RSA NetWitness Logs

Event Source Log Configuration Guide

RSA Adaptive Authentication (Hosted)

Last Modified: Friday, April 14, 2017

Event Source Product Information:

Vendor: RSA
Event Source: Adaptive Authentication (Hosted)
Supported Versions: 8.8, 8.9, 9.0, 9.1
Additional Downloads: sftpagent.conf.rsaaah

RSA Product Information:

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

RSA Adaptive Authentication (Hosted) Overview

RSA Adaptive Authentication (Hosted) is a risk-based two-factor authentication solution providing cost-effective protection for an entire user base. Adaptive Authentication secures online portals, SSL VPNs, and web access management portals for different types of organizations in the healthcare, insurance, enterprise, government, financial services, and other industries.

Based on the transparent two-factor authentication technology, Adaptive Authentication works behind the scenes to authenticate end users and transactions based on individual end user and device profiles.

To configure this event source, you need to download the daily log file from the Adaptive Authentication server, and then set up the SFTP and the File Reader Service.

Prepare the Log File

You must have RSA Adaptive Authentication (Hosted) configured so that it sends you a daily log file. The log file is sent in an encrypted, compressed format, so you need to decrypt and expand the file.

To prepare the Adaptive Authentication log file:

1. Ensure that you are receiving daily logs from the Adaptive Authentication server. If not, contact RSA Professional Services to enable this functionality.
2. The log file is sent with a .pgp extension, indicating that it is encrypted. Use your key to decrypt the file.
3. The output file from the decryption process is a ZIP archive. Expand the archive.
4. The output from the extraction process is a text file. Keep track of the name and path of this file.
5. When you configure the RSA NetWitness Suite SFTP Agent, set the directory parameter so that it matches the path of this file. For example, if you extract the file to **C:\AA_Hosted_Logs**, you should set the parameter as follows in the SFTP Agent configuration file:

   ```
   dir0=C:\AA_Hosted_Logs\
   ```

   Note: Each daily log file name includes a date and timestamp. As the number of files grows, you can delete the older files. The SFTP Agent transfers the information from the new file once only, when it is first placed into the monitored folder.

Set up the SFTP Agent and Configure Log Collector

You must complete these tasks to configure Atlassian Stash for File collection:

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

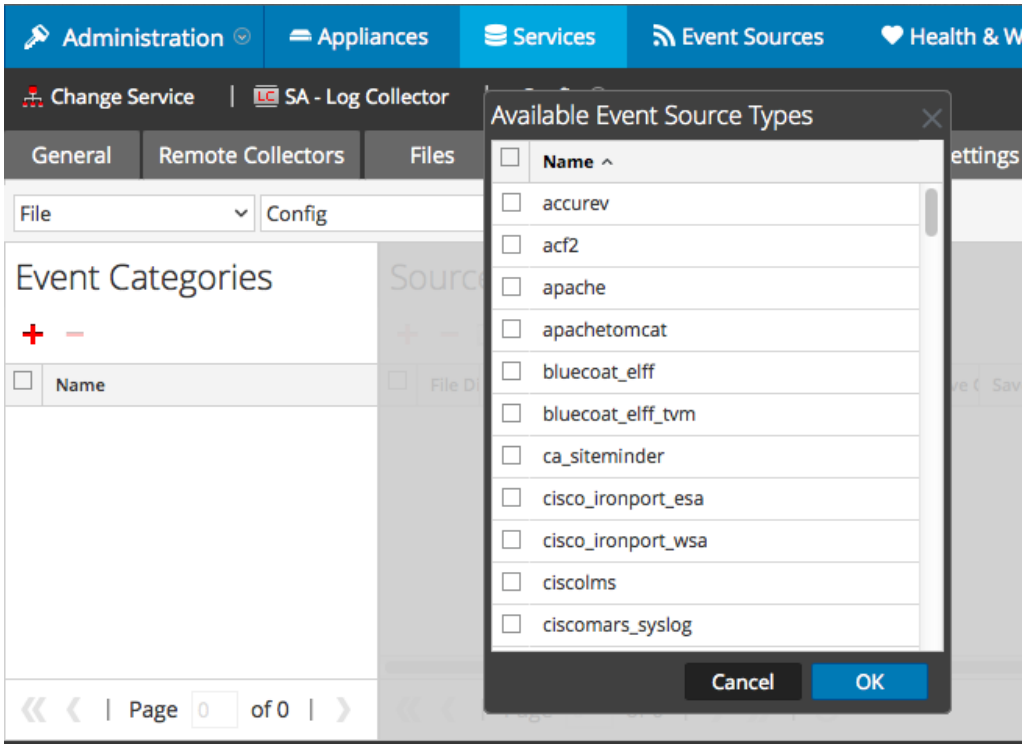
Perform the following steps to configure the Log Collector for File collection.

