Joni Pellikka

AVOIMEN LÄHDEKOODIN HAKEMISTOPALVELUT

Opinnäytetyö
Kajaanin ammattikorkeakoulu
Tradenomi
Tietojenkäsittelyn koulutusohjelma
Kevät 2012

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ
TIIVISTELMÄ

Koulutusala Luonnontieteiden koulutusala	Koulutusohjelma Tietojenkäsittelyn koulutusohjelma
Tekijä(t) Joni Pellikka	
Työn nimi Avoimen lähdekoodin hakemistopalvelut	
Vaihtoehtoiset ammattiopinnot Järjestelmän ylläpito	Ohjaaja(t) Tarja Karjalainen
	Toimeksiantaja Kajaanin ammattikorkeakoulu
Aika Kevät 2012	Sivumäärä ja liitteet 52

Tämän opinnäytetyön aiheena on tutustua pintapuolisesti avoimen lähdekoodin hakemistopalveluihin järjestelmän ylläpitäjän näkökulmasta. Mukaan on otettu kolme ehkä suosituinta avoimen lähdekoodin hakemistopalvelukokoonpanoa; Apache Directory Service, OpenLDAP ja OpenDS.

Hakemistopalvelut ja LDAP ovat kokonaisuudessaan todella laaja aihe, joten näihin palveluihin perehdytään tässä työssä pintapuolisesti käyden läpi tärkeimmät ominaisuudet, mitä järjestelmän ylläpitäjä mahdollisesti jokapäiväisessä työssä tulee tarvitsemaan. Työssä käydään läpi myös palveluiden asennusvaiheet.

Teoreettinen viitekehys työlle muodostuu opinnäytetyössä olevista eri hakemistopalveluista ja eri käyttöjärjestelmistä ja tietoverkoista yleisesti. Työssä tutkitaan hieman LDAP:n tekniikkaa yleisesti ottaen. Lähteet ja dokumentointi työlle on hyvin pitkälti ”kokeile ja epäonnistu” –teemalla, sillä avoimen lähdekoodin sovelluksille ei löydy virallista dokumentaatiota, vaan on turvauduttava paljon keskustelupalstojen lähteisiin.

Työn rajaus on suoritettu kotityökaluilla virtuaalisessa ympäristössä sekä Internetistä löytyvien ilmaisten avoimen lähdekoodin työkalujen avuilla. Työssä otetaan huomioon tärkeimpänä hakemistopalveluiden ominaisuudet nimenomaan järjestelmän ylläpitäjän näkökulmasta.

Asennukset ja konfiguroinnit onnistuivat ilman ylitsepääsemättömiä ongelmia. Tämän työn pohjalta tulee esiin mitä on mahdollisesti odotettavissa avoimen lähdekoodin hakemistopalvelun kanssa työskennellessä.

Kieli	Suomi
Asiasanat	LDAP, hakemistopalvelu, avoin lähdekoodi, Active Directory
Säilytyspaikka	☐ Verkkokirjasto Theseus ☐ Kajaanin ammattikorkeakoulun kirjasto

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

THESIS
ABSTRACT

School Business	Degree Programme Business Information Technology
Author(s) Joni Pellikka	
Title Open source directory services	
Optional Professional Studies System Administration	Instructor(s) Tarja Karjalainen
	Commissioned by Kajaani University of Applied Sciences
Date Spring 2012	Total Number of Pages and Appendices 52

The purpose of this thesis was to study open source directory services from the system administration point of view. The study includes three of the most popular open source directory services; Apache Directory Service, OpenLDAP and OpenDS.

Directory services and LDAP are really wide and extensive subjects as a whole so this thesis concentrates on the system administators' most important features of the services. The installing and configuring phases of the services are also included in the thesis.

The theoretical part consists of directory services, operating systems and the basics of information networks. The thesis also contains basic information on LDAP technology. Since open source software almost always lacks the official documentation, the sources and documents contain a lot of "fail and try again" –technique. Forums and fellow Linux-users had to be resorted to many times for help. The project itself was conducted with a home PC in virtual environment. All the software included is free open source software.

Installation and configuration of the open source directory services succeeded without insuperable problems. This thesis reveals the possibilities and potential obstacles when one considers using open source directory services.

Language of Thesis	Finnish
Keywords	LDAP, directory service, open source, Active Directory
Deposited at	☐ Electronic library Theseus ☐ Library of Kajaani University of Applied Sciences

SISÄLLYS

1 JOHDANTO 1

2 HAKEMISTOPALVELUT 1
2.1 LDAP 1
2.1.1 Alkuperä 1
2.1.2 Protokollan toiminta 2
2.1.3 Hakemistorakenne 2
2.1.4 URL:t 3
2.2 Active Directory 4
2.2.1 Rakenne 4
2.2.2 Toimialue 4
2.2.3 Organisaatioyksikkö 5
2.2.4 Sivustot 6
2.2.5 Teema 6
2.2.6 Global catalog 7
2.2.7 DNS-palvelu 7
2.3 Apache Directory Server 7
2.3.1 Apache Directory Studio 8
2.4 OpenDS 10
2.4.1 Alkuperä 10
2.5 OpenLDAP 11
2.5.1 Vaatimukset 11
2.5.2 Slapd 12

3 TOTEUTUS 13
3.1 Työympäristö 13
3.1.1 Linux-palvelimet 13
3.2 ApacheDS 14
3.2.1 Apache Directory Studio 15
3.2.2 Yhdistäminen toimialueen hakemistopalvelimeen 16
3.2.3 Haku LDAP-palvelimelta 18
3.2.4 Uuden kirjauksen luonti 19
3.2.5 Osiot 21

3.3 OpenDS 21
3.3.1 Asennus 21
3.3.2 Hallinta 24
3.3.3 Monitorointi 27
3.4 OpenLDAP 27
3.4.1 Berkleyn tietokanta 28
3.4.2 TLS 28
3.4.3 OpenLDAP:n asennus 29
3.4.4 Konfigurointi 29
3.4.5 Palvelun käynnistäminen ja sammuttaminen 30
3.4.6 Tietojen lisääminen tietokantaan 31
3.4.7 Autentikointi 32
3.5 Kerberos 33
3.5.1 Asennus 33
3.5.2 Konfigurointi 34
3.6 DNS 35
3.6.1 Asennus 35
3.6.2 Konfigurointi 35

4 POHDINTA JA JOHTOPÄÄTÖKSET 38
4.1 ApacheDS 38
4.2 OpenDS 39
4.3 OpenLDAP. 40
4.4 Lopputuomio 40

LÄHTEET 44

LIITTEET

SYMBOLILUETTELO

AD	Active Directory, Microsoftin hakemistopalvelu
ApacheDS	Apache Directory Server
CDDL	Common Development and Distribution License, Sunin avoimen lähdekoodin ohjelmiston lisenssi
CVS	Concurrent Versions System, paketinhallintaohjelmisto
DAP	Directory Access Protocol, tietoverkkoprotokolla
DB	Database, tietokanta
DC	Domain Controller, toimialueen isäntäkone
DN	Distinguished Name
DNS	Domain Name System
Domain tree	Toimialuepuu
DSA	Directory System Agent, hakemistopalvelun elementti
DSML	Directory Service Markup Language, hakemistopalvelun XML –pohjainen esitysmuoto
FQDN	Fully Qualified Domain Name, toimialueen täydellinen nimi
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
KDC	Key Distribution Center
ITU	International Telecommunication Union
LDAP	Lightweight Directory Access Protocol, hakemistopalveluprotokolla
LDIF	LDAP Data Interchange Format

MINA	Multipurpose Infrastructure for Network Applications
MMC	Microsoft Management Console
NAT	Network Address Translation
OSI	Open Systems Interconnection
OU	Organizational Unit
RDN	Relative Distinguished Name
Slapd	Standalone LDAP Daemon
SLP	Service Location Protocol
SPML	Service Provisioning Markup Language
SSL	Secure Sockets Layer, tietoverkkosalausprotokolla
TCP/IP	Transmission Control Protocol / Internet Protocol, tietoverkkoprotokolla
TLS	Transport Layer Security, salausprotokolla
URL	Uniform resource locator
X.500	Hakemistopalveluprotokolla
XED	XML Enabled Directory

1 JOHDANTO

Opinnäytetyöni tarkoituksena on tutkia avoimen lähdekoodin tarjoamia vaihtoehtoja Microsoftin Active Directory –hakemistopalvelulle, pääsäntöisesti järjestelmän ylläpitäjän näkökulmasta. Työtä tehdessä ja tarjontaa tutkiessa omasta mielestä kattavimmat ja lupaavimmat avoimen lähdekoodin hakemistopalvelut ovat ApacheDS, OpenDS ja OpenLDAP.

Avoin lähdekoodi tarkoittaa ohjelmiston tuottamis- ja kehitysmenetelmää, joka antaa käyttäjien tarkastella ja muokata ohjelman lähdekoodia. Avoimen lähdekoodin periaatteisiin kuuluu myös vapaus käyttää ohjelmaa mihin tahansa tarkoitukseen ja kopioida ja levittää sekä alkuperäistä, että muokattua versiota, ilmaiseksi. (Coss 2012.)

Alustava opinnäytetyöni aihe käsitteli menetelmiä, joilla saadaan eri käyttöjärjestelmät ja laitteet toimimaan Microsoftin Active Directoryssä, mutta aihe muotoutui jälkeen päin käsittelemään Active Directoryn korvaavia tuotteita. Suoraan vastaavanlaista opinnnäytetyötä en löytänyt vanhojen opinnäytetöiden arkistosta.

Päätavoitteeni tutkimuksessa on rakentaa mahdollisimman kattavasti Microsoftin Active Directoryä vastaava hakemistopalvelin avoimen lähdekoodin tarjoamilla palveluilla Linux-käyttöjärjestelmälle ja tarkastella palveluiden perusylläpitomenetelmät. Syvällisemmät perehtymiset konfigurointiin vaaditaan, mikäli johonkin näistä palvelinratkaisuista päätyy.

Mikäli avoimen lähdekoodin hakemistopalvelut eivät vastaa tarpeisiin tarpeeksi kattavasti, tutkin tarvittaessa myös lisäpalveluita niiden rinnalle. Tarkoitus on löytää mahdolliset hyödyt ja haitat avoimen lähdekoodin hakemistopalveluille.

2 HAKEMISTOPALVELUT

Tietoverkot ovat muotoutuneet aikojen saatossa peer-to-peer-verkoista hakemistopohjaisiin verkkoihin. Hakemistopohjaiset verkot ovat helpommin hallinnoitavissa ja täten ne ovat nykyään suosittuja. Hakemistopalveluiden ja tietoverkkojen hallintaa ja resurssien tarpeita vastaamaan IEEE (Institute of Electrical and Electronics Engineers) kehitti listan suosituksista ja standardeista nimeltään X.500. X.500 –protokollalle kehitettiin myöhemmin kevennetty versio LDAP (Lightweight Directory Access Protocol). (Price, J. A., Price B. & Fenstermacher S. 2008, 3.)

2.1 LDAP

LDAP on ohjelmistoprotokolla hakemistopalveluiden ja –tiedon siirtämiseen TCP/IP-verkossa. LDAP on määritelty IETF:n (Internet Engineering Task Force) toimesta. LDAP:lla on ollut suuri vaikutus myös muiden protokollien syntyyn, kuten myöhäisemmät X.500-versiot, XED (XML Enabled Directory), DSML (Directory Service Markup Language), SPML (Service Provisioning Markup Language) ja SLP (Service Location Protocol). (OpenLDAP 2012 d.)

2.1.1 Alkuperä

Tietoliikenneyrityksillä oli tieto hakemistopalveluiden vaatimuksista hallinnoimalla puhelinluetteloita useamman kymmenen vuoden ajan. Yritysten yhteistoimesta hakemistopalveluiden konsepti hioutui ja siitä muodostui X.500 -spesifikaatio; ITU:n (International Telecommunication Union) kehittämä ryhmä protokollia. (OpenLDAP 2012 d.)

X.500 hakemistopalvelua käytettiin X.500 DAP:n (Directory Access Protocol) toimesta, joka käytti toimintaan OSI-protokollaa (Open Systems Interconnection). LDAP suunniteltiin alunperin TCP/IP –protokollaa hyödyntäväksi kevyemmäksi versioksi X.500 –hakemistopalvelulle. (OpenLDAP 2012 d.)

Pian syntyivät erilliset LDAP-hakemistopalvelimet sekä myös palvelimet, jotka tukivat sekä DAP:ia, että LDAP:ia. LDAP:sta on tullut suositumpi yrityksissä, koska se ei vaadi OSI-verkkoa. Nykyään X.500-hakemistopalveluita voi myös käyttää TCP/IP-verkossa. (OpenLDAP 2012 d.)

2.1.2 Protokollan toiminta

Asiakasohjelma voi aloittaa LDAP-istunnon yhdistämällä LDAP-palvelimelle, jota kutsutaan DSA:ksi (Directory System Agent). Asiakasohjelma lähettää palvelimelle toimintapyynnön ja palvelin vastaa tähän. Erilaisia toimintapyyntöjä ovat esimerkiksi:

- StartTLS: suojattu yhteys käyttäen LDAPv3 TLS-laajennusta (Transport Layer Security)
- haku tietokannasta
- tietokannan tietojen vertailu
- uuden tiedon lisääminen
- olemassaolevan tiedon poistaminen/muokkaaminen. (OpenLDAP 2012 d.)

2.1.3 Hakemistorakenne

Protokolla käyttää LDAP-hakemistoja, jotka noudattavat X.500-mallia:

- Jokaisella kirjauksella on sarja ominaisuuksia.
- Jokaisella ominaisuudella on nimi (tyyppi tai kuvaus) ja yksi tai useampi arvo. Ominaisuudet määritellään skeemassa.
- Jokaisella kirjauksella on ainutlaatuinen tunnistus: DN (Distinguished Name), joka muodostuu RDN:stä (Relative Distinguished Name) ja isäntä-DN:stä. (OpenLDAP 2012 d.)

Kirjaus voi olla esimerkiksi seuraavanlainen:

dn: cn=Matti Maunio,dc=esimerkki,dc=fi

cn: Matti Maunio

givenName: Matti

sn: Maunio

telephoneNumber: +358 40 123 4567

mail: matti.maunio@esimerkki.fi

"dn" on kirjauksen tunnistus, "cn=Matti Maunio" on kirjauksen RDN ja "dc=esimerkki,dc=fi" on kirjauksen isäntä-DN. Muut lisäykset ovat kirjauksen ominaisuuksia. (OpenLDAP 2012 d.)

