RSA NetWitness Logs

Event Source Log Configuration Guide

Cisco Aironet AP (Wireless Access Point)

Last Modified: Friday, March 31, 2017

Event Source Product Information:

Vendor: Cisco
Event Source: Aironet AP (Wireless Access Point)
Version: IOS 12.2

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

To configure the Cisco Aironet AP event source, you must:

I. Configure Syslog Output on Cisco Aironet AP
II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog Output on Cisco Aironet AP

The following procedure describes how to configure Syslog output on your device.

To configure Cisco Aironet AP:

1. Connect to the Router box and enter the **CONFIG** mode.
2. Type **logging *IP address*** (where ***IP address*** is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector) and press **Enter** to set the logging host.
3. Type **logging trap *syslog level*** (where ***syslog level*** is the level of messages to be logged) and press **Enter** to set the logging level.

   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 *interface name*** (where ***interface name*** is the name of the logging source) and press **Enter** to set the logging interface.
5. Type **logging on** and press **Enter** to turn on logging.
6. Type **no service timestamps** and press **Enter** to turn of 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 any log** (where ***access list number*** is any number between 100 and 199) and press **Enter**.
      ii. Type **access-list *access list number* permit ip any any log** (where ***access list number*** is any number between 100 and 199) and press **Enter**.

      If you already have access lists on your router, ensure 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 **config-if** and press **Enter** to turn on the Configuration-Interface mode.
   c. Type **ip accounting output-packets** and press **Enter** to turn on IP accounting.
   d. Type **ip accounting access-violations** and press **Enter** to turn on IP access accounting.

e. Type **ip access-group *access-list number* in** (where ***access list number*** is any number between 100 and 199) and press **Enter** to set access list logging.

f. Type **ip access-group *access-list number* out** (where ***access list number*** is any number between 100 and 199) and press **Enter** to set access list logging.

g. Repeat steps **c** through **f** 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 **ip inspect name *inspection name* http** (where ***inspection name*** is any name you choose) and press **Enter** to set the inspection parameters. Repeat this step for each protocol to be inspected (tcp, udp, ftp, and so forth).

c. Type **ip inspect *inspection name* in** (where ***inspection name*** is one of the names you chose in step **b**) and press **Enter**.

d. Type **ip inspect *inspection name* out** (where ***inspection name*** is one of the names you chose in step **b**) and press **Enter**.

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

Note: It is likely that Wireless specific messages will appear as unknown messages.

Configure RSA NetWitness Suite

Perform the following steps in RSA NetWitness Suite:

- 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 Suite 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 **ciscorouter**.

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.

Trademarks