Metropolia Ammattikorkeakoulu
Tietotekniikan koulutusohjelma

Juha Karvali

Verkkoinfrastruktuurin kehittäminen Active Directory -migraation avulla

Insinöörityö 18.4.2010

Ohjaava opettaja: yliopettaja Markku Nuutinen

Metropolia Ammattikorkeakoulu Insinöörityön tiivistelmä

Tekijä Otsikko Sivumäärä Aika	Juha Karvali Verkkoinfrastruktuurin kehittäminen Active Directory -migraation avulla 76 sivua 18.4.2010
Koulutusohjelma	tietotekniikka
Tutkinto	insinööri (AMK)
Ohjaava opettaja	yliopettaja Markku Nuutinen

Tässä opinnäytetyössä käsitellään ”Yritys Oy:n” siirtymistä vanhoista Windows NT 4.0 -toimialueista Windows 2003 -palvelinarkkitehtuuriin ja Active Directoryn käyttöönottoon. Työssä esiteltiin Windows Server 2003 -palvelimien uusia parannettuja ominaisuuksia, kuten tietoturvaa ja hallinnointia, IT:n ja liiketoiminnan hyötyjä ajatellen

Vanhat toimialueet olivat rakentuneet vuosien aikana tehdyistä lukuisista yritysostoista. Jokainen toimialueista oli ympäristönä aivan erilainen ja haasteellinen. Keskitetyksi Active Directoryksi päivitettäviä alueellisia toimialueita olivat Aasia, Pohjois-Amerikka ja Eurooppa.

Yrityksen verkkoinfrastruktuurin kehittäminen sisälsi pitkäkestoisen suunnittelu- ja testausvaiheen, jonka jälkeen projekti toteutettiin kahdessa vaiheessa. Ensimmäisessä vaiheessa luotiin toimialuemetsän juuritoimialue ja olemassa olevat NT4-toimialueet päivitettiin Active Directory -toimialueiksi. Toisessa vaiheessa alueelliset toimialueet konsolidoitiin juuritoimialueeseen ja keskitetty hallinnointimalli otettiin käyttöön.

Tämän opinnäytetyön osalta pääpaino oli migraation jälkeisessä konsolidoinnissa, jossa tavoitteena oli optimoida ja keskittää resursseja sekä luoda keskitetty hallinnointimalli. Johtuen haasteellisista ja erilaisista toimialue ympäristöistä projektissa ei käytetty Microsoftin siihen tarkoitukseen luomia työkaluja. Ne korvattiin projektiryhmän jäsenen kirjoittamilla komentosarjoilla eli skripteillä. Joitakin asioita jouduttiin kuitenkin tekemään manuaalisesti. Projekti saatiin vietyä päätökseen sovitussa ajassa ja verkkoinfrastruktuuri saatiin nostettua suunnitellulle tasolle.

Hakusanat	Active Directory, käyttöönotto, konsolidointi

Helsinki Metropolia University of Applied Sciences **Abstract**

Author Title Number of Pages Date	Juha Karvali Network infrastructure development with Active Directory migration 76 pages 18.4.2010
Degree Programme	information technology
Degree	Bachelor of Engineering
Supervisor	Markku Nuutinen, Principal Lecturer

The thesis handled the transformation from Windows NT 4.0 domains to Windows 2003 Server architecture and deployment of Active Directory of ”Company Inc”. Thesis introduced and demonstrated the improved features of the Windows Server 2003 such as data security and management. These were presented keeping the benifits to IT and business in mind.

Old domains were build during the years through several business acquisitions. Everyone of its domains were unique and challenging as an environment. Asia, North America and Europe were to be updated from regional domain to centralized Active Directory.

The development of the enterprises network infrastructure contained a lenghty planning and testing stage after which the project was implemented in two stages. In the first stage the forest’s root domain was created and existing NT4 domain were updated as Active Directory domains. In the second stage regional domain were consolidated to the forest’s root domain and centralized management model was deployed.

The main primary goal for the thesis was in the consolidation after the migration in which the objective was to optimize and centralize the resources and creation of a centralized management model. Due to the challenging and unique domain environments the project did not use tools from Microsoft for these sort of purposes. The tools were substitute by script made by one of the project team member. Some of the things had to done manually. The project was completed within the agreed time and advanced network infrastructure was increased to achieve the desired level.

Keywords	Active Directory, deployment, Consolidation

Sisällys

Lyhenteet

AD	Active Directory, aktiivihakemisto.
ACE	Access Control Entries, Windows NT:n käyttöoikeusluettelon (access control list) tietue.
ACL	Access Control List, käyttöoikeusluettelo. Windows NT:ssä suojauskuvauksen osa, joka määrää, miten objekti on suojattu ja miten objektin käyttöä valvotaan.
ADSI	Active Directory Service Interface, Microsoftin ohjelmointi rajapinta hakemistojen mukkaukseen tarkoitetuille sovelluksille.
BDC	Backup Domain Controller,NT -toimialueen varaohjauskone.
DC	Domain Controller, toimialueen ohjauskone.
DFS	Distributed File Systems, hajautettu tiedostojärjestelmä.
DHCP	Dynamic Host Configuration Protocol, Protokolla, jonka avulla koneet saavat palvelimelta verkkoasetukset.
DNS	Domain Name Service, verkkojen käyttämä nimipalvelin.
DSA	Directory Service Agent, hakemistopalvelija joka hoitaa etenevät hakemistokyselyt DSA-yksiköltä toiselle kunnes haettu tieto löytyy.
FGDN	Fully Qualified Domain Name, Tietoverkoissa IP-verkkoosoitteen asemasta käytetty looginen nimi.
GC	Global Catalog, sisältää AD:n kaikkien objektien tiedot.
GPO	Group Policy Object, AD:n objekteja, jotka sisältävät ryhmäasetuksia.
GUID	Globally Unique Indentifier, kaikkialla yksikäsitteinen tunniste.
NTP	Network Time Protocol, protokolla täsmällisen aikatiedon välittämisen tietokoneiden välillä.
OU	Organisation Unit, organisaatioyksikkö.
PDC	Primary Domain Controller, NT-toimialueen pääohjauskone
RDN	Relative Distinquished Name, LDAP-hakemistopalvelun käyttämä nimeämismenetelmä, jolla yksilöidään objekti tietyn säilön sisällä.
RID	Relative Identifier, Suhteellinen tunnistenumero, jolla tehdään Windows toimialueen SID-tunnisteesta yksilöllinen.
SID	Security Identifier, Windows -toimialueen objektin suojaustunnus.
UPN	User Principal Name, Käyttäjän kirjautumisnimi AD-toimialueella.
WAN	Wide Area Network, Laaja tietoliikenneverkko, jolle on tyypillistä maantieteellinen ulottuvuus paikkakunnalta toiselle tai maan rajojen ulkopuolelle aina maanosien väliseksi verkoksi.
WINS	Windows Internet Name Service, TCP/IP-verkkojen DNS-palveluja vastaava nimipalvelu. Palvelu muuntaa Windowsverkon tietokoneiden nimet IP- osoitteiksi reititetyssä ympäristössä.
WMI	Windows Management Instrumentation, Windows-pohjaisten koneiden hallintaan kehitetty tekniikka.
WSUS	Windows Software Update Services, Microsoftin päivityspalvelu, joka asennetaan palvelimelle.

1 Johdanto

Tämän opinnäytetyön tarkoituksena on kehittää erään yrityksen verkkoinfrastruktuuri tasolle, joka vastaa yrityksen nykyisiä tarpeita. Yrityksellä oli käytössään Windows NT 4.0 -käyttöjärjestelmiin perustuvat NT-toimialueet, joiden tietoturva, hakemistopalvelut sekä hallintamahdollisuudet eivät vastanneet liiketoiminnan ja IT:n vaatimuksia. Projektissa NT-käyttöjärjestelmät päivitettiin Windows Server 2003 -käyttöjärjestelmiin. Samalla otettiin käyttöön Active Directory -arkkitehtuuri, johon NT-toimialueet migroitiin.

Tässä opinnäytetyössä yrityksestä käytetään nimeä Yritys Oy. Yritys Oy on monikansallinen yritys, jonka yli viisikymmentä toimipistettä sijoittuu Euroopan, Aasian ja Pohjois-Amerikan alueelle. Pääkonttori sijaitsee Suomessa. Yritys on vuosien kuluessa tehnyt lukuisia yritysostoja, joten verkkorakenteesta on tullut varsin haastava. IT-ympäristön ylläpidosta, lähituesta ja kehittämisestä vastasi ulkoistuskumppani, jolle työskentelin projektin aikana.

Ennen projektin käynnistymistä sitä suunniteltiin ja pohjustettiin pitkään. Suunnitteluun osallistui työnantajani puolelta viisi henkinen työryhmä ja Yritys Oy:n IT-johto. Tämä vaihe kesti yli vuoden ja sisälsi testiympäristön rakentamisen ja eri vaiheiden perusteellisen testaamisen.

Active Directoryn käyttöönotto ja konsolidointi tapahtui kahdessa eri vaiheessa. Projekti päätettiin toteuttaa toimipaikka kerrallaan, alkaen pääkonttorista. Ensimmäisessä vaiheessa luotiin toimialuemetsän juuritoimialue ”yritys.net” ja olemassa olevat NT-toimialueet päivitettiin Active Directory -toimialueiksi. Tämä vaihe saatiin päätökseen vuoden 2005 loppupuolella. Projektin toinen vaihe aloitettiin 2006, jolloin päivitetyt NT-toimialueet konsolidoitiin metsän juuritoimialueeseen. Projekti saatiin kokonaisuudessaan päätökseen syksyllä 2007.

Koko projekti kesti yli kolme vuotta ja siitä kertominen olisi ollut liian laaja opinnäytetyöksi. Tästä johtuen opinnäytetyössä käsitellään pääosin projektin toista vaihetta.

Tämän opinnäytetyön myötä tavoitteenani oli perehtyä Windows Server 2003-käyttöjärjestelmään sekä Active Directoryn tehokkaaseen hallintaan. Lisäksi kokemuksen saaminen ja ison monikansallisen projektin läpivieminen oli yksi työn tavoitteista.

2 Windows NT4 ja toimialueet

Windows NT 4.0 julkistettiin kesällä 1996, jolloin sitä kuvailtiin verrattoman helppokäyttöiseksi hallita sekä korkeampaan verkkosuorituskykyyn yltäväksi. Windows NT sisälsi täydellisen työkalupaketin intranetin kehittämiseen ja hallinnointiin. NT-palvelin oli tuolloin ainoa palvelinkäyttöjärjestelmä, jonka sisään oli rakennettu Web-palvelut. Ne tarjosivat sisään rakennetun intranet-ratkaisun. Se sisälsi myös Microsoft Internet Information Serverin *(IIS)*, jolla julkaistaan ja ylläpidetään Internetin WWW-sivustoja (1, s. 1).

NT 4.0 -toimialueiden kohdalla ei voi puhua hakemistopalveluista, koska hallittavien objektien tyypit ovat rajoittuneet vain kolmeen ja niille määritettäviä attribuutteja on vain muutamia. Hallittavia objekteja ovat tietokoneet, käyttäjät ja käyttäjäryhmät, joilla on siten pääsy verkon eri palveluihin (1, s. 1).

Julkistetut Windows NT 4.0:n versiot olivat Server, Workstation, Enterprise Edition, Terminal Server Edition ja Embedded Edition. Niissä oli entuudestaan tuttu Win 95-työpöydän ulkonäkö. Erilaisia lisäominaisuuksia julkaistiin erillisessä Option Pack-ohjelmistopaketissa: Internet Information Server 4.0 *(IIS 4.0)*, Microsoft Remote Access Service *(RAS)* (1, s. 1).

Erilaisia laajennuksia on tullut saataville vuosien mittaan:

- Distributed Files Systems (DFS)
- Web-hallinta (Web Admin)
- Load Balancing Service (WLBS)
- Routing and Remote Access Services (RRAS)
- Security Configuration Manager (SCM)
- NTLMv2 (SP4)
- Active Directory -asiakas (Dslient)

Windows NT:n tietoturvaan ja käyttöjärjestelmän toiminnallisuuteen tuomat uudistukset olivat aikoinaan merkittäviä ja osa on kelvollisia tänäkin päivänä.

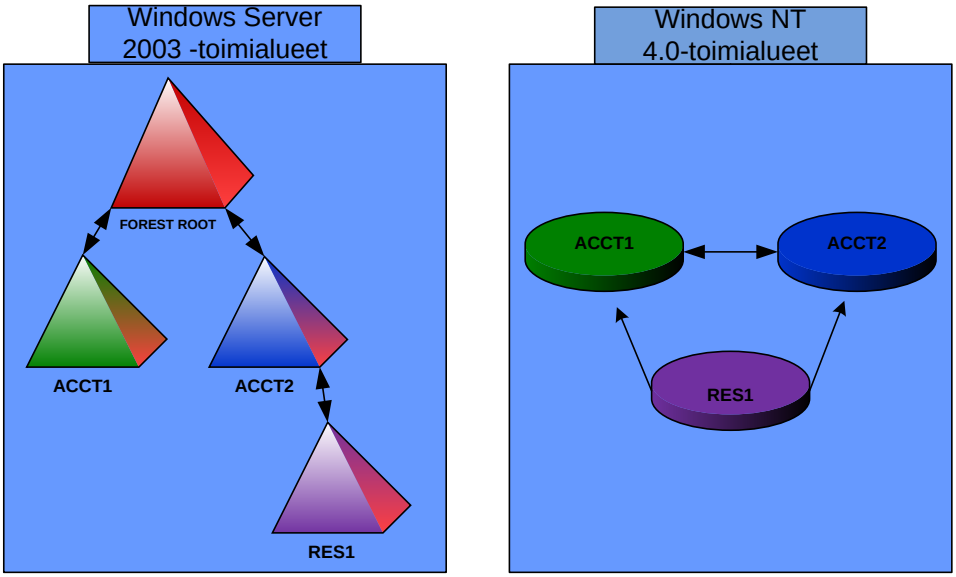
Hallinnointi ja verkkorajoitukset

Windows NT-toimialueilla objektien hallinta on rajoittunut vain käyttäjiin, tietokoneisiin ja käyttäjäryhmiin. Näille on tarjottu pääsy verkon palveluihin ja niiden kohdalla on mahdollista määritellä vain muutamia eri attribuutteja. NT:n kohdalla ei voida puhua hakemistopalvelusta. Windows NT-toimialueella on myös rajoituksena SAM *(Security Accounts Manager)* koko rajoitus, joka rajoittaa objektien määrä 40 000. Windows Server 2003-toimialueella objektien määrä on rajoitettu yli miljoonaan, joten enää ei tarvita uutta toimialuetta käsittelemään lisää objekteja (2).

Windows NT-toimialue on rakenteeltaan lattea, joten sen malli alkaa olla vanhentunut. Rakenteeseen ei ole juurikaan tullut mitään muutoksia Windows NT 3.1:n jälkeen.
Mikäli verkko sisältää useita hajautettuja toimipisteitä, tulee sen hallinta erittäin monimutkaiseksi (2).

Hajautetuille toimipisteille ja eri osastoille joutuu luomaan oman toimialueen, jotta resursseja voidaan erotella eikä käyttäjien kirjautuminen aiheuttaisi ongelmia. Lisäksi jokaiselle toimialueelle täytyy pystyttää yksi PDC-serveri *(Primary Domain Controller)* ja yksi tai useampi BDC-serveri *(Backup Domain Controller)* (2).

Mikäli organisaatiossa on tarvetta toimipisteiden välisten resurssien käyttöön, pitää näiden kaikkien toimipisteiden välille luoda luottosuhteet. Kuvasta 1 näkyy, että NT-toimialue ei myöskään tunne Active Directoryssä käytettävää kaksisuuntaisia ja siirtyviä luottosuhteita *(Two-Way Transitive Trust)*, vaan jokainen luottosuhde pitää erikseen asettaa voimaan. Se tekee verkon rakenteesta erittäin sekavan, aiheuttaen yhteysongelmia helposti. NT-toimialueella ei ole myöskään mahdollista delegoida ylläpito-oikeuksia kuin Domain-tasolla *(AD:ssa OU-tasolla)*, joten jokaisella toimialueella täytyy erikseen ylläpitää ryhmäkäytäntöjä, käyttäjätunnuksia ja oikeuksia (2).



Kuva 1. Active Directoryn ja NT 4.0-toimialueiden eroavaisuus luottosuhteissa.

Usean NT-toimialueen ylläpito aiheuttaa ongelmia, koska ne eivät tarjoa mahdollisuuksia asetusten keskitettyyn hallintaan. Windows NT-työasemalla tehdyt muutokset vaikuttavat vain kyseiseen työasemaan, joten esimerkiksi ryhmäkäytäntö-muutoksen tekeminen johtaisi siihen, että jokainen kone pitäisi käydä erikseen läpi. Toimialueella tehtävät muutokset vaikuttavat kyllä ohjauspalvelimiin, mutteivät työasemiin (3, s. 380).

Kaiken kaikkiaan usean NT-toimialueen ylläpito tulee monimutkaiseksi lattean ja monimutkaisen rakenteen sekä riittämättömien työkalujen puutteen vuoksi. Myös ylläpitoa kuormittaa jokaiselle toimialueelle erikseen pystytettävät PDC- ja BDC-palvelimet ja niiden ylläpito. On myös hyvä muistaa, että vain PDC voi hyväksyä päivityksiä toimialueen tietokantaan. Windows Server 2003:ssa kaikki DC:t *(Domain Controller)* voivat hyväksyä päivityksiä parantaen vikasietoisuutta (2).

Tuen päättyminen

Windows NT on saanut vuosien mittaan lukemattomia pikakorjauksia ja päivityksiä.
Laajempia päivityspaketteja on tullut useita ja viimeisin niistä on versio 6a.
Tämän jälkeen Microsoft ei ole enää julkistanut uusia päivitys-paketti versioita ja NT:n elinkaari on tullut tiensä päähän. Microsoft lopetti NT:hen tietoturvaan liittymättömien päivitysten jakelun jo 1. tammikuuta 2004. Tammikuussa 2005 lopetettiin myös käyttöjärjestelmän tietoturvaan liittyvät päivitykset sekä verkosta saatava online-tuki.

Tuotetuen loppumista voidaan pitää pakottavana syynä vaihtaa nykyaikaisempiin tuotteisiin. Ei ole järkevää jatkaa NT:n käyttöä, koska uusien tietoturva-aukkojen ilmetessä järjestelmät vaativat jatkuvaa päivittämistä tietoturvan ylläpitämiseksi. Myös vanhentuneen käyttöjärjestelmän käyttäminen työasemissa ja palvelimissa voi aiheuttaa käytettävyyden heikentymistä, koska niiden laitteistotuki alkaa heikentyä ja oheislaitteiden valmistajat eivät enää panosta vanhojen käyttöjärjestelmien laitteisto-ajureihin. Uusiin laitteisiin on mahdotonta löytää toimivia ajureita, ja laitteistojen suorituskyky heikentyy käyttäjämäärien lisääntyessä. Uudempien käyttöjärjestelmä-versioiden tuomat ominaisuudet tuovat merkitävän syyn päivittää, NT uudempaan käyttöjärjestelmään.

3 Windows Server 2003 -tuoteperheen esittely

Windows NT:n jälkeen julkistettiin Windows 2000-käyttöjärjestelmä. Se julkistettiin joulukuussa 1999. Saataville se tuli helmikuussa 2000. Windows 2000 Server-käyttöjärjestelmä on Windows NT 4.0 Serverin seuraaja. Alun perin sen nimeksi piti

tulla Windows NT 5.0. Windows 2000-tuoteperheeseen kuuluvat Professional-, Server-, Advanced Server- sekä Datacenter Server-käyttöjärjestelmäversiot. Se on tiedosto-, tulostus- ja sovelluspalvelin. Se sisältää IIS:n ja päätepalvelut *(Terminal Services)*. Siinä on tuki yksi- ja moniprosessorijärjestelmille aina neljää prosessoria käsittäviin järjestelmiin asti. Keskusmuistin tuki on sama kuin NT:ssä eli neljä gigatavua. Isoin uudistus oli Active Directory, jolla keskitetään muuan muassa käyttäjien, käyttäjäryhmien, tietokonetilien, tietoturva-asetusten ja sekä monien erilaisten verkkoresurssien hallinta. Active Directorystä kerrotaan enemmän seuraavassa luvussa (2).

