

RSA NetWitness Platform

Event Source Log Configuration Guide



BigFix Enterprise Suite

Last Modified: Tuesday, June 18, 2019

Event Source Product Information:

Vendor: [BigFix](#)

Event Source: Enterprise Suite

Versions: 7.2

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: bigfix

Collection Method: ODBC

Event Source Class.Subclass: Network.Configuration Management

Configure BigFix Enterprise Suite for ODBC Collection

To configure ODBC collection in NetWitness, 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 and Typespec](#) 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 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 **bigfix**.

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.
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**.

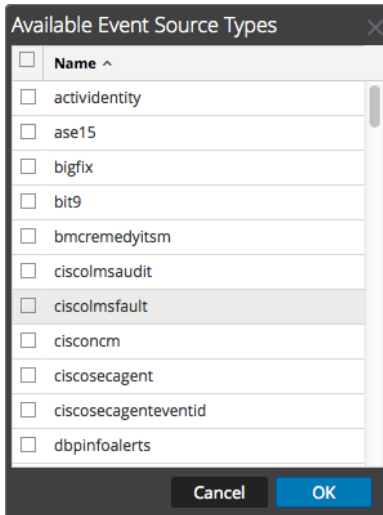
Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
Parameters section	
Database	Specify the database used by BigFix Enterprise Suite
PortNumber	Specify the Port Number. The default port number is 1433
HostName	Specify the hostname or IP Address of BigFix Enterprise Suite
Driver	Depending on your NetWitness Log Collector version: <ul style="list-style-type: none">• 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

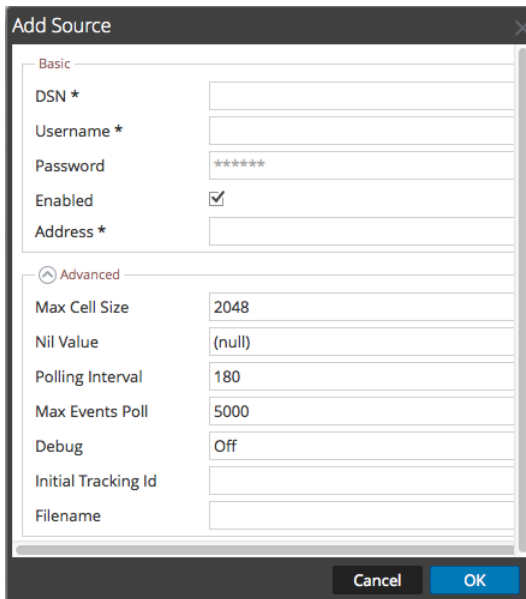
In step 6 below, select **bigfix** from the **Available Event Source Types** dialog.

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



10. Enter the DSN you configured during the **Configure a DSN** procedure.
11. For the other parameters, see [ODBC Event Source Configuration Parameters](#) in the SA User Guide.

Reference Tables and Typespec

This event source collects data from the **BES_Actions** table. The typespec file for this event source is **bigfix.xml**.

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.