Gängige Befehle

```
ls -lrt /var/log
tail -F /var/log/messages
less /var/log/messages
grep Testmeldung /var/log/*
```

Falls vorhanden:

```
multitail /var/log/messages
```

syslog

siehe syslog

logrotate

siehe logrotate

logs auswerten

Debian:

```
logcheck
```

openSuSE (13.1):

```
logdigest
logwatch
```

CentOS (ab 5):

```
logwatch
```

Log Analyse Software

- http://logstash.net/
- https://www.graylog.org/
- https://www.fluentd.org/

- http://loganalyzer.adiscon.com
- http://www.uberadmin.com/Projects/logtemplater/
- http://www.splunk.com (proprietär)
- http://www.octopussy.pm

[1)]

Log Analyse Konzepte

- Artificial Ignorance http://www.ranum.com/security/computer_security/papers/ai/index.html

User Logging

paket psacct installieren.

Log aktivieren

```
touch acct.log
accton acct.log
```

Log deaktivieren

```
accton
```

Logs auswerten

```
sa -a acct.log
lastcomm -f acct.log --user nutzer14
```

[1)]
Für Centos 6 benötigte Perl-Pakete:

```
perl-Apache-ASP
perl-App-Info
perl-Cache-Cache
perl-Crypt-PasswdMD5
perl-Date-Manip
perl-JSON
perl-List-MoreUtils
perl-Locale-Maketext-Lexicon
perl-Locale-Maketext-Simple
perl-Mail-Sender
perl-LDAP
perl-Net-SCP
perl-Net-Telnet
perl-Net-XMPP
perl-Proc-PID_File
perl-Proc-ProcessTable
```

```
perl-Readonly
perl-Regexp-Assemble
perl-Term-ProgressBar
perl-Unix-Syslog
perl-URI
perl-version
perl-XML-Simple
```

```
xargs yum install -y
```

while Schleife:

```
cat datei | while read line; do yum install -y $line; done
```