edeserver - Ubuntu 8.04.2 i386 Server @ Mini-ITX

Stefan Edenhofer
29.06.2009

Inhalt

Konfigurations-Anforderungen

- Beim SSH-Login soll die Möglichkeit bestehen, installierte X11-Applikationen mit
  X11-Forwarding durch den SSH-Tunnel zu starten.

- Da meistens kein Bildschirm am Server vorhanden ist, soll die aktuelle IP Adresse
  (z.B. bei DHCP) über eine Text-to-Speech Engine über die Soundkarte ausgegeben werden.

- Kleiner Datei-Server mit Zugriff über SSH, NFS, FTP, TFTP, SMB und HTTP(S)
  auf die HOME- und andere Verzeichnisse inkl. User-Quota und Papierkorb bei SMB.

- Ein(1) User-Management für die bereitgestellten, lokale Dienste wie
  SSH, NFS, FTP, SMB(!) und SQUID(!). Zusätzlich auch zentrale Benutzerverwaltung
  für Windows- und Linux-Clients, also Domänen-Kontroller (PDC) und NIS-Server.

- Redundanz der Daten über LVM und RAID 1 (Spiegelung).

- Netzwerk-Funktionen wie
  Web-Proxy (+Auth), DHCP-, (Dyn)DNS- und VPN-Server (mit unverschlüsseltem IP-Tunnel,
  mit OpenVPN und mit IPSec), Router, DSL-Router, Syslog-Server, TFTP-Server,
  VLAN-Tagging IEEE 802.1q.

- Büro-Funktionen wie
  Print Server, Fax Server, Email Server, VoIP Server, IM Server

- Webseite mit Status-Anzeige

Hardware und Bestellung

- Mainboard: Jetway J7F4K1G5D, Mini-ITX, 1500 MHz, CPU Via C7 1,5GHz FSB 133MHz 25W
  Grafik: S3 UniCrome Pro 3D 128bit, Audio: 6 Kanal Audio, 1 PCI, 1 ATA, 2 S-ATA
  Raid /8x USB 2.0, 2x LAN Gigabit Ethernet, 2xSeriell 1/1, 1xParallel, 1x DDR II 400/533 bis 1GB
  126,39 Euro, http://www.hrt.de

- Gehäuse: Morex Cubid 2688V schwarz (BxTxH (mm):295 x 272 x 63,5) mit
  Front Ports 2x USB, Platz für 1x HDD 3,5", 1x CD/DVD Slim Type, 1x FDD Slim Type, 1x PCI Slot,
  Gehäuse-Spannungsversorgung: 12V (Spannungswandlerplatine im Gehäuse),
  externes Netzteil: Eingang ~100-240V 50-60Hz, Ausgang 12-14V=
  80,- Euro, http://www.hrt.de

- RAM: Kingston KVR533D2N4/512, Typ: 512 MB DDR II, Speichertakt: PC4200 533 MHz, Latency: CL 4

58,19 Euro, http://www.kkcomputer.de

- 12V-Ventilator, der über der CPU sehr leise auf 7V (über "Peripheral Power" rot und gelb) läuft.
  Die 2 kleinen Lüfter des Gehäuses und der 1 CPU-Ventilator sind ausgesteckt.

- SEHR LEISE (!) Festplatte: MHW2080AT - 2,5" Fujitsu Hornet V80 80GB, ATA, 4200rpm, Cache 2 MB
  57,- Euro, http://www.bg-edv.de

- IDE-Adapter 2,5" HD auf 3,5" ATAPI 50pol auf 68pol
  4,- Euro, http://www.bg-edv.de

- CD-ROM-Laufwerk, Bildschirm und Tastatur temporär während der anfänglichen Installationphase

(- USB Drive: Verbatim Hi-Speed USWB 2.0 Store'n'Go 1 GB
  23,99 Euro, http://www.mediamarkt.de)

(- Morex JM139, PCI Riser Card
  13,- Euro, http://www.hrt.de)

(-1 x Versandskosten http://www.hrt.de mit UPS für 7,90 Euro)

BIOS Anpassung

Für Booten von USB:
Im BIOS muss im Menü "Integrated Peripherals" - "OnChip Device Function"
der Parameter "USB Device Legacy Support" auf "All On" sein, um von USB zu booten.

Um vom Stick bei vorhandener Festplatte zu booten:
"Advanced BIOS Features" - "Hard Disk Boot Priority" und "First/Second/Third Boot Device"
(CDROM, Hard Disk, USB-ZIP?)

Um ohne lokaler Tastatur booten zu können:
"Standard CMOS Features" - Parameter "Halt On" von "All Errors" => "All, But Keyboard"

Installation

Betriebssystem (Dauer: ca. 1/2 Stunde)

Mit temporär angeschlossener Tastatur, Bildschirm und CD-ROM Laufwerk am ATA Anschluß

Boot-CD mit Image "ubuntu-7.10-server-i386.iso"
(damals 7.10; nach (Dist.-)Upgrades inzwischen Ubuntu 8.04.2)
- F3 Keymap: Germany
- Language : English
- Location : other - Germany
- Hostname : edeserver
- Netzwerk-Konfiguration eth0: 10.0.0.2, Netmask 255.255.255.0,
  Defaultrouter: 10.0.0.1, DNS-Server: 10.0.0.1
  (Netzwerkkarte wird inzwischen erkannt - im Gegensatz zu Ubuntu 6.10 Server)
- Partitionierung manuell: - 4,0 GB / ext3 journaling
  - 1,0 GB swap swap (beim USB Drive ohne swap-Partition)
  - 75,0 GB /home ext3 journaling (separat wegen quota)
- System Clock to UTC
- Anlegen des ersten Benutzers
  (Warten, da bei ca. 83% die Basisresourcen neu generiert werden; ...und das dauert...)
- Keine Software (DNS, LAMP, Mail, OpenSSH, PostgreSQL, Print und Samba File Server,
  ich will's langsam)

  (Network Mirrors, Universe, Restricted und Backports benutzen)
  (Proxy Einstellung für apt (bei mir kein Proxy nötig))

sudo passwd root
Anmeldung als root

Basis-System (Dauer: ca. 10 Minuten)

Weitere Vorbereitung, um Remote und ohne CD-Laufwerk, lokaler Tastatur und
lokalem Bildschirm zu arbeiten:

cp /etc/apt/sources.list /etc/apt/sources.list.ORIG
nano /etc/apt/sources.list (CD als Quelle entfernt, auskommentierte Quellen aktiviert)
apt-get update
apt-get upgrade
apt-get dist-upgrade

apt-get install openssh-server

halt

Entferne temporäre Geräte (CD-ROM-Laufwerk, Bildschirm und Tastatur) und starte neu.

Neustart - Login als root

/etc/apt/sources.list

/etc/ssh/sshd_config
/root/.ssh/authorized_keys
/etc/init.d/ssh restart

/root/.bashrc

Anwendungs-Installation

Manuell zu installierende Anwendungen ("apt-get install <name>" und alles mit "Y" bestätigt):

Lokale Administration
openssh-server xauth nictools-pci espeak hdparm

Zugriff
ntp-server quota quotatool bind9 dhcp3-server samba smbfs smbclient libpam-smbpass
apache2 vsftpd squid xinetd tftpd tftp nfs-kernel-server cupsys cupsys-client
openvpn ejabberd

Analyse
traceroute iptraf nmap wireshark tcpdump

Sonst
mpg123 wcalc msmtp mutt centericq minicom lm-sensors putty-tools

Nach der Installation
Heruntergeladene Archiv-Dateien entfernen mit:
apt-get clean; apt-get autoclean; apt-get autoremove

Konfiguration

Manuell veränderte bzw. erzeugte Dateien:

Netzwerk/System
- /etc/network/interfaces

```
auto lo eth0
iface lo inet loopback

iface eth0 inet static
        address 10.0.0.2
        netmask 255.255.255.0
        network 10.0.0.0
        broadcast 10.0.0.255
        gateway 10.0.0.1
        dns-nameservers 10.0.0.2
```

- /etc/resolv.conf

```
domain geiz
search geiz
nameserver 10.0.0.2
```

- /etc/apt/sources.list

```
# deb cdrom:[Ubuntu-Server 7.10 _Gutsy Gibbon_ - Release i386 (20071016)]/ gutsy main restricted

# deb cdrom:[Ubuntu-Server 7.10 _Gutsy Gibbon_ - Release i386 (20071016)]/ gutsy main restricted

deb http://de.archive.ubuntu.com/ubuntu/ hardy main restricted
deb-src http://de.archive.ubuntu.com/ubuntu/ hardy main restricted

deb http://de.archive.ubuntu.com/ubuntu/ hardy-updates main restricted
deb-src http://de.archive.ubuntu.com/ubuntu/ hardy-updates main restricted

deb http://de.archive.ubuntu.com/ubuntu/ hardy universe
deb-src http://de.archive.ubuntu.com/ubuntu/ hardy universe
deb http://de.archive.ubuntu.com/ubuntu/ hardy-updates universe
deb-src http://de.archive.ubuntu.com/ubuntu/ hardy-updates universe

deb http://de.archive.ubuntu.com/ubuntu/ hardy multiverse
deb-src http://de.archive.ubuntu.com/ubuntu/ hardy multiverse
deb http://de.archive.ubuntu.com/ubuntu/ hardy-updates multiverse
deb-src http://de.archive.ubuntu.com/ubuntu/ hardy-updates multiverse

deb http://de.archive.ubuntu.com/ubuntu/ hardy-backports main restricted universe multiverse
deb-src http://de.archive.ubuntu.com/ubuntu/ hardy-backports main restricted universe multiverse

deb http://archive.canonical.com/ubuntu hardy partner
deb-src http://archive.canonical.com/ubuntu hardy partner

deb http://security.ubuntu.com/ubuntu hardy-security main restricted
deb-src http://security.ubuntu.com/ubuntu hardy-security main restricted
deb http://security.ubuntu.com/ubuntu hardy-security universe
deb-src http://security.ubuntu.com/ubuntu hardy-security universe
deb http://security.ubuntu.com/ubuntu hardy-security multiverse
deb-src http://security.ubuntu.com/ubuntu hardy-security multiverse
```

