RSA NetWitness Logs

Event Source Log Configuration Guide



EMC VPLEX

Last Modified: Wednesday, June 07, 2017

Event Source Product Information:

Vendor: EMC Event Source: VPLEX Version: All Additional Download: sftpagent.conf.emcvplex

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later Event Source Log Parser: emcvplex Collection Method: File Event Source Class.Subclass: Storage.Storage You must complete these tasks to configure EMC VPLEX 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

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.



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

Select emcvplex from the Available Event Source Types dialog.

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

🔊 Administration 🛛 🗕 Applia		Services	Sevent Source	s 🔍 🔍 Health & We	llness 🛛 🛱 Syste	m ity Analytics					
🚠 Change Service 🛛 🛙	SA - Log Collecto	r Config ⊚									
General Remote Co	ollectors File	s Event So	Event Dest	inations Settings	Appliance Service	e Configuration					
File ~	Config	~									
Event Categories		Sources									
+ -		🕂 🚽 🗹 🛓 Import Source 🗠 Export Source									
Name	F	le Di Addre File Sp	File Er Enable Ignore F	ile Di Seque Save Save	Mana Error Error	Error Mana Saved					
✓ apache											
						-					
<pre>《</pre>		<pre>((Page 0 of 0)) C</pre>									

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				×
		- B	Basic			_	
		Fi	ile Directory *	homeapache			
		A	ddress	127.0.0.1			
		Fi	ile Spec	^.*s			
		Fi	ile Encoding	UTF-8			
		E	nabled	\checkmark			
			Advanced				
			gnore Encoding Conversion Errors	\checkmark			
rectory *	homeapache	Fi	ile Disk Quota	10		\$	
	127.0.0.1	S	equential Processing	\checkmark			
c	^.*s	S	ave On Error	v			
ding	UTF-8	Si	ave On Success				
		E	ventsource SSH Key				ſ
		D	ebug	Off ~			
			Manage/Error Files				
			Error Files Size		Megabyte	~	
			Error Files Count		0		
			Error Files Reduction %		\$		
			Manage Saved Files				
	Cancel	ОК	Saved Files Size		Megabyte	~	
			Saved Files Count		0		
			Saved Files Reduction %		\diamond		
		<				•	•

- 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.