RSA NetWitness Logs

Event Source Log Configuration Guide

Oracle Access Manager

Last Modified: Friday, April 07, 2017

Event Source Product Information:

Vendor: Oracle
Event Source: Access Manager
Versions: 10.1.4.0.3, 11g R2
Additional Downloads: sftpagent.conf.oracleam, nicsftpagent.conf.oracleam

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: oracleam
Collection Method: File, ODBC (for v11g R2)
Event Source Class.Subclass: Security.Access Control

Configure Oracle Access Manager

You can use File collection for all supported versions of Oracle Access Manager. Additionally, for v11g R2, you can use ODBC collection.

- For file collection, see Configure NetWitness Suite for File Collection.
- For ODBC collection on version 11g R2, see Configure NetWitness Suite for ODBC Collection .

Configure NetWitness Suite for File Collection

For file collection, set up the SFTP Agent and configure the Log Collector in RSA NetWitness Suite.

I. Set up the SFTP Agent

II. Configure the Log Collector for File Collection

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see Install and Update SFTP Agent
- To set up the SFTP agent on Linux, see Configure SA SFTP Agent shell script

Configure the Log Collector for File Collection

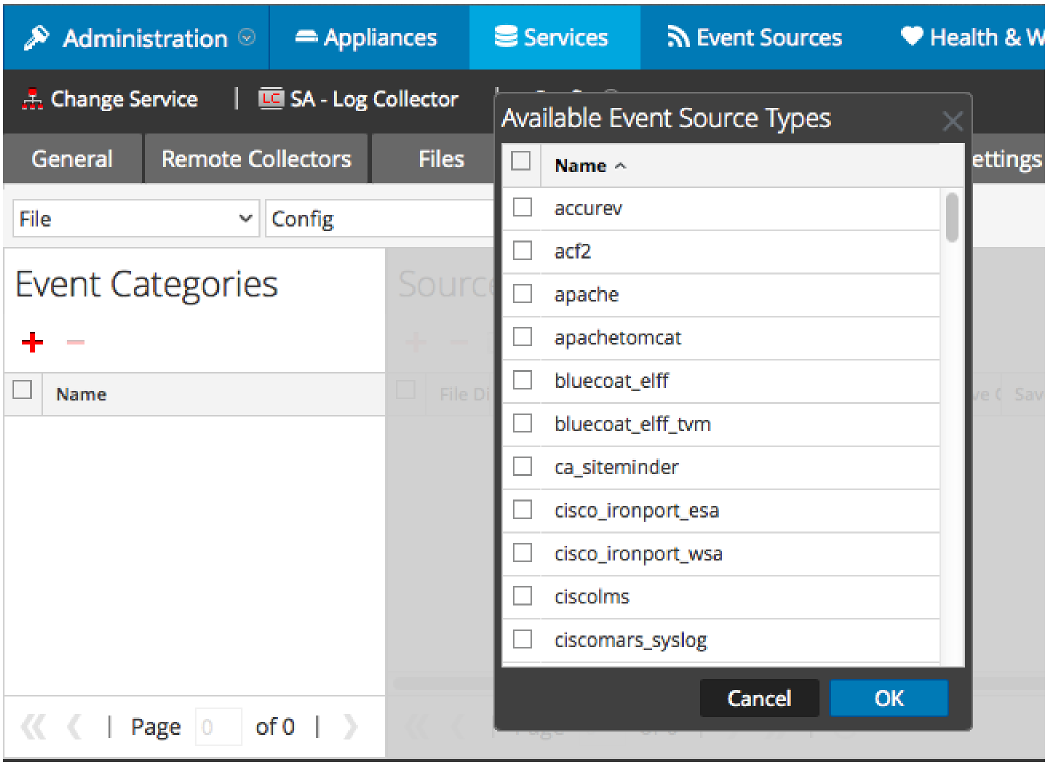
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **File/Config** from the drop-down menu.

   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

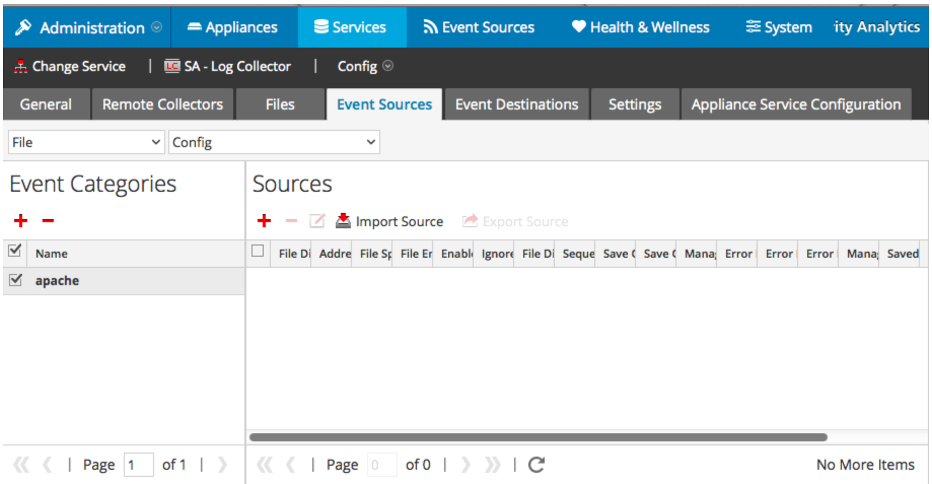
   The Available Event Source Types dialog is displayed.



