

RSA NetWitness Platform

Event Source Log Configuration Guide



Cyber-Ark

Last Modified: Tuesday, September 18, 2018

Event Source Product Information:

Vendor: [Cyber-Ark](#)

Event Source:

- Privileged Identity Management Suite: versions 7.x, 9.x, 10.x
- Privileged Account Security Solution: versions 8.x and 9.x

Versions: 7.x, 8.x, 9.x, 10.x

Additional Downloads: SecurityAnalytics.xsl, RFC5424Changes.xsl

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: cyberark

Collection Method: Syslog

Event Source Class.Subclass: Security.Access Control

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

- I. Configure Syslog Output on Cyber-Ark
- II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Cyber-Ark

To configure Cyber-Ark:

1. Navigate to the Cyber-Ark Suite additional downloads space on RSA Link: <https://community.rsa.com/docs/DOC-45507>.
2. Download the **CyberArk.zip** archive, and extract **SecurityAnalytics.xml** and **RFC5424Changes.xml**.
3. Save the files to the Cyber-Ark installation folder: `/Server/Syslog`.

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

4. Log on to the Cyber-Ark appliance with administrator credentials.
5. Open the Cyber-Ark installation folder.
6. In the **dbparm.ini** file, ensure that the following parameters are set:

| Field | Action |
|-------------------------|--|
| SyslogServerIP | Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector. |
| Server Port | Type 514 . |
| SyslogMessageCodeFilter | This field designates the messages that are sent from the Vault to RSA NetWitness Platform through the Syslog protocol. You can accept the default (all message codes are sent for users and secure activities), or select individual IDs. To specify individual IPs, use commas to separate individual messages or ranges of messages. For example, <code>SyslogMessageCodeFilter=1,2,5-10</code> . |
| SyslogTranslatorFile | Enter <code>Syslog\SecurityAnalytics.xml</code> This is the location of the translator file used to generate logs in syslog format and send to RSA NetWitness Platform. |
| UseLegacySyslogFormat | Enter No . |
| SyslogServerProtocol | Select UDP or TCP . |

7. Restart the Cyber-Ark service:
 - 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 RSA NetWitness Platform for Syslog Collection

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 **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 **cyberark**.

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 , 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.

Copyright © 2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

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