NetWitness® Platform

Apache Tomcat Event Source Log Configuration Guide

NETWITNESS
Platform

Apache Tomcat Server

Last Modified: Monday, December 2, 2024

Event Source Product Information:

Vendor: Apache

Event Source: Tomcat Server

Versions: 6.0, 7.0, 8.x

Note: NetWitness supports the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case in the NetWitness Community Portal for support.

Additional Downloads: sftpagent.conf.apachetomcat

Link: Apache Tomcat Server Additional Downloads

NetWitness Product Information:

Supported On: NetWitness Platform 12.3 and later

Event Source Log Parser: apachetomcat

Collection Method: File, Syslog (for 8.0.14 only)

Event Source Class.Subclass: Host.Web Logs

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

November 2024

Contents

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 NetWitness Link:

- To set up the SFTP agent on Windows, seeInstall 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

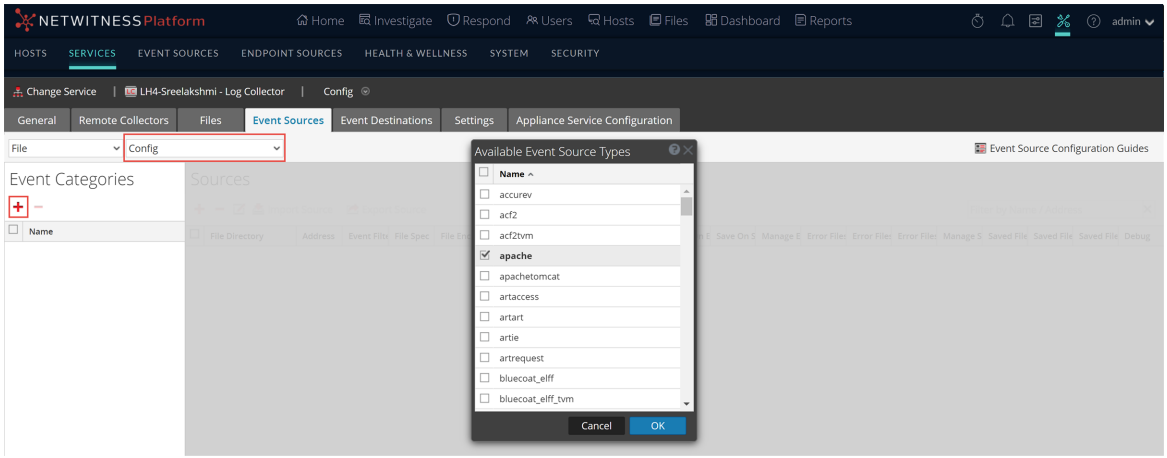
Perform the following steps to configure the Log Collector for File collection.

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.

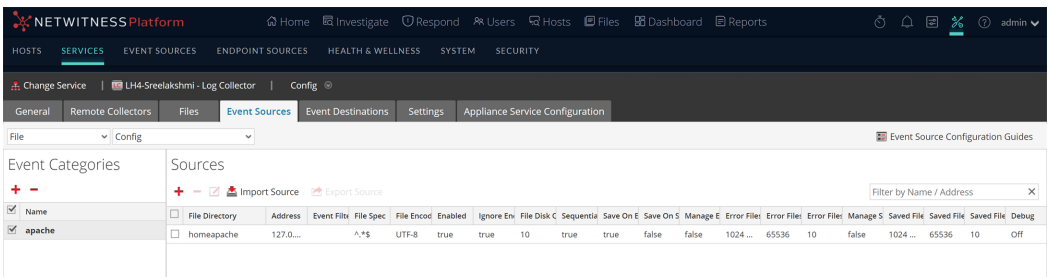


5. Select the correct type from the list and click **OK**.

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

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

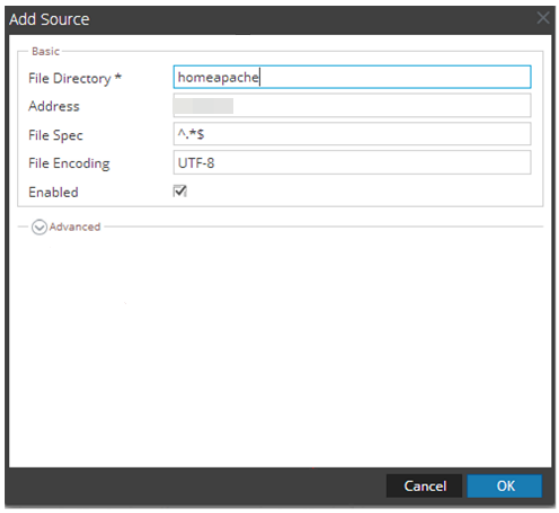
Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

