Steps of the Boot-Prozess until ready to work on the Linux Desktop Environment

BIOS – Basic Input Output System
Power on Self Test

Bootloader:
GRUB **GRUB2** **LILO** **SYSLINUX - Startfähige CDs, USB-Images** **ISOLINUX - Erstellt startfähige CDs, Disketten** **Isohybrid - Erweiterung für ISOLINUX zum hinzufügen eines MBR für USB** **EXTLINUX - Erstellen startfähiger CDs, USB-Sticks für Linux Dateisysteme** **PXELINUX - Netzwerkboot von Betriebssystemen** **Shim - Zum Aktivieren oder Deaktivieren von UEFI Secure Boot** **Systemd-Boot – Erstellen und Ausführen von EFI-Images** **U-Boot - Genutzt für Microcontroller & Embedded Systems**

Early userspace / Initrd (initial ram disk) / initramfs - CPIO-Archiv:

Kernel

SysVinit / Systemd

Virtual Terminal

Text-only-Terminal / Teletype (tty)

https://www.howtogeek.com/428174/what-is-a-tty-on-linux-and-how-to-use-the-tty-command/

https://unix.stackexchange.com/questions/20385/windows-managers-vs-login-managers-vs-display-managers-vs-desktop-environment
https://invidious.kavin.rocks/watch?v=4J5snV2wjtw

Display Server:

X-Window
Xorg / X11 (with xterm Terminalemulator)

XFree86
X11

Wayland
Mir

https://en.wikipedia.org/wiki/Windowing_system

Pseudo teletype Terminal

xterm
Wayland

https://www.howtogeek.com/428174/what-is-a-tty-on-linux-and-how-to-use-the-tty-command/

Display Manager (Login Manager):

Gnome Display Manager (GDM)
Lightway Display Manager (LightDm) by Canonical (Cinnamon)

Simply Desktop Display Manager (SDDM) recommended for KDE and LXQt

Inactive:

X Display Manager (XDM) / (Mother Display Manager)
KDE Display Manager (KDM)
Mint Display Manager (MDM)

https://en.wikipedia.org/wiki/X_display_manager

Window Manager:

Mutter (GNOME)
Muffin (Cinnamon)
Marco (Mate)

Kwin

Openbox (LXDE)

Xfwm / Xfce

Inactive:

Compiz
Metacity
IceWM
Windowmaker
FVWM95
twm
Sawfish

https://de.wikipedia.org/wiki/Fenstermanager
https://en.wikipedia.org/wiki/Comparison_of_X_window_managers

Desktopumgebungen (Paket aus Window Manager & Display Manager):

GNOME
Cinnamon
Mate

KDE

LXDE
LXQt

Xfce

https://en.wikipedia.org/wiki/Desktop_environment
https://en.wikipedia.org/wiki/Comparison_of_X_Window_System_desktop_environments

Emulated Terminal

GNOME Terminal
MATE Terminal

Konsole (KDE)

LX Terminal

Terminal (Xfce)

https://www.howtogeek.com/428174/what-is-a-tty-on-linux-and-how-to-use-the-tty-command/

Linux Deamons (Services)

Deamon Group	Deamon Name	Description
System Deamons	**grub-common**	
	kthreadd	**kernel thread deamon**
	systemd / initd	**mother process deamon**
	acpid	**advanced configuration and power interface deamon**
	alsa-utils	***advanced linux sound architecture utilities deamon***
	dbus-deamon	
Time Deamons	***ntpd***	***network time protocol deamon***
Network Deamons	***networkd***	***Network-manager deamon***
	avahi-deamon	***auto network configuration deamon (ZeroConf)***
	mdnsd	
	dhclient	**dhcp client deamon**
	dhcpcd	**dhcp control deamon**
	dns-clean	
	bluetooth	***bluetooth function deamon***
Logging Deamons	***syslogd***	***system logging deamon***
	syslog-ng	**syslog new generation system logging deamon**
	rsyslogd	**rocket-fast system for log processing deamon**
	rsync	
Task Scheduler Deamons	***cron***	***process planner for high available machines deamon***
	anacron	***process planner for clients (e.g Laptop) deamon***
	atd	***process planner for one time only deamon***
Security Deamons	***cryptdisk***	***encrypt decrypt disk deamon***
	polkitd	**policy kit deamon**
	apparmor /selinux	***apparmor /selinux security rules deamon***
Firewall Deamons	***iptables***	***interface network protection tables deamon***
	nftables	***netfilter tables firewall deamon***
	firewalld	***firewall deamon***
	ufw	***uncomplicated firewall deamon***
Desktop Environment Deamons	***gdm***	***Gnome login manager deamon***
	lightdm	***Light display manager deamon***
	sddm	***Simple desktop display manager deamon***
	Xorg	
Print Deamons	***lpd***	***line printer deamon***
	cupsd	**common unix printing solution**

Server Role Deamons	**dhcpd** **named** ***apache2 / httpd*** ***dovecot*** ***postfix*** **nmbd** **smbd** **mysqld** **vsftpd** **sshd**	**DHCP Server deamon** **Domain Name Server deamon** ***Webserser (Apache) http deamon*** ***IMAP- and POP Server deamon*** ***Mail Server deamon*** **Samba Nameserver deamon** **Samba File Server deamon** **MySQL Server deamon** **FTP Server deamon** **Secure shell deamon**

Paketmanagement DPKG / APT (Debian, Ubuntu)

Kommando	Aufgabe
dpkg	
dpkg --list abc	*Pakete suchen, deren Paketbeschreibung abc enthält*
dpkg --list	*Alle installierten Pakete ermitteln*
dpkg --listfiles paketname	*Liste aller Dateien des Pakets ermitteln*
dpkg --install datei.deb	*Paket installieren bzw. aktualisieren*
dpkg --configure datei.deb	*Paket konfigurieren*
dpkg --remove paketname	*Paket entfernen*
dpkg --purge paketname	*Paket vollständig entfernen (auch geänderte Dateien)*
apt	
apt update	*Metadaten aus den Paketquellen aktualisieren*
apt search suchbegriff	*Paket suchen*
apt show paketname	*Infos zu Paket anzeigen*
apt list	*Alle verfügbaren Pakete auflisten*
apt list --installed	*Alle installierten Pakete auflisten*
apt install name	*Paket installieren*
apt upgrade	*Alle Pakete aktualisieren*
apt full-upgrade	*Alle Pakete aktualisieren , aber bei Bedarf Pakete deinstallieren*
apt remove name	*Paket entfernen*
apt autoremove	*Nicht mehr benötigte Pakete deinstallieren*
apt autoclean	*Zwischengespeicherte Pakete aus Cache löschen*
apt-get	
apt-get update	*Metadaten aus den Paketquellen aktualisieren*
apt-cache show paketname	*Infos zu Paket anzeigen*
apt-cache search paketname	
apt-cache policy paketname	
apt-get install name	*Paket installieren*
apt-get upgrade	*Alle Pakete aktualisieren*
apt-get dist-upgrade	*Alle Pakete aktualisieren , aber bei Bedarf auch neue, abhängige Pakete installieren*
apt-get remove paketname	*Paket entfernen*
apt-get autoremove	*Nicht mehr benötigte Pakete deinstallieren*
apt-get autoclean	*Zwischengespeicherte Pakete aus Cache löschen*

Paketmanagement RPM (CentOS, RedHead, Fedora)

Kommando	Aufgaben
rpm -qf datei	*Paket ermitteln, das diese Datei zur Verfügung stellt*
rpm -qi paketname	*Paketbeschreibung anzeigen*
rpm -ql paketname	*Liste aller Dateien des Pakets ermitteln*
rpm -qc paketname	*Liste aller Konfigurationsdateien des Pakets ermitteln*
rpm -qa	*Informationen zu einem noch nicht installierten Paket ermitteln*
rpm -qpli datei.rpm	*Alle installierten Pakete ermitteln*
rpm -i datei.rpm	*Paket installieren*
rpm -U datei.rpm	*Paket aktualisieren*
rpm -V datei.rpm	*Paketinstallation überprüfen (verify)*
rpm -e paketname	*Paket entfernen*

Paketmanagement YUM / DNF (CentOS, RedHead, Fedora)

Kommando	Aufgabe
yum / dnf history	*Liste der letzten Yum-Aktionen anzeigen*
yum / dnf history info n	*Details zur Aktion n ermitteln*
yum / dnf repolist	*Liste aller Repositories ermitteln*
yum / dnf search 'abc'	*Pakete suchen, die den Begriff abc in der Paketbeschreibung enthalten*
yum / dnf list available 'abc'*	*Liste aller verfügbaren Pakete ermitteln,deren Name mit abc beginnt*
yum / dnf list installed	*Liste aller installierten Pakete ermitteln*
yum / dnf check-update	*Liste der verfügbaren Updates ermitteln*
yum / dnf localinstall datei.rpm	*Lokale Paketdatei installieren*
yum / dnf install name	*Paket installieren*
yum / dnf update name	*Ein Paket aktualisieren*
yum / dnf update	*Alle Pakete aktualisieren*
yum / dnf grouplist/groupinstall/...	*Paketgruppen bearbeiten*
yum / dnf remove name	*Paket entfernen*
yum / dnf module provides pname	*Modul zum angegebenen Paket ermitteln*
yum / dnf module list --all	*Module samt Versionen auflisten*
yum / dnf module info mname:n	*Details zum Modul anzeigen*
yum / dnf module enable mname:n	*Modulversion auswählen (ohne Installation)*
yum / dnf module disable mname	*Versionsauswahl aufheben*
yum / dnf module list --installed	*Installierte Module auflisten*
yum / dnf module install mname:n	*Modul installieren*
yum / dnf install @mname:n	*Modul installieren (Kurzschreibweise)*
yum / dnf module remove mname	*Modul deinstallieren*

Paketmanagement Zypper (OpenSuse)

Kommando	Aufgabe
zypper repos	*Liste aller Paketquellen ermitteln*
zypper addrepo uri name	*Neue Paketquelle einrichten*
zypper refresh	*Metadaten der Paketquellen neu einlesen*
zypper search abc	*Pakete suchen, deren Paketname abc enthält*
zypper search -d abc	*Pakete suchen, deren Beschreibung abc enthält*
zypper info paketname	*Informationen zu einem Paket ermitteln*
zypper -t package list-updates	*Liste aller Updates ermitteln*
zypper install name	*Paket installieren*
zypper -t package update	*ausgewählte Pakete aktualisieren*
zypper update	*Alle Pakete aktualisieren*
zypper dup	*Distributions-Update durchführen*
zypper remove name	*Paket entfernen*
zypper clean	*Zwischengespeicherte Pakete (Cache) löschen*

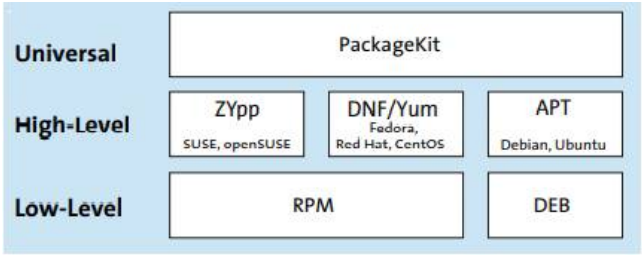


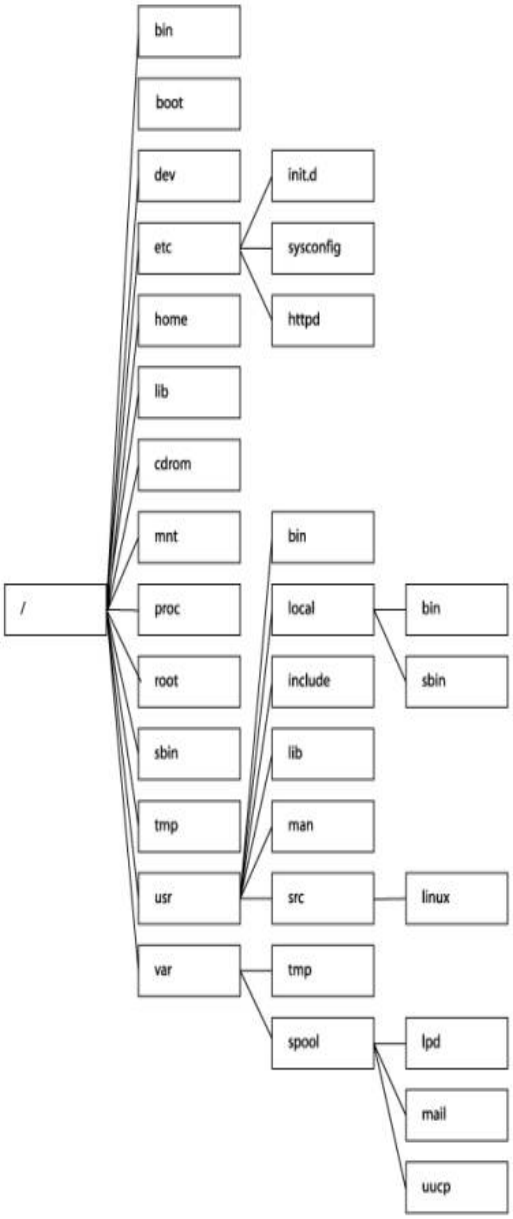
Abbildung 19.1 Low- und High-Level-Paketverwaltungssysteme

Source: Linux-Das-umfassende-Handbuch-für-Anfänger-und-Fortgeschrittene

Linux-Verzeichnisstruktur:

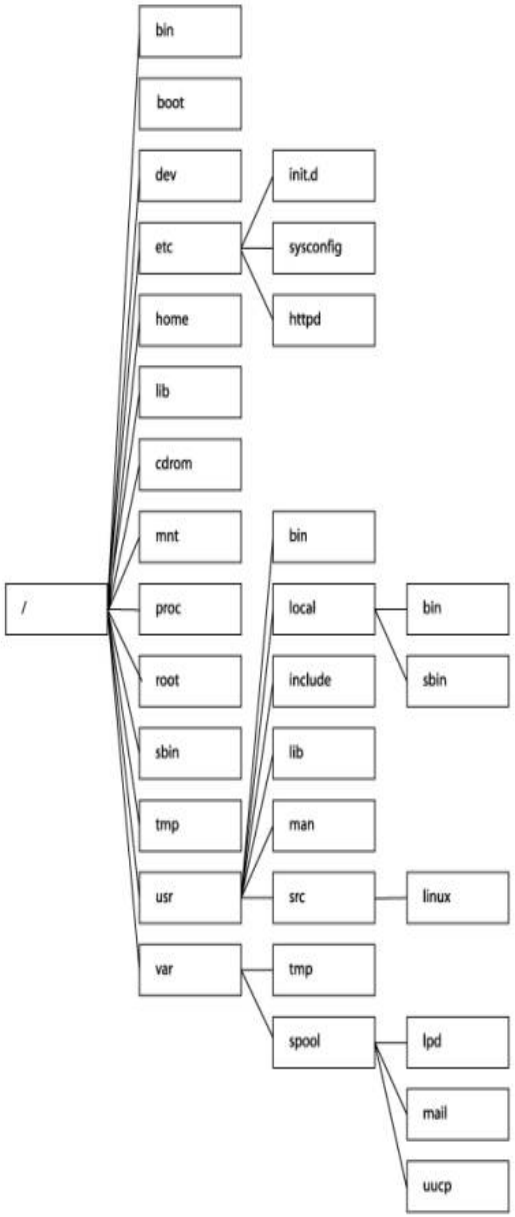
Quellen:

Grafik



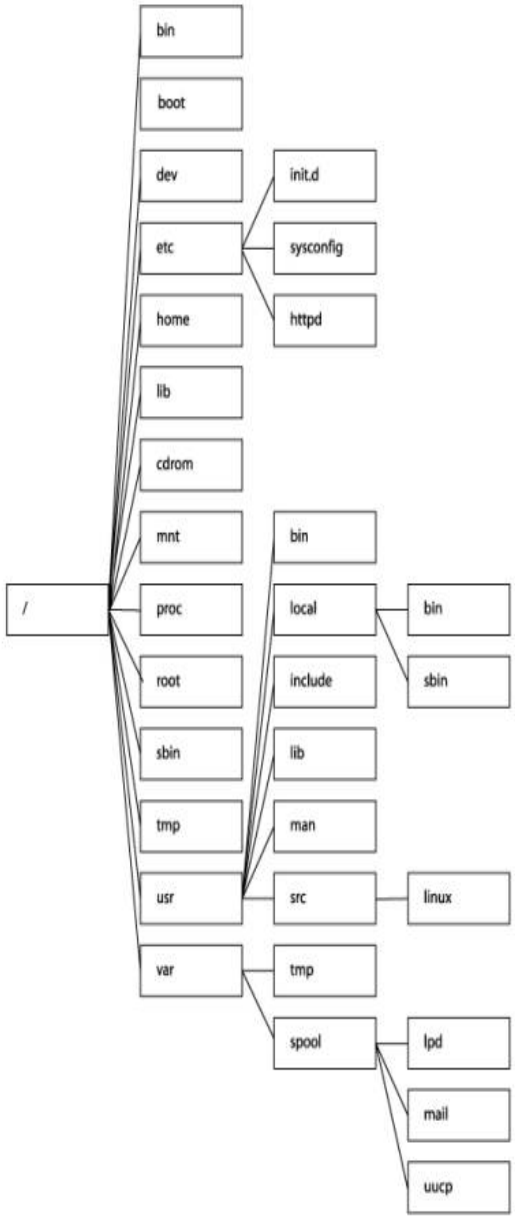
Ausschnitt eines Systems

Verzeichnisname	Beschreibung
***/bin → (usr/*bin)	**Enthält elementare Linux-Kommandos zur Systemverwaltung, die von allen Benutzern ausgeführt werden können. Weitere Programme befinden sich in /usr/bin. Bei modernen Distributionen ist /bin einfach ein Link auf /usr/bin; die Trennung zwischen /bin und /usr/bin wurde damit aufgehoben.**
/boot	**Hier befinden sich die zum Hochfahren des Systems unbedingt erforderlichen Dateien. In der Hauptsache ist das der Bootloader GRUB und der Kernel, im Normalfall eine Datei mit dem Namen vmlinuz. Aber auch andere Namen sind möglich.**
/cdrom	
/dev	**enthält alle Device-Dateien. Auf fast alle Hardware-Komponenten – etwa die serielle Schnittstelle oder eine Festplattenpartition – wird über sogenannte Device-Dateien zugegriffen. Diese werden dynamisch durch das udev-System eingerichtet. Bei den meisten Distributionen befindet sich das /dev-Verzeichnis in einer RAM-Disk, d. h., der Inhalt des Verzeichnisses bleibt bei einem Neustart des Rechners nicht erhalten. Dieses Verzeichnis enthält nur Spezialdateien, sogenannte Gerätedateien. Diese stellen eine einfach zu nutzende Schnittstelle zur Hardware dar. Hier finden sich auch Einträge für alle Festplatten und ihre Partitionen: /dev/hda ist die erste EIDE-, /dev/sda die erste SCSI-Festplatte im System. Höhere Buchstaben (hdb, hdc) stellen weitere Festplatten dar, Zahlen am Ende (sda1, sda2) sind die Partitionen der Festplatten. Da auf einer Festplatte nur vier primäre Partitionen möglich sind, wird häufig eine erweiterte Partition angelegt, die den größten Teil der Festplatte umfasst. In der erweiterten Partition können dann "logische Laufwerke" angelegt werden. Diese erhalten grundsätzlich die Partitionsnummern ab 5. Enthält eine Festplatte also eine primäre und eine erweiterte Partition, in der sich wiederum zwei logische Laufwerke befinden, gibt es auf dieser Platte Die Partitionen 1, 2, 5 und 6. Die primäre Partition ist 1, die erweiterte ist 2, und die beiden logischen Laufwerke sind 5 und 6.**
/etc	**Enthält Konfigurationsdateien für das ganze System. Innerhalb von /etc gibt es eine Menge Unterverzeichnisse, die die Konfigurationsdateien in Gruppen ordnen – z. B. /etc/apt für Dateien des Paketverwaltungssystems apt**
/home	**enthält die Heimatverzeichnisse aller regulären Linux-Anwender. Das Heimatverzeichnis ist jenes Verzeichnis, in dem sich der Anwender nach dem Einloggen automatisch befindet und auf dessen Dateien er uneingeschränkte Zugriffsrechte hat. Ein Sonderfall ist wie so oft root: Dessen Heimatverzeichnis lautet /root.**
/lib → (usr/lib ,lib32, lib64)	**Hier befinden sich die wichtigsten Funktionsbibliotheken des Systems. Enthält einige gemeinsame Bibliotheken (Shared Libraries) oder symbolische Links darauf. Die Dateien werden zur Ausführung von Programmen benötigt. /lib/modules enthält Kernelmodule, die im laufenden Betrieb dynamisch aktiviert bzw. deaktiviert werden. Weitere Bibliotheken befinden sich in /usr/lib[64]. Das Verzeichnis /lib/firmware enthält die Firmware diverser Hardware-Komponenten (z. B. WLANController). Bei aktuellen Distributionen ist /lib ein Link auf /usr/lib. Damit werden alle Bibliotheken zentral im /usr-Verzeichnis abgelegt.**
/lost+found	**Gibt es nur in ext-Dateisystemen. Das Verzeichnis ist normalerweise leer. Enthält es doch Dateien, dann handelt es sich um Dateifragmente, die beim Versuch, das Dateisystem durch fsck zu reparieren, nicht mehr zugeordnet werden konnten. Mit anderen Worten: Es wurden Sektoren gefunden, aber es ist unklar, zu welcher Datei der Sektor einmal gehört hat. Anstatt derartige Dateifragmente einfach zu löschen, kopiert fsck diese in das lost+found-Verzeichnis. fsck wird automatisch während des Systemstarts ausgeführt, wenn Linux nicht ordnungsgemäß beendet wurde (Stromausfall, Absturz etc.) oder wenn das Dateisystem längere Zeit nicht mehr überprüft wurde. Das Ziel von fsck ist es, das Dateisystem wieder in einen klar definierten Zustand zu bringen.**
/media	**Enthält Unterverzeichnisse wie cdrom oder <usb-stick-name>, an deren Stelle externe Dateisysteme eingebunden werden. Traditionell war hierfür /mnt üblich, in den vergangenen Jahren hat sich stattdessen zuerst /media und schließlich das Verzeichnis /run/media/<benutzername>/<datenträgername> durchgesetzt**



Ausschnitt eines Systems

/mnt	**Enthält die Einhängepunkte für Unterverzeichnisse wie cdrom oder <usb-stick-name>, an deren Stelle externe Dateisysteme eingebunden werden.**
/opt	**Ist für Zusatzpakete vorgesehen, wird von den gängigen Distributionen aber nur selten genutzt – vermutlich deswegen, weil unklar ist, wie sich Zusatzpakete von normalen Paketen unterscheiden.** **(Optionale Software) Kommerzielle Software oder sehr große Programme, die nicht unmittelbar zum System gehören, wie etwa KDE, Netscape, Mozilla usw. finden hier ihren Platz.**
/proc	**/proc ist eigentlich kein normales Verzeichnis, sondern stellt eine Schnittstelle zum Kernel dar.** **Jedes laufende Programm wird hier in einem Unterverzeichnis geführt, dessen Dateien viele Informationen z.B. über den aktuellen Programmstatus enthalten.** **Zudem gibt es eine umfangreiche Verzeichnisstruktur mit Daten über den Kernel und die Hardware des Systems.** **Enthält Unterverzeichnisse für alle laufenden Prozesse.** **Es handelt sich hierbei nicht um echte Dateien! Das /proc-Verzeichnis spiegelt lediglich die Linux-interne Verwaltung der Prozesse wider**
/root	**Dies ist das Heimatverzeichnis des Systemverwalters root.** **Es liegt traditionell im Wurzelverzeichnis, damit root auch dann auf seine Dateien (beispielsweise Diagnoseprogramme) zugreifen kann, wenn durch einen Fehler der Zugriff auf andere Partitionen nicht mehr möglich ist.** **Enthält die Dateien des Benutzers root, also des Systemadministrators.**
/run	**Enthält bei vielen aktuellen Distributionen Dateien mit den Prozess-Ids sowie weiteren Informationen von manchen Systemdiensten.** **In der Vergangenheit wurden diese Dateien im Verzeichnis /var/run gespeichert.** **Das Unterverzeichnis /run/lock/ enthält Locking-Dateien.** **Bei älteren Distributionen finden Sie die Locking-Dateien stattdessen in /var/lock.** **Bei vielen Distributionen werden entweder das gesamte /run-Verzeichnis oder zumindest einzelne /run-Unterverzeichnisse in einer RAMDisk abgelegt.** **Die überwiegend sehr kleinen Dateien in /run werden somit nie physisch auf einer Festplatte oder SSD gespeichert und gehen beim Neustart des Rechners verloren.**
***/sbin* → *(usr*/sbin)**	**Ähnlich wie /bin enthält auch /sbin wichtige Programme.** **Diese sind jedoch hauptsächlich für den Systemverwalter gedacht, da sie Funktionen erfüllen, auf die ein normaler Benutzer keinen Zugriff hat.** **Enthält Kommandos zur Systemverwaltung.** **Ein gemeinsames Merkmal aller darin gespeicherten Programme ist, dass sie nur von root ausgeführt werden dürfen.** **Bei modernen Distributionen ist /sbin ein Link auf /usr/sbin; alle Kommandos zur Systemverwaltung befinden sich nun in /usr/sbin**
/share	**Enthält manchmal architekturunabhängige Dateien, also Dateien, die unabhängig vom Prozessor sind.** **Der korrekte Ort ist eigentlich /usr/share.**
/srv	**Ethält bei einigen Distributionen (Fedora, RHEL) Daten für ServerProzesse, z. B. in /srv/www Dateien des Webservers oder in /srv/ftp Dateien des FTP-Servers.**
/sys	**Enthält das sysfs-Dateisystem. Es liefert wie das proc-Dateisystem Informationen über den Zustand des Rechners.**
/tmp	**Dieses Verzeichnis kann von jedem Benutzer und jedem Programm als temporäre Ablage für Dateien verwendet werden.** **Damit sich Benutzer nicht gegenseitig ihre Dateien löschen, ist das sogenannte Sticky-Bit dieses Verzeichnisses gesetzt.** **Enthält temporäre Dateien. Oft werden temporäre Dateien aber auch in /var/tmp gespeichert**
/usr	**Die umfangreichste Verzeichnisstruktur des Systems. Hier liegt der größte Teil der installierten Software.** **Auf vielen Systemen befinden sich in und unterhalb von /usr mehr Daten als in allen anderen Dateien zusammen.** **Die Programmdateien sind meist in /usr/bin, die Spiele in /usr/games.** **In Netzwerken, an die viele gleichartige Systeme angeschlossen sind, wird dieses Verzeichnis häufig auf einem zentralen Server gespeichert, und alle anderen Computer greifen über das Netzwerk darauf zu.** **Enthält alle Anwendungsprogramme, das komplette X-System, die Quellcodes zu Linux etc.** **Der Inhalt dieses Verzeichnisses ändert sich normalerweise nur bei Paketinstallationen und Updates.** **Für veränderliche Dateien ist das Verzeichnis /var vorgesehen.**



Ausschnitt eines Systems

/var	**Enthält veränderliche Dateien. Wichtige Unterverzeichnisse sind z. B. log (Logging-Dateien), docker (Docker-Dateien), lock (Locking-Dateien zum Zugriffsschutz auf Devices), mail (E-Mail-Dateien, oft auch in /var/spool/mail), Mysql (MySQL-Datenbankdateien), run (Dateien mit ProzessIDs von manchen Systemdiensten) und spool (zwischengespeicherte Druckdateien). Unter diesem Verzeichnis werden hauptsächlich Dateien gespeichert, die sich ständig verändern. Der Name /var steht für variabel, also veränderlich. Hier befinden sich beispielsweise die Verzeichnisse für ausgehende E-Mail und noch ungelesene eingehende, wenn der jeweilige Benutzer nicht dafür gesorgt hat, dass neue E-Mails automatisch in sein Heimatverzeichnis übertragen werden.**

/etc/passwd

Die Einträge in der Datei /etc/passwd haben folgende Bedeutungen:

⟨Benutzername⟩:⟨Kennwort⟩:⟨UID⟩:⟨GID⟩:⟨GECOS⟩:⟨Heimatverzeichnis⟩:⟨Shell⟩

```
hugo:x:1000:1000:Hugo Schulz:/home/hugo:/bin/sh
```

Benutzername	**Dieser Name sollte aus Kleinbuchstaben und Ziffern bestehen; das erste Zeichen sollte ein Buchstabe sein. Unix-Systeme unterscheiden oft nur die ersten 8 Zeichen – Linux hat diese Einschränkung nicht, aber in heterogenen Netzen sollten Sie darauf Rücksicht nehmen Widerstehen Sie der Versuchung, Umlaute, Satzzeichen und ähnliches in Benutzernamen aufzunehmen**
Kennwort	**Traditionell steht hier das verschlüsselte Kennwort des Benutzers. Unter Linux sind heute »Schattenkennwörter« (shadow passwords) üblich; shadow passwords statt das Kennwort in der allgemein lesbaren /etc/passwd-Datei abzulegen, steht es in der Datei /etc/shadow gespeichert, auf die nur der Administrator und einige privilegierte Prozesse Zugriff haben. In /etc/passwd macht ein »x« auf diesen Umstand aufmerksam. Jedem Benutzer steht das Kommando passwd zur Verfügung, um sein Kennwort selbst zu verändern.**
User-ID (UID)	**Die numerische Benutzerkennung – eine Zahl zwischen 0 und 2^32−1. Nach Konvention sind UIDs zwischen 0 und 99 (einschließlich) für das System reserviert, UIDs zwischen 100 und 499 können an Softwarepakete ausgegeben werden, falls diese Pseudobenutzer benötigen. UIDs für »echte« Benutzer haben bei den meisten Distributionen Werte ab 1000.**
Group-ID (GID)	**Bei den Novell/SUSE- und manchen anderen Distributionen wird eine bestimmte Gruppe, hier beispielsweise users, als gemeinsame Standardgruppe für alle Benutzer eingetragen. Diese Methode ist einfach zu verstehen und hat Tradition. Bei vielen Distributionen, etwa denen von Red Hat oder Debian GNU/Linux, wird für jeden neuen Benutzer automatisch eine eigene Gruppe angelegt, die die gleiche GID hat wie die UID des Benutzerkonto**
GECOS	**Dies ist das Kommentarfeld, auch GECOS-Feld genannt. GECOS steht für General Electric Comprehensive Operating System Das Feld enthält diverse Informationen über den Benutzer, vor allem seinen »richtigen« Namen und optionale Informationen wie die Zimmer- oder Telefonnummer. Diese Information wird von Programmen wie mail und finger benutzt. Oft wird der volle Name von News- und Mail-Programmen bei der Zusammenstellung der Absenderadresse verwendet.**
Heimatverzeichnis	**Das hier benannte Verzeichnis ist der persönliche Bereich des Benutzers, in dem er seine eigenen Dateien aufbewahren kann. Ein neu erstelltes Heimatverzeichnis ist selten leer, denn üblicherweise erhält ein neuer Benutzer vom Administrator einige Profildateien als Erstausstattung. Wenn ein Benutzer sich anmeldet, benutzt seine Shell das Heimatverzeichnis als aktuelles Verzeichnis, das heißt, der Benutzer befindet sich Unmittelbar nach der Anmeldung zunächst dort.**
Shell	**Der Name des Programms, das von login nach erfolgreicher Anmeldung gestartet werden soll – das ist in der Regel eine Shell. Das siebte Feld reicht bis zum Zeilenende. Der Benutzer kann mit dem Programm chsh diesen Eintrag selbst ändern. Die erlaubten Programme (Shells) sind in der Datei /etc/shells aufgelistet. Wenn ein Benutzer keine interaktive Shell haben soll, kann auch ein beliebiges anderes Programm mit allen Argumenten in dieses Feld eingetragen werden (ein gängiger Kandidat ist /bin/true). Das Feld kann auch leer bleiben. Dann wird automatisch die Standardshell /bin/sh gestartet.**

/etc/shadow

Die Einträge in der Datei /etc/shadow haben folgende Bedeutungen:

⟨Benutzername⟩:⟨Kennwort⟩:⟨Änderung⟩:⟨Min⟩:⟨Max⟩▷
◁:⟨Warnung⟩:⟨Frist⟩:⟨Sperre⟩:⟨Reserviert⟩

```
root:gaY2L19jxzHj5:10816:0:10000::::
daemon:*:8902:0:10000::::
hugo:GodY6c5pZk1xs:10816:0:10000::::
```

Benutzername	**Entspricht einem Eintrag in der Datei /etc/passwd. Dieses Feld »verbindet« die beiden Dateien.**
Kennwort	**Das verschlüsselte Kennwort des Benutzers. Ein leerer Eintrag bedeutet in der Regel, dass der Benutzer sich ohne Kennwort anmelden kann. Steht hier ein Stern oder ein Ausrufungszeichen, kann der betreffende Benutzer sich nicht anmelden. Es ist auch üblich, Benutzerkonten zu sperren, ohne sie komplett zu löschen, indem man einen Stern oder ein Ausrufungszeichen An den Anfang des zugehörigen Kennworts setzt.**
Änderung	**Das Datum der letzten Änderung des Kennworts, in Tagen seit dem 1. Januar 1970**
Min	**Minimale Anzahl von Tagen, die seit der letzten Kennwortänderung vergangen sein müssen, damit das Kennwort wieder geändert werden**
Max	**Maximale Anzahl von Tagen, die ein Kennwort ohne Änderung gültig bleibt. Nach Ablauf dieser Frist muss der Benutzer sein Kennwort ändern**
Warnung	**Die Anzahl von Tagen vor dem Ablauf der ⟨Max⟩-Frist, an denen der Benutzer eine Warnung erhält, dass er sein Kennwort bald ändern muss, weil die maximale Anzahl abläuft. Die Meldung erscheint in der Regel beim Anmelden.**
Frist	**Die Anzahl von Tagen ausgehend vom Ablauf der ⟨Max⟩-Frist, nach der das Konto automatisch gesperrt wird, wenn der Benutzer nicht vorher Sein Kennwort ändert. (In der Zeit zwischen dem Ende der ⟨Max⟩-Frist und dem Ende dieser Frist kann der Benutzer sich anmelden, muss aber sofort sein Kennwort ändern.)**
Reserviert	**Das Datum, an dem das Konto definitiv gesperrt wird, wieder in Tagen seit dem 1. Januar 1970.**

/etc/group

Die Einträge in der Datei /etc/group haben folgende Bedeutungen:

⟨Gruppenname⟩:⟨Kennwort⟩:⟨GID⟩:⟨Mitglieder⟩

```
root:x:0:root
bin:x:1:root,daemon
users:x:100:
projekt1:x:101:hugo,susi
projekt2:x:102:emil
```

Gruppenname	**Der textuelle Name der Gruppe, für die Verwendung in Verzeichnislisten usw.**
Kennwort	**Ein optionales Kennwort für diese Gruppe. Damit können auch Benutzer, die nicht per /etc/shadow oder /etc/group Mitglied der Gruppe sind, mit dem Befehl newgrp diese Gruppenzugehörigkeit annehmen. Ein »*« als ungültiges Zeichen verhindert einen Gruppenwechsel von normalen Benutzer in die betreffende Gruppe. Ein »x« verweist auf die separate Kennwortdatei /etc/gshadow.**
Group-ID (GID)	**Die numerische Gruppenkennung für diese Gruppe**
Mitglieder	**Eine durch Kommas getrennte Liste mit Benutzernamen. Die Liste enthält alle Benutzer, die diese Gruppe als sekundäre Gruppe haben, die also zu dieser Gruppe gehören, aber im GID-Feld der Datei /etc/passwd einen anderen Wert stehen haben. (Benutzer mit dieser Gruppe als primärer Gruppe dürfen hier auch stehen, aber das ist unnötig.)**

