

Check Point GAIa

Last Modified: Monday, August 6, 2018

Event Source Product Information:

Vendor: [Check Point](#)

Event Source: GAIa

Note: This event source is supported by the Red Hat Linux XML, and is discovered by the RSA NetWitness Platform Log Decoder as Linux.

Versions: R77.20

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: rhlinux, checkpointfw

Collection Method: Syslog

Event Source Class.Subclass: Host.Unix

Configure Check Point GAiA

To configure Syslog collection for the Check Point GAiA event source, perform the following tasks:

- I. Configure Syslog Output on Check Point GAiA
- II. Configure RSA NetWitness Platform for Syslog Collection

What is GAiA?

Check Point GAiA is a Secure Operating System for all Check Point Appliances, Open Servers and Virtualized Gateways. It is a 64-bit unified operating system delivering better security and higher efficiency than its predecessors. With Check Point GAiA, customers can benefit from a single, unified OS for all Check Point appliances, open servers and virtualized gateways.

As many enterprises and global service providers continue to make the transition to IPv6, GAiA is designed to support both IPv4 and IPv6 networks, with up to 70 million concurrent connections and a variety of dynamic routing protocols to meet the performance needs of the most demanding network environments

Configure Syslog Output on Check Point GAiA

To configure Syslog output on Check Point GAiA:



1. Log onto the GAiA Portal with administrative credentials.
2. From the left navigation pane, select **System Management > System Logging**.
3. In the **Remote System Logging** section, click **Add**.
The **Remote System Logging Entry** dialog appears.
4. In the **Remote System Logging Entry** dialog:
 - Enter the IP address of your RSA NetWitness Platform Log Decoder or Remote Log Collector.
 - Select any priority level that meets your needs. RSA recommends that you leave the default value, **All**, selected, to collect the most logging information available.
5. Click **OK** to save your changes.

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  **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.