SATAKUNNAN AMMATTIKORKEAKOULU

Kari Metsäjoki

2008

LINUX-KÄYTTÄJÄ WINDOWS-AKTIIVIHAKEMISTOSSA

Tekniikka Rauma

Tietotekniikan koulutusohjelma

LINUX-KÄYTTÄJÄ WINDOWS-AKTIIVIHAKEMISTOSSA

Metsäjoki, Kari

Satakunnan Ammattikorkeakoulu

Tekniikka Rauma

Tietotekniikan koulutusohjelma

Kesäkuu 2008

Ohjaaja: laboratorioinsinööri, DI Olli Vainio

UDK: 004.451

Asiasanat: Linux, palvelimet, UNIX, Windows 2003

Tämän työn tarkoituksena oli tutkia ja toteuttaa Linux-käyttöjärjestelmästä kirjautumista Windows-aktiivihakemistoon. Tämä saavutettiin luomalla aktiivihakemiston toimialueeseen käyttäjä, jonka oli tarkoitus pystyä kirjautumaan sekä Windows- että Linux-käyttöjärjestelmistä samoilla tunnuksilla. Työ suoritettiin käyttäen Linuxin Fedora-käyttöjärjestelmää ja palvelinohjelmistona toimi Microsoft Windows Server 2003 R2.

Kirjautuminen suoritettiin ensimmäiseksi käyttäen hyväksi LDAP-hakemistopalvelua yksinkertaisella autentikoinnilla, minkä lisäksi käyttäjän tunnistus tehtiin käyttäen Kerberos-autentikointia. Tämän jälkeen kirjautumiseen lisättiin tietoturvaa yksinkertaisen autentikoinnin ollessa puutteellinen, koska se lähettää tietonsa selkokielisenä yli verkon. Lisää tietoturvaa saavutettiin käyttämällä verkon tietojen salaamiseksi SSL-salausta ja sen tarvitsemaa sertifikaattia. Viimeisenä suoritettiin vaihtoehtoinen tapa toteuttaa Linux-kirjautuminen ja autentikointi aktiivihakemistoon käyttäen Winbindiä ja uudistunutta Sambaa.

Työn tuloksena aktiivihakemiston käyttäjä tunnettiin sekä Windows- että Linux-käyttäjänä. Vaikka uusien Linux-ohjelmaversioiden ilmestyminen työn tekemisen aikana toi omat lisänsä, saavutettiin työssä odotetut tulokset ja tavoitteet.

LINUX USER IN WINDOWS ACTIVE DIRECTORY

Metsäjoki, Kari

Satakunta University of Applied Sciences

School of Technology Rauma

Information Technology

Commissioned by Satakunta University of Applied Sciences

June 2008

Tutor: Olli Vainio, MSc (Eng), Laboratory Engineer

UDC: 004.451

Keywords: Linux, Servers, UNIX, Windows 2003

The purpose of this project was to study and implement logging in to Windows Active Directory from the Linux operating system. This was carried out using the Linux Fedora and Microsoft Windows Server 2003 R2 operating systems.

After making a user account to Windows Active Directory Domain and extending the schema via Windows Server 2003 R2, a Windows user could also be known as a UNIX user. The main idea was to use LDAP to look up user information in the Active Directory for UNIX users. With this UNIX information a Linux user could authenticate into Active Directory using the Kerberos authentication, which would encrypt crucial authentication traffic. Finally, more protection to data communications could be achieved using SSL encryption for less critical LDAP directory services traffic.

Finally, the same authentication and logging in to Active Directory was implemented using an alternative method. This was carried out using Winbind and a new version of Samba.

The objectives of this project were achieved: a user could log in to the Windows Active Directory using either the Linux or Windows operating system with the same user information in both cases.

ALKUSANAT

Tämä työ tehtiin Raumalla yhteistyössä Satakunnan Ammattikorkeakoulun Tekniikka Rauman kanssa. Työ suoritettiin kesän 2007 ja kevään 2008 välillä. Työn tarkoitus on olla tutkimuksena ja dokumenttina sekä mahdollisena pohjana koululle työn mahdollista tulevaisuuden käyttöönottoa varten. Työn valvojana toimi Tekniikka Rauman puolesta laboratorioinsinööri Olli Vainio.

Haluan omalta osaltani kiittää Satakunnan Ammattikorkeakoulun Tekniikka Raumaa, joka antoi minulle mahdollisuuden tähän opinnäytetyöhön ja tilat työn tekemiseksi. Haluan lisäksi kiittää kaikkia, jotka ovat minua kannustaneet tämän projektin valmiiksi saamisessa. Kiitokset myös Olli Vainiolle kaikesta avusta ja hyvistä neuvoista työn edetessä.

Raumalla 13.6.2008

Kari Metsäjoki

SISÄLLYS

TERMILUETTELO

DHCP (Dynamic Host Configuration Protocol)	Verkkoprotokolla, jonka tehtävä on jakaa IP-osoite palvelimen kanssa samaan verkkoon kytkeytyville laitteille
DNS (Domain Name System)	Nimipalvelujärjestelmä, joka muuntaa nimet IP-osoitteiksi
Gnome	Graafinen työpöytäympäristö, jota käytetään Linux-käyttöjärjestelmissä
IP-osoite	Numeerinen osoite, joka yksilöi Internet-verkossa olevan tietokoneen. Voi olla joko kiinteä (staattinen) tai vaihtuva (dynaaminen)
Kerberos	Todennusprotokolla, jonka avulla käyttäjät voivat tunnistautua toisilleen verkon yli salattuna
LDAP (Lightweight Directory Access Protocol)	Verkkoprotokolla, joka on tarkoitettu hakemistopalveluiden käyttöön ja pääasiassa käyttäjän tunnistukseen
NIS (Network Information Service)	Verkkopalvelu, joka tarjoaa keskitetyn käyttäjätunnistuksen

Ohjauspalvelin (Domain Controller)	Toimii aktiivihakemiston toimialueen ohjauskoneena, joka ylläpitää toimialueen resursseja ja tunnistaa toimialueelle kirjautuvat käyttäjät
OpenLDAP	Vapaa ja avoimen lähdekoodin versio LDAP-hakemistopalvelimesta
Osiointi	Tietokoneen kiintolevyn jakaminen osiin, eli osioihin, jotka näkyvät käyttäjälle kuin eri levyinä
Shell	Tekstimuotoinen käyttöliittymä (komentorivi), jossa tietokonetta käytetään antamalla komentoja
SSH	Pääteyhteysohjelma, jolla voi ottaa turvallisen pääteyhteyden toiseen tietokoneeseen tietoliikenneverkon yli
SSL (Secure Sockets Layer)	Salausprotkolla, jolla voidaan suojata tietoliikennettä IP-verkon yli
Toimialue (Domain)	Joukko Microsoft Windows -käyttöjärjestelmän sisältäviä tietokoneita, joita voidaan hallita keskitetysti

1 JOHDANTO

Satakunnan ammattikorkeakoulun Tekniikka Raumassa on käytössä Microsoftin aktiivihakemisto, jolla hallitaan sen toimialueeseen kuuluvia käyttäjiä. Linux-käyttöjärjestelmällä on kuitenkin joitakin etuja verrattuna Windows-käyttöjärjestelmiin, erityisesti palvelinpuolella. Linux eroaa muista käyttöjärjestelmistä siinä, että se on alustariippumaton käyttöjärjestelmä. Se on myös vapaa ja ilmainen kaikille. Sitä voidaan vapaasti muokata ja parannella, jos siihen vain taitoa löytyy. Samaa ei voi sanoa Windows-käyttöjärjestelmistä, joihin vain Microsoft voi tehdä muutoksia. Tämä tuo Linuxiin vapauden, jonka avulla sitä kehitetään jatkuvasti ja paljon nopeammin kuin mitään muuta käyttöjärjestelmää.

Tämän johdosta Tekniikka Raumassa on tavoitteena käyttää molempia käyttöjärjestelmiä, jolloin on tarpeellista käyttää ainoastaan yhtä käyttäjätietokantaa käyttäjien hallinnan helpottamiseksi. Tässä työssä tutkittiin mahdollisuuksia käyttää Microsoftin Windows-aktiivihakemistoa käyttäjätietokantana siten, että Linux-käyttäjät pystyisivät kirjautumaan koulun palvelimelle käyttäen aktiivihakemiston tunnuksia.

2 KÄYTETYT KOMPONENTIT

2.1 Windows Server 2003 R2

Työssä käytetty palvelinohjelmisto oli Windows Server 2003 R2 Enterprise Edition. Microsoft Windows Server 2003 R2 on ohjelmistopäivitys Windows Server 2003 -käyttöjärjestelmään, jonka avulla on entistä helpompaa laajentaa yhdistettävyyttä ja hallinnoida käyttäjiä, sijainteja, dataa ja sovelluksia läpi yrityksen tarpeen.

Parannuksia, joita R2 tuo mukanaan integroituna, on monia, mutta tässä työssä tärkeimmät näistä liittyivät Windows Server 2003- ja Linux/UNIX -käyttöjärjestelmien parannettuun yhteensopivuuteen. Siihen liittyen se sisältää kaksi komponenttia, jotka ovat Identity Management for UNIX sekä Subsystem for UNIX-based Applications. Näistä ensimmäinen on erittäin keskeinen työn aiheen kannalta, ja se vaatii tarkempaa tarkastelua.

2.2 Identity Management for UNIX

Identity Management for UNIX on Windows-palvelu UNIXia varten, ja siinä tapahtuu Windows- ja UNIX-pohjaisten käyttöjärjestelmien integrointi käyttäjien hallintaa varten. Se sisältää kaksi hallintatyökalua, jotka ovat Server for NIS ja Password Synchronization.

Server for NIS on työkalu, joka sulauttaa Windows- ja UNIX-pohjaiset Network Information Services (NIS) -palvelimet yhteen. Tämän se saa aikaan tekemällä aktiivihakemiston toimialueen ohjauspalvelimesta NIS-palvelimen yhdelle tai useammalle NIS-toimialueelle.

Password Synchronization yksinkertaistaa Windows- ja UNIX-palvelimien tapaa ylläpitää turvattuja salasanoja. Tämä työkalu mahdollistaa sen, että yhden käyttäjän ei tarvitse pitää erillisiä salasanoja omille Windows- ja UNIX-tileille tai muistaa vaihtaa ja säilyttää eri salasanoja eri paikoissa. (Microsoft Technet 2007.)

2.3 Fedora 8

Työssä käytettiin Windows Server -käyttöjärjestelmän kanssa toisena käyttöjärjestelmänä Linuxin Fedora 8 -versiota. Fedora syntyi syksyllä 2003, jolloin sen julkaisija, Red Hat, päätti jakaa Red Hat Linuxin kahteen osaan. Näin syntyi ei-kaupallinen Fedora ja siihen pohjautuva kaupallinen Red Hat Enterprise Linux. Vielä Fedoran 6 -versiossa oleva sana Core putosi pois jakelun nimestä toukokuussa 2007. Silloin julkaistussa 7-versiossa Red Hatin ylläpitämä järjestelmän ydinpaketit sisältävä Core-pakettilähde ja yhteisön ylläpitämä Extras-pakettilähde yhdistyivät yhdeksi paketiksi. (Linux.fi 2008.)

Fedora on siis käyttöjärjestelmä, joka esittelee viimeisimmät parannukset vapaaseen ja avoimeen lähdekoodiin. Se on aina ilmainen ja vapaa käyttöjärjestelmä kaikille, jotka sitä haluavat käyttää, muokata ja levittää. Se on rakennettu kaikille ihmisille ympäri maailmaa, jotka näin työskentelevät yhteisönä, toisin sanoen, Fedora Projektina. (Fedora wiki 2008.)

Linux Fedora -käyttöjärjestelmää on määrä julkaista uutena versiona ainakin kaksi kertaa vuodessa. Fedora 8 ilmestyi marraskuussa 2007, jonka mukaan tämä työ on kokonaisuudessaan tehty ja dokumentoitu.

2.4 Aktiivihakemisto

Active Directory (AD) eli aktiivihakemisto kuuluu tärkeisiin työssä käytettyihin komponentteihin, ja se sisältyy Windows Server 2003 -käyttöjärjestelmään.

Aktiivihakemistoon perustuvat kaikki hakemistopalvelut, joita Windows Server 2003 käyttää. AD on Microsoftin tapa toteuttaa hakemistopalvelut palvelimissa. Puhuttaessa hakemistopalvelusta (directory service) ja hakemistosta (directory) on niiden välille syytä tehdä ero. Hakemistopalvelu sisältää hakemiston tiedot eli tietovaraston, toisin sanoen tietokannan, ja se myös sisältää pääsyn tietovarastoon. Aktiivihakemiston varsinainen tehtävä on pienentää ylläpidettävien hakemistojen määrää.

Ensimmäisen kerran AD oli käytössä Windows 2000 Server -käyttöjärjestelmässä. Uuden version, Windows Server 2003:n myötä, aktiivihakemistosta tuli paljon laajempi ja tehokkaampi. Normaalisti AD ei välttämättä näy käyttäjälle ollenkaan, mutta Windows Server 2003 -aktiivihakemistoa on paljon miellyttävämpi hallita kuin edeltäjäänsä. Järjestelmään on tullut sisäisiä muutoksia, ja se on saanut monipuolisemmat hallinta- ja tukityökalut. (Kivimäki, Windows Server 2003 Active Directory 2005, 1.)

Käyttäjällä, jolla on järjestelmänvalvojan (Administrator) oikeudet, on pääsy kaikkiin aktiivihakemiston hallintaa koskeviin työkaluihin. Hänelle aktiivihakemistossa onkin kysymys yhdessä paikassa sijaitsevien objektien käsittelystä hallintaa koskevilla työkaluilla, eli hän voi hallinnoida järjestelmää keskitetysti. Suurin osa käyttöjärjestelmän objekteista on tallennettu aktiivihakemiston tietokantaan. Kulloinkin käytössä oleva työkalu määrää, millä tavalla ja mitä tietoja tietokannasta voidaan käsitellä. AD on lopulta erittäin laaja kokonaisuus, ja sillä on yleensä suuri rooli palvelinkäytössä. Tämän takia järjestelmänvalvojalla olisi syytä olla edes jonkinnäköinen käsitys sen keskeisistä ominaisuuksista ja työkaluista. (Kivimäki, Windows Server 2003 Active Directory 2005, 6.)

Jokaisella työkalulla on erilainen näkymä aktiivihakemistoon. Tämän työn kannalta tärkeäksi työkaluksi osoittautui Active Directory Users and Computers -hallintakonsoli, joka on myös normaalisti aktiivihakemistossa usein käytetty työkalu. Tällä työkalulla hallitaan toimialueen käyttäjiä, ryhmiä, tietokoneita ja muita objekteja. Hallintakonsoli aukeaa automaattisesti siihen toimialueeseen, jonka ohjauspalvelimeen ollaan kirjautuneena.

3 ASENNUS

3.1 Windows Server 2003 R2 Enterprise Edition

Ennen käyttöjärjestelmän asennusta on syytä ottaa selville, täyttääkö tietokoneen laitteisto asennettavan käyttöjärjestelmän vaatimukset. Microsoftilla on myös olemassa sivusto, jossa on luettelo erilaisista laitteista, jotka täyttävät Windows-logo-vaatimukset. Näin voidaan varmistaa, että Windows Server 2003 tukee käytettävissä olevaa laitteistoa. Kyseinen Windows Server Catalog -sivusto löytyy osoitteesta http://www.windowsservercatalog.com/default.aspx. On myös otettava huomioon, että jos on asennettuna jokin vanhempi Windows-versio, on mahdollisuus käynnistää asennusohjelma Windows Server 2003:n asennus CD:ltä. Tämän asennusohjelman alussa voi normaalin asennuksen sijaan valita Check system compatibility -vaihtoehdon, jonka avulla voidaan tarkistaa laitteiston yhteensopivuus ja tunnetut yhteensopivuusongelmat. Ohjelma luo raportin, josta selviävät mahdolliset yhteensopivuuden ongelmat. (Kivimäki, Windows Server 2003 2005, 10-12.)

Koska Windows Server 2003 -käyttöjärjestelmä on saatavilla ainoastaan englanninkielisenä, ei välttämättä kaikille siinä käytetyille sanoille, komennoille ja termeille löydy suomenkielistä vastinetta. Olen kaikissa tilanteissa antanut käyttöjärjestelmässä käytetyn englanninkielisen alkuperäisen sanan tai sanat suluissa oman suomennokseni jälkeen. Suomennoksissa olen pyrkinyt käyttämään suomenkielisten Windows-käyttöjärjestelmien ko. kohtia. Myös suurin osa lähteistä oli englannin kielellä, joten lukijan täytyy huomioida, että ne on käännetty englannista.

3.2 Aktiivihakemiston asennus

Windows Server 2003 -käyttöjärjestelmän asennus tapahtuu lähes samanlaisesti kuin Windows XP -käyttöjärjestelmän asennus, joten sen pitäisi olla melko yksinkertaista ja helppoa. Varsinaisen käyttöjärjestelmän asennuksen jälkeen voidaan siirtyä aktiivihakemiston asennukseen. Tämä tapahtuu menemällä Käynnistä-valikkoon (Start) ja valitsemalla sieltä hallintatyökalut (Administrative Tools) ja edelleen palvelimen

hallinta (Manage Your Server). Valitsemisen jälkeen aukeaa Manage Your Server -ikkuna, josta valitaan Lisää tai poista rooli (Add or remove a role). Valitsemalla Lisää tai poista rooli aukeaa palvelimen hallinnan opastus (Configure Your Server Wizard), josta painamalla Seuraava (Next) alkaa tietokone tarkistaa verkon asetuksia. Verkkoasetusten tarkistuksen jälkeen valitaan configuration options -ikkunasta custom configuration, josta päästään tekemään itse haluttavat asetukset uudelle roolille palvelimessa. Tämän jälkeen saavutaan kohtaan, jossa valitaan haluttu uusi rooli (Server Role) palvelimelle, valitaan vaihtoehto Domain Controller (Active Directory) ja painetaan Seuraava. Seuraavaksi nähdään lista, jossa ovat kaikki edellä tehdyt valinnat (Summary of Selections). Tämä voidaan hyväksyä ja jatkaa eteenpäin painamalla Seuraava tai korjata edellä tehtyjä valintoja painamalla Edellinen (Back).

Tällä hetkellä on päästy kohtaan, josta alkaa varsinainen aktiivihakemiston asennus ja eteen aukeaa Active Directory Installation Wizard -ikkuna opastamaan tulevia valintoja. Tästä jatketaan painamalla Seuraava ja myös seuraavassa kohdassa (Operating System Compatibility) painetaan Seuraava. Tämän jälkeen voidaan valita toimialueen ohjauspalvelimen tyyppi (Domain Controller Type), josta valitaan ohjauspalvelin uudelle toimialueelle (Domain controller for a new domain). Seuraavaksi kohdassa Create New Domain valitaan oletuksena (default) oleva määritys, joka on toimialue uuteen aktiivihakemiston metsään (Domain in a new forest). Seuraavaksi voidaan antaa uudelle toimialueelle nimi (New domain name) ja annetaan sille nimi, joka sopii tilanteen tarkoitukseen. Annoin nimeksi SAMK.local. Toimialueen nimeämisen jälkeen kysytään toimialueen NetBIOS-nimeä (NetBIOS domain name). Tämä toimialueen nimi tulee olemaan nimi, joka näkyy Windows-käyttöjärjestelmän kirjautumisikkunan kohdassa, missä ilmoitetaan toimialueen nimi, johon halutaan kirjautua. Jälleen nimeksi voidaan antaa mikä tilannetta milloinkin vastaa, joten annoin sen nimeksi SAMK. Tämän jälkeen Database and Log Folders -kohdassa voidaan valita paikka, jossa kaikki aktiivihakemiston tarvittavat lokitiedostot ja muu tieto (Database and Log Folders) halutaan säilytettäväksi. Jos jostain syystä halutaan näitä tietoja säilytettävän jossain määrätyssä paikassa, se valitaan tässä vaiheessa, mutta omassa tapauksessa jätin kohdekansion oletuksena olevaan sijaintiin, mikä lienee suotavaa. Tämän jälkeen tullaan Shared System Volume -ikkunaan, jossa voidaan valita sijainti kansiolle, jonka sisältöä käytetään toimialueiden ohjauspalvelin-

ten replikointia eli kopiointia varten. Jälleen valitsin oletuksena olevan kohdekansion. Nyt seuraavana oli vuorossa DNS Registration Diagnostics -kohta, jossa voidaan tarkistaa, pitävätkö Domain Name System -asetukset paikkansa. Jos asetukset eivät ole niin kuin pitäisi, tilannetta vastaavat virheilmoitukset lukevat Diagnostic Results -tekstin alapuolella, ja tilanne vaatii korjaavia toimenpiteitä. Korjaavat toimenpiteet voidaan tehdä joko nyt tai myöhemmin. Vaihtoehtona on myös asentaa ja konfiguroida DNS tähän palvelimeen ja käyttää sitä DNS-palvelinta tämän palvelimen suositeltuna DNS-palvelimena (Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server). Minä valitsin uuden DNS-palvelimen asennuksen, koska työssä on tarkoitus käyttää palvelinta itse DNS-palvelimena.