/etc/gshadow

Die Einträge in der Datei /etc/gshadow haben folgende Bedeutungen:

Benutzer und Gruppen

Name	Linuxname
Besitzer	u
Gruppe	g
Andere	o

Zugriffsrechte für ein Verzeichnis

Aktion	Kommando		Datei	Verzeichnis
In Verzeichnis wechseln	cd	verzeichnisname	–	x
Liste der Dateien ermitteln	ls	verzeichnisname/*	–	r
Dateiinformationen lesen	ls -l	verzeichnisname/*	–	rx
Neue Datei erzeugen	touch	verzeichnisname/ neuer dateiname	–	wx
Datei lesen	less	verzeichnisname/ dateiname	r	x
Vorhandene Datei ändern	cat >>	verzeichnisname/ dateiname	w	x
Datei löschen	rm	verzeichnis/ dateiname	–	wx
Programm ausführen		verzeichnisname/ programmname	x	x
Script-Datei ausführen		verzeichnisname/ scriptname	rx	x

Beispiele

drwxrw---	Verzeichnis = Besitzer (rwx) Gruppe (rw) Andere (-)
760 (chmod)	Verzeichnis = Besitzer (rwx = 4+2+1=7) Gruppe (rw = 4+2+0=6) Andere (- = 0+0+0=0)
u+rwx g+rw	Verzeichnis = Besitzer (rwx) Gruppe (rw) Andere (-)
017 (umask)	Verzeichnis = Besitzer (rwx = 7- 4 – 2 – 1 = 0) Gruppe (rw = 7 -4 -2 0 = 1) Andere (- = 7 -0 = 0)

Zugriffsrechte für Dateien

Zugriffsrecht	Alphanummerische Schreibweise	Gewichtung (chmod / umask)
read	r	4
write	w	2
execute	x	1
setuid	s / S (no x)	4
setgid	s / S (no x)	2
stickybit	t / T (no x)	1

Name	Beschreibung
setuid	Programm wird immer mit den Besitzerrechten ausgeführt
setgid	Verzeichnis oder Datei erhalten immer die Gruppenrechte
stickybit	Es können nur eigene Dateien gelöscht werden / Ausnahme root

Dateisysteme einbinden

/etc/fstab

Spalte 1

Aufgabe	Parameter
Die erste Spalte enthält den Device-Namen des Datenträgers. Statt des Device- Erste Spalte Namens können Sie auch den Volume Name oder die ID-Nummer des Dateisystems angeben. z.B /dev/sda2 *UUID="5a954fc1-00c6-4c25-a943-d4220eff350d"*	*/dev/…*

Spalte 2

Aufgabe	Parameter
Die zweite Spalte gibt an, bei welchem Verzeichnis der Datenträger in den Dateibaum eingebunden wird. Die in der zweiten Spalte angegebenen Verzeichnisse müssen bereits existieren. z.B /mnt/USB	*/../…*

Spalte 3

Aufgabe	Parameter
Die dritte Spalte gibt das Dateisystem an. Es ist auch zulässig, mehrere Dateisysteme durch Kommas getrennt anzugeben. Beispielsweise bietet sich iso9660,udf für CD und DVD-Laufwerke an, weil für CDs und DVDs in der Regel nur diese beiden Dateisysteme Infrage kommen. mount entscheidet sich zwischen den zur Auswahl stehenden Systemen automatisch für das richtige. Die Dateisystemnamen dürfen nicht durch Leerzeichen getrennt werden.	
Dateisystem automatisch erkennen	*auto*
Btrfs-Dateisystem	*btrfs*
Windows-Netzwerkverzeichnis (Samba)	*cifs*
ext-Dateisystem Version 2, 3 und 4	*ext 2 3 4*
Daten-CDs	*iso9660*
Unix-Netzwerkverzeichnis (NFS)	*nfs*
Windows-Dateisystem	*ntfs*
Prozessverwaltung (/proc)	*proc*
Windows-Netzwerkverzeichnis (Samba)	*smbfs*
Swap-Partitionen oder -Dateien	*swap*
Systemverwaltung (/sys)	*sysfs*
temporäres Dateisystem	*tmpfs*
Universal Disk Format (DVDs, CD-Rws)	*udf*
Windows-9x/ME-Dateisystem	*vfat*
XFS-Dateisystem	*xfs*

Spalte 4

Aufgabe	Parameter
Die vierte Spalte bestimmt Optionen für den Zugriff auf den Datenträger. Mehrere Optionen werden durch Kommata getrennt. Abermals dürfen keine Leerzeichen eingefügt werden!	
Standardoptionen verwenden	*defaults*
Kennzeichnung von Character- oder Block-Devices auswerten	*dev*
SSD-Trim aktivieren (ext4, btrfs, xfs und swap)	*discard*
Programmausführung zulassen (z. B. für CD/DVD-Laufwerke)	*exec*
Datenträger nicht beim Systemstart einbinden	*noauto*
Kennzeichnung von Character- oder Block-Devices ignorieren	*nodev*
keine Programmausführung erlaubt	*noexec*
Boot-Vorgang fortsetzen, wenn Dateisystem nicht vorhanden	*nofail*
Suid- und Guid-Zugriffsbits nicht auswerten	*nosuid*
Der Besitzer darf (u)mount ausführen	*owner*
Read Only (Schreibschutz)	*ro*
Swap (Swap-Datei oder -Partition)	*sw*
Suid- und Guid-Zugriffsbits auswerten	*suid*
Schreibzugriffe nicht puffern (sicherer, aber langsamer)	*sync*
Jeder darf mount ausführen, aber nur der Benutzer des letzten mount-Aufrufs darf umount ausführen.	*user*
Jeder darf mount und umount ausführen.	*users*
POSIX Access Control Lists aktivieren (ext2 , ext3, ext4, reiserfs, ifs, Btrfs)	**acl**
Erweiterte Dateisystemattribute aktivieren z.B nicht in Datensicherung berücksichtigen (ext2 , ext3, ext4)	**user_xattr**
Aktiviert Quota für Benutzer	**usrquota**
Aktiviert Quota für Gruppen	**grpquota**
Aktiviert Journal für Quotas für Benutzers	**usrjquota=aquota.user**
Aktiviert Journal für Quotas für Gruppen	**grpjquota=aquota.group**
Mit dieser Option wird das Format des Journals für die Quotas festgelegt. Ohne diese Option lässt sich die Partition nicht mehr mounten, da das Journal für die Quotas nicht geschrieben werden kann	**jqfmt=vfsv0**

Spalte 5

Aufgabe	Parameter
Die fünfte Spalte enthält Informationen für das Programm dump und wird von Linux ignoriert. Es ist üblich, für die Systempartition 1 und für alle anderen Partitionen oder Datenträger 0 einzutragen.	*0,1*

Spalte 6

Aufgabe	Parameter
Die sechste Spalte gibt an, ob und in welcher Reihenfolge die Dateisysteme beim Systemstart überprüft werden sollen. Oft wird 1 für die Systempartition und 0 für alle anderen Partitionen eingetragen. Das bedeutet, dass beim Rechnerstart nur die Systempartition auf Fehler überprüft und gegebenenfalls repariert wird. *Falls Sie möchten, dass weitere Partitionen automatisch überprüft werden, geben Sie bei diesen Partitionen die Ziffer 2 an, d. h., die Überprüfung soll nach der Kontrolle der Systempartition erfolgen. Wenn Einträge in der fünften und sechsten Spalte in /etc/fstab fehlen, wird 0 angenommen*	*0,1,2*

Beispiel:

Die Festplatte mit dem Geräteschnittstellennamen *`/dev/sda2`* wird unter dem Mountnamen *`/mnt/usb`* als *`Ext4`* Dateisystem mit der Option *`defaults`* (Default-Einstellungen) als Systemplatte *`(1`*) mit der Option Fehlerüberprüfung bei Systemstart aktiviert (*`1`*) eingebunden.

```
/dev/sda2    /mnt/usb    ext4    defaults  1   1
```

Syslog

Quelle: https://www.selflinux.org/selflinux/html/syslog03.html#d76e489

/etc/syslog.conf

Syslog Konfiguration - Facilities

Aufgabe	Parameter
Meldungen, die zur Authentifizierung gehören, beispielsweise falsche Passwörter.	*auth, authpriv*
Meldungen, die von Cron erzeugt wurden, oder von Prozessen, die von Cron gestartet werden (die Standard-Ausgabe und Stardard-Fehler-Ausgabe werden jedoch von Cron nicht an Syslog gereicht, sondern per EMail verschickt).	*cron*
Meldungen von allgemeinen Diensten, wie zum Beispiel einem FTP-Server	*daemon*
Meldungen des Systemkernels. Sollte von keinem Dienst verwendet werden. Hierzu gehören beispielsweise Hardware-bezogene Meldungen.	*kern*
Meldungen des Drucksystems (Druckerspooler)	*lpr*
Meldungen des Mailsystems (beispielsweise von sendmail und fetchmail).	*mail*
Nur für Syslog-interne Zwecke, sollte nie verwendet werden	*mark*
Meldungen des News-Systems, zum Beispiel eines Newsservers.	*news*
Meldungen von Syslog selbst.	*syslog*
Meldungen von Benutzersystemen wie zum Beispiel eigenen Scripten.	*user*
Meldungen von Unix-Unix-Copy (UUCP wird heute kaum noch verwendet).	*uucp*
Diese sind frei und können nach Belieben verwendet werden. Bei Diensten, bei denen man die zu verwendende Facility einstellen kann, kann man diese verwenden und je nach Bedarf verteilen.	*local 0 bis local 17*

Syslog Konfiguration - Priority

Aufgabe	Parameter
Unwichtige Meldungen, dienen nur zu Debug-Zwecken (Fehlerfindung vor allem bei der Entwicklung)	*debug*
Informative, nicht weiter wichtige Meldungen	*info*
Informative Meldungen, die größere Bedeutung haben als info.	*notice*
Warnungen, also Meldungen, die nicht-fatale Fehler anzeigen.	*warning*
Fehlermeldungen, die kleine Störungen anzeigen.	*err*
Kritische (schwerere) Fehler, die beispielsweise Teilausfälle anzeigen.	*crit*
Schwere Fehler, die erhebliche Störungen und Ausfälle anzeigen.	*alert*
Sehr schwere Fehler, die beispielweise den Totalausfall des Systems anzeigen können und schwere Kernelfehler (Hardwareausfälle).	*emerg*

Beispiel für /etc/syslog.conf :

```
kern.warning;user.warning                 /var/log/user-defined-message-data

kern.warning;*.err;authpriv.none          /dev/tty10

*.warn                                    @192.168.1.1
```

Syslog-ng

Quelle: https://www.selflinux.org/selflinux/html/syslog-ng03.html#d77e158

/etc/syslog-ng/syslog-ng.conf

Source-Objekt

Hier kann man die Quellen angeben, woher syslog-ng Meldungen empfangen soll.

```
source src { unix-stream("/dev/log"); internal(); };

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

udp( ip(0.0.0.0) port(514) )
```

Destination-Objekt

Mit dem Destination Objekt kann man Ziele festlegen, wohin ein Log-Stream gehen soll.

```
destination syslog { file("/var/log/syslog" owner("root") group("adm") perm (0640)); };

destination mylog { file("/var/log/syslog-$HOST" owner("root") group("adm") perm(0640)); };

destination a_udp { udp( "192.168.0.12" port(514) ); };

destination admin_tty { usertty(admin); };
```

Definitionen für Filter-Objekt:

Aufgabe	Parameter
Meldungen, die zur Authentifizierung gehören, beispielsweise falsche Passwörter.	*auth, authpriv*
Meldungen, die von Cron erzeugt wurden, oder von Prozessen, die von Cron gestartet werden (die Standard-Ausgabe und Stardard-Fehler-Ausgabe werden jedoch von Cron nicht an Syslog gereicht, sondern per EMail verschickt).	*cron*
Meldungen von allgemeinen Diensten, wie zum Beispiel einem FTP-Server	*daemon*
Meldungen des Systemkernels. Sollte von keinem Dienst verwendet werden. Hierzu gehören beispielsweise Hardware-bezogene Meldungen.	*kern*
Meldungen des Drucksystems (Druckerspooler)	*lpr*
Meldungen des Mailsystems (beispielsweise von sendmail und fetchmail).	*mail*
Nur für Syslog-interne Zwecke, sollte nie verwendet werden	*mark*
Meldungen des News-Systems, zum Beispiel eines Newsservers.	*news*
Meldungen von Syslog selbst.	*syslog*
Meldungen von Benutzersystemen wie zum Beispiel eigenen Scripten.	*user*
Meldungen von Unix-Unix-Copy (UUCP wird heute kaum noch verwendet).	*uucp*
Diese sind frei und können nach Belieben verwendet werden. Bei Diensten, bei denen man die zu verwendende Facility einstellen kann, kann man diese verwenden und je nach Bedarf verteilen.	*local 0 bis local 17*

Aufgabe	Parameter
Unwichtige Meldungen, dienen nur zu Debug-Zwecken (Fehlerfindung vor allem bei der Entwicklung)	*debug*
Informative, nicht weiter wichtige Meldungen	*info*
Informative Meldungen, die größere Bedeutung haben als info.	*notice*
Warnungen, also Meldungen, die nicht-fatale Fehler anzeigen.	*warning*
Fehlermeldungen, die kleine Störungen anzeigen.	*err*
Kritische (schwerere) Fehler, die beispielsweise Teilausfälle anzeigen.	*crit*
Schwere Fehler, die erhebliche Störungen und Ausfälle anzeigen.	*alert*
Sehr schwere Fehler, die beispielweise den Totalausfall des Systems anzeigen können und schwere Kernelfehler (Hardwareausfälle).	*emerg*

Filter Objekte legen fest, wie Meldungen von einem Source-Objekt gefiltert werden sollen. Hiermit lassen sich also gewünschte Messages aus dem gesamten Datenstrom eines Source-Objektes herauspicken.

filter f_cnews { level(notice, err, crit) and facility(news); };

filter f_authpriv { facility(auth, authpriv); };

Log-Objekt

Alle bisherigen Objekte waren Vorarbeiten, um jetzt Zeilen zu generieren, die wirklich Aktionen auslösen. Denn ohne die log-Objekte würde gar nichts passieren. Die anderen Objekte sind nur Daten-Definitionen. Die log-Objekte führen das eigentliche Logging aus, in dem sie die zuvor definierte Source-, Destination- und Filter-Objekte zu einer Log-Aktion verbinden

log { source(src); filter(f_syslog); destination(syslog); };

log { source(src); source(src1); filter(f_syslog); destination(syslog); };

log { source(src); filter(f_mail); filter(f_info); destination(mailinfo); };

Rsyslog **Quelle: https://www.heise.de/ct/artikel/Erweiterte-Systemueberwachung-mit-rsyslog-846750.html?seite=3**

/etc/rsyslog.conf

/etc/rsyslog.d

/etc/rsyslog.d/default.conf

Aufgabe	Parameter
Meldungen, die zur Authentifizierung gehören, beispielsweise falsche Passwörter.	*auth, authpriv*
Meldungen, die von Cron erzeugt wurden, oder von Prozessen, die von Cron gestartet werden (die Standard-Ausgabe und Stardard-Fehler-Ausgabe werden jedoch von Cron nicht an Syslog gereicht, sondern per EMail verschickt).	*cron*
Meldungen von allgemeinen Diensten, wie zum Beispiel einem FTP-Server	*daemon*
Meldungen des Systemkernels. Sollte von keinem Dienst verwendet werden. Hierzu gehören beispielsweise Hardware-bezogene Meldungen.	*kern*
Meldungen des Drucksystems (Druckerspooler)	*lpr*
Meldungen des Mailsystems (beispielsweise von sendmail und fetchmail).	*mail*
Nur für Syslog-interne Zwecke, sollte nie verwendet werden	*mark*
Meldungen des News-Systems, zum Beispiel eines Newsservers.	*news*
Meldungen von Syslog selbst.	*syslog*
Meldungen von Benutzersystemen wie zum Beispiel eigenen Scripten.	*user*
Meldungen von Unix-Unix-Copy (UUCP wird heute kaum noch verwendet).	*uucp*
Diese sind frei und können nach Belieben verwendet werden. Bei Diensten, bei denen man die zu verwendende Facility einstellen kann, kann man diese verwenden und je nach Bedarf verteilen.	*local 0 bis local 17*

Aufgabe	Parameter
Unwichtige Meldungen, dienen nur zu Debug-Zwecken (Fehlerfindung vor allem bei der Entwicklung)	*debug*
Informative, nicht weiter wichtige Meldungen	*info*
Informative Meldungen, die größere Bedeutung haben als info.	*notice*
Warnungen, also Meldungen, die nicht-fatale Fehler anzeigen.	*warning*
Fehlermeldungen, die kleine Störungen anzeigen.	*err , error*
Kritische (schwerere) Fehler, die beispielsweise Teilausfälle anzeigen.	*crit*
Schwere Fehler, die erhebliche Störungen und Ausfälle anzeigen.	*alert*
Sehr schwere Fehler, die beispielweise den Totalausfall des Systems anzeigen können und schwere Kernelfehler (Hardwareausfälle).	*emerg , panic*

Beispiel für /etc/rsyslog.conf :

auth , authpriv. * /var/log/auth.log
cron.info /var/log/cron.log

Logrotate

/etc/logrotate.conf

/etc/logrotate.d

Firewalld

Firewall Tools

firewall-config (GUI)

firewall-cmd (Command Line)

Konfigurationsdateien

/etc/firewalld/

/etc/sysconfig/network-scripts/ifcfg-xxx

/etc/firewalld/direct.xml

Status Firewall

firewall-cmd –state

firewall-cmd –get-active-zones

firewall-cmd –get-zones

firewall-cmd –get-default-zone

firewall-cmd –get-zone-of-interface=xxxx

firewall-cmd –get-services

Zonen konfigurieren

firewall-cmd –permanent --zone=xxx –add-interface=xxx

firewall-cmd –permanent --zone=xxx –remove-interface=xxx

firewall-cmd –permanent --set-default-zone

firewall-cmd –permanent --zone=xxx –add-service=xxx

firewall-cmd –permanent --zone=xxx –add-port=xxx/tcp

firewall-cmd –permanent --zone=xxx –add-port=xxx/udp

firewall-cmd –reload

Uncomplicated Firewall (UFW)

gufw (GUI)

ufw

Konfigurationsdateien

/etc/sysconfig/ufw

/etc/ufw

/lib/ufw/user.rules

Status Firewall

ufw status

ufw app list

ufw app info „xxx“

Firewall konfigurieren

ufw enable

ufw disable

ufw default allow xxx

ufw default deny xxx

ufw allow xxx (Portnummer oder Dienstname)

ufw deny xxx (Portnummer oder Dienstname)

ufw limit xxx/tcp

Nftables

Quellen: https://wiki.gentoo.org/wiki/Nftables **https://www.linux-community.de/ausgaben/linuxuser/2019/06/verkehrsregeln/2/**

Kommandos

nft	
nft list ruleset -a	
nft list ruleset > firewall.config	***Speichert die Firewallregeln in eine Datei***
nft -f firewall.config	***Liest die Firewallregeln aus der Datei firewall.config ein***

Chains / Ketten

filter	***for filtering packets***
route	***for rerouting packets***
nat	***for performing Network Address Translation. Only the first Packet of a flow hits this chain, making it impossible to use it for filtering***
prerouting	***This is before the routing decision, all packets entering the machine hit this hook***
input	***All packets for the local system hit this hook***
forward	***Packets not for the local system, those that need to be forwarded hit this hook***

Tabellenfamilien

ip

ip6

arp

bridge

inet

netdev

Tabellen

Standardmäßig existieren im Vergleich zu iptables keine Tabellen die Ketten beinhalten. Die Tabellen müssen neu erstellt werden.

