RSA NetWitness Logs

Event Source Log Configuration Guide

Oracle iPlanet Web Server

Last Modified: Tuesday, May 09, 2017

Event Source Product Information:

Vendor: Oracle
Event Source: iPlanet Web Server
Versions: 6.1 and 7
Supported Platforms:

- Windows 2003 Server Enterprise Edition
- Solaris 10 64-bit (SPARC)
- Red Hat Enterprise Linux 4

Additional Downloads: sftpagent.conf.oracleiplanetweb

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: oracleiplanetweb
Collection Method: File
Event Source Class.Subclass: Storage.Content Management System

To configure Oracle iPlanet Web Server, you must complete these tasks:

I. Depending on your version of Oracle iPlanet Web Server, do one of the following:

   - Configure Oracle iPlanet Web Server 7
   - Configure Oracle iPlanet Web Server 6.1

II. Configure Oracle iPlanet Web Server

III. Configure RSA NetWitness Suite to retrieve log files

Configure Oracle iPlanet Web Server 7

> **Note:** The web interface for Oracle iPlanet Web Server 7.0 displays the name Sun Java System Web Server.

To configure Oracle iPlanet Web Server 7, you must complete these tasks:

I. Depending on your platform, do one of the following:

   - Set up Oracle iPlanet Web Server 7 on Windows, or
   - Set up Oracle iPlanet Web Server 7 on Linux

II. Locate Log Files

Set up Oracle iPlanet Web Server 7 on Windows

Complete the following tasks:

- Set up file rotation and log extension for non-administration servers
- Set up file rotation and log extension for administration servers

To set up file rotation and log extension for non-administration servers for Windows 2003 Server Enterprise Edition:

1. Log on to the Oracle iPlanet Web Server console with administrator credentials.
2. On the **Configurations** tab, click on the instance for which you want to configure the log.
3. From the **Virtual Servers** tab, click the **General** tab.
4. On the Log Preferences page, follow these steps to configure **Access Log Preferences**:

   a. Under **Server Log Preferences**, leave the default settings or configure the settings to meet your needs.

b. Under **Log Archiving**, configure the settings to meet your needs.

c. Select only **Log these details**, and ensure that all of the check boxes are selected.

d. Click **Save**.

5. Click **Deployment Pending** > **Deploy** > **Close**.

To set up file rotation and log extension for administration servers for Windows 2003 Server Enterprise Edition:

1. On the home page, click the **Nodes** tab.
2. Click the **Administration Server** node.
3. Change the "access file location" and "log file location."
4. Open the **server.xml** file and follow these steps:

a. Edit the access-log node to have the extended log format. For example, add the following:

```
<access-log>
  <file>../logs/acces</file>
  <format>%Ses->client.ip% %Req->vars.auth-user% [%SYSDATE%]
"%Req->reqpb.clf-request%" %Req->srvhdrs.clf-     status%
%Req->srvhdrs.content-length% "%Req->headers.referer%"
"%Req->headers.user-agent%" %Req-     >reqpb.method% %Req-
>reqpb.uri% %Req->reqpb.query% %Req->reqpb.protocol%
%vsid%</format>
</access-log>
```

b. Following the virtual-server node, add event nodes for log rotation. For example, add the following:

```
<event>
  <interval>600</interval>
  <rotate-access-log>true</rotate-access-log>
</event>
<event>
  <interval>600</interval>
  <rotate-log>true</rotate-log>
</event>
```

> **Note:** You can adjust the interval category depending on your environment. The default interval is 600 seconds (10 minutes).