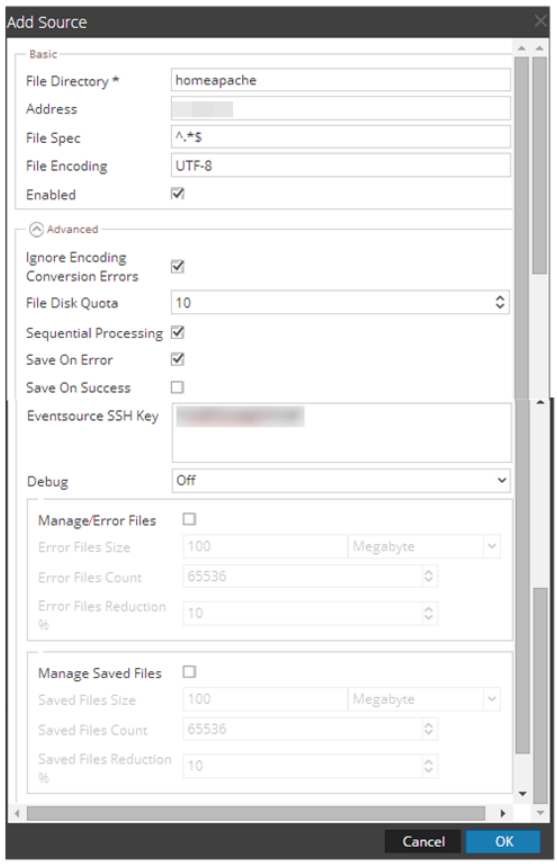


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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.





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 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 only need to configure either the Log Decoder or the Remote Log Collector for Syslog, not both.

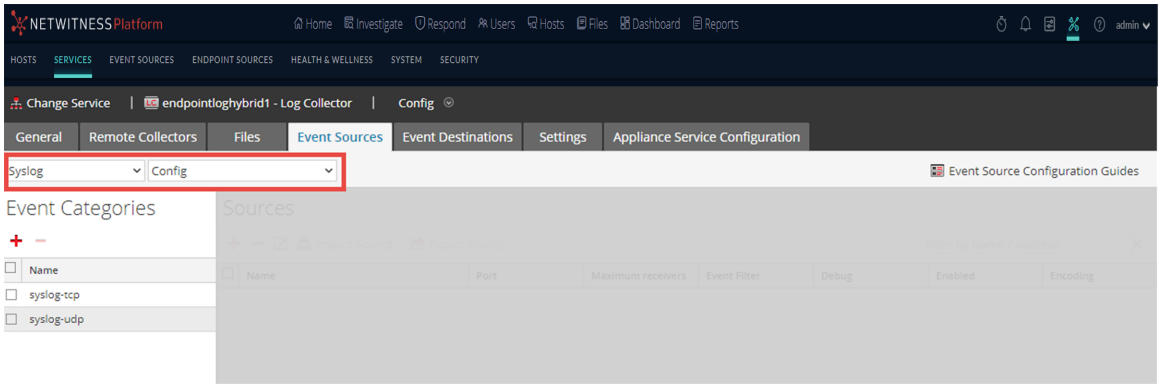
To configure Log Decoder for Syslog Collection

1. In the NetWitness Platform menu, select (Admin) > **Services**.
2. In the **Services** grid, choose 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 Remote Log Collector for Syslog Collection

1. In the NetWitness Platform menu, go to (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.

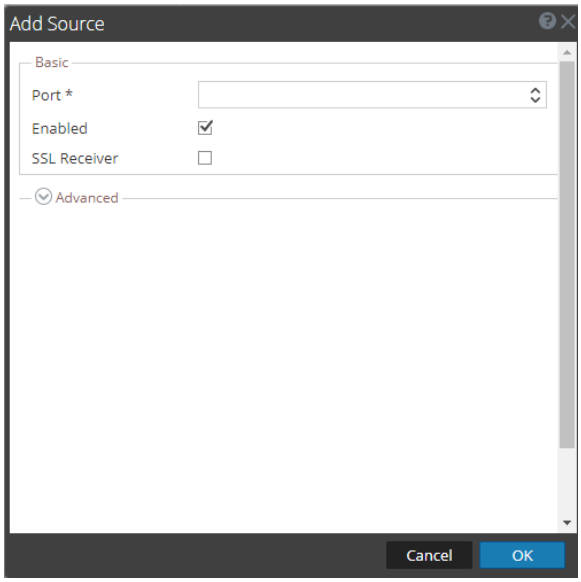


4. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog will appear.
5. Choose either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.

6. Choose the **New Type** in the **Event Categories** panel and click + in the **Sources** panel toolbar.

   The **Add Source** dialog will appear.



7. Enter **514** for the port and choose **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. You can continue to add Syslog event sources to your system without a need to do any further configuration in NetWitness Platform.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.