Firewall und Traffic Control
- /firewall
  Inkusive Traffic-Control fuer https-Pakete
  => chmod 555 /firewall
  => ln -s /firewall /etc/rcS.d/S39firewall

```
#!/bin/sh

TRUSTED="10.0.0.0/23"

fw_enable(){
  echo "Starting Firewall..."

  iptables -A INPUT -i lo -j ACCEPT
  iptables -A OUTPUT -o lo -j ACCEPT

  ### INPUT:
  iptables -A INPUT -p tcp --dport 22 -s $TRUSTED -j ACCEPT -m comment --comment "SSH"
  iptables -A INPUT -p tcp --dport 22 -m limit --limit 4/m -j ACCEPT -m comment --comment "SSH(limit)"
```

```
iptables -A INPUT -p icmp --icmp-type echo-request -s $TRUSTED -j ACCEPT -m comment --comment "ICMP"
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT -m comment --comment "ICMP(limit)"

iptables -A INPUT -p tcp --dport 21 -s $TRUSTED -j ACCEPT -m comment --comment "FTP(mode1=pass)"
iptables -A INPUT -p tcp --dport 60000:60199 -s $TRUSTED -j ACCEPT -m comment --comment "FTP(mode1=pass)"

iptables -A INPUT -p tcp --dport 53 -s $TRUSTED -j ACCEPT -m comment --comment "DNS"
iptables -A INPUT -p udp --dport 53 -s $TRUSTED -j ACCEPT -m comment --comment "DNS"

iptables -A INPUT -p udp --dport 67 --sport 68 -j ACCEPT -m comment --comment "DHCP"

#iptables -A INPUT -p udp --dport 69 -s $TRUSTED -j ACCEPT -m comment --comment "TFTP"

iptables -A INPUT -p tcp --dport 80 -s $TRUSTED -j ACCEPT -m comment --comment "HTTP"
iptables -A INPUT -p tcp --dport 443 -j ACCEPT -m comment --comment "HTTPS"

iptables -A INPUT -p udp --dport 123 -s $TRUSTED -j ACCEPT -m comment --comment "NTP"

iptables -A INPUT -p tcp --dport 139 -s $TRUSTED -j ACCEPT -m comment --comment "SMB"
#iptables -A INPUT -p udp --dport 137 -s $TRUSTED -j ACCEPT -m comment --comment "SMB"

iptables -A INPUT -p udp --dport 514 -s $TRUSTED -j ACCEPT -m comment --comment "SYSLOG"

iptables -A INPUT -p tcp --dport 631 -s $TRUSTED -j ACCEPT -m comment --comment "CUPS"

iptables -A INPUT -p tcp --dport 5222 -j ACCEPT -m comment --comment "JABBER"
iptables -A INPUT -p tcp --dport 5280 -s $TRUSTED -j ACCEPT -m comment --comment "JABBER-Admin"

iptables -A INPUT -p udp --dport 51194 -j ACCEPT -m comment --comment "OVPN"
iptables -A FORWARD -i tap+ -j ACCEPT -m comment --comment "FWD TAP all"
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT -m comment --comment "FWD allow answers"

iptables -A INPUT -p tcp --dport 111 -s $TRUSTED -j ACCEPT -m comment --comment "NFS"
iptables -A INPUT -p udp --dport 111 -s $TRUSTED -j ACCEPT -m comment --comment "NFS"
iptables -A INPUT -p tcp --dport 671 -s $TRUSTED -j ACCEPT -m comment --comment "NFS"
iptables -A INPUT -p tcp --dport 2049 -s $TRUSTED -j ACCEPT -m comment --comment "NFS"
iptables -A INPUT -p udp --dport 2049 -s $TRUSTED -j ACCEPT -m comment --comment "NFS"
iptables -A INPUT -p udp --dport 32772 -s $TRUSTED -j ACCEPT -m comment --comment "NFS"

iptables -A INPUT -p tcp --dport 3128 -s $TRUSTED -j ACCEPT -m comment --comment "SQUID"

iptables -A INPUT -p tcp --dport 18767 -s $TRUSTED -j ACCEPT -m comment --comment "netio"
iptables -A INPUT -p udp --dport 18767 -s $TRUSTED -j ACCEPT -m comment --comment "netio"

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT -m comment --comment "EST/REL"

iptables -A INPUT -p icmp --icmp-type echo-request -j LOG --log-prefix "Zuviel ICMP Request => DROP "
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "Zuviel SSH => DROP "
iptables -A INPUT -p tcp --dport 22 -j DROP

# Typische Windows-Broadcasts:
iptables -A INPUT -p tcp --dport 445 -j REJECT
iptables -A INPUT -p udp --dport 138 --sport 138 -j DROP
iptables -A INPUT -p udp --dport 137 --sport 137 -d 10.0.0.255 -j DROP

### ROUTING:
#iptables -A FORWARD -p icmp -s $TRUSTED -j ACCEPT
#iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
#iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward

### ABSCHLUSS:
iptables -A INPUT -j LOG --log-prefix "INPUT-DROP "
iptables -A FORWARD -j LOG --log-prefix "FORWARD-DROP "

iptables -A INPUT -j DROP
iptables -A FORWARD -j DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP

  ### Frueher in /etc/network/options:
  ## spoofprotect (alter Defaultwert = 1):
  # for f in /proc/sys/net/ipv4/conf/*/rp_filter; do
  # echo 1 > $f
  # done
  ## syncookies (alter Defaultwert = 0):
  # echo 1 > /proc/sys/net/ipv4/tcp_syncookies
  ## ip_forward (alter Defaultwert = 0, siehe oben):
}

fw_disable() {
  echo 0 > /proc/sys/net/ipv4/ip_forward
  iptables -P INPUT ACCEPT
  iptables -P FORWARD ACCEPT
  iptables -P OUTPUT ACCEPT
  iptables -F; iptables -X
  iptables -t nat -F; iptables -t nat -X
  iptables -t mangle -F; iptables -t mangle -X
}

fw_status(){
  echo "FILTER INPUT:"
  iptables -t filter -nvL INPUT
  iptables -t filter -nvL FORWARD
}

qos_disable() {
  # if not "qdisc pfifo_fast 0:" in "tc -s qdisc show dev eth0"
  tc qdisc del dev eth0 root
}

qos_enable() {
```

```
  tc qdisc add dev eth0 root handle 1: htb default 10
  tc class add dev eth0 parent 1: classid 1:1 htb rate 120kbit ceil 120kbit
  tc class add dev eth0 parent 1:1 classid 1:10 htb rate 120kbit ceil 120kbit prio 1
  tc class add dev eth0 parent 1:1 classid 1:20 htb rate 50kbit ceil 80kbit prio 2
  tc qdisc add dev eth0 parent 1:10 handle 10: sfq perturb 10
  tc qdisc add dev eth0 parent 1:20 handle 20: sfq perturb 10
  tc filter add dev eth0 protocol ip parent 1: prio 1 handle 6 fw flowid 1:20
  # Markiere Antworten auf https-Anfragen (tcp/443) fuer :
  iptables -t mangle -A OUTPUT -o eth0 -p tcp --sport 443 -j MARK --set-mark 6
}

qos_status() {
  echo "\nMANGLE OUTPUT:"
  iptables -t mangle -nvL OUTPUT
  echo "\nTraffic-Control:"
  #tc -s class show dev eth0
  tc -s qdisc show dev eth0
  #tc -s filter show dev eth0
}

case "$1" in
  stop)
    echo "Stopping Firewall..."
    fw_disable
    qos_disable
    exit 0
    ;;
  status)
    fw_status
    qos_status
    exit 0
    ;;
  fastadd)
    echo e.g. iptables -I INPUT 1 -p tcp --dport 100 -j ACCEPT
    exit 0
    ;;
  reload)
    fw_disable
    fw_enable
    exit 0
    ;;
  --help)
    echo "$0 {start|stop|status|reload}"
    exit 0
    ;;
  *)
    qos_disable
    fw_disable
# qos_enable
    fw_enable
    exit 0
    ;;
esac

exit 0
```

- /etc/fstab

```
# /etc/fstab: static file system information.
#
# <file system> <mount point> <type> <options> <dump> <pass>
proc /proc proc defaults 0 0
# /dev/hda1
UUID=f0e340ba-e36e-4586-bcb4-a600d845757a / ext3 defaults,errors=remount-ro 0 1
# /dev/hda3
UUID=769117a8-5b5d-4602-bcfe-52fb43771c45 /home ext3 defaults,usrquota 0 2
# /dev/hda2
UUID=00430a87-ff9c-4fcb-acd6-4a09f373a9ec none swap sw 0 0
/dev/hdb /media/cdrom0 udf,iso9660 user,noauto,exec 0 0
```

