

## Integrating Linux Server

<https://campus.barracuda.com/doc/96767908/>

By default, recent releases across most Linux distributions will have the rsyslog package already installed and enabled by default.

To send logs using syslog to the sensor please perform the following tasks as root:

1. Verify that rsyslog is installed, enabled and running.  
`systemctl status rsyslog`
2. Create filename `/etc/rsyslog.d/sensor.conf` and enter the following rule with the sensor's static IP address:  
`*.notice @IP_ADDRESS`
3. Restart rsyslog service.  
`systemctl restart rsyslog`

## Troubleshooting

**Service for rsyslog is installed but not enabled or running.**

```
systemctl enable --now rsyslog
```

**Service for rsyslog is not installed.**

SUSE: `yast -i rsyslog`

Fedora/RHEL/CentOS: `yum install rsyslog`

Ubuntu/Debian: `apt-get install rsyslog`

**Traffic for syslog is not sent to sensor from client.**

1. Verify that client can ping sensor.
2. Open two terminal windows on the client.
3. In the first terminal, enter the following command to determine the primary LAN interface (e.g. `eth0`):  
`ip a | grep UP`
4. In the same terminal, run the following command to inspect egress traffic on the primary interface for syslog traffic:  
`tcpdump -ni eth0 -Q out port 514`
5. In a second terminal generate syslog traffic:  
`logger "test message from log client"`

6. Monitor output in the first terminal to confirm outbound syslog traffic. An abbreviated example output is indicated below:  
`IP 172.29.91.84.40644 > 172.29.88.253.514: SYSLOG user.notice`
7. If outbound syslog traffic is observed on client then verify that no ACLs in network are dropping traffic sent to port 514.

For Linux servers, forward your rsyslogs from your server to your Barracuda XDR sensor over UDP port 514.

Depending on your version of Linux, the configuration may vary.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.