TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

Opinnäytetyö

Harri Kuosmanen

WINDOWS SERVER 2008:n ROOLIT JA ASENNUS

Työn ohjaaja Yliopettaja Jorma Punju
Työn teettäjä Datagroup Pirkanmaan Konttorikone Oy, valvojana Huoltoinsinööri Mikko Vääränen
Tampere 2009

TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikka
Tietoliikennetekniikka
Kuosmanen, Harri
Windows Server 2008:n roolit ja asennus
Opinnäytetyö
49 sivua
Työn ohjaaja
Yliopettaja Jorma Punju
Työn teettäjä
Datagroup Pirkanmaan Konttorikone Oy,
valvojana Huoltoinsinööri Mikko Vääränen
Toukokuu 2009
Hakusanat
Windows Server 2008, Server roles, Active Directory, Domain Controller

TIIVISTELMÄ

Opinnäytetyön tavoitteena on esitellä Microsoftin uutta Windows Server 2008 palvelinkäyttöjärjestelmää. Opinnäytetyössä käydään läpi palvelimen mahdollisia käytännön rooleja pk-yrityksissä, sekä käydään läpi kuinka normaali asennusrutiini suoritetaan. Opinnäytetyö käy läpi myös aiheita liittyen palvelinlaitteistoihin, Active Directoryyn, palvelimen tietoturvaan ja tietojen varmistukseen.

Windows Server 2008 on Microsoftin uusin versio suositusta palvelinkäyttöjärjestelmästä, joka on tullut markkinoille helmikuussa 2008. Käyttöjärjestelmän ollessa vielä näin tuore, siihen liittyvät uudet ominaisuudet ja toiminnot ovat vielä monelle hämärän peitossa.

Tulevaisuudessa useissa yrityksissä tullaan siirtymään Windows Server 2008 palvelinkäyttöjärjestelmään, koska tuki vanhoilta palvelinkäyttöjärjestelmiltä loppuu ajan kuluessa. Tulevaisuudessa nähdään myös tuleeko Windows Server 2008 käyttöjärjestelmästä suosittu vai jätetäänkö se yrityksissä kokonaan väliin uusien tieltä.

TAMK University of Applied Sciences
Computer Systems Engineering
Telecommunications Engineering

Kuosmanen, Harri	Windows Server 2008’s roles and installation
Engineering thesis	49 pages
Thesis supervisor	Senior Teacher Jorma Punju
Comissioning company	Datagroup Pirkanmaan konttorikone Oy, Service Engineer Mikko Vääränen

May 2009

Keywords	Windows Server 2008, Server roles, Active Directory, Domain controller

ABSTRACT

The goal of this thesis is to introduce Microsoft's new Windows Server 2008 operating system. In this thesis I am going to go through the roles of Windows Server 2008 that can be used in small and medium-sized enterprises, and how normal installation routine goes in Windows Server 2008. Thesis also goes through subjects like server hardware, Active Directory, the security of server and the importance of backups.

Windows Server 2008 is the most recent version of Microsoft's popular server operating system, which came to market in February of 2008. Because this operating system is still so young, that is why there is many people, who doesn't know a lot about the new features and functions that came with new version.

In the future there will be a lot of enterprises, who will upgrade their aged server operating systems to Windows Server 2008, because the support of old server operating systems aren’t infinite. In the future we will see, if Windows Server 2008 will become popular server operating system or do enterprises just leave it and wait for next release.

SISÄLLYS

KÄYTETYT TERMIT JA LYHENTEET

AD — Active Directory on Microsoftin toteutus hakemistopalvelusta. AD sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista.

Blade palvelin — Blade palvelimet ovat yksittäisiä kaikenkattavia tietokonepalvelimia, jotka on suunniteltu tilaa säästävästi.

CIFS — Common Internet File System on protokolla, joka mahdollistaa ohjelmien tekemät tiedostojen ja palveluiden pyynnöt Internetiin.

Cluster — Clusteri on ryhmä tietokoneita, jotka ovat linkitetty yhteen ja jakavat sekä käyttävät prosessointitehoa yhtenä tietokoneena.

DC — Domain Controller on Active Directory -toimialueella oleva ohjauspalvelin

DNS — Domain Name System on Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.

IP-osoite — Internet Protocol on Internet-kerroksen protokolla, joka huolehtii IP-pakettien toimittamisesta perille Internet verkossa.

IPV4 — IP-protokollan neljäs versio. Yleisin Internetissä käytössä oleva IP-protokolla.

IPV6 — IP-protokollan uusi versio, joka on tulevaisuuden korvaaja IPV4 versiolle.

DC	Key Distribution Center on osa turvallisuuskäytäntöä, jolla vähennetään luontaisesti riskiä avaimien vaihdon yhteydessä.
LDAP	Lightweight Directory Access Protocol on protokolla, jota Active Directory käyttää hakemistosta tehtäviin hakuihin.
MIME	Multipurpose Internet Mail Extensions määrittelee tavan, jolla sähköpostiviestejä pystytään välittämään erilaisia merkkivalikoimia käyttäen. MIMEN:n ansiosta sähköpostiviesteihin voidaan liittää liittetiedostoja.
NetBIOS	Network Basic Input/Output System on OSI-mallin istuntokerroksen palvelu, jonka avulla tietokoneet voidaan yksilöidä lähiverkossa.
POP3	Post Office Protocol on sähköpostiviestien hakemiseen tarkoitettu protokolla.
SMTP	Simple Mail Transfer Protocol on sähköpostiviestien välittämiseen sähköpostiohjelmasta vastaanottajalle tarkoitettu protokolla.
SQL	Structured Query Language on stardardoitu kyselykieli, jolla relaatiotietokantaan voi tehdä erilaisia hakuja, muutoksia ja lisäyksiä.
TFTP	Trivial File Transfer Protocol on tiedostonsiirtoprotokolla, joka on toiminnaltaan hyvin samankaltainen kuin File Transfer Protocol (FTP).
TCP/IP	Transmission Control Protocol / Interet Protocol on usean Internet-liikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmä.

1 JOHDANTO

Monissa pk-yrityksissä mietitään näinä aikoina palvelinten ja niiden käyttöjärjestelmien päivittämistä uuteen Windows Server 2008 käyttöjärjestelmään. Windows Server 2008 tuo mukanaan muutamia tärkeitä etuja ja uusia ominaisuuksia verrattuna vanhoihin Windows palvelinkäyttöjärjestelmiin, joten siihen siirtyminen on järkevää.

Opinnäytetyö käsittelee Windows Server 2008 -versioon asennettavissa olevia erilaisia palveluita ja sovelluksia. Työssä kerrotaan myös, kuinka Windows Server 2008 palvelimeen saadaan asetettua alkuasetukset pk-yrityksiä varten.

Tämä opinnäytetyö on kuitenkin vain pintaraapaisu todellisen Windows palvelimen ja sen palvelujen asennuksesta. Todellisuudessa palveluita ja niiden ominaisuuksia on rajattomasti, joten opinnäytetyö täytyi rajata ainoastaan perusasennukseen ja palvelimen toimintaan saattamiseen. Kun muut osa-alueet ovat kunnossa ja palvelin on asetettu toimintaan opinnäytetyössä esitetyillä tavoilla, on palvelin hyvässä mallissa todelliseen ympäristöön liittämistä varten. Todellisuudessa asetuksia ja ominaisuuksia täytyy konfiguroida huomattavasti tarkemmin ja ottaa huomioon monia pienempiä asioita, joita tämän opinnäytetyön laajuudessa on mahdoton käsitellä.

2 WINDOWS PALVELIN

Palvelimella tarkoitetaan tietoliikenteen yhteydessä palvelinohjelmistoa suorittavaa tietokonetta. Palvelinohjelmistojen tarkoituksena on tarjota erilaisia palveluita muille ohjelmille joko tietokoneverkon välityksellä tai paikallisesti samassa tietokoneessa. Palvelinta käyttävää sovellusta tai tietokonetta nimitetään asiakkaaksi.

Nykypäivän tärkeimpiä Windows palvelinsovelluksia ovat mm. web-, sähköposti-, tiedostonjako- ja tulostuspalvelut, jotka toteutetaan palvelinsovelluksien avulla. Ilman näitä nykypäivänä tarjolla olevia palveluja olisi vaikeaa elää ja toimia nyky-yhteiskunnassa.

2.1 Laitteistokokoonpano

Palvelimien laitteistoissa voi olla suuria eroja. Normaalisti pk-yrityksissä käytetään yhtä riittävän tehokasta palvelinta, joka pystyy suorittamaan tarvittavia palveluita ongelmitta. Suurissa yrityksissä käytetään useita palvelimia tai palvelinjärjestelmiä. Näissä järjestelmissä eri palvelut on jaettu palvelinten kesken tai suurissa sovelluksissa palvelua suorittaa yhtä aikaa useita palvelimia yhdessä. On olemassa myös ns. palvelinfarmeja, joissa palvelinten laskentateho voi olla jaettu useiden kymmenien tai jopa satojen palvelinten kesken. Näitä järjestelmiä hoitaa yleensä Blade-palvelinjärjestelmät. Esim. suuret web-sivustot käyttävät tällaista ratkaisua omien palveluidensa pyörittämiseen.

Valmiiden palvelinkokoonpanojen hinnat vaihtelevat tuhannesta eurosta aina kymmeniin tuhansiin euroihin, kun tarkoitetaan normaaleita palvelinympäristöjä pk-yrityskäyttöön.

2.2 Käyttöjärjestelmät

Nykyään palvelinratkaisuihin on saatavilla useita eri palvelinkäyttöjärjestelmiä. Suurimpia niistä ovat Microsoft Server, Sun Microsystemsin Sun Solaris ja Linux-puolelta Suse, Debian, Red Hat ja useat muut Linuxin jakeluversiot. Tässä työssä keskitytään kuitenkin ainoastaan Windows palvelimiin. Microsoftin julkaisemat palvelinkäyttöjärjestelmät ovat seuraavat:

- Windows NT Server (versio 3.1, myöhemmin muita versioita), syyskuu 1993
- Windows 2000 Server Family, heinäkuu 2000
- Windows Server 2003 Family, huhtikuu 2003
- Windows Home Server, heinäkuu 2007
- Windows Server 2008, helmikuu 2008. /1/

Windows Server 2008 on rakennettu samoista koodikirjastoista kuin Windows Vista, jonka myötä se jakaa samaa arkkitehtuuria ja toiminnallisuutta. Saman koodikirjaston johdosta käyttöjärjestelmä tukee suurimmaksi osaksi samoja uusia teknillisiä toteutuksia kuin mitä Windows Vistan toi tullessaan. Tällä tarkoitetaan ominaisuuksia, jotka liittyvät tekniikkaan, turvallisuuteen, hallinnointiin ja ylläpitoon. Esim. kokonaan uudelleenkirjoitettu verkkopino, jossa natiivinen IPV6-tuki, natiivinen langattomuus, nopeus ja suojausparannukset.

Palvelinkäyttöjärjestelmistä on olemassa useita eri versioita myös Windowsin puolella. Versiot ovat seuraavat:

- Windows Server 2008 Standard
- Windows Server 2008 Small Business Standard ja Premium
- Windows Server 2008 Enterprise
- Windows Server 2008 Datacenter
- Windows Web Server 2008.