Viimeiseksi tulee kohta Permissions, jossa on valittavana kaksi oikeuksiin liittyvää vaihtoehtoa. Ensimmäinen on Permissions compatible with pre-Windows 2000 Server operating systems ja jälkimmäinen Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems. Jotkut palvelimen ohjelmat, varsinkin vanhemmat palvelinohjelmistot, saattavat lukea tietoja toimialueen ohjauspalvelimesta toimiakseen ja tarvitsevat sitä varten yhteensopivuuden, mikä on syytä ottaa tässä vaiheessa huomioon. Ensimmäinen vaihtoehto tulisi valita, jos käytetään palvelinohjelmistoja ennen Windows 2000 -käyttöjärjestelmää ilmestyneissä käyttöjärjestelmissä tai käytettäessä Windows 2000- tai Windows Server 2003 -käyttöjärjestelmiä, jotka kuuluvat pre-Windows 2000-toimialueeseen. Toinen vaihtoehto on tarkoitettu valittavaksi, jos käytetään palvelinohjelmistoja ainoastaan Windows 2000- tai Windows Server 2003 -käyttöjärjestelmissä, jotka kuuluvat aktiivihakemiston toimialueeseen. Näistä valittaessa on myös syytä huomioida, että jos päätyy ensimmäiseen vaihtoehtoon, silloin toimialueelle tuntemattomat voivat lukea toimialueen tietoja vapaasti. Jos valitsee jälkimmäisen vaihtoehdon, silloin ainoastaan toimialueeseen kirjautuneet ja tunnetut käyttäjät voivat tutkia ja lukea toimialueen tietoja. Minulla ei ollut mitään syytä valita ensimmäistä vaihtoehtoa, joten päädyin jälkimmäiseen. Ennen asennuksen alkua vielä kysytään uutta järjestelmänvalvojan salasanaa, ja tätä salasanaa voidaan joskus tarvita aktiivihakemiston toimintaan palauttamiseen (Directory Services Restore Mode Administrator Password). Kyseinen salasana ei liity jo aikaisemmin annettuun toimialueen järjestelmänvalvojan salasa-

naan, vaan on ainoastaan tämän tietokoneen sisäinen salasana, jolla saadaan palautettua täällä tehdyt valinnat, jos jostain syystä aktiivihakemisto ei suostu käynnistymään ja se joudutaan palauttamaan. Annoin salasanaksi tilanteeseen sopivan restore ja jatkoin painamalla Seuraava. Nyt asennusohjelma näyttää vielä yhteenvedon (Summary) tehdyistä valinnoista. Nämä kannattaa toki lukea vielä läpi ja tarkistaa, että kaikki asiat ovat niin kuin ne oli tarkoitettu, eikä ole tullut mahdollisia inhimillisiä virheitä valintoja tehtäessä. Jos kaikki tiedot pitävät paikkansa, jatketaan painamalla Seuraava ja aktiivihakemiston varsinainen asennus alkaa.

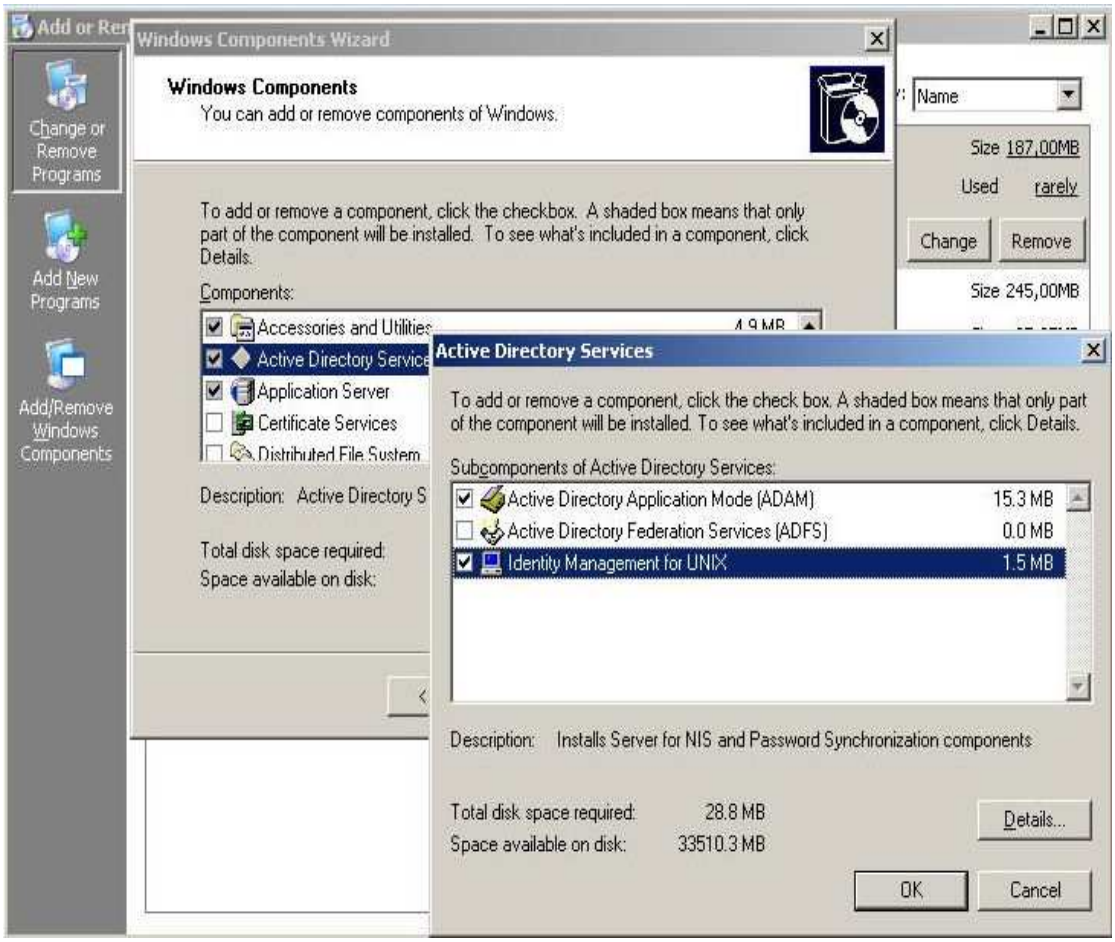
Tiedostojen kopioimisen aikana tullaan kysymään Windows Server 2003 Service Pack 1:n asennuslevyä, jolloin asennus ei jatku eteenpäin ilman sen antamista. Jos palvelimella on ennen ollut dynaaminen IP-osoite, ehdotetaan sen vaihtamista staattiseksi levyn antamisen jälkeen. Uudeksi staattiseksi IP-osoitteeksi annettiin 10.0.0.10, aliverkon peitteen ollessa 255.0.0.0. Tärkeintä osoitteen antamisessa on, että se vastaa käyttötilannetta. Työssä käyttöön tuli ainoastaan kolme konetta, ilman yhteyttä ulkoverkkoon, joten käytettiin yksityistä ”kymppiverkkoa”. Tällaista verkkoa, kuten normaalejakin verkkoja käytettäessä, on syytä tietää, että jos koneiden välissä on yhdyskäytävänä mahdollisesti reititin tai reitittävä kytkin, joilla ne on kytketty toisiinsa, on niillä oletuksena yleensä verkosta ensimmäinen IP-osoite. Jos näin on, annetaan oletusyhdyskäytävän (Default Gateway) osoitteeksi yhdistävän laitteen osoite 10.0.0.1. Työssäni osoitteiden nimeämisessä oli otettava huomioon se, että myöhemmin käyttöön otettava Linux-kone sekä aktiivihakemiston testausta varten oleva Windows-kone täytyi liittää samaan verkkoon kuin Windows-palvelin, jotta ne osaisivat toimia keskenään. Jos käytetään Windows-palvelimen Dynamic Host Configuration Protocol (DHCP) -palvelinta IP-osoitteiden jakoon, silloin DHCP antaa automaattisesti osoitteet.

Kun kaikki valinnat on tehty ja asennus on valmis, asennusohjelma vaatii palvelimen uudelleenkäynnistyksen aktiivihakemiston käyttöönottamiseksi. Uudelleenkäynnistyksen jälkeen sisäänkirjautumisikkunasta voi nähdä, että juuri luotu uusi toimialue SAMK on tullut toimialuevalikkoon, josta valitaan toimialue, johon halutaan kirjautua. Kirjautumalla juuri luotuun uuteen toimialueeseen SAMK järjestelmänvalvojan

tunnuksella Administrator saadaan ilmoitus, että kyseinen palvelin toimii nyt ohjauspalvelimena (Domain Controller).

3.3 Identity Management for UNIX

Kun aktiivihakemiston asennus on valmis, voidaan palvelinta laajentaa yhteensopivaksi Linuxille asentamalla Identity Management for UNIX -komponentti. Tämä tapahtuu avaamalla Käynnistä-valikosta (Start) ohjauspaneeli (Control Panel) ja ohjauspaneelista avataan Lisää tai poista sovellus (Add or Remove Programs) -ohjelma. Lisää tai poista sovellus -ikkunan auettua voidaan valita kolmesta eri vaihtoehdosta: voidaan muuttaa tai poistaa ohjelmia (Change or Remove Programs), lisätä uusia ohjelmia (Add New Programs) tai kolmantena lisätä tai poistaa Windows-komponentteja (Add/Remove Windows Components). Näistä valitaan viimeinen vaihtoehto eli Lisää tai poista Windows-komponentteja, josta aukeaa Windows Components Wizard -ikkuna. Tästä listasta nähdään jo asennetut Windows-komponentit ja komponentit, joita on mahdollista asentaa tai poistaa tämän ohjelman kautta. Rastitetaan listalta ruutu kohtaan Active Directory Services ja painetaan Details-painiketta, josta päästään muokkaamaan kyseisen komponentin osia. Active Directory Services -komponentissa on kolme osaa, joista tarvitaan ainoastaan yhtä, joka on jo työn alussa selvitetty Identity Management for UNIX. Rastitetaan ruutu tämän kohdalla. Valittaessa kyseinen osa nähdään ikkunan alalaidasta komponentin asennukseen tarvittava kovalevytila ja tämänhetkinen vapaan tilan määrä kovalevyllä. Alhaalla olevasta kuvauksesta (Description) myös nähdään sen asennukseen kuuluvat Server for NIS ja Password Synchronization -komponentit, joista työn alussa mainittiin (kuva 1). Identity Management for UNIX -komponentin valinnan jälkeen painetaan OK, jonka jälkeen Windows Components Wizard -ikkunassa valitaan Seuraava (Next), jolloin valittujen komponenttien asennus alkaa. Identity Management for UNIX -komponentti kuuluu R2-version tuomiin uusiin ominaisuuksiin, joten sen asennus vaatii Microsoft Windows Server 2003 R2 -asennuslevyä. Asennuksen valmistuttua saadaan kehotus, joka suosittelee palvelimen uudelleenkäynnistystä. Uudelleenkäynnistyksen jälkeen Identity Management for UNIX -komponentti on asennettu ja voidaan jatkaa työssä eteenpäin.



Kuva 1. Identity Management for UNIX -komponentin asennus.

3.4 Windows Services for UNIX 3.5

Tässä vaiheessa on syytä myös mainita, että samankaltaisen komponentin asennus onnistuu myös normaalissa Windows Server 2003 -versiossa uuden R2-version sijaan. Tämä tapahtuu asentamalla Services for UNIX (SFU) 3.5 -komponentti. Kyseisen komponentin voi ladata Microsoftin kotisivuilta osoitteesta http://www.microsoft.com/downloads/details.aspx?FamilyID=896c9688-601b-44f1-81a4-02878ff11778&DisplayLang=en. Komponentin asennus sen lataamisen jälkeen on hyvinkin yksinkertainen eikä vie sen enempää aikaa kuin edellisessä luvussa esitelty Identity Management for UNIX-komponentin asennus.

3.5 Linux Fedora 8

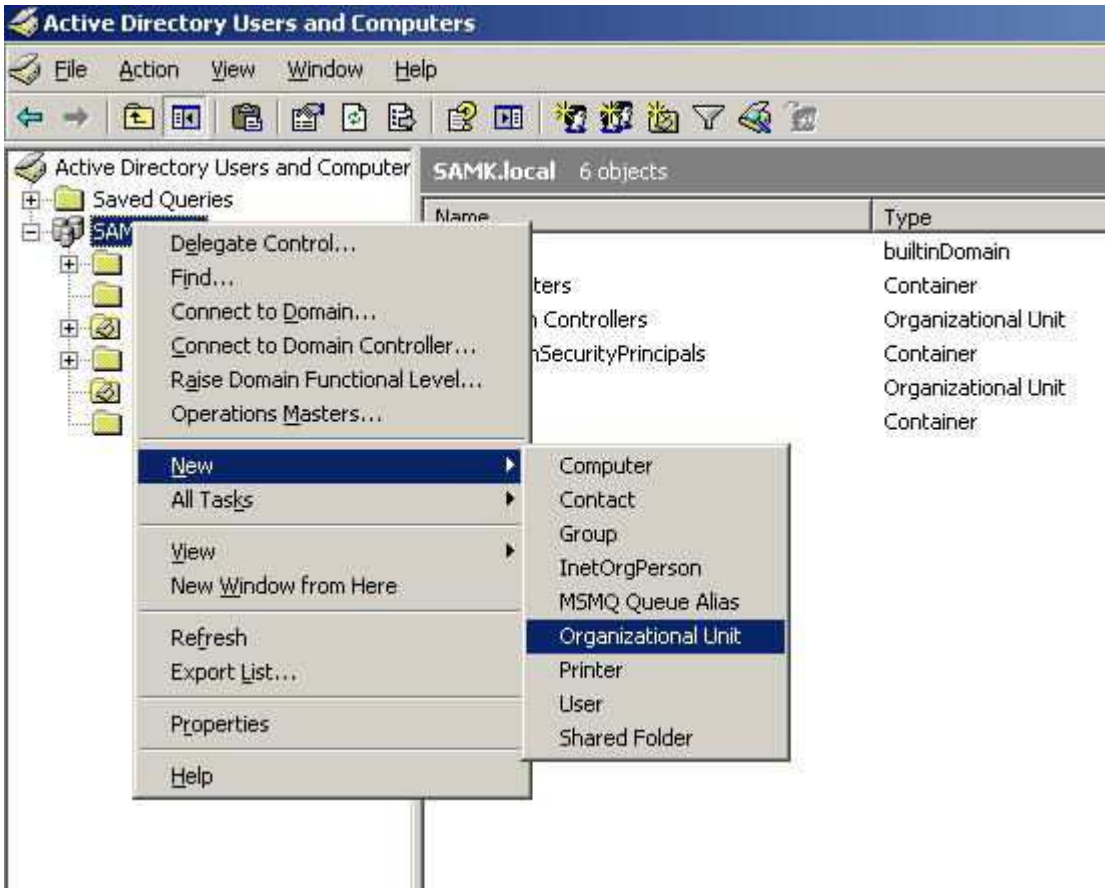
Fedora-käyttöjärjestelmän asennus on nykyisin hyvinkin helppoa, ja asennusohjelman antamat oletusvalinnat toimivat hyvänä lähtökohtana asennuksessa. Asennuksen valmistuttua käyttöjärjestelmän käynnistymisen jälkeen asennuksen loki on nähtävissä tiedostosta /root/install.log, ja asennuksessa käytetyt valinnat löytyvät tiedostosta /root/anaconda-ks.cfg.

Kun asennusohjelma on kopioinut tarvittavat tiedostot ja asentanut Fedora-käyttöjärjestelmän tietokoneen kovalevylle, se ilmoittaa asennuksen olevan valmis ja tietokone käynnistetään uudelleen asennuksen viimeistelyksi. Uudelleenkäynnistyksen jälkeen saavutaan tietokoneen asetuksien määrittelyyn. Kahden ensimmäisen sivun jälkeen valitaan, otetaanko käyttöjärjestelmässä käyttöön palomuuri vai ei. Jos palomuuria käytetään, voidaan listasta rastittaa palvelut, joihin halutaan sallia pääsy palomuurin läpi. Valitsemisen jälkeen valitut palvelut on merkitty palomuuriin luotetuiksi palveluiksi. Vahvistetaan valinnat, jonka jälkeen kysytään, halutaanko Security Enhanced Linux (SELinux) ottaa käyttöön. SELinux on ohjelma, joka tarjoaa tarkempaa turvallisuuden hallintaa kuin perinteisissä Linux-järjestelmissä. Se voidaan jättää pois päältä, asettaa vain varoittamaan kielletyistä asioista tai asettaa aktiiviseen tilaan. Ohjelma jätettiin oletustilaansa eli aktiiviseksi. Seuraavaksi asetetaan järjestelmälle päivämäärä ja aika sekä haluttaessa verkkoaikaprotokolla, jonka jälkeen voidaan Fedora-projektille lähettää profiili, joka auttaa projektin yhteisöä keskittämään työnsä suosittuihin laitteisiin ja alustoihin. Kyseisen profiilin lähettäminen on täysin anonyymiä ja sen lähetys ottaa käyttöön kuukausittaisen päivityksen. Jokainen voi valita, lähetetäänkö laitteistoprofiilia eteenpäin vai ei. Viimeisenä kohtana käyttäjää kehotetaan luomaan uusi käyttäjätili, joka ei ole ylläpitoa varten tarkoitettu tili. Tämän jälkeen tietokoneen asetuksien määrittäminen voidaan lopettaa ja eteen aukeaa Fedoran Tervetuloa-ikkuna, josta voidaan kirjautua sisään käyttäjänä root. Kirjautumisen jälkeen saavutaan Fedora 8 -käyttöjärjestelmän Gnome-työpöytäympäristöön ja käyttöjärjestelmä on valmis käytettäväksi.

3.6 Aktiivihakemiston valmistelu

Windows- ja Linux-puolen asennusten valmistuttua voidaan jatkaa työssä eteenpäin. Jatketaan valmistelemalla aktiivihakemisto UNIX-ryhmien ja -käyttäjien käyttöönottoon. Ensimmäiseksi tehdään uusi organisaatioyksikkö (Organizational Unit, OU), minne sijoitetaan uusi ryhmä (Group) ja ryhmään sijoitetaan uusi käyttäjä (User).

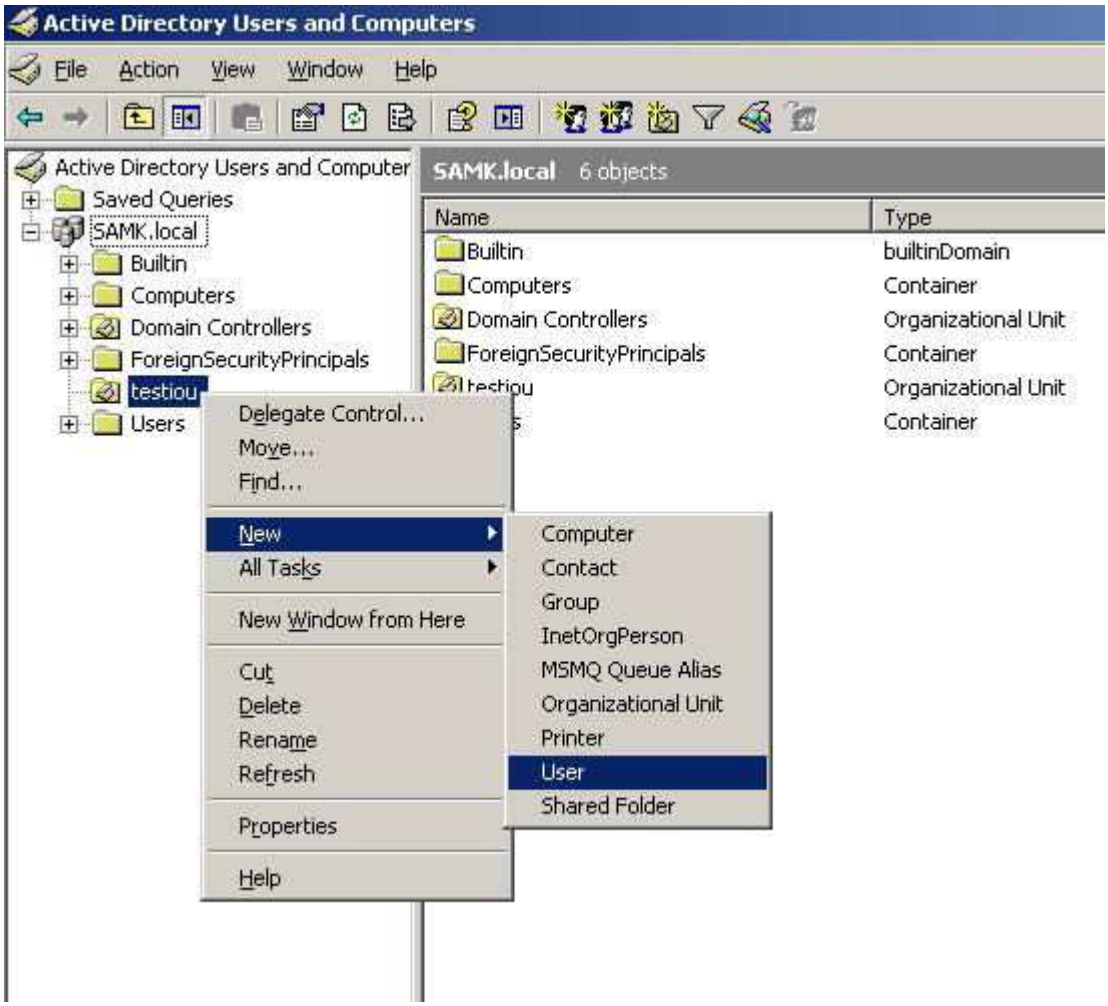
Kun aktiivihakemistoon on kirjauduttu järjestelmänvalvojan tunnuksilla, uuden organisaatioyksikön luominen tapahtuu menemällä Käynnistä-valikkoon (Start), josta valitaan Ohjelmat (Programs) ja Hallintatyökalut (Administrative Tools) ja edelleen Aktiivihakemiston Käyttäjät ja Tietokoneet (Active Directory Users and Computers). Valitsemisen jälkeen eteen aukeaa ikkuna, jossa näkyy aikaisemmin tehdyn uuden toimialueen puurakenne. Tästä ikkunasta voidaan selata toimialueeseen kuuluvia tietokoneita, organisaatioyksiköitä, ryhmiä, käyttäjiä ja monia muita toimialueen hallintaan liittyviä asioita. Nyt painetaan toimialueen nimen kohdalla, tässä tapauksessa SAMK.local, hiiren oikeanpuoleista painiketta ja valitaan aukeavasta valikosta Uusi (New) ja sieltä organisaatioyksikkö (kuva 2). Valitsemisen jälkeen eteen aukeaa New Object - Organizational Unit -ikkuna, johon kirjoitetaan uuden organisaatioyksikön nimi. Omassa työssäni valitsin nimeksi yksinkertaisesti testiou. Kirjoittamisen jälkeen painetaan OK, jonka jälkeen uuden organisaatioyksikön luominen on valmis ja se voidaan nähdä toimialueen puussa toimialueen SAMK.local objektina.



