Linux-ylläpito, kevät 2014
Verkkopalvelut

6. luentokalvosetti 21.3 – 25.4

Jani Jaakkola
jjaakkol@cs.helsinki.fi
http://www.cs.helsinki.fi/u/jjaakkol/lyp2014

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Locale: kielet ja merkistöt

Localet: Linuxin kielituki

- Linuxissa kielituki konfiguroidaan ympäristömuuttujilla, jotka on peritty POSIX-standardista
  - LC_MESSAGES: Ohjelmien käyttämä kieli
  - LC_CTYPE: Ohjelmien käyttämä merkistö
  - LC_PAPER: Paperin oletuskoko (A4 tai letter)
  - LC_COLLATE: Aakkosjärjestys
  - LC_TIME: Päivämäärän ja ajan formatointi
  - LC_MONETARY: Valuutta
  - ... ja muita
- Lisäksi:
  - LC_ALL: asettaa kaikki asetukset kerralla
  - LANG: vastaava, mutta voidaan yliajaa
  - LANGUAGE: Linuxin gettext-kirjaston väline, jolla voidaan konfiguroida lista haluttuja localeja
  - TZ: aikavyöhyke

Localet: listaus ja käyttö

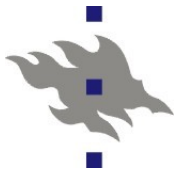
- */usr/bin/locale*
  - Käytössä oleva locale
  - Käytettävissä olevien locale-tietojen listaus
- Localet asetetaan sisäänkirjautumisen yhteydessä login-skriptien toimesta
  - Ssh-protokolla ei tiedä mitään merkistöistä, mutta osaa välittää locale-ympäristömuuttujat
  - On hyvin tyypillistä, että ssh-istunto:
    - Käyttää palvelinpäässä palvelimella localea kuin asiakas, koska ympäristömuuttujia ei välitetty, tai login-skriptit asettivat ne uudelleen
    - Asiakas ja palvelin ovat yhtä mieltä localesta, mutta tiedostojärjestelmässä merkistöt ovat jonkin muun localen mukaisia
  - Ratkaisuna on pyrkiä käyttämään kaikkialla UTF8-localea
    - Screen osaa tehdä locale-muutoksia lennossa tarpeen vaatiessa
- Ubuntussa *language-pack-FOO* -paketit

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tietokannat

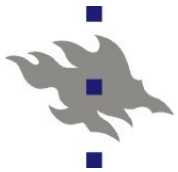
Linux ja SQL relaatiotietokannat

- Tietokantadaemonit:
  - Erotettu oman käyttäjätunnuksen taakse
  - Asiakasohjelmistot kommunikoivat joko IP- tai unix-pistokkeilla
    - Sunin JRE ei tunne unix-pistokkeita: Java-asiakkaita varten on tarjottava TCP/IP-tietokantayhteydet
- Tietokanta
  - Tietokantapalvelimen ohjelmistopaketin asennuksen tai ensimmäisen käynnistyksen yhteydessä konfiguroidaan ja alustetaan tyhjä tietokanta
  - Varmistuskopiot kannasta toteutettava erikseen: ajossa olevan tietokannan tiedostojen suoralla kopioinnilla todennäköisesti saa vain korruptoituneita varmistuskopioita
  - Tietokannan sisällä on tietokannan omat distribuutiosta erilliset käyttäjätunnukset
- OS tietokannat: MySQL ja Postgres
- Kaupallisia: Oracle ja DB2



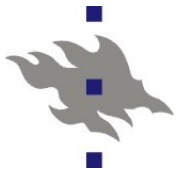
Tietokantojen käsitteitä

- Tietokantaklusteri
  - Yhden tietokantapalvelininstanssin sisältämät tietokannat
  - Tyypillisesti yksi hakemisto, josta löytyy varsinaiset tietokannat sisältävät tiedostot
  - Jokaisella klusterin tietokantainstanssilla on oma erillinen kokoelma tauluja
    - Tietokantainstanssien välillä ei voi jakaa tietoa, tai viitata toisen instanssin tauluihin
- Tietokannan sisäiset käyttäjätunnukset (tai roolit)
  - Tietokannalla on omat käyttöjärjestelmästä erilliset käyttäjätunnukset, joilla on erilaisia oikeuksia tietokannan sisäisiin resursseihin, kuten tauluihin
  - Myös superuser-tunnukset, joilla on kaikki oikeudet tietokantaan
  - PostgreSQL-tietokannassa käyttäjät ovat klusterikohtaisia
  - Autentikointi salasanalla tai unix-pistokkeilla



Tietoturva tietokannoissa

- Tietokannat syytä erottaa pahasta maailmasta
  - SQL-tietokannoista löytyy säännöllisesti tietoturva-aukkoja, joilla kannan käyttäjä voi ohittaa omat pääsyrajoituksensa tai hankkia itselleen tietokantakäyttäjän oikeudet
  - Mahdollisuuksia DOS-hyökkäykseenkin on useita
  - Vasta asennetun tietokannan oletusasetuksissa
    - Joko käytetään Unix-kikkoja varmistamaan, että vain tietyt Unix-käyttäjät pääsevät käsiksi kantoihin
    - Tai käytetään generoitua tietokannan superuser tunnusta



PostgreSQL

- Projekti aloitettu Berkeley-yliopistolla v.86
  - SQL-tuki vuonna 95
- Täydellisempi SQL- ja transaktiotuki
  - Postgres on käytössä laitoksella juuri SQL-tuen takia
  - ”the world's most advanced open source database”
- Aktiivisesti kehittyvä
  - Uusin versio 9.3.4 julkaistu 20.3.2014
- Erinomaisesti dokumentoitu
  - Linux-kurssille relevantti luku III. Server Administration:

    http://www.postgresql.org/docs/9.3/static/admin.html

PSQL: ominaisuudet

- Tietokannan sisäinen PL/pgSQL ohjelmointikieli
  - Tuki myös muille skriptikielille
- Indeksointi
- Transaktiot
- Liipaisimet (triggers): muutosten yhteydessä suoritettavat konsistenssitarkastukset
- Versiosta 9.0 eteenpäin online-replikointi
  - Versiosta 9.1 synkronoitu online-replikointi
- …jne

PSQL-tietokannan alustus

- Tietokantaklusteri (database cluster) on yhden psql-palvelimen alla oleva kokoelma tietokantoja
  - *Initdb* –komennolla alustetaan tietokantaklusteri
  - Tietokantaklusteri on hakemistorakenne missä varsinaiset tietokannat sijaitsevat
  - Tietokantaklusterilla on aina superuser-käyttäjä, jonka tunnus on oletusarvoisesti sama kuin klusterin omistava linux-käyttäjätunnus
  - Tietokantaklusterilla on merkistö
    - Uusissa tietokannoissa on syytä käyttää utf8-merkistöä
  - *PGDATA*-ympäristömuuttuja osoittaa tietokantaklusterihakemiston sijainnin tiedostojärjestelmässä
  - Tietokantatiedostoja suoraan käyttävät ohjelmat edellyttävät *PGDATA*-ympäristömuuttujan asettamista
    - mm. itse *postmaster*-daemoni

PSQL: konfigurointi

- Postgres käyttää sysv-semaforeja ja jaettua muistia
  - Kernelin oletusasetukset semaforien lukumäärälle ja jaetun muistin maksimimäärälle voivat olla liian pienet

  $ sysctl -w kernel.shmmax=134217728

  $ sysctl -w kernel.shmall=2097152
- Konfiguraatiotiedosto: *$PGDATA/data/postgresql.conf*
  - Konfiguraatiotiedoston voi valita komentoriviltä (*-c)*
  - Missä osoitteessa/portissa postgres palvelee
  - Montako asiakasta pääsee palvelimelle samaan aikaan
  - SSL-kryptauksen ja kerberos-autentikoinnin käyttö
  - Käytettävissä olevat resurssit (muisti, jaettu muisti)
  - Lokien sijainti ja kierrätys
  - Pakotetaanko muutokset levylle transaktion päättyessä?
  - Automaattinen siivous (VACUUM)
  - Ja paljon muuta

PSQL: pääsyoikeudet serverille

- Asiakasprosessien pääsyoikeuksien konfiguraatio: *$PGDATA/data/pg_hba.conf*
  - *Local*: unix-pistoke
  - *Host*: TCP-pistoke
  - *Hostssl:* SSL-kryptattu yhteys TCP:n yli
    - Asiakassertifikaatti vaaditaan jos CA-sertifikaatti on annettu
  - *database/user*: tietokanta-instanssi ja käyttäjätunnus
    - Käyttäjätunnus voi olla *All*
  - *IP/CIDR*: vaadittu IP-osoite tai osoitejoukko
  - *Auth-method*: miten autentikoidaan käyttäjä
    - Salasana, unix-pistoke, kerberos, ldap, ei mitenkään, jne.

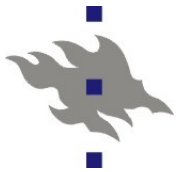
```
local      database  user  auth-method  [auth-option]
host       database  user  CIDR-address  auth-method  [auth-option]
hostssl    database  user  CIDR-address  auth-method  [auth-option]
hostnossl  database  user  CIDR-address  auth-method  [auth-option]
host       database  user  IP-address  IP-mask  auth-method  [auth-option]
hostssl    database  user  IP-address  IP-mask  auth-method  [auth-option]
hostnossl  database  user  IP-address  IP-mask  auth-method  [auth-option]
```

PSQL: Tietokannan hallinta

- Käyttäjien ja tietokantojen luonti
  - Fedoran oletusasetuksissa *postgres*-käyttäjätunnus pääsee käsiksi tietokantaan ilman salasanaa
  - *postgres*-tunnus myös on tietokannan superuser-tunnus
  - *createuser*-komennolla luodaan käyttäjätunnuksia
    - *createuser jjaakkol*
  - *createdb*-komennolla luodaan ja alustetaan tietokantoja
    - *createdb -O jjaakkol jjaakkol*
  - Tämän jälkeen Linux-käyttäjä jjaakkol pääsee *psql*-komennolla käsiksi jjaakkol-tietokantaan
    - Fedoran oletuskonfiguraatiossa käytetään paikallisia käyttäjätunnuksia suoraan postgres-autentikointiin

PSQL: Fedora asennus

- *yum install postgresql postgresql-server*
  - Asentaa asiakasohjelmiston ja palvelimen
  - Luo postgres-käyttäjätunnuksen
  - Alustaa tyhjän tietokantaklusterin oletuskonfiguraatiolla ensimmäisellä käynnistyskerralla, jos sitä ei aikaisemmin oltu alustettu (*/var/lib/pgsql*-hakemistossa)
  - */etc/rc.d/init.d/postgresql* -skripti tietokannan käynnistämistä varten
- *yum install php-pgsql*
  - Lisää postgres-tuen php-tulkkiin
- *yum install php-odbc postgresql-odbc*
  - Vaihtoehtoinen postgres-ajuri php:lle odbc-välirajapinnalla
- *yum install postgresql-libs*
  - Linuxin dll-hell: vanha postgresql-paketti ei välttämättä toimi uuden tietokannan kanssa

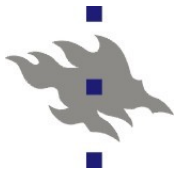


PostgreSQL Ubuntu

- Debianissa ja (siten myös ubuntussa) on viritykset, joilla useampi eri versio PSQL:stä voi olla asennettuna samalla koneelle
  - Konfiguraatiohakemisto */etc/postgresql/VERSION/main*
  - Tietokantaklusteri */var/lib/postgresql/VERSIO/main*
  - Tietokantaklusterin oletusnimi on *main*
  - Tietokantapaketin päivitys ei edellytä tietokannan uudelleen alustusta
  - Noudattaa FHS:n sääntöjä kirjaimellisesti