Standard -versio sisältää palvelinkäyttöjärjestelmän perusominaisuudet ja toiminnallisuudet pienempiin yrityksiin. Small Business -versiot sisältävät lisäominaisuuksia kuten Exchange Server ja SQL-server. Enterprise versio sisältää paremman ja laajemman rautatuen sekä tukee clusterointia. Datacenter on tarkoitettu isoihin palvelinjärjestelmiin, jotka hoitavat esim. virtualisointia. Web Server on nimensä mukaan tarkoitettu järeiden web-palvelinympäristön toteuttamiseen. /2/

2.3 Käyttömahdollisuudet

Palvelimista löytyy lähes rajattomat käyttömahdollisuudet. Erillisiä palvelinsovelluksia löytyy Windows serveriin sekä Microsoftin omista kehittämistään ja kolmannen osapuolen sovelluksista. Windowsin omista palveluista puhutaan nimellä roolit. Rooleja ovat:

- DHCP-palvelin
- DNS-palvelin
- toimialueen ohjauspalvelin, DC

- tiedostopalvelin
- sähköpostipalvelin (POP3, SMTP)
- tulostuspalvelin
- remote access / VPN-palvelin
- server cluster node
- terminaalipalvelin
- WINS-palvelin
- web-palvelin. /3/

Kolmannen osapuolen sovelluksia ovat esim. taloushallintaohjelmistot ja keskitetty virustorjunta.

2.3.1 DHCP-palvelin

DHCP (lyhenne sanoista *Dynamic Host Configuration Protocol*) on verkkoprotokolla, jonka yleisin tehtävä on jakaa IP-osoitteita uusille lähiverkkoon kytkeytyville laitteille. Ylläpitäjä antaa tietyn IP-osoiteavaruuden, jolloin jokainen laite pyytää käynnistyksen yhteydessä DHCP-palvelimelta oman IP-osoitteen. Annettu osoite on voimassa ennalta määrätyn ajan. Kun ennalta määrätty aika on kulunut, kysyy IP-laite osoitteelle lisäaikaa. Menettely yksinkertaistaa asiakaskoneiden asetuksien hallintaa huomattavasti, koska koneille ei tarvitse määrittää osoitteita käsin.

DHCP-palvelin voi jakaa asiakkaille myös muita asetuksia, kuten oletusyhdyskäytävän ja nimipalvelimen (tai nimipalvelimien) IP-osoitteen. Käytännössä DHCP-palvelin voi jakaa lähes mitä tahansa verkkoon liittyviä asetuksia, kuten reitittimille käyttöjärjestelmän lataamiseen käytetyn TFTP-palvelimen osoitteen.

Jos yrityksen sisäverkosta löytyy Windows palvelin, voidaan siitä samalla luoda DHCP-palvelin. Itse DHCP-palvelinprosessi ei rasi-

ta nykyajan palvelimia juuri lainkaan, ja sen takia palvelu voidaan helposti yhdistää jonkin palvelimen toimintojen rinnalle. Tällä tavalla voidaan helposti hallinnoida osoitteita, joita koneille asetetaan. On myös yleistä käyttää DHCP-palvelimena verkon reititinlaitetta, joka jakaa IP-osoitteita, mutta tällöin jaettejun verkko-osoitteiden hallinta tapahtuu reitittimen omasta käyttöliittymästä eikä saman palvelimen käyttöliittymästä, missä mahdolliset muutkin palvelut toimivat. Tästä syystä johtuen ylläpitäjän työ hankaloituu. /4/

2.3.2 DNS-palvelin

DNS eli *Domain Name System* on Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi. Internetin laitteet kommunikoivat keskenään numeeristen IP-osoitteiden avulla, joiden muistaminen olisi ihmisille toivotonta. Nimipalvelun ansiosta IP-osoitteiden sijasta voidaan käyttää helpommin muistettavia nimiä. Esimerkkinä voidaan mainita, että osoite www.tamk.fi kääntyy IPV4-osoitteeksi 193.167.70.44 DNS-palvelinten avulla ja tällä IPV4-osoitteella voidaan paikantaa palvelimen todellinen sijainti.

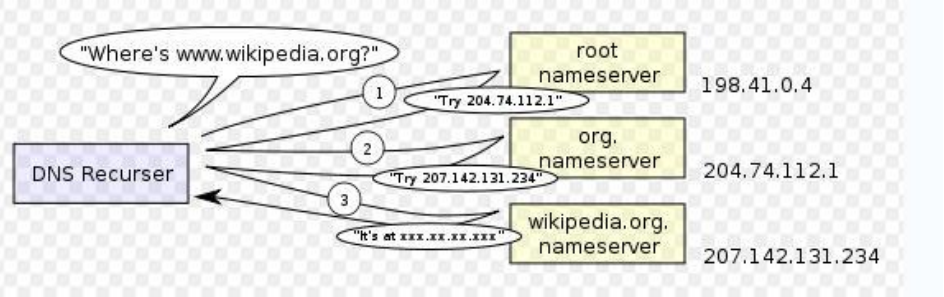
Nimipalvelun toteuttavia palvelintyyppejä on kaksi:

- nimipalvelukyselyihin vastauksia hakevat koneet eli *resolverit*.
- nimipalvelukyselyihin vastauksia antavat koneet eli *autoritääriset nimipalvelimet*.

Resolvereilla tarkoitetaan laitteita, jotka hakevat osoitteita autoritäärisiltä nimipalvelimilta (ensisijaisen autoritäärisen nimipalvelimen IP-osoite on asetettu laitteelle etukäteen). Tämä tapahtuu esim. siinä vaiheessa, kun käyttäjä kirjoittaa selainohjelman osoi-

teriville halutun osoitteen ja painaa enteriä. Autoritääriset nimipalvelimet taas vastaavat hakuihin ja palauttavat vastauksen alkuperäisen haun suorittavalle laitteelle, jonka jälkeen laite lähettää HTTP-pyynnön saamaansa IP-osoitteeseen hakeakseen halutun web-sivun.

Ensisijainen autoritäärinen nimipalvelin (kuvassa 1 - *DNS Recurser*) ei aina tiedä haetun osoitteen IP-osoitetta, vaan nimipalvelimen täytyy lähettää jatkokyselyitä useille juuripalvelimille, jotka kertovat mistä tieto mahdollisesti löytyy. Jos osoitetta ei löydy myöskään juuripalvelimilta, palautetaan käyttäjälle virheilmoitus. /5/



Kuva 1. DNS-kyselyn periaatteellinen toiminta /6/

2.3.3 Toimialueen ohjauspalvelin (DC)

Windows Server järjestelmissä toimialueen ohjauspalvelimella (*Domain Controller, DC*) tarkoitetaan palvelinta, joka vastaa turvallisuus autentikointikyselyihin (sisäänkirjaus, oikeuksien tarkistus jne.) Windows Server toimialueella. Vaikka DC:n versiot vaihtelevat Windows Serverien omien versioiden mukaan, on kuitenkin lähes kaikissa moderneissa DC:ssa muutama yhteinen olennainen ominaisuus. Näitä ominaisuuksia ovat LDAP tietokanta (*Lightwight Directory Access Protocoll database*), KDC palvelin (*Key Distribu-*

tion Center server), CIFS palvelin (*Common Internet File System server*) sekä paikalliset- että verkkopalvelut, joita tarvitaan yhteydenpitoon asiakas-palvelin välisessä kommunikoinnissa. Toimialueen ohjauspalvelimen yhtenä tärkeimpänä tehtävänä on AD -tietokannan hallinta, josta kerrotaan kappaleessa 2.4. /7/

2.3.4 Tiedostopalvelin

Tiedostopalvelimen tarkoituksena on jakaa palvelinkoneen massamuistitilaa ja sen sisältämiä tiedostoja asiakassovellusten käyttöön. Monesti palvelimessa olevaa massamuistia käytetään tiedostojen varastointipaikkana käyttäjien keskuudessa. Nykyaikana erilliset verkossa olevat tiedostopalvelimet (NAS, Network Attached Storage) ovat myöskin saaneet suosiota käyttäjiltä helppokäyttöisyyden ja edullisuuden vuoksi.

Tiedostopalvelintyyppejä on olemassa kahdenlaisia. Dedikoituja ja ei-dedikoituja. Dedikoitu palvelin on suunniteltu erityisesti tiedostopalvelinkäyttöön, jota käyttäjät voivat käyttää tiedostojen lukemiseen ja tallentamiseen. Ei-dedikoidut palvelimeksi voi ymmärtää esim. tietokoneen, josta kytketään päälle tiedostojenjakopalvelu ja se jakaa valittuja tiedostoja muille käyttäjille. Tätä tietokonetta ei siis käytetä pääasiassa tiedostojen jakoon, vaan muuhun käyttöön.

Tiedostopalvelimet voidaan myös luokitella pääsytyypin mukaan. Internetissä oleviin tiedostopalvelimiin päästään yhteyteen yleensä käyttämällä FTP- (*File Transfer Protocol*) tai HTTP-protokollaa (*Hypertext Transfer Protocol*) kun taas LAN:ssa (*Local Area Network, Lähiverkko*) oleviin tiedostopalvelimiin saadaan yhteys käyt-

tämällä SMB/CIFS tai NFS protokollaa riippuen järjestelmästä (Windows tai Unix-pohjainen järjestelmä). /8/

2.3.5 Tietokantapalvelin

Tietokantapalvelimen voi helposti ymmärtää väärin tiedostopalvelimena, vaikka se ei sitä ole. Tietokantapalvelin on sovellus, joka tarjoaa tietokantapalvelut muille tietokonesovelluksille tai tietokoneille asiakas-palvelin arkkitehtuurilla. Tietokantapalvelinkyselyihin käytetään tietokantasovelluksesta riippuen erilaisia kieliä kuten esim. SQL.

Tietokantapalvelin jakaa sovelluksen kahteen eri osiin, jotka ovat etu- ja takapää, ja jotka käyttävät käyttäjä-palvelin arkkitehtuuria. Etupää ajetaan asiakkaan tietokoneella, jossa haettu tai kysytty tieto näytetään. Takapää ajetaan palvelimella, jossa se suorittaa tehtäviä kuten tietoanalysointia tai tallennusta.

Tietokantapalvelimen etuja:

- Tietokantapalvelin mahdollistaa tiedon säilyttämisen yhdessä keskitetyssä paikassa.
- Tietokantapalvelin suorittaa monimutkaisia funktioita kuten haku, järjestely ja indeksointi itse palvelimessa. Tämä vähentää verkkoliikennettä, koska tietoja täytyy siirtää vähemmän asiakkaan ja palvelimen välillä.
- Tietokantapalvelimen tiedot säilytetään keskitetysti, joten on turvallisuus parempi.
- Tietokantapalvelin käyttää omaa prosessointitehoaan tietojen etsimiseen, eikä lähetä kaikkia tietoja käyttäjälle, jotta se voisi etsiä hakemansa tiedon, kuten se tehdään tiedos-

topalvelimella.

- Tietokantapalvelin sallii yhtäaikaisen pääsyn tietoihin. /9/

2.3.6 Tulostuspalvelin

Tulostuspalvelimen (Print/Printing Server) tarkoituksena on jakaa palvelimeen asennettuja tulostimia eteenpäin käyttäjille. Käyttäjät yhdistetään palvelimeen Windows -pohjaisessa tulostuspalvelinjärjestelmässä käyttäen *Microsoft Network Printing Protokollaa*. Tulostuspalvelimen avulla saadaan tulostimet jaettua, hallittua ja nimettyä keskitetysti käyttäjien käyttöön. Palvelimelle voidaan valmiiksi määritellä tulostusjonoja kuten PCL5e, PCL6 tai PostScript tarpeen mukaan ja niihin on myös voitu asettaa valmiiksi mukautettuja tulostusasetuksia. Näitä voivat olla esim. tulostin, jossa oletuksena mustavalkotulostus ja toinen tulostin, jossa oletuksena väritulostus.

