RSA NetWitness Platform

Event Source Log Configuration Guide

Apache Tomcat Server

Last Modified: Tuesday, January 14, 2020

Event Source Product Information:

Vendor: Apache
Event Source: Tomcat Server
Versions: 6.0, 7.0, 8.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 Downloads: sftpagent.conf.apachetomcat

Link: Apache Tomcat Server Additional Downloads

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: apachetomcat
Collection Method: File, Syslog (for 8.0.14 only)
Event Source Class.Subclass: Host.Web Logs

To configure Apache Tomcat, perform the following tasks:

- Configure File Collection
- Configure Syslog Collection (Unix/Linux only)

Note: For Apache Tomcat, you can choose to configure Syslog or File collection, but not both.

Configure File Collection

To configure file collection for Apache Tomcat, perform the following tasks:

I. Depending on your operating system, perform one of the following tasks:

- Configure File Collection on Windows, or
- Configure File Collection on Linux

II. Set up the SFTP Agent

III. Set up the File Service

Configure File Collection on Windows

To configure Apache Tomcat on Windows:

On the Apache Tomcat Server, in the **Server.xml** file, verify that the following section is present and not commented out:

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs" prefix="access_log." suffix=".txt"
pattern="%h||%l||%u||%t||%m||%v||%U||%q||%H||%s||%b||%{Referer}i||%{User-Agent}i||%
{Cookie}i"
resolveHosts="false"/>
```

Configure File Collection on Linux

To configure File Collection for Apache Tomcat on Linux:

On the Apache Tomact Server, in the **Server.xml** file, verify that the following section is present and not commented out:

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs" prefix="access_log." suffix=".txt"
pattern="%h||%l||%u||%t||%m||%v||%U||%q||%H||%s||%b||%{Referer}i||%{User-Agent}i||%
{Cookie}i"
resolveHosts="false"/>
```

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

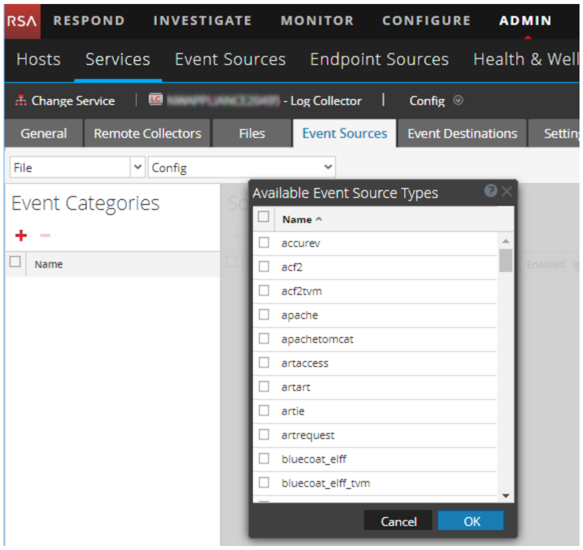
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **ADMIN** > **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.

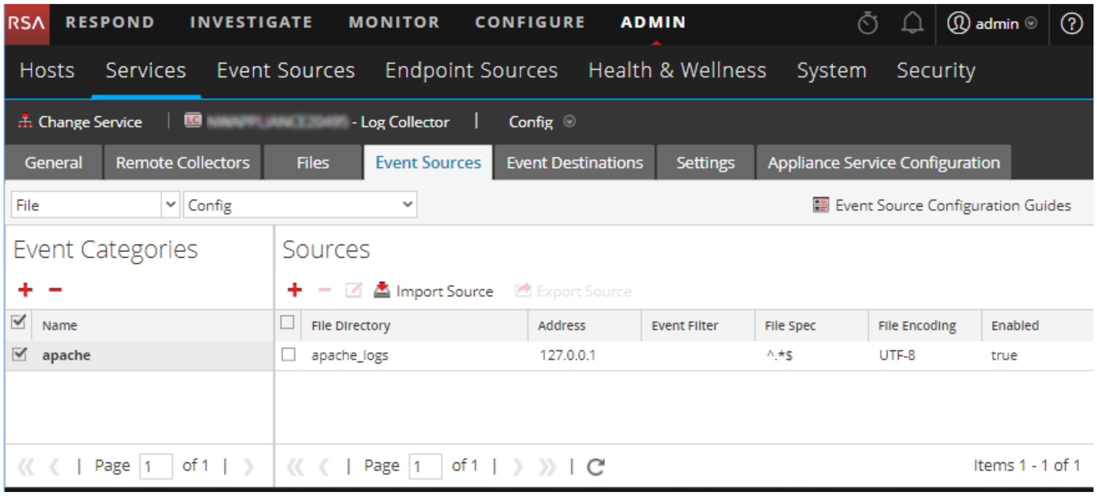


5. Select the correct type from the list, and click **OK**.

   Select **apachetomcat** 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.



