RSA NetWitness Logs

Event Source Log Configuration Guide



EMC Symmetrix Solutions Enabler

Last Modified: Friday, April 21, 2017

Event Source Product Information:

Vendor: EMC Event Source: Symmetrix Solutions Enabler Versions: Solutions Enabler 6.4, 6.5.3, 7.0, 7.1, 7.3.0.1, 7.6.1 Platforms: Symmetrix DMX, Symmetrix VMAX, Microsoft Windows 2000, 2003, and 2008, Solaris 9 and 10 Additional Downloads: sftpagent.conf.symmetrix

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later Event Source Log Parser: symmetrix Collection Method: Syslog, File Event Source Class.Subclass: Storage.Storage Depending upon your environment, configure EMC Symmetrix to send messages via Syslog or File. To configure EMC Symmetrix Solutions Enabler, you must complete one of the following tasks:

- Configure Syslog
 - 1. Configure RSA NetWitness Suite for Syslog Collection
 - 2. Configure EMC Symmetrix Solutions Enabler for Syslog
 - 3. Configure EMC Symmetrix Solutions Enabler in your OS
 - 4. Issue Commands in the Event Daemon
- Configure File collection
 - 1. Configure EMC Symmetrix Solutions Enabler for File Collection
 - 2. Configure EMC Symmetrix Solutions Enabler in your OS
 - 3. Issue Commands in the Event Daemon
 - 4. Set Up SFTP and Configure NetWitness Log Collector

Configure RSA NetWitness Suite for Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Suite Live.

Ensure that the parser for your event source is enabled:

- 1. In the **NetWitness** menu, select **Administration** > **Services**.
- In the Services grid, select a Log Decoder, and from the Actions menu, choose View > Config.
- 3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is symmetrix.

Configure Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

- 1. In the NetWitness menu, select Administration > Services.
- 2. In the Services grid, select a Log Decoder, and from the Actions menu, choose View > System.
- 3. Depending on the icon you see, do one of the following:
 - If you see [•] Start Capture</sup>, click the icon to start capturing Syslog.
 - If you see [•] Stop Capture</sup>, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

- 1. In the NetWitness menu, select Administration > Services.
- In the Services grid, select a Remote Log Collector, and from the Actions menu, choose View > Config > Event Sources.
- 3. Select Syslog/Config from the drop-down menu.

The Event Categories panel displays the Syslog 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 either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
- 6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

The Add Source dialog is displayed.

7. Enter 514 for the port, and select Enabled. Optionally, configure any of the Advanced

parameters as necessary.

Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Configure EMC Symmetrix Solutions Enabler for Syslog

To configure the EMC Symmetrix Solutions Enabler for syslog:

- 1. Log on to the Solutions Enabler with administrator credentials.
- Open the daemon_options file. The location of the file depends on your operating system:
 - On Solaris, /var/symapi/config/daemon_options.
 - On Windows, C:\Program Files\emc\symapi\config\daemon_options.
- 3. To configure the syslog event target in the daemon_options file, type the following:

```
storevntd:log_event_syslog_host = NW-IP-address
storevntd:log_event_syslog_port = 514
```

where *NW-IP-address* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

 To configure the Event Daemon to collect Audit Records and log them within the daemon_options file, type the following:

```
storevntd: log_event_targets = syslog
storevntd: log_symmetrix_events = tgt=syslog, sid=Symmetrix-id,
audit
```

If there are multiple Symmetrix arrays:

```
storevntd: log_event_targets = syslog
storevntd: log_symmetrix_events = tgt=syslog, sid=Symmetrix-id,
audit; \
    tgt=syslog, sid= Symmetrix-id, audit; \
    tgt=syslog, sid= Symmetrix-id, audit
```

5. Save and close the file.

Configure EMC Symmetrix Solutions Enabler in your OS

Configure Syslog for EMC Symmetrix Solutions Enabler on the appropriate OS.

