

# RSA NetWitness Logs

Event Source Log Configuration Guide



## IBM Guardium SQL Guard

Last Modified: Wednesday, March 22, 2017

### Event Source Product Information:

**Vendor:** [IBM](#)

**Event Source:** Guardium SQL Guard

**Versions:** 7, 8.0.2, 9.5.x

### RSA Product Information:

**Supported On:** NetWitness Suite 10.0 and later

**Event Source Log Parser:** guardium

**Collection Method:** Syslog

**Event Source Class.Subclass:** Security.Application Firewall

To configure the IBM Guardium event source, you must:

- I. Configure Syslog Output on IBM Guardium
- II. Configure RSA NetWitness Suite for Syslog Collection

## Configure Syslog Output on IBM Guardium

---

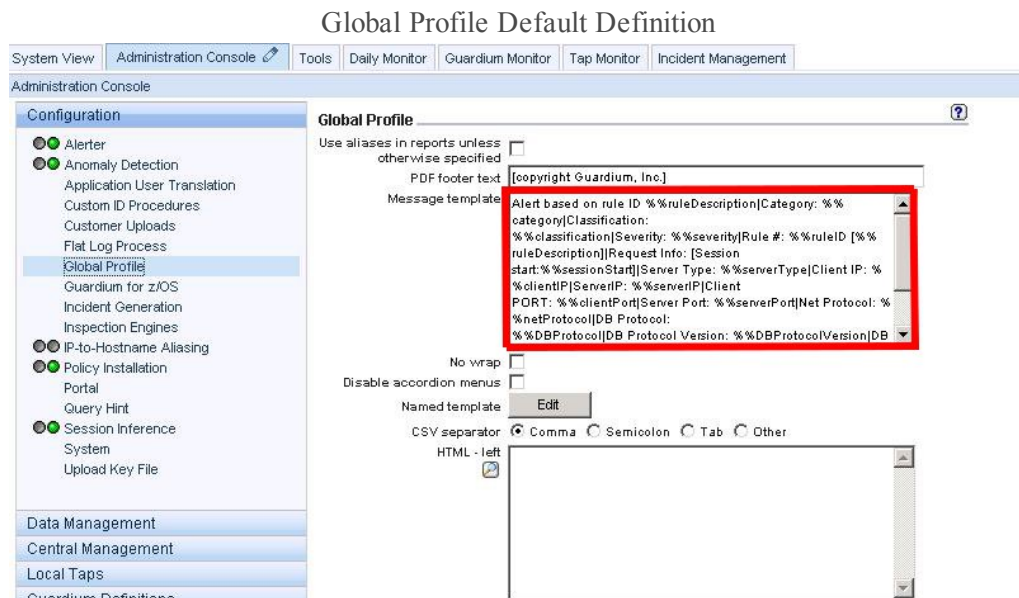
### To configure Guardium SQL Guard:

1. In the **Administration Console** tab, choose **Global Profile** and add one of the following texts in the **Message Template** field:

```
Alert based on rule ID %%ruleDescription|Category:
%%category|Classification: %%classification|Severity:
%%severity|Rule #: %%ruleID [%%ruleDescription]|Request Info:
[Session start:%%sessionStart]|Server Type: %%serverType|Client
IP: %%clientIP|ServerIP: %%serverIP|Client PORT:
%%clientPort|Server Port: %%serverPort|Net Protocol:
%%netProtocol|DB Protocol: %%DBProtocol|DB Protocol Version:
%%DBProtocolVersion|DB User: %%DBUser|Application User Name:
%%AppUserName|Source Program: %%SourceProgram|Request Type:
%%requestType|Last Error: %%lastError|SQL: %%SQLString
```

or

```
GUARDIUM_ALERT: rule-
id=%%ruleID^^category=%%category^^classification=%%classification
^^severity=%%severity^^session-start-time=%%sessionStart^^client-
hostname=%%clientHostname^^client-ip=%%clientIP^^server-
type=%%serverType^^server-ip=%%serverIP^^src-
program=%%SourceProgram^^os-user=%%OSUser^^db-user=%%DBUser^^app-
user=%%AppUserName^^service-name=%%serviceName^^req-
type=%%requestType^^rule-desc=%%ruleDescription^^sql=%%SQLNoValue
```



2. Access the Guardium appliance through a Secure Shell (SSH) connection using "cli" credentials.
3. In the SSH connection, enter the following command, where xxx.xxx.xxx.xxx is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector that you are using to collect Guardium syslog messages:

```
store remotelog add all.all xxx.xxx.xxx.xxx udp
show remotelog
```

**Note:** This command sends the syslog messages to RSA NetWitness Suite.

4. From the Configuration pane, click **Policy Installation**, and select a policy.
5. Click **Edit Installed Policy**. In the Policy Rules window, click **Add Access Rule**.
6. Complete any necessary fields. Then select an action, and click **Add Action**.
7. For Action, select **Alert Per Match**.
8. For Message Template, select RSA NetWitness Suite.
9. For Notification Type, select **syslog**.
10. Click **Add > Apply > Save** to save the policy.

## Configure RSA NetWitness Suite

---

Perform the following steps in RSA NetWitness Suite:

- 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 Suite 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 **guardium**.



### 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  **Stop Capture**, 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 © 2017 EMC Corporation. All Rights Reserved.

## **Trademarks**

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.