RSA NetWitness Logs

Event Source Log Configuration Guide

VSS Monitoring

Last Modified: Wednesday, May 03, 2017

Event Source Product Information:

Vendor: VSS Monitoring
Event Source: VSS Monitoring
Versions: 2.3

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: vssmonitoring
Collection Method: SNMP
Event Source Class.Subclass: Network.System

To configure the VSS Monitoring event source, perform the following tasks:

I. Configure VSS Monitoring to send SNMP traps

II. Configure RSA NetWitness Suite for SNMP

   i. Add the SNMP Event Source Type

   ii. (Optional) Configure SNMP Users

Configure VSS Monitoring to send SNMP traps

To configure VSS Monitoring to send SNMP traps:

1. Log on to the VSS Monitoring web console with administrator credentials.
2. From the **Settings** menu, select **SNMP Settings**.
3. In the **SNMP Settings** section, complete the fields as follows.

Field	Value
SNMP Version	V2
SNMP Trap Manager (s)	The IP address of the RSA NetWitness Suite Log Collector
Event notifications	Notify

4. Click **Submit**.

Configure RSA NetWitness Suite for SNMP

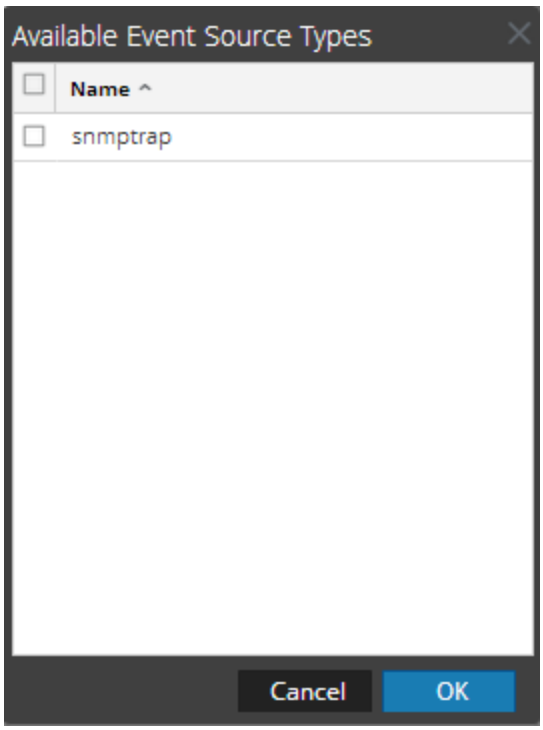
Add the SNMP Event Source Type

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:

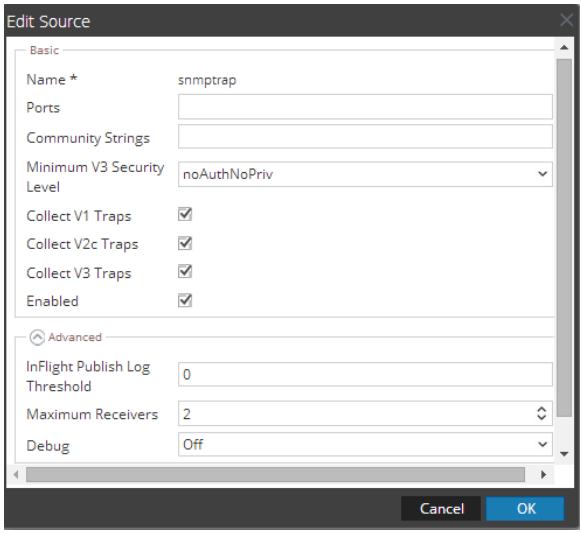
1. In the **RSA NetWitness Suite** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

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



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.



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

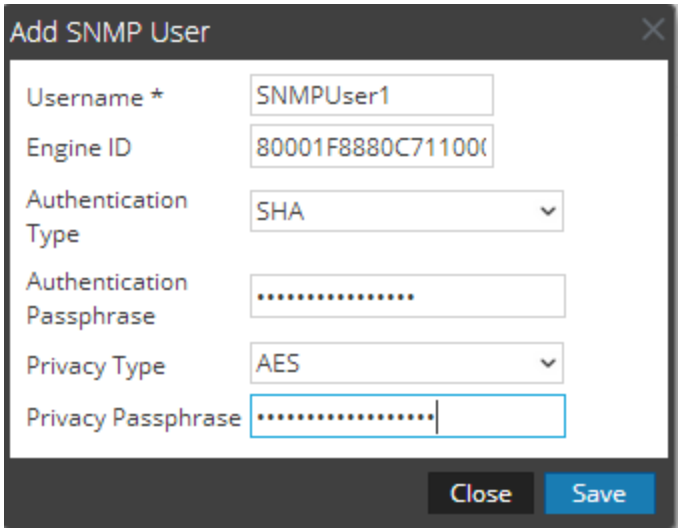
(Optional) Configure SNMP Users

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.



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

Parameter	Description
	• **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