SSH-Server

apt-get install openssh-server

runlevel: /etc/init.d/ssh, /etc/rc[2345].d/S20ssh, /etc/rc1.d/K20ssh

- /root/.ssh/authorized_keys

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAiG9131SVapP7FHPiZAbT2XdQ4UxXdcW+GsLvqmyltN1cI/PFID
/MCpXSyPk0jajT1YNbklF9hFALlNEsNye5TTUNUxasu4P+aQ2UdVLUmDgjSX1e2m2n/wvRTgOCmQC/DVRJ6eX2VGs4yk
/CEhyqf8ukWk2XTuGb+A168MuXUh6iapMfk0d1mKBRqOzIHCU8bu/+paMXtfMY9LCDESW0XYnK/XPommSanrxzYeSh9jyN2+fh/b9LwNYGrbE0WS4qHrsvYQWjDG9H
/jwTESzRqYmX8IigRfSMDXWhbT1krP0d3yIO5+SGBp+3oC/JNwCt/BQBGPq50qYkTHi2NaWWuQ== E.de
```

- /etc/ssh/sshd_config

```
Protocol 2
RhostsRSAAuthentication yes
PasswordAuthentication no
ChallengeResponseAuthentication no
AllowTcpForwarding yes
X11Forwarding yes
UsePrivilegeSeparation no
Subsystem sftp /usr/lib/ssh/sftp-server

Port 22
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
SyslogFacility AUTH
LogLevel INFO
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
IgnoreRhosts yes
PermitEmptyPasswords no
X11DisplayOffset 10
```

```
PrintLastLog yes
TCPKeepAlive yes
AcceptEnv LANG LC_*
PrintMotd no
UsePAM yes
```

=> /etc/init.d/ssh restart

Meine Shell-Einstellungen/-Erweiterungen

- /root/.bashrc

```
[...]
PS1='\u@\h:\w\$ '
alias ls="ls --color=auto"
alias ll="ls -Fal"
alias nano="nano -S"
```

- /cat_no_com

```
sed -r '/^\s*(#.*|)$/d' $1
```

- /home/www/e-doku.pl

```
#!/usr/bin/perl
use strict;
use POSIX qw( strftime );
use CGI::Carp qw(fatalsToBrowser);


# available tags for inputfile: #include, #title, #headsum, #head[123], #right, ### Kommentarzeile
# #bold ... bold#, #small ... small#, #today
# available tags in include file: ### e-doku START, ### e-doku STOP

my ($input, $docwidth) = ("", 80);
$0 =~ m/^(.*?)(\.[^.\\\/]+)?$/;
open CONF, $1.".conf"; #with:
#input <filename with detail informations>
#width <width of textfile output in characters>
while(<CONF>)
{ if ( $_ =~ m/^input\t+(.+)$/ ){ $input = $1; }
  elsif( $_ =~ m/^width\t+(\d+)$/ ){ $docwidth = $1; }
}
close CONF;

my ($typ, $web, $cli) = (0,1,2);
my $OUT = \*STDOUT; my $dok = ""; my $content = "";
my $error = "";
my $contenttype = "content-type: text/html\n";
if ( exists $ENV{REMOTE_ADDR} ) { $typ = $web; }
elsif( exists $ENV{OS} ) { $typ = $cli; } # Windows
elsif( exists $ENV{SHELL} ) { $typ = $cli; } # Linux
if( exists $ARGV[0] )
{ $OUT = \*OUTPUT; open OUTPUT, ">$ARGV[0]";
  if( $ARGV[0] =~ m/(\.html|\.htm)$/ ) { $typ = $web; $contenttype = ""; }
}

if( ! -e $input ){ print $contenttype."\n" if($typ==$web); print "Config \"$input\" not found :-(\n"; exit; }

&htmlhead if( $typ == $web);

open INPUT, "<$input";
while(<INPUT>)
{
  next if( $_ =~ m/^###/ );
  if( $typ == $web) { $_ =~ s/</</g; $_ =~ s/>/>/g; }
  $_ =~ s/^#include (.+)$/include($1)/eg;
  $_ =~ s/^#title (.+)$/head(0,$1)/eg;
  $_ =~ s/^#head1 (.+)$/head(1,$1)/eg;
  $_ =~ s/^#head2 (.+)$/head(2,$1)/eg;
  $_ =~ s/^#head3 (.+)$/head(3,$1)/eg;
  $_ =~ s/#small (.+) small#/small($1)/eg;
  $_ =~ s/#bold (.+) bold#/bold($1)/eg;
  $_ =~ s/#today/strftime "%d.%m.%Y", localtime/eg;
  $_ =~ s/^#right (.+)$/right($1)/eg;
  $_ =~ s/^#incl_nochange (.+)$/include($1)/eg;

  if( $typ == $web)
  {
    $_ =~ s/\t/ /g;
    $_ =~ s/&/&amp;/g; $_ =~ s/&amp;([gl]t);/&$1;/g;
    $_ =~ s/^( +)/spaces($1)/egm;
    $_ =~ s/\n/\n<br>/g;
    $_ =~ s/ß/&szlig;/g; $_ =~ s/([äöüÄÖÜ])/&$1uml;/g; $_ =~ tr/äöüÄÖÜ/aouAOU/;
  }

  $_ =~ s/psk="hiddenpassword"
  $_ =~ s/(wireless-key.*) \w+$/$1 hiddenpasswordinhex/gm;

  $dok = $dok.$_;
}
close INPUT;

$dok =~ s/<br>#headsum/$content/gm;
print $OUT $dok;

print $error;
&htmlfoot if( $typ == $web);
close OUTPUT;
exit;
# ------------

sub include { my ($file) = @_;
```

```
  my @border; my @starter;
  $border[$cli] = "+----------";
  $starter[$cli] = "\n| ";
  $border[$web] = "";
  $starter[$web] = "\n";
  open FILE, "<$file" or $error = $error."\n(*) \"$file\" not found.";
  my @file = <FILE>;
  close FILE;
  chomp @file;
  my @newfile = ();
  foreach(@file)
  {
    if( $_ =~ m/^### e-doku START$/ ) { @newfile = (); push @newfile, "[...]"; next; }
    if( $_ =~ m/^### e-doku STOP$/ ) { push @newfile, "[...]"; last; }
    push @newfile, $_;
  }
  my $content = join("$starter[$typ]", @newfile);
  if( $typ == $web) { $content =~ s/</</g; $content =~ s/>/>/g; }
  my $return = $border[$typ].$starter[$typ].$content."\n".$border[$typ];
  if( $typ == $web) {
    $return =~ s/^\n//;
    $return = "<table width=\"100%\"><tr><td class=\"file\">".$return."</td></tr></table>";
  }
  #print "HERE:".$return;
  return $return;
}

sub head { my ($layer, $text) = @_;
  if ( $typ == $web )
  {
    if($layer == 0) { $text = "<font class=\"title\">".$text."</font>"; }
    if($layer == 1) { $content = $content."\n<br>".$text; $text = "<font class=\"head1\">".$text."</font>"; }
    if($layer == 2) { $content = $content."\n<br>   ".$text; $text = "<font class=\"head2\">".$text."</font>"; }
    if($layer == 3) { $content = $content."\n<br>      ".$text; $text = "<font class=\"head3\">".$text."
</font>"; }
  }
  elsif ( $typ == $cli )
  {
    $content = $content."\n"." "x($layer-1).$text if($layer>0);
    $text = $text."\n"."-"x(length($text));
  }
  return $text;
}

sub small { my ($text) = @_;
  $text = "<font class=\"small\">".$text."</font>" if ( $typ == $web );
  return $text;
}

sub bold { my ($text) = @_;
  $text = "<b>".$text."</b>" if ( $typ == $web );
  return $text;
}

sub right { my ($text) = @_;
  if ( $typ == $cli ){ $text = " "x($docwidth-length($text)).$text; }
  elsif( $typ == $web ){ $text = "<div class=\"right\">".$text."</div>"; }
}

sub spaces { my ($text) = @_; return " "x(length($text)); }

#content-type: text/html\n\n
sub htmlhead { print $OUT "$contenttype
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>e-doku</title>
  <style type=\"text/css\"> <!--
    .normal { color: #000000; font-size: 10pt; }
    .file { font-family: \"lucida console\", courier, monospace;
            color: #000088; background: #EEEEEE; font-size: 9pt; }
    .title { color: #000000; font-weight: bold; text-align: center; font-size: 16pt; }
    .head1 { color: #DD0000; font-weight: bold; font-size: 12pt; }
    .head2 { color: #0000DD; font-weight: bold; font-size: 10pt; }
    .head3 { color: #000000; font-weight: bold; font-size: 10pt; }
    .small { color: #000000; font-size: 8pt; }
    .right { text-align: right; line-height: 0pt; }
  --> </style>
</head>
<body class=\"normal\">
";
}

sub htmlfoot { print $OUT "\n</body>\n</html>\n"; }
```

IP-Checker

apt-get install nictools-pci espeak

- /ip-tts

=> chmod 555 /ip-tts

=> ln -s /ip-tts /etc/rc2.d/S85ip-tts

```
#!/usr/bin/perl
use strict;
$| = 1;

# Skript zum Ausgeben der neuen bzw. veraenderten IP Adresse ueber Text-to-Speech
# Voraussetzungen: TTS-Engine "festival" oder "espeak"
# und Realtek-Tool "rtl8139-diag" in nictools-pci
# Benutzung:
# - In Runlevel 2 einfuegen (wird so mit Argument "start" aufgerufen)
```

