RSA NetWitness Logs

Event Source Log Configuration Guide

Oracle Directory Server

Last Modified: Thursday, June 29, 2017

Event Source Product Information:

Vendor: Oracle
Event Source: Oracle Directory Server (previously SunOne LDAP Directory Server)
Versions: 11.1.1.7.1
Additional Download: sftpagent.conf.sunoneldap, nicsftpagent1.conf.oracleds, nicsftpagent2.conf.oracleds
Platforms: Windows, Red Hat Linux

RSA Product Information:

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

Configure Oracle Directory Server

To configure Oracle Directory Server, you must complete these tasks in RSA NetWitness Suite:

I. Set Up the SFTP Agent

II. Set up the File Service

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

If you are using Linux, note the following when configuring the **sasftpagent.sh** file:

- Save two copies of the **sasftpagent.sh** file: **sasftpagent1.sh** and **sasftpagent2.sh**.
- In the files, set the following parameters:

  For the first file:

  - SCRIPT_NAME = sasftpagent1.sh
  - SA_CONFIG = sasftpagent1.conf

  For the second file:

  - SCRIPT_NAME = sasftpagent2.sh
  - SA_CONFIG = sasftpagent2.conf

Note: The cron jobs needed to run these two scripts will need the exact names of the sasftpagent instances that you specified in the SCRIPT_NAME parameter.

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:

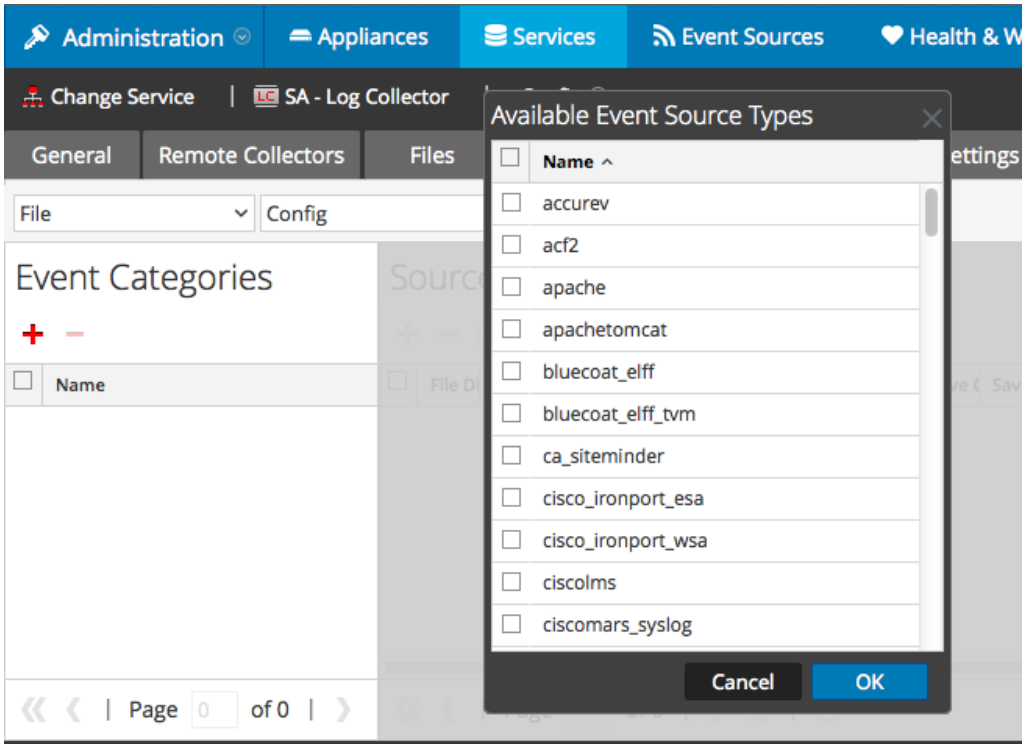
1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.

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.



