RSA NetWitness Logs

Event Source Log Configuration Guide

McAfee Network Data Loss Prevention

Last Modified: Wednesday, November 8, 2017

Event Source Product Information:

Vendor: McAfee
Event Source: Network Data Loss Prevention
Version: 8.6, 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 Suite 10.0 and later
Event Source Log Parser: mcafeereconnex, cef
Collection Method: ODBC, Syslog
Event Source Class.Subclass: Security.DLP

To integrate McAfee Network Data Loss Prevention with RSA NetWitness Suite, you can choose between Syslog and ODBC collection methods.

- Configure Syslog Collection
  - Configure NetWitness Suite for Syslog Collection
  - Configure McAfee Network DLP to Send Syslog
- Configure ODBC Collection
  - Configure NetWitness Suite for ODBC Collection
  - Configure McAfee Network DLP for ODBC Collection

Note: Alternatively, you can collect using the **cef** parser. However, if using the cef parser, make sure to disable the **mcafeereconnex** parser. For details, see Use the CEF Parser for Collection.

Configure NetWitness Suite for Syslog Collection

Perform the following steps in RSA NetWitness Suite:

- 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 Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration** > **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 **mcafeereconnex**.

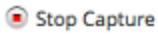
Configure Syslog Collection

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 **Administration** > **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 

, click the icon to start capturing Syslog.
   - If you see 

, 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 **Administration** > **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.

Once 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.

Configure McAfee Network DLP to Send Syslog

1. Log on to the McAfee Network DLP web console with administrative credentials.
2. Click **System**.
3. To configure the McAfee Network DLP, follow these steps:
   a. Navigate to the device listed as **Manager**, and in the **Configure** column, click **Configure**.
   b. Navigate to the **Syslog** section.
   c. In the **Syslog Server** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
   d. Click **Update**.

Configure NetWitness Suite for ODBC Collection

To configure McAfee Network DLP for ODBC Collection on RSA NetWitness Suite, perform the following tasks on the RSA NetWitness Suite:

I. Ensure the required parser is enabled

II. Configure a DSN

III. Add the Event Source Type

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 Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration** > **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 **mcafeereconnex**.

Configure a DSN

Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select **Administration** > **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/DSNs** from the drop-down menu.
5. The DSNs panel is displayed with the existing DSNs, if any.

6. Click + to open the **Add DSN** dialog.

   Note: If you need to add a DSN template, see the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in RSA Link.

7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

Field	Description
DSN Template	Choose one of the MySQL templates from the available choices.
DSN Name	Enter a descriptive name for the DSN
Parameters section	
Database	Specify the database used by McAfee Network (DLP)
PortNumber	Specify the Port Number. The default port number is **3306**
HostName	Specify the hostname or IP Address of McAfee Network (DLP)
Driver	Depending on your NetWitness Log Collector version: • For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3mysql27.so • For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3mysql26.so

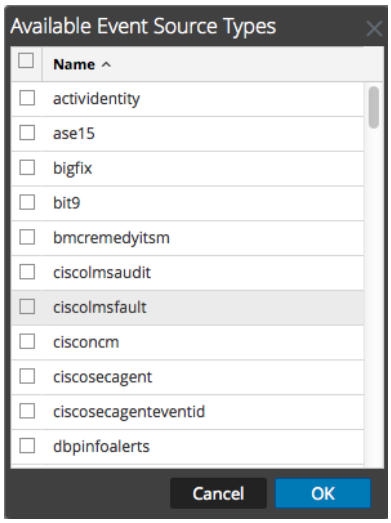
Add the Event Source Type

Add the ODBC Event Source Type:

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

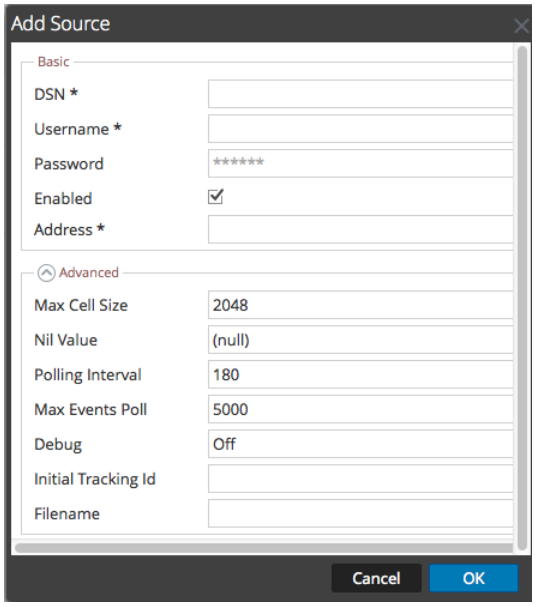


6. Choose the log collector configuration type for your event source type and click **OK**.

   From the **Available Event Source Types** dialog box, select **reconnex**.

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 *RSA NetWitness Suite Log Collection Guide*.

Configure McAfee Network DLP for ODBC Collection

1. Access the McAfee Network DLP iManager via SSH and authenticate with user credentials.

   Note: The default user name is **root** and the default password is **mcafee**.

2. To modify the firewall to accept the TCP connection on the MySQL port 3306, add the following line to the **/etc/sysconfig/iptables** file:

   ```
   A RH-Firewall-1-INPUT-p tcp-m tcp -dport 3306 -j ACCEPT
   ```

3. To create a user account to allow RSA NetWitness Suite access to the MySQL database, follow these steps:

   a. To log on to MySQL, type:

      ```
      mysql
      ```

   b. Type:

      ```
      GRANT ALL ON *.* TO 'user'@'samehost' IDENTIFIED BY
      'password';
      ```

      where:

      - *user* is the user name for the NetWitness Suite user account.
      - *samehost* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector
      - *password* is the password for the NetWitness Suite user account.

Use the CEF Parser for Collection

If you want to collect using the CEF parser, you must disable the **mcafeereconnex** parser.

Ensure that the CEF parser is enabled and the mcafeereconnex parser is disabled:

1. In the RSA NetWitness Suite menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > Config**.
3. You need to have **cef** enabled and **mcafeereconnex** disabled:
   - In the Service Parsers Configuration panel, search for **cef**, and ensure that the **Config Value** field for this parser is selected.
   - In the Service Parsers Configuration panel, search for **mcafeereconnex**, and ensure that the **Config Value** field for this parser is not selected.

Trademarks