RSA NetWitness Logs

Event Source Log Configuration Guide

Microsoft URLScan

Last Modified: Tuesday, November 7, 2017

Event Source Product Information:

Vendor: Microsoft
Event Source: URLScan
Version: 3.x

> **Note:** RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

Additional Download: sftpagent.conf.msurlscan

RSA Product Information:

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

You must complete these tasks to configure Microsoft URLScan to work with RSA NetWitness Suite:

I. Configure File Collection

    i. Set up the SFTP Agent

    ii. Configure the RSA NetWitness Suite Log Collector for File Collection

II. Configure the Microsoft URLScan event source

Configure File Collection

Download and configure the SFTP agent and configuration sample file, then configure File Collection on RSA NetWitness Suite.

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 SFTP Shell Script File Transfer

Configure the Log Collector for File Collection

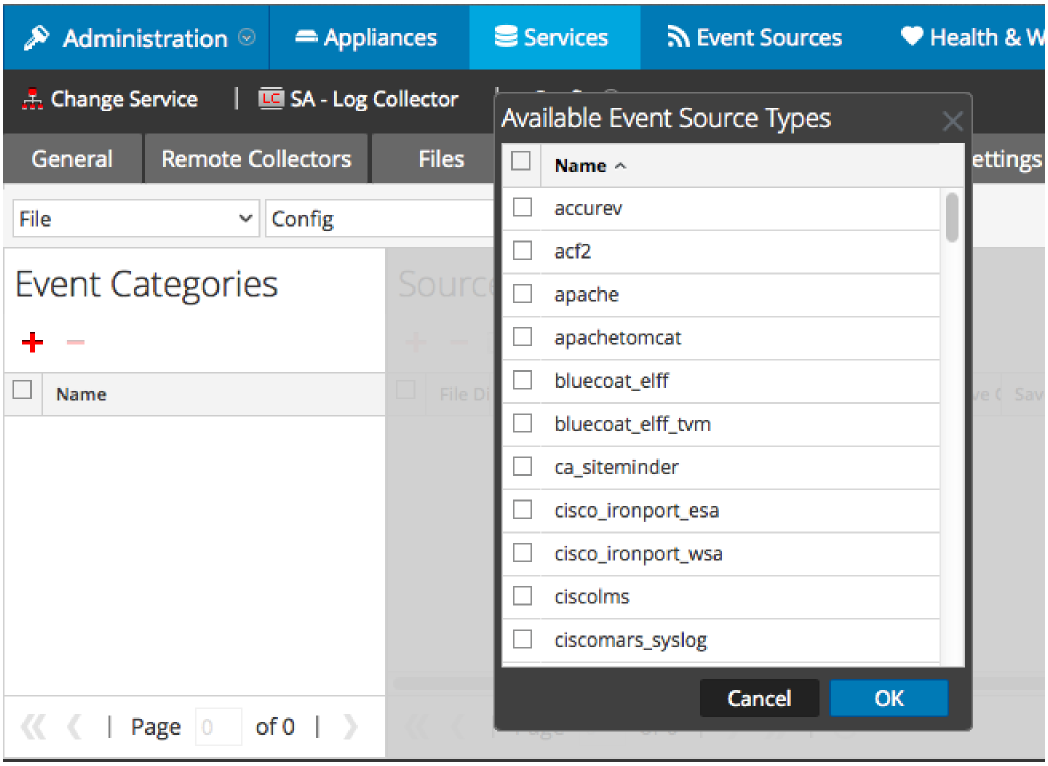
Perform the following steps to configure the Log Collector for File collection.

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.



Available Event Source Types

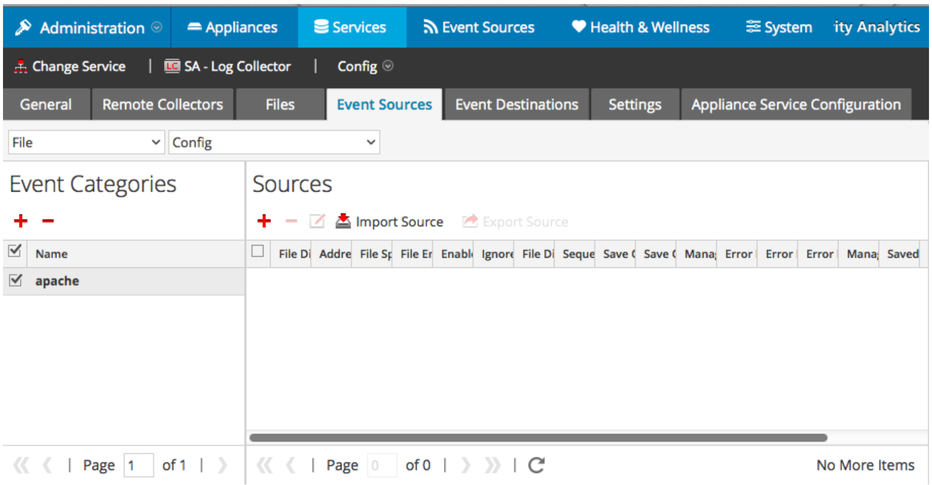
□	Name ^
□	accurev
□	acf2
□	apache
□	apachetomcat
□	bluecoat_elff
□	bluecoat_elff_tvm
□	ca_siteminder
□	cisco_ironport_esa
□	cisco_ironport_wsa
□	ciscolms
□	ciscomars_syslog

