RSA NetWitness Logs

Event Source Log Configuration Guide

Cisco IOS

Last Modified: Tuesday, May 09, 2017

Event Source Product Information:

Vendor: Cisco
Event Source: IOS
Versions: IOS 12.4, 15.x

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: ciscorouter
Collection Method: Syslog
Event Source Class.Subclass: Network.Router

Configure Cisco IOS

Note: Cisco IOS will be discovered as Cisco Switch Router on the RSA NetWitness Suite platform.

To configure Syslog collection for the Cisco IOS you must:

I. Configure NetWitness Suite for Syslog Collection

II. Configure Syslog Output on Cisco IOS

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.

Configure Syslog Output on Cisco IOS

To configure Syslog output on Cisco IOS:

1. Connect to the Router box and enter **CONFIG** mode.

2. Type **logging *IP-address***, and press ENTER to set the logging host

   where IP-address is the IP address of the RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.

3. Type **logging trap *syslog-level***, and press ENTER to set the logging level

   where syslog-level is the level of messages to be logged.

   Values for syslog level include: **emergencies, alerts, critical, errors, warnings, notifications, informational**, and **debugging**. Use **debugging** to ensure full logging.

4. Type **logging source-interface*vlan interface-name***, and press ENTER to set the logging interface

   where *vlan* is the VLAN that the RSA NetWitness Suite logging host is assigned to (if applicable) and *interface-name* is the name of the logging source.

5. Type **logging on**, and press ENTER to turn on logging.

6. Type **service timestamps log datetime localtime show-timezone msec year**, and press ENTER to enable timestamps.

7. If you do not want to use access lists, go to step **8**. Otherwise, proceed as follows.

a. Configure access lists:

   i. Type **access-list** ***access-list-number*** **permit tcp any log**, and press ENTER where access-list-number is any number between **100** and **199**.

   ii. Type **access-list** ***access-list-number*** **permit ip any log**, and press ENTER where access-list-number is any number between **100** and **199**.

   If you already have access lists on your router, make sure that your **access-list** command contains the **log parameter** shown. If you do not have access lists on your router, the parameter opens all traffic through your router while still allowing you to track the connection traffic.

b. Type **interface** ***interface_name***, and press ENTER:

```
router(config)#interface fastethernet 0/1
router(config-if)#
```

c. Type **ip access-group** ***access-list-number*** **in**, and press ENTER to set access list logging
   where access-list-number is any number between **100** and **199**.

d. Type **ip access-group*****access-list-number*****out**, and press ENTER to set access list logging
   where access-list-number is any number between **100** and **199**.

e. Repeat steps **c** and **d** for each logging source interface.

8. Configure audit trails (using IOS Firewall feature set commands):

   a. Type **ip inspect audit-trail**, and press ENTER to turn on the audit trail messages.

   b. Type i**p inspect name** ***inspection-name*****http**, and press ENTER to set the inspection parameters. Repeat this step for each protocol to be inspected, for example tcp, udp, and ftp.
   where inspection-name is any name you choose.

   c. Type **ip inspect** ***inspection-name*****in**, and press ENTER
   where inspection-name is one of the names you chose in Step b.

   d. Type **ip inspect*****inspection-name*****out**, and press ENTER
   where inspection-name is one of the names you chose in Step b.

   e. Repeat Steps c and d on each logging source interface.

Trademarks