RSA NetWitness Logs

Event Source Log Configuration Guide

ManageEngine NetFlow Analyzer

Last Modified: Monday, March 06, 2017

Event Source Product Information:

Vendor: ManageEngine
Event Source: NetFlow Analyzer
Versions: 8.0, 9.5

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: manageenginenetflow
Collection Method: ODBC
Event Source Class.Subclass: Security.Analysis

Configure ManageEngine NetFlow Analyzer

To configure ManageEngine NetFlow Analyzer to work with the RSA NetWitness Suite, you must complete these tasks:

I. Configure ManageEngine NetFlow Analyzer to Accept Remote Connections

II. Add ManageEngine NetFlow Analyzer as a Data Source and Configure the ODBC Server

Note: RSA NetWitness Suite appliance collects conversation and security logs from ManageEngine NetFlow Analyzer. You must configure each separately in RSA NetWitness Suite.

Configure ManageEngine NetFlow Analyzer to Accept Remote Connections

To configure the ManageEngine NetFlow Analyzer to accept remote connections:

1. Open a command prompt and navigate to **<ManageEngine_Home>/mysql/bin**.
2. To log on to MYSQL, run the following command:

   For Windows: `mysql -u root --port=13310`

   For Linux: `mysql -u root -S ../tmp/mysql.sock`
3. To enter the netflow database, run the following command:

   ```
   "use netflow;"
   ```
4. In the netflow database, run the following command:

   ```
   GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP ON *.* TO
   'remote_user'@'localhost' IDENTIFIED BY 'Password';
   ```

   where *remote_user* is the same user name for the ODBC connection

   and *localhost* is the IP address of the RSA NetWitness Suite

   and *Password* is the same password for the ODBC connection.

Configure NetWitness Suite for ODBC Collection

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

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 from 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 **manageenginenetflow**.

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 Configure DSNs in the NetWitness User Guide.

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 the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
Database	Enter **netflow**
PortNumber	Enter **13310**
HostName	Specify the hostname or IP Address of ManageEngine
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

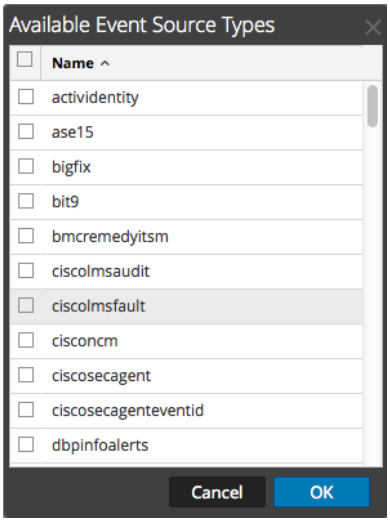
Add the Event Source Type

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.



Available Event Source Types

□	Name ^
□	activIdentity
□	ase15
□	bigfix
□	bit9
□	bmcremedyitsm
□	ciscolmsaudit
□	ciscolmsfault
□	cisconcm
□	ciscosecagent
□	ciscosecagenteventid
□	dbpinfoalerts

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

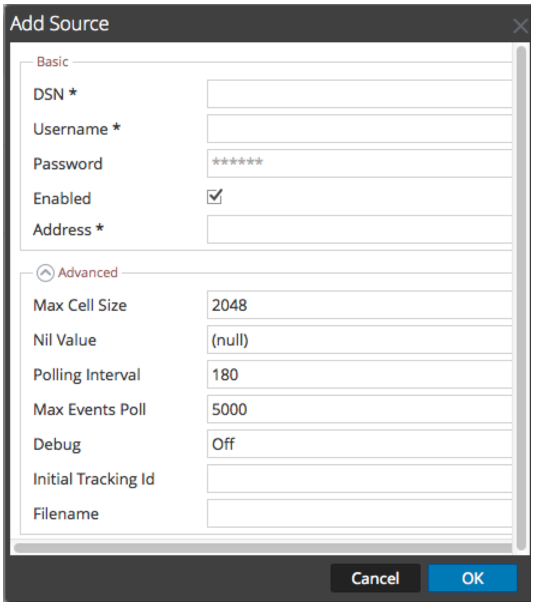
   From the **Available Event Source Types** dialog, select either of the following:

   - To collect conversation logs, select **netflowanalyzer_conversation**.
   - To collect security logs, select **netflowanalyzer_security**.

   To collect both types of logs, repeat this procedure and select the value that you did not select the first time.

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.



Basic

DSN *

Username *

Password ******

Enabled ☑

Address *

Advanced

Max Cell Size 2048

Nil Value (null)

Polling Interval 180

Max Events Poll 5000

Debug Off

Initial Tracking Id

Filename

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

Trademarks