RSA NetWitness Logs

Event Source Log Configuration Guide

HP OpenVMS

Last Modified: Friday, February 9, 2018

Event Source Product Information:

Vendor: HP
Event Source: OpenVMS
Version: All
Additional Downloads:

- ovmsextr.com
- ovmsextr.cfg
- openvmsextr.com

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: openvms
Collection Method: File
Event Source Class.Subclass: Host.Midrange

To configure HP OpenVMS, you must complete these tasks:

I. Configure HP OpenVMS to generate logs

II. Configure the Log Collector for File Collection

Configure HP OpenVMS to Generate Logs

To configure HP Open VMS:

1. Complete the following steps to download files from RSA Link:
   a. Go to RSA Link for NetWitness, to the following link: https://community.rsa.com/docs/DOC-53460. This is the Additional Downloads page for HP OpenVMS.
   b. Download the **ovmsextr.cfg** file.
   c. Depending on your version, download one of the following files:
      - For version 8.3 and earlier, download **ovmsextr.com**.
      - For version 8.4 and later, download **openvmsextr.com**.
   d. Copy the downloaded files to the HP machine.
2. In the **ovmsextr.cfg** file, edit the following fields.

Field	Description
ENVISION	Enter the IP address for the RSA NetWitness Suite Log Collector.
USERNAME	Enter the username that you have set up for your NetWitness SFTP user.
PASSWORD	Enter the password for the SFTP user.
DIRECTORY	(Optional) Enter the directory to which the log data should be sent.

Note: The **DIRECTORY=** line is required; however, the actual value for it is optional.

3. In the .com file, to change the FTP schedule from the default, every hour, modify the **SUBMIT** command at the beginning of the file.
4. Using a VMS account that has either the READALL or SETPRV privilege, run the .com script manually.

After you run the script once, the script will run automatically.

Note: You can stop the job by deleting the queue entry. Use the following command:

```
delete /entry=entry-number sysq_batch
```

where ***entry-number*** is the actual entry number for the job.

Configure the Log Collector for File Collection

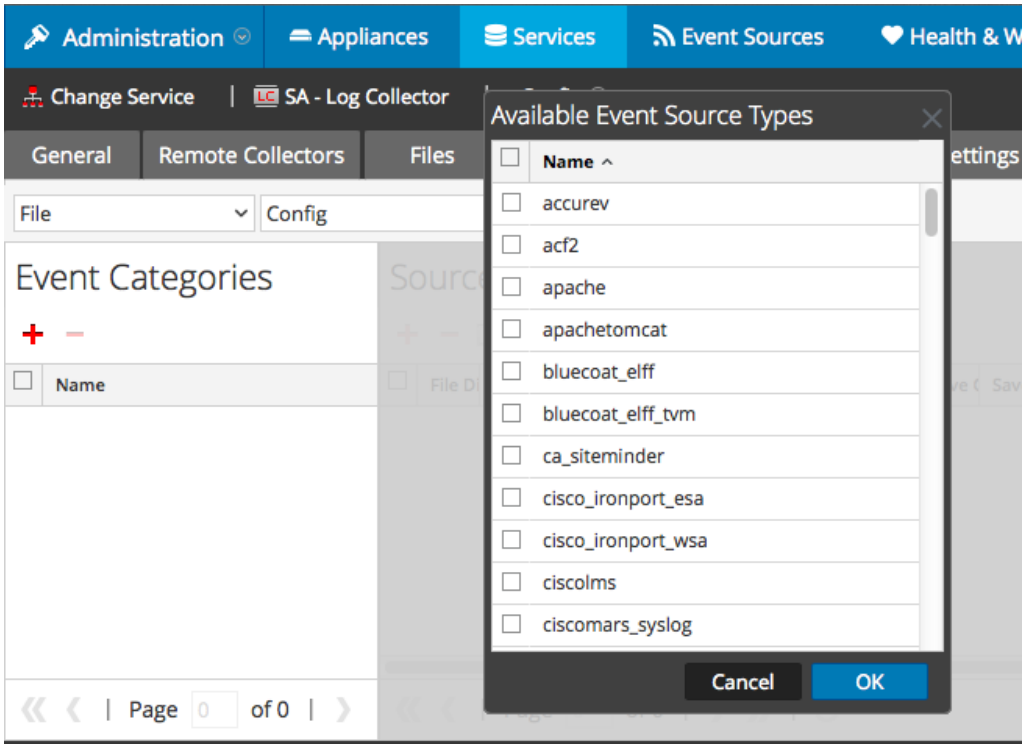
Perform the following steps to configure the Log Collector for File collection.

