HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Linux-ylläpito: Verkkopalvelut

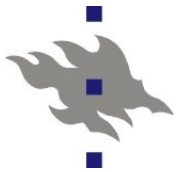
Jani Jaakkola
jjaakkol@cs.helsinki.fi
http://www.cs.helsinki.fi/u/jjaakkol/lyp2010/

Esimerkkivastaus

1. Miten asetat apachella seuraavat pääsyrajoitukset hakemistopolun /home/fs/*/intranet takaa tarjoiltaville tiedostoille (ilman .htaccess-tiedostojen apua):
   a. Vaaditaan ssl-kryptattu yhteys
   b. Tiedoston hakijan täytyy ensin autentikoida itsensä http basic autentikaatiolla. Käyttäjätunnukset ja salasanat löytyvät tiedostosta */etc/wwwusers*

- Vastaus:

<Directory /home/fs//intranet>*
SSLRequireSSL
AuthType Basic
AuthName "Salasana tarvitaan "
AuthUserFile "/etc/wwwusers"
require valid-user
</Directory>

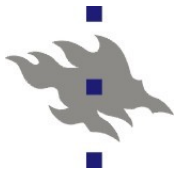


Esimerkkivastaus

- 2. Oletetaan että käyttäjien kotihakemistot ovat kaikki polun */home/fs/login_name/* takana. Miten konfiguroit apachen palauttamaan URL:in *https://serveri/i/login_name/foo.html* takaa tiedoston */home/fs/login_name/intranet/foo.html*
- Vastaus:

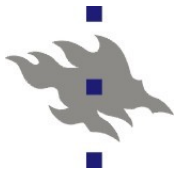
  AliasMatch "^/i/([a-z0-9_]+)$" "/home/fs/$1/intranet/"

  AliasMatch "^/i/([a-z0-9_]+)/(.)" "/home/fs/$1/intranet/$2"*



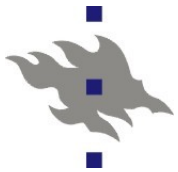
Java palvelut: Java EE

- Java Platform, Enterprise Edition, (oli: J2EE)
  - Speksi ja API web-palvelujen toteuttamiseen javalla
    - WWW-palvelut (servletit), tietokantarajapinta (JDBC), xml, etäproseduurikutsut (RMI), jne
  - Java EE sovellukset ovat (teoriassa) laitteisto-, KJ- ja toteutusriippumattomia
  - Sunin JDK on nykyään avoin ja löytyy distribuutioista
- Linux-ylläpitäjälle näkyvät osat:
  - Java EE sovelluspalvelin, jossa sovellukset toimivat
    - Sovelluspalvelinvaihtoehtoja on paljon: Tomcat, Jboss, IBM Websphere, Sun Java System Application Server...
  - Sovelluksella on standardoitu hakemistorakenne
    - Hakemiston voi zip-pakata Web Archive (WAR)-tiedostoksi
    - Hakemisto tai .war-tiedosto annetaan sovelluspalvelimen suoritettavaksi
  - J2EE-sovelluksilla on oma java-hiekkalaatikko



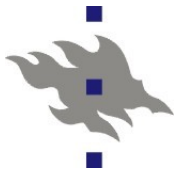
Java EE -sovellus

- Fedoran tomcat-paketissa asentuvat */var/lib/tomcat5/webapps* -hakemistoon
  - Oletuskonfiguraatiolla *webapps/<sovelluksen_nimi>* hakemistosta tiedostot näkyvät aivan kuin näkyisivät tavallisesta http-palvelimesta
    - *http://tomcat.serveri:port/<sovelluksen_nimi>*
  - *ROOT* -niminen sovellus näkyy tomcat-palvelimen juuressa
    - *http://tomcat.server:port/*
  - *<sovelluksen_nimi>/WEB_INF/web.xml*
    - *Sovelluskohtainen konfiguraatiotiedosto*
  - *<sovelluksen_nimi>/WEB_INF/classes*
    - Sovelluksen java-luokat
  - *<sovelluksen_nimi>/WEB_INF/lib*
    - Sovelluksen jar-kirjastopaketit



