



Kang Xu

Windows Server 2008:n verkkorakenne ja käyttöympäristö

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikan koulutusohjelma
Insinöörityö
20.4.2011

Tekijä Otsikko	Kang Xu Windows Server 2008:n verkkorakenne ja käyttöympäristö
Sivumäärä Aika	56 20.4.2011
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietokoneverkot
Ohjaaja	yliopettaja Matti Puska
<p>Tämän insinööriyön aiheena oli Windows Server 2008:n verkkorakenne ja käyttöympäristö.</p> <p>Insinööriyön tavoite oli saada käsitys Windows Server 2008 sisäverkon toimivuudesta, sen liikenteenhallinnasta, tietoturvasta ja palveluista teoriassa ja käytännössä.</p> <p>Insinööriyössä tutustuttiin ensi Windows Server 2008 -käyttöjärjestelmän ominaisuuksiin yleisesti, jonka jälkeen perehdyttiin sen tarjoamiin eri palveluihin. Teoriaosuudessa selvitettiin ensiksi DHCP:n, IIS:n, DNS:n ja AD DS:n toimintakuvat Windows Server 2008:n verkkoympäristössä. Teoriaosuuden loppupuolella käsiteltiin Windows Server 2008 verkon tietoturvaratkaisut OSI-mallin palvelintason - ja kuljetustason näkökulmista.</p> <p>Käytäntöosiossa rakennettiin verkko Virtual PC -ohjelmalla, joka sisälsi kolme Windows Server 2008 -käyttöjärjestelmällä varustettua virtuaalitietokonetta ja yhden Windows XP -käyttöjärjestelmällä varustetun virtuaalitietokoneen. Kaksi näistä Windows Server 2008 -tietokoneista toimii verkon palvelujen pääpalvelimena ja DNS-varapalvelimena. Kolmas Windows Server 2008 -tietokone toimii palvelujen testauskoneena. Yhteyden toimivuutta testattiin ja tarkistettiin kaikilla palveluilla, joita otettiin käyttöön verkossa. Palvelut ovat DHCP-, DNS-, AD DS-, ja IIS-palvelut.</p> <p>Windows Server 2008 -verkon teoriaosuus oli hyvin laaja, tämän takia kaikkien palvelujen teorat eivät ole kovin syvällisiä, mutta tarpeeksi laajasti selitetty, jotta saadaan käytännön osuudesta kokonaiskäsityksen. Käytännön osuudessa verkko toimii kaikkien palvelujen ja sovelluksien asennuksien jälkeen toivotulla tavalla.</p>	
Avainsanat	Windows Server 2008, DHCP, DNS, AD DS, IIS, IPsec

Author	Kang Xu
Title	Windows Server 2008 Network Infrastructure
Number of Pages	56
Date	20 April 2011
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Instructor Supervisor	Matti Puska, Principal Lecturer Matti Puska, Principal Lecturer
<p>The subject of this thesis is Windows Server 2008 Network Infrastructure. The object of this work is to gain an understanding of Windows Server 2008 internal network's functionality, traffic management, security and services that it offers, both in theory and practice.</p> <p>The first thing to do in this thesis was to explore the features of the Windows Server 2008 operation system. After that the different network services of Windows Server 2008 were learned. In theory we first studied the operations of DHCP, IIS, DNS and AD DS services inside Windows Server 2008 networks. In the end of the theory part, different security methods of OSI's network layer and transport layer were defined.</p> <p>An internal network was built in the practice section, which consisted of three computers with Windows Server 2008 operation system, and one computer with Windows XP operation system. The first two Windows Server 2008 computers operated as main and backup DNS servers. The third Windows Server 2008 and the Windows XP computers acted as a test machines for different functionalities. The functionality of all services including DHCP, DNS, AD DS and IIS were tested and inspected.</p> <p>Because of the extent of the theory part, it wasn't possible to cover the whole details of each of the services included in this thesis, but enough to get a clear picture of the objective of the practice part. After all the installations of different features and services, the Windows Server 2008 network works as desired and planned as in the beginning of the thesis.</p>	
Keywords	Windows Server 2008, DHCP, DNS, AD DS, IIS, IPsec

Sisällys

Tiivistelmä

Abstract

Lyhenteet

1	Johdanto	6
2	Windows Server 2008 yleisesti.....	7
2.1	Käyttöjärjestelmät.....	7
2.2	Virtualisointi	8
2.3	Tietoturva	9
2.4	Palvelinydin (Server Core).....	9
2.5	Windows Deployment Services (WDS)	10
3	Windows Server 2008:n verkkorakenne.....	11
3.1	Internet Protocol (IP)	11
3.1.1	Internet Protocol version 4 (IPv4).....	11
3.1.2	Internet Protocol version 6 (IPv6).....	12
3.2	Aktiivihakemisto (Active Directory)	13
3.2.1	Aktiivihakemiston roolit.....	13
3.2.2	Active Directory Domain Services (AD DS)	14
3.3	DNS (Domain Name Server).....	17
3.3.1	DNS:n hierarkia.....	17
3.3.2	DNS:n vyöhykkeet.....	18
3.3.3	DNS:n vyöhykesiirrot	18
3.3.4	DNS:n tiedot.....	19
3.3.5	DNS:n dynaamiset päivitykset	20
3.3.6	Palvelinnimien selvittäminen DNS-verkossa.....	21
3.4	Windows Server 2008:n DHCP (Dynamic Host Configuration Protocol).....	22

3.4.1	DHCP-osoitteiden jako	22
3.4.2	DHCP-osoitteiden kierrätettävyys	24
3.5	Internet Information Services 7.0 (IIS 7.0).....	25
3.5.1	IIS yleisesti.....	25
3.5.2	IIS 7.0:n parannuksia	25
3.5.3	IIS 7.0:n käyttäjäliittymän hallintaohjelma.....	26
3.5.4	Virtuaalihakemisto	27
4	Windows Server 2008:n tietoturva	28
4.1	Palvelintason tietoturva	28
4.2	Kuljetustason tietoturva.....	33
4.3	Windows Server 2008:n IPsec.....	34
5	Windows Server 2008:n verkko käytännössä.....	36
5.1	Windows Server 2008:n asentaminen	36
5.2	Windows Server 2008 -verkon rakentaminen.....	37
5.2.1	AD DS:n luonti	37
5.2.2	DNS-nimipalvelin asennus ja määrittely	38
5.2.3	DHCP-palvelin asennus ja määrittely	41
5.2.4	IIS-palvelun ja FTP:n asennus ja määrittely	44
5.2.5	Tiedostojen jako-oikeuksien määrittely	46
5.2.6	Kirjautumiskomentosarjan määrittely käyttäjäkoneelle	48
5.2.7	IPsec-protokollan määrittely	49
6	Yhteenveto	53
7	Lähteet.....	55

Lyhenteet

6to4	Muutosmekanismi, jolla muutetaan IPv6-osoitteet ymmärrettäviksi IPv4-verkon reitittimille.
3DES	<i>3 Data Encryption Standard</i> . Salausmenetelmä.
ACE	<i>Access Control Entry</i> . ACL (Access Control List):n elementti.
AD	<i>Active Directory</i> . Windows Server -käyttöjärjestelmien käyttämä aktiivihakemisto
AD CS	<i>Active Directory Certificate Services</i> . Aktiivihakemiston sertifikaattipalvelurooli.
AD DS	<i>Active Directory Domain Services</i> . Microsoftin kehittämä aktiivihakemistopalvelurooli.
AD FS	<i>Active Directory Federation Services</i> . Aktiivihakemiston todennuspalvelurooli.
AD LDS	<i>Active Directory Lightweight Directory Services</i> . Microsoftin kehittämä tietokanta- ja ohjelmistopalvelurooli.
AD RMS	<i>Active Directory Rights Management Services</i> . Aktiivihakemiston oikeuksien hallitapalvelurooli.
AES-128	<i>Advanced Encryption Standard 128-bit</i> . Lohkosalausmenetelmä.
APIPA	<i>Automatic Private IP Addressing</i> . Mekanismi, jolla määritetään tietokoneille IP-osoitteet, kun verkossa ei ole DHCP-palvelinta.
ASP.NET	<i>Active Server Pages .NET Frameworks</i> . Ohjelmistokomponenttikirjasto.
BITS	<i>Background Intelligent Transfer Service</i> . Microsoft Windows -käyttöjärjestelmien käyttämä tiedonsiirtomenetelmä.
CA	<i>Certificate Authority</i> . Itsenäinen kokonaisuus, jonka tehtävänä on digitaalisten varmenneiden jakaminen.
COM	<i>Component Object Model</i> . Microsoftin kehittämä binääriiliitäntä.
CNAME	<i>Canonical Name</i> . DNS:n resurssitieto.
DC	<i>Domain Controller</i> . Aktiivihakemiston ohjauskone.
DFS	<i>Distributed File System</i> . Microsoftin kehittämä tiedostojakelupalvelu käyttäen Windows-palvelinkäyttöjärjestelmiä.
DHCP	<i>Dynamic Host Configuration Protocol</i> . Verkkoprotokolla, jonka tärkein tehtävä on jakaa IP-osoiteasetuksia lähiverkossa oleville tietokoneille.

DNS	<i>Domain Name System.</i> Nimipalvelujärjestelmä, jonka tärkein tehtävä on muuttaa verkkotunnuksia IP-osoitteeksi.
EFS	<i>Encrypting File System.</i> Windows-käyttöjärjestelmien tiedostojen salausmenetelmä.
ESP	<i>Encapsulating Security Payloads.</i> IPsec-protokolla, joka tarjoaa tietosuojaa IPsec-paketeille.
FTP	<i>File Transfer Protocol.</i> Tiedonsiirtoprotokolla.
FTPS	<i>File Transfer Protocol Secure.</i> Suojattu FTP-protokolla.
GPO	<i>Group Policy.</i> Aktiivihakemiston ryhmäkäytäntöpalvelu.
GPM	<i>Group Policy Management.</i> GPO:n hallintakonsoli.
HTTP	<i>Hypertext Transfer Protocol.</i> Tiedonsiirtoprotokolla.
HTTPS	<i>Hypertext Transfer Protocol Secure.</i> Salattu HTTP-protokolla.
IF	<i>Identity Federation.</i> AD RMS:n sisältämä palvelurooli, joka sallii tiedostojen jakelua organisaatioiden välillä julkisen verkon kautta.
IIS	<i>Internet Information Protocol.</i> Microsoftin kehittämä web-palvelinohjelmisto.
IPsec	<i>IP Security Architecture.</i> Monen eri protokollan muodostama menetelmä IP-pakettien turvaamiseksi tiedonsiirrossa.
ISATAP	<i>Intra-Site Automatic Tunnel Addressing Protocol.</i> Muutosmekanismi, jolla välitetään IPv6-paketteja IPv4-verkossa.
LAN	<i>Local Area Network.</i> Lähiverkko.
MX	<i>Mail Exchanger.</i> DNS:n resurssitieto, jolla tunnistetaan verkon sähköpostipalvelimet.
NAP	<i>Network Access Protection.</i> Microsoftin kehittämä tietoturvaratkaisu.
NAT	<i>Network Address Translation.</i> Osoitteenmuunnostekniikka, jolla muutetaan yksityiset IP-osoitteet julkisiksi IP-osoitteeksi, ja toisinpäin.
NIC	<i>Network Interface Card.</i> Tietokoneen laitteisto, jolla yhdistetään tietokonetta IP-verkkoon.
NNTP	<i>Network News Transfer Protocol.</i> Julkisten keskusteluryhmien käyttämä tiedonsiirtoprotokolla.
NS	<i>Name Server.</i> DNS:n resurssitieto, jolla tunnistetaan DNS-palvelimet.
NTFS	<i>New Technology File System.</i> Microsoftin kehittämä tiedostojärjestelmä.

OU	<i>Organizational Units.</i> Aktiivihakemiston hakemistopalvelu, jolla voidaan ryhmittää objektit eriin ryhmiin.
PKI	<i>Public Key Infrastructure.</i> Julkisen avaimen infrastruktuuri, jolla voidaan yhdistää julkisen avaimen ja henkilön tai järjestelmän varmenneviranomaisen avulla.
PTR	<i>Pointer.</i> DNS:n resurssitieto, jolla etsitään palvelinnimiä IP-osoitteen perusteella
SMTP	<i>Simple Mail Transfer Protocol.</i> Sähköpostipalvelimien käyttämä tiedonsiirtoprotokolla.
SHA1	<i>Secure Hash Algorithm 1.</i> Tiivistefunktio.
SOA	<i>Start of Authority.</i> DNS resurssitieto, jolla määritetään verkon arvovaltaisin DNS-palvelin.
SRV	<i>Service Record.</i> DNS:n resurssitieto, jolla tunnistetaan aktiivihakemiston ohjauksoneita.
SSL	<i>Secure Sockets Layer.</i> Salausprotokolla, jolla suojataan tietoliikenteet julkisissa verkoissa.
TCP	<i>Transmission Control Protocol.</i> Kuljetuskerroksen tietoliikenneprotokolla.
Teredo	Microsoftin kehittämä tunneliprotokolla, jolla pystytään reitittämään IPv6-paketteja IPv4-verkkoon.
UDP	<i>User Datagram Protocol.</i> Kuljetuskerroksen tietoliikenneprotokolla.
URL	<i>Uniform Resource Locator.</i> WWW-sivujen tunniste.
UTF8	<i>UCS Transformation Format — 8-bit.</i> Kirjoitusmerkkien koodaustapa.
WDS	<i>Windows Deployment Services.</i> Microsoftin kehittämä verkkoasennuspalvelu, joka on tarkoitettu Windows-pohjaisille käyttöjärjestelmille.
WSUS	<i>Windows Server Update Services.</i> Microsoftin kehittämä ohjelmistopäivityspalvelu Windows-käyttöjärjestelmille.

1 Johdanto

Insinööriaiheena on Windows Server 2008:n verkkorakenne ja käyttöympäristö monien sen tarjoamien palveluiden ja sovelluksien hyväksi käyttäen. Tämän insinööriyön aiheen valintaan johtaneita syitä ovat kiinnostus Microsoftin uusinta Windows Server -palvelinkäyttöjärjestelmää kohtaan ja halu rakentaa kyseisellä käyttöjärjestelmällä sisäverkko, joka olisi käyttökelpoinen pieni- tai keskikokoiselle yritykselle.

Työn tavoitteena on rakentaa esimerkkiyritykselle toimiva sisäverkko, jossa kaikki verkon sisällä käytössä olevat tarpeelliset palvelut ja sovellukset sisältyvät Windows Server 2008 -käyttö- järjestelmään. Työ koostuu teoriaosuudesta sekä käytäntöosiosta testeineen ja tuloksineen.

Teoriaosuudessa selvitetään Windows Server 2008 -käyttöjärjestelmän DHCP (Dynamic Host Configuration Protocol)-, DNS (Domain Name Server)-, AD DS (Active Directory Domain Services)- ja IIS (Internet Information Services) -palveluiden käyttöä, niiden vaatimuksia ja tarjoamia mahdollisuuksia. Tämän lisäksi selvitetään TCP/IP:tä (Transmission Control Protocol/Internet Protocol) käsitteenä ja tarkastellaan IP (Internet Protocol) -osoitteiden toimintaa IP-verkkoissa.

Käytäntöosiossa tarkastellaan teoriaosuudessa mainitsemien palveluiden ja sovelluksien toimintaa Virtual PC -verkkoympäristössä kahdessa eri vaiheessa. Ensimmäisessä vaiheessa asennetaan kaikkiin tietokoneisiin Windows Server 2008 -käyttöjärjestelmät, yhdistetään tietokoneet samaan aliverkkoon ja testataan verkon yhteystoimivuutta. Toisessa vaiheessa asennetaan palvelut yksitellen ja tarkastellaan näiden yhteystoimivuudet.

Verkkoliikennettä tarkastellaan käyttäen Windows Server 2008 -käyttöjärjestelmän sisäänrakennettujen sovelluksia hyväksi. Käytäntöosiota pyritään rakentamaan ja esittämään mahdollisimman tarkasti ja yksityiskohtaisesti.

2 Windows Server 2008 yleisesti

2.1 Käyttöjärjestelmät

Windows Server 2008 -käyttöjärjestelmä julkaistiin 4. helmikuuta 2008. Sen tuorein versio on Windows Server 2008 R2 6.1 (Build 7600), joka julkaistiin 22. heinäkuuta 2009.

Windows Server 2008 -käyttöjärjestelmää on rakennettu samalla koodipohjalla kuin Windows Vista ja Windows 7, siksi näillä käyttöjärjestelmillä on paljon yhteistä arkkitehtuurissa ja toimivuudessa.

Microsoft Windows Server 2008 -käyttöjärjestelmästä on julkaistu viisi eri versiota, Web-, Itanium-, Standard-, Enterprise- ja Datacenter-versiot. Neljästä versiosta on olemassa sekä 32-bittinen että 64-bittinen-käyttöjärjestelmä. Itanium-versio tulee ainoastaan 64-bittisenä. [3.]