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

   Select **msurlscan_tvm** 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.



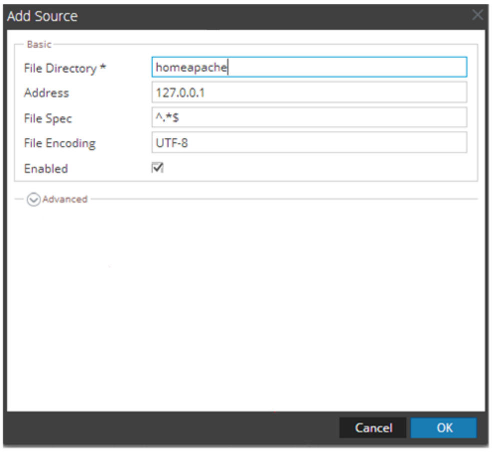
☑	Name
☑	apache

□	File Di	Addre	File Sp	File Er	Enabl	Ignore	File Di	Seque	Save (	Save (	Mana	Error	Error	Error	Mana	Saved

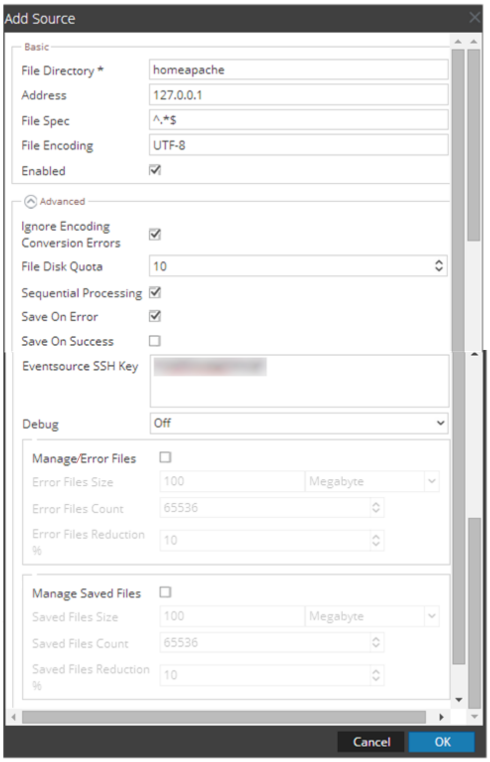
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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.



File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑



File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑

Ignore Encoding Conversion Errors ☑
File Disk Quota 10
Sequential Processing ☑
Save On Error ☑
Save On Success □
Eventsource SSH Key [redacted]
Debug Off

Manage/Error Files □
Error Files Size 100 Megabyte
Error Files Count 65536
Error Files Reduction % 10

Manage Saved Files □
Saved Files Size 100 Megabyte
Saved Files Count 65536
Saved Files Reduction % 10

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.

Configure the Microsoft URLScan Event Source

On the Microsoft URLScan event source, you need to edit the **urlscan.ini** file.

On the URLScan event source, perform the following steps:

1. Navigate to the `C:\Windows\System32\inetsrv\urlscan\` folder.
2. Open the **urlscan.ini** file in a text editor.
3. Ensure **EnableLogging** is set to 1:

   ```
   EnableLogging=1
   ```

4. Set **LoggingDirectory** to match the path set in the **sftpagent.conf** file for the **dir0** parameter. By default, the sftpagent.conf file has the following setting:

   ```
   dir0=C:\Windows\System32\inetsrv\urlscan\logs
   ```

   If you keep the default in the conf file, then you need to set LoggingDirectory as follows:

   ```
   LoggingDirectory=Logs
   ```

5. Save the file.
6. Restart the IIS Admin service.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.