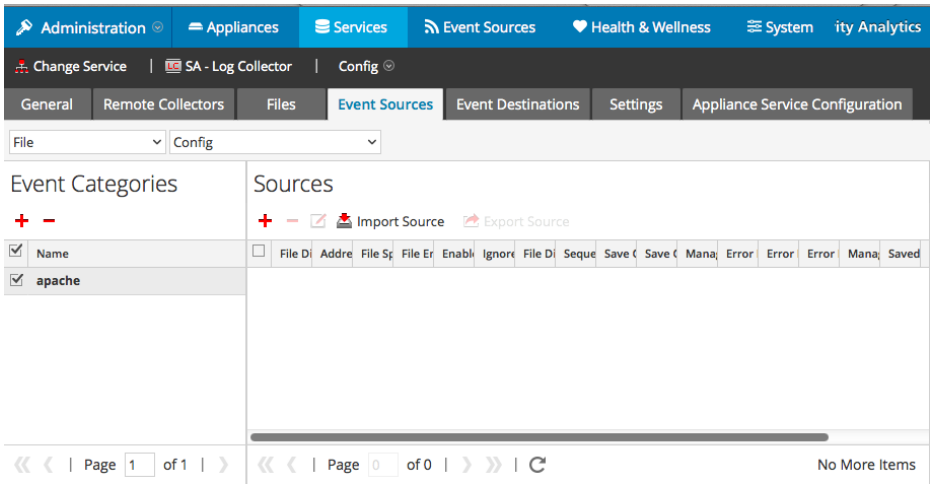
5. Select the correct type from the list, and click **OK**.

   From the **Available Event Source Types** dialog, select the appropriate choice or choices for your OS:

   - **sunoneldap** to collect audit logs on Windows
   - **oracleds_audit** to collect audit logs on Linux
   - **oracleds_access** to collect access logs on Linux

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

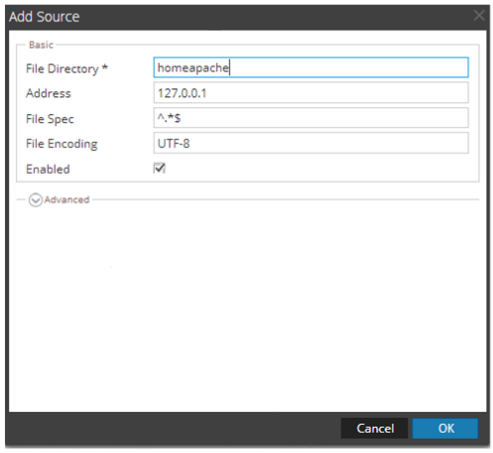
Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

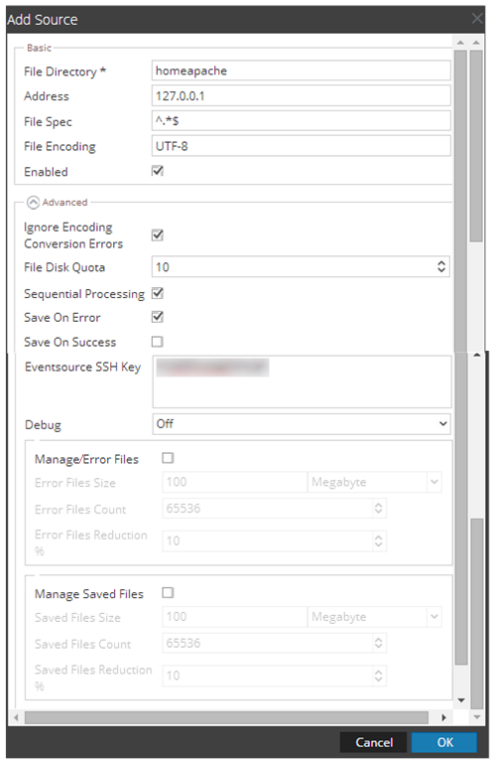


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.

   Note: Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.





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.

Trademarks