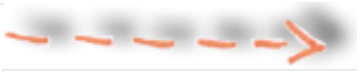
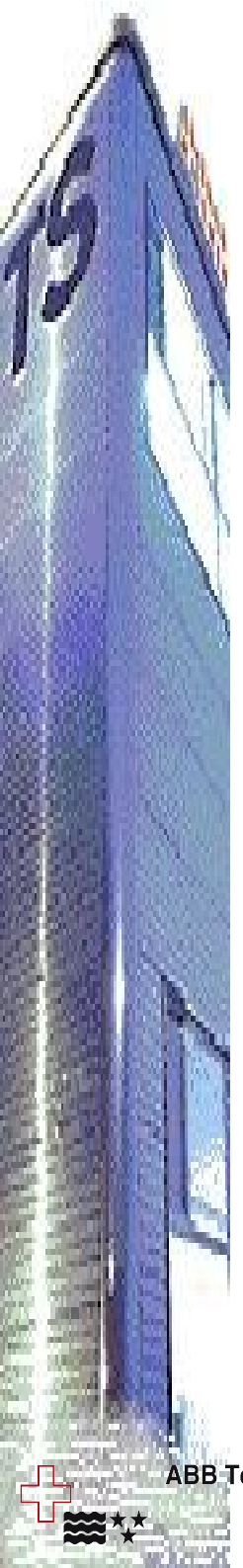
Systemprotokollierung

Lernziele



- Den Syslog-Daemon kennen und konfigurieren
- Protokolldateien mit logrotate verwalten
- Verstehen, wie der Systemkernel mit Nachrichten umgeht



Systemprotokollierung

- Programme haben ihren Benutzern von Zeit zu Zeit etwas mitzuteilen
  - der Vollzug einer Aufgabe
  - eine Fehlersituation
  - eine Warnung
- Textorientierte Programme schreiben auf das Terminal (Standard- oder Fehler-Device)
- Programme mit grafischer Oberfläche verwenden Messageboxen oder Statuszeilen

Systemprotokollierung

- Der Betriebssystemkern und die diversen Hintergrundprogramme haben nur die Systemkonsole
- Unter X11 erscheinen solche Nachrichten im *xconsole*-Fenster
- Meldungen an die Xconsole werden leicht übersehen
- Die Bildschirmmeldungen lassen sich nicht sichern

Der Syslog-Daemon

- Die Lösung dieses Problems bietet der Syslog-Daemon
  - `syslogd`
- Systemmeldungen können mit der *syslog()*-Funktion ausgegeben werden
- Der *syslogd* erhält die Nachrichten über das Socket `/dev/log`
- Der *syslogd* ist dadurch netzwerkfähig

Der Syslog-Daemon

- Die Konfiguration steht in

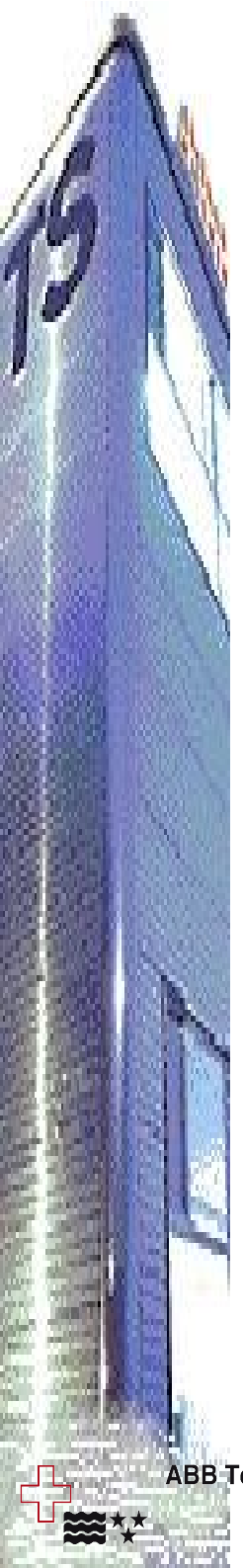
  `/etc/syslog.conf`

- Zwei Spalten bestimmen
  1. welche Meldungen ausgegeben werden
  2. wohin sie geschrieben werden

