HAKEMISTOPALVELUN KÄYTTÖÖNOTTO LAHDEN AMMATTIKORKEAKOULUSSA

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2006
Mika Känkänen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

MIKA KÄNKÄNEN: Hakemistopalvelun käyttöönotto Lahden ammattikorkeakoulussa

Tietoliikennetekniikan opinnäytetyö, 60 sivua

Kevät 2006

TIIVISTELMÄ

Opinnäytetyö käsittelee hakemistopalvelun käyttöönottoa Lahden ammattikorkeakoulussa. Työn tavoitteena oli tehostaa Lahden ammattikorkeakoulun käyttäjä- ja työasemahallintaa hakemistopalvelulla. Hakemistopalvelulla pystytään hallitsemaan keskitetysti käyttäjä- ja tietokonetilejä sekä muita tietoverkon objekteja. Hakemistopalvelun käyttö helpottaa laajan verkkoympäristön ylläpitoa.

Työssä perehdyttiin hakemistopalvelun käsitteisiin ja LDAP-rajapintaan. Selvitystyön perusteella valittiin lähempään tarkasteluun kaksi hakemistopalvelua: Novell eDirectory ja Microsoft Active Directory. Seuraavaksi tutkittiin tarkasteluun valittujen hakemistopalveluiden soveltuvuutta Lahden ammattikorkeakoulun käyttöön vertailemalla niitä kokonaisvaltaisesti.

Soveltuvin järjestelmä Lahden ammattikorkeakoulun tarpeisiin testien perusteella oli Active Directory. Käyttöönotto aloitettiin vuonna 2001 ja päätettiin vuonna 2004. Aluksi ylläpitohenkilöstö perehdytettiin tehtäviinsä, ja lopuksi palvelu otettiin käyttöön laitos kerrallaan.

Työ täytti asetetut vaatimukset ja odotukset. Hakemistopalvelu otettiin käyttöön siihen osoitettujen resurssien puitteissa odotetusti ja järjestelmälle asetetut tavoitteet saavutettiin. Yhtenäinen hakemistopalvelu mahdollistaa jatkossa useita lisäpalveluja sekä vaivattomamman ylläpidon. Tietojärjestelmän yhtenäisyydellä saavutettiin ja tullaan saavuttamaan myös jatkossa resurssi- ja kustannushyötyjä.

Avainsanat: Active Directory, aktiivihakemisto, hakemistopalvelu, käyttöönotto, Novell eDirectory

Lahti University of Applied Sciences
Faculty of Technology

MIKA KÄNKÄNEN:

The implementation of Directory Services in Lahti University of Applied Sciences

Bachelor's thesis in Telecommunications Technology, 60 pages

Spring 2006

ABSTRACT

This study deals with the implementation of directory services in Lahti University of Applied Sciences. The objective was to build a centralized system, which would cover all the faculties of Lahti University of Applied Sciences. Directory Services help to maintain user, computer accounts and other network objects. It is useful in a large information technology environment.

The study describes the options which were considered to offer directory services in Lahti University of Applied Sciences. Two options were taken into closer investigation: Novell eDirectory and Microsoft Active Directory. The study describes how the environment was designed, how the detailed implementation was made and what kind of tests were performed in the laboratory.

The most appropriate system was Microsoft Active Directory because of the administrator's strong knowledge and skills with Windows-based systems. The implementation was initiated in 2001 and completed in 2004. First, the administrators were trained into using the new system, then Active Directory was implemented faculty by faculty.

All objectives were achieved with the implementation. Centralized administration enables new facilities. User and workstation maintenance is now simple and easy. It is possible to take full advantage from the directory services by connecting more data systems to the Active Directory in the future. Also, it was noticed that implementing the directory services helps to save costs and resources in IT-operations.

Keywords: Microsoft Windows Active Directory, directory service, implementation, Novell eDirectory

SISÄLLYS

LYHENNELUETTELO

AD	Active Directory, aktiivihakemisto. Microsoftin kehittämä hakemistopalvelu.
ADMT	Active Directory Migration Tool. Microsoftin kehittämä ohjelmisto käyttäjä-, ryhmä- ja tietokoneobjektien kopiointiin ja siirtoon toisesta järjestelmästä aktiivihakemistoon.
ASCII	American Standard Code for Information Interchange. 7-bittinen, 128 koodipaikkaa sisältävä merkistö.
BDC	Backup Domain Controller. Windows NT 4.0 tai Windows NT 3.51 -toimialueen ohjauspalvelin.
C	Country. LDAP-määrityksen objektiluokka, joka kuvaa objektin maanimeä.
CN	Common Name. LDAP-määrityksen objektiluokka, joka kuvaa objektin yksilöllistä nimeä.
DC	Domain Component. LDAP-määrityksen objektiluokka, joka kuvaa toimialueen nimeä.
DC	Domain Controller. Microsoftin aktiivihakemistossa sijaitseva toimialueen ohjauspalvelin.
DFS	Distributed File System. Windows 2000- ja 2003 -palvelimien tarjoama palvelu, jolla verkon tiedostoresurssit saadaan näkymään keskitetysti yhdeltä palvelimelta.

DIT	Directory Information Tree. LDAP-protokollassa määritelty hierarkinen hakemistopuu.
DN	Distinguished Name. LDAP-protokollalla toteutetun hakemistopuun globaalisti yksilöllinen nimi.
DNS	Domain Name Service. Tietoverkoissa käytetty standardoitu nimipalvelujärjestelmä.
DDNS	Dynamic Domain Name Service. Aktiivihakemiston dynaaminen nimipalvelu.
FQDN	Fully Qualified Domain Name. DNS-palvelun jakama toimialueen täydellinen nimi.
FRS	File Replication Service. Aktiivihakemistossa käytettävä tiedostopalveluiden replikointi.
FSMO	Flexible Single Master of Operations. Aktiivihakemiston palvelimien hallitsemat toimintaroolit.
FUNET	Finnish University and Research Network. Suomen korkeakoulujen ja tutkimuksen tietoverkko on suomalaista tutkimusyhteisöä palveleva nopea tietoliikenneverkko.
GP	Group Policy. Aktiivihakemiston ryhmäkäytäntö, jolla määritellään asetuksia käyttäjille, työasemille ja palvelimille.
HAKA	Tieteellinen laskenta Oy:n operoima, korkeakoulurajat ylittävä luottamusverkosto ja käyttäjähallinto.
HTTP	HyperText Transfer Protocol. Yhteysprotokolla, jota käytetään www-sivujen välittämiseen palvelimelta selaimelle.

HTTPS HyperText Transfer Protocol over Secure sockets Layer. Yhteysprotokolla, jota käytetään www-sivujen välittämiseen palvelimelta selaimelle salatusti.

IP Internet Protocol. Standardein määritelty Internet-protokolla. TCP/IP-protokollan ydin.

IT Information Technology. Tietokonevälitteinen tieto- ja viestintäteknologia.

KCC Knowledge Consistengy Checker. Aktiivihakemiston paikansisäinen replikointiprosessi.

L Locality. LDAP-määrityksen objektiluokka, joka kuvaa paikkakuntaa.

LAMK Lahden ammattikorkeakoulu. Päijät-Hämeen koulutuskonsernikuntayhtymään kuuluva itsenäinen liikelaitos.

MSI Microsoft Windows Installer. Käytäntömäärityksillä jaettava sovelluspaketti.

LDAP Lightweight Directory Access Protocol. Standardimääritelty hakemistopalveluprotokolla.

NAL Novell Application Launcher. Novellin hakemistopalvelussa käytetty sovellusten hallintatyökalu.

NDS Novell Directory Services. Novellin kehittämä hakemistopalvelu.

NTLM Windows NT Challenge/Response Method. Microsoftin vanhempien käyttöjärjestelmien autentikointimenetelmä.

NTP Network Time Protocol. UDP-protokollapinossa määritelty aikapalveluprotokolla.

O Organization. LDAP-määrityksen objektiluokka, joka kuvaa organisaation nimeä.

OID Object Identifier. LDAP-protokollalla toteutetun attribuutin yksilöllinen tunniste.

OU Organization Unit. Organisaatioyksikkö, jolla määritellään aktiivihakemiston looginen rakenne.

PDC Primary Domain Cotroller. Ensisijainen toimialueen palvelin aktiivihakemistossa.

RAID Redundant Array of Independent (or Inexpensive) Disks. Yleensä palvelimessa käytössä oleva vikasietoinen levyjärjestelmä.

RDN Relative Distinguished Name. Yksilöllinen nimi LDAP-hakemistossa.

RDP Rapid Deployment. Microsoftin tarjoama aktiivihakemiston käyttöönottokoulutus Suomen korkeakouluille.

RFC The Requests for Comments. Asiakirjoja, jotka kuvaavat erilaisia sovittuja teknisiä ja organisatorisia määritelmiä.

RID Relative ID. Aktiivihakemiston toimialueen palvelimen rooli, jolla hallitaan ja jaellaan yksikäsitteisiä arvoja muille toimialueen palvelimille.

S State. LDAP-määrityksen objektiluokka, joka kuvaa paikkakuntaa.

SID	Security Identifier. Aktiivihakemiston objektin yksikäsitteinen tunniste.
SMS	Systems Management Server. Lähinnä aktiivihakemiston työasemien ja palvelinten etäkäyttö-, ohjelmistolevitys- ja inventointisovellus.
SRV	Service Resource Record. Nimipalvelussa käytetty tiettyyn protokollaan viittaava tietue.
SUS	Software Update Service. Ajastettu, organisaation sisäinen Microsoft -käyttöjärjestelmien tietoturvakorjausten päivityspalvelin.
TCP	Transmission Control Protocol. Standardein määritelty kuljetusprotokolla.
UDP	User Datagram Protocol. Yhteydetön, TCP-kuljetuskerroksessa toimiva protokolla.
UNIX	Open Group -yhteenliittymän kuvaama monen käyttäjän käyttöjärjestelmäpohja.
WWW	World Wide Web. Internetin palvelu, jossa selaimella käytetään palvelimilla sijaitsevia sivustoja.

1 JOHDANTO

Lahden ammattikorkeakoulu on Päijät-Hämeen koulutuskonsernikuntayhtymään kuuluva itsenäinen liikelaitos. Päijät-Hämeen koulutuskonserni on 14 päijäthämäläisen kunnan omistama kuntayhtymä. Liikelaitoksia Lahden ammattikorkeakoulun lisäksi on Päijät-Hämeen koulutuskonsernissa koulutuskeskus Salpaus ja Tuoterengas.

Lahden ammattikorkeakoulu on Suomen suurimpia monialaisia korkeakouluja. Lahden ammattikorkeakoulussa annetaan kuutta koulutusalan opetusta kymmenessä laitoksessa ja toimipisteitä on kaksitoista. Toimipisteiden välinen tietoliikenne on toteutettu Päijät-Hämeen koulutuskonsernin verkossa nopeilla runkoyhteyksillä. Opiskelijoita Lahden ammattikorkeakoulussa on yhteensä hieman yli 5000, joista noin 1000 on aikuisopiskelijoita. Vakituista henkilöstöä on noin 400. Työasemia on noin 2000.

Kuvatun IT-ympäristön ylläpito vaati tehokkaan järjestelmän, jossa käyttäjä- ja työasematietokantaa pystytään hallitsemaan keskitetysti. Oppilaitosten hajanaisten atk-järjestelmien korvaajaksi otettiin käyttöön hakemistopalvelu. Palvelu kattaa sekä oppilaitosten että ylläpidon tarpeet palvelinten, työasemien, levypalveluiden, tulostuksen sekä käyttäjien keskitetyssä hallinnassa.

Työn tavoitteena oli täyttää luetellut tarpeet. Tavoitteena oli myös hyödyntää hakemistopalvelun LDAP-toimintoja eri järjestelmien välisessä tiedonsiirrossa.

2 HAKEMISTOPALVELU

2.1 Yleiskuvaus

Hakemistopalvelu on tietovarasto, jossa säilytetään tietoa verkon käyttäjistä ja resursseista sekä niiden välisistä suhteista. Jokaiselle hakemistossa esiintyvälle objektille voidaan määritellä lukematon määrä erilaisia attribuutteja, jotka kertovat esimerkiksi käyttäjän etunimen ja puhelinnumeron. Hakemistopalvelussa esimerkiksi käyttäjätunnus on objekti ja puhelinnumero attribuutti. Hakemiston tiedot ovat fyysisesti palvelimen kovalevyllä tietokantatiedostoissa.

Hakemistopalvelua hyödynnetään esimerkiksi organisaation toimintatapojen keskittämisessä ja yhtenäistämisessä. Hakemistopalvelun käyttöä ei rajoita organisaation mahdollinen maantieteellinen hajanaisuus.

2.2 Lightweight Directory Access Protocol

Hakemistopalveluissa yleisesti käytetty standardirajapinta eli LDAPv3 (Lightweight Directory Access Protocol Version 3) on yhteystapa, jonka avulla asiakasohjelma pystyy kommunikoimaan LDAP-palvelimen kanssa TCP/IP-verkossa. LDAP on Internet-standardiksi muodostunut hakemistoprotokolla, joka kehitettiin kevennetyksi versioksi X.500 -kyselyprotokollasta. LDAP määriteltiin vuonna 1993 ja parannettu määritys julkaistiin vuonna 1995. 1997 julkaistiin LDAP-rajapinnasta versio 3, jota useimmat hakemistopalvelut ensisijaisesti käyttävät. Versiossa 3 on parannettu yhteystavan tietoturvaominaisuuksia ja laajennettu sen toimintoja. LDAP:n versio 3 toimii yleensä TCP-protokollan päällä, mutta voi myös toimia UDP-protokollan päällä. (Wahl, Howes, Kille 1997.)

LDAP-protokolla edellyttää, että hakemistossa on yksi tai useampi palvelin, joka tarjoaa pääsyn hierarkiseen hakemistopuuhun (Directory Information Tree, DIT). Puu koostuu entryistä, joka on kuvattu seuraavassa kappaleessa. LDAP-toimintoa käytetään tavallisimmin jonkin tiedon etsimiseen hakemistosta, entryjen lisäykseen, poistoihin tai muutoksiin. (Wahl ym. 1997.)

Entry on nimetty paikka, joka sisältää tiettyjä attribuutteja. Attribuutilla on aina nimi, tyyppi sekä yksi tai useampi arvo. Entryn nimi, RDN (Relative Distinguished Name), on yksilöllinen. Seuraavassa on esimerkki entryn nimestä ja sen sisältämistä attribuuteista:

"CN=user1, Mail=user1@testi.local, ObjectClass=People"

Esimerkissä CN=user1 on entryn RDN. (Wahl ym. 1997.) Entryn paikan hakemistossa määrittää yksikäsitteinen objektin LDAP-nimi DN (Distinguished Name). DN kostuu RDN-nimestä ja globaalin hakemiston polusta. (Wahl ym. 1997.)

