rsyslog server settings for receiving logs

Here are the steps you can follow to configure rsyslog to receive logs from remote servers:

1. Install rsyslog on the machine that you want to use as the central log server. On a Debian-based system, you can install rsyslog with the following command:

```
sudo apt-get install rsyslog
```

2. Open the rsyslog configuration file in a text editor. On a Debian-based system, this file is typically located at /etc/rsyslog.conf.

```
sudo nano /etc/rsyslog.conf
```

3. In the configuration file, uncomment the line that reads "module(load="imudp")" and "input(type="imudp" port="514")". This will configure rsyslog to listen for incoming log messages on UDP port 514. If you want to use a different port, you can specify it here.
4. Save and close the configuration file.
5. Restart the rsyslog service to apply the new configuration. On a Debian-based system, you can do this with the following command:

```
sudo service rsyslog restart
```

To view the logo, use the command

```
sudo less /var/log/syslog
```

You should get something like this

```
Dec 28 15:42:50 dev.softkeel.com [2265632.987952] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265632.988013] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.020799] TIMEGENERATED=2022-12-28 15:42:50
```

```
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.071709] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.081883] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.081972] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.239150] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=44680 DST=20.190.159.4 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.245651] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.245738] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.336217] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.339190] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.345274] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.345456] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:42:50 dev.softkeel.com [2265633.430714] TIMEGENERATED=2022-12-28 15:42:50
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=37918 DST=40.126.32.160 DPT=443 PROTO=TCP
Dec 28 15:43:19 dev.softkeel.com [2265661.777196] TIMEGENERATED=2022-12-28 15:43:19
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=48566 DST=172.217.16.37 DPT=443 PROTO=TCP
Dec 28 15:43:19 dev.softkeel.com [2265661.784642] TIMEGENERATED=2022-12-28 15:43:19
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=48566 DST=172.217.16.37 DPT=443 PROTO=TCP
Dec 28 15:43:20 dev.softkeel.com [2265662.835952] TIMEGENERATED=2022-12-28 15:43:20
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=45142 DST=216.58.215.74 DPT=443 PROTO=TCP
Dec 28 15:43:40 dev.softkeel.com [2265682.853984] TIMEGENERATED=2022-12-28 15:43:40
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=41048 DST=142.251.1.188 DPT=5228 PROTO=TCP
Dec 28 15:43:40 dev.softkeel.com [2265682.893813] TIMEGENERATED=2022-12-28 15:43:40
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=41048 DST=142.251.1.188 DPT=5228 PROTO=TCP
Dec 28 15:43:40 dev.softkeel.com [2265682.921793] TIMEGENERATED=2022-12-28 15:43:40
PUBLIC=77.87.125.200 SRC=10.0.110.7 SPT=41048 DST=142.251.1.188 DPT=5228 PROTO=TCP
```

Revision #4
Created 28 December 2022 14:39:49 by Ruslan
Updated 16 October 2023 10:14:50 by Yuliia Noha