Die Datei syslog.conf

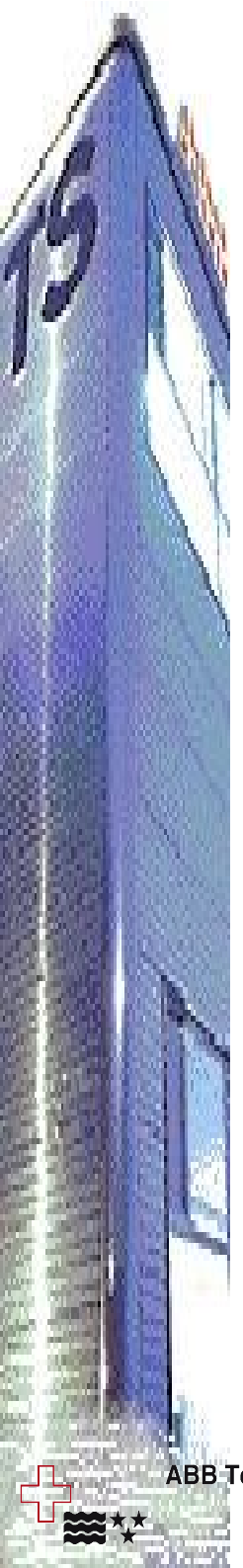
- Die Datei könnte folgendermassen aussehen:

```
kern.warn;*.err;authpriv.none  /dev/tty10
kern.warn;*.err;authpriv.none  |/dev/xconsole
*.emerg                        *
*.=warn;*.=err                 -/var/log/warn
*.crit                         /var/log/warn
*.*;mail.none;news.none        -/var/log/messages
```



Kategorien für den *syslogd*

Kategorie	Bedeutung
authpriv	Vertrauliche Meldungen der Sicherheitsdienste
cron	Meldungen von cron und at
daemon	Meldungen von Daemon-Programmen ohne eigene Kategorie
ftp	Meldungen des FTP-Daemons
kern	Systemmeldungen aus dem Betriebssystemkern
lpr	Meldungen des Druckersystems
mail	Meldungen des Mailsystems
news	Meldungen des Usenet-News-Systems
syslog	Meldungen des syslogd
user	Meldungen, die mit Benutzern zu tun haben
uucp	Meldungen des UUCP-Systems
local*r*	($0 \leq r \geq 7$) Frei verwendbar für lokale Nachrichten



Prioritäten für den *syslogd*

Priorität	Bedeutung
none	Dient dazu, Nachrichten einer Herkunftskategorie auszuschliessen (keine Priorität)
debug	Mitteilungen bei der Fehlersuche
info	Protokollierung des normalen Betriebsgeschehens
notice	Dokumentation besonderer Situationen
warning	(oder warn) Warnung über Zustände, die nicht gravierend sind
err	Fehlermeldungen aller Art
crit	Kritische Fehlermeldungen
alert	»Alarmierende« Nachrichten, die sofortiges Eingreifen erfordern
emerg	Die letzten Meldungen vor dem Absturz

Die Datei syslog.conf

- Die Erste Spalte kann mehrere Kategorien und Prioritäten enthalten

```
<Kategorie>.<Priorität>[;<Kategorie>.<Priorität>]...
```

- Ein Stern »*« steht als Platzhalter für alle Kategorien
- Kategorie und Priorität einer Meldung wird vom Anwender der Funktion *syslog()* bestimmt (i.d.R. vom Entwickler)

Die Datei syslog.conf

- Ein Auswahlkriterium in der Form
  - mail.info alle Meldungen des Mail-Daemon mit der Priorität info und höher
  - mail.=info nur Meldungen dieser Priorität
  - mail.!info alles ausser info und höher
  - mail.!=info alles ausser info
- Es können auch mehrere Kategorien mit derselben Priorität angegeben werden
  - mail,news.info

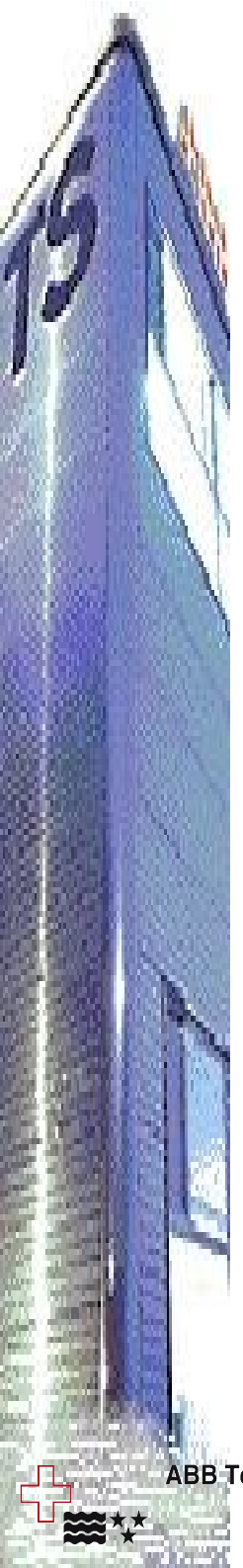
Die Datei syslog.conf

- Die rechte Spalte enthält das Ziel der Meldungen
  - eine Datei (Dateiname mit absolutem Pfad)
    - ein »-«-Zeichen vor dem Pfad bedeutet, dass nicht sofort ein *sync* ausgeführt wird
  - ein Gerät (etwa /dev/tty10)
  - eine benannte Pipe (FIFO) »|«-Zeichen
  - über das Netz an einen anderen syslogd »@«-Zeichen gefolgt von IP-Adresse
  - an Benutzer (username oder »*« für alle)