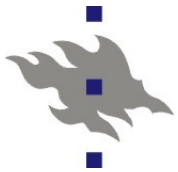
Tomcat

- Tomcat on Java EE -sovelluspalvelimen referenssitoteutus
  - *http://tomcat.apache.org/*
  - Toteuttaa sovelluspalvelimen, servlet- ja jsp-speksin
  - Tomcat löytyy distribuutioiden vakiokokoonpanosta
  - Versio 6 toteuttaa servlet speksin version 2.5 ja JSP-speksin version 2.1
  - Pohjalla Sunin omassa J2EE-referenssitoteutuksessa
  - Sovellusten dynaaminen asentaminen ja päivittäminen
  - Sovellukset näkyvät oletusarvoisesti tomcatin sisäänrakennusta http-palvelimesta
    - AJP-protokollalla tai reverse-proxylla sovellukset saa liitettyä osaksi apachen URL-avaruutta
  - *server.xml* – tomcat-palvelimen konfiguraatiotiedosto
    - Palvelimen lokit, sovellusten sijainti
    - Kuunteltavat portit: http-palvelin, mod_jk-palvelin ja portti tomcat:in alasajoa varten (salasanalla)



Fedora tomcat

- Toimii nykyään virallisella Sun JDK:lla
  - Oma tomcat-käyttäjätunnus
  - Konfiguraatio */etc/tomcat5* hakemistossa
  - Sovellukset */var/lib/tomcat5/webapps* hakemistossa
  - Tomcat connector:
    - Palikka, jolla sovelluksen saa näkymään Tomcatista ulos
    - Tavallinen http-palvelin, mod_jk-palvelin, SSL-tuki
  - Oletuskonfiguraatiossa kuuntelee http-connector portissa 8080 ja ajp-connector portissa 8009
  - *server.xml* - tomcat-daemonin konfiguraatiotiedosto
    - Portit, joita tomcat kuuntelee
    - *web.xml* – globaali konfiguraatiotiedosto kaikille J2EE-sovelluksille
    - Formaatti löytyy J2EE-speksistä



Tomcat 6 Ubuntussa

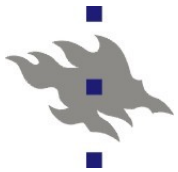
- Asennetaan ubuntu-paketit:
  - *tomcat6* – tomcat engine
  - *tomcat6-examples* – esimerkkisovellukset
  - *tomcat6-user* – skripti käyttäjäkohtaisen tomcat-enginehakemiston alustamiseen
    - Kuten TKTL:n *wanna-tomcat*
- */var/lib/tomcat6/webapps* – tomcat6 sovellukset
- */etc/tomcat6* - konfiguraatiotiedostot
- */var/log/tomcat6* – lokitiedostot

mod_jk

- Apache moduli, jolla tomcat-sovelluspalvelimen voi liittää osaksi apachen URL-avaruutta
  - Välittää ajp13-protokollalla Apachelle tulleet pyynnöt java-sovelluspalvelimelle
  - Ajp13 on TCP-protokolla: sovelluspalvelimen ei välttämättä tarvitse sijaita samalla fyysisellä palvelimella
  - Voi käyttää kuorman jakamiseen usealle fyysisellä tomcat-palvelimelle
  - Tukee autentikointia jaetulla salaisuudella
  - Vastaavan toiminnallisuuden voi toteuttaa *mod_proxy*:llä
  - Mahdollistaa staattisten tiedostojen palvelun suoraan sovelluspalvelimen hakemistoista
- Konfigurointi
  - *JkMount <URL> <työläinen>*
  - *workers.properties* -tiedosto, jolla sidotaan Apache:n URL-avaruuteen liitetyt työläiset tomcat-sovelluspalvelimen instansseihin

