RSA NetWitness Logs

Event Source Log Configuration Guide

EMC VNX (formerly CLARiiON)

Last Modified: Friday, May 12, 2017

Event Source Product Information:

Vendor: EMC
Event Source: VNX / CLARiiON
Platforms/Versions:

- Navisphere 6.28
- Unisphere 1.1

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: clariion
Collection Method: SNMP
Event Source Class.Subclass: Storage.Storage

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

- Configure the EMC event source to send SNMP traps.
- Configure SNMP traps on NetWitness Suite:
  1. Add the SNMP Event Source Type
  2. If you are using SNMPv3, configure SNMP Users

Configure EMC VNX to Send SNMP Traps

To configure EMC VNX, you must complete these tasks depending on your environment:

- Configure EMC VNX via Navisphere: Set up Distributed Monitoring and Set up Centralized Monitoring, or
- Configure EMC VNX via Unisphere: Set Up Distributed Monitoring via Unisphere

Set up Distributed Monitoring using Navisphere

To set up distributed monitoring using Navisphere:

1. Log on to the EMC Navisphere Manager with administrative credentials.
2. If an Enterprise Storage window is not already open, go to **File** > **New Enterprise Storage Window**.
3. Click on the **Monitors** tab.
4. Right-click the **Templates** folder, and select **Create New Template**.
5. In the **General** tab, set up the parameters as follow.

Field	Value
Template Name	RSA NetWitness Suite
Events	General
Event Severity	Informational, Warning, Error, Critical
Event Categories	Basic Array Feature Events, MirrorView Events, SnapView Events, SAN Copy Events, NQM Events, Alerts

6. In the **SNMP** tab, set up the parameters as follow.

Field	Value
SNMP Management Host	The IP address of RSA Security Analytics Log Decoder or Remote Log Collector

Field	Value
Community	public

7. Click **OK**.

8. Expand **Storage System**, right-click the storage system that you want to monitor, and select **Monitor Using Template**.

9. From the drop-down list, select the RSA NetWitness Suite template that you created, and click **OK**.

Set up Centralized Monitoring using Navisphere

To set up distributed monitoring using Navisphere:

1. Log on to the EMC Navisphere Manager with administrative credentials.

2. Create a domain that includes all the storage systems running the storage management server software that you want to monitor.

3. Use the **Portal Configuration** dialog box to do the following:

   a. Add a portal (use one of the systems in the domain).

   b. Assign the centralized monitoring agent to the portal configuration using the **Add Storage System** right-click option.

   c. Add any Agents managing legacy systems that you want to monitor to the portal.

4. In the **Portal Configuration** dialog box, click **OK**.

   Note: The EMC Navisphere Manager places an icon for the centralized monitoring agent in the **Monitors** tab of the Enterprise Storage window, and adds icons for any legacy systems to the **Storage** tree

5. To issue commands to the centralized monitoring agent, you must add the IP address of the portal to the monitoring agent's configuration file. On the central monitor, add the following for all the arrays that you want to monitor to the agent.config file:

   - **user system@*SP-A-IP-Address***

   - **user system@*SP-B-IP-Address***

Note: In Windows, this file is typically located at **C:\Program Files\EMC\Navisphere Agent**. For Windows, instead of directly editing the **agent.config** file, you can also do the configuration using **AgentInitConfig.exe** located in the Agent's installation directory.

6. Use the configuration wizard or the right-click menu options to do the following:
   - Add monitored Agents to the centralized monitoring configuration.
   - Create and apply centralized event monitoring templates to the monitoring agent.

   Warning: After you have created a centralized monitoring agent, do not add another centralized monitoring agent to the configuration.

7. If an Enterprise Storage window is not already open, go to **File** > **New Enterprise Storage Window**.
8. Click the **Monitors** tab.
9. Right-click the **Templates** folder, and select **Create New Template**.
10. In the **General** tab, set up the parameters as follow.

Field	Value
Template Name	RSA NetWitness Suite
Events	General
Event Severity	Informational, Warning, Error, Critical
Event Categories	Basic Array Feature Events, MirrorView Events, SnapView Events, SAN Copy Events, NQM Events, Alerts

11. In the **SNMP** tab, set up the parameters as follow.

Field	Value
SNMP Management Host	The IP address of RSA Security Analytics Log Decoder or Remote Log Collector
Community	public

12. Click **OK**.

13. Expand the **Storage System**, right-click the domain that you want to monitor, and select **Monitor Using Template**.
14. From the drop-down list, select the RSA NetWitness Suite template that you created, and click **OK**.

Set up Distributed Monitoring via Unisphere

To configure EMC VNX via Unisphere, you only need to set up distributed monitoring.

