RSA NetWitness Logs

Event Source Log Configuration Guide

Citrix Access Gateway

Last Modified: Thursday, May 11, 2017

Event Source Product Information:

Vendor: Citrix
Event Source: Access Gateway
Versions: 4.5, 4.6, and 5.0

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: citrixag
Collection Method: Syslog, File
Event Source Class.Subclass: Security.VPN

RSA NetWitness Suite supports two collection methods for the Citrix Access Gateway event source:

- Configure File Collection for version 5.0
- Configure Syslog Collection for version 4.6 and earlier

Configure File Collection for version 5.0

You must complete these tasks to configure Citrix Access Gateway for File collection:

I. Set up the SFTP Agent

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

III. Enable Logging on Citrix AG

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

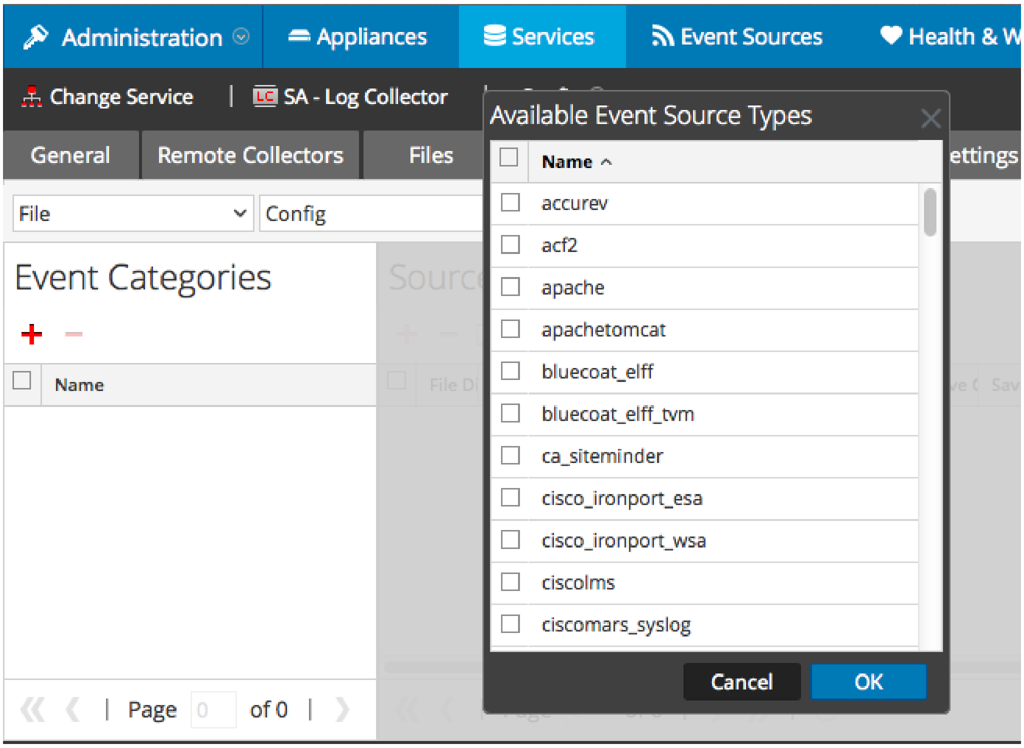
Perform the following steps to configure the Log Collector for File collection.

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 +.

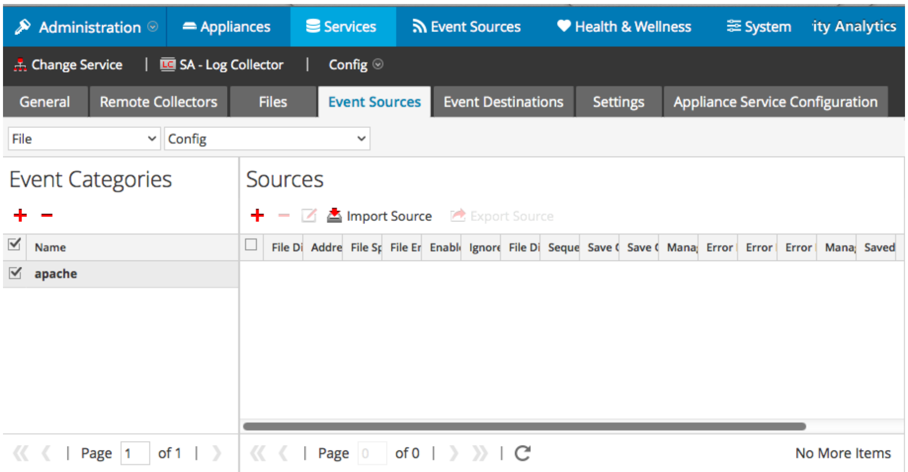
   The Available Event Source Types dialog is displayed.