5. Restart the administration server.

Set up Oracle iPlanet Web Server 7 on Linux

Complete the following tasks:

- Set up file rotation and log extension for non-administration servers
- Set up file rotation and log extension for administration servers

To set up file rotation and log extension for non-administration servers for Solaris 10 64-bit (SPARC) and Red Hat Enterprise Linux 4:

1. From the web console, click **Home**.
2. On the **Configurations** tab, click on the instance that you want to configure the log for.
3. From the **Virtual Servers** tab, click the **General** tab.
4. On the Log Preferences page, follow these steps to configure **Access Log Preferences**:
   a. Under **Server Log Preferences**, leave the default settings or configure the settings to meet your needs.
   b. Under **Log Archiving**, configure the settings to meet your needs.
   c. Select only **Log these details**, and ensure that all of the check boxes are selected.
   d. Click **Save**.
5. Click **Deployment Pending** > **Deploy** > **Close**.

To set up file rotation and log extension for administration servers for Solaris 10 64-bit (SPARC) and Red Hat Enterprise Linux 4:

1. Open the **server.xml** file and follow these steps:
   a. Edit the access-log node to have the extended log format. For example, add the following:

```
<access-log>
  <file>../logs/acces</file>
  <format>%Ses->client.ip% - %Req->vars.auth-user%
[%SYSDATE%] "%Req->reqpb.clf-request%" %Req->srvhdrs.clf-
   status% %Req->srvhdrs.content-length% %Req-
>headers.referer% %Req->headers.user-agent% %Req-
>reqpb.method%     %Req->reqpb.uri% %Req->reqpb.query% %Req-
>reqpb.protocol% %vsid% </format>

</access-log>
```

b. Following the virtual-server node, add event nodes for log rotation. For example, add the following:

```
<event>

<interval>240</interval>

  <rotate-access-log>true</rotate-access-log>

</event>

<event>

  <interval>240</interval>

  <rotate-log>true</rotate-log>

</event>
```

2. Restart the administration server.

Locate Log Files

To locate the log files:

1. Locate the iPlanet installation folder, and pick the server instances from which you want to collect logs.

2. Click the "logs" folder.

Configure Oracle iPlanet Web Server 6.1

To configure Oracle iPlanet Web Server 6.1 for Windows 2003 Server Enterprise Edition, you must complete these tasks:

I. Set up file rotation and log extension for non-administration servers

II. Set up file rotation and log extension for administration servers

> **Note:** The web interface for Oracle iPlanet Web Server 6.1 displays the name Sun ONE Web Server 6.1.

Set Up File Rotation and Log Extension for Non-Administration Servers

To set up file rotation and log extension for non-administration servers:

1. Log on to the Oracle iPlanet Web Server console with administrator credentials.
2. On the **Servers** tab, click **Manage Servers**.
3. Select a server, and click **Manage**.
4. On the **Logs** tab, click **Access Log Preferences**.
5. Select the "only log" format, and select all of the check boxes.
6. Click **OK** > **Apply**.
7. Click **Error Log Preferences**, and ensure the settings are as follows:

Field	Value
Error Log File Name	Enter the location of the error log file.
Log Level	Select **info**
Log VSID	Select **disabled**
Log Stdout	Select **enabled**
Log Stderr	Select **enabled**

Field	Value
Log To Console	Select **enabled**
Create Console	Select **disabled**
Use System Logging	Select **disabled**

8. Click **Archive Log** and set up the log rotation policy to meet your needs.

Set Up File Rotation and Log Extension for Administration Servers

To set up file rotation and log extension for administration servers:

1. Click **Administration Server**.
2. On the **Preferences** tab, click **Access Logging Options**.
3. Select the "only log" format, and select all of the checkboxes.
4. Click **OK** > **Apply**.
5. Click **Error Logging Options** and ensure the settings are as follows:

Field	Value
Error Log File Name	Enter the location of the error log file.
Log Level	Select **info**
Log VSID	Select **disabled**
Log Stdout	Select **enabled**
Log Stderr	Select **enabled**
Log To Console	Select **enabled**
Create Console	Select **disabled**
Use System Logging	Select **disabled**

6. To set up log rotation, open the **magnus.conf** file, and add the following line:

```
init fn="flex-rotate-init" rotate-start="hhmm" rotate-
interval="mm"
```

where:

- ***hhmm*** is the rotation start time in twenty-four hour format, for example, 2130, and
- ***mm*** is the rotation interval in minutes

7. Stop and start the server by running the following .bat files in admserv:

```
C:\Sun\WebServer6.1\https-admserv\stopsvr.bat
C:\Sun\WebServer6.1\https-admserv\startsvr.bat
```

Configure NetWitness Suite for File Collection

You must complete these tasks to configure RSA NetWitness Suite for File Collection.

