chmod: ”change mode bits”

- Muuttaa tiedoston oikeuksia
- Vanha numeerinen syntaksi:

  yksi oktaalinumero/3 bittiä, kolme numeroa user-group-other -järjestyksessä:

  4=r, 2=w, 1=x → 7=rwx, 5=rx jne

  jos nelinumeroinen, ensimmäinen numero 4=suid, 2=sgid, 1=sticky bit
- Symbolinen notaatio:

  [ugoa][+-=][rwxXst] # tarvittaessa monta kertaa pilkulla erotettuina

  u=user, g=group, o=others, a=all

  rwx=read,write,execute/search, s=suid tai sgid, t=sticky

  X = ehdollinen x (vain jos hakemisto tai jos jollakulla jo x)
- optioita: -R,--recursive, -v,--verbose, -c,--changes, -f,--quiet,

  --reference *file* (oikeudet samoiksi kuin *file:*llä)

umask

- Shellin (bash,sh) sisäinen komento: asettaa oletusarvon luotavien tiedostojen oikeuksille (rwx)
- Vanha syntaksi oktaalinen bittimaski **poistettaville** oikeuksille, esim.

  umask 022 # ryhmältä ja maailmalta w-oikeus pois

  umask 067 # ryhmältä rw pois, maailmalta kaikki pois
- Uusi syntaksi **sallitut** oikeudet kuten chmod'issa, esim. ylläolevat toisin esitettynä:

  umask u=rwx,g=rx,o=rx

  umask u=rwx,g=x,o=
- Ilman argumentteja tulostaa voimassaolevan asetuksen, oletuksena oktaalimuodossa, optiolla -S symbolisena

chroot

chroot [optiot] hakemisto [komento]

- “Virtuaalinen levyjärjestelmä”
- Vaihtaa juurihakemiston: annettu hakemisto toimii uutena juurena, sen ulkopuolella olevat eivät näy
- Uuden juuren alla pitää olla kaikki tarvittava, kuten /bin, /etc, /usr (riisuittuina turhista tiedostoista) ja dynaamiset kirjastot (/lib)
- Komento oletuksena "$SHELL -i" (/bin/sh -i)

chroot

- Käytetään asennusvaiheessa (chroot /target …), etenkin asennuspakettien teossa hakemistonäkymän muuttamiseen
- Käytetään usein myös sovelluksen tietoturvan parantamiseen ajamalla niitä dedikoidussa hakemistopuussa (ei kovin tehokas suoja, root pääsee yleensä ulos), esim. vsftpd
- Joskus kätevä toisen koneen levyn käsittelyssä

Esimerkki: initramfs hukassa

Tuhotaan initramfs vahingossa: rm /boot/initrd*

- Uuden voi luoda helposti: update-initramfs -u -k all
- Jos kone bootataan initramfs:n puuttuessa, se yleensä epäonnistuu, myös recovery boot; jos tallessa on vanha kernel ja sen initramfs tallessa, sitä voi käyttää.
- initramfs:n voi palauttaa varmuuskopiolta toisen virtuaalikoneen (tai alustakoneen) avulla.
- Viime kädessä initramfs:n voi luoda uudestaan toisen riittävän samanlaisen koneen avulla.

Esimerkki: initramfs hukassa

- Jos toinen kone on lähes identtinen, initramfs:n voi kopioida sieltä sellaisenaan. Usein se ei kuitenkaan toimi (initramfs saattaa sisältää konekohtaisia tunnisteita, kuten VG:n nimen, UUID:tä yms).
- Seuraavassa esimerkissä rakennetaan initramfs toisessa koneessa käyttäen rikkoutuneen koneen tiedostojärjestelmää chroot'in avulla.
- Oletaan että initramfs on hukattu koneessa tt3, liitetään sen levy koneeseen tt2, molemmissa LVM, koneen tt3 volume group ”tt3”, LVt "lvroot", "lvusr" &c.

Esimerkki: initramfs hukassa

- Chroot on tarpeen koska update-initramfs:n pitää nähdä tiedostojärjestelmä samoin kuin kohdekonekin
- Huom. tämä särkyy jos VG:t samannimisiä!
- Alustakoneessa:

  destroy tt3 # jos käynnissä

  virsh attach-disk tt2 ~/tt3.img vdb

    # --persistent ei yleensä tarpeen, --driver &c voi olla

Esimerkki: initramfs hukassa

- Virtuaalikoneessa tt2:

  vgscan

  mkdir -p /mnt/tt3

  mount /dev/tt3/lvroot /mnt/tt3

  mount /dev/tt3/lvusr /mnt/tt3/usr

  mount /dev/tt3/lvvar /mnt/tt3/var

  mount /dev/tt3/lvhome /mnt/tt3/home

  mount /dev/tt3/lvtmp /mnt/tt3/tmp

Esimerkki: initramfs hukassa

```
mount --bind /proc /mnt/tt3/proc
mount --bind /dev /mnt/tt3/dev
mount --bind /sys /mnt/tt3/sys
chroot /mnt/tt3
update-initramfs -u
exit # lopettaa chroot'in
umount /mnt/tt3/{usr,home,var,tmp,dev,proc,sys} /mnt/tt3
vgchange -a n tt3
```