PSQL: rutiinit

- *VACUUM* -komento
  - Siivoa tauluissa olevan tyhjän levytilan, päivittää tilastotiedot jne.
  - PSQL-versiossa 8.1 toteutettu daemonina
- Lokien siivous
- Varmistuskopiot
  - *pg_dump* ja *pg_dumpall* komennot SQL-varmistuskopioiden tekemiseen tietokannasta tai koko klusterista
  - Vastaavasti *pg_restore* tietokannan palauttamiseen
  - Postgresin eri versiot eivät välttämättä ole keskenään binääriyhteensopivia
  - Tietokannan sisältö tällöin siirrettävä versiosta toiseen SQL-kopion kautta
  - Suoraan tiedostojärjestelmästä otetut kopiot toimivat vain jos tietokanta tietokanta oli alhaalla kopiota otettaessa



MySQL

- ”The world most popular open source database”
- Nopeampi, mutta vähemmän SQL-ominaisuuksia
  - Aikoinaan mysql ei tukenut lukituksia ja transaktioita
    - Samanaikaisuuden hallinta jäi SQL-koodaajan vastuulle
    - Edelleen SQL-koodaajan täytyy pitää huolta käytetystä taulutyypistä, riippuen siitä haluaako hän käyttää transaktioita vai toteuttaa rinnakkaisuuden hallintaa lukituksin
- Aktiivisesti kehittyvä
- 2005: Oracle osti InnoBase Oy:n
  - Oracle omisti tämän jälkeen MySQL:n relaatiotautujen toteutuksen
- 2008: Sun Microsystems osti MySQL AB:n
- 2009: Oracle osti Sunin
  - Oracle omistaa nykyään MySQL:n. Oracle tuskin antaa MySQL:n kehittyä uskottavaksi kilpailijaksi Oraclen omalle tietokannalle
- 2009: MariaDB projekti perustetaan
  - Forkkaus MySQL:n GPL-koodista
  - Wikipedia ja Google vaihtoivat tietokantansa MariaDB:hen

MySQL: ominaisuudet

- Liipaisimet (triggers)
- Useampia tietokantataulujen sisäisiä formaatteja:
  - MyISAM: tehokas ja yksinkertainen taulutyyppi, mutta vain taulukohtaiset lukitukset, eikä siten transaktioita
  - InnoDB: Lukitukset, journalointi ja transaktiot
- Transaktiot käytettäessä InnoDB-taulutyyppiä
- Replikointi
- SQL tuki edelleen vähemmän täydellinen kuin Postgres:issa
- Ei tue SQL-standardin eheystarkistuksia

MySQL: asennus ja käyttö

- Asennus:
  - *yum install mysql mysql-server php-mysql*
  - /etc/rc.d/init.d/mysql start
    - *mysql_install_db* – tietokantaklusterin alustus
    - Käynnistysskriptit alustavat tietokantaklusterin ensimmäisellä käynnistyskerralla
  - Root salasanan asetus tässä vaiheessa:

```
mysql -u root
mysql> SET PASSWORD FOR ''@'localhost' = PASSWORD('newpwd');
SET PASSWORD FOR ''@'host_name' = PASSWORD('newpwd');
```

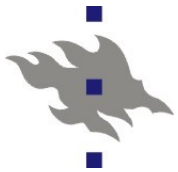
- */etc/my.cnf* – daemonin konfiguraatiotiedosto
- */var/lib/mysql* – tietokannan sijainti
- *mysqladmin* – tietokantojen hallinta
  - *mysqladmin create jjaakkol* – luo tietokannan nimeltä jjaakkol
- *Mysqldump* – tietokantojen varmistuskopiot

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Mikroverkot

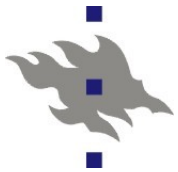
Linux ja mikroverkot

- Tarvitaan:
  - Protokolla ja ohjelmisto keskitetysti ylläpidettyjen käyttäjätunnusten jakamiseen mikroverkon työasemille
  - Protokolla tiedostojen ja konfiguraation jakamiseen
- Tavoitteita ja vaatimuksia:
  - Tietoturva: kryptaus ja palveluiden ja käyttäjien identiteetin varmistus
  - Luotettavuus: jos tunnusten jako ei toimi, ei mikroverkko toimi
    - Palveluiden replikointi: Yhden palvelun kaatuminen ei kaada koko verkkoa
    - Välimuistit: Yksittäinen työasema toimii, vaikka mikroverkko ei ole käytettävissä
  - Kertakirjautuminen (sigle sign on)
    - Käyttäjien on voitava vaihtaa ainakin salasanansa
  - Myös työasemakohtaiset käyttäjätunnukset
  - Keskitetty hallinta



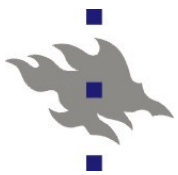
Linux mikroverkon toteutus

- Työasemissa tarvittava konfiguraatio:
  - glibc:n nss (Name Service Switch) pluginit
    - Linux-laitteiden käyttäjätunnuslistojen konfigurointiin
  - PAM (Pluggable Authentication Modules) autentikointipluginit
    - Linux-laitteiden käyttäjien autentikoinnin konfigurointiin
  - Nscd (Name Service Cache Daemon) – välimuisti Linux-laitteen käyttäjätunnuksille
  - Sssd – Välimuistidaemoni joka hoitaa käyttäjätunnusten hakemisen ja autentikoinnin
- Palvelimilla tarvittava konfiguraatio:
  - LDAP (Light Weight Directory Access Protocol) -palvelin käyttäjätunnusten ja konfiguraatiotiedon jakamiseen
  - NFS tai Samba tiedostojen jakoon
  - Kerberos kertakirjautumisten toteutukseen



PAM

- Pluggable Authentication Modules
  - Plugin-mekanismi autentikoinnin konfigurointiin autentikointia tarvitseville sovelluksille
- Olettaa, että sisäänkirjautuvan käyttäjän kanssa voi kommunikoida interaktiivisesti (tekstipohjaisesti)
  - Autentikointidialogit
    - Esim. anna käyttäjätunnus ja salasana
  - Näyttää käyttäjälle tiedotuksia ja virheilmoituksia
    - Esim your password has expired
  - Myös mahdollisesti salasanan vaihto
    - Vapaaehtoisen vaihdon lisäksi myös pakotettu vaihto
- Voidaan käyttää myös ei-interaktiiviseen autentikointiin
  - Tällöin tavallisesti oletetaan, että salasana tiedetään ilman erillistä kyselyä (esim. HTTP basic auth)

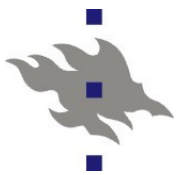


PAM: konfigurointi

- */etc/pam.d/* -hakemiston alla on oma konfiguraatiotiedosto jokaiselle pam-autentikoittia käyttävälle sovellukselle
  - Konfiguraatiotiedostossa autentikoinnissa käytettävät pam-modulit (ja modulien argumentit) niiden suoritusjärjestyksessä
  - *Required* -moduli: modulin on hyväksyttävä autentikointi, mutta kirjautumisen epäonnistuessa myös muut modulit silti suoritetaan järjestyksessä
    - *Requisite* -moduli: kuten *required*, mutta muita moduleja ei suoriteta
  - *Sufficient* -moduli: Jos tämä moduli hyväksyy autentikoinnin, ei muita moduleja ei enää suoriteta
  - Myös yksinkertainen syntaksi ehdolliseen autentikointivaiheiden ohittamiseen
- *include* -direktiivillä toteutetaan systeemin laajuinen autentikointikonfiguraatiotiedosto
  - Fedora pohjaisissa */etc/pam.d/system-auth*
  - Ubuntussa */etc/pam.d/common-auth*, */etc/pam.d/common-account* jne

PAM: konfigurointi

- Pam-konfiguraatiotiedostossa neljä eri lokeroa
  - Auth: autentikointimodulit
    - Autentikointimodulit varmistavat käyttäjän identiteetin
    - Tavallisesti kysymällä salasanaa
  - Account: käyttäjätunnusmodulit
    - Varmistaa käyttäjätunnuksen voimassaolon
  - Password: salasanan vaihtomodulit
    - Pakotettu ja vapaaehtoinen salasanan vaihto
  - Session: istunnon aloitus ja lopetus
    - Istunnon aloituksessa ja lopetuksessa suoritettavat toimenpiteet
    - Tyypillisesti suoritetaan ylläpidon oikeuksin
- *pam_unix* -moduli toteuttaa passwd/shadow -autentikoinnin ja salasanan vaihdon
- *pam_ldap* – Autentikointi LDAP-palvelimelle
- *pam_krb5* – Kerberos autentikointi ja tikettien luonti

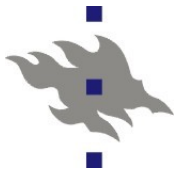


NSS: Name Service Switch

- Glibc-kirjaston sisäinen plugin-rajapinta käyttäjätunnustiedon listaamiseen
  - C-kirjaston funktiot käyttävät NSS-rajapintaa: getpwnam(), getpwuid(), getgrnam(), getgruid()
- Konfiguraatiotiedosto /etc/nsswitch.conf
- Toiminnallisuuden toteuttavat plugin-kirjastot löytyvät */lib/libnss*.so* -tiedostoista
  - Monella pluginilla on erikseen omat konfiguraatiotiedostot
- Oletuksena distribuutioissa on käytössä *libnss_files.so* -plugin
  - Toteuttaa */etc/passwd, /etc/shadow* ja */etc/group* -tiedostojen jäsentämisen
- glibc:n mukana asentuu myös *nscd* -daemoni
  - Toimii välimuistina nss-pluginien palauttamalle tiedolle
  - Osaa pitää tietoa keskusmuistissa ja levyllä

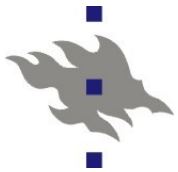
HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Mikroverkot: LDAP



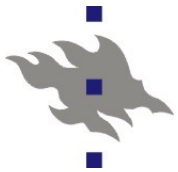
LDAP

- LDAP (Light Weight Directory Access Protocol)
  - Tieto on järjestetty hakemistohierarkioiksi
  - Tietokannanomainen tuote: hakemistoja on nopea lukea ja niihin voi tehdä tehokkaasti hakuja
    - Ei kuitenkaan transaktioita.
  - LDAP -hakemisto voi olla toteutettu oikean relaatiotietokannan avulla
  - Hakemistoja voidaan replikoida
  - Hakemistot voidaan hajauttaa useille palvelimille
    - Esim. Alihakemisto voi olla omalla palvelimella
    - LDAP-Proxyt
      - Palvelin voi antaa viitteen toiselle palvelimelle
      - Tai toimia itse proxy LDAP-asiakkaana
- Luennoijan viralline mielipide: Linux mikroverkon käyttäjätunnukset kannattaa toteuttaa juuri LDAP-protokollan avulla
  - MS:n Active Directory on myös toteutettu LDAP-palveluna