Beispiel:

nft add table ip xxx

output	***Packets that originate from the local system hit this hook***
postrouting	***This hook comes after the routing decision has been made, all packets Leaving the machine hit this hook***

Regeln erstellen:

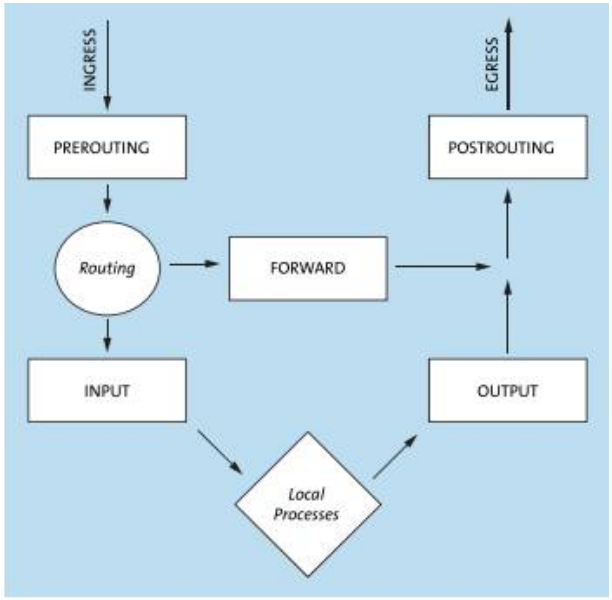
nft add rule ip Tabellenname xxx input tcp dport 22 ct state new,established accept

nft add rule ip Tabellenname xxx input tcp dport { 22, 80, 443 } ct state new,established accept

Aktionen

accept	***Accept the packet and stop the ruleset evaluation***
drop	***Drop the packet and stop the ruleset evaluation***
reject	***Reject the packet with an icmp message***
queue	***Queue the packet to userspace and stop the ruleset evaluation***
continue	
return	***Return from the current chain and continue at the next rule of the last chain. In a base chain it is Equivalent to accept***

Iptables | **Quelle: https://wiki.archlinux.de/title/Iptables** | **https://www.selflinux.org/selflinux/html/iptables03.html**



Graphic Erklärung:

PREROUTING	***Regeln für eingehende Network Address Translations (NAT)***
ROUTING	***Routingregeln***
INPUT	***Regeln für eingehende Verbindungen***
(Local Processes)	***(Verarbeitung der akzeptierten geregelten eingehenden Verbindungen)***
OUTPUT	***Regeln für ausgehende Verbindungen***
POSTROUTING	***Regeln für ausgehende Network Address Translations (NAT)***
	Regeln für geroutete Verbindungen an dahinterliegende Netzwerke
FORWARD	***Iptables -A FORWARD -m state –state NEW -p tcp –dport 80 -i eth0 -o eth2 -j ACCEPT***

Kommandos

iptables

iptables-save

iptables-restore

Tabellen

filter	***INPUT, OUTPUT; FORWARD***
nat	**PREROUTING, OUTPUT, POSTROUTING**
mangle	
raw	**PREROUTING, OUTPUT**

Targets / chains / Ketten

ACCEPT	***Das Paket wird durchgelassen***
DROP	***Das Paket wird ohne Rückmeldung an Absender verworfen***
REJECT	***Das Paket wird verworfen und der Absender erhält Fehlemeldung das das Paket verworfen wurde***
LOG	***Aktiviert das Logging einer Regel und übergibt das Logging z.B an Syslog, Rsyslog etc.***

Beispiel:

iptables -A OUTPUT -p tcp –dport http -d www.testwebseite.de -j RJECT

Multiport Module

Multiport Module --dport --sport	***Akzeptiert eine Reihe von Portnummern, Portnamen***

Beispiel:

iptables – A OUTPUT -p tcp -m state –state NEW,ETABLISHED –deport 80,443 -j ACCEPT

iptables – A OUTPUT -p tcp -m state –state NEW,ETABLISHED –deport http,https -j ACCEPT

Stateful Packet Inspection Module

Module state

Optionen

NEW	***Das Paket etabliert eine neue Verbidnung***
ESTABLISHED	***Das Paket gehört zu einer bestehende Verbindung***
RELATED	***Das Paket baut eine neue Verbindung auf, allerdings wurde diese Verbindung infolge einer bereit Existierenden Verbindung erzeugt***

INVALID ***Es konnte nicht bestimmt werden zu welcher Kategorie das Paket gehört***

Beispiel:

iptables – A OUTPUT -p tcp -m state –state NEW,ETABLISHED –deport 80 -j ACCEPT

Limit Module

Beispiel:

iptables -A INPUT -m state –state NEW -m limit –limit 10/minute -p tcp –dport ssh -j LOG –log-prefix „xxx“

Connection Limit Module

iptables -A FORWARD -d 172.16.1.1 -m state –state NEW -m connlimit -p tcp –dport http –connlimit-above 10 --connlimit-mask 24 -j REJECT

Recent Module

Beispiel:

iptables -A INPUT -m recent –update –name blacklist –seconds 60 -j DROP

iptables -A INPUT -p tcp –dport 445 -m recent –name blacklist –set

Logging

Target LOG

Beispiel:

iptables – A OUTPUT --m state –state NEW,ETABLISHED -p tcp –-deport http,https -j LOG

iptables – A OUTPUT --m state –state NEW,ETABLISHED -p tcp –-deport http,https -j LOG –log-prefix „xxx“

At

Quellen: https://www.debian.org/doc/manuals/debian-handbook/sect.task-scheduling-cron-atd.de.html

Cron

Quellen: https://www.debian.org/doc/manuals/debian-handbook/sect.task-scheduling-cron-atd.de.html

/etc/crontab/

/etc/cron.d/

/var/sppol/cron

/etc/cron.hourly
/etc/cron.daily
/etc/cron.weekly
/etc/cron.monthly

/etc/cron.allow
/etc/cron.deny

Bedeutung	Spalte
gibt an, welche Minute (0-59) das Programm ausgeführt werden soll.	*min*
gibt die Stunde an (0-23)	*hour*
gibt den Tag im Monat an (1-31).	*day*
gibt den Monat an (1-12)	*month*
gibt den Tag der Woche an (0-7 / 0 und 7 bedeuten jeweils Sonntag !)	*weekday*
gibt an, für welchen Benutzer das Kommando ausgeführt wird (meist root).	*user*
enthält das auszuführende Kommando.	*command*

Bedeutung	Code	Kürzel
nach jedem Reboot ausführen	*-*	*@reboot*
einmal im Jahr ausführen	*0 0 1 1 **	*@yearly / @annualy*
einmal pro Monat ausführen	*0 0 1 * **	*@monthly*
einmal pro Woche ausführen	*0 0 * * 0*	*@weekly*
einmal pro Tag ausführen	*0 0 * * **	*@daily*
einmal pro Stunde ausführen	*0 * * * **	*@hourly*

Beispiel für /etc/crontab :

Spaltenaufbau:

min hour day month weekday user command

Jede Nacht um 1:45 Uhr ein Backup ausführen im Benutzerkontext root :

45 1 * * * root /myscripts/backup-site

Anacron

Quellen: https://www.thomas-krenn.com/de/wiki/Anacron

/etc/anacrontab/

/var/spool/anacron

/etc/at.allow

/etc/at.deny

Beispiel für /etc/ancrontab :

Spaltenaufbau:

Anzahl Wiederholungen Verzögerungszeit in Minuten Cronjob-Art Nicewert Kommando

Beispiel:

```
1            5     cron.daily     nice  run-parts  /etc/cron.daily
7           25     cron.weekly    nice  run-parts  /etc/cron.weekly
@monthly    45     cron.monthly   nice  run-parts  /etc/cron.monthly
```

Systemd-Timer			**Quellen: https://wiki.archlinux.de/title/Systemd/Timers**
/etc/systemd/system			

Linux	Windows

Legende:

Fett – Bash Befehl, Kommando, Deamon, Programm, Package
Kursiv – wichtige Verzeichnisdateien nach Distributionen
normaler Text – Alternatives Programm

Anmerkungen:

- Die Namenserklärung des Kommandos kann von der Manpage ggf. abweichen, wenn der Autor der Meinung war, dass dies der besseren Gedächtnisstütze dienlich sein könnte.
- Kommandos können doppelt vorkommen wenn der Autor der Meinung war, dass die erneute Erwähnung hilfreich sein könnte.

Die Tabelle darf frei geteilt und vervielfältigt werden.
Der Urheber der Tabelle muss allerdings zu jederzeit ersichtlich sein:

Urheber: Lars Kammeier
Erstenstellung: 10.09.2020

Shells / Kommandozeilen:

bash => **bourne again shell**	
csh => **c-shell**	**DOS**
tcsh	**CMD**
zsh => **z-shell**	**PowerShell**
ksh	
rsh => **remote shell**	

Admintools:

screen
tmux

Variablen

$$ => **Momentane Prozess ID**	
$? => **Returncode des letzten Kommandos**	
$# => **Anzahl der Übergabeparameter**	
$1 $2 $3 .. $9 => **einzugebende Variablen**	
$0 => **Name des Scripts / Programmname**	
#! => **Shebangzeile / Programmauswahl**	
!n => **!Name des Kommandos in der Historie**	

Text & Sourcecode Editoren:

vi => **viewer**	
vim => **viewer improved**	**Editor**
nano => **another editor**	**Notepad**
GNU Emacs	
GNU zile	
jed => **John E. Davis Text Editor**	
jmacs / JOE => **Joes Own Editor**	
jove => **Jonathans Own Version of Emacs**	
gedit => **Gnome editor**	
Atom	
VSCode	

Manpages und Kommandospeicherorte:

man => **manual page for linux commands**	
which => **which location is the command stored**	**cmd /help /?**
whatis => **what is this command used for**	**PowerShell Get-help**
whereis => **where is the binary, source and manual page files stored**	

Libraries:

shared libraries.so	**Dynamic Link Libraries.dll**
ldd => **library dependencies**	
ldconfig => **library dependencies config**	
sash	
file => **show file type**	

Such & Filterwerkzeuge:

which => **which location is the command stored**	
whatis => **what is this command used for**	
whereis => **where is the binary, source and manual page files stored**	
locate	
find => **find files, directories which matches search cases**	
grep => **search for specific matches in files**	
pgrep => **process grep**	
cat	**Explorersuche**
bzcat => **bzip2 cat**	
xzcat => **xz cat**	
zcat => **gzip cat**	
head => **Kopfzeile der Datei + n-Zeilen**	
tail => **Fußzeile der Datei + n-Zeilen**	
cut => **Ausschneiden (Gesamt oder Teilstücke)**	
paste => **Einfügen des Inhalts**	
sort => **Sortierung der Ansicht (Alphabetisch usw.)**	
uniq => **Doppelter Inhalt ausblenden**	
wc => **word count**	
nl => **number line**	
tr => **translate**	
sed => **streaming editor**	

Backup:

wichtige Backupverzeichnisse: **Windows Sicherung**

/boot /etc /var /lib /sbin /bin /opt
/root /home /usr

sync => **synchronized and write temporare changes to the disk**

rsync

rsync => **write stored data changes to disk**
/etc/rsyncd.conf

Graphical Rsync (Grsync) => **synchronized 1:1 copies of hirachical folder structures**

dd => **diskdump**
od => **oktal dump**
tar => **tape archiver**
mt => **magnetic tape operation**

Client-Backup Programme:

Deja Dup (GUI-Programm auf Basis von duplicity arbeitet auf Dateiebene)

Back in Time (GUI-Programm auf Basis von rsync)
/home/username/.config/backintime/config

Duplicati (Web-GUI-Programm arbeitet auf Blockebene)

http://localhost:8200 / duplicati-cli
/home/username/.config/autostart
/etc/duplicati/config

sqlitebrowser
/home/username/.config/Duplicati/Duplicati-server.sqlite

Server-Backup Programme:

Inkrementell Backup Programme

Borg Backup (GUI-Frontends verfügbar)

borg init
/home/username/.config/borg
/home/username/.cache/borg
borg create
borg list
borg extract
borg delete

Linux	Windows

Bootsektor, Festplatten und Dateisysteme

BIOS => **Basic Input Output System**	**BIOS - Basic Input Output System**
UEFI => **Unified Extensible Firmware Interface**	**UEFI - Unified Extensible Firmware Interface**
MBR => **Master Boot Record**	**MBR - Master Boot Record**
GPT => **Globally Unique Identifier Partition Table**	**GPT - Globally Unique Identifier Partition Table**
hdparm => **hard disk parameters set and get**	
sdparm => **scsi disk parameters set and get**	
nvme => **nvme storage command line interface utility**	
fstrim => **filesystem trim and discard unused blocks on ssd devices**	

IDE-Bus:
*/dev/hd**

iSCSI:
*/dev/sd**

SSD / NVME:
*/dev/nvme0n**

lsblk => **list block devices**	
blkid => **block device id**	
/dev/disk/by-uuid	
sync => **synchronized and write temporare changes to the disk**	
fdisk => **format disk partition table**	
cfdisk => **cursor based format disk partiton table**	
gdisk => **GUID disk creator**	
parted => **partition editor**	
partprobe	
mkfs => **make file systems**	
mk2fs => **make partitions to filesystems (-c Overwrite Partition !)**	
mkswap => **make SWAP-Date / Partition**	
fsck / e2fsck => **file checker**	
/etc/fstab	
mount => **connect partitions/ portable disks to system read or read-write**	**Computerverwaltung**
umount => **disconnect partitions / portable disks from the system**	
/etc/fstab	
/etc/mtab	
/proc/mounts	

autofs package: (automatic mount)
/etc/auto.master
/etc/auto/mountpoints

Dateisysteme:

ext1, ext2, ext3, ext4

resize2fs	
tune2fs => **tuneable to filesystem parameters**	
debugfs => **file system debugger**	
dump2fs => **file system dumper**	

XFS

xfs_info	
xfs_fsr	
xfs_check	
xfs_repair	
xfs_dump	
xfsrestore	**NTFS**
	ReFs
Btrfs-tools package:	**FAT32**
btrfs => **btree file system**	**ExFAT**
btrfs-convert => **convert to btrfs**	
Fat	
ExFat => **extended FAT**	

LVM – Logical Volume Manager / Package lvm2 (Kernelmodule dm_mod)

vgscan -v	
/etc/lvm/cache/.cache	
/etc/lvm/lvm.conf	
pvcreate => **create physical volume for LVM**	
vgcreate => **create volume group of the bottom of the physical volume**	
mkfs => **make file systems**	
resize2fs => **resize the file system with current storage**	
lvreduce => **reduce the number of the logival volumes**	
vgreduce => **reduce the number of the volume groups**	
lvcreate => **create a logical volume**	

ZFS - Zettabyte File System

Redundant Arrays of Inexpensice Disks (RAID) / Internet Small Computer Systems Interface (iSCSI) / Storage Attached Network (SAN)

hdparm => **hard disk parameters set and get**	
sdparm => **scsi disk parameters set and get**	**Computerverwaltung**
	Systeminformationen
nvme => **nvme storage command line interface utility**	
fstrim => **filesystem trim and discard unused blocks on ssd devices**	

Software-RAID:

/etc/fstab	
/etc/mdadm/mdadm.conf	=> *configuration file for software raids → mdadm –examine –scan >> mdadm.conf*
/proc/mdstat	=> *contain status information of created raids*
mdadm	=> **multiple device administrator manager for raids**

Troubelshooting **iSCSI-Assistent**
Windows Server Datei und Speicherdienste

/usr/share/mdadm/check-array (Debian)	=> *raid integrity check*
/etc/cron.d/raid-check (RHEL, Fedora, CentOS)	=> *raid integrity check*
sfdisk	=> **clone raid information / partition table of mbr disks to new disk**
sgdisk	=> **clone raid information / partition table of gpt disks to new disk**
md_mod	
RAID-Hexcode → fd	

iSCSI:

iSCSI – Target:

/etc/default/iscsitarget → True	
/etc/ietd/ietd.conf	
targetcli	

iSCSI-Initiator:

eto/iscsi/iscsid.conf → automatic

Iscsiadm	=> **iscsi administration manager to detect and connect to iscsi partitions / disks**
scsi_id	=> **show iscsi information regarding to partitions / disks**

Bootmanager

Bootmanager konfigurieren und installieren:

GRUB – Legacy (Grand Unified Bootloader Legacy):

grub-install	
/boot/grub/menu.lst	=> *central configuration file for grub-legacy*
/boot/grub/device.map	=> *containes the location of the bootloader on the disk*
/etc/grub.d	

GRUB – Legacy (Grand Unified Bootloader Legacy) absichern:

grub-md5-crypt	=> **create password hash to secure bootloader password protected**
/boot/grub/menu.lst	=> *configuration file for grub-legacy*

GRUB 2 (Grand Unified Bootloader 2): **erweiterte Starteinstellungen**
(Shift-Taste + Neustart → UEFI)

grub-install / grub2-install	(Debian / RHEL, Fedora, CentOS, OpenSuse)
/boot/grub/grub.cfg	=> *auto configuration file do not edit*
/boot/grub2/grub.cfg	=> *auto configuration file do not edit*
*/etc/grub.d/**	=> *directory contains configuration files from grub2*
/etc/default/grub	=> *file to making changes*
grub-mkconfig / grub2-mkconfig	=> **create bootloader configuration file grub.cfg**
update-grub / update-grub2	=> **update bootloader configuration file grub.cfg**

GRUB 2 (Grand Unified Bootloader 2) Konfiguration und Menü anpassen:

/etc/grub.d/40_custom.	=> *customized options and boot menu*
/boot/grub/custom.cfg (Debian)	
/boot/grub2/custom.cfg (RHEL, Fedora, CentOS, OpenSuse)	

GRUB 2 (Grand Unified Bootloader 2) absichern:

Linux	Windows

Energieverwaltung

acpi => **Advanced Configuration and Power Interface**
dmesg |grep -i acpi
powertop
tlp

Datum & Zeiteinstellung:

date
Timezone – Variables
/etc/timezone
/etc/localtime
/usr/share/zoneinfo
/usr/bin/locale

uptime => **shows how long the machine is up since last power/off** **Datum & Uhrzeit**
tzselect => **timezones select (view timezones)** **Region**

hwclock – hardware clock

/etc/ntp.conf
/etc/ntp.drift

ntpdate – network time protocol date (Online NTP-Serverpool)

ntpd => **ntp - deamon**
/etc/ntp.conf
/etc/ntp.drift
ntp-keygen
ntpq => **network time protocol query**

chrony - synchronize time config

/etc/chrony.conf

Systemd-timesyncd.service

etc/systemd/timesyncd.conf
timedatectl => **time and date control**

Open NTPD

Tastaturlayout:

dpkg-reconfigure keyboard-configuration (Debian)
/etc/default/keyboard

localectl list-keymaps (RHEL, Fedora, CentOS)
localectl set-keymaps
/etc/vconsole.conf
/etc/X11/xorg.conf.d/00-keyboard.conf

grub2-mkconfig -o /boot/grub2/grub.cfg

(OpenSuse)
/etc/sysconfig/keyboard
/etc/X11/xorg.conf.d/00-keyboard.conf

Schriftart:

/etc/default/console-setup (Debian)

/etc/vconsole.conf (RHEL, Fedora, CentOS)

/etc/sysconfig/console (OpenSuse)

Netzwerkkonfiguration / DNS-Konfiguration / Troubelshooting

/etc/services => *contain port function and service information*

Netzwerkkonfiguration: **Netzwerk und Freigabecenter**

Temporäre Netzwerkkonfiguration

network-managerd => **network manager (default network manager on most distributions)**
nmcli => **network manager command line**
nmtui => **network manager textual user interface**

systemd-networkd (networkctl) => **systemd network manager**

ip => **interface configuration of network interfaces / ipaddress, routes (replacement of ifconfig, route)**
ifconfig => **interface configuration of network interfaces / ip-address, routes**
route => **add routes to the route table of the machine**

ifup => **network interface up / aktivate**
ifdown => **network interface down (deactivate**
ifquery => **network interface query / status**

iw => **interfaces wireless (replacement of iwconfig)**
iwconfig => **interfaces wireless configuration**
iwlist => **interfaces wireless list**
iwevent => **interface wireless event**

Permanente Netzwerkkonfiguration

/etc/NetworkManager/NetworkManager.conf => *configuration file for the network manager behaviour*
/etc/NetworkManager/conf.d

/etc/systemd/network/<Networkadaptername> => *configuration file set configuration settings for network adapters*

/etc/network/interfaces (Debian) => *configuration file for permanent network adapter configuration*
/etc/sysconfig/network-scripts/<Networkadaptername> (RHEL, Fedora, CentOS) => contain configuration file per network adapter for permanent network configuration
/etc/sysconfig/network/<Networkadaptername> (OpenSuse) => contain configuration file per network adapter for permanent network configuration

Zeroconf (Apple) / Avahi (Linux)

Avahi => **show all machines and ressources like (file-shares, ssh etc.) also private auto configuration**
/etc/avahi/avahi-daemon.conf => *configuration file for avahi*

DNS: **nslookup**
C:\Windows\System32\drivers\etc\hosts

hostnamectl => **hostname control**
hostname => **show host name**
/etc/hosts => *configuration file for hostname, hostalias and known hosts*
/etc/resolv.conf => *configuration file for dns-servers*
/etc/nsswitch.conf => *configuration file for authentication databases*

dig => **domain information groper**
nslookup => **name server look up**
getent => **get entree (user, group) of a database**
resolvectl => **resolve control of dns**

Troubelshooting: **ipconfig**
tracert
arp

ping / ping6 => **testing client response of ping packages** **ping**
traceroute / traceroute6 => **trace the route of packages taken from an ip network to a host** **ping6**
tracepath / tracepath6 => **traces path to a network host discovering MTU along this path** **nslookup**
arp => **shows arp information e.g arp table** **netstat**

ss => **socket statistics (new version of netstat)**
netstat => **network statistics of network connections and open ports**
netcat / nc /ncat => **network controled swiss army knife (unix domain sockets, port scan, simple data transfer)**
Nmap => **network mapper for advanced network scans & exploration, security auditing, etc**
tcpdump => **network sniffer for tcp, udp and icmp packages**

Firewall

/etc/services => *contain port function and service information*

Firewalls auf Netfilterbasis

Interface Network Protection Tables (iptables) **Windows-Firewall**
Drittanbietersoftware

create bash scripts for iptables firewall using Sysvinit or systemd syntax

iptables / ip6tables => **set temporary iptable rules regarding of ip version**
iptables-save / ip6tables-save => **safe iptables and or ip6tables rules to output or file using as firewall configuration**
iptables-restore / ip6tables-restore => **restore iptables and or ip6tables from file to firewall using as firewall configuration**
arptables
ebtables

Netfilter Tables (nftables):

/etc/nftables.conf => default configuration file for nftables

nft => **netfilter tables (replacement of iptables)**
nft-list
nft-export

rdiff-backup

rdiff-backup
/home/username/home-backup

duplicity

rsnapshot
/etc/rsnapshot.conf
/var/cache/rsnapshot/ - Default-Speicherort*
/etc/cron.d/rsnapshot

Tartarus

Komprimierung / Archivierung:

tar	**=> tape archiver**	**zip**
gzip	**=> g-zipper**	**7zip**
gunzip	**=> g-unzipper**	
lzop	**=> less slow zip compression and expand**	
bzip2	**=> b2-zipper**	
bunzip2	**=> b2-unzipper**	
zip	**=> zipper**	
unzip	**=> unzipper**	
zipinfo	**=> zipper information**	
xz	**=> x-zipper**	
unxz	**=> x-unzipper**	
cpio	**=> copy files in and out from archives**	

Barrierefreiheit:

Screenreader → Orca	
Braillezeile	
Bildschirmlupe	**Bildschirmlupe**
Bildschirmtastatur	**Bildschirmtastatur**
Gesten	**Cortana**
Spracherkennung	
Eyetracker	

Drucker:

Druck-Server

CUPS – Common Unix Printing Solution GUI

http://localhost:631 — **Geräte und Drucker**, **Spooler dienst**

CUPS – Common Unix Printing Solution

/home/username/.cups/name.ppd (KDE)

/etc/printcap => *old configuration file for printers show print waiting list*
/etc/cups/cupsd.conf => *configuration file for cups settings and admin website / Location & Operation Policy*
/etc/cups/printers.conf => *definition of all printers also print quotas possible*

/etc/cups/lpoptions => *configuration file to make changes which are different to the cupsd.conf*

/etc/cups/classes.conf => *contain information of print groups (number of printers as one class)*

/etc/cups/ppd/name.ppd => *configuration file for printers, printers options e.g pages, resolution etc.*
/var/cache/cups/.ppd* => *configuration file for all printers / all configuration information are in ppds.dat*

/usr/share/cups/mime/mime.types => *list of all printable filetypes*
/usr/share/cups/mime/mime.convs => *list of files types and programms which can handel this file types*
*/usr/lib/cups/filter/** => *contain rules for printing document types*

/var/spool/cups/ => caching print jobs

lpinfo => **list information about all available printers and print drivers of this system**
lpstat => **show status of all available cups printers**
lpoptions => **edit printer options of cups printers**

lpadmin => **line printer administration (create modify or delete printer or printer configuration)**

Drucker-Client

/home/username/.cups/lpoptions => *user specific configuration settings for printer*

lp / lpr => **line printer print file**
/var/spool/cups/ => caching print jobs
lpq => **line printer queue show print job information**
lprm => **line printer remove print job**

lpc => **line printer configuration shell**

ISO-Dateien erstellen

mkisofs => **ISO Dateisystem erstellen**
cdrecord => **ISO-Dateien auf CD / DVD schreiben**
wodim => **abgespeckte Alternative zu cdrecord**

Sonstiges:

script => **startet eine Aufzeichnung, Beenden mit „ exit "** — **Schrittaufzeichnung**

xmlto => **Wandelt Dokumente in HTML-Dokumente um**
passivetex => **Wandelt Dokumente in PDF-Dokumente um**

Adminmeldungen:
/etc/issue
/etc/issue.net
/etc/motd
wall => **erzeugt eine textbasierte Adminmeldung**
mesg n => **unterbindet die Anzeige textbasierter Adminmeldungen**

shutdown -k
systemctl

Router

/etc/sysctl.conf
/etc/ipv6/conf/
/etc/services/

Troubelshooting:

ping / ping6 => **testing client response of ping packages**
traceroute / traceroute6 => **trace the route of packages taken from an ip network to a host**
tracepath / tracepath6 => **traces path to a network host discovering MTU along this path**
arp => **shows arp information e.g arp table**

ss => **socket statistics (new version of netstat)**
netstat => **network statistics of network connections and open ports**
netcat /nc /ncat => **network controled swiss army knife (unix domain sockets, port scan, simple data transfer)**
nmap => **network mapper for advanced network scans & exploration, security audiling, etc**
tcpdump => **network sniffer for tcp, udp and icmp packages**

Dynamic Host Configuration Protocol (DHCP)-Server

DHCP-Server

/etc/dhcp3/dhcp.conf (Debian) => configuration file for dhcp server
/etc/dhcp.conf (RHEL, Fedora, CentOS, OpenSuse) => configuration file for dhcp server

/var/log/lmessages
/var/log/syslog
/var/log/dbamon.log

Leasvorgang

/var/lib/dhcp3/dhcpd.leases (Debian) => contain dhcp leases of managed clients
/var/lib/dhcpd/dhcpd.leases (RHEL, Fedora, CentOS, OpenSuse) => contain dhcp leases of managed clients
/var/db/dhcpd.leases (Internet System Consortium) => contain dhcp leases of managed clients

DHCP-Relay-Agent

/usr/sbin/dhcrelay -i <Networkcardname> <DHCP-Server IP> => **sends dhcp requests to the dhcp server**

Router Advertisement

/etc/radvd.conf => configuration file for router ipv6 leasing

DHCP-Client

/etc/grub.d/40_custom.

grub-mkpasswd-pbkdf2 => **create password hash to secure bootloader menu**

GRUB-Module:

/boot/grub/i386-pc => contain grub loadable modules
/boot/grub2/i386-pc => contain grub loadable modules

insmod => **install module from driver database to bootloader**
rmmod => **remove module from bootloader**

efibootmgr
/boot/efi/EFI/name/grub.cfg
/boot/efi/EFI/name/grubx64.efi

Alternative Bootloader:

LILO	
SYSLINUX	=> Startfähige CDs, USB-Images
ISOLINUX	=> Erstellt startfähige CDs, Disketten
Isohybrid	=> Erweiterung für ISOLINUX zum hinzufügen eines MBR für USB
EXTLINUX	=> Erstellen startfähiger CDs, USB-Sticks für Linux Dateisysteme
PXELINUX	=> Netzwerkboot von Betriebssystemen
Shim	=> Zum Aktivieren oder Deaktivieren von UEFI Secure Boot
Systemd-Boot	=> Erstellen und Ausführen von EFI-Images
U-Boot	=> Genutzt für Microcontroller & Embedded Systems

Early userspace / Initrd (initial ram disk) / initramfs - CPIO-Archiv:

Wird nicht benötigt wenn alle benötigten Treiber im Kernel integriert sind – Bei Distributionen oft nicht der Fall

Debian:

mkinitramfs => **make initial ram file system**
/etc/initramfs-tools/initramfs.conf => configuration file
/etc/initramfs-tools/initramfs.conf.d/
*/etc/initramfs-tools/modules/** => directory contains modules to create initial ram file system

update-initramfs => **update initial ram file system**

lsinitramfs => **list content of initial ram file system image**
unmkinitramfs => **unextract make initial ram file system**

RHEL, CentOS, Fedora, OpenSUSE

dracut
/etc/dracut.conf

mkinitrd (CentOS, OpenSUSE)
/etc/sysconfig/kernel

initrd (initial ram disk) manuell modifizieren:
/boot/initrd.img → entpacken, Konfiguration anpassen, mit cpio wieder packen

Kernel & Module

Kernelmodule laden, entladen und Informationen auslesen:

/lib/modules/kernel-version/
cat /proc/modules

kmod => **kernel modules auto loader**
/etc/modprobe.conf
/etc/modprobe.d/.conf* => contain kernel module configuration files
/lib/modules/KernelNummer/

insmod => **loading in module**
rmmod => **remove loaded module**
modprobe => **module probleme resolver for dependencies modules**
/lib/modules/modules.alias
/etc/modprobe.conf
/etc/modprobe.d/config.conf => configuration file for loading drivers of the kernel for the system

sysctl => **system control for customized kernel parameter settings**
/etc/sysctl.conf => configuration file storing configured kernel parameter settings

uname => **print system and kernel information**
lsmod => **list modules**
modinfo => **show modul information**
depmod => **show dependencies of modules**
/proc/sys/kernel

dmesg => **diagnostic kernel messages**

strace => **trace system calls and signals**
trace-cmd => **trace command which trace system calls and signals**

strings

Kernel, Module & Treiber Kompilierung

wget => **website get content**
/usr/src
/usr/src/linux/Documentation
/usr/src/linux/arch/x86/boot/bzImage

Alte Kompilierungsschritte bis Kernel Vesion 2.6:

make clean / make mrproper
make config => make question ask configured kernel configuration file by plain text interface
make depend => make dependencies of the kernel configuration file
make bzImage
make zImage

make modules => make / built kernel modules from .config file marked with m for modules
make modules_install => install maked / build modules to the system

grub-mkconfig / grub2-mkconfig = update-grub / update-grub2

Neue Kompilierungsschritte ab Kernel Version 2.6:

gcc => **Gnu Compiler Collection**

Möglichkeiten der Kernelkonfiguration:

make mrproper => **clean not necessary files (use it on downloaded kernel and /usr/src)**
/usr/src/

/boot/config-x.x.x.x.config

make oldconfig / cp .config => **make configuration file based of the old kernel configuration file and ask if settings are different**
make olddefconfig => **make configuration file based of the old kernel configuration file and answer with default settings if settings are different**
make listnewconfig => **shows new config symbols**

make menuconfig => **make menu configured kernel configuration file**
make config => **make question ask configured kernel configuration file by plain text interface**
make nconfig => **make enhanced text based menu configured kernel configuration file**
make defconfig => **make default configured kernel configuration file**

make xconfig => **make X-window / Qt based tool configured kernel configuration file**
make gconfig => **make GTK+ based tool configured kernel configuration file**
make localmodconfig => **make local modul configuration kernel configuration file by only current running modules and plugged in devices**

time make all

make => **make / built the linux kernel with the config file**

Module konfigurieren und installieren:

make modules => **make / built kernel modules from .config file marked with m for modules**
make modules_install => **install maked / build modules to the system**

make install => **make install the builded kernel to the system**

grub-mkconfig / grub2-mkconfig = update-grub / update-grub2

zusätzliche Kernelmodule für Software / Hardwarekomponenten:
dkms => **Dynamic Kernel Module Support**

Fehlerbehebung:

make clean
make mrproper

Kernel direkt tauschen:

kexec

SysVInit – Upstart – systemd – Prozess

Shutdown => **shutdown the system compatible with sysvinit and systemd**
reboot => **reboot the system compatible with sysvinit and systemd**
halt = shutdown -h => **stop the system compatible with sysvinit and systemd**

Distributionsspezifische Firewalls / Higher Level Table Interpreter

Firewall Deamon (firewalld) (RHEL, Fedora, CentOS, OpenSuse)

*/etc/firewalld/** => *configuration files for firewalld rules*
*/usr/lib/firewalld/** => *configuration files for firewalld rules*
*/etc/sysconfig/network-scripts/** => networkcard configuration file to include firewalld zone rules
/etc/firewalld/direct.xml => *configuration file to include iptables rules in firewalld*

firewall-cmd => **firewall command line for temporary and persistent firewalld rules**

firewall-config / YasT-Module => **graphical user interface for firewalld** (Yast-Module OpenSuse)

Uncomplicated Firewall (UFW) (Ubuntu)

