RSA NetWitness Platform

Event Source Log Configuration Guide

Cisco Switch

Last Modified: Monday, March 11, 2019

Event Source Product Information:

Vendor: Cisco
Event Source: Catalyst Switch
Versions: Cisco Catalyst 6500, Cisco Catalyst 2960-CX

RSA Product Information:

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

To configure the Cisco Switch event source, you must:

I. Configure Cisco Switch

II. Configure RSA NetWitness Platform for Syslog Collection

Configure Cisco Switch

To configure Cisco Switch, you must complete these tasks:

- Configure Cisco Catalyst Switch via web interface: for CATOS software
- Configure Cisco Switch to collect syslog messages: for IOS software

Configure Via Web Interface

Note: You can configure the Cisco Catalyst Switch using the web interface or without using the web interface.

To configure the Cisco Catalyst Switch via the web interface:

1. On a web browser, log on to the Switch's Visual Switch Manager.
2. Select **Fault** > **Logging Config**.
3. Scroll down to the **Syslog Status** area.
4. Add a system **Host**.
5. Set **Logging Level** to **Debugging**.
6. Set **Logging Timestamp Enable**.
7. Set **Facility** to **Local7**.
8. Apply the changes.

Configure Cisco Switch to Collect Syslog Messages

This section describes how to configure IOS software to communicate with RSA NetWitness Platform.

To configure Cisco Switch:

1. Connect to the Switch 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 Log Decoder or 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 NetWitness Platform 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 `ip inspect name` ***`inspection-name`*** `http` and press **Enter** to set the inspection parameters, where ***inspection-name*** is any name you choose.

Repeat this step for each protocol to be inspected (**tcp**, **udp**, **ftp**, and so forth).

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.

Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- 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 Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN** > **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

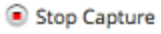
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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 

, 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.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.