2.1.4 URL:t

LDAP:n URL-muoto on seuraavanlainen:

ldap://host:port/DN?attributes?scope?filter?extensions

- host: LDAP-palvelimen FQDN (Fully Qualified Domain Name) tai IP-osoite
- port: LDAP-palvelimen verkon portti (vakiona 389)
- DN: tunnistusnimike
- attributes: lista ominaisuuksista mitä haetaan
- scope: määrittelee haun laajuuden
- filter: hakusuodatin
- extensions: lisäykset. (OpenLDAP 2012 d.)

Useat näistä osista ovat vapaaehtoisia. Esimerkiksi *ldap://ldap.esimerkki.fi/cn=Matti%20Maunio,dc=esimerkki,dc=fi* antaa kaikki ominaisuudet Matti Maunion kirjauksesta ldap.esimerkki.fi:stä. (OpenLDAP 2012 d.)

2.2 Active Directory

Active Directory on Microsoftin versio X.500 –standardista. Se on periaatteessa tietokanta, joka on rakennettu hakemistomuotoon. AD on suunniteltu niin, että sen sisältöä on käyttäjien helppo käyttää ja järjestelmävalvojien helppo kontrolloida ja ylläpitää. (Price, J. A., Price B. & Fenstermacher S. 2008, 4.)

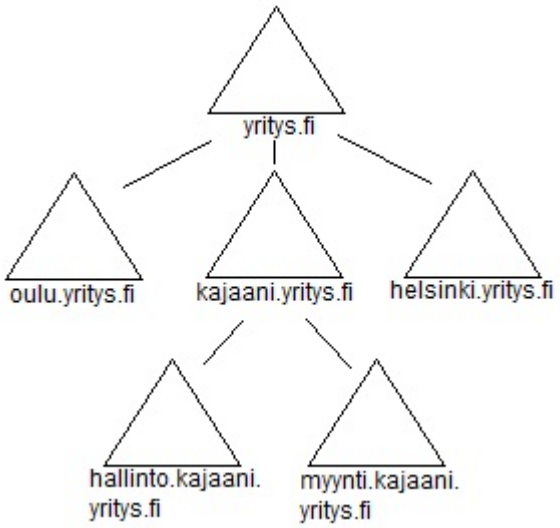
2.2.1 Rakenne

Active Directory jakautuu kahteen eri rakenteeseen, fyysiseen ja loogiseen. Fyysinen rakenne sisältää verkon konfiguroinnin, verkon laitteet ja verkon kaistanleveyden. Looginen rakenne pyrkii muokkaamaan Active Directoryn asetukset organisaation tarpeisiin, ottaen huomioon esimerkiksi työntekijöiden työtavat ja työkalut sekä työympäristön ylläpidon toimintatavat. (Clines S. & Loughry M. 2008, 12.)

2.2.2 Toimialue

Microsoftin käsitteen mukaan toimialue (domain) on alue, jonka sisällä olevat käyttäjät toimivat kaikki samojen turvallisuuskäytäntöjen ja sääntöjen mukaan. Toimialue sisältää ainakin yhden toimialueohjaimen (domain controller, DC), joka valtuuttaa käyttäjille pääsyn toimialueelle. (Clines S. & Loughry M. 2008, 12-13.)

Toimialueita pystytään yhdistämään keskenään luottosuhteilla. Tällaista monen toimialueen hierarkista rakennetta kutsutaan toimialuepuuksi (domain tree). Päätoimialue on puussa ylimmäisenä ja alatoimialueet jakautuvat siitä alaspäin (kuvio 1). Luottamussuhteet muodostuvat automaattisesti, kun uusia alatoimialueita lisätään toimialueeseen. Nämä suhteet ovat kaksisuuntaisia, joten käyttäjillä on pääsy kaikkiin saman puun toimialueisiin ja ne periytyvät eteenpäin. (Clines S. & Loughry M. 2008, 14.)



Kuvio 1. Toimialuepuu.

Usean toimialuepuun loogista ryhmää, jossa puut ovat liitetty toisiinsa perinnöllisillä oikeuksilla, kutsutaan metsäksi (forest). Saman metsän puilla pitää olla selkeästi toisistaan eroavat nimitykset, sekä puut käyttävät samaa teemaa (schema) ja yleistä luetteloa (global catalog). (Clines S. & Loughry M. 2008, 15.)

2.2.3 Organisaatioyksikkö

Organisaatioyksikkö (organizational unit, OU) on säiliö toimialueessa. Sinne säilötään toisiaan vastaavanlaisia objekteja, jotta ne olisivat helpommin hallittavissa. Esimerkkejä, mitä objekteja organisaatioyksikköihin voi säilöä:

- tulostimet
- jaetut tiedostot
- käyttäjät
- ryhmät
- ohjelmistot

Active Directoryn rakennetta suunniteltaessa tulisi jo ottaa huomioon jokaisen toimialueen omat organisaatioyksiköt. (Clines S. & Loughry M. 2008, 15-16.)

2.2.4 Sivustot

Sivusto on ryhmä IP-aliverkkoja linkitettynä nopeilla yhteyksillä. Aliverkot ovat osa verkon fyysistä topologiaa ja jokainen sivusto voi sisältää toimialueen hallintakoneita yhdestä tai useammasta toimialueesta. (Clines S. & Loughry M. 2008, 16.)

Sivustot määritellään jo Active Directoryn suunnitteluvaiheessa ja niiden tarkoitus on optimoida verkon replikoinnin ja autentikoinnin käyttämä kaistanleveys mahdollisimman vähäiseksi. Sivustoja voi myös käyttää verkon käyttäjien varmentamisen rajaamiseen: kun sivuston rajoitukset on määritelty, sivustoa lähin toimialueohjain autenktikoi käyttäjän. (Clines S. & Loughry M. 2008, 17.)

2.2.5 Teema

Active Directoryn teema on LDAP-rajapinnan fyysinen rakennemalli. Teema sisältää kaikkien objektiluokkien määritelmät ja ominaisuudet, joista luokkien sisältämät objektit muodostuvat. (Clines S. & Loughry M. 2008, 18.)

Rakennemalli on muokattavissa, mutta normaalisti siihen ei ole tarvetta. Mallin muokkaus tulee ajankohtaiseksi silloin, kun palvelimelle asennetaan ohjelmaa, joka käyttää Active Directoryä tiedon säilömiseen, esimerkiksi Microsoftin Exchange Server. (Clines S. & Loughry M. 2008, 18.)

Rakennemalliin täytyy kuulua ainakin seuraavat objektien määritelmät:

- nimi
- objektin tunnistaja (object identifier, OID)
- lista vaadituista ominaisuuksista
- lista vapaaehtoisista ominaisuuksista (Clines S. & Loughry M. 2008, 19.)

2.2.6 Global catalog

Yleinen luettelo (global gataloc, GC) on hakemisto, jonka ansiosta käyttäjä löytää verkon objekteja tietämättä missä toimialueessa nämä sijaitsevat. GC on tavallaan kopio Active Directorystä, mutta se ei sisällä kaikkia objektien ominaisuuksia vaan haun kannalta tärkeimmät, esimerkiksi etu- ja sukunimen. Toimialueessa toimii yksi tai useampi palvelin yleisten hakujen luettelona. Kun haku kohdistuu yleiseen luetteloon, tietoa etsitään metsälaajuisesti. (Clines S. & Loughry M. 2008, 21.)

2.2.7 DNS-palvelu

DNS (Domain Name Service, nimipalvelu) on Internetin käyttämä nimenselvennyspalvelu, joten Microsoft sisälsi tuen DNS -palvelulle myös Active Directoryyn. DNS kääntää palvelimien isäntänimet IP-osoitteiksi ja ohjaa näin dataliikenteen eri käyttäjien ja laitteiden välillä.

2.3 Apache Directory Server

Apache Directory Server (ApacheDS) on Apache Software Foundationin kehittämä avoimen lähdekoodin hakemistopalvelu. Se on kehitetty täysin Javalla ja se on hyväksytty LDAPv3 yhteensopivaksi Open Groupin toimesta. LDAP:n lisäksi se tukee Kerberos 5 ja Change Password –protokollia. (ApacheDS 2012 a.)

ApacheDS:n tärkeimpiin ominaisuuksiin kuuluvat muun muassa:

- Suunniteltu LDAP- ja X.500-alustaksi, mikä tekee ApacheDS:stä helposti ja monipuolisesti muokattavan hakemistopalvelimen.
- Palvelimen loppu- ja alkupään ohjelmistot ovat erotettu toisistaan täysin, joten hakemistojen, välityspalvelimien ja porttien luonti on helppoa.
- Palvelin käyttää verkkokoodinaan MINA:a (Multipurpose Infrastructure for Network Applications), joka parantaa suorituskykyä useampaa prosessia yhtäaikaa suorittaessa. (ApacheDS 2012 b.)

ApacheDS:n dokumentointi palvelun virallisilla Internetsivuilla on minimaalista, joten palvelun ominaisuudet, vaatimukset ja käyttö tulee vahvemmin esille asennus- ja käyttövaiheessa.

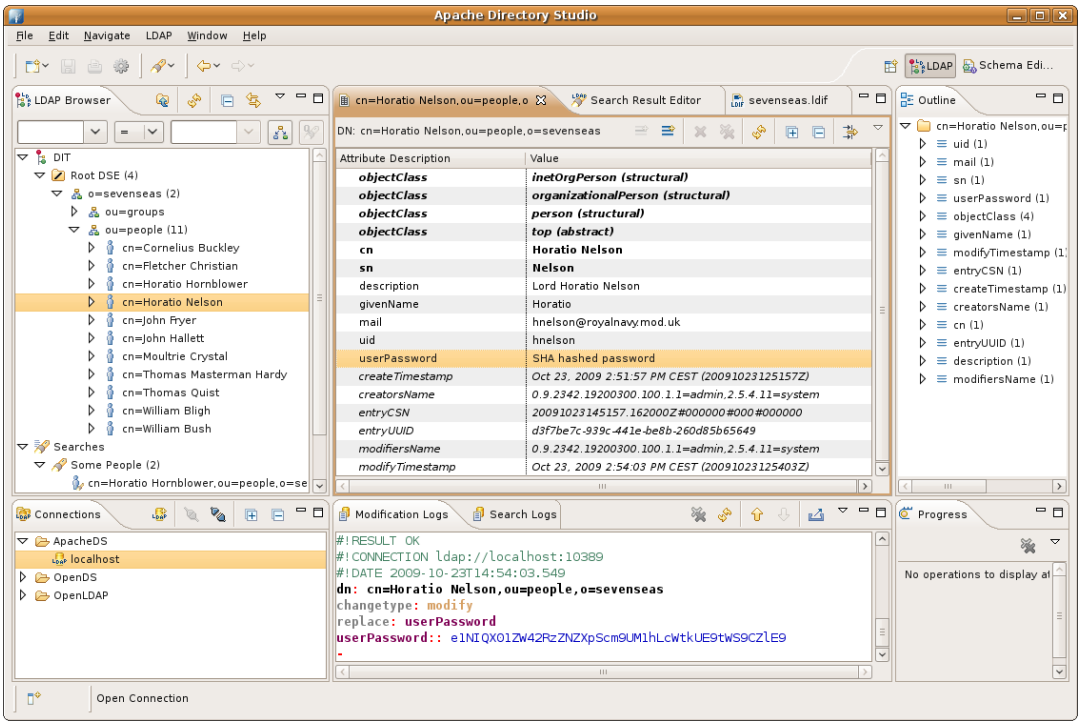
2.3.1 Apache Directory Studio

Apache Directory Studio on työkalu hakemistopalveluiden hallintaan ja ylläpitoon. Se on suunniteltu varta vasten ApacheDS:ä varten, mutta sitä voi käyttää minkä tahansa LDAP-palvelimen työkaluna.

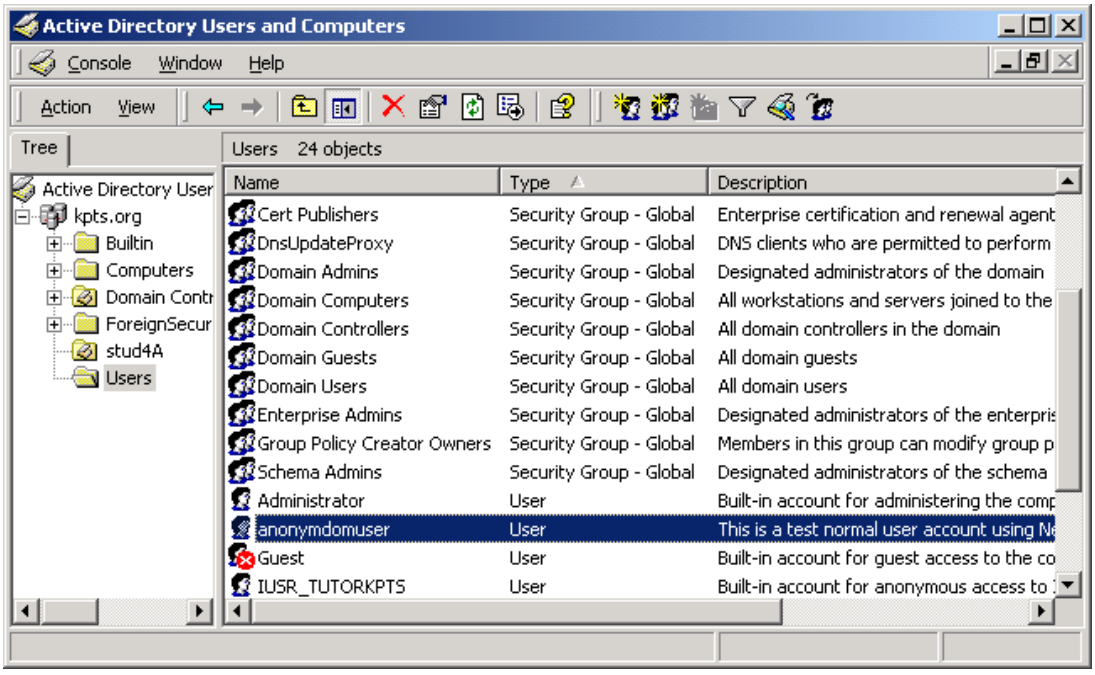
Apache Directory Studiolla voi muun muassa:

- selata LDAP-palvelimen rakennetta ja hakemistoja
- muokata LDIF-tiedostoja
- muokata teemoja
- ylläpitää ApacheDS:ä

Apache Directory Studion käyttöliittymä (kuvio 2) on hyvin samankaltainen, kuin Microsoftin Active Directoryn MMC-hallintatyökalu (kuvio 3). Tämän ansiosta varsinkin Active Directoryn kanssa paljon työskennelleet omaksuvat helposti Apache Directory Studion käytön.



