RSA NetWitness Logs

Event Source Log Configuration Guide

Cisco Security Agent

Last Modified: Thursday, July 27, 2017

Event Source Product Information:

Vendor: Cisco
Event Source: Security Agent
Versions: 4.0, 5.1, 6.0

RSA Product Information:

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

Depending on what you want to collect, perform the following tasks:

- To configure SNMP collection, see Configure SNMP Collection.
- To configure ODBC collection , see Configure ODBC Collection .

Configure SNMP Collection

Perform the following steps to configure SNMP collection:

I. Configure Cisco Security Agent for SNMP Traps Collection. Depending on your version:
   - Configure version 5.1 or 6.0, or
   - Configure version 4.0

II. Configure RSA NetWitness Suite for SNMP
   i. Add the SNMP Event Source Type
   ii. (Optional) Configure SNMP Users

Configure Cisco Security Agent 5.1 or 6.0 for Traps Collection

Note: Cisco Security Agent 6.0 supports Antivirus and Data Loss Prevention features.

To configure Cisco Security Agent version 5.1 or 6.0:

1. Connect to the Management Center for Cisco Security Agents, and log on with administrative credentials.
2. Select **Events > Alerts**.
3. Click **New**, and follow these steps to create a new alert:
   a. In the **Name** field, enter the name of the alert.
   b. In the **Description** field, enter a description of the alert.
   c. From the **Send Alerts** drop-down list, do one of the following:
      - For Cisco Security Agent 5.1, select **All events [V5.1 r69]**.
      - For Cisco Security Agent 6.0, select **All events [V6.0.1 r106]**.
   d. Under **Alert Method**, select **SNMP**.
   e. In the **Community name** field, type **public**.

f. In the **Manager IP address** field, enter the IP address of the RSA NetWitness Log Collector.

4. Click **Save**.

Configure Cisco Security Agent 4.0 for Traps Collection

Note: Make sure that the CSA Database is not full. If the database is full, no alerts will be forwarded.

To configure Cisco Security Agent 4.0:

1. Access the VPN Security Management Solution from the CiscoWorks event source.
2. Select **Administration > Management Center > Security Agents**.
3. From the tab at the top, select **Monitor**, and, from the drop-down list, select **Alerts**.
4. Click **New**, and follow these steps:
   a. In the **Name** field, enter the alert name.
   b. In the **Description** field, enter a description of the alert.
   c. From the Send Alerts list, select **All Events**.
   d. Select **SNMP**.
   e. In the **Community Name** field, type **public**.
   f. In the **Manager IP Address** field, enter the IP address of the RSA NetWitness Log Collector.
5. Click **Save**.

Add the SNMP Event Source Type

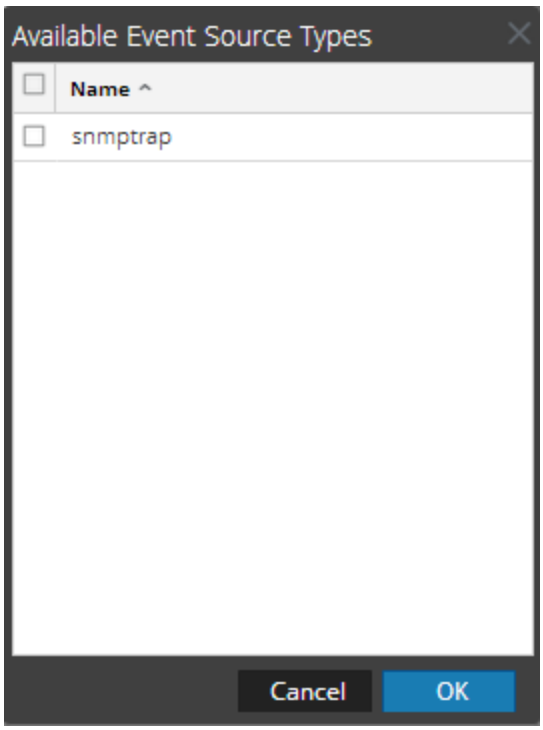
Note: If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

Add the SNMP Event Source Type:

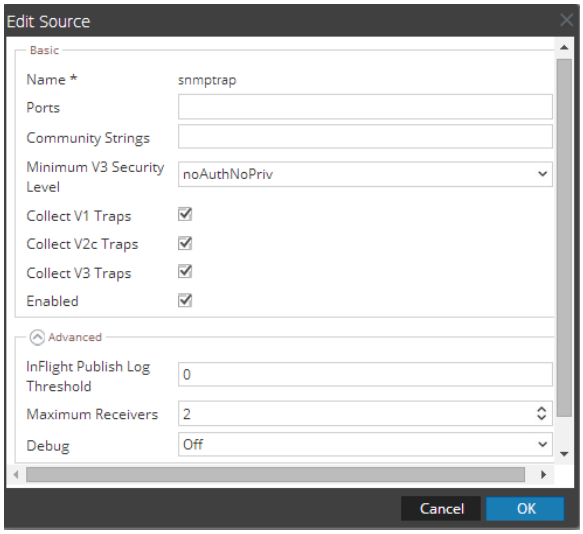
1. In the **RSA NetWitness Suite** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.