Windows Server 2003 julkistettiin keväällä 2003, jolloin tuli uudistuksia ja laajennuksia Active Directoryyn. Sen suorituskykyä ja skaalautuvuutta oli tehostettu. Käyttöjärjestelmästä oli nyt saatavilla myös 64-bittiset versiot. Sen tietoturvaa ja hallintaa on tehostettu oleellisesti jo asennusvaiheessa, jossa konfigurointi tehdään roolipohjaisesti. Roolipohjaisessa käyttöönotossa vain tarpeelliset palvelut kytketään käyttöön. Tämä edes auttaa tietoturvan ylläpitämistä ja myös päivitysten asentamisen tarve pienentyy (2).

Windows Server 2003-perhe sisältää neljä eri tuotetta;

Windows Server 2003 Web Edition sisältää Web-palvelinympäristön ja tarjoaa Web-palvelujen sekä -sovellusten nopeaan kehittämiseen ja käyttöönottoon tarkoitetun ympäristön. Web-palvelut perustuvat Microsoft .NET Frameworksin, Internet Information Services:n, ASP.NET:n ja verkon resurssien jakamiseen. Muuten sen ominaisuudet ovat huomattavasti rajoittuneemmat kuin muiden versioiden. Se ei voi toimia Active Directory *(AD)* ohjauspalvelimena, eikä sisällä päätepalveluita, Internet-todennuspalveluita eikä etäasennuspalveluita. Web Editionista löytyviä tärkeitä ominaisuuksia ovat Distributed File System *(DFS)*, Encrypting File Systems *(EFS)*, ja se on hallittavissa selainpohjaisen liittymän avulla etäyhteyttä käyttäen. Web Edition voi toimia AD:n jäsenpalvelimena, vaikka siihen ei voi asentaa AD:ta.

Järjestelmävaatimuksien puolesta suositellaan minimissään 550 MHz:n suoritin-nopeutta ja keskusmuistia *(RAM)* tulisi olla 256 Mt. Versio tukee enimmillään 2 Gt:n muistia ja kahta prosessoria (4).

Windows Server Standard Edition on päivitys Windows NT 4.0 ja Windows 2000-Servereistä. Se on peruspalvelin kaikenkokoisten yritysten jokapäiväiseen käyttöön. Siitä löytyy yleisimmin käytetyt ominaisuudet, kuten tiedostojen ja tulostinten jakamistoiminnon, suojatut Internet-yhteydet, keskitetyn pöytätietokoneiden käyttöönoton sekä monipuolisille työntekijöille, yhteistyökumppaneille ja asiakkaille tarkoitetut yhteiskäyttötoiminnot. Se voi toimia AD-ohjauspalvelimena, joten se sisältää myös keskitetyn sovellusten käyttöönoton. Standard edition sisältää runsaasti ominaisuuksia ja konfigurointi vaihtoehtoja. Siksi se soveltuu erinomaisesti erilaisiin yrityskohtaisiin ratkaisuihin. Järjestelmävaatimuksina suositellaan minimissä 550 MHz:n suoritin-nopeutta, ja keskusmuistia tulisi löytyä 256 Mt. Versio tukee enimmillään 4 Gt:n muistia ja kahta prosessoria (4).

Windows Server 2003 Enterprise edition on keskikokoisille ja suurille yrityksille tarkoitettu skaalautuvainen palvelin, joka voi sisältää yrityksen infrastruktuurin, alakohtaiset sovellukset ja sähköisen kaupankäynnin tapahtumat. Se sisältää Windows Server 2003 Standard Editionin ominaisuuksien lisäksi Cluster Service-tuen, ja metahakemistopalvelut. Klusterointi (ryvästystekniikka) tukee enimmillään kahdeksaa erillistä palvelinta. Se tukee Intelin 64 bittistä Itanium prosessoria ja ”lennossa vaihdettavaa” RAM-muistia sekä NUMA-muistiinosoitusta *(Non Unifrom Memory Access)*. Lisäksi Enterprise -palvelimet tukevat kahdeksaa prosessoria sekä 32 Gt:n Ram-muistia x86-tietokoneissa ja 64 Gt:n RAM-muistia Itanium-tietokoneissa

Suositeltava minimikeskusmuistin määrälle on 256 Mt ja prosessorin suositeltava kellotaajuus tulisi olla 733 MHz (4).

Windows Server 2003 Datacenter Edition tarjoaa korkeimman tason skaalautuvuutta ja käytettävyyttä. Se on vaativille ja kriittisille ympäristöille suunniteltu käyttöjärjestelmä. Datacenter Edition sisältää kumulatiivisesti aikaisempien esiteltyjen versioiden

ominaisuudet. Se voi toimia Active Directoryn ohjauspalvelimena. Datacenter Edition on myös ihanteellinen palvelinten yhdistämisympäristö.. Datacenter Edition on suorituskyvyltään tarkoitettu isoihin konesaleihin, joissa tarvitaan isoja skaalattavia tietokantoja ja tehokasta tapahtumien käsittelyä. Keskusmuisti on tuettu 32-bittisessä ympäristössä 64 gigatavuun ja 64-bittisessä ympäristössä aina 128 gigatavuun asti. Prosessoreiden tuettu vähimmäismäärä on kahdeksan kappaletta. Se tukee 32-bittisessä järjestelmässä enintään kolmeakymmentäkahta ja 64-bittisessä kuuttakymmentäneljää prosessoria. Datacenter on Microsoftin tehokkain ja monipuolisin palvelinjärjestelmä, ja sitä saa hankittua ainoastaan erillisten sopimusehtojen kautta, usein laitteiston paketin hankinnan yhteydessä. Keskusmuistin suositeltava minimi on yksi Gt. Prosessorien kellotaajuuksien tulisi olla vähintään 733 MHz (4).

Kaikki edellä mainitut versiot sisältävät samat ydinominaisuudet ja hallintatyökalut.

Windows Server 2003 tuoteperheen käyttöönotto tuo mukanaan muutamia keskeisiä etuja (4):

Järjestelmän hallittavuutta, luotettavuutta ja saavutettavuutta on huomattavasti paranneltu. Palvelinympäristö, joka perustuu edeltäjänsä Windows 2000:ssa käyttöönotettuihin järjestelmänhallinta- ja ylläpitokonsepteihin, kuten Active Directory-hakemistopalvelu, suojausarkkitehtuuri, Windows Scripts Host, päätepalvelut ja IntelliMirror. Siihen on lisätty uusina ominaisuuksina muun muassa .NET -tuki. Järjestelmä on tehokkain ja joustavin Microsoftin toimittama tietojenkäsittely-arkkitehtuuri. Se perustuu monipuolisiin, joustaviin ja integroituviin ominaisuuksiin.

Sen kehitysympäristö on monipuolisempi ja se perustuu alan standardeihin, joita voidaan hyödyntää uusien sovelluksien kehittämisessä tai jo olemassa olevien laajemmassa käytössä. Se mahdollistaa kehittäjien työskentelyn suoraan sovelluspalvelimella käyttäen sen Web-palveluita tai valmista koodia. Sovellukset voidaan suorittaa missä tahansa Web-sovellusympäristössä.

Tietoturvan ja sen hallintaa on tehostettu ottamalla käyttöön roolipohjaiset palvelimien oletuskonfigurointi. Se takaa asiakasyhteyksien suojauksen ja parantaa niiden yhteyksien laatua. Se sisältää joustavia viestintämenetelmiä ja mukautettavia työkaluja. Palvelujen ja viestintämuotojen sovittaminen tarpeisiin on helppoa. Suojausarkkitehtuurin ja Active Directory-hallintamallien avulla voi toteuttaa koko organisaation työasemien ja palvelimien suojausasetukset

4 Active Directoryn yleiskuvaus

Active Directory-palvelu tarkoittaa Microsoftin toteutusta hakemistopalvelusta. Siitä käytettään suomenkielistä termiä aktiivihakemisto ja sen lyhenne on AD. Windows Server 2003:n hakemistopalvelut perustuvat siihen ja se toimii Windows Serverin sydämenä. Aktiivihakemistopalvelu perustuu LDAP *(Light Weight Directory Access Protocol)* -protokollaan. Sen tarkemmat avoimet verkkoprotokollat ja määritykset löytyvät standardoiduista Internet-protokollista RFC 1777 ja 2251. Sen ydin LDAP on johdettu OSI X.500-hakemistomallista (5).

Hakemistopalvelu *(Directory Service)* eroaa hakemistosta *(Directory)* sisältämällä tiedot eli tietovaraston *(tietokannan)* ja tarjoamalla myös palvelut joiden avulla voidaan helposti hakea ja muokata hajautetuista hakemistoista olevaa tietoa. Active Directory-palvelu on skaalatutuva, hierarkkinen ja laajennettavissa oleva palvelu, jonka tehtävänä on vähentää ylläpidettävien hakemistojen määrää. Sen yhteisten rajapintojen ja työkalujen avulla voidaan helposti hallita eri objektien, kuten käyttäjien, tietokonetilien, tulostimien ja muiden verkon jaettujen resurssien attribuutteja eli ominaisuuksia. Lähes kaikki verkon hallintatoimet tapahtuvat sen kautta, kuten käyttäjien kirjautumisessa käytettävät tunnistepalvelut LAN Manager, Kerberos ja älykorttiin perustuvilla menetelmillä.

Windows NT:n yhteydessä puhuttiin hakemistopalveluista *(NT Directory Services)* mutta Windows NT ei sisältänyt standardin mukaista hakemistopalvelua. Active Directoryn ensimmäinen versio tuli Windows 2000-Server käyttöjärjestelmän mukana ja uudempi versio siitä tuli Windows Server 2003-käyttöjärjestelmän myötä. Windows

Server 2003-käyttöjärjestelmässä siihen tuli huomattavasti laajennuksia ja tehostettuja toimintoja.

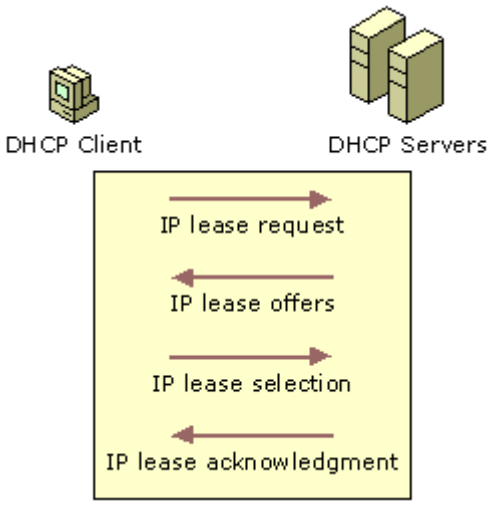
Active Directoryssä on siis kysymys loogisesti yhdessä paikassa sijaitsevien objektien käsittelystä erilaisilla työkaluilla eli hajautetun järjestelmän keskitetystä hallinnasta. Hallintatyökalusta riippuu mitä sinne tallennettuja tietoja voidaan käsitellä ja miten. Esimerkiksi ADSIEdit.mcs, Ldp.exe, Active Directory Replication Monitor ja Active Directory Users and Computers-hallintakonsoli tuottavat kaikki erilaisen näkymän Active Directorystä. Active Directory koostuu myös joukosta muita komponentteja ja se koostuu myös useista eri osioista *(partition)*. Hallintatyökaluja on monia, joten järjestelmänvalvojan tulisi olla edes jollakin lailla perillä AD:n keskeisistä ominaisuuksista ja hallintatyökaluista.

Active Directoryn käyttää nimipalvelujärjestelmää *(Domain Name Systems, DNS).* Se muuntaa tietokonenimet IP- osoitteiksi *(Internet Protocol)* ja organisoi tietokonejoukot toimialueiksi. DNS-järjestelmä on rakenteeltaan hierarkkinen. Se muodostuu eritasoisista palvelimista. DNS pitää itse asiassa olla määritelty ennen kuin Active Directory voidaan asentaa. Se voidaan myös asentaa ensimmäisen ohjauspalvelimen asentamisen yhteydessä.

Active Directoryn tietokantoja pidetään yllä ohjauspalvelimissa. Niihin varastoidaan tiedot eri objekteista ja niiden attribuuteista. Kun Active Directory otetaan käyttöön, syntyy uusi toimialue eli hallinnollinen ryhmä, jonka objektien tiedot on kerätty samaan hakemistotietokantaan. Kun koko verkon resurssien tiedot löytyvät hakemistosta, siihen on helppo suorittaa täsmennettyjä hakuja eri attribuuttien perusteella välittämättä niiden fyysisestä sijainnista. Tällaisen hakemiston hallinnointi on helppoa, koska muutoksia tarvitsee tehdä vain yhteen ohjauspalvelimeen. Pienen viiveen kuluessa ne monistavat tiedon palvelimesta toiseen kaikkiin verkon ohjauspalvelimiin ja tulevat voimaan koko toimialueella. Näin kaikissa verkon pisteissä ja osissa on yhteneväinen hakemistotietokanta.

4.1 DHCP-protokolla

Dynamic Host Configuration Protocol *(DHCP)* on standardi verkkoprotokolla, joka kuvataan RFC 1541:ssä ja uudempi DHCPv6 *(IPv6)* RFC 3315:ssä (6, s. 7). Sen avulla palvelin voi dynaamisesti jakaa IP-osoitteet verkkoon kytkeytyville laitteille, kuten kuvassa 2 esitetään.



Kuva 2. DHCP vuokraus prosessi (7).

DHCP voi myös jakaa paljon muitakin verkon asetuksia, joista yleensä jaetaan seuraavat:

- IP-osoite
- oletusyhdyskäytävä
- aliverkon peite
- nimipalvelimen osoite
- WINS serverin osoite.

Työasemille voidaan myös jakaa erilaisia informaatioasetuksia, joilla määritellään erikseen taulukossa 1 olevat vaihtoehtoiset tyypit ja niiden eri arvot. Nämä arvot toimitetaan työasemille.

Taulukko 1. DHCP:n informaatioasetukset (7).

Koodi	Kuvaus
3	Reititin
6	DNS serveri
15	DNS toimialueen nimi
44	WINS serveri (NetBIOS nimi serveri)
45	NetBIOS datagrammin jakelu serveri (NBDD)
46	WINS/NetBIOS solmutyyppi
47	NetBIOS vaikutusalueen ID

Työasemille voidaan myös määrittää protokolla-asetukset, jotka määrittelevät DHCP-palvelimen soveltamisalan, ja niiden ominaisuuksien asetukset, joita taulukko 2 esittää.

Taulukko 2. DHCP-protokolla-asetukset (7).

Koodi	Kuvaus
51	vuokra aika
53	DHCP viesti tyyppi
55	Spesiaali optio tyyppi, jota käytetään kun toimitetaan pyyntö parametriluettelona DHCP-palvelimen avulla
58	Uusimisen aika arvo (T1)
59	Uudelleen kytkemisen aika arvo (T2)

4.2 WINS- ja DNS-palvelut

WINS *(Windows Internet Name Service)* ja DNS ovat kumpikin nimenselvitys-palveluita. WINS:n tehtävä on määrittää NetBIOS-nimet IP-osoitteille sellaisissa verkoissa, jotka käyttävät NetBIOS:ia yli TCP/IP-protokollien. WINS pääasiassa tukee työasemia, jotka käyttävät Windowsin vanhempia versioita ja sovelluksia, joiden

toiminta tarvitsee NetBIOS:ia. Windows 2000, Windows XP ja Windows Server 2003 ja sitä uudemmat käyttöjärjestelmät käyttävät pääasiallisesti DNS:ää nimenselvitykseen (8). WINS- ja NetBIOS-standardien kuvaukset löytyvät dokumenteista RFC 1001 ja RFC 1002. Microsoft suosittaa käyttämään WINS-palvelua, koska käytössä on vielä paljon sovelluksia, jotka käyttävät NetBIOS nimen selvitystä (9). Vaikka AD ei WINS:iä tarvitsisikaan, vanhemmat Exchang Serverit 2000 ja 2003 käyttävät yhä sen toiminnallisuuksia. Lisäksi Exchange 2007 ja System Center Configuration Managerin tietyt toiminnallisuudet käyttävät NetBIOS-nimenselvitystä ja vaativat WINS:n (10;11).

4.3 LDAP-protokolla

Lightweight Directory Access Protocol on hakemistopalvelujen käyttöön tarkoitettu TCP/IP-protokollan päällä toimiva verkkoprotokolla. Se koostuu kolmesta osasta, joita ovat tietomuoto, protokolla ja ohjelmointirajapinta *(API)* (12). Se on johdettu monimutkaisemmasta X.500-mallista, ja sen ensimmäinen versio kehitettiin 1993. Sen kehittämisestä vastaa nykyään IETF eli International Engineering Task Force. Ensimmäinen laajasti käyttöön otettu versio LDAP:sta oli LDAPv2 vuonna 1995, jonka kuvaus on RFC 1777-dokumentista. Nykyään laajasti käytössä oleva versio on LDAPv3, ja sen kuvaus on RFC 2251:ssä. LDAP:a kuvataa myös muun muassa seuraavissa standardeissa:

- RFC 2252 - Mandatory Schema.
- RFC 2253 - Distinguished Names.
- RFC 2254 - LDAP URLs.
- RFC 2255 - Search Filters.
- RFC 2256 - User Schema.
- RFC 2829 - Authentication Methods.
- RFC 2830 - Transport Layer Security ja Digest Authentication.

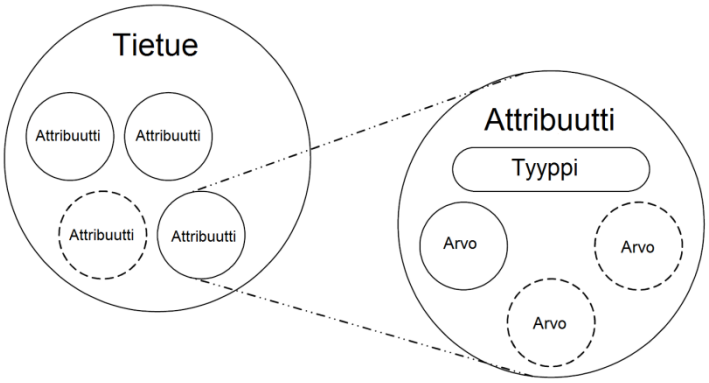
Active Directoryssä LDAP-hakemiston ylläpidosta huolehtii DSA-prosessi *(Directory Service Agents)*. Sen tehtäviin kuuluu asiakkaiden ja hakemiston väliseen yhteydenpitoon liittyvät toimenpiteet. Asiakkaat ottavat yhteyttä DSA-prosessiin

käyttämällä Microsoftin ADSI:a *(Active Directory Service Interface),* joka on hakemistojen käsittelyyn tarkoitettu rajapinta. LDAP käyttää tietojen tallentamiseen DIT-tietokantatiedostoa, *(Directory Information Table)* joka on Active Directoryssä ntds.dit-niminen tiedosto. Kun DSA kohdistaa muutoksia tähän tiedostoon, se ei tapahdu suoraan vaan erillisen Extensible Storage Enginen kautta. Se parantaa tietokannan suojausta. LDAP-standardi määrittelee neljä mallia, jotka ohjaavat hakemiston käyttöä. Nämä mallit ovat seuraavat (13):

- Tietomalli määrittelee, minkälaista tietoa hakemistoon voi tallentaa.
- Nimeämismalli määrittelee, kuinka tietueet nimetään ja organisoidaan hakemistossa.
- Toimintamalli määrittelee, kuinka hakemistossa oleviin tietoihin voidaan tehdä hakuja ja kuinka sen tietoja ylläpidetään.
- Tietoturvamalli määrittelee, kuinka hakemisto voidaan suojata luvattomalta käytöltä.