5. Select the correct type from the list, and click **OK**.

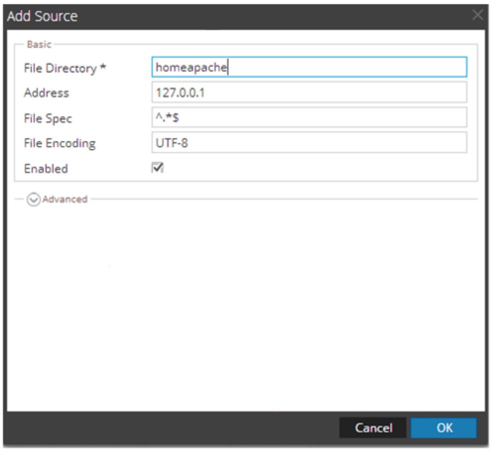
Select **oracleam** from the **Available Event Source Types** dialog.

The newly added event source type is displayed in the Event Categories panel.

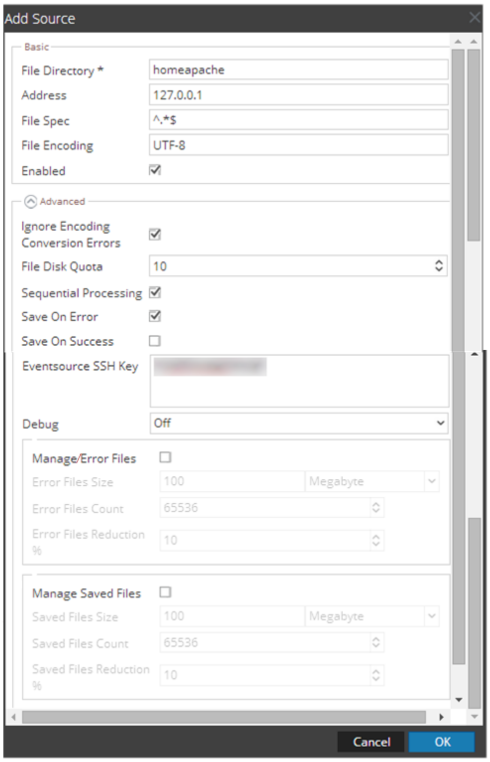


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

The Add Source dialog is displayed.



File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑



File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑
Ignore Encoding Conversion Errors ☑
File Disk Quota 10
Sequential Processing ☑
Save On Error ☑
Save On Success □
Eventsource SSH Key [redacted]
Debug Off
Manage/Error Files □
Error Files Size 100 Megabyte
Error Files Count 65536
Error Files Reduction % 10
Manage Saved Files □
Saved Files Size 100 Megabyte
Saved Files Count 65536
Saved Files Reduction % 10

7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.

8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

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 **oracleam**.

Synonyms

Oracle AM permits each Oracle instance to have its own schema name. Creating Synonyms is an additional step you must perform, to take care of these differing schema names.

You need to run the following synonym query in the Oracle environment. Use the same username that you chose when you set up ODBC collection.

```
create public synonym IAU_BASE for customerschema.IAU_BASE;
```

```
create public synonym OAM for cusotmerschema.OAM;
```

Where:

- ***IAU_BASE*** and ***OAM*** are the synonyms that customer will have to map to their respective schemas to.
- ***customerschema*** is the schema defined by the customer in their oracle instance.

So, synonym ***IAU_BASE*** should be mapped to ***customerschema.IAU_BASE***. And synonym **OAM** should be mapped to ***cusotmerschema.OAM***.

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 Oracle template from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
ServiceName	Enter the service name
PortNumber	The default port number is **1521**
HostName	Specify the hostname or IP Address of the Oracle database.

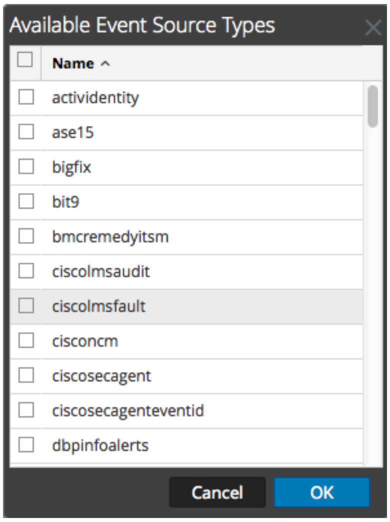
Field	Description
Edition Name	Enter the name of the Oracle edition
Driver	If you choose one of the native templates, you can accept the default value, **/opt/netwitness/odbc/lib/R3ora26.so**. If you choose one of the server templates, you need to point to the correct driver file on the Oracle server.

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

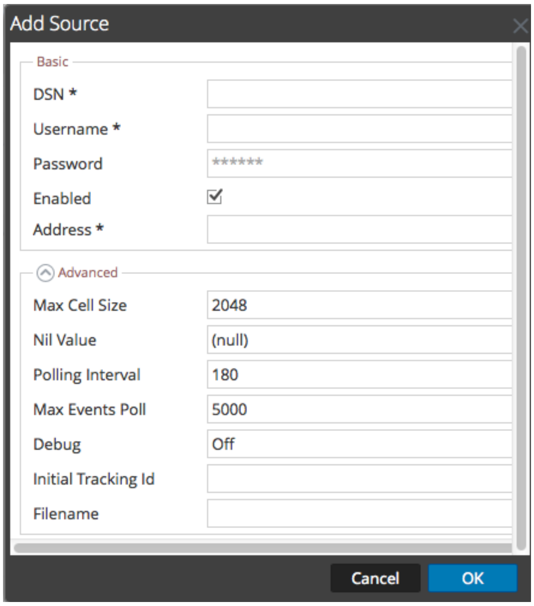
6. Choose the log collector configuration type for your event source type and click **OK**.

   For version 11gr2, select **oracleamtvm** 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.



Add Source

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