kill

- kill [-*signal*|-s *signal*] *pid [pid…]*

  lähettää prosessille *signaalin*
- Signaaliluettelo: `kill -l`, man 7 signal

  Tärkeimmät:

  15 TERM terminate (kill-komennon oletus)

  1 HUP hangup

  9 KILL kill (jättää tiedostot sulkematta jne)
- killall [-*signal*|--regexp|…] *nimi*

  lähettää signaalin prosesseille prosessin (tiedoston) nimen perusteella; paljon optioita (mm. prosessin ikä)

  Huom. joissakin käyttöjärjestelmissä killall tappaa kaikki prosessit!

script

- script [optiot] [*tiedosto*]
- Tekstipäätession tallentaminen myöhempää analyysia varten, *tiedosto* oletuksena **typescript**
- Optioita:

  -a, --append

  -c, --command

  -t, --timing
- Sessio päättyy kun script-komennon käynnistämä shell päättyy (exit, ctrl-d tms, shellistä riippuen)

screen

- "virtuaalinen pääteistunto"
- kätevä erityisesti huonon yhteyden takaa, ssh:n tms katkeaminen ei keskeytä pääteistuntoa vaan sitä voi jatkaa kun yhteyden taas saa
- screen [optiot] [komento]
- optioita mm.

  -r jatka taustalla olevaa istuntoa

  -d -r "kaappaa" toinen istunto
- istuntoja hallitaan (oletuksena) ctrl-a:lla, esim.

  C-a d irrota istunto (jätä taustalle)

  C-a 0 ... 9 valitse istunto numero 0-9

awk

- Skriptikieli etenkin vaihtelevanmittaisiin kenttiin jakautuvien tiedostojen käsittelyyn ja laskutoimituksien tekoon (vrt. sed)
- Kenttien oletuserotin tyhjä (välilyönnit, tab), vaihdettavissa -F:llä
- Kenttien arvoihin viitataan tyyliin $1 &c
- Komennot ryhmitellään {}:lla, ryhmän edessä voi olla ehto johon sitä sovelletaan, regexp tai yleinen ehtolauseke
- Taulukot assosiatiivisia, indeksi voi olla merkkijono
- Tulostetaan /etc/passwd:stä käyttäjätunnukset, joiden UID on alle 1000:

  awk -F: '$3<1000{print $1}' /etc/passwd
- Lasketaan yhteen xfs- ja ext4-tiedostojärjestelmien levytila:

  df -P -t xsf -t ext4 | awk '{t+=$2;u+=$3;a+=$4} END {print t,u,a}'
- Lasketaan käyttäjittäin levytilan käyttö hakemistossa:

  ls -l | awk '{t[$3]+=$5}END{for(i in t)print i,t[i]}'

expect

- Työkalu interaktiivisten tekstipohjaisten pääteoperaatioiden automatisoimiseen
- Osaa reagoida ohjelmien tulosteisiin ja toimia niiden mukaan ("keskustella" ohjelmien kanssa)
- Soveltuu myös väkisin salasanaa näppäimistöltä haluavien ohjelmien automatisoimiseen, esimerkiksi monen koneen salasanan vaihtamiseen kerralla, tai telnet-tyyppistä kirjautumista käyttävien laitteiden hallintaan
- Alla (taas yksi) skriptikieli Tcl
- https://core.tcl-lang.org/expect/index

Sekalaisia valvontatyökaluja

- vmstat, free: muistin tila
- w, who, last: käyttäjät
- uptime
- iostat, iotop: levykuorma (ja muu i/o)
- mpstat, top: prosessorikuormitus
- ip -s link, vnstat: verkkokuorma (tilastoja)
- sar: system activity reporter
- tcpdump, wireshark, iptraf: verkon käyttö
- strace: käyttöjärjestelmäkutsut
- cat /proc/{meminfo, cpuinfo, mdstat, ...}
- nagios, cacti, kgrellmd: yleisiä reaaliaikavalvontaohjelmia

