VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Henri Mäenpää

DOMAIN-SUUNNITELMA

Tekniikka ja liikenne
2010

VAASAN AMMATTIKORKEAKOULU

Tietotekniikan koulutusohjelma

TIIVISTELMÄ

Tekijä	Henri Mäenpää
Opinnäytetyön nimi	Domain-suunnitelma
Vuosi	2010
Kieli	suomi
Sivumäärä	61
Ohjaaja	Antti Virtanen

Tämän opinnäytetyön tarkoituksena oli tehdä suunnitelma ja mitoitus verkon peruspalveluille noin 3500 hengen kokoiselle organisaatiolle. Vaasan ammattikorkeakoulun tietoverkon rakenne toimi työssä esimerkkinä, jonka perusteella palvelut suunniteltiin ja mitoitettiin. Opinnäytetyöstä toteutettiin myös pieni osa harjoitustyöksi.

Suunnitelmassa ja mitoituksessa huomioitiin erityisesti verkon peruspalvelut, joihin kuului Active Directory-, DHCP-, DNS-, levy- ja tulostinpalvelut. Windows Server 2008 R2 -käyttöjärjestelmää käytettiin palvelujen toteuttamiseen. Lähteenä työssä toimi erityisesti Microsoftin materiaalit.

Harjoitustyössä suunnitelmasta toteutettiin pienen yritysverkon peruspalvelut. Verkko rakennettiin kolmen palvelimen avulla. Verkkoa suunniteltaessa täytyi erityisesti huomioida mihin palvelut sijoitetaan ja miten verkosta saataisiin vikasietoinen. Kaikkia palveluita ei pystytty asentamaan jokaiselle serverille, vaan ne täytyi jakaa niin, että tärkeillä palveluilla oli varmennus kahdella serverillä. Harjoitustyössä keskityttiin myös Active Directoryn -käyttäjien ja -ryhmien luontiin sekä niiden hallintaan.

Verkon peruspalvelut voidaan toteuttaa monilla eri tavoilla ja organisaationrakenteella on paljon vaikutusta niihin. Yhtä oikeaa tapaa ei ole, joten tässä työssä keskityttiin erityisesti Microsoftin tarjoamiin materiaaleihin, joiden perusteella peruspalvelut suunniteltiin ja mitoitettiin.

Asiasanat: Windows Server 2008, Active Directory, DHCP, DNS

VAASAN AMMATTIKORKEAKOULU

UNIVERSITY OF APPLIED SCIENCES

Information Technology

ABSTRACT

Author	Henri Mäenpää
Title	Domain-Plan
Year	2010
Language	Finnish
Pages	61
Name of Supervisor	Antti Virtanen

The purpose of this thesis was to design a basic network services function for an organization size of approx 3500 user. The basic network services were Active Directory-, DNS-, DHCP-, Print- and File -services. Vaasan ammattikorkeakoulu University of Applied Sciences (VAMK) was used as an example network. The thesis also included laboratory work which will be used for educational purposes at VAMK.

The basic network services were implemented by using Windows Server 2008 -operating system. Microsoft Technet was used as a primary source of information. Technet offered a lot of information which helped at the designing process of the example network.

A plan of network and network services was also used to create a small company network which was used for educational purposes. The network was created by using three servers. The network services were distributed among the three servers so that the best fault tolerance was achieved.

The hardest part regarding planning was to find out that there is no single one right way to design the network services because the structure of the organization considerably effects the designing process.

Keywords: Windows Server 2008, Active Directory, DHCP, DNS

LYHENNELUETTELO

AD	Active Directory Windows Server -käyttäjätietokanta
AS	Authentication Service Kerberos -autentikointi
DC	Domain Controller Toimialueen ohjainkone
DFS	Distributed File System Hajautettu tiedostojärjestelmä
DFS-R	Distributed File System replication Hajautettun tiedostojärjestelmän replikointi
DHCP	Dynamic Host Configuration Protocol IP-osoitteiden jakomenetelmä
DNS	Domain Name System Osoitteiden hallinta
FRS	File Replication Service Replikointipalvelu
FSMO	Flexible Single-Master Operation Domain Controller -roolit
GPO	Group Policy Object Käyttöoikeuksien ja asetuksien määrittely

KCC	The Knowledge Consistency Checker Replikoinnin hallinta
KDC	Key Dictribution System Käyttäjän autentikointi
LDAP	Lightweight Directory Access Protocol Hakemistopalveluprotokolla
NTLM	NT LAN Manager Microsoftin autentikointiprotokolla
PDC	Primary Domain Controller Windows NT –ohjauspalvelin
RDC	Remote Differential Compression DFS-pakkausprotokolla
RID	Relative ID Ohjauspalvelimen tunnistekoodi
SASL	Simple Authentication and Security Layer Käyttäjän tunnistus ja tietoturvaprotokolla
SID	Security Identifier Objektien tunnistekoodi
TCP/IP	Transmission Control Protocol / Internet Protocol Tietoliikenneprotokolla
TGS	Ticket-Granting Service Kerberos-tikettien vaihto

TGT	Ticket Granting Ticket
	Kerberos-tikettien autentikointi

SISÄLLYS

1 JOHDANTO

Kaikilla organisaatioilla on nykyään tietoliikenneverkko, verkon toiminta on tärkeä osa organisaation rakennetta. Tietoliikenneverkkojen suunnittelu on sen vuoksi suuressa roolissa, kun organisaation verkkoa perustetaan. On tärkeää, että rakenne, käyttäjämäärät ja palvelut mitoitetaan jo alussa oikein, koska muutosten tekeminen ja kapasiteetin lisääminen on huomattavasti vaikeampaa tai mahdotonta, jos verkko on ollut kauan toiminnassa. Oikein tehdyllä mitoituksella varmistetaan myös verkon parempi toiminnallisuus ja saadaan vähennettyä verkossa syntyviä vikoja.

Opinnäytetyön tarkoituksena oli tehdä mitoitus verkon peruspalveluille, käyttäen ensisijaisesti Windows-tuotteita. Mitoitus tehtiin noin 3500 hengen organisaatiolle ja siinä huomioitiin erityisesti käyttäjätietokanta, hakemistopalvelut, protokollat ja verkkopalvelut. Fyysiseen verkkoon työssä ei puututa vaan sen oletettiin olevan ja valmiina. Mitoituksesta toteutettiin myös pieni osa Tietoverkonpalvelut -kurssin laboratoriotyöksi. Laboratoriotyön avulla oli tarkoitus simuloida suunniteltua verkkoa ja toteuttaa siitä pieni osa.

2 OPINNÄYTETYÖN KUVAUS

Tämän opinnäytetyön tarkoituksena oli suunnitella noin 3500 hengen organisaatiolle tietoliikenneverkon peruspalvelut. Työssä otetaan mallia Vaasan ammattikorkeakoulun verkon rakenteesta, jota käytetään esimerkkinä palveluiden mitoituksessa. Mitoituksessa pyritään ensisijaisesti käyttämään Windows-tuotteita. Opinnäytetyössä ei otettu huomioon organisaatiokohtaisia palveluita, kuten esimerkiksi etäyhteyksiä ja sähköpostipalveluita. Vaan siinä keskitytään erityisesti verkon peruspalveluihin, joita esiintyy lähes jokaisessa organisaatiossa. Opinnäytetyössä huomioitaisiin seuraavat asiat:

Active Directory –hakemistopalvelut

- Metsä- ja puurakenne
- Toimialueiden ohjauspalvelimien (Domain Controller) sijoitus ja mitoitus
- Käyttäjätietokannat
- Organisaatioyksiköiden ja FSMO (Flexible Single-Master Operation) -roolien suunnittelu
- Käyttäjäntunnistus ja käyttöoikeuksien tarkistus Kerberos- ja LDAP -protokollalla

Protokollien ja verkkopalvelujen mitoitus sekä rakenteen suunnittelu

- Levy- ja tulostinpalvelut
- DNS
- DHCP

Suunnitelman jälkeen osa opinnäytetyöstä toteutettiin Tietoverkon palvelut–kurssin harjoitustyönä, jonka avulla oli tarkoitus simuloida suunniteltua verkkoa ja toteuttaa siitä pieni osa.

3 WINDOWS SERVER 2008 R2

3.1 Yleistä

Windows Server 2008 R2 on palvelinohjelmisto. Ohjelmisto julkaistiin helmikuussa 2008 ja se on uusin Microsoftin julkaisu Windows-serveristä. Se pohjautuu Windows Vista -käyttöjärjestelmään. Ohjelmisto sisältää paljon uudistuksia ja parannuksia Windows Server 2003:een verrattuna, joilla Microsoft pyrkii helpottamaan Server 2008 R2:n käyttöä, joustavuutta ja saatavuutta kaiken kokoisissa organisaatioissa. Windows Server 2008 R2 onkin vakiinnuttanut asemaansa laajalti kaikenkokoisissa organisaatioissa ja uudet ominaisuudet helpottavat huomattavasti sen käyttöönottoa./14/

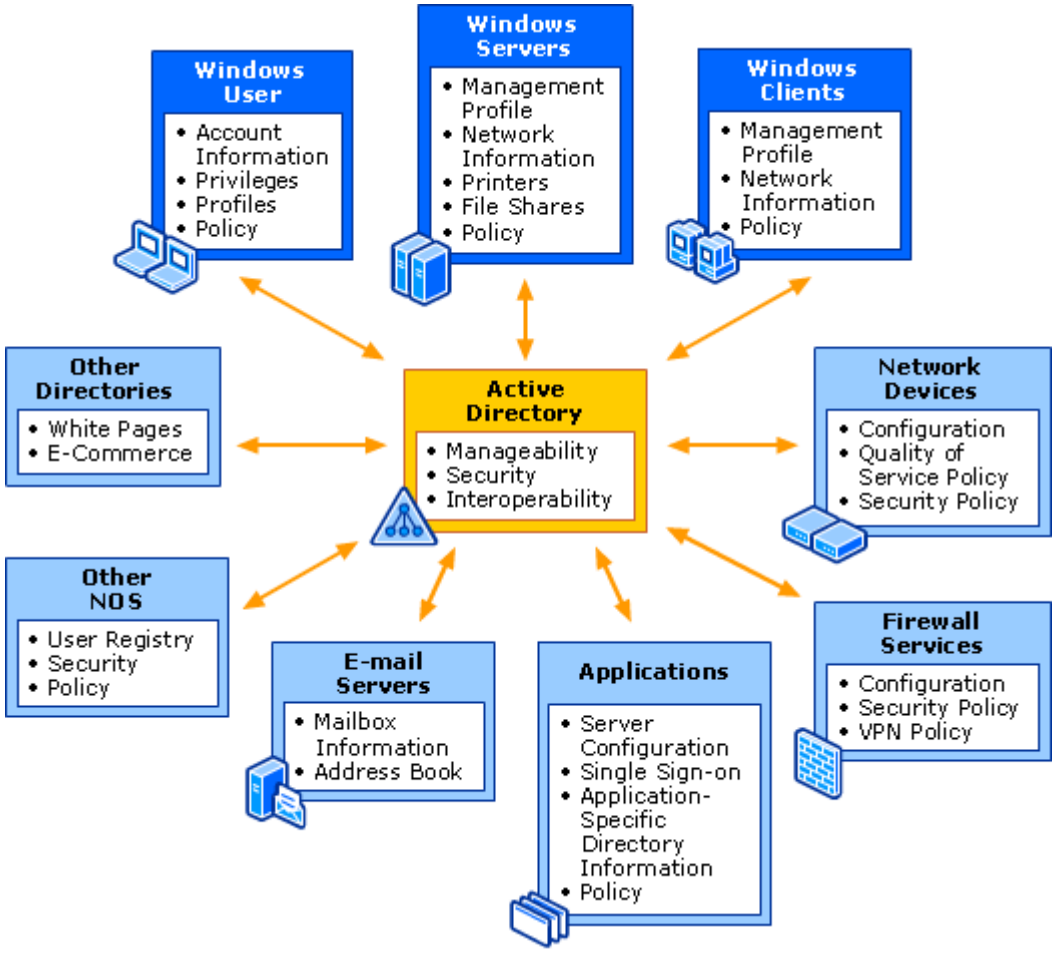
Tärkeimpinä parannuksina Windows Server 2008 R2:ssa ovat uusi Internet -työkalu, parannellut virtualisointiominaisuudet sekä parempi skaalautuvuus, luotettavuus ja käytettävyys. Uudistettu ohjelmisto tuo mukanaan myös paljon ominaisuuksia, joita on suunniteltu käytettäväksi Windows 7 -käyttöjärjestelmän kanssa. Opinnäytetyön mitoitus tehdään Windows Server 2008 R2:n ympärille ja osa ominaisuuksista esitellään tarkemmin työn kuluessa./14/

3.2 Active Directory

Active Directory on hakemistopalvelu, joka tarjoaa verkon käyttäjille hajautetun tietokantapalvelun. Sen avulla hallitaan verkossa sijaitsevien palvelujen, käyttäjien ja erityyppisten osoitteiden tietokantaa, kuten esimerkiksi tietokoneita, tulostimia ja käyttäjäryhmiä. Näitä tietoja kutsutaan objekteiksi. AD mahdollistaa keskitetyn tietokantojen hallinnan koko verkon alueelle, eivätkä organisaation eri yksiköt tai käyttäjät ole riippuvaisia sijainnista./2/

AD tuli käyttöön ensimmäisen kerran Windows Server 2000 -versiossa ja se on saanut sen jälkeen useita päivityksiä ja muutoksia, joista suurin osa on kuitenkin huomaamattomia. Nykyään AD on tärkeässä osassa organisaatioiden rakennetta, joissa on käytössä Windows Server. Kuvassa 1 on tarkempi kuvaus AD-tietokannasta ja sen sisällöstä. Active Directoryn avulla tiedot käyttäjistä,

tietokoneista, verkkoresursseista ja asetuksista saadaan keskitetysti yhteen tietokantaan, jota pystytään suojaamaan sekä hallitsemaan helposti. Tietokantaan pystytään esimerkiksi sisällyttämään tietoa sähköpostipalveluista ja ohjelmista.



Kuva 1. Active Directory tietokanta./1/

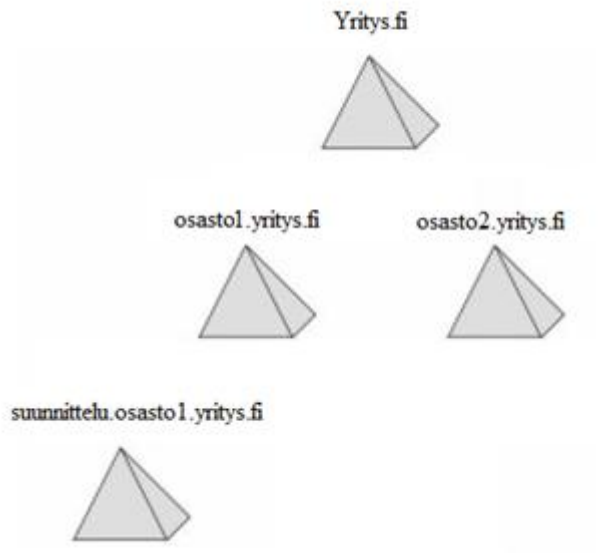
3.3 Active Directoryn rakenne

AD käyttää pohjanaan puumaista X.500 -hakemistopalvelua ja se sisältää useita eri hierarkiatasoja, joiden avulla pystytään hallinnoimaan ja helpottamaan verkon käyttöä. Rakenne on kuvattu Schemassa, joka sisältää myös määritykset siitä minkä tyyppisiä objekteja verkossa on. Verkossa sijaitsevia objekteja ylläpidetään Global Catalog -tietokannassa. Sen avulla verkossa olevia tietoja pystytään etsimään koko metsän alueella. Schema ja Global Catalog sijaitsevat AD-tietokannassa ja niitä ylläpidetään toimialueen ohjauspalvelimen eli Domain-

controllerin avulla. Active Directory on riippuvainen Domain-controllereista ja niiden toiminnasta kerrotaan tarkemmin tämän opinnäytetyön kappaleessa 3.7. /1/,/3/

Metsä ja puu ovat rakenteen perusta. Näiden avulla kuvataan AD-tietokannan rakennetta ja sen toimintaa. AD-rakenne voi muodostua pienimmillään metsästä ja yhdestä puusta. Metsä on rakenteen ylin taso ja muodostuu vähintään yhdestä toimialueesta ja AD-hakemistopuusta. Metsiä voi olla myös useita saman organisaation alueella, jos eri yksiköt halutaan erottaa toisistaan ja niillä on erilaiset rakennevaatimukset. Tämä menetelmä kuitenkin hankaloittaa AD-tietokannan ylläpitoa.

Metsän sisäinen rakenne muodostuu puista. Puilla kuvataan yleensä organisaation verkossa sijaitsevia eri yksiköitä. Jokaisella puulla on yksilöllinen DNS-nimi ja ne muodostuvat päädomaineista ja niiden alidomaineista. Tätä rakennetta kutsutaan hakemistopuuksi. Puut mahdollistavat, että organisaation eri toimipisteille saadaan erilainen sisäinen verkkorakenne. Kuvassa 2 on kuvattu yksi metsässä sijaitseva puu./1/,/2/

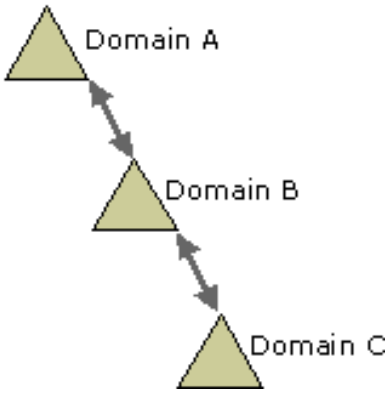


Kuva 2. Active Directory -puu.

Kuvassa 2 on metsässä sijaitsevat Yritys.fi -puu. Puussa on yksi päädomain ja 3 alidomainia. Jokaisella domainilla on oma DC (Domain-controller), jonka avulla AD-tietokantaa ylläpidetään ja käyttöoikeuksia hallitaan. Niiden avulla hoidetaan myös tietokannan replikointitoiminnot, joilla tietokannat pidetään samanlaisina koko verkon alueella.