Kuva 2. Uuden organisaatioyksikön luominen toimialueeseen.

Uusia organisaatioyksiköitä voidaan tehdä samalla tavalla niin monta kuin tarvitaan. Kun organisaatioyksikön luominen on valmis, voidaan jatkaa tekemällä juuri luotuun organisaatioyksikköön uusi käyttäjätili. Uuden käyttäjätilin luominen tapahtuu samassa Aktiivihakemiston Käyttäjät ja Tietokoneet -hallintakonsolissa kuin äsken luotu OU. Painamalla hiiren oikeanpuoleista painiketta sen OU:n kohdalla, mihin käyttäjä halutaan luoda, aukeaa valikko, josta valitaan Uusi ja sieltä Käyttäjä (kuva 3). Nyt tullaan New Object - User -ikkunaan, johon voidaan halutessa kirjoittaa uuden käyttäjän etunimi (First Name), sukunimi (Last Name), nimikirjaimet (Initials) sekä pakollisena tietona nimi, jolla voidaan kirjautua aktiivihakemiston toimialueeseen (User Logon Name). Toimialueena on automaattisesti aikaisemmin luotu SAMK.local. Annoin käyttäjälle kirjautumisnimeksi testikayttaja. Kun halutut tiedot on kirjoitettu, jatketaan painamalla Seuraava (Next). Painamisen jälkeen saavutaan

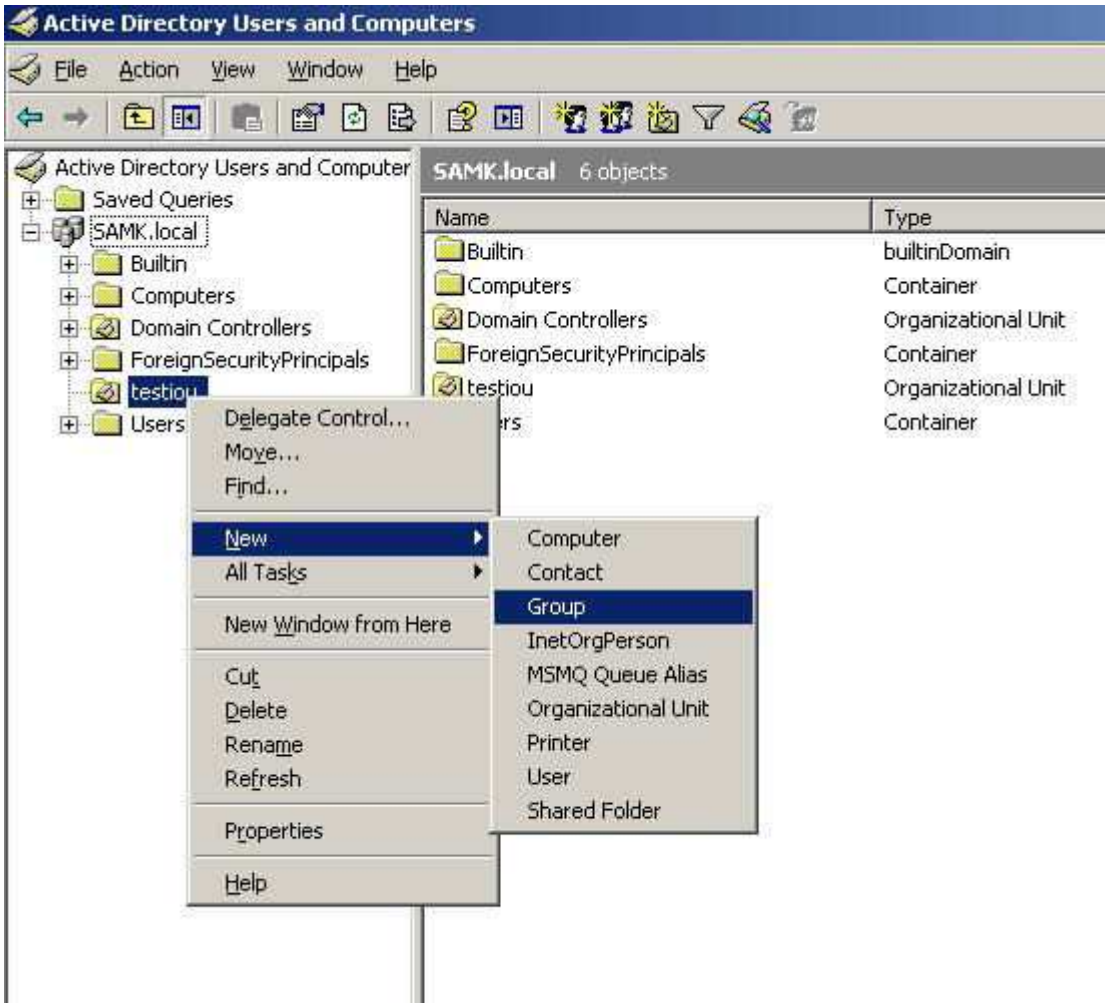
kohtaan, jossa kysytään uudelle käyttäjälle salasanaa. Normaalissa tapauksessa tähän kohtaan kirjoitetaan ainoastaan käyttäjän omassa tiedossa oleva salasana, jota tarvitaan kirjauduttaessa aktiivihakemiston toimialueeseen. Omassa työssäni kaikki tulevat kuitenkin ainoastaan testikäyttöön, joten on syytä käyttää salasanoja, jotka ovat myös jälkeenpäin helposti muistettavissa, niin kuin tässä työssä on aikaisemmissakin vaiheissa käytetty. On myös huomioitava, että palvelimessa on oletuksena päällä asetus (Password Policy), jonka mukaan salasanan täytyy täyttää sille asetetut vaatimukset. Tämä koskee salasanan pituutta, vaikeutta ja salasanojen historiasta riippuvia vaatimuksia. Tuon asetuksen voi myös halutessaan poistaa käytöstä Domain Security Policyn kautta. Uuden käyttäjätilin salasanaksi valitsin testi123. Salasanan kirjoittamisen jälkeen ikkunassa alhaalla on neljä rastitettavaa ruutua. Näistä ensimmäisessä (User must change password at next logon) on jo valmiiksi rasti. Jos ei haluta ensimmäisen kirjautumisen yhteydessä vaihtaa juuri kirjoitettua salasanaa, on tämä ruutu jätettävä tyhjäksi. Tämän jälkeen voidaan jatkaa painamalla Seuraava, jonka jälkeen painamalla valmis (Finish) uuden käyttäjätilin luominen on valmis. Nyt juuri luotu käyttäjä voidaan nähdä toimialueen puurakenteessa kohdassa testiou.



Kuva 3. Uuden käyttäjätilin luominen organisaatioyksikköön.

Uuden käyttäjätilin luomisen jälkeen lisätään organisaatioyksikköön testiou uusi ryhmä, johon lisätään juuri luotu uusi käyttäjä. Uuden ryhmän luominen tapahtuu samalla periaatteella kuin käyttäjän luominen. Painetaan hiiren oikealla painikkeella sen OU:n päällä, johon halutaan tehdä uusi ryhmä ja aukeavasta valikosta valitaan Uusi ja sieltä Ryhmä (kuva 4). Valitsemisen jälkeen aukeaa ikkuna, johon voidaan kirjoittaa uudelle ryhmälle nimi. Jatkoin edellä olevaan tyyliin ja ryhmän nimeksi annoin testiryhma. Nimen kirjoituksen jälkeen painetaan OK, ja uuden ryhmän luominen on valmis. Nyt uusi ryhmä on näkyvissä organisaatioyksikön testiou objektina. Käyttäjän lisääminen juuri luotuun ryhmään tapahtuu yksinkertaisesti painamalla hiiren oikeanpuoleista painiketta testikayttajan päällä ja valitsemalla aukeavasta vali-

kosta Lisää ryhmään (Add to a group), jonka jälkeen ryhmän nimi voidaan joko kirjoittaa tai etsiä luettelosta. Tämän tekemisen jälkeen valitaan OK, jolloin käyttäjä on lisätty juuri luotuun ryhmään testiryhma, ja se näkyy sen ominaisuuksissa (Properties) kohdassa Jäsenet (Members).



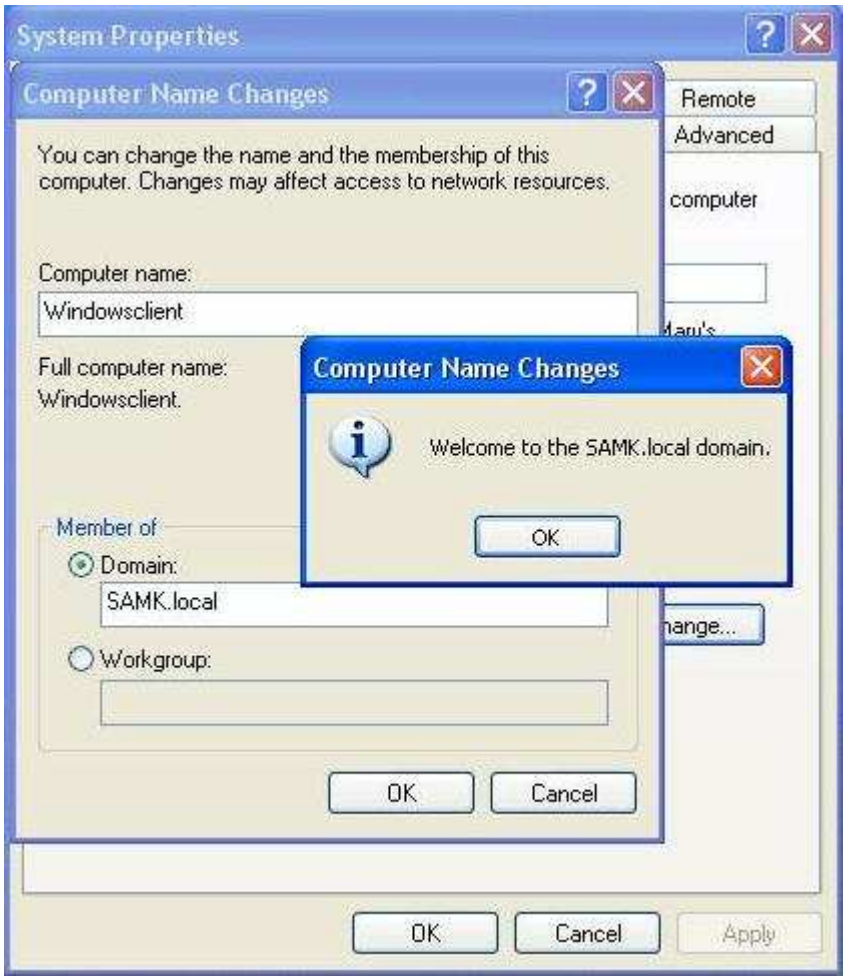
Kuva 4. Uuden ryhmän luominen organisaatioyksikköön.

3.7 Windows-kirjautuminen aktiivihakemistoon

Tällä hetkellä on edetty vaiheeseen, jossa voidaan testata, toimiiko luotu Windows-palvelin oikein ja toimiiko aktiivihakemiston toimialueen ohjauspalvelin niin kuin sen pitäisi. Otetaan käyttöön toinen erillinen Windows-käyttöjärjestelmän sisältävä tietokone, jolla testataan palvelimen toimivuus. Työpöydällä painetaan hiiren oike-

anpuoleista painiketta kohdassa Oma Tietokone ja valitaan sieltä aukeavasta valikosta Ominaisuudet. Ominaisuuksista valitaan Tietokoneen Nimi -välilehti, josta vaihdetaan tietokoneen nimi sellaiseksi kuin halutaan ja liitytään luotuun SAMK.local toimialueeseen. Tämä tapahtuu painamalla alhaalla olevaa Muuta-nappulaa (Change), josta asetetaan tietokoneen nimeksi haluttu, esimerkiksi Windowsclient, sekä ikkunan alalaidasta valitaan kohta Toimialue (Domain) ja syötetään sen ruutuun toimialueen DNS-nimi SAMK.local. Tämän jälkeen kysytään palvelimen Järjestelmänvalvojan salasanaa, jonka antamisen seurauksena saadaan viesti, jonka mukaan tietokone on onnistuneesti liitetty toimialueeseen (kuva 5).

Jos tämä ei onnistu ja saadaan jokin virheilmoitus, voidaan sitä tutkimalla etsiä ratkaisua liittymisen epäonnistumiseen. Muutama asia, jotka täytyy epäonnistumisen varalta tarkistaa, on että käytetty erillinen Windows-kone kuuluu samaan verkkoon kuin palvelin itse. Normaalisti Windows-palvelimen DHCP-palvelin antaa automaattisesti samaan verkkoon kuuluvan IP-osoitteen samaan verkkoon tuleville tietokoneille, näin ollen yhteys palvelimen ja kirjautujan välillä toimii automaattisesti. Tilanteessa, jossa halutaan määrittää verkkoasetukset manuaalisesti ilman DHCP:tä, voidaan IP-osoitteeksi antaa mikä tahansa vapaa osoite, joka kuuluu samaan aliverkkoon. On myös erittäin tärkeää antaa tälle koneelle ensisijaiseksi DNS-palvelimen osoitteeksi Windows-palvelimen IP-osoite. Jos kaikki asetukset ovat muuten kunnossa, näiden jälkeen toimialueeseen liittymisen pitäisi onnistua. Toimialueeseen liittämisen jälkeen kone täytyy käynnistää uudelleen, jonka jälkeen kirjautumisikkunassa voidaan toimialuevalikosta nähdä toimialue SAMK. Nyt tähän toimialueeseen voidaan kirjautua luodulla tunnuksella testikayttaja ja salasanalla testi. Tämän onnistuessa voidaan todeta aktiivihakemiston ja sen toimialueen ohjauspalvelimen toimivan aivan kuten sen kuuluisikin. Nyt voidaan myös nähdä Windows-palvelimelta Active Directory Users And Computers -hallintakonsolista uusi toimialueeseen liittynyt tietokone Windowsclient kohdassa Computers.

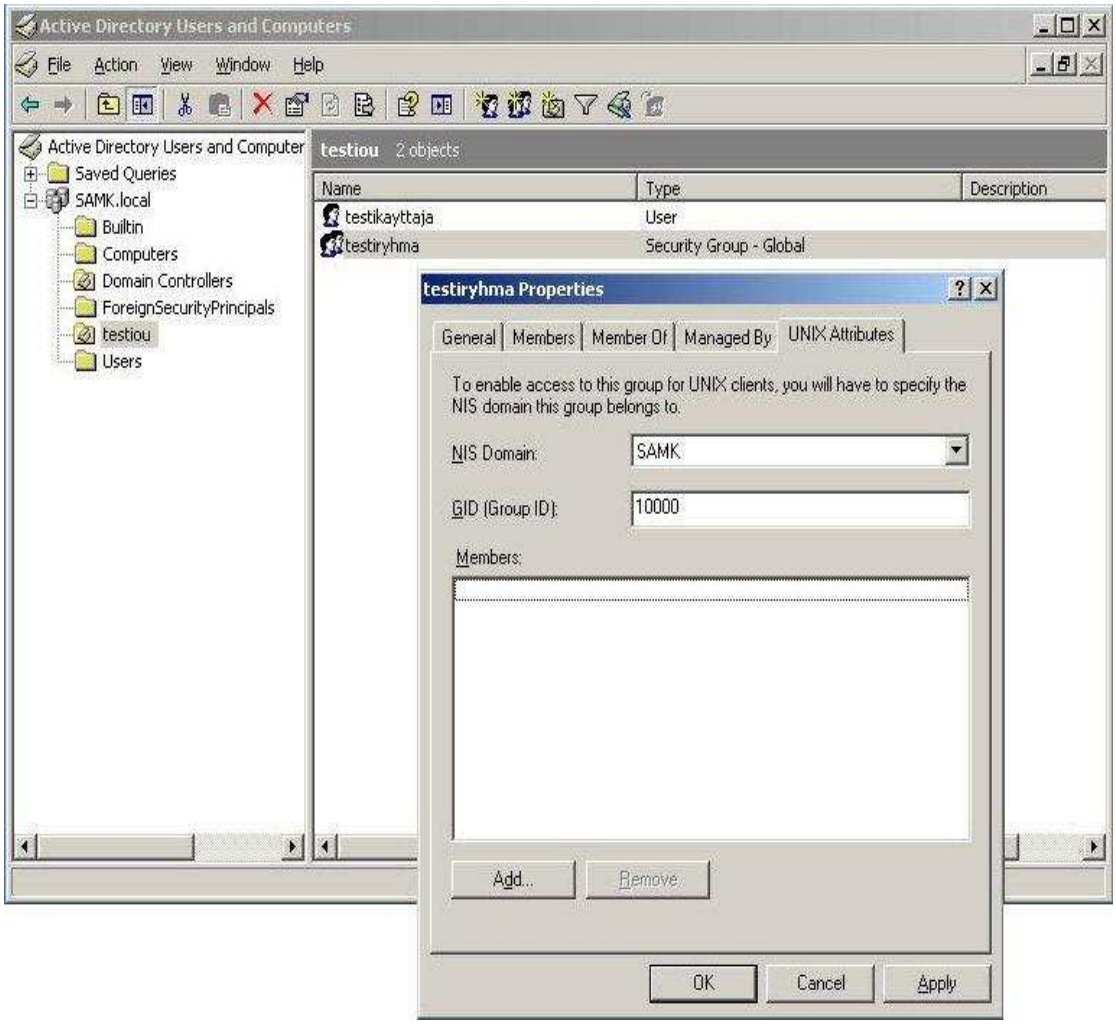


Kuva 5. Windows-koneen liittäminen aktiivihakemiston toimialueeseen.