```
# - In Runlevel 0 und 6 einfuegen (wird so mit Argument "stop" aufgerufen)

my $ITF = "eth0";
my $TMPFILE = "/tmp/ip-tts-ip-addr";
my $PIDFILE = "/tmp/ip-tts-pid";
my $NOLINK = "no-link";
my $SPK = "/usr/bin/espeak -v de";

if( $ARGV[0] eq "start" ) {
  exec "$0 daemon &"; exit 0; }
elsif( $ARGV[0] eq "stop" ) {
  open PID, "<$PIDFILE"; my $PID = <PID>; close PID;
  system "kill $PID"; system "rm $PIDFILE"; system "rm $TMPFILE"; exit 0; }
elsif( $ARGV[0] eq "daemon" ) {
  if( -e $PIDFILE ) { die "Daemon lauft schon! (PID-file <$PIDFILE> existiert.)"; }
  open PID, ">$PIDFILE"; print PID $$; close PID;
  &noip(); }

while(1)
{ my $IFC = qx "/sbin/ifconfig $ITF";
  $IFC =~ m/HWaddr (\S+)/; my $MAC = lc($1);
  my @ret = qx "rtl8139-diag -m"; chomp @ret;
  my $mycard=0;
  foreach my $line (@ret)
  {
    $mycard = 1 if( $line =~ m/$MAC/ );
    next if( $mycard == 0 );
    if( $line =~ m/Disconnects.*0x006b/ ) { $mycard = "UP" ; last; }
    if( $line =~ m/Disconnects.*0x0026/ ) { $mycard = "UP" ; last; }
    if( $line =~ m/Disconnects.*0x0004/ ) { $mycard = "DOWN"; last; }
  }
  if( $mycard eq "UP" )
  { $IFC =~ m/inet addr:([0-9.]+)/; my $NowIP = $1;
    open TMP, "<$TMPFILE"; my $OldIP = <TMP>; close TMP;
    if( $NowIP ne $OldIP )
    { &speak($NowIP); open TMP, ">$TMPFILE"; print TMP $NowIP; close TMP; }
  }
  elsif( $mycard eq "DOWN" )
  { open TMP, "<$TMPFILE"; my $OldIP = <TMP>; close TMP;
    if( $OldIP ne $NOLINK )
    { &speak("Keine Verbindung"); &noip(); }
  }
  sleep 15;
}

sub noip { open TMP, ">$TMPFILE"; print TMP $NOLINK; close TMP; }

sub speak { my $string = $_[0]; $string =~ s/\./ /g; system "$SPK '$string'"; } # system "echo $_[0] | festival --tts";
```

NTP-Server

apt-get install ntp-server
runlevel: /etc/init.d/ntp, /etc/rc[2345].d/S23ntp, /etc/rc1.d/K23ntp

- /etc/ntp.conf

```
# http://www.cis.udel.edu/~mills/ntp/html/index.html

server 127.127.1.1
fudge 127.127.1.1 stratum 12

# Use specific NTP servers
server 0.de.pool.ntp.org
server 1.de.pool.ntp.org
#server 10.0.0.2 iburst

tinker panic 0

logconfig all
enable stats

driftfile /var/lib/ntp/ntp.drift
logfile /var/log/ntpstats/ntp.log
statsdir /var/log/ntpstats/

#genereate logfiles
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

# disable monitoring feature
disable monitor
```

DNS-Server

apt-get install bind9
runlevel: /etc/init.d/bind9, /etc/rc[2345].d/S15bind9, /etc/rc[016].d/K85bind9
=> chmod 775 /etc/bind (nötig für dhcpd-Update; drwxr-sr-x -> drwxrwxr-x)
=> /etc/init.d/bind9 stop

- /etc/bind/named.conf (mit Key aus rndc.key)

```
#### /etc/bind/named.conf
# apt-get install bind9
# /etc/init.d/bind9 restart
# DNS-Client: /etc/resolv.conf: search geiz, nameserver 10.0.0.2
##### rndc
# dnssec-keygen -a hmac-md5 -b 128 -n HOST myzone
# creates 2 files; use the content of the files.
```

```
## /etc/bind/rndc.conf:
# key "rndc-key" { algorithm hmac-md5; secret "OqwFG5zOXqeYKWvN5emirw=="; };
# options { default-key "rndc-key"; default-server 127.0.0.1; default-port 953; };
## rndc reload
#### DDNS:
# In den Zonen hinzufuegen: allow-update { key rndc-key; };
# chmod 775 /etc/bind
####

options {
  directory "/var/cache/bind"; auth-nxdomain no; allow-recursion { localnets; };
  forwarders { 10.0.0.1; }; /* Fuer Win32: */ # pid-file none;
};

key "rndc-key" { algorithm hmac-md5; secret "OqwFG5zOXqeYKWvN5emirw=="; };
controls { inet 127.0.0.1 port 953 allow { 127.0.0.1; } keys { "rndc-key"; }; };

zone "." { type hint; file "/etc/bind/db.root"; };
zone "localhost" { type master; file "/etc/bind/db.local"; };
zone "127.in-addr.arpa" { type master; file "/etc/bind/db.127"; };
zone "0.in-addr.arpa" { type master; file "/etc/bind/db.0"; };
zone "255.in-addr.arpa" { type master; file "/etc/bind/db.255"; };

zone "geiz" { type master; file "/etc/bind/geiz.fw"; allow-update { key rndc-key; }; };
zone "0.0.10.in-addr.arpa" { type master; file "/etc/bind/geiz.bw"; allow-update { key rndc-key; }; };
zone "edenhofer.homeip.net" { type master; file "/etc/bind/geiz-ext.fw"; };
```

- /etc/bind/rndc.conf (NEU!, Key aus rndc.key)

```
key "rndc-key" { algorithm hmac-md5; secret "OqwFG5zOXqeYKWvN5emirw=="; };
options { default-key "rndc-key"; default-server 127.0.0.1; default-port 953; };
```

- /etc/bind/geiz.bw

```
$ORIGIN .
$TTL 300 ; 5 minutes
0.0.10.in-addr.arpa IN SOA dns.geiz. hostmaster.geiz. (
                               410 ; serial
                               21600 ; refresh (6 hours)
                               3600 ; retry (1 hour)
                               604800 ; expire (1 week)
                               86400 ; minimum (1 day)
                               )
                         NS dns.geiz.
$ORIGIN 0.0.10.in-addr.arpa.
1 PTR gateway.geiz.
10 PTR stefix.geiz.
11 PTR monster.geiz.
2 PTR edeserver.geiz.
$TTL 1800 ; 30 minutes
20 PTR edemobil.geiz.
30 PTR ninamobil.geiz.
```

- /etc/bind/geiz.fw

```
$ORIGIN .
$TTL 300 ; 5 minutes
geiz IN SOA dns.geiz. hostmaster.geiz. (
                               618 ; serial
                               21600 ; refresh (6 hours)
                               3600 ; retry (1 hour)
                               604800 ; expire (1 week)
                               86400 ; minimum (1 day)
                               )
                         NS dns.geiz.
$ORIGIN geiz.
dns CNAME erp
$TTL 1800 ; 30 minutes
edemobil A 10.0.0.20
                         TXT "00e7853a03d13cfd1955b414dfdff6ef7b"
edeserver A 10.0.0.2
erp CNAME edeserver
fw CNAME gateway
gateway A 10.0.0.1
stefix A 10.0.0.10
monster A 10.0.0.11
ninamobil A 10.0.0.30
                         TXT "31962ac3cc84635b44f4490ac50009d2e4"
```

- /etc/bind/geiz-ext.fw

```
$ORIGIN .
$TTL 300 ; 5 minutes
edenhofer.homeip.net IN SOA dns.geiz. hostmaster.geiz. (
                                229 ; serial
                                21600 ; refresh (6 hours)
                                3600 ; retry (1 hour)
                                604800 ; expire (1 week)
                                86400 ; minimum (1 day)
                                )
                         NS dns.geiz.
$ORIGIN homeip.net.
edenhofer A 10.0.0.2
```

- /etc/resolv.conf

```
domain geiz
search geiz
nameserver 10.0.0.2
```

=> /etc/init.d/bind9 start

DHCP-Server mit DDNS

apt-get install dhcp3-server
runlevel: /etc/init.d/dhcp3-server, /etc/rc[2345].d/S40dhcp3-server, /etc/rc1.d/K40dhcp3-server
- /etc/dhcp3/dhcpd.conf
=> /etc/init.d/dhcp3-server restart
(/etc/default/dhcp3-server musste in älterer Version angepasst werden: INTERFACES="eth0")

