ssh

- ssh (Secure SHell) suorittaa komennon tai avaa pääteistunnon etäkoneessa:

  `ssh [options] [user@]kone [komento]`

- Paljon optioita erikoistilanteisiin, mm.

  -X salli etäkoneen käyttää paikallista näyttöä

  -p *port* käytä porttia *port* oletuksen 22 asemesta

  -i *id_file* käytä epästandardia avaintiedostoa

  (oletuksena olevan $HOME/.ssh/id_rsa asemesta)

scp

- scp (Secure CoPy) kopioi tiedostoja etäkoneeseen:

  `scp [`*`optiot`*`] `*`tiedostot`*` [`*`user`*`]@kone:[kohde]`

  tai etäkoneesta:

  `scp [`*`optiot`*`] [`*`user`*`]@kone:tiedosto kohde`

  `missä kohde` voi olla hakemisto tai tiedostonimi.

  Yleisin optio on -r, joka kopioi koko hakemistopuun. Optio -i toimii kuten ssh:n kanssa, mutta portin vaihto-optio on -P *port*, kun taas -p säilyttää aikaleimat ja oikeudet.

ssh & scp: autentikointi

- Autentikointitapoja on useita, yleisimmät:
  - (etäkoneen) salasana
  - avaintiedostopari (identity file)

    luodaan komennolla `ssh-keygen -t rsa`

    salainen avain, yleensä id_rsa, sijaitsee lokaalissa koneessa, yleensä hakemistossa $HOME/.ssh

    julkinen avain, yleensä id_rsa.pub, sijaitsee etäkoneessa, yleensä tiedostossa $HOME/.ssh/authorized_keys (jossa niitä voi olla monta, jokainen omalla rivillään)

ssh & scp: autentikointi

- Avaimella voi olla oma salasanansa (passphrase)
- Avain + passphrase -yhdistelmällä saadaan aikaan ”two-factor authentication”: pitää kaapata sekä avain(tiedosto) että salasana ennen kuin voi autentikoitua toisena
- Vain rootin ssh-avaimella ei yleensä salasanaa

ssh & scp: autentikointi

- Esimerkki:

  ssh-keygen -t rsa

  ssh kone mkdir -p .ssh

  ssh kone 'cat >>.ssh/authorized_keys' <~/.ssh/id_rsa.pub

  tai, *jos etäkoneessa ei varmasti ole muita avaimia ennestään:*

  scp ~/.ssh/id_rsa.pub kone:.ssh/authorized_keys

ssh-agent

- Jos ssh-avaimella on salasana, sen toistuvalta kirjoittamiselta välttyy apuohjelmalla ssh-agent, joka pitää sitä muistissa session ajan. Se voi käynnistyä automaattisesti, ellei, käsin esim.

  exec ssh-agent bash

- Avaimen tallennus voi myös olla automaattista tai käsin komennolla

  ssh-add

.ssh/known_hosts

- ssh tallettaa tiedostoon ~/.ssh/known_hosts tunnettujen (aiemmin käytettyjen) koneiden avaimen tunnisteen (fingerprint). Jos avain on muuttunut, se valittaa mahdollisesta man-in-the -middle -hyökkäyksestä.
- Virheestä pääsee eroon poistamalla ao. rivin known_hosts -tiedostosta – tai rivit, niitä on yleensä kaksi (koneen nimellä ja IP:llä).
- Voi tehdä myös globaalin /etc/ssh/ssh_known_hosts

.ssh/known_hosts

- Rivin poistaminen known_hosts -tiedostosta onnistuu koneen nimelle komennolla

  ssh-keygen -R *hostname*

  tai millä tahansa editorilla (sekä nimelle että IP:lle), myös sed käy:

  sed -i 40d ~/.ssh/known_hosts

- Jos samassa koneessa pyörii useita ssh-demoneja (eri porteissa), known_hosts -tiedostoa joutuu editoimaan käsin (samalle IP:lle monta riviä)

.ssh/config, ssh_config

- ssh:n toimintaan vaikuttavia asetuksia voi tehdä globaalisti tiedostossa /etc/ssh/ssh_config tai käyttäjäkohtaisesti tiedostossa ~/.ssh/config (ks. man ssh_config). Esim.

```
AddKeysToAgent yes
CheckHostIP no
Host tt1
        Hostname tt1.student.it.jyu.fi
        User tt0
        Port 50022
        IdentityFile ~/.ssh/backup_id
```

.ssh/config, ssh_config

- Asetuksia voi eriyttää mm. käyttäjätunnuksen tai koneen mukaan match-säännöllä, esim.