4 LINUX-AUTENTIKOINTI AKTIIVIHAKEMISTOSSA

4.1 UNIX-ryhmä ja -käyttäjä aktiivihakemistossa

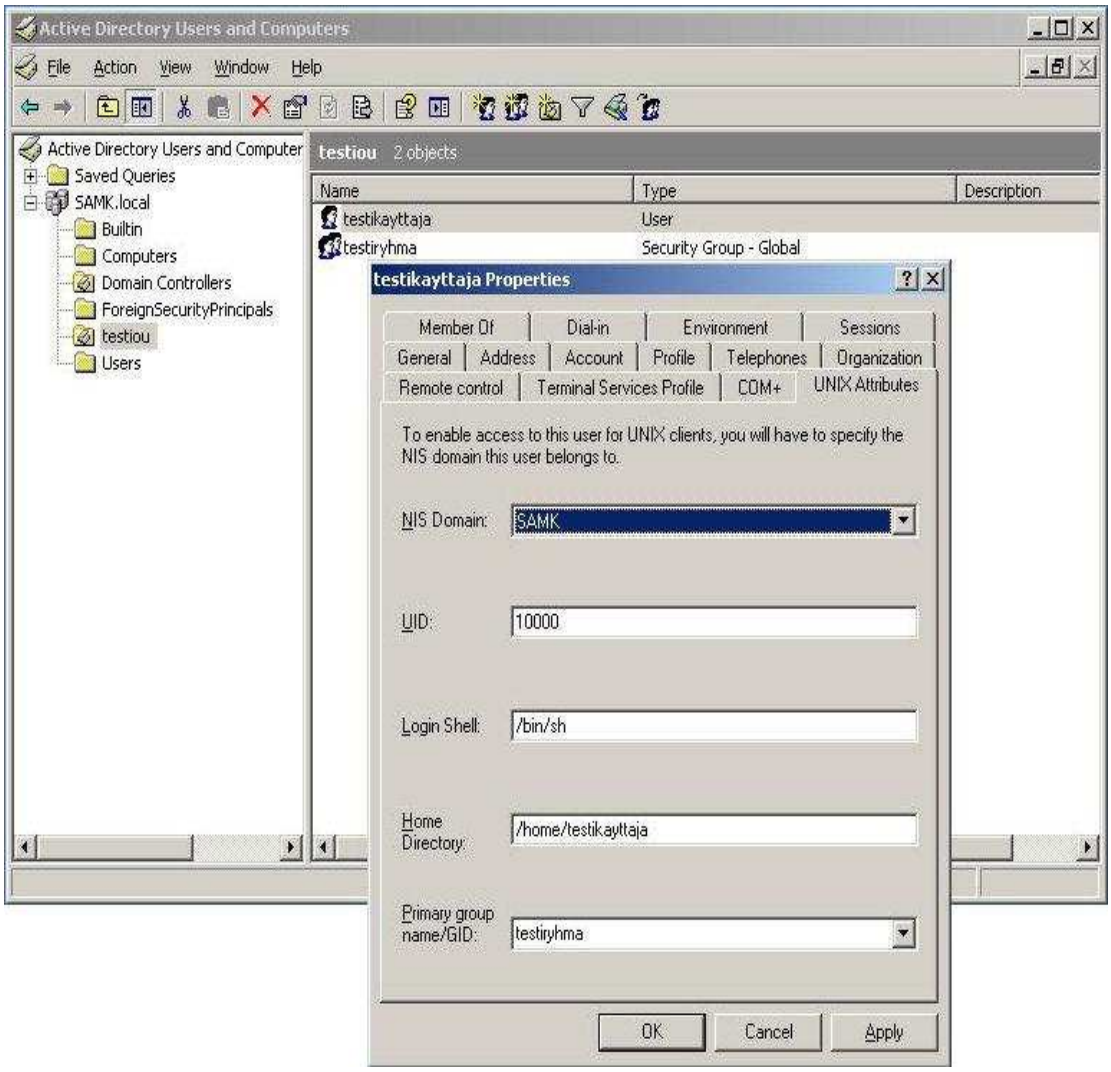
Kun aktiivihakemiston valmistelut ovat valmiita, voidaan jatkaa tekemällä objekteista testiryhma ja testikayttaja UNIX-yhteensopivia. Jatketaan samassa Aktiivihakemiston Käyttäjät ja Tietokoneet -hallintakonsolissa. Selataan toimialueen puuta kohtaan testiou, josta kaksoisklikataan juuri tehtyä ryhmää testiryhma. Eteen aukeaa ikkuna, josta nähdään ryhmän tiedot ja päästään haluttaessa muokkaamaan siihen liittyviä asetuksia. Ikkunassa nähdään oikealla oleva UNIX-Attributes -välilehti. Normaalissa Microsoft Windows Server 2003 -käyttöjärjestelmässä ei tätä ominaisuutta ole, vaan kyseessä on välilehti, joka tulee työssä aikaisemmin asennetun Identity Management for UNIX -komponentin ansiosta näkyviin. Mennään tuohon välilehteen. Välilehdestä mennään NIS Domain -alasvetovalikkoon. Tästä valikosta valitaan NIS-toimialue, johon ryhmän halutaan kuuluvan. Valitaan valikosta toimialue eli SAMK. Valitsemisen jälkeen aktiivihakemisto automaattisesti antaa tälle ryhmälle tunnisteen, Group ID:n (GID). Testiryhma sai tunnisteekseen 10000, jolloin kyseinen ryhmä tunnetaan myös UNIX-ryhmänä (kuva 6). UNIX-Attributes-välilehdestä nähdään myös kaikki jäsenet (Members), jotka kuuluvat kyseiseen UNIX-ryhmään. Tällä hetkellä ryhmässä ei vielä ole UNIX-jäseniä, jotka siihen kuuluisivat. Hyväksytään tehdyt valinnat painamalla OK, ja ryhmän UNIX-käyttöönotto on valmis. (Moskowitz & Boutell 2005, 170.)



Kuva 6. Aktiivihakemiston toimialueessa sijaitsevan ryhmän UNIX-käyttöönotto.

Ryhmän UNIX-käyttöönoton jälkeen voidaan suorittaa sama toimenpide käyttäjätilille. Selataan jälleen testiou kohtaan, josta kaksoisklikataan käyttäjää testikayttaja. Tästä aukeaa ikkuna, josta nähdään käyttäjää koskevia tietoja ja haluttaessa voidaan muokata käyttäjää koskevia asetuksia. Ikkunassa oikealla on samanlainen UNIX-Attributes-välilehti kuin oli aktiivihakemiston ryhmällä. Mennään tuohon välilehteen, josta mennään taas NIS Domain -alasvetovalikkoon. Valikosta valitaan NIS-toimialue, johon käyttäjän halutaan kuuluvan. Valitaan taas toimialue SAMK, jonka jälkeen aktiivihakemisto automaattisesti antaa käyttäjälle tunnisteen, User ID:n (UID). Käyttäjä sai tunnisteekseen 10000, jonka jälkeen käyttäjä tunnetaan myös

UNIX-käyttäjänä (kuva 7). Hyväksytään valinnat painamalla OK ja käyttäjän UNIX-käyttöönotto on valmis. (Moskowitz ym. 2005, 170.)



Kuva 7. Aktiivihakemiston toimialueessa sijaitsevan käyttäjän UNIX-käyttöönotto.

UNIX-Atrributes-välilehdestä nähdään myös kirjautumisessa käytettävä shell. Oletuksena on käytössä Bourne Shell (sh), mikä on yleisesti käytössä oleva shell UNIX-tileille. Sen alapuolella on tieto käyttäjälle testikayttaja luodusta kotihakemiston (Home Directory) sijainnista. Kotihakemiston osoittamaan sijaintiin talletetaan UNIX-käyttäjän tallentamat tiedostot Linux / UNIX -pohjaisista käyttöjärjestelmistä. Kotihakemiston sijainnin alapuolella nähdään ryhmä, johon testikayttaja ensisijaises-

ti kuuluu (Primary group name/GID). Jos tämä kohta on jostain syystä tyhjä tai osoittaa väärään ryhmään, se on syytä vaihtaa tässä vaiheessa oikeaksi virheiden ehkäisemiseksi. Jos ryhmää ei ole tehty UNIX-ryhmäksi, ei se myöskään näy tässä kohdassa, eikä käyttäjää voida lisätä haluttavaan UNIX-ryhmään. Kun käyttäjä on tehty UNIX-yhteensopivaksi ja sen ryhmä on valittu, pitäisi käyttäjän näkyä myös ryhmän tiedoissa UNIX-Attributes -välilehdellä kohdassa jäsenet (Members).

4.2 Dirsearch

Kun aktiivihakemiston toimialueen organisaatioyksikön ryhmä ja sen käyttäjä on tehty UNIX-yhteensopiviksi, on aika jatkaa eteenpäin ja luoda yleinen käyttäjä, joka edesauttaa UNIX/Linux-käyttäjiä kirjautumaan Windows-aktiivihakemistoon. Tämä on yleinen käyttäjätili, joka ei kuulu mihinkään organisaatioyksikköön tai ryhmään. Sen avulla UNIX/Linux-käyttäjät voivat etsiä ja käyttää hyväksi aktiivihakemistoa kirjautumisen onnistumiseksi. Voi aluksi tuntua kovin turvattomalta luoda tällainen käyttäjä, mutta loppujen lopuksi kyseisellä käyttäjällä ei ole muita oikeuksia kuin tehdä LDAP-tiedusteluja. Tämä erityinen tili autentikoi käyttäen yksinkertaista autentikointia. Yksinkertainen autentikointi lähettää käyttäjän tiedot selkokielisenä. Tämän takia autentikaatioprosessi vaatii lisäturvaa salatakseen lähettämiään tietoja. Tämä salaaminen tehdään vielä myöhemmin työn edetessä. Nyt kuitenkin jatketaan tekemällä tuo yleinen käyttäjätili. Jatketaan edelleen aktiivihakemiston Käyttäjät ja tietokoneet -hallintakonsolissa. Selataan toimialueen puussa kohtaan, jossa lukee Käyttäjät (Users). Jälleen painetaan sen päällä hiiren oikeanpuoleista painiketta ja valitaan aukeavasta valikosta Uusi ja sieltä Käyttäjä, jolloin eteen aukeaa opastus uuden käyttäjän luomiseksi. Tälle uudelle käyttäjälle voidaan antaa etu- tai sukunimeksi mitä tahansa, kunhan kirjautumisnimen kohdalle kirjoitetaan jokin tilanteeseen sopiva, esimerkiksi dirsearch. Dirsearchin sijaan käyttäjälle voidaan antaa millainen nimi tahansa, mutta tässä tapauksessa kyseinen nimi tuntuu loogiselta, koska kyseessä on käyttäjä, joka voi etsiä ja käyttää hyväksi aktiivihakemiston käyttäjätilejä. Jälleen annetaan salasanaksi jokin sellainen, joka muistetaan helposti myöhemmin työn edetessä. Jatkoin vanhaa kaavaa ja annoin salasanaksi testi123. Lopuksi hyväksytään uuden käyttäjän luominen painamalla Finish. Käyttäjän luomisen

jälkeen kaksoisklikataan juuri tehtyä käyttäjää dirsearch. Eteen aukeaa sama ikkuna kuin testikayttajan kohdalla. Valitaan välilehdistä kohta tili (Account), josta on syytä rastittaa kaksi kohtaa. Merkitään rasti kohtiin Käyttäjä ei voi vaihtaa salasanaa (User cannot change password) ja Salasana ei koskaan vanhene (Password never expires). Nyt aktiivihakemistoon käsiksi pääsemiseksi tehty käyttäjä on luotu ja se nähdään toimialueen puussa kohdassa Käyttäjät. (Moskowitz ym. 2005, 173.)

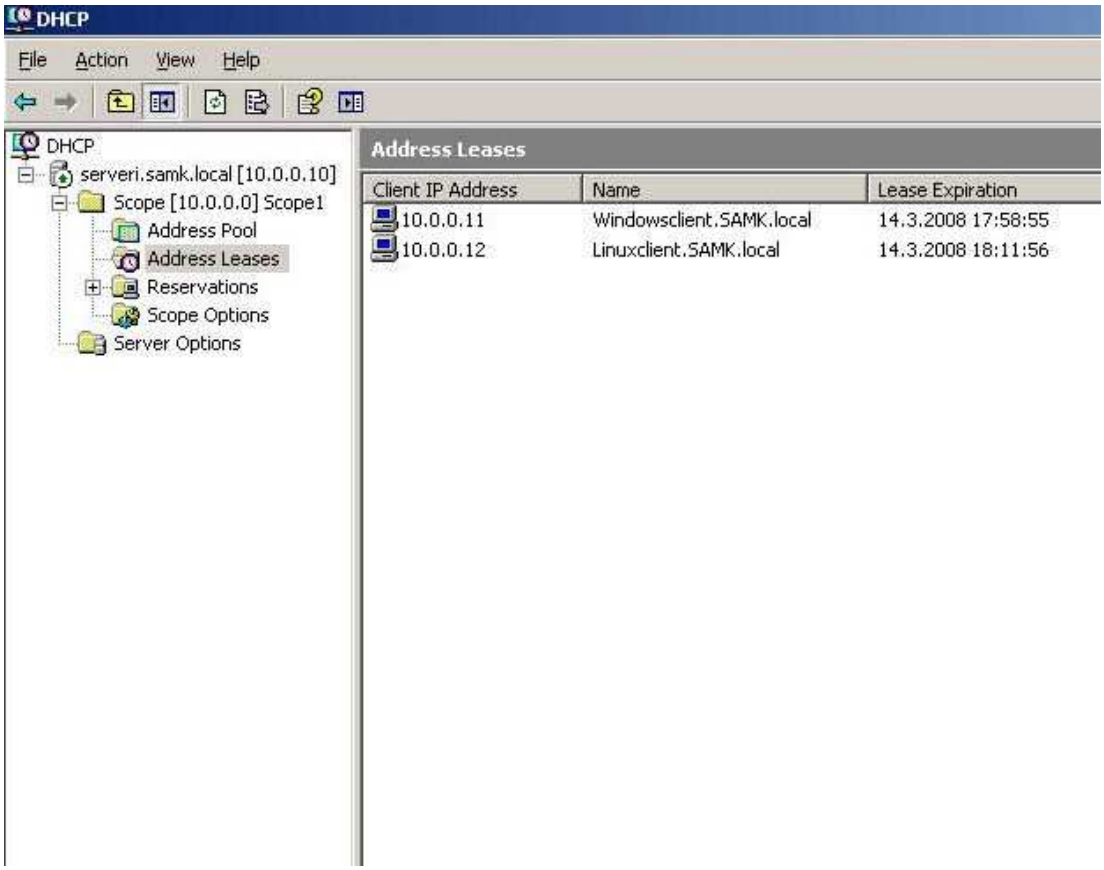
5 LINUX-AUTENTIKOINTI FEDORASSA

5.1 Verkkoasetukset

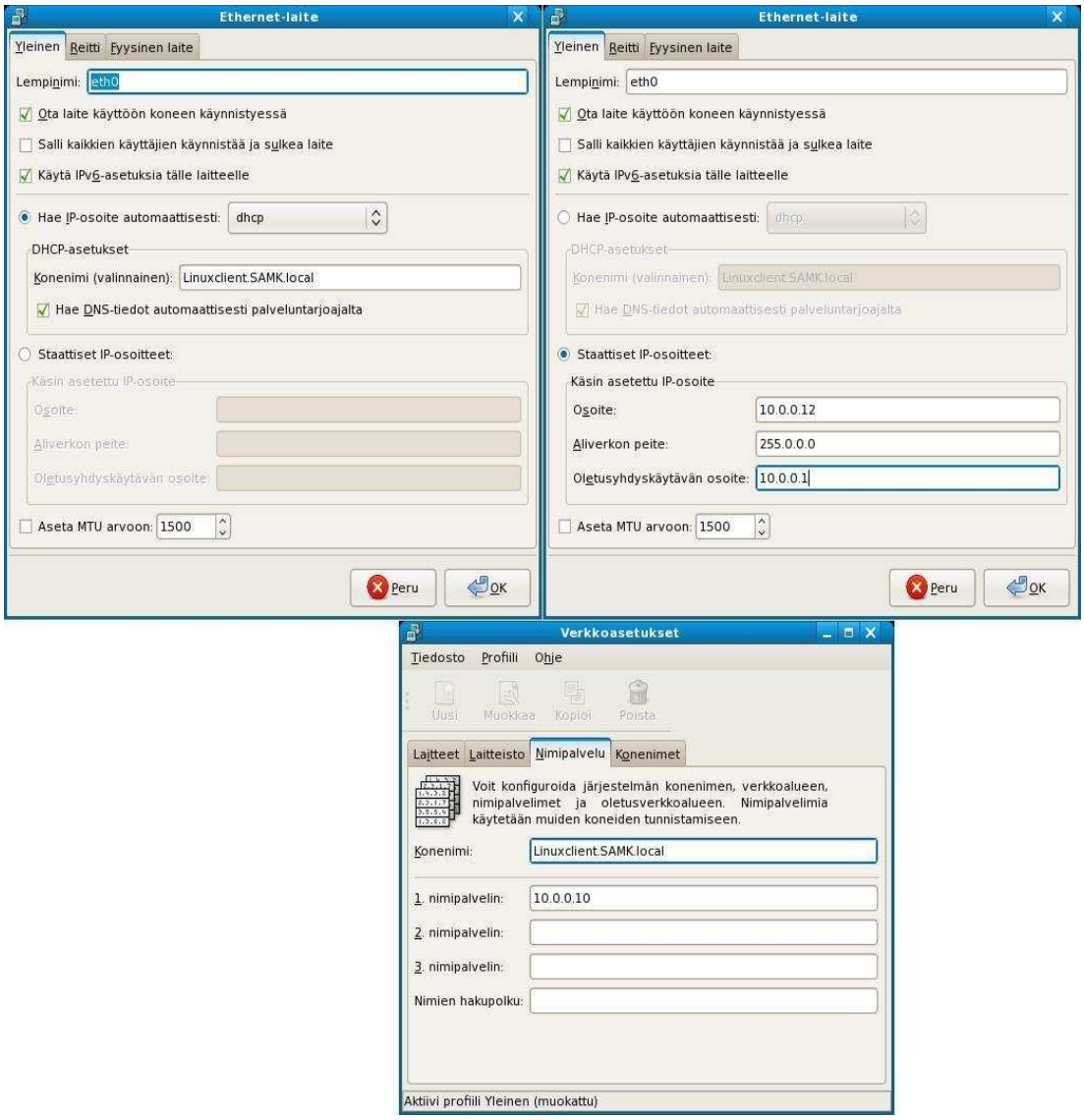
Kun kaikki valmistelut Windows Server -käyttöjärjestelmässä ovat valmiita, siirrytään valmistelemaan työn alussa asennettua Linuxia aktiivihakemistoon kirjautumista varten. Tämän koneen tarkoitus on ainoastaan olla auttavana osapuolena UNIX/Linux-käyttäjien kirjautumisessa aktiivihakemistoon käyttäen LDAP-autentikointia. Ensimmäiseksi tarkistetaan, että verkkoasetukset on oikein määritelty. Varsinkin jos Windows Server -palvelimeen ei ole asennettu DHCP-palvelinta, täytyy verkkoasetukset määrittää manuaalisesti niin, että Windows Server -palvelin ja Linux-tietokone ovat samassa verkossa. Vaikka Windows-palvelimella on oletuksena käytössä DHCP, on syytä varmistaa molempien koneiden sijaitseminen samassa verkossa. Linux-käyttöjärjestelmissä järjestelmänvalvojana (Administrator) toimii käyttäjä root (juuri), samoin kuin Windows-käyttöjärjestelmissä saman asian ajaa selkokielisesti Järjestelmänvalvoja (Administrator). Kun aikaisemmin asennettuun Fedoraan on kirjauduttu root-tunnuksilla, valitaan ylhäältä Windows-käyttöjärjestelmän kaltaisesta tehtäväpalkista Järjestelmä. Tästä valikosta päästään tekemään suurimmat järjestelmään liittyvät asetukset, valitaan sieltä Ylläpito ja edelleen Verkko, josta päästään muuttamaan verkon asetuksia. Verkkoasetusten ikkunassa on neljä välilehteä. Näistä mennään ensimmäiseen eli Laitteet-välilehteen. Tässä nähdään luettelo verkkolaitteista, joita Linux-kone sisältää. Valitaan listasta koneen käyttämä verkkokortti, jota kaksoisklikkaamalla eteen aukeavat verkkokortin asetukset. Painetaan kohtaan Staattiset IP-osoitteet ja annetaan Osoite kenttään IP-osoite, joka kuuluu samaan verkkoon kuin aikaisemmin asetettu Windows-palvelimen staattinen IP-osoite. Palvelimen osoitteen ollessa 10.0.0.10 ja Windows-koneen 10.0.0.11 voidaan jälleen antaa seuraava vapaana oleva osoite. Tässä tapauksessa seuraava osoite olisi 10.0.0.12 aliverkon peitteen ollessa 255.0.0.0. Oletusyhdyskäytävän osoitteeksi annetaan sama kuin Windows-koneelle (kuva 9). Jos käytössä on DHCP-palvelin, voidaan kaikki asetukset jättää oletuksena olevaan tilaan, jolloin IP-osoite haetaan automattisesti. DHCP-asetuksien alla on ruutu, johon voidaan kirjoittaa konenimi, joka koneelle halutaan antaa (kuva 9). Tähän kirjoitetaan Linuxclient.SAMK.local. Verk-

kolaitteen asetuksien hyväksymisen jälkeen palataan takaisin ikkunaan Verkkoasetukset. Nyt valitaan kolmantena oleva Nimipalvelu-välilehti. Jos koneelle on annettu manuaalisesti staattinen IP-osoite, voidaan Konenimi-kohtaan antaa koneelle haluttava nimi. Vaikka käytettäisiin asetusta, jolloin IP-osoite haetaan automaattisesti, voidaan tähän kohtaan silti kirjoittaa Linux-koneelle nimi, verkkoalue, nimipalvelimien (DNS) osoitteet sekä oletusverkkoalue. Jotta Linux-kone saataisiin kirjautumaan aktiivihakemiston toimialueeseen SAMK.local, annetaan sille sitä vastaava nimi kuten edellä DHCP-asetuksiin. Koneen nimen alku voi olla mikä tahansa, kunhan nimi loppuu siihen toimialueeseen, mihin halutaan kirjautua, esimerkiksi Linux-client.SAMK.local. Nimen antamisen jälkeen jatketaan nimipalvelimen osoitteeseen. DNS-osoitteeksi voidaan antaa Windows-palvelimen IP-osoite 10.0.0.10 (kuva 9). Toisen ja kolmannen osoitteen sekä nimien hakupolun sarakkeet voi jättää täyttämättä. Tietenkin jos käytössä on vaihtoehtoinen DNS-palvelin, jota on tarkoitus käyttää, jos ensimmäinen ei jostain syystä ole käytettävissä, voidaan tähän kohtaan antaa vaihtoehtoiset osoitteet. Kun Linux-koneelle on annettu IP-osoite (staattinen tai dynaaminen), konenimi ja DNS-osoite, voidaan hyväksyä uudet verkkoasetukset painamalla ylhäältä Tiedosto-valikosta Tallenna, jonka jälkeen voidaan jatkaa LDAP-asetuksiin.

Jos verkossa on käytetty DHCP-palvelinta IP-osoitteiden automaattiseen hakuun, voidaan palvelimen antamat IP-osoitteiden lainat nähdä palvelimelta kohdasta DHCP-palvelin (DHCP Server) ja sieltä selaamalla kohtaan Address Leases (kuva 8). Sieltä nähdään IP-osoitetta vastaava koneen nimi sekä lisätietoina lainan loppumisaika (Lease Expiration) ja osoitteen yksilöllinen tunnus (Unique ID).



