RSA NetWitness Platform

Event Source Log Configuration Guide

IBM ISS SiteProtector

Last Modified: Wednesday, November 20, 2019

Event Source Product Information:

Vendor: IBM
Event Source: Proventia Appliance, SiteProtector, Internet Scanner, RealSecure
Versions: Site Protector v2.x

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: iss
Collection Method: ODBC
Event Source Class.Subclass: Security.IDS

This document includes the following sections:

- Configure the Internet Scanner or RealSecure for ODBC collection
- Troubleshoot SiteProtector Database Issues

Configure IBM ISS for ODBC Collection

To configure the Internet Scanner or RealSecure for ODBC collection, perform the following tasks in RSA NetWitness Platform:

I. Ensure the required parser is enabled

II. Configure a DSN

III. Add the Event Source Type

For table reference, see Reference Tables 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 from 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 **iss**.

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**.

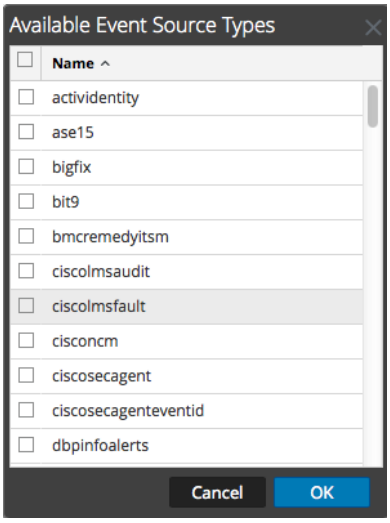
Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
Database	Specify the database used by RealSecure
PortNumber	Specify the Port Number. The default port number is **1433**
HostName	Specify the hostname or IP Address of RealSecure
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 ODBC Event Source Type

Add the ODBC Event Source Type:

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/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**.

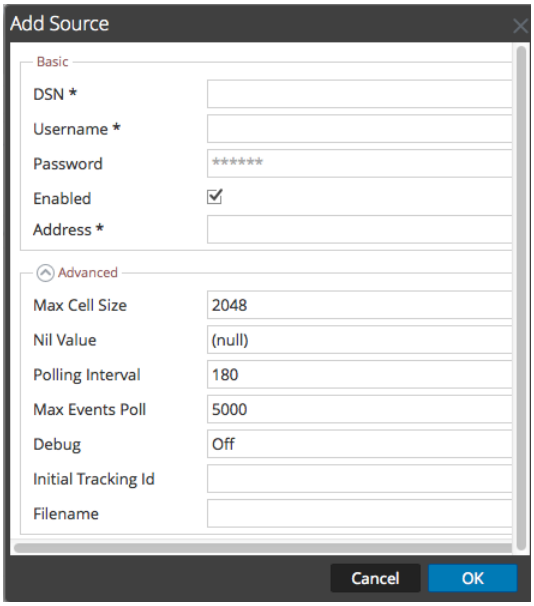
   In the **Available Event Source Types** dialog, choose either of the following values:

   - Siteprotector6_x
   - Siteprotector5_x

Note: RSA recommends you choose **Siteprotector6_x** from the dialog as it collects additional data. **Siteprotector5_x** is also supported, but contains fewer data columns.

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 Platform Log Collection Guide*.

Reference Tables

This event source collects data from the following tables, using the indicated typespec files.

- The following tables use the **siteprotector5_x.xml** typespec file:
  - SensorData
  - SensorDataAVP
  - attrs
  - Observances
  - SecurityChecks
  - Protocols
  - Products
  - ObservanceType
- The following tables use the **siteprotector6_x.xml** typespec file:
  - SensorData
  - SensorDataAVP
  - attrs
  - Observances
  - VulnStatus
  - ObjectType
  - AlertType
  - SecurityChecks
  - Protocols
  - Products
  - ObservanceType

Troubleshoot SiteProtector Database Issues

Since collection from SiteProtector queries the database, incorrect database configuration can result in errors. The **DBServerInfo** script from ISS can help you determine whether you have any problems with your database.

Warning: This script is subject to change by ISS. Be sure to download the latest copy.

Download the **DBServerInfo** file from this link and follow the instructions below:

ftp://ftp.iss.net/prv/perm/support/DBServerInfo/DBServerInfo_RSSP.exe

For complete information on this script, contact ISS.

Using DBServerInfo

Perform this task on the machine hosting the site database.

To use DBServerInfo:

1. To extract all of the files to a new folder on the database server machine:
   a. Perform one of the following tasks:
      - In Windows Explorer, double-click **DBServerInfo_RSSP.exe**
      - At a command prompt, type **DBServerInfo_RSSP.exe** and press **Enter**.
   b. Specify the appropriate unzip folder and click **Unzip**.
   c. Click **OK**.
   d. Click **Close**.
2. To run the utility from the selected folder, perform one of the following tasks:
   - In Windows Explorer, double-click **DBServerInfo.cmd** if you have Windows authentication.
   - At a command prompt, type **DBServerInfo**ServerName DBName SysadminID Password and press **Enter**.

   Note: All parameters are optional. The system defaults to local server, RealSecureDB database, and Windows authentication.

   Note: The output of the file is normally written to **c:\dbserverinfo_out.zip**.
3. (Optional) To find usage information, enter **DBServerInfo ?**.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.