Tietomalli

Tietomalli määrittelee hakemistoon tallennettavien tietojen attribuuttien tyypit ja niistä koostuvat tietuerakenteet. Tietueet rakentuvat attribuuteista, jotka voivat saada yhden tai useamman arvon. Syntaksissa määritellään, minkä muotoista tietoa attribuutit voivat saada arvoikseen. Syntaksissa määrätään myös miten attribuuttien arvoja vertaillaan hakuja tehtäessä (5, s. 2). Kuvassa 3 kuvataan tietueita, attribuutteja ja arvoja.



Kuva 3. Tietueiden syntaksi.

Nimeämismalli

Nimeämismallin mukaan tietueet järjestetään LDAP-hakemistoon puumaiseen rakenteeseen. Tätä mallia kutsutaan lyhenteellä DIT *(Directory Information Tree).* Active Directory käyttää neljää eri tapaa tiedon nimeämiseen ja järjestämiseen hakemistopuussa. Nämä tavat ovat Distinguished Name *(DN),* Relative Distinguished Name *(RDN),* Globally Unigue Identifier *(GUID)* ja User Principal Name *(UPN).* Nimeämismallin tarkka syntaksi määritellään standardissa RFC 2253.

Tietueiden järjestys hakemistopuussa perustuu niiden DN- eli yksikäsitteisiin nimiin. DN-nimi muodostetaan yhdistäen tietueen nimi ja hakemistopuussa tätä edeltävien tietueiden nimet. Se koostuu siis useasta yksikäsitteisestä nimestä eli RND:stä. RDN vastaa solmua hakemistopuussa, joka alkaa juurisolmusta ja päättyy hakemistotietueeseen (13). Yksinkertaisimmillaan RDN on muotoa:

<*attribuutin / tietueen-nimi* > = <*arvo*>.

RDN-nimi voi esiintyä samassa toimialueessa useamman kerran, kunhan organisaatioyksikkö (OU) on eri. Tästä johtuen sitä kutsutaan suhteelliseksi nimeksi (14, s. 404). Organisaatioyksikköön voidaan sijoittaa myös muita objekteja.

Otetaan mallin selventämiseksi esille esimerkki, jossa organisaatioyksikkö on Relative Distinguished-nimeltään OU=Osasto. Jos tässä organisaatioyksikössä olisi käyttäjä

nimeltään Juha, olisi se Relative Distinguished-nimeltään CN=Juhak. CN-lyhenne *(Common Name)* tarkoittaa tässä yksittäisen objektin normaalia nimeä, kuten esimerkiksi käyttäjätunnus. Jos kuvitellaan kyseinen OU sijaitsevaksi toimialueella, jonka nimi on metropol.local, saadaan esimerkin Distinguished Nameksi:

CN=Juhak,OU=Osasto,DC=metropol,DC=local.

UPN on käyttäjän ensisijainen nimi *(User Principal Name),* jota käytetään toimialueeseen kirjauduttaessa. Nimi koostuu kahdesta osasta, joista alkupää koostuu kirjautumistunnuksesta *(User Logon Name)* ja DNS-toimialuenimestä *(UPN suffix)* tai sen jälkiliitteestä. Kun käytettään edellisen kappaleen esimerkin tietoja, saadaan UPN-nimeksi juhak@metropolia.local. Näiden tunnuksien pitää olla ainutlaatuisia koko toimialueen-metsän sisällä. Jos halutaan käyttää kirjautumistunnusta samana kuin käyttäjän sähköpostiosoite, on se otettava huomioon toimialueen nimeämisen suunnittelussa (1, s. 441).

GUID *(Globally Unique Identifier)* on 128-bittinen heksadesimaalinumero, jonka Directory Service Agents-antaa objektille, kun se luodaan. GUID ei milloinkaan muutu, vaikka objekti siirrettäisiin tai sen toimialuenimi muutettaisiin, toisin kuin Windows NT-ympäristössä (15, s. 1-32).

Toimintamalli

LDAP-toimintamalli kuvaa hakemistoon suoritettavia operaatioita, jotka voidaan jakaa kolmeen eri osa-alueeseen ja jotka sisältävät eri vaiheita ja toimintoja. Ne voidaan jakaa seuraavasti: todennus-, kysely- ja päivitysoperaatiot. Todennusoperaatioita ovat *bind, unbind* ja *abandon*. Bind-operaatiolla asiakas suorittaa protokollaistunnon perustamisen ja käyttäjän tunnistautumisen LDAP-palvelimelle. Tätä ei pidä sekoittaa yhteydenottamiseksi palvelimeen, vaan se on lähinnä todentautumista palvelimelle. Unbind-operaatiolla lopetetaan yhteys eli operaatioista luopuminen ja yhteyden sulkeminen. Abandon-operaatiolla puolestaan keskeytetään jo käynnistetyt operaatiot (16).

Kyselyoperaatiot (*Query)* liittyvät hakemistossa olevan tiedon hakemiseen, suodattamiseen, vertailemiseen ja käyttämiseen. Yleisimmät kyselyoperaatiot ovat *search* ja c*ompare search.* Search-operaatiolla asiakas pyytää LDAP-palvelimelta kriteerien mukaista listausta lukua varten. Compare-operaatiolla pystytään tekemään LDAP-palvelimella oleviin attribuutteihin vertailua kysymällä, onko niillä jotain tiettyä arvoa. Vastauksena compare-kyselyihin saadaan joko ”TRUE” tai ”FALSE” (13, s. 51).

Kolmas toimintamallin osa on hakemiston päivitysoperaatiot *(update operations).* Päivitysoperaatioilla lisätään *(add),* muokataan *(modify)* ja poistetaan *(delete)* hakemistossa olevia tietoja. Nämä operaatiot ovat niin kutsuttuja atomisia, eli ne joko suoritetaan onnistuneesti loppuun tai niitä ei suoriteta ollenkaan. Modify DN-operaatiolla tietue voidaan siirtää DIT:n sisällä toiseen paikkaan, mutta sitä ei voi siirtää palvelimen rajojen yli (13, s. 52).

Tietoturvamalli

Tietoturvamalli kuvaa, miten LDAP-hakemistopalvelun tietoja voidaan käsitellä turvallisesti. Malli perustuu Bind-operaatioon. LDAP-malli on yhteyspohjainen protokolla *(connection-oriented)*, jossa asiakas avaa yhteyden todentumalla palvelimelle ja suorittaa operaatiot. LDAP-standardissa RFC2222 määritellään, miten Simple Authentication and Security Layer *(SASL)*-järjestelmän määrityksiä voidaan käyttää hakemiston suojaamiseen LDAPv3:ssa. SASL on yleinen todennusmalli, jonka standardissa määritellään useita eri todennusmetodeja. Tällaisia Active Directoryn tukemia todennusmetodeja ovat muun muassa Kerberos versio 5 ja MS Negotiate (17).

Active Directoryssä voidaan turvallisuussyistä hallita jaettujen resurssien käyttöoikeuksia suojauskuvauksilla *(Security descriptors)* ja käytönvalvonnan avulla. Suojauskuvaukset sisältävät luettelon jossa voidaan määrittää, miten eri käyttäjät voivat käyttää kutakin erilaisia objekteja, kuten tiedostoja, tulostimia, kansioita ja palveluita. Näitä luetteloita kutsutaan käyttöoikeusluetteloiksi *(Access Control List, ACL).*
Käytönvalvontaa hallinnoidaan objektin tasolla asettamalla erilaiset pääsyoikeustasot tai käyttöoikeudet. Objekteille myönnetään oikeuksia kuten esimerkiksi täydet, kirjoitus-

tai lukuoikeudet tai ei oikeuksia lainkaan. Käytönhallinta määrittää, miten eri käyttäjät voivat käyttää aktiivihakemiston objekteja. Objektien käyttöoikeudet määritetään oletusarvoisesti turvallisimman asetuksen mukaan.

Active Directory käyttää siis kahta erilaista käyttöoikeusluetteloa (ACL:ää). Discretionary Access Control Lists (DACL)-harkinnanvarainen käyttöoikeusluettelo, jonka tehtävä on tunnistaa käyttäjät ja ryhmät, joille on annettu tai estetty objektin käyttöoikeudet. Oletusarvoisesti oikeudet ovat objektin omistajalla tai henkilöllä, joka loi kyseisen objektin. Objekti sisältää Access Control Entries:n (ACE), jossa määrittellään käyttöoikeudet. Toinen AD:n käyttämä käyttöoikeusluettelo on System Access Control Lists (SACL) -järjestelmän käytönvalvonnan luettelo. Se tunnistaa käyttäjät ja ryhmät, joita halutaan valvoa, kun ne onnistuvat tai epäonnistuvat käyttämään objektia. Auditointia käytetään seuraamaan järjestelmän tai verkon turvallisuuden tapahtumia, identifioida turvallisuusrikkomuksia ja määritellä niiden laajuus sekä vahinkojen sijainti. Oletusarvoisesti tämäkin sisältää ACE:n, jossa nyt määritellään kirjataanko objektin onnistuneet tai epäonnistuneet yritykset tai onko objektin oikeuksiin tehty tai yritetty tehdä muutoksia (18).

Käyttäjiin tai objekteihin viitataan usein nimen perusteella, mutta käyttöjärjestelmä sisäisesti viittaa objekteihin niiden suojaustunnusten (Security Identifier, SID) perusteella. Toimialueen suojauspääobjektin SID luodaan ketjuttamalla toimialueen suhteellisen tunnuksen Relative Identifier (RID) tili SID:iin.

SID on yksilöllinen toimialueen sisällä, eikä sitä koskaan käytetä uudestaan. SID:stä yksilöllisen tekee sen loppuosa eli RID, joka on juokseva numerosarja. SID:n alkuosa tietyllä toimialueella on aina sama. Järjestelmä luo objektin tekohetkellä sille SID:n, joka yksilöi objektin. Administrator-tilin suojaustunniste on helposti selvitettävissä, koska sen suhteellinen tunniste RID on aina 500. Vaikka tilin nimeäisi uudelleen, RID ei muutu, minkä takia Administrator-tili on usein hyökkäyksen kohde. Siksi tilin poistamista kannattaa joskus harkita (18).

LDAP:n tunnistuksesta löytyy mm. seuraavat standardit:

- RFC2078 - Generic Security Service Application Program Interfac.
- RFC2251 - Lightweight Directory Access Protocol (v3).
- RFC1510 - The Kerberos Network Authentication Service (V5).

4.4 Active Directoryn looginen rakenne

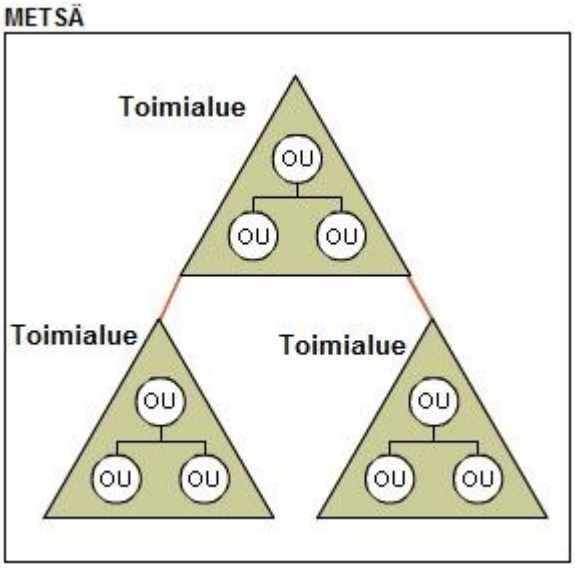
Ennen kuin voidaan suunnitella Active Directoryn looginen rakenne, on tärkeää ymmärtää Active Directoryn looginen malli. Active Directory on hajautettu tietokanta, joka tallentaa ja hallitsee tietoja verkkoresursseista, kuten myös sovelluskohtaisista tiedoista, jotka hakemisto on sallinut. Active Directoryn avulla järjestelmänvalvojat voivat järjestellä verkon osia (kuten käyttäjät, tietokoneet, laitteet ja niin edelleen) verkon hierarkkiseen eristyksen rakenteeseen. Ylimmän tason säilö on metsä, minkä sisällä ovat toimialueet ja toimialueen sisällä organisaatioyksiköt. Tällaista kutsutaan loogiseksi malliksi, koska se on riippumaton fyysisien näkökohtien käyttöönotoista, kuten toimialueen ohjauskoneiden tarvittavasta lukumäärästä kuhunkin toimialueeseen ja verkkotopologiaan. Loogisten rakenteiden avulla voidaan järjestää hakemisto-objekteja ja hallita verkkotilejä ja jaettuja verkkoresursseja (19) .

Active Directoryn loogisia rakenteita ovat (20):

- toimialuemetsät (Domain Forests).
- toimialuepuut (Domain Trees).
- toimialueet (Domains).
- organisaatioyksiköt (Organizational Units).

Toimialuemetsät

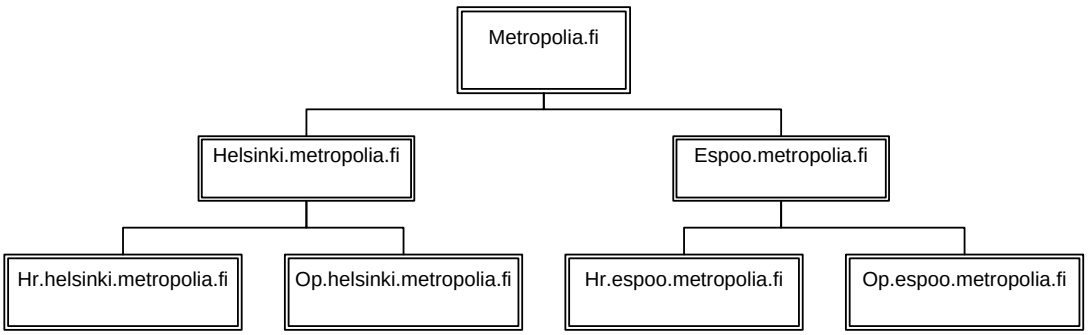
Toimialuemetsä on kokoelma yhdestä tai useammasta Active Directory-toimialueesta, jotka jakavat yhteisen loogisen rakenteen, yleisen luettelon, kansion rakenteen ja kansion kokoonpanon sekä automaattiset kaksisuuntaiset siirtyvät luottamussuhteet. Kukin toimialuemetsä on yksittäinen hakemistoinstanssi ja määrittää suojauksen rajat. Kuvassa 4 esitetään metsän, toimialueen ja organisaatioyksikön välisiä suhteita (20).



Kuva 4. Metsän, toimialueen ja organisaatioyksikön väliset suhteet.

Toimialuepuut

Toimialueilla on jatkuva nimirakenne (nimiavaruus), kun niiden sanotaan olevan samassa toimialuepuussa. Esimerkki toimialuepuusta näkyy kuvassa 5. Tässä esimerkissä juuri toimialueella metropolia.local:lla on kaksi lapsitoimialuetta-espoo.metropolia.local ja Helsinki.metropolia.local. Näillä toimialueilla on puolestaan alitoimialueita. Kaikki toimialueet ovat osa samaa puuta, koska niillä on yhteinen päätoimialue (20).



Kuva 5. Toimialueilla, jotka jakavat saman puun. On jatkuva nimirakenne.

Toimialueet

Active Directory-toimialue on yksinkertaisesti joukko tietokoneita, joilla on yhteinen kansiotietokanta (Global Catalog). Active Directory-toimialueen nimen on oltava yksilöllinen. Esimerkiksi kahta metropolia.fi -toimialuetta ei voi olla. Mutta voi olla päätoimialueena metropolia.fi, jonka alla on kaksi alitoimialuetta espoo.metropolia.fi ja helsinki.metropolia.fi (20).

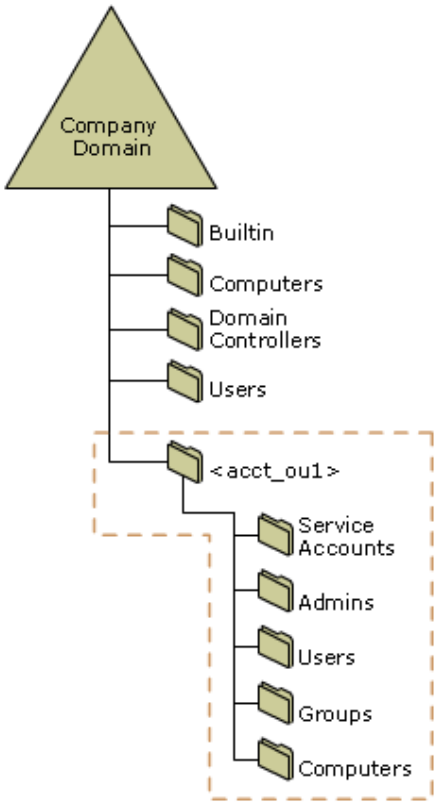
Määriteltäessä uutta toimialuetta verkkoon (yksityinen verkko tai Internet), sen nimi ei saa olla ristiriidassa jo olemassa olevien toimialueiden nimien kanssa tässä kyseisessä verkossa. Luotaessa toimialuetta Internetiin, se tulee ennen luomista rekisteröidä. Näin varmistetaan sen yksilöllisyys ja vältytään ongelmilta (20).

Kullakin toimialueella on oma turvallisuuspolitiikka ja luottamussuhteet muiden toimialueiden kanssa. Toimialue voi ulottua myös useampaa fyysiseen sijaintiin, minkä vuoksi se voi koostua useasta toimipaikasta ja nuo toimipaikat voivat sisältää useita aliverkkoja. Toimialueen hakemistotietokannassa ovat määritellyt objektit, kuten käyttäjätilit, ryhmät, tietokoneet, sekä jaetut resurssit, kuten tulostimet ja kansiot (20).

Organisaatioyksiköt

Toimialueen sisällä erityisen hyödyllinen hakemistoobjekti on organisaatioyksikkö (OU). Active Directoryssä organisaatioyksikköön voi sijoittaa käyttäjiä, ryhmiä,

tietokoneita ja toisia organisaatioyksiköitä. Organisaatioyksiköt tulisi järjestellä loogiseksi hierarkkiseksi rakenteeksi, joka sopii yrityksen toimintatapaan tai rakenteeseen. Esimerkkirakenne on esitetään kuvassa 6 (20).



Kuva 6. Tilien OU-rakenne (21).

Organisaatioyksikkö ei voi sisältää toisten toimialueiden objekteja. Organisaatioyksikkö on myös pienin vaikutusala tai yksikkö, johon voidaan määrittää ryhmäkäytännön asetuksia tai delegoida hallinnollisia oikeuksia. Taulukossa 3 kuvataan eri lapsi-OU:den käyttötarkoituksia.

Taulukko 3. Lista ja kuvaus niistä lapsi-OU:eista, joita voidaan tehdä OU-rakenteeseen (21).

OU	Käyttötarkoitus
Users	Sisältää normaali käyttäjätilit
Service Accounts	palvelut, jotka edellyttävät verkkoresurssien suorituksen käyttäjätileillä. Tähän organisaatioyksikköön luodaan käyttäjä-tilit, joilla ajetaan erillisiä palveluita.
Computers	Sisältävät muut tietokonetilit paitsi toimialueen ohjauskoneet.
Groups	Sisältää kaikenlaisia ryhmiä, paitsi hallinnointi ryhmät, joita ylläpidetään erikseen.
Admins	Sisältää järjestelmänvalvojille tarkoitettuja käyttäjä- ja ryhmätilejä, sallien heille ylläpitää erikseen muita käyttäjiä ja asetuksia. Tähän OU:hun tulee asentaa auditointi, jotta voidaan seurata muutoksia järjestelmänvalvoja tileihin.

Hallinnointivaltuudet voidaan delegoida yksittäiseen organisaatioyksikköön tai useisiin yksiköihin. Toimialueen sisällä organisaatioyksikön hierarkia on riippumaton muiden toimialueiden rakenteesta: kukin toimialue voi toteuttaa oman hierarkian. Toimialueilla, joita hallitaan keskitetysti, voidaan ottaa käyttöön rakenteeltaan samanlaiset hierarkkiset organisaatioyksiköt.