*/etc/ufw/** => configuration files for application rules e.g applications.d
/etc/sysconfig/ufw => configuration file for ufw
/lib/ufw/user.rules / user6.rules => *contain own user specific rules*
ufw => **uncomplicated firewall**

gufw => **graphical interface for universal firewall**

Alternativen:

pfsense

Firewall Builder

Systemprotokollierung:

tail -f

dmesg => **detect and show kernel ring buffer messages**
/proc/kmsg

logrotate => **compress and rotate logfiles**
/etc/logrotate.conf => *default configuration file*
*/etc/logrotate.d/** => *contains specific settings for programms using logrotate*

logger => **enter messages into the system log**

Systemd – Journald

journalctl => **journal control**
/etc/systemd/journald.conf => *configuration file for log files*
*/etc/systemd/journald.conf.d/**
*/run/lib/systemd/journald.conf.d/**
/var/log/journal => *contain log messages*

systemd-cat => **To view the journal database**
/var/log/syslog
/var/log/messages
/var/log/boot.log
/var/log/journal => *contain log messages*

System Logging Deamon (syslogd)

/etc/syslog.conf => *configuration file for the system logs also for forwading to central log server*
/etc/default/syslogd => *enhanced configuration file for getting network logs from other servers*
/var/log/syslog (Debian)
/var/log/messages (Redheat, Fedora, CentOS, OpenSUSE)
*/var/log/** => *folder for syslog logs for all services*

Rocket-fast system for log processing (rsyslog) (default Debian, RHEL, Fedora, CentOS, OpenSuse)

/etc/rsyslog.conf => *configuration file for log files*
/etc/rsyslog.d/mysql.conf => *configuration file for central log database*

Syslog new generation (syslog-ng)

/etc/syslog-ng/syslog-ng.conf => *configuration file for log files*

Logwatch

logwatch => **customizable log analysis system**
/usr/share/logwatch/default.conf => *default configuration settings for sending logging information via mail*
/usr/share/logwatch/logwatch.conf => *global default settings*
*/usr/share/logwatch/default.conf/services/** => *default configuration settings for services*

*/etc/logwatch/** => *customized configuration for services*

Logsurfer – process logfiles and perform certain actions

smartmontools package: (Self-Monitoring, Analysis and Reporting Technology)

smartctl - SMART Control
smartd - SMART Deamon
etc/default/smartmontools
etc/smartd.conf

cockpit (Web-Monitoring Tool)

Paketmanager:

Debian => **dpkg, apt, apt-get, apt-cache search**
RedHat, Fedora => **rpm, yum** — **Windows Store, Drittherstellersoftwareseiten**
Open Suse => **zypper**

Flatpak
Snap

Drittherstellersoftwareseiten (Kompilierung)

Softwarekompilierung

wget => **website get content**
/usr/src
/usr/src/linux/Documentation
/usr/src/linux/arch/x86/boot/bzImage

Speicherort:

/usr/src - Möglliches Verzeichnis zum entpacken von Softwareprogrammcodepaketen / Default-Installationsort für kompilierte Software

tar -xzvf => **tape archiver**
gunzip => **g-unzipper**
bunzip2 => **b2-unzipper**
unxz => **un x-zipper**
unzip => **unzipper**

configure / ./configure => **create the makefile for the software**

make => **make / built the linux program with the makefile (compiling)**
make install => **make install the compiled software to the system**

Berechtigungsverwaltung (Autorisierung)

id => **show user id (uid) or group id (gid) of the current user**
groups => **show group memeberships of the current user**
ls => **list files directories and other important informations**

Benutzerverwaltung

useradd => **add new user or system - user to the system**
/etc/passwd
/etc/shadow
usermod => **user modification e.g new group memebership and user settings**
userdel => **user delete**

newgrp => **new group membership which mean change temporarily primary with secondary group**
chown => **change ownership and / or group membership of the file or file hirachy**

Gruppenverwaltung — **AGDLP (NTFS, ACL, SharedFolders)**, **Windows Active Directory**, **Lokale Benutzerverwaltung**, **Gruppenrichtlinien**, **Ldap**

groupadd => **add new group to the system**
/etc/gshadow
groupmod => **group modification e.g gid or name**
groupdel => **group delete**

chgrp => **change group membership for file or file hirachy**

Berechtigungen konfigurieren

chmod => **change modus bits for file permissions (e.g 644 = rw - r- - r- -)**
umask => **unified file mode creation mask for default file permissions (e.g 027 = rwx r x- - - -)**

dhclient => dhcp-client configuration for dhcp lease by the server
/etc/resolv.conf => configuration file for dns-servers

Alternativen

dhcpcd
pump

Linux	Windows

Domain Name Service (DNS) – Server

hostnamectl – hostname control
hostname
/etc/hosts
/etc/resolv.conf
/etc/nsswitch.conf

bind / bind9 package:
/etc/named.conf (Fedora / ReadHead)
/var/named/named.ca (Fedora / ReadHead)
/etc/bind/named.conf (Debian)
/etc/bind/db.root (Debian)
named-checkconf
named-compilezone

dig – domain information groper
nslookup - name server look up
getent – get entree

DNS Sicherheit:
/etc/named.conf

DNSSEC – DNS Security Extensions:
/etc/named.conf → dnssec-enable yes; dnssec-validation yes;
dnssec-keygen
dnssec-signzone

Alternative DNS-Server:
dnsmasq
djbdns
PowerDNS

Webserver (Apache / Nginx)

http://localhost / http://servername/

Konfiguration (Apache) — **Microsoft Internet Informations Service (IIS)**

*/var/www/** (Debian, RHEL, Fedora, CentOS) => *document root directory*
/srv/www/htdocs (OpenSuse) => *document root directory*

Debian

/etc/apache2/apache2.conf => default configuration file (virtual hosts, authentication, file permissions, modules)
*/etc/apache2/conf.d/** => additional configuration files (eg. ssl packages, php packages etc)
/etc/apache2/httpd.conf => *old default configuration file*
/etc/apache2/ports.conf => *monitored and used ports for virtual host websites, include modules eg. ssl*

/etc/apache2/conf-available/ => *available configuration files*
/etc/apache2/conf-enabled/.conf* => *links to activated configuration files*

/etc/apache2/sites-available/ => *available sites (virtual hosts)*
/etc/apache2/sites-enabled/.conf* => *links to sites-available as activated virtual host websites*
/etc/apache2/envvars => *contain environment variables*

/etc/apache2/mods-available/ => *available additional modules*
/etc/apache2/mods-enabled/.conf* => *links to activated additional modules and configuration files*

apachectl => **apache control (start stop apache service etc.)**

a2enmod => **add module to mods-enabled directory (create link to activate module)**
a2dismod => **earase module to mods-enabled directory (remove link to disable module)**

a2ensite => **add virtual host to sites-enabled (create link)**
a2dissite => **erase virtual host to site enabled (remove link)**

RHEL, Fedora, CentOS

/etc/httpd/conf/httpd.conf => default configuration file (virtual hosts, authentication, file permissions, modules)
/etc/httpd/conf.d/.conf* => additional configuration files (eg. ssl packages, php packages virtual hosts etc)

/etc/httpd/conf/magic => mime-configuration (mod_mime)
/etc/httpd/conf.d/ssl.conf => configuration file for ssl listen ports

apachectl / httpd => **apache control (start stop apache service etc.)**
apache2 => **apache http protocol server to show and configure apache configuration options**

OpenSuse

/etc/apache2/httpd.conf => default configuration file (virtual hosts, authentication, file permissions, modules)
/etc/apache2/.conf* => global configuration files
/etc/apache2/conf.d/.conf* => additional configuration files (eg. ssl packages, php packages etc)
/etc/apache2/sysconfig.d/.conf* => system configuration files

/etc/apache2/vhosts.d/.conf* => websites (virtual hosts)
/etc/sysconfig/apache2 => default configurations
/etc/apache2/listen.conf => configuration file for default listen ports

apachectl / httpd => **apache control (start stop apache service etc.)**
apache2 => **apache http protocol server to show and configure apache configuration options**

a2enmod => **add module to mods-enabled directory (create link to activate module)**
a2dismod => **earase module to mods-enabled directory (remove link to disable module)**

Virtuelle Hosts Konfiguration

add <VirtualHost> Section into distribution configuration files for virtual hosts

/etc/apache2/sites-available/ (Debian) => *available sites (virtual hosts)*
/etc/httpd/conf.d/.conf* (RHEL, Fedora, CentOS) => additional configuration files (eg. ssl packages, php packages virtual hosts etc)
/etc/apache2/vhosts.d/.conf* (OpenSuse) => websites (virtual hosts)

Verzeichnisberechtigungen konfigurieren (lokal)

add <Directory> Section to apache configuration files or virtual host configuration files for specific access control (also inherience)

Authentifizierung konfigurieren (Server lokal)

/path/to/directory/.htaccess => creating file into selected directory to configure local user authentication

htpasswd (password clear-text-transfer) => **authentication passwd (create passwd file for authentication)**
htdigest (password digest encryption transfer) => **authentication passwd (create passwd file for authentication)**

Authentifizierung und Verzeichnisberechtigungen konfigurieren (Kerberos / LDAP)

module → libapache2-mod-authkerb
module → authnz_ldap

/path/to/directory/.htaccess => creating file into selected directory to configure local user authentication

Protokollierung:

*/var/log/apache2/** (Debian, OpenSuse)
*/var/log/httpd/** (RHEL, Fedora, CentOS)

HTTPS / SSL-TLS Konfiguration:

/etc/apache2/ports.conf (Debian) => *monitored and used ports for virtual host websites, include modules eg. ssl*
/etc/httpd/conf.d/ssl.conf (RHEL, Fedora,CentOS) => configuration file for ssl listen ports
/etc/apache2/listen.conf (OpenSuse) => configuration file for default listen ports, include modules

For certificate process see section openssl

Nginx-Webserver:

/etc/nginx/nginx.conf => *default configuration file*

/etc/nginx/sites-available/ => *available sites (virtual hosts)*
/etc/nginx/sites-enabled/ => *links to sites-available as activated virtual host websites*

Virtuelle Hosts Konfiguration

add <server> section into distribution configuration files for virtual hosts

/etc/nginx/sites-available/ => *available sites (virtual hosts)*
/etc/nginx/sites-enabled/ => *links to sites-available as activated virtual host websites*

Webserver Erweiterungen

GoAccess (Webseitenstatistiken)

SysVinit-Prozess (System-Five):

/sbin/init => first / mother process
/etc/inittab => *init configuration file → initialising /etc/rc.d/rc or /etc/init.d/rc script*
/etc/init.d.conf => configuration file for services if necessary

telinit -q / init - **reload init configuration file and change system runlevel**
runlevel - **shows current system runlevel and the system runlevel before**
telinit / init - **change the system runlevel**

Runlevel konfigurieren:

*/etc/rc.d/** (Debian) => defined services for the different runlevels
*/etc/init.d/rc.d/** (OpenSuse) => defined services for the different runlevels
*/etc/rc.d/rc.d/** (RedHat, Fedora, CentOS) => defined services for the different runlevels

update – rc.d (Debian) => **change services for runlevels**
insserv (OpenSuse) => **change services for runlevels**
chkconfig quota (RHEL, Fedora, CentOS) => **change services for runlevels**
chkconfig -l (RHEL, Fedora, CentOS)

Bootscripte:

/etc/init.d/rcS (Debian) => boot script for general settings (clock, mounts, troubelshooting etc)
/etc/init.d/boot (OpenSuse) => boot script for general settings (clock, mounts, troubelshooting etc)
/etc/rc.d/init.d/boot (RedHat, Fedora, CentOS) => boot script for general settings (clock, mounts, troubelshooting etc)

Dienststcripte:

*/etc/init.d/** (Debian, OpenSuse) => scripts to configure services status
*/etc/rc.d/init.d/** (RedHat, Fedora, CentOS) => scripts to configure services status

Upstart-Prozess:

/etc/init/.conf* => contains the runlevel configuration files for the services
initctl => **init control for interacting with the upstart process**

Systemd-Prozess:

Unit-Dateien:

/etc/systemd/system/.service* => *contain configuration files e.g example.service or example.d/local.conf*
/run/systemd/system => *dynamically created systemd unit*
/lib/systemd/system => *distibution specific configuration file e.g. example.service*
/usr/lib/systemd/system (OpenSuse) => *distribution specific configuration file e.g. example.service*

systemctl => **system control for systemd services and targets (runlevels)**
systemctl –user => **system control for systemd services and targets into the user environment**
loginctl => **login control of systemd shows sessions controled by systemd**

systemctl get-default => **show the current runlevel of the system**
systemctl isolate runlevelname => **change current runlevel into the runlevel you want**
systemd-run

Unit Dateien erstellen:

/etc/systemd/system/.service* => *create configuration file example.service or directory example.d/local.conf*

Unit Dateien installieren:

/etc/systemd/system/.service* => *create configuration file example.service or directory example.d/local.conf*
/etc/init.d/ => init scripts compatible with systemd tracked with lsb label
systemctl list-unit-files => **show available units with the status**

Gerätemanagement:

udev => **universal device manager**
/etc/udev
/etc/udev/rules.d
/etc/udev/udev.conf
udevmonitor => **user device monitor**
udevadm => **user device management tools**
lspci
lsusb
lsdev
dmesg | grep -i acpi

Gerätemanager

Speicherauslastung Festplatte / Arbeitsspeicher:

free => **free memory and swap spaces**

du => **disk utility**
df => **disk file**
lsblk => **list block devices**
blkid => **block device id**
/dev/disk/by-uuid

Taskmanager
Datenträgerverwaltung

Prozessmanager:

top => **table of processes**
htop => **highlighted table of processes**

iotop => **input-output table of processes**
collectl => **collection control table**

ps => **process listing**
pstree => **process tree**

watch => **showing updated output of a command until interrupt it**
jobs => **show shell jobs**
fg => **get process in foreground**
bg => **do process in background (use Strg + Z before)**

nice => **make new process nicer priority lower (e.g 50) or higher (e.g. 10)**
renice => **renice a running process nice value of the process**
ulimit => **unit limit process limit by using hardware ressources**

kill => **kill process by id**
pkill => **process kill by process id**
killall => **kill all process and sub-process which match process name**

Taskmanager
Prozessmonitor
Dienste

Kapazitätsplanung & Gerätemonitoring

Prozessmanager-Tools:

uptime => **shows first row of w + Entertaste**
w + Entertaste => **which time , which load average and which users are up**
lsof => **list open files**
ps => **process listing**
pstree => **process tree**

top => **table of processes**
htop => **highlighted table of processes**
iotop => **input-output table of processes**

vmstat => **virtual memory statistics (cpu, memory, processes, IO)**
collectl => **collection control table**

pidstat => **process id statistics**

Monitoring Tools

Smartmontools (Self-Monitoring, Analysis and Reporting Technology for Disks)

/etc/default/smartmontools

smartctl => **smart control and monitoring disks**
smartd => **smart disk monitoring deamon**
/etc/smartd.conf

Sysstat-Monitoring Tools

/etc/default/sysstat => configuration file

iostat => **input-output statistics for cpu, devices, partitions and network filesystems**
tapestat => **tape statistics**

nfsiostat => **network file system input-output statistics**
cifsiostat => **common internet file system input-output statistics**

mpstat => **multiple processor statistics**

Sar (system activity information reporter (cpu, memory, disk, network etc.)

sar => **system activity information reporter (cpu, memory, disk, network etc.)**
sa1 => **system activity planner for cronjob starting → sadc**
sadc => **system activity collector in binary format of cronjob → sa1**
sa2 => **system activity converter of collected data from sadc into human readable code**
sadf => **system activity data collection file to graph or multiple file converter**

Netzwerk Monitoring Tools

Taskmanager
Ressourcenmonitor
Ereignisanzeige
Gruppenrichtlinien
CMD

PowerShell

getent => **get entree from database**

passwd => **change password for user**
gpasswd => **change password for groups**
/etc/login.defs => *default configuration file for default values by user and group accounts*

makepasswd (Debian) => **make secure passwords**
mkpasswd (RHEL, Fedora, CentOS) => **make secure passwords**

chage => **change age / change password settings**

Datei & Verzeichnisverwaltung:

file => **list file type**
ls => **list files directories and other important informations**

mount => **connect partitions/ portable disks to system read or read-write**
umount => **disconnect partitions / portable disks from the system**
/etc/fstab
/etc/mtab
/proc/mounts

sync => **synchronized and write temporare changes to the disk**

mkdir => **make directory**
rmdir => **remove directory**
touch => **create new empty data**
ln => **create symbolic soft or hard links**

cp => **copy file or file hirachy**
mv => **move or rename file file hirachy**
rm => **remove file or file hirachy**

NTFS Datei und Verzeichniskonzept → Explorer

Aufgabenverwaltung:

at deamon (atd)

/var/spool/atjobs/
/var/spool/atspool/

At-Zugriffskontrolle:
/etc/at.allow/
/etc/at.deney/

at => **at that time run the job**
atq => **at queue / list all at – jobs**
atrm => **at remove / remove the job**

Aufgabenplanung
CMD
PowerShell

The cool greek prefix for time (crond)

Userjobs:
/var/spool/cron/crontabs (Debian)
/var/spool/cron/tabs (OpenSuse)
/var/spool/cron/ (RedHeat, Fedora, CentOS)

Rootjobs:
/etc/crontab/
/etc/cron.d/
/etc/cron.hourly/
/etc/cron.daily/
/etc/cron.weekly/
/etc/cron.monthly/

Cron-Zugriffskontrolle:
/etc/cron.allow/
/etc/cron.deney/
/var/spool/cron/allow/
/var/spool/cron/deney/

crontab => **cron table to view and edit the cron file**

Cron-Alternativen:
fcron
systemd.time

anacron

/etc/anacrontab/
/var/spool/anacron/
!! Führt Alternativ alle Jobs von cron aus → Speicherorte cron!!

