RSA NetWitness Logs

Event Source Log Configuration Guide

HyTrust CloudControl

Last Modified: Friday, May 19, 2017

Event Source Product Information:

Vendor: HyTrust
Event Source: CloudControl (formerly HyTrust Appliance)
Versions: 2.0.10264, 2.5.1, 3.0.2, 3.6, 4.0

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: hytrust
Collection Method: Syslog
Event Source Class.Subclass: Security.Access Control

Configure HyTrust CloudControl

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

I. Configure RSA NetWitness Suite for Syslog Collection

II. Configure Syslog Output on the appropriate version of HyTrust:

- Configure HyTrust 3.6, and later, or
- Configure HyTrust 3.0.2 and earlier

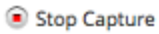
Configure RSA NetWitness Suite for Syslog Collection

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 

, 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 HyTrust 3.6 and later

This section describes how to configure HyTrust version 3.6.

To set up HyTrust Appliance (3.6) or HyTrust CloudControl (4.0) to send logs to RSA NetWitness Suite:

1. Log on to the HyTrust web interface.
2. Click **Configuration** > **Logging**.
3. In the **HTA Logging Configuration** section, complete the fields as follows:

Field	Action
Logging Level	From the drop-down list, select **INFO**.
HTA Logging Aggregation	Select **External**.
Logging Aggregation Template Type	Select **Proprietary**.
Syslog Server	Enter the IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.

4. In the **Host Default Logging Configuration** section, complete the fields as follows:

Field	Action
Default Logging Aggregation	Select **Explicit Syslog Server**.
Default Syslog Server	Enter the IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.

5. Click **Apply**.

Configure HyTrust 3.0.2 and Earlier

This section describes how to configure HyTrust versions up to and including 3.0.2.

To set up HyTrust Appliance to send logs to RSA NetWitness Suite:

1. Log on to the HyTrust web interface.
2. Click **Configuration** > **Logging**.
3. In the **HTA Logging Configuration** section, complete the fields as follows:

Note: In the following table **Logging Aggregation Template Type** is only required for HyTrust Appliance version 3.0.2.

Field	Action
Logging Level	From the drop-down list, select **INFO**.
HTA Logging Aggregation	Select **External**.
Logging Aggregation Template Type	Select **Proprietary**.
Syslog Server	Enter the IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.

4. Click **Validate**.

Note: Step four is not required for HyTrust Appliance version 3.0.2.

5. Click **Apply**.

Trademarks