

RSA NetWitness Logs

Event Source Log Configuration Guide



Enterprise IT-Security

Last Modified: Thursday, July 20, 2017

Event Source Product Information:

Vendor: [Enterprise IT-Security](#)

Event Source: SF-NoEvasion

Versions: 7.1

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: enterpriseitsfne

Collection Method: Syslog

Event Source Class.Subclass: Host.Mainframe

To configure the Enterprise IT event source to communicate with RSA NetWitness Suite, perform the following tasks:

- I. Configure the Enterprise IT event source
- II. Configure RSA NetWitness Suite for Syslog Collection

Configure the Enterprise IT Event Source

Perform the following tasks to configure the Enterprise IT Event Source:

1. Configure Enterprise IT-Security SF-NoEvasion components
2. Configure Enterprise IT-Security SF-NoEvasion to send syslog messages

Configure Enterprise IT-Security SF-NoEvasion components

Warning: Before enabling the necessary components for configuring NoEvasion to work with your RSA NetWitness Suite, you must configure the following information-providing features. For details, see your Enterprise IT-Security SF-NoEvasion installation documentation.

Feature	Related Utilities to Configure
Actor ID anonymity	SHERSHMF, PARM field, column 37 SSMFANYM, member of the _ HLQ_.SHRLCK.SCAN.SMFPARM data set.

Feature	Related Utilities to Configure
<p>Additional event tagging based on privileged user list, critical resource list, and automatic system element detection feature</p>	<p>SHERSMFR, PARM field, column 38</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: To enable additional event tagging, you must complete the following tasks:</p> <ul style="list-style-type: none"> • Configure the procedure that updates the privileged user list. The privileged user list is stored in the SSMFPRVU member of the _HLQ_.SHRLCK.SCAN.SMF Parm data set. • Define individual critical resources within the SSMFCRIR member of the _HLQ_.SHRLCK.SCAN.SMF Parm data set. </div>
<p>Additional device-related IP environment tagging, including Device_IP and Device_DNS tags</p>	<p>_HLQ_.SHRLCK.RSA.ENVRDATA.smfid data set</p>

To configure Enterprise IT-Security SF-NoEvasion:

Enable the following components:

- **SHERREAL** real-time sniffer
- **SHERBLOCK** real-time blocker and logger
- **Syslog Message Router** utility

Configure Enterprise IT-Security SF-NoEvasion to send syslog messages to NetWitness Suite

Warning: Before configuring NoEvasion to send syslog messages, you must download the RSA-specific **SIEM Connectors for z/OS mainframes** from <http://www.fedtke.com/engl/zseindex.htm>.

Note: All required materials, such as source code and sample JCL, are provided in the members of the **SSHKSAMP** samplib data set.

To configure Enterprise IT-Security SF-NoEvasion for syslog:

1. Use the SMP/E user modification UMODRSAF to create the EVNTRSAF load module.

Note: You do not need to modify the source code provided in the SSHKSAMP samplib data set.

2. Use the ALLOCREL job to allocate all required the RSA NetWitness Suite-related data sets for each system in the sysplex.
3. Use the test JCL provided in the EVNTRSAT job to test the RSA NetWitness Suite event log file creation.
4. Copy the JCL section from the EVNTRSAR sample into the SHERRPPR procedure.

Note: When copying the JCL section, you can omit the comments and copyright statements in the header.

Important: If you edit the active SHERRPPR STC proclib member, your changes become immediately active. This may cause JCL errors. To avoid these errors, use a test system first.

5. Copy the following members from the SSHKSAMP procedure into the `_HLQ_.SHRLCK.INITDECK` dataset.

Member	Copy-to Location
EVNTRSAE	<code>_HLQ_.SHRLCK.INITDECK (RSAUEN00)</code> Note: This member includes the USS STDENV standard environment statements and may require configuration. Contact your USS administrator for assistance.
EVNTRSAI	<code>_HLQ_.SHRLCK.INITDECK (RSAUCM00)</code> Note: You may need to configure the IP address of the syslog daemon in the BPXBATCH USS command.

6. To edit the location where the IP address of the RSA NetWitness Suite syslog daemon is stored, do one of the following:
 - Define the IP address of the RSA NetWitness Suite syslog daemon in the RSAUCM00 member of the `_HLQ_.SHRLCK.INITDECK` dataset.
 - To define the IP address of the RSA NetWitness Suite syslog daemon in the z/OS USS environment:
 - a. Create a separate `/home/RSA_NetWitness Suite_syslog_message_routing` script file by adapting the RSAUCM00 member.
 - b. Within the configuration of the script file, specify the IP address of the RSA NetWitness Suite syslog daemon as a parameter of the Syslog Message Router utility command.

Note: Use a DNS-based IP address to identify the syslog daemon.

7. Copy the control parameter input of the EVNTRSAT sample job and use it to create the RSAEVR00 member in the `_HLQ_.SHRLCK.INITDECK` dataset.

Configure RSA NetWitness Suite

Perform the following steps in RSA NetWitness Suite:

- Ensure the required parser is enabled
- Configure 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**.
2. 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 **enterpriseitsfne**.



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**, click the icon to start capturing Syslog.
- If you see  **Stop Capture**, 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**.
2. 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.

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.