Der Syslog-Daemon

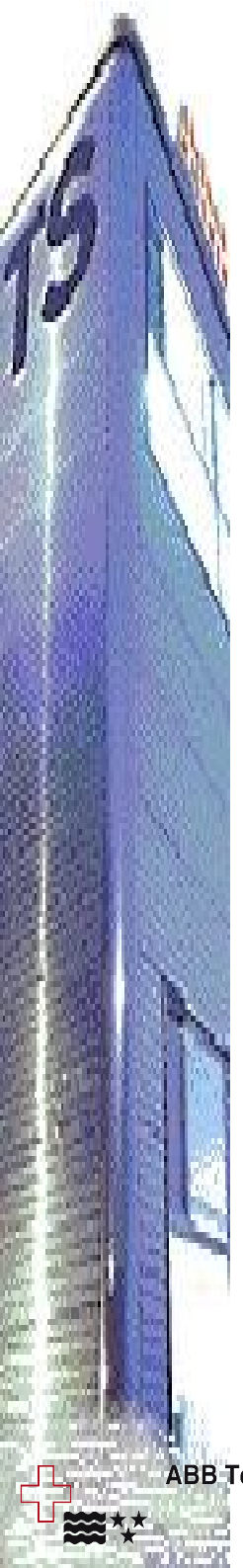
- Nach Änderungen an der *syslog.conf*, muss dem *syslogd* das Signal SIGHUP geschickt werden
- Testen kann man den syslogd-Mechanismus mit dem Programm *logger*
  - `logger -p local0.err -t TEST "Hallo Welt"`
- Die Meldungen enthalten normalerweise Datum, Rechnernamen, und den Prozess, der die Meldung verursacht hat

Fragen?



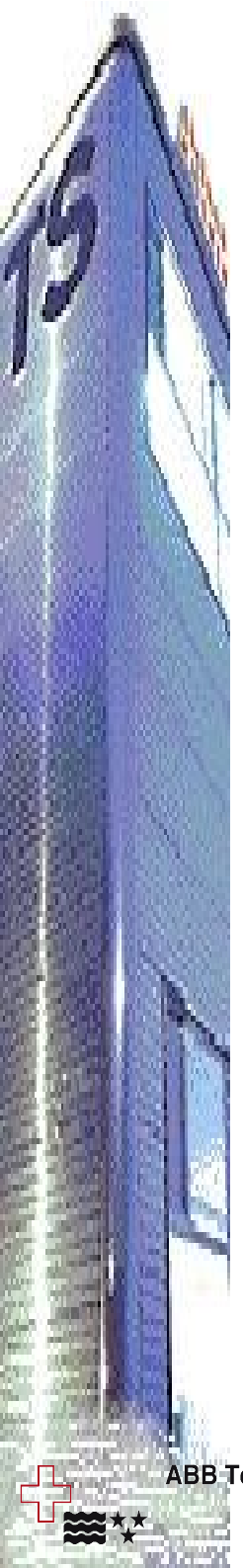
Übungen

- [8.1] Finden Sie heraus, wann zuletzt jemand per *su* auf Ihrem Rechner die Identität von *root* angenommen hat.



Übungen

- [8.2] Konfigurieren Sie den syslogd so, dass er zusätzlich zur aktuellen Konfiguration alle (!) Meldungen in eine neue Datei */var/log/test* protokolliert.
- Testen Sie das Ergebnis.



Übungen

- [8.3] Konfigurieren Sie den syslogd auf einem Rechner so, dass er Protokollnachrichten über das Netz entgegennimmt.
- Konfigurieren Sie den syslogd auf dem anderen Rechner so, dass er Nachrichten der Kategorie *local0* auf den ursprünglichen Rechner schickt.
- Testen Sie die Konfiguration.