Joustavan rakenteen avulla organisaatiot voivat luoda ympäristön vastaamaan hallinnointimallia. Hallinnointimallin tulee olla keskitetty tai hajautettu.

4.5 Palvelun fyysinen rakenne

Active Directoryn fyysistä rakennetta edustavat sen fyysiset osat. Oikein suunniteltuina ja konfiguroituina ne edesauttavat optimoimaan verkon toistamista ja kirjautumista kyseiseen fyysiseen verkkoon sopiviksi.

Active Directoryn fyysisiä rakenteita ovat aliverkot ja palvelinjoukot (20).

Aliverkot

Aliverkon voidaan ajatella olevan ryhmä verkko-osoitteita. Toisin kuin palvelinjoukot, jotka voivat sisältää useita IP-osoitealueita, aliverkoilla on tietty IP-osoitealue ja aliverkon peite. Aliverkkojen nimet muodostetaan verkko-osoitteesta ja bittipeitteestä, kuten esimerkiksi 196.166.15.0/24. Tässä verkko-osoite 196.166.15.5 ja aliverkon peite 255.255.255.0 muodostavat yhdessä aliverkon nimen 196.166.15.0/24 (20).

Palvelinjoukot

Palvelinjoukko on joukko tietokoneita, jotka kuuluvat yhteen tai useaan IP-aliverkkoon. Palvelinjoukkojen avulla voidaan kartoittaa verkon fyysinen rakenne. Palvelinjoukkojen kartoitus on riippumaton loogisista toimialuerakenteista, joten verkon fyysisen rakenteen ja loogisen rakenteen välillä ei välttämättä ole yhteyttä. Active Directoryn avulla voidaan luoda yhden toimialueen sisään useita palvelinjoukkoja tai yksi palvelinjoukko, joka palvelee useita toimialueita. Palvelinjoukossa ja toimialueen nimiavaruudessa käytettyjen IP- osoitealueiden välillä ei ole yhteyttä (20).

Fyysisen verkon osia, kuten toimialueen ohjauskoneita ja fyysisiä aliverkkoja, käytetään helpottamaan verkkoliikennettä ja asettamaan fyysiset rajat verkkoresursseille.

Yrityksen verkossa Active Directoryn fyysistä rakennetta erityisesti edustavat kaikki fyysiset aliverkot Active Directory -palvelinjoukot, joissa ohjauskoneet replikoivat keskenään (22).

4.6 Active Directoryn toiminnallisuustasot

Active Directoryn toimialueen palveluissa (AD DS) voidaan toimialueen ohjauskoneissa suorittaa eri versioita Windows Server-käyttöjärjestelmästä. Toimialueen tai metsän toiminnallisuustaso riippuu niissä käytettävien ohjauspalvelimien käyttämistä käyttöjärjestelmä versioista. Toimialueen tai metsän

toiminnallisuustaso määrittelee, mitä edistyksellisiä ominaisuuksia on käytettävissä (23).

4.6.1 Toimialueen toimitasot

Active Directoryn toimialueella on neljä eri toiminnallisuustasoa. Windows Server 2003 ympäristössä. Toiminnallisuustasoja ovat Windows 2000 mixed, Windows 2000 native, Windows Server 2003 intermin sekä varsinainen Windows Server 2003-tila (24).

Windows 2000 mixed mode (sekatila) on oletus uusilla Active Directory-toimialueilla Windows 2000 Server- ja Windows Server 2003-ympäristöissä. Tämän tilan ollessa käytössä Active Directory tukee Windows Server 2003- ja Windows Server 2000 Server- sekä Windows NT-varaohjauspalvelimia. Sekatilassa Windows 9x-käyttöjärjestelmät toimivat, kuten ne toimisivat Windows NT-toimialueella, mikäli niihin ei ole erikseen asennettu AD-asiakasohjelmistoja. Myös NT4-työasemat ja palvelimet käyttäytyvät samalla periaatteella.

Jotta tieto Active Directorystä saataisiin replikoitua Windows NT-varaohjaus-palvelimille, tulee olemassa oleviin Windows 2000- tai Windows Server 2003-ohjauskoneesiin asentaa PDC-emulaattori (Primary Domain Controller). Tässä tilassa on käytössä vain hakemiston perusominaisuudet ja uudet ominaisuudet kuten tuki universaaleille ryhmille, Ohjauspalvelimien uudelleen nimeäminen, Kerberoksen KDC -avain (Key Distribution Center) versionumerointi, sisäkkäiset ryhmät ja kirjautumisleimojen päivitysten replikointi eivät ole käytössä (24).

Windows 2000-native mode (natiivitila) tukee ainoastaan Windows 2000 Server- ja Windows Server 2003-palvelimia. Windows NT-palvelimia ei tueta. Tässä tilassa saadaan käyttöön joitakin edistyneitä tekniikoita, kuten esimerkiksi universaalit ryhmät, sisäkkäiset ryhmät ja niiden tyyppien muuntaminen, sekä (SID) historia on käytettävissä migraatiotilanteessa toimialueelta toiselle, jolloin resurssikohtaiset käyttäjätunnukset säilyvät. Ohjauskoneiden uudelleen nimeäminen, kirjautumisleimojen päivitys ja Kerberoksen KDC-avainversionumerointi eivät ole tuettuja. On erittäin tärkeä

tiedostaa, että otettaessa natiivitila käyttöön, menetetään samalla tuki NTLM-replikointiin. Tätä replikointia käyttävät mm. Windows NT-palvelimet, mutta se ei ole enää tuettu Windows Server 2003-palvelimilla (24).

Windows Server 2003 Interim mode (välitila) tukee vain Windows Server 2003-ohjauspalvelimia ja Windows NT-varaohjauspalvelimia. Windows 2000 Server ei ole tässä tuettuna. Tämä tila on tarkoitettu tilanteeseen, jossa ollaan tekemässä migraatiota suoraan Windows NT-ympäristöstä suoraan Windows Server 2003-ympäristöön eikä käytössä ole yhtään Windows 2000-ohjauspalvelinta. Ominaisuuksiltaan tämä välitila on samanlainen kuin sekatila. Välitilan käyttäminen on mahdollista ainoastaan toimialueen ensimmäisessä Windows Server 2003:ksi päivitetyssä ohjauspalvelimessa. Microsoft suosittelee, että varaohjauskoneesta tehdään varmistus ennen sen päivittämistä. Näiden päivitysten jälkeen on suositeltavaa nostaa toimialueen ja metsän toimintatasoa, jotta saadaan hyödynnettyä uusia ominaisuuksia(6, s. 145).

Windows Server 2003 mode (taso) tukee ainoastaan Windows Server 2003-ohjauspalvelimia. Windows NT-ja Windows 2000 Server-ohjauspalvelimet eivät ole tuettuja. Tässä tilassa voidaan käyttää kaikkia Active Directory uusia ominaisuuksia. Käyttäjä- ja tietokonetilien lisäämiseen toimialueelle voidaan käyttää redirusr- ja redircmp-työkaluja. Näiden avulla saadaan objektit syntymään tiettyyn haluttuun OU-ryhmään (6, s. 145;24). Lisätietoja näistä työkaluista löytyy Microsoftin artikkelista kb324949. Taulukkoon 4 on kerätty toimialueen toiminnallisuustasot ja niissä tuetut käyttöjärjestelmät.

Taulukko 4 Windows Server 200:n3 toimialueen toiminnallisuustasot

Toimialueen toiminnallisuustasot	Tuetut ohjauspalvelin käyttöjärjestelmät
Windows 2000 mixed	Windows NT 4.0 Windows 2000 Windows Server 2003
Windows 2000 native	Windows 2000 Windows Server 2003
Windows Server 2003 interim	Windows NT 4.0 Windows Server 2003
Windows Server 2003	Windows Server 2003

4.6.2 Metsän toimitasot

Active Directory-metsällä on kolme eri toiminnallisuustasoa Windows Server 2003-ympäristössä. Ne ovat Windows 2000 (oletus), Windows Server 2003 intermin (välitila, jos päivitetään Windows NT-toimialue) ja Windows Server 2003. Oletuksena metsän toimivat Windows 2000-toimitasolla, mutta ne voidaan korottaa Windows Server 2003-toimitasolle. Ennen korottamista tulee varmistua, että kaikki toimialueet ovat Windows 2000 native- tai Windows Server 2003-tasolla. Metsän toimitason korottaminen on peruuttamaton toimenpide, joten on syytä selvittää huolella muutosten vaikutus ja tuettavuus.

Metsän toiminnallisuustasojen käyttöjärjestelmä versiot ovat samat kuin toimialueiden toiminnallisuustasoissa, paitsi että Windows 2000 Native puuttuu, joten metsän toiminnakkisuustasoja on vain kolme. Toiminnallisuuksissa on joitakin eroja. Windows 2000-tasolla käyttöjärjestelmä toimii oletusominaisuuksilla, mutta nostettaessa Windows Server 2003 interim-tasolle, saadaan 13 lisäattribuuttia yleiseen hakemistoon. Myös hakemiston toistaminen tehostuu, koska saadaan käyttöön LVR-replikointi (Linked-Value replication). Se tarkoittaa, että muutosten replikointi tapahtuu objektien attribuuttitasolla. Esimerkiksi jos käyttäjäryhmästä poistetaan yksi käyttäjä, ei tarvitse toistaa koko käyttäjäryhmää uudestaan vaan ainoastaan tieto käyttäjän poistamisesta.

Tällaisella yoistamisella pystytään välttämään tehtyjen muutosten katoaminen tilanteessa, jossa kaksi ohjauspalvelinta tekee hakemistoon muutoksia yhtä aikaa (23;25).

Metsän ollessa Windows Server 2003-tilassa. Se toimii kaikkein edistyneimmillä ominaisuuksilla. Tällä toiminnallisuustasolla se pystyy myös muuttamaan hakemiston kaavaa (Schema) ja rakentamaan luottosuhteita metsien välille (25). Taulukkoon 5 on kerätty metsän toiminnallisuustasot ja niissä tuetut käyttöjärjestelmät.

Taulukko 5. Windows Server 2000-metsän toiminnallisuustasot.

Metsän toiminnallisuustasot	Tuetut ohjauspalvelin käyttöjärjestelmät
Windows 2000	Windows NT 4.0 Windows 2000 Windows Server 2003
Windows Server 2003 interim	Windows NT 4.0 Windows Server 2003
Windows Server 2003	Windows Server 2003

4.7 Ohjauspalvelinten roolit

Active Directory on suunniteltu siten, että ohjauspalvelimet ovat kaikki tasaveroisia Tämä tarkoittaa, että kaikilla ohjauskoneilla on oikeus kirjoittaa Active Directory-tietokantaan. Tällainen järjestelmä toimii erittäin hyvin suurimpaan osaa eri tietokantaoperaatioita. On kuitenkin olemassa sellaisia operaatioita, joiden tekemiseen on oikeudet vain yhdellä ohjauskoneella. Ohjauskoneita, jotka suorittavat tällaisia erityistehtäviä, kutsutaan toimintopalvelimiksi (operation master). Jokaisella toimintopalvelimella on oma Flexible Single Master Operations (FSMO)-rooli. Rooleja on yhtensä viisi erilaista (26):

- Schema master
- Domain naming master

- RID master
- PDC emulator
- Infrastructure master.

Ensimmäiset kaksi roolia, schema master ja domain naming master, ovat aina metsäkohtaisia rooleja. Tämä tarkoittaa, että jokaisessa metsässä täytyy aina löytyä kyseiset roolit omaava ohjauspalvelin. Muut kolme roolia on toimialuekohtaisia, mikä tarkoittaa, että jokaisesta metsässä olevasta toimialueesta täytyy löytyä yksi kutakin roolia hoitava ohjauspalvelin. Kun Active Directory asennetaan ja luodaan ensimmäinen ohjauspalvelin metsään, se saa kaikki kyseiset viisi roolia automaattisesti. Ja kun luodaan samaan metsään uusi toimialue ja sille ensimmäinen ohjauspalvelin, se saa aina kolme jälkimmäistä roolia. Kun kyseiseen metsään ja toimialueeseen luodaan lisää ohjauskoneita, voidaan näitä rooleja siirtää niille. Roolien sijoittamisesta kerrotaan lisää hiukan myöhemmin (26).

Schema master

Schema master-roolin omaava ohjauspalvelin on ainoa, jolla on kirjoitusoikeudet Active Directoryn rakenteeseen eli kaavaan. Jos halutaan tehdä muutoksia tähän kaavaan, täytyy järjestelmän ylläpitäjän (tunnuksen pitää kuulua ryhmään Schema Admins Security group) kirjautua kyseisen roolin omaavalle palvelimelle. Jos kaavaa yritetään muuttaa joltakin toiselta ohjauspalvelimelta, se epäonnistuu. Kaavaan tehdyt muutokset replikoituvat toisille ohjauspalvelimille kyseisen metsän alueella (26).

Domain naming master

Domain naming master-roolin omaavalta palvelimelta tehdään muutokset, kun halutaan lisätä tai poistaa toimialueita kyseisestä metsästä. Jos muutoksia yritetään tehdä ilman yhteyttä domain naming master-palvelimeen, ne tulevat epäonnistumaan. Roolin muita tehtäviä ovat mm. viittaukset ulkoisiin hakemistoihin ja huolehtiminen siitä, että toimialueen nimet ovat yksilöllisiä (26).

RID master

RID master-roolin *(Relative Identifier)* omaavan palvelimen tehtävä on varata suhteellisia suojaustunnisteita (RID) kaikille ohjauspalvelimille ja siten varmistaa, että kaikilla suojauspääobjekteilla on yksilöllinen tunnus (26).

PDC emulator

Primary Domain Controller (PDC) emulator–roolin omaava palvelin käsittelee kaikki replikointipyynnöt, jotka tulevat Windows NT 4.0–varaohjauspalvelimilta, sekä salasanapäivitykset työasemilta (Windows 9x- ja NT–työasemat), joissa ei ole Active Directory-asiakasohjelmistoa asennettuna. Toimialueen Windows NT4-BDC *(Backup Domain Controller)* -koneet näkevät kyseisen emulaattoriroolin omaavan palvelimen PDC-palvelimena ja replikoivat sen kanssa. Se myös ylläpitää päiväystä ja kellonaikaa toimialuelaajuisesti ja toimii samalla toimialueen pääselaimena *(domain master Browser)* eli vastaa omalta osaltaan toimialueen tietokoneluettelon luonnista. Emulaattorin tehtäviin kuuluu myös replikoida muuttuneet salasanapäivitykset asiakastietokoneilleen (26).

Infrastructure master

Infrastructure master-roolin vastuualueeseen kuuluu ylläpitää luetteloa toimialueen ulkopuolisista suojauspääobjekteista. Infrastructure master päivittää objektit paikallisesti ja replikoi muutokset muille ohjauskoneilla saattaen ne ajan tasalle. Eli jos Infrastructure master löytää viittauksen objektiin, jolle ei löydy vastinetta toimialueen hakemistosta *(Global Catalog)* ja objekti kuuluu kyseiseen toimialueeseen, replikoi se objektin viittauksen sisältämän GUID -tunnuksen ja mahdollisesti myös SID- tunnuksen muiden toimialueiden Infrastructure master-roolin omaaville palvelimille (26).

4.8 Ohjauspalvelinroolien sijoittaminen

Ohjauspalvelimien roolien sijoittelu on erittäin tärkeää pitkän aikavälin toimintakunnon ylläpitämiseksi masterroolien haltijoiden ongelmien välttämiseksi. Roolien väärä sijoitte saattaa aiheuttaa sen, ettei uusia objekteja, kuten käyttäjiä, ryhmiä tai tietokonetilejä, voida enää lisätä. Toimialueiden lisääminen ja poistaminen sekä Active Directoryn kaavan muutokset saattavat epäonnistua.

Roolin voidaan sijoittaa mille tahansa ohjauspalvelimella, mutta niiden sijoittamiseen kannattaa todella perehtyä, jotta niiden hallinnoimiseen käytetty aika voitaisiin minimoida ja Active Directoryn toiminta voitaisiin mahdollisimman hyvin taata. Mikäli jotakin tiettyä roolia ylläpitävä palvelin vikaantuu, on se ohjeita noudattamalla mahdollista saada yksinkertaisesti ja nopeasti takaisin toimintakuntoon. Suunnittelussa on otettava huomioon käytettävyys ja kuormituksen tasaaminen. Roolin sijoittamisessa huomioitavia asioita ovat (27):

- Ohjauspalvelimia kannattaa asentaa jokaiselle toimialueelle vähintäänkin kaksi. Se antaa lisää vikasietoisuutta. Silloin kumpikin näistä käsittelee Active Directoryn päivityksiä ja PDC emulator-, RID master-, sekä Infrastructure master-roolit voivat sijaita missä vain näistä ohjauspalvelimista.

- Kun toimialueella on useampi kuin yksi ohjauspalvelin, alkaa replikointi. Yleisen luettelon eli Global Catalogin tulisi sijaita jokaisella ohjauskoneella, paitsi sillä jolla on Infrastructure master-rooli.

- Metsän laajuisten roolien Schema master ja Domain naming master, tulisi sijaita metsän juuritoimialueella sijaitsevalla ohjauspalvelimella. Suorituskyky syistä näiden kyseisten roolien olisi hyvä sijaita samalla palvelimella.

- Metsän laajuisten roolien, Schema master ja Domain naming master tulisi sijaita sellaisella ohjauspalvelimella, jossa sijaitsee myös yleinen luettelo (GC).

Domain naming master-roolin ja yleisen luettelon ollessa samalla palvelimella on toimialueen nimien tarkistus nopeampaa.

- Toimialueen laajuiset roolit (RID master, PDC emulator ja Infrastructure master) voivat sijaita samalla ohjauspalvelimella.

- Yleistä luetteloa (GC) ei tulisi sijoittaa samalle palvelimelle, johon nämä edellä mainitut toimialueen laajuiset roolit on sijoitettu.

- Kun sijoitetaan toimialueen laajuiset roolit samalla palvelimella, tulisi siihen valita toimialueen suorituskyvyltään tehokkain ohjauspalvelin.

- Mikäli toimialueelle kirjautumisten käsittely aiheuttaa liikaa kuormitusta ohjauspalvelimella, tulisi toimialueelle lisätä ohjauspalvelimia ja tarvittaessa siirtää RID master ja/tai PDC emulator uudelle ohjauspalvelimelle.

On hyvä huomioida roolien omaavien ohjauspalvelimien käytettävyydessä, että Schema masterin, Domain naming masterin ja Infrastructure masterin lyhytaikainen poissaolo verkosta ei vaikuta Active Directoryyn. RID master voi olla myös verkosta pois muutaman tunnin, kunhan tällä välin ei tehdä useisiin satoihin objekteihin kohdistuvia muutoksia kyseisellä toimialueella. PDC emulaattori on rooli, joka pitäisi olla koko ajan verkossa saatavilla. Mikäli kyseinen palvelin joudutaan sammuttamaan, tulisi rooli siirtää siksi aikaa toiselle ohjauspalvelimelle (27).