3.4 Active directory -luottamussuhteet

Metsässä sijaitsevien eri domainien välisiä oikeuksia hallitaan luottamussuhteiden avulla. Ne määritelevät minkälaisia oikeuksia domainien sekä objektien välillä on. Oikeuksien hallinta tapahtuu transitiivisten luottamussuhteiden avulla (two-way trusts). Transitiiviset luottamussuhteet mahdollistavat, että järjestelmänvalvojan ei tarvitse määritellä käyttöoikeuksia jokaiselle domainille erikseen, vaan ne siirtyvät muiden domainien mukana automaattisesti. Kuvassa 3 on esimerkki hakemistopuusta.



Kuva 3. Active directory -puu. /13/

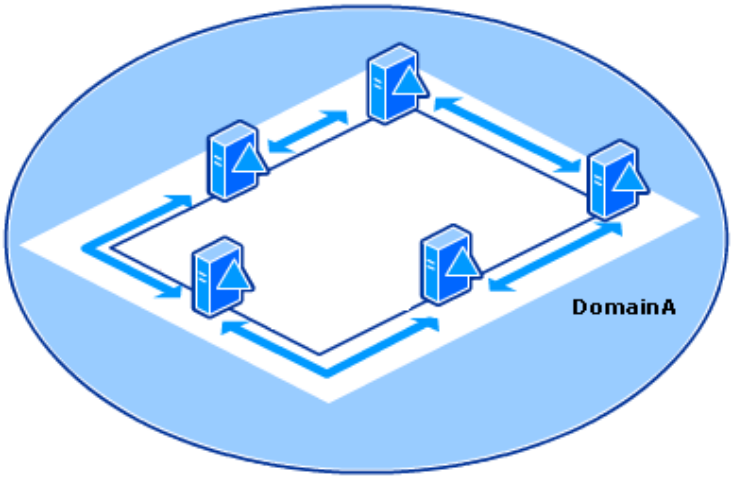
Transitiivisilla luottamussuhteilla tarkoitetaan, että jos kuvassa 3 näkyvä Domain A luottaa Domain B:hen ja Domain B luottaa Domain C:hen niin myös Domain C luottaa automaattisesti Domain A:han. Luottamussuhteiden hallintaan käytetään Kerberos- tai NTLM-protokollaa. Kerberos-protokollaa käytetään automaattisesti Windows 2000 ja uudemmissa käyttöjärjestelmissä, mutta jos se ei ole tuettu protokolla, niin käytetään NTLM-protokollaa./13/

3.5 Active directory -replikointi

Kaikissa Windows AD-verkoissa on yleensä enemmän kuin yksi DC. Kaikki verkon DC:t ovat samanarvoisessa asemassa ja jokainen sisältää kopion AD-tietokannasta. Tällä nostetaan verkon luotettavuutta ja toiminnallisuutta tilanteissa ,joissa jokin verkon DC-kone vikaantuu ja verkon resurssit pitää hakea toiselta DC-koneelta. On siis tärkeää, että tietokannat ovat jokaisella DC:lla samanlaisia ja päivittyvät automaattisesti. Tämä varmistetaan replikoinnin avulla. Replikointi on toiminto, jolla hoidetaan DC:n välisten tietokantojen päivitykset ja ylläpito. Ilman replikointia AD-verkko, jossa on useita DC:ta, ei voi toimia oikein.

Windows Server 2008:ssa tuli käyttöön uusi replikointipalvelu DFS (Distributed File System) -replikointi, joka korvasi aiemman version Windows Server 2003:n käytössä olevan FRS (*File Replication Servicen*) -palvelun. DFS–replikoinnin pääuudistuksena on uusi pakkausprotokolla RDC. Se on suunniteltu erityisesti toimimaan verkoissa, joissa yhteys nopeudet ovat rajoitettuja. RDC-tekniikan avulla tiedostoista pystytään päivittämään vain muutokset ja näin tietoliikennettä saadaan vähennettyä./6/

Replikointitopologioita pidetään yllä koko AD–verkon alueella KCC (The Knowledge Consistency Checker) -prosessin avulla. Se sijaitsee jokaisella verkon DC:lla ja luo yhteyksiä niiden välille AD- tietokannasta saamien tietojen mukaan. Yhteydet muodostetaan eri DC:n välille rengastopologian avulla. Tällä varmistetaan, että jokaisella DC:lla on vähintään kaksi yhteyttä ja päivitykset AD-tietokantaan saadaan tehtyä, vaikka jokin verkon DC:sta ei olisi toiminnassa. Kuvassa 4 on yksinkertainen esimerkki rengastopologiasta. Jokaisella koneella on vähintään kaksi yhteyttä, eikä replikointi ole riippuvainen kaikkien koneiden toiminnasta./4/



Kuva 4. Rengastopologia

3.6 Käyttäjän tunnistus ja käyttöoikeudet

Windows Server 2008 R2 käyttää AD-verkon käyttäjien tunnistukseen ja verkon käyttöoikeuksien hallintaan Kerberos- ja LDAP-protokollaa (Lightweight Directory Access Protocol). Kerberos on vastuussa käyttäjien tunnistuksesta ja LDAP:n avulla hoidetaan pääsy AD-hakemistopalveluun. Näiden protokollien avulla varmistetaan, että kaikilla käyttäjillä on turvallinen pääsy verkkoon ja on oikeus lukea sekä muokata siellä sijaitsevia tietoja.

3.6.1 LDAP

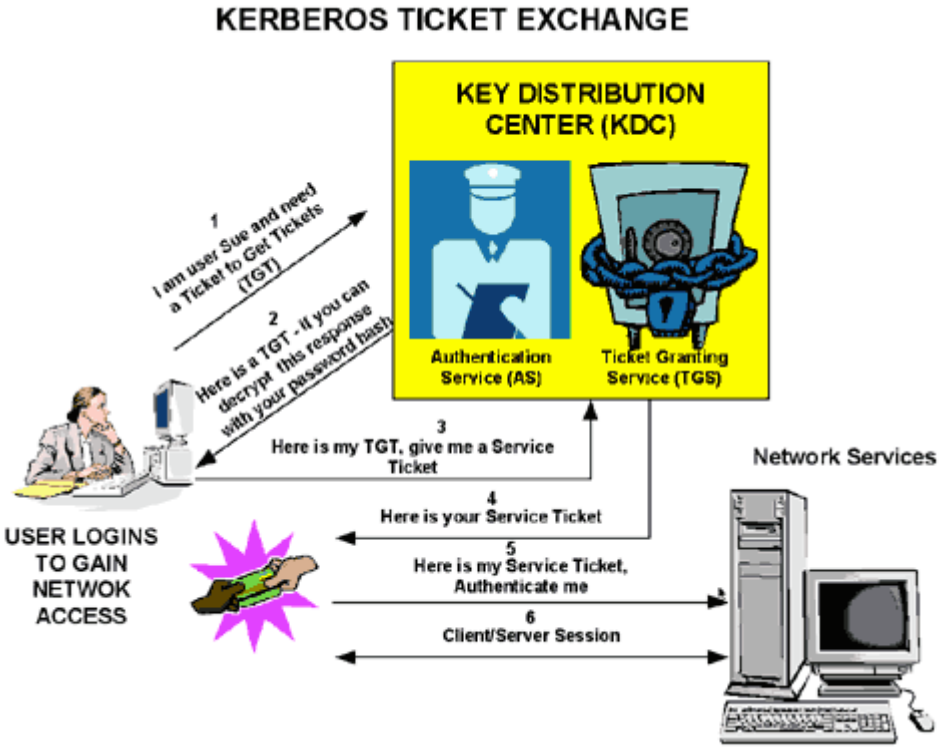
LDAP on protokolla, joka on kevennetty versio DAP-protokollasta ja toimii TCP/IP-protokollan päällä. Sen tarkoituksena on luoda pääsy X.500-hakemistopalveluun ja mahdollistaa luku- sekä kirjoitustoimintoja tietokantaan. LDAP tarjoaa myös yksinkertaisia käyttäjäntunnistus ja tietoturvaominaisuuksia SASL-tekniikoita käyttäen. LDAP:n toiminta perustuu Client-Server malliin. Verkossa on yksi tai useampia hakemistopalvelimia, jotka tarjoavat useille verkonkäyttäjille pääsyn samanaikaisesti tietokannassa oleviin tietoihin. Nykyään LDAP:a käytetään paljon osoitetietojen hakuun ja ylläpitoon esimerkiksi sähköpostisovelluksille.

AD-tietokannassa LDAP-rakenne muodostuu objekteista ja sen sisältämistä attribuuteista. Attribuuttien avulla määritellään objektien tyypit ja niiden sisältämä tieto. Attribuuttien määrä ja tyyppi voi myös vaihdella kyseessä olevan objektin mukaan. Esimerkiksi AD-verkossa tietyllä palvelimella sijaitsevan käyttäjän AD-polku merkittäisiin attribuuttien avulla seuraavasti:
LDAP://server1/CN=käyttäjä,OU=ryhmä,DC=yritys,DC=fi.
Polussa LDAP://server1 määrittelee, millä palvelimella kyseinen tieto sijaitsee. CN määrittelee objektin yleisnimen ja OU ryhmän missä käyttäjä sijaitsee. DC-attribuutilla määritellään toimialue./9/,/12/

3.6.2 Kerberos

Windows Server 2008 R2 -käyttäjien tunnistus tapahtuu Kerberos 5 -protokollan avulla. Se mahdollistaa tunnistuksen suojaamattomissa verkoissa ja on erityisesti suunniteltu Client-Server -mallia varten. Kerberos on kolmiosainen tunnistusmenetelmä, joka muodostuu Key Distribution Centre:stä (KDC), käyttäjästä ja palvelusta. KDC sijaitsee toimialueen DC-koneella ja sisältää Authentication Service:n (AS) ja Ticket-Granting Service:n (TGS). KDC:n tehtävänä on tunnistaa käyttäjä ja serveri, johon yhteys luodaan sekä jakaa tikettejä, joihin Kerberosin toiminta perustuu.

Kerberos 5 -käyttäjän ja -serverin tunnistus tapahtuu tikettien avulla. Tiketti on salattu viesti, mikä sisältää istuntoavaimen ja käyttäjän tunnistukseen tarvittavia tietoja. Sen avulla saadaan mahdollistettua, ettei verkossa lähetetä salasanoja palvelinten välillä, vaan tunnistus tapahtuu salattujen viestien avulla. Kuvassa 5 on esitetty Kerberos 5 -tiketin vaihto ja käyttäjän tunnistuksen periaate.



Kuva 5. Kerberos 5 -tiketin vaihto./8/

Kuvassa 5 käyttäjä kirjautuu verkkoon kerberos -protokollan avulla. Kun käyttäjä kirjautuu sisään, lähettää se ensimmäisenä TGT-tiketti pyynnön (Ticket Granting Ticket) autentikointipalvelulle AS. Kun AS vastaanottaa pyynnön, varmistaa se käyttäjän aitouden tietokannasta ja luo istuntoavaimen. AS lähettää sen jälkeen käyttäjälle viestin, mikä on salattu käyttäjän omalla salasanalla ja sisältää istuntoavaimen sekä TGT-tiketin. Tiketti on salattu TGS:n avaimella. Kun käyttäjä vastaanottaa viestin, se puretaan käyttäjän syöttämällä salasanalla. Oikealla salasanalla vietistä paljastuu TGT-tiketti. Käyttäjä lähettää seuraavaksi viestin TGS-palvelulle. Viesti sisältää TGT-tiketin, aikaleiman sekä palvelimen nimen, mihin käyttäjä haluaa yhdistää. TGS varmistaa tiketin aitouden omalla avaimellaan. TGS lähettää seuraavaksi viestin käyttäjälle, mikä sisältää kaksi tikettiä. Toinen tiketeistä on salattu käyttäjän avaimella ja toinen palvelimen avaimella. Tiketit sisältävät palveluavaimen, millä yhteys pystytään muodostamaan. Käyttäjä purkaa viestin omalla avaimella ja lähettää viestin palvelimella. Palvelin vastaanottaa viestin ja purkaa tiketin omalla avaimella, jonka jälkeen se muodostaa yhteyden käyttäjän kanssa./7/

3.7 Domain Controller

Windows Server 2008 R2:ssa Domain Controller -palvelu hoidetaan Active Directory Domain Service (AD DS) -roolin avulla. DC on ohjauspalvelin, joka tarjoaa ja ylläpitää AD:n tunnistus ja hakemistopalveluja. Jokainen toimialue sisältää vähintään yhden DC:n. Niitä voi olla myös useampia samalla toimialueella, jolloin molemmat DC:t sisältävät saman AD-tietokannan. Tällä saadaan nostettua verkon kapasiteettia ja mahdollistetaan verkon toiminta tilanteissa, joissa toinen DC vikaantuu. Toimialueella yksi DC pitää myös yllä koko AD-metsän yhteistä replikoituvaa Global Catalog -hakemistoa./5/

3.8 Levypalvelu

Levypalvelu hoidetaan Windows Server 2008 R2:ssa File Services -roolin avulla. Levypalvelun avulla saadaan keskitetty tiedostojen hallinta ja jako käyttöön, eikä tiedostoja tarvitse kuljettaa mukana, vaan ne löytyvät verkkolevyiltä. Käyttäjille pystytään tarjoamaan levypalvelun avulla omat sekä yhteiset verkkoasemat ja niitä voidaan hallita levypalvelimelta. Levypalvelun avulla saadaan organisaatioiden tieturvaa ja verkontoimivuutta nostettua, koska varmuuskopiointi ja hallinta pystytään tekemään keskitetysti yhdestä paikasta. Kustannukset saadaan myös näin alhaisemmiksi. Windows Server 2008 tukee myös Unix- ja Mac -käyttöjärjestelmiä Network File System (NFS) -palvelun avulla. NFS on protokolla, joka alun perin on suunniteltu Unix-järjestelmiin ja sen avulla pystytään tekemään tiedostonjako Windowsin, Unixin ja Macin välillä. Organisaatiot voivat siis käyttää verkossa useita eri käyttöjärjestelmiä./5/

3.9 Tulostinpalvelu

Tulostinpalvelu mahdollistaa tulostimien jaon ja hallinnan verkossa. Sen avulla verkon tulostimet saadaan keskitetysti yhdelle palvelimelle, mistä niitä pystytään hallitsemaan ja jakamaan verkon käyttäjille. Käyttäjät pystyvät muodostamaan yhteyden kaikkiin palvelimella oleviin tulostimiin ja tulostamaan niihin koko verkon alueelta. Tulostimille voidaan luoda myös käyttöoikeuksia palvelimelta, joilla pystytään rajaamaan eri käyttäjäryhmien pääsy niihin.

4 VERKKOPALVELUT

4.1 DHCP

Dynamic Host Configuration Protocol (DHCP) on verkkoprotokolla, jonka tehtävänä on jakaa automaattisesti TCP/IP-verkon käyttäjille IP-osoitteita. DHCP:n avulla jaetaan verkon käyttäjille myös yleensä aliverkon peite, oletusyhdyskäytävä ja DNS-palvelinosoitteet. Sen avulla verkon osoitteita pystytään ylläpitämään DHCP-palvelimella ja verkkoon liitetyille koneille ei tarvitse asettaa IP-osoitteita manuaalisesti vaan ne saavat automaattisesti vapaan IP-osoitteen.

DHCP-palvelin tarjoaa automaattisesti käyttäjille verkko-osoitteet ja niitä pystytään hallitsemaan keskitetysti. DHCP-palvelin käyttää Client-server -protokollaa osoitteiden jaossa. Kun asiakas kirjautuu verkkoon lähettää se osoite pyynnön DHCP-palvelimelle. DHCP-palvelin vastaanottaa pyynnön ja määrittää asiakkaalle osoitetiedot. Jos asiakas hyväksyy ne, määrittää DHCP-palvelin vielä voimassaoloajan osoitetiedoille. DHCP-palvelimelta voidaan määrittää myös kiinteät IP-osoitteet asiakkaille./10/

4.2 DNS

Domain Name System (DNS) on nimipalvelujärjestelmä. Sen tehtävänä on tarjota verkon asiakkaille nimenselvityspalveluja. DNS:n avulla pystytään muuntamaan verkkonimiä IP-osoitteiksi, joiden avulla verkon asiakkaat pystyvät muodostamaan yhteyksiä verkossa sijaitseviin kohteisiin. DNS helpottaa huomattavasti verkon käyttöä, sillä käyttäjien ei tarvitse muistaa hankalia IP-osoitteita. DNS-palvelua käytetään myös AD-ympäristössä, koska verkon nimeämisrakenne ja -hierarkia muodostetaan sen avulla. DNS:n avulla pidetään kirjaa myös AD-palveluista.

