NetWitness® Platform

Akamai Kona Event Source Configuration Guide

NETWITNESS
Platform

Akamai Kona

Last Modified: Monday, December 2, 2024

Event Source Product Information:

Vendor: Akamai

Event Source: Akamai Kona

Versions: 1.0

NetWitness Product Information:

Supported On: NetWitness 12.2 and later

Event Source Log Parser: cef

Note: The CEF parser parses this event source as **device.type=akamaikona**

Collection Method: Syslog

Event Source Class.Subclass: Security.Application Firewall

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

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

November 2024

Contents

To configure the Akamai Kona event source, you must:

I. Configure Syslog Output on Akamai Kona CEF Connector

II. Configure [[[Undefined variable SAVariables.ProductSuiteName]]] for Syslog Collection

Configure Syslog Output Akamai Kona CEF Connector

The Akamai Managed Kona Site Defender Service is a managed security service designed to help build a responsive cloud security strategy. It leverages the expertise and infrastructure provided by Akamai's Security Operations Center to help customers maintain attack readiness, get security monitoring and attack support, and receive ongoing security reporting.

Hardware and Software Requirements

The following are the software and hardware requirements for running the CEF connector:

- Sun JRE 1.8+
- 2 CPU cores
- 6 GB RAM
- 2 GB Free Disk Space
- Run a Linux Kernel greater than 2.6

Configuration Procedure

Perform the following steps to configure the Akamai Kona CEF connector.

1. Visit https://developer.akamai.com/tools/siem-integration to get the latest CEFConnector distribution package.
2. Download and unzip he distribution package anywhere on the file system.
3. Install CEF Connector as a service, by creating symbolic link to the **bin/AkamaiCEFConnector.sh** shell script in `/etc/init.d`.

   The shell script accepts the following commands:

   - start
   - stop
   - status
   - resetdb

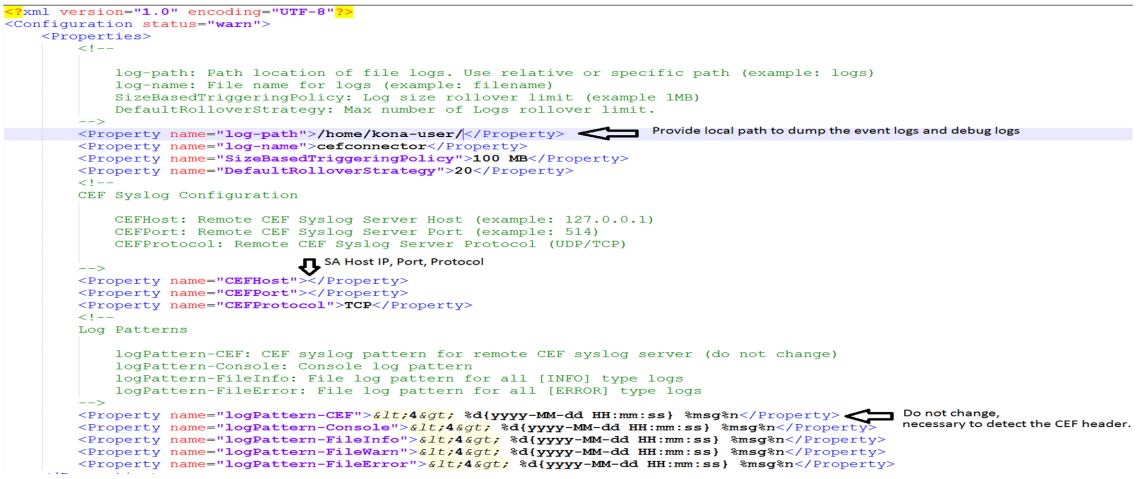
   Note: Resetdb deletes **cefconnector.db**, which contains the last successful offset data pull. Removing the file causes the connector to process **offset=NULL** as long as **timebased** setting is false. If **timebased** is true, a new offset is saved after the first successful pull.