4.9 Yleinen luettelopalvelin

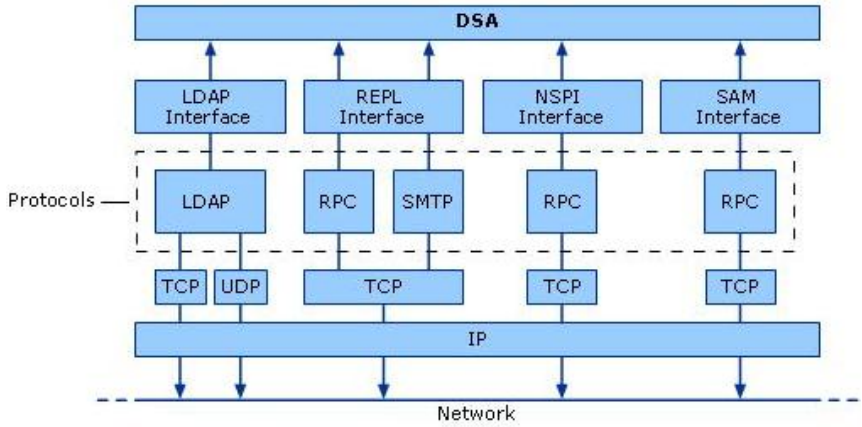
Yleinen luettelopalvelin eli Global Catalog (GC) on ohjauspalvelimen valinnainen palvelu. Palvelun tehtävänä on tallentaa metsän kaikkien objektien ne attribuutit (tiedot), jotka kaavassa on määritelty yleiseen luetteloon tallennettaviksi. Tämän luettelon luominen tapahtuu täysin automaattisesti replikointien yhteydessä. Yleinen luettelo replikoidaan muille saman palvelun omaaville ohjauspalvelimille normaalin replikointikäytännön mukana. Yleistä luetteloa käytetään muun muassa kun tehdään

hakuja koko Active Directoryyn tai käyttäjien kirjautuessa toimialueille, jolloin universaalienryhmien jäsenyydet ja kirjautumisnimi tarkistetaan yleisestä luettelosta. Jos tehdään muutoksia kirjautumisnimiin, tarvitaan yhteys yleiseen luetteloon, johon muutokset tallennetaan (28).

Oletuksena yleinen luettelo ylläpidetään vain ja ainoastaan metsään ensimmäiseksi luodulla ohjauspalvelimella. Mikä tahansa ohjauspalvelin voi ylläpitää yleistä luetteloa ja on suositeltavaa asentaa se lähes kaikkiin ohjauspalvelimiin. Mitä enemmän toimialueella on yleistä luetteloa ylläpitäviä palvelimia, sitä enemmän tapahtuu replikointia, mutta käyttäjien tekemät kyselyt nopeutuvat. On muistettava kuitenkin, ettei ole suositeltavaa pitää sitä kuitenkaan Infrastructure master-roolin kanssa samalla palvelimella). Jokaisessa toimipaikassa tulisi ainakin yhden palvelin ylläpitää yleistä luetteloa. Yleistä luetteloa ylläpitävät palvelimet tallentavat tietonsa DNS:ään. Tällöin tietyn toimipaikan koneet osaavat käyttää toimipaikan paikallista yleistä luettelopalvelinta. Tällöin verkkoliikennettä saadaan rajoitettua toimipaikkojen välillä. Mikäli jostakin syystä on toimipaikkoja, joissa ei sijaitse yleistä luettelopalvelinta, tulisi niille toimipaikoille tallentaa universaalit ryhmäoikeudet välimuistiin *(Enable Universal Groub Membership Caching)* (28).

Mikäli toimialueen toimitaso on Windows Server 2003, niin replikointi tehokkaampaa, koska silloin esimerkiksi ryhmien jäsenyyksistä tarvitsee replikoida vain muuttuneet objektit ja attribuutit.

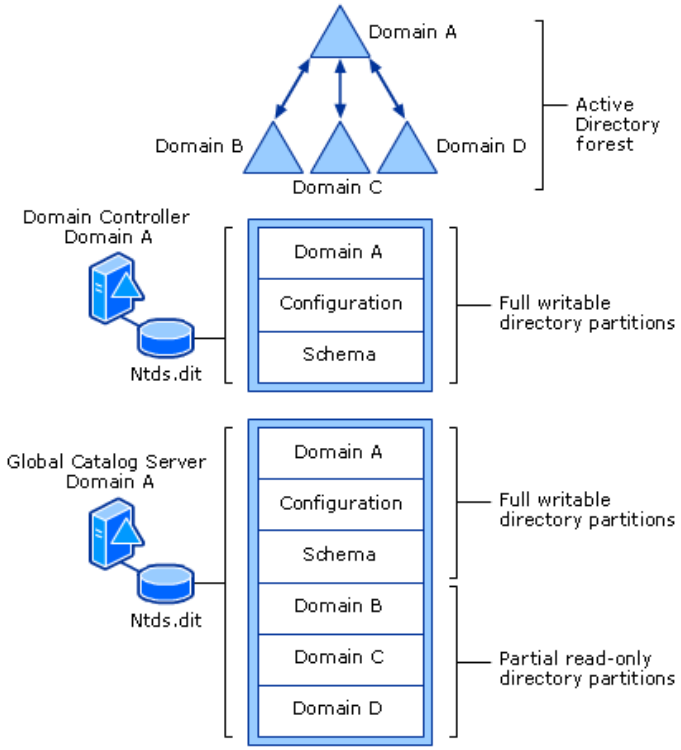
Kuvassa 7 diagrammi esittää Active Directoryn neljää eri rajapintaa, joissa kuvataan yleisen luettelon käyttämät protokollat niiden käyttämien sovellusten mukaan. Kyseiset protokollat ja rajapinnat ovat samat kaikissa toimialueen ohjauspalvelimissa (28).



Kuva 7. Yleisen luettelon käyttämät protokollat (28).

Yleisen luettelon tiedot ovat samat kaikilla ohjauspalvelimilla. Ntds.dit-tietokanta tallettaa objektien attribuutit yhteen tiedostoon. Toimialueen ohjauskoneessa, joka ei ole yleinen luettelopalvelin Ntds.dit-tiedosto sisältää toimialueensa kaikkien objektien tiedot ja lisäksi kirjoittaa kokoonpanon ja rakenteen hakemisto-osiot toimialueensa hakemisto-osioon.

Kuvassa 8 esitetään yleisen luettelopalvelimen fyysinen kuvaus metsän laajuisesta hajautuksesta.



Kuva 8. Yleisen luettelopalvelimen fyysinen rakenne.

4.10 Luottosuhteet

Luottosuhteet *(Trust Relationships)* tarkoittavat, että metsä tai sen toimialue luottaa johonkin toiseen metsään tai toimialueeseen. Tämä tarkoittaa sitä, että ne sallivat toiselta toimialueelta tai toisesta metsästä tulevat valtuutuspyynnöt. Niillä on pääsy toisiensa sisäisiin resursseihin. Puurakenne tarkoittaa hierarkkista toimialuerakennetta, jossa ylemmän tason toimialueen ja alemman tason välillä on luottosuhde. Active Directoryn-toimialueilla luottosuhteet muodostetaan automaattisesti toimialuepuun sisällä ja välille. Tällaista luottosuhdetta kutsutaan kaksisuuntaiseksi siirtyväksi Kerberos-luottosuhteeksi. Tällaisessa metsässä kaikki toimialueet luottavat toisiinsa ja muodostavat Kerberos-valtuutusalueen (14, s. 723–784).

Tällaisten automaattisen luottosuhteiden lisäksi voidaan manuaalisesti rakentaa luottosuhteita Windows NT4-toimialueisiin tai Windows 2000 - Active Directoryyn.

Lisäksi Active Directoryssä voidaan käsin luoda yksi- tai kaksisuuntaisia luottosuhteita, jotka ovat siirtyviä tai ei siirtyviä. Kaksisuuntaisessa luottosuhteessa luottamus pelaa kumpaankin suuntaa eli luotetaan vastakkaisen puolen suojausobjekteihin. Jos Active Directory tai Windows NT-toimialue luo yksisuuntaisen luottosuhteen, toimii se esimerkiksi siten, että Active Directoryn käyttäjät pystyvät kirjautumaan NT-toimialueelle, mutteivat toisin päin. Luottosuhteiden sopineiden toimialueiden välillä tieto kulkee suojatun kanavan kautta (14, s. 723–784).

4.11 Ryhmäkäytännöt

Ryhmäkäytännöillä tarkoitetaan järjestelmän kokoonpanoasetuksia, jotka voidaan liittää Active Directoryn objekteihin, kuten esimerkiksi organisaatioyksiköihin. Ryhmäkäytännöt on otettu käyttöön Microsoftin Windows 2000- käyttöjärjestelmässä. Ryhmäkäytännöt ovat mekanismi, joilla hallitaan Active Directory-toimialueita. Ryhmäkäytännöillä voidaan asettaan käyttäjille erilaisia ympäristöasetuksia, salasanakäytäntöjä, ohjelmien jakeluasetuksia, tulostimia, selainasetuksia sekä paljon muita asetuksia. Yksittäisten koneiden käytäntöjä kutsutaan paikallisiksi käytännöiksi (Local Policy), ja ne tallennetaan vain kyseiseen paikalliseen koneeseen. Muut ryhmäkäytännöt linkitetään Active Directory-hakemistopalvelun objekteiksi (Group Policy Objects, GPO) (6, s. 85–88).

Ryhmäkäytännöt ovat perusteiltaan samanlaiset Windows Server 2003:ssa kuin oli Windows 2000:ssa, mutta niiden hallitsemista ja toteuttamista on helpotettu monin tavoin. Hallintakonsolipuolelle on tullut uudistuksena Group Policy-laajennus, joka on tuonut samalla kaksi uutta hallintakonsolia (Resultant Set of Policy ja Group Policy Management Console). Muutoksien myötä on tullut esimerkiksi WMI-suodatus ja metsien välinen tuki. Laajennus on tuonut yli 150 uutta tai muutettua ryhmäkäytäntöä. Myös kokonaan uusia ryhminä on tullut muun muassa Terminal Services, Software Restriction Policies jne.

Windows NT 4.0:ssa käytännöt määritellään System Policy Editor-työkalulla. Se on NT:hen rakennettu oma käytäntöjen hallintaan tarkoitettu työkalu (Poledit.exe) (6, s. 85–88).

Toimialueilla on lisäksi olemassa oletusryhmäkäytäntöjä sekä ohjauspalvelinten ryhmäkäytäntöjä. Ryhmäkäytännöt voidaan määritellä lisäksi toimialueen organisaatioyksiköihin ja toimipaikkoihin.

Ryhmäkäytännöt tallennetaan GPO-objekteiksi. Nämä objektit ovat käytäntöjen ja niiden asetusten säilytyspaikkoja. Näitä GPO-objekteja voidaan linkittää vapaasti yhtä aikaa useampaan toimipaikkaan, toimialueeseen tai organisaatioyksikköön. Niitä voidaan myös linkittää yhteen ja samaan aktiivihakemiston osaan (6, s. 85–88).

Ryhmäkäytännöt ovat periytyviä isä-lapsisuhteen mukaisesti ylimmältä tasolta alaspäin kuvan 9 mukaisesti. Periytymisen kautta isäsäilölle asetetut GPO-objektit periytyvät lapsisäilöön. Asettaessa ryhmäkäytännöt toimialueelle, periytyy sen tämän säännön mukaan organisaatioyksiköille ja sen alla oleviin lapsiorganisaatioyksiköihin. Tämä periytyminen voidaan myös estää määrittelemällä lapsisäilöön asetus, joka eroaa isäsäilön asetuksesta. Myös ohittaminen voidaan asetuksilla estää, niin halutessa (6, s. 85–88).

Kuva 9. GPO-objektien periytymisen järjestys

Näiden erilaisten ryhmäkäytäntöjen soveltamisen järjestys eli käyttöönotto on järjestyksenvalvojien tärkeää tiedostaa. Ryhmäkäytäntöjä sovelletaan käyttäjille ja tietokoneille taulukon 6 mukaisesti. Ensimmäiseksi ajetaan paikalliset käyttäjä- ja

tietokonekäytännöt (Windows NT 4.0-käytännöt-Ntconfig.pol), joiden prosessointi-järjestyksen on määritellyt järjestelmänvalvoja, kuten muidenkin käytäntöjen kohdalla. Alimmainen GPO-linkki käsitellään viimeisenä, ja täten sillä on korkein vaikutus. Seuraavaksi ajetaan palvelinjoukon käytännöt siten, että kaikki GPO-linkitykset, jotka on tehty toimipisteelle, missä kyseinen tietokone sijaitsee. Tämän jälkeen ajetaan toimialueeseen linkitetyt käytännöt. Viimeisenä linkitetään organisaatioyksikön ryhmäkäytännöt ja sen alaryhmien ryhmäkäytännöt, jollei periytymistä ole estetty.

Taulukko 6. Ryhmäkäytäntöjen prosessointi järjestys (LSD-O).

Hyvänä muistisääntönä toimii yleisesti käytetty lyhenne LSD-O. Ryhmäkäytännöt käsitellään järjestelmän käynnistyessä ja sammutuksessa sekä käyttäjän kirjautuessa järjestelmään tai järjestelmästä ulos. Lisäksi ne ovat dynaamisia, eli ne käsitellään oletuksena 90 minuutin välein (+ 0…30 min.) ja ohjauspalvelimissa viiden minuutin välein. Paikallisesti muutetut käytännöt voivat olla voimassa korkeintaan kaksi tuntia. Tämän jälkeen toimialueen käytännöt otetaan jälleen käyttöön (29).

5 Windows Server 2003:n ominaisuudet

Windows Server 2003 sisältää lukuisan joukon uusia ominaisuuksia verrattuna aikaisempiin käyttöjärjestelmiin. Tietyt perustoiminnot ovat samoja kuin vanhemmissa Windows-versioissa, mutta niitä on voitu kehittää lisää. Tarkoituksena on esittää muutamia ominaisuuksia, joista Yritys Oy hyötyy. Pääpaino näissä on tietoturvalla. Seuraavaksi esiteltyjen ominaisuuksien lisäksi haluan mainita myös muutaman muun oleellisen syyn, miksi Yritys Oy päätti lähteä päivittämään ja näin ollen kehittämään

omaa verkkoinfrastruktuuriaan. Tällaisia syitä ovat uudet etäkäyttömahdollisuudet (mobiilikäyttäjät), parannettu laitteiston tuki ja keskitetympi hallinta.

5.1 Turvallisemmat käyttöoikeudet

Windows Server 2003:ssa on kansioiden ja tiedostojen oletuskäyttöoikeuksia kiristetty huomattavasti verrattuna vanhempiin Windows NT 4.0- ja Windows 2000-käyttöjärjestelmiin. Vanhemmissa käyttöjärjestelmissä luotaessa levyn juureen tiedoston tai kansion, sen Everyone-käyttöoikeusryhmälle sai NTFS-käyttöoikeuksiin ja myös jako-oikeuksiin täydet oikeudet. Jos näitä asetuksia ei muutettu, perivät kansioiden sisältämät tiedostot ja alikansiot kansion NTFS-oikeudet. Jokainen, joka pääsi paikallisesti tai verkon kautta lukemaan palvelimen levyä, sai täydet oikeudet kaikkiin kansion sisältämiin kansioihin ja tiedostoihin. Suositusten mukaisesti näitä kansio- ja tiedostokohtaisia oikeuksia tulisi määritellä tarvittaessa tiukemmiksi käyttämällä NTFS -oikeuksia (30).

Windows Server 2003:ssa tämä asia on muutettu siten, että oletuksena Everyone-ryhmällä ei ole mitään oikeuksia minkään levyjärjestelmän juureen. Järjestelmänvalvoja tunnuksella on vain täydet oikeudet näihin osioihin. 2003:ssa levyn juuressa olevien kansioiden oikeudet eivät myöskään periydy alikansioille. Kansioiden oletus jako-oikeuksiin on myös tehty muutoksia siten, että Everyone-ryhmällä on enää vain lukuoikeudet jaettuihin kansioihin (30).

Windows Server 2003 antaa User-ryhmälle oikeudet lukea ja suorittaa tiedostoja sekä lukea ja listata hakemiston sisältöä. Näin vältytään tilanteelta, jossa kenelläkään ei ole mitään oikeuksia. Users-ryhmälle annetut oikeudet eivät aiheuta läheskään yhtä suurta riskiä kuin Everyone-ryhmälle, koska ryhmän jäsenet eivät ole yhtä anonyymeja, koska Users-ryhmä saa valtuutukset Active Directorystä, toisin kuin Everyone-ryhmä (30).

Windows Server 2003:ssa lisäksi Everyone-ryhmä toteutetaan eri tavalla, kuin NT 4.0:ssa. Se ei nimittäin pidä sisällään enää Anonymous Logon-ryhmää. Näin ollen, jos ulkopuolelta otetaan anonyymisti yhteyttä, ei käyttäjä saa Everyone-ryhmälle annettuja

oikeuksia, vaan paljon heikommat oikeudet, joilla ei oikeastaan pysty tekemään paljoakaan (30).

5.2 Local Service- ja Network Service -palvelutunnukset

Palvelimen taustalle käynnistettyjen järjestelmäpalvelujen suorittamiseksi tarvitaan järjestelmän palvelutilejä. Vanhemmissa palvelinjärjestelmissä näitä ajettiin monesti paikallisen järjestelmänvalvojan tilillä, joka antoi ajettaville palveluille rajoittamattomat oikeudet. Mikäli esimerkiksi virus tai verkkomato pääsisi osaksi järjestelmän palveluja, on sillä täydet oikeudet ylikirjoittaa ja tuhota tiedostoja ja sen leviäminen tapahtuu huomattavasti nopeammin. Tästä johtuen ei ole järkevää antaa palveluille kyseisen laisia oikeuksia, jos ei ole pakko (6, s. 185–191).

Windows Server 2003:ssa on luotu kaksi erillistä palvelutunnusta järjestelmäpalveluiden ajamiseksi ilman järjestelmänvalvoja oikeuksia. Palvelutunnukset ovat nimeltään Local Service ja Network Service. Näiden käyttöä suositellaan aina kun mahdollista. Lisäksi jos salasana-asetukset vaativat salasanan vaihtamisen tietyn väliajoin ja joitakin palveluita ajetaan tällä tunnuksella. Aiheuttaa salasanan vaihtuminen, sen ettei palveluita voida enää ajaa, ennen kuin niiden salasanat on päivitetty. Myös tästä syystä niiden käyttöä tulisi välttää (6, s. 185–191).

5.3 Automaattiset päivitykset

Windows Server 2003:ssa on sisään rakennettu automaattinen päivitystoiminto, joka on mahdollista ottaa käyttöön. Windows NT:ssä kaikki tietoturvapäivitykset jouduttiin erikseen etsimään verkosta, lataamaan ja asentamaan. Tämä aiheutti sen, ettei kaikkia päivityksiä aina ollut asennettu. 2003-palvelimessa päivitysten lataaminen perustuu niin kutsuttuun Backround Intelligent Transfer Servicen (BITS) ominaisuuksiin. Kyseinen palvelu asettaa normaaleille verkkotoiminnoille etusijan ja lataa päivitykset vasta kun verkkoyhteys ei ole kuormitettuna. Tälle BITS-palvelulle voidaan asettaa kolme eri tilaa, jotka ovat tuttuja vähänkään tietokoneen päivitysten kanssa tekemissä olleille.

Ensimmäisessä toimitilassa palvelin ainoastaan ilmoittaa saatavilla olevista päivityksistä, mutta ei lataa tai asenna niitä ilman järjestyksenvalvojan erillistä lupaa. Toisessa toimitilassa palvelin lataa päivityksen koneelle valmiiksi, mutta ei kuitenkaan asenna niitä ennen kuin järjestelmänvalvoja on erikseen asennuksen hyväksynyt hetkellä, jolloin se ei haittaa palvelimen käyttöä. Kolmannessa ja viimeisessä toimitilassa palvelin lataa automaattisesti asennettavat päivitykset koneella ja asentaa ne järjestelmänvalvojan erikseen määrittelemässä asennusikkunassa.

Active Directoryssä näiden automaattisten päivitysten hoitaminen voidaan hoitaa vieläkin helpommin ryhmäkäytäntöjen ja Microsoftin Windows Software Update Services *(WSUS)*-palvelimen avulla, joka sijaitsee yrityksen omassa sisäverkossa. Rysäkäytännöillä määritellään tietokoneille niiden päivityspalvelimeksi yrityksen WSUS-palvelin, joka keskitetysti hakee päivityksen Microsoftin päivityspalvelusta. WSUS-palvelimeen on asennettava IIS-palvelu, sekä Microsoft SQL Server Express. WSUS:ssa tietokoneet ja palvelimet tulisi määritellä järkeviin ryhmiin, jotta saataisiin rakennettua Microsoftin suosittelemat testikoneet, joihin päivitykset asennettaisiin ensiksi testausta varten. Muutaman päivän viiveellä ne asennettaisiin myös muihin koneisiin. WSUS:sta saadaan myös tulostettua raportti, josta nähdään koneiden päivitysten tila ja tarvittaessa päivitysongelmiin pystytään reagoimaan.