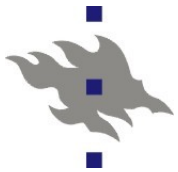
Linux ja SQL relaatiotietokannat

- Taustalla pyöriviä palveluita
  - Erotettu oman käyttäjätunnuksen taakse
  - Distribuution paketoinnin mukana tavallisesti valmis konfiguraatio
  - Pakettien asennuksen tai ensimmäisen käynnistyksen yhteydessä alustetaan tyhjä tietokanta
  - Asiakasohjelmistot kommunikoivat joko IP- tai unix-pistokkeiden kanssa
    - Sunin JRE ei tunne unix-pistokkeita: Java-asiakkaita varten on tarjottava TCP/IP-tietokantayhteydet
  - Varmistuskopiot hoidettava erikseen: ajossa olevan tietokannan tiedostojen suoralla kopioinnilla todennäköisesti saa vain korruptoituneita varmistuskopioita
  - Autentikointi tavallisesti erillisillä tietokannan sisäisillä käyttäjätunnuksilla tai unix-pistokkeilla
- OS tietokannat: MySQL ja Postgres
- Kaupallisia: Oracle ja DB2



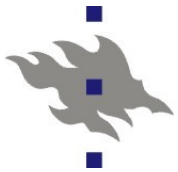
Tietokantojen käsitteitä

- 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



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
  - Vasta asennetun tietokannan oletusasetuksissa paikallisiin tietokantoihin ei ole salasanoja
    - Tosin käytetään Unix-kikkoja varmistamaan, että vain tietyt käyttäjät pääsevät käsiksi kantoihin



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
  - Versio 8.2 julkaistu 5.12.2006
  - Versio 8.2.3 julkaistu 7.2.2007
  - Versio 8.3.7 julkaistu 17.3.2009
  - Versio 8.4 julkaistu 1.7.2009
- Erinomaisesti dokumentoitu
  - Linux-kurssille relevantti luku III. Server Administration
    - http://www.postgresql.org/docs/8.4/static/admin.html

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.

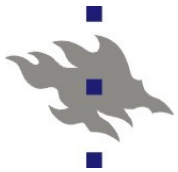
```
local      database  user  auth-method  [auth-option]
host       database  user  CIDR-address  auth-method  [auth-option]
hostssl    database  user  CIDR-address  auth-method  [auth-option]
hostnossl  database  user  CIDR-address  auth-method  [auth-option]
host       database  user  IP-address 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

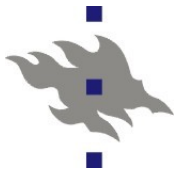


PostgreSQL Ubuntu

- 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
    - Nykyäänkin SQL-koodaajan täytyy pitää huolta käytetystä taulutyypistä: transaktiotuki on vain
- Sun osti MySQL AB:n
  - Lisää enterprise uskottavuutta
- Taulutyypit:
  - MyISAM: vanha perinteinen taulutyyppi ja edelleen oletus
    - Lukitukset, mutta ei transaktioita
  - InnoDB: Tukee transaktioita, mutta voi olla hitaampi
  - MERGE: useamman MyISAM taulun yhdistäminen yhdeksi

MySQL: asennus ja käyttö

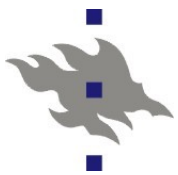
- Asennus:
  - *yum install mysql mysql-server php-mysql*
  - /etc/rc.d/init.d/mysql start
    - *mysql_install_db* – tietokantaklusterin alustus
    - Käynnistysskriptit alustavat tietokantaklusterin ensimmäisellä käynnistyskerralla
  - Root salasanan asetus tässä vaiheessa:

```
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

Linux ja mikroverkot

- Tarvitaan protokolla ja ohjelmisto käyttäjätunnusten jakamiseen mikroverkon työasemille
- Vaatimuksia
  - Tietoturva – kryptaus ja identiteetin varmistus
  - Luotettavuus: koko mikroverkko lakkaa toimimasta, jos tunnusten jako ei toimi
    - Replikointi:Yhden palvelimen kaatuminen ei riko koko verkkoa
    - Välimuistit: Yksittäinen työasema toimii, vaikka verkko olisi hetken poissa pelistä
  - Käyttäjätason rajapinta
    - Käyttäjien on voitava vaihtaa ainakin salasanansa
  - Työasemakohtaiset käyttäjätunnukset
- Linux toteutuksen apuvälineet:
  - glibc:n nss (Name Service Switch) pluginit
  - PAM (Pluggable Authentication Modules) autentikointipluginit

