RSA Security Analytics

Event Source Log Configuration Guide

Cyber-Ark

Last Modified: Thursday, July 30, 2015

Event Source Product Information:

Vendor: Cyber-Ark
Event Source:

- Privileged Identity Management Suite (version 7.x)
- Privileged Account Security Solution (versions 8.x and 9.x)

Versions: 7.x, 8.x, 9.x
Additional Downloads: SecurityAnalytics.xsl, RFC5424Changes.xsl

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Event Source Log Parser: cyberark
Collection Method: Syslog
Event Source Class.Subclass: Security.Access Control

Configure Cyber-Ark Suite

To configure Syslog collection for the Cyber-Ark event source, you must:

I. Configure Syslog Output on Cyber-Ark

II. Configure Security Analytics for Syslog Collection

Configure Syslog Output on Cyber-Ark

To configure Cyber-Ark:

1. Download the XSL files from RSA SecurCare Online:
   - **SecurityAnalytics.xsl**
   - **RFC5424Changes.xsl**

   Note: The contents of **RFC5424Changes.xsl** get imported into SecurityAnalytics.xsl.

2. Save the files to the Cyber-Ark installation folder: `/Server/Syslog`.
3. Log on to the Cyber-Ark appliance with administrator credentials.
4. Open the Cyber-Ark installation folder.
5. In the **dbparm.ini** file, ensure that the following parameters are set:
   - SyslogServerIP=*IPaddress*
     where *IPaddress* is the IP address of the RSA Security Analytics Log Decoder or RSA Security Analytics Remote Log Collector.
   - SyslogServerPort=**514**
   - SyslogMessageCodeFilter=*message codes*

     where *message codes* are the messages that will be sent from the Vault to RSA Security Analytics through the Syslog protocol. You can leave the default (all message codes are sent for users and secure activities), or select individual IDs.

     Note: If you decide to specify individual IPs, use commas to separate individual messages or ranges of messages. For example, `SyslogMessageCodeFilter=1,2,5-10`.
   - SyslogTranslatorFile=Syslog\SecurityAnalytics.xsl

     This is the location of the translator file used to generate logs in syslog format and send to RSA Security Analytics.
   - UseLegacySyslogFormat=No

- SyslogServerProtocol=*protocol*

  where *protocol* is either UDP or TCP.

6. To restart the Cyber-Ark service, perform these steps:

   a. From the desktop of the Vault Server, click the PrivateArk Server icon.

      The Server Central Administrator launches

   b. Click **Stop/Start** to restart the Cyber-Ark service.

Configure Security Analytics 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 Security Analytics.

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 Security Analytics 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.
4. Ensure that the parser for your event source is enabled.

   a. From the **System** pull-down menu, select **Config**.

   b. In the Service Parsers Configuration panel, search for your event source.

   c. Ensure that the **Config Value** field for your event source is selected.

To configure the Remote Log Collector for Syslog collection:

1. In the Security Analytics 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 Security Analytics.

Trademarks