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

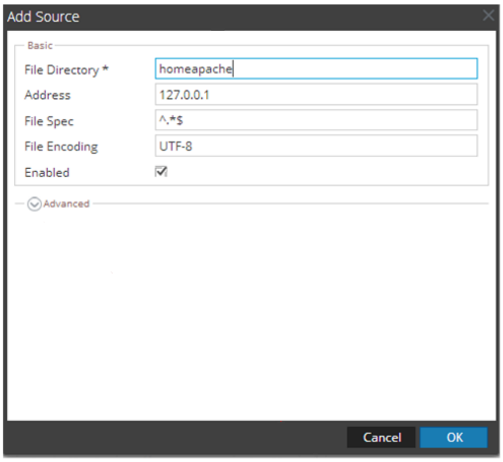
   Select **citrixag** from the **Available Event Source Types** dialog.

   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.

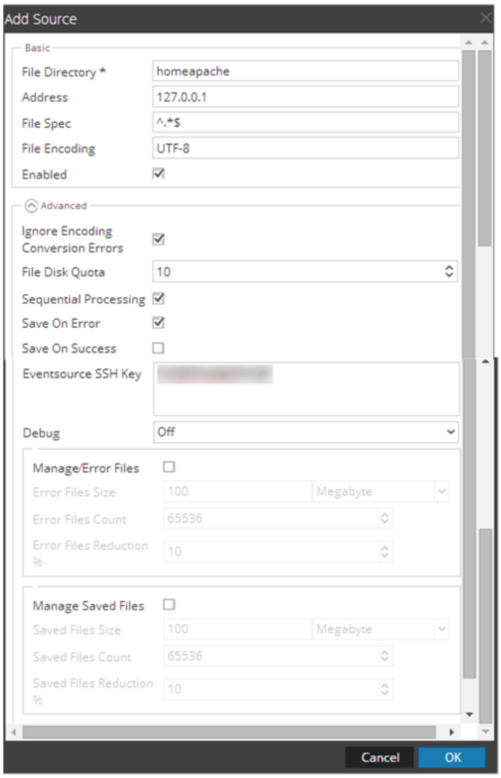


Add Source

Basic

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

Advanced



Add Source

Basic

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

Advanced

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.

Enable Logging on Citrix AG to send logs to RSA NetWitness Suite for version 5.0 and later

To enable logging on Citrix AG to send logs to RSA NetWitness Suite for version 5.0 and later:

1. Log on to the Citrix Access Gateway Administration Tool GUI.

2. Click on the **Management** tab.

3. On the left under **System Administration** select **Logging**.

4. Add **Server** and enter the IP address of the RSA NetWitness Suite Log Collector.

   For **Transfer protocol**, select **FTP**.

For **Port**, enter **21**.

For **Remote directory**, enter **/CITRIX_<*IP-address*>**

where *IP-address* is the IP address of the Citrix Access Gateway server.

For **Log type**, select **Audit**.

Configure Syslog Collection for version 4.6 and earlier

To configure Syslog collection for the Citrix Access Gateway you must:

- Configure Citrix Access Gateway versions 4.0 or 4.6 to Send Logs to RSA NetWitness Suite
- Configure RSA NetWitness Suite for Syslog Collection

Configure Citrix Access Gateway versions 4.0 or 4.6 to Send Logs to RSA NetWitness Suite

To configure Citrix Access Gateway versions 4.0 or 4.6 to send logs to RSA NetWitness Suite:

1. Log on to the Citrix Access Gateway Administration Tool.
2. Maximize **This Gateway**.
3. Click the **Logging/Settings** tab.
4. In the **Syslog settings** section, do the following:
   a. In the **Server** field, enter the IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.
   b. From the **Facility** drop-down list, select the appropriate value.
   c. In the **Broadcast interval (mins)** field, enter an integer value for how often you want log output.
   d. Click **Submit**.
   e. When the IP address pop-up window opens, click **OK**.
   f. When the Re-Initialization pop-up window opens, click **Initialize This Gateway**.

Configure RSA NetWitness Suite for Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:
   - If you see ▶ Start Capture , click the icon to start capturing Syslog.
   - If you see ■ Stop Capture , you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog 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 either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the

Advanced parameters as necessary.

Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Trademarks