Auf der Suche nach dem Log...

Eine kleine Einführung zum Thema sysklogd

von TeaAge

Wer kennt das nicht? Man kauft sich eine neue Hardware, möchte diese in Betrieb nehmen und nichts passiert.

Jetzt begibt man sich auf die Fehlersuche oder bittet um Hilfe (z.B. bei www.mandrivauser.de). Bei beiden Wegen sollte man erstmal selbst ein paar Informationen zusammentragen. Hierzu bietet sich das Paket *sysklogd* an mit den beiden Programmen zum Loggen (Mitschreiben/Aufzeichnen) von Kernel-Meldungen (*klogd) und* Meldungen von Systemprogrammen *(syslogd).*

Eine von sysklogd erstellte Logdatei ist beispielsweise die oft genannte */var/log/messages*.

Die Meldungen werden im Allgemeinen nach Verursacher und Priorität eingeordnet. Die (meiner Meinung nach) interessantesten Verursacher sind *kern* (Kernel-Meldungen)*, user* (Benutzerprogramme), *daemon* (Hintergrundprozesse) und *news* (der Newsserver). Bei den Prioritäten seien hier *emerg* (Panik), *warn* (Warnung), err (Error/Fehler) und *info* (informell) genannt.

Diese kleine Erläuterung brauchen wir jetzt für die */etc/syslog.conf,* die zentrale Konfigurationsdatei. Hier steht, was *sysklog* wo abspeichern soll. Dazu muss man den Verursacher und die Prioritäten mit einem „Satzzeichen“ verbinden.

Im folgenden Beispiel lassen wir alle Kernel-Meldungen mit der Priorität Error (und höher) in die Datei /var/log/kernel/error.log schreiben. Dazu müssten wir also in die Datei */etc/syslog.conf* die folgende Zeile einfügen:

```
kernel.err        /var/log/kernel/error.log
```

Oder man lässt sich **nur** die Warnung in eine eigene Datei schreiben:

```
*.=warn                    /var/log/warning.log
```

Punkt und Gleichheitszeichen dienen als Gleichheitszeichen und der Stern als Platzhalter, steht also für Alles.

Alle Dateien die in syslog.conf angegeben sind, müssen existieren. Sysklog ist nicht in der Lage eine Datei anzulegen. Die Datei muss erst erstellt werden, z.B. mit *touch :*

```
touch error.log
```

Nun, die Logs in eine Datei speichern und bei Bedarf abrufen ist ganz nett, aber bequemer ist es, die Ausgabe direkt, also in Echtzeit, auf die **Text-Konsole** zu werfen.

Drückt man in der grafischen Oberfläche die Tastenkombination STRG + ALT + F1, so kommt man in die erste der 6 Text-Konsolen. Die anderen 5 erreichen wir auf dem selben Weg (STRG + ALT + F2 bis F6). Auf F7 kommt man zurück zur grafischen Oberfläche (sofern eine gestartet ist) aber F8-F11 (bei Mandriva 2007.1 und früher auch F12) sind noch ungenutzt. Wechselt man zur Zehn (STRG + ALT + F10) sieht man nur einen schwarzen Bildschirm und einen blinkenden Cursor.

Wir wollen nun alle Kernel Meldungen auf die Text-Konsole Zehn (*tty10*) ausgeben lassen.

Dazu melden wir uns als *root* in einer Konsole an (Stichwort: *su*), wechseln in das Verzeichnis */etc* und öffnen mit dem Editor die Datei *syslog.conf* .

Hier fügen wir ein, dass alle Kernel-Warnungen (*kern.**) in die Konsole Nummer 10 geschrieben werden sollen (*/dev/tty10*).

```
kern.*            /dev/tty10
```

Abspeichern, ein kurzer Blick auf die Text-Konsole 10 bringt und wir sehen ... nichts.

Wir haben etwas vergessen! Wir müssen den sysklogd-Dienst erst neustarten bevor die Änderungen wirksam werden. Das geht am bequemsten im *Mandriva Control Center* unter *System* mit der Funktion *Ein- oder Ausschalten von Systemdiensten*. Schneller geht es jedoch über die Konsole mit dem Befehl */etc/init.d/syslog restart* .

Nachdem wir über das Stoppen und erneutem Starten von syslog informiert wurden, sehen wir mit STRG + ALT + F10 die ersten Log-Meldungen auf der Konsole 10.

Ich habe bei mir eine weitere Zeile in der syslog.-conf. Mit

```
*.*               /dev/tty12
```

bekomme ich alle Meldungen auf die 12. Konsole ausgegeben. Damit kann ich während der Arbeit im System auch mal hinter die Kulissen gucken. Läuft nun also mit neuer Hardware etwas schief, können wir dort auf erste Spurensuche gehen.

Weitere Informationen zu dem Thema findet ihr in den man-Pages zu sysklogd (*man sysklogd*) und syslog.conf (*man syslog.conf*).

Viel Spaß damit!