RSA NetWitness Logs

Event Source Log Configuration Guide

BeyondTrust Retina Network Security Scanner

Last Modified: Monday, June 26, 2017

Event Source Product Information:

Vendor: BeyondTrust
Event Source: Retina Network Security Scanner (formerly branded as eEye Retina Network Security Scanner)
Versions: 5.10

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: eeyeretina
Collection Method: Syslog, SNMP
Event Source Class.Subclass: Security.IDS

To configure the BeyondTrust Retina Network Security Scanner event source, perform either of the following tasks:

- Configure Syslog Collection
  I. Configure Syslog Output on BeyondTrust Retina Network Security Scanner
  II. Configure RSA NetWitness Suite for Syslog Collection
- Configure SNMP Collection
  I. Configure SNMP Output on BeyondTrust Retina Network Security Scanner
  II. Configure RSA NetWitness Suite for SNMP Collection

Configure Syslog Output on BeyondTrust Retina Network Security Scanner

The following procedure describes how to configure Syslog output on your device.

To configure collection through syslog for BeyondTrust Retina Network Security Scanner:

1. Open the BeyondTrust Retina Network Security Scanner web interface.
2. Click **Tools > Alerting**.
3. On the **Events** tab, select the events on which you want to trigger alerts.
4. On the **Actions** tab, under **Syslog**, follow these steps:
   a. In the **Enabled** field, select **True**.
   b. In the **Host** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
   c. From the **Priority** drop-down list, select **LOG_INFO**.
   d. From the **Facility** drop-down list, select **LOG_LOCAL0**.
5. Click **OK**.

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 **eeyeretina**.

Configure Syslog Collection

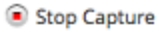
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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 

, 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.

Configure SNMP Output on BeyondTrust Retina Network Security Scanner

The following procedure describes how to configure SNMP output on your device.

To configure collection through SNMP for BeyondTrust Retina Network Security Scanner:

1. Open the BeyondTrust Retina Network Security Scanner web interface.
2. Click **Tools > Alerting**.
3. On the **Events** tab, select the events on which you want to trigger alerts.
4. On the **Events** tab, under **SNMP**, follow these steps:
   a. In the **Enabled** field, select **True**.
   b. In the **Host** field, enter the IP address for the RSA NetWitness Suite Log Collector.
5. Click **OK**.

Configure SNMP Event Sources on NetWitness Suite

The first time that you configure an SNMP event source on RSA NetWitness Suite, you need to add the SNMP event source type and configure SNMP users.

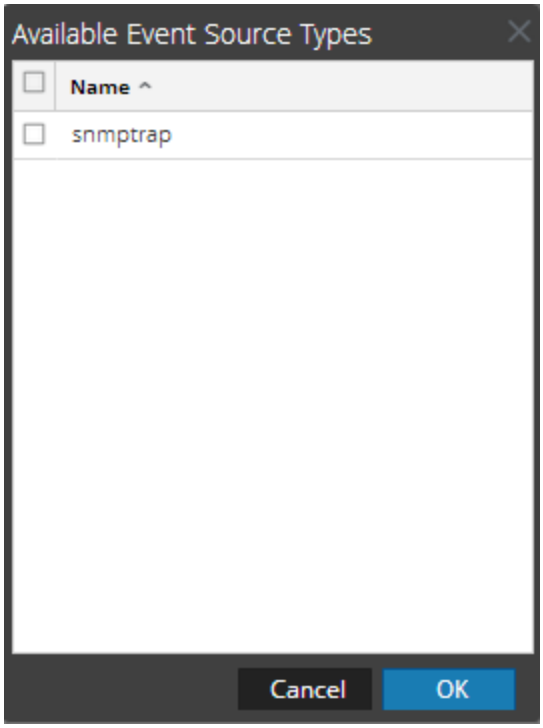
Add the SNMP Event Source Type

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

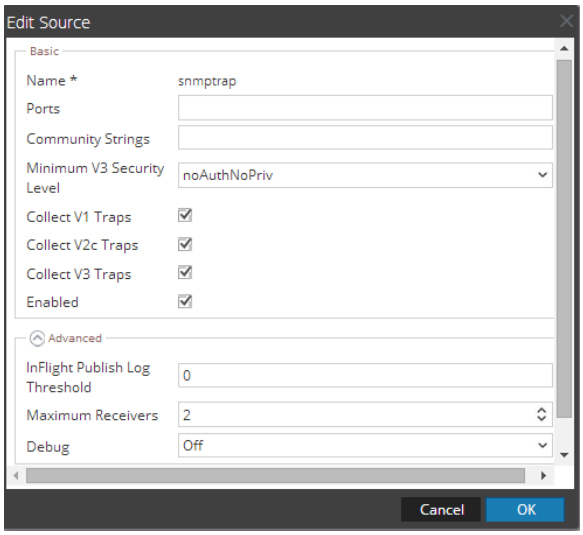
Add the SNMP Event Source Type:

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.



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.

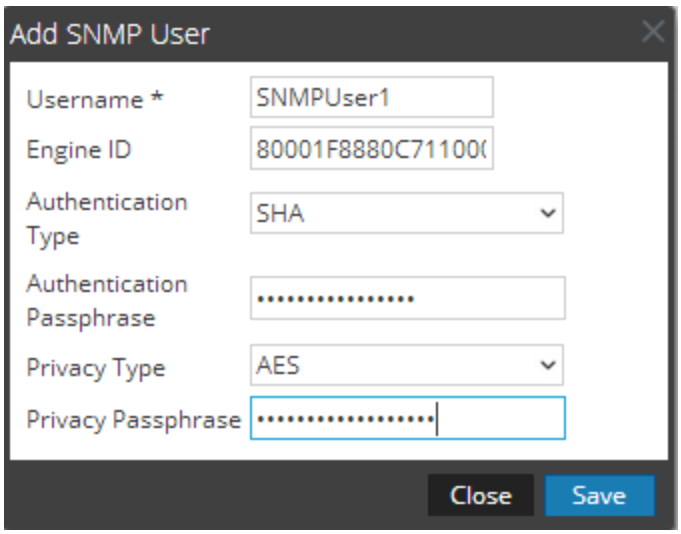
(Optional) Configure SNMP Users

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 • **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