RSA NetWitness Logs

Event Source Log Configuration Guide

Kernel Based Virtual Machine

Last Modified: Friday, May 19, 2017

Event Source Product Information:

Vendor: Open Source
Event Source: Linux KVM
Versions: 2.6.32-220
Additional Downloads: nicsftpagent.conf.kvm, kvm_rules.txt

RSA Product Information:

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

To configure Kernel Based Virtual Machine, complete the following tasks:

I. Configure Kernel Based Virtual Machine

II. Set Up the SFTP Agent and Configure the NetWitness Log Collector

Configure Kernel Based Virtual Machine

To configure Kernel Based Virtual Machine:

1. Download the Kernel Based Virtual Machine additional file, **kvm_rules.txt**, from RSA Link here: https://community.rsa.com/docs/DOC-53587
2. Open the **/etc/audit/audit.rules** file, and add the rules from the **kvm_rules.txt** file.
3. Restart the auditd daemon with the following command:

   ```
   # service auditd restart
   ```

Configure File Collection for RSA NetWitness Suite

To complete the File collection configuration, perform these tasks:

I. Set up SFTP Agent

II. Configure the RSA NetWitness Suite 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

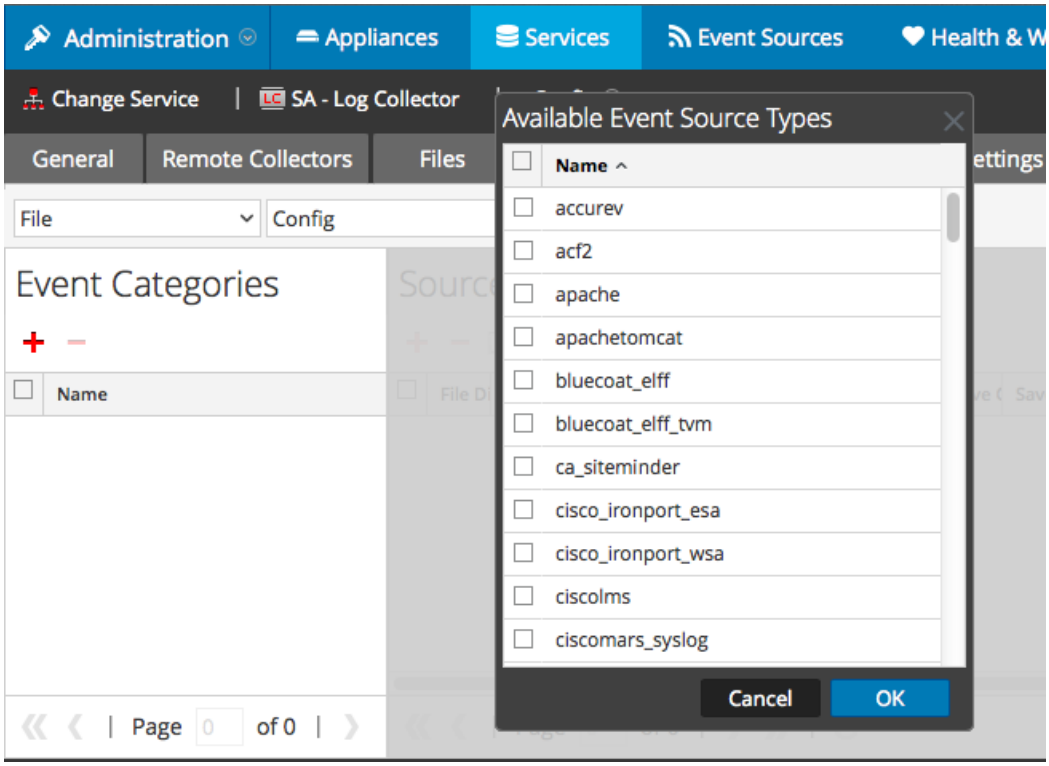
Perform the following steps to configure the Log Collector for File collection.

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 +.

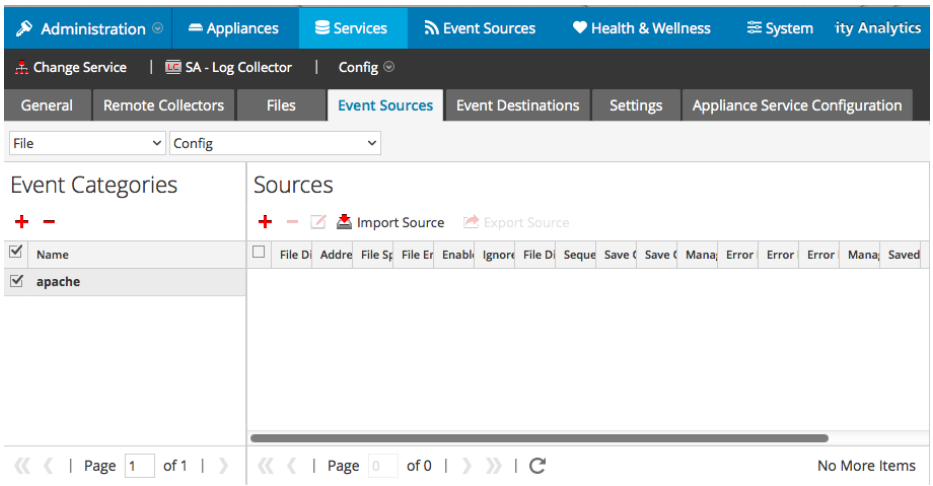
   The Available Event Source Types dialog is displayed.



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

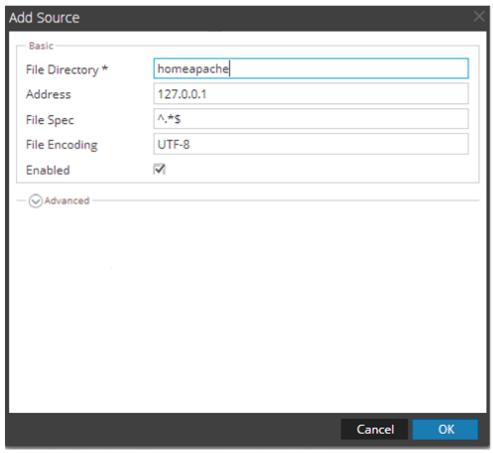
   Select **kvm** from the **Available Event Source Types** dialog.

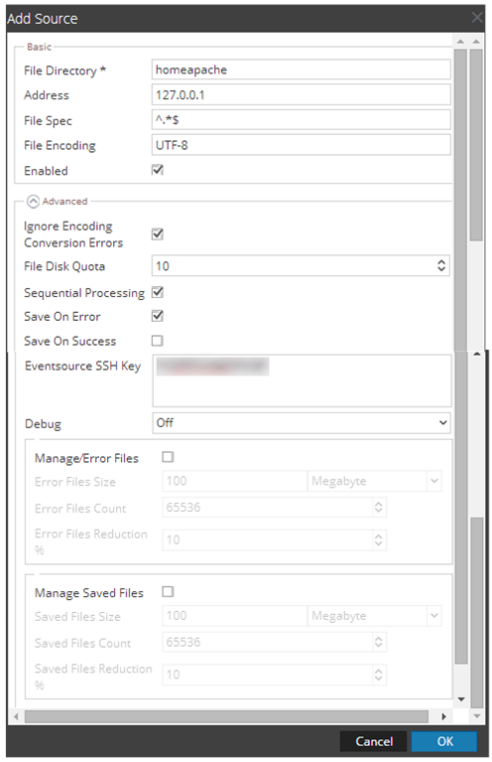
   The newly added event source type is displayed in the Event Categories panel.



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