LDAP-määrittelyssä on myös kuvattu skeema (schema), joka on kokoelma attribuuttien ja objektiluokkien tyyppimääritelmiä sekä muita LDAP-toiminteisiin liittyviä tietoja. LDAP-hakemistojen skeema on laajennettavissa. Kullakin attribuutilla on selväkielisen nimen lisäksi yksilöllinen tunniste eli OID (Object Identifier). Esimerkiksi Suomen korkeakoulurajojen ylittävä käyttäjähallinto, HAKA, on määritellyt funetEduPerson-skeeman, jossa funetEduPersonStudentID-attribuutin eli opiskelijanumeron OID on 1.3.6.1.4.1.16161.1.1.10. (Wahl ym. 1997.)

2.3 Tekniikoiden rajaus

Suunniteltaessa hakemistopalvelun käyttöönottoa Lahden ammattikorkeakouluun oli otettava huomioon se, että käyttöönotto oli tehtävä niillä resursseilla, jotka olivat jo ennestään käytössä. Hakemistopalvelun käyttöönoton kriteereiksi valit-

tiin jo hallittujen alustojen osaaminen ja tekniikoiden edeltävä tuntemus.

Päijät-Hämeen koulutuskonsernin yksiköissä oli käytössä sekä Novellin että Microsoftin verkkokäyttöjärjestelmiä, joten Lahden ammattikorkeakoulun ympäristöön mahdollisesti sopivaksi hakemistopalveluksi rajattiin Novellin Directory Services (NDS) tai Microsoftin Active Directory (AD).

NDS-järjestelmää on käytetty Päijät-Hämeen koulutuskonsernissa vuodesta 1996. Koulutuskonsernin NDS-palveluissa oli useita koulutuskeskus Salpauksen laitoksia, yksi ammattikorkeakoulun laitos sekä henkilökunnan käyttäjätilit. NDS on myös Päijät-Hämeen koulutuskonsernin henkilökunnan käyttämän sähköpostijärjestelmän, Novell GroupWisen, alustana toimiva järjestelmä. NDS-järjestelmässä on käytetty hyväksi Novell NetWare ZENworks for Desktops -ohjelmistoa, jonka ominaisuuksia hyödyntäen on mm. hallittu työasemia, jaeltu työasemille ohjelmistoja ja määritelty käyttäjäkohtaisia asetuksia.

Microsoft Active Directory ei ollut käyttöönottoa suunniteltaessa käytössä missään Päijät-Hämeen koulutuskonsernin yksikössä. Lahden ammattikorkeakoulu sitä vastoin käytti lähes yksinomaan Windows NT -toimialueita. Myös isommissa koulutuskeskus Salpauksen laitoksissa oli käytössä Windows NT -toimialueita. Suurin osa käyttäjätileistä koko Päijät-Hämeen koulutuskonsernissa oli Windows NT -toimialueissa.

2.4 Novell Directory Services

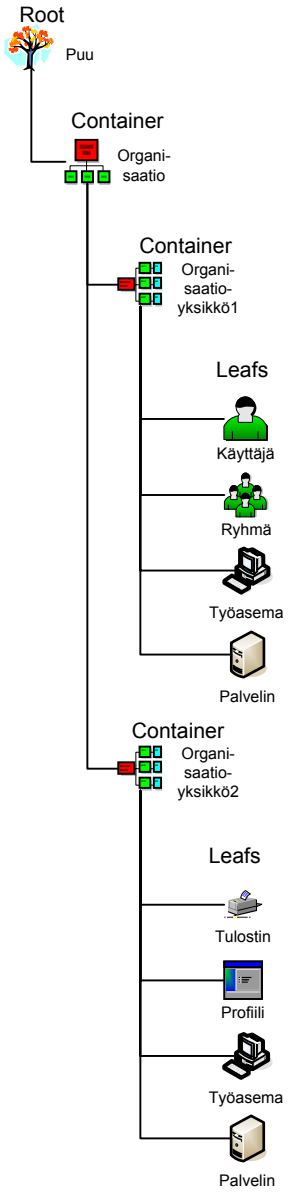
2.4.1 Rakenne

Novellin verkkokäyttöjärjestelmä, NetWare, ilmestyi 1980-luvun alussa nimellä ShareNet. Versiossa ei ollut juuri muuta verkkotoiminnallisuutta kuin tiedostojen ja tulostimien jakaminen verkossa käyttäjille. (Novell 1996.)

NetWaren versiot 2.x ja 2.3 olivat jo kehittyneitä verkkokäyttöjärjestelmiä, joiden avulla tallennettiin käyttäjä-, ryhmä-, tulostusjonotiedot ja tietoturva ACSII-muotoiseen, palvelinkohtaiseen tekstitiedostoon. Toiminto on nimeltään bindery. Rajoitteena oli kirjautumisen vaatiminen jokaiselle palvelimelle erikseen, koska käyttäjätiedot piti olla jokaisen palvelimen tietokannassa. (Novell 1996.)

Bindery-palvelun korvasi NDS-hakemistopalvelu (Novell Directory Services) versiossa 4.x. NDS-palvelun avulla kirjautuminen verkon resursseihin eli eri palvelinten resursseihin tapahtui keskitettyä hakemistopalvelua käyttäen. NDS-tuki oli ilmestyessä seuraaville käyttöjärjestelmille: DOS, Windows, OS/2, Macintosh ja UNIX. (Novell 1996.)

NDS on tietokantajärjestelmä, jossa järjestelmän informaatiota säilytetään puumaisessa hierarkisessa muodossa (kuvio 1). NDS-puu on jaettu osioihin (Partition), jotka levitetään valituille palvelimille, jotta palveluun saataisiin tietty vikasietoisuus. NDS esittää jokaisen verkon resurssin hakemistossa objektina. Objekteja NDS:ssä on juuri (root), säiliö (container) ja lehti (leaf). NDS-puurakenne haarautuu juuresta säiliöihin. (Novell 1996.)



KUVIO 1. Esimerkkirakenne eDirectorystä

Hakemiston juuri ei sisällä mitään tietoa. Sitä ei voi poistaa, nimetä uudelleen tai siirtää. NDS-hakemisto voi sisältää vain yhden juuren. Kaikki komponentit hakemiston rakenteessa ovat objekteja. Säiliöt voivat sisältää alisäiliöitä ja lehtiobjekteja. Objekteja käytetään järjestelmän loogisen hallinnan järjestelyyn ja niillä voidaan kuvata esimerkiksi eri maita, yhtiöitä, osastoja, työryhmiä ja jaettuja resursseja. Lehtiobjekteilla kuvataan mm. hakemistossa olevia käyttäjiä, ryhmiä, tulostimia, palvelimia, tallennuspaikkaa, aliaksia, työasemia ja tiedostoresursseja. (Novell 1996.)

Vuonna 1999 esiteltiin NDS-palvelusta uusi versio (versio 8), joka kantoi nimeä eDirectory. LDAP-tuki eDirectoryssä laajentui LDAP v3 -protokollalle. (Novell 2003, 353.)

Hakemistoa hallitaan Java-pohjaisella Novell ConsoleOne -ohjelmistolla (Novell 2005b, 11). Oletuksena ohjelma sallii eDirectoryn objektien, skeeman, partitioiden ja replikoiden sekä NetWare-palvelinresurssien hallinnan. (Novell 2006, 32.) Hallintatoimenpiteitä voidaan tehdä myös www-pohjaisella iManager-ohjelmistolla (Novell 2005c, 13).

2.4.2 ZENworks

Olennainen osa eDirectoryn tehokasta hallintaa on Novell ZENworks -ohjelmisto. Ohjelmistolla hallitaan verkon objekteja, kuten käyttäjiä, työasemia ja palvelimia. Ohjelmiston ominaisuudet olivat aiemmin integroitu NDS-palveluun, mutta ominaisuuksien ja muihin käyttöjärjestelmiin kytkentöjen laajentuessa on tuote eriytetty. (Novell 2005d, 9-13.)

Ohjelmiston ominaisuuksiin kuuluu:

- Desktop Management eli Windows-työasemien hallinta, kuten etätyöpöytäyhteys, inventointi, levykuvien ja käyttömääritelmien levitys
- Server Management eli NetWare-, Windows-, Linux- ja Solaris palvelinten hallinta, kuten ohjelmistojen levitys, päivitykset, inventointi jne.
- Handheld Management eli käsitietokoneiden hallinta
- Linux Management eli linux-palvelinten ja työasemien hallinta
- Asset Inventory eli verkon laitteiden inventointi ja laiterekisteri
- Data Management eli Novell iFolder, jolla tarjotaan levypalvelut organisaation verkkoon suojattuna internetin yli ja offline-tilan tiedostojen synkronoinnin verkon levypalvelimelle
- Instant Messenger eli tiedonvälityspalvelu
- Software Packaging eli MSI-pakettien hallinta
- Personality Migration eli työpöytänäkymien, hakemistojen ja tiedostojen

muunto ja varmistaminen
- Patch Management eli NetWare- ja Windows-järjestelmien päivitysten hallinta. (Novell 2005d, 9-13.)

2.4.3 Kirjautumispalvelut

Asiakkaiden kirjautuminen Novell eDirectory -järjestelmään tapahtuu Novell Client -ohjelmalla. Ohjelma on asennettava Windows ja Linux -työasemiin ennen kuin kirjautuminen on mahdollista. Kirjautumista tarvitaan, jotta asiakas pääsisi käyttämään hakemiston levy- ja tulostuspalveluja. (Novell 2005d, 31.)

Työasemaobjektin tuonti hakemistopuuhun hallittavaksi tapahtuu Novell ZENworks Desktop Management Automatic Workstation Import -toiminnon avulla. Työaseman ZENworks Desktop Desktop Management Agent -ohjelman Workstation Registration -osiolla otetaan yhteys palvelimen Import-palveluun, joka luo työasemaobjektin hakemistoon. Työasema rekisteröi itsensä hakemistoon aina, kun työasema käynnistyy tai käyttäjä kirjautuu joko hakemistoon, tai Windows 2000/XP -käyttäjä lopettaa istuntonsa. (Novell 2006, 105-106.)

Kun työasema on tuotu hakemistoon ja rekisteröity, voidaan sitä hallita keskitetysti verkon kautta. ZENworks-agentti on Windows-työasemissa nimeltään nalntsrv. Palvelu mahdollistaa työaseman hallinnan verkon yli työaseman järjestelmän oikeuksin. Hallintakomponenttien avulla voidaan esimerkiksi asettaa käyttäjien työpöytäasetuksia, ryhmäkäytäntöjä lähes kaikkien Windows 2000/XP -työaseman rekisteriasetuksen muutoksiin, käyttäjän työasemia etätyöpöydällä hallittaviksi, työasemien tilastotietoasetuksia, tulostusmäärityksiä jne. (Novell 2006, 119.)

Keskitettyjen käytäntöjen tekoon käytetään ConsoleOne-ohjelmistoa. Käytäntöjä voidaan kohdistaa säiliöille, palvelimille, palveluille, käyttäjille ja työasemille. (Novell 2006, 123.) Myös NAL-toiminnot tapahtuvat samalla agentilla. NAL on Novell ZENworks Desktop Management -ohjelmiston Novell Application Launcher -osio. Application Launcher -toiminnolla voidaan hallita sovellusten

jakelua työasemiin. Sovelluksia voidaan jaella Windows 98 SE-, Windows 2000- ja Windows XP -työasemiin. (Novell 2006, 209.)

2.4.4 Konteksti ja nimeäminen

Objektin kontekstilla tarkoitetaan sen sijaintia hakemistopuussa. Konteksti ilmaistaan peräkkäisillä Container-listauksilla pisteellä erotettuna. Esimerkiksi käyttäjä User1, joka on organisaatioyksikössä Users. Organisaatioyksikkö Users on edelleen organisaatioyksikössä laitos, joka kuuluu organisaatioon LAMK, ilmaistaan muodossa: User1.Users.laitos.LAMK. Esitettyä ilmaisumuotoa kutsutaan DN-nimeksi (Distinguished Name). (Novell 2003, 74.)

2.4.5 Skeema

Skeema määrittelee kaikki hakemiston objektit, joita on mahdollista tehdä hakemistopuuhun. Objektilla on aina määritelty jokin luokka (Class). Esimerkiksi puhelinnumero on luokassa User. (Novell 2003, 76.)

EDirectory-järjestelmän perusskeemaa (base schema) ei välttämättä ole tarpeellista laajentaa, mutta se on mahdollista. Jos perusskeemaan tehdään muutoksia eli lisätään esimerkiksi uusia luokkia tai attribuutteja kutsutaan skeemaa laajennetuksi skeemaksi (extended schema). (Novell 2003, 76.) Skeemaa hallitaan Novell iManager -ohjelmistolla. Sillä voi listata kaikki halutut luokat ja attribuutit. Ohjelmistolla näkee myös attribuutin tiedot. (Novell 2003, 77.)

2.4.6 Partitiointi

Hakemistopalvelun tietokantaa voidaan jakaa eri palvelimille. Syinä voivat olla esimerkiksi hitaat tai epäluotettavat yhteydet toimipaikkojen välillä, yhden palvelimen liiallinen kuormitus jne. Tällaista toimenpidettä kutsutaan partitioinniksi (partitioning). Partitioinnilla saadaan järjestelmään myös nopeutta ja luotettavuut-

ta. (Novell 2003, 82.)

Mikäli organisaation käytössä on hitaiden tai epäluotettavien tietoliikenteellisten yhteyksien päässä etäpiste, voidaan hakemistopalvelu hajauttaa perustamalla etäpisteeseen palvelin tai palvelimia, joissa on osa tai kaikki hakemistopalvelun tietokannasta. Etäpisteen palvelinpartitioinnilla saavutetaan tilanne, jossa käyttäjät kirjautuvat suoraan omassa toimipaikassa sijaitsevaan palvelimeen eivätkä esimerkiksi hankalien ja hitaiden tietoliikenneyhteyksien päähän. Myös puunäkymän osia voidaan osoittaa toiselle palvelimelle. Kun muutoksia ja toimenpiteitä tehdään määriteltyyn partitioon, ei synny hallitsematonta liikennettä etäpaikkojen välille tai liiallista kuormitusta pelkästään yhdelle palvelimelle. (Novell 2003, 85.)

2.4.7 Replikointi

Replika (replica) on kopio määritellystä partitiosta jollakin eDirectory-palvelimella. Novellin eDirectory-järjestelmässä suositellaan pidettäväksi yllä kolmea replikaa hakemistopalvelun tietokannasta. Asennettaessa eDirectory-palvelimia samaan puuhun kolme ensimmäistä palvelinta ottaa automaattisesti itselleen replika-roolin hakemistosta. (Novell 2003, 86.)