Die Protokolldateien

- Protokolldateien werden in der Regel unter */var/log* abgelegt
  - /var/log/messages
  - /var/log/warn
  - /var/log/Xorg.0.log
  - /var/log/boot.log
  - /var/log/lastlog
  - /var/log/mail.err|info|warn
  - /var/log/messages-20080113.bz2

Die Protokolldateien

- Die meisten Logdateien können im Textmode mit *cat*, *less* oder *tail* angeschaut werden
- Es existieren auch spezielle Programme zum beobachten von Logdateien
  - logsurfer
  - xlogmaster

Die Protokolldateien

- Die Protokolldateien können ziemlich schnell ziemlich gross werden
- Der *syslogd* schreibt kontinuierlich in die vorgegebenen Dateien
- Die Dateien können zur Laufzeit gelöscht oder umbenannt werden
- Danach muss dem *syslogd* das Signal *SIGHUP* geschickt werden

Das Programm *logrotate*

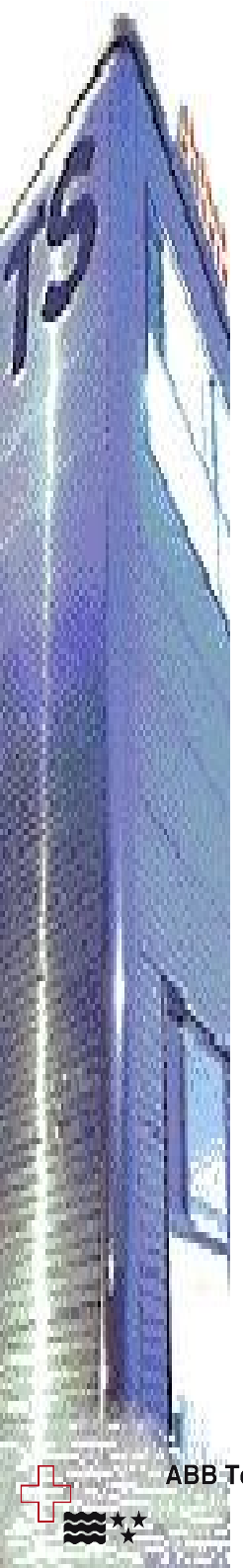
- *Logrotate* überwacht Protokolldateien regelmässig nach verschiedenen Kriterien
  - Grösse
  - Alter
- Die Konfiguration ist in */etc/logrotate.conf*
- In */etc/logrotate.d* können die Aktionen beschrieben werden
- *Logrotate* ist kein Daemon, sondern wird von *cron* regelmässig gestartet

Das Programm *logrotate*

- Als Beispiel ein Ausschnitt aus der Konfigurationsdatei von *fetchmail*

`/etc/logrotate.d/fetchmail`

```
/var/log/fetchmail {
    compress
    dateext
    maxage 365
    rotate 99
    size 1024k
    notifempty
}
```



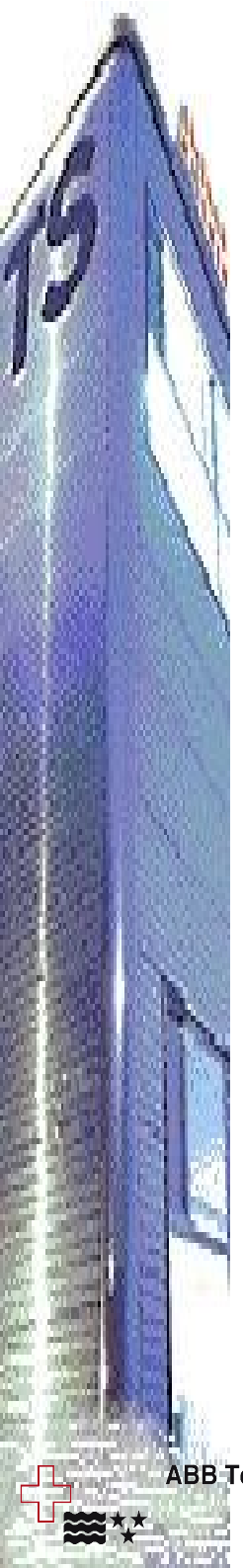
Übungen

- [8.4] Konfigurieren Sie logrotate so, dass Ihre neue Protokolldatei /var/log/test rotiert wird, sobald sie eine Grösse von 100 Byte überschreitet.
- Es sollen 10 Backups der rotierten Dateien aufgehoben werden, ausserdem sollen diese Backups komprimiert werden und einen Namen tragen, der das Datum ihrer Erstellung enthält.

Protokoll des Systemkerns

- Der Kernel schickt seine Nachrichten nicht an den *syslogd*
- Er stellt sie in einen internen Ringpuffer
- Der Prozess *klogd* liest die Meldungen über die Datei */proc/kmsg* und schickt sie an *syslogd*
- Zur Ausgabe des Ringpuffer verwendet man das Kommando
  - `dmesg`

Fragen?



Übungen

- [8.5] Was verrät die Ausgabe von *dmesg* Ihnen über die Hardware in Ihrem Rechner?