LDAP-standardi

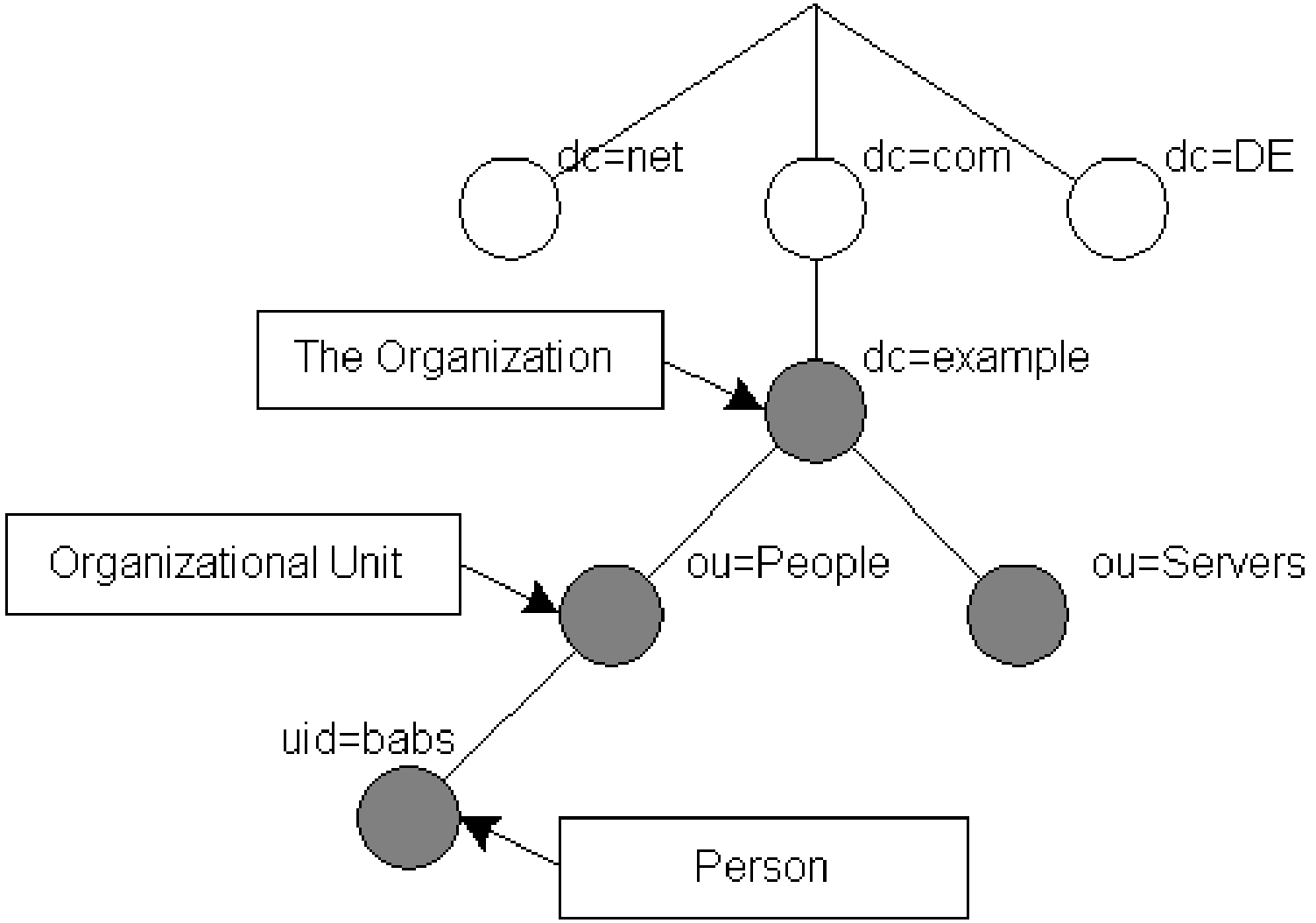
- Peräisin nyt jo kuolleesta OSI:n x.500-speksistä
  - LDAP oli vain kevyt rajapinta oikealle OSI:n DAP-hakemistopalvelulle, joka toimi täydellisen OSI-pinon päällä
  - Tyypilliseen OSI-speksin tapaan, DAP oli kovin raskas oikeasti toteutettavaksi ja käytettäväksi toteutettavaksi
  - LDAP ilmeisesti on riittävä kaikkiin tarkoituksiin joihin DAP-oli tarkoitettu(?)
- RFC2253 – Distinguished name (UTF-8 merkistö)
- RFC2251 – Itse protokolla
- RFC3377 – Lista relevanteista LDAP-RFC:istä

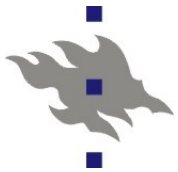


LDAP-hakemistot

- LDAP-tietue on yksikäsitteisellä nimellä (DN, distinguished name) identifioitu joukko attribuutteja
  - Attribuuteilla on nimi ja tyyppi
- Tietueet on järjestetty hakemistopuuksi
  - Nykyään tyypillisesti DNS-nimeen pohjautuvaksi
  - Hakemistosta voi olla viittaus kokonaan toiseen puuhun
- LDAP-hakemistolla on skeema
  - Skeemassa määritellään hakemistorakenne, tietueiden attribuutit, attribuuttien tyypit ja tietueiden ja attribuuttien semantiikka
  - LDAP-tietueella on useampi (mahdollisesti toisiaan periviä) luokkia (objectType)
  - LDAP-palvelin kieltäytyy skeemaa rikkovista päivityksistä
  - Yleisiä skeemoja:
    - NIS-skeema: NIS:istä tutut tiedot on kuvattu LDAP-hakemistoksi ja hakemiston tietueiden attribuuteiksi (RFC 2307)
    - InetOrgPerson: skeema henkilötiedoilla (RFC 2798)
    - X.509 sertifikaattien talletus LDAP-hakemistoon (RFC 4523)

LDAP-hakemistohierarkia





LDAP-tietue

- LDIF – LDAP Data Interchange Format
  - LDAP -tietokantaan talletetun tiedon tekstimuotoinen esitys
  - Verrattavissa relaatiotietokannasta otettuun SQL-muodossa olevaan varmistuskopioon
  - RFC 2849
  - LDIF formaatilla voidaan esittää myös tietokantaa tehtäviä muutoksia: attribuuttien lisäykset, poistot ja muutokset
- Esimerkki:

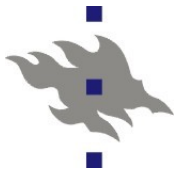
```
# jjaakkol, People, cs.helsinki.fi
dn: uid=jjaakkol,ou=People,dc=cs,dc=helsinki,dc=fi
uid: jjaakkol
cn: Jani Jaakkola
objectClass: account
objectClass: posixAccount
objectClass: top
userPassword:: 123456789
loginShell: /bin/bash
uidNumber: 4392
gidNumber: 4000
homeDirectory: /fs-2/6/jjaakkol
gecos: Jani Jaakkola
```

LDAP-autentikointi

- LDAP-palvelin on käyttäjätunnukset, joita vasten voidaan autentikoida käyttäjiä
  - LDAP-semantiikassa ”bind” tarkoittaa autentikointia
- LDAP-palvelimen käyttäjätunnukset ovat osa palvelimen hakemistohierarkiaa
  - Openldap osaa käyttää sellaisenaan posix-skeeman mukaisia käyttäjätunnuksia autentikointiin
- Autentikointityypit:
  - Anonyymi yhteys: ei suoriteta autentikointia lainkaan
  - Autentikoitu yhteys: ennen LDAP-kyselyjen suorittamista autentikoidaan (yleensä) salasanalla
  - Ylläpitäjänä autentikointi: palvelimella on erityinen ylläpito-tunnus, jolla on kaikki oikeudet tietokantaan
- Näkymä tietokantaan voi olla erilainen eri tunnuksille
  - Voidaan määritellä attribuuttikohtaisesti, mikä attribuutit näkyvät ja mitä voi käyttäjä itse muuttaa

LDAP-kysely

- LDAP-tietokantaa käytetään tekemällä sinne kyselyjä
  - Kuten SQL-kyselyt, mutta kyselykieli on paljon rajoitetumpi
- Kyselyssä tehdessä speksataan:
  - LDAP-palvelin
  - LDAP-hakemistohaara johon kysely tehdään
  - LDAP-käyttäjätunnus (voi olla anonyymi),jonka oikeuksin kysely tehdään
    - miten autentikoidaan: salasana, neuvottelu tai sertifikaatti
  - Itse kysely käyttäen LDAP-kyselysyntaksia
  - Vastauksessa halutut attribuutit (tai kaikki attribuutit)
- Komentorivityökalut palauttaa kyselyvastaukset LDIF-formaatissa



OpenLDAP

- OS LDAP-palvelin, asiakas ja kirjastot
  - Asennus: *yum install openldap openldap-server openldap-clients*
  - Migration tools perl-skriptit
    - NIS tai passwd tietokannan siirtämiseksi ldap-palvelimelle
- *slapd* – palvelinprosessi
  - Palvelu IP tai unix-pistokkeiden kautta
  - SSL/TLS-tuki
  - Eri vaihtoehtoja taustatietokannaksi
    - BDB- ja LDBM tietokantakirjastot (yksinkertainen ja tehokas)
    - SQL-tietokanta, SHELL-skripteillä lennossa generoitu data, */etc/passwd* – tiedoston jakaminen sellaisenaan
  - Replikointi (master/slave tyylinen)
  - LDAP-proxy välimuisti

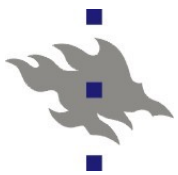
OpenLDAP asiakkaana

- *slapcat*
  - Koko tietokanta ulos LDIF-formaatisssa
    - Käyttä LDAP-tietokantaa suoraan tiedostojärjestelmän kautta
    - Ei tarvitse palvelinprosessia
    - Tarvitsee pääsyn suoraan tietokantahakemistoon
- */etc/openldap/ldap.conf*
  - Asiakkaiden oletuskonfiguraatio
- *ldapadd, ldapmodify*
  - Tietueiden lisääminen tietokantaan ja niiden muuttaminen
- *ldapdelete*
  - Tietueen poistaminen tietokannasta
- *ldapsearch*
  - Haku tietokannasta
- *ldappasswd*
  - LDAP-tietokannassa olevan käyttäjätunnuksen salasanan vaihto
  - Tai *pam_ldap* PAM-modulin avulla

OpenLDAP: käyttö asiakkaana

- Oleelliset yhteiset komentorivivivut
  - *-h <host>* ja *-H <ldap URI>*: LDAP-pavelimen valinta
  - -b <base>: kyselyhakemiston juuren valinta
  - *-D <binddn>*: LDAP-käyttäjätunnuksen valinta
  - *-x -w <passwd> -y <passwdfile>* : yksinkertainen salasana-autentikointi
- Kysely: *ldapsearch <options> <query> <attributes>*
- Muutokset: *ldapmodify <options>*
  - *-a* : tarvitaan jos lisätään uusia tietueita
- Poistot: *ldapdelete <distinguished name>*
  - Poistettavan tietueen valinta yhdellä tai useammalla *<dn>* optiolla
- Esimerkki: etsi TKTL:n LDAP-palvelimelta käyttäjän jjaakkol ryhmien gid:t

  ldapsearch -W -H ldaps://ldap1.cs.helsinki.fi
  -b dc=cs,dc=helsinki,dc=fi
  -D uid=jjaakkol,ou=People,dc=cs,dc=helsinki,dc=fi
  memberUid=jjaakkol gidNumber

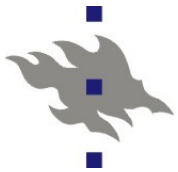


OpenLDAP: alustus ja käyttö

- LDAP-palvelin pitää laittaa SSL-kryptatun yhteyden taakse
  - LDAP-protokollossa salasanat selväkielisiä
  - SSL:n kautta palvelimen identiteetin varmistus
  - Käyttäjän oikeuksien konfiguraatio
    - Asiakaskoneiden täytyy nähdä kaikki tunnusten tiedot
      - Paitsi kenties salasanat
    - Käyttäjälle mahdollisuus vaihtaa oma salasana, kenties muitakin oman tunnuksen tietoja
- Tietokannan master käyttäjätunnuksen ja salasanan valinta
  - Tällä salasanalla pääsee muokkaamaan koko LDAP-tietokantaa
- *migrate_passwd.pl /etc/passwd passwd.ldif*
  - Konvertoi */etc/passwd* ja */etc/shadow* tiedoston ldif-formaattiin
- *slapadd*
  - LDIF-tiedoston siirtäminen suoraan openldap-tietokantaan