Replika-palvelin on dedikoitu palvelin. Sillä on kaksi päätehtävää: ylläpitää tietokannan kopiota vikasietoisuuden takaamiseksi ja tarjota kirjautumispalveluita esimerkiksi hitaan tai muuten epäluotettavan etätoimipaikan asiakkaille. Replika-palvelin pitää kopiota ainoastaan hakemistopalvelun tietokannasta. Se ei tarjoa esimerkiksi vikasietoisuutta tiedosto- tai tulostuspalveluihin. (Novell 2003, 86.)

Replikoita on useita eri tyyppejä:

- Master Replica
- Read/Write Replica
- Read-Only Replica
- Filtered Read/Write Replica
- Filtered Read-Only Replica

- Subordinate Reference Replica. (Novell 2003, 87.)

Master Replica -rooli on oletuksena palvelimella, johon eDirectory ensimmäisenä asennetaan. Master Replica -roolin omaavia palvelimia voi olla yhdessä partitiossa vain yksi kerrallaan. Palvelimen tehtävänä on hallinnoida replika-tapahtumia, kuten lisätä replikoita palvelimille, poistaa niitä, luoda uusia partitioita puuhun, poistaa sekä uudelleen sijoittaa partitioita. Lisäksi Master Replica -palvelin hallinnoi muita eDirectory-tapahtumia, kuten uusien objektien ja attribuuttien lisäämisen eDirectory-puuhun, sekä objektien ja attribuuttien poistamisen, uudelleennimeämisen ja uudelleensijoittamisen. (Novell 2003, 87.)

Palvelimella, jolla on Read/Write Replica -rooli, pystytään myös tekemään kirjoitusoperaatioita kuten Master Replica -palvelimeenkin. Read/Write Replica -palvelinta voidaan hyödyntää esimerkiksi etätoimipaikassa, jossa muutostapahtumia tulee paljon. Näin vähennetään liikennettä toimipisteiden välillä ja saavutetaan parempi käytettävyys jos tietoliikenteelliset yhteydet eivät ole luotettavat. (Novell 2003, 88.)

Palvelimen, jolla on Read-Only Replica -rooli, ensisijainen käyttötarkoitus on parantaa eDirectory-puun vikasietoisuutta. Palvelin ylläpitää kopiota määritellystä partitiosta. Siihen ei voi kirjoittaa tietoja. Jos Master Replica- tai Read/Write Replica -palvelimet tuhoutuvat tai vahingoittuvat, voidaan Read-Only Replica -palvelimen rooli korottaa kirjoitusoikeudelliseksi palvelimeksi. (Novell 2003, 88.)

Palvelin, jolla on Filtered Read/Write Replica -rooli, toimii samoin kuin Master Replica- tai Read/Write Replica -palvelimet, mutta sille on määritelty suodatin, jossa määrätään, mihin objekteihin tai objektiluokkiin on muutoksia mahdollista tehdä (Novell 2003, 88).

Palvelin, jolla on Filtered Read-Only Replica -rooli, toimii samoin kuin Read-Only Replica -palvelin, mutta sille on määritelty suodatin, jossa määrätään, mitä objekteja tai objektiluokkia palvelimeen replikoidaan (Novell 2003, 88).

Subordinate Reference Replica on sisäinen osoitin, jonka hakemisto itse poistaa, kun sen käyttötarve on täytetty. Hakemistopalvelu luo sisäisen osoittimen, kun halutaan selvittää nimiä yli partitiorajojen. Se ei tarjoa vikasietoisuutta, eikä siihen voi kirjoittaa tietoja. Sillä ei ole koko hakemiston tietoja, ja se sisältää vain tarvittavan informaation, jotta se voi selvittää objektien nimet yli partitiorajojen. (Novell 2003, 88-89.)

Onnistuneen replikoinnin edellytys on oleellinen Novell-käyttöjärjestelmän palvelu. Onnistuneen replikoinnin takaa aikapalvelu. Eri roolillisten palvelinten on oltava aina aikasynkronissa. Aikasynkronointia (Time synchronization) ohjaa palvelinten kesken aikapalvelu, joka on käyttöjärjestelmän palvelu. Hakemistopalvelun toimenpiteistä huolehtii sen oma sisäinen aika. Hakemistopalvelu saa ajan käyttöjärjestelmästä. (Novell 2003, 119.)

Oikeellisen ajan saaminen palvelimiin tapahtuu kerroksittain. Aika haetaan luotettavasta aikalähteestä aikapalvelin1:een UDP-protokollapinoon kuuluvalla NTP-protokollalla. Aikapalvelin2 ottaa taas aikansa aikapalvelin1:stä jne. Aikasynkronointi Novell-palvelinten kesken määritellään dsrepair.nlm -palvelun kautta eDirectory-palvelimella. (Novell 2003, 120-121.)

2.4.8 LDAP

Novell eDirectory-järjestelmässä LDAP on palvelu, joka asennetaan palvelimeen ja jonka kautta asiakkaat kommunikoivat hakemistopalveluiden kanssa. Asiakas pystyy lukemaan hakemistosta ja kirjoittamaan hakemistoon sille annettujen oikeuksien puitteissa. LDAP-palvelu on Novell Netware -palvelimessa nimeltään nldap.nlm, Windows 2000/NT -palvelimissa nldap.dlm, Linux, Solaris ja AIX -palvelimissa systemslibnldap.so tai HP-UX -palvelimessa libnldap.sl. (Novell 2003, 298.)

Novell eDirectoryn LDAP eroaa hakemistopalveluiden LDAP-standardirajapinnasta joiltakin osin, eli mm. LDAP-lyhenteiden erotteissa käytetään pilkkujen sijasta pisteitä. Myös LDAP-nimessä eDirectory käyttää sekä

LDAP-määritteen mukaista muotoa että omaa tyypittämätöntä muotoa. Esimerkiksi LDAP-polku CN=User1,OU=Users,O=yritys voidaan ilmaista eDirectoryssä muodossa: User1.Users.yritys. Novell eDirectory käyttää myös LDAP-määrityksestä poikkeavaa plus-merkkiä (+) LDAP-polussa. (Novell 2003, 307.) Novell eDirectoryssä käytettävät FQDN- ja DN-nimet pohjautuvat X.500-standardiin ja perustuvat taulukossa (taulukko 1) esitettyihin määritelmiin (Novell 2003, 74).

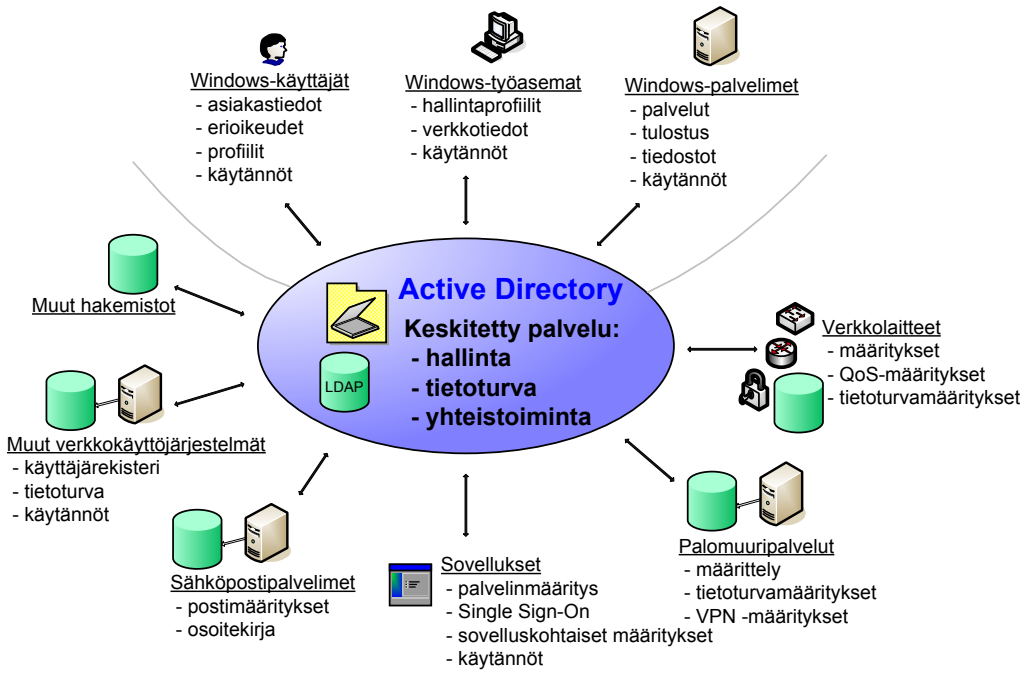
TAULUKKO 1: eDirectoryn käytettyjen objektityyppien lyhenteet (Novell 2003, 74)

Objektiluokka	Tyyppi	Lyhenne
Lehtiobjektiluokat	Common Name	CN
Organisaatio	Organization	O
Organisaatioyksikkö	Organizational Unit	OU
Maa	Country	C
Paikkakunta	Locality or State/Province	L tai S

2.5 Microsoft Active Directory

2.5.1 Rakenne

Active Directory eli aktiivihakemisto (kuvio 2) on Microsoftin kehittämä hakemistopalvelu Windows 2000- ja Windows 2003 -käyttöjärjestelmien toimialueen palveluissa. Aktiivihakemistossa on tietokanta, joka sisältää erityyppisiä tietoja verkon objekteista, kuten käyttäjistä, käyttäjäryhmistä, työasemista ja palvelimista. Aktiivihakemiston kommunikointirajapinta on LDAP. Aktiivihakemiston LDAP tukee versioita 2 ja 3. (Microsoft 2000a, 24.) Aktiivihakemistolla saadaan kaikki hakemistopalvelun hyödyt sekä pystytään määräämään eri verkon resursseille keskitetysti käyttömäärityksiä ja käytäntöjä. (Microsoft 2001a.)



KUVIO 2. Aktiivihakemisto

2.5.2 Windows 2000

Windows 2000 Server on Microsoftin kehittämä palvelinkäyttöjärjestelmä, jolle voidaan määrätä eri rooleja käyttötarkoituksen mukaan. Yksi Windows 2000 -palvelinkäyttöjärjestelmän rooleista on toimialueen ohjauskone. Toimialueen ohjauskoneen tuottama palvelu on aktiivihakemisto, Active Directory. (Microsoft 2001a.)

Windows 2000 -järjestelmä eroaa valmistajan aiemmista palvelintuotteista, Windows NT:n eri versioista, uutena ominaisuutena tulleen hakemistopalvelunsa osalta. Active Directory mahdollistaa yhtenäisen, laajan maantieteellisen tai organisaation kattavan käyttäjä- ja laitetietokannan. Käyttäjä kykenee aktiivihakemistossa kirjautumaan mille tahansa toimialueelle liitetylle työasemalle asetetuista määrityksistä riippuen ja saada käyttöönsä omat määritellyt resurssit riippumatta maantieteellisestä tai organisatorisesta sijainnista. (Microsoft 2001a.)

Organisaatioissa, joissa käytetään aktiivihakemistoa, on huolehdittava siitä, että palvelinlaitteisto on vikasietoinen, luotettava ja nopea. Vikasietoisuus toteutetaan yleensä RAID1- tai RAID5-tasoisilla hotswap-levyjärjestelmillä ja vähintään kahdella palvelinlaitteella. Mikäli jokin palvelimen levyistä tai toinen toimialueen ohjauskoneista vikaantuisi, autentikointi- ja levypalvelut toimivat silti keskeytyksettä. Laitteiden on sijaittava mahdollisimman tieto- ja paloturvallisessa ympäristössä eli käytännössä tarkoitusta varten rakennetussa konehuoneessa. (Microsoft 2001a.)

2.5.3 Nimi- ja kirjautumispalvelut

Nimipalvelun ja -palvelimen toiminta on olennainen osa aktiivihakemiston toimintaa. Aktiivihakemistossa käytettävä nimipalvelu on nimeltään Dynamic Domain Name System (DDNS). Se perustuu standardoituun DNS-palveluun. Nimipalvelun tehtävänä on aktiivihakemiston työasemien ja palvelinten nimiselvitys, koneeseen kytkettyjen palveluiden määritys, nimikyselyt organisaation verkon ulkopuolelle sekä sisäisen verkon työasemien nimien dynaaminen ylläpito.

DDNS-toiminnon avulla palvelimet ja muut asiakkaat päivittävät vyöhykkeen tietokantaa automaattisesti. (Lowe-Norris 2001, 117.)

Aktiivihakemistossa on myös mahdollista käyttää esimerkiksi olemassa olevaa UNIX-pohjaista nimipalvelua. Nimipalvelun on kuitenkin tuettava dynaamisia päivityksiä ja SRV-tietueita (Service Location). (Lowe-Norris 2001, 117.)

Aktiivihakemistossa suositellaan käytettäväksi Windows 2000 -pohjaista dynaamista DNS:ää paremman tietoturvan saavuttamiseksi. Aktiivihakemiston DDNS:ssä on mahdollista määritellä nimikyselyt ainoastaan toimialueeseen liitettyjä työasemia tai palvelimia koskeviksi, mikä parantaa nimipalvelun tietoturvaa. Aktiivihakemistoon integroitu DDNS parantaa myös nimipalvelun käytettävyyttä, tietoturvaa ja nopeutta. Vikasietoisuuden takaamiseksi on suositeltavaa käyttää vähintään kahta DNS-palvelinta. DNS on määritelty RFC-dokumenteissa 1034 ja 1035. (Lowe-Norris 2001, 117.)

Kirjautumispalvelimia suositellaan myös olevan vähintään kaksi. Toisen vikaantuessa kaikki palvelut toimivat keskeytyksettä. Organisaation toimialueen ohjauspalvelinten eli kirjautumispalvelimien määrä riippuu verkon koosta, rakenteesta sekä tarvittavasta palvelutasosta. Pienessä verkossa kirjautumis- ja nimipalvelimet voivat olla samoissa palvelinlaitteissa. (Microsoft 2001a.)