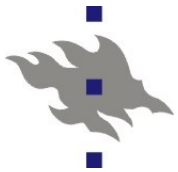


NSS: Name Service Switch

- Glibc-kirjaston sisäinen plugin-rajapinta käyttäjätunnustiedon listaamiseen
  - C-kirjaston funktiot käyttävät NSS-rajapintaa: getpwnam(), getpwuid(), getgrnam(), getgruid()
- Konfiguraatiotiedosto /etc/nsswitch.conf
- Plugin-kirjastot, jotka toteuttavat toiminnallisuudet 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

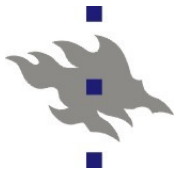
NIS – Network Information Service

- Perinteinen Sunin protokolla vuosien takaa
  - Ensimmäiset mikroverkkototeutukset 80-luvun loppupuolelta(?)
  - Käyttää Sunin RPC-mekanismia
    - NFS:stä tuttu
- Perinteinen NIS-protokolla ei ole kryptattu ja koneiden IP-osoitteisiin luotetaan
- NIS-protokollan uudemman ja fiksumman version, NIS+:n tuki Linuxissa huono
  - Open source NIS+ -palvelimen kehitystyö on lakannut
- NIS kannattaa unohtaa ellei satu jo omistamaan SUN-palvelimia



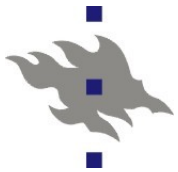
Viritykset

- Aikoinaan Linuxin ja/tai distribuutioiden tuki mikroverkkokonfiguraatioille on ollut huono
  - Nykyäänkin joutuu konfiguroimaan asioita käsin
- Monenlaisia tee-se-itse järjestelmiä on käytetty ja edelleen käytössä
  - Laitoksella on kotitekoinen järjestelmä
  - Serveri voi yksinkertaisesti kopioida ssh:lla säännöllisesti tarvittavat tiedostot (*/etc/passwd* ja */etc/shadow*)
  - Levyttömillä työasemilla yksinkertainen tiedostojen jako (NFS:n yli) voi olla riittävä ratkaisu
- MS:n AD voi toimia Linuxin käyttäjätunnustietokantana
  - Samba ja winbindd
  - Services for Unix



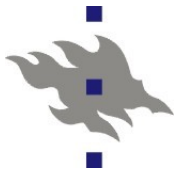
LDAP

- 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
- Linux-mikroverkon käyttäjätietokanta kannattaa nykyään toteuttaa LDAP-protokollan avulla
  - MS:n Active Directory on myös toteutettu LDAP-palveluna