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.

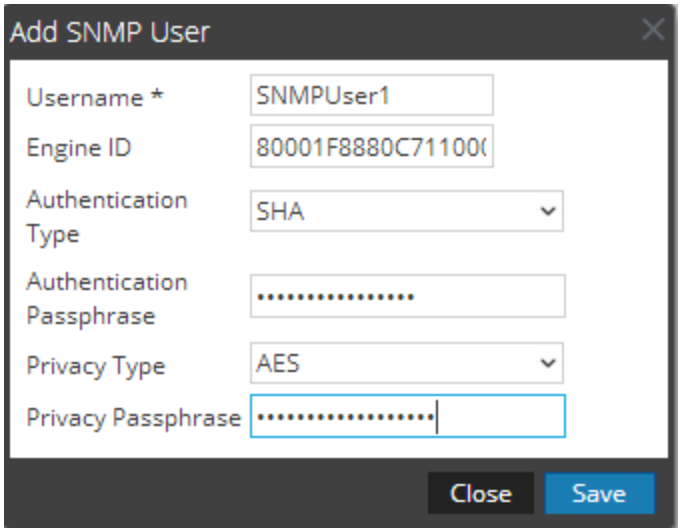
(Optional) Configure SNMP Users

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.

Configure ODBC Collection

If you want to only use ODBC collection, complete the following tasks:

I. Ensure the required parser is enabled

II. Configure a DSN

III. Add the Event Source Type

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 from 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 **mckessonhpf**.

Configure a DSN

Configure a DSN (Data Source Name):

1. In the **NetWitness** 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 **ODBC/DSNs** from the drop-down menu.
5. The DSNs panel is displayed with the existing DSNs, if any.
6. Click + to open the **Add DSN** dialog.

Note: If you need to add a DSN template, see Configure DSNs in the NetWitness User Guide.

7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

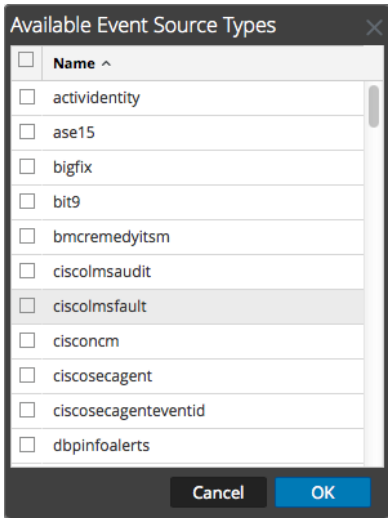
Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
Database	Specify the database used by Cisco Security Agent
PortNumber	Specify the Port Number. The default port number is **1433**
HostName	Specify the hostname or IP Address of Cisco Security Agent
Driver	Depending on your NetWitness Log Collector version: • For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3sqls27.so • For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqls26.so

Add the Event Source Type

Add the ODBC Event Source Type:

1. In the **NetWitness** 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 **ODBC/Config** from the drop-down menu.

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



6. Choose the log collector configuration type for your event source type and click **OK**.

   Depending on how you are collecting logs, select either of the following from the **Available Event Source Types** dialog:

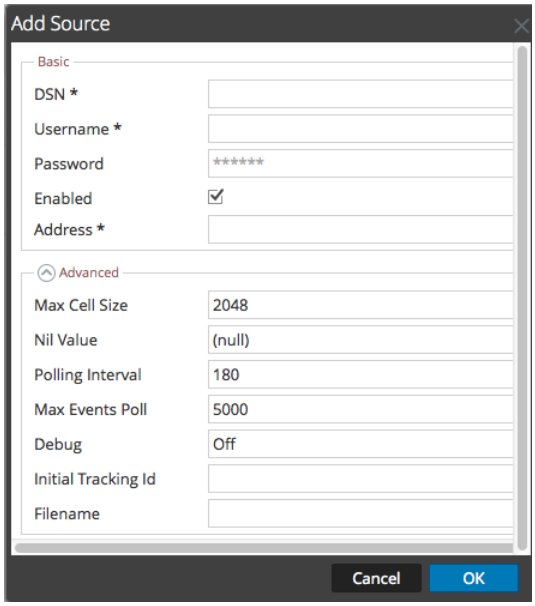
   - To collect logs based on the event time, select **CiscoSecAgent**.

     Note: If there are multiple Cisco Security Agent event sources reporting to the same Log Collector in different time zones, some logs may be lost. In this case, you must collect logs based on event ID.

   - To collect logs based on the event ID, select **CiscoSecAgentEventId**.

     Note: In cases where the logs database is purged on the Cisco Security Agent, the counter value is reset to 0 and the Cisco Security Agent will stop collecting logs.

7. In the **Event Categories** panel, select the event source type that you just added.
8. In the **Sources** panel, click + to open the **Add Source** dialog.



9. Enter the DSN you configured during the **Configure a DSN** procedure.
10. For the other parameters, see ODBC Event Source Configuration Parameters in the NetWitness Suite Log Collection Guide.

Trademarks