

# RSA NetWitness Logs

## Event Source Log Configuration Guide



## Safestone DetectIT

Last Modified: Monday, April 24, 2017

### Event Source Product Information:

**Vendor:** [Safestone](#)

**Event Source:** DetectIT

**Versions:** 14.3

### RSA Product Information:

**Supported On:** NetWitness Suite 10.0 and later

**Event Source Log Parser:** detectit

**Collection Method:** Syslog

**Event Source Class.Subclass:** Security.Analysis

To configure Syslog collection for Safestone DetectIT you must:

- I. Configure Syslog Output on Safestone DetectIT
- II. Configure NetWitness Suite for Syslog Collection

## Configure Syslog Output on Safestone DetectIT

**Warning:** You must install Safestone DetectIT from the Safestone downloads web page.

### To configure Safestone DetectIT:

1. Log on to the IBM i console with the **Alert** profile.
2. To set up the Safestone DetectIT basic system controls, follow these steps:
  - a. In the **DetectIT System Master** menu, select **Security Audit and Detection**, and press ENTER.
  - b. In the **Security Audit and Detection** menu, select **System Control Maintenance**, and set values as follows.

Field	Value
Daily Reporting Time	2200
	<b>Note:</b> If you want to use your own routines to control the reporting time, set the <b>Daily Reporting Time</b> field to <b>9999</b> , and insert the command ALERTEOD in the appropriate part of your own user-defined End Of Day procedure.
Timeout Control Method	R
	<b>Note:</b> If you are already using the OS/400 time-out facility and you do not want to affect users who do not use DetectIT, set the <b>Timeout Control Method</b> field to <b>R</b> . If you set this field to <b>M</b> , DetectIT will control time-out processing.
Timeout Run Priority	10
Sign On Attempts Allowed	3

Field	Value
System Security Level	3
Output Program Usage Audit	Y
Store Records for Number of Days	3

- c. To update the settings, press F14.
  - d. In the Maintain RGZPFM for Daily Reporting window, press ENTER to return to the **DetectIT System Master** menu.
3. If you do not use the UNIX system log daemon (syslogd) within PASE on your IBM i, to create the TCP/IP connection for syslogd, follow these steps:

**Note:** DetectIT uses UNIX remote syslog processing to send transactions to RSA NetWitness Suite. You must create a TCP/IP connection for syslogd so that DetectIT can control the running of syslogd. After you configure the TCP/IPO connection, DetectIT job ALERTDS07 will run syslogd.

- a. In the **DetectIT System Master** menu, select **Security Audit and Detection**, and press ENTER.
  - b. In the **Security Audit and Detection** menu, select **Work with TCP/IP Connections**, and press ENTER.
  - c. To add a new product connection, in the Work with TCP/IP window, press F6 .
  - d. In the Product selection screen (TCP/IP) window, navigate to **SYSLOGD** and, in the **Opt** column, type **1** to select syslogd.
  - e. To accept the default port number, press ENTER
  - f. Press ENTER until you return to the **DetectIT System Master** menu.
4. To create the TCP/IP profile, follow these steps:

**Note:** A TCP/IP profile acts as a global switch, allowing an administrator to activate or deactivate the transaction process with RSA NetWitness Suite.

- a. In the **DetectIT System Master** menu, select **Security Audit and Detection**, and press ENTER.
- b. In the **Security Audit and Detection** menu, select **Work with Profile TCP/IP Address**, and press ENTER.
- c. To add a new profile TCP/IP address, in the Work with Profile TCP/IP Address window, press F6.
- d. In the Maintain TCP/IP address for profile window, type **\*NETWITNESS**, and press ENTER.
- e. Set the values as follows.

Field	Value
TCP/IP Address	127.000.000.001
Comment / Description	Integration with the RSA NetWitness Suite

- f. To apply the settings, press ENTER.
  - g. Press F3 until you return to the **DetectIT System Master** menu.
5. To set up Syslog/Syslog forwarding, follow these steps:

**Note:** For DetectIT to send transactions to RSA NetWitness Suite, you must configure another appliance to receive UNIX remote syslog entries. Ensure that, for example, the TCP/IP host table and the DNS server that can be accessed by the IBM i contain the required remote identification details. To set these requirements, contact your infrastructure personnel or see the appropriate documentation.

