

RSA NetWitness Logs

Event Source Log Configuration Guide



Cloudera Navigator

Last Modified: Thursday, May 11, 2017

Event Source Product Information:

Vendor: [Cloudera](#)

Event Source: Navigator

Versions: 4.8, 5.x

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: clouderanavigator

Collection Method: Syslog

Event Source Class.Subclass: Security.Access Control

To configure Cloudera Navigator, you must complete the following tasks:

- Configure Cloudera Navigator
- Configure NetWitness Suite for Syslog

Configure Cloudera Navigator

1. To configure the "auditStream" logger to integrate with syslog, click **CM** > **Management Services** > **Configuration**.

2. Search for **Navigator server logging safety valve**, and enter the following:



```
log4j.logger.auditStreamEnVision = TRACE, SYSLOG
log4j.additivity.auditStreamEnVision = false
log4j.appender.SYSLOG = org.apache.log4j.net.SyslogAppender
log4j.appender.SYSLOG.SyslogHost = <IP address of the RSA
NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log
Collector>
log4j.appender.SYSLOG.Facility = Local2
log4j.appender.SYSLOG.FacilityPrinting = true
```

Configure NetWitness Suite for Syslog

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.