I. Set up the SFTP Agent

II. Configure the Log Collector for File Collection

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

The **sftpagent.conf.oracleiplanetweb** contains information on setting up the SFTP Agent for Oracle iPlanet. You can download the file from RSA Link here: https://community.rsa.com/docs/DOC-58032.

Configure the Log Collector for File Collection

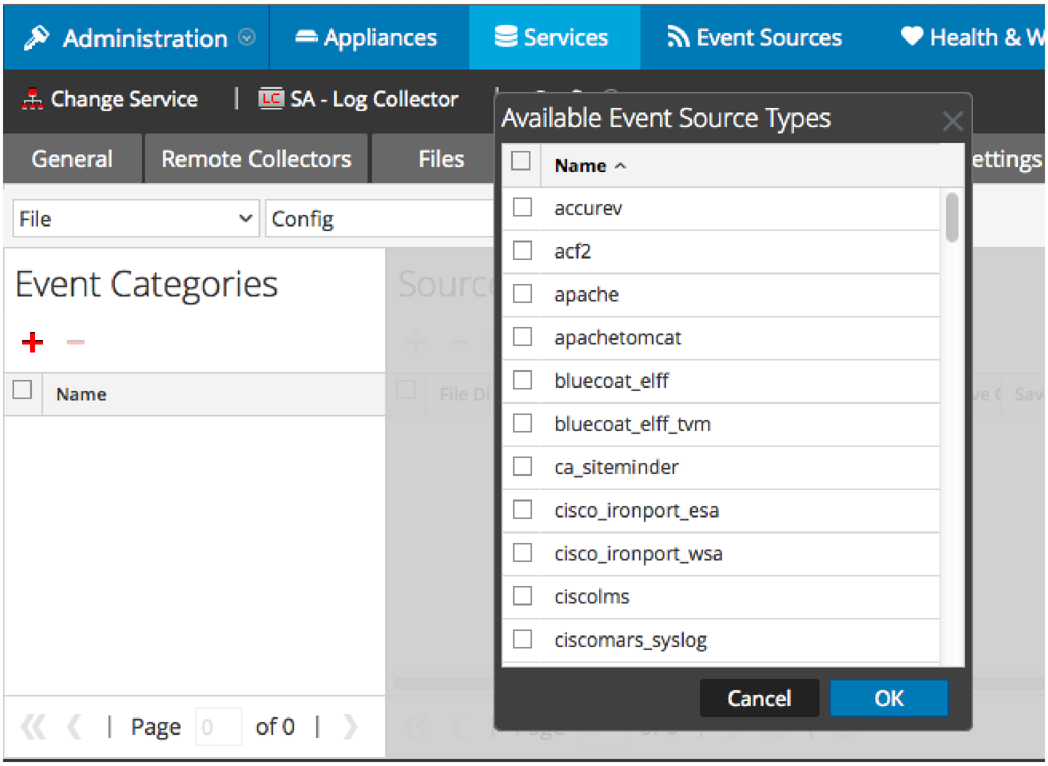
Perform the following steps to configure the Log Collector for File collection.

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 +.