- a. To access an IBM i PASE shell session, in the **DetectIT System Master** menu or any available command line, type:
 

```
CALL PGM(QP2TERM)
```
- b. To ensure that the syslog configuration file, **syslog.conf**, exists, change directories to **/QOpenSys/etc**, and type:
 

```
ls syslog.conf
```
- c. If the syslog configuration file does not exist, to create the **syslog.conf** file, follow these steps:

i. Type:

```
echo "# Created for Safestone DetectIT integration with the
RSA NetWitness Suite" > syslog.conf
```

ii. Type:

```
chmod 640 syslog.conf
```

iii. To add the details of the appliance receiving the UNIX remote syslog entries, type:

```
echo "*.info\t@RemoteMachineName" >> syslog.conf
```

where *RemoteMachineName* is the name of the appliance receiving the UNIX remote system entries. This name must be registered within your TCP/IP host table or DNS server.

iv. To review the contents of the **syslog.conf** file, type:

```
cat syslog.conf
```

6. To set up the audit collection details, follow these steps:

- a. In the **DetectIT System Master** menu, select **Security Audit and Detection**, and press ENTER.
- b. In the **Security Audit and Detection** menu, select **Set Up Auditing Details**, and press ENTER.
- c. Set the values as follows.

Field	Value
Log Update Frequency (mins)	The interval at which to send messages to RSA NetWitness Suite. <div style="border: 1px solid green; padding: 5px; margin-top: 5px;"><b>Note:</b> If you set this value to <b>000</b>, messages will be collected and sent to NetWitness only when the DetectIT End Of Day procedure runs.</div>
Omit Internal Job Messages	Y
Retain System Audit (Days)	1
Retain Archive Reports (Days)	0
Retain File	0

Field	Value
Monitor (Days)	
File mon. freq update (mins)	000
Omit Object Auditing?	Y
Audit SQL requests?	N
Exit Point freq update (mins)	000

- d. Press ENTER.
- e. Set the values as follows.

Field	Value
Use QAUDJRN Auditing	If you are not using QAUDJRN, set this field to <b>Y</b> . To use QAUDJRN with your own routines, or other third-party routines, set this field to <b>U</b> .
QAUDJRN Auditing - QAUDLVL	Enter the required values. To retrieve current system values, press F9.
QAUDJRN Auditing - QAUDLVL2	Enter the required values.

**Note:** These fields can only be updated from V5R3M0 and later.

- f. To apply the settings, press ENTER until you return to the **Security Audit and Detection** menu.
7. To configure the messages to send to RSA NetWitness Suite, follow these steps:
- a. In the command line from the **Security Audit and Detection** menu, type:

STRALERT

**Note:** If the message, "Subsystem name ALERT active," is displayed, the subsystems are already started. Ignore this message.

- b. In the **Security Audit and Detection** menu, select **Work With Message**

**Monitor**, and press ENTER.

A list of messages is displayed.

- c. To select a message that you want to send to RSA NetWitness Suite, follow these steps:
  - i. Press DOWN until you locate the message ID.
  - ii. Type **12** against the message ID, and press ENTER.
  - iii. In the Message Action Item window, set the **External interface** field to **\*NETWITNESS**. Leave the other fields as default.
  - iv. Press ENTER.
  - v. Repeat steps i to iv for every message that you want to send to NetWitness.
- d. If you do not find a message that you want to send to NetWitness, to add the message, follow these steps:
  - i. Press F6.
  - ii. In the **Enter Security Message ID** field, enter a message ID that DetectIT has configured within RSA NetWitness Suite, and press ENTER.
  - iii. In the **Message description** field, enter the description of the message, and press ENTER.
  - iv. In the Message Action Item window, set the **External interface** field to **\*NETWITNESS**. Leave the other fields as default.
  - v. Press ENTER, and press F3.
  - vi. Repeat steps i to v for every message that you want to send to RSA NetWitness Suite.

## 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 **detectit**.

### 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.