

NetWitness[®] Platform

PostgreSQL Event Source Log Configuration Guide

PostgreSQL

Last Modified: Wednesday, May 15, 2024

Event Source Product Information:

Vendor: [PostgreSQL](#)

Event Source: PostgreSQL

Versions: 8.4, 9.x, 15.x

Note: NetWitness supports the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case in the NetWitness Community Portal for support.

RSA Product Information:

Supported On: NetWitness Platform 12.0 and later

Event Source Log Parser: postgresql

Collection Method: Syslog

Event Source Class.Subclass: Storage.Database

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 and 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/>.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

February, 2024

Contents

Configure Syslog Output on PostgreSQL	6
Configure NetWitness Platform	8
Ensure the Required Parser is Enabled	8
Configure Syslog Collection	8
Getting Help with NetWitness Platform	11
Self-Help Resources	11
Contact NetWitness Support	11
Feedback on Product Documentation	12

PostgreSQL is an open source object-relational database system that has a reputation for reliability, data integrity, and correctness. This event source runs on all major operating systems, including Linux, UNIX (AIX, BSD, HP-UX, SGI IRIX, Mac OS X, Solaris, Tru64), and Windows. PostgreSQL has full support for foreign keys, joins, views, triggers, and stored procedures, and includes most SQL:2008 data types. This event source also supports storage of binary large objects, and has native programming interfaces for C/C++, Java, .Net, Perl, Python, Ruby, Tcl, and ODBC.

To configure the PostgreSQL event source, you must:

- I. Configure Syslog Output on PostgreSQL
- II. Configure NetWitness Platform for Syslog Collection

Configure Syslog Output on PostgreSQL

To configure PostgreSQL to communicate with the RSA NetWitness Platform, you must edit the **postgresql.conf** file. This file is typically located in the following locations:

```
var/lib/pgsql/data
```

or

```
usr/local/pgsql/data
```

To configure PostgreSQL to work with RSA NetWitness Platform:

1. Open **postgresql.conf** in a text editor. The changes that you need to make are in the **ERROR REPORTING AND LOGGING** section of the file.

- a. For the **log_destination** parameter, add **syslog** to the list of destinations. For example:

```
log_destination = 'stderr, csvlog, syslog'
```

- b. Set the Syslog facility and identity lines as follows:

```
syslog_facility = 'local0'
syslog_ident = 'postgres'
```

Note: The facility setting is used in the syslog.conf file to point to the IP address of the RSA NetWitness Platform Log Decoder or Remote Log Collector. The identity value appears as the first portion of each logged message, enabling you to identify the PostgreSQL-generated messages.

- c. For the **log_min_messages** parameter, set the value to the minimum level of messages to log. For example, to log **error**, **log**, **fatal**, and **panic** level messages, set the parameter as follows:

```
log_min_messages = error
```

- d. If you want to log the duration of each SQL statement, set the **log_min_duration_statement** parameter to **0**. You can set this parameter to **-1** to disable it.

- e. Set the following parameters to **on** (by default, they are set to **off**):

```
log_connections = on
log_disconnections = on
log_duration = on
```

- f. Set the **log_line_prefix** parameter exactly as follows:

```
log_line_prefix = '#PostgreSQL: %i^%t^%u^%d^%r^%c^%s^'
```

Warning: The **log_line_prefix** parameter is used to format the log messages so that RSA NetWitness Platform can parse those messages. If you do not set this parameter correctly, the log messages cannot be processed by RSA NetWitness Platform.

- g. Set the **log_statement** parameter to **all**.

```
log_statement = 'all'
```

- h. Save and close the **postgresql.conf** file.

2. Add the following line to the **etc/syslog.conf** file:

```
local0.* @platform_IP_address
```

where *platform_IP_address* is the IP address of the NetWitness Log Decoder or Remote Log Collector.

3. Ensure that you are logged on as the root user, and enter the following command:

```
service postgresql restart
service syslog restart
```

This completes the configuration. PostgreSQL should now log messages to RSA NetWitness Platform.

Configure NetWitness Platform



Perform the following steps in RSA NetWitness Platform:

- 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 **postgresql**.



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.

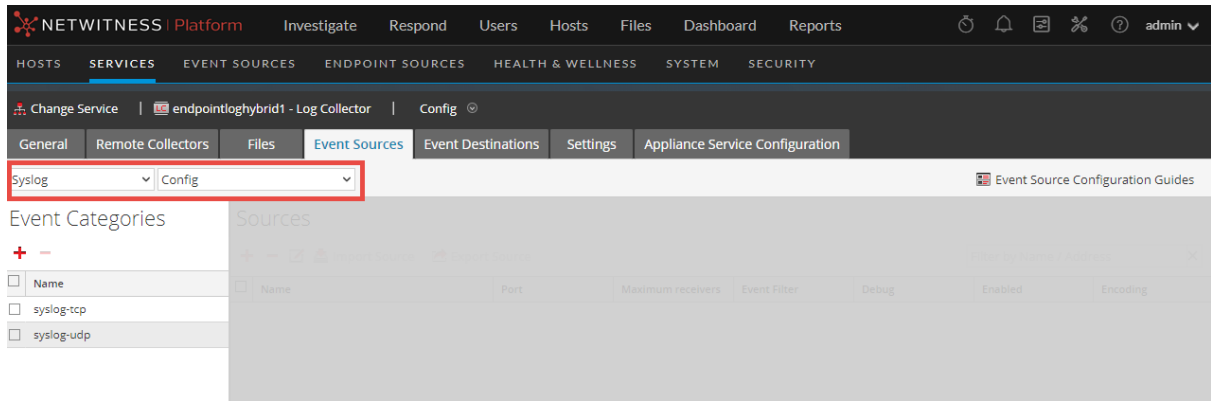
To configure Log Decoder for Syslog Collection

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

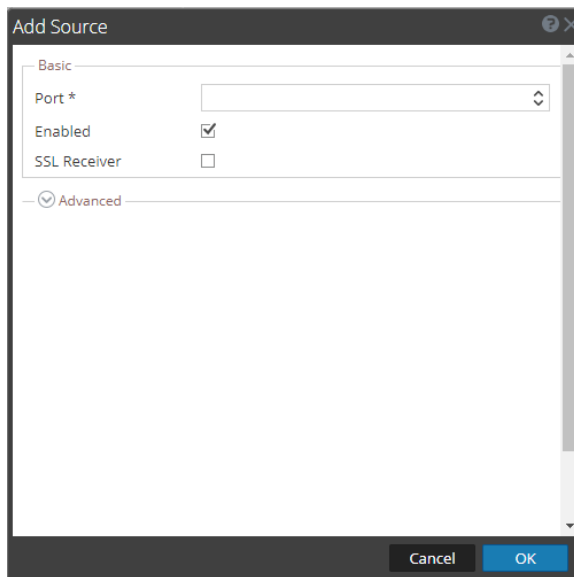
1. In the NetWitness Platform menu, go to  (Admin) > **Services**.
2. In the **Services** grid, select a Remote Log Collector and from the **Actions** () menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog / Config** from the drop-down menu.

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.