

RSA NetWitness Logs

Event Source Log Configuration Guide



HP Integrity NonStop Server™

Last Modified: Wednesday, August 09, 2017

Event Source Product Information:

Vendor: [HP](#)

Event Source: Integrity NonStop Server™

Prerequisites:

- XYGATE Merged Audit version 1.71 or later
- The Xypro RSA enVision Log Adapter module

Versions: All NonStop OS releases supported by HP

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: hnonstopserver

Collection Method: Syslog

Event Source Class.Subclass: Security.Analysis

To configure Syslog collection for the HP Integrity NonStop Server event source, you must:

- I. Configure HP Integrity NonStop Server
- II. Configure NetWitness Suite for Syslog Collection

Configure HP Integrity NonStop Server

XYGATE is a suite of access control, authentication, compliance and audit software that enhances security functions native to the HP NonStop™ Server platform. XYGATE brings industry-best security to HP NonStop server customers, including sophisticated audit reporting, log amalgamation and seamless integration with the RSA NetWitness Suite solution.

Log Adapter Module

To obtain the Xypro RSA Log Adapter module:

1. Send a request to RSAFilter@xypro.com.

Note: This module must be purchased from Xypro.

2. Instructions for installation and configuration will be provided by Xypro.

BASE24 Events

XYPRO supports the collection of BASE24 / BASE24-eps events, on NonStop systems, to be collected by XYGATE Merged Audit and sent to the RSA NetWitness Suite platform.

Note the following:

- Since 2010, HP bundles XYGATE Merged Audit (XMA) with all HP NonStop systems
- XMA collects, merges, filters, normalizes and writes NonStop audit data to a single SQL database
- XYPRO has developed an **RSA Log Adapter** to enable XMA to feed security events to the RSA NetWitness Suite
- XYPRO also has developed two Log Collectors to enable XMA to collect security event information from the BASE24 and BASE24-eps applications



- The BASE24 Log Collector and/or BASE24-eps Log Collector enable event information within those applications to be collected by XMA and the RSA Log Adapter enables the normalized information to be sent to RSA NetWitness Suite
- XYPRO recommends the customer contact their XYPRO sales representative for assistance

Configure NetWitness Suite for 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.