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**.
- 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.

RSA RESPOND INVESTIG	GATE MONITOR CONF	IGURE ADMIN	Ō û admin ⊗ ?
Hosts Services Event	Sources Endpoint Sour	ces Health & Wellnes	ss System Security
A Change Service	- Log Collector Co	nfig ©	
General Remote Collectors	Files Event Sources Ev	ent Destinations Settings	Appliance Service Configuration
File 🗸 Config	~		📰 Event Source Configuration Guides
Event Categories	Sources		
+ -	🕂 🗕 🗹 📥 Import Source 🛛	Export Source	
☑ Name	File Directory	Address Event Filter	File Spec File Encoding Enabled
☑ apache	apache_logs	127.0.0.1	^.*\$ UTF-8 true
<pre></pre>	<pre></pre>	» C	ltems 1 - 1 of 1

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.

Basic File Directory * Address 127.0.0.1 File Spec A*s File Encoding UTF-8 Enabled © Advanced Ignore Encoding Conversion Errors Ø Save On Error Ø Save On Success Eventsource SSH Key Debug Off Manage/Error Files Error Files Size 100 Kerror Files Reduction 10 Saved Files Size 100 Manage Saved Files Saved Files Reduction 10 Saved Files Reduction 10 Saved Files Reduction			P	Add Source			
File Directory* Address 127.0.0.1 File Spec Address 11 Conversion Errors Image Error Save On Error Save On Error Save On Error Debug Off Image Error Files Error Files Size 100 Manage Saved Files Size 100 Manage Saved Files Size 100 Manage Saved Files Size 100 Megabyte Saved Files Size 100 Megabyte Saved Files Size 100 Megabyte Saved Files Reduction 10 Saved Files Reduction				Basic			
Address 127.0.0.1 File Spec ^.*\$ File Encoding UTF-8 Enabled Ø Concel OK Advanced Ignore Encoding Ø Save On Error Ø Save On Error Ø Save On Success Eventsource SSH Key Debug Off ✓ Manage/Error Files □ Error Files Size 100 Megabyte ♥ Error Files Size 100 Megabyte ♥ Error Files Size 100 Megabyte ♥ Saved Files Count 65536 Saved Files Count 65536 Saved Files Count 65536				File Directory *	homeapache		
File Spec ^.*5 File Encoding UTF-8 Enabled Image: Encoding Conversion Errors Image: Encoding Save On Error Image: Eventsource SSH Key Debug Off Debug Off Image: Error Files Image: Error Files Error Files Size 10 Error Files Size 10 Error Files Size 10 Image: Error Files Image: Error Files Error Files Size 10 Image: Error Files Image: Error Files Error Files Size 10 Image: Error Files Image: Error Files Error Files Reduction 10 Image: Saved Files Image: Saved Files Saved Files Reduction 10 Image: Saved Files Reduction 10 Image: Saved Files Reduction Image: Saved Files Saved Files Reduction Image: Saved Files Reduction Image: Saved Files Reduction Image: Saved Files				Address	127.0.0.1		
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 Debug Off V Manage/Error Files Error Files Size 10 Error Files Size 10 Saved Files Size 10 Saved Files Size Saved Files Reduction 10 Saved Files Size Saved Files Reduction Saved Files Reduction				File Spec	^.*s		
Enabled pache .1 Sequential Processing Save On Error Save On Error Save On Success Eventsource SSH Key Debug Off Wanage/Error Files Error Files Size 10 Manage Saved Files Saved Files Size Saved Files Size Saved Files Size Saved Files Saved Files Size				File Encoding	UTF-8		
Advanced Ignore Encoding Conversion Errors File Disk Quota 10 Sequential Processing Save On Error Save On Success Eventsource SSH Key Debug Off Manage/Error Files Error Files Size 10 Manage Saved Files Saved Files Size 10 Manage Saved Files Saved Files Size 10 Saved Files Reduction 10				Enabled			
Ignore Encoding Conversion Errors N1 Sequential Processing Save On Error Save On Error Save On Success Eventsource SSH Key Debug Off V Manage/Error Files Error Files Size 100 Manage Saved Files Saved Files Size 100 Manage Saved Files Saved Files Count Saved Files Count Saved Files Count Saved Files Reduction 10				Advanced			
pache D.1 Sequential Processing Ø Save On Error Ø Save On Success Eventsource SSH Key Debug Off Manage/Error Files Error Files Size 10 Ø6 Manage Saved Files Saved Files Size 10 Saved Files Size 10 Ø6			×	Ignore Encoding Conversion Errors	\checkmark		
3.1 Save On Error Save On Success Eventsource SSH Key Debug Off Manage/Error Files Error Files Size 100 Megabyte Y Saved Files Size Saved Files Size 10 % Saved Files Size 10 % Saved Files Size 10 %	[homeapache		File Disk Quota	10		0
Save On Error Save On Success Eventsource SSH Key Debug Off Manage/Error Files Error Files Size Error Files Size Error Files Count 65536 Error Files Count Saved Files Size Saved Files Size Saved Files Size Saved Files Count Saved Files Reduction To Saved Files Reduction Saved Files Reduction Saved Files Count Saved Files Count Saved Files Count Saved Files Count Saved Files Count Saved Files Reduction To Saved Files Reduction Saved Files Reduction To Saved Files Reduction Saved Files Reduction Saved Files Reduction Saved Files Reduction Saved Files Reduction Saved Files Reduction Saved Files Reduction To Saved Files Reduction Saved Files Reducti	127	.0.0.1		Sequential Processing	\checkmark		
Save On Success Eventsource SSH Key Debug Off Manage/Error Files Error Files Size 100 Megabyte Fror Files Count 65536 Error Files Reduction 10 Manage Saved Files Saved Files Size 100 Megabyte Saved Files Size 100 Megabyte Saved Files Count Saved Files Coun	^.*s			Save On Error	\checkmark		
Eventsource SSH Key Debug Off Manage/Error Files Error Files Size 100 Manage Saved Files Saved Files Size 100 Manage Saved Files Saved Files Count 65536 Saved Files Count Saved Files Reduction	UTF-	8		Save On Success			
Cancel OK Cancel OK Other in the second seco	\checkmark			Eventsource SSH Key			
Debug Off Manage/Error Files							
Cancel OK				Debug	Off		~
Manage/Error Files □ Error Files Size 100 Megabyte ✓ Error Files Reduction 10 ♦ Manage Saved Files □ ✓ Saved Files Size 100 Megabyte ✓ Saved Files Count 65536 ♦ ✓ Saved Files Size 100 Megabyte ✓ Saved Files Count 65536 ♦ ♦ Saved Files Reduction 10 ♦ ♦					-		
Cancel OK Cance				Manage/Error Files	400		
Cancel OK Cancel OK				Error Files Size		Megabyte	v
Cancel OX Cancel				Error Files Count		0	
Cancel OK Saved Files Size 100 Megabyte ~ Saved Files Count 65536 Saved Files Reduction 10 % %				Error Files Reduction %		٥	
Cancel OK Saved Files Size 100 Megabyte Saved Files Count 65536 Saved Files Reduction 10 Save				Manage Saved Files			
Saved Files Count 65536 O Saved Files Reduction 10 O			Cancel OK	Saved Files Size		Megabyte	\sim
Saved Files Reduction 10				Saved Files Count		0	
				Saved Files Reduction %		٥	
				<		6	•

- 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**.
- 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.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

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