Configure EMC Symmetrix Solutions Enabler in Solaris

To configure EMC Symmetrix Solutions Enabler in Solaris, issue the following commands from the Solutions Enabler Command Line Interface (CLI):

1. To determine if User Authorization is enabled for a Symm, and to see the current role assignments in effect for it, type the following:

```
symauth -sid Symmetrix-id list
symauth -sid Symmetrix-id list -users
```

2. To allow 'storevntd' from any host, type the following:

```
symauth -sid Symmetrix-id commit <<!
assign user storevntd to role Auditor;
!</pre>
```

3. To allow 'storevntd' from only a specific host, type the following:

```
symauth -sid Symmetrix-id commit <<!
assign user H:jupiter\storevntd to role Auditor
!</pre>
```

Configure EMC Symmetrix Solutions Enabler in Windows

To configure EMC Symmetrix Solutions Enabler in Windows, issue the following commands from the Solutions Enabler Command Line Interface (CLI):

1. To tell if User Authorization is enabled for a Symm and see the current role assignments in effect for it, type the following:

```
symauth -sid Symmetrix-id list
symauth -sid Symmetrix-id list -users
```

- 2. To allow 'storevntd' from any host:
 - a. Enter the following command into a new text file:

```
assign user storevntd to role Auditor;
```

b. From the Solutions Enabler CLI, type the following:

symauth -sid Symmetrix-id commit -file <newfilename>
where <newfilename> is the name of the new file.

- 3. To allow 'storevntd' from only a specific host:
 - a. Enter the following command into a new text file:

assign user H:jupiter\storevntd to role Auditor

b. From the Solutions Enabler CLI, type the following:

symauth -sid Symmetrix-id commit -file <newfilename>

Issue Commands in the Event Daemon

To issue commands in the Event Daemon, start the Event Daemon from the Solutions Enabler CLI and enter the following:

• To determine whether the Event Daemon is running and query its current state, type the following:

```
stordaemon list
stordaemon show storevntd
```

• To start the Event Daemon automatically when the OS starts, type the following:

```
stordaemon install storevntd -autostart
```

• To start the Event Daemon, type the following:

stordaemon start storevntd

• To restart the Event Daemon, type the following:

stordaemon restart storevntd

Note: If you are performing an upgrade, you must restart the Event Daemon to confirm any changes.

Configure EMC Symmetrix Solutions Enabler for File Collection

To configure the EMC Symmetrix Solutions Enabler for file reader:

- 1. Log on to the Solutions Enabler with administrator credentials.
- Open the daemon_options file. The location of the file depends on your operating system:
 - On Solaris, /var/symapi/config/daemon_options.
 - On Windows, C:\Program Files\emc\symapi\config\daemon_options.
- 3. To configure the syslog event target in the daemon_options file, type the following:

```
storevntd:log_event_syslog_host = NW-IP-address
storevntd:log event syslog port = 514
```

where *NW-IP-address* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

4. To configure the Event Daemon to collect Audit Records and log them within the **daemon_options** file, type the following:

```
storevntd: log_event_targets = file
storevntd: log_symmetrix_events = tgt=file, sid=Symmetrix-id,
audit
```

If there are multiple Symmetrix arrays:

```
storevntd: log_event_targets = file
storevntd: log_symmetrix_events = tgt=file, sid=Symmetrix-id,
audit; \
    tgt=file, sid= Symmetrix-id, audit; \
    tgt=file, sid= Symmetrix-id, audit
```

5. Save and close the file.

Configure EMC Symmetrix Solutions Enabler in your OS

Configure File Collection for EMC Symmetrix Solutions Enabler on the appropriate OS.