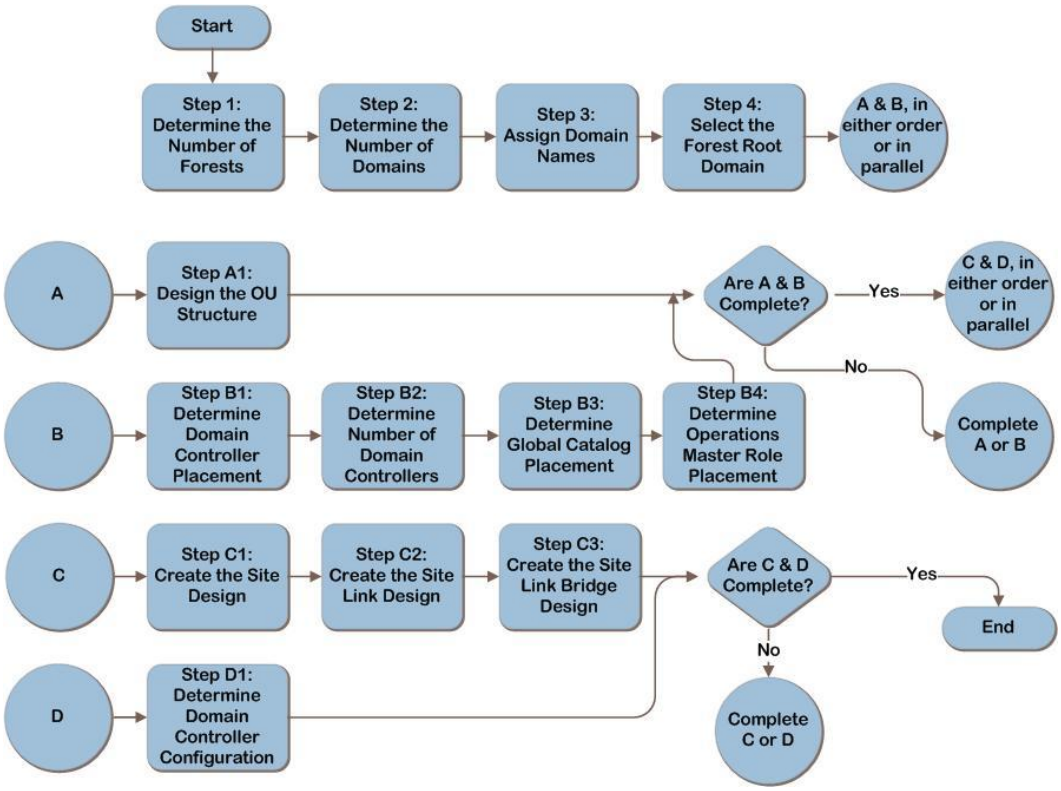
DNS-tietoja ylläpidetään DNS-palvelimien avulla. Niiden tehtävänä on hoitaa verkon nimikyselyjä ja välittää niitä eteenpäin toisille DNS-palvelimille, mikäli tietoa ei löydy omalta DNS-alueelta. DNS-nimikyselyn periaate on että, nimiä

vastaavat IP-osoitteet on tallennettu hajautettuun tietokantaan. DNS-palvelin etsii tietoja ensin omalta DNS-alueeltaan ja mikäli tietoa ei löydy, välitetään kysely aina ylemmälle DNS-tasolle. Kun kysely on tehty ja haettu osoite on löytynyt, DNS-palvelin tallentaa haun tuloksen välimuistiin, minkä avulla se pystyy vähentämään ja nopeuttamaan DNS-liikennettä, jos tietoa haetaan uudelleen./11/

5 VERKON SUUNNITTELU JA MITOITUS

5.1 Active Directory

AD on yksi verkon tärkeimmistä osa-alueista, siksi sen suunnittelu ja mitoitus on tärkeässä roolissa. Se sisältää tiedon kaikista verkon käyttäjistä ja laitteista. On siis tärkeää, että AD:n rakenne suunnitellaan kunnolla ja verkon käyttäjämäärät mitoitetaan oikein jo alussa. AD:n suunnittelu voidaan jakaa karkeasti neljään osaan, metsien, toimialueiden, organisaatioyksiköiden (Organizational Unit) ja verkon fyysisen rakenteen suunnitteluun. Kuvassa 6 on esitetty tarkemmin AD:n suunnitteluprosessi.



Kuva 6. Active Directoryn suunnitteluprosessi./5/.

Metsäsuunnittelussa päätetään, jaetaanko AD:n rakenne yhteen vai useampaan metsään. Tähän päätökseen vaikuttaa, minkä kokoinen organisaatio on kyseessä ja moneenko toimipisteeseen se on jaettu. AD:n rakennetta ei ole järkevää jakaa useampaan kuin yhteen metsään, jos organisaatio sijaitsee yhdessä toimipisteessä

ja sitä ei ole jaettu kahteen erilaiseen osastoon, joilla on eri oikeudet. Useampi kuin yksi metsä lisää myös kustannuksia ja AD:n hallinta vaikeutuu, sillä rakenteita täytyy luoda useita.

Toimialuesuunnittelussa päätetään, montako eri toimialuetta metsään luodaan, sekä määritellään toimialueille nimet. Niiden määrään vaikuttaa eniten, miten organisaation rakenne on luotu. Toimialueiden määrää kannattaa suunnitella jo verkon perustamisvaiheessa oikein, sillä niiden lisääminen ja poistaminen voi olla myöhemmin vaikeaa. Jokainen toimialue lisää myös hieman laitteistokustannuksia.

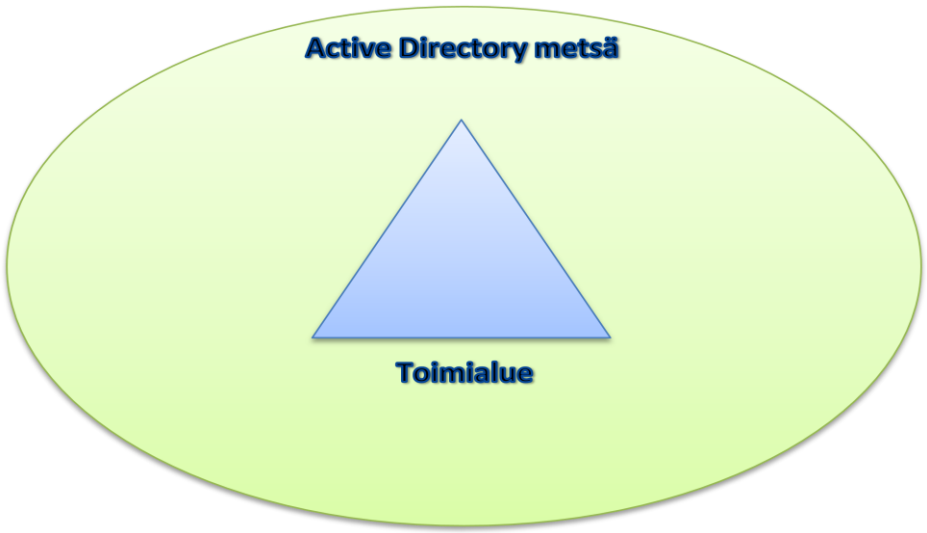
AD:n toimialueella sijaitsevia objekteja hallitaan organisaatioyksiköiden avulla. Ne ovat kansioita, joiden avulla pystytään muodostamaan toimialueella sijaitsevista objekteista helposti hallittavia ryhmiä. Suunnitelman avulla pyritään jakamaan toimialueen objektit loogisiin ja helposti hallittaviin ryhmiin, niiden oikeuksien sekä tyyppien mukaan.

Verkon fyysisen rakenteen suunnittelulla pyritään optimoimaan verkkoliikenne. Sen avulla on tarkoitus määritellä DC:lle sekä eri tietokannoille parhaat sijainnit verkossa./5/

5.2 Active Directory -rakennesuunnitelma

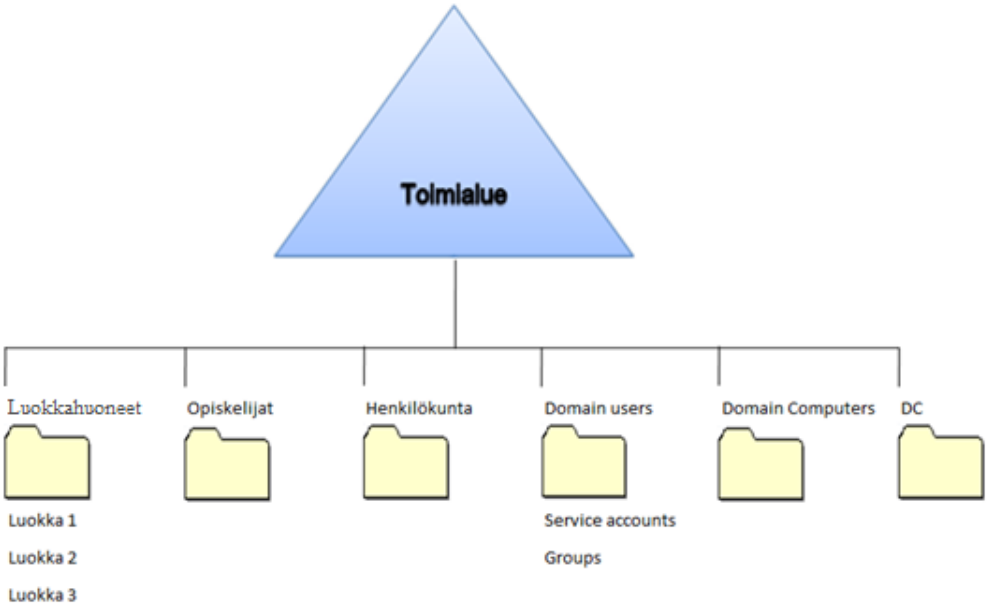
AD:n suunnittelu aloitetaan metsä- ja toimialuerakenteesta. Rakenteeseen vaikuttaa eniten, minkälaiseen ympäristöön AD on tarkoitus ottaa käyttöön. Mitoitus on tarkoitus tehdä noin 3500 hengen organisaatiolle, joka on koulu ja sijaitsee yhdessä toimipisteessä. Tämän vuoksi on järkevää perustaa ainoastaan yksi metsä ja toimialue. Yksi metsä on yleensä järkevin ratkaisu monessa organisaatiossa ja useampaa metsää kannattaa harkita vain tilanteissa, joissa organisaation rakenne sitä erikseen vaatii. Esimerkiksi organisaatio, joka on jaettu maantieteellisesti eri yksikköihin voi vaatia useampaa metsää. Yhtä metsää on myös huomattavasti helpompi hallita ja sen perustaminen sekä ylläpito on myös halvempaa. Toimialueiden määrään vaikuttaa eniten, minkälainen organisaation

rakenne on. Niitä ei ole järkevää lisätä, muista kuin teknisistä tai rakenteesta johtuvista syistä. Yksi toimialue on tästä syystä järkevin ratkaisu, koska kyseessä on koulu ja samaan verkkoon on tarkoitus päästä koko koulun alueelta. Yhden toimialueen avulla verkon hallinta saadaan myös helpommaksi ja verkon palauttaminen ongelmatilanteista on helpompaa. Lopuksi määritellään toimialueille vielä nimet sekä metsälle juuritoimialue. Juuritoimialue pitää tietokantaa metsän järjestelmänvalvojista. Nämä järjestelmänvalvojat pystyvät muokkaamaan AD:n rakennetta. Juuritoimialueen sijainti kannattaa suunnitella hyvin, sillä sijaintia ei voida muuttaa enää myöhemmin. Tässä tapauksessa toimialueita on vain yksi ja siitä tulee automaattisesti juuritoimialue. Kuvassa 7 on suunniteltu AD-rakenne.



Kuva 7. Active Directoryn -rakenne.

Organisaatioyksiköiden suunnittelu aloitetaan organisaation rakenteen tutkimisella. Sen avulla pyritään määrittelemään, minkälaisia objekteja ja oikeuksia toimialueelta löytyy. Organisaatioyksiköiden rakenne kannattaa alussa pitää mahdollisimman yksinkertaisena ja muodostaa objekteista vain järkeviä ryhmiä, niiden tyyppien ja oikeuksien mukaan. Ryhmiä on helppo muokata myöhemmin, jos niiden oikeuksiin tai rakenteeseen täytyy tehdä muutoksia. Kuvassa 8 on luotu Organisaatioyksikkörakenne.



Kuva 8. Organisaatioyksikkörakenne.

Organisaatioyksikkörakenne on pyritty pitämään mahdollisimman yksinkertaisena ja helposti hallittavana. Rakenne on jaettu kuuteen eri organisaatioyksikköön. Domain users, Domain Computers ja DC luodaan automaattisesti, kun AD-verkko pystytetään. Kaikki uudet käyttäjät, tietokoneet ja DC:t luodaan automaattisesti näiden organisaatioyksiköiden sisälle. Henkilökunta, opiskelijat ja luokkahuoneet on luotu erikseen. Käyttäjät ja tietokoneet, joita halutaan hallita näiden organisaatioyksiköiden avulla, täytyy erikseen siirtää kyseisten kansioiden alle.

Järjestelmänvalvojia ja palvelinten tunnuksia hallitaan Domain users -organisaatioyksikön avulla. Ne kannattaa pitää omana hallittavana ryhmänään, eikä niitä ole järkevää sijoittaa muihin organisaatioyksiköihin. Järjestelmänvalvoja voivat esimerkiksi vahingossa rajoittaa omia oikeuksiaan, jos moni organisaatioyksikkö on vastuussa niistä. Koulun henkilökunta ja opiskelijat on saatu jaettua kahteen ryhmään. Henkilökunnalla on verkossa suuremmat käyttöoikeudet kuin oppilailla ja sen vuoksi käyttäjät on järkevä jakaa kahteen organisaatioyksikköön. Koulun tietokoneet saadaan puolestaan jaettua järkevästi luokkahuoneiden mukaan. Luokkatunnuksien avulla koneista saadaan muodostettua helposti hallittavia ryhmiä.

5.3 Active Directory Domain Controller –suunnitelma

DC:en määrään ja niiden sijoitteluun vaikuttaa eniten verkon fyysinen rakenne. On suositeltavaa, että DC:en määrä pyritään pitämään mahdollisimman alhaisena. Tämän avulla verkon käytettävyyttä ja hallintaa saadaan paremmaksi. Jokaisella organisaation toimipisteellä, pitäisi kuitenkin olla vähintään kaksi DC:a, jotka on sijoitettu fyysisesti kahteen eri paikkaan. Vikatapauksissa yleensä toinen DC on vielä toiminnassa ja organisaatio toimintaa voidaan jatkaa. Jos organisaatio on jaettu moniin pieniin toimipisteisiin, DC:ta ei ole kuitenkaan järkevä sijoittaa jokaiseen niistä. DC:t kannattaa tälläisissa organisaatioissa sijoittaa keskitetysti yhteen paikkaan.

Käyttäjämäärät vaikuttavat myös DC:en määrään ja niiden sijoittamiseen. Jos toimialueelle on paljon käyttäjiä, täytyy sinne sijoittaa useampia DC:ta, että käyttäjien kirjautumisesta, palveluihin pääsystä ja replikoinnista saataisiin tehokasta. Taulukossa 1 on käyttäjämäärien mukaan tehty DC-mitoitus ja taulukossa 2 on muistivaatimukset.

Taulukko 1. Domain Controller vaatimukset./5/

Toimialueen käyttäjämäärä	**Domain Controllerien määrä**
1-499	yksi - yksi prosessorinen
500-999	yksi - kaksi prosessorinen
1,000-2,999	kaksi - kaksi prosessorista
3,000-10,000	kaksi - neljä prosessorista

Taulukko 2. Domain Controller muistivaatimukset./5/

Toimialueen käyttäjämäärä	**Domain Controllerin muisivaatimus**
1-499	512 MB
500-999	1 GB
>1,000	2 GB

VAMK:n kokoiselle noin 3500 hengen organisaatiolle on järkevää asentaa kaksi DC:a. Verkonkuorma jakautuu tasaisesti, koska kyseessä on koulu ja DC:t saadaan sijoitettua fyysisesti erilleen toisistaan. VAMK:in tapauksessa, toinen DC sijoitettaisiin Raastuvankadulle ja toinen Palosaarelle.

DC:n mitoituksen jälkeen, päätetään Global Catalog -tietokantojen määrä ja sijainti. Global Catalog sijaitsee yleensä jokaisella toimialueella vähintään yhdellä DC:lla ja se sisältää tiedon koko metsän toimialueista sekä niiden objekteista. Global Catalog replikoituu automaattisesti ja tietokannan avulla pystytään etsimään koko metsän objekteja nopeasti.

Global Catalog -tietokantojen sijaintiin ja määrään vaikuttaa eniten metsänrakenne. Useasta toimialueesta muodostuvassa metsässä Global Catalog -tietokannan koko kasvaa ja se lisää replikointitietojen kokoa, joten sitä ei ole järkevää pitää yllä jokaisella DC:lla. Yleensä jokaisella toimialueella on vain yksi Global Catalog -serveri, mutta joissain tapauksissa niiden määrää joudutaan kasvattamaan. Exchange Server käyttää esimerkiksi Global Catalog -tietokantaa ja verkon toimintaa nopeutetaan asentamalla se useammalle serverillä./5/

Yhden toimialueen metsässä on järkevää asentaa Global Catalog -tietokanta jokaiselle DC:lle. Kaikki Global Catalog -tietokannan tiedot välittyvät jo normaalien replikointitoimintojen yhteydessä ja se ei lisää verkon tai servereiden kuormitusta.

5.3.1 Domain Controller FSMO -roolit

AD:n DC:lle täytyy myös määritellä Operation Master -roolit (FSMO). FSMO (Flexible Single Master of Operation) -roolit ovat eri DC:lle määrättyjä tehtäviä. Vaikka kaikki DC:t ovat samanarvoisia, täytyy osa toiminnoista määritellä erikseen tietylle DC:lle. FSMO-rooleja on viisi koko metsän alueella. Jokaisella toimialueella esiintyviä rooleja ovat PDC Emulator Master, Relative ID (RID) Master ja Infrastructure Master. Metsässä sijaitsevia rooleja ovat Schema Master ja Domain Naming Master./5/

PDC Emulator Master -roolin avulla hoidetaan toimialueella tapahtuvat salasanamuutokset ja se ylläpitää toimialueen käyttäjäryhmiä. Roolin avulla hoidetaan myös yhteensopivuus vanhempien Windows NT 4.0 PDC:en kanssa.

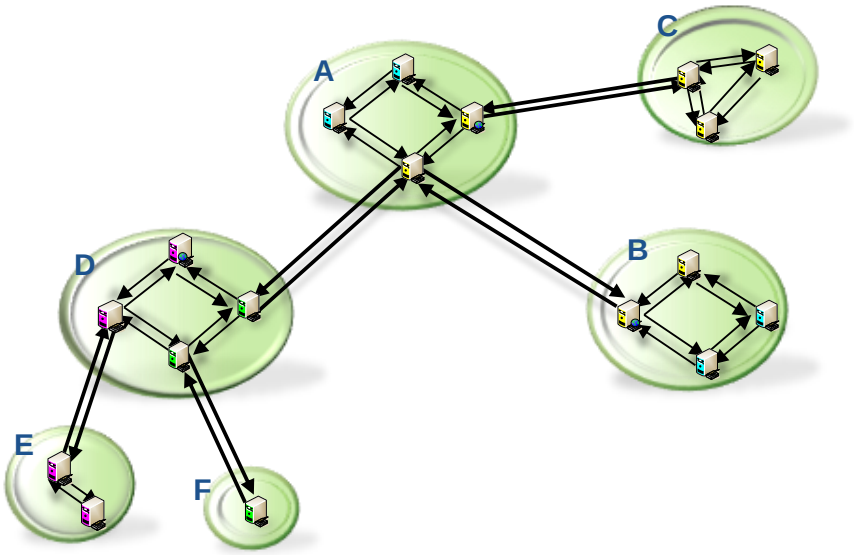
Relative ID Masterin tehtävänä on jakaa DC:lle yksilöllisiä tunnistuskoodeja (RID). Niiden tarkoituksena on varmistaa, että jokaiselle metsän objektille saadaan yksilöllinen turvakoodi (SID). SID-koodiin liitetään DC:n RID-koodi ja sen avulla pystytään erottamaan eri toimialueilla sijaitsevat samannimiset objektit.