```
#### /etc/dhcp3/dhcpd.conf
# /etc/default/dhcp3-server: INTERFACES="eth0 eth1"
# iptables -I INPUT 1 -p udp --dport 67 -j ACCEPT
#### DHCP Client:
# send host-name "edemobil";
# request subnet-mask, broadcast-address, routers, ntp-servers,
# domain-name-servers, domain-name, time-offset, host-name;
# timeout 10;
#### DYNAMIC DNS UPDATES:
## ohne DDNS:
#ddns-update-style none;
#ddns-updates off;
## mit DDNS:
# Auf Client-Seite: /etc/dhcp3/dhclient.conf: send host-name "edemobil"; timeout 10;
# ddns-updates on = default;
# key "rndc-key" siehe named.conf (aus dnssec-keygen -a hmac-md5 -b 128 -n HOST myzone)
# host declaration with update-static-leases true;
ddns-update-style interim;
key "rndc-key" { algorithm hmac-md5; secret "OqwFG5zOXqeYKWvN5emirw=="; };
zone geiz. { primary 127.0.0.1; key "rndc-key"; }
zone 0.0.10.in-addr.arpa. { primary 127.0.0.1; key "rndc-key"; }
####

default-lease-time 3600; # 1 Stunde
max-lease-time 14400; # 4 Stunden
authoritative;
log-facility local7;
# ??? one-lease-per-client true;
# ??? option sip code 120 = string;
# ??? option sipproxy code 120 = {unsigned integer 8, array of ip-address};
# ??? (in subnet:) option sip "1 172.16.52.13";
# ??? (in subnet:) option sipproxy 0 9pcsf-stdn4nbg29lucentlab3com0;
# ??? (in subnet:) option sipproxy 1 172.16.52.13;
# ??? option wpad-url code 252 = text;
# ??? option wpad-url "http://192.168.99.123/proxy.pac\n";

subnet 10.0.0.0 netmask 255.255.255.0 {
  range 10.0.0.128 10.0.0.254;
  option subnet-mask 255.255.255.0;
  option broadcast-address 10.0.0.255;
  option routers 10.0.0.1;
  option ntp-servers 10.0.0.2;
  option domain-name-servers 10.0.0.2;
  option domain-name "geiz";
}

host edemobil-wlan { hardware ethernet 00:04:23:74:40:7c; fixed-address 10.0.0.20; update-static-leases true; }
host edemobil-lan { hardware ethernet 00:c0:9f:2b:b3:12; fixed-address 10.0.0.20; update-static-leases true; }

host ninamobil-wlan { hardware ethernet 00:1f:3b:7d:c1:c3; fixed-address 10.0.0.30; update-static-leases true; }
host ninamobil-lan { hardware ethernet 00:1d:72:f5:bb:b1; fixed-address 10.0.0.31; update-static-leases true; }
```

X11-Basis

apt-get install xauth
runlevel: /etc/init.d/x11-common, /etc/rcS.d/S70x11-common

Samba-Server inkl. Papierkorb-Funktion

apt-get install samba smbfs smbclient libpam-smbpass
runlevel:
/etc/init.d/samba, /etc/rc[2345].d/S20samba, /etc/rc[016].d/K19samba
/etc/init.d/cron, /etc/rc[2345].d/S89cron, /etc/rc1.d/K11cron
smbclient -U <USERNAME> //10.0.0.2/shared <PASSWORD> -c "cd SUBDIR; dir *.txt"
- /etc/samba/smb.conf

```
### /etc/samba/smb.conf
# apt-get install samba smbfs smbclient
### Passwort-Abgleich von passwd nach smbpasswd:
# apt-get install libpam-smbpass
## /etc/pam.d/common-password - Zeile hinzufuegen:
# password required pam_smbpass.so use_authtok use_first_pass
### Mounten (apt-get install smbfs)
# mount -t smbfs (-o username=<user>(/<windomain>)(,password=<passwort>)(,uid=1000(,gid=1000))) //10.0.0.10/remotedir /localdir
# //10.0.0.10/remotedir /localdir smbfs rw,username=<user>,password=<mypass> 0 0
### Zeige Freigaben fuer <user> auf <server>
# smbclient -N -L <server>
# smbclient -U <user> -L <server>
### Fuehrt einen Befehl aus:
# smbclient -U <user //<server>/<freigabe> -c <command> (<password>)
### Listet den Inhalt des Verzeichnisses:
# smbclient -U <user> //<server>/<freigabe> -c ls (<password>)
# auch -c "get <remote-datei> (<lokale-datei>)"
# auch -c "put <lokale-datei> (<remote-datei>)"
### Samba-Remote-Konsole:
# smbclient -U <user> //<server>/<freigabe> (<password>)
### Windows speichert Hostnamen der Server unter
# HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions
### Firewall:
# iptables -A INPUT -p tcp --dport 139 -j ACCEPT
# iptables -A INPUT -p tcp --dport 445 -j REJECT
##############################

[global]
```

```
  workgroup = GEIZ
  server string = edeserver
; dns proxy = no
; log file = /var/log/samba/log.%m
; max log size = 1000
; syslog = 0
; panic action = /usr/share/samba/panic-action %d
  security = user
  encrypt passwords = true
  passdb backend = smbpasswd
  smb passwd file = /etc/samba/smbpasswd
  map to guest = bad user
  guest account = nobody
  invalid users = root
  socket options = TCP_NODELAY

########## Papierkorb ########

  vfs object = recycle:repository=.recycle
               recycle:versions=True
               recycle:touch=True
               recycle:keeptree=True
               recycle:exclude=~$*,.~*#,*.tmp,*.temp
               recycle:exclude_dir=temp,tmp,cache

########## Printing ##########

  load printers = yes
  printing = cups
  printcap name = cups

########## Freigaben #########

  ### Defaults:
  # [homes] path = /home/%S
  # available = yes # Freigabe ist aktiviert
  # browseable = yes # Zeigt Freigabe in Liste
  # guest ok = no # Anonyme, unangemeldete Benutzer bleiben draussen
  # writeable = no # <=> read only = yes # Nur lesender Zugriff
  # write list = # Bei read only=yes: Liste, die schreiben darf
  # create mask = 0744 # Bei write*: chmod für neue Dateien
  # directory mask = 0755 # Bei write*: chmod für neue Verzeichnisse

[homes]
  comment = Privat-Verzeichnis
  browseable = no
  ### Methode 1 - Nur der Besitzer darf lesen und schreiben:
  ;valid users = %S
  ;writable = yes
  ### Methode 2 - Besitzer darf schreiben, Gruppe users lesen:
  write list = %S
  read list = @users
  ###
  create mask = 0640
  directory mask = 0750

[www]
  path = /home/www
  comment = GEIZ-Webseite
  write list = @users
  read list = @users
  create mask = 0664
  directory mask = 0775

[shared]
  path = /home/shared
  comment = GEIZ-Gemeinsam
  write list = @users
  read list = @users
  create mask = 0664
  directory mask = 0775

[public]
  path = /home/public
  comment = GEIZ-Public
  guest ok = yes
  writeable = yes
  create mask = 0666
  directory mask = 0777

[printers]
  comment = All Printers
  path = /var/spool/samba
  printable = yes
  browseable = yes
  guest ok = yes
  public = no
  writable = no
  create mode = 0700
  # Zeigt "Bereit" anstatt "Zugriff verweigert":
  use client driver = yes

[print$]
   comment = Printer Drivers
   path = /var/lib/samba/printers
   browseable = yes
   read only = yes
   guest ok = no
```

- /etc/pam.d/common-password

