RSA NetWitness Logs

Event Source Log Configuration Guide

Microsoft Windows Server Update Service

Last Modified: Thursday, June 08, 2017

Event Source Product Information:

Vendor: Microsoft
Event Source: Windows Server Update Service
Versions: 3.0 SP 2, the version of WSUS that is packaged with Windows Server 2012

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: mswsus
Collection Method: ODBC
Event Source Class.Subclass: Network.Configuration Management

To configure Microsoft Windows Server Update Service to work with RSA NetWitness Suite:

I. Create a SQL Server User

II. Configure NetWitness Suite for ODBC Collection

> **Note:** RSA does not support ODBC collection from the Microsoft internal database at this time.

Create a SQL Server User

You must create a SQL Server user. You use these credentials when you Configure the ODBC Service, later in this configuration.

To create a SQL Server logon:

1. Open the SQL Server Management Studio with administrative credentials, and access the Database Engine.
2. To create a new login, follow these steps:
   a. From the **Object Explorer** navigation menu, expand your database server, which is the top item in the navigation pane.
   b. Expand **Security**.
   c. Right-click **Logins** and select **New Login**.
   d. From the **Select a page** navigation menu, select **General**.
   e. From the **Login name** field, type a login username. For example, **audit_reader**.
   f. Select **SQL Server authentication**.
   g. Create and confirm a password.
   h. Ensure that **Enforce Password Expiration** is not selected.
   i. Click **OK**.
   j. Click **Security** > **Login**, and right-click **audit_reader**.
   k. Select **Properties**, and from the **Select a page** navigation menu, select **User Mapping**.
   l. Ensure that **Map** is checked for the **SUSDB** database.
   m. Select the **SUSDB** database, and under 'Database role membership', check **db_accessadmin** and **db_datareader**.
   n. Click **OK**.
3. To set the login account permission, follow these steps:
   a. From the **Object Explorer** navigation menu, right-click your database server, and select **Properties**.

  b. From the **Select a page** navigation menu, select **Permissions**.
  c. From the **Login or roles** section, select **audit_reader**.
  d. From the **Explicit permissions** section, select the Grant column for **Connect SQL**, if it is not selected by default.
  e. Click **OK**..

4. To set the database access permission, follow these steps:
  a. From the **Object Explorer** navigation menu, expand your database server.
  b. Expand **Databases**.
  c. Right-click **SUSDB** and select **Properties**.
  d. From the **Select a page** navigation menu, select **Permissions**.
  e. From the **Login or roles** section, select **audit_reader**.
  f. From the **Explicit permissions** section, select the Grant column for **Connect**.
  g. Click **OK**.

Configure NetWitness Suite for ODBC Collection

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

i. Configure a DSN

ii. Ensure the required parser is enabled

iii. Restart the ODBC Collection Service

iv. Add the Event Source Type

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**.

```
Database=<Specify the database used by Microsoft Windows
Server Update Service, default is SUSDB>
```

```
PortNumber=<Specify the Port Number, default is 1433>
```

```
HostName=<Specify the hostname or IP Address of the
Microsoft WSUS event source>

Driver=/opt/netwitness/odbc/lib/R3sqls26.so
```

Note: The Driver field refers to the complete path to your ODBC driver.

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 **mswsus**.

Restart ODBC Collection

Restart the ODBC collection service:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ under **Actions** and select **View** > **System**.
4. Click **Collection** > **ODBC**.
   - If the available choice is **Start**, click **Start** to start ODBC collection.
   - If the available choices are **Stop** and **Pause**, click **Stop**, wait a few moments, and then click **Start**.

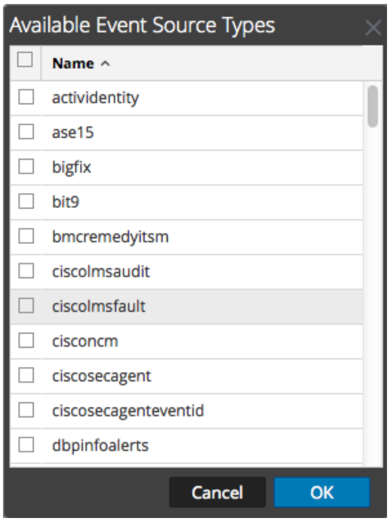
Add the Event Source Type

The required parser is **mswsus**: choose this in step 6.

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.

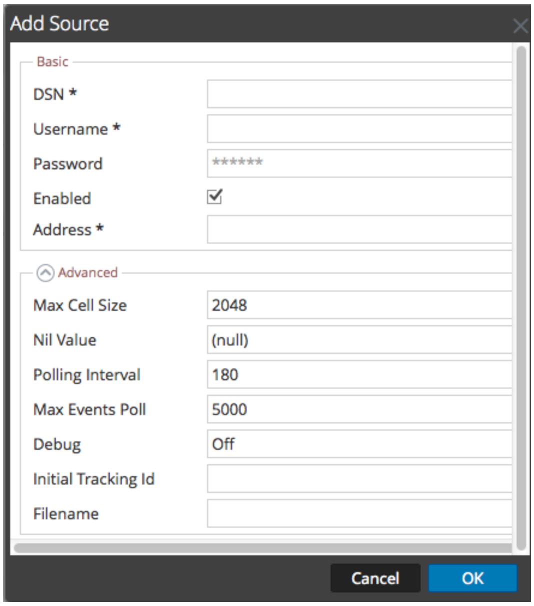


Available Event Source Types

□ **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**.
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.



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	

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.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.