Microsoftin laatimat minimi- ja suosituslaitteistovaatimukset Windows Server 2008 -käyttöjärjestelmälle ovat seuraavanlaiset:

Proessori	Minimi: 1 GHz Suositus: 2 GHz Optimaalinen: 3 GHz tai nopeampi (Windows Server 2008 Itanium-pohjaiset järjestelmät vaativat Intel Itanium 2 -prosessoria toimiakseen)
Muisti	Minimi: 512 MB RAM Suositus: 1 GB RAM Optimaalinen: 2 GB RAM (täysiasennus) tai 1 GB RAM (Server Core -asennus) tai enemmän Maksimaalinen (32-bittinen): 4 GB (Standard-versio) tai 64 GB (Enterprise- ja Datacenter-versiot) Maksimaalinen (64-bittinen): 32 GB (Standard-versio) tai 2 TB (Enterprise -, Datacenter -, ja Itanium-pohjaiset järjestelmät)

Levytila	Minimi: 8 GB Suositus: 40 GB (täysiasennus) tai 10 GB (Server Core -asennus) Optimaalinen: 80 GB (Täysiasennus) tai 40 GB (Server Core -asennus) tai enemmän
Levykeasema	DVD-ROM-asema
Muut laitteet	SVGA (800 x 600) tai korkeampi näyttöresoluutio Näppäimistö Microsoftin hiiri tai vastaava yhteensopiva osoitinlaite. [16.]

2.2 Virtualisointi

Windows Server 2008:n virtualisointiominaisuus Hyper-V-teknologiaa hyväksi käyttäen on yksi Windows Server 2008 -käyttöjärjestelmän uusista lisäyksistä, jota ei ole aikaisemmissa Windows Server -käyttöjärjestelmissä. Hyper-V-teknologialla pystytään sallimaan monia eri käyttöjärjestelmiä ajamaan samanaikaisesti yhdessä fyysisessä järjestelmässä. Esimerkiksi monia ohjauskonejärjestelmiä ja -alustoja voidaan yhdistää yhdeksi palvelimeksi palvelun vahvistamiseksi tai luoda useita palvelinympäristöjä yhdelle fyysiselle palvelimelle testaus- tai kehitysympäristössä. Käytännössä tämä tarkoittaa sitä, että DHCP-, tiedosto- ja IIS-palvelimen sijaan on vain yksi palvelin, jolla ajetaan kaikki edellä mainittujen palvelimien ohjelmat ja sovellukset ja joka suorittaa vaaditut tehtävät verkossa.

Hyper-V-ominaisuus sisältyy Windows Server 2008 Standard-, Enterprise- ja Datacenter-versioissa. Hyper-V toimii ainoastaan 64-bittisellä alustalla. [1, s. 2—3.]

2.3 Tietoturva

Windows Server 2008 -käyttöjärjestelmässä on joukko uusia tietoturvaratkaisuja:

BitLocker Drive Encryption -ominaisuudella pystytään salaamaan kokonaisia tiedostovolyymejä. Se suojaa sekä tavallisia että käyttöjärjestelmän tiedostoja, ja näin estää luvattomilta pääsyn esimerkiksi ohjauskoneen aktiivihakemiston tietokantaan.

Kun käyttäjät liittyvät etäyhteydellä sisäverkkoon, on mahdollista, että käyttäjien tietokoneet ovat saastuneet viruksilla tai heiltä puuttuu asianmukaiset ja uusimmat päivitykset, mikä voi vaarantaa sisäverkon tietoturvallisuuden. *Network Access Protection (NAP)* tarkistaa jokaisen etäyhteyttä käyttävän käyttäjän, ennen kuin heidät päästetään sisäverkkoon. Saastutetut käyttäjätilit voidaan pitää eristyksessä siihen asti, kunnes ongelma on korjattu.

Improved Security Log -ominaisuudella pystytään tarkemmin seuraamaan ja tallentamaan sisäverkon tapahtumia ja laatimaan tarkemmat virheilmoitukset. [17.]

2.4 Palvelinydin (Server Core)

Windows Server 2008 tarjoaa kaksi erilaista asennustapaa, täysiasennus ja Server Core -asennus. Server Core on Windows Server 2008 -käyttöjärjestelmän uusi ominaisuus, jota ei ole aikaisemmissa Windows Server -käyttöjärjestelmissä.

Server Core -ominaisuudella pystytään säästämään tietokoneen resursseja asentamalla ainoastaan ne tarpeelliset palvelu- ja sovelluskomponentit, joita palvelin välttämättä tarvitsee suorittaakseen tiettyä palvelinroolia verkossa. Server Core tarjoaa monia hyöty verrattuna täysasennukseen.

Server Core -asennus asentaa vähemmän sovelluksia palvelimeen, eli ottaa käyttöönsä vähemmän levytilaa. 1 GB riittää käyttöjärjestelmäasennukseen. Palvelimeen asennetaan myös vähemmän sovelluksia ja tästä johtuen on myös vähemmän päivityksiä. Ja koska oletusportteja on auki vähemmän kuin normaaliasennuksessa, minimoidaan myös eri hyökkäyksien mahdollisuuksia. Server Core -asennuksella

asennetut käyttöjärjestelmät ovat helpompia hallinnoida edellä mainituista syistä johtuen.

Server Core -ominaisuus tukee seuraavia palvelinrooleja:

- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Services (AD LDS)
- DHCP-palvelin
- DNS-nimipalvelin
- Tietokantapalvelut
- Tulostuspalvelut
- Internet-palvelut
- Hyper-V.

Suurin ero näissä kahdessa asennustavassa on se, että Server Core -asennuksessa ei ole graafista käyttöliittymää, vaan kaikki on tehtävä tekstipohjaiselta komentoriviltä. [2.]

2.5 Windows Deployment Services (WDS)

WDS-ominaisuus mahdollistaa käyttöjärjestelmien automatisoidun asennuksen samanaikaisesti eri tietokoneisiin ja palvelimiin Windows Server 2008:n sisäverkossa verkkopohjaisen asennuksen kautta. Sitä voi käyttää esimerkiksi, jos halutaan asentaa samaa käyttöjärjestelmää samoilla päivityksillä ja sovelluksilla samaan aikaan kahteenkymmeneen eri tietokoneeseen. WDS sisältyy kaikkiin Windows Server 2008 -versioihin, sekä 32-bittisille että 64-bittisille alustoille. [1, s. 13–14.]

3 Windows Server 2008:n verkkorakenne

3.1 Internet Protocol (IP)

3.1.1 Internet Protocol version 4 (IPv4)

Tietokoneet kommunikoivat toistensa kanssa tietokoneverkoissa IP- ja TCP/IP-protokollaa hyväksi käyttäen. IPv4 on tällä hetkellä ylivoimaisesti maailman käytetyin verkkoprotokolla.

Monia IP-osoitteita on varattu yksityiseen käyttöön. Osoitteet eivät ole julkisesti käytössä, koska niitä ei näy Internetin reitittimien reititystaulukoissa. Yksityiset IP-osoitteita voidaan käyttää ainoastaan sisäverkoissa.

Tietokone ottaa käyttöön APIPA (Automatic Private IP Addressing) -osoitteen, jos sille ei ole manuaalisesti määritettyä tai DHCP-palvelimelta saatua IP-osoitetta. APIPA-osoitteet ovat välillä 169.254.1.0–169.254.254.255. APIPA sallii tietokoneiden kommunikointia paikallisverkossa, jossa ei ole DHCP-palvelinta. Jos tietokoneella on APIPA-osoite käytössä verkossa, josta kuitenkin löytyy DHCP-palvelin, tarkoittaa tämä sitä, että joko tietokoneen verkkoasetukset eivät ole oikein konfiguroituja tai DHCP-palvelin on poiskytketty. Tietokoneet, joilla on APIPA-osoitteet käytössä, yrittävät säännöllisesti ottaa yhteyttä DHCP-palvelimeen saadakseen virallisen IP-osoitteen. APIPA-ominaisuus on käytössä Windows 98- tai uudemmissa Windows-käyttöjärjestelmissä.

Suurin osaa verkon sovelluksista käyttää kahta kuljetuskerroksen protokollaa:

User Datagram Protocol (UDP) -protokollaa käytetään esimerkiksi video- tai ääni-tiedostojen lähettämisessä. Sovellukset, jotka käyttävät UDP:tä, eivät vaadi varmennusta pakettien perillemenosta.

Transmission Control Protocol (TCP) -protokolla on luotettavampi mutta hitaampi kuin UDP-protokolla, koska se vaatii vahvistusta yhteyden toimivuudesta ennen kuin paketteja voidaan lähettää. Sovellukset, jotka vaativat kadonneiden ja turmeltuneiden

pakettien uudelleenlähettämistä, käyttävät TCP-protokollaa, kuten sähköposti- ja web-selailu -sovellukset.

On hyvin tärkeää päättää jo verkon suunnitteluvaiheessa, mikä IP-osoite annetaan millekin palvelimelle tai reitittimelle, koska IP-osoitteiden vaihtaminen jo olemassa olevassa verkossa on hyvin aikaa vievä prosessi, joka saattaa luoda myös ylimääräisiä reititysongelmia (taulukko 1).

Taulukko 1. Esimerkki IP-osoitteiden jaosta verkossa.

Rooli	Varatut osoite
Oletusyhdyskäytävä	192.168.1.1
Toissijainen yhdyskäytävä	192.168.1.2
DHCP-palvelin	192.168.1.3
Ensisijainen DNS-palvelin	192.168.1.4
Toissijainen DNS-palvelin	192.168.1.5
Väliaikaiset staattiset IP-osoitteet	192.168.1.10-.29
Staattiset IP-osoitteet	192.168.1.30-.99
DHCP-palvelimelle varatut IP-osoitteet	192.168.1.100-.250

Luomalla tarkka suunnitelma IP-osoitteiden jaosta voidaan helpottaa vian etsintää verkon olemassaolon aikana.

3.1.2 Internet Protocol version 6 (IPv6)

IPv4:n käyttö standardisoitiin vuonna 1981, vuosia ennen kuin nykyistä Internet-verkkoa muodostettiin. IPv4:n IP-osoitteiden määrä on vain rajallinen. Tämä on yksi pääsyistä, minkä takia kehitettiin IPv6, jotta Internet-verkkoja voidaan laajentaa tulevaisuudessa.

IPv6 sisältyi jo Windows XP Service Pack 1- ja Windows Server 2003 -käyttöjärjestelmiin, mutta se on kytketty pois käytöstä oletusasetuksessa. Windows Vista-, Windows 7- ja Windows Server 2008 -käyttöjärjestelmissä IPv6 on käytössä oletusasetuksessa. IPv6:n tukea ei ole tarjolla Windows 2000:lle, Windows 98:lle tai vanhemmille käyttöjärjestelmille.

IPv6:n tärkein parannus verrattuna IPv4:ään on sen suuri osoiteavaruus. IPv4:n osoiteavaruutta ei pystytä laajentamaan. Jotta nykyistä Internet-verkkoa voidaan vielä laajentaa suuremmaksi, IPv6:n käyttöönotto on väistämätöntä. Toinen tärkeä ominaisuus on, että IPv6 sallii 4 GB:n kokoisten pakettien lähettämisen verkon kautta.

IPv6:ta voidaan käyttää IPv4-verkoissa käyttämällä IPv6 Transition -tekniikkaa. Windows Server 2008:n kanssa yhteensopivat tekniikat ovat 6to4, ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) ja Teredo.

Vie aikaansa ennen kuin voidaan kokonaan siirtyä IPv6-protokollan käyttöön, koska nykymaailman Internet-verkon infrastruktuuri, sen sisältämät palvelimet ja tietokoneet on sijoitettu hyvin laajasti maailman eri organisaatioille. [4; 5; 6.]

3.2 Aktiivihakemisto (Active Directory)

3.2.1 Aktiivihakemiston roolit

Aktiivihakemisto on Microsoft Windows Server -käyttöjärjestelmien tärkein osa. Windows Server 2008 -käyttöjärjestelmässä aktiivihakemistoa laajennettiin kattamaan lisää aktiivihakemistorooleja, joita ei ollut aikaisemmissa Windows Server -käyttöjärjestelmissä. Windows Server 2008 -käyttöjärjestelmä tukee seuraavia aktiivihakemistorooleja:

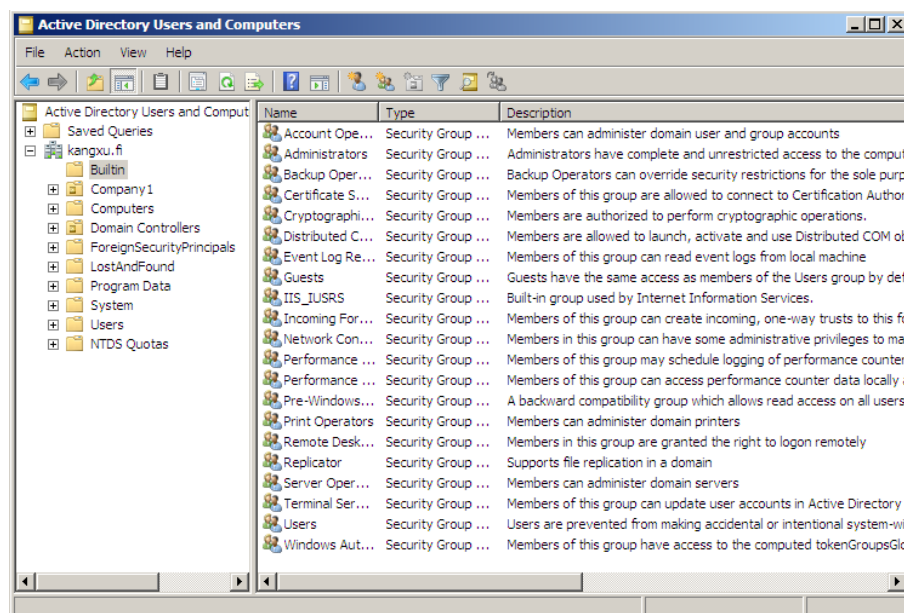
- Active Directory Domain Services (AD DS)
- Active Directory Certificate Services (AD CS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Rights Management Services (AD RMS)
- Active Directory Federation Services (AD FS). [7, s. 11.]

3.2.2 Active Directory Domain Services (AD DS)

Aktiivihakemiston tärkein rooli on toimia Active Directory Domain Services (AD DS) -palvelimena. Tämän tehtävän omaavaa palvelinta kutsutaan yleisesti Domain Controlleriksi (DC) eli ohjauskoneeksi. Se sisältää kaikki tarvittavat tiedot kaikista objekteista sen hallitsemilla toimialueilla. AD DS:llä voidaan hallinnoida verkkoa hyvin keskitetysti.

AD DS:n sisältämät objektit ovat esimerkiksi käyttäjät, tietokoneet ja ryhmät. Kun käyttäjä tarvitsee pääsyä verkkoon, täytyy verkon ylläpitäjän luoda ensiksi käyttäjätili kyseiselle käyttäjälle. Tämä tili luokitellaan objektiksi aktiivihakemiston sisällä. Kun luodaan käyttäjätili aktiivihakemistossa, tili on se objekti, joka toimii liitântänä käyttäjään, jolle tiliä luotiin. Käyttäjiä ei luoda. Tietokonetilit luodaan samalla tavalla, ja logiikkaa on myös sama. Ryhmätilit yhdistetään ryhmiin, joissa käyttäjä- tai tietokonetilit on ryhmitetty yhteen. [1, s. 209–211.]

Ensisijainen työkalu aktiivihakemiston käyttämiseen on Active Directory Users and Computers -ikkuna (kuva 1).

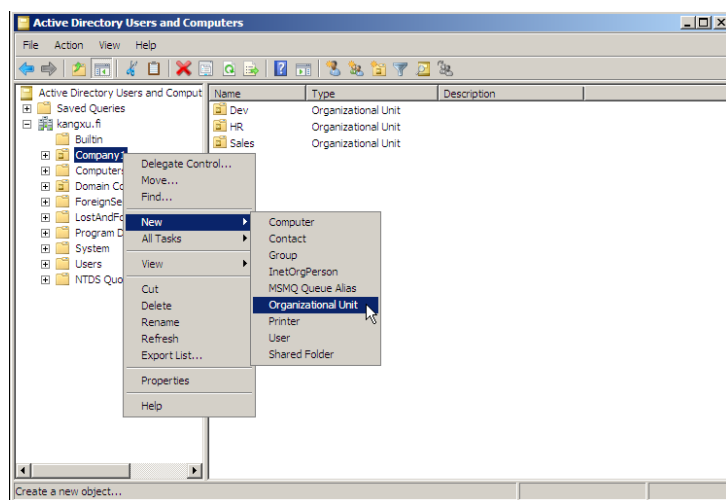


Kuva 1. Active Directory Users and Computers -ikkuna.

Toimialue koostuu yleisesti organisaatioyksiköistä (Organizational Units, OU), joilla on kaksi tärkeää tehtävää (kuva 2), hallintaoikeuksien jako tietylle yksilölle tai ryhmälle ja hallinnointi ryhmäkäytännöllä.

Hallintaoikeuksien jakoa tietylle yksilölle tai ryhmälle voidaan käyttää jos yhdellä toimialueella on esimerkiksi tuhat käyttäjää. Käyttäjät täytyy näin jakaa omiin organisaatioyksikköihin, joilla on oma ylläpitohenkilökunta. Voidaan luoda myyntiorganisaatioyksikkö yrityksen myyntiosastolle. Tämän jälkeen lisätään kaikki myyntiosaston käyttäjä- ja tietokonetilit juuri luotuun organisaatioyksikköön. Lisäksi voidaan luoda ylläpitoryhmä, jolle delegoidaan kaikki hallinnolliset oikeudet hallita myyntiorganisaatioyksikköä.