6 Yritys Oy:n Active Directory

Seuraavaksi esittelen käyttöön otetun Active Directoryn rakenteen määritykset, joita noudatetaan koko toimialuemetsän alueella.

Seuraavia lyhenteitä käytetään kuvastamaan tekstissä käytettäviä rooleja ja tehtäviä:

YIT tarkoittaa ”Yritys IT”, joka tarkoittaa Yritys Oy:n keskitettyä IT organisaatiota.

YITCS tarkoittaa ”Yritys IT client support”, jolla tarkoitetaan Yritys Oy:n työasematukitiimiä, joka antaa tukipalveluja toimipaikkojen

järjestelmänvalvojille ja muille IT-tukihenkilöille Yritys Oy:n organisaatiossa.

YITHC tarkoittaa ”Yritys IT hosting center”, jolla tarkoitetaan tila- ja infrastruktuuripalveluja, joita tarjotaan keskitetystä palvelin huoneesta.

RHS tarkoittaa ”Regional Hub Site”, jolla tarkoitetaan kolmea alueellista keskustoimipaikkaa (yksi Euroopassa, yksi Aasiassa ja yksi Amerikassa).

6.1 Nimeämiskäytännöt

Tässä kuvatut nimeämiskäytännöt otettiin vaiheittain käyttöön. Toimialueiden OU-rakenteen ja järjestelmänvalvojien tilien liittyvät käytännöt otettiin käyttöön heti juuritoimialueen luonnin jälkeen. Käyttäjä- ja tietokonetilien sekä muun muassa verkkotulostimien osalta siihen siirryttiin konsolidointivaiheessa.

Toimialueet

Taulukossa 7 on kuvattu toimialueiden FGDN ja NetBios nimet migraatiovaiheen jälkeen. Konsolidointivaiheessa kolme viimeistä toimialuetta yhdistettiin juuritoimialueen alle. Kun kaikki niiden alla olevat resurssit ja tilit on siirretty juuritoimialueelle, voidaan ne ajaa alas.

Taulukko 7. Toimialueiden nimistandardit migraatiovaiheen jälkeen.

Domain	FQDN	NetBIOS name
Forest root domain	yritys.net	
Europe regional domain	eu.yritys.net	netcals
America regional domain	am.yritys.net	netcalsna
Asia Pasific regional domain	ap.yritys.net	netcalsap

Toimipaikka ja OU-rakenne

Toimipaikkojen ja OU-rakenteiden kohdalla nimeämiskäytäntö on yhdenmukainen. Ensimmäiset kaksi kirjainta tulee maakoodin mukaan ja kolme viimeistä kirjainta toimipisteen kaupungin mukaan.
Jos toimipaikka sijaitsee Helsingissä, saadaan maakoodiksi ”FI” ja kolme viimeistä kirjainta kaupungista eli ”HEL”. Näin saadaan kyseiselle toimipaikalle lyhenne ”FIHEL”.

Ryhmät

Erilaiset ryhmien nimistandardit perustuvat kolmesta välilyönnillä erotetusta osasta. Ensimmäinen osan viisi kirjainta tulee toimipaikan mukaan. Toisen osan kaksi kirjainta tulee taulukon 8 mukaisesti, perustuen ryhmän tyyppiin. Viimeisessä osassa kuvataan ryhmän tarkoitus. Ryhmän nimi voisi olla esimerkiksi ”FIHEL GG Marketing”.
Taulukko 8. Erilaiset ryhmät lyhenteet, joita käytetään raportissa

Group type	
DL	Domain Local
GG	Global Group
UG	Universal Group

Käyttäjätunnukset ja tietokoneet

Aikaisemmassa Windows 2000-ympäristöissä käyttäjätunnuksen viisi ensimmäistä kirjainta muodostuvat sukunimestä ja sitä seuraavat kolme kirjainta etunimestä.

Etunimi Sukunimi → sukunetu

AD:n kirjautumisnimi on samaa muotoa kuin käyttäjän sähköpostiosoitekin. Kirjautumisnimi on muotoa ”etunimi.sukunimi@yritys.net”. Jos esiintyy mahdollisia samannimisiä, niiden kohdalla keskelle sijoitetaan toisen nimen ensimmäinen kirjain:

”etunimi.t.sukunimi@yritys.net”. Käyttäjän yleinen nimi ja AD:n näyttämä nimi on muotoa: ”Sukunimi, Etunimi”

Järjestelmänylläpitoon tarkoitetut käyttäjätunnukset eroavat muista kirjautumisnimistä loppuun tulevalla alaviivalla ja s-kirjaimella. Järjestelmän ylläpitäjäntunnus on siis muotoa ”etunimi.sukunimi.s@yritys.net” ja aikaisemmissa Windows versioissa ”sukunetu_s”.

Tietokoneiden nimeämiskäytännöt

Ohjauspalvelimien, jäsenpalvelimien ja työasemien nimeämisessä käytetään myös toimipaikan koodia alussa ja loppuosat sitten erottavat ne toisistaan.

Ohjauspalvelimissa toimipaikka koodin perään lisätään kirjaimet DC *(Domain Controller)* ja loppuosaan juokseva järjestysnumero, joka alkaa 01:stä. Jäsenpalvelimissa nimen loppuosa koostuu kahdesta roolia kuvaavasta kirjaimesta ja juoksevasta järjestysnumerosta alkaen 01:stä. Roolia kuvastavia lyhenteitä ovat esimerkiksi, FP *(File and Print)* ja TS *(Terminal Server).* Työasemissa alku muodostuu toimipaikan mukaan ja sitä seuraa kolme juoksevaa järjestysnumeroa alkaen 001:stä. Loppuun tulee kirjain D tai L, riippuen onko kyseessä pöytäkone vai kannettava.

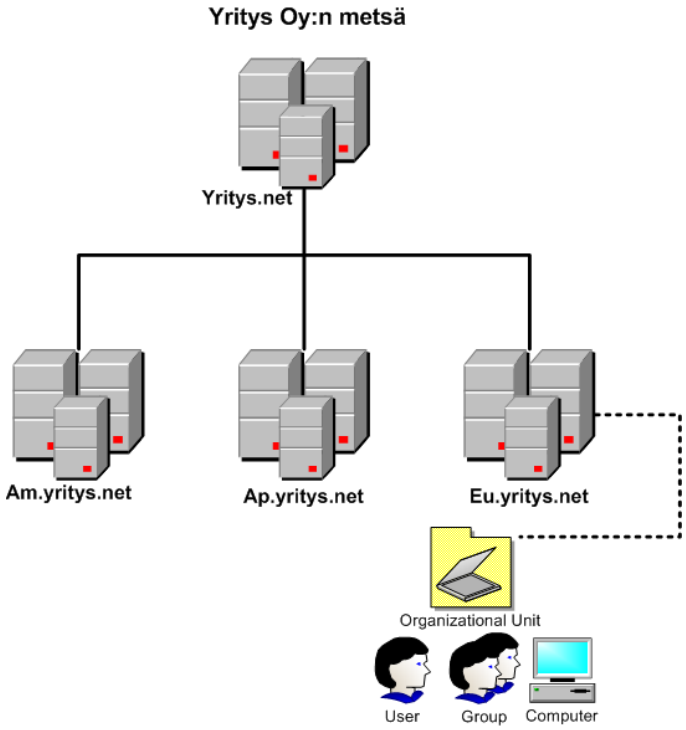
Seuravassa on esimerkit palvelimien ja työasemien nimeämisestä:

ohjauspalvelin (FIHELDC01)
jäsenpalvelin (FIHELFP01)
työasema (FIHEL001D).

6.2 Active Directoryn looginen rakenne

Metsä ja toimialueet

Kuvassa 10 kuvataan Yritys Oy:n toimialue-metsän looginen rakenne projektin ensimmäisen vaiheen jälkeisessä tilanteessa.



Kuva 10. Yritys Oy:n Active Directoryn toimialuemetsän toimialuerakenne

Ensimmäisen vaiheen jälkeen Yritys Oy:n Active Directoryn looginen rakenne käsittää toimialue-metsän, jonka sisällä on neljä eri toimialuetta. Toisen vaiheen jälkeen kaikki alitoimialueet oli siirretty yritys.net-juuritoimialueeseen.

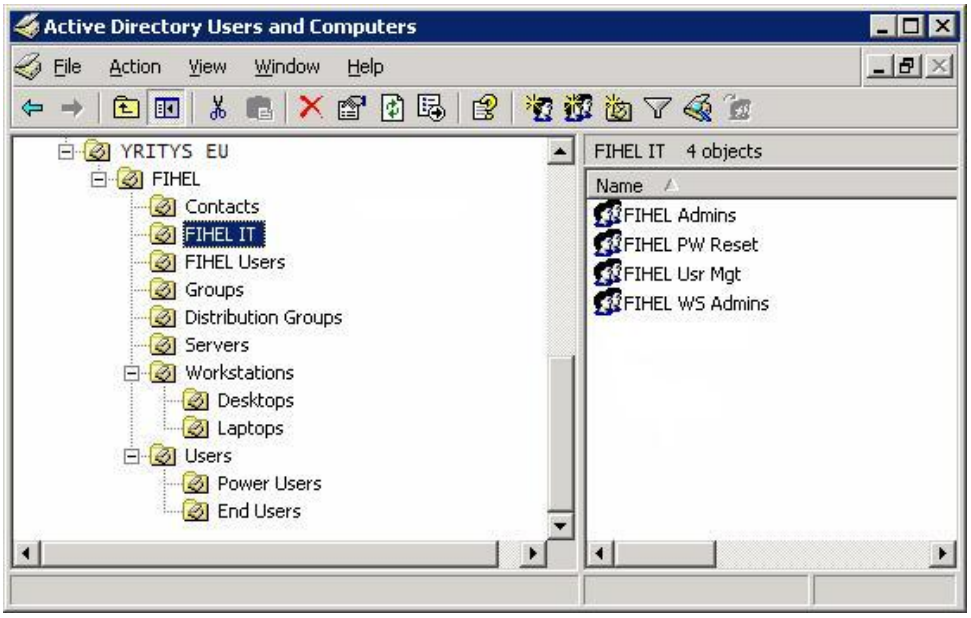
OU-struktuuri

Jokainen toimipaikka on esitetty omana organisaatioyksikkönään. Kaikki organisaatioyksiköt ovat samassa Active Directory toimialueessa yritys.net.

Seuraavanlainen OU-rakenne luodaan jokaisen OU:n alle:

<TOIMIPAIKKA KOODI>
Contacts (OU) [ulkopuoliset edelleen lähetettävät osoitteet, kontaktit]
Distribution groups (OU)
< *TOIMIPAIKKA KOODI* > IT (OU) [sisältää IT järjestelmänvalvoja ryhmät, järjestelmänvalvonta-ja palvelutilit] (salasananvanhenemis- sääntö ei kosketa tätä ryhmää)
<*Toimipaikkakoodi*> Admins [toimipaikan (OU) järjestelmänvalvojat]
< *Toimipaikkakoodi* > WS Admins [työasema järjestelmänvalvojat]
< *Toimipaikkakoodi* > pw reset [salasanan resetointi ja lukittuneiden tilien aukaisu]
< *Toimipaikkakoodi* > usr mgt [käyttäjien ominaisuuksien muuttaminen]
< *TOIMIPAIKKA KOODI* > USERS (OU)
< *Toimipaikkakoodi* >USERS [toimipaikan kaikki käyttäjät]
Users (OU)
Power users (OU)
End users (OU)
Workstations (OU)
Desktops (OU)
Laptops (OU)
Servers (OU) [jäsenpalvelimet]
Groups (OU) [Toimipaikan järjestelmänvalvojat voivat luoda lisä ryhmiä tänne]

Kuvassa 11 esitetään Helsingin toimipaikan OU-rakenne, joka on luotu edellä olevan mallin mukaisesti.



Kuva 11. Helsingin toimipaikan OU-rakenne

AD-attribuutit

Active Directory tietokantaan tallennettiin käyttäjistä oleellisimmat attribuutit. Kunt tämän jälkeen otettiin käyttöön monipuoliset haut, olivat nämä tiedot toiset käyttäjien ja muiden järjestelmien käytettävissä.

Käyttäjien seuraavat attribuutit täytetään:

- näyttönimi
- sukunimi
- etunimi
- puhelinnumero [+maakoodi - aluekoodi-numero]
- sähköpostiosoite
- toimisto= 1 <alue koodi> 2<toimipaikka koodi> (esimerkiksi 1eu2fihel)
- osasto
- yritys.

Lisäksi seuraavia attribuutteja suositellaan lisättäväksi:

- osoite (Maa / alue, kaupunki)
- fax
- matkapuhelinnumero
- titteli.

Office-kenttää käytettiin osoittamaan käyttäjän alueellinen ja toimipaikkasijainti.
Kenttää voidaan käyttää rajaamaan hakuja alueeseen, maahan tai toimipaikkaan perustuen. Yllä luetelluissa kentissä tulee käyttää ainoastaan UK-kirjainmerkkejä yhteensopivuusongelmien välttämiseksi.

6.3 Active Directoryn fyysinen rakenne

IP-osoitteet

Toimipaikkojen IP-osoitteen on esitetty liitteessä 1.

Toimipisteet ja toimipistelinkit

Nykyinen Active Directory-toimipaikkareplikointi rakenne jää pysyväksi. Alueellisten Active Directory-toimipaikkojen välillä on replikointiyhteys yritys.netin alueelliseen keskitettyyn verkkotoimipaikkaan. Alueellisilla keskitetyillä verkkotoimipaikoilla on replikointiyhteys FIDHC-palvelimeen (*Schema- ja Domain naming master).*

Domain Controllerit, Global Catalog palvelimett ja FSMO-roolit

YIT oli vuokrannut palvelinkeskuksen Helsingistä. Sieltä ajettiin juuritoimialueen ohjauspalvelimia ja kaikkia alueellisia ohjauspalvelimia, eu.yritys.net, am.yritys.net ja

ap.yritys.net. Lapsitoimialueiden ohjauspalvelimia ei enää tarvita projektin toisen vaiheen jälkeen ja ne ajettiin alas.

Kukin alueellinen toimipaikka isännöi kahta yritys.netin ja yhtä kyseisen alueen ohjauspalvelinta. Alueellisia ohjauspalvelimia ajettiin niin kauan kuin palvelut alueelliselta ohjauspalvelimelta olivat tarpeellisia.

Paikalliset järjestelmänvalvojat eivät saaneet kirjautua suoraan ohjauspalvelimille. Hätätilanteita varten toimipaikkojen järjestelmänvalvojille luotiin erilliset tietojen palautustilit *(disaster recovery accounts)*, joilla he onnistuivat kirjautumaan ohjauspalvelimille. Tällaisia tilanteita ovat esimerkiksi, kun YIT ei saanut yhteyttä palvelimeen tai verkkokortti aiheutti ongelmia.

Järjestelmän katastrofitilannetta varten ohjauspalvelimien mukana oli toimitettu valmiiksi konfiguroidut Windows Server 2003:n palautus-CD-levyt. Näillä CD-levyillä paikallinen järjestelmänvalvoja sai palvelimen takaisin yrityksen verkkoon ja YIT:in tehtäväksi jäi loppu palauttamisprosessi. Jokaisen toimialueen Active Directory tietokannasta otetaan varmuuskopio YITHC:ssä sijaitsevista ohjauspalvelimista. Varmuuskopiointiprosessista vastasi YIT. Varmuuskopiointiprosessi on kuvattu erillisessä dokumentissa, jota ei ole sisällytetty tähän opinnäytetyöhön.

Toimintopalvelimien *(FSMO)* roolit oli valtuutettu tietyille metsän tai toimialueen ohjauspalvelimille. Alla on esitetty näiden roolien sijoittaminen:

Schema master-metsän laajuinen	FIDHCDC01, DITHC FIHEL, GC
Domain naming master-metsän laajuinen	FIDHCDC01, DITHC FIHEL, GC
PDC emulator-yksi toimialuetta kohden	FIDHCDC01, DITHC FIHEL, GC
RID master-yksi toimialue kohden	FIDHCDC01, DITHC FIHEL, GC

Infrastructure master-yksi toimialue kohden FIDHCDC02, DITHC FIHEL

PDC-emulaattori ja RID master oli sijoitettu alueellisen toimipaikan ensimmäiselle asennetulle ohjauspalvelimelle. Nämä palvelimet ylläpitivät yleistä luetteloa *(Global Catalog)*. Nämä roolit täytyi olla asennettuna lapsitoimialueille, kunnes ne ajettiin tarpeettomina alas.

7 Konsolidointi

Ennen kuin päästiin aloittamaan varsinainen konsolidointi, täytyi seuraavista tehtävistä huolehtia. Toimipaikkojen OU-rakenne täytyi olla luotuna juuritoimialueeseen. Toimipaikkojen järjestelmävalvojien ryhmät lisättiin, joille sitten delegoitiin oikeudet. Otettiin suunnitellut toimipaikkakohtaiset ryhmäkäytännöt käyttöön sekä asetettiin Active Directory-ryhmien oikeudet yrityksen käyttämiin globaaleihin sovelluksiin.

7.1 Ohjauspalvelimien migraatio

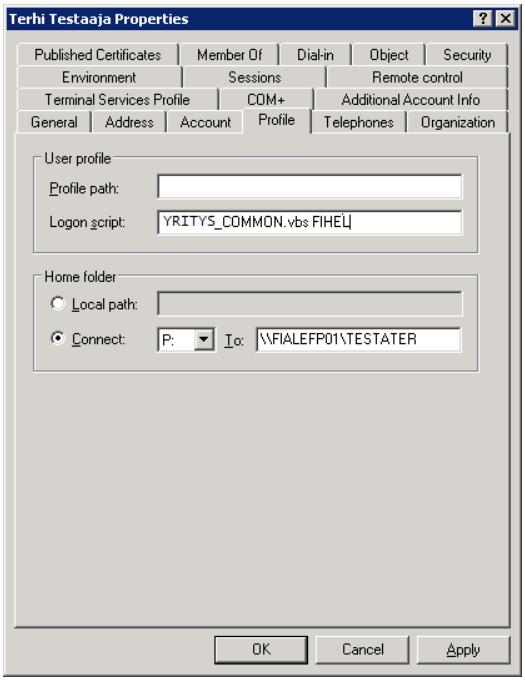
Ohjauspalvelimien DHCP ja DNS palveluista otettiin varmuuskopiot ennen migraatio prosessin aloittamista. Tämän jälkeen Dcpromo-komennolla poistettiin se kyseisestä Active Directorystä ja vaihdettiin uudeksi toimialueeksi yritys.net. Palvelin ylennettiin tämän jälkeen toimialueen ohjauspalvelimeksi. DHCP- ja DNS-palvelut palautettiin palvelimelle. DHCP- ja DNS-palvelujen toiminnallisuus, sekä Active Directory-replikointi varmistettiin ennen seuraavan palvelimen migraatiota. Nämä samat toimenpiteet tehtiin kaikille ohjauspalvelimille.

7.2 Toimipaikkojen migraatio

Ennen varsinaisia migraatiotehtävää arvioitiin resurssit ja muut IT-Infrastruktuuri sidonnaiset ongelmat. Tämä tehtiin yhdessä sovellusten ja palvelujen omistajien kanssa.

Sovelluspuolella jouduttiin myös keskustelemaan ohjelmistojen tarjoajien kanssa. Tämä jouduttiin tekemään, koska Helsingissä tuotetaan palveluja koko globaalille ympäristölle. Palveluja täytyi päästä käyttämään myös yritys.net:in toimialueen ulkopuolelta. Palvelut testattiin yhteistyössä sovellustoimittajien kanssa ennen jatkamista.