```
password required pam_unix.so nullok obscure md5
password required pam_smbpass.so use_authtok use_first_pass
```

Samba und Squid können auch (wie SSH, FTP, NFS) die Unix-Benutzer mit deren Passwort
aus /etc/passwd und /etc/shadow benutzen (siehe Änderungen in /etc/pam.d/common-password).

!!! Passwort-Änderungen nur über "passwd", da dies dann mit Samba synchronisiert wird.

useradd : -m für create-home, -G für zusätzliche Gruppe, -s für Shell,
-d für anderes Home-Directory
smbpasswd: -a für neuer User, -n für kein Passwort (das wird dann über passwd gesetzt)

Passwort setzen über Skript in Kommandozeile (nur diese, mir bekannte Methode
sendet Update an "smbpasswd"):
pass=<passwort>;(echo $pass;sleep 1;echo $pass)|passwd <user> 2>/dev/null

Anlegen eines Benutzers:
useradd -m -g users -s /bin/bash (-c "Name") (-d /path/to/home) <user>
smbpasswd -an <user>
passwd <user>

Eigenschaften eines Benutzers ändern:
usermod -c "Neuer Name" <user>
usermod -g users <user>
passwd <user>

Löschen eines Benutzers:
smbpasswd -x <user>
userdel -r <user>

Benutzer, die zur geschlossenen Benutzergruppe gehören, sollen in die Gruppe "users",
damit die Gruppen-Zugriffsberechtigung zutrifft.

Datei- und Ordner-Berechtigungen:

Private Ordner und Dateien im Apache:
Ist es beabsichtigt, daß der Apache prinzipiell auf einen privaten Ordner/eine private
Datei zugreifen könnte, da ja z.B. der Ordner mit .htaccess geschützt ist, aber über
das Dateisystem keine Zugriffe von anderen erfolgen können soll, dann:
chmod 751 /home/<user>
chown <user>:www-data <privater-ordner-oder-datei>
chmod 750 <privater-ordner-oder-datei>

Um auf die entsprechenden Gruppen-Verzeichnisse /home/www und /home/shared zugeifen zu können:
chown root:users <gruppenordner>
chmod 775 <gruppenordner>

(Anonymer FTP-Zugang (nicht aktiv):
Der FTP-Ordner für Anonymous Read
chown root:nogroup <ordner>
chmod >=754 <ordner>
Dateien für Anonymous Read
chmod >=004 <download-dateien>
chown ???:??? <download-dateien> (nicht Owner ftp und nicht Gruppe nogroup)
Der FTP-Unterordner für Anonymous Write
chgrp nogroup <upload-ordner>
chmod 030 <upload-ordner> (Dateien unsichtbar)
chmod 074 <upload-ordner> (Dateien sichtbar)
)

Druck-Server
apt-get install cupsys cupsys-client cupsys-driver-gutenprint foomatic-db-gutenprint gimp-gutenprint
nano /etc/cups/cupsd.conf
/etc/init.d/cupsys restart

Drucker Canon iPixma 4200 mit USB angeschlossen

lpinfo -v
network socket
direct usb://Canon/iP4200
network http
network ipp
network lpd
direct parallel:/dev/lp0
direct scsi
serial serial:/dev/ttyS0?baud=115200
serial serial:/dev/ttyS1?baud=115200
network smb

lpadmin -E -p iP4200 -v usb://Canon/iP4200 -P my_iP4200.ppd -u allow:all
lpadmin -d iP4200 (set default printer)
cupsenable iP4200 (enable the printer)
accept iP4200 (start accepting jobs)

Via http://localhost:631/admin/
- [v] Erlaube entfernte Verwaltung / allow remote administration

(# /etc/cups/printers.conf)
(# lpadmin -x iP4200 (delete the printer))

nano /etc/samba/smb.conf
(siehe Abschnitte ### Printing, [printers], [print$])
/etc/init.d/samba restart

Probleme:
- Leider weiss ich nicht, wie ich an die Datei my_iP4200.ppd komme?!?
  (Hab sie von Ubuntu Desktop nach automatischer Erkennung gesichert.)

- Beim Traffic Control mit tc wird der gesamte Druckvorgang sehr langsam,
  obwohl sich die Einstellungen eigentlich nicht auswirken sollten...

Plattenplatz-Management quota
  apt-get install quota quotatool
  runlevel: /etc/init.d/quota , /etc/rcS.d/S35quota , /etc/rc[06].d/K85quota,
        /etc/init.d/quotarpc, /etc/rc[2345].d/S21quotarpc, /etc/rc[016].d/K79quotarpc
- /home/quota.user
  quotatool -u stefan -b -q 1000MB -v /home
  quotatool -u nina -b -q 1000MB -v /home

User Quota für Disk /home (Meine Empfehlung: Quota nicht auf Filesystem/Partition,
das/die vom System benutzt wird, daher z.B. /home)
nano /etc/fstab (Hinzufügen von "usrquota" z.B. bei
  "/dev/sda2 /home ext3 defaults,usrquota 0 2")

mount -o remount /home

touch /home/quota.user
chmod 600 /home/quota.user

Überprüfen der bisherigen quota-Konfiguration mit
quotacheck -av
quotaon -av

Softlimit bei 50MB und Hardlimit bei 60MB:
quotatool -u <user> -b -q 50MB -v /home
quotatool -u <user> -b -l 60MB -v /home

oder auch # edquota -u <user>

Arbeiten mit quota:
- Start Quotad: quotaon -av (erledigt auch vorhandenes Runlevel-Skript)
- Stop Quotad : quotaoff -av (erledigt auch vorhandenes Runlevel-Skript)
- Check Status: quotaon -aup
- Check Quota : repquota -a
- Check Verzeichnisgrößen: du -sh /home/*

NFS Server
  apt-get install nfs-kernel-server
  runlevel:
    /etc/init.d/portmap, /etc/rc[2345].d/S17portmap, /etc/rc0.d/S32portmap,
    /etc/rc6.d/S32portmap, /etc/rcS.d/S43portmap, /etc/rc1.d/K81portmap,
    /etc/init.d/nfs-common, /etc/rc[2345].d/S20nfs-common, /etc/rc[01].d/K20nfs-common,
    /etc/rcS.d/S44nfs-common, /etc/init.d/nfs-kernel-server,
    /etc/rc[2345].d/S20nfs-kernel-server, /etc/rc[016].d/K80nfs-kernel-server
- /etc/exports

```
### apt-get install nfs-kernel-server
### Freigaben:
# Aktiviere veraenderte NFS-Freigaben mit: exportfs -ra
# Zeige NFS-Freigaben mit: showmount -e <server>
# Verbinde NFS-Freigabe mit: (Client mit "apt-get install nfs-common")
# mount <server>:<pfad> /mnt
# mount -o rsize=8192,wsize=8192 <server>:<pfad> /mnt
# in /etc/fstab: <server>:<pfad> /mnt nfs rw,rsize=8192,wsize=8192 0 0
### Ports:
# daemon tcp/udp config
# portmapper 111
# nfsd 2049
# mountd 671 /etc/default/nfs-kernel-server: RPCMOUNTDOPTS=-p 60200
# statd ? /etc/default/nfs-common: STATDOPTS=-p 60201 -o 60202
# lockd ??? options lockd nlm_udpport=60203 nlm_tcpport=60203
# rpc.rquotad /etc/default/quota: RPCRQUOTADOPTS=-p 60204
### Firewall:
# iptables -A INPUT -p tcp --dport 111 -s $TRUSTED -j ACCEPT
# iptables -A INPUT -p udp --dport 111 -s $TRUSTED -j ACCEPT
# iptables -A INPUT -p tcp --dport 671 -s $TRUSTED -j ACCEPT
# iptables -A INPUT -p tcp --dport 2049 -s $TRUSTED -j ACCEPT
# iptables -A INPUT -p udp --dport 2049 -s $TRUSTED -j ACCEPT
# iptables -A INPUT -p udp --dport 32772 -s $TRUSTED -j ACCEPT

#/public *(rw,async)

/home 10.0.0.0/24(rw,async,no_subtree_check)
```

CenterICQ
  apt-get install centericq
X /root/.centericq/config

IM-Server (Jabber/XMPP)
apt-get install ejabberd
  runlevel: /etc/init.d/ejabberd, /etc/rc[2345].d/S20ejabberd, /etc/rc[016].d/K20ejabberd
nano /etc/hosts (+edenhofer.homeip.net)
/firewall mit tcp/5222 und tcp/5288

dpkg-reconfigure ejabberd
        edenhofer.homeip.net / admin / <password>

http://edenhofer.homeip.net:5280/admin

admin@edenhofer.homeip.net / <password>

ejabberdctl register stefan edenhofer.homeip.net <passwort>
ejabberdctl register nina edenhofer.homeip.net <passwort>

(# ejabberdctl register <user> edenhofer.homeip.net <passwort>)
(# ejabberdctl unregister <user> edenhofer.homeip.net)

mutt
apt-get install msmtp mutt
runlevel: /etc/init.d/sendmail, /etc/rc[2345].d/S21sendmail, /etc/rc[016].d/K19sendmail
X /root/.muttrc
X /root/.msmtprc (chmod 600 /root/.msmtprc)

SYSLOG-Server
- /etc/default/syslogd -> "-r" in SYSLOGD="-r" hinzufügen
(trotz Syslog-Meldung "process `syslogd' is using obsolete setsockopt SO_BSDCOMPAT")

```
SYSLOGD="-r"
```

FTP-Server vsftpd
apt-get install vsftpd
runlevel:
/etc/init.d/vsftpd, /etc/rc[2345].d/S20vsftpd, /etc/rc1.d/K20vsftpd
- /etc/vsftpd.conf

```
# /etc/vsftpd.conf
# ------------------------------------------------------------------------
# - curl --ftp-pasv -u anonymous:password ftp://10.0.0.2/down.txt
# - curl --ftp-pasv -u anonymous:password -X "NLST -la" ftp://10.0.0.2/
# - curl --ftp-pasv -u anonymous:password -T up.txt ftp://10.0.0.2/upload/up.txt
# ------------------------------------------------------------------------
# Sinnvolle Methode Nr. 1 (Client im passiven Modus):
# Sinnvoll, wenn Client auch hinter Firewall sitzt.
# Der Client muss auf ausgehenden, passiven Modus geschaltet werden.
# An der Firewall am/zum FTP-Server müssen dann hohe Ports offen sein.
# Es ist also empfehlenswert, mit einem Portbereich (h) zu arbeiten:
# pasv_min_port=60000, pasv_max_port=60099 und
# iptables -A INPUT -p tcp --dport 21 -j ACCEPT
# iptables -A INPUT -p tcp --dport 60000:60099 -j ACCEPT
# Sinnvolle Methode Nr. 2 (Client im aktiven Modus):
# Sinnvoll, wenn der Client auf hohe Ports hören darf, also
# hinter keiner Firewall sitzt. Dann kann auch die serverseitige
# Firewall relativ unberührt bleiben, also eingehend nur:
# iptables -A INPUT -p tcp --dport 21 -j ACCEPT
# - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
# connect_from_port_20= (Default: NO, marked with *)
# | pasv_enable= (Default: YES, marked with *)
# | | Client in passivem Modus
# V V V Client <-> Server TCP Ports
# -----+-------+-------+---------------------------
# *NO *YES NO H -> 21, H <- H
# *NO *YES YES H -> 21, H -> h <= Sinnvolle Methode Nr. 1
# YES *YES NO H -> 21, H <- 20
# (YES) *YES YES H -> 21, H -> H
# YES NO NO H -> 21, H <- 20 <= Sinnvolle Methode Nr. 2
# YES NO YES N/A
# *NO NO NO H -> 21, H <- H
# *NO NO YES N/A
# ------------------------------------------------------------------------
# User-Management:
# User anlegen (a oder b):
# a) Normaler User: useradd -m -s /bin/bash <user>
# b) FTP User : useradd -m -s /bin/bash -d /any/path <user>
# passwd <user>
# userdel -r <user>
# ------------------------------------------------------------------------

#### Global:
listen=YES
xferlog_enable=YES
#chroot_local_user=YES
ftpd_banner="edeserver"
use_localtime=YES
#hide_ids=YES
#deny_file={.ht*,}
#hide_file={.ht*,}

