

# RSA NetWitness Logs

## Event Source Log Configuration Guide



## Damballa Failsafe

Last Modified: Thursday, May 11, 2017

### Event Source Product Information:

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

**Event Source:** Damballa Failsafe

**Version:** 5.0.2, 6.2.0

### RSA Product Information:

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

**Event Source Log Parser:** damballa

**Collection Method:** Syslog

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

# Configure Damballa

---

Damballa Failsafe is a threat protection solution. The Damballa Failsafe sensors monitor DNS, egress and proxy traffic and use deep packet inspection engines to correlate suspicious behaviors to identify and isolate a breach.

To configure Syslog collection for the Damballa Failsafe event source, you must:

- I. Configure Syslog Output on Damballa Failsafe
- II. Configure RSA NetWitness Suite for Syslog Collection

## Configure Syslog Output on Damballa Failsafe

To configure Damballa Failsafe to send syslog messages to the RSA NetWitness Suite platform:

1. Log onto the Failsafe Management Console
2. From the top menu, choose **Setup > Integration Settings**.
3. From the Settings menu, select the **Syslog** tab.

The Integration Settings dialog box appears.

**Integration Settings**  
Manage your settings.

Lancope SMC   ArcSight ESM   Q1 QRadar   **Syslog**

**Syslog Settings**

**Enable Publishing to Syslog?**

**Syslog Hostname**

**Enable Syslog Header**

**Syslog Facility** kernel ▾

**Syslog Severity** emergency ▾

**Syslog Port (Destination)**  (optional)

**Syslog Port (Source)**  (optional)

Save

4. In the Integration Settings dialog box, configure the Syslog Settings below and then select **Save**.

Field	Action
<b>Enable Publishing to Syslog</b>	Select
<b>Syslog Hostname</b>	Enter the IP address of your RSA NetWitness Suite Log Decoder or Remote Log Collector.
<b>Enable Syslog</b>	Select

Field	Action
<b>Header</b>	
<b>Syslog Facility</b>	Select <b>local6</b>
<b>Syslog Severity</b>	Select <b>emergency</b>
<b>Syslog Port (Destination)</b>	Enter 514

The integration of Damballa Failsafe with RSA NetWitness Suite supports the following events:

- Connection Attempt
- DNS Query
- Malware Download
- Domain Flux

## 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 **damballa**.



### 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.