Toimipaikkamigraation esivalmisteluihin kuului myös käyttäjätilien luonti yritys.net-toimialueelle. Käyttäjille lisättiin toimipaikkaspesifinen kirjautumiskomentosarja, kuten kuva 12 osoittaa. Visual Basicillä tehtyn ”yritys_common.vbs” ja välilyönnin jälkeen kirjoitetaan toimipaikka, nimistandardien mukaisesti. Kuvan käyttäjän kirjautuessa käynnistettiin root\netlogon-kansiossa oleva skripti nimeltään ”yritys_common.vbs”, joka löytyy myös liitteestä 3. Kyseisessä skiptillä määriteltiin toimipaikan verkkotulostimet ja jaetut verkkokansiot. Kyseisen toimipaikan tulostimet ja verkkokansiot, skripti sai kutsumalla ”FIHEL. INI”-tiedostoa, johon ne oli määritelty. Jokaisella toimipaikalla oli oma ” <toimipaikka>. INI ”-tiedostonsa.



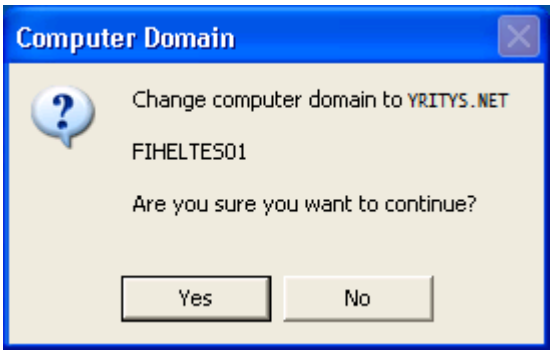
Kuva 12 käyttäjälle lisätään toimipaikka spesifinen skripti

Tiedosto- ja sovelluspalvelimille täytyi myös asettaa käyttäjien ja ryhmien oikeudet kohdalleen, jonka jälkeen myös jäsenpalvelimet toimialueiksi muutettiin yritys.net.

7.3 Tietokoneet ja käyttäjät

Käyttäjän migraatiota varten tarkistettiin käyttäjiltä ja koneesta mahdolliset käytettävät Terminal-yhteydet, yhteisten sovellusten käyttö ja se, mihin käyttäjä oli tallentanut tiedostonsa. Koneeseen kirjauduttiin käyttäjien tunnuksella ja kirjattiin muistiin kaikki Outlook-sähköpostiohjelmaan liitetyt kansiot polkuineen. Tallennettiin myös kaikki Outlookin käyttäjän luomat säännöt ja hälytykset. Tämän jälkeen koneeseen kirjauduttiin vanhan toimialueen järjestelmänvalvojatunnuksella ja lisättiin juuritoimialueen järjestelmänvalvontaryhmät paikalliseen järjestelmänvalvojaryhmään.

Näiden jälkeen koneeseen kirjauduttiin yritys.netin järjestelmänvalvojatunnuksella ja ajettiin tietokoneen migraatiota varten tehty ”yritys_computer_migrate.vbs”-skripti. Näytölle tuli kuvan 13 mukainen ilmoitus, jossa kerrottiin koneen nimi ja kysyttiin lupaa jatkamiselle.



Kuva 13. Migraatio sciptin vahvistus

Hyväksymisen jälkeen tulee kuvan 14 mukainen kysymys kyseisen tietokoneen roolista. Vaihtoehtoina tässä tilanteessa oli valita joko 1 tai 2, jonka mukaan tietokone nimettiin uudestaan.

Kuva 14. Tietokoneen roolin valitseminen

Näiden ikkunoiden jälkeen varmistettiin vielä oikea kohdeorganisaatioyksikkö, johon kone siirrettiin. Seuraavassa ikkunassa saatiin ilmoitus koneen uudesta nimestä. Skripti osasi automaattisesti luoda nimen nimeämisstandardin ja seuraavan vapaan järjestysnumeron mukaisesti. Tietokone käynnistyi uudelleen ja siihen kirjauduttiin järjestelmänvalvojana. Koneen toimialue ja nimi tarkistettiin ja käytiin muuttamassa Exchange-sähköpostipalvelimelle käyttäjän ensisijaiseksi tiliksi yritys.net-tili.

Uloskirjautumisen jälkeen koneeseen kirjauduttiin käyttäjän yritys.net-tunnuksella. Outlook käynnistettiin ja määriteltiin käyttäjän sähköpostitili. Seuraavaksi kirjauduttiin uudestaan ulos ja takaisin järjestelmänvalvojana. Vanhasta profiilista kopioitiin käyttäjäkohtaiset tiedostot ja asetukset käyttäjän uuteen profiiliin. Tämän jälkeen kirjauduttiin vielä kerran ulos ja käyttäjän tunnuksella sisään. Liitettiin Outlookiin mahdolliset kansiot takaisin ja palautettiin käyttäjän säännöt ja hälytykset takaisin. Käyttäjien kaikkien ohjelmistojen toimivuus varmistettiin testaamalla ne. Vanha käyttäjätunnus lukittiin pois käytöstä, mutta ei poistettu. Käyttäjän uuden tunnuksen salasana vaihdettiin käyttäjän kanssa ennakkoon sovituksi ja asetettiin salasanan pakkovaihto toimintaan.

8 AD:n lisäpalvelut

Ryhmäkäytännöt

Active Directoryssä delegoitiin toimipaikkojen järjestelmänvalvojille oikeuksia, joilla oli mahdollisuus käsitellä ryhmäkäytäntö linkkejä *(GP links)* ja ryhmäkäytäntöobjekteja *(GPO).* Heille ei kuitenkaan annettu oikeuksia luoda uusia sääntöjä vaan ainoastaan muokata toimipaikkansa YIT:in luomia sääntöjä. YIT loi yhteiset GPO:tit kaikkien käytettäväksi. Nämä ryhmäkäytännöt linkitettiin toimipaikkojen organisaatioyksikköihin, jotka omistavat kyseiset objektit.

DHCP-palvelu

Tarjosivat Active Directoryn ohjauspalvelimet jokaisessa toimipaikassa.
Toimipaikkojen migraation ajaksi YIT hoiti DHCP- varajärjestelyt. Olemassa oleva konfiguraatio jätettiin sellaisenaan pystyyn. Oletuksena YITCS-henkilöstö huolehti DHCP- palvelimien konfiguroinnista ja ylläpidosta.

WINS-palvelu

Olemassa oleva WINS-rakenne jäi käyttöön. DNS tulee korvaamaan WINS-palvelut heti, kun verkossa ei ole enää 9x- tai NT4-työasemia.

DNS-palvelu

Kaikki Active Directory ohjauspalvelimet tarjosivat myös DNS- palveluja. Työasemat ja jäsenpalvelimet tuli konfiguroida käyttämään toimipisteensä ohjauspalvelinta ensisijaisena DNS palvelimena. Toissijaiseksi DNS palvelimeksi tuli asettaa alueellinen keskitetty verkkotoimipaikka. Nämä asetukset tehtiin automaattisesti ryhmäkäytäntöjen avulla yritys.netin kaikille asiakas koneille.

Yritys.net-vyöhyke *(AD-toimialue)* ja yritys.com *(Internet toimialue)* isännöitiin DNS-palvelimelta Active Directoryyn palvelimeen integroituna alueena. Yritys Oy oli rekisteröinyt yritys.net tunnuksen itselleen, mutta Internetistä ei löytynyt delegoituja merkintöjä, jotka viittasivat siihen.

Toimipaikkojen DNS palvelimet olivat konfiguroitu edelleen lähettämään ulkoiset nimi kyselyt alueellisesti keskitetylle toimipaikalle. Alueellisien toimipaikkojen DNS palvelimet käyttivät juuri vihjeitä ulkoisten nimien selvittämiseksi.

Kaikki alueellisesti keskitetyt toimipaikat oli konfiguroitu käyttämään juuritoimialueen ohjauspalvelinta toissijaisena ja itseään ensisijaisena DNS- palvelimena. DNS- vyöhykkeiden konfiguroinnista ja ylläpidosta vastasi YIT.

Aikatahdistus

Active Directoryssä täytyi käyttää oikeaa aikaa, johtuen Kerberos-todennuksesta. Active Directory toimialue-metsän juuritoimialue konfiguroitiin synkronoimaan aika “Finnish Centre for Metrology and Accreditation” -palvelimilta käyttäen NTP-protokollaa.

Viruksentorjunta

Kaikki työasemat ja palvelimet suojattiin viruksentorjuntaohjelmistoilla. Viruksentorjuntaohjelmistojen asentaminen, valvonta ja ylläpito hoidettiin keskitetysti. Käyttöön rakennettiin myös skripti, joka osasi ilmoittaa koneista, jotka löytyvät AD:sta. Mutta niissä ei ole viruksentorjuntaohjelmistoa asennettuna. Viruksentorjunta-ohjelmistot asetettiin noudattamaan Microsoftin KB822158-artikkelin suosituksia. Myös kolmannen osapuolen ohjelmistoihin kohdistuvia asetuksia jouduttiin lisäämään.

9 Yhteenveto

Tässä opinnäytetyössä oli tarkoitus käsitellä Yritys Oy:n siirtymistä vanhoista Windows NT-toimialueista Windows 2003-palvelin arkkitehtuuriin ja Active Directoryn käyttöönottoon. Tarkoituksena oli myös esitellä Windows Server 2003:en uusia parannettuja ominaisuuksia, joista IT ja liiketoiminta tulisi hyötymään.

Opinnäytetyötä tehdessäni työskentelin järjestelmäasiantuntijana IT-yrityksessä, jolle Yritys Oy oli ulkoistanut järjestelmien kehityksen, ylläpidon ja valvonnan. Työnantajani oli panostanut Microsoftin järjestelmiin ja toimi Microsoft-kultapartneritasolla.

Toimin osana projektiryhmää, johon kuului viisihenkisen suunnitteluryhmän lisäksi Yritys Oy:n IT-johtaja ja toimipaikkojen järjestelmänvalvojat. Pääsin osallistumaan lähestulkoon jokaiseen projektin yksittäiseen vaiheeseen. Tehtäviini kuului muun muassa ohjauspalvelimien kokoaminen, konfigurointi, palautuslevykkeiden luominen, toimipaikkojen järjestelmävalvojien tukeminen, lähitukipalvelut, keskitetty virustorjunta, palvelimien ja käyttäjien migroiminen sekä Active Directoryn konfiguroiminen, ylläpito ja hallinnointi.

Lähdeaineistona käytettiin muutamaa poikkeusta lukuun ottamatta Microsoftin tuottamia aineistoja tai Microsoftin tunnustamien suomalaisasiantuntijoiden kirjoittamia kirjoja. Microsoftin tuottamat online-artikkelit olivat näistä kaikkein suosituimpia, koska niiden sisältöä yleensä päivitetään tiedon muuttuessa. Projektin aikana minulle välittyi myös valtavasti tietämystä muilta ryhmän jäseniltä.

Asiakkaan verkkoinfrastruktuurin kehitysprojekti oli kokonaisuudessaan erittäin isotöinen. Projektin aikana kohdattiin muutamia aikatauluun liittyviä ongelmia. Tällaisina ongelmina mainittakoon ulkomaan toimipaikkojen järjestelmänvalvojien teknisenosaamisen puuttuminen ja sen myöntäminen. Tämä aiheutti toimialueiden konsolidointivaiheen viimeisinä vuorokausina ympärivuorokautista mentorointia projektiryhmän muutamilta jäseniltä. Toimialueiden migraatiovaiheet ja vanhojen toimialueiden alasajo saatiin kuitenkin suoritettua sovittuna ajanjaksona.

Helsingin tukiessa toimipaikkakohtaisia migraatioita ne etenivät hyvin. Eniten haasteita aiheuttivat mobiilikäyttäjät, jotka olivat paljon työmatkoilla. Myös joidenkin käyttäjien työtehtävät aiheuttivat sen, ettei lähituki päässyt normaalina työaikana migroimaan heidän koneitaan eikä käyttäjäprofiileja. Asia saatiin ratkaistua lähituen työskentelemällä muutamina iltoina ja viikonloppuisin.

Varsinainen projekti saatiin päätökseen sovitussa aikataulussa. Projektin valmistuttua huomattiin, että ohjauspalvelimiin asennettu muisti ei ollut riittävä viruksentorjuntasovellusten pyörittämiseen. Muistia jouduttiin ostamaan lisää ja muistit lähetettiin toimipaikoille järjestelmänvalvojien asennettaviksi. Mukaan laitettiin erittäin yksityiskohtainen ohje. Ohjeessa käskettiin muun muassa ennen ohjauspalvelimen alasajoa ottamaan yhteyttä suomessa sijaitsevaan valvomoon, josta palvelimien toimivuutta keskitetysti seurattiin. Näin vältyttiin turhilta hälytyksiltä.

Infrastruktuurin kehittämisen seuraavassa vaiheessa päivitetään Microsoft Exchange 5.5-sähköpostipalvelin uudempaan Exchange 2007-versioon. Myös Active Directoryn metsän toimitason päivittäminen Windows Server-2008 tasolle alkaa olla ajankohtainen.

Opinnäytetyössä päästiin tavoitteisiin ja yrityksen verkkoinfrastruktuuri saatiin tasolle, joka vastasi yrityksen tarpeita. Se toi säästöjä IT:n ylläpito ja kehitykseen liittyvissä kustannuksissa. Liiketoiminnan kannalta yhteisten keskitettyjen sovellusten käyttö ja tietoturva toi paremman ja turvallisemman käyttöympäristön.

Opinnäytetyön aikana tutustuin perusteellisesti Windows Server 2003:een ja sen uusien ominaisuuksien tuomiin hyötyihin. Uusista ominaisuuksista mainittakoon esimerkiksi uudet tiukemmat tietoturva-asetukset, roolipohjaiset käyttöönotot, klusterointi sekä useat hallinnointi työkalut. Active Directory ei ollut minulle entuudestaan tuttu ja olin erittäin kiinnostunut sen oppimisesta. Työn aikana minulle tuli tutuksi miten Active Directoryn eri objektien ja verkkoresurssien ominaisuuksia hallitaan. DNS-nimipalvelun toiminnan ja ohjauspalvelimien toistamispalvelujen oppiminen olivat erittäin kiinnostavia. Active Directoryn tehokkaan hallinnoinnin oppiminen olikin yksi tärkeimmistä tavoitteistani ja siinä onnistuin hyvin. Opinnäytetyö oli monikansallisena

projektina erittäin laaja ja haastava. Sen läpivieminen toi minulle erittäin hyvää kokemusta vastaavanlaisten projektien läpiviemiseksi.

Lähteet

1. **Kivimäki, Jyrki.** *Active Directory - verkonhallinta.* Helsinki : IT Press, 2003.

2. **Reimer, S., Mulcare, M.** *Active Directory for Microsoft -Windows Server 2003 technical referense.* Redmond, WA : Microsoft Press, 2003.

3. **Kivimäki, Jyrki.** *Windows tietoturva.* Helsinki : IT-Press, 1999.

4. **Microsoft.** Yleistä tueteperheestä. *Windows Server 2003.* [Online] Microsoft. http://www.microsoft.com/finland/products/windowsserver2003/evaluation/overview/default.mspx.

5. **Microsoft.** Active Directory LDAP Compliance. *Windows Server 2008 R2.* [Online] Microsoft, October 2003. http://www.microsoft.com/windowsserver2003/techinfo/overview/ldapcomp.mspx.

6. **Stanek, William R.** *Microsoft Windows Server 2003 - Asiantuntijan käsikirja.* Helsinki : IT Press 2005, 2004.

7. **Microsoft.** Windows 2000 Server - Managing DHCP Options. *Microsoft TechNet.* [Online] Microsoft, 2000. http://technet.microsoft.com/en-us/library/cc958941.aspx.

8. **Microsoft.** WINS Technical Referense. *Windows Server TechCenter.* [Online] March 28, 2003. http://technet.microsoft.com/en-us/library/cc736411(WS.10).aspx.

9. **Microsoft.** *AD Technical reference guide.* Redmond, Seattle WA : Microsoft Corporation.

10. **Microsoft.** Configuration Manager and Service Location. *System Center TechCenter.* [Online] Microsoft, 2007. [Cited: 3 25, 2010.] http://technet.microsoft.com/en-us/library/bb632435.aspx.

11. **Microsoft.** Configuration Manager and Name Resolution. *System Center TechCenter.* [Online] 2009. [Cited: 3 25, 2010.] http://technet.microsoft.com/en-us/library/bb680365.aspx.

12. **Wilcox, M.** *Implementing LDAP.* s.l. : Wrox Press, 1999.

13. **Tuttle S., Ehlenberger A., Gorthi R., Leiserson J., Macbeth R., Owen N., Ranahandola S., Storrs M. and Yang C.** Understanding LDAP Design and Implementation. *ibm.com/redbooks.* [Online] 2004. http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf.

14. **Kivimäki, Jyrki.** *Active Directory - Tehokas hallinta.* Jyväskylä : Readme.fi, 2005.

15. **Spealman J., Hudson K.** *Windows Server 2003 Active Directory Infrastructure.* Redmond, Washington : Microsoft Press, 2006.

16. **Microsoft.** Functions (Windows). *Windows Developer Center.* [Online] Microsoft, 2009. http://msdn.microsoft.com/en-us/library/aa366112(VS.85).aspx.

17. **Thompson, Dan.** Understanding LDAP. [Online] 2000. http://download.microsoft.com/download/3/d/3/3d32b0cd-581c-4574-8a27-67e89c206a54/uldap.doc.

18. **Microsoft.** Access control in Active Directory. *Windows Server TechCenter.* [Online] January 21, 2005. http://technet.microsoft.com/en-us/library/cc785913(WS.10).aspx.

19. **Microsoft .** What Are Domains and Forest. *Microsoft Technet.* [Online] http://technet.microsoft.com/de-de/library/cc759073(WS.10).aspx.

20. **Microsoft.** Using Active Directory Service. *Microsoft Technet.* [Online] [Cited: 1 24, 2006.] http://technet.microsoft.com/en-us/library/bb726976.aspx.

21. **Microsoft.** Delegating Administration of Account and Resource OUs. *Microsoft TechNet.* [Online] March 28, 2003. http://technet.microsoft.com/en-us/library/cc784406(WS.10).aspx.

22. **Microsoft.** How Active Directory Replication Topology Works. *Microsoft Technet.* [Online] Microsoft, February 26, 2009. [Cited: April 5, 2010.] http://technet.microsoft.com/en-us/library/cc755994(WS.10).aspx#w2k3tr_repto_how_rrnv.

23. **Microsoft.** What Are Active Directory Functional Levels. *Microsoft Technet.* [Online] Microsoft, February 14, 2010. [Cited: April 5, 2010.] http://technet.microsoft.com/en-us/library/cc787290(WS.10).aspx#w2k3tr_fnlvl_what_huat.

24. **Microsoft.** Technet Functional Levels Backround Information. *Microsoft Server TechNet.* [Online] Microsoft, 28. March 2003. [Viitattu: 6. April 2010.] http://technet.microsoft.com/en-us/library/cc738038(WS.10).aspx.

25. **Microsoft.** Performing an Authoritative Restore of Active Directory Objects. *Windows Server TechCenter.* [Online] Microsoft, 10. April 2006. http://technet.microsoft.com/en-us/library/cc779573(WS.10).aspx.

26. **Microsoft.** What are Operations Masters? *Microsoft Technet.* [Online] Microsoft, 10. December 2009. [Viitattu: 14. April 2010.] http://technet.microsoft.com/en-us/library/cc779716(WS.10).aspx.

27. **Microsoft.** Planning Operations Master Role Placement. *Windows Server TechCenter.* [Online] Microsoft, 28. March 2003. [Viitattu: 14. April 2010.] http://technet.microsoft.com/en-us/library/cc773367(WS.10).aspx.

28. **Microsoft.** How the Global Catalog Works. *Windows Server TechCenter.* [Online] Microsoft, 19. March 2010. [Viitattu: 2. April 2010.] http://technet.microsoft.com/en-us/library/how-global-catalog-servers-work(WS.10).aspx.