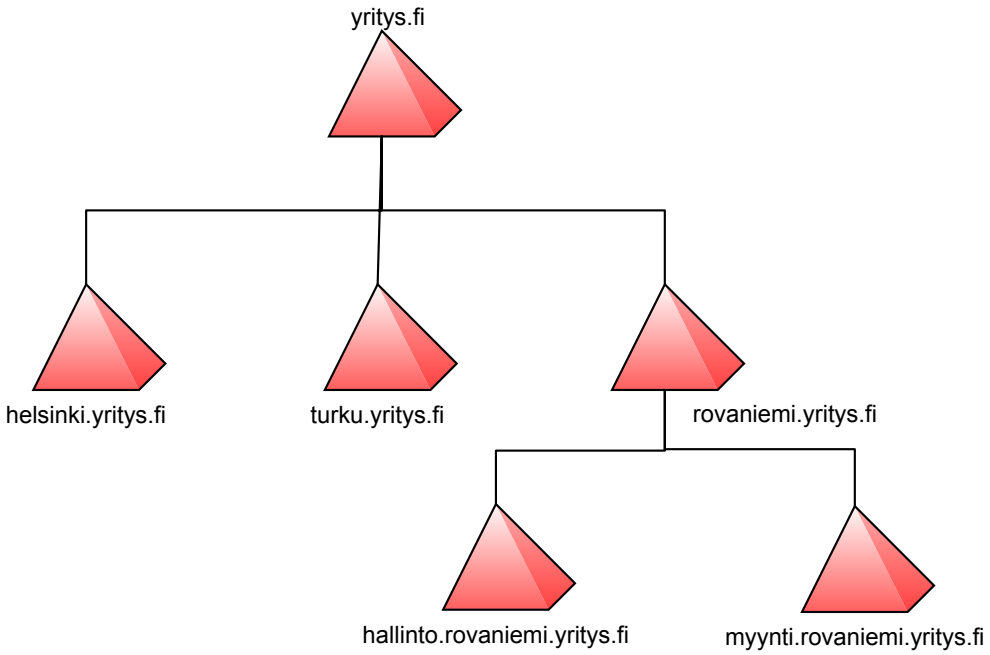
Palvelinten tarvittavan määrän laskemiseen organisaation tarpeisiin on olemassa Microsoftin www-sivuilta saatava työkalu, Active Directory Sizer. Ohjelmisto laskee palvelinten kuorman ja tarpeen syötettyjen tietojen pohjalta. Syötettäviä tietoja ovat esimerkiksi käyttäjien, ryhmien ja kirjautumistapahtumien arvioitu määrä, tietoliikenteellisten yhteyksien taso sekä käytetyiden toimialueen palvelimen prosessoreiden teho ja määrä. (Microsoft, 2001b.)

2.5.4 Toimialue

Toimialue (domain) on käsite, johon Windows 2000 -aktiivihakemiston looginen rakenne perustuu. Toimialue on vähintään yhden toimialueen ohjauspalvelimen

tarjoama palvelu, joka on aktiivihakemiston pienin osa. Toimialue rajoittaa verkon objektit, toimialueen DNS-nimen, suojauspalvelut ja menettelykäytännöt yhteen hallinnolliseen kokonaisuuteen. Toimialueen malleja kuvataan metsä- ja puurakenteilla. Kun ensimmäinen hakemistopalvelun tietokantaa ylläpitävä palvelin asennetaan, on siinä automaattisesti metsä ja toimialue, jota sanotaan toimialuepuun juuritoimialueeksi. Toimialueen symboli on kirjallisissa julkaisuissa yleensä kolmio. (Lowe-Norris 2001, 33.)

Toimialueita pystytään yhdistämään luottosuhteilla (kuvio 3). Monen toimialueen hierarkista rakennetta kutsutaan puurakenteeksi eli toimialuepuuksi (domain tree), johon tulee aina automaattisesti luottosuhde toimialueiden välille. Toimialuepuu on myös nimeämiskäytännön raja, jonka nimen loppuosan määrä juuritoimialue, eli toimialueiden nimet ovat hierarkisia. (Lowe-Norris 2001, 34.)



KUVIO 3. Toimialuepuu

Monen toimialuepuun rakennetta kuvataan määrityksellä metsä (forest), joka on monen toimialuepuun muodostama toiminnallinen kokonaisuus. Metsiä voidaan koota luottosuhteilla toisiinsa liittymättömiksi toimialuepuiksi ja eri metsillä voi olla erilaiset hierarkiset nimeämiskäytännöt. Microsoft Windows 2000 Active

Directory -palvelun metsän juuritoimialuetta ei voi poistaa. Jos se poistetaan, metsä lakkaa olemasta. (Lowe-Norris 2001, 35.)

2.5.5 Organisaatioyksikkö ja ryhmäkäytäntö

Organisaatioyksikkö eli OU (Organizational Unit) on hakemiston puumaisen rakenteen objekti, joka toimii säiliönä muille objekteille. Se on hallittavuuden kannalta tärkein objekti toimialueessa. Aktiivihakemiston käyttäjä-, työasema-, ryhmä-, yms. objektit sijoitetaan lähes aina organisaatioyksiköihin. Organisaation rakenne voidaan esimerkiksi kuvata ja jaotella aktiivihakemistossa organisaatioyksiköiden hierarkisella sijoittelulla eli organisaatioyksiköiden sisäkkäisillä sijoitteluilla. Yleensä tällaista rakennetta kutsutaan organisaatioyksikkörakenteeksi. (Lowe-Norris 2001, 35.)

Toinen säiliö, johon objekteja sijoitetaan, on järjestelmäsäiliö (Container). Hakemistopalvelu luo säiliön tarvittaessa itse. Tällaisia säiliöitä ovat mm. Computers- ja Users -järjestelmäsäiliöt, jossa Active Directory säilöö oletuksena työasema- ja käyttäjäobjekteja. (Lowe-Norris 2001, 36.)

Ryhmäkäytäntö eli Group Policy on sääntö tai määritys, jonka pystyy määrittelemään tietokone- tai käyttäjäobjektille keskitetysti. Suuren organisaation tai tietoverkon käyttäjiä, työasemia ja palvelimia on mielekkäintä hallita keskitetysti ryhmäkäytäntöjen avulla. Ryhmäkäytäntöjen voidaan sanoa olevan aktiivihakemistoa käyttävän organisaation keskitettyyn hallintaan suurin vaikuttavin osa-alue. Ryhmäkäytännön voi kohdistaa vain organisaatioyksikköön. Ryhmäkäytännöllä voidaan vaikuttaa lähes kaikkiin Windows 2000- ja Windows XP -työasemissa oleviin rekisteriasetuksiin. Ryhmäkäytäntöasetuksia, joita voidaan kohdistaa esimerkiksi Windows XP -työasemaan, on noin 1300 kappaletta. (Lowe-Norris 2001, 245.)

Ryhmäkäytäntöjä muokataan Group Policy Editorilla, joka on Microsoftin Management Consoleen liitettävä ohjelma. Muu ryhmäkäytäntöjen hallinta tehdään Group Policy Management Console -ohjelmalla. (Lowe-Norris 2001, 245.) Ryh-

mäkäytäntöjen määrittelytiedot eli ryhmäkäytäntöoliot sijaitsevat aktiivihakemiston yksittäisessä järjestelmäsäiliössä. Säiliön LDAP-polku on:

LDAP://CN=Policies,CN=System,DC=yritys,DC=fi

Ryhmäkäytäntöjen mallipohjien avaintiedot sijaitsevat toimialueen palvelimien järjestelmälevyn tiedostoissa ja hakemistoissa eli asennuksen yhteydessä määritellyn Sysvol-hakemiston alla olevassa Policies-hakemistossa. Kukin ryhmäkäytäntö on omassa hakemistossa, joka on nimetty ryhmäkäytännön Security ID:n mukaisesti. (Lowe-Norris 2001, 265.)

Ryhmäkäytäntöoliot yhdistetään tarpeen mukaan hakemistopuussa olevaan organisaatioyksikköön tai organisaatioyksiköihin. Yhden ryhmäkäytännön yhdistämisten määrää ei ole rajoitettu. Voidaan siis esimerkiksi tehdä ryhmäkäytäntöjä, jotka määrittävät globaalin organisaation työntekijöiden www-aloitussivun halutuksi useaan eri organisaatioyksikköön eli organisaation toimipisteisiin. (Lowe-Norris 2001, 265.)

Ryhmäkäytännöillä on myös mahdollista jakaa MSI-sovelluspaketteja eli esimerkiksi jaella haluttuihin verkon työasemiin haluttu sovellus. Windows Installer -palvelu asentaa sovelluksen tietokoneeseen automaattisesti verkon levyresurssista. (Microsoft 2001a.)

2.5.6 Replikointi

Replikointitarpeita palvelee kaksi replikointitapahtumaa: tiedostoreplikointi ja aktiivihakemiston replikointi. Aktiivihakemiston replikointi perustuu kolmen hakemistopartition replikointiin: skeematiedon (Schema information), määrittelytiedon (Configuration information) ja toimialueen datan (Domain data). Toimialueen palvelimet luovat automaattisesti replikointirenkaan, jossa replikoidaan vain muuttuneet tiedot. (Microsoft 2000b, 45-46.) Toimipaikan sisäistä replikointia kutsutaan intrasite-replikoinniksi. (Lowe-Norris 2001, 93.)

Tiedostoreplikointiprosessia ohjaa FRS-replikointi (File Replication Service). FRS replikoi mm. aktiivihakemiston DFS-juuren ja sysvol-kansion, missä kaikki ryhmäkäytännöt ja kirjautumisskriptit sijaitsevat fyysisesti. Replikointi tapahtuu oletuksena 15 minuutin välein. (Microsoft 2000b, 334.)

Toimipaikka (Site) on käsite, joka sisältää yhden tai useamman toimialueen palvelimen palvelevan osion verkosta. Toimipaikan verkon komponentit ovat kaikki samassa nopeiden tietoliikenteellisten yhteyksien ulottuvilla olevassa fyysisessä verkossa. Jos organisaatiolla on esimerkiksi kaksi käyttäjä- ja työasemamäärältään isoa toimipistettä, joiden välillä on hidas, epäluotettava tai kuormitettu tietoliikenneyhteys, on verkko syytä jakaa kahteen toimipaikkaan. Kummassakin paikassa on oltava vähintään yksi toimialueen palvelin, joka palvelee toimipisteen kirjautumisia. Toimipaikkarakenteella luodaan varmemmat ja nopeammat kirjautumispalvelut ja tietokantahaut. (Lowe-Norris 2001, 93.)

Eri toimipaikkojen toimialueen palvelimien tietokantojen muutoksissa replikoidaan eli kahdennetaan vain muuttuneet tiedot toimipaikkojen välillä. Toimipaikkojen välistä replikointi kutsutaan intersite-replikoinniksi. (Lowe-Norris 2001, 93.)

Toimipaikkarakenne ei synny automaattisesti. Toimipaikkojen suunnittelu ja luonti on ylläpitäjien tehtäviä. Kun toimipaikat on luotu ja määritelty, aktiivihakemistoon tehtyjen toimialueiden replikointi tapahtuu luotujen toimipaikkojen määrityksien avulla automaattisesti. Tätä paikansisäistä replikointia prosessoi palvelu nimeltään Knowledge Consistengy Checker (KCC). (Lowe-Norris 2001, 93.)

Bridge Head -palvelin on yksi toimialueen manuaalisesti asetettavista palvelimista, jonka tehtävänä on hoitaa replikointi mahdollisten site-yhteyksien välillä. Tavallistakin toimialueen palvelinta voidaan käyttää replikointiin, mutta erillisellä Bridge Head -palvelimella prosessia hallitsee luotettava dedikoitu palvelin, joka ei häiritse toimialuepalvelimien kirjautumisprosesseja. (Microsoft 2000b, 171.)

2.5.7 Global Catalog

Kun aktiivihakemistosta haetaan tietoja, haku kohdistuu ensimmäiseksi yleiseen luetteloon (Global Catalog). Luettelossa on valittuja objekteja ja attribuutteja verkon olioista. Yleisen luettelon avulla optimoidaan aktiivihakemistoon tehtyjä hakuja. Jos tietoa yleisestä luettelosta ei löydy, haku kohdistetaan aktiivihakemistoon. (Lowe-Norris 2001, 40.)

Yksi tai useampi toimialuepalvelin toimii aktiivihakemistossa yleisten hakujen luettelona. Kun haku kohdistuu yleiseen luetteloon, tietoa etsitään metsälaajuisesti. Yleisessä luettelossa on tieto kaikkien toimialueiden olioista koko metsässä. Jos käytössä on maantieteellisesti kattava toimialuepuu, on toimialueen palvelimien yleisten luettelojen sijoittelulla suuri merkitys verkkoliikenteeseen. Kannattavinta on sijoittaa vähintään yksi Global Catalog toimipaikkaa kohden. Yleinen luettelo määritellään aktiiviseksi toimialueen palvelimessa Site and Services -ohjelmistolla valitsemalla haluttu palvelin yleistä luetteloa ylläpitäväksi. Yleisen luettelon ominaisuuksia voidaan myös muokata Schema Manager -ohjelmistolla. Ylläpitäjä voi valita, mitä hakuja yleiseen luetteloon on mahdollista kohdistaa. (Lowe-Norris 2001, 40.)

2.5.8 FSMO-roolit

Toimialueen ohjauskoneilla eli palvelimilla on aina määriteltävissä viisi FSMO-roolia (Flexible Single Master Operation). FSMO-toiminnoilla pystytään jakamaan verkon palvelinten kuormaa määrittelemällä tiettyjä rooleja halutuille palvelimille. Asennettaessa metsän ensimmäinen palvelin, on siinä automaattisesti kaikki FSMO-roolit. (Lowe-Norris 2001, 43.)

FSMO-roolien jakautumisessa verkossa toimialueen palvelimien kesken ei ole automatiikkaa, vaan suunnittelun ja hallinnan on tapahduttava ylläpitäjien toimesta. Roolien hallinta tapahtuu Active Directory Users and Computers, Schema Manager tai Active Directory Domain and Trusts -työkalujen avulla. Viidestä FSMO-roolista, kaksi roolia on metsälaajuisia ja kolme toimialueen rooleja. (Lo-

we-Norris 2001, 43.)

Schema master -roolilla sallitaan omistajapalvelimen tehdä muutoksia aktiivihakemiston skeemaan. Roolin hallinta tapahtuu Schema Manager -työkalulla. Schema master -rooli on metsälaajuinen. (Lowe-Norris 2001, 44.) Domain naming master -roolin omistajapalvelin hallitsee mahdollisia muutoksia toimialueen nimiavaruuteen. Roolin hallinta tapahtuu Active Directory Domain and Trusts -työkalun avulla. Domain naming master -rooli on metsälaajuinen. (Lowe-Norris 2001, 45.)

Jos vanhempia Windows NT- tai Windows 3.51 -palvelimia on aktiivihakemistossa toimialuepalvelimen roolissa (aktiivihakemiston Mixed Mode), PDC emulator replikoi niille SAM-tietokannan ja mainostaa PDC-roolia. Vanhojen palvelinversioiden palvelimet hallitsevat BDC-rooleja, jotka saavat aina replikointitietonsa PDC emulator -roolilliselta palvelimelta. Myös salasanavaihtojen tieto välittyy aktiivihakemiston Mixed Modessa palvelimeen, jolla on PDC emulator -rooli. Kyseinen palvelin välittää tiedot edelleen palvelimille, joilla on BDC-rooli. PDC emulator -rooli on toimialuelaajuinen. (Lowe-Norris 2001, 45.)

