

RSA NetWitness Logs

Event Source Log Configuration Guide



IBM Domino

Last Modified: Thursday, October 19, 2017

Event Source Product Information:

Vendor: [IBM \(Lotus\)](#)

Event Source: Lotus Domino

Versions: 8.5, 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.

Platforms: Windows 2003, 2008

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: lotusdomino

Collection Method: SNMP

Event Source Class.Subclass: Host.Mail Servers

To configure IBM Lotus Domino , you must complete these tasks:

- Configure IBM Lotus Domino to send SNMP
- Configure SNMP Event Sources on the NetWitness Suite

Configure IBM Lotus Domino to send SNMP

To configure Lotus Domino to send data to RSA NetWitness Suite, you must complete these tasks:

- I. Set Up SNMP Services on Lotus Domino Server
- II. Configure SNMP Services on the Lotus Domino Server

Set Up SNMP Services on Lotus Domino Server

To set up SNMP services on the Lotus Domino server:

1. To install the **Lotus Domino** SNMP Agent as a service, open a command prompt, change directories to the **Lotus\Domino** directory, and type:

```
lnsnmp -Sc
```

2. Confirm that the Microsoft SNMP service is installed.
3. To start the **SNMP** and **LNSNMP** services, type:

```
net start snmp  
net start lnsnmp
```
4. Click **Start > Programs > Administrative Tools > Services > SNMP Service**.
5. On the **Traps** tab, in the **Community name** field, type **public**.
6. Click **Add to list**.
7. In the **Traps destinations** section, click **Add**.
8. In the **Host name, IP or IPX address** field, enter the IP address of your RSA NetWitness Suite Log Decoder or Remote Log Collector.
9. Click **Add**.
10. Click **OK**.
11. Confirm that the startup types for both SNMP Server and Lotus Domino SNMP Agent are set to **Automatic**.
12. To complete the configuration of the Domino SNMP agent, perform the following tasks:

- a. To support SNMP queries, start the QuerySet add-in task. On the Domino Server console, type:

```
load qryset
```
- b. To support SNMP traps for Domino events, start the Event Interceptor add-in task. On the Domino Server console, type:

```
load intrcpt
```
- c. To support Domino statistic threshold traps, start the Statistic Collector add-in task. On the Domino Server console, type:

```
load collect
```
- d. To automatically restart the add-in tasks the next time that Domino is restarted, open the **NOTES.INI** file, and add **qryset** and **collect**, or **intrcpt** and **collect** to the **ServerTasks** variable.

Configure SNMP Services

Note: Configurations may vary based on your environment. For more information, see the *Lotus Domino Domain Monitoring Red* paper.

To configure SNMP services:

1. Log on to the Domino Administrator utility with your administrative credentials.
2. On the **Files** tab, select the **Monitoring Configuration (events4.nsf)** document.
3. In the Monitoring Configuration pane, expand the DDM Configuration tree, and select **DDM Probes > By Type**.
4. Select **Enable Probes > Enable All Probes In View**.

Note: You may receive a warning after performing this action. This is a normal result because some of the probes require additional configuration.

5. In the Monitoring Configuration pane, select **DDM Filters**.
6. Select **New DDM Filter**, and select the filter that you want to edit.
7. Select **Apply filter to enhanced and simple events** and **Log All Event Types**.
8. Depending on your environment, apply the filter to all servers in a domain or only to specific servers.
9. Do one of the following:

- If creating a new filter, click **Save & Close**.
 - If editing an existing filter, click **Edit Document**.
10. In the Monitoring Configuration pane, select **Event Handlers > By Server**.
 11. Select **New Event Handler** and set the following parameters.

| Tab | Field | Action |
|--------|-----------------------------|--|
| Basics | Server(s) to monitor | Do one of the following: <ul style="list-style-type: none"> • Select Notify of the event on any server in the domain, • Select Notify of the event only on the following servers:, and choose which servers you want to monitor. |
| | Notification trigger | Select Any event that matches a criteria . |
| Event | Criteria to match | Select Events can be any type . |
| | | Select Events must be one of these severities , and select all severities. |
| | | Select Events can have any message . |
| Action | Notification method | Select SNMP Trap . |
| | Enablement | Select Enable this notification . |

12. Click **Save & Close**.

Note: As you are following the instructions to configure SNMP event sources, you must type **public** into the **Community Strings** parameter in step 8 below.

Configure SNMP Event Sources on the NetWitness Suite

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 Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration > 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 **lotusdomino**.

The first time that you configure an SNMP event source on RSA NetWitness Suite, you need to add the SNMP event source type and configure SNMP users.

