# RSA NetWitness Logs

Event Source Log Configuration Guide



# **Oracle Directory Server**

Last Modified: Thursday, June 29, 2017

### **Event Source Product Information:**

Vendor: Oracle Event Source: Oracle Directory Server (previously SunOne LDAP Directory Server) Versions: 11.1.1.7.1 Additional Download: sftpagent.conf.sunoneldap, nicsftpagent1.conf.oracleds, nicsftpagent2.conf.oracleds Platforms: Windows, Red Hat Linux

**RSA Product Information:** 

Supported On: NetWitness Suite 10.0 and later Event Source Log Parser: sunoneldap Collection Method: File Event Source Class.Subclass: Security.Access Control

# **Configure Oracle Directory Server**

To configure Oracle Directory Server, you must complete these tasks in RSA NetWitness Suite:

- I. Set Up the SFTP Agent
- II. Set up the File Service

## 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

If you are using Linux, note the following when configuring the **sasftpagent.sh** file:

- Save two copies of the sasftpagent.sh file: sasftpagent1.sh and sasftpagent2.sh.
- In the files, set the following parameters:

For the first file:

- SCRIPT\_NAME = sasftpagent1.sh
- SA\_CONFIG = sasftpagent1.conf

For the second file:

- SCRIPT\_NAME = sasftpagent2.sh
- SA\_CONFIG = sasftpagent2.conf

**Note:** The cron jobs needed to run these two scripts will need the exact names of the sasftpagent instances that you specified in the SCRIPT\_NAME parameter.

## **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.
- 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.

Administration 🛛 🗕 Appl		liances	es 😂 Services		Svent Sources		🛡 Health & W			
📥 Change Service 🔰 🧧 SA - Log Collector				Ava	Available Event Source Types					
General	Remote C	ollectors	Files		Name ^				ettings	
File	~	Config			accurev					
-					acf2					
Event Categories			Sour	CE 🗆	apache					
+ -					apacheto	mcat				
Name				Di	bluecoat_	elff			ve ( Sav	
					bluecoat_	elff_tvm				
					ca_sitemi	nder				
					cisco_iror	iport_esa				
					cisco_iror	iport_wsa				
					ciscolms					
					ciscomars	s_syslog				
						Cane		OK		
« <   P	Page 0 c	of0   🔪				Canc				

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

From the **Available Event Source Types** dialog, select the appropriate choice or choices for your OS:

- sunoneldap to collect audit logs on Windows
- oracleds\_audit to collect audit logs on Linux
- oracleds\_access to collect access logs on Linux

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.

✗ Administration ☺ = Appl	iances Services	€ Event Sources	Health & Wellness	System ity Analytics
🏯 Change Service 🛛 🛛 🚾 SA - Log	Collector   Config ⊙			
General Remote Collectors	Files Event Sou	rces Event Destination	ons Settings Apj	oliance Service Configuration
File ~ Config	~			
Event Categories	Sources			
+ -	🕂 — 🗹 📥 Import	Source 🛛 🖄 Export Sour		
☑ Name	File Di Addre File Sr	File Er Enable Ignore File Di	Seque Save (Save (Mana	Error Error Mana Saved
⊠ apache				
<pre>《  Page 1 of 1 )</pre>	巛 🔇   Page 0	of0   > >>>   C <sup>4</sup>		No More Items

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.

			Add Source				
			Basic				
			File Directory *	homeapache			
			Address	127.0.0.1			
			File Spec	^.*s			
			File Encoding	UTF-8			
			Enabled	$\checkmark$			
			Advanced				
		×	Ignore Encoding Conversion Errors	V			
	homeapache		File Disk Quota	10		0	
dress 127.0.0.1 S   Spec ^.*\$ S			Sequential Processing 🗹 Save On Error 🛛 🗹				
$\checkmark$			Eventsource SSH Key		1		
			Debug	Off		~	
			Manage/Error Files				
			Error Files Size		Megabyte	$\sim$	
			Error Files Count		0		
			Error Files Reduction %		$\diamond$		
			Manage Saved Files				
		Cancel OK	Saved Files Size		Megabyte	$\sim$	
			Saved Files Count		$\diamond$		
			Saved Files Reduction		^		

- 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.

Copyright © 2017 EMC Corporation. All Rights Reserved.

#### 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.