

# rsyslog

- [Meldungen per Regex in eine andere Datei umleiten](#)
- [Remote-Logging mit rsyslog](#)

# Meldungen per Regex in eine andere Datei umleiten

Mit diesem Beispiel lassen sich Meldungen, die von „apache2“ gesendet werden und nicht den String „PHP Notice“ enthalten in die Datei /var/log/apache2-global-error.log schreiben.

```
if $programname == 'apache2' and not ($msg contains 'PHP Notice') then /var/log/apache2-global-e
```

Das ist z.B. sehr nützlich, wenn man einen Cluster loadbalancer Server hat und diese zentral loggen läßt. Es gibt dann nur ein Error-Log, das man bequem durchsuchen kann und einen Überblick über die Fehler im gesamten Netz zeigt.

# 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 Sendequueue vorzuhalten:

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