

# NetWitness<sup>®</sup> Platform XDR

## Linux Event Source Log Configuration Guide

# Linux

## 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, and 15
- Debian GNU/Linux 3.1 and 4.0

**Note:** NetWitness 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 XDR 11.7 and higher

**Note:** Linux is supported from NetWitness Platform XDR 11.5. However, NetWitness recommends you to update NetWitness Platform XDR to the latest version.

**Event Source Log Parser:** rhlinux

**Collection Method:** Syslog

**Event Source Class.Subclass:** Host.UNIX

## Contact Information

NetWitness Community at <https://community.netwitness.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

## Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

## License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates and are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

## Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

## Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

## Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at <https://www.netwitness.com/standard-form-agreements/>.

© 2023 RSA Security LLC or its affiliates. All Rights Reserved.

September, 2022

# Contents

---

<b>Configure Novell SuSE 15 SP2</b> .....	<b>6</b>
<b>Configure Novell SuSE 10.2</b> .....	<b>7</b>
Configure UDP .....	7
Configure TCP .....	7
<b>Configure Other Linux Versions</b> .....	<b>9</b>
<b>Configure Auditd on Red Hat Linux</b> .....	<b>10</b>
Configure Auditd for Red Hat 5 and Later .....	10
Configure Auditd for Red Hat 4 and Earlier .....	10
<b>Configure WTMP Logs for Red Hat Linux</b> .....	<b>12</b>
<b>Configure the iptables Service</b> .....	<b>13</b>
<b>Configure NetWitness Platform XDR</b> .....	<b>14</b>
Ensure the Required Parser is Enabled .....	14
Configure Syslog Collection .....	14
<b>Getting Help with NetWitness Platform XDR</b> .....	<b>17</b>
Self-Help Resources .....	17
Contact NetWitness Support .....	17
Feedback on Product Documentation .....	18

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

- Follow the appropriate configuration instructions for your Linux vendor:
  - [Configure Novell SuSE 15 SP2](#)
  - [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 NetWitness Platform XDR](#)

## Configure Novell SuSE 15 SP2

---

Perform the steps specified in SuSE System Analysis and Tuning Guide, [System Log Files](#), to collect SuSE 15 SP2 logs.

## 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 NetWitness Log Decoder or Remote Log Collector.
  - `yy` is the port number on which the 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 NetWitness Log Decoder or Remote Log Collector.
- yy is the port number on which the 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 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 NetWitness Log Decoder or Remote Log Collector.
4. Restart the auditd service.
5. To ensure that the audit logs are forwarded to the 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 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 NetWitness Link: [Linux](#).
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 NetWitness Platform XDR

---



Perform the following steps in NetWitness Platform XDR:

- [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 NetWitness Platform XDR Live.

**Ensure that the parser for your event source is available:**

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.

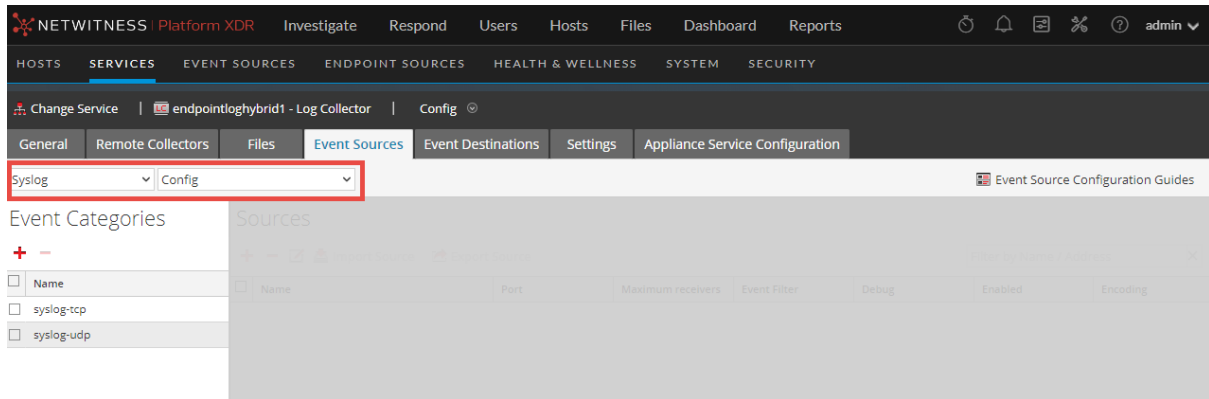
**To configure Log Decoder for Syslog Collection**

1. In the NetWitness Platform XDR menu, select  (Admin) > **Services**.
2. In the **Services** grid, choose 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 Remote Log Collector for Syslog Collection

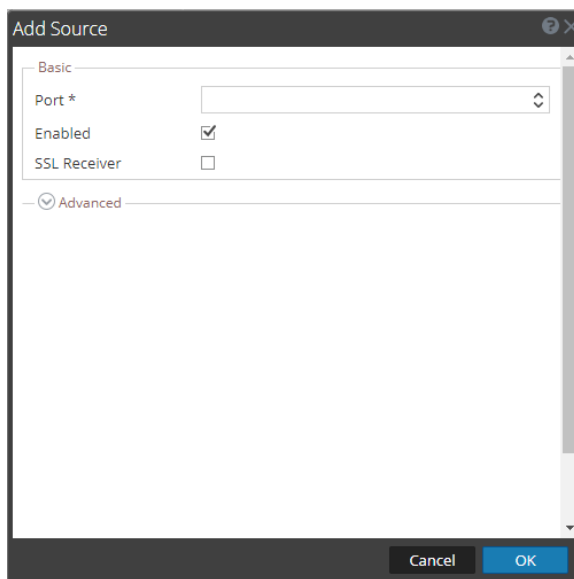
1. In the NetWitness Platform XDR menu, go to  (Admin) > **Services**.
2. In the **Services** grid, select a Remote Log Collector and from the **Actions** () menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog / Config** from the drop-down menu.

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 will appear.
5. Choose either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Choose the **New Type** in the **Event Categories** panel and click **+** in the **Sources** panel toolbar.

The **Add Source** dialog will appear.



7. Enter **514** for the port and choose **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. You can continue to add Syslog event sources to your system without a need to do any further configuration in NetWitness Platform XDR.



# Getting Help with NetWitness Platform XDR

## Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: <https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation>.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: <https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions>.
- See the NetWitness Knowledge Base: <https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base>.
- See the documentation for Logstash JDBC input plugin here: <https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html>.
- See Troubleshooting section in the guides.
- See also [NetWitness® Platform Blog Posts](#).
- If you need further assistance, [Contact NetWitness Support](#).

## Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform XDR or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	<a href="https://community.netwitness.com">https://community.netwitness.com</a> In the main menu, click <b>Support</b> > <b>Case Portal</b> > <b>View My Cases</b> .
International Contacts (How to Contact NetWitness Support)	<a href="https://community.netwitness.com/t5/support/ct-p/support">https://community.netwitness.com/t5/support/ct-p/support</a>
Community	<a href="https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions">https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions</a>

## Feedback on Product Documentation

You can send an email to [nwdocsfeedback@netwitness.com](mailto:nwdocsfeedback@netwitness.com) to provide feedback on NetWitness Platform documentation.