Esimerkki: levytilaongelma

- Tilanne: /usr on täynnä, /home'ssa tilaa vaikka kuinka, ei LVM:ää tai ei vapaata levytilaa VG:ssä.
- Ongelma: /home'n pienentäminen on aina vaikeaa, ei juuri koskaan onnistu ilman boottia ja voi olla vaikeaa bootatenkin (esim. jos /home on xfs, jota ei voi pienentää) ja /usr:n laajentaminen on helppoa vain jos käytössä on LVM ja volume groupissa on tilaa.
- Ratkaisu: siirretään osa /usr:stä, esimerkiksi /usr/src, /home'n alle ja linkitetään se takaisin:

  ```
  mkdir /home/usr
  mv /usr/src /home/usr
  ln -s /home/usr/src /usr
  ```

- Helppoa ja nopeaa, mutta ylläpidon kannalta jatkossa hankalaa ja virhealtista - paras kohdella tilapäisratkaisuna ja siirtää /usr/src takaisin tai omaksi tiedostojärjestelmäkseen jos ja kun levyn lisäys myöhemmin sen sallii.
- Siirrettävän alihakemiston valinnassa syytä olla varovainen, erityisesti ei pidä siirtää mitään mikä on bootissa tarpeellista. Hyviä vaihtoehtoja /usr:n alla ovat /usr/src, /usr/local ja /usr/share/doc, mahdollisesti jopa koko /usr/share; /var:n alta voi bootin puolesta yleensä siirtää melkein mitä vain, mutta se yleensä edellyttää ao. alihakemistoa käyttävien palveluiden sammuttamista (/var/run ei pidä siirtää). Ennen siirtoa pitää tietysti aina katsoa paljonko tilaa siirrettävän hakemiston alla on (tyhjää hakemistoa ei kannata siirtää).

Levytila loppu? Checklist

- Onko levytila loppu? df; df -i; grep space /var/log/syslog
  - Voiko jotain tarpeetonta poistaa? apt-get autoremove; apt-get clean; apt-get purge... ; du...; ls -l | sort -k5n; find ... -type f -size +10000
- Jos LVM käytössä:
  - Onko olemassaolevissa VG:ssä tilaa? vgs, vgdisplay
    - Jos on: lvextend... (tai lvresize), resize2fs tai xfs_growfs tai ...
  - Onko 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: umount, fsck -f, resize2fs, lvreduce
- 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 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 ...
- Muista päivittää /etc/fstab sekä grub ja initramfs tarvittaessa

Esimerkki: Kerberos ei toimi

- Jos Kerberos-autentikointi (pam) ei toimi, yleisimmät syyt ovat
  - /etc/krb5.conf virheellinen (väärä realm tms)
  - palomuuri blokkaa portin 88
  - kello on pielessä (Onko ntpd/chronyd asennettuna? Blokkaakoko palomuuri sen?)
  - käyttäjätunnus puuttuu /etc/passwd:stä (tai LDAPista tai NISistä tms)
- Autentikontiongelmista tulee yleensä virheilmoitus /var/log/auth.log'iin. Kerran sieltä löytyi tällainen viesti:

  sshd[1472]: pam_krb5(sshd:auth): (user tt) mkstemp("/tmp/krb5cc_pam_o2YOkN") failed: No such file or directory

  Jos mkstemp valittaa ”No such file or directory”, se tarkoittaa että hakemistoa, jonka alle se yrittää tilapäistä tiedostoa luoda, ei ole - ja tässä tapauksessa todellakin /tmp oli kadonnut. Syyksi osoittautui se yleisin eli ”operator error”, samasta lokitiedostosta löytyi myös tällainen:

  xx3 sudo: xx0 : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/bin/rm -r -f /tmp/

