Satakunnan ammattikorkeakoulu
OPINNÄYTETYÖ

Tomi Nordberg

SATAKUNNAN AMMATTIKORKEAKOULU

Tomi Nordberg
2008

LDAP-AUTENTIKOINTI ERI KÄYTTÖJÄRJESTELMISSÄ

Tekniikka Rauma
Tietotekniikan koulutusohjelma

LDAP-AUTENTIKOINTI ERI KÄYTTÖJÄRJESTELMISSÄ

Tomi Nordberg
Satakunnan ammattikorkeakoulu
Tekniikka Rauma
Tietotekniikan koulutusohjelma

Helmikuu 2008
Valvoja: DI Vesa Raikisto
Ohjaaja: DI, laboratorioinsinööri Olli Vainio
UDK: 004.7
Asiasanat: Linux, palvelimet, protokollat, tietoliikenneverkot, Windows

Työn tavoitteena oli saada eri käyttöjärjestelmät käyttämään yhteistä Linux-palvelimella sijaitsevaa käyttäjätietokantaa. Käyttäjätietokannan piti olla yhteinen, niin että käyttäjä pystyi käyttämään samaa käyttäjätunnusta käyttöjärjestelmästä riippumatta. Kirjautumisen tuli olla myös turvallista, jolloin huomioon piti ottaa mahdolliset väärinkäytöstilanteet ja verkossa kulkevan tiedon salaaminen. Kirjautuvat käyttöjärjestelmät koostuivat Microsoftin eri Windows-versioista, Debian Linuxista ja Sun Solaris 10:stä.

Työn toteuttaminen tapahtui Satakunnan ammattikorkeakoulun Tekniikka Rauman itseopiskeluluokassa, jossa oli pystytettynä tarvittava testiverkko tietokoneiden välillä. Palvelimena toimi Debian Sarge -pohjainen tietokone ja käytössä oli kaksi muuta tietokonetta palvelimelle sisään kirjautuvia käyttöjärjestelmiä varten. Eri käyttöjärjestelmät tuli asettaa käyttämään LDAP-protokollaa sisään kirjautumisen yhteydessä ja tallennettaessa käyttäjää koskevia tietoja palvelimelle. Windows-ympäristöä varten palvelimelle piti ottaa käyttöön Samba-ohjelmisto.

Järjestelmä saatiin toimivaksi kokonaisuudeksi ja palvelin toimi muiden työryhmän koneiden käyttäjätietokantana. Kaikkien käyttäjätietojen keskittäminen yhdelle tai useammalle varapalvelimelle oli hyvä tapa saada yrityksen työntekijöiden sisään kirjautumiset toimimaan joustavasti ja hallitusti. Debian Linux oli vakaa käyttöjärjestelmä, mikä teki siitä luotettavan ja varman vaihtoehdon palvelimen käyttöjärjestelmäksi.

LDAP AUTHENTICATION IN DIFFERENT OPERATING SYSTEMS

Tomi Nordberg
Satakunta University of Applied Sciences
School of Technology Rauma
Information Technology

Commissioned by DNA OY
Supervisor: Vesa Raikisto, MSc
February 2008
Tutor: Olli Vainio, MSc, Laboratory Engineer
UDK: 004.7
Keywords: Linux, servers, protocols, telecommunications networks, Windows

The purpose of the project was to allow the users of different operating systems to log in using one centralized network database containing all the account and password information. The operating system for the database was Debian Sarge running OpenLDAP-software with Samba to negotiate with the client computers. The security of the connections was also a concern, so the connections used in the project should be relatively safe against hackers and brute force attacks against the database.

To achieve the given objectives, a small network of three computers was created. One of them was the server running Debian Sarge, the other two were clients running other operating systems. The different operating systems run on the computers were to be configured so that they would use LDAP as the login protocol.

Eventually the test network used in the project was working properly, and all the clients were connecting to the central server correctly using encrypted connections. The server was logging information, and using that information hacking attempts were recognized in time.

SISÄLLYS

TERMISTÖ

Active Directory
Active Directory (AD) on monipuolinen käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista. Active Directory -hakemistopalvelu mahdollistaa keskitetyn resurssien jakamisen käyttäjille ja sovelluksille sekä tarjoaa selkeän tavan nimetä, kuvata, paikallistaa, hallita ja suojata käytössä olevia verkon resursseja. Active Directory -hakemistopalvelu on sisällytetty Microsoft Windows Server 2003 ja Microsoft Windows Server 2000 -käyttöjärjestelmiin.

Autentikointi
(Käyttäjän) todennus

Cisco
Yhdysvaltalainen verkko- ja kommunikaatioteknologiayhtiö

Debian Sarge
Linux-jakelu, Sarge vastaa versionumeroa 3.1.

Domain Controller, Primary Domain Controller
Windows-verkossa sijaitseva palvelin, joka on vastuussa todennuksesta ja tietoturvasta

Fedora Core 6
Linux-jakelu

Hakemistopalvelu
Palvelu, jonka tehtävä on säilöä, vastaanottaa ja antaa eteenpäin tietoja

Hakkerointi
Esim. tietokoneeseen murtautuminen turvallisuusaukkoja hyödyntäen

LDAP
Lightweight Directory Access Protocol, X.500:sta kevennetty hakemistopalvelu

Linux

Unixin kaltainen, vapaa open-source-pohjainen käyttöjärjestelmä

Käyttöjärjestelmä

Ohjelmisto, joka vastaa tietokoneen resurssien jakamisesta käyttäjälle

NSCD

Name Service Cache Daemon, taustalla ajettava palvelu Linuxilla, joka vastaa nimipalveluista

NSS –moduuli

Name Service Switch, määrittelee, mistä nimipalvelusta tiedot haetaan

OpenLDAP

Ilmainen open-source-projekti, jonka avulla voi käyttää LDAP-protokollaa

OSI-pino

Seitsemästä kerroksesta koostuva kuvaus verkon protokollan rakenteesta

OU, Organizational Unit

OU:iden avulla voidaan luokitella hakemistoissa sijaitsevia objekteja

Palvelin

Tietokone, joka palvelee verkkoa käyttäviä työasemia

PAM –moduuli

Pluggable Authentication Module, apuväline käyttäjäntunnistukseen Linuxissa

Protokolla

Kokonaisuus sääntöjä, joiden avulla määritellään internetissä tapahtuva tietty tapahtuma. (http, ftp, ym.)

Schema, kaava

Malli, jolla kuvataan toimialueessa esiintyvien käsitteiden suhteita

SAMBA

Kokoelma palveluita ja protokollia, jolla Windowsin levynjaot ym. saadaan käyttöön muihinkin käyttöjärjestelmiin

Solaris

Sun Microsystemsin kehittämä käyttöjärjestelmä

SSL-salaus

Secure Sockets Layer, salausprotokolla, jolla pyritään estämään esim. salakuuntelu, tiedon muokkaaminen ym.

TCP-protokolla

Transmission Control Protocol, yksi internetin ydinprotokollista

Toimialue, domain

Verkossa sijaitseva ryhmä tietokoneita, jotka jakavat tietyn hakemiston

Unix

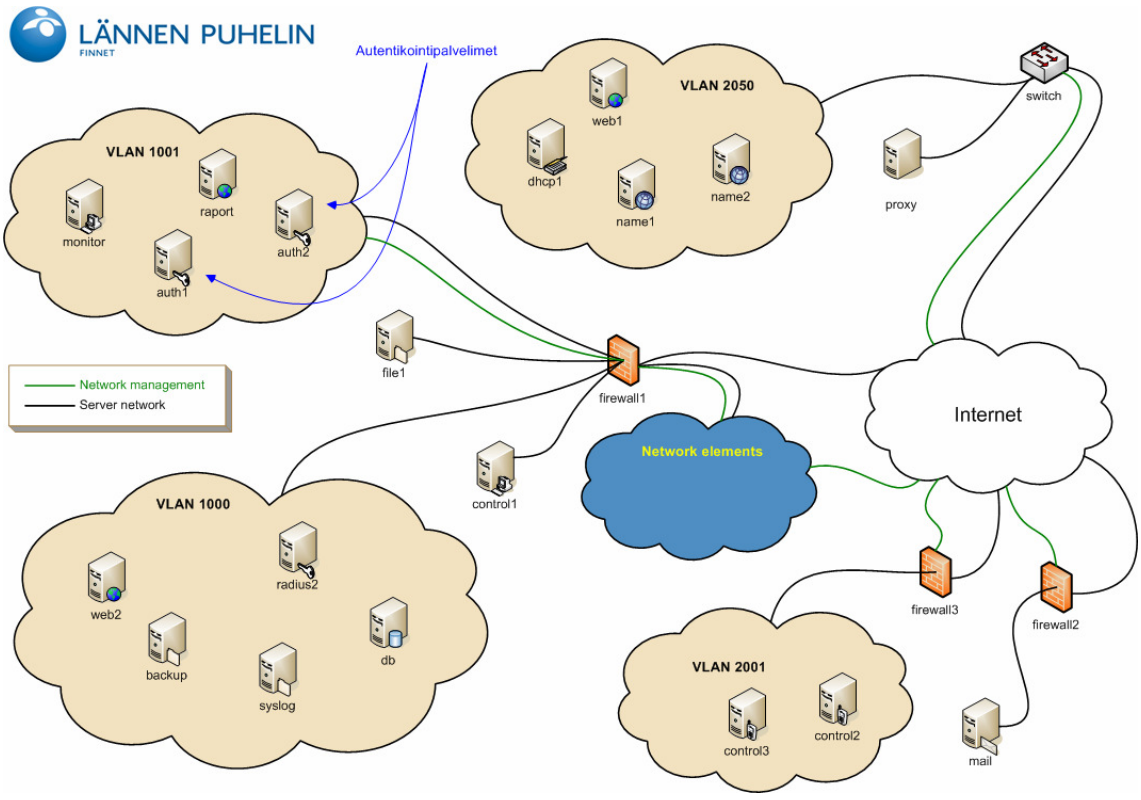
AT&T:n työntekijöiden kehittämä käyttöjärjestelmä

X.500-standardi

Joukko tietokoneen verkkostandardeja, jotka määrittelevät tietynlaisen hakemistopalvelun

1 JOHDANTO

Työn tarkoituksena oli toteuttaa yrityksen käyttäjien autentikointi siten, että kaikki käyttäjätunnukset ja salasanat sijaitsevat yhdellä Debian Sarge -palvelimella ja niitä haetaan sisään kirjauduttaessa käyttäen hyväksi LDAP-protokollaa. Lisäksi eri käyttäjätunnuksilla tuli olla erilaiset käyttöoikeudet ja tiedonsiirron piti olla suojattu vakoilu- ja hakkerointiyrityksiltä. Työn tilasi Lännen Puhelin Oy loppuvuodesta 2006. Heinäkuussa 2007 Lännen Puhelin Oy yhdistyi muiden Finnet Oy:n valtakunnallisten liiketoimintojen kanssa, minkä seurauksena tapahtui nimenmuutos Lännen Puhelin Oy:stä DNA Oy:ksi. Lännen Puhelimen toivomuksiin kuului eri käyttöjärjestelmien yhteensopivuus tulevan autentikointipalvelimen kanssa. Työssä tutkittaviin käyttöjärjestelmiin kuuluivat mm. eri Windows-versiot, Linux, Solaris ja Radius-tuki Ciscon laitteille. Työtä määritellessä minulle annettiin alla oleva periaatekuva tulevasta verkosta.



