Rsyslogserver Remotelogging

Hauseigenes Apt-Repo: https://apt.iteas.at

Mit Rsyslog (Default in vielen Distributionen) ist es ein leiches in 15 Minuten einen zentralen voll funktionsfähigen Loggingserver zu bauen. Nachdem Rsyslog schon in **Ubuntu 18.04** vorinstalliert ist, muss man genau garnichts nach installieren.

Am Server passt man das Konfigurationsfile `/etc/rsyslog.conf` wie folgt an. Die folgende Sektion muss einkommentiert werden:

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

Nun noch ein Template wir denn gerne unsere Logs gerne abgelegt hätten. Das ganze unter dem gleichen File, gleich darunter:

```
...
$template remote-incoming-logs,"/var/log/remote-
logging/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?remote-incoming-logs
& ~
...
```

Den Zugriff könnte man noch mit `$AllowedSender TCP, 127.0.0.1, 192.168.10.0/24, *.example.com` einschränken. Jetzt noch das Verzeichnis erstellen und die richtigen Berechtigungen vergeben.

```
mkdri /var/log/remote-logging
chown syslog:syslog /var/log/remote-logging
```

Nun startet man den Server neu:

```
systemctl restart rsyslog.service
```

Somit ist der Serverpart fertig. Also nächstes kommt die Clientkonfiguration.

Rsyslog Clientkonfiguration

Diese besteht aus einer Datei: `/etc/rsyslog.d/51-remote.conf` Der Inhalt ist simpel. Nach dem anlegen dieser Datei starten wir auch auf unserem Client Rsyslog neu.

```
$PreserveFQDN on
```

```
$ActionQueueFileName queue
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1

*.* @meinserver.supertux.lan:514;RSYSLOG_SyslogProtocol23Format
```

```
systemctl restart rsyslog.service
```

Ab nun loggt unser Client bereits brav zentral im FQDN mit Unterfiles pro Pogramm.