Infrastructure Master hoitaa eri toimialueiden välisten objektien ja käyttäjäryhmien oikeuksien hallinnan. Schema Masterin avulla ylläpidetään AD:n Schemaa. ja Domain Naming Master vastaa metsässä tapahtuvien toimialueiden lisäyksestä ja poistamisesta.

FSMO-roolit kannattaa sijoittaa niin, että mahdollisimman harva DC on vastuussa niistä. Kaikki roolit voivat olla saman DC:n hallinnassa. Joissain tapauksissa rooleja joudutaan kuitenkin sijoittamaan eri DC:lle verkon kuormituksen jakamiseksi. Näissä tapauksissa RID- ja PDC-emulator kannattaa sijoittaa suoraan replikointi yhteyteen, koska käyttäjissä tapahtuvat muutokset pitää saada tallennettua molemmille DC:lle. Infrastructure Master -rooli kannattaa sijoittaa eri DC:lle kuin Global Catalog -rooli. Ei ole suositeltavaa pitää niitä samalla DC:lla, koska käyttöoikeudet eivät päivity tällöin oikein toimialueiden välillä. Schema Master ja Domain naming Master kannatta pitää aina samalla DC:lla, kuin Global Catalog -rooli, koska niitä käytetään harvoin ja toimialueiden luonti ei onnistu ilman Global Catalog -palvelinta. Kaikki FSMO-roolit pitää kuitenkin sijoittaa niin, että kaikilla DC:lla on pääsy niihin. Ne on paras sijoittaa paikkaan, jossa on eniten käyttäjiä ja ne ovat luotettavassa yhteydessä koko verkkoon. Verkossa jossa on vain yksi metsä ja toimialue kannattaa kaikki roolit sijoittaa samalle DC:lle. Roolien jakamisesta eri sijainteihin ei ole mitään etua.

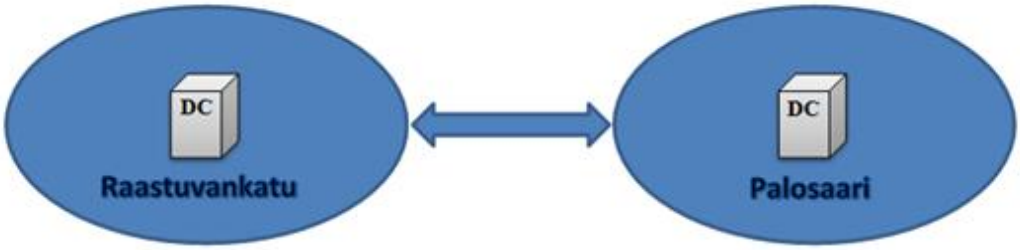
5.3.2 Active Directory -looginen rakenne

Lopuksi fyysisestä verkkorakenteesta luodaan looginen rakenne, jolla pyritään kuvaamaan AD:n rakennetta. Fyysinen rakenne on tarkoitus jakaa osiin DC:en sijaintien mukaan. Loogisen rakenteen avulla pyritään muodostamaan oikeanlaiset replikointiasetukset ja sijoittamaan AD:n palvelut mahdollisimman lähelle paikkaa, missä niitä tarvitaan. Kuvassa 9 on esimerkki loogisesta verkkorakenteesta, jossa toimialueen eri DC:sta on luotu ryhmiä, joiden avulla saadaan luotua järkeviä ja tehokkaita replikointiasetuksia niiden välille.



Kuva 9. Looginen-verkkorakenne./5/

Rakenteen avulla pystytään verkon replikointitoiminnot ja niiden aikavälit määrittelemään oikeiksi, jolloin DC:ssa tapahtuvat muutokset saadaan replikoitua mahdollisimman nopeasti koko verkon alueelle. Sen avulla on myös tarkoitus saada luotua mahdollisimman monia yhteyksiä DC:en välille, jolloin verkon toimintavarmuus kasvaa. Jos AD-verkon rakenne on pystytty pitämään yksinkertaisena ja DC:n määrä vähäisenä, voi yhteydet eri fyysisten paikkojen välille muodostaa automaattisesti. DC:t osaavat muodostaa automaattisesti replikointiyhteydet eri DC:n välille, jos niillä on pääsy koko verkon alueella ja se on hyvin reititetty. Vakiona replikointi suoritetaan 180 min välein. Kuvassa 10 on looginen rakenne verkosta, missä on vain kaksi DC:a samassa verkossa.



Kuva 10. Looginen verkkorakenne

5.4 DHCP

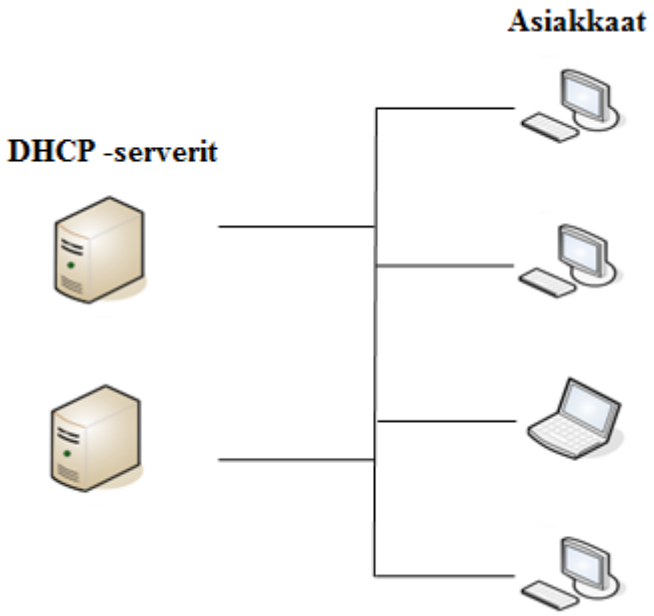
DHCP-palvelun suunnittelu aloitetaan verkkorakenteesta ja palvelun toteutustavasta. DHCP-palvelu voidaan toteuttaa organisaatiossa hajautetusti tai keskitetysti ja verkko-osoitteiden jako serverien tai reitittimien avulla.

Hajautetussa DHCP-palvelussa, jokaiselle aliverkolla on oma DHCP-serveri. Hajautetun toteutustavan etuna on, että DHCP-liikennettä saadaan vähennettyä verkosta. Verkkoon täytyy kuitenkin asentaa useita DHCP-servereitä, jos organisaatiossa on paljon aliverkkoja. Tämä vaikeuttaa verkonhallintaa. Keskitetysti toteutetussa DHCP-palvelussa serverit sijaitsevat samassa paikassa, mistä ne hoitavat verkko-osoitteiden jaon koko verkonalueelle.

Suunniteltaessa DHCP-palvelun sijoittamista reitittimelle tai serverille, päätökseen vaikuttaa eniten verkon asiakasmäärät. Reitittimet välittävät paljon verkkoliikennettä. DHCP-palvelua ei ole sen vuoksi kannattavaa sijoittaa reitittimeen kuin pienissä verkoissa esimerkiksi pk-yrityksissä, joissa verkon käyttäjämäärät ovat pieniä ja verkkoliikenne vähäistä. Verkoissa joissa on paljon asiakkaita, DHCP-palvelu kannattaa asentaa erilliselle serverille. DHCP-serveriä pystytään helposti hallitsemaan ja DHCP-liikenne nopeutuu, koska se hoidetaan erillisellä palvelimella.

VAMK:n kokoisessa organisaatiossa DHCP-palvelu kannattaa hoitaa keskitetysti kahdella klusteroidulla serverillä. Verkkossa on paljon asiakkaita ja se muodostuu useista aliverkoista. Kahden DHCP-serverin avulla DHCP-liikenne saada jaettua

tasaisesti molemmille palvelimille ja verkon toimintavarmuutta saadaan nostettua vikatapauksissa, joissa toinen palvelin ei ole toiminnassa. Kuvassa 11 on kahden DHCP-serverin verkkorakenne.



Kuva 11. Kahden DHCP-serverin verkko.

DHCP-serverit jakavat liikenteen ja asiakkaat saavat aina verkko-osoitteet vaikka toinen servereistä vikaantuisi. Niillä on yhteinen tietokanta, minkä perusteella ne pystyvät pitämään kirjaa verkko-osoitteista ja niiden jakamisesta./10/

5.5 DNS

DNS-serverit ovat tärkeässä roolissa AD-verkossa. AD vaatii, että verkossa on vähintään yksi toimiva DNS-serveri. DNS:n avulla AD muodostaa yhteydet esimerkiksi eri DC:n välille ja ilman toimivaa DNS-serveri, AD-verkkoa ei voi muodostaa.

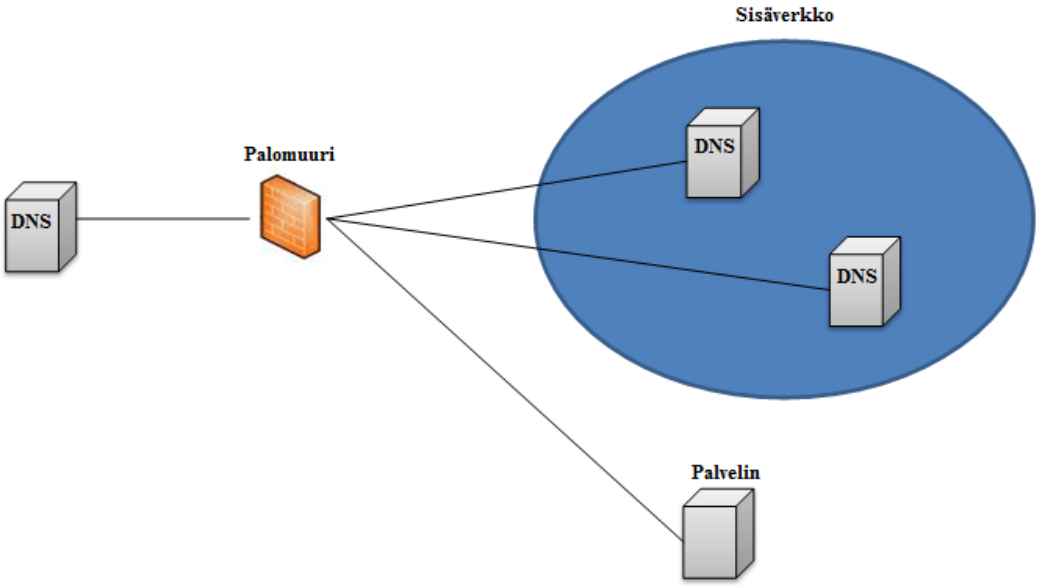
DNS-servereitä suunniteltaessa täytyy huomioida erityisesti minkälaiseen verkkoon ne tulevat. Verkonrakenne vaikuttaa erityisesti DNS-serverien määrään ja niiden sijaintiin. On suositeltavaa, että verkossa olisi vähintään kaksi DNS-serveriä ja ne olisivat sijoitettu paikkaan, mihin jokaisella verkon asiakkaalla olisi

pääsy. Verkon viansietokykyä pystytään kasvattamaan, kun verkkoon sijoitetaan useampi serveri. Usean serverin avulla verkon kuormitus saadaan jaettua ja DNS-liikenne pystytään välittämään vaikka toinen serveri vikaantuisi./11/

AD-verkossa on kannattavaa asentaa DNS-serveri kaikille DC:lle. Tämän avulla saadaan replikoitua DNS-tiedot samaan aikaan muiden AD-tietojen kanssa ja verkon kuormitus pystytään jakamaan. DNS-serveri kuitenkin nostaa hieman DC:n laitteistovaatimuksia, sillä DNS-serveri lataa käynnistyessään kaikki DNS-tiedot RAM-muistiin. Yksi DNS-tieto käyttää noin 100 tavua muistia ja isoissa verkoissa muistivaatimukset kasvavat huomattavasti./11/

DNS-servereitä sijoittaessa kannattaa myös huomioida tietoturva. Sisäverkon DNS-serverit on järkevää erottaa ulkoverkosta palomuurin avulla. Lisäksi sisä- ja ulkoverkon DNS-tiedot kannattaa erottaa toisistaan. Tämän avulla ulkoverkosta ei ole suoraa pääsyä sisäverkon DNS-tietoihin, vaan ne ohjataan ulkoisen serverin kautta. Tämän avulla saadaan verkon tietoturvaa nostettua ja ulkoverkon liikenne pystytään ohjaamaan halutuille palvelimille.

VAMK:n kokoiselle organisaatiolle DNS-servereitä tulisi sisäverkkoon kaksi ja ne sijaitsisivat DC:lla. Kahden DNS-serverin avulla varmistettaisiin verkon toiminta ja kuormitusta saataisiin jaettua. Lisäksi ulkoverkossa olisi yksi DNS-serveri, jolla tuleva liikenne saataisiin ohjattua halutulle palvelimelle esimerkiksi DMZ-alueelle. Kuvassa 12 on näkyvillä suunniteltu verkkorakenne.



Kuva 12. DNS-verkkorakenne.

Kuvassa 12 näkyy DNS-verkonrakenne. Verkossa on kolme DNS-serveriä, kaksi sisäverkossa ja yksi ulkoverkossa. Palomuurin avulla verkko on jaettu kahteen eri alueeseen. Palvelin on erotettu sisäverkosta ja siihen saa yhteyden myös ulkoverkosta. Tämän avulla verkon tietoturvaa saadaan nostettua. Ulkoverkon DNS-serveri pystyy ohjamaan saapuvan liikenteen halutulle palvelimella. Lisäksi se välittää eteenpäin sisäverkon DNS-servereiltä saapuvaa liikennettä.

5.6 Tulostinpalvelu

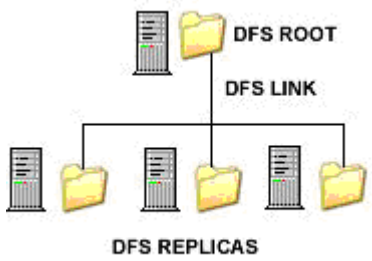
Tulostinpalvelun suunnitteluun vaikuttaa eniten organisaation rakenne. Useista yksiköistä koostuvassa organisaatiossa tulostinpalvelimien sijoittaminen on huomattavasti hankalampaa, kuin pienissä organisaatioissa. Lisäksi joidenkin organisaatioiden sisäinen rakenne vaatii, että ne on erotettu toisistaan. Tulostinpalvelimien määrään ja niiden sijoittamisessa täytyy myös huomioida verkon käyttäjämäärät. Microsoftin testien mukaan yksi tulostinpalvelin pystyy palvelemaan 1500 tulostinta ja 5000-10000 asiakasta. Tulostinpalvelimien määrää voidaan joutua kuitenkin kasvattamaan, jos verkon tulostimia käytetään paljon ja niillä tulostetaan suuria tiedostoja esimerkiksi PDFiä./5/

VAMK:n kokoiselle organisaatiolle tulostinpalvelimia tulisi neljä kappaletta. Neljän tulostinpalvelimen avulla verkon kuormitusta saataisiin vähennettyä ja organisaatio pystyttäisiin jakamaan kahteen osaan käyttäjien mukaan. Kaksi tulostinpalvelinta sijoitettaisiin Raastuvankadulle ja kaksi Palosaarelle. Tämän avulla eri yksiköiden välistä tulostinliikennettä saataisiin vähennettyä. Lisäksi molemmissa yksiköissä toinen tulostinpalvelin tulisi vain henkilökunnan käyttöön, jonka avulla jaettaisiin koulun yleisen alueen ulkopuolella sijaitsevat tulostimet. Tämän tulostinpalvelimen tarkoitus on nostaa verkon tietoturvaa.

5.7 Levypalvelu

Monissa organisaatioissa levypalvelu kannattaa hoitaa Distributed File System-tekniikan (DFS) avulla. Sen avulla Levypalvelu voi muodostua useista palvelimista ja ne pystytään yhdistämään yhdeksi suureksi tiedostopalvelimeksi. DFS:n avulla pystytään nopeuttamaan verkon tiedostojen jakoa ja niiden saatavuutta. Verkon asiakkaiden ei tarvitse välttämättä tietää palvelimien fyysistä sijaintia, vaan kaikki tiedostot löytyvät yhden kansion alta. DFS mahdollistaa myös tiedostojen jaon Unix ja Mac -käyttöjärjestelmiin. Kuvassa 13 näkyy DFS -kansiorakenne.

DFS Root tarjoaa käyttäjille yhteyden verkkojakoihin ja luo nimiavaruuden, mikä näkyy verkkojaoissa. Se sisältää käyttäjien kansioita ja tiedostoja. DFS Linkin avulla käyttäjät ohjataan oikeille palvelimille, missä tiedostot sijaitsevat. DFS Replicat ovat kohteita, mistä käyttäjän kansiot ja tiedostot löytyvät. Mikäli halutut tiedot löytyvät useammalta palvelimelta käyttäjä ohjataan lähimmälle./5/,/15/,/16/



Kuva 13. DFS rakenne. /15/

Windows Server 2008 R2 tukee myös Distributed File System replication -tekniikkaa (DFS-R). Se mahdollistaa, että kaikki DFS-palvelimien tiedot replikoituvat automaattisesti, kun niissä tapahtuu muutoksia. DFS-R -tekniikan etuina on, että verkon kaikkien asiakkaiden ei tarvitse olla yhteydessä samoille palvelimille vaan käyttäjämäärät voidaan jakaa eri palvelimien välillä. Tämän avulla saadaan verkon ja palvelimien kuormitusta tasattua.

DFS-R parantaa myös verkon viansietokykyä tilanteissa, joissa jokin palvelimista kaatuu tai siihen ei saada yhteyttä. Käyttäjät pääsevät silti käsiksi tiedostoihin muiden palvelimien avulla, eikä se haittaa verkon toimintaa. Vaikka DFS-R replikoi tiedot kaikille palvelimille, ei se poista varmuuskopioinnin tarvetta. DFS-R -tekniikan avulla voidaan estää palvelimissa tapahtuvat kovalevy viat, mutta tiedostojen korruptoitumiset ovat silti mahdollisia.