Kuvio 2. Apache Directory Studio. (ApacheDS 2012 c.)



Kuvio 3. Active Directory MMC-hallintaohjelma. (Tenouk 2012.)

2.4 OpenDS

OpenDS on käyttäjien ja oman yhteisön kehittämä ilmainen ja kattava avoimen lähdekoodin hakemistopalvelu. OpenDS on suunniteltu kehittäjien mukaan vastaamaan suurienkin toimialueiden tarpeita luotettavalla toiminnalla ja on helposti asennettavissa ja hallittavissa. (OpenDS 2012 a.)

OpenDS:n parissa työskentelee tällä hetkellä muun muassa kokeneet Sunin insinöörit ja hakemistopalveluiden ammattilaiset. OpenDS:n koodi on lisensoitu CDDL:lle (Common Development and Distribution License) ja kaikilla on mahdollisuus olla kehityksessä mukana joko käyttäjänä tai kehittäjänä. (OpenDS 2012 a.)

OpenDS:n lähdekoodia hallinnoidaan Apache Subversionilla. Subversion on avoimen lähdekoodin versionhallintaohjelmisto. Projekti on perustettu CollabNet:n toimesta vuonna 2000 ja se on laajalti käytössä niin yksityisillä, kuin isommilla organisaatioilla. (Apache Subversion 2012 a.)

2.4.1 Alkuperä

OpenDS oli aluksi Sun Microsystems Inc.:n omistama sisäinen projekti joka käynnistyi alkuvuonna 2005. Projektin parissa työskenteli aluksi pieni ryhmä insinöörejä. Avoimeksi lähdekoodiksi projekti julkaistiin vuoden 2006 kesällä. (OpenDS 2012 b.)

Sen sijaan, että kehitys olisi kohdistettu jo olemassa oleviin avoimen lähdekoodin hakemistopalveluihin, Sun alkoi luomaan omaa variaatiota LDAP –pohjaisesta hakemistopalvelusta. Tämä antaa mahdollisuudet kehittää tuotteen rakenteen vastaamaan täysin omien asiakkaiden tarpeita sekä tarvittaessa tehdä myös merkittäviäkin muutoksia projektiin ja koodiin. Tämän lisäksi myös toisten projektien tavoitteet ja visiot saattavat poiketa halutuista, joten kompromisseihin ei ole tarvetta. (OpenDS 2012 b.)

2.5 OpenLDAP

OpenLDAP on yhteistyöllä suunniteltu ja kehitetty avoimen lähdekoodin LDAP-palvelu. Projektissa työskentelee maailmanlaajuinen vapaaehtoisyhteisö Internetin välityksellä. Kehitykseen mukaan pääsee melkeinpä kuka vain, jos innostusta ja osaamista löytyy. (OpenLDAP 2012 a.)

OpenLDAP-ohjelmistoon kuuluu:

- ”stand-alone” LDAP-palvelin (slapd), jossa integroituna replikointipalvelu
- Software Developer Kit (kehitystyökalu)
- työkalut palvelimen ajamiseen sekä valmiita asetuksia
- yhteisön tarjoamat lisäpaketit (OpenLDAP 2012 b.)

2.5.1 Vaatimukset

OpenLDAP-palvelu vaatii, riippuen siitä, mitä ominaisuuksia siitä haluat käyttää, toimiakseen muutamia kolmannen osapuolen ohjelmistoja. Näitä ovat muun muassa:

- Transport Layer Security (tulee useassa käyttöjärjestelmässä mukana)
- Simple Authentication and Security Layer (tulee useassa käyttöjärjestelmässä mukana)
- Kerberos Authentication Service
- Oraclen Berkley Database –tietokantaohjelmisto (OpenLDAP 2012 c.)

2.5.2 Slapd

Slapd on LDAP-hakemistopalvelu, joka toimii usealla alustalla. Siitä voi luoda oman hakemistopalvelun. Sen voi yhdistää toiseen LDAP-palveluun, tai sitä voi pyörittää itsekseen. (OpenLDAP 2012 d.)

Slapd sisältää muun muassa:

- LDAPv3:n
- Simple Authentication and Security Layer (tunnistukseen ja tietoturvaan)
- Transport Layer Security (tunnistukseen ja tietoturvaan)
- topologiaohjauksen
- tietokannan kulunvalvonnan
- usean kielen tuen
- usean tietokannan tuen
- omien moduulien tuen
- replikoinnin (OpenLDAP 2012 d.)

3 TOTEUTUS

Opinnäytetyön tavoitteena oli rakentaa Linux-käyttöjärjestelmälle Microsoftin Active Directoryä vastaava hakemistopalvelu käyttäen tarjolla olevia avoimen lähdekoodin palveluita. Tätä tavoitetta varten rakennettiin oma toimialue, jossa oli Microsoftin ja Linuxin palvelimia sekä työasemia.

3.1 Työympäristö

Päätin luodan opinnäytetyöni työympäristön virtuaalisena, koska tämä mahdollisti projektin toteuttamisen ilman muita fyysisiä rajoitteita, kuin oman tietokoneen resurssit. Tämän lisäksi olemme koulussa opiskelleet käyttöjärjestelmien käyttöä virtuaalisesti, joten sen takia ei pitäisi ongelmia ilmetä.

Virtuaalisen työympäristön tarjoaa VMWare Workstation 7.1.3 build-324285. Virtuaalisia koneita pystytän seuraavan verran:

- 3 Linux-palvelinta (jokaiselle palvelulle oma)
- 1 Linux työasemakone
- 1 Microsoft Windows työasemakone

3.1.1 Linux-palvelimet

Linuxin distribuutiona päätin käyttää Ubuntua ja sen versiota 11.10. Palvelimia asennetaan jokaiselle avoimen lähdekoodin hakemistopalvelulle yksi kappale ja tarvittaessa (esim. replikointia varten) lisää.

Tarkoitus on aluksi asentaa jokaiselle Linuxille eri hakemistopalvelin ja tehdä kaikki konfiguroinnit niille valmiiksi, jonka jälkeen yhdistän tarvittaman määrän Linux-palvelimia samalle toimialueelle ja määrään ne toimialueen domain controlleriksi. Tällä saan testattua tiedon kopioimista domain controllerilta toiselle eri hakemistopalvelimissa.

Virtuaalisille Linux-palvelimelle annoin seuraavanlaiset ominaisuudet:

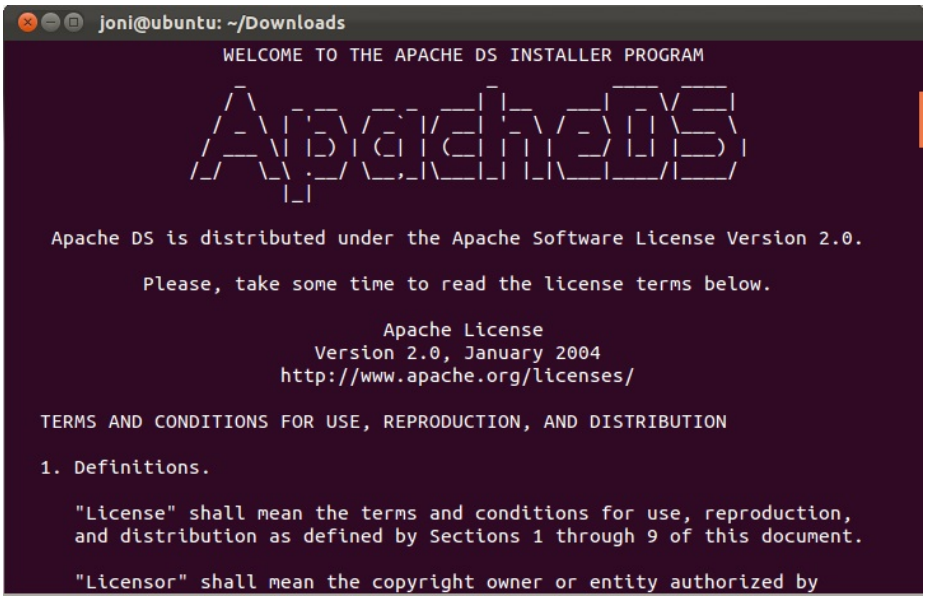
- jakeluna Ubuntu 11.10
- keskusmuistia 1024 MB
- verkkosovitin aluksi NAT:na, jotta virtuaalikoneella on helppo pääsy internettiin
- kiintolevytilaa 15 GB.

Käyttöjärjestelmien asennettua ne päivitetään ja varmistetaan, että niistä löytyy perustyökalut ja ohjelmat, joita hakemistopalveluiden ylläpitoon tarvitaan, kuten:

- Java (ei ole pakollinen kaikille palvelimille).
- LDAPUtils (sisältää skriptejä, joilla luodaan ja hallitaan käyttäjätunnuksia LDAP-hakemistopalveluissa).

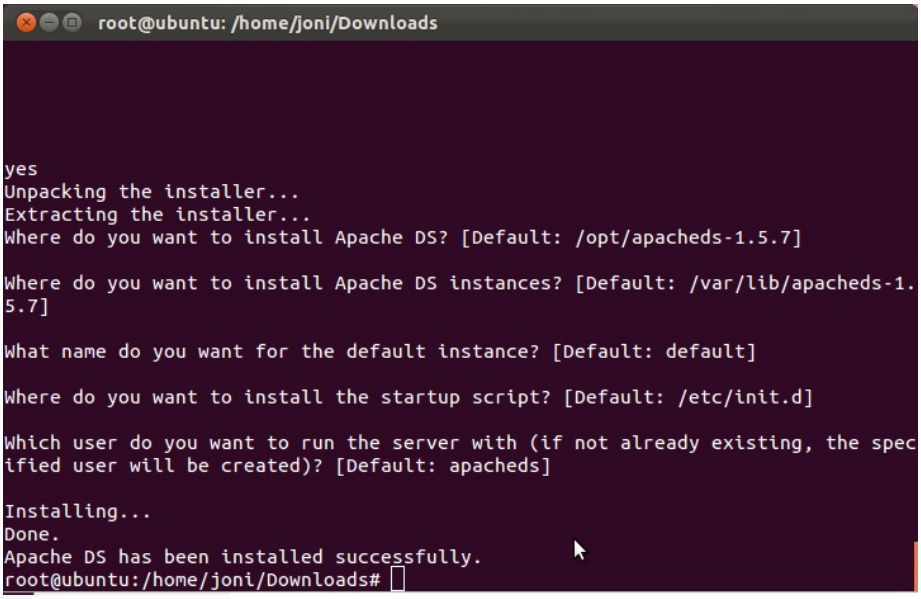
3.2 ApacheDS

ApacheDS hakemistopalvelun asennus hoituu Ubuntu 11.10:lle helposti. Asennuspaketti ladataan Apachen sivuilta ja asennusohjelma (kuvio 4) hoitaa palvelun asennuksen.



Kuvio 4. ApacheDS:n asennusohjelma.

Asennusohjelma kysyy asennusvaiheessa hakemistopalvelun perustiedot, jotka tulevat esille kuviossa 5.



Kuvio 5. ApacheDS:n asennus.

Hakemistopalvelu käynnistetään komennolla:

root@ubuntu:/etc/init.d# ./apacheds-1.5.7-default start

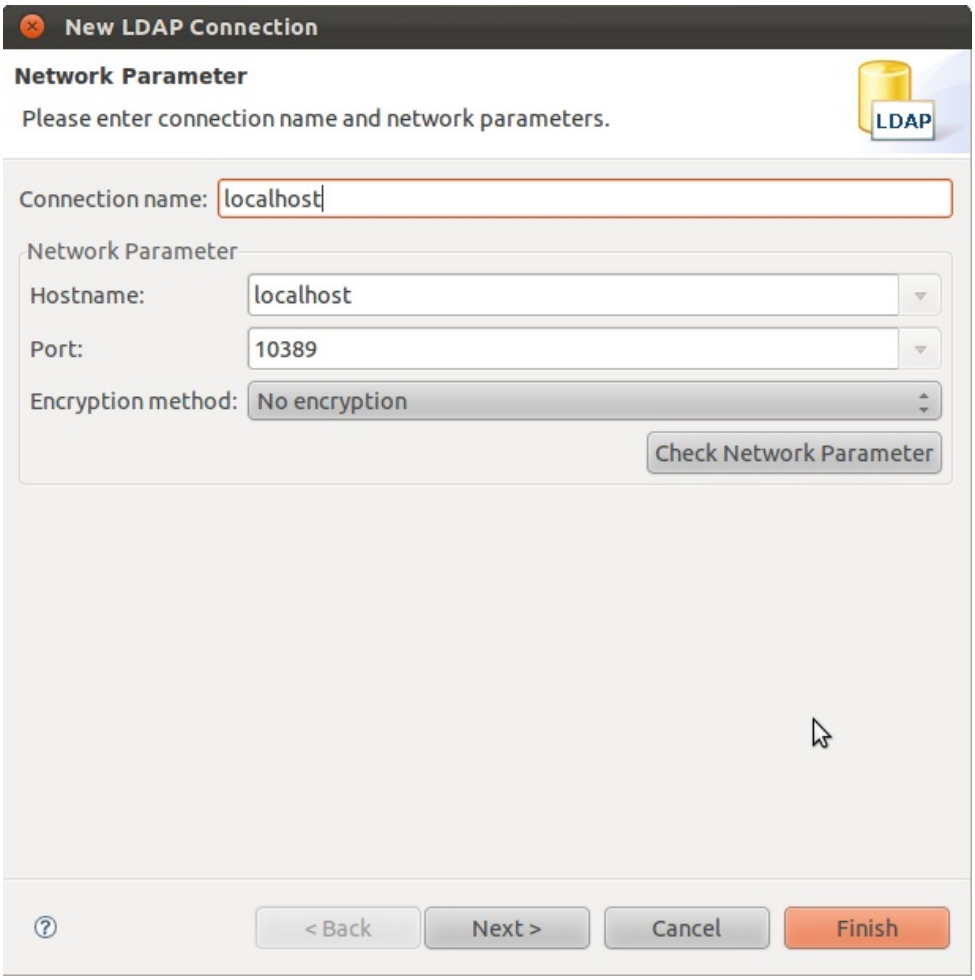
Käytin ApacheDS:n hallintaan Apache Directory Studiota, koska se on suunniteltu nimen omaan ApacheDS:ä varten ja siinä on tuttu käyttöliittymä Microsoftin Active Directoryn käytön kokemuksilla.

