Remote-Logging mit rsyslog

Um den Empfang von Remote-Messages im rsyslog zu ermöglichen sind in /etc/rsyslog.conf zwei, bzw. 4 Zeilen einzukommentieren:

```
# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

Üblicherweise werden Syslog-Messages per UDP übertragen. Will man aber auch auf einem TCP-Port empfangen muss das entsprechende Modul geladen und konfiguriert werden:

```
# provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

Damit der entfernte Server nun auch Meldungen sendet ist folgendes zu tun:

```
*.* @syslog.meinserver.de
```

Damit werden sämtliche Syslog-Einträge per UDP an den entfernten Server geschickt. Sollen die Pakete über TCP laufen wird ein zweites @ vor den Server gepackt. Die Portangabe ist optional, default-Port ist 514. Sollen die Meldungen an einen anderen Port geschickt werden, ist das hierüber konfigurierbar.

```
*.* @@syslog.meinserver.de:1234
```

Die Meldungen lassen sich auch auf wichtige Sachen einschränken. Beispielsweise nur Emergencies und Alerts, etc.

```
*.emerg,*.alert     @syslog.meinserver.de
*.emerg,*.alert,*.crit,*.err,*.warning  @syslog.meinserver.de
```

Bei instabilen Verbindungen kann es helfen die Meldungen in einer Sendequeue vorzuhalten:

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

Revision #1
Created 2021-04-30 12:12:21 UTC by magenbrot
Updated 2021-04-30 12:13:31 UTC by magenbrot