NetWitness® Platform

Trellix ePolicy Orchestrator Logstash Event Source Log Configuration Guide

Event Source Product Information:

Vendor: Trellix

Event Source: ePolicy Orchestrator

Versions: 7.2

NetWitness Product Information:

Supported On: NetWitness Platform 12.3 and later

Event Source Log Parser: epolicy

Collection Method: Logstash

Event Source Class.Subclass: Security.Antivirus

NETWITNESS Platform

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/.

September 2024

Contents

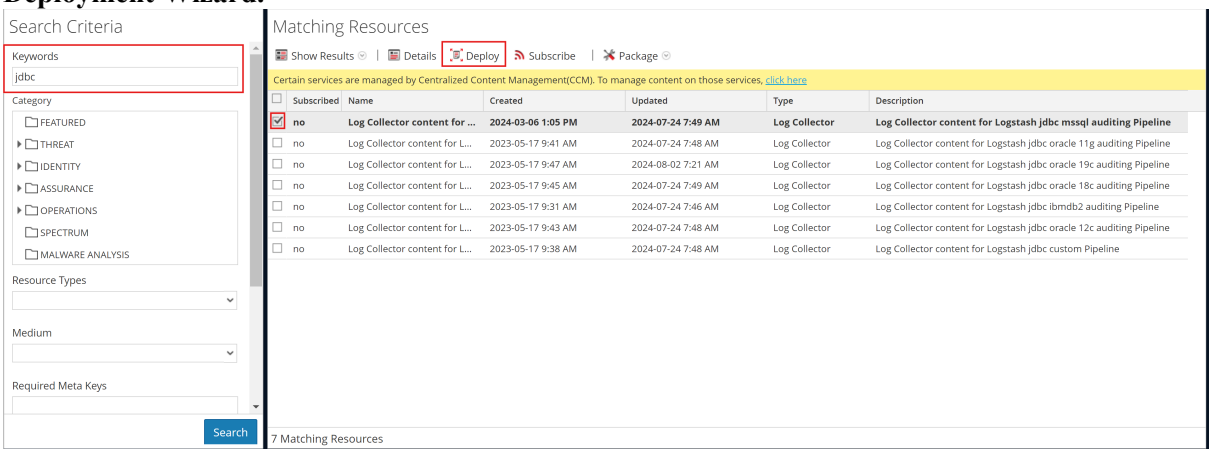
Configure Trellix ePolicy Orchestrator Event Source

Deploy Logstash JDBC Pipeline from NetWitness Live

Logstash JDBC Pipeline files require resources available in Live to collect logs.

To deploy Logstash JDBC Pipeline files from Live:

1. In the NetWitness Platform menu, select **Configure > Live Content**.
2. Type **Jdbc** into the Keywords text box and click Search to browse Live for Logstash JDBC Pipeline files.
3. Select the item returned from the search based on the DB version.
4. Click **Deploy** to deploy the Logstash JDBC Pipeline files to the appropriate Log Collector in the **Deployment Wizard.**

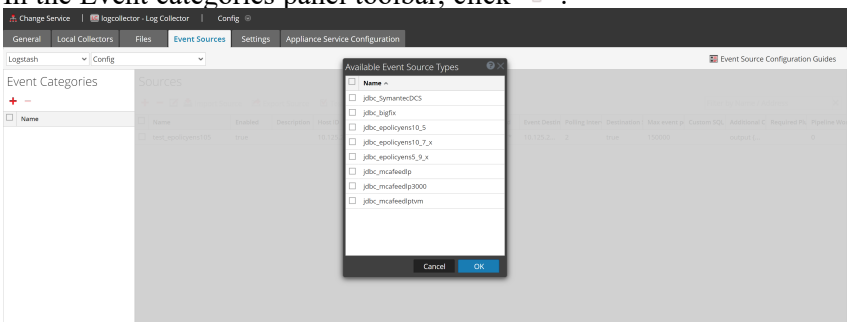


Setup Logstash ePolicy JDBC Event Sources (Pipelines) in NetWitness Platform

To setup the ePolicy JDBC Event Source:

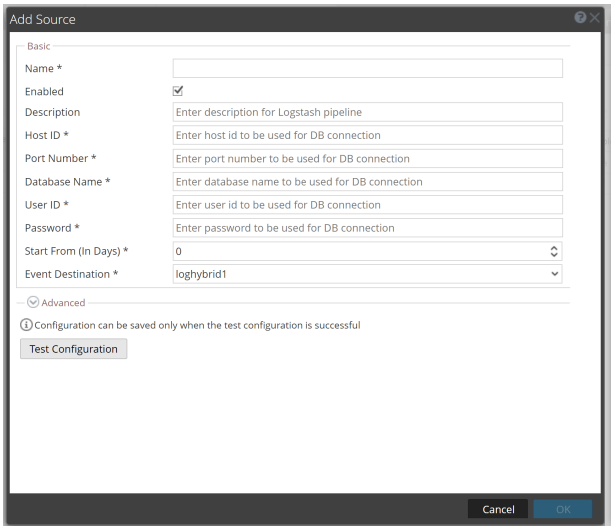
1. In the **NetWitness** menu, select  (Admin) > **Services**.
2. In the Services grid, select a Log Collector service and from the **Actions** () menu, choose **View** > **Config** > **Event Sources**.
3. Select **Logstash/Config** from the drop-down menu.

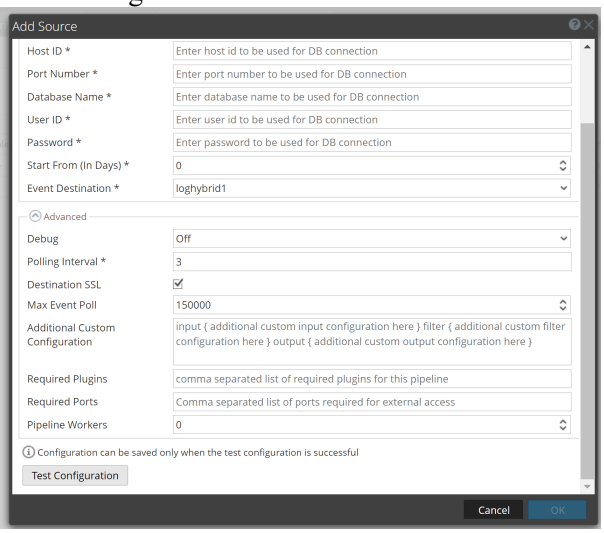
4. In the Event categories panel toolbar, click  .



5. From the **Available Event Source Types** list
   - For versions 3.5, select **jdbc_ePolicy**.
   - For versions 3.5, 3.6.0 or 3.6.1, select **jdbc_epolicyvirus**.
   - For version 5.9x, select **jdbc_epolicyvirus5_9_x**.
6. In the **Sources** panel, click  .

   The **AddSource** dialog box is displayed.
7. Define the Parameter described in the JDBC Collection Configuration Parameters.

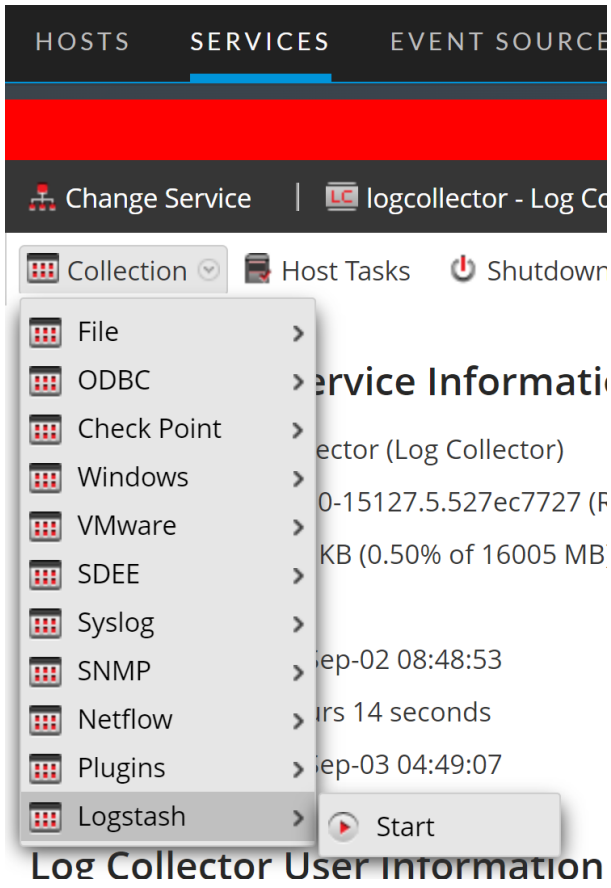




8. Click **Test Configuration**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information based on message shown and retry.

   Note: The log collector may take 1 to 3 minutes to return the test results. If it exceeds the time limit, the test times out and NetWitness platform displays a Request Timed Out error.
9. If the test is successful, click **OK**. The new event source is displayed in the **Sources** panel.
10. Save the configuration. From the Actions menu, choose System and in the Collection drop-down menu, select Logstash > Start to start the log collection, if it's not started already.