LDAP-palvelimen konfigurointi

- Generoidaan tarvittavat LDIF-tiedostot tietokannan populoimiseksi
  - Tarvittaessa tyhjä tietokanta
  - Generoidaan migrate-skripteillä voidaan tehdä olemassaolevasta passwd-datasta
- Konfiguroidaan */etc/openldap/slapd.conf*
  - Tässä kohtaan pitäisi generoida ja asentaa SSL-sertifikaatti
  - Tietokannan pääsyrajoitukset!
    - Myös */etc/hosts.allow*
  - Käynnistetään tietokanta
- Ladataan ldif-tiedostot tietokantaan
  - *ldapadd -v -Dcn=Manager,dc=cs,dc=helsinki,dc=fi -x -W -Hldap://localhost/ -f base.ldif*
- Testataan
  - *ldapsearch, ldapmodify*

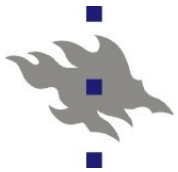


LDAP-mikroverkkoasiakas

- nss_ldap
  - Glibc nss-plugin ldap-autentikointiin
  - Konfiguraatiotiedosto */etc/ldap.conf*
  - SSL:llä Serverin identiteetin tarkastus
    - Myös asiakassertifikaatti mahdollinen
    - Tällä voidaan estää käyttäjätunnuslistan vuotaminen ulos serveriltä
- pam_ldap
  - LDAP-asiakaskoneella ei ole normaalikonfiguraatiossa oikeuksia päästä käsiksi edes salasanojen kryptattuihin salasanoihin
  - pam_ldap-moduli tarkastaa käyttäjän antaman salasanan LDAP-palvelimelta
    - Salasanan tarkastukseen asiakkaalla on oikeus
  - Ssh-palvelimesta ChallengeResponseAuth-vipu päälle

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Kerberos



Kerberos-protokolla

- Kerberos on single-sign-on protokolla käyttäjien, palvelinten ja palveluiden autentikointiin ja identiteetin varmistukseen
  - Autentikointiprosessissa varmistetaan sekä palvelun että asiakkaan identiteetti
- Käyttää ainoastaan symmetrisiä kryptausalgoritmeja
  - Ei julkisia avaimia
- Windows AD käyttää kerberos autentikointia
- Standardi: RFC 4120
- Alla olevan verkon ei tarvitse olla luotettava
- Käyttää jaettuja salaisuuksia julkisten avainten sijaan
  - Jaettu salaisuus on käyttäjän salasana tai jaettu salainen avain

Kerberos: terminologiaa

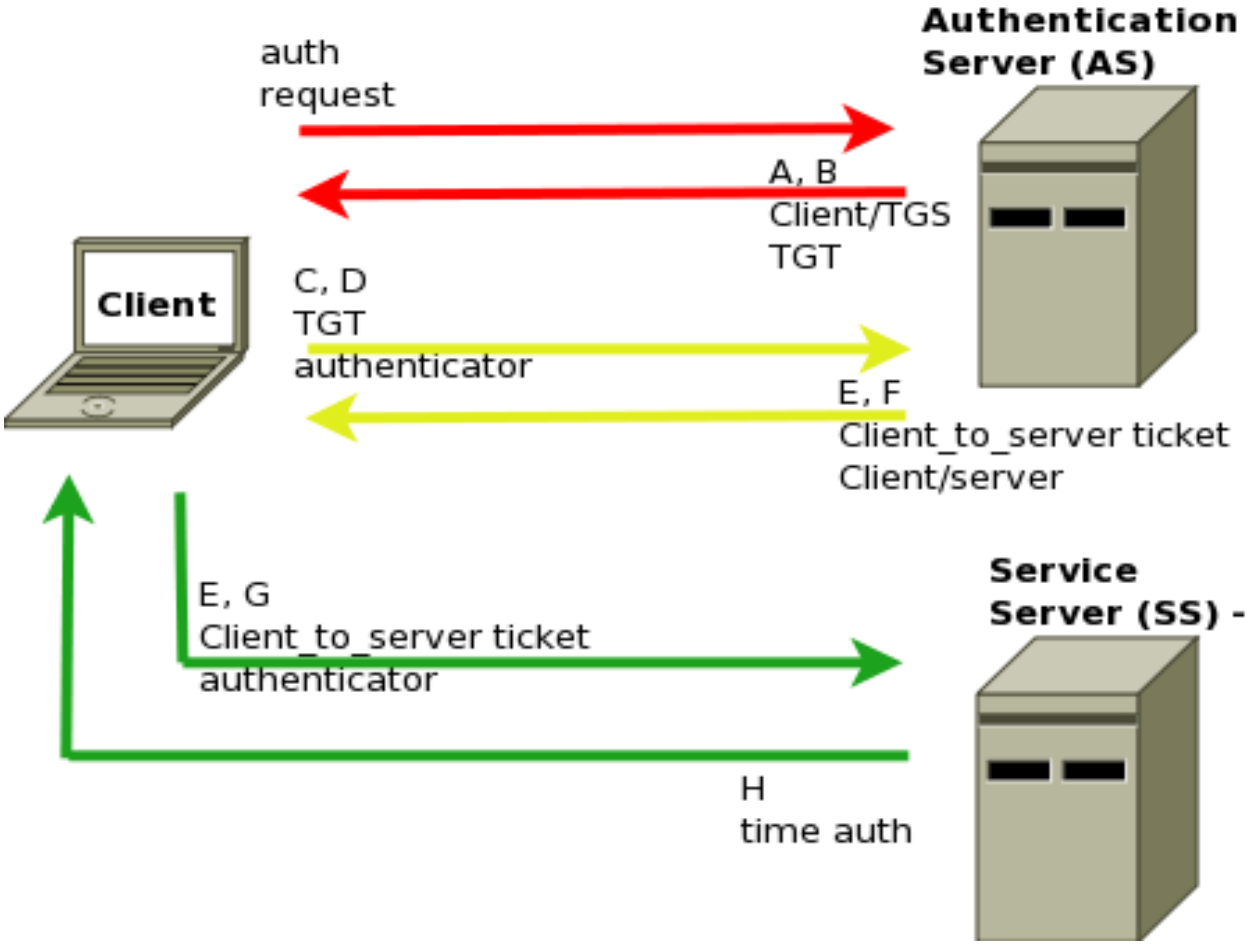
- Kerberos-toimialue (Windows domain, kerberos realm):
  - Mikroverkon alue, jolla käytetään samaa kerberos-autentikointilähdettä ja samoja jaettuja kerberos-identiteettejä
  - Tavallisesti nimetty DNS-nimellä käyttäen isoja kirjaimia. Esim CSWIN.CS.HELSINKI.FI
- Kerberos-identiteetti (kerberos principal)
  - Käyttäjä, kone tai palvelu kerberos-toimialueen sisällä:
    - Käyttäjätunnus: jjaakkol@CSWIN.CS.HELSINKI.FI
    - Konetunnus: host/melkki.cs.helsinki.fi@CSWIN.CS.HELSINKI.FI
    - Palvelu: nfs/sr3-3.cs.helsinki.fi@CSWIN.CS.HELSINKI.FI
    - Windows-konetunnus: sr3-3$CSWIN.CS.HELSINKI.FI
- Autentikointipalvelin AS (Authentication Server)
  - Toimialuetta hallitseva palvelin, jolla on hallussaan salaiset jaetut avaimet (Windows Domain Server)
- Kerberos tiketti (ticket)
  - Autentikointiprosessin tuloksena syntynyt salainen avain, jolla palveluihin autentikointi tapahtuu

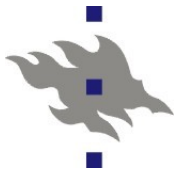
Kerberos-autentikointiprosessi

- Replay-hyökkäykset estetään käyttämällä kaikissa protokollaneuvotteluissa aikaleimoja
- Aluksi käyttäjä pyytää autentikointipalvelimelta salasanaansa vastaan TGT tiketin (Ticket Granting Ticket)
  - TGT on kryptattu käyttäjän salanalla
- TGT:n salaista avainta vasten käyttäjä saa autentikointipalvelimelta palvelutikettejä, joilla hän pääsee käsiksi varsinaisiin palveluihin
- Palvelut varmistavat omalla salaisella avaimellaan palvelutiketin kelvollisuuden ja voimassaolon
  - Ainoastaan palvelun salaisella avaimella voi purkaa AS:n palvelulle myöntämät palvelutiketit ja siten antaa kelvollinen vastaus palvelupyyntöihin
    - Samalla varmistetaan palvelun identiteetti

Kerberos autentikointiprosessi

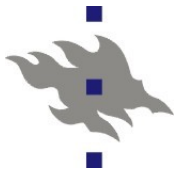
- Kuva lainattu wikipediasta
- Huom: AS ja palvelin eivät keskustele keskenään autentikointiprosessissa





Kerberos-toteutukset

- Vaihtoehtoina Heimdal-kerberos ja MIT-kerberos
  - Heimdal kerberos kirjoitettiin alunperin kiertämään Yhdysvaltojen kryptografian maastavientikieltoa
- Tyypillisesti distribuutioissa on käytössä MIT-kerberos
- Kerberos-palvelimena voi toimia Windows AD
  - Jos mikroverkossa on jo käytössä AD-toimialue, niin sitä voi (ja kannattaa) käyttää myös Linux-asiakkailla
  - Windows AD palvelin on välttämätön, jos mikroverkossa on Windows-asiakkaita



Kerberos komentorivillä

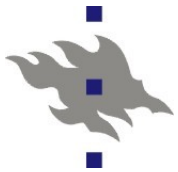
- */etc/krb5.conf* – MIT kerberoksen konfiguraatio
  - Hyväksytyt kryptausalgorimit
  - Käytetty kerberos-domain ja kerberos autentikointipalvelimet
    - Voidaan hakea myös automaattisesti DNS:stä
- */etc/krb5.keytab*
  - Lista laitteen jaetuista kerberos-salaisuuksista
  - Ainoastaan ylläpitäjän luettavissa: jos salaisuudet vuotavat, tulevat MITM hyökkäykset mahdollisiksi
- */usr/bin/kinit* – Uusien kerberos TGT-tikettien luonti salasanaa tai salaista avainta vasten
- */usr/bin/klist* – Käytössä olevien kerberos tikettien listaus
- */usr/bin/ktutil* – Salaisten avainten hallinta

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Windows AD

Windows AD: Active Directory

- MS:n ratkaisu mikroverkon toteutukseen
- Windows 2000 julkaisun mukana markkinoille tuote ratkaisu mikroverkon toteutukseen
- Toteuttaa autentikoinnin kerberos-protokollalla
- Käyttäjien ja työasematunnusten hallinta tapahtuu LDAP-protokollalla
- Linuxin LDAP- ja kerberos-työkalut toimivat AD-palvelinta vasten sellaisenaan
  - AD toimialuetta voi ylläpitää ja hallita Linuxista käsin
- *msktutil* -työkalulla voi luoda AD-konetunnuksia Linuxista käsin ja liittää Linux-työasemia osaksi AD-domainia
- Linux- ja Windows-työasematunnukset voi helposti pitää erillisinä



SSSD

- Daemoni käyttäjätunnustiedon hakemiseen ja hallintaan
  - Ylläpitää paikallista persistenttiä tietokantaa verkon käyttäjätunnuksista levyllä
  - Toimii myös offline tilassa
  - Osaa hakea käyttäjätunnukset LDAP-tietokannasta
  - Tukee kerberosta
    - Autentikointi ja tikettien hallinta (myös päivitys)
  - AD-tuki: osaa käyttää koneen kerberostikettiä AD-autentikointiin ja käyttäjätunnusten hakuun
  - Tukee useampia autentikointilähteitä
  - Modulaarinen
  - Toimii erillisillä NSS- ja PAM-moduleilla
- Konfiguraatohakemisto */etc/sssd*
- Välimuisti */var/lib/sss*
- Käytössä yliopiston AD:hen liitetyissä Cubbli-Linuxeissa