Configure EMC Symmetrix Solutions Enabler in Solaris

To configure EMC Symmetrix Solutions Enabler in Solaris, issue the following commands from the Solutions Enabler Command Line Interface (CLI):

1. To determine if User Authorization is enabled for a Symm, and to see the current role assignments in effect for it, type the following:

```
symauth -sid Symmetrix-id list
symauth -sid Symmetrix-id list -users
```

2. To allow 'storevntd' from any host, type the following:

```
symauth -sid Symmetrix-id commit <<!
assign user storevntd to role Auditor;
!</pre>
```

3. To allow 'storevntd' from only a specific host, type the following:

```
symauth -sid Symmetrix-id commit <<!
assign user H:jupiter\storevntd to role Auditor
!</pre>
```

Configure EMC Symmetrix Solutions Enabler in Windows

To configure EMC Symmetrix Solutions Enabler in Windows, issue the following commands from the Solutions Enabler Command Line Interface (CLI):

1. To tell if User Authorization is enabled for a Symm and see the current role assignments in effect for it, type the following:

```
symauth -sid Symmetrix-id list
symauth -sid Symmetrix-id list -users
```

- 2. To allow 'storevntd' from any host:
 - a. Enter the following command into a new text file:

```
assign user storevntd to role Auditor;
```

b. From the Solutions Enabler CLI, type the following:

symauth -sid Symmetrix-id commit -file <newfilename>
where <newfilename> is the name of the new file.

- 3. To allow 'storevntd' from only a specific host:
 - a. Enter the following command into a new text file:

assign user H:jupiter\storevntd to role Auditor

b. From the Solutions Enabler CLI, type the following:

symauth -sid Symmetrix-id commit -file <newfilename>

Set Up SFTP and Configure NetWitness Log Collector

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 emc_symmetrix from the Available Event Source Types dialog.

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

🔊 Administration 🛛 🗕 Appli		ance	Services		2	Svent Sources		Health & Wellness			88	E Syste	m i	ity Analytics					
📩 Change S	ervice 🗵	🖲 SA - Log (ector Config ©																
General	Remote Co	ollectors	F	iles	Ev	ent So	urces	Eve	nt Des	stinatio	ons	Setti	ngs	Арр	liance	Servic	e Con	figurati	ion
File	~	Config				~													
Event Categories				Sources															
+ -	+	🕂 🚽 🗹 📥 Import Source 🛛 🖄 Export Source																	
Name				File Di	Addre	File Sp	File Er	Enable	Ignore	File Di	Seque	Save (Save (Mana	Error	Error	Error	Mana	Saved
🗹 apache																			
« < I F	Page 1 o	f1 》	<	<	Page	e 0	of 0	$ \rangle$	»» I	C							No	More I	tems

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

The Add Source dialog is displayed.