Checklist: palvelu X ei toimi

- Onko tarkoituskaan toimia - löytyykö dokumentaatiota?
- Levy täynnä?
- Muisti vähissä?
- CPU ylikuormittunut?
- Lokeissa virheilmoituksia (/var/log/*)? dmesg? journalctl -xe?
- Jos lokeja ei löydy: onko (r)syslog kunnossa?
- Konfiguraatiotiedostossa (/etc/*palvelu**,* /etc/default/*palvelu)* vikaa? Typoja, näkymättömiä kontrollimerkkejä, tab-merkkejä, tyhjää rivin lopussa (etenkin \:n perässä)? (cat -vET)
- Jos prosessi ei pyöri (systemctl status, ps -ef), voiko sen käynnistää käsin? Onko debug-optiota? Tuleeko virheilmoituksia?

Checklist: palvelu X ei toimi

- Enabled-linkki puuttuu (www-palvelimissa)?
- Jonkin tiedoston tai hakemiston oikeudet, omistaja tai ryhmä väärin?
- Jokin kriittinen hakemisto tai tiedosto puuttuu kokonaan?
- Verkkokonfiguraatio pielessä, etenkin jos käyttää toista konetta tietokannalle tms: reititys, netmask, dns?
- Palomuuri liian kireällä? Jokin olennainen conntrack-moduli tms puuttuu?
- TCP wrapper pielessä?
- Kello pielessä (ntp:n portti auki palomuurissa)? Aikavyöhyke oikein?
- Palvelun tarvitsema käyttäjätunnus puuttuu, lukittu, muuten rikki?

Levytila loppu? Checklist

- Onko levytila/inodet loppu? df; df -i; grep space /var/log/syslog

  apt-get autoremove

  apt-get clean

  purge-old-kernels # paketissa "byobu"

  - voiko jotain tarpeetonta poistaa? apt-get purge ...
- Onko kryptattuja levyosioita aktivoimatta? /etc/crypttab
  - Jos on: /etc/init.d/cryptdisks force-start, tai cryptsetup luksOpen...
- Onko swappia liikaa? top, vmstat, cat /proc/swaps, swapon -s
  - Jos on: swapoff …
- Onko jotakin jäänyt mountin alle?
- Muista päivittää /etc/fstab sekä grub ja initramfs tarvittaessa

Levytila loppu? Checklist

- Mikä levytilaa syö?

  du [-s] …

  find *dir* -type f -size +10000 -mtime -7

  sudo lsof | sort -k7n
- Mikä inodeja syö?

  du --inodes …
- Mikä prosessi käyttää levynsyöppötiedostoa?

  lsof *file*

  fuser *file*
- Kuka omistaa tiedoston? ls -l *file*

Levytila loppu? Checklist

- Jos LVM käytössä:
  - Onko olemassaolevissa VG:ssä tilaa? vgs, vgdisplay
    - Jos on: lvextend... (tai lvresize), resize2fs tai xfs_growfs tai ...
  - Käyttämättömiä levyjä? pvs; ls /dev/?d?; ls /dev/disk/by-uuid
    - jos on: parted tai fdisk, pvcreate, vgextend, lvextend...
  - Onko aktivoimattomia VG:tä? vgscan
    - jos on: vgchange -a y ...
  - Voiko jotain filesysteemiä pienentää?
    - jos voi: lvreduce -r -L … *tai* umount, fsck -f, resize2fs, lvreduce

Levytila loppu? Checklist

- Ellei LVM:ää:
  - Onko jossakin osiossa tilaa?
    - jos on: mv, ln -s tai partitiointi uusiksi ja resize2fs
  - Onko käyttämättömiä levyjä tai levyllä tyhjiä osioita tai osioimatonta tilaa?
    - jos on: parted/fdisk, mkfs, mount, mv, ln -s tai jopa koko täyden partition siirto
- Onko jonkin osion/LV:n tiedostojärjestelmä pienempi kuin itse osio? resize2fs
- Osio/LV suurennettu suurentamatta kryptattua osaa? cryptsetup resize