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

NFS verkkotiedostojärjestelmä

NFS verkkotiedostojärjestelmä

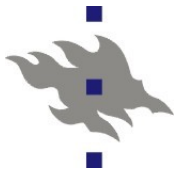
- Sunin Network File System-protokollasta on itse asiassa olemassa jo kolme eri versiota
  - NFSv2, RFC1095 vuodelta 1989
  - NFSv3, RFC1813 vuodelta 1995
  - NFSv4, RFC3530 vuodelta 2003
- Suunniteltu Unix-tyyppisiä käyttöjärjestelmiä varten
  - Tiedosto-oikeudet, hard- ja symlinkit, device-nodet, jne
- Käyttävät Sunin RPC-mekanismia
  - Portmap-daemoni, joka kertoo missä portissa varsinaiset palvelut sijaitsevat
  - Mountd-palvelu, NFS-mountin autentikointi
  - NLM, Network Lock Manager protokolla, tarjoaa tiedostolukot NFSv2 ja NFSv3 palvelimilla
  - Statd-palvelu, kaatumisista toipumiseen, erityisesti NFS-lukkojen tapauksessa

NFSv2:n ominaisuuksia

- Tilattomuus
  - Ei tunne avoimen tiedoston käsitettä
  - Toimii UDP:n yli (tavallisesti)
  - Protokolla vaatii, että onnistunut tiedostonkirjoitus on kirjoitus levylle saakka
- Tilalliset lukot eri protokollalla
  - Mekanismi lukkojen palauttamiseen koneiden kaatuessa
- NFS-tiedostokahvat
  - Ei käytetä tiedostonimiä tiedostoihin viitattaessa
  - NFS-tiedostokahva on toteutustasolla viittaus suoraan tiedoston inode-numeroon tiedostojärjestelmän ohitse
  - Tämän vuoksi NFS-toteutuksen on sijaittava kernelin sisällä: Linuxissa (ja Posixissa) ei ole API:a tiedoston avaamiseen inode-numeron perusteella

NFSv3:n ominaisuuksia

- Tuki >2GB kokoisille tiedostoille
  - Vuonna 89 tällaista ei vielä tarvittu
- Isommat luku/kirjoituspyynnöt verkossa (>8192B)
- Heikko välimuistin konsistenssi
  - Palvelin osaa kertoa jos tiedostolle on tapahtunut muutoksia, sen sijaan että asiakkaan pitäisi aktiivisesti kysyä
    - Laitoksella tämä aiheutti ”erikoisen” lukitusongelman yhdessä samban kanssa
- Palvelimelta voi kysyä tiedoston käyttöoikeuksia
- Protokollaan lisätty bitti, jolla palvelin voi vastata pyyntöön jo ennen kuin tieto on kirjoitettu levylle asti
  - Transaktio: asiakkaan täytyy pitää tieto omassa välimuistissaan palvelimen kaatumisen varalta



NFSv4

- Tilattomuudesta luovuttu
  - Samalla protokollalla tieto lukoista ja avoimista tiedostoista
  - Kaatumisista toipuminen rakennettu sisään protokollaan
  - Tiedostolukot ovat määräaikaisia, eivät pysyviä
  - Asiakas voi ylläpitää omassa välimuistissaan omaa versiota tiedostosta
    - Palvelin ottaa yhteyttä asiakkaaseen ja pyytää asiakasta vapauttamaan tiedoston, jos jokin muu asiakas tarvitsee sitä
- Tuki kerberos 5 autentikoinnille
  - Mekanismi uusien autentikointiprotokollien lisäämiseen
  - MS AD:n kerberos-autentikointi toimii sellaisenaan
- SPKM3 autentikointi sertifikaateilla
- Tuki Posix ACL -standardille
- TCP-tuki pakollinen
- Mountd-protokollasta luovuttu:
  - NFS-palvelin tarjoaa vain yhden juurihakemiston jossa varsinaiset NFS-jaot ovat alihakemistoja

NFS:n ikuisuusongelmia

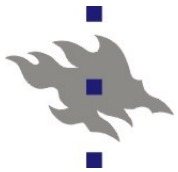
- NFS-välimuistiongelmat
  - Asiakkaat eivät näe kaikki muutoksia heti
  - Jaettujen tiedostojen käyttö NFS-asiakkaiden välillä vaatii ohjelmoijalta NFS:n omituisuuksien ymmärtämistä
  - ESTALE – auki olevan tiedoston katoaminen
- Lukko-ongelmat
  - Asiakas lukitsee tiedoston ja katoaa verkosta
    - Mikään ei siivoa tiedostolukkoa pois
- Tietoturvaongelmat
  - Aidon autentikoinnin ja kryptauksen liittäminen NFS:ään on hankalaa
- NFS-jumittamiset
  - Kun NFS-serveri kaatuu kaikki NFS:ää käyttävät prosessit jäävät jumiin D-tilaan
- Hitaus
  - UDP-vuonvalvonta ja konsistenssin ylläpidon raskaus

NFS-palvelin Linuxissa

- Asiakkaassa ja Palvelimessa:
  - *rpc.idmapd* – *uid:n* kuvaus toimialueen identiteetiksi ja takaisin
  - *rpc.gssd* – Käyttäjän tikettien välitys kernelin NFS-asiakkaalle
  - *portmap* – Paikallisten RPC-palveluiden listaus
  - *rpc.statd* – toipumispalvelu (lukkojen palautukseen)
- Palvelimessa:
  - *rpc.mountd* – Asiakkaan mount-pyynnön autentikointi
  - NFS-palvelu ja lukkopalvelu on sisäänrakennettu kerneliin
  - *rpc.rquotad* – etäquota
  - rpc.svcgssd – Asiakkaan kerberos-tikettien validointi
- Tiedostot
  - */etc/exports*
    - paikalliset NFS-jaot
  - */var/lib/rmtab*
    - NFS-asiakkaiden mounttaukset
  - */var/lib/nfs/statd*
    - Toipumispalvelun rpc.statd lista palvelimista jois

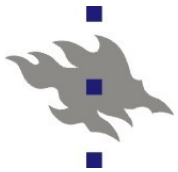
HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Samba



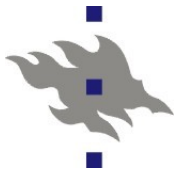
Samba

- CIFS/SMB-protokollan toteutus
  - Common Internet File System tai Server Message Block
  - SMB peräisin muinaisesta Windows for Workgroups käyttöjärjestelmästä (IPX-protokollan päällä)
  - CIFS oli MS:n yritys tehdä Sambasta Internet-standardi
  - Windows-laitteiden natiivi protokolla
- Windows-verkossa SMB tarvitaan
  - Tiedostojakoihin
  - Tulostukseen
  - Etähallinteen
- Samba-palvelin toteuttaa CIFS/SMB palvelimen
  - Itse protokolla on suurelta osin dokumentoimaton
    - Iso osa toteutuksen yksityiskohdista on selvitetty reverse engineering menetelmillä
  - Samba osaa toimia AD-toimialueessa tulostuspalvelimena ja tiedostopalvelimena (myös Windows-logon profiileille)



Politiikkapäätöksiä

- MS on hylännyt perinteiset verkossa välitettävät selväkieliset salasanat
  - Samba-palvelimet on syytä liittää aina osaksi Windows-toimialuetta
  - Jos tämä ei jostain syystä ole vaihtoehto, niin NTLM-autentikointi on edelleen käytettävissä
    - Tällöin Samba-palvelimen on säilytettävä salasanat NTLM-hasheina
- Autentikointimekanismin valinta
  - Share-level security – autentikointi yhdellä jaetulla salasanalla
  - User-level security – autentikointi käyttäjätunnuksella ja salasanalla, ei domainia
    - Salasanatietokannan valinta: smbpasswd, tdbsam, LDAP
  - ADS security – Samba on liitetty osaksi AD-toimialuetta
- Samba ei osaa toimia AD-toimialueen toteuttavana palvelimena (luotettavasti)
  - Toimi luotettavasti vain historiallisen NT-domain protokollan yhteydessä

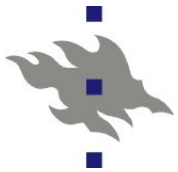


Samba-3.x

- Tuki Samban liittämiselle osaksi MS:n AD-toimialuetta
  - Osaa Windowsien LDAP/Kerberos autentikoinnin
- *net* – työkalu
  - Tarkoituksena vastata Windows:ien *net*-komennon toimintaa
  - *net ads join* – Samba-palvelimen liittämiseksi osaksi AD-toimialuetta
    - Luo uuden konetunnuksen
- Windows-tulostusajurit ja tulostinten konfiguraatio voivat sijaita samba-tulostuspalvelimelta
- LDAP-tuki
  - Samban omat tietokannat voivat sijaita LDAP-serverillä

Samba ja Linux?

- Samban avulla Linux palvelinta voi käyttää Windows-verkon
  - Tiedostopalvelimena
  - Tulostuspalvelimena
  - Wins (ennen NBNS)-nimipalvelimena
    - Wins-protokolla ei enää ole tarpeellinen
- Linux-asiakas voi Samban avulla
  - Käyttää Windows-verkon tunnuksia sellaisenaan
  - Käyttää Windows-verkon tiedosto- ja tulostuspalveluja komentoriviltä käsin
    - Eri asia kuin Linux-kernelin sisäinen CIFS-ajuri
  - Tehdä yksinkertaista Windows-verkon hallintaa Samban mukana tulevan *net* komentorivityökalun avulla
  - *Smbtar* -työkalun avulla tehdä windows-työasemista varmistuskopioita



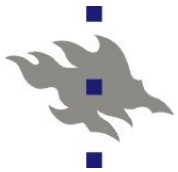
Samban konfigurointi

- Konfiguraatiotiedosto *smb.conf*
  - *.ini-tiedostosyntaksi*
  - Aluksi globaalit asetukset
  - Tiedostojakoon tai printteriin riittyvät asetukset kulmasulkeissa annetun jaon nimen jälkeen

```
[global]
workgroup = WKG
netbios name = MYNAME
security = user
[share1]
path = /tmp
[share2]
path = /my_shared_folder
comment = Some random files
```

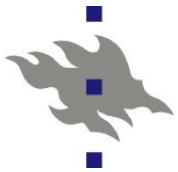
Tiedostojakojen konfigurointi

- Huomioon otettavaa:
  - Unix-puolella isoilla ja pienillä kirjaimilla on väliä, windows-puolella ei
  - Symboliset linkit näkyvät Windows-puolella aitoina tiedostoina tai hakemistoina
    - Näytä symbolisia linkkejä voi tehdä samba-jaon yli
- Konfigurointiparametreja
  - *Path*
    - Polku samballa jaettuun hakemistoon
  - *Force group, force user*
    - Pakotetaan tiedostoille annettu Linux-käyttäjä
  - *Admin users*
    - Rootin oikeuksin windowsista käsin toimivat käyttäjät
  - *Read list, write list, valid users*
    - Lista sallituista käyttäjistä
  - *Create mask, force create mode, force directory mode*
    - Unix-oikeuksien pakotus tehdyille tiedostoille



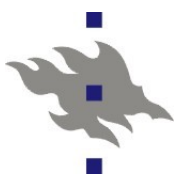
Printterijakojen konfigurointi

- Autentikointi kuten tiedostojakojen kanssa
  - Anonyymit tulostukset myös mahdollisia
- Toteutus
  - Samba vain vastaanottaa valmiita tulostustöitä Windows-asiakkailta. Linuxin oma tulostuspalvelu pitää olla jo valmiiksi konfiguroitu
- AD-toimialueessa tulostusajurit asennetaan erikseen jokaiseen tulostusta käyttävään Windows-asiakkaaseen
  - Tulostusajurit voi tallettaa samba-palvelimelle keskitetysti
    - *[printers]* jako sisältää kaikille tulostimille yhteiset asetukset
    - *[print$]* tiedostojako sisältää asennetut ajurit
    - Windows-asiakkaat automaattisesti hakevat ja asentavat ajurin
  - CUPS-postscript tulostusajurit voivat kokonaan korvata tavalliset printterivalmistajien tulostusajurit