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.

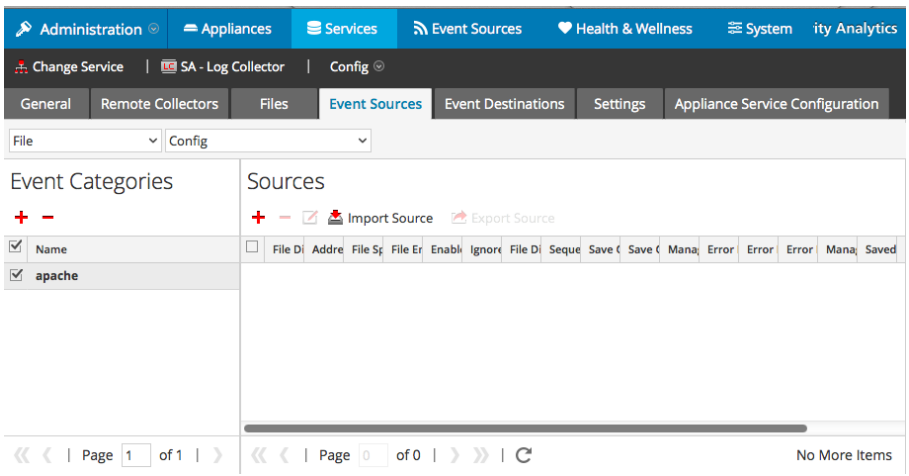


5. Select the correct type from the list, and click **OK**.

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

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

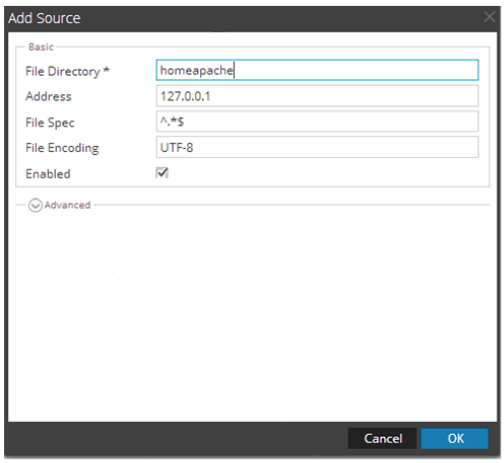
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

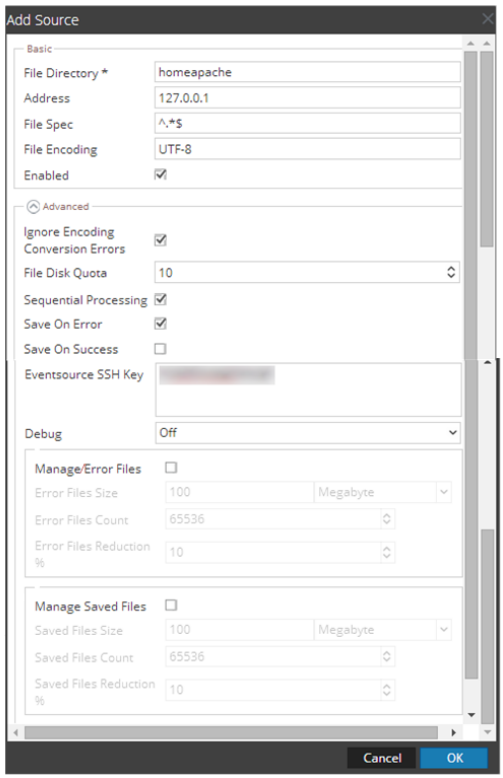


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.