RSA NetWitness Platform

Event Source Log Configuration Guide

Aruba Networks ClearPass Policy Manager

Last Modified: Wednesday, February 20, 2019

Event Source Product Information:

Vendor: Aruba Networks
Event Source: ClearPass Policy Manager
Versions: 5.2, 6.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

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

To configure the Aruba Networks ClearPass Policy Manager event source, you must:

I. Configure Syslog Output on Aruba Networks ClearPass Policy Manager

II. Configure RSA NetWitness Platform for Syslog Collection

Configure Aruba Networks ClearPass Policy Manager

Aruba Networks ClearPass Policy Manager integration with RSA NetWitness Platform supports system events, audit records, and session logs (with support for limited columns).

Configuration Steps

To configure Aruba Networks ClearPass Policy manager to work with RSA NetWitness Platform:

1. Log onto the ClearPass Policy Manager Web console.
2. From the left menu, choose **Administration > External Servers > Syslog targets**.
3. Click **Add Syslog Target**, and enter the information provided below in the **Add Syslog Target** window:

Field	Action
Host Address	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Description	Type **NetWitness**
Server Port	Enter **514**

4. Click **Save**.
5. To add logs for System Events:
   a. From the left menu, choose **Administration > External Servers > Syslog Export Filters**
   b. Click **Add Syslog Filter**, and enter the information provided below in the **Syslog**

Export Filters window in the **General** tab:

Field	Action
Name	Type **Aruba-ClearPass system event**
Description	Type **System Events**
Export Template	Select **System Events** from the drop-down menu.
Export Event Format Type	Select **Standard** from the drop-down menu.
Syslog Server	Choose the Syslog target that you created in step 3.

c. Click **Save**.

6. To add logs for Audit Records:

a. Click **Add Syslog Filter** again, and enter the information provided below in the **Syslog Export Filters** window in the **General** tab:

Field	Action
Name	Type **Aruba-ClearPass audit event**
Description	Type **Audit Records**
Export Template	Select **Audit Records** from the drop-down menu.
Export Event Format Type	Select **Standard** from the drop-down menu.
Syslog Server	Choose the Syslog target that you created in step 3.

b. Click **Save**.

7. To add Session Logs (with support for limited columns):

a. Click **Add Syslog Filter** again, and enter the information provided below in the **Syslog Export Filters** window in the **General** tab:

Field	Action
Name	Type **Aruba-ClearPass Session_Logs**
Description	Type **Session Logs**
Export Template	Select **Session Logs** from the drop-down menu.
Export Event Format Type	Select **Standard** from the drop-down menu.
Syslog Server	Choose the Syslog target that you created in step 3.

b. Click on the **Filter and Columns** tab next to the **General** tab.

c. Choose a **Data Filter** from the drop-down list.

> **Note:** RSA supports all of the Data Filter options.

d. Select a list of columns to be appended to the Syslog event from the **Predefined Field Groups** and **Available Columns** drop-down lists.

> **Note:** There is a list of columns that RSA currently supports in the Supported Columns for Session Logs section. All **Predefined Field Groups** are currently supported by RSA except for **Posture Request** and **RADIUS Response**.

e. Click **Save**.

8. Perform the following steps to add Insight logs.

a. Click **Add Syslog Filter** again, and enter the information provided below in the **Syslog Export Filters** window in the **General** tab.

Field	Action
Name	Type **Aruba-ClearPass Insight_Logs**
Description	Type **Insight Logs**
Export Template	Select **Insight Logs** from the drop-down menu.
Export Event Format Type	Select **Standard** from the drop-down menu.
Syslog Server	Choose the Syslog target that you created in step

Field	Action
	3.

b. Click the **Filters and Columns** tab (located next to the **General** tab).

c. Choose a data filter from the drop-down list.

d. From the **Predefined Field Groups** and **Available Columns** drop-down lists, select a list of columns to be appended to the Syslog event.

> **Note:** There is a list of columns that RSA currently supports in the Supported Columns for Insight Logs section.

e. Click **Save**.

Supported Columns for Session Logs

The following table shows supported Syslog Event fields for adding Session Logs.

Supported Syslog Event Fields for Session Logs		
access_device_ip	access_device_port	account_authentication_type
account_delay_time	account_input_octets	account_input_packets
account_output_octets	account_output_packets	account_session_time
accounting_service_type	acct_session_id	alert_message
audit_posture_token	auth_method	auth_source
authentication_action	authentication_type	called_station_id
calling_station_id	client_ip	client_port
command_privelege_level	end_host_id	enforcement_profiles
error_code	flags	framed_ip_address
login_status	monitor_mode	nas_ip_address
nas_port	nas_port_type	protocol
remote_ip	request_timestamp	roles

Supported Syslog Event Fields for Session Logs		
service_name	session_id	system_posture_status
tacacs_protocol_authentication_method	tacacs_protocol_authentication_service	termination_cause
user_session_id	username	

Supported Columns for Insight Logs

The following table shows supported Syslog Event fields for adding Insight Logs.

Supported Syslog Event Fields for Insight Logs		
Auth.Error-Code	Auth.Host-MAC-Address	Auth.Login-Status
Auth.NAS-IP-Address	Auth.Protocol	Auth.Roles
Auth.Service	Auth.Source	Auth.Username
CppmAlert.Alerts	CppmConfigAudit.Action	CppmConfigAudit.Category
CppmConfigAudit.Name	CppmConfigAudit.Updated-At	CppmConfigAudit.Updated-By
CppmErrorCode.Error-Code-Details	CppmNode.CPPM-Node	CppmSystemEvent.Action
CppmSystemEvent.Category	CppmSystemEvent.Description	CppmSystemEvent.Source
CppmSystemEvent.Timestamp	Endpoint.Added-At	Endpoint.Conflict
Endpoint.Device-Category	Endpoint.Device-Family	Endpoint.Device-Name
Endpoint.IP-Address	Endpoint.MAC-Address	Endpoint.MAC-Vendor
Endpoint.Status	Endpoint.Updated-At	Guest.Created-At
Guest.Enabled	Guest.Expires-At	Guest.MAC-Address
Guest.Starts-At	Guest.Username	Guest.Visitor-Company
Guest.Visitor-Name	OnboardCert.Issuer	OnboardCert.Mac-Address
OnboardCert.Revoked-At	OnboardCert.Subject	OnboardCert.Updated-At

Supported Syslog Event Fields for Insight Logs		
OnboardCert.Username	OnboardCert.Valid-From	OnboardCert.Valid-To
OnboardEnrollment.Device-Name	OnboardEnrollment.Device-Product	OnboardEnrollment.Device-Version
OnboardEnrollment.MAC-Address	OnboardEnrollment.Updated-At	OnboardEnrollment.Username
OnboardOCSP.Remote-Address	OnboardOCSP.Response-StatusName	OnboardOCSP.Timestamp
Radius.Calling-Station-Id	Radius.Duration	Radius.Input-bytes
Radius.NAS-IP-Address	Radius.Output-bytes	Radius.Start-Time
Radius.Username	Tacacs.Authen-Service	Tacacs.Auth-Source
Tacacs.NAS-IP-Address	Tacacs.Roles	Tacacs.Username

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 **arubacppm**.

Configure Syslog Collection

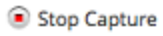
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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.