Samba 4.x

- Ei ole valmis, testiversioita julkaistu
- Uusi Samban sisäinen VFS-malli
  - Virtuaalitiedostojärjestelmät
- ADS-palvelimen toteutus
  - KDC
  - LDAP
  - Registry
  - ACL:t



Samba Linux-mikroverkon tiedostopalvelimena

- Samba-palvelin ja kernelin SMB-ajuri toteuttavat laajennokset, jolla symlinkit ja muut unix-tiedostojärjestelmien erikoisuudet toimivat
- Samba-tiedostojärjestelmän liittämiseen tarvitaan aina autentikointi
  - Kerberos + AD tai salana
- *pam_mount* PAM-modulilla voi toteuttaa tiedostojärjestelmän liittämisen login-prosessin aikana
  - Jolloin myös käyttäjän salasana on saatavilla

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

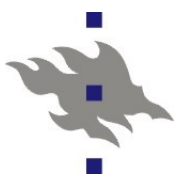
Tulostus

LPR/LPD: Berkeley Printing System

- Vanha Unixien tulostusjärjestelmä 70-luvulta
  - Nykydistroissa ei enää ole käytössä, mutta monet komentorivin tulostuskomennot periytyvät suoraan:
  - */usr/bin/lpr -Pprinter <tiedosto>*
    - Lisää tiedoston tulostusjonoon
    - Komento ei ota kantaa tulostettavan tiedoston formaattiin
    - Nykyään tavallisesti postscriptia, mutta erilaisilla suotimilla melkein mikä tahansa tiedostoformaatti saattaa kelvata
  - */usr/bin/lpq -Pprinter*
    - Tulostusjonon listaus
  - */usr/bin/lprm -Pprinter <työ>*
    - Työn poistaminen tulostusjonosta
- LPD-verkkotulostusprotokolla
  - Edelleen käytössä, valitettavasti
  - Printterit tukevat usein suoraan
  - Ei tue autentikointia eikä printterien ominaisuuksien listausta

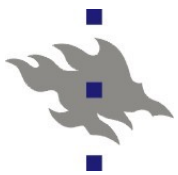
PPD-Tulostussuotimet

- Postscript Printer Description -tiedosto: *.ppd*
  - Standardi tapa listata postscript-printterin tai postscriptia ymmärtävän printteriajurin ominaisuudet
  - Antaa myös mahdollisuuden interaktiivisesti valita käytettävät printterin ominaisuudet
    - 2-puoleisuus, nidonta, paperin koko ja tyyppi jne..
  - Usein ps-tulostimen valmistaja tarjoaa valmiin tulostimen tai sen ajurin kanssa yhteensopivan ppd-tiedoston
  - ppd-tiedostoilla voi myös antaa optioita ghostscript-tulkin sisäisille tulostusajureille
- *Foomatic* on suodatinohjelmisto ja tulostintietokanta
  - Osaa tunnistaa printterin ja konfiguroida tulostusdaemonille suotimet, jotta printterille voi tulostaa postscript-tiedostoja
  - Generoi printterille tai suotimille sopivan *.ppd*-tiedoston
- *Gutenprint* on kokoelma tulostusajureita ja tulostusrajapinta
  - Alkujaan GIMP-kuvankäsittelyohjelman tulostukseen



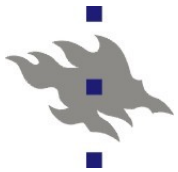
CUPS: Common Unix Printing System

- CUPS on nykyisin käytössä olevat Linux-tulostusdaemoni
  - Toteuttaa IPP-tulostusprotokollan asiakkaana ja palvelimena
    - Myös automaattisen lähiverkosta löytyvien tulostinten lisäämisen käyttöönoton
    - udev:in avulla paikallisten printterien automaattisen lisäykset ja poistot
  - Töiden jonotuksen
  - Tulostinten ja tulostinten ominaisuuksien listauksen
  - Tarjoaa kirjaston sovellusten käyttöön
    - Kirjaston kautta sovellukset näkevät ja voivat käyttää tulostinlistoja ja ppd-tiedostoja tulostuksen konfigurointiin
  - Tarjoaa WWW-käyttöliittymän palvelimen konfigurointiin
  - Tulostinajurirajapinta, ilman postscript-tulkkia
  - Toteuttaa http-pohjaisen selaimelta käytettävän käyttöliittymän tulostuspalvelimen konfigurointiin ja ylläpitoon
    - Tämän kautta myös PPD-tiedostojen asetusten konfigurointi
- Cups on myös Mac OSX:n tulostusdaemoni
  - Apple osti cupsin vuonna 2007



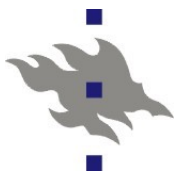
CUPS: arkkitehtuuri

- Tulostusasiakkaat
  - Kysyvät *client.conf* tiedostosta listatulta cups-palvelimelta tulostinten tiedot
- Paikallinen daemoni
  - Listaa koneeseen suoraan liitetyt paikalliset printterit ja niiden konfiguraatiot
  - Listaa broadcasteille ilmoitetut lähiverkon tulostimet
    - Protkollana Cupsin oma tai DNS Service Disvocery (dnssd)
    - Voi jakaa paikalliset tulostimet verkkoon
  - Voidaan konfiguroida pollaamaan tunnettua keskitettyä tulostuspalvelinta
- Keskitetty CUPS-tulostuspalvelin
  - Tuntee kaikki verkon tulostimet ja niiden konfiguraatiot
  - Välittää tulostuslistan lähiverkkoon broadcasteilla
  - Toteuttaa keskitetyn jonotuksen, töiden hallinan ja autentikoinnin



Cups verkossa

- IPP: Internet Printing Protocol
  - CUPS:in natiivi tulostusprotokolla
  - RFC-standardiprotokolla internet tulostukseen
  - Verkkotulostinten listaus
  - Töiden lähetys, pysäytys ja peruutus
  - Tulostinten ppd-tiedostojen listaus ja ppd-konfiguraation välitys
  - Autentikointi kaikilla http:n tuntemilla menetelmillä
  - Modernit verkkotulostimet tukevat IPP:tä
- LPD-tuki
  - Cups osaa toimia lpd-asiakkaana ja palvelimena
  - Ei toteuta lpd-jononhallintaa
- Samba-tuki
  - CUPS:in samba-tuella CUPS voi toimia tulostuspalvelimena Windows-tulostusajureita käyttäville Windows-koneille
  - Samba-backendilla CUPS voi tulostaa työn Windows-palvelimelle



CUPS asennus ja konfiguraatio

- Oletusasennuksesta pitäisi löytyä:
  - Cups-kirjastot (ubuntun *libcups2* -paketti)
  - Cups-asiakasohjelmistot: (Ubuntun *cups-client*)
  - Cups-daemoni (Ubuntun *cups* -paketti
- */etc/cups/cupsd.conf*
  - Cups-daemonin konfiguraatiotiedosto
- */etc/cups/client.conf*
  - Cups-kirjastoa käyttävien sovellusohjelmien konfiguraatio
- */etc/cups/printers.conf*
  - Tunnetut printterit listaava konfiguraatiotiedosto, automaattisesti ylläpidetty
- */etc/cups/ppd/*
  - Hakemisto tulostinten ppd-tiedostoille
  - Tulostinkohtainen konfiguraatio talletettu täne
- */var/log/cups/: access_log, error_log ja page_log*
  - Cups-palvelimen pääsyloki, virheloki ja tulostettujen sivujen loki
  - *page_log* -tiedostossa yksi rivi tulostettua sivua kohti

Cups-komentoriviltä

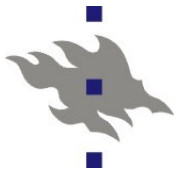
- */usr/bin/lpstat*
  - Tulostusjonojen tila
- */usr/bin/lpoptions*
  - Tulostimen tuntemat konfigurointioptiot, myös tulostinkohtaiset
  - Voi asettaa oletusoptioida *~/.lpoptions* -tiedostoon
  - Samat optiot voi asettaa myös suoraan cups *lpr*:n komentoriviltä
- */usr/sbin/lpadmin*
  - Ylläpitäjän työkalu tulostimen asetuksen konfigurointiin
- */usr/sbin/cupsctl*
  - Ylläpitäjän työkalu tulostusdaemonin konfigurointiin
- */usr/sbin/cupsenable, cupsdisable, cupsaccept, cupsreject*
  - Tulostusjonojen käynnistys ja pysäytys ja tulostusjonojen sulkeminen ja avaaminen

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Virtualisointi

Virtualisointi

- Yhdellä laitteella ajetaan samanaikaisesti useampaa käyttöjärjestelmäinstanssia
  - Instanssin käyttöjärjestelmä (KJ) on riippumaton virtuaalikoneen käyttöjärjestelmästä
  - Instanssit näkevät virtuaalisen laitteiston
    - Esim. vain osan fyysisestä laitteistosta. Instanssille on varattu vain osa koneen muistista tai CPU:ista
    - Laitteisto voi olla emuloitua. esim. Yksi fyysinen verkkokortti jaettu kaikkien instanssien kesken (virtuaalisilta)
    - Instanssin KJ:lta ei tarvita erityistä tukea virtuaalilaitteistolle
      - Virtuaalilaitteisto tavallisesti emuloi jotain tunnettua oikeaa laitteistoa (VGA-näytönohjaimet, verkkokortit, SCSI-ohjaimet)
  - Instansseja voidaan luoda ja sulkea lennossa
  - Tarvitaan ohjelmisto, joka toteuttaa virtuaalilaitteiston: hypervisor
  - Instanssi voi siirtyä fyysiseltä raudalta toiseen
    - Live Migration, jos hypervisor vain tukee



Miksi virtualisoida?

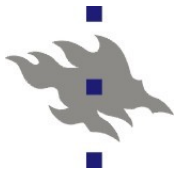
- Tehostetaan fyysisten laitteiden käyttöastetta
  - Asennetaan useita virtuaalipalvelimia yhdelle fyysiselle laitteelle
  - Hypervisor jakaa prosessoritehoa ja muistia tarpeen mukaan
- Luotettavuus
  - Riippumattomuus fyysisestä laitteesta: instansseja voi siirtää laitteelta toiselle
    - ”live migration” -tuen avulla myös ilman palvelukatkoksia
  - Virtuaalikoneen voi replikoida verkon yli toiselle laitteistoille
  - Virtuaalikoneen snapshotteja voi käyttää varmistuskopiointiin ja ongelmatilanteista toipumiseen
- Yhteensopivuussyyt
  - Tarvitaan käyttöjärjestelmää X, mutta ei haluta ostaa pelkästään sitä varten erillistä rautaa
- Tietoturvasyyt
  - Erotetaan ohjelmistot ja käyttäjät omille hiekkalaatikoilleen
- Ylläpidon ja asennuksien helppous
  - Etähallinta, etäasennukset ja monitorointi hypervisorin kautta

Virtualisoinnin huonot puolet?

