NetWitness® Platform

Imperva SecureSphere Event Source Log Configuration Guide

NETWITNESS
Platform

Imperva SecureSphere

Last Modified: Monday, May 27, 2024

Event Source Product Information:

Vendor: Imperva

Event Source: SecureSphere

Versions: 6, 7, 8, 8.5, 9, 9.5, 10, 14.12.1.10

Additional Downloads: Impervawaf.txt

RSA Product Information:

Supported On: NetWitness Platform 12.0 and later

Event Source Log Parser: impervawaf

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/.

February, 2024

Contents

Configure Imperva SecureSphere

To configure Syslog collection for Imperva SecureSphere you must:

- Configure NetWitness Platform for Syslog Collection
- Configure Syslog Output on Imperva SecureSphere

Configure NetWitness Platform for 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.

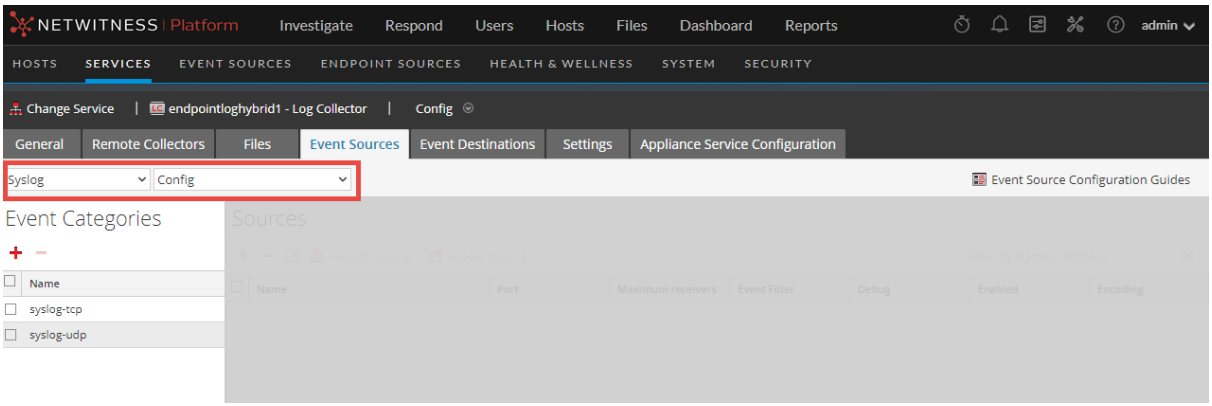
To configure Log Decoder for Syslog Collection

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.

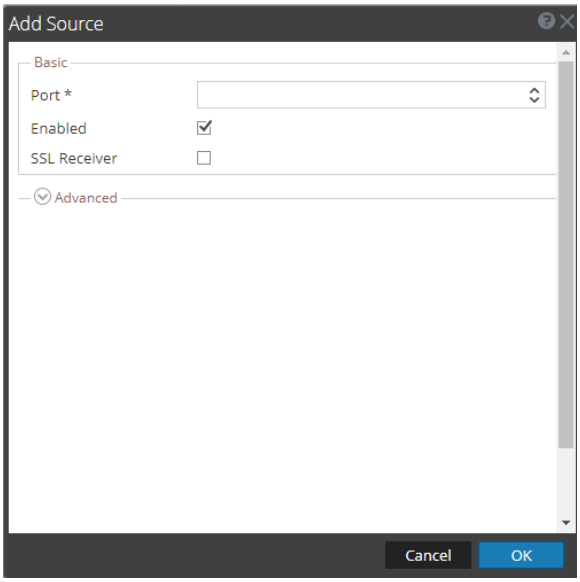


4. In the **Event Categories** panel toolbar, click +.

   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.

Configure Syslog Output on Imperva SecureSphere

These instructions describe how to configure Imperva SecureSphere to communicate with the RSA NetWitness Platform.

To configure Imperva SecureSphere:

1. Connect to the SecureSphere web interface.
2. Select the **Policies** > **Action Sets** tab.
3. To set up Alerts monitoring, follow these steps:
   a. Select **Create New**  .

   Note: In version 10.0, select **Create New**  .

   b. In the **Name** field, type `Security Platform Alerts`.
   c. From the **Apply to event type** drop-down list, select **Any Event Type**.
   d. Click **Create**.
   e. Select the action set, **Security Platform Alerts**.
   f. Move the **Server System Log** > **Log to System Log (syslog)** action from **Available Action Interfaces** to **Selected Actions** by clicking the green arrow next to the action.
   g. Expand **Selected Actions**, and complete the fields as follows.

Field	Action
Name	Type: `Security Platform Alerts`.
Syslog Host	Enter the IP address of the NetWitness Log Decoder or Remote Log Collector.
Syslog Host Level	Type: `Info`.
Message	Copy and paste text from the **impervawaf.txt** file. Use the line below **Security Alerts**. This file is available on the NetWitness Community as an Additional Download here: impervawaf.txt
Facility	Type: `Syslog`.

   h. Select **Run on Every Event**.
   i. Click **Save**.
4. To set up Events, follow these steps:

a. Select **Create New**  .

Note: In version 10.0, select **Create New** 

b. In the **Name** field, type: `Security Platform Events`.

c. From the **Apply to event type** drop-down list, select **System Events**.

d. Click **Create**.

e. Select the action set, **Security Platform Events**.

f. Move the **Server System Log** > **Log to System Log (syslog)** action from **Available Action Interfaces** to **Selected Actions** by clicking the green arrow next to the action.

g. Expand **Selected Actions**, and complete the fields as follows.

Field	Value
Name	Type: `Security Platform Events`.
Syslog Host	Enter the IP address of the NetWitness Log Decoder or Remote Log Collector.
Syslog Host Level	Type: `Info`.
Message	Copy and paste text from the **impervawaf.txt** file. Use the line below **Security Events**. This file is available on the NetWitness Community as an Additional Download here: impervawaf.txt
Facility	Type: `Syslog`.

h. Select **Run on Event**.

i. Click **Save**.

5. To set up Database Activity Monitoring, follow these steps:

a. Select **Create New**  .

Note: In version 10.0, select **Create New** 

b. In the **Name** field, type: `Security Database Activity Monitoring`

c. From the **Apply to event type** drop-down list, select **Audit**.

d. Click **Create**.

e. Select the action set, **Security Database Activity Monitoring**.

f. Move the **Gateway Syslog** > **Log audit events to System Log (Gateway syslog)** action from the **Available Action Interfaces** to the **Selected Actions** by clicking the green arrow next to the action.

g. Expand **Gateway Syslog > Log audit events to System Log (Gateway syslog)**, and complete the fields as follows.

Field	Value
Name	Type: `Security Database Activity Monitoring`
Primary Host	Enter the IP address of your RSA NetWitness Suite Log Decoder or Remote Log Collector.
Primary Port	Type: `514`
Syslog Host Level	Type: `Info`
Message	Copy and paste text from the **impervawaf.txt** file. Use the line below **Security Database Activity Monitoring**. This file is available on the NetWitness Community as an Additional Download here: impervawaf.txt
Facility	Type: `Syslog`

h. Click **Save**.

6. Click the **Policies** > **Audit** tab.
7. Select the **External Logger** tab for a particular policy that you want to apply the new action set.
8. Select the name of your newly created action set, **Security Database Activity Monitoring**, and click **Save**.

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.