

RSA NetWitness Logs

Event Source Log Configuration Guide



NETASQ Unified Manager

Last Modified: Thursday, June 29, 2017

Event Source Product Information:

Vendor: [NETASQ](#)

Event Source: Unified Manager

Versions: 8.1.3, 9.0.2, and 9.0.3.2

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: netasqutm

Collection Method: Syslog

Event Source Class.Subclass: Security.Firewall

Configure NETASQ Unified Manager

To configure Syslog collection for the NETASQ Unified Manager you must:



- I. Configure NetWitness Suite for Syslog Collection
- II. Configure Syslog Output on NETASQ Unified Manager

Configure 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.

Configure Syslog Output on NETASQ Unified Manager

NETASQ Unified Manager uses protocol conformity analysis, application filtering, and anti-virus analysis to inspect authorized traffic flows and strengthen application security. NETASQ enables you to establish and configure user-based security policies, giving you greater control over which network resources each user is authorized to access.

Configuring Log Format

You must run a system command on your NETASQ server that sets up the log files so that the RSA NetWitness Suite can correctly parse the messages. On your NETASQ server, run the following command:

```
setconf /usr/Firewall/ConfigFiles/Communication/config  
Syslog LogtypePos 1
```

The RSA NetWitness Suite requires logs in a certain format. You must run a Unix or Linux command to prepare the logs, and then you can set up the forwarding of the logs to the RSA NetWitness Suite.

After you configure the log format, configure the appropriate version of your NETASQ UTM event source:

- [Configure NETASQ Unified Manager version 9 or later](#)
- [Configure NETASQ Unified Manager version 8.1](#)

Configure NETASQ Unified Manager version 9 or later

You configure NETASQ Unified Manager version 9 through a web interface.


To configure NETASQ Unified Manager 9 to send logs to the RSA NetWitness Suite platform:

1. Start the **NETASQ Unified Manager** web application by entering the following URL:

```
https://NETASQ_IPaddress/admin
```

where *NETASQ_IPaddress* is the IP address of the NETASQ firewall.

2. Log on with your credentials.

3. From the navigation bar, select **Configuration > Notifications > Logs - Syslog**.
4. Select the **Syslog** tab.
5. Select the **Enable sending logs by Syslog** field.
6. Create a destination server object for your RSA NetWitness Suite server:
 - a. In the **Destination server** field, click the **Create an object** icon (.
 - b. In the Create an object window, ensure **Host** is selected, and enter the following information.

Field	Value
Object Name	Enter a descriptive name for the host, such as RSANetWitness Suite .
DNS resolution	Select None (static IP) .
IP address	Enter the IP address for your RSA NetWitness Suite Log Decoder or Remote Log Collector.

- c. Click **Apply**.
- d. In the **Port** field, select **syslog**.
- e. In the Families of Sent Logs section, select the types of messages to send to the RSA NetWitness Suite Log Decoder or Remote Log Collector..

Note: Use the **Allow all** or **Block all** buttons to enable or disable all messages. Clicking on an individual family toggles its state between enabled and disabled.

- f. Click **Apply**.
- g. In the confirmation window, click **Save** to save the new configuration.

Configure NETASQ Unified Manager version 8.1

You configure NETASQ Unified Manager version 8.1 through the a **NETASQ Unified Manager** application.

To configure NETASQ Unified Manager 8.1 to send logs to the RSA NetWitness Suite platform:

1. Start the **NETASQ Unified Manager** application.
2. Enter the IP address of the firewall, your logon credentials, and click **Connect**.
3. Create a host object for your RSA NetWitness Suite server.
 - a. In the navigation pane, select **Objects**.
 - b. In the Object database window, select **New > Host**.
 - c. In the Host Creation Wizard, enter the following information.

Field	Value
Host Name	Enter a descriptive name for the host, such as RSA NetWitness Suite .
DNS resolution type	Select Static .
IP	Enter the IP address for your RSA NetWitness Suite Log Decoder or Remote Log Collector.
Use System Logging	Select disabled .

- d. Click **Next**, and skip the second screen by clicking **Finish**.
 - e. Click **OK** to close the Object database window.
4. Configure the logs and syslog information.
 - a. From the navigation pane, select **Logs**.
 - b. In the Log configuration window, select **Syslog**.
 - c. Select **Forward logs to an external syslog server**.
 - d. Click **Host** and select the object that you just created. Click **OK**.
 - e. Click **Port** and select **Services > syslog**. Click **OK**.
 - f. From the list of available logs, select the logs from which you wish to collect, and then click **Send**.

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.