3.2.1 Apache Directory Studio

Apache Directory Studiolla on helppo hallita omaa hakemistopalvelinta, varsinkin, jos on pohjalla kokemusta Windows Active Directorystä. Apache Directory Studiolla onnistuu hakemistopalvelun perustoiminnat helposti kattavan käyttöliittymän ansiosta.

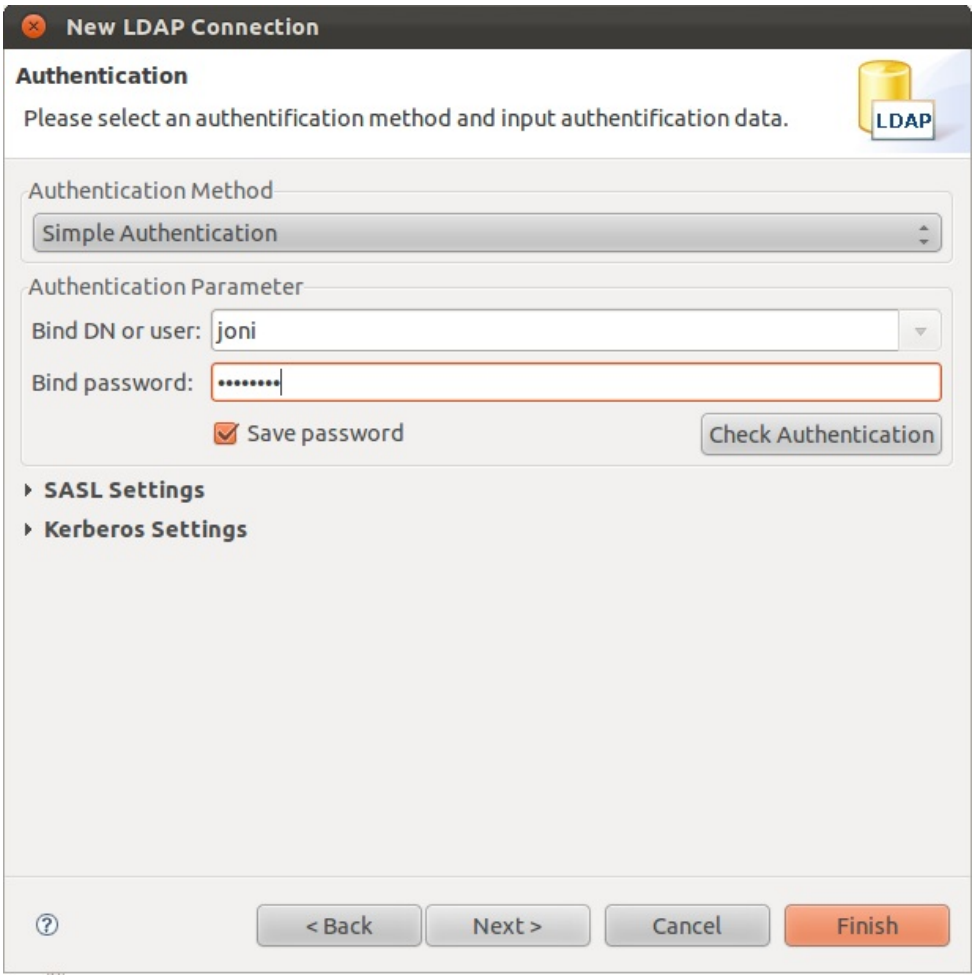
3.2.2 Yhdistäminen toimialueen hakemistopalvelimeen

Yhdistäminen palvelimeen muokkaamaan hakemistopalvelun tietoja onnistuu helposti omalla työkalulla (kuvio 6). ApacheDS käyttää oletuksena hakemistopalveluissa porttia 10389. (OpenDS käyttää porttia 1389 ja OpenLDAP porttia 389).



Kuvio 6. Uuden yhteyden luominen Apache Directory Studiolla.

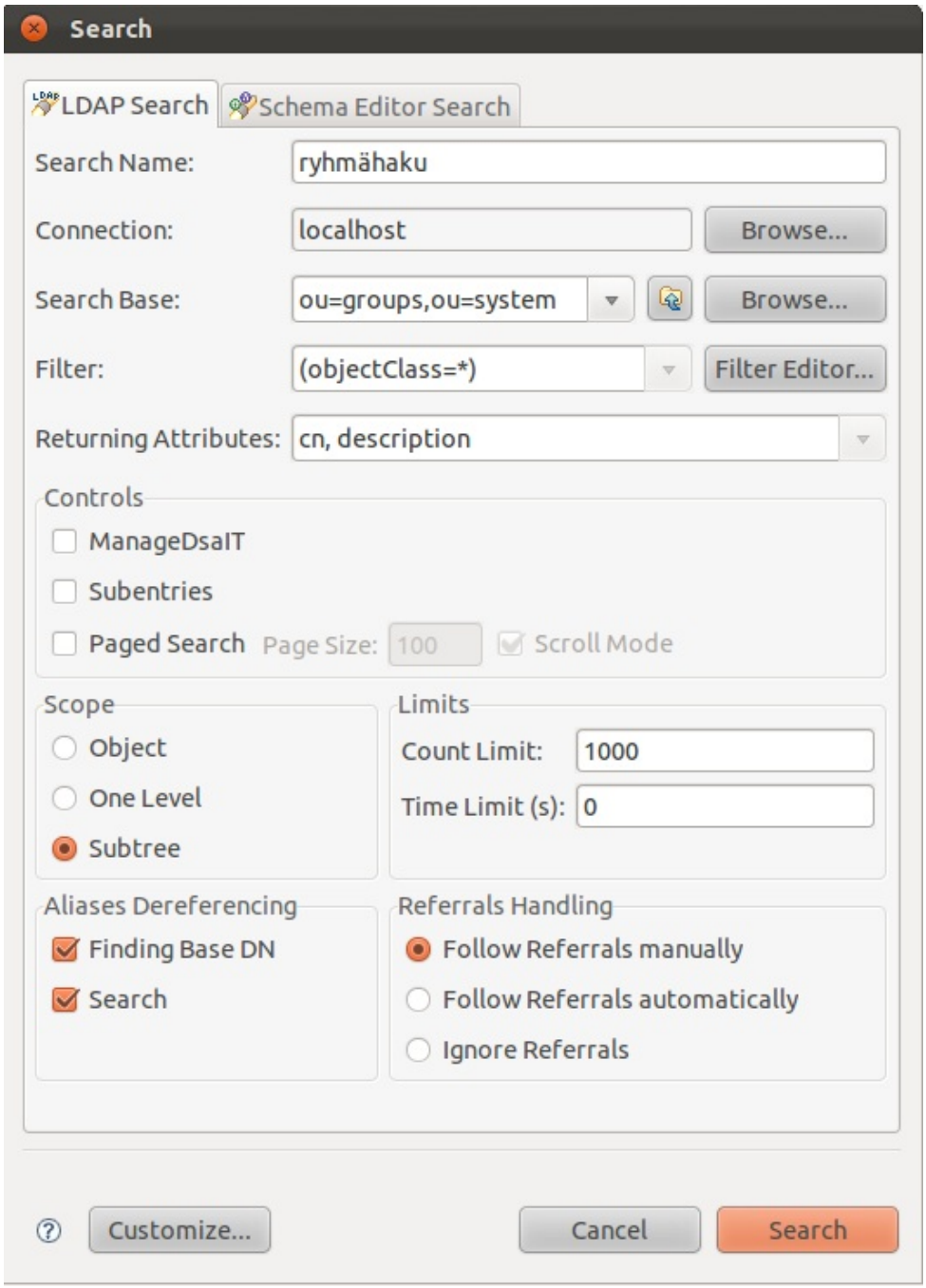
Tämän jälkeen määritetään käyttäjätunnus ja autentikointitapa, jolla palvelimelle halutaan kirjautua, sekä halutessaan muokataan autentikoinnin salausasetuksia (kuvio 7).



Kuvio 7. Uuden LDAP-yhteyden luominen Apache Directory Studiolla.

3.2.3 Haku LDAP-palvelimelta

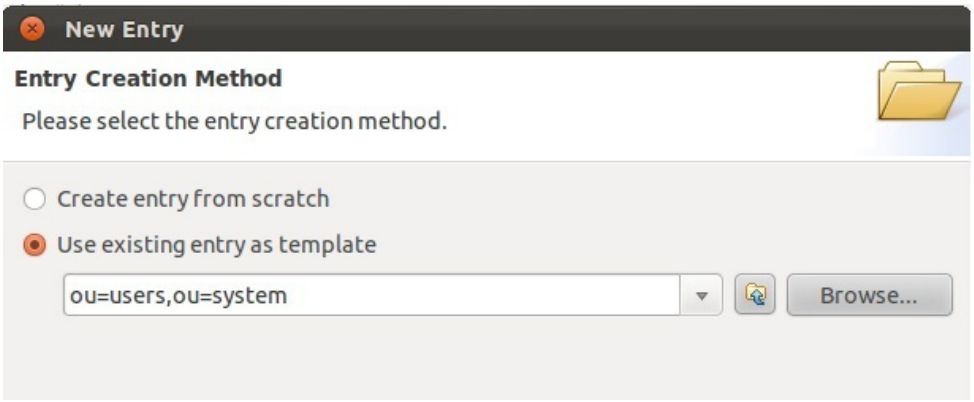
Apache Directory Studiolla on oma hakutyökalu, joka on kuvattuna kuviossa 8. Tämä esimerkkihaku hakee palvelimelta ryhmiä ja hakee niiden vastaavat cn ja description arvot.



Kuvio 8. LDAP-haku Apache Directory Studiolla.

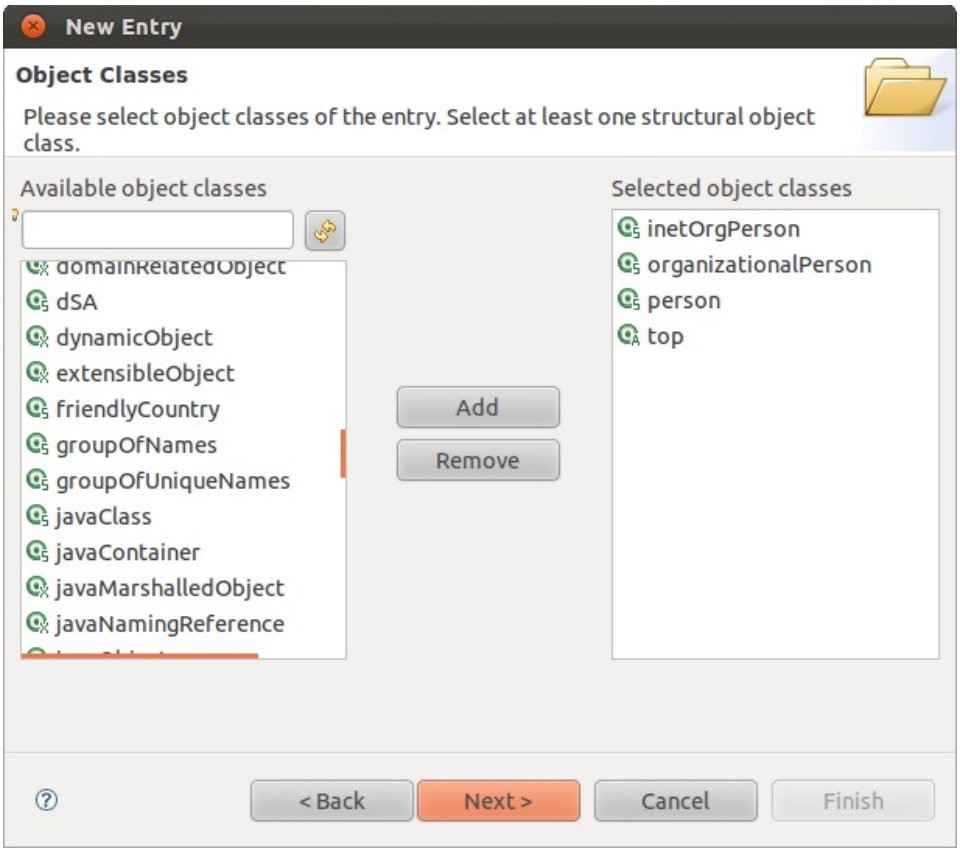
3.2.4 Uuden kirjauksen luonti

Uuden kirjauksen voi luoda kokonaan puhtaalta pöydältä tai sen pohjan voi kopioida toisesta kirjauksesta:



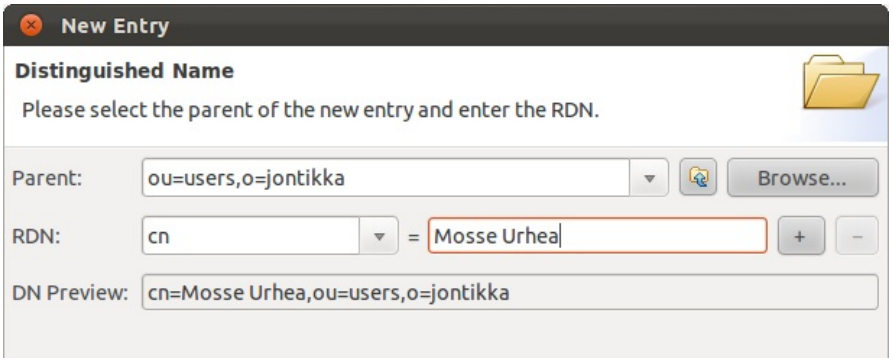
Kuvio 9. Uuden kirjauksen luontivaihe Apache Directory Studiossa.

Tämän jälkeen työkalu pyytää valitsemaan vasemmalta halutut luokat uudelle kirjaukselle, kuten kuviosta 10 näkyy.



Kuvio 10. Uuden kirjauksen luontivaihe Apache Directory Studiossa.