Kuva 1. Havainnollistamiskuva tulevan verkon rakenteesta.

Sovimme, että työ suoritetaan Satakunnan ammattikorkeakoulun Tekniikka Rauman itseopiskeluluokan tiloissa ja käytettävät laitteet tulisivat myös koululta. Käytössä oli alun perin kaksi tietokonetta, joista toisessa oli käyttöjärjestelmänä Windows XP ja toi-

nen kone oli Linux-palvelin, jossa käyttöjärjestelmänä oli Fedora Core 6. Myöhemmin tuli käytettäväksi myös kolmas tietokone, jossa oli käyttöjärjestelmänä Windows XP.

Työtilassa toteutettiin pienimuotoinen koeverkko, jossa oli Fedora Core 6 -pohjainen palvelin ja Windows XP -asiakaskone. Tässä vaiheessa tavoitteena ei ollut kirjautua Windows-järjestelmän kautta sisälle käyttäen LDAPia, joten käyttöjärjestelmäksi asennettiin Windows XP:n tilalle Debian 3.1r4:n (Debian Sarge) ja Fedora Core 6 toimi palvelimena, jossa pyöri OpenLDAP-niminen ohjelmisto. Kun tämä järjestely alkoi toimia, myös palvelinkoneeseen asennettiin Debian Sarge.

Työn edetessä selvisi, että etsittäessä tietoa ja apuja Linuxin käyttöönottamiseen ja ylläpitämiseen, on Internet korvaamaton tiedonlähde. Siksi suurin osa lähdemateriaalista onkin peräisin eri Internet-sivustoilta.

2 LDAP

Lightweight Directory Access Protocol, LDAP, perustuu vuonna 1988 syntyneeseen X.500-standardiin. X.500 on raskas ja monimutkainen protokolla, joka keskustelee OSI-pinon yli verkossa. Koska tämä standardi oli niin raskas, siitä kehitettiin kevyempi versio, LDAP, jotta hakemistopalvelut saataisiin laajempaan käyttöön. Ensimmäinen versio LDAP:sta näki päivänvalon vuonna 1993 Michiganin yliopistossa. Nykyään käytössä oleva versio LDAP:sta on LDAPv2, joka on kuvattu maaliskuussa 1995 kehitetyssä RFC 1777:ssa. Toinen nimitys tälle protokollalle on X.500 Lite, mutta nimitystä ei yleisesti ottaen käytetä paljoakaan. (Tietoliikenneohjelmistojen ja Multimedian Laboratorio 1997.)

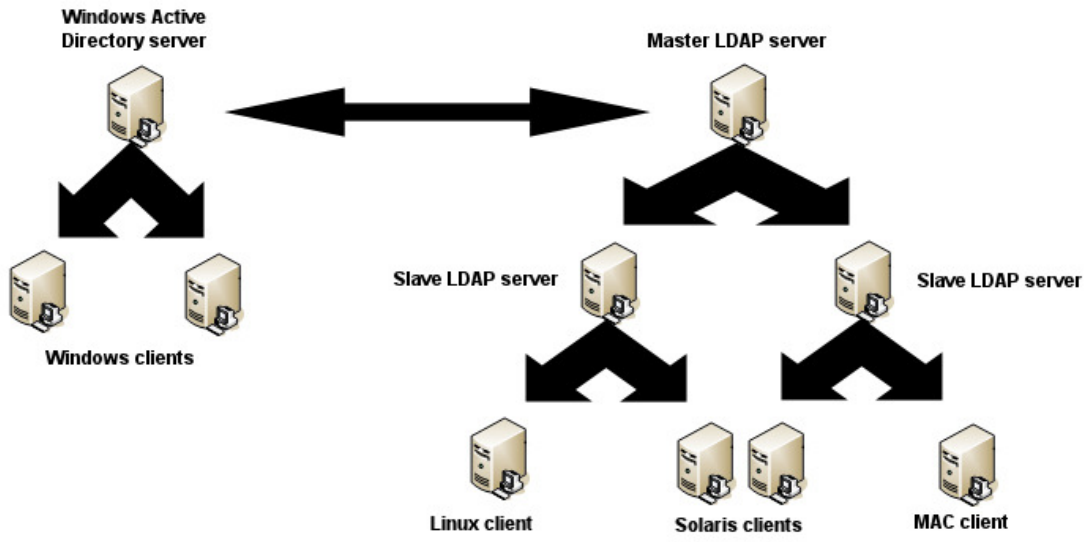
LDAP on siis X.500-standardia kevyempi ja yksinkertaisempi hakemistopalvelu, ja sen keveys perustuu mm. siihen, että se kulkee suoraan TCP-protokollan päällä ja tarjoaa vain tärkeimmät X.500:n palvelut: *bind*, *unbind*, *search*, *modify*, *add*, *delete* ja *abandon*. LDAP-palvelimia on yleensä useita, ja nämä palvelimet muodostavat hierarkian, jossa yksi palvelin on ns. isäntäpalvelin, joka voi muokata alemman tason palvelinten hake-

mistorakennetta. Yhteys palvelinten ja asiakkaiden välillä on perusasetuksilla suojaamaton, joten yhteys kannattaa rakentaa käyttäen esimerkiksi SSL-salausta, mitä tässäkin projektissa on käytetty palvelimen ja Linux-työasemien välillä. Taulukossa on tärkeimmät X.500:ssa käytetyt palvelut ja lyhyet kuvaukset niistä.

Taulukko 1. LDAP:n palveluja.

Komento	Toiminto
Bind	Yhteyden avaukseen
Unbind	Yhteyden lopetukseen
Search	Hakujen suorittamiseen
Modify	Tietueen arvojen muuttamiseen
Add	Tietueen lisäämiseen
Delete	Tietueen poistamiseen
Compare	Arvojen vertailuun
Abandon	Haun keskeyttämiseen

LDAPia käytetään usein ”virtuaalisena puhelinluettelona”, jolloin se toimii verkon käyttäjille niin, että nämä voivat selata toistensa tärkeimpiä tietoja. LDAP on kuitenkin paljon monipuolisempi, sillä käyttäjät voivat selata tietoja verkon yli useilta LDAP-palvelimilta ympäri maailmaa. LDAP-palvelin voi siis sijaita melkein missä päin maailmaa tahansa ja asiakaskone voi ottaa palvelimeen yhteyden ja esittää sille tiedustelun. Jos käyttäjä haluaa muokata hakemiston tietoja, tällä täytyy olla tarvittavat oikeudet operaatioon, ja palvelinkone tarkistaa käyttäjän oikeudet yhteyttä muodostettaessa. Kuvassa havainnollistetaan, kuinka yksi tai useampi LDAP-palvelin voi palvella usean eri käyttöjärjestelmän asiakaskoneita.



Kuva 2. LDAP-palvelimet voivat palvella käyttäjiä useilta eri käyttöjärjestelmiltä.

2.1 LDAPin hyvät puolet

LDAPin hyvät puolet tulevat esille, kun esimerkiksi yrityksen hakemistotietokanta halutaan keskittää yhdelle palvelimelle niin, että kaikkien käyttöjärjestelmien käyttäjätunnukset ja salasanat sijaitsevat yhdessä paikassa. Verrattuna vanhempaan DAP-standardiin (X.500), on LDAP paljon kevyempi ja vaatii palvelimelta ja verkolta vähemmän tehoa ja siksi LDAP onkin yleistynyt käytössä paljon DAPia enemmän. LDAP-palvelimeksi voidaan siis sijoittaa hieman vanhempikin kone ilman että suorituskyky siitä kärsii.

2.2 LDAP-sovelluksia

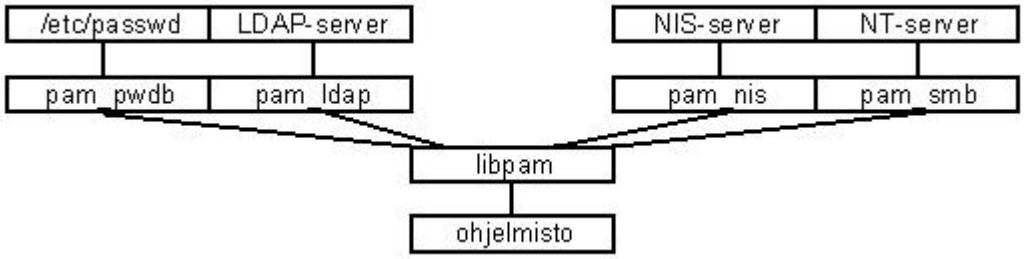
LDAP on hyvin monikäyttöinen protokolla ja se onkin melko yleisesti käytössä monissa eri tehtävissä. Käyttämällä PAM-moduuleita LDAPia voidaan käyttää autentikointiprotokollana. Cisco ja Microsoft ovat yhteistyössä kehittäneet laajennuksen LDAPiin, jonka avulla tiedon replikointi verkossa on helpottunut huomattavasti. Ehkä tunnetuin LDAP-sovellus on kuitenkin Microsoftin Active Directory, joka toimii valtaosassa käyttäjien tietokoneita, joissa on käytössä Windows-käyttöjärjestelmä. (Red Hat Documentation 2006.)

