RSA NetWitness Logs

Event Source Log Configuration Guide

JBoss Application Server

Last Modified: Thursday, May 25, 2017

Event Source Product Information:

Vendor: JBoss
Event Source: JBoss Application Server
Versions: 4.2, 5.0, 7.0
Additional Download: sftpagent.conf.jboss

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: jboss
Collection Method: File, Syslog (7.0 and later)
Event Source Class.Subclass: Host.Application Servers

The JBoss Application Server is a production-ready Java 2 Enterprise Edition (J2EE) application server. It builds on top of the JBoss 3.2 line of open source Java application servers with improved standards compliance and major feature enhancements.

JBoss Application Server is a certified J2EE 1.4 application server. The certification guarantees that JBoss conforms to the formal J2EE specification. That allows developers to safely reuse J2EE components (e.g., Enterprise JavaBeans or EJBs) across different application servers.

Note: For JBoss version 7.0 and later, you can choose to configure Syslog or File collection, but not both.

To configure JBoss Application Server, complete these tasks:

- Set up File Collection
- On UNIX / Linux, you can collect access logs via Syslog

Set up File Collection

Perform the following tasks to set up file collection for the JBoss Application Server:

- Configure JBoss Application Server for File Collection
- Set Up the SFTP Agent
- Set Up the File Service

Configure JBoss For File Collection

Perform the appropriate instructions for your OS and version:

- Configure JBoss version 5.0 and earlier on Linux, or
- Configure JBoss version 7.0 and later on Linux, or
- Configure JBoss on Windows

To configure JBoss Application Server version 5.0 and earlier on Linux:

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

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
prefix="localhost_access_log." suffix=".log"
pattern="%h||%l||%u||%t||%m||%v||%U||%q||%H||%s||%b"
directory="${jboss.server.log.dir}"
resolveHosts="false"/>
```

To configure JBoss Application Server version 7.0 and later on Linux:

1. Open the **/usr/share/jboss-as/standalone/configuration/Standalone.xml** file, and find the following section:

```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-
server="default-host" native="false">
<connector name="http" protocol="HTTP/1.1" scheme="http" socket-
binding="http"/>
<virtual-server name="default-host" enable-welcome-root="true">
<alias name="localhost"/>
<alias name="example.com"/>
</virtual-server>
```

```
</subsystem>
```

2. After the alias lines, insert the following lines:

```
<access-log
pattern="%h||%l||%u||%t||%m||%v||%U||%q||%H||%s||%b"
prefix="localhost_access_log.">
<directory path="." relative-to="jboss.server.log.dir">
</access-log>
```

3. Save the file, and restart the **jboss** service.

To configure JBoss Application Server on Windows:

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

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
prefix="localhost_access_log." suffix=".log"
pattern="%h||%l||%u||%t||%m||%v||%U||%q||%H||%s||%b"
directory="${jboss.server.log.dir}"
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 SA SFTP Agent shell script

Configure the Log Collector for File Collection

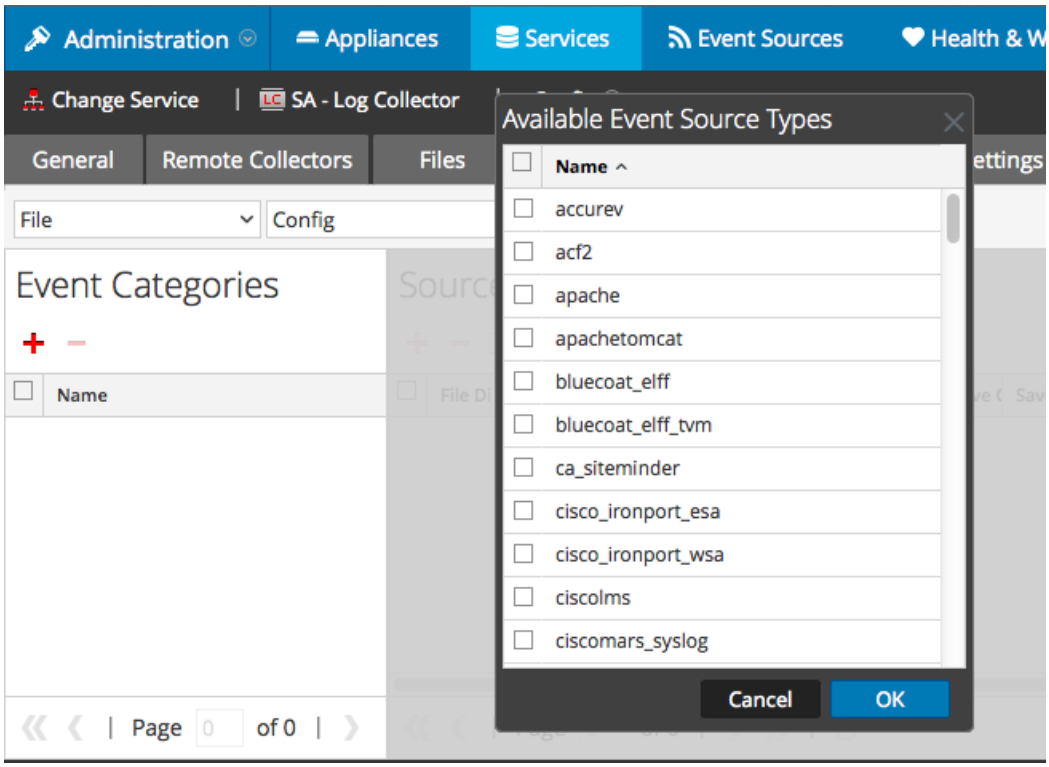
Perform the following steps to configure the Log Collector for File collection.

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 +.

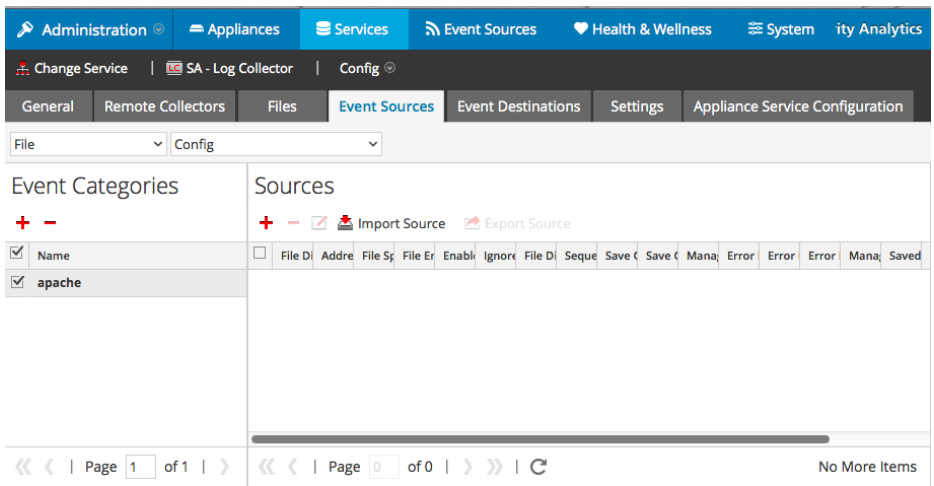
The Available Event Source Types dialog is displayed.



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

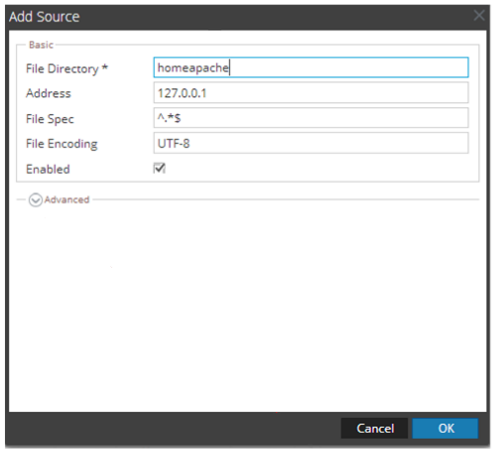
   Select **jboss** from the **Available Event Source Types** dialog.

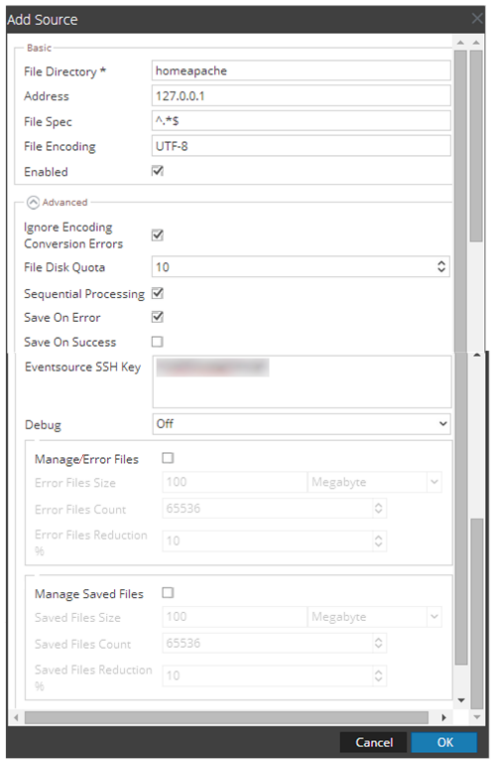
   The newly added event source type is displayed in the Event Categories panel.



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

   The Add Source dialog is displayed.





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.

Set up Syslog

On a UNIX / Linux platform, perform the following tasks to set up Syslog collection for the JBoss Application Server:

- Configure JBoss Application Server for Syslog Collection
- Configure RSA NetWitness Suite for Syslog Collection

Configure JBoss Application Server for Syslog Collection

Note: RSA supports Syslog collection for the JBoss standalone mode only.

To configure Syslog on JBoss:

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

```
#### MODULES ####

$ModLoad imfile # load the imfile input module

# Watch /usr/share/jboss-as/standalone/log
$InputFileName /usr/share/jboss-as/standalone/log/jboss_access_
log
$InputFileTag %JBOSS-
$InputFileStateFile state-jboss-access
$InputRunFileMonitor

*.* @ipaddress
```

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

2. Open the **/usr/share/jboss-as/standalone/configuration/Standalone.xml** file, and find the following section:

```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-
server="default-host" native="false">
 <connector name="http" protocol="HTTP/1.1" scheme="http" socket-
binding="http"/>
 <virtual-server name="default-host" enable-welcome-root="true">
 <alias name="localhost"/>
 <alias name="example.com"/>
 </virtual-server>
</subsystem>
```

3. After the alias lines, insert the following lines:

```
<access-log pattern="%m:
%h||%l||%u||%t||%m||%v||%U||%q||%H||%s||%b" prefix="jboss_
access_log" rotate="false">
 <directory path="." relative-to="jboss.server.log.dir"/>
</access-log>
```

4. Save the file, and restart the **jboss** and **rsyslog** services.

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