RSA NetWitness Logs

Event Source Log Configuration Guide

RSA Certificate Manager

Last Modified: Wednesday, April 26, 2017

Event Source Product Information:

Vendor: RSA, The Security Division of EMC
Event Source: Certificate Manager
Versions: 6.8
Additional Download:

- BatchLauncher.vbs
- latestfile.vbs
- main.bat
- RSACMlog.conf
- test.bat
- tologs.vbs
- sftpagent.conf.rsacm

RSA Product Information:

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

To configure RSA Certificate Manager, you must complete the following tasks:

I. Configure RSA Certificate Manager

II. Set Up Windows Task Scheduler

III. Set up the SFTP Agent and NetWitness Log Collector

Configure RSA Certificate Manager

To configure RSA Certificate Manager:

1. Set up RSA Certificate Manager according to vendor instructions.
2. On the RSA Certificate Manager host, create a folder named **NetWitnessScripts** on the **C:** drive. Within the **NetWitnessScripts** folder, create a folder named **nwlogs**.
3. Within the **NetWitnessScripts/nwlogs** folder on the **C:** drive, create a folder named **logerrors**.
4. Download the **BatchLauncher.vbs** script, the **latestfile.vbs** script, the **main.bat** file, the **RSACMlog.conf** file, the **test.bat** file, and the **tologs.vbs** script from RSA Link, and paste them into the **NetWitnessScripts** folder. The files are located here: https://community.rsa.com/docs/DOC-58037
5. In the **RSACMlog.conf** file, specify the required folder paths.

   Note: When the scripts run on your RSA Certificate Manager machine, they create three text files named **FileList.txt**, **LatestFile.txt**, and **SentFileList.txt**. Do not delete these files from the **C:\NetWitnessScripts** folder. You need these files to collect logs from RSA Certificate Manager and send them RSA NetWitness Suite.

Set Up Windows Task Scheduler

To set up Windows Task Scheduler:

Warning: In the following procedure, create only one scheduled task.

1. On the RSA Certificate Manager host, click **Start** > **Settings** > **Control Panel**.
2. Click **Scheduled Task > Add Scheduled Task**.
3. In the Scheduled Task Wizard, click **Next**.
4. Select any application from the list, and click **Next**.
5. In the **Type a name for this task** field, type **RSACM**.
6. Under **Perform this task**, select **Daily**, and click **Next**.
7. Select the start time and start date, and click **Next**.
8. In the **user name** and **password** fields, enter your server logon credentials, and click **Next**.
9. Select **Open advanced properties for this task when I click Finish**, and click **Finish**.
10. On the **Task** tab of the Advanced Properties window, in the **Run** field, type **C:\WINDOWS\system32\wscript.exe "C:\NetWitnessScripts\BatchLauncher.vbs" "C:\NetWitnessScripts\main.bat"**.
11. On the **Schedule** tab, click **Advanced**.
12. Select **Repeat task**, and complete the fields as follows.

Field	Action
Every	Select how frequently you want RSA NetWitness Suite to receive logs from Certificate Manager. RSA recommends every 12 hours as the frequency.
Until	Select **Duration**.
Hour (s)	Type **24**.

13. Click **Apply**.

Set Up SFTP Agent and NetWitness Log Collector

To configure RSA NetWitness Suite, set up the SFTP Agent and 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

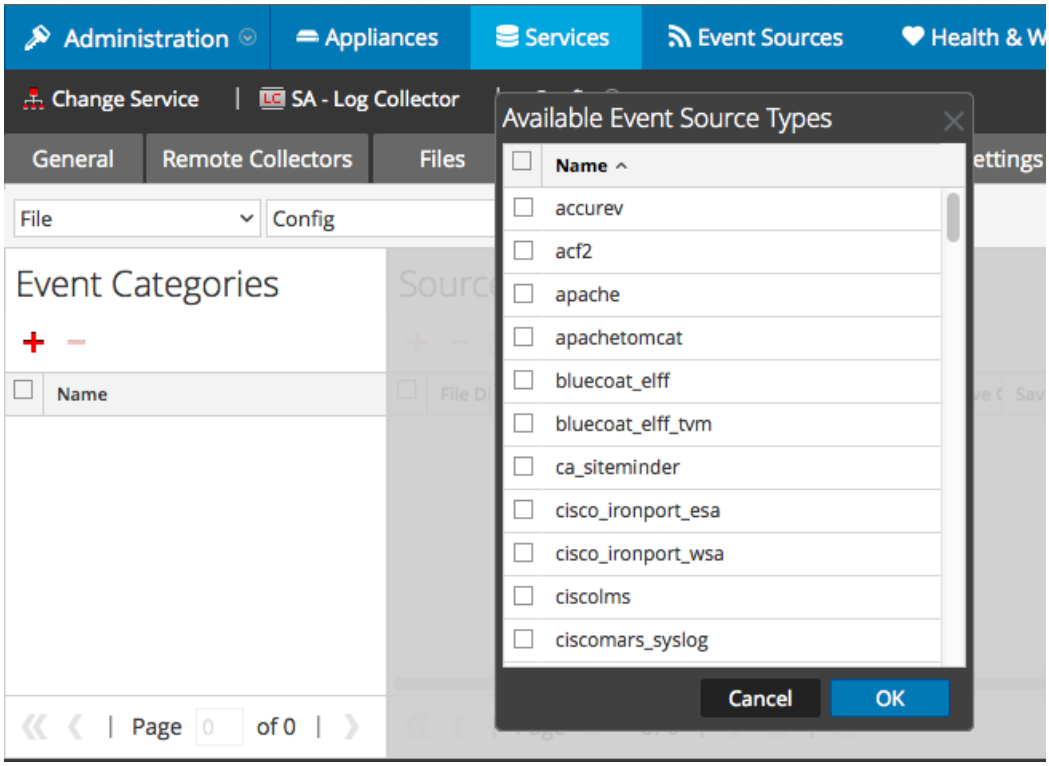
Perform the following steps to configure the Log Collector for File collection.