#### FTP Verbindungseigenschaften:
#connect_from_port_20=YES
#pasv_enable=NO
pasv_min_port=60000
pasv_max_port=60199

#### Entscheidung für "Benutzergruppe" (Default: anonymous_enable=YES, local_enable=NO):
# Anonyme Benutzer: anonymous_enable=YES; lokale Benutzer: local_enable=YES
# Für virtuelle Benutzer aus "user_config_dir" ist local_enabled und guest_enabled
anonymous_enable=NO
local_enable=YES
#guest_enable=YES
#user_config_dir=/etc/vsftpd-users

#### Anonyme und lokale Benutzer Zugriffe sperren:
# Betrifft nicht virtuelle Benutzer, da die Optionen dort wieder freigeschaltet werden können.
#dirlist_enable=NO
#download_enable=NO
#???nopriv_user=ftp

#### Anonymous Read:
# FTP-Root ist normalerweise home von User ftp => "anon_root"
```

```
# anon_root: "chmod 754" und "chown root:nogroup" (Verzeichnisse darüber: egal)
# Download von Dateien mit mindestens: "chmod 004 *", nicht Owner ftp und nicht Gruppe nogroup
# Optional kann die Passworteingabe abgeschaltet werden.
# Optional kann die Datenrate für anonyme User beschränkt werden (in Bytes/s).
#anon_root=/ftproot
#no_anon_password=YES
#anon_max_rate=50000

#### Anonymous und lokale User - Write (Erweiterung von Anonymous Read):
# Anonymous:
# Extra Unter-Verzeichnis "upload" o.ä. nötig mit mindestens:
# chmod 030 (Dateien unsichtbar) oder 074 (Dateien sichtbar) für Gruppe nogroup
# write_enable=YES, anon_upload_enable=YES nötig
# Lokale User: write_enable=YES nötig
write_enable=YES
#anon_upload_enable=YES

#### Liste mit ftp-berechtigten anonymous, lokalen oder virtuellen Benutzern:
# userlist_enable aktiviert Liste mit blockierten Benutzern, da Default
# userlist_deny=YES ist. userlist_deny=NO invertiert zur erlaubten Benutzerliste.
# /etc/vsftpd.conf-allowed-user mit Liste der erlaubten User (1 pro Zeile)
#userlist_enable=YES
#userlist_deny=NO
#userlist_file=/etc/vsftpd.conf-allowed-user

#### user_config_dir=/etc/vsftpd-users/, dann /etc/vsftpd-users/USERFILE:
#local_root=/ftproot
#write_enable=YES
#dirlist_enable=YES
#download_enable=YES
#anon_upload_enable=YES
#anon_mkdir_write_enable=YES
#anon_other_write_enable=YES
```

CA

- /root/ca/*
  /root/ca/pki-ca.conf
  /root/ca/pki-ca.global

HTTP-Server apache2

apt-get install apache2
runlevel:
/etc/init.d/apache2, /etc/rc[2345].d/S91apache2, /etc/rc[016].d/K09apache2

- /etc/apache2/apache2.conf (geändert: #Include /etc/apache2/httpd.conf;
  #Include /etc/apache2/ports.conf; #Include /etc/apache2/sites-enabled/;
  Include apache-ede.conf)
- /etc/apache2/apache-ede.conf

```
#[h1]Apache Webserver
#[h2]Konfigurationen ------------------------------------
### Server Side Includes (SSI, link to: html.txt):
# <Directory> Options +Includes
# AddHandler server-parsed .shtml
### CGI / Perl:
# <Directory>-Options +ExecCGI
# AddHandler cgi-script .cgi .pl
### AUTHENTICATION - .htaccess:
# <Directory|VirtualHost>-AllowOverride AuthConfig
# <.htaccess> AuthType Basic
# <.htaccess> AuthName "Authentication"
# <.htaccess> AuthUserFile conf/apache.user (htpasswd -bc apache.user <name> <password>)
# <.htaccess> Require valid-user
### AUTHENTICATION only at HTTPS (Redirect from HTTP via .htaccess):
# LoadModule rewrite_module [...]
# <VirtualHost *.80> AccessFileName .htaccess-80
# <VirtualHost *.443> AccessFileName .htaccess
# <Directory> AllowOverride All
# <.htaccess-80> Options +FollowSymLinks +ExecCGI
# <.htaccess-80> RewriteEngine on
# <.htaccess-80> RewriteRule ^(.*) https://%{SERVER_NAME}%{REQUEST_URI}
### AUTHENTICATION - Directory (ohne .htaccess):
# <Directory|VirtualHost> AllowOverride AuthConfig
# <Directory|VirtualHost> AuthType Basic
# <Directory|VirtualHost> AuthName "Authentication"
# <Directory|VirtualHost> AuthUserFile conf/apache.user (htpasswd -bc apache.user <name> <password>)
# <Directory|VirtualHost> Require user ede
### HTTPS (apache 2.0.52 + mod_ssl, http://hunter.campbus.com ):
# Creation of Certificates: => link to pki-ca.txt
### Install Apache as Windows Service:
# httpd.exe -k install
# httpd.exe -k start
#[h2]Anpassung der Konfigurationsdatei apache2.conf ------------------------------------
# #ServerRoot "c:/apache"
# #Listen 80
# #ServerAdmin @@ServerAdmin@@
# #ServerName localhost:80
# #DocumentRoot "c:/apache/htdocs"
# #<Directory "c:/apache/htdocs"> [...] </Directory>
# #ScriptAlias /cgi-bin/ "c:/apache/cgi-bin/"
# #<Directory "c:/apache/cgi-bin"> [...] </Directory>
# Include conf/extra/httpd-manual.conf => Options [...] +Includes
## debian/ubuntu-Server:
# #Include /etc/apache2/httpd.conf
# #Include /etc/apache2/ports.conf
# #Include /etc/apache2/sites-enabled/
# Include apache-ede.conf
#[h2]Erweiterung der Konfiguration ------------------------------------
#[conf]apache-ede.conf
```

```
CustomLog /var/log/apache2/access.log combined

#ServerRoot "d:/apache"
ServerRoot "/etc/apache2"

SetEnv COMPUTERNAME edeserver

ServerName "Apache Webserver"
ServerAdmin WebMaster@MyWebServer.de
SSLSessionCache none

Listen 80
Listen 443

LoadModule ssl_module /usr/lib/apache2/modules/mod_ssl.so
LoadModule rewrite_module /usr/lib/apache2/modules/mod_rewrite.so
LoadModule userdir_module /usr/lib/apache2/modules/mod_userdir.so
LoadModule include_module /usr/lib/apache2/modules/mod_include.so

AddHandler cgi-script .cgi .pl
AddHandler server-parsed .html

AliasMatch favicon.ico$ "/home/www/scharfEs.ico"

Alias /www /home/stefan/DATEN/www

<Directory />
    Options FollowSymLinks
    AllowOverride None
    Order deny,allow
    Deny from all
    Satisfy all
</Directory>

UserDir /home/*/www
UserDir disabled root
<Directory /home/*/www>
  Options Indexes Includes ExecCGI
  AllowOverride All
  Order Deny,Allow
  Allow from All
</Directory>

<Directory /home/stefan/DATEN/www>
  Options Indexes Includes ExecCGI
  Order allow,deny
  Allow from all
</Directory>

<VirtualHost *:80>
    ServerName "Apache Webserver"
    AccessFileName .htaccess-open
    DocumentRoot "/home/www"
    <Directory "/home/www">
        Options Indexes Includes ExecCGI
        Order Deny,Allow
        Allow from All
    </Directory>
    SSLEngine Off
</VirtualHost>

<VirtualHost *:443>
    ServerName "Apache Webserver"
    AccessFileName .htaccess-secure
    DocumentRoot "/home/www"
    <Directory "/home/www">
        Options Indexes Includes ExecCGI
        Order Deny,Allow
        Allow from All
        #AllowOverride AuthConfig
        #AuthType Basic
        #AuthName "secure edeserver"
        #AuthUserFile apache.user
        #Require user ede
    </Directory>
    SSLEngine On
    SSLCertificateFile edenhofer-homeip-net.crt
    SSLCertificateKeyFile edenhofer-homeip-net.key
</VirtualHost>
#[/conf]
```

- /etc/apache2/edenhofer-homeip-net.key
- /etc/apache2/edenhofer-homeip-net.crt
- /home/stefan/www/.htaccess-open

```
Options +FollowSymLinks
RewriteEngine on
#RewriteCond %{HTTPS} off
RewriteRule ^(.*) https://%{SERVER_NAME}%{REQUEST_URI}
```

- /home/stefan/www/.htaccess-secure

```
AuthType Basic
AuthName "Authentication"
AuthUserFile /home/stefan/users4www
# htpasswd -bc /home/stefan/users4www <user> <password>
Require valid-user
```

- /home/stefan/users4www

Powermanagement hdparm

apt-get install hdparm
runlevel: /etc/init.d/hdparm
X /etc/hdparm.conf

LM-Sensors
apt-get install lm-sensors
runlevel:
/etc/init.d/lm-sensors, /etc/rcS.d/S47lm-sensors
=> sensors-detect: Scan for "Super I/O sensors" => f71805f to /etc/modules,
=> (modprobe f71805f;) sensors
- /etc/modules

SQUID-Server
apt-get install squid
runlevel: /etc/init.d/squid, /etc/rc[2345].d/S30squid, /etc/rc[016].d/K30squid
- /etc/squid/squid.conf

