RSA NetWitness Logs

Event Source Log Configuration Guide

MySQL Enterprise

Last Modified: Wednesday, November 15, 2017

Event Source Product Information:

Vendor: MySQL
Event Source: MySQL Enterprise
Versions: 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 Suite 10.0 and later
Event Source Log Parser: mysql
Collection Method: SNMP
Event Source Class.Subclass: Storage.Database

Configure MySQL Enterprise to Send Logs to NetWitness Suite

Depending on your version of MySQL, perform one of the following tasks:

- Configure MySQL Enterprise version 5.6 and newer
- Configure MySQL Enterprise version 5.1 to 5.5

Configure MySQL Enterprise version 5.6

1. Log on to the MySQL Enterprise Dashboard with Administrator credentials.
2. Click the **Configuration** > **Event Handlers** tab.
3. In the **SNMP Traps** section, do the following:
   a. Ensure **Enable SNMP Notifications** is selected.
   b. Select **Use SNMP v2**.
   c. In the **Target** field, enter the IP address of your RSA NetWitness Suite Log Collector.
   d. In the **Port** field, type: **162**
   e. In the **Community String** field, type: **public**
   f. Click **Save**.
4. Click the **Advisors** > **Add to Schedule** tab.
5. For each rule that you want to report on, expand the appropriate category and select the rule.
6. Click **Schedule**, and configure as follows:
   a. In the **Frequency** field, select the log frequency that you want.
   b. Ensure **Use SNMP Traps** is selected.
   c. Click **Schedule**.
7. Click the **Advisors** > **Current Schedule** tab, and ensure that your scheduled rules have been successfully added.

Configure MySQL Enterprise version 5.1

1. Log on to the MySQL Enterprise Dashboard with Administrator credentials.
2. Click the **Settings** > **Global Settings** tab.
3. In the **SNMP Traps** section, do the following:
    a. Ensure **Enable SNMP Notifications** is selected.
    b. In the **Target** field, enter the IP address of your RSA NetWitness Suite Log Collector.
    c. In the **Port** field, type: **162**
    d. In the **Community String** field, type: **public**
    e. Click **Submit**.
    f. Click **Save**.
4. Click the **Advisors** > **Add to Schedule** tab.
5. For each rule that you want to report on, expand the appropriate category and select the rule.
6. Click **Schedule**, and configure as follows.
    a. In the **Frequency** field, select the log frequency that you want.
    b. Ensure **Use SNMP Traps** is selected.
    c. Click **Schedule**.
7. Click the **Advisors > Current Schedule** tab, and ensure that your scheduled rules have been successfully added.

Configure SNMP Event Sources on NetWitness Suite

To set up SNMP on RSA NetWitness Suite, perform the following tasks:

I. Add the SNMP Event Source Type

II. Configure SNMP Users

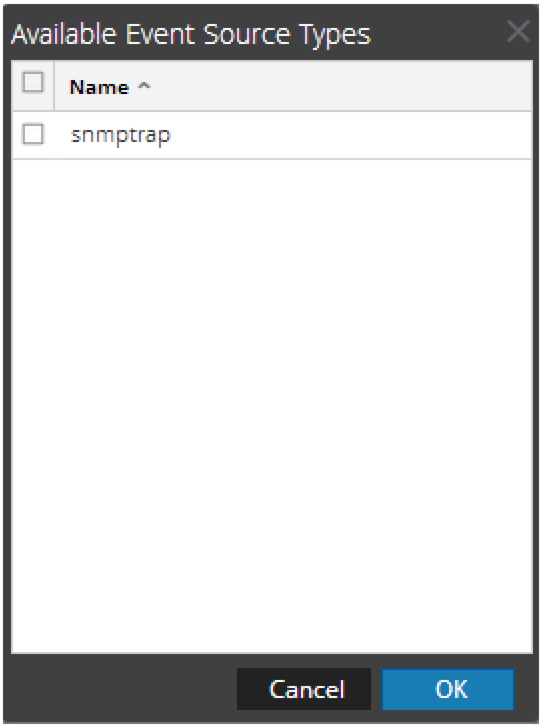
Add the SNMP Event Source Type

> **Note:** If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

Add the SNMP Event Source Type:

1. In the **RSA NetWitness Suite** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

   The Sources panel is displayed with the existing sources, if any.
5. Click + to open the **Available Event Source Types** dialog.



