

NetWitness[®] Platform XDR

JBoss Application Server Event Source Log Configuration Guide

JBoss Application Server

Event Source Product Information:

Vendor: [JBoss](#)

Event Source: JBoss Application Server

Versions:

- Application Server versions 4.2, 5.0, 7.0
- Enterprise Application Platform (EAP) versions 4.3, 5.1, 6.4, 7.1 on Windows

Additional Download: `sftpagent.conf.jboss`

NetWitness Product Information:

Supported On: NetWitness Platform XDR 11.5 or later

Event Source Log Parser: `jboss`

Collection Method: File, Syslog (7.0 and later)

Event Source Class.Subclass: `Host.Application Servers`

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

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates and are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

November, 2022

Contents

Set up File Collection	6
Configure JBoss for File Collection	6
Set Up the SFTP Agent	8
Configure the Log Collector for File Collection	8
Set up Syslog	11
Configure JBoss Application Server for Syslog Collection	11
Configure NetWitness Platform XDR for Syslog Collection	12
Getting Help with NetWitness Platform XDR	13
Self-Help Resources	13
Contact NetWitness Support	13
Feedback on Product Documentation	14

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, 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 based on 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
- Configure JBoss EAP 4.3, 5.1 on Windows
- Configure JBoss EAP 6.4 on Windows
- Configure JBoss EAP 7.1 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"/>
```

To configure the JBoss EAP 4.3 or 5.1 on Windows:

1. Locate **JBoss_install_directory\server\default\deploy\jbossweb.sar\server.xml** and find **AccessLogValve**. Uncomment section and edit it like below:

```
<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"/>
```

2. Save the file, and restart the **Jboss** server.

Access log file is created in **Jboss\server\log** directory.

To configure the JBoss EAP 6.4 on Windows:

1. Open the **/JBoss_install_directory/standalone/configuration/standalone.xml** file and search for **virtual-server** section.

```
<subsystem xmlns="urn:jboss:domain:web:2.2" 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 Domain"/>
</virtual-server>
</subsystem>
```

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

```
<directory path="." relative-to="jboss.server.log.dir">
</access-log>
```

3. Save the file and restart the **Jboss** server.

By default, access logging output is under **{jboss.server.log.dir}/default-host** i.e. under **\$JBOSS_HOME/standalone/log/default-home**.

To configure the JBoss EAP 7.1 on Windows:

1. Open the **/usr/share/jboss-as/standalone/configuration/standalone.xml** file and search for subsystem domain, **undertow**.
2. Add the following access log pattern like below.