```
http_port 3128
acl lokalesnetz src 10.0.0.0/24
dns_nameservers 10.0.0.2
visible_hostname edeserver
append_domain .geiz
#request_body_max_size 300 MB
acl denyextensions urlpath_regex -i "/etc/squid/deny-extensions"

# Authentikation mit lokalen Usern:
auth_param basic program /usr/lib/squid/pam_auth
auth_param basic children 5
auth_param basic realm edeserver squid server
auth_param basic credentialsttl 2 hours
acl authenticated proxy_auth

hosts_file /etc/hosts
coredump_dir /var/spool/squid
access_log /var/log/squid/access.log squid
logfile_rotate 5

# Hier wird nicht gecachet:
cache_mem 1 MB
cache_dir ufs /var/spool/squid 1 1 1 read-only
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex .*
cache deny QUERY

acl apache rep_header Server ^Apache
broken_vary_encoding allow apache

#refresh_pattern ^ftp: 1440 20% 10080
#refresh_pattern ^gopher: 1440 0% 1440
#refresh_pattern . 0 20% 4320

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8

acl SSL_ports port 443 563 # https, snews
acl SSL_ports port 873 # rsync
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl Safe_ports port 631 # cups
acl Safe_ports port 873 # rsync
acl Safe_ports port 901 # SWAT

acl purge method PURGE
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost

http_access allow authenticated
http_access deny denyextensions
http_access allow lokalesnetz
http_access deny all

http_reply_access allow all

icp_port 0
htcp_port 0
snmp_port 0
icp_access deny all
htcp_access deny all
snmp_access deny all

extension_methods REPORT MERGE MKACTIVITY CHECKOUT
```

- /etc/squid/deny-extensions

```
\.exe$
```

```
\.zip$
\.gz$
\.bz2$
\.mp3$
\.avi$
\.mpg$
\.mpeg$
\.ram$
\.rpm$
\.scr
\.bat
\.com
\.cmd
```

TFTP-Server

apt-get install xinetd tftpd (tftp)
runlevel: /etc/init.d/inetd, /etc/init.d/xinetd,
/etc/rc[2345].d/S20xinetd, /etc/rc[016].d/K20xinetd

- /etc/xinetd.d/tftp

```
service tftp
{
  disable =no
  socket_type =dgram
  protocol =udp
  wait =yes
  user =root
  server =/usr/sbin/in.tftpd
  server_args =-n -s /home/tftpd
}
```

- mkdir /home/tftpd; chmod 777 /home/tftpd
  # Oder über inetd (anstelle von xinetd):
  # netkit-inetd, /etc/inetd.conf:
  # tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd /home/tftp

OpenVPN-Server

- # apt-get install openvpn
  runlevel: /etc/init.d/openvpn, /etc/rc[2345].d/S16openvpn, /etc/rc[016].d/K80openvpn
- # openssl dhparam -out /etc/openvpn/dh1024.pem 1024
- /etc/openvpn/Remote-Access.conf

```
mode server
dev tap
proto udp
port 51194
ifconfig 10.0.1.1 255.255.255.0

ifconfig-pool 10.0.1.10 10.0.1.99
ifconfig-pool-persist ipp.txt

keepalive 10 120
verb 1
mute 10

tls-server
duplicate-cn
dh dh1024.pem
ca edenhofer-ca.crt
cert edenhofer-homeip-net.crt
key edenhofer-homeip-net.key

user nobody
group nogroup
comp-lzo
persist-key
persist-tun

status logfile.log

push "route 10.0.0.0 255.255.255.0 10.0.1.1"
```

- /etc/openvpn/edenhofer-ca.crt
- /etc/openvpn/edenhofer-homeip-net.crt
- /etc/openvpn/edenhofer-homeip-net.key

Webseite mit Status-Anzeige

- /updates-getinfo

```
apt-get -qq update ; apt-get -s dist-upgrade > /updates-getinfo.txt
sed -i -r "/^(Inst|Conf)/d" /updates-getinfo.txt
```

- /home/www/e-status.cgi
  Damit das Lesen der Quota funktioniert:
  # chmod 644 /home/quota.user

```
#!/usr/bin/perl
use strict;
use POSIX qw( strftime );
use CGI::Carp qw(fatalsToBrowser);

&header;

print "<h2>Server status on ".strftime("%a %d.%m.%Y %H:%M:%S", localtime(time))."</h2>";

print "\n<b>System</b>: "; system "uname -a";

print "\n<b>Uptime</b>: "; system "uptime";
```

```
print "\n<b>Disk space usage (incl. intranet)</b>:\n"; system "df -h | sed '1p;/^\\//p;d'";

if( -e "/usr/sbin/repquota" ) { print "\n<b>Quota</b>:\n"; system "/usr/sbin/repquota -a"; } # Geht nicht!!!

print "\n<b>RAID Status</b>:\n".&mycat("/proc/mdstat") if( -e "/proc/mdstat" );

print "\n<b>NTP status</b>:\n"; system "ntpq -pn";

print "\n<b>Processes for access methods</b>:\n"; system "ps --ppid 1,2 | egrep \"sshd|dhcp|named|squid|apache|smbd|ftp|nfsd\" |
/e-group.pl 4";

print "\n<b>Users logged on</b>:\n"; system "/usr/bin/who";

if( -e "/usr/bin/sensors" ) { print "\n<b>Temperatur</b>:\n"; system "/usr/bin/sensors | grep Temp"; }

if( -e "/backup" ) { print "\n<b>Last backup</b>: "; system "du -h /backup/backup-web* | tail -n1"; }

if( -e "/updates-getinfo.txt" )
{ print "\n<b>APT Status</b> at ".&mydate("/updates-getinfo.txt").":\n".&mycat("/updates-getinfo.txt"); }

print "<br><h2>Contact:</h2>".&mycat("/contact.txt") if( -e "/contact.txt" );

&footer;
exit;
# ------------
sub mydate { my @f=stat($_[0]); return strftime "%d.%m.%Y %H:%M", localtime($f[9]); }
sub mycat { my $f=$_[0]; open FILE, $f; my @file = <FILE>; close FILE; return join("",@file); }
sub header { print "content-type: text/html\n\n<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">\n<html>\n<head>
<title>Status</title></head>\n<body><pre>\n"; }
sub footer { print "\n</pre></body></html>\n"; }
```

- /e-group.pl

```
#!/usr/bin/perl
use strict; # Stefan Edenhofer, 15.02.2009

my @data = ();
my %kwc = ();
my ($col, $file);

if( -p STDIN ) # via Pipe
{
  if ( $#ARGV == -1 ) { ; }
  elsif(($#ARGV == 0 )&&($ARGV[0]=~m/\d+/)) { $col = $ARGV[0]-1; }
  else { &usage(); }
  while(<STDIN>) { push @data, $_; }
}
else # via program argument
{
  if ( $#ARGV == -1 ) { &usage(); }
  elsif(($#ARGV == 0 )&&($ARGV[0]=~m/.+/)) { $file = $ARGV[0]; }
  elsif(($#ARGV == 1 )&&($ARGV[0]=~m/.+/)&&($ARGV[1]=~m/\d+/)) { $file = $ARGV[0]; $col = $ARGV[1]-1; }
  else { &usage(); }
  open IN, $file or &filerr(); while(<IN>) { push @data, $_; } close IN;
}

foreach(@data)
{
  my $matcharea = $_;
  $matcharea =~s/[\r\n]//g;
  if( defined $col ) { $matcharea=~s/^\s+//; my @ds = split /\s+/, $matcharea; $matcharea = $ds[$col]; }
  if(length($matcharea)>0){ if($kwc{$matcharea}>0) { $kwc{$matcharea} ++; } else { $kwc{"$matcharea"} = 1; } }
}
foreach my $k (sort keys %kwc) { printf "%3dx %s\n", $kwc{$k}, $k; }
exit;
#--------
sub usage { print "Usage: \"$0 file (col)\" or \"prgout | $0 (col)\"\n"; exit; }
sub filerr { print "Error: Could not open \"$_[0]\".\n"; exit; }
```

- /etc/crontab

```
[...]
#*/15 * * * * root /e-orga-copy
0 0,6,12,18 * * * root /updates-getinfo
```

Immer Eintrag in /var/log/syslog, den wir ausschalten mit:
der Änderung #LSBNAMES='-l' zu LSBNAMES='-L 0' in
- /etc/init.d/cron

Gesamtinstallation benötigt 510 MB Plattenplatz.

System auf USB Drive

Keine swap-Partition

Verzeichnis /var/log in tmpfs:

/mktmpfsdirs
ln -s /mktmpfsdirs /etc/rcS.d/S39mktmpfsdirs

/etc/fstab
tmpfs /var/log tmpfs defaults,noatime 0 0

ToDo

Hardware Probleme:
- Buzzer Onboard funktioniert nicht

Software & Konfiguration:
- Backup
- Powermanagement (BIOS und ACPI; Festplatte soweit entlasten, daß hdparm funktioniert.)
- LVM / RAID
- Email Server ? exim4
- Fax Server ? hylafax
- VoIP Server ? asterisk
- NIS Server ? Tja, es werden ja doch immer mehr Linux-Rechner daheim...
- PDC Server ? ...und vielleicht auch noch ein Windows-Client?
- DSL-Router ? pppoeconfig
- VPN Server: iproute2 (ip tunnel gre,...; siehe ubuntu.txt), IPSec (OpenS/WAN)
- VLAN-Tagging IEEE 802.1q