2.3 Käyttäjätilit Linuxissa

Linux käyttää käyttäjätiliensä hallintaan pääasiassa kahta työkalua: PAM- ja NSS -moduuleita (Pluggable Authentication Module / Name Service Switch). Näistä kahdesta tärkeämpi moduuli on PAM. Se antaa järjestelmälle tiedon siitä, kirjautuuko käyttäjä sisälle ja kertoo myös hieman tämän oikeuksista. NSS sisältää yleisimpiä tietoja, joita käyttöjärjestelmä tarvitsee. PAM ja NSS käsitellään tarkemmin jäljempänä. (The Linux Kernel Archives 2007.)

3 PAM (PLUGGABLE AUTHENTICATION MODULE)

PAM on kokoelma kirjastoja, joiden avulla pääkäyttäjä voi määritellä, kuinka ohjelmat tunnistavat käyttäjän. PAM on siitä kätevä järjestelmä, että sen avulla voi tehdä järjestelmään kirjautumiseen liittyviä muutoksia niin, ettei jokaiseen kirjautumista vaativaan ohjelmaan tarvitse erikseen tehdä uusia asetuksia. Se siis hoitaa ohjelman puolesta käyttäjän tunnistamisen, ja kirjautumismenetelmän muuttamiseksi pitää vain määritellä toinen PAM-moduuli käyttöön. Kuvasta näkyy, kuinka ohjelmisto valitsee oikean kirjaston, jota käyttämällä tarvittava tieto löytyy.



Kuva 3. Ohjelmisto ottaa tarvitsemansa tiedot sopivan PAM-moduulin kautta.

Kun Linux oli vielä lapsenkengissä, käyttäjätunnistus tapahtui yksinkertaisesti tarkistamalla käyttäjän salasana /etc/password -tiedostosta. Tämä oli suhteellisen epäluotettava tapa tunnistaa käyttäjät, sillä salasanatiedosto oli helppo paikallistaa ja sieltä sai kaapattua käyttäjien salasanat. PAMia käytettäessä salasana tallennetaan /etc/shadows -tiedostoon ”shadow password”-muodossa ja vain järjestelmän pääkäyttäjällä on oikeus tähän tiedostoon. (Smith 2005, 419.)

Tässä työssä kirjautuminen tulee toteuttaa useiden käyttöjärjestelmien välillä. Tällöin kirjautumisen yhteydessä tulee siis määritellä, mitä PAM-moduulia käytetään. Esimerkiksi Solaris- ja Radius -järjestelmille ovat omat moduulinsa käyttäjätunnistusta varten.

3.1 PAMin asetukset

Käytettäessä PAMia autentikoinnissa tulee joitakin tiedostoja muokata sopivanlaisiksi. Näitä tiedostoja löytyy Debianissa /etc/pam.d –hakemistosta, ja tässä työssä muokattuja

tiedostoja ovat *common-account*, *common-auth* ja *common-password*. Näiden tiedostojen muokkaamista käsitellään tarkemmin luvussa 8.

3.2 PAM-moduuleja

pam_cracklib.so on moduuli, joka tarkistaa salasanan vahvuuden ja turvallisuuden. Moduuli käyttää libcrack-koodia, kun se testaa, onko salasana liian helposti murrettavissa tai onko yhtäläisyyksiä vanhaan salasanaan liian paljon. Sanasto löytyy /usr/lib/cracklib_dict -tiedostosta. (Linux Devcenter 2001a.)

pam_env.so on moduuli, joka mahdollistaa ympäristömuuttujien lisäämisen tai poistamisen sisäänkirjautumista varten. Moduulin asetukset löytyvät tiedostosta /etc/security/pam_env.conf.

pam_limits.so on moduuli, jonka avulla pääkäyttäjä voi määritellä rajoituksia eri käyttäjille määritellyille resursseille, kuten muistinkäyttö ja prosessoriaika. Asetukset löytyvät tiedostosta /etc/security/limits.conf.

pam_unix.so on moduuli, joka toteuttaa perinteisen unix-kirjautumisen, salasanojen käytön ja käyttäjien luomisen. Se käyttää salasanatiedostoja /etc/passwd ja /etc/shadow.
pam_deny.so on moduuli, joka estää pääsyn ohjelmaan. Se voi estää käyttäjää kirjautumasta sisään tai vaihtamasta salasanaansa. (Linux Devcenter 2001b.)

pam_ldap.so on moduuli, joka ohjaa kahta muuta moduulia: autentikointia ja salasananhallintaa. pam_ldap.so.1 ja pam_unix.so.1 -moduuleita käytetään toistensa yhteydessä, jolloin unix-osapuoli tukee normaalia unix-autentikointia ja ldap-osapuoli tukee normaalia vahvempia mekanismeja, kuten CRAM-MD5-salausta.

pam_localuser.so on moduuli, jonka avulla saadaan koneeseen sekä paikalliset ja verkkokirjautumiset. Käyttämällä pam_localuser.so, pam_wheel.so tai pam_listfile-moduuleita, saadaan kirjautuvat käyttäjät rajoitettua helposti joko paikallisiin tai verkon kautta kirjautuviin käyttäjiin. (About.com: Focus on Linux 2004.)

pam_mount.so on moduuli, joka hoitaa SMB-palvelinten välistä yhteyttä. Sen avulla saadaan käyttöön näiden palvelinten tarjoama kiintolevytila Unix (Linux)-työasemilla.

pam_smb.so-moduulin avulla voidaan autentikoitua erilliseen SMB-palvelimeen ja käyttää hyväksi esimerkiksi sen tulostus- ja levypalveluita.

4 NSS (NAME SERVICE SWITCH)

Name Service Switch eli NSS korvaa monet Unixin asetustiedostot, kuten /etc/password, /etc/group ja /etc/hosts, keskitetyllä tietokannalla. Tällainen tietokanta on esimerkiksi Windowsin Active Directory. NSS selvittää kirjastoistaan käyttäjien ID:t, käyttäjänimet, ym. Näiden kirjastojen avulla esimerkiksi LDAP:n käyttö on läpinäkyvää niille ohjelmille, jotka käyttävät sitä. NSS toimii siis sovellusten ja tietokannan välissä, ja välittää sieltä tiedon sovelluksille. (BeezNest 2005.)

4.1 PAM ja NSS käytettäessä LDAP-protokollaa

Käytettäessä LDAPia hyväksi käyttäjätunnistuksessa pitää edellä mainitut PAM ja NSS-tiedostot muokata sellaisiksi, että ne osaavat hakea tiedot LDAP-protokollan kautta. LDAP-moduulit, joita käytetään, ovat pam_ldap ja nss_ldap. PAM- ja NSS-moduulit kutsuvat näitä moduuleita, kun LDAP on käytössä.

4.2 NSS-moduulin konfigurointi

Name Service Switch määritellään tekemällä muutoksia /etc/nsswitch.conf -tiedostoon. NSS:lle tulee kertoa, mistä hakea tarvittavat tiedot, joten muutoksia tehdään passwd, group ja shadow -kohtiin. Jotta paikallinen kirjautuminen olisi mahdollista, tulee ensin määritellä näihin kohtiin ”files” ja vasta sitten ”ldap”, jolloin NSS hakee ensin käyttäjää paikallisista lähteistä, ja jos sieltä ei käyttäjää löydy, se etsii tiedot LDAPin yli. Jos LDAP määritellään ensin, on edessä ongelmia, jos verkkoyhteys on poikki tai LDAP-

palvelin ei ole toiminnassa. Siksi kannattaa ensisijaisesti hakea tiedot paikallisista tiedostoista.
Esimerkki nsswitch.conf -tiedoston syntaksista:

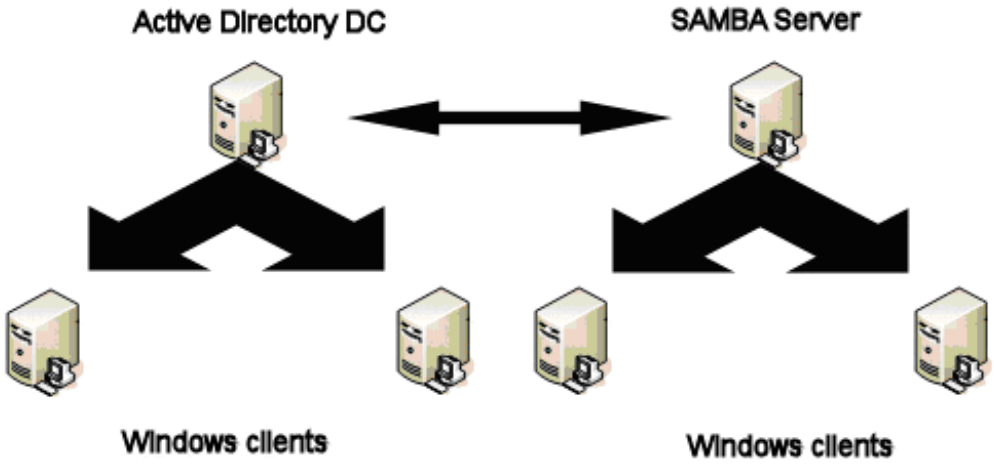
```
passwd:     files ldap compat
group:      files ldap compat
shadow:     files ldap compat
```

Enemmän asetuksista kerrotaan luvussa 7, jossa määritellään testikokoonpanon asetukset tarkemmin.

