RSA NetWitness Logs

Event Source Log Configuration Guide

RSA ECAT

Last Modified: Monday, November 6, 2017

Event Source Product Information:

Vendor: RSA, The Security Division of EMC
Event Source: ECAT
Versions: 3.4, 4.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

Supported On:
version 3.4: NetWitness Suite 10.0 and later
version 4.x: Security Analytics 10.4 and later
Event Source Log Parser: rsaecat
Collection Method: Syslog
Event Source Class.Subclass: Security.Antivirus

To configure Syslog collection for RSA ECAT you must:

I. Configure NetWitness Suite for Syslog Collection

II. Configure Syslog Output on RSA ECAT

Configure 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 **rsaecat**.

Configure Syslog Collection

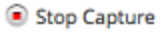
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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 

, click the icon to start capturing Syslog.
- If you see 

, 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.

Configure Syslog Output on RSA ECAT

Use the appropriate instructions for your version:

- Configure RSA ECAT Version 4.x, or
- Configure RSA ECAT Version 3.4

Configure RSA ECAT Version 4.x

To configure RSA ECAT to send logs to the RSA NetWitness Suite Log Decoder or Remote Log Collector:

1. Open ECAT and log in using the proper credentials.
2. On the menu bar select **Configure** > **Monitoring and External Components**.
3. Right-click in the dialog box, and then select **Add Component**.
4. In the dialog box, you see the fields required to enable Syslog messaging:

Field	Action
Unique Name	Enter a descriptive name.
IP	Enter the IP address of the RSA NetWitness Suite Log Decoder or Remote Log Collector.
Port	Enter port **514**.

5. Click the **Settings** button.
6. In the Configure Syslog dialog box, select **UDP** for the transport protocol.
7. Click **Save** twice, to close the dialog boxes.
8. Click on the check box to enable the component.
9. Press **Close** to finish.

Configure RSA ECAT Version 3.4

To configure RSA ECAT to send logs to the RSA NetWitness Suite Log Decoder or Remote Log Collector:

1. Open ECAT and log in using the proper credentials.
2. On the menu bar select **Tool** > **Monitoring Configuration**.
3. Under Monitoring Configuration, select the **Syslog** tab.
4. In the Syslog configuration tab, you will see the fields required to enable Syslog messaging:

Field	Action
Enabled	Must be checked for the messages to be sent.
Syslog server protocol	Select **UDP**.
Syslog server IP address	Enter the IP address of the RSA NetWitness Suite Log Decoder or Remote Log Collector.
Syslog server port	Select port **514**.
Suspect level threshold	RSA recommends to select **0**.

5. Press **Ok** to finish.

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.