# RSA NetWitness Platform

Event Source Log Configuration Guide

**RSA**

# Oracle WebLogic Server

Last Modified: Tuesday, November 17, 2020

**Event Source Product Information:**

**Vendor**: Oracle
**Event Source**: WebLogic Server
**Versions**: 10.0, 10.3, 10.3.2, 10.3.5, 10.3.6, 12.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 Download**: sftpagent.conf.oracleweblogic

**RSA Product Information:**

**Supported On**: NetWitness Platform 10.0 and later
**Event Source Log Parser**: oracleweblogic
**Collection Method**: File
**Event Source Class.Subclass**: Host.Application Servers

# Configure Oracle WebLogic Server

You must complete these tasks to configure Oracle WebLogic Server:

I.  Configure Oracle WebLogic Server to generate logs

II.  Configure Oracle Weblogic Server for Access Logs

III.  Set Up the SFTP Agent

IV.  Configure the Log Collector for File Collection

## Configure Oracle WebLogic Server for Generate Logs

### To configure the Oracle WebLogic Server:

1.  Connect to the Oracle WebLogic Server web console with administrator credentials.

2.  To enable modification, click **Lock & Edit**.

3.  In the **Domain Structure** section, click **Environment** > **Servers**.

4.  In the **Servers** table, click the name of the server that you want to configure.

5.  Select **Logging** > **General**tab.

6.  In the **Log file name** field, enter the directory and the file name that you want your logs to appear as. The default value is **../../logs/_SERVER_NAME_.log**, where _SERVER_NAME_ is the name of your server.

7.  Retain or modify the rest of the default values to your specifications.

8.  If you made any changes to the default settings, click **Save**, and click **Activate Changes**.

## Configure Oracle WebLogic Server for Access Logs

### To configure the Oracle WebLogic Server for access logs:

1.  Connect to the Oracle WebLogic Server web console with administrator credentials.

2.  To enable modification, click **Lock & Edit**.

3.  In the **Domain Structure** section, click **Environment** > **Servers**.

4.  In the **Servers** table, click the name of the server that you want to configure.

5.  Select **Logging** > **HTTP**.

6. In the **Logging: HTTP**:

    a. Select the **HTTP Access Log File Enabled** check box, if it is not already selected.

    b. In the **Log File Name** field, enter a path and a filename for the **HTTP** access log

7. At the bottom of the page, click **Advanced**.

8. In the **Format** list box, determine the format of the **HTTP** log file by selecting **Common Format**.

9. Click **Save**.

10. To activate these changes, in the **Change Center** of the **Administration Console**, click **Activate Changes**.

11. After you finish, **Restart** the server.

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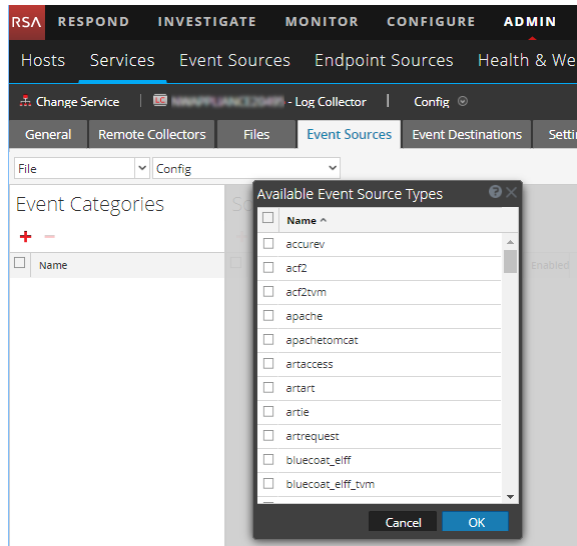
5. Select the correct type from the list, and click **OK**.

   From the **Available Event Source Types** dialog, select either:

   - **oracleweblogic**,

   - **oracleweblogicaccess** or

   - **oracleweblogicar** (for Audit Recorder)

   To configure, perform this procedure each time selecting a different type.