Ryhmäkäytännöllä puolestaan voidaan antaa samassa ryhmässä oleville käyttäjä- ja tietokonetilille samat asetukset. Esimerkiksi koko myyntiosaston henkilökunta tarvitsee tiettyä sovellusta koneisiinsa. Voidaan lähettää kyseinen sovellus kaikille ryhmän käyttäjille ryhmäkäytäntöä hyväksi käyttäen. Ensimmäisenä asiana luodaan uusi organisaatioyksikkö myyntiosastolle. Tämän jälkeen liitetään kaikki käyttäjät kyseiseen organisaatioyksikköön. Lopuksi luodaan ja linkitetään ryhmäkäytäntö.



Kuva 2. Organisaatioyksikön luonti.

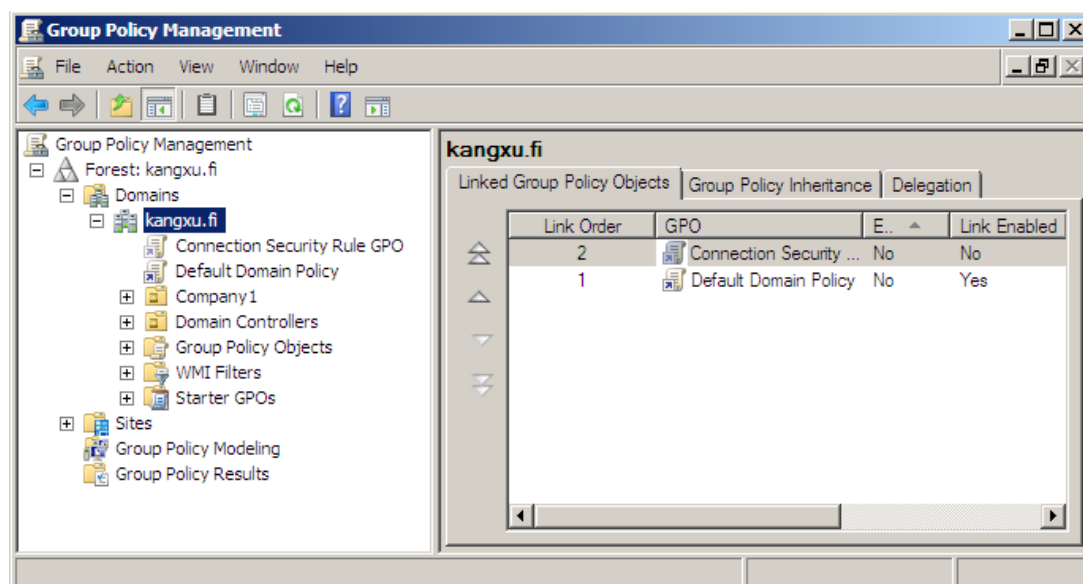
Aktiivihakemiston ryhmäkäytäntöominaisuudella voidaan hallita, muuttaa ja asettaa käyttäjä-, tietokone- ja ryhmätilit hyvin keskitetysti. Käytäntöasetuksessa voidaan määrittää tiettyjä asetuksia, joita halutaan asettaa käyttöön. On olemassa kaksi

erilaista tapaa määrittää käytäntöasetuksia: käytäntö joka vaikuttaa käyttäjiin, ja käytäntö, joka vaikuttaa tietokoneisiin.

Edellisen tapaisella käytännöllä voidaan esimerkiksi estää tiettyjä käyttäjiä pääsemästä rekisterinmuokkaus-työkaluihin riippumatta siitä, millä tietokoneella he ovat kirjautuneena.

Jälkimmäinen käytäntö toimii samalla tavalla kuin edellinen, mutta pätee ainoastaan verkossa oleviin tietokoneisiin. Esimerkiksi voidaan asettaa tietokoneen paikallisylläpitäjätili pois päältä riippumatta siitä, kuka käyttäjä on sillä hetkellä kirjautuneena kyseiseen tietokoneeseen.

Ryhmäkäytäntöobjektit sisältävät monia käytäntöasetuksia, joilla voidaan määrittää erilaisia asetuksia käyttäjä- tai tietokonetilille (kuva 3). [8, s. 229–237.]



Kuva 3. Ryhmäkäytännön hallintakonsoli.

3.3 DNS (Domain Name Server)

3.3.1 DNS:n hierarkia

Internet-verkossa tietokoneet tunnistavat ja löytävät toisiinsa käyttäen IP-osoitetta hyväksi, mutta ihmiset muistavat paremmin nimiä kuten *www.kangxu.fi*, kuin numeerisia IP-osoitteita. Nimipalvelujärjestelmän (Domain Name Server, DNS) tarkoitus on kääntää nämä ihmisystävälliset nimet tietokoneystävällisiksi ja toisinpäin. Koska Internet-maailmassa on miljoonia web-sivuja, ja jokaisella omanlaatuinen nimi, maailmanlaajuinen DNS-verkosto on tehty hyvin hierarkkiseksi.

DNS käyttää puumaista nimeämishierarkiaa. Nimettömät juuripalvelimet sijaitsevat tämän hierarkian ylimmällä tasolla ja seuraavalla tasolla yleiset vyöhykkeet (kuten .com, .org, .net) ja maankohittaiset vyöhykkeet (kuten .us, .uk, .fi) (taulukko 2). Eri organisaatioilla on erilaiset kakkostason vyöhykkeet (kuten *microsoft.com* tai *cisco.com*). Sama organisaatio voi myös luoda alavyöhykkeitä omaan käyttöönsä (kuten *corp.microsoft.com*). Vyöhykkeet, alivyöhykkeet ja palvelimen nimet erotetaan pisteellä ("."). Palvelimen nimet ja alemmitasoiset vyöhykkeet näkyvät DNS-nimessä ensimmäisinä ja ylimmän tasoiset vyöhykkeet lopussa (esimerkiksi *HRserver1.corp.microsoft.com*). [9.]

Taulukko 2. Esimerkkejä DNS-hierarkiassa käytettävissä olevat vyöhykkeiden päätteet.

Päätteet	Keille suunnattu
.com	Commercial, kaupalliset organisaatiot
.edu	Educational, koulutukselliset instituutiot
.gov	Governmental, hallitukselliset instituutiot
.mil	Military, sotilaalliset organisaatiot
.net	Network, verkkopalveluorganisaatiot
.org	Organizational, muu organisaatio
.int	International, kansainvälinen organisaatio
.fi, .us, .uk jne.	Suomi, USA, UK, maatunnus

3.3.2 DNS:n vyöhykkeet

Jokainen vyöhyke DNS-hierarkissa, kuten *microsoft.com*, *corp.microsoft.com*, ja *HRserver1.corp.microsoft.com*, ovat toisistaan erillään olevat alueet. Jokaisella vyöhykkeellä on oma hallintanimipalvelin. Esimerkiksi pääkonttorin DNS-palvelimella hallitaan *microsoft.com* ja *north.microsoft.com* vyöhykkeet, mutta sivukonttorin DNS-palvelimella hallitaan *west.microsoft.com*.

DNS-palvelimen toimialueet voidaan määrittää monella eri tavalla:

Ensisijaisen vyöhykkeen (Primary Zone) DNS-palvelin toimii vyöhykkeen ensisijaisena palvelimena. Tämä tarkoittaa sitä, että DNS-palvelimella on oikeus vastata DNS-tiedusteluihin, sallia muutoksia ja päivityksiä DNS-vyöhykkeellä ja tehdä lisäyksiä DNS-tietokantaan.

Toissijaisen vyöhykkeen (Secondary zone) DNS-palvelin toimii vyöhykkeen varapalvelimena. Varapalvelin saa kopion sen vastuussa olevasta vyöhykkeestä ensisijaiselta palvelimelta, kun muutoksia on tehty vyöhykkeen sisällä tai tietyin väliajoin. Varapalvelimella on oikeus vastata DNS-tiedusteluihin, mutta se ei saa tehdä muutoksia ja päivityksiä DNS-vyöhykkeellä tai lisäyksiä DNS-tietokantaan.

Tynkävyyhykkeen (Stub zone) DNS-palvelin toimittaa aina sen vastaanottamia palvelupyyntöjä vyöhykkeen ensisijaiselle- tai toissijaiselle DNS-palvelimelle. Palvelin sisältää ainoastaan NS (Name Server)-, SOA (Start of Authority)- ja A-tiedot.

Integroitussa aktiivihakemistovyöhykkeessä (Active Directory-integrated zone) säilytetään kaikki tiedot aktiivihakemistossa. Vyöhyketiedot monistetaan samaan aikaan aktiivihakemisto-monistusprosessin kanssa. Kaikki aktiivihakemiston tietoturvaratkaisut pätevät myös tälle vyöhykkeelle. [10.]

3.3.3 DNS:n vyöhykesiirrot

DNS:n vyöhykesiirto on prosessi, jolloin kaikki resurssitiedot ensisijaiselta DNS-palvelimelta kopioidaan toissijaiselle DNS-palvelimelle. Tällä tavalla voidaan

tasapainottaa verkon DNS-palvelupyynnöt monille eri palvelimille. Näin sallitaan myös jatkuvaa toimintaa DNS-palvelimilta, jos ensisijainen palvelin lopettaa toimintansa. Toissijainen palvelin voi tällöin toimia väliaikaisesti pääpalvelimena, ja sillä on oikeus tehdä vyöhykesiirtoja muille toissijaisille palvelimille.

Vyöhykesiirron menetelmät ovat seuraavat:

Täyssiirron (Full Transfer) käynnistyessä toissijainen DNS-palvelin kopioi kaikki resurssitiedot ensisijaiselta DNS-palvelimelta. Täyssiirtoon sisältyy kaikki vyöhykkeen tiedot. Tämä menetelmä vaatii paljon verkon kaistaresursseja.

Inkrementaalisella vyöhykesiirto (Incremental Zone Transfer) -menetelmällä kopioidaan ainoastaan ne resurssirekisteritiedot, jotka ovat muuttuneet edellisen siirron jälkeen. Tällä menetelmällä säästetään verkon kaistaresursseja. Inkrementaalinen vyöhykesiirto tapahtuu ainoastaan silloin, kun muutoksia on tehty vyöhykkeellä.

Aktiivihakemistosiirto (Active Directory Transfer) tapahtuu, kun aktiivihakemisto tekee aktiivihakemistomonistuksen ohjauskoneeseen.

DNS-ilmoitus (DNS Notify) -mekanismilla ilmoitetaan ensisijaisessa DNS-palvelimessa tapahtuva muutos toissijaiselle DNS-palvelimelle. Tämän viestin saatuaan toissijainen DNS-palvelin aloittaa joko täyssiirron tai inkrementaalisen vyöhykesiirron. [10.]

3.3.4 DNS:n tiedot

Verkkoresurssit, kuten ohjauskoneet, sähköpostipalvelimet ja käyttäjien tietokoneet tunnistetaan resurssitiedoilla. DNS-palvelin tukee monia erityyppisiä tietoja eri verkkoresursseille (taulukko 3). [10.]

Taulukko 3. Yleisesti käytössä olevat DNS-tiedot.

Resurssitiedot	Käyttötarkoitus
A	Yleisin tapa tunnistaa tietokoneen. A-tieto muuttaa palvelinnimeä IPv4 IP-osoitteeksi.
AAAA	A-tieto IPv6:lle. Käytetään neljä A:ta, koska IPv6:ssa on 128-bittiä, joka on neljä kertaa pidempi kuin IPv4:n 32-bittistä IP-soitetta.
CNAME	<i>Canonical Name</i> -tieto. Tämä resurssitieto toimii olemassa olevan A- tai AAAA-tiedon peitenimenä. CNAME-tietoa voidaan käyttää silloin kun yhdellä IP-osoitteella on enemmän kuin yksi palvelinimi.
MX	<i>Mail Exchanger</i> -tieto. MX-tiedolla tunnistetaan verkon sähköpostipalvelimet.
NS	<i>Name Server</i> -tieto. NS-tiedolla tunnistetaan verkon DNS-palvelimet. Jos verkossa on useita DNS-palvelimia, tällöin kaikilla palvelimella on oltava oma NS-tieto.
PTR	<i>Pointer</i> -tieto, joka tunnetaan myös nimellä reverse DNS lookup-tiedoksi. PTR-tiedolla etsitään palvelinimiä IP-osoitteen perusteella.
SOA	<i>Start of Authority</i> -tieto. SOA-tieto määrittää verkon arvovaltaisim DNS-palvelin.
SRV	<i>Serve Record</i> -tieto. SRV-tietoa käytetään verkon aktiivihakemiston ohjauskoneiden tunnistamisessa.

3.3.5 DNS:n dynaamiset päivitykset

Nykyään suuri osa tietokoneista saa IP-osoitteensa DHCP-palvelimelta. Koska DHCP:n IP-osoitteet muuttuvat aika ajoin, on hyvin epäkäytännöllistä muuttaa tietokoneiden resurssitiedot manuaalisesti.

DNS:n dynaamisella päivityksellä sallitaan tietokoneiden päivittää omat resurssitiedonsa. Kun tietokone saa uuden IP-osoitteen, joko tietokone itse tai DHCP-palvelin lähettää DNS-palvelimelle uuden päivitetyn resurssitiedon. Manuaalisesti määritetyt tietokoneet voivat myös käyttää DNS:n dynaamista päivitystä, mutta sillä on enemmän hyötyä DHCP:n asiakkaille. Näin käy esimerkiksi silloin, kun asiakkaat vaihtavat verkkoa tai kun DHCP-palvelimelta saamien IP-osoitteiden laina-aika on umpeutunut.

3.3.6 Palvelinnimien selvittäminen DNS-verkossa

Koska DNS on hyvin laajasti jakautunut maailmalla, yksittäinen DNS-palvelin ei pysty vastaamaan kaikkiin DNS-tiedusteluihin. Tästä syystä DNS-tiedustelut ovat yleensä hyvin itseään toistavia, mikä tarkoittaa sitä, että DNS-palvelimen, joka vastaanottaa DNS-tiedustelun, täytyy itse vielä tiedustella muilta DNS-palvelimilta löytääkseen oikean nimipalvelun.

Seuraavassa esitellään tyypillinen DNS-tiedustelusessio:

1. Tietokone lähettää DNS-tiedustelun paikalliselle DNS-palvelimelle. Esimerkiksi halutaan saada selville, mikä on *www.microsoft.com* IP-osoite.
2. Paikallinen DNS-palvelin lähettää tiedustelun DNS-juuripalvelimelle tunnistukseen DNS-palvelimen, jolla on kakkostason vyöhykkeet (tässä tapauksessa .com) tietokannassaan.
3. Tämän jälkeen paikallinen DNS-palvelin lähettää tiedustelun kakkostason DNS-palvelimelle, joka on vastuussa DNS-tiedusteluihin vastaamisesta .com-vyöhykkeeseen liittyen.
4. .com DNS-palvelin palauttaa paikalliselle DNS-palvelimelle vastauksena listan, joka sisältää *microsoft.com*-verkon DNS-palvelimien IP-osoitteita.
5. Paikallinen DNS-palvelin lähettää tiedustelun *microsoft.com*-verkon DNS-palvelimille saadakseen selville palvelinnimen. Esimerkiksi tässä tapauksessa paikallispalvelin valitsee listalta yhden DNS-palvelimen, ja lähettää tälle tiedustelun *www.microsoft.com* IP-osoitteesta.
6. *Microsoft.com*-verkon DNS-palvelin vastaa tiedustelun IP-osoitteella, jota pyydettiin.
7. Paikallinen DNS-palvelin välittää saamansa IP-osoitteen asiakastietokoneelle. DNS-tiedustelusessio on valmis.

DNS-palvelimet tallentavat DNS-tiedustelusessiot välimuistiinsa, jotta voisivat vastata samojen palvelinnimien DNS-tiedusteluihin ainoastaan kahdella askeleella. Tämän lisäksi tietokoneetkin tallentavat pyytämiään palvelinnimiä välimuistiinsa.

DNS-liikenteet käyttävät sekä TCP- että UDP-protokollaa ja molemmat niistä oletusporttia 53. DNS-tiedustelut käyttävät melkein ainoastaan UDP-protokollaa. [11.]

3.4 Windows Server 2008:n DHCP (Dynamic Host Configuration Protocol)

3.4.1 DHCP-osoitteiden jako

Suurin osa IPv4 verkkolaitteista saa IP-osoiteasetukset DHCP-palvelimelta. Tietokoneet, jotka ovat automaattisesti määritetty saamaan asetukset DHCP-palvelimelta, ovat paljon helpompia hallita kuin manuaalisesti määritetyt. Aina kun tietokoneita siirretään paikasta toiseen tai joudutaan vaihtamaan DNS-palvelimia tai päivitetään oletusyhdykskäytävää, kaikki päivitetyt IP-osoiteasetukset saadaan automaattisesti DHCP-palvelimelta.

DHCP-palvelin määrittää automaattisesti asiakkaan IP-osoiteasetukset keskustelemalla asiakkaan kanssa DHCP-viestien avulla. Näin DHCP-palvelin varmistaa, etteivät IP-osoiteasetukset joita annetaan asiakkaalle ole muiden tietokoneiden käytössä.

DHCP-asiakas on tietokone, joka saa IP-osoiteasetuksensa DHCP-palvelimelta.

DHCP-palvelin on tietokone, joka toimittaa IP-osoiteasetuksia monelle eri DHCP-asiakkaalle. Ylläpitäjä päättää, mitkä IP-osoiteasetukset on saatavilla millekin asiakkaille.

