System-Log's:

Unter Linux kann alles was auf dem Rechner passiert mitgeloggt werden. Diese Aufgabe übernimmt der so genannte Syslogger. Wir kümmern uns um den "syslogd".

Alle Meldungen die entstehen bevor der Syslogger gestartet wurde, werden im Kernel-Ringbuffer gespeichert und können mit "dmesg" abgerufen werden.

Die Log-Kategorien

Kern	→	Meldungen die vom Kernel kommen
auth	→	Meldungen vom Sicherheitssystem (login, ...)
authpriv	→	Vertrauliche Meldungen vom Sicherheitssystem
mail	→	Meldungen vom Mailsystem
news	→	Meldungen vom Newssystem
uucp	→	Meldungen vom UUCP-System
cron	→	Meldungen vom CRON
lpr	→	Meldungen vom Drucksystem
daemon	→	Alle Dienste die keine eigene Kategorie haben
user	→	Meldungen normale Anwendungen
ftp	→	Meldungen vom ftp-Server
local0 - local7	→	Frei verfügbar

Prioritäten

None	→	wird verwendet um Log-Kategorien aus zu schließen
debug	→	Zur Fehleranalyse
info	→	Protokollierung zum Normalen Programmablauf
notice	→	Protokollierung bemerkenswerter Situationen
warn	→	Warnungen aller Art
err	→	Fehlermeldungen aller Art
crit	→	Meldungen über Kritische Situationen, die gerade nochmal gut gegangen sind
alert	→	Meldungen die ein Sofortiges eingreifen erforderlich machen
emerg	→	Letzte Meldung vor dem Absturz

Die Konfigurationsdatei: /etc/syslog.conf

```
1   *.*;auth,authpriv.none          -/var/log/messages
2   auth,authpriv.*                 -/var/log/auth.log

3   kern.*                          -/var/log/kernel.log
4   kern.err                        *
5   mail.*                          /dev/null

6   *.alert                         /var/log/hiiilllllffffeeee.log
7   *.*                             @172.16.107.30
8   *.*                             /dev/tty10
9   *.=crit                         /var/log/crit.log
```

zu 1.) Meldungen aller Kategorien und aller Prioritäten außer auth und authpriv, werden in die /var/log/messages geschrieben, der Cache darf verwendet werden.
zu 2.) Alle meldungen der Kategorien auth und authpriv, aller Prioritäten werden in die /var/log/auth.log geschrieben, der Cache darf verwendet werden.
zu 3.) Alle Meldungen der Kategorie "kern" mit jeder Priorität werden in Die Datei /var/log/kernel.log geschrieben.
zu 4.) Alle Meldungen der Kategorie "kern" mit der Priorität "err" werden in die Loginshells aller angemeldeten benutzer geschrieben.
zu 5.) Alle Meldungen der Kategorie "mail" werden nach /dev/null geschrieben
zu 6.) Alle Meldungen aller Kategorien die die Priorität "alert" oder schlimmer haben werden in die "/var/log/hiiilllllffffeeee.log" geschrieben. Der Cache darf nicht verwendet werden.
zu 7.) Alle Meldungen werden an den Syslogger des Rechners 172.16.107.30 übergeben.
zu 8.) Alle Meldungen werden auf's TTY10 geschreiben.
zu 9.) Alle Meldungen die die Priorität haben werden in die "/var/log/crit.log" geschrieben.

Zusatz zu 7.) Der Syslogger auf dem entfernten Rechner muß mit der Option „-r" gestartet worden sein.

Logrotate:

Logrotate wird verwendet um die Logdateien zu verwalten. Damit die Logdateien nicht zu groß werden und eventuell das laufende System beeinträchtigen. Die Konfigurationsdatei:

/etc/logrotate.conf

```
/var/log/meine_log_datei.log {
 size 4M
 rotate 8
 olddir /var/log/alte_logdateien
 compress
 prerotate
     echo " die Datei meine_log_datei.log wird gleich rotiert"
     >>/root/lr.txt
 endscript
 postrotate
     echo " die Datei meine_log_datei.log wurde gerade rotiert"
     >>/root/lr.txt
 endscript
}
```

Hier Wird sich also auf die Datei "/var/log/meine_log_datei.log" bezogen, wenn Sie eine Größe vin 4MB Erreicht hat soll sie Rotiert werden. Sie soll gezippt werden un in den Ordner "/var/log/alte_logdateien" verschoben werden.

Es sollen 8 versionen dieser Datei erhalten bleiben. Vor und Nach der Rotation soll etwas in die "/root/lr.txt" geschrieben werden. Logrotate wird nun folgendermaßen ausgeführt:

logrotate /etc/logrotate.conf

Dies sollte nun z.B. per cron regelmäßig passieren.