

RSA NetWitness Platform

Event Source Log Configuration Guide



Dell iDrac

Last Modified: Tuesday, April 30, 2019

Event Source Product Information:

Vendor: [Dell](#)

Event Source: Integrated Dell Remote Access Controller (iDRAC)

Versions: DRAC 5, iDRAC 6, iDRAC 9.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: dellidrac

Collection Method: SNMP, Syslog (iDRAC 6, 9.x)

Event Source Class.Subclass: Security. Access Control

For this event source, configuration depends upon your version:

- If you have Dell iDRAC 6, see the following sections:
 - I. [Configure the Dell iDRAC 6 for SNMP Collection](#)
 - II. [Configure RSA NetWitness Platform for SNMP](#)
 - i. Add the SNMP Event Source Type
 - ii. (Optional) Configure SNMP Users
 - III. Depending on your iDRAC version, perform one of the following procedures:
 - [Configure iDRAC 9.x for Syslog Collection](#), or
 - [Configure iDRAC 6 for Syslog Collection](#)
 - IV. [Configure RSA NetWitness Platform for Syslog](#)

Note: For the Dell iDRAC 6 event sources, you must configure both SNMP and Syslog collection, in order for RSA NetWitness Platform to collect all available messages.

- If you have Dell DRAC 5, see the following sections:
 - I. [Configure the Dell DRAC 5 for SNMP Collection](#)
 - II. [Configure RSA NetWitness Platform for SNMP](#)
 - i. Add the SNMP Event Source Type
 - ii. (Optional) Configure SNMP Users

Configure the Dell iDRAC 6 for SNMP Collection

The following procedure describes how to configure Dell iDRAC 6 to send messages, in SNMP format, to RSA NetWitness Platform.

To configure iDRAC 6 for SNMP collection:

1. Open a browser and log on to iDRAC 6 with the username **root** and the password **calvin**.
2. Select **iDRAC Settings**.
3. Click the **Network/Security** tab.
4. In the **Network Settings** section, set the settings as follows:

- a. From the **NIC Selection** drop-down list, select **Dedicated**.
 - b. Select **Enable NIC**.
5. In the **IPv4 Settings** section, set the settings as follows:
 - a. In the **IP Address**, **Subnet Mask**, and **Gateway** fields, enter the appropriate values.
 - b. Select **Enable IPv4**.
6. In the **IPMI Settings** section, set the settings as follows:
 - a. Select **Enable IPMI Over LAN**.
 - b. From the **Channel Privilege Level Limit** drop-down list, select **Administrator**.
7. Click **Apply**.

Configure the Dell DRAC 5 for SNMP Collection

The following procedure describes how to configure Dell DRAC 5 to send messages, in SNMP format, to RSA NetWitness Platform.

To configure iDRAC 5 for SNMP collection:


1. Open a browser and log on to the DRAC with the username **root** and the password **calvin**.
2. Select **Remote Access**.
3. Click the **Configuration** tab.
4. In the **Network Interface Card Settings** section, set the settings as follows:
 - a. From the **NIC Selection** drop-down list, select **Dedicated**.
 - b. Select **Enable NIC**.
5. In the **IPv4 Settings** section, set the parameters as follows:
 - a. In the **IP Address**, **Subnet Mask**, and **Gateway** fields, enter the appropriate values.
 - b. Select **Enabled**.
6. In the **IPMI Settings** section, set the parameters as follows:
 - a. Select **Enable IPMI Over LAN**.
 - b. From the **Channel Privilege Level Limit** drop-down list, select **Administrator**.
7. Click **Apply Changes**.

Configure RSA NetWitness Platform for SNMP

Add the SNMP Event Source Type

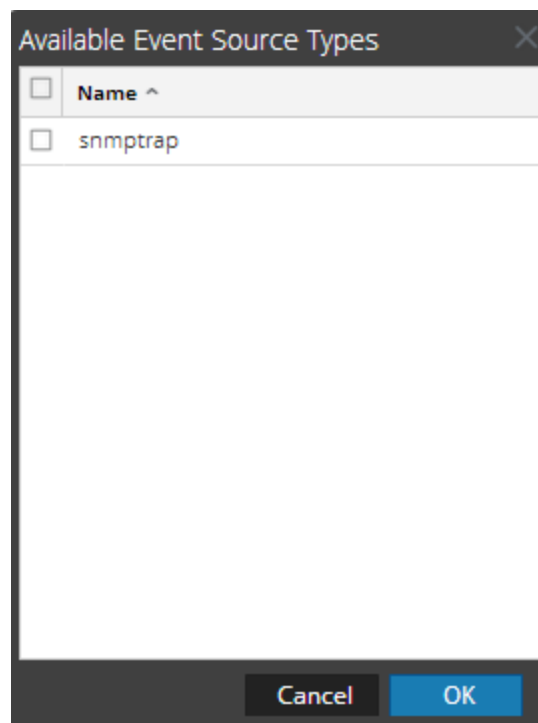
Note: If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

Add the SNMP Event Source Type:

1. In the **RSA NetWitness 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.

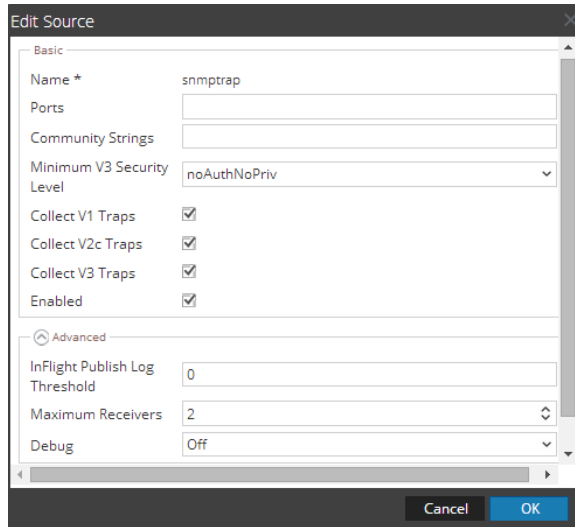
The Sources panel is displayed with the existing sources, if any.

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.




The screenshot shows the 'Edit Source' dialog box for the 'snmptrap' event source. The dialog is divided into two sections: 'Basic' and 'Advanced'. In the 'Basic' section, the 'Name' is 'snmptrap', 'Ports' is empty, 'Community Strings' is empty, 'Minimum V3 Security Level' is set to 'noAuthNoPriv', and 'Collect V1 Traps', 'Collect V2c Traps', 'Collect V3 Traps', and 'Enabled' are all checked. In the 'Advanced' section, 'InFlight Publish Log Threshold' is set to '0', 'Maximum Receivers' is set to '2', and 'Debug' is set to 'Off'. The dialog has 'Cancel' and 'OK' buttons at the bottom right.

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

(Optional) Configure SNMP Users

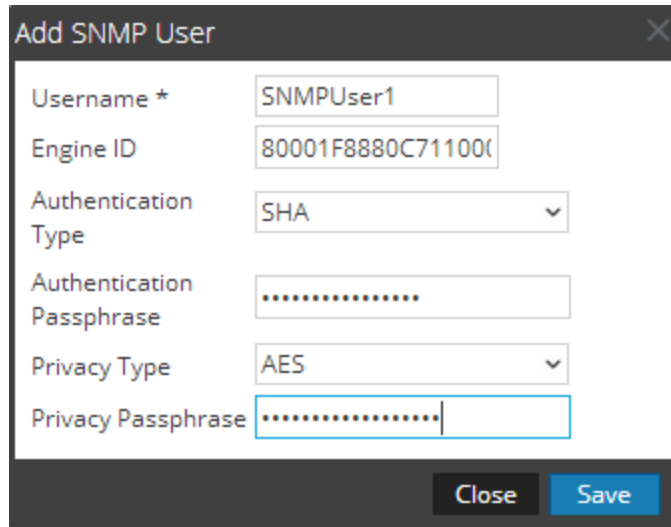
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

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.



- 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: <ul style="list-style-type: none"> None (default) - only security level of noAuthNoPriv can be used for traps sent to this service SHA - Secure Hash Algorithm

Parameter	Description
	<ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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 iDRAC 9.x for Syslog Collection

To configure iDRAC 9.x for Syslog collection:

1. Select **Configuration**.
2. Click the **System Settings** tab.
3. Click **Remote Syslog Settings** and make the following changes:
 - a. Select **Remote Syslog Enabled**.
 - b. In the **Syslog Server** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
 - c. Provide the Port Number.
 - d. Click **Apply**.
4. To enable Remote system Log for all the events go to **configuration > System Settings > Alerts**.

The Alert option expands.
5. Click **Alert Configuration**. Choose either of the following options:
 - Select the **Remote System Log** check box to configure all event alerts to Remote syslog, or
 - Select the individual events that you want to configure for Remote syslog, then select the remote syslog option.

Configure iDRAC 6 for Syslog Collection

To configure iDRAC 6 for syslog collection:

1. Select **System**.
2. Click on the **Setup** tab.
3. Click **Remote Syslog Settings** and make the following changes:
 - a. Select **Remote Syslog Enabled**.
 - b. In the **Syslog Server** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
 - c. Click **Apply**.

Configure RSA NetWitness Platform for Syslog

If you have Dell iDRAC 6 or 9.x, perform the following steps in RSA NetWitness Platform to configure Syslog collection:

- 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 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 **delldrac**.



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**.

- Depending on the icon you see, do one of the following:
 - If you see  **Start Capture**, click the icon to start capturing Syslog.
 - If you see  **Stop Capture**, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

- In the **NetWitness** menu, select **Administration > Services**.
- In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
- Select **Syslog/Config** from the drop-down menu.

The Event Categories panel displays the Syslog event sources that are configured, if any.
- In the Event Categories panel toolbar, click **+**.

The Available Event Source Types dialog is displayed.
- Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
- Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.
- 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.

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

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