Kun tulostin on jaettu tulostuspalvelimella, voi käyttäjä itse helposti lisätä itselleen haluamansa tulostimen, ja aloittaa tulostimen käyttämisen samalla tavalla kuin paikalliskirjoittimen kanssa. Ainoana erona siinä on, että itse tulostusjono sijaitsee tulostuspalvelimella, eikä käyttäjän omalla koneellaan. Tämä ei kuitenkaan näy käyttäjälle erilaisena. /10/

2.3.7 Remote Access / VPN

Remote Access tarkoittaa sananmukaisesti etäpääsyä eli etäyhteyttä haluttuun laitteeseen. Windows 2008 järjestelmässä (myös osassa vanhemmissa) voidaan palvelimelle asettaa *Routing and Remote Access* niminen rooli, jonka avulla palvelimesta voidaan

tehdä reitityspalvelin, jonka tarkoituksena on tuoda reitityspalvelut itse palvelimeen.
VPN:llä (Virtual Private Network) tarkoitetaan tapaa, jolla voidaan esim. yhdistää yksi tai useampi verkko julkisen verkon yli, joista muodostuu näennäisesti yksityinen verkko. Toinen käyttötapa on se, että yrityksen verkkoon voidaan yhdistää tietokone sisäverkon ulkopuolelta ja sallia siltä pääsy yrityksen sisäisiin järjestelmiin.

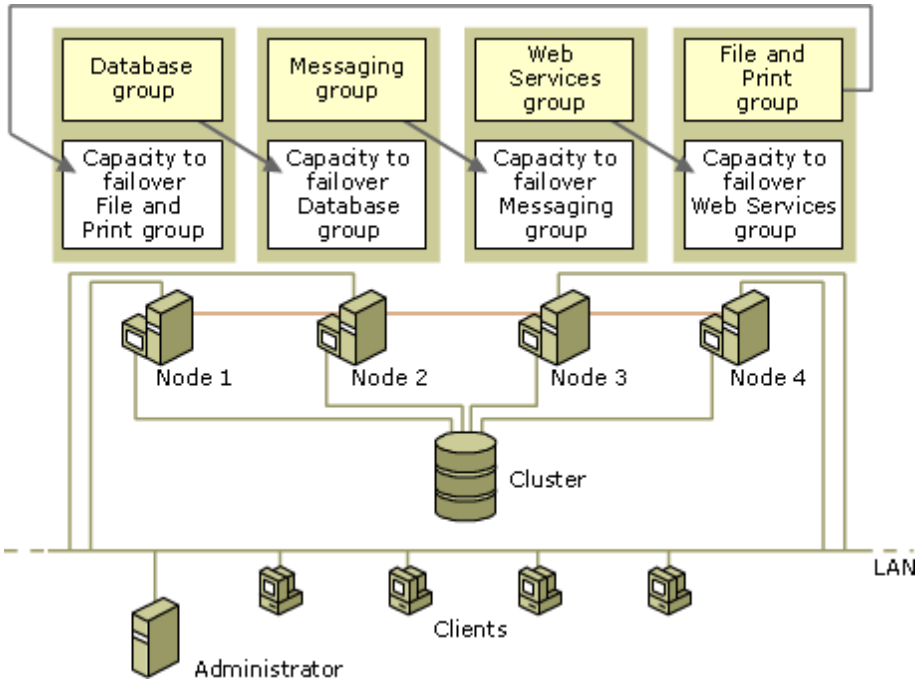
Etäpääsyn avulla voidaan palvelin asettaa palvelemaan edellä mainittuja VPN-palveluja, joka on tärkeänä osana nykypäiväisiä yrityksien järjestelmiä. VPN mahdollistaa täydellisen etätyöskentelyn esim. kotoa tai työmatkoilta, kun Internet-yhteys on saatavilla. Sama palvelu on myös mahdollista toteuttaa hieman rajoitetummin, kun käytetään verkon palomuurilaitetta VPN-pyyntöjen hallitsemiseen. /11/

2.3.8 Server cluster node

Palvelinclusteri (Server Cluster) on ryhmä itsenäisiä tietokoneita, jotka tunnetaan nimellä *nodes*. Nodet työskentelevät yhdessä yhtenä järjestelmänä varmistaakseen kritikaalisten sovellusten ja resurssien saatavuuden. Näiden nodejen käyttöjärjestelmien täytyy olla joko Windows Server 2008, Enterprise- tai Datacenter editioneita. Clusterointi sallii käyttäjien ja järjestelmänvalvojien pääsyn ja hallinnan yhdestä ainoasta järjestelmästä useiden järjestelmien sijaan.

Palvelinclusteri voi sisältää jopa kahdeksan nodea ja clusterit voidaan konfiguroida useilla eri tavoilla. Kuvassa 2 on nähtävissä esimerkki clusterijärjestelmästä, johon kuulu 4 nodea. Kaikki nodet

palvelevat samoja sovelluksia, jolla saavutetaan loistava vikasietoisuus. /12/



Kuva 2. Clusterin rakenne

2.3.9 Terminaalipalvelin

Terminaalipalvelin on terminointiin erikoistunut palvelin joka yhdistää useita kommunikointikanavia yhteen. Koska nämä kanavat ovat kaksisuuntaisia, kaksi mallia paljastuu: useat kokonaisuudet yhdistyy yhteen resurssiin ja yksittäinen kokonaisuus useisiin resursseihin. Molemmat näistä malleista on laajasti käytössä. Kummatkin, sekä fyysiset, että virtuaaliset resurssit voidaan tarjota terminaalipalvelimen kautta: keskitetty tietokoneen käyttö voi tarjota useille käyttäjille pääsyn etäyhteydellä virtuaaliseen käyttöjärjestelmään.

Terminaalipalvelin mahdollistaa ns. tyhmät päätteet, joissa ei ole

varsinaisesti omaa prosessointitehoa, vaan käyttöjärjestelmä ja käyttöliittymä tuodaan käyttäjän näytölle tietoverkon yli eikä käyttäjä huomaa eroa normaaliin järjestelmään. Tällä tavoin järjestelmä tarjoaa paremman tietoturvan, halvemmat kustannukset (voidaan käyttää vanhoja tietokoneita) ja paremman hallittavuuden verrattuna normaaliin järjestelmään, jossa jokaisella käyttäjällä on oma tietokone.

Järjestelmässä on kuitenkin huonotkin puolensa, jos järjestelmää ei ole varmistettu hyvin. Keskustietokoneen hajoaminen, jumiutuminen tai verkkoyhteyksien aiheuttaa kaikkien terminaaliyhteyksien katkeamisen. Tämä voidaan kuitenkin estää esim. käyttämällä clusterijärjestelmää ja kahdennettuja tietoliikenneyhteyksiä, jos palvelu halutaan varmennettua täydellisesti. /13/

2.3.10 WINS-palvelin

WINS-palvelin (*Windows Internet Name Service server*) tarkoittaa palvelinta, joka muuntaa laitteiden NetBIOS nimet IP-osoitteiksi, kuten DNS muuntaa toimialuenimet IP-osoitteiksi. WINS-palvelin mahdollistaa kaikkien asiakaskoneiden nimien pitämisen uniikkeina TCP/IP-verkossa. /14/

2.3.11 Web-palvelin

Web-palvelin tarkoittaa tietokonetta tai ohjelmistoa, joka jakaa dokumentteja HTTP-protokollalla asiakasohjelmille ja koneille. HTML-kielellä kirjoitetut dokumentit muodostavat web-sivuja, jotka voidaan näyttää asiakaskoneessa selainohjelman avulla.

Palvelin ottaa vastaan HTTP-pyyntöjä TCP/IP-verkosta, joko maailmanlaajuisesta Internetistä tai intranetistä ja vastaa niihin. HTTP-pyyntö voi palauttaa HTML-dokumentin, tekstitiedoston, kuvan tai yleensä minkälaisen tahansa tiedoston tai virheen. Lähetettävän tiedoston tyypin kertoo asiakkaalle MIME-tiedostotyyppi. Palvelin voi asettaa myös asiakasohjelmalle pienen määrän dataa, jonka asiakasohjelma palauttaa palvelimelle hakiessaan seuraavaa dokumenttia.

Tietokone voidaan muuttaa palvelimeksi palvelinohjelmiston avulla. Käyttöjärjestelmän on tuettava TCP/IP-verkkoa, ja siinä on oltava Internet-yhteys. Palvelimissa on yleensä kiinteä verkkoyhteys ja pysyvä IP-osoite, jolle on määritelty nimi DNS-nimipalveluun. Web-palvelimien nimi alkaa yleensä 'www.'. /15/

Web-palvelimen asennus Windows 2008 Server käyttöjärjestelmässä on pääpiirteittäin yksinkertainen ja se onnistuu asentamalla roolin nimeltä IIS-service. IIS:n avulla normaali Web-palvelin saadaan pystytettyä. On kuitenkin paljon asioita ja yksityiskohtia, joita täytyy ottaa huomioon omaa web-palvelinta pystyttäessä, kuten mm. tietoturva.

2.3.12 Keskitetty virustorjunta

Nykyajan tietoturvauhkien takia on selvää, että virustorjunta on oltava kunnossa jokaisella yrityksen PC-koneella ja tämän takia suurimmat tietoturvayhtiöt ovat toteuttaneet omia versioitaan keskitetystä virustorjunnasta.

Keskitetyn virustorjunnan tarkoituksena on helpottaa verkon työasemien yhteisten virustorjuntaohjelmien toimintaa. Lähes jokaisella suuremmalla virustorjuntaohjelmavalmistajalla on olemassa yrityksien keskitettyyn käyttöön oleva hallintaohjelmisto. Tämä hallintaohjelmisto pyörii yrityksen itse haluamallaan palvelimella, josta on mahdollista jakaa tietokoneille ajantasainen ja identtinen tai mukautettu virustorjunta ja palomuuriohjelmisto.

Keskitetty virustorjunta nopeuttaa ja helpottaa suuresti yrityksien virustorjuntatilanteen tarkkailua sekä ohjelmien asentamista uusiin tai vanhoihin koneisiin. Hallintaohjelmasta on helppo seurata yrityksen sisäistä tietoturvatilannetta ja se osaa ilmoittaa ja antaa raportteja ylläpitäjälle, jos yritykseen kohdistuu tietoturvauhkia. Aiheeseen syventynyt yrityksen IT-henkilö kykenee rakentamaan palvelun, jonka avulla virustorjunta asentuu automaattisesti yrityksen kaikkiin tietokoneisiin ja rajoittamaan käyttäjän oikeuksia koskien virustorjuntaohjelmiston toimintaa.

Kuvasta 3 on nähtävissä kuinka tietoturvayhtiö F-Securen valmistama Policy Manager toimii periaatteellisesti. /16/

Kuva 3. F-Secure Policy Managerin toiminta

2.4 Active Directory (AD)

Active Directory (AD) on käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista. Se mahdollistaa keskitetyn resurssien jakamisen käyttäjille ja sovelluksille, sekä tarjoaa tavan nimetä, kuvata, paikallistaa, hallita ja suojata käytössä olevia verkon resursseja. AD hakemistopalvelu on sisällytetty Microsoft Windows palvelinkäyttöjärjestelmiin Microsoft Windows Server 2000 lähtien. /17/

2.4.1 Rakenne

Loogiset rakenteet auttavat organisoimaan hakemisto-objekteja ja hallitsemaan verkon tilejä sekä jaettuja resursseja.