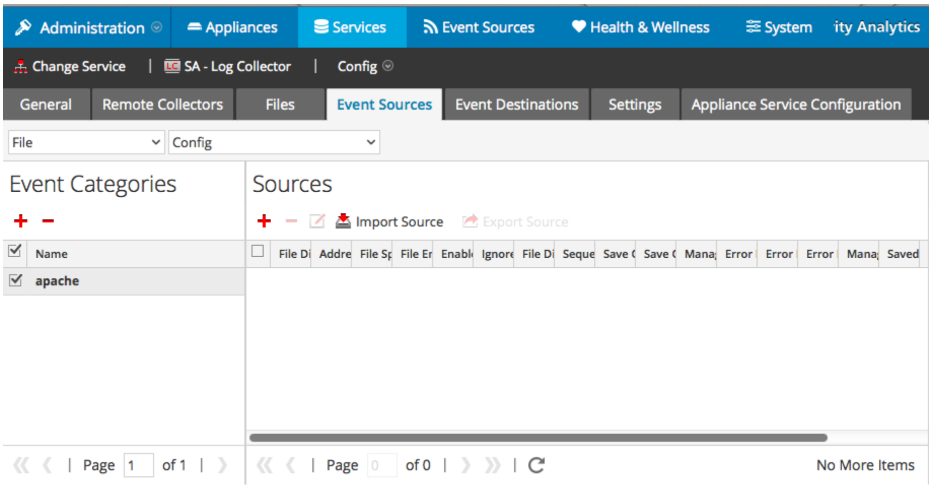
   The Available Event Source Types dialog is displayed.



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

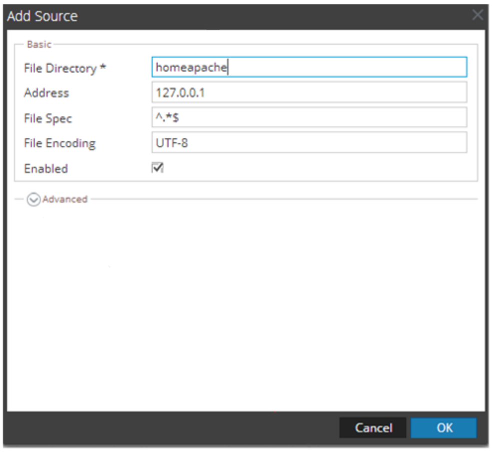
   Select **oracleiplanetweb** from the **Available Event Source Types** dialog.

   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.

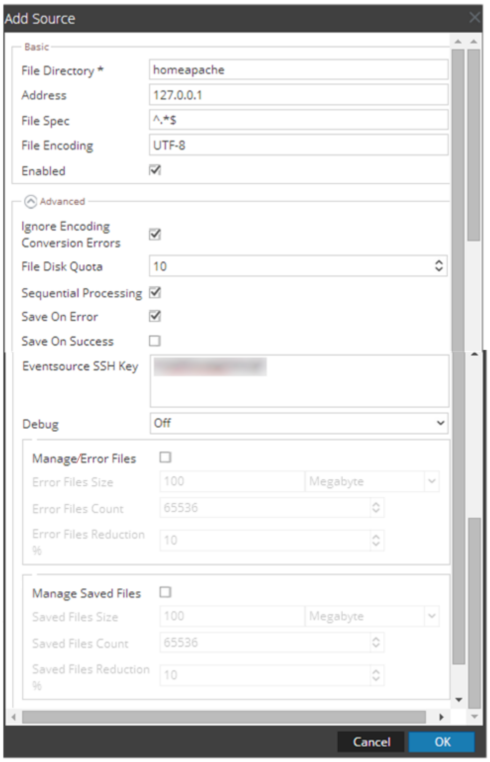
The Add Source dialog is displayed.



Add Source

Basic

File Directory *	homeapache
Address	127.0.0.1
File Spec	^.*$
File Encoding	UTF-8
Enabled	☑



Add Source

Basic

File Directory *	homeapache
Address	127.0.0.1
File Spec	^.*$
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	[redacted]	
Debug	Off	
Manage/Error Files	□	
Error Files Size	100	Megabyte
Error Files Count	65536	
Error Files Reduction %	10	
Manage Saved Files	□	
Saved Files Size	100	Megabyte
Saved Files Count	65536	
Saved Files Reduction %	10	

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

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.