RSA NetWitness Logs

Event Source Log Configuration Guide

Microsoft Network Access Protection

Last Modified: Thursday, May 18, 2017

Event Source Product Information:

Vendor: Microsoft
Event Source: Network Access Protection
Versions: 1.1

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: msnap
Collection Method: ODBC
Event Source Class.Subclass: Security.Access Control

To configure Microsoft Network Access Protection to work with RSA NetWitness Suite, you must complete these tasks:

I. Configure the SQL Server Database

II. Configure SQL Logging for the Network Policy Server

III. Configure NetWitness Suite for ODBC Collection

Configure the SQL Server Database

To configure the SQL Server database:

1. Connect to the target SQL database for Network Policy Server (NPS) logging.
2. Log on to the Microsoft SQL Server Management Studio with administrative credentials.
3. Right-click **Databases**, and click **New Database**.
4. In the **Database Name** field, type **MSNAP**.
5. Accept the default values, and click **OK**.

Configure SQL Logging for the Network Policy Server

Configuring SQL logging for the Network Policy Server is done differently depending on your version of the Microsoft Windows server.

- For configuration instructions with Microsoft Windows Server 2008 R2, see Configure Using Microsoft Windows Server 2008 R2.
- For configuration instructions with Microsoft Windows Server 2008, see Configure Using Microsoft Windows Server 2008.

Configure Using Microsoft Windows Server 2008 R2

To configure SQL logging using Microsoft Windows Server 2008 R2:

1. To open the NPS console, click **Start** > **Run**, and type **nps.msc**.
2. Log on to the NPS console with administrative credentials.
3. In the navigation pane, click **Accounting**.
4. In the **Accounting** section, click **Configure Accounting**.
5. Click **Next**.
6. Ensure that **Log to SQL Server Database** is selected, and click **Next**.
7. Ensure that all the event types are selected.
8. Depending on your security policy, select **If logging fails, discard connection requests**.
9. Click **Configure**, and from Data Link Properties window, follow these steps.
    a. Click the **Connection** tab.
    b. Enter the SQL server database name.
    c. Select **Use a specific user name and password**
    d. Enter the administrative user from the SQL server database and the password.
    e. Select **Allow saving password**.

f. In the **select the database on the server** drop-down list, select **MSNAP**.

g. Click **OK**.

10. Click **Next**, and click **Next** again.
11. Click **Rebuild**, and click **Finish**.

Configure Using Microsoft Windows Server 2008

To configure SQL logging using Microsoft Windows Server 2008:

1. To open the NPS console, click **Start** > **Run**, and type **nps.msc**.
2. Log on to the NPS console with administrative credentials.
3. In the navigation pane, click **Accounting**.
4. In the **SQL Server Logging Properties** section, click **Change SQL Server Logging Properties**.
5. Accept the default values, and click **Configure**.

   Note: Depending on your security policies, set the appropriate logging failure actions.

6. From Data Link Properties window, follow these steps.

   a. Click the **Connection** tab.

   b. Enter the SQL server database name.

   c. Select **Use a specific user name and password**

   d. Enter the administrative user from the SQL server database and the password.

   e. Select **Allow saving password**.

   f. In the **select the database on the server** drop-down list, select **MSNAP**.

   g. Click **OK**.

Configure NetWitness Suite for ODBC 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 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 **msnap**.

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**.

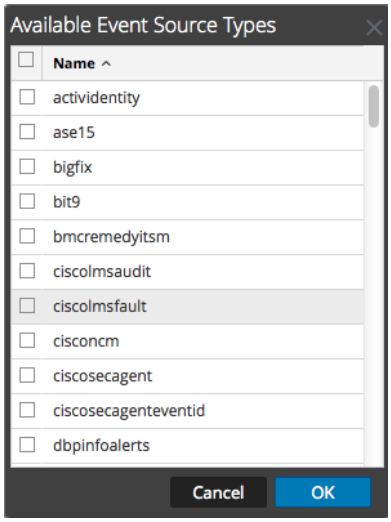
Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
Database	Specify the database used by Microsoft Network Access Protection. Enter **MSNAP** (this should match the database you created or selected in the Configure the SQL Server Database section).
PortNumber	Specify the Port Number. The default port number is **1433**
HostName	Specify the hostname or IP Address of Microsoft Network Access Protection
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 **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.

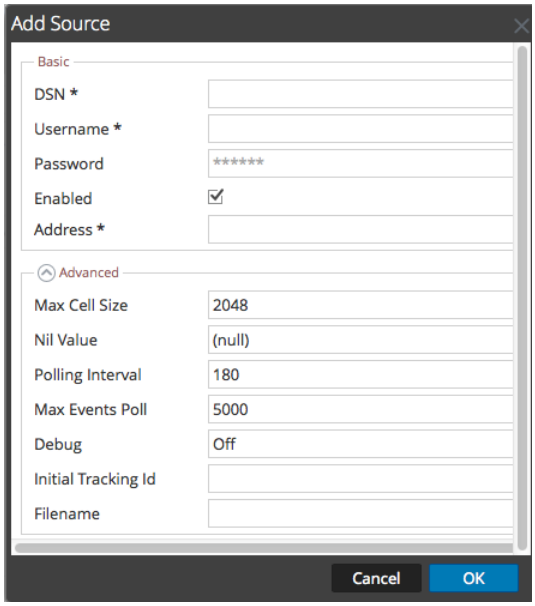
   The Event Categories panel is displayed with the existing sources, if any.
5. Click + to open the **Available Event Source Types** dialog.



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

   Select **msnap** from the **Available Event Source Types** dialog.

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 ODBC Event Source Configuration Parameters in the NetWitness Suite Log Collection Guide.

Trademarks