- Fyysisen laitteen kaatuminen vie mukanaan kaikki laitteessa asustaneet virtuaalikoneet
  - Virtuaalikoneiden replikoinnilla pyritään välttämään tämä tilanne
- Virtuaalikoneet ovat aina jonkin verran hitaampia kuin fyysiset koneet
  - Tyypillisesti CPU-tehossa ei ole isoja eroja, IO-tehossa erot voivat olla huomattavia
- Virtuaalikoneella voi olla odottamatonta latenssia, jos muistia tai CPU-aikaa ei olekaan saatavilla juuri silloin, kun sitä tarvittaisiin
- Monet oikean laitteiston ominaisuudet eivät toimi kunnolla virtuaalikoneissa
  - Multimedia
  - 3D-kiihdytys

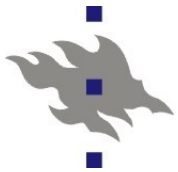
Virtuaalikonesovellukset

- Virtual Appliance
- Kokonaisia valmiita palvelinasennuksia voidaan jakaa valmiiksi asennettuina ja konfiguroituina virtuaalikonetiedostoina
- Palvelinohjelmiston mukana siis tulee kylkiäisenä käyttöjärjestelmäasennus, joka on valmiiksi konfiguroitu yhteensopivaksi palvelinohjelmiston kanssa
- Valmiita virtuaalikoneita on helppo monistaa klusteri- ja pilvilaskentakäytössä



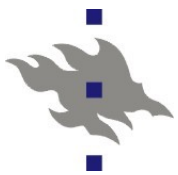
Hypervisor

- **Hypervisor** on ohjelmisto joka jakaa aidot fyysiset resurssit virtuaalikoneiden käyttöön ja toteuttaa virtuaalikonerajapinnan
  - Tyypin 1 bare bone hypervisor on itse samalla käyttöjärjestelmä
    - MS:n Hyper-V, VMWaren ESX
  - Tyypin 2 hypervisor toimii **isäntäkäyttöjärjestelmän** (Host OS) alla
    - Isäntäkäyttöjärjestelmä toimii kuten normaali KJ, mutta jakaa osan resursseista hypervisorin käyttöön
    - Tyypillisesti hypervisor tarvitsee KJ:lta lisäpalveluita, joita tavalliset sovellukset eivät tarvitse
      - Linuxissa KVM tai erilliset kernelin modulit
  - Hypervisorin toteuttamaan virtuaalikoneeseen asennettua käyttöjärjestelmää **vieraskäyttöjärjestelmäksi** (guest OS)
    - Vieraskäyttöjärjestelmään voidaan tehokkuussyistä haluta asentaa erillisiä virtuaalilaiteajureita, jotka toimivat tehokkaammin kuin aidon raudan emulointi



Hypervisorin käyttö

- Hypervisor tarjoaa:
  - Mahdollisuuden uusien virtuaalikoneiden luomiseen
    - Varataan levytila, CPU:t ja virtuaaliset verkkolaitteet
    - Virtuaalikone voi myös nähdä oikeita fyysisiä laitteita
      - Esim. Levypartitioita tai USB-väyliä
  - Virtuaalikoneen käynnistyksen virtuaaliselta medialta
    - Cdrom, dvd, verkkobuutti, kovalevy
  - Virtuaalikoneiden suspendointi
  - Snapshotit virtuaalikoneista
  - Virtuaalikoneiden exporttaus ja importtaus
    - Eri hypervisoreilla on omat epäyhteensopivat formaatit instanssien talletukseen
  - Konsolin luoduille virtuaalikoneille
    - Näytönohjaimen, näppäimistön ja hiiren emulointi
  - Resurssien käytön monitoroinnin
  - Käyttöliittymän ja API:n

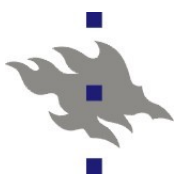


Virtuaalikonetyypit: Emulointi

- Virtuaalilaitteisto on toteutettu ohjelmistolla
  - Emuloidun laitteiston ei tarvitse olla sama kuin fyysisen koneen
  - Toisaalta emulointi on ainoa vaihtoehto, jos fyysinen rauta ei ole yhteensopivaa
- Usein kertaluokan verran hitaampaa kuin koodin natiivi suoritus
  - Tämä ei ole kuitenkaan kiveen kirjoitettu sääntö: Just In Time kääntäjät voivat olla hyvin tehokkaita
- Ei tarvitse virtualisointitukea isäntäkäyttöjärjestelmältä eikä laitteistolta
- Esim. Qemu

Virtuaalikonetyypit: paravirtualisointi

- Paravirtualisoinnissa vieraskäyttöjärjestelmä toimii yhteistyössä hypervisorin kanssa
  - Intelin käskykannassa on joitain käskyjä, joiden suoritus virtuaalikoneessa järjestelmävalvojatilassa aiheutti poikkeuksen ja jotka oli emuloitava
  - Paravirtualisoinnissa vieraskj ei suorita näitä komentoja ollenkaan, vaan käyttää hypervisorin tarjoamia palveluja
  - Vieraskäyttöjärjestelmä ei oleta, että fyysiset prosessorit ja muistit ovat aina välittömästi sen käytettävissä
  - Edellyttää että vieraskj on muokattu käyttämään hypervisorin palveluita
- Paravirtualisointi on potentiaalisesti tehokkaampaa
  - Ei turhaa emulointia
  - Ei tuhlata laitteistoresursseja, jotka eivät oikeasti ole käytössä
- Esim. Xen

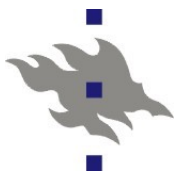


Virtuaalikonetyypit: Laitteistotason virtualisointi

- Vieraskäyttöjärjestelmään ei tehdä muutoksia
  - Vieraskäyttöjärjestelmää pyöritetään sellaisenaan oikealla laitteistolla
  - Tämä voi edellyttää joidenkin konekäskyjen emulointia poikkeuksien kautta hypervisorilla
- Intel ja AMD tukevat laitteistovirtualisointia
  - AMD:n AMD-V laajennos kaikissa uusissa AMD CPU:issa
  - Intelin VT-x laajennos suuressa osissa CPU:ita
- Vieraskäyttöjärjestelmä voi kuitenkin tarvita erillisiä ajureita virtuaalilaitteistolle
  - Usein kuitenkin virtuaalilaitteet näyttävät joltain yleisesti käytetyltä vanhalta laitteelta ja voidaan käyttää olemassa olevia vanhoja ajureita
    - Esim. Vmwaren virtuaaliverkkokortit ja SCSI-ohjaimet
- VMWare, KVM ja Xen kaikki tukevat laitteistotason virtualisointia

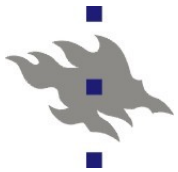
Virtuaalinen IO-laitteisto

- Hypervisor tavallisesti osaa emuloida joitain aitoja fyysisiä IO-laitteita:
  - Gigabitin verkkokortti (tyypillisesti Intelin e1000)
  - Yksinkertainen ei-kiihdytetty VGA-näytönohjain (tyypillisesti Cirrus)
  - SCSI RAID-ohjain
  - Äänikortti
- Aitojen laitteiden emulointi ei ole tehokasta
  - API:t suunniteltu laitteita varten, ei ohjelmistoja
- Paravirtualisoitujen IO-laitteiden API:t ovat nimenomaan virtualisointia varten suunniteltuja
  - Kommunikointi hypervisorin kanssa tapahtuu jaetun muistin kautta
  - VMWaressa modulit vmxnet3, vmw_pvscsi, wmw_balloon
  - KVM+qemu: OS virtio ajurit



Ohjelmistoja ja yrityksiä

- Virtualisoinnista on tullut bisnestä (ja jopa hypeä)
- Oracle: Solaris Zones
  - Solariksen virtualisointi
- Oracle: VirtualBox
  - Helppokäyttöinen työpöytävirtualisointiympäristö
- MS: Hyper V
  - MS:n oma hypervisor, tukee myös virallisesti Linuxia
- Citrixin XEN
- KVM – Kernel Virtual Machine
  - Linuxin kernelistä löytyvät tuki virtuaalikoneiden toteutukselle käyttäjätason prosesseina
- Qemu: Prosessori ja laitteistoemulaattori
- *Virt-manager:* daemoni, API, komentorivityökalut ja käyttöliittymä KVM+Qemu virtuaalikoneiden hallintaan
- VMWare
  - Monta eri tuotetta eri markkinasegmenteille
  - ESX barebone hypervisor

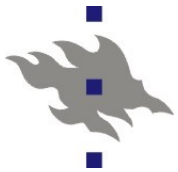


XEN

- Käynnistyslataaja lataa ylemmän tason XEN-hypervisor minikäyttöjärjestelmän
  - Toimii Intel-prosessorien suojaustasolla 0
  - Virtuaalikoneissa tasolla 1 pyörivät käyttöjärjestelmät pyytävät hypervisorilta resursseja käyttöönsä: muistia, laitteistoa, keskeytyksiä
    - Hypervisor siis tarjoaa paravirtualisointirajapinnan
- Domain0 instanssi:
  - Modifioitu isäntäkäyttöjärjestelmä (Linux, NetBSD tai Solaris), jonka xen-hypervisor käynnistää automaattisesti
  - Isäntäkäyttöjärjestelmä toteuttaa fyysiset laiteajurit ja tarjoaa ne hypervisorin käyttöön
  - Ylläpitäjä kirjautuu sisään domain0 instanssiin ja sieltä käsin ylläpitää vieraskäyttöjärjestelmiä

KVM ja Virtual Machine Manager

- Kernel-based Virtual Machine
  - KVM on kernelin moduli, joka tarjoaa käyttäjätason ohjelmistolle rajapinnan (*/dev/kvm*), jonka avulla käyttäjätasolta voidaan toteuttaa virtuaalikoneita
    - Tarvitaan AMD:n tai Intelin virtualisointilaajennokset
  - Mahdollistaa laitteistopohjaisen virtualisoinnin
- Qemu ja Virtualbox ovat KVM-rajapintaa käyttäviä hypervisor ohjelmia
- *Virtual-manager* ohjelmistolla ylläpidetään virtuaalikoneita
  - *libvirtd* – daemoni joka käynnistää virtuaalikoneet
  - *virsh* – Yleiskäyttöinen komentorivityökalu virtuaalikoneiden hallintaan
  - *virt-manager* – GUI työkalu virtuaalikoneiden hallintaan
  - *virt-clone* ja *virt-image* – Virtuaalikoneiden kloonaus ja konfigurointi valmiin imagen pohjalta

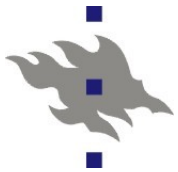


VMWare

- VMWare
  - Pitkä lista vaihtoehtoisia virtualisointituotteita eri käyttötarpeisiin (ja lompakon paksuuksiin)
  - VMWare Infrastructure
    - Maksullinen useista fyysisistä koneista koostuvan virtuaalikoneverkon hallintajärjestelmä
  - VMWare ESX
    - Bare Bone-tyyppinen Linux-pohjainen käyttöjärjestelmäasennus, jossa isäntäkäyttöjärjestelmä tarjoaa vain verkkopalvelut virtuaalikoneiden ylläpitoon
  - VMWare Workstation
    - Työasemalle asennettava virtuaalikoneohjelmisto
  - VMWare Player
    - Virtuaalikonesovelluksia suorittava ilmainen ohjelmisto
    - Ei tue virtuaalikoneiden luontia

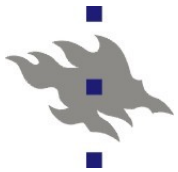
HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Sähköposti



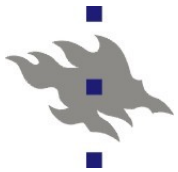
Sähköposti

- Sähköpostin välitys internetissä on aidosti hankala asia
  - Historiallista painolastia on paljon
  - Näiden luentojen pohjalta ei pidä mennä pystyttämään ISP:n tai edes domainin sähköpostipalvelinta
- Postinvälitysprotokolla SMTP
  - SMTP – Simple Mail Transfer Protol
    - RFC821 vuodelta 1982
    - Tällä protokollalla meilit välitetään edelleen
  - ESMTP – Mekanismi uusien ominaisuuksien neuvotteluun SMTP-yhteydessä
    - RFC1896 vuodelta 1995
    - Mahdollistaa 8-bittiset merkistöt, TLS-yhteyden neuvottelun, yhteyksien autentikoinnin jne..