DFS-R -tekniikka soveltuu hyviin ympäristöihin, missä verkonkuormaa halutaan jakaa eri palvelimien välillä. Ongelmana replikoinnissa voi kuitenkin olla verkkoliikenteen määrän kasvu. Se ei välttämättä sovellu ympäristöihin, missä palvelimille tallennetaan kaiken aikaa suuria tiedostoja ja niihin tehdään paljon muutoksia. Tämä voi aiheuttaa, että replikointiliikenne kasvaa liian suureksi, eikä verkko pysty käsittelemään sitä. Se on mahdollista kuitenkin estää rajoittamalla replikointiliikennettä ja luomalla replikoinnille aikavälit. DFS-R sopeutuu parhaiten ympäristöihin missä tiedostoja luetaan paljon, mutta niihin ei tehdä suuria muutoksia.

DFS olisi myös hyvä toteutustapa VAMK:n kokoisen organisaation levypalveluksi, koska verkossa liikkuu vähän suuria tiedostoja ja niissä tapahtuvat muutokset ovat pieniä. Tiedostoihin pitää olla pääsy myös koko verkon alueelta. DFS:n avulla tiedostojen jako onnistuisi helposti ja verkon kuormitus saataisiin jaettua. Palvelimet tulisi sijoittaa paikkoihin, missä on eniten käyttäjiä. VAMK:n tapauksessa palvelimet sijoitettaisiin Palosaarelle ja Raastuvankadulle. Tämän avulla käyttäjillä olisi nopea pääsy tiedostoihin molemmissa paikoissa.

Levypalvelimia sijoitettaessa täytyy myös tilankäyttö arvioida. VAMK:lla on tällä hetkellä käytössä, jokaiselle käyttäjälle ennalta määrätyt hakemistojen koot. Niiden avulla palvelimien tilantarve voidaan arvioida, jos henkilökunnalle annetaan 10 GB:n ja opiskelijoille 200MB:n kotihakemistot niin palvelimille täytyy varata noin 3 TB levytilaa. Lisäksi käytössä on yhteisiä verkkoasemia ja sovelluksia, jotka käyttävät levypalvelua, joten palvelimien kooksi kannatta alustavasti määritellä ainakin 6 TB. Tilantarve voi kuitenkin kasvaa tulevaisuudessa, joten voi olla kannattava määritellä palvelimille jo alussa ylimääräistä tilaa.

Palvelimia sijoitettaisiin aluksi kolme kappaletta. Yksi palvelin tulisi Raastuvankadulle ja kaksi Palosaarelle. Jokaisella palvelimella olisi tilaa vähintään 2 TB. DFS mahdollistaa, että palvelimia on mahdollista lisätä kansiorakenteeseen myöhemmin, jos palvelimien kapasiteettia halutaan kasvattaa. Kaikkiin palvelimiin olisi mahdollisuus saada yhteys koko verkon alueelta, mutta ne olisi sijoitettu järkevästi tilantarpeen mukaan. Molemmat yksiköt käyttäisivät ensisijaisesti lähintä palvelinta, mutta kaikkiin tiedostoihin olisi kuitenkin pääsy koko verkon alueelta. Lopuksi verkkoon lisättäisiin vielä yksi palvelin, minkä avulla hoidettaisiin varmuuskopiointi.

5.8 Verkkorakenteen yhteenveto

Active Directory

- Yksi metsä ja yksi toimialue
- 2 Domain Controlleria

DHCP

- 2 serveriä

DNS

- 2 Sisäverkkoon ja 1 ulkoverkkoon

Tulostinpalvelu

- 4 Tulostinpalvelinta. 2 yleiseen käyttöön ja 2 henkilökunnalle

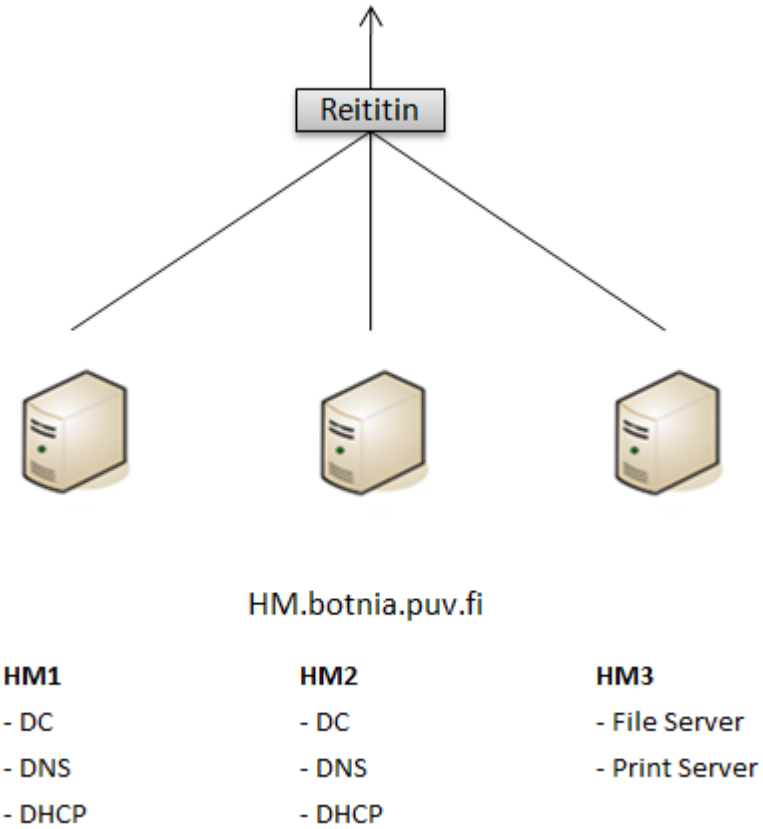
Levypalvelu

- DFS-tekniikka
- 3 levypalvelinta
- Varmuuskopiointipalvelin

6 LABORATORIOTYÖ

6.1 Yleistä

Työssä rakennetaan pieni yritysverkko käyttäen kolmea Windows Server 2008 R2 -serveriä. Verkko rakentuu AD-ympäristöön ja sen avulla pyritään simuloimaan oikean yritysverkon toimintaa. Verkkoon asennetaan viisi erilaista verkkopalvelua. Servereistä HM1 ja HM2 hoitavat DC-, DNS-, ja DHCP-palvelut. Servereillä ajetaan samoja palveluita, joiden avulla varmistetaan verkon toimivuus myös vikatilanteissa, joissa toinen serveri ei ole toimintakunnossa. Verkossa on myös File- ja Print Server -palvelut ja ne sijaitsevat HM3-serverillä. Kuvassa 16 on esitetty verkon rakenne.



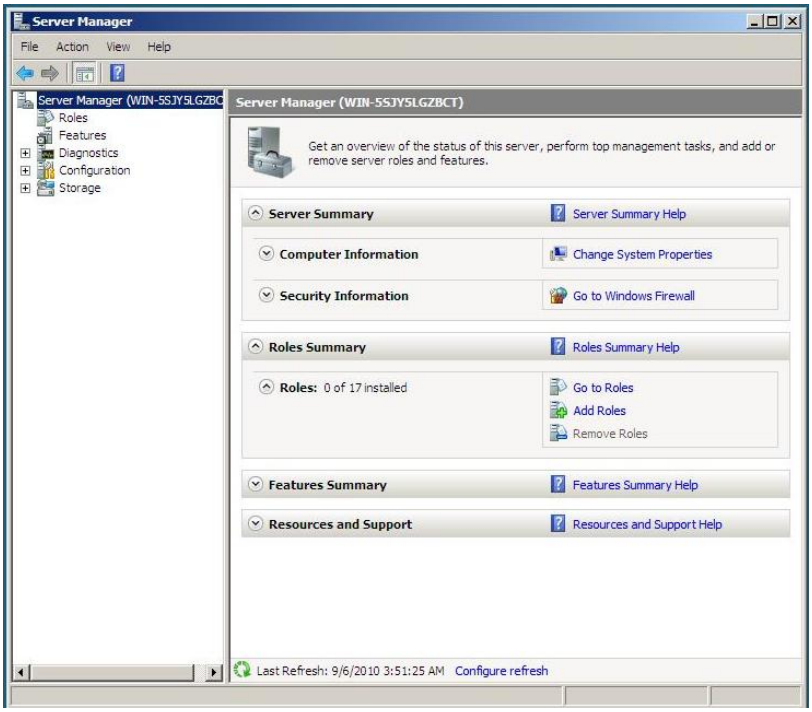
Kuva 16. Laboratorioverkon-rakenne.

Työssä luodaan HM.botnia.puv.fi niminen toimialue. Toimialueella sijaitsevat serverit ja työasemat yhdistetään toisiinsa reitittimellä, josta on pääsy ulkoverkkoon ja servereillä sijaitseviin palveluihin.

6.2 Windows Server 2008 R2 -asennus

Windows Server 2008 R2 -asennus tapahtuu samanlailla, kuin muidenkin Windows-tuotteiden asennus ja se muistuttaakin paljon Windows 7 -asennusta. Asennus käynnistetään DVD:ltä ja sen aikana määritellään lähes kaikki samat asetuksen, mitä muidenkin Windows-tuotteiden kohdalla tehdään. Asennuksen aikana valitaan myös Windows Serverin -versio. Valittavissa on kaksi erilaista Windows Server 2008 R2 -asennusta, Full Installation ja Server Core Installation. Full Installation on asennus, jossa on mukana kaikki käyttöjärjestelmän komponentit ja Core Installation sisältää vain ydinkomponentit. Windows-serverin versioksi valittiin tässä opinnäytetyössä ”Windows Server 2008 R2 Enterprise (Full Installation)”.

Windows-serverin asennuksen jälkeen kaikkiin asetuksiin päästään käsiksi Server Manager -konsolin avulla. Konsolin avulla pystytään lisäämään serverille erilaisia rooleja helposti sekä pystytään muokkaamaan niiden asetuksia. Server Manager on keskeisessä roolissa, kun serveriä pystytetään. Kuvassa 17 on Server Manager -konsoli.



Kuva 17. Server Manager -konsoli.

6.3 HM1-serverin asennus

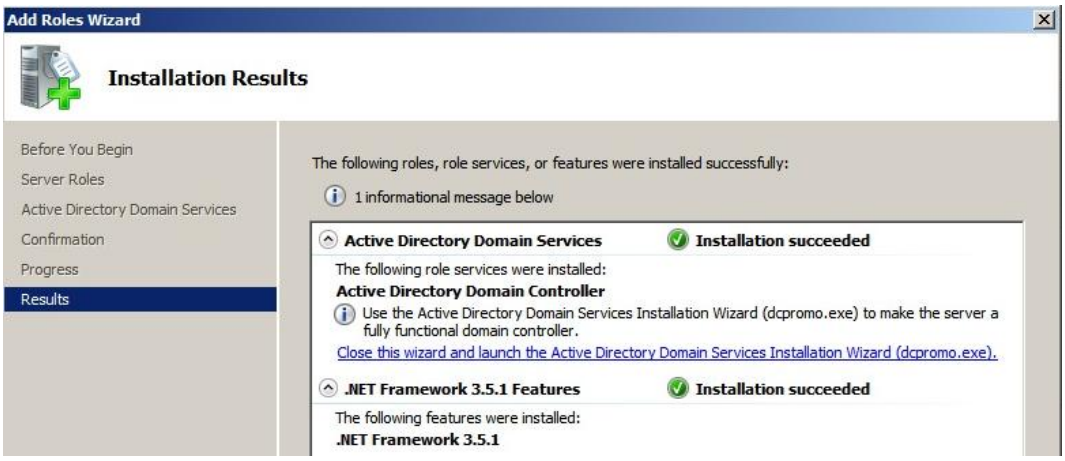
Asennus aloitetaan määrittelemällä servereille staattiset IP-numerot. Servereillä täytyy määritellä IP-osoitteet, joiden avulla serverit ja niiden palvelut löytyvät. Mikäli IP-osoitteet muuttuvat serverien palvelujen asennuksen jälkeen voi palvelujen väliset yhteydet kadota ja verkko ei toimi. Reitittimeltä täytyy muistaa ottaa myös DHCP-ominaisuus pois päältä, ettei verkossa jaettavat IP-osoitteet mene sekaisin. Taulukossa 3 on servereille määritetyt IP-osoitteet.

Taulukko 3. Serverien IP-osoitteet.

	HM1	HM2	HM3
IP	192.168.10.1	192.168.10.2	192.168.10.3
mask	255.255.255.0	255.255.255.0	255.255.255.0
gateway	192.168.10.4	192.168.10.4	192.168.10.4
DNS	192.168.10.1	192.168.10.2	192.168.10.1

6.3.1 Active Directory

AD-verkon asennus aloitetaan lisäämällä ohjauspalvelimen-rooli (Active Directory Domain Services) Server Managerilla. Asennus suorittaa tarpeelliset asennukset, jonka jälkeen se pyytää suorittamaan Installation Wizardin (dcpromo.exe). Wizardin avulla serveristä pystytään tekemään toimialueen DC. Kuvassa 18 on dcpromo.exe Installation Wizard ja suoritettu ohjauspalvelimen asennus.



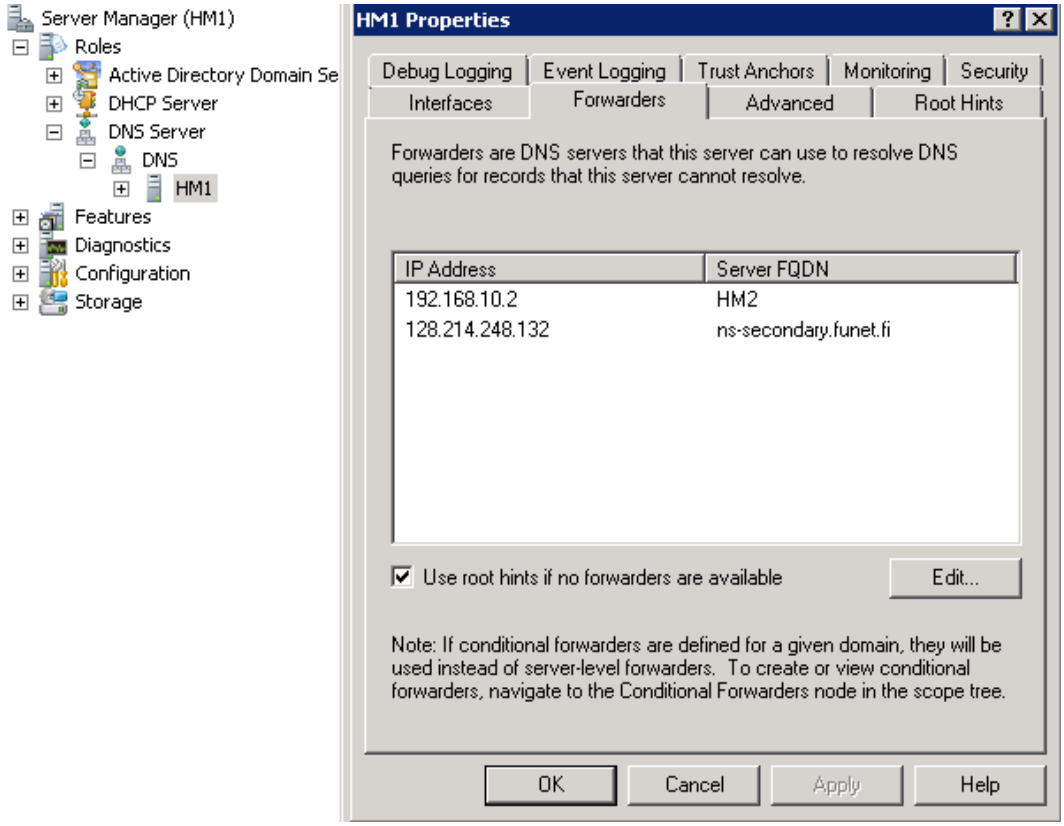
Kuva 18. Ohjauspalvelin-roolin asennus.

Kun dcpromo.exe asennus käynnistyy, täytyy määritellä luodaanko DC valmiiseen AD-verkkoon vai luodaanko uusi AD-metsä. Tässä työssä luotiin uusi metsä ja asennuksessa valittiin ”Create new domain in a new forest”. Uudelle toimialueelle annettiin nimeksi hm.botnia.puv.fi. Asennus haluaa seuraavaksi määritellä metsän toimintatason, mikä määrää DC:n käyttöjärjestelmä-versioiden yhteensopivuudet. Tässä työssä luotiin uusi metsä ja kaikilla servereillä käytettiin uusinta AD-versiota, joten niiden ei tarvitse olla yhteensopivia vanhempien AD-versioiden kanssa. Toimintatasoksi valittiin ”Windows Server 2008 R2”.

Seuraavaksi asennus ehdottaa DNS-palvelun asennusta. Koska kyseisessä verkossa ei ole valmiiksi DNS-serveriä ja AD -verkko kuitenkin vaatii sen, täytyy ensimmäisestä toimialueen DC:sta tehdä myös DNS-serveri. AD:lle määritellään vielä lopuksi salasana, jonka jälkeen AD- ja DNS-palvelu asentuu serverille.

Asennuksen jälkeen serveri täytyy käynnistää uudelleen, minkä jälkeen toimialueelle pystyy kirjautumaan järjestelmänvalvojan tunnuksilla. AD- ja DNS-rooli näkyy tämän jälkeen Server Manager -konsolilla valmiiksi asennettuna.

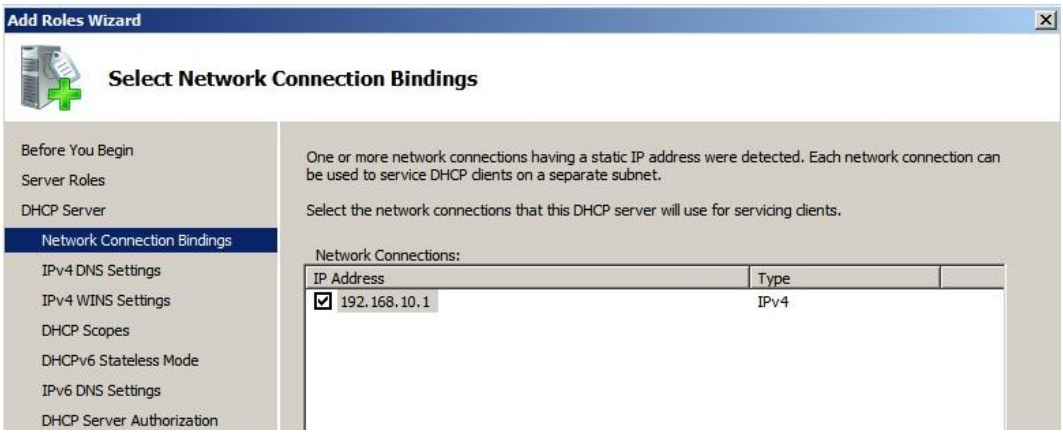
DNS-serverille täytyy muistaa roolin asennuksen jälkeen määritellä myös liikenteenohjaus. Sen avulla DNS-tietoja voidaan hakea muilta DNS-servereiltä, mikäli haettua tietoa ei löydy omasta tietokannasta. HM1-serverin DNS-asetuksiin lisättiin HM2-serverin IP-osoite sekä ulkoisen Funet.fi DNS-serverin osoite. Näiden osoitteiden avulla pystytään liikenne ohjaamaan sisäverkosta ulkoverkkoon. Kuvassa 19 on HM1-serverin DNS-asetuksien luonti.



