Die Datei /etc/syslog.conf

grundlegende Form jeder Zeile:

```
Herkunft.Priorität[;Herkunft.Priorität]...   --Tabulatortaste-->   Aktion
```

- mehrere Herkunftskategorien in einer Regel werden durch Kommas voneinander getrennt
- mehrere Herkunfts-/Prioritäts-Paare gleichzeitig werden durch Strichpunkt getrennt
- sowohl Herkunft als auch Priorität können durch "*" ersetzt werden, das als Wildcard (für alle) dient.

Herkunftskategorien

kern	Systemmeldungen direkt vom Kernel
auth	Meldungen vom Sicherheitsdienst des Systems (login, ...)
authpriv	Vertrauliche Meldungen der internen Sicherheitsdienste (auch: "security")
mail	Meldungen des Mail-Systems
news	Meldungen des News-Systems
uucp	Meldungen des UUCP-Systems
lpr	Meldungen des Druckerdaemons
cron	Meldungen des Cron-Daemons
syslog	Meldungen des syslog-Daemons selbst
daemon	Meldungen aller anderer Daemon-Prozesse
user	Meldungen aus normalen Anwenderprogrammen
local0-local7	frei verwendbar

Prioritäten in absteigender Reihenfolge

emerg	Der letzte Spruch vor dem Absturz (auch: "panic")
alert	Alarmierende Nachricht, die sofortiges Eingreifen erforderlich macht
crit	Meldung über eine kritische Situation, die gerade nochmal gut gegangen ist
err	Fehlermeldungen aller Art aus dem laufenden Betrieb (auch: "error")
warn	Warnungen aller Art aus dem laufenden Betrieb (auch: "warning")
notice	Dokumentation besonders bemerkenswerter Situationen im Rahmen des normalen Betriebs
info	Protokollierung des normalen Betriebsablaufes
debug	Mitteilungen interner Programmzustände bei der Fehlersuche
none	Ist keine Priorität im eigentlichen Sinn, sondern dient zum Ausschluß einzelner Herkünfte

- Eine angegebene Priorität meint immer die genannte oder eine höhere. Wenn jedoch vor der Priorität ein Gleichheitszeichen (=) steht, so ist nur die genannte Priorität gemeint. (z. B. mail.=info)
- Ein vorangestelltes "!" bedeutet Negation dieser Stufe und höher. Vor allem in Kombination sinnvoll (mail.*;mail.!err), um bestimmte Meldungen niedriger Prioritätsstufen auszuwählen.
- Es können auch mehrere Kategorien mit der selben Priorität angegeben werden (mail,news.info)

Aktionen

Eine Aktion ist immer eine Weiterleitung einer Nachricht.

1. **Ausgabe der Nachricht in eine Datei.**
   Angabe des Dateinamens mit absolutem Pfad (mit führendem Slash)
   Durch ein "-" vor dem Dateinamen wird asynchrones Schreiben erlaubt. (schneller durch RAM)
2. **Weiterleitung der Nachricht an einen Syslog-Daemon eines anderen Rechners im Netz.**
   Angabe des Zielrechnernamens mit vorangestelltem "@". Dort muss der Syslog-Daemon mit der Kommandozeilenoption **-r** (remote) gestartet worden sein.
   sinnvoll für eine gemeinsame Auswertung oder gegen das Verwischen von Hackerspuren
3. **Ausgabe der Nachricht auf den Bildschirm von angemeldeten Usern**
   Angabe des Benutzernamens (oder einer durch Kommas getrennten Liste von Benutzernamen)
   Ein "*" steht für alle angemeldeten Benutzer
4. **Schreiben in eine benannte Pipe (FIFO: First In First Out)**
   Angabe des FIFO-Namens mit absolutem Pfad und vorangestelltem "|" (z. B. | /dev/xconsole)

Test mit dem Programm logger:

Erzeugen von Protokolleinträgen, per Default mit dem Herkunfts-Prioritäten-Paar user.notice

```
logger -p local0.err -t Test "Hallo Welt"
```

Beispielsdatei /etc/syslog.conf

```
# /etc/syslog.conf - Configuration file for syslogd(8)
#
# For info about the format of this file, see "man syslog.conf".
#

#
#
# print most on tty10 and on the xconsole pipe
#
kern.warn;*.err;authpriv.none     /dev/tty10
kern.warn;*.err;authpriv.none    |/dev/xconsole
*.emerg                           *

# enable this, if you want that root is informed
# immediately, e.g. of logins
#*.alert                         root

#
# all email-messages in one file
#
mail.*                           -/var/log/mail

#
# all news-messages
#
# these files are rotated and examined by "news.daily"
news.crit                        -/var/log/news/news.crit
news.err                         -/var/log/news/news.err
news.notice                      -/var/log/news/news.notice
# enable this, if you want to keep all news messages
# in one file
#news.*                  -/var/log/news.all

#
# Warnings in one file
#
*.=warn;*.=err                   -/var/log/warn
*.crit                            /var/log/warn

#
# save the rest in one file
#
*.*;mail.none;news.none          -/var/log/messages

# enable this, if you want to keep all messages
# in one file
*.*                              -/var/log/allmessages
*.*                              /dev/tty11
```

Nach dem Bearbeiten der /etc/syslog.conf ist der **syslogd** zum Einlesen der neuen Konfiguration zu bewegen:
 # killall -HUP syslogd

Probleme von syslogd:

- keine Authentifizierung (mit Option –r nimmt er *jede* Meldung auf Port 514/UDP entgegen)
- verbindungslose Übertragung via UDP (Pakete können verloren gehen)
- überträgt Meldungen unverschlüsselt im Klartext
- unflexible Konfiguration (20 Herkünfte und 8 Prioritäten)
- die Anwendung selbst bestimmt die zu verwendende Herkunft und Priorität beim Logging , nicht syslogd
- beim Weiterleiten über mehrere Loghosts wird die ursprüngliche Quelle überschrieben, kein FQDN