DHCP:n laina-aika määrittää, kuinka kauan IP-osoitteet on lainassa kullekin DHCP-asiakkaalle. Laina-aika voi olla 1 minuutista 999 päivään tai rajaton. Oletusasetuksessa laina-aika on 8 päivää Windows Server 2008 käyttöjärjestelmässä.

Ennen kuin asiakkaalle annetaan tarvittavat IP-osoiteasetukset, DHCP-palvelin ja asiakkaan välillä on käytävä nelivaiheinen viestien vaihto.

Asiakas lähettää *DHCPDiscovery*-viestin paikallisessa verkossa selvittääkseen, onko verkossa vapaita DHCP-palvelimia.

Jos paikallisverkosta löydetään DHCP-palvelin, joka pystyy tarjoamaan asiakkaalle IP-osoiteasetukset, palvelin lähettää *DCHPOffer*-viestin takaisin kyseiselle asiakkaalle. DHCPOffer-viesti sisältää listan asetusparametrissa ja vapaana oleva IP-osoite DHCP-palvelimen osoitevarastosta. Jos DHCP-palvelimella on varattu IP-osoite kyseisen

asiakkaan MAC-osoitteen mukaan, annetaan tämä IP-osoite kyseiselle asiakkaalle. On myös mahdollista, että enemmän kuin yksi DHCP-palvelin lähettää DHCP-viestiä takaisin palvelua pyytävälle asiakkaalle.

Asiakas vastaa ainoastaan yhteen DHCPOffer-viestiin *DHCPRequest*-viestillä. Tämä on yleensä ensimmäinen DHCPOffer-viesti, jonka asiakas vastaanottaa. Tässä viestissä asiakas pyytää DHCP-palvelimelta kaikki asetusparametrit ja IP-osoitteen, jotka sisältyivät DHCPOffer-viestissä. Vaihtoehtoisesti asiakas voi myös pyytää DHCP-palvelimelta IP-osoitteen, joka oli ennenkin ollut asiakkaan käytössä.

Jos asiakkaan haluama IP-osoite on vielä vapaana, DHCP-palvelin vastaa *DHCPAck*-viestillä vahvistaakseen asiakkaalle. Asiakas ottaa IP-osoitteen käyttöönsä.

Käytössä on myös muita DHCP-viestejä:

DHCP-asiakas lähettää *DHCPDecline*-viestin DHCP-palvelimelle ilmoittaakseen, että palvelimen tarjoama IP-osoite on hylätty. Asiakas hylkää tarjouksen, jos tämä huomaa, että tarjottu IP-osoite on jo käytössä. DHCPDecline-viestin jälkeen asiakkaan täytyy aloittaa koko prosessia uudestaan.

DHCP-palvelin lähettää DHCP-asiakkaalle *DHCPNack*-viestin tarkoituksena hylätä DHCPRequest-viesti. Tämä voi käydä silloin, kun palvelin huomaa, että pyydetty IP-osoite on virheellinen, koska asiakasta on siirretty toiseen aliverkkoon, tai asiakkaan laina-aika on umpeutunut, eikä sitä voida enää uusia.

DHCPRelease-viestillä asiakas luovuttaa IP-osoitteen DHCP-palvelimelle ja nolaa laina-aikansa. Tämä viesti lähetetään sille DHCP-palvelimelle, jolta asiakas alun perin sai IP-osoitteensa.

Jo voimassa olevan IP-osoitteen omaava asiakas lähettää *DHCPInform*-viestin pyytääkseen lisää asetusparametrejä DHCP-palvelimelta. Tällä viestillä voidaan myös havaita luvattomia DHCP-palvelimia verkossa.

Kaikki DHCP-liikenteet käyttävät UDP-protokollaa. Viestit DHCP-asiakkaalta DHCP-palvelimille käyttävät UDP-lähdeporttia 68 ja UDP-kohdeporttia 67. Vastaavasti viestit

DCHP-palvelimelta DHCP-asiakkaalle käyttävät UDP-lähdeporttia 67 ja UDP-kohdeporttia 68.

Yleensä DHCP IP-osoitteen toimeksiantoon sisältyvät seuraavat konfiguraatiodiedot (tosin monia erilaisia vaihtoehtoja ovat määritettävissä):

- IP-osoitteen laina-ajan pituus, eli kuinka pitkäksi aikaa annettu IP-osoite on asiakkaan käytössä
- IP-osoite
- aliverkon peite
- oletusyhdykäytävä
- Ensisijainen ja toissijainen DNS-palvelimet
- DHCP-palvelimen IP-osoite. [12.]

3.4.2 DHCP-osoitteiden kierrätettävyys

Estääkseen IP-osoitetta jäämästä ainoastaan yhden asiakkaan käyttöön DHCP-palvelin ottaa asiakkaan IP-osoitteen takaisin laina-ajan päädyttyä. Lainajajan puolivälissä asiakas lähettää DHCP-palvelimelle IP-osoitteen uusimispyynnön. DHCP-palvelin vastaanottaa pyynnön ja nollaa lainajajan laskuria. Jos DHCP-palvelimeen ei saa yhteyttä, asiakas joutuu tekemään uudestaan lainajajan uusimispyynnön jäljellä olevan ajan puolivälissä. Jos DHCP-palvelin ei ole vieläkaan saatavilla, kun lainajajasta on kulunut 87,5 %, asiakas yrittää paikantaa uutta DHCP-palvelinta ja hankkii uuden IP-osoitteen.

Kun asiakkaan tietokone sammutetaan normaalisti tai ylläpitäjä käyttää *ipconfig /release*-komentoa komentorivillä, asiakas lähettää DHCPRelease-viestin DHCP-palvelimelle, jolta sai IP-osoitteen. DHCP-palvelin merkitsee palautettua IP-osoitteen vapaaksi ja siirtää sitä takaisin omaan IP-varastoon. Palautettu IP-osoite voidaan tästä lähtien antaa muiden asiakkaiden käyttöön tätä pyydetäessä. Jos asiakas yllättäen katkaisee yhteydensä verkkoon eikä ole lähettänyt DHCPRelease-viestiä, kyseisen asiakkaan IP-osoitetta ei palauteta DHCP-palvelimelle ennen kuin laina-aika on umpeutunut. Tämän takia on järkevää pitää IP-osoitteiden laina-ajat lyhyenä.

Esimerkiksi sopiva aika on kuusi tuntia langattomissa verkoissa, joissa asiakkaat katkaisevat ja kytkevät yhteyden hyvin säännöllisesti. [12.]

3.5 Internet Information Services 7.0 (IIS 7.0)

3.5.1 IIS yleisesti

IIS on Microsoftin kehittämä palvelinohjelmistokokonaisuus. IIS 7.0 sisältyy ainoastaan Windows Vista -käyttöjärjestelmän yritysversioon ja Windows Server 2008 -käyttöjärjestelmään. IIS on Windows Server 2008 -käyttöjärjestelmän oletus -asennuksessa kytketty pois päältä, mutta se voidaan ottaa käyttöön vaihtoehtoisena ominaisuutena.

IIS:n päätarkoitus on ylläpitää organisaation web-selainta ja web-sovelluksia .NET Framework -ohjelmistokomponenttikirjastoa hyväksi käyttäen.

Ennen kuin voidaan asentaa, päivittää tai luoda web-sivuja IIS 7.0-palvelimella, täytyy ensiksi ymmärtää sen toimintakuvat, parannukset verrattuna edellisiin versioihin, ja tutustua hallintatyökaluihin ja käyttäjäliittymään.

3.5.2 IIS 7.0:n parannuksia

IIS versio 7.0 on saanut paljon arkkitehtuurisia lisäyksiä ja parannuksia liittyen sen sovellusalustaan. Näillä parannuksilla halutaan nostaa palvelimen luotettavuutta, suorituskkyä, parantaa tietoturvallisuutta ja helpottaa ylläpitoa.

Modulaarisessa asennuksessa voidaan asentaa yli 40 erilaista ominaisuutta tai komponenttia. Joitakin näistä komponenteista asennetaan oletusasennuksessa, mutta ne ovat kuitenkin poistettavissa. Muut ominaisuudet voidaan asentaa itsenäisesti IIS-asennuksen jälkeen.

Uusilla hallintatyökaluilla voidaan samanaikaisesti hallita sekä IIS- että ASP.NET (Active Server Pages .NET Frameworks) -asetuksia yhdestä paikasta käsin. IIS 7.0:lla

on uusi tekstipohjainen komentorivi-työkalu nimeltään *appcmd.exe*, joka sisältää hallinta- ja asennus- ja määrittelykomentosarjat.

IIS 7.0:n *vianmäärittämis-* ja *vianetsintä-*työkaluilla saadaan näkyviin virheviestit, lokit ja tilannekoodit, joilla helpotetaan vianetsintää, diagnosointia ja virheiden korjaamista verkossa.

SSL-protokollaa tukeva FTP (File Transfer Protocol) -palvelin. SSL (Secure Sockets Layer)-protokollalla suojataan kaikki FTP-palvelimen sisään- ja ulospäin suuntautuva liikenne. SSL-protokollatuen lisäksi FTP-palvelin sisältää myös virtuaalikäyttäjänimituen ja käyttäjäeristäytymisominaisuuden. FTP-palvelinta voidaan määrittää käyttämään UTF8 (UCS Transformation Format — 8-bit)-, IPv6-, COM (*Component Object Model*)- ja .NET Frameworks -laajennuspaketit.

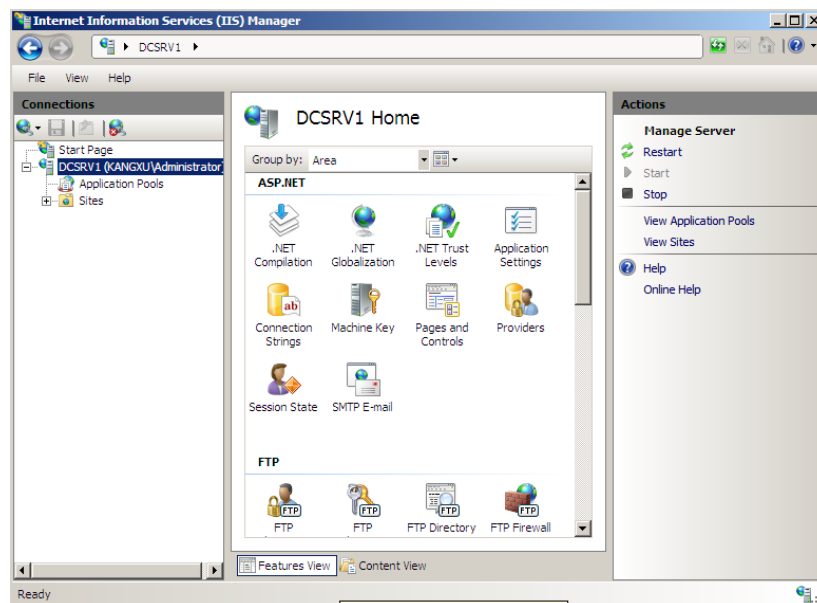
Ylläpitotuki jaetuilla oikeuksilla ja etäkäytöllä -ominaisuudella ylläpitäjät voivat kirjautua IIS:n hallintakonsoliin, jossa voivat tehdä vain ne tehtävät, jotka niille jaetut oikeudet sallivat. Etäkäyttöominaisuudella voidaan antaa tietyille ylläpitäjille oikeudet käyttää hallintakonsolia HTTP (Hypertext Transfer Protocol)/SSL-protokollaa hyväksi käyttäen.

IIS 7.0 tukemia protokollia ovat esimerkiksi

- FTP
- FTPS (FTP Secure)
- SMTP (Simple Mail Transfer Protocol)
- NNTP (Network News Transfer Protocol)
- HTTP/HTTPS (HTTP Secure). [13.]

3.5.3 IIS 7.0:n käyttäjäliittymän hallintaohjelma

IIS 7.0 -käyttäjäliittymän hallintaohjelmalla hallinnoidaan IIS- ja ASP.NET-palvelua (kuva 4), palvelimen tilaa, sen diagnosointia ja tietoturvaratkaisuja. Toinen tärkeä työkalu on IIS Manager snap-in-työkalu, jolla määritetään ja hallinnoidaan monia toimintoja IIS 7.0 -palvelimessa. [13.]



Kuva 4. IIS 7.0 -käyttäjiliittymän hallintaohjelma -ruutu.

3.5.4 Virtuaalihakemisto

Virtuaalihakemisto on hakemistonimi (tunnetaan myös nimellä "Polku"), jolla määritetään tiettyä fyysistä hakemistoa paikallis- tai etäpalvelimissa. Hakemistonimestä tulee osa tietyn sovelluksen URL (Uniform Resource Locator) -nimeä. Näin käyttäjät voivat syöttää URL:ää selaimeen osoitekenttään päästääkseen haluamiinsa tiedostoihin tietyn palvelimen fyysisessä hakemistossa.

IIS 7:ssa jokaiselle sovellukselle täytyy olla oma virtuaalihakemisto, joka on nimeltään juurivirtuaalihakemisto. Juurivirtuaalihakemistolla voidaan määrittää sovelluksille polku oman sisältönsä fyysiseen hakemistoon. Jokaisella sovelluksella voi olla enemmän kuin yksi virtuaalihakemisto. Esimerkiksi yhtä virtuaalihakemistoa voidaan käyttää siihen, että sovellus näyttää tiettyjä valokuvia jostain toisesta järjestelmästä, muttei kuitenkaan haluta siirtää valokuvia paikalliseen fyysiseen hakemistoon, joka on määritetty sovelluksen juurivirtuaalihakemistossa.

Virtuaalihakemistoon päässyt voidaan suojata käyttäjänimellä, salasanoilla ja *LogonMethod*-ominaisuudella. [13.]

4 Windows Server 2008:n tietoturva

4.1 Palvelintason tietoturva

Fyysinen tietoturva

Palvelimen fyysinen sijainti on yksi palvelintietoturvan tärkeimmistä osa-alueista. Palvelimet pitäisi olla fyysisesti lukitun oven takana, jonne on pääsynhallinta. Tämän lisäksi palvelimet pitäisi olla määritetty niin, että ainoastaan oikeutetut ylläpitäjät pääsevät fyysisesti kirjautumaan palvelimeen konsolin kautta.

Windows Firewall

Windows Server 2008 sisältää integroidun palomuurin, joka on oletetusti kytkettynä käyttöjärjestelmäsäätöjen jälkeen. Palomuri on täysin integroitu palvelinasennuksen kanssa. Tämä tarkoittaa sitä, että esimerkiksi kun ajetaan palvelinroolinasennusta ja valitaan tietty palvelinrooli asennettavaksi tietokoneeseen, palomuri avaa automaattisesti ainoastaan ne tarvittavat oletusportit, jotka tarvitaan asennettavaa palvelinroolia varten.

Tiettyissä tapauksissa, kun kolmannen osapuolen sovellusta ei ole integroitu käyttöjärjestelmän kanssa tai pitää avata tietty erikoisportti toimiakseen, täytyy tehdä manuaalista määrittystä palomuurin suhteen. Esimerkiksi luodaan pakettien sisääntulo- ja ulosmenosäännöt, miten ohjata liikenteet palvelimelle. Näillä määritetään, miten palvelin kommunikoi ulkomaailman kanssa.

Sääntöjä voidaan luoda seuraavien tekijöiden mukaan:

Voidaan luoda sääntö, joka sallii tietyn *ohjelman* ajamisen palvelimella. Esimerkiksi määritetään sääntö, jolla annetaan *c:\Program Files\Custom Programs\Ohjelma.exe*-tiedostolle oikeus lähettää ja vastaanottaa liikennettä.

Avataan tietty *TCP- tai UDP-portti* tietylle sovellukselle tai palvelulle.

Windows Server 2008:lla on sisäänrakennettuja, *ennalta määritettyjä sääntöjä (Predefined)*, esimerkiksi säännöt, jotka sallivat AD DS:n, DFS:n (Distributed File System), BITS:n (*Background Intelligent Transfer Service*) ja HTTP:n liikennettä.

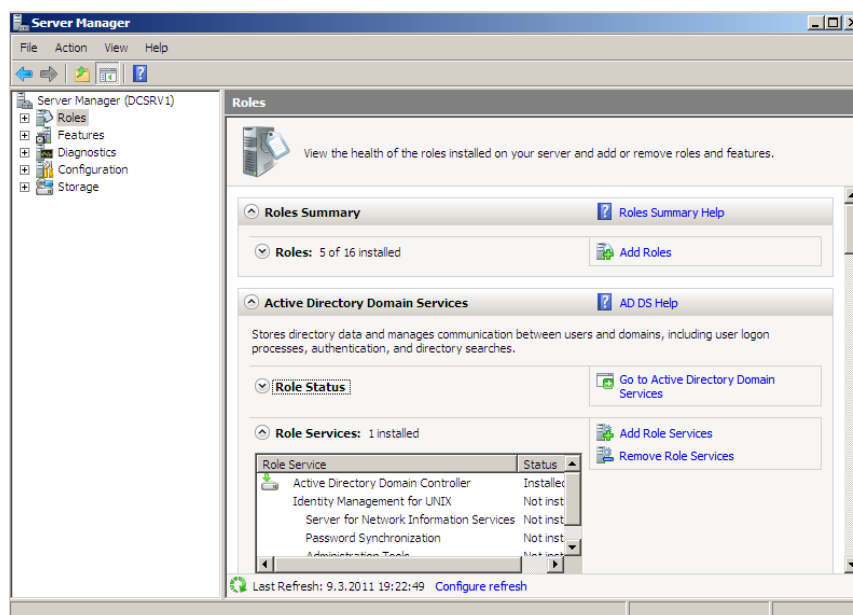
Voidaan myös luoda *tapauskohtaisesti määritetyt säännöt*, jos ohjelma-, portti- tai predefined-kohtaiset säännöt eivät salli sovellusten toimintaa. [14.]