Kuva 8. DHCP-palvelimen antamat IP-osoitteet.

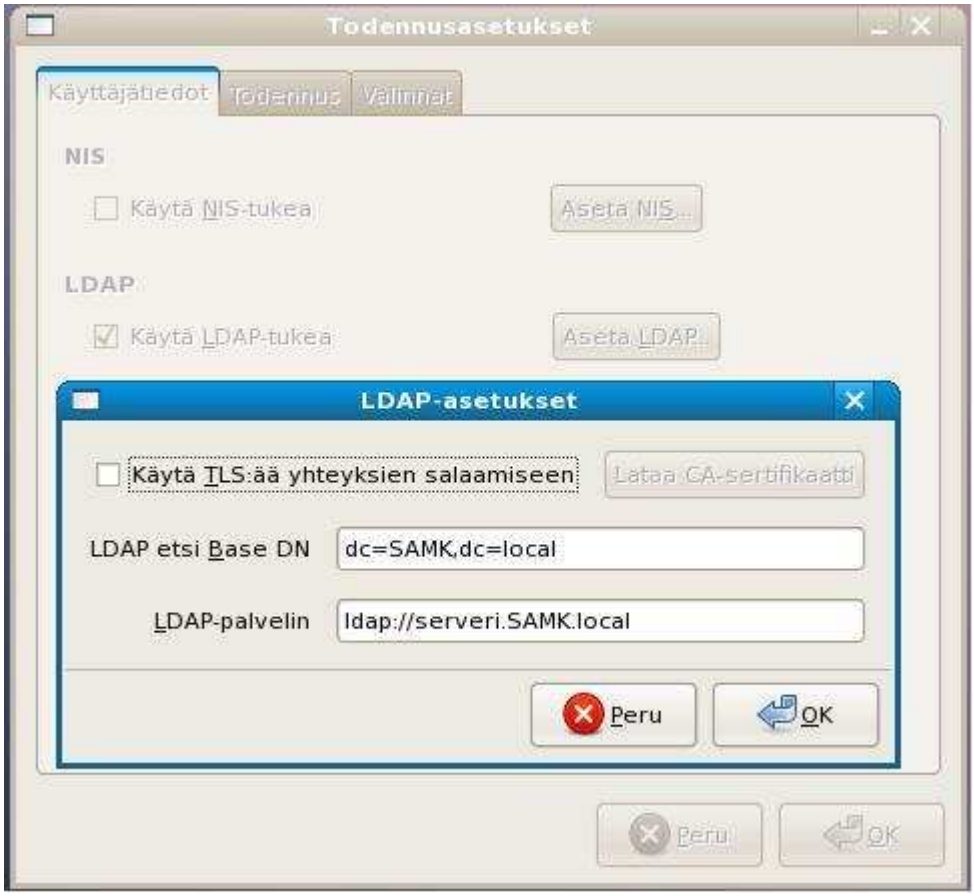


Kuva 9. Käytettävän Linux-koneen dynaamiset ja staattiset verkkoasetukset.

5.2 LDAP

Jotta käytössä oleva Linux osaisi tehdä LDAP-kyselyitä, on käytettävä Fedoran sisäänrakennettua autentikointityökalua (Authentication Tool) LDAP-asetuksien määrittämiseksi. Tämä tapahtuu menemällä samaan Järjestelmä-valikkoon kuin edellisessäkin kappaleessa. Tällä kertaa valikosta valitaan Ylläpito ja sieltä eteenpäin kohta, jossa lukee Todennus. Tämän valitsemisen jälkeen eteen aukeaa Todennusasetukset-ikkuna. Rastitetaan ensimmäisestä eli Käyttäjätiedot-välilehdestä kohta Käytä

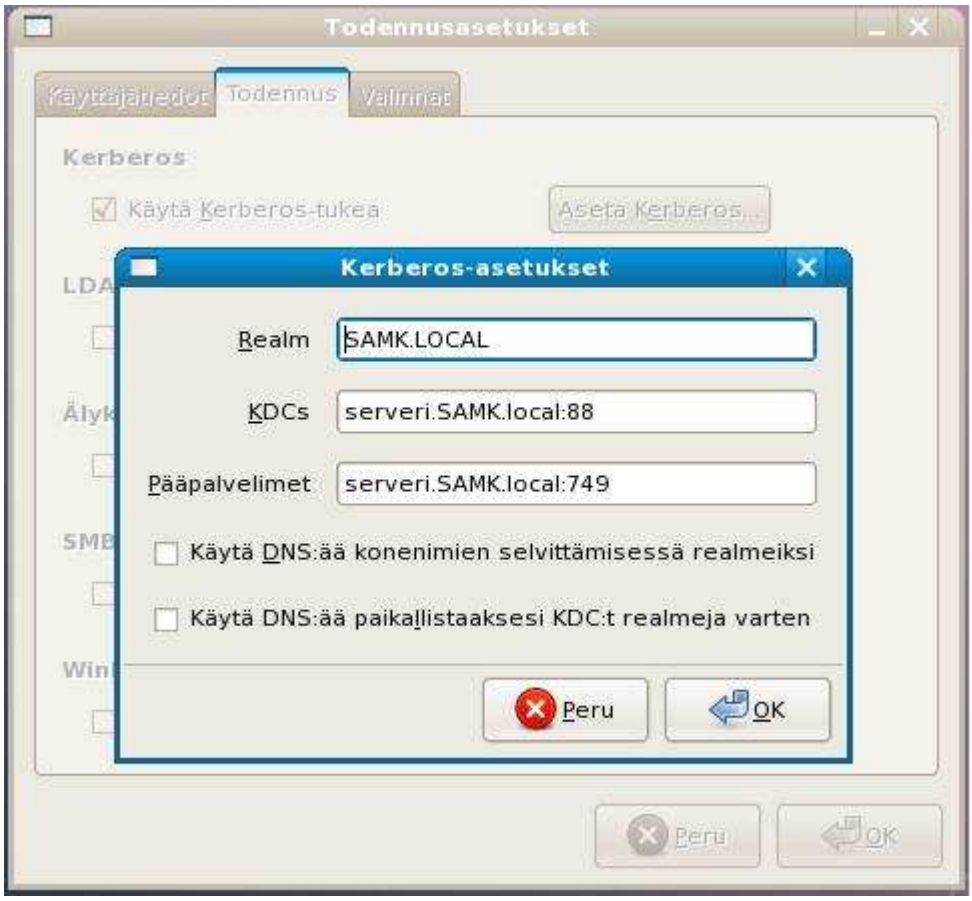
LDAP-tukea. Rastituksen jälkeen painetaan tekstin oikealla puolella olevaa Aseta LDAP… -painiketta, josta päästään LDAP-asetukset-ikkunaan. Tästä ikkunasta on täytettävä kaksi kohtaa. Ensimmäiseksi kohtaan LDAP etsi Base DN kirjoitetaan aktiivihakemiston dn-nimi (distinguished name). Nimeksi työssäni tuli dc=SAMK,dc=local, jossa kohta SAMK tarkoittaa toimialuetta ja local sen osoitteen päätettä. Seuraavaksi kohtaan LDAP-palvelin on tarkoitus antaa yksinkertaisesti Windows-palvelimen LDAP-palvelimen osoite. Työssäni osoite oli ldap://serveri.SAMK.local/. Osoitteessa serveri osoittaa käytetyn toimialueen ohjauspalvelimen nimeen ja pääte SAMK.local toimialueeseen. Näiden kirjoituksen jälkeen LDAP-asetukset on määritelty (kuva 10). Hyväksytään asetukset valitsemalla OK ja palataan Todennusasetukset -ikkunaan. Seuraavassa vaiheessa määritetään Kerberos-autentikoinnin asetukset.



Kuva 10. LDAP-asetuksien määrittäminen.

5.3 Kerberos

Nyt on aika konfiguroida käytössä oleva Linux-kone käyttämään kerberos-autentikointia Windows-palvelimen kanssa. Käytössä oleva Fedora tekee tämän määrittämisen varsin helpoksi. Jatketaan Todennusasetukset-ikkunassa, mutta tällä kertaa valitaan keskimmäinen eli Todennus-välilehti. Tässä välilehdessä rastitetaan ruutu kohdassa Käytä Kerberos-tukea. Rastituksen jälkeen painetaan Aseta Kerberos… -painiketta ja päästään Kerberos-asetukset-ikkunaan. Kerberos-asetuksissa täytetään kaikki kolme kohtaa. Ensimmäiseksi Realm-ruutuun täytetään aktiivihakemiston toimialueen osoite (SAMK.LOCAL) ja tässä kohdassa täytyy muistaa kirjoittaa nimi kokonaisuudessaan isoilla kirjaimilla. Jos osoite on kirjoitettu käyttäen pieniä kirjaimia, aivan kuten muissa työn vaiheissa, ei Kerberos-autentikointi yksinkertaisesti toimi. Seuraavaan eli KDCs-ruutun kirjoitetaan aktiivihakemiston toimialueen ohjauspalvelimen osoite (serveri.SAMK.local). Viimeiseen eli Pääpalvelimet-ruutuun, annetaan käytettävän pääpalvelimen osoite. Pääpalvelin tässä tapauksessa on toimialueen ohjauspalvelin, joten annetaan sen osoite. Näiden tietojen syöttämisen jälkeen Kerberos-autentikoinnin asetukset on määritelty (kuva 11). Ikkunan alalaidassa olevat kaksi rastitettavaa ruutua voidaan jättää tyhjiksi, koska annetut osoitteet olivat suoraan DNS-nimiä. Näiden avulla koneen ei tarvitse itse etsiä IP-osoitteita vastaavia DNS-nimiä. Voidaan hyväksyä asetukset painamalla OK ja Todennusasetukset-ikkunasta poistutaan painamalla OK. (Moskowitz ym. 2005, 174.)



Kuva 11. Kerberos-autentikoinnin asetuksien määrittäminen.

5.4 Ldap.conf

Kun LDAP-asetukset ja Kerberos-autentikointi ovat kunnossa, on aika siirtyä muokkaamaan Linux-koneessa sijaitsevaa ldap.conf -tiedostoa. Aktiivihakemistossa toimialueen ohjauspalvelin vastaa sille esitettyihin LDAP-kyselyihin. Oletuksena aktiivihakemisto ei salli nimettömiä LDAP-tiedusteluja. Tämä tarkoittaa sitä, että käyttäjien on kirjauduttava sisään aktiivihakemiston LDAP-käyttöliittymään aktiivihakemiston tuntemalla käyttäjätunnuksella ja salasanalla. Tässä vaiheessa käytetään hyväksi aikaisemmin luotua dirsearch-käyttäjätiliä. Sen tarkoitus on antaa oma LDAP dn-nimi (distinguished name) tarvittaessa, jotta päästään käsiksi aktiivihakemistoon. Tämän toimimiseksi täytyy ldap.conf -tiedoston sisältöä muokata tarkoitukseen sopivaksi. Toisin sanoen, ldap.conf -tiedostossa kerrotaan Linux-koneelle, mitä attribuutteja

käyttää Microsoft Windows Server 2003 R2 -version kanssa keskusteluun. (Moskowitz ym. 2005, 175.)

Tässä vaiheessa on syytä mainita, että jos käytössä on Identity Management for UNIX -komponentin sijaan Services for UNIX (SFU) 3.5 -komponentti, täytyy ldap.conf -tiedoston muokkaamiseen käyttää eri attribuutteja kuin tässä työssä on käytetty. Moskowitzin ja Boutellin kirjassa on selvitetty attribuutit, joita käytetään, jos on käytössä SFU-komponentti, ja kirjan jatko-osassa Wep Appendixissa on erikseen kerrottu, mitä attribuutteja käyttää Windows Server 2003 R2 -käyttöjärjestelmän kanssa, jota on laajennettu käyttäen Identity Management for UNIX -komponenttia.

Linux-koneella ldap.conf -tiedosto löydetään kaksoisklikkaamalla työpöydältä Tietokone-kuvaketta. Tämän jälkeen valitaan Tiedostojärjestelmä, josta mennään kansioon /etc ja sieltä avataan ldap.conf-tiedosto. Käytettäessä Fedorassa Gnome-työpöytäympäristöä tiedosto aukeaa automaattisesti Gedit-tekstinkäsittelyohjelmalla. Tällä ohjelmalla voidaan muokata tiedostossa olevia rivejä aivan kuten Windows-käyttöjärjestelmässä käytettävällä muistiolla. Tiedostossa #-merkillä merkityt rivit ovat tiedoston kommentteja ja ilman kyseistä merkkiä olevat rivit ovat tiedostossa annettuja komentoja. Alkuperäisessä ldap.conf-tiedostossa ovat melkein kaikki rivit kommentteina, ainoastaan muutama löytyy varsinaisina komentoina. Rivit jotka ldap.conf-tiedostoon pitää lisätä tai muokata kommenteista, ovat seuraavat:

binddn cn=dirsearch,cn=Users,dc=SAMK,dc=local
bindpw testi123

nss_base_passwd dc=SAMK,dc=local
nss_base_shadow dc=SAMK,dc=local
nss_base_group dc=SAMK,dc=local

nss_map_objectclass posixAccount user
nss_map_objectclass shadowAccount user

nss_map_attribute uid sAMAccountName
nss_map_attribute uidNumber uidNumber
nss_map_attribute gidNumber gidNumber
nss_map_attribute loginShell loginShell *
nss_map_attribute gecos name *
nss_map_attribute homeDirectory unixHomeDirectory

nss_map_objectclass posixGroup group

nss_map_attribute uniqueMember member
nss_map_attribute cn sAMAccountName *

pam_login_attribute sAMAccountName

pam_filter objectcategory=User *

uri ldap://serveri.SAMK.local/
base dc=SAMK,dc=local

(Moskowitz & Boutell 2007, 14-15.)

Kaksi viimeistä riviä ovat automaattisesti tiedostossa jo valmiina. Ne eivät sijaitse tiedoston lopussa, vaan päätin itse muokata tiedostoa siten, että kaikki tehtävät muutokset siirsin tiedoston loppuun tilanteen selventämiseksi. Tehdessäni aikaisemmin todennusasetuksia nämä kaksi riviä syntyivät automaattisesti uusien asetuksien hyväksymisen jälkeen. On samantekevää, lisääkö nämä kaikki tarvittavat rivit tiedoston loppuun itse vai etsiikö jokaisen rivin erikseen kommentteina olevista riveistä ja muokkaa niitä. Itse näin parhaaksi lisätä jokaisen rivin tiedoston loppuun, jolloin tiedoston sisältö jäi selkeämmäksi. Edellä olevaan listaan on myös lisätty muutama rivinvaihto, jotta sitä olisi helpompi lukea. Ristiriitaisuuksien estämiseksi on kuitenkin suositeltavaa selata tiedoston sisältö alusta loppuun läpi ja tarkistaa, etteivät listassa esiintyvät rivit esiinny siellä jo valmiina komentoina ilman etumerkkiä. Listassa tähdellä (*) merkityt rivit eivät löydy tiedoston sisällöstä ollenkaan edes kommentteina, joten ne täytyy lisätä itse kirjoittamalla vaikka tiedoston loppuun. Muokattaessa ldap.conf-tiedostoa on myös huomioitava komennoissa erittäin tarkkaan isojen ja pienten kirjaimien paikat. Jos tiedostoa ei ole muokattu täysin oikein edellä olevan listan mukaan, eivät Linuxilla tehtävät LDAP-kyselyt yksinkertaisesti toimi. Kun tiedoston muokkaaminen on valmis, voidaan jatkaa kotihakemiston tekemiseen Linuxin käyttäjille.

5.5 Kotihakemiston luominen

Kun kaikki valmistelut LDAP-kyselyille ja Kerberos-autentikoinnille ovat valmiita, on vielä yksi askel ennen kuin voidaan kirjautua aktiivihakemistoon Linuxin kautta. Kun uusi käyttäjä kirjautuu tietylle työasemalle ensimmäistä kertaa, sillä ei ole kotihakemistoa, jota käyttää aktiivihakemistossa. Tätä varten on luotava käyttäjälle uusi kotihakemisto. Käyttäjällä on kolme tapaa kirjautua Linux-koneella, joten on tehtävä muutoksia kolmeen tiedostoon samassa Linux-koneessa kuin edellisissä kohdissa tehdyt asetukset ja muutokset. Nämä kolme tapaa, joilla käyttäjä voi kirjautua, ovat joko komentopäätteeltä (shell), salatulta komentopäätteeltä (ssh) tai gnome-työpöytäympäristön kautta. Nyt kotihakemiston tekemiseksi on muokattava näihin kolmeen kirjautumistapaan viittaavia tiedostoja. Tämä tapahtuu selaamalla root-käyttäjänä tietokoneelta kansioon /etc/pam.d/. Kyseisessä kansiossa muokattavat tiedostot ovat login, sshd ja gdm. Jokaiseen näihin tiedostoihin lisätään tiedoston loppuun seuraava rivi:

session required pam_mkhomedir.so skel=/etc/skel umask=0077

(Moskowitz ym. 2005, 179.)

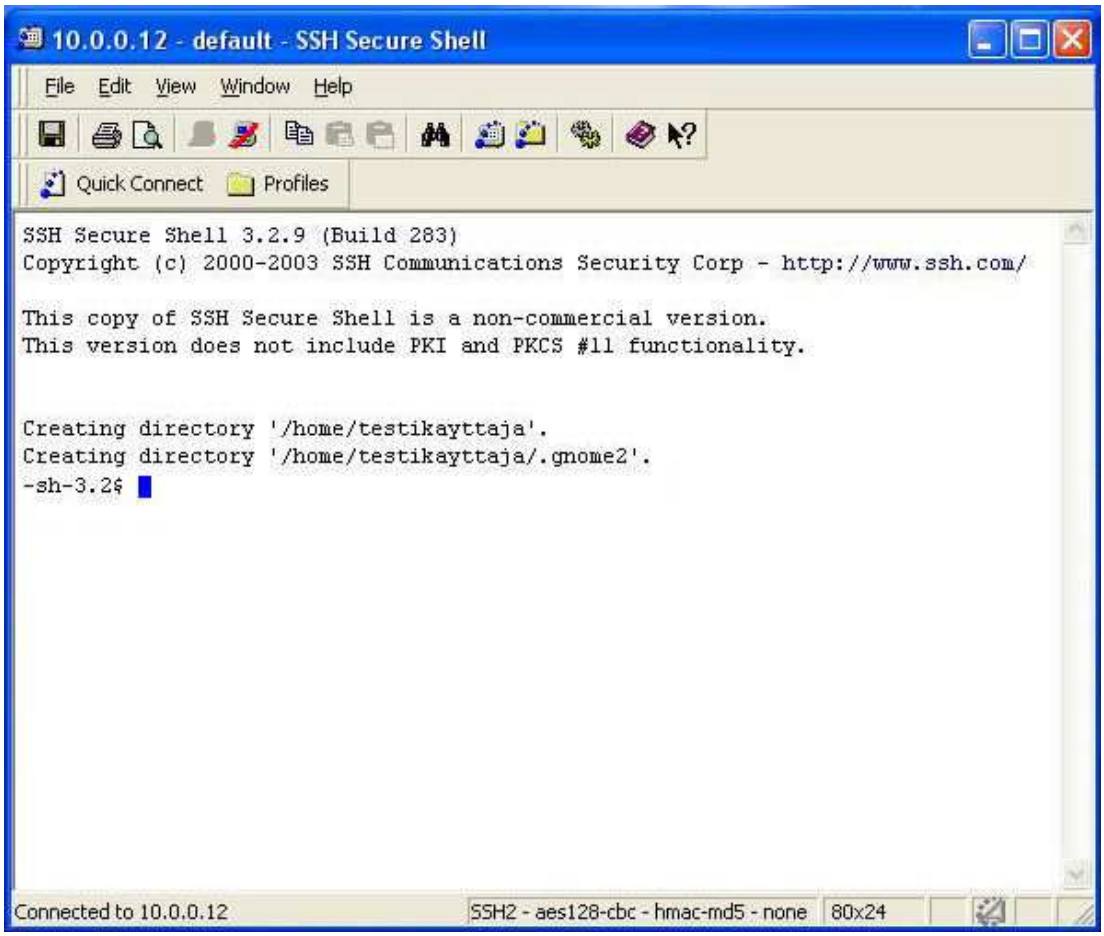
PAM (Pluggable Authentication Modules) on moduuli, jossa tapahtuu käyttäjän tunnistus Linuxissa. Edellisessä kappaleessa tehtävät muutokset koskevat juuri PAM-moduulia, jonka avulla käyttäjä tunnistetaan kirjauduttaessa joko komentopäätteeltä, työpöytäympäristöltä tai salatulta komentopäätteeltä. Tämän moduulin kaikki muut asetukset näkyvät tiedostossa /etc/pam.conf, mutta kaikki /etc/pam.d/ -kansioon tehdyt muutokset korvaavat pam.conf -tiedoston muutokset.

