RSA NetWitness Platform

Event Source Log Configuration Guide

Symantec Critical Systems Protection

Last Modified: Wednesday, April 17, 2019

Event Source Product Information:

Vendor: Symantec
Event Source: Critical Systems Protection, Data Center Security Server
Versions: 5.2.4, 5.2.8, 5.2.9

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: symanteccsp
Collection Method: SNMP, ODBC
Event Source Class.Subclass: Security.IPS

RSA NetWitness Platform can collect log information from Symantec CSP using either ODBC or SNMP collection. See the appropriate section below to configure your preferred collection method.

- Configure ODBC Collection for Symantec CSP
- Configure SNMP Collection for Symantec CSP

Configure ODBC Collection for Symantec CSP

To configure ODBC collection, perform the following procedures:

I. Ensure the required parser is enabled

II. Configure a DSN

III. Add the Event Source Type

IV. Restart the ODBC Collection Service

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 Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN** > **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 **symanteccsp**.

Configure a DSN

Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select **ADMIN** > **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 the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in RSA Link.

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 Symantec CSP
PortNumber	Specify the Port Number. The default port number is **1433**
HostName	Specify the hostname or IP Address of Symantec CSP
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

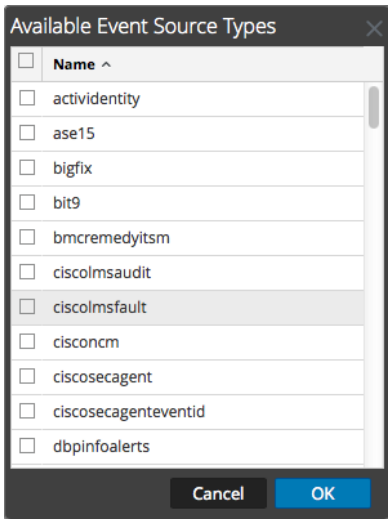
Add the ODBC Event Source Type:

1. In the **NetWitness** menu, select **ADMIN** > **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.

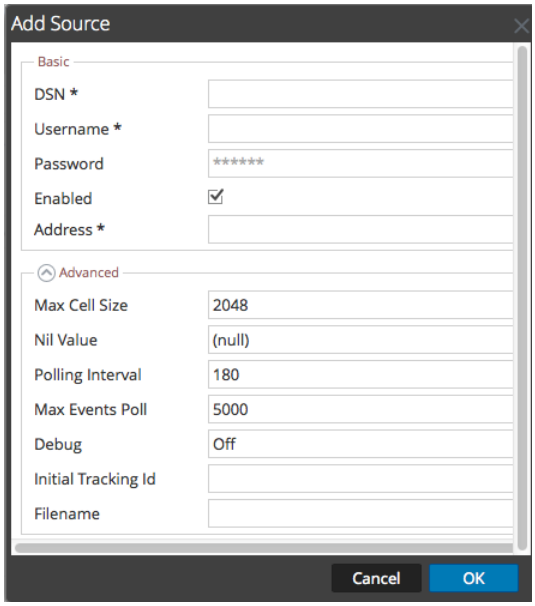


6. Choose the log collector configuration type for your event source type and click **OK**.

   Select **symanteccspeventid** from the Available Event Source Types dialog

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 the "ODBC Event Source Configuration Parameters" topic in the *RSA NetWitness Platform Log Collection Guide*.

Restart the ODBC Collection Service

Restart the ODBC collection service:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View** > **System**.
4. Click **Collection** > **ODBC**.
   - If the available choice is **Start**, click **Start** to start ODBC collection.
   - If the available choices are **Stop** and **Pause**, click **Stop**, wait a few moments, and then click **Start**.

Configure SNMP Collection for Symantec CSP

Perform the following tasks to configure Symantec CSP to work with RSA NetWitness Platform:

- Configure Symantec CSP to send SNMP traps.
- Configure Symantec CSP as an SNMP event source on RSA NetWitness Platform:
  i. Add the SNMP Event Source Type
  ii. Configure SNMP Users

Configure Symantec CSP to Send SNMP Traps

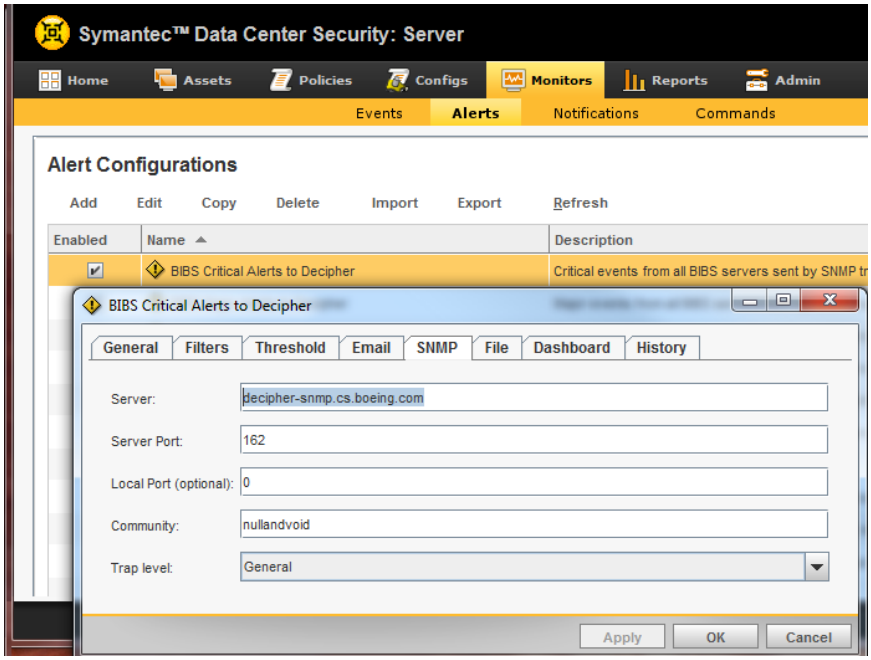
You must configure Symantec Critical Systems Protection to send SNMP traps to the RSA NetWitness Platform.