Palvelintietoturva

Windows Server 2008:n oletusasennuksessa monet vähemmän käytetyt sovellukset ja palvelut on kytketty pois päältä, ennen kun ylläpitäjät manuaalisesti ottavat niitä käyttöön. Integroitu palomuri on automaattisesti käytössä, mutta se päästää läpi ainoastaan ne palvelu- ja sovellusliikenteet, joita palvelin välttämättä tarvitsee toimiakseen. Koska jokainen käyttöön otettu sovellus tai palvelu lisää kokonaistietoturvariskiä, on tärkeää ensiksi määrittää palvelimelle palvelinrooli, ja sen mukaan otetaan ainoastaan tarvittavat palvelut ja sovellukset käyttöön.

Riippuen organisaation koosta palvelimille voidaan antaa yksi tai monia rooleja verkossa. Suuressa organisaatiossa yhdellä palvelimella voi olla vain yksi palvelurooli kuten toimia DHCP- tai DNS-palvelimena. Tämä skenaario ei ole kuitenkaan kovin toteuttamiskelpoinen pienissä yrityksissä. Tästä syystä yksi fyysinen palvelin voi toimia sekä DHCP- että DNS-palvelimena riippuen yrityksen tarpeesta.

Server Manager -hallintakonsoli on työkalu, jolla määritetään palvelinroolia (kuva 5). Esimerkiksi palvelin, joka toimii DNS-palvelimena ja jossa tiedosto- ja tulostinpalvelut ovat poissa käytöstä, Server Manager automaattisesti avaa DNS-palvelulle vaaditut portit ja vastaavasti sulkee kaikki portit, jotka liittyvät tiedosto- ja tulostinpalveluun.



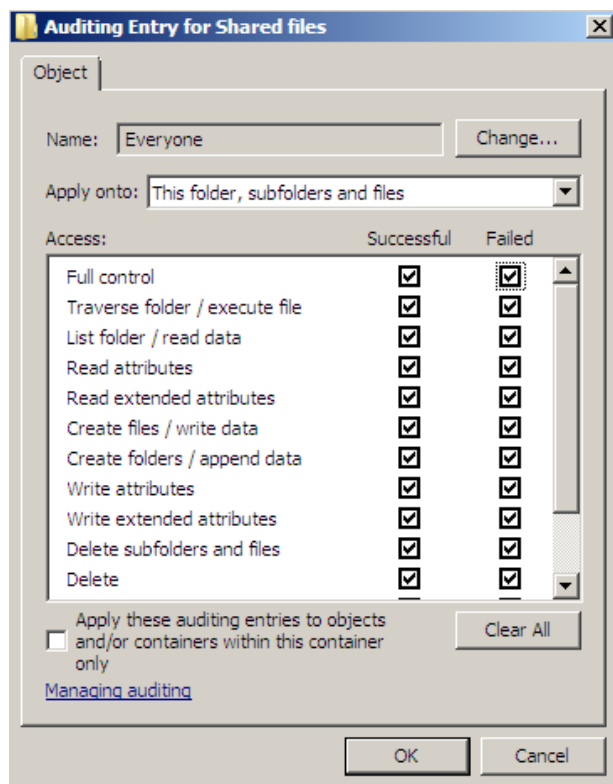
Kuva 5. Server Manager -hallintakonsoli.

Tiedostotietoturva

Windows Server 2008 -käyttöjärjestelmissä tiedostoja suojataan NTFS (New Technology File System) -käyttöoikeudella (kuva 6). Jokainen objekti, joka voi olla sekä tiedosto että kansio, merkitään ACE:lla (Access Control Entry), jolla fyysisesti rajoitetaan, ketkä pääsevät tiedostoihin käsiksi. NTFS-käyttöoikeudella pystytään määrittämään esimerkiksi tiedoston luku- ja kirjoitusoikeudet.

Toinen käyttöoikeus on jako-oikeus (Share-Level permission). Jako-oikeudella määritetään verkkopohjainen käyttöoikeus, eli tiedostoa omaavalla palvelimella määritetään, ketkä verkossa pääsevät käsiksi tiedostoihin, jotka fyysisesti sijaitsevat muualla verkossa. Vaikka jako-oikeutta voidaan käyttää myös paikallisella palvelimella, on kuitenkin turvallisempi käyttää NTFS-käyttöoikeuksia, koska siinä on enemmän vaihtoehtoja.

Hyödyllistä tiedostotietoturvan kannalta on myös tehdä valvontatarkastus tiedostojen käytöstä. Tietyn palvelimen, kansion tai tiedoston valvontatarkastuksella saadaan ilmoituksia siitä, ketkä ovat päässeet tai yrittäneet päästä niihin käsiksi.



Kuva 6. Valvontatarkastuksen valinnat.

Windows Server 2008 -käyttöjärjestelmä antaa tukea myös EFS:lle (Encrypting File System), jolla salataan tiedostojen sisältöä NTFS-tiedostojärjestelmän varustetuilla volyymeillä.

Muut tietoturvamekanismit

Virustorjuntaohjelmat ovat myös eräs tärkeimmistä tietoturvaratkaisuista Windows Server 2008:n käyttöympäristössä. Monet virukset on erityisesti koodattu tekemään vahinkoa tietyille palvelimen sovellukselle. Virukset saattavat saastuttaa palvelinta, jonka kautta muutkin tietokoneet verkossa vaarantuvat.

Microsoft Forefront -ohjelmalla voidaan samanaikaisesti ajaa viittä eri virustorjuntaohjelmaa samalla palvelimella. Jos virus jää yhdeltä virustorjuntaohjelmalta huomaamatta, on hyvät mahdollisuudet, että neljä muuta huomaavat sen. Virustorjuntaohjelmien tietokantaa päivitetään päivittäin.

Oikeutettu varmuuskopio-ohjelma sallii ainoastaan ne ylläpitäjät ottamaan varmuuskopiota palvelimesta, joille on jaettu kyseinen käyttöoikeus. Säännöllinen varmuuskopioiden ottaminen parantaa verkon tietoturvallisuutta. Esimerkiksi päivittäin otetut varmuuskopiot sisältävät uudemmat ohjelmakohtaiset päivitykset kuin viikoittain otetuissa varmuuskopioissa.

Lokeilla voidaan seurata verkon tapahtumia hyvin keskitetysti. Lokit ovat kuin verkon päiväkirja, jolla kirjataan tietyt tai halutut tapahtumat tulevaisuuden vianetsinnän helpottamiseksi.

Windows Server Update Services (WSUS)

WSUS-palvelimella ladataan Windowsin uusimmat päivitykset Microsoftin omalta palvelimelta (kuva 8). Tämän jälkeen WSUS-palvelin toimii organisaation verkon sisäisenä päivityspalvelimena, josta kaikki verkon tietokoneet ja palvelimet voivat hakea viimeisimmät päivityksensä. Tällä ratkaisulla kulutetaan paljon vähemmän laajakaistayhteyttä Windows-päivityksiin, kuin jos kaikki organisaation tietokoneet ja palvelimet hakisivat päivityksensä suoraan Microsoftin palvelimilta Internetin kautta.

Tietoturvaratkaisuna WSUS tarkistaa kaikki hakemansa päivitykset. Kaikki päivitykset ovat testattuja ja Microsoftin hyväksymiä. WSUS-palvelimen ylläpitäjä voi itse valita, mitkä päivitykset jaetaan millekin tietokoneille tai palvelimille riippuen niiden roolista verkossa ja tarpeesta. Ylläpitäjä voi myös määrittää WSUS-palvelinta jakamaan tietyt päivitykset tietyille tietokoneille ja palvelimille tiettyyn aikaan. Esimerkiksi kaikki tietoturvapäivitykset jaetaan välittömästi kaikille heti, kun ne ovat saatavilla. Muut päivitykset jaetaan keskiyöllä, kun verkon sisäinen liikenne on vähimmillään.

WSUS-palvelimen vaatimukset käyttöjärjestelmältä ovat seuraavat:

- Windows Server 2003 SP1/SP2 tai Windows Server 2008
- Internet Information Services (IIS)
- Background Intelligent Transfer Service (BITS)

- Windows Internal Database -rooli käytössä palvelimella tai SQL Server 2005 asennettuna joko paikallisena asennuksena tai etäkäyttöä tukevalla palvelimella
- Microsoft .NET Framework 2.0 tai uudempi. [15.]

4.2 Kuljetustason tietoturva

Kuljetustasontietoturva yleisesti

Kuljetustason tietoturvalla turvataan tietokoneiden ja palvelimien välistä liikennettä ja niiden kommunikointia. Liikennettä voidaan salakirjoittaa, jotta tiedostot olisivat hyödyttömiä hyökkääjille niitä siepattaessa. Koska hyvinkin turvatuista verkoista voi löytyä haavoittuvuuksia, pitää ottaa käyttöön monitasoisia tietoturvaratkaisuja. Jos yksi taso murretaan, hyökkääjä joutuu vielä läpäisemään toisen ja kolmannen tason ennen kuin pääsee käsiksi haluamiinsa tiedostoihin. Esimerkiksi voidaan käyttää salasanojen salaamiseen 128-bittistä salausta, joka on vaikeasti murrettava. Suojaus on turha, jos hyökkääjä saa verkon salasanan tai PIN-koodin verkon käyttäjältä. Varmistamalla vielä toinen taso ensimmäisen tason lisäksi vaikeutetaan hyökkääjän läpäisyn mahdollisuutta.

Kuljetustason tietoturva on yksi tärkeimmistä tietoturva-aiheista. Tietokoneiden ja palvelimien välinen kommunikoinnin suojaaminen ja turvaaminen on elintärkeätä verkon turvallisuudelle. Windows Server 2008 -käyttöjärjestelmä tarjoaa tietoturvamekanismeja kuljetustasolle IPsec-, AD CS (Active Directory Certificate Services)-, AD RMS (Active Directory Right Management Services)- ja PKI (Public Key Infrastructure) -teknologiaa hyväksi käyttäen.

Active Directory Certificate Services (AD CS)

Windows Server 2008 -käyttöjärjestelmässä on sisäänrakennettu Certificate Authority (CA) -teknologia, joka tunnetaan nimellä Active Directory Certificate Services (AD CS).

AD CS:llä voidaan luoda ja hallita varmenteita, ja se on vastuussa varmenteiden kelpoisuudesta verkossa. Yleensä AD CS:ää käytetään Windows Server 2008:n ympäristössä, jos ei ole tarvetta käyttää kolmannen osapuolen varmennepalveluja. Sisäverkon käyttäjille voidaan luoda erillinen CA liikenteiden salausta varten. [7, s. 12.]

AD DS:n oikeuksien hallinta

Active Directory Right Management Services (AD RMS) on Digital Rights Management -teknologiaan perustuva ominaisuus, jolla voidaan asettaa rajoituksia eri sisällöille, kuten miten niitä hallinnoidaan, lähetetään ja tarkastellaan. RMS käyttää PKI -teknologia salatakseen salattavaa sisältöä, kuten dokumentit ja sähköpostiviestit.

AD RMS sisältää palveluroolin, joka tunnetaan nimellä Identity Federation (IF). IF:llä voidaan sallia organisaatio jakamaan tiedostoa muiden organisaatioiden kanssa yleisen verkon kautta. [7, s. 16–18.]

4.3 Windows Server 2008:n IPsec

IP Security eli IPsec on tietoturvamekanismi, jonka pääasiallinen tehtävä on salata ja turvata kaikki tietoliikenne tietokoneiden välillä. IPsec toimii OSI-mallin 3. kerroksessa eli verkkokerroksessa. Se salaa kaikki paketit, jotka kulkevat asiakaskoneiden välillä. IPsec sisällyttää oman tunnisteensa jokaisen paketin tunnistekentän eteen ja lähettää kyseinen paketin määrättyyn kohteeseen purettavaksi.

IPsec:llä on monia erilaisia käyttöönottotapoja, esimerkiksi Network Interface Card (NIC) sisäänrakennettu IPsec, jolla pystytään salaamaan ja purkamaan paketteja ilman että käyttöjärjestelmän tarvitsee olla tietoinen siitä. Tämän lisäksi Windows Server 2008 sisältää IPsec-toteutuksen, jolla voidaan määrittää IPsec käyttämään PKI:n sertifikaattiverkkoa.

Windows Server 2008:n IPsec tarjoaa seuraavat tietoturvaratkaisut:

Data privacy -ratkaisulla kaikki tietoliikenteet yhdestä IPsec-tietokoneesta toiseen on täysin salattu 3DES (*3 Data Encryption Standard*) -algoritmilla, joka estää luvattomilta pääsyn tiedostoihin.

Data integrity -ratkaisulla IPsec-paketissa käytetään ESP (Encapsulating Security Payloads) -tunnistetta, jolla varmistetaan, ettei paketin sisältämiä tiedostoja ole muutettu.

Anti-replay capability -ratkaisulla IPsec estää luvattomasti napattujen pakettien uudelleenlähettämisen, joka tunnetaan myös nimellä "replay"-hyökkäyksenä. Tällä menetelmällä hyökkääjä voi teeskennellä olevansa oikea käyttäjä ja tätä kautta päästä käsiksi palvelimiin.

Per-packet authenticity -ratkaisussa IPsec käyttää hyväksi varmenteita ja Kerberos -oikeutusmenetelmää varmistaakseen, että IPsec-paketin lähettäjä on oikeasti se, joka väittää olevansa.

NAT traversal -ratkaisulla Windows Server 2008:n IPsec sallii IPsec-paketit reititettäväksi Network Address Translation (NAT) -toteutuksen läpi.

Diffie-Hellman 2048-bit key support -ratkaisulla Windows Server 2008:n IPsec tukee Diffie-Hellman 2048-bittistä avaimen käyttöä. [14.]

5 Windows Server 2008:n verkko käytännössä

Käytäntöosiossa koottiin verkko, joka koostui kolmesta Windows Server 2008 -käyttöjärjestelmällä varustetuista tietokoneesta ja yhdestä Windows XP -käyttöjärjestelmällä varustetusta käyttäjäkoneesta, joiden nimet ovat dcsrv1, srv2, srv3 ja XP. Dcsrv1 toimii ohjauspalvelimena, aktiivihakemistona, ensisijaisena DNS-palvelimena, DHCP- ja IIS-palvelimena. Srv2 toimii toissijaisena DNS-palvelimena. Srv3 toimii asiakastietokoneena, jolla testattiin IPsec-ominaisuutta. XP-tietokone toimii tiedostojen jako- ja kirjautumiskomentosarjan testauskoneena. Verkkoa rakennettiin Virtual PC 2007 -ohjelmalla. Verkon rakentaminen suoritettiin vaiheittain. Ensimmäisenä asiana käyttöjärjestelmän asennuksien jälkeen määritettiin staattiset IP-asetukset molempiin palvelimiin. Tämä jälkeen varmistettiin, että yhteys toimii palvelimien välillä. Kun ensimmäisen tason yhteys saatiin, rakennettiin aktiivihakemisto-palvelu, jolla hallinnoitiin kaikki verkkoon liittyvät toiminnot. DNS-palvelinta määritettiin, jotta saatiin oikeanlaiset nimipalvelut käyttöön. DHCP-palvelimella hallittiin IP-osoitteiden jako verkon käyttäjille. IIS-palvelulla ylläpidettiin web-palvelinta.

Verkkorakenteella haluttiin havainnollistaa pieni- tai keskikokoisen yrityksen sisäverkkoa; siksi ei määritetty Internet-yhteyttä ulkomaailmaan. Kaikki palvelimet ja käyttäjäkoneet toimivat suljetussa testiympäristössä.

5.1 Windows Server 2008:n asentaminen

Verkkoon asennettiin kolme 32-bittistä Windows Server 2008 Standard -käyttöjärjestelmää oletusasetuksella ja yksi Windows XP Professional SP3 (Service Pack 3), koska Virtual PC 2007 -ohjelma ei tue 64-bittisiä käyttöjärjestelmäasennuksia. Kaikille kolmelle Server 2008 -käyttöjärjestelmälle varattiin 1024 MB RAM-muistia, 65 GB kovalevytilaa ja yksi LAN (Local Area Network) -liitäntä. XP-tietokoneelle varattiin 512 MB RAM-muistia ja 20 GB kovalevytilaa. Emokoneen prosessorina oli Pentium Dual-Core T4200 2 GHz. Oletusasennuksessa asennettiin puhdas Windows Server 2008 Standard -käyttöjärjestelmä, johon ei sisältynyt yhtään ylimääräistä palvelua tai sovellusta.

