Die Datei /etc/syslog-ng/syslog-ng.conf

globale Optionen:
wie geht Syslog-NG mit Hostnamen um, wenn es Nachrichten über mehrere Logserver weiterreicht
```
options { keep_hostname(no); chain_hostnames(yes); };
```

keep_hostname(no)	bei Weiterleitung über mehrere Loghosts den Namen des Ursprungsrechners beibehalten
chain_hostname(yes)	ist keep_hostname abgeschaltet, werden die Namen der weiterreichenden Server einfach an den bereits vorhandenen Hostnamen angehängt
sync(0)	Anzahl gepufferter Zeilen, bei Systemabsturz gehen Meldungen verloren
use_fqdn(yes)	FQDN nutzen
use_dns(no)	DNS Auflösung abschalten

Quellen:
Es gibt 8 unterschiedliche Source-Treiber. Jede geöffnete Verbindung erzeugt einen eigenen Prozess. Die Verbindungsanzahl ist beschränkbar mit der Option "max-connections" (Default = 10).
```
source quellname  { internal(); file("/proc/kmsg"); };
```

Source	Beschreibung
internal	Treiber für eigene Meldungen des Daemons syslog-ng; unbedingt erforderlich
unix-stream	Öffnet den angegebenen Unix-Socket im »SOCK_STREAM«-Modus und lauscht auf Nachrichten
unix-dgram	Öffnet den Unix-Socket im »SOCK_DGRAM«-Modus und empfängt davon Nachrichten
file	Öffnet die angegebene Datei (liest z. B. aus /proc/kmsg)
pipe, fifo	Öffnet die angegebene Named Pipe und liest Meldungen (als Quelle)
udp	Lauscht auf dem angegebenen UDP-Port auf Nachrichten
tcp	Lauscht auf dem angegebenen TCP-Port auf Nachrichten
sun-stream	Öffnet das angegebene Stream-Gerät (nur auf Solaris)

Filter:
Filter legen fest, wie Syslog-NG mit den Nachrichten verfährt, die es von den Quellen erhält.
```
filter filtername { level(warn) and facility(kern); };
```

Filterfunktion	Beschreibung
facility	Trifft auf Nachrichten zu, die von der angegebenen Facility stammen
level, priority	Trifft auf Nachrichten mit der angegebenen Priorität zu
program	Filtert Nachrichten, bei denen das Programmnamen-Feld dem angegebenen regulären Ausdruck entspricht
host	Filtert Nachrichten, bei denen das Hostnamen-Feld dem angegebenen regulären Ausdruck entspricht
match	Wendet den angegebenen regulären Ausdruck auf die gesamte Nachricht an
filter	Ruft eine weitere Filterregel auf

Funktionen verknüpfbar mit booleschen Operationen (and, or, not und Klammern).
Einige Filterfunktionen verstehen sogar reguläre Ausdrücke.

Ziele:
Destination-Treiber bestimmen, wohin und auf welchem Weg die Nachricht weitergeleitet werden soll.
```
destination zielname { file ("/var/log/messages"); };
```

Destination	Beschreibung
file	Schreibt die Nachricht in die angegebene Datei
pipe, fifo	Übergibt die Meldung an die angegebene Named Pipe
unix-stream	Schickt die Nachricht an den »SOCK_STREAM«-Unix-Socket
unix-dgram	Schickt die Nachricht an den »SOCK_DGRAM«-Unix-Socket
udp	Schickt die Nachricht an den angegebenen UDP-Port
tcp	Schickt die Nachricht an den angegebenen TCP-Port
usertty	Schickt Nachricht als Konsolenmeldung an den angegebenen User, falls dieser angemeldet ist
program	Startet ein angegebenes Programm und übergibt die Nachricht an dessen Standardeingabe

Logpfade
setzen den kompletten Weg eines Loggingwunsches zusammen: Sources → Filters → Destinations
auch mit mehreren Sourcen, Filtern oder Zielen
```
log { source(quellname); filter(filtername); destination(zielname); };
```

Herkunftskategorien (facility)

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 (level)

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

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"
```

Aktivieren des syslog-ng unter SUSE:

im File »/etc/sysconfig/syslog« folgenden Eintrag ergänzen `SYSLOG_DAEMON="syslog-ng"`
und dann den Daemon neu starten

behebt Probleme von syslogd:

- verbindungslose Übertragung via UDP (Pakete können verloren gehen) auf TCP umschaltbar
- flexible Konfiguration
- die Anwendung selbst bestimmt die zu verwendende Herkunft und Priorität beim Logging , nicht syslogd
- Adressen der Quell-remote-Logginghosts sind festlegbar
- beim Weiterleiten über mehrere Loghosts wird die ursprüngliche Quelle bei Bedarf nicht mehr überschrieben
- kennt FQDNs
- noch keine Authentifizierung, aber nachrüstbar
- überträgt Meldungen noch immer unverschlüsselt im Klartext, aber nachrüstbar

Quellen: Christian Schmitz Linux-Magazin 11/2003

Beispielsdatei /etc/syslog.conf

 # Globale Optionen

```
options { keep_hostname(no); chain_hostnames(yes); sync(0); };
```

 # Quellen

der Identifier der ersten Quelle traegt den Namen lokal
der Treiber internal muss vorhanden sein
der Treiber unix-stream liest aus der Gerätedatei /dev/log
der Treiber file liest aus /proc/kmsg die Kernelmeldungen
mehrzeilig

```
source lokal  {
        internal();
        unix-stream("/dev/log");
        file("/proc/kmsg");
};
```

syslog-ng nimmt Meldungen auf TCP-Port 3333 von 192.168.0.24 entgegen
einzeilig

```
source remote { tcp(ip 192.168.0.24) port(3333) max-connections(10); };
```

 # Filter

erfasst alle Meldungen mit den Loglevel warn, err und crit

```
filter warnung { level(warn, err, crit); };
```

Suche nach allen Meldungen, die den regexp "ftp" enthalten

```
filter ftp { match("ftp"); };
```

auf Konsole 10 nur sehr wichtige Nachrichten ausgeben

```
filter konsole {
   level(err) and not facility(authpriv)
   or level(warn) and facility(kern);
};
```

Erfassen aller Meldungen des Mailsystems

```
filter email { facility(mail); };
```

 # Destinations

Wichtige Meldungen an TTY10 senden

```
destination konsole { file("/dev/tty10"); };
```

Alle Mail-Nachrichten in Datei /var/log/mail schreiben

```
destination email { file ("/var/log/mail"); };
```

Weiterleiten an den Loghost 172.16.0.33 via UDP an Port 514, der wiederum eine source definiert haben muss

```
destination loghost { udp(ip(172.16.0.33) port(514)); };
```

 # Logpfade

enthalten den kompletten Weg von Quelle ueber Filter zum Ziel
Weiterleitung aller Meldungen der Quelle namens lokal mit den Regeln des Filters konsole
an die Destination konsole

```
log { source(lokal); filter(konsole); destination(konsole); };
```

schreibt Nachrichten des lokalen Mailsystems in die Datei /var/log/mail

```
log { source(lokal); filter(email); destination(email); };
```

Nachrichten aus dem Netzwerk weiterleiten, die ftp betreffen

```
log { source(remote); filter(ftp); destination(loghost); };
```

Nach dem Bearbeiten der /etc/syslog-ng/syslog-ng.conf ist der **syslog-ng** zum Einlesen der neuen Konfiguration zu bewegen:

 # killall -HUP syslog-ng