  (name changed to protect the guilty)

  ja korjaukseksi riitti:

  sudo mkdir /tmp; sudo chmod 1777 /tmp # tai chmod o=rwxt,ug=rwx /tmp
- Omia (tai muiden ylläpitäjien) tumpelointeja epäillessä voi tutkia mitä on tehty:

  zgrep sudo /var/log/authlog*

  history # komentohistoriaa voi toki selata myös nuolinäppäimillä

  cat /root/.bash_history /home/tunnus/.bash_history

Checklist: palvelu X ei toimi

- Onko tarkoituskaan toimia - löytyykö dokumentaatiota?
- Levy täynnä?
- Muisti vähissä?
- CPU ylikuormittunut?
- Lokeissa virheilmoituksia? /var/log/..., dmesg?
- Jos lokeja ei löydy: onko (r)syslog kunnossa? Lokit ohjattu poikkeukselliseen paikkaan?
- Konfiguraatiotiedostossa vikaa? /etc/*palvelu*,* /etc/default/*palvelu*
- Jos prosessi ei pyöri, voiko sen käynnistää käsin? Onko debug-optiota? Tuleeko virheilmoituksia?
- Enabled-linkki puuttuu (etenkin 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 (onko ntp tms asennettuna ja kunnossa)? Aikavyöhyke oikein?
- Tarvittava käyttäjätunnus puuttuu, lukittu, muuten rikki?

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, ...}
- nagios, cacti, kgrellmd: yleisiä reaaliaikavalvontaohjelmia

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.

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

RAID

- RAID (Redundant Array of Inexpensive Disks) on mekanismi, jolla useita levyjä yhdistämällä parannetaan turvaa levyvaurioiden varalta ja/tai levyjärjestelmän suorituskykyä.
- Useita RAID-tasoja, jotka eroavat vaurionsietokyvyn, nopeuden ja kapasiteetin suhteen, mm.

  RAID0: nopea, ei hukkaa levytilaa, ei mitään suojaa, yhden levyn särkyminen hukkaa kaiken

  RAID1 eli peilaus, kaikki data joka levyllä, paras suoja, syö paljon tilaa, nopeuttaa vähän

  RAID5: nopea lukea mutta hidas kirjoittaa, kohtalainen suoja (kestää yhden levyn särkymisen), vie vähän tilaa (yhden levyn per pakka)

  RAID6: nopea lukea, hidas kirjoittaa, hyvä suoja (kestää kahden levyn särkymisen), vie kohtalaisesti tilaa (kaksi levyä per pakka)

  RAID10 (tai 1+0): nopea sekä lukea että kirjoittaa, hyvä suoja (jopa puolet levyistä saa särkyä), vie paljon tilaa (puolet levyistä
- Virtuaalikoneissa RAIDia ei yleensä käytetä, virtuaalikonealustoissa kylläkin.
- Toteutus voi olla levyohjainkortin firmwaressa (”rautaraid”) tai käyttöjärjestelmätasolla (”softaraid”)
- LVM sisältää softaraid-toiminnallisuutta, mutta rajoitetusti eikä sitä usein Linux-ympäristöissä käytetä
- Linuxin standardisoftaraid nykyisin on md, komentorivityökalu mdadm
- md:n alla olevat levyt voivat olla myös levypartitioita eivätkä vain kokonaisia levyjä
- md:n käytön voi todeta (pseudo)tiedostosta /proc/mdstat ja sen (bootti)konfiguraation tiedostosta /etc/mdadm/mdadm.conf
- Boottaaminen onnistuu md-pakalta ainakin raid1:n kanssa, edellyttää huolellisuutta grub-konfiguraation kanssa
- md:n alla levyt voi vaihtaa isompiinkin ja ottaa koko tilan käyttöön lennosta (ei yleensä onnistu rautaraidilla)

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, rsnapshotin kanssa voi käyttää preexec skriptiä). Parempi, joskin enemmän (oikeuksien ja palomuurin) säätämistä vaativa tapa on tehdä dumppi suoraan (tai ssh:n yli), esim. rsnapshotilla:

```
backup_script     /usr/bin/pg_dump -C -h xdbkone -U xuser xdb -f x.dump && gzip x.dump  xdb/
backup_script     /usr/bin/mysqldump -h omatv -r mythconverg.dump mythconverg    mythdb/
```

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).

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

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).

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; 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!