Relative Identifier master eli suhteellisten tunnisteiden isäntä hallitsee ja jakelee yksikäsitteisiä RID-arvoja (Relative ID) muille toimialueen palvelimille. RID-arvon perusteella mikä tahansa toimialueen palvelimista voi luoda objektille sen yksikäsitteisen turvatunnuksen eli SID-arvon (Security Identifier). Jotta päällekkäisiä SID-arvoja ei tulisi, on yhden palvelimen eli RID-roolillisen palvelimen hallittava arvojen jakelua toimialueessa. Relative Identifier master -rooli on toimialuelaajuinen. (Lowe-Norris 2001, 45.)

Jos metsässä on enemmän kuin yksi toimialue, Infrastructure master eli pohjarakenteen isäntä pitää yllä viittauksia muiden toimialueen olioihin. Palvelin, jolla Infrastructure master -rooli, on koko ajan tietoinen omaan toimialueeseen kytkettyjen toisen toimialueen olioista, vaikka niitä siirreltäisiin, poistettaisiin tai luotaisiin lisää. Viittaukset tapahtuvat olion SID-turvatunnuksella. Infrastructure master -rooli on toimialuelaajuinen. RID-, PDC- ja Infrastructure Master -roolihallinnat

tehdään Active Directory Users and Computers -työkalun avulla. (Lowe-Norris 2001, 46.)

Yhden toimialueen ja kahden palvelimen mallissa ei ole välttämättä tarpeellista muuttaa ensimmäiseksi asennetun toimialueen palvelimen FSMO-rooleja. Laajan, monen toimialueen ja usean etäällä toisistaan fyysisten yhteyksien päässä olevien palvelinten roolit on suunniteltava huolellisesti. (Microsoft 2001a.) Esimerkiksi 14 toimialueen metsässä on automaattisesti vähintään 44 palvelinta, joilla on FSMO-rooli. Näistä rooleista kaksi FSMO-roolia ovat metsälaajuisia ja 42 toimialuekohtaista roolia. (Lowe-Norris 2001, 43.)

2.5.9 Skeema

Schema eli skeema on aktiivihakemiston LDAP-rajapinnan fyysinen rakennemalli. Se on perusasetus aktiivihakemistoon tallennettaville luokille, attribuuteille ja syntakseille. Skeemassa määritellään esimerkiksi, mikä attribuutti kuuluu mihinkin luokkaan. Oletuksena on esimerkiksi määritelty, että tieto käyttäjän puhelinnumerosta kuuluu user- eli käyttäjäluokkaan. (Lowe-Norris 2001, 64.)

Rakennemalli on muokattavissa ja laajennettavissa. Skeemaa muokataan Active Directory Schema -työkalulla. Skeemaan lisättyjä tietoja ei voi poistaa. (Microsoft 2000a, 241.) Muokkaajan on oltava Schema Admins -ryhmän jäsen. Metsää kohden on olemassa vain yksi Schema Admins -ryhmä. Ryhmä sijaitsee juuritoimialueessa. Juuritoimialueen pääkäyttäjillä on siten muita toimialueen pääkäyttäjiä suuremmat oikeudet määrätä, kuinka aktiivihakemisto suunnitellaan. (Lowe-Norris 2001, 159.)

Rakennemalli koostuu luokista (Class) ja attribuuteista (Attribute). Rakennemalli on johdettu X.500-hakemistopalvelusta. Luokat voivat periä ominaisuuksia toisiltaan ja sen takia kaikilla olioilla on yksilöllinen tunniste, OID. Kokonainen OID osoittaa olion sijainnin puussa sekä oman yksilöllisen tunnisteen numerosarjan lopussa. (Lowe-Norris 2001, 65-66.)

2.5.10 LDAP

Active Directory -järjestelmä tukee LDAP-rajapinnan natiivikutsuja ja se on johdettu X.500-standardin määritelmien mukaan. Aktiivihakemiston DN eli Distinguished Name -muodossa käytetään kolmea määritelmää (taulukko 2). (Lowe-Norris 2001, 30.)

TAULUKKO 2. Aktiivihakemiston nimityypit

Objektiluokka	Tyyppi	Lyhenne
Lehtiobjektiluokat	Common Name	CN
Organisaatioyksikkö	Organizational Unit	OU
Toimialue	Domain Component	DC

Kaikki hakemiston objektien nimet ovat yksikäsitteisiä. Esimerkiksi LDAP-polun nimessä:

LDAP://CN=user1,OU=Users,DC=yritys,DC=fi

DC kertoo toimialueen FQDN-nimen ja OU kertoo organisaatioyksikön, jossa CN-käyttäjäobjekti (user1) sijaitsee. (Lowe-Norris 2001, 30.)

2.5.11 Migraatio

Windows 2000 -toimialueeseen on mahdollista migratoida olemassa olevia ympäristöjä. Migratoinnilla tarkoitetaan käyttäjä-, ryhmä-, luottosuhde- ja tietokoneobjektien sekä niiden keskinäisten kytkentöjen kopiointia tai siirtoa jostain toisesta järjestelmästä aktiivihakemistoon. (Microsoft 2003.) Migratointityökaluja on saatavilla Windows NT -järjestelmille sekä Novell-järjestelmälle. Windows-toimialueiden migratointiin on Microsoftilla ilmainen Active Directory Migration Tool (ADMT). Ohjelmiston versio 1 ei kopioi käyttäjien salasanoja ja versio 2 kopioi myös salasanat (Microsoft 2003b, 6).

ADMT-työkalulla on mahdollista testata ennen todellista migratointia operaation

mahdolliset käyttäjätunnusten tai ryhmien päällekkäisyydet tai muut virheet. Testitapahtumasta tehdään logi, jota tulkitsemalla nähdään päällekkäiset käyttäjät sekä ryhmät ja muut virheet. (Microsoft 2003, 6.)

2.5.12 Windows 2003

Vuonna 2003 julkaistu Windows Server 2003 toi joukon parannuksia aikaisempaan palvelinversioon. Samalla myös aktiivihakemisto päivittyi uuteen versioon. Microsoft Windows Server 2003 Active Directory -tuotteen uusia toimialue- ja metsäkohtaisia ominaisuuksia ovat:

- Mahdollisuus nimetä toimialueen palvelin uudestaan ilman uudelleenasennusta tai aktiivihakemiston poistoa palvelimesta.
- Mahdollisuus nimetä toimialue uudestaan. Windows 2003 -aktiivihakemistossa voidaan nimetä vain DNS- tai Netbios-nimi tai kummatkin mistä tahansa metsän toimialueesta.
- Mahdollisuus ohjata uusien käyttäjä- ja tietokoneobjektien oletussijainti ryhmäkäytännöillä suojattuun organisaatioyksikköön suojaamattoman container-säiliön sijaan.
- Mahdollisuus tehdä kaksisuuntainen luottosuhde metsien välille.
- Mahdollisuus muuttaa toimialueen rakennetta eli toimialueita voidaan siirtää uuteen paikkaan toimialuehierarkiassa.
- Mahdollisuus passivoida aktiivihakemiston rakenteen eli skeeman luokkia ja objekteja sen sijaan, että ne jäisivät näkyviin aktiivihakemiston skeemaan.
- Mahdollisuus dynaamisten apuluokkien linkitykseen yksittäisille objekteille kokonaisten luokkien sijaan.
- Mahdollisuus hyötyä Global Catalogin eli yleisen luettelon uusien attribuuttien lisäämisen aiheuttamasta pienemmästä verkkokuormasta, koska replikoidaan vain lisätyt osat eikä koko luetteloa.
- Mahdollisuus hyötyä aktiivihakemiston parantuneista replikointitapahtumien suorituksista, koska mm. ryhmäjäsenyyden muutos replikoidaan vain muuttuneen henkilötiedon osalta eli ei replikoida koko ryhmää.

- Mahdollisuus kieltää toisen toimialueen tai metsän kaikkien käyttäjien pääsy tiettyyn toimialueeseen ja sitten sallia vain valittujen käyttäjä- ja ryhmäkohtaisten oikeuksien pääsy tiettyyn resurssiin.
- Mahdollisuus hyötyä aktiivihakemiston parannetusta oletustietoturvasta. (Microsoft 2005.)

Microsoft Windows Server 2003 Active Directory -tuotteen uusia palvelimen käyttöjärjestelmäkohtaisia ominaisuuksia ovat:

- Voidaan muokata usean objektin ominaisuuksia kerralla Active Directory Users and Computers -työkalulla.
- Voidaan siirtää Active Directory Users and Computers -työkalulla objekteja toiseen organisaatioyksikköön hiiren raahaustoimintoa käyttäen.
- Aktiivihakemiston hakutoimintoja on tehostettu nopeimpien hakujen mahdollistamiseksi.
- Tiettyjen hakuehtojen mukaan tehtyjä hakuja voidaan tallentaa myöhempää käyttöä varten.
- Tehokkailla komentojonotyökaluilla voidaan esimerkiksi luoda suuria käyttäjämäärien nopeasti.
- Skeemaan on lisätty InetOrgPerson-luokka.
- Aktiivihakemiston partitioinnilla saavutetaan hyötyjä jos tarvitaan vain tiettyjen ominaisuuksien replikointia tietyille palvelimille.
- Uuden toimialueen palvelimen asennusaikaa voidaan vähentää asentamalla aktiivihakemisto varmuuskopiosta.
- Universaalien ryhmien tiedot talletetaan toimialueen palvelimen välimuistiin, joten hitaan yhteyden yli ei tarvitse hakea tietoa mahdollisesti etäällä sijaitsevasta yleisen luettelon palvelimesta.
- Aktiivihakemiston ylläpitoon käytettävät hallintatyökalut allekirjoittavat ja kryptaavat oletuksena LDAP-yhteyden tehden LDAP-liikenteestä turvallisempaa.
- Ryhmäkäytännöillä voidaan määritellä tilarajoituksia (quota). (Microsoft 2005.)

Windows 2000 -aktiivihakemisto on mahdollista päivittää Windows 2003 -tasoiseksi. Päivityksessä on suositeltavaa, että Windows 2000 -toimialueiden palvelimille asennetaan korvaavaksi palvelimiksi Windows 2003 -palvelimet. Päivitys on myös mahdollista tehdä olemassa oleviin palvelimiin, mutta toimenpide on riskialttiimpi. Päivitys tapahtuu seuraavien toimenpiteiden mukaisesti uusilla palvelimilla:

- Tarkistetaan repadmin-komennolla replikoinnin oikeellisuus sekä toimivuus.
- Tarkistetaan gpotool-komennolla ntfrs- eli tiedostoreplikointi.
- Määritellään vain yksi toimialueen palvelimista yleisten luettelon palvelimeksi.
- Tarkistetaan netlogon- ja sysvol -kansioiden toiminta dcdiag /e /test:frssysvol -käskyllä.
- Tarkistetaan replikoinnin toiminta käskyllä repadmin /replsum /bysrc /bydest /sort:delta.
- Yleisen luettelon -palvelimessa käskyllä adprep /forestprep valmistellaan metsä Windows 2003 -skeeman mukaiseksi (versiosta 13 versioon 30).
- Toimialueen palvelin valmistellaan päivitykseen adprep /domainprep -käskyllä.
- Mahdolliset uudet palvelimet asennetaan tavallisiksi member-palvelimiksi toimialueeseen.
- Korotetaan uudet Windows Server 2003 -palvelimet toimialueiden palvelimiksi dcpromo-komennolla, jonka jälkeen siirretään kaikki FSMO-roolit uudelle palvelimelle, kun on tarkistettu, että aktiivihakemisto toimii halutusti.
- Asennetaan uuteen toimialueen palvelimeen DNS-palvelu (mieluiten vikasietoisemmassa AD-Intergrated -tilassa), jonka jälkeen tarkistetaan palvelimen ja aktiivihakemiston toiminta.
- Siirretään aikapalvelu uuteen PDC-emulator -roolin omaavaan palvelimeen, jonka jälkeen toistetaan sama kuvio niin monella palvelimella kuin on tarpeen.
- Lopuksi poistetaan tarpeiden mukaan vanhat toimialueen palvelimet käs-

kyllä dcpromo -> demote.

- Kun toimialueessa on pelkästään Windows 2003 -palvelimia, on tarkoituksenmukaisinta kohottaa toimialueen toiminnallisuus Windows 2003 -tasolle jolloin saavutetaan kaikki aktiivihakemiston mahdolliset toiminnallisuudet. (Microsoft 2004.)

Kaikissa päivityksen vaiheissa on syytä ottaa järjestelmän varmuuskopiot, eli System State varmistetaan aktiivihakemiston jokaisesta toimialueen palvelimesta. (Microsoft 2004.)

2.5.13 Toiminnallisuustaso

Aktiivihakemiston toimialueessa ja metsässä on useita toimintatasoja riippuen aktiivihakemiston käyttötarkoituksesta ja toimialueen palvelimien käyttöjärjestelmätasosta. Tasoa kuvataan ilmaisulla toiminnallisuustaso (functional level). (Glenn, Simpson 2004, 2-23.)

Toimialueessa on neljä mahdollista toiminnallisuustasoa:

- Windows 200 Mixed -tila, joka on oletustoiminnallisuustaso. Toimialueessa voi olla toimialueiden palvelimina Windows NT 4.0-, Windows 2000- ja Windows 2003 -palvelimia. Oletustaso tarjoaa aktiivihakemistossa kaikkein vähiten toiminnallisia ominaisuuksia.
- Windows 2000 Native on tila, jossa voi olla toimialueiden palvelimina Windows 2000- ja Windows 2003 -palvelimia.
- Windows Server 2003 Interim -tilassa voi olla toimialueiden palvelimina Windows NT 4.0- ja Windows 2003 -palvelimia. Tila on tarkoitettu käytettäväksi Windows NT 4.0 -toimialueen päivityksessä Windows 2003 -aktiivihakemistoksi.
- Windows Server 2003 -tilassa voi olla toimialueiden palvelimina ainoastaan Windows 2003 -palvelimia. Ainoastaan tässä toiminnallisuustasossa on kaikki aktiivihakemiston toiminnalliset ominaisuudet. (Glenn, Simpson 2004, 2-23.)

Metsässä on kolme mahdollista toiminnallisuustasoa:

- Windows 200 -tila on metsän oletustila ja jossa toimialueen palvelimien on mahdollista olla Windows NT 4.0-, Windows 2000- ja Windows 2003 -tasoisia.
- Windows Server 2003 Interim on tila, jossa voi olla toimialueiden palvelimina Windows NT 4.0- ja Windows 2003 -palvelimia. Tila on tarkoitettu käytettäväksi Windows NT 4.0 -metsän päivityksessä Windows 2003 -aktiivihakemistoksi.
- Windows Server 2003 on tila, jossa voi olla toimialueiden palvelimina ainoastaan Windows 2003 -palvelimia. Ainoastaan tässä toiminnallisuustasossa on kaikki aktiivihakemiston metsän toiminnalliset ominaisuudet. (Glenn, Simpson 2004, 2-23 - 2-24.)