JDBC Collection Configuration Parameters

The tables below list the configuration parameters required for integrating different database event source with NetWitness Platform through JDBC logstash pipeline.

Basic Parameters

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the check-box to enable the event source configuration to start collection. The check-box is selected by default.
Description	Enter a text description for the event source.
Host ID*	Enter the IP address of the machine where the database server is installed.
Port Number*	Enter the port number that you configured for your event source. The default value of port number is 1433.

Name	Description
Start Date*	Number of days before today to begin data collection (0-90, default: 0). For example, if today is 2024-09-12 and startDate is set as 10, collection starts from 2024-09-02 00:00:00 (YYYY-MM-DD HH:MM:SS). If not set, it takes default value ans starts collection from today 00:00:00.
Database Name*	Enter the name of the database where the audit table exists.
User ID*	Enter the username of database.
Password*	Enter the password to log into the database.
PollingInterval*	Polling interval takes the input in minutes. Based on the minutes entered, the pipeline will pull the data from the database. For example, If the polling interval is 1, then the pipeline will pull the data from the database for every 1 minute. If the polling interval is 2, then the pipeline will pull the data from the database for every 2 minute. This filed takes the values between 1 to 60.
Event Destination*	Select the NetWitness Log Collector or Log Decoder to which event needs to be sent from the drop-down list.
Test Configuration	Checks the configuration parameters specified in this dialog to ensure they are correct.

Advanced Parameters

Click  next to **Advanced** to view and edit the advanced parameters, if necessary.

Name	Description
Debug	**Caution:** Only enable debugging (set this parameter to **On** or **Verbose**) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. **Caution:** Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.

Name	Description
Polling Interval*	Enter the polling interval in minutes (1-60). This determines how often data is pulled from the database. The default value is set to 3.
Destination SSL	Select the checkbox to communicate using destination SSL.
Max Event Poll	Specify the maximum number of events that can be collected during a polling cycle. By default, this is set to 1,50,000 which is also the maximum value.
Custom SQL Statement*	By default this field is empty. It accepts any valid custom SQL query (overriding the default query) to run and collect data from the database.
Additional Custom Configuration	Use this text box for any additional configuration, in case you have multiple inputs or another set of outputs to send somewhere in addition to a NetWitness Log Collector or Log Decoder. For example, you can configure the data to be sent to Elasticsearch. In this case each event that is sent to Netwitness Platform will also be send to Elasticsearch.
Required Plugins	Specify the required plugins in a comma separated list. **Note:** - Backup and restore is not supported for custom plugins. - If the test connection failed due to required plugin is not installed, you must install the required plugin, for more information, see Install or Manage Logstash Plugin.
Required Ports	Enter the list of ports required for external access.
Pipeline Workers	Number of pipeline worker threads allocated for logstash pipeline.

Configure NetWitness Platform to Collect Events

To configure NetWitness platform to collect events:

You must start capture on the Log Decoder to which you are sending the Logstash data. To start or restart network capture on a Log Decoder:

1. In the NetWitness Platform menu, select  **(Admin) > Services**. The Services view is displayed.
2. Select a **Log Decoder** service.
3. Under **Actions**, select **View** > **System**.
4. In the toolbar, click **Start Capture**.

Note: If the toolbar is displaying the **Stop Capture ()** icon, then capture has already started.

Log Decoders can handle events up to 32 KB by default. If your events are being cut off, you need to change the event size.

To change Event Size Limit:

1. At `http://<LogDecoder_IP>:50102/decoder/config` (replace <LogDecoder_IP> with the IP address of your Log Decoder), change the Log Decoder REST configuration.

2. Set `pool.packet.page.size` to 64 KB.

3. Restart the Log Decoder to apply the changes.

Note: If you are collecting events larger than 64 KB, you can reduce the size of incoming data by dropping unnecessary logs or fields from specific event sources.

Ensure the Required Parser is Enabled

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 **epolicy**.

Reference tables and Typespec

This event source collects data from the following tables, using the indicated typespec files.

- The ServerEvents table uses the **jdbc_epolicy_pipeline_template.conf** typespec file.
- The Events table uses the **jdbc_epolicyvirus_pipeline_template.conf** typespec file.
- The following tables are used in **jdbc_epolicyvirus5_9_x_pipeline_template.conf**.
  - EPOEvents
  - EPExtendedEventMT

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.