Linux Ubuntu kao mrežni SysLog server

written by js | 2023-05-13
Ubuntu automatski instalira SysLog /var/log/syslog.

[1] Editiraj:

- `nano /etc/rsyslog.conf`

[2] Makni komentar sa sljedećih redaka:

```
module(load="imudp")
input(type="imudp" port="514")
module(load="imtcp")
input(type="imtcp" port="514")
```

[3] Restartaj servis:

- `systemctl restart rsyslog`

[4] Pošalji event programom "nc" (netcat, https://cygwin.com/packages/summary/netcat.html):

- `echo "$env:ComputerName Proba123 šđčćž ŠĐČĆŽ" | nc <%IPadresaSysLogServera%> 514`

[5] Ako želiš da svaki ili neki PC na mreži ima svoj posebni syslog fajl, umjesto da svi zapisuju u /var/log/syslog:

(v. https://www.questioncomputer.com/syslog-server-on-ubuntu-20-04/)

- `nano /etc/rsyslog.d/30-custom.conf`

```
if $fromhost-ip startswith '10.11.12.13' then /var/log/network/10.11.12.13.log
& stop
if $fromhost-ip startswith '10.11.12.14' then /var/log/network/10.11.12.14.log
& stop
```

- `mkdir /var/log/network`
- `chown syslog:adm /var/log/network`
- `systemctl restart rsyslog`

---

syslog rsyslog xsyslog xrsyslog event xevent eventlog network