5 SAMBA

SAMBA on toteutus, jonka tarkoituksena on saada Windows- ja Unix-pohjaiset käyttöjärjestelmät sulaan sopuun keskenään. Windows ja muut käyttöjärjestelmät eivät ole keskenään kovinkaan yhteen sopivia, joten tähän tarkoitukseen kehitettiin SAMBA. Se toimii niin, että tietokoneen käyttäjän ei tarvitse tietää, mikä käyttöjärjestelmä palvelinkoneessa (tai työasemassa) on, vaan se yhdistää näitä käyttöjärjestelmiä läpinäkyvänä komponenttina taustalla. SAMBA toimii Unix-pohjaisissa tietokoneissa, tässä tapauksessa Debian Linuxin päällä, ja vaihtaa tietoja Windows-käyttöjärjestelmällisten tietokoneiden kanssa. Sen avulla Unix-käyttäjät pääsevät Windowsin verkkoon kiinni ilman sen suurempia ongelmia ja Windows-käyttäjät taas voivat käyttää Unix-palvelimen tarjoamia tiedosto- ja tulostinpalveluita normaalisti, kuin käytettävä resurssi olisi toisella Windows-työasemalla.

SAMBA toimii käyttäen CIFS- eli Common Internet File System -protokollaa, joka perustuu Microsoftin Server Message Block- eli SMB-protokollaan. Tästä protokollasta SAMBA on myös saanut nimensä. (Samba 2001.) Kuvassa SAMBA-palvelin toimii yhdessä Active Directory Domain Controllerin kanssa Windows-työasemien käyttäjätietokantana.



Kuva 4. SAMBA:n avulla Linuxista saadaan palvelin myös Windows-käyttäjille.

6 NT-TOIMIALUE

Ennen Active Directory -toimialueita Windows-verkoissa käytettiin NT-toimialueita. Samba-palvelin osaa toimia Domain Controller -koneena NT-toimialueessa, muttei Active Directory -toimialueessa. Siksi tässä työssä käytetään NT-toimialueita. Windows NT -toimialue koostuu tietokoneista, joissa on käyttöjärjestelmänä Microsoft Windows ja joilla on yhteinen keskustietokanta. Täällä tietokannassa sijaitsevat kaikki verkon käyttäjätilit ja tietoturvatiedot, joita toimialueen käyttäjät tarvitsevat. Kaikki toimialueen käyttäjät tarvitsevat oman käyttäjätilinsä tietokantaan, ja tälle tilille voidaan määritellä resurssit, joihin käyttäjällä on käyttöoikeus.

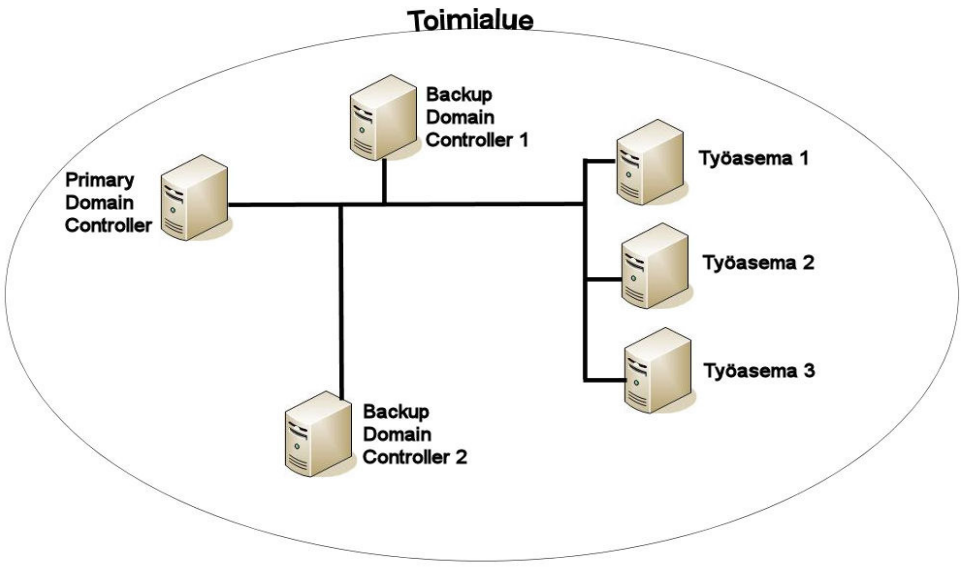
Toimialueessa tietokanta sijaitsee tietokoneilla, jotka on määritelty DC:ksi eli Domain Controllereiksi. Domain Controller on palvelin, joka hoitaa turvallisesti kaiken käyttäjän ja toimialueen välisen tiedonvaihdon, tietoturvan keskittämisen ja toimialueen hallitsemisen. Windows NT -toimialue toimii parhaiten suhteellisen suurissa verkoissa, yrityksten tai järjestöjen toimialueena. (Wikipedia 2007.)

6.1 Windows-työryhmät

Toinen tapa yhdistää verkon käyttäjiä on käyttää Windowsin työryhmiä (Workgroup). Työryhmän tietokoneet ovat irrallaan verkossa, eli verkkoon liittyminen ei vaadi minkäänlaista kirjautumista. Työryhmässä ei ole erillisiä palvelimia ja työasemia, vaan se toimii Peer-to-Peer-periaatteella. Työryhmät ovat vaikeita hallita, jos niissä on paljon käyttäjiä, eivätkä ne ole erityisen hyviä tietoturvan kannalta. Windowsin työryhmät sopivatkin parhaiten pieniin verkkoihin tai kotitoimiston tarpeisiin.

6.2 Toimialueen ominaisuuksia

Toimialue ei vaadi mitään erityistä verkkorakennetta tai -asetuksia, vaan siihen liittyneet tietokoneet voivat yhtä hyvin olla joko osa samaa verkkoa tai sijaita eri puolella maailmaa. Hyviä puolia tietokoneiden liittämiseen toisiinsa toimialueella ovat mm. keskitetty hallinto ja hyvä laajenemisvara. Keskitetyllä hallinnalla koko toimialueen asetuksia voidaan hallita yhteydellä yksittäiseen tietokantaan ja verkon resurssit voidaan määritellä niin, että käyttäjän oikeudet eri resursseihin tiedetään yhden sisäänkirjautumisen jälkeen. Lisäksi toimialueiden avulla verkoista voidaan luoda erittäin suuria. Haittapuolia ovat nopeasti verkossa leviävät virukset ja tiedostojen tietoturva, jos käyttäjän salasana saadaan selville. Kuvassa on esitetty mahdollinen toimialue ja siinä toimivat tietokoneet ja palvelimet.



Kuva 5. Esimerkki toimialueen palvelimista ja työasemista.

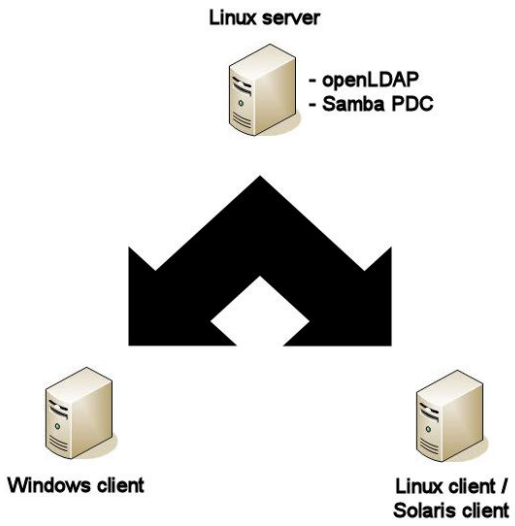
6.3 Domain Controller

Domain Controller, DC, on palvelin, joka Windows-toimialueella vastaa tietoturvaa vaativista pyynnöistä, kuten sisäänkirjautuminen ja käyttöoikeuksien tiedustelu. Windows NT:ssä keskuspalvelimena toimii PDC (Primary Domain Controller), joita voi olla vain yksi kappale. Kaikki muut DC:t ovat BDC:itä (Backup Domain Controller).

PDC sisältää "pääkopion" tietokannasta, josta löytyvät kaikki käyttäjätiedot. BDC:stä löytyy kopio tästä tietokannasta, mutta tiedosto on vain-luku-muotoa. Ainoastaan PDC pystyy siis muokkaamaan käyttäjätietoja, ja muokatut tiedostot vain kopioituvat luettavaksi BDC:hin. PDC kopioi tietokantaa BDC:ille tietyin väliajoin, ja nämä toimivat varmuuskopioina PDC:stä. BDC voi myös toimia autentikaatiopalvelimena käyttäjän kirjautuessa sisään, ja jos PDC jostain syystä kaatuu, se voi ottaa itselleen PDC:n roolin pääpalvelimena pääkäyttäjän näin määritellessä.

7 PALVELIN JA TYÖASEMAT

Käyttöön annettiin kolme tietokonetta, joiden avulla luotiin pieni testiverkko, jossa testattiin eri käyttöjärjestelmiä ja asetuksia. Lopuksi kahdella koneella pyöri Debian Sarge -Linux ja yhdellä Windows XP. Ensimmäiseksi luotiin tilanne, jossa toinen Linux-kone toimi palvelimena ja toinen työasemana. Työasemalla kirjauduttiin sisään käyttämällä palvelimella sijaitsevaa käyttäjänimeä LDAP-protokollan yli. Kolmas tietokone toimi myös työasemana, jossa Windows XP -työasema määritellään käyttämään palvelimelle luotua toimialuetta ja tätä kautta kirjautumaan sisälle Windowsiin käyttäen palvelimella sijaitsevia käyttäjätietoja. Kuvassa näkyy yksinkertaistettuna työssä käytetyn testiverkon rakenne.



Kuva 6. Käytetyn testiverkon yksinkertaistettu rakenne.

7.1 Palvelinasetukset Linux-työasemaa varten

Palvelimella toimi käyttöjärjestelmänä Debian Sarge. Sen asennus on tehty helpoksi ja mitään suurempia ongelmia ei syntynytkään, lukuun ottamatta pieniä yhteensopivuusongelmia näytönohjaimen ajureiden kanssa, jotka onneksi saatiin ratkaistuksi.

