

RSA NetWitness Platform

Event Source Log Configuration Guide



PostgreSQL

Last Modified: Thursday, October 10, 2019

Event Source Product Information:

Vendor: [PostgreSQL](#)

Event Source: PostgreSQL

Versions: 8.4, 9.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: postgresql

Collection Method: Syslog

Event Source Class.Subclass: Storage.Database

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 RSA 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 enabled:

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 should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **ADMIN > 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  **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 the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **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 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.

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. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.