NetWitness® Platform

Cisco Firepower System Event Streamer (eStreamer) Event Source Log Configuration Guide

NETWITNESS
Platform

Cisco Firepower System Event Streamer (eStreamer)

Event Source Product Information:

Vendor: Cisco

Event Source: FirePower System Event Streamer

Versions: 6.x, 7.x

NetWitness Product Information:

Supported On: NetWitness Suite 12.3 and later

Event Source Log Parser: cef

Collection Method: Syslog

Event Source Class.Subclass: Security.Access Control

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

February, 2024

Contents

To configure the Cisco FirePower System Event Streamer, you must:

I. Configure eStreamer on Cisco FirePower System Event Streamer

II. Configure RSA NetWitness Suite for Syslog Collection

Configure eStreamer on Cisco FirePower

The Firepower System Event Streamer (eStreamer) eNcore CLI client uses a message-oriented protocol to stream events and host profile information to your client application from eStreamer server (Cisco FMC). Your client can request event and host profile data from a Management Center, and intrusion event data only from a managed device. Your client application initiates the data stream by submitting request messages, which specify the data to besent, and then controls the message flow from the Management Center or managed device after streaming begins. Please follow the official document provided by cisco to configure the eStreamer
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215631-understand-estreamer-and-troubleshoot-en.html

Note: It is recommended that we should not run the external cisco python or shell script inside Netwitness components like logcollector or logdecoder. Please run those scripts inside a seperate VM/server from customer environment.

Note: service port should be 514 and use the logcollector/logdecoder IP to send events from eStreamer to Netwitness. Please select adaptor in estreamer.conf as cef .

Configure RSA NetWitness Suite

Perform the following steps in RSA NetWitness Suite:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is **cef**.

Configuring Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

To configure the Log Decoder for Syslog collection:

1. In the NetWitness menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose View > System.
3. Depending on the icon you see, do one of the following

- If you see 

, click the icon to start capturing Syslog.
- If you see 

, this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu. The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +. The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar. The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. You can continue to add Syslog event sources to your system without any further configuration in Netwitness.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.