Checklist: iptables

- Minne säännöt on talletettu ja miten ne ajetaan bootissa päälle? (/etc/network/iptables.up.{run,rules}, /etc/network/interfaces, /etc/networkd-dispatcher/...)
- Ovatko käytössä olevat säännöt samat kuin talletetut (iptables -S tai -L, tai iptables-save)?
- Onko jokin tarpeellinen palvelu sallimatta? DNS, NTP, Kerberos?
- Paluuliikenne (ESTABLISHED,RELATED) sallimatta johonkin suuntaan?
- Tarvittava apumoduli lataamatta (-j CT --helper ftp tms)?
- Onko liikenne localhostin (lo) kanssa sallittu?
- Jos säännöt lataa uudestaan (iptables-apply [-c]), tuleeko virheilmoituksia?

Checklist: iptables

- Näkyykö lokissa (/var/log/kern.log) jotain outoa? Kannattaisiko lokitusta lisätä?
- Porttinumeroissa tai -nimissä typoja?
- -s ja -d tai --sport ja --dport tai -i ja -o tai INPUT ja OUTPUT väärinpäin?
- --source ja --sport tai --dest ja --dport sekaisin?
- Puuttuuko -p tai -m jostain?
- Laite väärä -i:n tai -o:n kanssa?
- tcp ja udp vaihtuneet, tai toinen puuttuu vaikka molemmat tarvittaisiin?
- Verkkoalueissa typoja tai vääriä maskeja (/24 vs /16 tms)?
- Vastaavatko palomuurisäännöt palvelun asetuksia (ftp:n, NFS:n yms portit)?

Häirikköjahti

Miten pahantekijä löydetään?

- top
- lsof
- ps -ef, ps -fu *user,* ps -fp *pid*
- crontab -u *user* -l
- grep CRON /var/log/syslog
- atq
- /var/log/auth.log (erit. ssh-yhteydet)
- käyttäjien www-sivut (etenkin php yms)

Häirikköjahti

Mitä tehdään kun syyllinen löytyy?

- Varo liian järeitä toimia, ei pidä aiheuttaa enempää haittaa kuin on pakko (onko lääke pahempi kuin tauti?)
- kill [-9] *pid*
- chmod -x *file,* mv *file file.*tmp, rm [-f] *file*
- crontab -u *user* -r
- atrm *n*
- mv ~*user*/.ssh/authorized_key …
- usermod -s /bin/false *user*
- systemctl stop … # tilapäisesti

Varmuuskopioinnista

- "a sysadmin is only as good as their backups"
- push vs pull - kuka luottaa kehen
- full vs incremental
- media: levyt, USB-tikut, nauhat...
- koherenssi (eri tiedostoista eriaikaisia kopioita)
- avoimet tiedostot
- tietokannat
- LVM/cqow2 snapshots
- käyttöjärjestelmätuki
- salaus, avaintenhallinta
- automatisointi myös koneille jotka eivät aina päällä

PXE

- Preboot eXecution Environment
- Koneen BIOSiin tai verkkokortin firmwareen tms rakennettu verkkoboottausmekanismi
- Olennaisesti DHCP- ja TFTP-clientit ja niiden päälle rakennettu boottausmekanismi: hakee ensin itselleen IP-osoitteen ja tarvittavat parametrit (kuten tftp-palvelimen osoitteen ja ladattavan tiedoston nimen) dhcp:llä ja sitten käyttöjärjestelmän (tai sen latausohjelman) tftp:llä
- Edellyttää dhcp-palvelimelta ominaisuuksia, joita kaikissa toteutuksissa ei ole; tarvittaessa ne voidaan järjestää erillisellä proxyDHCP-palvelimella, joka välittää tarvittavat lisäparametrit vain pxe-clienteiksi tunnistetuille koneille

