

RSA NetWitness Logs

Event Source Log Configuration Guide



EMC Celerra

Last Modified: Thursday, May 11, 2017

Event Source Product Information:

Vendor: [EMC](#)

Event Source: Celerra

Versions: 7.0, 7.1

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: celerra

Collection Method: SNMP

Event Source Class.Subclass: Storage.Storage

Configure EMC Celerra

Perform the following tasks to configure EMC Celerra to work with RSA NetWitness Suite:

- Configure EMC Celerra to send SNMP traps.
- Configure EMC Celerra as an SNMP event source on RSA NetWitness Suite:
 - i. Add the SNMP Event Source Type
 - ii. Configure SNMP Users

Configure EMC Celerra to Send SNMP Traps

You have to configure your EMC Celerra event source to send SNMP traps.


To configure EMC Celerra version 7.x:

1. Log onto EMC Unisphere with your credentials.
2. On the Dashboard, click on the Celerra system from which you want to send SNMP logs.
3. Click **System > Monitoring and Alerts > Notifications**.
4. Form the **Event** tab, click **Create**.
5. In the **Additional notifications** section, enter the following information:
 - For the **Facility**, choose one or more facilities for which you want to send SNMP traps.
 - For **Severity**, select **Info**.
 - For **Action**, select **Trap**.
 - For **Destination Type**, enter the IP address for the RSA NetWitness Suite Log Collector; public.
6. Click **Apply**, then **OK** to save your changes.

Add the SNMP Event Source Type

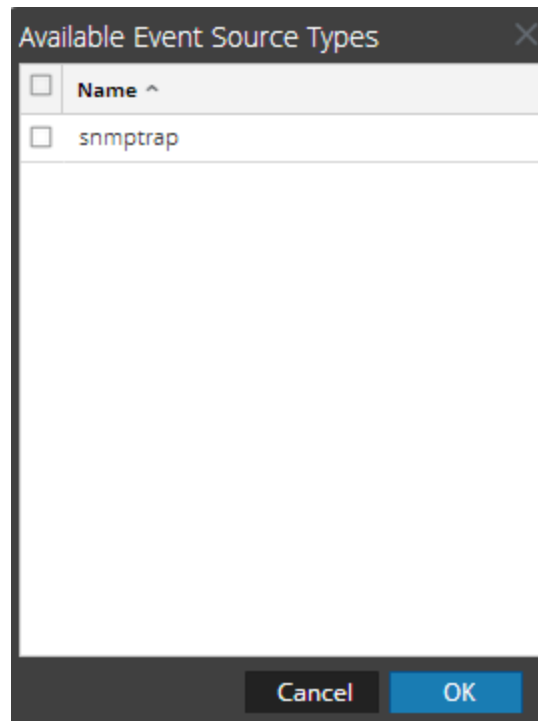
Note: If you have previously added the `snmptrap` type, you cannot add it again. You can edit it, or manage users.

Add the SNMP Event Source Type:

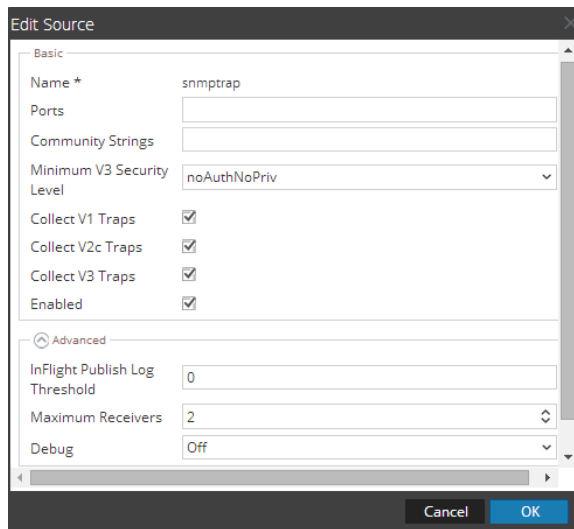
1. In the **RSA NetWitness Suite** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

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

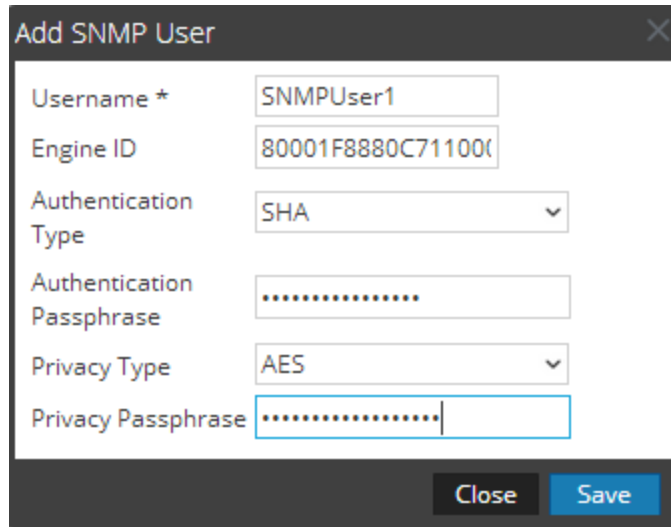
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

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.



- 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 *	<p>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.</p> <p>The Username and Engine ID combination must be unique (for example, logcollector).</p>
Engine ID	<p>(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.</p> <p>For all event sources sending SNMPv3 informs, you must add just the username with a blank engine id.</p>
Authentication Type	<p>(Optional) Authentication protocol. Valid values are as follows:</p> <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.

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.