Ensimmäinen askel projektissa oli asentaa tarvittavat ohjelmistot, joita olivat mm. slapd ja ldap-utils. Pidin Debianin ominaisuudesta, että asennuksen yhteydessä asennusohjelma (apt-get) kysyy keskeisimmät asetukset käyttäjältä, jolloin asennusoperaatio nopeutuu ja helpottuu huomattavasti. Esimerkiksi OpenLDAP-ohjelmistoa asennettaessa asennusohjelma kysyy mm. DNS-toimialueen nimeä, organisaation nimeä sekä muitakin tärkeimpiä asetuksia.

Esimerkki 1:ssä näkyy slapd:n asennuksen kysymät tärkeimmät tiedot, jonka perusteella asennusohjelma luo toimivan asetustiedoston slapd.conf.

```
Omit OpenLDAP server configuration? no
DNS domain name: example.org
Name of your organization: example_organization
Admin password: ldap
Database backend to use: BDB
Do you want your database to be removed when slapd is purged? no
Allow LDAPv2 protocol? no
```

Esimerkki 1. slapd:n asennuksen yhteydessä kysytyt tiedot.

Kun OpenLDAP oli asennettu, sen toimivuus testattiin yksinkertaisesti tiedustelemalla sen tietokantaa komennolla *ldapsearch*. Tietokannasta löytyivät luonnollisesti tässä vaiheessa vain ohjelman omat tiedot.

Seuraavaksi palvelimelle piti saada käyttäjiä, jotta työasemakoneelle pääsisi kirjautumaan niitä käyttäen. LDAP:ssa tietokanta on hierarkkinen ja käyttäjät asetellaan eri ryhmiin, joten nämä tuli myös luoda tässä vaiheessa. Vielä tässä vaiheessa lähes kaikki asetukset tehtiin tekstipohjaisena, jolloin käyttäjät, ryhmät ja muut tiedot lisätään tietokantaan luomalla .ldif-päätteisiä tiedostoja, joista tiedot luetaan tietokantaan. Tiedot .ldif-tiedostoista lisätään tietokantaan komennolla *ldapadd*. Tietokantaan lisättiin People ja Group -nimiset OU:t (Organizational Unit) base.ldif-tiedostosta komennolla:

```
ldapadd –x –D ”cn=admin,dc=example,dc=org” –W –f base.ldif
```

Tässä admin on pääkäyttäjä ja example.org on testausmielessä annettu nimi toimialueelle. Äsken luotuihin Organizational Uniteihin luotiin samalla tavalla käyttäjäryhmä ldapusers Group-OU:iin. Tänne käyttäjäryhmään tulee itse käyttäjien tiedot, jotka luotiin seuraavaksi. Testikäyttäjän nimeksi annoin ”nursi”. Näillä asetuksilla palvelin oli kyllä toimiva, mutta tietoturva oli vielä turhan heikko, koska kaikki tieto verkossa siirtyi tekstimuodossa ilman mitään suojauksia. Tämän vuoksi käyttöön otettiin Secure Sockets Layer (SSL) -salaus, jolloin kaikki LDAP:in tiedot tunneloidaan SSL-salausta hyväksikäyttäen portin 636 kautta.

Esimerkki 2:ssä lisätään käyttäjä tietokantaan. Siinä määritellään käyttäjän nimi, ryhmä ja muut asetukset. Tiedoston sisältö lisätään tietokantaan komennolla *ldapadd*.

```
dn: cn=nursi,ou=People,dc=example,dc=org
cn: Myuser
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
sn: User
uid: myuser
uidNumber: 1025
gidNumber: 9000
homeDirectory: /tmp
```

Esimerkki 2. Käyttäjän luomiseen tarvittava .ldif -tiedosto.

Esimerkki 3:ssa on asetustiedoston slapd.conf kohdat, joihin tehtiin muutoksia SSL-salauksen käyttöönottamiseksi. Siinä määritellään tarvittavien avainten sijainnit.

```
TLSCACertificateFile      /etc/ldap/cacert.pem
TLSCertificateFile        /etc/ldap/servercrt.pem
TLSCertificateKeyFile     /etc/ldap/serverkey.pem
```

Esimerkki 3. slapd.conf-tiedostoon tehdyt muutokset.

SSL-salauksen käyttöönottamiseksi tietokoneelle asennettiin openssl-ohjelmisto. SSL:n tietoturva perustuu salaisiin ja julkisiin avaimiin, jotka täytyy luoda palvelimelle. Avaimia luotaessa täytyy olla hyvin tarkka, että kaikki tiedot tulevat jokaiseen avaimeen täysin samalla tavalla, koska muuten avainpari ei toimi. Kun avainparit on luotu, pitää salauksen käyttöönotto kertoa myös OpenLDAP:lle. Tämä tapahtuu lisäämällä slapd.conf -tiedostoon määrittelyt avainten sijainneista.

7.2 Palvelinasetukset Windows XP -työasemaa varten

Jotta palvelin osaisi palvella myös Windows XP -käyttäjiä, tuli koneelle asentaa Samba ja muut tarvittavat työkalut. Palvelimesta tehdään siis Samba PDC, Primary Domain Controller, jonka toimialueeseen Windows-käyttäjät (tai Linux-käyttäjät Samban kautta) liittyvät.

Apt-get-komentoa käyttämällä haettiin Samban paketit ja asennuksen yhteydessä asennusohjelma kysyy taas tuttuun tapaan tärkeimpiä asetuksia, mm. toimialueen nimeä, salasanan salaamista ja WINS-asetuksia. Jotta Samba toimisi mukavasti OpenLDAP:n kanssa yhteen, tulee OpenLDAP:n asetuksiin lisätä Samban schema, joka lisää tietokantaan sen tarvitsemia kohtia.

Samban asetukset tehdään lähinnä /etc/samba/ -hakemistossa sijaitsevaan smb.conf -tiedostoon. Tähän tiedostoon tulee määritellä myös LDAP-asetuksia, kuten machine, user ja group -OU:t ja LDAP:n pääkäyttäjä, admin. Lisäksi Samballe kerrotaan myös tietysti LDAP-osoite, tässä tapauksessa nursildap.com.

Esimerkki 4. Palvelimen smb.conf -tiedostoon tehtyjä muutoksia, joilla määritellään tärkeimmät tarvittavat asetukset ja pääkäyttäjä.

```
workgroup = ldapsrv
passdb backend = ldapsam:ldap://127.0.0.1
ldap suffix = dc=nursildap,dc=com
ldap machine suffix = ou=machines
ldap user suffix = ou=users
ldap group suffix = ou=groups
ldap admin dn = cn=admin,dc=nursildap,dc=com
ldap delete dn = no
add machine script =  /usr/local/smbldaptools/smbldap-useradd -w "%u"
ldap password sync = yes
enable privileges = yes
```

Esimerkki 4. smb.conf -tiedoston tärkeimmät muutokset.

Samballe tulee myös luoda pääkäyttäjän salasana, kuten myös OpenLDAP:ssa tehtiin. Komento, jolla tämä onnistuu, on *smbpasswd*. Käyttäjien luominen onnistuu joko manuaalisesti käyttämällä vaikkapa komentoja *groupadd*, *adduser, smbpasswd*… jne., mutta koska tarkoitusta varten on kehitetty myös erillisiä ohjelmia, on helpompaa luoda tietokanta niiden avulla.

Phpldapadmin on käyttäjien ja ryhmien luomiseen tarkoitettu ohjelma, ja se toimii selaimessa ja tukee myös salattua yhteyttä. Sitä käyttämällä saa helposti ja kätevästi luotua tarvittavat asetukset Samba-käyttäjille. Ensimmäinen vaihe käyttäjien luomisessa tietokantaan Phpldapadminia käyttäen on luoda tarvittavat OU:t käyttäjiä, ryhmiä ja konenimiä varten. Kun toimialuetta käytetään, pitää Primary Domain Controllerille kertoa tietokoneet, joilla on oikeus liittyä toimialueeseen. Konenimet voidaan lisätä manuaalisesti ilman scripteja tai sitten niitä käyttäen. Koska käytössä oli vain pieni testiverkko, asennettiin Windows-koneen nimi manuaalisesti, jolloin kirjaxp-konenimi lisättiin ”machines” OU:iin. Jälkeenpäin määriteltiin smb.conf -tiedostoon koneiden lisääminen automaattisesti scriptien (mm. perl ja smbldap-useradd) avulla. Koneille tulee myös määritellä henkilökohtainen UID (User ID), samoin kuin käyttäjille. Nämä numeroinnit kannattaa ajatella jo etukäteen järkevästi, että UID:n tunnistaa helposti jälkeenpäin oikeanlaiseksi. Projektissa käyttäjien numerointi aloitettiin 10000:sta ja koneiden 30000:sta ylöspäin. Käyttäjät lisätään ”users” -OU:iin ja heille kannattaa myös luoda kotihakemisto, jonne Windowsin asetukset ja käyttäjän tiedostot tallentuvat. Tämän vaiheen unohtaminen tuotti virheilmoituksia kirjautumisen yhteydessä, mutta ei estänyt

käyttäjää kirjautumasta sisälle (asetukset ja tiedostot luonnollisesti menetetään ilman kotihakemistoa uloskirjautumisen yhteydessä.). Käyttäjän hakemisto luotiin /home/ -hakemistoon *mkdir*-käskyllä ja sinne kopioitiin /etc/skel/ -hakemistosta tarvittavat tiedostot, joita uusi käyttäjä tarvitsee. Lisäksi vielä hakemistolle tulee antaa omistajaksi käyttäjätunnuksen omistaja komennolla *chown -R käyttäjätunnus /home/käyttäjätunnus* ja sille tulee määritellä oikea ryhmä (OU) komennolla *chgrp -R users /home/käyttäjätunnus*.

