

RSA NetWitness Logs

Event Source Log Configuration Guide



Symantec DLP

Last Modified: Thursday, April 12, 2018

Event Source Product Information:

Vendor: [Symantec](#)

Event Source: Data Loss Prevention

Versions: 10.5.1, 11, 12.x, 14.x, 15.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: NetWitness Platform 10.0 and later

Event Source Log Parser: symantecdpl

Collection Method: Syslog

Event Source Class.Subclass: Security.DLP

To configure Symantec DLP to work with RSA NetWitness Platform, perform the following tasks:

- Configure Symantec DLP
- Configure Syslog Collection in NetWitness Platform

Configure Symantec DLP

Complete the following tasks on the Symantec DLP event source:

1. [Configure System Events](#)
2. [Configure Response Rules](#)
3. [Enable Rules](#)

Configure System Events

To configure system events:

1. On your Vontu system, depending on your operating system, choose one of the following:
 - For Windows, change directories to `\Vontu\Protect\config`.
 - For Linux, change directories to `/opt/Vontu/Protect/config`.
2. Open **Manager.properties** in a text editor.
3. Remove the number sign (#) from the line, `#systemevent.syslog.host=`, and then enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
4. Remove the # from the line, `#systemevent.syslog.port=`, and then type **514**.
5. Remove the # from the line, `#systemevent.syslog.format= [{0}] {1} - {2}`.
6. Save and close the file.
7. Restart the Vontu server.

Configure Response Rules

To configure response rules:

1. Log on to the Symantec DLP user interface.
2. Click **Policies > Response Rules > Add Response Rule**.
3. Select **Automated Response**.

4. Click **Next**.
5. In the Configure Response Rule window, complete the fields as follows.

Field	Action
Rule Name	Enter a rule name.
Description	Enter a description for the rule name.

6. From the **Action** drop-down list, select **All: Log to a Syslog Server**.
7. Click **Add Action**.
8. Complete the fields as follows.

Field	Action
Host	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Port	Type 514 .
Message	<p>For versions before 11.6, enter the following:</p> <pre>\$POLICY\$\$INCIDENT_ID\$\$SUBJECT\$\$SEVERITY\$\$MATCH_COUNT\$\$RULES\$\$SENDER\$\$RECIPIENTS\$\$BLOCKED\$\$FILE_NAME\$\$PARENT_PATH\$\$SCANS\$\$TARGET\$\$PROTOCOL\$\$INCIDENT_SNAPSHOT\$</pre> <p>For versions 11.6 up to (but not including) version 12, enter the following:</p> <pre>\$POLICY\$\$INCIDENT_ID\$\$SUBJECT\$\$SEVERITY\$\$MATCH_COUNT\$\$RULES\$\$SENDER\$\$RECIPIENTS\$\$BLOCKED\$\$FILE_NAME\$\$PARENT_PATH\$\$SCANS\$\$TARGET\$\$PROTOCOL\$\$INCIDENT_SNAPSHOT\$</pre> <p>For versions 12 and above, enter the following:</p> <pre>\$BLOCKED\$\$INCIDENT_ID\$\$INCIDENT_SNAPSHOT\$\$POLICY\$\$RECIPIENTS\$\$SENDER\$\$SEVERITY\$\$SUBJECT\$\$FILE_NAME\$\$INCIDENT_ID\$\$MATCH_COUNT\$\$PARENT_PATH\$\$PATH\$\$POLICY\$\$RULES\$\$QUARANTINE_PARENT_PATH\$\$SCAN\$\$TARGET\$\$PROTOCOL\$</pre> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p>Warning: This is one continuous entry. Do not add spaces or hyphens.</p> </div>
Level	Select 4 .

9. Click **Save**.

Enable Rules

To enable rules:

1. Click **Policies > Policy List**.
2. Select a policy that you want to report on.
3. Click the **Response** tab.
4. From the drop-down list, select the rule you created in the previous task.
5. Click **Add Response Rule**.

Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- 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 Platform 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 `symantecdlp`.



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 © 2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.