4. Configure the `config/CEFConnector.properties` file with the user specific parameters provided by Akamai. For details, see CEF Connector Properties.

5. Configure the `config/log4j2.xml` file to provide the RSA NetWitness Logs and Packets Host IP, Port, and Protocol properties in the CEF Syslog Configuration Section.

   Log Pattern for CEF should be provided in the following format:

   `<PARITY_NUM> %d{yyyy-MM-dd HH:mm:ss} %msg%n`



> **Note:** Logs can be collected on the local machine if the **log-path** is provided with the **log-name** (Optional). Log patterns (Console log, File Information, File Warning, and File Error) are optional, but might prove useful.

6. Start the CEF Connector service, using the shell script.

Once you start the service, logs are collected in the Common Event Format (CEF).

CEF Connector Properties

The following table describes the available settings in the `config/CEFConnector.properties` file.

Name	Description
Connector.refresh.period *	The rate that the connector will pull from the SIEM API in seconds. Default Value is **60**. Set this parameter to a positive integer value. Any other value will be ignored (default value will be used).
Akamai.data.requesturlhost *	Request URL for API. This value cannot be blank or commented out.
akamai.data.configs *	Security configuration IDs, separated with commas (,). This parameter cannot be black or commented out.
akamai.data.timebased *	Boolean value for using an offset token. • Set to **true** to pull data from a specific time • Set to **false** to use an offset token

Name	Description
akamai.data.timebased.from	If **timebased** is true, the **from** field in epoch format will be used as the beginning timestamp to pull security events. This field will be ignored if the **timebased** is false.
akamai.data.timebased.to	If **timebased** is true, the **to** field in epoch format will be used as the end timestamp to pull security events. If no value or invalid format is provided, default value will be used. This field will be ignored if the **timebased** is false.
akamai.data.limit	Limits the number of events to pull. If no value is provided or an invalid value is provided, the default limit on the API side will be used. Default value is 200000. Set this parameter to a positive integer value. Any other value will be ignored (default value will be used).
akamai.data.accesstoken *	OPEN API credentials need to be provisioned by the customer in Akamai LUNA portal and to be configured by the SIEM administrator.
akamai.data.clienttoken *	OPEN API credentials need to be provisioned by the customer in Akamai LUNA portal and to be configured by the SIEM administrator.
akamai.data.clientsecret *	OPEN API credentials need to be provisioned by the customer in Akamai LUNA portal and to be configured by the SIEM administrator.
akamai.data.baseurl *	OPEN API credentials need to be provisioned by the customer in Akamai LUNA portal and to be configured by the SIEM administrator.
akamai.cefformatheader *	CEF Header Values are separated by "|". If "|" is part of a static string, then it must be escaped with "\\". Values can be static or generated from available functions: **requestURL()**, **eventClassId()**, **name()**, **severity()**, **appliedAction ()**,**ipv6src()**. There need to be 7 values, separated by "|" and starting with **CEF:**
akamai.cefformatextension *	CEF Extension Values are separated by a space. Values can be any of the following: • static • generated from available functions (**eventClassId()**, **name()**, **severity()**, **appliedAction()**,**ipv6src()**), or • pulled from JSON API. JSON API is defined by **${}** and each JSON object is separate by a period (.). Static Values are defined by quotation marks. Function generated values are defined by **()** and must be one of the available functions defined in documentation. Each space-separated value needs to be a pair.
akamai.base64fields	If an API JSON object is base64 encoded, it must be defined here.
akamai.urlencoded	If an API JSON object is URL-encoded, it must be defined here.

Name	Description
akamai.multivaluedelim	Delimiter used to separate multi-valued CEF fields. Default value is a comma (,). Specifying **" "** (a space) is treated the same as "" (empty string) and the default value is used.
connector.consumer.count	Limits the number of consumer threads. Default value is 3.

Access the SIEM API

To access the SIEM API from behind a proxy server, ensure that your proxy:

- Whitelists the domains ***.cloudsecurity.akamaiapis.net**
- Does not interfere with HTTP request headers for those domains. If, due to a strict enterprise security policy, your proxy does change these headers, make sure that at a minimum you allow and do not change the Host and Authorization headers.