29. **Microsoft.** Group Policy processing and precedence. *Windows Server TechNet.* [Online] Microsoft, 2005. http://technet.microsoft.com/en-us/library/cc785665(WS.10).aspx#Startup_and_logon.

30. **Microsoft.** Configuring Windows Server 2003 Security Settings. *Windows Server TechCenter.* [Online] Microsoft, 22. August 2005. http://technet.microsoft.com/en-us/library/cc758749(WS.10).aspx.

31. **Microsoft.** Windows Server 2003 Deployment Kit: Designing and Deploying Directory and Security Services. *Microsoft Download Center.* [Online] 13. 7 2004.

http://www.microsoft.com/downloads/details.aspx?familyid=6cde6ee7-5df1-4394-92ed-2147c3a9ebbe&displaylang=en.

Liite 1: Toimipaikkojen IP-osoitteet

EU Site documentation

Site name	Site short name (AD name)	IP subnet	Bandwidth
Yritys IT Hosting Centre		10.1.201.0	
Helsinki palvelinkeskus		10.1.200.0	
Helsinki, Finland		10.1.44.0	
Site 1		10.1.37.0 10.1.50.0 10.1.51.0 10.1.101.0	
Site 2		10.1.154.0	
Site 3		10.1.46.0 10.1.69.0 10.1.90.0	
Site 4		10.1.108.0	
Site 5		10.1.58.0 10.1.110.0 10.1.118.0 10.1.119.0	
Site 6		10.1.31.0	
Site 7		10.1.109.0	
Site 8		10.1.19.0	
Site 9		10.1.34.0	
Site 10		10.1.56.0	
Site 11		10.1.57.0	
Site 12		10.1.62.0	
Site 13		10.1.64.0	
Site 14		10.1.65.0	
Site 15		10.1.30.0	
Site 16		10.1.18.0 10.1.116.0	
Site 17		10.1.107.0	
Site 18		10.1.105.0	
Site 19		10.1.102.0	
Site 20		10.1.20.0 10.1.54.0 10.1.55.0 10.1.156.0 10.1.4.0	

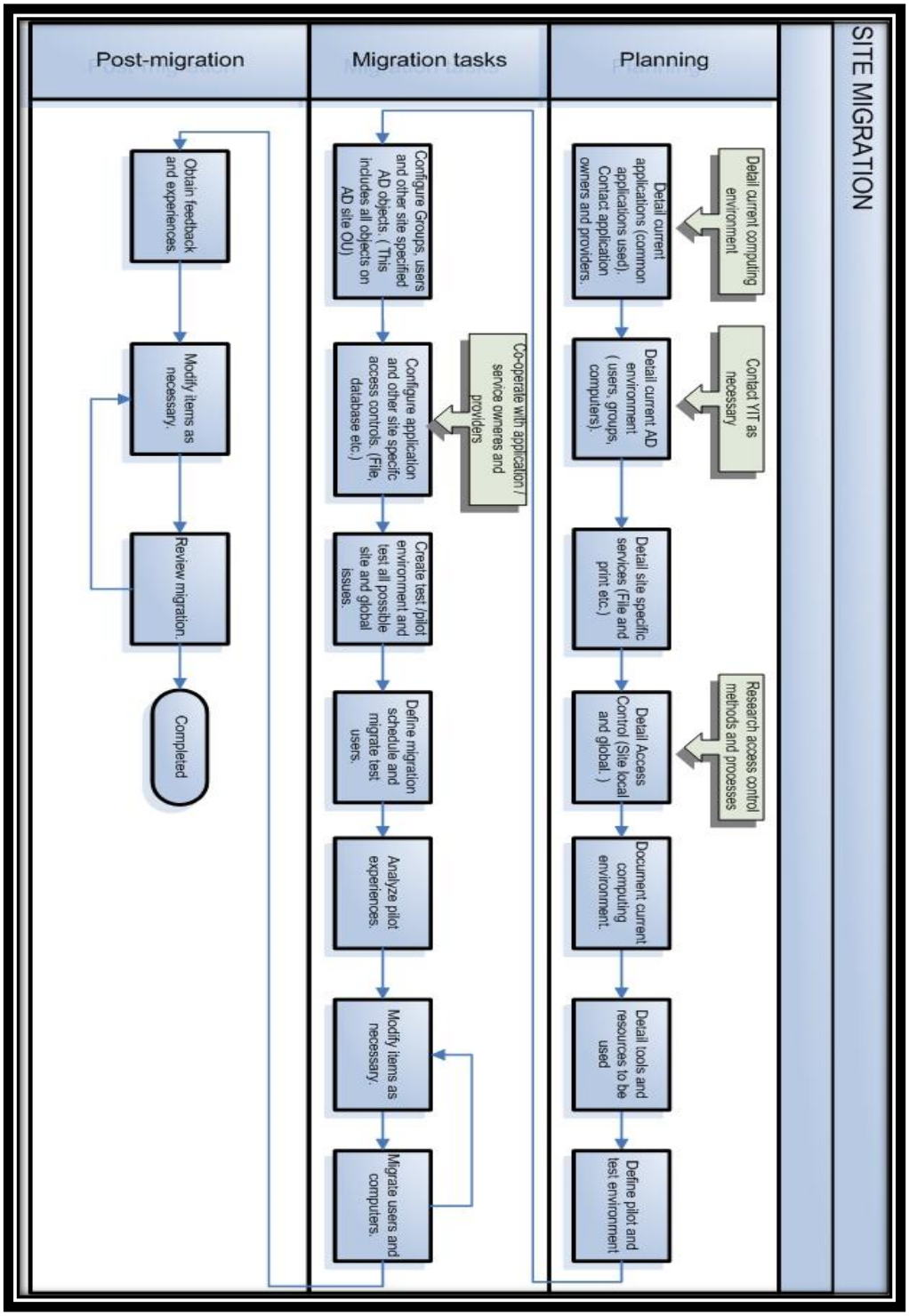
AP Site documentation

Site name	Site short name (AD name)	IP subnet	Bandwidth
Site 21		10.1.168.0	
Site 22		10.1.169.0	
Site 23		10.1.167	
Site 24		10.1.162	
Site 25		10.1.163	
Site 26		10.1.161	
Site 27		10.1.175	
Site 28		10.1.172	
Site 29		10.1.170	
Site 30		10.1.171	
Site 31		10.1.173	
Site 32		10.1.160	

AM Site documentation

Site name	Site short name (AD name)	IP subnet	Bandwidth
Site 33		10.1.151.0	
Site 34		10.1.153.0	
Site 35		10.1.150.0	
Site 36		10.1.152	
Site 37		10.1.32.0	
Site 38		10.1.13.0	
Site 39		10.1.12.0	
Site 40		10.1.9.0	
Site 41		10.1.6.0	
Site 42		10.1.25.0	
Site 43		10.1.28.0	
Site 44		10.1.26.0	
Site 45		10.1.27.0	
Site 46		10.1.24.0	
Site 47		10.1.10.0	
Site 48		10.1.29.0	
Site 49		10.1.1.0	

Liite 2: Toimipaikkamigraation prosessikaavio



Liite 3: Yritys_common.vbs-skripti

```
On Error Resume Next
Const ForReading = 1
Set oShell = WScript.CreateObject("WScript.Shell")
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set WshNetwork = CreateObject("WScript.Network")
Set objADSysInfo = CreateObject("ADSystemInfo")
strOU = Wscript.Arguments(0)
strUSERLDAP = 0
strLogonServer = oShell.ExpandEnvironmentStrings("%LOGONSERVER%")
strUSERNAME = oShell.ExpandEnvironmentStrings("%USERNAME%")
strCOMPUTERNAME = oShell.ExpandEnvironmentStrings("%COMPUTERNAME%")
strMOMEDRIVE = oShell.ExpandEnvironmentStrings("%HOMEDRIVE%")
strHOMEPATH = oShell.ExpandEnvironmentStrings("%HOMEPATH%")
strTRGINI = "" & strLogonServer & "\NETLOGON\" & strOU & "\" & Wscript.Arguments(0) & ".INI"
strLOGFILE = "" & strHOMEDRIVE & "" & strHOMEPATH & "\YRITYS_Logon.log"
Set objLogFile = objFSO.CreateTextFile(""& strLogFile & "")

'Create log
If Not objFSO.FileExists("" & strTRGINI & "") Then
   objLogFile.WriteLine("[LOGON SCRIPT]")
   objLogFile.WriteLine("START=" & Now & "")
   objLogFile.WriteLine("LOGONSERVER=" & strLogonServer & "")
   objLogFile.WriteLine("CONFIGURATION FILE=" & Wscript.Arguments(0) & "")
   objLogFile.WriteLine("COMPUTERNAME=" & strCOMPUTERNAME & "")
   objLogFile.WriteLine("USERNAME=" & strUSERNAME & "")
   objLogFile.WriteLine("ERROR=Can't open " & strTRGINI & ". VBSERRNUMBER:" & Err.Number & "")

   objLogFile.Close()
   Set objLogFile = Nothing
   Set oShell = Nothing
   Set objFSO = Nothing
   Set WshNetwork = Nothing
   Wscript.Quit(0)
End If

'Open .INI file for reading
Err.Clear
objLogFile.WriteLine("[LOGON SCRIPT]")
objLogFile.WriteLine("START=" & Now & "")
objLogFile.WriteLine("LOGONSERVER=" & strLogonServer & "")
objLogFile.WriteLine("CONFIGURATIONFILE=" & Wscript.Arguments(0) & "")
objLogFile.WriteLine("COMPUTERNAME=" & strCOMPUTERNAME & "")
objLogFile.WriteLine("USERNAME=" & strUSERNAME & "")
Set objTRG_INI_FILE = objFSO.OpenTextFile("" & strTRGINI & "", ForReading)
objLogFile.WriteLine("SUCCESS=Open " & strTRGINI & ";(" & Err.Number & ")")
Err.Clear
'Process .INI file line by line

Do Until objTRG_INI_FILE.AtEndOfStream
   strTRG_INI_LINE = UCase(objTRG_INI_FILE.Readline)
   'Check resource
   If Left(strTRG_INI_LINE, InStr(strTRG_INI_LINE,"=")) = UCase("PRINTER=") Then
      strTRG_PRINTER = Replace(strTRG_INI_LINE,UCase("PRINTER="),"")
      If Not strTRG_PRINTER = "" Then
      'Add printer connection
      WshNetwork.AddWindowsPrinterConnection "" & strTRG_PRINTER & ""
      If Err.Number <> 0 Then
         objLogFile.WriteLine("ERROR=PRINTER;" & strTRG_PRINTER & ";" & Err.Number & "")
         Err.Clear
      Else
         objLogFile.WriteLine("SUCCESS=PRINTER;" & strTRG_PRINTER & ";" & Err.Number & "")
         Err.Clear
      End If
      End If
   End If
   'Check share resources
   If Left(strTRG_INI_LINE, InStr(strTRG_INI_LINE,"=")) = UCase("SHARE=") Then
      strTRG_COMMONSERVER = Replace(strTRG_INI_LINE,UCase("SHARE="),"")
      If Not strTRG_COMMONSERVER = "" Then
```

```
      strCOMMONSHARE = split(strTRG_COMMONSERVER,";")
      strCOMMONDRIVELETTER = strCOMMONSHARE(0)
      strCOMMONSHAREPATH = strCOMMONSHARE(1)
      'Map network drive. If drive exist remove it first.
      Set objDrives = WshNetwork.EnumNetworkDrives
      For i = 0 to objDrives.Count - 1 Step 2

         If UCase(objDrives.Item(i)) = UCase(strCOMMONDRIVELETTER) Then

           WshNetwork.RemoveNetworkDrive"" & strCOMMONDRIVELETTER & "",True
            If Err.Number <> 0 Then
                        objLogFile.WriteLine("ERROR=REMOVE DRIVE;" & strCOMMONDRIVELETTER & ";" & Err.Number
& "")
            Err.Clear
            Else
                        objLogFile.WriteLine("SUCCESS=REMOVE DRIVE;" & strCOMMONDRIVELETTER & ";" &
Err.Number & "")
            Err.Clear
            End If
         End If

      Next
      WSHNetwork.MapNetworkDrive "" & strCOMMONDRIVELETTER & "", "" & strCOMMONSHAREPATH & "",True
      If Err.Number <> 0 Then
         objLogFile.WriteLine("ERROR=SHARE;" & strCOMMONDRIVELETTER & ";" & strCOMMONSHAREPATH & ";" &
Err.Number & "")
         Err.Clear
      Else
         objLogFile.WriteLine("SUCCESS=SHARE;" & strCOMMONDRIVELETTER & ";" & strCOMMONSHAREPATH & ";"
& Err.Number & "")
         Err.Clear
      End If
      End If
   End If

   'Group Based Share Resources
   If Left(strTRG_INI_LINE, InStr(strTRG_INI_LINE,"=")) = UCase("GROUP=") Then
      'Parse group and share attributes
      strTRG_GROUPSERVER = Replace(strTRG_INI_LINE,UCase("GROUP="),"")
      If Not strTRG_GROUPSERVER = "" Then
         strGROUPSHARE = split(strTRG_GROUPSERVER,";")
         strUSRGROUP = strGROUPSHARE(0)
         strGROUPDRIVELETTER = strGROUPSHARE(1)
         strGROUPSHAREPATH = strGROUPSHARE(2)
         'Bind to user with ldap
         If strUSERLDAP = 0 Then
         strUser = objADSysInfo.UserName
         Set objUser = GetObject("LDAP://" & strUser)
         strUSERLDAP = 1
         End If
         'Check groups where user belong to
         For Each strGroup in objUser.Groups
         strGROUPMEM = strGroup.CN
         If UCase(strGROUPMEM) = UCase(strUSRGROUP) Then
            objLogFile.WriteLine("SUCCESS=USER MEMBER OF;" & strGROUPMEM & ";" & Err.Number & "")
            'Map network drive. If drive exist remove it first.
            Set objDrives = WshNetwork.EnumNetworkDrives
            For i = 0 to objDrives.Count - 1 Step 2

               If UCase(objDrives.Item(i)) = UCase(strGROUPDRIVELETTER) Then

                  WshNetwork.RemoveNetworkDrive"" & strGROUPDRIVELETTER & "",True
                   If Err.Number <> 0 Then
                                       objLogFile.WriteLine("ERROR=REMOVE GROUP DRIVE;" & strGROUPDRIVELETTER
& ";" & Err.Number & "")
                              Err.Clear
                   Else
                                       objLogFile.WriteLine("SUCCESS=REMOVE GROUP DRIVE;" &
strGROUPDRIVELETTER & ";" & Err.Number & "")
                              Err.Clear
                   End If
               End If
```

```
            Next
            'Map Network Drive
            WSHNetwork.MapNetworkDrive "" & strGROUPDRIVELETTER & "", "" & strGROUPSHAREPATH & "",True
            If Err.Number <> 0 Then
               objLogFile.WriteLine("ERROR=GROUP " & strGROUPMEM & " SHARE;" & strGROUPDRIVELETTER & ";" &
strGROUPSHAREPATH & ";" & Err.Number & "")
                  Err.Clear
            Else
               objLogFile.WriteLine("SUCCESS=GROUP " & strGROUPMEM & " SHARE;" & strGROUPDRIVELETTER & ";"
& strGROUPSHAREPATH & ";" & Err.Number & "")
                  Err.Clear
            End If
         End If
         Next
         strGROUPMEM = ""
      End If
   End If

   'Group Based Printer Resources
   If Left(strTRG_INI_LINE, InStr(strTRG_INI_LINE,"=")) = UCase("GROUPPRINTER=") Then
      'Parse group and printer attributes
      strTRG_GROUPPRINTER = Replace(strTRG_INI_LINE,UCase("GROUPPRINTER="),"")
      If Not strTRG_GROUPPRINTER = "" Then
         strGROUPPRINTER = split(strTRG_GROUPPRINTER,";")
         strUSRPRGROUP = strGROUPPRINTER(0)
         strGROUPPRINTERSHARE = strGROUPPRINTER(1)
         If strUSERLDAP = 0 Then
         strUser = objADSysInfo.UserName
         Set objUser = GetObject("LDAP://" & strUser)
         strUSERLDAP = 1
         End If
         'Check groups where user belong to
         For Each strGroup in objUser.Groups
         strGROUPMEM = strGroup.CN
         If UCase(strGROUPMEM) = UCase(strUSRPRGROUP) Then
            objLogFile.WriteLine("SUCCESS=USER MEMBER OF;" & strGROUPMEM & ";" & Err.Number & "")
         'Add printer connection
         WshNetwork.AddWindowsPrinterConnection "" & strGROUPPRINTERSHARE & ""
         If Err.Number <> 0 Then
            objLogFile.WriteLine("ERROR=GROUP PRINTER;" & strGROUPPRINTERSHARE & ";" & Err.Number & "")
            Err.Clear
         Else
            objLogFile.WriteLine("SUCCESS=GROUP PRINTER;" & strGROUPPRINTERSHARE & ";" & Err.Number & "")
            Err.Clear
         End If
         End If
         Next
         strGROUPMEM = ""
      End If
   End If

   'Common external commands or batch jobs
   If Left(strTRG_INI_LINE, InStr(strTRG_INI_LINE,"=")) = UCase("COMM=") Then
      'Parse command attributes
      strTRG_COMM = Replace(strTRG_INI_LINE,UCase("COMM="),"")
      If Not strTRG_COMM = "" Then
         strCOMM = split(strTRG_COMM,";")
         strCOMMPATH = strCOMM(0)
         strCOMMVISIBLE = strCOMM(1)
         strCOMMWAIT = strCOMM(2)
            'Run command
            ErrReturn = oShell.Run(strCOMMPATH,strCOMMVISIBLE,strCOMMWAIT)
            If ErrReturn <> 0 Then
               objLogFile.WriteLine("ERROR=COMM;" & strCOMMPATH & ";" & Err.Number & "")
               Err.Clear
            Else
               objLogFile.WriteLine("SUCCESS=COMM;" & strCOMMPATH & ";" & Err.Number & "")
               Err.Clear
            End If
      End If
   End If

   ' Group based external commands or batch jobs
```

```
    If Left(strTRG_INI_LINE, InStr(strTRG_INI_LINE,"=")) = UCase("GROUPCOMM=") Then
       'Parse command attributes
       strTRG_GROUPCOMM = Replace(strTRG_INI_LINE,UCase("GROUPCOMM="),"")
       If Not strTRG_GROUPCOMM = "" Then
          strGROUPCOMM = split(strTRG_GROUPCOMM,";")
          strUSRCOMMGROUP = strGROUPCOMM(0)
          strGROUPCOMMPATH = strGROUPCOMM(1)
          strGROUPCOMMVISIBLE = strGROUPCOMM(2)
          strGROUPCOMMWAIT = strGROUPCOMM(3)
          If strUSERLDAP = 0 Then
          strUser = objADSysInfo.UserName
          Set objUser = GetObject("LDAP://" & strUser)
          strUSERLDAP = 1
          End If
          'Check groups where user belongs to
          For Each strGroup in objUser.Groups
          strGROUPMEM = strGroup.CN
          If UCase(strGROUPMEM) = UCase(strUSRCOMMGROUP) Then
             'Run command
             ErrReturn = oShell.Run(strGROUPCOMMPATH,strGROUPCOMMVISIBLE,strGROUPCOMMWAIT)
             If ErrReturn <> 0 Then
                objLogFile.WriteLine("ERROR=GROUPCOMM;" & strGROUPCOMMPATH & ";" & Err.Number & "")
                Err.Clear
             Else
                objLogFile.WriteLine("SUCCESS=GROUPCOMM;" & strGROUPCOMMPATH & ";" & Err.Number & "")
                Err.Clear
             End If
          End If
          Next
          strGROUPMEM = ""
       End If
    End If
Loop
objLogFile.WriteLine("END=" & Now & "")
objLogFile.Close()
Set objLogFile = Nothing
Set objTRG_INI_FILE = Nothing
Set objDrives = Nothing
Set oShell = Nothing
Set objFSO = Nothing
Set WshNetwork = Nothing
Wscript.Quit(0)
```