AD -palvelulla voidaan luoda sekä loogiset että fyysiset rakenteet verkon osia varten. Loogisia rakenteita ovat:

- Organisatoriset yksiköt (Organizational units)
- Toimialueet (Domains)
- Toimialuepuut (Domain trees)
- Toimialuemetsät (Domain forests)

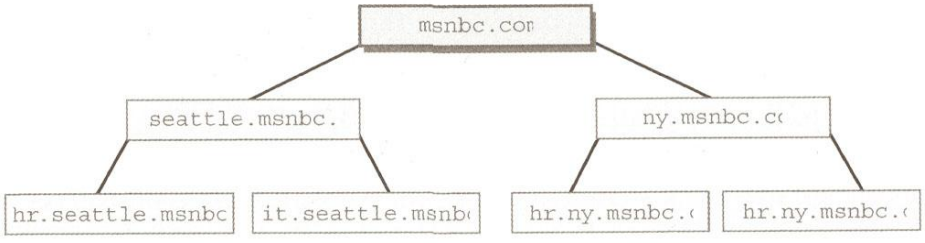
Fyysisiä rakenteita ovat:

- Aliverkot (Subnets)
- Palvelinjoukot (Sites)

2.4.1.1 Toimialueet

Jokaisella AD -toimialueella on DNS-toimialuenimi, kuten tamk.fi. Kun yksi tai useita toimialueita jakavat samat hakemistotiedot, niitä kutsutaan *metsäksi*. Metsän sisällä olevat toimialuenimet voivat olla DNS-nimihierarkiassa *epäjatkuvia* tai *jatkuvia.*

Kun toimialueilla on jatkuva nimeämisrakenne, niiden sanotaan olevan samassa toimialuepuussa. Kuvassa 4 on nähtävissä esimerkki toimialuepuusta, jossa juuritoimialueella msnbc.com on kaksi lapsitoimialuetta: seattle.msnbc.com ja ny.msnbc.com. Näihin toimialueisiin taas kuuluu alitoimialueita. Kaikki toimialueet kuuluvat samaan puuhun, koska niillä on sama juuritoimialue.



Kuva 4. Jatkuva nimeämisrakenne

Epäjatkuvassa nimeämisrakenteessa toimialueessa on kaksi tai useampia erillisiä toimialuepuita. /18/

2.4.1.2 Organisatoriset yksiköt

Organisatoriset yksiköt ovat toimialueiden sisällä olevia aliryhmiä, joiden rakenne usein vastaa organisaation toiminnallista tai liiketoiminnallista rakennetta. Organisatoristen yksiköiden voidaan ajatella olevan loogisia säilöjä, joihin voidaan sijoittaa tilejä, jaettuja resursseja ja muita organisatorisia yksiköitä. Esim. tamk.fi-toimialuetta varten voitaisiin luoda organisatoriset yksiköt nimeltään Opiskelijat, Opettajat ja IT-henkilöt. Tätä mallia voitaisiin myöhemmin laajentaa lisäämällä lapsiyksiköitä. Opiskelijat-yksikkö voisi sisältää lapsiyksiköt Tietotekniikka, Tietojenkäsittely jne.

Organisatoriseen yksikköön sijoitetut objektit voivat olla peräisin vain isätoimialueesta. Esim. teiskontie.tamk.fi-toimialueeseen liitetyt organisatoriset yksiköt voivat sisältää vain tähän toimialueeseen kuuluvia objekteja. Et voi lisätä näihin säiliöihin objekteja finlaysoninkatu.tamk.fi-toimialueesta, mutta voit luoda erillisiä organisatorisia yksiköitä, joiden rakenne vastaa teiskontie.tamk.fi-yksikön liiketoiminnallista rakennetta.

Organisatoristen yksiköiden avulla organisaation liiketoiminnalliseen tai toiminnalliseen rakenteeseen liittyvien objektin organisoiminen on hyvin helppoa. Tämä ei ole kuitenkaan ainoa syy käyttää organisatorisia yksiköitä. Muita syitä käyttää organisatorisia yksiköitä ovat:

- Organisatoristen yksiköiden avulla voidaan määrittää ryhmäkäytäntö toimialueen pientä resurssijoukkoa varten ilman, että ryhmäkäytäntö pitäisi ottaa käyttöön koko toimialueessa. Tämä auttaa asettamaan ja hallitsemaan ryhmäkäytäntöjä organisaation eri tasoilla.

- Organisatoriset yksiköt luovat pieniä, paremmin hallittavissa olevia näkymiä toimialueen hakemisto-objekteista. Tämä auttaa hallitsemaan resursseja tehokkaammin
- Organisatoristen yksiköiden avulla voidaan delegoida valtuuksia ja helposti ohjata toimialueresurssien hallinnallista käyttöä. Tämä auttaa ohjaamaan toimialueessa valvontaoikeuksien laajuutta. Voit esim. sallia käyttäjälle A hallintaoikeuden yhteen organisatoriseen yksikköön, mutta et muihin yksikköihin. Samalla voit sallia käyttäjälle B hallintaoikeuden jokaista toimialueen organisatorista yksikköä varten. /18/

2.4.1.3 Palvelinjoukot ja aliverkot

Palvelinjoukko (*site*) 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 toimialuerakenteen välillä ei välttämällä ole yhteyttä. AD:n 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 mitään yhteyttä.

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 bittimaskista, kuten esimerkiksi 192.168.19.0/24. Tässä verkko-osoite 192.168.19.0 ja aliverkon peite 255.255.255.0 muodostavat yhdessä aliverkon nimeltä 192.168.19.0/24.

Tietokoneet määritetään palvelinjoukkoihin sen mukaan, mikä on niiden sijainti aliverkossa tai aliverkkojoukossa. Jos aliverkkoon kuuluvat tietokoneet voivat kommunikoida tehokkaasti toistensa kanssa verkon kautta, yhteys on hyvin toimiva. Ideaalisessa tilanteessa palvelinjoukko koostuu aliverkoista ja tietokoneista, joiden verkkoyhteys on hyvin toimiva. Ideaalisessa tilanteessa palvelinjoukko koostuu aliverkoista ja tietokoneista, joiden verkkoyhteys on hyvin toimiva. Jos aliverkot ja tietokoneet eivät ole hyvin yhteydessä verkkoon, on ehkä määritettävä useita palvelinjoukkoja. /18/

2.5 Tietoturva

Tietoturva on nykypäivän yrityksissä yksi tärkeimmistä asioista. Yrityksen salaiset tiedot eivät saa missään tapauksessa vuotaa yrityksen ulkopuolelle. Tietoturvaa vaarantavat tietokonevirukset, madot, tietomurrot ja myöskin käyttäjien yleinen huolimattomuus.

Varsinkin uusissa käyttöjärjestelmissä on paljon paikkaamattomia tietoturva-aukkoja, joita kutsutaan haavoittuvuuksiksi. Nämä haavoittuvuudet johtuvat ohjelmointivirheistä, jotka mahdollistavat hakkereiden, virusten ja matojen pääsyn yrityksen verkkoon. Näistä ongelmista tiedotetaan esim. suomalaisella www.cert.fi Internet-

sivustolla.

Näitä uhkia voidaan vähentää yrityksen omien tietoturvakäytäntöjen avulla. Palomuurit, käyttäjien oikeudet, salasanojen vahvuudet, virustorjuntaohjelmistot ja monet muut asiat vaikeuttavat, hidastavat ja estävät uhkien syntyä. /19/

2.6 Varmistus

Tietokonekomponentit eivät koskaan kestä ehjänä ikuisesti ja tämän takia syytä hoitaa tietojen varmistus kunnolla. Vielä muutama vuosi sitten nauhavarmistus oli ainoa varma ja oikea tapa ottaa tiedot talteen palvelinrikon varalta. Nykyään on kuitenkin markkinoille tullut verkkokiintolevyjä, joihin varmennus onnistuu ilman nauhanvaihto-ongelmia. Valitut palvelimen tiedot varmennetaan yhdelle tai useammalle verkkolevylle kokonaisuudessaan tai osittain, jotka voi sijaita joko samassa huoneessa, rakennuksessa tai jopa toisella paikkakunnalla. Nykyajan Internet-yhteysnopeudet ovat nopeudeltaan sellaista nopeusluokkaa, että kaukovarmistukset ovat mahdollisia Internet-yhteyden yli.

Windows Server 2008 tuo mukanaan täysin uuden varmistuspalvelun nimeltään *Windows Server Backup*, joka tukee varmistuslaitteina muistitikkuja, verkkolevyjä ja paikallisia levyjä. Nauhavarmistus ei enää 2008 -versiossa onnistu Windowsin oman työkalun avulla, vaan on käytettävä kolmannen osapuolen sovelluksia, jos haluaa käyttää nauhavarmistusta.

Varmistus suoritetaan käyttäjän asettamana ajankohtana. Varmistus ajoitetaan yleensä yöaikaan, koska silloin ei palvelimella ole

muuta kuormitusta. /20/

3 ASENNUS

Kun yritykseen on valittu laitteistot omia tarpeita varten, voidaan laitteistojen asennus aloittaa. Tässä opinnäytetyön osassa ei käydä läpi itse palvelinlaitteiston asennusta, kuten RAID tai muut asetukset, vaan keskitytään ainoastaan palvelinkäyttöjärjestelmän ja sen roolien ja palveluiden asennukseen.

Seuraavaksi esitetyllä asennustavalla saadaan palvelin saatettua sellaiseen tilaan, jossa palvelimen alkuasetukset on asetettu ja palvelin on hyvällä mallilla kohti todellista toimintaympäristöä. Todellisessa yritysympäristössä on paljon asioita (palvelimen asetuksia ja ulkoisia tekijöitä), joita täytyy ottaa huomioon, ennen kuin palvelin aiotaan asettaa toimintaan.

3.1 Palvelinkäyttöjärjestelmän asennus

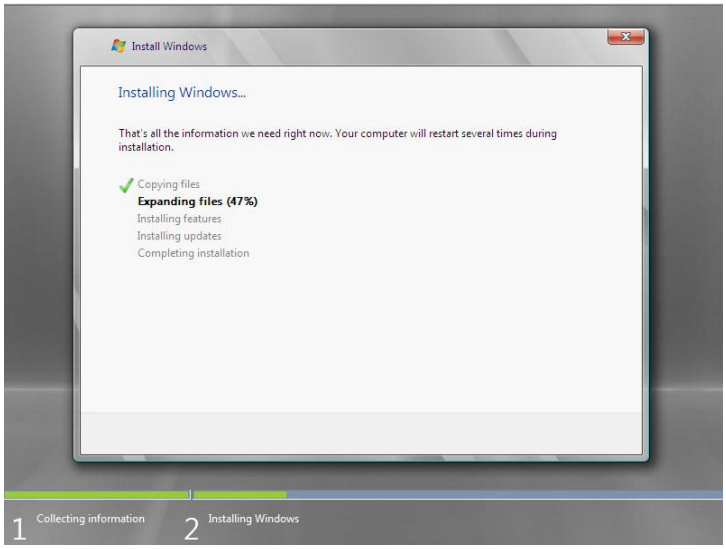
Testipalvelimeen tullaan tässä asennuksessa asentamaan Windows Server 2008 Enterprise käyttöjärjestelmä. Palvelimelle asetetaan seuraavat roolit ja palvelut: DC, DNS-palvelin, DHCP-palvelin, WINS-palvelin, tiedostopalvelut, terminaalipalvelin ja tulostuspalvelin. Kaikkiin rooleihin ja palveluihin ei kuitenkaan kiinnitetä tarkempaa huomiota, vaan ne annetaan olla oletusasetuksilla.