SMTP-postinvälityksen osapuolet

- MUA – Mail User Agent
  - Käyttäjän työpöydällä oleva sähköpostiohjelma
  - Thunderbird, mozilla, evolution, kmail, pine
- MSA – Mail Submission Agent
  - Palvelin, jolle MUA välittää viestin edelleen siirrettäväksi
  - Ei välttämättä käytä SMTP-protokollaa
    - Unixeissa MSA:na toimii */usr/sbin/sendmail* binääri (tai wräpperi)
    - MSA:n ei silti onneksi tarvitse olla sendmail
      - Muut MSA:t emuloivat sendmail:in /usr/sbin/sendmail komentoa (jonkin verran)
- MTA – Mail Transfer Agent
  - Välittää sähköpostit vastaanottajapalvelimelle tai välityspalvelimelle (relay)



SMTP-postinvälityksen osapuolet

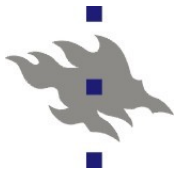
- Välityspalvelin (SMTP-relay)
  - SMTP-protokollassa ei oleteta suoraa yhteyttä lähettävän ja varsinaisen vastaanottavan SMTP-palvelimen välillä
  - Välityspalvelimia käytetään:
    - Sähköpostien jonottamiseen varsinaisen palvelimen ollessa alhaalla
    - Kuorman tasoittamiseen
- MDA – Mail Delivery Agent
  - Toimittaa sähköpostit vastaanottajan MUA:n saataville
  - *procmail*
  - POP-protokolla
  - IMAP-protokolla

SMTP:n ominaisuudet

- Historiallisesti tavoitteena mahdollistaa viestinvälitys isojen keskuskoneiden välillä – eikä mitään muuta
  - Alkujaan ei minkäänlaista autentikointia
  - Ihmiset eivät kantaneet viestinvälitykseen pystyviä koneita povitaskuissaan
  - Kaikki SMTP-palvelimet suostuivat toimimaan välityspalvelimina kaikille muille palvelimille
  - Spam ja virukset olivat vielä keksimättä
  - Ei minkäänlaisia identiteettitarkistuksia
- Kirjekuoren käsite (envelope)
  - envelope sender ja envelope recipient
  - SMTP-protokollassa neuvotellaan erikseen vastaanottajan osoite ja osoite johon mahdolliset virheet palautetaan
  - Näillä osoitteilla ja välitetyn meilin sisällössä näkyvillä osoitteilla ei välttämättä ole mitään tekemistä keskenään!

Lisää SMTP:n ominaisuuksia

- Välityspalvelimet
  - Viestin ei tarvitse kulkea suorinta mahdollista reittiä
  - Lähettävän MTA:n ja vastaanottavan MTA:n välissä voi olla mielivaltaisen monta välityspalvelinta
  - Redundanssia ja kuorman tasausta
- Viestijonot
  - MTA:t varautuvat tietoliikennekatkoksiin, kuormitustilanteisiin ja palvelinten kaatuiluun viestijonoilla
- Vaihtoehtoiset vastaanottaja MTA:t
  - Domain voi listata DNS-tietueissaan useita viestejä vastaanottavia palvelimia ja niiden väliset prioriteetit



SMTP autentikointi

- Nykyään kaikki tulevat SMTP-yhteydet joudutaan jotenkin autentikoimaan
  - Ammattimaiset spammerit löytävät nopeasti avoimet välityspalvelimet
  - Siksi MTA:t konfiguroidaan välittämään eteenpäin ainoastaan omasta domainista tulevat viestit
    - mail.cs.helsinki.fi -palvelin suostuu välittämään kaikki cs.helsinki.fi-domainin IP-osoitteista tulevat viestit
    - Vastaavasti ISP:iden meilipalvelimet suostuvat välittämään eteenpäin vain ISP:n omista IP-osoitteista tulevat viestit
    - Ficora on komentanut ISP:t oletusarvoisesti blokkaamaan SMTP:n kokonaan asiakasliittymistä (27.8.2004)
  - Oman domainin ulkopuolelta tuleville viesteille
    - Vaaditaan ennen viestin välitystä SMTP-autentikointi, salasanalla tai muulla menetelmällä (POP-before-SMTP)
    - MSA-portti, jossa vaaditaan aina autentikointi

MTA välinen autentikointi

- Viestit joiden recipient -osoite on MTA:n vastaanottamassa domainissa täytyy perinteisesti päästää läpi ilman autentikointia
  - Ja spam ja virukset leviävät
  - Ratkaisu #1: mustat listat
    - Ei vastaanoteta tunnettujen spämmiä lähettäviä palvelinten viestejä
    - Ei vastaanoteta tunnettujen kuluttajaliittymien IP-osoitteista lähetettyjä meilejä (ts. Vaaditaan jokin ISP:n MTA väliin)
    - ISP:t blokkaavat myös itse kuluttajaliittymien SMTP-liikennettä
  - Ratkaisu #2: jonain kauniina päivänä globaali MTA-palvelinten välinen autentikointi:
    - SPF
    - MS:n Sender-ID

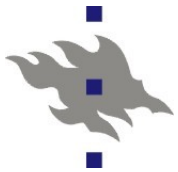
SPF – Sender Policy Framework

- Menetelmä jolla viestin domainista X vastaanottava MTA voi varmistua siitä että viestin lähettävällä MTA:lla on oikeus lähettää viestejä domainista X
  - Domainin X DNS-tietueisiin on lisätty lista domainin X MTA-palvelimista
  - SPF suojaa SMTP:n envelope-sender kentän väärennöksiltä
  - viestin sisäisessä From: -kentässä voi edelleen lukea mitä tahansa
  - SPF voi aiheuttaa ongelmia viestien edelleenlähetykselle
  - Kyseenalaista auttaako spam-ongelmaan lainkaan

```
x40-4:~$ host -t TXT cs.helsinki.fi
cs.helsinki.fi text "v=spf1 ip4:128.214.9.1 ip4:128.214.9.2 ~all"
```

Miksi MSA työasemassa?

- MUA:n voi konfiguroida lähettämään viestit suoraan keskitetylle MTA:lle
  - MSA työasemassa ei ole lainkaan välttämätön
- Työasemassa olevan MSA:n edut
  - Mahdollistaa paikalliset postilaatikot
  - Keskitetty paikka konfiguroida tunnelointi organisaation varsinaiselle MTA:lle
  - Postien paikallinen jonotus verkkokatkosten vuoksi
    - Ei pelkästään hyvä asia: käyttäjät eivät välttämättä huomaa postin jääneen jonoon
  - Mahdollistaa viestien lähetys daemoneilla ja skripteille jotka eivät osaa puhua SMTP:ta

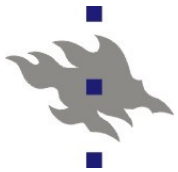


Erilaiset meilikonfiguraatiot

- Kiinteä työasema intranetissä, ei paikallisia postilaatikoita
  - Helppo tapaus
  - Paikallinen MSA yksinkertaisesti toimittaa kaikki viestit eteenpäin domainin MTA:lle
  - Ei kuuntele ulkoista SMTP-porttia lainkaan
- Työasema, jolla on joitain paikallisia postilaatikoita
  - Tyypillinen distron asennuksen jälkeinen oletuskonfiguraatio
  - Daemonien generoimat viestit toimitetaan paikallisiin postilaatikoihin
  - Loput toimitetaan edelleen eteenpäin domainin MTA:lle
  - Ei kuuntele ulkoista SMTP-porttia lainkaan

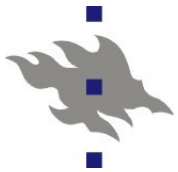
Lisää meilikonfiguraatioita

- Liikkuva työasema vaihtuvalla IP-osoitteella
  - Kannettavat, joiden verkko vaihtuu sen mukaan missä ne kulloinkin sattuvat sijaitsemaan
  - Liikkuvan työaseman MSA:n pitää tällöin
    - Osata vaihtaa käytössä oleva MTA aina IP-osoitteen vaihtuessa
    - Tai autentikoida itsensä jollekin kiinteällä MTA:lle
    - Tai unohtaa paikallinen MSA ja jättää ongelma kokonaan käyttäjälle ja MUA:lle
- Varsinainen keskitetty meilipalvelin
  - Toimii domainin työasemien välityspalvelimena
  - Vastaanottaa domainiin tulevat viestit
  - Sisältää domainin käyttäjien postilaatikot
  - Suodattaa viestejä



Postilaatikot

- Tiedostojärjestelmässä:
  - Perinteinen mbox-formaatti
    - Meilit peräkkäin yhdessä tekstitiedostossa From-riveillä eroteltuna
    - Tehoton, ainakin ilman erillistä indeksointia
  - Maildir-formaatti
    - Meilit yksittäisinä tiedostoina hakemistossa
  - Kumpaakin voi jakaa NFS yli
- Erilaiset tietokannat
- POP-etäpostilaatikko
  - Käyttäjän MUA hakee säännöllisesti serverille saapuneet viestit ja säilöö ne käyttäjän työasemalle
- IMAP
  - Viestit ja arkistot pysyvät palvelimella
  - Postilaatikoita voi olla useita ja ne voivat olla jaettuja



SMTP-ongelmien debuggaus

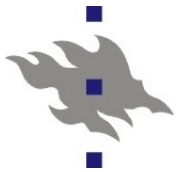
- Viestin kaikki otsakkeet
  - Kun käyttäjää pyytää forwardoimaan ongelmatapauksen eteenpäin otsakkeet lähes aina hukkuvat matkalla
- MTA:n lisäämät Received: -otsakkeet ovat ainoa keino selvittää viestistä mitä sille oikein matkalla tapahtui
- Envelope-Sender ja Return-Path voivat olla hyödyllisiä
  - Kuten todettua From: ja To: kentät eivät välttämättä kerro mitään
- MTA:n loki

Linux MTA:t

- Sendmail
  - Ikivanhaa softaa – Yhtä vanha kuin SMTP
  - Monimutkainen, hankarasti konfiguroitava historiallinen jäänne
  - Muut MTA-softat tyypillisesti ovat jonkin verran komentoriviyhteensopivia sendmail:in kanssa
- Exim
  - Debianissa
- Qmail
  - Dan Bernstein - ”Threat or Menace”
- Postfix
  - Helppo, ei asenneongelmia
- Courier
  - Integroitu SMTP, IMAP, POP, LDAP, SSL ja HTTP
  - Käytössä laitoksella

Sendmail

- Näistä ei varmaan koskaan pääse eroon
  - Siksi hyvä ymmärtää jonkin verran sendmailin toiminnasta
- Konfiguraatiotiedosto */etc/mail/sendmail.cf*
  - Hillitön makrohässäkkä jossa itse asiassa on suuri osa meilien käsittelyn toteutuksesta
  - Nykyään kyseinen konfiguraatiotiedosto itse asiassa generoidaan m4-makroilla */etc/mail/sendmail.mc* tiedostosta
- Jonkinlainen tuki kaikelle mahdolliselle
  - Jos vain osaa konfiguroida
  - Myös meilinvälitykselle ilman SMTP:tä
- Paikalliset aliakset */etc/aliases* tiedostossa
- Nykyään MSA ja MTA toiminto eriytetty eri käyttäjätunnuksille



Postfix

- Luennoijan suositus uuteen työasema-asennukseen
- Helpohko konfiguroida
- Ei pahoja asenneongelmia
- Ei liikaa historiallista painolastia
- Hyvä dokumentointi
- Tärkeimmät ”uudet” ominaisuudet tuettu
  - STARTTLS TLS-yhteyden neuvottelu
  - SASL SMTP-autentikointi