Lopuksi määritellään kirjauksen lopullinen DN ja kirjaus on valmis (kuvio 11).



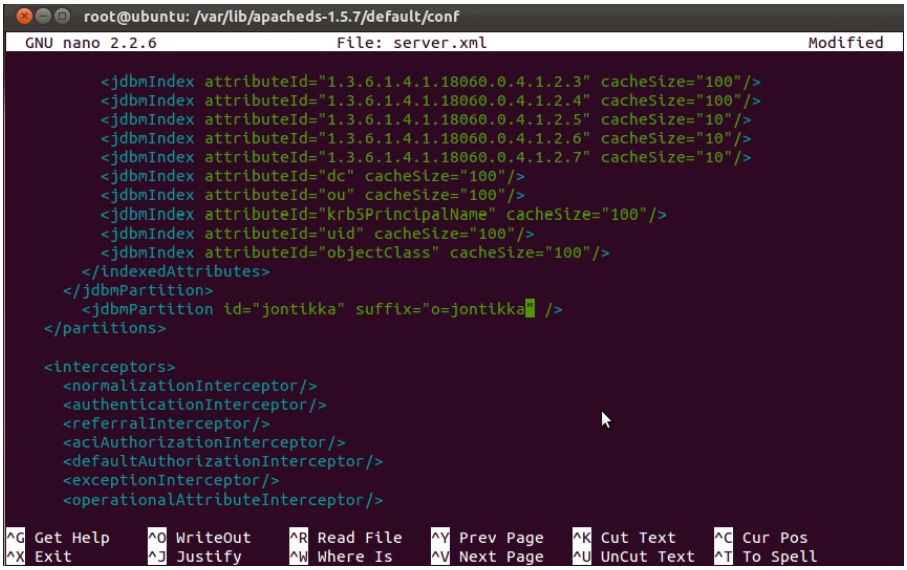
Kuvio 11. Uuden kirjauksen luontivaihe Apache Directory Studiossa.

Kirjauksia voi tämän jälkeen muokata helposti selaamalla niitä Apache Directory Studiossa ja valitsemalla hiiren toisella painikkeella ”Edit entry” –valinnan.

3.2.5 Osiot

ApacheDS:ssä kirjaukset ovat tallennettuina omina osioina. Jokainen osio on oma puu (DIT). Osioita voi olla useampia ja ne eivät ole välttämättä kytköksissä toisiinsa.

Kuviosta 12 nähdään kuinka osion lisääminen onnistuu helpoiten *server.xml* -tiedostoa muokkaamalla ja lisäämällä sinne esimerkiksi kirjauksen ”o=jontikka”:

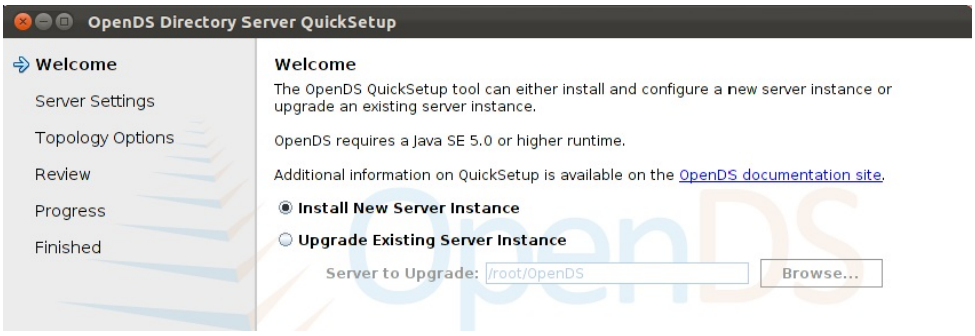


Kuvio 12. Osa ApacheDS:n *server.xml* –tiedostoa.

3.3 OpenDS

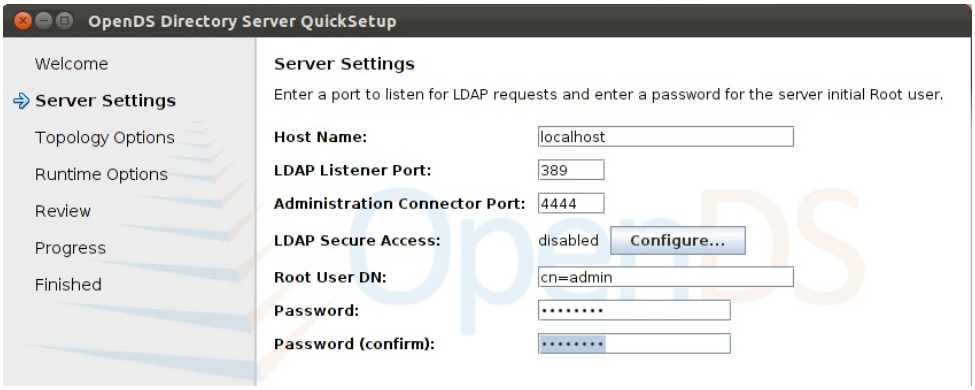
3.3.1 Asennus

OpenDS:n asennus oli helppo operaatio. Hakemistopalvelu löytyy java.net:n sivuilta *.zip*-pakettina, joka ladataan palvelimelle ja puretaan haluttuun kansioon. Tämän jälkeen hakemistopalvelu asennetaan yksinkertaisesti komennolla *setup*, jolloin asennusvelho käynnistyy ja pyytää perustiedot. Asennusvelholla voi halutessaan päivittää jo olemassaolevaa hakemistopalvelinta tai luoda kokonaan uuden, kuten kuviosta 13 voi huomata.



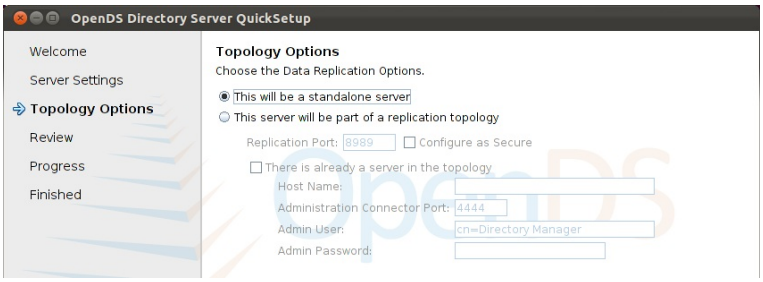
Kuvio 13. OpenDS:n asennusvaihe.

Tämän jälkeen syötetään kuviossa 14 esiintyvät hakemistopalvelimen perustiedot: isäntänimi, LDAP-portti, ylläpitoportti, ylläpitotunnus ja –salasana. Tässä vaiheessa voi myös ottaa käyttöön SSL- ja StartTLS-suojaukset ja muokata niiden ominaisuudet.



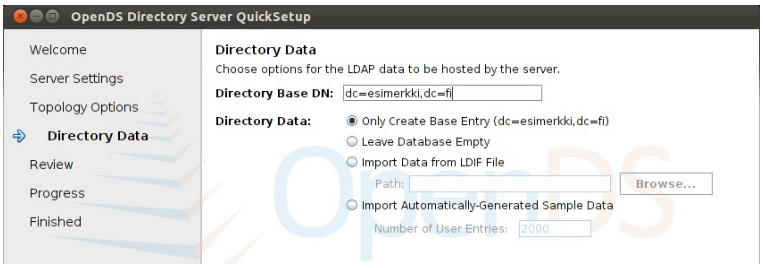
Kuvio 14. OpenDS:n asennusvaihe.

Seuraavana voidaan yhdistää asennettava palvelin replikoitavaksi toisten palvelimien kanssa. Porttinumeroon pitää kiinnittää huomio, sillä mikäli samalle isäntäkoneelle asennetaan useampi hakemistopalvelin ja ne halutaan replikoivan keskenään, pitää jokaiselle määritellä eri portti. Mikäli asennettava palvelin halutaan replikoivaksi toisen palvelimen kanssa, syötetään kyseisen palvelimen tiedot kuvion 15 mukaisesti.



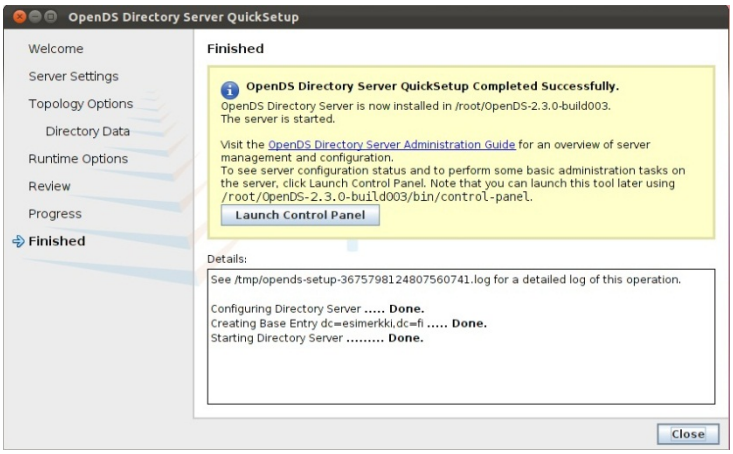
Kuvio 15. OpenDS:n asennusvaihe.

Kuvio 16 esittää, miten seuraavana luodaan hakemistopalvelun DN. Asennukseen voi tuoda myös ulkopuolisen LDIF-tiedoston (LDAP Data Interchange Format), josta voi hakea LDAP-palvelimelle valmiiksi annetut kirjaukset.



Kuvio 16. OpenDS:n asennusvaihe.

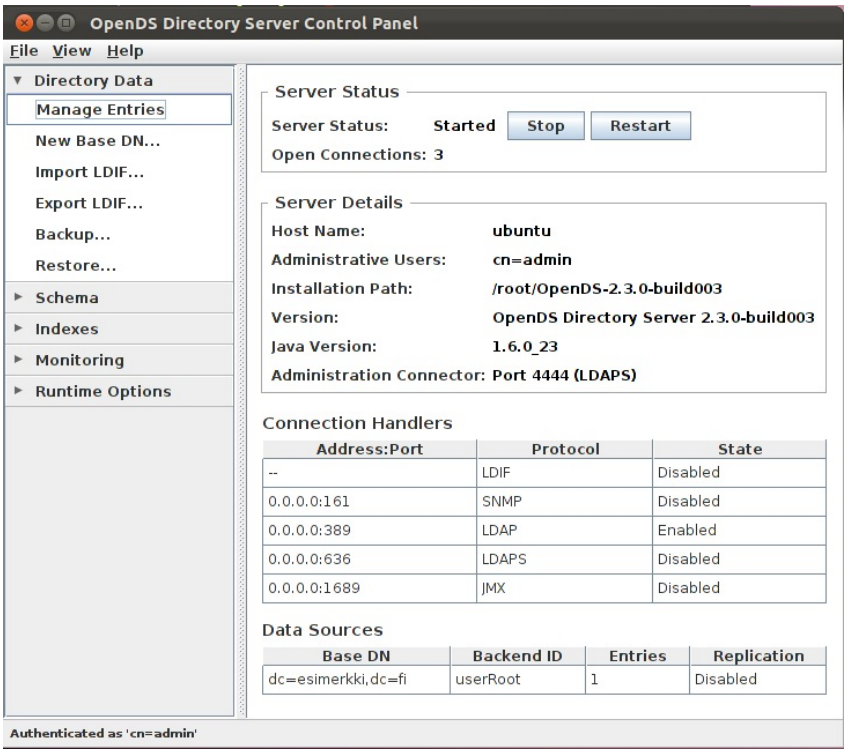
Asennus suorittaa tämän jälkeen tarvittavat toimenpiteet ja hakemistopalvelu on asennettuna palvelimelle (kuvio 17).



Kuvio 17. Valmis OpenDS:n asennus.

3.3.2 Hallinta

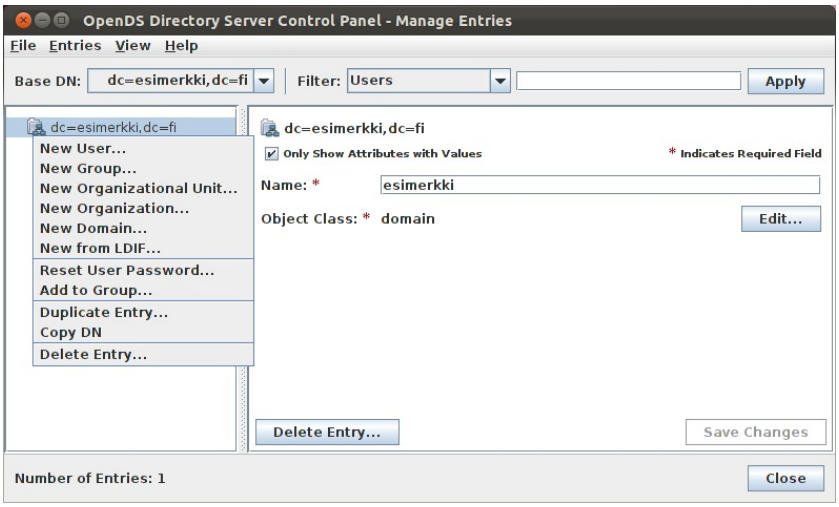
OpenDS:n hallintaan on hallintatyökalu, joka on hyvin kattava ja helppokäyttöinen (kuvio 18).



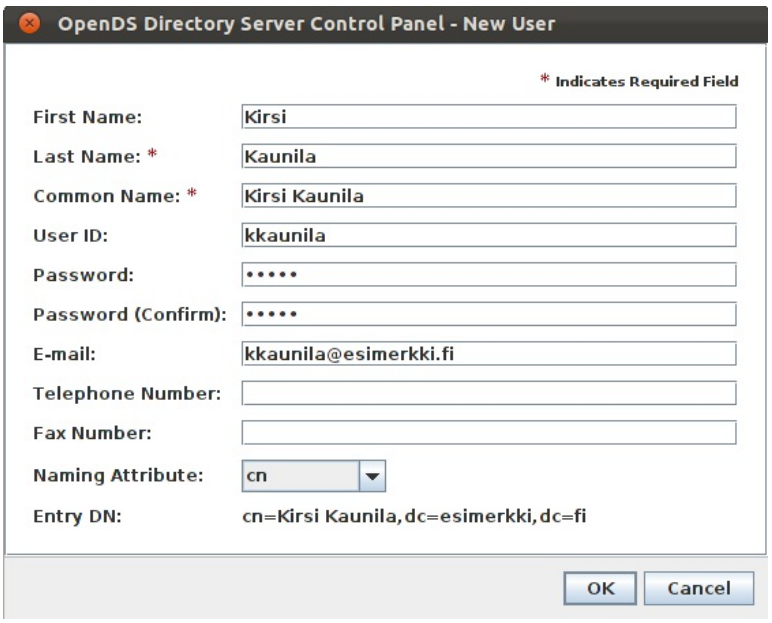
Kuvio 18. OpenDS:n hallintatyökalun pääikkuna.