Itse käyttöjärjestelmän asennus on hyvin yksinkertaista. Asennus käynnistyy asennusmedialta automaattisesti palvelimen käynnistyessä, kun asennusmedia on koneen sisällä. Asennus etenee seuraavassa järjestyksessä:

1. *Valitse kieliasetukset --> Valitse Install --> Syötä tuoteavain --> Valitse Full Installation --> Hyväksy lisenssiehdot.* Seuraavaksi voidaan valita joko päivitys tai muokattu asennus. Päivitysasennuksella on mahdollista päivittää vanha Windows Server käyttöjärjestelmä uuteen versioon ja muokatulla valinnalla asennetaan täysin uusi käyttöjärjestelmä.

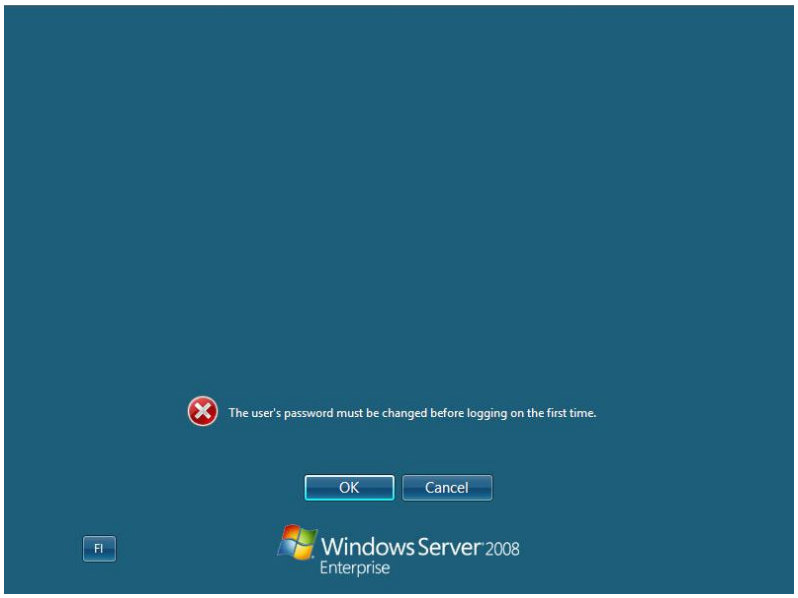
2. Tässä työssä asennetaan käyttöjärjestelmä tyhjälle pohjalle, joten *valitaan Custom (advanced).* Seuraavassa ikkunassa voidaan osioida kiintolevy haluttuun kokoon. Windows Server 2008:n suositeltu asennusosion koko on 40 GT (minimi 10 GT), joten jos mahdollista, niin luodaan vähintään 40 GT:n osio. Kun osio on luotu valitaan osio ja painetaan *next.*

   Kun aiemmat valinnat on tehty itse käyttöjärjestelmän asennus alkaa (kuva 5) ja käyttöjärjestelmä asentuu automaattisesti loppuun. Asennusaika voi vaihdella kymmenestä minuutista puoleen tuntiin riippuen koneen suorituskyvystä. Tietokone käynnistyy kaksi kertaa uudestaan asennuksen aikana.



Kuva 5. Käyttöjärjestelmän asennusruutu

3. Asennuksen päätyttyä käyttäjää pyydetään asettamaan järjestelmänvalvojan salasanan (kuva 6). Salasanan täytyy olla 8 merkkiä pitkä ja sen täytyy sisältää vähintään yksi iso kirjain ja numero. Tämä salasana on koneen pääkäyttäjän salasana ja se on hyvä olla ainoastaan järjestelmänvalvojien tiedossa tietoturvasyistä.

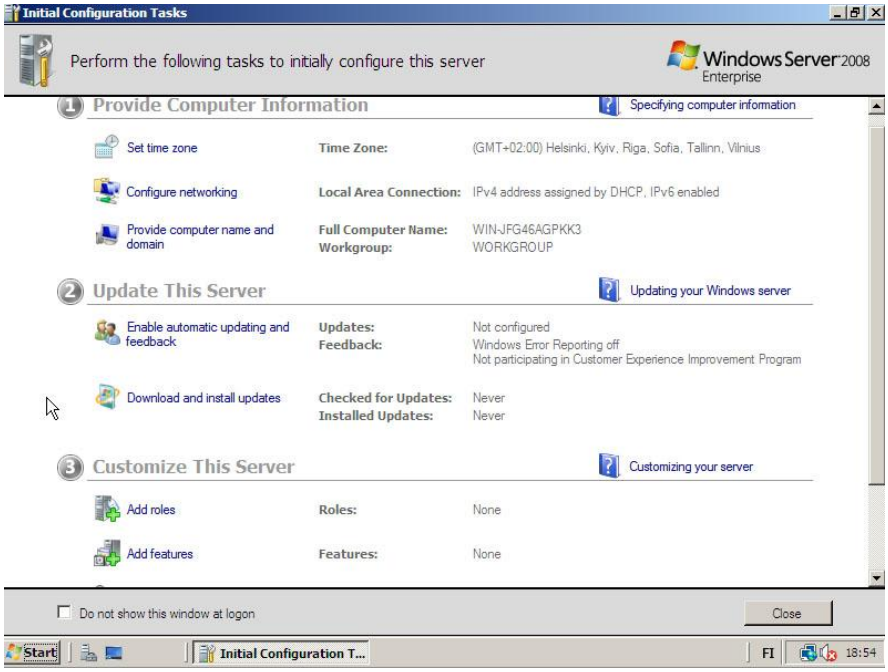


Kuva 6. Salasanan vaihtoilmoitus

3.2 Normaalien asetusten ja roolien määritys

Salasanan vaihdon jälkeen käyttöjärjestelmä käynnistyy perustilaan ja ruutuun tulee *Initial Configuration Tasks* -ikkuna (kuva 7). Tästä ikkunasta nähtävillä suositeltu perusasetusten ja ominaisuuksien (alkuasetusten) määritysjärjestys, joka on seuraava:

1. Aseta aikavyöhyke.
2. Aseta verkkoasetukset.
3. Aseta koneen verkkonimi ja toimialue.
4. Aseta automaattisten päivitysten ja virheraporttien asetukset.
5. Lataa ja asenna päivitykset.
6. Lisää rooleja.
7. Lisää ominaisuuksia.
8. Aktivoi etähallinta.
9. Konfiguroi Windowsin palomuuri.

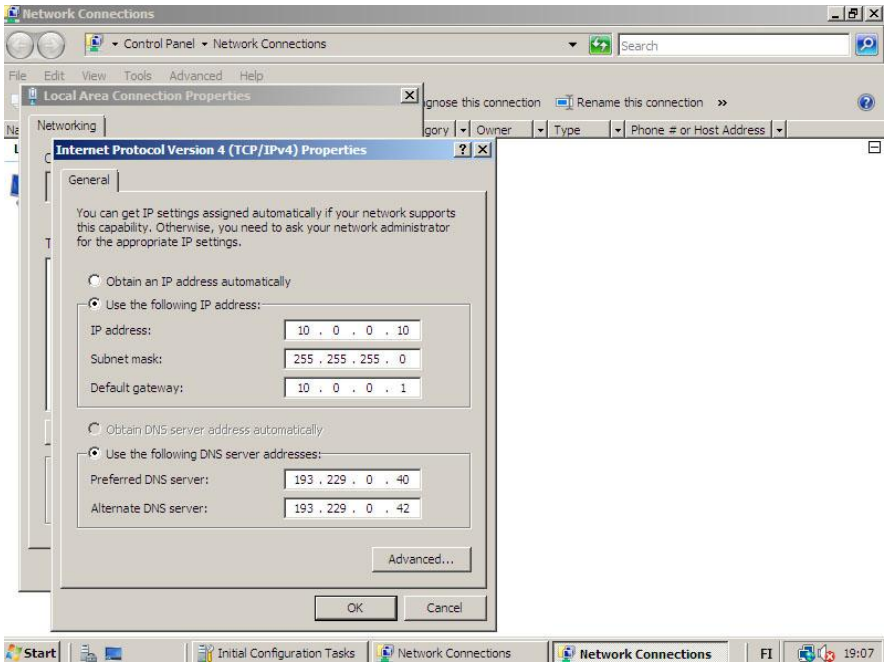


Kuva 7. Alkuasetusruutu

Asetukset voidaan määritellä painamalla haluttua kuvaketta, josta aukeaa kyseisen ominaisuuden määritysikkuna.

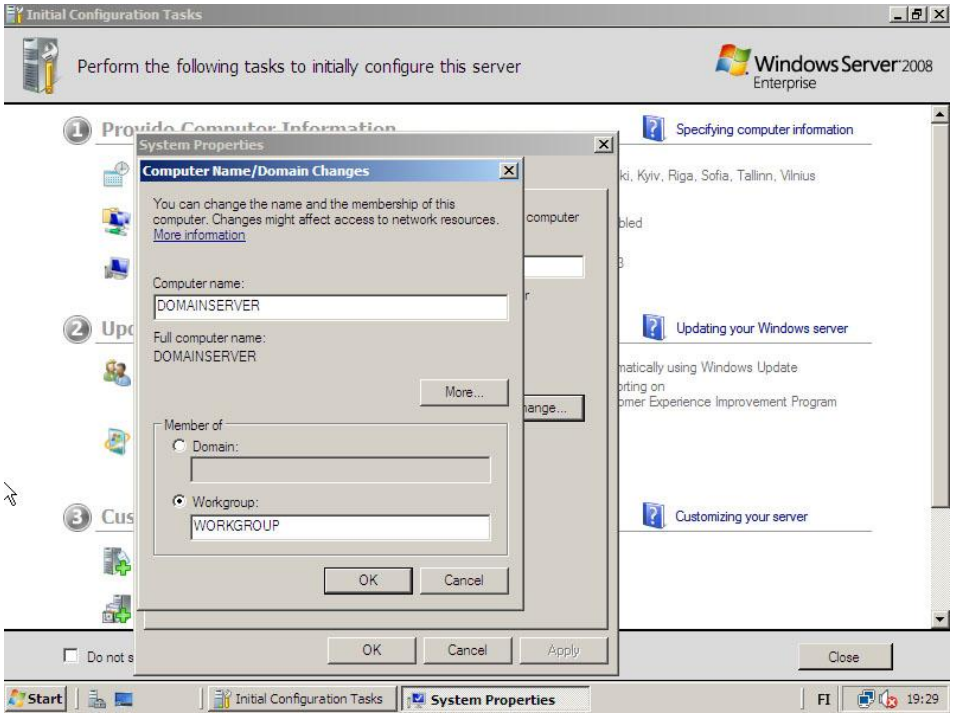
1. Aikavyöhyke on useimmiten heti asennuksen jälkeen oikein, kun asennusvaiheessa valittiin kieliasetukset, jonka mukaan aikavyöhyke asettuu.