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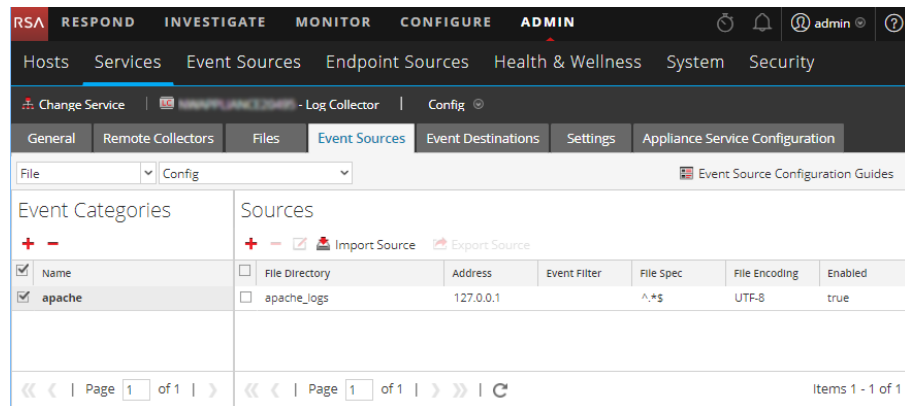
6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

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.
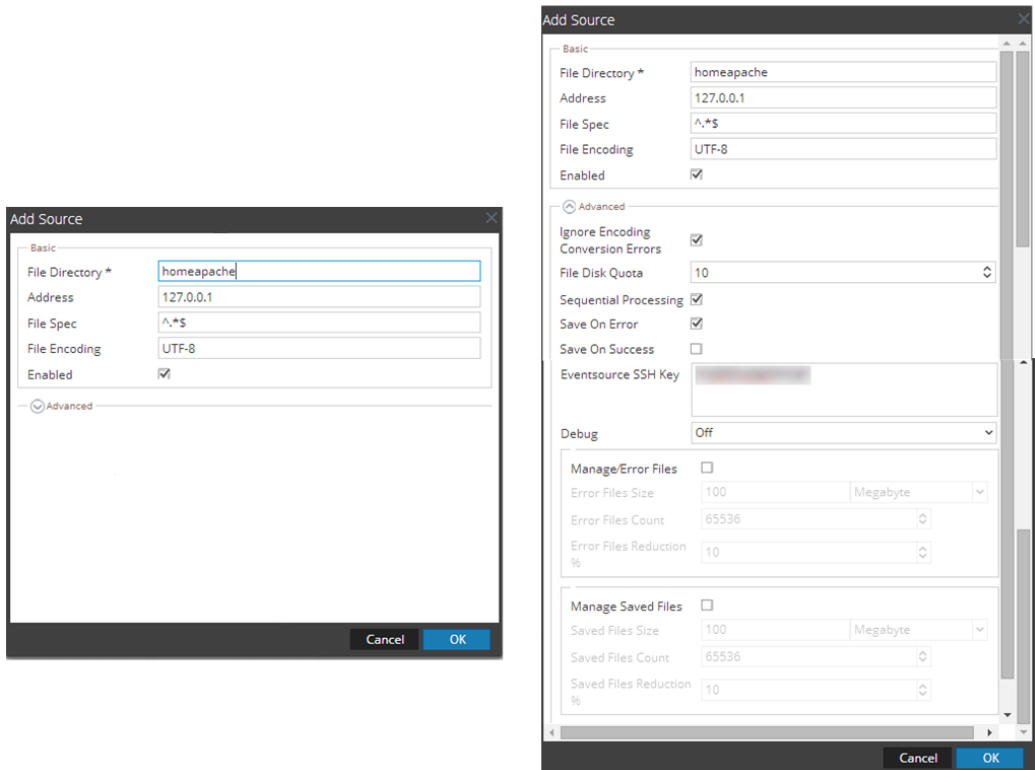
7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.

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.

## Trademarks

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