Kuva 19. DNS-liikenteen ohjaus.

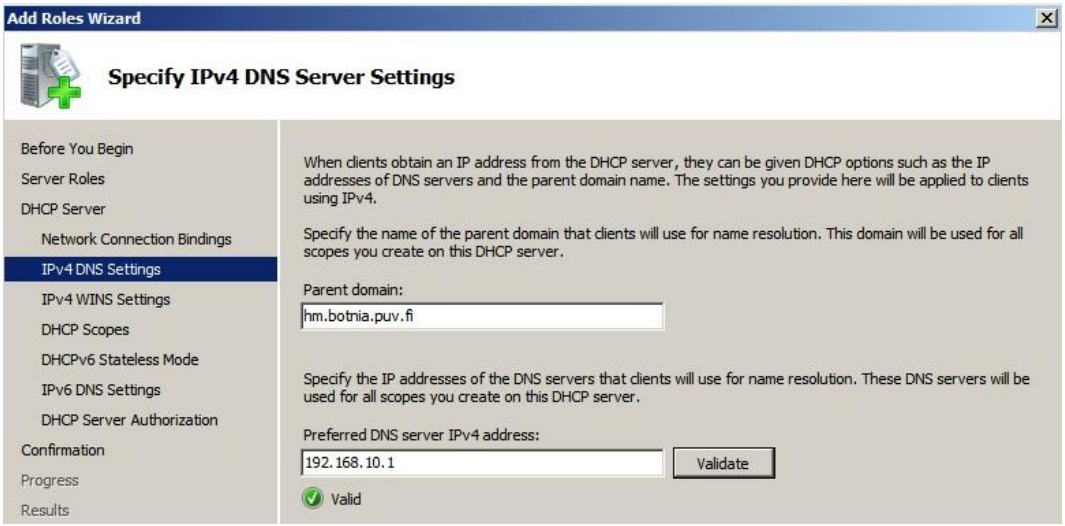
6.3.2 DHCP

DHCP-palvelun asennus aloitetaan samanlailla, kuin AD-roolin asennus. Server Manager -konsolilla valitaan Add Roles ja DHCP. Ensimmäisenä asennus haluaa tietää, mitä yhteyttä käytetään DHCP-serverinä. Yhteydellä täytyy olla staattinen IP-numero, jotta sitä voidaan käyttää DHCP-palvelun asennuksessa. Serverille määriteltiin alussa staattinen IP, joten kyseistä verkkoyhteyttä voidaan käyttää DHCP-palvelun asennuksessa. Kuvassa 20 on DHCP-verkkoyhteyden valinta.



Kuva 20. DHCP-verkkoyhteyden valinta.

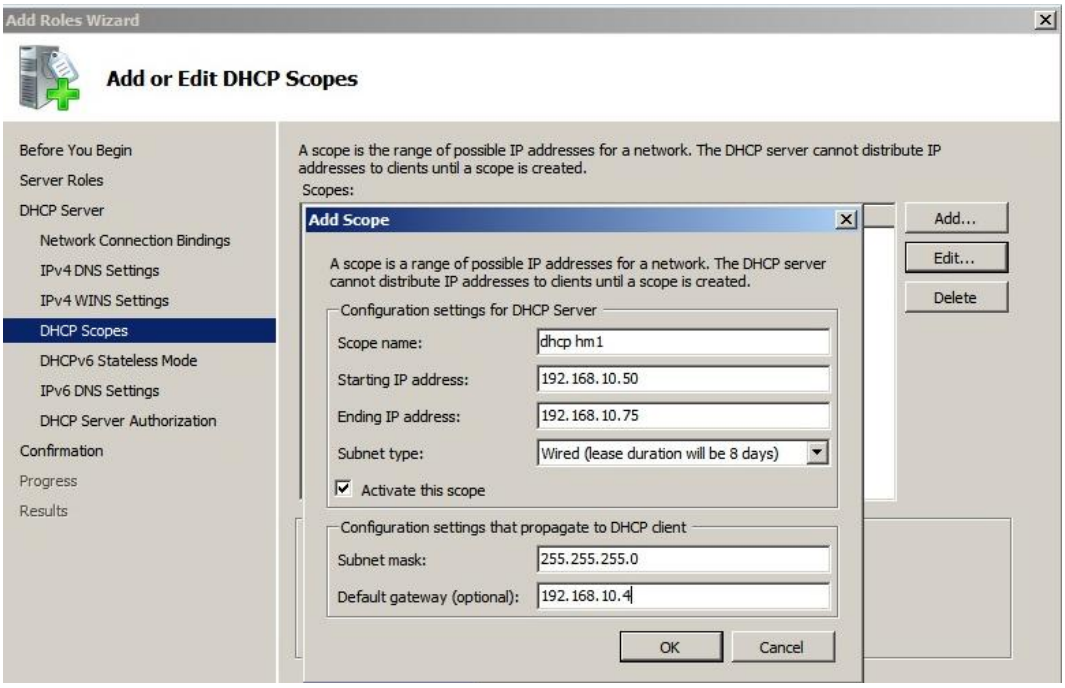
DHCP:lle määritellään seuraavaksi toimialue, missä sitä käytetään ja ensisijainen DNS-osoite. DNS-osoitteena voidaan käyttää serverin omaa IP-osoitetta, koska DNS-palvelu löytyy samalta serveriltä. Kuvassa 21 on toimialueen ja DNS-serverin asetusten määrittely.



Kuva 21. Toimialue ja DNS-osoitteet.

DHCP-serverille täytyy myös määritelle IP-alue (Scope), jota se jakaa verkkoon. Koska verkkoon tulee kaksi DHCP-serveriä, verkossa käytettävät IP-osoitteet jaetaan kahteen osaan. HM1 jakaa osoitteet alueelta 192.168.10.50-192.168.10.75 ja HM2 192.168.10.76-192.168.10.100. Näin verkkoon saadaan jaettu IP-osoitteita molemmilta servereiltä, eivätkä osoitteet mene päällekkäin. DHCP-

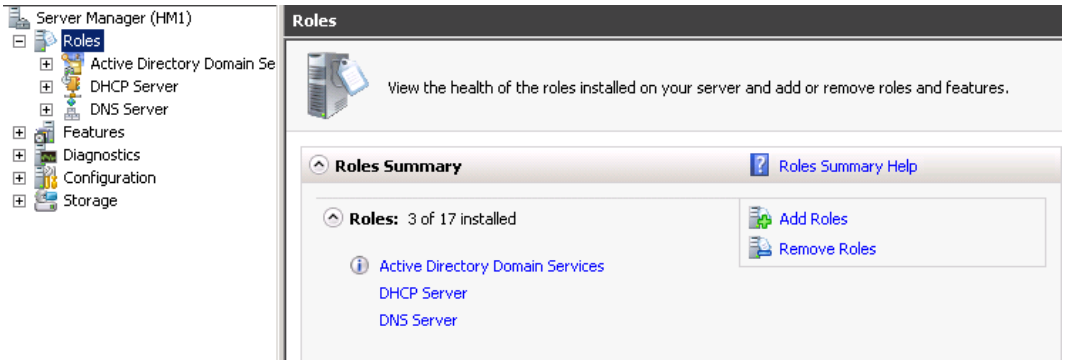
serveri eivät ole myöskään riippuvaisia toisistaan ja ne toimivat myös vikatilanteissa. Kuvassa 22 on IP-alueen luonti.



Kuva 22. IP-alueen luonti.

IP-alueiden luonnin jälkeen serveri näyttää vielä yhteenvedon asetuksista, jonka jälkeen DHCP-palvelu asentuu serverille.

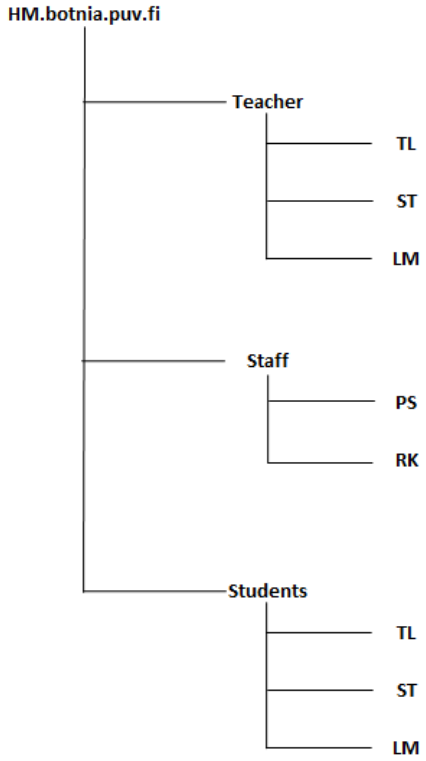
DHCP-roolin asennuksen jälkeen kaikki HM1-serverin roolit on asennettu ja ne näkyvät Server Manager –konsolilla. Kuvassa 23 näkyy serverille asennetut AD-DNS- ja DHCP-roolit.



Kuva 23. AD- DNS- ja DHCP-roolit.

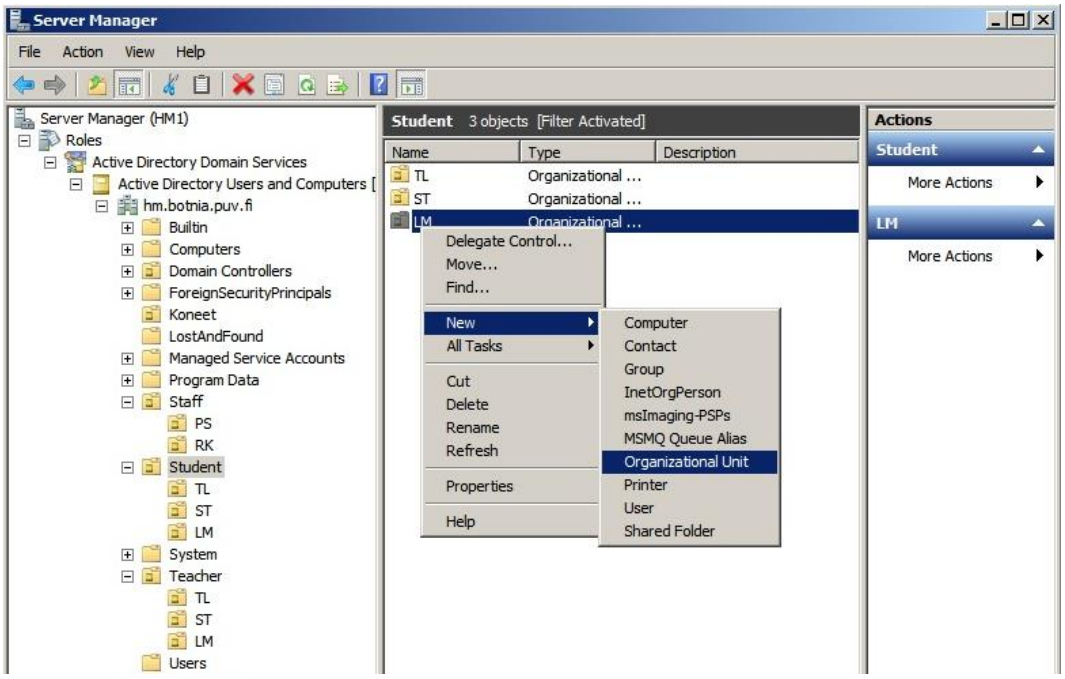
6.3.3 Käyttäjien ja ryhmien luonti

Tässä työssä verkkoon luotiin organisaatioyksikkörakenne, jossa käytettiin esimerkkinä VAMK:n rakennetta. Käyttäjät jaettiin eri organisaatioyksikköihin henkilökunnan, oppilaiden sekä yksiköiden mukaan. Jokaiseen organisaatioyksikköön luotiin myös käyttäjä, jonka avulla niiden toimintaa pystyttiin testaamaan. Kuvassa 24 on esitetty organisaatioyksikkörakenne.



Kuva 24. Organisaatioyksikkörakenne.

Käyttäjät jaetaan kolmeen eri organisaatioyksikköön, joiden sisällä käyttäjät jaetaan yksiköiden mukaan omiin ryhmiin. Näin käyttäjistä saadaan järkeviä ja helposti hallittavia ryhmiä. Käyttäjien ja ryhmien luonti tapahtuu Active Directory Users and Computers -valikosta. Kuvassa 25 on esitetty organisaatioyksikkörakenteen luonti.

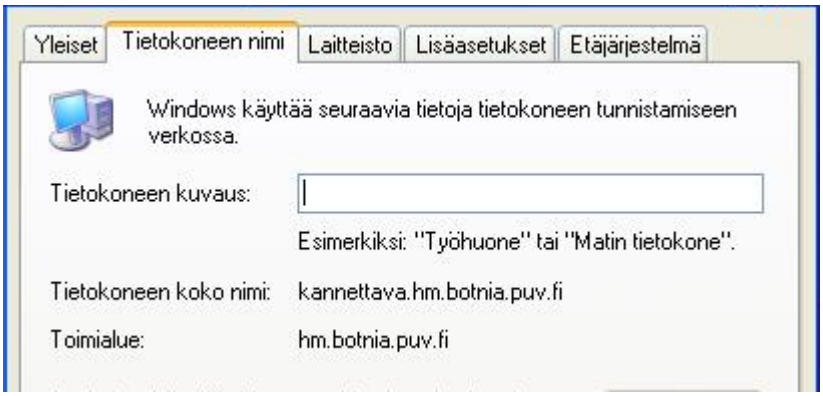


Kuva 25. Organisaatioyksiköiden luonti.

Organisaatioyksiköiden luonti ja hallinta muistuttaa paljon normaalia Windowsin käyttämää kansiorakennetta. Käyttäjät ja ryhmät luodaan organisaatioyksiköiden alle ja niille pystytään luomaan yhteisiä käyttöoikeuksia ja käynnistysasetuksia. Rakenne kannattaa muistaa pitää kuitenkin mahdollisimman yksinkertaisena. Käyttäjiä ei kannata sijoittaa useisiin eri ryhmiin, sillä oikeuksien ja asetuksien hallinta voi muodostua hankalaksi, jos käyttäjä on sijoitettu moneen eri paikkaan. Organisaatioyksikkörakennetta muokatessa kannattaa huomioida, että kaikki muokkaukset vaikuttavat kaikkiin sen alapuolella oleviin käyttäjiin ja ryhmiin. Windows onkin tästä syystä estänyt niiden poistamisen, jos rakennetta halutaan muokata kuitenkin vapaammin, asetuksista täytyy erikseen pistää päälle Advanced Features, jonka jälkeen organisaatioyksiköistä pystytään poistamaan Accidental Delete -ominaisuus.

6.3.4 HM1-serverin testaus

Serverin toiminta testataan kirjautumalla luodulla käyttäjillä toimialueelle, jos kirjautuminen onnistuu AD, DNS ja DHCP toimii oikein. Kuvasta 26 nähdään, että AD on toiminnassa ja luodulla käyttäjällä pystyttiin kirjautumaan toimialueelle. Kirjautuminen varmistaa myös, että DNS-serveri on toiminnassa. Verkkoon ei pystyttäisi kirjautumaan, mikäli DNS-serveriin ei saataisi yhteyttä.



Kuva 26. Toimialueelle liittyminen.

Kun toimialueelle oli liitytty, nähtiin myös, että DHCP-serveri oli antanut työasemalle IP-osoitteen ennalta määrätyltä alueelta sekä DNS-osoitteet. Kuvassa 27 on työaseman saama IP-osoite sekä DNS-osoitteet.

```
Ethernet-sovitin Lähiverkkoyhteys:

        Yhteyskohtainen DNS-liite . . . . : hm.botnia.puv.fi
        Kuvaus  . . . . . . . . . . . . . : Realtek RTL8169/8110 Family Gigabit
Ethernet NIC
        Fyysinen osoite . . . . . . . . . : 00-16-D4-CC-0C-D2
        DHCP käytössä . . . . . . . . . . : Kyllä
        Automaattinen määritys käytössä . : Kyllä
        IP-osoite . . . . . . . . . . . . : 192.168.10.50
        Aliverkon peite . . . . . . . . . : 255.255.255.0
        Oletusyhdyskäytävä. . . . . . . . : 192.168.10.4
        DHCP-palvelin . . . . . . . . . . : 192.168.10.1
        DNS-palvelimet  . . . . . . . . . : 192.168.10.1
                                            192.168.10.2
        Käyttölupa myönnetty  . . . . . . : 26. lokakuuta 2010 12:16:58
        Käyttölupa vanhentuu  . . . . . . : 3. marraskuuta 2010 12:16:58
```

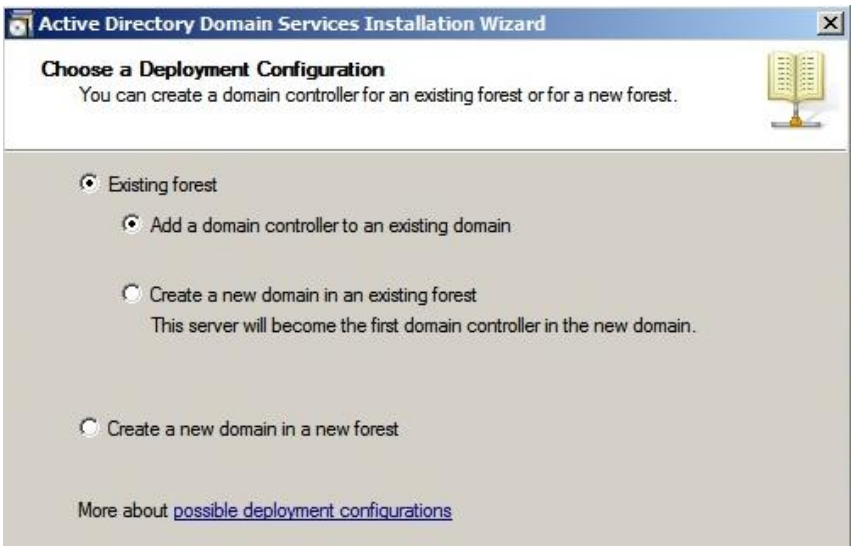
Kuva 27. Työaseman IP-osoite sekä DNS-osoitteet.