Asennuksen jälkeen määritettiin dcsrv1:lle ja srv2:lle omat staattiset IP-asetukset. Käytäntö-osiossa käytettiin koko 192.168.0.0/24-verkkoavaruutta hyväksi. Dcsrv1-palvelimelle annettiin IPv4-osoite 192.168.0.1, aliverkon peitteellä 255.255.255.0. Srv2-palvelimille annettiin 192.168.0.2 255.255.255.0. Srv2:lle määritettiin myös vaihtoehtoinen IPv4-osoite 192.168.0.200 255.255.255.0. Tällä hetkellä molemmat palvelimet ovat vielä osaa *WORKGROUP*-ryhmää, joka on oletusasetuksena. Srv3 ja Windows XP -tietokone liitettiin verkkoon vasta, kun aktiivihakemisto, DNS- ja DHCP-palvelimet oli asennettu ja määritetty.

Dcsrv1- ja srv2-palvelimiin on myös mahdollista määrittää IPv6-osoitteet, jotta IPv6-pakettien lähettäminen kangxu-verkossa olisi mahdollista ilman "IPv4 to IPv6" -menetelmiä ja myös siltä varalta, että tulevaisuudessa siirrytään kokonaan IPv6-osoitteiden käyttöön nykymuotoisessa verkossa.

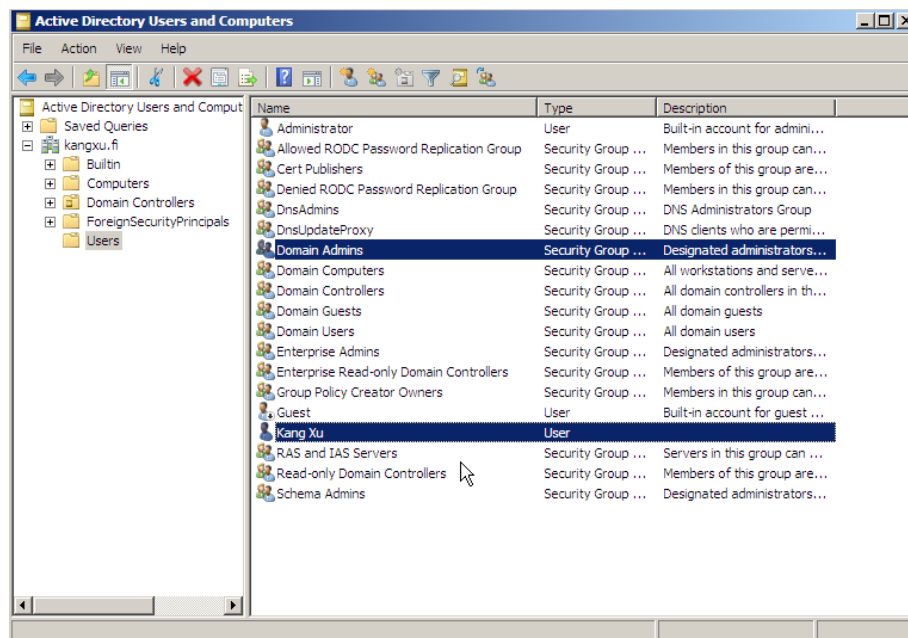
5.2 Windows Server 2008 -verkon rakentaminen

5.2.1 AD DS:n luonti

Aktiivihakemistoa asennettiin ainoastaan dcsrv1-tietokoneeseen. Asennusta aloitettiin syöttämällä komentoa *dcpromo* tekstipohjaisella komentorivillä. Koska aktiivihakemisto asennettiin ensimmäistä kertaa verkossa, täytyi luoda kokonaan uusi verkkotunnus uudessa metsässä (Forest). Verkkotunnuksena käytettiin nimeä *kangxu.fi*. Metsän ja verkon toimivuustasoksi valittiin Windows Server 2008 -taso, koska kaikki Windows Server 2008 -käyttöjärjestelmän tarjoamat uudistukset toimivat tällä tasolla. Windows Server 2008:n taso tukee myös vanhoja Windows Server -käyttöjärjestelmätasoja.

Aktiivihakemiston asennuksen jälkeen dcsrv1-palvelin kuului automaattisesti *kangxu.fi*-verkkoon.

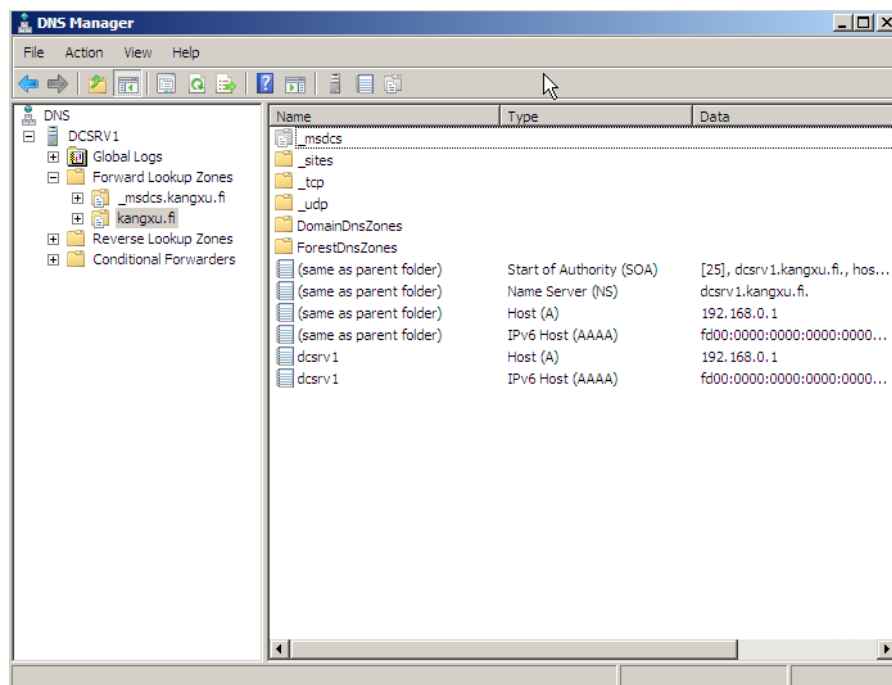
Asennuksen jälkeen luotiin uusi käyttäjätili ylläpitäjälle nimellä *Kang Xu*, joka kuuluu ryhmään *Domain Admins* (kuva 7). Tällä käyttäjällä voidaan hallinnoida kaikki mahdolliset toiminnot ja oikeudet *kangxu.fi*-verkossa, koska sillä on korkein mahdollinen oikeus.



Kuva 7. Uusi Kang Xu -käyttäjä luotu.

5.2.2 DNS-nimipalvelin asennus ja määrittely

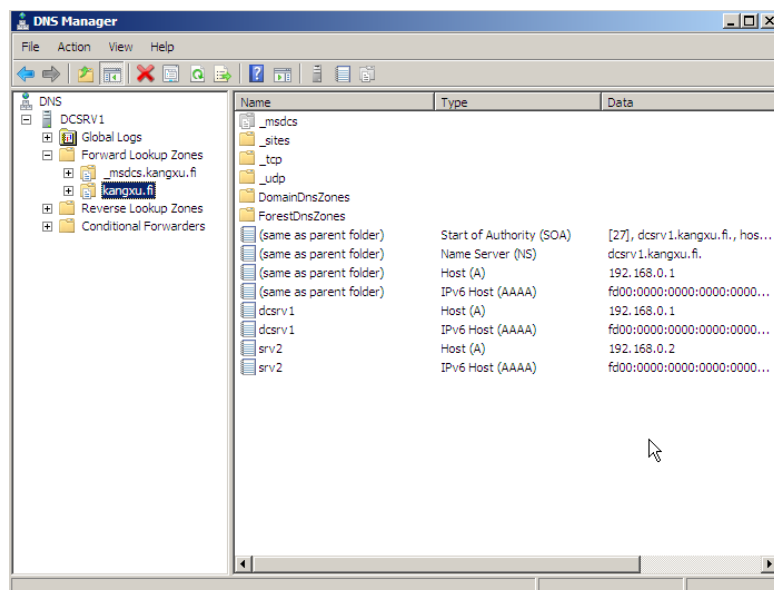
Dcsrv1:n aktiivihakemiston asennuksen aikana asennettiin samalla myös DNS-palvelun. Dcsrv1 toimii tällöin myös ensisijaisena DNS-palvelimella, jolla on kaikki mahdolliset muutos- ja päivitysoikeudet *kangxu.fi*-verkossa. DNS-palvelin käyttää myös samoja staattisia IP-osoitteita, jotka määritettiin heti Windows Server 2008 -käyttäjärjestelmän asennuksen jälkeen. Kuten kuvasta 8 huomaa, sekä IPv4- että IPv6-osoitteelle löytyy oma NS-resurssitieto *kangxu.fi*-verkossa. Verkkotunnus ensisijaiselle nimipalvelimelle on *dcsrv1.kangxu.fi*.



Kuva 8. Ensisijaisen DNS-palvelimen listaamat resurssitiedot kangxu.fi -verkossa.

AD:n ja ensisijaisen DNS-palvelimen asennuksen jälkeen asennettiin srv2-palvelimeen oma DNS-rooli, jotta tämä voisi toimia toissijaisena DNS-palvelimena *kangxu.fi*-verkossa. Toissijaisen DNS-palvelimen asennuksessa valittiin DNS:n ”Secondary Zone”, koska jos ensisijainen palvelin jostain syystä kytkeytyy pois päältä, verkossa olisi edelleen toimiva DNS-palvelin, jolla on kaikki viimeisimmät päivitettyt resurssitiedot kangxu-verkosta ennen kuin ensisijaisen DNS-palvelin lopetti toimimasta.

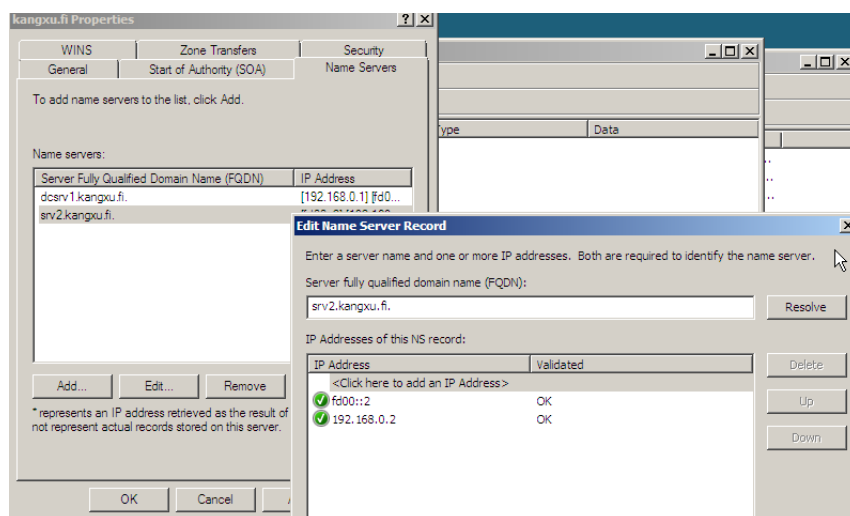
Srv2:een asennettiin DNS-palvelurooli kaikilla oletusasetuksilla. Palvelun asennuksessa luotiin uusi toissijainen toimialue *kangxu.fi*-verkolle, jonka ensisijainen palvelin osoittaa 192.168.0.1-osoitteeseen eli dcsrv1:een. Srv2:n DNS Manager -konsolista nähtiin samantien, että verkko on luotu, sillä srv2-palvelimen resurssitiedot näkyvät dcsrv1-palvelimella (kuva 9).



Kuva 9. Toissijaisen DNS-palvelimen IP-osoite on 192.168.0.2, eli srv2:n IP-osoite.

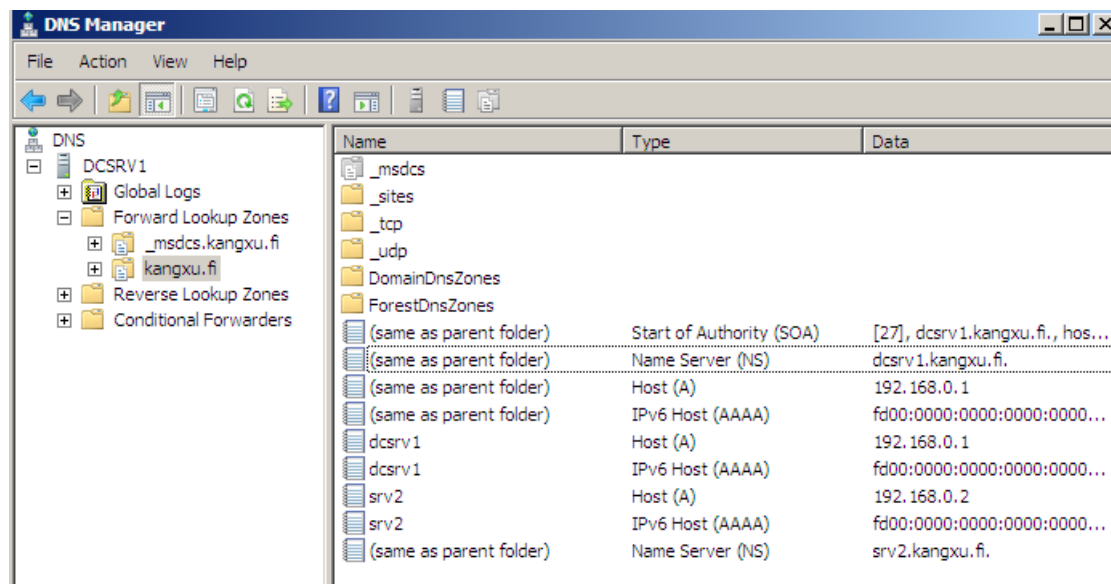
Dcsrv1:n DNS-palvelimella otettiin vyöhykesiirto-ominaisuus käyttöön sallimalla tämä srv2:ssa olevalle DNS-palvelimelle, koska ellei sallita vyöhykesiirtoa, srv2:ssa oleva toissijainen DNS-palvelin ei pysty päivittämään oman *kangxu.fi*-verkon tietoja dcsrv1:ltä.

Toissijaiselle DNS-palvelimelle luotiin NS-resurssitieto ensisijaiseen DNS-palvelimeen. NS-tiedolla selvitettiin sekä srv2:n IPv4- että sen IPv6-osoite, joka tunnistettiin verkkotunnuksella (kuva 10).



Kuva 10. Resurssitietojen luominen toissijaiselle DNS-palvelimelle ensisijaiseen DNS-palvelimeen.

Kaikki tarpeelliset resurssitiedot lisättiin onnistuneesti ensisijaiseen DNS-palvelimen DNS Manager -konsoliin (Kuva 11.). DNS-palvelimet asennettiin onnistuneesti, ja verkko *kangxu.fi* on toiminnassa.



Kuva 11. Kaikki näkyvät resurssitiedot ensisijaisessa DNS-palvelimessa.

Toissijaisen DNS-palvelimen toimivuutta testattiin sammuttamalla ensisijainen DNS-palvelin eli dcsrv1:tä. Sammuttamisen jälkeen huomattiin, että toissijainen DNS-palvelin alkoi toimia ensisijaisena DNS-palvelimena niin kauan, kunnes dcsrv1 kytkeytyy takaisin päälle. Koska dcsrv1:ssä oli myös verkon ainoa AD DS -palvelu, kangxu.fi-verkon kaikki tiedostojako-, oikeus- ja hallinnointipalveluun liittyvät ominaisuudet olivat myös pois käytöstä.

5.2.3 DHCP-palvelin asennus ja määrittely

DHCP-palvelinta asennettiin dcsrv1-palvelimeen. Asennuksen jälkeen siirrettiin srv2-palvelin DHCP-asiakkaaksi, jolloin se saa kaikki IP-määrytykset DHCP-palvelimelta. Asennuksen jälkeen kaikki verkkoon liittyvät asiakastietokoneet saavat automaattisesti IP-asetusparametrit DHCP-palvelimelta.

DHCP-roolin asennuksessa varmistettiin, että DHCP-palvelin tulee käyttämään IP-osoitetta 192.168.0.1 *kangxu.fi*-verkossa, ja ensisijainen DNS-palvelin toimii myös IPv4-osoitteessa 192.168.0.1. Samat määritykset tehtiin myös IPv6:lle eli osoitteelle fd00::1.

Määritetyt DHCP:n asennusparametrit ovat seuraavat:

- Nimi: kangxu.fi IPv4
- Ensimmäinen jaossa oleva IP-osoite: 192.168.0.20
- Viimeinen jaossa oleva IP-osoite: 192.168.0.254
- Aliverkon peite: 255.255.255.0
- Oletusyhdykäytävä: 192.168.0.1 (Eli dcsrv1), koska tämä on verkon pääpalvelin.