Sicherheit (Basis)

w + Entertaste => **which time , which load average and which users are up**
/var/run/utmp

who => **who is logged in**
whoami => **who user i am at the moment**
last => **which users was last logged in**
/var/log/wtmp
/var/log/btmp

su -l => **change usr identity**
sudo => **temporary execution of root rights**
/etc/sudoers
/etc/group

fuser => **show file , process, user and port which is current using it**

find / -perm => **find user, processes which has the suid-bit set**

lsof => **list open files**

nmap => **network mapper → (GUI = zenmap)**
netstat => **network statistics**
socket

systemd.socket
/etc/systemd/system/sockets.target.wants
/etc/nologin

Lokale / Globale Gruppenrichtlinien
Bitlocker
Windows Hello Biometrikauthentifizierung
Windows Firewall
Appsicherheit
AppLocker
Windows Defender
Windows Sicherheits Center
Kernisolierung
PGP
GPG

TCP-Wrapper-Bibliothek / Eingeschränkter Dienstezugriff

/etc/host.allow => configuration file to allow service access
/etc/host.deney => configuration file to deney service access
ldd /path /to/ program => *show dependencies also tcp wrapper library*

Festplattenverschlüsselung:

dm-crypt

LUKS (Linux Unified Key Setup)

cryptsetup luksFormat / bei Fehler luksFormatN
cryptsetup luksOpen
cryptsetup luksClose
cryptsetup luksDump
cryptsetup luks benchmark
/etc/crypttab/
/etc/fstab/

Alternative Verschlüsselungen
cryptfs/loop
Loop-aes
truecrypt
veracrypt

Prüfsummen

md5sum
sha256sum
sha512sum

Dateiverschlüsselung und Signaturen

Open-PGP (GnuPGP)

gpg –gen-key
~/gnupg
gpg.conf
gpg – encrypt
gpg – decrypt
gpg – detach-sign
gpg – verify
gpg – gen-revoke
gpg – import
gpg - agent → default-cache-ttl

Erweiterte Dateiberechtigungen

ulimit => **unit limit process limit by using hardware ressources**
/etc/security/limits.conf

POSIX Access Control Lists (ACLs)

*grep -i acl /boot/config** => *show if acl feature is available on the kernel version*

inetd – internet super server deamon
/etc/inetd.conf
/etc/init.d
/etc/initab

xinetd - extended internet super server deamon
/etc/xinetd.conf
/etc/xinetd.d
/etc/systemd/logind.conf

/etc/hosts.allow
/etc/hosts.deney

goaccess **=> go to access to log files (read and display logresults in terminal or via html file)**

ModSecurity (Web Application Firewall WAF / Websitesicherheitsfilter)

/etc/modsecurity/ (Debian) => configuration files
/etc/httpd/modsecurity.d/ (RHEL, Fedora, CentOS) => configuration files

Webalizer (Websitesicherheitsfilter)

webalizer **=> web log analyzer to display graphical log results**

Proxy-Server

Squid Cache-Proxy:

/etc/squid.conf => configuration file for squid services and access control e.g proxy, application level gateway
/etc/squid/squid.conf => configuration file for squid services and access control e.g proxy, application level gateway
/var/log/squid/

squid

Squid Cache Statistiken

telnet → GET cache_object://localhost/info HTTP/1.0

Squid Application Level Gateway

/etc/squid.conf => configuration file for squid services and access control e.g proxy, application level gateway

Squid Firewall Preforierung (versteckte ausgehende Verbindung über HTTP / HTTPs verhindern)

/etc/squid.conf => configuration file for squid services and access control e.g proxy, application level gateway

ACL-Listen:

/usr/local/squid/etc/squid<Dateiname>

Alternativen

Bfliter
Pound
Privoxy
Tinyproxy

Dateiserver (Samba / NFS)

Samba-Server (selbständiger Dateiserver mit Windows-Kompatibilität):

Deamons:
smbd
nmbd
winbindd

SAMBA-Server Konfiguration:

/etc/samba/smb.conf (Debian) => *default configuration file*
/etc/smb/smb.cnf (RHEL, Fedora, CentOS) => *default configuration file*

/etc/samba/smbpasswd => *old samba internal user and password smb database if ldap not exist*
/var/lib/samba/private/passdb.tdb => *new samba internal user and password smb database if ldap not exist*

/etc/samba/users.map => database for aliases windows-user to linux-user

/var/log/samba/log.smbd / log.nmbd

testparm / testparm -v **=> test parameter of the configuration file**
smbstatus / net status share **=> show samba status information of the current version**
smbcontrol **=> send commands to samba deamons**
smbpasswd **=> create samba account and password**
smblookup **=> shows dns information of specific client / server**
getfacl / setfacl
pdbedit

smbclient **=> shows shared folders and other informations**
smbtree **=> shows all windows and samba servers with their shared folders and objects**
wbinfo

Miglied im Active Directory:
/etc/samba/smb.conf
/etc/nsswitch.conf

SAMBA-Client:

smbclient **shows shared folders and other informations**
smbtree **shows all windows and samba servers with their shared folders and objects**
smbmount **simple mount of a smb fileshare**

Server Message Block (SMB):

Dateimanager → Strg + L → smb:// servername / verzeichnisname /

Common Internet File System (CIFS) – Legacy SMB1:

mount -t cifs

Windows:

ll *hostname\sharename*

SAMBA-Domänencontroller:

samba-tool

SAMBA Domänencontroller installieren und konfigurieren:

samba tool domain provision

/var/lib/samba/private/krb5.conf → kopieren nach /etc for Kerberos-Authentication
/etc/samba/smb.conf (Debian) - *configuration file*
/var/lib/samba/sysvol *sysvol file for group policy database*

samba-tool drs kcc -k yes - replikation by two or more domain controllers
samba-tool drs showrpl
samba-tool drs replicate

samba-tool fsmo show **show domain controller roles**

Eigenständiger DNS Bind9 konfigurieren:

/etc/bind/named.conf.options
/etc/bind/named.conf.local

Zeitserver installieren und konfigurieren:

/etc/ntp.conf
/var/lib/samba/ntp_signd

Domänenkontroller Replikation sysvol:

/etc/xinetd.d
/etc/rsyncd.conf
/etc/samba/rsync.secret configuration file for *sysvol* replication of the master DC

/etc/samba/rsync.pass configuration file for the sysvol replication for the DC-clients

SAMBA Domänenkontroller Benutzer und Gruppenverwaltung:

/etc/nsswitch.conf

Gruppenverwaltung:

samba-tool group list
samba-tool group listmembers

samba-tool group add
samba-tool group addmembers

samba-tool group removemembers

Benutzerverwaltung:

samba-tool user list
samba-tool user create
samba-tool user enable
samba-tool user disable

Microsoft Dateiserver
Active Directory Domänencontroller

netstat **=> network statistics**
ss **=> show sockets and network statistics**
iptraf / iptraf-ng **=> ip traffic statistics / ip traffic statistics new generation**

Monitoringdatensammlung Tools:

collectd (The system statistic collection deamon collecting data for moitoring programs)

/etc/collectd/collectd.conf => *configuration file*
/var/lib/collectd/ => *default safe path for logging files*

Monitoringdatenhaltung Tools:

rrdtool **=> round-robin database tool stores collected statistic data into his database**

Monitoring Tools zur Darstellung:

Cacti (The complete Rrd-tool based graphing solution):

http://localhost/cacti => weblink to the admin website

MRTG (multi router traffic graph with Rrd-tool)

cfgmaker **=> configuration file maker */etc/mrtg.cfg***
indexmaker **=> create index.html file for mrtg admin website**

/var/www/mrtg/index.html => html admin website
/etc/mrtg.cfg => configuration file
http://localhost/mrtg => weblink to the admin website

Nagios (network hagios / Nagios Ain`t Gonna insist On Sainthood)

http://localhost/nagios3 => weblink to the admin website

Naemon (Nagios Fork / Thruk)

http://localhost/thruk/ => weblink to the admin website

/etc/naemon/naemon.cfg => default configuration file
/etc/naemon/conf.d/* => configuration files
/etc/thruk/ => configurationfile for admin-website

Icinga (Zulu word for „it examines")

Munin

Check-MK

Virtualisierung Containering:

VirtualBox
VMware Workstation
Vagrant

VMware vSphere
ESXi
XEN
RedHat Enterprise Virtualization

VirtualBox
VMware Workstation
Vagrant

Hyper-V
Docker
VMware vSphere

chroot

Kernel based Virtual Machine (KVM) **=> linux specific virtual technology for server distributions**

/dev/kvm

/etc/libvirt/* => default configuration files
/var/run/libvirt/libvirt-sock => default directory to administrate with virtual commands / group libvirt

/var/lib/libvirt/images => default directory for virtual machine disks
/var/lib/libvirt/qemu/save/ => default directory to save virtual machine status (snapshot)

/etc/default/libvirt-guests/ (Debian) => configuration files for virtual-guests
/etc/sysconfig/libvirt-guests/ (RHEL, Fedora, CentOS, OpenSuse) => configuration files for virtual-guests

Starten von virtuellen Maschinen

kvm **(Debian)**
/usr/libexec/qemu-kvm (RHEL, CentOS)
qemu-kvm **(Fedora, OpenSuse)**

Konfiguration von virtuellen Maschinen

virt-top **=> virtual table of processes for kvm and xen**
virt-view **=> virtual display view of a machine**

virt-manager **=> virtual graphical manager for kvm and xen**
virsh **=> virtual secure shell for kvm and xen**

virtclone **=> virtual machine cloning**

Docker

docker run **=> create docker container and run it immediatly**
docker start **=> start available docker container**
docker stop **=> stop available docker container**
docker rm **=> docker container remove**

docker exec **=> starts +n process into docker container**
docker ps **=> docker processes currently running**

docker volume **=> administrate docker container shared volumes**

docker volume ls **=> docker container shared volume list**

docker rm -v **=> delete docker container and container linked shared volume**
docker volume rm **=> delete docker container shared volume with specific id-number**
docker volume prune **=> delete all not linked container shared volumes**

docker inspect **=> show configuration and status of docker container**
docker logs **=> docker container log information of running services**

Remoteverbindungen

Vorläufer Remotverbindungen:

TeleNetwork (Telnet)
RSH
Rlogin

Remotedesktops:

xhost
/etc/X11/xorg.conf
/etc/X11/xorg.conf.d
DISPLAY Variable
XDMCP
VNC
XRDP
SPICE

Remotedesktop (RDP)
Admincentor
ssh

Secure Shell (SSH) **Remoteverbindung Windows → Linux = SSH-Client Putty**

SSH-Server:

/etc/ssh/sshd_config
/home/username/.ssh/authorized_keys
/etc/nologin
/var/log/auth.log

SSH-Client:

ssh username@client/servername/ipadress.domainname
/etc/ssh/ssh_config
/home/username/.ssh/config
/etc/ssh/ssh_known_hosts
/home/username/.ssh/known_hosts
/var/log/auth.log

ssh-keygen **=> ssh key generation**
ssh-copy-id **=> ssh copy public key id to the destination client/server**

secure copy (scp)

scp **=> secure copy from client to client or clinet to server (no ftp function !)**

sftp **=> secure file transfer protocol from client to client or client to server**

tune2fs -l /partition/path => *show if acl is the default mount option*

/etc/fstab → enhanced mount options with rw, errors=remount, acl

getfacl **=> get the current permissions overview including inherited access control list**
setfacl **=> set access control list rules also default access control list rules**

POSIX Access Control Lists (ACLs) Backups

getfacl R */path lto /acl-file-hirachy > acl.bak*

setfacl – restore = acl.bak

Erweiterte Dateiattribute

/etc/fstab → enhanced mount options with rw, errors=remount, user_xattr

lsattr **=> list file attributes which are set**
getfattr **=> get extemded file attributes**
setfattr **=> set extemded file attributes**
chattr **=> change file attributes**

Erweiterte Dateibefähigung / Dateiberechtigung (Capabilities)

getcap **=> get file capabilities / special user permissions for the file**
setcap **=> set file capabilities / special user permissions for the file**

Quotas / Journaled-Quotas

/etc/fstab → enhanced mount options with usrquota, grpquota (Quotas)

/etc/fstab → enhanced mount options with usrquota, grpquota, usrjquota=aquota.user, grpjquota=aquota.group, jqfmt=vfsv0 (Journald-Quotas)

quotaon (Debian) **=> activate disk quota**
quotaoff (Debian) **=> disable disk quota → command is needed for the first time starting initialising as next step**
quotacheck (Debian) **=> initialising process for disk quotas**

systemctl start systemd-quotacheck (OpenSuse, RHEL, Fedora, CentOS) => initialising process for disk quotas

edquota **=> set user and group quotas for partitions and also grace period**
repquota **=> report quota settings for user and groups**

Pluggable Authentication Modules (PAM) Authentifizierung:

ldd /path /to/ program => *show dependencies also pam packages*

*/etc/security/** => *configuration files for specific pam modules also for selfcreated modules*
/etc/pam.conf => *default configuration if /etc/pam.d/ not exist*
*/etc/pam.d/** => *configuration files for servies using pam (e.g. samba)*
/etc/pam.d/other => *used for services which has not a configuration in /etc/pam.d/*

authconfig / authselect (RHEL, Fedora, CentOS) => *used to change files under /etc/pam.d/** *authconfig is the old command*

/lib/security/ *stores PAM-Modules which are shared libraries that provides functions*

PAM – Authentifizierung mit System Security Services Deamon (SSSD):

/etc/sssd/sssd.conf *configuration file*
/etc/nsswitch.conf *configuration file for authentication databases*

Name Service Switch (nss)
/etc/nsswitch.conf *configuration file for authentication databases*

Name Service Caching Deamon (nscd) **caching authentications for ldap, samba etc. if needed**
/etc/nscd.conf

Chroot / SELinux / AppAmor

chroot **add specific chroot entry into configration files of the services**

AppAmor (Default Debian, OpenSuse):

/etc/appamor.d/ directory for apprmor service profiles

aa-status / apparmor_status **shows status of apparmor and loaded profiles**

aa-enforce **profile rules are mandatory**
aa-complain **only logs issues which are diffrent to the profile rules**

aa-unconfined **shows services which havn`t a apparmor profile yet**

/etc/init.d/apparmor **entload the apparmor profiles – deactivate**

AppArmor Profile erstellen:

Aa-genprof servicename → using the service as normal use → key S for scan dependencies → Choose include files and permissions / behaviour → safe profile with key S

aa-logprof **scan service and dependencies again and provides new choosing of includes, Permissions / behaviour**

SELinux (Default RHEL, Fedora, CentOS):

/etc/selinux/config configuration file for selinux module
*/etc/selinux/** containe rules for every service using selinux

sestatus **shows current configuration status of selinux**

ls -Z / getfattr -n security.selinux -d filename **shows security informations of a file for selinux**
ps axZ | grep servicename **shows security context of a service**

restorecon -R **change context to the right one using selinux**
chcon R selinux-attribut string /path /to / file **change attribut context from selinux to the right direction**

getsebool -a **shows all boolean values for selinux**
setsebool -P servicename booleanname booleanvalue **set boolean value for the selinux value**

system-config-selinux **graphical programm to change boolean values for selinux**

SELinux Alert (sealert)

LANG= sealert -a *varlog/audit/audit.log* **troubelshooting program to search audit.log for selinux issues**

Fail2Ban - Intrusion Prevention Software Framework Prevent Brute Force Attacks

/etc/fail2ban/fail2ban.conf => *global settings for fail2ban*
/etc/fail2ban/jail.conf => *default settings for jails „not change"*
/etc/fail2ban/jail.local => *copy of jail.conf / customized settings file for the services*
*/etc/fail2ban/filter.d/** => *contains filter rules*
*/etc/fail2ban/action.d/** => *contains actions to take if rules are triggerd*
/var/log/fail2ban.log

iptables -L -n **=> shows activated rules**

fail2ban-client **=> check ban status and set ban status of specific clients to false if it blocks wrong**
fail2ban-server

fail2ban-regex **=> check own created rules of regular expression rules for control of right functionality**

Scanlogd (einfacher Portscanner)

/var/log/messages

Tripwire (Datei-Integritätstester)

/etc/tripwire/twcfg.txt => configuration file for tripwire database, integritiy policies etc. → convert with twadmin to tw.cfg file
/etc/tripwire/tw.pol => database containing integrity policies

twadmin **=> tripwire administration to generating site key, local key and creating policy database**
twprint **=> print database information and integrity check results as human readable output**
tripwire **=> initialising tripwire database, start and report integrity check, create and update policies**

Advanced Intrusion Detection System (AIDE)

/etc/aide.conf
/etc/default/aide
/var/log/aide.log

OpenVAS

samba-tool user delete

Passwortrichtlinien:

samba-tool domain passwordsettings show
samba-tool domain passwordsettings set

Alternative Benutzer und Gruppenverwaltung:
RSAT

Client Beitritt zur Domäne:

Windows-kompatibler SAMBA-Dateiserver

/etc/samba/smb.conf → zusätzliche Parameter: inherit acls = yes ; store DOS attributes = yes ; vfs objects = acl_xattr

Linux-Clients:

/etc/krb5.conf kopieren von Domänencontroller

/etc/samba/smb.conf

kinit	**kerberos ticket initialisation**
klist	**kerberos ticket list**

/etc/hosts configure domain controller ip adress

net ads join -U	**domain joining**
net ads testjoin	**test domain joining was succesfull**

/etc/nsswitch.conf → winbind winbind compatibility

tdbdump

Installation Kerberos-Client (siehe Abschnitt Kerberos)

Windows Clients:

Einstellungen → Info → Diesen PC umbenennen → Ändern → OK → Neustart

Alternativen:
Samba Web Administration Tool (SWAT)

Dateiserver (Samba / NFS)

Network File System (NFS)-Server:

portmap nfs-server package

Deamons:
portmap
rpc.mountd

NFS-Server konfigurieren:

/etc/exports	*define pseudo file system hirachy and folders*
exportfs	**test and share nfs file shares**
rpcinfo -p	**shows NFS version informations**

/etc/idmapd.conf mapping user and group ids to the shares
/etc/default/nfs-common (Debian) → NEED_IDMAPD=yes
/etc/sysconfig/nfs (RHEL, Fedora, CentOS, OpenSuse) → NFS4_SUPPORT="yes"

Zugriffsbeschränkungen:
/etc/exports
/etc/hosts.allow

NFS-Client:

mount -t nfs4 nfs.servername:/
/etc/fstab

/etc/default/nfs-common (Debian) → NEED_IDMAPD=yes
/etc/sysconfig/nfs (RHEL, Fedora, CentOS, OpenSuse) → NFS4_SUPPORT="yes"