Configure RSA NetWitness Platform

Perform the following steps in [[[Undefined variable SAVariables.ProductSuiteName]]]:

- 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 Platform Live.

Ensure that the parser for your event source is available:

1. In the **NetWitness** menu, select (Admin) > **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**.

Configure 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. You only need to configure either the Log Decoder or the Remote Log Collector for Syslog, not both.

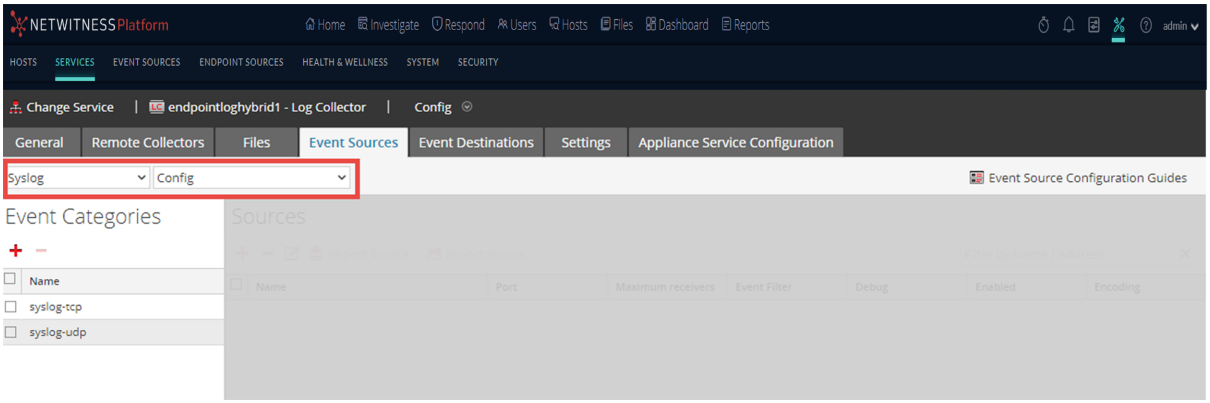
To configure Log Decoder for Syslog Collection

1. In the NetWitness Platform menu, select (Admin) > **Services**.
2. In the **Services** grid, choose 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 Start Capture , click the icon to start capturing Syslog.
   - If you see Stop Capture , you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure Remote Log Collector for Syslog Collection

1. In the NetWitness Platform menu, go to (Admin) > **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.

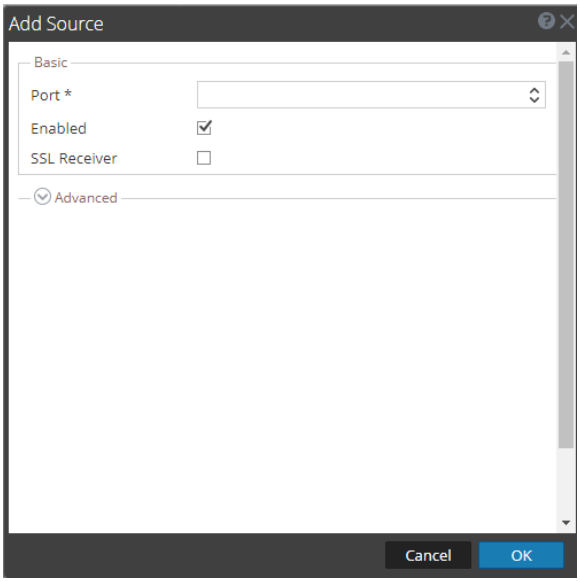


4. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog will appear.

5. Choose either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Choose the **New Type** in the **Event Categories** panel and click + in the **Sources** panel toolbar.

   The **Add Source** dialog will appear.



7. Enter **514** for the port and choose **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

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

After 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 a need to do any further configuration in NetWitness Platform.

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.