LDAP-standardi

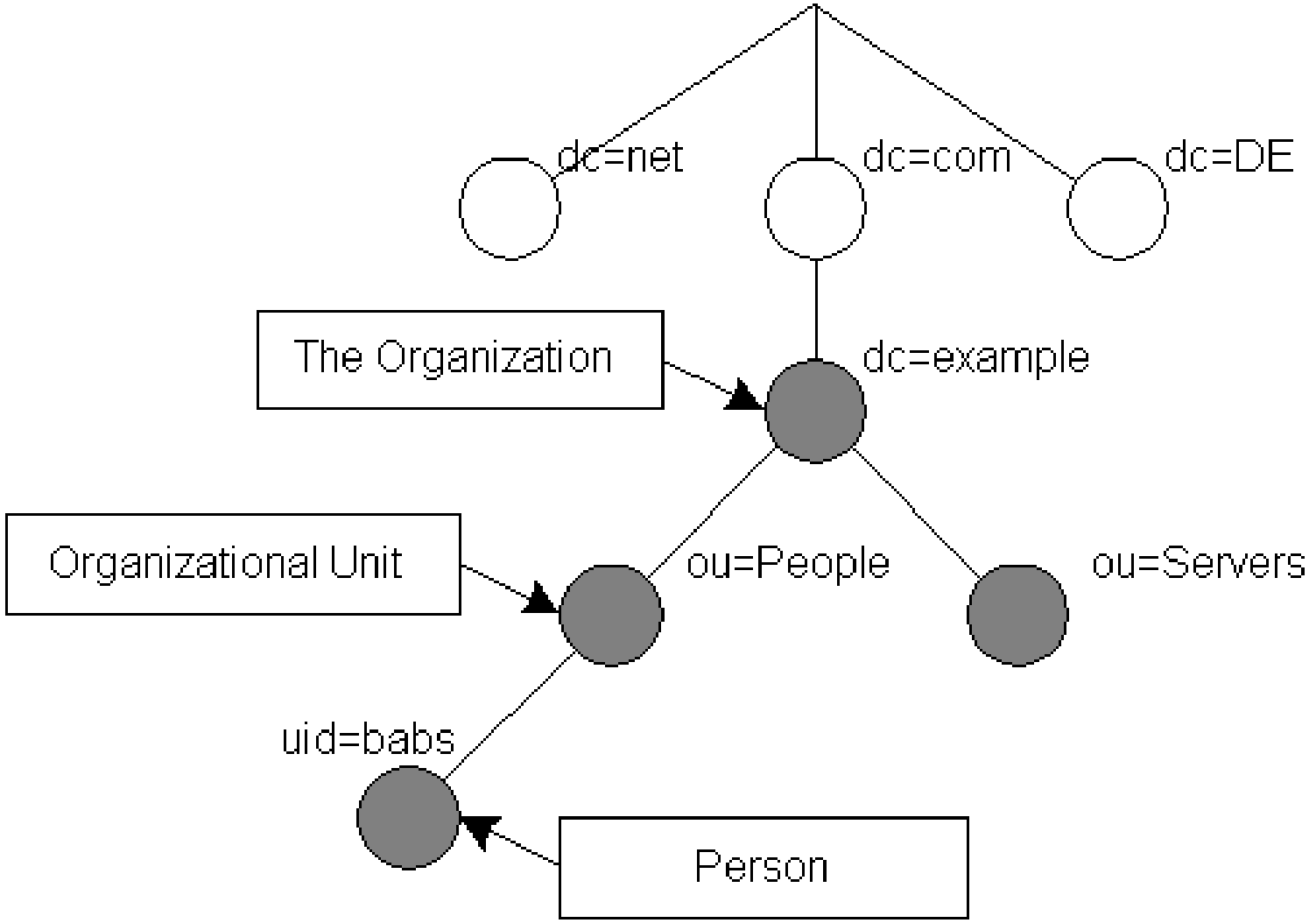
- Peräisin nyt jo kuolleesta OSI:n x.500-speksistä
  - LDAP oli vain kevyt rajapinta oikealle OSI:n DAP-hakemistopalvelulle, joka toimi täydellisen OSI-pinon päällä
  - Tyypilliseen OSI-speksin tapaan, DAP oli kovin raskas oikeasti toteutettavaksi ja käytettäväksi toteutettavaksi
  - LDAP ilmeisesti 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
  - Tiedon rakenne, tietueiden attribuutit, attribuuttien tyypit ja semantiikka
  - Unix-mikroverkoissa käytetään NIS-skeemaa
    - NIS:istä tutut tiedot on kuvattu LDAP-hakemistoksi ja hakemiston tietueiden attribuuteiksi (RFC 2307)
    - NIS services for Windows toteuttaa tämän AD-palvelimella
  - Muita skeemoja:
    - InetOrgPerson: skeema henkilötiedoilla (RFC 2798)
    - X.509 sertifikaattien talletus LDAP-hakemistoon (RFC 4523)

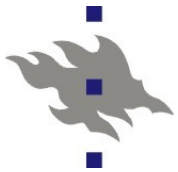
LDAP-hakemistohierarkia



LDAP-tietue

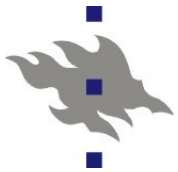
- LDIF – LDAP Data Interchange Format
  - LDAP -tietokantaan talletetun tiedon tekstimuotoinen esitys
  - Verrattavissa relaatiotietokannasta otettuun SQL-muodossa olevaan varmistuskopioon
  - RFC 2849
  - LDIF formaatilla voidaan esittää myös tietokantaa tehtäviä muutoksia: attribuuttien lisäykset,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