Esimerkki: initramfs hukassa

- Taas alustakoneessa:

  virsh detach-disk tt2 vdb

  virsh start tt3

- Lopuksi tt3:ssa varmuuden vuoksi initramfs-update -u -k all
- Tällaisenakin operaatio edellyttää virtuaalikoneiden olevan riittävän samanlaisia (sama käyttöjärjestelmäversio, sama kernel-versio); joitakin kriittisiä ohjelmia (lvm, cryptsetup, mdadm) voi joutua asentamaan apukoneeseen. Joskus voi olla tarpeen luoda apukone varta vasten.

apt-get

- Pakettienhallinnan "high-level front-end"
- Ohjelmien asennus ja päivitys (repositoryistä) sekä poisto, mm:

```
update   # päivitä pakettilistaus
install     # asenna paketteja
upgrade # päivitä paketteja; yleensä dist-upgrade parempi
dist-upgrade # päivitä riippuvuuksineen, poista turhiksi käyneitä
remove  # poista paketteja; yleensä purge parempi
purge     # poista paketteja konfiguraatioineen
autoremove # poista turhiksi käyneet
source    # asenna sorsakoodipaketteja
```

apt-get optioita

- Yleisimmät optiot (toimivat myös apt-komennon kanssa):

  -d, --download-only

  -f, --fix-broken

  -m, --ignore-missing

  -s, --simulate, --dry-run

  -y, --yes, --assume-yes; --assume-no

  --reinstall

  --allow-unauthenticated

apt, apt-*

- apt on uusi, vain interaktiiviseen käyttöön tarkoitettu front-end: lähes kuten apt-get, muutama lisäominaisuus (search), ei toimi hyvin skripteissä
- koko joukko apt-* -komentoja eri tarkoituksiin:

  apt-add-repository

  apt-cdrom # cf. /var/lib/apt/cdroms.list

  apt-key # repositoryn avainten hallinta

  apt-cache # haku apt-"kakusta"; vrt apt search

  - muitakin on, ks. man -k apt

apt: sources.list

- apt*-komentojen repositoryt on määritelty tiedostoissa /etc/apt/sources.list ja /etc/apt/sources.list.d/*.{list,sources}
- syntaksi (.list -formaatti):

  deb[-src] [optiot] URI suite [component(s)]

  - optioita mm. arch=, lang=, trusted=, signed-by=
  - URI mm. file: cdrom: http: ftp: ssh:
- uusi syntaksi (.sources -formaatti):

  omilla riveillään avainsanat Types:, URIs:, Suites;, Components:, option: value

apt.conf

- apt-järjestelmän asetukset:

  /etc/apt/apt.conf, /etc/apt/apt.conf.d/*

- paljon mahdollisia asetuksia, esim.

  Acquire::http::Proxy "http://lonka6.it.jyu.fi:3142";

  Acquire::AllowInsecureRepositories;

  DPkg::Pre-Install-Pkgs {"/usr/sbin/dpkg-preconfigure --apt || true";};

- muutosten jälkeen apt update
- Ks. man apt.conf

dpkg

- dpkg (Debian PacKaGe manager) on apt*n alla oleva "low-level" pakettienhallintamekanismi
- Tarpeen mm. haluttaessa asentaa paketti tiedostosta (eikä repositorystä) tai jyrätä apt'in riippuvuudenhallinta, tai kun halutaan tutkia asennettuja paketteja
- Paljon lähinnä skripteissä tarvittavaa toiminnallisuutta
- Apukomennot dpkg-deb ja dpkg-query; dpkg osaa yleensä kutsua niitä tarvittaessa (joskus kutsuttava suoraan jos tarvitaan erikoisempia optioita)

dpkg

Yleisimmät optiot:

-i, --install [*file.deb* | -R, --recursive *dir*]

--configure [*package*|-a|--pending]

vrt. dpkg-reconfigure *package*

-r, --remove [*package*|-a|--pending]

-P, --purge [*package*|-a|--pending]

--unpack *file.deb*

-V, --verify [*package*] # checksum-tarkistus

-C, --audit [*package*] # dpkg:n tietokannan tarkistus

dpkg-query

- komentona näissä toimii myös pelkkä dpkg:

  dpkg -l, --list *paketinnimimalli*

  dpkg -s, --status *paketti*

  dpkg -L, --listfiles *paketti* [*…*]

  dpkg -S, --search *tiedostonimimalli*

  dpkg -p, --print-avail *paketti* [*…*]
- komennolla dpkg-query saa enemmän optioita, esim. dpkg --control-list *paketti*

  ks. man dpkg-query

dpkg-deb

- Työkalu pakettien rakentamiseen, purkamiseen ja muuttamiseen. Komentona toimii useimmiten myös dpkg (sopivilla optioilla). Ylläpitäjälle hyödyllisimpiä optioita:

  dpkg -I, --info *file.deb*

  dpkg -c,--contents [*file.deb* | *dir*]

  dpkg -f,--field *file.deb*

- Paljon lisää komentoja ja optioita, suurin osa tarpeen lähinnä ohjelmien kehittäjille

  ks. man dpkg-deb

dmesg

- Tulostaa *konsoliviestit*
- Optioita mm.