7.3 Linux-työaseman asetukset

Linux-työasemassa oli käyttöjärjestelmänä Debian Sarge, kuten myös palvelimessa, joten sen asetusten saaminen kohdilleen ei ollut enää niin suuri ongelma. Työasemaan tuli asentaa myös OpenLDAP, LDAP:n PAM-moduulit ja NSCD eli Name Service Cache Daemon. Asennettaessa asennusohjelma kysyi taas tärkeimmät asetukset, libnss-ldap-pakettia asennettaessa määritellään LDAP-palvelimen osoite ja muut tiedot, samoin kuin PAM-moduulia eli libpam-ldap-pakettia asennettaessa.

Kuten palvelimessakin, tuli työasemalle määritellä NSS:lle, mistä tarvittavat tiedot haetaan. Nämä määrittelyt tehdään /etc/-hakemistossa sijaitsevaan nsswitch.conf-tiedostoon ja passwd, group ja shadow -kohtiin lisätään ”files ldap”, jolloin tiedot haetaan ensin paikallisista tiedostoista, jonka jälkeen vasta LDAP:ia käyttäen. Näin vältetään tietojen haku turhaan ensin LDAP:n yli, jos halutaan kirjautua vain paikallisesti.
Myös hakemiston /etc/pam.d tiedostoihin tuli tehdä muutoksia, ja common-account, common-auth ja common-password -tiedostoihin lisättiin tiedot LDAP:n PAM-moduuleista. Näin järjestelmä osaa tulkita LDAP:n kautta tapahtuvan autentikaation ohjelman näin tehdessä.

Esimerkki 5:ssä on lisätty nsswitch.conf -tiedoston passwd, group ja shadow -kohtiin tarvittavat muutokset, että tiedot haettaisiin oikeasta paikasta.

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap
```

Esimerkki 5. nsswitch.conf -tiedoston muutokset.

Viimeiseksi muutoksia tehtiin myös /etc/ldap/-hakemistossa sijaitsevaan ldap.conf -tiedostoon. Tänne lisättiin tässä vaiheessa vain palvelimen tiedot. Kun vielä NSCD tuli käynnistettyä uudelleen, LDAP-palvelimen ja työaseman yhteistyö tuli testattua onnistuneesti vaihtamalla työasemalta käyttäjän salasanan. Tämän jälkeen myös kirjautuminen työasemalle onnistui käyttäen palvelimella sijaitsevaa käyttäjänimeä ”nursi”.
Tässä vaiheessa kirjautuminen kyllä onnistui, mutta käyttäjänimi ja salasana siirtyivät verkon yli selväkielisenä, joten pätevän hakkerin olisi helppo kaapata myös pääkäyttäjän salasana. Ratkaisu tähän ongelmaan on SSL-salauksen käyttäminen tietoja siirrettäessä. SSL-salausta käytettäessä tuli vastaan pieni ongelma, eli salausavaimen tiedoissa pitää olla palvelimen nimi, ei IP-osoitetta. Tämä on ongelma siksi, että example.org-nimi oli tarkoitettu vain testikäyttöön ja sitä käytettäessä haetaan väärää IP-osoitetta. Ongelma kierrettiin (väliaikaisesti) lisäämällä example.org:n työaseman hosts-listaan, jolloin nimen IP-osoitetta ei lähdetä kyselemään palvelimelta, vaan ohjataan sokeasti määriteltyyn osoitteeseen.

Salauksen käyttöönotto tapahtuu määrittelemällä se LDAP-asetuksiin ja ldap.conf -tiedostoon tulikin muutoksena URI-kohdan osoitteen muuttaminen ldaps:// -muotoon ldap:// sijaan ja TLS_REQCERT allow –kohdan lisääminen, jolloin työasema pyytää palvelimen sertifikaattia, eikä sitä tarvitse lisätä jokaiseen työasemaan erikseen.

Esimerkki 6. ldap.conf -tiedostoon tehtiin muutokset niin, että palvelin löytyy sieltä ja liikenne palvelimen ja työaseman välillä on SSL-salattua.

```
BASE    dc=example,dc=org
URI     ldaps://example.org
TLS_REQCERT allow
```

Esimerkki 6. ldap.conf -tiedoston muutokset.

Myös libnss-ldap.conf ja pam_ldap.conf -tiedostoihin tuli lisätä ldaps:// kertomaan, että käytetään salattua yhteyttä ja eri porttia. Näiden muutosten jälkeen olikin taas aika käynnistää NSCD uudelleen ja testata yhteyttä. Testaus tapahtui yksinkertaisesti tiedustelemalla palvelimen tietokantaa *ldapsearch*-komennolla. Kun testaamalla tuli todettua,

että molemmat, suojaamaton ja suojattu yhteys toimivat, oli aika kirjautua sisälle käyttäen juuri määriteltyä suojattua yhteyttä.

7.4 Windows XP -työaseman asetukset

Windows-työaseman määrittelyt oli hyvin helppo tehdä. Koska palvelimella pyöri Samba moitteettomasti, käytännössä ainoa asia, joka työasemalle tuli määritellä, oli toimialue. Kun konetta lisätään toimialueelle, kysytään toimialueen salasanaa, jonka antamalla saatiin myös Windows-työasema toimimaan normaalisti, eli kirjauduttaessa sisälle oikean toimialueen ollessa käytössä Windows osaa hakea Samba PDC -palvelimelta käyttäjän tiedot ja kirjautuu sisälle normaalisti.

8 PALVELIMEN JA TYÖASEMIEN ASETUKSET

8.1 Palvelimen asetukset

Palvelimella tehtiin tarvittavien ohjelmien asennuksen jälkeen muutoksia muutamiin tiedostoihin, ja näitä tiedostoja olivat mm. slapd.conf, nsswitch.conf ja smb.conf. Slapd.conf on siis OpenLDAP-asetustiedosto, joka määrää itse LDAP-palvelimen toiminnot ja asetukset, nsswitch.conf-tiedostossa kerrotaan järjestelmälle, mistä etsiä käyttäjätietoja, ja smb.conf-tiedostossa on asetukset samballe.

8.1.1 slapd.conf

```
# This is the main slapd configuration file. See slapd.conf(5) for
more
# info on the configuration options.

########################################################################
#
# Global Directives:

# Features to permit
#allow bind_v2

# Schema and objectClass definitions
```

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include              /etc/ldap/schema/samba.schema

# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck     on

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile         /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile        /var/run/slapd.args

# Read slapd.conf(5) for possible values
loglevel        256

# Where the dynamically loaded modules are stored
modulepath /usr/lib/ldap
moduleload back_bdb

#######################################################################
#
# Specific Backend Directives for bdb:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend              bdb
checkpoint 512 30

#######################################################################
#
# Specific Backend Directives for 'other':
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
#backend             <other>

#######################################################################
#
# Specific Directives for database #1, of type bdb:
# Database specific directives apply to this databasse until another
# 'database' directive occurs
database        bdb

# The base of your directory in database #1
suffix          "dc=example,dc=org"

# Where the database file are physically stored for database #1
directory       "/var/lib/ldap"

# Indexing options for database #1
index           objectClass eq

# Save the time that the entry gets modified, for database #1
lastmod         on

# Where to store the replica logs for database #1
# replogfile          /var/lib/ldap/replog
```

```
# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
access to attrs=userPassword
        by dn="cn=admin,dc=example,dc=org" write
        by anonymous auth
        by self write
        by * none

# Ensure read access to the base for things like
# supportedSASLMechanisms.  Without this you may
# have problems with SASL not knowing what
# mechanisms are available and the like.
# Note that this is covered by the 'access to *'
# ACL below too but if you change that as people
# are wont to do you'll still need this if you
# want SASL (and possible other things) to work
# happily.
access to dn.base="" by * read

# The admin dn has full write access, everyone else
# can read everything.
access to *
        by dn="cn=admin,dc=example,dc=org" write
        by * read

# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to
#access to dn=".*,ou=Roaming,o=morsnet"
#        by dn="cn=admin,dc=example,dc=org" write
#        by dnattr=owner write

#######################################################################
#
# Specific Directives for database #2, of type 'other' (can be bdb
too):
# Database specific directives apply to this databasse until another
# 'database' directive occurs
#database        <other>

# The base of your directory for database #2
#suffix               "dc=debian,dc=org"
# Tähän lisäys SSL -salauksen käyttöönottamiseksi
TLSCACertificateFile  /etc/ldap/cacert.pem
TLSCertificateFile    /etc/ldap/servercrt.pem
TLSCertificateKeyFile /etc/ldap/serverkey.pem
```

8.1.2 nsswitch.conf

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.
```

```
passwd:         files ldap compat
group:          files ldap compat
shadow:         files ldap compat