Hallintatyökalun pääikkunasta voi kätevästi esimerkiksi käynnistää ja sulkea palvelun, sekä näkee palvelimen perustiedot. Kuviosta 19 näkyy, kuinka työkalulla on helppo hallita ja muokata hakemistopalvelun tietokantaa ja lisätä kirjauksia. Käyttäjien (kuvio 20), ryhmien (kuvio 22), OU:den (kuvio 21), organisaatioiden ja domainien luonnille löytyy helpot työkalut. Mikäli haluaa, voi uudet kirjaukset syöttää myös LDIF-muodossa.

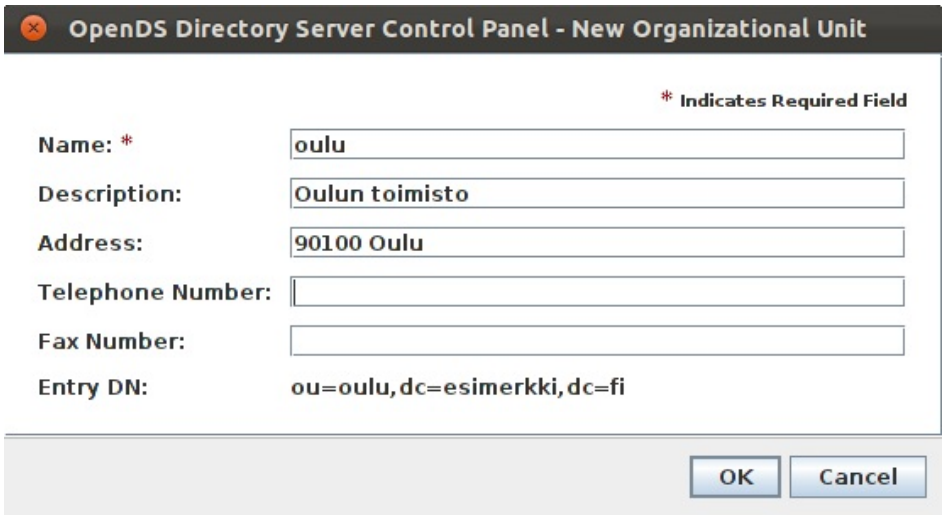
Samaisella työkalulla voi myös hallita käyttäjien salasanoja ja lisätä sekä poistaa käyttäjiä eri ryhmistä. Kirjauksia voi kopioida ja duplikoida, jolloin uusien samankaltaisen kirjausten lisääminen on helppoa.



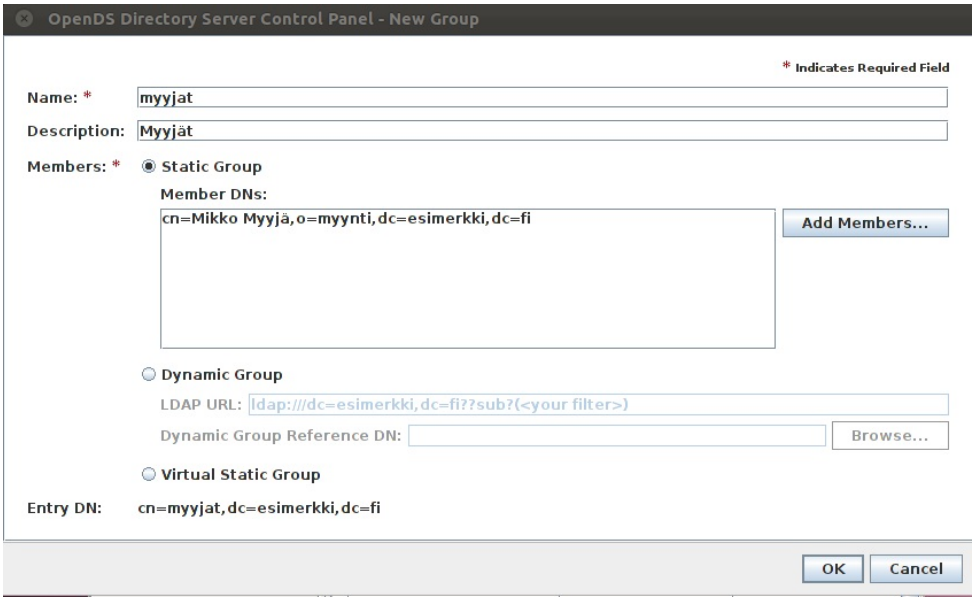
Kuvio 19. OpenDS:n hallintatyökalun kirjauksien muokkaus.



Kuvio 20. Uuden käyttäjän lisääminen OpenDS:n hallintatyökalulla.



Kuvio 21. Uuden OU:n lisääminen OpenDS:n hallintatyökalulla.



Kuvio 22. Uuden ryhmän luominen OpenDS:n hallintatyökalulla.

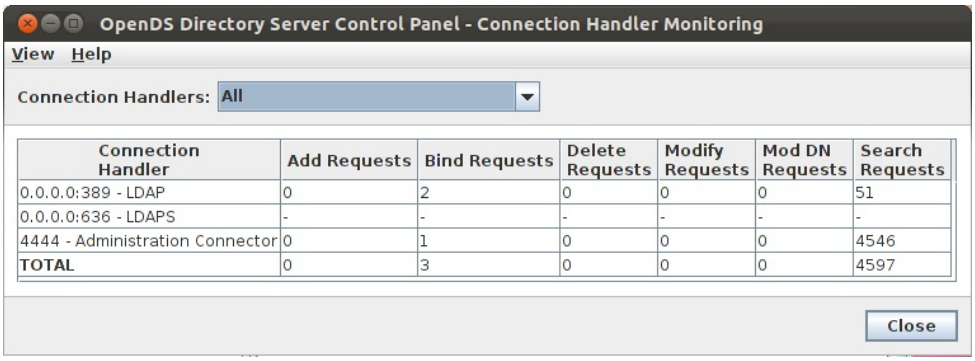
Hallintatyökalulla voi myös muokata, lisätä ja poistella skeemoja. Kirjauksille voi siis antaa omia ominaisuuksia ja arvoja näille ominaisuuksille, mikäli niitä ei valmiina jo valtavasta skeemalistasta löydy.

3.3.3 Monitorointi

Hallintatyökalu pitää sisällään seurantatyökalun, jolla voi hyvin tarkkailla palvelimen tietoja ja toimintaa. Seurantatyökalu on jaettu kolmeen osaan; perustiedot, yhteyksien hallinta ja tehtävien hallinta.

Perustiedoista löytyy palvelimen nimi, käyttöjärjestelmä ja muistinkäyttö. Sieltä näkee myös palvelimen Javan tiedot, eli version ja muistinkäytön. Tämän lisäksi siellä on seurattavana pyyntöjen ja kirjauksien lisäykset ja muokkaamiset sekä liikenne tietokannan ja työasemien välillä.

Kuviossa 23 näkyy, kuinka yhteyksien hallinnasta nähdään hakemistopalvelimelle tällä hetkellä voimassa olevat yhteydet. täältä myös nähdään hakemistopalvelimen tietokantaan kohdistuvien pyyntöjen määrät, ja mistä ne on lähetetty.



Kuvio 23. Yhteyksien seurantaikkuna OpenDS:n hallintatyökalussa.

3.4 OpenLDAP

OpenLDAP:n asennus vaatii hieman enemmän töitä, koska se vaatii toimiakseen Berkleyn tietokantaohjelmiston. Asennus on kuitenkin suoraviivainen toimenpide.

3.4.1 Berkleyn tietokanta

OpenLDAP, tai tarkemmin ottaen slapd, vaatii toimiakseen Berkleyn tietokantaohjelmiston. Se asentuu palvelimelle paketin lataamisen jälkeen seuraavilla komennoilla:

cd db-5.3.15.NC

cd build_unix

../dist/configure –prefix=/usr/local/ (määritetään asennushakemistoksi /usr/local/)

make

make install

3.4.2 TLS

TLS ei ole vaatimuksena OpenLDAP:n käyttöön, mutta se tuo hyvän lisän salaus- ja autentikointimenetelmiin. Ilmainen OpenSSL-paketti sisältää TLS-kirjastot, joita voi käyttää OpenLDAP:n kanssa. OpenSSL:n asennus onnistuu paketin lataamisen jälkeen samalla tavalla, kuin Berkleyn tietokantakin:

gzip -d openssl-0.9.8.tar.gz

tar xfv openssl-0.9.8.tar

cd openssl-0.9.8

./config shared --openssldir=/usr/local

make

make install

3.4.3 OpenLDAP:n asennus

OpenLDAP:n asennuspaketti löytyy OpenLDAP:n Internetsivuilta. Se puretaan haluamaan kansioon normaalisti ja asennus hoituu seuraavilla komennoilla:

./configure

make depend

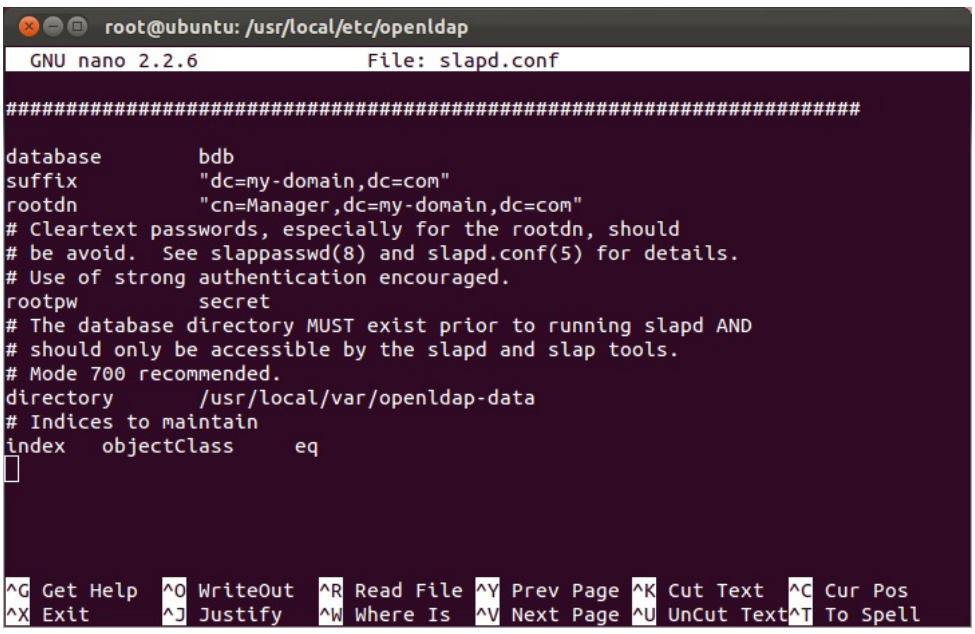
make

make test

make install

3.4.4 Konfigurointi

OpenLDAP:n perustietojen konfigurointi tapahtuu pääosin *slapd.conf* -tiedostoa muokkaamalla. Kuviosta 24 käy ilmi, mitä kyseinen tiedosto esimerkiksi sisältää.



Kuvio 24. *Slapd-conf* –tiedosto.

3.4.5 Palvelun käynnistäminen ja sammuttaminen

OpenLDAP:n käynnistäminen ja ajaminen tapahtuu komennolla *slapd*. Tilan voi tarkistaa esimerkiksi komennolla *ps aux | grep slapd*, joka tulostaa rivit:

root 2105 0.0 0.3 14956 3420 ? Ssl 14:26 0:00 ./slapd

root 2110 0.0 0.0 4456 772 pts/0 S+ 14:27 0:00 grep --color=auto slapd

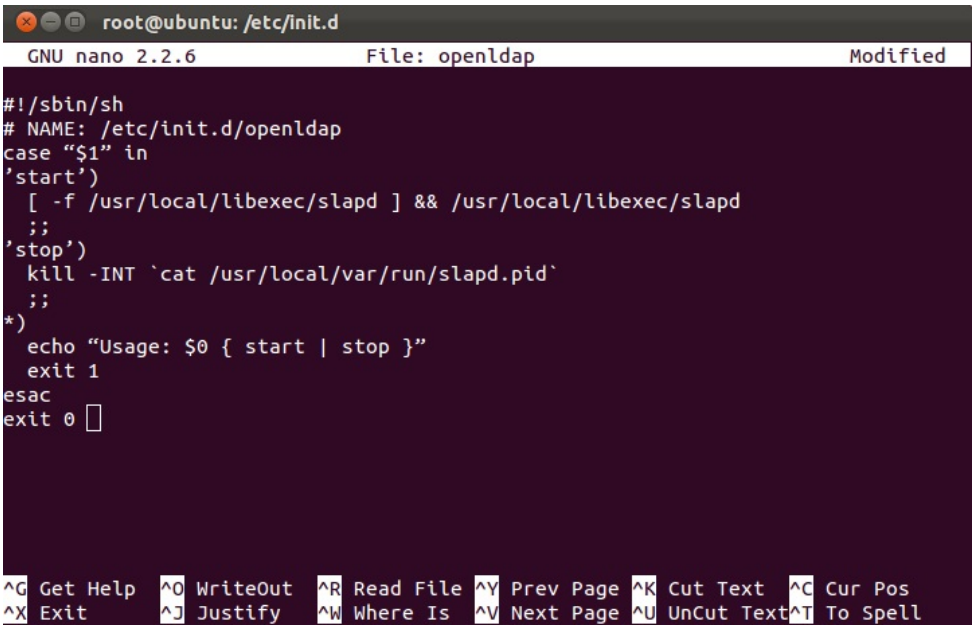
Palvelu on näin ollen päällä.

OpenLDAP-palvelun lopettaminen onnistuu komennolla:

sudo kill -INT `cat /usr/local/var/run/slapd.pid`

Palvelun voi myös sulkea komennolla *kill -9*, mutta se ei ole suositeltu tapa, sillä se saattaa korruptoida hakemistopalvelun tietokantaa.