2. Verkkoasetukset tulee määrittää kerralla oikein, koska myöhemmin asennettava toimialueen ohjainpalvelin käyttää näitä staattisia verkkoasetuksia toimialueen DNS-nimen luomiseen. Tähän palvelimeen asetetaan palvelimen IP-osoitteeksi 10.0.0.10, aliverkon peitteeksi 255.255.255.0 ja oletusyhdyskäytäväksi 10.0.0.1. DNS-palvelimiksi asetetaan Elisan DNS-palvelimet 193.229.0.40 ja 193.229.0.42 (kuva 8). DNS-palvelimet riippuvat palveluntarjoajasta, joten käytä niitä DNS-palvelimia, joita palveluntarjoajasi suosittelee.



Kuva 8. Verkkoasetukset

3. Koneen verkkonimi on hyvä olla tiedossa jo ennen kuin tähän asti päästään, koska se tulee olemaan toimialueen ohjauspalvelimen verkkonimi. Verkkonimen pääsee vielä tässä vaiheessa muuttamaan (toimialueen ohjauspalvelimen asentamisen jälkeen tämä ei ole mahdollista), kun valitaan kuvake ikkunasta ja valitaan *Change.* Tässä palvelimessa nimeksi asetetaan DOMAINSERVER ja koska toimialuetta ei vielä ole, niin annetaan oletustyöryhmän olla valittuna (kuva 9). Jos palvelin liitettäisiin valmiina olevaan toimialueeseen, niin *Domain* valintaan voitaisiin asettaa olemassa oleva toimialue.



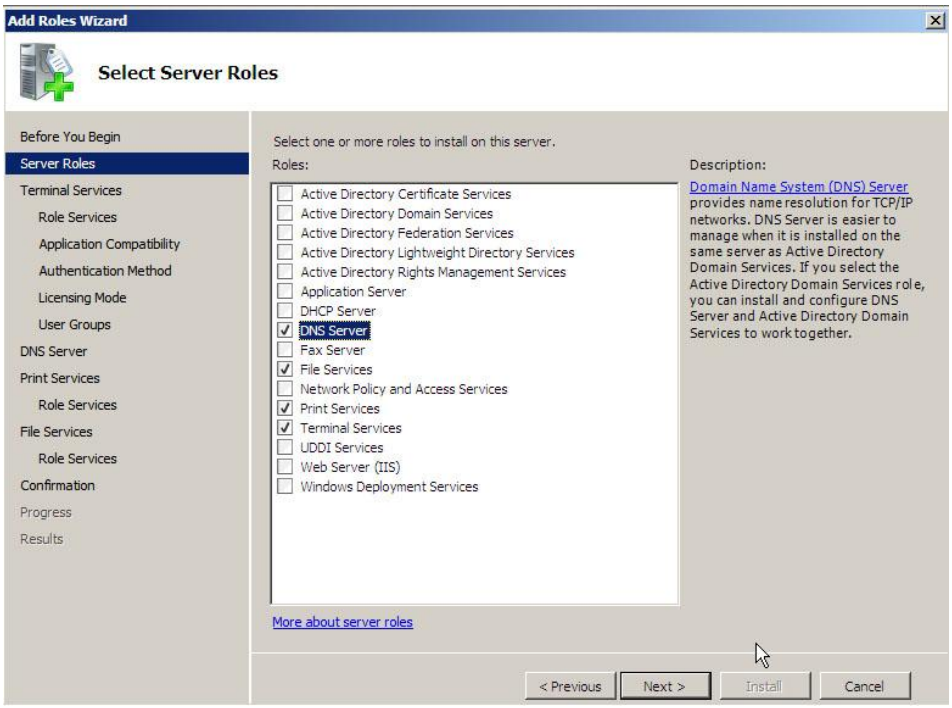
Kuva 9. Koneen verkkonimi ja toimialue

4. Automaattiset päivitykset kuvaketta painettua avautuu ikkuna, josta voidaan valita, joko automaattiset Windows update oletusasetukset tai määritellä tarkemmin valitsemalla *Manually configure settings.* Automaattiasetukset riittävät normaalisti, mutta joissakin tapauksissa palvelimen päivitykset halutaan ajaa tiettynä ajankoh-

tana tai eri muodossa, niin silloin voidaan mennä tarkempiin asetuksiin.

5. Päivitykset lähtevät latautumaan, kun painetaan kuvaketta ja valitaan *Check for updates*. Verkkoasetukset tulee olla oikein ja yhteys internettiin on oltava olemassa, koska ilman niitä päivityksiä ei voida hakea.

6. Roolien lisäysvalinnasta päästään lisäämään rooleja. Avautuvaan ikkunaan valitaan *next*, josta päästään roolien valintaikkunaan (kuva 10).

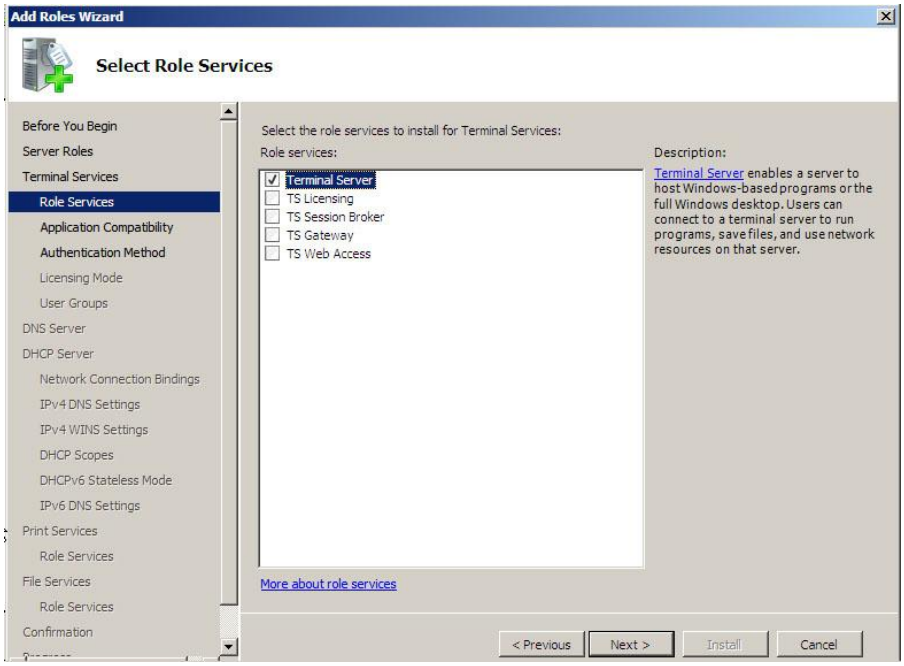


Kuva 10. Roolien valinta

Rooleiksi valittiin DNS Server, File Services, Print Services ja Terminal Services. Samasta ikkunasta on myös mahdollista määrittää DC rooleja, mutta ne käydään läpi erikseen. Jokaista roolia varten on oikealla *Description* lisätietopalkki, joka kertoo kunkin

roolin merkityksen. Terminaalipalvelin ominaisuuksia ei sinällään tarvita, mutta ne asennetaan sen takia, että tarvittaessa saadaan mahdollistettua järjestelmänvalvojalle toinen samanaikainen työpöytä palvelimelle.

Roolien valinnan jälkeen painetaan *next* ja ruutuun avautuu lisävalintaikkuna liittyen terminaalipalvelin (kuva 11). Tästä ikkunasta valitaan ainoastaan *Terminal Server*, joka riittää haluttuihin terminointiominaisuuksiin.



Kuva 11. Terminaalipalvelimen lisävalinnat

Seuraavaksi kysytään kysymys liittyen etätyöpöytäohjelman autentikointiin. Näistä voidaan valita joko verkkotason autentikointi tai ilman sitä. Verkkotason autentikointi vaatii, että käyttäjän koneessa käytetään jotain ennalta määrättyä sertifikaattia käyttäjien tunnistamiseen. Normaalissa tilanteessa sitä ei käytetä, joten valinta on *Do not require Network Level Authentication.*

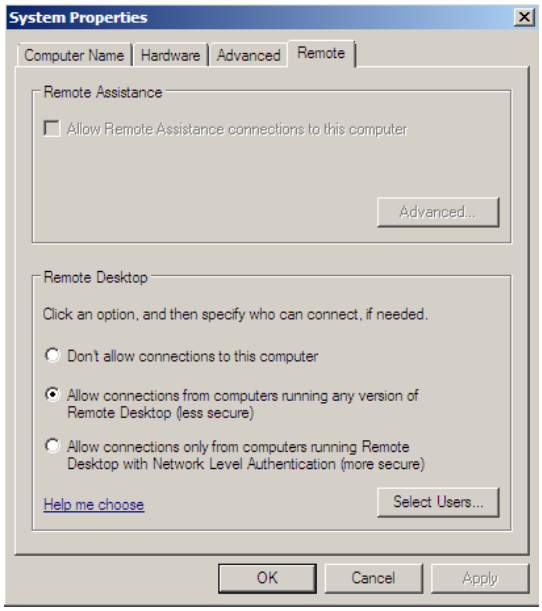
Seuraavaksi kysytään kysymys liittyen terminaalipalvelin lisen-

sointiin. Tässä tapauksessa terminaalipalvelinta ei käytetä muuhun kuin järjestelmänvalvojan käyttöön, joten asetuksella ei ole merkitystä. Seuraavassa ikkunassa kysytään myös terminaalipalvelin käyttäjäryhmiä ja oletuksena oleva Administrators on riittävä.

Print Services ja *File Services* roolit voivat olla oletusasetuksilla tässä tapauksessa. File Services valinnoista on mahdollista lisätä esim. tiedostojen replikointipalvelu toisten palvelinten kanssa, mutta tässä tapauksessa se ei ole tarpeen.
Tämän jälkeen voidaan aloittaa asennus painamalla Install-painiketta. Asennuksen jälkeen pyydetään käyttäjää käynnistämään kone uudestaan, joka on välttämätön toimenpide.

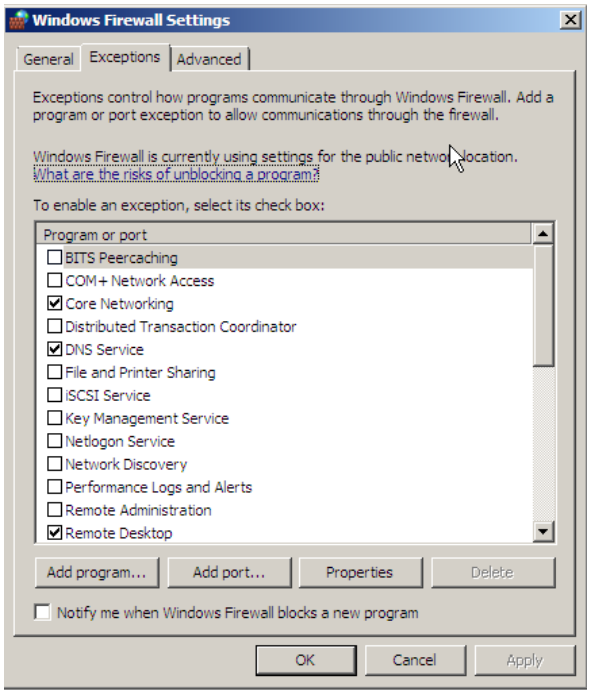
7. Ominaisuuksien lisäysvalinnasta päästään ikkunaan, josta voidaan lisätä palvelimelle ominaisuuksia. Tässä asennuksessa valitsemma ainoastaan *WINS Server* ominaisuuden ja valitsemme *next* → *Install*.