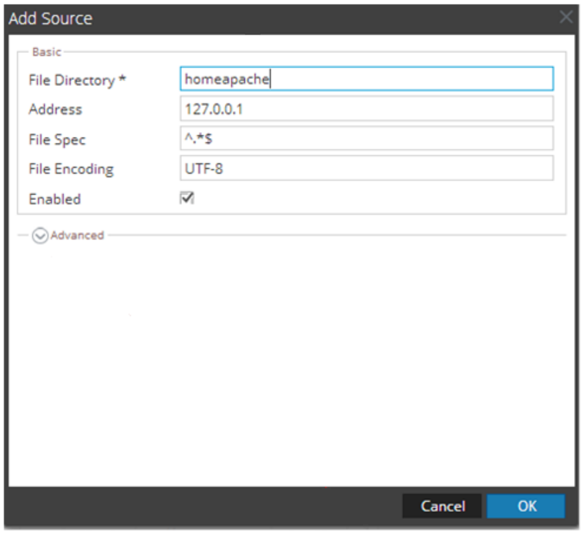
	Name
☑	apache

	File Directory	Address	Event Filter	File Spec	File Encoding	Enabled
□	apache_logs	127.0.0.1		^.*$	UTF-8	true

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.



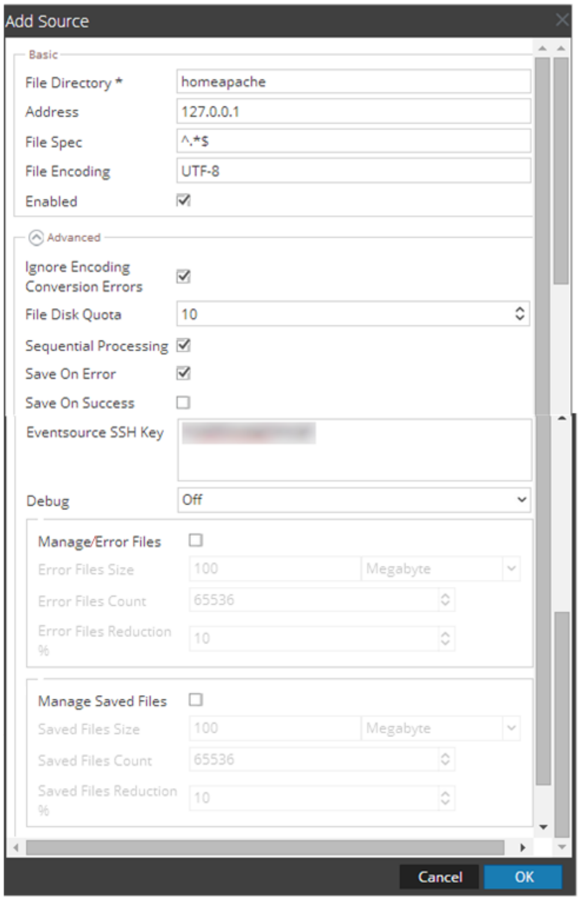
File Directory * homeapache

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 Syslog Collection

Perform the following tasks to configure Syslog collection:

- Configure Syslog on the Apache Tomcat event source
- Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog on the Apache Tomcat Event Source

On Linux, you can collect access logs via Syslog.

To configure Syslog on Apache Tomcat:

1. Add the following text to the **Host** element in **\usr\local\tomcat8\conf\Server.xml**:

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="/var/log/"
   prefix="tomcat_access_log" suffix="" pattern="%m:
   %h||%l||%u||%t||%m||%v||%U||%q||%H||%s||%b||%{Referer}i||%{User-Agent}i||%
   {Cookie}i resolveHosts="false" rotatable="false"
/>
```

2. Save the **Server.xml** file, and do the following:

   a. Change directory to `/usr/local/tomcat8/bin`

   b. Stop the Apache Tomcat server, using the following command: `./shutdown.sh`

   c. Restart the Apache Tomcat server, using the following command: `./startup.sh`

3. Add the following to the end of the **/etc/rsyslog.conf** file:

```
#### MODULES ####
$ModLoad imfile # load the imfile input module
# Watch /var/log/
$InputFileName /var/log/tomcat_access_log
$InputFileTag %APACHETOMCAT-
$InputFileStateFile state-apachetomcat-access
$InputRunFileMonitor
*.* @ipaddress
```

   where ipaddress is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

4. Save **/etc/rsyslog.conf** and restart the **rsyslog** service.

Configure RSA NetWitness Platform 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 **ADMIN** > **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 **ADMIN** > **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.

After 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

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