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 +.

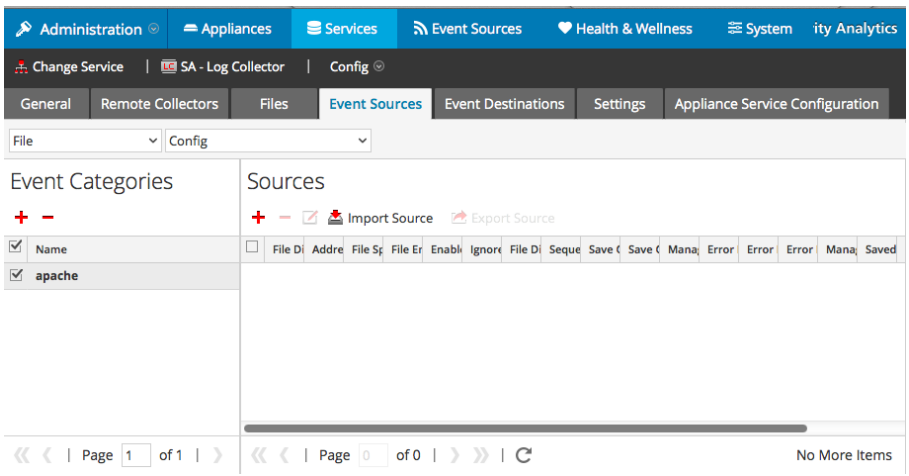
   The Available Event Source Types dialog is displayed.



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

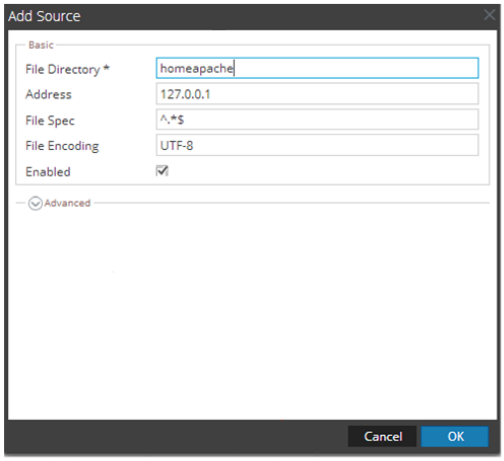
   Select **rsaaah** from the **Available Event Source Types** dialog.

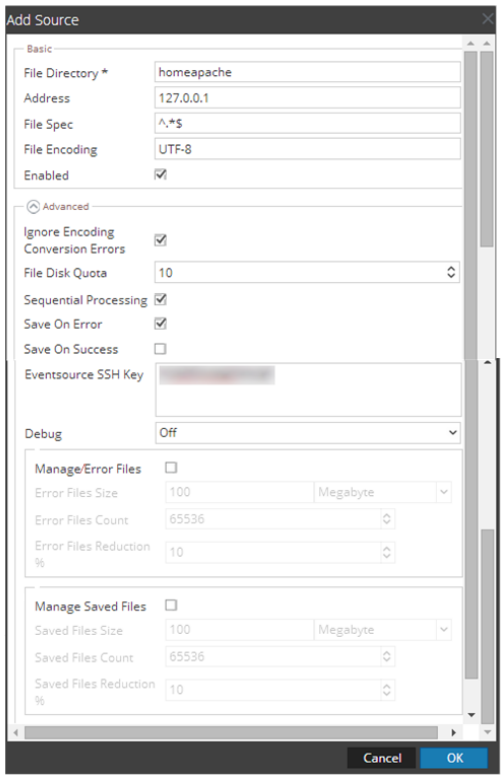
   The newly added event source type is displayed in the Event Categories panel.



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