iSCSI

- ”internet SCSI” (Small Computer System Interface)
- Alemman tason levynjakomekanismi kuin NFS, CIFS ym: iSCSI-levy (*target)* näkyy asiakaskoneelle (*initiator*) laitteena eikä tiedostojärjestelmänä.
- iSCSIlla voidaan jakaa levyä koneesta toiseen niin, että se käyttäytyy kuten lokaali levy: sitä voidaan partitioida, käyttää LVM:n fyysisenä volumena jne.
- Yleinen datacenter-ympäristöissä ja erityisesti juuri virtuaalikoneiden kanssa.
- Mahdollistaa (virtuaalisten) levyjen migraation helposti, asiakaskoneita juurikaan häiritsemättä.
- Toimii periaatteessa kaikenlaisten SCSI-laitteiden kanssa, mutta eniten käytetään levyjen jakamiseen (joskus nauhureidenkin).
- iSCSI-palvelin on usein dedikoitu verkkolevy (tai levyjärjestelmä, *storage array*), mutta voi olla normaali palvelinkonekin (löytyy useimmille yleisille käyttöjärjestelmille).
- Ei salaa liikennettä, usein toteutettu erillisellä dedikoidulla sisäverkolla

Tietokannoista

- Ylläpitäjän näkökulmasta tietokannat ja niitä käyttävät sovellukset tuovat kaksi erityiskysymystä: käyttöoikeuksien säätämisen ja varmuuskopioinnin.
- Eri tietokannoilla (PostgreSQL, MariaDB/MySQL jne) on omat oikeuksienhallintamekanisminsa. Tietokantoja käyttävät ohjelmistot yleensä asentavat tarvittavat tietokannat ja niiden oikeudetkin kohdalleen, mutta usein niitä joutuu säätämään, erityisesti jos tietokanta on eri koneessa kuin sovellus.
- Vaikka tietokannat (yleensä) sijaitsevatkin tiedostojärjestelmässä, niiden varmuuskopiointi ei onnistu tiedostoja kopioimalla koherenssiongelman vuoksi, vaan siihen pitää käyttää ao. tietokannan omaa dumppauskomentoa (pg_dump, mysql_dump). Helpoin tapa on usein dumpata tietokanta säännöllisesti (cronilla) lokaalille levylle ja varmuuskopioida se normaaliin tapaan (vaatii pientä huolellisuutta ajoituksen kanssa ettei sitä yritetä kopioida kesken dumpin). Parempi, joskin enemmän (oikeuksien ja palomuurin) säätämistä vaativa tapa on tehdä dumppi suoraan (tai ssh:n yli), esim.

  ```
  /usr/bin/pg_dump -C -h xdbkone -U xuser xdb -f x.dump && gzip x.dump
  ```

  ```
  /usr/bin/mysqldump -h omatv -r mythconverg.dump mythconverg
  ```

Sähköpostipalvelimista

- Sähköposti on yksi monimutkaisimpia järjestelmiä sekä teknisesti että juridisesti - omaa, maailmalle näkyvää sähköpostipalvelinta ei pidä pystyttää perehtymättä asiaan kunnolla.
- Omassa palvelimessa kuitenkin voi ja on syytäkin pitää *lokaalia* sähköpostipalvelua, joka välittää postia ulospäin (ottaa sitä vastaan vain oman koneen sisältä). Tarkoitukseen voi käyttää mitä tahansa normaalia sähköpostipalvelinohjelmistoa kuten sendmail, postfix, exim jne (yleensä ns. *smarthost* -asetuksella, jolla kaikki uloslähtevä posti ohjataan tiettyyn palvelimeen) tai jotain yksinkertaisempaa kuten nullmailer. Olennainen yksityiskohta on huolehtia siitä, että lähtevässä postissa on toimiva paluuosoite, että vastaukset ja virheviestit ohjautuvat jollekin koneelle, joka osaa ne käsitellä, ja että kaikki järjestelmän generoimat virheviestit päätyvät ylläpitäjälle (usein laitetaan ylläpitäjän oikea osoite tiedostoon /root/.forward).

