RSA NetWitness Logs

Event Source Log Configuration Guide

EMC Greenplum Database

Last Modified: Thursday, August 03, 2017

Event Source Product Information:

Vendor: EMC
Event Source: Greenplum Database
Version: 4.0
Additional Download: nicsftpagent.conf.greenplum

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: greenplum
Collection Method: File
Event Source Class.Subclass: Storage.Database

Greenplum specializes in enterprise data cloud solutions for large-scale data warehousing and analytics. The Greenplum Database is built from modified PostgreSQL in a massively parallel processing (MPP) database.

In the Greenplum architecture, data is partitioned across multiple segment servers, and each segment owns and manages a distinct portion of the overall data. All communication takes place through a network connection.

To configure Greenplum Database to work with RSA NetWitness Suite, you must complete these tasks:

I. Set up the SFTP Agent on the Linux/Unix Greenplum Server

II. Configure the NetWitness Suite 10.0 and later 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

While configuring the SFTP agent, use the following table for setting some of the parameters:

Setting	Description
ENVISION	Set this value to the IP address of the RSA NetWitness Log Collector
ENVISION_ DIRECTORY	EMC_GREENPLUM_***device_ip*** Where ***device_ip*** is the IP address for the event source For example, if the IP address is 172.16.0.51, set the parameter as follows: `ENVISION_DIRECTORY=EMC_GREENPLUM_172.16.0.51`

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:

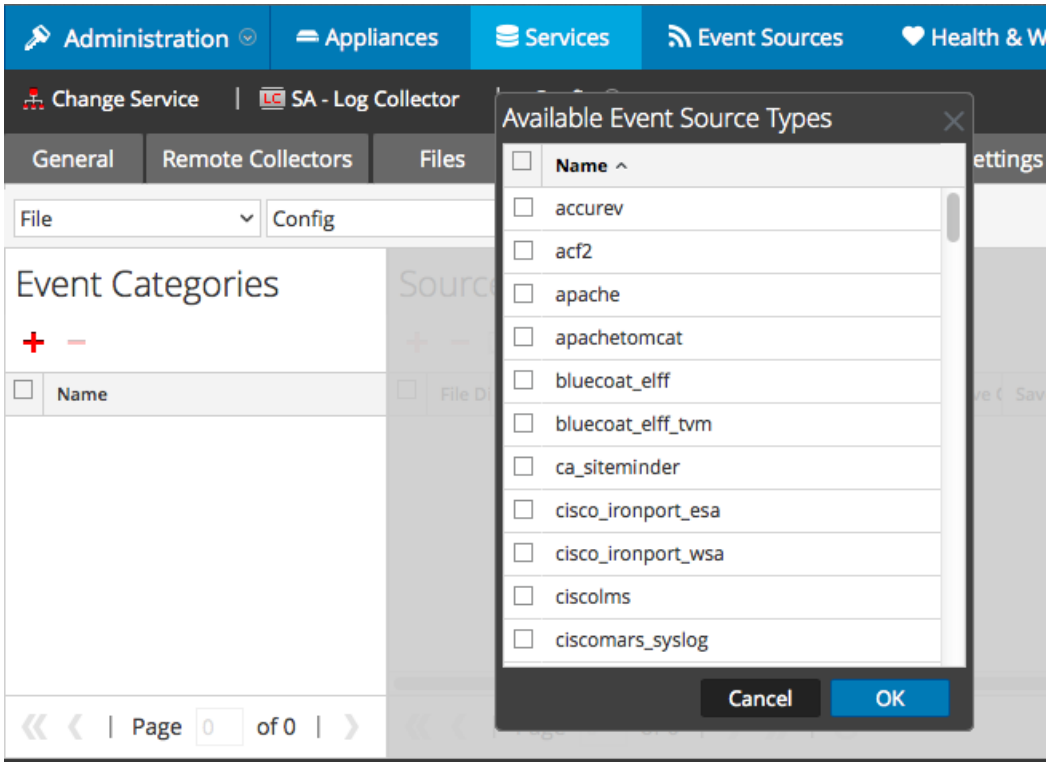
1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.

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.

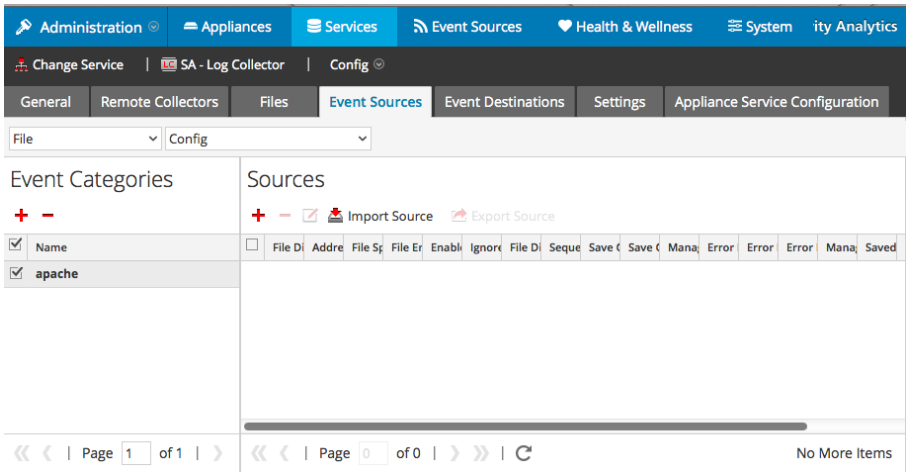


5. Select the correct type from the list, and click **OK**.

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

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

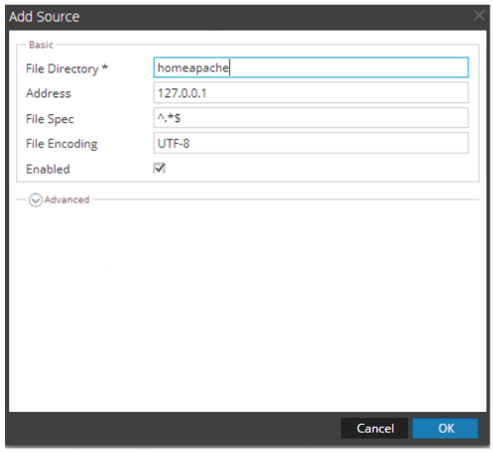
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

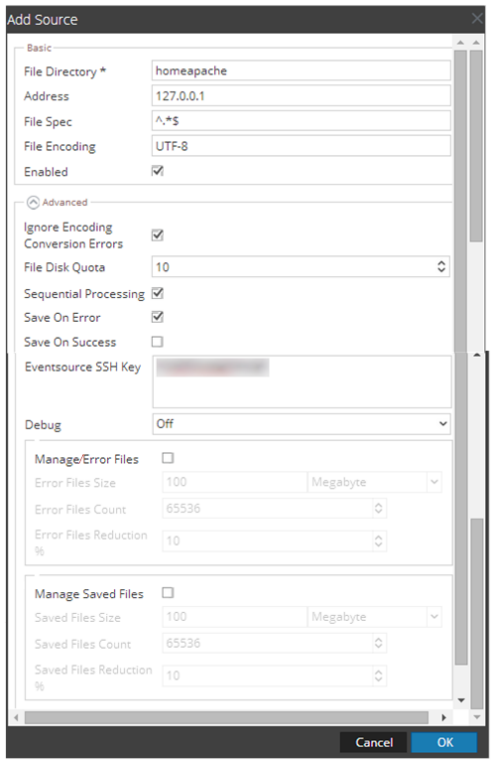


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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