To set up distributed monitoring using Unisphere:

1. Log on to the EMC Unisphere Manager with administrative credentials.
2. Click the **All Systems** drop-down list, and select the VNX server that you want to configure.
3. Click **System** > **Monitoring and Alerts** > **Notifications**.
4. From the **Configure** tab, click **Configuration Wizard**, and follow these steps to complete the configuration wizard:
   a. In the Welcome to the Event Monitor Wizard window, click **Next**.
   b. In the **Wizard Template Name** field, type NetWitness Suite, and select **Distributed Monitoring**. Click **Next**.
   c. Ensure that all the host names are selected, and click **Next**.
   d. Select **General**, and in the **General** section, ensure that **All errors, warnings and information messages** is selected. Click **Next**.
   e. Select **Send SNMP Traps**, and click **Next**.
   f. Set the parameters as follow, and click **Next**.

Field	Value
SNMP Management Host	The IP address of RSA Security Analytics Log Decoder or Remote Log Collector
Community	public

   g. Click **Finish**.

Configure SNMP Traps on NetWitness Suite

In RSA NetWitness Suite, you need to configure the SNMP event source type (if you have not done so before), and, if you are using SNMPv3, configure SNMP users.

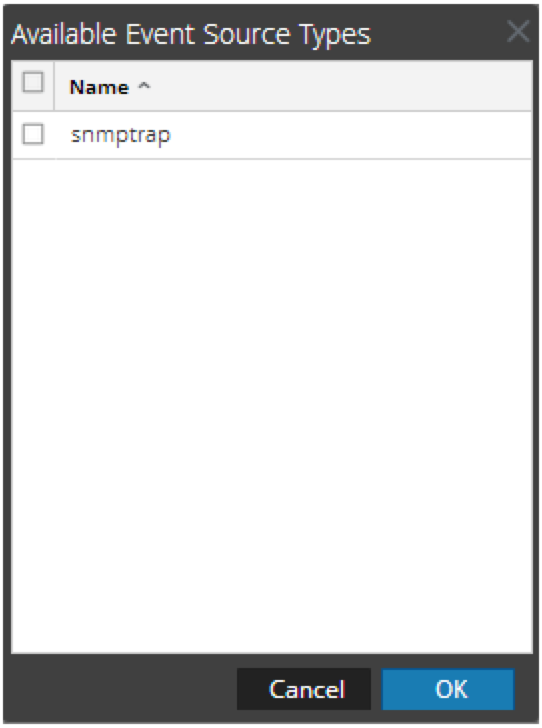
Add the SNMP Event Source Type

> **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.

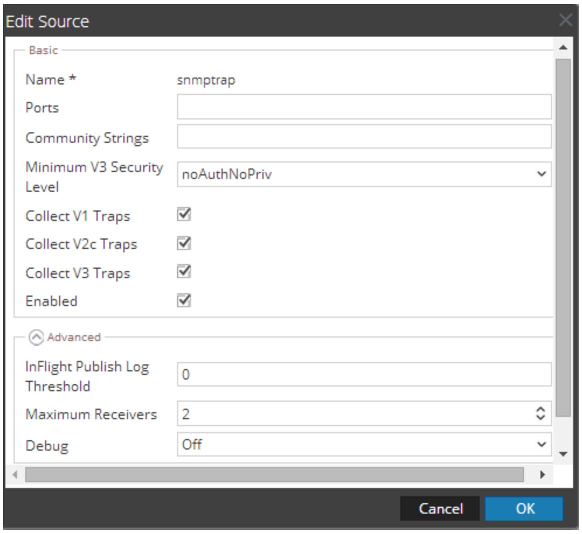


□	Name
□	snmptrap

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.



Name *	snmptrap
Ports	
Community Strings	
Minimum V3 Security Level	noAuthNoPriv
Collect V1 Traps	☑
Collect V2c Traps	☑
Collect V3 Traps	☑
Enabled	☑
InFlight Publish Log Threshold	0
Maximum Receivers	2
Debug	Off

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**.

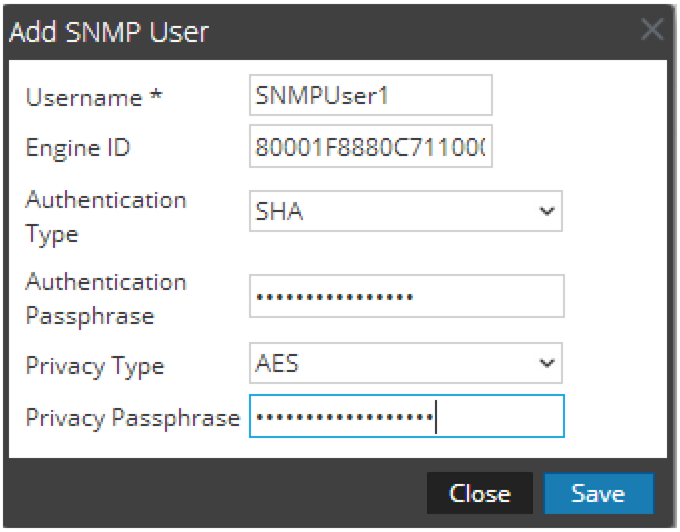
2. In the **Services** grid, select a **Log Collector** service.

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.



Username *	SNMPUser1
Engine ID	80001F8880C71100(
Authentication Type	SHA
Authentication Passphrase	••••••••••••••••
Privacy Type	AES
Privacy Passphrase	••••••••••••••••••

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 • **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