Toiminnallisuustaso määritellään Active Directory Domain and Trusts -työkalulla valitsemalla toimialueen toiminnallisuusvalikosta kohta: Raise Domain Functional Level (Spealman, Hudson, Craft 2003).

2.5.14 Muut palvelut

Windows-työasemien ja palvelinten hallinnan ja onnistuneiden hakemistokirjautumisien edellytys on tietokoneen liittäminen toimialueeseen. Ylläpitäjällä on oltava Add workstations to domain -oikeus. Oletuksena liittämisen yhteydessä tietokoneen pääkäyttäjäryhmään (Administrators) lisätään toimialueen pääkäyttäjäryhmä (Domain Admins) sekä metsän pääkäyttäjäryhmä (Enterprise Admins). Liitetty tietokonetili lisätään automaattisesti Computers-järjestelmäsäiliöön, mikäli sille ei ole luotu etukäteen tiliä organisaatioyksikkörakenteeseen. (Microsoft 2001a.)

Verkon pääkäyttäjäryhmät on mahdollista ottaa pois tietokoneen pääkäyttäjäryhmästä. Tästä huolimatta tietokoneeseen kohdistetut ryhmäkäytännöt tulevat voimaan. Ryhmäkäytäntöjä työasemassa hallitsee Windows Installer -palvelu, joka toimii järjestelmän oikeuksilla. Sama palvelu hallitsee myös aktiivihakemiston

kautta jaeltujen MSI-pakettien automaattiasennuksia. (Microsoft 2001a.)

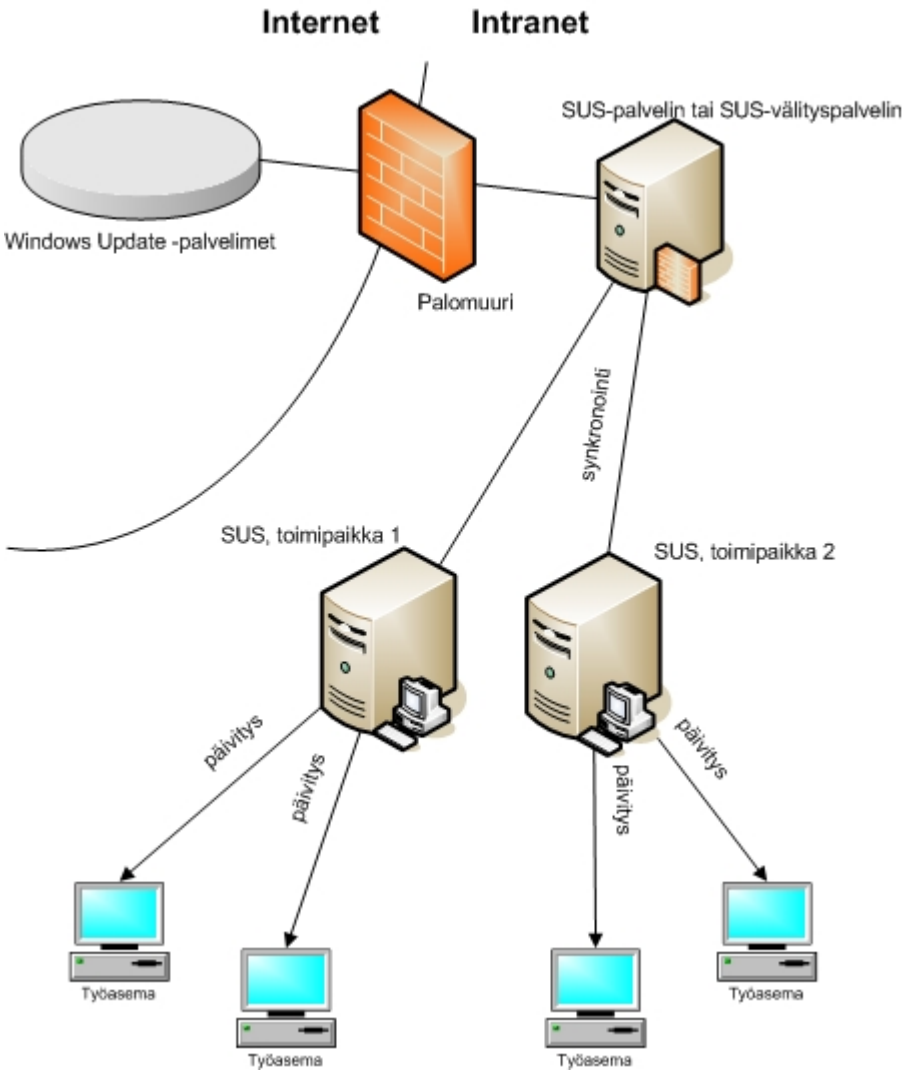
Tietokonetili nimetään liittämisen yhteydessä muotoon tietokonenimi.yritys.fi jos toimialueen nimi on yritys.fi. Tietokoneelle tulee automaattisesti yksikäsitteinen FQDN-nimi. Nimen on oltava yksikäsitteinen koko metsän alueella. (Lowe-Norris 2001, 166.)

Aktiivihakemiston hyödyntäminen on tehokkaampaa, mikäli hakemistopalvelun asiakkaina on Windows 2000- tai XP -käyttöjärjestelmillä varustettuja työasemia. Ainoastaan mainittuihin käyttöjärjestelmiin on mahdollista kohdistaa keskitettyjä asetuksia eli ryhmäkäytäntöjä. Myös verkon tietoturva on paremmalla tasolla kyseisillä käyttöjärjestelmillä. Windows 2000- ja XP -käyttöjärjestelmät käyttävät käyttäjän todentamiseen Kerberos-autentikointia, joka on tietoturvallisempi kuin vanhempien Windows-järjestelmien autentikointitekniikka, NTLM. (Lowe-Norris 2001, 428.)

Toimialueessa olevat tiedosto-, tulostus- ym. palvelimet kannattaa päivittää vähintään Windows 2000 -tasoisiksi. Päivityksellä saavutetaan parempi tietoturva turvallisemman todentamisella ja helpompi ylläpidettävyys sekä hallittavuus. (Microsoft 2001a.)

Distributed File System, DFS, on palvelu, jolla verkon tiedostoresurssit saadaan näkymään keskitetysti yhdeltä palvelimelta. DFS on puumainen, hajautettu tiedostorakenne. DFS esiteltiin jo Windows NT -käyttöjärjestelmän yhteydessä, mutta käytettäessä DFS-palvelua aktiivihakemistossa, on siinä tiettyjä etuja: DFS voidaan kytkeä kiinteästi aktiivihakemistoon (domain DFS root), joten palvelu on vikasietoisempi ja helpottaa DFS-juuren paikantamista. DFS-linkit kootaan yhdeksi linkkihakemistoksi, joka julkaistaan käyttäjille esimerkiksi ryhmäkäytännöillä. Käyttäjät näkevät kaikki julkaistut tiedostoresurssien linkit yhden verkkoaseman alihakemistoina. DFS-palvelu otetaan käyttöön Dfsutil.exe-työkalulla. (Microsoft 2000a, 233.)

Software Update Services, SUS Windows 2000- ja Windows 2003 -palvelimiin asennettava työasemien ja palvelinten tietoturvapäivityksiin erikoistunut Microsoftin maksuton palvelintuote, jolla pystytään päivittämään organisaation Windows-käyttöjärjestelmien tietoturvapäivitykset verkon yli ajastetusti (kuvio 4). SUS-palvelun ylläpito tapahtuu www-pohjaisesti HTTP- tai HTTPS -yhteydellä. (Microsoft 2003a, 4.)



KUVIO 4. Software Update Services -järjestelmän toiminta (Microsoft 2003a.)

Organisaatioon asennetaan SUS-palvelin, joka hakee määritellyin aikavälein halutunkieliset tietoturvakorjaukset Windows 2000-, Windows XP- ja Windows Server 2003 -käyttöjärjestelmiin. Organisaation palvelimeen asennetaan SUS- ja IIS-palvelut. Määrittelyjen jälkeen palvelin hakee halutuin aikavälein korjauspäivitykset organisaation verkosta mahdollisen palomuurin takaa Microsoftin Windows Update -palvelimilta. Palvelin jakaa tulleet uudet päivitykset ylläpitäjän hyväksynnän jälkeen määritellyihin työasemiin HTTP-liikennettä käyttäen. Palvelin voidaan myös määritellä hyväksymään kaikki uudet päivitykset automaattisesti, mutta se ei ole suotavaa, koska tällöin ei organisaation verkossa olevien työasemien päivitysten vaikutusta pystytä testaamaan ennen päivityksen asennusta. (Microsoft 2003a, 6.)

Organisaatioon voidaan asentaa useita SUS-palvelimia tasaamaan kuormaa tai hitaiden yhteyksien toimipaikkoihin. Organisaatioon voidaan myös asentaa pelkästään yksi SUS-välityspalvelin, joka hakee päivitykset Windows Update -palvelimilta ja jakaa päivitykset sitten organisaation SUS-palvelimiin. (Microsoft 2003a, 22.)

Helpoin tapa määritellä automaattiset päivitykset organisaation työasemiin on tehdä se toimialueen ryhmäkäytännöllä. (Microsoft 2003a, 44.) Myös ne työasemat, jotka eivät sijaitse toimialueessa, on mahdollista määritellä käyttämään SUS-palvelinta kirjaamalla palvelu joko suoraan rekisteriin tai tekemällä määrityksen työasemakohtaisella käytännöllä. (Microsoft 2003a, 52.)

3 KÄYTTÖÖNOTTO

3.1 Tavoitteet

Lahden ammattikorkeakoulun tavoite oli saada käyttöön toimiva hakemistopalvelu, jonka ylläpito on turvallista, edullista ja helppoa. Käyttöönoton alussa tavoitteeksi asetettiin laitosten käyttäjätietokannan yhtenäistäminen. Yhtenäinen käyttäjätietokanta poistaisi päällekkäisen käyttäjätunnusten luonti- ja ylläpitotyön.

Käyttöönoton edetessä tavoitteet tarkentuivat. Kun käyttöönotettavaa järjestelmää tunnettiin, ymmärrettiin paremmin hakemistopalveluun liittyvät mahdollisuudet ja siitä saatavat hyödyt. Lisätavoitteeksi otettiin käyttöönoton edetessä mahdollistaa alusta tuleville käyttäjän tunnistuspalveluille, kuten intranet ja yhteiset tiedosto- ja tulostuspalvelut, jotka korvaisivat laitosten omat tiedostopalvelimet.

Yhtenäinen käyttäjähallinta mahdollistaisi keskitetyn levyjärjestelmän hankinnan, joka vähentäisi laitoksissa tehtyä työtä palvelimen asennuksissa ja ylläpidossa. Hankinnalla saataisiin myös pitkällä tähtäimellä suuria kustannussäästöjä aikaiseksi. Käyttäjien liikkuvuuden lisäksi tavoiteltiin yhtenäistä ympäristöä, jossa käyttäjien olisi helppo toimia ja johon saataisiin keskitetyn järjestelmän tuomat yhtenäisen ohjeistuksen hyödyt.

Tavoitteena oli myös saada kaikkien suunniteltujen toimien ansiosta aikaan joka alueella kustannussäästöjä eli esimerkiksi ylläpidossa sekä laitehankinnoissa. Ylläpito helpottuisi, koska laitoksittain tapahtuva palvelinlaitteiden hallinta jäisi kokonaan pois. Yhtenäinen ympäristö toisi myös mukanaan ylläpidettävän järjestelmän, jossa olisi helppo delegoida ylläpitovastuuta esimerkiksi ylläpitohenkilöstön lomien ajaksi.

3.2 Valinta

Teknisiltä ominaisuuksiltaan tarkempaan tutkimukseen valitut hakemistopalvelut olivat tasavertaisia eikä niiden välillä havaittu ratkaisevia eroja. Kumpaankin tarkastelun alla olevaan järjestelmään oli saatavissa hyviä niiden toimintaa tukevia palveluja.

Halu tutustua uuteen hakemistopalvelutekniikkaan johti Microsoftin tuotteen testaukseen. Testeistä saatujen myönteisten kokemusten perusteella päätettiin aktiivihakemisto ottaa käyttöön tekniikan laitoksessa, jotta Microsoftin hakemistopalvelutuotteen käytöstä saataisiin kokemuksia laajemmassa ympäristössä. Toimivan ja helppokäyttöisen hakemistopalvelun kokemusten perusteella yhdessä laitoksessa, oli loppujen lopuksi luontevaa siirtyä koko Lahden ammattikorkeakoulun kattavaan hakemistopalveluun. Lahden ammattikorkeakoulun hakemistopalveluksi valittiin Microsoftin Active Directory.

Lahden ammattikorkeakoulun lisenssisopimus tuki valmiiksi käyttöönotossa tarvittavia palvelinympäristöjä eli Windows Server -tuotteita, joten käyttöönotosta ei koitunut ylimääräisiä lisenssikustannuksia. Valinnassa painottui lisäksi järjestelmään saatu maksuton tuki käyttöönottohetkellä.

3.3 Aikataulu

Käyttöönotto käynnistyi Microsoft Finlandin vuosina 2000-2001 tarjoamasta Windows 2000 Active Directory RDP -koulutuksesta. Microsoftin tarjoaman koulutuksen tarkoituksena oli helpottaa aktiivihakemiston käyttöönottoja Suomen ammattikorkeakouluissa. Houkuttimena koulutukseen lähtiessä oli Windows 2000 -palvelinlisenssien hankintaan annetut 50 %:n alennukset, mikäli käyttöönotto saataisiin suoritettua asetettuun määräaikaan mennessä. Houkuttimena oli myös kahdelle henkilölle annettu ilmainen, noin kymmenen päivää kestänyt koulutus Windows 2000 -palvelinjärjestelmästä, aktiivihakemistosta ja käyttöönotosta siirryttäessä Windows NT -järjestelmistä Windows 2000 -järjestelmään.

Lahden ammattikorkeakoulusta koulutukseen osallistui kaksi henkilöä. Koulutus järjestettiin pääosin pääkaupunkiseudulla vajaana kymmenenä päivänä syksyn 2000 ja kevään 2001 aikana. RDP-ohjelma kesti vuoden 2003 syksyyn asti. Lahden ammattikorkeakoulun edustajat olivat mukana koulutuksen loppuun. Koulutus antoi mahdollisuuden saada tarvittavaa tietoa ja taitoa käyttöönoton suunnittelemiseen ja toteutukseen.

