RSA NetWitness Platform

Event Source Log Configuration Guide

Cisco Secure Access Control Server

Last Modified: Tuesday, January 29, 2019

Event Source Product Information:

Vendor: Cisco
Event Source: Access Control Server
Versions:

- Software Only: 4.2
- Appliance: 5.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: ciscosecureacs
Collection Method: Syslog
Event Source Class.Subclass: Security.Access Control

To configure Syslog collection for the Cisco ACS you must:

I. Configure Syslog Output on Cisco ACS for your version:
   - Configure Cisco ACS version 4.2, or
   - Configure Cisco ACS version 5.x

II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Cisco ACS

Set Up Cisco ACS 4.2

To set up Cisco ACS 4.2 for Syslog collection:

1. Click **Interface Configuration** > **Advanced Options**.
2. Select all of the options, and click **Submit**.
3. Click **System Configuration** > **Logging**.
4. In the **Syslog** column, click the **Configure** link of an entry listed that you want to configure.
5. Under **Enable Logging**, select **LOG to Syslogreport**.
6. Select only the following columns in the following order:
   - **Failed Attempts**
     Message-Type, User-Name, Group-Name, Caller-ID, Called-Station-Id, Authen-Failure-Code, Author-Failure-Code, Author-Data, NAS-IP-Address, NAS-Port, Network Device Group, System-Posture-Token, Application-Posture-Token, AAA Server, Access Device, Network Access Profile Name, Priv-lvl
   - **Passed Authentications**
     Message-Type, User-Name, Group-Name, Caller-ID, Called-Station-Id, NAS-IP-Address, NAS-Port, Network Device Group, System-Posture-Token, Application-Posture-Token, AAA Server, Access Device, Network Accss Profile Name, Real Name, Description, Priv-lvl
   - **RADIUS Accounting**
     User-Name, Group-Name, Calling-Station-Id, Called-Station-Id, NAS-IP-Address, NAS-Port, Acct-Status-Type, Acct-Session-Id, Acct-Session-Time, Service-Type, Framed-IP-Address, Framed-Protocol, Login-IP-Host, Acct-Authentic, AAA

Server, ExtDB Info, Access Device, Acct-Terminate-Cause, Acct-Input-Octets, Acct-Output-Octets

- **TACACS+ Accounting**
  User-Name, Group-Name, Caller-Id, Acct-Flags, priv-lvl, elapsed_time, service, bytes_in, bytes_out, NAS-IP-Address, NAS-Portname, cmd
- **TACACS+ Administration**
  User-Name, Group-Name, Caller-Id, Acct-Flags, priv-lvl, cmd, service, NAS-IP-Address, NAS-Portname, reason
- **Backup and Restore**
  No fields available
- **Database Replication**
  No fields available
- **Administration Audit**
  No fields available
- **ACS Service Monitoring**
  No fields available

7. Under **Syslog Servers**, complete the fields as follows:
   - In the **IP Address** field, enter the IP address of the RSA NetWitness Platform.
   - In the **Port** field, type `514`.
   - In the **Max Message Length** field, type `1024`.
8. Click **Submit**.
9. Repeat steps 4 through 8 for each of the required logs.
10. Complete the following steps so that the log files are created with a time stamp that the RSA NetWitness Platform can correctly interpret:
    a. Select **System Configuration** > **Date Format Control**.
    b. Select the **Use 'Month/Day/Year' format**.
    c. Select **Submit & Restart**.

Set Up Cisco ACS Appliance 5.x

To set up Cisco ACS Appliance Syslog collection:

1. Log on to the Cisco Secure ACS online User Interface with administrator credentials.
2. To configure RSA NetWitness Platform as a log target, follow these steps:
   a. Click **System Administration** > **Log Configuration** > **Remote Log Targets**.

      Note: In version 5.5, click **System Administration** > **Configuration** > **Log Configuration** > **Remote Log Targets**.

   b. Click **Create**.
   c. In the **Name** field, enter the name of your RSA NetWitness Platform.
   d. In the **IP Address** field, enter the IP address of your RSA NetWitness Platform.
   e. Click **Submit**.
3. To configure which logs to send to RSA NetWitness Platform, follow these steps:
   a. Click **System Administration** > **Log Configuration** > **Logging Categories** > **Global**.
   b. Select a logging category for which you want to receive logs.
      i. Click the **Remote Syslog Target** tab.
      ii. In the **Available Targets** field, click the target that you created in step 2.
      iii. Click the "greater than" button (>).
      iv. Click **Submit**.
   c. Repeat step 3b for each logging category for which you want to receive logs.

      Note: For version 5.5 and higher, the Maximum length can now be changed and the valid options are from 200 to 8192. The default value is 1024. RSA recommends a value of 2048.

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 **ciscosecureacs**.

Configure RSA NetWitness Platform for Syslog Collection

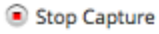
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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 

, 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.