NetWitness® Platform

Trellix ePolicy Orchestrator Event Source Log Configuration Guide

NETWITNESS
Platform

Trellix ePolicy Orchestrator (formerly McAfee ePolicy Orchestrator)

Last Modified: Monday, June 24, 2024

Event Source Product Information:

Vendor: Trellix

Event Source: ePolicy Orchestrator

Versions: 3.5, 3.6.0, 3.6.1, 4.0, 4.5, 4.6, 5.x

RSA Product Information:

Supported On: NetWitness Platform 12.0 and later

Event Source Log Parser: epolicy

Collection Method: ODBC, Syslog

Event Source Class.Subclass: Security.Antivirus

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

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

February, 2024

Contents

To configure ODBC collection in RSA NetWitness Platform, perform the following procedures:

I. Ensure the required parser is enabled

II. Configure a DSN

III. Add the Event Source Type

For table reference, see Reference Tables below.

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 **epolicy**.

Configure a DSN

Configure a DSN (Data Source Name):

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. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
4. The DSNs panel is displayed with the existing DSNs, if any.
5. Click + to open the **Add DSN** dialog.

   Note: To add a DSN template, see the **Configure a DSN** topic in the *Log Collection Configuration Guide*, available in NetWitness Community.
6. Choose a **DSN Template** from the drop down menu and enter a name for the DSN. (Use this name when you set up the ODBC event source type.)
7. Fill in the parameters and click **Save**.

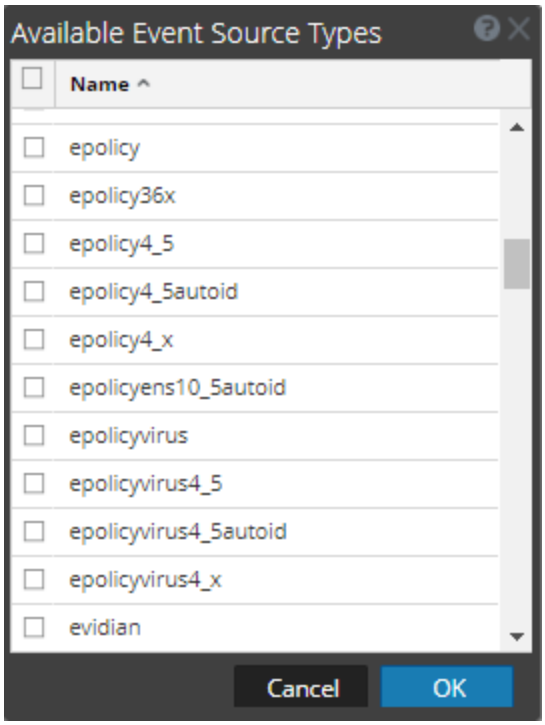
Field	Description
DSN Template	Choose the **MSSQL_Server_Windows_Template** from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
Database	Specify the database used by McAfee ePolicy Orchestrator
PortNumber	Specify the Port Number. The default port number is **1433**
HostName	Specify the hostname or IP Address of McAfee ePolicy Orchestrator
Driver	Depending on your NetWitness Log Collector version: • For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3sqls27.so • For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqls26.so

Add the Event Source Type

Add the ODBC Event Source Type:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/Config** from the drop-down menu.

   The Event Categories panel is displayed with the existing sources, if any.
5. Click + to open the **Available Event Source Types** dialog.



6. Choose the log collector configuration type for your event source type and click **OK**.

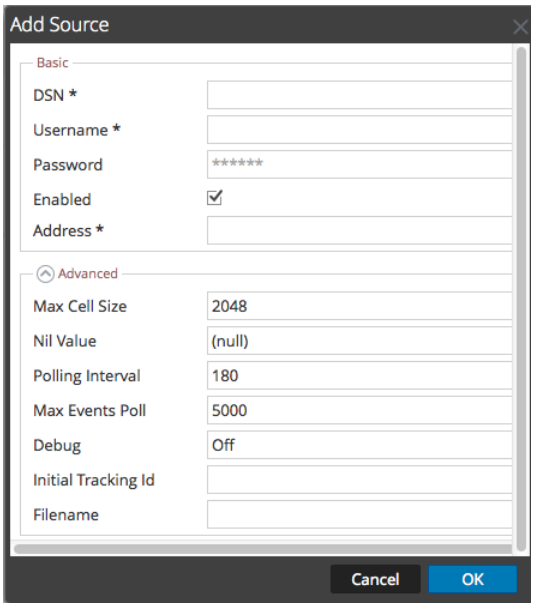
   For collecting ePolicy system logs:

   - For version 3.5, select **ePolicy**.
   - For versions 3.6.0 or 3.6.1, select **ePolicy36x**.
   - For version 4.0, select **ePolicy4_x**.
   - For version 4.5 and newer, select **ePolicy4_5**.
   - (Optional) If you want to use AutoID as the tracking column, select **ePolicy4_5Autoid**

   For collecting ePolicy virus logs:

- For versions 3.5, 3.6.0, or 3.6.1, select **epolicyvirus**.
- For version 4.0, select **epolicyvirus4_x**.
- For version 4.5 and newer, select **epolicyvirus4_5**.
- For version 5.9.x, select **epolicyvirus5_9_x**.
- (Optional) If you want to use AutoID as the tracking column, select **ePolicyvirus4_5Autoid**.