8. Etätyöpöytäyhteyden palvelimeen saadaan mahdollistettua painamalla *Enable Remote Desktop* kuvaketta ja valitsemalla ikkunasta *Allow connections from computers running any version of Remote Desktop* -valinta (kuva 12). Tämä valinta on jo aktiivinen, koska koneeseen on aiemmin asennettu terminaalipalvelin.



Kuva 12. Etätyöpöytäyhteyden aktivointi

9. Windowsin palomuuri on oletuksena päällä, mutta jos on tarvetta tehdä erikoisia muutoksia, niin se on mahdollista palomuurin asetusten *Exceptions* välilehdeltä (kuva 13).



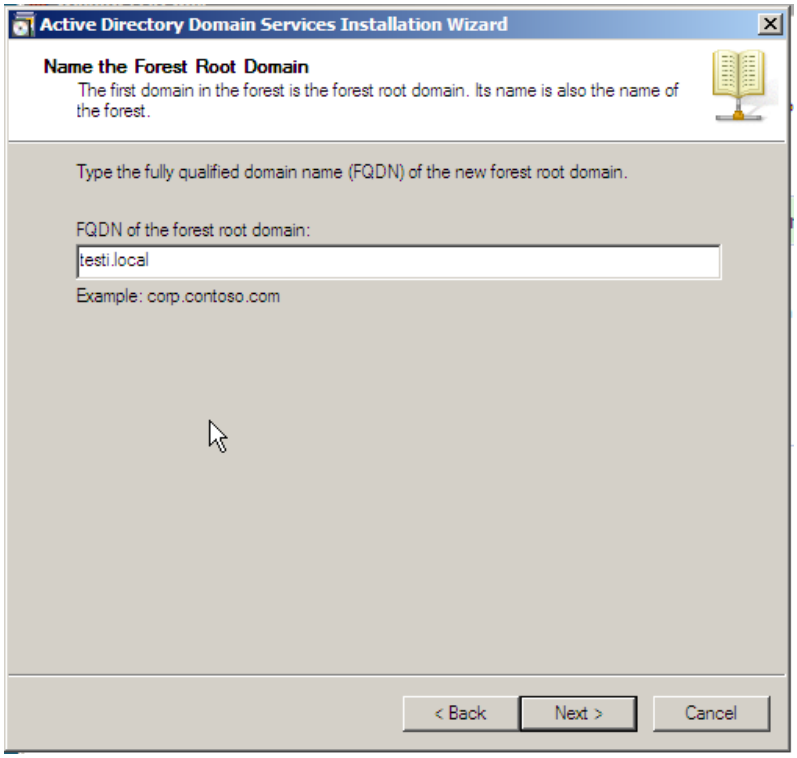
Kuva 13. Windowsin palomuurin poikkeusehdot

Tarkkoihin palvelimen roolien asetuksiin ja ominaisuuksiin päästään käsiksi *administrative toolsien* kautta, jotka ovat löydettävissä start-valikosta.

3.3 DC:n asennus

DC voidaan asentaa, joko ennen tai jälkeen roolien asentamisen, mutta etukäteen asennettuna täytyy DNS-palvelin asentaa DC:n asentamisen yhteydessä. Toimialueen ohjauspalvelin ominaisuuden asennus käynnistyy painamalla *Start* ja kirjoittamalla hakukenttään *dcpromo*. Asennusohjelma latautuu hetken aikaa, jonka jälkeen ruutuun tulee asennusikkuna.

Uutta toimialuetta asentaessa ei tarvita edistyneitä asetuksia, jotka ovat valittavana ensimmäisessä asennusikkunassa. Asennusohjelman edetessä kysytään käyttäjältä luodaanko uusi vai vanha toimialue, johon valitaan uusi. Seuraavaksi kysytään *FQDN of the forest root domainia*, jolla tarkoitetaan sitä toimialue-nimeä, joka verkkoon halutaan asettaa. Jos palvelinta käytetään ainoastaan lähiverkossa, niin on syytä käyttää toimialue-nimeä kuten *testi.local* (kuva 14). Jos palvelinta taas käytetään oikeana Internetin toimialue-palvelimena, niin voidaan käyttää esim. *testi.com* toimialue-nimeä, jossa testi.com on yrityksen tai muun yhteisön oma verkkotunnus.



Kuva 14. Toimialuenimen asetus

Seuraavaksi käyttäjältä kysytään metsän toimintatasoa. Toimintatasoja on 3, jotka ovat 2000, 2003 ja 2008. Jos palvelin on ainoa toimialueen ohjauspalvelin, joka verkossa tulee olemaan, niin ei ole tarvetta käyttää muuta tasoa kuin 2008. Jos käytössä on muita toimialueen ohjauspalvelimia, jotka halutaan liittää samaan metsään, voidaan taso muuttaa siinä tapauksessa tasoa vastaavaksi.

Tämän jälkeen asennusohjelmassa kysytään vielä toimialueen pääkäyttäjän salasanaa, joka on syytä olla vahva ja tiedossa ainoastaan järjestelmänvalvojalla. Seuraavassa käynnistyksessä tämä on ainoa salasana, jota voidaan käyttää palvelimeen kirjautumisessa. Tämän jälkeen asennus viedään loppuun ja palvelin on käynnistettävä uudestaan asennuksen päätyttyä.

Jos on tarvetta asentaa palvelin DHCP-palvelin rooliin, niin se on

syytä tehdä kun DC:n asennus on saatu loppuun. DHCP-palvelimen asennus onnistuu uuden roolin lisäämisen kautta. DHCP-palvelimen asennuksen yhteydessä täytyy määrittää DHCP-alue ja palvelimen avulla jaettavat tiedot.

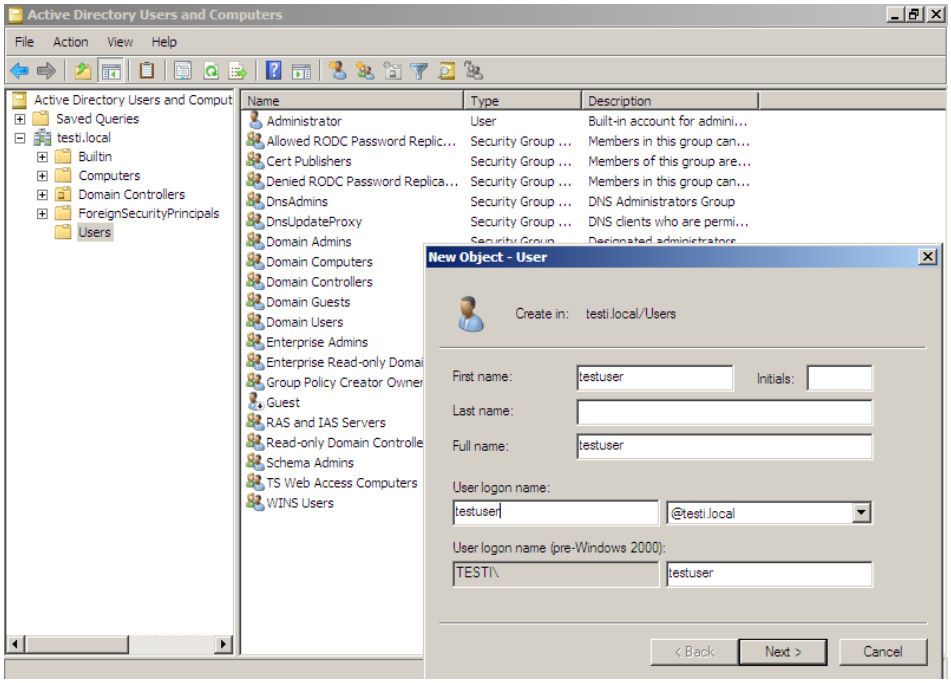
3.4 DC:n asetukset

Kun kaikki tarvittavat roolit ja ominaisuudet on asennettu, on syytä syventyä DC:n eri asetuksiin. Palvelin ja toimialue on tällä hetkellä täysin toimintakuntoinen, mutta toimialueelle ei ole tehty käyttäjätilejä. Tietokoneet täytyy liittää toimialueelle käsin ja ne ilmestyy AD:n *Computers* osaston alle.

3.4.1 Käyttäjien ja ryhmien lisäys

Käyttäjien lisääminen on hyvin yksinkertaista, mutta tarkempien käyttäjäoikeuksien määritteleminen vie aikaa ja vaivaa.

Käyttäjien lisääminen onnistuu *Active Directory Users and Computers* hallinnasta, joka löytyy *administrative toolseista*. Käyttöliittymä on nähtävissä kuvasta 15, jossa on käyttäjän lisäys käynnissä. Käyttäjä voidaan lisätä valitsemalla *Action --> New --> User.* Käyttäjästä kysytään etu- ja sukunimi sekä kirjautumisnimi toimialueelle. Seuraavassa ruudussa kysytään salasanaa, joka käyttäjälle asetetaan sekä muita mahdollisia salasanapolitiikkoja. Salasanan täytyy olla vahva jo Windows Server 2008 oletusasetuksilla, joten esim. *password* ei käy salasanaksi, mutta taas *P@ssw0rd* käy.



Kuva 15. Käyttäjän lisääminen AD:n

Kun käyttäjä on lisätty, se lisätään automaattisesti *Domain Users* käyttäjäryhmään, joka tarkoittaa sitä, että käyttäjällä on oikeus kirjautua toimialueella. Käyttäjällä on kuitenkin rajoitetut käyttöoikeudet, joten tietokoneen asetusten muuttaminen ei onnistu.

Kuvan 15 listassa näkyy automaattisesti luotuja oletuskäyttäjäryhmiä, joille on valmiiksi määritelty oikeuksia eri toimintoihin. Käyttäjiä voidaan lisätä näihin käyttäjäryhmiin valitsemalla haluttu käyttäjä ja valitsemalla *Action → Add to a Group*. Ryhmää voidaan hakea nimellä ja lisätä ryhmään painamalla ok. Tietokoneiden ryhmiin onnistuu samalla tavalla, kun haetaan vain haluttu tietokone *Computers* osaston alta.

Uusien käyttäjäryhmien lisääminen onnistuu lähes samalla tavalla kuin uudenkin käyttäjän. Lisääminen onnistuu kun valitaan *Action → New → Group* ja lisätessä kysytään ryhmän nimeä sekä ryh-

män laajuuksia, mutta normaalisti ei tarvitse asettaa kuin ryhmän nimi ja ryhmän lisäys on valmis.

On syytä olla tarkkana käyttäjille myönnettyjen oikeuksien kanssa. *Domain Admins* ryhmään ei pitäisi päästää ketään käyttäjää, joka sitä ei oikeasti tarvitse, koska tällä käyttäjällä on täydet oikeudet toimialueen tietokoneisiin ja tällä tavoin lisää tietoturvariskiä.

3.4.2 Käyttäjien asetusten määritys

Yksittäisten käyttäjien tarkempien asetuksien määritykseen päästään käsiksi kun valitaan käyttäjä ja sen jälkeen *Action* → *Properties*. Yksittäiselle käyttäjälle saadaan määriteltyä tarkempia yhteystietoja, profiilin voimassaoloaikoja, profiilin polkuja, kotikansioita, ryhmiä yms.