5.6 Linux-kirjautuminen aktiivihakemistoon

Kun kaikki tähänastiset muutokset on saatu tehtyä, voidaan kirjautua aktiivihakemistoon käytetyn Linux-tietokoneen kautta. Ensimmäiseksi kirjaudutaan ulos Fedorasta. Tämän jälkeen kirjaudutaan sisään käyttäjänä testikayttaja ja salasanalla testi. Jos kaikki valmistelut ja muutokset on tehty edellä olevien ohjeiden mukaan, pitäisi ruu-

dulle tulla ilmoitus, jossa kerrotaan testikayttajalle tehdystä kotihakemistosta. Tämän jälkeen työpöydän pitäisi ilmestyä aivan normaaliin tapaan. Tämä tarkoittaa sitä, että nyt Linux-käyttäjä on autentikoitu Windows-palvelimen aktiivihakemistoon. Microsoft Windows Server 2003 R2 -käyttöjärjestelmän ansiosta nyt aktiivihakemiston palvelin pitää sisällään Linux-käyttäjän ja -ryhmän tunnisteet (UID,GID) ja muut tilin tiedot, sekä Windows-käyttäjät voivat kirjautua aktiivihakemistoon samalla tilillä kuin Linux-käyttäjät. Kuvassa 12 on esimerkki kotihakemiston luomisen onnistumisesta kirjauduttaessa SSH:n kautta. (Moskowitz ym. 2005, 179–180.)

Jos vaiheet tähän asti on tehty samanlaisesti kuin edellä on selostettu eikä kirjautumista saada onnistumaan, on epäonnistumisen syy suurella todennäköisyydellä sama kuin minulla oli työtä tehdessä. Fedoran asennuksen alussa oletuksena käyttöön otettu SELinux estää aktiivisena kotihakemiston luonnin turvallisuussyistä. Itse huomasin tämän olevan syy kotihakemiston luonnin epäonnistumisessa. Fedorassa sijaitsevasta lokitiedostosta selviää varsin selvästi, mitä koneella tapahtuu. Näin löysin ratkaisun tähän ongelmaan. Tuo kyseinen lokitiedosto sijaitsee hakemistossa /etc/var/log ja löytyy nimellä messages. SELinuxin voi ottaa pois päältä valitsemalla Sovellukset, josta mennään kohtaan Järjestelmätyökalut ja sieltä SELinux Management. SELinuxin hallintatyökalun auettua se voidaan ottaa pois päältä valitsemalla System Default Enforcing Mode -alasvetovalikosta viimeinen vaihtoehto eli Disabled. Tämän jälkeen Fedora ilmoittaa SELinuxin pois päältä kytkemisen vaativan uudelleenkäynnistyksen. Toinen vaihtoehto on valita listasta keskimmäinen vaihtoehto eli Permisssive. Tämä vaihtoehto ainoastaan listaa lokitiedostoon kaikki tapahtuvat virheet eikä estä niitä tapahtumasta, jolloin se on periaatteessa sama asia kuin jos se olisi pois päältä. Permissive-vaihtoehto ei myöskään vaadi tietokoneen uudelleenkäynnistystä. SELinuxin aktiivitilan vaihdon jälkeen kirjautuminen onnistuu aivan kuin sen pitäisikin. Kirjautumisen onnistumisen jälkeen uusille käyttäjille luodut kotihakemistot löytyvät root-käyttäjänä kansiosta */home*. Kun kirjautuminen Linuxin kautta Windows-aktiivihakemistoon ja uuden kotihakemiston luonti on suoritettu onnistuneesti, on aika siirtyä jo työssä aikaisemminkin mainittuun SSL-salaukseen.



Kuva 12. Kotihakemiston luominen kirjautumisen yhteydessä uudelle UNIX/Linux-käyttäjälle kirjautuessa SSH-pääteyhteysohjelman kautta

6 SSL

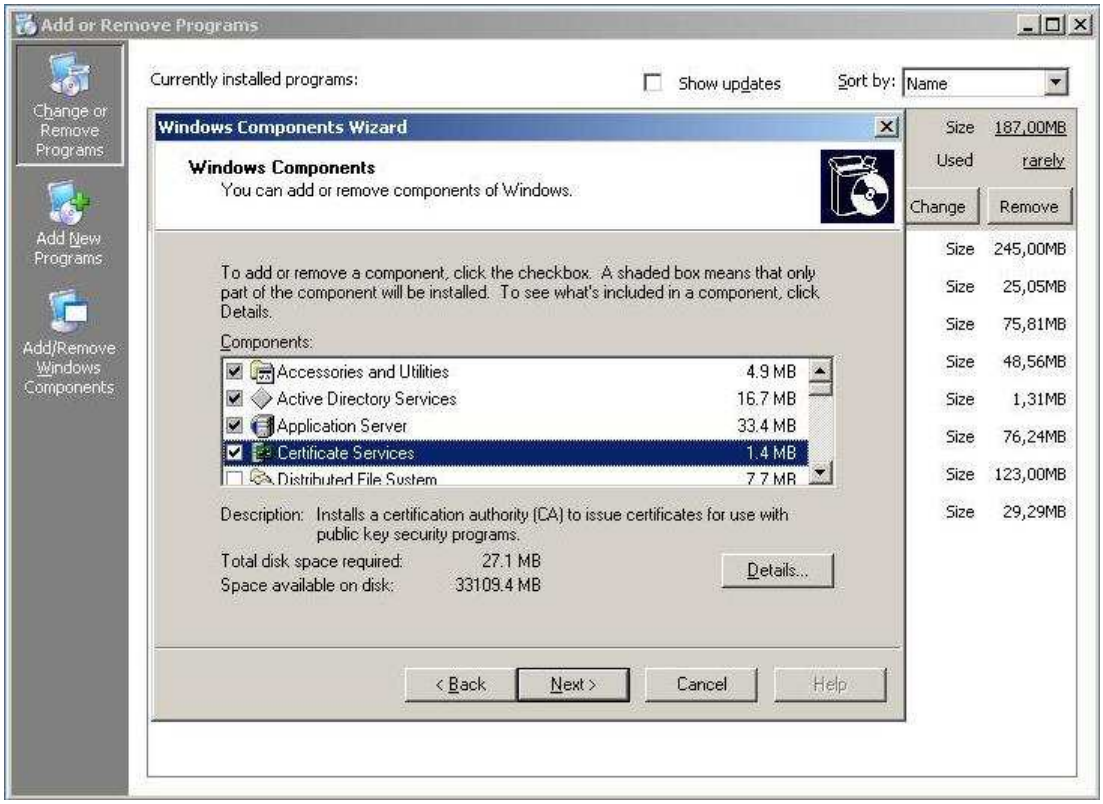
6.1 SSL aktiivihakemistossa

Työssä käytetään Kerberosta kriittisen autentikaatioliikenteen salaukseen, kuten käyttäjien kirjautumiseen ja salasanojen muuttumiseen. On kuitenkin suositeltavaa myös salata vähemmän kriittistä LDAP-hakemistopalveluliikennettä kuten käyttäjäluetteloa, kotihakemistojen sijainteja ja käyttäjien kokonimiä. LDAP-liikenne on mahdollista salata käyttäen SSL-salausta. Koska hakemistopalvelun liikenne ei ole niin vaarallista kuin salasanojen autentikointi, tämä on ainoastaan lisäturvaa tuova ominaisuus, eikä ole kaikille välttämätön toimenpide. Kuitenkin niille, jotka haluavat olla perusteellisia tietoturvan kanssa, tämä on heille hyvä lisäominaisuus. (Moskowitz ym. 2005, 180.)

6.1.1 Sertifikaatti

Salauksen onnistumiseksi meidän on tehtävä kaksi asiaa. Näistä ensimmäiseksi täytyy aktiivihakemistossa ottaa käyttöön SSL. Aktiivihakemisto tukee LDAP-liikennettä SSL-salauksen kautta ja SSL vaatii sertifikaattien (certificates) käytön kirjautujan ja palvelimen välillä. Tämän johdosta jokaisessa käytössä olevassa toimialueen ohjauspalvelimessa on oltava x.509 sertifikaatti. Sertifikaatin tekemiseksi meidän on luotava aktiivihakemistoon Certification Authority (CA). CA luodaan menemällä palvelimen koneelta Ohjauspaneeliin (Control Panel) ja valitsemalla sieltä Lisää tai poista sovellus (Add or Remove Programs). Ikkunan auettua valitaan vasemmalta, kuten työssä aikaisemminkin lisättäessä komponentteja, Lisää tai poista Windows-komponentteja (Add/Remove Windows Components). Nyt aukeavasta listasta rastitetaan ruutu kohdassa sertifikaattipalvelut (Certificate Services) (kuva 13), jonka jälkeen käyttäjälle annetaan varoitus, jonka mukaan CA:n asennuksen jälkeen tietokonetta ei voida enää poistaa toimialueesta, johon se on liittynyt. Hyväksytään varoitus painamlla Yes ja painetaan Seuraava (Next). Tämän jälkeen komponentin asennus kysyy CA:n tyyppiä (CA Type), josta valitaan Enterprise Root CA

ja ikkunassa oleva ruutu kohdassa Use custom settings to generate the key pair and CA certificate voidaan jättää tyhjäksi. Seuraavaksi saavutaan CA Identifying Information -ikkunaan, jossa voidaan antaa luotavalle CA:lle nimi. Tähän on syytä merkitä nimi, joka kuvaa sertifikaatin tarkoitusta ja joka muistetaan myös myöhemmissä vaiheissa. Annoin nimeksi ADSERTIFIKAATTI, jonka jälkeen ikkunan alalaidassa voidaan määrittää sertifikaatin voimassaoloaika. Oletuksena oleva viisi vuotta voidaan jättää voimassaoloajaksi ja jatketaan eteenpäin valitsemalla Seuraava. Certificate Database Settings -ikkunassa voidaan määrittää palvelimelle hakemiston sijainti, jossa Windows säilyttää sertifikaatin tarvitsemia tietoja. Tämän voi huoletta jättää oletuksena olevaksi sijainniksi, jonka jälkeen CA:n asennus voi alkaa.

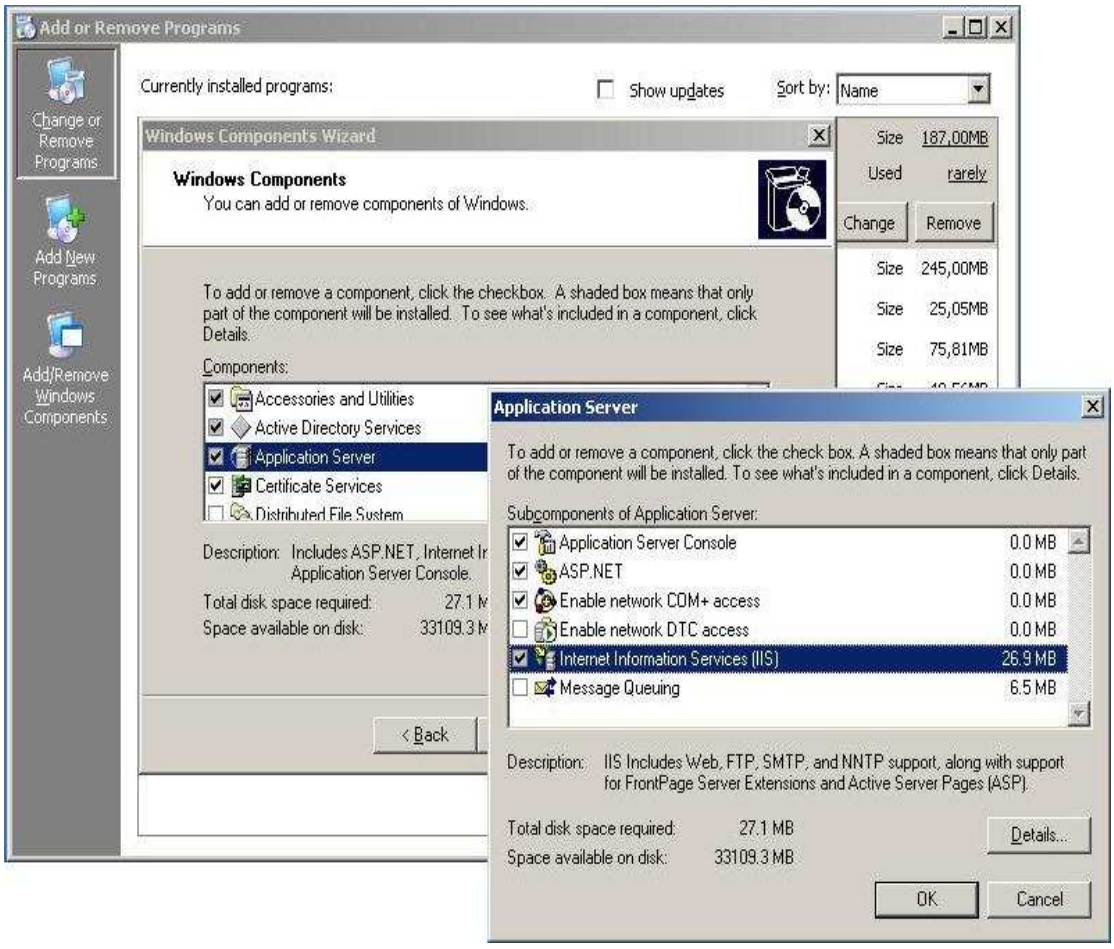


Kuva 13. Certificate Services -komponentin asennus.

Asennuksen aikana voidaan kysyä Service Pack 1:n levyä, joten se on syytä pitää käden ulottuvilla asennusta tehtäessä. Jos palvelimella ei ole asennettuna IIS (Internet Information Services) -komponenttia, asennusohjelma huomauttaa siitä ja vaatii sen asennusta, koska CA ja sen sisältämä Certificate Services Web Enrollment Support tarvitsevat sitä toimiakseen. IIS-komponentin voi asentaa Lisää tai poista Win-

dows komponentteja -ikkunasta. Sieltä rastitetaan kohta Application Server ja painetaan Details-painiketta, josta nähdään komponenttiin sisältyvät osat. Aukeavasta Application Server -ikkunasta varmistetaan, että Internet Information Services (ISS) on rastitettu (kuva 14) ja hyväksytään valinnat painamalla OK. Asennuksen suorittamista varten painetaan Seuraava, jonka jälkeen IIS-komponentin asennus alkaa. Jos palvelimella kuitenkin on valmiina asennettuna IIS, CA:n asennus voi vaatia sen väliaikaista pysäyttämistä. Jos pysäyttämistä kysytään asennuksen aikana, se voidaan hyväksyä yksinkertaisesti painamalla YES. On myös mahdollista, että CA:n asennus kysyy Active Server Pages (ASPs) käyttöönottoa IIS-komponenttia varten, jotta sertifikaattipalvelut voivat auttaa käyttämään web enrollment -palveluita. Tällaisessa tilanteessa myös sen käyttöönotto on syytä hyväksyä painamalla YES.

Asennuksen päätyttyä on kaksi vaihtoehtoa uuden sertifikaatin suhteen. Tietokone voidaan pakottaa saamaan sertifikaatti kirjoittamalla Windowsin komentokehotteeseen (Command Prompt) käsky *gpupdate /force*. Jos tämä ei onnistu noin 15 minuutin kuluessa, voidaan aktiivihakemiston toimialueen ohjauspalvelin käynnistää uudelleen. Näiden jälkeen portti 636 on valmiina ottamaan vastaan salattua aktiivihakemiston liikennettä. (Moskowitz ym. 2005, 184.)



Kuva 14. IIS-komponentin asennus.

6.1.2 SSL-liikenteen varmistus

Kun CA on asennettu ja sen avulla portin 636 pitäisi olla valmiina vastaanottamaan salattua aktiivihakemiston liikennettä, on syytä varmistaa liikenteen toimivuus. Windows Server 2003 -käyttöjärjestelmän tukityökaluissa (Windows 2003 Support Tools) on LDP niminen työkalu, jonka avulla voidaan varmistaa, että aktiivihakemisto voi vastaanottaa SSL-liikennettä. Tukityökalut voidaan käynnistää Windows Server 2003 CD-levyltä. Se löytyy ensimmäisen levyn polusta /support/tools. Mennään tuohon kansioon ja sieltä kaksoisklikataan tiedostoa suptools.msi. Tämän jälkeen on hyväksyttävä sopimusehdot kyseiselle tuotteelle, vahvistaa tuotteen haltijan nimi ja organisaatio sekä määrittää sijainti tukityökalujen asennukselle. Sijainnin määrityk-

sen jälkeen tukityökalujen asennus kopioi tarvittavat tiedostot tietokoneen kovalevylle, jonka jälkeen asennus on valmis. Asennuksen jälkeen käynnistetään LDP menemällä Käynnistä-valikkoon ja valitsemalla sieltä Suorita (Run), jonka jälkeen aukeavaan ikkunaan kirjoitetaan ldp ja painetaan OK. Ohjelman käynnistyttyä valitaan ylhäältä valikosta Connection ja sieltä Connect. Connect-ikkunan Server kohtaan kirjoitetaan toimialueen ohjauspalvelimen osoite serveri.SAMK.local, Port kohtaan vaihdetaan portiksi 636, rastitetaan ruutu kohdassa SSL ja painetaan OK. Tämän jälkeen isoon harmaaseen ikkunaan pitäisi tulla tietoa, jonka mukaan nyt on kirjauduttu toimialueen ohjauspalvelimeen. Nyt voidaan ylhäältä valita Connection ja sieltä Bind. Eteen auenneeseen Bind-ikkunaan syötetään tehdyn dirsearch käyttäjän käyttäjänimi sekä salasana ja kirjoitetaan Domain-ruutuun toimialueen nimi SAMK.local ja painetaan OK. Nyt ikkunaan tuli tieto siitä, että on autentikoitu dirsearch käyttäjänä. Viimeiseksi valitaan ylhäältä View ja sieltä Tree. Eteen aukeaa ikkuna, joka voidaan jättää tyhjäksi ja painaa OK. Painalluksen jälkeen ikkunan vasemmalle laidalle ilmestyy aktiivihakemiston puurakenne, josta aktiivihakemiston rakenne voidaan selata aivan normaalisti. Tämä rakenteen selaaminen tapahtuu salattuna portin 636 kautta. Nyt voidaan todeta, että SSL-salaus toimii tarkoituksenmukaisesti. (Moskowitz ym. 2005, 184-185.)

6.1.3 Sertifikaatin kopiointi

Tällä hetkellä CA on asennettu ja aktiivihakemisto on valmis ottamaan vastaan SSL-liikennettä portin 636 kautta. Seuraavaksi on kaikille Linux-koneille kopioitava CA:n sertifikaatti, jonka avulla Linux-käyttäjät voivat luottaa toimialueen ohjauspalvelimen sertifikaattiin, jonka CA on myöntänyt. Sertifikaatin kopioimiseksi voidaan käyttää Certificates Snap-in -ohjelmaa. Ohjelman käynnistämiseksi mennään Käynnistä-valikkoon ja valitaan sieltä Suorita. Tämän jälkeen ikkunaan kirjoitetaan MMC ja painetaan OK. Eteen aukeaa MMC-konsoli (Console1), josta valitaan ylhäältä File ja sieltä Add/Remove Snap-in. Add/Remove Snap-in -ikkunassa alhaalta painetaan Add, jonka jälkeen Add Standalone Snap-in -ikkunasta valitaan Certificates ja painetaan Add. Tämän jälkeen kysytään minkä tyyppisiä sertifikaatteja halutaan hallita.

Kolmesta vaihtoehdosta valitaan Computer account ja jatketaan painamalla Seuraava. Seuraavassa kohdassa valitaan tietokone, jota halutaan hallita, tässä tapauksessa valitaan tällä hetkellä käytössä oleva tietokone eli Local Computer. Tämän jälkeen painetaan Valmis. Add Standalone Snap-in -ikkunasta poistutaan painamalla Sulje (Close) ja Add/Remove Snap-in -ikkunassa hyväksytään tehdyt valinnat painamalla OK. Nyt on mahdollisuus luoda CA:n julkinen sertifikaatti, joka on voimassa aina autentikoidessa aktiivihakemistoon. (Moskowitz ym. 2005, 185.)

Nyt uuden sertifikaatin luomiseksi selataan konsolin ikkunassa kohtaan Certificates (Local Computer), josta valitaan Personal ja edelleen Certificates. Valinnan jälkeen nähdään ikkunan oikealla puolella sertifikaatti ADSERTIFIKAATTI, painetaan sertifikaatin nimen päällä hiiren oikeanpuoleista painiketta ja aukeavasta valikosta valitaan All Tasks ja Export, josta päästään sertifikaatin luonnin opastukseen (The Certificate Export Wizard). Tervetuloa-ikkunassa painetaan Seuraava, jonka jälkeen kysytään salaisen avaimen luontia, jossa valitaan oletuksena oleva alempi vaihtoehto No, do not export the private key ja painetaan Seuraava. Seuraavaksi Export File Format -ikkunassa kysytään sertifikaatin tiedostotyyppiä, josta valitaan keskimmäinen vaihtoehto eli Base-64 encoded X.509 (.CER). Tämä valinta luo .cer-tiedostopäätteisen sertifikaattitiedoston, joka on luettavissa Linuxin käyttäjille. Tiedostotyypin valitsemisen jälkeen painetaan Seuraava, jonka jälkeen valitaan sertifikaatille sijainti, johon se luodaan sekä asetetaan sille nimi. Nimeksi voidaan antaa mitä halutaan, mutta totesin järkeväksi käyttää samaa nimeä kuin aikaisemminkin (ADSERTIFIKAATTI). Sertifikaatin sijainniksi on syytä määrittää sellainen polku, josta se on hetken kuluttua helposti löydettävissä. Sertifikaatin nimen ja sijainnin määrityksen jälkeen painetaan Seuraava ja viimeisenä vahvistetaan edellä tehdyt valinnat painamalla Valmis (Finish), jonka jälkeen saadaan ilmoitus sertifikaatin luonnin onnistumisesta. Viimeiseksi on tarkoitus kopioida juuri luotu sertifikaatti jokaisen käytössä olevan Linux-koneen kovalevylle. Se miten kopioinnin suorittaa on jokaisen oma valinta. Pääasia on kopioida sertifikaatti valitusta sijainnista Linux-koneen kansioon /etc/openldap. Kopioinnin jälkeen SSL-salaus on aktiivihakemiston puolesta valmis ja voidaan jatkaa salauksen käyttöönottoa käytössä olevalla Fedoralla.