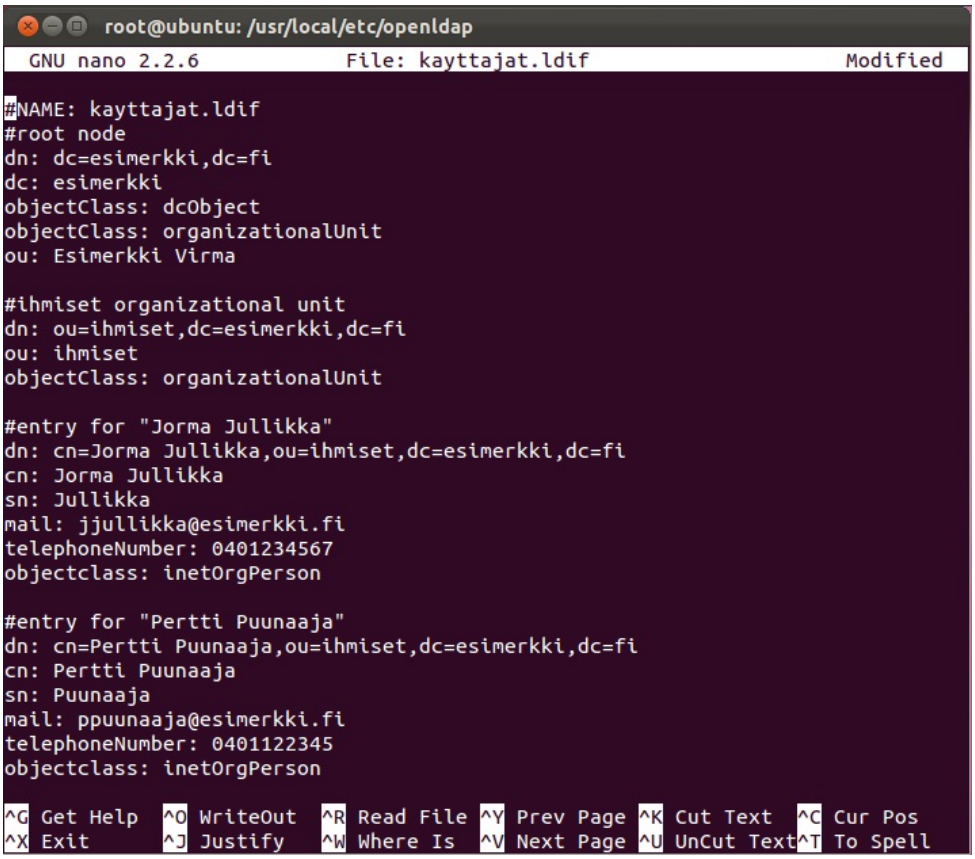
Palvelun saa myös käynnistymään automaattisesti tietokoneen käynnistyksen yhteydessä ja sammumaan ennen tietokoneen sammumista. Tämä onnistuu luomalla kuviossa 25 esiintyvä yksinkertainen skripti */etc/init.d*-hakemistoon.



Kuvio 25. Automaattinen käynnistys- ja sulkemisskripti OpenLDAP:lle.

3.4.6 Tietojen lisääminen tietokantaan

OpenLDAP:n tietokannan ja kirjausten muokkaus sekä uusien kirjausten lisääminen palvelimelle tapahtuu *ldapmodify*-työkalulla. Kätevintä on luoda kuviossa 26 esiintyvä LDIF-tiedosto, joka viedään *ldapmodify*-työkalulla palvelimelle sisältöineen.



Kuvio 26. Esimerkki *ldif* –tiedostosta.

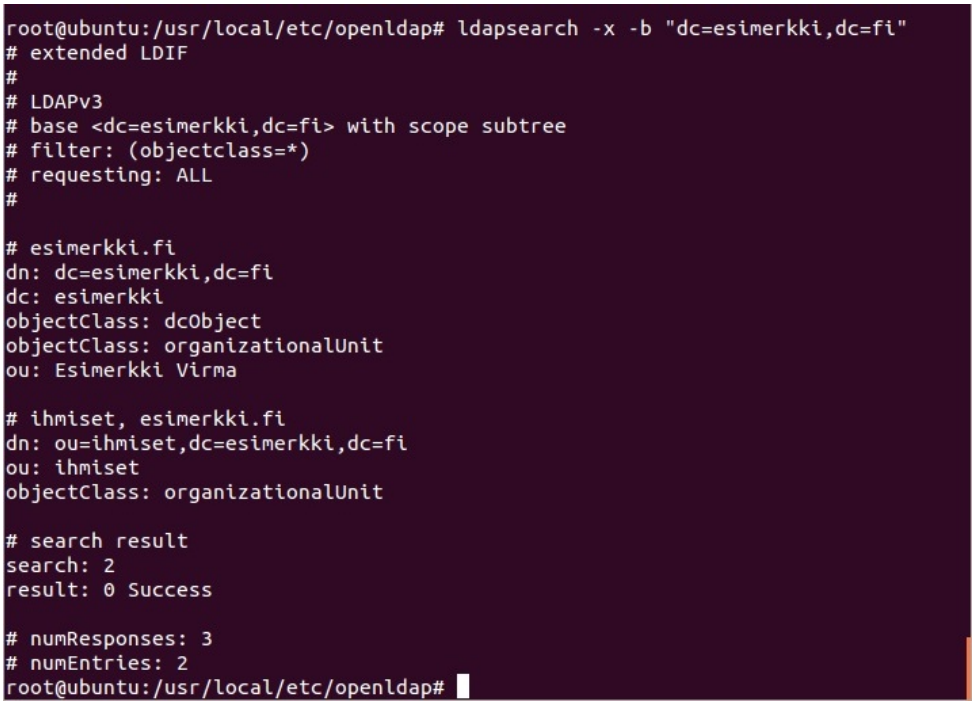
Kun tiedosto on luotu, se voidaan viedä palvelimelle komennolla:

ldapmodify -D "cn=admin,dc=esimerkki,dc=fi" -w secret \ -x -a -f kayttajat.ldif

Tietokannan tietojen päivittämisen voi tarkastaa hakemalla palvelimelta kirjauksia seuraavalla komennolla:

ldapsearch -x -b "dc=esimerkki,dc=fi"

Tämä komento tulostaa kuviosta 27 esiintyvät tulokset.



Kuvio 27. Haku *ldapsearch* –komennolla.

3.4.7 Autentikointi

OpenLDAP tukee kolmea eri autentikointimuotoa:

- anonyymi
- ei-autentikoitu
- käyttäjätunnuksella ja salasanalla autentikoitu

Palvelimelle pääsee kirjautumaan anonyymisti syöttämättä mitään käyttäjätunnusta tai salasanaa. Tämän ominaisuuden saa otettua OpenLDAP-palvelimelta pois muuttamalla riviä *disallow bind_anon* tiedostossa *slapd.conf*.

Ei-autentikoitu menetelmä on syöttää käyttäjätunnus, mutta ei salasanaa. Tällä menetelmällä kirjauduttaessa saadaan oletuksena samat oikeudet kuin anonyymissä kirjautumisessa. Tätä ominaisuutta voi muokata samasta tiedostosta muokkaamalla riviä *allow bind_anon_cred.*

Käyttäjätunnus ja salasana syötettynä saadaan paras mahdollinen autentikointi tietoturvan ja monitoroinnin kannalta. Tällä tavalla varmistetaan, että käyttäjä, joka palvelimelle kirjautuu, on oikeutettu tekemään mahdollisia muutoksia käyttäjän rajoitusten mukaisesti.

3.5 Kerberos

Mikäli palvelimessa on Linux –käyttöjärjestelmä, avoimen lähdekoodin hakemistopalvelut eivät suoraan tue muilta alustoilta, esimerkiksi Windows –käyttöjärjestelmistä, kirjautumista palvelimelle. Tämän saavuttaakseemme pitää palvelimelle asentaa kolmannen osapuolen ohjelmisto: Kerberos.

Kerberos on verkon tunnistus- ja autentikointiohjelmisto. Se muodostaa käyttäjän ja palvelimen lisäksi kolmannen osapuolen, joka mahdollistaa esimerkiksi eri käyttöjärjestelmien keskeiset kirjautumiset.

3.5.1 Asennus

Kerberospalvelimen asennus onnistuu muutamalla yksinkertaisella komennolla. Aluksi pitää asentaa *krb5-kdc* and *krb5-admin-server* -paketit:

apt-get install krb5-kdc krb5-admin-server.

Pakettien asennus pyytää lopuksi syöttämään oman Kerberos nimen “realmille”, eli alueelle, jossa Kerberospalvelin toimii. Uusi alue luodaan asennuksen päätteeksi komennolla *krb5_newrealm*.

3.5.2 Konfigurointi

Kerberospalvelinta pääsee muokkaamaan komennolla *kadmin.local*. Tämän jälkeen jälkeen komentorivi muuttuu muotoon *kdamin.local*.

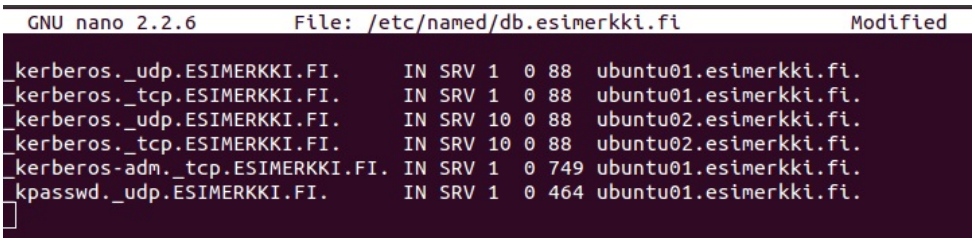
Käyttäjiä, ryhmiä ja muita tietoja kutsutaan Kerberoksessa ”principaleiksi”. Näitä pääsee lisäämään helposti komennolla *addprinc principal/instance*. Instanssia käytetään harvinaisimmissa tapauksissa, kuten esimerkiksi tässä tapauksessa (kuvio 28) admin-tunnuksen luomiseen.

```
kadmin.local:  addprinc ubuntu/admin
WARNING: no policy specified for ubuntu/admin@ubuntu; defaulting to no policy
Enter password for principal "ubuntu/admin@ubuntu":
Re-enter password for principal "ubuntu/admin@ubuntu":
Principal "ubuntu/admin@ubuntu" created.
```

Kuvio 28. Kerberoksen konfigurointi.

Kyseiselle admin –tunnukselle annetaan järjestelmänvalvojan oikeudet, joka tapahtuu lisäämällä rivi ”*ubuntu/admin@esimerkki.fi *” tiedostoon *kadm5.acl*. Tämä vaatii Kerberos-palvelimen uudelleenkäynnistyksen, joka hoituu komennolla *krb5-admin-server restart*.

KDC (Key Distribution Center) tarkoittaa kolminaisuutta, joka koostuu ”principalien” tietokannasta, autentikointipalvelimesta ja pääsynhallintapalvelimesta. Jokaiselle Kerberosalueelle pitää olla vähintään yksi KDC. Jotta käyttäjät tunnistaisivat Kerberosalueen KDC:n, täytyy luoda */etc/named/db.esimerkki.fi*–tiedosto ja lisätä sinne kuviossa 29 esiintyvät rivit.



Kuvio 29. *db.esimerkki.fi* –tiedosto.

Tämä ohjaa tulevat autentikointipyynnöt oikeille palvelimelle ja pystyy näin autentikoimaan käyttäjät ja antamaan heille tarvittavat oikeudet.

3.6 DNS

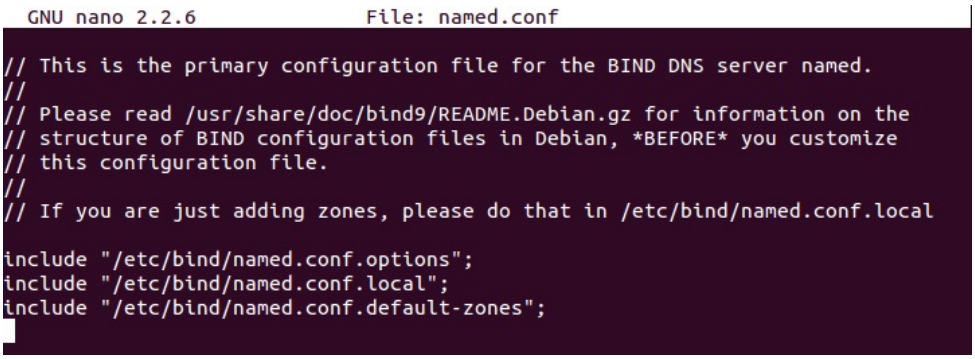
Työssä esiintyneet hakemistopalvelut eivät sisällä myöskään minkään sortin DNS -palvelua. Tämän vuoksi se pitää Ubuntu –palvelimelle asentaa erikseen. DNS-palvelu on palvelimelle erittäin tärkeä, varsinkin jos organisaatiossa on käytössä useita kymmeniä työkoneita ja palvelimia.

3.6.1 Asennus

DNS –palvelun asennus on todella yksinkertainen prosessi. Palvelu asennetaan palvelimelle komennolla *apt-get install bind9*. Tämän lisäksi on syytä asentaa hyödyllinen lisäpaketti testaamiseen ja viankorjaukseen, *dnsutils*, myöskin *apt-get install* –komennolla.

3.6.2 Konfigurointi

DNS –palvelun konfigurointitiedostot löytyvät hakemistosta */etc/bind*, jossa tärkein tiedosto on kuviossa 30 esiintyvä *named.conf*.



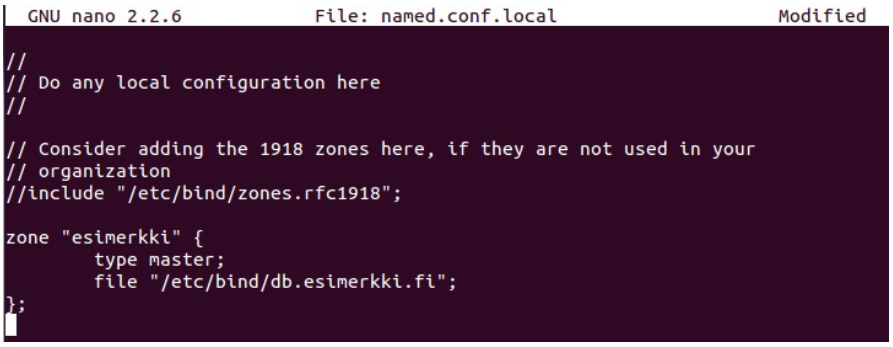
Kuvio 30. *named.conf* –tiedosto.