Immespache 127.00.1 127.00.1 127.00.1 A^+S UTF-8 W Concel OK				Add Source			
File Directory * homeapache Address 127.0.0.1 File Spec ^.^s File Coroling UTF-8 Enabled Ø Conversion Errors Ø Save On Error Ø Save On Success 0 Eventsource SSH Key 0 Debug Off Manage Error Files 0 Error Files Size 100 Manage Saved Files 0 Saved Files Size 100 Manage Firer Files Size 0 Manage Saved Files 0 Saved Files Size 100 Manage Files Reduction 10 Saved Files Reduction 10				Basic			
Address 127.0.0.1 File Spec A*5 File Encoding UTF-8 Enabled Ø Advanced Ignore Encoding Ø Conversion Errors Ø Save On Error Ø Save On Success © Eventsource SSH Key Debug Øff Manage/Error Files © Error Files Size 100 Megabyte V Error Files Size 100 Megabyte V Saved Files Count 65536 0 S Saved Files Count 65536 0 S Saved Files Size 100 Megabyte V Saved Files Size 100 Megabyte V Saved Files Count 65536 0 S Saved Files Size 100 Megabyte V Saved Files Reduction 10 0 K				File Directory *	homeapache		
File Spec ^*S File Encoding UTF-8 Enabled Image Encoding 127.0.0.1 Image Encoding ^*S Image Encoding UTF-8 Image Encoding Image Encoding Imag				Address	127.0.0.1		
File Encoding UTF-8 Enabled Ignore Encoding Conversion Errors Conversion Errors Save On Error Save On Success Eventsource SSH Key Debug Off Manage/Error Files Error Files Size 100 Manage Saved Files Saved Files Reduction 10 Saved Files Reduction 10 Saved Files Reduction 10				File Spec	^.*s		
Inomeapache 127.0.0.1 \x^5 JTF-8 A Save On Error Save On Success Eventsource SSH Key Debug Off Manage/Error Files Error Files Sale 10 Saved Files Count 65536 0 Manage Saved Files Saved Files Size 10 Saved Files Size 10 Saved Files Size 10 Saved Files Reduction 10 0 %				File Encoding	UTF-8		
pache I				Enabled	\checkmark		
apache 0.1 Save On Success Evensource SSH Key Debug Off Manage/Error Files Error Files Size 10 Saved Files Size Saved Files Size Saved Files Size Saved Files Reduction 10 Saved Files Reduction 10				Advanced			
homeapache 127.0.0.1 A.*5 UTF-8 2 2 Save On Error Save On Success Eventsource SSH Key Debug Off Manage/Error Files Error Files Size 10 Error Files Count 65536 O Kanage Saved Files Saved Files Size 10 Saved Files Count Saved Files Count Saved Files Reduction 10 10			×	Ignore Encoding Conversion Errors	V		
127.0.0.1 ^.^*s UTF-8 IVT Save On Success Eventsource SSH Key Debug Off Manage/Error Files Error Files Size Error Files Size Error Files Count Error Files Size Saved Files Count Saved Files Reduction 10 Saved Files Reduction		homeapache		File Disk Quota	10		
**S Save On Error ✓ ITF-8 Save On Success □ Eventsource SSH Key □ □ Debug Off □ ManageError Files □ Error Files Size 100 Megabyte Error Files Count 655366 ○ Manage Saved Files □ ○ Save On Error 10 ○ Manage Saved Files Count 65536 ○ Saved Files Count 65536 ○ Saved Files Reduction 10 ○ We abyte ✓ ✓	1	27.0.0.1		Sequential Processing	V		
-S Save On Success Eventsource SSH Key Debug Off Debug Off Manage/Error Files Error Files Size 100 Megabyte Fror Files Reduction 10 0 Saved Files Size 100 Megabyte Saved Size Size 100 Megabyte Saved Size Size 100 Megabyte Saved Size Size Size Size Size Size Size Size	^.*9			Save On Error	\checkmark		
Image: Cancel OK Cancel OK Image: Concel Image: Concel Image	e Encoding UTF-8			Save On Success			
Debug Off Manage/Error Files I Error Files Size 100 Megabyte Error Files Count 65536 0 Error Files Reduction 10 0 Manage Saved Files I I Saved Files Size 100 Megabyte Saved Files Count 65536 0 Saved Files Count 65536 0 Saved Files Reduction 10 0 % 10 0	abled 🔽			Eventsource SSH Key		10	
Debug Off Manage Error Files							
Cancel OK				Debug	Off		
Cancel OK				Manage/Error Files			
Cancel OK				Error Files Size		Megabyte	
Cancel OK				Error Files Count		0	
Cancel OK Cancel OK Saved Files Size 100 Megabyte Saved Files Count 65536 Saved Files Reduction 10 %				Error Files Reduction %		\diamond	
Cancel OK Saved Files Size 100 Megabyte • Saved Files Count 65536 0 Saved Files Reduction 10 0				Manage Saved Files			
Saved Files Count 65536 0 Saved Files Reduction 10 0	_		Cancel OK	Saved Files Size		Megabyte	~
Saved Files Reduction 10				Saved Files Count		0	
4				Saved Files Reduction		0	
4				96	19	×	
				•		Canad	

- 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.