6.4 HM2-serverin asennus

HM2-serverille asennetaan kaikki samat palvelu, mitkä löytyvät HM1-serveriltä. Palvelujen asentaminen tapahtuu samanlailla ja asennuksen aikana täytyy tehdä vain pieniä muutoksia.

6.4.1 Active Directory

AD asennetaan samanlailla siihen asti, kunnes täytyy määritellä luodaanko uusi metsä vai asennetaanko DC jo olemassa olevaan metsään. HM1-serverille on luotu jo metsä, joten HM2-serveri asennetaan kyseiseen metsään toiseksi DC:ksi. Kuvassa 28 on DC:n rakenteen ja sijainnin määrittely.



Kuva 28. DC:n luonti olemassa olevaan metsään.

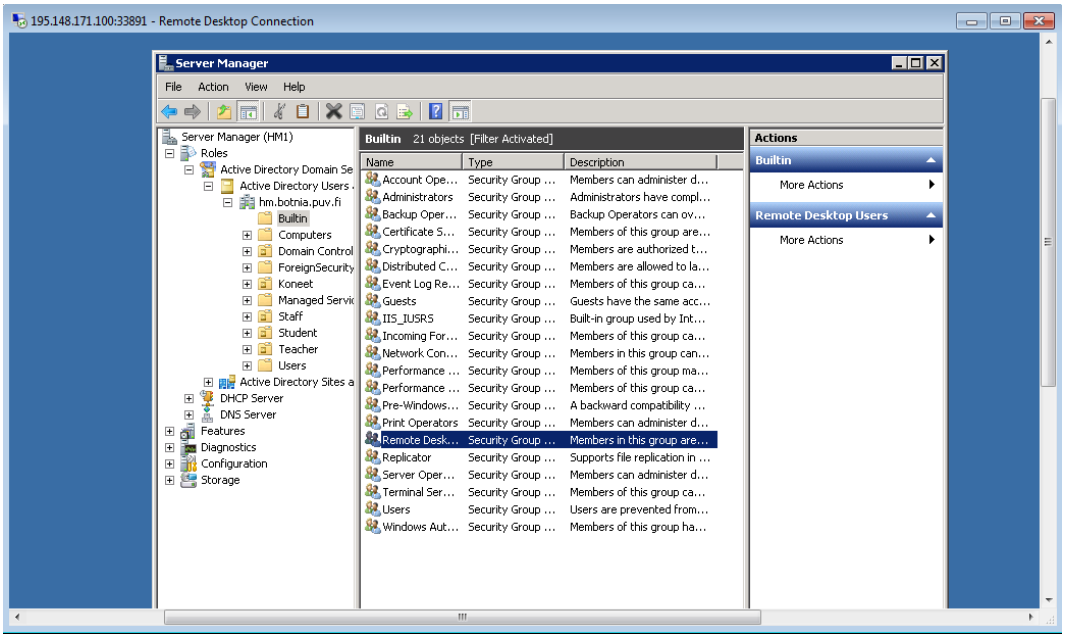
Seuraavaksi AD:lle täytyy määritellä, mihin toimialueeseen se liitetään. Toimialueeksi määriteltiin hm.botnia.puv.fi. Asennus vaatii myös toimialueen järjestelmänvalvojan salasanan, jotta liittyminen toimialueen toiseksi DC:ksi onnistuu. Tämän jälkeen asennus suoritetaan samanlailla, kuin HM1-serverin asennus. Asennuksen lopussa HM2-serveri ottaa vielä yhteyden HM1-serverille ja replikoi AD-tietokannan.

6.4.2 DHCP

DHCP-serverin asennuksessa ainoana erona HM1-serveriin verrattuna on IP-alueen luonti, jota DHCP-serveri jakaa. HM2-serverille täytyy määritellään eri IP-alue. Eri IP-alueen avulla molemmat serverit pystyvät jakamaan samaan aikaan IP-osoitteita verkkoon ja ne eivät mene päällekkäin. IP-alueen määrittely tapahtuu Kuvan 22 mukaisesti, mutta IP-alueeksi määritellään HM2-serverille 192.168.10.76- 192.168.10.100.

6.4.3 Remote Desktop

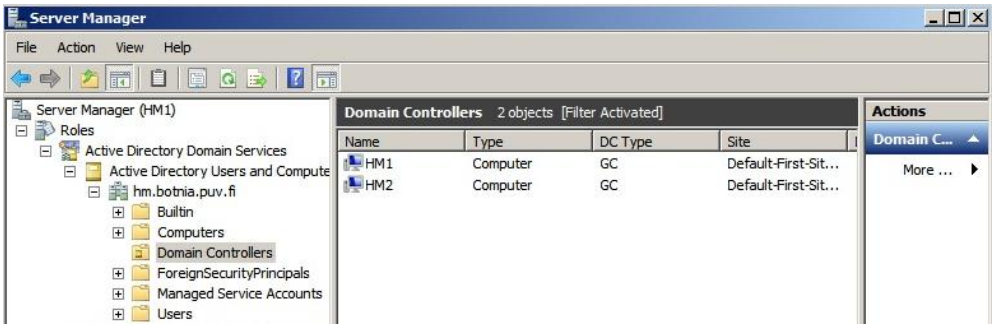
Serverille asennettiin myös etäyhteys (Remote Desktop), jonka avulla palvelimeen saadaan yhteys myös verkon ulkopuolelta. Etäyhteys asennetaan lisäämällä Remote Desktop -rooli Server Managerista. Etäyhteyttä varten reitittimestä täytyy ohjata portti 3389 kyseiselle serverille. Tämän jälkeen halutut käyttäjät lisätään Remote Desktop User -ryhmään, joka löytyy ”Builtin” organisaatioyksikön alta. Tässä työssä kaikki käyttäjät lisättiin kyseiseen ryhmään. Kuvassa 30 on etäyhteyden avulla esitetty Remote Desktop User -käyttäjien määrittely.



Kuva 30. Remote Desktop User -käyttäjien määrittely.

6.5 AD-, DNS- ja DHCP-palvelujen testaus

AD-, DNS- ja DHCP-asennuksien jälkeen, HM1- ja HM2-serverien tulisi löytää toisensa verkosta ja toimia myös tilanteissa, joissa toinen serveri ei ole käytettävissä. Toimialueelle asennetut DC:t saadaan näkyviin Server Manager -konsolin avulla. Molemmat DC:t löytyvät Domain Controllers -hakemiston alta. Kuvassa 31 on Server Manager -konsoli ja verkkoon asennetut DC:t.



Kuva 31. Domain Controllers -hakemisto.

Tämän jälkeen verkon toimintaa testattiin kytkemällä HM1-serveri pois verkosta. AD-verkkoon pitäisi silti olla pääsy ja HM2-serverin tulisi pystyä antamaan myös IP-osoite. Kuvasta 32 nähdään, että yhteys pystytään muodostamaan AD-verkkoon ja IP-soite saadaan HM2-serverin IP-alueelta 192.168.10.76-192.168.10.100.

Kuva 32. HM2-serverin testaus.

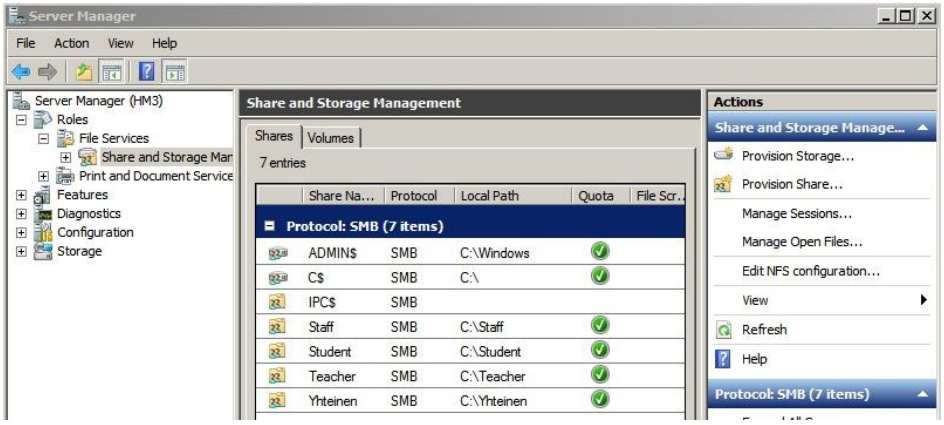
6.6 HM3-serverin asennus.

Verkossa sijaitsevat levy- ja tulostinpalvelut asennetaan HM3-serverille. Palvelut saadaan asennettua Server Manager -konsolilla, lisäämällä File Services ja Print Services -roolit. Roolien asennuksessa ei tarvitse tehdä mitään erityisiä asetuksia. Ainoastaan File Service -roolin aikana tarvitsee valita asennettavaksi myös File Server Resource Manager ja Network file system -lisäpalvelut. Näiden palvelujen avulla pystytään levyjakoja tarkkailemaan paremmin ja ne voidaan tehdä myös muiden käyttöjärjestelmien välille. Kuvassa 33 on HM3-serverille asennetut roolit.

Kuva 33. HM3-serverin roolit.

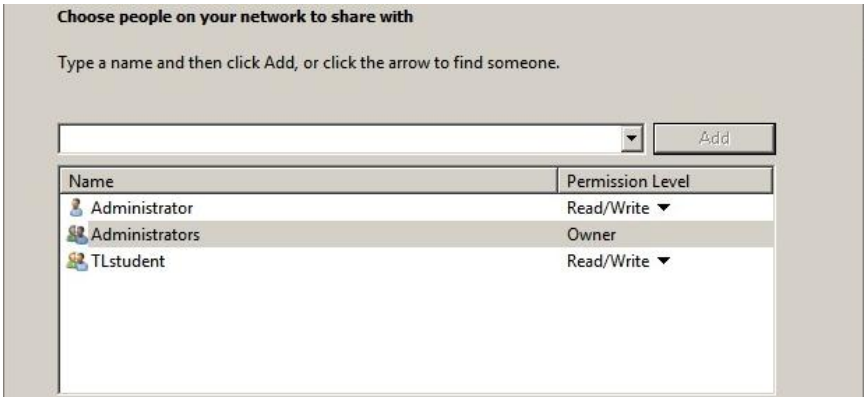
6.6.1 Levyjako

Serverille tehtyjä levyjakoja pystytään hallitsemaan Share and Storage Managmentin avulla. Kuvassa 34 on luotu henkilökunnalle, opiskelijoille ja opettajille oma verkkojako sekä yksi yhteinen verkkojako.



Kuva 34. Verkkojako

Kansioiden alle luotiin myös, jokaiselle käyttäjäryhmälle oma verkkojako ja niihin määriteltiin oikeudet, joiden avulla rajoitettiin muiden käyttäjien pääsyä. Kuvassa 35 on esimerkki TLstudent-kansion käyttöoikeuksien määrittelystä.

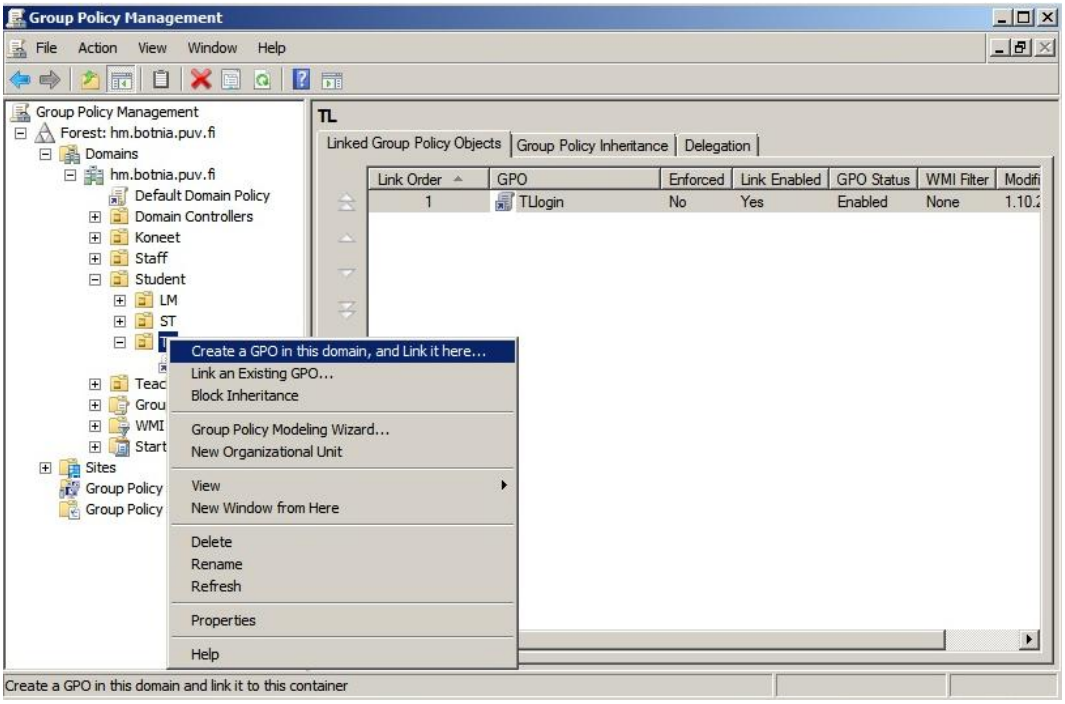


Kuva 35. Käyttöoikeuksien määrittely.

TLstudent-käyttäjäryhmälle määriteltiin luku sekä kirjoitusoikeus kyseiseen kansioon ja ainoastaan järjestelmänvalvojalla on lisäksi pääsy kansion tietoihin.

6.6.2 Logon-Script

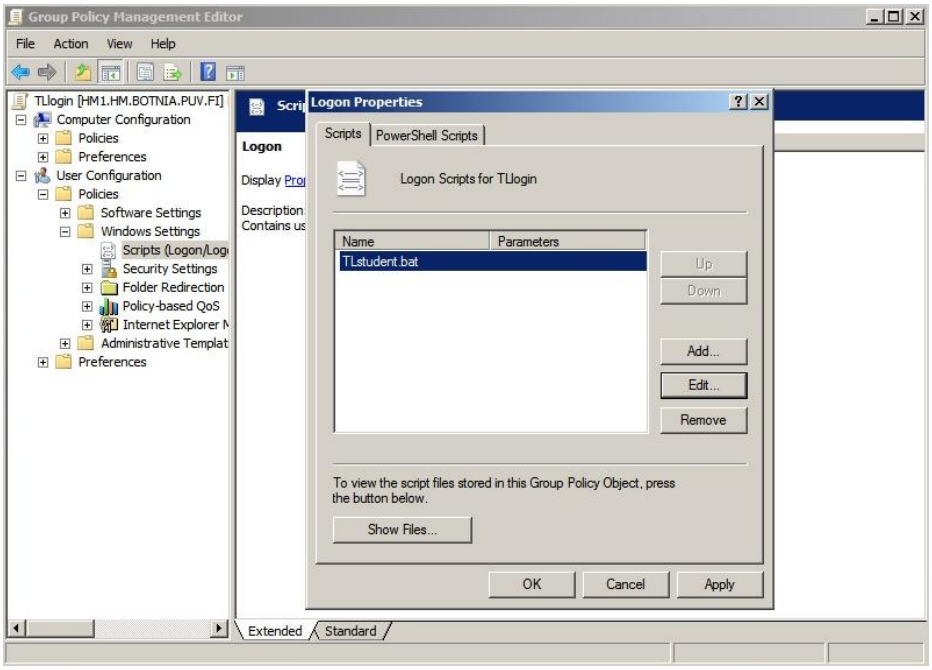
Kaikille käyttäjille määriteltiin myös Logon-Script, jonka avulla verkkojaot lisätään automaattisesti käyttäjälle kirjautuessa. Sen avulla käyttäjien ei tarvitse itse määritellä ja etsiä jakoja levypalvelimelta. Logon-Scriptit määritellään organisaatioyksiköiden Group Policyn avulla. Se lisätään Group Policy Management -konsolin avulla. Jokaiselle organisaatioyksikölle linkitetään oma GPO (Group Policy Object), johon Logon-Script määritellään käyttäjien mukaan. Kuvassa 35 on esitetty GPO:n luonti.



Kuva 35. GPO:n luonti

GPO vaikuttaa kaikkiin organisaatioyksikön alla oleviin käyttäjiin ja sen avulla pystytään luomaan erilaisia käynnistysasetuksia ja oikeuksia. Se helpottaa suurien käyttäjäryhmien hallintaa, sillä jokaiselle käyttäjälle ei tarvitse määritellä erikseen asetuksia. GPO:lla voidaan esimerkiksi määritellä tietokoneille ohjelmat, mitkä käynnistyvät, kun käyttäjä kirjautuu sisään.

Logon-Scriptin määrittely tapahtuu GPO:n User Configuration -> Policies -> Windows Settings -valikon alta. Logon-Script liitetään Logon Properties -valikkoon, jonka jälkeen se tulee käyttöön kaikille organisaatioyksikön käyttäjille. Kuvassa 36 on Logon-Script määrittely.



Kuva 36. Logon-Script määrittely.