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

8.1.3 smb.conf

```
[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will
part of
   workgroup = ldapsrv

# server string is the equivalent of the NT Description field
   server string = %h server (Samba %v)

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable its WINS
Server
;   wins support = no

# WINS Server - Tells the NMBD components of Samba to be a WINS Client
# Note: Samba can be either a WINS Server, or a WINS Client, but NOT
both
;   wins server = w.x.y.z

# This will prevent nmbd to search for NetBIOS names through DNS.
   dns proxy = no

# What naming service and in what order should we use to resolve host
names
# to IP addresses
;   name resolve order = lmhosts host wins bcast


#### Debugging/Accounting ####

# This tells Samba to use a separate log file for each machine
# that connects
   log file = /var/log/samba/log.%m

# Put a capping on the size of the log files (in Kb).
   max log size = 1000

# If you want Samba to only log through syslog then set the following
# parameter to 'yes'.
;   syslog only = no
```

```
# We want Samba to log a minimum amount of information to syslog. Eve-
rything
# should go to /var/log/samba/log.{smbd,nmbd} instead. If you want to
log
# through syslog you should set the following parameter to something
higher.
   syslog = 0

# Do something sensible when Samba crashes: mail the admin a backtrace
   panic action = /usr/share/samba/panic-action %d


####### Authentication #######

# "security = user" is always a good idea. This will require a Unix
account
# in this server for every user accessing the server. See
# /usr/share/doc/samba-doc/htmldocs/ServerType.html in the samba-doc
# package for details.
;   security = user

# You may wish to use password encryption.  See the section on
# 'encrypt passwords' in the smb.conf(5) manpage before enabling.
   encrypt passwords = true

# If you are using encrypted passwords, Samba will need to know what
# password database type you are using.
#   passdb backend = tdbsam guest
   passdb backend = ldapsam:ldap://127.0.0.1
   ldap suffix = dc=nursildap,dc=com
   ldap machine suffix = ou=machines
   ldap user suffix = ou=users
   ldap group suffix = ou=groups
   ldap admin dn = cn=admin,dc=nursildap,dc=com
   ldap delete dn = no
# be a PDC
domain logons = yes
add machine script =  /usr/local/smbldaptools/smbldap-useradd -w "%u"
ldap password sync = yes
#allow user privileges
enable privileges = yes

   obey pam restrictions = yes

;   guest account = nobody
   invalid users = root

# This boolean parameter controls whether Samba attempts to sync the
Unix
# password with the SMB password when the encrypted SMB password in
the
# passdb is changed.
;   unix password sync = no

# For Unix password sync to work on a Debian GNU/Linux system, the
following
# parameters must be set (thanks to Augustin Luton <alu-
ton@hybrigenics.fr> for
# sending the correct chat script for the passwd program in Debian Po-
tato).
```

```
   passwd program = /usr/bin/passwd %u
   passwd chat = *Enter\snew\sUNIX\spassword:* %n\n
*Retype\snew\sUNIX\spassword:* %n\n .

# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
;   pam password change = no


########## Printing ##########

# If you want to automatically load your printer list rather
# than setting them up individually then you'll need this
;   load printers = yes

# lpr(ng) printing. You may wish to override the location of the
# printcap file
;   printing = bsd
;   printcap name = /etc/printcap

# CUPS printing.  See also the cupsaddsmb(8) manpage in the
# cupsys-client package.
;   printing = cups
;   printcap name = cups

# When using [print$], root is implicitly a 'printer admin', but you
can
# also give this right to other users to add drivers and set printer
# properties
;   printer admin = @ntadmin


######## File sharing ########

# Name mangling options
;   preserve case = yes
;   short preserve case = yes


############ Misc ############

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting
;   include = /home/samba/etc/smb.conf.%m

# Most people will find that this option gives better performance.
# See smb.conf(5) and /usr/share/doc/samba-doc/htmldocs/speed.html
# for details
# You may want to add the following on a Linux system:
#         SO_RCVBUF=8192 SO_SNDBUF=8192
   socket options = TCP_NODELAY

# The following parameter is useful only if you have the linpopup
package
# installed. The samba maintainer and the linpopup maintainer are
# working to ease installation and configuration of linpopup and sam-
ba.
;   message command = /bin/sh -c '/usr/bin/linpopup "%f" "%m" %s; rm
%s' &
```

```
# Domain Master specifies Samba to be the Domain Master Browser. If
this
# machine will be configured as a BDC (a secondary logon server), you
# must set this to 'no'; otherwise, the default behavior is recom-
mended.
;   domain master = auto

# Some defaults for winbind (make sure you're not using the ranges
# for something else.)
;   idmap uid = 10000-20000
;   idmap gid = 10000-20000
;   template shell = /bin/bash

#======================= Share Definitions =======================

[homes]
   comment = Home Directories
   browseable = no

# By default, the home directories are exported read-only. Change next
# parameter to 'yes' if you want to be able to write to them.
   writable = no

# File creation mask is set to 0700 for security reasons. If you want
to
# create files with group=rw permissions, set next parameter to 0775.
   create mask = 0700

# Directory creation mask is set to 0700 for security reasons. If you
want to
# create dirs. with group=rw permissions, set next parameter to 0775.
   directory mask = 0700

# Un-comment the following and create the netlogon directory for Do-
main Logons
# (you need to configure Samba to act as a domain controller too.)
;[netlogon]
;   comment = Network Logon Service
;   path = /home/samba/netlogon
;   guest ok = yes
;   writable = no
;   share modes = no

[printers]
   comment = All Printers
   browseable = no
   path = /tmp
   printable = yes
   public = no
   writable = no
   create mode = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/printers
   browseable = yes
   read only = yes
   guest ok = no
```

```
# Uncomment to allow remote administration of Windows print drivers.
# Replace 'ntadmin' with the name of the group your admin users are
# members of.
;   write list = root, @ntadmin

# A sample share for sharing your CD-ROM with others.
;[cdrom]
;   comment = Samba server's CD-ROM
;   writable = no
;   locking = no
;   path = /cdrom
;   public = yes

# The next two parameters show how to auto-mount a CD-ROM when the
#          cdrom share is accesed. For this to work /etc/fstab must
contain
#          an entry like this:
#
#       /dev/scd0   /cdrom  iso9660 defaults,noauto,ro,user   0 0
#
# The CD-ROM gets unmounted automatically after the connection to the
#
# If you don't want to use auto-mounting/unmounting make sure the CD
#          is mounted on /cdrom
#
;   preexec = /bin/mount /cdrom
;   postexec = /bin/umount /cdrom
```

8.2 Linux-työaseman asetukset

Työasema saatettiin toimintakuntoon asentamalla tarvittavat ohjelmistot ja sen jälkeen muokkaamalla niiden asetustiedostoja sopiviksi. Työaseman tärkeimmät muokatut asetustiedostot olivat *nsswitch.conf*, *common-auth*, *common-account*, *common-password* ja *ldap.conf*. slapd.conf:sta asetukset vaihdettiin samanlaisiksi kuin palvelimellakin.

8.2.1 nsswitch.conf

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         files ldap
group:          files ldap
shadow:         files ldap

hosts:          files dns
networks:       files
```

```
protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

8.2.2 common-auth

```
#
# /etc/pam.d/common-auth - authentication settings common to all ser-
vices
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use
the
# traditional Unix authentication mechanisms.
#
#auth      required   pam_unix.so nullok_secure
auth       sufficient pam_ldap.so
auth       required   pam_unix.so nullok_secure use_first_pass
```

8.2.3 common-account

```
#
# /etc/pam.d/common-account - authorization settings common to all
services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authorization modules that define
# the central access policy for use on the system.  The default is to
# only deny service to users whose accounts are expired in
/etc/shadow.
#
#account   required   pam_unix.so
account               sufficient pam_ldap.so
account               required   pam_unix.so try_first_pass
```

8.2.4 common-password

```
#
# /etc/pam.d/common-password - password-related modules common to all
services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define  the services to be
#used to change user passwords.  The default is pam_unix
```

```
# The "nullok" option allows users to change an empty password, else
# empty passwords are treated as locked accounts.
#
# (Add `md5' after the module name to enable MD5 passwords)
#
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option
in
# login.defs. Also the "min" and "max" options enforce the length of
the
# new password.

#password   required   pam_unix.so nullok obscure min=4 max=8 md5
password   sufficient pam_ldap.sp
password   required   pam_unix.so nullok obscure min=4 max=8 md5
use_first_pass

# Alternate strength checking for password. Note that this
# requires the libpam-cracklib package to be installed.
# You will need to comment out the password line above and
# uncomment the next two in order to use this.
# (Replaces the `OBSCURE_CHECKS_ENAB', `CRACKLIB_DICTPATH')
#
# password required     pam_cracklib.so retry=3 minlen=6 difok=3
# password required     pam_unix.so use_authtok nullok md5
```

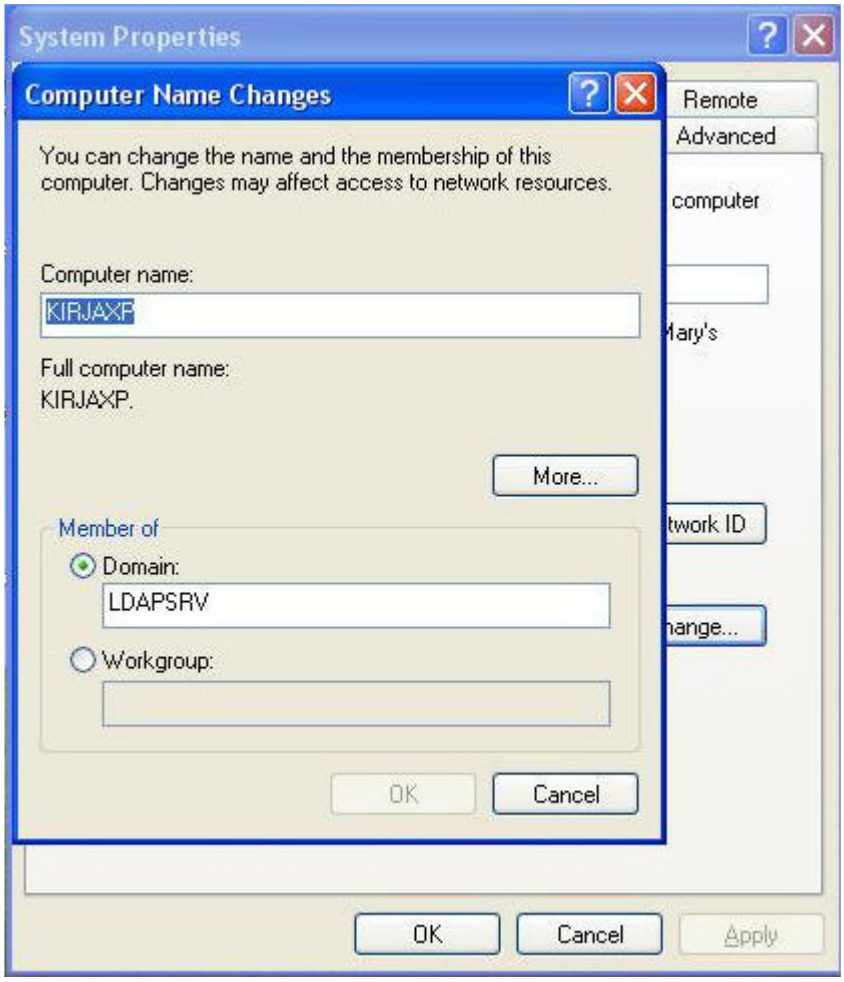
8.2.5 ldap.conf

```
# $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf,v 1.9 2000/09/04
19:57:01 kurt Exp $
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=example,dc=org
URI     ldaps://example.org
TLS_REQCERT allow

#SIZELIMIT 12
#TIMELIMIT 15
#DEREF               never
```

8.3 Windows-työaseman asetukset

Windows-työasemien asetusten määrittäminen on Samban ansiosta hyvin helppoa. Koska Samba ”matkii” Windows-ympäristöä, ei käyttöjärjestelmälle tarvitse kuin kertoa, mihin toimialueeseen liittyä. Windows XP:ssä toimialue määritetään järjestelmän asetusten (Ohjauspaneeli – Järjestelmän Asetukset / Control Panel – System) Tietokoneen

Nimi (Computer Name) -välilehdellä. Kun toimialue eli domain on määritelty, järjestelmä kysyy toimialueen pääkäyttäjän nimeä ja salasanaa, ja kun nämä on annettu oikein, toivottaa järjestelmä tietokoneen tervetulleeksi, jos tietokoneen nimi löytyy palvelimen tiedoista.