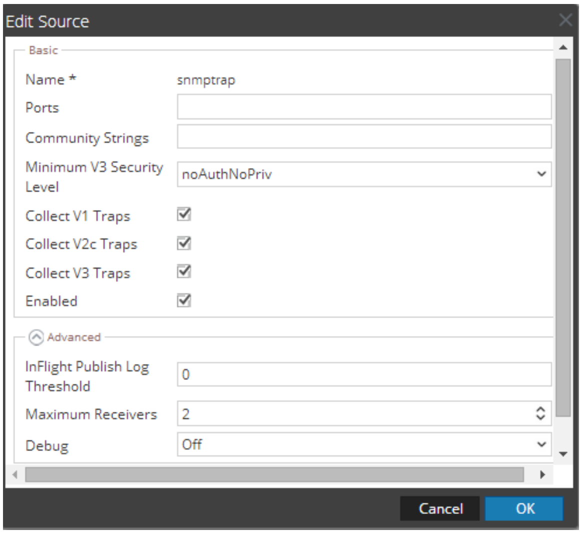
Available Event Source Types

□	Name ^
□	snmptrap

6. Select **snmptrap** from the Available Event Source Types dialog and click **OK**.

7. Select **snmptrap** in the Event Categories panel.

8. Select **snmptrap** in the Sources panel and then click the Edit icon to edit the parameters.



Edit Source

Basic

Name *	snmptrap
Ports	
Community Strings	
Minimum V3 Security Level	noAuthNoPriv
Collect V1 Traps	☑
Collect V2c Traps	☑
Collect V3 Traps	☑
Enabled	☑

Advanced

InFlight Publish Log Threshold	0
Maximum Receivers	2
Debug	Off

9. Update any of the parameters that you need to change.

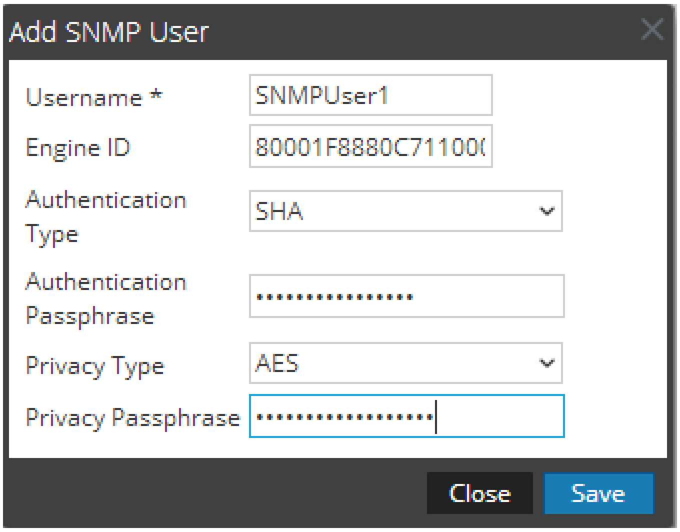
(Optional) Configure SNMP Users

If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

Configure SNMP v3 Users

1. In the **RSA NetWitness Suite** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/SNMP v3 User Manager** from the drop-down menu.

   The SNMP v3 User panel is displayed with the existing users, if any.
5. Click + to open the **Add SNMP User** dialog.



Add SNMP User

Username * SNMPUser1

Engine ID 80001F8880C71100(

Authentication Type SHA

Authentication Passphrase ••••••••••••••••

Privacy Type AES

Privacy Passphrase ••••••••••••••••••

6. Fill in the dialog with the necessary parameters. The available parameters are described below.

SNMP User Parameters

The following table describes the parameters that you need to enter when you create an SNMP v3 user.

Parameter	Description
Username *	User name (or more accurately in SNMP terminology, security name). RSA NetWitness Suite uses this parameter and the **Engine ID** parameter to create a user entry in the SNMP engine of the collection service. The **Username** and **Engine ID** combination must be unique (for example, **logcollector**).
Engine ID	(Optional) Engine ID of the event source. For all event sources sending SNMP v3 traps to this collection service, you must add the username and engine id of the sending event source. For all event sources sending SNMPv3 informs, you must add just the username with a blank engine id.
Authentication Type	(Optional) Authentication protocol. Valid values are as follows: • **None** (default) - only security level of **noAuthNoPriv** can be used for traps sent to this service • **SHA** - Secure Hash Algorithm • **MD5** - Message Digest Algorithm
Authentication Passphrase	Optional if you do not have the **Authentication Type** set. Authentication passphrase.
Privacy Type	(Optional) Privacy protocol. You can only set this parameter if Authentication Type parameter is set. Valid values are as follows: • **None** (default) • **AES** - Advanced Encryption Standard • **DES** - Data Encryption Standard
Privacy Passphrase	Optional if you do not have the **Privacy Type** set. Privacy passphrase.
Close	Closes the dialog without adding the SNMP v3 user or saving modifications to the parameters.
Save	Adds the SNMP v3 user parameters or saves modifications to the parameters.

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.