3.4.2.1 Kirjautumisscriptit

Kotikansioiden ja kirjautumisscriptien asetus on usein tarpeellinen käyttäjille. Nämä voidaan ohjata myös *Group Policy Objektien* (GPO) avulla, mutta yksittäisten käyttäjien omat asetukset määritetään tätä kautta. Sisäänkirjautumisscriptit voivat olla, joko .cmd, .bat, .js tai .vbs muotoisia. Näiden scriptien avulla voidaan käyttäjälle määrittää esim. useita verkkoasemia. Scriptit ajetaan, kun käyttäjä kirjautuu toimialueen tietokoneella sisään verkkoon. Alla esimerkki kirjautumisscriptistä, jossa käyttäjälle asetetaan kaksi verkkoasemaa:

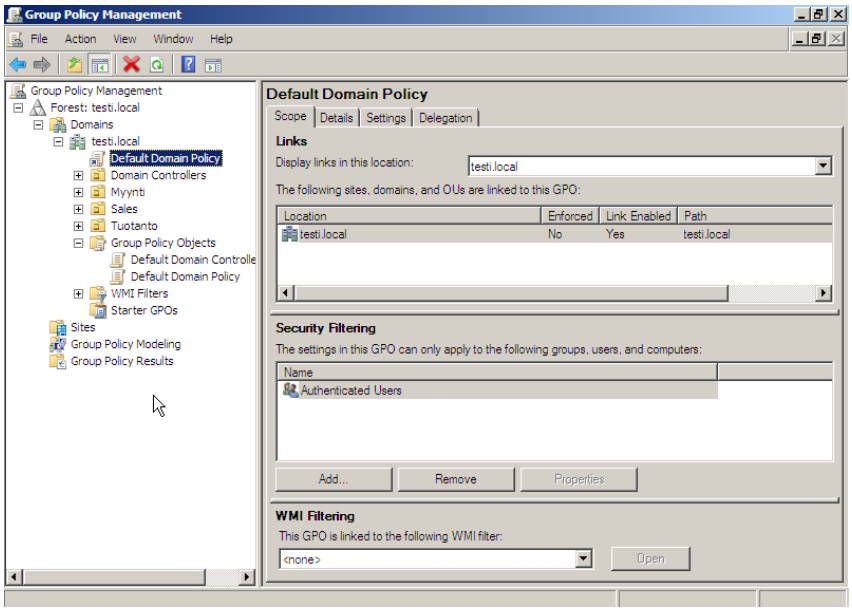
```
net use x: "\\testipalvelin\kotikansiot\%username%"
net use z: "\\testipalvelin\yhteiset\myynti"
```

Scriptissä lainausmerkkien sisässä olevat tekstit esittää verkko-osoitetta verkkojakoon.

3.4.3 Tilikäytännöt (GPO)

Tilikäytännöillä tarkoitetaan oikeuksia ja asetuksia, joita voidaan linkittää ryhmille, koneille tai yksittäisille käyttäjille. Tilikäytäntöjä päästään muuttamaan *Group Policy Managementin* kautta, joka löytyy myöskin *administrative toolseista.* Ryhmille, koneille ja käyttäjille voidaan määritellä satoja erilaisia oikeuksia ja asetuksia, joten niitä ei kannata alkaa luettelemaan.

Kuvasta 16 on nähtävissä GPM:n hallintaliittymä. Tilikäytäntöjä hallitaan objekteilla, joita voidaan luoda tai muokata ja ne voidaan asettaa koskemaan tiettyjä käyttäjäryhmiä tai käyttäjiä.

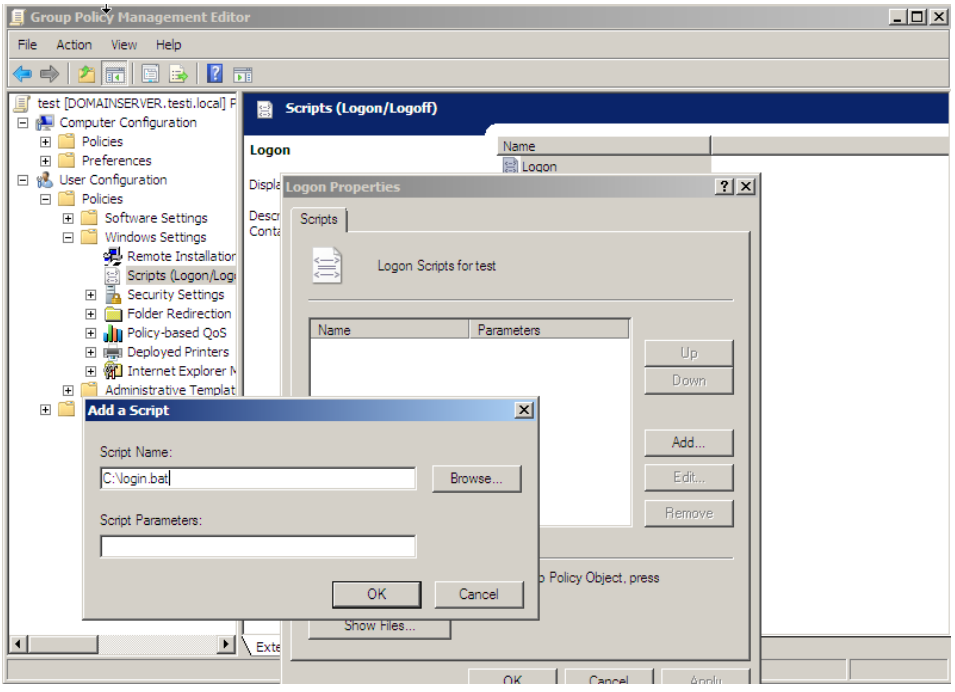


Kuva 16. Group Policy Management hallintaliittymä

Kuvassa 16 on myös nähtävissä oikealla *Security Filtering* alue, johon voidaan määritellä ryhmät, koneet ja käyttäjät, joita ko. objekti ja sen asetukset koskee.

Objektit luodaan Group Policy Objects kansion alle, josta löytyy valmiiksi *Default Domain Policy* objekti, jolla voi määritellä koko toimialuetta koskevia asetuksia. Uuden objektin saa luotua *Action → New* ja syötetään objektia kuvaava nimi. Valittua objektia päästään muokkaamaan valitsemalla haluttu objekti ja *Action → Edit..*

Kuvassa 17 on nähtävissä objektien muokkausliittymä. Kuvassa on määrittelyssä objekti, jolla määritellään objektiin kirjautumisskripti (logon.bat), jota objektiin linkitetyt ryhmät tai käyttäjät käyttävät kirjautuessaan toimialueelle.



Kuva 17. GPO:n muokkaus

3.4 Tiedostopalvelun käyttöönotto

Yksinkertaisen kansiojaon saadaan tehtyä, kun selataan resurssienhallinnasta haluttuun sijaintiin, valitaan haluttu kansio hiiren oikealla napilla ja valitaan *Share.* Tämän jälkeen kysytään käyttäjiä ja/tai ryhmiä joille sallitaan pääsy kansioon. *Share* nappia painamalla kansio on jaettu, ja käyttäjät joilla on oikeudet verkkokansioon pääsevät kirjautumaan kansioon toisilta tietokoneilta.

4 LOPPUPÄÄTELMÄT JA TULEVAISUUS

Tämä pintaraapaisu Windows Server 2008 palvelinkäyttöjärjestelmään antoi todella paljon näkemystä Windows palvelimen tarpeellisuudesta ja toimintatavoista yrityskäytössä. Tiedonhaun yhteydessä huomasin, että aikaisempi kokemus Microsoftin palvelinkäyttöjärjestelmistä ei ollutkaan niin vahva kuin olisi voinut alun perin kuvitella. Näillä lisätiedoilla on kuitenkin helppo edetä eteenpäin, ja aiheeseen liittyvästä kirjallisuudesta löytyy tarkemmin tietoa palvelimen lisäominaisuuksista.

Uusi Windows Server 2008 palvelin tullaan asentamaan kesän 2009 aikana Datagroup Pirkanmaan Konttorikone Oy:n toimitiloihin. Palvelimen on tarkoitus korvata vanhat Windows Server 2000 ja 2003 palvelimet ja tällä tavalla keskittää palvelut yhdelle palvelimelle. Tämä vähentää ylläpidon tarvetta ja on samalla ekologisempi ratkaisu.

LÄHTEET

1 Windows NT käyttöjärjestelmät ja niiden julkaisuajankohdat [Viitattu 22.3.2009]
http://en.wikipedia.org/wiki/Windows_NT

2 Windows Server 2008 käyttöjärjestelmäversiot [Viitattu 3.5.2009]
http://www.microsoft.com/windowsserver2008/en/us/editions-overview.aspx
Jyrki Kivimäki, Windows Server 2003 Active Directory. Readme.fi 2005, s. XXIII

3 Palvelimen roolit
William R. Stanek, Microsoft Windows 2003 Server asiantuntijan käsikirja. Edita Prima Oy 2003. s. 7

4 DHCP-palvelin
Eriq Oliver Neale, Microsoft Small Business Server 2003 Unleashed. Sams Publishing 2006. s. 96-97

5 DNS-palvelin
Eriq Oliver Neale, Microsoft Small Business Server 2003 Unleashed. Sams Publishing 2006. s. 87-88

6 DNS-kyselyn periaatteellinen toiminta [Viitattu 19.4.2009]
http://en.wikipedia.org/wiki/File:An_example_of_theoretical_DNS_recursion.svg

7 DC [Viitattu 6.5.2009]
http://technet.microsoft.com/en-us/library/cc786438.aspx
Melissa M. Meyer, Michael Cross, Hal Kurz, Brian Barber, Windows Server 2003 Active Directory Infastructure. Syngress 2006. s. 17-18

8 Tiedostopalvelin, Tietojen jakaminen
William R. Stanek, Microsoft Windows 2003 Server asiantuntijan käsikirja. Edita Prima Oy 2003. s. 315-320

9 Tietokantapalvelin [Viitattu 19.4.2009]
http://www.it.lut.fi/kurssit/04-05/010626000/linux-tyot/Tietokantapalvelimet-Mikko_Pehkonen-raportti.pdf
http://www.articleworld.org/Database_server

10 Tulostuspalvelin
William R. Stanek, Microsoft Windows 2003 Server asiantuntijan käsikirja. Edita Prima Oy 2003. s. 421-423

11 Remote Access / VPN
Eriq Oliver Neale, Microsoft Small Business Server 2003 Unleashed. Sams Publishing 2006. s. 145, 155

12 Server cluster node [Viitattu 19.4.2009]
https://technet.microsoft.com/en-us/library/cc783804.aspx

13 Terminaalipalvelin
Eriq Oliver Neale, Microsoft Small Business Server 2003 Unleashed. Sams Publishing 2006. s. 163-165

14 WINS
William R. Stanek, Microsoft Windows 2003 Server asiantuntijan käsikirja. Edita Prima Oy 2003. s. 469-471

15 Web-palvelin [Viitattu 19.4.2009]
http://www.pcmag.com/encyclopedia_term/0,2542,t=Web+server&i=54342,00.asp

16 F-Secure Policy Manager toiminta [Viitattu 19.4.2009]
http://www.f-secure.fi/export/system/fsgalleries/datasheets/fin-fsavsbs.pdf

17 AD, Peruskäsitteet
Jyrki Kivimäki, Windows Server 2003 Active Directory. Readme.fi 2005, s. 1

18 AD, Rakenne
William R. Stanek, Microsoft Windows 2003 Server asiantuntijan käsikirja. Edita Prima Oy 2003. s 133-140

19 Tietoturva
Eriq Oliver Neale, Microsoft Small Business Server 2003 Unleashed. Sams Publishing 2006. s. 177-179

20 Varmistus [Viitattu, 5.5.2009]
http://technet.microsoft.com/en-us/library/cc770266.aspx