Koulutukseen osallistuneille järjestettiin Internetin kautta pääsy Microsoftin tukipalveluun, josta annettiin ilmaiseksi kolme tukitapausta kaikkia Suomen ammattikorkeakouluja kohti mahdollisia käyttöönotossa tapahtuvia vaikeita, tukea vaativia tilanteita varten. Verkkopalvelussa oli myös keskustelufoorumi, jossa Suomen ammattikorkeakoulujen edustajat käyttöönotoissa pystyivät vaihtamaan kokemuksia ja kommunikoimaan käyttöönoton ongelmissa. Microsoft oli mukana käyttöönotossa tarkistaen ja kommentoiden koulutuksessa mukana olevien ammattikorkeakoulujen tekemiä käyttöönottosuunnitelmia käyttöönottojen seurannan palavereissa.

Microsoftin asettamaa aikataulua ei ollut mahdollista toteuttaa Lahden ammattikorkeakoulun laitosten pirstaleisen ja hallinnollisesti hajanaisen tietojärjestelmäympäristön tuoman hidasteen ja vaativuuden takia. Aikataulu ja käyttöönoton loppuun saamisen päivämäärä oli aluksi vaikeaa asettaa, koska tarvittavia käyttöönotto- ja ylläpitoresursseja ei ollut. Käyttöönotto olisi vaatinut alusta alkaen kokopäiväistä vastuutettua ylläpitohenkilöä.

Myöhemmin aikataulua tarkennettiin, kun järjestelmän käyttöönottoon ja ylläpitoon saatiin resurssit. Samaan aikaan tulleet opetusministeriön vaatimukset käyttäjähallintojen saamiseksi kuntoon Suomen ammattikorkeakouluissa vauhdittivat myös sekä resurssien osoittamista että aikataulun tiukentamisesta ja tarkentamista. Tavoitteeksi Lahden ammattikorkeakoulun kaikkien laitosten saamiseksi yhtenäisen hakemistopalvelun käyttäjiksi asetettiin viimeistään vuoden 2004 kevät.

3.4 Suunnittelu

Hakemistopalvelun käyttöönottoa koskevassa aloituspalaverissa 13.11.2000 käsiteltiin hakemistopalvelun tuomia hyötyjä, sen käyttöönoton myötä tuomia kustannuksia ja käyttöönoton aikataulua. Microsoftin aktiivihakemiston käyttöä puolsi ilmainen käyttöönottokoulutus. Lisäksi pääosa Lahden ammattikorkeakoulun laitoksista käytti jo ennestään Windows-toimialueita. Järjestelmien vaihto toisen valmistajan tuotteisiin ei katsottu pienillä resursseilla järkeväksi. Kokonaan toisen valmistajan järjestelmän käyttöönotto olisi vaatinut koko ylläpitohenkilöstön uudelleenkoulutuksen Lahden ammattikorkeakoulussa.

Aloituspalaverissa valittiin kunkin järjestelmää koskevan osion prosessoimiseen vastuuhenkilö tai asiantuntija sekä määriteltiin pilottiprosessi ja siihen tarvittavat resurssit. Palaverissa päätettiin aloittaa alustavan käyttöönottosuunnitelman mukainen kartoitus ammattikorkeakoulun työasemamäärän, käytössä olleiden järjestelmien, osaamisen ja verkkotopologian osalta. Hakemistopalvelun käyttöönottosuunnitelmaa koostettiin ennalta kerättyjen tietojen pohjalta. Palaverissa kuullun aktiivihakemiston esittelyn perusteella todettiin hyötyjen olevan kustannusten arvoisia. Aloituspalaverissa päätettiin myös aloittaa järjestelmän testaus.

Aktiivihakemiston käyttöönotossa lähdettiin liikkeelle ja noudatettiin seuraavaa prosessia: järjestelmän käyttöönotosta tehtiin Microsoftin kanssa yhteistyössä käyttöönottosuunnitelma, hankittiin tarvittava käyttöönoton ja ylläpidon vaatima koulutus, tehtiin määritellyt testit, asennettiin pilottiympäristö ja otettiin varsinainen tuotantoympäristö käyttöön.

3.5 Testi- ja pilottiympäristö

Ennen varsinaisen palvelinlaitteiston hankintaa ja asennusta palvelinohjelmiston asennus ja tarvittavien toimintojen testaus tehtiin kevyemmällä, saatavilla olleella testilaitteistolla. Testaukseen käytettiin kolmea Pentium-tasoista työasemaa. Testilaitteet olivat yhden aktiivilaitteen takana, jolloin oli mahdollista testata palvelimia eri vlaneissa (virtuaalinen verkko) laitteita siirtämättä. Testilaitteiden alkeel-

linen vikasietoisuus varmistettiin ohjelmistopohjaisella RAID1-tason levypeilauksella.

Testejä tehtiin useaan kertaan eri kokoonpanoilla. Testeissä oli mukana kahdesta viiteen henkilöä, eikä ongelmia tässä vaiheessa havaittu. Palvelinlaitteiston, vikojen, toimenpiteiden ja kuormitusten dokumentoinnin suoritti vastuutettu pääkäyttäjä. Määritellyn OU-rakenteen suunnittelu (Organizational Unit) ja siinä tehdyt muutokset dokumentoitiin. Työasemien, esimerkiksi yhden mikroluokan, oikeudet ja määritykset suunniteltiin tehtäväksi ryhmäkäytännöillä.

Koska palvelimilla luotiin kokonaan uusi Windows 2000 -toimialue ja -metsä, toimialue asetettiin natiivitilaan. Kaikki FSMO-roolit määriteltiin olemaan yhdessä toimialueen palvelimessa sillä poikkeuksella, että Infrastructure Master -rooli asetettiin eri toimialueen palvelimeen kuin Global Catalog -server.

Havaittiin myös, että RID-master -roolillisesta palvelimen System State -varmuuskopiosta ei kannata palauttaa mitään RID-arvoja. Jos RID-master -roolillisesta toimialueen palvelimen varmuuskopioista palauttaa aikaisemman tilanteen, menevät jo ennestään jaetut relative ID:t jossain vaiheessa päällekkäin, mikä voi aiheuttaa ylitsepääsemättömiä ongelmia hakemistopalvelun toiminnassa.

3.6 Käyttöönoton toteutus

Aktiivihakemiston käyttöönotto käynnistyi laitteiston hankinnalla ja asentamisella. Olemassa olevien Windows NT -järjestelmien palvelinlaitteistojen käyttö ei ollut mielekästä tulevan järjestelmän tehovaatimusten ja uuden juuritoimialueen asennuksen antaman joustavuuden takia. Käyttöönotto oli kuvatulla tavalla helpompi ja käytännössä ainoa vaihtoehto rakentaa koko organisaation kattava verkkokäyttöjärjestelmä ja hakemistopalvelu. Microsoftin aktiivihakemiston mitoitusohjelmalla (Active Directory Sizer) saatujen arvojen mukaan päätettiin hankkia kaksi kriittisen toimintatason toimialuepalvelinta.

Laitteet sijoitettiin yhteen Päijät-Hämeen koulutuskonsernin konesaleista. Kone-

salissa on kahdennettu, automaattinen ilmastointi, sähkönsyöttö on varmistettu varavirtalaitteilla ja tietoturva on varmistettu sekä kulunvalvonnalla että kameravalvonnalla. Konesalin tietoliikenneyhteydet on kahdennettu, ja ne ovat runkoyhteyksien tasoa eli riittävän nopeat. Hankittavaan laitteistokokonaisuuteen asennettiin Windows 2000 Active Directory -testiympäristön ja pilottimäärityksien pohjalta.

Tuotantoympäristön palvelimien aktiivihakemiston tietokannan suorituskyky ja vikatilanteesta palautuminen optimoitiin asentamalla käyttöjärjestelmä ja tietokanta erilliselle datalevylle. Tietokanta asennettiin erilliselle RAID5-tasoiselle levylle, koska Windows 2000 -palvelin otti kyseisen levyn rautapohjaisen välimuistin pois käytöstä, mikä olisi mahdollisesti hidastanut hieman käyttöjärjestelmän toimintaa. Myös komentojonotiedostojen ja tiettyjen ryhmäkäytäntöjen jakelun hoitava Sysvol-järjestelmäkansio määriteltiin samalle datalevylle, jossa tietokanta sijaitsee.

Aktiivihakemiston organisaatioyksikkörakenne tehtiin ylläpito-organisaation rakenteen mukaan eli pääosin toimipisteittäin. Kussakin toimipisteessä oli atk-käytönsuunnittelija, joka sai hallittavakseen toimipisteensä organisaatioyksikön. Tarvittaessa pääylläpitäjän oli helppo lisätä toiselle ylläpitäjälle oikeuksia haluamalleen toimipisteelle esimerkiksi lomien sijaisuuden ajaksi. Tähän rakenteeseen päädyttiin, koska tässä vaiheessa ei vielä ollut keskitettyä ylläpito-organisaatiota.

Uuteen hakemistopalveluun migratoitiin olemassa olevat, kahden laitoksen NT 4.0 -toimialueiden käyttäjät ja käyttäjäryhmät. Uuden hakemistopalvelun rakentamisen jälkeen aloitettiin varsinainen käyttöönotto tekniikan laitoksesta, jonka Windows NT 4.0 -toimialueen käyttäjät sekä ryhmät kopioitiin Windows 2000 Active Directory -hakemistopalveluun käyttäen Microsoftin ADMT-ohjelmistoa.

Ohjelmistosta oli ensimmäistä laitosta migratoitaessa saatavilla vasta versio 1, jolla ei saanut kopioitua käyttäjien salasanoja. Kaikki salasanat tehtiin uusiksi skriptin avulla ja jaettiin laitoksen opintotoimiston kautta tutoropettajille, jotka luovuttivat salasanat edelleen käyttäjille.

Salasanoja ei olisi muutenkaan ollut mielekästä kopioida, koska salasanavaatimukset olivat hakemistopalvelussa tiukemmat. Uusien salasanojen jakelun myötä saatiin myös levitettyä käyttäjille asennekasvatusta salasanan kompleksisuudesta sekä sen henkilökohtaisuudesta. Samassa yhteydessä saatiin myös poistettua vanhentuneita tunnuksia.

Myöhemmin migratoitiin myös kahden suuren laitoksen käyttäjät ja käyttäjäryhmät noin vuoden palvelleeseen hakemistopalveluun. Migratoinnissa käytettiin versiota 2, jolla kopioitiin myös salasanat. Käyttöönoton suurin työ, suurimman osan laitosten liittäminen aktiivihakemistoon tapahtui aina saman prosessin mukaan sinä ajankohtana, kun käyttöönotettavan laitoksen ylläpitäjän ja koulutusjohtajan kanssa saatiin sovittua aikataulu:

Ylläpitäjä perehdytettiin järjestelmän käyttöön ja vastuutettiin omaan työtehtäväänsä allekirjoituttamalla ylläpitositoumus. Käyttäjätunnukset luotiin aiemmista järjestelmistä tehtyjen listojen perusteella skriptien avulla. Tiedotettiin käyttäjiä ennen käyttöönottoa ja käyttöönoton aikana tapahtuvista muutoksista. Ohjeistettiin käyttäjiä sekä jaettiin käyttäjätunnukset ensin opintotoimistoon. Toimistovirkailijat luovuttivat tunnukset opettajille, jotka edelleen luovuttivat tunnuksen opiskelijalle allekirjoitettua käyttäjätunnussitoumusta vastaan. Muutettiin DNS-määritykset työasemien IP-asetuksista ja liitettiin työasemat toimialueeseen. Lopuksi siirrettiin levy- ja tulostuspalvelut palvelintiimin ylläpitämiin palvelimiin.

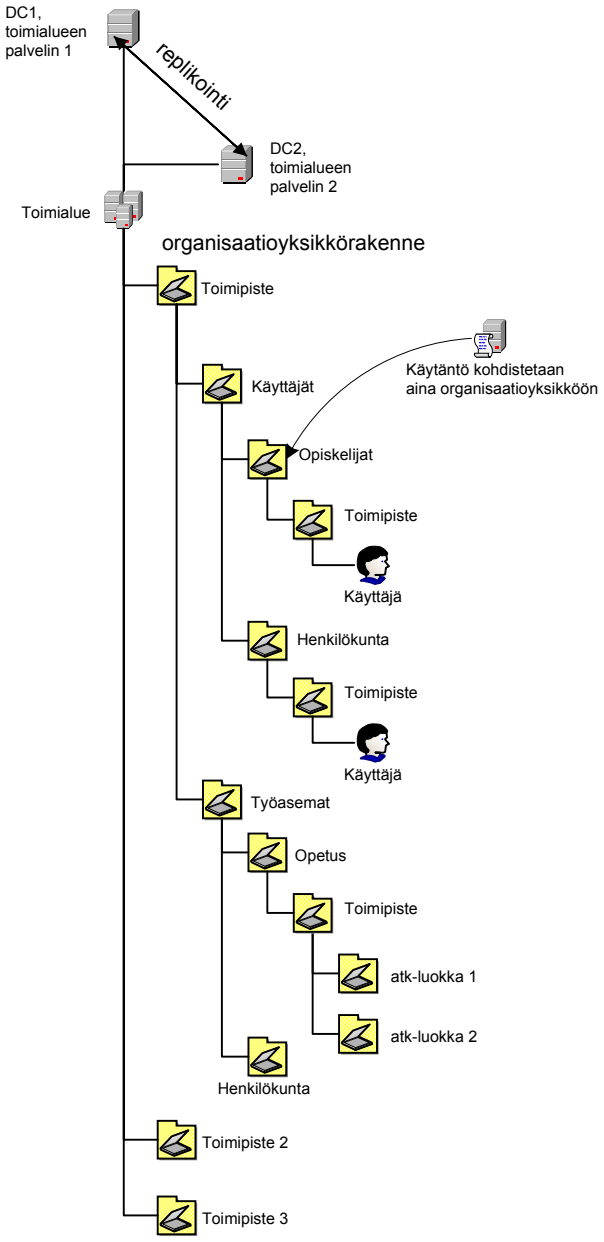
Suurin työ laitosten ylläpitäjille oli kaikkien laitoksen työasemien liittäminen toimialueeseen, joskaan siihen ei mennyt aikaa isommassakaan laitoksessa yhtä työpäivää kauemmin.

Pääkäyttäjätasoiset hallintaoikeudet vastuutettiin kahdelle järjestelmän ylläpitoon perehtyneelle henkilölle. Organisaatioyksikkörakenteen ylläpitäjät allekirjoittivat käyttösitoumuksen, jossa oli järjestelmän käytön ohjeet sekä tietoturvamääritykset. Pääkäyttäjät perehdyttivät lyhyesti kaikki organisaatioyksikkörakenteen ylläpitäjät tehtäviinsä.

Jokaisen käyttäjätunnuksen käyttäjäksi määriteltiin todellinen henkilö ja laitoksissa ennen käytössä olleet työasemakohtaiset toimialuetunnukset poistettiin käytöstä. Aktiivihakemiston tietoturva määriteltiin Päijät-Hämeen koulutuskonsernin johtoryhmän hyväksymän ja määräämän tietoturvapolitiikan pohjalta.

