# RSA NetWitness Platform

Event Source Log Configuration Guide



## **Microsoft Network Policy Server**

Last Modified: Thursday, October 31, 2019

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

Vendor: Microsoft Event Source: Network Policy Server Versions: 3.2, 4.0 Additional Downloads: sftpagent.conf.msias

**RSA Product Information:** 

Supported On: NetWitness Platform 10.0 and later Event Source Log Parser: msias Collection Method: File and Windows Event Logs Event Source Class.Subclass: Security.Access Control You can configure RSA NetWitness Platform to collect logs from Microsoft Network Policy Server, using either File collection, Windows Eventing collection, or both.

- I. Configure Microsoft NPS
- II. Configure RSA NetWitness Platform for Windows and/or File Collection:
  - Configure File Collection
  - Configure Windows Collection

## **Configure Microsoft NPS**

This section describes how to set up the Microsoft Network Policy Server event source for Windows collection.

#### To configure Microsoft NPS for Windows collection:

- 1. Start the Network Policy Server management utility.
- 2. Select the Remote Access Logging folder.
- 3. Double click on the Local File logging method.
- 4. On the Settings tab, ensure that the following boxes are selected:
  - Accounting Requests
  - Authentication Requests
  - Periodic Status
- 5. On the Log File tab, confirm the following settings:
  - In the Directory field, select C:\WINDOWS\system32\LogFile.
  - In the Format field, select IAS (Legacy).
  - In the Create a new log file field, select Daily.
  - In the When disk is full delete older log files field, ensure the check box is selected.

### **Configure File Collection**

To configure Microsoft Network Policy Server for File collection, you must complete these tasks:

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

**Note:** To configure File Collection, you need a Log Collector that is at version 10.5.2 or later.

#### 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**.
- 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.

RSA RESPOND INVESTIGAT	E MONITOR CONFIGURE ADMIN
Hosts Services Event So	urces Endpoint Sources Health & Well
A Change Service	- Log Collector   Config ©
General Remote Collectors F	Files Event Sources Event Destinations Settin
File 💙 Config	~
Event Categories Sc	Available Event Source Types
+ -	Name ^
Name	acf2
	acf2tvm
	apache
	apachetomcat
	artart
	artie
	artrequest
	bluecoat_eim
	Cancel OK

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

Select msias\_tvm from 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.

RESPOND INVESTIG	ATE MONITOR CON	FIGURE AD	лім	δĢ	(ℓ) admin ⊚ (?)
Hosts Services Event	Sources Endpoint Sou	rces Health	& Wellness	System Seci	urity
🚠 Change Service 🔰 🚾	- Log Collector   C	onfig 👳			
General Remote Collectors	Files Event Sources E	vent Destinations	Settings App	liance Service Conf	iguration
File 💙 Config	~			📰 Event Source C	onfiguration Guides
Event Categories	Sources				
+ -	🕂 😑 🗹 📥 Import Source	🖄 Export Source			
Name Name	File Directory	Address I	event Filter File S	pec File Encod	Ing Enabled
🗹 apache	apache_logs	127.0.0.1	^.*s	UTF-8	true

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			
		Advanced			
		Ignore Encoding Conversion Errors	V		
*	homeapache	File Disk Quota	10		
	127.0.0.1	Sequential Processing	2		
	^.*s	Save On Error			
	UTF-8	Save On Success			
		Eventsource SSH Key			
		Debug	Off		
		Manage/Error Files			
		Error Files Size		Megabyte	
		Error Files Count		0	
		Error Files Reduction		0	
		Manage Saved Files			
	Cano	OK Saved Files Size		Megabyte	
		Saved Files Count		0	
		Saved Files Reductio %		$\diamond$	
		4			
				Cancel	

- 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.

## **Configure Windows Collection**

To configure WinRM, see the following document on RSA Link: Microsoft WinRM Configuration and Troubleshooting. For more details about Windows Collection in the RSA NetWitness Platform, see the Configure Windows Collection topic on RSA Link.

Copyright  $\ensuremath{\mathbb{C}}$  2019 Dell Inc. or its subsidiaries. All Rights Reserved.

#### Trademarks

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