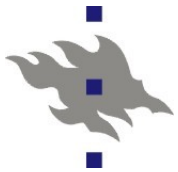
LDAP-autentikointi

- LDAP-palvelimella 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
- *slurpd* - replikointidaemoni

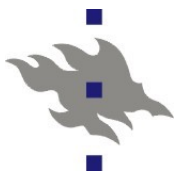
OpenLDAP asiakkaana

- *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
  -
- *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

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

Linux-tulostus

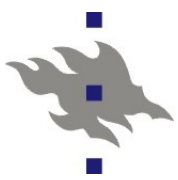
- Linuxissa ei ole mitään yhtenäistä yleisesti käytettyä ohjelmointi API:a tulostukseen
  - Joukko erilaisia postscriptiä generoivia kirjastoja kyllä löytyy, esim. gnome-print
- Tulostus tapahtuu generoimalla postscript-tiedostoja, jotka annetaan tulostusdaemonille printterille lähetettäväksi
  - Postscript on Adoben kehittämä tekstin ja grafiikan kuvauskieli, jota useat (kalliimmat) tulostimet ymmärtävät sellaisenaan
  - Tulostusdaemoni toteuttaa töiden jonotuksen ja lähetyksen eteenpäin vuorollaan printterille tai verkkopalvelimelle
- Linuxin tulostusajureita kutsutaan suotimiksi (filter)
  - Suotimet tulkkaavat sovellusten generoiman postscriptin (ja muitakin tiedostotyyppejä) printterin ymmärtämään muotoon
  - Usein *ghostscript* postscript-tulkin backend-ajureita
  - Hplip: HP Linux imaging and printing on HP:n itse toteuttama ajuri HP:n printtereille
  - Myös esikatselu tavallisesti toteutettu ghostscript-tulkilla

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

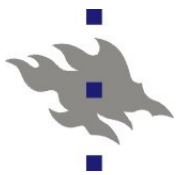
PPD-Tulostussuotimet

- 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



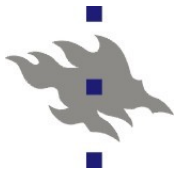
CUPS: Common Unix Printing System

- 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



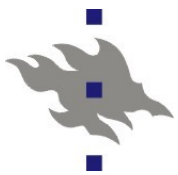
CUPS: arkkitehtuuri

- 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

NFS verkkotiedostojärjestelmä

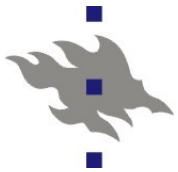
- Sunin Network File System-protokollasta on itse asiassa olemassa jo kolme eri versiota
  - NFSv2, RFC1095 vuodelta 1989
  - NFSv3, RFC1813 vuodelta 1995
  - NFSv4, RFC3530 vuodelta 2003
- Suunniteltu Unix-tyyppisiä käyttöjärjestelmiä varten
  - Tiedosto-oikeudet, hard- ja symlinkit, device-nodet, jne
- 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)
  - Speksi 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 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 välimuistissa siltä varalta että serveri kaatuu



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
- Kerberos 5 autentikointi, SPKM3
  - Mekanismi uusien autentikointiprotokollien lisäämiseen
  - MS AD:n kerberos-autentikointi toimii sellaisenaan
- 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

- Palvelut
  - Portmap – RPC-palveluiden kuvaus portteihin
  - rpc.mountd – etämounttauspalvelu
  - Varsinainen NFS-palvelu ja lukkopalvelu kerneliin sisäänrakennettu
  - rpc.statd - toipumispalvelu
  - rpc.rquotad - etäquota
- Tiedostot
  - */etc/exports*
    - paikalliset NFS-jaot
  - */var/lib/rmtab*
    - NFS-asiakkaiden mounttaukset
  - */var/lib/nfs/statd*
    - Toipumispalvelun rpc.statd lista palvelimista joi