Lahden ammattikorkeakoulun ylläpidolliset ja hallinnolliset tarpeet täyttyivät yhden toimialueen käyttöönotolla. Yhdessä toimialueessa organisaatioyksiköt edustavat toimipisteitä. Organisaatioyksikön tarkoitus on toimia hallinnollisena alueena ja kullakin alueella on mahdollista tehdä käyttäjä- ja laitemäärityksiä ryhmäkäytännöillä.

Suunniteltu organisaatioyksikkörakenne (kuvio 5) mahdollisti joustavan ylläpidon. Rakennetta on helppo muokata organisaation tarpeiden mukaan. Organisaation hallinnollisen rakenteen muuttuessa hajautetusta yksikkörakenteesta keskitettyyn rakenteeseen on rakenne helppo muuttaa esimerkiksi muuttamalla toimipisteiden organisaatioyksiköt yhden käyttäjä- ja yhden työasemaorganisaatioyksikön alle.



KUVIO 5. Toimipisteisiin delegoidulla ylläpitovastuulla toteutettu organisaatioyksikkörakenne aktiivihakemistossa

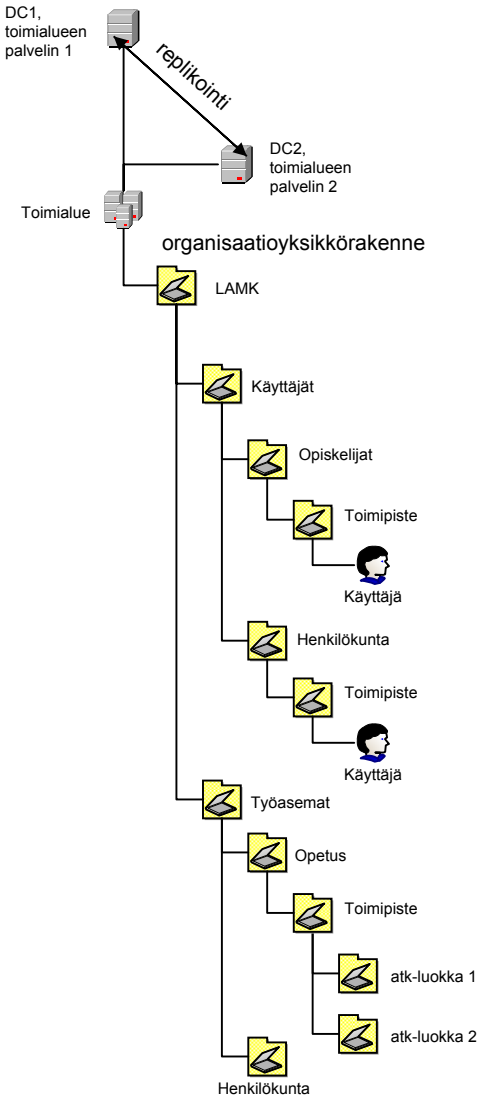
Syksyllä 2003 aktiivihakemiston ja Windows-käyttöjärjestelmäympäristön toimintaa suojattiin ottamalla käyttöön automaattisten tietoturvakorjausten päivityspalvelin, SUS. Palvelua varten tehtiin käyttöönottosuunnitelma, jonka perusteella hankittiin dedikoitu palvelinlaite, ja onnistuneiden testien jälkeen otettiin käyttöön kaikissa aktiivihakemistossa sijaitsevissa työasemissa. Aktiivihakemiston ryhmäkäytännöillä määriteltiin, että työasemat hakevat organisaation SUS-palvelimelta uudet tietoturvakorjaukset kerran päivässä.

Vuoden 2004 keväällä toimipaikkakäyttöönottojen toteuduttua katsottiin tarpeelliseksi päivittää aktiivihakemisto versioon Windows Server 2003 Active Directory sen uusista ominaisuuksista saatavien hyötyjen vuoksi sekä tietoturvallisemman toimintaympäristön varmistamiseksi. Windows 2003 -aktiivihakemistossa on oletuksena parempi tietoturvataso kuin Windows 2000 -aktiivihakemistossa.

Päivitystä varten käytiin lyhyt seminaarikoulutus, jonka perusteella tehtiin kirjallinen käyttöönottosuunnitelma. Suunnitelmassa kuvattiin päivityksen vaiheet ja aikataulutettiin muutosten ajankohdat. Laboratoriossa tehtyjen testien jälkeen päivitys tehtiin neljän tunnin aikana heti kun Lahden ammattikorkeakoulun opetus siirtyi kesätauolle kesäkuun alussa. Samassa yhteydessä uusittiin kolme vuotta käytössä olleet kaksi toimialueen palvelinta. Päivityksen lopuksi metsä asetettiin Windows Server 2003 -toiminnallisuustasolle.

Vuoden 2004 keväällä organisaatioyksikkörakennetta muutettiin palvelemaan paremmin Päijät-Hämeen koulutuskonsernin tietohallintopalveluiden muuttunutta organisaatiota (kuvio 6). Liikelaitoskohtaisesta rakenteesta siirryttiin keskitettyyn rakenteeseen. Rakenne oli tarpeen muuttaa, koska hakemistopalvelun ylläpitäjät eivät enää olleet vastuussa vain yhdestä toimipisteestä, vaan muuttuneen organisaatiorakenteen mukaisesti osaltaan kaikkien toimipisteiden työasemista.

Uusi organisaatioyksikkörakenne palveli myös käyttäjätunnusautomatiikkaa, joka saatiin käyttöönotettua ennen syksyn 2004 opetuksen alkua. Keväällä 2004 aloitettiin prosessi, jonka tarkoituksena oli saada Lahden ammattikorkeakoulun opiskelijoiden käyttäjätunnusten luonti ja muokkaus automaattiseksi. Hakemistoon tehtiin Funetin- ja Winha-määritysten mukaiset skeemalaajennukset. Automatiikka käsittelee tunnuksia opiskelijanumeron perusteella kerran päivässä.



KUVIO 6. Keskitetyn organisaation mukainen organisaatioyksikkörakenne Lahden ammattikorkeakoulun aktiivihakemistossa

4 YHTEENVETO

4.1 Työn onnistuminen

Aktiivihakemiston käyttöönotto Lahden ammattikorkeakoulussa sekä tulevaisuudessa koulutuskeskus Salpauksessa oli ja on pitkä, koko hakemistopalvelun elinkaaren kestävä prosessi. Varsinaista loppua sille on mahdotonta määritellä. Rakennetta, käyttäjätoiminnallisuutta sekä hakemistoa on muokattu koko elinkaaren ajan. Tästä syystä on myös vaikea määritellä opinnäytetyön päättymisen raja. Eräänä etappina voidaan pitää Lahden ammattikorkeakoulun laitoksissa olevien työasemien liittäminen toimialueeseen. Mutta kyseisen prosessi on vain osa käyttöönottoa ja kaikkien vaikutusalueiden käyttöönotto jatkuu vielä pitkälle tulevaisuuteen.

Työasemakäyttöönoton aikana ei teknisten prosessien toteuttaminen ollut ongelma. Käyttöönotto onnistui pääosin odotetusti, vaikka käyttöönottoon kuluikin arvioitua enemmän aikaa. Järjestelmän käyttöönoton tekninen toteutus oli käyttöönoton prosessissa nopein ja helpoin osuus. Suurin osa Lahden ammattikorkeakoulun laitoksista saatiin järjestelmän piiriin aikataulun puitteissa noin vuoden aikana. Tekninen osuus käyttöönotossa olisi voinut olla paljon nopeampikin, mikäli ei olisi tarvinnut huomioida samanaikaisesti hallinnollisia prosesseja ja niihin tehtävin muutoksia.

Suuri ongelma käyttöönoton alkuvaiheilla oli resurssien puute. Koska käyttöönottoa lähestyttiin aluksi tutkivasti, ei käyttöönotolla ollut kiire. Kun hakemistopalvelun ominaisuuksiin tutustuttiin paremmin ja luottamus sitä kohtaan kasvoi, osoitettiin käyttöönottoon myös enemmän resursseja, joka puolestaan nopeutti prosessia.

Suurimpana haasteena oli loppujen lopuksi useimpien laitoksien tietoteknisten toimintatapojen ja tietoturvakäytäntöjen täydellinen muutos sekä muutos koko IT-

ylläpitorakenteessa. Käyttöönoton kuluessa jouduttiin useaan otteeseen muuttamaan myös Lahden ammattikorkeakoulun IT-henkilöstöorganisaation toimintatapoja. Ylläpitoprosessien muuttuminen ja ohjeistuksen toteuttaminen hajautetuista yksiköistä keskitettyyn malliin veivät aikaa varsinkin hallinnollisten muutosten takia.

Pitkään kestäneeseen käyttöönottoaikaan vaikutti myös se, ettei nopealle käyttöönotolle ollut pakottavaa tarvetta. Käyttöönoton joka vaiheessa oli tavoitteena, että sekä käyttäjät että henkilöstö ehtivät sopeutumaan muutoksiin.

4.2 Jatkotoimet ja tulevaisuus

Hakemistopalvelun tuoma ylläpito-organisaation muutos sysäsi koko Lahden ammattikorkeakoulun IT-toiminnot rakenteelliseen toimintatapojen muutosprosessiin. IT-organisaation toimintojen keskittäminen alkoi vuoden 2003 syksyllä. Ylläpidon tehtävien delegoiminen aktiivihakemiston rakennemallien osiin on joustavaa keskittämisen eri vaiheissa, koska organisaatioyksikkörakennetta voi helposti muokata tarpeiden mukaan.

Koska keskittäminen koskee myös koko Päijät-Hämeen koulutuskonsernia, myös koulutuskeskus Salpauksessa ja Tuoterenkaassa otetaan käyttöön Lahden ammattikorkeakoulussa käytetty hakemistopalvelu. Käyttäjä- ja työasemaobjektit hakemistossa lähes kolminkertaistuvat vuoden 2006 loppuun mennessä.

Kesällä 2005 otetaan käyttöön myös SMS-palvelu, joka mahdollistaa kattavan Windows-työasemien ja -palvelimien etähallinnan koko Päijät-Hämeen koulutuskonsernissa. Asennettaessa SMS palvelimelle se laajentaa myös aktiivihakemiston skeemaa.

Lahden ammattikorkeakoulun tarpeita palvelemaan tehty käyttäjätunnusautomatiikka on tehty myös käsittelemään koulutuskeskus Salpauksen käyttäjätunnuksia. Automatiikka tullaan ottamaan käyttöön keväällä 2006, jolloin lähes kaikki Päijät-Hämeen koulutuskonsernissa opiskelevat käyttäjien tunnukset tehdään, käsitellään

ja poistetaan automaattisesti.

Käyttäjähallinnon keskittäminen suo tulevaisuudessa mahdollisuuden liittyä sujuvasti korkeakoulujen keskinäisiin hakemistoprosesseihin. Tekniikka antaa mahdollisuuden kirjautua Suomen korkeakoulujen verkkopalveluihin omalla käyttäjätunnuksella. Myös opiskelijoiden käyttöön tarkoitettujen Wille- ja Reppu-järjestelmien kirjautuminen on toteutettu aktiivihakemistoautentikoinnilla.

Lahden ammattikorkeakoulun käyttäjätietojen saaminen yhtenäiseen hakemistopalveluun mahdollistaa myös kytkennän Päijät-Hämeen koulutuskonsernin laajuiseen yhtenäiseen käyttäjätietosynkronointiin. Tietolähteiden yhdistäjäksi ja tekniikan toteuttajaksi on suunniteltu metahakemistoa. Tulevaisuudessa metahakemistolla saavutetaan haluttujen käyttäjätietojen synkronointi kaikkiin mahdollisiin järjestelmiin Päijät-Hämeen koulutuskonsernissa lähes reaaliajassa.

5 LÄHTEET

J. Spealman, K. Hudson, M. Craft. 2003. MCSE Self Paced Training Kit (Exam 70-294). Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure. Microsoft Press.

Lowe-Norris, A. 2001. Windows 2000 Active Directory. Tehokäyttäjän opas. Talentum Media Oy. Gummerus Kirjapaino Oy, Jyväskylä.

Microsoft. 2000a. MCSE Training Kit. Microsoft Windows 2000 Server. Windows Microsoft Press.

Microsoft. 2000b. MCSE Training Kit. Microsoft Windows 2000 Active Directory Services. Windows Microsoft Press.

Microsoft. 2001a. Rapid Deployment -koulutus. Helsingissä Microsoftin koulutustiloissa talvella 2000-2001.

Microsoft. 2001b. Windows 2000 Active Directory Sizer Tool. Päivitetty 19.6.2001. Saatavissa: http://www.microsoft.com/technet/prodtechnol/windows2000serv/downloads/w2kadst.mspx

Microsoft. 2003a. Deploying Microsoft Software Update Services. Windows Microsoft Press.

Microsoft. 2003b. Active Directory Migration Tool (ADMT) [verkkodokumentti] Saatavissa: http://www.microsoft.com/windows2000/downloads/tools/admt/default.asp

Microsoft. 2004. How to upgrade Windows 2000 domain controllers to Windows Server 2003 [verkkodokumentti]. Saatavissa: http://support.microsoft.com/?kbid=325379

Microsoft. 2005. New Active Directory features in Windows Server 2003 [verkkodokumentti] Saatavissa: http://technet2.microsoft.com/WindowsServer/en/Library/bb99fdd4-f8e0-490f-adae-6814cf081ff71033.mspx

Novell. 1996. Novell NetWare 4 Administration Student Manual, Course 520. Novell Inc.

Novell. 2003. Novell eDirectory 8.7.1 Administration Guide [PDF-dokumentti]. Saatavissa: http://www.novell.com/documentation/

Novell. 2005a. Novell Client for Windows 4.91, Installation and Administration Guide. [PDF-dokumentti]. Saatavissa: http://www.novell.com/documentation/

Novell. 2005b. Novell ConsoleOne 1.3.x User Guide [PDF-dokumentti]. Saatavissa: http://www.novell.com/documentation/

Novell. 2005c. Novell iManager 2.6 Administration Guide [PDF-dokumentti]. Saatavissa: http://www.novell.com/documentation/

Novell. 2005d. Novell ZENworks Suite, Getting started guide [PDF-dokumentti]. Saatavissa: http://www.novell.com/documentation/

Novell. 2006. Novell ZENworks 7 Desktop Management Administration Guide [PDF-dokumentti]. Saatavissa: http://www.novell.com/documentation/

Wahl, M. Howes, T. Kille, S. 1997. Network Working Group. Request for Comments: 2251. Lightweight Directory Access Protocol (v3) [tekstidokumentti]. Saatavissa: http://www.ietf.org/rfc/rfc2251.txt

W. Glenn, M. Simpson. 2004. MCSE Self-Paced Training Kit (Exam 70-297): Designing a Microsoft Server 2003 Active Directory and Network Infrastructure. Microsoft Press.