RSA NetWitness Logs

Event Source Log Configuration Guide

Novell eDirectory

Last Modified: Tuesday, May 09, 2017

Event Source Product Information:

Vendor: Novell
Event Source: eDirectory
Version: 8.8
Supported Platforms: Microsoft Windows and Linux

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: edirectory
Collection Method: SNMP
Event Source Class.Subclass: Security.Access Control

To configure Novell eDirectory, you must complete these tasks:

- Configure Novell eDirectory to send SNMP
- Configure SNMP Event Sources on the NetWitness Suite

Configure Novell eDirectory to send SNMP

Depending on your platform, select one of the following tasks:

- Configure Novell eDirectory on a Microsoft Windows Server
- Configure Novell eDirectory on a Linux Server

Configure Novell eDirectory on a Microsoft Windows Server

To configure Novell eDirectory on a Microsoft Windows server, you must complete these tasks:

I. Configure the Novell eDirectory event source

II. Configure Novell eDirectory on a Microsoft Windows Server

Configure the Novell eDirectory Event Source

To configure the Novell eDirectory event source:

1. Open the Novell iManager web interface, and authenticate with administrator credentials.
2. Select **Roles and Tasks**.
3. Expand **SNMP** in the left-hand pane and select **SNMP Overview**.
4. Select the SNMP Group that you want to monitor.
5. On the **General** tab, select **Traps**.
6. For every trap that you want to monitor, select the box for that trap in the **Active** column.
7. Click **Apply**.

Configure Novell eDirectory on a Microsoft Windows Server

To configure the Novell eDirectory on a Microsoft Windows Server:

1. To open the Services MMC, on the server running Novell eDirectory, click **Start** > **Program** > **Administrative Tools** > **Services**.

2. Double-click the SNMP service and select the **Traps** tab.
3. In the **Community name** section, type **public**.
4. Click **add to list**.
5. In the **Traps destinations** section, select **Add**, and enter the IP address of the RSA NetWitness Suite Log Collector.
6. Click **Add**.
7. Click **OK**.

Configure Novell eDirectory on a Linux Server

To configure Novell eDirectory on a Linux Server, you must complete these tasks:

I. Configure the Novell eDirectory event source

II. Configure the Master Agent

III. Start the Master Agent

IV. Start the Subagent

Note: On your Linux system, **net-snmp** should be installed by default. If this service is not on your Linux system, you must install this to configure Novell eDirectory.

Configure the Novell eDirectory Event Source

To configure the Novell eDirectory event source:

1. Open the Novell iManager web interface, and authenticate with administrator credentials.
2. Select **Roles and Tasks**.
3. Expand **SNMP** in the left-hand pane and select **SNMP Overview**.
4. Select the SNMP Group that you want to monitor.
5. On the **General** tab, select **Traps**.
6. For every trap that you want to monitor, select the box for that trap in the **Active** column.
7. Click **Apply**.

Configure the Master Agent

To configure the Master Agent:

1. Open the **snmpd.conf** file, which is located in the `/etc/snmp` directory on OES Linux or SLES and in the `/etc` directory on other Linux platforms.
2. In the **snmpd.conf** file, enter the hostname:

   ```
   trapsink myserver public port
   ```

   where:

   - ***myserver*** is the IP address of the RSA NetWitness Suite Log Collector
   - ***port*** is the port number: default value is 162
3. In the **snmpd.conf** file, add the following line:

   ```
   master agentx
   ```

4. Locate and change the following lines. If these lines are not in the **snmpd.conf** file, add the lines.

Original Content	Changed Content
com2sec notConfigUser default public	com2sec demouser default public
group notConfigGroup v1 notConfigUser	group demogroup v1 demouser
view systemview included system	view all included .1
access notConfigGroup "" any noauth exact systemview none none	access demogroup "" any noauth exact all all all

Warning: When you change any configuration file, you must restart the Master Agent and the Subagent.

Start the Master Agent

To start the Master Agent, run the following command:

```
/usr/sbin/snmpd -C -c /etc/snmpd.conf
```

Start the Subagent

To start the Subagent:

1. To start the Subagent, run the following command:

   ```
   /etc/init.d/ndssnmpsa start
   ```

2. When prompted, enter your user name and password. When you are logged on, if **INTERACTION = ON** is set in the `/etc/opt/novell/eDirectory/conf/ndssnmp/ndssnmp.cfg` file, you are prompted to remember your password.