AppArmor & SELinux

- **AppArmor** on Ubuntun access control system *ohjelmille*: sillä voidaan rajoittaa mitä resursseja tietty ohjelma saa käyttää.
- Konfiguraatiotiedostot hakemistossa /etc/apparmor.d, tiedostonimenä yleensä ohjelman koko polku, jossa kauttaviivat korvattu pisteillä, esim. /usr/sbin/ntpd:lle /etc/apparmor.d/usr.sbin.ntpd
- Kvm-virtuaalikoneiden apparmor-profiilit ovat /etc/apparmor.d/libvirt -hakemistossa ja nimiltään muotoa libvirt-*UUID* ja libvirt-*UUID*.files
- Paikalliset muutokset ensisijaisesti hakemistossa /etc/apparmor.d/local
- **SELinux** (Security Enhanced Linux) on (etenkin RedHatin käyttämä) vastaava mekanismi: monipuolisempi ja järeämpi mutta myös vastaavasti monimutkaisempi ja vaikeampi käyttää ja konfiguroida kun apparmor.

Intrusion detection

- Tuotantokäytössä olevan palvelimen valvontaa hyökkäysten ja muiden ongelmien varalta voi automatisoida erilaisilla työkaluilla.
- IDS = Intrusion Detection System

  NIDS = Network IDS, HIDS = Host IDS, PIDS = protocol-based IDS ...
- Ohjelmia mm.
  - Tripwire
  - AIDE
  - OSSEC
  - Snort
  - Samhain
- Ei korvaa palomuuria vaan täydentää sitä (usein osana palomuuripakettia, erityisesti rautapalomuuridistroissa).

Docker

- Docker on c*ontainer* (”kontti”)-tyyppinen ”kevytvirtualisointi”: ei omaa käyttöjärjestelmää vaan käyttää alustakoneen ydintä, i/o:ta jne, mutta oma levyjärjestelmä ja osittain nimiavaruus (alustakoneen kanssa jaettua mm. /sys, osin /proc ja /dev, kernelin modulit, SELinux)
- Kevyt, vie vähän muistia (ei omaa ydintä), käynnistyy nopeasti (millisekunteja)
- Paljon paremmin alustakoneesta eristetty kuin pelkkä chroot
- Toimii myös ”oikean” virtuaalikoneen sisällä
- Kätevä tapa paketoida sovellus kaikkine kirjastoineen ja muine riippuvuuksineen

Ylläpitäjän oikeudet ja velvollisuudet

- https://www.jyu.fi/itp/ohjeet/manuals/tietoturva-ja-kayttosaannot/kayton-ja-yllapidon-saannot/tietojarjestelmien-yllapitosaannot
- Erityisesti:
  - Kaikenlainen henkilötietojen käsittely pitää perustella ja dokumentoida; huom. lokitiedot usein sisältävät henkilötietoja!
  - Omiin virtuaalikoneisiin ei saa lisätä muita käyttäjiä (eikä varsinkaan ylläpitäjiä) sopimatta siitä erikseen.
  - Ylläpitäjiä olisi kuitenkin syytä olla useita, jos koneessa ylimalkaan pyörii jokin palvelu jatkuvasti; tarvittaessa varaylläpitäjän voi saada henkilökunnasta. Palvelut kannattaa sammuttaa silloin kun niitä ei tarvita (esim. lomien ajaksi), testiviritykset päälle vain silloin kun niitä testataan.
  - Asennettaessa ohjelmia niiden lisenssit pitää tarkastaa. Ubuntun ja Debianin oletusrepositoryistä ohjelmia voi asentaa melko huolettomasti, mutta erityisesti kaupallisessa käytössä sielläkin voi olla rajoituksia (sitä tosin ei yliopiston koneilla saa tehdä muutenkaan). Muiden ohjelmien lisenssit pitää lukea tarkasti.
  - Tekijänoikeudet ja tavaramerkit pitää muistaa myös kaikenlaisen maailmalta haettujen kuvien ja muun materiaalin sekä jopa koneiden ja polkunimienkin kanssa.
  - Omaa konettaan saa skannailla mutta muita ei (ilman eri lupaa).
  - Ylläpitäjä voi joutua vastuuseen myös muiden tekemisistä, jos suhtautuu koneensa tietoturvaan leväperäisesti!