

RSA NetWitness Logs

Event Source Log Configuration Guide



VMware vRealize Operations Manager

Last Modified: Friday, June 02, 2017

Event Source Product Information:

Vendor: [VMware](#)

Event Source: vRealize Operations Manager (formerly vCenter Operations Manager)

Versions: 5.8.2 (vCenter Operations Manager), 6.0 (vRealize Operations Manager)

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: vmware_vcops

Collection Method: SNMP, Syslog

Event Source Class.Subclass: Host.Virtualization

RSA supports two collection methods for the VMware vRealize Operations Manager event source:

- SNMP Traps
- Syslog

Configure vRealize Operations Manager for SNMP

To configure vRealize Operations to send SNMP traps data to RSA NetWitness Suite, you must complete these tasks:

- I. Configure SNMP Services. The procedure depends on your version:
 - Set up SNMP on vRealize Operations Manager, or
 - Set up SNMP on vCenter Operations Manager
- II. On the RSA NetWitness Suite, perform the following tasks:
 - i. Add the SNMP Event Source Type
 - ii. Configure SNMP Users

Configure SNMP Services on vRealize Operations Manager

This section describes how to configure SNMP services on the vRealize Operations event source.

To configure vRealize Operations to send SNMP messages to RSA NetWitness Suite:

1. Log onto the vRealize Operations Web UI.
2. Click the **Administration** icon in the left navigation pane.
3. Click **Outbound Alert Settings**, then click **+** in the toolbar to add a plug-in.
4. From the **Plug-In Type** drop-down menu, select **SNMP Trap**.
5. In the SNMP server settings section, make the following changes.
 - Enter a descriptive **Instance Name**.
 - For **Destination Host**, enter the IP address of your RSA NetWitness Suite Remote Log Collector.
 - For **Port**, enter **162**.
 - For **Community**, enter **public**.
6. Click **Save**.

7. To start the outbound alert service for this plug-in, select the instance in the list and click **Enable** on the toolbar.

This instance of the SNMP Trap plug-in is configured and running.

Configure SNMP Services on vCenter Operations Manager

This section describes how to configure SNMP services on the vCenter Operations Manager event source.

To configure vCenter Operations Manager to send SNMP messages to RSA NetWitness Suite:

1. Log onto the vCenter Operations Manager Administration Web UI.
2. Click the **SMTP/SNMP** tab.
3. In the SNMP server settings section, make the following changes.
 - Select **Enable SNMP services**.
 - For Host(FQDN/IP) enter the IP address of your RSA NetWitness Suite Remote Log Collector.
 - For Port, enter 162
 - For Community, enter public.
4. Click **Update**.
5. Click the **Status** tab.
6. In the Application Controls section, click **Restart**.

When adding the SNMP Event Source Type below, note the following settings:


- Type **public** into the **Community Strings** parameter:

- Type **162** into the **Ports** parameter:

Add the SNMP Event Source Type

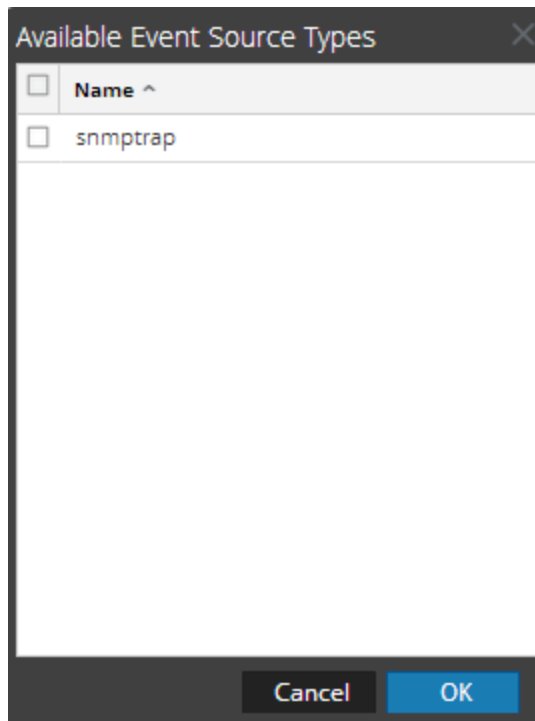
Note: If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

Add the SNMP Event Source Type:

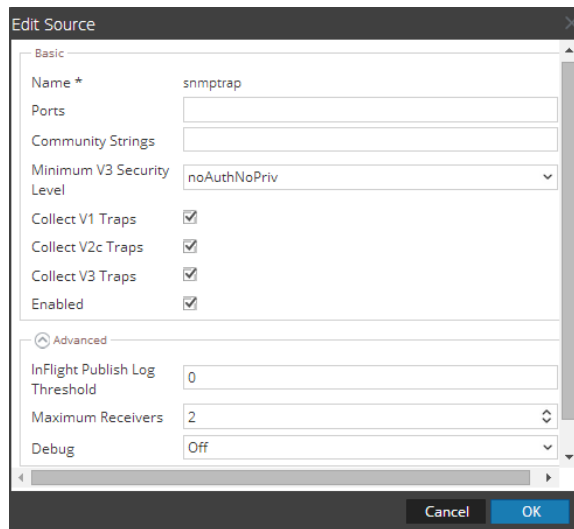
1. In the **RSA NetWitness Suite** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

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

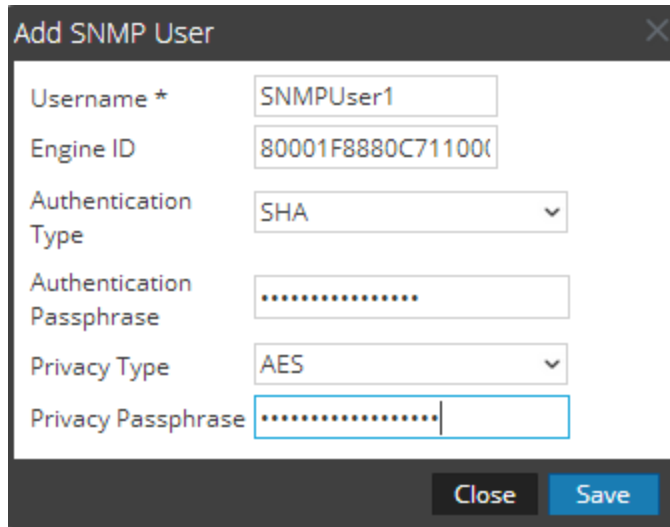
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

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: <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 vRealize Operations Manager for Syslog

To configure vRealize Operations Manager to send Syslog data to RSA NetWitness Suite, you must complete these tasks:

- I. Configure Syslog on vRealize Operations Manager
- II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog on vRealize Operations Manager

This section describes how to configure forwarding of vRealize Operations Manager logs to a Syslog Server.

To configure Syslog on vRealize Operations:

1. Log onto the vRealize Operations Web UI.
2. Click the **Administration** icon in the left navigation pane.
3. Click **Audit**, then click **Configure**.
4. Select **Output** and enter the IP address of your RSA NetWitness Suite Remote Log Collector.
5. Click **OK**.



Syslog messages are now forwarded to the RSA NetWitness Suite Remote Log Collector.

Configure RSA NetWitness Suite for 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  **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:

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.

Copyright © 2017 EMC Corporation. All Rights Reserved.

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.