7. In the **Event Categories** panel, select the event source type that you just added.
8. In the **Sources** panel, click + to open the **Add Source** dialog.



9. Enter the DSN you configured during the **Configure a DSN** procedure.
10. For the other parameters, see the **ODBC Event Source Configuration Parameters** topic in the *Log Collection Configuration Guide*, available in NetWitness Community.

Reference Tables

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

- The **ServerEvents** table uses the **epolicy.xml** typespec file.
- The following tables use the **epolicy36x.xml** typespec file:
  - ServerEvents
  - EPOAuditEvents
  - EPOAuditEventMsgs
- The **OrionAuditLog** table uses the following typespec files:

  - epolicy4_5.xml
  - epolicy4_5autoid.xml
  - epolicy4_x.xml
- The **Events** table uses the **epolicyvirus.xml** typespec file.
- The **EPOEvents** table uses the following typespec files:
  - epolicyens10_5autoid.xml
  - epolicyvirus4_5.xml
  - epolicyvirus4_5autoid.xml
  - epolicyvirus4_x.xml

Configure Syslog Event Sources on the NetWitness Platform

This section provides instructions for configuring the Trellix EPO with NetWitness Log Collector. It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products to install the required components.

Perform the below steps on the NetWitness Platform to configure Syslog Event Source:

- Enable the Required Parser.
- Configure NetWitness Platform for Syslog Collection.

Enable the Required Parser

If you do not see your parser in the list while performing this procedure, you need to download it in NetWitness Platform Live.

To enable the required parser:

1. In the **NetWitness** Platform 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, **epolicy** and ensure that the **Config Value** field for your event source is selected.

   The new device is listed under the Log Decoder(s) General Tab within the **Service Parsers Configuration**.

   Note: The required parser is ***epolicy***.

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

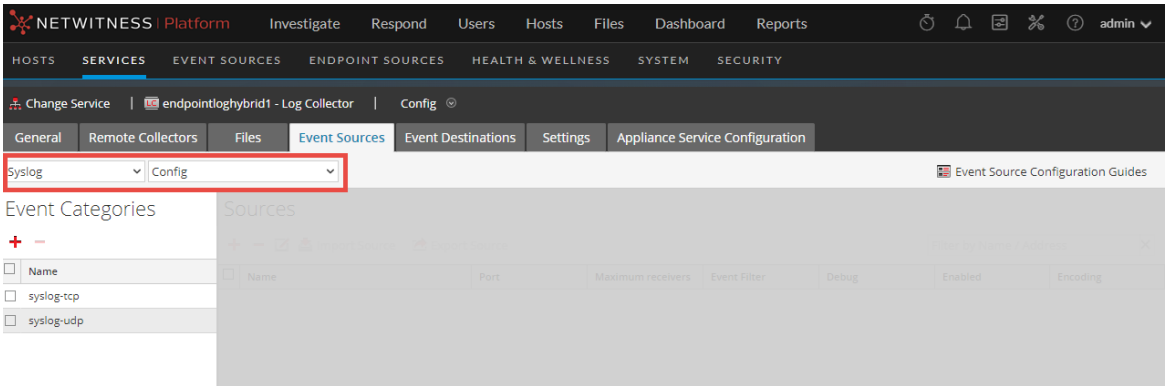
1. In the NetWitness Platform menu, select (Admin) > **Services**.
2. In the **Services** grid, choose a Log Decoder and from the **Actions (** **)** menu, choose **View** > **System**.

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.



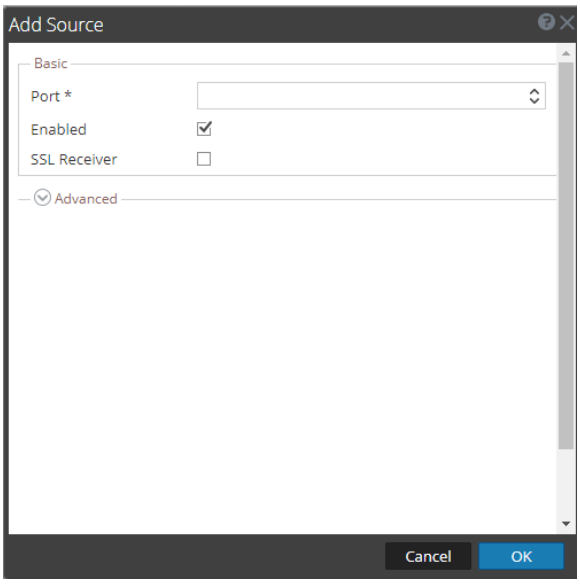
4. In the **Event Categories** panel toolbar, click +.

   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.

Configuring Syslog Server on Trellix ePolicy Orchestrator

1. Select **Menu → Configuration → Registered Servers**, then click **New Server**.
2. From the **Server type** menu on the **Description** page, select **Syslog Server**, specify a unique name and any details, then click **Next**.
3. From the **Registered Server Builder** page, configure these settings:
   a. **Server name** — Enter the IP address of the NetWitness Log Decoder or Remote Log Collector.
   b. **TCP port number** — Type the syslog server TCP port. The default is 6514.
   c. **Enable event forwarding** — Click to enable event forwarding from **Agent Handler** to this syslog server.
   d. **Test** — Click **Test Connection** to verify the connection to your syslog server.
4. Click **Save**.

Note: For more information, see Trellix Doc Portal

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.