Tämän lisäksi hakemistosta löytyy myös seuraavat tiedostot:

- named.conf.options, kertoo DNS-palvelimelle, mistä tiedostot löytyvät
- db.root, kuvailee maailman juurinimipalvelimet.

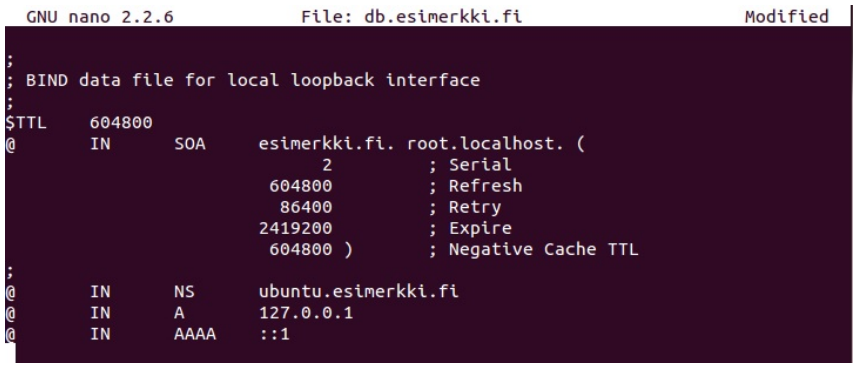
DNS –palvelimelle kannattaa antaa oman palveluntarjoajan nimipalvelimet *named.conf* –tiedostoon, jotta nimipalvelimet päivittyvät automaattisesti ja toimivat kokoajan.

Jotta palvelimesta saadaan DNS –palvelun isäntäkone (Primary Master), täytyy *named.conf.local* –tiedostoon tehdä kuviossa 31 esiintyvät muutokset.



Kuvio 31. *named.conf.local* –tiedosto.

Tämän jälkeen pitää luoda uusi tiedosto *db.esimerkki.fi* ja muokata sinne kuvion 32 esittämät palvelimen tiedot:



Kuvio 32. *db.esimerkki.fi* –tiedosto palvelimen omilla tiedoilla.

Kyseiseen tiedostoon voi tämän jälkeen lisäillä tarvittavia DNS –kirjauksia, esimerkiksi:

- isäntänimi vastaamaan IP-osoitetta
- aliasosoite haluamalle oikealle osoitteelle
- sähköpostin ohjausosoitteet.

DNS –palvelu vaatii vielä tämän jälkeen ”Reverse Zone” –tiedoston, eli tiedoston, joka antaa DNS –palvelimelle mahdollisuuden etsiä osoitteita vastaavat isäntänimet. Tiedostoon */etc/bind/named.conf.local* täytyy lisätä kuviossa 33 esiintyvä tieto.

```
zone "192.168.0.in-addr.arpa" {
        type master;
        notify no;
        file "/etc/bind/db.192";
};
```

Kuvio 33. Osa *named.conf.local* –tiedostoa.

Viimeisenä pitää vielä luoda db.192 –tiedosto (db.127 –tiedostosta kopioituna) ja tehdä siihen samat muutokset kuin aiemmin db.esimerkki.fi –tiedostolle (kuvio 32).

Tämän jälkeen palvelimella on toimiva DNS –palvelu ja se osaa ohjata lähiverkon koneiden tietokanta- ja hakemistohaut sekä –pyynnöt toimialueelta.

4 POHDINTA JA JOHTOPÄÄTÖKSET

Avoimen lähdekoodin hakemistopalvelut yllättivät minut positiivisesti. Tiesin, että kun kyse on Linux –pohjaisesta palvelimesta, on odotettavissa tosi paljon komentorivipohjaista konfigurointia ja säätämistä. Ottaen huomioon Linux –käyttöjärjestelmäkokemukseni, pelkäsin, että törmään työssä ylitsepääsemättömiin ongelmiin.

Aluksi minulla oli mukana myös neljäs palvelu: 389 Directory Server. Tämä projekti jäi asennusvaiheessa pois, koska se osottautui ylivoimaiseksi haasteeksi. Ensinnäkin, se on optimoitu Fedora-käyttöjärjestelmälle, joten minun olisi pitänyt ottaa työhön mukaan myös uusi käyttöjärjestelmä (jota en ole koskaan ennen käyttänyt). Toisekseen, etsiessäni Internetistä asennusapua ja dokumentaatiota kyseisestä palvelimesta törmäsin useasti vastauksiin, joissa kehotettiin kääntymään suosiolla toisen palvelun puoleen.

Suurimmat ongelmat, mitä kohtasin tätä työtä tehdessäni, johtuivat vähäisestä Linux –kokemustaustastani. Komentorivikehote tuli tämän työn myötä tosi tutuksi välineeksi ja Linuxin yleiskäyttö, varsinkin palvelinkäytössä, tuli entistä tutummaksi. Alan vähätellen ymmärtää joitain järjestelmän ylläpitäjiä, jotka kääntyvät Linux –palvelimien puoleen palvelinratkaisuissa.

4.1 ApacheDS

ApacheDS oli hakemistopalveluista ainoa, joka oli vähäänkään tuttu ennestään minulle. Apache on tuttu palvelu ammattikorkeakoulun Linux –kursseilta, joten ApacheDS:n kehitystiimi oli jossain määrin tuttu.

ApacheDS:n positiivisin yllätys oli vartavasten sille kehitetty oma hallintatyökalu Apache Directory Studio. Kyseistä työkalua voi käyttää muissakin LDAP –palvelimissa, mutta päätin käyttää sitä vain ApacheDS:n kanssa.

Palvelun asennus oli helppo toimenpide, mutta ApacheDS pohjautuu täysin Javaan, joten sen kanssa voi tulla ongelmia joidenkin palvelinratkaisuiden kanssa.

Positiivista:

- Hallintatyökalu.
- Asennus.

Negatiivista:

- Java (tukeeko palvelin?).

4.2 OpenDS

OpenDS osoittautui lupaavaksi palveluksi. Koska sen taustalla toimii Sun organisaatio, on odotettavissa, ettei sen kehitys ja tuki ole loppumassa ihan lähi aikoina. Taustaorganisaatio tuo myös lupaavat odotukset tulevaisuudelle.

OpenDS toimii täysin Javan tekniikalla, joten tämä mahdollisesti tuo hankaluuksia joissain palvelinratkaisuissa. Vaikka OpenDS:ä voi käyttää myös komentorivipohjaisena, itse koin parhaimpana ominaisuutena OpenDS:n hallintatyökalun. Se oli tosi selkeä ja kattava ja sen käyttö onnistui heti ilman erillisiä opastuksia.

Palvelimen asennus oli myös helppo projekti, eikä se vaatinut sen kummemmin mitään esivalmisteluja.

Positiivista:

- Taustaorganisaatio.
- Hallintatyökalu.
- Helppo asennus.

Negatiivista:

- Java (tukeeko palvelin?).

4.3 OpenLDAP.

OpenLDAP on ehkä tunnetuin avoimen lähdekoodin hakemistopalvelu ”open source” –piireissä. Tästä johtuen työtäni aloittaessa minulla oli positiivisin mielikuva OpenLDAP:sta.

Työni saatua päätökseen, OpenLDAP oli vajonut negatiivisimmaksi palveluksi mielestäni. Sen asennus vaati eniten työtä (Berkleyn tietokannan asennus) ja sen konfigurointi tapahtuu ainoastaan komentoriviltä.Tämän ei pitäisi olla ongelma paljon Linuxia palvelinkäytössä käyttäneen ammattilaisen käsissä, mutta koska komentorivi ja Linux –komennot ovat hieman hakusessa itselläni, tuotti tämä kaikista eniten ongelmia työssäni.

Positiivista:

- Dokumentaatio.
- Vankka ”open source” –yhteisö taustalla.

Negatiivista:

- Asennus.
- Hallinta ja konfigurointi.

4.4 Lopputuomio

Pääsääntöisesti avoimen lähdekoodin hakemistopalveluilla ei pääse yhtä hyvin hallitsemaan ja ylläpitämään toimialuetta kuin Microsoftin Active Directoryllä. Linux –palvelimille on tarjolla lukuisia lisäpalveluita, joita voi näiden hakemistopalvelujen rinnalle asentaa ja ne yleensä toimivat hyvin keskenään ja kompensoivat toisten palveluiden heikkouksia.

Tämän työn pohjalta huomaa jo heti, että esimerkiksi autentikointi- ja DNS –palvelut vaativat jo kääntymään kolmannen osapuolen palveluihin. Microsoftin Active Directorystä löytyy nämä ominaisuudet jo valmiina. Tämän lisäksi yksi suuri ero on, että Active Directory löytyy valmiina jo Windows Server –käyttöjärjestelmistä, joten hakemistopalvelua ei tarvitse Microsoft –ympäristössä erikseen asentaa.

Tämän työn pohjalta ei pysty suoraan sanomaan, kuinka hyvin mahdollisilla kolmannen osapuolen sovelluksilla pystyy Active Directoryn ominaisuudet replikoimaan. Tämä vaatisi lukemattomat määrät työtunteja, jotta kaikkiin palveluihin voisi perehtyä vaadittavalla tavalla. Linux –ympäristössä työskennellessä uudet palvelut ja lisäohjelmistot mitä palvelimille asennetaan vaativat tosi paljon perehtymistä niiden ominaisuuksiin ja konfigurointiin.

Loppujen lopuksi päätös pohjautuu omiin mielitymyksiin. Mikäli on työskennellyt paljon Linux –ympäristössä (varsinkin palvelinpuolella) ja haluaa kustomoida palvelusta ja palvelimesta mieleisensä, saa avoimen lähdekoodin palveluilla varmasti toimivan ratkaisun toimialueen ylläpitoon. Tämä vaatii enemmän työtä ja perehtymistä, mutta tuo enemmän vapautta.

Mikäli haluaa varmasti toimivan ja helppokäyttöisen hakemistopalvelun, suosittelen kallistumaan Active Directoryn puoleen. Opintojen pohjalta kokemukseni Active Directorystä ovat positiiviset. Toimialueen hallinta oli helppoa ja ylläpito kätevää. Lukemattomat ulkopuoliset dokumennoinnit ja tottakai Microsoftin oma kattava tuki pitävät huolen, että ongelmiin löytyy varmasti ratkaisu. Maksua vastaan, tottakai.

Lopuksi vielä vertailussa taulukoituna hakemistopalveluiden perustiedot (taulukko 1) ja tärkeimmät tekniset tiedot (taulukko 2):

Taulukko 1. Hakemistopalvelut vertailussa: perustiedot.

	Active Directory	ApacheDS	OpenLDAP	OpenDS
Sivusto	http://www.microsoft.com/	http://directory.apache.org/	http://www.openldap.org/	http://www.opends.org/
Lisenssi	Microsoft	Apache License 2.0	OpenLDAP Public License	Common Development and Distribution License
Dokumentaatio	kattava	minimaalinen	kattava	kattava
Koodi	C/C++/.NET	Java	C/C++	Java
Organisaatio taustalla	Microsoft	Apache Software Foundation	OpenLDAP Foundation	Sun
Alkuperä	Microsoft	uusi	Michiganin yliopisto	uusi
Hallintatyökalu ylläpitoon	kyllä	ei	ei	kyllä
Asennus	sisällettynä Windows Server -käyttöjärjestelmiin	asennusohjelma	paketti/build	asennusohjelma

Taulukko 2. Hakemistopalvelut vertailussa: tekniset tiedot.

	Active Directory	ApacheDS	OpenLDAP	OpenDS
Back-End	useita, mm. MySQL	JDBM ja kustomoitu	useita, mm. Berkleyn tietokanta	Javapohjainen Berkleyn tietokanta
useampi Back-End	kyllä	kyllä	kyllä	kyllä
Front-End	LDAP, MMC-manager, web-manager	LDAP, Kerberos, DNS, NTP, DHCP	LDAP/LDAPS	LDAP/LDAPS. DSMLv2 gateway (SOAP/HTTP)
Replikointi	Multi-Master	Multi-Master (2 masters) (tulossa)	Single-Master	Multi-Master (max 8 masteria)
Seuranta	LDAP, kustomoitavat MMC-hallintatyökalut	LDAP	LDAP	LDAP/SNMP/JMX
Skeemat	vakiot	koottu	dynaamiset/ldap	dynaamiset/ldap/gui

LÄHTEET

ApacheDS 2012 a. http://directory.apache.org/apacheds/1.5/index.html (Luettu 24.1.2012)

ApacheDS 2012 b. http://directory.apache.org/apacheds/1.5/features.html (Luettu 12.2.2012)

ApacheDS 2012 c. http://directory.apache.org/studio/static/users_guide/ldap_browser/images/tools_ldap_perspective_1.png (Luettu 2.5.2012)

Apache Subversio 2012 a. http://subversion.apache.org/ (Luettu 11.4.2012).

Apache Subversio 2012 b. http://subversion.apache.org/features.html (Luettu 11.4.2012).

Clines S. & Loughry M. 2008. Active Directory For Dummies, 2nd Edition. Wiley Publishing, Inc.

Coss 2012. http://coss.fi/avoimuus/ (Luettu 21.5.2012).

OpenDS 2012 a. https://www.opends.org/wiki/page/About (Luettu 27.1.2012)

OpenDS 2012 b. https://www.opends.org/wiki/page/ProjectDefinition#section-ProjectDefinition-WhatIsOpenDS (Luettu 27.1.2012)

OpenLDAP 2012 a. http://www.openldap.org/project/ (Luettu 12.2.2012)

OpenLDAP 2012 b. http://www.openldap.org/faq/data/cache/30.html (Luettu 12.2.2012)

OpenLDAP 2012 c. http://www.openldap.org/doc/admin24/install.html (Luettu 12.2.2012)

OpenLDAP 2012 d. http://www.openldap.org/doc/admin24/intro.html (Luettu 12.2.2012)

Price, J. A., Price B. & Fenstermacher S. 2008. Mastering Active Directory for Windows Server 2008. Wiley Publishing, Inc.

Tenouk 2012 http://www.tenouk.com/ModuleM_files/image007.png (Luettu 2.5.2012)