  -T "ihmisystävälliset" aikaleimat (epäluotettava)

  -c tyhjennä puskuri tulostuksen jälkeen

  -w jatkuva tulostus

- Viestejä säilytetään pienehkössä rengaspuskurissa, vanhemmat hukkuvat nopeasti; jos halutaan säilyttää pitempään, voi tehdä cron-jobin joka kopioi viestit tiedostoon vaikka minuutin välein tyyliin

  dmesg -c >>/var/log/dmesg

journalctl

- systemd:n (journald:n) lokien käsittely
- lokit oletuksena binäärisiä, eivät suoraan luettavissa (mutta yleensä osin ohjattu tekstitiedostoihin joko suoraan tai ryslogd:n kautta)
- /run/log/journal/*
- paljon optioita haluttujen tietojen valikointiin ja muotoiluun ja käsittelyyn, mm.

-r	uusin ensin
-u *unit*	tietyn palvelun viestit
-S *since* -U *until*	viestit jälkeen/ennen tietyn ajankohdan
-f	jatkuva uusien viestien tulostus

rsyslogd

- systeemilokien käsittelijä
- työnjako rsyslogd:n ja systemd:n välillä vaihtelee
- /etc/rsyslog.conf
- /etc/rsyslog.d/*
- /var/log/*
- logger
- syslog(3)
- edeltäjä syslogd jossain myös yhä käytössä

logrotate

- Yleinen työkalu muuten hallitsemattomasti kasvavien lokitiedostojen kierrätykseen
- Toimii lähes kaikkien tiedostoihin lokittavien ohjelmien kanssa
- Palvelukohtaiset säännöt hakemistossa /etc/logrotate.d
- Lokien kierrätystahti (päivittäin, viikottain), säilytysaika ja pakkaus määriteltävissä palvelukohtaisesti (yleensä tulee asennuspaketin mukana)
- Suoritus päivittäin: /etc/cron.daily/logrotate

Ftp

- ”file transfer protocol” - vanha ja pikkuhiljaa katoava, mutta yhä siellä täällä käytössä.
- Ei salausta tiedonsiirrolle eikä edes autentikoinnille, turvallinen vain julkisen tiedon anonyymiin jakeluun (anymous upload myös OK jos sellaista tarvitaan); nyttemmin toimii myös SSL:n kanssa (aika turha, koska saman tien voi yleensä käyttää https:ää tai sftp:tä).

Ftp

- Käyttää kahta tcp-porttia (20 ja 21), erikseen ohjaus- ja tiedonsiirtoväylät, kaksi toimintatapaa (active & passive – edellisessä palvelin ottaa datayhteyden takaisinpäin), vaatii erikoissäätöjä palomuureissa
- Ftp-palvelinohjelmia paljon, mm. vsftpd (yleisin Linuxeissa nykyisin), Pure-FTPd, ProFTPD
- Asiakasohjelmina nykyisin lähinnä web-selaimet (joissa toimii vain passive mode), erityisesti myös wget ja curl, mutta myös dedikoituja ftp-clientteja on yhä (komentorivikomento ftp, gftp ym)

Ftp komentoriviltä

```
$ ftp ftp.stak.tk
Name (ftp.stak.tk:tt0): ftp                 # tai anonymous
331 Please specify the password.
Password:                                   # pelkkä return (ei salasanaa)
230 Login successful.
ftp> dir
500 Illegal PORT command.                   # active mode ei toimi (palomuuri...)
ftp: bind: Address already in use
ftp> passive                                # optio -p olisi tehnyt tämän myös
ftp> dir                                    # toimii :-)
ftp> get 0README
```

Ftp: wget, curl

- wget ftp://ftp.stak.tk/0README

  --no-passive-ftp # active mode

  optioita voi laittaa .wgetrc -tiedostoon

- curl ftp://ftp.stak.tk/0README

  -o 0README.new # tulos tiedostoon

  -P eth0 # active mode (argumenttina laite, IP tai nimi)

  --ftp-pasv # passive mode (default)

  optioita voi laittaa .curlrc -tiedostoon

- Molemmissa paljon muitakin optioita (man-sivut kertovat lisää)
- Autentikointiasetuksia voi laittaa tiedostoon .netrc

Ftp-palvelin: vsftpd

apt-get install vsftpd

nano /etc/vsftpd.conf # tarkista ainakin rivit

anonymous_enable, anon_upload_enable, anon_mkdir_write_enable, local_enable, chroot_local_user, ls_recurse_enable, write_enable, xferlog_enable, nopriv_user

- Jos anonymous -käyttö on sallittu, sitä varten pitää tehdä hakemisto (ftp-käyttäjälle)