```
<subsystem xmlns="urn:jboss:domain:undertow:4.0">
<buffer-cache name="default"/>
<server name="default-server">
<http-listener name="default" socket-binding="http" redirect-socket="https"
enable-http2="true"/>
<https-listener name="https" socket-binding="https" security-
realm="ApplicationRealm" enable-http2="true"/>
<host name="default-host" alias="localhost">
<location name="/" handler="welcome-content"/>
<access-log pattern="%h|%l|%u|%t|%m|%v|%U|%q|%H|%s|%b"
prefix="localhost_access_log."/>
<filter-ref name="server-header"/>
<filter-ref name="x-powered-by-header"/>
<http-invoker security-realm="ApplicationRealm"/>
</host>
</server>
</subsystem>
```

3. Save the file and restart the **JBoss** server.
Undertow writes the access logs in a file named **localhost_access_log.log** in the **standalone\log\localhost_access_log.log** folder.

Set Up the SFTP Agent


To set up the SFTP Agent Collector, download the appropriate PDF from NetWitness Link:

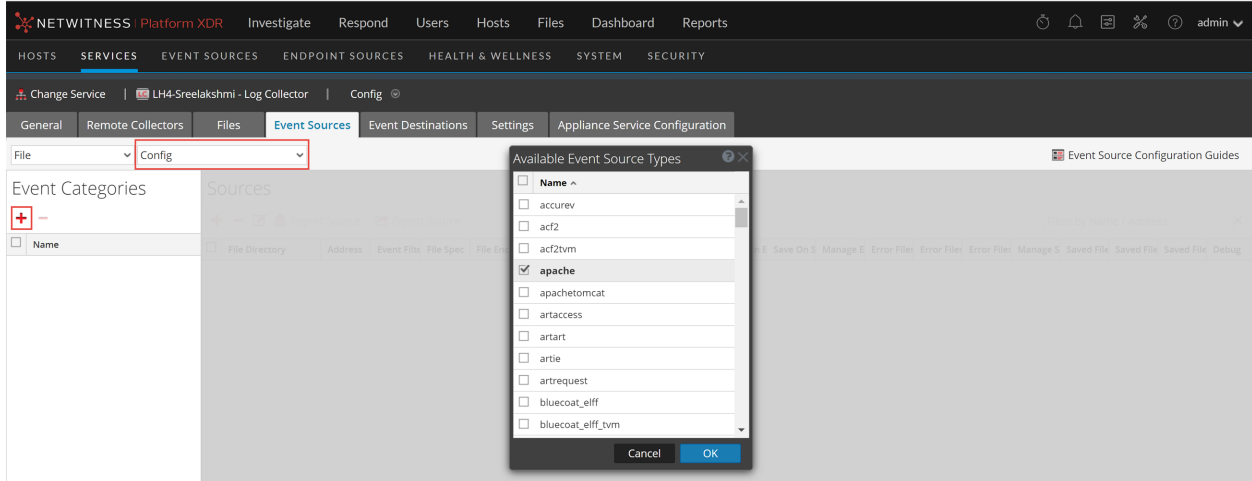
- To set up the SFTP agent on Windows, see [Install and Update SFTP Agent](#)
- To set up the SFTP agent on Linux, see [Configure SFTP Shell Script File Transfer](#)

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.

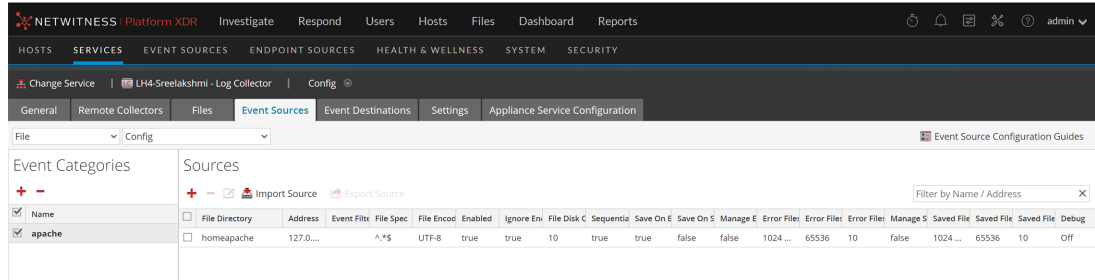


1. Select the correct type from the list and click **OK**.

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

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

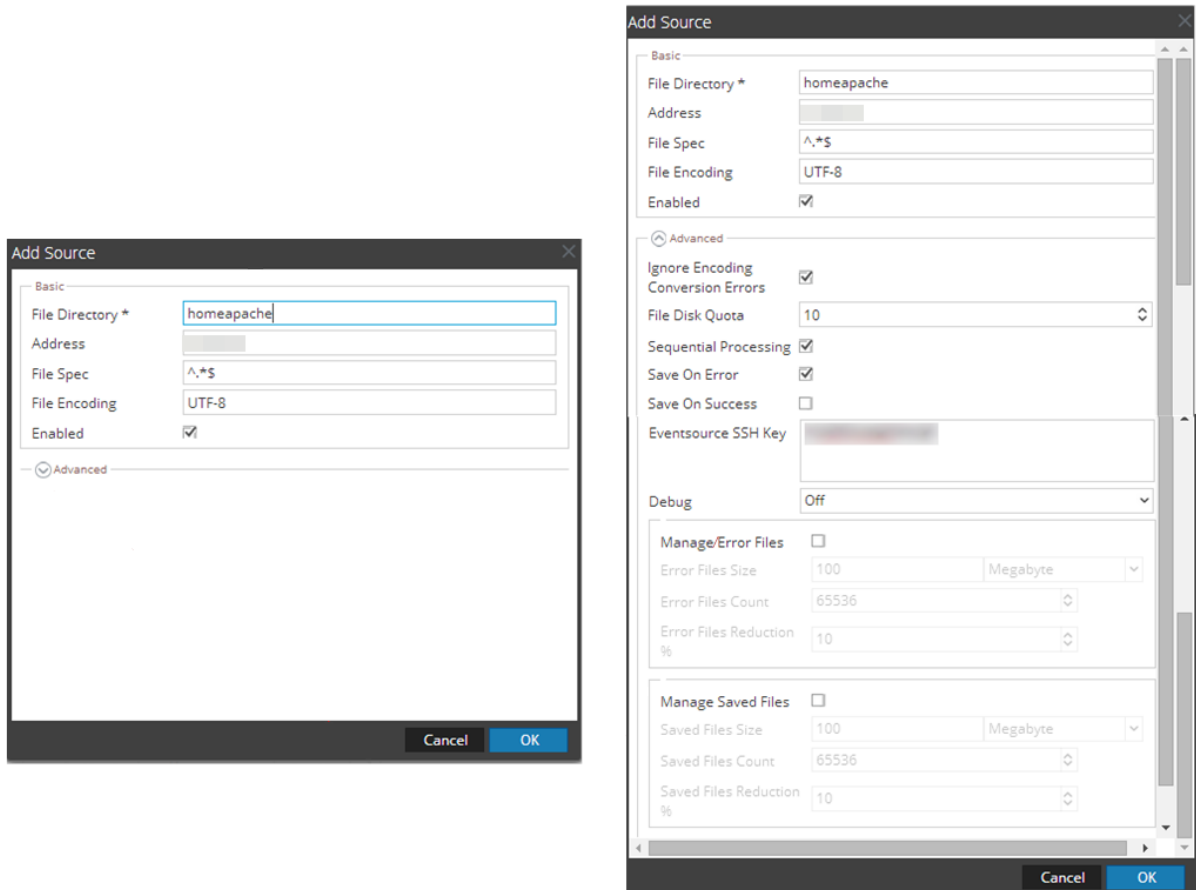
Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



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.

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 NetWitness Platform XDR for Syslog Collection.](#)

Configure JBoss Application Server for Syslog Collection

Note: NetWitness 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 NetWitness Platform XDR Log Decoder or 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 NetWitness Platform XDR for Syslog Collection


Note: Syslog collection must be configured only for the first time when you set up an event source which uses Syslog to send its output to NetWitness.

For Syslog, you can configure either the Log Decoder or the Remote Log Collector. You do not need to configure both.

To configure Log Decoder for Syslog Collection

1. In the **NetWitness** 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** 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.

Getting Help with NetWitness Platform XDR

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 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 XDR 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 nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.