6.2 SSL Linuxissa

Otettaessa käyttöön SSL-salaus Linux-koneella, jotta se tukisi salattuja yhteyksiä aktiivihakemiston LDAP-palvelimelle, on tehtävä kaksi muutosta jo aikaisemminkin muokattuun ldap.conf-tiedostoon. Ensimmäiseksi otetaan käyttöön SSL LDAP-yhteyksiä varten korvaamalla tiedostossa sijaitseva rivi *uri ldap://serveri.SAMK.local* rivillä *uri ldaps://serveri.SAMK.local*. Ainoa muutos riviin on ldap-sanan korvaaminen sanalla ldaps. Toinen muutos tiedostoon tehdään lisäämällä tai muokkaamalla valmiina olevista kommenteista tiedoston loppuun seuraavat kaksi riviä:

tls_checkpeer yes

tls_cacert /etc/openldap/ADSERTIFIKAATTI.cer

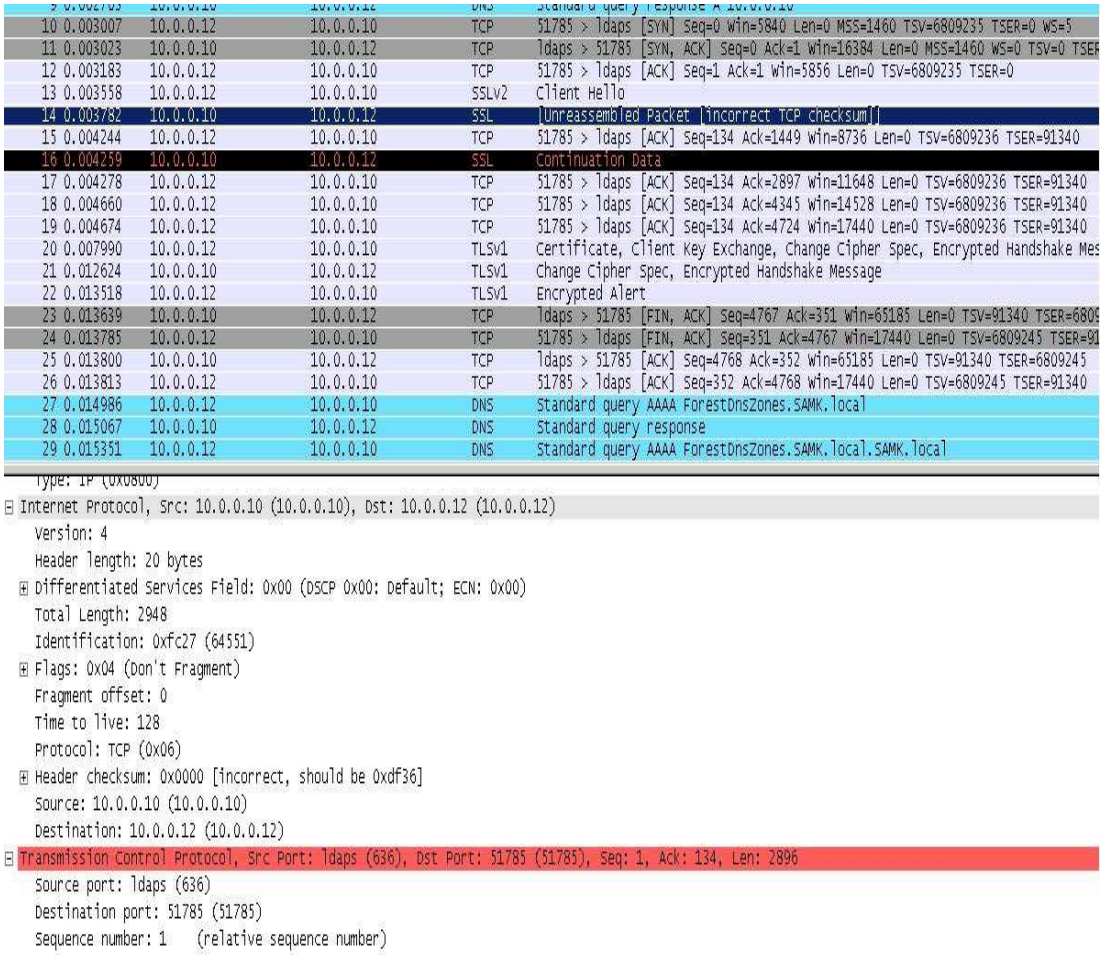
Näistä ensimmäinen rivi löytyy tiedostosta jo valmiina kommenttina ja se takaa, että Linux-käyttäjä muistaa varmistaa palvelimen SSL-sertifikaatin. Toista ja viimeistä riviä ei löydy tiedostosta ennestään, joten se on lisättävä itse ja se kertoo käyttäjälle työssä tehdystä Windows-pohjaisesta CA:stä. Näiden rivien lisäämisen jälkeen Linuxin ja Windows-aktiivihakemiston välinen LDAP-liikenne on salattu SSL-salauksen avulla. Salauksen lopullisen toimivuuden voi tarkistaa kirjautumalla Fedoraan käyttäjänä testikayttaja salasanalla abc123. Jos kirjautuminen onnistuu normaalisti, kaikki asiat ovat kunnossa.

Minulla kirjautuminen ei heti onnistunut, jolloin ongelman ratkaisu löytyi yksinkertaisesti ldap.conf -tiedoston sisällöstä. Tiedosto sisältää komentona rivin *ssl no*, joka kiinnitti huomioni salausta tehdessäni, koska tarkoitus on nimenomaan käyttää SSL-salausta yhteyksiin aktiivihakemiston LDAP-palvelimelle. Vaihdetaan tuo kyseinen rivi *no* riviin *on*. Tiedoston sisältöä selailtaessa myös pistää silmään sen lopussa oleva komento *tls_cacertdir /etc/openldap/cacerts*, joka mielestäni viittaa selkokielisesti sertifikaatin sijaintiin. Tämä kyseinen rivi on tiedostossa myös alun perin ilman, että mitään muutoksia on tehty. Vaikka sertifikaatti kopioitiin jo aikaisemmin tiedoston osoittamaan sijaintiin */etc/openldap*, tehdään samanlaisesti ja kopioidaan tehty serti-

fikaatti ADSERTIFIKAATTI.cer myös tuon rivin osoittamaan sijaintiin, eli kansioon cacerts. Näiden kahden muutoksen jälkeen SSL-salaus toimii ongelmitta.

Yksi tapa varmistaa Linux- ja Windows-koneen välisen kommunikoinnin salaus on tutkia niiden välillä liikkuvaa liikennettä kirjautumisen aikana. Tämä onnistuu mahdollisesti monilla analysointiohjelmilla, mutta itse päätin käyttää Wireshark -nimistä ohjelmaa, vanhalta nimeltään Ethereal. Se on ilmainen verkkoprotokollien analysointiin tarkoitettu avoimen lähdekoodin ohjelma, joka tukee satoja eri protokollia. Se on vapaasti ladattavissa sen kotisivuilta osoitteesta http://www.wireshark.org/download.html.

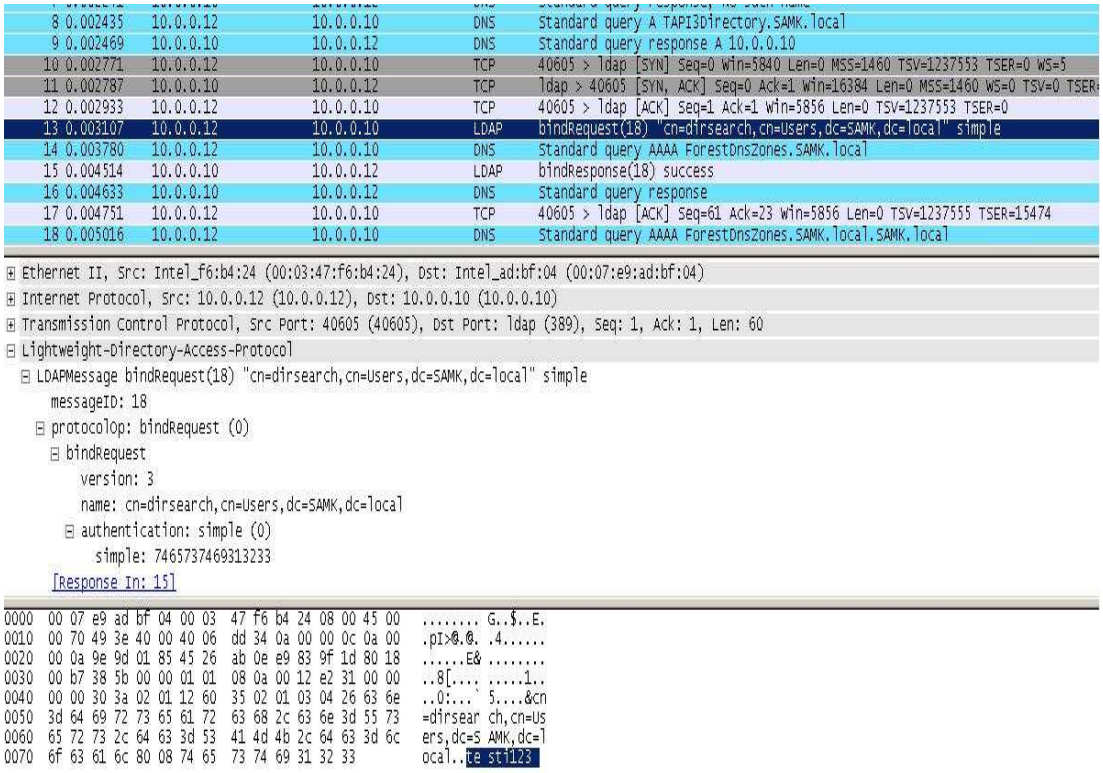
Kirjauduttaessa Linux-koneelta Windows-palvelimelle käyttäen SSL-salausta saadaan Wiresharkin analysoinnin tuloksena kuvassa 15 olevat tulokset.



Kuva 15. SSL-liikenne kirjautumisen aikana Wiresharkin avulla.

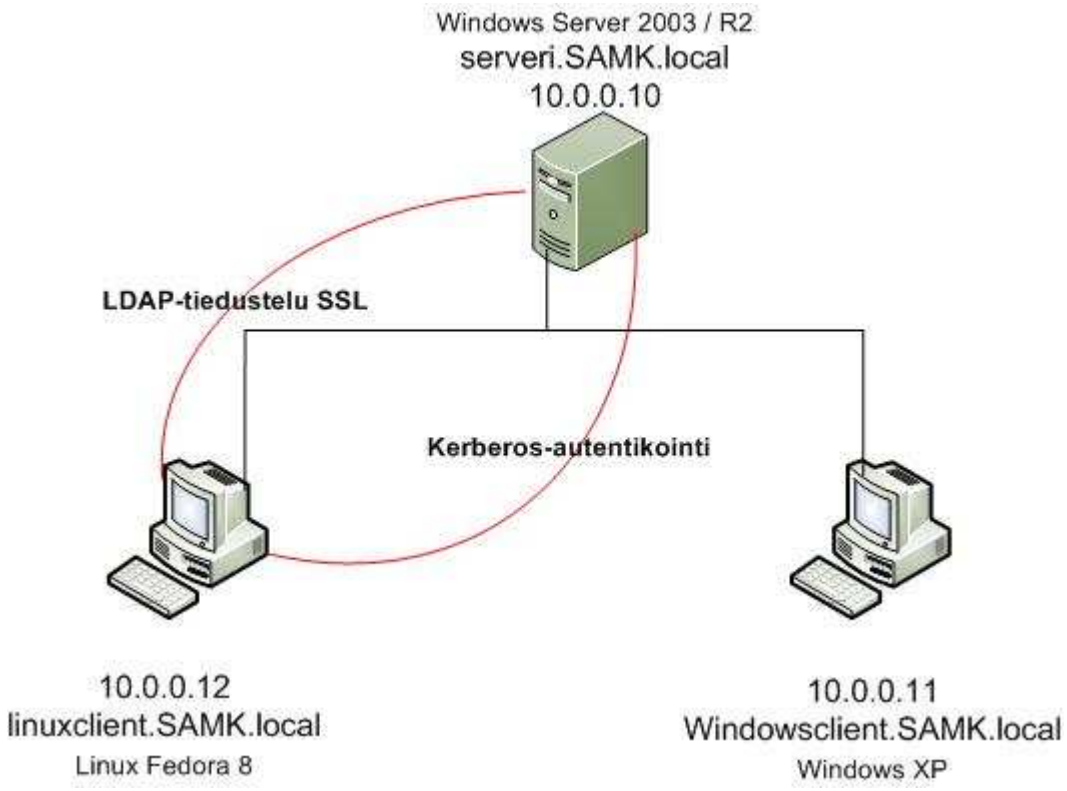
Wiresharkin avulla nähdään pakettien numerot saapumisjärjestyksessä. Niistä selviää paketin aika, lähde - ja kohde IP-osoite, paketin protokolla ja paketin lisätietoja. Yllä olevasta kuvasta nähdään kolmannentoista (13) paketin olevan Linux-koneen lähettämä SSL-protokollan Hello-paketti, jonka kohde IP-osoite on käytössä oleva Windows-palvelin ja portti numero 636. Tämän paketin jälkeen alkaa SSL-liikennettä kulkea näiden kahden koneen välillä tasaisin väliajoin Windows-koneelta Linux-koneelle kirjautumisen loppuun saakka. Näiden tulosten avulla voidaan lopullisesti todeta salaus ja koko työn toimivuus varmasti.

Ilman SSL-salausta analysoimalla Wiresharkin avulla kirjautumisen aikana liikkuvia paketteja (kuva 16) huomataan saman kolmannentoista (13) paketin olevan LDAP-protokollapaketti, joka käyttää jo aikaisemminkin mainittua yksinkertaista autentikointia ja porttia numero 389. Myös työn alussa mainittiin tämän yksinkertaisen autentikoinnin lähettävän käyttäjänimet ja salasanat selkokielisinä. Tämä selviää kuvassa tummansinisinä merkityistä kohdista. Ylempänä paketin tiedoista selviää käyttäjänimi dirsearch ja alemmista tiedoista sen tilin salasana testi123.



Kuva 16. Verkkoliikenne kirjatumisen aikana Wiresharkin avulla ilman SSL-salausta.

Kaikkien näiden todisteiden nojalla voidaan todeta aktiivihakemistossa tunnetun Linux-käyttäjän testikayttaja kirjautuminen Windows aktiivihakemiston toimialueeseen SAMK.local. Tämä tapahtuu käyttäen hyväksi LDAP-tiedusteluja, jotka on salattu SSL-salauksella käyttäen sertifikaattia. Näiden lisäksi käyttäjän tunnistukseen käytetään Kerberos-autentikointia (kuva 17).



Kuva 17. Työn lopputuloksen kokonaiskuva.

7 LINUX-AUTENTIKOINTI WINBIND/SAMBA:LLA

Työtä aloittaessani tein työn kokonaisuudessaan Fedoran Core 6 -versiolla, ja kun Fedoran kahdeksas versio ilmestyi, tein työn alusta loppuun dokumentoiden sen. Fedoran kahdeksas versio toi uudistuksien myötä mukanaan vaihtoehtoisen tavan toteuttaa edellä selvitetty Linux-kirjautuminen Windows-aktiivihakemistoon. Tämän se tekee käyttäen apunaan Winbindiä ja uudistettua Sambaa. Vielä seitsemännessä Fedoran versiossa tämä ei ollut tietääkseni täysin toimiva ja käytännöllinen, mutta kahdeksannessa se on jo toteutettavissa hyvinkin helposti.

Tässä vaiheessa täytyy ottaa huomioon se, että mitään työssä ennen tehtyjä muutoksia Linux-koneen tiedostoiden sisältöihin ei tarvita. Myöskään Windows-puolella ei tarvitse laajentaa palvelinympäristöä asentamalla R2-version tuomaa Identity Management for UNIX -komponenttia.

Voidaan aloittaa luomalla aktiivihakemiston toimialueeseen uusi käyttäjätili. Nimeksi voidaan antaa esimerkiksi winbindsamba ja salasanaksi winbind. Käyttäjän luomisen jälkeen se voidaan halutessa lisätä ryhmään testiryhmä tai johonkin muuhun ryhmään.

Tämän jälkeen siirrytään Linux-koneelle ja voidaan jatkaa ottamalla käyttöön Winbind ja Samba. Aloitetaan Todennusasetuksilla, eli valitaan ylhäältä tehtäväpalkista Järjestelmä, josta mennään kohtaan Ylläpito ja sieltä valitaan Todennus. Todennusasetuksien konfigurointityökalun auettua asetetaan ensimmäisestä Käyttäjätiedot-välilehdestä Winbind niin, että Winbind-toimialueeksi määritetään isoilla kirjaimilla SAMK. Turvatyypiksi valitaan ads, joka tarkoittaa Active Directory Securitya, jolloin aktiivihakemiston tunnukset kelpaavat sellaisenaan ilman, että niitä luotaisiin Linux-koneelle. Winbind ADS Realm -kohtaan kirjoitetaan toimialueen nimi SAMK.LOCAL, kaikki isoilla kirjaimilla ja Winbind-toimialueen ohjauskoneet -kohtaan annetaan toimialueen ohjauspalvelimen osoite, eli serveri.SAMK.local. Viimeiseksi Mallikuori -kohtaan valitaan /bin/bash. Tämän jälkeen Winbind-asetukset

voidaan hyväksyä (kuva 18) ja jatkaa seuraavaan eli Todennus-välilehteen. Tältä välilehdeltä rastitetaan ruutu kohdassa Käytä Kerberos-tukea ja asetetaan Kerberos niin, että REALM kohtaan kirjoitetaan toimialue kokonaan isoilla kirjaimilla, eli SAMK.LOCAL. Tämän jälkeen kohtiin KDCs ja Päätepalvelimet annetaan toimialueen ohjauspalvelimen osoite serveri.SAMK.local. Näiden jälkeen hyväksytään Kerberos-asetukset ja Todennusasetukset ovat valmiita. (Vainio 2008, 3-4.)

Kuva 18. Winbind-asetuksien määrittäminen.

Kun äsken käytettyjen graafisten työkalujen avulla tehdyt muutokset hyväksytään, tekee se myös automaattisesti muutokset niiden asetuksien sisältämiin tekstitiedostoihin. Aivan kuten aikaisemmin työssä tehdyt LDAP- ja Kerberos-asetukset menivät suoraan myös ldap.conf -tiedostoon ja molempien omiin tekstitiedostoihin. Tällä kertaa joudutaan tekemään vielä yksi muutos Samban asetuksiin muokkaamalla sen asetuksia sisältävää tekstitiedostoa. Selataan kansioon /etc/samba/, mistä avataan tiedosto smb.conf. Tiedoston sisällöstä löydetään rivi *winbind use default domain* =

false. Vaihdetaan tämän rivin arvo *false* arvoksi *true*, jolloin Samban asetukset ovat valmiita. Seuraavaksi jatketaan jo työssä aikaisemminkin muutoksia tehtyyn PAM-moduuliin. Jotta kirjautuminen saataisiin onnistumaan jälleen kolmella yleisimmällä tavalla, aivan kuten kohdassa 5.5, tehdään muutoksia niiden vaatimiin tiedostoihin. Nämä kolme tiedostoa ovat samat kuin aikaisemminkin, eli sshd, login ja gdm, jotka sijaitsevat kansiossa /etc/pam.d. Näihin jokaiseen tiedostoon lisätään tiedostoon rivi:

session required pam_mkhomedir.so skel=/etc/skel umask=0076

Rivi on kokonaisuudessaan aivan sama, paitsi viimeinen numero on muuttunut yhden pienempään kuin viimeksi. Näiden muutosten avulla pitäisi kirjautumisen onnistua myös tunnuksilla, joilla ei ole kotihakemistoa valmiiksi tehtynä, vaan se luodaan tämän komennon seurauksena ensimmäisen kirjautumisen yhteydessä.

