# RSA NetWitness Platform

Event Source Log Configuration Guide

# Linux

**Last Modified: Friday, December 20, 2019**

**Event Source Product Information:**

**Vendors**: Red Hat Enterprise, Debian, Novell
**Event Source**: Linux
**Versions**:

- Red Hat: 3.x, 4.x, 5.x, 6.0, 7.x
- Novell SuSE Linux Enterprise 9, 10, 10.2, 11, 12.x
- Debian GNU/Linux 3.1 and 4.0

**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.

**RSA Product Information:**

**Supported On**: NetWitness Platform 10.0 and later
**Event Source Log Parser**: rhlinux
**Collection Method**: Syslog
**Event Source Class.Subclass**: Host.UNIX

To configure your version of Linux, perform the following tasks:

- Follow the appropriate configuration instructions for your Linux vendor:
  - Configure Novell SuSE 10.2
  - Configure Other Linux Versions
- If you use Red Hat Linux, you must also perform the following tasks:
  1. Configure Auditd on Red Hat Linux
  2. Configure WTMP Logs for Red Hat Linux
  3. Configure the iptables Service
- Configure RSA NetWitness Platform

# Configure Novell SuSE 10.2

You can use either UDP or TCP. Follow the appropriate instructions for the protocol that you are using.

## Configure UDP

### To configure SuSE Linux using UDP:

1. On the Linux appliance, log on as **root**.
2. Open the **/etc/syslog-ng/syslog-ng.conf.in** file.
3. At the end of the file, add the following lines:

```
# send everything to log host
destination loghost {
   udp("xxx.xxx.xxx.xxx" port(yy));
};
log {
   source(src);
   destination(loghost);
};
```

where:

- xxx.xxx.xxx.xxx is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
- yy is the port number on which the RSA NetWitness Log Decoder or Remote Log Collector is listening for incoming syslog messages.

4. Run the following commands:

```
SuSEconfig --module syslog-ng
/etc/init.d/syslog restart
```

> **Note:** If you have Novell SuSE 9 or earlier, you must stop and start the service by running these commands:
>
> ```
> /etc/init.d/syslog stop
> /etc/init.d/syslog start
> ```

## Configure TCP

Perform the following steps on the Linux event source to configure SuSE Linux to send syslog in TCP packets.

### To configure SuSE Linux 10.2 to send syslog in TCP packets:

1. On the Linux machine, log on as **root**.
2. Open the **/etc/syslog-ng/syslog-ng.conf** file.
3. At the end of the file, add the following lines:

```
# send everything to log host
destination loghost {
   tcp("xxx.xxx.xxx.xxx" port(yy));
};
log {
   source(src);
   destination(loghost);
};
```

   where:

   - xxx.xxx.xxx.xxx is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
   - yy is the port number on which the RSA NetWitness Log Decoder or Remote Log Collector is listening for incoming syslog messages.

4. Run the following commands:

```
SuSEconfig --module syslog-ng
/etc/init.d/syslog start
```

# Configure Other Linux Versions

**To configure any other Linux version:**

1. On the Linux appliance, open the **/etc/syslog.conf** file in a text editor. If you are using Redhat Linux 6.0 or higher, open **/etc/rsyslog.conf**.
2. To configure the event source to log all messages of debug level and higher to the syslog server, add the following line:

   ```
   *.debug @xxx.xxx.xxx.xxx
   ```

   where xxx.xxx.xxx.xxx is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
3. Save the file, and close the text editor.
4. To restart the syslog service, depending on your version of Linux, run the following command:
   - For Redhat Linux 6.0:

     ```
     service rsyslog restart
     ```
   - For other versions of Linux:

     ```
     service syslog restart
     ```

# Configure Auditd on Red Hat Linux

If you use Red Hat Linux, you must configure Auditd. Perform the steps in the appropriate section for your deployment:

- Configure Auditd for Red Hat 5 and Later
- Configure Auditd for Red Hat 4 and Earlier

## Configure Auditd for Red Hat 5 and Later

Follow these instructions to configure auditd for versions 5 and later of Red Hat Linux.

**To configure Auditd for Red Hat 5 and later:**

1. Install **audispd-plugins**.
2. Open **/etc/audit/auditd.conf**, and change the dispatcher attribute to **/sbin/audispd**.

3. In **/etc/syslog.conf**, verify that all logs are directed to the RSA NetWitness Log Decoder or Remote Log Collector.
4. Restart the auditd service.
5. To ensure that the audit logs are forwarded to the RSA NetWitness Log Decoder or Remote Log Collector, perform the following steps:
   a. In **/etc/audisp/plugins.d/syslog.conf**, verify that all logs are directed to the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
   b. Enable audit messages forwarding to syslog by editing **/etc/audisp/plugins.d/syslog.conf** and change the `active = no` clause to `active = yes`.

## Configure Auditd for Red Hat 4 and Earlier

Follow these instructions to configure auditd for versions 4 and earlier of Red Hat Linux.

### To configure Auditd for Red Hat 4 and earlier:

1. Open **/etc/init.d/auditd**, and comment out the following lines:
   - Replace line 58,

     ```
     daemon $prog "$EXTRAOPTIONS"
     ```

     with the following:

     ```
     #daemon $prog "$EXTRAOPTIONS"
     ```
   - Replace line 71,

     ```
     killproc $prog
     ```

     with the following:

     ```
     #killproc $prog
     ```
2. Restart the auditd service.

# Configure WTMP Logs for Red Hat Linux

**To configure WTMP logs for Red Hat Linux:**

1. Create a new directory named ***$Home*/wtmp**, where *$home* is your home directory.
2. Download the **nicwtmp.sh** script RSA Link: https://community.rsa.com/docs/DOC-47131
3. Place the **nicwtmp.sh** file in the **wtmp** directory.
4. Schedule the script to run as a Cron task every hour. For instructions, see the Red Hat Linux Product Documentation, or search the web for how to schedule a cron job on RHEL.

# Configure the iptables Service

**Note:** Before configuring the iptables service, you must configure Red Hat Linux as described in Other Linux Configuration Instructions.

### To configure the iptables service to obtain syslog events:

1. To check the status of the iptables service, open a command prompt, and run the following command:

   ```
   iptables status
   ```

   If the iptables service is not running, to start the service type the following command:

   ```
   iptables start
   ```

2. To enable iptables to send logs through syslog, insert a LOG rule just before the rule from which you want to collect logs. Follow these steps:

   a. To log an event, run the following command:

   ```
   # /sbin/iptables -I <ipchain_name> <rule-id/serial no> -j LOG --log-level 7
   ```

   b. To add a prefix to the log, run the following command:

   ```
   # /sbin/iptables -I <ipchain_name> <rule-id/serial no> -j LOG --log-level 7 --log-prefix "<any desired prefix>"
   ```

   c. To save the new LOG rule, type the following command:

   ```
   iptables-save
   ```

# Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- Ensure the required parser is enabled
- Configure Syslog Collection

## 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 Platform Live.

### Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN** > **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 **rhlinux**.

## Configure Syslog Collection

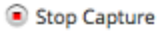
**Note:** You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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 **ADMIN** > **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 

, click the icon to start capturing Syslog.
- If you see 

, 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 **ADMIN** > **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.

After 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.

## Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.