  Match User ”!root,*”

  SendEnv LANG LC_*

  lähettäisi kieliympäristön paitsi jos tunnus (etäkoneessa) on root

- Muita ehtoja localuser, host, originalhost ja exec (mielivaltainen komento, tulkitaan todeksi jos palautuskoodi on nolla)

.ssh/config, ssh_config

- Asetusten prioriteettijärjestys alimmasta ylimpään on

  /etc/ssh/ssh_config

  ~/.ssh/config

  komentorivioptiot
- /etc/ssh/ssh_config siis vain oletusasetukset, ei rajoita mitä käyttäjät voivat tehdä

sshd_config

- ssh-*demonin* asetuksia (globaaleja) säädetään tiedostolla /etc/ssh/sshd_config, esim.

  PermitRootLogin prohibit-password

  DenyUsers evilguy

  AllowGroup sudo

  ForceCommand ...

- Match kuten ssh_config'issa, ehtoina user, group, host, address*, localaddress*, localport

  * myös CIDR, esim. 130.234.208.0/23

Web-palvelinohjelmistot

- apache: suurin ja kaunein, kaikki softat tukevat, mutta resurssisyöppö: www.apache.org
- nginx (”engine X”): kevyempi mutta kuitenkin ”full-featured”, kaikki edes melko usein tarvittava kalusto löytyy: www.nginx.org
- lighttpd: kevytversio, ominaisuuksia kuitenkin riittävästi useimpiin tarpeisiin: www.lighttpd.net
- paljon muitakin erilaisiin erikoistarpeisiin

lighttpd

- apt-get install lighttpd
- nano /var/www/index.html

  http://s19.vm.it.jyu.fi, http://tt1.student.it.jyu.fi

  http://130.234.209.19, http://172.20.209.19
- /etc/lighttpd/lighttpd.conf

  /etc/lighttpd/conf-{available,enabled}

lighttpd

- lighty-enable-mod userdir
- nano $HOME/public_html/index.html (ilman sudoa)

  http://s19.vm.it.jyu.fi/~tt0
- service lighttpd force-reload

lighttpd.conf

server.modules = { ... }

server.document-root = ”/var/www”

server.errorlog = ”/var/log/lighttpd/error.log”

server.username = ”www-data”

server.groupname = ”www-data”

lighttpd.conf

server.port = 80

index-file.names = { ”index.php”, ”index.html”...}

url.access-deny = { ”~”, ”.inc” }

static-file.exclude-extensions = { ”.php”, ”.pl”, ”.fcgi” }

name-based virtual hosts

- /etc/lighttpd/conf-available/95-local.conf:

  $HTTP[”host”]==”s019.vm.it.jyu.fi” {

    server.document-root=”/var/www/s019”

  }
- mkdir /var/www/s019; nano /var/www/s019/index.html

name-based virtual hosts

- sudo lighty-enable-mod local
- service lighttpd force-reload
- http://s019.vm.it.jyu.fi on nyt eri kuin http://130.234.209.19

php

apt-get install php5-cgi

lighty-enable-mod fastcgi

lighty-enable-mod fastcgi-php

service lighttpd force-reload

nano ~/public_html/koe.php

access log, dir listing

- lighty-enable-mod accesslog

  tail -f /var/log/lighttpd/access.log
- lighty-enable-mod dir-listing # ei suositeltava!

  mkdir /var/www/testi; touch /var/www/testi/kala

  http://s19.vm.it.jyu.fi/testi

busybox

- Etenkin asennusvaiheessa (avattaessa konsoli Alt-F2:lla jne), joskus muutenkin minimalistisissa asennuksissa käytettävä staattinen binääri, joka sisältää riisutut versiot yleisimmistä komennoista
- Bootin jäädessä (initramfs) -promptiin käytössä on juuri busybox

busybox

- Monissa komennoissa vähemmän optioita kuin standardiversioissa (uudemmissa busyboxin versioissa enemmän optioita)
- https://busybox.net/downloads/BusyBox.html