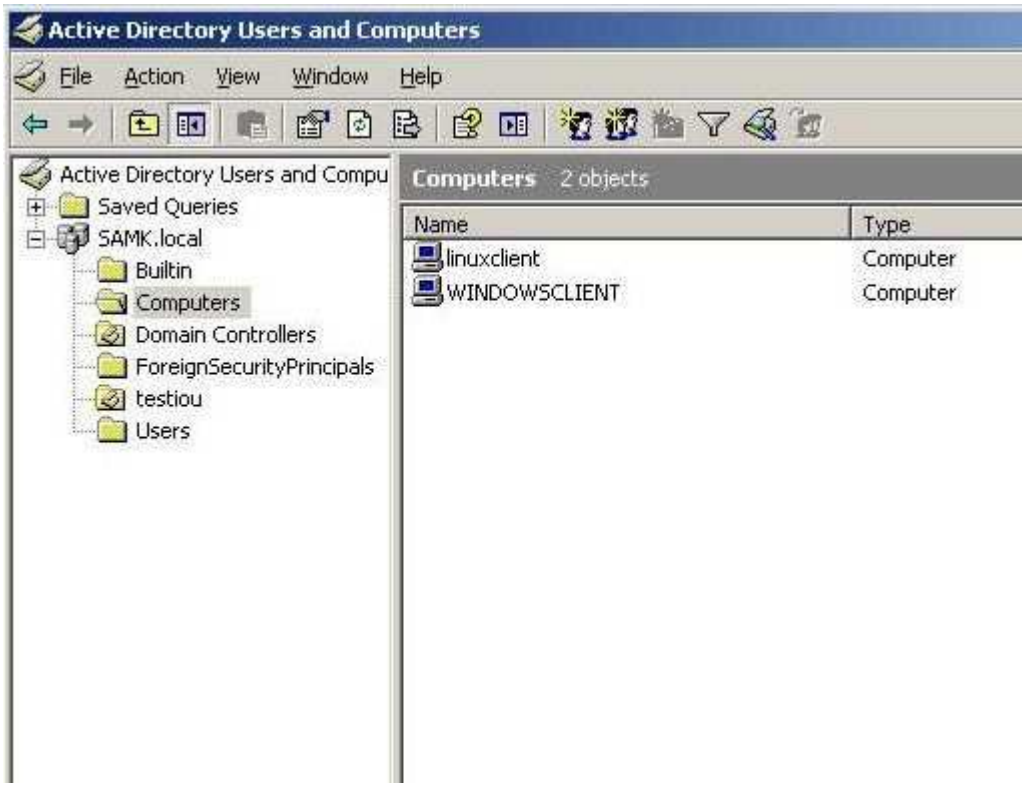
Tehdään vielä viimeinen muutos ennen aktiivihakemiston toimialueeseen liittymistä, joka on kotihakemistoja varten tehtävä hakemisto. Kotihakemistot, jotka luodaan käyttäjän ensimmäisen kirjautumisen yhteydessä, menevät automaattisesti kansioon /home/SAMK. Tehdään /home-hakemistoon kansio nimeltä SAMK. Kansio voidaan luoda yksinkertaisesti menemällä hakemistoon /home ja luomalla sinne uusi kansio. Toinen vaihtoehto on valita ylhäältä valikosta Sovellukset, josta mennään kohtaan Järjestelmätyökalut ja sieltä valitaan Pääte. Tästä aukeaa sovellus, josta voidaan käyttää Fedoran komentoriviä. Annetaan päätteelle komento *mkdir /home/SAMK*.

Kansion luomisen jälkeen ollaan valmiita liittämään Linux-kone Windows-toimialueeseen. Aikaisemmissa vaiheissa toimialueeseen liittymistä ei tarvittu, vaan kirjautuminen onnistui ilman sitä. Kun käytössä on Samba ja Winbind, on toimialueeseen liittyminen välttämätöntä.

Ennen aktiivihakemiston toimialueeseen liittämistä on huomioitava kaksi asiaa. Ensimmäiseksi on tarkistettava, että molempien tietokoneiden, Linux-koneen ja Windows-palvelimen, kellonajat ovat lähellä toisiaan. Jos kellonajat eroavat paljon toisistaan, ei toimialueeseen liittyminen yksinkertaisesti toimi. Toiseksi on vielä tarkistettava, että toimialueeseen liitettävän tietokoneen, eli Linux-koneen DNS-nimi kuuluu samaan toimialueeseen (SAMK.local). Kun nuo kaksi kohtaa on tarkistettu ja verkkoasetukset ovat kunnossa työn aikaisempien vaiheiden mukaan, on Linux-kone

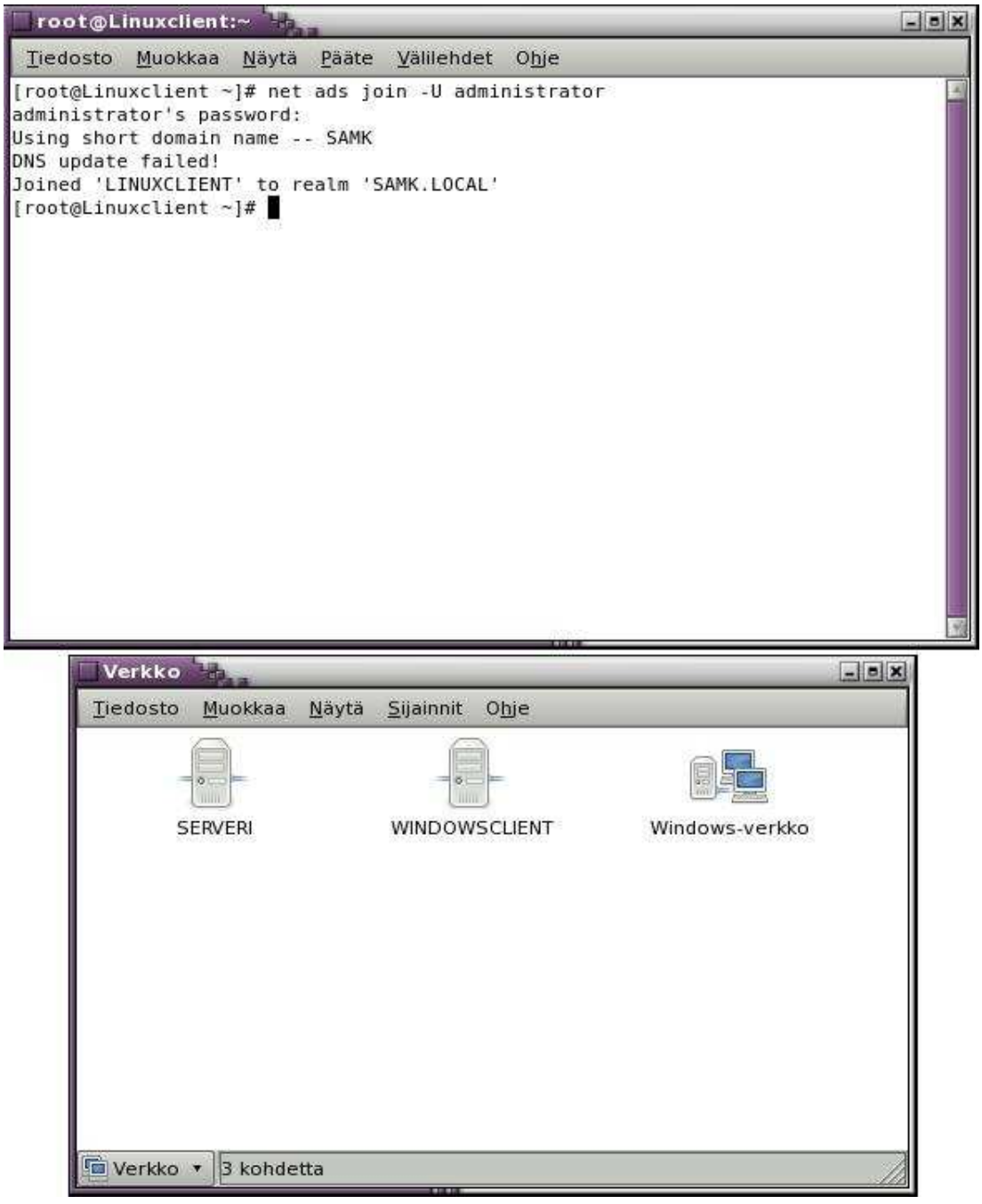
valmis liitettäväksi toimialueeseen. Annetaan päätteelle komento *net ads join -U administrator*. Komennon antamisen jälkeen kysytään järjestelmänvalvojan salasanaa. Kun se on annettu, saadaan viesti liittymisen onnistumisesta (kuva 20) ja nyt Linux-kone on onnistuneesti lisätty aktiivihakemiston toimialueeseen SAMK.local. (Moskowitz ym. 2005, 163-164.)

Toimialueeseen liittymisen onnistuminen voidaan tarkistaa Windows-palvelimelta. Tämä tapahtuu menemällä Aktiivihakemiston Käyttäjät ja Tietokoneet (Active Directory Users and Computers) -hallintakonsoliin. Sieltä valitaan toimialueen puusta kohta tietokoneet (Computers), josta nähdään kaikki toimialueeseen kuuluvat tietokoneet. Nyt listassa pitäisi näkyä toimialueeseen äsken liitetty tietokone Linuxclient sekä jo aikaisemmin toimialueeseen liitetty Windowsclient (kuva 19). Jos tietokone, joka yritettiin liittää toimialueeseen, ei jostain syystä näy tässä listassa, on syytä tarkistaa edellä mainitut kaksi kohtaa tilanteen korjaamiseksi. Kun kohdat on tarkistettu, voidaan tietokone liittää uudelleen toimialueeseen.



Kuva 19. Aktiivihakemiston toimialueen tietokoneet.

Myös Linux-koneelta ovat nähtävissä kaikki verkon tietokoneet, jotka ovat yhteydessä toisiinsa. Tämä tapahtuu menemällä Tietokoneeseen ja sieltä Verkkoon. Listassa pitäisi näkyä aktiivihakemiston testausta varten käytetty Windows-kone Windows-client sekä itse Windows-palvelin Serveri (kuva 20).

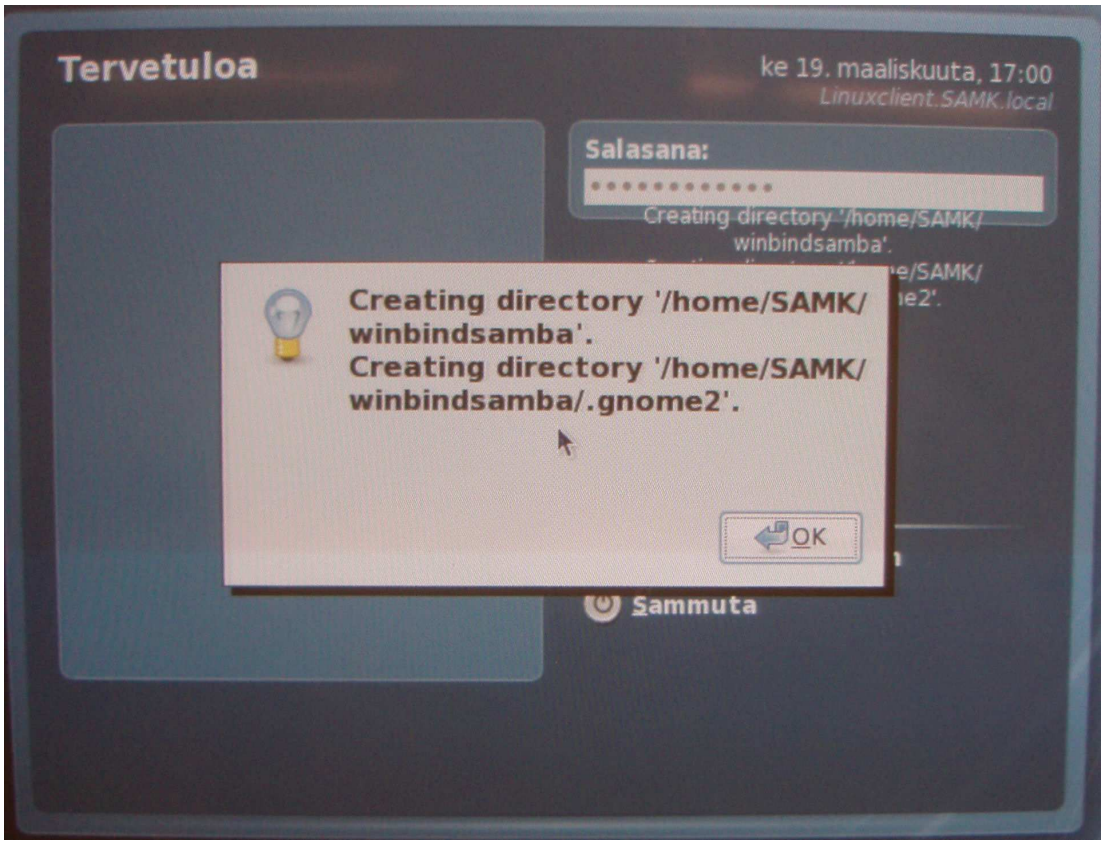


Kuva 20. Linux-tietokoneen liittäminen aktiivihakemiston toimialueeseen ja verkon tietokoneet.

Jos Fedorassa ei ole ennestään asennettu Sambaa, on sen asennus suoritettava ennen seuraavaa vaihetta tai jopa ennen toimialueeseen liittämistä. Jos toimialueeseen liittyminen ei onnistu sen takia, että Sambaa ei ole asennettu, saadaan siitä virhesanoma. Samban asennus tapahtuu Fedoran asennuslevyltä. Sen voi asentaa ainakin kahdella tavalla. Ensimmäinen vaihtoehto on valita tehtäväpalkista Sovellukset ja sieltä Lisää tai poista ohjelmistoja, mistä päästään Fedoran pakettien hallintaan. Toinen vaihtoehto on selata Fedoran asennuslevyä kansioon Packages, missä sijaitsevat kaikkien pakettien asennustiedostot. Levyltä löytyy Sambaan liittyen kolme pakettia, jotka ovat samba - client, samba - common ja samba. Näistä kaksi ensimmäistä on asennettu oletuksena Fedoran asennuksen yhteydessä. Asennuslevyltä löytyvät paketit ovat RPM-paketteja (RPM Package Manager), jotka ovat pakatussa muodossa olevia asennusohjelmia. Aivan samanlaisesti toimivat Windows-käyttöjärjestelmissä msi-paketit (Windows Installer). Asennetaan viimeisenä mainittu paketti, joka minulla oli samba-3-0-26a-6.fc8.i386.rpm, kaksoisklikkaamalla pakettia. Asennuksen jälkeen pitäisi Samban olla kokonaisuudessaan asennettuna. Viimeisenä käynnistetään Linux-koneella Winbind- ja Samba-palvelut. Tämän voi tehdä kahdella tavalla. Voidaan valita tehtäväpalkista Järjestelmä, mistä mennään kohtaan Ylläpito ja sieltä valitaan Palvelut. Sieltä voidaan määrittää, mitkä kaikki palvelut ovat käytössä, ja ne voidaan asettaa käynnistymään aina tietokoneen käynnistymisen yhteydessä, mikä tässä tapauksessa pitää tehdä molempien palveluiden kohdalla. Sieltä käynnistetään Samba ja tietenkin Winbind, jos sitä ei ole vielä käynnistetty. Toinen vaihtoehto on mennä Fedoran päätteeseen ja antaa sille komennot *service smb start* ja *service winbind start*, jolloin palvelut käynnistyvät.

Kun Samban ja Winbindin palvelut on käynnistetty ja kaikki muutokset on tehty, ollaan valmiita kirjautumaan Linux-koneelta Windows-aktiivihakemistoon. Kirjaudutaan ulos Fedorasta, minkä jälkeen kirjaudutaan sisään käyttäjänä winbindsamba salasanalla winbind. Kirjautumisen hyväksymisen jälkeen saadaan samanlainen ilmoitus kuin aikaisemminkin. Tällä kertaa ilmoitus kertoo kotihakemiston luomisesta käyttäjälle winbindsamba (kuva 21), minkä jälkeen Gnomen työpöytä ilmestyy aivan kuten normaalissa kirjautumisessa.

Näin ollen Linux-käyttäjän kirjautuminen aktiivihakemistoon Windows-toimialueen käyttäjänä on suoritettu onnistuneesti Samban ja Winbindin avulla.



Kuva 21. Kotihakemiston luominen kirjautumisen yhteydessä uudelle UNIX/Linux-käyttäjälle kirjautuessa Gnome-työpöytäympäristön kautta.

8 YHTEENVETO

Windowsin ja Linuxin välinen yhteensopivuus on erittäin laaja käsite. Organisaatioilla on yhä useammin käytössä Windows-palvelimet ja aktiivihakemisto, mutta kuitenkin halutaan käyttää myös Linuxin tarjoamia mahdollisuuksia. Tässä työssä käytettiin Windows Server -käyttöjärjestelmää ja aktiivihakemistoa käyttäjätietojen hallitsemiseen keskitetysti. Linux-palvelimet ja työasemat käyttivät näitä tietoja hyväkseen. Käyttäjätietojen keskittämisen voi toteuttaa myös käyttäen Linux-palvelimien ylläpitämää käyttäjätietokantaa, jota Windows-työasemat käyttävät. (Nordberg 2008.)

Työssä käytetyillä kahdella menetelmällä saavutetaan lähes sama tulos. Ensimmäinen LDAP-hakemistopalveluun liitetty menetelmä on monimutkaisempi toteuttaa. Siinä Linux-tunnuksien vaatimia lisäkenttiä käyttäjätiedoista tallennetaan aktiivihakemistoon, jolloin useamman toimialueen ympäristössäkin Linux-käyttäjän tunnus (UID) säilyy aina samana. Jälkimmäinen Winbind/Sambaan perustuva menetelmä on helppo ottaa käyttöön yhden toimialueen ympäristössä. Satakunnan Ammattikorkeakoulu on päättänyt siirtyä yhteen toimialueeseen, joten jälkimmäinen menetelmä vaikuttaa tarkoitukseen sopivammalta.

Tämän työn ohjeiden mukaan on mahdollista laajentaa verkkoa moniin työasemiin ja useampiin palvelimiin. Kaikkiin verkon Linux-koneisiin on vain tehtävä samat muutokset kuin työssä tehtiin koneelle Linuxclient.

Tämän työn jatko olisi seuraavaksi tehdä Linux-koneesta VPN-palvelin (Virtual Private Network). VPN-palvelin ohjaisi ammattikorkeakoulun oman verkon ulkopuolelta tulevat käyttäjät kirjautumaan aktiivihakemistoon niin, että tietoturva säilyy.

Oma kynnykseni lähteä tähän työhön Linuxin takia toi työn alussa ristiriitaisia ajatuksia, Linux-kokemukseni ollessa melkein olematon. Tässä vaiheessa ajatusmaailmani on kuitenkin vahvasti muuttunut. Ihmisillä saattaa olla automaattisesti kielteinen näkemys Linuxin käytöstä sen väitetyn monimutkaisuuden ja vaikeuden takia.

Nykyään Linux-käyttöjärjestelmiä kuitenkin kehitetään enemmän ja enemmän käyttäjäystävällisiksi niiden nousevan suosion johdosta. Voin tähänastisena Windows-käyttäjänä todeta molempien käyttöjärjestelmien olevan kuitenkin loppujen lopuksi käytettävyydeltään hyvinkin samanlaisia. Työn tuomien kokemuksien avulla seuraavana tehtävänä aion hankkia itselleni Linux-käyttöjärjestelmän omaan jokapäiväiseen käyttööni.

Oppimani kannalta työ antoi minulle paljon tietoutta ja taitoa molempien käyttöjärjestelmien puolesta. Tulevaisuudessa samankaltaisen projektin vastaanottaminen tapahtuu mieluisasti ja uskon sellaisessa onnistuvani uudestaankin, vielä paremmin. Toivon tekemäni työn antavan Satakunnan ammattikorkeakoululle mahdollisuuden käyttää ja soveltaa opinnäytetyön tuloksia omaan käyttöön sellaisen tarpeen tullessa.

LÄHDELUETTELO

Fedora wiki (2008). Fedora Overview [verkkosivu]. [Viitattu 2.1.2008]. Saatavissa: http://fedoraproject.org/wiki/Overview

Kivimäki, J. (2005). Windows Server 2003 - Tehokas hallinta. Jyväskylä. Gummeruksen Kirjapaino Oy.

Kivimäki, J. (2005). Windows Server 2003 Active Directory - Tehokas hallinta. Jyväskylä. Gummeruksen Kirjapaino Oy.

Linux.fi (2008). Fedora [verkkosivu]. [Viitattu 2.1.2008]. Saatavissa: http://linux.fi/index.php/Fedora_Core

Microsoft (2007). Yleistä Windows Server 2003 -tuoteperheestä [verkkosivu]. [Viitattu 29.10.2007]. Saatavissa: http://www.microsoft.com/finland/windowsserver2003/evaluation/overview/default.mspx

Microsoft Technet (2007). What´s New in Windows Server 2003 R2 [verkkosivu]. [Viitattu 29.10.2007]. Saatavissa: http://technet2.microsoft.com/windowsserver/en/library/f9d70026-ae8b-4969-8755-1ea1edc4e38e1033.mspx?mfr=true

Moskowitz, B. & Boutell, T. (2005). Windows and Linux Integration: Hands-on Solutions for a Mixed Environment. United States of America. Sybex.

Moskowitz, B. & Boutell, T. (2007). Windows and Linux Integration: Hands-on Solutions for a Mixed Environment (Web Appendix) [verkkoliite]. New Jersey. Wiley Publishing, Inc. [Viitattu 17.1.2008]. Saatavissa: http://www.winlinanswers.com/book/download.php?file=downloads/4428awebfinal.pdf

Nordberg T. 2008. LDAP-autentikointi eri käyttöjärjestelmissä. AMK-opinnäytetyö. Satakunnan Ammattikorkeakoulu, Tekniikka Rauma, tietotekniikan koulutusohjelma.

Vainio O. (2008). Satakunnan Ammattikorkeakoulu Tekniikka Rauma Verkkotyökurssi, LINUX Windows-verkon tiedostopalvelimena ja WWW palvelimena [moniste]. Rauma.