DHCP-roolin asennuksen jälkeen varmistettiin, että srv2 on ottanut käyttöönsä IP-osoitteen 192.168.0.20, joka on ensimmäinen vapaana oleva osoite DHCP-varastossa (kuva 12).

```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

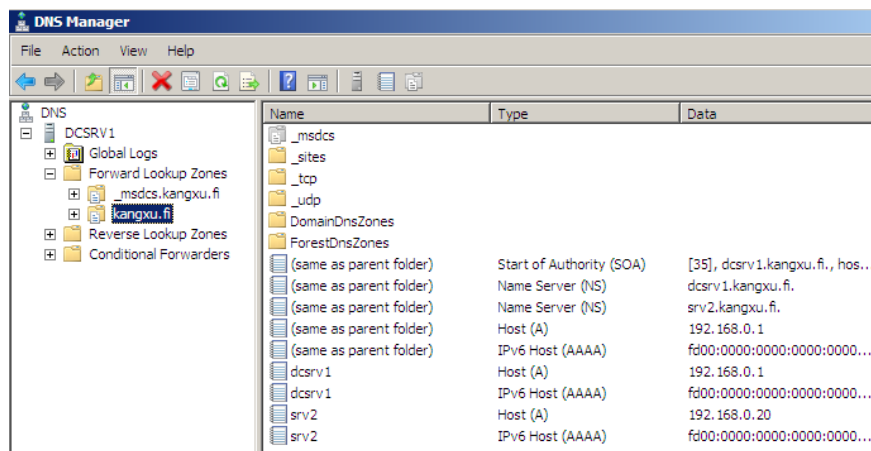
Host Name . . . . . : srv2
Primary Dns Suffix . . . . . : kangxu.fi
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : kangxu.fi

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : kangxu.fi
Description . . . . . : Intel 21140-Based PCI Fast Ethernet Adapter
(Emulated)
Physical Address. . . . . : 00-03-FF-FF-13-83
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address . . . . . : fd00::2(Preferred)
Link-local IPv6 Address . . . . . : fe80::a439:a5ab:dc63:efdd%10(Preferred)
IPv4 Address. . . . . : 192.168.0.20(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 10. joulukuuta 2010 16:11:10
Lease Expires . . . . . : 16. joulukuuta 2010 16:11:09
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DNS Servers . . . . . : fd00::1
                        192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled
```

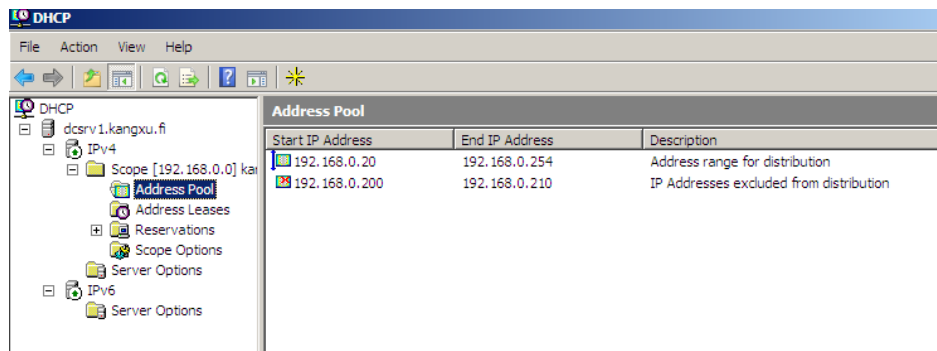
Kuva 12. Srv2 sai uuden IP-osoitteen DHCP-palvelimelta.

Tarkistettiin myös, että sama IP-osoite on päivitetty DNS-tietokantaan (kuva 13).



Kuva 13. Srv2:n IP-osoite on nyt 192.168.0.20.

DHCP-palvelimen asennuksen jälkeen otettiin IP-osoitteet 192.168.0.200–192.168.0.210 pois DHCP-varaston käytöstä siltä varalta, että jos tulevaisuudessa haluttaisiin staattisesti määrittää nämä IP-osoitteet tietyille tietokoneille. Nämä DHCP-varastosta pois käytöstä otettuja IP-osoitteita ei jaeta DHCP-asiakkaille (kuva 14).



Kuva 14. Pois käytöstä olevat IP-osoitteet.

DHCP-palvelin on asennettu ja määritetty oikein, koska kaikki tietokoneet, jotka liittyvät *kangxu.fi*-verkkoon, ovat saaneet juuri määritetyt IP-parametrit DHCP-palvelimen omasta IP-tietokannasta.

DHCP-palvelin helpottaa yrityksen sisäisen verkon hallintaa, koska ylläpitäjien ei tarvitse manuaalisesti määrittää tarvittavia IP-parametrejä kaikille verkossa oleville tietokoneille.

5.2.4 IIS-palvelun ja FTP:n asennus ja määrittäminen

IIS7-palvelu asennettiin dcsrv1-palvelimeen. Sovelluspalveluksi valittiin FTP-palvelua, koska se on yksinkertainen ja helppokäyttöinen protokolla, joka toimii tässä tapauksessa esimerkkinä. IIS 7.0 asennettiin Windows Server 2008:n oletusasennusparametreilla, koska asetuksissa tasapainotettiin tietoturvallisuutta, helppokäyttöisyyttä ja sujuvaa toimivuutta.

ASP .NET asennettiin IIS 7.0 asennuksen aikana, koska sitä vaaditaan, jotta IIS 7.0 toimii. Asennuksen jälkeen varmistettiin nettiselaimella, että IIS 7.0:n Default Web Site -sivu toimii oletussivuna (kuva 15).

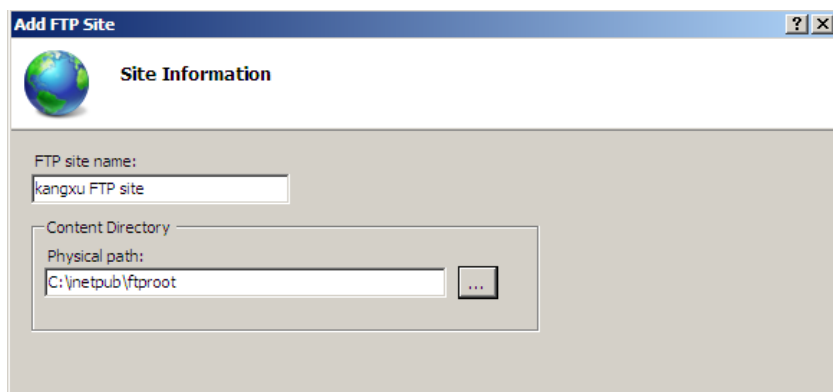


Kuva 15. IIS 7.0:n oletussivu.

IIS 7.0 asennuksen jälkeen luotiin virtuaalihakemisto *Default Web Site* -sivulle nimeltä "kangxu". Tämän virtuaalihakemiston fyysinen hakemisto sijaitsee paikallisella kovalevyllä. Hakemiston polku on C:\Reserch. Tämä mahdollistaa tiedostojen jaon IIS:n kautta. Kaikki asiakkaat verkossa pääsevät käsiksi "kangxu"-kansioon eli tiedostoihin, jotka fyysisesti sijaitsevat dcsrv1-palvelimen C:\Reserch -kansiossa.

Oletusasetuksessa on *Anonymous Authentication* -menetelmä käytössä. Se muutettiin *Forms Authentication* -menetelmäksi, koska se tarjoaa parempia todennusmahdollisuuksia.

FTP-asennuspakettia IIS:lle haettiin internetistä. Tiedoston nimi oli *FTP 7.5 for IIS 7.0 (x86)*. Paketti asennettiin kokonaan, eli kaikki mahdolliset ominaisuudet asennettiin. Asennuksen jälkeen luotiin IIS Manager -konsolin kautta FTP-sivu, joka on eri kokonaisuus kuin *Default Web Site* -sivu. Nimeksi sivulle annettiin *kangxu FTP site*, ja fyysiseksi poluksi dcsrv1-palvelimella annettiin *C:\inetpub\ftproot* (kuva 16).



Kuva 16. FTP-sivun nimen ja fyysisen polun tekeminen.

FTP-sivun IP-osoitteeksi määritettiin 192.168.0.1, joka on sama kuin dcsrv1-palvelimen IP-osoite ja oletusportiksi 21. FTP:lle annettiin verkkotunnus *ftp.kangxu.fi*. SSL-asetuksissa sallitaan SSL:n käyttö, mutta sitä ei vaadita palvelimen eikä asiakkaan FTP-yhteyden toteuttamisen kannalta. Näin käytetään SSL:ää aina kun on mahdollista, jossa taataan parempi tietoturva FTP-palvelua käytettäessä. Todennusmenetelmäksi otettiin *Anonymous*-vaihtoehto, ja oikeutusmenetelmäksi määritettiin *Anonymous Users* -vaihtoehto. Näin se sallii kaikki verkon tuntemattomatkin käyttäjät käyttämään FTP-palvelua. Todennus- ja oikeutusmenetelmiä voidaan kuitenkin muuttaa tulevaisuudessa, jos verkossa vaaditaan tiukempaa oikeusmäärittelyä käyttäjille. FTP-palvelun käyttäjille sallitaan ainoastaan *Read*-oikeus. Tätä oikeutta voidaan myös muuttaa tarvittaessa.

FTP-sivun onnistuneen luonnin jälkeen määritettiin *administrator*-käyttäjälle sekä *Read*- että *Write*-oikeus *kangxu FTP Site* -sivulle.

FTP-sivun toimivuutta testattiin srv3-tietokoneella ottamalla yhteyttä dcsrv1-palvelimeen. Syötettiin srv3:n komentoriville komento: *ftp 192.168.0.1*. Komennon jälkeen pyydettiin käyttäjänimeä, jolloin syötettiin *Anonymous*. FTP-palvelimeen saatiin yhteys onnistuneesti (kuva 17).


```

ftp> ?
Commands may be abbreviated.  Commands are:

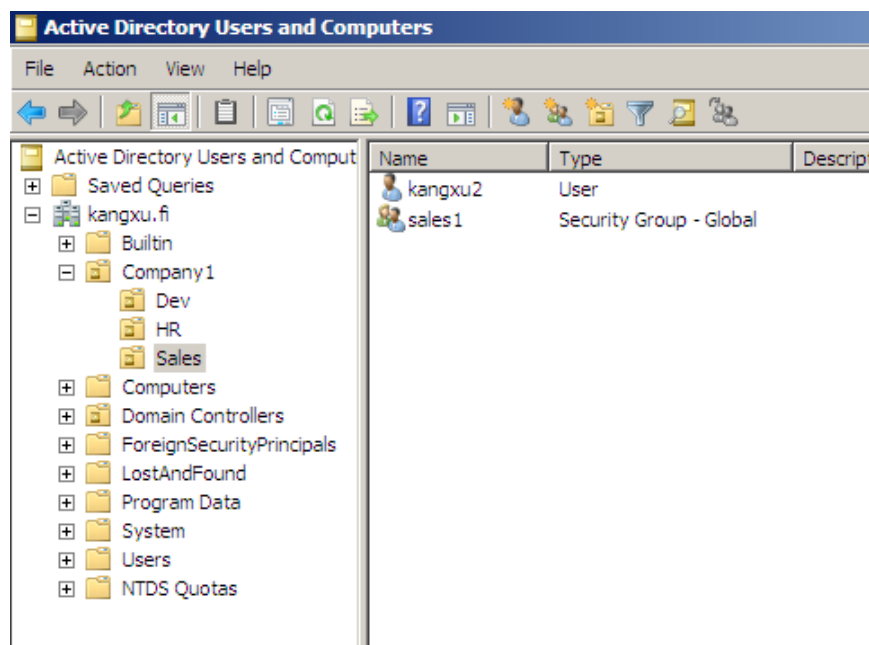
!                delete          literal          prompt          send
?                debug            ls               put             status
append          dir             mdelete         pwd             trace
ascii          disconnect     nmdir           quit            type
bell           get            nget            quote           user
binary         glob           mkdir           recv            verbose
bye            hash           nls             remotehelp
cd             help           mput            rename
close          lcd            open            rmdir
ftp>

```

Kuva 17. FTP-yhteys yhdistyi.

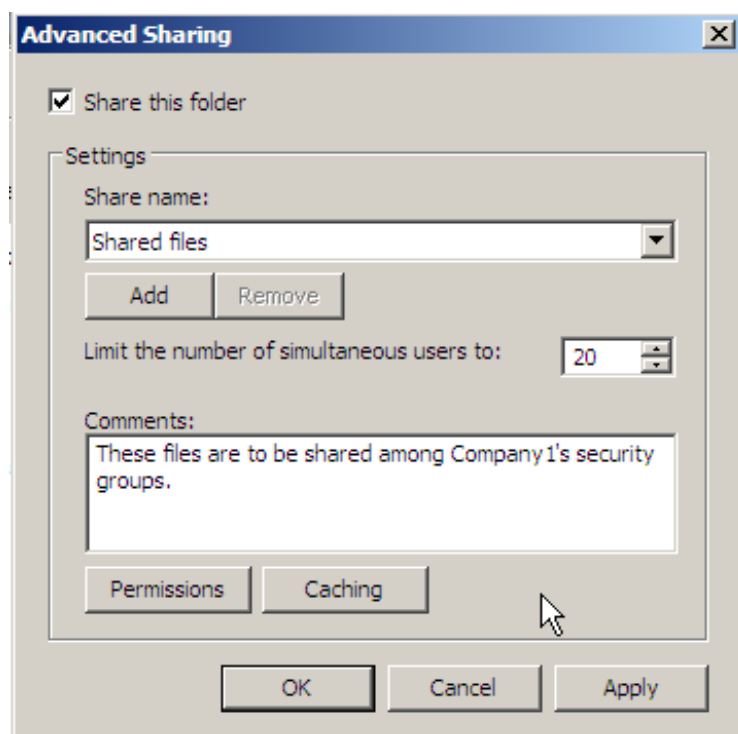
5.2.5 Tiedostojen jako-oikeuksien määrittely

Aktiivihakemistossa luotiin *kangxu.fi*-verkkoon organisaatioyksikkö nimeltään "*Company1*", joka sisältää kolme alioorganisaatioyksikköä, joiden nimet ovat "*Dev*", "*HR*" ja "*Sales*". Näiden alioorganisaatioyksikköiden sisään luotiin vastaavasti ryhmät "*Dev1*", "*HR1*" ja "*Sales1*". Näillä luoduilla ryhmillä hallinnoidaan ryhmäkäytännön avulla ryhmäjäsenien oikeuksia *kangxu*-verkossa. Dev1-ryhmään lisättiin käyttäjä kangxu4, HR1-ryhmään käyttäjä kangxu3 ja Sales1-ryhmään käyttäjä kangxu2. Näillä käyttäjillä eri ryhmissä testattiin tiedostojen jako-oikeuksia (kuva 18).



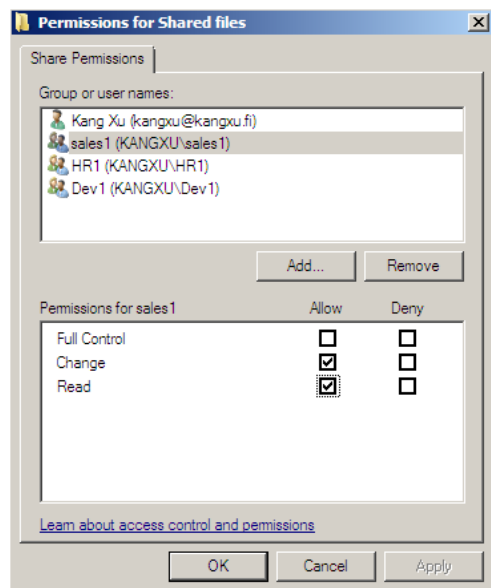
Kuva 18. Aktiivihakemistoon luodut organisaatioyksiköt, ryhmät ja käyttäjät.

Dcsrv1-palvelimella otettiin "File sharing"-ominaisuus eli tietostojen jako käyttöön. Tämän jälkeen luotiin kansio C:\Shared files, jossa pidetään jaettavat tiedostot. Yhtäaikaaisesti sallitaan ainoastaan 20 käyttäjää, jottei sisäverkko ja dcsrv1-palvelin jumittuisivat liiallisesta yhtäaikaisestä käytöstä (kuva 19).



Kuva 19. Shared files -kansion jakoasetukset.

Oikeuksia jaettiin ryhmille siten, että Sale1-ryhmä saa "Change"- ja "Read"-oikeudet. Näillä oikeuksilla kaikki Sales1-ryhmän käyttäjät voivat muokata Shared files -kansion kaikki tiedostot, mutta eivät voi muuttaa niiden käyttöoikeuksia. Käyttöoikeuksien hallintaan vaaditaan "Full Control"-oikeutta. HR1- ja Dev1-ryhmille annetaan ainoastaan "Read"-oikeus, jolla sallitaan ainoastaan lukuoikeus (kuva 20). Ainoastaan Kang Xu -käyttäjätillä, jota luotiin, kun otettiin AD DC -palvelua käyttöön, on "Full Control" -oikeus käytössä. Tämä johtuu siitä, että kyseinen käyttäjä kuuluu Domain Administrator -käyttäjäryhmään, jolla on eniten oikeuksia koko kangxu.fi-verkossa.



Kuva 20. Jako-oikeuksien hallinnointi.

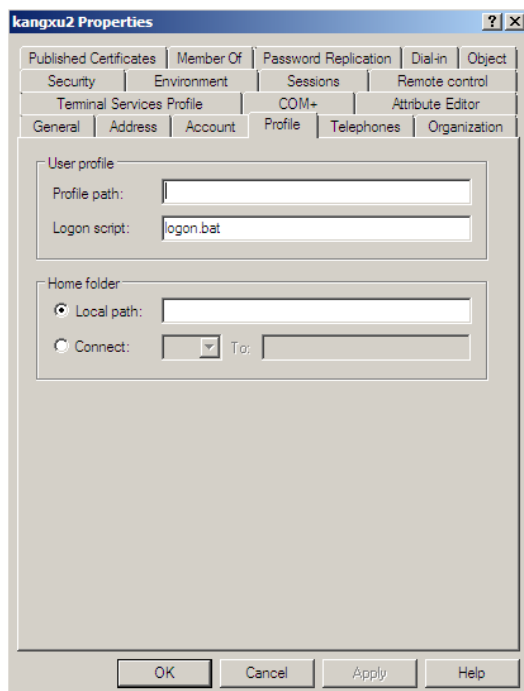
Jako-oikeuksien toimivuutta testattiin kangxu2-, kangxu3- ja kangxu4-käyttäjätileillä. Kangxu2-käyttäjällä pystyttiin muokkaamaan, poistamaan, tallentamaan, luomaan ja lukemaan Shared files -kansion kaikki tiedostot onnistuneesti. Kangxu3- ja kangxu4-käyttäjätileillä pystyttiin ainoastaan lukemaan ja näkemään Shared files -kansion tiedostot. Testausta suoritettiin Windows XP -tietokoneella, jolla vuorotellen kirjaututtiin *kangxu.fi*-verkkoon kaikilla käyttäjätileillä.

