 🛛	h.
	 Advanced Settings 	L
	 Database Storage Statistics 	L
	 Backup/Restore Database 	L
	- Browse Files	L
	 Packet Capture 	L
	- Update	

 In the Flow Collector interface, click Support > Browse Files in the main menu. The Browse Files page opens.

-flo	ow-proxyparser/logs					
ani.	t Directory	_				
	Name 🌢	Size	• 1	ast Modified	٥	

2. Open the syslog file.

FlowCollector for NetFlow VE > https://gprocessor.log K +		
A https://	rocessor.log 🖾 🔻 🦉 🤉 Search	
📙 Lancope 🔒 Documentation 🔚 CC-KB 🍰 Demo Servers 🦲 Sandbox	Servers 🔒 Videos 逼 Cisco 🔒 Partners 🔒 Training 🔒 Trial Res Ӹ Tools Ӹ Sales Ы Security Info	
<pre>0015-00-11 17:02:11.062 INTO main con.lancope.wew.syslogprocess.Configuration = Syslog Processor configuration: 0015-00-12 17:02:11.064 INTO main con.lancope.wew.syslogprocess.Configuration = Sorigd Structory: /lancope/var/ww-flow-proxyparser/templates 0015-00-12 17:02:11.064 INTO main con.lancope.wew.syslogprocess.Configuration = Log directory: /lancope/var/ww-flow-proxyparser/templates 0015-00-12 17:02:11.064 INTO main con.lancope.wew.syslogprocess.Configuration = Log level: INTO 0015-00-12 17:02:11.064 INTO main con.lancope.wew.syslogprocess.Configuration = Log level: INTO 0015-00-12 17:02:11.064 INTO main con.lancope.wew.syslogprocess.Configuration = Log level: INTO 0015-00-12 17:02:11.064 INTO main con.lancope.wew.syslogprocess.Configuration = New start is the 0015-00-12 17:02:11.064 INTO main con.lancope.wew.syslogprocess.Configuration = New start is the 0015-00-12 17:02:11.065 INTO main con.lancope.wew.syslogprocess.Configuration = New start to log: 40 0015-00-12 17:02:11.065 INTO main con.lancope.wew.syslogprocess.Configuration = Set issuell 0015-00-12 17:02:11.065 INTO main con.lancope.wew.syslogprocess.Configuration = Histering 0015-00-12 17:02:11.065 INTO main con.lancope.wew.syslogprocess.Configuration = Histering 0015-00-12 17:02:11.065 INTO main con.lancope.wew.syslogprocess.Configuration = Histering 0015-00-12 17:02:11.067 INTO main con.lancope.wew.syslogprocess.Configuration = Histering 0015-00-12 17:02:11.067 INTO main con.lancope.wew.syslogprocess.Configuration = Histering 0015-00-12 17:02:11.067 INTO main con.lancope.wew.syslogprocess.C</pre>		

- 3. Check that the marked files are not blank. If there are then, there is an issue.
 - Listeners has the number of the proxies.
 - Handlers is only one that parses out the data.
 - Emitters take parsed data from the handler and convert it into a format the engine

is looking for.