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 +.

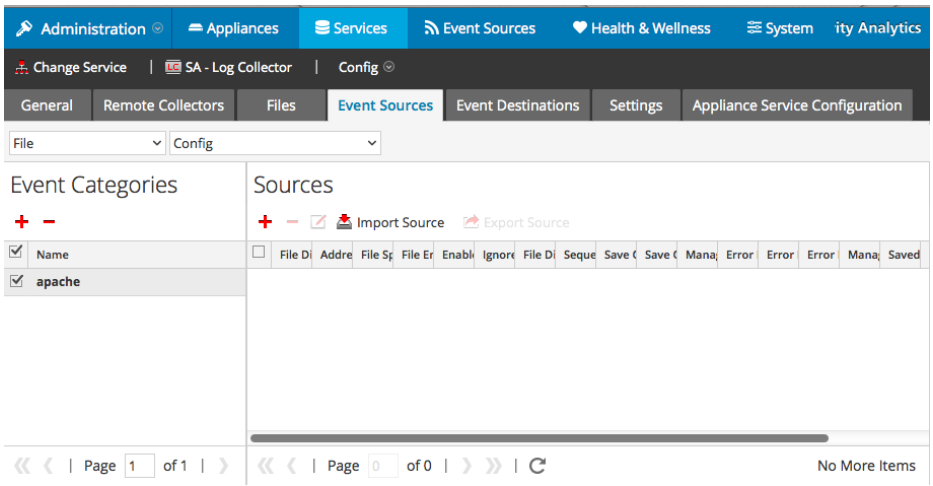
   The Available Event Source Types dialog is displayed.



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

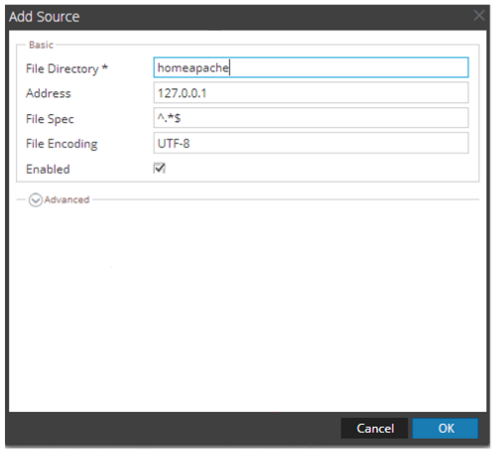
   Select **rsacm** from the **Available Event Source Types** dialog.

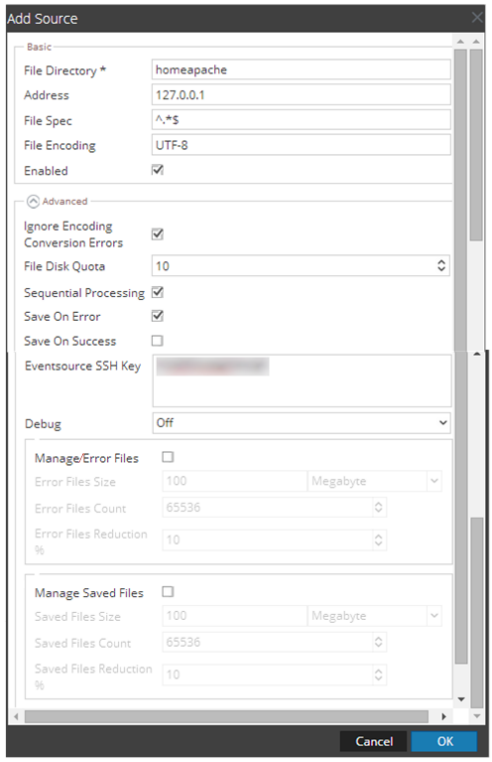
   The newly added event source type is displayed in the Event Categories panel.



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

The Add Source dialog is displayed.





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