Add the SNMP Event Source Type

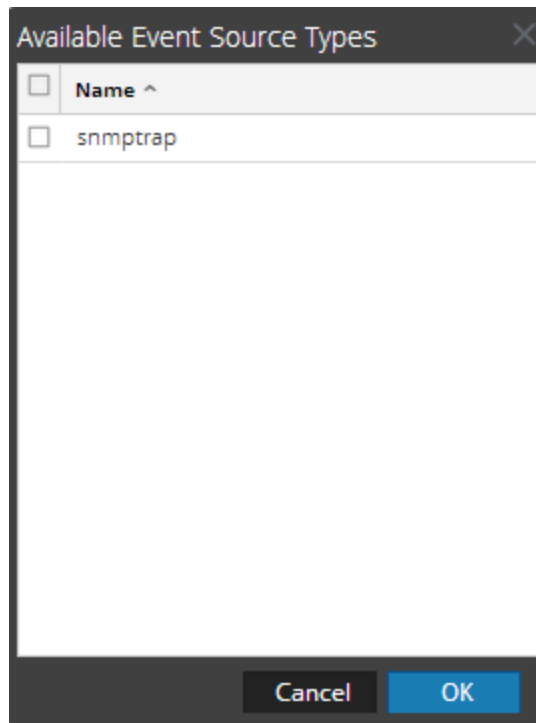
Note: If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

Add the SNMP Event Source Type:

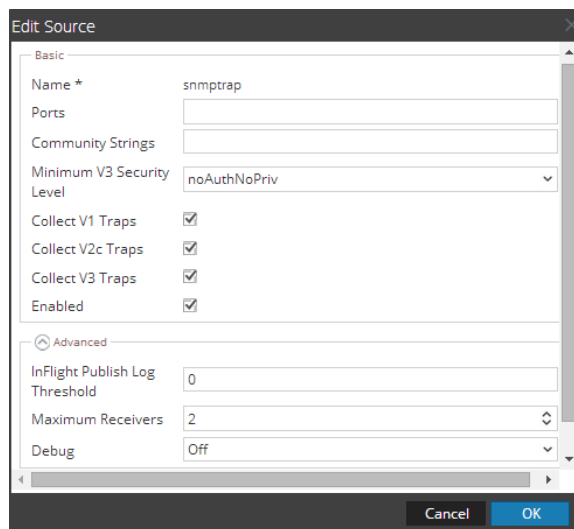
1. In the **RSA NetWitness Suite** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the **Log Collector Event Sources** tab, select **SNMP/Config** from the drop-down menu.

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

5. Click **+** to open the **Available Event Source Types** dialog.



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

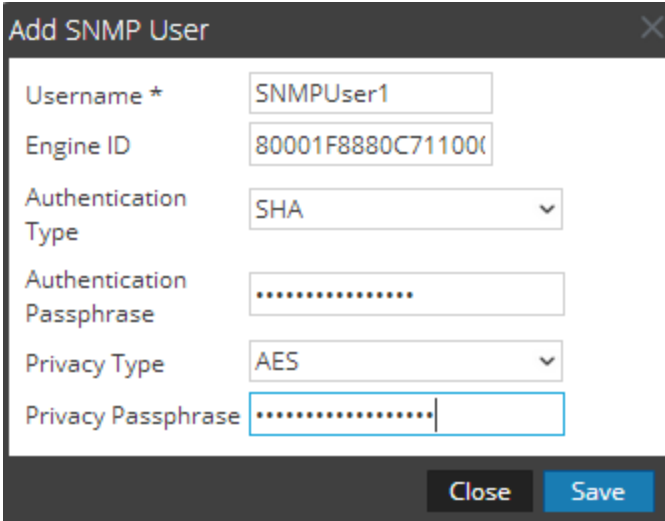
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

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.



The screenshot shows the 'Add SNMP User' dialog box with the following fields and values:

| Field | Value |
|---------------------------|------------------|
| 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 * | <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 • MD5 - Message Digest Algorithm |
| Authentication Passphrase | <p>Optional if you do not have the Authentication Type set. Authentication passphrase.</p> |
| Privacy Type | <p>(Optional) Privacy protocol. You can only set this parameter if Authentication Type parameter is set. Valid values are as follows:</p> <ul style="list-style-type: none"> • None (default) • AES - Advanced Encryption Standard • DES - Data Encryption Standard |
| Privacy Passphrase | <p>Optional if you do not have the Privacy Type set. Privacy passphrase.</p> |
| Close | <p>Closes the dialog without adding the SNMP v3 user or saving modifications to the parameters.</p> |
| Save | <p>Adds the SNMP v3 user parameters or saves modifications to the parameters.</p> |

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.