Note: The administrator performing this task must be familiar with the Symantec Critical Systems Protection Console.

To configure Symantec Critical Systems Protection for SNMP:

1. Log on to the Symantec Data Center Security console.
2. Click **Monitors** > **Alerts**.
3. Select an alert for which you want to activate an SNMP alert.
4. In the window that opens for that alert, select the **SNMP** tab.
5. Fill in the fields with the following information:
   - Server: enter IP address of the IP address of the RSA NetWitness Log Decoder or Remote Log Collector
   - Server Port: enter **162**
   - Community: enter **nullandvoid**
   - Trap level: select **General**

   Here is an example of the alert window configured for SNMP collection:



6. Click **Apply**.

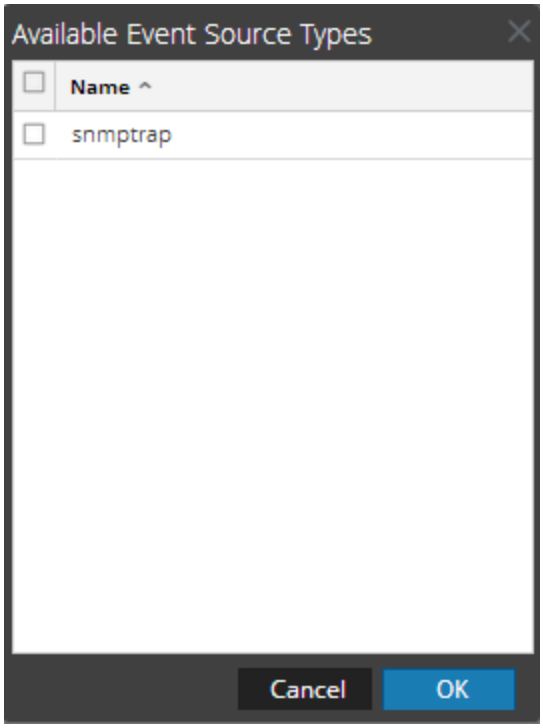
Add the SNMP Event Source Type

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

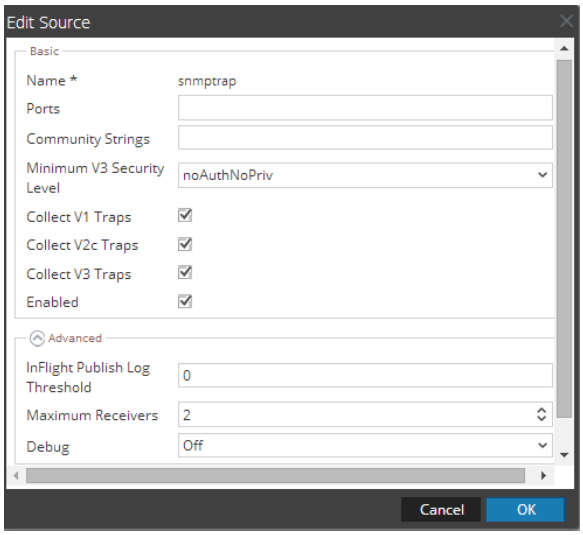
Add the SNMP Event Source Type:

1. In the **RSA NetWitness Platform** 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.

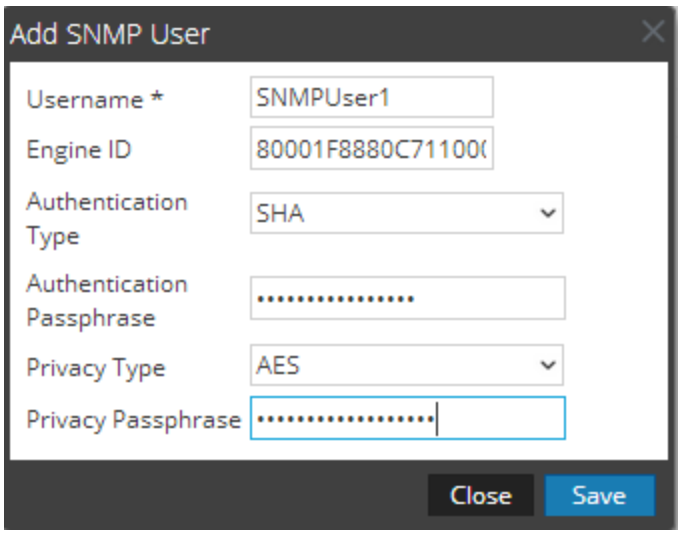
(Optional) Configure SNMP Users

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 Platform** 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 Platform 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

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.