• Firewall

2015-11-11 16:34:26,754 2070 muin com.lancepe.ows.syslogracess.Configuration - Syslog Processor configuration:	
2015-11-11 16:34:36,354 39F0 main conlancepe.exe.syslogprocess.Configuration - Script directory: /lancepe/var/sx-flow-proxyparser/tem	plates
2015-11-11 16:34:20,354 2070 main com.lancepe.sws.syslogprocess.Configuration - Log directory: /lancepe/var/sw-fiew-promyparser/logs	
2015-11-11 16:34:26,354 20FC main com.lancepe.sws.syslogprocess.Configuration - Log to console: false	
1015-11-11 16:34:10,354 DMPO main com.lancope.ows.syslogprocess.com/Eguration - Log level: 1990	
2015-11-11 16:34:26,355 JW/O main com. lancepe.sws.syslogsrocess.Configuration - Metrics to console: 0	
2015-11-11 16:34:26,355 TMPO muin com. lancape.sws.syslagprocess.configuration - Metrics to log: 60	The C is the count. These
2015-11-11 16:34:26,355 20FO main com.lancope.sws.syslogprocess.Configuration - Run as duemon: false	
1985-11-11 16:34:36,355 1990 main com.lancope.sws.syslogprocess.Configuration - Pid file location: not specified	should go up when logs
2015-11-11 16:34:20,355 20FC main com.lancope.sws.syslagsrocess.Configuration - Set firewall rules: true	entenne ge op miterrege
2015-11-11 16:34:26,355 20FO main com.lancope.ows.syslagsrocess.configuration - Core control:	aoina through
2015-11-11 16:34:20,355 10/0 main com.lancepe.sws.syslogprocess.Configuration - Listemers:	going an ough.
2013-11-11 16:34:20,355 JMPD main com.lancepe.sws.syslogprocess.Configuration - 0: syslog: port-0514	2
2015-11-11 16:34:26,355 IMPO main com.lancope.sws.syslagprocess.Configuration - Mandlers:	
2015-11-11 16:34:26,355 JMPO main com.lancope.sws.syslogprocess.Configuration - 0: proxy: sourceip-10.205.14.14 emitter-proxylengine	
2015-11-11 16:34:20,355 JMPC main com.lancepe.sws.syslagprocess.Configuration - Emilters:	
2015-11-11 16:34:26,355 18FO main com.lancepe.ows.syslogsrocess.Configuration - 0: pb/2mg/proxylongine:	
1015-11-11 16:34:16,355 DMPO main com.lancope.sws.syslogprocess.Configuration - Firewall:	
2013-11-11 16:34:20,355 DMPD main com.lancope.sws.syslogprocess.Comfiguration - 0: MEDDMECT: iface-eth+ protocol-wdp destport=0514 sr	(pert-S)
2015-11-11 16:34:20,356 2070 main com.lancepe.sws.syslagprocess.Configuration - 1: 20: port=014 protocol=udp asporter=true (p=10.205	.34.34
2015-11-11 16:34:26,357 1990 main com.lancope.sws.syslogprocess.ParserFactory - Setting up parser table	
2015-11-11 16:34:26,429 DMPD muin com.lancope.sws.syslogprocess.Metrics - Enabling periodic metrics log	
2015-11-11 16:34:20,580 DMPC main com.lancope.server.firewall.firewall&uleOACDmpl - writing /Lancope/var/admin/plugins/firewall/8514-5	151.06
1015-11-11 16:34:17,751 1970 main com.lancope.sws.syslagprocess.cores.bisruptoriore - Core configuration started	
2015-11-11 16:34:27,753 DMO main com lancepe sws.syslogprocess.cores.Disruptoriore - Core configuration: Lingle producer, Blacking wa	it st ney, 1 worker
2013-11-11 16:34:27,881 20PO main com.lancepe.sws.syslagprocess.lyslagProcessor - Starting metrics lag jub	
2015-11-11 16:34:17,404 1970 pool-2-thread-1 com.lancope.swn.syslagprocess.Metrics - Listeners: ci0 rate1:.0 rate1:.0 rate1:.0 rate1:.0	· // 2
2015-11-11 16:34:27,005 DMPD pool-2-thread-2 com lancepe.sws.syslogprocess.cores.DEsruptorCore - Starting thread 11 for listener sysle	c(#534)
2015-11-11 16:34:27,886 2M/D pool-2-thread-1 com.lancope.sws.syslagprocess.Metrics - Handlers: ci0 mini.0 maxi.0 meani.0	2
2015-11-11 16:34:27,006 DMPD pool-2-thread-1 com.lancope.ows.syslogprocess.Netrics - Smitters: c:0	. 1
2015-11-11 16:35:27,007 DM/D pool-2-thread-1 com.lancope.sws.syslagprocess.Metrics - Listeners: c:0 rate1.0 rate1.0 rate5.0 rate15	· /
2015-11-11 16:05:27,887 DMPD pool-2-thread-1 com lancape.sws.syslagsrocess.metrics - ManGersi ci0 mini.0 maxi.0 meani.0	
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

4. Check that the count is counting upwards to show that you are receiving data.

# **Contacting Support**

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

# Change History

Document Version	Published Date	Description
1_0	March 2, 2023	Initial Version.
1_1	December 20, 2023	Updated a step in the Configuring the Flow Collector section.

# **Copyright Information**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <u>https://www.cisco.com/go/trademarks</u>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)