   > **Note:** If your server goes down, the Master Agent and the Subagent also go down. To start the Master Agent and the Subagent while restarting the server, run the following commands:
   >
   > ```
   > chkconfig snmpd on
   > chkconfig ndssnmpsa on
   > chkconfig ndssnmpsa <run levels>
   > ```

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.

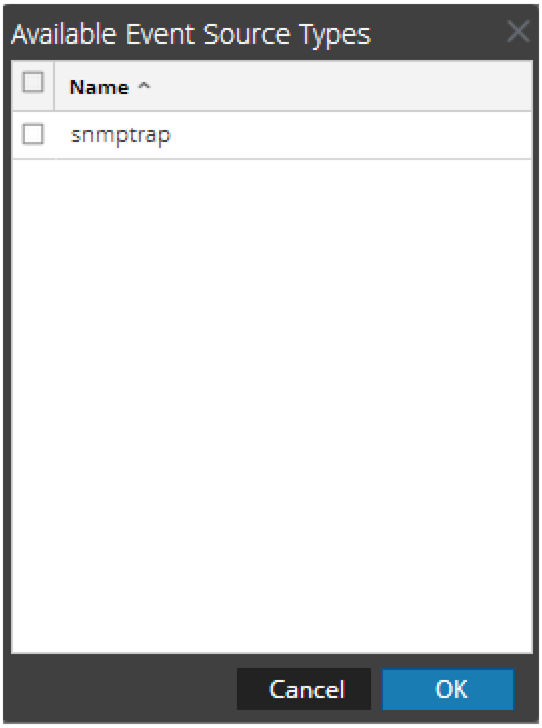
Add the SNMP Event Source Type

> **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.

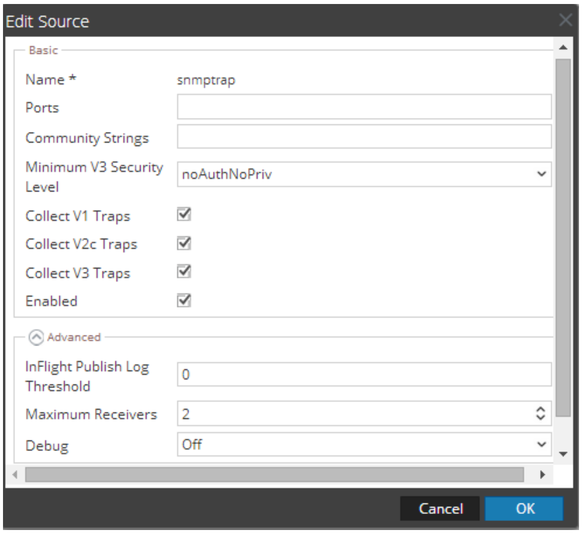
   The Sources panel is displayed with the existing sources, if any.
5. Click + to open the **Available Event Source Types** dialog.



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.


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.

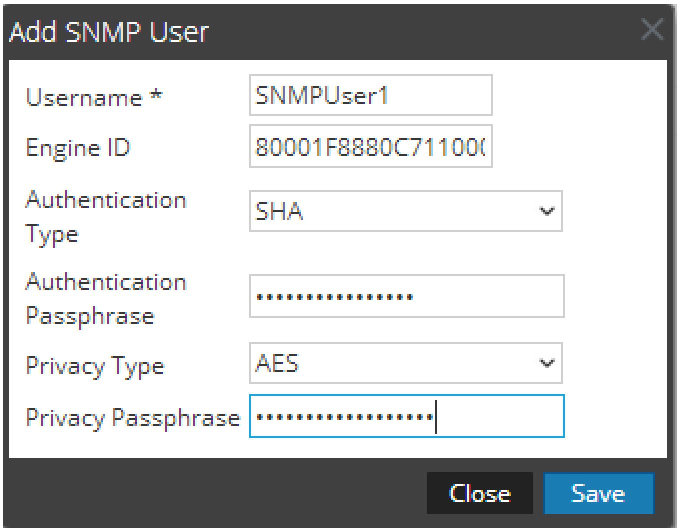
(Optional) Configure SNMP Users

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.



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.