5.2.6 Kirjautumiskomentosarjan määrittely käyttäjäkoneelle

Kirjautumiskomentosarjalla (logon script) voidaan määrittää tietokone suorittamaan tiettyä tehtävää käynnistytettäessä tai liittyttäessä tiettyyn verkkoon. Kirjautumiskomentosarja luotiin Notepad-ohjelmalla ja se tallennettiin "logon.bat"-tiedostoksi polulle C:\Windows\SYSTEM32\sysvol\kangxu.fi\scripts. Tämä kansio on ohjauskoneen Netlogon-oletuskansio. Kun kirjautumiskomentosarjaa määritetään tietylle käyttäjälle tai ryhmälle, niitä haetaan suoraan tästä kansioista.

Kirjautumiskomentosarja sisältää ainoastaan komennon "*gpupdate*", jolla käyttäjä sisäänkirjautuessaan kangxu.fi-verkkoon päivittää kaikki itseään vaikuttavat

ryhmäkäytännöt. Kirjautumiskomentosarja määritettiin kangxu2-käyttäjättilille (kuva 21).



Kuva 21. Logon.bat -tiedosto määritettiin kangxu2-käyttäjättilille.

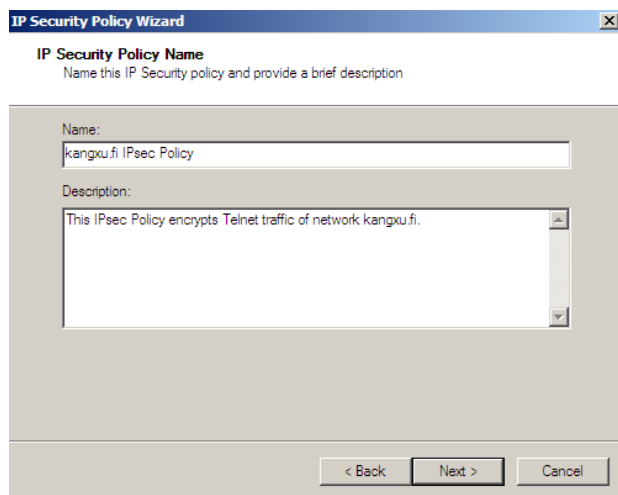
Logon.bat-tiedostoa testattiin kirjautumalla kangxu2-käyttäjättiliin Windows XP-tietokoneella. Työpöydän ilmantuessa huomattiin, että kyseistä kirjautumiskomentosarja suoritettiin onnistuneesti.

5.2.7 IPsec-protokollan määrittäminen

Testiympäristössä testattiin IPsec-protokollan käyttöä salaamalla Telnet-yhteyttä srv2:n ja srv3:n välillä. Toisena testinä luotiin koko verkkoa kattava IPsec-tietoturvaratkaisu, jolla salattiin kaikki verkkoliikenteet Windows Server 2008 -käyttöjärjestelmän IPsec -oletusasetuksella.

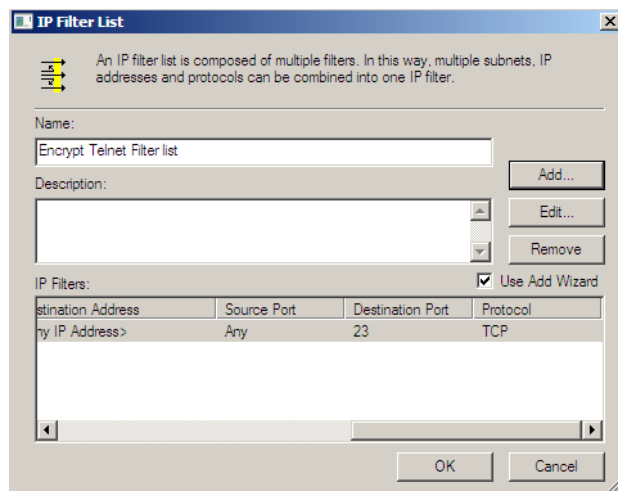
Sekä dcsrv1- että srv2- palvelimiin otettiin manuaalisesti Telnet-palvelu käyttöön. Telnet-palvelun käyttö muutettiin "Automatic :iksi", jotta se käynnistyy automaattisesti aina kun palvelimet käynnistyvät.

Dcsrv1-palvelimeen luotiin GPM (Group Policy Management) -konsolilla uusi GPO (Group Policy) -määrittely, jotka kutsutaan myös ryhmäkäytännöksi. Tämä luotu GPO toimii ainoastaan *kangxu.fi*-verkossa ja sen aliverkoissa. IPsec GPO:n luonnin jälkeen muutettiin käytännön ominaisuutta luomalla uuden IPsec-käytäntö tulevalle IPsec-määrittelykselle. IPsec-käytännölle annettiin nimeksi *kangxu.fi IPsec Policy* (kuva 22). Tämän jälkeen luotiin uuden IPsec-sääntö ja IPsec-suodatin, joilla turvataan kaikki halutut tietoliikenteet verkossa.



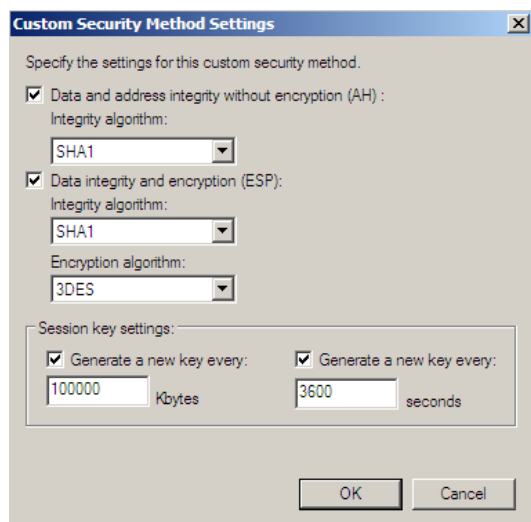
Kuva 22. Uusi IPsec-käytäntö.

Suodatinta määritettiin niin, että se vastaanottaa ainoastaan Telnet-liikenteen TCP-portista 23, joka on Telnet-liikenteen oletusportti (kuva 23).



Kuva 23. IPsec-käytännön suodatin määrittely.

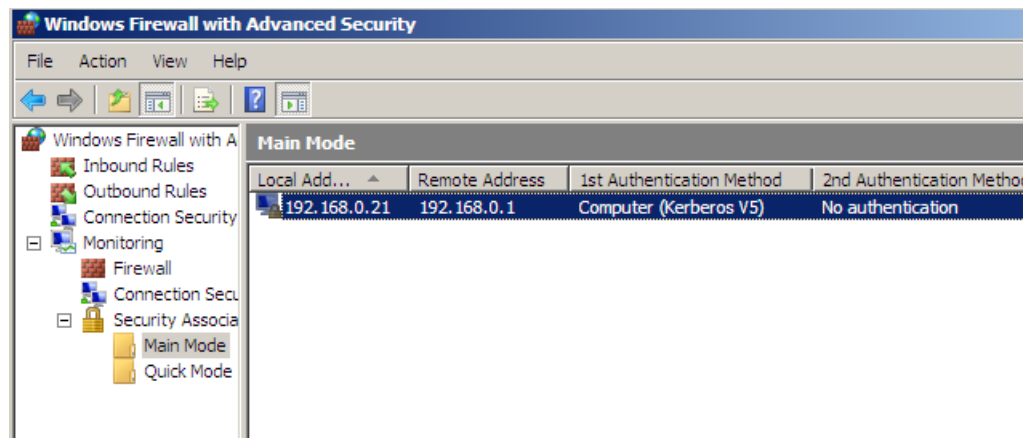
Suodattimelle määritettiin parametrit, joilla kohdellaan Telnet-liikennettä, kun sitä havaitaan. Kun Telnet-liikennettä huomataan, osoitteiden ja tiedostojen eheyden varmistamiseen käytetään SHA1 (Secure Hash Algorithm 1) -algoritmiä ja tiedostojen salaamiseen 3DES (3 Data Encryption Standard) -salausfunktiota. Uusia IPsec-avaimia generoidaan joka 3600 sekunnin eli tunnin välein tai kun Telnet-liikenteessä ylittyy 100 000 kilotavua (KB) eli 100 megatavua (MB) (kuva 24). Nämä ovat Windows Server 2008 -käyttöjärjestelmän oletusasetukset. Asetukset voidaan muuttaa ilman, että määrittystä tarvitaan ottaa pois käytöstä.



Kuva 24. Määritetyt parametrit IPsec-suodattimelle, kun Telnet-liikennettä havaitaan.

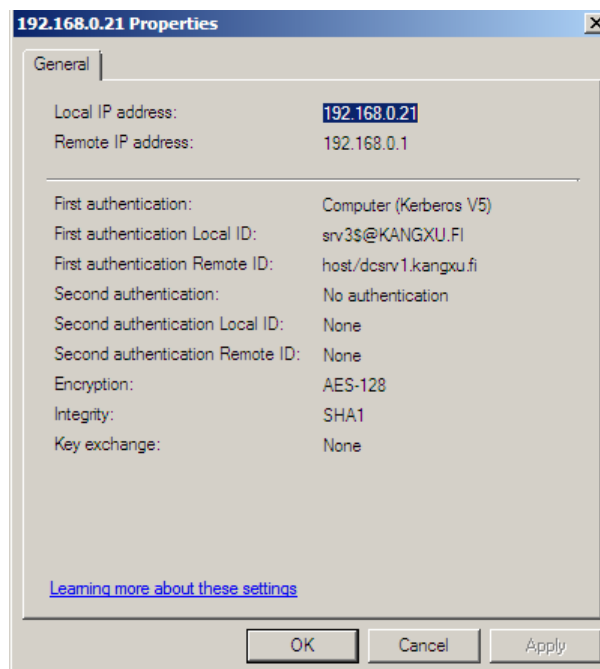
Uusi ryhmäkäytäntö luotiin kaiken muun verkkoliikenteen salaamiseksi. Tämän käytännön säännöksi eli "*rule .ksi*" valittiin "*Isolation*", koska halusin, että yhteyksiä rajoitetaan todennusmenetelmän perusteella, kuten esimerkiksi verkon käyttäjätunnuksen perusteella. Todennuksen pakollisuudessa otettiin käyttöön vaihtoehto "*Request authentication for inbound and outbound connections*". Tällä vaihtoehdolla voidaan käyttää todennusmenetelmää aina kun on mahdollista, mutta se ei ole pakollista. Todennusmenetelmäksi valittiin Windows Server 2008 -käyttöjärjestelmän oletusasetus eli "*Default*"-asetus. Asetuksella käytetään valmiiksi määritettyä todennusmenetelmää. Nämä asetukset pätevät kaikkeen verkkoliikenteeseen *kangxu.fi*-verkossa lukuun ottamatta Telnet-liikennettä.

Seuraavaksi testattiin juuri luodun säännön toimivuutta luomalla *ping*-liikennettä verkossa. Tämän jälkeen tarkistettiin srv3:ssa olevasta *Windows Firewall with Advanced Security* -konsolista, että juuri luotu liikenne on salattu (kuva 25).



Kuva 25. Salattu *ping*-liikenne.

Kuva 26 näyttää *ping*-komennon tuottaman SA (Security Associate) -attribuutin yksityiskohtaisesti. Tarkemmin sanottuna *ping*-paketin salaukseen käytettiin AES-128-salausta, ja eheyteen SHA1-algoritmia.



Kuva 26. SA-attribuutti *ping*-liikenteestä.

6 Yhteenveto

Insinööritöön tavoitteena oli rakentaa pieni- tai keskikokoiselle yritykselle toimiva sisäverkko tietoturvaratkaisuineen perustuen Windows Server 2008 -käyttöjärjestelmään.

Teoriaosuudessa eniten työtä tuottivat työn rakenne, järjestys ja sisältö. Työni sisälsi DHCP-, DNS-, AD DS- ja IIS-palvelut sekä tietoturvallisuusratkaisut Windows Server -verkkoympäristössä, joista jokainen aihe olisi ansainnut oman työnsä. Koska valitsemani aihe oli sen verran laaja, kaikkia aiheita ja teoriaa palvelujen käytöstä ei ollut mahdollista kirjoittaa kovinkaan pitkästi ja syvällisesti, mutta kuitenkin sen verran, että vähänkin IP-verkkoihin perehtyneelle lukijalle käytännön osuuden ymmärtäminen on helppoa teoriaosuuden läpilukemisen jälkeen.

Käytäntöosiossa ensimmäisessä vaiheessa Windows Server 2008 -käyttöjärjestelmän asennus ja tietokoneiden sijoittaminen samaan aliverkkoon oli hyvin yksinkertaista ja eteni ilman suurempia ongelmia. Toisessa vaiheessa yksittäisten palveluiden asennukset veivät eniten aikaa koko työssä, mutta asennukset ja määrittelyt etenivät kuitenkin hyvin hallitusti ja alkuperäisen suunnitelman mukaisesti. Kokeilin palvelujen erilaisten ominaisuuksien tarjoamia ratkaisuja ja mahdollisuuksia, minkä takia monet palvelujen asennukset menivät uusiksi käytäntöosion edetessä. Tämä johtui siitä, että halusin saada aidon tuntuksen ja tietoturvallisen, mutta samalla helposti hallinnoitavan sisäverkkorakenteen ja -ympäristön.

Windows Server 2008 -käyttöjärjestelmä on tehty mahdollisimman helposti hallinnoitavaksi verkkoylläpitäjille, ja sen palvelujen ja sovelluksien käyttöönotto on yksinkertaisempaa, helpompaa ja selkeämpää kuin Microsoftin edellisissä Windows Server -käyttöjärjestelmissä. Sen uudet palvelut ja ominaisuudet ovat tuoneet lisää vakautta ja parempaa tietoturvaa palvelimille verkkoympäristössä. Kaiken kaikkiaan voin todeta, että Windows Server 2008 -käyttöjärjestelmä on hyvin tehty ja toteutettu palvelinkäyttöjärjestelmäkokonaisuus.

Erilaisten palvelujen ja tietojen kerääminen ja soveltaminen järkevissä järjestyksissä yhdeksi kokonaisuudeksi oli varsin aikaavievä prosessi, mutta jälkeenpäin voin todeta

oppineeni paljon uutta Microsoftin viimeisimmästä Windows Server
-käyttöjärjestelmästä ja sen käytöstä.

7 Lähteet

- 1 Darril Gibson: MCITP Windows Server 2008 Server Administrator. Indianapolis: Wiley Publishing, Inc., 2008.
- 2 Server Core Installation Option Getting Started Guide. (WWW-dokumentti.) Microsoft Corporation. <http://technet.microsoft.com>. Luettu 26.11.2010.
- 3 Windows Server 2008 Operation System. (WWW-dokumentti.) <http://www.operating-system.org>. Luettu 25.11.2010.
- 4 IPv6 - The Next Generation Internet. (WWW-dokumentti.) www.ipv6.com. Luettu 28.11.2010.
- 5 Microsoft Vista and IPv6. (WWW-dokumentti.) www.ipv6.com. Luettu 28.11.2010.
- 6 Windows Server 2008 and IPv6. (WWW-dokumentti.) www.ipv6.com. Luettu 28.11.2010.
- 7 Sam Reimer & Mike Mulcare: Windows Server 2008 Active Directory Resource Kit. Washington: Microsoft Press, 2008.
- 8 Dan Holme: Self-paced Training Kit (Exam 70-640): Configuring Windows Server 2008 Active Directory. Washington: Microsoft Press, 2008.
- 9 DNS Hierarchy. (WWW-dokumentti.) <http://www.inetdaemon.com>. Luettu 3.12.2010.
- 10 Understanding DNS Zones. (WWW-dokumentti.) <http://www.tech-faq.com>. Luettu 3.12.2010.
- 11 DNS Resolution. (WWW-dokumentti.) <http://docsrv.sco.com>. Luettu 4.12.2010.
- 12 Dynamic Host Configuration Protocol. (WWW-dokumentti.) <http://technet.microsoft.com>. Luettu 8.12.2010.
- 13 Planning Your IIS Architecture. (WWW-dokumentti.) <http://learn.iis.net>. Luettu 11.12.2010.
- 14 Windows Firewall with Advanced Security and IPsec. (WWW-dokumentti.) <http://technet.microsoft.com>. Luettu 12.12.2010.

- 15 Windows Server Update Services. (WWW-dokumentti.)
<http://technet.microsoft.com>. Luettu 14.12.2010.
- 16 Windows Server 2008 System Requirements. (WWW-dokumentti.)
<http://msdn.microsoft.com>. Luettu 25.11.2010.
- 17 Security and Policy Enforcement. (WWW-dokumentti.) www.microsoft.com. Luettu 25.11.2010.