Kuva 7. Windows XP:n toimialueen määrittäminen.

8.4 Solaris-asetukset

Solaris-työasemaa varten palvelimen asetuksia piti säätää hieman. OpenLDAP:n ja Solariksen ldap-sovelluksen välillä on pieni yhteensopivuusongelma, jota varten on olemassa korjaus, jonka asensinkin palvelimelle. Ilman tätä korjausta Solariksen automaattinen ldap-asetustenhakuohjelma ei suostu toimimaan niin kuin pitäisi. Palvelin opetettiin myös käyttämään Solariksen käyttäjien tarvitsemia schema-tiedostoja.

Itse työaseman asetuksia määritellessä tehdään muutoksia muutamiin tiedostoihin, jotka ovat päätteeltään .ldap, eikä .conf, kuten Linuxin puolella. Tämä johtuu siitä, että asetukset kirjataan näihin .ldap -päätteisiin tiedostoihin ja ldapclient-ohjelma muuntaa näistä tiedostoista sopivat samannimiset .conf -tiedostot.

nssswitch.ldap-tiedostoon määrittelin tuttuun tapaan *files dns*, jolloin nimipalvelin hakee osoitteet ensin paikallisista tiedostoista, ja vasta tämän jälkeen kyselee palvelimilta. Solaris osaa hakea LDAP-palvelimelta asetukset automaattisesti, mutta tämä ei tapahtunut täysin ongelmitta, vaikka lopulta käyttöjärjestelmä saatiinkin hakemaan asetukset palvelimelta. Asetusten haku tapahtui lopulta komennolla "`ldapclient -v init -a proxyDN=cn=fake,ou=People,dc=example,dc=com`".

Seuraavat muutokset tulivat pam.conf -tiedostoon, johon määritellään miten eri palvelut toimivat.

Lopulta myös Solaris saatiin toimimaan yhdessä palvelimen kanssa. Solaris on periaatteessa helppo tuoda mukaan työasemana, kun asetukset ovat kunnossa, mutta nämä asetukset opin itse vasta yrityksen ja erehdyksen kautta. (Alkaloid Networks Docupedia 2007.)

9 ONNISTUNUT KIRJAUTUMINEN

Kun palvelin ja työasemat oli saatu määritetyiksi, oli aika testata kokonaisuuden toimimista. Kirjautuminen onnistui loppujen lopuksi niin, että yksi palvelin pyöritti eri LDAP-protokollaa käyttäviä ohjelmia ja työasemat suostuivat kirjautumaan sisälle, riippumatta käytössä olevasta käyttöjärjestelmästä. Pieniä ongelmia piti kuitenkin vielä ratkoa, kuten esimerkiksi Windows-kirjautumisen yhteydessä huomattu yksityiskohta, eli käyttäjälle tuli myös luoda palvelinkoneelle työtila-hakemisto, jotta käyttäjän asetukset tallentuisivat palvelimelle. Muuten projekti onnistui mukavasti, eikä mitään vakavampia yllätyksiä päässyt syntymään.

Työn tavoitteena oli luoda yksi keskitetty palvelin, joka sisältäisi kaikkien verkkoa käyttävien käyttäjien tiedot ja niitä piti voida käyttää hyväksi kirjauduttaessa sisään eri työasemilla eri puolella verkkoa. Käyttöjärjestelmä ei saanut vaikuttaa kirjautumiseen ja tiedon tuli luonnollisesti olla salattua, ettei tietojen hakkerointi olisi liian helppoa.

Luotu testiverkko täytti kaikki nämä tavoitteet, palvelimen käyttöjärjestelmänä oli vaadittu Debian Sarge, ja se pyöritti OpenLDAP-ohjelmistoa. Tiedot kulkivat verkossa SSL-salattuna, ja jos sama käyttäjätunnus/salasana-pari olisi syötetty tarpeeksi monta kertaa väärin, palvelimelle tätä varten asennettu fail2ban-niminen ohjelmisto olisi estänyt seuraavat yritykset estämällä käyttäjän joko tietyksi ajaksi tai kokonaan. Sisään voitiin kirjautua myös useilla eri käyttöjärjestelmillä ilman, että käyttäjälle tulisi mitään ongelmia kirjautumisen yhteydessä.

Käytössä ollut verkko oli hyvin pieni. Todellisessa ympäristössään LDAP toimisi kyllä näillä asetuksilla hyvin, mutta vaatisi lähes jatkuvaa ylläpitoa. Jos verkossa olisi useita kymmeniä tai satoja tietokoneita, olisi ylläpitäjällä melkoinen työ valvoa uusia ja vanhoja käyttäjiä ja heidän konetunnuksiaan. Siksi projektissa käytettiinkin hieman valmiita scriptejä, jotka helpottavat uusien käyttäjien luomista ja heidän ylläpitoaan. Jos verkon ylläpitäjän pitäisi luoda käsin kaikille käyttäjille omat tunnukset, hakemistot, oikeudet ym., olisi tehtävä verkon koosta riippuen melkein mahdoton tai ainakin suhteellisen työläs.

Yksi parannus projektiin olisi jakaa palvelimen kuormitus ja varmistaa tietojen säilyminen lisäämällä verkkoon toinen tai useampia palvelimia. Näin palvelimet jakaisivat käyttäjätiedot keskenään ja ylläpitäisivät tietokantaa muutosten tapahtuessa. Lisäksi toisesta palvelimesta löytyisi aina tietojen varmuuskopiot, jos jostain syystä kävisi niin, että ensisijainen palvelin menisi rikki, jolloin samalla menetettäisiin koko verkon toimivuus palvelimen puuttuessa ja kaikkien käyttäjien tietojen hävitessä bittiavaruuteen. Lisäksi kaikki käyttäjätiedustelut eivät ohjautuisi vain yhdelle palvelimelle, vaan verkkoliikenne voitaisiin jakaa myös toisille palvelimille, jolloin kaikkien palvelinten käyttöaste alenisi.

Tulevien käyttöjärjestelmien kannalta tämän kaltaisen autentikointipalvelimen pitäisi olla suhteellisen turvallinen vaihtoehto. Erilaisia moduuleja ja scheemoja lisäämällä

voidaan lisätä palvelimen yhteensopivuutta vaikka tukemaan Microsoftin uutta Windows Vistaa tai muita tulevaisuuden käyttöjärjestelmiä.

Lähteet

About.com: Focus on Linux. Linux Command Library [verkkodokumentti]. 2004. [viitattu 23.4.2007]. Saatavissa: http://linux.about.com/library/cmd/blcmdl8_pam_localuser.htm

Alkaloid Networks Docupedia. Solaris LDAP client with OpenLDAP server [verkkodokumentti]. 2007. [viitattu 22.7.2007]. Saatavissa: http://docs.lucidinteractive.ca/index.php/Solaris_LDAP_client_with_OpenLDAP_server

BeezNest. Name Service Switch under UNIX/Linux [verkkodokumentti]. 2005. [viitattu 20.4.2007]. Saatavissa: http://glasnost.beeznest.org/articles/151

Linux Devcenter. Introduction to PAM [verkkodokumentti]. 2001. [viitattu 9.5.2007]. Saatavissa: http://www.linuxdevcenter.com/pub/a/linux/2001/09/27/pamintro.html?page=1

Linux Devcenter. PAM Modules [verkkodokumentti]. 2001. [viitattu 9.5.2007]. Saatavissa: http://www.linuxdevcenter.com/pub/a/linux/2001/10/05/PamModules.html

Microsoft TechNet. Active Directory Collection [verkkodokumentti]. 2003. [viitattu 23.4.2007]. Saatavissa: http://technet2.microsoft.com/windowsserver/en/library/6f8a7c80-45fc-4916-80d9-16e6d46241f91033.mspx?mfr=true

Red Hat Documentation. Uses for LDAP [verkkodokumentti]. 2006. [viitattu 12.5.2007]. Saatavissa: http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/ref-guide/s1-ldap-uses.html

Samba. Samba: An Introduction [verkkodokumentti]. 2001. [viitattu 23.4.2007]. Saatavissa: http://fi.samba.org/samba/docs/SambaIntro.html

Smith, R. W. Linux in a Windows World. Yhdysvallat: O'Reilly Media Inc, 2005. 419s.

The Linux Kernel Archives. The Linux-PAM System Administrators' Guide [verkkodokumentti]. 2007. [viitattu 12.5.2007]. Saatavissa: http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/Linux-PAM_SAG.html

Tietoliikenneohjelmistojen ja Multimedian Laboratorio. LDAP (Lightweight Directory Access Protocol) [verkkodokumentti]. 1997. [viitattu 9.5.2007]. Saatavissa: http://www.tml.tkk.fi/Studies/Tik-110.300/1997/Essays/ldap.html

Wikipedia. Windows Server Domain [verkkodokumentti]. 2007. [viitattu 12.5.2007]. Saatavissa: http://en.wikipedia.org/wiki/Windows_Server_domain