NFS-Server-und-Client optimieren:

NFS-Server:

/proc/net/rpc/nfsd shows current performance → th value is important
/etc/default/nfs-kernel-server (Debian) → RPCNFSDCOUNT=8
/etc/sysconfig/nfs (RHEL, Fedora, CentOS, OpenSuse) → USE_KERNEL_NFSD_NUMBER="4"

NFS-Client:

/etc/fstab → add parameters „rsize" and „wsize" to nfs mount points

Kerberos:

FTP-File Transfer Protocol

FTP-Server:

Very Secure FTP Server (VSFTP):

Deamons: vsftpd

/etc/vsftpd.conf	*(Debian, OpenSuse)*
/etc/vsftpd/vsftpd.conf	(RHEL, Fedora, CentOS)
/srv/ftp/.messages	(Debian, OpenSuse
/var/ftp/.messages	(RHEL, Fedora, CentOS)

Pure-FTPd:

pure-ftpd
*/etc/pure-ftpd/**
*/usr/sbin/pure-ftp**

ProFTPd:

/etc/proftpd/proftpd.conf

Grafische Benutzeroberfläche für ProFTPd:

gadmin-proftpd package

FTP-Client:

?	**=> show list of ftp commands**
ftp username@servername / ftp servername	**=> connect to the ftp server**
open	**=> open ftp connection to the server if auto connection failed**
close	**=> close server ftp connection**
quit	**=> close ftp client**
ls	**=> list files and directories**
cd verzeichnisname	**switch into hirachies**
get	**=> download data from ftp server to the current directory**
mget *.muster	**=> download all matched data from ftp server to the current directory**
reget dateiname	**=> reconnect and redownload matched data**
lls	**=> list files and directories of the local client**
lcd	**=> change current hirachy of the local client**
put	**=> upload matched file and / or hirachy**

Alternative FTP-Clients

curl
lftp

Mail-Server

Mail Transfer Agents (MTAs):

Cyrus
Sieve
Qmail
Courier

Exchange

/var/spool/mail/accountname	=> default stored place for user mails
/var/mail	

Postfix

/etc/postfix/main.cf	=> default configuration file also for send and recipient restriction rules
/etc/postfix/master.cf	

/var/log/syslog/mail.log

sftp username@client/servername/ipadress.domainname
get
mget *.muster
ls
put

ssh-agent (eval $(ssh-agent))

ssh-add	**=> ssh add passphrase to ssh-agent for auto login**

sshfs **=> secure shell filesystem in userspace**

username@client/servername/ipadress.domainname:path mountpoint

gnome-keyring

file-manager seahorse

Alternativen:

Putty
WinSCP
Synergy

Open Lightweight Directory Access Protokoll (LDAP) Server

LDAP-Server: — **Microsoft Active Directory (angepasstes LDAP-Verzeichnis)**, **LDAP-Addon für OpenLDAP**, **include Kerberos**

Traditionelle / statische Konfiguration:

slapd -f /path /to /slapd.conf

/etc/ldap/slapd.conf	(Debian)	- configuration file
/etc/openldap/slapd.conf	(RHEL,Fedora,CentOS, OpenSuse)	- configuration file
/var/lib/ldap/		- datafiles of the ldap database

Umstellung auf traditionelle / statische Konfiguration von moderner / dynamischer Configuration:

/etc/default/slapd → Variable SLAPD_CONF=/path/to/sldap.conf (Debian)
/etc/sysconfig/openldap → Variable OPENLDAP_CONFIg_BACKEND="files" (OpenSuse)

Konvertierung Einstellungen traditionelle Configuration in moderne Konfiguration:

slaptest -f /path /to /slapd.conf -F /path /to /slapd.d

/etc/default/slapd → Variable SLAPD_CONF=/etc/ldap/sldap.d (Debian)
/etc/sysconfig/openldap → Variable OPENLDAP_CONFIG_BACKEND="ldap" (RHEL, Fedora, CentOS, OpenSuse)

Moderne / dynamische Konfiguration:

/etc/openldap/slapd.d/*	- news configuration files
/etc/ldap/slapd.conf	
/var/lib/ldap/	- datafiles of the ldap database

LDAP-Server-Tools (Für Standardaufgaben alternativ LDAP-Client-Kommandos):

slapadd		**add data of an ldif file into the ldap database**
slapcat		**create ldif file based on the ldap database**
slapindex		**reinex ldap entries**
slapacl	–	**check access control lists**
/etc/ldap/acl.conf		
slappasswd	–	**create a password or password hash for ldap accounts**

LDAP-Client:

/etc/ldap/slapd.conf	-	configuration file for the connection to the LDAP-Server
/etc/ldap/ldif/	-	*possible foldar to safe and connect ldif files*
ldapsearch		**search ldap database of search matches**
getent	–	**get entree**
ldapadd (ldapmodify -a)		**add data of an ldif file into the ldap database**
ldapmodify		**modify ldap database by terminal entree or regarding of entrees in a ldif file**
ldapvi (Debian)		**ldap client with vi interface**
ldapmodrdn		**change RDNs of ldap hirachy**
ldappasswd	–	**create or change ldap password for accounts**
slappasswd	–	**create a password or password hash for ldap accounts**
ldapwhoami	–	**shows who ldap account you are at the moment**
ldapdelete	–	**delete matched ldap entrees in the ldap hirachy database**

Grafische Werkzeuge für die LDAP Verwaltung:

LDAP Account Manager
Phpldapadmin
Gosa
Jxplorer
Apache Directory Studio

PAM – Authentifizierung mit LDAP:

/etc/security/pam_ldap.so	*pammodule for ldap*
/etc/nsswitch.conf	
/etc/pam_ldap.conf (Debian)	configuration file
/etc/ldap.conf (OpenSuse)	configuration file
/etc/pam.d/common-auth (Debian)	
/etc/pam.d/system-auth-ac (RedHat, Fedora, CentOS)	
/etc/security/limits.conf	*configuration file for ressource limits*
/etc/security/limits.d	*new configuration file for ressource limits*

PAM – Authentifizierung mit System Security Service Deamon (SSSD):

/etc/sssd/sssd.ldif	
/etc/sssd/sssd.conf	configuration file
/etc/nsswitch.conf	

LDAP mit Kerberos:

siehe Abschnitt Kerberos

Virtual-Private-Network (VPN)

OpenVPN: — **Remotezugriff (VPN, Direct Access)**, **Netzwerkrichtlinien und Zugriffsdienste (RADIUS)**, **Gruppenrichtlinien**

Server:

openvpn
/etc/openvpn/server.conf
/etc/openvpn/keys/
/etc/openvpn/ccd/vpn-nutzername
/etc/sysctl.conf
/etc/openvpn/update-resolver.conf (Debian)
/var/log/openvpn/openvpn.log

OpenVPN-Server starten:

/lib/systemd/system/openvpn@.service (Debian)
/usr/lib/systemd/system/openvpn@.service (RHEL, Fedora, CentOs, OpenSuse)

Client:

/etc/openvpn/client.conf
/etc/openvpn/keys/
/etc/openvpn/update-resolver.conf (Debian, RHEL, Fedora, CentOs, OpenSuse)
/etc/openvpn/update-systemd-resolved (Ubuntu)

OpenVPN-Client starten:

openvpn
/lib/systemd/system/openvpn@client.service (Debian)
/usr/lib/systemd/system/openvpn@client.service (RHEL, Fedora, CentOs, OpenSuse)

Datenbank-Server

MySQL / MariaDB

/var/lib/mysql	*=> store sql-databases*
/etc/mysql/mariadb.cnf,/50-server.cnf (Debian)	=> configuration file (mariadb)
/etc/mysql/mysql.conf.d/mysqld.cnf (Debian)	=> configuration file (mysql)
/var/log/mysql/error.log	=> logging file (mysql, mariadb)
/etc/my.cnf.d/mysql-server.cnf (RHEL, Fedora, CentOS)	*=> configuration file (mysql)*
/var/log/mysql/mysqld.log (RHEL, Fedora, CentOS)	=> logging file (mysql)
/etc/my.cnf.d/mariadb-server.cnf (RHEL, Fedora, CentOS)	*=> configuration file (mariadb)*
/var/log/mariadb/mariadb.log (RHEL, Fedora, CentOS)	*=> logging file (mariadb)*
/etc/my.cnf (OpenSuse)	=> configuration file (mysql, mariadb)

https://localhost:9392

Snort (Intrusion Detection & Intrusion Prevention System)

/etc/snort/snort.conf	=> configuration file also for snort rules
*/var/log/snort/**	=> logging data
snort	**=> start tests, save results in logfiles**

Sicherheit (Erweitert)

Kerberos — **Microsoft Kerberos**

Kerberos-Server Konfiguration:

/etc/krb5.conf	=> configuration file for kerberos roles and administrator server
/etc/krb5kdc/kdc.conf (Debian)	=> enhanced configuration file for kerberos parameters
/etc/krb5kdc/kadm5.acl (Debian)	=> configuration of acls for the database for user and services
/var/lib/kerberos/krb5kdc/kdc.conf (RHEL, Fedora, CentOS, OpenSuse)	=> enhanced configuration file for kerberos parameters
/var/lib/kerberos/krb5kdc/kadm5.acl (RHEL, Fedora, CentOS, OpenSuse)	=> configuration of acls for the database for user and services
/etc/krb5.keytab	=> default central keytab data
/etc/krb5kdc/stash	=> file which contains the master password of the database
/var/log/krb5/kdc.log	
/var/log/krb5/kadmind.log	

Kerberos-Datenbank erstellen (dezentrale Datenbank noch ohne LDAP):

kdb5_util -s create	**=> create kerberos database**

Kerberos Principals für Benutzer, Computer und Dienste vergeben:

kadmin.local / kadmin (command menu)
/etc/krb5kdc/kadmin.local

listprincs	**=> list possible principals to set for a user**
addprinc username / domainname	**=> add user principals**
addprinc -randkey host/ domainname	**=> add host principal with random password**
addprinc -randkey servicename / domainname	**=> add service principal with random password**
ktadd -k /path /to/ servicename.keytab servicename/ domainname	**=> create own keytabfile for every service**
ktrem	**=> key termination / delete kerberos key**
delprinc username : hostname : servicename / domainname	**=> delete user: host: service principal from database**
add_policy	**=> create password policies**

ktutil key utility (command menu)

rkt ***/etc/krb5.keytab or /path/ to/ servicename.keytab***	***=> show content of the keytab file***
ktadd -k hostname /domainname	**=> create own keytabfile for every service**

Kerberos Server-Replikation (Master / Slave):

Kerberos-Master:

/etc/krb5.conf	=> configuration file for kerberos roles and administrator server
addprinc -randkey slavehostname / domainname	**=> add service principal with random password**
ktadd -k hostname /domainname	**=> create own keytabfile for every service**

kopieren auf Kerberos Slave:

/etc/krb5kdc/kdc.conf (Debian)	=> enhanced configuration file for kerberos parameters
/etc/krb5kdc/kadm5.acl (Debian)	=> configuration of acls for the database for user and services
/var/lib/kerberos/krb5kdc/kdc.conf (RHEL, Fedora, CentOS, OpenSuse)	=> enhanced configuration file for kerberos parameters
/var/lib/kerberos/krb5kdc/kadm5.acl (RHEL, Fedora, CentOS, OpenSuse)	=> configuration of acls for the database for user and services
/etc/krb5kdc/stash	=> file which contains the master password of the database

erstellen und konfigurieren:

/etc/krb5kdc/kpropd.acl (Debian)	
/var/lib/kerberos/krb5kdc/kpropd.acl (RHEL, Fedora, CentOS, OpenSuse)	
/etc/xinetd.d/kpropd	=> service to replicate data between master and slave

Kerberos-Master:

kdb5_util dump
kprop -d -f path/ to/ replicabackup

Kerberos-Client Konfiguration:

/etc/krb5.conf	=> configuration file for kerberos roles and administrator server also for clients
kinit	
klist	
kdestroy	

Kerberos mit PAM:

Install package lib-pam-krb5	**(Debian)**
Install package lib-pam-krb5 & pam_krb5-32bit	**(RHEL, Fedora, CentOS, OpenSuse)**
pam-config –add –krb5 –krb5-minimum_uid=1001	
/etc/pam.d/pam-config	

Kerberos über LDAP:

LDAP-Server Konfiguration:

/usr/share/doc/krb5-kdc-ldap/kerberos.schema.gz	→ */etc/ldap/schema*
/etc/default/slapd	→ *export KRB5_KTNAME=/etc/ldap/slapd.keytab*

Kerberos-Server Konfiguration:

kdb5_util dump /root/domainname.backup
/etc/krb5.conf

kdb5_ldap_util create -D cn=admin,dc=example,dc=net \ -r EXAMPLE.NET -s -sscope sub
kdb5_ldap_util stashsrvpw -D cn=admin,dc=example,dc=net -f /etc/krb5kdc/service.keyfile \ cn=kdc,ou=kerberos-adm,dc=example,dc=net
kadmin.local -q listprincs
kdb5_util -update load example.net.backup
addprinc -randkey ldap/k1.example.net
ktadd -k /etc/ldap/slapd.keytab ldap/k1.example.net

Grafische Tools:

LAM-Pro

Kerberos-Alternativen:

MIT Kerberos
Heimdal Kerberos
GNU Shisi

Public-Key-Infrastructure X.509 (PKI) — **Microsoft-Zertifizierungsstelle**, **Gruppenrichtlinien**, **Registry**

Openssl & Zertifikatsinformationen lesen:

openssl version -a	**=> show openssl version informations**
openssl help	**=> show openssl commands**
openssl x509 -text	**=> show openssl certificate information**
openssl ciphers -v	**=> show possible cipher suites**
openssl speed	**=> show encryption speed and benchmarks**

Zertifikate erstellen

openssl req	**=> create certificate request**
openssl x509 -inform	

Zertifikat erneuern:

openssl x509 -x509toreq	**=> old certification information to certificate request**

Zertifizierungsstelle konfigurieren:

Root-Certifiaction Authority:

/etc/openssl/root-ca.conf	=> certification authority configuration file
/etc/openssl/certs/	=> stored new created certificates
/etc/openssl/db/	=> database index and serial numbers of created certificates
/etc/openssl/private/	=> stored private keys of the certificate authority and the ocsp

openssl gen	
openssl req	**=> create certificate request**
openssl ca -selfsign	
openssl ca -gencrl	**=> create certificate revocation list**

/var/log/syslog/mail.info
/var/log/syslog/mail.warn
/var/log/syslog/mail.err
postfix/local => postfix default stored mails for users

postconf => postfix configuration information and set options in main.cf
queue / mailq => show list queue of not yet sended mails
postqueue => show mails in waiting list and restart sending
postmap => postfix mapping file to db / create postfix database for future use

Postfix-Relay

/etc/postfix/main.cf → add variables relay_domains, transport_maps
/etc/postfix/relay_domains => add all domains and subdomains which postfix is a relay

postmap => if /etc/postfix/transport not exist use this command to create db

Postfix Aliase & Weiterleitungen

/etc/postfix/virtual => central configuration file for user aliases

Postfix mit Dovecot

/etc/postfix/main.cf → smtpd_sasl_auth_enable = yes, smtpd_sasl_path = private/auth, smtpd_sasl_type = dovecote
→ smtpd_tls_auth_only=yes

Dovecot-Server:

/etc/dovecot/conf.d/10-master.cfg → section service auth ... → enable

Sendmail

/etc/mail/sendmail.cf
/etc/mail/sendmail.mc
/var/log/mail.log

Exim

/etc/exim4/
/var/log/exim4/mainlog
/var/log/exim4/paniclog
/var/log/exim4/rejectlog

Warteschlangen (Queues):

/var/spool/postfix/* - Postfix
/var/spool/mqueue - Sendmail
var/spool/exim4/* - Exim
sendmail-bp
mailq

Mail Delivery Agents (MDAs):

Procmail
Maildrop
Postfix

POP/IMAP-Server

Courier-IMAP
UW-IMAP

Dovecot

/etc/dovecot/dovecot.conf
/etc/dovecot/conf.d/*
/etc/dovecot/conf.d/10-ssl.conf
/etc/dovecot/conf.d/10-auth.conf

doveadm

Dovecot => show configuration values of the config file
doveconf
doveadm

Mail User Agent (MUA):

Kmail
Evolution
Thunderbird
Outlook
Apple Mail

E-Mail Aliase / Weiterleitungen:

/etc/aliases/
newaliases

SpamAssasin & ClamAV

SpamAssasin

/usr/share/spamassassin/*
/etc/default/spamassassin

/etc/spamassassin/local.cf (Debian) => add whitelisting entries for domains, users
/etc/mail/spamassassin/local.cf (RHEL, Fedora, CentOS) => add whitelisting entries for domains, users

swaks (swiss army knife for smtp)

ClamAV

/etc/default/clamav-milter
/etc/clamav/clamav-milter.conf => configuration file for clamav
/var/lib/clamav => contain the clamav database

/var/log/mysql/mysqld.log (OpenSuse) => loggingf ile (mysql, mariadb)

mysql => mysql server to client connection also for sql commands
mysqladmin => used for administrative tasks and automatized scripts

mysqldump => create database backup
mylvmbackup => create lvm snapshot for databse backup
XtraBackup => alternative program for big databases no for mariadb

Mysqlbinlog => restore logged changes into database
/etc/mysql/my.cnf → log_bin = /var/log/mysql/mysql-bin.log

openssl ocsp

Sub-Certification Authority:

/etc/openssl/sub-ca.conf => certification authority configuration file
/etc/openssl/certs/ => stored new created certificates
/etc/openssl/db/ => *database index and serial numbers of created certificates*
/etc/openssl/private/ => *stored private keys of the certificate authority and the ocsp*

openssl req => create certificate request

openssl ca

Zertifizierungsstelle und Zertifikate testen:

openssl s_client

CA.pl - Pearl Script Frontend für openssl

Alternativen:

XCA (graphical interface for *openssl*)
OpenCA
DogTag (Fedora)
OpenXPKI