Logon-Script liitetään .bat tiedostona ja se voidaan tehdä NET USE tai VBS komennoilla. Tässä työssä käytettiin NET USE komentoja. TLstudent-käyttäjäryhmän Logon-Script näyttää esimerkiksi seuraavalta:

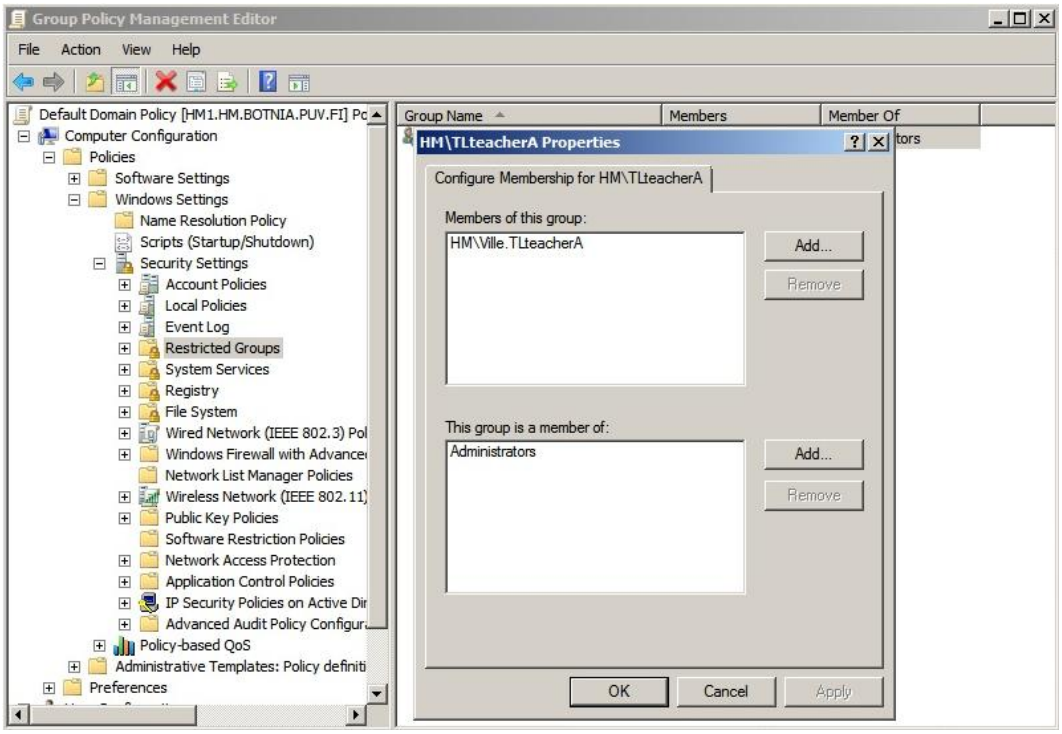
NET USE U: \\HM3\Student\TL
NET USE Z: \\HM3\Yhteinen

Logon-Script liittää automaattisesti käyttäjälle oman yksikön sekä yhteisen levyjaon. Levyjaot näkyvät käyttäjälle U- ja Z-verkkolevyinä. Kuvassa 37 näkyy verkkolevyt, jotka käyttäjä on saanut automaattisesti kirjautuessaan.

Kuva 37. Käyttäjän saamat verkkolevyt.

6.7 Local-Admin oikeudet.

AD:n avulla voidaan määritellä käyttäjille myös paikalliset järjestelmänvalvojan oikeudet(Local Admin). Näiden oikeuksien avulla käyttäjä pääsee kirjautumaan tietokoneelle järjestelmänvalvojana ja pystyy esimerkiksi asentamaan ohjelmia kyseiselle tietokoneelle. Paikallisia järjestelmänvalvojan oikeuksia ei tarvitse asentaa jokaiselle tietokoneelle erikseen, vaan ne voidaan määritellä GPO:n avulla koko toimialueelle. Tässä työssä luotiin yhdelle käyttäjälle paikallisen järjestelmänvalvojan oikeudet. Kuvassa 38 on GPO:n avulla luodut oikeudet.

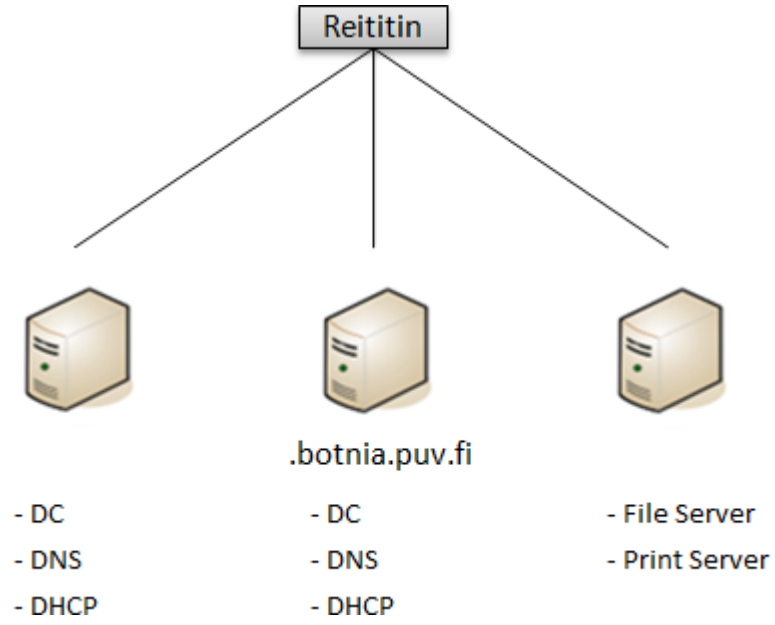


Kuva 38. Paikalliset järjestelmänvalvojan oikeudet.

Oikeudet luodaan GPO:n Restricted Groups -ryhmän avulla. Ryhmään määritellään käyttäjät, joille oikeudet tulevat käyttöön sekä ryhmä mihin heidät liitetään paikallisella tietokoneella. Kuvassa 37 on luotu Ville nimiselle käyttäjälle paikalliset järjestelmänvalvojan oikeudet. Kun Ville kirjautuu tietokoneelle, tulee hänelle automaattisesti Administrators-ryhmän oikeudet.

6.8 Työohje

Tämän työn tarkoituksena on rakentaa pieni yritysverkko, johon toteutetaan AD-, DNS-, DHCP- sekä levy- ja tulostinpalvelut. Palvelut toteutetaan kolmen serverin avulla ja niissä käytetään Windows Server 2008 -käyttöjärjestelmää. Palvelut asennetaan niin, että kaksi serveriä hoitavat DC-, DNS- ja DHCP -palveluita ja levy- ja tulostinpalvelut tulevat yhdelle serverille. Tavoitteena on saada toimiva ja vikasietokykyinen verkko, jolla pyritään simuloimaan oikean yritysverkon rakennetta. Työ toteutetaan 2-3 hengen ryhmissä. Kuvassa 39 on esitetty verkon rakenne.



Kuva 39. Verkon rakenne.

1) Työ aloitetaan käyttöjärjestelmien asennuksella. Käyttöjärjestelmäksi asennetaan Windows Server 2008 R2. Asennuksen jälkeen Servereille määritellään vielä nimet sekä staattiset IP-osoitteet samasta aliverkosta.

2) Palvelujen asennus aloitetaan määrittelemällä, mitkä serverit hoitavat DC -roolit. Tämän jälkeen palvelujen asennus aloitetaan ensimmäiselle DC:lle. Server Manager -konsolista valitaan asennettavaksi Active Directory Domain Services. Kun asennus on suoritettu, käynnistetään dcpromo.exe Wizard, jonka avulla määritellään uudelle toimialueelle nimi (xx.botnia.puv.fi). Asennuksen aikana AD

lisää palvelimelle myös automaattisesti DNS-roolin, koska sitä ei ole jo valmiiksi kyseisessä verkossa.

3) Seuraavaksi palvelimelle lisätään DHCP-rooli. Asennuksessa määritellään, mitä verkkokorttia käytetään DHCP-serverinä ja mitä IP-aluetta (Scope) se jakaa. Verkkoon asennetaan kaksi DHCP-serveriä, joten niille täytyy määritellä eri IP-alueet. Alueeksi voidaan määritellä esimerkiksi .50-.75 ja .76-.100.

4) Toiselle DC:lle voidaan DHCP-roolin asennuksen jälkeen asentaa samat palvelut, mitä toiselle serverille asennettiin. Palvelujen asennus toteutetaan saman lailla kuin aikaisemmin. Ainoana erona on DC:n liittäminen jo valmiiseen toimialueeseen (existing forest). DHCP-serverille täytyy muistaa myös määritellä eri IP-alue. Tämän jälkeen toimialueella sijaitsevien koneiden pitäisi saada IP-osoite ja käyttäjien pitäisi pystyä kirjautumaan verkkoon, vaikka toinen DC:sta ei olisi toiminnassa. Toimintaa voidaan testata esimerkiksi kytkemällä toinen DC ulos verkosta.

5) Levy- ja tulostinpalvelujen asennus toteutetaan kolmannelle serverille. Palvelut asennetaan Server Managerilla lisäämällä File- ja Print Services –roolit.

6) Verkkoon voidaan palvelujen asennuksen jälkeen luoda muutamia käyttäjiä ja organisaatioyksiköitä, joiden avulla verkon toimintaa saadaan testattua. DC:lle voidaan luoda esimerkiksi Student-niminen organisaatioyksikkö, jonka sisään voidaan luoda käyttäjä. Käyttäjiä ja ryhmiä hallitaan Active Directory User and Computers –konsolilla. Käyttäjälle voidaan tämän jälkeen tehdä levypalvelimelle jako, jonka avulla pystytään verkon toimintaa testaamaan. Jako voidaan lisätä myös käyttäjien Logon-Script asetuksiin, jolloin se ilmestyy automaattisesti käyttäjän kirjauduttua. Logon-Scriptit luodaan Group Policy Objectin avulla. Organisaatioyksikköön linkitetään GPO, jonka asetuksista määritellään käyttäjille Logon-Script. Logon-Script tehdään luomalla .bat tiedosto, jonka sisälle lisätään halutut komennot. Esimerkiksi verkkojaot voidaan lisätä NET USE Z: \\palvelin\jako komennolla.

6.9 Tulokset

Windows Server 2008 R2:n avulla pienen yritysverkon pystyttäminen onnistuu helposti, jos on hieman tietämystä Windows-käyttöjärjestelmistä ja verkon toiminnasta. Verkon hallinta ja servereiden välinen asetuksien luonti vaatii, kuitenkin paljon perehtymistä Windows Server 2008 R2 -käyttöjärjestelmään. Käyttäjien ja ryhmien luonnissa täytyy suunnitella tarkkaan, miten niiden oikeuksia pystytään hallitsemaan tehokkaasti sekä uudet käyttäjät saadaan liitettyä verkkoon.

Organisaatioyksiköissä esimerkiksi rakenteen muokkaaminen voi tuottaa ongelmia, jos ei niissä olevaa Accidental Delete -ominaisuutta tiedä. Se estää niiden poistamisen ja ominaisuus on Windows Server 2008 R2 käyttöjärjestelmässä automaattisesti päällä. Organisaatioyksikkörakennetta suunniteltaessa täytyy myös uusien käyttäjien liittäminen toimialueelle miettiä tarkasti. Käyttäjien täytyy saada oikeudet automaattisesti heille kuuluviin oikeuksiin ja verkkolevyihin.

Verkkolevyjen lisääminen käyttäjille Logon-Scriptin avulla pitää myös suunnitella oikein. Logon-Scriptit vaikuttavat kaikkiin Organisaatioyksiköiden alla oleviin käyttäjiin ja rakenne on tästä syystä suunniteltava tarkasti. Logon-Scriptejä tehtäessä täytyy muistaa myös, etteivät ne vaikuta Organisaatioyksikön alla oleviin käyttäjäryhmiin.

Pienen yritysverkon pystyttäminen onnistui mielestäni hyvin tässä opinnäytetyössä ja servereiden välille saatiin muodostettua toimivat yhteydet. Verkkoon luotiin myös pääsy etäyhteydellä ulkoverkosta botnia.puv.fi osoitteella. Verkon organisaatioyksikkörakenteet saatiin myös muodostettua oikein ja käyttäjät saivat niiden avulla automaattisesti halutut oikeudet ja Logon-Scriptit.

Opinnäytetyössä jäi toteuttamatta myös joitain ominaisuuksia ja jatkoa ajatellen niiden lisääminen olisi tärkeää verkon toiminnalle. Esimerkiksi verkkoon ei lisätty AD:n ja tiedostopalvelimen varmuuskopiointia, minkä avulla verkon toimintavarmuutta olisi saatu nostettua myös jatkossa. Varmuuskopioinnin lisääminen olisi tärkeää, jos verkko olisi käytössä oikeassa organisaatiossa ja verkkoon tulisi päivittäin uusia käyttäjiä ja tietoa.

7 YHTEENVETO

Nykyään kaikilla organisaatioilla on jo tietoliikenneverkko ja siksi niiden suunnittelu on tärkeässä roolissa. Verkon palvelujen suunnittelu täytyy tehdä jo alussa oikein, että verkko toimii jatkossakin ja suurilta ongelmilta vältyttäisiin. Windows Server 2008 tarjoaakin käyttäjille paljon erilaisia palveluita ja niiden suunnittelu sekä toteutus onkin tehty käyttöjärjestelmässä helpoksi. Sen avulla pystytään verkkoon lisäämään nopeasti uusia palveluita ja niiden hallinta on helppoa.

Opinnäytetyössä toteutettiin verkkopalvelujen suunnittelu ja mitoitus noin 3500 hengen organisaatiolle. Työssä keskityttiin erityisesti AD-, DNS-, DHCP- sekä Levy- ja Tulostinpalveluihin. Suunnittelussa ja mitoituksessa oli paljon työtä, mutta mielestäni se onnistui hyvin. Organisaation verkkoa suunniteltaessa täytyy huomioida, että yhtä oikeaa tapaa ei ole vaan palveluihin vaikuttaa suuresti organisaatio ja sen rakenne. Työtä tehdessä täytyikin tehdä paljon oletuksia, mutta pyrin käyttämään Vaasan ammattikorkeakoulun verkkoa esimerkkinä. Suunnitelmaa ja mitoitusta tehdessä törmäsikin paljon uusin asioihin, mitä ei ole ennemmin tullut mietittyä.

Opinnäytetyössä piti toteuttaa myös harjoitustyö suunnitelman perusteella, mutta vain pienemmässä mittakaavassa. Harjoitus työssä toteutettiin pieniverkko kolme serverin avulla, mihin AD-, DNS-, DHCP-, Levy- ja Tulostinpalvelut sijoitettiin. Työ oli mielenkiintoinen, koska se toteutettiin Windows Server 2008 -käyttöjärjestelmällä. Vaikka minulla ei ollut ennestään tarkempaa tietoa kyseisen käyttöjärjestelmästä ja palvelujen asentamisesta, se onnistui mielestäni hyvin. Microsoft on tehnyt Windows Server 2008 käytön helpoksi. Suurimmat ongelmat työssä oli käyttäjien ja Logon-Scriptien tekemisessä. Käyttäjien hallinta on tehty Windows Server 2008:ssa helpoksi, mutta kaikki asetukset eivät ole automaattisesti päällä, vaan ne pitää aktivoida erikseen. Joidenkin asetuksien löytäminen oli hankalaa, koska käyttöjärjestelmä oli uusi minulle.

LÄHTEET

/1/ Microsoft Corporation 2010. Active Directory Collection [online] [Viitattu 26.5.2010] Saatavilla www-muodossa: http://technet.microsoft.com/en-us/library/cc780036(WS.10).aspx

/2/ Microsoft Corporation 2010. Active Directory Services [online] [Viitattu 26.5.2010] Saatavilla www-muodossa: http://technet.microsoft.com/en-us/library/bb742424.aspx#XSLTsection135121120120

/3/ Microsoft Corporation 2010. Global Catalog [online] [Viitattu 1.6.2010] Saatavilla www-muodossa: http://technet.microsoft.com/en-us/library/cc728188(WS.10).aspx

/4/ Microsoft Corporation 2010. How Active Directory Replication Topology Works [online] [Viitattu 26.5.2010] Saatavilla www-muodossa: http://technet.microsoft.com/enus/library/cc755994(WS.10).aspx#w2k3tr_repto_how_ludi

/5/ Microsoft Corporation 2010. Infrastructure Planning and Design [online] [Viitattu 13.7.2010] Saatavilla www-dokumentti: http://technet.microsoft.com/en-us/library/cc196387.aspx

/6/ Microsoft Corporation 2010. Introduction to DFS Replication [online] [Viitattu 26.5.2010] Saatavilla www-muodossa: http://technet.microsoft.com/en-us/library/cc781091(WS.10).aspx

/7/ Microsoft Corporation 2010. Kerberos Authentication [online] [Viitattu 26.5.2010] Saatavilla www-muodossa: http://technet.microsoft.com/en-us/library/dd582583(WS.10).aspx

/8/ Microsoft Corporation 2010. Kerberos Explained [online] [Viitattu 10.6.2010] Saatavilla www-muodossa: http://technet.microsoft.com/en-us/library/bb742516.aspx

/9/ Microsoft Corporation 2010.Lightweight Directory Access Protocol [online] [Viitattu 9.6.2010] Saatavilla www-muodossa: http://msdn.microsoft.com/en-us/library/aa367008(v=VS.85).aspx

/10/ Microsoft Corporation 2010.Planning DHCP [online] [Viitattu 9.6.2010] Saatavilla www-muodossa: http://technet.microsoft.com/en-us/library/cc778368(WS.10).aspx

/11/ Microsoft Corporation 2010.Planning DNS Servers [online] [Viitattu 9.6.2010] Saatavilla www-muodossa: http://technet.microsoft.com/en-us/library/cc732715.aspx

/12/ Microsoft Corporation 2010. Protocols and Interfaces to Active Directory [online] [Viitattu 9.6.2010] Saatavilla www-muodossa: http://technet.microsoft.com/en-us/library/cc961766.aspx

/13/ Microsoft Corporation 2010. Trust [online] [Viitattu 26.5.2010] Saatavilla www-muodossa: http://technet.microsoft.com/en-us/library/cc786873(WS.10).aspx

/14/ Microsoft Corporation 2010. Windows Server 2008 [online] [Viitattu 26.5.2010] Saatavilla www-muodossa: http://www.microsoft.com/windowsserver2008/en/us/whats-new.aspx

/15/ Windows Networking 2010. Distributed-File-System[online] [Viitattu 4.8.2010] Saatavilla www-muodossa: http://www.windowsnetworking.com/articles_tutorials/Windows2003-Distributed-File-System.html

/16/ Perti IT Knowledge Base 2010. Planning a DFS Architecture[online] [Viitattu 4.8.2010] Saatavilla www-muodossa: http://www.petri.co.il/planning-dfs-architecture-part-one.htm